Съюз на математиците в България

МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ

Доклади на Петдесет и петата пролетна конференция
на Съюза на математиците в България
Трявна, 5 – 9 април 2026 г.

Част 1

Union of Bulgarian Mathematicians

MATHEMATICS AND EDUCATION IN MATHEMATICS

Proceedings of the Fifty-Fifth Spring Conference
of the Union of Bulgarian Mathematicians
Tryavna, April 5 – 9, 2026

Part 1

Докладите се издават със съдействието на
Института по математика и информатика при БАН
и Академия „Питагор“, част от Училище по математика „Питагор“

FIFTY-FIFTH SPRING CONFERENCE
OF THE UNION OF BULGARIAN MATHEMATICIANS

Tryavna, April 5 – 9, 2026

Program committee:

Chair:
Prof. Tsonka Baicheva, D.Sc. (IMI – BAS)

Secretaries:
Chief Assist. Prof. Nikolay I. Nikolov, Ph.D. (IMI – BAS)
Assoc. Prof. Milen Borisov, Ph.D. (IMI–BAS)
Assoc. Prof. Borislava Kirilova, Ph.D. (Sofia University)

Members:
Acad. Petar Kenderov (IMI – BAS)
Acad. Oleg Mushkarov (IMI – BAS)
Prof. Nikolai Nikolov, D.Sc., Corr. Member of the Bulg. Acad. Sci. (IMI–BAS)
Prof. Peter Boyvalenkov, D.Sc., Corr. Member of the Bulg. Acad. Sci. (IMI–BAS)
Prof. Stepan Terzian, D.Sc. (Rousse University)
Prof. Stoyan Kapralov, D. Sc. (UBM Gabrovo)
Prof. Boyan Zlatanov, Ph.D. (Plovdiv University)
Prof. Maya Stoyanova, Ph.D. (Sofia University)
Prof. Stanislav Harizanov, Ph.D. (IICT and IMI – BAS)
Assoc. Prof. Krasimira Ivanova, Ph.D. (IMI – BAS)
Assoc. Prof. Parvan Parvanov, Ph.D. (Sofia University)
Assoc. Prof. Sevdalina Georgieva, Ph.D. (Technical University, Varna)
Assoc. Prof. Philip Petrov, Ph.D. (Sofia University)

Technical secretary:
Albena Vassileva (IMI – BAS)

Organizing committee:

Chair:
Mitko Kunchev (UBM Rousse)

Members:
Galina Bobeva, Ph.D. (Rousse Math School)
Tsvetana Kyumyurdjieva (Gabrovo Science and Math School)
Evelina Mincheva (Rousse Math School)
Anelia Angelova (Regional Dept. of Education, Rousse)
Kornelia Pashova (Gabrovo Science and Math School)
Velina Koeva (Gabrovo Science and Math School)
Albena Vassileva (IMI – BAS)
Ivanka Stoyanova (IMI – BAS)

Editorial board of the series:

Editor-in-chief:
Acad. Petar Kenderov

Acad. Oleg Mushkarov
Prof. Nikolai Nikolov, D.Sc., Corr. Member of the Bulg. Acad. Sci.
Prof. Peter Boyvalenkov, D.Sc. Corr. Member of the Bulg. Acad. Sci.
Prof. Ivan Landjev, D.Sc.
Albena Vassileva – secretary

Guest editor of Part 1 of the volume:
Assoc. Prof. Ivan Derzhanski, Ph.D. (IMI–BAS)

Layout editor:
Albena Vassileva

Print:
Pythagoras Private High School, Sofia

© Union of Bulgarian Mathematicians, 2026

ПЕТДЕСЕТ И ПЕТА
ПРОЛЕТНА КОНФЕРЕНЦИЯ
НА СЪЮЗА НА МАТЕМАТИЦИТЕ В БЪЛГАРИЯ
Трявна, 5 – 9 април 2026 г.

Програмен комитет:

Председател:
проф. дн Цонка Байчева (ИМИ – БАН)

Секретари:
гл. ас. д-р Николай И. Николов (ИМИ – БАН)
доц. д-р Милен Борисов (ИМИ – БАН)
доц. д-р Бориславa Кирилова (ФМИ – СУ)

Членове:
акад. Петър Кендеров (ИМИ – БАН)
акад. Олег Мушкаров (ИМИ – БАН)
чл.-кор. Николай Николов (ИМИ – БАН)
чл.-кор. Петър Бойваленков (ИМИ – БАН)
проф. дмн Степан Терзиян (РУ)
проф. дмн Стоян Капралов (СМБ Габрово)
проф. д-р Боян Златанов (ФМИ – ПУ)
проф. д-р Мая Стоянова (ФМИ – СУ)
проф. д-р Станислав Харизанов (ИИКТ и ИМИ – БАН)
доц. д-р Красимира Иванова (ИМИ – БАН)
доц. д-р Първан Първанов (ФМИ–СУ)
доц. д-р Севдалина Георгиева (ТУ – Варна)
доц. д-р Филип Петров (ФМИ–СУ)

Технически секретар:
Албена Василева (ИМИ – БАН)

Организационен комитет:

Председател:
Митко Кунчев (СМБ Русе)

Членове:
д-р Галина Бобева (МГ „Баба Тонка“ – Русе)
Цветана Кюмюрджиева (ПМГ „Акад. Иван Гюзелев“ – Габрово)
Евелина Минчева (МГ „Баба Тонка“ – Русе)
Анелия Ангелова (РУО – Русе)
Корнелия Пашова (ПМГ „Акад. Иван Гюзелев“ – Габрово)
Велина Коева (ПМГ „Акад. Иван Гюзелев“ – Габрово)
Албена Василева (ИМИ – БАН)
Иванка Стоянова (ИМИ – БАН)

Редакционна колегия на поредицата:

Главен редактор:
акад. Петър Кендеров

акад. Олег Мушкаров
чл.-кор. Петър Бойваленков
чл.-кор. Николай Николов
проф. дмн Иван Ланджев
Албена Василева – секретар

Гост-редактор на Част 1 на тома:
доц. д-р Иван Държански

Предпечатна подготовка:
Албена Василева

Печат:
ЧСУ „Питагор“, София

© Съюз на математиците в България, 2026

Формат: 1000 × 700/16	Дадена за печат на 23.03.2026 г.
Печатни коли 20	Подписана за печат на 24.03.2026 г.
Тираж 150	**ISSN 1313-3330** (Print), **2815-4002** (Online)

П Р Е Д Г О В О Р

През тази година град Трявна ще бъде домакин на 55-ото издание на пролетната конференция на Съюза на математиците в България. Ще бъде продължена повече от половинвековна традиция на СМБ – в началото на месец април да се събират учени от Българската академия на науките, университетски преподаватели, учители и изявени ученици в областта на математиката и информатиката от цялата страна, за да представят своите постижения и да дискутират върху актуални проблеми, свързани с развитието на научните изследвания и образованието в тези две области. Участието в конференцията дава възможност за създаване на нови контакти между колеги, неформални срещи за обмяна на идеи и възможности за съвместна работа.

В тазгодишното издание на конференцията ще бъдат отбелязани с доклади три 80-годишнини. Първият доклад ще бъде посветен на акад. Стефан Додунеков – световно признат български математик, създател на школата по Теория на кодирането в България. Бил е преподавател в различни български и чуждестранни университети, автор на книги, учебници и учебни пособия по математика за средните училища, директор на Института по математика и информатика и председател на Българска академия на науките, дългогодишен председател на СМБ и основател и президент на Математическото дружество на Югоизточна Европа. Вторият доклад ще отбележи юбилея на акад. Петър Попиванов. Основните научни интереси и публикации на акад. Попиванов са в областта на частните диференциални уравнения, като резултатите от неговите изследвания са публикувани в стотици научни статии. Акад. Попиванов има богата и разнообразна организационна дейност и широки литературни интереси, по-специално към творчеството на Достоевски. Третият доклад е посветен на проф. Аврам Ескенази. Той работи в областта на информатиката и информационните технологии и е един от пионерите в компютърно-базираното обучение у нас. Проф. Ескенази е водил над 90 курса в различни български университети.

В памет на проф. Иван Тонов, който ни напусна през 2025 година, с доклад ще бъде отбелязан неговия принос в теорията и практиката на преподаването на методи, стратегии и тактики за решаване на задачи от елементарната математика и за цялостното развитие и укрепване на състезателната математика в България.

На 80-годишнината от рождението на акад. Додунеков ще бъде посветен и минисимпозиум в рамките на конференцията. В работата му ще вземат участие учени от страната и чужбина, които ще представят свои последни разработки в области, в които е работил акад. Додунеков, или в нови направления на математиката и информатиката.

Пролетната конференция на СМБ има три основни секции, като и тази година ще бъде спазена традицията да бъдат представени доклади по покана в трите секции. В секция А – Математически структури, доклад ще изнесе М. Иванов. Ще бъде предложено ново доказателство на Ader характеризация на елипса с минимално Banach-Mazur разстояние до единичната окръжност на нормирана равнина по отношение на контактни и екстремални точки. В секция Б – Математическо моделиране и информатика, М. Добрева ще разгледа една нова тенденция за използването на дигитализираното културно-историческо наследство в училищното обучение по информатика. Докладът ще представи реални примери от международната практика

за интегриране на културното наследство в училищното обучение по информатика в контекста на засилването на компетенциите в STEM и проектно-базираното обучение, които илюстрират, че културното наследство може успешно да служи като контекст за развитие на алгоритмично мислене, работа с данни, дигитални умения и грамотност в областта на изкуствения интелект в училище. В секция В – Образование по математика и информатика, Н. Павлова ще разгледа добри практики в подготовката на учители по математика в епохата на изкуствения интелект. Ще бъдат представени данни относно мнението и стила на работа на бъдещите учители при прилагане на генеративен изкуствен интелект в работата им, както и някои добри практики. Освен докладите по покана, ще бъдат представени и 3 научни доклада в секция А, 6 в секция Б и 13 в секция В.

Традиционно в рамките на конференцията се организират семинари за учители. Тази година те ще бъдат два. Темата на първия семинар е „STEAM работилница „Математика във Варненския некропол“, V хилядолетие преди Христа“ и ще бъде воден от Т. Маринова, Н. Борисова и С. Георгиева. Във втория семинар, “Електронни ресурси за профилирана подготовка по математика – модул „Вероятности и анализ на данни“, М. Божкова и Д. Григорова ще запознаят аудиторията с разработените от тях електронни ресурси, предназначени да подпомогнат преподаването и усвояването на материала по вероятности и анализ на данни, изучаван в модули 3 и 4 на профилираната подготовка по математика.

В три дискусии ще се обсъждат актуални проблеми на съвременното образование. Първата дискусия е посветена на възможностите, ограниченията и предизвикателствата на изкуствения интелект в образованието. Във втората ще се дискутира ролята на математиката в STEM образованието в България. Третата дискусия ще се фокусира върху формàта на изпитите по математика за Националното външно оценяване в 7. клас. В програмата на конференцията е предвидено и представяне на института INSAIT и програмата Explorer. Ще се проведе и традиционната Ученическа секция на Ученическия институт по математика и информатика, на която ще бъдат представени изследователски проекти на ученици по математика, информатика и информационни технологии.

Благодарна съм на председателя на СМБ акад. Ю. Ревалски и на членовете на Програмния комитет за положените усилия и за съдействието по изготвянето на програмата на конференцията, както и на членовете на Организационния комитет за организацията. Специални благодарности за тримата секретари на научните секции – гл. ас. Н. Николов (ИМИ-БАН), доц. М. Борисов (ИМИ-БАН) и доц. Б. Кирилова (ФМИ-СУ) за цялостната работа по рецензирането на предложените за участие в конференцията доклади и на техническия секретар А. Василева за всеотдайността, с която подготви съобщенията за конференцията, осъществи комуникацията с авторите и основната част от изготвянето на научната програма, както и предпечатната подготовка на тома на конференцията.

Желая ползотворна работа на всички участници в 55-ата Пролетна конференция на СМБ!

Велико Търново, 09.03.2026 г.

проф. дн Цонка Байчева
Председател на Програмния комитет
на 55. Пролетна конференция на СМБ

ДОКЛАДИ ПО ПОКАНА

INVITED TALKS

МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2026
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2026
Proceedings of the Fifty-Fifth Spring Conference
of the Union of Bulgarian Mathematicians
Tryavna, Bulgaria, April 5–9, 2026

ON THE BANACH-MAZUR ELLIPSE

V. D. Babev[1], M. Ivanov[2], R. Nikolov

[1] Faculty of Mathematics and Informatics, Sofia University "'St. Kliment Ohridski"', Sofia, Bulgaria

[2] Radiant Life Technologies Ltd., Nicosia, Cyprus

e-mails: [1] babev@fmi.uni-sofia.bg, [2] milen@radiant-life-technologies.com

We provide a new proof of Ader's [1] characterisation of the ellipse of minimal Banach-Mazur distance to the unit circle of a normed plane in terms of contact and extremal points. Our method reveals the relation of this problem to the Chebyshev alternance.

Keywords: Banach-Mazur distance, normed plane, distance ellipse, Chebyshev alternance

ЕЛИПСА НА БАНАХ-МАЗУР

В. Д. Бабев[1], М. Иванов[2], Р. Николов

[1] Факултет по математика и информатика, Софийски университет „Св. Климент Охридски“, София, България

[2] Radiant Life Technologies Ltd., Никозия, Кипър

emails: [1] babev@fmi.uni-sofia.bg, [2] milen@radiant-life-technologies.com

Представяме ново доказателство на характеризацията на Адер за елипсата с минимално разстояние на Банах–Мазур до единичната окръжност на нормирана равнина, която характеризация е, че контактните и екстремалните точки имат определено свойство, подобно на алтернанс. Нашият метод явно посочва връзката с чебишовия алтернанс.

Ключови думи: разстояние на Банах-Мазур, нормирана равнина, елипса на най-добро приближение, чебишов алтернанс

https://doi.org/10.55630/mem.2026.55.009-018

2020 Mathematics Subject Classification: Primary 46B20; Secondary 52A10, 41A50.

[1] Research partially supported by Grant No. 80-10-116 from 28.05.2025 of the Research Fund of Sofia University.

[2] Research partially supported by the Bulgarian National Science Fund under Grant No. KP-06-H92/6 (December 8, 2025).

1 Introduction

Recall that the Banach-Mazur distance between the isomorphic normed spaces X and Y is denoted by

$$d(X,Y) := \inf\{\|T\| \cdot \|T^{-1}\| :\ T : X \to Y \text{ isomorphism}\}, \tag{1}$$

for details see e.g. [13, Section 6.1.1].

If X and Y are of one and the same finite dimension, then the minimum in (1) is attained.

An important characteristic of a finite dimensional space is its distance to the Euclidean space. Here we study this characteristic in the simplest case: the plane.

So, for a 2-dimensional normed space $(X, \|\cdot\|)$

$$d_2(X) := d(X, \mathbb{R}^2),$$

where $\mathbb{R}^2$ is considered with the standard Euclidean norm $|\cdot|$. It is easy to check that

$$d_2(X) = \min\{\|T\| :\ T : X \to \mathbb{R}^2,\ T(B_X) \supset B_{\mathbb{R}^2}\}, \tag{2}$$

where B_X and S_X stand for the unit ball and the unit sphere of X respectively. Indeed, $T(B_X) \supset B_{\mathbb{R}^2}$ is equivalent to $\|T^{-1}\| \le 1$, so we have that $d_2(X)$ is at most the right-hand side of (2). On the other hand, multiplying the operator T by a real constant does not change $\|T\| \cdot \|T^{-1}\|$, so we may assume that $\|T^{-1}\| = 1$ in (1).

Using *polar decomposition*, we can reduce (2). Note that if U is in $\mathbf{O}(2)$ – the group of isometries of $\mathbb{R}^2$, that is, $U^{-1} = U^t$ if considered as a matrix – then $\|UT\| = \max\limits_{x \in S_X} |UTx| = \max\limits_{x \in S_X} |Tx| = \|T\|$, and similarly $\|T^{-1}U^{-1}\| = \|T^{-1}\|$, so we can quotient by $\mathbf{O}(2)$. Denote by $\mathbf{PD}(X, \mathbb{R}^2)$ the operators from X to $\mathbb{R}^2$ that are positive definite symmetric matrices in any basis. By [4, Theorem 7.3.1, p.449] each isomorphism $T : X \to \mathbb{R}^2$ can be represented as $T = UT_1$, where $U \in \mathbf{O}(2)$ and $T_1 \in \mathbf{PD}(X, \mathbb{R}^2)$. Therefore,

$$d_2(X) = \min\{\|T\| :\ T \in \mathbf{PD}(X, \mathbb{R}^2),\ T(B_X) \supset B_{\mathbb{R}^2}\}. \tag{3}$$

We prove in a new way the following characterisation, which is essentially contained in [1, 10].

Theorem 1. Let $\dim X = 2$. There is a unique $\hat{T} \in \mathbf{PD}(X, \mathbb{R}^2)$ such that $\hat{T}(B_X) \supset B_{\mathbb{R}^2}$ and

$$\|\hat{T}\| = d_2(X). \tag{4}$$

$\hat{T}$ is characterised by the following property:

There are $x_i \in S_X$, $i = 1, 2$, with $x_1 \ne \pm x_2$, and $y_i \in S_X$, $i = 1, 2$, with $y_1 \ne \pm y_2$, such that:

$$|\hat{T}x_i| = \|\hat{T}\|, \quad i = 1, 2, \tag{5}$$

$$|\hat{T}y_i| = 1, \quad i = 1, 2, \tag{6}$$

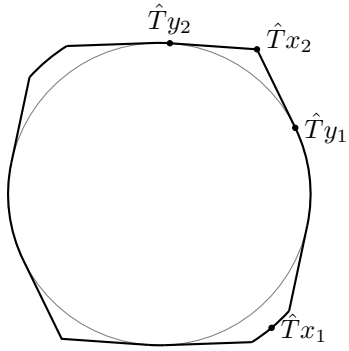
$$y_1 \in \operatorname{cone}\{x_1, x_2\}, \quad y_2 \in \operatorname{cone}\{-x_1, x_2\}. \tag{7}$$

Here

$$\operatorname{cone}\{x, y\} := \{\alpha x + \beta y :\ \alpha, \beta \ge 0\}.$$

Note that the condition characterising the optimal operator depends only on the operator itself and not on $d_2(X)$. This is to be expected, because the problem suitably stated is convex. Not strictly convex, however, so the uniqueness is not immediate.

As an illustration, consider the following picture.



From it we can also see one important, but immediate, corollary. Since one of the angles between $\hat{T}y_1$ and $\hat{T}y_2$, and between $\hat{T}y_2$ and $-\hat{T}y_1$ (say the one between $\hat{T}y_1$ and $\hat{T}y_2$ as on the picture) will be $\leq \pi/2$; and since $\hat{T}x_2$ will be within the angle between the tangents to the unit circle at $\hat{T}y_1$ and $\hat{T}y_2$, due to convexity, the distance from $\hat{T}x_2$ to zero, that is $d_2(X)$, is at most $\sqrt{2}$. Therefore,

$$d_2(X) \leq \sqrt{2}.$$

Note that Theorem 1 easily follows from
Ader's Non-separation Principle ([1]). For the unique $\hat{T}$ there is no angle such that all points $x \in S_X$ with $|\hat{T}x| = \|\hat{T}\|$ are inside this angle and all points $y \in S_X$ with $|\hat{T}y| = 1$ are outside.

Here, an angle is

$$\operatorname{cone}\{a, b\} \cup \operatorname{cone}\{-a, -b\}$$

for some $a, b \in \mathbb{R}^2$.

The original work [1] states that there should be at most 4 points realising Ader's Non-separation Principle, and for these 4 points it is then clear that the alternance described in Theorem 1 must be in place. By Maurey's result [10], see also [3], the ellipse of minimal Banach-Mazur distance is unique, which yields the uniqueness part of Theorem 1.

Obviously, the problem can be re-stated more geometrically like: find the minimal $k \geq 1$ such that there is an ellipse inscribed in B_X whose homothetic image with ratio k is circumscribed about B_X. We will actually be using this form below, but we mention it here to point out the relationship to the celebrated Löwner–John ellipse, see e.g. [7], that is, the ellipse of maximal area inscribed in B_X. The Löwner–John ellipsoid is extensively used for estimating the Banach-Mazur distance to Euclidean space, probably because Ader's result [1] had apparently been forgotten until Grundbacher and Kobos recently unearthed it, see [3].

However, if B_X is not symmetric, the estimate through the Löwner–John ellipsoid can grow progressively worse with the dimension. Consider $\mathbb{R}^n$ and let B_{X_n} be the convex hull of $B_{\mathbb{R}^n}$ and $\pm\sqrt{n}e$, where $e \in S_{\mathbb{R}^n}$. Then $B_{\mathbb{R}^n}$ is the Löwner–John ellipsoid for B_{X_n}, see [14] for a nice and simple proof, so it gives only the generic estimate $\sqrt{n}$. On the other hand, by the rotational symmetry of B_{X_n} around the axis through e, $d(X_n, \mathbb{R}^n) \leq \sqrt{3}$.

Our interest in the specifically two-dimensional case comes from our previous works [6, 5, 11, 12]. Of course, similar problems can also be considered in different metrics, like e.g. Hausdorff, see [8, 2, 9].

In conclusion, note that the convexity of B_X will not be used at all in the proofs

below, which is not surprising, as they go through Chebyshev approximation.

2 An equivalent problem in polar co-ordinates

In view of (3), Theorem 1 characterises the solution of the optimisation problem

$$\begin{cases} \|T\| \to \min \\ T \in \mathbf{PD}(X, \mathbb{R}^2), \quad \|T^{-1}\| \le 1. \end{cases}$$

By substituting T^{-1} in place of T, this problem can be rewritten as

$$\begin{cases} \|T^{-1}\| \to \min \\ T \in \mathbf{PD}(\mathbb{R}^2, X), \quad \|T\| \le 1, \end{cases} \tag{8}$$

which is more suited for our purposes. Theorem 1 is immediately equivalent to the following Proposition 1 with which we will be working from now on.

Proposition 1. The only solution to (8), say $\tilde{T}$, is characterised by the following property:

There are $u_i, v_i \in S_{\mathbb{R}^2}$, $i = 1, 2$, with $u_1 \neq \pm u_2$, $v_1 \neq \pm v_2$, $v_1 \in \operatorname{cone}\{u_1, u_2\}$, $v_2 \in \operatorname{cone}\{-u_1, u_2\}$, and

$$\|\tilde{T}u_i\| = 1/\|\tilde{T}^{-1}\|, \quad \|\tilde{T}v_i\| = 1, \quad i = 1, 2. \tag{9}$$

Let a co-ordinate system be fixed in X in which

$$S_X = \{r(\varphi)(\cos\varphi, \sin\varphi) : \ \varphi \in \mathbb{R}\}, \tag{10}$$

for a strictly positive, π-periodic and continuous $r : \mathbb{R} \to \mathbb{R}^+$.

In these fixed coordinates each $T \in \mathbf{PD}(\mathbb{R}^2, X)$ is identified with a matrix

$$T = \begin{pmatrix} a & b \\ b & c \end{pmatrix}, \quad a, c > 0, \quad \det T = ac - b^2 > 0.$$

Obviously,

$$x \in T(S_{\mathbb{R}^2}) \iff |T^{-1}x| = 1 \iff x^t T^{-2} x = 1.$$

That is, $T(S_{\mathbb{R}^2})$ is the ellipse:

$$a_1 x_1^2 + 2b_1 x_1 x_2 + c_1 x_2^2 = 1,$$

where

$$\begin{pmatrix} a_1 & b_1 \\ b_1 & c_1 \end{pmatrix} = T^{-2},$$

so $a_1, c_1 > 0$ and $b_1^2 < a_1 c_1$. In polar co-ordinates then $T(S_{\mathbb{R}^2}) = \{\rho(\varphi)(\cos\varphi, \sin\varphi) : \varphi \in \mathbb{R}\}$, where

$$\rho^{-2}(\varphi) = a_2 + b_2 \cos 2\varphi + c_2 \sin 2\varphi, \tag{11}$$

with $a_2 = (a_1 + c_1)/2$, $b_2 = (a_1 - c_1)/2$ and $c_2 = b_1$, so

$$a_2 > 0, \quad a_2^2 > b_2^2 + c_2^2. \tag{12}$$

Usually this is expressed in terms of $\cos 2(\varphi - \theta)$, where θ is the tilt angle. Let $\mathcal{E}$ be the family of all ellipses in polar co-ordinates, that is, all curves in the form (11) for all values of the parameters a_2, b_2, c_2 which satisfy (12). It is clear that the cone (12) parametrises one-to-one the ellipses, as well as $\mathbf{PD}(\mathbb{R}^2, X)$, which we will use when establishing the uniqueness part of our main result. Let

$$\mathcal{C} := \{\log\rho : \ \rho \in \mathcal{E}\}. \tag{13}$$

Let also, see (10),

$$f := \log r.$$

Since $\|T\| \le 1$ is equivalent to $T(S_{\mathbb{R}^2}) \subset B_X$, which in polar co-ordinates translates to

$$\rho \le r \iff g := \log \rho \le f,$$

the constraint in (8) becomes $g \in \mathcal{C}$, $g \le f$. For the objective, since $\rho(\varphi)(\cos\varphi, \sin\varphi) \in T(S_{\mathbb{R}^2})$, we have $|T^{-1}(\rho(\varphi)(\cos\varphi, \sin\varphi))| = 1$, hence $|T^{-1}(\cos\varphi, \sin\varphi)| = 1/\rho(\varphi)$. For $x = r(\varphi)(\cos\varphi, \sin\varphi) \in S_X$,

$$|T^{-1}x| = \frac{r(\varphi)}{\rho(\varphi)} = \exp(f(\varphi) - g(\varphi)),$$

and the problem (8) is equivalent to

$$\begin{cases} \max\limits_{\varphi} \exp(f(\varphi) - g(\varphi)) \to \min \\ g \in \mathcal{C}, \quad g \le f. \end{cases}$$

Since the exponential is strictly monotonically increasing, Proposition 1 is equivalent to Proposition 2 below. There, for a π-periodic function h

$$\|h\|_\infty := \max_{\varphi} |h(\varphi)|.$$

Proposition 2. The optimisation problem

$$\begin{cases} \|f - g\|_\infty \to \min \\ g \in \mathcal{C}, \quad g \le f \end{cases} \tag{14}$$

has a unique solution $\bar{g}$ characterised by the following property:

There are points

$$\varphi_1 < \psi_1 < \varphi_2 < \psi_2 < \varphi_1 + \pi \tag{15}$$

such that for $i = 1, 2$

$$f(\varphi_i) - \bar{g}(\varphi_i) = \|f - \bar{g}\|_\infty \text{ and } \bar{g}(\psi_i) = f(\psi_i). \tag{16}$$

We will prove this proposition in the next section.

3 Chebyshev Alternance of second order on the circle

Let $C_\pi(\mathbb{R})$ be the Banach space of all continuous π-periodic functions on $\mathbb{R}$ with the norm $\|\cdot\|_\infty$.

Let $\mathfrak{R}$ be the function that maps the triple $(a, b, c) \in \mathbb{R}^3$ to $\mathfrak{R}(a, b, c) \in C_\pi(\mathbb{R})$ given by

$$\mathfrak{R}(a, b, c) := a + b\cos 2\varphi + c \sin 2\varphi,$$

see (11). So, if K is the cone given by (12) then

$$\mathcal{C} = \{-(1/2)\log \mathfrak{R}(a, b, c) : (a, b, c) \in K\}.$$

Obviously, $\mathcal{C}$ is invariant under addition of a constant, that is,

$$\forall r \in \mathbb{R},\ \forall g \in \mathcal{C} \Rightarrow g + r \in \mathcal{C}. \tag{17}$$

This fact allows considering the standard Chebyshev, that is, *uniform*, approximation instead of the one-sided one (14).

Proposition 3. Let $\mathfrak{d}$ be the distance from f to $\mathcal{C}$, that is, the value of

$$\begin{cases} \|f - g\|_\infty \to \min \\ g \in \mathcal{C}. \end{cases} \tag{18}$$

The function $\bar{g} \in \mathcal{C}$ is a solution to (18) if and only if the function $(\bar{g} - \mathfrak{d}) \in \mathcal{C}$ is a solution to (14).

Proof. Let $\bar{g}$ be a solution to (18) and let for short $g_1 := \bar{g} - \mathfrak{d}$. Since $\bar{g} - f \leq \|\bar{g} - f\|_\infty = \mathfrak{d}$, we get $g_1 \leq f$. Let $g_2 \leq f$ be a solution to (14) and let $c := \|f - g_2\|_\infty$.

Since g_1 is feasible for (14), we have $c \leq \|f - g_1\|_\infty = \max(f - g_1) = \max(f - \bar{g}) + \mathfrak{d} \leq 2\mathfrak{d}$. That is,

$$c \leq \|f - g_1\|_\infty \leq 2\mathfrak{d}. \tag{19}$$

On the other hand, if $g_3 := g_2 + c/2$ then $\mathfrak{d} \leq \|f - g_3\|_\infty$. Let $\varphi \in \mathbb{R}$ be arbitrary. If $f(\varphi) \leq g_3(\varphi)$ then $g_2(\varphi) \leq f(\varphi) \leq g_2(\varphi) + c/2$, so $|f(\varphi) - g_3(\varphi)| \leq c/2$. If $f(\varphi) > g_3(\varphi)$ then $|f(\varphi) - g_3(\varphi)| = f(\varphi) - g_3(\varphi) = (f(\varphi) - g_2(\varphi)) - c/2 \leq c/2$. So,

$$\mathfrak{d} \leq \|f - g_3\|_\infty \leq c/2. \tag{20}$$

From (19) and (20) it follows that $c = 2\mathfrak{d}$, so (19) gives that g_1 is a solution to (14), and (20) gives that g_3 is a solution to (18). □

We will prove in the present framework the well known geometrical theorem that at most one ellipse centered at the origin passes through three distinct points.

Lemma 1. Let

$$\varphi_1 < \varphi_2 < \varphi_3 < \varphi_1 + \pi \tag{21}$$

be fixed. Let $A : \mathbb{R}^3 \to \mathbb{R}^3$ be the linear operator

$$A(a, b, c) := (\mathfrak{R}(a, b, c)(\varphi_1), \mathfrak{R}(a, b, c)(\varphi_2), \mathfrak{R}(a, b, c)(\varphi_3)).$$

Then A is an isomorphism.

Proof. In co-ordinates

$$A = \begin{pmatrix} 1 & \cos 2\varphi_1 & \sin 2\varphi_1 \\ 1 & \cos 2\varphi_2 & \sin 2\varphi_2 \\ 1 & \cos 2\varphi_3 & \sin 2\varphi_3 \end{pmatrix},$$

so $\det A = 4 \sin(\varphi_2 - \varphi_1) \sin(\varphi_3 - \varphi_1) \sin(\varphi_3 - \varphi_2) > 0$, since all three differences are in $(0, \pi)$. □

Proposition 4. Let $g_1, g_2 \in \mathcal{C}$.

If g_1 and g_2 coincide at three points as in (21) then $g_1 = g_2$.

If there are φ_1, φ_2 such that $0 < |\varphi_1 - \varphi_2| < \pi$, and

$$g_1(\varphi_1) = g_2(\varphi_1),\ g_1'(\varphi_1) = g_2'(\varphi_1) \text{ and } g_1(\varphi_2) = g_2(\varphi_2), \tag{22}$$

then $g_1 = g_2$.

Proof. Let $g_i = -(1/2) \log \mathfrak{R}(a_i, b_i, c_i)$ for $i = 1, 2$. If g_1 and g_2 coincide at three points as in (21) then, since log is injective, $\mathfrak{R}(a_1, b_1, c_1)$ and $\mathfrak{R}(a_2, b_2, c_2)$ also coincide at those three points, so by Lemma 1 we get $a_1 = a_2$, $b_1 = b_2$ and $c_1 = c_2$.

Let now (22) hold. Since

$$g_i'(\varphi) = -\frac{1}{2} \left(\frac{d}{d\varphi} \mathfrak{R}(a_i, b_i, c_i)(\varphi) \right) / \mathfrak{R}(a_i, b_i, c_i)(\varphi),$$

the three conditions translate to $\mathfrak{R}(a_1, b_1, c_1)$ and $\mathfrak{R}(a_2, b_2, c_2)$ agreeing at φ_1 in value and derivative, and at φ_2 in value. This implies

$$\begin{pmatrix} 1 & \cos 2\varphi_1 & \sin 2\varphi_1 \\ 0 & -2 \sin 2\varphi_1 & 2 \cos 2\varphi_1 \\ 1 & \cos 2\varphi_2 & \sin 2\varphi_2 \end{pmatrix} \begin{pmatrix} a_2 - a_1 \\ b_2 - b_1 \\ c_2 - c_1 \end{pmatrix} = 0.$$

The determinant of the above matrix is $4\sin^2(\varphi_2-\varphi_1)>0$, so $a_1=a_2$, $b_1=b_2$ and $c_1=c_2$. □

We are ready to prove the uniqueness part of our main result.

Proposition 5. Let $\bar g\in\mathcal{C}$. Assume that there exist points φ_i,ψ_i, $i=1,2$, satisfying (15) and such that

$$f(\varphi_i)-\bar g(\varphi_i)=\bar g(\psi_i)-f(\psi_i)=\|f-\bar g\|_\infty,\quad i=1,2. \tag{23}$$

Then $\bar g$ is the unique solution to (18).

Proof. Let $\hat g\in\mathcal{C}$ be such that

$$\|f-\hat g\|_\infty\le\|f-\bar g\|_\infty. \tag{24}$$

If we can prove that from this follows $\hat g=\bar g$ then obviously $\bar g$ is a solution to (18) and, moreover, unique.

Assume that

$$\bar g\ne\hat g. \tag{25}$$

Let $h:=\bar g-\hat g$. We can write $h(\varphi_i)=(f-\hat g)(\varphi_i)-(f-\bar g)(\varphi_i)$. By (23) we have $(f-\bar g)(\varphi_i)=\|f-\bar g\|_\infty$, so $h(\varphi_i)=(f-\hat g)(\varphi_i)-\|f-\bar g\|_\infty\le\|f-\hat g\|_\infty-\|f-\bar g\|_\infty\le 0$ by (24). Thus $h(\varphi_i)\le 0$. Similarly, $h(\psi_i)=(f-\hat g)(\psi_i)+(\bar g-f)(\psi_i)=(f-\hat g)(\psi_i)+\|f-\bar g\|_\infty\ge\|f-\bar g\|_\infty-\|f-\hat g\|_\infty\ge 0$. We have shown that

$$h(\varphi_i)\le 0\le h(\psi_i),\quad i=1,2. \tag{26}$$

Consequently, there exist $\xi_i\in[\varphi_i,\psi_i]$, $i=1,2$ (in particular, $\xi_1<\xi_2$) such that $h(\xi_i)=0$ for $i=1,2$. If there were a third point in $[\varphi_1,\varphi_1+\pi)$ at which $h=0$, then Proposition 4 would have implied $\bar g=\hat g$, contradicting (25), so

$$h(\varphi)\ne 0,\quad \forall\varphi\in[\varphi_1,\varphi_1+\pi)\setminus\{\xi_1,\xi_2\}. \tag{27}$$

Also, if $h'(\xi_i)=0$ for some $i=1,2$, then again Proposition 4 implies $\bar g=\hat g$, so

$$h'(\xi_i)\ne 0,\quad i=1,2. \tag{28}$$

From (27) and $\xi_1\le\psi_1<\varphi_2\le\xi_2$ it follows that $h(\varphi)\ne 0$ for all $\varphi\in(\psi_1,\varphi_2)$. Since h is continuous, it has a constant sign on (ψ_1,φ_2), so there are two possibilities:

Case 1. $h>0$ on (ψ_1,φ_2). Since $h(\varphi_2)\le 0$, see (26), we have $h(\varphi_2)=0$, that is, $\xi_2=\varphi_2$. From (28) it follows that $h'(\varphi_2)<0$, so $h(\varphi_2+\delta)<0$ for $\delta>0$ small enough. Since $h\ne 0$ on $(\xi_2,\psi_2]$ by (27), we get $h(\psi_2)<0$, contradiction to (26).

Case 2. $h<0$ on (ψ_1,φ_2). Since $h(\psi_1)\ge 0$, we have $\xi_1=\psi_1$, and $h'(\xi_1)<0$, so h is strictly positive to the left of ξ_1, implying $h(\varphi_1)>0$, contradiction. □

Proposition 6. Let $g\in\mathcal{C}$ be arbitrary. Let $\alpha<\beta<\alpha+\pi$. Let $\varepsilon>0$.

There exists $g_\varepsilon\in\mathcal{C}$ such that $\|g_\varepsilon-g\|_\infty<\varepsilon$ and

$$g_\varepsilon(\varphi)<g(\varphi),\ \forall\varphi\in(\alpha,\beta),\quad g_\varepsilon(\varphi)>g(\varphi),\ \forall\varphi\in(\beta,\alpha+\pi).$$

Proof. Let $g=-(1/2)\log\mathfrak{R}(a,b,c)$ for some $(a,b,c)\in K$. Let $\gamma:=(\alpha+\beta)/2$. Let A be the operator from Lemma 1 for α,γ,β in place of the φs in (21).

Let $(a_t,b_t,c_t)=A^{-1}(\mathfrak{R}(a,b,c)(\alpha),\exp(2t)\mathfrak{R}(a,b,c)(\gamma),\mathfrak{R}(a,b,c)(\beta))$. It is clear that for small enough $t>0$ the point $(a_t,b_t,c_t)\in K$ and for $g_t:=-(1/2)\log\mathfrak{R}(a_t,b_t,c_t)$

$$g_t(\alpha)=g(\alpha),\ g_t(\beta)=g(\beta)\text{ and }g_t(\gamma)=g(\gamma)-t<g(\gamma).$$

Since $(a_t,b_t,c_t)\to(a,b,c)$, as $t\to 0$, and $\mathfrak{R}$ is continuous, we have $\|g-g_t\|_\infty<\varepsilon$ for t small enough. Take $g_\varepsilon=g_t$ for some small enough t.

If we assume that $g_\varepsilon(\xi) \geq g(\xi)$ for some $\xi \in (\alpha, \beta)$, then, since $g_\varepsilon(\gamma) < g(\gamma)$ there will be three different points in the interval $[\alpha, \beta]$ where g_ε and g coincide, which contradicts Proposition 4. So,

$$g_\varepsilon(\varphi) < g(\varphi), \ \forall \varphi \in (\alpha, \beta).$$

From this it follows in particular that $g'_\varepsilon(\beta) \geq g'(\beta)$. Since $g'_\varepsilon(\beta) = g'(\beta)$ would contradict Proposition 4, we have that $g'_\varepsilon(\beta) > g'(\beta)$. In particular $g_\varepsilon(\beta+\delta) > g(\beta+\delta)$ for all $\delta > 0$ small enough. If there were $\xi \in (\beta, \alpha + \pi)$ such that $g_\varepsilon(\xi) \leq g(\xi)$ this would contradict Proposition 4. So,

$$g_\varepsilon(\varphi) > g(\varphi), \ \forall \varphi \in (\beta, \alpha + \pi).$$

□

Of course, Proposition 6 can be proved by simply adding an appropriate trigonometric polynomial to $\mathfrak{R}$, but we chose to demonstrate a way that would work just as well for other families as long as they satisfy the interpolation Proposition 4.

Proposition 7. Let $\bar{g}$ be a solution to (18), that is,

$$\|f - \bar{g}\|_\infty = \mathfrak{d} = \min\{\|f - g\|_\infty : \ g \in \mathcal{C}\}. \tag{29}$$

Then there exist points φ_i, ψ_i, $i = 1, 2$, satisfying (15) and (23).

Proof. If $\mathfrak{d} = 0$ then $f = \bar{g}$ and any points satisfying (15) will do.

Therefore, let $\mathfrak{d} > 0$ and

$$\Phi := \{\varphi \in \mathbb{R} : \ f(\varphi) - \bar{g}(\varphi) = \mathfrak{d}\}, \quad \Psi := \{\psi \in \mathbb{R} : \ \bar{g}(\psi) - f(\psi) = \mathfrak{d}\}.$$

Because of the assumption $\mathfrak{d} > 0$ the sets Φ and Ψ do not intersect.

If $\Phi = \emptyset$ then $\max(f - \bar{g}) < \mathfrak{d}$. Consider $g_\varepsilon := \bar{g} - \varepsilon$. Because of (17) the functions $g_\varepsilon \in \mathcal{C}$. For $\varepsilon > 0$ small enough we still have $\max(f - g_\varepsilon) = \max(f - \bar{g}) + \varepsilon < \mathfrak{d}$, while $\min(f - g_\varepsilon) = \min(f - \bar{g}) + \varepsilon > -\mathfrak{d}$. So, $\|f - g_\varepsilon\|_\infty < \mathfrak{d}$, contradiction to (29). In a similar way, $\Psi \neq \emptyset$.

Fix $\varphi_1 \in \Phi$. Since $\Psi + \pi = \Psi$, because f and $\bar{g}$ are π-periodic, and $\Psi \neq \emptyset$, we have $\Psi \cap [\varphi_1, \varphi_1 + \pi] \neq \emptyset$. Let

$$\psi_1 := \min \Psi \cap [\varphi_1, \varphi_1 + \pi], \quad \psi_2 := \max \Psi \cap [\varphi_1, \varphi_1 + \pi].$$

Since $\varphi_1, \varphi_1 + \pi \in \Phi$ and $\Phi \cap \Psi = \emptyset$, it follows that $\psi_i \in (\varphi_1, \varphi_1 + \pi)$ for $i = 1, 2$.

We claim that

$$\Phi \cap [\psi_1, \psi_2] \neq \emptyset, \tag{30}$$

(note Ader's Non-separation Principle).

Assume (30) were false. Since $(f - \bar{g})$ is a continuous function, which is $\mathfrak{d}$ at φ_1 and $-\mathfrak{d}$ at ψ_1, it vanishes somewhere in (φ_1, ψ_1). Let $\alpha := \max\{\xi < \psi_1 : \ f(\xi) = \bar{g}(\xi)\}$. In a similar way, let $\beta := \min\{\xi > \psi_2 : \ f(\xi) = \bar{g}(\xi)\}$. We have then

$$[\psi_1, \psi_2] \subset (\alpha, \beta), \quad [\alpha, \beta] \subset (\varphi_1, \varphi_1 + \pi).$$

Moreover, it is easy to see that

$$\Phi \cap [\alpha, \beta] = \emptyset,$$

because (30) was assumed false, and $f \leq \bar{g}$ on $[\alpha, \psi_1]$ and $[\psi_2, \beta]$.

By construction, $\Psi \cap ([\varphi_1, \alpha] \cup [\beta, \varphi_1 + \pi]) = \emptyset$. Since $\Psi + \pi = \Psi$, the latter translates to

$$\Psi \cap [\beta, \alpha + \pi] = \emptyset.$$

So, there is $\varepsilon > 0$ such that

$$\max_{[\alpha,\beta]}(f-\bar{g})+\varepsilon < \mathfrak{d}, \quad \max_{[\beta,\alpha+\pi]}(\bar{g}-f)+\varepsilon < \mathfrak{d}.$$

From Proposition 6 there is $g_\varepsilon \in \mathcal{C}$ such that $\|g_\varepsilon - \bar{g}\|_\infty < \varepsilon$ and

$$g_\varepsilon < \bar{g} \text{ on } (\alpha,\beta), \quad g_\varepsilon > \bar{g} \text{ on } (\beta,\alpha+\pi).$$

We will show that

$$\|f-g_\varepsilon\|_\infty = \max_{[\alpha,\alpha+\pi]}|f-g_\varepsilon| < \mathfrak{d}. \tag{31}$$

Indeed, $\max_{[\alpha,\beta]}(f-g_\varepsilon) \le \max_{[\alpha,\beta]}(f-\bar{g}) + \|\bar{g}-g_\varepsilon\|_\infty < \mathfrak{d}$, and $\max_{[\alpha,\beta]}(g_\varepsilon - f) = g_\varepsilon(\xi) - f(\xi)$ for some $\xi \in [\alpha,\beta]$, but since $f = \bar{g}$ at α and β, and $\max_{[\alpha,\beta]}(g_\varepsilon - f) \ge g_\varepsilon(\psi_1) - f(\psi_1) = \mathfrak{d} + (g_\varepsilon(\psi_1) - \bar{g}(\psi_1)) \ge \mathfrak{d} - \|\bar{g}-g_\varepsilon\|_\infty > 0$; we have that $\xi \in (\alpha,\beta)$, thus $\max_{[\alpha,\beta]}(g_\varepsilon - f) = g_\varepsilon(\xi) - f(\xi) < \bar{g}(\xi) - f(\xi) \le \mathfrak{d}$.

In a similar way, $\max_{[\beta,\alpha+\pi]}(f-g_\varepsilon) = f(\xi)-g_\varepsilon(\xi)$ for some $\xi \in (\beta,\alpha+\pi)$, so $< f(\xi)-\bar{g}(\xi) \le \mathfrak{d}$, and $\max_{[\beta,\alpha+\pi]}(g_\varepsilon - f) \le \max_{[\beta,\alpha+\pi]}(\bar{g}-f) + \|\bar{g}-g_\varepsilon\|_\infty < \mathfrak{d}$.

Thus (31) is verified, but it contradicts (29). Therefore, there is $\varphi_2 \in \Phi \cap (\psi_1,\psi_2)$ and φ_i, ψ_i satisfy (15) and (23). □

In view of the work so far the following completes our study.

Proposition 8. The problem (18) has a solution.

Proof. Here it is easier to work with the standard form of the ellipses in polar co-ordinates. Take $(a,b,c) \in K$, that is, $a > \sqrt{b^2+c^2}$, and set

$$b' := \sqrt{b^2+c^2}, \quad b = b'\cos 2\theta,\ c = b'\sin 2\theta.$$

Then

$$\mathfrak{R}(a,b,c) = a + b'\cos 2(\varphi-\theta).$$

K translates to

$$K' := \{(a,b',\theta) :\ a > b' \ge 0,\ \theta \in [0,\pi]\},$$

and

$$\mathcal{C} = \{-(1/2)\log(a+b'\cos 2(\varphi-\theta)) : (a,b',\theta) \in K'\}.$$

Let $(a_n,b'_n,\theta_n) \in K'$ be such that for

$$g_n(\varphi) := -\frac{1}{2}\log(a_n + b'_n\cos 2(\varphi-\theta_n))$$

we have

$$\lim_{n\to\infty}\|f-g_n\|_\infty = \mathfrak{d}.$$

By taking a subsequence we may assume that $\theta_n \to \theta$, as $n \to \infty$. Since

$$g_n(\theta_n+\pi/4) = -\frac{1}{2}\log a_n,$$

and $\|g_n\|_\infty < \|f\|_\infty + \mathfrak{d} + 1$ for large enough ns, the sequence $\{\log a_n\}_{n=1}^\infty$ is bounded, so there is $r > 0$ such that

$$r \le a_n \le 1/r, \quad \forall n \in \mathbb{N}.$$

Therefore, we may assume that $a_n \to a > 0$, as $n \to \infty$. We also assume that $b'_n \to b' \le a$, as $n \to \infty$. If $b' = a$ then

$$g_n(\theta_n+\pi/2) = -\frac{1}{2}\log(a_n - b'_n) \to \infty, \text{ as } n \to \infty,$$

which is a contradiction. So, $(a, b', \theta) \in K'$ and by continuity it follows that the corresponding $g \in \mathcal{C}$ solves (18). □

References

[1] O. B. Ader, An affine invariant of convex regions, *Duke Math. J.* 4 (1938), no. 2, 291–299.

[2] P. M. Gruber, P. Kenderov, Approximation of convex bodies by polytopes, *Rend. Circ. Mat. Palermo*, Ser. II, 31 (1982), 195–225.

[3] F. Grundbacher, T. Kobos, On certain extremal Banach–Mazur distances and Ader's characterization of distance ellipsoids, *Mathematika* 72 (2026), e70062. https://doi.org/10.1112/mtk.70062

[4] R. A. Horn, C. R. Johnson, *Matrix Analysis*, 2nd ed., Cambridge University Press, Cambridge, 2013. ISBN 978-0-521-83940-2.

[5] M. Ivanov, A. J. Pallarés, S. Troyanski, On the geometry of Banach spaces with modulus of convexity of power type 2, *Studia Math.* 197 (2010), no. 1, 81–91.

[6] M. Ivanov, S. Troyanski, Uniformly smooth renorming of Banach spaces with modulus of convexity of power type 2, *J. Funct. Anal. 237* (2006), 373–390.

[7] F. John, Extremum problems with inequalities as subsidiary conditions, in: *Studies and Essays Presented to R. Courant on his 60th Birthday*, January 8, 1948, Interscience Publishers, New York, 1948, pp. 187–204.

[8] P. S. Kenderov, Polygonal approximation of plane convex compacta, *J. Approx. Theory* 38 (1983), 221–239.

[9] P. S. Kenderov, N. K. Kirov, A dynamical systems approach to the polygonal approximation of plane convex compacts, *J. Approx. Theory* 74 (1993), no. 1, 1–15.

[10] B. Maurey, unpublished.

[11] R. Nikolov, On a geometric characteristic of Banach spaces with modulus of convexity of power type 2, *C. R. Acad. Bulg. Sci.* 70 (2017), no. 9, 1189–1194.

[12] R. Nikolov, On a differential inequality, *Ann. Sofia Univ.*, Fac. Math. and Inf. 104 (2017).

[13] A. Pietsch, *History of Banach Spaces and Linear Operators*, Birkhäuser, Boston, 2007. ISBN 978-0-8176-4367-6.

[14] S. Rakov, On uniformly smooth renormings of uniformly convex Banach spaces, *J. Soviet Math.* 31 (1985), 2713–2721.

МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2026
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2026
Proceedings of the Fifty-Fifth Spring Conference
of the Union of Bulgarian Mathematicians
Tryavna, Bulgaria, April 5–9, 2026

DIGITISED CULTURAL HERITAGE AS DATA: EMERGING TRENDS IN ITS USE IN SCHOOL-LEVEL COMPUTER SCIENCE EDUCATION

Milena Dobreva
Institute of Mathematics and Informatics at the Bulgarian Academy of Sciences, Sofia, Bulgaria
University of Strathclyde, Scotland, UK
e-mail: milena.dobreva@strath.ac.uk

Decades of active digitisation of cultural heritage in galleries, libraries, archives and museums (GLAM institutions) have led to the accumulation of vast amounts of openly accessible digital content. Research and education are the two fields in which this content is most frequently used. The strongest connections have been developed with the teaching of history, literature, art, and music, where digitised materials provide primary sources and rich illustrative resources. However, the contemporary trend of approaching digital collections as data makes this type of open content particularly suitable for incorporating authentic tasks related to data collection, cleaning, analysis, and visualisation. Such tasks are highly appropriate for projects that integrate diverse skills from computer science education and can be offered both as individual and group assignments.

The paper presents real-life examples from international practice of integrating cultural heritage into school-level computer science education, within the broader context of strengthening STEM competencies and project-based learning. These examples demonstrate that cultural heritage can successfully serve as a meaningful context for developing algorithmic thinking, data literacy, digital skills, and AI literacy in schools.

Keywords: Digital Cultural Heritage, collections as data

ДИГИТАЛИЗИРАНОТО КУЛТУРНО НАСЛЕДСТВО КАТО ДАННИ: НОВИ ТЕНДЕНЦИИ ЗА ИЗПОЛЗВАНЕТО МУ В УЧИЛИЩНОТО ОБУЧЕНИЕ ПО ИНФОРМАТИКА

Милена Добрева
Институт по математика и информатика при Българска академия на науките, София, България
Университет на Стратклайд, Шотландия, Великобритания
e-mail: milena.dobreva@strath.ac.uk

https://doi.org/10.55630/mem.2026.55.019-030

2020 Mathematics Subject Classification: 94 (Information and Communication).

Десетилетията активна дигитализация на културно наследство в библиотеките, музеите, архивите и галериите доведоха до натрупване на огромно количество свободно достъпно дигитално съдържание. Научните изследвания и образованието са двете области, където това съдържание се използва най-често. Най-силно развити като възможност за предоставяне на първични източници и богат илюстративен материал са връзките с обучението по история, литература, изкуство, музика. Но съвременната тенденция да се разглеждат дигиталните сбирки като данни (collections as data) прави този тип отворено съдържание много подходящо за включване на реални задачи по събиране, почистване, анализ и визуализация на данни. Този тип задачи са много подходящи за проекти, които интегрират различни умения от обучението по информатика и могат да се предлагат както като лични, така и като групови задачи.

Докладът ще представи реални примери от международната практика за интегриране на културното наследство в училищното обучение по информатика в контекста на засилването на компетенциите в STEM и проектно-базираното обучение, които демонстрират, че културното наследство може успешно да служи като контекст за развитие на алгоритмично мислене, работа с данни, дигитални умения и грамотност в областта на изкуствения интелект в училище.

Ключови думи: дигитално културно наследство, сбирките като данни

1. Introduction

Digitisation has reshaped access to cultural heritage by making primary sources accessible 24/7 from any point in the world. In many educational contexts, digitised heritage entered classrooms as a visibility and access intervention: teachers could project artworks and manuscript pages, use museum objects as discussion prompts, or ask students to interpret historical photographs. This content-oriented use is valuable, but it typically retains a "view-and-interpret" model in which learners are consumers of content preselected (or curated) by teachers.

Over the last decade, a complementary model has gained momentum: digitised heritage is increasingly approached as data. In the collections-as-data paradigm, the central educational object is not only the digital surrogate (for example, an image of a print or a scanned letter) but the dataset that represents the collection at scale – metadata exports, full-text corpora, linked data graphs, annotation layers, or derivative datasets made available for computational reuse. This shift aligns with broader changes in education: the rise of computational thinking in school curricula, growing attention to data literacy, and a pedagogical emphasis on inquiry, authentic problems, and project-based learning.

The question this paper addresses is therefore not whether digitised cultural heritage is useful in education – it clearly is – but how educational approaches have evolved, and how the collections-as-data perspective contributes to that evolution by enabling new kinds of learning activity. Rather than treating cultural heritage as an optional illustration, collections-as-data approaches position it as means for developing competencies in computation, data analysis, and even artificial intelligence (AI) literacy.

To examine this domain systematically, the paper is structured as follows. Section 2 formulates the research questions that guide the study. Section 3 outlines the methodological framework adopted to address these questions. Section 4 reviews the principal

pedagogical approaches situated at the intersection of ICT education and cultural heritage. Section 5 analyses in greater depth the potential of the *collections as data* paradigm for supporting computational thinking and data literacy. Section 6 presents illustrative examples demonstrating how major cultural heritage institutions actively contribute to bridging heritage and formal education. Section 7 discusses the implications of these developments for curriculum design and ICT competency frameworks. The paper concludes by synthesising key findings and identifying research gaps and directions for future work.

2. Research Questions and Methodology

This paper explores four questions.

RQ1. How have educational approaches for using digitised cultural heritage evolved from content-focused models toward data-oriented learning activities?

RQ2. What learning outcomes are most plausibly supported by collections-as-data work with cultural heritage in school and early higher education?

RQ3. What forms of pedagogy and curriculum design best support meaningful integration of cultural heritage datasets within computational thinking and data literacy objectives?

RQ4. Which contemporary initiatives demonstrate workable models for integrating cultural heritage datasets into educational practice, and what can be learned from them?

3. Methodology

The paper is exploratory rather than offering a systematic review of the literature. We explored literature and policy reports across four intersecting areas: (1) digitisation and access initiatives in the cultural heritage sector; (2) collections-as-data and computational use of digitised collections; (3) education research on inquiry, project-based learning, computational thinking, and data literacy; and (4) documentation from major cultural heritage platforms that explicitly support educational reuse.

The goal is integrative rather than exhaustive: to suggest current trends and a practical framework for educational integration, supported by real-life examples. While the present paper is not an empirical classroom study, it specifies what would be required for rigorous evaluation of collections-as-data learning interventions, including learning artefacts, process documentation, and assessment of transferable competencies.

4. Evolution of Educational Approaches to Digitised Cultural Heritage

The question how to best use digitised cultural heritage in education is as old as digitisation itself – from the very onset of digitisation activities, education was considered a major domain of using digital content alongside research and leisure [6]. Back in 2015, we argued that there is a paradox within the educational use of cultural heritage collections: despite the rapid expansion of digitised collections and the availability of millions of digital objects through large-scale infrastructures, their integration into formal education remained limited even within the most likely adopters, Humanities and Arts disciplines [6]. The article highlighted a persistent disconnect between digital library development and actual educational practice, noting that most initiatives are supply-driven rather than grounded in empirically studied teacher and learner needs. Evidence of sustained

classroom use was scarce, and terminology, interfaces, and workflows were often poorly aligned with mainstream e-learning environments. Overall, the paper concluded that the challenge is not the lack of digitised content, but the absence of coherent pedagogical frameworks, interoperable tools, and evidence-based models that would make digital libraries meaningfully reusable within educational systems. How much progress we can report ten years later? Let us explore the most popular trends for educational use today.

4.1 Transmission and resource supplementation

In transmission-oriented models, digitised cultural heritage primarily supplements teaching by providing illustrative materials or authoritative sources. The learner's role is to absorb and reproduce knowledge, supported by digital images, document excerpts, or curated presentations. Digitised heritage in this mode operates similarly to a textbook illustration, although with greater quality and in some cases with the option to manipulate the object (e.g. zoom into it, or rotate it). This approach is very popular in subjects such as history, art, music as explored in the academic literature [2, 4, 10]. A modification of this approach is the use of virtual reality and games as presented by Xu and al. [14] with the idea to offer an engaging environment supporting learning about the past.

4.2 Constructivism and inquiry with primary sources

Constructivist approaches reconsider learners as active meaning-makers. Inquiry-based learning encourages students to examine sources, ask questions, and justify interpretations. Digitised cultural heritage became particularly valuable here because it provides access to primary sources that support evidence-based argumentation. Teacher-facing programmes that curate sets of primary sources and propose inquiry questions reflect this shift, making it feasible to integrate authentic materials without requiring specialist archival training. This type of use of digital heritage is again strongest in the Humanities and arts and is particularly relevant to the efforts to improve critical thinking and counteract misinformation.

4.3 Project-based learning and authentic tasks

Project-based learning extends inquiry by organising learning around extended tasks with tangible outputs. In heritage contexts, projects may involve curating a digital exhibit, producing interpretive narratives, or comparing sources across time and place. Digitised collections enable project work by reducing access barriers and allowing learners to assemble evidence sets that would be impractical to gather physically. Project-based learning is the space where cultural heritage can offer objects or datasets which help to improve ICT skills. For example, traditional hats from a local festival had been used to improve computer-aided design skills [13].

4.4 Computational thinking and data literacy

The contemporary emphasis on computational thinking and data literacy changes the traditional pedagogical space. Learners are increasingly expected to understand how data is structured, processed, analysed, and communicated. In this environment, digitised heritage becomes not only a source of meaning but also a source of data. Collections-as-data approaches provide authentic datasets for teaching data practices: learners can define questions, extract subsets, clean records, visualise patterns, and critically interpret

results. Such examples are already tried in higher education [7] – currently combining tasks of identifying datasets, cleaning them and analysing and visualising the data using Jupyter notebooks and Python.

4.5 From digital humanities practice to educational method

Collections-as-data ideas emerged in close relation to digital humanities practice, where researchers sought to use computational methods on corpora, catalogues, and large-scale digitised collections. Educational adoption increasingly follows the same trajectory: methods developed for research are translated into classroom-appropriate forms. This translation is not a simple simplification. It involves deciding which elements of research workflows should be made visible to learners, which should be scaffolded, and which should be deferred. For example, learners may not need to build a full production pipeline, but they benefit from experiencing the logic of a pipeline: selecting evidence, documenting transformations, and validating interpretations.

The educational value lies in method literacy. When students work with heritage-as-data, they are learning how modern knowledge is produced: not only by reading sources, but by structuring evidence, testing patterns, and communicating uncertainty. This resonates with broader aims in contemporary education to develop evidence-based reasoning, to demystify digital tools, and to prepare learners for environments in which data-informed claims are common. With a growing amount of accumulated open software on platforms such as Hugging Face, Github, or DARIAH campus, we are currently living in times of accumulating openly available software and the challenges of discovery of tools which may be suitable to use as illustrations in education [8]. At the same time, the number of openly available datasets based on digital collections is growing; this created the need to describe datasets using datasheets [1]; however, these datasheets are not particularly focused on the potential for educational reuse. We could expect that in the future such descriptions could be extended with reuse guidance.

4.6 Shifts in what counts as 'authentic' learning

Digitised cultural heritage changes what authenticity can mean in classrooms. In earlier models, authenticity was achieved by viewing an original source (even if mediated digitally) and treating it as evidence for interpretation. In collections-as-data learning, authenticity extends to the practices of contemporary analysis: working with imperfect records, understanding constraints of datasets, and justifying methodological choices. Students encounter the reality that cultural heritage data is heterogeneous and historically shaped, and they learn that responsible analysis requires both technical skill and contextual awareness.

These shifts align with the wider evolution from knowledge-as-content toward knowledge-as-practice. This is an essential component of critical thinking, a skill much discussed but never sufficiently supported to form such a level of skills which would stop the spread of disinformation.

These shifts also open a pathway for stronger integration between humanities and computing/information technology education. Rather than using cultural heritage merely to 'decorate' computational lessons, collections-as-data approaches can make heritage a central domain where computation is learned as a way of asking and answering questions.

5. What 'Collections as Data' Could Add to the Educational System?

Collections as data had been introduced relatively recently introduced [3, 5, 11] and represent the trend of treating digital collections, such as texts, images, audio, and videos, as datasets allowing for computational analysis. There are several noteworthy characteristics of collections as data that can help enrich educational practice.

5.1 From item-level interpretation to collection-scale questions

Collections-as-data approaches expand the unit of analysis. Instead of focusing solely on interpreting a single document or object, learners can ask collection-scale questions: how topics change over time, how places and historical personalities are connected, or how descriptive terms cluster. This supports a feedback loop between a narrow interpretation of one source/document and aggregate analysis: computational outputs suggest hypotheses, while source analysis validates and refines them. This may seem a strange advantage, but a general tendency of the Bulgarian educational system is to reduce the number of primary sources used. To what extent replacing the human reading and analysis of multiple sources with a skill to query larger digital collections without knowing the sources in detail raises many questions – here we are merely noting a shift rather than offering an opinion on what this shift will cause in the long term in terms of skills.

5.2 Data practices as part of disciplinary understanding

Treating cultural heritage as data makes data practices pedagogically visible. Students learn that data cleaning, normalisation, and linking are not neutral pre-processing steps; they shape what can be asked and answered. This helps learners understand that evidence in digital environments is constructed through a chain of choices. Choices are possibly easiest illustrated in visualisation tasks where the students have to make a choice which aspects of a dataset are worth illustrating visually.

5.3 Alignment with contemporary curriculum goals

Collections-as-data pedagogy aligns with major curriculum goals in computing and cross-curricular STEM. It supports computational thinking (decomposition, abstraction, pattern recognition, algorithmic reasoning), data literacy (data quality, analysis, interpretation, communication), and transferable skills (teamwork, documentation, reproducibility, critical reflection). Because cultural heritage materials are meaning-rich, they also support motivation and interdisciplinary relevance: students can see how computational methods apply to questions that matter culturally and socially.

There is also an additional motivation for working on these skills. A recent European Commission report [9] argued that STEM skills are in short supply in the creative industries. Including more activities involving the transformation of datasets from the cultural heritage domain within STEM education in schools could support cultivating more interest in a career in the creative industries. For the time being there is no systematic evidence gathered around this but it is worth exploring.

6. Initiatives and Examples of Cultural Heritage Datasets in Education

This section highlights initiatives that explicitly support educational reuse of digitised cultural heritage and, in several cases, provide dataset-oriented access that enables collections-as-data learning.

6.1 Europeana: Europe-wide cultural heritage for teaching and learning

The European data space for cultural heritage, Europeana, has developed a sustained education ecosystem that supports educators in integrating Europe's digital cultural heritage into learning activities. Europeana Classroom provides a curated entry point for educators, offering learning resources that draw on Europeana's aggregated collections and are designed for classroom use. Complementing this, the 'Teaching with Europeana' initiative and associated educator community activities support the creation and sharing of learning scenarios that use Europeana data and digital objects in formal and non-formal education.

Europeana has also collaborated with European Schoolnet over multiple years to embed digital cultural heritage into educational practice, including teacher engagement activities and the development of classroom learning scenarios). From a collections-as-data perspective, Europeana's emphasis on reusable, openly accessible digital culture provides a pathway from item-level learning resources toward more data-oriented uses, especially when educators and students engage with metadata, thematic sets, and aggregation mechanisms across institutions.

6.2 Digital Public Library of America: Primary Source Sets and API-enabled learning

The Digital Public Library of America (DPLA) provides educational materials that package digitised heritage into teachable units. Its Primary Source Sets are designed to support critical thinking and content learning by combining sets of primary sources with teaching guides and contextual information. These sets help educators operationalise inquiry-based learning with cultural heritage at scale.

For more data-oriented learning, DPLA also supports programmatic engagement through its API and openly downloadable metadata. Tutorial and training materials have been developed to introduce learners to retrieving DPLA metadata via the API and manipulating it with data tools such as OpenRefine, demonstrating a bridge from curated educational sets to dataset-based workflows.

6.3 Library of Congress: Teaching with primary sources, newspapers, and datasets

The Library of Congress offers extensive teacher-facing materials and professional development designed to help educators integrate primary sources from its digital collections. Its classroom materials are created to be ready-to-use in instruction.

For dataset-oriented engagement, the Library's digital newspaper collection Chronicling America provides access to digitised historic newspapers through 196 and is frequently recommended as a starting point for classroom exploration of newspaper archives.

6.4 Smithsonian: Open access collections, datasets, and educator tooling

The Smithsonian's Open Access initiative has released millions of digital assets under CC0 licence, including collections metadata. This expands educational possibilities from viewing and remixing assets to computational reuse of structured records. The Smithsonian also provides a public data repository for open access metadata and supports discovery and reuse through channels such as GitHub.

For educators, the Smithsonian Learning Lab provides an educational environment that explicitly connects open access content with teaching and learning . The combination of open release and educator-facing tools offers a model for connecting collections-as-data infrastructures to classroom practice.

6.5 What these initiatives have in common: design patterns for educational reuse

All these examples come from big GLAM institutions or accumulated resources. One worth-noting aspect is that the initiative to connect digital heritage materials comes from the providers, and is not equally strong in the educational institutions. Although the initiatives above differ in scale and geography, they reveal recurring patterns that are useful for educators and institutions planning collections-as-data learning. First, they provide an on-ramp that is pedagogically familiar: curated classroom materials, learning scenarios, or themed sets that translate collections into teachable units. Second, several of them expose pathways to scale, such as APIs, bulk metadata downloads, or dataset repositories, enabling learners to move from item-level exploration to dataset-based inquiry. This is currently more suitable for higher education students, but may also be beneficial for advanced secondary school learners. Third, they invest in educator capacity through teacher-focused documentation and teachers' networks, recognising that sustainable educational reuse depends on the educators' confidence and time.

In this section we explored how several big GLAM institutions and projects are creating educational materials. In the next section we will explore how these developments influence the curriculum and teachers.

7. Implications for Curriculum and Teachers

7.1 Curriculum design

Integrating cultural heritage datasets effectively requires curriculum design that treats heritage not as an add-on but as a domain through which core competencies are developed. Educators can sequence tasks from simple to complex: starting with curated sets and basic descriptive analysis, moving toward student-defined questions, subset extraction, data cleaning, and visualisation. Interdisciplinary framing can make objectives transparent: computational techniques are used to answer questions anchored in cultural and historical meaning. Cultural heritage can fit nicely into project-based learning and is suitable for group work projects. Such projects can be developed within the blocks where teachers have the freedom of choice of the most suitable topic(s) and activities.

7.2 Teacher professional development

Teacher preparation is a central constraint and opportunity for integrating more cultural heritage materials in the classroom. The digital competences of teachers have been discussed for a considerable time, and with the quick shifts in technologies, it is one of the topics with constantly shifting priorities [12].

Collections-as-data pedagogy requires confidence with data workflows as well as familiarity with working responsibly with cultural materials. This for sure is not common knowledge among all teachers, but partnerships with GLAM professionals can strengthen teachers' domain knowledge and provide access to contextual documentation and support.

8. Conclusion

Despite growing practice, most often receiving a push from GLAM institutions, the evidence base for learning outcomes in collections-as-data education remains uneven. Future research can explore several aspects:

(a) which competencies are most reliably developed through heritage datasets;
(b) what scaffolding is needed for different age groups;
(c) how interdisciplinary collaboration affects learning; and
(d) how tools designed to support educators influence learning outcomes.

Methodologically, mixed approaches are likely to be most informative, combining analysis of learner artefacts (datasets, visualisations) with observation and reflection, skills much needed for the current generation, which is prone to many technological distractors.

The educational role of digitised cultural heritage has evolved from resource supplementation toward inquiry-based learning and, increasingly, toward computationally enabled analysis. This shift is visible in higher education. The collections-as-data paradigm supports this trend by enabling learners to treat cultural heritage as a domain for data experimentation, aligned with modern curriculum priorities such as computational thinking, data and AI literacy.

Initiatives such as Europeana's education ecosystem, DPLA's primary source and API resources, the Library of Congress's teacher programmes and dataset guidance, and the Smithsonian's open access releases demonstrate that educational reuse can be supported at scale when open collections are complemented by educator-facing materials and infrastructure. To realise the full potential of collections as data, educators and cultural heritage institutions should co-design learning pathways that connect meaning-rich heritage contexts to data-centred methods.

Integrating collections as data into education also raises a practical question: how should learning be evaluated when outputs combine technical work, interpretive reasoning, and communication? Conventional assessment in computing often gives advantage to functional correctness of code, while humanities assessment often recognises argumentation and use of sources. Collections-as-data learning requires assessment approaches that combine both.

Implications for GLAM-Education Partnerships and Green Considerations

Collections-as-data, for the time being, heavily depends on the initiative of GLAMs. While educators can use openly published resources independently, deeper learning designs often require clarity about the licensing of data, documentation of fields, and robust access mechanisms. Multiple downloads of identical datasets from the same educational institutions is an aspect which may have a negative green impact – the educational planning is essential, also as it should avoid unnecessary loads and repeated downloads.

Lowering the adoption threshold

Europeana's educator-facing resources and classroom scenarios exemplify how curated materials can lower adoption barriers for teachers. Similarly, the Library of Congress positions its classroom materials as ready-to-use, created by teachers for teachers. These approaches recognise that classroom time and teacher capacity are limited, and that high-quality documentation is a requirement for educational reuse.

Usefulness of cultural heritage materials in introducing FAIR principles

The educational use of cultural heritage datasets is also offering an opportunity to explore what FAIR (findable, accessible, interoperable and reusable) datasets mean in real-life practice. Datasets can also introduce the importance of personal data and GDPR basics in a more natural manner than pure theoretical one.

Future work

This paper outlined some new trends and opportunities to use cultural heritage datasets in ICT education. For the time being, there is a strong push from larger GLAM institutions to offer pathways into education. As we explored, the use of cultural heritage datasets in education can support diverse skills, from technical ones in cleaning, analysing and visualising data as a precursor to data science, to greater skills for a transition from single source analysis to complex reasoning involving multiple objects.

Future research must move beyond exploratory pilots and focus on systematic empirical evaluation. In particular, there is a need for longitudinal classroom studies that measure the impact of heritage datasets on computational thinking, data literacy, and algorithmic reasoning using validated assessment frameworks. Comparative studies examining heritage datasets versus generic educational datasets would clarify whether cultural context adds measurable cognitive or motivational benefits.

Further work is also required on pedagogical design. This includes creating age-appropriate dataset packages, metadata simplification strategies, and reusable task templates aligned with national ICT curricula.

Another possible direction concerns the integration of cultural heritage datasets into emerging AI literacy initiatives. Heritage collections offer complex, heterogeneous, and often biased datasets that can support critical reflection on data provenance, representation, and algorithmic injustice. Finally, sustainable implementation depends on professional development ecosystems. Partnerships between GLAM institutions, teacher training programmes, and ICT curriculum designers are essential to ensure that learning is useful and enjoyable.

Acknowledgements

This paper is partially supported by the project BG16RFPR002-1.016-0002 "ERA Chair in fostering digital cultural heritage via open innovations and open science" funded by the Programme "Research, Innovation and Digitalization for Smart Transformation" 2021-2027 (PRIDST) and co-funded by the European Union.

References

[1] H. Alkemade, Claeyssens, S., Colavizza, G., Freire, N., Lehmann, J., Neudecker, C., Osti, G. and van Strien, D. (2023) "Datasheets for Digital Cultural Heritage Datasets", *Journal of Open Humanities Data*, 9(1), p. 17. Available at: https://doi.org/10.5334/johd.124

[2] Camuñas-García D, Cáceres-Reche MP, Cambil-Hernández MDLE (2023), "Mobile game-based learning in cultural heritage education: a bibliometric analysis". *Education + Training*, Vol. 65 No. 2 pp. 324–339, doi: https://doi.org/10.1108/ET-06-2022-0247

[3] Candela, G., Dritsou, V., Chambers, S., Benardou, A., Irollo, A. and Tasovac, T. (2024). Introduction to Collections as Data. Version 1.0.0. DARIAH Campus [Training module]. https://hdl.handle.net/21.11159/019595c5-1bc8-751c-8201-bcdb34955a96

[4] Challenor, J., & Ma, M. (2019). A Review of Augmented Reality Applications for History Education and Heritage Visualisation. *Multimodal Technologies and Interaction*, *3*(2), 39. https://doi.org/10.3390/mti3020039

[5] Collections as Data: Part to Whole (Andrew Mellon Project, 2021-2023) Deliverables [https://collectionsasdata.github.io/part2whole] Last visited: 12-12-2023

[6] Dobreva, M., Angelova, G., Agre, G. (2015) *Bridging the Gap between Digital Libraries and eLearning.* Cybernetics and Information Technologies, Vol. 15 (4). De Gruyter. pp. 92–110.

[7] Dobreva, M., & Candela, G. (2025). Introducing Collections as Data in Postgraduate and Professional LIS Education. *Proceedings of the Association for Information Science and Technology.* 62 (1), pp. 1425–1427, https://doi.org/10.1002/pra2.1424

[8] EADH (2021) Interdisciplinary perspectives on data. Collection of Jupyter Notebooks. https://data.cervantesvirtual.com/eadh-notebooks

[9] European Commission. (2025). *Communication: A stem education strategic plan: Skills for competitiveness and innovation (COM(2025) 89 final)* (Tech. Rep.). Available online: https://education.ec.europa.eu/document/stem-education-strategic-plan-legal-document

[10] Miguel-Revilla, D., López-Torres, E., Ortuño-Molina, J. *et al.* Cultural heritage and iconic elements for history education: a study with primary education prospective teachers in Spain. *Humanit Soc Sci Commun* **11**, 1590 (2024). https://doi.org/10.1057/s41599-024-04123-w

[11] Padilla, T.G. (2018) Collections as Data: Implications for Enclosure, College & Research Libraries News; Chicago79, no. 6 (June 2018): 296, https://crln.acrl.org/index.php/crlnews/article/view/17003/18751.

[12] Skantz-Åberg, E., Lantz-Andersson, A., Lundin, M., & Williams, P. (2022). Teachers' professional digital competence: an overview of conceptualisations in the literature. *Cogent Education*, *9*(1). https://doi.org/10.1080/2331186X.2022.2063224

[13] UNESCO (2021). Teaching and Learning with Living Heritage A Resource Kit for Teachers Based on the Lessons Learnt from a Joint UNESCO-EU Pilot Project. 49 pp. Available on: https://ich.unesco.org/doc/src/52066-EN.pdf

[14] Xu, N. et al. 2024. HeritageSite AR: Design and Evaluation of a Mobile Augmented Reality Exploration Game for a Chinese Heritage Site. J. Comput. Cult. Herit. 17, 4, Article 67 (December 2024), 29 pages. https://doi.org/10.1145/3700881

МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2026
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2026
Proceedings of the Fifty-Fifth Spring Conference
of the Union of Bulgarian Mathematicians
Tryavna, Bulgaria, April 5–9, 2026

GOOD PRACTICES IN MATHEMATICS TEACHER TRAINING IN THE ERA OF ARTIFICIAL INTELLIGENCE

Nataliya Pavlova
Faculty of Mathematics and Computer Science, University of Shumen, Shumen, Bulgaria
email: n.pavlova@shu.bg

This article touches upon some issues regarding the preparation of mathematics teachers in the context of the massive introduction of technologies based on artificial intelligence in education. The use of generative artificial intelligence breaks the classical methods of training and assessment into a new form, which must be very quickly felt and applied by future teachers. Under the new conditions, the motivation for learning and the understanding of "knowledge" and "skill" are set within very broad limits, which modern teachers should mark and follow with their students. Data are presented regarding the opinion and work style of future teachers when applying generative artificial intelligence in their work. Some good practices are presented.

Keywords: mathematics, teachers, students, artificial intelligence, motivation, provocation, technology

ДОБРИ ПРАКТИКИ В ПОДГОТОВКАТА НА УЧИТЕЛИ ПО МАТЕМАТИКА В ЕПОХАТА НА ИЗКУСТВЕНИЯ ИНТЕЛЕКТ

Наталия Павлова
Факултет по математика и информатика, Шуменски университет „Епископ Константин Преславски“
email: n.pavlova@shu.bg

В дадената статия се поставят някои въпроси относно подготовката на учители по математика в контекста на масовото навлизане в образованието на технологии, базирани на изкуствен интелект. Използването на генеративен изкуствен интелект пречупва класическите методи за обучение и оценяване в нова форма, която трябва много бързо да се усети и приложи от бъдещите учители. При новите условия мотивацията за учене и разбирането за „знание“ и „умение“ са поставени в много широки граници, които съвременният учител се очаква да маркира и следва със

https://doi.org/10.55630/mem.2026.55.031-045
2020 Mathematics Subject Classification: 97A40, 97B50, 97C70.

своите ученици. Представени са данни относно мнението и стила на работа на бъдещите учители при прилагане на генеративен изкуствен интелект в работата им. Представени са някои добри практики.

Ключови думи: математика, учители, ученици, изкуствен интелект, мотивация, провокация, технологии

Въведение

След предизвикателствата от навлизането на информационните и комуникационните технологии в образованието, преминати през последните десетилетия, от няколко години образователната система бе поставена пред ново и още по-сериозно предизвикателство – масовия достъп до генеративен изкуствен интелект, съпроводен от множество възможности, проблеми и страхове. Още през 2020 година е подчертано, че „поради динамиката на промените образователната система трябва да бъде достатъчно гъвкава, за да се съсредоточи върху развитието на знанията и уменията, които могат да се използват в бъдеще, а не само на настоящия пазар на труда“ [24]. На този фон е особено важно да се наблегне на универсалните умения за бързо анализиране и оценяване на информацията и оптимизиране на последващите действия за вземане на решения, и най-вече на нестандартните ситуации, поставящи обучаемите пред необходимостта да мислят критично и нестандартно. Традиционният стремеж към безпогрешно решаване на задачи по известен алгоритъм вече е изместен към неутъпкания път на изследването, съчетан със сблъскването с редица грешки и промяна на гледната точка. Семьонов и Абилкасимова споделят, че класическата оценка за определяне на способностите на база верен-грешен отговор вече не е актуална: „Сега ситуацията е напълно обратна, основният елемент от живота на човек е обратната връзка: направил си нещо – видял си резултата, в някои аспекти този резултат те устройва, в други аспекти не – получил си обратна връзка от околната среда, реагираш на нея, правиш следващата стъпка, следващия опит“ [17]. Именно тази способност за преодоляване и справяне с грешките е особено важна в съвременния свят. Авторите апелират: „бъдещите учители следва да се запознаят не само с основния обем учебно съдържание, но и да се подготвят за дейностите, на които те ще обучават учениците“ [17].

Тук няма да акцентираме върху възможностите на генеративния изкуствен интелект в чисто административен и организационен план, въпреки че тези опции ще спестят изключително много ценно време на учителите. Обект в дадената статия е подготовката на бъдещите учители по математика в условията на нарастващо присъствие на технологии, базирани на генеративен изкуствен интелект. Предметът засяга методическите аспекти с фокус върху уменията за съзнателното и отговорно използване на технологиите при справяне със задачи и последващо предаване на тези умения на учениците.

Методи

В статията е използван комбиниран подход, включващ литературен обзор на актуални изследвания и педагогически изследвания със студенти – бъдещи учители по математика в периода 2020–2025 г. Събрани са данни чрез наблюдения, анкетни проучвания и анализ на студентски разработки при работа с и без генеративен

изкуствен интелект. Резултатите са анализирани с цел идентифициране на нагласи, тенденции и добри практики в подготовката на бъдещи учители.

Ключови изследователски въпроси

Масовото навлизане на възможността за използване на генеративния изкуствен интелект в работата на ученици и студенти породи редица изследователски въпроси, засягащи различни аспекти на необходимата промяна в образованието – организацията на учебния процес, административното му обслужване, възможността за персонализация на обучението, методически възможности, породени от новите условия и т.н. Дадените категории могат да бъдат разбити и по-ясно. Така например Аванг и колектив [3] разглеждат адаптивни учебни системи, сериозни игри, добавена реалност, виртуална реалност, педагогически изследвания и математически калкулатори.

Спецификата на математиката, която дава не само конкретни знания, но основно стимулира хората да мислят, я поставя в особена ситуация при обучение, което позволява използването от обучаемите на технологии, базирани на изкуствен интелект. Според Танг „успешното внедряване на изкуствения интелект в образователната среда зависи от преодоляването на няколко предизвикателства, включително неадекватна инфраструктура, недостатъчно обучение на учителите, пристрастия в системите с изкуствен интелект, прекомерна зависимост от технологиите и опасения относно поверителността на данните и етиката“ [19].

В таблица 1 са представени някои идеи, представени в статии от последните две години, които са категоризирани според основните приноси в по-окрупнена форма.

Таблица Изследователски въпроси

Автори	**Категория**	**Основни приноси**
Noster, N., Gerber, S., Siller, H.-S., 2024 [12]	Методика	Анализира подходите, които бъдещи учители използват при решаване на математически задачи с ChatGPT; идентифицира как технологичните умения и познанията по математика влияят на използването на генеративния изкуствен интелект.
Dilling, F., Herrmann, M., 2024 [7]	Методика	Изследва използването на големите езикови модели за подпомагане на логическото мислене и създаването на геометрични доказателства; подчертава предимствата и недостатъците на ChatGPT при преподаването на математика.
Blonder, R., Feldman-Maggor, Y., Rap, S., 2024 [4]	Методика	Анализира как чрез диалози с ChatGPT могат да се подобрят педагогическите умения на бъдещи учители и да подобри подготовката им чрез интерактивни упражнения. Фокусът е върху учители по природни науки.

Автори	Категория	Основни приноси
Atchley, P., Pannell, H., Wofford, K., Hopkins, M., Atchley, R., 2024 [2]	Методика/ Административни възможности	Анализира възможностите за използване на приложения, базирани на изкуствения интелект във висшето образование, като поставя акценти върху положителните и отрицателните аспекти при комбинирано преподаване и оценяване.
Chalkiadakis, A., Seremetaki, A., Kanellou, A., Kallishi, M., Mastrokoukou, S., Morfopoulou, A., Moraitaki, M., 2024 [5]	Работа с обучаеми със специални потребности	Представя възможности за използване на технологии за подкрепа на ученици със специални потребности; поставя въпроси за ролята на приложения, базирани на изкуствения интелект и виртуална реалност за приобщаване в образованието.
Engelbrecht, J., Borba, M., 2024 [8]	Методика/ Административни възможности	Представя възможности за прилагане на ИКТ в математическото образование; поставя въпроси за интеграцията на генеративния изкуствен интелект в учебния процес.
Nikolova, N., Zafirova-Malcheva, T., Kirilova, B., Mihnev, P., 2024 [11]	Методика/ Работа с обучаеми със специални потребности	Представя ценен литературен обзор в областта на развитието на дигитални компетенции в българските средни училища; включва подходи за подкрепа на ученици със специални потребности чрез технологии и приложения, базирани на изкуствения интелект.
Zhuang, Y., Zhang, S., 2025 [22]	Методика	Проучва възприятията на бъдещите учители за използване на генеративния изкуствен интелект при организиране на беседа.
Espino, C., 2025 [9]	Методика	Разглежда перспективите, приложенията и предизвикателствата на генеративния изкуствен интелект в работата на бъдещите учители, като засяга и етични въпроси при използването на изкуствен интелект в класната стая.
Setälä, M., Heilala, V., Sikström, P., Kärkkäinen, T., 2025 [18]	Административни възможности	Изследва използването на генеративния изкуствен интелект в гимназиалната математика през призмата на приемането и удоволствието от използването на технологията; предоставя препоръки за интеграция на генеративния изкуствен интелект в училищните програми.

Автори	Категория	Основни приноси
Tang, W., 2025 [19]	Методика	Анализира тенденции, предизвикателства и възможности при използването на генеративния изкуствен интелект в математическото образование; предлага насоки за ефективното му внедряване.
Awang, L. A., Yusop, F. D., Danaee, M., 2025 [3]	Методика	Предлага систематичен преглед на литературата и маркира бъдещи направления на генеративния изкуствен интелект в математическото образование; идентифицира педагогически стратегии и потенциал на генеративния изкуствен интелект.

От представения обзор, засягащ само „потребителските аспекти“ на използването на приложения с изкуствен интелект, може да се направи извод, че авторите, проучващи преподавателската работа с помощта на такива приложения, засягат основно следните въпроси:

- Методически аспекти (използване на промптинга с дидактична цел, създаване на материали, оценяване, мотивиране, персонализиране, планиране на обучението и т.н.).
- Административни възможности.
- Работа с обучаеми със специални потребности.

Следва да отбележим, че голяма част от разгледаните източници представят систематичен обзор на литература по темата, целящ маркиране на бъдещи клонове в развитието на методическите и технологичните аспекти в обучението по математика и други дисциплини. Тенденциите в развитието на технологиите, базирани на изкуствен интелект, и бързото адаптиране на обучаемите към новите условия поставя проучванията по дадената тема в изключително динамична позиция. Нагласите, възможностите и психосоциалните фактори се променят експоненциално и образованието остава в догонваща позиция, въпреки старанията да се предвидят и урегулират нормативно процесите в административен, технологичен и методически план.

Проблемът за „илюзорното знание“

Още с навлизането на възможността за търсене в Интернет учениците започнаха да задават въпроси от сорта „Защо ми е да го уча, щом мога лесно да намеря информацията в мрежата?“, а след работата с чатботове с генеративен изкуствен интелект тази илюзия за знание стана още по-силна. Учителите са поставени пред предизвикателството да използват вродената склонност за справяне с проблема с най-малко усилия в посока да провокират самостоятелното достигане до нови знания и стремеж към поставяне на изследователски въпроси. Мотивацията за натрупване на знания и умения стана още по-трудна, особено сред учениците със слаб интерес към математиката.

Целеполагането се измести от класическото описание на очаквания резултат според учебните програми към достигане на една глобална цел – стимулиране на самостоятелно поставяне на въпроси и намиране на тяхното решение. Наред с натрупване на знания и умения учениците следва да проявяват креативност и творчество. Самостоятелното справяне с непознати и нестандартни задачи и търсене на такива задачи може да бъде новата цел, към която да се стремим дори и при работа с немотивирани ученици.

Класическите методи в нов контекст

В описаната ситуация се налага да погледнем по нов начин на класическите методи за обучение. На този етап традиционната лекция може да бъде изнесена от аватар и нейното съдържание да бъде генерирано. Все пак следва да отбележим, че това не е целесъобразно в този момент. Все още има грешки и неточности в съдържанието, предлагано от генеративния изкуствен интелект. Беседата като метод също може да бъде променена, като центърът падне върху обучаемия и се стимулира умението да се формулират и преформулират въпроси, както и да се оценява получения отговор [14]. Илюстрацията и демонстрацията могат да бъдат базирани на използването на широк набор от технологии. Всъщност всеки един класически метод на обучение може да получи нови изрази в условията на масово използване на генеративен изкуствен интелект. В различните университети се подхожда по различен начин – някъде се създават специални дисциплини, насочени към разглеждане на възможностите на генеративния изкуствен интелект в методически план, на други места се интегрират тези елементи в съществуващи дисциплини, а най-често се съчетават двата подхода. Така например в Шуменския университет се въведе факултативна дисциплина „Приложения с изкуствен интелект в работата на учителя“, но на практика тези въпроси се засягат и в редица съществуващи дисциплини. В Софийски университет се предлага избираема дисциплина „Елементи на изкуствения интелект“. При работата в рамките на всички дисциплини е добре да се прилага така наречената „политика на светофара“ [20], при която се дефинира по какъв начин следва да се използва генеративния изкуствен интелект при решаването на конкретна задача.

Етични норми

Въпросите, свързани с етичното използване на готови материали, преминаха на едно ново ниво. Илюзията за липсата на нещо „нередно“ при представяне на генериран текст за свое дело доведоха до необходимостта да се обърне специално внимание върху етичната страна на въпроса при подготовка на учители. Добра практика е внедряването на подобни въпроси в съществуващи дисциплини от ОКС „бакалавър“ и „магистър“, като следва да отбележим, че това е необходимо за всички студенти, а не само за бъдещите учители. Една възможност при подготовката на педагогически специалисти е включването на подобни въпроси в рамките на задължителната дисциплина „Информационни и комуникационни технологии в обучението и работа в дигитална среда“ за бакалаври и дисциплина, насочена към педагогическите изследвания – за магистри [15].

Нагласи на бъдещите учители

Съществуват много изследвания, насочени към нагласите за използване на генеративен изкуствен интелект от бъдещи и действащи учители. Динамичната ситуация обаче внася постоянни промени както в способностите и желанието да се използват тези технологии, така и към усещанията от „самостоятелно“ свършената работа. Така през 2023 година участници в такова проучване посочиха някои негативи към идеята да се използва изкуствен интелект [26], а оценката на възможностите в бъдещата им работа е представена на фигура 1.



Фигура 1. Отговори на въпроса „Считате ли, че работата с чатбот с AI е полезна в работата на учителя?“ [26]

Данните от мащабно проучване сред 23 218 студенти от 109 държави на тема „Higher Education Students' Evolving Perceptions of ChatGPT: Global Survey Data from the Academic Year 2024–2025“ са предоставени за използване [1], като следва да отбележим, че сред респондентите има и около 300 български студенти.

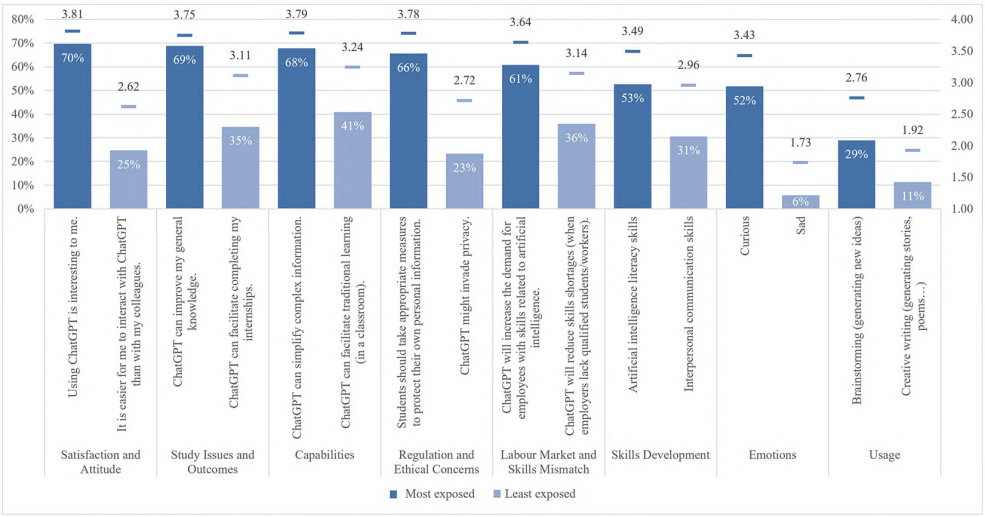
На фигура 2 [16] са посочени най-често и най-рядко избираните възможности в анкета, насочена към нагласите при използване на ChatGPT. В момента се събират данни за проучване на нагласите, актуални към 2025 година. Следва да отбележим, че тези данни до голяма степен кореспондират с наблюдаваните и дискутираните на локално ниво резултати.

Наблюдения върху работата на бъдещите учители

Тук ще представим някои експерименти проведени сред бъдещи учители по математика, свързани с приложението на генеративен изкуствен интелект, отчитащи не само начина на приложение, но и етичната страна на въпроса.

Задачи-провокации

В периода 2020-2025 г. сред над 300 обучаеми в следдипломна квалификация „Учител по математика“ и студенти от специалностите „Информационни технологии, информатика и математика“ и „Педагогика на обучението по икономика и математика“, в рамките на дисциплините „Методика на обучението по математика“, „Училищен курс по геометрия“ и „Елементи от комбинаторика, теория на вероятностите и статистика в училищния курс по математика“ за самостоятелна работа, наред с „коректни задачи“ се предлагаха и преопределени, неопределени и задачи с подвеждащи чертежи. Студентите не бяха предупреждавани за това. „Задачите в



Фигура 2. Най-често и най-рядко избираните възможности в анкета, насочена към нагласите при използване на ChatGPT [16]

училищния курс по математика обикновено са определени. Ако по някакъв начин се появи друг вид задача според условието, учениците дори не го забелязват, защото нямат такава подготовка. Ако пък информацията в задачата не е достатъчна, то това може да се отъждествви с неумение да се реши задачата.“ [25] Тук ще представим някои примери на такъв тип задачи и ще анализираме стила на работа и реакциите на студентите преди и след достъпа до чатботове с изкуствен интелект:

Задача 1: (Преопределена, противоречива). Дължините на бедрата на трапец са 6 cm и 14 cm. Средната му основа го дели на две части, чиито лица се отнасят в отношение 7 към 13. Да се намери радиуса на вписаната в трапеца окръжност.

Задачата беше давана за домашна работа. Почти всички студенти се „справяха“ със задачата, като достигаха до отговор $\frac{4\sqrt{5}}{3}$ см. Решението изглеждаше правдоподобно и много малка част от обучаемите достигаха до извода, че описаната в задачата фигура реално не съществува. До момента, в който студентите имаха достъп до чатботове с изкуствен интелект, процентът на забелязалите противоречието бе под 4 %.

Задача 2: (Преопределена, непротиворечива) На парти имало 37 човека, които харесвали народна музика, 37 човека, които слушали само рап, 74 – само поп-фолк и 111 – само рок. Други нямало!

За „късмет” DJ-ят имал по един диск от всеки стил.

Каква е вероятността при произволно избран диск той да угоди на хората, които обичат поп-фолк?

Задачата беше давана за самостоятелна работа в час. Близо половината от обучаемите се подвеждаха поради наличието на много числови данни в задачата, но бързо осъзнаваха грешката си. В допълнение към тази задача на тези, които допускаха грешка, се задаваше задача да съставят задача по дадените данни така,

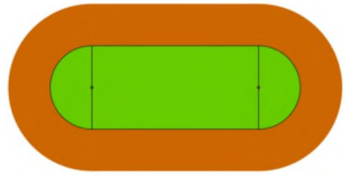
че тяхното решение да е вярно. След което и допълнителни подточки, базирани на същите данни. При тази задача никой от обучаемите не прибягна към помощта на чатботовете, въпреки че имаха такава възможност.

Студентите приеха много положително идеята класическите системи от задачи по темата да бъдат обогатявани с подобен вид задачи.

Задача 3: (Указано в условието неопределена) Представете си, че трябва да направите проект за изграждане на писта за лека атлетика, която трябва да е като на илюстрацията (Фигура 3). Пространството, заобиколено от пистата, ще се използва за състезания по различни спортни дисциплини. То трябва да бъде засято с трева. [23]

А) определете вие необходимите размери на пистата и пресметнете колко кв. м. трева ви е необходима.

Б) ако пистата е широка 30 метра, то колко ще е дълга оградата ѝ?

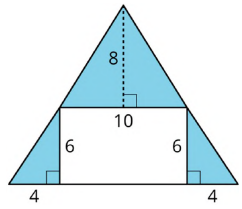


Фигура 3. Стадион [23]

В задачата се изисква от учениците да вложат творчество и да проучат реалистични размери на съществуващи писти. При работата с бъдещи учители тази задача бе давана като пример, като бяха поискани подобни задачи от обучаемите. Основните примери, които бяха предложени от студентите, бяха свързани с поставяне на плочки с различни размери и при различни условия, конструиране на покриви и т.н. Преобладаващата част от студентите се опираха на вече създадени примери в рамките на материалите по проекта MEGA [10], които те приемаха с голямо въодушевление, или такива, свързани с природни науки и изкуство [6].

Задача 4: (подвеждащ чертеж)

Намерете лицето на оцветената част (Фигура 4) по два различни начина. [21]



Фигура 4. „Триъгълник“ [23]

Задачата бе давана за самостоятелна работа по време на занятия, с предварителна кратка беседа за начините, по които бихме могли да намерим лицето, след което групата се разделяше на две, като всяка група изчисляваше лицето по съответния начин. Студентите се учудваха защо им се предлага толкова лека задача, но въпреки

това разсъждаваха и решаваха задачата. Някои студенти изчисляваха и по двата начина. Всички бяха подведени от чертежа, но впоследствие достигаха до извода, че чертежът е некоректен. Някои студенти начертаха точен чертеж. Задачата бе приета с голям интерес, като в методическите си разработки на по-късен етап студентите включваха подобни задачи. Никой от студентите не прибегна до помощта на чатбот. Обяснението за това може да е, че чертежът не беше предоставен като файл. За точния чертеж студентите предпочитаха да използват GeoGebra.

Влиянието на генеративния изкуствен интелект

За периода 2020-2023 г., въпреки че в рамките на самостоятелната работа студентите имаха възможност да обменят информация помежду си, под 4% от тях осъзнаха проблемите в Задача 1, като половината от тях предложиха аргументи за несъществуващия обект, а останалите преценихa, че задачата е „сгрешена“ и само посочиха този факт. Приблизително 5 % не представиха решение на задачата, а останалите представиха „решение“, достигащо до отговора, описан по-горе. След навлизането на възможността за използване на чатботове с изкуствен интелект тези проценти се промениха коренно. Почти всички специализанти и студенти „забелязваха“ проблема, като този път преобладаваща част от тях само посочваха, че задачата е сгрешена, без да дават подробно обяснение къде е проблемът.

При неопределените задачи, когато те бяха давани за самостоятелна работа, почти всички студенти достигаха до извода, че нещо липсва, и също приемаха, че задачата е „сгрешена“.

В занятието, където се обсъждаха дадените решения, бъдещите учители осъзнаваха „капаните на шаблона“, в който са попаднали, и възможностите за провокиране на мисленето с помощта на подобен тип задачи. За съжаление в последващите методически разработки много малко от тях предлагаха авторски, или поне различни от предложените в обучението задачи от типа на Задача 1. Задачи от останалите типове се срещаха в някои от разработените от студентите и специализантите уроци, но също бяха базирани на разгледаните примери и посочените ресурси.

В продължение на задачата за наблюдение на проявените разлики в представянето на студентите с и без използване на чатботове с изкуствен интелект, както и на показаните данни от изследването на нагласите на обучаемите, през 2025 година сред студенти бе проведен експеримент, насочен към стимулиране и забрана за използване на генеративен изкуствен интелект за решаване на методически задачи. Основните задачи, които се поставяха пред студентите, бяха:

- Да се състави план-конспект на урок/педагогическа ситуация.
- Да се опише STEAM проект.
- Да се предложат софизми, приложими в обучението по математика.
- Да се състави дидактически тест/задачи и игри за деца от детска градина с диагностична цел.

Обхванати бяха студенти от образователна квалификационна степен (ОКС) „бакалавър“ от специалностите „Информационни технологии, информатика и математика“, „Педагогика на обучението по икономика и математика“ и от ОКС „магистър“

„Педагогика на обучението по математика“ в рамките на задължителни и избираеми дисциплини с методически и педагогически характер, както и от ОКС „професионален бакалавър“ от специалност „Предучилищна педагогика и чужд език (Английски език)“, гр. Добрич, в рамките на дисциплината „Методика на формиране на елементарни математически представи и понятия“.

Задачите се даваха в различни условия – по време на занятията студентите можеха да използват само учебници, книги за учителя и помагала. За софизмите се използваха примери от Методика на обучението по математика [25]. За домашна работа студентите трябваше да се справят с аналогични задачи, но с различна тематика. Този път условието беше да се използва генеративен изкуствен интелект, като се укаже в цвят или да се опише при представянето каква част е генерирана, а каква е авторска. По време на представянето на задачите студентите коментираха своите преживявания в двата варианта на работа.

Поради различните нива на сложност на материята при учителите по математика и детските учители се оформиха коренно различни резултати при справяне със задачите при работа в двата варианта.

При бъдещите детски учители работата без технологии се оказа достатъчно продуктивна, като голяма част от студентите предложиха авторски игри, примери и сценарии за реализирането на педагогическите ситуации. При студентите, подготвящи се за учители (5. – 12. клас), тенденцията бе да се повтаря схемата предложена в предоставените учебници, без обогатяване на предложените примери и системи от задачи.

При работата с помощта на генеративен изкуствен интелект при бъдещите учители се оформиха три основни групи потребители:

1. *Силно използващи.* Тези студенти не бяха променили нищо с аргумента, че няма какво повече да се направи.

2. *Балансирано използващи.* Тези студенти генерираха идеи за задачи, игри и създаваха изображения, които пречупваха през своя поглед, за да ги адаптират за използване. Използваха и за методическото описание на урока.

3. *Неизползващи.* Тези студенти отказваха да използват подобен тип помощ или я използваха минимално. Аргументът им беше, че така им е по-приятно да работят, като следва да отбележим, че голяма част от тях използваха готови ресурси от интернет.

При учителите в детските градини съотношението между трите групи се получи в съотношение 50% – 23% – 27%, а в училище – 83% – 17% – 0%. Близо половината студенти забравяха да отбележат в цвят генерираната част или да отбележат генерираната част от текста, въпреки изискванията в задачата и разрешението да се използват чатботове. При последваща дискусия се изясняваше, че основно са използвали ChatGPT, като студентите сами посочваха какво са генерирали и защо са решили точно за това да използват чатбота. Детските учители генерираха и изображения за своите игри. Въпреки запознаването с различни платформи за генериране на план-конспекти, базирани на изкуствен интелект, студентите масово използваха ChatGPT. Съчетаването на работа с и без използване на чатбот доведе студентите до основния извод, а именно – трябва да полагат усилия, за да включват

в генерираните материали авторски елементи, за да не станат безпомощни в случаите, когато нямат възможност да използват генеративен изкуствен интелект и други ИКТ. Студентите осъзнават необходимостта да са подготвени за различни условия за работа, но забелязват своята „пристрастеност“ към използването на изцяло готов продукт. Някои студенти споделиха страхове за своето когнитивно развитие в условията, когато „могат“ да решат практически всяка поставена задача, без да полагат усилия.

Тенденциите според ChatGPT

Основавайки се на гореизложеното, с помощта на ChatGPT [13] ще резюмираме основните тенденции в подготовката на учители по математика в епохата на изкуствения интелект. Дадените направления кореспондират с описаните в Таблица 1 приноси.

1. Интеграция на ИИ в обучението по методика на математиката

- Използване на ИИ инструменти за генериране на план-конспекти, задачи, варианти на тестове, онагледяване и упражнения.
- Включване в подготовката на учители на модули за работа с платформи, базирани ИИ (адаптивни системи, образователни чатботове).

2. Промяна на фокуса от преподаване на съдържание към преподаване на умения

- Засилване на акцентите върху критично мислене, математическо моделиране, умение за формулиране на проблеми, проверка на коректността на решения, генерирани от ИИ.

3. Развитие на дигитална компетентност на учителя

- Умения за работа с ИИ като помощник: анализ на решения, генериране на примери, проверка на домашни.
- Етика и безопасност при използването на ИИ в училищна среда.

4. Персонализирано обучение на бъдещите учители

- Платформи, които анализират учебния процес на студентите и предлагат персонални препоръки за подобрение, основани на потребностите на всеки отделен обучаем.

5. Развитие на методи за оценяване, подпомогнати от ИИ

- Автоматизирано оценяване на рутинни задачи.
- Анализ на грешки и типични затруднения на учениците.
- Нови формати за изпити, отчитащи възможността за използване на ИИ.

6. Хибридни модели на практика

- Реалистични симулации на класна стая с виртуални ученици, които реагират като реални.
- Наблюдение и анализ на урок, подпомогнато от ИИ инструменти (педагогически анализ на реч, темпо, взаимодействия).

7. Интердисциплинарност

- Обвързване на математиката с информатиката, природни науки и други учебни предмети.

Представените по-горе идеи кореспондират основно с втория пункт от тези направления, но индиректно засягат и първи, и трети пункт.

Заключение

Условията, в които се подготвят бъдещите учители са толкова динамични, че на практика образователната система остава постоянно в догонваща позиция. Нагласите и стилът на работа с генеративен изкуствен интелект също търпят постоянни промени, изместващи се към пренасянето на поставяните задачи към избран чатбот. Основавайки се на проведените проучвания и експериментирайки с различни подходи, можем да твърдим, че е важно да се обогатят системите от задачи, включвани в рамките на различни дисциплини, и задаваните на студентите курсови работи с нетрадиционни за училищната математика задачи (неопределени, преопределени, с подвеждащи чертежи и т.н.), които да провокират критичното мислене и използването на изследователски подход.

Предизвикването на различни емоции при сблъсък с неочакван проблем стимулира мисленето и предизвиква самостоятелно търсене на подобни казуси и задачи. Подобен подход е важен при работа и с ученици, и със студенти, като е особено важно бъдещите учители да го усетят и в ролята си на обучаеми, за да могат органично да го внедрят в работата си като учители.

References

[1] Aristovnik, A., Ravšelj, D., Keržič, D., Tomaževič, N., Umek, L., Brezovar, N., et al. 2025, *Higher Education Students' Evolving Perceptions of ChatGPT: Global Survey Data from the Academic Year 2024–2025*, Mendeley Data, V1, https://doi.org/10.17632/nv2343nwsb.1

[2] Atchley, P., Pannell, H., Wofford, K., Hopkins, M., Atchley, R. Human and AI collaboration in the higher education environment: opportunities and concerns. *Cognitive Research: Principles and Implications*, 2024, 9(1). https://doi.org/10.1186/s41235-024-00547-9

[3] Awang, L. A., Yusop, F. D., Danaee, M. Current practices and future direction of artificial intelligence in mathematics education: A systematic review. *International Electronic Journal of Mathematics Education*, 2025, 20(2), em0823. https://doi.org/10.29333/iejme/16006

[4] Blonder, R., Feldman-Maggor, Y. & Rap, S. Are They Ready to Teach? Generative AI as a Means to Uncover Pre-Service Science Teachers' PCK and Enhance Their Preparation Program. *J Sci Educ Technol* (2024). https://doi.org/10.1007/s10956-024-10180-2

[5] Chalkiadakis, A., Seremetaki, A., Kanellou, A., Kallishi, M., Mastrokoukou, S., Morfopoulou, A., Moraitaki, M. Impact of Artificial Intelligence and Virtual Reality on Educational Inclusion: A Systematic Review of Technologies Supporting Students with Disabilities. *Education Sciences*, 2024. 14(11), 1223. https://doi.org/10.3390/educsci14111223

[6] Chehlarova, N., Gachev, G. Online contest „Mathematics and art“ for the development of key competencies, *Pedagogica*, Volume 93, Number 1. 2021. https://doi.org/10.53656/ped2021-1.07, 87-99

[7] Dilling, F., Herrmann, M. Using large language models to support pre service teachers' mathematical reasoning — an exploratory study on ChatGPT as an instrument for creating mathematical proofs in geometry, *Frontiers in Artificial Intelligence*. 2024, Vol. 7, Art. 1460337, https://www.frontiersin.org/journals/artificial-intelligence/articles/10.3389/frai.2024.1460337/full

[8] Engelbrecht, J., Borba, M. Recent developments in using digital technology in mathematics education. ZDM–Mathematics Education, 2024, 56(2), pp. 281-292. https://doi.org/10.1007/s11858-023-01530-2

[9] Espino, C. Pre Service Teachers' Perspectives on Generative AI: Insights, Applications, and Challenges in the Classroom, *International Journal on Studies in Education (IJonSE)*. 2025, Vol. 7, № 3, pp. 732–747, https://doi.org/10.46328/ijonse.1930

[10] MEGA, https://www.smbvarna.eu/ÑĂĐμÑĄÑČÑĂÑĄĐÿ/ĐůĐř-ÑČÑĞĐÿÑĆĐμĐżÑŔ

[11] Nikolova N., Zafirova-Malcheva T., Kirilova B., Mihnev P. Development of digital competences in the Bulgarian secondary school context–a literature review of good practices. *Front. Educ.* 9:1434797. 2024. https://doi.org/10.3389/feduc.2024.1434797

[12] Noster, N., Gerber, S., Siller, H.-S. Pre Service Teachers' Approaches in Solving Mathematics Tasks with ChatGPT, *Digital Experiences in Mathematics Education*. 2024, Vol. 10, pp. 543–567, https://doi.org/10.1007/s40751-024-00155-8.

[13] OpenAI. ChatGPT (December version) [Large language model]. 2025. https://chat.openai.com/.

[14] Pavlova, N. Flipped dialogic learning method with ChatGPT: A case study. *International Electronic Journal of Mathematics Education*, vol. 19, no.1., 2024. https://doi.org/10.29333/iejme/14025.

[15] Pavlova, N., Marchev, D. Use of artificial intelligence – ethical norms and implementation in the training of future teachers, *Mathematics and Education in Mathematics*, 2024, pp. 154-160, https://doi.org/10.55630/mem.2024.53.154-160

[16] Ravšelj D, Keržič D, Tomaževič N, Umek L, Brezovar N, A. Iahad N, et al. (2025) Higher education students' perceptions of ChatGPT: A global study of early reactions. *PLoS ONE* 20(2): e0315011. https://doi.org/10.1371/journal.pone.0315011

[17] Semenov, A., Abylkassymova, A. Training the Future Mathematics Teacher: the Key to Change, *Lomonosov Pedagogical Education Journal*. 2024, Vol. 22, № 2 . pp. 9–28, https://msupedj.ru/articles/article/11102/

[18] Setälä, M., Heilala, V., Sikström, P., Kärkkäinen, T. The Use of Generative Artificial Intelligence for Upper Secondary Mathematics Education Through

the Lens of Technology Acceptance, In *Proceedings of the 40th ACM/SIGAPP Symposium on Applied Computing (SAC '25)*. Association for Computing Machinery, New York, NY, USA, 74–82. https://doi.org/10.1145/3672608.3707817

[19] Tang, W. Artificial Intelligence in Mathematics Education: Trends, Challenges, and Opportunities. *IJRME* 2025, 3, pp. 75-90. https://doi.org/10.24090/ijrme.v3i1.13496

[20] Traffic Light System for Generative AI Use in Module Assignments: UCD College of Arts and Humanities, https://www.ucd.ie/artshumanities/study/aifutures/trafficlightsystem/

[21] Writing Equations for Lines, https://math.libretexts.org/Bookshelves/PreAlgebra/Pre-Algebra_II_(Illustrative_Mathematics_-_Grade_8)/02%3A_Dilations_Similarity_and_Introducing_Slope/2.03%3A_New_Page/2.3.2%3A_Writing_Equations_for_Lines

[22] Zhuang, Y., Zhang, S. Pre service mathematics teachers' perceptions of using GenAI for practicing teacher questioning: A semester long study, Eurasia Journal of Mathematics, *Science and Technology Education*. 2025, Vol. 21, № 9, Art. em2689, https://doi.org/10.29333/ejmste/16764

[23] Георгиева, С. *Проблемно-творчески модел на обучение по математика в 6. клас*, УИ „Епископ Константин Преславски“, ISBN 978-619-201-474-2, 2021. [Georgieva, S. *Problemno-tvorcheski model na obuchenie po matematika v 6. klas*, UI „Episkop Konstantin Preslavski“, ISBN 978-619-201-474-2, 2021.] (in Bulgarian)

[24] Иванова, Кр., Нишева, М., Ескенази, А., Ангелова, Г., Манева, Н. Изкуствен интелект в и за образованието в България – мерки за постигане на надежден интелигентен растеж, *XIII Национална конференция „Образованието и изследванията в информационното общество”* (2020), 7-20. [Ivanova, Kr., Nisheva, M., Eskenazi, A., Angelova, G., Maneva, N. Izkustven intelekt v i za obrazovanieto v Balgariya – merki za postigane na nadezhden inteligenten rastezh, *XIII Natsionalna konferentsiya „Obrazovanieto i izsledvaniyata v informatsionnoto obshtestvo”* (2020), 7-20.] (in Bulgarian)

[25] Нинова, Ю., Петров, Ф. *Методика на обучението по математика (Обща методика)*, Университетско издателство „Св. Климент Охридски“, ISBN: 978-954-07-6137-4, 2025. [Ninova, Yu., Petrov, F. *Metodika na obuchenieto po matematika (Obshta metodika)*, Universitetsko izdatelstvo „Sv. Kliment Ohridski“, ISBN: 978-954-07-6137-4, 2025.] (in Bulgarian).

[26] Павлова, Н. Нагласи на бъдещите учители за прилагане на изкуствен интелект в обучението, *Математика и информатика*, 67(4), 418-432. 2024. https://doi.org/10.53656/math2024-4-5-att

СЕКЦИЯ А: МАТЕМАТИЧЕСКИ СТРУКТУРИ

SECTION A: MATHEMATICAL STRUCTURES

МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2026
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2026
Proceedings of the Fifty-Fifth Spring Conference
of the Union of Bulgarian Mathematicians
Tryavna, Bulgaria, April 5–9, 2026

FOCAL SURFACES OF DEVELOPABLE RULED SURFACES AND THEIR INVARIANTS

Cvetelina Dinkova[1], Radostina Encheva[2]
Faculty of Mathematics and Informatics,
Konstantin Preslavsky University of Shumen, Shumen, Bulgaria
e-mails: [1]c.dinkova@shu.bg, [2]r.encheva@shu.bg

In this work the focal surfaces of developable ruled surfaces generated by a unit speed Frenet curve and its focal curve in the Euclidean three-dimensional space are investigated. For each curve, we construct the associated tangential surface and derive a parametrization of its focal surface. Working with respect to the natural parameter of the base curve, we obtain relations between the coefficients of the two fundamental forms of the original developable surfaces and those of their focal surfaces. The focal surfaces obtained in both cases are themselves developable. Formulas relating to their mean curvatures are established.

Keywords: Frenet curves, Focal curves, Ruled surfaces, Developed surfaces, Focal surfaces, Gauss curvature, Mean curvature

ФОКАЛНИ ПОВЪРХНИНИ НА РАЗВИВАЕМИ ПРАВОЛИНЕЙНИ ПОВЪРХНИНИ И ТЕХНИТЕ ИНВАРИАНТИ

Цветелина Динкова[1], Радостина Енчева[2]
Факултет по математика и информатика,
Шуменски университет „Епископ Константин Преславски“, Шумен, България
e-mails: [1]c.dinkova@shu.bg, [2]r.encheva@shu.bg

В тази работа са изследвани фокалните повърхнини на развиваеми линейни повърхнини, получени от крива на Френе, параметризирана спрямо естествен параметър, и нейната фокална крива в Евклидовото тримерно пространство. За всяка крива конструираме съответната тангенциална повърхнина и извеждаме параметризация

https://doi.org/10.55630/mem.2026.55.049-059

2020 Mathematics Subject Classification: 53A04; 53A05; 51M15.

* This research is partially supported by Scientific Research Grant RD-08-58/27.01.2026 of Konstantin Preslavsky University of Shumen.

на нейната фокална повърхнина. Работейки относно естествения параметър на базовата крива, получаваме зависимости между коефициентите на двете основни форми на оригиналните развиваеми повърхнини и тези на техните фокални повърхнини. Получените и в двата случая фокални повърхнини са развиваеми. Установени са формули, свързващи средните им кривини.

Ключови думи: Крива на Френе, Фокална крива, Праволинейна повърхнина, Развиваема повърхнина, Фокална повърхнина, Гаусова кривина, Средна кривина

1 Introduction

Ruled surfaces are important in both classical and contemporary differential geometry because of their intricate structures and their extensive use in geometric modelling, computer-aided design, and kinematic surface creation. Their geometry is determined by the invariants of the basic base curve, and these invariants—namely, curvature and torsion—offer a fundamental framework for evaluating the behaviour of such surfaces under Euclidean motions. An interesting approach in this context is the examination of focal surfaces, which occur as envelopes of normal lines and include essential curvature information for the original surface. For cylinders, cones, and offset surfaces, focal surfaces show important geometric relations, and hence they have been extensively studied. Focal and generalized focal surfaces are crucial for curvature-based constructs like manufacturing, optical modelling, and computer-aided geometric design, according to recent studies. Georgiev and Pavlov (see [4], [5], [6], [7], [8]), in particular, show how focal surfaces reflect classical surfaces' intrinsic geometry and how their invariants can characterise curvature-dependent offset surfaces. In [11], Güler provides an intriguing perspective on the focal surfaces of offset surfaces. Despite this progress, the focal surfaces of developable ruled surfaces generated by space curves remain less explored. Tangential surfaces—ruled surfaces formed by attaching tangent lines along a Frenet curve—are a fundamental class of developable surfaces. Their focal surfaces obviously preserve developability, a classical result in the differential geometry of surfaces (see [2],[3],[15]), but it is not immediately clear how their fundamental forms and curvature invariants relate to those of the original ruled surfaces.

In this paper, we construct new surfaces in the Euclidean space $\mathbb{E}^3$ as tangential surfaces generated by a pair of spatial curves, a Frenet curve $\boldsymbol{\gamma}$ and its focal curve $\boldsymbol{C}_\gamma$. By examining tangential surfaces obtained by a Frenet curve and by its focal curve, we aim to clarify the geometric structure of their focal surfaces and to establish explicit relationships between their invariants. The final section illustrates the theoretical findings with an explicit example involving a cylindrical curve and its focal curve, together with visualizations of the corresponding developable and focal surfaces.

The following section presents key terminology and important information regarding focal curves and focal surfaces.

2 Preliminaries

2.1 Frenet curves in the Euclidean three-space

The Euclidean three-dimensional space $\mathbb{E}^3$ is regarded as an affine space, and it has a vector space $\mathbb{R}^3$ that is related to it. The position column vector from $\mathbb{R}^3$ can be used to represent any point in $\mathbb{E}^3$. The scalar (or dot) product $\langle \boldsymbol{a}, \boldsymbol{b} \rangle \in \mathbb{R}$ and the vector cross product $\boldsymbol{a} \times \boldsymbol{b} \in \mathbb{R}^3$ are well-known operations for any two column vectors $\boldsymbol{a} \in \mathbb{R}^3$ and $\boldsymbol{b} \in \mathbb{R}^3$. The norm of the vector $\boldsymbol{a}$ is $\|\boldsymbol{a}\| = \sqrt{\langle \boldsymbol{a}, \boldsymbol{a} \rangle} = \sqrt{\boldsymbol{a}^2}$.

Assume $\gamma : I \longrightarrow \mathbb{E}^3$ be a curve described by a vector parametric equation

$$\boldsymbol{\gamma}(q) = (x(q),\, y(q),\, z(q))^T \,, \quad q \in I \tag{1}$$

on an interval $I \subseteq \mathbb{R}$. The coordinate functions $x(q)$, $y(q)$, $z(q)$ are supposed to have continuous derivatives up to order 3. We will refer to that curve as a regular C^3 space curve. If the derivatives $\boldsymbol{\gamma}'(q)$, $\boldsymbol{\gamma}''(q)$ and $\boldsymbol{\gamma}'''(q)$ are linearly independent vectors in $\mathbb{E}^3$ for every $q \in I$, then the curves are known as Frenet curves. For a Frenet curve γ, the Euclidean curvatures of γ in $\mathbb{E}^3$ (a curvature $\varkappa$ and a torsion τ) are determined by

$$\varkappa(q) = \frac{\|\boldsymbol{\gamma}'(q) \times \boldsymbol{\gamma}''(q)\|}{\|\boldsymbol{\gamma}'(q)\|^3} > 0,\ \tau(q) = \frac{\langle \boldsymbol{\gamma}'(q) \times \boldsymbol{\gamma}''(q), \boldsymbol{\gamma}'''(q) \rangle}{\|\boldsymbol{\gamma}'(q) \times \boldsymbol{\gamma}''(q)\|^2} \neq 0 \tag{2}$$

Moreover, there are three unit vectors

$$\boldsymbol{t}(q) = \frac{\boldsymbol{\gamma}'(q)}{\|\boldsymbol{\gamma}'(q)\|}, \boldsymbol{n}(q) = \frac{\big(\boldsymbol{\gamma}'(q) \times \boldsymbol{\gamma}''(q)\big) \times \boldsymbol{\gamma}'(q)}{\|\boldsymbol{\gamma}'(q) \times \boldsymbol{\gamma}''(q)\|.\|\boldsymbol{\gamma}'(q)\|}, \boldsymbol{b}(q) = \frac{\boldsymbol{\gamma}'(q) \times \boldsymbol{\gamma}''(q)}{\|\boldsymbol{\gamma}'(q) \times \boldsymbol{\gamma}''(q)\|} \tag{3}$$

defined at any point $\boldsymbol{\gamma}(q)$ of the curve. A positively orientated orthonormal basis known as a Frenet frame is formed by these three vectors.

In the case that the Frenet curve $\gamma : I \longrightarrow \mathbb{E}^3$ is a unit speed curve, namely, $\|\boldsymbol{\gamma}'(q)\| = 1$ for any $q \in I$, the parameter q is usually substituted with the parameter s, and the vector equation (1) is referred to as an arc-length parametrisation of γ. In this instance, a more straightforward form of the formulas (2) and (3) can be used. Especially, the torsion and the curvature are defined by the equations

$$\varkappa(s) = \|\boldsymbol{\gamma}''(s)\| > 0 \quad \text{and} \quad \tau(s) = \frac{\langle \boldsymbol{\gamma}'(s) \times \boldsymbol{\gamma}''(s), \boldsymbol{\gamma}'''(s) \rangle}{\|\boldsymbol{\gamma}''(t)\|^2} \neq 0,$$

respectively. Further, the Frenet-Serret equations

$$\boldsymbol{t}'(s) = \varkappa(s)\boldsymbol{n}(s), \quad \boldsymbol{n}'(s) = -\varkappa(s)\boldsymbol{t}(s) + \tau(s)\boldsymbol{b}(s), \quad \boldsymbol{b}'(s) = -\tau(s)\boldsymbol{n}(s).$$

for the unit speed curve γ are fulfilled.

Henceforth, we shall use "$'$" for the differentiation concerning a natural parameter and "$\cdot$" as the differentiation concerning an arbitrary parameter.

Definition 1. *[10, p.241] The **focal curve** of a regular C^3 space curve $\gamma : I \to \mathbb{E}^3$ is the curve given by*

$$\boldsymbol{C}_{\boldsymbol{\gamma}}(q) = \boldsymbol{\gamma}(q) + c_1(q)\boldsymbol{n}(q) + c_2(q)\boldsymbol{b}(q),$$

where $\boldsymbol{n}$ is a principal unit normal vector field of γ, $\boldsymbol{b}$ is a binormal unit vector field of $\boldsymbol{\gamma}$. The coefficients $c_1(q)$ and $c_2(q)$ are smooth functions called focal curvatures of γ, given by

$$c_1(q) = \frac{1}{\varkappa(q)}, \quad c_2(q) = -\frac{\frac{d}{dq}\varkappa(q)}{\| \frac{d\boldsymbol{\gamma}(q)}{dq} \| \varkappa(q)^2\tau(q)} = \frac{\frac{dc_1(q)}{dq}}{\| \frac{d\boldsymbol{\gamma}(q)}{dq} \| \tau(q)},$$

where $\varkappa(q) > 0$ and $\tau(q) \neq 0$ are the Euclidean curvatures of γ.

In other words, the focal curve of an immersed smooth curve γ, in the Euclidean space $\mathbb{E}^3$, consists of the centres of its osculating spheres. The functions $c_1(q)$ and $c_2(q)$ are well defined because $\varkappa(q)$ and $\tau(q)$ are non-zero functions. In addition, the parametrization of the focal curve of the unit speed curve $\boldsymbol{\gamma}$ becomes

$$\boldsymbol{C}_\gamma(s) = \boldsymbol{\gamma}(s) + \frac{1}{\varkappa(s)}\boldsymbol{n}(s) + \left(\frac{1}{\varkappa(s)}\right)' \frac{1}{\tau(s)}\boldsymbol{b}(s). \tag{4}$$

According to [16], for the Frenet frame $\boldsymbol{T}$, $\boldsymbol{N}$, and $\boldsymbol{B}$, as well as the Euclidean curvatures $\varkappa_{C_\gamma}$ and τ_{C_γ} of the curve C_γ, we have

$$\boldsymbol{T} = \delta\boldsymbol{b},\ \boldsymbol{N} = -\varepsilon\boldsymbol{n},\ \boldsymbol{B} = \delta\varepsilon\boldsymbol{t};\ \varkappa_{C_\gamma} = \frac{|\tau|}{|c_1\tau + c_2'|} = \varepsilon\frac{\tau}{c_1\tau + c_2'},\ \tau_{C_\gamma} = \frac{\varkappa}{c_1\tau + c_2'}, \tag{5}$$

where $\delta = sign(c_1\tau + c_2')$ and $\varepsilon = sign(\tau)\delta$. We consider only non-spherical curves γ, where $c_1\tau + c_2' \neq 0$.

The differential geometry of space curves is described in more detail in [10].

2.2 Ruled surfaces associated with a space curve

This section presents precise formulas for the invariants of ruled surfaces related to a space curve. A ruled surface in $\mathbb{E}^3$ is (locally) represented by the mapping $S(u,v) : I \times I \longrightarrow \mathbb{E}^3$ defined as $S(u,v) = \boldsymbol{\gamma}(u) + v\boldsymbol{l}(u)$, where $\gamma : I \longrightarrow \mathbb{E}^3$ and $l : I \longrightarrow \mathbb{E}^3\backslash\{0\}$ are smooth functions, and I is an open interval. We designate γ as the base curve and l as the director curve. The straight lines $v \to \boldsymbol{\gamma}(u) + v\boldsymbol{l}(u)$ are referred to as the rulings of $S(u,v)$ (see [10]). Let $S(u,v)$ represents a ruled surface. We define $S(u,v)$ as *developable* if its Gaussian curvature is zero. From this point further on, we shall presume that $\|\boldsymbol{l}(u)\| = 1$. It is easy to show that the Gaussian curvature $K(u,v)$ and the Mean curvature $H(u,v)$ of a ruled surface $S(u,v)$ are

$$K(u,v) = -\left(\frac{\det(\boldsymbol{\gamma}'(u), \boldsymbol{l}(u), \boldsymbol{l}'(u))}{EG - F^2}\right)^2,$$

$$H(u,v) = \frac{\det(\boldsymbol{\gamma}'(u) + v.\boldsymbol{l}'(u), \boldsymbol{l}(u), \boldsymbol{\gamma}''(u) + v.\boldsymbol{l}''(u)) - 2\langle\boldsymbol{\gamma}'(u), \boldsymbol{l}(u)\rangle.\det(\boldsymbol{\gamma}'(u), \boldsymbol{l}(u), \boldsymbol{l}'(u))}{2\sqrt{EG - F^2}^3}$$

where $E = E(u,v) = S_u^2 = \|\boldsymbol{\gamma}'(u) + v\boldsymbol{l}'(u)\|^2$, $F = F(u,v) = \langle S_u, S_v\rangle = \langle\boldsymbol{\gamma}'(u), \boldsymbol{l}(u)\rangle$ and $G = G(u,v) = S_v^2 = \|\boldsymbol{l}(u)\|^2 = 1$ are the coefficients of the First Fundamental Form of $S(u,v)$. By $\det(\cdot,\cdot,\cdot)$ we denote the determinant of the corresponding column vectors. The ruled surface $S(u,v)$ is a smooth surface if and only if $\boldsymbol{\gamma}'(u)\times\boldsymbol{l}(u) + v.\boldsymbol{l}'(u)\times\boldsymbol{l}(u) \neq 0$ for all $(u,v) \in I \times I$. Some special types of developable ruled surfaces can be found in [1] and [12].

2.3 Focal surfaces of regular surfaces

Definition 2. *Let $S(u,v)$ be a parametric surface of class $\mathcal{C}^2$, and let $\mathfrak{N}(u,v)$ be its unit normal vector field. The parametric offset surface is defined as*

$$\overline{S}(u,v) = S(u,v) + d \cdot \mathfrak{N}(u,v),$$

where d is a nonzero real constant.

Definition 3. *Let $S(u,v)$ be parametric surface of class $\mathcal{C}^2$ and $\mathfrak{N}(u,v)$ be its unit normal vector field. The parametric representations of the focal surfaces of $S(u,v)$ is given by*

$$\overline{S}_1(u,v) = S(u,v) + \frac{1}{\kappa_1}.\mathfrak{N}(u,v),\ \overline{S}_2(u,v) = S(u,v) + \frac{1}{\kappa_2}.\mathfrak{N}(u,v), \tag{6}$$

where κ_1 and κ_2 are principal curvatures of the surface $S(u,v)$.

3 Main results

3.1 Focal surfaces of developable ruled surfaces

The focal surfaces of developable ruled surfaces are likewise developable surfaces. This assertion is a known fact in the classical differential geometry of surfaces. It can be proven using approaches based on the differential geometry of line congruences (see [13],[14]). Let $S_1(s,v) = \boldsymbol{\gamma}(s) + v.\boldsymbol{t}(s)$ be a tangential ruled surface with a base curve γ and a director curve represented by the unit tangent vector $\boldsymbol{t}$ of γ. The obtained surface is developable because the determinat $\det(\boldsymbol{\gamma}'(s), \boldsymbol{l}(s), \boldsymbol{l}'(s)) = \det(\boldsymbol{t}(s), \boldsymbol{t}(s), \boldsymbol{t}'(s))$ is equal to zero. The following theorem will give us an explicit reprezentation of the focal surface of the tangential ruled surface $S_1(s,v)$. We will utilise this representation to provide an alternative proof that the generated surface is also developable and to determine the relation between the mean curvatures of the associated surfaces.

Theorem 1. *Let (1) be a parametrization of a unit speed Frenet curve $\gamma : I \longrightarrow \mathbb{E}^3$ of class C^3 with Frenet frame $\boldsymbol{t}(s), \boldsymbol{n}(s), \boldsymbol{b}(s)$, and let $\varkappa(s) \neq 0$ and $\tau(s) \neq 0$ be the Euclidean curvature and the Euclidean torsion of γ, respectively. Suppose that $S_1(s,v) = \boldsymbol{\gamma}(s) + v.\boldsymbol{t}(s)$ is the developable tangential surface associated with the unit speed Frenet curve γ. Then the focal surface $\overline{S}_1(s,v)$ of $S_1(s,v)$ is also developable and has representation*

$$\overline{S}_1(s,v) = \boldsymbol{\gamma}(s) + v.\left(\boldsymbol{t}(s) + \frac{\varkappa(s)}{\tau(s)}\boldsymbol{b}(s)\right),\ v \in \mathbb{R} \setminus \{0\}.$$

The Mean curvature $\overline{H}_1(s,v)$ of $\overline{S}_1(s,v)$ can be expressed by the Mean curvature $H_1(s,v)$ of $S_1(s,v)$ with the following equation

$$\overline{H}_1(s,v) = -\frac{\tau(1+4v^2H_1^2)}{4|vH_1 + v^2H_{1s}|}, \tag{7}$$

where H_{1s} is the partial derivative of $H_1(s,v)$ with respect s.

Proof. The coefficients of the First Fundamental Form of $S_1(s,v)$ are given by the following equalities

$$\begin{aligned} E_1 &= E_1(s,v) = S_{1s}^2 = \|\boldsymbol{\gamma}'(s) + v\boldsymbol{t}'(s)\|^2 = \|\boldsymbol{t}(s) + v.\varkappa(s)\boldsymbol{n}(s)\|^2 = 1 + v^2\varkappa^2(s), \\ F_1 &= F_1(s,v) = \langle S_{1s}, S_{1v}\rangle = \langle \gamma'(s), \boldsymbol{t}(s)\rangle = \langle \boldsymbol{t}(s), \boldsymbol{t}(s)\rangle = 1, \\ G_1 &= G_1(s,v) = S_{1v}^2 = \|\boldsymbol{t}(s)\|^2 = 1, \end{aligned} \tag{8}$$

where $S_{1s} = \boldsymbol{\gamma}'(s) + v\boldsymbol{t}'(s)$, $S_{1v} = \boldsymbol{t}(s)$ are the partial derivatives of $S_1(s,v)$ with respect to s and v, respectively. Hence we get that

$$S_{1s} \times S_{1v} = -v\varkappa(s)\boldsymbol{b}(s) \text{ and } \|S_{1s} \times S_{1v}\| = |v|\varkappa(s).$$

Then the unit normal vector function $\mathfrak{N}_1(s,v) = \dfrac{S_{1s} \times S_{1v}}{\|S_{1s} \times S_{1v}\|}$ of $S_1(s,v)$ is

$$\mathfrak{N}_1(s,v) = -\varepsilon_1\boldsymbol{b}(s),\ \varepsilon_1 = sign(v). \tag{9}$$

From $S_{1ss} = \dfrac{\partial S_{1s}}{\partial s} = -\varkappa^2(s).v.\boldsymbol{t}(s) + (\varkappa(s) + v.\varkappa'(s))\boldsymbol{n}(s) + v.\tau(s)\varkappa(s).\boldsymbol{b}(s)$,

$S_{1sv} = \dfrac{\partial S_{1s}}{\partial v} = \boldsymbol{t}'(s) = \varkappa(s)\boldsymbol{n}(s)$ and $S_{1vv} = \dfrac{\partial S_{1v}}{\partial v} = \dfrac{\partial \boldsymbol{t}(s)}{\partial v} = \vec{o}$ the coefficients of the

Second Fundamental Form of $S_1(s,v)$ are

$$\begin{aligned} L_1 &= L_1(s,v) = \langle \mathfrak{N}_1(s,v), S_{1uu} \rangle = -|v|\varkappa(s).\tau(s), \\ M_1 &= M_1(s,v) = \langle \mathfrak{N}_1(s,v), S_{1uv} \rangle = -\varepsilon_1 \varkappa(s).\langle \boldsymbol{b}(s), \boldsymbol{n}(s) \rangle = 0, \\ N_1 &= N_1(s,v) = \langle \mathfrak{N}_1(s,v), S_{1vv} \rangle = 0. \end{aligned} \tag{10}$$

It is clear that for any parameter values (s,v), the Gaussian curvature $K_1(s,v)$ of the developable surface $S_1(s,v)$ is vanished and the Mean curvature $H_1(s,v)$ can be expressed by

$$H_1(s,v) = \frac{-|v|\varkappa(s).\tau(s)}{2v^2\varkappa^2(s)} = \frac{-\tau(s)}{2|v|\varkappa(s)}. \tag{11}$$

If $\kappa_1(s,v)$ and $\kappa_2(s,v)$ are the principal curvatures of the surface $S_1(s,v)$ then from $K_1(s,v) = \kappa_1(s,v).\kappa_2(s,v) = 0$ and $H_1(s,v) = \dfrac{\kappa_1(s,v) + \kappa_2(s,v)}{2}$ it follows that

$$\kappa_1(s,v) = 2H_1(s,v) = \frac{-\tau(s)}{|v|\varkappa(s)} \text{ and } \kappa_2(s,v) = 0. \tag{12}$$

Then from the equation (6) in **Definition 3** and the equations (9) and (12) it follows

$$\overline{S}_1(s,v) = S_1(s,v) + \frac{1}{\kappa_1}.\mathfrak{N}_1(s,v) = \boldsymbol{\gamma}(s) + v.\left(\boldsymbol{t}(s) + \frac{\varkappa(s)}{\tau(s)}\boldsymbol{b}(s)\right).$$

From the equalities

$$\det(\boldsymbol{\gamma}'(s), \boldsymbol{l}(s), \boldsymbol{l}'(s)) = \det\left(\boldsymbol{t}(s), \boldsymbol{t}(s) + \frac{\varkappa(s)}{\tau(s)}\boldsymbol{b}(s), \left(\boldsymbol{t}(s) + \frac{\varkappa(s)}{\tau(s)}\boldsymbol{b}(s)\right)'\right) =$$

$$\det\left(\boldsymbol{t}(s), \boldsymbol{t}(s) + \frac{\varkappa(s)}{\tau(s)}\boldsymbol{b}(s), \left(\frac{\varkappa(s)}{\tau(s)}\right)'\boldsymbol{b}(s)\right) = 0.$$

it follows that the surface $\overline{S}_1(s,v)$ is developable. Let us now compute the coefficients of the First Fundamental Form of $\overline{S}_1(s,v)$. We obtain that

$$\begin{aligned} \overline{E}_1 &= \overline{E}_1(s,v) = \overline{S}_{1s}^2 = \left\| \boldsymbol{t}(s) + v.\left(\frac{\varkappa(s)}{\tau(s)}\right)'\boldsymbol{b}(s) \right\|^2 = 1 + v^2\left(\frac{\varkappa(s)}{\tau(s)}\right)'^2, \\ \overline{F}_1 &= \overline{F}_1(s,v) = \langle \overline{S}_{1s}, \overline{S}_{1v} \rangle = \langle \boldsymbol{t}(s) + v.\left(\frac{\varkappa}{\tau}\right)'\boldsymbol{b}(s), \boldsymbol{t}(s) + \frac{\varkappa}{\tau}\boldsymbol{b}(s) \rangle = 1 + v.\frac{\varkappa}{\tau}\left(\frac{\varkappa}{\tau}\right)', \\ \overline{G}_1 &= \overline{G}_1(s,v) = \overline{S}_{1v}^2 = \left\| \boldsymbol{t}(s) + \frac{\varkappa(s)}{\tau(s)}\boldsymbol{b}(s) \right\|^2 = 1 + \left(\frac{\varkappa(s)}{\tau(s)}\right)^2, \end{aligned} \tag{13}$$

where $\overline{S}_{1s} = \boldsymbol{t}(s) + v.\left(\dfrac{\varkappa(s)}{\tau(s)}\right)'\boldsymbol{b}(s)$ and $\overline{S}_{1v} = \boldsymbol{t}(s) + \dfrac{\varkappa(s)}{\tau(s)}\boldsymbol{b}(s)$ are the partial derivatives of $\overline{S}_1(s,v)$ with respect to s and v, respectively. Consequently, we find that

$$\overline{S}_{1s} \times \overline{S}_{1v} = \left(-\frac{\varkappa(s)}{\tau(s)} + v.\left(\frac{\varkappa(s)}{\tau(s)}\right)'\right)\boldsymbol{n}(s) \text{ and } \|\overline{S}_{1s} \times \overline{S}_{1v}\| = \left|-\frac{\varkappa(s)}{\tau(s)} + v.\left(\frac{\varkappa(s)}{\tau(s)}\right)'\right|.$$

Then the unit normal vector function $\overline{\mathfrak{N}}_1(s,v) = \dfrac{\overline{S}_{1s} \times \overline{S}_{1v}}{\|\overline{S}_{1s} \times \overline{S}_{1v}\|}$ of $\overline{S}_1(s,v)$ is determined

by

$$\overline{\mathfrak{N}}_1(s,v)=\overline{\varepsilon}_1\boldsymbol{n}(s),\ \text{where}\ \overline{\varepsilon}_1=sign\left(-\frac{\varkappa(s)}{\tau(s)}+v.\left(\frac{\varkappa(s)}{\tau(s)}\right)'\right). \tag{14}$$

From

$$\overline{S}_{1ss}=\frac{\partial\overline{S}_{1s}}{\partial s}=-\tau(s)\left(-\frac{\varkappa(s)}{\tau(s)}+v.\left(\frac{\varkappa(s)}{\tau(s)}\right)'\right)\boldsymbol{n}(s)+v\left(\frac{\varkappa(s)}{\tau(s)}\right)''\boldsymbol{b}(s),$$

$$\overline{S}_{1sv}=\frac{\partial\overline{S}_{1s}}{\partial v}=\left(\frac{\varkappa(s)}{\tau(s)}\right)'\boldsymbol{b}(s)\ \text{and}\ \overline{S}_{1vv}=\frac{\partial\overline{S}_{1v}}{\partial v}=\frac{\partial}{\partial v}\left(\boldsymbol{t}(s)+\frac{\varkappa(s)}{\tau(s)}\boldsymbol{b}(s)\right)=\vec{o}$$

and the equation (14), the coefficients of the Second Fundamental Form of $\overline{S}_1(s,v)$ are given by

$$\begin{aligned}&\overline{L}_1=\overline{L}_1(s,v)=\langle\overline{\mathfrak{N}}_1(s,v),\overline{S}_{1uu}\rangle=-\tau\left|-\frac{\varkappa}{\tau}+v.\left(\frac{\varkappa}{\tau}\right)'\right|,\\&\overline{M}_1=\overline{M}_1(s,v)=\langle\overline{\mathfrak{N}}_1(s,v),\overline{S}_{1uv}\rangle=0,\ \overline{N}_1=\overline{N}_1(s,v)=\langle\overline{\mathfrak{N}}_1(s,v),\overline{S}_{1vv}\rangle=0.\end{aligned} \tag{15}$$

It is easy to see that the Mean curvature $\overline{H}_1(s,v)$ of the developable surface $\overline{S}_1(s,v)$ is

$$\overline{H}_1(s,v)=\frac{-\tau(s)\left(1+\left(\frac{\varkappa}{\tau}\right)^2\right)}{2\left|-\frac{\varkappa}{\tau}+v.\left(\frac{\varkappa}{\tau}\right)'\right|}. \tag{16}$$

Finally from equations (11) and (16) we reached to the equation (7). □

The next statement gives us relations between the coefficients of the First and the Second Fundamental Form of $\overline{S}_1(s,v)$ and $S_1(s,v)$.

Theorem 2. *Let* (1) *be a parametrization of a unit speed Frenet curve* $\gamma: I\longrightarrow\mathbb{E}^3$ *of class* C^3 *with a Frenet frame* $\boldsymbol{t}(s),\boldsymbol{n}(s),\boldsymbol{b}(s)$, *and let* $\varkappa(s)\neq0$ *and* $\tau(s)\neq0$ *be the Euclidean curvature and the Euclidean torsion of* γ, *respectively. Suppose that* $S_1(s,v)=\boldsymbol{\gamma}(s)+v.\boldsymbol{t}(s),\ v\in\mathbb{R}\setminus\{0\}$ *is the developable tangential surface associated with* γ *and* $\overline{S}_1(s,v)=\boldsymbol{\gamma}(s)+v.\left(\boldsymbol{t}(s)+\frac{\varkappa(s)}{\tau(s)}\boldsymbol{b}(s)\right)$ *is its focal surface. Then the coefficients of the First and the Second Fundamental Form of* $\overline{S}_1(s,v)$ *can be expressed by the coefficients of the First and the Second Fundamental Form of* $S_1(s,v)$ *as follows*

$$\overline{E}_1(s,v)=E_1(s,v)+v^2\left(\left(\frac{\varkappa(s)}{\tau(s)}\right)'^2-\varkappa^2(s)\right),$$

$$\overline{F}_1(s,v)=F_1(s,v)+v\left(\frac{\varkappa(s)}{\tau(s)}\right)\left(\frac{\varkappa(s)}{\tau(s)}\right)',\ \overline{G}_1(s,v)=G_1(s,v)+\left(\frac{\varkappa(s)}{\tau(s)}\right)^2,$$

$$\overline{L}_1(s,v)=\frac{L_1(s,v)}{|v|\varkappa(s)}\left|-\frac{\varkappa(s)}{\tau(s)}+v.\left(\frac{\varkappa(s)}{\tau(s)}\right)'\right|,\ \overline{M}_1(s,v)=0,\ \overline{N}_1(s,v)=0.$$

Proof. The proof follows immediately from equations (8), (10), (13) and (15). □

Corollary 1. *Let* (1) *be an arbitrary parametrization of a Frenet curve* $\gamma: J\longrightarrow\mathbb{E}^3$ *of class* C^3 *with a Frenet frame* $\boldsymbol{t}(u),\boldsymbol{n}(u),\boldsymbol{b}(u)$, *and let* $\varkappa(u)\neq0$ *and* $\tau(u)\neq0$ *be the Euclidean curvature and the Euclidean torsion of* γ, *respectively. If* $\overline{S}_1(u,v)$ *is the*

focal surface of the tangential surface $S_1(u,v)$ of γ then the Mean curvature $\overline{H}_1(u,v)$ of $\overline{S}_1(u,v)$ can be expressed by the Mean curvature $H_1(u,v)$ of $S_1(u,v)$ as follows

$$\overline{H}_1(u,v) = -\frac{\tau\dot{s}(1+4v^2H_1^2)}{4|v\dot{s}H_1 + v^2H_{1u}|}, \tag{17}$$

$$\overline{E}_1(u,v) = E_1(u,v) + v^2\left(\left(\frac{\varkappa(u)}{\tau(u)}\right)_u^2 - \dot{s}^2\varkappa^2(u)\right),$$

$$\overline{F}_1(u,v) = F_1(u,v) + v\frac{\varkappa(u)}{\tau(u)}\left(\frac{\varkappa(u)}{\tau(u)}\right)_u,\ \overline{G}_1(u,v) = G_1(u,v) + \left(\frac{\varkappa(u)}{\tau(u)}\right)^2, \tag{18}$$

$$\overline{L}_1(u,v) = \frac{L_1(u,v)}{|v|\varkappa}\left|-\frac{\varkappa(u)}{\tau(u)} + \frac{v}{\dot{s}}\left(\frac{\varkappa(u)}{\tau(u)}\right)_u\right|,\ \overline{M}_1(u,v) = \overline{N}_1(u,v) = 0.$$

where H_{1u} and $\left(\frac{\varkappa(u)}{\tau(u)}\right)_u$ are the derivatives of $H_1(u,v)$ and $\frac{\varkappa(u)}{\tau(u)}$ with respect u and $s = s(u)$ is the arc-length function of γ.

Proof. The proof follows immediately from Theorem 1 replacing the parameter s with the arc-length function $s = s(u)$ of γ. □

Following the above construction, we shall examine an additional tangential surface closely associated with the curve γ. Utilising a unit speed parametrization of the curve γ with an arc-length parameter u and applying the equality (4) for its focal curve C_γ, we differentiate with regard to u and find that $\frac{dC_\gamma(u)}{du} = (c_1\tau + c_2')\boldsymbol{b}(u)$. Thus, the surface $S_2(u,v) = C_\gamma(u) + v\delta\boldsymbol{b}(u)$, where $\delta = sign(c_1\tau + c_2')$, constitutes a tangential ruled surface, characterised by a base curve C_γ and a director curve represented by the unit binormal vector $\boldsymbol{b}$ of γ. The acquired surface is evidently developable, and its focal surface also maintains this property of developability according to Theorem 1.

Theorem 3. *Let (1) be a parametrization of a unit speed Frenet curve $\gamma : I \longrightarrow \mathbb{E}^3$ of class C^3 with a Frenet frame $\boldsymbol{t}(u), \boldsymbol{n}(u), \boldsymbol{b}(u)$, and let $\varkappa(u) \neq 0$ and $\tau(u) \neq 0$ be the Euclidean curvature and the Euclidean torsion of γ, respectively. Suppose that $S_2(u,v) = C_\gamma(u) + v\delta\boldsymbol{b}(u)$ is the developable surface associated with the Focal curve $\boldsymbol{C}_\gamma$ of the unit speed Frenet curve γ. Then the focal surface $\overline{S}_2(u,v)$ of $S_2(u,v)$ is also developable and is represented as*

$$\overline{S}_2(u,v) = \boldsymbol{C}_\gamma(u) + v\delta\widetilde{\boldsymbol{D}}(u),\ \text{where } \widetilde{\boldsymbol{D}}(u) = \frac{\tau(u)}{\varkappa(u)}\boldsymbol{t}(u) + \boldsymbol{b}(u),\ v \in \mathbb{R}\setminus\{0\}. \tag{19}$$

The Mean curvature $\overline{H}_2(u,v)$ of $\overline{S}_2(u,v)$ can be expressed in terms of the Mean curvature $H_2(u,v)$ of $S_2(u,v)$ by the next equation

$$\overline{H}_2(u,v) = -\frac{\varkappa\delta(1+4v^2H_2^2)}{4|v(c_1\tau + c_2')H_2 + \delta v^2H_{2u}|}, \tag{20}$$

where H_{2u} is the partial derivative of $H_2(u,v)$ with respect u.

Proof. Applying Theorem 1 for the curve C_γ we get that

$$\overline{S}_2(u,v) = C_\gamma(u) + v\left(\boldsymbol{T}(u) + \frac{\varkappa_{C_\gamma}(u)}{\tau_{C_\gamma}(u)}\boldsymbol{B}(u)\right).$$

Replacing with the expressions (5) we obtain (19). The surface $\overline{S}_2(u,v)$ is obviously developable. Next, the equation (20) follows immediately from the equation (17) in the Corollary 1 having in mind that the arc-length prime $\dot{s}_{C_\gamma}$ of C_γ is equal to $|c_1\tau + c_2'| = \delta(c_1\tau + c_2')$. □

The vector $\widetilde{\boldsymbol{D}}(u)$ is referred to as the modified Darboux vector field along the curve γ. The next statement gives us the relations between the coefficients of the First and the Second Fundamental Form of $\overline{S}_2(u,v)$ and $S_2(u,v)$.

Theorem 4. *Let (1) be a parametrization of a unit speed Frenet curve $\gamma : I \longrightarrow \mathbb{E}^3$ of class C^3 with Frenet frame $\boldsymbol{t}(u), \boldsymbol{n}(u), \boldsymbol{b}(u)$, and let $\varkappa(u) \neq 0$ and $\tau(u) \neq 0$ be the Euclidean curvature and the Euclidean torsion of γ, respectively. Suppose that $S_2(u,v) = C_\gamma(u) + v\delta\boldsymbol{b}(u)$ is the developable surface associated with γ and $\overline{S}_2(u,v)$ is its focal surface. Then the coefficients of the First and the Second Fundamental Form of $\overline{S}_2(u,v)$ can be expressed by the coefficients of the First and the Second Fundamental Form of $S_2(u,v)$ as follows*

$$\overline{E}_2(u,v) = E_2(u,v) + v^2\left(\left(\frac{\tau(u)}{\varkappa(u)}\right)'^2 - \tau^2(u)\right),$$

$$\overline{F}_2(u,v) = F_2(u,v) + v\left(\frac{\tau(u)}{\varkappa(u)}\right)\left(\frac{\tau(u)}{\varkappa(u)}\right)',\ \overline{G}_2(u,v) = G_2(u,v) + \left(\frac{\tau(u)}{\varkappa(u)}\right)^2,$$

$$\overline{L}_2(u,v) = L_2(u,v)\left|\frac{\delta(c_1\tau + c_2')\frac{\tau(u)}{\varkappa(u)} - v.\left(\frac{\tau(u)}{\varkappa(u)}\right)'}{v\tau}\right|,\ \overline{M}_2(u,v) = 0,\ \overline{N}_2(u,v) = 0.$$

Proof. Let us denote by $\widetilde{s}$ the arc-length parameter of the curve C_γ. Then $\dot{\widetilde{s}} = \delta(c_1\tau + c_2')$. Applying Theorem 1, the equalities (18) in Corollary 1 and (5) the proof is completed. □

4 Application

Let $\boldsymbol{\gamma}(u) = (a(u\sin(u) + \cos(u)), a(\sin(u) - u\cos(u)), bu)$, where a and b are nonzero constant, is a cylindrical curve with a constant speed parametrization. According to [9], the corresponding focal curve C_γ is defined as follows:

$$\boldsymbol{C}_\gamma(u) = \left(\frac{\left(a^2+b^2\right)(2\cos(u) - u\sin(u))}{a\left(u^2+2\right)}, \frac{\left(a^2+b^2\right)(2\sin(u) + u\cos(u))}{a\left(u^2+2\right)}, \frac{u^3\left(a^2+b^2\right)}{b\left(u^2+2\right)}\right).$$

The pictures below depict the curves γ and C_γ, the surfaces $S_1(u,v)$ and $S_2(u,v)$, together with their corresponding focal surfaces $\overline{S}_1(u,v)$ and $\overline{S}_2(u,v)$.

Conclusion

In this paper, we investigated the focal surfaces of developable ruled surfaces generated by a unit speed Frenet curve and by its associated focal curve. Constructing the tangential surfaces corresponding to these curves, we derived explicit parametrizations of their focal surfaces and examined the relations between their geometric invariants. Working with respect to the natural parameter of the base curve allowed us to obtain precise expressions for the coefficients of the first and second fundamental forms of both the original developable surfaces and their focal surfaces.



Figure 1: From left to right: The developable surface $S_1(u, v)$, its focal surface $\overline{S}_1(u, v)$ together with the curve γ for $a = 1, b = 2$ and both surfaces

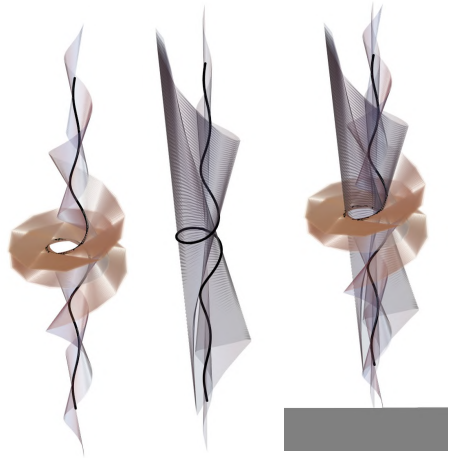


Figure 2: From left to right: The developable surface $S_2(u, v)$, its focal surface $\overline{S}_2(u, v)$ together with the curve C_γ for $a = 1, b = 2$ and both surfaces

The study establishes a geometric correspondence between a Frenet curve, its tangential surface, and the focal surface of that tangential surface, revealing a deeper structural connection within the family of developable surfaces. Furthermore, we obtained explicit formulas relating the mean curvatures of the original surfaces to those of their focal surfaces, showing how curvature information is transferred through the focal construction.

The theoretical results were illustrated through an example involving a cylindrical curve and its focal curve, together with visualizations of the associated developable and focal surfaces. This example highlights the practical applicability of the derived formulas and confirms the geometric behaviour predicted by the theory.

The results provide a basis for further research on the focal surfaces in applications such as geometric modelling, computer-aided design and construction, and analysis of new surfaces.

Acknowledgments

The authors express their gratitude to the reviewer for the perceptive remarks and useful suggestions.

References

[1] P. Alegre, K. Arslan, A. Carriazo, C. Murathan, G. Ozturk. Some special types of developable ruled surface, *Hacettepe Journal of Mathematics and Statistics*, **39** (3), (2010), 319 – 325.

[2] M. P. do Carmo. Differential geometry of curves and surfaces, (Revised and updated second ed.), Dover Publications, 2016.

[3] L. P. Eisenhart, A Treatise in Differential Geometry of Curves and Surfaces, New York, Ginn Camp., 1969.

[4] G. H. Georgiev, M. D. Pavlov. Focal surfaces of hyperbolic cylinders, *AIP Conf. Proc.*, **1910** (1), (2017), 050005. https://doi.org/10.1063/1.5013987.

[5] G. H. Georgiev, M. D. Pavlov. Curvature Dependent Offsets to Elliptic Cones, *Far East Journal of Mathematical Sciences*, **102** (11), (2017), 2757–2783. https://doi.org/10.17654/MS102112757

[6] G. H. Georgiev. Generalized offset surfaces to a torus, *AIP Conference Proceedings*, **2048** (1), (2018), 0500071–0500078.

[7] G. H. Georgiev, M. D. Pavlov. Focal and generalized focal surfaces of parabolic cylinders, *ARPN Journal of Engineering and Applied Sciences*, **13** (15), (2018), 4458-4465.

[8] G. H. Georgiev, M. D. Pavlov. Generalized offset surfaces to a pseudosphere, *AIP Conf. Proc.*, **2172** (1), (2019), 060002. https://doi.org/10.1063/1.5133530

[9] G. H. Georgiev, R. P. Encheva, C. L. Dinkova. Geometry of cylindrical curves over plane curves. *Applied Mathematical Sciences*, **113** (9) (2015), 5637–5649. http://dx.doi.org/10.12988/ams.2015.56456

[10] A. Gray, E. Abbena, S. Salamon. Modern Differential Geometry of Curves and Surfaces. New York, Chapman and Hall/CRC, 2006.

[11] F. Güler. The focal surfaces of offset surface. *Optik-International Journal for Light and Electron Optics*, **271**, (2022), 170053. https://doi.org/10.1016/j.ijleo.2022.170053.

[12] S. Izumiya, N. Takeuchi. Special curves and ruled surfaces. *Cotributions to Algebra and Geometry*, **44** (2003), 203–212.

[13] H. Pottmann, J. Wallner. Computational Line Geometry. Mathematics and Visualization. Springer Berlin, Heidelberg. 2010 doi:10.1007/978-3-642-04018-4.

[14] M.D. Shepherd. Line congruences as surfaces in the space of lines, *Differential Geometry and its Applications*, (1999), 1–26.

[15] Dirk J. Struik. Lectures on Classical Differential Geometry. 2nd ed., Dover Publications, 1961.

[16] R. Uribe-Vargas. On vertices, focal curvatures and differential geometry of space curves. *Bull. of the Brazilian Math. Soc.* **36** (2005), 285–307.

МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2026
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2026
Proceedings of the Fifty-Fifth Spring Conference
of the Union of Bulgarian Mathematicians
Tryavna, Bulgaria, April 5–9, 2026

A DIOPHANTINE INEQUALITY WITH MIXED POWERS OF FOUR PRIMES OF A SPECIFIC TYPE

Tatiana L. Todorova
Faculty of Mathematics and Informatics, Sofia University "St. Kliment Ohridski", Sofia, Bulgaria
e-mail: tlt@fmi.uni-sofia.bg

In this paper we study a Diophantine inequality with one prime and three prime squares. We prove that it has infinitely many solutions in primes p_i such that each $p_i + 2$ ($i = 1, \dots, 4$) is an almost-prime of prescribed order.

Keywords: Diophantine inequality, Davenport-Heilbronn method, Rosser's weights, vector sieve, almost primes.

ДИОФАНТОВО НЕРАВЕНСТВО СЪС СМЕСЕНИ СТЕПЕНИ НА ЧЕТИРИ ПРОСТИ ЧИСЛА ОТ СПЕЦИАЛЕН ТИП

Татяна Л. Тодорова
Факултет по математика и информатика,
Софийски университет „Св. Климент Охридски", София, България
e-mail: tlt@fmi.uni-sofia.bg

В статията разглеждаме диофантово неравенство с едно просто и квадратите на три прости числа. Доказваме, че то има безбройно много решения в прости числа p_i, такива че всяко от числата $p_i + 2$, $i = 1, ..., 4$, е почти просто от някакъв ред.

Ключови думи: Диофантово неравенство, метод на Девънпорт-Хейлброн, тегла на Розер, векторно решето, почти прости числа.

1 Introduction

In 1967 Baker [1] demonstrate that for real numbers $\eta, \lambda_i \in \mathbb{R},\ \lambda_i \neq 0,\ i = 1, 2, 3$ which are not all of the same sign, $\lambda_1/\lambda_2 \in \mathbb{R} \setminus \mathbb{Q}$ there are infinitely many ordered triples of primes p_1, p_2, p_3 such that

$$|\lambda_1 p_1 + \lambda_2 p_2 + \lambda_3 p_3 + \eta| < \mathcal{E} \tag{1}$$

https://doi.org/10.55630/mem.2026.55.060-077
2020 Mathematics Subject Classification: 11D75, 11N36, 11P32.

with $\mathcal{E} = (\log max\, p_j)^{-A}$, $A > 0$. Baker's result was refined several times, and the best-known result belongs to Matomäki [12] with $\mathcal{E} = (\max p_j)^{-2/9+\theta}$ as here $\theta > 0$. Baker and Harman [2] proved that under the generalized Riemann hypothesis, it is possible to reach $\mathcal{E} = (\max p_j)^{-1/4+\theta}$.

Let

$$\lambda_i \in \mathbb{R},\ \lambda_i \neq 0,\ i = 1, 2, 3, 4, \tag{2}$$

$$\lambda_1, \lambda_2, \lambda_3, \lambda_4 \quad \text{not all of the same sign}, \tag{3}$$

$$\lambda_1/\lambda_2 \in \mathbb{R} \setminus \mathbb{Q}, \tag{4}$$

$$\eta \in \mathbb{R}\,. \tag{5}$$

Under conditions (2)-(5) Languasco and Zaccagnini [11] considered the diophantine inequality

$$|\lambda_1 p_1 + \lambda_2 p_2^2 + \lambda_3 p_3^2 + \lambda_4 p_4^2 + \eta| < \mathcal{E}$$

and proved that it has infinitely many solutions in primes with $\mathcal{E} = (\max p_j)^{-1/18+\theta}$. Wang and Yao [19] improved their result with $\mathcal{E} = (\max p_j)^{-1/14+\theta}$. Under the conditions $\lambda_1/\lambda_2 \in \mathbb{R}\setminus\mathbb{Q}$, and if both λ_1/λ_2 and λ_1/λ_3 are algebraic, they proved that the exponent can be replaced by $-\dfrac{3}{40} + \theta$. The known best result, due to Ge, Zhao, and Wang [9] is $\mathcal{E} = (\max p_j)^{-5/64+\theta}$. Later, Gambini [8] generalised this problem and proved the existence of infinitely many primes $p_1, ..., p_4$ such that

$$|\lambda_1 p_1 + \lambda_2 p_2^2 + \lambda_3 p_3^2 + \lambda_4 p_4^k + \eta| < \mathcal{E}$$

with $\mathcal{E} = (\max p_1, p_2^2, p_3^2, p_4^2)^{-\psi(k)+\theta}$, $\psi(k) = \min\{\frac{1}{14}, \frac{14-5k}{28k}\}$ and $1 < k < 14/5$.

Diophantine inequalities in which the prime variables p_i satisfy additional restrictions – for example, that $p_i + 2$ is an almost-prime of given order – form another important category. The well-known hypothesis states that there are infinitely many prime numbers p such that $p + 2$ is also prime. In 1973, Chen [5] demonstrated that there are infinitely many primes p for which $p + 2 = P_2$. Here, P_r represents an integer that has no more than r prime factors, counted with their multiplicities.

In 2015, Dimitrov and Todorova [7] merged the problems studied by Baker and Chen. For $\mathcal{E} = (\log \max p_j)^{-B}$, they showed that inequality (1) admits solutions under the conditions $p_1+2 = P_8$, $p_2+2 = P_8'$, and $p_3+2 = P_8''$. Subsequently, Dimitrov [6] improved the exponent to $\mathcal{E} = (\max p_j)^{-1/12+\theta}$, while requiring $p_1 + 2 = P_{28}$, $p_2 + 2 = P_{28}'$, and $p_3 + 2 = P_{28}''$. Later, the author [15] established the existence of infinitely many triples of primes satisfying (1) with $\mathcal{E} = (\max p_j)^{-1/18+\theta}$ and conditions $p_1 + 2 = P_7$, $p_2 + 2 = P_7'$, $p_3 + 2 = P_7''$.

In 2025, Todorova and Georgieva [17] proved that there are infinitely many prime triples for which

$$|\lambda_1 p_1 + \lambda_2 p_2 + \lambda_3 p_3^2 + \eta| < (\max p_j)^{-1/12+\theta}$$

and

$$p_1 + 2 = P_{20}'\,, \quad p_2 + 2 = P_{20}''\,, \quad p_3 + 2 = P_{42}'''\,.$$

This paper is concerned with a Diophantine inequality in mixed powers of primes, requiring that each $p_i + 2$, $i = 1, 2, 3, 4$, is almost a prime. Specifically, we prove the theorem below.

Theorem 1. If conditions (2), (3), (4), (5) are satisfied and $\theta > 0$, then there exist

infinitely many ordered quadruples of primes p_1, p_2, p_3, p_4 with

$$|\lambda_1 p_1 + \lambda_2 p_2^2 + \lambda_3 p_3^2 + \lambda_4 p_4^2 + \eta| < (\max p_j)^{-\frac{1}{200}+\theta} \tag{6}$$

and

$$p_1 + 2 = P_{20}', \quad p_2 + 2 = P_{41}'', \quad p_3 + 2 = P_{41}''', \quad p_4 + 2 = P_{41}^{\mathrm{iv}}. \tag{7}$$

2 Notations

Throughout, the symbols p, p_1, p_2, p_3, p_4 denote prime numbers. We write $\varphi(n)$ for Euler's totient function and $\mu(n)$ for the Möbius function. The greatest common divisor and the least common multiple of m_1 and m_2 are denoted by (m_1, m_2) and $[m_1, m_2]$, respectively. Congruence modulo k is abbreviated as $m \equiv n\,(k)$ instead of $m \equiv n \pmod{k}$. The integer part of a real number y is written $[y]$, and we set $e(y) = e^{2\pi i y}$.

The notation $k \sim K$ means $K/2 < k \leq K$. The letter ε stands for an arbitrarily small positive constant, not necessarily the same at each occurrence. This convention allows us, for example, to write $x^{\varepsilon} \log x \ll x^{\varepsilon}$.

3 Auxiliary Results

Our argument makes use of a vector sieve and relies on the theorem stated below.

Lemma 1. Suppose that $\mathcal{D} \in \mathbb{R}, \mathcal{D} > 4$. There exists an arithmetical functions $\lambda^{\pm}(d)$ (called Rosser's functions of level $\mathcal{D}$) with the following properties:

1. For any positive integer d, we have
$$|\lambda^{\pm}(d)| \leq 1, \qquad \lambda^{\pm}(d) = 0 \quad \text{if} \quad d > \mathcal{D} \quad \text{or} \quad \mu(d) = 0.$$

2. If $n \in \mathbb{N}$ then
$$\sum_{d|n} \lambda^{-}(d) \leq \sum_{d|n} \mu(d) \leq \sum_{d|n} \lambda^{+}(d).$$

3. If $\mathbf{z} \in \mathbb{R}$ is such that $\mathbf{z}^2 \leq \mathcal{D}$ and if
$$\mathcal{B}^{\pm}(\mathcal{D}, \mathbf{z}) = \sum_{d|P(\mathbf{z})} \frac{\lambda^{\pm}(d)}{\varphi(d)}, \quad s = \frac{\log \mathcal{D}}{\log \mathbf{z}}, \tag{8}$$
then we have
$$\mathcal{B}(\mathbf{z}) \leq \mathcal{B}^{+}(\mathcal{D}, \mathbf{z}) \leq \mathcal{B}(\mathbf{z}) \left(F(s) + O\left((\log \mathcal{D})^{-\frac{1}{3}} \right) \right), \tag{9}$$
$$\mathcal{B}(\mathbf{z}) \geq \mathcal{B}^{-}(\mathcal{D}, \mathbf{z}) \geq \mathcal{B}(\mathbf{z}) \left(f(s) + O\left((\log \mathcal{D})^{-\frac{1}{3}} \right) \right), \tag{10}$$

where $F(s)$ and $f(s)$ satisfy

$$
\begin{aligned}
&F(s) = \frac{2e^{\gamma}}{s} && \text{if} \quad 0 < s \le 3;\\
&F(s) = \frac{2e^{\gamma}}{s}\left(1 + \int_{2}^{s-1} \frac{\log(t-1)}{t}\,dt\right) && \text{if} \quad 3 \le s \le 5;\\
&f(s) = \frac{2e^{\gamma}\log(s-1)}{s}, && \text{if} \quad 2 \le s \le 4;\\
&(sF(s))' = f(s-1) && \text{if} \quad s > 3;\\
&(sf(s))' = F(s-1) && \text{if} \quad s > 2.
\end{aligned} \tag{11}
$$

Here, γ is Euler's constant $\gamma \approx 0.577$.

Proof: See Greaves [10, Chapter 4] and [4]. □

Mertens' theorem yields

$$\mathcal{B}(\mathbf{z}) = \frac{2C_2 e^{-\gamma}}{\log \mathbf{z}}\Big(1 + O\Big(\frac{1}{\log \mathbf{z}}\Big)\Big), \tag{12}$$

with

$$C_2 = \prod_{p \ge 3}\Big(1 - \frac{1}{(p-1)^2}\Big) \approx 0.66016\ldots$$

being the twin prime constant. From the basic estimates of the linear sieve, namely (9) and (10), it follows that

$$0 \le \mathcal{B}^{-}(\mathcal{D}, \mathbf{z}) \le \mathcal{B}(\mathbf{z}) \le \mathcal{B}^{+}(\mathcal{D}, \mathbf{z}). \tag{13}$$

The proof of our theorem requires bounds for two kinds of exponential sums taken over primes; these bounds are supplied by the next two lemmas.

Lemma 2. Suppose $\alpha \in \mathbb{R}$ and α satisfy conditions

$$\left|\alpha - \frac{a}{q}\right| < \frac{1}{q^2}\,, \quad a \in \mathbb{Z}\,, \quad q \in \mathbb{N}\,, \quad (a,q) = 1\,, \quad q \ge 1\,. \tag{14}$$

Let $\xi(d)$ be complex numbers defined for $d \le D$ and $\xi(d) \ll 1$. If

$$W(X) = \sum_{d \sim D} \xi(d) \sum_{\substack{p \sim X \\ p+2 \equiv 0\,(d)}} e(\alpha p)\log p \tag{15}$$

then for any arbitrary small $\varepsilon > 0$ we have

$$W(X) \ll X^{\varepsilon}\left(\frac{X}{q^{1/2}} + X^{1/2}q^{1/2} + X^{2/3}D + X^{5/6}\right).$$

Proof: The proof is contained in the proof of Lemma 1 from [18]. □

Lemma 3. Suppose $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ satisfies condition (14), $D \in \mathbb{R}$, $D \le x^{1/6}$, $\lambda(d)$ are complex numbers defined for $d \le D$ and $\lambda(d) \ll \tau(d)$. Then for any arbitrary small $\varepsilon > 0$ and $b \in \mathbb{Z}$ for the sum

$$W = \sum_{d \le D} \lambda(d) \sum_{\substack{n \sim x \\ n \equiv b\,(d)}} e\big(\alpha n^2\big)\Lambda(n) \tag{16}$$

we have

$$W \ll x^{\varepsilon}\Big(\frac{xD^{1/2}}{q^{1/4}} + x^{1/2}D^{1/2}q^{1/4} + x^{7/8}D^{3/4} + x^{1/3}D^{1/2}q^{1/2} + \frac{x^{7/6}D^{1/2}}{q^{1/2}}\Big). \tag{17}$$

Proof: The proof follows the argument of Theorem 1 in [16]. Using Vaughan's identity, we decompose the sum W into $O(\log x)$ type I sums

$$W_1 = \sum_{\substack{d\sim D\\(b,\,d)=1}} \lambda(d) \sum_{m\sim M} a(m) \sum_{\substack{\ell\sim L\\ m\ell\equiv b\,(d)}} e(\alpha(m\ell)^2)$$

or

$$W_1' = \sum_{\substack{d\sim D\\(b,\,d)=1}} \lambda(d) \sum_{m\sim M} a(m) \sum_{\substack{\ell\sim L\\ m\ell\equiv b\,(d)}} \log(\ell) e(\alpha(m\ell)^2)$$

with $M \le x^{1/3}$ and $O(\log x)$ type II sums

$$W_2 = \sum_{\substack{d\sim D\\(b,\,d)=1}} \lambda(d) \sum_{\substack{\ell\sim L\\ m\ell\equiv b\,(d)}} b(\ell) \sum_{m\sim M} a(m) e(\alpha(m\ell)^2)$$

with $M \in [x^{1/3},\, x^{2/3}]$ and

$$ML \sim x, \quad a(m) \ll \tau(m)\log m, \quad b(\ell) \ll \tau(\ell)\log \ell\,. \tag{18}$$

To evaluate the sum W_2 we will consider only the case $x^{1/2} \le M \le x^{2/3}$. The evaluation in the case $x^{1/2} \le L \le x^{2/3}$ is the same. Following the same steps as in the evaluation of W_2 for $D < x^{1/6}$ from the proof of Theorem 1 in [16], we successively obtain

$$W_2^2 \le x^{\varepsilon}\Big(xMD + V_2\Big),$$

where

$$V_2^2 \ll x^{\varepsilon}\Big(x^3LD + x^2D^2 \sum_{z\le xLD} \min\Big\{\frac{x^2}{z},\, \frac{1}{||\alpha z||}\Big\}\Big).$$

So, from Lemma 2.2 from [20], ch. 2,§2.1 we obtain

$$W_2 \ll x^{\varepsilon}\Big(\frac{xD^{1/2}}{q^{1/4}} + x^{1/2}D^{1/2}q^{1/4} + x^{7/8}D^{3/4}\Big). \tag{19}$$

Again, proceeding as in the evaluation of W_1 for $D < x^{1/6}$ from Theorem 1 [16], we successively obtain

$$W_1^2 \ll x^{\varepsilon}\Big(xMD + MD \sum_{z\ll xMD} \min\Big\{\frac{x^2}{z},\, \frac{1}{||\alpha z||}\Big\}\Big)$$

and from Lemma 2.2 from [20], ch. 2,§2.1 we receive

$$W_1 \ll x^{\varepsilon}\Big(x^{1/3}D^{1/2}q^{1/2} + x^{5/6}D + \frac{x^{7/6}D^{1/2}}{q^{1/2}}\Big). \tag{20}$$

Therefore, equations (19) and (20) yield

$$W \ll x^{\varepsilon}\Big(\frac{xD^{1/2}}{q^{1/4}} + x^{1/2}D^{1/2}q^{1/4} + x^{7/8}D^{3/4} + x^{1/3}D^{1/2}q^{1/2} + \frac{x^{7/6}D^{1/2}}{q^{1/2}}\Big).$$

□

Remmark 1. By applying the properties of the von Mangoldt Λ function and Lemma

3 in the range $D \le x^{1/12}$, we find that

$$\sum_{d\le\mathcal{D}}\lambda(d)\sum_{\substack{p^2\sim x\\ p\equiv b\,(d)}} e\big(\alpha p^2\big) \ll x^{\varepsilon}\bigg(\frac{x^{1/2}D^{1/2}}{q^{1/4}} + x^{1/4}D^{1/2}q^{1/4} + x^{7/16}D^{3/4} + x^{1/6}D^{1/2}q^{1/2} + \frac{x^{7/12}D^{1/2}}{q^{1/2}}\bigg).$$

The next lemma gives the necessary estimate.

Lemma 4. Let D, $\widetilde{D}$, Δ, $L(\beta)$ and $\widetilde{L}(\beta)$, $I(\beta)$ and $\widetilde{I}(\beta)$ be defined by (26), (25), (43), (44), (29), (30). If $|\beta| < \Delta$, restriction (24) are fulfilled, then for large enough X and an arbitrarily large fixed positive real number A, the following equalities

$$L(\beta) - I(\beta)\sum_{d\le D}\frac{\lambda(d)}{\varphi(d)} = O\bigg(\frac{X}{(\log X)^{A/2-3}}\bigg) + O\Big(X^{4/5+\xi/2}(\log X)^{14}\Big),$$

$$\widetilde{L}(\beta) - \widetilde{I}(\beta)\sum_{d\le \widetilde{D}}\frac{\lambda(d)}{\varphi(d)} = O\bigg(\frac{X^{1/2}}{(\log X)^{A/2-3}}\bigg) + O\Big(X^{2/5+\xi/2}(\log X)^{14}\Big)$$

are fulfilled.

Proof: This is Lemma 13 from [17]. □

The following lemmas provide estimates for the integrals $I(\beta)$ and $\widetilde{I}(\beta)$ and for the integrals derived from them.

Lemma 5. For integrals $I(\beta)$ and $\widetilde{I}(\beta)$, defined by (29) and (30), we have

$$I(\beta) \ll \frac{1}{|\beta|},$$

$$\widetilde{I}(\beta) \ll \frac{1}{|\beta|\sqrt{X}}. \tag{21}$$

Proof: The statement is followed by partial integration. □

Remmark 2. We notice that the trivial estimate

$$\widetilde{I}(\beta) \ll X^{1/2} \tag{22}$$

is valid.

Lemma 6. Let Δ be defined by (25). Then for integrals $I(\beta)$ and $\widetilde{I}(\beta)$, defined by (29) and (30), we have

$$\int\limits_{-\Delta}^{\Delta}|I(\beta)|^2 d\beta \ll X \quad \text{and} \quad \int\limits_{-\Delta}^{\Delta}|\widetilde{I}(\beta)|^2 d\beta \ll 1.$$

Proof: This is Lemma 15 from [17]. □

We shall also require the estimates provided by the following Lemma.

Lemma 7. Let Δ, D, $\widetilde{D}$ be defined by (25), (26) and condition (24) are fulfilled. Then for sums $L(\beta)$ and $\widetilde{L}(\beta)$ (see (43) and (44)), we have

$$\int\limits_{-\Delta}^{\Delta} |L(\beta)|^2 d\beta \ll X \log^5 X \quad \text{and} \quad \int\limits_{-\Delta}^{\Delta} |\widetilde{L}(\beta)|^2 d\beta \ll \sqrt{X} \log^5 X\,.$$

Proof: This is Lemma 16 from [17] □

Remmark 3. We notice that the trivial estimate

$$|\widetilde{L}(\beta)| \ll X^{1/2} \log X \tag{23}$$

is valid.

4 Beginning of the proof

Let $0 < \lambda_0 < 1$, $\xi, \delta, \alpha, \widetilde{\delta}, \widetilde{\alpha}$, be positive real numbers that we will specify later, but for now only assume the conditions

$$\begin{aligned} &\xi + 3\delta < \frac{12}{25}, \quad \xi + \delta < \frac{3}{8}, \quad \xi + 3\widetilde{\delta} < \frac{6}{25}, \quad \xi + \widetilde{\delta} < \frac{3}{16}, \\ &0 < \alpha < \delta/2, \quad 0 < \widetilde{\alpha} < \widetilde{\delta}/2. \end{aligned} \tag{24}$$

We define

$$\Delta = X^{\xi - 1}, \tag{25}$$

$$D = X^{\delta}, \quad \widetilde{D} = X^{\widetilde{\delta}}, \tag{26}$$

$$\mathcal{E} = X^{-\frac{1}{200} + \theta}, \ \theta > 0 \text{ is arbitrary small}, \quad H = \frac{1000 \log^2 X}{\mathcal{E}}, \tag{27}$$

$$z = X^{\alpha}, \quad \widetilde{z} = X^{\widetilde{\alpha}}, \tag{28}$$

$$I(\beta) = \int\limits_{\lambda_0 X}^{X} e(\beta y) dy, \tag{29}$$

$$\widetilde{I}(\beta) = \int\limits_{\lambda_0^{\frac{1}{2}} X^{\frac{1}{2}}}^{X^{\frac{1}{2}}} e(\beta y^2) dy, \tag{30}$$

$$P(z) = \prod_{2 < p < \mathbf{z}} p, \quad \mathcal{B}(\mathbf{z}) = \prod_{2 < p < \mathbf{z}} \left(1 - \frac{1}{p-1}\right). \tag{31}$$

Consider the sum

$$\Gamma(X) = \sum_{\substack{\lambda_0 X < p_1, p_2, p_3, p_4 \le X \\ (p_1 + 2, P(z)) = 1, \\ (p_i + 2, P(\widetilde{z})) = 1, i = 2,3,4 \\ |\lambda_1 p_1 + \lambda_2 p_2^2 + \lambda_3 p_3^2 + \lambda_4 p_4^2 + \eta| < \mathcal{E}}} \log p_1 \log p_2 \log p_3 \log p_4\,,$$

with $\mathcal{E}$ given by (27). If we prove the inequality $\Gamma(X) > 0$ then the inequality (6) would have a solution in primes p_1, p_2, p_3, p_4 satisfying $(p_1 + 2, P(z)) = 1$, $(p_i + 2, P(\widetilde{z})) = 1, i = 2, 3, 4$. If the number $p_i + 2$ has ℓ_i prime factors counted with multiplicity, then from

(28) we find that $\ell_1 < \dfrac{1}{\alpha}$ and $\ell_i < \dfrac{1}{\widetilde{\alpha}}$ for $i = 2, 3, 4$. This means that $p_1 + 2$ would be an almost prime of order $[1/\alpha]$ and $p_i + 2$, $i = 2, 3, 4$ would be an almost prime of order $[1/\widetilde{\alpha}]$.

To transform the sum $\Gamma(X)$ we take a function υ such that

$$\begin{array}{lll} \upsilon(x) = 1 & \text{for} & |x| \le 3\mathcal{E}/4 \\ 0 < \upsilon(x) < 1 & \text{for} & 3\mathcal{E}/4 < |x| < \mathcal{E} \\ \upsilon(x) = 0 & \text{for} & |x| \ge \mathcal{E}\,. \end{array} \tag{32}$$

The function υ has derivatives of sufficiently large order, and its Fourier transform

$$\Upsilon(x) = \int\limits_{-\infty}^{\infty} \upsilon(t) e(-xt) dt \tag{33}$$

satisfy

$$|\Upsilon(x)| \le \min\left(\frac{7\mathcal{E}}{4}, \frac{1}{\pi|x|}, \frac{1}{\pi|x|}\left(\frac{k}{2\pi|x|\mathcal{E}/8}\right)^k\right) \tag{34}$$

for all $k \in \mathbb{N}$. For the existence of such a function, see [13].

Using the function $\upsilon(x)$ we get

$$\Gamma(X) \ge \Gamma_0(X) = \sum_{\substack{\lambda_0 X < p_1, p_2, p_3, p_4 \le X \\ (p_1+2, P(z))=1, \\ (p_i+2, P(\widetilde{z}))=1, i=2,3,4}} \upsilon(\lambda_1 p_1 + \lambda_2 p_2^2 + \lambda_3 p_3^2 + \lambda_4 p_4^2 + \eta) \times \log p_1 \log p_2 \log p_3 \log p_4\,. \tag{35}$$

Our goal is to demonstrate that for specific values of α and $\widetilde{\alpha}$ (as large as possible), there exists a sequence $X_1, X_2, \ldots \to \infty$ such that $\Gamma_0(X_j) > 0$. Then the number of prime solutions p_i of (6) in the interval $(\lambda_0 X_j, X_j]$ with $p_1 + 2 = P_{[1/\alpha]}$ and $p_i + 2 = P_{[1/\widetilde{\alpha}]}$ for $i = 2, 3, 4$ is positive. This approach allows us to generate an infinite sequence of quadruples of primes p_1, p_2, p_3, p_4 that satisfy the desired properties.

Let $\Lambda_1 = \sum\limits_{d|(p_1+2, P(z))} \mu(d)$ and $\Lambda_i = \sum\limits_{d|(p_i+2, P(\widetilde{z}))} \mu(d)$, $i = 2, 3, 4$ be the characteristic functions of primes p_i, such that $(p_1 + 2,\ P(z)) = 1$ and $(p_i + 2,\ P(\widetilde{z})) = 1$ for $i = 2, 3, 4$, respectively. Then from (35) it follows that

$$\Gamma_0(X) = \sum_{\substack{\lambda_0 X < p_i \le X \\ i=1,2,3,4}} \upsilon(\lambda_1 p_1 + \lambda_2 p_2^2 + \lambda_3 p_3^2 + \lambda_4 p_4^2 + \eta) \times \Lambda_1\Lambda_2\Lambda_3\Lambda_4 \log p_1 \log p_2 \log p_3 \log p_4\,. \tag{36}$$

Let $\lambda^{\pm}(d)$ and $\widetilde{\lambda}^{\pm}(d)$ represent the lower and upper bounds of Rosser's weights at levels D and $\widetilde{D}$, respectively (see Lemma 1). If

$$\Lambda_1^{\pm} = \sum_{d|(p_1+2, P(z))} \lambda^{\pm}(d) \quad \text{and} \quad \Lambda_i^{\pm} = \sum_{d|(p_i+2, P(\widetilde{z}))} \widetilde{\lambda}^{\pm}(d)\,, i = 2, 3, 4 \tag{37}$$

then, from Lemma 1 we have $\Lambda_i^- \le \Lambda_i \le \Lambda_i^+$, $i = 1,\ 2,\ 3,\ 4$.

We will utilize the following simple inequality

$$\Lambda_1\Lambda_2\Lambda_3\Lambda_4 \geq \Lambda_1^-\Lambda_2^+\Lambda_3^+\Lambda_4^+ + \Lambda_1^+\Lambda_2^-\Lambda_3^+\Lambda_4^+ + \Lambda_1^+\Lambda_2^+\Lambda_3^-\Lambda_4^+ + \Lambda_1^+\Lambda_2^+\Lambda_3^+\Lambda_4^- - 3\Lambda_1^+\Lambda_2^+\Lambda_3^+\Lambda_4^+ \tag{38}$$

see [[3], Lemma 13]. Using (36) and (38) we get

$$\begin{aligned}\Gamma_0(X) \geq \Gamma(X) = \sum_{\lambda_0 X<p_1,p_2,p_3,p_4\leq X} & \upsilon(\lambda_1 p_1+\lambda_2 p_2^2+\lambda_3 p_3^2+\lambda_4 p_4^2+\eta)\\ & \times\big(\Lambda_1^-\Lambda_2^+\Lambda_3^+\Lambda_4^+ + \Lambda_1^+\Lambda_2^-\Lambda_3^+\Lambda_4^+ + \Lambda_1^+\Lambda_2^+\Lambda_3^-\Lambda_4^+\\ & + \Lambda_1^+\Lambda_2^+\Lambda_3^+\Lambda_4^- - 3\Lambda_1^+\Lambda_2^+\Lambda_3^+\Lambda_4^+\big)\log p_1\log p_2\log p_3\log p_4\,.\end{aligned} \tag{39}$$

We substitute the function $\upsilon(\lambda_1 p_1+\lambda_2 p_2^2+\lambda_3 p_3^2+\lambda_4 p_4^2+\eta)$ in (39) with its inverse Fourier transform (33) and get

$$\begin{aligned}\Gamma(X) = \int_{-\infty}^{\infty}\Upsilon(t) \sum_{\substack{\lambda_0 X<p_i\leq X\\ i=1,2,3,4}} & e\big((\lambda_1 p_1+\lambda_2 p_2^2+\lambda_3 p_3^2+\lambda_4 p_4^2+\eta)t\big)\\ & \times\log p_1\log p_2\log p_3\log p_4\big(\Lambda_1^-\Lambda_2^+\Lambda_3^+\Lambda_4^+ + \Lambda_1^+\Lambda_2^-\Lambda_3^+\Lambda_4^+\\ & + \Lambda_1^+\Lambda_2^+\Lambda_3^-\Lambda_4^+ + \Lambda_1^+\Lambda_2^+\Lambda_3^+\Lambda_4^- - 3\Lambda_1^+\Lambda_2^+\Lambda_3^+\big)\,dt\,.\end{aligned} \tag{40}$$

Thus,

$$\Gamma(X) = \Gamma_1(X)+\Gamma_2(X)+\Gamma_3(X)+\Gamma_4(X)-3\Gamma_5(X) \tag{41}$$

where $\Gamma_1(X)$, $\Gamma_2(X)$, $\Gamma_3(X)$, $\Gamma_4(X)$, and $\Gamma_5(X)$ are the contributions of the consecutive terms on the right side of (40). It is clear that

$$\begin{aligned}\Gamma_1(X) = \int_{-\infty}^{\infty}\Upsilon(t) \sum_{\lambda_0 X<p_1,p_2,p_3,p_4\leq X} & e\big((\lambda_1 p_1+\lambda_2 p_2^2+\lambda_3 p_3^2+\lambda_4 p_4^2+\eta)t\big)\\ & \times\Lambda_1^-\Lambda_2^+\Lambda_3^+\Lambda_4^+\log p_1\log p_2\log p_3\log p_4\,dt\,,\end{aligned}$$

$$\begin{aligned}\Gamma_2(X)=\Gamma_3(X)=\Gamma_4(X)\\ = \int_{-\infty}^{\infty}\Upsilon(t) \sum_{\lambda_0 X<p_1,p_2,p_3,p_4\leq X} & e\big((\lambda_1 p_1+\lambda_2 p_2^2+\lambda_3 p_3^2+\lambda_4 p_4^2+\eta)t\big)\\ & \times\Lambda_1^+\Lambda_2^-\Lambda_3^+\Lambda_4^+\log p_1\log p_2\log p_3\log p_4\,dt\,,\end{aligned}$$

$$\begin{aligned}\Gamma_5(X) = \int_{-\infty}^{\infty}\Upsilon(t) \sum_{\lambda_0 X<p_1,p_2,p_3,p_4\leq X} & e\big((\lambda_1 p_1+\lambda_2 p_2^2+\lambda_3 p_3^2+\lambda_4 p_4^2+\eta)t\big)\\ & \times\Lambda_1^+\Lambda_2^+\Lambda_3^+\Lambda_4^+\log p_1\log p_2\log p_3\log p_4\,dt\,.\end{aligned}$$

Therefore,

$$\Gamma(X) \geq \Gamma_1(X)+3\Gamma_2(X)-3\Gamma_5(X)\,. \tag{42}$$

We proceed to estimate $\Gamma_1(X)$. The integrals $\Gamma_i(X)$, $i=2,...,5$ can be handled analogously. Changing the order of summation and taking into account (37), we obtain

$$\Gamma_1(X) = \int_{-\infty}^{\infty}\Upsilon(t)e(\eta t)L^-(\lambda_1 t)\widetilde{L}^+(\lambda_2 t)\widetilde{L}^+(\lambda_3 t)\widetilde{L}^+(\lambda_4 t)dt\,,$$

where

$$L^{\pm}(t) = \sum_{d|P(z)} \lambda^{\pm}(d) \sum_{\substack{\lambda_0 X < p \le X \\ p+2 \equiv 0 \,(d)}} e(pt)\log p \tag{43}$$

and

$$\widetilde{L}^{\pm}(t) = \sum_{d|P(\tilde{z})} \widetilde{\lambda}^{\pm}(d) \sum_{\substack{\lambda_0 X < p^2 \le X \\ p+2 \equiv 0 \,(d)}} e(p^2 t)\log p\,. \tag{44}$$

We denote that $\lambda^{\pm}(d), \widetilde{\lambda}^{\pm}(d)$ are real numbers such that $|\lambda^{\pm}(d)| \le 1$ and $|\widetilde{\lambda}^{\pm}(d)| \le 1$. Furthermore, $\lambda^{\pm}(d) = 0$ and $\widetilde{\lambda}^{\pm}(d) = 0$ if $2|d$ or $\mu(d) = 0$. Following the Davenport–Heilbronn version of the circle method (see [[20], Ch. 11]), we split the integral $\Gamma_1(X)$ into three distinct parts:

$$\Gamma_1(X) = \Gamma_1^{(1)}(X) + \Gamma_1^{(2)}(X) + \Gamma_1^{(3)}(X)\,, \tag{45}$$

where

$$\Gamma_1^{(1)}(X) = \int\limits_{|t|\le\Delta} \Upsilon(t) e(\eta t) L^{-}(\lambda_1 t)\widetilde{L}^{+}(\lambda_2 t)\widetilde{L}^{+}(\lambda_3 t)\widetilde{L}^{+}(\lambda_4 t)dt, \tag{46}$$

$$\Gamma_1^{(2)}(X) = \int\limits_{\Delta<|t|<H} \Upsilon(t) e(\eta t) L^{-}(\lambda_1 t)\widetilde{L}^{+}(\lambda_2 t)\widetilde{L}^{+}(\lambda_3 t)\widetilde{L}^{+}(\lambda_4 t)dt, \tag{47}$$

$$\Gamma_1^{(3)}(X) = \int\limits_{|t|\ge H} \Upsilon(t) e(\eta t) L^{-}(\lambda_1 t)\widetilde{L}^{+}(\lambda_2 t)\widetilde{L}^{+}(\lambda_3 t)\widetilde{L}^{+}(\lambda_4 t)dt\,. \tag{48}$$

The quantities $\Delta = \Delta(X)$ and $H = H(X)$ are defined in equations (25) and (27), respectively. Lemma 2 of [7] provides the following result:

$$\Gamma_1^{(3)}(X) \ll 1. \tag{49}$$

The estimate of $\Gamma_i^{(3)}(X), i = 2, 3, 4$ is the same. It is easy to see from equation (42) that

$$\begin{aligned} \Gamma \ge \big|\Gamma_1^{(1)}(X) + 3\Gamma_3^{(1)}(X) - 3\Gamma_5^{(1)}(X)\big| \\ + O\big(|\Gamma_1^{(2)}(X)|\big) + O\big(|\Gamma_2^{(2)}(X)|\big) + O\big(|\Gamma_5^{(2)}(X)|\big) + O\big(1\big)\,. \end{aligned} \tag{50}$$

We will estimate $\Gamma_1^{(1)}(X)$ and $\Gamma_1^{(2)}(X)$ in Sections 5 and 6, respectively. The estimation of the sums $\Gamma_i^{(1)}(X)$, $\Gamma_i^{(2)}(X)$, $i = 2, 3, 4$ is carried out in the same way. In Section 7, we will finalize the proof of the theorem.

5 Asymptotic formula for $\Gamma_1^{(1)}(X)$

From now on, we will put

$$\mathcal{B}^{\pm} = \mathcal{B}^{\pm}(D,\, z), \quad \widetilde{\mathcal{B}}^{\pm} = \mathcal{B}^{\pm}(\widetilde{D},\, \widetilde{z}). \tag{51}$$

To find asymptotic formulae for $\Gamma_1^{(1)}(X)$ we need the following

Lemma 8. Let Δ, D, $\widetilde{D}$, z, $\tilde{z}$, $I(\beta)$, $\widetilde{I}(\beta)$, $L(\beta)$ and $\widetilde{L}(\beta)$ be defined by (25), (26), (28),

(29), (30), (43), (44) and

$$R = \int\limits_{-\Delta}^{\Delta} \Upsilon(t) e(\eta t) \Big(\mathcal{B}^{\pm} \big(\widetilde{\mathcal{B}}^{\pm}\big)^3 I(\lambda_1 t) \widetilde{I}(\lambda_2 t) \widetilde{I}(\lambda_3 t) \widetilde{I}(\lambda_4 t) \\ - L^{\pm}(\lambda_1 t) \widetilde{L}^{\pm}(\lambda_2 t) \widetilde{L}^{\pm}(\lambda_3 t) \widetilde{L}^{\pm}(\lambda_4 t) \Big) dt \,.$$

Then

$$R \ll \mathcal{E} \bigg(\frac{X^{3/2}}{(\log X)^{A/2-8}} + X^{7/5+\xi/2} (\log X)^{19} \bigg) .$$

Proof: Using estimate (34) we found that

$$R \ll \mathcal{E} \big(J_1 + J_2 + J_3 + J_4 \big) , \tag{52}$$

where

$$J_1 = \int\limits_0^{\Delta} \Big| \mathcal{B}^{\pm} I(\lambda_1 t) - L^{\pm}(\lambda_1 t) \Big| \Big| \widetilde{\mathcal{B}}^{\pm} \widetilde{I}(\lambda_2 t) \Big| \Big| \widetilde{\mathcal{B}}^{\pm} \widetilde{I}(\lambda_3 t) \Big| \Big| \widetilde{\mathcal{B}}^{\pm} \widetilde{I}(\lambda_4 t) \Big| dt,$$

$$J_2 = \int\limits_0^{\Delta} \big| L^{\pm}(\lambda_1 t) \big| \Big| \widetilde{\mathcal{B}}^{\pm} \widetilde{I}(\lambda_2 t) - \widetilde{L}^{\pm}(\lambda_2 t) \Big| \Big| \widetilde{\mathcal{B}}^{\pm} \widetilde{I}(\lambda_3 t) \Big| \Big| \widetilde{\mathcal{B}}^{\pm} \widetilde{I}(\lambda_4 t) \Big| dt,$$

$$J_3 = \int\limits_0^{\Delta} \big| L^{\pm}(\lambda_1 t) \big| \big| \widetilde{L}^{\pm}(\lambda_2 t) \big| \Big| \widetilde{\mathcal{B}}^{\pm} \widetilde{I}(\lambda_3 t) - \widetilde{L}^{\pm}(\lambda_3 t) \Big| \Big| \widetilde{\mathcal{B}}^{\pm} \widetilde{I}(\lambda_4 t) \Big| dt,$$

$$J_4 = \int\limits_0^{\Delta} \big| L^{\pm}(\lambda_1 t) \big| \big| \widetilde{L}^{\pm}(\lambda_2 t) \big| \big| \widetilde{L}^{\pm}(\lambda_3 t) \big| \Big| \widetilde{\mathcal{B}}^{\pm} \widetilde{I}(\lambda_4 t) - \widetilde{L}^{\pm}(\lambda_4 t) \Big| dt.$$

From Lemma 4, (24), (13) and (12) follows

$$J_1 \ll \bigg(\frac{X}{(\log X)^{A/2}} + X^{4/5+\xi/2} (\log X)^{11} \bigg) J_{11}, \tag{53}$$

where

$$J_{11} = \int\limits_0^{\Delta} \big| \widetilde{I}(\lambda_2 t) \big| \big| \widetilde{I}(\lambda_3 t) \big| \big| \widetilde{I}(\lambda_4 t) \big| dt \,.$$

Using the Cauchy-Schwarz inequality and Lemma 6, we get

$$J_{11} \ll \bigg(\int\limits_0^{\Delta} \big| \widetilde{I}(\lambda_2 t) \big|^2 dt \bigg)^{1/2} \bigg(\int\limits_0^{\Delta} \big| \widetilde{I}(\lambda_3 t) \big|^2 \big| \widetilde{I}(\lambda_4 t) \big|^2 dt \bigg)^{1/2} \\ \ll \bigg(\int\limits_0^{\Delta} \big| \widetilde{I}(\lambda_3 t) \big|^2 \big| \widetilde{I}(\lambda_4 t) \big|^2 dt \bigg)^{1/2} .$$

Repeated application of the Cauchy–Schwarz inequality together with the trivial bound

(22) yields

$$J_{11} \ll \Big(\int_0^{\Delta} \big|\widetilde{I}(\lambda_3 t)\big|^4 dt\Big)^{1/4} \Big(\int_0^{\Delta} \big|\widetilde{I}(\lambda_4 t)\big|^4 dt\Big)^{1/4} \tag{54}$$

$$\ll X^{1/2}\Big(\int_0^{\Delta} \big|\widetilde{I}(\lambda_3 t)\big|^2 dt\Big)^{1/4} \Big(\int_0^{\Delta} \big|\widetilde{I}(\lambda_4 t)\big|^2 dt\Big)^{1/4}.$$

From Lemma 6 we have $J_{11} \ll X^{1/2}$, and (53) implies

$$J_1 \ll \frac{X^{3/2}}{(\log X)^{A/2}} + X^{13/10+\xi/2}(\log X)^{11}. \tag{55}$$

To estimate J_2 we will use Lemma 4 and (12):

$$J_2 \ll \Big(\frac{X^{1/2}}{(\log X)^{A/2-1}} + X^{2/5+\xi/2}(\log X)^{12}\Big) J_{21}, \tag{56}$$

where

$$J_{21} = \int_0^{\Delta} \big|L^{\pm}(\lambda_1 t)\big|\big|\widetilde{I}(\lambda_3 t)\big|\big|\widetilde{I}(\lambda_4 t)\big| dt.$$

Applying twice the Cauchy-Schwarz inequality and Lemma 7 we obtain

$$J_{21} = \Big(\int_0^{\Delta} \big|L^{\pm}(\lambda_1 t)\big|^2 dt\Big)^{1/2} \Big(\int_0^{\Delta} \big|\widetilde{I}(\lambda_3 t)\big|^2 \big|\widetilde{I}(\lambda_4 t)\big|^2 dt\Big)^{1/2}$$

$$\ll X^{1/2}\big(\log X\big)^{5/2}\Big(\int_0^{\Delta} \big|\widetilde{I}(\lambda_3 t)\big|^4 dt\Big)^{1/4} \Big(\int_0^{\Delta} \big|\widetilde{I}(\lambda_4 t)\big|^4 dt\Big)^{1/4}.$$

We estimate the last two integrals above using an argument analogous to the one for (54). So, from (56) we get

$$J_2 \ll \frac{X^{3/2}}{(\log X)^{A/2-7/2}} + X^{7/5+\xi/2}(\log X)^{29/2}. \tag{57}$$

By the same reasoning, we obtain

$$J_3 \ll \Big(\frac{X^{1/2}}{(\log X)^{A/2-2}} + X^{2/5+\xi/2}(\log X)^{13}\Big) J_{31}, \tag{58}$$

where

$$J_{31} = \int_0^{\Delta} \big|L^{\pm}(\lambda_1 t)\big|\big|\widetilde{L}^{\pm}(\lambda_2 t)\big|\big|\widetilde{I}(\lambda_4 t)\big| dt.$$

Using trivial estimate (23) and the Cauchy-Schwarz inequality we obtain

$$J_{31} = X^{1/2}\log X\Big(\int_0^{\Delta} \big|L^{\pm}(\lambda_1 t)\big|^2 dt\Big)^{1/2} \Big(\int_0^{\Delta} \big|\widetilde{I}(\lambda_4 t)\big|^2 dt\Big)^{1/2}.$$

Applying Lemma 7 and Lemma 6 yields

$$J_{31} \ll X(\log X)^{7/2}.$$

Combined with (58) we receive

$$J_3 \ll \frac{X^{3/2}}{(\log X)^{A/2-11/2}} + X^{7/5+\xi/2}(\log X)^{33/2}. \tag{59}$$

An analogous treatment of J_4 gives

$$J_4 \ll \left(\frac{X^{1/2}}{(\log X)^{A/2-3}} + X^{2/5+\xi/2}(\log X)^{14}\right) J_{41}, \tag{60}$$

where

$$J_{41} = \int_0^{\Delta} \left|L^{\pm}(\lambda_1 t)\right| \left|\widetilde{L}^{\pm}(\lambda_2 t)\right| \left|\widetilde{L}^{\pm}(\lambda_3 t)\right| dt.$$

Applying the Cauchy–Schwarz inequality twice and using Lemma 7, we obtain

$$\begin{aligned} J_{41} &\ll \left(\int_0^{\Delta} \left|L^{\pm}(\lambda_1 t)\right|^2 dt\right)^{1/2} \left(\int_0^{\Delta} \left|\widetilde{L}^{\pm}(\lambda_2 t)\right|^4 dt\right)^{1/4} \left(\int_0^{\Delta} \left|\widetilde{L}^{\pm}(\lambda_3 t)\right|^4 dt\right)^{1/4} \\ &\ll X^{1/2}(\log X)^{5/2} \left(\int_0^{\Delta} \left|\widetilde{L}^{\pm}(\lambda_2 t)\right|^4 dt\right)^{1/4} \left(\int_0^{\Delta} \left|\widetilde{L}^{\pm}(\lambda_3 t)\right|^4 dt\right)^{1/4}. \end{aligned} \tag{61}$$

Let $i = 2$ or $i = 3$. From $\Delta \ll 1$ (see (25)) and λ_i-fixed follows that

$$\begin{aligned} \int_0^{\Delta} \left|\widetilde{L}^{+}(\lambda_i t)\right|^4 dt &= \frac{1}{\lambda_i} \int_0^{\lambda_i \Delta} \left|\widetilde{L}^{+}(t)\right|^4 dt \ll \int_0^{1} \left|\widetilde{L}^{+}(t)\right|^4 dt \\ &\ll \sum_{\substack{d_i \mid P(z) \\ i=1,2,3,4}} \sum_{\substack{(\lambda_0 X)^{\frac{1}{2}} < p_j \le X^{\frac{1}{2}} \\ p_j + 2 \equiv 0 \,(d_j) \\ j=1,2,3,4}} \log p_1 \log p_2 \log p_3 \log p_4 \int_0^{1} e((p_1^2 + p_2^2 - p_3^2 - p_4^2)t) dt \end{aligned}$$

Arguing as in §6 [17] we obtain that

$$\int_0^{\Delta} \left|\widetilde{L}^{+}(\lambda_i t)\right|^4 dt \ll X \log^5 X.$$

Therefore, from (61) and above inequality we get

$$J_{41} \ll X \log^5 X,$$

so from (60) we receive

$$J_4 \ll \frac{X^{3/2}}{(\log X)^{A/2-8}} + X^{7/5+\xi/2}(\log X)^{19}. \tag{62}$$

From (55), (57), (59) and (62) follows the statement of the lemma. □

From Lemma 8 and from (46) we get

$$\Gamma_1^{(1)}(X) = \mathcal{B}^-\big(\widetilde{\mathcal{B}}^+\big)^3 \int\limits_{|t|\le\Delta} \Upsilon(t)e(\eta t)I(\lambda_1 t)\widetilde{I}(\lambda_2 t)\widetilde{I}(\lambda_3 t)\widetilde{I}(\lambda_4 t)dt + O\Big(\frac{\mathcal{E}X^{3/2}}{(\log X)^{A/2-8}}\Big) + O\Big(\mathcal{E}X^{7/5+\xi/2}(\log X)^{19}\Big). \tag{63}$$

Let

$$\mathcal{J}(X) = \int\limits_{-\infty}^{\infty} \Upsilon(t)e(\eta t)I(\lambda_1 t)\widetilde{I}(\lambda_2 t)\widetilde{I}(\lambda_3 t)\widetilde{I}(\lambda_4 t)dt\,,$$

$$\mathcal{J}_1(X) = \int\limits_{\Delta}^{\infty} \Upsilon(t)e(\eta t)I(\lambda_1 t)\widetilde{I}(\lambda_2 t)\widetilde{I}(\lambda_3 t)\widetilde{I}(\lambda_4 t)dt\,,$$

$$\mathcal{J}_2(X) = \int\limits_{-\infty}^{-\Delta} \Upsilon(t)e(\eta t)I(\lambda_1 t)\widetilde{I}(\lambda_2 t)\widetilde{I}(\lambda_3 t)\widetilde{I}(\lambda_4 t)dt\,.$$

We evaluate $\mathcal{J}_1(X)$; the integral $\mathcal{J}_2(X)$ is estimated in the same way. Using Lemma 5, (34) and (25) we get

$$\mathcal{J}_1(X) \ll \frac{\mathcal{E}}{X^{3/2}} \int\limits_{\Delta}^{\infty} \frac{dt}{|\lambda_1\lambda_2\lambda_3\lambda_4|t^4} \ll \frac{\mathcal{E}}{\Delta^3 X^{3/2}} = \mathcal{E}X^{3/2-3\xi}\,. \tag{64}$$

Using restriction (24) we choose

$$\xi = \frac{1}{100}\,, \quad \delta = \frac{47}{300} - \varepsilon \quad \text{and} \quad \widetilde{\delta} = \frac{23}{300} - \varepsilon\,, \tag{65}$$

where ε is an arbitrarily small positive number. From (63), (64), (13), (12) we get

$$\Gamma_1^{(1)}(X) = \mathcal{J}(X)\mathcal{B}^-\big(\widetilde{\mathcal{B}}^+\big)^3 + O\Big(\frac{\mathcal{E}X^{3/2}}{(\log X)^{A/2-8}}\Big)\,. \tag{66}$$

Applying the method of Lemma 4 in [7] with the parameter restriction

$$\lambda_0 < \min\Big(\frac{\lambda_1}{4|\lambda_4|},\ \frac{\lambda_2}{4|\lambda_4|},\ \frac{\lambda_3}{4|\lambda_4|},\ \frac{1}{16}\Big),$$

we derive the lower bound

$$\mathcal{J} \gg \mathcal{E}X^{3/2}.$$

The constant implicit in the Vinogradov symbol $\gg$ depends solely on λ_1, λ_2, λ_3 and λ_4.

6 Asymptotic formula for $\Gamma_1^{(2)}(X)$

Relation (50) shows that obtaining a nontrivial lower bound for Γ requires proving that the integrals $\Gamma_i^{(2)}$, $i = 1, ..., 5$ are sufficiently small. To achieve this, we exploit the irrationality of the ratio λ_1/λ_2. This property will enable us to give a nontrivial estimate for at least one of the sums $L^{\pm}(\lambda_1 t)$ or $\widetilde{L}^{\pm}(\lambda_2 t)$.

Let

$$V(t,\, X) = \min\Big\{\big|L^{\pm}(\lambda_1 t)\big|^{1/2}, \Big|\widetilde{L}^{\pm}(\lambda_2 t)\Big|\Big\}\,. \tag{67}$$

Given our choice of parameters in (65) and by Lemma 2, if $\lambda_1 t$ is irrational, we obtain

$$|L^{\pm}(\lambda_1 t)|^{1/2} \ll X^{\varepsilon}\left(\frac{X^{1/2}}{q^{1/4}} + X^{1/4}q^{1/4} + X^{5/12}\right).$$

One readily verifies that for

$$q \in \left[X^{19/75},\, X^{87/150}\right], \tag{68}$$

the bound

$$|L^{\pm}(\lambda_1 t)|^{1/2} \ll X^{99/200+\varepsilon}$$

holds. From the choice made in (65) and by Remark 1, if $\lambda_2 t$ is irrational, we obtain the estimate

$$|\widetilde{L}^{\pm}(\lambda_2 t)| \ll X^{\varepsilon}\left(\frac{X^{323/600}}{q^{1/4}} + X^{173/600}q^{1/4} + X^{99/200} + X^{123/600}q^{1/2} + \frac{X^{373/600}}{q^{1/2}}\right).$$

Hence, for any q, satisfying condition (68),

$$|\widetilde{L}^{\pm}(\lambda_2 t)| \ll X^{99/200+\varepsilon}.$$

The following statement holds.

Lemma 9. Let $t,\, X,\, \lambda_1,\, \lambda_2 \in \mathbb{R}$,

$$|t| \in (\Delta,\, H)\,, \tag{69}$$

where Δ and H are denoted by (25) and (27), $\lambda_1,\, \lambda_2$ satisfies (4) and $V(t,\, X)$ is defined by (67). Then there exists a sequence of real numbers $X_1,\, X_2, \ldots \to \infty$ such that

$$V(t\,, X_j) \ll X_j^{\frac{99}{200}+\varepsilon}\,, \quad j = 1, 2, \ldots\,. \tag{70}$$

Proof: The proof is identical to that of Lemma 8 in [15]. Since $\lambda_1/\lambda_2 \in \mathbb{R} \setminus \mathbb{Q}$, Corollary 1B of [14] guarantees that there are infinitely many coprime pairs (a, q) with q arbitrarily large, satisfying

$$\left|\frac{\lambda_1}{\lambda_2} - \frac{a}{q}\right| < \frac{1}{q^2}. \tag{71}$$

For sufficiently large q we choose X such that

$$q = X^{1/3}. \tag{72}$$

The argument of Lemma 8 in [15] produces an infinite sequence $q^{(1)}, q^{(2)}, \ldots$ satisfying (71). In view of (72), this generates an infinite sequence $X_1, X_2, \ldots$ such that, for each X_j, either $\lambda_1 t$ or $\lambda_2 t$ admits a rational approximation with a denominator in the interval (68). Therefore, (70) is satisfied and the proof is complete. □

To estimate the integral $\Gamma_1^{(2)}$ we will use (67) to notice that

$$|L^{-}(\lambda_1 t)||\widetilde{L}^{+}(\lambda_2 t)| \le V(t\,, X_j)\left(|L^{-}(\lambda_1 t)|^{\frac{1}{2}}|\widetilde{L}^{+}(\lambda_2 t)| + |L^{-}(\lambda_1 t)|\right).$$

Next, from (34), above inequalities and estimate (70) for integral $\Gamma_1^{(2)}(X_j)$, denoted by (47) we find

$$\begin{aligned}\Gamma_1^{(2)}(X_j) &\ll \mathcal{E}V(t\,, X_j)\Big(\mathcal{I}_1(X_j) + \mathcal{I}_2(X_j)\Big) \\ &\ll \mathcal{E}X_j^{99/200+\varepsilon}\Big(\mathcal{I}_1(X_j) + \mathcal{I}_2(X_j)\Big)\,,\end{aligned} \tag{73}$$

where

$$\mathcal{I}_1(X_j) = \int\limits_{\Delta}^{H} |L^-(\lambda_1 t)|^{\frac{1}{2}} |\widetilde{L}^+(\lambda_2 t)||\widetilde{L}^+(\lambda_3 t)||\widetilde{L}^+(\lambda_4 t)|dt,$$

$$\mathcal{I}_2(X_j) = \int\limits_{\Delta}^{H} |L^-(\lambda_1 t)||\widetilde{L}^+(\lambda_3 t)||\widetilde{L}^+(\lambda_4 t)|dt\,.$$

Using twice the Cauchy-Schwarz inequality, we get

$$\mathcal{I}_1(X_j) \ll \Big(\int\limits_{\Delta}^{H} \big|L^-(\lambda_1 t)\big|^2 dt\Big)^{\frac{1}{4}} \Big(\int\limits_{\Delta}^{H} \Big|\widetilde{L}^+(\lambda_2 t)\Big|^4 dt\Big)^{\frac{1}{4}} \times \Big(\int\limits_{\Delta}^{H} \Big|\widetilde{L}^+(\lambda_3 t)\Big|^4 dt\Big)^{\frac{1}{4}} \Big(\int\limits_{\Delta}^{H} \Big|\widetilde{L}^+(\lambda_4 t)\Big|^4 dt\Big)^{\frac{1}{4}}. \tag{74}$$

Arguing as in §6 [7] and §6 [17] we obtain that

$$\begin{aligned} &\int\limits_{\Delta}^{H} \big|L^{\pm}(\lambda_j t)\big|^2 dt \ll H X_j \log^5 X_j, \\ &\int\limits_{\Delta}^{H} \Big|\widetilde{L}^{\pm}(\lambda_i t)\Big|^4 dt \ll H X_j \log^5 X_j. \end{aligned} \tag{75}$$

So

$$\mathcal{I}_1(X_j) \ll H X_j \log^5 X_j. \tag{76}$$

To estimate $\mathcal{I}_2(X_j)$ we use twice the Cauchy-Schwarz inequality and get

$$\mathcal{I}_2(X_j) \ll \Big(\int\limits_{\Delta}^{H} \big|L^-(\lambda_1 t)\big|^2 dt\Big)^{\frac{1}{2}} \Big(\int\limits_{\Delta}^{H} \Big|\widetilde{L}^+(\lambda_3 t)\Big|^4 dt\Big)^{\frac{1}{4}} \Big(\int\limits_{\Delta}^{H} \Big|\widetilde{L}^+(\lambda_4 t)\Big|^4 dt\Big)^{\frac{1}{4}}.$$

Using estimates (75) we get

$$\mathcal{I}_2(X_j) \ll H X_j \log^5 X_j. \tag{77}$$

From (73), (76), (77) and (27) with $\theta > 2\varepsilon$ follows

$$\Gamma_1^{(2)}(X_j) \ll \mathcal{E} H X_j^{\frac{3}{2}-\frac{1}{200}+\varepsilon} \log^5 X_j \ll \mathcal{E} X_j^{\frac{1}{200}-\theta} X_j^{\frac{3}{2}-\frac{1}{200}+\varepsilon} \log^7 X_j \ll \mathcal{E} X_j^{3/2-\varepsilon/2}\,. \tag{78}$$

7 End of the proof

From (45), (49), (66) and (78) we obtain

$$\Gamma_1(X_j) = \mathcal{J}(X_j)\mathcal{B}^-\big(\widetilde{\mathcal{B}}^+\big)^3 + O\Big(\frac{\mathcal{E} X_j^{3/2}}{(\log X_j)^{A/2-8}}\Big)\,. \tag{79}$$

Similarly, we can determine $\Gamma_2(X_j)$ and $\Gamma_5(X_j)$. From (42) and (79) we get

$$\Gamma(X_j) \geq \mathcal{J}(X_j)\bigg(\mathcal{B}^-\big(\widetilde{\mathcal{B}}^+\big)^3 + 3\mathcal{B}^+\big(\widetilde{\mathcal{B}}^+\big)^2\widetilde{\mathcal{B}}^- - 3\mathcal{B}^+\big(\widetilde{\mathcal{B}}^+\big)^3\bigg).$$

Using (9), (10), (12), (13) and (51)we obtain

$$\Gamma(X_j) \geq \mathcal{J}(X_j)\mathcal{B}(z)\mathcal{B}(\widetilde{z})^3\bigg(f(s) + 3f(\tilde{s}) - 3F(s)F(\tilde{s})^3\bigg),$$

where f and F are functions of the linear sieve as described in Lemma 1. Setting $s = \tilde{s} = 3,14999$ and employing relations (11) yields

$$\Gamma(X_j) \geq 0,000178\mathcal{J}(X_j)\mathcal{B}(z)\mathcal{B}(\widetilde{z})^3.$$

From (65) with $\varepsilon = 0,00001$ and from

$$s = \frac{\log D}{\log z}, \quad \tilde{s} = \frac{\log \widetilde{D}}{\log \widetilde{z}}$$

we receive $\frac{1}{\alpha} = 20,1063...$ and $\frac{1}{\widetilde{\alpha}} = 41,0868....$ Therefore,

$$p_1 + 2 = P'_{20}, \quad p_2 + 2 = P''_{41}, \quad p_3 + 2 = P'''_{41}, \quad p_4 + 2 = P^{\text{iv}}_{41}$$

and the proof of Theorem 1 is complete.

Acknowledgements: The author was partially supported by the Scientific Fund of Sofia University "St. Kliment Ohridski" under Grant 80-10-35/23.05.2025.

References

[1] Baker, A. On some Diophantine inequalities involving primes. *J. Reine Angew.Math.*, *228*, 1967, 166–181.

[2] Baker, R. Harman, G. Diophantine approximation by prime numbers. *J. Lond. Math. Soc.*, *25:2*, 1982, 201–215.

[3] Brüdern, J.; Fouvry, E. Lagrange's Four Squares Theorem with almost prime variables. *J. Reine Angew. Math.*, *454*, 1994, 59–96.

[4] Cai Y. On Chen's theorem (II). *Journal of Number Theory*, *128:5*, 2008, 1336–1357.

[5] Chen J. R. On the representation of a large even integer as the sum of a prime and the product of at most two primes. *Sci. Sinica*, *16*, 1973, 157–176.

[6] Dimitrov, St. Diophantine approximation by special primes. *AIP Conf. Proc.*, *2048*, 2018.

[7] Dimitrov, St.; Todorova, T. L. Diophantine approximation by prime numbers of a special form. *Annuaire Univ. Sofia, Fac. Math. Inform.*, *102*, 2015, 71–90.

[8] Gambini, A. Diophantine approximation with one prime two squares of primes and one k th power of a prime. *Open Mathematics*, *19.1*, 2021, 373-387.

[9] Ge, Wenxu, Feng Zhao, and Tianqin Wang. On Diophantine approximation with one prime and three squares of primes. *Frontiers of Mathematics in China*, *14.4*, 2019, 761-779.

[10] Greaves, G. Sieves in number theory. *Springer-Verlag* New York, 2001.

[11] Languasco, A. , Zaccagnini A. A Diophantine problem with a prime and three squares of primes. *Journal of Number Theory*, *132.12*, 2012, 3016-3028.

[12] Matomäki, K. Diophantine approximation by primes. *Glasgow Math. J.*, *52*, 2010, 87–106.

[13] Segal, B. I. On a theorem analogous to Waring's theorem. *Dokl. Akad. Nauk SSSR (N. S.)*, *2*, 1933, 47–49.
[14] Shmidt W. M. Diophantine Approximation, *Mir*, Moscow, 1983.
[15] Todorova, T. L. Diophantine approximation by prime numbers of a special form. *Serdica Mathematical Journal*, *47:3*, 2021, 255–272.
[16] Todorova, T.L. On the distribution of $\alpha p^2 + \beta$ modulo one for primes p such that $p + 2$ has no more two prime divisors. *Mathematics and Education in Mathematics*, *53*, 2024, 39—56.
[17] Todorova, T.L.; Georgieva, A. A Diophantine Inequality Involving Mixed Powers of Primes with a Specific Type. *Mathematics*, *13(19)*, 2025, 3065.
[18] Todorova, T. L.; Tolev, D. I. On the distribution of αp modulo one for primes p of a special form. *Math. Slovaca*, *60*, 2010, 771–786.
[19] Wang, Y., Yao, W. Diophantine approximation with one prime and three squares of primes *Journal of Number Theory*, *180*, 2017, 234–250.
[20] Vaughan, R. C. The Hardy–Littlewood method. *Cambridge Univ. Press*, 2nd ed.; 1997.

МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2026
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2026
Proceedings of the Fifty-Fifth Spring Conference
of the Union of Bulgarian Mathematicians
Tryavna, Bulgaria, April 5–9, 2026

THE EDGE-ISOPERIMETRIC INEQUALITY FOR POWERS OF CYCLES

Kristiyan Vasilev
Institute of Mathematics and Informatics, Bulgarian Academy of Sciences, Sofia, Bulgaria
e-mail: kr.vasilev@math.bas.bg

This note provides a complete solution to a certain version of the edge-isoperimetric problem for powers of cycle graphs. Namely, it shows that the maximum number of edges induced by a vertex subset of C_n^s of size k is achieved by a set of k consecutive vertices.

Keywords: edge-isoperimetric inequality, cycle graph

ИЗОПЕРИМЕТРИЧНОТО НЕРАВЕНСТВО ЗА РЕБРАТА НА СТЕПЕНИТЕ НА ЦИКЛИЧЕН ГРАФ

Кристиян Василев
Институт по математика и информатика, Българска академия на науките, София, България
e-mail: kr.vasilev@math.bas.bg

В тази статия се дава пълно решение на определена версия на реброво-изопериметричната задача за степени на циклични графи. По-точно се доказва, че максималният брой ребра в индуциран подграф на C_n^s, породен от множество от k върха, се постига, когато това множество се състои от k последователни върха.

Ключови думи: реброво-изопериметрично неравенство, цикличен граф

1 Introduction

Let $G = (V, E)$ be a simple undirected graph. We consider the graph edge-isoperimetric problem in the following form: given a graph G and $k \in \mathbb{N}$, what is the largest number

https://doi.org/10.55630/mem.2026.55.078-084

2020 Mathematics Subject Classification: 05C35, 05C42.

* The research was performed under the Project i-METODE, No BG05SFPR001-3.004-0012, funded under the procedure "Support for the development of project-based doctoral study" from the Programme "Education 2021–2027", co-financed by the European Union.

of edges in an induced subgraph of G with k vertices, that is

$$\max_{|U|=k, U\subset V} e(U).$$

For a d-regular graph, a minimizer of this quantity has the smallest graph perimeter (number of edges between a vertex subset and its complement) among k-sets. Recently, this question (in an equivalent supersaturation setting) for Johnson graphs was studied by A. M. Raigorosdkii and his students [3] (see also references therein). Various results on this and related quantities can be found in [2].

The sth power G^s of graph G is a graph that has the same set of vertices, but in which two vertices are adjacent when their distance in G is at most s. This note solves the edge-isoperimetric problem for the powers C_n^s of the cycle graph C_n.

Theorem 1. *If n, k, and s are positive integers such that $n \geq k$ and $n > s$, then the maximum*

$$\max_{U\subset V(C_n^s), |U|=k} e(U)$$

is attained by any set of k consecutive vertices of C_n^s.

Let n, k, and s be positive integers. We are interested in the maximal number of edges in an induced subgraph of C_n^s with k vertices. Note that if $s \geq n/2$, then $C_n^s \cong K_n$, so without loss of generality we may assume throughout this paper that $s < n/2$. We may also assume that $k \geq s+2$, since otherwise any set of k consecutive vertices is optimal because all pairs of vertices are adjacent in C_n^s.

Note that Theorem 1 does not provide the classification of maximizers, which remains an open question. An example $U = \{1, 3, 5\}$ for $n = 6$, $s = 2$ and $k = 3$ shows that the complete classification may be complicated.

Remark 1. *After the paper was sent, the author was informed that this result was recently (and independently) obtained by Makai, Pasch, Petrova and Schiller [4]. The proof is different, although the main idea is the same.*

Notation. From now on we will abuse notation slightly and we will associate vertex set of C_n^s with the elements of $\mathbb{Z}/n\mathbb{Z}$, which we will also identify with the elements of $[n]$ by their natural correspondence. We also define the following distances on $[n]$: the counterclockwise, clockwise, and cyclic distances $d_+(i,j) := |i-j|$, $d_-(i,j) = n - |i-j|$, and $d = \min(d_+, d_-)$. Also, for a subset U of $\mathbb{Z}/n\mathbb{Z}$ and an element $v \in \mathbb{Z}/n\mathbb{Z}$, let $d_+(v, U) := \min\{k \in [n] : v + k \in U\}$. For a vertex $u \in \mathbb{Z}/n\mathbb{Z}$ and a subset $U \subset \mathbb{Z}/n\mathbb{Z}$ such that $u \in U$, we denote the set of the clockwise neighbors of u in the set U by

$$N_+^U(u) := \{v \in U, v \neq u : d_+(u,v) \leq s\}.$$

Similarly,

$$N_-^U(u) := \{v \in U, v \neq u : d_-(u,v) \leq s\}$$

and

$$N^U(u) := N_-^U(u) \cup N_+^U(u).$$

Note that since $n \geq 2s+1$, we have $N_-^U(u) \cap N_+^U(u) = \varnothing$ for all $u \in C_n^s$ and all $U \subset C_n^s$.

2 Application of general bounds

2.1 Bound from Turán's theorem

A classical method for finding the maximal number of edges in a subgraph is the celebrated Turán's theorem.

Theorem 2 (Turán's)**.** *Let G be a graph with clique number $\omega(G)$ and let $k > \omega(G)$. Then*

$$\max_{U\subset V,|U|=k} e(U) \leq \binom{k}{2} - \frac{\omega(G)}{2}\left\lfloor \frac{k}{\omega(G)} \right\rfloor \left(\left\lfloor \frac{k}{\omega(G)} \right\rfloor - 1 \right).$$

The following lemma was used by Katona in his celebrated proof of the Erdős–Ko–Rado theorem.

Lemma 1. *For $2s+1 \leq n$ one has $\omega(C_n^s) = s+1$.*

Proof. Let K be a clique in C_n^s and let $u \in K$. Then all vertices of K are among the $2s$ neighbors of u in C_n^s. Let $N_-(u) := \{u_1, u_2, \ldots, u_s\}$ and $N_+(u) := \{v_1, v_2, \ldots, v_s\}$, where $d_-(u, u_i) = i$ and $d_+(u, v_i) = i$. Then note that for $i = 1, 2, \ldots, s$, we have $d(u_{s+1-i}, v_i) = s+1$, so at most one of u_{s+1-i} and v_i is in K. This means that $|K| \leq s+1$.

On the other hand, any $s+1$ consecutive vertices of C_n^s form a clique, so indeed $\omega(C_n^s) = s+1$. □

Now the application of Theorem 2 to C_n^s gives the following bound:

Corollary 1. *For $k \geq s+2$ we have*

$$\max_{U\subset V,|U|=k} e(U) \leq \binom{k}{2} - \frac{s+1}{2}\left\lfloor \frac{k}{s+1} \right\rfloor \left(\left\lfloor \frac{k}{s+1} \right\rfloor - 1 \right).$$

This gives

$$\max_{U\subset V,|U|=k} e(U) \leq \frac{sk^2}{2(s+1)} + \mathcal{O}(k).$$

2.2 Spectral bound

Another classical method for bounding the number of edges in a subgraph of a graph G is to use the spectral decomposition of the adjacency matrix A of G. Despite the fact that the following machinery is well known [1], it is complicated to find the bound in a pure form. We use the following

Proposition 1. *Let $G = (V, E)$ be a graph and $U \subset V$. If A is the adjacency matrix of G and χ_U is the characteristic vector of U, then*

$$2e(U) = \langle A\chi_U, \chi_U \rangle.$$

Proof. Note that $(A\chi_U)_i$ is exactly the number of neighbors of i among the vertices of U. Therefore $\langle A\chi_U, \chi_U \rangle$ is equal to the sum of the degrees of the vertices of U with respect to the subgraph of G induced by U, which is equal to $2e(U)$. □

Since A is real and symmetric, it admits an orthonormal eigenbasis $v_1, v_2, \ldots, v_n$. Let $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_n$ be the corresponding eigenvalues.

Lemma 2. *Let $U \subset V$ and $c_i := \langle v_i, \chi_U \rangle$ for $i = 1, 2, \ldots, n$. Then*

$$\sum_{i=1}^{n} c_i^2 = |U|.$$

Proof. Note that $\chi_U = \sum_{i=1}^{n} c_i v_i$. Therefore,

$$|U| = \langle \chi_U, \chi_U \rangle = \sum_{i,j=1}^{n} c_i c_j \langle v_i, v_j \rangle = \sum_{i=1}^{n} c_i^2.$$

□

Lemma 3. *If $U \subset V$ and $c_i := \langle v_i, \chi_U \rangle$, we have*

$$2e(U) = \sum_{i=1}^{n} \lambda_i c_i^2.$$

Proof. By Proposition 1 we have

$$2e(U) = \langle A\chi_U, \chi_U \rangle = \left\langle \sum_{i=1}^{n} \lambda_i c_i v_i, \sum_{j=1}^{n} c_j v_j \right\rangle = \sum_{i,j=1}^{n} \lambda_i c_i c_j \langle v_i, v_j \rangle = \sum_{i=1}^{n} \lambda_i c_i^2.$$

□

For regular graphs, the largest eigenvalue of the adjacency matrix, as well as its corresponding eigenvector, are known explicitly, [1].

Lemma 4. *For a d-regular graph G, we have $\lambda_1 = d$ and $v_1 = (1, 1, 1, \ldots, 1)^T$.*

We can now apply the lemmas to obtain the following:

Corollary 2. *Let $U \subset C_n^s$ with $|U| = k$, then*

$$e(U) \leq sk^2/n + \lambda_2(k/2 - k^2/2n).$$

Proof. We have

$$2e(U) = \sum_{i=1}^{n} \lambda_i c_i^2 \leq 2sc_1^2 + \lambda_2 \left(\sum_{i=2}^{n} c_i^2 \right) \leq 2sc_1^2 + \lambda_2 \left(|U| - c_1^2 \right) = \frac{2sk^2}{n} + \lambda_2 \left(k - \frac{k^2}{n} \right).$$

□

2.3 Numerical comparison

We present a numerical comparison of the general methods with the exact value for various values of k and s when $n = 1000$. As observed from the data, the spectral bound

k	s	Exact maximum	Spectral bound	Turán's bound
54	37	1295	1980	1431
118	53	4823	6149	6849
359	16	5608	5737	60691
210	115	17480	22511	21945
243	175	27125	36369	29403
313	295	48675	61627	48828
433	196	65562	73512	93331
404	372	80910	88116	81406
439	384	94656	99895	96141
473	462	111573	112499	111628

Table 1: Comparison of the exact answer and bounds for various k and s

is particularly accurate when $s \ll k$ holds.

Conversely, when k and s are close, i.e., $s \approx k$, Turán's bound provides a good approximation. Recall that Turán's theorem gives

$$\text{Turán's bound} = \binom{k}{2} - \frac{s+1}{2}\left\lfloor \frac{k}{s+1} \right\rfloor \left(\left\lfloor \frac{k}{s+1} \right\rfloor - 1 \right) = \frac{k(k-1)}{2},$$

which is close to the exact maximum

$$sk - \frac{s(s+1)}{2} \approx k\left(k - \frac{1}{2}\right) - \frac{k^2}{2} \approx \frac{k(k-1)}{2},$$

since in this regime $k - \dfrac{s+1}{2} \approx \dfrac{k-1}{2}$ and $s \approx k$.

However, in the intermediate regime where both k and s are large but $k/s \gtrsim 2$, neither bound provides an accurate approximation, as both the spectral and Turán's estimates deviate significantly from the exact maximum.

3 Proof of the main result

Proof of Theorem 1. Recall that we may assume $n/2+1, k \geq s+2$. Let $\mathcal{S}$ be the family of all sets $S \subset \mathbb{Z}/n\mathbb{Z}$ with k elements that maximize the number of edges in the induced subgraph. A subset $P \subseteq \mathbb{Z}/n\mathbb{Z}$ is called a *block* if it consists of consecutive elements of $\mathbb{Z}/n\mathbb{Z}$, i.e $P = \{p_1, p_2, \ldots, p_r\}$, where $d(p_i, p_{i+1}) = 1$ for $i = 1, 2, \ldots, r-1$. For a set $U \in \mathcal{S}$ define $f(U)$ as the maximal number of elements of U contained in a block of size s. For a subset $T \in \mathbb{Z}/n\mathbb{Z}$, which is contained in a block of size s, let $l_T, r_T \in T$ be the endpoints of T such that T is located clockwise from l_T and counterclockwise starting from r_T, see Fig. 1. Note that r_T and l_T are well-defined, since $s < n/2$.

In the figures below, black points indicate elements of the set under consideration, white points indicate non-elements, and gray points represent points whose membership is irrelevant to the argument.

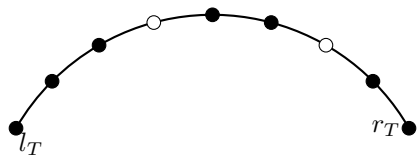


Figure 1: The endpoints of T

For a vertex $u \in \mathbb{Z}/n\mathbb{Z}$ and a subset U of $\mathbb{Z}/n\mathbb{Z}$, such that $u \in U$, define $h(u, U)$ as the size of the largest block consisting of elements of U that contains u.

Let $g(U) \subset 2^U$ be the set of all subsets of U with $f(U)$ elements that are contained in a block of size s. Let

$$h(U) := \max_{T \in g(U)} h(l_T, U)$$

and let $w(U)$ be a subset $T \in g(U)$ such that $h(U) = h(l_T, U)$, see Fig. 2.

We are now ready to choose an extremal element. Let $\mathcal{S}_1$ be the family of all sets $S \in \mathcal{S}$ that maximize $f(S)$. Let $\mathcal{S}_2$ be the family of all sets $S \in \mathcal{S}_1$ for which the quantity $h(S)$ is maximized. Pick any $M \in \mathcal{S}_2$ and let for simplicity $\mathcal{B}$ be a block of size s that

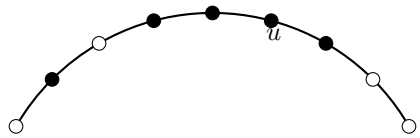


Figure 2: An example with $h(u, U) = 4$

contains $w(M)$, $A := w(M) \cap \mathcal{B}$, $u := l_A$, and and let $\mathcal{A} \subset M$ be the block of size $h(M)$ that contains u. Note that $h(M)$ may be more than s as M may contain $\mathcal{B}$.

Without loss of generality we may assume that $\mathcal{B} \subseteq \mathcal{A}$ or $\mathcal{A} \subseteq \mathcal{B}$ as otherwise we can just shift $w(M)$ counterclockwise until we reach the end of $\mathcal{B}$ while preserving the maximality of $w(M)$, so we may also assume that $u - 1 \notin M$.

Assume for contradiction that the set $C := \{w \in M \setminus A : d_+(w, A) > s\}$ is nonempty and let $v \in C$ be such that $d_+(v, A)$ is minimal, see Fig. 3. Consider the set $M' := M \setminus \{v\} \cup \{u - 1\}$. Note that $u - 1$ is adjacent to all vertices in $N_+^M(v)$ as all clockwise neighbors of v lie in the set $\{w \in M \setminus A : d_+(w, A) \leq s\}$ by the minimality of $d_+(v, M)$ on C. We further have that $|N_-^M(v)| + 1 \leq |A|$ as v and all of its counterclockwise neighbors lie in a block of size s and so by maximality of A, it must have at least as many elements. Since $u-1$ is adjacent to at least $|A|-1$ elements from $\mathcal{B}$ (as $|\mathcal{B}| \leq s$, at most one vertex is $s+1$ units apart from $u-1$), which shows that replacing v with $u-1$ gains $|A|-1-|N_-^M(v)| \geq 0$ edges in M'. However, the latter contradicts the maximality of $h(M)$ as adding $u - 1$ increases $\mathcal{A}$.

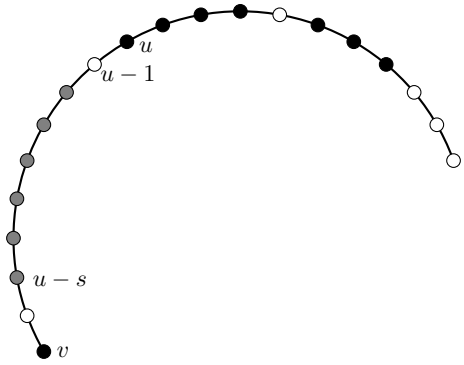


Figure 3: Swapping v and $u - 1$

Thus, all $v \in M$ satisfy at least one of the following:

1. $v \in A$;
2. $v \in \mathcal{A}$;
3. $v \in N_-^M(u)$.

We now show that $A \subseteq \mathcal{A}$. Assume for contradiction that $r_A \notin \mathcal{A}$. Then replace r_A by $u - 1$. We have that $u - 1$ is adjacent to all the other vertices in A (except maybe

r_A, which we removed) and is adjacent to all other vertices in M as all of them are on $N_-^M(u)$. Hence, the number of edges has not decreased, while $\mathcal{A}$ has increased, which again contradicts the maximality of $h(M)$. Thus, $A \subseteq \mathcal{A}$.

Finally, if $v \in N_-^M(u) \setminus \mathcal{A}$, then note that we can replace v by $u-1$ as all elements of $N_-^M(u)$ are neighbors of $u-1$ and $u-1$ has $\min(|\mathcal{A}|, s)$ neighbors from $\mathcal{A}$, which is at least the number of neighbors of v in $\mathcal{A}$. This once again contradicts the maximality of $\mathcal{A}$. Hence $|\mathcal{A}| = k$ as required.

□

Corollary 3. *If $k + s < n$, then we have*

$$\max_{U \subset C_k^s} e(U) = sk - \frac{s(s+1)}{2}.$$

Proof. Let $U := \{1, 2, \ldots, k\}$. By the previous theorem it suffices to compute $e(U)$, which we will do by counting the degree of each vertex.

The case $k \geq 2s$. Each of the vertices $s+1, \ldots, k-s$ has $2s$ neighbors. The vertices $i \in \{1, 2, \ldots, s\}$ and $k-i \in \{k-s+1, \ldots, k\}$ are of degree $s+i-1$. This gives a total of

$$\frac{2s(k-2s) + 2\sum_{i=1}^{s} s+i-1}{2} = sk - \frac{s(s+1)}{2}$$

edges.

The case $k < 2s$. Here each of the vertices $i, k-i \in \{1, 2, \ldots, k-s\}$ is of degree $i-1+s$. Also each vertex i for $i = k-s+1, k-s+2, \ldots, s$ has $i-1+k-i = k-1$ neighbors, which gives a total of

$$\frac{(2s-k)(k-1) + 2\sum_{i=1}^{k-s}(i-1+s)}{2} = sk - \frac{s(s+1)}{2}$$

edges. □

Acknowledgments. The author is grateful to Kalina Petrova for bringing paper [4] to his attention and to Danila Cherkashin for help in writing the paper. The author is also grateful to the anonymous reviewer for his remarks, which led to a significant clarification of the proof.

References

[1] Andries E. Brouwer and Willem H. Haemers. *Spectra of graphs* Springer Science & Business Media, 2011.

[2] F. Chung. Discrete isoperimetric inequalities. In *Surveys in Differential Geometry IX*, International Press, pages 53–82, 2024.

[3] Nikita A. Dubinin, Elizaveta A. Neustroeva, Andrei M. Raigorodskii, and Yakov K. Shubin. Lower and upper bounds for the minimum number of edges in some subgraphs of the Johnson graph. *Matematicheskii Sbornik*, 215(5):71–95, 2024.

[4] Tamás Makai, Matija Pasch, Kalina Petrova, and Leon Schiller. Sharp thresholds for higher powers of Hamilton cycles in random graphs. *arXiv preprint arXiv:2502.14515*, 2025.

СЕКЦИЯ Б: МАТЕМАТИЧЕСКО МОДЕЛИРАНЕ И ИНФОРМАТИКА

SECTION B: MATHEMATICAL MODELING AND INFORMATICS

МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2026
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2026
Proceedings of the Fifty-Fifth Spring Conference
of the Union of Bulgarian Mathematicians
Tryavna, Bulgaria, April 5–9, 2026

THE FOUR BASIC FUNCTIONS IN THE LEXICOGRAPHIC GENERATION OF THE SUBSETS OF A GIVEN SET

Valentin Bakoev
Faculty of Mathematics and Informatics, St. Cyril and St. Methodius University
of Veliko Tarnovo, Bulgaria
e-mail: v.bakoev@ts.uni-vt.bg

Here we apply a novel approach to generate subsets of a given set in lexicographic order and on this basis derive alternative functions for computing the successor and predecessor of a given subset. We also derive functions for ranking a given subset and unranking a given integer in a subset. We provide recursive and non-recursive implementations of these four basic functions. They run in linear time with respect to the cardinality of the given set and are easy to understand and use.

Keywords: subset, lexicographic order, characteristic vector, successor, predecessor, ranking, unranking

ЧЕТИРИТЕ ОСНОВНИ ФУНКЦИИ ПРИ ЛЕКСИКОГРАФСКО ГЕНЕРИРАНЕ НА ПОДМНОЖЕСТВАТА НА ДАДЕНО МНОЖЕСТВО

Валентин Бакоев
Факултет „Математика и информатика“, ВТУ „Св. св. Кирил и Методий“,
Велико Търново, България
e-mail: v.bakoev@ts.uni-vt.bg

Тук прилагаме нов подход за генериране на подмножествата на дадено множество в лексикографска наредба и на тази основа извеждаме алтернативни функции за изчисляване на наследника и предшественика на дадено подмножество. Също така успяхме да изведем функции за номериране на дадено подмножество и деномериране на дадено цяло число в подмножество. Предоставяме рекурсивни и нерекурсивни реализации на тези четири основни функции. Те се изпълняват в линейно време спрямо мощността на даденото множество и са лесни за разбиране и използване.

https://doi.org/10.55630/mem.2026.55.087-097

2020 Mathematics Subject Classification: 68R05, 06A05, 11B37, 68Q25.

* Partially supported by the Bulgarian National Science Fund grant number KP-06-H62/2/13.12.2022.

Ключови думи: подмножество, лексикографска наредба, характеристичен вектор, следващо подмножество, предишно подмножество, номериране, деномериране

1 Introduction

The problem of generating all subsets of a given set has important applications and therefore occupies a well-deserved place in books on combinatorial algorithms [9, 11, 8, 12, 2, 7] and others. The most popular are two orders of the generated subsets: the lexicographic order and the minimum-change (Gray code) order. Moreover, the corresponding generation algorithms may operate either byte-wise or bitwise. When subsets are generated bitwise, i.e., via their characteristic vectors, it is very natural to use the lexicographic order of these vectors. That is why S. Skiena [13, p. 454] (as well as many other authors) notes: "To generate all subsets in order, simply count from 0 to $2^n - 1$." and use the least significant n bits of the binary representation of each such integer as the characteristic vector of a subset. However, this simplest method **does not imply** a lexicographic order of the subsets themselves.

Various types of algorithms that generate all subsets of a given set in lexicographic order can be found in [9, 1, 2, 3, 14] and others. The functions for computing the successor and predecessor, as well as for ranking and unranking, play an important role in the generation of combinatorial objects [7, 12, 8, 2] and others. If such functions are created, they are always considered when generating given combinatorial objects. The four basic functions used in generating combinatorial objects and the relationships between them are illustrated in Figure 1, where c denotes the **c**urrent object and n denotes the **n**ext one.

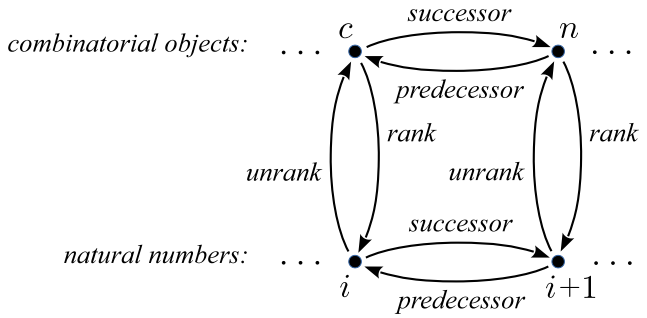


Figure 1: The four basic functions in generating combinatorial objects.

We **note** that these functions depend on the chosen order—for different orders of the same set of combinatorial objects, the corresponding functions differ from each other. Regarding their utility, Frank Ruskey notes: "One of the primary uses of ranking algorithms is that they provide *perfect hashing functions* for a class of combinatorial objects", and also: "Ranking (and unranking) is generally only possible for some of the elementary combinatorial objects" [12, p. 5].

In [4] and especially in [6] we study three basic combinatorial objects and the relationship between them according to Figure 2. We implement a new approach that, for

a given integer n, generates a sequence of serial numbers such that their binary representation, as characteristic vectors of length n, determine the lexicographic order of the subsets of a given set of n elements.

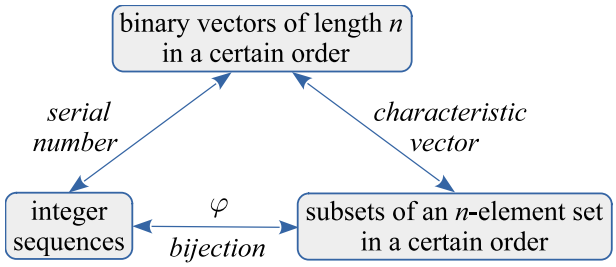


Figure 2: Basic combinatorial objects and the relationships between them.

In the monograph [6] we extended the study from [4], following the approach illustrated in Figure 1. It is written in Bulgarian, published in a small edition and therefore cannot be known to a wide audience, unlike the present work. Since the discussed problem is important and not well known, and the obtained results are new, we believe that they deserve to be presented and popularized, which is our main goal. Therefore, here we present **alternative algorithms** for the functions that compute the **successor** and **predecessor** of a given subset. We also derive **original formulas** and provide algorithms for **ranking** and **unranking** functions.

This article is organized as follows. In Section 2, we give some basic concepts and preliminary results. In Section 3, we present alternative functions for computing the subset that is the successor or predecessor of a subset defined by a given term of the integer sequence $s(n)$. The rank function (which ranks a subset given by a term of $s(n)$) and the unrank function (which unranks a natural number in a term of $s(n)$) are presented in Section 4. The last section contains some concluding remarks.

2 Basic notions and preliminary results

Here we summarize the basic notions and preliminary results from [4].

Let $\mathbb{N} = \{0, 1, 2, \dots\}$ be the set of natural numbers, and $\mathbb{N}^+ = \mathbb{N}\backslash\{0\}$. For $n \in \mathbb{N}^+$, the set of all n-dimensional binary vectors is denoted by $\{0,1\}^n = \{(x_1, x_2, \dots, x_n) | \, x_i \in \{0,1\}, \text{ for } i = 1, 2, \dots, n\}$ and is called the *n-dimensional Boolean cube* (*hypercube*). Furthermore, we define $\{0,1\}^0 = \{()\}$, where $()$ denotes the *empty vector* (with 0 coordinates). Therefore $|\{0,1\}^n| = |\{0,1\}|^n = 2^n$.

Let $\alpha = (a_1, a_2, \dots, a_n)$ and $\beta = (b_1, b_2, \dots, b_n)$ be arbitrary vectors of $\{0,1\}^n$. The natural number $\#\alpha = \sum_{i=1}^{n} a_i.2^{n-i}$ is called the *serial number* of the vector α. It is the natural number with the n-digit binary representation $a_1 a_2 \dots a_n$.

The vector α *precedes lexicographically* β, denoted by $\alpha \leq \beta$, when either $\alpha = \beta$, or $\exists i, 1 \leq i \leq n$, such that $a_i < b_i$ and $a_j = b_j$, for all $j < i$. The relation $R_{\leq} \subseteq \{0,1\}^n \times \{0,1\}^n$, called *lexicographically precedes*, is defined as $(\alpha, \beta) \in R_{\leq}$ when $\alpha \leq \beta$. Obviously, it is reflexive, transitive and *strictly antisymmetric*, that is, for any $\alpha, \beta \in$

$\{0,1\}^n$, with $\alpha \neq \beta$, either $\alpha \leq \beta$, or $\beta \leq \alpha$ holds. In this case, α and β are said to be *lexicographically comparable*. Hence $R_{\leq}$ is a *total order* in $\{0,1\}^n$.

Let $n \in \mathbb{N}^+$ and $U = \{x_1, x_2, \ldots, x_n\}$ be an universal set, whose elements are ordered according to the total order relation[1] $R_{\prec}$: $x_1 \prec x_2 \prec \cdots \prec x_n$. Let $A = \{x_{i_1}, x_{i_2}, \ldots, x_{i_k}\}$ and $B = \{x_{j_1}, x_{j_2}, \ldots, x_{j_m}\}$ are subsets of U_n whose elements are also ordered according to $R_{\prec}$. Assume that $|A| = k \leq m = |B|$—otherwise we rename the subsets. We say that A *lexicographically precedes* B and write $A \preceq B$ when either $A = \emptyset$, or $A = B$, or there exists an integer $r, 1 \leq r \leq k$, such that $x_{i_r} \prec x_{j_r}$ and $x_{i_p} = x_{j_p}$, for all $p < r$.

Usually, $\mathcal{P}(U)$ denotes the power set of U. Obviously, the relation *lexicographically precedes* $R_{\preceq}$, defined on $\mathcal{P}(U)$, is reflexive, transitive and *strictly antisymmetric* (for every $X, Y \subseteq U$, $X \neq Y$, either $X \preceq Y$, or $Y \preceq X$ holds, and then X and Y are said to be *lexicographically comparable*). Hence $R_{\preceq}$ is a *total order* in $\mathcal{P}(U)$.

Definition 1. Let $U = \{x_1, x_2, \ldots, x_n\}$ be a given set, $n \in \mathbb{N}^+$, and $X \subseteq U_n$. The vector $\alpha = (a_1, a_2, \ldots, a_n) \in \{0,1\}^n$ defined as:

$$a_i = \begin{cases} 0, \text{ if } x_i \notin X, \\ 1, \text{ if } x_i \in X, \end{cases}$$

for $i = 1, 2, \ldots, n$, is called the *characteristic vector* of the subset X.

Theorem 2. *Let U be a given n-element set, $n \in \mathbb{N}$. The function $f : \mathcal{P}(U) \to \{0,1\}^n$ is defined as $f(X) = \alpha$, where $\alpha \in \{0,1\}^n$ is the characteristic vector of X, for any $X \in \mathcal{P}(U)$. Then f is a bijection.*

For a given integer $n \in \mathbb{N}$, the notation $U_n = \{x_n, x_{n-1}, \ldots, x_2, x_1\}$, where $x_n \prec x_{n-1} \prec \cdots \prec x_2 \prec x_1$, is more convenient further on. Thus $U_0 = \emptyset$ and $U_n = \{x_n\} \cup U_{n-1}$.

The *sequence $p(n)$ of all subsets of U_n*, which is an **ordering** of the elements of $\mathcal{P}(U_n)$, is defined recursively as follows:

$$p(n) = \begin{cases} \emptyset, \text{ if } n = 0, \\ \emptyset, (\{x_n\} \cup p(n-1)), \widetilde{p}(n-1), \quad \text{if } n > 0, \end{cases} \tag{1}$$

where $\{x_n\} \cup p(n-1)$ means that the new element x_n for U_n is appended to each subset of $p(n-1)$, and $\widetilde{p}(n-1)$ means $p(n-1)$ without the empty set, i.e., $p(n-1) \backslash \emptyset$.

Theorem 3. *Let $n \in \mathbb{N}$ and $U_n = \{x_n, x_{n-1}, \ldots, x_2, x_1\}$ be a given set and $R_{\prec}$ be a total order relation such that $x_n \prec x_{n-1} \prec \cdots \prec x_2 \prec x_1$. Let the sequence $p(n)$ of all subsets of U_n be obtained according to formula (1). Then the subsets of $p(n)$ are in lexicographic order.*

In [4], recursive definitions are also given for: (a) the *sequence $c(n)$ of characteristic vectors* corresponding to the subsets of $p(n)$, and (b) the *sequence $s(n)$ of serial numbers* corresponding to the characteristic vectors of $c(n)$. Thus:

$$c(n) = \begin{cases} (), \text{ if } n = 0, \\ \mathbf{0}^n, (1, c(n-1)), (0, \widetilde{c}(n-1)), \quad \text{if } n > 0, \end{cases} \tag{2}$$

where $\mathbf{0}^n$ denotes the zero vector with n coordinates, $(1, c(n-1))$ denotes all vectors of $c(n-1)$ prefixed by 1, and $(0, \widetilde{c}(n-1))$ denotes all vectors of $c(n-1)$ except the vector

[1] Such as alphabetical order, index order, ASCII, Unicode, etc.

$\mathbf{0}^{n-1}$ prefixed by 0. And for the sequence $s(n)$:

$$s(n) = \begin{cases} 0, \text{ if } n = 0, \\ 0, (2^{n-1} + s(n-1)), \widetilde{s}(n-1), \text{ if } n > 0, \end{cases} \tag{3}$$

where $2^{n-1} + s(n-1)$ means that the integer 2^{n-1} is added to each term of $s(n-1)$ and $\widetilde{s}(n-1)$ means $s(n-1)$ without the term 0. Therefore:

Theorem 4. *The thus defined sequences $c(n)$ and $s(n)$ determine an ordering of the characteristic vectors and their serial numbers such that the corresponding subsets of U_n (resp. of $p(n)$) are in lexicographic order.*

Example 5. Let $U_3 = \{x, y, z\}$. Following the given definitions, we construct the corresponding subsets and sequences as follows:

- $U_0 = \emptyset$. Then $p(0) = \emptyset$; $c(0) = ()$, and $s(0) = 0$.
- $U_1 = \{z\}$. Then $p(1) = \emptyset, \{z\}$; $c(1) = (0), (1)$, and $s(1) = 0, 1$.
- $U_2 = \{y, z\}$. Then $p(2) = \emptyset, \{y\}, \{y, z\}, \{z\}$; $c(2) = (0, 0), (1, 0), (1, 1), (0, 1)$, and $s(2) = 0, 2, 3, 1$.
- $U_3 = \{x, y, z\}$. Then $p(3) = \emptyset, \{x\}, \{x, y\}, \{x, y, z\}, \{x, z\}, \{y\}, \{y, z\}, \{z\}$; $c(3) = (0, 0, 0), (1, 0, 0), (1, 1, 0), (1, 1, 1), (1, 0, 1), (0, 1, 0), (0, 1, 1), (0, 0, 1)$, and $s(3) = 0, 4, 6, 7, 5, 2, 3, 1$.

Based on these definitions and statements, the following algorithm was created. It sequentially generates the sequences $s(1), s(2), \ldots, s(n)$ for a given input n and implements formula (3) by performing **two main steps**. The first step is called **copy**—it copies the terms of $\widetilde{s}(i-1)$ into the same array `s` after the element with index `len`, which is the length of $s(i-1) = 2^{n-1}$. The second step is called **increase and shift**—it increases all terms of $s(i-1)$ by 2^{i-1} and shifts them to the right by 1 position in the array `s`. In doing so, `s[0]` retains its value 0. Here is its code in the C programming language.

Algorithm 1: Computes the sequence $s(n)$ for a given input $n > 0$

```
const int num = 26; // max. |U| - according to the English alphabet
const int max_len = 1 << num;  // max. |P(U)|=2^{26}
int s[max_len]; // to store s(n)
// ...
void Gen_Subsets_Lex (int n) { // 0 < n <= num
   s[0]= 0;  s[1]= 1;  // initialization: s(1)
   int len= 2;  // current length
   for (int i= 2; i <= n; i++) { // main loop - generation of s(i)
      for (int j= 1; j < len; j++) { // I step: copy s(i-1)
         s[j + len]= s[j];
      }
      for (int j= len; j > 0; j--) { // II step: increase the
         s[j]= s[j-1] + len;         // terms of s(i-1) by 2^{i-1}
      }                              // and shift them right by 1
      len *= 2;
   }
}
```

The results of the algorithm execution for $n \leq 5$ are shown in Table 1 in the form of an irregular triangle $T(n, k)$.

Table 1: The sequences $s(n)$, computed by Algorithm 1, for $n = 0, 1, \ldots, 5$.

n	$T(n,k)$, for $k =$ 0, 1, 2, 3, 4, 5, 6, 7, ...
0	0
1	0, 1
2	0, 2, 3, 1
3	0, 4, 6, 7, 5, 2, 3, 1
4	0, 8, 12, 14, 15, 13, 10, 11, 9, 4, 6, 7, 5, 2, 3, 1
5	0, 16, 24, 28, 30, 31, 29, 26, 27, 25, 20, 22, 23, 21, 18, 19, 17, 8, 12, 14, 15, 13, 10, 11, 9, 4, 6, 7, 5, 2, 3, 1

The time complexity and space complexity of the Algorithm 1 are of the type $\Theta(2^n)$, which is exponential with respect to the size of the input, but linear with respect to the size of the output. So it is a *Constant Amortized Time* (*CAT*) algorithm [12]. All of this was used in the creation of the sequence A356120 in the OEIS [10].

3 Successor and predecessor functions

Algorithms for computing the successor and predecessor of a given subset are discussed in [9, 14, 2, 3, 5]. Starting from a given subset $A \subseteq U_n$ and using them, one can generate all or some of all subsets of a given set U_n in lexicographic order.

Once the sequence $s(n)$ is generated, it is trivial to compute the successor or predecessor of its kth term, as well as to rank this term or unrank the corresponding integer. So we will derive the four basic functions **in the case when** $s(n)$ **is not available**, but using its properties presented above. Here we mean the successor/predecessor of a given term of $s(n)$. If we need a true subset, we need to start with a given subset and go through its characteristic vector, its serial number (which is a term of $s(n)$), its successor/predecessor, and back to its corresponding subset.

3.1 Successor function

Given integers n and t, where t is a **t**erm of $s(n)$, i.e., $0 \le t < 2^n$. We want to derive a recurrence formula for the **successor** (or next term) of t in the sequence $s(n)$. So, if $t = 1$, it is the last term of $s(n)$ and has no successor. Otherwise, we reason as follows:

1) If $t < 2^{n-1}$, then t is the result of the first step (copy) of Algorithm 1 and hence its successor is the same as for the sequence $s(n-1)$.

2) If $2^{n-1} \le t < 2^n$, then t is the result of the second step of the algorithm. To obtain its successor, we get the successor of $t - 2^{n-1}$ for the sequence $s(n-1)$ and then increase it by 2^{n-1}.

It remains to consider the boundary conditions. When on the ith iteration of the main loop: (1) $t = 0$ occurs, then t it is followed by 2^{i-1}—see Table 1. And (2) $t = 2^{i-1} + 1$ occurs (concerns the terms where the two subsequences are concatenated), the next term

is 2^{i-2}. Thus we obtain the formula:

$$succ(n,t) = \begin{cases} 2^{n-1}, \text{ if } t = 0, \\ 2^{n-2}, \text{ if } t = 2^{n-1}+1, \\ succ(n-1,t), \text{ if } t < 2^{n-1}, \\ 2^{n-1} + succ(n-1, t-2^{n-1}), \text{ if } t \geq 2^{n-1}. \end{cases} \tag{4}$$

Equality (4) implies the correctness of the following algorithm, which computes the successor of t.

Algorithm 2: Recurfive function for computing the successor of t in the sequence $s(n)$

```
int successor_rec (int n, int t) { // t >= 1 in the first call
   int hlen= 1 << (n - 1);  // = 2^{n-1} = half the length of s(n)
   if (0 == t)  return  hlen;
   if (t == hlen + 1)  return  hlen >> 1; // i.e. hlen/2;
   if (t < hlen)  return  successor_rec (n - 1, t);
   else  return  hlen + successor_rec (n - 1, t - hlen);
}
```

The time complexity of this algorithm is $O(n)$, since the value of n decreases by 1 in each recursive call, and the value of t decreases by 2^{n-1} when $2^{n-1} \leq t < 2^n$. Thus, the value of t is remains correct, i.e., in the interval $[0, 2^{n-1}]$. We note that a small optimization is possible if we pass `hlen` as a parameter, instead of `n`.

Here is the code of the non-recursive version of the same function. It again implements formula (4) with the same time complexity $O(n)$.

Algorithm 3: Function for computing the successor of t in $s(n)$

```
int successor (int n, int t) {
   int hlen= 1 << (n-1);  int succ= 0;
   while (t >= 0) {
      if (0 == t) { succ += hlen;  break; }
      if (t >= hlen) {
         if (t == hlen+1) { succ += hlen >> 1;  break; }
         else { succ += hlen;  t -= hlen; }
      }
      hlen >>= 1;
   }
   return succ;
}
```

3.2 Predecessor function

Now, for given integers $n \in \mathbb{N}^+$ and t, $0 \leq t < 2^n$, we want to derive a recurrence formula for the **predecessor** (or previous term) of t in the sequence $s(n)$. If $t = 0$, this is the first term of $s(n)$ and has no predecessor. Otherwise, we reason analogously:

1) If $t < 2^{n-1}$, then t is the result of the first step of the Algorithm 1 and therefore its predecessor is the same as in the sequence $s(n-1)$.

2) If $t \geq 2^{n-1}$, then t is the result of the second step of the algorithm. Therefore, its predecessor is like that in the sequence $s(n-1)$, i.e., that of $t - 2^{n-1}$, but increased by 2^{n-1}.

Boundary conditions—when on the i iteration of the main loop: (1) $t = 2^{i-1}$ occurs, then its predecessor is 0, see Table 1. And (2) $t = 2^{i-2}$ occurs (concerns the terms where the two subsequences are concatenated), then its predecessor is $2^{i-1}+1$. Thus we obtain a formula analogous to (4), the difference being in the boundary conditions.

$$pred\,(n,t) = \begin{cases} 0, \text{ if } t = 2^{n-1}, \\ 2^{n-1}+1, \text{ if } t = 2^{n-2}, \\ pred\,(n-1,t), \text{ if } t < 2^{n-1}, \\ 2^{n-1} + pred\,(n-1, t-2^{n-1}), \text{ if } t > 2^{n-1}, \end{cases} \tag{5}$$

Here is the code of a recursive function that implements formula (5) for given parameters $n \in \mathbb{N}^+$ and $t, 0 < t < 2^n$. We present the slightly optimized version (as noted above) that uses the parameter `hlen` instead of `n` and therefore, on the first call, the value of the argument corresponding to `hlen` should be 2^{n-1}.

Algorithm 4: Recursive function for computing the predecessor of t in $s\,(n)$

```
int predecessor_rec (int hlen, int t) {
   if (t == hlen)  return  0;
   if (t == hlen/2)  return  hlen + 1;
   if (t < hlen)  return  predecessor_rec (hlen >> 1, t);
   else  return  hlen + predecessor_rec (hlen >> 1, t - hlen);
}
```

Formula (5) implies the correctness of this algorithm. Its time complexity is $O(n)$ with the same arguments as for the Algorithm 2. And here is the non-recursive version.

Algorithm 5: Function for computing the predecessor of t in $s\,(n)$

```
int predecessor (int n, int t) {
   int hlen= 1 << (n - 1);
   int p= 0; // predecessor
   while (t > 0) {
      if (t == hlen/2) { p += hlen + 1;  break; }
      if (t >= hlen) {
         if (t == hlen)  break;
         else { p += hlen;  t -= hlen; }
      }
      hlen >>= 1;
   }
   return p;
}
```

4 Ranking and unranking functions

After an extensive search, we found only one source [2], where ranking and unranking functions are mentioned, but referring to reverse lexicographic order of subsets. There are no algorithms, explanations, correctness, etc., just their code (in the C++ language) is presented in less than a page. Both functions are related to the sequence A108918 in the OEIS, called "Reversed binary words in reversed lexicographic order" [10].

4.1 Ranking function

The *ordinal* (or *sequential*) *number* of a subset is the position of that subset in the sequence $p(n)$—it is the same as the position of its characteristic vector in $c(n)$, or the position of its serial number in $s(n)$. The ordinal number is an integer, which is the result of the corresponding *ranking function* applied to it. **Note** that it changes depending on the selected order of the subsets, while the serial number of the corresponding characteristic vector is unique, like the serial number of a device.

Let $n \in \mathbb{N}^+$ and $t, 0 \leq t < 2^n$, be an arbitrary term of $s(n)$. We want to compute the ordinal number of t in $s(n)$, which is its rank, denoted by r, or more precisely by $r(n,t)$. So, we are looking for r, $0 \leq r < 2^n$, such that $s(n,r) = t$. Our reasons are analogous to the previous ones: if $t = 0$, then $r = 0$, otherwise there are two possibilities for t:

1) If $t < 2^{n-1}$, then t is the result of the first step (copy) of Algorithm 1. Then its rank in the sequence $s(n-1)$ is $r - 2^{n-1}$, and then $s(n,r) = t = s(n-1, r-2^{n-1})$. Hence $r(n,t) = 2^{n-1}$ plus the rank of t in $s(n-1)$, which is $r(n,t) = 2^{n-1} + r(n-1,t)$.

2) If $t \geq 2^{n-1}$, then t is the result of the second step of the algorithm. Hence the integer 2^{n-1} is added to the element with rank $(r-1)$ in $s(n-1)$, and thus the result is t. Then $s(n,r) = t = s(n-1, r-1) + 2^{n-1}$, whence $r(n,t)$ is 1 plus the rank of $(t - 2^{n-1})$ in $s(n-1)$, which is $r(n,t) = 1 + r(n-1, t-2^{n-1})$.

Therefore, the recursive definition of r for given parameters n and t is:

$$r(n,t) = \begin{cases} 0, \text{ if } t = 0, \\ r(n-1,t) + 2^{n-1}, \text{ if } t < 2^{n-1}, \\ 1 + r(n-1, t-2^{n-1}), \text{ if } t \geq 2^{n-1}. \end{cases} \tag{6}$$

Here is the code of the ranking function that implements formula (6) and therefore this function is correct.

Algorithm 6: Recursive ranking function for the sequence $s(n)$

```
int rank_term_rec (int n, int t) {
    if (0 == t)  return  0;
    int hlen = 1 << (n-1);
    if (t < hlen)  return  hlen + rank_term_rec (n - 1, t);
    else  return  1 + rank_term_rec (n - 1, t - hlen);
}
```

The time complexity of Algorithm 6 is again $O(n)$ for the same reasons as the previous functions. The small optimization by passing `hlen` as a parameter instead of `n` is obvious. And here is the C code of the non-recursive ranking function.

Algorithm 7: Ranking function for the sequence $s(n)$

```
int rank_term (int n, int t) {
    int hlen= 1 << (n-1);  int r= 0;
    while (t) {
        if (t < hlen)  r += hlen;
        else { r++;  t -= hlen; }
        hlen >>= 1;
    }
    return r;
}
```

4.2 Unranking function

Now we need to solve the inverse problem of the ranking problem: for given integers n and r, $0 \le r < 2^n$, find the element t of $s(n)$ with rank r, i.e., such that $s(n,r) = t$. The reasons are analogous to those for deriving formula (6). If $r = 0$, then $t = 0$, otherwise:

1) If $r \le 2^{n-1}$, then t is the result of the second step of Algorithm 1, i.e., the integer 2^{n-1} is added to the element with rank $(r-1)$ in $s(n-1)$. Therefore, $s(n,r) = t = 2^{n-1} + s(n-1, r-1)$.

2) If $r > 2^{n-1}$, then t is simply copied from $s(n-1)$ to position r after executing the first step of the algorithm. Hence the rank of t in $s(n-1)$ is $r - 2^{n-1}$, i.e., $s(n,r) = t = s(n-1, r-2^{n-1})$.

So, the recursive definition of t as a function of the parameters n and r is:

$$t(n,r) = \begin{cases} 0, \text{ if } r = 0, \\ t(n-1, r-1) + 2^{n-1}, & \text{if } r \le 2^{n-1}, \\ t(n-1, r-2^{n-1}), & \text{if } r > 2^{n-1}. \end{cases} \tag{7}$$

The following two algorithms implement formula (7), which determines their correctness. Here is the C code of a recursive and a non-recursive function that unranks the integer r in a term t of $s(n)$. On the first call of the recursive function, the value of the argument corresponding to `hlen` must be 2^{n-1}.

Algorithm 8: Recursive unranking function for the sequence $s(n)$

```
int unrank_rec (int hlen, int r) {
   if (r <= hlen) {
      if (0 == r)  return 0;
      else  return hlen + unrank_rec (hlen/2,r - 1);
   }
   else  return unrank_rec (hlen/2, r - hlen);
}
```

Algorithm 9: Unranking function for the sequence $s(n)$

```
int unrank (int n, int r) {
   int hlen= 1 << (n-1);
   int t = 0;
   while (r) {
      if (r <= hlen) { t += hlen;  r--; }
      else  r -= hlen;
      hlen >>= 1;
   }
   return t;
}
```

Obviously, the time complexity the last two algorithms is $O(n)$.

5 Conclusions

Here we have considered a different approach to generating subsets of a given set in lexicographic order, which has advantages and disadvantages compared to the usual approach [6]. This approach presents a new perspective on such generation and helped us to

derive alternative successor and predecessor functions, as well as to derive original ranking and unranking functions for the lexicographic order. These four basic functions run in linear time $O(n)$ and are easy to understand. In addition to the various applications (e.g. those in [14]), ranking and unranking functions can be useful in compact representation of subsets, in generating random subsets, etc. We now consider the next step—using the presented ranking and unranking functions to derive other similar functions that operate directly on the subsets themselves, without going through their characteristic vectors.

The proposed approach can be applied to the generation of other combinatorial objects and to the derivation of their four basic functions.

References

[1] A. Aho, J. Hopcroft, J. Ullman, The Design and Analysis of Computer Algorithms. Addison-Wesley Publishing Company, 1974.

[2] J. Arndt, MATTERS COMPUTATIONAL: Ideas, Algorithms, Source Code, Springer, 2011.

[3] J. Arndt, Subset-lex: did we miss an order? https://arxiv.org/abs/1405.6503. Last accessed 12 Feb. 2026.

[4] V. Bakoev, An Algorithm for Generating All Subsets in Lexicographic Order, 2022 International Conference Automatics and Informatics (ICAI), Varna, Bulgaria, (2022), 271–275.

[5] V. Bakoev, Generating sets in lexicographic order and with minimal change, St. Cyril and St. Methodius Univ. Publ. House, Veliko Tarnovo, 2023. (monograph, in Bulgarian)

[6] V. Bakoev, Binary vectors: orderings, integer sequences, and generating of sets, St. Cyril and St. Methodius Univ. Publ. House, Veliko Tarnovo, 2023. (monograph, in Bulgarian)

[7] D. Knuth, The art of computer programming, Volume 4A: Combinatorial Algorithms, Part 1. Addison-Wesley, 2011.

[8] D. Kreher, D. Stinson, Combinatorial algorithms: generation, enumeration and search, CRC Press, 1999.

[9] A. Nijenhuis, H. Wilf, Combinatorial Algorithms for Computers and Calculators, 2nd ed., Academic Press, 1978.

[10] OEIS Foundation Inc., *The On-line Encyclopedia of Integer Sequences*. https://oeis.org/. Last accessed 12 Feb. 2026

[11] E. Reingold, J. Nievergelt, N. Deo, Combinatorial algorithms, Theory and practice. New Jersey, Prentice-Hall, 1977.

[12] F. Ruskey, Combinatorial Generation. Working Version (1j-CSC 425/520), 2003. Available at http://page.math.tu-berlin.de/∼felsner/ SemWS17-18/Ruskey-Comb-Gen.pdf. Last accessed 12 Feb. 2026

[13] S. Skiena, The Algorithm Design Manual. 2nd ed., Springer-Verlag London Limited, 2008.

[14] I. Stojmenović, M. Miyakawa, Applications of a subset generating algorithm to base enumeration, knapsack and minimal covering problems. *The Computer Journal*, Vol. 31, No. 1, (1988), 65–70.

МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2026
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2026
Proceedings of the Fifty-Fifth Spring Conference
of the Union of Bulgarian Mathematicians
Tryavna, Bulgaria, April 5–9, 2026

PERFORMANCE OPTIMIZATION OF HYBRID GNN–LLM PIPELINES FOR CODE COMPARISON

Daniel Damyanov
Department of Information Technologies, St. Cyril and St. Metodius University of Veliko Tarnovo, Bulgaria
e-mail: d.damyanov@ts.uni-vt.bg

This study proposes a set of techniques for optimizing the performance of hybrid pipelines combining large language models (LLMs) and graph neural networks (GNN) for comparison of program code fragments. On the basis on previous work [1] on semantic normalization and graph embeddings, the main computational bottlenecks are identified and solutions are proposed including parallel processing, dynamic skipping of redundant operations, caching, and optimization of graph representation. The article contributes to the practical implementation of semantic-based systems for comparing code in real conditions.

Keywords: performance optimization, GNN, LLM, code comparison, parallel processing, caching, semantic normalization

ОПТИМИЗАЦИЯ НА ПРОИЗВОДИТЕЛНОСТТА НА ХИБРИДНИ GNN-LLM ИЗЧИСЛИТЕЛНИ КОНВЕЙЕРИ ЗА СРАВНЕНИЕ НА КОД

Даниел Дамянов
Катедра „Информационни технологии“, ВТУ „Св. Св. Кирил и Методий“, Велико Търново
e-mail: d.damyanov@ts.uni-vt.bg

Настоящото изследване предлага набор от техники за оптимизиране на производителността на хибридни конвейери, комбиниращи големи езикови модели (LLMs) и графови невронни мрежи (GNN) за сравнение на фрагменти от програмен код. Въз основа на предишна работа [1] по семантична нормализация и графови вграждания, където основните проблемни места бяха забелязани в изчислителния процес и предлагат решения за паралелна обработка, динамично пропускане на излишни операции, кеширане и оптимизация на графовото представяне. Статията допринася за

https://doi.org/10.55630/mem.2026.55.098-106
2020 Mathematics Subject Classification: 68R10, 68U15.

практическата реализация на семантични системи за сравнение на код при реални условия.

Ключови думи: оптимизация на производителността, GNN, LLM, сравнение на код, паралелна обработка, кеширане, семантична нормализация.

1 Introduction

Issues related to performance and code optimization have always concerned researchers and developers [2]. After the successful development of a hybrid architecture for semantic code comparison based on LLM and GNN in previous related work [1] the possible weaknesses of the architecture and algorithms have been identified by the need for its practical optimization. The original pipeline includes several computationally intensive steps: semantic normalization via LLM, generation of multiple columns (AST, CFG, DFG), embedding via GNN and transformer, as well as merge and classification. Despite the high accuracy achieved, the temporal complexity of the system limits its applicability in real environments, especially when processing large codebases or in automatic evaluation systems with strict time constraints. The purpose of this article is to propose and evaluate performance optimization strategies that maintain semantic accuracy but significantly reduce turnaround time. The focus is on parallelization, dynamic strategies for skipping redundant computations, caching intermediate results, and graph performance optimization.

2 Related work

Real-time optimization of ML-pipelines [10], especially those involving GNN upgrades and transformers [8], represent a serious area of study. Several essential directions can be defined in optimizing this problem, consisting in parallel processing of graphs that are huge in volume[3]: dynamic sparsity approach in neural networks, embedding caching and graph representation optimization. All approaches use parameterization, which comes at the expense of additional memory and computational effort during the training and inference of models [5]. Looking at the optimizations that can be made using parallel processing, an effective optimization technique combines parallel processing with sparse matrix representations, enabling efficient graph computations on a single GPU can achieve significant acceleration (compared to CPU and previous GPU approaches) [11]. Speaking of sparsity, it can be divided into two categories: static sparse learning and dynamically sparse learning. Static sparse learning determines the structure of the sparse network at the initial stage of training by using certain preset sparse ratios by layers [3]. Dynamic sparse learning, in turn, is designed to reduce computations as well as memory footprint throughout the training phase [12]. Another widely adopted optimization is embedding caching approach for handling common code fragments reducing computational overhead in which pre-computed vector representations are stored in memory or a database for quick access on subsequent queries.

3 The approach

3.1 Refinement of Amdahl's Law and Use of Hybrid Architectures [6]

Amdahl's Law (1) provides an upper bound on the acceleration achievable through parallelization for a single parallel portion of a program:

$$S = \frac{1}{((1-p) + \frac{p}{n})} \tag{1}$$

where p denotes the fraction of the program that can be parallelized, and n is the number of processors;

In the context of machine-learning systems, where different processing stages can be parallelized to different degrees and on different hardware- Amdahl's law can be generalized through hierarchical parallelization. For our particular pipeline, we can extend it by taking into account hierarchical parallelization. This is a generalized formula for speedup in parallel computing – an extended version of Amdahl's Law when there are several parallelizable parts, each with a different number of processors (2):

$$S_{total} = \frac{1}{(1 - \sum P_i) + \sum(\frac{P_i}{N_i})} \tag{2}$$

where:

S_{total} is the overall acceleration of the program;

P_i is the proportion (percentage) of the program that can be parallelised in Part I;

N_i is the number of processors/cores used for Part I;

$1 - \sum P_i$ is the serial (non-parallelizable) part of the program;

$\sum(\frac{P_i}{N_i})$ is the effective time of parallel parts when executed on the processor N_i;

whereas $\sum P_i \leq 1$.

The original process is strictly consistent, but in the current development, parallelization is proposed, which is carried out by the following stages: independent processing of code fragments within a single comparison task, then parallel generation of AST, CFG and DFG, after normalization, simultaneous execution of GNN and Transformer encoders on the already prepared columns and text. For the original sequential pipeline, the following values for P shall be defined:

$P_1 = 0.30$ (code fragment processing)

$P_2 = 0.5$ (generation of AST, CFG, DFG)

$P_3 = 0.15$ (GNN + Transformer Coding)

$P_4 = 0.05$ (non-parallelizable parts: serialization, IO)

The total parallelizable fraction is therefore $P = 0.95$, while the strictly sequential part accounts for 5% of the execution time. At maximum parallelism ($N_1 = \infty$, $N_2 = 3$, $N_3 = 2$), the experiments were conducted on a Lenovo IdeaPad 5 Pro 16ACH6 laptop, with an AMD Ryzen 5 5600H processor (6 physical cores, 12 logical threads) and 16 GB of RAM. The parallel execution parameters are configured relative to the number of physical CPU cores. Access to the external LLM service is restricted by a semaphore with

capacity C_{LLM}=2, which limits the maximum number of simultaneous LLM requests. It is important to note that **only the code fragment processing stage (P_1) is constrained by the external LLM service**, while the remaining parallel stages are CPU-bound. Consequently, the LLM semaphore does not represent a global bottleneck for the entire pipeline. Under these assumptions, the maximum theoretical acceleration according to the extended Amdahl's law can be calculated as follows:

$$S_{total} = \frac{1}{(1 - 0.95) + (\frac{0.3}{2} + \frac{0.5}{6} + \frac{0.15}{6})} = \frac{1}{0.308} = 3.25 \tag{3}$$

Current result represents **a maximum theoretical acceleration of 3.25x** through parallelization alone. Unlike Amdahl, the Gustafson & Barsis law addresses **weak scaling [7]**, where the problem grows with available resources: $S_{scaled} = N - s * (N - 1)$, where N is the number of processors, s is the sequential part.

In the following lines direct optimizations are given that can improve and optimize calculations in a product environment:

Dynamic skipping of unnecessary normalizations

Not all code snippets need full LLM-normalization. Current system approach applies lexical analysis for complexity (e.g. number of unique identifiers, presence of commutative operations). If the evaluated complexity is below a certain threshold, normalization is skipped and the original columns are used directly.

Caching intermediate results

In order to reduce computational costs and improve the overall performance of the system, part of the intermediate results are cached in RAM or in a local database. Caching is particularly effective for operations with high computational complexity and deterministic outcome. The following intermediate artifacts are cached:

- **Normalized code**, since the normalization process is an expensive operation in terms of time and resources;
- **Generated graph representation**s associated with a hash of the normalized code, allowing reuse with identical input data;
- Graph and text embedding used in the subsequent stages of learning and similarity extraction;
- Optimize the size of columns:
  - Some nodes from the abstract syntactic tree (AST) that do not carry any essential semantic information for the analysis (e.g., certain literals or syntactic constructions without affecting the logic of the program);
  - Using compact node and edge encodings in the combined graph, which reduces memory requirements and allows for faster processing by GNN;
  - Selection of an informative subgraph for GNN embedding based on attention mechanisms that focus on critical areas of the program, such as regions around the main control structures.

3.2 Hierarchical parallelization of stages

Code fragments are processed independently enabling parallel execution of multiple pipeline stages. Access to LLM-based normalization is regulated via a semaphore to limit concurrency. This design minimizes the serial component, in accordance with the extended Amdahl's law (Figure 1).

```
public async Task<CodePairResult[]> ProcessBatchAsync(
        CodePair[] pairs,
        CancellationToken cancellationToken)
    {
        var results = new CodePairResult[pairs.Length];

        await Parallel.ForAsync(
            0,
            pairs.Length,
            new ParallelOptions
            {
                MaxDegreeOfParallelism = _maxDegreeOfParallelism,
                CancellationToken = cancellationToken
            },
            async (i, ct) =>
            {
                await _llmSemaphore.WaitAsync(ct);
                CodePair normalized;
                try
                {
                    normalized = await LLMNormalizer.NormalizeAsync(pairs[i], ct);
                }
                finally
                {
                    _llmSemaphore.Release();
                }
                results[i] = await ProcessSinglePairAsync(normalized, ct);
            });

        return results;
    }
```

Figure 1. Process batch implementation C#

In the context of the ParallelCodeProcessor, and with reference to the explanation of the implementation (Formula 2), the pipeline can be designed as a hierarchically parallelized system composed of several successive stages summarized in Table 1. Each stage exhibits a different degree of parallelization and may utilize a different number of processing units allowing for a more accurate estimation of the overall speedup:

Table 1: Stages of parallel implementation

Stage i	**Description**	**Parallelizable partition** P_i	**Number of resources** N_i
1	LLM Normalization	P_1	$N_1 = C_{LLM}$
2	Graph processing embedding	P_2	N_2 =CPU/GPU cores
3	Post-processing	P_3	N_3 =MaxDegreeOfParallelism

The Serial Part $1 - \sum P_i$ includes initialization, synchronization, serialized requests to external services. Therefore, the maximum acceleration of the pipeline is limited by the size of the semaphore for LLM requests and by the least parallelizable stage. Even with a high degree of parallelism at the other stages, the limit on the number of competing LLM applications constitutes a dominant serial component that sets the upper limit of

the S_{total}.

Rate limiting + exponential backoff (production-grade)

When interacting with external LLM services that impose restrictions on the frequency and number of requests, it is necessary to implement mechanisms for load control and resilience in case of temporary failures. The main goals in the use of *rate limiting and exponential backoff* are to prevent exceeding the API limits imposed by the LLM service provider (rate limits, quota), Figure 2, to ensure the stability of the system in case of temporary errors, related to congestion or network latency, controlling competitive access to limited external resources through a defined maximum number of concurrent requests. It also achieves a reduction in the probability of cascading failures in the parallel pipeline under high load, preserving the theoretical acceleration defined by Amdahl's extended law by minimizing the uncontrollable serial component. In the pipeline under consideration, rate limiting is implemented through a semaphore that limits the number of competing LLM requests (C_{LLM}), while Exponential Backoff applies when errors occur related to exceeding the limits or temporarily unavailability of the service. This combination allows for adaptive load management without compromising on the parallelization of the other stages.

```
private async Task<T> ExecuteWithBackoffAsync<T>(
    Func<CancellationToken, Task<T>> action,
    CancellationToken ct,
    int maxRetries = 5)
{
    var delay = TimeSpan.FromSeconds(1);

    for (int attempt = 0; attempt < maxRetries; attempt++)
    {
        try
        {
            return await action(ct);
        }
        catch (RateLimitException) when (attempt < maxRetries - 1)
        {
            await Task.Delay(delay, ct);
            delay = delay * 2; // exponential backoff
        }
    }
    throw new InvalidOperationException("LLM request failed after retries.");
}
```

Figure 2. Exponential backoff retry mechanism

Resource Profile:

1. Using CPU Cores and ThreadPool for Load Balancing
2. GPU memory for batch processing of ML operations
3. Network bandwidth to limit competing LLM API requests
4. Parallel graph generation (AST, CFG, DFG)

Graph operations demonstrate different characteristics of parallelism, which are summarized in Table 2:

Table 2: Summary analysis of the types of graphs and their characteristics

Graph type	Parallelism	Complexity	Memory	Dependencies
AST	Inner tree	$O(n)$	Low	Minimal
CFG	Over basic blocks	$O(n)$	Medium	Control dependencies
DFG	Over data flow ways	$O(n^2)$	High	Data dependencies

3.3 Experimental evaluation

The following hardware, software resources and analysis metrics were used to perform the tests and subsequent analysis:

Hardware: AMD Ryzen 5 5600H (6C / 12T), 16 GB RAM, integrated GPU, outer GPU NVIDIA RTX 3050 4GB GDDR6

Software: C#, Python (PyTorch, Hugging Face Transformers), Graph-tool.

Data: Extended dataset of 2000 triplets of code fragments, including samples of different levels of complexity.

Metrics: Time to analyze a pair of code fragments, F1-Score, Precision, Recall, memory load.

Summary results and analysis

The proposed optimizations unequivocally lead to a significant reduction in analysis time (over 58%), Table 3, with minimal loss of accuracy ($\Delta F1 \leq 0.004$). Dynamic skipping reduces calls to LLMs by about 35%. Caching shows the greatest effect on repetitive code patterns. The theoretical model based on Amdahl's extended law predicts maximum acceleration $S_{total} = 3.25$ for the evaluated hardware configuration. Working with real application the observed speedup reaches approximately $2.38\times$, approaching to about 73% of the theoretical upper bound. This discrepancy is primarily attributed to unavoidable practical factors, including synchronization overhead, partial serialization within the LLM-constrained stages, and latency introduced by external service requests. The fact that the empirically measured acceleration remains below S_{total} confirms that the theoretical value represents a correctly formulated upper limit, rather than an expected practical outcome.

Table 3: Results

Configuration	Medium time (ms)	F1-Score	Time reduction
Original pipeline	298	0.917	–
Parallelization	210	0.917	29.5%
Dynamic skipping	185	0.915	37.9%
Caching	155	0.917	48.0%
Graph optimization	142	0.914	52.3%
All optimizations	125	0.913	58.1%

4 Discussion

Generalization across hardware configurations

Although the experimental evaluation was conducted on a specific hardware setup, the proposed optimizations are largely hardware-agnostic. Techniques such as dynamic comparison skipping and embedding caching operate at the algorithmic and architectural level rather than relying on low-level hardware acceleration. As a result, similar performance trends are expected across different CPU-and-memory-based environments, with absolute execution times varying depending on available computational resources.

Interaction effects between optimizations

The applied optimizations are not independent and exhibit complementary interaction effects. In particular, caching of normalized code embeddings amplifies the effectiveness of dynamic skipping, as repeated or structurally similar submissions can be filtered early in the pipeline without invoking expensive LLM or GNN computations. While this interaction significantly reduces reliance on external ML services (e.g., LLM APIs), it introduces moderate deployment complexity and additional memory overhead for cache management. Nevertheless, these trade-offs are acceptable in scenarios such as automatic grading and large-scale code monitoring, where multiple comparisons are executed in parallel and cost efficiency is critical. Optimizations are especially effective in the context of **automatic grading of student tasks** and **code-based monitoring**, where multiple comparisons are performed in parallel. Dynamic skipping and caching reduce dependence on external ML services (LLM API), which reduces costs and increases autonomy. Limitations include slightly increased deployment complexity and the need for additional memory for caching.

5 Conclusion

Applying Discriminative Projection Using Fisher's Linear Discriminant

After obtaining joint graph–text embeddings from the GNN and Transformer encoders, an optional linear discriminative projection based on Fisher's Linear Discriminant (FLD) is applied. The objective is to maximize inter-class variance while minimizing intra-class variance between semantically similar and non-similar code pairs. Unlike deep models, FLD introduces negligible computational overhead and serves as an effective dimensionality reduction and class-separability enhancement technique prior to the final similarity estimation. This step is particularly beneficial in production scenarios with cached embeddings and dynamic skipping, where fast discrimination is required. The transition from the original sample space to a smaller dimensional space is related to the accuracy and separability of the data [9]. Current work and optimizations demonstrate that hybrid GNN–LLM code comparison pipelines could be significantly accelerated through a combination of parallelization, dynamic strategies, caching, and graph optimization. Experiments have shown a reduction in analysis time by over 58% while maintaining high semantic accuracy. This opens up the possibility of wider practical application in real systems. Subsequent future research may include the following improvements:

1. Integrated with distributed computing for multi-large codebases.
2. Adaptive dynamic skipping thresholds trained with reinforcement training.
3. Quantizing and packaging GNN and Transformer models for even faster edge device execution.

References

[1] Damyanov D., Semantic normalization on graph models searching structure matchings in code, Mathematics and Education in Mathematics (to appear).

[2] Donchev, I., An alternative to virtual functions in modern C++. Application in training, Mathematics, Computer Science and Education, Vol. 8, Issue 2, (2025), pp. 144-159
[3] Dong X., Gu Y., Sun Y., Wang L., PASGAL: Parallel And Scalable Graph Algorithm Library, (2024), https://doi.org/10.48550/arXiv.2404.17101
[4] Gale T., Elsen E., Hooker S., The State of Sparsity in Deep Neural Networks, (2019), DOI: 10.48550/arXiv.1902.09574
[5] Hoefler T., Alistarh D., Dryden T., Peste A., Sparsity in Deep Learning: Pruning and growth for efficient, Journal of Machine Learning Research 23, (2021), pp. 1-124, DOI: 10.48550/arXiv.2102.00554
[6] Holm M., Scientific Computing on Hybrid Architectures, Department of Information Technology, Uppsala University, ISSN 1404-5117, (2013), Sweden
[7] Karbowski A., Amdahl's and Gustafson-Barsis laws revisited, Pomiary Automatyka Robotyka, vol. 29(4), (2025), pp. 35-38, https://doi.org/10.48550/arXiv.0809.1177
[8] Pugacheva D., Ermakov A., Lyskov I., Igor M., Zotov Y., Enhancing GNNs Performance on Combinatorial Optimization by Recurrent Feature Update, Cornell University, (2024), DOI: 10.48550/arXiv.2407.16468.
[9] Petrov M., Dochkova J., Comparison of the PCA and FLD Approaches in Glial Tumors Classification Systems, Baltic J. Modern Computing, Vol. 13, No. 1, (2025), pp. 221-232, https://doi.org/10.22364/bjmc.2025.13.1.12
[10] Ramisetty S., Chandrasekaran T., Eruvaram V. K., Pulicharla M. R., Optimizing Real-Time Data Pipelines for Machine Learning: A Comparative Study of Stream Processing Architectures, World Journal of Advanced Research and Reviews, (2024), pp.1653–1660, DOI: 10.30574/wjarr.2024.23.3.2818
[11] Yang C., Buluc A., Owens J., GraphBLAST: A High-Performance Linear Algebra-based Graph Framework on the GPU, ACM Transactions on Mathematical Software (TOMS), Volume 48, Issue 1, (2022), pp.1-51, https://doi.org/10.1145/3466795
[12] Yin L., Li G., Fang M., Shen L., Huang T., Wang Z., Menkovski V., Ma X., Pechenizkiy M., Liu S., Dynamic Sparsity Is Channel-Level Sparsity Learner, 37th Conference on Neural Information Processing Systems NeurIPS, (2023), pp. 67993 – 68012, https://doi.org/10.48550/arXiv.2305.19454

МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2026
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2026
Proceedings of the Fifty-Fifth Spring Conference
of the Union of Bulgarian Mathematicians
Tryavna, Bulgaria, April 5–9, 2026

SEMANTIC NORMALIZATION ON GRAPH MODELS SEARCHING STRUCTURE MATCHINGS IN CODE

Daniel Damyanov[1], Zlatko Varbanov[2]
Department of Information Technologies, St. Cyril and St. Metodius University
of Veliko Tarnovo, Bulgaria
e-mails: [1]d.damyanov@ts.uni-vt.bg, [2]zl.varbanov@ts.uni-vt.bg

This study proposes an innovative approach to detecting structural matches in programming codes, which addresses the fundamental limitation of existing methods – their sensitivity to syntactic changes while maintaining logical equivalence. A hybrid architecture integrating semantic normalization through large language models (LLMs) with multispecies graph representation (AST, CFG, DFG) and embedding techniques from Graph Neural has been developed Networks (GNN) and Transformer models.

Keywords: semantic normalization, graph neural networks, large language models, structural matching, program code analysis, plagiarism detection, machine learning for code.

СЕМАНТИЧНА НОРМАЛИЗАЦИЯ ВЪРХУ ГРАФОВИ МОДЕЛИ ПРИ ТЪРСЕНЕ НА СЪВПАДЕНИЯ НА СТРУКТУРИ В КОД

Даниел Дамянов[1], Златко Върбанов[2]
Катедра „Информационни технологии“, ВТУ „ Св. Св. Кирил и Методий“,
Велико Търново, България
e-mails: [1]d.damyanov@ts.uni-vt.bg, [2]zl.varbanov@ts.uni-vt.bg

Настоящото изследване предлага иновативен подход за откриване на структурни съвпадения в програмните кодове, който адресира фундаменталното ограничение на съществуващите методи – тяхната чувствителност към синтактични промени, като същевременно се запазва логическа еквивалентност. Разработена е хибридна архитектура, интегрираща семантична нормализация чрез големи езикови модели (LLMs) с многовидово графово представяне (AST, CFG, DFG) и техники за вграждане от Graph Neural – мрежови (GNN) и трансформър модели.

https://doi.org/10.55630/mem.2026.55.107-116
2020 Mathematics Subject Classification: 68R10, 68U15.

Ключови думи: семантична нормализация, графови невронни мрежи, големи езикови модели, структурно съвпадение, анализ на програмен код, откриване на плагиатство, машинно обучение на код.

1 Introduction

The rapid development of artificial intelligence and technology companies have necessitated the widespread use of language models to generate any text and even solutions to many programming problems. Localizing similarities between two solutions to the same problem becomes a key problem in both academic and industrial environments when duplicating methods, for example. Experience has shown that students tend to abuse this, especially when it comes to writing non-trivial code and alternative designs, such as those described in [4]. In the modern technological era, these approaches have quite significant limitations, since their effectiveness decreases sharply when the code is heavily changed syntactically, but retains its logical structure. As a common example, renaming variables, changing the order of instructions, or adding comments are often enough to fool classical algorithms. Even embedding-based methods that seek to capture semantic dependencies can prove to be sensitive to such transformations if no pre-normalization of the code is performed. There is a growing need for new approaches that are resistant to syntactic changes and focusing on the real logic and data flow in the program. The current article addresses the problem of detecting structural matches in programming codes and proposes a new approach that combines semantic normalization through large language models (LLMs) with graph code representation (AST, CFG, DFG) and optimization through Graph Neural Networks (GNN).

2 Related work

Through extensive research, two main tools that do code analysis stand out, MOSS[1] and JPlag [8], that use token-based methods as well as AST-based approaches relying on Tree Edit Distance by measuring their editorial distance, or to put it another way: the minimum cost of transforming one tree into another through rudimentary operations [4]. Another very common approach is by implementing a Flow Management Graph (CFG) [1] or Program Dependencies Graph (PDG) [6]. As mentioned in the introductory part, it is quite common practice to detect duplication of methods and classes in real applications, which in turn has a direct connection also with finding plagiarized code in exams, term papers, diploma theses, etc [14]. A very common approach is the application of subgraph matching algorithms to detect the presence of predefined patterns. The main obstacle to this approach is semantic equivalence in syntactic divergence. As an example, two program constructs that can implement identical logic but differ in their superficial representation, can be deduced into several main components of differences:

1. Exchange of operands in commutative operations (e.g., $a + b$ vs. $b + a$), which is syntactically different but semantically equivalent.
2. Use of different control structures (e.g., for loop vs. while loop).

[1] https://theory.stanford.edu/ aiken/moss

3. Alternative formulations of Boolean conditions (e.g., $i < 10$ vs. $i \leq 9$).
4. Use different identifiers for local variables.

In a brief summary of the conventional graph isomorphism algorithms described so far, it is that their logic is based on the coincidence of names and structure, and such pairs cannot be recognized as equivalent. This specificity gives rise to the need for methods to transform graph models into a unified, normalized form, preserving semantics, but eliminating non-fundamental syntactic variations. such as CodeBERT[2] and GraphCodeBERT[3], use semantic embeddings, but rarely combine normalization with graph embeddings, providing an opportunity for improvement by implementing hybrid models.

3 Our approach

3.1 Methodology

The applications described above use semantic normalization as its task is to transform the graph model of the program, in which syntactically different, but semantically equivalent constructions are reduced to the same canonical form[10]. The problem faced by the application is to reduce the syntactic diversity without losing semantics, so that different implementations of the same logic become indistinguishable to the matching algorithm. The process is based on two main steps:

1. Graph Model Extraction: Convert the code into a suitable graph (AST, CFG, PDG).
2. Applying normalizing approaches: recursively traversing graph and applying a set of rules that reorder, simplify, and unify nodes.

To overcome the limitations of existing approaches, a hybrid semantic code comparison architecture is presented that integrates semantic normalization, multispecies graph representations, and fusion embedding techniques. The overall system illustrated in Figure 1 consists of seven successive stages. The following lines will describe in detail the sequence and logic behind each stage.

The lifecycle in the application is divided into four stages, which are described in detail synthesized in the following points.

Stage One – semantic normalization through large language models (LLMs) as an essential and most critical stage is the transformation of the input code into a canonical semantic form. This process is carried out by calling a pre-trained LLM that uses CodeLlama, but can also use another specialized finetuned model to perform the following operations on the submitted code:

Stage Two – unifying identifiers, local variables, functions, and parameters are renamed based on their semantic role, rather than randomly selected names by the programmer. For example, variables used for summation are renamed to sum or counter, and temporary counters are renamed to i, j, k.

Stage Three – executes canonization of expressions, syntactically different, but semantically equivalent expressions are rewritten in standard form. This includes:

[2]https://github.com/microsoft/CodeBERT
[3]https://huggingface.co/microsoft/graphcodebert-base

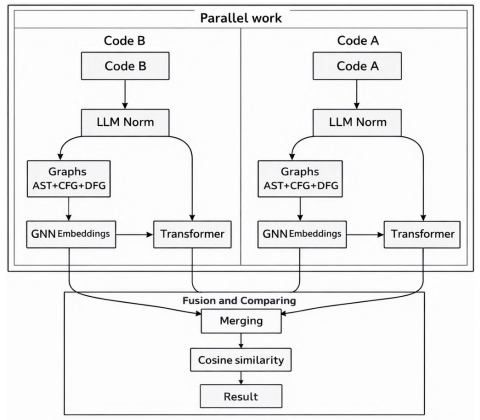


Figure 1. Semantic Code Comparison System Architecture

1. Rearranging operands into commutative operations (e.g., $b + a$ becomes $a + b$).
2. Replacing equivalent control structures (e.g., transforming a while loop into an equivalent for loop, where applicable).
3. Simplifying Boolean conditions.

Stage Four – eliminating syntactic noise, removing comments, unnecessary blanks and non-declarative elements. The end result is normalized code (normA, normB) that retains the full functionality and logic of the original, but in a significantly more unified and semantically clear form.

Stage Five – generating of a combined graph model after obtaining normalized code, code proceeds to analyze extracting three main types of columns, which together describe both the structure and behavior of the program: Generating an abstract syntactic tree (AST): it has the function of capturing the hierarchical syntactic structure of the code, making it widely used for static analysis. One of the applications of static analysis is for automated programming evaluation exercises [13]. Creating a flow control graph (CFG): its objective is to show the possible sequences of execution of instructions through an oriented graph, where the nodes are base blocks and the edges represent control transitions, an approach that is increasingly used to evaluate tasks assigned to students [13]. Data Dependency Graph (DFG) illustrates def-use dependencies between variables, showing how data is transmitted and transformed. These three columns are combined into a single enriched graph (graphA, graphB), where the nodes inherited from the AST carry operator/expression type information, and the edges are a union of the edges from the three source columns.

Stage Six – generating of embedding in order to convert the normalized code representations into a vector form suitable for comparison, two independent but complementary approaches are applied: graph embedding through GNN [7] (GNN_Encode), the combined graph is processed by the Gated Graph Neural Network (GNN) using the GGNN (Gated Graph Neural Network) architecture) [9]. GNN iteratively updates the vector representation h_v each v node by aggregating messages from its neighbors. The process can be described by the following equations:

(1) $$m_v^{(t+1)} = \sum_{u \in N(v)} W * h_t^{(u)}$$

(2) $$h_v^{(t+1)} = GRU(h_v^{(t)}, m_v^{(t+1)})[9]$$

Where:
$m_v^{(t+1)}$ – Message received from node v of iteration t
$h_v^{(t+1)}$ – State (embedding) of node v of iteration t
$N(v)$ – Set of adjacent nodes of node v
W – Trainable Tag Matrix
GRU – Gated Recurrrent Unit function

Stage Seven – the final embedding of the whole graph (embedGraphA) is obtained by applying an attention mechanism for weighted summation of the node embedding at the end of the propagation process, and for better visual perception it is summarized in a visualization of the information flow in Figure 2. At the end of the learning process, semantic learning is carried out – i.e., it is the GRU mechanism that learns which information is important.

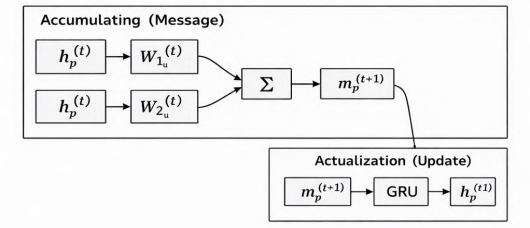


Figure 2. Visualization of the information flow

Text embedding via Transformer (Transformer_Encode) in Figure 1, parallel normalized code (normA) is fed as a sequence of tokens to a transformer-based encoder (e.g., CodeBERT). The output of the [CLS] token or the time axis average take is used as a semantic vector representation of the entire code snippet (embedTextA). Instead of relying solely on cosine similarity and empirically chosen thresholds, the fused embedding can be further processed by a supervised classifier. In particular, a Support Vector Machine (SVM) with a radial basis function (RBF) kernel was evaluated as a final decision layer, where the input feature vector corresponds to the fused embedding E_{fused}. The SVM learns an optimal separating hyperplane between plagiarized and non-plagiarized code pairs, improving robustness near the decision boundary. A Support Vector Machine (SVM) is used as a classifier leading to a high efficiency of the system [11].

3.2 Fusion and classification

Combining the strengths of structural (GNN) and semantic (Transformer) modeling, the two embedding are merged. Instead of simply concatenating, the program relies on the use of an attention fuse mechanism to dynamically weigh the contribution of each embedding. Let “Egraph” and “Etext” (1, 2) be the embedding for the graph, the calculation of attention weights is performed using the formula in Figure 2, as a

softmax-mathematical function that converts a vector of real numbers into a vector of probabilities, is given by (3, 4):

$$e_{graph} = W_{graph} * E_{graph} + b_{graph} \tag{3}$$

$$e_{text} = W_{text} * E_{text} + b_{text} \tag{4}$$

$$\alpha_{graph}, \alpha_{text} = softmax([e_{graph}, e_{text}])[3] \tag{5}$$

$$\alpha_{graph} = \frac{exp(e_{graph})}{exp(e_{graph}) + exp(e_{text}))} \tag{6}$$

$$\alpha_{text} = \frac{exp(e_{text})}{exp(e_{graph}) + exp(e_{text}))} \tag{7}$$

$$E_{fused} = \alpha_{graph} * E_{graph} + \alpha_{text} * E_{text} \tag{8}$$

Where $\alpha_{graph} + \alpha_{text} = 1$, $0 \leq \alpha_{graph}, \alpha_{text} \leq 1$

The adopted approach allows the model to learn when structural information is more important (e.g., when comparing algorithms) and when semantic information is more useful (e.g., when comparing expressions). Finally, the merged embedding fusedA and fusedB for the two code fragments are compared by calculating their **cosine similarity**:

similarity=(fusedA*fusedB)/(||fusedA||*||fusedB||)

This similarity value, placed in the interval [0, 1], is used as a statistic measure of the structural and semantic match between the two code fragments. Before start of real test limits are set for accepting or rejecting the validity of the input data:
$E_{graph} = [0.8, 0.2, 0.3]$ (Strong structural information)
$E_{text} = [0.4, 0.6, 0.5]$ (moderate semantic information)

The current development is written in C#, and in order to minimize the volume of the submitted article, the pseudocode for the main work of the application from Figure 3 is shown.

3.3 Experimental analysis

The Dataset was initially prepared, and over 1,200 code triplets were generated for the experiments, covering different types of semantic transformations that directly respond to the problems identified in the introduction. Examples are divided into two categories, first into transformations in Positive examples, such as renaming identifiers (87% of the time) – validates the effectiveness of LLM normalization; change of control structures (64% of cases) – tests the canonization of expressions; reordering operations (45% of the time) – checks resistance to syntactic variations; combined transformations (23% of the cases) – demonstrates robustness of the entire pipeline. The second category are negative examples with different algorithmic implementations (71% of cases), alternative business

```
string codeA = """
    for (int i = 0; i < 10; i++){
    total += numbers[i];
    }
    """;
string codeB = """
        int sum = 0;
        for(int j=0; j <= 9; j++){
        sum  =sum + numbers[j];
        }
    """;
double similarity = comparator.CompareCode(codeA, codeB);
Console.WriteLine($"Similarity: {similarity:P2}");
```

Figure 3. Code Semantic Comparison Algorithm

logic (29% of cases).

3.4 Metrics per rating

The system was evaluated using standard metrics focused on the effectiveness of the proposed architecture:

1. Precision, Recall, F1-Score
2. Time to analyze a file
3. Performance on different types of clones (Type 1-4)

Table 1: sample input tests.

Status	Test	Description	Expected	Received	Error
PASS	A1_IdenticalCode	Completely identical code	95.0%	92.3%	2.7%
PASS	A2_CommentsOnly	Added comments	90.0%	88.1%	1.9%
PASS	B1_RenamedVariables	Renamed variables	85.0%	82.4%	2.6%

Table 2: Statistics on categories

Category	Number of tests	Medium error	Performance
Category A	2	2.3%	100.0%
Category B	3	8.7%	66.7%

Table 3: Summary results

Metrics	Value
Overall success rate	80.0%
Meduim error	6.8%

Table 4: Comparative effectiveness of different methods

Method	Precision	Recall	F1-score	Analysis time
AST	0.723	0.681	0.701	124 ms
AST + CFG	0.815	0.792	0.803	187 ms
AST + CFG + DFG	0.892	0.863	0.877	234 ms
+ Semantic normalization	**0.934**	**0.901**	**0.917**	**298 ms**

The results described in Table 4 demonstrate that the proposed semantic normalization improves the F1-Score by 4.6% compared to traditional graph methods, confirming the hypothesis that normalization significantly increases accuracy.

Table 5: Performance by clone type

Cloning type	Without normalization	With semantic normalization	Approval
Type 1 (identical)	0.982	0.991	+0.9%
Type 2 (rename)	0.845	0.943	**+11.6%**
Type 3 (structural changes)	0.723	0.887	**+22.7%**
Type 4 (semantic)	0.512	0.768	**+50.0%**

The results in Table 5 reveals that the most significant improvement was observed in **Type 4 clones** (+50.0%), which directly confirms the expected efficiency of semantic normalization in the most complex cases of structurally distinct but semantically equivalent code.

Statistical significance

Related tests achieving a statistical significance at a confidence level of 95%, with an average improvement of 42.7% ($p < 0.01$), the error or standard deviation 8.3%, and the confidence interval: [38.2%, 47.2%]

3.5 Case studies and practical applications

The experimental data carried out have identified specific cases where the proposed approach significantly exceeds traditional methods of deception when writing code:

Name change + method rearrangement → 98% similarity after normalization

This case demonstrates the effectiveness of LLM normalization in combined syntactic changes

Comment translation + formatting change → 87% similarity

Confirms resistance to non-fundamental syntactic variations

Swapping for loop with while + changing conditions → 79% similarity

Illustrates successful canonicalization of control structures

The system and architecture designed in this way can be successfully applied to detect plagiarism in student assignments, automatic evaluation of program exercises, analysis of the evolution on a code basis.

3.6 Limitations and future work

Identified limitations through conducted experiments confirmed some of the theoretical limitations of the approach:

Time complexity: Increase by 25-30% due to normalization

Parser dependent: The quality of analysis depends on the accuracy of the syntactic parser

Complex semantic transformations: Still a challenge

Future improvements are based on the experimental results, identifying the following directions for future development:

Integration with ML-based approaches for better recognition of semantic similarities

Support for additional programming languages

Performance optimization through parallel processing of graph components

4 Conclusion

The research and subsequent development of a detection application present a different approach to semantic comparison of program codes, which largely solves the fundamental problem of existing methods, namely their sensitivity to syntactic changes while preserv-

ing the logical structure. Through a combination of semantic normalization with large LLM language models, multispecies graph representation (AST, CFG, DFG) and hybrid embedding merger (GNN + Transformer), the developed system achieves a significant improvement in the accuracy of detecting structural matches. The experimental results demonstrate a convincing effectiveness of the proposed approach. The system reaches an F1-Score of 0.917, which represents an improvement of 4.6% over traditional graph methods and over 21% compared to the basic AST-based approaches. A significant improvement was observed in Type 4 semantic clones (+50.0%), which unequivocally confirms the method's ability to recognize structurally distinct but logically equivalent conversions. The architecture shown successfully addresses the key challenges identified in the literature: resistance to renaming identifiers, canonicalization of control structures, and elimination of syntactic noise. One of the essential processes in the application, in which data is pre-prepared by merging embeddings, allows dynamic balancing between structural (GNN) and semantic (Transformer) information, significantly optimizing the comparison process for different types of code transformations. Although the noted limitations are mainly related to the time complexity and dependence on the accuracy of the syntactic parser used, the proposed approach offers significant advantages for academic and industrial practice. The system can be used in the detection of plagiarism in a learning environment, the automatic evaluation of programming exercises and the analysis of the evolution of codebases. Future research may focus on performance optimization through parallel processing, expanding support for additional programming languages, and integrating with more advanced ML-based semantic analysis techniques. The proven effectiveness of semantic normalization opens up new opportunities to improve existing code analysis systems and offers a solid foundation for developing smarter programmatic analysis tools in the age of artificial intelligence.

References

[1] Allen F., Control flow analysis. *ACM SIGPLAN Notices*, Volume 5, Issue 7, (1970), pp. 1-19, https://doi.org/10.1145/390013.808479

[2] Bahdanau D., Cho. K., Benigo Y., *Neural Machine Translation by Jointly Learning to Align and Translate*, (2014), https://doi.org/10.48550/arXiv.1409.0473.

[3] Bishop, C. M., *Pattern Recognition and Machine Learning (Information Science and Statistics)*, Springer, (2006), ISBN 978-1-4939-3843-8

[4] Donchev, I., An alternative to virtual functions in modern C++. *Application in training, Mathematics, Computer Science and Education*, Vol. 8, Issue 2, (2025), pp. 144-159

[5] Dulucq S., Touzet H., Analysis of Tree Edit Distance Algorithms, Combinatorial Pattern Matching, *14th Annual Symposium*, CPM 2003, Morelia, Michocán, Mexico, June 25-27, (2003), pp. 83-95, DOI: 10.1007/3-540-44888-87

[6] Halder R., Cortesi A., Abstract program slicing on dependence condition graphs, *Science of Computer Programming*, 78(9), (2013), pp. 1240-1263, DOI: 10.1016/j.scico.2012.05.007

[7] John K., Potika K. (2025). Diverse GNN Encoder-Decoder for Graph Anomaly Detection, *IEEE Conference on Artificial Intelligence (CAI)*, Santa Clara, CA, USA: IEEE, (2025), DOI: 10.1109/CAI64502.2025.00021, pp. 89-94

[8] Prechelt L, Malpohl G, Philippsen M., Finding Plagiarisms among a Set of Programs with JPlag, *JUCS – Journal of Universal Computer Science*, 8(11), (2002), pp. 1016-1038, https://doi.org/10.3217/jucs-008-11-1016

[9] Li Y., Tarlow D., Brockschmidt M., Zemel R., *Gated Graph Sequence Neural Networks*, (2017), https://doi.org/10.48550/arXiv.1511.05493

[10] Lubin J., Ferguson J., Ye K., Yim J., Chasins E. S., Equivalence by Canonicalization for Synthesis-Backed Refactoring. *Proceedings of the ACM on Programming Languages*, Volume 8, Issue PLDI, (2004), 1879-2004.

[11] Petrov M., A model of a two-stage classification system for glial tumors in magnetic resonance imaging, *International Conference AUTOMATICS AND INFORMATICS'2023*, Varna, October 05 – 07, (2023), DOI: 10.1109/ICAI58806.2023.10339009

[12] Putra I. S., Rukmono S., Perdana S. R., Abstract Syntax Tree (AST) and Control Flow Graph (CFG) Construction of Notasi Algoritmik, *International Conference on Data and Software Engineering (ICoDSE)*, Bandung, Indonesia: IEEE, (2021), DOI: 10.1109/ICoDSE53690.2021.9648437

[13] Sendjaja K., Rukmono. A. S., Perdana S. R., Evaluating Control-Flow Graph Similarity for Grading Programming Exercises, *International Conference on Data and Software Engineering (ICoDSE)*, Bandung Indonesia: IEEE, (2021), pp.1-6, DOI: 10.1109/ICoDSE53690.2021.9648464

[14] Wang W., Li G., Ma B., Xia X., Jin Z., Detecting Code Clones with Graph Neural Network and Flow-Augmented Abstract Syntax Tree, *IEEE 27th International Conference on Software Analysis, Evolution and Reengineering (SANER)*, (2020), pp. 261-271, DOI: 10.1109/SANER48275.2020.9054857

МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2026
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2026
Proceedings of the Fifty-Fifth Spring Conference
of the Union of Bulgarian Mathematicians
Tryavna, Bulgaria, April 5–9, 2026

BIDIRECTIONAL TRANSLATION BETWEEN TEXT-BASED AND BLOCK-BASED PROGRAMMING LANGUAGES IN THE LOGO TRADITION

Hristo Hristov
Institute of Mathematics and Informatics at the Bulgarian Academy of Sciences,
Sofia, Bulgaria
e-mail: h.hristov@posteo.net

This article presents a free and open-source, minimal implementation of bidirectional translation between text and blocks for a subset of Berkeley Logo, designed for programming turtle robots in mathematics and informatics explorations. The robots are intended to be assembled by students using off-the-shelf electronic components. The programming environment is web-based and can also be used offline. It supports switching between two editing modes – blocks and text – and four turtle-geometry commands: FORWARD and BACK (for relative translation), LEFT and RIGHT (for relative rotation). Its purpose is to provide a foundation for more advanced implementations that build on the blocks–text translation and can also be applied to projects beyond turtle geometry. Blocks mode is easier for beginners, particularly on touchscreen devices, while text mode offers greater flexibility. Switching between modes allows students to work in the way best suited to their skill level and device.

Keywords: turtle, robot, programming, logo, geometry

ДВУПОСОЧЕН ПРЕВОД МЕЖДУ ТЕКСТОВО-БАЗИРАНИ И БЛОКОВО-БАЗИРАНИ ЕЗИЦИ ЗА ПРОГРАМИРАНЕ В ТРАДИЦИЯТА НА LOGO

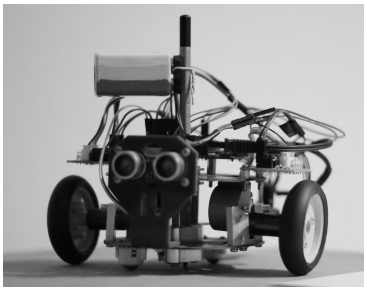
Христо Христов
Институт по математика и информатика, Българска академия на науките, София
e-mail: h.hristov@posteo.net

Тази статия представя минимална имплементация на двупосочен превод между текст и блокове за подмножество на Berkeley Logo, предназначена за програмиране на костенурки-роботи при изследвания по математика и информатика. Тя е свободен софтуер с отворен код. Роботите са предназначени да бъдат сглобявани от ученици с помощта на готови електронни компоненти. Програмната среда

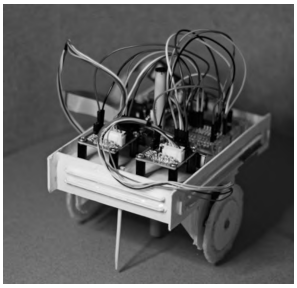
https://doi.org/10.55630/mem.2026.55.117-125
2020 Mathematics Subject Classification: 51-04, 68-04, 97-03, 97P40.

е уеб-базирана и може да се използва офлайн. Тя позволява превключване между два режима на редактиране, блоков и текстов, и поддържа четири команди в костенурковата геометрия: FORWARD и BACK (за относително преместване), LEFT и RIGHT (за относително завъртане). Целта ѝ е да послужи като основа на по-усъвършенствани реализации, които надграждат двупосочния превод между текстово-базирани и блоково-базирани езици за програмиране и могат да се използват и за проекти извън костенурковата геометрия. Блоковият режим е по-лесен за начинаещи, особено на устройства със сензорен екран, докато текстовият режим предлага по-голяма гъвкавост. Превключването между режимите позволява на учениците да работят по най-подходящия за тяхното ниво и устройство начин.

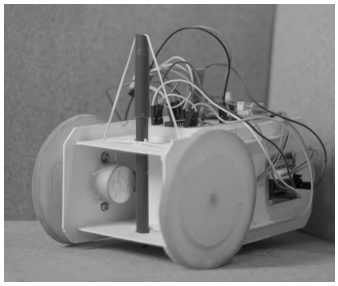
Ключови думи: костенурка, робот, програмиране, лого, геометрия



(a) Leo v1



(b) Leo v2



(c) Leo v3

Figure 1: Handmade turtle-robots

1 Introduction

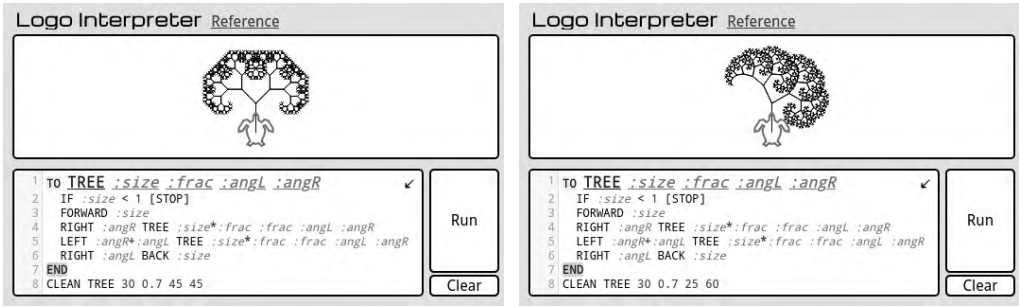
1.1 Constructionism, Logo and turtle-robots

Back in 1971, when computers were not yet widely available at schools and homes, Seymour Papert and Synthia Solomon wrote the article "Twenty Things To Do With A Computer"[5], envisioning computers being programmed by students, not vice versa. This article's 50th anniversary has been celebrated with a special collection of articles describing good educational practices in various countries, including Bulgaria [7].

There are two possible directions of the programming interaction between a child and a computer [5, p.1], leading to two approaches to education – "Constructionist approach" and "Instructionist approach". The "constructionist" approach led to the development of Logo, which became not only a programming language, but also a computer environment for explorations, philosophy and even a culture [3].

Papert characterizes the turtle as an "object to think with" [4, p.9]. Accordingly, he employed robots that can trace any geometric shape using just two commands: "FORWARD" and "RIGHT". And he called these robots *turtles ... in honor of a famous species of cybernetic animal made by Grey Walter, an english neurophysiologist.*[5, p.3]. Figure 2 presents variations of tree fractals using recursion, a conditional statement and the two

commands FORWARD and RIGHT, plus two additional commands BACK and LEFT (to avoid negative numbers as inputs).



(a) 0.7, 45, 45 (b) 0.7, 25, 60

Figure 2: Tree fractals drawn in the jslogo[10] interpreter with different parameters

1.2 Block-based and text-based

Block-based programming environments are specifically designed to help novices tinker and explore to learn programming. By using blocks over text-based languages, these environments reduce the learner's cognitive demands by limiting possible syntactic and grammatical mistakes and focusing only on developing algorithmic thinking [1, p.1]. Wrapping blocks with another blocks makes the program's structure clear and easy to understand. Blocks can also be labeled with pictures, instead of text, which allows children to learn programming before they learn reading and writing. Especially before they learn typing on a keyboard. Blocks are also easier to use on a smartphone or tablet, because these devices have a touchscreen, but lack a keyboard. Dragging blocks on such hardware is generally more accessible than typing characters.

Text-based languages require reading and typing on a keyboard (even if it is a virtual one, displayed on the screen). Young children may not yet have sufficiently developed these skills to use them effectively in the acquisition of another skill, such as programming. Consequently, the learning curve may become steep, which can lead to discouragement for some learners, particularly those who already have limited confidence in their abilities in other domains. Developing proficiency in programming can provide a foundation for learners to build confidence in their ability to acquire other skills, particularly when the learning experience is engaging and meaningful. This sense of self-efficacy may transfer to other areas, including problem-solving, communication, and emotional intelligence. Therefore, minimizing unnecessary barriers to programming can be an effective strategy in math and computer science education.

Once initial barriers are removed, overly "user-friendly" interfaces can limit deeper understanding, particularly for older students skilled in typing or motivated to master it. In text mode, copying, pasting, and multi-line editing are faster than with blocks, and experienced users can navigate code efficiently in editors like Vim[1] or GNU Emacs[2],

[1] `https://www.vim.org/`
[2] `https://www.gnu.org/software/emacs/`

with the entire source visible unless sections are folded or separated.

Text-based programs can be exported simply by copying the source code, while blocks often require a specific file format or multiple screenshots for large programs. Syntax in text languages can be complex, with structure determined by brackets, quotes, or indentation, which vary across languages. Blocks make these structures more visible, supporting debugging and comprehension. Each approach has strengths and limitations, and switching between them allows learners to focus on the program itself rather than the mechanics of programming.

1.3 The design for the turtle-robot

Papert and Solomon's vision of turtles being affordable for every child [5, p.3] is now achievable and enhanced. Recent studies evidence that robotics in education improves cognitive skills, fosters interdisciplinary learning, and bridges the gap between theory and practice [8, p.1]. In 2025, we developed Leo v2[3] (Figure 1b), designed for students to assemble their own turtle robot at minimal cost while retaining essential turtle-geometry functionality. Using off-the-shelf components, the robot can be programmed offline via a free, open-source compiler compatible with GNU+Linux, OpenBSD, macOS, or Windows, making hands-on exploration of geometric and algorithmic concepts accessible to all learners.

The article "Turtle Geometry with Arduino and Snap! – Developing Interactive Tools for Learning and Experimentation in Mathematics and Informatics" [2] guides students, parents, and teachers through acquiring widely available electronic components, cutting the robot body from cardboard, assembling it, and programming its microcontroller. Schematics, CAD drawings, and 3D models[4] are provided under the GPL v3 license, enabling users to build upon and share their own designs. CAD files also allow batch production of the robot body from cardboard, wood, or metal, using laser cutters, making it feasible for schools, municipalities, or governments to supply all students, though individuals can build their own with minimal support. A student who assembles a personal robot can provide peers with both inspiration and guidance, encouraging the creation of modified, personalized versions. As Papert and Solomon noted in 1971, turtles can have "sense organs". From simple touch, light, and sound sensors to advanced accelerometers and tilt detectors, exemplifying a low floor, high ceiling approach to learning [5, p.3].

1.4 The Previous Step: Blocks → Text Translator

The Leo v2 design [2] includes a translator from the block-based Snap![5] to text-based Arduino[6], enabling its ATmega328P[7] microcontroller to be programmed in both languages. This translator was developed to ease the learning curve for students familiar with block-based programming but less confident with text. The present work extends this effort by implementing bidirectional translation between blocks and text within a small subset of Berkeley Logo[8].

[3] https://hristov-imi-tezo.gitlab.io/vtu-ndmi-2024/

[4] https://gitlab.com/hristov-imi-tezo/vtu-ndmi-2024

[5] https://snap.berkeley.edu/

[6] https://docs.arduino.cc/language-reference/

[7] https://ww1.microchip.com/downloads/en/DeviceDoc/Atmel-7810-Automotive-Microcontrollers-ATmega328P_Datasheet.pdf

[8] https://people.eecs.berkeley.edu/~bh/v2ch14/manual.html

1.5 Evolution of Turtle Programming

Text-based languages are historically the primary method for programming turtles, originating when the first Logo language was created for text-driven computers. Modern interpreters, such as UCBLogo[9] (offline) and jslogo[10] (online), support virtual turtle programming. Block-based languages, widely used in education, include Snap![5] and Scratch[11] [6, p.31]. Snap! also supports microcontroller programming via the S4A Connector library[12], making it suitable for physical turtle robots. This evolution illustrates how combining blocks and text enables learners to progress from low-floor, high-ceiling visual programming to more advanced text-based programming.

1.6 Current goal

Bidirectional translation between text and blocks has also been implemented in CoffeeScript to program a virtual turtle in Pencil Code[13]. The Droplet library[14], used there, is employed for the same purpose in the implementation provided with this article (Appendix). The current work presents a minimal implementation of bidirectional translation for a small subset of Berkeley Logo, supporting only FORWARD and RIGHT. It serves as a foundation for further developments, including sending programs to a physical turtle robot such as Leo v2; an example of such a more developed environment is presented in Further developments.

2 Materials and methods

The provided implementation for bidirectional translation (Appendix) has two dependencies:

1. Droplet[14] – the JavaScript library used in Pencil Code[13]
2. Ace[15] – a JavaScript text editor library, used by Droplet for the text mode

If they are downloaded in advance, the programming environment can be used offline. The needed files are:

- **ace.js**[16] – the Ace text editor
- **mode-coffee.js**[17] – CoffeeScript mode for Ace
- **worker-coffee.js**[18] – CoffeeScript worker for Ace
- **theme-chrome.js**[19] – the default theme for Ace
- **droplet-full.js**[20] – the Droplet editor

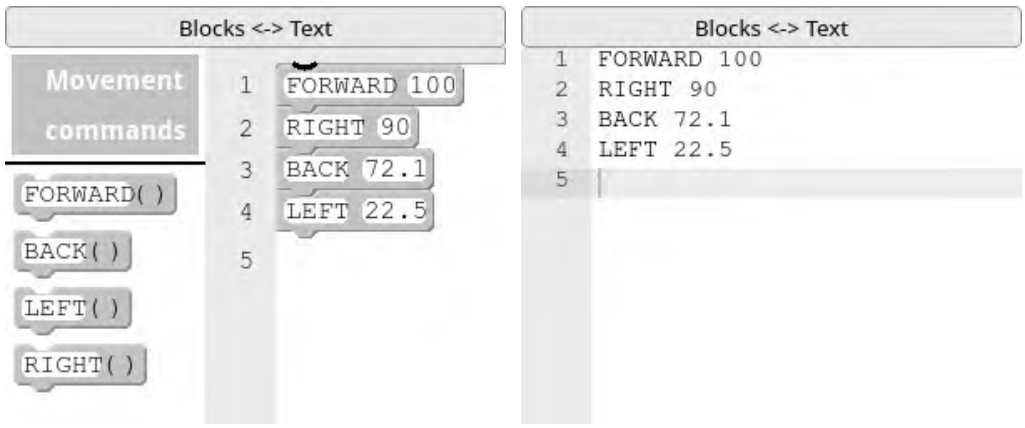
[9] https://people.eecs.berkeley.edu/~bh/logo.html
[10] https://www.calormen.com/jslogo/
[11] https://scratch.mit.edu/
[12] https://snap.creativelearninglab.click/course/view.php?id=2
[13] https://gym.pencilcode.net/draw/
[14] https://droplet-editor.github.io/
[15] https://ace.c9.io/
[16] https://cdn.jsdelivr.net/npm/ace-builds@1.43.5/src-noconflict/ace.js
[17] https://cdn.jsdelivr.net/npm/ace-builds@1.43.5/src-noconflict/mode-coffee.js
[18] https://cdn.jsdelivr.net/npm/ace-builds@1.43.5/src-noconflict/worker-coffee.js
[19] https://cdn.jsdelivr.net/npm/ace-builds@1.43.5/src-noconflict/theme-chrome.js
[20] https://droplet-editor.github.io/assets/droplet-full.js

- **droplet.css**[21] – stylesheet for Droplet

They can also be found in the repository of this article[22].

3 Results

The implementation for bidirectional translation between text and blocks provided with this article (Appendix) can serve as a foundation and a minimal working example. It contains a palette with four blocks – FORWARD, BACK, LEFT and RIGHT (Figure 3a). When dragged to the blocks editor, they receive a default value and become FORWARD 100, BACK 100, LEFT 90 and RIGHT 90. Only blocks attached to the top-left corner are translated to text when the "Blocks ↔ Text" button is clicked (Figure 3b). Clicking again restores the blocks editing mode, translating the text back to blocks and reintegrating any detached blocks.



(a) Blocks mode (b) Text mode

Figure 3: Basic user interface (Appendix)

4 Discussion

The minimal implementation presented in the Results section and Appendix is not sufficient for exploring geometric and algorithmic concepts using turtle geometry, as it lacks both a virtual turtle and a connection to a physical one. Its purpose is to provide a foundation for more developed implementations that build on the blocks–text translation and can also be applied to projects unrelated to turtle geometry. Blocks mode is easier for beginners, especially on touchscreen devices, while text mode allows greater flexibility. Switching between modes lets students work in the way best suited to their skill level and device. UTF-8 icon support enables programs to use icon-based syntax in both modes. Blocks mode also aids debugging by clarifying program structure, particularly when the code is complex or poorly formatted.

[21] `https://cdn.jsdelivr.net/npm/droplet-editor@0.0.2/css/droplet.css`
[22] `https://gitlab.com/hristov-imi-tezo/smb-2026`

Using Droplet or any other library which can work offline allows independence from internet or server connections, ensuring long-term accessibility: future users can explore geometric and algorithmic concepts with these robots under the same conditions, even as technology evolves, assuming electricity is available.

5 Further developments

The provided implementation is minimal, serving as a foundation for further development. It has been extended[23] to program physical turtle robots such as Leo v2, with source code and the microcontroller program shared in the Git repository of this article[24] under GPL v3.

Future work includes supporting a larger subset of Berkeley Logo — procedures, recursion, loops, and conditionals — so students can test programs virtually with UCBLogo before using a robot. Hardware support for PENUP/PENDOWN would allow movement without leaving a trace, and translation between different text languages would enable use of Scheme, Python, JavaScript, Arduino, C++, C, or assembly depending on task or learning goals.

6 Acknowledgments

My deepest gratitude to my mentor Evgenia Sendova for inspiring me to explore and teach mathematics through turtle geometry.

Appendix

index.html[25]

```
<!DOCTYPE html>
<html>
  <head>
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <link rel="stylesheet" href="lib/droplet/droplet.css"/>
    <style>
      #toggleBtn {
        position: absolute; left: 0; right: 0; top: 0; height: 25px;
      }
      #droplet-editor-wrapper {
        position: absolute; left: 0; right: 0; top: 25px; bottom: 0;
      }
    </style>
  </head>
  <body>
    <button id="toggleBtn" onclick="editor.toggleBlocks()">Blocks <-> Text<
    /button>
    <div id="droplet-editor-wrapper">
      <div id="droplet-editor"></div>
    </div>
    <script src="lib/ace/ace.js"></script>
    <script src="lib/droplet/droplet-full.js">
```

[23] https://hristov-imi-tezo.gitlab.io/smb-2026/ui
[24] https://gitlab.com/hristov-imi-tezo/smb-2026
[25] https://hristov-imi-tezo.gitlab.io/smb-2026/assets/src/index.html

```
    </script>
    <script>
      const movementBlocksArr = [
        { block: "FORWARD()",          // forward movement block
          expansion: "FORWARD 100" }, // default value: 100 mm
        { block: "BACK()",             // backward movement block
          expansion: "BACK 100" },    // default value: 100 mm
        { block: "LEFT()",             // left rotation block
          expansion: "LEFT 90" },     // default value: 90 degrees
        { block: "RIGHT()",            // right rotation block
          expansion: "RIGHT 90" }     // default value: 90 degrees
      ];
      const dropletEditorOptions = {
        // CoffeScript is the selected language for parsing,
        // because it works better with the Logo language syntax
        // than the other languages currently supported by the Droplet
    library
        // (JavaScript, CoffeeScript, HTML, C and partially Python, Java,
    BASIC)
        mode: "coffee",
        palette: [{
          name: "Movement commands",
          color: "blue",
          blocks: movementBlocksArr
        }]};
      const editor = new droplet.Editor(
        document.getElementById('droplet-editor'),
        dropletEditorOptions
      );
    </script>
  </body>
</html>
```

References

[1] Dong, Yihuan and Marwan, Samiha and Catete, Veronica and Price, Thomas and Barnes, Tiffany (2019) Defining Tinkering Behavior in Open-ended Block-based Programming Assignments, Association for Computing Machinery, SIGCSE '19, pp. 1204–1210, https://doi.org/10.1145/3287324.3287437

[2] Hristov, H. (2025) Turtle Geometry with Arduino and Snap! – Developing Interactive Tools for Learning and Experimentation in Mathematics and Informatics, Mathematics, Computer Science and Education, Volume 8 Issue 1, pp. 48-68, https://journals.uni-vt.bg/mcse/eng/vol8/iss1/art7

[3] Papert, Seymour A. (1999) What is Logo? And Who Needs It?. Logo philosophy and implementation. Logo Computer Systems Inc., https://dailypapert.com/what-is-logo-and-who-needs-it/

[4] Papert, Seymour A. (1980) Mindstorms: children, computers, and powerful ideas. ISBN:978-0-465-04627-0, https://www.media.mit.edu/publications/mindstorms/

[5] Papert, Seymour A. and Solomon, Cynthia (1971) Twenty Things To Do With A Computer https://doi.org/1721.1/5836

[6] Perin, Ana Paula Juliana and dos S. Silva, Deivid Eive and Natasha

M. C. Valentim (2023) Investigating block programming tools in high school to support Education 4.0: A Systematic Mapping Study, Informatics in Education, volume 22, issue 3, pp. 463-498, https://doi.org/10.15388/infedu.2023.21

[7] Sendova, Evgenia (2021) An Eternal Source of Inspiration or What the Bulgarian Turtle Told Achilles This Time in Gary Stager, Twenty Things to Do with a Computer Forward 50, Constructing Modern Knowledge Press, 63-92, ISBN 978-1-955604-01-7

[8] Zhang, Deyu and Wang Jiawen and Jing Yanbin and Shen Ao (2024) The impact of robotics on STEM education: Facilitating cognitive and interdisciplinary advancements, Applied and Computational Engineering, volume 69, pp. 7-12, https://doi.org/10.54254/2755-2721/69/20241433

МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2026
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2026
Proceedings of the Fifty-Fifth Spring Conference
of the Union of Bulgarian Mathematicians
Tryavna, Bulgaria, April 5–9, 2026

AI-DRIVEN CYBERSECURITY IN CRITICAL INFRASTRUCTURE: A BIBLIOMETRIC ANALYSIS (2015–2025)

Evgeniya Nikolova[1], Todor Slavov[2]
[1]Institute of Mathematics and Informatics, Bulgarian Academy of Sciences, Sofia, Bulgaria
[2]Faculty of Computer Science and Engineering, Burgas Free University, Burgas, Bulgaria
e-mails: [1]enikolova@bfu.bg, [2]tslavov@bfu.bg

This paper presents a bibliometric analysis of 1,862 research documents (2015–2025) focused on the application of Artificial Intelligence (AI) for Critical Infrastructure (CI) cybersecurity. Data from Scopus and Web of Science were processed using the Bibliometrix R-package. The study quantifies publication dynamics and maps thematic and sector-specific patterns in AI methods applied to OT/ICS/SCADA cybersecurity after 2020. Sector-specific analysis reveals distinct technological profiles: the Energy sector *remains anchored in SCADA security and False Data Injection detection; the Transport sector shows a shift toward Federated Learning for connected mobility; and the Water sector highlights a niche but growing focus on Explainable AI (XAI) and IoT. These findings map the transition from general infrastructure protection to domain-specific AI countermeasures.*

Keywords: Artificial intelligence; critical infrastructure; OT/ICS/SCADA; cybersecurity; anomaly detection; federated learning; false data injection; bibliometric analysis.

КИБЕРСИГУРНОСТ В КРИТИЧНАТА ИНФРАСТРУКТУРА: БИБЛИОМЕТРИЧЕН АНАЛИЗ (2015–2025)

Евгения Николова[1], Тодор Славов[2]
[1]Институт по математика и информатика, Българска академия на науките, София,
[2]Център по информатика и технически науки, Бургаски свободен университет
e-mails: [1]enikolova@bfu.bg, [2]tslavov@bfu.bg

Тази статия представя библиометричен анализ на 1862 научни публикации (2015–2025), свързани с прилагането на изкуствен интелект (ИИ) на критичната инфраструктура. Данните представляват библиографски записи и метаданни (заглавия,

https://doi.org/10.55630/mem.2026.55.126-133
2020 Mathematics Subject Classification: 68M25, 68T01.

резюмета, ключови думи, година, източник/списание или конференция и др.), извлечени от базите Scopus и Web of Science и обработени с помощта на R-пакета Bibliometrix. Изследването установява значително увеличение на научната продукция след 2020 г. Секторният анализ разкрива различни технологични профили: енергийният сектор остава фокусиран върху SCADA сигурността и откриване на инжектиране на фалшиви данни; транспортният сектор показва преминаване към федерирано обучение за свързана мобилност; водният сектор фокус върху обясним ИИ (XAI) и IoT. Тези резултати картографират прехода от обща защита на инфраструктурата към специфични за областта ИИ решения.

Ключови думи: Изкуствен интелект; критична инфраструктура; OT/ICS/SCADA; откриване на аномалии; федерирано обучение; инжектиране на фалшиви данни; тренд анализ.

1. INTRODUCTION

Critical infrastructure (CI) refers to systems and assets whose disruption would have a significant impact on societal safety, economic stability, and essential services. Core examples include energy systems, transportation networks, and water utilities. The digital transformation of these sectors has increased connectivity and automation [4], but it has also expanded the exposure of operational technology (OT) environments such as industrial control systems (ICS) and supervisory control and data acquisition (SCADA). Compared to conventional IT, OT/ICS/SCADA systems are constrained by legacy protocols, long equipment lifecycles, strict availability requirements, and safety-critical operating conditions. Consequently, cyber incidents in CI can propagate beyond data loss to physical disruption and public safety impacts.

In parallel, artificial intelligence (AI) techniques, most notably machine learning (ML) and deep learning (DL), have become central to contemporary cyber defense research. AI-based approaches are widely explored for intrusion detection, anomaly detection, malware/threat identification [1], and resilience-oriented monitoring. However, CI cybersecurity literature is highly heterogeneous. AI methods are applied across different domains (e.g., power grids, connected mobility, water distribution), evaluated under different assumptions, and described using partially overlapping terminology. This fragmentation makes it difficult to identify which research directions are stabilizing, which are declining, and which are emerging— especially because trends differ substantially across CI sectors.

Recent surveys (2022–2024) on AI for cybersecurity often adopt a narrative approach or focus predominantly on a single CI domain (most often smart grids/energy), while treating critical infrastructure as a monolithic application area. In addition, many reviews do not provide transparent, reproducible merged corpus across major bibliographic databases. The present study provides mapping and comparing sector-stratified thematic structures for OT/ICS/SCADA security in Energy, Transport, and Water, revealing distinct technological trajectories rather than a single "CI cybersecurity" trend. Unlike prior single-sector reviews, our results explicitly quantify and visualize cross-sector divergence (e.g., federated learning visibility in Transport versus XAI signals in Water), which is not observable when CI is analyzed as one aggregate corpus.

The paper is organized into three main structural sections: introduction, methodology, and results and discussion. The methodological section presents the PRISMA-oriented

research design, the data sources used, the study objectives, and the applied bibliometric analytical approaches. In the Results and Discussion section, the publications are systematized and analyzed through sector-specific thematic mapping, accompanied by a critical discussion of the methodological robustness and limitations of the approach used.

2. METHODOLOGY

This study applies a PRISMA-guided systematic search and transparent dataset accounting, combined with bibliometric mapping and keyword-based thematic analysis, to identify research patterns in AI-driven cybersecurity for critical infrastructure (CI), with a focus on OT/ICS/SCADA contexts, over 2015–2025. PRISMA 2020 guidelines were used to ensure transparent reporting of identification, screening, and inclusion [3].

The study aims to analyze publications in the field of AI-based cybersecurity for critical infrastructure by examining publication dynamics, the formation of thematic clusters, the evolution of emerging and maturing topics, and sectoral differences in accordance with the protection needs of three sectors: energy, transport, and water.

Two bibliographic databases were used: Scopus and Web of Science Core Collection. Queries were constructed using three semantic blocks: (1) AI methods, (2) CI/OT/ICS/SCADA domains, and (3) security objectives (e.g., intrusion/anomaly/threat detection). Searches were restricted to 2015–2025, English language, and peer-reviewed journal articles and conference/proceedings papers. Exclusion terms were used to reduce off-scope retrieval. Full database queries (Scopus TITLE-ABS-KEY and WoS TS) are provided in the online repository (Data availability).

Records were retrieved from Scopus (n = 1,774) and Web of Science Core Collection (n = 971) for the period 2015–2025 (total n = 2,745) and imported into R for merging and deduplication using bibliometrix [2] via the Biblioshiny interface. Automated deduplication was performed primarily by DOI, supported by title-based matching, resulting in a final unique corpus of n = 1,862 documents (duplicates removed = 883). Because objective of the study is bibliometric mapping and thematic trend analysis, eligibility was assessed at the metadata level (titles/abstracts/keywords) and no formal full-text eligibility stage was conducted. Although the merged corpus contains a small number of 2026-indexed records (n = 4), all analyses in this paper were restricted to publications from 2015–2025. Due to database indexing conventions (e.g., early access/online-first records), a very small number of records tagged as 2026 may appear in the metadata exports; however, the study's interpretation and reported trends focus on the 2015–2025 window and are not affected materially by this negligible fraction.

Bibliometric mapping and thematic analysis were conducted in R using bibliometrix/biblioshiny [2]. Conceptual structure was derived via co-word analysis, operationalized as keyword co-occurrence networks and thematic maps. To reduce noise from heterogeneous indexing, thematic mapping was performed primarily using **Author Keywords**.

For sector-oriented analysis, the merged corpus was stratified into **Energy (N=716), Transport (N=1131), and Water (N=233)** using rule-based **multi-label** tagging applied to a concatenated metadata field (Title + Abstract + Author Keywords; TI + AB + DE). Boolean sector flags were generated using domain-specific dictionaries (e.g., grid/power/SCADA for Energy; rail/traffic/vehicle/V2X for Transport; water/wastewater/treatment for Water), allowing overlaps across sectors when multiple keyword sets matched a record.

A supplementary thematic evolution analysis (cut-point 2020) was conducted for the Energy sub-corpus using **All Keywords** to increase term coverage; outputs (tables/figures) are provided in the online repository (Data availability). Borderline inclusion and tagging cases were discussed with a second researcher to ensure consistent application of criteria.

3. RESULTS AND DISCUSSION

Our work focuses on three CI sectors (Energy, Transport, Water) selected due to data availability and relevance to OT/ICS/SCADA security; other CI sectors were left for future work.

3.1. Sector-Specific AI Strategies

Table 1. Summary of Sector-Specific Bibliometric Profiles (2015–2025)

Sector	Sub-corpus size N	High-frequency themes	Distinctive/emerging
Energy	716	FDI; SCADA	Increased attention to grid-specific adversarial models (e.g., false data injection; state estimation)
Transport	1131	SCADA/ICS security; anomaly detection; intrusion detection; cybersecurity	Federated learning (privacy/privacy-preserving mobility)
Water	233	Anomaly detection; industrial control systems; intrusion detection; ML/DL	Niche growth toward explainable AI (XAI) and IoT trust/monitoring in water distribution contexts

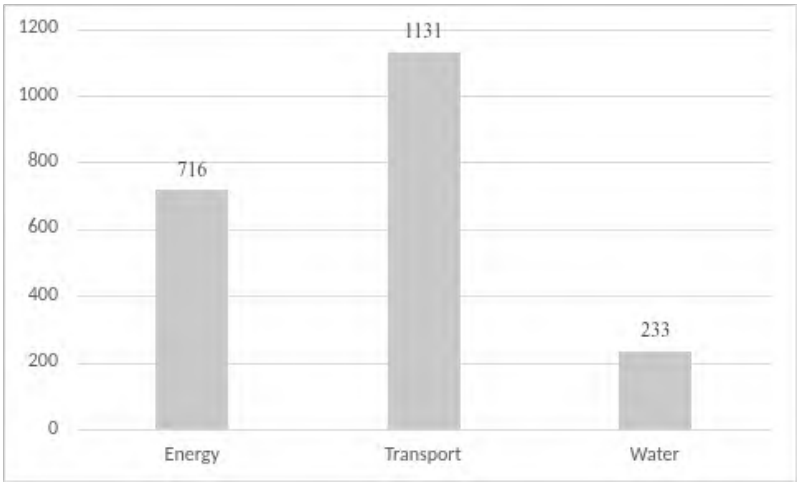


Figure 1. Sub-corpus sizes by sector

Table 2. Emerging vs. Declining/Maturing Thematic Clusters

Category	Identified Themes (Keywords)	Context / Sector Impact
Emerging / recently visible themes	Federated learning; XAI	Transport: federated learning cluster (CF = 243); Water: explainable AI cluster (CF = 26)
Maturing / baseline themes	Signature-based detection; Standard NNs/LSTMs; General **SCADA** terms	Recurrent across sector maps; foundational vocabulary

	Energy	**Transport**	**Water**
Emerging themes	—	Federated Learning	XAI (+ IoT signal)
Maturing / baseline themes	SCADA / Anomaly Detection / Intrusion Detection	SCADA / ICS Security / Anomaly Detection	Anomaly Detection / ICS / ML

Figure 2. Summary matrix of sector association of emerging vs baseline themes

Our work focuses on three CI sectors (Energy, Transport, Water) selected due to data availability and relevance to OT/ICS/SCADA security; other CI sectors were left for future work. The analysis was conducted separately for Energy (N=716), Transport (N=1,131), and Water (N=233), emphasizing the distinctive thematic patterns and, where applicable, their temporal evolution within each sector. Tables 1 and 2 collectively summarize the sector-specific bibliometric profiles for 2015–2025, detailing sub-corpus sizes, high-frequency keywords, distinctive and emerging topics across Energy, Transport, and Water, and categorizing thematic clusters into emerging versus maturing trends with their sectoral context and impact. Sub-corpus sizes are visualized in Figure 1, while sector association of emerging versus baseline themes is summarized in Figure 2.

Detailed time-slice outputs (Energy evolution split at 2020) are available in the online repository (Data availability).

3.1.1. Energy Sector The Energy sub-corpus (N=716) is dominated by OT/ICS/SCADA-oriented security and AI-based detection (Fig. 3). In the thematic map, machine learning co-occurs strongly with SCADA, anomaly detection, and industrial control systems, indicating a shared baseline for monitoring and detection, while additional clusters (cybersecurity, intrusion detection, deep learning) reflect the consolidation of AI-based protection methods in OT environments. A supplementary thematic evolution analysis (split at 2020) suggests a shift from broader CI themes toward more specialized network-security topics, including links from power-system protection to state estimation and false-data-injection attack detection; outputs are available in the online repository (Data availability). Overall, Energy-sector research remains SCADA-centered, with increasing emphasis on grid-specific attack models.

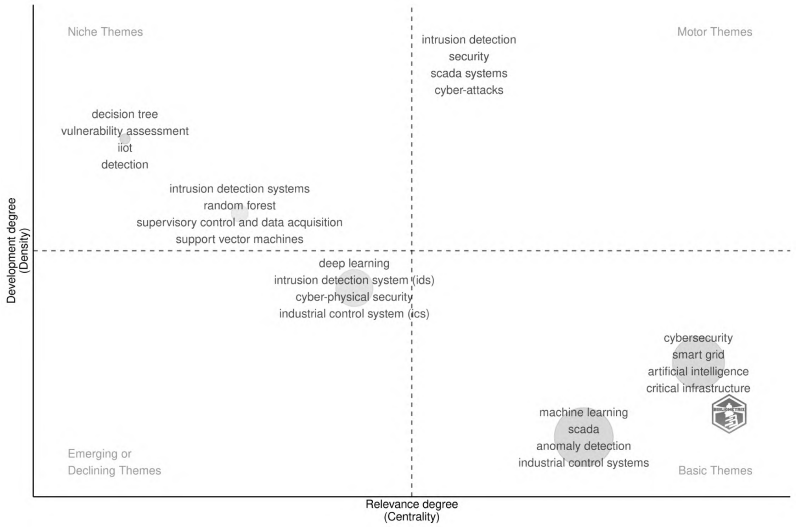


Figure 3. Thematic Map of the Energy sector

3.1.2. Transport Sector The Transport sub-corpus highlights a different thematic emphasis (Fig. 4). General security terminology remains pervasive, while the thematic map separates methodological directions: anomaly detection and intrusion detection are prominent, and federated learning emerges as a sector-differentiating theme, indicating growing attention to distributed and privacy-preserving learning aligned with connected mobility and geographically distributed data sources (ClusterFrequency: anomaly detection = 555; federated learning = 243).

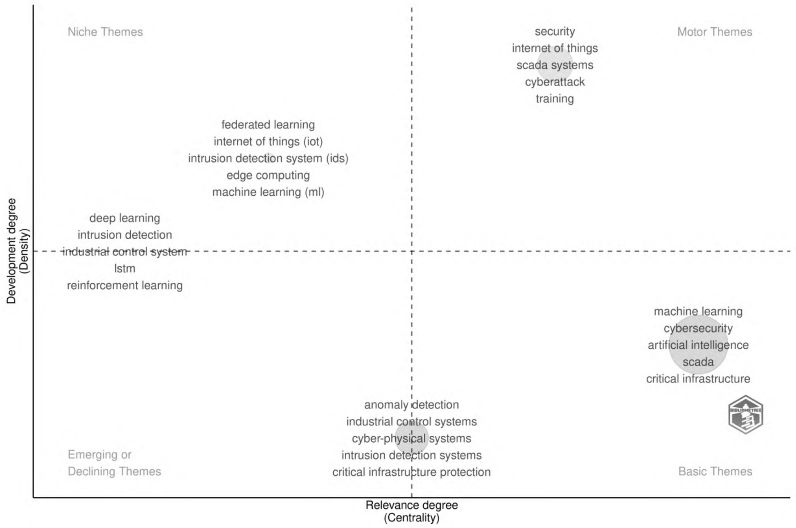


Figure 4. Thematic Map of the Transport sector

3.1.3. Water Sector The Water sub-corpus shows a compact but coherent landscape emphasis (Fig. 5), with anomaly detection and machine learning anchored around industrial control systems and water distribution contexts. Notably, the presence of an explainable AI (XAI) cluster suggests increasing emphasis on interpretability and operator trust, alongside a separate IoT-related security signal.

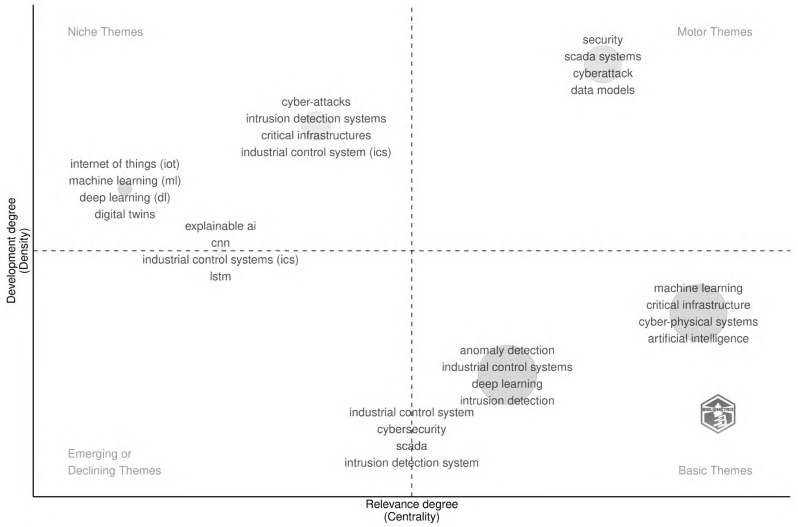


Figure 5. Thematic Map of the Water sector

3.2. Methodological robustness and limitations. To characterize the robustness of the thematic structure, **Callon centrality and density** are used, which reflect the relevance of the topic to the field and its internal cohesion, respectively. Themes with high centrality and density are interpreted as well-developed and influential, whereas low centrality/low-density themes are considered emerging or declining and should be treated cautiously. Sensitivity to preprocessing and threshold choices (e.g., keyword normalization and minimum frequency) further supports interpreting the results as high-level conceptual patterns rather than definitive taxonomies.

This study integrates PRISMA-guided dataset accounting with bibliometric science mapping in bibliometrix/biblioshiny [2], ensuring transparent retrieval, screening, merging, and deduplication, while thematic mapping characterizes the conceptual structure of the final corpus. Nevertheless, several methodological limitations should be noted. First, the reliability of co-word thematic mapping is bounded by metadata quality and database/export coverage (e.g., inconsistent or missing Author Keywords/abstracts across Scopus and Web of Science), which can affect term frequencies and cluster composition. Second, thematic structures are sensitive to analysis settings (field selection, Louvain clustering, and minimum-frequency thresholds); therefore, clusters should be interpreted as high-level, reproducible signals rather than definitive taxonomies. Third, deduplication performed primarily via DOI (supported by title-based matching when DOI is missing) may leave residual duplicates or merge near-duplicate records. Finally,

sector stratification relied on rule-based multi-label tagging over TI+AB+DE, which may introduce false positives/false negatives when sector context is implicit or expressed using non-standard vocabulary; the 2020 split is an analytic contrast point and may mask earlier or later waves of emergence.

4. CONCLUSION

Using a bibliometric dataset of 1,862 documents, this study investigates the evolution of AI-based cybersecurity across critical infrastructure sectors. While anomaly detection remains a universal baseline, AI strategies are increasingly sector-specific: the Energy sector focuses on countering physics-aware attacks (e.g., False Data Injection), the Transport sector emphasizes decentralized, privacy-preserving models (Federated Learning), and the Water sector highlights the need for Explainable AI (XAI) to ensure operator trust. Future research will focus on bridging gaps in the Water and Transport sectors through the development of interpretable AI models suitable for resource-constrained edge devices, thereby strengthening the resilience of distributed Industrial IoT and cyber-physical systems against adversarial AI threats.

Data availability. The full deduplicated dataset (n = 1,862), sector labels, and derived bibliometric tables are available at: https://github.com/tslavov-git/Bibliometric-Analysis

References

[1] Aminu, M., Akinsanya, A., Oyedokun, O., and Akinwande, O. T. (2024). A review of advanced cyber threat detection techniques in critical infrastructure: Evolution, current state, and future directions. *International Journal of Computer Applications Technology and Research*, 13(8), 74–87. https://www.irejournals.com/paper-details/1706103.

[2] Aria, M., and Cuccurullo, C. (2017). bibliometrix: An R-tool for comprehensive science mapping analysis. *Journal of Informetrics*, 11(4), 959–975. https://doi.org/10.1016/j.joi.2017.08.007.

[3] Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., et al. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ*, 372, n71. https://doi.org/10.1136/bmj.n71.

[4] Zolanvari, M., Teixeira, M. A., Gupta, L., Khan, K. M., and Jain, R. (2019). Machine learning-based network vulnerability analysis of industrial internet of things. *IEEE Internet of Things Journal*, 6(4), 6822–6834. https://doi.org/10.1109/JIOT.2019.2912020.

МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2026
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2026
Proceedings of the Fifty-Fifth Spring Conference
of the Union of Bulgarian Mathematicians
Tryavna, Bulgaria, April 5–9, 2026

EVALUATING SYSTEMATIC LINGUISTIC REASONING IN LARGE LANGUAGE MODELS VIA LINGUISTICS OLYMPIAD PROBLEMS

Tsvetelina Stefanova, Tsvetozar Georgiev
Department of Computer Systems and Technologies,
Angel Kanchev University of Ruse, Bulgaria
e-mails: tsstefanova@uni-ruse.bg, tgeorgiev@ecs.uni-ruse.bg

Current evaluation benchmarks for large language models often conflate genuine reasoning ability with memorization and statistical pattern matching. As a result, high benchmark scores do not necessarily indicate the capacity to induce abstract rules or to reason systematically from limited data. In this paper, we propose a methodological framework for evaluating linguistic reasoning in large language models based on problems from international and national linguistics olympiads. These problems are designed to be solvable without prior knowledge of the target language, requiring instead the induction of formal linguistic rules from small, self-contained datasets. We formalize linguistics olympiad problems as closed-world reasoning tasks and introduce a structured evaluation protocol that combines answer correctness, reasoning quality, hallucination detection, and generalization analysis.

Keywords: large language models, linguistic reasoning, rule induction, evaluation methodology, linguistics olympiads

ОЦЕНЯВАНЕ НА СИСТЕМАТИЧНОТО ЛИНГВИСТИЧНО РАЗСЪЖДЕНИЕ В ГОЛЕМИ ЕЗИКОВИ МОДЕЛИ ЧРЕЗ ЗАДАЧИ ОТ ЛИНГВИСТИЧНИ ОЛИМПИАДИ

Цветелина Стефанова, Цветозар Георгиев
Катедра „Компютърни системи и технологии“,
Русенски университет „Ангел Кънчев“, България
e-mails: tsstefanova@uni-ruse.bg, tgeorgiev@ecs.uni-ruse.bg

Съществуващите методи за оценяване на големи езикови модели често смесват способността за разсъждение с механично възпроизвеждане на статистически зависимости, което затруднява разграничаването между истинско логическо извеждане и

https://doi.org/10.55630/mem.2026.55.134-149
2020 Mathematics Subject Classification: 68T50, 68T01, 91F20.

запаметяване. В статията се предлага методологична рамка за оценяване на лингвистичното разсъждение в големи езикови модели чрез задачи от международни и национални олимпиади по лингвистика. Тези задачи са конструирани така, че да бъдат решавани без предварителни знания за съответния език и изискват извеждане на абстрактни езикови правила от ограничен набор данни. Оценяването се основава на съчетание от коректност на отговора, качество на аргументацията, наличие на халюцинации и способност за обобщение.

Ключови думи: големи езикови модели, лингвистично разсъждение, извеждане на правила, методология за оценяване, олимпиади по лингвистика

1. Introduction

The rapid evolution of Large Language Models (LLMs) has led to near-human performance on standard Natural Language Processing (NLP) benchmarks. However, a critical question remains: do these models exhibit genuine systematic reasoning, or do they merely rely on approximate retrieval from vast training corpora?

Current evaluation paradigms face a significant challenge known as "epistemic contamination" or data leakage. As noted by Lin et al. [8] in KUMO, publicly released benchmarks are often inadvertently subsumed into training data, rendering them unreliable as tests of novel reasoning. Furthermore, standard benchmarks such as MMLU (Massive Multitask Language Understanding) or GLUE (General Language Understanding Evaluation) conflate linguistic competence (latent knowledge of grammar) with performance (the application of that knowledge), a distinction highlighted by Waldis et al. in the Holmes benchmark [15]. To truly assess an LLM's inductive logic, we require a "closed-world" evaluation environment where success depends solely on in-context learning rather than prior world knowledge.

Linguistics olympiad problems—Rosetta-Stone-style puzzles requiring the decipherment of unseen languages—offer an ideal testbed for this purpose. Unlike translation tasks that benefit from massive pre-training on high-resource languages, linguistics olympiad problems are designed to be solvable without external knowledge, relying instead on meta-linguistic awareness and logical deduction [12].

While recent initiatives have begun to explore this domain, existing methodologies remain fragmented. LingOly [1] and Linguini [13] have established valuable datasets for low-resource languages, demonstrating that LLMs struggle with "language-agnostic" generalization. However, these benchmarks largely rely on exact-match accuracy metrics, which fail to capture the reasoning process. As shown by Bhattacharya et al. [2] in their analysis of counting systems, LLMs often achieve correct answers via pattern matching while failing to induce the underlying compositional operators (e.g., multiplication in base-20 systems), suggesting a disconnect between output correctness and logical faithfulness.

In this paper, we introduce a rigorous, research-grade framework for evaluating systematic linguistic reasoning. Building on the agentic insights of LingBench++ [7] and the reasoning critiques of CriticBench [9], we propose a multi-dimensional evaluation protocol. Our methodology goes beyond surface-level accuracy to evaluate Reasoning

Transparency, Hallucination Rates, and the Generalization Gap between seen and unseen linguistic structures. By formalizing these metrics, we aim to provide a standardized instrument for measuring the transition of LLMs from stochastic parrots to systematic reasoners.

2. Related Work

Current evaluation paradigms for Large Language Models can be broadly categorized into knowledge-intensive benchmarks, general reasoning suites, and specialized linguistic challenges. Our proposed framework addresses the gaps at the intersection of these fields.

2.1 From Knowledge Retrieval to Rule Induction

Standard benchmarks such as MMLU and GLUE primarily evaluate an LLM's ability to retrieve information seen during pre-training. However, distinguishing between memorization (approximate retrieval) and generalization (rule application) remains a fundamental challenge. [12] was among the first to propose Rosetta-Stone-style puzzles as a proxy for low-shot learning, establishing that these tasks require "meta-linguistic awareness" rather than semantic knowledge. More recently, the authors of LingOly [1] expanded this domain by compiling over 90 low-resource languages (e.g., Nivkh, Burushaski). Their findings demonstrate that model performance degrades significantly on "unseen" languages, suggesting that high performance on major languages is often an artifact of data contamination rather than genuine inductive capability. Similarly, Linguini [13] and IOLBENCH [4] have formalized these problems into "language-agnostic" benchmarks, yet they largely retain Exact Match (EM) or Character n-gram F-score (chrF) accuracy as the sole metric for success. While LingOly and Linguini focus on low-resource generalization, other datasets have targeted the structural diversity of these problems. MODELING [3] allows for finer-grained evaluation of specific linguistic reasoning skills, though it focuses on easier, author-constructed problems. Conversely, Majmudar & Filatova [10] explore the generative capabilities of models, demonstrating that while LLMs can solve complex puzzles, they still struggle to generate novel, solvable linguistic problems, highlighting a gap between passive solving and active design.

2.2 The Evaluation Gap: Accuracy vs. Faithfulness

A critical limitation of current benchmarks is the assumption that a correct answer implies correct reasoning. CriticBench [9] reveals that LLMs frequently generate "hallucinated reasoning"—sound-looking but logically invalid explanations that fortuitously arrive at the correct label. This phenomenon is particularly acute in compositional tasks. Bhattacharya et al. [2] demonstrated in their study of counting systems that while LLMs can memorize number sequences (e.g., "uno, dos, tres"), they fail to induce the underlying mathematical operators (e.g., Base-20 multiplication) unless explicitly prompted with symbols. This finding underscores the necessity of our proposed Reasoning Quality metric: an evaluation framework must verify the derivation of the rule, not just the final output.

2.3 Theoretical Grounding: Competence vs. Performance

Our methodology is grounded in the distinction between Linguistic Competence (latent grammatical knowledge) and Performance (the ability to use it), as explored in

Holmes [15]. While Holmes uses probing classifiers to assess latent knowledge, our framework focuses on the application of that knowledge in a few-shot setting. Furthermore, we draw on KUMO [8] to justify our "Generative Evaluation" approach. Lin et al. argue that static benchmarks become contaminated the moment they are released; thus, a robust evaluation protocol must rely on "closed-world" problems where the rules are self-contained within the prompt, mimicking the "Unseen" conditions of valid psychometric testing.

2.4 Agentic and Multi-Step Reasoning

Finally, the transition from prompt-based solvers to agentic architectures represents the state-of-the-art in this domain. LingBench++ [7] introduced a "Check-of-Thought" framework where separate agents generate and verify linguistic hypotheses. While effective, LingBench++ focuses on measuring the performance boost provided by agents. In contrast, our paper proposes using similar multi-step protocols as a measurement instrument—using the divergence between "Direct-Shot" and "Agentic-Verified" performance to quantify a model's Self-Correction Capability, a key indicator of robust reasoning.

3. Methodology

3.1 Problem Selection and Scope

To evaluate systematic linguistic reasoning in LLMs, we choose problems exclusively from official linguistics olympiads, including the International Linguistics Olympiad (IOL), the North American Computational Linguistics Olympiad (NACLO), the UK Linguistics Olympiad (UKLO), and selected national competitions. These sources are chosen because their problems are carefully designed, verified by expert linguists, and accompanied by official solutions. Only problems with publicly available solutions are included, ensuring reproducibility and verifiability.

To prevent model performance from reflecting memorization rather than reasoning, tasks satisfy two strict inclusion criteria:

1. **Unseen / Anti-Contamination:** Target languages must fall below a "digital poverty" threshold, favoring low-resource, extinct, or isolated languages (e.g., Nivkh, Burushaski, Sumerian). This ensures that models cannot rely on pre-training exposure to solve the problems [1, 5].
2. **Closed-World / Self-Containment:** Each problem is solvable solely from the problem statement; any reference to external knowledge constitutes hallucination [9].

Each problem is manually annotated by its dominant linguistic phenomenon. The benchmark covers six primary domains: morphology, phonology, syntax, semantics and pragmatics, writing systems and orthography, and historical/comparative linguistics. Problems may involve multiple interacting phenomena and are labeled accordingly.

To avoid bias toward specific linguistic structures, the dataset is typologically stratified across three cognitive domains [2]:

- **Morphological Induction:** segmentation of agglutinative or polysynthetic words.

- **Syntactic Alignment:** inference of non-English word orders (e.g., VSO, OVS) or ergative-absolutive systems.
- **Compositional Systems:** recursive numerical or kinship systems requiring multi-step arithmetic or rule application.

Problems are further stratified into three difficulty levels—*Introductory*, *Intermediate*, and *Advanced*—based on olympiad round, number of inference steps, and ambiguity. Introductory problems involve single rules and few examples, intermediate problems require combining several rules, and advanced problems demand high-level abstraction and reasoning under incomplete data.

3.2 Dataset Structure

All problems are stored in a standardized schema (Table 1), including:

- **Problem ID:** unique identifier encoding olympiad, year, problem number.
- **Source Metadata:** olympiad name, year, round, original language.
- **Phenomenon Labels:** one or more linguistic categories.
- **Difficulty Level:** Introductory, Intermediate, or Advanced.
- **Problem Statement:** verbatim text including tables, scripts, examples.
- **Input–Output Pairs:** structured representations of linguistic examples.
- **Question Targets:** explicit outputs required from the model (e.g., translations, forms, rules).
- **Gold Solution:** official solution with final answers and reasoning steps.
- **Evaluation Type:** exact-match, partial credit, or rubric-based evaluation.

The dataset is stored in a machine-readable format (JSON) while preserving human-readable statements for qualitative analysis. Problems are grouped hierarchically by domain and difficulty. To minimize contamination, recent problems are reserved for evaluation, and a challenge problem set with rare languages or unusual systems is designed to test generalization.

3.3 Prompting and Inference Protocol

Models are evaluated using a fixed prompting protocol to ensure comparability. Each prompt includes the original problem statement preceded by a standardized instruction:

> "Solve the following linguistics problem. Explain your reasoning step by step and provide the final answer clearly."

No additional examples are provided. Non-ASCII scripts are preserved. Inference parameters (temperature, max output length) are fixed.

To differentiate pattern matching from structured reasoning, two computational conditions are defined [7, 11, 16]:

1. **Baseline / Monolithic Chain-of-Thought:** single-pass "Field Linguist" prompt enforcing a linear chain-of-thought.
2. **Agentic Check-of-Thought Loop:** decomposed into specialized agents (Grammar Induction, Consistency Checker, Solver) for iterative verification.

Table 1: Benchmark Dataset Schema

Field	Description	Type
Problem ID	Unique identifier encoding olympiad, year, and problem number	String
Olympiad Source	IOL, NACLO, UKLO, or national olympiad	Categorical
Year	Year of publication	Integer
Round	Contest round (e.g., preliminary, final)	Categorical
Linguistic Domain	Morphology, phonology, syntax, semantics, orthography, historical	Multi-label categorical
Difficulty Level	Introductory / Intermediate / Advanced	Ordinal
Language(s)	Target language(s) or scripts involved	String / List
Problem Statement	Original problem text (verbatim)	Text
Data Examples	Input–output linguistic examples	Structured text
Question Targets	Required outputs (translations, forms, rules)	Text
Gold Answer	Official final answer	Text
Gold Reasoning	Official solution explanation	Text
Evaluation Type	Exact-match / Partial / Rubric-based	Categorical

3.4 Evaluation Metrics

LLM performance is measured along three dimensions: answer accuracy, reasoning quality, and generalization/hallucination. Additional metrics from literature (A_{surf}, R_{faith}, $SLRS$) are provided for conceptual grounding [9, 13].

3.4.1 Problem-Level Accuracy

Problem-Level Accuracy serves as the primary quantitative metric for assessing model performance, measuring the correspondence between the model's generated answers and the ground-truth solutions provided in the linguistics olympiad datasets. Unlike reasoning metrics, this measure focuses strictly on the correctness of the final output (the "performance" aspect of the competence-performance distinction). Let $P = \{p_1, \ldots, p_N\}$ denote the benchmark problem set. For each problem p_i, the model generates output y_i compared against the gold solution y_i^*.

For problems with a single deterministic answer, correctness is defined through an indicator function:

$$A_i = \mathbb{I}(y_i = y_i^*) \tag{1}$$

where $\mathbb{I}(\cdot)$ equals 1 when the prediction exactly matches the reference and 0 otherwise. This exact-match criterion ensures objective scoring for discrete outputs such as translations or morphological forms.

For multi-part problems, scoring is decomposed to account for structured responses:

$$A_i = \sum_{j=1}^{k_i} w_{ij} \cdot \mathbb{I}(y_{ij} = y_{ij}^*) \tag{2}$$

where k_i is the number of components and w_{ij} is normalized weight. This formulation captures partial correctness without overvaluing trivial sub-items.

Interpretation of accuracy must remain cautious. Correct outputs may arise from superficial pattern matching rather than genuine rule induction, meaning accuracy reflects behavioral agreement rather than validated reasoning. To reduce evaluation noise, normalization procedures are applied before comparison, resolving orthographic variation, formatting differences, or equivalent symbolic representations.

Aggregate benchmark accuracy is computed as:

$$A_{\text{avg}} = \frac{1}{N} \sum_{i=1}^{N} A_i \tag{3}$$

and serves as a descriptive baseline for performance reporting and stratified analysis across problem types or difficulty levels. Within the broader framework, Problem-Level Accuracy underpins composite scoring and generalization analysis, providing the measurable outcome layer that anchors subsequent multidimensional evaluation of linguistic reasoning.

3.4.2 Reasoning Quality Score

Problem-Level Accuracy does not reveal whether correct outputs are supported by valid linguistic reasoning. In linguistics olympiad problems, correct answers may result from superficial pattern matching or partial memorization. To address this limitation, we introduce a Reasoning Quality Score (R_i) that evaluates the extent to which models explicitly induce and apply rules from the provided data.

Explanations generated by models are evaluated by expert annotators using a standardized scoring rubric (Table 2), yielding a score $R_i \in [0, 1]$ for each problem instance. Let M denote the number of annotators. The final reasoning score is computed as:

$$R_i = \frac{1}{M} \sum_{m=1}^{M} r_{im}, \tag{4}$$

where r_{im} is the score assigned by annotator m to problem p_i.

The rubric assesses logical coherence, empirical grounding, completeness of rule systems, and consistency of application. High scores reflect explicit hypothesis formation, systematic testing, and principled abstraction, while lower scores indicate descriptive, incomplete, or unsupported reasoning.

Annotators follow detailed guidelines and participate in calibration sessions to ensure scoring consistency across domains and difficulty levels. The Reasoning Quality Score enables identification of cases in which high accuracy is achieved through invalid reasoning and supports comparisons between prompting strategies and model architectures.

Although based on human evaluation, the formalized criteria provide a foundation for future automated assessment methods.

3.4.3 Composite Problem Score

To integrate surface-level correctness and reasoning validity into a unified evaluation signal, we define a Composite Problem Score (S_i) for each problem instance p_i:

$$S_i = \alpha A_i + (1 - \alpha) R_i, \quad \alpha = 0.7 \tag{5}$$

where A_i denotes Problem-Level Accuracy and R_i denotes the Reasoning Quality

Table 2: Scoring Rubric for Reasoning Quality

Score	Descriptor	Criteria
1.0	Fully correct	Correctly infers all relevant linguistic rules; reasoning is logically coherent, complete, and strictly grounded in the provided data; final answer follows unambiguously from the explanation.
0.75	Largely correct	Core linguistic rules correctly identified, minor omissions or imprecision; reasoning mostly coherent and leads to a correct solution.
0.50	Partially correct	Some correct insights or sub-rules identified, overall rule system incomplete or inconsistently applied.
0.25	Flawed	Substantial errors or unsupported assumptions; explanation poorly aligned with problem statement.
0.00	Invalid / Absent	No meaningful reasoning, explanation incorrect or irrelevant.

Score.

This formulation reflects that correct outputs are necessary but insufficient indicators of systematic reasoning. The weighting parameter $\alpha = 0.7$ prioritizes answer correctness while preserving a substantial contribution from explanatory quality.

The composite score penalizes superficial pattern matching and distinguishes partial understanding from complete failure. Dataset-level performance is summarized as:

$$S_{\text{avg}} = \frac{1}{N} \sum_{i=1}^{N} S_i \tag{6}$$

where N is the number of problems in the dataset.

Aggregate scores are interpreted together with domain-specific and difficulty-stratified results. The metric also supports cross-condition analyses and sensitivity studies in which α is varied to examine alternative evaluation priorities.

3.4.4 Generalization and Hallucination

Systematic linguistic reasoning requires both reliable generalization and adherence to closed-world constraints. We therefore introduce complementary metrics for generalization and hallucination.

Generalization Gap

Let P_s denote the set of structurally familiar (seen) instances within problems, and P_u denote held-out or structurally novel (unseen) instances. The Generalization Gap is defined as:

$$\Delta G = S_{\text{avg}}(P_s) - S_{\text{avg}}(P_u) \tag{7}$$

where $S_{\text{avg}}(\cdot)$ represents the mean Composite Problem Score over the corresponding subset.

Small values of ΔG indicate stable abstraction and rule transfer, whereas large values suggest reliance on memorization or shallow heuristics. Domain-specific gaps ΔG_d can also identify particularly challenging linguistic phenomena.

Hallucination Rate

While generalization measures extrapolative competence, the Hallucination Rate quantifies violations of the closed-world assumption. For each problem p_i, a binary indicator h_i is defined:

$$h_i = \begin{cases} 1 & \text{if external or unverifiable information is present,} \\ 0 & \text{otherwise.} \end{cases}$$

The Hallucination Rate is:

$$H = \frac{1}{N} \sum_{i=1}^{N} \mathbb{I}(h_i = 1) \tag{8}$$

Hallucinations include references to external linguistic knowledge not inferable from the problem statement. Detection is performed by trained annotators using standardized procedures. Low values of H indicate epistemic discipline, while high values reflect dependence on memorized priors. Low hallucination rates alone, however, do not guarantee high reasoning quality.

Joint Interpretation

Generalization and hallucination metrics are interpreted jointly to characterize model behavior. Four typical regimes can be distinguished:

1. Low ΔG, Low H: Robust rule induction and disciplined reasoning.
2. Low ΔG, High H: Apparent generalization driven by external knowledge.
3. High ΔG, Low H: Faithful but brittle reasoning with limited abstraction.
4. High ΔG, High H: Reliance on heuristics and memorization.

This typology enables fine-grained diagnosis of model reasoning strategies and ensures that high performance reflects genuine inductive reasoning rather than opportunistic use of background knowledge.

3.4.5 Additional Metrics

In addition to the core metrics above, we incorporate complementary measures from prior computational linguistics and explainability research. These metrics function as diagnostic tools rather than primary benchmarks, enabling comparison with established evaluation traditions and providing additional interpretative signals.

One such measure is **Surface Form Accuracy ($A_{\mathbf{surf}}$)**, computed using character-level n-gram overlap (chrF++ [13]). This metric captures graded similarity between model outputs and gold references, particularly in problems involving transliteration, inflection, or multi-token outputs where strict exact matching may be overly rigid. While not a substitute for problem-level correctness, it reflects structural correspondence at a subword level.

A second auxiliary measure is **Reasoning Faithfulness ($R_{\mathbf{faith}}$)**, assessed through rubric-guided evaluation of intermediate reasoning traces. This score reflects the extent to which explanations remain grounded in the provided data and logically support the final answer, helping distinguish valid inference from post hoc rationalization.

To combine these auxiliary dimensions, we define the **Strict Linguistic Reasoning Score (SLRS)**:

$$SLRS = (1 - H) \cdot [\alpha A_{\text{surf}} + (1 - \alpha) R_{\text{faith}}], \quad \alpha = 0.6 \tag{9}$$

where H denotes the hallucination rate. This formulation ensures that high scores require structural similarity, faithful reasoning, and absence of unsupported inferences.

Overall, these optional metrics enrich diagnostic analysis and support fine-grained model comparison, while the primary evaluation remains grounded in accuracy, reasoning quality, and generalization performance.

3.5 Human Baselines and Inter-Rater Reliability

To contextualize model performance, we establish human baselines using solutions produced by trained linguistics students and former olympiad participants. These individuals possess explicit experience with rule-induction tasks and serve as an upper-bound reference for systematic reasoning under the same informational constraints imposed on the models [11, 12]. Human solvers are provided with the identical problem statements and are instructed to produce both final answers and step-by-step reasoning, mirroring the model evaluation protocol.

Multiple expert annotators independently evaluate a stratified subset of model outputs covering all linguistic domains and difficulty levels. Each annotator assigns a reasoning quality score according to the rubric in Table 2, without access to the model identity or other evaluators' scores. Inter-rater agreement is quantified using Cohen's κ for pairwise agreement and Krippendorff's α for multi-annotator settings. High agreement scores indicate that the rubric yields stable and reproducible judgments, mitigating subjectivity in reasoning evaluation.

In addition, human performance can be compared to model outputs in terms of error types and reasoning completeness, providing insight into which linguistic phenomena are inherently challenging versus those where models systematically fail. This dual analysis enables a nuanced understanding of the reasoning gap between humans and LLMs [8].

3.6 Error Analysis

Beyond aggregate metrics, a detailed qualitative error analysis should be conducted to identify systematic failure modes in LLM reasoning. Errors are manually categorized into four primary types:

1. **Incorrect Rule Induction:** The model proposes coherent but empirically unsupported linguistic rules (e.g., misgeneralizing a morphological suffix).
2. **Failure to Apply a Correct Rule:** The model identifies the relevant pattern but applies it inconsistently or incompletely, leading to partially correct answers.
3. **Misinterpretation of Problem Constraints:** Errors arise from overlooking explicit restrictions, misreading examples, or misprocessing linguistic problem formatting.
4. **Language-Specific Misinterpretation:** Failures stem from unfamiliar scripts, morphological complexity, or typological features absent from high-resource training data [6, 14].

Representative examples from each category are to be presented to illustrate the

model's reasoning limitations. This analysis serves two purposes: it distinguishes between superficial pattern matching and deeper linguistic reasoning failures, and it identifies which domains (e.g., morphology, syntax, compositional systems) pose the greatest challenge.

Error analysis also informs potential improvements in prompting strategies, agentic verification loops, and model fine-tuning [7].

3.7 Statistical Analysis

Quantitative results are reported using descriptive statistics, including mean composite scores, standard deviations, and confidence intervals, computed separately for each linguistic domain and difficulty level. For comparisons between model variants under matched problem conditions, non-parametric paired tests are employed, such as the Wilcoxon signed-rank test, which do not assume normality and are suitable for ordinal or bounded metrics like reasoning quality [9].

For multiple comparisons, p-values are adjusted using Bonferroni or Holm-Bonferroni corrections to control family-wise error. Effect sizes (e.g., Cohen's d or Cliff's delta) are reported alongside significance to quantify the magnitude of observed differences. Statistical analysis also examines correlations between problem difficulty, linguistic domain, and error types, highlighting systematic patterns in model reasoning capabilities.

Where possible, visualization of performance distributions, error frequencies, and reasoning scores provides an intuitive complement to numerical analysis, enhancing interpretability for both human and computational audiences.

3.8 Reproducibility, Limitations, and Ethical Considerations

Reproducibility is a central design goal. All benchmark problems, prompts, scoring rubrics, and annotation guidelines are released alongside evaluation code. Model versions, inference parameters, and random seeds are explicitly documented to allow exact replication of reported results [4]. Anonymized human annotation data and inter-rater agreement statistics are provided to support independent verification.

Despite these precautions, several limitations persist:

- **Training Data Contamination:** Some olympiad problems or solutions may be publicly available online, making full elimination of pre-training leakage challenging.
- **Reasoning vs. Pattern Matching:** The rubric-based evaluation improves interpretability, but distinguishing genuine multi-step reasoning from sophisticated pattern matching is inherently imperfect [8, 11].
- **Coverage Bias:** Certain linguistic traditions or problem styles may be underrepresented, biasing evaluation toward particular reasoning strategies.

Ethically, the benchmark avoids personal or sensitive data. Care is taken to include typologically diverse languages, scripts, and low-resource systems, mitigating language and cultural biases. The methodology is intended to complement existing NLP evaluation paradigms, providing a linguistically grounded perspective on systematic reasoning in LLMs [1, 2].

4. Benchmark Usage and Evaluation Protocol

This section specifies how the proposed benchmark and evaluation framework are intended to be used in future studies. As this work presents a methodological proposal rather than an empirical evaluation, the focus is on defining standardized usage scenarios, interpretation guidelines, and reporting conventions. The benchmark is conceived as a diagnostic instrument for linguistic reasoning, not as a leaderboard-oriented performance test.

4.1 Intended Evaluation Scenarios

The proposed framework is designed to support multiple evaluation scenarios that correspond to distinct research questions about systematic linguistic reasoning in large language models.

First, the benchmark enables controlled comparisons between different prompting and reasoning protocols. Researchers may contrast direct, single-pass prompting with structured multi-step or agentic approaches, as defined in Section 3.3. Because all problems satisfy the closed-world requirement, differences in performance can be attributed to reasoning strategy rather than access to external knowledge.

Second, the benchmark supports cross-model comparisons under fixed conditions. By holding the dataset, scoring metrics, and evaluation protocol constant, researchers can examine how architectural differences or training regimes affect rule induction and generalization, independent of memorized linguistic content.

Third, the framework is suitable for generalization studies. By separating training examples from structurally similar but unseen test items within each problem, researchers can analyze systematic generalization using the Generalization Gap metric defined in Section 3.4.

Crucially, the benchmark is not intended to measure broad linguistic competence. Instead, it isolates a narrow but theoretically meaningful capability: the induction and application of abstract linguistic rules from sparse, artificialized input.

4.2 Evaluation Procedure

To ensure reproducibility and comparability across studies, we define a standardized evaluation procedure governing problem presentation, model interaction, and score computation. Each evaluation run consists of four stages.

Problem Presentation. Each model is presented with a single linguistic problem instance comprising a set of training examples and one or more held-out test queries. No external tools, retrieval mechanisms, or linguistic resources are permitted. All information required to solve the problem must be contained within the prompt.

Reasoning Trace Generation. Models are instructed to produce both a final answer and an explicit reasoning trace. The reasoning trace is required for the computation of the Reasoning Quality Score and for detecting closed-world violations. Suppressing intermediate reasoning is therefore incompatible with the proposed evaluation framework.

Hallucination Detection. The reasoning trace is examined for references to real-world linguistic facts, typological generalizations, or external language knowledge. Any such reference constitutes a violation of the closed-world assumption and is recorded when computing the Hallucination Rate.

Score Computation. For each problem instance, Problem-Level Accuracy, Reasoning Quality Score, and the Composite Problem Score are computed as defined in Section 3.4. These scores jointly characterize both outcome correctness and the validity of the reasoning process.

4.3 Interpretation of Evaluation Metrics

The evaluation metrics proposed in Section 3.4 are intended to be interpreted jointly, as each captures a different aspect of model behavior.

Problem-Level Accuracy measures whether the model produces the correct output form, but does not provide insight into how the answer was derived. As shown in prior work, correct outputs may result from coincidental pattern matching or memorization rather than systematic reasoning.

The Reasoning Quality Score evaluates the internal coherence and data-consistency of the model's inferred rule system. High scores indicate explicit identification and consistent application of abstract rules, while low scores reflect heuristic or logically invalid reasoning, even when the final answer is correct.

The Composite Problem Score integrates these two dimensions, ensuring that surface correctness and reasoning validity are not evaluated in isolation. This composite measure is intended as the primary problem-level indicator within the framework.

Importantly, scores should be reported separately for different linguistic domains (morphological, syntactic, compositional), as aggregate values may obscure domain-specific reasoning failures.

4.4 Generalization and Hallucination Analysis

Beyond problem-level performance, the framework explicitly targets two systemic behaviors: generalization and hallucination.

The Generalization Gap quantifies the discrepancy between performance on structurally familiar instances and unseen test items. A large gap suggests reliance on surface-level associations rather than abstraction of underlying rules, particularly in compositional systems such as counting or kinship structures.

The Hallucination Rate captures the frequency with which models violate the closed-world assumption by introducing external linguistic knowledge. High hallucination rates indicate that apparent success may be driven by memorized typological facts rather than in-context learning.

Analyzing these metrics together allows researchers to distinguish between models that fail due to insufficient inductive capacity and those that succeed only by bypassing the intended reasoning constraints.

4.5 Reporting and Comparability Guidelines

To support meaningful comparison across studies, we recommend that future work using the proposed benchmark adhere to a standardized reporting format. At minimum,

researchers should report: (i) Problem-Level Accuracy, (ii) Reasoning Quality Score, (iii) Composite Problem Score, (iv) Generalization Gap, and (v) Hallucination Rate, disaggregated by linguistic domain.

Comparisons across fundamentally different evaluation setups—such as single-pass prompting versus agentic reasoning pipelines—should be accompanied by explicit discussion of the additional computational and structural assumptions involved.

These guidelines are intended to ensure that the benchmark functions as an interpretable evaluation instrument rather than as a single-number performance metric.

5. Conclusions and Future Work

In this work, we have proposed a benchmark and evaluation framework for assessing systematic linguistic reasoning in large language models. The methodology emphasizes problems derived from official linguistics olympiads, the preservation of a closed-world problem structure, and careful stratification across linguistic phenomena and problem difficulty. By integrating both problem-level correctness and reasoning quality metrics, the framework enables a nuanced assessment of model capabilities beyond surface-level accuracy.

Crucially, our benchmark is designed as a diagnostic tool rather than a competition leaderboard. It supports evaluation scenarios that isolate the effects of prompting strategies, architectural differences, and generalization ability under controlled conditions. The incorporation of explicit reasoning traces, hallucination detection, and domain-specific analysis ensures that performance reflects genuine inductive reasoning rather than memorization or pattern matching.

Looking forward, several avenues for future work emerge. First, the benchmark can be extended to include additional languages, scripts, and typological phenomena, particularly from under-represented linguistic families, to further stress-test compositional reasoning and cross-linguistic generalization. Second, agentic or multi-step evaluation protocols can be refined, potentially incorporating verification loops, analogical prompting, or self-correction mechanisms to study their impact on reasoning quality. Third, while the current framework relies on human-annotated reasoning scores, the development of automated or semi-automated reasoning evaluation tools could enhance scalability and reproducibility.

Finally, the benchmark opens opportunities for cross-disciplinary research, linking computational linguistics, cognitive science, and language pedagogy. By providing a standardized, linguistically grounded instrument for evaluating reasoning, this work lays the foundation for future studies that rigorously probe the capabilities and limitations of large language models in systematic, symbolic-like problem solving.

Acknowledgements

This research is supported by the Scientific Research Fund of "Angel Kanchev" University of Ruse, Bulgaria.

References

[1] A. Bean, S. Hellsten, H. Mayne, J. Magomere, E. A. Chi, R. Chi, S. A. Hale, and H. R. Kirk. 2024. LINGOLY: a benchmark of olympiad-level linguistic

reasoning puzzles in low-resource and extinct languages, *Proceedings of the 38th International Conference on Neural Information Processing Systems (NIPS '24)*, Vol. 37. Curran Associates Inc., Red Hook, NY, USA, Article 825, pp. 26224–26237, 2024. https://dl.acm.org/doi/10.5555/3737916.3738741

[2] A. R. Bhattacharya, I. Papadimitriou, K. Davidson, D. Alvarez-Melis, Investigating the interaction of linguistic and mathematical reasoning in language models using multilingual number puzzles, *Proceedings of the 2025 Conference on Empirical Methods in Natural Language Processing*, pp. 28322–28332, 2025, https://aclanthology.org/2025.emnlp-main.1438.pdf

[3] N. A. Chi, T. Malchev, R. Kong, R. A. Chi, L. Huang, E. A. Chi, R. T. McCoy, D. Radev, *Proceedings of the 6th Workshop on Research in Computational Linguistic Typology and Multilingual NLP (SIGTYP 2024)*, pp. 113–119, 2024, https://aclanthology.org/2024.sigtyp-1.14.pdf

[4] S. Goyal, S. Dan, IOLBENCH: Benchmarking LLMs on Linguistic Reasoning, *arXiv preprint arXiv:2501.04249*, 2025.

[5] J. Khouja, L. Yang, R. Kearns, K. Korgul, V. Neacsu, S. Hellsten, A. Bean, H. Mayne, A. Mahdi, LINGOLY-TOO: Disentangling Reasoning from Knowledge with Templatised Orthographic Obfuscation, *arXiv preprint arXiv:2503.02972*, 2025.

[6] J. Hwang, K. Tanmay, S.-J. Lee, A. Agrawal, P. P. Liang, H. Palangi, K. Ayush, Learn Globally, Speak Locally: Bridging the Gaps in Multilingual Reasoning, *arXiv preprint arXiv:2507.05418*, 2025.

[7] D.-C. Lian, R.-S. Huang, P.-E. Chen, C. Lim, Y.-K. Lin, G.-Y. Tseng, T.-C. Yang, Z.-Y. Lin, P.-C. Chen, S.-K. Hsieh, LingBench++: A Linguistically-Informed Benchmark and Reasoning Framework for Multi-Step and Cross-Cultural Inference with LLMs, *arXiv preprint arXiv:2507.16809*, 2025.

[8] H. Lin, X. Wang, R. Yan, B. Huang, H. Ye, J. Zhu, Z. Wang, J. Zou, J. Ma, Y. Liang, Generative Evaluation of Complex Reasoning in Large Language Models (KUMO), *arXiv preprint arXiv:2504.02810*, 2025.

[9] Z. Lin, Z. Gou, T. Liang, R. Luo, H. Liu, Y. Yang, CRITICBENCH: Benchmarking LLMs for Critique-Correct Reasoning, *Findings of the Association for Computational Linguistics: ACL 2024*, pp. 1552–1587, 2024, https://aclanthology.org/2024.findings-acl.91.pdf

[10] N. Majmudar, E. Filatova, Can LLMs Solve and Generate Linguistic Olympiad Puzzles?, *Proceedings of the 2025 Conference on Empirical Methods in Natural Language Processing*, pp. 19163–19200, 2025, https://aclanthology.org/2025.emnlp-main.969.pdf

[11] R. Ramji, K. Ramji, Inductive Linguistic Reasoning with Large Language Models, *Findings of the Association for Computational Linguistics: ACL 2025*, pp. 22783–22810, 2025, https://aclanthology.org/2025.findings-acl.1171.pdf

[12] G. G. Sahin, Y. Kementchedjhieva, P. Rust, I. Gurevych, PuzzLing Machines: A Challenge on Learning From Small Data, *Proceedings of the 58th Annual Meeting of the Association for Computational Linguistics*, pp. 1241–1254, 2020, https://aclanthology.org/2020.acl-main.115.pdf

[13] E. Sánchez, B. Alastruey, C. Ropers, P. Stenetorp, M. Artetxe, M. R. Costa-jussà, Linguini: A Benchmark for Language-Agnostic Linguistic Reasoning,

arXiv preprint arXiv:2409.12126, 2024.

[14] Y.-F. Shih, Z.-L. Lin, S.-K. Hsieh, Reasoning Over the Glyphs: Evaluation of LLM's Decipherment of Rare Scripts, *arXiv preprint arXiv:2501.17785*, 2025.

[15] A. Waldis, Y. Perlitz, L. Choshen, Y. Hou, I. Gurevych, Holmes: A Benchmark to Assess the Linguistic Competence of Language Models, *Transactions of the Association for Computational Linguistics*, vol. 12, pp. 1616–1647, 2024, https://aclanthology.org/2024.tacl-1.88.pdf

[16] H. Zhu, Y. Liang, W. Xu, H. Xu, Evaluating Large Language Models for In-Context Learning of Linguistic Patterns in Unseen Low Resource Languages, *Proceedings of the First Workshop on Language Models for Low-Resource Languages (LoResLM 2025)*, pp. 414–426, 2025, https://aclanthology.org/2025.loreslm-1.31.pdf

СЕКЦИЯ В: ОБРАЗОВАНИЕ ПО МАТЕМАТИКА И ИНФОРМАТИКА

SECTION C: EDUCATION IN MATHEMATICS AND INFORMATICS

МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2026
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2026
Proceedings of the Fifty-Fifth Spring Conference
of the Union of Bulgarian Mathematicians
Tryavna, Bulgaria, April 5–9, 2026

ANALYSIS OF SELECTED MATHEMATICAL PROBLEMS IN SCHOOL EDUCATION

Ivaylo Dimitrov[1], Miroslav Hristov[2], Mehmed Kodzha[3]
[1] Nancho Popovich High School of Mathematics, Shumen, Bulgaria
[2] Shumen University, Shumen, Bulgaria
[3] Nancho Popovich High School of Mathematics, Shumen, Bulgaria
e-mails: [1]pmg.iv.dimitrov@abv.bg, [2]miroslav.hristov@shu.bg, [3]mkodzha@gmail.com

The process of composing mathematical problems is a key element of mathematics education, requiring a high degree of precision, logical consistency, and clarity of formulation. Nevertheless, in practice various types of inaccuracies are often encountered, which can hinder the correct understanding or solution of problems and, in some cases, even lead to incorrect results. This article presents a systematic analysis of inaccuracies occurring in the formulation and solution of mathematical problems. The study covers inaccuracies in problem statements (unclear or ambiguous conditions) as well as in mathematical content (logical inconsistencies and improperly formulated requirements). Through the analysis of specific examples, a classification of these inaccuracies is proposed and recommendations for their avoidance are offered. The results of the study aim to support teachers, methodologists, and authors of educational materials in creating higher-quality and pedagogically effective mathematical problems.

Keywords: mathematical problems, school education

АНАЛИЗ НА ПОДБРАНИ МАТЕМАТИЧЕСКИ ЗАДАЧИ В УЧИЛИЩНОТО ОБРАЗОВАНИЕ

Ивайло Димитров[1], Мирослав Христов[2], Мехмед Коджа[3]
[1,3]ППМГ „Нанчо Попович", Шумен, България,
[2] Шуменски университет, Шумен, България
e-mails: [1]pmg.iv.dimitrov@abv.bg, [2]miroslav.hristov@shu.bg, [3]mkodzha@gmail.com

Процесът на съставяне на математически задачи е ключов елемент от обучението по математика, който изисква висока степен на прецизност, логическа последователност и яснота на формулировките. Въпреки това, в практиката често се допускат различни видове неточности, които могат да затруднят правилното разбиране или

https://doi.org/10.55630/mem.2026.55.153-162
2020 Mathematics Subject Classification: 97D10, 97D99.

решаване на задачите, а в някои случаи да доведат и до некоректни решения. Настоящата статия представя систематичен анализ на допуснати неточности при съставяне и решаване на математически задачи. Изследването обхваща неточности във формулировката (неясни или двусмислени условия) и математическото съдържание (логически несъответствия, некоректно поставени изисквания). Чрез анализ на конкретни примери се прави класификация на неточностите и се предлагат препоръки за тяхното избягване. Резултатите от изследването имат за цел да подпомогнат учителите, методистите и авторите на учебни материали в създаването на по-качествени и педагогически ефективни математически задачи.

Ключови думи: математически задачи, училищно образование

1 Въведение

Математическите задачи са основен инструмент в процеса на обучение по математика, тъй като те не само проверяват знанията и уменията на учениците, но и стимулират логическото мислене, аналитичните способности и креативността. Въпреки централната им роля в образователния процес, съставянето на качествени математически задачи остава предизвикателство както за учителите, така и за авторите на учебни помагала.

Процесът на създаване на математически задачи е сложен и многостранен. Той изисква не само отлични познания в конкретната област на математиката, но и дълбоко разбиране на възрастовите, когнитивните и психологическите особености на учениците, както и ясно осъзнаване на конкретните образователни цели. В този контекст задачата не е просто средство за упражнение или контрол, а внимателно подбран и формулиран инструмент за изграждане на математическа грамотност.

Неточностите при формулирането на задачи могат да възникнат на различни етапи — от създаването на самата идея до нейното конкретно формулиране и проверка. Те могат да бъдат свързани с неточна или неясна математическа формулировка, двусмислие, липса на логическа последователност или несъответствие между въпрос и решение. Подобни неточности не само затрудняват учениците, но и могат да доведат до неразбиране на ключови математически понятия и до формиране на погрешни представи.

Неточностите при съставяне на задачи могат да окажат влияние и върху процеса на преподаване и оценяване. Те могат да подведат учителя при преценката на нивото на усвояване на знанията и да възпрепятстват ефективната обратна връзка.

Настоящата статия има за цел да анализира допуснати неточности при съставянето на математически задачи, да разгледа причините за тяхната поява и да предложи препоръки за тяхното избягване. Чрез този анализ се надяваме да допринесем за създаването на по-ефективни и педагогически издържани математически задачи, които да подпомагат учебния процес и да насърчават развитието на математическата култура у учениците.

В статията се изследват задачи със следните типове неточности:

- несъществуваща геометрична конфигурация;
- нарушено аналитично условие;
- непълна формулировка.

2 Задачи

В настоящата секция са представени и анализирани подбрани математически задачи, използвани в училищното образование и ученическите състезания по математика, в които се наблюдават различни видове неточности. Всеки пример е подбран с цел да онагледи типични пропуски и несъответствия във формулирането, съдържанието или методическата насоченост на задачата. Представените примери служат като основа за формулиране на изводи и препоръки към практиката на съставяне на задачи.

Чрез този анализ се цели не само да се посочат и коригират конкретни недостатъци, но и да се стимулира критичен подход към създаването на учебни задачи, с оглед повишаване на тяхната ефективност и педагогическа стойност.

2.1 Задачи с несъществуваща геометрична конфигурация

В тази подсекция се изследват две задачи.

Първата задача, която разглеждаме, е от учебник по ООП Математика за 9. клас от раздела за начален преговор.

Задача 1. [3] В правоъгълен триъгълник с хипотенуза 7 cm е вписана окръжност с радиус 2 cm. Намерете периметъра на триъгълника.

Решение. Предложеният отговор в [3] е 18 cm. Идеята на авторите е да се приложи формулата

$$r = \frac{a+b-c}{2} \tag{1}$$

за радиуса на вписаната окръжност в правоъгълен триъгълник. Заместваики $r = 2\ cm$ и $c = 7\ cm$, получаваме $2 = \frac{a+b-7}{2}$, откъдето $a + b = 11\ cm$. По този начин за периметъра на триъгълника получаваме $P = a + b + c = 11 + 7 = 18\ cm$. Както се вижда, задачата се решава лесно и не би представлявала трудност за учениците. Къде е проблемът?

Нека изследваме даденият правоъгълен триъгълник с хипотенуза 7 cm по-подробно. От Питагоровата теорема $a^2 + b^2 = c^2$ следва, че $b = \sqrt{49 - a^2}$. Заместваме в (1) и получаваме

$$r(a) = \frac{a + \sqrt{49 - a^2} - 7}{2}; \quad 0 < a < 7. \tag{2}$$

Функция (2) достига максимум при $a = \frac{7\sqrt{2}}{2}$ и

$$r_{max}\left(\frac{7\sqrt{2}}{2}\right) = \frac{7(\sqrt{2}-1)}{2}\ cm \approx 1,45\ cm. \tag{3}$$

Получената стойност в (3) показва, че максималният радиус на вписана окръжност в правоъгълен триъгълник с хипотенуза 7 cm е $r_{max} \approx 1,45\ cm$. Това доказва, че в такъв триъгълник не може да се впише окръжност с радиус 2 cm.

От друга страна, ако изследваме периметъра като функция на a, т.е.

$$P(a) = a + \sqrt{49 - a^2} + 7; \quad 0 < a < 7,$$

се оказва, че $P_{max}\left(\frac{7\sqrt{2}}{2}\right) = 7(\sqrt{2}+1)\ cm \approx 16,9\ cm$. Това означава, че максималният периметър на правоъгълен триъгълник с хипотенуза 7 cm е $7(\sqrt{2}+1)\ cm \approx 16,9\ cm < 18\ cm$.

Направена е корекция на условието на задачата в [4]. Новото условие изглежда така:

Коригирано условие. [4] В правоъгълен триъгълник с хипотенуза 5 cm е вписана окръжност с радиус 2 cm. Намерете периметъра на триъгълника.

Разликата с предишното условие е в дължината на хитотенузата на триъгълника. В този случай задачата отново не е коректна, понеже не съществува и такъв триъгълник. Тук най-големият радиус на вписаната окръжност е $r_{max} = \frac{5(\sqrt{2}-1)}{2} \approx 1,04\ cm$.

Втората задача е от учебник по профил математика за 12. клас от раздел "Екстремални задачи в равнината".

Задача 2. [5] Нека t е допирателната в точка C към описаната около $\triangle ABC$ окръжност, за който $\sphericalangle ACB = 120^0$ и лицето му е $\sqrt{3}$. Точките P и Q са от правата t, като $\sphericalangle PBC = \sphericalangle CBA$ и $\sphericalangle QAC = \sphericalangle CAB$ и нито една от тези две точки не е от AB. Намерете дължината на AB, за която периметърът на четириъгълника $ABPQ$ е най-малък.

Решение. В [5] са посочени следните отговори: $P_{ABPQ_{min}} = 4\sqrt{2}$ и $AB = \sqrt{2}$. Първо ще покажем как се получават тези резултати, след което ще изследваме по-подробно задачата за неточности.

Нека да направим следните означения: $BC = a$, $AC = b$, $AB = c$, $\sphericalangle CAB = \sphericalangle QAC = \alpha$ и $\sphericalangle CBA = \sphericalangle PBC = 60^0 - \alpha$. Лесно се изразяват останалите ъгли в $\triangle ACQ$ и $\triangle BCP$ (фиг. 1).

От $S_{ABC} = \sqrt{3} \Rightarrow ab = 4$ и от косинусовата теорема в $\triangle ABC$ получаваме

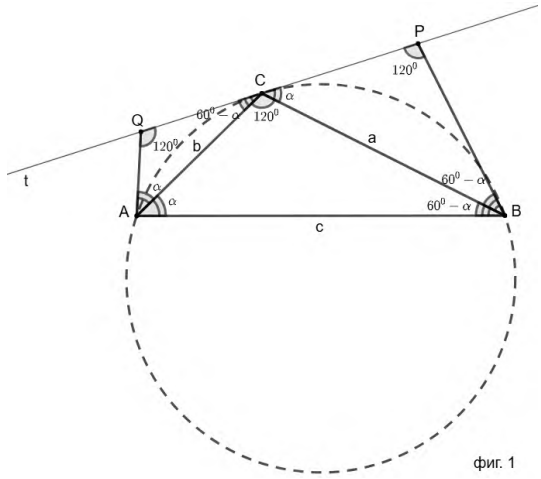
$$c^2 = a^2 + b^2 + 4. \tag{4}$$

Използвайки подобието $\triangle ABC \sim \triangle ACQ \sim \triangle BCP$, изразяваме всички страни на четириъгълника $ABPQ$ чрез страната $AB = c$ и за периметъра му получаваме

$$P_{ABPQ}(c) = \frac{2c^2 + 4}{c}, \quad c > 0. \tag{5}$$

Изследвайки (5), като функция на c, установяваме, че има единствена точка на екстремум $c = \sqrt{2}$, в която има минимум. Оттук за минималния периметър на $ABPQ$ получаваме $P_{ABPQ_{min}} = 4\sqrt{2}$. Това са и посочените отговори в [5].

Сега да направим задълбочен анализ на проблема. С непосредствена проверка,



заместваики $c = \sqrt{2}$ в (4), получаваме $a^2 + b^2 = -2$, което е невъзможно. Къде е проблемът?

Противоречието се дължи на това, че за да удовлетворява условията от задачата, страната $AB = c$ трябва да отговаря на определени критерии. Какви са те?

От $ab = 4$ и от известното неравенство $(a - b)^2 \geq 0$ получаваме

$$a^2 + b^2 \geq 8. \tag{6}$$

Заместваики (6) в (4), получаваме $c^2 \geq 12$, откъдето $c \geq 2\sqrt{3}$. Понеже (5) е растяща функция в $(\sqrt{2}; +\infty)$ и $2\sqrt{3} \in (\sqrt{2}; +\infty)$, то за най-малкият периметър на $ABPQ$ се получава $P_{ABPQ_{min}}(2\sqrt{3}) = \dfrac{14\sqrt{3}}{3}$ при $AB = c = 2\sqrt{3}$. Това е правилният отговор на задачата. Можем да заключим, че не е достатъчно изискването $c > 0$ в (5) и оценката $c \geq 2\sqrt{3}$ е критичен момент в решението на задачата, който задължително трябва да забележим. Това още веднъж потвърждава важността на допустимите стойности на променливата при изследване на функция за екстремуми.

Впрочем ако се състави функция на страната $BC = a$ или $AC = b$ на $\triangle ABC$ и се изследва за екстремум, не би се наложило да изискваме допълнителни условия за тях. Единственото изискване за тези страни е те да са строго положителни. По този начин най-малкият периметър би се получил в точките на минимум за тези функции.

2.2 Задачи с нарушено аналитично условие

В подсекция 2 се разглеждат две задачи.

Първата задача е от сборник за подготовка за Държавен зрелостен изпит по профил математика.

Задача 3. [1] Безкрайната сума $S = 1 + \dfrac{1}{cos150^0} + \dfrac{1}{cos^2150^0} + ... + \dfrac{1}{cos^n150^0} + ...$ е равна на:

А) $\sqrt{3}$ Б) $2\sqrt{3}-3$ В) $4-2\sqrt{3}$ Г) $1-\frac{\sqrt{3}}{2}$

Решение. Посоченият отговор в [1] е Б) $2\sqrt{3}-3$. Първо ще покажем как се получава този отговор.

От формулата

$$S=\frac{a_1}{1-q} \tag{7}$$

за сумата на безкрайно намаляваща геометрична прогресия с $a_1=1$ и $q=\frac{1}{cos150^0}=-\frac{2}{\sqrt{3}}$, получаваме $S=\frac{1}{1-\left(-\frac{2}{\sqrt{3}}\right)}=\frac{\sqrt{3}}{2+\sqrt{3}}=2\sqrt{3}-3$. Къде е проблемът?

Виждаме, че след директно заместване във формула (7) се получава предложеният отговор. Не е трудно да се забележи, че $\mid q \mid = \left|-\frac{2}{\sqrt{3}}\right| = \frac{2}{\sqrt{3}} > 1$, което нарушава условието за сходимост на безкрайна геометрична прогресия и ни лишава от правото да приложим формула (7).

Това, както и в Задача 1, още веднъж потвърждава факта, че не винаги директното заместване във формулите води до правилния резултат. Напротив, преди всичко първо е нужно да се уверим в коректността на условието, след което да се насочим към познатите формули, с помощта на които бихме достигнали до желания резултат.

Задача 3 е коригирана в [2] по следния начин:

Коригирано условие. [2] Безкрайната сума $S=1+cos150^0+cos^2150^0+...+cos^n150^0+...$ е равна на:

А) $\sqrt{3}$ Б) $4+2\sqrt{3}$ В) $4-2\sqrt{3}$ Г) $1-\frac{\sqrt{3}}{2}$

Новото условие е коректно, понеже $\mid q \mid = \left|-\frac{\sqrt{3}}{2}\right| = \frac{\sqrt{3}}{2} < 1$ и след прилагане на формула (7) се получава верният отговор $S=4-2\sqrt{3}$.

Втората задача в тази подсекция е от общинския кръг на Националната олимпиада по математика за 11. клас.

Задача 4. [6] Решете уравнението

$$\frac{1}{1}+\frac{1}{1+2}+\frac{1}{1+2+3}+...+\frac{1}{1+2+3+...+x}=\frac{2022}{2021}.$$

Първо ще представим авторското решение:

Решение. [6] Използвайки формулата $1+2+3+...+x=\frac{x(x+1)}{2}$ за лявата страна

на уравнението, то може да се запише във вида $\frac{1}{1}+\frac{2}{2.3}+\frac{2}{3.4}+...+\frac{2}{x(x+1)}=\frac{2022}{2021}$. След разделяне уравнението на 2, получаваме

$$\frac{1}{2}+\frac{1}{2.3}+\frac{1}{3.4}+...+\frac{1}{x(x+1)}=\frac{1011}{2021}. \tag{8}$$

Представяйки всяка една от дробите, в лявата страна на (8), във вида $\frac{1}{x(x+1)}=\frac{1}{x}-\frac{1}{x+1}$, свеждаме (8) до

$$1-\frac{1}{x+1}=\frac{1011}{2021}. \tag{9}$$

След решаване на (9) получаваме крайният отговор $x=\frac{1011}{1010}$.

Нека сега се задълбочим в предложеното решение. На пръв поглед задачата изглежда коректна. В условието обаче е пропуснато да се отбележи на кое множество принадлежи x, но не е трудно да се предположи, че $x \in \mathbb{N}$. При така полученото решение обаче $x \notin \mathbb{N}$. Но това означава, че лявата страна на уравнението няма смисъл. Това е достатъчно да направим извода, че условието не е коректно зададено. Всички събираеми в лявата страна са положителни, а дори сборът само на първите две е по-голям от дясната страна $\left(\frac{1}{1}+\frac{1}{1+2}=\frac{4}{3}>\frac{2022}{2021}\right)$. Това от своя страна също доказва некоректността на условието. Задачата би била смислена единствено ако крайният отговор $x \in \mathbb{N}$.

Едно коректно условие на задачата би изглеждало по следния начин:

$$\frac{1}{1}+\frac{1}{1+2}+\frac{1}{1+2+3}+...+\frac{1}{1+2+3+...+x}=\frac{4040}{2021}.$$

В общия случай, ако числото k е дясната страна на уравнението, то $k=\frac{2x}{x+1}$, $x \in \mathbb{N}$.

2.3 Задачи с непълна формулировка

В третата подсекция се анализира една задача.

Последната задача, която ще изследваме в тази секция, е от Пролетен математически турнир за 4. клас. Резултатите от състезанието се вземат предвид при приема в 5. клас в математически гимназии.

Задача 5. [7] Намерете всички решения на ребуса ПМС+РУСЕ=2014, ако на еднаквите букви съответстват еднакви **ненулеви** цифри, а на различните букви съответстват различни цифри.

Нека да разгледаме решението, което се предлага от авторите, след което ще анализираме внимателно условието на задачата:

Решение. [7] Понеже П не може да е нула, то има пренос към хилядите. Тогава

Р=1. От друга страна С и Е са различни и никое от тях не е 1 или 0. Следователно С+Е не може да е 4. Получаваме, че С+Е=14, откъдето С>4, М+С=10 и П+У=9.

Ако С=5, то М=5: абсурд.

Ако С=6, то Е=8, М=4; сега П и У са 2 и 7 в някакъв ред.

Ако С=7, то Е=7: абсурд.

Ако С=8, то Е=6, М=2; сега П и У са 4 и 5 в някакъв ред.

Ако С=9, то М=1=Р: абсурд.

И така, решенията са: 246+1768, 746+1268, 428+1586 и 528+1486.

Нека сега се задълбочим в условието на задачата. Повтаря се само буквата С, на която по условие съответства **ненулева** цифра. За различните букви обаче нямаме ограничение да са **ненулеви** (според условието). В решенията, които се предлагат, не е използвана цифрата нула за различните букви. Това е пропуск и риск да бъдат ощетени някои ученици. Важно е да отбележим, че състезанието участва в приема за 5. клас в редица математически гимназии в България. Ето кои са другите решения, които отговарят на даденото условие, а не са посочени: 374+1640, 674+1340, 928+1086 и 946+1068.

В предложеното от авторите решение се казва, че П не може да е нула. Трябва да подчертаем обаче, че от условието и това не става ясно. По условие не се изисква ПМС да е трицифрено число, което би означавало, че на буквата П също може да съответства цифрата нула. В такъв случай се получават още две решения: 028+1986 и 046+1968.

3 Заключение

Математическата задача е едно от най-мощните и универсални средства за обучение, развитие и оценяване в училищната практика. Тя изпълнява не само дидактична функция, но и формира трайни когнитивни и социални умения, които подготвят учениците за справяне с реални житейски предизвикателства. Именно поради тази централна роля, качеството на съставените математически задачи е от ключово значение за постигане на ефективно и смислено обучение.

Извършеният анализ в настоящата статия показва, че неточностите при съставянето на математически задачи са често срещан и подценяван проблем, който може да окаже сериозно влияние върху учебния процес. Независимо дали се касае за съдържателни, логически, езикови или методически неточности, тяхното присъствие в учебните материали или в устните и писмени изпитвания може да доведе до значителни затруднения за учениците, включително до:

- неправилно разбиране на поставената задача;
- изграждане на погрешни математически представи и концепции;
- формиране на негативно отношение към математиката като учебен предмет;
- занижени постижения и ниска мотивация за учене.

Причините за допускането на подобни неточности са комплексни. Те могат да произтичат от липсата на достатъчно педагогически опит, недостатъчна езикова яснота, непознаване на психологическите особености на възрастовата група или неосъзнато прилагане на неподходящи методически решения. В някои случаи неточностите се дължат и на недооценяване на ролята на яснотата и последователността

при формулирането на задачите.

Една от основните констатации на настоящото изследване е необходимостта от създаване и прилагане на систематизирани критерии за оценка на качеството на математическите задачи преди тяхното използване в учебния процес. Подобен инструмент може да включва:

- проверка за математическа коректност и единственост на решението;
- проверка за логическа последователност и пълнота на условието;
- езикова редакция за ясност и недвусмислие;
- съобразяване с възрастовите, когнитивните и културните особености на целевата група.

Също така е важно да се насърчава обменът на добри практики между учители и автори на учебни материали, както и провеждането на обучения, свързани със съставянето на качествени математически задачи. Чрез подобряване на уменията за създаване на задачи се повишава не само качеството на обучението, но и се създава учебна среда, която мотивира, вдъхновява и развива учениците.

В заключение можем да кажем, че всяка математическа задача е не само инструмент за проверка, но и носител на ценности, култура и начин на мислене. Именно затова грижливото ѝ съставяне и внимателното ѝ формулиране са от съществено значение за постигане на дългосрочни образователни резултати. Справянето с неточностите при съставяне на математически задачи е не само технически въпрос, но и важна стъпка към по-качествено и справедливо образование.

Благодарности: Това изследване е частично финансирано от проект за научни изследвания РД-08-114/05.02.2026 на Шуменски университет.

Литература

[1] К. Банков, С. Наков, Г. Николова, Д. Петрова, И. Цветкова. *Математика профилирана подготовка – задачи и тестове за Държавен зрелостен изпит.* София, Издателство Просвета, 2021. [K. Bankov, S. Nakov, G. Nikolova, D. Petrova, I. Cvetkova. Matematika profilirana podgotovka – zadachi i testove za Darzhaven zrelosten izpit. Sofia, Izdatelstvo Prosveta, 2021.] (in Bulgarian)

[2] К. Банков, С. Наков, Г. Николова, Д. Петрова, И. Цветкова. *Математика профилирана подготовка – задачи и тестове за Държавен зрелостен изпит.* София, Издателство Просвета, 2022. [K. Bankov, S. Nakov, G. Nikolova, D. Petrova, I. Cvetkova. Matematika profilirana podgotovka – zadachi i testove za Darzhaven zrelosten izpit. Sofia, Izdatelstvo Prosveta, 2022.] (in Bulgarian)

[3] Т. Витанов, М. Кьосева, П. Недевски. *Математика 9. клас.* София, Издателство Анубис, 2018. [T. Vitanov, M. Kyoseva, P. Nedevski. Matematika 9. klas. Sofia, Izdatelstvo Anubis, 2018.] (in Bulgarian)

[4] Т. Витанов, М. Кьосева, П. Недевски. *Математика 9. клас.* София, Издателство Клет България, 2024. [T. Vitanov, M. Kyoseva, P. Nedevski. Matematika 9. klas. Sofia, Izdatelstvo Klett Bulgaria, 2024.] (in Bulgarian)

[5] В. Златилов, Д. Капралова, Е. Каращранова, И. Тонов, М. Христова, И. Шаркова. *Математика профилирана подготовка – практическа математика.* София, Издателство Регалия 6, 2021. [V. Zlatilov, D. Kapralova,

E. Karashtranova, I. Tonov, M. Hristova, I. Sharkova. Matematika profilirana podgotovka – prakticheska matematika. Sofia, Izdatelstvo Regaliya 6, 2021.] (in Bulgarian)
[6] Национална Олимпиада по Математика – общински кръг. Шумен, 2021. [Nacionalna Olimpiada po Matematika – obshtinski krag. Shumen, 2021.] (in Bulgarian)
[7] Пролетен математически турнир. Русе, 2014. [Proleten matematicheski turnir. Ruse, 2014.] (in Bulgarian)

МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2026
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2026
Proceedings of the Fifty-Fifth Spring Conference
of the Union of Bulgarian Mathematicians
Tryavna, Bulgaria, April 5–9, 2026

A COMPETENCE-BASED METHODOLOGICAL FRAMEWORK FOR MEANINGFUL DERIVATION OF FORMULAE FOR AREAS, SURFACE AREAS AND VOLUMES IN THE PREPARATION OF FUTURE MATHEMATICS TEACHERS

Desislava Georgieva
Faculty of Mathematics and Informatics, St Cyril and St. Methodius University of Veliko Tarnovo, Bulgaria
e-mail: d.georgieva@ts.uni-vt.bg

The article focuses on the development of the methodological competence of future mathematics teachers through a systematic approach to teaching formulae for areas, surface areas and volumes of geometric figures in secondary school. A conceptual–methodological model is proposed, including a competence-based methodological framework for the meaningful introduction of the formulae. This framework reveals how the formulae should be introduced by the teacher and is therefore intended for university training in "Methodology of Mathematics Education"; it includes didactic technologies for the formation of methodological skills in students. The model employs object–activity modelling, geometric transformations, analogies and generalisations to achieve conceptual understanding and learning situations for professional reflection of future mathematics teachers.

Keywords: inductive-integrative didactic framework; methodological competence; geometric modelling; meaningful derivation of formulae; preparation of future mathematics teachers

КОМПЕТЕНТНОСТНА МЕТОДИЧЕСКА РАМКА ЗА СМИСЛОВО ИЗВЕЖДАНЕ НА ФОРМУЛИ ЗА ЛИЦА, ПОВЪРХНИНИ И ОБЕМИ В ПОДГОТОВКАТА НА БЪДЕЩИ УЧИТЕЛИ ПО МАТЕМАТИКА

Десислава Георгиева
Факултет по математика и информатика, ВТУ „Св. св. Кирил и Методий", Велико Търново, България
e-mail: d.georgieva@ts.uni-vt.bg

https://doi.org/10.55630/mem.2026.55.163-170

2020 Mathematics Subject Classification: 97G30, 97D40, 97B50.

Статията се фокусира върху развитието на методическата компетентност на бъдещите учители по математика чрез системен подход за преподаване на формули за лица, повърхнини и обеми на геометрични фигури в средното училище. Предложен е концептуално-методически модел, включващ компетентностна методическа рамка за смислово въвеждане на формулите. Тази рамка разкрива *как да се въвеждат формулите от учителя* и затова е предназначена за университетското обучение по „Методика на обучението по математика“ и включва дидактически технологии за формиране на методически умения у студентите. Моделът използва предметно-действено моделиране, геометрични преобразувания, аналогии и обобщения за постигане на концептуално разбиране и обучаващи ситуации за професионална рефлексия на бъдещите учители по математика.

Ключови думи: индуктивно-интегративна дидактическа рамка; методическа компетентност; геометрично моделиране; смислово извеждане на формули; подготовка на бъдещи учители по математика

Introduction

The future mathematics teacher must be not merely a bearer of knowledge but a mediator of mathematical thinking. Their *methodological competence* is a complex, integrative characteristic. It also includes *specialised methodological skills* for using effective didactic techniques for introducing and studying mathematical concepts in an accessible, engaging and effective way, consistent with the age characteristics of the students and contemporary educational realities.

In the mathematics curricula for secondary school, state educational requirements stand out concerning the knowledge and application of formulae for areas of figures and volumes of solids. *The thesis* is that the unstable memorisation and reproduction of formulae by students is a symptom of a deeper problem – namely, the methodological competence of the teacher, based on dominant reproductive teaching methods. If the teachers themselves perceive formulae as "symbols to be memorised" or ready-made list elements, this will inevitably transfer into school practice. Therefore, university preparation plays an important role in overcoming this problem through the formation of the methodological competence of future teachers.

From a methodological perspective, a *formula* represents neither a concept nor a statement, but a symbolic record of a quantitative relationship between quantities, expressing a generalised result of mathematical reasoning or experiment. A formula has four levels of representation: action-based (through modelling, measuring, cutting); visual–schematic (through drawing, figure, net); symbolic (through literal–numerical notation); verbal (a verbal equivalent of the symbolic notation).

For brevity, the term "*formulae*" is used in the article to include formulae for: areas of plane figures, surface areas of solids and volumes of solids. These are studied across several educational stages at school, which determines their significant place in mathematics education.

This gives rise to the following research questions: According to what methodological model should the introduction of the formulae in school be organised? Which approaches support the revealing of their logic? What didactic technologies should student future mathematics teachers master?

The object of the study is the methodological competence of students – future mathematics teachers – in the discipline "Methodology of Mathematics Education". **The subject** of the study is specialised methodological skills, as an essential component of the professional–methodological competence of the future teacher, for mastering specific didactic techniques in introducing the formulae. **The aim** and tasks of the study relate to: theoretical analysis of specific didactic techniques for introducing the formulae; development of a methodological framework based on a combined approach for introducing the formulae; and illustration of corresponding models of didactic technologies.

Problematic and brief theoretical analysis

An analysis of the author's teaching practice in the discipline "Methodology of Mathematics Education" outlines a persistent tendency towards mechanical application of the formulae. A significant proportion of the students also encounter difficulties in arguing their derivation. Methodologically, this is associated with the widespread declarative approach in school education "presentation – memorisation – application". Formulae are often provided ready-made by the teacher, without tracing their origin and without connection to modelling activities and analogies with already studied formulae. As a result, students build a weak connection between the geometric figure and the corresponding formula, and algorithmic exercises do not require in-depth understanding. **It follows** that the sustainable mastery of formulae by students requires effective ***methodological competence*** on the part of the teacher – to possess knowledge of current educational approaches and developed methodological skills for applying methods, techniques and learning resources for activity-based and meaningful introduction of formulae.

Pedagogical and methodological studies by a number of authors investigate contemporary approaches to inquiry-based and activity-based learning grounded in constructivism. The scientific literature emphasises that through the inquiry approach learners are encouraged to seek solutions to a given problem rather than merely memorise rules and procedures [2]. Learning through discovery increases learners' interest in studying mathematics [8]. They understand mathematical concepts more deeply and are more capable of transferring their knowledge to new situations [7]. Activities of Grade 6 students with manipulative materials (tangram type) lead to better achievement in mathematics [6]. Higher results have been achieved in teaching students using a multisensory approach based on the "concrete – representational – abstract" (CRA) framework [5]. The importance of experimentation has been emphasised [4]. It is appropriate to combine computer dynamic models with manipulatives [1].

These and other studies show that contemporary education oriented towards the acquisition of skills and functional literacy requires teachers to demonstrate approaches and technologies grounded in constructivism. The methodology of mathematics education, as a scientific field and academic discipline, is also charged with this task: to improve students' pedagogical competence as a basis of their professional–methodological competence. Overcoming the aforementioned problems directs us towards the development of a methodological model for teaching the topic "Areas and Volumes of Figures". In the context of university instruction, the proposed framework is considered not as a direct technology for work with pupils, but as a means for developing the methodological competences of students – future mathematics teachers – in planning and implementing the introduction of geometric formulae.

Competence-oriented methodological framework for developing the methodological competences of future teachers when introducing geometric formulae

In university instruction, this framework is regarded as a meta-methodological model aimed at developing the methodological competences of student future mathematics teachers: competence for methodological planning of the introduction of new knowledge; competence for organising productive cognitive activity of students; competence for reasoned geometric explanation and justification of relationships.

The proposed framework is based on an inductive-empirical integrated approach that combines:

- an inquiry approach (experiment, rediscovery);
- a constructive and activity-based approach (modelling, constructing);
- general scientific methods of cognition – comparison, analogy and generalisation.

The methodological novelty of the framework lies in the systematic unification of these approaches into a single sequence of cognitive and meta-methodological actions through which students simultaneously experience the process of conceptual comprehension and reflect on its pedagogical organisation.

The framework is based on the following principles: learner activity; visualisation and modelling; analogy and generalisation (transition from particular cases to a general relationship); reflection (comprehension both of the mathematical results and of the methodological decisions).

The didactic implementation includes consecutive interrelated stages:

1. **A problem situation** motivating the need for the formula and directing students towards planning an appropriate introduction.
2. **Manipulative and experimental activity** with material, schematic and dynamic models for activity-based construction of the formula, accompanied by discussion of possibilities for organising student activity.
3. **Visual–logical comprehension** and comparison with already known relationships, emphasising methodological decisions for supporting generalisation.
4. **Formulation of the relationship** between quantities as a generalisation of the performed actions and observations, combined with analysis of linguistic and symbolic precision.
5. **Bidirectional transition** between symbolic and verbal formulation of the formula, considered as a means for developing the future teacher's skills in mathematical communication.

It follows that mastering the proposed didactic technologies functions as a means for developing students' professional-methodological competence.

Within the model, the ***formula*** is regarded as the result of an inquiry process, in which students analyse how in the school environment it can be:

- derived through geometric actions (cutting, rearranging, completing, comparing figures with equal areas or volumes);
- connected with real and modelled situations;

- interpreted geometrically (each quantity has a visual meaning, and the factors in the formulae are interpreted as geometric characteristics);
- presented as the result of purposeful investigation rather than as a ready-made rule.

An essential point is that students not only perform the activities but also conduct subsequent methodological reflection on the conditions for their effective use in school practice.

The role of the instructor in the university environment is to model professional actions: to organise an environment for inquiry, to direct attention to essential relationships through questions, to support generalisation and mathematical formalisation, and to stimulate students' methodological reflection. Hence, the framework is aimed at:

- understanding formulae as the result of activity rather than ready-made rules;
- building skills for geometric reasoning and argumentation;
- purposeful development of future teachers' methodological competences for planning and implementing the introduction of formulae through rediscovery technologies.

In accordance with this framework, didactic technologies for justified derivation of the formulae have been developed, which students analyse, modify and plan for application in their future pedagogical practice.

Areas of plane figures – didactic technologies

The preparation of student future teachers begins with methodological updating and rediscovery of the area of a rectangle as basic knowledge for deriving the other formulae. Covering the rectangle with unit squares ensures the transition from concrete measurement to a generalised relationship. Students analyse the cutting of the rectangle along the diagonal and justify the methodological advantages of the activity-based approach. The subsequent folding forms two triangles whose area is half the area of the rectangle (Fig. 1). The practical activity aims at awareness of the didactic logic of the derivation.

In a parallelogram, an internal height is dropped and a right triangle is separated and moved in order to transform the parallelogram into a rectangle (Fig. 2). The area of the rhombus is considered as a special case of the parallelogram. Students master a universal model for transforming figures applicable in pedagogical practice. They independently investigate transformations of a trapezium (Figs. 3, 4 and 5), formulating methodological decisions and using analogy for memorisation. The generalisations include: "The area of an arbitrary figure is found as the sum or difference of the areas of its component figures" and "The areas of quadrilaterals – rectangle, parallelogram, rhombus and trapezium – are found as the product of a side (or the arithmetic mean of the bases) and the corresponding height; for a triangle the result is divided by two".

Students design their own didactic implementations, deriving the formula for the area of a regular polygon as the sum of the areas of its constituent triangles. Under the guidance of the instructor, they examine images in textbooks and dynamic visualisation of the transformation of the circle into a rectangle, selecting appropriate digital tools and presenting the results through brief methodological presentations. This develops skills for didactic design and reasoned selection of technologies.

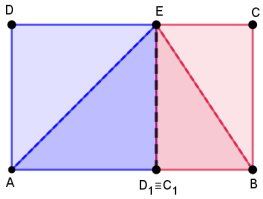


Fig. 1. Triangle

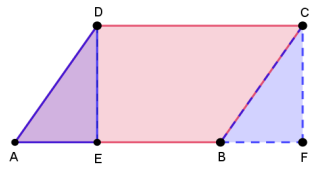


Fig. 2. Parallelogram

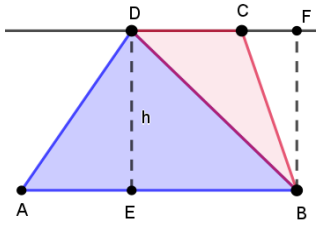


Fig. 3. Trapezium – Method 1

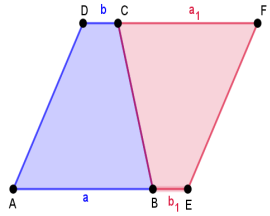


Fig. 4. Trapezium – Method 2

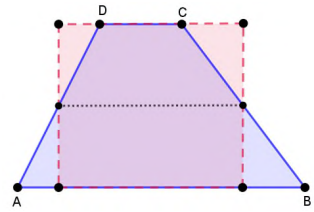


Fig. 5. Trapezium – Method 3

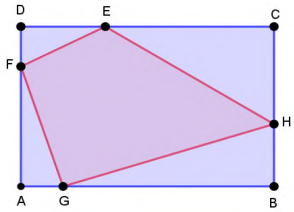


Fig. 6. Quadrilateral

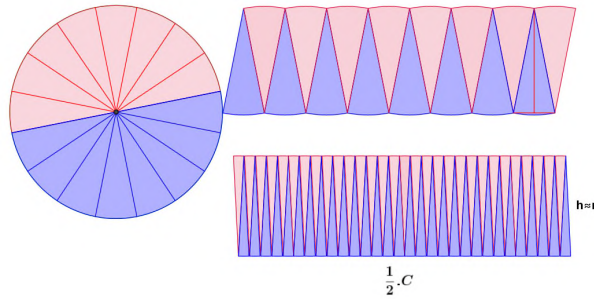


Fig. 7. Circle

Didactic technology – surface areas of solids

The net of a right prism is constructed, with students analysing the number and type of the obtained faces and establishing the relationship between the perimeter of the base and the lateral surface area. In this way the formula $S = P.h$ is comprehended as a structural relationship between quantities rather than as a ready-made rule.

Through modelling of a right circular cylinder, future teachers discover the analogy with the prism and on this basis justify the formulae for lateral and total surface area.

An analogous approach is applied when constructing nets of a pyramid and a cone, where students trace the common relationships between the formulae. Methodologically it is appropriate to compare the surface areas of the prism and the cylinder in order to highlight both the similarities and the essential differences.

When deriving the formula for the surface area of a sphere, students use modelling and experimentation. A polystyrene ball is cut into two hemispheres. At the centre of

the cut a string is fixed and wound so as to cover the entire circle of the section. A second string is fixed at the "pole" and wound along the surface of the hemisphere. By comparing the lengths, students establish that the second string is twice as long, which leads to the conclusion that the surface area of the sphere is four times the area of the great circle. Students understand the role of the teaching experiment.

Didactic technology – volumes of solids

Through modelling of a rectangular parallelepiped and filling it with unit cubes (or through instructional videos), students trace the number of cubes in one layer and the number of layers. In this motivated way the formula for volume as the product of the area of the base and the height is reached. On this basis, an analogy is established with the volumes of a right prism and a right circular cylinder.

From cardboard, a regular quadrilateral pyramid and a prism with equal bases and equal heights are constructed. Through experimental filling with granular material (or through animation) it is established that three pyramids fill one prism. From this, students trace the logic for discovering the relationship for the volume of a pyramid and verify its validity for a cone and a cylinder.

Additionally, a cylinder is modelled with a diameter twice that of a tennis ball. After successive pouring of granular material and placing the ball, the change in level is recorded, which leads to the derivation of the formula $V_{ball} = \frac{4}{3}\pi r^3$.

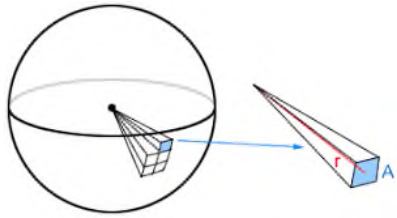


Fig. 8. Volume of a ball

Alternatively, the volume of the sphere is justified through its decomposition into many "pyramids" with convex bases (Fig. 8). The volume of each of them is approximated by $V \approx \frac{1}{3}Ar$, where A is the area of the base. Through logical generalisation students reach the conclusion that the sum of the bases corresponds to the surface area of the sphere, from which the formula follows: $V_{ball} = \frac{1}{3}\ r.S = \frac{1}{3}\ r.\ 4\pi r^2 = \frac{4}{3}\pi r^3$.

At the contemporary stage, the methodological competence of the teacher is expanding with skills for blended learning (online learning, application of digital technologies and educational software, flipped classroom, etc.). Therefore, in the methodological implementation it is appropriate to integrate modern digital tools, for example GeoGebra, which extend work with manipulatives through dynamic visualisations and support conceptual understanding.

The proposed didactic solutions show how, through transformation, cutting, completing and comparison of figures, meaningful derivation of formulae can be achieved. The pedagogical value of the approach is expressed in ensuring a transition from concrete action to theoretical generalisation and in developing reasoned geometric thinking in future teachers.

Conclusion

The developed competence-based methodological framework offers a systematically organised methodological model for introducing formulae for areas, surface areas and volumes in the university preparation of future mathematics teachers. Its leading characteristic is the transition from declarative presentation to meaningful productive discovery through modelling, geometric transformations, analogies and generalisations.

The author's contributions can be summarised in the following directions: an inductive–integrative didactic framework for introducing geometric formulae has been synthesised; a sequence of cognitive actions ensuring their meaningful derivation has been structured; didactic solutions aimed at enriching the methodological competence of future mathematics teachers have been proposed.

The proposed framework has a conceptual–methodological character and outlines prospects for subsequent empirical verification of its effectiveness.

Acknowledgements:

I thank Prof. Dr Darinka Galabova for the provided support and the objective opinion.

References

[1] Chehlarova, T. Qualification course for teachers "Studying stereometry with dynamic constructions", *Mathematics and education in mathematics*, 49 (2020). 269-274. (in Bulgarian).

[2] Diano Jr., F., Monterde, N., & Diaz, J. Discovery approach in teaching mathematics among Grade Six Students. *Solid State Technology*, 64(2), (2021). 5157-5162.

[3] Gurmu, F., Tuge, C. & Hunde, A. Effects of GeoGebra-assisted instructional methods on students' conceptual understanding of geometry. *Cogent Education*, 11(1), (2024),

[4] Kenderov, P., Chehlarova, T., Sendova, E., A Virtual Mathematics Laboratory in support of educating educators in inquiry-based style, Educating the educators: International approaches to scaling-up professional development in mathematics and science education, (2014). 167-176.

[5] Melhem, D., et al. Improving Geometric Thinking Skills Through a Multisensory-Based CRA Framework in Students with Learning Difficulties and Various Sensory Preferences. *Educational Process*, 16, (2025), 1-17.

[6] Milenkovic. A., Stevanic, J., Zdravkovic, N. The impact of discovery-based learning with physical manipulatives in teaching the area of triangles and quadrilaterals on students' achievement. *Journal of Pedagogical Research*, 9 (3), (2025), 102-115.

[7] Pugosa, C., et al. Effects of heuristic method on students' performance in mathematics. British Journal of Teacher Education and Pedagogy, 3(2), (2024). 69-86.

[8] Ramadhani, M., Kartono, & Haryani, S. The effect of using discovery learning-based mathematics learning modules on students' interest in learning mathematics. *International Journal of Research and Review*, 10(4), (2023), 476-480.

МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2026
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2026
Proceedings of the Fifty-Fifth Spring Conference
of the Union of Bulgarian Mathematicians
Tryavna, Bulgaria, April 5–9, 2026

AREAS IN CONVEX QUADRILATERAL

Plamen Gostev
Faculty of Mathematics and Informatics, Sofia University
Sofia High School of Mathematics, Bulgaria
e-mail: gostev@fmi.uni-sofia.bg

The concept of area is first introduced in primary school. As they go through secondary education, students delve deeper into the essence of area problems. The more advanced and interesting aspects are mainly explored in specialized Mathematics High Schools and within extracurricular math courses.
In the current article, we'll prove two well-known problems. We will then solve two geometry problems on convex quadrilaterals using parameters instead of concrete constants. The goal is to demonstrate quick and elegant solutions to a group of problems with a convex quadrilateral divided into smaller quadrilaterals. We will also provide ideas for creating similar problems.

Keywords: convex quadrilateral, area, ratio

ЛИЦА В ИЗПЪКНАЛ ЧЕТИРИЪГЪЛНИК

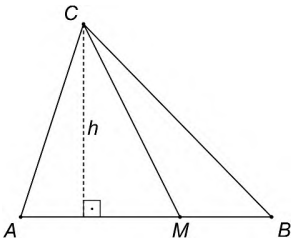
Пламен Гостев
Факултет по математика и информатика на СУ „Св. Климент Охридски“
Софийска математическа гимназия „Паисий Хилендарски“
e-mail: gostev@fmi.uni-sofia.bg

Понятието лице се среща още в началния етап на образование на учениците. В средния курс на обучение те навлизат повече в същината на задачите за лица. По-интересните и сложни задачи се разглеждат в математическите гимназии и в часовете за извънкласна работа.
В настоящата статия ще докажем две популярни основни задачи, след което ще решим две геометрични задачи за четириъгълник, но обобщени с параметър, а не с конкретна константа. С помощта на тези задачи ще демонстрираме бързи и елегантни решения на група от задачи за произволен изпъкнал четириъгълник, разделен на части, както и идеи за съставяне на подобни задачи.

Ключови думи: изпъкнал четириъгълник, лице, отношение

https://doi.org/10.55630/mem.2026.55.171-176
2020 Mathematics Subject Classification: 97G40.

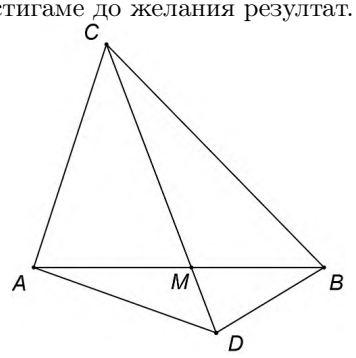
Основна задача 1: Точка M е от страната AB на ΔABC. Да се докаже, че $S_{AMC} : S_{BMC} = AM : BM$ и $S_{AMC} : S_{ABC} = AM : AB$.



Доказателство: Щом точките A, M и B лежат на една права и точка C не лежи на тази права, то триъгълниците ABC, AMC и BMC имат обща височина (h на чертежа).

Тогава $S_{ABC} = 0,5.h.AB$, $S_{AMC} = 0,5.h.AM$ и $S_{BMC} = 0,5.h.BM$. Разделяйки почленно последните две и първите две равенства, достигаме до желания резултат.

Основна задача 2: Даден е изпъкнал четириъгълник $ADBC$, диагоналите на който се пресичат в точка M. Да се докаже, че $S_{ACD} : S_{BCD} = AM : BM$.



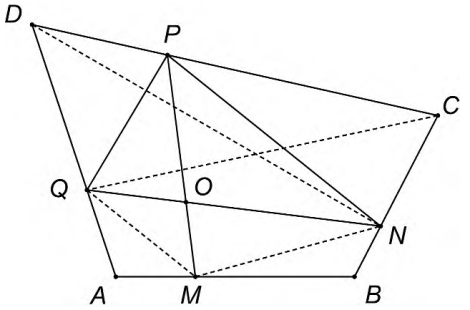
Доказателство: Прилагайки основна задача 1, получаваме:

$S_{AMC} : S_{BMC} = AM : BM$ и $S_{AMD} : S_{BMD} = AM : BM$.

Използвайки свойствата на пропорцията, достигаме до искания извод.

С помощта на подход, демонстриран в статия [1], и тези две основни задачи ще решим задача 1.16 на стр. 13 и задачи 4.21 и 4.22 на стр. 84 от книгата [2].

Задача 1. Точките M, N, P и Q лежат съответно на страните AB, BC, CD и AD на изпъкнал четириъгълник $ABCD$. Ако $MP \cap NQ = O$, $AM : MB = DP : PC = x$ и $BN : NC = AQ : QD = y$, намерете отношенията $MO : OP$ и $QO : ON$.



Решение: Ще използваме основна задача 1, за да изразим лицето на ΔQNP чрез лицата на ΔQND и ΔQNC:

$$S_{QNP} = S_{QNCD} - S_{NCP} - S_{QPD} = S_{QNCD} - \frac{1}{x+1}S_{NCD} - \frac{x}{x+1}S_{QCD} =$$

$$= S_{QNCD} - \frac{1}{x+1}\left(S_{QNCD} - S_{QND}\right) - \frac{x}{x+1}\left(S_{QNCD} - S_{QNC}\right) =$$

$$= S_{QNCD} - \frac{1}{x+1}S_{QNCD} + \frac{1}{x+1}S_{QND} - \frac{x}{x+1}S_{QNCD} + \frac{x}{x+1}S_{QNC}.$$

$$\Rightarrow S_{QNP} = \frac{1}{x+1}S_{QND} + \frac{x}{x+1}S_{QNC}\ .$$

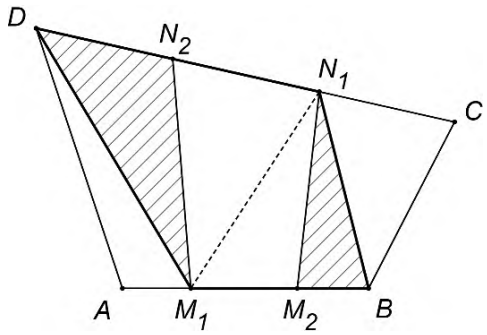
Аналогично $S_{QNM} = \frac{1}{x+1}S_{QNA} + \frac{x}{x+1}S_{QNB}$.

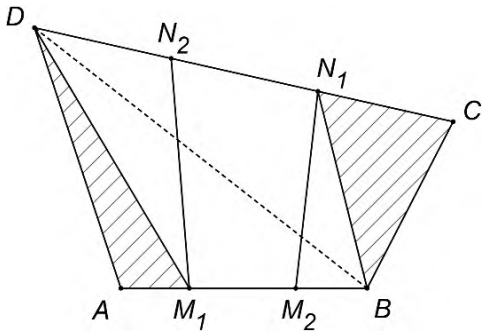
Но $S_{QNA} = yS_{QND}$ и $S_{QNB} = yS_{QNC}$. Заместваме в горното равенство

$$S_{QNM} = \frac{1}{x+1}yS_{QND} + \frac{x}{x+1}yS_{QNC} = y\left(\frac{1}{x+1}S_{QND} + \frac{x}{x+1}S_{QNC}\right) = y.S_{QNP}.$$

От основна задача 2 следва, че $MO : OP = y$. Аналогично $QO : ON = x$.

Задача 2. Точките M_1 и M_2 лежат на страната AB, а точките N_1 и N_2 – на страната CD на изпъкнал четириъгълник $ABCD$. Ако $AM_1 = M_2B = x.AB$ и $CN_1 = N_2D = x.CD$, където $0 < x < 0,5$, намерете отношението $S_{M_1M_2N_1N_2} : S_{ABCD}$.

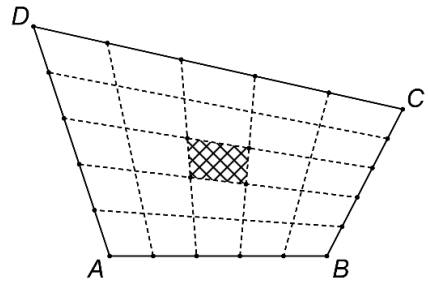




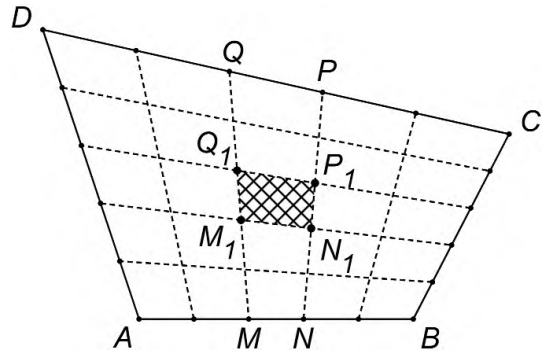
Решение: Отново ще използваме основна задача 1:
$S_{AM_1D} + S_{BCN_1} = x.S_{ABD} + x.S_{BCD} = x.(S_{ABD} + S_{BCD}) = x.S_{ABCD}$
$S_{M_1N_2D} + S_{M_2BN_1} = \frac{x}{1-x}S_{M_1N_1D} + \frac{x}{1-x}S_{M_1BN_1} = \frac{x}{1-x}(S_{M_1N_1D} + S_{M_1BN_1}) =$
$= \frac{x}{1-x}S_{M_1BN_1D} = \frac{x}{1-x}(S_{ABCD} - (S_{AM_1D} + S_{BCN_1})) = \frac{x}{1-x}(S_{ABCD} - x.S_{ABCD}) =$
$= \frac{x}{1-x}.(1-x)S_{ABCD} = x.S_{ABCD}.$

Тогава сборът от четирите лица $S_{AM_1D} + S_{M_1N_2D} + S_{M_2BN_1} + S_{BCN_1} = 2x.S_{ABCD}$.
$\Rightarrow S_{M_1M_2N_1N_2} = S_{ABCD} - (S_{AM_1D} + S_{M_1N_2D} + S_{M_2BN_1} + S_{BCN_1}) = (1-2x)S_{ABCD}$.

Задача 3. Всяка от четирите страни на изпъкнал четириъгълник $ABCD$ е разделена на 5 равни части. Точките са свързани до образуването на четириъгълна мрежа (както на чертежа). Да се докаже, че лицето на централния четириъгълник е 25 пъти по-малко от лицето на четириъгълника $ABCD$.



Решение: Ще използваме означените на чертежа точки M, N, P, Q, M_1, N_1, P_1 и Q_1. От задача 1 получаваме, че $MM_1 : M_1Q = NN_1 : N_1P = 2 : 3$, също така $MQ_1 : Q_1Q = NP_1 : P_1P = 3 : 2$. От тези равенства следва, че $MM_1 = Q_1Q = \frac{2}{5}MQ$ и $NN_1 = P_1P = \frac{2}{5}NP$.

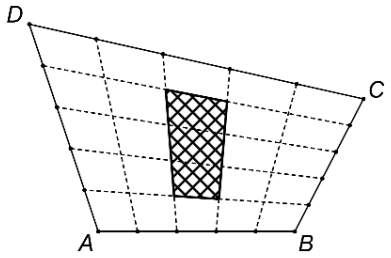


Ако използваме аналогични разсъждения за всяка от 16-те вътрешни пресечни точки стигаме до извода, че всяка една от пунктираните отсечки е разделена на 5 равни части от четирите си пресечни точки.

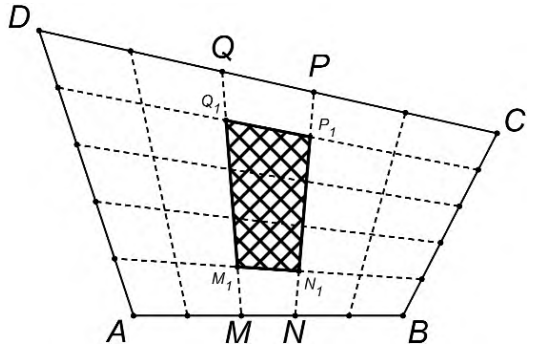
От задача 2 следва, че $S_{M_1N_1P_1Q_1} = \frac{1}{5}S_{MNPQ}$, но по условие $AM = BN = \frac{2}{5}AB$ и $CP = DQ = \frac{2}{5}CD$. Тогава $S_{MNPQ} = \frac{1}{5}S_{ABCD}$ (задача 2), откъдето получаваме, че $S_{M_1N_1P_1Q_1} = \frac{1}{25}S_{ABCD}$.

От решените вече задачи можем да съставим разновидности от задачи за четириъгълник, чиито страни са разделени на произволен брой равни части. В настоящата статия ще разгледаме примери, в които всяка страна е разделена на 5 или 6 равни части. Подходът остава същият независимо от броя на частите, на които са разделени страните на четириъгълника. Трябва да съобразим, че ако този брой е четен, то тогава не съществува „централен“ четириъгълник, но може чрез групиране на няколко малки четириъгълника да се получи по-голям, който да бъде „централен“ четириъгълник.

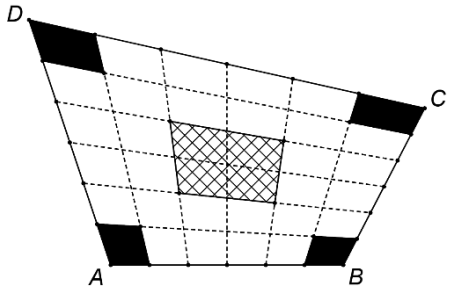
Задача 4. Всяка от четирите страни на изпъкнал четириъгълник $ABCD$ е разделена на 5 равни части. Точките са свързани до образуването на четириъгълна мрежа (както на чертежа). Докажете, че лицето на защрихования четириъгълник е $0,12$ от лицето на четириъгълника $ABCD$.



Решение: Използвайки доказаното в предишната задача, можем да твърдим, че $MM_1 = QQ_1 = \frac{1}{5}MQ$ и $NN_1 = PP_1 = \frac{1}{5}NP$. Тогава от основна задача 2 стигаме до извода, че $S_{M_1N_1P_1Q_1} = \frac{3}{5}S_{MNPQ}$. В задача 3 видяхме, че $S_{MNPQ} = \frac{1}{5}S_{ABCD}$, с което стигаме до заключението, че лицето на защрихования четириъгълник е $\frac{3}{25} = 0,12$ от лицето на четириъгълника $ABCD$.



Задача 5. Всяка от четирите страни на изпъкнал четириъгълник $ABCD$ е разделена на 6 равни части. Точките са свързани до образуването на четириъгълна мрежа (както на чертежа). Докажете, че:

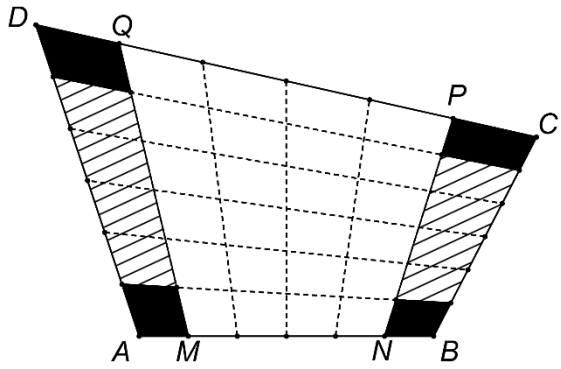


а) лицето на защрихования четириъгълник е $\frac{1}{9}$ от лицето на четириъгълника $ABCD$;

б) лицето на защрихования четириъгълник е равно на сбора от лицата на плътно оцветените четириъгълници.

Решение: а) Решението е аналогично на това на задача 3.

б) От доказаното в задача 2, приложено за четириъгълника $ABCD$, получаваме, че $S_{MNPQ} = \frac{4}{6}S_{ABCD} = \frac{2}{3}S_{ABCD}$. Тогава $S_{AMQD} + S_{BNPC} = \frac{1}{3}S_{ABCD}$. В задача 3 видяхме, че всяка от пунктираните линии е разделена на 6 равни части от пресечните си точки. Следователно сборът от лицата на двата защриховани четириъгълника е $\frac{4}{6}S_{AMQD} + \frac{4}{6}S_{BNPC} = \frac{2}{3}(S_{AMQD} + S_{BNPC})$.

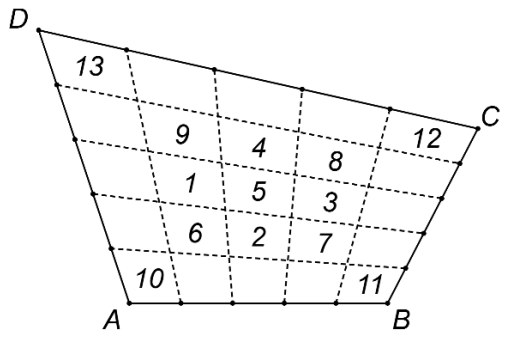


Оттук сборът от лицата на четирите плътно оцветени четириъгълника е

$$\frac{1}{3}(S_{AMQD} + S_{BNPC}) = \frac{1}{3}.\frac{1}{3}S_{ABCD} = \frac{1}{9}S_{ABCD}.$$

Използвайки и подточка а), получаваме исканото твърдение.

Задача 6. Всяка от четирите страни на изпъкнал четириъгълник $ABCD$ е разделена на 5 равни части. Точките са свързани до образуването на четириъгълна мрежа (както на чертежа). Някои от лицата на малките четириъгълници са номерирани. Да се докаже, че:



а) $S_1 + S_3 = S_2 + S_4 = 2.S_5$;

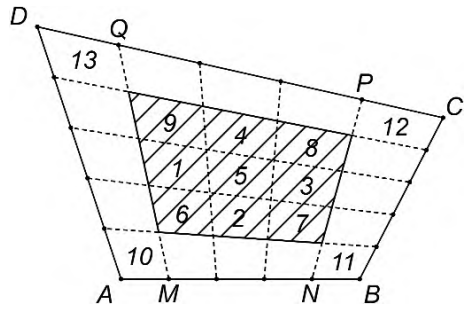
б) $S_6 + S_7 + S_8 + S_9 = 4.S_5$;

в) $S_6 + S_7 + S_8 + S_9 = S_{10} + S_{11} + S_{12} + S_{13}$.

Решение: а) В задача 4 доказахме, че лицето на четириъгълника, образуван от 4, 5 и 2, е $\frac{3}{25}$ от лицето на $ABCD$. Аналогично и лицето на четириъгълника, образуван от 1, 5 и 3, е $\frac{3}{25}$ от лицето на $ABCD$. Щом двата четириъгълника имат равни лица и

номер 5 е общ за тях, то стигаме до $S_1+S_3 = S_2+S_4$. Но от доказаното в задача 3 и 4 следва, че $S_5 = \frac{1}{3}(S_4 + S_5 + S_2) = \frac{1}{3}(S_1+S_5+S_3)$, откъдето $S_2+S_4 = S_1+S_3 = 2.S_5$.

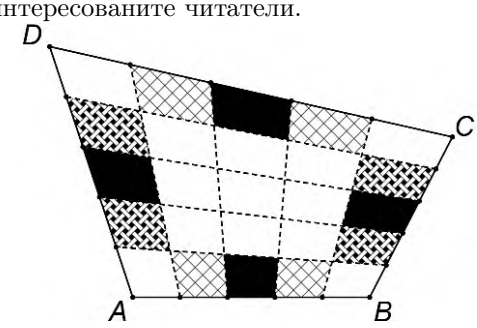
б) Прилагайки задача 2 за четириъгълника $ABCD$, $AM = BN = \frac{1}{5}AB$ и $CP = DQ = \frac{1}{5}CD$ получаваме $S_{MNPQ} = \frac{3}{5}S_{ABCD}$. Но видяхме, че вътрешните отсечки са разделени на равни части, тогава лицето на щрихования четириъгълник или $S_1 + S_2 + S_3 + \ldots + S_8 + S_9$ е $\frac{3}{5}S_{MNPQ} = \frac{9}{25}S_{ABCD} = 9S_5$.



От резултата, получен в подточка а), следва, че $S_1 + S_3 + S_2 + S_4 = \frac{4}{25}S_{ABCD}$, откъдето $S_6 + S_7 + S_8 + S_9 = \frac{4}{25}S_{ABCD} = 4.S_5$.

Решението на подточка в) от задача 6 и следващата задача 7, които се получават със сходни разсъждения, ще оставим на заинтересованите читатели.

Задача 7. Всяка от четирите страни на изпъкнал четириъгълник $ABCD$ е разделена на 5 равни части. Точките са свързани както на чертежа до образуването на четириъгълна мрежа. Да се докаже, че трите сбора от лицата на еднакво щрихованите четириъгълници са равни помежду си.



Заключение. Авторът се надява, че читателят ще се заинтригува от геометричните конфигурации и самостоятелно ще разшири темата чрез съставяне на нови задачи и модели или с обобщение на показаните.

Литература

[1] С. Атанасов, *Лица, Олимпийски теми 2004*, УНИМАТ СМБ, 88 – 99.
[S. Atanasov, *Areas, Olympic problems 2004*, UNIMAT SMB, 88 – 99.] (in Bulgarian)

[2] В. В. Прасолов, *Задачи по планиметрии*, Москва, МЦНМО, 2006.
[V. V. Prasolov, *2D geometry problems*, Moscow, МЦНМО, 2006.] (in Russian)

МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2026
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2026
Proceedings of the Fifty-Fifth Spring Conference
of the Union of Bulgarian Mathematicians
Tryavna, Bulgaria, April 5–9, 2026

DIVERGENT SERIES – SYNERGY BETWEEN MATHEMATICAL FALLACIES AND SUMMATION METHODS

Kamelia Koleva
Vasil Levski National Military University, Faculty "Logistics and Technologies", Department "Communication and Information Systems"
e-mail: kameliabk72@gmail.com

Summation methods for divergent series are an important element of modern mathematical analysis, meaningfully expanding the classical concept of convergence. The incorrect application of algebraic operations to divergent series leads to mathematical fallacies. The report emphasizes the pedagogical potential of the interaction between summation methods and mathematical fallacies. It is shown that their targeted combination in an educational environment promotes the development of critical and analytical thinking, logical and mathematical culture in students, and an understanding of the important role of definitions and statements in mathematics. Examples of real-world models are considered, demonstrating the applicability of Cesàro's and Abel's summation methods.

Keywords: education, mathematical fallacy, divergent series, summation methods, Cesàro summation, Abel summation

РАЗХОДЯЩИТЕ РЕДОВЕ – СИНЕРГИЯ МЕЖДУ СОФИЗМИ И МЕТОДИ ЗА СУМИРАНЕ

Камелия Колева
Национален Военен Университет „Васил Левски", Факултет „Логистика и технологии"
e-mail: kameliabk72@gmail.com

Методите за сумиране на разходящи редове са важен елемент от съвременния математически анализ, разширявайки класическото понятие за сходимост по смислен начин. Паралелно с това неправилното прилагане на алгебрични действия към разходящите редове води до софизми. Докладът акцентира върху педагогическия потенциал на взаимодействието между методите за сумиране и математическите софизми. Показано е, че целенасоченото им съчетаване в образователна среда допринася за развитието на критично и аналитично мислене, логическа и математическа

https://doi.org/10.55630/mem.2026.55.177-185
2020 Mathematics Subject Classification: 40A05, 40G05, 97E40.

култура у обучаемите, както и за осъзнаване на важната роля на дефинициите и твърденията в математиката. Разгледани са примери за реални модели, демонстриращи приложимостта на методите за сумиране на Чезаро и на Абел.

Ключови думи: образование, софизъм, разходящ ред, методи за сумиране, метод на Чезаро, метод на Абел

1 Въведение

Сумирането е вероятно първата математическа операция, която хората са извършвали и върху която са се замисляли. А темата за безкрайна сума от числа – числовите редове – е била интересна за учените още в Древен Вавилон и в Древна Гърция. Изкушенията на математиците да манипулират с безкрайни суми, т.е. да ги третират като крайни суми, е водело до някои противоречиви и парадоксални резултати. Съвременните определения на понятията сума на ред и неговата сходимост или разходимост, основани на понятието граница, окончателно се формулират в началото на XIX в., вследствие на работите на Болцано (1817 г.) и Коши (1821 г.) [12]. Въпреки това великите математици от XVII в. и XVIII в., колкото и свободно да са манипулирали с редове, са знаели достатъчно добре дали са сходящи. В този период Нютон и Лайбниц са първите, които систематично са използвали редове за приближено решаване на алгебрични и диференциални уравнения, но рядко са използвали разходящи редове. Последните се срещат в работите на Ойлер, Фурие, Поасон, Рамануджан и др. основно чрез формални манипулации без строгото им обосноваване. Но дори и след класическата дефиниция на Коши за ред математиците умишлено са избягвали разходящите редове (Даламбер, Лаплас, Лагранж). Разсъжденията върху разходящи редове според Даламбер били „подозрителни“ даже ако резултатите от тях се съгласуват с истината. Не без основание е забележката на Абел от 1828 г., че разходящите редове са „изобретение на дявола“. Една от основните причини е била, че за времето никой формално не е определил как трябва да се дефинира сумата на разходящ ред. Както още и Ойлер е предвиждал, че „загадките на разходящите редове възникват най-вече не от някаква мистерия в самите разходящи редове като такива, а от нежеланието да се дават формални дефиниции ...“ [4, с. 15].

В края на XIX в., с напредъка на различни области на математическия анализ, теорията на разходящите редове придобива систематично изучаване чрез строго дефинираните методи за сумиране на Чезаро, на Хьолдер, на Абел, на Борел и др. Те намират приложения при изследването на асимптотични разлагания; в теорията на редовете на Фурие; в числения анализ и теорията на апроксимациите; в квантовата механика и квантовата теория на полето; в приближени методи за решаване на задачи в математическата физика и др. Детайлно изследване на различни методи за сумиране с подробни теоретични постановки, както и техни приложения могат да се видят в [4].

Настоящият доклад е продължение на [9, 10, 11], в които чрез използването на подходящи софизми се представя нестандартен и мотивационно наситен методически подход за изучаване на числовите редове. Чрез него се предлага по-лесно усвояване на фундаменталните математически понятия ред, сходимост и сума на ред, повишава се интересът на обучаемите към математиката чрез критично и ана-

литично мислене. Да припомним, че *математически софизъм* наричаме привидно коректно математическо разсъждение или „доказателство“, което използва скрита логическа или аналитична грешка и води до неправилен извод. В контекста на разходящите редове, математическите софизми възникват при формално прилагане на алгебрични правила извън областта им на валидност.

Тук си поставяме няколко основни цели:

- да разширим класическата дефиниция за сходимост на ред на Коши чрез представяне на някои по-известни и подходящи за целите ни методи за сумиране на разходящи редове;
- да съпоставим умишлените непозволени операции при софизмите със строгите дефиниции при методите за сумиране, и така да се изяснят още по-детайлно грешките при софизмите.
- да покажем, че софизмите имат огромен педагогически потенциал при историческото осмисляне на развитието на математиката и за по-дълбокото разбиране на математическите понятия, както и за разширяване на техния обхват;
- да покажем как абстрактният анализ среща реалния смисъл чрез илюстриране на модели за приложение на методите за сумиране.

2 Теоретични постановки

Първо ще припомним класическата дефиниция за сума на ред [4, 12].

Определение 1. Нека е дадена безкрайната редица от числа $a_1, a_2, a_3, \ldots, a_n, \ldots$. Безкрайната сума

$$a_1 + a_2 + a_3 + \cdots + a_n + \cdots = \sum_{n=1}^{\infty} a_n$$

се нарича *числов ред* (накратко *ред*), а отделните събираеми $a_1, a_2, a_3, \ldots, a_n, \ldots$ се наричат *членове (елементи)* на реда; a_n – *общ член* на реда.

За реда

$$\sum_{n=1}^{\infty} a_n = a_1 + a_2 + a_3 + \cdots + a_n + \cdots$$

образуваме редицата от *частичните (парциалните) му суми* $S_1, S_2, \ldots, S_n, \ldots$, където $S_1 = a_1$, $S_2 = a_1 + a_2$, …, $S_n = a_1 + a_2 + a_3 + \cdots + a_n, \ldots$.

Казва се, че редът $\sum_{n=1}^{\infty} a_n$ е *сходящ със сума* S, и записваме $\sum_{n=1}^{\infty} a_n = S$, ако редицата от частичните му суми $\{S_n\}_n^{\infty}$ е сходяща със сума S, т.е. $\lim\limits_{n\to\infty} S_n = S$.

Ако $\{S_n\}_1^{\infty}$ е разходяща ($\lim\limits_{n\to\infty} S_n = \pm\infty$ или $\lim\limits_{n\to\infty} S_n$ не съществува) се казва, че редът $\sum_{n=1}^{\infty} a_n$ е *разходящ.*

В предисловието на своя труд „Курс по анализ“ (1821 г.) Коши пише, че „разходящите редове нямат сума“ [12, с. 107].

Когато даден ред е разходящ в класическия смисъл (по Коши), за да се получи специфична и полезна информация за него, трябва да се използва подходящ метод за

сумиране. Съществуването на единствена алгебрична константа, обикновено наричана „сума“ за разходящ ред, е естествено свързана с асимптотичното му разлагане и не противоречи на разходимостта му в класическия смисъл [1].

Методите за сумиране представляват най-общо правило, операция или функция за конструиране на обобщени суми на редове, обобщени граници на редици или обобщени стойности на несобствени интеграли [2].

Тук се стремим да направим обобщение на класическото определение за сума на ред, което да важи и за разходящи редове. Ще наричаме това понятие „сума“, като ще използваме отново означението $\sum$, за да покажем, че сме съпоставили на безкрайна редица от числа реално число (въпреки че това не е границата на частичните суми, както обикновено).

Определение 2. Ще казваме, че редът $\sum_{n=0}^{\infty} a_n$ *се сумира към* s чрез някакъв *метод за сумиране* P и ще записваме

$$\sum_{n=0}^{\infty} a_n = s\,(P) \quad \text{или} \quad P\sum_{n=0}^{\infty} a_n = s$$

и ще казваме, че редът е P-*сумируем* или *сумируем* чрез P към s (вж. [4, с. 6-7]), [5, с. 462-463]).

Най-разпространените методи за сумиране удовлетворяват следните 4 свойства:

1) *мащабируемост*: Ако $\sum_{n=0}^{\infty} a_n = s(P)$, то следва, че $\sum_{n=0}^{\infty} ka_n = ks(P)$.

2) *адитивност*: Ако $\sum_{n=0}^{\infty} a_n = s\,(P)$ и $\sum_{n=0}^{\infty} b_n = t\,(P)$, то следва, че $\sum_{n=0}^{\infty} (a_n + b_n) = (s+t)(P)$.

3) *стабилност*: Ако $a_0 + a_1 + a_2 + a_3 + \cdots = s$ следва, че $a_1 + a_2 + a_3 + \cdots = s - a_0$ и обратно.

4) *регулярност*: Методът за сумиране P се нарича *регулярен*, ако той сумира всеки сходящ ред до неговата обичайна сума, т.е. от $\sum_{n=0}^{\infty} a_n = s$ следва, че $\sum_{n=0}^{\infty} a_n = s(P)$.

Първите 3 свойства са въведени от Харди като аксиоми [4, с. 6]. Свойствата 1) и 2) обобщено определят свойството *линейност* на метода. Свойството регулярност възниква естествено за методите, тъй като дава възможност сумиращите методи да се разглеждат като разширения на класическата сходимост, а не като нейни алтернативи.

В математическия анализа и в неговите приложения обикновено се използват регулярни линейни методи за сумиране. Ще разгледаме два от тях, които представляват особен интерес за приложенията [8, с. 63].

Определение 3. (**метод на Чезаро – метод на средните аритметични**) За числовия ред $\sum_{n=1}^{\infty} a_n$ разглеждаме редицата $S_1, S_2, \ldots, S_n, \ldots$ от частичните му суми и редицата

$$c_1 = S_1,\ c_2 = \frac{S_1 + S_2}{2},\ c_3 = \frac{S_1 + S_2 + S_3}{3}, \ldots$$
$$c_n = \frac{S_1 + S_2 + S_3 + \cdots + S_n}{n} = \frac{1}{n}\sum_{k=1}^{n} S_k,\ \ldots$$

от *средните аритметични* на частичните суми. Ако съществува $\lim\limits_{n\to\infty} c_n = s$, то казваме, че даденият ред е *сумируем по Чезаро* или C-сумируем и записваме $\sum_{n=1}^{\infty} a_n = s(C)$. Числото s се нарича *обобщена (в смисъл на Чезаро) сума* за реда или C-сума за реда. Използват се и означенията $(C,\ 1)$-сума или C_1-сума (вж. [4, с. 7], [5, с. 464]).

В [7, с. 8] е представено и матричното дефиниране на метода на Чезаро от първи ред – C_1.

Определение 4. (**метод на Абел – метод на степенните редове**) За числовия ред $\sum_{n=1}^{\infty} a_n$ разглеждаме степенния ред $\sum_{n=1}^{\infty} a_n x^{n-1}$. Ако последният ред е сходящ за всяко x от интервала $(0,\ 1)$ и неговата сума $f(x) = \sum_{n=1}^{\infty} a_n x^{n-1}$ има граница $\lim\limits_{x\to 1^-} f(x) = s$, то казваме, че даденият ред е *сумируем по Абел* или A-сумируем и записваме $\sum_{n=1}^{\infty} a_n = s(A)$. Числото s се нарича *обобщена (в смисъл на Абел) сума* за реда (вж. [4, с. 7], [8, с. 64]).

Методът на Абел понякога се нарича и **метод на Поасон**, или **метод на Поасон-Абел**, след като Поасон е използвал същия метод за сумиране на редове на Фурие [4, с. 8].

3 Примерни педагогически ситуации

Пример 1 [4, с. 2, с. 6, с. 94]. За известния ред на Гранди $1 - 1 + 1 - 1 + \ldots$ намираме сумата му s по 3 различни начина:

- $s = 1 - 1 + 1 - 1 + \cdots = (1 - 1) + (1 - 1) + \ldots = 0$;
- $s = 1 - 1 + 1 - 1 + \cdots = 1 + (-1 + 1) + (-1 + 1) + \ldots = 1$;
- $s = 1 - 1 + 1 - 1 + \ldots = 1 - (1 - 1 + 1 - \ldots) = 1 - s \Rightarrow 2s = 1 \Rightarrow s = \frac{1}{2}$.

Така получаваме три различни суми за реда, т.е. $s = 0 = 1 = \frac{1}{2}$!, което води до

софизъм!

След анализиране на реда на Гранди според определение 1 получаваме за частичните му суми:

$$S_1 = 1,\ S_2 = 1-1 = 0,\ \ S_3 = 1-1+1 = 1,\ \ldots\ ,\ S_n = \begin{cases} 1, \text{ ако } n \text{ е нечетно} \\ 0, \text{ ако } n \text{ е четно} \end{cases},\ \ldots$$

откъдето следва, че редът е разходящ, понеже $\lim\limits_{n\to\infty} S_n$ не съществува (редицата има две точки на сгъстяване 0 и 1). Следователно трите манипулации, които извършваме с него, са недопустими и оттам следва грешното заключение като софизъм.

Ще покажем как методът на Чезаро позволява да присвоим „легално“ една от горните три стойности за сума на реда на Гранди. Разглеждаме редицата от средноаритметичните на частичните суми за реда:

$$c_1 = S_1 = 1,\ c_2 = \frac{S_1+S_2}{2} = \frac{1}{2},\ c_3 = \frac{S_1+S_2+S_3}{3} = \frac{2}{3}\ ,\ \ldots\ ,\ c_n = \frac{1}{n}\sum_{k=1}^{n} S_k, \ldots$$

$$S_k = \sum_{i=1}^{k} (-1)^{i-1} = \frac{(-1)^{k-1}+1}{2},\ k \geq 1$$

$$c_n = \frac{1}{n}\sum_{k=1}^{n} S_k = \frac{1}{n}\sum_{k=1}^{n} \frac{(-1)^{k-1}+1}{2} = \frac{1}{2n}\sum_{k=1}^{n}\left[(-1)^{k-1}+1\right] = \frac{1}{2n}\left(\sum_{k=1}^{n}(-1)^{k-1} + \sum_{k=1}^{n} 1\right)$$

$$c_n = \frac{1}{2n}\left(S_n + n\right) = \frac{S_n}{2n} + \frac{1}{2} \quad \Longrightarrow \quad \lim_{n\to\infty} c_n = \frac{1}{2}\ \ (\text{ понеже } |S_n| \leq 1)$$

Получихме, че по метода на Чезаро $1-1+1-1+\ldots = \frac{1}{2}$ (C).

Сега ще проверим какво се случва с реда на Гранди

$$1-1+1-1+\cdots = \sum_{k=1}^{\infty}(-1)^{k-1},$$

като приложим метода на Абел. Съставяме степенния ред

$$\sum_{k=1}^{\infty}(-x)^{k-1} = 1-x+x^2-x^3+\cdots,$$

който е сходящ за всяко $0 < x < 1$ и има сума $f(x) = \frac{1}{1+x}$. Тогава

$$\lim_{x\to 1^-} f(x) = \frac{1}{1+1} = \frac{1}{2}.$$

Потвърждава се, че редът на Гранди има същата сума и по метода на Абел, т.е. $1-1+1-1+\ldots = \frac{1}{2}$ (A). Получената сума по двата метода може да се използва, за да се разширят знанията за геометричния ред, т.е. да се направи негово продължение. При класическото сумиране знаем, че геометричният ред

$$\sum_{n=0}^{\infty} q^n = 1 + q^1 + q^2 + \cdots + q^n + \cdots$$

е сходящ със сума $S = \frac{1}{1-q}$ при $|q| < 1$, т.е. $1 + q^1 + q^2 + \cdots + q^n + \cdots = \frac{1}{1-q}$. Ако заместим в последното равенство с $q = -1$, получаваме отново $1-1+1-1+\ldots = \frac{1}{2}$.

Така чрез методите на Чезаро и Абел ние разширяваме областта на сходимост на геометричния ред от $(-1,\ 1)$ на $[-1,\ 1)$.

Пример 2 (вж. [5, с. 465]). Да разгледаме реда $1-2+3-4+5-\ldots$.

За да намерим сумата му s прилагаме два различни начина за комбиниране на членовете му по двойки:

- $s=(1-2)+(3-4)+(5-6)+\ldots=-1-1-1-\cdots=-\infty$;
- $s=1+(-2+3)+(-4+5)+\cdots=1+1+1+\cdots=\infty$.

Така стигаме до софизъм, според който положителната и отрицателната безкрайност са равни: $s=-\infty=+\infty$!

За частичните суми на реда имаме:

$S_1=1,\ \ S_2=1-2=-1,\quad S_3=1-2+3=2,\quad S_4=S_3-4=-2,$

$S_5=S_4+5=3,\ \ldots$

Лесно се съобразява, че $|S_n|\to\infty$ при $n\to\infty$, т.е. редицата от частичните суми е разходяща, следователно редът не е сходящ.

Да видим как бихме могли да присвоим „сума“ за реда чрез някой метод за сумиране. Прилагаме метода на Чезаро, като за целта разглеждаме редицата от средните аритметични на горните частични суми:

$$c_1=S_1=1, c_2=\frac{S_1+S_2}{2}=0,\ c_3=\frac{S_1+S_2+S_3}{3}=\frac{2}{3},\ c_4=0,\ c_5=\frac{3}{5},\ c_6=0,$$

$$c_7=\frac{4}{7},\ldots,\ c_n=\begin{cases}0, & \text{ако } n \text{ е четно}\\ \dfrac{n+1}{2n}, & \text{ако } n \text{ е нечетно}\end{cases},\ \ldots$$

Вижда се, че редицата от средните аритметични суми по Чезаро не е сходяща, тъй като има две точки на сгъстяване 0 и $\frac{1}{2}$ при $n\to\infty$. Следователно даденият разходящ ред няма обобщена сума в смисъл на Чезаро.

По метода на Абел съпоставяме на дадения ред степенния ред

$$\sum_{k=1}^{\infty}k(-x)^{k-1}=1-2x+3x^2-4x^3+\cdots$$

който е сходящ за всяко $0<x<\ 1$ и има сума $f(x)=\dfrac{1}{(1+x)^2}$. Тогава

$$\lim_{x\to1^-}f(x)=\frac{1}{(1+1)^2}=\frac{1}{4}.$$

Така получихме, че даденият ред не е сходящ в класическия смисъл, както и няма сума по метода на Чезаро, но има обобщена сума по метода на Абел, като

$$1-2+3-4+5-\ldots=\frac{1}{4}\ (A).$$

С този пример проверихме твърдението, че методът на Абел е „по-силен“ от метода на Чезаро (вж. [8, с. 66], [4, с. 108]).

Разгледаните от нас примери са не само математически софизми и не остават само в сферата на математическия анализ. Методите за сумиране на Чезаро и Абел в тях не правят разходящите редове сходящи, а могат да опишат смислено реални модели. Тези методи извличат устойчива средна стойност при динамични системи или при процеси, които осцилират и не са в покой, но са предсказуеми във времето.

Редът от Пример 1 се появява в системите за превключване (Switching systems – вж. [6]), които често генерират 2-периодични траектории (например реле, термостат и др.). Тези системи естествено водят до периодично превключване между два дискретни режима, т.е. до цикъл от вида $(x_1, x_2,\ x_1, x_2,\ \ldots)$. Специален случай е редицата $(1,\ -1,\ +1,\ -1,\ \ldots)$, която съответства на реда на Гранди (Пример 1). За него класическата граница не съществува, т.е. системата няма стационарна точка в обичайния смисъл. Но за реда съществува средната стойност по Чезаро, т.е. $\lim\limits_{n\to\infty} \dfrac{1}{n}\sum\limits_{k=1}^{n} x_k = \dfrac{x_1 + x_2}{2} = 0$, което означава, че трептенето в системата е симетрично и центрирано около нулата.

Частичните суми на реда $1-1+1-1+\cdots$, се колебаят между 0 и 1, а за редицата $(1,\ 0,\ 1,\ 0,\ \ldots)$ средната стойност на Чезаро $c_n \to \dfrac{1}{2}$ описва дългосрочното поведение на дискретната система чрез осредняване във времето (времето се разпределя равномерно между двете състояния).

Пример 2 има интересна интерпретация в икономическия „модел на паяжината“ (Cobweb model – вж. [3]). Той описва динамиката на цената и количеството и води до редици от вида $x_t = A(-\lambda)^t$. Когато системата е нестабилна, т.е. $|\lambda| > 1$, отклоненията от равновесието се описват чрез редицата $x_t = t(-1)^t$, която при сумиране води до разходящия ред $1 - 2 + 3 - 4 + \ldots$. Членът „$+n$“ се интерпретира като „увеличение“, а „$-n$“ като „намаление“, при което абсолютната стойност расте с времето. Степенният ред $\sum\limits_{t=1}^{\infty} x_t r^t,\ 0 < r < 1$ има икономическа интерпретация като настоящата стойност на осцилиращите отклонения. Това е точно Абеловата трансформация на реда и

$$1 - 2 + 3 - 4 + \ldots = \frac{1}{4},$$

което дава дисконтирания дългосрочен ефект на нестабилните колебания (ефект, оценен чрез намаляващи във времето тегла) и регуляризираната корекция на равновесието (корекция, получена чрез аналитично удължаване на иначе разходящия ред).

4 Заключение

В доклада представяме разходящите редове като естествена среда за възникване на математически софизми. В синергия с тях методите за сумиране на Чезаро и Абел илюстрират не само класическата дефиниция за сходимост на ред, а и как част от формалните алгебрични операции могат да бъдат коректно интерпретирани в по-обхватни и строго дефинирани понятия за сумиране. Представените примери, в които целенасочено се съчетават софизми и сумиращи методи, са ценен дидактически ресурс за развитието на критично и аналитично мислене у студентите, осмисляне на ролята на дефинициите и областта на приложимост на математическите твърдения. Разглеждането на разходящите редове през призмата на софизмите и методите за сумиране обогатява както теоретичната перспектива, така и по ефективен начин интегрира интуиция, формализъм и строгост в съвременното математическо образование. Примерите за разходящи редове, свързаните с тях софизми и обобщените

методи за сумиране не са само формални конструкции, а имат смислена интерпретация в широк кръг контексти, където класическите понятия за сходимост се оказват недостатъчни. В този смисъл те разкриват потенциала на обобщените сумиращи подходи като инструмент за описание и анализ на разнообразни реални процеси.

Литература

[1] J. Q. Chagas, J. A. T. Machado and A. M. Lopes. Overview in Summabilities: Summation Methods for Divergent Series, Ramanujan Summation and Fractional Finite Sums, *Mathematics,* **9** (2021), 2–38.

[2] Encyclopedia of Mathematics, „Summation methods“ [Online]. Available: `http://encyclopediaofmath.org/index.php?title=Summation_methods&oldid=48907`.

[3] G. Gandolfo. Economic Dynamics, 4th ed., Berlin, Germany: Springer, 2009.

[4] G. H. Hardy. Divergent Series. Oxford, Clarendon Press, 1949.

[5] K. Knopp. Theory And Application Of Infinite Series, Blackie And Son Limited, 1954.

[6] D. Liberzon. Switching in Systems and Control, Boston, MA, USA: Birkhäuser, 2003.

[7] E. Malkowsky, V. Rakočević. Summability methods and applications. Mathematical Institute of the Serbian Academy of Sciences and Arts, vol. 24, Belgrade, 2020.

[8] В. А. Илин, В. А. Садовничи, Бл. Х. Сендов. Математически анализ, втора част. София, Наука и изкуство, 1989. [V. A. Ilin, V.A.Sadovnichi, Bl. H. Sendov. Matematicheski analiz, vtora chast. Sofiya, Nauka i izkustvo, 1989.] (in Bulgarian)

[9] К. Колева. Активизиране на обучението по Висша математика чрез използването на софизми, *VI International Scientific and Technical Conference „Engineering. Technologies. Education. Security“*, V. Tarnovo, (2018), 256–259. [K. Koleva. Aktivizirane na obuchenieto po Vissha matematika chrez izpolzvaneto na sofizmi, *VI International Scientific and Technical Conference „Engineering. Technologies. Education. Security“*, V. Tarnovo, (2018), 256–259.] (in Bulgarian)

[10] К. Колева. „Приятната“ и „неприятната“ безкрайност при числовите редове, *Сборник доклади от Годишната университетска научна конференция на НВУ „Васил Левски“,* Велико Търново, (2025), 163–175. [K. Koleva. „Priyatnata“ i „nepriyatnata“ bezkraynost pri chislovite redove, *Sbornik dokladi ot Godishnata universitetska nauchna konferentsiya na NVU „Vasil Levski“*, Veliko Tarnovo, (2025), 163–175.] (in Bulgarian)

[11] К. Колева. Софизмите като средство за развитие на рефлексивната дейност на курсантите, *Сборник доклади от Годишната университетска научна конференция на НВУ „Васил Левски“,* Велико Търново, (2024), 117-129. [K. Koleva. Sofizmite kato sredstvo za razvitie na refleksivnata deynost na kursantite, *Sbornik dokladi ot Godishnata universitetska nauchna konferentsiya na NVU „Vasil Levski“*, Veliko Tarnovo, (2024), 117–129.] (in Bulgarian)

[12] Г. М. Фихтенгольц. Основы математического анализа, том 2, Москва, Наука, 1968. [G. M. Fihtengolts. Osnovy matematicheskogo analiza, tom 2, Moskva, Nauka, 1968.] (in Russian)

МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2026
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2026
Proceedings of the Fifty-Fifth Spring Conference
of the Union of Bulgarian Mathematicians
Tryavna, Bulgaria, April 5–9, 2026

STEAM WORKSHOP „MATHEMATICS IN THE VARNA NECROPOLIS, 5TH MILLENNIUM BC"

Tanya Marinova[1], Nataliya Borisova[2], Sevdalina Georgieva[3]
[1,2]Dobri Chintulov Primary School, Varna, Bulgaria,
[3]Technical University of Varna, Department of Language and Continuing Education and Sports
e-mails: [1]tanya.b.marinova@gmail.com, [2]borisova.nataliya.nb@gmail.com,
[3]sevdalina.m.georgieva@tu-varna.bg

This paper presents a mathematics-focused STEAM workshop grounded in the cultural and historical context of the Varna Chalcolithic Necropolis (5^{th} millennium BC). The proposed model organises learning around the examination of historical–archaeological hypotheses through mathematical reasoning. A set of interdisciplinary tasks has been developed to engage students with authentic data, including the calculation of percentages and proportions, the interpretation of charts, elementary probability and combinatorics, and geometric constructions. The instructional materials comprise worksheets, digital resources with real datasets hosted on an author-developed website, and 3D-printed replicas of selected artefacts. A unified framework for diagnosing learning outcomes is proposed, intended to be applicable across different grade levels. The workshop's effectiveness is supported by survey feedback from teachers, who rate it highly in terms of relevance, interest, and usefulness.

Keywords: STEAM education; mathematical modelling; data analysis; interdisciplinary tasks; teacher professional development; Varna Chalcolithic Necropolis

STEAM РАБОТИЛНИЦА „МАТЕМАТИКА ВЪВ ВАРНЕНСКИЯ НЕКРОПОЛ, V ХИЛ. ПР. ХР."

Таня Маринова[1], Наталия Борисова[2], Севдалина Георгиева[3]
[1,2]ОУ „Добри Чинтулов", Варна,
[3]Технически университет - Варна, Департамент по „Езиково и продължаващо обучение и спорт"
e-mails: [1]tanya.b.marinova@gmail.com, [2]borisova.nataliya.nb@gmail.com,
[3]sevdalina.m.georgieva@tu-varna.bg

В статията се представя STEAM работилница по математика, изградена върху културно-историческия контекст на Варненския халколитен некропол (V хил. пр. Хр.).

https://doi.org/10.55630/mem.2026.55.186-197
2020 Mathematics Subject Classification: 97M10, 97A30, 97B50, 97C70.

Моделът организира учебната дейност около проверка на историко-археологически хипотези чрез математически аргументи. Разработена е система от интердисциплинарни задачи за работа с реални данни, изчисляване на проценти и пропорции, анализ на диаграми, вероятности, комбинаторика и геометрични построения. Дидактическите средства включват работни листове, дигитални ресурси с реални данни, публикувани в авторски сайт и реплики на артефакти, изработени чрез 3D печат. Предложена е унифицирана система за диагностика на учебните постижения, приложима при работа в различни класове. Ефективността на работилницата е потвърдена чрез анкетна обратна връзка от учители, които я оценяват високо по отношение на актуалност, интерес и полезност.

Ключови думи: STEAM обучение; математическо моделиране; анализ на данни; интердисциплинарни задачи; продължаваща квалификация на учители; Варненски халколитен некропол.

В условията на компетентностно ориентирано обучение по математика акцентът се поставя върху моделиране, интерпретация на данни и аргументация. Това налага системно планиране на учебните дейности и целенасочена подкрепа на учителите при използването на интердисциплинарни задачи и оценяването на процеса на тяхното решаване [10]. Внедряването на STEAM дейности в училище показва, че за ефективна работа в клас са нужни методическа подготовка на учителите и добра организация на учебния процес. Необходима е междупредметна интеграция чрез обща изследователска задача и осигуряване на ресурси [1].

ТЕОРЕТИЧНА РАМКА И ИСТОРИЧЕСКИ КОНТЕКСТ

В настоящата статия компонентът „A“ се разглежда като Arts & Humanities – изкуства и хуманитарни науки, както и като културно-историческа рамка, която дава смисъл на данните и насочва тълкуването им. В този STEAM подход изкуствата подпомагат развиването на умения за работа с интердисциплинарни задачи, като насочват учениците да пренасят знания и подходи от една област в друга. Насърчава се и свързването на научните идеи с лични ценности, творчески решения и осъзнаване на последствията от избора. Така учебният процес става по-разбираем и ангажиращ. Постига се надхвърляне на рамките на отделните дисциплини и се подпомага формирането на социална отговорност чрез работа с реални данни и ситуации от ежедневието и обществения живот [12]. Интегрирането на културно наследство в STEAM създава предпоставки за обектно и изследователски ориентирано учене. Професионални програми, насочени към STEAM и културно наследство, подчертават, че достъпните за учениците изследователски дейности и учителската готовност са ключови фактори за успешно прилагане на подобни практики [10]. Когато културното наследство се използва като основа за формулиране на STEAM задачи и за обсъждане на резултатите, често се наблюдава по-висока ангажираност на учениците и по-лесно осъществяване на междупредметни връзки [7].

Обект на изложението е учебният процес по математика в прогимназиален и гимназиален етап, реализиран чрез STEAM дейности, в които данни и артефакти от културното наследство служат като контекст за математически задачи. Предмет на статията е STEAM модел, чрез който учениците изследват и проверяват историко-археологически хипотези, свързани с Варненския некропол, като използват матема-

тически аргументи. Целта е да се представи система от интердисциплинарни задачи в контекста на Варненския некропол и модел за проследяване и анализ на постигнатите учебни резултати на учениците.

ВАРНЕНСКИЯТ НЕКРОПОЛ КАТО STEAM РЕСУРС

Като културно-исторически контекст е избран Варненският халколитен некропол (V хил. пр. Хр.), който предоставя богата база от артефакти и количествени данни, подходящи за създаване на учебни задачи. Археометричните изследвания върху златни сплави от археологически находки показват как обективни измерими характеристики (напр. състав и процентни съотношения) могат да се превърнат в данни за класификация, сравнение и аргументация в образователни ситуации [5]. Варненският халколитен некропол е праисторически обект, открит през 1972 г. в района на Варненското езеро, близо до град Варна. Некрополът е датиран към средата и втората половина на V хил. пр. Хр. и се свързва с археологическата култура Варна [4]. През 1976 г. в бр. 66 на „Държавен вестник" Варненският некропол е обявен от Министерството на културата за археологически паметник от национално значение. Още с откриването му първите изследователи – Иван Иванов, Мария Гимбутас, Колин Ренфрю и др. – поставят въпроса за зараждането на европейската цивилизация през V хил. пр. Хр., като изтъкват аргументите за организирано общество и икономически статус [3]. Варненският некропол е един от немалкото къснохалколитни некрополи, проучени на територията на североизточната част на Балканския полуостров, но неговите особености продължават да занимават учените в търсенето на обяснението на „феномена Варна".

Разбира се, на първо място интересът към този блестящ паметник е предизвикан от разнообразието и многобройността на гробните дарове. Сред тях най-голям интерес привличат златните предмети. Те са над 3 000 на брой, а общото им тегло надвишава 6 кг., като теглото на златото само в гробове 4, 36 и 43 е над 4 кг. Досега за V хил. пр. Хр. другаде не е известна подобна концентрация на изделия от злато. Теглото и количеството на златните находки от Варненския некропол надвишават неколкократно същите показатели на всички открити досега синхронни предмети от този благороден метал в целия свят. Това, както и големият брой медни изделия – над 160, позволяват да приемем, че в района около днешния град Варна е функционирал производствен център за металообработка. Наличието му поставя нови аспекти в социално-икономическото развитие – рударството, металургията и свързаният с тях търговски обмен, създаващи предпоставки за промяна в обществената структура и концентрация на власт [9].

Посочените констатации сочат с голяма сигурност възможността за съществуване на добре организирана общност на прага на държавната формация [4]. В хронологическия контекст тази протодържавна формация изпреварва с повече от хилядолетие първите трайни държавни общества на Древния Изток.

Дигиталните технологии разширяват възможностите за визуализация и анализ и улесняват включването на обекти от културното наследство в учебни задачи [8]. Технологиите за 3D реконструкция, съчетани с виртуални среди, улесняват възприемането на формите и пропорциите, като създават възможност за работа с реалистични модели на артефактите [6]. За работа с данни и визуални ресурси се използват дигитални колекции и описания на находки, както и авторски сайт с учебни материали

(линк в Бележки). За да се превърнат тези ресурси в устойчиви STEAM практики, са необходими подготовка на учители и методическа подкрепа [10].

МЕТОДИЧЕСКИ МОДЕЛ И ОРГАНИЗАЦИЯ НА STEAM ДЕЙНОСТИ

Моделът цели учениците да:

1. **моделират и решават** приложни задачи, свързани с данни и ситуации от Варненския халколитен некропол;
2. **интерпретират и анализират** данни от таблици / диаграми и **извеждат** количествени изводи, релевантни към разглежданите хипотези;
3. **изчисляват и сравняват** вероятности и **оценяват** как резултатите подкрепят или опровергават дадено твърдение;
4. **аргументират и обосновават** исторически хипотези, като **свързват** математически резултати с исторически факти и изводи.

Дейността се осъществява в следните етапи:

1. Мотивация чрез поставяне на историческа хипотеза, свързана с конкретен факт или артефакт от Варненския некропол.
2. Решаване на система от задачи с предоставени данни.
3. Проверка на формулираните хипотези, чрез математически аргументи и формулиране на изводи.

Дидактически средства

Инструментариумът на STEAM работилницата „Математика във Варненския некропол" е организиран в платформата WIX, в която в тематични модули, съдържащи интердисциплинарни задачи, са прикачени работни листове, хипервръзки към видео файлове, AI и приложен софтуер; картинна линия на времето; тематични исторически карти, изображения, таблици, диаграми и схеми. За STEAM дейностите са изработени реплики на артефакти от некропола, изпълнени на 3D принтер.

СИСТЕМА ОТ ИНТЕРДИСЦИПЛИНАРНИ ЗАДАЧИ

Задачите са организирани в три ключови направления на изследвания обект – хронология (Модул 1), социално-икономически анализ (Модул 2) и геометрични конструкции (Модул 3). Модулите могат да се разглеждат като единен, последователен цикъл или да се интегрират избирателно в учебния процес, в зависимост от спецификата на учебното съдържание и възрастта на учениците.

МОДУЛ 1. Култура Варна (V хил. пр. Хр.) в историческото време и пространство

ИСТОРИЧЕСКА ХИПОТЕЗА: Халколитното общество, живяло край Варна в V хил. пр. Хр., е създало протодържавна форма повече от хилядолетие преди първата трайна държава в света – Египет (3 200 г. пр. Хр.).

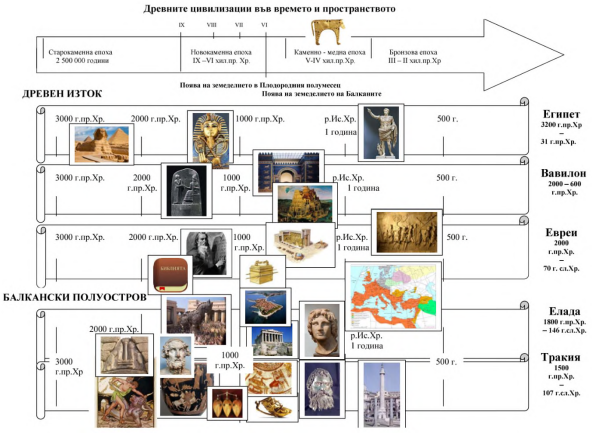
ЗАДАЧИ ЗА ПРОВЕРКА НА ХИПОТЕЗАТА ЧРЕЗ МАТЕМАТИЧЕСКИ АРГУМЕНТИ:

Задачата изисква учениците да определят мястото на Варненския некропол на картинната линия на времето (*Фигура 1*), като пресметнат:

а/ Колко години са изминали от Варненския некропол (V хил. пр. Хр.) до създаването на Египет (3 200 г. пр. Хр.) ?

б/ Колко години са изминали от Варненския некропол до основаването на Вавилон (1894 г. пр. Хр.) ?

в/ Колко години са изминали от Варненския некропол (V хил. пр. Хр.) до днес?



Фигура 1

Очаквани резултати и изводи:

Учениците доказват хипотезата, като разчитат линията на времето с помощта на изображенията и посочват мястото на Варненския некропол върху нея. Резултатите от направените изчисления доказват, че халколитното общество, живяло край Варна в V хил. пр. Хр., създало прото-държавна форма, е по-старо от Древен Египет с около 1 300 години, от Вавилон – с около 2 606 г., а от Варненския некропол до днес са изминали около 6 525 г.

МОДУЛ 2. Хората от Варненския некропол (V хил. пр. Хр.) са изградили високо развито общество

ИСТОРИЧЕСКА ХИПОТЕЗА: Хората от Варненския некропол (V хил. пр. Хр.) са изградили високо развито общество с изградена социална йерархия и лидери, религиозни вярвания, първи познават и обработват злато (метали) в света.

ЗАДАЧИ ЗА ПРОВЕРКА НА ХИПОТЕЗАТА, ЧРЕЗ МАТЕМАТИЧЕСКИ АРГУМЕНТИ:

Тема: Процент, 5. клас

Учениците анализират данните за артефактите, за да попълнят *Таблица 1.* и докажат йерархията в обществото на хората от Варненския некропол.

В некропола са открити керамични изделия, златни предмети, медни сечива и кремъчни инструменти. Броят им според материала е даден на диаграмата на *Фигура 2.*

Учениците доказват значението на златото спрямо другите материали в гробните дарове, като изчислят процентното съотношение на материалите.

Очаквани резултати и изводи:

Разпределението на богатството във Варненския халколитен некропол ясно показва общество с изразена йерархия: 76% от цялото злато е концентрирано само в 4 от общо 294 гроба, а общото съотношение на предметите – 77% златни, 15% керамични, 5% медни, 3% кремъчни – свидетелства за напреднала металургия и специален

Гроб №	Брой златни предмети	Общо тегло в грама	Злато в %
1	217	1094,35	
4	348	1554,7	
36	857	782,16	
43	1003	1524,39	

Таблица 1



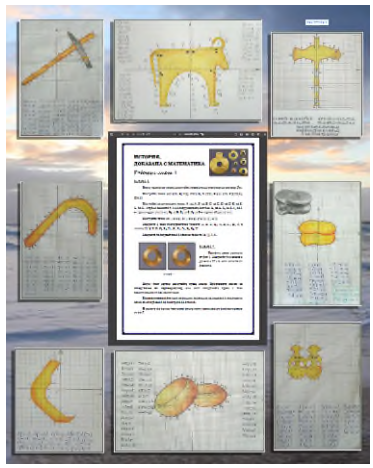
Фигура 2

статус на златото.

Тема: Декартова координатна система, 6. клас

Учениците конструират в Декартова координатна система избрани от тях артефакти от некропола.

Очаквани резултати: Учениците се насочват в избора си към артефакти, които са символи на власт *(Фигура 3)*.



Фигура 3

Тема: Вероятности и статистика, 7. клас

В задачата се прилага вероятностен модел с цел да се аргументира, че бикчетата са сред най-редките златни предмети в некропола и практически не се срещат при случаен избор. Броят на златните предмети е 3078, като 3 от тях са златни бикчета.

Очаквани резултати и изводи: Общо златни предмети: $N = 3078$, златни бикчета: $k = 3$.

Вероятност да се избере бикче: $P(\text{бикче}) = \dfrac{k}{N} = \dfrac{3}{3078} \approx 0,000975 \approx 0,0975\%$

Вероятност да се избере предмет, който не е бикче: $P(\text{не бикче}) = \dfrac{N-k}{N} = \dfrac{3075}{3078} \approx 0,999 \approx 99,9\%$.

Рядкостта на златните бикчета (под 0,1% шанс да бъдат открити) и вероятността под 1% сред три предмета да се падне поне едно показват, че те са силно селектирани ритуални символи.

Тема: Комбинаторика с условия, 8. клас

Учениците анализират наличните данни от некропола. Обосновават твърдението, че при наличие на бикче в даден гроб то обикновено се среща в съчетание с други ритуални предмети. Използват това, че в гроб № 36 има 857 златни предмета, от които 2 са бикчета.

Очаквани резултати и изводи: Приемат, че трите предмета са избрани случайно, т.е. всяка тройка от 3 различни предмета измежду 857-те е еднакво вероятна. Търсят вероятността в избраната тройка да има поне едно бикче.

Общо комбинации: $C_{857}^{3} = \dfrac{857 \cdot 856 \cdot 855}{6} = 104\ 536\ 860$

Комбинации без бикчета: $C_{855}^3 = \dfrac{855 \cdot 854 \cdot 853}{6} = 103\ 805\ 835$

Комбинации с поне 1 бикче: $C_{857}^3 - C_{855}^3 = 104\ 536\ 860 - 103\ 805\ 835 = 731\ 025$

Вероятност: $P(\text{поне 1 бикче}) = \dfrac{73\ 025}{104\ 536\ 860} \approx 0,006996 \approx 0,7\%$

Шансът да се избере поне едно бикче сред 3 предмета е около 0,7%, тоест под 1%. Това подкрепя тезата за силна селекция и целенасочено ритуално значение на бикчетата.

Тема: Пермутации, 9. клас

Учениците изследват, че подредбата на предметите в гроб № 43 е ритуално кодирана, а не случайна. В ритуална композиция има: 4 еднакви златни гривни, 1 гривна, изработена от черупка на мида *Spondylus,* 1 брадва-скиптър.

Очаквани резултати и изводи: Пермутации с повторения: $P = \dfrac{6!}{4! \cdot 1! \cdot 1!} = \dfrac{720}{24 \cdot 1 \cdot 1} = 30$

Ако всички предмети бяха различни: $P = 6! = 720$

Ограниченията в броя на възможни подредби показват, че предметите са разположени по ритуален модел, вероятно с цел символика, статус или култова функция.

Тема: Класическа вероятност и комбинаторика, 10. клас

Задачата изисква учениците да обосноват, че в гроб №43 е представена ясно изразена социална йерархия, като се позоват на разнообразието и количественото разпределение на златните артефакти, В гроб №43 има 990 златни предмета от 28 различни типа. Археолог избира 3 предмета, без значение от реда. Колко различни комбинации от типове може да избере? Колко вариации (с подредба) може да избере?

Очаквани резултати и изводи: $C_{28}^3 = \dfrac{28!}{3! \cdot 25!} = 3276$, $V_{28}^3 = 28 \cdot 27 \cdot 26 = 19\,656$

Подредбата на артефактите следва ограничени ритуални модели, а голямото разнообразие от комбинации разкрива сложна социална структура.

Тема: Условна вероятност и статистика, 11. клас

Учениците анализират разпределението на артефактите в некропола, за да обосноват, че появата на скиптър е статистически свързана с гробове, съдържащи повече от 100 златни предмета. Само 4 гроба съдържат скиптри. От общо 294 гроба 5 съдържат над 100 златни предмета.

Очаквани резултати и изводи:

R**:** „гробът е с над 100 златни предмета“, S**:** „гробът съдържа скиптър“

Брой гробове: N=294. Брой гробове с R: nR=5. Брой гробове с S: nS=4

Наблюдение: всички 4 гроба със S са сред тези 5 с R.

При допускане за случайно (независимо) разпределение на скиптрите между 294-те гроба, вероятността и четирите гроба със скиптър да попаднат сред само петте гроба с над 100 златни предмета е: $P \approx 0,0000000164$

$P(R) = nR/N = 5/294$, $P(S) = nS/N = 4/294$, $P(S \cap R) = 4/294$, $P(S \mid R) = 0,8 = 80\%$ Условна вероятност $P(S|R^-) = 0$. Ако S и R бяха независими, щеше да важи: $P(S \mid R) = P(S)$. Но тук $P(S) \approx 0,0136$, $P(S \mid R) = 0,8$, т.е. $P(S \mid R) \neq P(S)$. Следователно събитията „гробът е богат“ и „гробът съдържа скиптър“ са зависими.

Наличието на скиптър не е резултат от случайни фактори, а представлява статистически значим индикатор, свързан с гробове, съдържащи над 100 златни пред-

мета. Това подкрепя интерпретацията, че скиптърът е маркер на високо социално положение или специфичен елитен статус в рамките на разглежданата общност.

Тема: Статистически модели и интерпретации, 12. клас

В задачата учениците анализират разпределението на златните предмети по гробове и обосновават, че то следва асиметрично разпределение, характерно за социални системи.

Данни от 10 гроба: Брой предмети: 5; 8; 12; 15; 20; 25; 30; 50; 100; 990.

Очаквани резултати и изводи: Изчислена средна стойност:

$$x^{-} = \frac{5 + 8 + \cdots + 990}{10} = 127,5$$

Изчислена медиана: Медиана $= \frac{20 + 25}{2} = 22,5$

Сравнени средна стойност и медиана $\rightarrow x^{-} >$ медиана

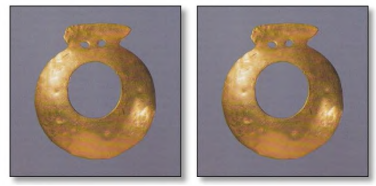
Асиметричното разпределение, при което средната стойност значително превишава медианата, допълнително доказва наличие на малоброен, но изключително богат слой. Всички тези данни очертават високо организирано общество с преддържавни характеристики още през V хил. пр. Хр.

МОДУЛ 3. Геометрични конструкции и измервания с реплики на артефакти.

ХИПОТЕЗА: Халколитното общество, създало Варненския некропол (V хил. пр. Хр.), е използвало някои от гробните дарове като измервателни уреди или геометрични еталони. [11]

ИЗСЛЕДОВАТЕЛСКИ ДЕЙНОСТИ ЗА ПРОВЕРКА НА ХИПОТЕЗАТА ЧРЕЗ МАТЕМАТИЧЕСКИ АРГУМЕНТИ:

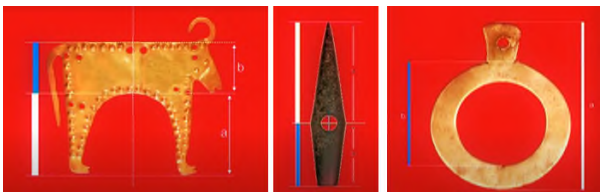
В задачата учениците конструират прост чертожен инструмент от копия на артефактите на Фигура 4, свързани през отворите с нишка с дължина 10 cm. С него се построява перпендикуляр към дадена права, а чрез промяна на дължината на нишката се изследват варианти за построяване на симетрала на отсечка и се определя какъв геометричен инструмент реализира конструкцията.



Фигура 4

Учениците измерват оцветените отсечки от изображенията на Фигура 5, изчисляват зададените отношения и обсъждат връзката им с известна математическа константа. Формулират предложения за използване на златната пластина при построяване на успоредни и перпендикулярни прави и за ролята на костната апликация като еталон за изчертаване на перпендикуляри (Фигура 6).

Очаквани резултати и изводи: Учениците създават вариант на чертожен инструмент – пергел и установяват, че двете бикчета са пропорционални фигури. Отношението на елементите им отговаря на легендарното златно сечение. Отворите на златната пластина и костната апликация позволяват да се изчертаят успоредни и перпендикулярни прави. Учениците изразяват оригинални предположения за какво са служели разглежданите предмети, но независимо от предназначението им, убе-



Фигура 5



Фигура 6

дително откриват математическите прозрения на хората, живели край град Варна преди близо 7 000 години.

ДИАГНОСТИКА НА УЧЕБНИТЕ ПОСТИЖЕНИЯ НА УЧЕНИЦИТЕ

Предложената система от интердисциплинарни задачи е предназначена за ученици от прогимназиален и гимназиален етап на обучение и представлява задачи, съобразени с учебното съдържание, а хипотезите са свързани с Варненския халколитен некропол. Настоящата статия предлага унифициран модел за проследяване на резултатите, приложим при използване в различни класове.

Резултатите се проследяват чрез:

- анализ на ученическите решения: правилност, последователност на стъпките, наличие на извод и аргументация.
- структурирано педагогическо наблюдение по време на работа по задачите.

Критерии и показатели

За всеки индикатор учителят отбелязва степен на проявление и предоставя кратко доказателство (елемент от решението, реплика или действие). Използва се тристепенна скала: 0 – не се наблюдава; 1 – частично; 2 – наблюдава се уверено.

Критерий 1. Моделиране и решаване на приложни задачи в контекста на Варненския некропол.

Показатели: коректно извлечени данни от условието, избран подход/модел, завършено решение.

Критерий 2. Интерпретация и анализ на данни (таблица/диаграма) и извеждане на количествени изводи, релевантни към разглежданите хипотези.

Показатели: сравнения, проценти/отношения, формулиран количествен извод към хипотезата.

Критерий 3. Оценка на резултата: изчисляване, сравняване на вероятности и оценяване дали резултатите подкрепят/опровергават твърдение.

Показатели: изброяване/структуриране на случаи, вероятностен извод („по-вероятно/по-малко вероятно“) и оценка на твърдението.

Критерий 4. Аргументация на историческа хипотеза чрез свързване на математически резултати с исторически факти и изводи.

Показатели: заключение от типа „резултатът подкрепя/не подкрепя хипотезата, защото. . .“.

ПРИЛОЖИМОСТ, ОГРАНИЧЕНИЯ И ПЕРСПЕКТИВИ

Работилницата „Математика във Варненския некропол“ предлага широки възможности за интегриране в обучението. В прогимназиален етап тя подпомага усвояването на симетрия, пропорции и проценти, вероятности, работа с таблици и диаграми, както и геометрични построения. В часовете по история материалите се използват при теми за Праисторията и ранните цивилизации чрез анализ на артефакти и обсъждане на данни. В гимназиален етап работилницата се вписва в профилираната подготовка по математика (статистика, комбинаторика, геометрия) и в исторически модули, свързани със социални структури и технологични практики. Макар да е допълващ, а не основен учебен модул, тя развива ключови компетентности – критическо мислене, анализ на данни, интерпретация на източници, работа в екип и елементи на изследователски подход. Перспективите на модела включват разработване на допълнителни учебни ресурси и утвърждаване на Варненския некропол като устойчив пример за работа с културно-историческо наследство в междупредметна среда. В този контекст математиката се използва както за проверка на твърдения и аргументиране на изводи, така и за визуализация и по-добро осмисляне на данните.

ОБРАТНА ВРЪЗКА ОТ УЧИТЕЛИ

На XXIV Регионална научно-практическа конференция „Математика и информатика – реалности и перспективи“ (28–30 ноември 2025 г.), организирана от СМБ – секция Варна, работилницата беше част от програмата с практически сесии. Проведено е анкетно проучване сред 194 учители по математика и информатика за оценката на полезността на работилниците. Разработката е оценена като най-актуална (75%), най-интересна (82%) и най-полезна (79%). В отворените отговори е описана като „любопитен поглед към историята през очите на математиката“, „богато съдържание, реално приложимо във всички възрасти“ и „чудесно съчетание между история и математика“. Подчертава се практическата насоченост и вложеният труд на авторите. Резултатите потвърждават високата оценка на учителите за приложимостта и потенциала на работилницата като ресурс за интердисциплинарни уроци.





ЗАКЛЮЧЕНИЕ

Моделът на работилницата „Математика във Варненския некропол“ показва как културно-исторически обект с висока значимост, Варненският халколитен некропол, може да се използва като основа за STEAM дейности. В тези дейности математиката се прилага като инструмент за проверка на хипотези и аргументация на изводи. Системата от интердисциплинарни задачи подпомага свързването на математически знания като моделиране, работа с данни и вероятности с историческа интерпретация. По този начин се развиват умения за доказателствено мислене и обосновано представяне на резултати. Предложеният модел за проследяване осигурява практичен механизъм за диагностика на учебните постижения чрез анализ на решенията и наблюдение. Създават се и условия за сравнимост на резултатите при прилагане в различни класове. Като следваща стъпка се предвижда изследване за проверка на надеждността и приложимостта на индикаторите и за оценка на ефекта на модела.

БЛАГОДАРНОСТ

С благодарност към Регионален исторически музей – град Варна в лицето на д-р Владимир Славчев за оказаното съдействие.

Литература

[1] A. K. Amanova, L. A. Butabayeva, G. A. Abayeva, A. N. Umirbekova, S. K. Abildina, A. A. Makhmetova. A systematic review of the implementation of STEAM education in schools, *Eurasia Journal of Mathematics, Science and Technology Education* 21(1) (2025), em2568, doi:10.29333/ejmste/15894.

[2] S. Chavdarova-Kostova, [*Handbook for implementing the competency-based approach in the training of future teachers*], Sofia, MON, 2022 (in Bulgarian).

[3] I. Ivanov, M. Avramova. 2000. Varna Necropolis. The Dawn of European Civilization. Sofia, Agató (in Bulgarian)

[4] R. Krauss, C. Schmid, D. Kirschenheuter, J. Abele, V. Slavchev, B. Weninger, Chronology and development of the Chalcolithic necropolis of Varna I, *Documenta Praehistorica* 44 (2017), 282–305, doi:10.4312/dp.44.17.

[5] V. Leusch, M. Brauns, E. Pernicka, Precise and accurate analysis of gold alloys: Varna, the earliest gold of mankind—a case study, in: A. L. Dussubieux, M. Golitko, B. Gratuze (Eds.), *Recent Advances in Laser Ablation ICP-MS for Archaeology*, Berlin, Heidelberg, Springer, 2016, 95–113, doi:10.1007/978-3-662-49894-1_7.

[6] I. Liritzis, P. Volonakis, S. Vosinakis, 3D and VR visualization of cultural heritage, *Applied Sciences* 11 (2021), 3635, doi:10.3390/app11083635.

[7] L. R. Listiyani, I. Wilujeng, S. Suyanto, D. H. Pratama, EthnoSTEM-based learning tools: Connecting cultural heritage with STEM education, *International Electronic Journal of Elementary Education* 17(4) (2025), 593–609, doi:10.26822/iejee.2025.402.

[8] D. Psarros, M. I. Stamatopoulos, C.-N. Anagnostopoulos, Information technology and archaeological excavations: A brief overview, *Scientific Culture* 8(2) (2022), 147–167, doi:10.5281/zenodo.6323149.

[9] R. Rusev, V. Slavchev, G. Marinov, Y. Boyadzhiev, [*Varna – Prehistoric Center of Metalworking*], Varna, IK Dangrafik, 2010 (in Bulgarian).

[10] A. Sofianidis, E. Petridou, E. Stylianou, et al., Bridging STEAM and cultural heritage through inclusive inquiry: The SciArt professional development program, *Education Sciences* 15(11) (2025), 1551, doi:10.3390/educsci15111551.
[11] H. Smolenov, H. Michailov, *The Lost Aurolithic Civilization? Codes from a Black Sea Atlantis*, Sofia, Magoart, 2010.
[12] P. C. S. Taylor, E. Taylor, Transformative STEAM education for sustainable development, in: S. Rahmawati, P. C. S. Taylor (Eds.), *Empowering Science and Mathematics for Global Competitiveness. Proceedings of the Science and Mathematics International Conference (SMIC 2018)*, London, CRC Press, 2019, 118–124.

БЕЛЕЖКИ

В статията са използвани:

- Varna Chalcolithic Necropolis (I–III, V millennium BC), (достъп: 29.12.2025).
- T. Marinova, N. Borisova, `https://borisovanataliyanb.wixsite.com/varnenskinekropol`
- Darzhaven vestnik. (1976). Br. 66.
- BNT Varna, [50 godini BNT Varna: Taynite na Varnenskoto zlato – kultura ili tsivilizatsiya], онлайн видео, (достъп: 29.12.2025). `https://youtu.be/HERpziESc9Q?si=SFyiAcgid_ArvLbK`
- M. Gimbutas, [Intervju], Narodno delo, No. 181 (9635), 31 July 1976 (in Bulgarian).
- Gyucha, Attila, Parkinson, William. First kings of Europe: Exibition Catalog, (2023)
- N. Borisova, Drevnite civilizatsii vav vremeto i prostranstvoto, Ponyatiya, tsennosti, promeni. Istoriyata: Vreme i realnosti, Vol. 13, Shumen: ShU "Ep. K. Preslavski", 2018 (in Bulgarian).

МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2026
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2026
Proceedings of the Fifty-Fifth Spring Conference
of the Union of Bulgarian Mathematicians
Tryavna, Bulgaria, April 5–9, 2026

THE ELLIPSE, PARABOLA, AND HYPERBOLA AS SECTIONS OF A ROTATIONAL CONE WITH A PLANE

Irena A. Parvanova[1], Yana Kancheva[2]
[1]Department of Applied Mathematics and Informatics, Technical University of Sofia, Bulgaria,
[2]Dept. of Applied Geodesy, Faculty of Geodesy, University of Architecture, Civil Engineering and Geodesy, Sofia, Bulgaria
e-mails: [1]irena.parvanova@tu-sofia.bg, [2]kancheva_fgs@uacg.bg

The paper examines problems illustrating the three main cases of sections of a rotational cone with a plane, solved by the methods of descriptive geometry. The examples are presented in cabinet projection and can be useful in illustrating results achieved by the means of analytical geometry and in teaching descriptive geometry to university students of engineering majors.

Keywords: descriptive geometry; parallel projection; plane sections of a rotational cone

ЕЛИПСАТА, ПАРАБОЛАТА И ХИПЕРБОЛАТА КАТО СЕЧЕНИЯ НА РОТАЦИОНЕН КОНУС С РАВНИНА

Ирена Първанова, Яна Кънчева
[1]Факултет „Приложна математика и информатика“, Технически университет – София
[2]Катедра „Приложна геодезия“, Геодезически факултет, Университет по строителство, архитектура и геодезия, София
e-mails: [1]irena.parvanova@tu-sofia.bg, [2]kancheva_fgs@uacg.bg

Статията разглежда задачи, илюстриращи трите основни случая на сечения на ротационен конус с равнина, решени с методите на дескриптивната геометрия. Показаните примери са изпълнени в кабинетна проекция и могат да бъдат от полза при онагледяването на резултати, постигнати със средствата на аналитичната геометрия и в обучението по дескриптивна геометрия на студенти от инженерните специалности на висшите учебни заведения.

Ключови думи: дескриптивна геометрия, успоредно проектиране, равнинни сечения на ротационен конус

https://doi.org/10.55630/mem.2026.55.198-204

2020 Mathematics Subject Classification: 51N05, 51M04, 53A04, 51M04, 53A04.

Въведение: Темата „Конични сечения“ присъства във всички курсове по Аналитична и Дескриптивна геометрия във висшите учебни заведения, а в последните години е част и от учебните програми по математика в средния курс за учениците – профил „Математика“. В тази статия авторите показват три примера, изработени в кабинетна проекция, като се надяват направените чертежи да бъдат от полза при онагледяването на важните елементи на елипсата, параболата и хиперболата и начина на намирането им при пресичане на ротационен конус с равнина.

Изложение: Елипсата, параболата и хиперболата са документирано представени като сечения на ротационен конус с равнина за първи път от великия немски художник, математик и изкуствовед Албрехт Дюрер в първата математическа книга, издадена на немски език – „Underweysung der messung mit dem zirckel und richtscheyt in Linen ebnen unnd gantzen corporen“ , в далечната 1514 година. За целта Дюрер използва метода на спомагателните успоредни равнини и ортогонално проектиране върху две взаимно перпендикулярни равнини – метод, придобил впоследствие известност като Монжова проекция (най-вече в държавите от източния блок). Трите показани в статията примери са решени в кабинетна проекция с цел да се постигне добра нагледност на получените резултати. Кабинетната проекция е вид наведена аксонометрия, при която проекционната (аксонометрична) равнина се поставя успоредна или съвпадаща с втора координатна равнина ν. По този начин фигурите, които се намират в ν и в равнини, успоредни на нея, се изобразяват в истинския си вид. Секущата равнина α и в трите примера е поставена перпендикулярна на втора координатна равнина с цел сечението да бъде намерено по най-лесен начин и след построяване му равнината да бъде завъртяна до съвпадане с ν и да бъде показан истинският вид на получената крива. За намирането на точки от сечението е използвана вторичната проекция на конуса във втора координатна равнина и прободите на образователните на конуса със секущата равнина. Изработването на чертежите изисква познаване на свойствата на успоредното проектиране и основни конструкции, използвани в дескриптивната геометрия, които могат да бъдат намерени в [3] и [4]. Подробно описани и решени задачи за изобразяване на сечението на ротационен конус с равнина в монжова проекция могат да бъдат намерени в [1], [2] и [5].

Построенията, направени при изработването на първия чертеж, са описани подробно, като са отбелязани най-важните характеристики на получената крива. Към изработването на втория и третия чертеж са отбелязани важните разлики и характерните особености на другите две сечения.

Пример 1. В кабинетна проекция да се изобрази ротационен конус с връх $V(3; 14; 8)$ и основа в първа координатна равнина μ с радиус $R = 3$. Да се изобрази сечението на конуса с равнината $\alpha[8; \infty; 6]$ и да се покаже истинският му вид.

Построенията са извършени в следната последователност:

1. Изобразен е аксонометричният кръст на кабинетна проекция и са нанесени дадените точка V и дирите на равнината α. Тъй като равнината α е успоредна на оста y на координатната система, то тя е перпендикулярна на втора координатна равнина ν и тогава $n'_\alpha \equiv \alpha'_2$. Това означение показва, че вторите вторични проекции на всички елементи от равнината α са върху нейната втора диря.

2. Построена е проекцията на основата на конуса – елипсата k' с център V'_1,

определена от двойката спрегнати диаметри $E'F'$ и $G'H'$ – проекции на диаметрите на окръжността, успоредни на координатните оси на първа координатна равнина μ.

3. Построени са контурните образователни на конуса – допирателните към елипсата, минаващи през проекцията на върха на конуса – точката V'. Определена е видимата част на основата.

4. Намерена е втората вторична проекция на конуса – равнобедрен триъгълник $E'_2F'_2V'_2$. Тъй като секущата равнина е перпендикулярна на ν, то търсеното сечение във втора координатна равнина се вижда като отсечка – част от втората диря на равнината α.

Ъгълът $\varphi = \sphericalangle(n'_\alpha, x')$ е линеен ъгъл на двустенния ъгъл $\sphericalangle(\alpha, \mu)$.

Ъгълът на наклона на образователните на конуса спрямо равнината на основата му е означен с ϕ, $\phi = \sphericalangle(n'_\alpha, x')$.

От връзката между тези два ъгъла се определя видът на сечението, като възможностите са три:

- При $\varphi < \phi$ сечението е елипса или част от елипса. Тогава секущата равнина пресича всички образователни на конуса или техните продължения.
- При $\varphi = \phi$ сечението е парабола. Тогава секущата равнина е успоредна на една образователна на конуса и пресича останалите.
- При $\varphi > \phi$ сечението е хипербола. Тогава секущата равнина е успоредна на две образователни на конуса и пресича останалите.

В случая сечението е елипса, тъй като $\varphi < \phi$.

5. Намерени са пресечните точки на втората диря на равнината α с бедрата на триъгълника $E'_2F'_2V'_2$ – точки A'_2 и B'_2, като $|A'_2B'_2| = 2a$ е дължината на голямата ос на елипсата.

Голямата ос на елипсата лежи върху пресечната права s на равнина β, минаваща през оста на конуса и перпендикулярна на секущата равнина α с равнината α. Тъй като оста на симетрия на търсеното сечение – правата s е успоредна на втора координатна равнина, то проекциите на отсечките, лежащи на нея, са с реалната си дължина.

6. Намерена е средата на отсечката $A'_2B'_2$ – $C'_2 \equiv D'_2$. Точките C и D са краищата на малката ос на елипсата. Във втора координатна равнина ν малката ос се проектира в точка, тъй като е перпендикулярна на нея.

За намиране на допълнителни точки от сечението могат да се намерят още прободи на образователни на конуса с равнината α, както и да се използва съответствието между проекцията на основата на конуса и проекцията на сечението. Това съответствие е хомология с център – точка V', ос – m'_α и двойка съответни точки – F' и A'.

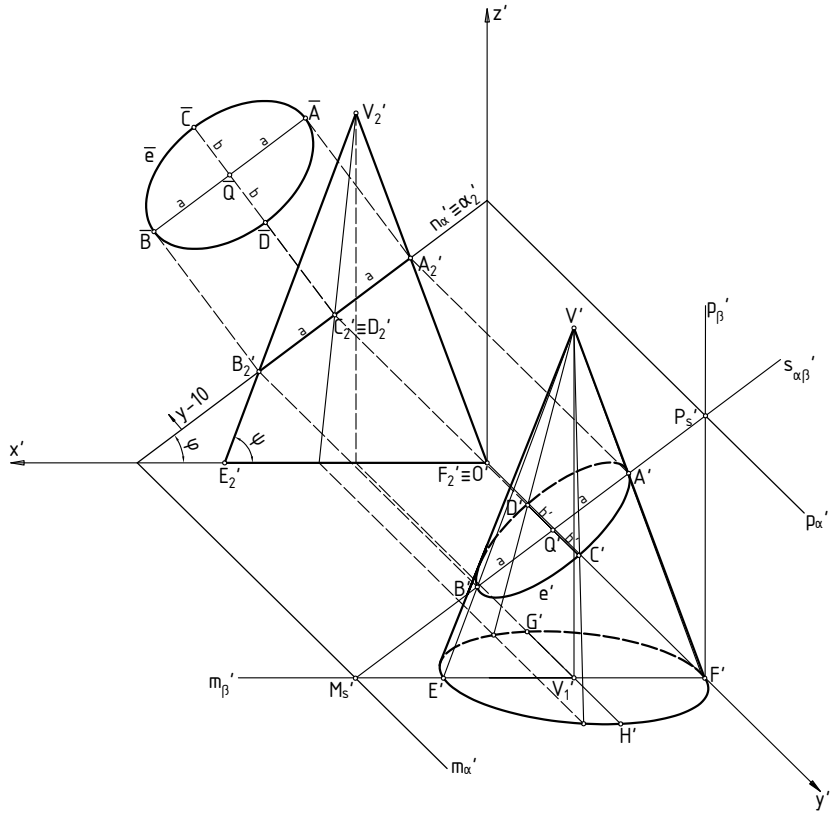
7. Намерени са аксонометричните проекции на върховете на елипсата – точки A', B', C', D', като за целта са използвани образователните на конуса. Отсечките $A'B'$ и $C'D'$ са двойка спрегнати диаметри на аксонометричната проекция на елипсата, тъй като при успоредно проектиране се запазва успоредността, запазват се пропорциите, но не се запазват ъглите.

8. Построена е проекцията на сечението, като за отделянето на видимата от невидимата му части са отбелязани допирните точки на елипсата до контурните образователни на конуса. За оформянето на елипсата e' могат бъдат намерени допълнителни точки, както и да се намерят осите, като се приложи конструкцията на

Риц.

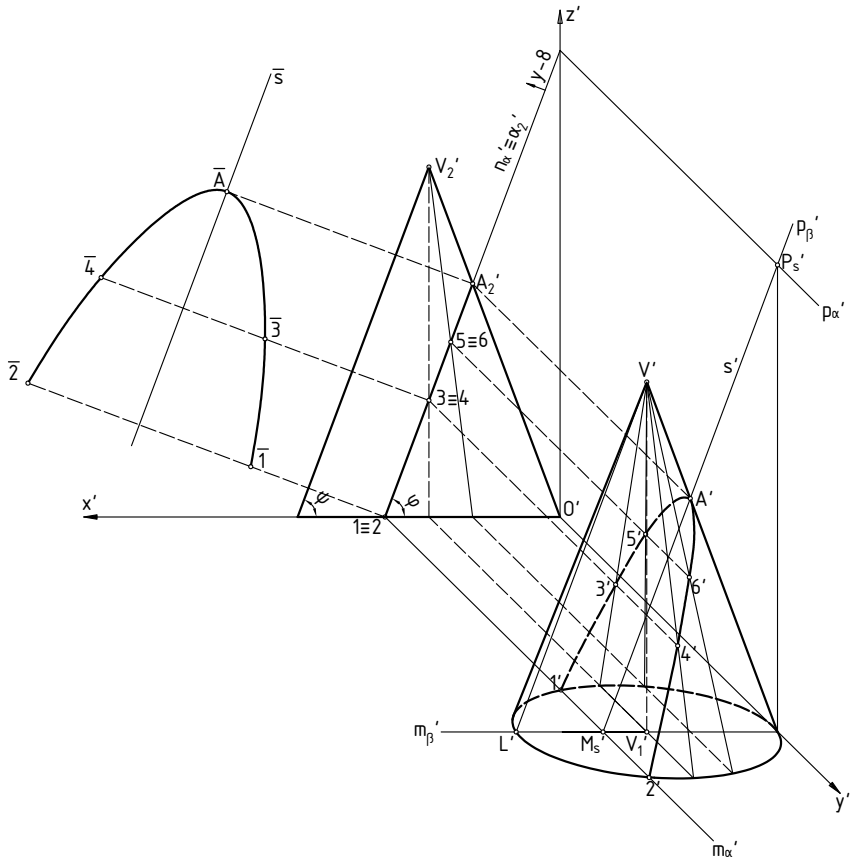
9. За намирането на истинския вид на сечението – елипсата $\bar{e}$ – равнината α е завъртяна на 90° до съвпадане с ν, след което е плъзната към проекцията на конуса. Точките $\bar{A}, \bar{B}, \bar{C}$ и $\bar{D}$ са склопените положения на върховете на елипсата до ν и са получени, като са отчетени y-координатите им от аксонометричния чертеж. Дължината $|\bar{C}\bar{D}| = 2b$ е реалната дължина на малката ос на елипсата.

Построенията са показани на чертеж 1.



Чертеж 1

Пример 2. В кабинетна проекция да се изобрази ротационен конус с връх $V(3;14;8)$ и основа в първа координатна равнина μ с радиус $R=3$. Да се изобрази сечението на конуса с равнина $\alpha[4;\infty;z_\alpha]$, което да бъде парабола, и да се покаже истинският му вид.

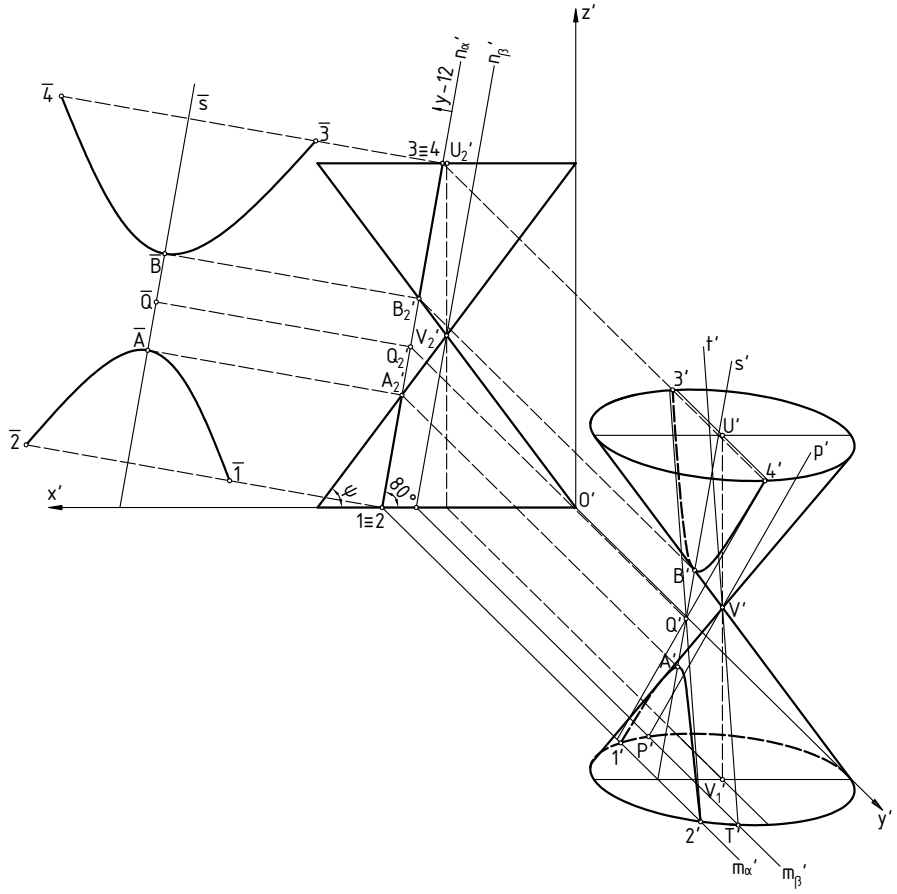


Чертеж 2

Построенията при изработването на чертежа към този пример са направени в същата последователност, както в първия пример. При построяването на втората диря на равнината α е използвано условието сечението да се получи парабола, като $n'_\alpha \equiv \alpha'_2$ е построена успоредна на едно от бедрата на вторичната проекция на конуса. Пресечната точка на дирята на равнината α с другото бедро на $\Delta E'_2F'_2V'_2$ е вторичната проекция на върха на параболата – точката A. Намерени са двете пресечни точки на първата диря на равнината α с основата на конуса и още 4 произволни точки, като са използвани прободите на образувателните на конуса със секущата равнина. Показана е и проекцията на оста на параболата – s', както и аксонометричната проекция на образувателната на конуса, на която равнината α е успоредна

– $V'L'$.
Построенията са показани на чертеж 2.

Пример 3. В кабинетна проекция да се изобрази двоен ротационен конус с връх $V(3;18;4)$ и основа в първа координатна равнина μ с радиус $R = 3$. Да се изобрази сечението на конуса с равнината $\alpha[4.5;\infty;z_\alpha]$, ако $\sphericalangle(\alpha,\mu) = 80°$, и да се покаже истинският му вид.



Чертеж 3

При построяването на проекцията на конуса са изобразени две еднакви елипси с центрове V_1' и U', след което са начертани контурните образователни. Видима е горната основа на конуса и предната част от околната му повърхнина.
За построяването на втората диря на равнината α е използвано, че $\sphericalangle(\alpha,\mu) = \sphericalangle(n'_\alpha, x') = 80°$.
Тъй като $\varphi > \phi$, то сечението е хипербола. Пресечните точки на n'_α с контурните за

вторичната проекция на конуса образователни са вторичните проекции на върховете на хиперболата – точки A_2' и B_2'.
Намерени са пресечните точки на равнината α с двете основи на конуса. Получените 6 точки еднозначно определят хиперболата.
Показана е и проекцията на реалната ос на хиперболата – s'.
За намирането на асимптотите на хиперболата е построена равнина β, която минава през върха на конуса и е успоредна на равнината α. Тази равнина пресича конуса в две образователни – VT и VP. Тези две образователни са направленията на асимптотите на хиперболата. Намерен е центърът на хиперболата – точката Q – среда на отсечката AB. Построени са прави, минаващи през точка Q и успоредни на VT и VP. Това са асимптотите на хиперболата.

Чертежите са изработени с помощта на AUTOCAD.

Благодарности. Авторите биха искали да благодарят на НИС на ТУ - София за финансовата подкрепа.

Литература

[1] Радулов, В., Първанова, И., *Ръководство по дескриптивна геометрия, Равнинни сечения*,(2006) УАСГ, ISBN 13978-954-724-031-5
Radulov, V., Parvanova, I., 2006. *Descriptive geometry, Plane sections, Textbook* , UACG, (in Bulgerian)

[2] Радулов, В., Първанова, И., 2012. *Ръководство по дескриптивна геометрия, Равнинни сечения*,(2012) Регалия 6, ISBN 978-954-745-220-6
Radulov, V., Parvanova, I., 2012. *Descriptive geometry, Plane sections, Textbook* , Regalia 6,(in Bulgerian)

[3] Чорбаджиев, Д., *Дескриптивна геометрия*, УАСГ, (1992).
Chorbadgiev, D., 1992. *Descriptive geometry*, UACG (in Bulgerian)

[4] Данаилова, Н., Велинова, Л., Колев, М., *Аксонометрия, Курсови и изпитни задачи* , УАСГ, ISBN 978-954-724-035-4 (2012).
Danailova, N., Velinova, L., Kolev, M., 2012. *Axonometry, Textbook* , UACG (in Bulgerian)

[5] Зарева, Ц., 2013. *Учебно помагало по дескриптивна геометрия, Равнинни сечения, сенки, отвори*,(2013) УАСГ, ISBN 978-954-724-064-3
Zareva, C., 2013. *Descriptive geometry, Plane sections, shadows, perforations, Textbook* , UACG,(in Bulgerian)

МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2026
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2026
Proceedings of the Fifty-Fifth Spring Conference
of the Union of Bulgarian Mathematicians
Tryavna, Bulgaria, April 5–9, 2026

AUXILIARY PROJECTION PLANES IN SOLVING SOME METRIC PROBLEMS

Irena A. Parvanova[1], Yana Kancheva[2]
[1]Department of Applied Mathematics and Informatics, Technical University of Sofia, Bulgaria,
[2]Dept. of Applied Geodesy, Faculty of Geodesy, University of Architecture, Civil Engineering and Geodesy, Sofia, Bulgaria
e-mails: [1]irena.parvanova@tu-sofia.bg, [2]kancheva_fgs@uacg.bg

The article considers four problems on constructing a transversal and an axis of crossed lines and one problem on constructing a section of a pyramid with a plane and determining the distance from a point to a plane, solved using the methods of descriptive geometry. The examples shown are presented in Monge projection and axonometry and can be useful in illustrating results achieved by the means of analytical geometry and in teaching descriptive geometry to university students of engineering majors.

Keywords: metric problems, crossed lines, axis, transversal

ПОМОЩНИ ПРОЕКЦИОННИ РАВНИНИ ПРИ РЕШАВАНЕТО НА НЯКОИ МЕТРИЧНИ ЗАДАЧИ

Ирена Първанова[1], Яна Кънчева[2]
[1]Факултет „Приложна математика и информатика“, Технически университет – София
[2]Катедра „Приложна геодезия“, Геодезически факултет, Университет по строителство, архитектура и геодезия, София
e-mails: [1]irena.parvanova@tu-sofia.bg, [2]kancheva_fgs@uacg.bg

Статията разглежда четири задачи за построяване на трансверзала и ос на кръстосани прави и една задача за построяване на сечение на пирамида с равнина и определяне на разстояние от точка до равнина, решени с методите на дескриптивната геометрия. Показаните примери са изпълнени в монжова проекция и аксонометрия и могат да бъдат от полза при изработването на чертежи, онагледяващи решаването на редица задачи в стереометрията и в обучението на студенти от инженерните специалности на висшите учебни заведения.

Ключови думи: метрични задачи, кръстосани прави, ос, трансверзала

https://doi.org/10.55630/mem.2026.55.205-213

2020 Mathematics Subject Classification: 51N05, 51M04, 53A04, 51M04, 53A04.

Въведение: Задачи за построяване на трансверзала на кръстосани прави и намиране на разстоянето между кръстосани прави са важна част от решаването на редица задачи в инженерните науки и са част от учебния материал в курса по стереометрия за 11. клас – профил „Математика“. В тази статия авторите показват няколко примера, решени в монжова проекция и аксонометрия, като се надяват направените чертежи да бъдат от полза при правилното и точно построяване на перпендикуляр от точка към равнина и на ос и трансверзала на кръстосани прави в задачи от курса по стереометрия и в курсовете по дескриптивна геометрия.

Изложение: Два от показаните примери са изпълнени в монжова проекция – основен прекционен модел, използван най-често от инженери и архитекти. Останалите три примера са изработени в кавалиерна и кабинетна проекция с цел по-добра нагледност и да могат да бъдат използвани като основни конструкции при изработването на чертежи към задачи в стереометрията. Изработването на чертежите изисква познаване на свойствата на успоредното проектиране и основни конструкции, използвани в дескриптивната геометрия, които могат да бъдат намерени в [3]. При разработването на първите две задачи правите са избрани така, че да се покажат предимствата на допълнителното ортогонално проектиране с цел максимално опростяване на построенията. Когато права се постави перпендикулярна на дадена равнина, то ортогонолната ѝ проекция в равнината е точка. Когато равнина се постави перпендикулярна на проекционна ранинина, то равнината се проектира в права. Когато отсечка е успоредна на проекционна равнина, то при проектирането се запазва нейната дължина. С поставянето на основните геометрични обекти в частно положение спрямо проекционна равнина се опростява решението на редица задачи в дескриптивната геометрия – прибод на права с равнина, основните метрични задачи, намирането на сечение на тяло с равнина, намирането на истински вид на равнинна фигура и други. Основни конструкции, използвани при работа с трета и четвърта помощни проекционни равнини в монжова проекция могат да бъдат разгледани в [3] и [1].

Пример 1. В монжова проекция да се изобрази трансверзалата на правите $a[A(0;7;1.5), N^a(8;0;1.5)]$ и $b[B(4;6;7), M^b(-5.5;1.5;0)]$, която минава през точката $T(2;3;2.5)$. Да се определи дължината на частта от трансверзалата, заключена между двете прави.

Построенията са извършени в следната последователност:

1. Изобразени са проекциите на дадените прави a и b и точката T.

2. Въведена е трета помощна проекционна равнина π, която е перпендикулярна едновременно на първа проекционна равнина μ и на дадената права a. Това е възможно, тъй като като правата a е успоредна на първа проекционна равнина μ. $x_{1,3} \equiv \pi_1$ е построена на произволно място, перпендикулярна на a_1.

3. Намерена е третата проекция на правата a – точката a_3, на правата b – правата b_3 и на точката T – T_3.

4. Построена е третата проекция на трансверзалата на двете прави – правата t_3, която минава през точките a_3 и T_3.

5. Отбелязана е пресечната точка на t_3 и a_3 – Q_3 и чрез ординали са намерени първа и втара проекции на точката Q – Q_1 и Q_2.

6. Построени са първа и втора проекции на търсената трансверзала, като $t_1 = P_1Q_1$, $t_2 = P_2Q_2$.

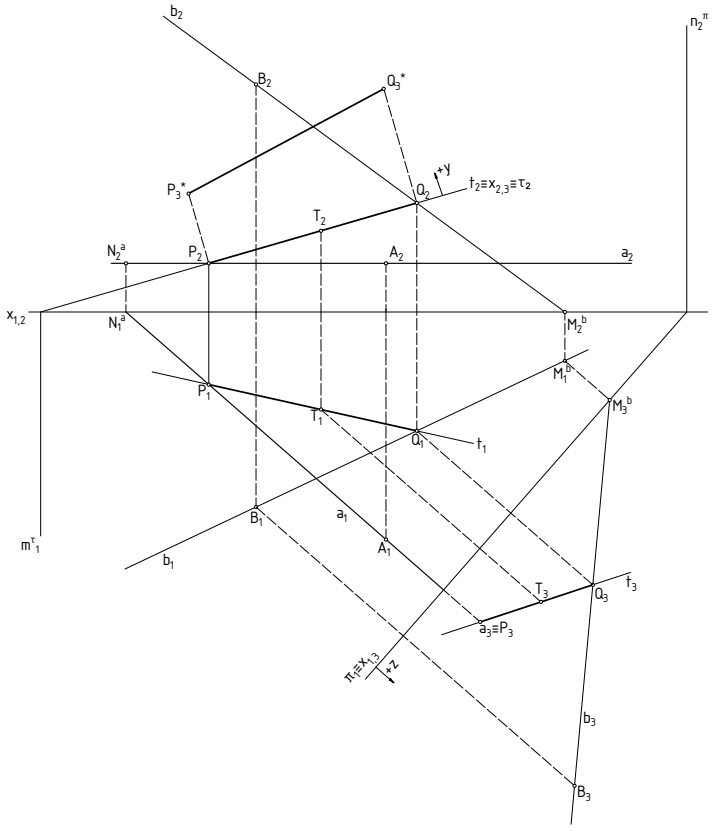
7. Отбелязани са проекциите на пресечната точка на правата t с правата a – точка P. $P_1 = t_1 \cap a_1$, $P_2 = t_2 \cap a_2$.

8. За намирането на дължината на отсечката PQ е въведена нова помощна проекционна равнина τ, която минава през правата t и е перпендикулярна на втора проекционна равнина ν. $x_{2,3} \equiv \tau_2$.

9. $|PQ| = |P_3^*Q_3^*|$.

Показаната задача е изключително важна в пътното строителство и развива умения у студентите за работа с помощни проекционни равнини. За решаването ѝ може да се използва и стереометричното решение, като се построят две равнини – α, минаваща през правата a и точката T и β, минаваща през правата b и точката T, след което се намери пресечната им права – това е търсената трансверзала. Така обаче, чертежът се натоварва със значително повече построения.

Построенията са показани на чертеж 1.

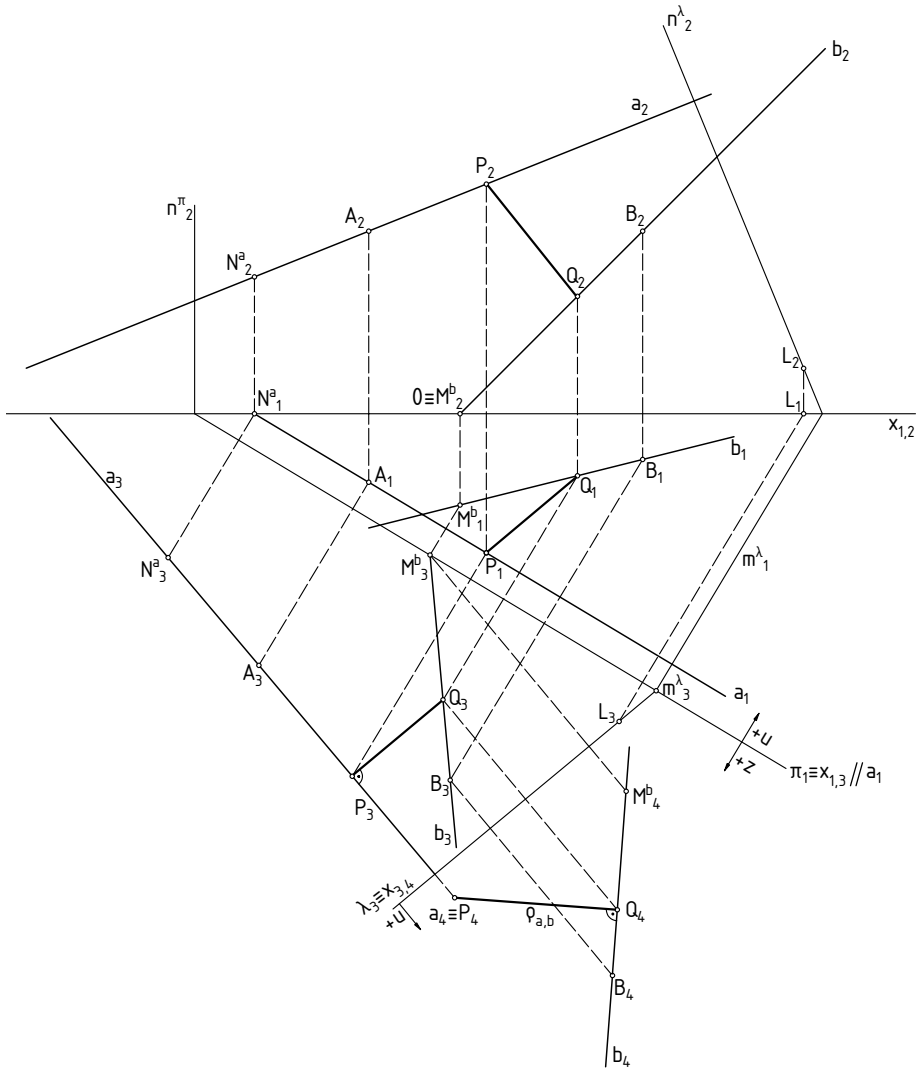


Чертеж 1

Във втория показан пример двете прави са в общо положение спрямо проекци-

онните равнини. Тогава се налагат две смени на проекционния апарат с цел отново една от правите да се проектира в точка. По този начин търсената ос на кръстосаните прави ще се вижда като перпендикуляр от точка към права.

Пример 2. В монжова проекция да се изобрази оста-отсечка PQ на правите $a[A(2;1.5;4), N^a(4.5;0;3)]$ и $b[B(-4;1;4), M^b(0;2;0)]$ и да се определи разстоянието между тях.



Чертеж 2

Построенията са показани на чертеж 2 и са извършени в следната последовател-

ност:

1. Изобразени са проекциите на дадените прави a и b.

2. Въведена е трета помощна проекционна равнина π, която е перпендикулярна едновременно на първа проекционна равнина μ и е успоредна на дадената права a. $x_{1,3} \equiv \pi_1$ е построена на произволно място, успоредна на a_1. С цел добра нагледност е показана и втората диря на новата проекционна равнина – n_2^{α}, която е перпендикулярна на оста $x_{1,2}$.

3. Намерени са третите проекции на правите a и b – a_3 и b_3.

4. Въведена е четвърта помощна проекционна равнина λ, която е перпендикулярна на π и правата a. $x_{3,4} \equiv \lambda_3$ е построена на произволно място, перпендикулярна на a_3. Така в четвърта проекция правата a ще се проектира в точка. Отново с цел добра нагледност са показани първата и втората дири на равнината λ – m_1^{λ} и n_2^{λ}.

5. Намерени са четвъртите проекции на правите a и b – точката a_4 и правата b_4.

6. Построена е оста-отсечка на правите в четвърта проекция – отсечката P_4Q_4. $P_4 \equiv a_4$, $P_4Q_4 \perp b_4$. Тъй като четвърта проекционна равнина е перпендикулярна на правата a, то тя е успоредна на търсената ос-отсечка и тогава правият ъгъл между PQ и правата b се запазва. Също така се запазва и дължината на отсечката PQ, т. е. $|PQ| = |P_4Q_4|$. По дефиниция това е раз/-сто/-я/-ни/-е/-то между двете кръстосани прави a и b.

7. Последователно чрез ординали са намерени трета, първа и втора проекции на точката Q – $Q_3 \in b_3$, $Q_1 \in b_1$ и $Q_2 \in b_2$.

8. За намирането на P_3 е построен перпендикуляр от Q_3 към a_3. Тъй като правата a е успоредна на трета проекционна равнина π, то правият ъгъл между отсечката PQ и правата a в трета проекция се запазва.

9. Чрез ординали са намерени P_1 и P_2 – $P_1 \in a_1$, $P_2 \in a_2$.

10. Построени са първа и втора проекции на оста-отсечка на правите – отсечките P_1Q_1 и P_2Q_2.

Следващите три примера са изработени в аксонометрия с цел да се постигне добра нагледност и да се направят приложения на показаните в първите две задачи основни конструкции. Основните конструкции, използвани при работа в аксонометрия могат да бъдат разгледани в [3] и [4]. Задачите са решени в кавалиерна и кабинетна проекция, тъй като това са видове аксонометрии, при които аксонометричната равнина е успоредна на втора координатна равнина ν. Тогава, ако отсечка е успоредна на ν или лежи в нея, то тя се изобразява с истинската си дължина, запазват се ъглите между правите, успоредни на ν и видът на фигурите, успоредни на ν или намиращи се в нея. Така втора координатна равнина може да бъде използвана като трета помощна проекционна равнина в монжова проекция. Телата, показани в трите примера, са избрани така, че един от ръбовете на основата да е перпендикулярен на ν и вторичната му проекция да бъде точка.

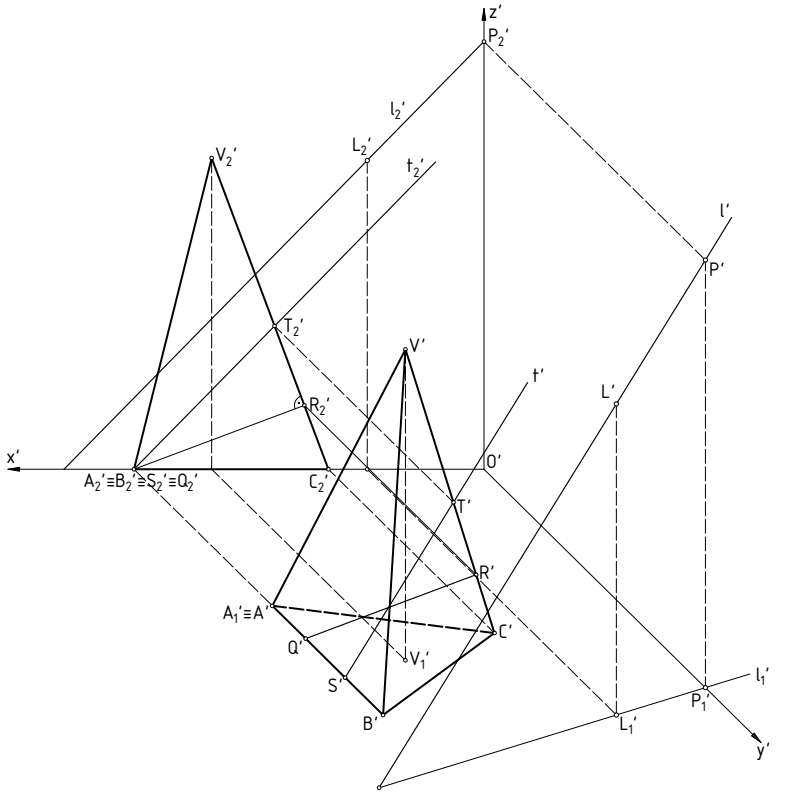
Пример 3. В кавалиерна проекция да се изобразят пирамида с връх $V(7;7;8)$ и основа триъгълник $ABC[A(9;5;0), B(9;9;0), C(4;6;0)]$ и права $l[L(3;9;8), P(0;8;11)]$. Да се построят оста-отсечка на основния ръб AB и околния ръб VC и трансверзалата t на AB и VC, която е успоредна на правата l.

Построенията са показани на чертеж 3 и са извършени в следната последователност:

1. Изобразен е аксонометричният кръст на кавалиерна проекция.

2. Изобразена е основата на пирамидата и е нанесен върхът – точка V.

3. Изобразени са околните ръбове на пирамидата, като е определена видимостта им.



Чертеж 3

4. Изобразена е дадената права l – l', l'_1.

5. Намерена е втората вторична проекция на пирамидата – триъгълник $A'_2C'_2V'_2$. Тъй като отсечката AB е перпендикулярна на ν, то $A'_2 \equiv B'_2$.

6. Намерена е l'_2 – втората вторична проекция на правата l.

7. Построена е t'_2, успоредна на l'_2 и минаваща през $A'_2 \equiv B'_2$.

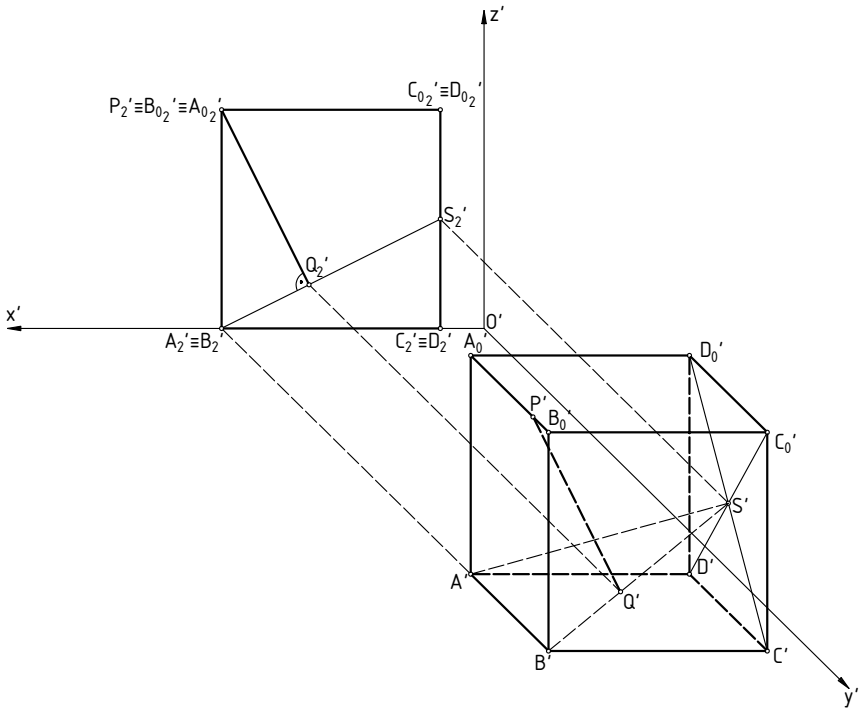
8. Отбелязана е пресечната точка на t'_2 с $V'_2C'_2$ – точка T'_2 и е намерена $T' \in V'C'$.

9. Построена е аксонометричната проекция на търсената трансверзала – правата t', която минава през T' и е успоредна на l'.

10. През точката $A'_2 \equiv B'_2$ е построена отсечка, перпендикулярна на $V'_2C'_2$ – $Q'_2R'_2$. Тази отсечка е вторичната проекция на търсената ос-отсечка на основния и околния ръб, като $|Q'_2R'_2| = |QR|$.

11. Намерени са аксонометричните проекции на точките Q и R – $R' \in V'C'$, $R'Q' \parallel R'_2Q'_2$.

Пример 4. В кабинетна проекция да се изобрази куб $ABCDA_0B_0C_0D_0$ с една стена в първа координатна равнина μ с ръб $AB[A(6;16;0), B(6;21;0)]$. Да се намери центъра на стената CDC_0D_0 – точката S и да се определи раз/-сто/-я/-ни/-е/-то между правите A_0B_0 и BS.

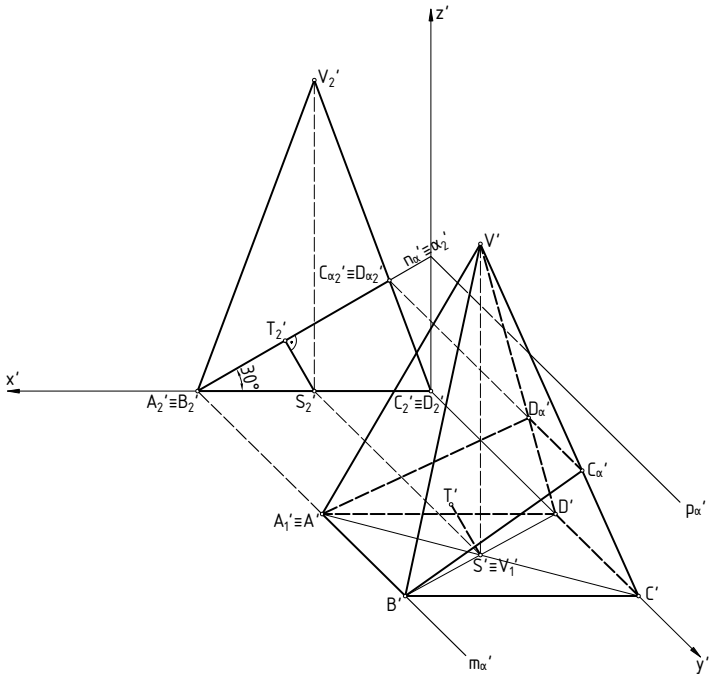


Чертеж 4

При изработването на този чертеж построенията са направени в същата последователност като в предния пример при намирането на оста-отсечка на правите и са показани на чертеж 4. Дължината на отсечката PQ е търсеното разстояние. $|PQ| = |P'Q'|$.

В последния пример е показано решение на задачата за намиране на разстояние от точка до равнина – една от основните метрични задачи – и за построяване на сечение на тяло с равнина. Секущата равнина е поставена перпендикулярна на втора координатна равнина и по този начин тя се изобразява в права. Това улеснява намирането на върховете на сечението.

Пример 5. В кабинетна проекция да се изобрази правилна четириъгълна пирамида с височина $h = 8$ и основа в първа координатна равнина μ със страна $AB[A(6;9;0), B(6;15;0)]$. Да се изобрази сечението на пирамидата с равнина α, минаваща през ръба AB и сключваща ъгъл 30° с равнината на основата. Да се определи разстоянието от точката S – център на основата на пирамидата до равнината α.



Чертеж 5

Построенията са показани на чертеж 5 и са извършени в следната последователност:

1. Изобразена е пирамидата, като $|A'B'| = |C'D'| = 3$, $|B'C'| = |A'D'| = 6$, $|V_1'V'| = h = 8$.

2. Намерена е втора вторична проекция на пирамидата – равнобедрен триъгълник $A_2'C_2'V_2'$.

3. Построена е втората диря на секущата равнина – $n_\alpha' \equiv \alpha_2'$, която минава през A_2' и сключва ъгъл 30° с x'. Ъгълът $\sphericalangle(x', n_\alpha')$ е линеен ъгъл на двустенния ъгъл $\sphericalangle(\alpha, \mu)$. Тъй като равнината α минава през отсечката AB, която е перпендикулярна на ν, то равнината α също е перпендикулярна на ν. Тогава вторите вторични проекции на всички точки от равнината α са върху нейната втора диря – $n_\alpha' \equiv \alpha_2'$.

4. Отбелязани са пресечните точки на n_α' с $V_2'A_2'$ – $C_{\alpha 2}' \equiv D_{\alpha 2}'$.

5. Намерени са върховете на сечението C_α' и D_α'. Сечението е трапецът $A'B'C_\alpha'D_\alpha'$.

6. През точка S' е построен перпендикуляр към n_α'. Петата на перпендикуляра е означена с T_2'. Дължината на отсечката $S_2'T_2'$ е разстоянието от точката S до равнината α. Правият ъгъл се запазва, тъй като едното му рамо – втората диря на равнината α – лежи в равнина, успоредна на проекционната равнина.

7. Построена е отсечка $S'T'$, успоредна и равна на $S_2'T_2'$. Това е аксонометричната проекция на перпендикуляра от центъра на основата на пирамидата към равнината

на сечението.

Решени и подробно описани задачи за построяване на равнинно сечение на пирамида и призма могат да бъдат разгледани в [2] и [5].

Чертежите са изработени с помощта на AUTOCAD.

Благодарности. Авторите биха искали да благодарят на НИС на ТУ - София за финансовата подкрепа.

Литература

[1] Радулов, В., Първанова, И., *Ръководство по дескриптивна геометрия, Монжова проекция*, (2005) УАСГ, ISBN 954-724-027-7
Radulov, V., Parvanova, I., 2006. *Descriptive geometry, Plane sections, Textbook*, UACG, (in Bulgarian)

[2] Радулов, В., Първанова, И., 2012. *Ръководство по дескриптивна геометрия, Равнинни сечения*, (2012) Регалия 6, ISBN 978-954-745-220-6
Radulov, V., Parvanova, I., 2012. *Descriptive geometry, Plane sections, Textbook*, Regalia 6, (in Bulgarian)

[3] Чорбаджиев, Д., *Дескриптивна геометрия*, УАСГ, (1992).
Chorbadgiev, D., 1992. *Descriptive geometry*, UACG (in Bulgarian)

[4] Данаилова, Н., Велинова, Л., Колев, М., *Аксонометрия, Курсови и изпитни задачи*, УАСГ, ISBN 978-954-724-035-4 (2012).
Danailova, N., Velinova, L., Kolev, M., 2012. *Axonometry, Textbook*, UACG (in Bulgarian)

[5] Зарева, Ц., 2013. *Учебно помагало по дескриптивна геометрия, Равнинни сечения, сенки, отвори*, (2013) УАСГ, ISBN 978-954-724-064-3
Zareva, C., 2013. *Descriptive geometry, Plane sections, shadows, perforations, Textbook*, UACG,(in Bulgarian)

МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2026
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2026
Proceedings of the Fifty-Fifth Spring Conference
of the Union of Bulgarian Mathematicians
Tryavna, Bulgaria, April 5–9, 2026

UKRAINIAN EXPERIENCE IN TEACHING HIGHER MATHEMATICS IN ENGLISH: OUTCOMES AND CHALLENGES

Nataliia Snizhko
Department of Higher Mathematics,
Zaporizhzhia Polytechnic National University, Zaporizhzhia, Ukraine
e-mail: snizhko.nataliia@gmail.com

This article examines the implementation and effectiveness of an English-medium mathematics course for engineering students at the National University "Zaporizhzhia Polytechnic". The study analyzes student attitudes, challenges, motivational factors, and academic outcomes among participants of EMI and traditional Ukrainian-language groups. Quantitative results show no significant differences in final grades, confirming that foreign-language instruction does not hinder students' acquisition of mathematical content. Qualitative findings highlight the cognitive benefits of bilingual learning, including enhanced attention to conceptual structures and improved professional language skills. The study identifies the need for adapted teaching materials and emphasizes the importance of methodological support for successful EMI implementation.

Keywords: higher mathematics, bilingual instruction, English Medium Instruction (EMI), bilingual mathematics education, subject-oriented bilingual teaching/learning models

УКРАИНСКИ ОПИТ В ПРЕПОДАВАНЕТО НА ВИСША МАТЕМАТИКА НА АНГЛИЙСКИ ЕЗИК: РЕЗУЛТАТИ И ПРЕДИЗВИКАТЕЛСТВА

Наталия Снижко
Катедра „Висша математика“,
Национален университет „Запорожка политехника“, Запорожие, Украйна
e-mail: snizhko.nataliia@gmail.com

Статията разглежда внедряването и ефективността на курс по висша математика на английски език за студенти по инженерни специалности в Национален университет „Запорожка политехника“. Анализирани са отношението на студентите, основните затруднения, мотивационните фактори и учебните резултати в EMI групата

https://doi.org/10.55630/mem.2026.55.214-222
2020 Mathematics Subject Classification: 97C30, 97C50, 97M10.

и традиционната група на украински език. Количественият анализ показва липса на значима разлика в крайните оценки, като потвърждава, че обучението на чужд език не възпрепятства усвояването на математическото съдържание. Качествените резултати подчертават когнитивните ползи от двуезичното обучение, включително засилено внимание към концептуалните структури и подобрени професионални езикови умения. Проучването изтъква необходимостта от адаптирани материали и методическа подкрепа за успешното прилагане на EMI.

Ключови думи: висша математика, двуезично обучение, обучение чрез английски език (EMI), двуезично математическо образование, предметно-ориентирани модели за двуезично обучение/преподаване

Introduction

The ongoing processes of globalization and the international integration of higher education systems require technical universities to reconsider their instructional strategies and learning settings. As the dominant language of international communication, English has become an essential element of engineers' professional skill sets. The Bologna Process further promotes student mobility and enhances the competitiveness of graduates, motivating Ukrainian institutions to align their academic programs with European educational frameworks.

Bilingual instruction (Ukrainian – English) presents a productive pathway for fostering both intercultural awareness and professional competencies. Within such courses, English functions not only as a language to be learned but also as the primary medium through which subject knowledge is delivered (EMI – English Medium Instruction). While EMI practices in technical disciplines are still evolving in Ukraine, their relevance is steadily increasing, creating a clear need to adapt teaching methodologies to national educational realities. Teaching mathematics in English is particularly justified, as mathematical concepts and symbolic representations are universally shared across scientific communities, making the discipline an ideal platform for developing professional language proficiency without compromising conceptual understanding.

Theoretical background

Bilingual education is seen as the integration of content and language, where a foreign language becomes a tool for acquiring specialized knowledge. Modern research highlights various models of bilingual learning, but at the university level, the EMI model is considered the most effective. EMI involves teaching professional subjects in English without formally focusing on language goals [12; 15]. EMI is used in Europe, Asia, and South America, and experiences from some countries show that English is becoming the standard in many engineering programs [1; 7].

Language factors in mathematics learning are a special subject of research by scholars [4]. In mathematics education, EMI offers additional advantages. First, the universality of mathematical symbols helps students understand content even if their language skills are limited. Second, mathematical terminology is highly precise, and equivalents in different languages have clear meanings, which aids memory and natural vocabulary acquisition. Third, switching to another language system promotes analytical and critical

thinking, as students must rethink familiar concepts and focus on logical connections instead of mechanically using formulas [2; 9; 11].

Ukrainian research on this topic is still fragmented and mostly focuses on specific aspects of foreign language mathematical training for engineers. The lack of a comprehensive concept for bilingual mathematics (engineering) education, national teaching methods, and didactic materials complicates the implementation of EMI courses [13; 14]. However, existing publications [3; 5] emphasize the urgent need to develop this area.

Organization of the EMI course and research methodology

At the National University "Zaporizhzhia Polytechnic", a course in higher mathematics has been taught in English since 2016 for students majoring in Power Engineering, Electrical Engineering, and Electrical Mechanics. This course is implemented as a full component of the educational program. Students in the English-speaking group follow the same curriculum as those in the Ukrainian-speaking groups. Groups are formed solely based on students' choice, and no selection based on language proficiency is applied. All students simultaneously take a course in English for Specifics Purposes (ESP), which ensures support for their language competencies.

During 2021–2024, 89 students participated in the study, including 29 enrolled in the EMI course and 60 studying in Ukrainian. Data were collected through Google Forms surveys and online questionnaires, which included various types of questions such as Likert scales, open-ended, and multiple-choice items. Statistical analysis involved comparison of final mathematics grades using the independent samples t-test. In addition, qualitative analysis was used to interpret students' motivations, challenges, and impressions.

The study is limited to a relatively small number of students from a single university. This is partly due to the consequences of the pandemic and the introduction of martial law in Ukraine. Nevertheless, the trend is clear, allowing us to assess the benefits, challenges, and cognitive effects of bilingual higher mathematics education.

Results and discussion

Student attitudes and main challenges. The survey conducted at the beginning of the course showed the following. The results demonstrated a high level of student awareness of bilingual education (over 92% of respondents were familiar with the concept) and a positive attitude toward the EMI mathematics course (about 84% supported the idea of a bilingual mathematics course). The majority of respondents (76%) believed that studying mathematical subjects in English broadens their professional prospects, promotes academic mobility, and increases competitiveness in the labor market. At the same time, only about one-third of students (38%) rated their initial English proficiency as sufficient for participating in an EMI course. However, later most respondents noted that language difficulties significantly decreased during the first few months.

Student motivation focuses on educational and professional opportunities (100% of bilingual group respondents), the desire to improve foreign language proficiency (65%), master subject-specific (mathematical) terminology (83%), and gain experience in intercultural communication.

At the end of the course, students' emotional feedback indicates that the English-medium mathematics course is perceived as engaging and useful (nearly 90%). Students highly value the opportunity to practice English-language mathematical discourse while

solving problems, explaining methods, and participating in discussions

Alongside positive evaluations, students also note several challenges. The most frequently mentioned issue is the lack of English-language textbooks and teaching materials adapted to the Ukrainian mathematical tradition (82%). For example, the Ukrainian and Western European traditions differ significantly in their approaches to teaching topics related to function differentiation and the definite integral. Differences in notation, structure, and problem types make it difficult to use foreign resources without additional adaptation. There are also differences in basic school mathematics. In Ukrainian schools, considerable attention is devoted to studying solid geometry, logarithms, and trigonometry, while noticeably less emphasis is placed on combinatorics, statistics, financial calculations, working with graphical information, and the ability to formalize real-life problems (different balance between the theoretical and practical components). Therefore, we believe that it is necessary to develop specialized teaching materials that take into account the specifics of Ukrainian mathematical preparation while also meeting international standards. Relying solely on foreign textbooks is insufficient and may complicate the learning process. Thus, it is advisable to create adapted English-language manuals, glossaries, and online courses, at least during the initial stages of English-medium instruction.

Another challenge is the slower pace of instruction in a foreign language and, as a result, the possible lack of classroom hours needed to cover the mathematical material (49%). In addition, at the initial stages of bilingual instruction the instructor often needs to provide terminology in both languages and compile a glossary for each topic. As a result, within the scheduled classroom hours for the higher mathematics course, students in English-medium groups manage to cover a smaller amount of material than those studying in their native language. This may affect the completion of the curriculum. These reasons require the instructor to carefully select course materials. The issue of insufficient classroom hours can be partially addressed through blended learning, more intensive independent work, and the use of interactive platforms that help compensate for the slower pace of classroom instruction.

A comprehensive analysis shows that the success of bilingual mathematics instruction largely depends on the instructor's pedagogical expertise. English does not pose a barrier if the instructor possesses deep professional knowledge and can adapt the material to the students' pace and language characteristics. We agree with [8] and believe that a high level of methodological and subject-matter competence in a mathematics instructor can, to some extent, compensate for possible limitations in their foreign language proficiency. An important condition is collaboration between mathematics instructors and ESP teachers, as effective bilingual education requires an integrated approach that includes both mathematical and language components.

The impact of EMI instruction on the acquisition of mathematical content. A central question of this study was whether delivering a higher mathematics course in a foreign language has an impact on students' comprehension and mastery of the subject matter. Naturally, it is particularly important to ensure that students' learning is not adversely affected by instruction being delivered in a foreign language.

To address this question, we conducted a detailed analysis of students' assessment results in higher mathematics. The assessments were carried out at the end of the course using a standardized 0–100 point scale. Two distinct groups were examined: the

experimental group, which participated in the EMI mathematics course, and the control group, which completed the traditional course in Ukrainian. To evaluate the potential effect of the language of instruction, we tested the hypothesis of equality of means between the two independent populations.

The experimental group consisted of 29 students who took the EMI course, while the control group included 60 students who studied in Ukrainian. The sample means were 72.70 and 71.61, respectively, with standard deviations of 6.28 and 3.44.

Given the difference in sample sizes and the fact that the sample variances were not substantially different ($1/2 < S1/S2 < 2$), a two-sample t-test with a two-sided critical region was applied. The empirical t-value (1.0545) was calculated using the Student's t-statistic. Since the p-value (0.3073) exceeds the significance level ($\alpha = 0.05$), we have no grounds to reject the null hypothesis that the means of the two groups are equal. This indicates that any observed differences in the scores are likely due to random variation rather than the language of instruction. The data do not contradict the null hypothesis that the means of the two samples are equal.

Therefore, it can be concluded that teaching higher mathematics in English does not adversely (negatively) affect students' mastery of the subject content. This finding aligns with previous research on the impact of bilingual programs on learning outcomes [6] and supports evidence on the effectiveness of bilingual instruction for engineering and technical students.

Thus, the results support the feasibility of implementing English-medium mathematics courses in technical universities, provided that a sufficient level of mathematical preparation is maintained and teaching materials are adapted to meet the needs of students with varying levels of language proficiency.

Cognitive effects of bilingual instruction in higher mathematics. The combination of the native language, English, and the language of mathematics creates a unique cognitive space that activates higher-order thinking. Switching the linguistic environment while studying mathematical concepts requires students to pay closer attention to the logical structure of the material, as familiar language patterns are no longer immediately apparent. Learning terminology in English forms new semantic connections, expands conceptual contexts, and deepens understanding by necessitating the integration of symbolic, verbal, and logical elements.

Formulas learned in isolation, like memorized fragments of text, are often forgotten, misunderstood, or altered by students. Learning through a foreign language forces students to pay closer attention to formulas and to engage more deeply with their meaning, since changing the language of instruction also changes the names and symbols of mathematical objects.

A simple example is the Ukrainian formula for calculating the area of a rectangle:

$$S = a \cdot b,$$

read as "*добуток сторін прямокутника* (a на b) (literal translation from Ukrainian: *the product of the sides of the rectangle (a times b)*). However, the English version of the same formula looks different, even though the concept remains unchanged:

$$A = l \cdot w,$$

read as "*length (l) times width (w)*". As we can see, both the sides of the rectangle and its area are denoted by different letters in the two languages, and the formulas

are therefore read differently. Other examples of formulas and notational conventions can also be found, where the appearance and pronunciation differ between English and Ukrainian.

Formulas, notations, objects	Ukrainian	English
Hyperbolic functions	sh, ch, th, cth, arsh, arch, arth, arcth	sinh, cosh, tanh, coth, $\sinh^{-1}$, $\cosh^{-1}$, $\tanh^{-1}$, $\coth^{-1}$
Newton-Leibniz formula	$\int_a^b f(x)dx = F(b) - F(a)$	$\int_a^b f(x)dx = [F(x)]_a^b$
Geometric series	$\sum_{n=0}^{\infty} q^n = \frac{1}{1-q}, \quad \lvert q\rvert < 1$	$\sum_{n=0}^{\infty} r^n = \frac{1}{1-r}, \quad \lvert r\rvert < 1$
Area (volume) element in a multiple integral; region of integration in a definite multiple integral	$\iiint f(x;y;z)\ dx\ dy\ dz$ $\iint_D f(x;y)\ dx\ dy$	$\iiint f(x;y;z)\ dA$ $\iint_A f(x;y)\ dA$
Taylor series term (two variables)	$\frac{1}{n!}\left(\Delta x \cdot \frac{\partial}{\partial x} + \Delta y \cdot \frac{\partial}{\partial y}\right)^n f(a;b)$	$\frac{1}{n!}\left[\left(h \cdot \frac{\partial}{\partial x} + k \cdot \frac{\partial}{\partial y}\right)^n f\right]_{(a;b)}$
Field theory operators	grad f, div$\mathbf{A}$, rot$\mathbf{A}$, ∇u, rot grad f, div rot$\mathbf{A}$ In formulas (in textbooks), "verbal" operator notation is used most often.	∇f, $\nabla \cdot \mathbf{A}$, $\nabla \times \mathbf{A}$ (curl $\mathbf{A}$), $\nabla^2 u$, $\nabla \times (\nabla f)$, $\nabla \cdot (\nabla \times \mathbf{A})$ The formulas have an operator form; "verbal" operator names are used only in the text.
Quadratic surfaces	*однопорожнинний* (*двопорожнинний*) гіперболоїд [literal translation "hyperboloid of one (two) *cavities*"]	hyperboloid of one (two) *sheets*

Thus, using a foreign language in instruction prevents students from relying on memorized symbolic patterns. Instead, they must focus on understanding the meaning behind each symbol. This results in greater attention during classes and leads to a deeper comprehension of fundamental concepts.

In Ukrainian, the mathematical concepts "*область значень функції*", "*розмах (вибірки)*", "*точки, розташовані на одній прямій*", and "*множина покриття*" (in Bulgarian "*множество от стойности на функция*", "*размах (на разсейването)*", "*точки, принадлежащи на една права*", "*покритие*") are expressed by different terms. However, in English all of these correspond to the single term "*range*". There is no phonetic, etymological, or visual connection between the respective Ukrainian words; as a result,

the relationships among these concepts may appear formal, artificial, or even nonexistent to students. When English is used as the language of instruction, students are more likely to perceive these concepts as manifestations of a common underlying idea, facilitating abstraction, transfer of knowledge, and the construction of more coherent mental models.

Studying higher mathematics in English can offer several cognitive advantages for students, not only in terms of conceptual integration but also in terms of algorithmic thinking. English mathematical discourse tends to favor concise, operator-based formulations and standardized terminology, which often results in definitions and statements that are more procedural and step-oriented. This stylistic tendency supports the development of algorithmic thinking – an important cognitive skill for later work in numerical methods, computational mathematics, and applied modeling, where problems are naturally expressed as sequences of operations rather than purely symbolic manipulations.

As an example, let us consider the definition of the limit of a function of two variables.

Typical of Ukrainian textbooks	Typical of American/British textbooks
Функція $f(x;y)$ має границю L при $(x;y)\to(a;b)$, якщо для довільного числа $\varepsilon>0$ існує число $\delta>0$ таке, що для всіх $(x;y)$, які задовольняють $0<\sqrt{(x-a)^2+(y-b)^2}<\delta$, виконується $\lvert f(x;y)-L\rvert<\varepsilon$	Let $f(x,y)$ be a function defined on a neighborhood of $(a;b)$. We say that $\lim(x;y)\to(a;b)f(x;y)=L$ if for every $\varepsilon>0$ there exists $\delta>0$ such that whenever $0<\sqrt{(x-a)^2+(y-b)^2}<\delta$ it follows that $\lvert f(x;y)-L\rvert<\varepsilon$

As we can see, the formulation in Ukrainian consists of a single long sentence with a complex grammatical structure and several embedded conditions. A student needs to decode the text in order to discern the algorithm for verifying the limit. In the English version, the structure is clearly visible: "if ... then ..." / "whenever ... it follows that ...". The operational sequence of actions is explicitly specified:

1) choose ε;
2) find the corresponding δ;
3) check the condition for $(x;y)$;
4) verify that $|f-L|<\varepsilon$.

Experience in English-medium instruction strengthens students' language competencies through the systematic use of mathematical discourse, which is typically inaccessible in traditional foreign-language courses. At the same time, mathematical symbolism acts as a cognitive bridge between linguistic systems, enabling students to construct meaning regardless of their level of English proficiency. Altogether, this fosters the development of analytical thinking, the ability to articulate arguments, and the capacity to compare and generalize mathematical approaches.

From a psychological perspective, bilingual instruction also shows a positive influence on students' mastery of mathematics. On the one hand, learners naturally experience communication and learning barriers, including language-related difficulties that arise when studying mathematics in a foreign language. However, when students overcome these psychological obstacles – provided that appropriate didactic, organizational, and

psychological conditions are created – they develop essential emotional and volitional qualities needed for studying mathematics, such as readiness to face challenges, resilience to stress, and the ability to understand and accept alternative viewpoints.

By employing diverse approaches, bilingual instruction creates a motivating environment for students [10]. Therefore, EMI can positively influence many students' attitudes toward mathematics.

Conclusions

The study confirms that implementing an English-medium mathematics course in a technical university setting is both pedagogically feasible and academically effective. Students demonstrate positive attitudes toward bilingual instruction and clearly recognize its value for their professional development, mobility, and competitiveness. Despite initial language-related challenges, most learners adapt quickly, and their mathematical performance remains comparable to that of students studying in their native language. Statistical analysis of assessment results shows no significant difference between the EMI and non-EMI groups, indicating that learning mathematics through English does not hinder content mastery.

At the same time, successful implementation of such courses requires careful consideration of methodological and organizational factors. The lack of adapted English-language materials aligned with the Ukrainian mathematical tradition remains a significant barrier, highlighting the need for specialized textbooks, glossaries, and digital resources. Instructors' methodological expertise and cooperation between mathematics and ESP teachers are essential to maintaining a balanced pace of instruction and supporting students with varying levels of language proficiency.

Overall, the results demonstrate that EMI-course in mathematics promotes deeper cognitive engagement, enhances analytical and critical thinking, and enriches students' mathematical and linguistic competencies. With appropriate didactic support, bilingual mathematics instruction can become a valuable component of modern engineering education in Ukraine.

References

[1] J. Airey. "I don't teach language". The linguistic attitudes of physics lecturers in Sweden. *AILA Review*, 25(1) (2013), 64–79. ISSN 1461-0213, E-ISSN 1570-5595. https://doi.org/10.1075/aila.25.05air

[2] R. Barwell, J. Moschkovich, S. Staats. Teaching and learning mathematics in multilingual classrooms. Proceedings of the 32nd Conference of the International Group for the Psychology of Mathematics Education, July 17–21, Morelia, Mexico. Vol. 1 (2008), p. 202. ISBN 978-968-9020-06-6

[3] R. Bolitho, R. West. The internationalisation of Ukrainian universities: The English language dimension. Kyiv, Stal (2017). ISBN-978-617-676-123-5

[4] N. F. Ellerton, P. C. Clarkson. Language factors in mathematics teaching and learning. In A. J. Bishop, K. Clements, C. Keitel, J. Kilpatrick, & C. Laborde (Eds.), International handbook of mathematics education (Vol. 4, pp. 987–1033). Dordrecht, Springer (1996). ISBN 978-94-010-7155-0. https://doi.org/10.1007/978-94-009-1465-0_30

[5] B. A. Goodman. Implementing English as a medium of instruction in a Ukrainian University: Challenges, adjustments, and opportunities. *International Journal of Pedagogies and Learning*, 9(2) (2014), 130–141. IS sN 1833-4105. https://doi.org/10.1080/18334105.2014.11082026

[6] S. Jianhong, L. Junsheng, L. Hongjun, L. Qiming. Analysis of factors affecting the effectiveness of bilingual instruction. In 2010 International Conference on Educational and Information Technology (ICEIT 2010) (Vol. 2, pp. V2-412–V2-414). Chongqing, IEEE (2010). ISBN 978-1-4244-8033-3, E-ISBN 978-1-4244-8035-7 https://doi.org/10.1109/ICEIT.2010.5607604

[7] R. G. Klaassen. The international university curriculum: Challenges in English-medium engineering education (Doctoral dissertation). Technische Universiteit Delft (2001). ISBN 9051705689. https://doi.org/10.4233/uuid:dea78484-b8c2-40d0-9677-6a508878e3d9

[8] E. Kováčiková, J. Luprichová. CLIL as the vehicle of transition from mono- to bilingual instruction at Slovak universities. *Journal of Teaching English for Specific and Academic Purposes*, 11(3) (2023), 753–763. ISSN 2334-9182, E-ISSN 2334-9212.https://doi.org/10.22190/JTESAP231003056K

[9] C. Laborde. Language and mathematics. In P. Nesher & J. Kilpatrick (Eds.), Mathematics and cognition (p.p. 53-69). New York, Cambridge University Press (1990). ISBN 9521366089, 9521367875

[10] J. Novotná, M. Hofmannová. CLIL and mathematics education. (2000). Available from: https://www.researchgate.net/publication/228491266_CLIL_and_mathematics_education

[11] L. T. Prochazkova. Mathematics for language, language for mathematics. *European Journal of Science and Mathematics Education*, 1(1) (2013), 23–28. E-ISSN 2301-251X. https://doi.org/10.30935/scimath/9383

[12] A.-M. Sandstrom. English-taught Bachelor's programs in Europe. *International Higher Education*, (96) (2018), 12–13. ISSN 1084-0613. https://doi.org/10.6017/ihe.2019.96.10775

[13] N. Snizhko. Implementation of bilingual education in Ukrainian institutions of higher education. *Viae Educationis: Studies of Education and Didactics*, 2(3) (2023), 35–39. ISSN 2956-2856. https://doi.org/10.15804/ve.2023.03.04

[14] N. Snizhko. Model of Bilingual Mathematics Teaching at a Technical University. *Problems of Education*, 2(101) (2024), 44-57. ISSN 2710-3986. https://doi.org/10.52256/2710-3986.2-101.2024.03 (in Ukrainian)

[15] B. Wächter, F. Maiworm (Eds.). English-taught programmes in European higher education: The state of play in 2014. Bonn, LemmensMedien GmbH (2014). ISBN 978-3-86856-017-6

МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2026
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2026
Proceedings of the Fifty-Fifth Spring Conference
of the Union of Bulgarian Mathematicians
Tryavna, Bulgaria, April 5–9, 2026

THE IMPORTANCE OF PROVIDING FULL SOLUTIONS IN MATHEMATICS ASSESSMENT

Ralitza Stamenkova
Faculty of Mathematics and Informatics, Sofia University "St. Kliment Ohridksi", Sofia, Bulgaria
e-mail: r.stamenkova@fmi.uni-sofia.bg

This article explores the potential educational benefits of providing not only correct answers but also detailed solutions to each question in a mathematics assessment. The analysis is grounded in theoretical principles from mathematics didactics, formative assessment theory, and established practices in preparing for standardised tests. In the context of the Bulgarian educational system, it is argued that the lack of detailed feedback in mathematics tests limits the opportunities for error correction, the development of mathematical thinking, and the cultivation of metacognitive skills in students. A review of freely available materials and regulatory documents was conducted, and these were then compared with those of other educational systems. The necessity to publish solutions in accordance with current educational standards and for test-format tasks was formulated as a result. In conclusion, the findings of this study recommend that teachers, authors of educational content, and educational institutions take note of the implications of these observations.

Keywords: mathematics assessment, feedback in mathematics education, metacognitive skills, test preparation practices, mathematics didactics

ЗНАЧЕНИЕТО НА ПРЕДОСТАВЯНЕТО НА ПЪЛНИ РЕШЕНИЯ ПРИ ОЦЕНЯВАНЕТО ПО МАТЕМАТИКА

Ралица Стаменкова
Факултет по математика и информатика, Софийски университет „Св. Климент Охридски", София, България
e-mail: r.stamenkova@fmi.uni-sofia.bg

Настоящата статия разглежда добавената образователна стойност на предоставянето не само на верните отговори, но и на подробни решения към всеки тестов въпрос по математика. Анализът се основава на теоретични постановки от дидактиката на

https://doi.org/10.55630/mem.2026.55.223-231
2020 Mathematics Subject Classification: 97D99.

математиката, теорията на формативното оценяване и утвърдените практиките при подготовката за стандартизирани изпити. В контекста на българската образователна система се аргументира, че липсата на подробна обратна връзка в математическите тестове ограничава възможностите за корекция на грешките, развитие на математическо мислене и формиране на метакогнитивни умения у учениците. Чрез преглед на свободно достъпни материали и нормативни документи и сравнение с други образователни системи се формулира нуждата от публикуване на решения според действащите образователни стандарти и за задачите в тестов формат. В заключение се формулират препоръки към учители, автори на учебно съдържание и образователни институции.

Ключови думи: оценяване по математика, обратна връзка в обучението по математика, метакогнитивни умения, подготовка за изпити, дидактика на математиката

Introduction. Assessment is of central importance in the domain of mathematics education, directly impacting both the learning process and students' motivation and attitudes towards learning. In the Bulgarian educational context, however, mathematical tests are predominantly utilized as a metric for evaluating outcomes rather than as a catalyst for learning and growth. In most cases, students are provided solely with the correct answers, without any elaboration on the rationale behind the solution or the reasons why the other options are incorrect [7]. Research in the field of mathematics education emphasizes that assessment which does not require or provide an explanation of the strategies and reasoning used fails to capture students' actual level of understanding and has a limited educational effect [10].

This approach is particularly appropriate for textbooks that contain solved problems and facilitate direct interaction with a teacher. In contrast, the majority of collections and educational materials provide merely a key with the correct answers. This practice is institutionally established, with detailed solutions published for exam materials, albeit exclusively for problems requiring an extended response. The phrase "Any other correct and complete solution will be awarded the maximum number of points" suggests that there may be alternative approaches to solving the problem, yet it is often unclear to students and parents what criteria categorize a solution as "correct and complete". It is evident that a discrete study of this topic is necessary.

Nevertheless, the present study focuses on the question of solutions to the tasks in the test section. The purpose of this article is not to engage in a discussion of the extent to which the test format is suitable for the assessment of mathematics. A salient issue is the substandard performance in mathematics examinations. A public debate has emerged on social media and among proactive parents regarding the emphasis placed on mechanising the process of solving tests by students. The results of the national external assessment following the 7th and 10th grade, in addition to the state matriculation exams, indicate systematic difficulties with tasks requiring reasoning and solutions involving sequential actions. In this context, the present article examines how the provision of detailed solutions could contribute to the improvement of the educational process within the current assessment standard.

Methodology and Research Design. This study adopts a qualitative research design combining document analysis and a comparative analytical approach to examine the

presence, structure and educational role of detailed solutions in mathematics assessment materials. The analysis is based on freely available, officially published materials that reflect current mathematics assessment practices in secondary education. The sources are divided into three main groups: 1) Normative and official assessment documents from the Bulgarian education system; 2) Publicly available exam materials (2006–2025) with answer keys for students and teachers; 3) Assessment materials from international education systems (Austria, the International Baccalaureate and the SAT), selected for their structural comparability with Bulgarian assessments, and for their established practices for publishing detailed solutions and feedback. Materials were selected based on the following criteria: public accessibility; official or institutional status; relevance to mathematics education in lower and upper secondary education; availability of test-format assessment tasks; a direct link to practices for providing feedback; transparency of solutions; and compliance with curricula and assessment standards. These criteria ensure the inclusion of materials representative of established assessment practices that are suitable for qualitative comparative analysis. The analysis was conducted in three stages: 1) Qualitative content analysis of the assessment materials for determining the provision of solutions and the level of detail (e.g. whether only a final answer is provided or a step-by-step reasoned solution); 2) Comparative analysis of Bulgarian materials and selected international examples with an emphasis on the structure of solutions and the treatment of distractors; 3) Interpretative analysis based on the theories of formative assessment and constructivist mathematics pedagogy for the evaluation of the pedagogical implications of the provision or withholding of detailed solutions. While the study does not claim to be statistically generalisable, it aims to provide analytical insight and conceptual clarity. The qualitative approach enables detailed examination of assessment practices and their educational implications, thereby contributing to the broader scientific discourse on feedback, learning support and assessment design in mathematics education.

The utilization of exam materials as a pedagogical instrument. A considerable number of students and parents employ tests from prior years as a means of preparation. It is evident that the official website of the Ministry of Education and Science (MES) disseminates answer keys; however, there is an absence of official detailed solutions to the test questions.

Research in the field of formative assessment demonstrates that the most effective feedback is specific and provides an explanation of the problem-solving process [4]. Merely indicating the correct answer does not fulfil these criteria. As Hattie and Timperley observe, feedback constitutes a significant factor in academic achievement, with its efficacy contingent upon the nature of the feedback itself and its manner of presentation [8]. The provision of the correct answer in a mathematics test cannot be considered an effective pedagogical practice. Contemporary research in the field of education further supports this, demonstrating that feedback has the highest educational value when it is focused on the problem-solving process, includes explanations, and supports reasoning, rather than when it is reduced solely to information about the final result [11] [16].

It is important to establish effective mechanisms through which students and parents can access the knowledge and skills necessary to find solutions that are aligned with the curriculum for their respective grade. At present, students and teachers are offering freely accessible solutions online. It has been observed that certain educational institutions choose to furnish comprehensive solutions on a voluntary basis, or for the purpose of

promotional activities. Parents and students are turning to forums and social networks for assistance, leveraging artificial intelligence-based tools to generate solutions. The substantial involvement of participants in the process is indicative of public engagement. However, it also highlights a discrepancy that demands resolution at a more authoritative level. Indeed, the authors of the tests possess solutions that are in accordance with current educational standards and which explicitly address the relevant knowledge and skills that each individual task aims to test and assess.

The constructivist approach in mathematics education. Mathematics, as a school subject, demands strict reasoning, a logical sequence of steps, and conceptual understanding. It is therefore of particular educational value to provide detailed solutions and analysis of distractors in mathematics tests.

In accordance with the principles of the constructivist approach in mathematics education, the importance of detailed solutions for students can be emphasised in the following aspects:

- It is evident that a considerable proportion of mathematical problems require a sequence of operations that are linked together. A detailed solution is instrumental in clarifying the individual steps and facilitating the identification of any potential errors.
- It has been demonstrated that a significant percentage of students use past examination papers for the purpose of self-preparation. When following the complete solution, the focus is directed towards the connections between concepts and the logical sequence of actions, rather than merely the final answer. This is an essential component of the sustainable acquisition of mathematical knowledge.
- The development of students' competencies is supported by detailed solutions, which facilitate self-regulated learning and reflection.

The constructivist paradigm in mathematics education is founded on the premise that learning is an active process of knowledge construction. This is characterized by the student interacting with mathematical tasks to construct understanding rather than merely reproducing end results passively. In the context of cognitive constructivism, as articulated by Jean Piaget, the process of cognitive development unfolds through the mechanisms of assimilation and accommodation [12] [13], which are predicated on the presence of cognitive conflict and the subsequent act of reflection. The review of detailed mathematical solutions is of particular significance, as it enables students to compare their own strategies with those employed by experts. The restriction of information to a simple final answer, without the availability of detailed solutions and reasoning, serves to limit opportunities for reflection and contradicts fundamental constructivist principles. This position is corroborated by empirical studies demonstrating that the analysis of ready-made, reasoned solutions facilitate conceptual understanding and reflection on the problem-solving process [20].

The analysis is further complemented by Lev Vygotsky's social constructivist theory, which underlines the significance of mediation and scaffolding in the zone of proximal development [19]. Within the Bulgarian education system, detailed solutions can be interpreted as a form of institutionalized didactic media that compensates for the limited individual feedback in mass education. The primary function of these tools is to

facilitate the transition of students to a state of conscious and self-regulated problem solving. In his research on mathematical problem solving, Schoenfeld emphasizes that successful problem solving depends not only on the availability of formal knowledge, but also on strategic control, monitoring of actions, and conscious decision-making during the process. In this sense, access to detailed, reasoned solutions has been demonstrated to support the development of metacognitive skills and the understanding of the strategies used [15].

Research on worked examples by Atkinson and other scholars [1] [14] [20] demonstrates that the analysis of detailed solutions significantly enhances the acquisition of new mathematical knowledge when compared to practices where learners are only provided with final answers. Empirical studies conducted within a school environment demonstrate that the utilization of worked examples in the teaching of algebra contributes to the development of both procedural and conceptual understanding. This approach has been shown to reduce the cognitive load on students and to facilitate the transition to independent problem solving [5] [18].

In the context of Bulgarian assessment, this suggests that the publication of official solutions and comments on the tasks would fulfil an informative as well as an educational function.

The distinction between instrumental and relational understanding, as introduced by Richard Skemp [17], is of relevance in this context. The emphasis on the final answer has been shown to primarily stimulate instrumental understanding. Conversely, the systematic presentation and discussion of detailed solutions have been shown to support the development of relational understanding, which is essential for long-term mathematical literacy and the successful construction of knowledge in higher grades. From a constructivist perspective, mathematical understanding is manifested through the student's ability to justify and argue their solutions, rather than merely achieving the correct result. In this regard, explanations and reasoning represent an integral component of the learning and assessment process [10].

Despite the efforts made towards the digitization of educational resources, many of these electronic resources and tests offer only definitive conclusions, thereby failing to accommodate the need for ongoing academic development and critical thinking skills. This limitation renders them suboptimal from an educational standpoint. There is an increasing trend among teachers of utilizing automated tests within their professional practice. While it is evident that this approach fosters competencies in test-taking and time management, the question remains: in the absence of a definitive solution, how does this contribute to the development of cognitive skills, and to what extent are the students' solutions aligned with educational standards? It should be noted that some teachers insist on detailed solutions to test answers, thus enabling them to assess their students' actual academic performance and at the same time to apply the accepted test format scheme. It is noteworthy that certain automated tests offer feedback in the form of a reasoned and justified correct answer. Contemporary research indicates that digital environments have the potential to enhance the educational value of detailed solutions by incorporating interactive elements that encourage students to engage with the individual steps of a calculation, as opposed to merely reproducing pre-established algorithms [2]. It is evident that a coherent strategy is required at the institutional level to establish a set of standards that can then be applied universally.

Detailed solutions that are publicly available and meet educational standards, the curriculum, and the educational goals set for the relevant stage, as well as the tasks from national external assessments and state matriculation exams, are beneficial for students. Furthermore, they establish a benchmark for young teachers to follow, serve as educational resources for specialists from diverse fields who have retrained as teachers, and function as a support instrument for parents who provide assistance.

Examples are drawn from the State Matriculation examination in mathematics – profiled training, held on 25 August 2025 [21].

6. The sine of the angle that the line with equation $3x + y + 5 = 0$ *forms with the ordinate axis is:*

Possible solution paths

Option I. The solution according to the material provided involves applying the formula for the cosine of the angle between two lines (φ) – the given line and the abscissa axis – with equation $y = 0$, because it is equal to the sine of the angle sought (x): $x = 90^\circ - \varphi \Rightarrow \sin(90^\circ - \varphi) = \cos\varphi$. The following formula for an angle between two lines $g_1 : a_1 \cdot x + b_1 \cdot y + c_1 = 0$ and $g_2 : a_2 \cdot x + b_2 \cdot y + c_2 = 0$ is to be applied:

$$\cos\varphi = \left| \frac{a_1 a_2 + b_1 b_2}{\sqrt{a_1^2 + b_1^2}\sqrt{a_2^2 + b_2^2}} \right| \Rightarrow \cos\varphi = \left| \frac{3 \cdot 0 + 1 \cdot 1}{\sqrt{3^2 + 1^2}\sqrt{0^2 + 1^2}} \right| \Rightarrow \cos\varphi = \frac{1}{\sqrt{10}}$$

$$\Rightarrow \sin x = \sin(90^\circ - \varphi) = \cos\varphi = \frac{\sqrt{10}}{10}$$

Option II. A different approach, which is also recommended by ChatGPT, is to calculate the gradient, i.e. the tangent of the angle (α) between the line and the positive direction of the x-axis. In this particular case:

$$\tan\alpha = -3$$

The angle sought is acute and has a magnitude of $x = \alpha - 90^\circ$. Through the application of consecutive trigonometric transformations, the following gradient value is calculated:

$$\tan x = \frac{1}{3} \Rightarrow \frac{\sin x}{\cos x} = \frac{1}{3}$$

The fundamental trigonometric identity is used to determine the value of $\sin x$.

Option III. The problem can also be resolved with knowledge from the ninth grade. A sketch of the line through its intersection points with the coordinate axes $(0; -5)$, $\left(-\frac{5}{3}; 0\right)$ illustrates the angle sought and the right-angled triangle enclosed between the line and the coordinate axes with sides of lengths 5 and 5/3. The hypotenuse is determined by the Pythagorean theorem, and the sine sought is equal to the ratio of the opposite side to the hypotenuse.

9. Which of the common fractions is used to write the infinite repeating decimal $1.\overline{36}$*?*

$$A)\frac{15}{11} \qquad B)\frac{7}{5} \qquad C)\frac{11}{7} \qquad D)\frac{11}{4}$$

Possible solutions

Option I. Many students have memorized a formula for such cases

$$1+\frac{36}{99}=1+\frac{4}{11}=\frac{15}{11}$$

Option II. The authors' anticipated solution is most likely the one suggested in current textbooks, namely, to consider the number as the whole part plus the sum of an infinite geometric progression:

$$a_1=\frac{36}{100}, q=\frac{1}{100}$$

$$1,(36)=1+\frac{36}{100}+\frac{36}{10000}+\frac{36}{1000000}+\ldots$$

$$1,(36)=1+S_\infty$$

$$S_\infty=\frac{36}{100}.\frac{1}{1-\frac{1}{100}}\Rightarrow S_\infty=\frac{36}{100}.\frac{1}{\frac{99}{100}}\Rightarrow S_\infty=\frac{4}{11}$$

$$1.\overline{36}=1+\frac{4}{11}\Rightarrow 1.\overline{36}=\frac{15}{11}$$

An alternative approach involves the writing of decimal fractions, for example, where the first term is equivalent to 0.36 and the quotient is 0.01.

$$1.\overline{36}=1+0.36+0.0036+0.000036+\ldots$$

$$1.\overline{36}=1+S_\infty$$

$$S_\infty=0.36.\frac{1}{1-0.01}\Rightarrow S_\infty=\frac{0.36}{0.99}\Rightarrow S_\infty=\frac{4}{11}$$

Option III. The response provided by ChatGPT to this question is based on an alternative approach. The following notation is introduced:

$$x=1.3636363636\ldots$$

$$100x=136.36363636\ldots$$

$$100x-x=135\Rightarrow 99x=135$$

$$x=\frac{15}{11}\Rightarrow 1.\overline{36}=\frac{15}{11}$$

Option IV. Verification of the answers is also considered appropriate. Direct verification by division, i.e. 5th grade knowledge, demonstrates that the first distractor is the correct answer. Verification of the other distractors is also suggested: answer B is expressed as a decimal fraction, with a value of 1.4, answer D is given as a decimal notation of 2.75, and answer C is greater than 1.5.

It is evident that state matriculation examinations demand a comprehensive mathematical aptitude and a range of strategies. A thorough analysis of potential approaches can provide authors with valuable insights, particularly regarding the extent to which the task, as articulated, encompasses the pertinent knowledge and skills. This phenomenon is particularly evident in the tasks from the external assessments at the end of grades 7 and 10, which can be solved by examining all possible cases, i.e. by directly checking the distractors.

In parallel with other educational systems. In Austria [3], with the support of the Ministry of Education, two platforms have been created. The first platform comprises pairs of files, with problems and solutions. The second platform offers more flexible access to individual problems from previous years, with the option of thematic filtering and sorting by complexity, video files with solutions explanations are provided as well. The format employed is not a test, but rather a short-answer format.

The International Baccalaureate [9] provides access to the Mark scheme, which contains detailed solutions with clearly indicated individual steps and the corresponding scoring.

The Scholastic Assessment Test (SAT) [6] is the closest in format and mathematics curriculum to the national external assessment at the end of 10th grade in Bulgaria. Each sample test contains a detailed explanation of the solution to each problem, as well as an analysis of distractors and common mistakes in reasoning and calculations.

The presentation of detailed solutions to individual problems from mathematics tests is a key factor in improving the quality of mathematics education in Bulgaria. This approach aligns with the principles of effective international standardized exams, transforming assessment into a catalyst for learning rather than merely a tool for selection, thereby fostering the development of mathematical thinking. Consequently, it is crucial that, in addition to the answer key, comprehensive solutions to the national tests are also provided. It is recommended that authors and publishers who offer educational materials with assessments adopt this standard procedure.

Conclusion. The absence of detailed feedback following standardized assessments within the Bulgarian education system constitutes a missed learning opportunity that has been overlooked. From a constructivist perspective, mathematics tests should not function solely as a tool for selection and ranking, but as a means of forming knowledge, diagnosing typical errors, and developing metacognitive skills. The integration of comprehensive solutions and a thorough examination of distractors would align Bulgarian practices with established international models, thereby enhancing the educational value of mathematics assessment.

References

[1] P. Atkinson, R. Derry, A. Renkl and D. Wortham, Learning from examples: Instructional principles from the worked examples research, *Review of Educational Research,* vol. 70, no. 2, p. 181–214, 2000.

[2] R. K. Atkinson and A. Renkl, Interactive Example-Based Learning Environments: Using Interactive Elements to Encourage Effective Processing of Worked Examples, *Educational Psychology Review,* vol. 19, no. 3, pp. 375-386, 2007.

[3] Austria, Aufgabenpool, Bundesministerium Bildung, [Online]. Available: https://aufgabenpool.at/amn/index.php?id=AM. [Accessed 12 2025].

[4] P. Black and D. Wiliam, Assessment and classroom learning, *Assessment in Education: Principles, Policy & Practice,* vol. 5, no. 1, p. 7–74, 1998.

[5] W. M. Carroll, Using Worked Examples as an Instructional Support in the Algebra Classroom, *Journal of Educational Psychology,* vol. 86, no. 3, pp. 360-367.

[6] CollegeBoard, *SAT Suite of Assessments: Math Test – Practice and Explanations,* New York: College Board, 2022.

[7] S. Fairbairn, How the Use of Answer Keys Affects the Learning of Math for Academically Weak Students, Lethbridge: University of Lethbridge, Faculty of Education, 1999.

[8] J. Hattie and H. Timperley, The power of feedback, *Review of Educational Research,* vol. 77, no. 1, pp. 81-112, 2007.

[9] IBO, *Mathematics: Analysis and Approaches – Assessment Guidance,* Cardiff: In-

ternational Baccalaureate Organization, 2021.
[10] M. Mann and M. C. Enderson, Give Me a Formula Not the Concept! Student Pr ormula Not the Concept! Student Preference to Mathematical Problem Solving, *Journal for Advancement of Marketing Education,* no. 25, pp. 15-24, 2017.
[11] T. Ovadiya, Fostering Reflection and Attention to Enhance Struggling Students' Mathematical Problem Solving—A Case Study, *Education Sciences,* vol. 15, no. 11, p. 1538, 2025.
[12] J. Piaget, The Psychology of Intelligence, London: Routledge, 1950.
[13] J. Piaget, To Understand Is to Invent: The Future of Education, New York: Grossman, 1973.
[14] A. Renkl, Worked-out examples: instructional explanations support learning by self-explanations, *Learning and Instruction,* vol. 12, no. 5, pp. 529-556, 2002.
[15] A. H. Schoenfeld, Mathematical Problem Solving, Academic Press, 1985.
[16] S. Sebastian, B. Nils and B. Lukas, Prompt the problem – investigating the mathematics educational quality of AI-supported problem solving by comparing prompt techniques, *Frontiers in Education,* vol. 9, p. 2024.
[17] R. R. Skemp, Relational Understanding and Instrumental Understanding, *The Arithmetic Teacher,* vol. 26, no. 3, pp. 9-15, 1978.
[18] J. Sweller and G. A. Cooper, The Use of Worked Examples as a Substitute for Problem Solving in Learning Algebra., *Cognition and Instruction,* vol. 2, no. 1, p. 59–89, 1985.
[19] L. S. Vygotsky, Mind in Society: The Development of Higher Psychological Processes, Cambridge: Harvard University Press, 1978.
[20] A. Weinberg, E. Wiesner, B. Benesh and T. Boester, Undergraduate Students' Self-Reported Use of Mathematics Textbooks, *PRIMUS,* vol. 22, no. 2, p. 152–175, 2012.
[21] МОН, Изпитни материали за ДЗИ – 2025 г. [Examination Materials for the State Matriculation Exams – 2025] (in Bulgarian), 12 2025. [Online]. Available: `https://www.mon.bg/nfs/2025/08/2dzi_matematika_v2.pdf`.

МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2026
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2026
Proceedings of the Fifty-Fifth Spring Conference
of the Union of Bulgarian Mathematicians
Tryavna, Bulgaria, April 5–9, 2026

HARNESSING THE POWER OF PRIMES: AN EDUCATIONAL GAME APPROACH TO PRIME NUMBERS IN MIDDLE SCHOOL

Mariela Stancheva
Faculty of Mathematics and Informatics, Sofia University "St. Kliment Ohridski"
e-mail: marielastan4eva@gmail.com

This study introduces an innovative, game-based approach to teaching specific abstract concepts in Number Theory (prime numbers, the Fundamental Theorem of Arithmetic, and divisibility rule) to middle school students by immersing them in a simplified cryptographic world. The author developed two original educational board games: "The White Hat and the Ancient Key" and "Hacker Duel," which use custom components (cards representing "doors" with composite numbers and "keys" with prime factors) to make the principles tangible. The first game is a cooperative and strategic exercise in prime factorization that models the concept of asymmetric complexity which is central to cryptography, while the second is a competitive duel focusing on distinguishing between common and different prime factors to understand the least common multiple (LCM) and greatest common divisor (GCD). Preliminary observations from implementation in Bulgarian schools suggest that this method effectively improves students' computational skills, encourages active use of divisibility rules, and fosters proactive mathematical thinking about fundamental concepts such as the uniqueness of factorization, demonstrating that educational board games offer a promising, innovative enrichment to traditional mathematics instruction.

Keywords: educational game, serious game, prime numbers, factorization, game-based learning

ОВЛАДЯВАНЕ СИЛАТА НА ПРОСТИТЕ ЧИСЛА: ОБРАЗОВАТЕЛЕН ИГРОВИ ПОДХОД КЪМ ПРОСТИТЕ ЧИСЛА В ПРОГИМНАЗИАЛЕН ЕТАП

Мариела Станчева
Факултет по математика и информатика, Софийски университет „Св. Климент Охридски“
e-mail: marielastan4eva@gmail.com

https://doi.org/10.55630/mem.2026.55.232-241
2020 Mathematics Subject Classification: 97F60.

Статията представя новаторски, базиран на игри подход за преподаване на специфични абстрактни концепции в Теорията на числата (прости числа, Основна теорема на аритметиката и признаци за делимост) на ученици в прогимназиален етап, чрез въвеждането им в опростен криптографски свят. Авторката разработва две образователни настолни игри: „Бялата шапка и древният ключ“ и „Хакерски дуел“, които използват специално създадени компоненти (карти, представляващи „врати“ със съставни числа и „ключове“ с прости множители), за да направят изучаваните концепции осезаеми. Първата игра е кооперативно и стратегическо упражнение по разлагане на прости множители, което моделира концепцията за асиметрична сложност – централна за криптографията. Втората игра е състезателен дуел, фокусиран върху разграничаването между общи и различни прости множители за усвояване на най-малко общо кратно (НОК) и най-голям общ делител (НОД). Предварителните наблюдения от прилагането на метода в български училища сочат, че той ефективно подобрява изчислителните умения на учениците, насърчава активното използване на признаците за делимост и развива проактивно математическо мислене върху фундаментални концепции като единствеността на разлагането. Това доказва, че образователните настолни игри предлагат обогатяване на традиционния подход в обучението по математика.

Ключови думи: образователна игра, сериозна игра, прости числа, разлагане на прости множители, обучение базирано на игри

Introduction

Mathematics education in school setting often encounters difficulties in connecting abstract concepts to the real world. This problem is particularly pronounced in teaching elements of Number Theory, such as prime numbers, the Fundamental Theorem of Arithmetic, and divisibility rules. Core concepts such as *prime numbers* and *factorization* appear disconnected from their practical application. Cryptography is the natural domain for the application of these concepts. However, because it remains an unfamiliar area to students of this age, this limits the opportunities for effective learning. This article presents a novel approach to overcoming this difficulty by using game components and a simplified cryptographic world to introduce students to a practical application of number theory. This approach, based on the principle that the game experience can compensate for a lack of life experience, is implemented in two original educational board games – “The White Hat and the Ancient Key” and “Hacker Duel”.

Problem Description

The initiation of learning elements of Number Theory varies across different curricula. In Bulgaria, the study of number theory begins in the fifth grade (12-13 years old) with prime numbers, the Fundamental Theorem of Arithmetic, and divisibility rules for 2, 3, and 5. In the Cambridge IGCSE syllabi [6], prime numbers, as well as other number theory concepts, are usually taught to students in lower or upper secondary school age (14-16 years old). In the Common Core State Standards for Mathematics, the study of prime numbers is in 4th grade (10-11 years old).

As a result of studying the foundations of number theory, students are expected to be able to factor a natural number into prime factors, know the divisibility rules for 2, 3,

and 5, and find the least common multiple (LCM) and greatest common divisor (GCD) of two or three numbers.

Since cryptography is unfamiliar to most students and somewhat to teachers at the lower secondary level, we propose an approach that connects an abstract mathematical concept with this unfamiliar area to explain its application. This approach is of particular importance for the development of mathematics education as a whole, as the problem of finding real world applications of science concepts has other similar manifestations.

The proposed approach is based on creating game components and a simplified world for board games. Thus, through different games, students can quickly gain practical experience, and this can be used to make the connection between abstraction and its application.

Attempts to Use Educational Games to Explain Complex Scientific Concepts

Several attempts have been described previously to present complex scientific concepts through educational games.

1. Related to studying quantum mechanics in high school: Quantum Race; Particle in a Box; Quantum TiqTaqToe [2], [3];
2. Related to genetics and evolution theory in lower and upper secondary school: Radix Endeavour [4];
3. Related to prime numbers: Prime Climb

The main principle followed is that the game world and the game rules should lead to the exploration of scientific abstraction through game experiences. This is also the main difference between scientific simulations used in education and the game world used in educational games.

Various board games exist that are related to the study of cryptography. The objective of the cryptographic world described in this article is to provide a natural environment for practicing specific mathematical algorithms associated with the prime factorization of natural numbers.

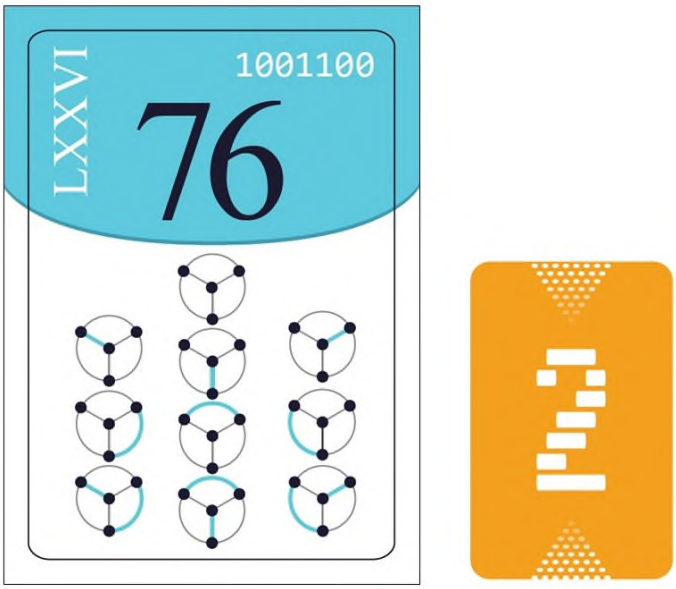
Developing a Simplified Cryptographic World and Game Components for It

Game Components: These consist of two sets of cards with numbers on them, respectively called *doors* and *keys,* which differ in size and design (Figure 1).

Figure 1 Door card 76 and key card 2

In the specific implementation, there are 36 doors with two-digit numbers on them. The images on the doors are related to various mathematical problems. Players rarely manage to guess what that problem might be. These design elements provoke players to ask the question: "What is this?" This proactive questioning by the players allows the teacher/mentor to answer this question and thus conduct a discussion in a broader mathematical context. The doors also have the door number written in Roman numerals and in the binary numeral system. These elements are usually recognized by the players.

The keys are selected to correspond to the prime factors of the numbers on the doors. For example, for a door with number 69, we have two keys labelled – 3 and



23, respectively. The number of keys depends on the selection of doors. In the specific implementation, there are 96 keys with only prime numbers. Some of the keys are coloured yellow and others green. This design element aims to provoke a question related to Mersenne numbers. This could lead to a discussion related to the discovery of prime numbers.

The duration of the games mainly depends on the number of doors. The number of doors itself is not fixed. In the specific implementation with 36 doors, the duration of the games is within one school hour (45 minutes). This facilitates their use as a learning tool. The teacher can reduce the number of participating doors and accordingly the keys. Thus, the playing time of the game will be reduced if the teacher determines that such a change is necessary.

Simplified Cryptographic World: The game world has a simple set of rules by which it operates. Players try to open the doors using the keys. A door can be unlocked if and only if keys whose product is equal to the number on that door are placed on it (Figure 2).

Figure 2: Door card 69 and the key cards 3 and 23 that unlock it

Bayta Girl's World: The game world is connected to a girl named Bayta from this world. Players are introduced to Bayta's world through a short story. This is a world where people use secrets from the past to build the future. But evil forces have taken over the Ministry of the Future and locked secrets important to humanity behind 36 doors.

Different games in this game world and with these game components are created by assigning different missions to the players.

Based on this world, various games have been developed. They have passed the stages of conceptual model and prototype and are currently used in schools at the lower and upper secondary levels in Bulgaria. This allows for future studies of its impact in the



Door Keys that unlock the door

educational environment.

Description of the Educational Game "The White Hat and the Ancient Key" for Studying Prime Numbers, Divisibility Rules, and the Fundamental Theorem of Arithmetic

The game is detailed in the publication „The game approach in building a general mathematical common sense [5],” while a brief video outlining the rules can be viewed here: `https://youtu.be/gkOCrOa-PDM`

Educational Goals of the Game:

Approaches to teaching the factorization of a natural number into prime factors vary. The game is compatible with all of them, and therefore its use does not depend on the chosen teaching method for the topic. The educational goals of the game are as follow:

1. Explain the key role of prime numbers in the set of natural numbers as fundamental building blocks.
2. Encourage students to actively use the divisibility rules for 2, 3, and 5.
3. Give the teacher a tool to demonstrate operations with asymmetric complexity – the foundation of modern cryptography.
4. Give the teacher a tool to show an application of the Fundamental Theorem of Arithmetic and prime numbers in cryptography.
5. Improve the student's computational skills regarding the factorization of two-digit numbers into prime factors.

Observations on Achieving the Educational Goals:

Although systematic studies on the game's effectiveness have not yet been conducted, we share our first observations of its being used in a class setting.

1. During the game, the question naturally arises as to whether a door cannot be unlocked by a different combination of keys. The emergence of this question is also described in other situations. This question allows for commenting on the unique factorization of a natural number into prime factors, up to the order. Since the keys are only prime numbers, the unlocking of each door happens with a single

combination of keys. When this question arises, the fact that there are only prime numbers among the keys is usually also commented on. This emphasizes the role of prime numbers as the building blocks of natural numbers and the role of the Fundamental Theorem of Arithmetic as ensuring a unique "recipe" for creating every number.

2. In the course of the game, players are convinced that when searching for suitable keys for a given door it is easier to use the divisibility rules. This provokes curiosity about the rule's definition. Observations show that the divisibility rules for 2 and 5 are used very intuitively. The divisibility rule for 3 is used if it has been recently studied. Otherwise, players remember that such a rule exists but need time or help to recall it.
3. During the game, the question often arises: "Are there other divisibility rules?" Since the doors have only two-digit numbers, division by 11 is easily discovered and used, although students might encounter difficulties when needing to precisely define the divisibility rule for 11 for numbers larger than two digits.
4. At the beginning of the game, the question arises whether the use of a calculator is permissible. Players are convinced that the use of a calculator to ease the game makes sense only in combination with a divisibility rule. This explains the asymmetric complexity of the operations of multiplication and factoring a number into prime factors.
5. The game helps develop the players' computational abilities, as well as train short-term memory. Teachers report that even students who perform poorly on computational tasks tend to calculate mentally during the game.
6. The game has low competitiveness and a high degree of social interaction. It is interesting for "Socializers" type players (The Bartle classification [1]), who, according to Bartle's model, represent about 80% of all players.

This game was the first in a series based on the developed card sets. Several teachers have implemented it in their classrooms, and the results of their observations are currently being summarized and analyzed. At the Az Sam Balgarche Private Secondary School in Varna, the game has been in use since 2023. Our colleague there introduced supplementary worksheets of her own design to accompany the game.

At Cosmos International School, lessons based on the game have been conducted since 2023; the faculty reports that this approach enables them to increase student motivation in mastering the relevant curriculum material.

A demonstration lesson for teachers, focusing on the game's potential to introduce students to the world of cryptography, was held on October 11, 2025, with the support of Science on Stage – Europe (https://www.science-on-stage.eu/news/workshop-quantum-science-and-technology-sofia).

Furthermore, on January 13, 2026, a demonstration session featuring the game 'The White Hat and the Ancient Key' was conducted with teachers and members of the Regional Management of Education (RUE) – Razgrad at the Exarch Joseph Foreign Language Grammar School in Razgrad. The subsequent observations from this session are also pending analysis.

The Role of the Teacher: Before the game, the teacher organizes the players into groups and explains the rules. During the game, the teacher answers questions related to the rules of the game. After the game, the teacher can use all the situations that arose during the game to outline the important problems whose solutions the players discovered. This can be done by asking the following exemplary questions, both from the teacher and if formulated by the students during the game:

1. Could a door be unlocked with two different combinations of keys? (No, because the keys are only prime numbers, and every number is factored into prime factors in a unique way.)
2. What is this due to? (To the fact that all keys are prime numbers and the Fundamental Theorem of Arithmetic holds.)
3. Which is easier – to check if the keys unlock a door or to determine which keys would unlock a door? (The first is multiplication and is simpler, the second is factorization and is more complex.)
4. What can help us find suitable keys? (Divisibility rules.)

Developing the Educational Game "Hacker Duel" for Studying Least Common Multiple and Greatest Common Divisor

Players' Mission: To elect the best "white hats" for freeing the secrets by winning more keys.

Game Rules: The game is played by two players. They take turns playing first and second on each turn. At the start of the game, each player receives 6 doors. The rest of the doors are in a face-down pile. All keys are placed on the table face-up. The player whose turn it is selects one of their doors and places it on the table face-up and challenges the other player to attack the door. The other player selects one of their doors and answers the challenge, in turn challenging the first player to attack their door. Each player finds the keys for the opponent's door. A winning pair of keys is any pair that can be formed from two identical keys, one from the unlocking of the first door and the second from the unlocking of the second door. The second player wins the keys from the winning pairs, and the first player takes all the remaining keys (Figure 4). The two doors are removed from the game. Each player draws a new door from the door card pile.

End of the Game: The game ends when the doors run out. The player who has collected more keys wins.

Interaction Between Players: The game is strategic.

Number of Players: 2

Game Duration: The game lasts between 40 and 50 minutes. The teacher can reduce the duration by reducing the number of doors.

Educational Goals of the Game:

Approaches to teaching the algorithms for finding the least common multiple (LCM) and greatest common divisor (GCD) vary. The game is compatible with all of them, and therefore its use does not depend on the chosen teaching method for the topic.

1. Students to make a clear distinction between the common and different prime factors of two numbers.



Figure 3: Game play situation "Hacker Duel"

2. Students to improve their computational skills for the factorization of two-digit numbers into prime factors.
3. The teacher to demonstrate the importance of coprime numbers in cryptography.
4. The teacher to encourage students to actively use the divisibility rules for 2, 3, and 5.

Observations on Achieving the Educational Goals:

Although systematic studies on the game's effectiveness have not yet been conducted, observations made during the game's use can be shared.

1. The game is highly competitive. It is of interest to "Killers" type players according to Bartle's model, because of this high competitiveness. The game is also of interest to "Explorers" type players because of the possibility to discuss optimal strategies when combining doors.
2. Observations find that players quickly arrive at the idea of coprime numbers and ask questions about effective ways to find them.

Additional Opportunities for Designing Games Based on the Game Components

The game components are designed to work with natural numbers and their representation as a product of prime factors. Given the connection between this representation and the reduction of common fractions to normal form, a game similar to "Hacker Duel" can be constructed, which develops in a different game world and demonstrates the fundamental property of common fractions to be expanded or normalized by multiplication or division by the same number in the numerator and denominator. This would be the main rule in a new game world.

A new game based on the „door cards“ is currently under development, focusing specifically on understanding the principles of constructing Roman numerals. This game is still in the design phase.

A comprehensive STEM project has been developed based on these cards and their underlying concepts. The objective of the project is for students to create their own cards using physical models. During the project activities, students are required to complete the elements on the 'door cards' (including decimal, binary, and Roman notation for a selected number) and choose an image associated with that door. As a subsequent step, students must create „keys“ for their chosen number, determining the appropriate color based on whether the number is a Mersenne number or not.

Throughout this project, students investigate various mathematical properties of the number assigned to their door and provide a visualization of a property of their choice. Upon completion, all student-created cards are compiled into a single deck, which is then used to play „The White Hat and the Ancient Key.“ Data and results from the implementation of these projects are currently being collected and are pending further analysis.

The binary representation of numbers featured on the 'door cards' can be utilized to design educational games that demonstrate efficient computational algorithms. These include exponentiation by squaring (the square-and-multiply algorithm) and multiplication via bitwise shifting (binary multiplication)

Observations on the Effect of Different Design Elements of the Game Components on Player Behaviour

Door Cards:

1. Each door card has a number that is written in Roman notation and in the binary numeral system. This design element is recognized by players independently, without outside help.
2. The images on the door cards are related to various number patterns, set theory, combinatorics. It turns out that many lower secondary school teachers find it difficult to answer questions related to these mathematical topics. This taught us to add a short guide on the topics related to the design in the future. Currently, this problem is solved with short posts on the game's website, which provide an explanation of how the corresponding number sequence or problem arises and some applications.
3. An image related to a mathematical concept as a design element can prove extremely useful for the horizontal advancement of students in different areas of mathematics. I consider the addition of supplementary educational materials related to the emerging questions to be a significant factor in increasing general mathematical literacy. Further studies are needed on the influence of different design elements on general mathematical literacy and the increase of curiosity. Very often, questions related to the images on the door cards arise during the game and might potentially be distracting. Practice shows that in such a case, the teacher should postpone the answer to this question for the discussion after the game.

Key Cards:

Each key card (except the special keys 0 and 1) is in one of two colours – yellow or green – corresponding to whether the prime number depicted on it is a Mersenne prime or not. This design element often generates interest and provides an opportunity for

teachers/mentors to discuss the issue of the impossibility of giving an effective algorithm for generating the next prime number in an efficient way. This is an occasion to conduct a discussion about the Sieve of Eratosthenes, and from there, about other problems whose solution is a sieve-type algorithm (e.g., lucky numbers, through a sieve similar to the Sieve of Eratosthenes but without preserving positions). For this design element, it is also necessary to add supplementary materials for teachers so that they can freely discuss these interesting problems related to natural numbers.

Conclusion

The presented educational games "The White Hat and the Ancient Key" and "Hacker Duel" demonstrate an effective method for overcoming the traditional challenges in teaching number theory. By creating a simplified cryptographic world, the games successfully connect abstract mathematical concepts such as prime numbers, the Fundamental Theorem of Arithmetic, and divisibility rules with a tangible game experience. Observations show that this approach not only improves students' computational skills but also provokes curiosity and proactive thinking about fundamental mathematical questions that often remain misunderstood. Teachers, in turn, can use the discussions that arise during the game to reinforce knowledge and expand students' general mathematical literacy. In the future, systematic research is needed to confirm the effectiveness of these games, but the experience so far in Bulgarian schools shows that the use of board games in the educational process is a promising and innovative method for teaching mathematics.

References

[1] Bartle, R. (1996) Hearts, clubs, diamonds, spades: Players who suits muds. MUSE Ltd, Colchester, Essex, United Kingdom.

[2] Chiarello, F. & Castellano, M.G. (2016). Board games and Board game design as Learning tools for Complex scientific Concepts: some experiences. international Journal of game-based learning, 6(2),

[3] Chiofalo, M.L.; Foti, C.; Michelini, M.; Santi, L.; Stefanel, A. (2022) Games for Teaching/Learning Quantum Mechanics: A Pilot Study with High-School Students. Educ. Sci. 2022, 12, 446. https://doi.org/ 10.3390/educsci12070446

[4] Klopfer, E.; Haas, J.; Osterweil, S. & Rosenheck, L. (2018) Resonant Games Design Principles for Learning Games that Connect Hearts, Minds, and the Everyday. The MIT Press Cambridge, Massachusetts London, England

[5] Stancheva M. (2023) The game approach in building a general mathematical common sense, National Conference SMART STEM Education and Innovation, Sofia

[6] Watson, F., Rycroft-Smith L. & Gould, T. (2022) What does research suggest about the teaching around factors, multiples and prime numbers?

МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2026
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2026
Proceedings of the Fifty-Fifth Spring Conference
of the Union of Bulgarian Mathematicians
Tryavna, Bulgaria, April 5–9, 2026

THE EXPANDING SCOPE OF ARTIFICIAL INTELLIGENCE INTEGRATION IN MATHEMATICS EDUCATION: A COMPREHENSIVE REVIEW

Tsvetelina Stefanova[1], Slavi Georgiev[2,3]
[1]Department of Computer Systems and Technologies, University of Ruse
[2]Institute of Mathematics and Informatics, Bulgarian Academy of Sciences
[3]Department of Applied Mathematics and Statistics, University of Ruse
e-mails: [1]tsstefanova@uni-ruse.bg, [2,3]sggeorgiev@uni-ruse.bg

As of early 2026, Artificial Intelligence (AI) has transitioned from an experimental auxiliary tool to a foundational pillar of modern mathematical pedagogy. This paper evaluates the rapid evolution of AI-driven mathematics tools over the academic year 2025–2026, emphasizing the shift toward adaptive, Socratic tutoring systems. We analyze key platforms and tools such as Khanmigo, Mathos AI, and Tutor CoPilot, assessing their impact on student mastery and teacher efficiency. Empirical studies from recent years suggest that AI-assisted human tutoring can lead to measurable improvements in student topic mastery. However, the integration of AI in mathematics education faces ongoing challenges regarding cognitive over-reliance and data privacy. This review synthesizes contemporary research to provide a framework for balanced AI integration that prioritizes conceptual understanding over automated problem-solving.

Keywords: artificial intelligence, mathematics education, intelligent tutoring systems, adaptive learning systems, Socratic AI tutoring, human–AI hybrid instruction, conceptual understanding

РАЗШИРЯВАЩИЯТ СЕ ОБХВАТ НА ИНТЕГРИРАНЕТО НА ИЗКУСТВЕНИЯ ИНТЕЛЕКТ В ОБУЧЕНИЕТО ПО МАТЕМАТИКА: ВСЕОБХВАТЕН ОБЗОР

Цветелина Стефанова[1], Слави Георгиев[2,3]
[1]Катедра „Компютърни системи и технологии“, Русенски университет „Ангел Кънчев“
[2]Институт по математика и информатика, Българска академия на науките
[3]Катедра „Приложна математика и статистика“, Русенски университет „Ангел Кънчев“
e-mails: [1]tsstefanova@uni-ruse.bg, [2,3]sggeorgiev@uni-ruse.bg

https://doi.org/10.55630/mem.2026.55.242-254
2020 Mathematics Subject Classification: 97D40, 97P80, 97U50, 97U70.

Към началото на 2026 г. изкуственият интелект (ИИ) преминава от експериментален помощен инструмент към основна опора на съвременната математическа педагогика. Настоящата статия оценява бързата еволюция на ИИ-базираните платформи и инструменти за обучение по математика през академичната 2025–2026 година, като акцентира върху прехода към адаптивни, сократически системи за подпомагане на ученето. Анализирани са ключови платформи като Khanmigo, Mathos AI и Tutor CoPilot, като се оценява влиянието им върху усвояването на учебното съдържание от учениците и ефективността на учителите. Емпирични проучвания от последните години показват, че обучението с помощта на изкуствен интелект може да доведе до измерими подобрения в овладяването на учебните теми от учениците. Въпреки това приложението на ИИ в обучението по математика продължава да се сблъсква със съществени предизвикателства, свързани с предоверяване на ИИ и защита на личните данни. Настоящият обзор синтезира актуални изследвания и предлага рамка за балансирана интеграция на ИИ, която поставя приоритет върху концептуалното разбиране, а не върху автоматизираното решаване на задачи.

Ключови думи: изкуствен интелект, обучение по математика, интелигентни обучаващи системи, адаптивни обучаващи системи, сократическо ИИ-обучение, хибридно обучение човек–ИИ, концептуално разбиране

1. Introduction

The period 2025–2026 represents a watershed moment in the digital transformation of education. Global investment in the EdTech AI sector reached an estimated $7.6 billion in 2025, with projections suggesting a rise to over $30 billion by 2029, reflecting both the growing maturity of AI solutions and their mainstream adoption in schools and universities [32]. In mathematics education, AI integration serves two primary functions: enhancing student learning through personalized, adaptive exercises and feedback, and improving teacher efficiency by automating time-consuming administrative burdens such as grading, progress monitoring, and lesson planning. These capabilities increasingly position AI as not merely a supplementary tool, but as an integral component of the instructional ecosystem. Current leadership sentiment reflects this shift, with 69% of K–12 leaders viewing AI's impact on mathematics instruction as inherently positive, citing its potential to support differentiation, remediation, and enrichment at scale [3, 20].

2. Literature Review: Trends in AI-Mediated Mathematics Education (2025–2026)

Recent research indicates that AI-mediated mathematics education has entered a phase of consolidation, moving from experimental use toward systematic integration into instructional practice. Whereas earlier studies largely framed AI as a computational or assessment aid, literature from 2025–2026 increasingly conceptualizes AI as a pedagogical mediator embedded within human-guided learning environments [28, 36, 40]. This shift is evident across systematic reviews, bibliometric analyses, and empirical studies.

2.1. From Automation to Pedagogical Mediation

Systematic reviews document a clear move away from solver-centric automation toward adaptive tutoring, formative feedback, and instructional scaffolding. The longitu-

dinal review (2015–2025) reports a decline in purely answer-generating systems and a rise in tools designed to support learning processes and conceptual understanding [28]. It is similarly noted in [36] that recent studies increasingly evaluate AI tools based on pedagogical impact rather than computational efficiency. These trends extend earlier concerns regarding over-reliance on automated solvers, as highlighted in our previous research [35], and place greater emphasis on design features such as delayed answer release, adaptive hints, and reflective prompts.

2.2. Learning Outcomes and Mastery

Empirical studies suggest that AI-supported mathematics instruction can lead to measurable learning gains when pedagogically aligned. The review of AI-powered assessments [25] reports improvements in student performance, engagement, and feedback quality, particularly in algebra and calculus. Research on intelligent tutoring systems (ITS) such as DreamBox, ALEKS, and Mathspace shows that adaptive readiness models can enhance mastery by sequencing content and enforcing prerequisite knowledge [37]. Several platforms now hold "strong" evidence ratings under the Every Student Succeeds Act (ESSA) framework.

Human–AI hybrid tutoring models receive particular attention. [39] demonstrates that AI-augmented human tutoring significantly increases the likelihood of topic mastery, with especially strong effects for less-experienced tutors, indicating that AI can amplify pedagogical expertise rather than replace it.

2.3. Socratic and Dialogue-Based Approaches

A prominent trend in the 2025–2026 literature is the rise of Socratic and dialogue-based tutoring systems. Bibliometric analyses identify dialogic scaffolding and non-directive tutoring as emerging focal concepts in mathematics education research [40]. Enabled largely by Large Language Models (LLMs), these systems aim to promote metacognitive regulation by guiding learners through questions and hints instead of providing direct solutions. However, studies caution that generative dialogue alone does not guarantee pedagogical soundness, noting risks of fluent but mathematically incorrect explanations when models are insufficiently constrained [5]. Consequently, teacher-in-the-loop designs are increasingly emphasized as a necessary safeguard [22].

2.4. Teacher Support, Risks, and Equity

Recent literature also frames AI as a tool for teacher support. Survey evidence indicates that educators using AI-based tools for lesson planning, assessment, and feedback report substantial reductions in administrative workload [3], potentially enabling greater focus on student reasoning and targeted intervention [34]. At the same time, studies consistently highlight risks of cognitive over-reliance. Excessive dependence on solver tools has been linked to weakened independent problem-solving and retention, particularly in scan-to-solve workflows [6, 38].

Equity and governance concerns remain unresolved. Uneven access to advanced AI tutoring systems may exacerbate existing educational inequalities [7], while policy-oriented research underscores growing challenges related to data privacy, procurement transparency, and accountability as AI becomes embedded in assessment and learning analytics [24].

2.5. Summary

Overall, the 2025–2026 literature portrays AI-mediated mathematics education as shifting toward integrated, dialogic, and human–AI hybrid models. Evidence suggests that educational impact depends less on raw problem-solving capability and more on pedagogical alignment – specifically, the ability of AI systems to support explanation, verification, and conceptual understanding under human oversight. The focus shifts from the question "Should we use AI?" to "How do we integrate it ethically and pedagogically?". The main challenge remains the balance between automated assistance and preserving students' ability to think critically without external help. These findings motivate the comparative analysis of tools and use cases presented in the following sections.

3. Comparative Analysis of Contemporary AI Tools Used in Mathematics Education

The 2025–2026 AI-in-education landscape is characterized by the convergence of large language models (LLMs) and natural language processing (NLP) with domain-specific symbolic mathematics engines. Rather than treating AI as a monolithic category, current tools differ substantially in pedagogical intent, degree of automation, and the role assigned to teachers and learners.

Table 1 provides a functional comparison of major AI tool categories currently used in mathematics education, organized by pedagogical designation rather than underlying technology alone. For each category, the table summarizes representative platforms, key innovations introduced during 2025–2026, and the strongest forms of research-backed educational impact reported in recent studies. This structure reflects the paper's focus on how design choices – such as answer withholding, adaptive sequencing, or human-in-the-loop support – shape learning outcomes.

Table 1: Pedagogical Design, Innovation, and Impact of Contemporary AI Mathematics Tools

Core Designation	***Sample Tools***	***2025–2026 Innovation***	***Research-Backed Impact***
Socratic Tutor	**Khanmigo, Google Socratic, Astra AI, Thetawise, Rori**	**Teacher-in-the-Loop Safeguard:** Tools now feature dashboards that allow teachers to toggle "reveal answer" privileges and view chat logs to identify misconceptions without manual grading.	**Active Recall Efficacy:** By refusing to provide direct answers, these tools enforce active recall. Cognitive science research confirms this method increases long-term retention by up to 50% compared to passive review.

Adaptive Solver	**Wolfram Alpha, Mathos AI, Microsoft Math Solver, Photomath, Symbolab**	**Domain-Specific Fine-Tuning:** Unlike general chatbots, these solvers are now fine-tuned specifically on mathematical notation and step-by-step logic, aiming to eliminate calculation hallucinations.	**Procedural Fluency:** Studies on tools like Microsoft Math Solver show that when combined with "similar problem" generation, they significantly improve students' ability to solve multi-step calculus and algebra problems.
Intelligent Tutoring System (ITS) with Real-time Assessment	**ALEKS, DreamBox Learning, Mathspace, Knewton Alta, Eedi**	**Predictive Readiness Models:** Systems like Mathspace and ALEKS now use AI to predict a student's knowledge state, blocking advanced topics until prerequisite skills are statistically mastered.	**ESSA Strong Evidence:** ITS platforms like DreamBox hold the highest strong rating under the Every Student Succeeds Act (ESSA) [14], proving students achieve more growth in math proficiency than peers.
Visual Scaffolding	**GeoGebra, Desmos, Solvely, Graspable Math, Polypad**	**Dynamic 3D & AR Visualization:** Recent updates (e. g., Desmos 3D) allow students to manipulate variables in real-time to visualize abstract concepts like multivariable calculus and geometric transformations.	**Conceptual Grounding:** Research indicates that dynamic graphing tools help ground abstract symbols in concrete visuals, measurably improving student performance on conceptual questions regarding functions.
Human-AI Hybrid	**Tutor CoPilot, Thinkster Math, ASSISTments, MATHia, Brainly, TutorMe**	**Real-Time Pedagogical Prompting:** AI analyzes the live session and whispers suggestions to the human tutor (e. g., *"Ask them to explain the next step"*), turning novice tutors into experts.	**Mastery Gains:** A Stanford University RCT (2024-25) on Tutor CoPilot proved that students were 4% more likely to master a topic when their human tutor used AI prompts [39].

General AI Model	**ChatGPT, Gemini, DeepSeek, Claude, Microsoft Copilot**	**Chain-of-Thought (CoT) Processing:** These models generate a hidden internal monologue to plan, critique, and verify their logic before outputting a final answer.	**Benchmark Breakthroughs:** CoT reasoning has raised AI performance on difficult math competitions (like the AIME) from ˜11.67% (GPT-4o) to ˜81.67% (o1), significantly reducing logic errors [5].

The table highlights a clear shift toward Socratic and adaptive tutoring systems, in which AI is designed to prompt reasoning, enforce active recall, and support conceptual understanding rather than deliver immediate solutions. At the same time, solver-oriented systems remain prominent, particularly for procedural fluency, benefiting from recent advances in domain-specific fine-tuning that reduce mathematical hallucinations. Intelligent Tutoring Systems (ITS) occupy a middle ground, combining automated assessment with mastery-based progression models that have accumulated strong empirical validation.

Notably, human–AI hybrid tools emerge as the category with the most consistent evidence of learning gains, aligning closely with the abstract's emphasis on AI-assisted human tutoring. By augmenting – not replacing – human instructors through real-time pedagogical prompts, these systems demonstrate measurable improvements in topic mastery while mitigating risks of cognitive over-reliance. General-purpose AI models, while increasingly capable due to chain-of-thought reasoning, remain pedagogically ambiguous and require careful instructional framing to avoid reverting to answer-centric use.

Table 1 makes explicit that contemporary mathematics AI tools are converging on natural-language interaction while diverging sharply in pedagogical posture – from dialogue-driven scaffolding to solution-centric automation to human-in-the-loop augmentation. The distribution of research-backed outcomes suggests that learning gains are most robust when AI systems are embedded within pedagogically constrained or hybrid instructional designs, rather than used as fully autonomous solvers.

3.1. Advancements in Socratic and Generative Assistants

The most significant technical leap in 2025 was the reduction of hallucinations in general-purpose models through the adoption of reinforcement learning and chain-of-thought architectures. **DeepSeek**, with its R1 model released in early 2025, exemplified this shift by introducing a thinking phase, where the AI plans multi-step solutions before generating output. This architecture raised performance on high-stakes benchmarks like the AIME to levels previously attainable only by closed-source proprietary models [11]. Similarly, **Google's Gemini** ecosystem evolved with the release of the Deep Think capability in its 2.5 Pro model, which iteratively explores hypotheses for complex logic puzzles. Google further refined this for education with "Gems" – customized AI personas that educators can fine-tune to align with specific curricular standards, effectively creating bespoke teaching assistants for distinctive classroom needs [19]. Antropic's **Claude** continued this trend with its 3.5 and 4.0 model updates in mid-2025, introducing "Artifacts" – a feature that renders interactive code and quizzes in a dedicated window, transforming static text interactions into dynamic, visual learning experiences [2]. In

the realm of dedicated educational assistants, **Khanmigo** expanded its utility beyond student tutoring. As of April 2025, it features a comprehensive "Teacher Tools" suite integrated directly into Learning Management Systems (LMS) like Canvas. This update allows educators to automate the creation of rubrics, exit tickets, and lesson plans without leaving their gradebook environment, significantly reducing administrative overhead [33].

3.2. Innovations in Symbolic, Visual, and Solver Tools

Tools rooted in symbolic computation have integrated Large Language Model (LLM) capabilities to enhance accessibility without sacrificing accuracy. Mathos AI (formerly MathGPTPro) released a "PDF Homework Helper" in 2025 that goes beyond simple photo scanning. Students can now upload entire document files, where the AI overlays annotations and step-by-step guidance directly onto the page. This system utilizes a specialized model that claims 20% higher accuracy than standard GPT-4 implementations for calculus tasks [23]. Wolfram Alpha has solidified its role as the grounding engine for the AI ecosystem. Through a robust 2025 plugin architecture, it now integrates seamlessly with ChatGPT and other LLMs, allowing them to verify their computational outputs against Wolfram's structured data libraries, effectively solving the arithmetic hallucination problem [30].

Visual graphing tools have also seen substantial updates to support higher education. **Desmos Studio** updated its 3D Calculator in early 2026 to include enhanced visualization controls – such as disabling lighting for clearer surface viewing – and expanded regression capabilities (cubic, quartic, and sinusoidal) that allow students to model complex, real-world data sets [12]. **GeoGebra** similarly launched "Math Practice", an adaptive mode that provides step-by-step feedback on algebraic problems, encouraging students to explore multiple solution paths rather than adhering to a single rigid method [18]. **Photomath** refined its visual scaffolding approach by launching "Animated Steps", which break down static scan results into dynamic progressions to help learners visualize the procedural flow of a solution [31]. **Solvely** and **Microsoft Math Solver** have also integrated similar scan-to-solve upgrades, with Microsoft's **Math Progress** in Teams now using AI to identify class-wide error trends and automatically generate targeted practice assignments [26].

3.3. Evolution of Adaptive Learning Platforms

Comprehensive learning platforms have focused heavily on accessibility and verified content reliability. **DreamBox Learning** (now part of Discovery Education) released significant updates in January 2025, including new "Racecourse" lessons for fraction fluency and enhanced accessibility features that allow students with low vision to navigate complex manipulatives using keyboard commands [9]. **Brainly** addressed the reliability crisis with its 2025 "AI Learning Companion", which uses scan-to-solve technology to provide explanations verified against a database of textbooks, distinguishing itself from raw generative text by citing specific academic sources [8]. **ALEKS** and **Mathspace** continued to refine their adaptive engines, with Mathspace's 2025 updates focusing on its Mixture-of-Experts AI, which now provides voice-based coaching to support students with reading difficulties. Finally, human-hybrid systems like **Tutor CoPilot** and **Astra AI** have moved toward a teacher-in-the-loop model, where the AI provides real-time sug-

gestions to human tutors or parents, effectively augmenting rather than replacing human instruction [39].

3.4. Evidence of Student Usage

Available surveys and institution-level studies indicate that GenAI use for learning is now mainstream across secondary and higher education, though prevalence varies by sampling and definitions. In the United States, high-school students' self-reported use of GenAI for schoolwork rose from 79% (Jan 2025) to 84% (May 2025), with ChatGPT the dominant tool (69% reporting use for assignments/homework) [1]. Meanwhile, among U.S. teens overall, 64% report using AI chatbots; usage concentrates in a few mainstream systems – ChatGPT (59%), Gemini (23%), and Meta AI (20%) – with others trailing [15].

In higher education, the same concentration pattern appears. An institutional study reports ChatGPT as the primary tool (89.3% of AI users), with Gemini (13.5%) and Copilot (7.7%) far behind and other platforms each $<5\%$ [10]. A separate survey similarly shows students assembling tool portfolios, but with strong skew: ChatGPT is cited most (606 mentions), followed by Copilot (67) and Gemini (51), with a longer tail including Grammarly, Claude, and math-oriented apps such as Gauth [27].

For mathematics, students commonly combine general chatbots with specialized solvers. A 2025 study of engineering students reports frequent use of ChatGPT (62.7%) alongside high usage of Mathway (51.7%) and Photomath (48%), reflecting a pragmatic blend of explanation-seeking and scan/stepwise solution workflows [16]. Finally, tool choice can be region- and access-dependent: qualitative evidence from pre-sessional international students (UK) documents multi-tool habits shaped by VPN and language constraints, including reliance on region-specific systems such as DeepSeek alongside global tools and routine AI-to-AI cross-checking [4].

4. Primary Use Cases in Education

AI-enabled mathematics platforms are increasingly used to build *personalized learning pathways*, where learner data are continuously collected and analyzed to adapt the sequence, difficulty, and pacing of practice. In adaptive learning platforms, this typically involves model-based estimation of student knowledge and readiness, allowing systems to recommend targeted exercises and feedback aligned with the learner's evolving profile [35, 37].

Closely related is *misconception remediation*: rather than treating errors as generic "wrong answers", diagnostic approaches aim to infer which misconception is most likely and to trigger immediate, targeted interventions. Tools such as Eedi explicitly operationalize this idea through diagnostic questioning and misconception mapping to support rapid, instructionally meaningful feedback [17].

A second dominant use case is *multimodal interaction*, reflecting the broader movement toward systems that combine text with image and speech. In practice, this enables students to scan printed or handwritten mathematics and receive step-by-step guidance (a workflow popularized by tools such as Photomath), while emerging multimodal foundation models expand the feasibility of voice-based and visually grounded tutoring scenarios [25].

Finally, AI is increasingly framed as a *teacher-empowerment layer*, accelerating routine tasks such as generating practice sets, drafting lesson materials, and producing feedback at scale. Survey evidence from 2025 suggests that teachers who use AI tools at least weekly estimate time savings of roughly six hours per week on average – highlighting why administrative relief is often cited as a primary driver of adoption [3].

5. Challenges and Ethical Considerations

There are many challenges arising with the introduction of AI mathematical instruments in education [29]. While the potential of AI-supported mathematics instruction is widely acknowledged, the 2025–2026 literature is equally explicit about the risk of *cognitive disengagement*. When students treat AI as an "answer vending machine", learning can shift from sense-making to output optimization, weakening productive struggle and durable problem-solving habits. This is particularly acute in mathematics because low-friction workflows (scan $\rightarrow$ answer) invite students to bypass verification and explanation; in Bulgaria, practitioners and education media have repeatedly noted extensive use of Photomath for homework and even tests, often with limited critical assessment – an archetypal "vending machine" pattern that prioritizes completion over comprehension [38]. The same shortcut dynamic is increasingly reinforced by general AI chatbots (especially ChatGPT), which are now widely used for schoolwork and for clarifying/double-checking solutions in policy and survey reports [1, 21]. Large surveys of educators therefore report substantial concern that AI can erode critical-thinking and research skills, underscoring the need for classroom norms that require justification, reflection, and error-checking rather than solution acquisition [6].

A second constraint is *reliability*, which matters because students increasingly consult general-purpose LLMs as if they were authoritative math engines. Even as frontier systems have achieved striking results on demanding tasks (including widely reported near "gold medal" performance on Olympiad-level subsets), outputs can still contain subtle reasoning gaps, incorrect intermediate steps, or explanations misaligned with a learner's grade level. Recent "live" evaluations such as MathArena highlight this asymmetry: many leading models score very highly on final-answer competitions, yet are less dependable on proof-style/justification-heavy tasks, with proof-based Olympiad settings still leaving substantial room for improvement [5]. As a result, a student may receive the correct final answer while internalizing an invalid method or a fluent but mathematically unsound explanation. Consequently, "Socratic" scaffolding and teacher oversight are design requirements, not add-ons: the key question is whether systems can *consistently* support valid, student-appropriate reasoning, surface assumptions, and promote verification. This aligns with evaluation-focused work emphasizing representative datasets and meaningful metrics, since superficial accuracy can mask pedagogically harmful failure modes (e. g., plausible-but-wrong steps and curriculum misalignment). In practice, the photo-based convenience and step-by-step outputs common in student-facing math tools can be beneficial, but without structured norms for checking and explaining, they may unintentionally amplify uncritical acceptance [13].

Finally, the expansion of AI in classrooms intensifies *equity and privacy* concerns. Access to high-quality AI tutoring and teacher-support systems may widen existing gaps if advanced tools are concentrated in well-funded schools, contributing to a broader AI literacy divide [7]. In parallel, schools face growing scrutiny around student-data gover-

nance, procurement transparency, and the downstream risks of breaches or surveillance-oriented deployments – issues that become more acute as AI tools integrate deeper into assessment, learning analytics, and identity-related systems [24].

Conclusions

Evidence from 2025–2026 indicates that AI is becoming an increasingly entrenched component of mathematics education – less a short-lived trend than a structural shift in how learners practice, receive feedback, and access support. The most effective deployments to date align with a human–AI hybrid approach, in which technology amplifies teacher and tutor expertise – through targeted scaffolding, formative feedback, and workflow automation – rather than attempting to substitute for instructional judgment. In parallel, the rapid rise of model capability, including demonstrations of near-gold-medal performance on elite mathematical benchmarks, underscores a crucial pedagogical inflection point: the central question is no longer whether AI can solve difficult problems, but whether it can reliably help students learn to solve them through age-appropriate reasoning, explanation, and metacognitive support.

Solver-style apps (camera-based and symbolic engines) make mathematics fast and frictionless via scan-to-solution, stepwise transformations, visualization, and instant checking – useful for practice, but also prone to turning learning into "outsourced thinking". At the same time, benchmarking shows rising accuracy on answer-checkable tasks (high scores on final-answer competitions) while proof-quality reasoning and fully reliable explanations remain less stable. With student adoption now high (e. g., 84% of US high-schoolers report using GenAI for schoolwork, and teens' chatbot use is led by ChatGPT and Gemini), teachers and tutors should integrate AI as a *coach* and *checker* – for hints, what-if prompts, explanation requests, and misconception diagnosis – while reserving full solver mode for moments that require student justification, comparison of methods, and reflection (e. g., a written reasoning chain or error analysis before consulting full solutions).

Future research should prioritize (i) causal classroom evidence beyond short interventions, including longitudinal studies that test retention, transfer, and mathematical identity; (ii) measurement frameworks that distinguish conceptual growth from answer productivity (e. g., explanation quality, error diagnosis, and strategy diversity); and (iii) implementation science for equitable and privacy-preserving adoption, covering procurement, data governance, and teacher professional development. A particularly promising direction is the design and evaluation of "Socratic-by-default" systems that can adapt their questioning strategies to student level while remaining robust to hallucinations and misuse – shifting AI evaluation from raw problem-solving accuracy to instructional reliability and learning impact.

Acknowledgements

This research is supported by the Scientific Research Fund of "Angel Kanchev" University of Ruse, Bulgaria.

References

[1] Adair, A., et al. U.S. High School Students' Use of Generative Artificial Intelligence. New Evidence from High School Students, Parents, and Educators. College Board Research, 2025, https://research.collegeboard.org/media/pdf/AI%20Research%20Brief%201_vf_0.pdf, last visited 04.02.2026

[2] Anthropic. Claude 3.5 Sonnet, 2024. https://www.anthropic.com/news/claude-3-5-sonnet, last visited 04.02.2026

[3] Ash, A.M. Three in 10 Teachers Use AI Weekly, Saving Six Weeks a Year, 2025. https://news.gallup.com/poll/691967/three-teachers-weekly-saving-six-weeks-year.aspx, last visited 05.01.2026

[4] Attewell, S. Student Perceptions 2025: Insights from a Group of Pre-sessional International Students at the University of Manchester. AI in universities and colleges, 2025. https://nationalcentreforai.jiscinvolve.org/wp/2025/09/01/student-perceptions-2025-insights-from-a-group-of-pre-sessional-international-students-at-the-university-of-manchester/, last visited 04.02.2026

[5] Balunović, M., et al. MathArena: Evaluating LLMs on Uncontaminated Math Competitions. arXiv:2505.23281v3 [cs.AI], 2026. https://doi.org/10.48550/arXiv.2505.23281

[6] Benedek, M., B.R. Sziklai. Impact of AI tools on learning outcomes: decreasing knowledge and over-reliance. arXiv:2510.16019v1 [cs.CY], 2025. https://doi.org/10.48550/arXiv.2510.16019

[7] Booth, R. Generation AI: fears of 'social divide' unless all children learn computing skills, 2026, https://www.theguardian.com/education/2026/jan/05/generation-ai-fears-of-social-divide-unless-all-children-learn-computing-skills, last visited 05.01.2026

[8] Brainly Staff. Report: How Students Are Embracing AI This Back-to-School Season (2025), Insights: The Brainly Blog, 2025. https://brainly.com/insights/report-how-students-are-embracing-ai-this-back-to-school-season-2025, last visited 04.02.2026

[9] Charlotte, N.C. New Enhancements to DreamBox Math by Discovery Education Improves Accessibility for Elementary Students. Discovery Education, 2025. https://www.discoveryeducation.com/details/new-enhancements-to-dreambox-math-by-discovery-education-improves-accessibility-for-elementary-students/, last visited 04.02.2026

[10] Contractor, Z., G. Reyes. Generative AI in Higher Education: Evidence from an Elite College. arXiv:2508.00717 [econ.GN], 2025. https://doi.org/10.48550/arXiv.2508.00717

[11] DeepSeek. DeepSeek-R1 Release: Reasoning Models and Benchmarks. DeepSeek API Docs, 2025. https://api-docs.deepseek.com/news/news250120, last visited 04.02.2026

[12] Desmos Studio. What's New at Desmos Studio. Desmos Help Center, 2025. https://help.desmos.com/hc/en-us/articles/4405017454477--What-s-New-at-Desmos-Studio#h_01KC4GCCYWN5KTS2GYYJWWC2QY, last visited 04.02.2026

[13] Dyuzhov, A. Top 5 Best AI Tools for Math in 2025. AI Hub, Overchart AI, 2025.

https://overchat.ai/ai-hub/best-ai-tools-for-math-in-2025, last visited 04.02.2026
[14] Evidence for Essa. DreamBox Math, DreamBox Learning, 2025. https://www.evidenceforessa.org/program/dreambox-learning/, last visited 04.02.2026
[15] Faveiro, M., O. Sidoti. Teens, Social Media and AI Chatbots 2025. Pew Research Center, 2025. https://www.pewresearch.org/internet/2025/12/09/teens-social-media-and-ai-chatbots-2025/, last visited 04.02.2026
[16] Garcia, K.F., et al. Engineering students' perceptions and actual use of AI-based math tools for solving mathematical problems. Acta Psychologica, 256, 105004, 2025. https://doi.org/10.1016/j.actpsy.2025.105004
[17] Garcia, M.B., et al. Modernizing mathematics education with artificial intelligence: a narrative review of AI-powered tools, thematic trends, and instructional applications, SSRN, 2025, https://dx.doi.org/10.2139/ssrn.5621770
[18] GeoGebra. GeoGebra Math Practice, 2026. https://www.geogebra.org/mathpractice/en, last visited 04.02.2026
[19] Google Support. Use Deep Think in Gemini Apps. Gemini Apps Help, 2025. https://support.google.com/gemini/answer/16345172, last visited 04.02.2026
[20] Gqoli, N., J. Baidoo. The integration of artificial intelligence in mathematics education: towards developing a conceptual framework for understanding student perspectives in higher education. E-Journal of Humanities, Arts and Social Sciences Vol.6 No.10, pp 2660-2674, 2025. https://doi.org/10.38159/ehass.202561031
[21] International Bank for Reconstruction and Development, Artificial Intelligence In Bulgarian School Education. Digital Innovations in Education, Brief №6, The World Bank, 2024. https://documents1.worldbank.org/curated/en/099609411142514872/pdf/IDU-2c378d78-1beb-40e2-889c-a389b89cd321.pdf, last visited 04.02.2026
[22] Khanmigo ECHO: Transforming classroom education by training teachers to use AI. The University of New Mexico, 2025, https://projectecho.unm.edu/story/khanmigo-echo-transforming-classroom-education-by-training-teachers-to-use-ai/, last visited 05.01.2026
[23] Mathos AI. Mathos AI Vs. MathGPT.AI: Which AI Math Tutor Is Right for You?, 2025. https://www.mathgptpro.com/blog/mathos-ai-mathgpt-ai-math-tutor-right, last visited 04.02.2026
[24] Merod, A. Risks from AI use are growing alongside its popularity in schools, 2025, https://www.k12dive.com/news/risks-from-ai-use-are-growing-alongside-its-popularity-in-schools/802387/, last visited 05.01.2026
[25] Meylani, R. AI-powered assessments in mathematics education: a systematic review of contemporary research literature. Dokuz Eylül Üniversitesi Buca Eğitim Fakültesi Dergisi 66:3642–3674, 2025. https://doi.org/10.53444/deubefd.1527781
[26] Microsoft Support. Getting Started with Math Progress, 2025. . https://support.microsoft.com/en-us/topic/getting-started-with-math-progress-a3e786d8-afcd-43e7-bc45-ef65d6c72bc9#id0edd=educators, last visited 04.02.2026
[27] Mohammad, N.M., et al. How college students use ChatGPT. Pedagogical Research, 10(4), em0250, 2025. https://doi.org/10.29333/pr/17428
[28] Nguyen, D.T., Q.V. Pham. The evolving landscape of AI integration in math-

ematics education: A systematic review of trends (2015-2025). EURASIA Journal of Mathematics, Science and Technology Education, 21(10), em2714, 2025. https://doi.org/10.29333/ejmste/17078

[29] Nikiforova-Ilieva, K., T. Georgiev. Understanding the role of AI chatbots in education: a cross-context analysis of awareness, trust, and implementation. 2025 10th International Conference on Energy Efficiency and Agricultural Engineering, Stara Zagora, Bulgaria, 2025. https://doi.org/10.1109/EEAE65901.2025.11273728

[30] Palacio, A.B. Unleashing the Power of Wolfram Alpha API with Python and ChatGPT., Packt, 2023. https://www.packtpub.com/en-us/learning/how-to-tutorials/unleashing-the-power-of-wolfram-alpha-api-with-python-and-chatgpt, last visited 04.02.2026

[31] Photomath. Math from all angles: Photomath for different learning styles, Build Your Math Mind, 2025. https://photomath.com/articles/math-from-all-angles-photomath-for-different-learning-styles/, last visited 04.02.2026

[32] Research and Markets. AI in Education Market Report 2025, 2025. https://www.researchandmarkets.com/reports/5896034/ai-in-education-market-report?srsltid=AfmBOoq9jGNebo6mOS3v6D085N6mokSVr0YfYY6wiaIicT97QCHuZqRz, last visited 04.02.2026

[33] Rutgers Canvas. Feature Release: Khanmigo Teacher Tools, 2025. https://canvas.rutgers.edu/2025/04/24/feature-release-khanmigo-teacher-tools/, last visited 04.02.2026

[34] Sevilla, A., Cuevas-Ruiz, P., Rello, L. et al. Artificial Intelligence in Education: Computer-Assisted Learning and AI-guided Tutors. Ital Econ J (2025). https://doi.org/10.1007/s40797-025-00354-1

[35] Stefanova, T., S. Georgiev. Possibilities for using AI in mathematics education. Mathematics and Education in Mathematics, 53, 117-125, 2024. https://doi.org/10.55630/mem.2024.53.117-125

[36] Sutomo, W.A.B., T. Turmudi. Integration of artificial intelligence in mathematics learning: systematic literature review. Supremum Journal of Mathematics Education 9(1):29-41, 2025. https://doi.org/10.35706/sjme.v9i1.100

[37] Tan, L.Y., et al. Artificial intelligence-enabled adaptive learning platforms: A review. Computers and Education: Artificial Intelligence 9, 100429, 2025. https://doi.org/10.1016/j.caeai.2025.100429

[38] Vasileva, G. Mobile app solves math problems in seconds, marica.bg, 2017. https://uchiteli.bg/news/mobilno-prilozhenie-reshava-zadachi-po-matematika-za-sekundi/3579, last visited 04.02.2026

[39] Wang, R.E., et al. Tutor CoPilot: a human-AI approach for scaling real-time expertise. arXiv:2410.03017v2 [cs.CL], 2025. https://doi.org/10.48550/arXiv.2410.03017

[40] Yildiz, S.G., S.G. Körpeoğlu. Trends and insights of AI in mathematics education: A bibliometric analysis. International Electronic Journal of Mathematics Education 20(3), em0837, 2025. https://doi.org/10.29333/iejme/16401

МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2026
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2026
Proceedings of the Fifty-Fifth Spring Conference
of the Union of Bulgarian Mathematicians
Tryavna, Bulgaria, April 5–9, 2026

OPTIMIZATION PROBLEM IN FINANCIAL RESOURCE MANAGEMENT IN PROFILED INFORMATION TECHNOLOGY EDUCATION

Bilyana Stoynova
University of National and World Economy, Sofia, Bulgaria
e-mail: bilyana.stoynova@unwe.bg

The article examines opportunities for software-based solving of economic problems by students at the upper-secondary level. A financial resource management problem and its optimal solution are presented. The problem is solved by different groups of students using traditional software methods, and the use of artificial intelligence (AI) is introduced to support the development of students' analytical skills. For this purpose, Excel Solver and generative artificial intelligence (AI) are used. The application of these methods in the educational process is presented, taking into account the level of mathematical knowledge of the students in the respective grade.

Keywords: optimization problem, Excel Solver, AI, mathematics education, information technology and economics

ОПТИМИЗАЦИОННА ЗАДАЧА ЗА УПРАВЛЕНИЕ НА ФИНАНСОВИ РЕСУРСИ В ПРОФИЛИРАНОТО ОБУЧЕНИЕ ПО ИНФОРМАЦИОННИ ТЕХНОЛОГИИ

Биляна Стойнова
Университет за национално и световно стопанство, София, България
e-mail: bilyana.stoynova@unwe.bg

Статията разглежда възможности за софтуерно решаване на икономически задачи от ученици в гимназиален етап. Представена е задача за управление на финансови ресурси и нейното оптимално решение. Задачата се решава от различни групи ученици чрез традиционни софтуерни методи и се въвежда използването на изкуствен интелект (ИИ) за развиване на аналитичните умения на учениците. За целта се използват Excel Solver и генеративен изкуствен интелект (ИИ). Представено е приложението на тези методи в образователния процес, като е съобразено с нивото на математически познания за съответния клас ученици.

https://doi.org/10.55630/mem.2026.55.255-264
2020 Mathematics Subject Classification: 97N80, 97P80, 97M40.

Ключови думи: оптимизационна задача, Excel Solver, ИИ, обучение по математика, информационни технологии и икономика

Въведение

В обучението си по икономика в средното училище учениците често решават икономически казуси, в които са включени задачи от линейното оптимиране. Този дял от математиката предоставя възможности за решаване на широк кръг икономически задачи, които могат да повлияят при вземането на разумни бизнес решения. Правилното планиране, човешките ресурси, маркетинг и реклама, дистрибуция, животновъдство са само малка част от областите, в които задачите от линейното оптимиране намират приложение за оптималното разпределение на ресурси [1].

Ход и методология на изследването

Много често като добър пример в обучението по икономика се представя задачата за използване на ресурси, която може да бъде приложена при вземане на финансови решения. Инвестиционните решения изискват баланс между възвращаемост и риск, като понякога са ограничени от бюджет и определени условия.

За целта на изследването е използвана задача за оптимално разпределение на капитал между различни финансови инструменти с цел максимизиране на възвръщаемостта при зададени ограничения.

Експериментално задачата е представена и решавана от две групи ученици от два последователни випуска. Първата група е съставена от 52 ученици от 12. клас, а втората група от 55 ученици от следващия випуск 12. клас. Учениците са във втори гимназиален етап на средното си образование и се обучават в профил „Предприемачески“. Два от профилиращите им предмети са „Предприемачество“ и „Информационни технологии“. С решение на Педагогическия съвет на училището, в профилиращия предмет „Информационни технологии“ е включен избираем модул за 12. клас „Обработка на социално-икономическа информация“. Тъй като модулът е избираем, учебната програма се съставя от преподаващия учител. Изборът на теми е съобразен с това да подпомага основния профил, а именно „Предприемачество“. От друга страна, модулът „Обработка на социално-икономическа информация“ е част от иновативен проект по програма на МОН „Иновативни училища“ за иновативни предмети и се преподава онлайн. Затова учебната програма предвижда голям брой практически задачи с насоченост към икономиката. Модулът се изучава само през първия срок, за да могат учениците да използват получените знания за финалния си проект по „Предприемачество“, който е през втория срок на 12. клас.

В онлайн часовете на модул „Обработка на социално-икономическа информация“ се решават широк кръг икономически задачи с помощта на софтуер. Задачата за използване на ресурси е в основата на голям брой от тях. Тъй като в училищния курс по математика учениците не се запознават с теоретичната постановка на задачи от линейното оптимиране, при решаването на задачата в часа по информационни технологии се разглежда информативно математическия модел на задачата.

Първата група ученици решава задачата единствено с помощта на MS Excel. За решаването ѝ се използва методът на линейното програмиране (LP), реализиран чрез добавката за MS Excel – Excel Solver. За целта се използват дадените данни, които се въвеждат в таблица на MS Excel под ръководството на учителя. Задачата се

задава като Assignments (Възложени задачи) в MS Teams, тъй като това е работната среда в онлайн часовете по предмета „Обработка на социално-икономическа информация“. Това дава възможност на учителя да проследява в реално време изпълнението на задачата от всеки ученик и да подпомага процеса с указания и препоръки. Целта е всички ученици да получат правилното решение на задачата, като чрез задаване на въпроси към учителя и изпълнението на отделните стъпки се стимулира тяхното логическо мислене. Възложената на всеки ученик задача се връща към него с обратна връзка от учителя върху изпълнението на задачата. Организираната по този начин работа с учениците в онлайн часовете показва добри резултати, защото дава възможност на учителя да подпомага учениците във всеки момент, в който изпитват затруднение. Тази възможност е особено важна и полезна, знаейки колко нетърпеливи са учениците и колко често бързо губят интерес към материала, ако не им се обърне своевременно внимание.

С бързото развитие на технологиите се оказа, че втората група ученици вече използват генеративен изкуствен интелект в помощ за написване на домашни и в обучението си в училище. Затова при тях, освен подпомагано от учителя решаване на задачата чрез MS Excel, се експериментира и въвеждане на използването на изкуствен интелект (ИИ), с помощта на който да се получават отговори, свързани с поставената задача. Целта е да се провокират учениците да развиват логическото си мислене, както и да откриват връзка между математическия модел на задачата и изучавани до момента математически понятия. Учениците от тази група също получават заданието си чрез Assignments (Възложени задачи) в MS Teams, но освен решението на задачата в MS Excel от тях се изисква и да получат с помощта на ИИ отговор на въпроси като: Какъв е математическият модел на задачата? Какви математически елементи и понятия от изучаваните до момента разпознавате? Кой дял от математиката се занимава с този тип задачи? Каква е икономическата интерпретация на задачата? Прави се сравнение между получените решения, има ли разлика в крайния резултат?

Отговорите на отделните въпроси, получени с помощта на ИИ, се коментират и обсъждат в онлайн часа. Ролята на учителя е аргументирано и компетентно да подпомага учениците чрез конкретни и подробни инструкции [2], чрез които те да достигат до правилни заключения и да развиват умения за разпознаването на неправилни твърдения, с които би могъл да ни подведе ИИ. Учениците се стимулират да използват различни модели на ИИ. Прави се сравнение между получените отговори и се дискутират резултатите от изследването. Учителят дава обратна връзка по време на часа и при връщане на възложените задачи в MS Teams.

Въвеждане и представяне на задачата пред учениците

Класически модел на задача за разпределение на ресурси

Да се намери максималната стойност на линейната функция $z = c_1x_1 + c_2x_2 + \cdots + c_nx_n$, при ограничения:

$$\begin{gathered} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n + x_{n+1} \leq b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n + x_{n+2} \leq b_2 \\ \cdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n + x_{m+2} \leq b_m \end{gathered}$$

$$x_j \geq 0,\ j = (1,\ \ldots,\ n),$$
$$b_i \geq 0,\ i = (1,\ \ldots,\ m)$$

Задача за инвестиционен портфейл, която учениците трябва да решат с MS Excel

Инвеститор разполага с бюджет от 200 000, който трябва да разпредели оптимално между шест различни инвестиционни инструмента, като целта е да постигне максимална възвръщаемост при определени ограничения. Всеки от инструментите предлага различна възвращаемост и риск, като са поставени минимални и максимални ограничения за инвестиране. Няма да бъде използвана конкретна валута, а само числови стойности.

Инвестиционните възможности включват:

1. Криптовалути – предлагат най-висока възвращаемост от 25%, но са и най-рискови с 40% риск. Минималната инвестиция е 1 000, а максималната – 30 000.
2. Акции – с възвращаемост от 12% и риск 20%. Минималната инвестиция е 5 000, максималната – 80 000.
3. Недвижими имоти – предлагат 9% възвращаемост при 25% риск. Минимално трябва да се инвестират 20 000, с максимум до 140 000.
4. Злато – с 8% възвращаемост и 15% риск. Минималната инвестиция е 5 000, максималната – 60 000.
5. Корпоративни облигации – възвращаемост 6% при нисък риск от 5%. Минималната инвестиция е 15 000, максималната – 120 000.
6. Държавни облигации – най-малко рискови (1%), но и с най-ниска възвращаемост от 4%. Минималната инвестиция е 10 000, максималната – 50 000.

С цел намаляване на инвестиционния риск, в нито един единствен инструмент не може да се инвестират повече от 30% от общия бюджет (т.е. не повече от 60 000). Това е т.нар. диверсификация – инвестиционна стратегия, която допълнително ограничава максималните инвестиции за някои инструменти с цел максимална възвращаемост. Сумарният риск не трябва да надвишава 10% от бюджета.

Математически модел на конкретната задача, който учениците могат да получат с помощта на изкуствен интелект (ИИ)

Дефинираме променливите x_j като количеството средства, инвестирани във всеки от шестте инструмента: x_1 – инвестиция в криптовалути; x_2 – инвестиция в акции; x_3 – инвестиция в недвижими имоти; x_4 – инвестиция в злато; x_5 – инвестиция в корпоративни облигации; x_6 – инвестиция в държавни облигации.

Целта е да се намери максималната стойност на целевата функция (общата очаквана възвращаемост):

$$\max z = 0,25x_1 + 0,12x_2 + 0,09x_3 + 0,08x_4 + 0,06x_5 + 0,04x_6$$

Коефициентът пред всяка променлива е очакваната възвращаемост (в десетични дроби).

Ограниченията, които са поставени, са следните:

Бюджет – общата инвестиция трябва да бъде не повече от 200 000:

$$x_1 + x_2 + x_3 + x_4 + x_5 + x_6 \leq 200\ 000$$

Риск – сумарният риск не трябва да надвишава 10% от бюджета, т.е. 20 000 (коефициентите са процентните рискове на инструментите):

$$0,40x_1 + 0,20x_2 + 0,25x_3 + 0,15x_4 + 0,05x_5 + 0,01x_6 \leq 20\ 000$$

Минимални/максимални инвестиции за всеки инструмент:

$$1\ 000 \leq x_1 \leq 30\ 000$$
$$5\ 000 \leq x_2 \leq 80\ 000$$
$$20\ 000 \leq x_3 \leq 140\ 000$$
$$5\ 000 \leq x_4 \leq 60\ 000$$
$$15\ 000 \leq x_5 \leq 120\ 000$$
$$10\ 000 \leq x_6 \leq 50\ 000$$

Диверсификация – не повече от 30% от бюджета, т.е. 60 000 в един инструмент:

$$x_j \leq 60\ 000;\ \forall\ j = 1, \cdots, 6.$$

Решение на задачата за оптимизация на инвестиции с Excel Solver

Стандартно в часовете по информационни технологии задачата се решава с помощта на Excel Solver. Тъй като в гимназиалния етап учениците не са запознати със задачи от линейното оптимиране, то обикновено задачи от такъв тип биват представяни като икономически задачи, даващи връзка между профилиращите предмети „Предприемачество“ и „Информационни технологии“. В 11. клас учениците изучават модул „Обработка и анализ на данни“ като част от профилираща предмет „Информационни технологии“, в който широко е застъпена работа със софтуерния продукт MS Excel и в 12. клас вече използват свободно възможностите му. Предвид този факт, на тях се предоставя конкретната задача, която биха могли да решават с помощта на MS Excel, без да познават теоретичната постановка на математическия модел на задачата. Целта на модул „Обработка на социално-икономическа информация“, в който се демонстрира тази задача, е именно надграждане на уменията и знанията, придобити в 11. клас, и интегриране на материала от всички профилиращи предмети.

На учениците се представя примерен алгоритъм за решаването за задачата.

Подготовка на таблицата в Excel – попълваме данните от задачата – фиг.1.

	A	B	C	D	E	F	G	H
1	**Instrument**	**Expected Return**	**Max Risk**	**Min Investment**	**Max Investment**	**Amount Invested**	**Return Contribution**	**Risk Contribution**
2	Cryptocurrencies	25%	40%	1 000	30 000			
3	Stocks	12%	20%	5 000	80 000			
4	Real Estate	9%	25%	20 000	140 000			
5	Gold	8%	15%	5 000	60 000			
6	Corporate Bonds	6%	5%	15 000	120 000			
7	Government Bonds	4%	1%	10 000	50 000			
8	**Total**							
9								

Фигура 1. Попълване на данните в таблица в Excel

Добавяме необходимите изчислителни клетки, както е показано на фиг. 2.

- Обща инвестиция = SUM(всички инвестиции) – трябва да е по-малка или равна на 200 000; =SUM(F2:F7)
- Възвращаемост за всеки отделен инструмент (инвестиции*очаквана възвра-

	A	B	C	D	E	F	G	H
1	Instrument	Expected Return	Max Risk	Min Investment	Max Investment	Amount Invested	Return Contribution	Risk Contribution
2	Cryptocurrencies	0,25	0,4	1000	30000		=F2*B2	=F2*C2
3	Stocks	0,12	0,2	5000	80000		=F3*B3	=F3*C3
4	Real Estate	0,09	0,25	20000	140000		=F4*B4	=F4*C4
5	Gold	0,08	0,15	5000	60000		=F5*B5	=F5*C5
6	Corporate Bonds	0,06	0,05	15000	120000		=F6*B6	=F6*C6
7	Government Bonds	0,04	0,01	10000	50000		=F7*B7	=F7*C7
8	Total					=SUM(F2:F7)	=SUMPRODUCT(F2:F7;B2:B7)	=SUMPRODUCT(F2:F7;C2:C7)
9								

Фигура 2. Въвеждане на необходимите формули в Excel

щаемост); =F2*B2; =F3*B3; =F4*B4; =F5*B5; =F6*B6;=F7*B7

- Риск за всеки отделен инструмент (инвестиции*макс. риск);=F2*C2; =F3*C3; =F4*C4; =F5*C5; =F6*C6; =F7*C7
- Общ риск = SUMPRODUCT(инвестиции, макс. риск) – трябва да е $\leq 10\%$ от 200 000 (т.е. $\leq$ 20 000); = SUMPRODUCT(F2:F7;C2:C7).

Обща възвращаемост = SUMPRODUCT (инвестиции, очаквана възвращаемост) – това е целева функция, на която намираме максимална стойност; =SUMPRODUCT (F2:F7;B2:B7).

За решението на задачата използваме помощния инструмент на Excel за оптимизационни задачи – Solver. Намира се в меню Data → Solver.

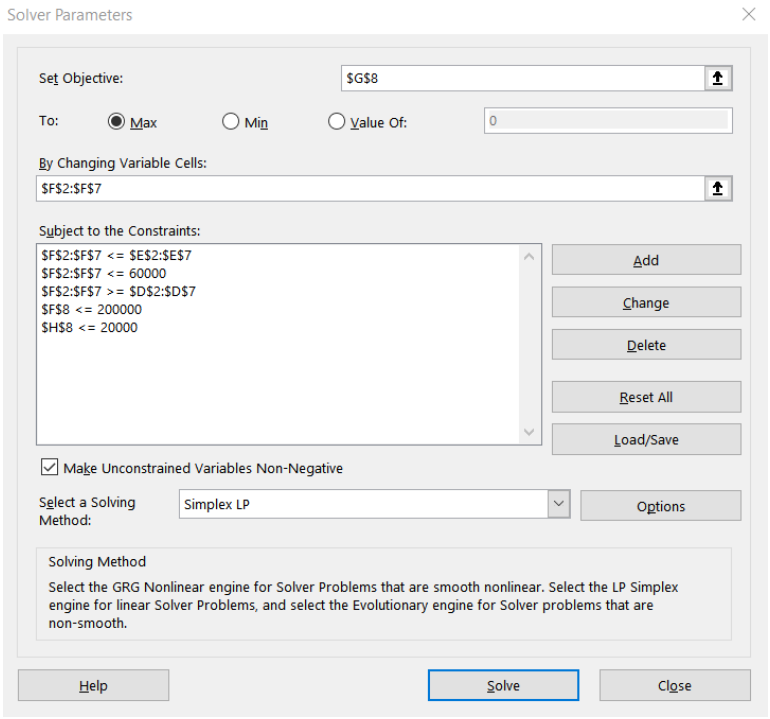
Както е показано на фиг. 3, в полето Set Objective поставяме клетката, в която се пресмята очакваната обща възвращаемост от инвестицията – G8. Избираме да намираме нейния максимум. В полето By Changing Variable Cells поставяме диапазона от клетки, който съответства на инвестиционната сума за всеки инвестиционен инструмент – F2:F7. След това въвеждаме условията, които вече поставихме в математическия модел на задачата, използвайки съответните адреси на клетки от таблицата. Избираме метода, чрез който ще пресмятаме – SimplexLP [4].

След избор на бутон Solve, Solver намира оптималното разпределение в колона F, което максимизира възвращаемостта, не надвишава общия допустим риск, спазва всички минимални и максимални ограничения за инвестиции и не инвестира повече от 30% в един актив. На фиг. 4 са представени резултатите от решението с Excel Solver, като максималната възвращаемост при съответните условия е 14 493,75 при неизползван максимално бюджет от 200 000, а именно 164 375 и максимален риск от 10% от бюджета.

На фиг. 5. е представено съобщението от програмата, с което получаваме потвърждение за получено оптимално решение на задачата.

Икономическа интерпретация на получените данни в контекста на обучението в профил „Предприемачески“

Въпреки че криптовалутите предлагат 25% печалба, се инвестират само 24 375 от 30 000. Това е така, защото са много рискови (40%) и имаме ограничение – не повече от 30% в един актив. В случая по-малката печалба е по-добро решение. Корпоративните облигации предлагат само 6% печалба, но получават най-много – 60 000, защото рискът им е малък (5%). Добрата инвестиция е добро съотношение между печалба и риск, а не само голяма печалба. Остават 35 625 неизползвани от 200 000.



Фигура 3. Въвеждане на условия в Excel Solver

	A	B	C	D	E	F	G	H
1	**Instrument**	**Expected Return**	**Max Risk**	**Min Investment**	**Max Investment**	**Amount Invested**	**Return Contribution**	**Risk Contribution**
2	Cryptocurrencies	25%	40%	1 000	30 000	24 375	6 094	9 750
3	Stocks	12%	20%	5 000	80 000	5 000	600	1 000
4	Real Estate	9%	25%	20 000	140 000	20 000	1 800	5 000
5	Gold	8%	15%	5 000	60 000	5 000	400	750
6	Corporate Bonds	6%	5%	15 000	120 000	60 000	3 600	3 000
7	Government Bonds	4%	1%	10 000	50 000	50 000	2 000	500
8	**Total**					164 375	**14 493,75**	**20 000**

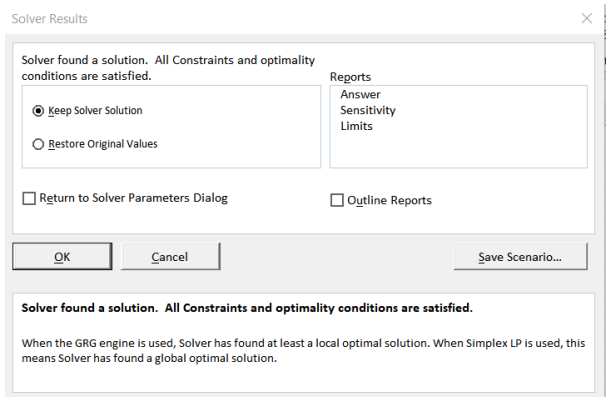
Фигура 4. Резултати от изчисленията с Excel Solver

Това е така, защото са изпълнени всички задължителни минимуми. Ако остатъка се инвестира в нещо с ниска печалба, ще се намали средната възвращаемост. Акциите предлагат 12% печалба, но получават само минимума от 5 000, защото при техния риск от 20% имаме по-добри варианти (корпоративни облигации дават 6% с много по-малък риск).

За учениците от 12. клас научаването на такъв тип задачи и решаването им с помощта на MS Excel е особено полезно, като им помага да използват научения алгоритъм в проектите си по предприемачество и бизнес.

Въвеждане на изкуствен интелект (ИИ) в помощ на учениците при изучаване на непозната материя

Интегрирането на ИИ в образованието е нелека задача. Целта на учителя е да покаже на учениците как правилно и смислено да използват мощта му. За целите на



Фигура 5. Съобщение за намерено решение в Excel Solver

образованието се използва генеративен изкуствен интелект, като най-често използваните езикови модели са: ChatGPT, Gemini, Claude, Copilot, DeepSeek, Perplexity и др. Обикновено се използват безплатните версии на моделите, които са по-ограничени, но подходящи за учебни цели. Изследваната група ученици използва предимно ChatGPT в помощ при написване на домашните си. Тъй като учениците имат опит с този чатбот, отговорите на поставените въпроси те трябва да получават с негова помощ. Освен това, за да се направи сравнение между отговорите от различни езикови модели, учителят включва и използването на езиковия модел на Google – Gemini. От учениците не се изисква решението на задачата с ИИ, тъй като то в повечето случаи е доста дълго, изпълнено с неясна терминология и объркващо за тях. Разбира се, винаги има любопитни, които, виждайки дългите обяснения на чатбота, само прелистват отговора. Част от по-запознатите с работата с ИИ задават конкретен въпрос за решението на задачата с Excel Solver, като получават постъпков алгоритъм за решение на задачата, който обикновено трудно изпълняват без помощта на учителя.

„Какъв е математическият модел на задачата?“ Учениците получават подробен отговор и с двата модела, който се различава само по стила на описание.

Тъй като за да получим подходящ за възрастта и знанията на учениците отговор, е от голямо значение какво ще бъде нашето запитване (prompt), то насоките от учителя към учениците са да се включват повече допълнителни инструкции, описание на контекст, очакван резултат, примери. Обяснява се на учениците същността на генеративния ИИ, т.е. че тези езикови модели са обучени да следват инструкции, затова тези инструкции трябва да са по-детайлни за стил, тон, формат и др. В тази връзка, за въпроса „Какви математически елементи и понятия от изучаваните до момента разпознавате?“, отговорите, които получават учениците, донякъде се разминават с очакваните, защото моделът не е получил подробни указания. При включване на допълнителна информация към чатбота за класа, в който се обучават в учениците в момента (12. клас), те получават отговор, в който са включени само понятия от контекста на изучавания материал по математика в 12. клас (включва се и материала от профилираното обучение по математика, който учениците не изучават). Ако запитването се разшири за материала по математика от 1. – 12. клас,

то тогава отговорите са доста обширни и конкретни, припомняйки на учениците математически понятия от целия им курс на обучение по математика в училище.

За отговора на въпроса: „Каква е икономическата интерпретация на задачата?“ също съществено значение имат инструкциите към чатбота. Сравнявайки отговорите, които получават, учениците забелязват, че в някои случаи отговорите са твърде сложно обяснени и са неразбираеми за тях. Чрез споделяне на екрана си пред класа всеки ученик показва своите резултати, получени с двата инструмента ChatGpt и Gemini. Прави се сравнение между получените отговори и се провежда дискусия за правилното използване на възможностите на ИИ.

Тъй като има ученици, които са експериментирали с въпрос към ИИ за директно решаване на задачата, разглеждат се и получените от тях отговори пред класа. Оказва се, че и двата чатбота се опитват да „прескочат“ част от ограничителните условия на задачата с цел получаване на по-голяма възвращаемост. Така получени решения на задачата объркват учениците, които все още нямат необходимите математически познания за съответната материя. Въпреки това, сравнявайки резултатите от получените решения, учениците правят изводи за разликата в получените резултати от решението на задачата с помощта на MS Excel и ИИ.

Предимството при използване на Excel Solver за решаване на задачи от линейното оптимиране е, че е лесен и интуитивен за употреба. Това, че Solver е инструмент от MS Excel, го прави по-познат като интерфейс и подходящ за ученици. Визуализацията на данните и възможността за бърза промяна на параметрите правят Excel удобен за генериране на различни примери и бързи анализи. Този метод е подходящ за по-прости задачи, включващи образователни примери. От друга страна, включването на ИИ в образованието е ключов момент за нови възможности в преподаването и по-лесното възприемане на сложния материал от учениците [3]. Фундаментална за икономиката наука като математиката може да бъде представена на разбираем и достъпен език за учениците. „Страхът от математиката“, който традиционно имат учениците, обучаващи се в профил „Предприемачество“, трябва да бъде преодолян с помощта на „различни“ методи и похвати. Създаването на интересно и провокиращо учебно съдържание е важна крачка към увеличаване на интереса на учащите се към математиката. 80% от тези ученици продължават обучението си в направление „Икономика“ във ВУЗ в страната, където тенденцията ще бъде увеличаване на приема с математика [5].

Заключение

Представените възможности за решаване на задачи от линейното оптимиране за управление на финансови ресурси предоставят ефективна възможност за автоматизиране на процеса на вземане на решения. В условията на онлайн и дистанционно обучение използването на софтуер значително подпомага усвояването и осмислянето на математически и икономически задачи, като в конкретния случай улеснява анализа на задачи за оптимално разпределение на ресурси.

Чрез представяне на два широко използвани подхода – Excel Solver и модели, базирани на изкуствен интелект – се демонстрира как съвременните технологии могат успешно да се прилагат за намиране на оптимални решения при разпределение на инвестиционен бюджет. Получените резултати показват, че и двата подхода са ефективни, като се различават по степен на гъвкавост, възможности за автоматизация и

ниво на абстракция. Excel Solver предлага лесен за използване и интуитивен интерфейс, което го прави особено подходящ за работа с ученици в гимназиалния етап, докато инструментите, базирани на изкуствен интелект, предоставят по-големи възможности за моделиране, анализ и експериментиране. Но от друга страна, поради склонността си към „халюцинации“ тези модели могат да заблудят учениците. В това отношение използването на ИИ може да бъде неефективно, поради голямата вероятност ИИ да генерира неверни и измислени твърдения, без да се основава на факти, да изкривява данни и др. По-голямата част от учениците нямат навика и търпението да проверяват информацията, която получават. Ролята на учителя трябва да бъде именно в изграждането на тези ключови умения и навици.

Приложението на тези методи в реални икономически модели допринася за по-обосновано вземане на решения и за по-ефективно използване на ограничени ресурси. Включването на софтуер при изучаването на математически задачи от икономиката, които традиционно затрудняват значителна част от учениците, повишава интереса им към учебното съдържание и създава условия за развитие на логическото мислене чрез математика.

Благодарности

Статията е подкрепена от Университетски проект за научни изследвания на УНСС-НИД НИ-19/2025/А.

This work was supported by UNWE Research Program, Research Grant Nr.**NID NI-19/2025/A.**

Литература

[1] K. Ivanova, T. Atanasova, Linear optimization. Mathematical methods in economics. Graduate School of Telecommunications and Posts. ISBN: 978 954 9332-93-3. (2015) (in Bulgarian)

[2] P. A. Kirschner, J. Sweller, R. E. Clark. Why minimal guidance during instruction does not work. (2006).

[3] R. Luckin, W. Holmes, M. Griffiths, L. B. Forcier. Intelligence Unleashed: An argument for AI in Education, pp. 23-30. Pearson. (2016)

[4] V. Tchernogorov. 2012. Solving linear optimization tasks with MS Excel 2010, Sofia University

[5] resolution No. 84 of June 6, 2025 on amendments and supplements to regulatory acts of the Council of Ministers, Republic of Bulgaria

МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2026
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2026
Proceedings of the Fifty-Fifth Spring Conference
of the Union of Bulgarian Mathematicians
Tryavna, Bulgaria, April 5–9, 2026

GAMIFICATION IN COMPUTER MODELING AND INFORMATION TECHNOLOGIES FOR 6TH GRADE: FUNCTIONS AND FORMULAS IN SPREADSHEETS

Elena Traykova[1], Miroslava Nikolova[2], Philip Petrov[3]
[1,3] Sofia University "St. Kliment Ohridski", Sofia, Bulgaria
[2] National High School of Natural Sciences and Mathematics "Acad. Lyubomir Chakalov", Sofia, Bulgaria
e-mails: [1]etraykova@fmi.uni-sofia.bg, [2]miroslava.nikolova@npmg.org, [3]philip@abv.bg

The article presents a technology for gamification in Computer Modeling and Information Technologies for the 6th grade. It was tested with students from the National High School of Natural Sciences and Mathematics "Acad. Lyubomir Chakalov". The authors formulated a hypothesis for the optimal application of the gamification teaching method.

Keywords: gamification, IT, spreadsheets, lower secondary school

ИГРОВИЗАЦИЯ ПО КОМПЮТЪРНО МОДЕЛИРАНЕ И ИНФОРМАЦИОННИ ТЕХНОЛОГИИ ЗА 6. КЛАС: ФОРМУЛИ И ФУНКЦИИ В ЕЛЕКТРОННИ ТАБЛИЦИ

Елена Трайкова[1], Мирослава Николова[2], Филип Петров[3]
[1,3] Софийски университет „Св. Климент Охридски", България
[2] Национална природо-математическа гимназия „Акад. Любомир Чакалов", София, България
e-mails: [1]etraykova@fmi.uni-sofia.bg, [2]miroslava.nikolova@npmg.org, [3]philip@abv.bg

Представено е технологично средство за игровизация в часове по Компютърно моделиране и информационни технологии в 6. клас. Извършена е апробация с ученици от Националната природо-математическа гимназия „Акад. Любомир Чакалов". Изказана е хипотеза за оптималното приложение на игровизацията в обучението.

Ключови думи: игровизация, ИТ, електронни таблици, прогимназия

https://doi.org/10.55630/mem.2026.55.265-271
2020 Mathematics Subject Classification: 97U50, 97U70.

1. Въведение

Поддържането на мотивацията за учене при учениците е едно от сериозните предизвикателства пред съвременното образование. Пренасищането на подрастващите с леснодостъпни, разнообразни, атрактивни и силно стимулиращи форми на забавление все по-често води до затруднения при фокусиране на вниманието им върху учебни задачи. Основен фактор за това са компютърните технологии. Децата още от „най-ранна възраст се потапят в необятния свят на технологии и още в предучилищна възраст стават техни активни ползватели“ [1]. Това неминуемо се отразява при училищното образование и все по-често учебните занятия се възприемат от учениците като безинтересни, а ученето се свежда до формално и неприятно задължение. В прогимназиален етап значителна част от учениците все още не осъзнават напълно стойността на образованието, не притежават устойчива самодисциплина, това води до натрупване на немалко дефицити.

Изправени пред тази даденост, съвременните учители полагат значителни усилия за разнообразяване на уроците. Сред утвърдените техники е *дидактическата анимация* [3], а в частност *игровизацията* [11] и *игрово-базираното обучение* [2, 4] са възможни подходи. Тези подходи са особено популярни през последните години при обучението по информатика, и то до степен да се приемат за утвърден модел. Свидетелство за това са редица научни изследвания в различни етапи на обучение – [5, 6, 7, 8, 12, 13] и др. Показателно за прилагането на игровизацията в световен мащаб е скорошно изследване [9] на обучението в начален етап. Резултатите от изследването са очаквани. Във възрастовата група от начален и прогимназиален етап учениците използват компютри и мобилни устройства предимно за да играят, т.е. игрите за тях са значими и интересни.

Когато в часове по информатика учителите преподават програмиране чрез създаване на компютърни игри, прави се естествена синергия между учебното съдържание и онова, което учениците оценяват като приятно и забавно – играят игрите, които сами създават. Не толкова лесно и тривиално е да бъдат приложени подобни методи по други учебни предмети. Това важи дори за Информационни технологии (ИТ) и много теми от Компютърно моделиране и информационни технологии (КМИТ), въпреки че са пряко обвързани с употреба на компютърна техника. В [2] се изтъква, че „учениците често губят интерес към изучаването на ИТ, защото не виждат връзка между придобитите знания и умения и ежедневните си задачи“. Причина е именно, че ежедневните им занимания с ИТ все по-често се свеждат само и единствено до играене на компютърни игри, а не с текстообработка, електронни таблици, презентации, графика и др. По-теоретичните теми са най-силно засегнати. Въпреки това и при тях игровизацията е възможна. Пример за това може да се посочи с [10], където методът е приложен за изучаване на въпроси от „компютърни мрежи“ и „компютърни вируси и информационна сигурност“ в гимназиален етап. Най-често подобни експерименти показват проява на позитивни емоции както при учениците, така и при техните учители, но не се наблюдава значимо повишаване на нивото на знания и умения на учениците. Затова търсеният ефект е по-скоро към позитивна нагласа за учене.

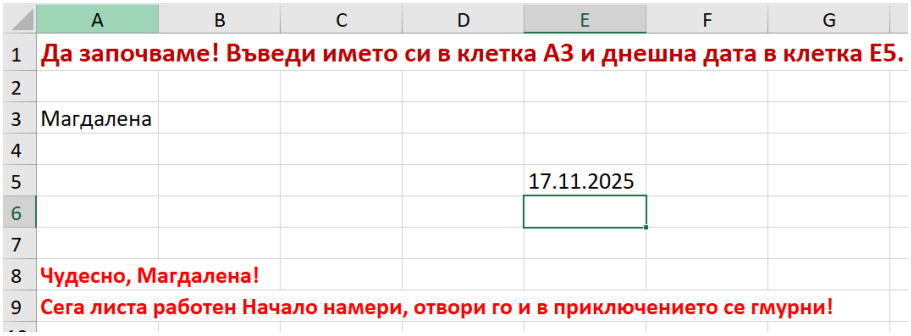
Настоящата статия представя постановка за използване на игровизация по КМИТ в урок за упражнение по една от традиционно трудните за преподаване теми от

учебната програма за 6. клас – обработка на таблични данни (формули и функции). Подходът е изпробван в реална учебна обстановка през първия срок на 2025/2026 г.

2. Игровизация при обучение с електронни таблици

Планът на урока е изготвен от първия автор в рамките на „Стажантска практика по информатика и информационни технологии“ към едногодишен курс за следдипломна квалификация към Факултета по математика и информатика на Софийския университет „Св. Климент Охридски“. Учениците, с които е апробиран, са шестокласници от Националната природо-математическа гимназия „Акад. Любомир Чакалов“ в град София. Урокът е предвиден за упражнение на вече изучавани функции в среда за електронни таблици (sum, min, max и average). Заложена е идея учениците да работят по електронна таблица (workbook) с множество различни работни листове (sheets), като на всеки лист е зададена задача с предизвикателство. Само при правилно решение на текущата задача (даване на верен отговор в точно определена клетка) се появява съобщение, което насочва учениците на кой работен лист трябва да продължат. Там те попадат на нова задача, чието вярно решение ги препраща към следващата (това се повтаря до достигане до финален работен лист). При подаване на погрешен отговор се предвиждат често допусканите от учениците грешки и пренасочването се извършва към работен лист с помощно съобщение.

Технологично, в Microsoft Excel, описаното може да се постигне изключително лесно, дори без използването на Visual Basic for Applications. Първата задача се намира на работния лист, визуализиращ се по подразбиране при отварянето на файла. Изисква се въвеждане на име и днешна дата (упражнение на типове данни) в точно определени клетки (упражнение на адресация на клетките). След въвеждане на данните в точен формат и на правилното място, се визуализира инструкция за следващата стъпка (фиг. 1).



Фиг. 1. Правилно въведен отговор при Задача 1

Фиг. 1. Правилно въведен отговор при Задача 1

За въвеждането на дата в коректен формат (и евентуално точна за съответния ден) за клетка E5 се използва инструментът *Data* > *Data Validation* > *Select Allow: Date*. Като се задава датата в определени граници, се подсигурява, че е въведена правилно. Съобщението при правилно въведени данни се показва на екрана с помощта на следните формули:

A8: =IF(AND(A3<>0,E5<>0),CONCATENATE("Чудесно, A3,"!"),)

A9: =IF(AND(A3<>0,E5<>0), "Сега листа работен Начало намери, отвори го и в приключението се гмурни!)

За да бъдат скрити заложените формули и да не бъдат откриваеми при обхождане по екрана, е извършена „защита“ на съответните клетки (*Format Cells > Protection > Hidden*) и на работния лист (*File > Protect Workbook > Protect Current Sheet*). Така дори когато някоя от клетките е избрана като текуща, зададените формули не се виждат.

Самите задачи са разнообразни, както и начините, по които са формулирани. За втората задача е предвидена цветна таблица с въведени различни математически изрази и символи. От учениците се очаква да намерят израз от една конкретна клетка и да го изчислят. При даване на верен отговор, записан в точно определена клетка (B10), отново се появява съобщение, насочващо към следващия работен лист и към следващата задача. В конкретната задача решението е –68,8, а формулата за показването на съобщението е:

B10: =IF(B10=-68.8,

CONCATENATE("Браво, Sheet1!A3,"! Отиди на лист с име Сол!"),)

Третата задача (фиг. 2) е създадена по идея от учебника [14, с. 33]. Като се ползват данни за измервания на температурата на различни дати в три часови диапазона (сутрин, обед и вечер), от учениците се очаква да извършат съответното агрегиране по тях.

1	Разгледай таблицата, в края погледни и задачата свърши!			
2				
3	Дата	Температура		
4		Измерване сутрин	Измерване по обяд	Измерване вечер
5	1.10.2025	0	10	5
6	2.10.2025	1	12	6
7	3.10.2025	-1	8	6,1
8	4.10.2025	2	12	10
9	5.10.2025	4	15	8
10	6.10.2025	3,5	14	10
11	7.10.2025	2,2	16	9,5
12	8.10.2025	9,3	21	10,1
13	9.10.2025	8,9	20,7	9
14	10.10.2025	8,6	15	10
15	11.10.2025	6,8	10	9,8
16	12.10.2025	7,2	21	10,1
17	13.10.2025	2,9	15,4	10
18	14.10.2025	6,5	15,9	9,9

31	27.10.2025	1,2	16	9,8
32	28.10.2025	3,6	19,1	8,3
33	29.10.2025	3,9	18	7,6
34	30.10.2025	4,6	20,1	10,5
35				
36	Минималната температура сутрин:			
37	Максимална температура сутрин:			
38	Средна температура сутрин:			
39				
40	Средна температура по обяд:			
41				
42	Средна температура вечер:			
43				
44	Средна средна температура: *средноаритметично на средните температури*			
45	Средната средна температура намери и листа с този номер отвори!			

Фиг. 2. Постановка на Задача 3

Като допълнителен дидактически елемент с междупредметна връзка с математиката може да се постави въпрос към учениците „дали средното на средните стойности е същото като средното на всички стойности?“.

При правилни изчисления учениците разбират, че трябва да отидат на работен лист с име *sheet9.45* (9,45 е очакваният верен отговор). В четвъртата задача (фиг. 3) се изисква изчисление на обща цена за 20 продукта (количество, умножено по единична цена) в лева и после превръщане на левовете в евро по зададения курс. Следва да се изчисли обща сума, ДДС и сума за плащане (в лева и в евро):

Последната задача е създадена по идея от подобна в учебника [15, с. 32] и е с препратка към предстоящите коледни празници. Инструкцията към задачата е:

	A	B	C	D	E	F
1	**Бързичко счетоводител ти стани,**					
2	**фактурата за магазина довърши!**					
3	**Внимавай парите да не оплетеш,**					
4	**сумите в евро като преведеш!**					
5	**Дата на фактурата сложи,**					
6	**данъчен служител да не те глоби.**					
7	*1€ = 1,95583*					
8						
9	**Фактура - зареждане на магазин ЕКСЕЛънс**					
10	Дата на фактурата:					
11						
12	Артикул	Количество	М.ед.	Единична цена в лв.	Обща цена в лв.	Обща цена в €
13	Хляб, бял	100	бр.	2.90 лв.		
14	Хляб, типов	120	бр.	2.00 лв.		
15	Хляб, пълнозърнест	90	бр.	2.50 лв.		
16	Кисело мляко 2%	200	бр.	1.80 лв.		

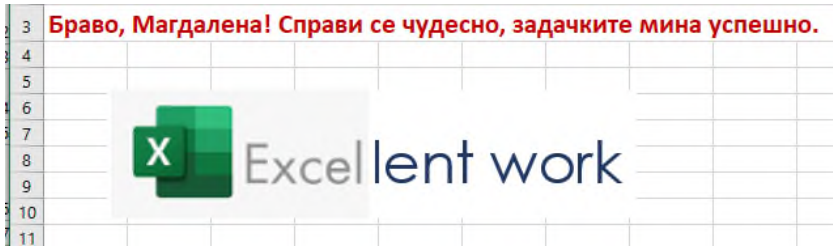
(1) **ОБЩО:**	
(2) **ДДС 20%**	
ОБЩО ЗА ПЛАЩАНЕ: (1) + (2)	

Фиг. 3. Постановка на Задача 4

На 1 декември две елфчета правят по 100 подаръка, като от следващия ден всяко елфче подготвя различен брой подаръци. Едното елфче подготвя броя подаръци от предния ден плюс брой подаръци, равен на датата по 2, а другото – броя подаръци от предния ден плюс още 18.

В поместена таблица се очаква учениците да оформят изрази за пресмятане на броя подаръци, подготвяни от всяко елфче през всеки ден, и да посочат кое елфче ще подготви най-много подаръци до различни периоди през месеца. Отговорите се посочват в конкретни клетки, чрез падащи списъци.

Правилното решение на последната задача води до финалния работен лист, на който се получава и наградата под формата на поздравление за добрата работа (фиг. 4).



Фиг. 4. Последен работен лист с поздрав за добре свършена работа

3. Резултати и заключение

Очакванията на авторите за проведения урок се оправдаха. Учениците работиха, без да се разсейват със странични дейности, общуваха помежду си и си помагаха. Бяха отчетливо по-активни спрямо обичайното. Очаквано, в хода на работата се налагаше и оказване на помощ на отделни ученици по разясняване на условия и откриване на технически грешки. В края на часа отзивите бяха показателни: децата искрено се вълнуваха дали ще има подобни задачи с игри и през следващата седмица, което еднозначно показа, че обучението им е харесало.

След провеждане на контролна работа в края на раздела и сравняване на резултатите от различните паралелки може да се заключи, че експерименталният урок не е довел до натрупване на повече знания и умения. Мнението на базовия учител е, че ефектът от урока е основно с мотивационен характер и евентуално би имал отражение върху трайността на усвоеното и нагласата към ученето в средносрочен и дългосрочен план.

След проведения урок авторите затвърдиха своите предварителни очаквания и формирана хипотеза, че игровизацията е по-адекватно да бъде прилагана в уроците за упражнение, а не при въвеждането на нови знания. Подходът дава съществено различен контекст за приложение на вече изучени знания и стимулира активното взаимодействие и обмена на знания между учениците.

Предвижда се изследването да бъде продължено в 11. клас по ИТ (профилирана подготовка) в уроците за ограничения и защита на електронни таблици, като на учениците ще се възложи да подготвят (под формата на проектно-базирано обучение) свои авторски учебни материали, в съответствие с описания технологичен модел, които впоследствие да се ползват като задачи игри за по-малките ученици.

Литература

[1] З. Димитрова. Педагогически аспекти на феномена „дигитално детство" и дигиталната социализация на децата от поколението „Алфа". Съвременна хуманитаристика, (1), 6-27, 2022. [Z. Dimitrova. Pedagogicheski aspekti na fenomena „digitalno detstvo" i digitalnata sotsializatsiya na detsata ot pokolenieto „Alfa". Savremenna humanitaristika, (1), 6-27, 2022.] (in Bulgarian)

[2] S. Ivanov. Using gamification methods in information technology education. In EDULEARN19 Proceedings (pp. 2712-2718). IATED. 2019.

[3] А. Калчева. Ролята на учителя като аниматор. Педагогика, 87(5), 693-701, 2015. [A. Kalcheva. Rolyata na uchitelya kato animator. Pedagogika, 87(5), 693-701, 2015.] (in Bulgarian)

[4] Т. Терзиева. Развитие на когнитивни умения чрез компютърни образователни игри. Педагогика, 93(7), 879-888, 2021. [T. Terzieva. Razvitie na kognitivni umeniya chrez kompyutarni obrazovatelni igri. Pedagogika, 93(7), 879-888, 2021.] (in Bulgarian)

[5] Р. Георгиева. Игрово базирано обучение по програмиране за начинаещи в режим на Pygame Zero – примерни задачи с turtle графика на Python. Математика и информатика, 66(2), 170-187, 2023. [R. Georgieva. Igrovo bazirano obuchenie po programirane za nachinaeshti v rezhim na Pygame Zero – primerni zadachi s turtle grafika na Python. Matematika i informatika, 66(2), 170-187, 2023.] (in Bulgarian)

[6] М. Узунова. Прилагане на игровия подход в обучението по информатика. Knowledge: International Journal, 54(2), 2022. [M. Uzunova. Prilagane na igroviya podhod v obuchenieto po informatika. Knowledge: International Journal, 54(2), 2022.] (in Bulgarian)

[7] Е. Горанова. Изграждане на компетенции за разработване на компютърни игри по компютърно моделиране у бъдещи учители. Годишник на Тракийски университет, Том 21, 2024. [E. Goranova. Izgrazhdane na kompetentsii za

razrabotvane na kompyutarni igri po kompyutarno modelirane u badeshti uchiteli. Godishnik na Trakiyski universitet, Tom 21, 2024.] (in Bulgarian)

[8] С. Нейкова-Карагаева. Геймификация: инструмент за повишаване на мотивацията и постиженията на учениците в профилираното обучение по информатика. Информационни и комуникационни технологии в бизнеса и образованието (pp. 187-195), Икономически университет-Варна, 2024. [S. Neykova-Karagaeva. Geymifikatsiya: instrument za povishavane na motivatsiyata i postizheniyata na uchenitsite v profiliranoto obuchenie po informatika. Informatsionni i komunikatsionni tehnologii v biznesa i obrazovanieto (pp. 187-195), Ikonomicheski universitet-Varna, 2024.] (in Bulgarian)

[9] Л. Алексиева, Г. Костадинова, Д. Илиева, Д. Кенанова. Подходи за преподаване на информационни и комуникационни технологии в началните класове в България и по света: сравнителен анализ и препоръки за развитие. Педагогически и социални изследвания, 8(2), 3-36, 2024. [L. Aleksieva, G. Kostadinova, D. Ilieva, D. Kenanova. Podhodi za prepodavane na informatsionni i komunikatsionni tehnologii v nachalnite klasove v Balgariya i po sveta: sravnitelen analiz i preporaki za razvitie. Pedagogicheski i sotsialni izsledvaniya, 8(2), 3-36, 2024.] (in Bulgarian)

[10] Г. Карабельова, Ф. Петров. Приложение на играта „Аз имам..., кой има...?“ при преговорни уроци по информационни технологии в прогимназиален и гимназиален етап. Математика и информатика, 65(4), 2022. [G. Karabelyova, F. Petrov. Prilozhenie na igrata „Az imam..., koy ima...?“ pri pregovorni urotsi po informatsionni tehnologii v progimnazialen i gimnazialen etap. Matematika i informatika, 65(4), 2022.] (in Bulgarian)

[11] K. Kapp. The Gamification of Learning and Instruction: Game-based Methods and Strategies for Training and Education. John Wiley & Sons, 2012.

[12] D. Tuparova, G. Tuparov, V. Veleva, E. Nikolova. Educational Computer Games and Gamification in Informatics and Information Technology Education – Teachers‘ Points of View. 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), 0766 – 0771. IEEE, 2018.

[13] С. Анева, Е. Тодорова. Развитие на дигитални и алгоритмични умения на учениците чрез използване на Visual Basic For Applications. Математика и информатика, 67(3), 2024. [S. Aneva, E. Todorova. Razvitie na digitalni i algoritmichni umeniya na uchenitsite chrez izpolzvane na Visual Basic For Applications. Matematika i informatika, 67(3), 2024.] (in Bulgarian)

[14] А. Ангелов, Д. Тупарова, Г. Тупаров, К. Марчева, К. Стоянова, М. Спирова. Компютърно моделиране и информационни технологии за 6. клас. Просвета плюс. 2022. [A. Angelov, D. Tuparova, G. Tuparov, K. Marcheva, K. Stoyanova, M. Spirova. Kompyutarno modelirane i informatsionni tehnologii za 6. klas. Prosveta plyus. 2022.] (in Bulgarian)

[15] Н. Николова, Е. Стефанова, М. Николова, Д. Петрова, О. Константинов, С. Иванов. Компютърно моделиране и информационни технологии за 6. клас. Просвета, 2022. [N. Nikolova, E. Stefanova, M. Nikolova, D. Petrova, O. Konstantinov, S. Ivanov. Kompyutarno modelirane i informatsionni tehnologii za 6. klas. Prosveta, 2022.] (in Bulgarian)

IN MEMORIAM

МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2026
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2026
Proceedings of the Fifty-Fifth Spring Conference
of the Union of Bulgarian Mathematicians
Tryavna, Bulgaria, April 5–9, 2026

IN MEMORIAM: IVAN TONOV – THE MAN FOR WHOM MATHEMATICS WAS AN ADVENTURE, HEURISTICS – A GUIDE, AND HUMOR – A JOYFUL "AHA"

Philip Petrov[1], Evgenia Sendova[2]
[1]Sofia University "St. Kliment Ohridski", Sofia, Bulgaria
[2]Institute of Mathematics and Informatics, Bulgarian Academy of Sciences, Sofia, Bulgaria
e-mails: [1]philip@abv.bg, [2]jenny.sendova@gmail.com

On September 30, 2025, Prof. Ivan Tonov set out on his final journey. He was our dear friend and an irreplaceable colleague! Representatives of several generations gathered for the farewell, transforming the sad occasion into a celebration of his life! Everyone carried memories filled with love and admiration: his remarkable seminars with *wordless theorems*; the witty "Tonov problems"; the numerous textbooks to which he made invaluable contributions; his devoted work with young mathematical talents; and his deep care for future mathematics teachers, who, in his words, *must know how to realize the connection between academic and school mathematics*, while respecting the specifics of both...

For Tonov there was no better practice than science itself, and his love for mathematics was always something to be shared — with students, teachers, and colleagues from all over the world.

Keywords: in memoriam, Ivan Tonov

IN MEMORIAM: ИВАН ТОНОВ – ЧОВЕКЪТ, ЗА КОГОТО МАТЕМАТИКАТА БЕШЕ ПРИКЛЮЧЕНИЕ, ЕВРИСТИКАТА – ПЪТЕВОДИТЕЛ, А ХУМОРЪТ – РАДОСТНО „АХА"

Филип Петров[1], Евгения Сендова[2]
[1] Софийски университет „Св. Климент Охридски", София, България
[2] Българска академия на науките, София, България
e-mails: [1]philip@abv.bg, [2]jenny.sendova@gmail.com

На 30 септември 2025 г. изпратихме в последния му път проф. Иван Тонов – скъп приятел и незаменим колега! На поклонението се стекоха представители на няколко поколения, които превърнаха скръбното събитие в прослава на живота му! Всеки имаше какво да си спомни с обич и възхита – прекрасните му семинари с теореми

https://doi.org/10.55630/mem.2026.55.275-281
2020 Mathematics Subject Classification: 01A70.

без думи, остроумните „задачи-тоновки“, многобройните учебници с безценното му участие, работата му с младите математически таланти; грижата му за бъдещите учители, които „трябва да знаят как да реализират връзката между академичната и училищната математика“, като държат сметка за спецификата и на двете... За него нямаше по-добра практика от науката, а любовта му към математиката беше предмет на споделяне с ученици, учители и колеги от цял свят!

Ключови думи: in memoriam, Иван Тонов

Проф. Тонов завършва висше образование в Софийския университет през 1970 г. като „Специалист по алгебра“ с квалификация „Преподавател в средните училища“. През първите години от работната си кариера е научен сътрудник в Математически институт при БАН. През 1981 г. защитава кандидатската си дисертация на тема „Многообразия от асоциативни алгебри“, а три години по-късно става доцент в Математическия факултет на Софийския университет. Постепенно насочва усилията си в подготовката на учители по математика и посвещава кариерата си на тази тематика.

В първите години от научната му кариера стават особено популярни неговите книги от серията „Алеф“ [1, 2, 3, 4]. По-късно се фокусира в написването на методическа литература за основни и средни училища. Много са учебниците и учебни помагала за ученици и студенти, на които проф. Тонов е бил автор или съавтор. Внушителен е и броят на научните му публикации в областта на алгебрата (алгебри с тъждествени съотношения), теория на числата, дидактика на математиката, състезателната математика и др.

Особено сполучлива линия на творческо му търсене е развитието на евристичните методи за решаване на задачи по математика и методите за работа с талантливи ученици. Един от първите му по-обемни трудове [5] е именно сборник със задачи от математически състезания. През последните 50 години Тонов е бил автор на огромен брой задачи за олимпиади и състезания. През 1997 г. става инициатор и съосновател на Младежката балканска олимпиада по математика. Също така ръководи отбора на България в Международната олимпиада по математика. Около същата тематика той създава и магистърската програма „Технологии за обучение по математика и информатика“. През 2012 г. става професор във Факултета по математика и информатика на СУ „Св. Климент Охридски“ с тема на хабилитационния труд „Евристиката – наука, изкуство, занаят“ [6], който беше издаден през настоящата година (2025) и само след месец се наложи да се допечатва с втори тираж.

В академичния живот на Факултета по математика и информатика проф. Тонов беше член и ръководител на катедра „Обучение по математика и информатика“, както и заместник-декан. В Съюза на математиците в България е член от 1971 г., като през 1982 г. е избран за член на Централното ръководство (сегашен Управителен съвет) и няколко мандата е заместник-председател. Участвал е в организацията на редица научни семинари и конференции, олимпиади и конгреси. Член е на Германското математическо дружество.

Връзката между Иван Тонов и съпругата му Таня беше емблематична за Факултета по математика и информатика. Когато някой имаше служебна среща с някого от тях, той не казваше „отивам при Тонов/Тонова“, а „отивам при Тонови“. Те бяха

винаги неразделни! Имаха обща визия за развитието на математическото образование и я допълваха по собствен уникален начин. Тя може да се илюстрира с последното изречение от анотацията на едно от техните учебни помагала [9, 10, 11, 12]: *И в двете части се акцентира върху логическото мислене и развиването на наблюдателност, въображение и съобразителност.* За Иван Тонов математиката беше не просто техника за решаване на задачи, а също така изкуство, което развива творчески заложби. Доц. Тонова, като негов достоен съратник, цитира това виждане в своята докторска дисертация [13] чрез цитат от монографията му [6]: *От голямо значение е изследователският подход в обучението на учениците и студентите. Този подход се проявява в решаването на всяка задача, при преподаването на всеки елемент от новите знания и затвърдяването на вече изучения материал. Необходимо е учащите се да се потопят в подходяща изследователска среда – в кухнята на математическото изследване...*

Също така проф. Тонов беше изразен противник на прекомерните регулации. В последното си участие на конференцията на Съюз на математиците в България, в пленарната зала той не се поколеба да се възпротиви срещу някои от догматично наложените норми, както и срещу част от предлаганите промени, и попита Министъра: *Защо българските ученици вече не учат математика, а учат „за НВО“?* Неколкократно е споделял и възмущението си, че при промени на учебни програми *нито веднъж не са се допитали до катедрата ни за мнение.* Уви, тази негова битка остана незавършена. Нека ние, неговите последователи, я продължим и доведем до край!

Ще споделим накратко някои впечатления на колеги и приятели.

Жени Сендова *(приятел и съавтор): Помня с обич и умиление разговорите ни с Иван (още от студентските му години) и съвместните писания на учебници и материали в математически списания на тема образование. И до днес си припомняме с колеги и приятели дълбочината на възгледите му на тема „Евристика“, класификацията на задачите от „упражнение“ до „отворен проблем“, съпровождани с шеговити цитати и случки в математически контекст. На една лекция пред членовете на секция „Образование по математика и информатика“, ИМИ–БАН (фиг. 1), той сподели удоволствието от последната си находка в предизвикателствата пред нас, загрижените за математическото образование: „Modeling the master teacher and teaching the master model – това трябва да следваме в работата си и няма да развалям тази мисъл със собствен превод. . . “*

Един от разговорите ми с Иван на тема тестове през 1993 г. се превърна в статията PRO TEST? – ПРОТЕСТ [8]. Мисля, че тя е актуална и до днес, затова ще приведа фрагменти от този разговор:

> *Той:* Напоследък все това се носи из въздуха: „Всичко ще се решава с тестове!“ Само дето не ми е съвсем ясно кое е това всичко. . .
>
> *Аз*: Е, това е естествена реакция на лозунги от типа: „Кадрите решават всичко“ или на ходатайства в стил: „Внимавай, като го изпитваш, той е наше момче. . .“. И само като легенда до нас достигаше, че „в някои страни тапията е нищо, важно е какъв коефициент на интелигентност ще покажеш на теста. . .“
>
> *Той:* Не казвам, че тестовете са лошо нещо, даже в определени ситуации



Фиг. 1. Поканен доклад в секция *Образование по математика и информатика*, Институт по математика и информатика, Българска академия на науките

може да са много полезни – например за преодоляване на някои технически грешки, които децата в началното училище често допускат. Въпросът е да не фетишизираме тестовете като единствено и универсално средство за изпитване. Ако съдим за математическите знания на децата само по резултатите, показани на тестове, не поставяме ли в неизгодно положение тези, които честно смятат, но не получават нито един от посочените отговори. В същото време някой, без да знае как да реши задачата, може да избере верен отговор.

Аз: От друга страна, не е ли много важно човек да може да прави „груба“ оценка на отговора и да избере един разумен резултат...

Той: Нямам нищо против стратегията на учениците, които избират верния резултат, като елиминират неправдоподобните резултати. Но представи си реакцията на човек, който не получава нито един от посочените отговори. Какво ще бъде неговото психическо състояние?

Аз: Искаш да кажеш, че понякога е важен не конкретният отговор, а пътят, по който ученикът е стигнал до него. Например в теста на фиг. 2 се пита: *Коя от дадените по-долу фигури е излишна?.* Учениците биха имали основание да изберат всеки един от отговорите:

A – защото е единствената фигура без черна точка

B – защото е единствената фигура без защрихована рамка

C – защото е единствената фигура без правоъгълна форма

D – защото е единствената фигура без защрихована вътрешност

E – защото е единствената фигура, която не се отличава с категоричен признак

Авторът на теста обаче явно е имал предвид само една възможност...

Той: Разбира се, не става въпрос въобще да се откажем от тестовете. Те са много полезни при усвояване на конкретни сръчности. Тестовете могат



Фиг. 2. Тест, дискутиран в английското списание PLUS

да обогатят традиционното изпитване, но в никакъв случай не трябва да го изместват.

При друг случай коментирахме с Иван как да разнообразим условията на задачите за най-малките така, че да разберат, че и в „мини“-математиката се изисква разум и досетливост. Така се роди задачата „Тинтири – минтири“ (публикувана в рубриката m+ на списание Математика плюс, бр. 2 от 1993 г.), която за мен е типична „тоновка“:

> Фирмата „Дрън-дрън“ предлага най-новите си стоки – тинтири и минтири. Оказва се, че 175 тинтири струват по-скъпо от 125 минтири, но по-евтино от 126 минтири. Ако е известно, че стоките в „Дрън-дрън“ струват винаги цяло число лева и аз имам само 100 лева, ще мога ли да си купя 3 тинтири и 1 минтири?

Сега, като се замислих, се запитах как ли всъщност е единственото число на „минтири“. Няма начин да е „минтир“, както предлага ChatGPT, но Иван Тонов винаги ми е оставял храна за размисъл дори когато съм можела да реша задачата му...

Снежинка Матакиева (автор на учебници и учебни помагала, бивш експерт по математика в МОН и най-вече завинаги учител): *Споменете ми за проф. Тонов датират от далечната 1991 г. Тогава реших да се преквалифицирам и тъй като имах завършен „научен профил магистърски блок В“, а нямах учителска правоспособност, записах ускорен курс за следдипломна квалификация към ФМИ на Софийския университет. Професор Тонов ни водеше лекции по Увод в теория на числата. Неговата аудитория винаги беше препълнена. Голям ерудит, а сладкодумец – нямаше равен. Всички ние със затаен дъх слушахме лекциите му. Мъдър, духовит и същевременно много земен. Нямаше бариери от типа студент – преподавател. Всички ние го обожавахме.*

Друг ярък спомен за професора е от съвместната ни работа, когато работех като експерт в МОН, а проф. Тонов беше председател и в последствие активен член на комисията от Института по математика и информатика, която подготвяше задачите за олимпиади и състезания. Както винаги, той беше точен, акуратен, с грижа за учениците да се открие и развива техният математически талант. Самият той бивш състезател, не щадеше сили да предаде своите знания и опит на по-младите.

Рядко се ражда толкова интелигентен и съпричастен към знанието човек, оставил светла диря след себе си!

Ани Търсанкова (дългогодишен секретар на списание „Математика и информатика“) по повод задачите ни припомни за едно заседание на редколегията, на

което започнала да чете изпратени материали за математически конкурс с авторски задачи. При една от тях Иван просто подскочил и извикал: *Аз тази задача вече съм я решавал!*

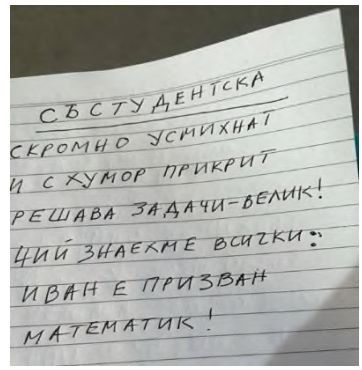
Филип Петров (студент и колега): *В един от първите ми разговори, вече като колеги във ФМИ, споделих с проф. Тонов, че много трудно помня имена и дати, поради което историята в училище винаги ми е била мъчен предмет. Тогава той буквално ме обсипа с информация за различни български и световни математици – кой в коя година какво бил открил, кой на кого кое твърдение бил оборил, и подобни неща. Честно казано в онзи момент не проумявах дали го прави, защото съм го предизвикал да ме научи на нещо, или за да ми покаже очевидното си превъзходство. Все едно стоях пред човек, който е жива математическа енциклопедия!*

Само няколко месеца по-късно същият проф. Тонов истински запали искрата на интереса ми към историята на математиката. На Пролетната конференция на СМБ през 2016 г. в град Плевен той представи статията си „Великото изкуство“ или чудесата на XVI век“ [7]. С обаятелния си разказ за Лука Пачоли, Сципион дел Феро, Николо Тарталя, Джероламо Кардано и Луиджи Ферари проф. Тонов ме потопи в една изцяло нова за мен атмосфера. Изведнъж разбрах, че „сухата теория“ не само е жива, а е и подвластна на биологичните закони – теориите всъщност можели да мутират и да еволюират по същият начин, както се случва с хората, животните и растенията.

Това меко казано беше един повратен момент за моята кариера. Искрено ми се ще по някакъв начин аз да съм мотивирал проф. Тонов да напише тази красива статия (както се казва – „ама надали“), но не това е най-важното. По-ценен беше урокът, който получих. Урок, който зароди любовта ми към историята. Урок, който ме накара да разбера, че научните спорове са полезни. Урок, който ме вдъхнови и аз да търся как да използвам исторически примери по време на преподаването си. Защото „този исторически подход може да послужи като стратегически резерв за повишаване качеството на обучението по математика и повишаване на уменията на учениците да решават задачи“ [7].

Петър Кендеров (академик в Българска академия на науките) разказа за находчивостта на Иван Тонов в житейски ситуации: *Корените на Ученически институт по математика и информатика (УчИМИ) са много дълбоки. Следи от тях намираме в Ученическата секция на СМБ, организирана от Физико-математическото дружество на Стара Загора още през 30-те години на миналия век. Вече в по-нови времена, на Ученическата секция на пролетна конференция на СМБ някъде през 80-те години, с екип от млади математици, включващ Иван Тонов, Любомир Давидов и Чавдар Лозанов, трябваше да определим най-добре представилите се автори на изследователски проекти и реферати и да разпределим наградите. Оказа се, че проектът, удостоен с първа награда – ръчен часовник, има двама автори. Докато умувахме какво да правим, Иван Тонов усмихнато заяви: „Много просто – единият ще го носи първите шест месеца, а вторият – следващите шест...“.*

Последната приятелка, която се отзова чак от Нова Зеландия със спомен за Иван Тонов от студентските им години, бе **Краси Попова**, (днес Krassie Petrova, Senior Research lecturer at the Auckland University of Technology, Dept of Computer Science & Software Engineering, Auckland):



Тази оценка, идваща от връстниците му по време, когато правят първи стъпки в математическите изследвания, и запазена до днес, говори много!

Поклон пред всичко, което си направил за математиката и математическото образование през живота си, скъпи приятелю! Следата, която си оставил, вдъхновява и ще вдъхновява поколения занапред!

Литература

[1] Иван Тонов. Приложение на комплексните числа в геометрията. Народна просвета, София, 1988. [Ivan Tonov. Prilozhenie na kompleksnite chisla v geometriyata. Narodna prosveta, Sofiya, 1988.] (in Bulgarian)

[2] Иван Тонов. Матрици и детерминанти. Народна просвета, София, 1979 г. [Ivan Tonov. Matritsi i determinanti. Narodna prosveta, Sofiya, 1979 g.] (in Bulgarian)

[3] Иван Тонов. Комплексни числа. Народна просвета, София, 1977. [Ivan Tonov. Kompleksni chisla. Narodna prosveta, Sofiya, 1977.] (in Bulgarian)

[4] Иван Тонов. Срещи с алгебрата. Народна просвета, София, 1984. [Ivan Tonov. Sreshti s algebrata. Narodna prosveta, Sofiya, 1984.] (in Bulgarian)

[5] Иван Тонов, Л. Давидов, В. Чуканов, В. Петков. Математически конкурси. Народна просвета, София, 1977. [Ivan Tonov, L. Davidov, V. Chukanov, V. Petkov. Matematicheski konkursi. Narodna prosveta, Sofiya, 1977.] (in Bulgarian)

[6] Иван Тонов. Евристиката – наука, изкуство, занаят. Университетско издателство „Св. Климент Охридски“, ISBN: 978-954-07-6142-8, София, 2025. [Ivan Tonov. Evristikata – nauka, izkustvo, zanayat. Universitetsko izdatelstvo „Sv. Kliment Ohridski“, ISBN: 978-954-07-6142-8, Sofiya, 2025.] (in Bulgarian)

[7] Иван Тонов. „Великото изкуство“ или чудесата на XVI век. Математика и математическо образование, СМБ, Плевен, 2016. [Ivan Tonov. „Velikoto izkustvo“ ili chudesata na XVI vek. Matematika i matematichesko obrazovanie, SMB, Pleven, 2016.] (in Bulgarian)

[8] Евгения Сендова. Pro test? – протест. Обучението по математика и информатика, бр. 2, 1993. [Evgeniya Sendova. Pro test? – protest. Obuchenieto po matematika i informatika, br. 2, 1993.] (in Bulgarian)

[9] Иван Тонов, Таня Тонова. Учебно помагало за задължително-избираема подготовка по математика 7 клас, ISBN: 978-954-01-2617-3, Просвета, София, 2011. [Ivan Tonov, Tanya Tonova. Uchebno pomagalo za zadalzhitelno-izbiraema podgotovka po matematika 7 klas, ISBN: 978-954-01-2617-3, Prosveta, Sofiya, 2011.] (in Bulgarian)

[10] Иван Тонов, Таня Тонова. Учебно помагало за задължително-избираема подготовка по математика 5 клас, II преработено издание, ISBN:978-954-01-2497-1, Просвета, София, 2010. [Ivan Tonov, Tanya Tonova. Uchebno pomagalo za zadalzhitelno-izbiraema podgotovka po matematika 5 klas, II preraboteno izdanie, ISBN:978-954-01-2497-1, Prosveta, Sofiya, 2010.] (in Bulgarian)

[11] Иван Тонов, Таня Тонова. Учебно помагало за задължително-избираема подготовка по математика 6 клас, ISBN: 978-954-01-2043-0, Просвета, София, 2007. [Ivan Tonov, Tanya Tonova. Uchebno pomagalo za zadalzhitelno-izbiraema podgotovka po matematika 6 klas, ISBN: 978-954-01-2043-0, Prosveta, Sofiya, 2007.] (in Bulgarian)

[12] Иван Тонов, Таня Тонова. Учебно помагало за задължително-избираема подготовка по математика 5 клас, ISBN: 978-954-01-1893-2, Просвета, София, 2010. [Ivan Tonov, Tanya Tonova. Uchebno pomagalo za zadalzhitelno-izbiraema podgotovka po matematika 5 klas, ISBN: 978-954-01-1893-2, Prosveta, Sofiya, 2010.] (in Bulgarian)

[13] Таня Тонова. Когнитивни модели в обучението по математика на ученици от 3 – 6 клас. Докторска дисертация. Софийски университет „Св. Климент Охридски“, 2012 г. [Tanya Tonova. Kognitivni modeli v obuchenieto po matematika na uchenitsi ot 3 – 6 klas. Doktorska disertatsiya. Sofiyski universitet „Sv. Kliment Ohridski“, 2012 g.] (in Bulgarian)

ЮБИЛЕЙНИ ДОКЛАДИ

ANNIVERSARIES

МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2026
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2026
Proceedings of the Fifty-Fifth Spring Conference
of the Union of Bulgarian Mathematicians
Tryavna, Bulgaria, April 5–9, 2026

80TH BIRTH ANNIVERSARY OF ACAD. STEFAN DODUNEKOV

Peter Boyvalenkov[1], Stefka Bouyuklieva[2]
[1]Institute of Mathematics and Informatics, Bulgarian Academy of Sciences, Sofia, Bulgaria
[1]Faculty of Mathematics and Informatics, Veliko Tarnovo University, Veliko Tarnovo, Bulgaria
e-mails: [1]peter@math.bas.bg, [2]stefka@ts.uni-vt.bg

80 ГОДИНИ ОТ РОЖДЕНИЕТО НА АКАД. СТЕФАН ДОДУНЕКОВ

[1]Петър Бойваленков, [2]Стефка Буюклиева
[1]Институт по математика и информатика, Българска академия на науките, София
[1]Факултет по математика и информатика, Великотърновски университет
e-mails: [1]peter@math.bas.bg, [2]stefka@ts.uni-vt.bg

Осемдесет години от рождението на акад. Стефан Додунеков са повод не само за почит към големия учен, но и за благодарност към Учителя, който остави трайна следа в умовете, сърцата и съдбите на поколения математици и информатици. Световно признат учен, той е сред големите имена в теорията на кодирането и една от най-значимите фигури в съвременната българска математика и информатика.

Неговият научен принос е изключителен и добре известен, трудовете му са широко достъпни и високо цитирани в международната научна литература. Също толкова впечатляваща е обществената и административната му дейност: дългогодишен председател на Съюза на математиците в България, три мандата директор на Института по математика и информатика при БАН, както и председател на Българската академия на науките, но за съжаление, за твърде кратък период. Значима е и ролята му като преподавател в редица български университети.

Стефан беше изключителна личност – голям учен, вдъхновяващ педагог и истински лидер. Школата, която създаде, макар и неформална като структура, се превърна в общност, в която освен колеги сме и приятели. В края на всяка година се събираме на национален семинар по теория на кодирането, място за обмен на идеи, за сверяване на часовниците и за подкрепа на младите изследователи, почти винаги с международно участие. От 2012 година насам семинарът носи името „Проф. Стефан Додунеков“, като продължава да следва неговата увереност и надежда и да ни помага във всякакви ситуации – научни, професионални и житейски.

Редуването на официалното обръщение „акад. Додунеков“ с личното име Стефан

https://doi.org/10.55630/mem.2026.55.285-297
2020 Mathematics Subject Classification: 01A70, 68P30.

е съзнателен избор, чрез който искаме да изразим, че за нас той беше едновременно голям учен и ръководител, но и вдъхновител, колега и приятел.

1 Обществена и научно-организационна дейност

Обществената и научно-организационната дейност на акад. Стефан Додунеков заема изключително място в историята на българската математика и информатика. Той принадлежи към онази сравнително малка група учени, които съчетават високо международно научно признание с дълбока и последователна ангажираност към развитието на научните институции, образованието и професионалната общност в България.

В продължение на дълги години акад. Додунеков е председател на *Съюза на математиците в България* (СМБ). По време на неговото ръководство СМБ се утвърждава като водеща професионална и обществено значима организация, обединяваща университетски преподаватели, изследователи и учители по математика от цялата страна. Неговата дейност е насочена към укрепване на връзките между университетската наука, средното образование и работата с изявени ученици, като последователно се отстоява разбирането, че математиката е стратегическа дисциплина за интелектуалното и технологичното развитие на обществото.

Сред основните приоритети на акад. Додунеков като председател на СМБ е подкрепата на математическото образование на всички нива. Под егидата на Съюза се развива и укрепва извънкласната работа по математика, националните математически олимпиади и ученически състезания, както и дейността на школи за талантливи ученици. СМБ активно участва в методическата подкрепа и подготовката на националните отбори за международни състезания, като в този процес акад. Додунеков последователно отстоява високите професионални стандарти и значението на системната и дългосрочна подготовка. По време на неговото председателство СМБ разширява и своята издателска, просветителска и експертна дейност. Чрез конференции, семинари и публикации СМБ се утвърди като значим фактор в обсъждането на учебни програми, учебно съдържание и методика на преподаването по математика. Акад. Додунеков активно защитава позицията на математическата общност в диалог с държавните институции и образователната администрация.

Значителен е и приносът му като директор на *Института по математика и информатика при Българската академия на науките*. Управлението му се отличава с целенасочена подкрепа за фундаменталните научни изследвания, насърчаване на младите учени и докторанти и разширяване на международното сътрудничество и проектната дейност. В условията на сериозни институционални и финансови предизвикателства пред Института и цялата академия той последователно отстоява значението на дългосрочната научна перспектива и академичната автономия. В особено трудните 2010–2012 години, когато на сътрудниците на института се наложи излизане в неплатен отпуск за „връзване“ на бюджета, Стефан пръв даде личен пример.

В особено сложен обществен и институционален контекст акад. Стефан Додунеков е избран за председател на *Българската академия на науките*. Макар и кратък, неговият мандат се характеризира с ясна и аргументирана позиция в защита на БАН като национална научна институция и на науката като обществено благо.

В този период той е сред най-разпознаваемите публични гласове на българската научна общност.

Съществена част от обществената дейност на акад. Додунеков е трайно свързана с образованието. Освен като университетски преподавател, той има дългогодишен принос към елитното средно математическо образование. Той разглежда образователната система като непрекъснат процес от училището до научните изследвания на най-високо равнище и последователно подкрепя ранното откриване и развитието на млади таланти.

Важно място в дейността на акад. Додунеков заема Ученическият институт по математика и информатика (УчИМИ). Създаден през септември 2000 г. с учредители Съюзът на математиците в България, фондация „Еврика“, Международна фондация „Св. Св. Кирил и Методий“ и Институтът по математика и информатика при БАН (през 2005 г. се присъединява и Американска фондация за България), УчИМИ се разви и укрепна като важна съставна част на системата за работа с млади таланти. През изминалите години в сесиите (зимна и пролетна) и лятната изследователска школа на УчИМИ са преминали над 2000 ученици от 8. до 12. клас. УчИМИ ежегодно излъчва и двамата български представители за 6-седмичната сесия на Research Science Institute на MIT. За УчИМИ акад. Додунеков казваше: „Дори и само това да остане от нашите дела, ще е достатъчно ...“.

Особено място в неговата дейност заема развитието на международните контакти и регионалното сътрудничество, най-вече в рамките на Югоизточна Европа. Акад. Додунеков е сред активните поддръжници на сътрудничеството между математическите дружества и научните институции в региона. Съюзът на математиците в България, под негово ръководство и с неговото активно участие, се включва в организацията и провеждането на редица регионални конференции, работни срещи и научно-образователни форуми, както в областта на университетската математика, така и в сферата на математическото образование и ученическите състезания. В този контекст следва да се открои и приносът на акад. Додунеков към дейността на *Mathematical Society of South Eastern Europe* (MASSEE), организацията наследник на Балканския математически съюз. Той е сред основателите на MASSEE през 2003 г. (по време на първата конференция на организацията), неин президент (2007–2011), разпознаваем и уважаван представител на българската математическа общност в тази организация, последователен поддръжник на идеята за координирано развитие на математиката в страните от Югоизточна Европа. В рамките на MASSEE той допринася за изграждането на устойчиви връзки между математическите дружества и научните институции в региона, както и за насърчаване на научния обмен и подкрепата на млади изследователи.

Чрез своя авторитет, организационен опит и лична ангажираност акад. Стефан Додунеков утвърждава присъствието на българската математическа общност в регионалното и международното научно пространство. Неговата обществена и научно-организационна дейност представлява съществена част от наследството му и оставя траен отпечатък върху институционалното развитие и обществената роля на българската математика.

2 Школата по теория на кодирането в България

Ролята на акад. Стефан Додунеков за развитието на теорията на кодирането в България е фундаментална и с дълготрайни последици. Благодарение на неговата научна визия, педагогически усет и организационна дейност в страната се формира устойчива научна школа по алгебрична и комбинаторна теория на кодирането, получила международно признание и осигурила приемственост между няколко поколения изследователи.

Стефан постави основите и разви тази школа чрез съчетаване на дълбоки теоретични изследвания с целенасочена работа с млади учени. Под негово ръководство и влияние теорията на кодирането се утвърди като самостоятелно и перспективно направление в българската математическа и информатична общност. Характерна особеност на школата е тясната връзка между алгебричните методи, комбинториката и дискретната математика, в съчетание с компютърни подходи, което я прави разпознаваема в международен контекст.

Въпреки че не съществува като формална институционална структура, школата функционира като сплотена научна общност. Важен елемент от нейната дейност е *Ежегодният национален семинар по теория на кодирането*, който служи като форум за представяне на нови резултати, обсъждане на текущи проблеми и подготовка на докторанти. В рамките на семинара се провеждат и предварителни обсъждания на дисертационни трудове, които играят съществена роля за повишаване на научното им качество.

По идея на Стефан започна организирането на международни научни форуми в областта, които съществено допринасят за видимостта на българската школа. Главният сред тях е т.нар. българо-руски (всъщност международен) семинар *„Алгебрична и комбинаторна теория на кодирането“* (Algebraic and Combinatorial Coding Theory, ACCT), провеждан на всеки две години от 1998 до 2020 г. включително с редуващо се домакинство в България и Русия (през 1990 г. в СССР), както и международният семинар *„Оптимални кодове“* с осем издания между 1995 и 2017 г., организиран от секция „Математически основи на информатиката“ към Института по математика и информатика при БАН. Тези прояви привличат водещи световни специалисти и предоставят възможност за активно участие на млади изследователи. И двата семинара имат съществен принос за международната видимост на българската школа по теория на кодирането и за утвърждаването ѝ като активен и разпознаваем участник в световната научна общност.

Създадената от акад. Стефан Додунеков школа по теория на кодирането представлява едно от най-значимите му наследства. Тя не само допринася за развитието на конкретно научно направление, но и утвърждава модел на научна работа, основан на високи стандарти, приемственост и международна отвореност.

Основните научни направления, развивани в рамките на българската школа по теория на кодирането, включват:

- **Линейни и нелинейни кодове.** Това е основното направление, което всъщност включва и някои от изброените по-долу тематики. Освен Стефан Додунеков, основен принос към изследванията, насочени към конструкцията, класификацията и метричните свойства на линейни и нелинейни блокови кодове, включително кодове с добри и оптимални параметри, имат Николай Манев,

Иван Ланджев, Илия Буюклиев, Емил Колев, Цонка Байчева и др. [2, 4, 7, 43]. Изследват се и важни класове кодове, като кодове на Рийд-Малер [42], MDS и near-MDS кодове [31, 32], и др. Работата в това направление поставя теоретична основа за редица по-нататъшни резултати в рамките на школата.

- **Комбинаторни методи в теорията на кодирането.** Кодове се изследват чрез връзките им с комбинаторни конфигурации, блок-дизайни и дискретни структури. Комбинаторният подход позволява ефективно доказване на граници и създаване на нови класове кодове. Такива методи са използвани от Владимир Тончев, Стоян Капралов, Иван Ланджев, Илия Буюклиев и голяма част от останалите колеги в школата [7, 9, 44, 47].

- **Оптимални кодове.** Значителна част от научните усилия в рамките на школата е насочена към изследването на кодове, достигащи или доближаващи теоретичните граници. Тези резултати имат фундаментално значение за разбирането на пределите на коректното кодиране и декодиране. В този смисъл изследването на оптималността в зависимост от конкретните цели и ограничения на разглежданите модели присъства като водещ мотив в работите на почти всички представители на школата, занимавали се с линейни и нелинейни кодове. По отношение на нелинейните кодове принос имат Байчева и Колев [43], а при линейните кодове публикациите са много и се отнасят до конструкции, класификации [7, 10] и теоретични резултати, свързани както с границата на Грийсмър [8, 40, 45, 46], така и с други известни граници [32].

- **Самодуални и LCD кодове.** (Стефка Буюклиева, Николай Янков, Радка Русева, Мария Джумалиева-Стоева). В центъра на интереса са алгебричните и комбинаторните свойства на самодуалните и LCD кодовете [11, 15], методите за тяхната конструкция и класификация [13], както и връзките им с приложения в криптографията и сигурността на информацията [12, 17]. Много популярни в научните среди напоследък са изследванията на обвивката (hull) на линейните кодове над различни крайни полета и дори над пръстени [14].

- **Кодове над пръстени.** Това направление в школата ни се развива предимно от Иван Ланджев. Заедно с различни съавтори той изследва кодове над верижни пръстени [36, 37, 39]. Изследвания на кодове над пръстена $\mathbb{Z}_4$ има и Буюклиева [16], а Тодорка Александрова, Христо Костадинов и Николай Манев продължават работата си върху целочислените кодове (integer codes) [38].

- **Връзки между кодове, дизайни и крайни геометрии** (Иван Ланджев, Ася Русева, Светлана Топалова, Стела Банчева). Кодове се интерпретират чрез геометрични и комбинаторни структури, което позволява пренос на идеи между теорията на кодирането, комбинаториката и крайните геометрии и води до нови конструктивни и класификационни резултати [41, 45, 48, 49, 50].

- **Автоморфизми на кодове и симетрични структури.** (Илия Буюклиев, Стефка Буюклиева, Светлана Топалова, Стела Банчева). Анализът на групите от автоморфизми разкрива дълбоката вътрешна симетрия на кодовете и подпомага тяхната класификация с точност до изоморфизъм [15, 17, 5, 50].

- **Кодове и дизайни в полиномиални метрични пространства.** (Петър Бойваленков, Светла Никова, Даньо Данев, Силвия Бумова, Петър Казаков, Мая Стоянова, Константин Делчев). Работата в тази област започна през 1988 г. в Евклидовия случай и с получаване и изследване на граници за сферични кодове, като постепенно бяха включени нови обекти (например сферични дизайни, вж. например [18, 3, 28]) и нови пространства (в частност, класическите Хемингови пространства и някои безкрайни проективни пространства, вж. например [27, 23]). След 2014 г. изследванията се насочиха към универсални граници за различни видове енергии и анализ на оптимални кодове и дизайни (вж. например [22, 24]).

- **Връзки между теорията на кодирането и дискретната математика.** (Красимир Манев, Илия Буюклиев, Валентин Бакоев). Тук се развиват взаимодействия с теорията на графите, комбинаторните дизайни и други дискретни структури, което е характерно за интердисциплинарния дух на школата [19, 6, 47].

Всички тези научни направления и резултатите в тях свидетелстват за трайното влияние на Стефан върху жизнеността на школата, която той създаде и която продължава да се развива и днес, и която очевидно има бъдеще в България.

3 Научна дейност

Научната дейност на акад. Стефан Додунеков се отличава с дълбочина, широта и трайно влияние върху развитието на теорията на кодирането и свързаните с нея области. Неговите изследвания се характеризират с ясно изразен алгебричен и комбинаторен подход, както и с умело съчетаване на фундаментална теория и конкретни конструктивни резултати.

Основните научни приноси на акад. Додунеков са публикувани в значителен брой статии в престижни международни списания и сборници от конференции, които се отличават с високо качество и широка цитируемост. Резултатите му намират отражение както в развитието на теоретичните основи на кодирането, така и в изграждането на нови методи за конструиране и анализ на кодове.

Неговата научна дейност се отличава с активно и последователно международно сътрудничество с водещи учени и научни школи от различни страни. Чрез съвместни публикации, изследователски проекти и дългосрочни професионални контакти той допринася съществено за интегрирането на българската школа по теория на кодирането в световния научен контекст. Много от неговите съавтори са сред утвърдените имена в областта, а съвместните им работи се превръщат в отправна точка за по-нататъшни изследвания и развитие на нови направления.

Особено важен аспект от научната и академичната му биография са многобройните му пътувания като гост-изследовател и гост-професор в престижни международни научни центрове. В периода февруари 1983 – август 1985 г. акад. Додунеков работи в Института по проблеми на предаването на информация към Академията на науките на СССР в Москва – един от водещите световни центрове по теория на информацията и кодирането. Този период има огромно влияние върху формирането и развитието на неговите научни интереси и международни контакти.

През 1990–1992 г., както и в периодите 1993–1994, 1998 и 1999 г., акад. Додунеков е гост-професор в *Department of Electrical Engineering (Data Transmission Group)* на *Linköping University of Technology*, Швеция. Сътрудничеството му с тази институция се отличава с дългосрочност и интензивност и води до съвместни изследвания в областта на теорията на кодирането и предаването на информация.

Неговите международни академични ангажименти включват още гостувания в *Department of Information Theory* на *Technical University of Ulm* (1994), в *Department of Applied Mathematics and Informatics* на *Delft University of Technology* (1997), в изследователската група *LACO* на *University of Limoges* (2002), както и в *Institute of Informatics* на *University of Bergen*, Норвегия (2001, 2003). През 2004 г. и няколко пъти в следващите години той е гост и на *Alfréd Rényi Institute of Mathematics* към Унгарската академия на науките.

Тези продължителни и многократни гостувания са ясно свидетелство за високия международен авторитет на акад. Стефан Додунеков и за устойчивите му научни връзки с водещи европейски школи. Те имат съществено значение както за развитието на собствените му научни изследвания, така и за международната видимост и утвърждаването на българската школа по теория на кодирането.

Акад. Додунеков отдаваше особено значение на връзката между научните изследвания и подготовката на млади учени. Значителна част от публикациите му са резултат от съвместна работа с докторанти и млади изследователи, което допринася не само за тяхното професионално израстване, но и за устойчивото развитие на научното направление в България.

Конкретните области от теорията на кодирането, в които акад. Додунеков има съществен принос, са представяни и на предишни пролетни конференции, затова тук само ще ги споменем.

- **Оптимални линейни кодове**. В тази тематика са първите публикации на Додунеков, това е и заглавието на дисертацията му за званието „доктор на математическите науки“ [1]. Това направление продължава да се развива в България от Николай Манев. Иван Ланджев, Илия Буюклиев, както и техните докторанти.

- **Радиус на покритие на линейни кодове**. Додунеков заедно с Манев, Тончев и Данев (всички част от българската школа по кодиране) успяват да опровергаят две хипотези, свързани с радиус на покритие, като контрапримерите са публикувани съответно в [29] съвместно с Д. Данев, и в [30], съвместна работа с Н. Манев и Вл. Тончев. Ранните изследвания на Цонка Байчева и Евгения Великова също се отнасят до радиус на покритие на циклични кодове.

- **Кодове с малък дефект**. Изследванията са съвместни с Иван Ланджев и се отнасят до MDS и near-MDS кодове (виж например [31, 32]).

- **Кодове в Евклидови пространства**. След работата [33] на Додунеков, Ериксон и Зиновиев върху новия за тогава каскаден метод за конструиране на добри сферични кодове това направление се разшири и разви към получаване и изследване на т.нар. универсални граници от Петър Бойваленков и негови докторанти и съавтори (виж например [18, 21, 20, 22, 19, 24]).

- **Подходящи (proper) за декодиране линейни кодове**. Ефективността на линеен код, който може да поправя до t грешки при q-ичен симетричен канал без памет с вероятност за грешка в един символ равна на ε, се характеризира с вероятността една грешка (при предаване) да остане неоткрита. Тази вероятност е функция на ε и зависи от разпределението на теглата на кода, както и от разпределението на теглата на съседните класове с минимално тегло $\leq t$. Когато вероятността за неоткрита грешка е растяща функция на ε, кодът се нарича ε-подходящ (ε-*proper*). В работата си Додунеков и неговите съавтори Росица Додунекова и Евгения Николова извеждат достатъчни условия за ε-proper кодове, а също така изследват различни класове кодове в тази връзка [34].

- **Самодуални кодове**. Акад. Додунеков заедно с Радинка Йоргова и ван Зантен изучават двоичните самодуални кодове, които имат автоморфизъм от ред pq, където p и q са различни нечетни прости числа [35]. С помощта на разработения метод авторите са се опитали да атакуват известната (все още нерешена) задача за съществуването на екстремален самодуален код с параметри $[72, 36, 16]$. Това направление продължава да се развива от Стефка Буюклиева, Николай Янков, Радка Русева и др.

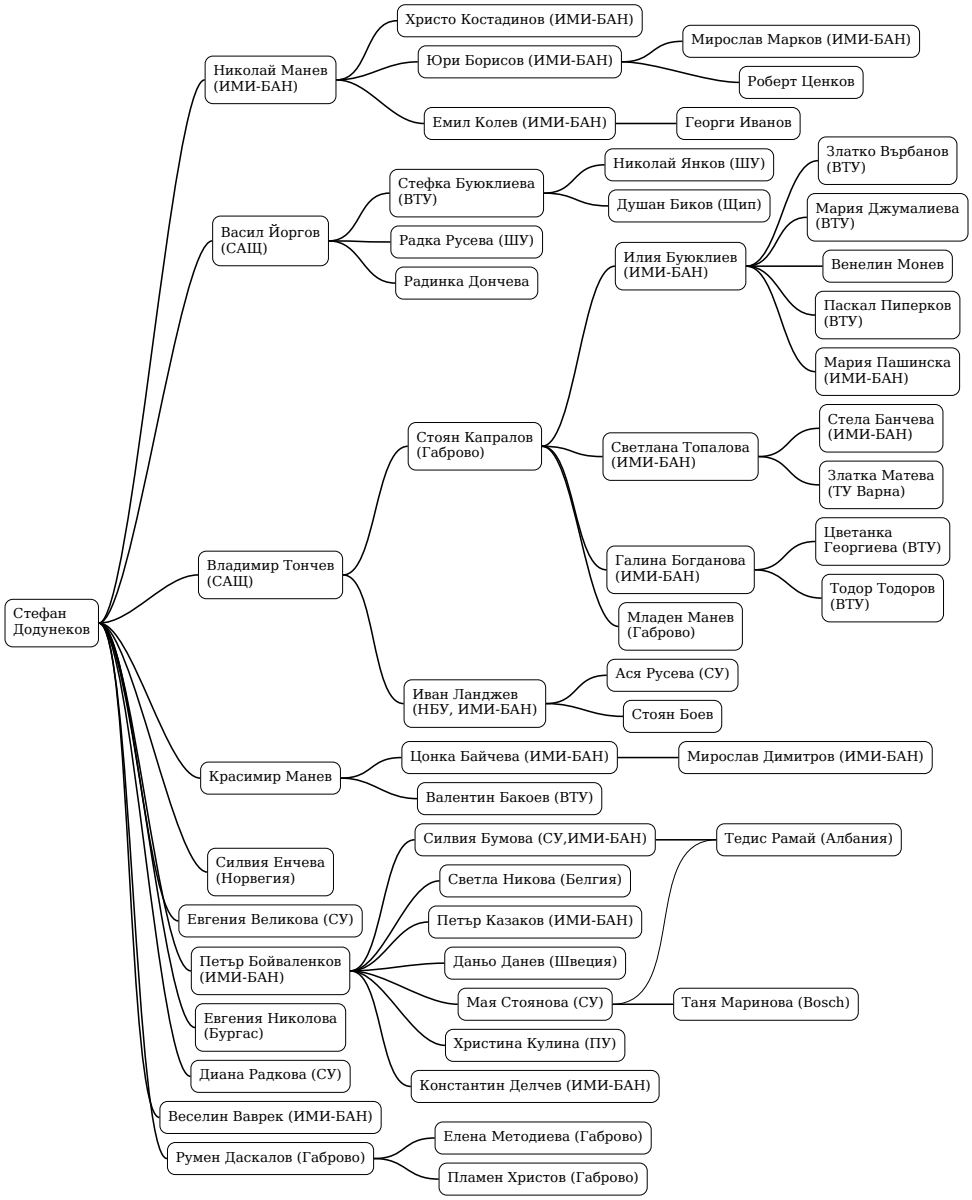
Тези теми не изчерпват цялата научна дейност на акад. Стефан Додунеков. Неговите резултати и подходи продължават да оказват влияние върху съвременните изследвания и представляват важна част от научното наследство на българската математическа школа.

4 Учител и научен ръководител

Една от най-значимите и трайни роли на Стефан е тази на учител и научен ръководител. Неговото влияние далеч надхвърля рамките на собствените му научни резултати и се проявява най-ясно в поколенията учени, които той обучава, вдъхновява и подкрепя през годините.

Като преподавател акад. Додунеков се отличава с изключителна яснота на изложението, високи изисквания и дълбоко уважение към студентите и учениците си. Той притежаваше рядката способност да представя абстрактни алгебрични идеи по достъпен и мотивиращ начин, като насърчаваше самостоятелното мислене и стремежа към задълбочено разбиране. За много от своите ученици (в частност за пишещите тези редове) той остава Учителят с главна буква — личност, оказала решаващо влияние върху техния професионален и житейски път.

Особено значима е дейността му като научен ръководител. Стефан ръководи самостоятелно или съвместно с други колеги редица докторски дисертации в областта на теорията на кодирането и дискретната математика. Първите му докторанти Николай Манев и Васил Йоргов поставят началото на системно обучение и научни изследвания в областта на теорията на кодирането в България. Към основоположниците на школата се отнасят също Владимир Тончев и Красимир Манев, които допринасят за разширяването на тематичния обхват и за утвърждаването на интердисциплинарния характер на направлението. Тези учени от своя страна стават научни ръководители на следващо поколение изследователи и по този начин осигу-



Академично генеалогично дърво на българската школа по теория на кодирането

ряват естествената приемственост в рамките на школата. В тази връзка изготвихме академично генеалогично дърво на школата, в което са включени докторантите на акад. Додунеков, техните докторанти и следващите поколения. На някои места са използвани многоточия, тъй като с течение на времето тематичният обхват значително се разширява и вече включва и дисертации извън класическата област на

теорията на кодирането.

В работата си с докторантите Стефан съчетаваше взискателност с постоянна готовност за помощ. Той умееше да насочва младите изследователи към съществени и перспективни проблеми, като същевременно им предоставяше необходимата свобода за самостоятелно развитие. За него подготовката на докторанти не беше формално задължение, а дългосрочна инвестиция в бъдещето на научното направление.

Ролята му на учител не се изчерпва с университетското образование. Като преподавател по алгебра в Националната природо-математическа гимназия той оставя дълбока следа в подготовката на поколения ученици, много от които по-късно избират пътя на науката. По този начин неговото влияние обхваща целия образователен спектър — от средното училище до най-високите академични степени.

Чрез своите ученици и последователи акад. Стефан Додунеков изгражда жива и устойчива научна общност. Днес неговите възпитаници са професори, доценти и изследователи в България и в чужбина, а създадената от него традиция на високи научни и етични стандарти продължава да се развива и предава на следващите поколения.

В спомените на своите ученици и колеги Стефан остава не само изключителен учен и преподавател, но и човек с дълбоко човешко отношение и рядка способност да вдъхновява. Той умееше да вижда потенциала у младите хора, често преди самите те да го осъзнаят, и да им дава увереност в моменти на съмнение. Съчетавайки принципност с доброжелателност и чувство за хумор с високи изисквания, той създаде среда, в която науката беше не просто професия, а призвание. За мнозина неговите думи, съвети и личен пример продължават да бъдат морален и професионален ориентир и днес.

Литература

[1] Ст. Додунеков, „Оптимални линейни кодове“, дисертация за присъждане на научното звание Доктор на математическите науки, 1985.

[2] T. Baicheva, S. Dodunekov, and P. Kazakov. On the cyclic redundancy-check codes with 8-bit redundancy. *Computer Communications* 21, no. 11 (1998): 1030-1033.

[3] S. Boumova, P. Boyvalenkov, D. Danev, Necessary conditions for existence of some designs in polynomial metric spaces, *Europ. J. Combin.* 20, (1999), 213-225.

[4] T. Baicheva, I. Bouyukliev, S. Dodunekov, V. Fack. Binary and ternary linear quasi-perfect codes with small dimensions. *IEEE transactions on information theory* 54, no. 9 (2008): 4335-4339.

[5] A. Betten, S. Topalova, and S. Zhelezova. Parallelisms of invariant under cyclic groups of order 4. International Conference on Algebraic Informatics. Cham: Springer International Publishing, 2019.

[6] I. Bouyukliev, V. Bakoev. A method for efficiently computing the number of codewords of fixed weights in linear codes. *Discrete applied mathematics* 156.15 (2008): 2986-3004.

[7] I. Bouyukliev, S. Bouyuklieva, and S. Kurz. Computer classification of linear codes. *IEEE Transactions on Information Theory* 67, no. 12 (2021): 7807-7814.

[8] I. Bouyukliev, Classification of Griesmer codes and dual transform. *Discrete*

mathematics 309, no. 12 (2009): 4049-4068.
[9] I. Bouyukliev and M. Dzhumalieva-Stoeva. Representing equivalence problems for combinatorial objects. Serdica Journal of Computing 8.4 (2014): 327-354.
[10] I. Bouyukhev, D. Jaffe, and V. Vavrek. The smallest length of eight-dimensional binary linear codes with prescribed minimum distance. *IEEE Transactions on Information Theory* 46.4 (2002): 1539-1544.
[11] S. Bouyuklieva. Optimal binary LCD codes. *Designs, Codes and Cryptography* 89, no. 11 (2021): 2445-2461.
[12] S. Bouyuklieva, Self-dual codes, In *Concise Encyclopedia of Coding Theory*, Chapman and Hall/CRC, 79–96, 2021.
[13] S. Bouyuklieva and I. Bouyukliev, An Algorithm for Classification of Binary Self-Dual Codes, *IEEE Transactions on Information Theory*, 58(6) (2012), 3933-3940,
[14] S. Bouyuklieva, I. Bouyukliev, and F. Özbudak. Sequence of numbers of linear codes with increasing hull dimensions. *Designs, Codes and Cryptography* 94, no. 2 (2026): 39.
[15] S. Bouyuklieva, and Javier de la Cruz. On the structure of binary LCD codes having an automorphism of odd prime order. *IEEE Transactions on Information Theory* 68, no. 10 (2022): 6426-6433.
[16] S. Bouyuklieva and M. Harada, On Type IV self-dual codes over Z4, *Discrete Mathematics* 247 (2002), 25-50.
[17] S. Bouyuklieva, R. Russeva, and N. Yankov. On the structure of binary self-dual codes having an automorphism of order a square of an odd prime. *IEEE Trans. Inform. Theory* 51, no. 10 (2005): 3678–3686.
[18] P. Boyvalenkov, Extremal polynomials for obtaining bounds for spherical codes and designs, *Discr. Comput. Geom.* 14 (1995), 167–183.
[19] P. Boyvalenkov and D. Danev, Linear Programming Bounds, In *Concise Encyclopedia of Coding Theory*, Chapman and Hall/CRC, 79–96, 2021.
[20] P. Boyvalenkov and D. Danev, On linear programming bounds for codes in polynomial metric spaces, *Probl. Peredachi Inf.*, 34(2) (1998), 16-31 (in Russian); English translation in *Probl. Inform. Transm.* 34(2) (1998), 108–120.
[21] P. Boyvalenkov, D. Danev, and S. Bumova, Upper bounds on the minimum distance of spherical codes, *IEEE Trans. Inform. Theory*, 42 (1996), 1576–1581.
[22] P. Boyvalenkov, P. Dragnev, D. Hardin, E. Saff, and M. Stoyanova, Universal lower bounds for potential energy of spherical codes, *Constructive Approximation* 44 (2016), 385-415.
[23] P. Boyvalenkov, P. Dragnev, D. Hardin, E. Saff, and M. Stoyanova, Energy bounds for codes and designs in Hamming spaces, *Designs, Codes and Cryptography* 82(1) (2017), 411–433.
[24] P. Boyvalenkov, P. Dragnev, D. Hardin, E. Saff, and M. Stoyanova, On polarization of spherical codes and designs, *Journal of Mathematical Analysis and Applications*, 524(2) (2023), art. 127065 (29 pages).
[25] P. Boyvalenkov, D. Cherkashin, The kissing number in 48 dimensions for codes with certain forbidden distances is 52 416 000, *Results in Mathematics*, 80(1) (2025), art. 3 (12 pages).

[26] P. Boyvalenkov, P. Dragnev, D. Hardin, E. Saff, and M. Stoyanova, Universal minima of discrete potentials for sharp spherical codes, *Revista Matematica Iberoamericana*, 41(2) (2025), 603–650.
[27] P. Boyvalenkov, S. Nikova, On lower bounds on the size of designs in compact symmetric spaces of rank 1, *Archiv der Mathematik* 68 (1997), 81–88.
[28] P. Boyvalenkov, M. Stoyanova, New nonexistence results for spherical designs, *Advances in Mathematics of Communications* 7(4) (2013), 279–292.
[29] D. Danev, S. Dodunekov. A family of ternary quasi-perfect BCH codes. *Designs, Codes and Cryptography*, 49 (2008), No 1, 265–271.
[30] S. Dodunekov, K. Manev, V. Tonchev. On the covering radius of binary (14,6) codes containing the all-one vector. *IEEE Trans. Inform. Theory*, IT-34 (1988), No. 3, 591–595.
[31] S. Dodunekov, I. Landjev. On near-MDS codes. *Journal of Geometry*, 54 (1995), 30–43.
[32] S. Dodunekov, I. Landjev. Near-MDS Codes over some small fields, *Discrete Mathematics*, 213 (2000), 55–65.
[33] S. Dodunekov, T. Ericson, V. A. Zinoviev. Concatenation Methods for Construction of Spherical Codes in N-dimensional Euclidean space. *Problems of Information Transmission*, 27 (1991), No. 4, 34–38.
[34] R. Dodunekova, S. Dodunekov, and E. Nikolova. A survey on proper codes. *Discrete applied mathematics* 156, no. 9 (2008): 1499-1509.
[35] R. Dontcheva, A. J. van Zanten, and Stefan M. Dodunekov. Binary self-dual codes with automorphisms of composite order. *IEEE Transactions on Information Theory* 50, no. 2 (2004): 311-318.
[36] T. Honold, I. Landjev, Linear Codes over Finite Chain Rings, *Electronic Journal of Combinatorics* 7, (2000), R11.
[37] T. Honold, I. Landjev, Codes over rings and ring geometries, Chapter 7. In: De Beule J., Storme L. (eds.) Current research topics in Galois geometries, pp. 161–186. Nova Science Publishers, New York (2012).
[38] T. Alexandrova, H. Kostadinov, and N. Manev. "General construction of integer codes correcting single error in t2-TQAM."Computers and Electrical Engineering 127 (2025): 110572.
[39] I. Landjev, E. Rogachev, Sperner's theorem for non-free modules over finite chain rings. *Des. Codes Cryptogr.* 93, 373–390 (2025).
[40] I. Landjev, E. Rogachev, A. Rousseva, Characterization of some minihypers in $PG(r, 3)$ and the nonexistence of some ternary Griesmer codes. *Des. Codes Cryptogr.* 94, 22 (2026).
[41] I. Landjev, L. Storme, Galois geometries and coding theory, *Current Research Topics in Galois Geometry*, pp. 187 – 214, (2011).
[42] M. Markov, and Yuri Borissov. The weight distribution of the fourth-order Reed–Muller code of length 512. *Designs, Codes and Cryptography* 93, no. 7 (2025): 2487-2502.
[43] P. Östergard, Tsonka Baicheva, and Emil Kolev. Optimal binary one-error-correcting codes of length 10 have 72 codewords. *IEEE Transactions on Information Theory* 45, no. 4 (1999): 1229-1231.
[44] M. Pashinska-Gadzheva, and I. Bouyukliev. "Algorithm 1059:

LinCodeWeightInv—Library for Computing the Weight Distribution of Linear Codes over Finite Fields." ACM Transactions on Mathematical Software 51, no. 4 (2025): 1-22.

[45] A. Rousseva, I. Landjev, The geometric approach to the existence of some quaternary Griesmer codes. *Des. Codes Cryptogr.* 88, 1925–1940 (2020).

[46] A. Rousseva, I. Landjev, Linear codes close to the Griesmer bound and the related geometric structures. *Des. Codes Cryptogr.* 87, 841–854 (2019).

[47] V. Tonchev, On Pless symmetry codes, ternary QR codes, and related Hadamard matrices and designs. *Designs, Codes and Cryptography* 90, no. 11 (2022): 2753-2762.

[48] V. Tonchev, Codes and Designs. In *Concise Encyclopedia of Coding Theory*, Chapman and Hall/CRC, 79–96, 2021.

[49] S. Topalova, and S. Zhelezova. On point-transitive and transitive deficiency one parallelisms of $PG(3, 4)$. Designs, Codes and Cryptography 75.1 (2015): 9-19.

[50] S. Topalova, and S. Zhelezova. Isomorphism and invariants of parallelisms of projective spaces. In *International Congress on Mathematical Software*, pp. 162-172. Cham: Springer International Publishing, 2020.

МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2026
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2026
Proceedings of the Fifty-Fifth Spring Conference
of the Union of Bulgarian Mathematicians
Tryavna, Bulgaria, April 5–9, 2026

HAPPY 80TH ANNIVERSARY, ACAD. PETAR POPIVANOV!

Nedyu Popivanov
Institute of Information and Communication Technologies,
Bulgarian Academy of Sciences
e-mail: nedyu@parallel.bas.bg

ЧЕСТИТ 80-И ЮБИЛЕЙ, АКАДЕМИК ПЕТЪР ПОПИВАНОВ!

Недю Попиванов
Институт по информационни и комуникационни технологии,
Българска академия на науките
e-mail: nedyu@parallel.bas.bg



https://doi.org/10.55630/mem.2026.55.298-302
2020 Mathematics Subject Classification: 01A70.

Видният български математик, академик Петър Радоев Попиванов, е роден на 6.04.1946 г. в гр. София. Баща му е известният български биолог, имуно-генетик и бивш дългогодишен министър на народното здраве – академик Радой Попиванов. Корените на фамилията Попиванови са от град Лясковец, близо до Велико Търново. През последните 220 години от тази фамилия излизат адвокати, учени, политици, духовници, поборници за националното освобождение на България. Отец Иван, прадядо на акад. Петър Попиванов, е бил главен изповедник на църквата „Св. Богородица“ във Велико Търново и през 1835 г. е заклевал съзаклятниците, участници във Велчовата завера. Синът на отец Иван, Христо, се жени за дъщерята на поп Стоян Брусев, един от участниците в четата на капитан дядо Никола, която тръгва от Петропавловския манастир през август 1856 г. Името му е издълбано на паметника на участниците в четата край Габрово. Едно от децата им е дядото на Петър Попиванов (със същото име), участвал в двете Балкански войни и после и в Първата световна, вече с чин полковник. При него е бил офицер за свръзка Райко Даскалов. Като съратник на Райко Даскалов и Александър Стамболийски, дядото на Петър Попиванов е бил последователно началник-щаб на жандармерията и окръжен управител на София. Негови близки роднини са генералите Радой Сираков, началник на дивизия, сражавала се при Одрин и Чаталджа, а после в Междусъюзническа война при Кресна и Климент Бояджиев – командващ Първа българска армия по време на успешното ѝ настъпление в Сърбия през 1915 г.

Средното си образование акад. П. Попиванов получава в 22-ро СПУ – София през 1964 г. с отличен успех и златен медал. През 1969 г. завършва висшето си образование по математика, специалност комплексен анализ, във ФМФ на СУ „Св. Климент Охридски“ с отличен успех (5,97). През следващата 1970 г. става редовен аспирант в МГУ „Ломоносов“. Негов научен ръководител е изтъкнатият учен в областта на диференциалните уравнения проф. Ю. В. Егоров. Защитава кандидатска дисертация в областта на псевдодиференциалните уравнения през 1973 г. През 1986 г., след защита на втора докторска дисертация по микролокален анализ пред СНС по математика в София, получава научната степен „доктор на математическите науки“.

Творческият път на акад. П. Попиванов преминава в Института по математика и информатика (до 1988 г. Институт по математика и механика) при БАН, на който остава верен от постъпването си през 1969 г. досега. Преминава през всички степени на научното израстване – от научен сътрудник (1973 г.), старши научен сътрудник (1978 г.), професор (1988 г.), член-кореспондент на БАН (1995 г.) до академик (2003 г.).

Тук ще се опитам да обясня популярно областта на работа, кръга на научни интереси, както и научните постижения на юбиляря. Неговата научна дейност е в областта на частните диференциални уравнения (ЧДУ), интензивно развивана от десетките хиляди изследователи, работещи в нея. За справка: преди години само в раздел №35 (Partial Differential Equations) на Math. Reviews се реферираха над 15% от всички реферирани математически публикации, като също така могат да се посочат и ред други подраздели, където също се реферираха статии по ЧДУ. Причината, разбира се, е много проста – с ЧДУ се моделират редица реални процеси в природата, физиката, химията, биологията, медицината, икономиката и др. Богатството на всички тези явления и обекти води до необходимостта да се изследват най-различни

видове ЧДУ с широк спектър от разнообразни свойства, методи за изследване и, разбира се, резултати. Тук са намерили място както строго теоретични разработки, така и чисто приложни задачи от областта на линейните и нелинейни ЧДУ, като се започне от получаването на най-тънки априорни оценки със средствата на хармоничния анализ в духа на Калдерон – Зигмунд – Михлин – Стайн – Мейер и се достигне до конкретни числени реализации за съответния математически модел.

В тази огромна и трудно обозрима област резултатите на акад. Петър Попиванов заемат място, което ще се опитам по-детайлно да очертая. Тъй като значителна част от резултатите на акад. П. Попиванов са в областта на линейния и нелинейния микролокален анализ, ще се спра по-подробно на някои негови достижения в тези две направления на анализа. Ще припомня, че през 60-те и 70-те години на XX век се разви основно линейният микролокален анализ. Следвайки резултатите на ред изтъкнати математици в тази област като Хьормандер, Ниренберг, Трев, Сато, Егоров, Кондратиев, Мелин, Шьостранд, Петър Попиванов получи ред нови резултати в теорията на израждащите се елиптични гранични задачи и по-специално за тангенциалната задача с наклонената производна, поставена от Поанкаре още в началото на XX век при изучаването на приливите в океаните. Тези изследвания П. Попиванов продължава (включително и през последните години) и в нелинейния случай с техниката на вискозните решения.

В по-общ план: около 1968 год. П. Лакс и други колеги се занимаваха с обратната задача на спектралната теория (теория на разсейването, Лаксови двойки и т.н.), което им позволи да получат в явен вид решенията на специални класове еволюционни нелинейни ЧДУ, като уравнението на Кортевег де Фриз, нелинейният оператор на Шрьодингер и т.н. През 80-те години настъпи тематична преориентация и това доведе до създаването на нелинейния микролокален анализ, който между другото изучава разпространението на особености на решения на нелинейни ЧДУ, включително „раждането“ на нови особености, които не възникват в линейния случай. Особено за приложенията на нелинейните ЧДУ често (дори само за ориентация) важна роля играе намирането на специални решения с определени симетрии. По такъв начин задачата за нелинейното ЧДУ се редуцира до изследване на качествената картина на нелинейни ОДУ и оттук често до използване на специални функции, за които има широко развита теория още от XVIII, XIX и XX век. По-конкретно, уравнението на Монж-Ампер от геометрията, както и пъстра гама от нелинейни параболични и хиперболични уравнения, изследвани за наличие на радиални решения, бягащи вълни и т.н. Нека отбележа изрично, че през последните 5 години П. Попиванов има поне 15 работи, свързани с построяване на решения в явен вид за ред уравнения на математическата физика (например Уравнението на Лиувил, Уравнението на Трош, Вълновото уравнение, описващо черна дупка на Шварцшилд, Задачата на Робен).

Тук ще спомена и малко наукометрия:

1. Акад. П. Попиванов е публикувал над 180 научно- изследователски статии. Всичките са в списания с IF (Импакт фактор) или със SJR.

2. Монографии: 5, плюс една глава от монография.

3. Учебни помагала по ОДУ и ЧДУ: 6.

4. Ред научно-популярни статии, като и юбилейни за Блез Паскал, Якоби, Гаус, Брадистилов, Илиев, Сендов, общо над 50.

5. Рецензии: за докторантури, хабилитации, професури, чл. кор. и академици на БАН: общо над 75.

Акад. П. Попиванов е преподавал дълги години ОДУ и ЧДУ във ФМИ на СУ „Св. Кл. Охридски“ (18 години) и в ЮЗУ „Неофит Рилски“, Благоевград (общо 11 години). Аз лично имах удоволствието да слушам един семестър негови упражнения по ЧДУ! Той има 4 успешно защитили докторанти, двама от които са професори – Г. Попов в Нант, Франция, и Д. Палагачев в Бари, Италия. Съавтор е на Ръководство по ЧДУ за СУ, което претърпява 5 издания, включително и 2 основно преработени, както и на учебник по ОДУ за студенти от ЮЗУ.

Признат експерт в областта на диференциалните уравнения, акад. П. Попиванов е член на редакционния съвет на „Journal of Pseudo-Differential Operators and Applications“, издаван от Birkhäuser, 15 години е бил член на редакционния съвет на „Annali di Ferrara” и 20 години на „Доклади на БАН“.

Списъкът за участието му на конференции, конгреси и изнасяне на доклади на семинари по покана е дълъг: гост-професор в Университет Париж 11, Институт А. Поанкаре, Екол политекник (Париж), Университет П. Сабатие (Тулуза), Университет Рен, Университетите в Болоня, Флоренция, Триест, Торино, Пиза, Ферара, Бари, Каляри, Месина, Катания – Италия, Московския държавен университет „М. В. Ломоносов“ и Институт „Стеклов“ – Русия, Института „Вайерщрас“ в Берлин и университетите в Потсдам, Кемниц, Клаустхал – Германия, Университетите на Лунд, Вахьо и Линчопинг – Швеция, Университетите на Чоу, Цукуба, Токио, Хирошима, Киото, Нагоя, Осака – Япония, Вайцмановия институт, Университетите в Технион и Ариел – Израел, Университетите в Белград и Нови Сад – Сърбия, Университета в Йоанина – Гърция и Виенския университет.

Богата и разнообразна е организационната дейност на акад. П. Попиванов в работата на ИМИ и БАН като член на Управителния съвет на БАН (2004–2013), Председател на Научния съвет на ИМИ (1995–2008), ръководител на секция Диференциални уравнения в ИМИ (1989–2011). Бил е секретар (8 години), а сега е заместник-председател на Отделението за природо-математически науки при Събранието на академиците и член-кореспондентите на БАН. Той е „Доктор хонорис кауза“ на Русенския университет „А. Кънчев“, носител на почетния знак на БАН за 60-та си годишнина, на най-високото отличие на БАН – Почетния знак „Марин Дринов“ с лента за 65-годишния си юбилей и на Почетния знак на Председателя на БАН за 70-годишния си юбилей. Член е на Съюза на математиците в България, American Mathematical Society и българското общество „Достоевски“. Ръководител е от 2003 г. на Националния колоквиум по математика, провел 164 заседания от създаването си през 1973 г. досега и 102 сбирки пред последните 22 години.

Акад. П. Попиванов е работил дълги години в Съюза на научните работници на България, сега Съюз на учените в България (СУБ), чийто член е от 1975 г. Бил е член на Президиума и председател на секция „Математика“ при СУБ (1998–2004), член на редакционния съвет на списание „Наука“ (от 2007 г.), член на Комисията за високи научни постижения на СУБ (от 2001 г.), награден е с юбилейна грамота на СУБ – 2014 г.

Представянето на акад. П. Попиванов би било непълно, ако не отбележим неговото дългогодишно изучаване и изследване на творчеството на Достоевски, както и проблемите, които то поставя пред един изследовател с физико-математическа нагласа. Възникват ред въпроси от геометрията, основи на математиката и математическата логика. Тук ще акцентираме по-подробното и задълбочено изследване в третото издание на книгата му за Достоевски от 2024 год. в изд. „Захарий Стоянов“, където е обяснен математическият апарат и богато са илюстрирани моделите на Поанкаре, на геометрията на Лобачевски-Бояй. Накратко казано, описана е една симбиоза от литературно-критически, философски и природо-математически изследвания, чрез които подобно на пъстра мозайка се разкрива в по-голяма дълбочина богатото идейно наследство на великия писател. Чрез тези свои изследвания П. Попиванов, според мен, запълва една празнота, останала след многобройните изследвания на литератори, критици, философи, богослови, психиатри и т.н., именно поради тяхната сравнително ниска компетентност в областта на математиката. Аз лично съм впечатлен от усилията на П. Попиванов да анализира и да вникне в труда на великия Достоевски в тази сложна тематика, който прави абсолютно неочакван паралел между тези сякаш толкова далечни предмети! Моделът на Поанкаре на хиперболичната геометрия в единичния кръг е впечатляващ. Още по-силно впечатление правят разсъжденията на Достоевски за връзката между безкрайното и неевклидовото. Все пак, не трябва да забравяме, че той е инженер по образование, както е бил инженер по пътищата и мостовете Поанкаре...

Ще спра дотук!

На фона на всичко казано ще отбележа, че ние, колегите и приятелите на акад. Петър Попиванов, също сме впечатлени от неговия енциклопедичен талант и му пожелаваме още дълги години творческа активност и висок научен ентусиазъм.

Честит юбилей, академик Петър Попиванов!

МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2026
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2026
Proceedings of the Fifty-Fifth Spring Conference
of the Union of Bulgarian Mathematicians
Tryavna, Bulgaria, April 5–9, 2026

PROF. AVRAM MOIS ESKENAZI: AN "IRREDUCIBLE TEST" FOR HIGH SCIENTIFIC, SOCIAL, AND HUMAN VALUE

Krassimira Ivanova
Institute of Mathematics and Informatics
Bulgarian Academy of Sciences
e-mail: kivanova@math.bas.bg

This article marks the 80^{th} anniversary of Prof. Dr. Avram Eskenazi and traces his exceptional scientific and teaching career. As a pioneer in computer education, creator of innovative methods for software quality assessment, with outstanding contributions to the development of software technologies, and a thinker with a bright public position, he left a lasting imprint on the science, education, and technological policy in Bulgaria. This article is an appreciation of his overall value – as a scientist, educator, and inspiring person, whose life and work represent a true "irreducible test" of high scientific, social, and human significance.

ПРОФ. АВРАМ ЕСКЕНАЗИ: ЕДИН „НЕПРИВОДИМ ТЕСТ“ ЗА ВИСОКА НАУЧНА, ОБЩЕСТВЕНА И ЧОВЕШКА СТОЙНОСТ

Красимира Иванова
Институт по математика и информатика, Българска академия на науките
e-mail: kivanova@math.bas.bg

Статията отбелязва 80-годишния юбилей на проф. д-р Аврам Ескенази и проследява неговия изключителен научен и преподавателски път. Като пионер в компютърното обучение, създател на иновативни методи за оценка на качеството на софтуера, с изключителни приноси в развитието на софтуерните технологии и мислител с ярка обществена позиция, той оставя траен отпечатък в науката, образованието и технологичната политика на страната. Тази статия е признателност към неговата цялостна стойност – като учен, педагог и вдъхновяващ човек, чийто живот и дело представляват истински „неприводим тест“ за висока научна, обществена и човешка значимост.

https://doi.org/10.55630/mem.2026.55.303-308
2020 Mathematics Subject Classification: 01A70.

На 14 май 2026 г. проф. д-р Аврам Моис Ескенази навършва 80 години – годишнина, която дава рядката възможност не просто да направим равносметка на един впечатляващ научен и преподавателски път, а и да погледнем напред с оптимизъм. Защото, както знаят всички негови колеги и ученици, възрастта при проф. Ескенази е по-скоро формален параметър, отколкото ограничение: любопитството, енергията и готовността му да влиза в дебат за най-новите технологични предизвикателства остават удивително младежки.

Осемдесетата годишнина на проф. д-р Аврам Ескенази е подходящ повод не само за юбилейно отбелязване, но и за осмисляне на един научен и професионален път, който по удивително последователен начин отразява пътя, който софтуерът измина от помощен инструмент до ключов фактор за икономическо, образователно и обществено развитие. В продължение на повече от пет десетилетия проф. Ескенази не просто следва тези процеси, а активно участва в тяхното формиране, като съчетава научна строгост, практическа ориентация и ясно изразена обществена отговорност.

Роден на 14 май 1946 г. във Варна, той отрано проявява изключителни математически способности. Обучението му в математическата паралелка на Първо средно политехническо училище и участието в математическата школа във Варна поставят стабилни основи за бъдещото му развитие. Особено място в ранната му биография заема неговата учителка по математика Станка Дякова, на която проф. Ескенази с признателност отдава решаваща роля за формирането на интереса му към математиката. През годините той самият ще се превърне в такъв преподавател – от онези, които не просто преподават материя, а формират начин на мислене. Кулминация на тези ученически години е бронзовият медал от VI Международна олимпиада по математика в Москва през 1964 г., когато той е част от българския национален отбор.

След завършването на Математическия факултет на Софийския университет „Климент Охридски“ през 1969 г. професионалният му път естествено се свързва с Института по математика и информатика при Българската академия на науките. Именно там той развива своята научна кариера – от млад научен сътрудник до професор – и допринася съществено за институционалното утвърждаване на информатиката в рамките на Академията.

Компютърно-базирано обучение и автоматизирано оценяване

Едно от най-ранните и последователни научноизследователски направления в работата на проф. Ескенази е компютърно-базираното обучение и автоматизацията на оценяването. Още през 70-те години той се насочва към въпроси, които днес изглеждат напълно естествени, но за времето си са били изключително новаторски: как компютрите могат да подпомагат обучението, как могат да се генерират и оценяват тестове автоматично и какви са педагогическите последици от това.

Тези идеи намират израз в дисертационния му труд, защитен през 1978 г., посветен на компютърно подпомогнатото генериране на тестове [6]. Работата му в тази област поставя основите на по-късните му изследвания върху компютърно-базираното обучение и го нарежда сред пионерите на тази тематика в България – години преди появата на термини като e-learning и digital education. Характерно за този период е разбирането му, че софтуерът не е просто технически артефакт и автоматизацията не е само технически проблем, а е сложна система, свързана с човешки, организа-

ционни и социални фактори.

Качество на софтуера и класификационни методи за оценка

Втората силна и международно разпознаваема линия в научната работа на проф. Ескенази е свързана с оценката и осигуряването на качеството на софтуерните продукти. В края на 80-те години той предлага оригинален модел за оценка на качеството на софтуера, който преодолява някои от основните недостатъци на доминиращите по това време йерархични тежки за прилагане подходи за оценка на софтуерното качество, като субективност и висока трудоемкост [5].

В основата на този модел стои прагматичното разбиране, че за много практически цели не винаги е необходимо да се изчислява точна числова стойност на качеството на даден софтуерен продукт. Много по-съществено е да се определи неговото място сред други добре познати продукти от същия тип и с утвърдено качество. По тази причина проф. Ескенази използва класификационни методи и техники за разпознаване на закономерности и класификация, при които софтуерните продукти се групират в класове като „отлични“, „добри“ или „незадоволителни“.

Чрез въвеждането на понятията за представителни множества от атрибути и неприводими тестове, представляващи минимални набори от характеристики, достатъчни за разграничаване на класове, проф. Ескенази разработва формален механизъм за идентифициране на онези характеристики, които реално разграничават класовете по качество. При оценката на нов софтуерен продукт неговите характеристики се съпоставят с тези на представителните множества, а неприводимите тестове определят минималните набори от атрибути, които са достатъчни за точно разпознаване на класа му. В случаите, когато резултатът не е еднозначен – например ако максималният брой гласове от представителите на класа не е уникален – методът допуска отсъствие на класификация, като по този начин се избягва произволно оценяване и се запазва надеждността на анализа.

Предложеният метод е реализиран в програмна система, чрез която е оценявано качеството на различни типове софтуер – от системи за управление на бази от данни до системи за автоматизирано обучение [4].

Този подход се отличава със своята концептуална яснота, намалена субективност и практическа приложимост, което му осигурява трайно място в научната литература.

Организация на софтуерното производство и практическа приложимост

Третото направление, което ясно се откроява в работата на проф. Ескенази, е разглеждането на софтуера като резултат от организиран производствен процес. За него софтуерът никога не е бил само код, а сложен продукт, чието качество зависи от методите на разработване, управлението на екипите и ясното дефиниране на отговорностите.

Това разбиране намира особено ярък израз в участието му в разработването на първия български бизнес софтуерен продукт за труд и работна заплата, създаден още през 1972 г. Продуктът се използва от над 1500 организации и представлява ранен пример за устойчиво софтуерно решение, което се развива и адаптира десетилетия наред. През 1983 г. за него е регистрирана първата в България търговска

марка за програмен продукт – ФИКС [3] – събитие с особено значение за утвърждаването на софтуера като обект на интелектуална собственост.

Информатика, общество и изкуствен интелект

През последните години научните интереси на проф. Ескенази все по-ясно се насочват към социалните и икономическите аспекти на информатиката и към ролята на информационните технологии в развитието на обществото. В тази насока той участва като член на работната група на БАН, разработила Рамката за национална стратегия за развитието на изкуствения интелект в България (2019) [2] и последвалата Визия за развитие на ИИ до 2030 г. [1]. В тези документи проф. Ескенази допринася с балансиран и аналитичен поглед, основан на дългогодишен опит. Като част от този ангажимент неговата позиция към развитието на изкуствения интелект се проявява ясно: тя е балансирана, критична и далеч от технологичния ентусиазъм без мярка. За него ИИ е не само мощен инструмент, но и сериозно предизвикателство, което изисква етика, законодателство и отговорна политика. В рамките на споменатите стратегически документи проф. Ескенази формулира принципите за устойчиво развитие на изкуствения интелект, като посочва три взаимосвързани стълба: общността, която разработва технологиите; широкия кръг от потребители и институции, които ги прилагат; и средата, която създава условия за това развитие чрез образование, законодателство, етични норми и обществено доверие. Този подход отразява неговото убеждение, че технологичният напредък трябва да бъде съпътстван от отговорна политика и обществен диалог.

Секция „Софтуерни технологии“ – научна визия и развитие

През 1985 г. проф. Ескенази създава и оглавява секция „Автоматизация на софтуерното производство“, преназначена по-късно в секция „Софтуерни технологии“ в ИМИ – БАН. В продължение на 26 години под негово ръководство секцията се утвърждава като едно от водещите звена в ИМИ – БАН, в което се развиват изследвания по софтуерно инженерство, качество на софтуера, управление на софтуерни процеси и приложни софтуерни системи. Характерно за управленския и научния стил на проф. Ескенази е разбирането, че научните структури трябва да отразяват динамиката на самата област, а не да се превръщат в самоцел. Именно поради това в определен момент – когато развитието на информатиката и софтуерното инженерство налага нови форми на сътрудничество и по-широки интердисциплинарни рамки – секция „Софтуерни технологии“ се обединява с другата водеща информатична секция в института – секция „Информационни изследвания“, на която дългогодишен ръководител беше проф. Петър Бърнев, поета след смъртта му от проф. Петър Станчев. Това обединение не е формален акт, а израз на споделено разбиране, че научните изследвания в бързо развиващи се области изискват концентрация на експертиза, обмен на идеи и готовност за промяна на установените организационни модели.

Този епизод е показателен за по-широкото виждане на проф. Ескенази за развитието на науката: той никога не се е вкопчвал в съществуващи структури или позиции, а е разглеждал организационните форми като средство, а не като цел. За него по-важни са били живият научен диалог, възможността за развитие на младите изследователи и адекватният отговор на новите предизвикателства пред софтуер-

ните технологии. Именно тази отвореност към промяна и динамика позволява на ръководените от него екипи да се адаптират към нови теми, методи и приложения, без да губят научната си идентичност.

В рамките на секцията и по-късно в разширените ѝ формати се развиват изследвания, които обхващат както фундаментални въпроси на софтуерното инженерство, така и конкретни приложни задачи. Под ръководството на проф. Ескенази се създава среда, в която теорията и практиката се разглеждат като взаимно допълващи се, а качеството, организацията и отговорността се утвърждават като водещи принципи на научната и проектната работа.

Преподавателска и обществена роля

Наред с научната си дейност проф. Ескенази има огромен принос в изграждането на новите поколения информатици. В продължение на десетилетия той води общо над 90 курса във ФМИ на Софийския университет, Икономическия университет – Варна, Нов български университет и други висши училища, като възпитава поколения специалисти с ясно изразено системно мислене. Той създава и въвежда за пръв път обучението по „Организация на данни“ (1975, ФМИ – СУ), „Системи за управление и организация на данни“ (1977, ФМИ – СУ), „Автоматизация на обучението“ (1980, ФМИ – СУ), „Организация и производство на програмно осигуряване“ (1984, ФМИ – СУ), Управление на софтуерното производство (2005, ИУ – Варна), Софтуерен бизнес (2011, ИУ – Варна) [7]. Хиляди студенти са минали през неговите лекции – често взискателни, винаги системни и нерядко поднесени с типичната за него фина ирония, която прави и най-сложните теми по-човешки.

Към всичко това се добавят ръководството на 10 защитили докторанти и около 20 защитили дипломанти, участието и ръководството на десетки международни и национални проекти, активна редакторска дейност, участие в научни съвети, журита, експертни групи и комисии.

Обществено признание

Научната и преподавателската дейност на проф. Аврам Ескенази е призната с множество национални и международни отличия, сред които: Грамота от Изпълнителния съвет на ФНИ (2016), ACM Senior member (2009), Международна награда за приноси в информационните теории и приложения ITHEA (2003), Почетна грамота от International University София за дългогодишна преподавателска дейност (2003), Грамота на МОН за постигнати съществени резултати при разработката на НИП „Изследване на софтуерни обекти и процеси и приложение към софтуерния маркетинг“ (И-406) през IV конкурсна сесия на НФ „НИ“ 1994-1997 (1998), Почетна значка на БАН (1986), Сребърна значка на ДКНТП за внедрен програмен продукт (1981).

През 2016 г. по случай неговата 70-годишнина проф. Ескенази бе удостоен с най-високото отличие на ИМИ – Медал с лента на ИМИ и грамота за неговите заслуги към ИМИ–БАН и значителния му принос към съвременната наука. Същата година бе избран за професор-емеритус на ИМИ, а през 2019 г. бе удостоен със званието „Почетен член на ИМИ“.

През 2022 г. проф. Аврам Ескенази бе отличен с академичната награда „Проф. Цани Каляджиев“ на Икономическия университет – Варна. Наградата се присъж-

да на всеки две години за изключителни постижения в науката на учени от България и чужбина в чест на основателя и пръв ректор на университета, проф. Цани Каляндjиев.

Но зад всички титли, награди и публикации стои човек – весел, общителен, с младежки ентусиазъм и самочувствие, изградено върху реални постижения. Колегите го познават като учен с ясна позиция и готовност за аргументиран спор, а студентите – като преподавател, който умее да заразява с интерес към професията.

И може би точно в това се крие най-ценното усещане, което проф. Ескенази оставя у всеки, който има шанса да разговаря с него – рядката комбинация от научна трезвост, непоколебим оптимизъм и онази детска любознателност, която не само не угасва с годините, а сякаш се задълбочава. Неговата позитивна енергия, ненатрапчивото остроумие и искреният интерес към всяка смислена тема правят всеки разговор с него истинско удоволствие – и напомнят, че най-голямата наука е да останеш човек.

Осемдесетата годишнина на проф. Аврам Ескенази е повод за признание и благодарност, но не и за заключителна равносметка. Защото неговият пример показва, че в науката най-важното не е колко години си навършил, а дали си запазил способността да се учудваш, да питаш и да търсиш по-добрите решения. А в това отношение проф. Ескенази остава ненадминат.

Литература

[1] Angelova, G. et al., AI for Smart Growth – Strategy for the Development of Artificial Intelligence in Bulgaria until 2030 (preliminary vision), 2020 (in Bulgarian: ИИ за интелигентен растеж – Стратегия за развитието на ИИ в България до 2030 г. (предварителна визия), Работна група на БАН, юни 2020) http://www.bas.bg/wp-content/uploads/2020/07/Proposal-National-Strategy-AI-2030-24June2020.pdf

[2] Angelova, G. et al., Framework for National Strategy for the Development of AI in Bulgaria, July 2019 (in Bulgarian: Рамка за Национална стратегия за развитието на ИИ в България, юли 2019) http://www.bas.bg/wp-content/uploads/2020/07/Towards-AI-Strategy-BAS-Vision-1July2019.pdf

[3] BG/N/1983/466, reg.N:13943, reg. date: 24.06.1983. https://portal.bpo.bg/bpo-registers/marks/view/BG_N_1983_466

[4] Eskenasi, A., Radev, R. Evaluation of the quality of authoring systems. Education and Computing, 5(1-2), 43-47 (1989) https://doi.org/10.1016/S0167-9287(89)80009-3

[5] Eskenasi, A.: Evaluation of software quality by means of classification methods. Journal of Systems and Software, 10(3), 213-216 (1989) https://doi.org/10.1016/0164-1212(89)90033-2

[6] Eskenazi, A. Automatic Text Generation (in Bulgarian: Автоматично генериране на тестове). PhD Thesis, dipl. 8185 / 06.07.1978

[7] Kaltinska, R., Biography of Prof. Eskenazi, presented at the "Museum of Mathematics and Informatics in Bulgaria". https://mmib.math.bas.bg/?page_id=10562 (last accesses at 12.02.2026)

CONTENTS

PREFACE 5

INVITED TALKS

V. D. Babev, M. Ivanov, R. Nikolov. On the Banach-Mazur Ellipse 9

Milena Dobreva. Digitised cultural heritage as data: emerging trends in its use in school-level computer science education 19

Nataliya Pavlova. Good practices in mathematics teacher training in the era of artificial intelligence 31

SECTION A: MATHEMATICAL STRUCTURES

Cvetelina Dinkova, Radostina Encheva. Focal surfaces of developable ruled surfaces and their invariants 49

Tatiana L. Todorova. A Diophantine inequality with mixed powers of four primes of a specific type 60

Kristiyan Vasilev. The edge-isoperimetric inequality for powers of cycles 78

SECTION B: MATHEMATICAL MODELING AND INFORMATICS

Valentin Bakoev. The four basic functions in the lexicographic generation of the subsets of a given set 87

Daniel Damyanov. Performance optimization of hybrid GNN–LLM pipelines for code comparison 98

Daniel Damyanov, Zlatko Varbanov. Semantic normalization on graph models searching structure matchings in code 107

Hristo Hristov. Bidirectional translation between text-based and block-based programming languages in the Logo tradition 117

Evgeniya Nikolova, Todor Slavov. AI-driven cybersecurity in critical infrastructure: A bibliometric analysis (2015–2025) 126

Tsvetelina Stefanova, Tsvetozar Georgiev. Evaluating systematic linguistic reasoning in large language models via linguistics olympiad problems 134

SECTION C: EDUCATION IN MATHEMATICS AND INFORMATICS

Ivaylo Dimitrov, Miroslav Hristov, Mehmed Kodzha. Analysis of selected mathematical problems in school education 153

Desislava Georgieva. A competence-based methodological framework for meaningful derivation of formulae for areas, surface areas and volumes in the preparation of future mathematics teachers 163

Plamen Gostev. Areas in convex quadrilateral 171
Kamelia Koleva. Divergent series – synergy between mathematical fallacies and summation methods 177
Tanya Marinova, Nataliya Borisova, Sevdalina Georgieva. STEAM workshop „Mathematics in the Varna Necropolis, 5^{th} Millennium BC" 186
Irena A. Parvanova, Yana Kancheva. The ellipse, parabola, and hyperbola as sections of a rotational cone with a plane 198
Irena A. Parvanova, Yana Kancheva. Auxiliary projection planes in solving some metric problems 205
Nataliia Snizhko. Ukrainian experience in teaching higher mathematics in English: outcomes and challenges 214
Ralitza Stamenkova. The importance of providing full solutions in mathematics assessment 223
Mariela Stancheva. Harnessing the power of primes: An educational game approach to prime numbers in middle school 232
Tsvetelina Stefanova, Slavi Georgiev. The expanding scope of artificial intelligence integration in mathematics education: A comprehensive review .. 242
Bilyana Stoynova. Optimization problem in financial resource management in profiled information technology education 255
Elena Traykova, Miroslava Nikolova, Philip Petrov. Gamification in computer modeling and information technologies for 6^{th} grade: functions and formulas in spreadsheets 265

IN MEMORIAM

Philip Petrov, Evgenia Sendova. In Memoriam: Ivan Tonov – the man for whom mathematics was an adventure, heuristics – a guide, and humor – a joyful "aha" 275

ANNIVERSARIES

Peter Boyvalenkov, Stefka Bouyuklieva. 80^{th} birth anniversary of Acad. Stefan Dodunekov 285
Nedyu Popivanov. Happy 80^{th} anniversary, Acad. Petar Popivanov! 298
Krassimira Ivanova. Prof. Avram Mois Eskenazi: An "Irreducible Test" for high scientific, social, and human value 303

СЪДЪРЖАНИЕ

ПРЕДГОВОР 5

ДОКЛАДИ ПО ПОКАНА

В. Д. Бабев, М. Иванов, *Р. Николов*. Елипса на Банах-Мазур 9

Милена Добрева. Дигитализираното културно наследство като данни: нови тенденции за използването му в училищното обучение по информатика 19

Наталия Павлова. Добри практики в подготовката на учители по математика в епохата на изкуствения интелект 31

СЕКЦИЯ А: МАТЕМАТИЧЕСКИ СТРУКТУРИ

Цветелина Динкова, Радостина Енчева. Фокални повърхнини на развиваеми праволинейни повърхнини и техните инварианти 49

Татяна Л. Тодорова. Диофантово неравенство със смесени степени на четири прости числа от специален тип 60

Кристиян Василев. Изопериметричното неравенство за ребрата на степените на цикличен граф 78

СЕКЦИЯ Б: МАТЕМАТИЧЕСКО МОДЕЛИРАНЕ И ИНФОРМАТИКА

Валентин Бакоев. Четирите основни функции при лексикографско генериране на подмножествата на дадено множество 87

Даниел Дамянов. Оптимизация на производителността на хибридни GNN-LLM изчислителни конвейери за сравнение на код 98

Даниел Дамянов, Златко Върбанов. Семантична нормализация върху графови модели при търсене на съвпадения на структури в код 107

Христо Христов. Двупосочен превод между текстово-базирани и блоково-базирани езици за програмиране в традицията на Logo 117

Евгения Николова, Тодор Славов. Киберсигурност в критичната инфраструктура: библиометричен анализ (2015–2025) 126

Цветелина Стефанова, Цветозар Георгиев. Оценяване на систематичното лингвистично разсъждение в големи езикови модели чрез задачи от лингвистични олимпиади 134

СЕКЦИЯ В: ОБРАЗОВАНИЕ ПО МАТЕМАТИКА И ИНФОРМАТИКА

Ивайло Димитров, Мирослав Христов, Мехмед Коджа. Анализ на подбрани математически задачи в училищното образование 153

Десислава Георгиева. Компетентностна методическа рамка за смислово извеждане на формули за лица, повърхнини и обеми в подготовката на бъдещи учители по математика 163
Пламен Гостев. Лица в изпъкнал четириъгълник 171
Камелия Колева. Разходящите редове – синергия между софизми и методи за сумиране 177
Таня Маринова, Наталия Борисова, Севдалина Георгиева. STEAM работилница „Математика във Варненския некропол, V хил. пр. Хр.“ 186
Ирена Първанова, Яна Кънчева. Елипсата, параболата и хиперболата като сечения на ротационен конус с равнина 198
Ирена Първанова, Яна Кънчева. Помощни проекционни равнини при решаването на някои метрични задачи 205
Наталия Снижко. Украински опит в преподаването на висша математика на английски език: резултати и предизвикателства 214
Ралица Стаменкова. Значението на предоставянето на пълни решения при оценяването по математика 223
Мариела Станчева. Овладяване силата на простите числа: образователен игрови подход към простите числа в прогимназиален етап 232
Цветелина Стефанова, Слави Георгиев. Разширяващият се обхват на интегрирането на изкуствения интелект в обучението по математика: всеобхватен обзор 242
Биляна Стойнова. Оптимизационна задача за управление на финансови ресурси в профилираното обучение по информационни технологии 255
Елена Трайкова, Мирослава Николова, Филип Петров. Игровизация по компютърно моделиране и информационни технологии за 6. клас: формули и функции в електронни таблици 265

IN MEMORIAM

Филип Петров, Евгения Сендова. IN MEMORIAM: Иван Тонов – човекът, за когото математиката беше приключение, евристиката – пътеводител, а хуморът – радостно „Аха“ 275

ЮБИЛЕЙНИ ДОКЛАДИ

Петър Бойваленков, Стефка Буюклиева. 80 години от рождението на акад. Стефан Додунеков 285
Недю Попиванов. Честит 80-и юбилей, академик Петър Попиванов! 298
Красимира Иванова. Проф. Аврам Ескенази: един „неприводим тест“ за висока научна, обществена и човешка стойност 303

Съюз на математиците в България

МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ

Част 2

Доклади на Петдесет и петата пролетна конференция
на Съюза на математиците в България
Трявна, 5 – 9 април 2026 г.



Union of Bulgarian Mathematicians

MATHEMATICS AND EDUCATION IN MATHEMATICS

Part 2

Proceedings of the Fifty-Fifth Spring Conference
of the Union of Bulgarian Mathematicians
Tryavna, April 5 – 9, 2026

Докладите се издават със съдействието на
Института по математика и информатика при БАН

FIFTY-FIFTH SPRING CONFERENCE
OF THE UNION OF BULGARIAN MATHEMATICIANS

Tryavna, April 5–9, 2026

Program committee:

Chair:
Prof. Tsonka Baicheva, D.Sc. (IMI–BAS)

Secretaries:
Chief Assist. Prof. Nikolay I. Nikolov, Ph.D. (IMI–BAS)
Assoc. Prof. Milen Borisov, Ph.D. (IMI–BAS)
Assoc. Prof. Borislava Kirilova, Ph.D. (Sofia University)

Members:
Acad. Petar Kenderov (IMI–BAS)
Acad. Oleg Mushkarov (IMI–BAS)
Prof. Nikolai Nikolov, D.Sc., Corr. Member of the Bulg. Acad. Sci. (IMI–BAS)
Prof. Peter Boyvalenkov, D.Sc., Corr. Member of the Bulg. Acad. Sci. (IMI–BAS)
Prof. Stepan Terzian, D.Sc. (Rousse University)
Prof. Stoyan Kapralov, D. Sc. (UBM Gabrovo)
Prof. Boyan Zlatanov, Ph.D. (Plovdiv University)
Prof. Maya Stoyanova, Ph.D. (Sofia University)
Prof. Stanislav Harizanov, Ph.D. (IICT and IMI–BAS)
Assoc. Prof. Krasimira Ivanova, Ph.D. (IMI–BAS)
Assoc. Prof. Parvan Parvanov, Ph.D. (Sofia University)
Assoc. Prof. Sevdalina Georgieva, Ph.D. (Technical University, Varna)
Assoc. Prof. Philip Petrov, Ph.D. (Sofia University)

Technical secretary:
Albena Vassileva (IMI–BAS)

Organizing committee:

Chair:
Mitko Kunchev (UBM Rousse)

Members:
Galina Bobeva, Ph.D. (Rousse Math School)
Tsvetana Kyumyurdjieva (Gabrovo Science and Math School)
Evelina Mincheva (Rousse Math School)
Anelia Angelova (Regional Dept. of Education, Rousse)
Kornelia Pashova (Gabrovo Science and Math School)
Velina Koeva (Gabrovo Science and Math School)
Albena Vassileva (IMI–BAS)
Ivanka Stoyanova (IMI–BAS)

Editorial board of the series:

Editor-in-chief:
Acad. Petar Kenderov
Acad. Oleg Mushkarov
Prof. Nikolai Nikolov, D.Sc., Corr. Member of the Bulg. Acad. Sci. (IMI–BAS)
Prof. Peter Boyvalenkov, D.Sc., Corr. Member of the Bulg. Acad. Sci. (IMI–BAS)
Prof. Ivan Landjev, D.Sc.
Albena Vassileva — secretary

Guest editors of Part 2 of the volume:
Prof. Peter Boyvalenkov, D.Sc., Corr. Member of the Bulg. Acad. Sci. (IMI–BAS)
Prof. Tsonka Baicheva, D.Sc.
Prof. Ivan Landjev, D.Sc.
Prof. Hristo Kostadinov, Pd.D.

Layout editor:
Assoc. Prof. Danila Cherkashin, D.Sc

Print:
Pythagoras Private High School, Sofia

© Union of Bulgarian Mathematicians, 2026

ПЕТДЕСЕТ И ПЕТА
ПРОЛЕТНА КОНФЕРЕНЦИЯ
НА СЪЮЗА НА МАТЕМАТИЦИТЕ В БЪЛГАРИЯ
Трявна, 5 – 9 април 2026 г.

Програмен комитет:

Председател:
проф. дн Цонка Байчева (ИМИ – БАН)

Секретари:
гл. ас. д-р Николай И. Николов (ИМИ – БАН)
доц. д-р Милен Борисов (ИМИ – БАН)
доц. д-р Бориславa Кирилова (ФМИ – СУ)

Членове:
акад. Петър Кендеров (ИМИ – БАН)
акад. Олег Мушкаров (ИМИ – БАН)
чл.-кор. Николай Николов (ИМИ – БАН)
чл.-кор. Петър Бойваленков (ИМИ – БАН)
проф. дмн Степан Терзиян (РУ)
проф. дмн Стоян Капралов (СМБ Габрово)
проф. д-р Боян Златанов (ФМИ – ПУ)
проф. д-р Мая Стоянова (ФМИ – СУ)
проф. д-р Станислав Харизанов (ИИКТ – БАН и ИМИ – БАН)
доц. д-р Красимира Иванова (ИМИ – БАН)
доц. д-р Първан Първанов (ФМИ – СУ)
доц. д-р Севдалина Георгиева (ТУ – Варна)
доц. д-р Филип Петров (ФМИ – СУ)

Технически секретар:
Албена Василева (ИМИ – БАН)

Организационен комитет:

Председател:
Митко Кунчев (СМБ Русе)

Членове:
д-р Галина Бобева (МГ „Баба Тонка“ – Русе)
Цветана Кюмюрджиева (ПМГ „Акад. Иван Гюзелев“ – Габрово)
Евелина Минчева (МГ „Баба Тонка“ – Русе)
Анелия Ангелова (РУО – Русе)
Корнелия Пашова (ПМГ „Акад. Иван Гюзелев“ – Габрово)
Велина Коева (ПМГ „Акад. Иван Гюзелев“ – Габрово)
Албена Василева (ИМИ – БАН)
Иванка Стоянова (ИМИ – БАН)

Редакционна колегия на поредицата:

Главен редактор:
акад. Петър Кендеров

акад. Олег Мушкаров
чл.-кор. Петър Бойваленков
чл.-кор. Николай Николов
проф. дмн Иван Ланджев
Албена Василева – секретар

Гост-редактори на Част 2 на тома:
чл.-кор. Петър Бойваленков
проф. дн Цонка Байчева
проф. дмн Иван Ланджев
проф. д-р Христо Костадинов

Предпечатна подготовка:
доц. дн Данила Черкашин

Печат:
ЧСУ „Питагор“, София

© Съюз на математиците в България, 2026

Формат: 1000 × 700/16	Дадена за печат на 23.03.2026 г.
Печатни коли 9	Подписана за печат на 24.03.2026 г.
Тираж 150	**ISSN 1313-3330** (Print), **2815-4002** (Online)

INTRODUCTION

On September 5, 2025, the 80th anniversary of the birth of Acad. Stefan Dodunekov was commemorated — an erudite scholar of recognized international authority, founder and long-time leader of the Bulgarian school of coding theory, Director of IMI–BAS (1999–2012), long-time President of the Union of Bulgarian Mathematicians (2003–2012), President of the Bulgarian Academy of Sciences (2012), and a person of vision and consistency in pursuing his goals.

We dedicate this volume of articles by his PhD students, students, and colleagues to mark the anniversary of his birth and to express our gratitude for all that he created. A program committee consisting of

— Corresponding Member Peter Boyvalenkov
— Professor Tsonka Baicheva
— Professor Ivan Landjev
— Professor Hristo Kostadinov

invited colleagues from Bulgaria and abroad who knew Acad. Dodunekov and worked with him over the years to contribute to the volume. The included papers address topics close to his scientific interests or present results in new directions of mathematics and computer science related to the development of modern communication technologies.

The volume contains 13 articles by mathematicians from Bulgaria, the United States, Russia, Spain, Japan, Singapore, Poland, and France who were his coauthors or partners in organizing joint scientific events.

ПРЕДГОВОР

На 5 септември 2025 година се навършиха 80 години от рождението на акад. Стефан Додунеков — ерудиран учен с доказан международен авторитет, основател и дългогодишен ръководител на българската школа по теория на кодирането, директор на ИМИ-БАН (1999–2012), дългогодишен председател на СМБ (2003–2012), председател на БАН (2012), човек с визия и последователност в осъществяване на целите си.

Посвещаваме този сборник със статии на негови докторанти, ученици и колеги, за да отбележим годишнината от рождението му и нашата признателност за сътвореното от него. Програмен комитет в състав

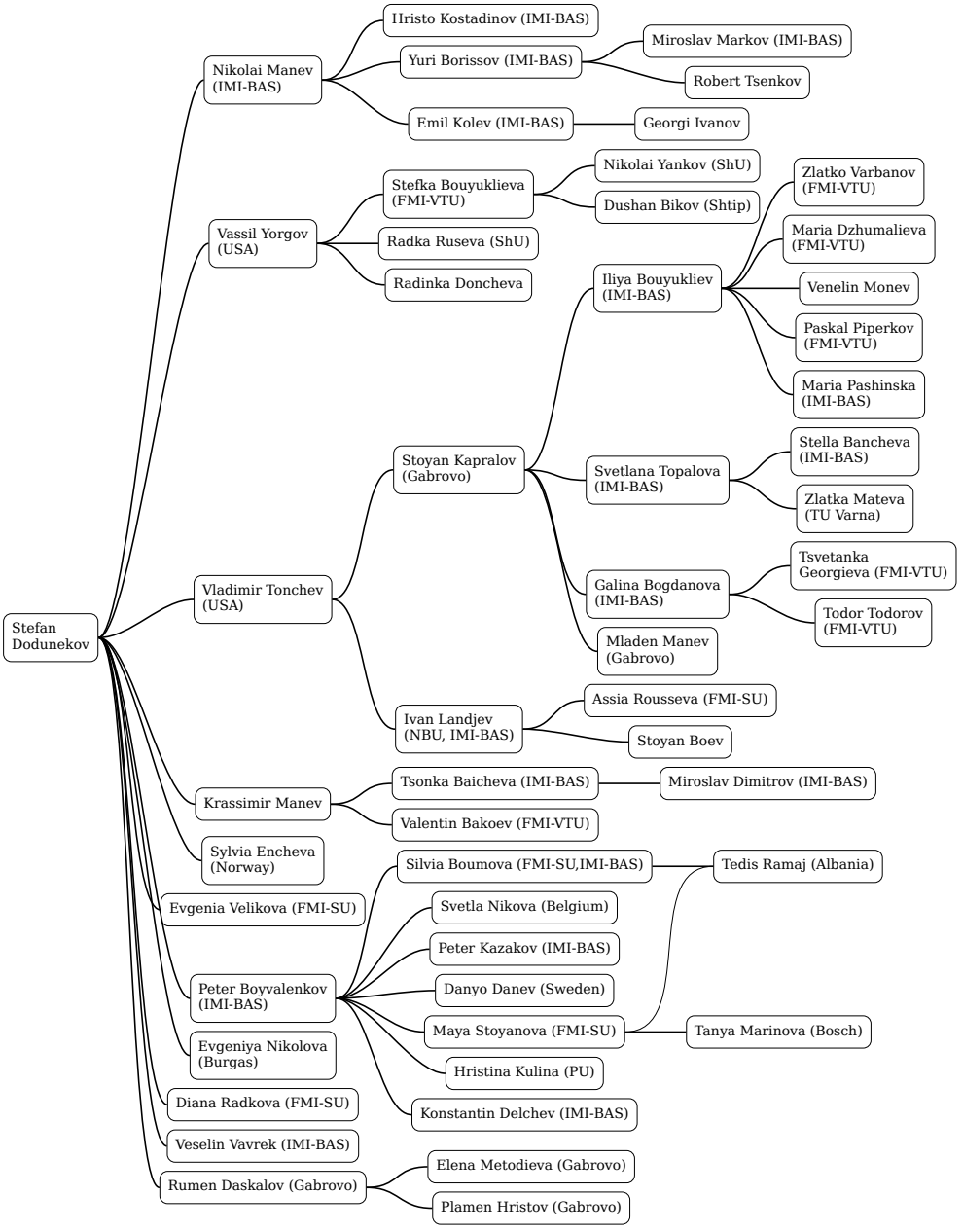
— Член-кореспондент Петър Бойваленков
— Професор Цонка Байчева
— Професор Иван Ланджев
— Професор Христо Костадинов

покани за участие колеги от страната и чужбина, които са познавали акад. Додунеков и са работили с него през годините. Включени са работи по тематики, които са близки до неговите научни интереси или представят резултати в нови направления на математиката и информатиката, свързани с развитието на съвременните комуникационни технологии.

Сборникът включва 13 статии на математици от България, САЩ, Русия, Испания, Япония, Сингапур, Полша и Франция, които са били негови съавтори или партньори в организирането на съвместни научни мероприятия.



Prof. Dodunekov at IMI-BAN, around 2010



Academic genealogy tree of the Bulgarian school of coding theory

МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2026
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2026
Proceedings of the Fifty-Fifth Spring Conference
of the Union of Bulgarian Mathematicians
Tryavna, Bulgaria, April 5–9, 2026

INTEGER CODES AND THEIR APPLICATIONS: AN OVERVIEW [1]

T. Alexandrova, H. Kostadinov, and N. L. Manev

Abstract

The paper is a short overview of the known applications of codes over a ring of integers modulo a given positive integer to error controlling in digital communications and storage. The presented successful applications demonstrate that integer codes with their simple encoding and decoding are at least commensurable with other codes with similar parameters. Moreover in many situations they are preferable.

2020 Mathematics Subject Classification: 94B12, 94B60, 94-02.

Key words: integer codes, QAM, flash memory, optical channels.

1 Introduction. Integer codes is the name used to refer to codes over a ring $\mathbb{Z}_q$ of integers modulo a given positive integer q (not necessarily a power of a prime). They are defined as the dual space of an $m \times n$ parity-check matrix $\mathbf{H}$ with elements from $\mathbb{Z}_q$, namely

$$\mathcal{C}(\mathbf{H}) = \{\mathbf{c} \in \mathbb{Z}_q^n \mid \mathbf{c}\mathbf{H}^T = \mathbf{0}\}.$$

We will write only $\mathcal{C}$ if there is no possibility for ambiguity.

$\mathcal{C}$ is said to be $[n, n-m]_q$ integer code although it is a linear space only in the case q prime. In general so defined codes are algebraic modules over a ring. Their properties, although very close, differ from ones of linear spaces. In particular the size of $\mathcal{C}$ may differ from q^{n-m}.

Maybe the first application of integer codes was proposed by Varshamov and Tenengolz in [23, 22] as codes correcting single asymmetric errors. Since that time integer codes have been successfully used in many applications. Vinck and Morita [5] have applied such codes to magnetic recording and frame synchronization. Kostadinov, Morita and Manev proposed in [12, 13] integer codes to be applied to coded modulation. The papers [11, 15, 10, 2] present investigations in the same direction.

[1]The research of the first author is supported, in part, by Center of Excellence in Informatics and ICT under the Grant BG16RFPR002-1.014-0018-C01, financed by the Research, Innovation and Digitalization for Smart Transformation Programme 2021–2027 and co-financed by the European Union. The research of the second author has been partially supported by the National Science Fund of Bulgaria under Grant KP-06-N82/5. The research of the third author is supported, in part, by National Center for High Performance and Distributed Computing under Grant DO1-325/01.12.2023.

https://doi.org/10.55630/mem.2026.55.320-328

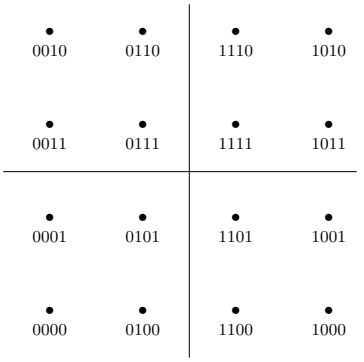


Figure 1: 16-SQAM constellation with Gray mapping

Other areas of applications of integer codes are flash memory [3, 6, 7, 8] and several specific uses given in [19, 20, 17, 21, 18, 16, 14].

The successful application of integer codes to many different areas in communications and storage is due to not only their simple encoding and decoding but the fact that integer codes can be constructed to correct the dominant in the channel type of errors. By choosing a proper parity-check matrix one can construct a code correcting specific types of errors.

Definition 1.1. *Let k_i, l_j, $i = 1, \ldots, s$, $j = 1, \ldots, m$ be positive integers. A code $\mathcal{C}(\mathbf{H})$ is said to be w $(\pm k_1, \pm k_2, \ldots, \pm k_s, l_1, l_2, \ldots, l_m)$-**error correctable** if it can correct any error vector with at most w nonzero entries with values l_j or $\pm k_i$.*

Requirements for error-correcting properties of integer codes lead to a lower bound for q. For example, if the code $\mathcal{C}(\mathbf{H})$ is a single $(\pm k_1, \pm k_2, \ldots, \pm k_s, l_1, l_2, \ldots, l_m)$-error correctable then

$$q \geq (2s + m)n + 1.$$

The goal of this paper is to present in short the research results on integer codes with an accent on construction of such codes for practical applications in digital communication and storage.

2 Application to coded Quadrature Amplitude Modulation. The name coded modulation schemes is commonly used for communication schemes that integrate modulation and error-correcting techniques. Quadrature Amplitude Modulation (QAM) is a communication scheme for transmission of data by signals that are sum of two orthogonal signals with prescribed amplitudes. Signals are represented as points in the plane and form a finite lattice called constellation. The most implemented constellation scheme is Square Quadrature Amplitude Modulation (SQAM) whose constellation of signal points is a square or rectangular lattice with sides parallel to coordinate axes. However Triangular Quadrature Amplitude Modulation (TQAM) and several specific types of constellations are also studied.

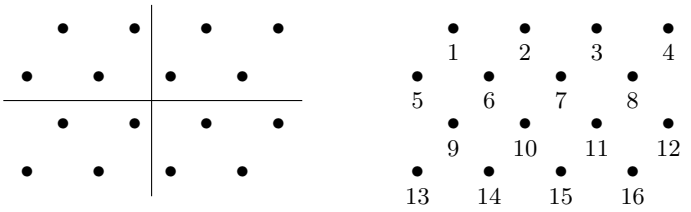


Figure 2: 16-TQAM constellations and a possible numbering of its points by elements of $\mathbb{Z}_{17}$

Signal points of TQAM form a lattice of equilateral triangles. They are placed in rows parallel to the horizontal axis and the constellation is symmetric with respect to the origin. If the side of triangles has length $2d$, the distance between horizontal rows is $h = d\sqrt{3}$ (which is the altitude of the equilateral triangles). An example of 16-TQAM is given in Figure 2.

Due to the noise in the communication channel the sent point can be erroneously detected as another point, most probably as one of the nearest neighbor points. In the case of SQAM there are 4 such points (see Figure 1) while in the case of TQAM there are 6 nearest points (see Figure 2). Figure 2 shows that the nearest points correspond to differences $E = \{\pm 1, \pm 3, \pm 4, \pm 5\}$ between their labels. It is easy to see (the numbers of next row increase by t) that in the general case of t^2-TQAM constellation labeled by the nonzero elements of $\mathbb{Z}_{t^2+1}$ the set of possible differences to the nearest neighbors' labels is

$$E = \{\pm 1, \pm(t-1), \pm t, \pm(t+1)\}.$$

In [2] single $(\pm 1, \pm(t-1), \pm t, \pm(t+1))$-error correctable codes with maximum possible length are described. Namely, the following is proven

Theorem 2.1 ([2]). *Let*

$$H_{a_0} = \{a_0 t + a_1 \mid 3a_0 + 1 \leq a_1 \leq t - 2a_0 - 2\}.$$

For a given even integer $t \geq 6$, the integer code $\mathcal{C}(\mathbf{H})$ over $\mathbb{Z}_{t^2+1}$ with parity-check matrix $\mathbf{H} = (H_0, H_1, H_2, \ldots, H_m)$, where $m \leq \frac{t-2}{5}$, is single $(\pm 1, \pm(t-1), \pm t, \pm(t+1))$-error correctable.

Table 1 contains the parity-check matrices $\mathbf{H}$ with maximum possible length of single $(\pm 1, \pm(t-1), \pm t, \pm(t+1))$-error correctable integer codes for even $t:\ 6 \leq t \leq 20$.

The graphs in Figure 3 present the probability of error per bit (BER) in the cases when the code defined by $\mathbf{H} = (12, 6, 5, 4, 3, 2, 1)$ and Gray encoding are used in a channel with Gaussian noise.

Let us remark that any shorten matrix of the ones given in Table 1 also defines a code with the same error-correcting property but with a lower coding rate. However,

t	q	**H**
6	37	(1,2,3,4)
8	65	(1,2,3,4,5,6,12)
10	101	(1,2,3,4,5,6,7,8,14,15,16)
12	145	(1,2,...,10,16,17,18,19,20)
14	197	(1,2,...,12,18,...,24,35,36)
16	257	(1,2,...,14,20,...,28,39,...,42,56)
18	325	(1,2...,16,22,...,32,43,...,48,64)
20	401	(1,2...,18,24,...,36,47,...,54,70,71,72)

Table 1: Parity-check matrices H of single $(\pm 1, \pm(t-1), \pm t, \pm(t+1))$-error correctable integer codes over $\mathbb{Z}_{t^2+1}$ for even $t:\ 6 \leq t \leq 20$. [2]

depending on noise characteristics of the communication channel shortened codes can give better performance.

3 Application to Flash Memory. Flash memory requires error control coding like other devices for communication or storage. However due to the used technology of vertically stacked cells, in contrast with the classical case, the error vectors with the same weight are not equally probable.

A mathematical model that corresponds well to the writing and reading is as follows. If the cells have q states then one can consider pages and blocks as vectors over the ring $\mathbb{Z}_q$ and errors can be considered as changes of the values of vectors' entries. Changes of the entries of the vectors are mainly in an upward direction with limited-magnitude values but decreasing with 1 can be observed, too. Hence errors are of type ± 1 and $(2, 3, \ldots l)$ for a small l.

Asymmetric limited-magnitude error-correcting codes were proposed by Varshamov and Tenengolz [23, 22] and in a more general form by Ahlswede, Aydinian, and Khachatrian [1]. Another general method for construction of asymmetric limited-magnitude error-correcting codes is provided by Cassuto, Schwartz, Bohossian and Burck [3]. In 2011, Klove and Bose [6] proposed systematic codes that correct single limited-magnitude systematic asymmetric errors and achieve a higher rate than the ones given in [3]. They also showed how their code construction can be slightly modified to give codes correcting symmetric errors of limited magnitude. Later Klove, Lou, Naydenova and Yari [7] extended their results and gave a necessary and sufficient condition for the existence of a code over $GF(p)$ correcting a single asymmetric error.

In [8] we propose constructions of codes over $\mathbb{Z}_{2^n+1}$ correcting single asymmetric errors of type $(1, 2)$, $(\pm 1, \pm 2)$ or $(1, 2, 3)$. The argument $q = 2^n + 1$ is chosen due to the fact that it is the smallest integer greater than a power of two. The choice of q is essential since the use of the inappropriate size of the alphabet can generate problems in implementation of encoding and decoding procedures.

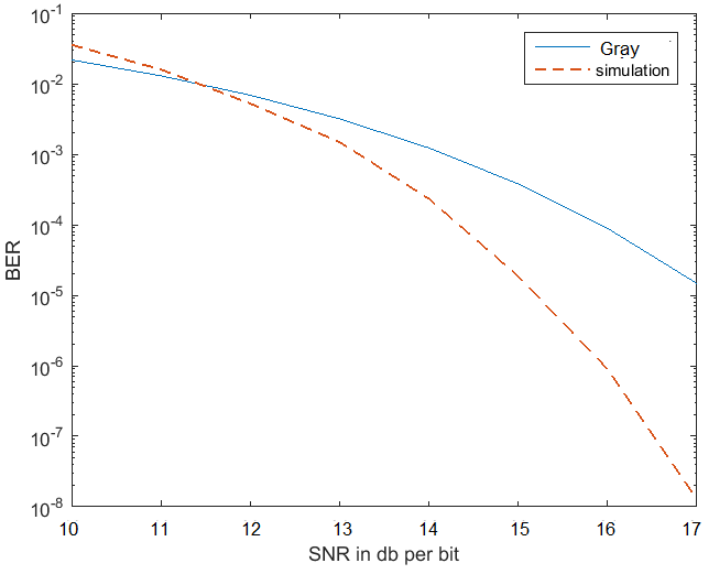


Figure 3: BER of 64-TQAM vs. signal to noise ratio [2]

Theorem 3.1 ([8]). *Let* $q = 2^n + 1$ *and* $A_s = \{s2^i \pmod q \mid i = 0, 1, \ldots\}$ *be the cyclotomic coset of 2 modulo* q *with leader* s. *Let* $A_s^0 = \{s2^{2i} \pmod q \mid i = 0, 1, \ldots\}$, $A_s^1 = \{s2^{2i+1} \pmod q \mid i = 0, 1, \ldots\}$. *Then* $|A_s|$ *is even with* $|A_s| = 2n$ *for* $(s, q) = 1$ *and both the integer codes with* $\mathbf{H} = (A_1^0)$ *and* $\mathbf{H} = (A_1^1)$ *are single* $(1, 2)$ *asymmetric error correctable.*

Corollary 3.2 ([8]). *Under the notations of Theorem 3.1, let* $s_1, s_2, \ldots, s_t$ *be all different leaders of cyclotomic cosets of 2 modulo* A. *Then*

$$\mathbf{H} = (A_{s_1}^0 \ A_{s_2}^0 \ \cdots \ A_{s_t}^0)$$

is a parity-check matrix of a single $(1, 2)$ *asymmetric error correctable* $[2^{n-1}, 2^{n-1} - 1]$ *code over* $\mathbb{Z}_q$.

Corollary 3.3. *[8] If* $n > 2$ *the code with* $\mathbf{H} = (A_1^0)$ *is a single* $(1, 2, 3)$ *asymmetric error correctable.*

Theorem 3.4 ([8]). *Under the notations of Theorem 3.1 let* A_s^{00} *be the set of first* $\lfloor (|A_s^0|)/2 \rfloor$ *elements of* A_s^0. *If* $|A_s| \geq 8$ *then* A_s^{00} *is a parity-check matrix of a single* $(\pm 1, \pm 2)$ *error correctable code.*

Corollary 3.5 ([8]). *Using notation and conditions of Theorem 3.1 the code with*

$$\mathbf{H} = (A_{s_1}^{00} \ A_{s_2}^{00} \ \cdots \ A_{s_t}^{00})$$

is a single $(\pm 1, \pm 2)$ *error correctable code over* A *when* $|A_{s_i}| \geq 4$ *and* s_i *are distinct leaders.*

4 Application to optical channels. In this section we describe integer codes and their use for error-correction in a binary channel with specific dominant errors. The channel is a theoretical model of wireless optical channels (see [4]). However our approach is applicable to any binary channel.

Any binary sequence can be considered as a sequence of blocks of bits with the same length b. (We call such blocks b-*bytes*, but b is not necessarily equal to 8). Any block can be interpreted as a nonnegative integer less than 2^b, that is, as an element of $\mathbb{Z}_q$ with $q \geq 2^b$. Hence the sequence can be considered as a sequence of elements of $\mathbb{Z}_q$ and encoding by integer codes over $\mathbb{Z}_q$ can be applied to.

It seems that the natural choice is $q = 2^b$, but it is not the right choice in general. Indeed the situation is more complex. Note that changing one bit in a b-byte is equivalent to adding or subtracting 2^i, $i = 0, 1, \ldots, b-1$, to the integer corresponding to the b-byte. However 2^i divides 2^b that generates complications. If $q > 2^b$ there are elements of $\mathbb{Z}_q$ which cannot be transmitted over the channel, thus, they must not appear as coordinates of the codewords. Hence, the encoding procedure has to comply with this requirement.

Let $B \in \mathbb{Z}_q$ be the integer corresponding to a given b-byte sent through the communication channel. The received b-byte is presented by number $V = B + E$, where $-2^b < E < 2^b$.

Single bit errors in a b-byte are presented in [9] by:

E1 The $(i+1)$-th bit $1 \to 0$: $E = -2^i, i = 0, 1, \ldots, b-1$.

E2 The $(i+1)$-th bit $0 \to 1$: $E = 2^i, i = 0, 1, \ldots, b-1$.

All other error configurations in a single b-byte correspond to combinations of E1 and E2, thus E is a sum of powers (positive or negative) of 2.

In [9] we propose a construction of a class of integer codes over $\mathbb{Z}_{2^b+1}$ that can correct up to two bit errors per a b-byte. Such error configurations have been observed in experiments with many binary channels, e.g., with wireless optical channels. The construction is based on cyclotomic cosets of 2 modulo $q = 2^b + 1$.

Theorem 4.1 ([9])**.** *Any integer code over $\mathbb{Z}_q$, $q = 2^b + 1$, having parity-check matrix $\mathbf{H} = (h_1, h_2, \ldots, h_n)$, where h_j is a leader of cyclotomic coset with length $2b$ can correct a single $\pm 2^i$-error, $i = 0, 1, \ldots, b-1$.*

Theorem 4.2 ([9])**.** *Let $\mathcal{E}$ be a set of cyclotomic cosets containing C_1. If there exist $h_2, \ldots, h_n \in \mathbb{Z}_A$ such that $\mathcal{E}, h_2\mathcal{E}, \ldots, h_n\mathcal{E}$ are disjoint sets of different cosets then the code with parity-check matrix $\mathbf{H} = (1, h_2, \ldots, h_n)$ can correct error values that belong to $\mathcal{E}$ and, of course, bit error configurations corresponding to them.*

The considered set of error values is a proper subset of

$$\mathcal{E} = \bigcup C_{2^k \pm 1},\ k = 1, \ldots, \lfloor b/2 \rfloor.$$

Example 4.3 ([9])**.** *Let $\mathbf{b} = \mathbf{10}$, $\mathbf{n} = \mathbf{3}$. In this case a code that corrects up two bits errors in a single b-byte per codeword has parity-check matrix $\mathbf{H} = (1\ 19\ 27)$:*

$$\mathcal{E} \subset C_1 \cup C_3 \cup C_5 \cup C_7 \cup C_9 \cup C_{15} \cup C_{17} \cup C_{31}, \quad C_{33} = C_{31},$$

$$19\mathcal{E} \subset C_{19} \cup C_{57} \cup C_{35} \cup C_{39} \cup C_{171} \cup C_{105} \cup C_{43} \cup C_{109},$$
$$27\mathcal{E} \subset C_{27} \cup C_{59} \cup C_{55} \cup C_{51} \cup C_{53} \cup C_{155} \cup C_{107} \cup C_{47}.$$

Length $n = 3$ is the maximal possible value for such a code.

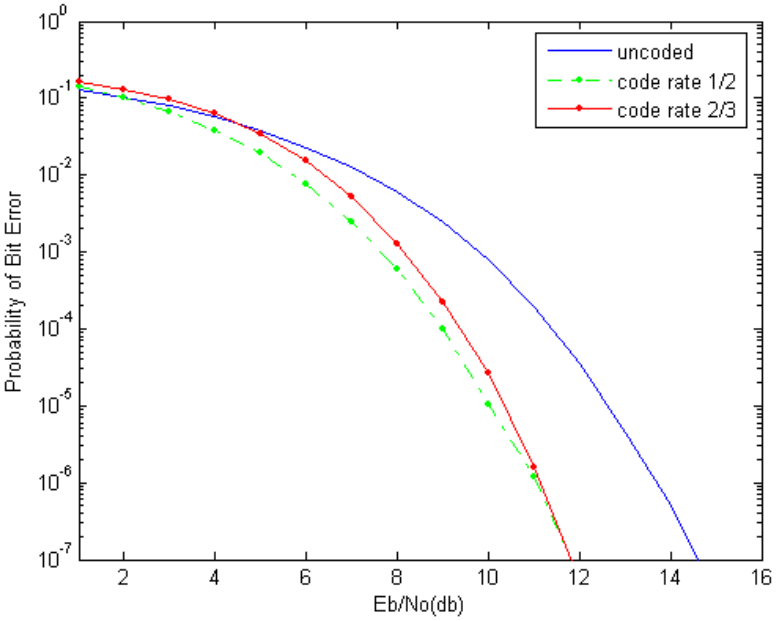


Figure 4: BER for the code given in Example 4.1 and the code with $\mathbf{H} = (1\ 23)$ over $\mathbb{Z}_{512}$, see [9].

Figure 4 presents in graphical form probability of bit error (BER) versus signal/noise ratio per bit in decibels for a noisy wireless optical channel. To simulate the channel we have used the MATLAB file given in [4]. The blue solid curve gives BER in the case when no error-correcting code is used. The red (solid line with dots) curve corresponds to applying the code given in Example 4.1. The green curve corresponds to the code defined by $\mathbf{H} = (1\ 23)$ over $\mathbb{Z}_{512}$. The code from Example 4.1 demonstrates slightly worse performance which is the price of the higher code rate.

5 Conclusion. The successful applications to several devices for communications and storage which are presented in this paper demonstrate that integer codes with their simple encoding and decoding are at least commensurable with other codes with similar parameters. Moreover, in many situations they are preferable.

REFERENCES.

[1] R. AHLSWEDE, H. AYDINIAN, and L. KHACHATRIAN. Undirectional error control codes and related combinatorial problems. In *Proc. of the Eighth International Workshop on Algebraic and Combinatorial Coding Theory (ACCT'2002)*, pages 6–9, 2002.

[2] T. ALEXANDROVA, H. KOSTADINOV, and N. MANEV. General construction of integer codes correcting single error in t^2-TQAM. *Computers and Electrical Engineering*, 127:110572, 2025.
[3] Y. CASSUTO, M. SCHWARTZ, V. BOHOSSIAN, and J. BURCK. Codes for asymmetric limited-magnitude errors with application to multi-level flash memories. *IEEE Trans. Inf. Theory*, 56:1582–1595, 2010.
[4] Z. GHASSEMLOOY, W. POPOOLA, and S. RAJBHANDARI. *Optical Wireless Communications, System and Channel Modelling with MATLAB*. CRC Press. ISBN 13: 978-1-4398-5235-4.
[5] A.J. HAN VINCK and H. MORITA. Codes over the ring of integers modulo m. *IEICE Trans. on Fundamentals*, E81-A(10):2013–2018, 1998.
[6] T. KLOVE and B. BOSE. Systematic, single limited magnitude error correcting codes for flash memories. *IEEE Trans. Inf. Theory*, 57:4477–4487, 2011.
[7] T. KLOVE, J. LOU, I. NAYDENOVA, and S. YARI. Some codes correcting asymmetric errors of limited magnitude. *IEEE Trans. Inf. Theory*, 57:7459–7472, 2011.
[8] H. KOSTADINOV and N. MANEV. Integer codes correcting asymmetric errors in nand flash memory. *Mathematics*, 9:1269, 2021.
[9] H. KOSTADINOV and N. MANEV. A general construction of integer codes correcting specific errors in binary communication channels. *Mathematics*, 11:2521, 2023.
[10] H. KOSTADINOV and N. MANEV. New integer coded hexagonal QAM schemes and their performance in AWGN channel. In *Studies in Computational Intelligence*. Volume 1076, pages 100–110. Springer, 2023.
[11] H. KOSTADINOV, H. MORITA, N. IIJIMA, A.J. HAN VINCK, and N. MANEV. Soft decoding of integer codes and their application to coded modulation. *IEICE Trans. on Fundamentals*, E39-A(7):1363–1370, 2010.
[12] H. KOSTADINOV, H. MORITA, and N. MANEV. Integer codes correcting single errors of specific types $(\pm e_1, \pm e_2, \ldots, \pm e_s)$. *IEICE Trans. on Fundamentals*, E86-A(7):1843–1849, 2003.
[13] H. KOSTADINOV, H. MORITA, and N. MANEV. Derivation on bit error probability of coded QAM using integer codes. *IEICE Trans. on Fundamentals*, E87-A(12):3397–3403, 2004.
[14] M.J. MIHALJEVIĆ, A. RADONJIĆ, L. WANG, and S. XU. Security enhanced symmetric key encryption employing an integer code for the erasure channel. *Symmetry*, 14:1709, 2022.
[15] H. MORITA. Nearest-neighbor error correcting codes on a hexagonal signal constellation. In *ISIT 2015*, pages 2480–2484, 2015.
[16] N. K. POKHREL and P. K. DAS. Low-density and high-density asymmetric CT-burst correcting integer codes. *Advances in Mathematics of Communications*, 18(3):842–856, 2024.
[17] A. RADONJIC. (Perfect) integer codes correcting single errors. *IEEE Commun. Lett.*, 22(1):17–20, 2018.
[18] A. RADONJIC. Integer codes correcting double errors and triple-adjacent errors within a byte. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 28(8):1901–1908, 2020.
[19] A. RADONJIC and V. VUJICIC. Integer codes correcting burst errors within a byte. *IEEE Trans Comput*, 62(2):411–415, 2013.
[20] A. RADONJIC and V. VUJICIC. Integer codes correcting single errors and burst asymmetric errors within a byte. *Inf. Process. Lett.*, 121:45–50, 2017.
[21] A. RADONJIC and V. VUJICIC. Integer codes correcting sparse byte errors. *Cryptography and Communications*, 11:1069–1077, 2019.
[22] R. VARSHAMOV. A class of codes for asymmetric channels and a problem from the additive theory of numbers. *IEEE Trans. on Information Theory*, 19(1):92–95, 1973.
[23] R. VARSHAMOV and G. TENENGOLZ. A code for correcting a single asymmetric error. *Automatika i Telematika*, 26(2):288–292, 1965. (in Russian).

Todorka Alexandrova, Hristo Kostadinov, Nikolai Manev
Institute of Mathematics and Informatics, Bulgarian Academy of Sciences
Acad. G. Bonchev Str., Bl. 8, 1113 Sofia, Bulgaria
Centre of Excellence in Informatics and Information and Communication Technologies
1113 Sofia, Bulgaria
e-mail: `toty@math.bas.bg, hristo@math.bas.bg, nlmanev@math.bas.bg`

КРАТЪК ОБЗОР НА ЦЕЛОЧИСЛЕНИТЕ КОДОВЕ И ТЕХНИТЕ ПРИЛОЖЕНИЯ

Т. Александрова, Х. Костадинов и Н. Л. Манев

Абстракт

Статията представлява кратък преглед на известните приложения на кодове над пръстени от цели числа по модул дадено естествено число за контрол на грешките в цифровите комуникации и съхранението на данни. Представените приложения показват, че целочислените кодове с тяхното просто кодиране и декодиране са поне съизмерими с други кодове с подобни параметри и в много ситуации са за предпочитане за използване в практиката.

Ключови думи: кодове над пръстени от цели числа, квадратурно-амплитудна модулация, флаш памети, оптични канали.

МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2026
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2026
Proceedings of the Fifty-Fifth Spring Conference
of the Union of Bulgarian Mathematicians
Tryavna, Bulgaria, April 5–9, 2026

NEW OPTIMAL $(v, k, 1)$ OPTICAL ORTHOGONAL CODES WITH $k = 3, 5, 6$ [1]

Tsonka Baicheva and Svetlana Topalova

Abstract

The known classifications of optimal optical orthogonal codes with small k show that when the code length v grows, the number of nonequivalent codes increases very fast. This either makes the complete classification for relatively big values of v infeasible, or the number of the obtained codes is so big that it is very difficult to choose among them a code with the properties you need. That is why in the present work we do not obtain all the codes with the considered parameters. We construct sets of new optimal $(v, k, 1)$ optical orthogonal codes with $k = 3, 5$, and 6 for relatively small values of the code lengths v for which no classification results are known. The codes in each of these sets differ from one another in many codewords. They can be used in practical applications, as well as in further research on the topic.

2020 Mathematics Subject Classification: 94B60, 94B65.

Key words: coding theory, optimal optical orthogonal code, binary cyclically permutable constant weight code, cyclic difference family, cyclic design.

1 Introduction.

1.1 Definitions and notations. Denote by $\mathbb{Z}_v$ the additive group of integers modulo v. Let M be a k-subset of $\mathbb{Z}_v$, where $M = \{m_1, m_2, \ldots, m_k\}$. Then $M + t$ denotes a t-translate of M, where $M + t = \{m_1 + t, m_2 + t, \ldots, m_k + t\}$, $t \in \mathbb{Z}_v$.

A $(v, k, 1)$ optical orthogonal code (OOC) can be defined as a collection

$$\mathcal{C} = \{C_1, \ldots, C_s\}$$

of k-subsets of $\mathbb{Z}_v$ (*codewords*), such that any two translates of a codeword share at most one element, and any two translates of two distinct codewords also share at most one element:

$$|C_i \cap (C_i + t)| \leq 1, \quad 1 \leq i \leq s, \quad 1 \leq t \leq v - 1, \tag{1}$$

$$|C_i \cap (C_j + t)| \leq 1, \quad 1 \leq i < j \leq s, \quad 0 \leq t \leq v - 1. \tag{2}$$

[1]The first author was partially supported by the National Science Fund of Bulgaria under Grant KP-06-N82/5. The second author was partially supported by the National Science Fund of Bulgaria under Contract No KP-06-H92/3 - 08.12.2025.

https://doi.org/10.55630/mem.2026.55.329-339

Originally, OOCs were defined as a collection of $\{0,1\}$ sequences [18], but, for some purposes, it is easier to present the codewords as subsets of $\mathbb{Z}_v$, and that is why the above definition is widely used too [11]. Condition (1) is called the auto-correlation property and (2) — the cross-correlation property. A $(v,k,1)$ OOC is equivalent to a binary $(v,k,1)$ cyclically permutable constant weight (CPCW) code.

Two $(v,k,1)$ OOCs $\mathcal{C}$ and $\mathcal{C}'$ are *isomorphic* if there exists a permutation φ of $\mathbb{Z}_v$, which maps the collection of translates of each codeword of $\mathcal{C}$ to the collection of translates of a codeword of $\mathcal{C}'$. These two codes are *multiplier equivalent* if φ is an automorphism of $\mathbb{Z}_v$ (of the cyclic group of order v). An automorphism of a $(v,k,1)$ OOC $\mathcal{C}$ is a permutation α of $\mathbb{Z}_v$, which maps the collection of translates of each codeword of $\mathcal{C}$ to the collection of translates of a codeword of $\mathcal{C}$. If α is an automorphism of $\mathbb{Z}_v$, the automorphism of the OOC is called a multiplier automorphism.

Consider a codeword $C_i = \{c_1, c_2, \ldots, c_k\}$, $1 \le i \le s$. Denote by $\triangle C_i$ the multiset of the values of the differences $c_n - c_m,\ n \ne m,\ n,m = 1,\ 2,\ \ldots,\ k$. The auto-correlation property means that all the differences of a codeword of a $(v,k,1)$ OOC are distinct. For a $(v,k,1)$ OOC $\mathcal{C}$ the cross-correlation property means that $\triangle C_i \bigcap \triangle C_j = \emptyset$ for two distinct codewords $C_i, C_j \in \mathcal{C}$. If all possible $v-1$ nonzero differences are covered by the differences of the codewords, the $(v,k,1)$ OOC is called *perfect*.

OOCs are related to various other combinatorial structures [19]. We shall define some of them below.

Let $V = \{P_i\}_{i=1}^{v}$ be a finite set of *points*, and $\mathcal{B} = \{B_j\}_{j=1}^{b}$ a finite collection of k-element subsets of V, called *blocks*. $D = (V, \mathcal{B})$ is a *(partial) design* with parameters 2-$(v,k,1)$ if any 2-subset of V is contained in (at most) exactly one block of $\mathcal{B}$. A 2-$(v,k,1)$ design is also called a Steiner system and denoted by $S(2,k,v)$.

Two 2-$(v,k,1)$ (partial) designs D and D' are *isomorphic* if there exists a permutation of the points which maps each block of D to a block of D'. An automorphism of D is an isomorphism to itself.

A 2-$(v,k,1)$ (partial) design is *cyclic* if it has an automorphism permuting its points in one cycle. A cyclic (partial) design is *strictly cyclic* if each block orbit under this automorphism is of length v (no short orbits). Two cyclic 2-$(v,k,1)$ (partial) designs D and D' are *multiplier equivalent* if there exists an automorphism of $\mathbb{Z}_v$ which maps each block of D to a block of D'. A multiplier automorphism of the (partial) design D is an automorphism of $\mathbb{Z}_v$ which maps each block of D to a block of D.

A k-element subset of $\mathbb{Z}_v$ is called *full* if the number of its distinct translates is v, and *short* if it is less than v.

A $(v,k,1)$ *cyclic difference family* can be defined as a set $D = \{B_1,\ B_2, \ldots, B_s\}$ of k-element subsets of $\mathbb{Z}_v$ (blocks), such that $B_n = \{b_{n1},\ b_{n2}, \ldots, b_{nk}\}$ and each nonzero element of $\mathbb{Z}_v$ either appears in the short block $\{0, v/k, 2v/k, \ldots, (k-1)v/k\}$ (possible if k divides v), or is obtained exactly once as a difference $b_{ni} - b_{nj}$ for $i,j = 1, \ldots, k$ and $i \ne j$.

Two $(v,k,1)$ cyclic difference families are *equivalent* if there is an automorphism α of $\mathbb{Z}_v$ which maps each k-element subset of the first family to a translate of a subset of the second family.

The size s of a $(v,k,1)$ OOC is the number of its codewords. It cannot exceed

$$\left\lfloor \frac{v-1}{k(k-1)} \right\rfloor .$$

OOCs which reach this bound are called *optimal*. If the size is exactly $(v-1)/k(k-1)$, the $(v,k,1)$ OOC is perfect. That is why optimal $(v,k,1)$ OOCs with $k=3,5,6$ are perfect if and only if $v=6n+1$, $v=20n+1$, and $v=30n+1$ respectively.

A perfect $(v,k,1)$ OOC corresponds to a cyclic $(v,k,1)$ difference family and to a strictly cyclic 2-$(v,k,1)$ design. An optimal $(v,k,1)$ OOC which is not perfect corresponds to a strictly cyclic partial 2-$(v,k,1)$ design. The blocks of this partial design correspond to the codewords and their translates. Each codeword and its translates correspond to one block orbit of length v under the cyclic automorphism of order v. Binary constant weight codes are related to $(v,k,1)$ OOCs too [32].

We illustrate the above definitions and relations by the following two examples.

Example 1.1. *A* $(61,5,1)$ *perfect OOC.*

optimal perfect $(61,5,1)$ *OOC = optimal perfect* $(61,5,1)$ *CPCW code =*
= cyclic $(61,5,1)$ *difference family = cyclic* 2-$(61,5,1)$ *design =*
= cyclic Steiner system $S(2,5,61)$

codeword	*covered nonzero differences — 60 of 60*
{0,1,3,13,34}	*1 2 3 10 12 13 21 27 28 30 31 33 34 40 48 49 51 58 59 60*
{0,4,9,23,45}	*4 5 9 14 16 19 20 22 23 25 36 38 39 41 42 45 47 52 56 57*
{0,6,17,24,32}	*6 7 8 11 15 17 18 24 26 29 32 35 37 43 44 46 50 53 54 55*

Example 1.2. *An optimal* $(44,5,1)$ *OOC.*

optimal $(44,5,1)$ *OOC = optimal* $(44,5,1)$ *CPCW code =*
= partial cyclic 2-$(44,5,1)$ *design*

codeword	*covered nonzero differences 40 of 43*
{0,1,3,28,40}	*1 2 3 4 5 7 12 16 17 19 25 27 28 32 37 39 40 41 42 43*
{0,6,14,24,35}	*6 8 9 10 11 14 15 18 20 21 23 24 26 29 30 33 34 35 36 38*

noncovered nonzero differences: $13, 22, 31$.

OOCs have various applications [8, 18], [21] and have been widely studied. A summary of the known results follows.

1.2 Known results and the present paper. Optimal $(v,k,1)$ OOCs are widely studied in many papers. Results obtained for other combinatorial objects like CPCW codes, cyclic difference families and cyclic combinatorial designs hold for the corresponding OOCs too.

The existence problem is completely solved for $(v,3,1)$ [10] and $(v,4,1)$ OOCs [38]. The complete investigation of the existence problem of optimal $(v,k,1)$ OOCs for $k \geq 5$ is still open. Existence of optimal OOCs with $k=5$ and 6 for particular values of v are obtained in [1, 7, 14, 29, 30, 34]. Some existence results follow from results about cyclic difference families and combinatorial designs [11, 15, 16, 24, 28]. Constructions

of optimal OOCs are presented in [9, 13, 23, 31, 32, 36, 35, 37]. The nonexistence of optimal $(v, 5, 1)$ OOCs with $v \equiv 22 \pmod{40}$ and of a $(62, 6, 1)$ OOC is proved in [12].

Classification results about optimal $(v, k, 1)$ OOCs or related to them combinatorial structures can be found in [2, 3, 4, 5, 6, 22, 20, 25, 26, 27], and [33].

The results obtained in these works show that when v grows, the number of nonequivalent codes becomes extremely big. This makes the classifications for the next bigger lengths practically unusable. In the present work we consider the first values of v where classification or nonexistence results are not known, but instead of complete classifications we find hundreds to thousands of multiplier nonequivalent optimal $(v, k, 1)$ OOCs such that each obtained code differs from the rest in many codewords. An access to these codes allows potential users to easily choose the most appropriate code for a given application with no need of any additional, sometimes complicated, mathematical computations. On the other hand, some of the constructed codes can be used with recursive constructions of OOCs of relatively big length which use OOCs with certain smaller parameters and possibly some additional properties [17, 23, 37]. It is also possible that the present results will reveal previously unnoticed dependencies that can possibly be used in the construction of new infinite families.

In the present paper we construct sets of multiplier nonequivalent optimal $(v, k, 1)$ OOCs with $k = 3, 5$, and 6 and $63 \leq v \leq 200$, $90 \leq v \leq 123$, and $106 \leq v \leq 121$ respectively. We do not consider $k = 4$ because this has been done in [6]. The investigation is computer-aided. Section 2 deals with the description of the implemented algorithm. A summary of the results is given in Section 3 and the codes themselves are available online at http://www.moi.math.bas.bg/ tsonka/(v,3,1)OOC.rar,
http://www.moi.math.bas.bg/ tsonka/(v,5,1)OOC.rar and
http://www.moi.math.bas.bg/ tsonka/(v,6,1)OOC.rar.

2 The construction algorithm. Our aim is to construct a set of optimal $(v, k, 1)$ OOCs with different properties which to be easily usable in possible applications or in future research. The classification algorithms from [2]-[6] obtain the codes in lexicographic order, and each code usually differs from the previous (next) one in only the last one or two codewords. Therefore it is not a good idea to just run the classification software for some time, and use the obtained codes for any possible purposes. That is why here we develop an algorithm A which is very similar to those used in [2]-[6], but instead of finding all OOCs with definite parameters it constructs a set of multiplier nonequivalent optimal OOCs which differ from one another in a relatively big number of codewords.

Similar to the classification algorithms, A is a back-track search algorithm implying minimality tests on some of the partial solutions. Before starting the search we construct an array L of all possibilities for codewords (namely all k-element subsets with the autocorrelation property) and consider them with respect to both lexicographic order and the action of the automorphisms of $\mathbb{Z}_v$. This makes it possible to define a lexicographic order on the solutions too, and to easily check by the minimality test if a solution can be mapped to a lexicographically smaller one by some of the automorphisms of $\mathbb{Z}_v$. If so, the solution is rejected. This way only multiplier nonequivalent codes are constructed.

Suppose that the algorithm A has chosen the first n codewords, and that there are m elements of the array L which can be added as $(n+1)$-st codeword. A classification algorithm would extend the partial solution by one codeword in all possible m ways,

but A extends it in at most e ways. For that purpose it uses only the lexicographically smallest e codewords because the minimality test will reject the code C if it is mapped by some automorphism of $\mathbb{Z}_v$ to a lexicographically smaller code C'. Therefore we have to be sure that C' is constructed. This may not be true if when there are more than e possibilities for the $n+1$-st codeword, only e out of them are chosen at random. That is why our algorithm extends the partial solution of n codewords using the lexicographically smallest e (out of all m) possibilities for the $(n+1)$-st codeword.

As a result at most e branches of the nodes of the search tree are considered for $n > 1$. Thus codes with all possibilities for the first and second codeword are constructed and each of the obtained codes differs in many codewords from most of the other codes.

3 Results. We use the algorithm A to construct sets of $(v, 3, 1)$ OOCs with $e = 1, 2$ or 3. Classification results for $k = 3$ are known for all $v \leq 61$ [4], and for $v = 67$ [25]. The number of the obtained multiplier nonequivalent $(v, 3, 1)$ OOCs is presented in Table 1 for all $v \leq 200$ for which neither classification [4, 25] nor nonexistence results [10] are known.

In the results available online the $(v, 3, 1)$ OOCs with length v are listed in the files E$e$oc_v_3_1_1.txt. For instance, the file E2oc_79_3_1_1.txt contains the $(79, 3, 1)$ OOCs obtained for $e = 2$. This is pointed out in the file too. It starts with the explanation: "These are NOT ALL codes with the upper parameters. The codes below are constructed by backtrack search, but only the first 2 possibilities for the n-th codeword $(n > 2)$ are considered".

For $k = 5$ and 6 we further restrict the search that the algorithm A performs by using only the first e_0 possibilities for the second codeword. The OOCs with length v and weight k are in the file Ee_0_$e$oc_v_k_1_1.txt. For instance the file E51_3oc_90_5_1_1.txt contains $(90, 5, 1)$ OOCs obtained for $e_0 = 51$ and $e = 3$.

Classification results for $k = 5$ are known for all $v \leq 89$ [4], and for $v = 101$ [25]. The number of the obtained multiplier nonequivalent $(v, 5, 1)$ OOCs is presented in Table 2 for all $v \leq 123$ for which neither classification [4, 25] nor nonexistence results [12] are known.

Classification results for $k = 6$ are known for all $v \leq 105$ [4], and for $v = 121$ [25]. The number of the obtained multiplier nonequivalent $(v, 6, 1)$ OOCs is presented in Table 3 for all $v \leq 121$ for which neither classification [4, 25] nor nonexistence results [12] are known.

Some of the constructed $(v, k, 1)$ OOCs are invariant under nontrivial automorphisms of $\mathbb{Z}_v$. In this case the corresponding partial designs have multiplier automorphisms. Information about them is presented in Table 4, where $Aut_{\mathbb{Z}_v}$ is the number of automorphisms of $\mathbb{Z}_v$, the total number of $(v, k, 1)$ OOCs with these parameters is given in column *codes* and the number of multiplier automorphisms is presented as $M : N$, where N is the number of OOCs which have M multiplier automorphisms.

4 Final remarks and open problems. The powerful parallel computers available nowadays allow to obtain classification results for lengths which have not been covered in previous works, but the extremely great number of codes makes these results difficult to use. That is why our aim in the present paper is to construct only a 'representative' part of the codes, namely codes which differ substantially from one another. We hope that the online availability of the constructed optimal $(v, k, 1)$ OOCs will make them usable

Table 1: Optimal $(v, 3, 1)$ OOCs with $63 \leq v \leq 200$

$e = 3$

length	size	codes
63	10	$\geq$362252
64	10	$\geq$530156
65	10	$\geq$1019787
66	10	$\geq$2491070
69	11	$\geq$978887
70	11	$\geq$1632062
71	11	$\geq$1587574
72	11	$\geq$9434672
73	12	$\geq$104647
74	12	$\geq$953899
75	12	$\geq$5107667
76	12	$\geq$3338259
77	12	$\geq$10048011

$e = 2$

length	size	codes
78	12	$\geq$889982
79	13	$\geq$11470
80	13	$\geq$193280
81	13	$\geq$359508
82	13	$\geq$456202
83	13	$\geq$358501
84	13	$\geq$2613409
85	14	$\geq$83589
87	14	$\geq$864447
88	14	$\geq$1938951
89	14	$\geq$826409
90	14	$\geq$8446453
91	15	$\geq$144426
93	15	$\geq$1777834
94	15	$\geq$1289924
95	15	$\geq$3951297

$e = 1$

length	size	codes
96	15	$\geq$1873
97	16	$\geq$6
98	16	$\geq$168
99	16	$\geq$321
100	16	$\geq$635
101	16	$\geq$278
102	16	$\geq$1216
103	17	$\geq$7
104	17	$\geq$210
105	17	$\geq$685
106	17	$\geq$498
107	17	$\geq$246
108	17	$\geq$2579
109	18	$\geq$15
111	18	$\geq$293
112	18	$\geq$1124
113	18	$\geq$270
114	18	$\geq$1803
115	19	$\geq$39
117	19	$\geq$515
118	19	$\geq$244
119	19	$\geq$729
120	19	$\geq$4714
121	20	$\geq$27
122	20	$\geq$102
123	20	$\geq$395
124	20	$\geq$330
125	20	$\geq$1048
126	20	$\geq$4816
127	21	$\geq$15
128	21	$\geq$183
129	21	$\geq$280
130	21	$\geq$1402
131	21	$\geq$297
132	21	$\geq$2588
133	22	$\geq$61
135	22	$\geq$1060
136	22	$\geq$1480
137	22	$\geq$261
138	22	$\geq$2858
139	23	$\geq$12
141	23	$\geq$448
142	23	$\geq$296
143	23	$\geq$1075
144	23	$\geq$6924
145	24	$\geq$22
146	24	$\geq$85
147	24	$\geq$737
148	24	$\geq$360
149	24	$\geq$249
150	24	$\geq$6049
151	25	$\geq$5
152	25	$\geq$243
153	25	$\geq$592
154	25	$\geq$2220
155	25	$\geq$1215
156	25	$\geq$3458
157	26	$\geq$7
159	26	$\geq$398
160	26	$\geq$2272
161	26	$\geq$1360
162	26	$\geq$7980
163	27	$\geq$4
165	27	$\geq$1655
166	27	$\geq$301
167	27	$\geq$241
168	27	$\geq$6792
169	28	$\geq$23
170	28	$\geq$443
171	28	$\geq$576
172	28	$\geq$562
173	28	$\geq$224
174	28	$\geq$3441
175	29	$\geq$117
176	29	$\geq$407
177	29	$\geq$443
178	29	$\geq$761
179	29	$\geq$223
180	29	$\geq$8280
181	30	$\geq$4
183	30	$\geq$622
184	30	$\geq$2102
185	30	$\geq$2206
186	30	$\geq$4707
187	31	$\geq$28
189	31	$\geq$1556
190	31	$\geq$1325
191	31	$\geq$227
192	31	$\geq$7820
193	32	$\geq$3
194	32	$\geq$110
195	32	$\geq$2128
196	32	$\geq$1476
197	32	$\geq$166
198	32	$\geq$8557
199	33	$\geq$4
200	33	$\geq$841

Table 2: Optimal $(v, 5, 1)$ OOCs with $90 \leq v \leq 123$ for $e_0 = 51$

$e = 3$

length	size	codes
90	4	$\geq$21372
91	4	$\geq$32407
92	4	$\geq$46949
93	4	$\geq$104572
94	4	$\geq$113907
95	4	$\geq$196781

length	size	codes
96	4	$\geq$406483
97	4	$\geq$302082
98	4	$\geq$613765
99	4	$\geq$916558
100	4	$\geq$1241082

length	size	codes
103	5	$\geq$72
104	5	$\geq$278
105	5	$\geq$1844
106	5	$\geq$1260
107	5	$\geq$1772

$e = 2$

length	size	codes
108	5	$\geq$5632
109	5	$\geq$6676
110	5	$\geq$18672
111	5	$\geq$33326
112	5	$\geq$45744
113	5	$\geq$52711

length	size	codes
114	5	$\geq$181952
115	5	$\geq$168511
116	5	$\geq$256721
117	5	$\geq$443632
118	5	$\geq$506751

length	size	codes
119	5	$\geq$612808
120	5	$\geq$1762705
121	6	$\geq$16
122	6	$\geq$330
123	6	$\geq$145

Table 3: Optimal $(v, 6, 1)$ OOCs with $106 \leq v \leq 120$ for $e_0 = 11$

$e = 3$

length	size	codes
106	3	$\geq$10980
107	3	$\geq$18664
108	3	$\geq$47543
109	3	$\geq$47604
110	3	$\geq$106081

length	size	codes
111	3	$\geq$172996
112	3	$\geq$217699
113	3	$\geq$236986
114	3	$\geq$655131
115	3	$\geq$583691

$e = 2$

length	size	codes
116	3	$\geq$693968
117	3	$\geq$1065289
118	3	$\geq$1143590

length	size	codes
119	3	$\geq$1218363
120	3	$\geq$1358001

Table 4: $(v, k, 1)$ OOCs invariant under nontrivial automorphisms of $\mathbb{Z}_v$

length	weight	codes	$\mathrm{Aut}_{\mathbb{Z}_v}$	Number of automorphisms:Number of codes
63	3	362252	36	1: 361991 2: 147 3: 81 6: 33
65	3	1019787	48	1: 1019767 3: 20
67	3	34709	66	1: 34311 3: 395 11: 2 33: 1
69	3	978887	44	1: 978824 2: 61 11: 1 22: 1
72	3	9434672	24	1: 9434366 2: 306
73	3	104647	72	1: 104071 3: 570 9: 6
74	3	953899	36	1: 953832 3: 65 9: 2
75	3	5107667	40	1: 5107637 2: 5 4: 5 5: 16 10: 2 20: 2
76	3	3338259	36	1: 3338194 3: 65
79	3	11470	78	1: 11364 3: 105 39: 1
80	3	193280	32	1: 193198 2: 74 4: 8
87	3	864447	56	1: 864346 2: 96 4: 2 7: 1 28: 2
91	3	144426	72	1: 143226 2: 24 3: 1160 6: 4 9: 8 12: 4
93	3	1777834	60	1: 1777497 2: 178 3: 138 5: 6 6: 10 10: 1 15: 3 30: 1
97	3	6	96	1: 5 3: 1
103	3	7	102	1: 6 3: 1
105	3	685	48	1: 683 3: 2
109	3	15	108	1: 14 3: 1
111	3	293	72	1: 292 2: 1
123	3	395	80	1: 394 2: 1
127	3	15	126	1: 14 3: 1
129	3	280	84	1: 279 2: 1
139	3	12	138	1: 11 3: 1
141	3	448	92	1: 447 2: 1
151	3	5	150	1: 4 3: 1
157	3	7	156	1: 6 3: 1
159	3	398	104	1: 397 2: 1
163	3	4	162	1: 3 3: 1
177	3	443	116	1: 442 2: 1
181	3	4	180	1: 3 3: 1
183	3	622	120	1: 621 2: 1
193	3	3	192	1: 2 3: 1
199	3	4	198	1: 3 3: 1
90	5	21372	24	1:21366 2: 6
91	5	32407	72	1: 32367 2: 4 3: 36
93	5	104572	60	1: 104401 3: 171
95	5	196781	72	1: 196634 2: 8 3: 139
96	5	406483	32	1: 406440 2: 43
99	5	916558	60	1: 916517 2: 41
101	5	8	100	1: 6 5: 2
104	5	278	48	1: 254 3: 24
105	5	1844	48	1: 1841 2: 1 4: 2
114	5	181952	36	1: 181924 3: 28
115	5	168511	88	1: 168472 2: 27 4: 12
119	5	612808	96	1: 612802 2: 6
120	5	1762705	32	1: 1762531 2: 154 4: 20
122	5	330	60	1: 262 3: 16 5: 52
123	5	145	80	1: 130 5: 15
109	6	47604	108	1: 47475 3: 129
111	6	172996	72	1: 172886 3: 108 9: 2
112	6	217699	48	1: 217582 2: 117
114	6	655131	36	1: 655041 3: 86 6: 1 9: 2 18: 1
117	6	1065289	72	1: 1064783 2: 258 3: 232 4: 4 6: 8 12: 4
119	6	1218363	96	1: 1218266 2: 91 4: 6

both in applications and in future research. Another approach might be to construct only the codes with certain properties important for particular applications. The full classification of the considered $(v, k, 1)$ OOCs remains an open problem.

Acknowledgments. The research that led to these results was carried out using the infrastructure purchased under the National Roadmap for RI, financially coordinated by the MES of the Republic of Bulgaria (grant No D01-98/26.06.2025).

REFERENCES.

[1] R.J.R. ABEL and M. BURATTI. Some progress on $(v, 4, 1)$ difference families and optical orthogonal codes. *Journal of Combinatorial Theory, Series A*, 106:59–75, 2004.

[2] T. BAICHEVA and S. TOPALOVA. Classification of optimal $(v, 4, 1)$ binary cyclically permutable constant weight codes and cyclic $S(2, 4, v)$ designs with $v \leq 76$. *Problems of Information Transmission*, 47(3):224–231, 2011.

[3] T. BAICHEVA and S. TOPALOVA. Classification results for $(v, k, 1)$ cyclic difference families with small parameters. In *International book series: Information Science and Computing*, number 25, pages 24–30. 2012.

[4] T. BAICHEVA and S. TOPALOVA. Classification of maximal optical orthogonal codes of weight 3 and small lengths. *Serdica Journal of Computing*, 9(1):83–92, 2015.

[5] T. BAICHEVA and S. TOPALOVA. Classification of optimal $(v, k, 1)$ binary cyclically permutable constant weight codes with $k = 5$, 6 and 7 and small lengths. *Designs Codes and Cryptography*, 87:365–374, 2019.

[6] T. BAICHEVA and S. TOPALOVA. An update on optimal $(v, 4, 1)$ binary cyclically permutable constant weight codes and cyclic 2-$(v, 4, 1)$ designs with small v. *Problems of Information Transmission*, 60(3):189–198, 2024.

[7] T. BAICHEVA and S. TOPALOVA. On the existence of optimal $(v, 5, 1)$ and $(v, 6, 1)$ binary cyclically permutable constant-weight codes. *Axioms*, 15(1):35, 2026.

[8] I.C.M. BIRD and A.D. KEEDWELL. Design and applications of optical orthogonal codes — a survey. *Bulletin of the Institute of Combinatorics and its Applications*, 11:21–44, 1994.

[9] S. BITAN and T. ETZION. Constructions for optimal constant weight cyclically permutable codes and difference families. *IEEE Transactions on Information Theory*, 41(1):77–87, 1992.

[10] E.F. BRICKELL and V. WEI. Optical orthogonal codes and cyclic block designs. *Congresus Numerantium*, 58:175–182, 1987.

[11] M. BURATTI and A. PASOTTI. Further progress on difference families with block size 4 or 5. *Designs Codes and Cryptography*, 56:1–20, 2010.

[12] M. BURATTI and D. R. STINSON. New results on modular Golomb rulers, optical orthogonal codes and related structures. *Ars Mathematica Contemporanea*, 1:1–27, 2020.

[13] Y. CHANG, R. FUJI-HARA, and Y. MIAO. Combinatorial constructions of optimal optical orthogonal codes with weight 4. *IEEE Transactions on Information Theory*, 49:1283–1292, 2003.

[14] Y. CHANG and L. JI. Optimal $(4up, 5, 1)$ optical orthogonal codes. *Journal of Combinatorial Designs*, 12:346–361, 2004.

[15] K. CHEN and L. ZHU. Existence of $(q, 6, 1)$ difference families with q a prime power. *Designs, Codes and Cryptography*, 15:167–173, 1998.

[16] K. CHEN and L. ZHU. Existence of $(q, k, 1)$ difference families with q a prime power and $k = 4, 5$. *Journal of Combinatorial Designs*, 7:21–30, 1999.

[17] W. CHU and S. W. GOLOMB. A new recursive construction for optical orthogonal codes. *IEEE Transactions on Information Theory*, 49:3072–3076, 2003.

[18] F.R.K. CHUNG, J.A. SALEHI, and V.K. WEI. Optical orthogonal codes: design, analysis and applications. *IEEE Transactions on Information Theory*, 35:595–604, 1989.

[19] C. COLBOURN and J. DINITZ, editors. *Handbook of Combinatorial Designs*. CRC Press, Boca Raton, FL.,USA, 2007.

[20] C. J. COLBOURN and M. J. COLBOURN. On cyclic Steiner systems $S(2, 6, 91)$. *Abstracts of papers presented to the American Mathematical Society*, 5(12):463, 1982.

[21] C.J. COLBOURN, J.H. DINITZ, and D.R. STINSON. Applications of combinatorial designs to communications, cryptography, and networking. In *Surveys in combinatorics*, pages 37–100. Cambridge University Press, 1999.

[22] M.J. COLBOURN and R.A. MATHON. On cyclic Steiner 2-designs. *Annals of Discrete Mathematics*, 7:215–253, 1980.
[23] R. FUJI-HARA and Y. MIAO. Optical orthogonal codes: their bounds and new optimal constructions. *IEEE Transactions on Information Theory*, 46:2396–2406, 2000.
[24] H. HANANI. Balanced incomplete block designs and related designs. *Discrete Mathematics*, 11:255–369, 1975.
[25] I. HETMAN, T. BAICHEVA, and S. TOPALOVA. Construction of $(v, k, 1)$ cyclic difference families with small parameters. *Journal of Algebra Combinatorics Discrete Structures and Applications*, 13(1):111–119, 2026.
[26] Z. JANKO and V. D. TONCHEV. Cyclic 2-(91, 6, 1) designs with multiplier automorphisms. *Discrete Mathematics*, 97:265–268, 1991.
[27] R. JULIAN, R. ABEL, and M. BURATTI. Difference families. In CH. COLBOURN and J. DINITZ, editors, *Handbook of Combinatorial Designs*, Discrete mathematics and its applications, pages 392–410. CRC Press, Boca Raton, FL., 2nd edition, 2007. ser. ed. K. Rosen.
[28] R. JULIAN, R. ABEL, S. COSTA, and N. FINIZIO. Directed-ordered whist tournaments and $(v, 5, 1)$ difference families: existence results and some new classes of Z-cyclic solutions. *Discrete Applied Mathematics*, 143:43–53, 2004.
[29] S. MA and Y. CHANG. A new class of optimal optical orthogonal codes with weight five. *IEEE Transactions on Information Theory*, 50:1848–1850, 2004.
[30] S. MA and Y. CHANG. Constructions of optimal optical orthogonal codes with weight five. *Journal of Combinatorial Designs*, 13:54–69, 2005.
[31] O. MORENO, Z. ZHANG, P. V. KUMAR, and V. A. ZINOVIEV. New constructions of optimal cyclically permutable constant weight codes. *IEEE Transactions on Information Theory*, 41(2):448–455, 1995.
[32] Q. A. NGUYEN, L. GYÖFRI, and J. L. MASSEY. Constructions of binary constant weight cyclic codes and cyclically permutable codes. *IEEE Transactions on Information Theory*, 38(3):940–949, 1992.
[33] COLIN REID and ALEX ROSA. Steiner systems $S(2, 4, v)$ — a survey. *The Electronic Journal of Combinatorics*:#DS18, 2010.
[34] Y. TANG and J. YIN. Combinatorial constructions for a class of optimal OOCs. *Science in China (A)*, 45:1268–1275, 2002.
[35] S. WANG, L. WANG, and J. WANG. A new class of optimal optical orthogonal codes with weight six. In *Proceedings of Seventh International Workshop of Signal Design and its Applications in Communications*, Bengaluru, India, 2015.
[36] X. WANG and Y. CHANG. Further results on $(v, 4, 1)$-perfect difference families. *Discrete Mathematics*, 310:1995–2006, 2010.
[37] J. YIN. Some combinatorial constructions for optical orthogonal codes. *Discrere Mathematics*, 185:201–219, 1998.
[38] C. ZHAO, Y. CHANG, and F. FENG. The existence of optimal $(v, 4, 1)$ optical orthogonal codes achieving the Johnson bound. *IEEE Transactions on Information Theory*, 70:8746–8757, 2024.

Tsonka Baicheva, Svetlana Topalova
Institute of Mathematics and Informatics
Bulgarian Academy of Sciences
78 Nikola Gabrovski Street, P.O. box 323
5000 Veliko Tarnovo, Bulgaria
e-mail: `tsonka@math.bas.bg, svetlana@math.bas.bg`

НОВИ ОПТИМАЛНИ $(v, k, 1)$ ОПТИЧНИ ОРТОГОНАЛНИ КОДОВЕ С $k = 3, 5, 6$

Цонка Байчева и Светлана Топалова

Абстракт

Известните класификации на оптимални оптични ортогонални кодове с малки k показват, че когато дължината на кода v нараства, броят на нееквивалентните кодове се увеличава много бързо. Това или прави пълната класификация за относително големи стойности на v невъзможна, или броят на получените кодове е толкова голям, че е много трудно да се избере сред тях код с необходимите свойства. Ето защо в настоящата работа не получаваме всички кодове с разглежданите параметри. Конструираме множества от нови оптимални $(v, k, 1)$ оптични ортогонални кодове с $k = 3, 5$ и 6 за относително малки стойности на дължините на кода v, за които не са известни резултати от класификацията. Кодовете във всеки от тези множества се различават един от друг по много кодови думи. Те могат да бъдат използвани в практически приложения, както и в по-нататъшни изследвания по темата.

Ключови думи: теория на кодирането, оптимален оптичен ортогонален код, двоичен константно тегловен циклично пермутационен код, циклични разностни фамилии, цикличен дизайн.

МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2026
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2026
Proceedings of the Fifty-Fifth Spring Conference
of the Union of Bulgarian Mathematicians
Tryavna, Bulgaria, April 5–9, 2026

VERIFYING THE COMPUTED WEIGHT DISTRIBUTION FOR THE BINARY REED–MULLER CODE R(4,9) [1]

Yuri Borissov and Miroslav Markov

Abstract

We revisit pivotal aspects of computing the weight distribution of the binary Reed–Muller code $R(4,9)$ and introduce a verification technique based on the Heninger–Rains–Sloane integrality congruences for Reed–Muller codes. The consistency checks fully confirm the correctness of the distribution obtained in our previous work: *"The weight distribution of the fourth-order Reed–Muller code of length 512"*, *Designs, Codes and Cryptography* **93**, 2487–2502 (2025).

2020 Mathematics Subject Classification: 94B70, 94B05, 68Q25.

Key words: binary Reed–Muller code, weight distribution, affine equivalence.

1 Introduction. Binary Reed–Muller codes are classical linear codes that admit efficient majority-logic decoding. However, general results on their weight structure are scarce: complete distributions are known for first- and second-order codes [15] and their duals (via the MacWilliams identities), and for arbitrary order for weights below $2d_{\min}$ [7].

The code $R(4,9)$ was historically among the smallest with unknown distribution [11]; recent work [2] determines its spectrum, renewing interest in this code, while the exact distribution requires substantial computation. In [12], we resolved this problem by applying the methodology described in D. V. Sarwate's Ph.D. thesis from 1973 [14], using newer results on the affine-equivalence classification of Boolean functions [10, 5]. Since the solution is computer-assisted, it is essential to employ rigorous verification procedures to confirm the correctness of the computed results. Here, we present a verification technique for those computations derived from specific theorems concerning the weight distribution of arbitrary Reed–Muller codes modulo certain powers of 2 [6].

We also briefly assess the goodness-of-fit of the Cusick–Cheon conjectured bounds [4] for estimating the number of balanced Boolean functions, by comparing them with the exact count of weight 256 codewords in $R(4,9)$ reported in [12].

The paper is organized as follows. In Section 2, we recall necessary background. Section 3 revisits key steps in the computation of the weight distribution of $R(4,9)$. Section 4 explains our verification technique. We conclude in Section 5.

[1] The research of the first author was partially supported by the Center of Excellence in Informatics and ICT established under the Grant No BG16RFPR002-1.014-0018, financed by the Research, Innovation and Digitalization for Smart Transformation Programme and co-financed by the European Union. The research of the second author has been partially supported by the the National Science Fund of Bulgaria under Grant KP-06-N82/5.

https://doi.org/10.55630/mem.2026.55.340-349

2 Preliminaries. For basic definitions and notations, we refer to [11]. To fix terminology, we recall the following standard notions.

Definition 2.1 (Weight distribution)**.** *Let C be a binary linear code of length n. Its weight distribution is the vector $\mathrm{W}(C) = (A_0, \ldots, A_n)$, where A_i is the number of codewords of Hamming weight i.*

Definition 2.2 (Weight enumerator)**.** *The single-variable weight enumerator of C is the polynomial in one indeterminate z*

$$\mathrm{W}[z; C] = \sum_{i=0}^{n} A_i z^i.$$

Definition 2.3 (Two-variable weight enumerator)**.** *For $\mathrm{W}(C) = (A_0, \ldots, A_n)$, the two-variable weight enumerator is*

$$\mathrm{W}_C(x, y) = \sum_{i=0}^{n} A_i x^i y^{n-i}.$$

Let $\mathcal{B}_m$ denote the set of Boolean functions in m variables; each $f \in \mathcal{B}_m$ corresponds to a binary vector of length $n = 2^m$ via its truth table.

Definition 2.4 (Reed–Muller codes)**.** *For $0 \le r \le m$, the r-th order binary Reed–Muller code $R(r, m)$ comprises those vectors of length $n = 2^m$ whose associated Boolean functions have algebraic degree at most r.*

We also use the general affine group $\mathrm{GA}(m, 2)$ acting on $\mathbb{F}_2^m$, where m is a positive integer and $\mathbb{F}_2 = \{0, 1\}$. In fact, $\mathrm{GA}(m, 2)$ is the group of automorphisms of $R(r, m)$ for $0 < r < m - 1$ [11, Ch. 13.9].

Affine equivalence. For $A \in \mathrm{GA}(m, 2)$ and $f \in \mathcal{B}_m$, let $(f \circ A)(x) = f(A(x))$. Cosets $C_1 = f_1 + R(r, m)$ and $C_2 = f_2 + R(r, m)$ are *affine equivalent* if $f_2 = f_1 \circ A$.

We list three standard facts used in this paper.

Fact 2.5. *The code $R(r, m)$ is a linear $[n, k, d]$ code with parameters*

$$n = 2^m, \qquad k = \sum_{i=0}^{r} \binom{m}{i}, \qquad d = 2^{m-r}.$$

In particular, the binary $R(4, 9)$ is a linear $[512, 256, 32]$ code.

Fact 2.6. *$R(s, 2s + 1)$ is doubly-even self-dual for $s \ge 1$. In particular, $R(4, 9)$ is a doubly-even self-dual code.*

And, finally the extensively used in this study.

Fact 2.7. *Affine-equivalent cosets of $R(r, m)$ have identical weight enumerators.*

3 Revisiting the computation for $R(4,9)$.

3.1 Theoretical basis. We employ two theorems stated in Chapter 5 of Sarwate's thesis [14, Thms. 5.12 and 5.13]. Let H_r^m denote the set of homogeneous polynomials (forms) in m binary variables of degree r, supplemented with the zero polynomial 0.

Theorem 3.1 ([14], Th. 5.12)**.** *For $0 \le r \le m$,*

$$\mathrm{W}\big[z; R(r+2,m+2)\big] = \sum_{p \in \mathsf{H}_{r+2}^{m+1}} \mathrm{W}^2\big[z;\, p + R(r+1,m+1)\big].$$

Theorem 3.2 ([14], Th. 5.13)**.** *If $p = e + f x_{m+1}$ with $e \in \mathsf{H}_{r+2}^m$ and $f \in \mathsf{H}_{r+1}^m$, then*

$$\mathrm{W}\big[z; C(p)\big] = \sum_{g \in \mathsf{H}_{r+1}^m} \mathrm{W}\big[z;\, e+g+R(r,m)\big] \cdot \mathrm{W}\big[z;\, e+f+g+R(r,m)\big],$$

where $C(p) = p + R(r+1, m+1)$.

In conjunction, we use the affine-equivalence classifications of two types of Boolean objects:

- quartic Boolean forms in eight variables due to Langevin and Leander [10];
- cosets of the quotient space $R(4,7)/R(2,7)$ due to Gillot and Langevin [5].

These classification results drastically reduce the computational burden: the former reduces the number of necessary weight-enumerator computations in Theorem 3.1 (implicitly) from $|\mathsf{H}_4^8| = 2^{\binom{8}{4}} = 2^{70}$ to a manageable 999 representatives; the latter simplifies the coset weight-enumerator computations in Theorem 3.2. Briefly, prior to implementing this machinery based on Fact 2.7, a substantial amount of pre-computation is required to create the orbits in $R(4,7)/R(2,7)$ and to compute the weight distributions of orbit representatives. Further work is also needed to resolve some incompatibilities between the two classifications; the interested reader is referred to [12, §3.2] for details.

3.2 Implementation. We employed HPC resources (dual Xeon Gold 5118, 48 cores; 256 GB RAM; NVIDIA V100 32 GB). Pre-computation took about 23 hours, and compressed storage plus in-RAM arrangement of orbit data required around 118 GB of memory in the worst case scenario; the generic computation took about 17 hours.

The voluminous table of the resulting distribution is presented in Table 3 of the Appendix for the sake of completeness.

4 Verification.

The correctness of the affine-equivalence classifications publicly available online [8, 9] is widely accepted in prior literature [5].

Since our methodology is computer-assisted, rigorous validation measures are indispensable to guarantee correctness and reliability of the computed results. But, before describing the verification tests employed here, we discuss the relationship between the self-duality of $R(4,9)$ and the weight distribution given in Table 3.

4.1 Self-duality. We start with the following well-known lemma whose proof is given for completeness.

Lemma 4.1. *A binary linear doubly-even code C of dimension equal to half the code length n is self-dual.*

Proof. Let $c_1, c_2 \in C$. Since C is doubly-even, the identity

$$\mathrm{wt}(c_1 + c_2) = \mathrm{wt}(c_1) + \mathrm{wt}(c_2) - 2\,\mathrm{wt}(c_1 * c_2)$$

reduces modulo 4 to $\mathrm{wt}(c_1 * c_2) \equiv 0 \pmod 2$. Here $c_1 * c_2$ denotes the binary vector of length n having 1s precisely where both c_1 and c_2 have 1s. Thus the inner product $c_1 \cdot c_2$ vanishes, i.e., $c_1 \perp c_2$. Hence C is self-orthogonal, and if $\dim(C) = n/2$ then C is self-dual. □

Now, we prove the following proposition.

Proposition 4.2. *Let C be a binary linear code of length 512 with the weight distribution reported in Table 3. Then C is doubly-even self-dual.*

Proof. Direct calculation gives $\sum_{i=0}^{512} A_i = 2^{256}$, implying $\dim(C) = 256$. So, the claim follows from the preceding lemma taking into account that all weights in Table 3 are divisible by 4. □

We recall a useful form of Gleason's theorem for doubly-even self-dual codes; see, e.g., [1, Th. 1, Part 2].

Theorem 4.3 (Gleason)**.** *Let C be a binary self-dual code of length n in which every weight is divisible by 4. Then n is divisible by 8, and the two-variable weight enumerator $\mathrm{W}_C(x, y)$ is a polynomial in*

$$f_1(x, y) = x^4 y^4 (x^4 - y^4)^4, \qquad f_2(x, y) = x^8 + 14x^4 y^4 + y^8,$$

that is,

$$\mathrm{W}_C(x, y) = \sum_{i,j} \omega_i \, f_1(x, y)^i \, f_2(x, y)^j, \qquad \text{where } n = 24i + 8j,$$

for suitable complex numbers ω_i.

In particular, for the intended distribution of $C = R(4, 9)$, we have:

Theorem 4.4 (Gleason for $R(4, 9)$)**.** *Let C be a binary linear code with weight distribution from Table 3 in the Appendix. Then there exist integers ω_i for $0 \le i \le 21$ such that*

$$\mathrm{W}_C(x, y) = \sum_{i=0}^{21} \omega_i \, f_1(x, y)^i \, f_2(x, y)^{64-3i}, \tag{1}$$

where $f_1(x, y), f_2(x, y)$ are defined above.

Table 1: Integer solutions ω_i (Gleason expansion) obtained from matching the smallest 22 weights $k \equiv 0 \pmod 4$.

i	ω_i
0	1
1	−896
2	366 400
3	−90 591 488
4	15 125 312 416
5	−1 804 090 983 680
6	158 633 285 104 000
7	−10 462 864 561 216 000
8	521 844 917 396 785 920
9	−19 703 740 374 727 094 272
10	560 488 125 281 758 654 464
11	−11 885 355 149 550 800 420 864
12	184 790 978 198 497 210 204 160
13	−2 057 511 108 351 137 030 602 752
14	15 886 111 690 015 316 194 099 200
15	−81 428 598 375 642 719 259 197 440
16	261 053 953 183 414 744 116 101 120
17	−481 398 485 705 822 986 116 792 320
18	451 352 262 788 439 851 856 297 984
19	−176 727 086 611 150 405 833 326 592
20	20 139 935 110 366 512 638 066 688
21	−279 475 807 551 445 268 430 848

Proof. For $n = 512$, Proposition 4.2 and Theorem 4.3 easily yield

$$\sum_{t=0}^{128} A_{4t}\, x^{4t} y^{512-4t} = \sum_{i=0}^{21} \omega_i\, f_1(x,y)^i\, f_2(x,y)^{64-3i}.$$

By comparing coefficients on both sides for the 22 smallest values of t we obtain a nonsingular linear (triangle) system in the unknowns ω_i, with free-coefficient vector $(A_0, A_4, \ldots, A_{84})$. Solving yields integer solutions (listed in Table 1); substituting back verifies the identity. □

Remark 4.5. *Note that one can get an equivalent form of (1) using instead of $f_1(x,y)$ the weight enumerator of the binary Golay code $g_1(x,y) = x^{24} + 759x^{16}y^8 + 2576x^{12}y^{12} + 759x^8y^{16} + y^{24}$ but then the coefficients obtained will be fractional [3].*

4.2 Heninger–Rains–Sloane tests. We use the following congruence due to Heninger–Rains–Sloane.

Theorem 4.6 ([6, Thm. 11]). *Let $W_{r,m}(z)$ denote the single-variable weight enumerator of the binary Reed–Muller code $R(r,m)$, with $0 \le r \le m$. Then*

$$W_{r,m}(z) \;\equiv\; \left(1 + z^{2^{m-r}}\right)^{2^r} \pmod{2^{r+1}}. \tag{2}$$

In particular, for $R(4,9)$ we obtain

$$W_{4,9}(z) \;\equiv\; f(z) \pmod{32}, \qquad f(z) \;:=\; \left(1 + z^{32}\right)^{16}. \tag{3}$$

This yields the following coefficient-level test:

- If k is not divisible by 32, then the coefficient A_k in the computed distribution must satisfy $A_k \equiv 0 \pmod{32}$.
- If $k = 32j$ with $0 \le j \le 16$, then $A_{32j} \equiv \binom{16}{j} \pmod{32}$.

Any valid weight distribution for $R(4,9)$ must satisfy these congruences. As seen from Table 2 in the Appendix, our computed distribution does meet them, providing a robust sanity check for its correctness.

Beyond congruence (2), Heninger, Rains and Sloane [6] prove the following recursive modulus relation (their Thm. 12):

$$W_{r,m+1}(z) \;\equiv\; W_{r,m}\!\left(z^2\right) \pmod{2^{m+1}}.$$

This yields a coefficient-level congruence between adjacent values of m for any fixed r.

Specializing to $r = 4$ and $m = 8$ gives the following strong consistency check for the weight distribution of $R(4,9)$:

$$W_{4,9}(z) \;\equiv\; W_{4,8}\!\left(z^2\right) \pmod{512}. \tag{4}$$

This can be applied whenever a reliable enumerator for $W_{4,8}(z)$ is available — for example, see the OEIS [13] entry A146976 for the $[256, 163, 16]$ Reed–Muller code.

A direct computation gives:

$$\begin{aligned} W_{4,8}\!\left(z^2\right) \pmod{512} = 1 &+ 304\,z^{32} + 256\,z^{48} + 248\,z^{64} + 256\,z^{80} + 400\,z^{96} + 28\,z^{128} \\ &+ 48\,z^{160} + 256\,z^{176} + 200\,z^{192} + 256\,z^{208} + 272\,z^{224} + 70\,z^{256} \\ &+ 272\,z^{288} + 256\,z^{304} + 200\,z^{320} + 256\,z^{336} + 48\,z^{352} + 28\,z^{384} \\ &+ 400\,z^{416} + 256\,z^{432} + 248\,z^{448} + 256\,z^{464} + 304\,z^{480} + z^{512}. \end{aligned}$$

Reducing modulo 512 the coefficients of the weight enumerator according to Table 3 yields exactly the same polynomial. This agreement confirms the congruence (4) and provides yet another strong consistency check for the computed distribution.

4.3 Cusick–Cheon approximation for balanced codewords in $R(4,9)$. Using the conjectured formulas provided in [4], we compute the lower and upper bounds for the number of codewords of weight 256 in the code $R(4,9)$. The actual computed value taken from Table 3 is positioned between the two bounds (both in decimal representation):

163241999092516819880381083582751276743897086608529035075014230421205629148 43,
163241999092516820004355772879343685230973976925480717778374838321083266745 02,
163321726512315142984410036687517745717705357656062517802592398845331002839 48.

It is noteworthy that the actual value coincides with the lower bound for the first 16 most significant digits, which provides yet another strong empirical support for the conjectured estimates in [4].

5 Conclusion. Recent advances in the structural classification of Boolean functions, together with modern high-performance computing, make Sarwate's recursive methodology [14] practical for computing the exact weight distribution of $R(4,9)$. To corroborate these computations, we employ a verification scheme based on the Heninger–Rains–Sloane congruences [6]. For $R(4,9)$, the resulting modulus tests provide independent consistency checks for the distribution reported in [12]. The congruence-based checks are applicable to any Reed–Muller code given a candidate weight enumerator; nevertheless, further validations always remain desirable.

Acknowledgments. We are grateful to Stefka Bouyuklieva for helpful discussion related to Lemma 1.

Appendix. Data tables: Heninger–Rains–Sloane test and complete weight distribution of $R(4,9)$.

Table 2: Heninger–Rains–Sloane congruence test according to (3). The third and fourth columns coincide.

k	$f(z)$	$f(z) \bmod 32$	$A_k \bmod 32$
0	1	1	1
32	16	16	16
64	120	24	24
96	560	16	16
128	1 820	28	28
160	4 368	16	16
192	8 008	8	8
224	11 440	16	16
256	12 870	6	6
288	11 440	16	16
320	8 008	8	8
352	4 368	16	16
384	1 820	28	28
416	560	16	16
448	120	24	24
480	16	16	16
512	1	1	1

Table 3: Weight Distribution of the [512,256,32] Reed–Muller code

Weight		Number of codewords
0	512	1
32	480	52955952
48	464	919315326720
56	456	271767121346560
60	452	860689275027456
64	448	89163020044002040
68	444	1777323352931696640
72	440	64959328938397057024
76	436	2094952122987829002240
80	432	86129855718211879936768
84	428	3718387228743293604986880
88	424	216407674400647746861465600
92	420	15958945395035022932054114304
96	416	1570964763114053055495174389136
100	412	207755244457303752035637154283520
104	408	34164336816436357675455725024378880
108	404	5992987676360073735151889707696128000
112	400	983217921810034263357552475089021004288
116	396	140881159168600922710983130625456163782656
120	392	17178463264607761296016540993629780705771520
124	388	1770270551281316280504947079180771901717872640
128	384	154198773988541804525321284585063483246993999900
132	380	113804373667128124744559508641773260684479892029 44
136	376	713793445298874211607839796879716106185715280216064
140	372	381616600344013129894862647690541247659597966711193 60
144	368	1744077996406613042017016863461234839306732612077058560
148	364	6832093649302361264113692814929677508406436591321481216 0
152	360	22997442048004658024533166375957838291089128020282067517 44
156	356	66674424868716978552789375387240003239187186349775851094016
160	352	16685597009641605873508056645831229244989283581517157330074 08
164	348	36117082274027891545154187373048131661136552390031364702863360
168	344	67748359898954710779361510124773951426962118474135604146110464 0
172	340	11032441933713096201663286389373184730113421621201515757397082112
176	336	15622509549761981330767923193778086142683556715677647652508417766 4
180	332	19266675322170971615767029917766543442504401756881968874572795084 80
184	328	20723534026876536792281002394151796205045793736436788802938336133120
188	324	19467144274183785293997555336377185623484125923840436555628706529280 0
192	320	15990449901813409988192707661615966056925120850571707914776940752826 32
196	316	11498415685246302189888474222781442491860129957714864173250891967627264
200	312	72459467570743603819378812718772497540870770484626494838959726267809792
204	308	40054993226393655422034298725822449978056412171282746567439522386149376 0
208	304	19440716119784239090594261981448498630646086750443974295489951777517324 80
212	300	82912118532783785444361572212137368354501088010426952045243530869735424 00
216	296	31095502600701130763682713427899390240950550846409105550583369693522427904
220	292	10262265243551021935495943795989790043448061584592614216685442619215865446 4
224	288	29820628130211072662300075044545013251288181062960712347847355409523781096 0
228	284	76339691963166668867675510699680388300388184743872831189110938463079759872 0
232	280	17224527761762198963574524869345731758046653437351694799190878995825516871 68
236	276	34267504602573059044705476415066421758676994653154784033541236313665086423 04
240	272	60131635994896839993127999354917771797727242479988779533784429205014179338 24
244	268	93095513202488540513326927728892454124955629888945474125328180450571164057 60
248	264	12718986044129514620716674156341900030463015021774940408815989741288144568320
252	260	15336997499945305387056357527918950456934399969250231086077675815418680311808
256		16324199909251682000435577287934368523097397692548071777837483832108326674502

REFERENCES.

[1] E. BERLEKAMP, F. J. MACWILLIAMS, and N. J. A. SLOANE. Gleason's theorem on self-dual codes. *IEEE Transactions on Information Theory*, 18:409–414, 1972.

[2] C. CARLET and P. SOLÉ. The weight spectrum of two families of Reed–Muller codes. *Discrete Mathematics*, 346(10):113568, 2023.

[3] P. CHARPIN. Open problems on cyclic codes. In V. S. PLESS and C. W. HUFFMAN, editors, *Handbook of Coding Theory*, pages 963–1063. Elsevier, 1998.

[4] T. W. CUSICK and Y. CHEON. Counting balanced boolean functions in n variables with bounded degree. *Experimental Mathematics*, 16(1):101–105, 2007.

[5] V. GILLOT and PH. LANGEVIN. Classification of some cosets of the Reed–Muller code. *Cryptography and Communications*:10.1007/s12095–023–00652–4, 2023.

[6] N. HENINGER, E. M. RAINS, and N. J. A. SLOANE. On the integrality of n-th roots of generating functions. *Journal of Combinatorial Theory, Series A*, 113:1732–1745, 2006.

[7] T. KASAMI and N. TOKURA. On the weight structure of Reed–Muller codes. *IEEE Transactions on Information Theory*, 16:752–759, 1970.

[8] PH. LANGEVIN. Classification of boolean quartic forms in eight variables, 2007. URL: `https://langevin.univ-tln.fr/project/quartics.html`.

[9] PH. LANGEVIN. Classification of $R(4,7)/R(2,7)$, 2012. URL: `https://langevin.univ-tln.fr/project/rm742/rm742.html`.

[10] PH. LANGEVIN and G. LEANDER. Classification of boolean quartic forms in eight variables. In B. PRENEEL and O. A. LOGACHEV, editors, *Boolean Functions in Cryptology and Information Security*, pages 139–147. IOS Press, 2008.

[11] F. J. MACWILLIAMS and N. J. A. SLOANE. *The Theory of Error-Correcting Codes*. North-Holland, Amsterdam, 1977.

[12] M. MARKOV and Y. BORISSOV. The weight distribution of the fourth-order Reed–Muller code of length 512. *Designs, Codes and Cryptography*, 93:2487–2502, 2025.

[13] OEIS FOUNDATION INC. The on-line encyclopedia of integer sequences. URL: `https://oeis.org/`. Last accessed 8 Jan. 2026.

[14] D. V. SARWATE. *Weight Enumeration of Reed–Muller Codes and Cosets*. PhD thesis, Department of Electrical Engineering, Princeton University, Princeton NJ, 1973. Advisors: E. R. Berlekamp and J. D. Ullman.

[15] N. J. A. SLOANE and E. R. BERLEKAMP. Weight enumerator for second-order Reed–Muller codes. *IEEE Transactions on Information Theory*, 16:745–751, 1970.

Yuri Borissov, Miroslav Markov
Institute of Mathematics and Informatics
Bulgarian Academy of Sciences
Acad. G. Bonchev Str., Bl. 8
1113 Sofia, Bulgaria
e-mail: `youri@math.bas.bg, miro@math.bas.bg`

ВЕРИФИКАЦИЯ НА ИЗЧИСЛЕНОТО РАЗПРЕДЕЛЕНИЕ НА ТЕГЛАТА ЗА ДВОИЧНИЯ КОД НА РИЙД-МАЛЕР R(4,9)

Юри Борисов и Мирослав Марков

Абстракт

В първата част на настоящата работа преразглеждаме основните етапи от пресмятането на разпределението на теглата на двоичния код на Рийд-Малер $R(4,9)$, представено в нашата предходна статия "The Weight Distribution of the Fourth-Order Reed–Muller Code of Length 512", Designs, Codes and Cryptography 93, 2487-2502. Във втората част въвеждаме техника за проверка, основана на целочислени сравнения, предложени от Хенингер, Рейнс и Слоун, която е приложима към кодовете от тази фамилия. Показваме, че този тип проверки напълно потвърждават коректността на полученото разпределение на теглата.

Ключови думи: двоичен код на Рийд-Малер, разпределение на теглата, афинна еквивалентност.

МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2026
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2026
Proceedings of the Fifty-Fifth Spring Conference
of the Union of Bulgarian Mathematicians
Tryavna, Bulgaria, April 5–9, 2026

ON MAXIMUM DISTANCE SEPARABLE AND COMPLETELY REGULAR CODES [1]

J. Borges, J. Rifà, and V. A. Zinoviev

Abstract

We investigate when a maximum distance separable (MDS) code over $\mathbb{F}_q$ is also completely regular (CR). For lengths $n = q + 1$ and $n = q + 2$ we provide a complete classification of the MDS codes that are CR or at least uniformly packed in the wide sense (UPWS). For the more restricted case $n \leq q$ with $q \leq 5$ we obtain a full classification (up to equivalence) of all nontrivial MDS codes: there are none for $q = 2$; only the ternary Hamming code for $q = 3$; four nontrivial families for $q = 4$; and exactly six linear MDS codes for $q = 5$ (three of which are CR and one admits a self-dual version). Additionally, we close two gaps left open in a previous classification of self-dual CR codes with covering radius $\rho \leq 3$: we precisely determine over which finite fields the MDS self-dual completely regular codes with parameters $[2, 1, 2]_q$ and $[4, 2, 3]_q$ exist.

2020 Mathematics Subject Classification: 94B60, 94B25.

Key words: maximum distance separable codes, completely regular codes.

1 Introduction. Let $\mathbb{F}_q$ denote the finite field of order q, where q is a prime power, and let $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$. Let C be a linear $[n, k, d]_q$ *code* with $0 < k < n$.

For any $\mathbf{v} \in \mathbb{F}_q^n$ its *distance* to the code C is $d(\mathbf{v}, C) = \min\{d(\mathbf{v}, \mathbf{x}) \mid \mathbf{x} \in C\}$. The *external distance* of C (see [7]) is the number s of nonzero weights in $C^\perp$. The *packing radius* of C is $e = \lfloor (d-1)/2 \rfloor$ and the *covering radius* is $\rho = \max_{\mathbf{v} \in \mathbb{F}_q^n} \{d(\mathbf{v}, C)\}$. Clearly $e \leq \rho$, with equality if and only if C is perfect. It is well known that any nontrivial perfect code (with more than two codewords) satisfies $e \leq 3$ [19, 20].

Definition 1.1 ([7])**.** *A code C is* completely regular *(CR) if for any $\mathbf{v} \in \mathbb{F}_q^n$ and any $t \in \{0, \ldots, n\}$, the value $B_{\mathbf{v},t} = |\{\mathbf{x} \in C \mid d(\mathbf{v}, \mathbf{x}) = t\}|$ depends only on t and $d(\mathbf{v}, C)$.*

[1]This work has been partially supported by the Spanish Ministerio de Ciencia e Innovación under Grants PID2022-137924NB-I00 (AEI/FEDER UE), RED2022-134306-T, and also by the Catalan AGAUR Grant 2021SGR-00643. The research of the third author of the paper was carried out at the Institute for Information Transmission Problems of the Russian Academy of Sciences within the program of fundamental research on the topic "Mathematical Foundations of the Theory of Error-Correcting Codes" and was also partly supported by the Higher School of Modern Mathematics MIPT, Moscow College of Physics and Technology, 1 Klimentovskiy per., Moscow, Russia.

https://doi.org/10.55630/mem.2026.55.350-356

For a more detailed description and basic properties of CR codes over finite fields, see [5, 6], or [15, Chap. 2], for example.

A more general class of codes is the class of uniformly packed codes in the wide sense [2].

Definition 1.2 ([2]). *A code $C \subseteq \mathbb{F}_q^n$ with covering radius ρ is* uniformly packed in the wide sense *(UPWS) if there exist rational numbers $\beta_0, \ldots, \beta_\rho$ such that*

$$\sum_{i=0}^{\rho} \beta_i B_{\mathbf{x},i} = 1, \tag{1}$$

for any $\mathbf{x} \in \mathbb{F}_q^n$. The numbers $\beta_0, \ldots, \beta_\rho$ are called the packing coefficients.

If C is a $[n, k, d]_q$ code, the Singleton bound [16] establishes that $d \leq n - k + 1$. If C attains equality, then C is a *maximum distance separable* (MDS) code.

The Griesmer bound [10, 18] is $n \geq \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil$, $(k \geq 1)$. If C attains equality, then C is a *Griesmer* code.

In this paper we study the possible parameters of MDS codes (which are also Griesmer codes) over $\mathbb{F}_q$. For length $n = q + 1$ and $n = q + 2$ we give a complete classification of the MDS codes that are completely regular or at least uniformly packed in the wide sense. For $q \leq 5$, we obtain a full classification (up to equivalence) of all nontrivial MDS codes. For $q = 2$, as is well known, there are only trivial cases. For $q = 3$, there is only one nontrivial case, which is a self-dual Hamming code. For $q = 4$, the nontrivial cases are a Hamming code, its dual code, a self-dual code, and the so-called hexacode. The case $q = 5$ is the most interesting. We determine that there are 6 nontrivial such codes over $\mathbb{F}_5$, up to equivalence. Three of them are CR codes. In addition, we point out in which cases such codes are self-dual. Moreover, we specify exactly in which finite fields the MDS codes with parameters $[2, 1, 2]_q$ and $[4, 2, 3]_q$ are also self-dual. Such codes are completely regular as stated in [6].

The main conjecture on MDS codes is the following

Conjecture 1.3. *If C is a nontrivial* MDS $[n, k, d]_q$ *code ($2 \leq k \leq n-2$), then $n \leq q+1$ unless q is even and $k = 3$ or $k = q - 1$, in which case $n \leq q + 2$.*

This conjecture was first considered by Segre [13] and is proven for a large number of cases. For our purposes, the following case, proven in [1] is useful.

Proposition 1.4. *If C is an* MDS $[n, k, d]_p$ *code with p prime and $2 \leq k \leq n - 2$, then $n \leq p + 1$.*

2 Preliminary results. The next result can be derived from Remark 5.13 in [12].

Proposition 2.1. *Let q be an odd prime power. Then -1 is a square in $\mathbb{F}_q$ if and only if $q \equiv 1 \pmod 4$.*

Recall that the quadratic character χ of $\mathbb{F}_q$ is defined as $\chi(a) = 1$ if a is a square, and $\chi(a) = -1$ if a is not ($a \in \mathbb{F}_q^*$). The next result is Lemma 6.24 in [12].

Proposition 2.2. *Let q be an odd prime power and $t, a_1, a_2 \in \mathbb{F}_q^*$. The equation*

$$a_1 x_1^2 + a_2 x_2^2 = t \tag{2}$$

has exactly $q - \chi(-a_1 a_2)$ solutions, where χ is the quadratic character of $\mathbb{F}_q$.

In [6] it is stated that any $[4, 2, 3]_q$ code is CR and taking a generator matrix of the form

$$G = \begin{pmatrix} 1 & 0 & \alpha & \beta \\ 0 & \xi & \beta & -\alpha \end{pmatrix}, \tag{3}$$

where $\alpha, \beta \in \mathbb{F}_q^*$, such code is also self-dual if $1 + \alpha^2 + \beta^2 = 0$ and $\xi^2 = 1$. But in [6] it is not specified in which finite fields these conditions can be satisfied. By using Proposition 2.2, we can precise such finite fields.

Corollary 2.3. *A self-dual $[4, 2, 3]_q$ code exists if and only if $q \notin \{2, 5\}$.*

For completely regular codes, we will use the following properties.

Lemma 2.4. *Let C be a linear code with minimum distance d, covering radius ρ, packing radius e and external distance s.*

(i) $\rho \leq s$ *[7].*

(ii) If $d \geq 2s - 1$*, then C is* CR *[7].*

(iii) $\rho = s$ *if and only if C is* UPWS *[3].*

(iv) If C is CR*, then* $\rho = s$ *[17].*

(v) If C is UPWS *and* $\rho = e + 1$*, then C is* CR *[9, 14].*

Note that, by (iii) and (iv), a CR code is always a UPWS code.

The only self-dual perfect code is the ternary Hamming $[4, 2, 3]_3$ code (see, for example, [6, Lemma 13]). Since a Hamming code has parameters

$$[n = (q^m - 1)/(q - 1), n - m, 3]_q,$$

it is an MDS code if and only if $m = 2$. In such case, the parameters are $[q + 1, q - 1, 3]_q$ and the dual simplex code has parameters $[q + 1, 2, q]_q$. Since a simplex code has only one nonzero weight, Hamming codes have external distance $s = 1$. Hence a Hamming code is CR by Lemma 2.4 (ii).

The following equivalence is easy to see, but not usually mentioned.

Proposition 2.5. *Let C be an $[n, k, d]_q$ code with $k \geq 2$. Then C is an* MDS *code if and only if C is a Griesmer code and $d \leq q$.*

All the following results on MDS codes can be found in [11, Sect. 7.4].

Proposition 2.6. *Let C be an* MDS *$[n, k, d]_q$.*

(i) $C^\perp$ is MDS*.*

(ii) The number of minimum weight codewords in C (i.e. codewords of weight d) is $A_d = \binom{n}{d}(q-1)$.

(iii) If $2 \le k \le n-2$, then $k \le \min\{n-2, q-1\}$ and $n \le 2(q-1)$.

In [8], the number of weights of MDS codes is determined.

Proposition 2.7 ([8])**.** *Let C be an* MDS *$[n,k,d]_q$ code and let s' be the number of nonzero weights of C.*

(i) If C is an $[n, n-1, 2]_2$ code with $n > 2$, then $s' = \lfloor n/2 \rfloor \neq k$.

(ii) If C is a $[q+1, 2, q]_q$ code, then $s' = 1$.

(iii) If C is a $[2^m+2, 3, 2^m]_{2^m}$ code, then $s' = 2$.

In all other cases $s' = k$, assuming that Conjecture 1.3 is true.

3 Trivial MDS **codes.** Trivial MDS $[n,k,d]_q$ codes are those with $k = 1$ or $k \ge n-1$.

For $k = 1$, we have the MDS repetition codes C_R with parameters $[n,1,n]_q$. Such codes and their duals, the $[n, n-1, 2]_q$ codes, are CR (by Lemma 2.4 (ii), since the codes C_R have just one nonzero weight). For $q = 2$, C_R codes have covering radius $\rho = \lfloor n/2 \rfloor$ (see [4, Thm. 1]) and identical external distance $s = \lfloor n/2 \rfloor$ by Proposition 2.7. Hence, binary C_R codes are UPWS by Lemma 2.4 (iii). Moreover, since the packing radius is $e = \lfloor (n-1)/2 \rfloor$, we have that $e = \rho$ if n is odd, and $e+1 = \rho$ if n is even. Therefore, C_R is a perfect code if n is odd, and a quasi-perfect UPWS code if n is even. In any case, C_R is a CR code by Lemma 2.4. For $q > 2$ and $n > 2$, we have $\rho = n - \lceil n/q \rceil$ (see [4, Thm. 1]) and the external distance is $s = n-1$ (Proposition 2.7). Hence, C_R is UPWS if and only if $q \ge n$.

Note that if a C_R code is self-dual then $n = 2$. In such case, the codes $[2,1,2]_q$ are CR. Take a generator matrix $G = (1 \;\; \alpha)$ for a $[2,1,2]_q$ C_R code. Then C_R is self-dual if and only if $\alpha^2 = -1$. In fact, these codes or direct sums of them are the only self-dual CR codes with $d \le 2$ (see [6, Thm. 36(i)]). However, in [6] the finite fields where such codes exist are not specified. As a direct consequence of Proposition 2.1 we can establish the following result.

Theorem 3.1. *Let C be a self-dual* CR *$[n,k,d]_q$ code. If $d \le 2$, then C is necessarily an* MDS *$[2,1,2]_q$ code, or a direct sum of j codes with these parameters (and C is not* MDS *for $j > 1$). Such codes exist if and only if q is even or $q \equiv 1 \pmod 4$.*

4 Nontrivial MDS **codes.** Nontrivial MDS $[n,k,d]_q$ codes are those with $2 \le k \le n-2$. Assuming that the MDS *conjecture* (Conjecture 1.3) is true, we have that $n \le q+1$ except in some exceptional cases where $n = q+2$. We start with these extremal cases.

According to Conjecture 1.3, a nontrivial MDS code of length $n = q+2$ is a $[2^m + 2, 3, 2^m]_{2^m}$ code or a $[2^m+2, 2^m-1, 4]_{2^m}$ code, where $m > 1$.

Theorem 4.1. *Let C be an* MDS *$[q+2, k, d]_q$ code, where $q = 2^m$ and $m > 1$.*

(i) If C is an MDS *$[2^m+2, 3, 2^m]_{2^m}$ code with odd m, then C is not* UPWS *(and so, not* CR*).*

(ii) If C is an MDS $[2^m+2, 2^m-1, 4]_{2^m}$ *code, then C is* CR.

For $n = q+1$ we have MDS codes with parameters $[q+1, k, q-k+2]_q$. We start with the particular case $k = 2$.

Proposition 4.2. *Let C be an* MDS $[q+1, 2, q]_q$ *code.*

(i) If q is odd, then C is UPWS *and* CR *if and only if $q = 3$.*

(ii) If q is even, then C is UPWS. *For $q = 2^2$, C is* CR. *For $q = 2^3$, C is not* CR.

Now, we have the following strong result for any $k \geq 2$.

Theorem 4.3. *If C is a nontrivial* MDS $[q+1, k, q-k+2]_q$ *code, then C is not* UPWS *(and so not* CR*) with the following exceptions:*

(i) $k = q-1$, in which case C is a Hamming perfect and CR *code.*

(ii) $k = 2$ with q even or $q = 3$, in which case C is UPWS. *For $q = 3$, C is also* CR.

(iii) $k = q-2$ with q even, in which case C is UPWS. *Moreover, for any $m > 1$, there exists a* CR $[q+1, q-2, 4]_q$ *code, where $q = 2^m$.*

For $n \leq q$, we begin by establishing the following result.

Theorem 4.4. *If C is an* MDS $[n, k, d]_q$ *code with $n \leq q$, then C is* UPWS.

In general, it seems hard to determine in which cases an MDS code C is also CR. However, for small fields we may consider some particular cases.

It is well known that all binary MDS codes are trivial. For $q = 3$, we have $n \leq 4$, by Proposition 2.6 (iii). Hence, we have the only nontrivial case of $[4, 2, 3]_3$ codes which are the self-dual CR Hamming ternary codes. If $q = 4$ then, by Proposition 2.6 (iii), we have $n \leq 6$. So, we have the possible parameters $[6, 4, 3]_4$, $[6, 3, 4]_4$, $[6, 2, 5]_4$, $[5, 3, 3]_4$, $[5, 2, 4]_4$ and $[4, 2, 3]_4$. The case of a $[6, 3, 4]_4$ code corresponds to the well-known two-weight *hexacode* (see, e.g., [11, p. 383]). Such code is CR by Lemma 2.4 (ii) since $s = 2$. In fact, it is a particular case of Theorem 4.1 (ii). The other two cases with $n = 6$ can be discarded after the following result.

Lemma 4.5. *There do not exist codes with parameters $[6, 4, 3]_4$ or $[6, 2, 5]_4$.*

For the remaining cases, note that a $[5, 3, 3]_4$ code is a Hamming code and a $[5, 2, 4]_4$ code is the corresponding simplex dual. Finally, a $[4, 2, 3]_4$ code exists and it is CR. In fact, any $[4, 2, 3]_q$ code is CR by Lemma 2.4 since $s \leq 2$ (see also Proposition 23 in [6]). By Corollary 2.3 a $[4, 2, 3]_4$ code is self-dual taking a generator matrix

$$G = \begin{pmatrix} 1 & 0 & \alpha & \alpha^2 \\ 0 & 1 & \alpha^2 & \alpha \end{pmatrix},$$

where α is a primitive element in $\mathbb{F}_4$.

The next smallest interesting finite field where to study MDS codes is $\mathbb{F}_5$. Now, we determine the possible parameters for nontrivial MDS codes over $\mathbb{F}_5$. Since Conjecture 1.3 is proven for prime fields, and applying Proposition 2.6, we only have to consider the cases: $(n, k) \in \{(6, 4), (6, 3), (6, 2), (5, 3), (5, 2), (4, 2)\}$.

Theorem 4.6. *If C is a nontrivial* MDS $[n,k,d]_5$ *code, then C is one of the following codes, up to equivalence:*

(i) A CR $[6,4,3]_5$ *code or its dual* $[6,2,5]_5$ *which is not* UPWS.

(ii) A $[6,3,4]_5$ *code, which is not* UPWS. *A self-dual version of such code exists.*

(iii) A CR $[5,3,3]_5$ *code or its dual* $[5,2,4]_5$ *which is* UPWS.

(iv) A $[4,2,3]_5$ *code which is* CR *and not self-dual.*

5 Summary. In summary we have found the following infinite families of MDS codes which are CR codes:

(i) The trivial $[n,n-1,2]_q$ codes for any n and q, and the $[n,1,n]_2$ codes.

(ii) Any $[2^m+2,2^m-1,4]_{2^m}$ code for $m>0$.

(iii) The Hamming $[q+1,q-1,3]_q$ codes for any q.

(iv) The $[2^m+1,2^m-2,4]_{2^m}$ codes equivalent to doubly-extended Reed-Solomon codes, for any $m>1$.

In addition, for $n \leq q$, we have the sporadic codes (not included above) with parameters: $[4,2,3]_4$, the punctured code of a $[5,2,4]_4$ CR code (item (iv) above, for $m=2$); $[5,3,3]_5$ (see Theorem 4.6 (iii)); and $[4,2,3]_5$ (see Theorem 4.6 (iv)).

REFERENCES.

[1] S. BALL. On sets of vectors of a finite vector space in which every subset of basis size is a basis. *J. Eur. Math. Soc.*, 14:733–748, 2012.

[2] L. A. BASSALYGO, G. V. ZAITSEV, and V. A. ZINOVIEV. Uniformly packed codes. *Problems Inform. Transmiss.*, 10(1):9–14, 1974.

[3] L. A. BASSALYGO and V. A. ZINOVIEV. A note on uniformly packed codes. *Problems Inform. Transmiss.*, 13(3):22–25, 1977.

[4] M. C. BHANDARI and C. DURAIRAJAN. On the covering radius of simplex codes. *Journal of Discrete Mathematical Sciences and Cryptography*, 6:59–69, 2003.

[5] J. BORGES, J. RIFÀ, and V. A. ZINOVIEV. On completely regular codes. *Problems Inform. Transmiss.*, 55(1):1–45, 2019.

[6] J. BORGES and V. A. ZINOVIEV. On self-dual completely regular codes with covering radius $\rho \leq 3$. *Finite Fields and their Applications*, 105:102617, 2025.

[7] P. DELSARTE. An Algebraic Approach to the Association Schemes in Coding Theory. Technical report 10, Philips Res. Rep. Suppl., 1973.

[8] M. F. EZERMAN, M. GRASSL, and P. SOLÉ. The weights in MDS codes. *IEEE Trans. Inform. Theory*, IT-57:392–396, 2011.

[9] J. M. GOETHALS and H. C. A. VAN TILBORG. Uniformly packed codes. *Philips Res.*, 30:9–36, 1975.

[10] J. H. GRIESMER. A bound for error-correcting codes. *IBM J. Res. Develop.*, 4:532–542, 1960.

[11] W. C. HUFFMAN and V. PLESS. *Fundamentals of error-correcting codes*. Cambridge Univ. Press, New York, 2003.

[12] RUDOLF LIDL and HARALD NIEDERREITER. *Finite fields*, number 20. Cambridge university press, 1997.

[13] B. SEGRE. Curve razionali normali ek-archi negli spazi finiti. *Ann. Mat. Pur. Appl.*, 39(1):357–379, 1955.

[14] N. V. SEMAKOV, V. A. ZINOVIEV, and G. V. ZAITZEV. Uniformly packed codes. *Problems Inform. Transmiss.*, 7:38–50, 1971.

[15] M. SHI and P. SOLÉ, editors. *Completely Regular Codes in Distance Regular Graphs*. CRC Press, Boca Raton FL, 2025.
[16] R. C. SINGLETON. Maximum distance q-ary codes. *IEEE Trans. Inform. Theory*, IT-10:116–118, 1964.
[17] P. SOLÉ. Completely regular codes and completely transitive codes. *Discrete Maths.*, 81:193–201, 1990.
[18] G. SOLOMON and J. J. STIFFLER. Algebraically punctured cyclic codes. *Inform. and Control*, 8:170–179, 1965.
[19] A. TIETÄVÄINEN. On the nonexistence of perfect codes over finite fields. *SIAM J. Appl. Math.*, 24(1):88–96, 1973.
[20] V. A. ZINOVIEV and V. K. LEONTIEV. On non-existence of perfect codes over Galois fields. *Probl. Upravlen. Teor. Inform.*, 2(2):123–132, 1973. English translation in Probl. Control Inf. Theory, vol. 2, no. 2, pp. 16–24, 1973.

Josep Rifà, Joaquim Borges
Department of Information and Communications Engineering
Universitat Autònoma de Barcelona
08193 Bellaterra (Barcelona), Spain
e-mail: josep.rifa@uab.cat, joaquim.borges@uab.cat

Victor Alexandrovich Zinoviev
A.A. Kharkevich Institute for Information Transmission Problems
Russian Academy of Sciences
Bol'shoi Karetnyi 19, Moscow, Russia
Russia and Higher School of Modern
Mathematics of the Moscow College of Physics and Technology in Dolgoprudny,
1 Klimentovskiy per., Moscow, Russia
e-mail: vazinov@iitp.ru

ЗА МАКСИМАЛНО РАЗДАЛЕЧИМИ И НАПЪЛНО РЕГУЛЯРНИ КОДОВЕ

J. Borges, J. Rifà, and V. A. Zinoviev

Абстракт

Изследваме кога един максимално раздалечим (MDS) код над $\mathbb{F}_q$ е също и напълно регулярен (CR). За дължини $n = q + 1$ и $n = q + 2$ даваме пълна класификация на MDS кодовете, които са CR или поне равномерно опаковани в широк смисъл (UPWS). За по-ограничения случай $n \leq q$ при $q \leq 5$ получаваме пълна класификация (с точност до еквивалентност) на всички нетривиални MDS кодове: няма такива за $q = 2$; само троичният код на Хеминг за $q = 3$; четири нетривиални семейства за $q = 4$; и точно шест линейни MDS кода за $q = 5$ (три от които са CR, а един допуска самодуална версия). Освен това запълваме две празнини, оставени в предишна класификация на самодуални CR кодове с радиус на покритие $\rho \leq 3$: точно определяме над кои крайни полета съществуват MDS самодуални напълно регулярни кодове с параметри $[2, 1, 2]_q$ и $[4, 2, 3]_q$.

Ключови думи: максимално раздалечим код, напълно регулярен код.

МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2026
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2026
Proceedings of the Fifty-Fifth Spring Conference
of the Union of Bulgarian Mathematicians
Tryavna, Bulgaria, April 5–9, 2026

ON CYCLIC INVARIANTS OF THE FREE ASSOCIATIVE ALGEBRA [1]

S. Boumova and V. Drensky

Abstract

Let $K\langle X_d\rangle$ be the free associative algebra of rank $d \geq 2$ over a field K. Lane in 1976 and Kharchenko in 1978 proved that the algebra of invariants $K\langle X_d\rangle^G$ is free for any subgroup $G \leq \mathrm{GL}_d(K)$ and any field K. Later, Kharchenko introduced an additional action of the symmetric group $\mathrm{Sym}(n)$ on the homogeneous component of degree n of $K\langle X_d\rangle$, given by permuting the positions of the variables. This equips $K\langle X_d\rangle$ with the structure of a $(K\langle X_d\rangle, \circ)$-$S$-algebra. Then Koryukin showed that the algebra of invariants $K\langle X_d\rangle^G$ is finitely generated for every reductive group G with respect to this action.

In our paper we study the algebra $K\langle x_1, \ldots, x_d\rangle^{C_d}$ of invariants of the cyclic group C_d, $d \geq 2$, where K is an arbitrary field of characteristic 0. We compute the Hilbert series of $K\langle x_1, \ldots, x_d\rangle^{C_d}$. When $K = \mathbb{C}$ we find a vector space basis of $\mathbb{C}\langle x_1, \ldots, x_d\rangle^{C_d}$ and explicitly describe the generators of $\mathbb{C}\langle x_1, \ldots, x_d\rangle^{C_d}$ as a free algebra. Moreover, we describe a finite generating set for the S-algebra $(\mathbb{C}\langle x_1, \ldots, x_d\rangle^{C_d}, \circ)$. We also transfer the results for $K = \mathbb{C}$ to the case of an arbitrary field of characteristic 0 for the S-algebra $(K\langle x_1, x_2, x_3\rangle^{C_3}, \circ)$ and find a minimal generating set for it as an S-algebra.

2020 Mathematics Subject Classification: 13A50, 15A72, 16S10, 16W22.

Key words: classical invariant theory, noncommutative invariant theory, cyclic invariants, action of Kharchenko–Koryukin.

1 Introduction. Let K be an arbitrary field of characteristic zero and let $K[X_d] = K[x_1, \ldots, x_d]$ be the d-generated polynomial algebra (the free commutative associative unital algebra of rank $d > 1$) over K. Classical invariant theory studies the algebra of invariants $K[X_d]^G$ which consists of all polynomials invariant under the action of a subgroup G of the general linear group $\mathrm{GL}_d(K)$.

The origins of the theory can be found in the work of Lagrange in the 1770s and Gauss in 1801. In his *Méchanique analytique* [15] Lagrange considered the problem of the transformation of homogeneous polynomials by linear substitutions of the variables. In

[1] The first named author was partially supported by the European Union-NextGenerationEU, through the National Recovery and Resilience Plan of the Republic of Bulgaria, Project No BG-RRP-2.004-0008-C01.

https://doi.org/10.55630/mem.2026.55.357-369

Disquisitiones Arithmeticae [8] Gauss studied the representation of integers by quadratic binary forms and used the discriminant to distinguish nonequivalent forms.

But it is accepted that the real invariant theory began in the 1840s with works by George Boole in England and by Otto Hesse in Germany. See Corry [4] and Wolfson [27] for details and references. For the history of the early invariant theory see also the survey by Meyer [17] from 1892, the books by Klein [13] and Weyl [25, the beginning of Chapter II] and the papers by Parshall [22] and Rota [23]. See also the references in our paper [1]. In two papers published in 1841 and 1842 Boole continued the work of Lagrange on linear transformations of homogeneous polynomials. He established the principles of invariance and introduced a series of invariant expressions. The ideas of Boole were further developed by Cayley in a series of papers started in 1845, who was the first to use the word "invariant". Later, in 1853, Sylvester introduced the term "syzygies" for the relations between invariants. The approach of Hesse was inspired by geometry: the study of critical points in plane curves with the help of the Hessian determinant.

Later, the development of the theory continued in the work of Salmon in Great Britain, Aronhold, Clebsch and Gordan in Germany, Brioschi and Cremona in Italy, Hermite in France. According to Weyl the main line of the research in this period was "the development of formal processes and the actual computation of invariants".

The next step of the development of invariant theory was in the work of Hilbert in 1890-1892 who developed general methods to solve in the affirmative many of the main problems of the theory. His nonconstructive proofs were accepted sceptically by many of his contemporary mathematicians. Gordan (known as "König der Invariantentheorie", the king of invariant theory) commented that *"Das ist nicht Mathematik, das ist Theologie."* ("This is not mathematics, this is theology." It is not clear if Gordan really said this since the earliest reference to it is 25 years after the events and after his death, nor is it clear whether the quote was intended as criticism, or praise, or a subtle joke.)

A special role is played by the 14th problem of Hilbert [10] from his famous talk at the International Congress of Mathematicians in 1900 which was motivated by the problem whether algebras of invariants are always finitely generated. In 1915, Emmy Noether [20] proved that if G is finite, then the algebra $K[X_d]^G$ is finitely generated. (In 1926 she extended this to the case of fields of any characteristic [21].) For reductive linear groups, finite generation also follows from classical invariant theory. However, in general the answer to the 14th problem of Hilbert is negative. In 1959 Nagata [19] gave a counterexample showing that the algebras $K[X_d]^G$ are not finitely generated for a class of infinite linear groups.

We now turn to the noncommutative case. Here, the commutative polynomial algebra $K[X_d]$ is replaced by its natural noncommutative counterpart: the free associative algebra $K\langle X_d\rangle$ — the algebra of noncommuting polynomials in d variables that satisfies the same fundamental universal property: For any associative algebra R every map $X_d \to R$ can be uniquely extended to a homomorphism $K\langle X_d\rangle \to R$.

The first paper on invariant theory of groups acting on the free associative algebra was published in 1936 by Margarete Wolf [26]. She described the symmetric polynomials in $K\langle X_d\rangle$, i.e. the elements of the algebra of invariants $K\langle X_d\rangle^{\mathrm{Sym}_d}$, proved that $K\langle X_d\rangle^{\mathrm{Sym}_d}$ is a free algebra which is not finitely generated and found a free generating set of this algebra.

The noncommutative analogue of the theorem of Noether on finite generation turns

out to be far more restrictive. For finite subgroups $G \leq \mathrm{GL}_d(K)$, results of Dicks and Formanek [5] and Kharchenko [12] in the 1980s show that the algebra $K\langle X_d\rangle^G$ is finitely generated if and only if G acts by scalar multiplication on the vector space spanned by the variables X_d. This characterization was later generalized to infinite groups by Koryukin [14].

Kharchenko [12] introduced an action of the symmetric group Sym_n on the homogeneous component of degree n in $K\langle X_d\rangle$, defined by permuting the positions of the variables. In this way $K\langle X_d\rangle = (K\langle X_d\rangle, \circ)$ becomes an S-algebra. Kharchenko asked whether the algebra of G-invariants $(K\langle X_d\rangle^G, \circ)$ is finitely generated as an S-algebra for all finite groups G. In 1984, Koryukin [14] proved that $(K\langle X_d\rangle^G, \circ)$ is finitely generated for every reductive group G.

A central problem in both commutative and noncommutative invariant theory is to describe the invariants of significant groups. In the present paper we study the algebra $\mathbb{C}\langle X_d\rangle^{C_d}$ of invariants under the action of the cyclic group C_d on the free associative algebra $\mathbb{C}\langle X_d\rangle$. We compute its Hilbert series and construct a homogeneous set of generators of $\mathbb{C}\langle X_d\rangle^{C_d}$ as a free algebra. Finally, we find a finite generating set of $\mathbb{C}\langle X_3\rangle^{C_3}$ as an S-algebra.

Related problems concerning noncommutative symmetric polynomials, i.e. for the algebra of invariants $\mathbb{C}\langle X_d\rangle^{\mathrm{Sym}_d}$ were considered in [1] and in [2] for the invariants $\mathbb{C}\langle x_1, x_2\rangle^{D_{2n}}$ of the dihedral group D_{2n}.

2 Preliminaries. The general linear group $\mathrm{GL}_d(\mathbb{C})$ acts naturally on the d-dimensional complex vector space V_d with basis $\{v_1, \ldots, v_d\}$. The coordinate functions $x_i : V_d \to \mathbb{C}$ are defined by

$$x_i(\xi_1 v_1 + \cdots + \xi_d v_d) = \xi_i, \quad \xi_1, \ldots, \xi_d \in \mathbb{C}, \quad i = 1, \ldots, d.$$

This induces an action of $\mathrm{GL}_d(\mathbb{C})$ on the algebra of polynomial functions $\mathbb{C}[X_d] = \mathbb{C}[x_1, \ldots, x_d]$ via

$$g(f) : v \to f\big(g^{-1}(v)\big), \quad g \in \mathrm{GL}_d(\mathbb{C}),\ f(X_d) \in \mathbb{C}[X_d],\ v \in V_d.$$

For a subgroup G of $\mathrm{GL}_d(\mathbb{C})$, the algebra of G-invariants consists of all polynomials fixed under this action of G, i.e.

$$\mathbb{C}[X_d]^G = \big\{ f \in \mathbb{C}[X_d] \mid g(f) = f \text{ for all } g \in G \big\}.$$

For our purposes it is more convenient to assume that $\mathrm{GL}_d(\mathbb{C})$ acts canonically on the vector space KX_d with basis X_d and extend its action diagonally to $\mathbb{C}[X_d]$ by

$$g\big(f(x_1, \ldots, x_d)\big) = f\big(g(x_1), \ldots, g(x_d)\big), \quad g \in \mathrm{GL}_d(\mathbb{C}), f \in \mathbb{C}[X_d].$$

The action of $\mathrm{GL}_d(\mathbb{C})$ on the polynomial functions $\mathbb{C}[X_d]$ coincides with the diagonal action of its opposite group $\mathrm{GL}_d^{\mathrm{op}}(\mathbb{C})$ induced by the canonical action of $\mathrm{GL}_d^{\mathrm{op}}(\mathbb{C})$ on the vector space KX_d. Since the map $g \to g^{-1}$ is an isomorphism of $\mathrm{GL}_d(\mathbb{C})$ and $\mathrm{GL}_d^{\mathrm{op}}(\mathbb{C})$, the invariant algebras obtained from these two actions are the same.

2.1 Foundational Theorems. The foundations of commutative invariant theory for finite groups G rest on several classical theorems.

Theorem 2.1. (Endlichkeitssatz of Emmy Noether [20]) *If G is a finite subgroup of $\mathrm{GL}_d(K)$ and the field K has characteristic zero, then the algebra of invariants $K[X_d]^G$ is finitely generated. Moreover, its homogeneous generators can be chosen so that their degrees are bounded by the order of G.*

Theorem 2.2. (Basissatz of Hilbert [9]) *Over an arbitrary field K of any characteristic every ideal of $K[X_d]$ is finitely generated.*

As a consequence of Theorems 2.1 and 2.2 one immediately obtains that if G is a finite group and the set of polynomials $\{f_1(X_d), \dots, f_n(X_d)\}$ generates $K[X_d]^G$, then there are finitely many polynomials (syzygies) $w_1(Y_n), \dots, w_m(Y_n)$ such that the factor algebra $K[Y_n]/(w_1(Y_n), \dots, w_m(Y_n))$ of the polynomial algebra $K[Y_n]$ modulo the ideal generated by $w_1(Y_n), \dots, w_m(Y_n)$ is isomorphic to $K[X_d]^G$.

Theorem 2.3. (Chevalley [3] and Shephard and Todd [24]) *If the field K is of characteristic zero and G is a finite subgroup of $\mathrm{GL}_d(K)$, then the algebra of invariants $K[X_d]^G$ is isomorphic to a polynomial algebra, i.e. has a system of algebraically independent generators if and only if G is generated by pseudo-reflections (matrices of finite order conjugate to a diagonal matrix of the form $\mathrm{diag}(1, \dots, 1, \xi)$, where $\xi \neq 1$ is a root of unity).*

The symmetric and the dihedral groups are among the well known groups which satisfy the conditions of this theorem.

The algebra $K[X_d]^G$ decomposes into its homogeneous components:

$$K[X_d]^G = K \oplus \big(K[X_d]^G\big)^{(1)} \oplus \big(K[X_d]^G\big)^{(2)} \oplus \cdots .$$

Then the Hilbert (or Poincaré) series of $K[X_d]^G$ is the formal power series

$$H\big(K[X_d]^G, t\big) = \sum_{n \geq 0} \dim \big(K[X_d]^G\big)^{(n)} t^n.$$

According to the Hilbert–Serre theorem, this series is rational with a denominator of a very special form:

$$H\big(K[X_d]^G, t\big) = p(t) \prod_{i=1}^{m} \frac{1}{1 - t^{a_i}}, \quad p(t) \in \mathbb{Z}[t].$$

The explicit form of the Hilbert series of $K[X_d]^G$ is given by Molien in 1897.

Theorem 2.4. (Molien [18]) *Over a field of characteristic zero the Hilbert series of the algebra of invariants $K[X_d]^G$ of a finite group G is*

$$H\big(K[X_d]^G, t\big) = \frac{1}{|G|} \sum_{g \in G} \frac{1}{\det\big(1 - gt\big)}.$$

2.2 Invariants of the cyclic group. Now we summarize the facts for the invariants of the cyclic group C_d of order d needed for our project. We assume that $G = C_d$ is generated by ρ which shifts cyclically the variables $x_1, \dots, x_d$:

$$\rho(x_1) = x_2, \rho(x_2) = x_3, \dots, \rho(x_{d-1}) = x_d, \rho(x_d) = x_1.$$

Then for any field K of characteristic zero $K[X_d]^{C_d}$ is spanned by all

$$\frac{1}{d}\sum_{k=0}^{d-1} \rho^k(x_1^{n_1} \cdots x_d^{n_d}),\ n_i \geq 0.$$

In the sequel we shall work over $K = \mathbb{C}$. We shall change the basis X_d of $\mathbb{C}X_d$ to

$$y_k = x_1 + \varepsilon^{-k}x_2 + \varepsilon^{-2k}x_3 + \cdots \varepsilon^{-k(d-1)}x_d, k = 0, 1, \dots, d-1,$$

where $\varepsilon = \cos\left(\frac{2\pi}{d}\right) + i\sin\left(\frac{2\pi}{d}\right)$ is a primitive d-root of 1. Then

$$\rho(y_k) = \varepsilon^k y_k, k = 0, 1, \dots, d-1,$$

$$\rho(y_0^{n_0}y_1^{n_1} \cdots y_{d-1}^{n_{d-1}}) = \varepsilon^{n_1+2n_2+\cdots+(d-1)n_{d-1}} y_0^{n_0}y_1^{n_1} \cdots y_{d-1}^{n_{d-1}}$$

and $\mathbb{C}[X_d]^{C_d} = \mathbb{C}[y_0, y_1, \dots, y_{d-1}]^{C_d} = \mathbb{C}[Y_d]^{C_d}$ is spanned by monomials $y_0^{n_0}y_1^{n_1} \cdots y_{d-1}^{n_{d-1}}$ such that $n_1 + 2n_2 + \cdots + (d-1)n_{d-1} \equiv 0 \pmod d$.

The following statement is well known and follows easily from Theorem 2.1 of Emmy Noether.

Proposition 2.5. *The algebra of invariants $\mathbb{C}[Y_d]^{C_d}$ is generated by y_0 and the monomials $u = y_1^{n_1} \cdots y_{d-1}^{n_{d-1}}$ such that*

$$1 \leq n_1 + \cdots + n_{d-1} \leq d, n_1 + 2n_2 + \cdots + (d-1)n_{d-1} \equiv 0 \pmod d$$

and which cannot be presented as products of two or more polynomials of this kind.

In other words, we consider the multiplicative semigroup $[Y_d] = [y_0, y_1, \dots, y_{d-1}]$ of all monomials in d variables. Then the algebra $\mathbb{C}[Y_d]^{C_d}$ of invariants of C_d is spanned by the subsemigroup of all monomials

$$y_0^{n_0}y_1^{n_1} \cdots y_{d-1}^{n_{d-1}} \text{ with } n_1 + 2n_2 + \cdots + (d-1)n_{d-1} \equiv 0 \pmod d,$$

and is generated by the monomials which generate this subsemigroup.

Example 2.6. *(i) $d = 3$. All monomials $y_1^{n_1}y_2^{n_2}$, $n_1 + n_2 \leq 3$, $n_1 + 2n_2 \equiv 0 \pmod 3$ are y_1y_2, y_1^3, y_2^3 and $\mathbb{C}[y_0, y_1, y_2]^{C_3}$ is generated by $y_0, y_1y_2, y_1^3, y_2^3$.*

(ii) $d = 4$. The number of monomials $y_1^{n_1}y_2^{n_2}y_3^{n_3}$ of degree $2, 3$ and 4 and such that $n_1 + 2n_2 + 3n_3 \equiv 0 \pmod 4$ is equal, respectively, to $2, 2$ and 5. The monomials $y_1y_3, y_2^2, y_1^2y_2, y_2y_3^2, y_1^4, y_3^4$ together with y_0 generate $\mathbb{C}[y_0, y_1, y_2, y_3]^{C_4}$. The other 3 monomials of degree 4

$$y_1^2y_3^2 = (y_1y_3)^2, y_1y_2^2y_3 = (y_1y_3)(y_2^2), y_2^4 = (y_2^2)^2$$

are products of the first two monomials y_1y_3, y_2^2.

(iii) $d = 5$. *It is easy to see that* $\mathbb{C}[y_0, y_1, y_2, y_3, y_4]^{C_5}$ *is generated by*

$$\deg = 1 : y_0; \quad \deg = 2 : y_1y_4, y_2y_3; \quad \deg = 3 : y_1^2y_3, y_1y_2^2;$$
$$\deg = 4 : y_1^3y_2, y_1y_3^3, y_2^3y_4, y_3y_4^3; \quad \deg = 5 : y_1^5, y_2^5, y_3^5, y_4^5.$$

If K is an arbitrary field of characteristic 0 and we consider the action of C_d on $K[X_d]$ by cyclical shifting of the variables it is natural to start with the elementary symmetric polynomials

$$e_n(x_1, \dots, x_d) = \sum_{i_1 < \dots < i_n} x_{i_1} \cdots x_{i_n}, \ n = 1, \dots, d,$$

and then to extend them to a system of generators of $K[X_d]^{C_d}$ of the form

$$x_1^{n_1}x_2^{n_2} \cdots x_{d-1}^{n_{d-1}}x_d^{n_d} + x_2^{n_1}x_3^{n_2} \cdots x_d^{n_{d-1}}x_1^{n_d} + \cdots + x_d^{n_1}x_1^{n_2} \cdots x_{d-2}^{n_{d-1}}x_{d-1}^{n_{d-1}}.$$

Alternatively, instead to start with the elementary symmetric polynomials, we can search for a generating set which consists only of cyclic sums of monomials.

The case $d = 2$ is trivial, because the algebra $K[X_2]^{C_2}$ coincides with the algebra of symmetric polynomials in two variables which is generated by e_1, e_2. In the next example we give systems of generators of $K[X_d]^{C_d}$ for $d = 3$ and 4.

Example 2.7. *(i)* $d = 3$. *By Example 2.6 (i) we have to add one polynomial of degree* 3 *to the three symmetric polynomials* e_1, e_2, e_3. *There are two possibilities:*

$$u_1 = x_1^2x_2 + x_2^2x_3 + x_3^2x_1, \quad u_2 = x_1x_2^2 + x_2x_3^2 + x_3x_1^2.$$

Since $u_1 + u_2$ *is a symmetric polynomial,* u_2 *can be expressed in terms of* e_1, e_2, e_3 *and* u_1. *Hence* $K[X_3]^{C_3}$ *is generated by* e_1, e_2, e_3, u_1. *Pay attention that here* e_1, e_2, e_3 *are cyclic sums of* x_1, x_1x_2 *and* $x_1x_2x_3$, *respectively.*

(ii) $d = 4$. *By Example 2.6 (ii) the algebra* $K[X_4]^{C_4}$ *is generated by* e_1, e_2, e_3, e_4 *and three polynomials of degree* 2, 3 *and* 4. *Easy computations show that these three polynomials are*

$$u = x_1x_2 + x_2x_3 + x_3x_4 + x_4x_1,$$
$$v = x_1^2x_2 + x_2^2x_3 + x_3^2x_4 + x_4^2x_1,$$
$$w = x_1^3x_2 + x_2^3x_3 + x_3^3x_4 + x_4^3x_1.$$

The other cyclic sums of degree ≤ 4 *can be expressed in terms of* $e_1, e_2, e_3, e_4, u, v, w$:

$$x_1x_3 + x_2x_4 = e_2 - u,$$
$$x_1^2x_3 + x_2^2x_4 + x_3^2x_1 + x_4^2x_2 = e_1e_2 - e_3 - e_1u,$$
$$x_1x_2^2 + x_2x_3^2 + x_3x_4^2 + x_4x_1^2 = -2e_3 + e_1u - v,$$
$$x_1^3x_3 + x_2^3x_4 + x_3^3x_1 + x_4^3x_2 = e_1^2e_2 - e_1e_3 - 2e_2^2 + 4e_4 - ue_1^2 + 3ue_2 - u^2,$$
$$x_1x_2^3 + x_2x_3^3 + x_3x_4^3 + x_4x_1^3 = ue_1^2 - 3ue_2 + u^2 - w,$$
$$x_1^2x_2^2 + x_2^2x_3^2 + x_3^2x_4^2 + x_4^2x_1^2 = -2e_1e_3 + 4e_4 + 2ue_2 - u^2,$$
$$x_1^2x_3^2 + x_2^2x_4^2 = e_2^2 - 2e_4 - 2ue_2 + u^2.$$

It is easy to see that $K[X_4]^{C_4}$ *is generated also by the cyclic sums of*

$$x_1, x_1x_2, x_1x_3, x_1^2x_2, x_1^2x_3, x_1^3x_2, x_1^3x_3.$$

2.3 Noncommutative Invariant Theory. Now we go to invariant theory of groups acting on the free associative algebra $K\langle X_d\rangle$. The general linear group $\mathrm{GL}_d(K) = \mathrm{GL}(KX_d)$ acts naturally on the vector space KX_d with basis X_d. Via algebra homomorphisms, this action extends to $K\langle X_d\rangle$:

$$g(f(x_1, \cdots, x_d)) = f(g(x_1), \cdots, g(x_d)),\ g \in \mathrm{GL}_d, f(x_1, \cdots, x_d) \in K\langle X_d\rangle.$$

Clearly, for every subgroup $G \leq \mathrm{GL}_d(K)$ the algebra of G-invariants $K\langle X_d\rangle^G$ is the set of all polynomials unchanged by this action of the elements of G.

2.4 Fundamental Results on Finite Generation. The following results illustrate the strong divergence between commutative and noncommutative invariant algebras with respect to finite generation. They were found independently by Dicks and Formanek [5] and Kharchenko [12] for finite groups and extended by Koryukin [14] to arbitrary groups.

Theorem 2.8. ([14]) *Let $G \leq \mathrm{GL}_d(K)$ over any field K, and let KZ_m be the minimal subspace of KX_d with $K\langle X_d\rangle^G \subseteq K\langle Z_m\rangle$. Then the algebra $K\langle X_d\rangle^G$ is finitely generated if and only if G acts on KZ_d by scalar multiplication.*

Corollary 2.9. *([5, 12]) For finite $G \leq \mathrm{GL}_d(K)$, the algebra of invariants $K\langle X_d\rangle^G$ is finitely generated if and only if G is cyclic and consists of scalar matrices.*

Corollary 2.10. ([14]) *If G acts irreducibly on KX_d, then $K\langle X_d\rangle^G$ is either trivial or not finitely generated.*

The analog of the Chevalley–Shephard–Todd theorem for the free associative algebra $K\langle X_d\rangle$ also takes a substantially different form.

Theorem 2.11. (i) (Lane [16], Kharchenko [11]) *For any $G \leq \mathrm{GL}_d(K)$ and any field K, the algebra $K\langle X_d\rangle^G$ is free.*

(ii) (Kharchenko [11]) *For finite groups G, there exists a Galois correspondence between free subalgebras of $K\langle X_d\rangle$ containing $K\langle X_d\rangle^G$ and subgroups of G: a subalgebra F with $K\langle X_d\rangle^G \subseteq F$ is free if and only if $F = K\langle X_d\rangle^H$ for some $H \leq G$.*

The analogue of the formula of Molien for the Hilbert series of the algebra of invariants is expressed in the following elegant way.

Theorem 2.12 (Dicks and Formanek [5])**.** *Let* $\mathrm{char}(K) = 0$. *Then for a finite group $G \leq \mathrm{GL}_d(K)$*

$$H\big(K\langle X_d\rangle^G, t\big) = \frac{1}{|G|}\sum_{g\in G}\frac{1}{1-\mathrm{tr}(g)t}.$$

For thorough expositions on this topic, see the surveys by Formanek [7] and Drensky [6] and the paper [1].

In the next section we shall use the following well known fact.

Lemma 2.13. *Let $Z = Z_1 \cup Z_2 \cup \cdots$ be a set of homogeneous variables such that $\deg(Z_n) = n$, and $|Z_n| = g_n$, $n = 1, 2, \ldots$. Then the Hilbert series of the free algebra $K\langle Z\rangle$ with respect to the grading induced by the grading of the set Z is*

$$H(K\langle Z\rangle, t) = \frac{1}{1-g(t)},\ \textit{where}\ g(t) = \sum_{n\geq 1} g_n t^n.$$

3 The algebra $\mathbb{C}\langle X_d\rangle^{C_d}$ of invariants of the cyclic group. As in the commutative case we assume that $G = C_d$ is generated by ρ which shifts cyclically the variables $x_1, \ldots, x_d$. The next theorem gives the Hilbert series and information on the free generators of the algebra of invariants $K\langle X_d\rangle^{C_d}$.

Theorem 3.1. (i) *For any field K of characteristic zero the Hilbert series of the algebra of invariants $K\langle X_d\rangle^{C_d}$ is*

$$H(K\langle X_d\rangle^{C_d}, t) = \frac{1-(d-1)t}{1-dt} \text{ and } \dim\left((K\langle X_d\rangle^{C_d})^{(n)}\right) = d^{n-1},\ n = 1, 2, \ldots.$$

(ii) *The generating function of the set of homogeneous free generators of the algebra $K\langle X_d\rangle^{C_d}$ is*

$$g(t) = \frac{t}{1-(d-1)t},$$

i.e. for each $n \geq 1$ the system of homogeneous free generators has $(d-1)^{n-1}$ elements of degree n.

Proof. (i) The matrix of the generator ρ of C_d with respect to the basis X_d is

$$\begin{pmatrix} 0 & 0 & \ldots & 0 & 1 \\ 1 & 0 & \ldots & 0 & 0 \\ 0 & 1 & \ldots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & 0 \end{pmatrix}.$$

Hence $\mathrm{tr}(\rho^k) = 0$ for $k = 1, 2, \ldots, d-1$, and $\mathrm{tr}(\rho^0) = \mathrm{tr}(I_d) = d$. Hence Theorem 2.12 gives

$$H(K\langle X_d\rangle^{C_d}, t) = \frac{1}{d}\sum_{k=0}^{d-1}\frac{1}{1-\mathrm{tr}(\rho^k)t} = \frac{1}{d}\left(\frac{1}{1-dt} + (d-1)\right)$$
$$= \frac{1-(d-1)t}{1-dt} = 1 + \frac{t}{1-dt} = 1 + \sum_{n\geq 1} d^{n-1}t^n.$$

The latter equality means that $\dim\left((K\langle X_d\rangle^{C_d})^{(n)}\right) = d^{n-1}$, $n = 1, 2, \ldots$.

(ii) The statement follows immediately from Lemma 2.13 because

$$H(K\langle X_d\rangle^{C_d}, t) = \frac{1-(d-1)t}{1-dt} = \frac{1}{1-g(t)}$$

implies that $g(t) = \dfrac{t}{1-(d-1)t}$. □

We shall change the basis of the vector space $\mathbb{C}X_d$ and shall work in the free associative algebra $\mathbb{C}\langle Y_d\rangle = \mathbb{C}\langle y_0, y_1, \ldots, y_{d-1}\rangle$, where C_d acts on the generators $y_0, y_1, \ldots, y_{d-1}$ by

$$\rho(y_k) = \varepsilon^k y_k,\ k = 0, 1, \ldots, d-1,\ \varepsilon = \cos\left(\frac{2\pi}{d}\right) + i\sin\left(\frac{2\pi}{d}\right).$$

Now we shall describe a vector space basis of the algebra $\mathbb{C}\langle Y_d\rangle^{C_d}$ and a set of its free generators.

Theorem 3.2. (i) *The algebra* $\mathbb{C}\langle Y_d\rangle^{C_d}$ *has a basis which consists of all monomials* $y_{i_1}\cdots y_{i_n}$ *such that* $i_1+\cdots+i_n\equiv 0 \pmod d$.

(ii) *The set of all monomials from* (i) *such that for all* $m=1,2,\dots,n-1$ *the beginning monomial* $y_{i_1}\cdots y_{i_m}$ *satisfies* $i_1+\cdots+i_m\not\equiv 0 \pmod d$ *forms a set of free generators of* $\mathbb{C}\langle Y_d\rangle^{C_d}$.

Proof. (i) The generator ρ of C_d acts on the monomials of $\mathbb{C}\langle Y_d\rangle$ by

$$\rho(y_{i_1}\cdots y_{i_n})=\varepsilon^{i_1+\cdots+i_n}y_{i_1}\cdots y_{i_n}$$

and hence $y_{i_1}\cdots y_{i_n}\in\mathbb{C}\langle Y_d\rangle^{C_d}$ if and only if $i_1+\cdots+i_n\equiv 0 \pmod d$.

(ii) The set Z of the monomials from (i) forms a subsemigroup of the free noncommutative multiplicative semigroup $\langle Y_d\rangle$ generated by Y_d. By (i) $\mathbb{C}\langle Y_d\rangle^{C_d}$ is the semigroup algebra of the semigroup Z. Hence Z is a free semigroup because the algebra $\mathbb{C}\langle Y_d\rangle^{C_d}$ is free. If $y_{i_1}\cdots y_{i_n}\in\mathbb{C}\langle Y_d\rangle^{C_d}$ and for some beginning $y_{i_1}\cdots y_{i_m}$ we have $i_1+\cdots+i_m\equiv 0 \pmod d$, then a similar congruence $i_{m+1}+\cdots+i_n\equiv 0 \pmod d$ holds for the ending $y_{i_{m+1}}\cdots y_{i_n}$. Hence both $y_{i_1}\cdots y_{i_m}$ and $y_{i_{m+1}}\cdots y_{i_n}$ belong to $\mathbb{C}\langle Y_d\rangle^{C_d}$ and $y_{i_1}\cdots y_{i_n}=(y_{i_1}\cdots y_{i_m})(y_{i_{m+1}}\cdots y_{i_n})$ is not a free generator of $\mathbb{C}\langle Y_d\rangle^{C_d}$. If $i_1+\cdots+i_m\not\equiv 0 \pmod d$ for all $m=1,\dots,n-1$, this means that $y_{i_1}\cdots y_{i_n}$ is a free generator of the semigroup Z and the set of free generators of Z is also a set of free generators of $\mathbb{C}\langle Y_d\rangle^{C_d}$. □

Below we give an algorithm how to construct a free generating set of the algebra $\mathbb{C}\langle Y_d\rangle^{C_d}$.

Algorithm 3.3. *The following procedure allows one to construct inductively a system of free generators of* $K\langle Y_d\rangle^{C_d}$.

(i) Let $n=1$. *There is only one monomial* y_0 *which satisfies the condition of Theorem 3.2 (i). We form the set* $Z_1=\{y_0\}$ *which consists of free generators of degree 1 and the set* $U_1=\{y_1,\dots,y_{d-1}\}$ *of monomials of degree 1 which are not free generators. Obviously* $|Z_1|=1$ *and* $|U_1|=d-1$.

(ii) Let $n=2$. *For each of the* $d-1$ *elements* y_i *of* U_1 *there is exactly one element* $y_j=y_{d-i}$ *such that* $y_iy_j\in\mathbb{C}\langle Y_d\rangle^{C_d}$. *We include these* y_iy_j *in the set* Z_2 *of free generators of degree 2. Obviously* $|Z_2|=d-1$. *For each* $y_i\in U_1$ *there are* $d-1$ *variables* y_j *such that* y_iy_j *does not belong to* $\mathbb{C}\langle Y_d\rangle^{C_d}$. *We include these products* y_iy_j *in the set* U_2. *Hence* $|U_2|=(d-1)^2$.

(iii) Let $n>2$. *By induction we have constructed the set* Z_{n-1} *of monomials of degree* $n-1$ *which are free generators and the set* U_{n-1} *of* $(d-1)^{n-1}$ *monomials which are not in* $\mathbb{C}\langle Y_d\rangle^{C_d}$ *and do not have a beginning which is in* $\mathbb{C}\langle Y_d\rangle^{C_d}$. *For each* $y_{i_1}\cdots y_{i_{n-1}}\in U_{n-1}$ *there is a single variable* y_j *such that* $y_{i_1}\cdots y_{i_{n-1}}y_j\in\mathbb{C}\langle Y_d\rangle^{C_d}$. *We include these* $|U_{n-1}|=(d-1)^{n-1}$ *monomials in the set* Z_n *of generators of degree* n, *which agrees with Theorem 3.1 (ii). The other* $d-1$ *monomials* $y_{i_1}\cdots y_{i_{n-1}}y_k$, $k\neq j$, *have the property that neither they nor their beginnings belong to* $\mathbb{C}\langle Y_d\rangle^{C_d}$. *They form the set* U_n *with* $|U_n|=|U_{n-1}|(d-1)=(d-1)^n$.

In this way, step by step, we shall construct the free generating set of $\mathbb{C}\langle Y_d\rangle^{C_d}$.

(iv) For each of the d^{n-1} *monomials* $y_{i_1}\cdots y_{i_{n-1}}\in\mathbb{C}\langle Y_d\rangle$ *there is a unique* y_j *such that* $y_{i_1}\cdots y_{i_{n-1}}y_j\in\mathbb{C}\langle Y_d\rangle^{C_d}$ *and this agrees with the equality* $\dim\big((K\langle X_d\rangle^{C_d})^{(n)}\big)=d^{n-1}$ *from Theorem 3.1 (i).*

Remark 3.4. *As in the commutative case, by Theorem 3.1 the dimension of* $(K\langle X_d\rangle^{C_d})^{(n)}$ *and the number of free generators of degree* n *in* $K\langle X_d\rangle^{C_d}$ *do not depend on the field* K*. Hence any basis of the* $\mathbb{Q}$*-vector space* $\left(\mathbb{Q}\langle X_d\rangle^{C_d}\right)^{(n)}$ *is a basis also for* $\left(K\langle X_d\rangle^{C_d}\right)^{(n)}$ *Similarly, any basis of the factor space*

$$\left(\mathbb{Q}\langle X_d\rangle^{C_d}\right)^{(n)} / \sum_{k=1}^{n-1} \left(\mathbb{Q}\langle X_d\rangle^{C_d}\right)^{(k)} \left(\mathbb{Q}\langle X_d\rangle^{C_d}\right)^{(n-k)}$$

is a part of a free generating set of $\mathbb{Q}\langle X_d\rangle^{C_d}$ *and hence also of* $K\langle X_d\rangle^{C_d}$*.*

4 The S-algebra $(\mathbb{C}\langle Y_d\rangle^{C_d}, \circ)$. Till the end of the paper we consider the free algebra $K\langle X_d\rangle$ as an S-algebra, equipping the homogeneous component $(K\langle X_d\rangle)^{(n)}$ of degree n with the right action of the symmetric group Sym_n that permutes positions of the variables, namely

$$(x_{i_1}\cdots x_{i_n})\circ\sigma = x_{i_{\sigma^{-1}(1)}}\cdots x_{i_{\sigma^{-1}(n)}},\ \sigma\in\mathrm{Sym}_n.$$

As we have mentioned in the introduction, this action was introduced by Kharchenko [12] and investigated by Koryukin [14]. In this section we shall describe the generators of the S-algebra $(\mathbb{C}\langle Y_d\rangle^{C_d}, \circ)$.

Theorem 4.1. *Let*

$$U = \{u_0 = y_0, u_1, \ldots, u_k\},\ u_i = y_1^{n_{i,1}}\cdots y_{d-1}^{n_{i,d-1}},\ i = 1,\ldots,k,$$

be the set of generators of the algebra $\mathbb{C}[Y_d]^{C_d}$ *from Proposition 2.5. Then the same monomials considered as elements of* $\mathbb{C}\langle Y_d\rangle$ *generate the algebra* $(\mathbb{C}\langle Y_d\rangle^{C_d}, \circ)$*.*

Proof. By Theorem 3.2 (i) the algebra $\mathbb{C}\langle Y_d\rangle^{C_d}$ has a basis of all monomials $y_{i_1}\cdots y_{i_n}$ such that $i_1+\cdots+i_n \equiv 0 \pmod d$. Hence it is sufficient to show that such monomials belong to the S-subalgebra of $\mathbb{C}\langle Y_d\rangle$ generated by the set U. There is a $\sigma\in\mathrm{Sym}_n$ such that

$$y_{i_1}\cdots y_{i_n}\circ\sigma = y_0^{n_0}y_1^{n_1}\cdots y_{d-1}^{n_{d-1}}$$

and $n_1+2n_2+\cdots+(d-1)n_{d-1}\equiv 0 \pmod d$. Working in $\mathbb{C}[Y_d]^{C_d}$,

$$y_0^{n_0}y_1^{n_1}\cdots y_{d-1}^{n_{d-1}} = u_0^{n_0}u_1^{p_1}\cdots u_k^{p_k}$$

for suitable $p_1,\ldots,p_k$. Going back to $\mathbb{C}\langle Y_d\rangle^{C_d}$ there is a $\tau\in\mathrm{Sym}_n$ such that

$$y_0^{n_0}y_1^{n_1}\cdots y_{d-1}^{n_{d-1}}\circ\tau = u_0^{n_0}u_1^{p_1}\cdots u_k^{p_k}.$$

Hence $y_{i_1}\cdots y_{i_n}\circ\sigma\tau = u_0^{n_0}u_1^{p_1}\cdots u_k^{p_k}$ and this shows that all monomials in the basis of $\mathbb{C}\langle Y_d\rangle^{C_d}$ belong to the S-subalgebra of $\mathbb{C}\langle Y_d\rangle^{C_d}$ generated by the set U. □

Example 4.2. *It follows from Example 2.6 that the following monomials generate the* S*-algebra* $(\mathbb{C}\langle Y_d\rangle^{C_d}, \circ)$ *for* $d = 3, 4, 5$*:*

(i) $d = 3$*. The* S*-algebra* $(\mathbb{C}\langle Y_3\rangle^{C_3}, \circ)$ *is generated by* $y_0, y_1y_2, y_1^3, y_2^3$*.*

(ii) $d = 4$*. The set* $\{y_0, y_1y_3, y_2^2, y_1^2y_2, y_2y_3^2, y_1^4, y_3^4\}$ *generates* $(\mathbb{C}\langle Y_4\rangle^{C_4}, \circ)$*.*

(iii) $d = 5$*. The* S*-algebra* $\mathbb{C}\langle Y_5\rangle^{C_5}$ *is generated by*

$$y_0, y_1y_4, y_2y_3, y_1^2y_3, y_1y_2^2, y_1^3y_2, y_1y_3^3, y_2^3y_4, y_3y_4^3, y_1^5, y_2^5, y_3^5, y_4^5.$$

5 The S-algebra $(\mathbb{C}\langle X_3\rangle^{C_3}, \circ)$. As in Example 2.7 it is interesting to find the generators of the S-algebra $(K\langle X_d\rangle^{C_d}, \circ)$ in terms of the canonical action of C_d by shifting the variables. The case $d = 2$ is well understood and its investigation started in the paper by Wolf [26].

Example 5.1. *We shall show that the S-algebra $(K\langle X_3\rangle^{C_3}, \circ)$ is generated by the same cyclic sums as $K[X_3]^{C_3}$:*

$$v_1 = x_1 + x_2 + x_3,\ v_2 = x_1x_2 + x_2x_3 + x_3x_1,$$

$$v_{31} = x_1^2x_2 + x_2^2x_3 + x_3^2x_1,\ v_{32} = x_1x_2^2 + x_2x_3^2 + x_3x_1^2.$$

The S-algebra $(K\langle Y_3\rangle^{C_3}, \circ)$ is generated by $y_0, y_1y_2, y_1^3, y_2^3$, where

$$y_0 = x_1 + x_2 + x_3,\ y_1 = x_1 + \varepsilon^2x_2 + \varepsilon x_3,\ y_2 = x_1 + \varepsilon x_2 + \varepsilon^2x_3,\ \varepsilon = -\frac{1}{2} + i\frac{\sqrt{3}}{2}.$$

Since $y_0 = v_1$, it is sufficient to show that y_1y_2, y_1^3, y_2^3 belong to the S-subalgebra of $(\mathbb{C}\langle X_3\rangle, \circ)$ generated by v_1, v_2, v_{31}, v_{32}. Direct computations show that

$$y_1y_2 = v_1^2 + (\varepsilon - 1)v_2 + (\varepsilon^2 - 1)v_2 \circ (12),$$

$$y_1^3 = v_1^3 + (\varepsilon^2 - 1)v_{31} \circ (1 + (23) + (13)) + (\varepsilon - 1)v_{32} \circ (1 + (23) + (13)),$$

$$y_2^3 = v_1^3 + (\varepsilon - 1)v_{31} \circ (1 + (23) + (13)) + (\varepsilon^2 - 1)v_{32} \circ (1 + (23) + (13)).$$

Direct computations also show that this system is minimal. For example, we cannot express y_1^3 in terms of the operation $\circ$ by v_1, v_2, v_{31}.

When we consider the graded free subalgebras of $K\langle X_d\rangle$, the number of homogeneous free generators of a given degree is the same for all systems of free generators. We do not know whether a similar fact holds for the number of generators of the S-subalgebras $(F, \circ)$ of $(K\langle X_d\rangle, \circ)$. Since the action of Kharchenko-Koryukin commutes with the linear change of the basis of the vector space KX_d, what is obvious, that a generating system of $(F, \circ)$ does not depend on the basis of KX_d.

Conjecture 5.2. *Every two minimal generating systems of an S-subalgebra of $(K\langle X_d\rangle, \circ)$ have the same number of elements of a given degree.*

Example 5.1 confirms Conjecture 5.2 for the special case of $(\mathbb{C}\langle X_3\rangle^{C_3}, \circ)$ and two explicitly given generating systems.

REFERENCES.

[1] S. BOUMOVA, V. DRENSKY, D. DZHUNDREKOV, and M. KASABOV. Symmetric polynomials in free associative algebras. *Turk. J. Math.*, 46:1674–1690, 2022.

[2] S. BOUMOVA, V. DRENSKY, and Ş. FINDIK. On dihedral invariants of the free associative algebra of rank two. arXiv: `2601.12144`.

[3] C. CHEVALLEY. Invariants of finite groups generated by reflections. *Am. J. Math.*, 77:778–782, 1955.

[4] L. CORRY. Teoria degli invarianti. In *Enciclopedia Italiana — Storia della Scienza*. Volume VII, pages 1025–1029. 2003. Translation: www.tau.ac.il/ corry/publications/articles/pdf/invariants.pdf.

[5] W. DICKS and E. FORMANEK. Poincaré series and a problem of S. Montgomery. *Linear and Multilinear Algebra*, 12(1):21–30, 1982.
[6] V. DRENSKY. Commutative and noncommutative invariant theory. In *Mathematics and Education in Mathematics*, pages 14–50, 1995. Proceedings of the 24-th Spring Conference of the Union of Bulgarian Mathematicians, Svishtov, Bulgaria.
[7] E. FORMANEK. Noncommutative invariant theory. *Contemporary Mathematics*, 43:87–119, 1985.
[8] C. F. GAUSS. *Disquisitiones Arithmeticae*. Gerh. Fleischer, Leipzig, 1801. English translation by A.A. Clarke, Yale University Press, New Haven-London, 1966.
[9] D. HILBERT. Über die Theorie der algebraischen Formen. *Math. Ann.*, 36:473–534, 1890.
[10] D. HILBERT. Mathematische Probleme. *Göttinger Nachrichten*:253–297, 1900. Also Archiv der Mathematik und Physik, 3 (1901) No. 1, 44–63; Translation: Bull. Amer. Math. Soc., 8 (1902), No. 10, 437–479.
[11] V. K. KHARCHENKO. Algebra of invariants of free algebras (in Russian). *Algebra Logika*, 17(4):478–487, 1978. Translation: Algebra and Logic, 17 (1978), No. 4, 316–321.
[12] V. K. KHARCHENKO. Noncommutative invariants of finite groups and Noetherian varieties. *Journal of Pure and Applied Algebra*, 31:83–90, 1984.
[13] F. KLEIN. *Vorlesungen über die Entwicklung der Mathematik im 19. Jahrhundert*. Springer-Verlag, Berlin-Heidelberg-New York, 1979. Translation: Development of mathematics in the 19th century. Transl. by M. Ackerman. Lie Groups: History, Frontiers and Applications, Vol. IX. Brookline, Massachusetts: Math. Sci. Press, 1979.
[14] A. N. KORYUKIN. Noncommutative invariants of reductive groups (in Russian). *Algebra Logika*, 23(4):419–429, 1984. Translation: Algebra and Logic, 23 (1984), No. 4, 290–296.
[15] J. L. LAGRANGE. *Méchanique analitique*. Paris, 1788.
[16] D. R. LANE. *Free Algebras of Rank Two and Their Automorphisms*. PhD thesis, Bedford College, London, 1976.
[17] FR. MEYER. Bericht über den gegenwärtigen Stand der Invariantentheorie. *Deutsche Math. Ver.*, I:79–292, 1892. Review: F. Franklin, Bull. New York Math. Soc. III (1894), 187–190.
[18] T. MOLIEN. Über die Invarianten der linearen Substitutionsgruppen. *Sitzungsberichte der Koniglich Preussischen Akademie der Wissenschaften*, 52:1152–1156, 1897.
[19] M. NAGATA. On the 14-th problem of Hilbert. *Amer. J. Math.*, 81:766–772, 1959.
[20] E. NOETHER. Der Endlichkeitssatz der Invarianten endlicher Gruppen. *Mathematische Annalen*, 77:89–92, 1915. Reprinted in Gesammelte Abhandlungen. Collected Papers. Springer-Verlag, Berlin-Heidelberg-New York-Tokyo, 1983, 181–184.
[21] E. NOETHER. Der Endlichkeitssatz der Invarianten endlicher linearer Gruppen der Charakteristik *p*. *Nachrichten Göttingen*:28–35, 1926.
[22] K. H. PARSHALL. Toward a history of nineteenth-century invariant theory. In D. E. ROWE and J. MCCLEARY, editors, *Ideas and their Reception*, pages 155–206. Academic Press, 1989.
[23] G.-C. ROTA. What is invariant theory, really? In *Algebraic Combinatorics and Computer Science. A Tribute to Gian-Carlo Rota*, pages 41–56. Springer, Milano, 2001.
[24] G. C. SHEPHARD and J. A. TODD. Finite unitary reflection groups. *Can. J. Math.*, 6:274–304, 1954.
[25] H. WEYL. *The Classical Groups, Their Invariants and Representations*. Princeton Univ. Press, Princeton, N.J., 1946. New Edition, 1997.
[26] M. C. WOLF. Symmetric functions of non-commutative elements. *Duke Mathematical Journal*, 2(4):626–637, 1936.
[27] P. R. WOLFSON. George Boole and the origins of invariant theory. *Historia Mathematica*, 35(1):37–46, 2008.

Silvia Boumova
Sofia University "St. Kliment Ohridski", Faculty of Mathematics and Informatics
James Bourchier Blvd, 5, 1126 Sofia, Bulgaria
and Institute of Mathematics and Informatics, Bulgarian Academy of Sciences
Acad. G. Bonchev Str., Bl. 8, 1113 Sofia, Bulgaria
e-mail: `boumova@fmi.uni-sofia.bg, silvi@math.bas.bg`

Vesselin Drensky
Institute of Mathematics and Informatics
Bulgarian Academy of Sciences
Acad. G. Bonchev Str., Bl. 8
1113 Sofia, Bulgaria
e-mail: drensky@math.bas.bg

ЗА ЦИКЛИЧНИТЕ ИНВАРИАНТИ НА СВОБОДНАТА АСОЦИАТИВНА АЛГЕБРА

С. Бумова и В. Дренски

Абстракт

Нека $K\langle X_d\rangle$ е свободната асоциативна алгебра от ранг $d \geq 2$ над поле K. Лейн през 1976 г. и Харченко през 1978 г. доказват, че алгебрата от инвариантите $K\langle X_d\rangle^G$ е свободна за всяка подгрупа $G \leq \mathrm{GL}_d(K)$ и всяко поле K. По-късно Харченко въвежда допълнително действие на симетричната група $\mathrm{Sym}(n)$ върху хомогенната компонента от степен n на $K\langle X_d\rangle$, зададено чрез пермутиране на позициите на променливите. Това снабдява $K\langle X_d\rangle$ с допълнителна структура на $(K\langle X_d\rangle, \circ)$-$S$-алгебра. След това, Корюкин показва, че алгебрата на инвариантите $K\langle X_d\rangle^G$ е крайно породена по отношение на това действие за всяка редуктивна група G.
В нашата статия изучаваме алгебрата $K\langle x_1, \ldots, x_d\rangle^{C_d}$ на инвариантите на циклична група C_d, $d \geq 2$, където K е произволно поле с характеристика 0. Изчисляваме реда на Хилберт за $K\langle x_1, \ldots, x_d\rangle^{C_d}$. Когато $K = \mathbb{C}$ намираме базис на линейно пространство на $\mathbb{C}\langle x_1, \ldots, x_d\rangle^{C_d}$ и явно описваме пораждащите на $\mathbb{C}\langle x_1, \ldots, x_d\rangle^{C_d}$ като свободна алгебра. Освен това описваме и крайно пораждащо множество за S-алгебрата $(\mathbb{C}\langle x_1, \ldots, x_d\rangle^{C_d}, \circ)$. Пренасяме резултатите за $K = \mathbb{C}$ към случая на произволно поле K с характеристика 0 за S-алгебрата $(K\langle x_1, x_2, x_3\rangle^{C_3}, \circ)$ и намираме минимално пораждащо множество за нея като S-алгебра.

Ключови думи: класическа теория на инвариантите, некомутативна теория на инвариантите, циклични инварианти, действие на Харченко-Корюкин.

МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2026
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2026
Proceedings of the Fifty-Fifth Spring Conference
of the Union of Bulgarian Mathematicians
Tryavna, Bulgaria, April 5–9, 2026

GRIESMER CODES, GREY–RANKIN BOUND AND THE PROJECTIVE DUAL TRANSFORM [1]

Stefka Bouyuklieva and Iliya Bouyukliev

Abstract

Professor Stefan Dodunekov made influential contributions across several domains of coding theory, number theory, and algebra. In this survey we focus on three areas in which his scientific interests were particularly substantial. The first two concern families of linear codes meeting the Griesmer bound and the Grey–Rankin bound, which have long served as central benchmarks in the study of optimal codes. The third theme is the projective dual transform, which has proven essential in the study of codes related to these bounds, and which has offered a unifying geometric and algebraic framework. Based on his contributions to this field, we emphasize both their prominence and their continuing influence on contemporary research related to various classes and families of linear codes over a finite field.

2020 Mathematics Subject Classification: 11T71, 94B05, 51E30.

Key words: Griesmer bound, Grey–Rankin bound, projective dual transform.

Professor Dodunekov was one of the most influential figures in Bulgarian coding theory and made significant contributions to several interrelated mathematical disciplines. His research spanned coding theory, algebra, and number theory, but his most profound impact was arguably in the structural analysis of optimal linear codes and in the development of geometric and algebraic tools for their investigation.

This survey focuses on three research directions in which Dodunekov played an initiating and guiding role. Two of them concern codes related to classical bounds, namely the Griesmer bound and the Grey–Rankin bound, which define fundamental limitations on the parameters of linear codes. The third direction focuses on the projective dual transform, which emerges as an indispensable tool for studying codes related to these bounds. Our goal is to provide an overview of Dodunekov's contributions in each of these areas and to trace how the initial questions he posed influenced subsequent developments.

Let $\mathbb{F}_q^n$ denote the n-dimensional vector space over the finite field $\mathbb{F}_q$, where q is a prime power. A q-ary linear $[n,k,d]_q$ code C is a k-dimensional subspace of $\mathbb{F}_q^n$ with minimum Hamming distance d. One of Dodunekov's foundational contributions to the theory of linear codes concerns the problem of determining the minimal length $n_q(k,d)$,

[1] Partially supported by the Bulgarian National Science Fund under Contracts No KP-06-H62/2-2022 and No KP-06-H92/3 - 08.12.2025.
https://doi.org/10.55630/mem.2026.55.370-381

that is, the smallest integer n for which a linear $[n, k, d]_q$ code exists. One of the main bounds for the length of a linear q-ary code with dimension k and minimum distance d is the Griesmer bound

$$n \geq g_q(k, d) = \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil .$$

Codes meeting this bound are traditionally called *Griesmer codes*. In a series of papers [8, 10], Dodunekov established the remarkable fact that for fixed q and k, and for all sufficiently large values of d, one has $n_q(k, d) = g_q(k, d)$, that is, Griesmer codes exist for all but finitely many distances. Consequently, the determination of $n_q(k, d)$ remains an open problem for only a finite set of exceptional values of d.

Another important result due to Dodunekov, crucial for the structure of binary optimal codes, asserts that for a binary Griesmer code, if the minimum distance is even, then *all* codewords have even weights. This structural property becomes fundamental in several classification results and influences the geometry of the corresponding projective configurations [11].

Two linear codes are considered equivalent if one can be obtained from the other by coordinate permutations, nonzero scalar multiplications of coordinates, and field automorphisms. To classify linear codes with given parameters means to find exactly one representative from each equivalence class.

Dodunekov's work initiated a broader line of research that led to the description of infinite families of Griesmer codes. In particular, every Griesmer code can be viewed as a member of an infinite family with the following properties:

- The lengths of successive codes in the family differ by a constant equal to the length of the simplex code of the same dimension.
- Although the number of inequivalent codes of a fixed length initially grows with the length, there exists a constant L such that for all lengths exceeding L, the number of inequivalent representatives stabilizes.
- All codes in the family can be transformed into a family Ψ of codes of fixed length, whose weights are multiples of a power of q. For several parameter sets, the structure of the codes in Ψ is explicit enough to enable complete classification.

A key tool in the development of this theory is the *projective dual transform*, which provides a geometric mechanism for transferring structural properties between the families and for understanding the invariant characteristics of optimal codes. Its role in the study of Griesmer codes and their generalizations has proven to be fundamental and continues to influence modern research in coding theory.

In addition to his contributions to the theory of Griesmer codes, Dodunekov made significant advances in the study of codes meeting the Grey–Rankin bound. Together with several collaborators, he obtained classifications of such optimal codes in dimensions 6 and 8 [9]. Let C be a binary self-complementary code with length n and minimum d. Then

$$|C| \leq \frac{8d(n-d)}{n-(n-2d)^2},$$

provided that $n > (n-2d)^2$.

A third major direction of Dodunekov's research, developed jointly with Simonis, concerns the systematic investigation of the *projective dual transform* [7]. Their studies examined the transform from several complementary perspectives, including conditions for self-duality and connections to various geometric and algebraic constructions.

This transform is based on the natural duality between points and hyperplanes in the projective geometry $\mathrm{PG}(k-1,q)$: any point $a=(a_1,a_2,\ldots,a_k)$ defines a hyperplane H_a which consists of all points $x=(x_1,x_2,\ldots,x_k)$ such that $(a,x)=\sum a_i x_i = 0$. The projective dual transform is a powerful tool in the classification of infinite families of Griesmer codes. It is based on the fact that all codes from a family can be mapped to projective dual codes with fixed length and weights. An important result in this direction was the demonstration of a direct correspondence between such families of codes and bent Boolean functions, including self-dual bent functions. This relation allowed the introduction of the notion of *projective self-polar codes*, which connect optimal linear codes, projective geometries, and bent functions.

1 The Projective Dual Transform. One of the central concepts unifying several of Dodunekov's contributions to coding theory is the *projective dual transform*. In this section we outline the projective dual transform and present the basic notions required in later parts of the survey. Our presentation emphasizes the structural ideas rather than technical details.

There are several definitions of the dual transform, depending on the purpose for which it is used. Most commonly, the transform is defined constructively using tools from projective geometry [7], or algebraically via matrix representations [1, 5]. In [2], we instead employed characteristic vectors. A convenient way to represent a linear code is via its *characteristic vector*, which is defined relative to the q-ary simplex code. The simplex code $\mathcal{S}_{q,k}$ is the unique (up to equivalence) $[\theta(q,k),k,q^{k-1}]_q$ one-weight code, where

$$\theta(q,k)=\frac{q^k-1}{q-1}.$$

Its generator matrix $S_{q,k}$ has as columns a complete set of representatives of the points of the projective space $\mathrm{PG}(k-1,q)$.

Let C be an $[n,k]_q$ linear code with generator matrix G. The *characteristic vector* of C with respect to G is the vector $\chi(C,G)=(\chi_1,\ldots,\chi_{\theta(q,k)})\in\mathbb{Z}^{\theta(q,k)}$, where χ_i is the number of columns of G that are equal or proportional to the i-th column of $S_{q,k}$. The characteristic vector records the multiplicities of projective points in the generator matrix and satisfies $\sum_{i=1}^{\theta(q,k)}\chi_i=n$.

Consider the $\theta(q,k)\times\theta(q,k)$ matrix $M_k=S_{q,k}^T S_{q,k}$ over $\mathbb{F}_q$ and let $\mathcal{N}(M_k)$ denote the binary matrix obtained by replacing each nonzero entry of M_k by 1. This matrix is symmetric and invertible over $\mathbb{Z}$. If χ is the characteristic vector of an $[n,k]_q$ code C, then the product $\chi\mathcal{N}(M_k)$ yields the weights of a maximal set of nonproportional codewords in C. Consequently, the full weight distribution of C can be computed without enumerating all codewords. This observation lies at the heart of several algorithmic and theoretical applications of the projective dual transform.

Definition 1.1. *Let C be an $[n,k]_q$ linear code with characteristic vector χ. Let $\alpha,\beta\in\mathbb{Q}$ be such that $\alpha w+\beta$ is a nonnegative integer for every nonzero weight w of C. The*

projective dual code *of C with respect to the parameters (α, β) is the linear code $D_{\alpha,\beta}(C)$ whose characteristic vector is*

$$\chi_{\alpha,\beta} = \alpha(\chi\mathcal{N}(M_k)) + \beta.\mathbf{1},$$

where $\mathbf{1}$ denotes the all-ones vector of length $\theta(q,k)$.

Equivalently, the generator matrix of $D_{\alpha,\beta}(C)$ consists of $\alpha w_i + \beta$ copies of the i-th column of $S_{q,k}$, where w_i runs over the weights of a maximal set of nonproportional codewords in C. This formulation shows the close connection between the projective dual transform and geometric constructions in projective spaces.

The parameters α and β control the transformation of the weights and allow for considerable flexibility. In particular, divisibility properties of the original code naturally lead to fractional values of α that reduce the length of the dual code.

A key result gives explicit formulas for the parameters of the dual code.

Theorem 1.2. *Let C be an $[n,k]_q$ linear code and let $\alpha, \beta \in \mathbb{Q}$ satisfy the admissibility conditions above. Then the length of $D_{\alpha,\beta}(C)$ is*

$$n_D = \alpha n q^{k-1} + \beta\frac{q^k - 1}{q-1},$$

and its nonzero weights are

$$q^{k-2}\big(\alpha((q-1)n + \chi_i) + \beta q\big),$$

where χ_i ranges over the coordinates of the characteristic vector χ of C.

An immediate and important consequence is the following.

Corollary 1.3. *If C is a projective linear code, then its projective dual $D_{\alpha,\beta}(C)$ is a two-weight code.*

This result explains the central role of the projective dual transform in the construction and classification of two-weight and few-weight codes, which are closely related to optimal codes, strongly regular graphs, and finite geometries.

A linear code C is called *projective self-dual* if it is equivalent to its projective dual $D_{\alpha,\beta}(C)$ for suitable parameters α and β. A projective self-dual code is a σ-self-dual code with respect to a transformation function σ of degree one as defined by Dodunekov and Simonis in [7, Definition 17]. A weaker notion is that of *formal projective self-duality*, where only the parameters and the weight distribution coincide. In [2], we studied projective self-dual codes in greater detail and described their connections with self-dual and self-polar incidence structures. We introduced the notion of self-polar codes and established several of their properties. We also investigated the relationship between self-polar codes and self-dual bent functions. For the parameters α and β for which $D_{\alpha,\beta}(C)$ is equivalent to the projective self-dual code C we use the following proposition given as Proposition 6 in [7].

Proposition 1.4. *Suppose C is not a replicated simplex code. Then C is a formally projective self-dual code for some α and β if and only if*

$$\alpha = \pm q^{1-\frac{k}{2}}, \quad \beta = -\frac{q-1}{1+q^{k-1}\alpha}n. \tag{1}$$

Projective self-duality, formal projective self-duality, and self-polarity are discussed in more detail in Section 3. Let us mention that every self-polar code is projective self-dual, but the converse is not necessarily true.

2 Griesmer codes and the projective dual transform. One of the fundamental properties for Griesmer codes is that, for fixed field size q and dimension k, there exists a threshold d_0 such that for every $d \geq d_0$ there exists a Griesmer code with minimum distance d. Equivalently, beyond this point the Griesmer bound is not merely a theoretical limit but is achieved by actual codes.

In this section we prove that the classification problem for Griesmer codes exhibits a *stabilization* property: as the length increases within the natural Griesmer parameter families, the number of inequivalent Griesmer codes does not keep growing indefinitely. More precisely, after a certain length threshold the number of equivalence classes becomes constant. The projective dual transform provides a unifying framework for two closely related tasks:

(i) reducing the classification of long Griesmer codes to the classification of shorter divisible codes, and

(ii) determining the point at which the number of inequivalent codes in a Griesmer family stabilizes (the constant L).

We briefly summarize both aspects. For fixed dimension k, a full classification of Griesmer codes can be organized by the families $\{\Psi_t(k, d_0)\}_{t=0}^{\infty}$, $1 \leq d_0 \leq q^{k-1}$, where the codes in the family $\Psi_t(k, d_0)$ have parameters

$$\left[g_q(k, d_0) + t\frac{q^k - 1}{q - 1},\ k,\ d_0 + tq^{k-1}\right]_q. \tag{2}$$

Classifying codes of growing length in (2) is hard even for small q and k. The key reduction is that for each fixed d_0 the classification of Griesmer codes with minimum distance $d_0 + tq^{k-1}$ can be reduced to classifying codes of a fixed length n' whose weights are all divisible by a prescribed integer ξ (usually a power of the characteristic). When n' is small, this reduction makes classification feasible.

The reduction relies on the remarkable fact that divisibility of the minimum distance forces divisibility of all codeword weights.

Theorem 2.1 ([10])**.** *Let C be a Griesmer $[n, k, d]_p$ code over $\mathbb{F}_p$, where p is a prime. If $p^e \mid d$, then p^e divides all weights of C.*

The binary case was proved by Dodunekov and Manev (see [10]), and later generalized to all prime fields (e.g. [12]). Note that there is a similar conjecture for divisible codes over composite fields, but it still remains an open problem. A consequence that is particularly useful in this context is the following persistence principle: if p^i divides a projective Griesmer code with minimum distance d_0, then the same divisor divides every Griesmer code in the family with minimum distance $d_0 + tq^{k-1}$ for $t \geq 1$. Recall that a linear code is projective, if any two columns of its generator matrix are non-proportional, or equivalently, the coordinates of its characteristic vector are only 0's and 1's.

Let C be a projective Griesmer code and assume that C is δ-divisible with $\delta = p^s$, $s \geq 0$, which means that all weights in C are divisible by δ. Choose

$$\alpha = \frac{1}{\delta}, \qquad \beta = -\frac{d_0}{\delta}.$$

Applying the projective dual transform to C yields a two-weight code $C' = D_{\alpha,\beta}(C)$ of length

$$n' = \frac{n}{\delta} q^{k-1} - \frac{d_0}{\delta} \frac{q^k - 1}{q - 1}, \tag{3}$$

with nonzero weights

$$w_0 = \frac{q^{k-2}}{\delta}\big(n(q-1)+1\big) - \frac{q^{k-1}}{\delta} d_0, \quad w_1 = w_0 - \frac{q^{k-2}}{\delta}. \tag{4}$$

If we take a δ-divisible Griesmer code which is not projective, its projective dual code for the same values of α and β has the same length n' but the number of its nonzero weights is equal to the number of the different coordinates of the characteristic vector of C. In particular, the integer $\xi = \frac{q^{k-2}}{\delta}$ divides all nonzero weights of C'. This is the mechanism underlying the reduction: instead of classifying Griesmer codes at growing lengths $n + t\frac{q^k-1}{q-1}$, one classifies codes of a fixed length n' whose nonzero weights lie in an arithmetic progression with step ξ.

Denote by $\Omega_t(k, d_0)$ the family of linear codes of dimension k, effective length n' given by (3), and nonzero weights in the set $\{w_0, w_1, \ldots, w_t\}$, where

$$w_i = w_0 - i\frac{q^{k-2}}{\delta},\ i = 1, \ldots, t, \qquad 1 \leq t \leq -\beta',$$

and by $\Omega_{1-\beta'}(k, d_0)$ the family, consisting of codes of effective length n' and nonzero weights from the set $\{w_0, \ldots, w_{-\beta'}\}$ but with dimension $\leq k$. Clearly,

$$\Omega_1 \subseteq \Omega_2 \subseteq \cdots \subseteq \Omega_{-\beta'} \subseteq \Omega_{1-\beta'}.$$

Theorem 2.2. *There is a one-to-one correspondence between the families $\Omega_1(k, d_0)$ and $\Psi_0(k, d_0)$, $\Omega_2(k, d_0)$ and $\Psi_1(k, d_0)$, ..., $\Omega_{1-\beta'}(k, d_0)$ and $\Psi_{-\beta'}(k, d_0)$. Moreover, every code in $\Psi_{-\beta'+j}(k, d_0)$ for $j \geq 0$ can be obtained from a code in $\Psi_{-\beta'}(k, d_0)$ by concatenating j copies of the simplex code of dimension k.*

This theorem was proven in [1]. We illustrate the method with a classification of linear codes over $\mathbb{F}_5$.

Example 2.3. Consider the families $\Psi_t(3, 8)$, $t \geq 0$, of Griesmer codes with parameters $[11 + 31t, 3, 8 + 25t]_5$. The parameters are $k = 3$, $d_0 = 8$, $\delta = 1$, $\alpha = 1$, $\beta = -8$. If C is a projective $[11, 3, 8]_5$ code, then $D_{1,-8}(C)$ is a $[27, 3, 20]_5$ code whose weights are all divisible by $\xi = 5$.

To classify the codes in $\Psi_t(3, 8)$, it therefore suffices to classify all codes of length 27 whose weights are multiples of 5. There are two inequivalent $[27, 3]_5$ with nonzero weights $\{20, 25\}$. Hence $\Omega_1(3, 8)$ consists of two codes and therefore there are two inequivalent $[11, 3, 8]_5$ Griesmer codes.

Further, $\Omega_2 = \Omega_1 \cup [27, 3, \{15, 20, 25\}]$ (14 codes)$\}$, $\Omega_3 = \Omega_2 \cup [27, 3, \{10, 15, 20, 25\}]$ (25 codes)$\}$, $\Omega_4 = \Omega_3 \cup [27, 3, \{5, 10, 15, 20, 25\}]$ (9 codes)$\}$, and finally $\Omega_5 = \Omega_4 \cup \{[27, 2, \{20, 25\}]$ (one code)$\}$, $[27, 2, \{15, 20, 25\}]$ (one code) $\}$, $[27, 2, \{10, 15, 20, 25\}]$ (one code)$\}$. By Theorem 2.2, these families correspond to the following classes of Griesmer codes (we list the number of inequivalent codes after the parameters):

$$\Psi_0 : \{[11, 3, 8] - 2\}, \quad \Psi_1 : \{[42, 3, 33] - 16\}, \quad \Psi_2 : \{[73, 3, 58] - 41\},$$

$$\Psi_3 : \{[104, 3, 83] - 50\}, \quad \Psi_4 : \{[135, 3, 108] - 53\}, \quad \Psi_5 : \{[166, 3, 133] - 53\}.$$

A recurring theme in the classification of Griesmer codes is that within the families $\Psi_t(k, d_0)$, the number of inequivalent codes does not grow indefinitely with t. Instead, after a certain threshold the number stabilizes. A convenient way to describe this phenomenon uses *concatenation* with the simplex code together with the projective dual transform. Let C_1 and C_2 be q-ary linear codes of dimension k, generated by G_1 and G_2, respectively. We say that a code C is obtained by *concatenation* (or gluing) of C_1 and C_2 if it has a generator matrix of the form $(G_1 \,|\, G_2)$. If C_2 is the q-ary simplex code of dimension k, then the particular choice of generator matrices is irrelevant: any two such concatenations yield equivalent codes.

The next lemma formalizes the fact that appending simplex blocks to a Griesmer code preserves Griesmer optimality and shifts the parameters in the expected way.

Lemma 2.4. *Let C be a Griesmer $[g_q(k, d), k, d]_q$ code. If we concatenate C with t copies of the q-ary simplex code of dimension k, then we obtain again a Griesmer code.*

A second ingredient is a restriction on column multiplicities in generator matrices of Griesmer codes, originally proved by Dodunekov and crucial in controlling when a simplex block must occur.

The following lemma presents a standard result in the literature on linear codes meeting the Griesmer bound that implies exactly this type of restriction on column multiplicities in a generator matrix of an optimal code.

Lemma 2.5. *If $d \leq sq^{k-1}$, then any generator matrix of a code C with parameters $[t + g_q(k, d), k, d]_q$ contains not more than $t + s$ mutually proportional columns.*

These results motivate viewing Griesmer codes in intervals according to distance and length. The intervals for the minimum distance are $(tq^{k-1}, (t+1)q^{k-1}]$, $t \geq 0$. For $d = (t+1)q^{k-1}$, there is a unique $[\frac{q^k-1}{q-1}(t+1), k, d]$ code and it is obtained by concatenating $t+1$ copies of the simplex code. Correspondingly, the relevant intervals for the length are $(t\frac{q^k-1}{q-1}, (t+1)\frac{q^k-1}{q-1}]$.

Fix k and $d_0 \leq q^{k-1}$, and consider the Griesmer families $\Psi_t(k, d_0)$, consisting of all Griesmer codes with parameters $\left[g_q(k, d_0) + t\frac{q^k-1}{q-1},\ k,\ d_0 + tq^{k-1}\right]_q$, $t \geq 0$. For each fixed k there is an integer t_0 such that for all $t \geq t_0$ there exists at least one Griesmer code with these parameters. More importantly for classification, the number of inequivalent codes in the family eventually stabilizes.

Theorem 2.6. *There exists a constant L such that for all $t \geq L$ (with fixed k and $d_0 < q^{k-1}$) the number of inequivalent Griesmer codes with parameters*

$$\left[g_q(k,d_0) + t\tfrac{q^k-1}{q-1},\ k,\ d_0 + tq^{k-1}\right]_q$$

is constant. Furthermore, $L \leq P(k,d_0) = g_q(k,d_0)(q-1) - d_0 q$.

Idea of proof. Write $d_0 = q^{k-1} - d'$ and $g_q(k,d_0) = \frac{q^k-1}{q-1} - n'$, so that

$$n' = \frac{q^k-1}{q-1} - g_q(k,d_0).$$

Then the parameters of the codes in $\Psi_t(k,d_0)$ can be rewritten as

$$\left[(t+1)\tfrac{q^k-1}{q-1} - n',\ k,\ d_0 + tq^{k-1}\right]_q.$$

Choosing $t = n'$ the corresponding length equals

$$n_t = (n'+1)\frac{q^k-1}{q-1} - n',$$

which can be realized by taking $n'+1$ simplex blocks and deleting n' columns. According to Lemma 2.5, any generator matrix of a code with these parameters can have at most $t+1$ mutually proportional columns. Hence at least one full simplex block remains inside the generator matrix, and therefore codes at level $t = n'$ are obtained from codes at level $t = n' - 1$ by concatenation with one simplex block. This shows that the number of inequivalent codes does not increase beyond $L = n' - 1$.

Using the correspondence between Griesmer families and the associated dual-transform families $\Omega_q(d_0,k)$, one obtains $L \leq P(k,d_0)$. □

As a consequence, for fixed k one can also bound the number of inequivalent Griesmer codes at a given length by a constant depending only on k. The constant L depends on both the dimension k and the base distance d_0. Intuitively, it is larger when d_0 is smaller, and its value is affected by the divisors of d_0.

3 Linear codes related to Grey–Rankin bound. The classes of codes considered in this part are binary linear projective two-weight codes which are subcodes of codes attaining the Grey–Rankin bound. Such codes play a distinguished role in coding theory, as they lie at the interface between linear codes, combinatorial designs, and spectral properties of Boolean functions. Together with Stefan Dodunekov, we constructed all binary self-complementary $[120, 9, 56]$ codes with nonzero weights 56, 64, and 120 which have an automorphism of order 3 [3].

Any characteristic vector of a projective linear code can naturally be interpreted as a truth table of a Boolean function. In this identification, the two-weight property corresponds to the Walsh spectrum taking only two values, a property characteristic of bent Boolean functions. Thus, codes provide a natural starting point for how coding theory can be used to study bent functions, and in particular, self-dual and anti-self-dual bent functions.

All code families and constructions discussed below, including the self-complementary lifting, are defined within the considered class of optimal two-weight codes. Consequently, the lifting procedures and duality properties preserve both the extremal nature of the codes and their interpretation in terms of Boolean functions.

Let C be a binary $[n, k]$ linear code with a characteristic vector χ with respect to the generator matrix G. Recall that the projective dual transform associates to (C, G) a new code $D_{\alpha,\beta}(C)$ whose characteristic vector is $\chi_{\alpha,\beta} = \alpha\,\chi M_k + \beta.\mathbf{1}$, where M_k is the incidence matrix of the simplex code. Since the code is binary, $\theta(2, k) = 2^k - 1$ and $\mathcal{N}(M_k) = M_k$.

Definition 3.1 (Projective self-polar code)**.** *A binary linear code C is called* projective self-polar *if there exists a characteristic vector χ of C and admissible parameters (α, β) such that the projective dual transform preserves the characteristic vector, i.e.*

$$\chi = \chi_{\alpha,\beta}.$$

This formulation emphasizes the existence of a *polarizing representation* of the code, rather than invariance only up to code equivalence. It is this fixed-point property that allows a direct connection to self-duality in combinatorics and Boolean function theory.

Further, we associate a $2^k \times 2^k$ binary matrix M_C with the code C which depends on the parameters (α, β), where

$$M_C = \begin{pmatrix} 0 & \chi \\ \chi_{\alpha,\beta}^T & M_k \end{pmatrix}. \tag{5}$$

If $\chi_{\alpha,\beta} = \chi$, then M_C is symmetric. More generally, if M_C is equivalent to its transpose via row and column permutations, then M_C can be interpreted as an incidence matrix of a self-dual incidence structure. If, in addition, the same permutation realizes both row and column coincidence, the structure is self-polar. Recall that an incidence structure $S = (\mathcal{P}, \mathcal{B}, I)$ with incidence matrix N is *self-polar* if there exists a permutation matrix P such that

$$PN = N^T P^T.$$

A projective self-polar code in the sense of Definition 3.1 gives rise to a self-polar incidence structure via the matrix M_C in (5). This provides a combinatorial interpretation of the self-polar property of the code.

Example 3.2. Consider the binary linear code C with characteristic vector

$$\chi = (011100110100000) \in \mathbb{Z}^{15}.$$

This code has parameters $[6, 4, 2]$ and weight enumerator $W(y) = 1 + 6y^2 + 9y^4$. For $\alpha = -\frac{1}{2}$ and $\beta = 2$ we obtain

$$\chi_{\alpha,\beta} = -\tfrac{1}{2}\,\chi M_4 + 2.\mathbf{1} = (011100110100000) = \chi,$$

hence C is projective self-polar. The associated matrix M_C is symmetric and defines a self-polar incidence structure.

4 From self-polar codes to bent Boolean functions. The matrix M_k is closely related to the Sylvester-type Hadamard matrix H_k, namely

$$H_k = (-1)^{\overline{M}_k}, \qquad \overline{M}_k = \begin{pmatrix} 0 & \mathbf{0} \\ \mathbf{0}^T & M_k \end{pmatrix}.$$

Consequently, multiplication by M_k in the characteristic-vector formalism corresponds to Walsh–Hadamard transforms of Boolean functions. This observation underlies the transition from codes to Boolean functions.

Let $f : \mathbb{F}_2^k \to \mathbb{F}_2$ be a Boolean function with truth table $[f]$. Associate to f the code C_f whose characteristic vector χ_f is the truth table without the coordinate at 0 (so $[f] = (f(0), \chi_f)$). For bent functions (which exist only for even k), the Walsh spectrum takes only the values $\pm 2^{k/2}$, and this forces C_f to be a two-weight code with weights $2^{k-1} \pm 2^{\frac{k}{2}-1}$. This property gives us that the length of the code C_f is

$$n_f = \begin{cases} 2^{k-1} \pm 2^{\frac{k}{2}-1}, & \text{if } f(0) = 0 \\ 2^{k-1} \pm 2^{\frac{k}{2}-1} - 1, & \text{if } f(0) = 1. \end{cases}$$

Denote by Φ_{k^ϵ} the family of binary two-weight codes with length $n = 2^{k-1} + \epsilon 2^{\frac{k}{2}-1}$ and nonzero weights $w_1 = 2^{k-2} + \epsilon 2^{\frac{k}{2}-1}$ and $w_2 = 2^{k-2}$, where $\epsilon = \pm 1$, and by Φ'_{k^ϵ} the family of codes of length $n = 2^{k-1} + \epsilon 2^{\frac{k}{2}-1} - 1$. These families of two-weight codes were studied in [4]. Take

$$\begin{aligned} \alpha &= \epsilon \tfrac{1}{2^{\frac{k}{2}-1}}, & \beta &= -\epsilon 2^{\frac{k}{2}-1}, & &\text{if } C \in \Phi_{k^\epsilon}, \\ \alpha &= -\epsilon \tfrac{1}{2^{\frac{k}{2}-1}}, & \beta &= 1 + \epsilon 2^{\frac{k}{2}-1}, & &\text{if } C \in \Phi'_{k^\epsilon}. \end{aligned}$$

A code $C \in \Phi_{k^\epsilon}$ is *self-polar* in the sense of Definition 3.1, when it has a characteristic vector χ such that

$$\chi = \epsilon \frac{1}{2^{\frac{k}{2}-1}} \chi M_k - \epsilon 2^{\frac{k}{2}-1} . \mathbf{1}.$$

Definition 4.1 ([6])**.** *The bent Boolean function $f : \mathbb{F}_2^k \to \mathbb{F}_2$ is called self-dual if $(-1)^f = \frac{1}{2^{k/2}} f^W$ and anti-self-dual if $(-1)^f = -\frac{1}{2^{k/2}} f^W$, where*

$$f^W(x) = \sum_{y \in \mathbb{F}_2^k} (-1)^{f(y) + x \cdot y}.$$

The following theorem gives us, that if f is a self-dual or anti-self-dual bent function, the corresponding two-weight code is self-polar.

Theorem 4.2 ([2], Theorem 5.2)**.** *Let f be a self-dual or anti-self-dual bent function and C_f be its corresponding code with a characteristic vector χ_f as defined above. Then*

$$C_f \in \begin{cases} \Phi_{k^-}, & \text{if } f(0) = 0 \text{ and } f \text{ is self-dual}, \\ \Phi_{k^+}, & \text{if } f(0) = 0 \text{ and } f \text{ is anti-self-dual}, \\ \Phi'_{k^-}, & \text{if } f(0) = 1 \text{ and } f \text{ is anti-self-dual}, \\ \Phi'_{k^+}, & \text{if } f(0) = 1 \text{ and } f \text{ is self-dual}. \end{cases}$$

In all cases the characteristic vector $\chi_{f,\alpha,\beta}$ of its projective dual code coincides with χ_f for the corresponding suitable values of α and β.

We now describe the self-complementary lifting (SCL) construction purely on the level of codes. Let C be a binary code with characteristic vector χ. Define a new code B with characteristic vector

$$\chi_B = (\overline{\chi}, 0, \chi, 0, \chi, 0, \chi), \qquad \overline{\chi} = \mathbf{1} + \chi. \tag{6}$$

The code B has dimension $k+2$ and preserves the two-weight property. Moreover, if C is projective self-polar, then so is B (with respect to the appropriately lifted parameters).

Interpreting χ as a truth table, the construction (6) yields a Boolean function in $k+2$ variables. A direct computation using block Hadamard matrices shows that SCL maps self-dual bent functions to anti-self-dual bent functions and vice versa.

Theorem 4.3. *Let C be a projective self-polar code and let f be the Boolean function associated with its characteristic vector. Then f is a self-dual or anti-self-dual bent function. Conversely, every self-dual or anti-self-dual bent function arises from a projective self-polar code in one of the corresponding two-weight families.*

5 Conclusion. In this survey we have highlighted three interwoven research directions that illustrate the depth and lasting influence of Dodunekov's work in coding theory, and in which we had the privilege to collaborate with him and subsequently to continue developing his ideas. His results on Griesmer codes clarified the asymptotic attainability of the Griesmer bound and revealed strong divisibility and rigidity properties that underpin the structure and classification of optimal linear codes. These ideas were further enriched through joint and subsequent works on codes meeting the Grey–Rankin bound, including complete classifications in specific dimensions and the identification of extremal constructions. Central to these developments is the projective dual transform, introduced and systematically investigated in [7]. The later extensions of these methods, linking optimal linear codes with projective geometries and bent Boolean functions, demonstrate how the questions and tools initiated by Dodunekov have continued to generate new results and to shape ongoing research in coding theory.

REFERENCES.

[1] I. BOUYUKLIEV. Classification of Griesmer codes and dual transform. *Discrete Mathematics*, 309(12):4049–4068, 2009.

[2] I. BOUYUKLIEV and S. BOUYUKLIEVA. Dual transform and projective self-dual codes. *Advances in Mathematics of Communications*, 18:328–341, 2024.

[3] I. BOUYUKLIEV, S. BOUYUKLIEVA, and S. DODUNEKOV. On binary self-complementary $[120, 9, 56]$ codes having an automorphism of order 3 and associated SDP designs. *Probl. Inf. Transm.*, 43:89–96, 2007.

[4] I. BOUYUKLIEV, S. BOUYUKLIEVA, and M. PASHINSKA-GADZHEVA. On some families of codes related to the even linear codes meeting the Grey–Rankin bound. *Mathematics*, 10(23):4588, 2022.

[5] A. E. BROUWER and E. van EUPEN. The correspondence between projective codes and 2-weight codes. *Des., Codes and Crypt.*, 11:262–266, 1997.

[6] C. CARLET, L. E. DANIELSEN, M. G. PARKER, and P. SOLÉ. Self-dual bent functions. *Int. J. Inform. Coding Theory*, 1(4):384–399, 2010.

[7] S. DODUNEKOV and J. SIMONIS. Codes and projective multisets. *Electron. J. Combin.*, 5(1), 1998.

[8] S. M. DODUNEKOV. Minimum block length of a linear q-ary code with specified dimension and code distance. *Probl. Inform. Transm.*, 20:239–249, 1984.

[9] S. M. DODUNEKOV, S. B. ENCHEVA, and S. N. KAPRALOV. On the [28,7,12] binary self-complementary codes and their residuals. *Designs, Codes and Cryptography*, 4:57–67, 1994.
[10] S. M. DODUNEKOV and N. L. MANEV. An improvement of the Griesmer bound for some small minimum distances. *Discrete Applied Math.*, 12:103–114, 1985.
[11] I. LANDJEV. The geometric approach to linear codes. In *Finite geometries, Proc. of the Fourth Isle of Thorns Conference*, pages 247–257. Kluwer, 2001.
[12] H. N. WARD. Divisibility of codes meeting the Griesmer bound. *J. Comb. Theory Ser. A*, 83(1):79–93, 1998.

Stefka Bouyuklieva
Faculty of Mathematics and Informatics
St. Cyril and St. Methodius University of Veliko Tarnovo
5000 Veliko Tarnovo, Bulgaria
e-mail: stefka@ts.uni-vt.bg

Iliya Bouyukliev
Institute of Mathematics and Informatics
Bulgarian Academy of Sciences
78 Nikola Gabrovski Street, P.O. box 323
5000 Veliko Tarnovo
e-mail: iliyab@math.bas.bg

ГРИЙСМЪРОВИ КОДОВЕ, ГРАНИЦА НА ГРЕЙ-РАНКИН И ПРОЕКТИВНО-ДУАЛНА ТРАНСФОРМАЦИЯ

Стефка Буюклиева и Илия Буюклиев

Абстракт

Академик Стефан Додунеков има значителен принос в няколко области на математиката, които включват теория на кодирането, теория на числата и алгебра. В това изследване се фокусираме върху три области, в които научните му интереси са били особено значителни. Първите две се отнасят до семейства линейни кодове, достигащи границите на Грийсмър и на Грей-Ранкин, които отдавна служат като централни ориентири в изучаването на оптимални кодове. Третата тема се отнася до проективно-дуалната трансформация, която играе съществена роля при изучаването на кодове, свързани с тези граници, и която предлага обединяваща геометрична и алгебрична насока на изследванията. Въз основа на приноса му в тази област, ние подчертаваме както тяхната важност, така и продължаващото му влияние върху съвременните изследвания, свързани с различни класове и семейства линейни кодове над крайно поле.

Ключови думи: Граница на Грийсмър, граница на Грей-Ранкин, проективно-дуална трансформация.

МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2026
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2026
Proceedings of the Fifty-Fifth Spring Conference
of the Union of Bulgarian Mathematicians
Tryavna, Bulgaria, April 5–9, 2026

ON T-AVOIDING SPHERICAL CODES AND DESIGNS IN 32-DIMENSIONAL EUCLIDEAN SPACE [1]

P. Boyvalenkov, D. Cherkashin, P. Dragnev, D. Yorgov, and V. Yorgov

Abstract

In this article, we show that the minimal vectors of the extremal even unimodular lattices in $\mathbb{R}^{32}$ define T-avoiding universally optimal spherical codes for suitable sets T. Moreover, these codes are minimal T-avoiding spherical designs and maximal T-avoiding codes for appropriate choices of T.

2020 Mathematics Subject Classification: 05B30, 94B65.

Key words: spherical codes, spherical designs, linear programming.

1 Introduction. Let $\mathbb{S}^{n-1} = \{\mathbf{x} = (x_1, \ldots, x_n) : x_1^2 + \cdots + x_n^2 = 1\}$ be the unit sphere in $\mathbb{R}^n$. A spherical code is a non-empty finite set $C \subset \mathbb{S}^{n-1}$. Consider

$$I(C) := \{\mathbf{x} \cdot \mathbf{y} : \mathbf{x}, \mathbf{y} \in C, \mathbf{x} \neq \mathbf{y}\},$$

the set of all inner products of distinct points of C, and denote by $s = \max I(C)$ the largest inner product (also known as a maximal cosine) of C. We refer to C as an s-code or as a spherical (n, N, s)-code, where $|C| = N$.

We are interested in spherical codes and designs (in particular, s-codes and τ-designs) which avoid some sets of inner products in $[-1, 1)$.

Definition 1.1. *Let $T \subset [-1, 1)$. A spherical code $C \subset \mathbb{S}^{n-1}$ is called T-avoiding if $I(C) \cap T = \varnothing$. If C is an s-code, then we assume $T \subset [-1, s)$ to avoid trivial cases.*

Spherical codes that are *well-distributed* have many applications in various fields. Of course, well-distributed can have many meanings (and so many applications). To quantify it, the notion of the discrete h-energy of a spherical code C for a given interaction potential h is considered (see, e.g., [1, 10] and references therein).

[1]The research of the first two authors is supported, in part, by Bulgarian NSF grant KP-06-Austria/8-2025. The research of the third author is supported, in part, by the Lilly Endowment.
https://doi.org/10.55630/mem.2026.55.382-392

Definition 1.2. *Given a function $h : [-1, 1] \to (-\infty, +\infty]$, continuous on $(-1, 1)$, we consider the h-energy of a spherical code C as*

$$E_h(C) := \sum_{\mathbf{x} \neq \mathbf{y} \in C} h(\mathbf{x} \cdot \mathbf{y}). \tag{1}$$

A spherical code C is called universally optimal *[6], if it has minimum h-energy among all codes on $\mathbb{S}^{n-1}$ of cardinality $|C|$ for all absolutely monotone potentials*[2] *h.*

The notion of T-avoiding universally optimal codes is then introduced in a natural way.

Definition 1.3. *Given $T \subset [-1, 1)$, a T-avoiding code C is called* T-avoiding universally optimal *if for any absolutely monotone potential h it has minimum h-energy among all T-avoiding codes on $\mathbb{S}^{n-1}$ with cardinality $|C|$.*

An important meaning of good distribution is given by the concept of spherical designs [11].

Definition 1.4. *A spherical τ-design is a spherical code $C \subset \mathbb{S}^{n-1}$ such that*

$$\int_{\mathbb{S}^{n-1}} p(\mathbf{x}) d\sigma_n(\mathbf{x}) = \frac{1}{|C|} \sum_{\mathbf{x} \in C} p(\mathbf{x}) \tag{2}$$

(σ_n is the normalized surface measure) holds for all polynomials $p(\mathbf{x}) = p(x_1, x_2, \ldots, x_n)$ of total degree at most τ.

In particular, codes with small $|I(C)|$ which are spherical τ-designs with large τ are good candidates for being well-distributed. In this paper we consider a class of codes on $\mathbb{S}^{31}$ which arise from even extremal unimodular lattices in $\mathbb{R}^{32}$. Such codes are spherical 7-designs and have $|I(C)| = 6$ as $0, -1 \in I(C)$ and the set $I(C) \setminus \{-1\}$ is symmetric about 0. With suitably chosen T, these codes are T-avoiding universally optimal and enjoy optimality as maximal codes and minimal designs in their class. We provide corresponding statements in Sections 4–6.

The interest in T-avoiding spherical codes came apparently after Gonçalves and Vedana [12] proved that four known extremal even unimodular lattices in $\mathbb{R}^{48}$ have the maximal possible density among the lattices with certain forbidden distances. The proof in [12] continues the research of Viazovska [22] and Cohn–Kumar–Miller–Radchenko–Viazovska [7, 8] who show the sphere packing optimality of E_8 and Leech lattices. In [3], T-avoiding $(48, 52416000, 1/2)$-codes with $T = (-1/3, -1/6) \cup (1/6, 1/3)$ were proved to be maximal as T-avoiding $1/2$-codes (with certain mild assumptions) and minimal as T-avoiding spherical 11-designs. The universal optimality of these codes has been studied in [5]. The paper [4] considers T-avoiding codes in other dimensions.

2 Preliminaries. We apply a linear programming technique which is briefly explained in this section.

For a given dimension n, we associate the sequence of Gegenbauer polynomials $\left(P_i^{(n)}\right)_{i=0}^{\infty}$ (see [19]), that are orthogonal on $[-1, 1]$ with weight $w(t) := (1 - t^2)^{(n-3)/2}$,

[2] A potential function h is absolutely monotone if its derivatives are nonnegative, i.e. $h^{(j)} \geq 0$, $j \geq 1$.

which we normalize by $P_i^{(n)}(1) = 1$. Given a code $C \subset \mathbb{S}^{n-1}$, the i-th moment of C, $i \geq 1$, is defined by

$$M_i(C) := \sum_{\mathbf{x},\mathbf{y} \in C} P_i^{(n)}(\mathbf{x} \cdot \mathbf{y}).$$

A key property of Gegenbauer polynomials is their positive definiteness [18], which implies that $M_i(C) \geq 0$ for every code C and positive integer i.

A code C is a spherical τ-design if and only if $M_i(C) = 0$, $i = 1, \ldots, \tau$. Note also that for an antipodal C (such that $C = -C$) it follows that $M_i(C) = 0$ for all odd i.

The linear programming technique we use is based on building a function f with a proper sign on $[-1, 1] \setminus T$ and proper coefficients in the Gegenbauer expansion

$$f(t) = \sum_{i=0}^{\deg f} f_i P_i^{(n)}(t). \tag{3}$$

The Fourier coefficients in (3) can be computed in a standard way.

The following key identity (see [11, 15]) is based on a double-counting for $f(\mathbf{x} \cdot \mathbf{y})$ over $C \times C$:

$$f(1) \cdot |C| + \sum_{\mathbf{x},\mathbf{y} \in C, \mathbf{x} \neq \mathbf{y}} f(\mathbf{x} \cdot \mathbf{y}) = f_0 \cdot |C|^2 + \sum_{i=1}^{\deg f} f_i M_i(C), \tag{4}$$

where $f(t)$ is a polynomial and $C \subset \mathbb{S}^{n-1}$ is a code. Additional assumptions on f, $T \subset [-1, 1]$, and moments $M_i(C)$ give bounds on the cardinalities of maximal T-avoiding codes, minimal T-avoiding designs and on h-energy of C.

For any point $\mathbf{x} \in C$ and inner product $t \in I(C)$, we denote by $A_t(\mathbf{x})$ the number of points of C with inner product t with $\mathbf{x}$. The system of nonnegative integers $(A_t(\mathbf{x}) : t \in I(C))$ is called the *distance distribution of C with respect to the point* $\mathbf{x}$. If the numbers $A_t(\mathbf{x})$ do not depend on the choice of $\mathbf{x}$ for any $t \in I(C)$, then the code C is called *distance invariant*. If the code is distance invariant, we shall omit $\mathbf{x}$ in the notation $A_t(\mathbf{x})$. Then the distance distribution of a distance-invariant code C is naturally defined as the system of positive integers

$$F(C) := \{A_{t_i} : t_i \in I(C) \cup \{1\}\},$$

where $I(C) = \{t_1, \ldots, t_d\}$ and $t_1 < \cdots < t_d < t_{d+1} := 1$. The distance distribution of a distance-invariant τ-design with $d \leq \tau - 1$ can be found from a Vandermonde-type system, see [11, Theorem 7.4]. Furthermore, the definition of design implies the following quadrature formula for any polynomial f of degree at most τ

$$Nf_0 = \sum_{i=1}^{d+1} A_{t_i} f(t_i). \tag{5}$$

Note that the above-mentioned Vandermonde system can be obtained from (5) for $f = 1, t, \ldots, t^d$.

3 Extremal even unimodular lattices in $\mathbb{R}^{32}$ and their codes.

3.1 Lattices. The codes we are interested in are found as the sets of minimum length vectors in *extremal even unimodular lattices* as defined below. We first provide general definitions and then focus on dimension 32.

A lattice $L \in \mathbb{R}^n$ is called *even* if all norms (squared lengths) of vectors of L are even. It is called *unimodular* if it coincides with its dual lattice

$$L^* := \{\mathbf{x} \in \mathbb{R}^n : \mathbf{x} \cdot \mathbf{y} \in \mathbb{Z} \ \forall \mathbf{y} \ \in L\}.$$

If L is even unimodular, then 8 divides n. It is known that the minimum norm of an even unimodular lattice L satisfies

$$\min\{\mathbf{x} \cdot \mathbf{x} : \mathbf{x} \in L, x \neq 0\} \leq 2\left[\frac{n}{24}\right] + 2. \tag{6}$$

The vectors of L can be partitioned into *layers*

$$L_m := \{\mathbf{x} \in L : \mathbf{x} \cdot \mathbf{x} = m\}.$$

An even unimodular lattice is called *extremal* if the bound (6) is attained; in other words, in the extremal lattices the layers L_m with $m < 2[n/24] + 2$ are empty.

In $\mathbb{R}^{32}$ the extremal even unimodular lattices have not been classified yet. King [14] proved that there are more than 10^7 non-isometric extremal even unimodular lattices without roots. All these lattices attain the bound (6) and are extreme; i.e., they realize a local maximum of the density function [17]. Recently these lattices were examined in terms of optimality for the Gaussian potential function

$$E(\alpha, L) = \sum_{\mathbf{x} \in L} e^{-\alpha(\mathbf{x} \cdot \mathbf{x})},$$

see Heimendahl–Marafioti–Thiemeyer–Vallentin–Zimmermann [13]. In particular, they show that for $\alpha = \pi$ such a lattice is a local maximum.

We consider the set $\mathcal{C}$ of spherical codes obtained by rescaling to $\mathbb{S}^{31}$ the first non-empty layer L_4 of an extremal even unimodular lattice L in $\mathbb{R}^{32}$.

3.2 The set $\mathcal{C}$ of codes on $\mathbb{S}^{31}$ from minimum norm 4 vectors. The first nontrivial layer L_4 of an extremal even unimodular lattice in $\mathbb{R}^{32}$ contains 146880 vectors. After rescaling to $\mathbb{S}^{31}$, we obtain a spherical code $C \in \mathcal{C}$ with cardinality $|C| = 146880$, set of inner products

$$I(C) = \left\{-1, -\frac{1}{2}, -\frac{1}{4}, 0, \frac{1}{4}, \frac{1}{2}\right\}. \tag{7}$$

Furthermore, C is a spherical $7\frac{1}{2}$-design; i.e., a 7-design with $M_{10}(C) = 0$. Since $|I(C)| = 6 < \tau = 7$, C is distance regular [11, Theorem 7.4]. Its distance distribution is given by

$$\mathcal{F}(C) = \{1, 1240, 31744, 80910, 31744, 1240, 1\}. \tag{8}$$

See, for example, [17, 20]. The quadrature rule (5) takes the form

$$\begin{aligned} 146880 f_0 = f(-1) + f(1) + 1240 \left(f\left(-\frac{1}{2}\right) + f\left(\frac{1}{2}\right)\right) \\ + 31744 \left(f\left(-\frac{1}{4}\right) + f\left(\frac{1}{4}\right)\right) + 80910 f(0), \end{aligned} \tag{9}$$

holding true for every polynomial f of degree at most 7.

For certain specific choices of T, we shall prove that all these codes are simultaneously maximal spherical T-avoiding codes among the codes that are 3-designs (an additional condition of such a type is inevitable, see Remark 4.1). Also, these codes are minimal (tight) T-avoiding spherical 7-designs.

3.3 Lattices in $\mathbb{R}^{32}$ obtained from self-dual binary codes. Of the more than 10^7 extremal even unimodular lattices in dimension 32, there are few that have been studied in detail [21]. Five of them can be called special since they can be obtained from the five (see Conway–Pless [9] for the classification) extremal doubly-even binary self-dual codes of length 32, denoted by CP_i, $i = 1, 2, \ldots, 5$. As follows from their self-duality and extremality, all these five codes have dimension 16 and minimum distance 8.

Let C be one of those five codes. We define a lattice $L(C)$ using construction B (see [10, Chapter 7]) followed by an extension (doubling). One first maps C into $\mathbb{R}^{32}$ by

$$G(C) = \big\{\, \mathbf{x} = (x_1, \ldots, x_{32}) \in \mathbb{Z}^{32} \;\big|\; x_1 + \cdots + x_{32} \equiv 0 \pmod 4, \quad \mathbf{x} \pmod 2 \in C \,\big\}.$$

Then a "doubling" is performed via

$$L(C) = \frac{1}{\sqrt{2}} G(C) \cup \frac{1}{\sqrt{2}} \left(\left(\frac{1}{2}, \frac{1}{2}, \cdots, \frac{1}{2} \right) + G(C) \right).$$

The resulting lattice is extremal, even, and unimodular. We are mostly interested in $L(C)_4$, the first non-empty layer of $L(C)$.

In search of classifying patterns, Venkov [20] introduced and investigated the parameter

$$D(L) = \big\{\, e_{2,2}(\mathbf{x}, \mathbf{z}) = \big|\{\mathbf{y} \in L(C)_4 \;\big|\; \mathbf{x} \cdot \mathbf{y} = 2,\ \mathbf{z} \cdot \mathbf{y} = 2\}\big|, \quad \mathbf{x}, \mathbf{z} \in L(C)_4 \ \text{ with } (\mathbf{x}, \mathbf{z}) = 0 \,\big\}.$$

He showed that $D(L)$ consists of even integers between 0 and 60. We see that $D(L(CP_i))$ contains the maximum value 60 as follows. The vectors

$$\mathbf{y}_1 = \frac{1}{\sqrt{2}}(2, 0, \ldots, 0, 2),\ \mathbf{y}_2 = \frac{1}{\sqrt{2}}(0, 2, \ldots, 0, 0, 2), \ldots$$

$$\mathbf{y}_{30} = \frac{1}{\sqrt{2}}(0, 0, \ldots, 2, 0, 2),\ \mathbf{y}_{31} = \frac{1}{\sqrt{2}}(-2, 0, \ldots, 0, 2),$$

$$\mathbf{y}_{32} = \frac{1}{\sqrt{2}}(0, -2, \ldots, 0, 0, 2), \ldots,\ \mathbf{y}_{60} = \frac{1}{\sqrt{2}}(0, 0, \ldots, -2, 0, 2)$$

belong to the norm 4 layer of $L(C)$ and $\mathbf{x} \cdot \mathbf{y}_i = \mathbf{z} \cdot \mathbf{y}_i = 2$ for $i = 1, 2, \ldots, 60$.

Venkov showed that every lattice L with $60 \in D(L)$ can be constructed as above, and so such L coincides with one of the $L(CP_i)$. In order to show that the five lattices $L(CP_i)$ are not isometric Koch and Venkov [21] classified $D(L(CP_i))$ for $1 \le i \le 5$ and noted that these sets are distinct.

We confirm this result using the computational algebra system Magma [2], by showing that the five lattices have automorphism groups of different orders, namely:

$$\begin{aligned} 975175680 &= 2^{21} \cdot 3 \cdot 5 \cdot 31, \\ 48126558103142400 &= 2^{31} \cdot 3^5 \cdot 5^2 \cdot 7 \cdot 17 \cdot 31, \\ 91321742131200 &= 2^{31} \cdot 3^5 \cdot 5^2 \cdot 7, \\ 16911433728 &= 2^{28} \cdot 3^2 \cdot 7, \\ 1509949440 &= 2^{25} \cdot 3^2 \cdot 5. \end{aligned}$$

The current Magma lattice database contains 19 non-isometric extremal even unimodular lattices of dimension 32. All of them have different automorphism group orders with the least one being $12288 = 2^{12} \cdot 3$. The lattices $L(CP_i)$, $i = 2, 3, 4, 5$, have the largest automorphism groups. Among the remaining lattices in the Magma database, just one is with an automorphism group order greater than $2^{21} \cdot 3 \cdot 5 \cdot 31$ and that number is $1244160000 = 2^{13} \cdot 3^5 \cdot 5^4$.

4 Maximal T-avoiding (1/2)-codes in 32 dimensions. In this section we prove that every code $C \in \mathcal{C}$ is a maximal T-avoiding $(1/2)$-code for $T = (0, 1/4)$ under the additional assumption that the code is at least a 3-design. As noted above, all such codes have cardinality 146880 and are, in fact, spherical $7\frac{1}{2}$-designs.

Remark 4.1. *One may be tempted to favor the embedding of the kissing configuration of the Leech lattice in a maximal T-avoiding $(1/2)$-code in 32 dimensions for some T. However, an easy calculation shows that the second moment of that embedding is positive; i.e., it is not even a 2-design. This prevents a contradiction when maximality is proven via polynomials in (4) with negative coefficient f_2 for codes which are at least 2-designs. Therefore, we can possibly have maximal codes with less than 196560 points if we additionally require that our codes are at least spherical 2-designs*[3]*.*

Theorem 4.2. *Let $C \subset \mathbb{S}^{31}$ be a $(0, 1/4)$-avoiding $(1/2)$-code that is (at least) a spherical 3-design. Then $|C| \leq 146880$. This bound is attained by every code $C \in \mathcal{C}$.*

Proof. Assume that $C \subset \mathbb{S}^{31}$ is a $(0, 1/4)$-avoiding $(1/2)$-code and a spherical 3-design. Consider (4) with C and the degree 10 polynomial

$$f(t) = (t+1)\left(t+\frac{1}{2}\right)^2\left(t+\frac{1}{4}\right)^2 t\left(t-\frac{1}{4}\right)\left(t-\frac{1}{2}\right)^3.$$

Note that $f(1) = 675/1024$ and $f_0 = 5/1114112$ in the Gegenbauer expansion (3) of f.

Since $f(t) \leq 0$ for every $t \in [-1, 1/2] \setminus (0, 1/4)$, the left-hand side of (4) does not exceed $f(1)|C| = 675|C|/1024$. For the right-hand side we first see that since $M_i(C) = 0$ for $i = 1, 2, 3$, the signs of the coefficients f_i, $i = 1, 2, 3$, do not matter (in fact, we have $f_2 < 0$ and $f_3 < 0$; see the Leech lattice obstruction Remark 4.1). Next, we observe that $f_i > 0$ for $i \in \{4, \ldots, 10\} \setminus \{8\}$, while $f_8 = 0$. We conclude that the right-hand side of (4) is at least $f_0|C|^2 = 5|C|^2/1114112$. This gives

$$|C| \leq \frac{f(1)}{f_0} = 146880.$$

[3] In fact, our proofs will require strength 3.

It follows from the above argument that any attaining code C must be a spherical 7-design with vanishing ninth and tenth moment (in particular, a spherical $7\frac{1}{2}$-design). Moreover, the inner products of C must belong to $\{-1, \pm 1/2, \pm 1/4, 0\}$. Every code $C \in \mathcal{C}$ possesses these properties and, therefore, attains the bound. □

The polynomial for Theorem 4.2 was constructed based on the properties of the attaining codes. Indeed, the fact that the codes are antipodal spherical 7-designs with $M_{10} = 0$ prompts us to use a degree-10 polynomial with $f_8 = 0$. Further, the necessary vanishing at the inner products and the endpoints of the interval T determine the roots of the polynomial to be as in the set $I(C)$ from (7) with the corresponding multiplicities. Lucky or not, the resulting polynomial is good as shown in the proof.

We conclude this section with the explicit Gegenbauer expansion of the polynomial f used in the above proof. It is

$$f(t) = \sum_{i=0}^{10} f_i P_i^{(32)}(t),$$

with

$$f_0 = \frac{5}{1114112},\ f_1 = \frac{65}{992256},\ f_2 = -\frac{31}{196608},\ f_3 = -\frac{93}{165376},\ f_4 = \frac{217}{417792},$$
$$f_5 = \frac{899}{58368},\ f_6 = \frac{2387}{188416},\ f_7 = \frac{20119}{894976},\ f_8 = 0,\ f_9 = \frac{3441}{11776},\ f_{10} = \frac{14911}{47104}.$$

5 Tight T-avoiding spherical 7-designs in 32 dimensions. In this section we show how minimality results for T-avoiding spherical designs on $\mathbb{S}^{31}$ with some T can be derived. Such designs were called *tight T-avoiding* in [4]. We shall prove that every code $C \in \mathcal{C}$ is a tight T-avoiding spherical 7-design with $T = (-1/4, 0) \cup (1/4, 1/2)$.

Theorem 5.1. *Let $C \subset \mathbb{S}^{31}$ be a T-avoiding spherical 7-design, where $T = (-1/4, 0) \cup (1/4, 1/2)$. Then $|C| \geq 146880$. This bound is attained by every code $C \in \mathcal{C}$.*

Proof. We apply (4) for C and with the degree 7 polynomial

$$f(t) = t(t+1)\left(t+\frac{1}{2}\right)^2\left(t+\frac{1}{4}\right)\left(t-\frac{1}{4}\right)\left(t-\frac{1}{2}\right).$$

It is easy to see that $f(t) \geq 0$ for every $t \in [-1, 1] \setminus T$ for the left-hand side and that the right-hand side is equal to $f_0|C|^2$. Since $f(1) = 135/64$ and $f_0 = 1/69632$, we obtain $|C| \geq f(1)/f_0 = 146880$. □

Again, the properties of the attaining designs suggest the right polynomial for use in (4). It has degree 7 to provide $\sum_{i=1}^{7} f_i M_i(C) = 0$ in the right-hand side and zeros in $I(C)$ from (7) with appropriate multiplicities to make the sum in the left-hand side nonnegative.

6 Universally optimal T-avoiding codes in 32 dimensions. Let L be any fixed even unimodular extremal lattice in $\mathbb{R}^{32}$ and L_4 be the collection of 146880 vectors of minimal norm. Among several possible choices of T we consider the symmetric case, where

$$T := \left(-\frac{1}{2}, -\frac{1}{4}\right) \cup \left(\frac{1}{4}, \frac{1}{2}\right).$$

With this choice of T, we denote the class of T-avoiding codes on $\mathbb{S}^{31}$ by

$$\mathcal{C}_T := \{C \subset \mathbb{S}^{31} : |C| = 146880, \quad I(C) \cap T = \varnothing\}. \tag{10}$$

The following theorem establishes that for any absolutely monotone potential function h a universal lower bound on the h-energy of codes in the class $\mathcal{C}_T$ holds. Clearly, $\mathcal{C} \subset \mathcal{C}_T$.

Theorem 6.1. *Let h be absolutely monotone with $h^{(8)} > 0$ in $(-1, 1)$ and $C \in \mathcal{C}_T$. Then*

$$\begin{aligned} E_h(C) \geq 146880 \Bigg[& h(-1) + 1240h\left(-\frac{1}{2}\right) + 31744h\left(-\frac{1}{4}\right) \\ & + 80910h\left(0\right) + 31744h\left(\frac{1}{4}\right) + 1240h\left(\frac{1}{2}\right)\Bigg]. \end{aligned} \tag{11}$$

This bound is attained by every code $C \in \mathcal{C}$.

Proof. First, we note that every code $C \in \mathcal{C}$ has the same energy as given by the right-hand side of (11). Indeed, any such code has the same inner products and distance distribution as explained in Section 3.2 and the calculation of its h-energy from (1) with the quadrature rule (9) gives the right-hand side of (11).

So, our goal is to show that (11) holds for any T-avoiding code C. Consider the multiset

$$\mathcal{I} := \{t_1, \ldots, t_8\} = \left\{-1, -1, -\frac{1}{2}, -\frac{1}{4}, 0, 0, \frac{1}{4}, \frac{1}{2}\right\}.$$

Denote by $H_7(t; h, \mathcal{I})$ the polynomial, which interpolates the potential function h at the points of $\mathcal{I}$ (a repeated node indicates derivative interpolation). Newton's interpolation formula implies that

$$H_7(t; h, \mathcal{I}) = h(t_1) + \sum_{i=1}^{7} h[t_1, \ldots, t_{i+1}](t - t_1)\ldots(t - t_i), \tag{12}$$

where $h[t_1, \ldots, t_{i+1}]$, $i = 1, \ldots, 7$, are the corresponding divided differences and

$$P_i(t) := (t - t_1)\ldots(t - t_i), \quad i = 1, \ldots, 7$$

are the associated partial products. The absolute monotonicity of h implies that all divided differences are non-negative.

The positive definiteness of the partial products $P_i(t)$ can be verified directly, with which we now proceed. Since $t + c$ has positive Gegenbauer coefficients for any $c \geq 0$ and positive definiteness is preserved under multiplication of polynomials (this is the so-called Krein condition in [16]), we conclude that the partial products P_i, $i = 1, \ldots, 6$, are positive definite. The last partial product

$$P_7(t) = (t + 1)^2\left(t + \frac{1}{2}\right)\left(t + \frac{1}{4}\right)t^2\left(t - \frac{1}{4}\right) = \sum_{i=0}^{7} f_i P_i^{(32)}(t),$$

with

$$f_0 = \frac{97}{104448}, \; f_1 = \frac{619}{41344}, \; f_2 = \frac{12245}{116736}, \; f_3 = \frac{2139}{5168}, f_4 = \frac{13981}{13056},$$

$$f_5 = \frac{4433}{2432},\ f_6 = \frac{11935}{7296},\ f_7 = \frac{341}{608},$$

is explicitly seen to be positive definite. We next utilize the Hermite error formula, which yields (recall that $T = (-1/2, -1/4) \cup (1/4, 1/2)$)

$$h(t) - H_7(t; h, \mathcal{I}) = \frac{h^{(8)}(\xi)}{8!}(t+1)^2 \left(t + \frac{1}{2}\right)\left(t + \frac{1}{4}\right) t^2 \left(t - \frac{1}{4}\right)\left(t - \frac{1}{2}\right) \geq 0$$

for every $t \in [-1, 1] \setminus T$.

To complete the argument, we combine the h- and f-energies using (4) with C, $H_7(t; h, \mathcal{I})$, and the above conclusions. In the left-hand side of (4) we estimate

$$E_h(C) = \sum_{\mathbf{x},\mathbf{y} \in C, \mathbf{x} \neq \mathbf{y}} h(\mathbf{x} \cdot \mathbf{y}) \geq \sum_{\mathbf{x},\mathbf{y} \in C, \mathbf{x} \neq \mathbf{y}} f(\mathbf{x} \cdot \mathbf{y})$$

since $h(t) \geq H_7(t; h, \mathcal{I})$ for all inner products of C. The right-hand side is at least $(H_7)_0 |C|^2$ since all Gegenbauer coefficients of $H_7(t; h, \mathcal{I})$ are non-negative. Therefore, we have

$$E_h(C) \geq 146880^2 \left((H_7)_0 - \frac{H_7(1)}{146880} \right).$$

It remains to see that the right-hand side of the last inequality is equal to the right-hand side of the bound (11). This fact follows from the quadrature formula (5) written for any of the 7-designs in $\mathcal{C}$.

If equality holds for some code C, then all moments $M_i(C)$, $i = 1, \ldots, 7$, vanish, so C has to be a 7-design. Moreover, the interpolation conditions imply that the inner products of C belong to the set $\{0, -1, \pm 1/2, \pm 1/4\}$ (see (7)). From [11, Theorem 7.4] such a code is distance-invariant. Utilizing the quadrature formula (5) associated with the design property, we conclude that such a code has the same distance distribution as (8), which concludes the proof. □

REFERENCES.

[1] S. V. BORODACHOV, D. P. HARDIN, and E. B. SAFF. *Discrete Energy on Rectifiable Sets*. Springer Monographs in Mathematics. Springer, 2019.

[2] W. BOSMA, J. CANNON, and C. PLAYOUST. The Magma algebra system. I. The user language. *Journal of Symbolic Computation*, 24:235–265, 1997.

[3] P. BOYVALENKOV and D. CHERKASHIN. The kissing number in 48 dimensions for codes with certain forbidden distances is 52 416 000. *Results in Mathematics*, 80, 2025. Article 3.

[4] P. BOYVALENKOV, D. CHERKASHIN, and P. DRAGNEV. Universal optimality of T-avoiding spherical codes and designs. arXiv:2501.13906, 2025.

[5] P. BOYVALENKOV and P. DRAGNEV. Energy of codes with forbidden distances in 48 dimensions. Accepted in *Applied and Numerical Harmonic Analysis* (Springer book series), 2025.

[6] H. COHN and A. KUMAR. Universally optimal distribution of points on spheres. *Journal of the American Mathematical Society*, 20(1):99–148, 2007.

[7] H. COHN, A. KUMAR, S. D. MILLER, D. RADCHENKO, and M. VIAZOVSKA. The sphere packing problem in dimension 24. *Annals of Mathematics*, 185:1017–1033, 2017.

[8] H. COHN, A. KUMAR, S. D. MILLER, D. RADCHENKO, and M. VIAZOVSKA. Universal optimality of the E_8 and Leech lattices and interpolation formulas. *Annals of Mathematics*, 196:983–1082, 2022.

[9] J. H. CONWAY and V. PLESS. On the enumeration of self-dual codes. *Journal of Combinatorial Theory, Series A*, 28:26–53, 1980.

[10] J. H. CONWAY and N. J. A. SLOANE. *Sphere Packings, Lattices and Groups*. Springer, New York, 3rd edition, 1999.
[11] P. DELSARTE, J.-M. GOETHALS, and J. J. SEIDEL. Spherical codes and designs. *Geometriae Dedicata*, 6:363–388, 1977.
[12] F. GONCALVES and G. VEDANA. Sphere packings in Euclidean space with forbidden distances. *Forum of Mathematics, Sigma*, 13:e49, 2025. Cambridge University Press.
[13] A. HEIMENDAHL, A. MARAFIOTI, A. THIEMEYER, F. VALLENTIN, and M. C. ZIMMERMANN. Critical even unimodular lattices in the Gaussian core model. *International Mathematics Research Notices*, 2023(6):5352–5396, 2023.
[14] O. KING. A mass formula for unimodular lattices with no roots. *Mathematics of Computation*, 72:839–863, 2003.
[15] V. I. LEVENSHTEIN. Designs as maximum codes in polynomial metric spaces. *Acta Applicandae Mathematicae*, 25:1–82, 1992.
[16] V. I. LEVENSHTEIN. Universal bounds for codes and designs. In V. S. PLESS and W. C. HUFFMAN, editors, *Handbook of Coding Theory*, chapter 6, pages 499–648. Elsevier, Amsterdam, 1998.
[17] G. NEBE. Boris Venkov's theory of lattices and spherical designs. In *Diophantine Methods, Lattices, and Arithmetic Theory of Quadratic Forms*. Volume 587, Contemporary Mathematics. AMS, 2013.
[18] I. J. SCHOENBERG. Positive definite functions on spheres. *Duke Mathematical Journal*, 9:96–108, 1942.
[19] G. SZEGO. *Orthogonal Polynomials*. AMS, Providence, RI, 1975.
[20] B. B. VENKOV. Even unimodular Euclidean lattices of dimension 32. *Zap. Nauchn. Sem. LOMI*, 116:44–55, 1982. In Russian.
[21] B. B. VENKOV and H. KOCH. Uber ganzzahlige unimodulare euklidische Gitter. *J. Reine Angew. Math.*, 398:144–168, 1989.
[22] M. VIAZOVSKA. The sphere packing problem in dimension 8. *Annals of Mathematics*, 185:991–1015, 2017.

Peter Boyvalenkov, Danila Cherkashin
Institute of Mathematics and Informatics
Bulgarian Academy of Sciences
Acad. G. Bonchev Str., Bl. 8
1113 Sofia, Bulgaria
e-mail: peter@math.bas.bg, jiocb@math.bas.bg

Peter Dragnev, Daniel Yorgov
Department of Mathematical Sciences
Purdue University Fort Wayne
Fort Wayne, IN 46805, USA
e-mail: dragnevp@purdue.edu, yorgovd@purdue.edu

Vassil Yorgov
Department of Mathematics and Computer Science
Fayetteville State University
Fayetteville, NC 28301, USA
e-mail: vyorgov@gmail.com

ВЪРХУ T-ИЗБЯГВАЩИ СФЕРИЧНИ КОДОВЕ И ДИЗАЙНИ В 32-МЕРНОТО ЕВКЛИДОВО ПРОСТРАНСТВО

П. Бойваленков, Д. Черкашин, П. Драгнев, Д. Йоргов и В. Йоргов

Абстракт

В тази статия показваме, че минималните вектори на екстремалните четни унимодуларни решетки в $\mathbb{R}^{32}$ образуват универсално оптимални T-избягващи сферични кодове за подходящи множества T. Освен това тези кодове са минимални T-избягващи сферични дизайни и максимални T-избягващи кодове при подходящ избор на T.

Ключови думи: сферични кодове, сферични дизайни, линейно програмиране.

МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2026
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2026
Proceedings of the Fifty-Fifth Spring Conference
of the Union of Bulgarian Mathematicians
Tryavna, Bulgaria, April 5–9, 2026

THE PUNCTURED DODECACODE IS UNIQUE [1]

M. Grassl, D. Krotov, L. Sok, and P. Solé

Abstract

The punctured dodecacode is an additive 4-ary code of length 11 and distance 5 which is uniformly packed. We show that any code with the same weight distribution is equivalent to it. This code is also shown to be nonlinear.

We also establish the nonexistence of analogs of the dodecacode and the punctured dodecacode in Doob graphs. To that end, we classify two-weight codes of weights 6 and 8 in Doob graphs and 4-ary Hamming graphs of diameter 9 and the corresponding strongly regular graphs.

2020 Mathematics Subject Classification: 94B25, 05E30, 94B05.

Key words: dodecacode, additive code, trace Hermitian duality, uniformly packed code, completely regular code, Doob graph, strongly regular graph.

1 Introduction. The dodecacode, introduced in [6] for the needs of quantum computing, is the most famous additive $\mathbb{F}_4$-code. It is trace Hermitian self-dual. It has length 12 and distance 6. The parameters of possible uniformly packed quaternary codes were found in [2] to belong to an infinite family of codes of length $\frac{2^{2m+1}+1}{3}$ and codimension $2m+1$. The punctured dodecacode is the case $m=2$ of this family. As a uniformly packed code, it is completely regular [13], and its coset graph is a distance-regular graph of diameter 3 [12, 1]. In this note, we show that it is unique (not only in the Hamming scheme $H(11,4)$, but also in all schemes $D(m,11-2m)$ with the same algebraic parameters) and not $\mathbb{F}_4$-linear.

The main part of the note consists of two sections. In Section 2, we show that the punctured dodecacode is unique as an additive 4-ary length-11 code (i.e., a code in $H(11,4)=D(0,11)$) with the given weight distribution. This part also includes some partial classification results for additive 4-ary codes (Section 2.3). In Section 3, we

[1]The work of Markus Grassl is carried out under the 'International Centre for Theory of Quantum Technologies 2.0: R&D Industrial and Experimental Phase' project (contract no. FENG.02.01-IP.05-0006/23). The project is implemented as part of the International Research Agendas Programme of the Foundation for Polish Science, co-financed by the European Funds for a Smart Economy 2021-2027 (FENG), Priority FENG.02 Innovation-friendly environment, Measure FENG.02.01. The work of Denis Krotov is supported within the framework of the state contract of the Sobolev Institute of Mathematics (FWNF-2026-0011). Lin Sok is supported by Nanyang Technological University Research Grant No. 04INS000047C230GRT01.

https://doi.org/10.55630/mem.2026.55.393-404

establish the nonexistence of such codes in the Doob graphs $D(m, 11-m)$, $0 < m \leq 5$, and of analogs of the dodecacode in $D(m, 12-m)$, $0 < m \leq 6$. This part also includes a classification of additive two-weight codes in $D(m, 9-m)$, $0 \leq m \leq 4$ (Section 3.2) and the corresponding strongly regular graphs. The results of the classification up to equivalence of the following codes, which were used for obtaining the results in Section 3, can be found in [8, Appendix]: weight-$\{6, 8\}$ codes in Doob graphs $D(m, 9-2m)$; additive 4-ary codes of length 6, distance at least 3 and size at least 2^6.

2 Codes in Hamming metric space.

2.1 Preliminaries. An *additive* $\mathbb{F}_4$*-code* of length n is an additive subgroup of $\mathbb{F}_4^n$. Two additive $\mathbb{F}_4$-codes are *equivalent* if one of them is obtained from the other by a permutation of coordinates and, for each coordinate independently, multiplication by a constant and/or conjugation. (Note that this equivalence is wider than the equivalence of linear codes, where the conjugation can be applied to all coordinates simultaneously.) The Hamming weight is denoted by $wt(\cdot)$. The trace denoted by Tr(), is defined by $\mathrm{Tr}(z) = z + z^2$. The two inner products that we consider here are the *Hermitian inner product*

$$\langle x, y\rangle = \sum_i x_i y_i^2,$$

and the *trace Hermitian inner product*

$$\mathrm{Tr}(\langle x, y\rangle) = \sum_i x_i y_i^2 + x_i^2 y_i.$$

Thus $\mathrm{Tr}(\langle x, y\rangle) = \langle x, y\rangle + \langle y, x\rangle$. The duals of a code C with respect to these two inner products are denoted by $C^\perp$ and $C^{\perp_T}$, respectively. The dodecacode is an additive $\mathbb{F}_4$-code of length 12 and binary dimension 12 that is self-dual with respect to the trace Hermitian inner product. It is cyclic, and puncturing it at any coordinate yields a code of parameters $(11, 2^{12}, 5)_4$. The dual weight distribution of the punctured dodecacode, in Magma notation, is

```
[ <0,1>, <6,198>, <8,495>, <10,330> ].
```

2.2 Results. The proof of the main result is based on trace Hermitian duality. We need a pair of Lemmas.

Lemma 2.1. *If an additive* $\mathbb{F}_4$*-code* C *is even, then* C *is self-orthogonal for the trace Hermitian inner product.*

Proof. (see also [6, Th. 4]) The semilinearity of the Hermitian inner product implies

$$\langle x+y, x+y\rangle = \langle x, x\rangle + \langle y, y\rangle + \langle x, y\rangle + \langle y, x\rangle.$$

Using $\langle x, x\rangle \equiv wt(x) \pmod 2$ and $\langle x, y\rangle + \langle y, x\rangle = \mathrm{Tr}(\langle x, y\rangle)$ we obtain (see also eq. (7) in [6])

$$wt(x+y) \equiv wt(x) + wt(y) + \mathrm{Tr}(\langle x, y\rangle) \pmod 2.$$

If C is even, this implies $\mathrm{Tr}(\langle x, y\rangle) = 0$. □

The following is proved in [7].

Lemma 2.2. *Up to equivalence, there is a unique additive self-dual $\mathbb{F}_4$-code of length* 11 *and distance* 5*, where the duality is understood with respect to the trace Hermitian inner product.*

Note that equivalence includes all monomial transformations as well as conjugation of coordinates.

We are now ready for a characterization of the punctured dodecacode by its weight distribution. A characterization by the minimum distance is hopeless in view of the existence of the quadratic residue code of parameters $[11, 6, 5]_4$ (but see the next subsection for partial classification results).

Theorem 2.3. *Up to equivalence, the punctured dodecacode is a unique additive $\mathbb{F}_4$-code with the dual weight distribution*

```
[ <0,1>, <6,198>, <8,495>, <10,330> ].
```

Proof. Consider an additive code C of length 11 with the same weight distribution as the punctured dodecacode. Its dual, say D, contains 2^{10} codewords. It is even since its weights are 6, 8, 10. By Lemma 2.1, D is trace Hermitian self-orthogonal. Consider a weight-5 codeword x in $C = D^{\perp_T}$. Such a word exists by the MacWilliams identity. The code $N = D \cup (x + D)$ is additive and self-orthogonal of size 2^{11}, hence self-dual. (Note that $\mathrm{Tr}(\langle x, x\rangle) = 0$). It has distance 5. By Lemma 2.2, it is unique, up to equivalence. By construction, D is the even part of N, as an even subcode of size half the size of N. The result follows. □

We could prove the following result by inspection, but a conceptual proof is better. The following was shown to the last author by Jon-Lark Kim.

Proposition 2.4. *The punctured dodecacode is not $\mathbb{F}_4$-linear.*

Proof. The code D of the preceding proof, being even and $\mathbb{F}_4$-linear, would be Hermitian self-orthogonal by [11]. But there is no Hermitian self-orthogonal code of length 11 and distance 6 over $\mathbb{F}_4$ by [5]. □

2.3 Partial classification results. In order to show the uniqueness of the punctured dodecacode, we have also obtained some partial classification results.

Shortening an additive code over $\mathbb{F}_4$ with parameters $C = (n, 2^{k_2}, d)_4$ reduces the dimension at most by two, i. e., results in a code $C' = (n-1, 2^{k_2'}, \geq d)_4$ where $k_2' \in \{k_2 - 2, k_2 - 1, k_2\}$. In order to find all inequivalent additive $(11, 2^{12}, 5)_4$ codes over $\mathbb{F}_4$, we start with the $(5, 1, 5)_4$ code generated by the all-one vector. Then we try to increase the dimension by one, while the minimum distance is at least 5. Having found all $(n, 2^k, d \geq 5)_4$ codes with covering radius ≤ 4, i. e., codes for which the dimension cannot be increased, we add a zero coordinate to the codes and continue. We exclude codes whose dimension is too small to reach $(11, 2^{12}, 5)_4$.

Table 1 shows the number of inequivalent additive $(n, 2^k, 5)_4$ codes that we have found. We only found two $(11, 2^{12}, 5)_4$ codes, corresponding to the punctured dodecacode and the $\mathbb{F}_4$-linear quadratic residue code.

$n\backslash k$	0	1	2	3	4	5	6	7	8	9	10	11	12	13
5	1	1	1	0										
6	1	2	5	1	0	0								
7	1	3	15	32	43	1	0							
8	1	4	34	322	5114	26299	1579	0	0					
9								$\geq$89116	2298	0	0			
10										$\geq$20935	37	0	0	
11												$\geq$24	2	0

Table 1: The number $N(n,k,5)$ of equivalence classes of additive $(n,2^k,\geq 5)_4$ codes. According to our approach, we classify $(n,2^k,\geq 5)_4$ codes by lengthening $N(n-1,k-2,5)+N(n-1,k-1,5)+N(n-1,k,5)$ codes of length $n-1$. The notation $\geq N_0$ means that we lengthened only $N(n-1,k-1,5)+N(n-1,k,5)$ codes of size 2^{k-1} and 2^k and N_0 is the number of codes having at least one coordinate with at most two symbols.

There is also a unique additive $(7,2^5,5)_4$ code, with generator matrix

$$\begin{pmatrix} 1 & 0 & \omega & \omega^2 & 0 & \omega^2 & 1 \\ \omega & 0 & 0 & 1 & \omega^2 & \omega & 1 \\ 0 & 1 & \omega & 1 & \omega^2 & \omega^2 & \omega \\ 0 & \omega & \omega & \omega^2 & 1 & 0 & \omega^2 \\ 0 & 0 & 1 & \omega^2 & \omega & 1 & \omega \end{pmatrix},$$

where $\omega^2=\omega+1$. It is cyclic and has the weight distribution

```
[ <0,1>, <5,21>, <6,7>, <7,3> ].
```

Note that the best $\mathbb{F}_4$-linear codes have parameters $[7,2,5]_4$ and $[7,3,4]_4$. Hence, this code has twice as many codewords as the largest $\mathbb{F}_4$-linear code of length 7 and distance 5.

3 Codes in Doob metric space.

3.1 Preliminaries. A set C of vertices in a connected regular graph is called a *completely regular code* with covering radius ρ and *intersection array* $I=\{b_0,\ldots,b_{\rho-1};c_1,\ldots,c_\rho\}$ (for short, CR-ρ, I-CR, or just CR code) if each vertex in $C^{(i)}$ has exactly b_i neighbors in $C^{(i+1)}$ and exactly c_i neighbors in $C^{(i-1)}$, $b_\rho=c_0=0$, where $C^{(i)}$ is the set of vertices at distance i from C and ρ is the largest i such that $C^{(i)}$ is nonempty. A connected graph is called *distance-regular* with intersection array I if every singleton is an I-CR code. Distance-regular graphs of diameter 2 are called *strongly regular*.

The Doob graph $D(m,n)$ is the Cartesian product of m copies of the Shrikhande graph on 16 vertices and n copies of the complete graph K_4 of order 4. Usually, for Doob graphs it is implied that $m>0$, while $D(0,n)$ is the 4-ary Hamming graph $H(n,4)$. It is known that $D(m,n)$ is a distance-regular graph with intersection array $\{3d,3d-3,\ldots,3;1,2,\ldots,d\}$, where $d=2m+n$ is its diameter; in particular, all $D(m,n)$ have the same intersection array as $H(2m+n,4)$. If we associate the vertices of $D(m,n)$ with the elements of the module $M=\mathbb{R}_{16}^m\times\mathbb{F}_4^n$ over the Galois ring $\mathbb{R}_{16}=\mathrm{GR}(4^2)$, then we can define linear codes as submodules of M and additive codes as subgroups of the

additive group of M. In particular, treating $\mathbb{R}_{16}$ as a module over $\mathbb{Z}_4$, we see that such additive codes are submodules of $(\mathbb{Z}_4^2)^m \times (\mathbb{Z}_2^2)^n$. In [9], the concept of additive codes in $D(m,n)$ was further generalized by allowing some of the last n coordinates to have the structure $\mathbb{Z}_4$ instead of $\mathbb{Z}_2^2$. The formal definition below is based on that extended concept of additive codes.

We first recall that the *Cayley graph* on an Abelian group G with a connecting set $S \subset G \setminus \{\mathrm{Id}\}$, $S = S^{-1}$, is the graph with the vertex set G where two vertices $a, b \in G$ are adjacent if and only if $b - a \in S$. Let the *Doob graph* $D(m, n' + n'')$ be defined as the Cayley graph on the additive group of the module $V = (\mathbb{Z}_4^2)^m \times (\mathbb{Z}_2^2)^{n'} \times \mathbb{Z}_4^{n''}$ with connecting set $S = S^* \cup S' \cup S''$, where S^* (S', S'', respectively) consists of vectors of V with one of the first m symbols (the next n' symbols, the last n'' symbols, respectively) lying in $\{01, 10, 11, 03, 30, 33\}$ ($\{01, 10, 11\}$, $\{1, 2, 3\}$, respectively) and all other symbols are zero, 00 or 0 (we naturally consider vectors of V as words of length $m + n' + n''$ where the first m symbols are from $\mathbb{Z}_4^2$, the next n' symbols are from $\mathbb{Z}_2^2$, and the last n'' symbols are from $\mathbb{Z}_4$). The (Doob) weight $\mathrm{wt}(x)$ of a vector x in V is the sum of the weights of all symbols of x, where

$$\text{for } x^* \in \mathbb{Z}_4^2,\ \mathrm{wt}(x^*) = \begin{cases} 0 & \text{if } x^* = 00, \\ 1 & \text{if } x^* \in \{01, 03, 10, 30, 11, 33\}, \\ 2 & \text{otherwise;} \end{cases}$$

$$\text{for } x' \in \mathbb{Z}_2^2,\ \mathrm{wt}(x') = \begin{cases} 0 & \text{if } x' = 00, \\ 1 & \text{if } x' \in \{01, 10, 11\}; \end{cases}$$

$$\text{for } x'' \in \mathbb{Z}_4,\ \mathrm{wt}(x'') = \begin{cases} 0 & \text{if } x'' = 0, \\ 1 & \text{if } x'' \in \{1, 2, 3\}. \end{cases}$$

The (Doob) distance between $x, y \in V$ is defined as $\mathrm{wt}(y - x)$ and coincides with the natural shortest-path distance in the graph $D(m, n' + n'')$.

As in the case of codes in the Hamming space $H(n, 4)$, the weight distributions of a code and its dual are connected by the MacWilliams transform (the formulas are the same as in $H(2m + n' + n'')$). However, the duality should be defined properly, with respect to a special inner product $\langle \cdot, \cdot \rangle_-$ (see [3, Theorem 6.6]): for $x^*, y^* \in (\mathbb{Z}_4^2)^m$, $x', y' \in \mathbb{Z}_4^{n'}$, $x'', y'' \in (\mathbb{Z}_2^2)^{n''}$,

$$\big\langle (x^*, x', x''), (y^*, y', y'') \big\rangle_- = \sum_{i=1}^{m} (x^*_{2i-1} y^*_{2i-1} - x^*_{2i} y^*_{2i}) + 2 \cdot \sum_{i=1}^{2n'} x'_i y'_i + \sum_{i=1}^{n''} x''_i y''_i. \quad (1)$$

In particular, similarly to the codes in $H(n, q)$, a code with distance at least 3 is CR-2 (completely regular with covering radius 2) if and only if its dual has two nonzero weights.

3.2 Two-weight codes of size 64. Our first aim is to classify additive codes of size 64 in $D(m, n' + n'')$, $2m + n' + n'' = 9$, with nonzero weights 6 and 8 and dual distance at least 3. The last condition means that either $m = n'' = 0$ or the code has at least one element z of order 4, which can only be possible if $2m + n'' \geq 6$ (otherwise, $0 < \mathrm{wt}(2z) < 6$). In [8, Appendix A], we list all, up to equivalence, additive weight-$\{6, 8\}$ (two-weight with weights 6 and 8 and one-weight with weight 6 or 8) codes in Doob graphs $D(m, n' + n'')$ of diameter $2m + (n' + n'') = 9$ such that $2m + n'' \geq 6$ and in

$$B_1:\left(\begin{array}{cccc|c} 21 & 10 & 10 & 10 & 10\\ 31 & 01 & 01 & 01 & 01\\ \hline 20 & 02 & 20 & 00 & 00\\ 02 & 22 & 02 & 00 & 00 \end{array}\right),\quad B_2:\left(\begin{array}{cccc|c} 21 & 10 & 10 & 10 & 10\\ 12 & 11 & 01 & 01 & 01\\ \hline 20 & 02 & 20 & 00 & 00\\ 22 & 20 & 02 & 00 & 00 \end{array}\right),$$

$$B_3:\left(\begin{array}{cccc|c} 21 & 21 & 10 & 00 & 10\\ 20 & 10 & 01 & 10 & 01\\ \hline 12 & 01 & 01 & 01 & 01 \end{array}\right),\quad B_4:\left(\begin{array}{cccc|c} 21 & 21 & 10 & 00 & 10\\ 20 & 10 & 01 & 10 & 01\\ \hline 13 & 01 & 01 & 01 & 11 \end{array}\right),$$

$$B_5:\left(\begin{array}{cccc|c} 21 & 21 & 10 & 00 & 10\\ 20 & 10 & 01 & 10 & 01\\ \hline 32 & 03 & 01 & 01 & 10 \end{array}\right),\quad B_6:\left(\begin{array}{cccc|c} 21 & 21 & 10 & 00 & 10\\ 31 & 20 & 01 & 10 & 00\\ \hline 21 & 33 & 01 & 01 & 01 \end{array}\right).$$

Table 2: Generator matrices of additive weight-$\{6,8\}$ codes of type $\mathbb{Z}_4^2\mathbb{Z}_2^2$ (B_1, B_2) and type $\mathbb{Z}_4^3$ (B_3, B_4, B_5, B_6) in $D(4,1+0)$. Here and further, the two vertical lines in the matrix separate the three groups of coordinates (one or two of which can be empty), while the horizontal line separates the rows of order 4 and the rows of order-2.

$D(0,9+0)=H(9,4)$. The approach of the classification is rather straightforward. We start with the collection consisting of one trivial code having only the all-zero codeword. For each code C from the collection, we try to continue it by adding a new element c to the generator set in all possible ways and checking if the resulting code $\mathrm{span}(C\cup\{c\})$ has the required weights and is not equivalent to any code from our collection. If it is a new weight-$\{6,8\}$ code, we add it to the collection. When all codes from the collection are checked for augmentation, the process stops.

In Tables 2, 3, 4, as a recapitulation, we list only weight-$\{6,8\}$ codes of size 64. The following proposition summarizes the computational results.

Proposition 3.1. *In $D(m,n'+n'')$, $2m+n'+n''=9$, there are exactly 22 equivalence classes of weight-$\{6,8\}$ codes of size 64. Namely, $B_1,\dots,B_6$ in $D(4,1+0)$ (Table 2), $C_1,\dots,C_8$ in $D(3,0+3)$ (Table 3), $D_1,\dots,D_8$ in $D(0,9+0)=H(9,4)$ (Table 4). The weight distribution of all these codes is $\{0^1,6^{36},8^{27}\}$; the dual codes (with respect to the inner product (1)) are completely regular with intersection array $\{27,16;1,12\}$; the coset graphs of the dual codes are strongly regular with parameters $(64,27,10,12)$; these strongly regular graphs belong to only 7 equivalence classes, corresponding to the groups $\{B_1,C_2,D_2,D_6\}$, $\{B_2,B_3,C_1,C_3,C_8,D_1,D_5\}$, $\{B_4\}$, $\{B_5,C_4,C_6\}$, $\{B_6,C_5,C_7\}$, $\{D_3,D_4,D_7\}$, $\{D_8\}$ of codes.*

Remark 3.2. *By construction, the graphs from codes of group type $\mathbb{Z}_4^i\mathbb{Z}_2^j$ are strongly regular Cayley graphs over $\mathbb{Z}_4^i\mathbb{Z}_2^j$ (in our case, (i,j) is $(0,6)$, $(2,2)$, or $(3,0)$); however, we cannot say that we have found all such graphs. The reason is that being representable as a coset graph of a code in a Doob graph or a Hamming graph $H(n,4)$ implies certain relations between vectors from the connecting set of a Cayley graph. More strongly regular Cayley graphs with the same parameters can hypothetically be constructed as coset graphs of binary linear or $\mathbb{Z}_2\mathbb{Z}_4$-linear two-weight codes.*

$$C_1 : \left(\begin{array}{ccc||ccc} 21 & 10 & 10 & 1 & 1 & 0 \\ 12 & 01 & 01 & 1 & 0 & 1 \\ \hline 22 & 02 & 20 & 0 & 0 & 0 \\ 02 & 22 & 02 & 0 & 0 & 0 \end{array}\right), \quad C_2 : \left(\begin{array}{ccc||ccc} 21 & 10 & 10 & 1 & 1 & 0 \\ 10 & 21 & 01 & 1 & 0 & 1 \\ \hline 22 & 02 & 20 & 0 & 0 & 0 \\ 02 & 22 & 02 & 0 & 0 & 0 \end{array}\right),$$

$$C_3 : \left(\begin{array}{ccc||ccc} 21 & 21 & 21 & 0 & 0 & 0 \\ 31 & 31 & 00 & 1 & 1 & 0 \\ \hline 02 & 10 & 10 & 1 & 0 & 1 \end{array}\right), \quad C_4 : \left(\begin{array}{ccc||ccc} 21 & 21 & 21 & 0 & 0 & 0 \\ 31 & 31 & 00 & 1 & 1 & 0 \\ \hline 22 & 30 & 10 & 1 & 0 & 1 \end{array}\right),$$

$$C_5 : \left(\begin{array}{ccc||ccc} 21 & 21 & 21 & 0 & 0 & 0 \\ 30 & 20 & 10 & 1 & 1 & 0 \\ \hline 33 & 11 & 20 & 1 & 0 & 1 \end{array}\right), \quad C_6 : \left(\begin{array}{ccc||ccc} 21 & 21 & 10 & 2 & 0 & 0 \\ 20 & 10 & 01 & 1 & 1 & 0 \\ \hline 12 & 01 & 01 & 1 & 0 & 1 \end{array}\right),$$

$$C_7 : \left(\begin{array}{ccc||ccc} 21 & 21 & 10 & 2 & 0 & 0 \\ 20 & 10 & 01 & 1 & 1 & 0 \\ \hline 33 & 20 & 11 & 1 & 0 & 1 \end{array}\right), \quad C_8 : \left(\begin{array}{ccc||ccc} 21 & 21 & 10 & 2 & 0 & 0 \\ 21 & 30 & 01 & 1 & 1 & 0 \\ \hline 30 & 02 & 01 & 1 & 0 & 1 \end{array}\right).$$

Table 3: Generator matrices of additive weight-$\{6, 8\}$ codes of type $\mathbb{Z}_4^2\mathbb{Z}_2^2$ (C_1, C_2) and type $\mathbb{Z}_4^3$ (C_3, C_4, C_5, C_6, C_7, C_8) in $D(3, 0 + 3)$.

$$D_1 : \begin{pmatrix} 10\,10 & 10\,10 & 10\,10 & 00\,00 & 00\,00 \\ 01\,01 & 01\,01 & 01\,01 & 00\,00 & 00\,00 \\ 01\,01 & 10\,10 & 00\,00 & 10\,10 & 00\,00 \\ 11\,11 & 01\,01 & 00\,00 & 01\,01 & 00\,00 \\ 11\,01 & 01\,00 & 11\,00 & 10\,00 & 10\,00 \\ 10\,11 & 11\,00 & 10\,00 & 01\,00 & 01\,00 \end{pmatrix}, \quad D_2 : \begin{pmatrix} 10\,10 & 10\,10 & 10\,10 & 00\,00 & 00\,00 \\ 01\,01 & 01\,01 & 01\,01 & 00\,00 & 00\,00 \\ 01\,01 & 10\,10 & 00\,00 & 10\,10 & 00\,00 \\ 11\,11 & 01\,01 & 00\,00 & 01\,01 & 00\,00 \\ 11\,01 & 01\,00 & 11\,00 & 10\,00 & 10\,00 \\ 01\,00 & 01\,10 & 10\,00 & 01\,00 & 01\,00 \end{pmatrix},$$

$$D_3 : \begin{pmatrix} 10\,10 & 10\,10 & 10\,10 & 00\,00 & 00\,00 \\ 01\,01 & 01\,01 & 01\,01 & 00\,00 & 00\,00 \\ 01\,01 & 10\,10 & 00\,00 & 10\,10 & 00\,00 \\ 01\,10 & 01\,00 & 10\,00 & 01\,01 & 00\,00 \\ 01\,11 & 11\,00 & 01\,00 & 10\,00 & 10\,00 \\ 10\,10 & 00\,01 & 01\,00 & 01\,00 & 01\,00 \end{pmatrix}, \quad D_4 : \begin{pmatrix} 10\,10 & 10\,10 & 10\,10 & 00\,00 & 00\,00 \\ 01\,01 & 01\,01 & 01\,01 & 00\,00 & 00\,00 \\ 01\,01 & 10\,10 & 00\,00 & 10\,10 & 00\,00 \\ 01\,10 & 01\,00 & 10\,00 & 01\,01 & 00\,00 \\ 01\,11 & 11\,00 & 01\,00 & 10\,00 & 10\,00 \\ 11\,00 & 01\,11 & 01\,00 & 01\,00 & 01\,00 \end{pmatrix},$$

$$D_5 : \begin{pmatrix} 10\,10 & 10\,10 & 10\,10 & 00\,00 & 00\,00 \\ 01\,01 & 01\,01 & 01\,01 & 00\,00 & 00\,00 \\ 01\,01 & 10\,10 & 00\,00 & 10\,10 & 00\,00 \\ 11\,01 & 01\,00 & 11\,00 & 01\,01 & 00\,00 \\ 11\,11 & 01\,01 & 00\,00 & 10\,00 & 10\,00 \\ 10\,11 & 11\,00 & 10\,00 & 01\,00 & 01\,00 \end{pmatrix}, \quad D_6 : \begin{pmatrix} 10\,10 & 10\,10 & 10\,10 & 00\,00 & 00\,00 \\ 01\,01 & 01\,01 & 01\,01 & 00\,00 & 00\,00 \\ 01\,01 & 10\,10 & 00\,00 & 10\,10 & 00\,00 \\ 11\,01 & 01\,00 & 11\,00 & 01\,01 & 00\,00 \\ 11\,11 & 01\,01 & 00\,00 & 10\,00 & 10\,00 \\ 01\,00 & 01\,10 & 10\,00 & 01\,00 & 01\,00 \end{pmatrix},$$

$$D_7 : \begin{pmatrix} 10\,10 & 10\,10 & 10\,10 & 00\,00 & 00\,00 \\ 01\,01 & 01\,01 & 10\,00 & 10\,00 & 00\,00 \\ 11\,11 & 01\,10 & 01\,00 & 00\,10 & 00\,00 \\ 11\,01 & 01\,00 & 00\,01 & 01\,01 & 00\,00 \\ 10\,01 & 11\,01 & 00\,01 & 00\,00 & 10\,00 \\ 11\,00 & 01\,11 & 11\,00 & 01\,00 & 01\,00 \end{pmatrix}, \quad D_8 : \begin{pmatrix} 10\,10 & 10\,10 & 10\,10 & 00\,00 & 00\,00 \\ 01\,01 & 01\,01 & 10\,00 & 10\,00 & 00\,00 \\ 11\,11 & 01\,10 & 01\,00 & 00\,10 & 00\,00 \\ 11\,01 & 01\,00 & 00\,01 & 01\,01 & 00\,00 \\ 10\,11 & 00\,11 & 01\,01 & 00\,00 & 10\,00 \\ 00\,11 & 11\,01 & 01\,00 & 01\,00 & 01\,00 \end{pmatrix}.$$

Table 4: Generator matrices of additive weight-$\{6, 8\}$ codes in $D(0, 9 + 0) = H(9, 4)$.

$$\left(\begin{array}{cccccc|c} 00&21&21&10&00&10\\ 00&20&10&01&10&01\\ 00&12&01&01&01&01\\ \hline 20&22&20&00&00&00 \end{array}\right), \left(\begin{array}{cccccc|c} 00&21&21&10&00&10\\ 00&20&10&01&10&01\\ 00&13&01&01&01&11\\ \hline 20&20&20&00&00&00 \end{array}\right), \left(\begin{array}{cccccc|c} 00&21&21&10&00&10\\ 00&20&10&01&10&01\\ 00&13&01&01&01&11\\ \hline 20&22&00&02&00&00 \end{array}\right),$$

$$\left(\begin{array}{cccccc|c} 00&21&21&10&00&10\\ 00&20&10&01&10&01\\ 00&13&01&01&01&11\\ \hline 20&02&20&02&00&00 \end{array}\right), \left(\begin{array}{cccccc|c} 00&21&21&10&00&10\\ 00&20&10&01&10&01\\ 00&32&03&01&01&10\\ \hline 20&22&20&00&00&00 \end{array}\right), \left(\begin{array}{cccccc|c} 00&21&21&10&00&10\\ 00&20&10&01&10&01\\ 00&32&03&01&01&10\\ \hline 20&02&20&02&00&00 \end{array}\right),$$

$$\left(\begin{array}{cccccc|c} 00&21&21&10&00&10\\ 00&31&20&01&10&00\\ 00&21&33&01&01&01\\ \hline 20&22&20&00&00&00 \end{array}\right), \left(\begin{array}{cccccc|c} 00&21&10&10&10&10\\ 00&31&01&01&01&01\\ \hline 00&20&02&20&00&00\\ 00&02&22&02&00&00\\ 20&02&20&00&00&00 \end{array}\right), \left(\begin{array}{cccccc|c} 00&21&10&10&10&10\\ 00&12&11&01&01&01\\ \hline 00&20&02&20&00&00\\ 00&22&20&02&00&00\\ 20&02&20&00&00&00 \end{array}\right).$$

Table 5: Lengthenings of type $\mathbb{Z}_4^3\mathbb{Z}_2^1$ and type $\mathbb{Z}_4^2\mathbb{Z}_2^3$.

3.3 Lengthening to codes in Doob graphs of diameter 11 and 12. We aim to classify all additive codes of size 1024 with nonzero weights 6, 8, 10 in Doob graphs $D(m, n'+n'')$, $m > 0$, of diameter $2m + n' + n'' = 11$. If such a code C_{11} exists, then shortening it in one of the first m positions or two of the last $n' + n''$ positions leads to a weight-$\{6, 8\}$ code C_9 of size 64 in $D(m-1, n'+n'')$, $D(m, (n'-2)+n'')$ (if $n' \geq 2$), $D(m, (n'-1)+(n''-1))$ (if $n', n'' \geq 1$), or $D(m, n'+(n''-2))$ (if $n'' \geq 2$). As such codes C_9 exist only in $D(4, 1+0)$ and $D(3, 0+3)$, we conclude that the only option for C_{11} is $D(m, n'+n'') = D(5, 1+0)$. Now, our approach is quite straightforward. Starting with one of the six weight-$\{6, 8\}$ codes found in $D(4, 1+0)$, we extend the code to $D(5, 1+0)$ by adding 00 to the beginning of each codeword. Next, we add a row to the generator matrix in all possible ways and check that the resulting code has a larger cardinality (128 or 256 in the first iteration) and desired nonzero weights 6, 8, 10. After filtering only inequivalent representatives from the found collection of codes, we repeat the same procedure and repeat iterating until no new codes are found. Summarizing the results, we have found only codes of size 128 and 256, with weight distributions $\{0^1, 6^{42}, 8^{55}, 10^{30}\}$ and $\{0^1, 6^{54}, 8^{111}, 10^{90}\}$, respectively; as a corollary, we have Proposition 3.3 below. The check matrices of inequivalent representatives are given in Tables 5 and 6 (note that we do not claim that there are no other additive weight-$\{6, 8, 10\}$ codes of size at least 128 in $D(5, 1)$; our search was restricted only to those codes that have a shortening of size 64 in $D(4, 1)$).

Proposition 3.3. *In Doob graphs of diameter* 11*, there are no additive codes of size* 1024 *with weights* 6*,* 8*,* 10*.*

Corollary 3.4. *In Doob graphs $D(m, 11-2m)$, $m > 0$, there is no additive completely regular code C with intersection array $\{33, 30, 15; 1, 2, 15\}$.*

Proof. Since the given intersection array is the same as that of the punctured dodecacode D^- in $H(11, 4)$ and since the graphs $D(m, 11-2m)$ and $H(11, 4)$ have the same

$$\left(\begin{array}{ccccc|c} 00 & 21 & 10 & 10 & 10 & 10 \\ 00 & 31 & 01 & 01 & 01 & 01 \\ 21 & 11 & 11 & 10 & 00 & 01 \\ \hline 00 & 20 & 02 & 20 & 00 & 00 \\ 00 & 02 & 22 & 02 & 00 & 00 \end{array}\right), \left(\begin{array}{ccccc|c} 00 & 21 & 10 & 10 & 10 & 10 \\ 00 & 12 & 11 & 01 & 01 & 01 \\ 21 & 11 & 11 & 10 & 00 & 01 \\ \hline 00 & 20 & 02 & 20 & 00 & 00 \\ 00 & 22 & 20 & 02 & 00 & 00 \end{array}\right), \left(\begin{array}{ccccc|c} 00 & 21 & 21 & 10 & 00 & 10 \\ 00 & 20 & 10 & 01 & 10 & 01 \\ 00 & 12 & 01 & 01 & 01 & 01 \\ \hline 20 & 22 & 20 & 00 & 00 & 00 \\ 02 & 20 & 00 & 02 & 00 & 00 \end{array}\right)$$

$$\left(\begin{array}{ccccc|c} 00 & 21 & 21 & 10 & 00 & 10 \\ 00 & 20 & 10 & 01 & 10 & 01 \\ 00 & 13 & 01 & 01 & 01 & 11 \\ \hline 20 & 20 & 20 & 00 & 00 & 00 \\ 02 & 22 & 00 & 02 & 00 & 00 \end{array}\right), \left(\begin{array}{ccccc|c} 00 & 21 & 21 & 10 & 00 & 10 \\ 00 & 20 & 10 & 01 & 10 & 01 \\ 00 & 32 & 03 & 01 & 01 & 10 \\ \hline 20 & 22 & 20 & 00 & 00 & 00 \\ 02 & 20 & 00 & 02 & 00 & 00 \end{array}\right), \left(\begin{array}{ccccc|c} 00 & 21 & 21 & 10 & 00 & 10 \\ 00 & 31 & 20 & 01 & 10 & 00 \\ 00 & 21 & 33 & 01 & 01 & 01 \\ \hline 20 & 22 & 20 & 00 & 00 & 00 \\ 02 & 22 & 02 & 02 & 00 & 00 \end{array}\right),$$

$$\left(\begin{array}{ccccc|c} 00 & 21 & 10 & 10 & 10 & 10 \\ 00 & 31 & 01 & 01 & 01 & 01 \\ \hline 00 & 20 & 02 & 20 & 00 & 00 \\ 00 & 02 & 22 & 02 & 00 & 00 \\ 20 & 02 & 20 & 00 & 00 & 00 \\ 02 & 22 & 02 & 00 & 00 & 00 \end{array}\right), \left(\begin{array}{ccccc|c} 00 & 21 & 10 & 10 & 10 & 10 \\ 00 & 12 & 11 & 01 & 01 & 01 \\ \hline 00 & 20 & 02 & 20 & 00 & 00 \\ 00 & 22 & 20 & 02 & 00 & 00 \\ 20 & 02 & 20 & 00 & 00 & 00 \\ 02 & 22 & 02 & 00 & 00 & 00 \end{array}\right).$$

Table 6: Lengthenings of type $\mathbb{Z}_4^3\mathbb{Z}_2^2$ and type $\mathbb{Z}_4^2\mathbb{Z}_2^4$.

parameters as distance-regular graphs, the weight distributions of C and D^- coincide, see, e.g., [10, Proposition 1.21]. The weight distributions of the dual codes $C^\perp$ (with respect to the inner product (1)) and $D^{-\perp}$ also coincide by the MacWilliams transform [3, Theorem 6.6]. □

Proposition 3.5. *In Doob graphs of diameter* 12*, there are no additive codes of size* 4096 *with weights* 6*,* 8*,* 10*,* 12*.*

Proof. For the graph $D(m, 12-2m)$, $0 < m < 6$, the claim follows from Proposition 3.3 (indeed, if we have a code with required parameters, then shortening it in the last coordinate leads to a code of size 1024 in $D(m, 11-2m)$, which does not exist).

For the case $m = 6$, we consider an additive code of type $\mathbb{Z}_4^\delta\mathbb{Z}_2^\gamma$ in $D(6, 0)$, with weights 6, 8, 10, 12. The type-$\mathbb{Z}_2^{\gamma+\delta}$ subcode has Doob distance at least 6, and it is equivalent to an additive $(6, 2^{\gamma+\delta}, 3)_4$ code, a 4-ary code of length 6. In its turn, by concatenation (mapping the 4 quaternary symbols to the binary triples 000, 011, 101, 110), each of such codes can be mapped to a binary linear $(18, 2^k, \{6, 8, 10, 12\})$ code, $k = \gamma + \delta$. Such codes are classified with the software [4]: there are 2859, 258, and 3 equivalence classes of such codes for $k = 6, 7, 8$, respectively. By inverse concatenation, we get 646 equivalence classes of additive $(6, 2^6, 3)_4$ codes (including one distance-4 code, known as the hexacode), see [8, Appendix B.1], 14 equivalence classes of additive $(6, 2^7, 3)_4$ codes, see [8, Appendix B.2], and no additive $(6, 2^8, 3)_4$ codes (only 626 of the 2859 binary $(18, 2^6, \{6, 8, 10, 12\})$ codes can be represented as quaternary by concatenation; on the other hand, some codes can be represented in more than one way; that is why we say that the number of equivalence classes of quaternary codes is larger than 626). So, now we know all additive distance-6 codes of type $\mathbb{Z}_2^k$, $k \geq 6$ in $D(6, 0)$. To confirm the results,

$n\backslash k$	0	1	2	3	4	5	6	7	8
3	1	1	1	0					
4	1	2	5	3	1	0			
5	1	3	14	32	40	9	1	0	
6	1	4	30	181	885	1660	646	14	0

Table 7: The number $N(n,k,3)$ of equivalence classes of additive $(n,2^k,\geq 3)_4$ codes.

we have made a search similar to that in Section 2.3, see Table 7.

In the case $k=6$, we have $\gamma=0$ and $\delta=6$, and for a putative additive code C of type $\mathbb{Z}_4^6$ in $D(6,0)$ its type-$\mathbb{Z}_4^2$ subcode is exactly $2C$. So, we can start with a generator matrix of $2C$ (which comes from a binary generator matrix of an additive $(6,2^6,3)_4$ code by replacing 1s by 2s) and try to lift it row-by-row. From the 646 additive $(6,2^6,3)_4$ codes we found, there are only two codes such that any row of the generated matrix (but not all six rows) can be lifted, with (additive) generator matrices

$$\begin{pmatrix} 01\ 00\ 10\ 00\ 00\ 10\\ 00\ 00\ 00\ 10\ 10\ 10\\ 00\ 00\ 01\ 01\ 00\ 01\\ 00\ 01\ 00\ 01\ 01\ 00\\ 10\ 00\ 11\ 01\ 01\ 10\\ 00\ 10\ 10\ 00\ 10\ 10 \end{pmatrix}, \qquad \begin{pmatrix} 10\ 01\ 01\ 01\ 01\ 11\\ 00\ 10\ 01\ 01\ 00\ 01\\ 00\ 01\ 10\ 00\ 01\ 01\\ 00\ 00\ 01\ 10\ 01\ 10\\ 00\ 01\ 00\ 01\ 10\ 10\\ 01\ 00\ 00\ 01\ 01\ 01 \end{pmatrix}$$

(the second code has distance 4 and is equivalent to the well-known hexacode). By lifting row-by-row (and keeping only inequivalent codes at each step), we find that for each of the two matrices, it is not possible to lift the first 3 rows to produce a code of type $\mathbb{Z}_4^3\mathbb{Z}_2^3$ in $D(6,0)$. It follows that a distance-6 even-weight code of type $\mathbb{Z}_4^6$ does not exist in $D(6,0)$.

For the type $\mathbb{Z}_4^5\mathbb{Z}_2^2$, it is slightly more complicated. The reason is that $2C$ is of type $\mathbb{Z}_2^5$, which is not the whole type-$\mathbb{Z}_2^7$ subcode of C. So, if we have a putative type-$\mathbb{Z}_2^7$ subcode (from a 4-ary additive $(6,2^7,3)_4$ code) where the rows of some concrete generator matrix cannot be lifted, this does not lead to a direct contradiction. The strategy is to try to lift each nonzero codeword of the putative type-$\mathbb{Z}_2^7$ subcode. For each of the 14 candidates C for such a subcode, obtained from the 14 additive $[6,3.5,3]_4$ codes by replacing 1s by 2s, we try to lift each nonzero codeword. A codeword b is called *liftable* if there is another word c such that $b-2c$ and the additive code obtained as the additive closure of $C\cup\{c\}$ has only (Doob) weights 0, 6, 8, 10, 12 (not necessarily all of them). Clearly, if there is a type-$\mathbb{Z}_4^5\mathbb{Z}_2^2$ code with required weights, then its type-$\mathbb{Z}_2^7$ subcode must have at least $31=2^5-1$ liftable codewords. However, among the 14 candidates for such a subcode, 4 codes have only 7 liftable codewords and 10 codes have only 1 liftable codeword. This means that a required code does not exist. □

4 Conclusion and open problems. We have shown that the punctured dodecacode is characterized by its weight distribution and that it is not $\mathbb{F}_4$-linear. It is the case

$m = 2$ of an infinite family of putative uniformly packed codes introduced in [2]. The case $m = 3$ of that family would lead us to consider a dual code D of binary dimension $2(2m + 1) = 2 \times 7 = 14$ and length 43. Its weight distribution would be, in Magma notation:

```
[ <0, 1>, <28, 3612>, <32, 8127>, <36, 4644> ].
```

While this code would still be even and trace Hermitian self-orthogonal, the classification of self-orthogonal codes either for the Hermitian or trace Hermitian codes is far beyond the tables in [5] and [7]. A computer search for an analog of the dodecacode with length 44 and a cyclic automorphism group has failed to produce an example.

REFERENCES.

[1] URL: `https://mathworld.wolfram.com/Shi-Krotov-SoleGraph.html`.

[2] L. A. BASSALYGO, G. V. ZAITSEV, and V. A. ZINOVIEV. On uniformly packed codes. *Probl. Inf. Transm.*, 10(1):6–9, 1974. Translated from Probl. Peredachi Inf., 10(1): 9–14, 1974.

[3] E. A. BESPALOV and D. S. KROTOV. Some completely regular codes in Doob graphs. In M. SHI and P. SOLÉ, editors, *Completely Regular Codes in Distance Regular Graphs*, chapter 6, pages 379–448. CRC Press, 2025.

[4] I. BOUYUKLIEV and S. BOUYUKLIEVA. QextNewEdition. URL: `http://www.moi.math.bas.bg/moiuser/~data/Software/QextNewEdition`.

[5] I. BOUYUKLIEV and P. R. J. ÖSTERGÅRD. Classification of self-orthogonal codes over F_3 and F_4. *SIAM Journal on Discrete Mathematics*, 19(2):363–370, 2005.

[6] A. R. CALDERBANK, E. M. RAINS, P. M. SHOR, and N. J. A. SLOANE. Quantum error correction via codes over GF(4). *IEEE Trans. Inf. Theory*, 44(4):1369–1387, 1998.

[7] L. E. DANIELSEN and M. G. PARKER. On the classification of all self-dual additive codes over $GF(4)$ of length up to 12. *Journal of Combinatorial Theory, Series A*, 113(7):1351–1367, 2006.

[8] M. GRASSL, D. KROTOV, L. SOK, and P. SOLÉ. The punctured dodecacode is unique. *arXiv preprint arXiv:2601.08008v1*, 2026.

[9] D. S. KROTOV. Perfect codes in Doob graphs. *Des. Codes Cryptography*, 80(1):91–102, 2016.

[10] D. S. KROTOV and V. N. POTAPOV. Completely regular codes and equitable partitions. In M. SHI and P. SOLÉ, editors, *Completely Regular Codes in Distance Regular Graphs*, chapter 1, pages 1–84. CRC Press, 2025.

[11] F. J. MACWILLIAMS, A. M. ODLYZKO, N. J. A. SLOANE, and H. N. WARD. Self-dual codes over $GF(4)$. *Journal of Combinatorial Theory, Series A*, 25(3):288–318, 1978.

[12] M. SHI, D. S. KROTOV, and P. SOLÉ. A new distance-regular graph of diameter 3 on 1024 vertices. *Des. Codes Cryptography*, 87(9):2091–2101, 2019.

[13] M. SHI and P. SOLÉ, editors. *Completely Regular Codes in Distance Regular Graphs*. CRC Press, Boca Raton FL, 2025.

Markus Grassl
International Centre for Theory of Quantum Technologies
University of Gdansk, Gdansk, Poland
e-mail: `markus.grassl@ug.edu.pl`

Denis Krotov
Sobolev Institute of Mathematics
Novosibirsk 630090, Russia
e-mail: `dk@ieee.org`

Lin Sok
School of Physical and Mathematical Sciences
Nanyang Technological University
21 Nanyang Link
Singapore 637371, Singapore
e-mail: lin.sok@ntu.edu.sg

Patrick Solé
I2M (Aix Marseille Univ, CNRS)
Marseilles, France
e-mail: sole@enst.fr

СКЪСЕНИЯТ ДОДЕКАКОД Е ЕДИНСТВЕН

M. Grassl, D. Krotov, L. Sok и P. Solé

Абстракт

Скъсеният додекакод е адитивен 4-ичен код с дължина 11 и разстояние 5, който е равномерно опакован. Показваме, че всеки код със същото разпределение на теглата е еквивалентен на него. Освен това е установено, че този код е нелинеен. Също така доказваме несъществуването на аналози на додекакода и на скъсения додекакод в графите на Doob. За тази цел класифицираме двутеглови кодове с тегла 6 и 8 в графи на Doob и в 4-ични графи на Хеминг с диаметър 9, както и съответните силно регулярни графи.

Ключови думи: додекакод, адитивен код, следова ермитова двойственост, равномерно опакован код, напълно регулярен код, граф на Doob, силно регулярен граф.

МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2026
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2026
Proceedings of the Fifty-Fifth Spring Conference
of the Union of Bulgarian Mathematicians
Tryavna, Bulgaria, April 5–9, 2026

ON THE MAXIMAL LENGTH OF NEAR-MDS CODES [1]

Ivan Landjev and Assia Rousseva

Abstract

This paper summarizes the known results about near-MDS codes proved in the past thirty years. The main focus is put on the problem of determining the value of the function $m'(k,q)$ defined as the maximal length of a near-MDS code of dimension k over the field with q elements. For dimensions $k > q+2$ we improve the upper bound $m'(k,q) \leq 2q+k-2$ which follows from the nonexistence of maximal arcs over fields of odd characteristic. In analogy with the main conjecture for MDS codes we formulate some conjectures on the exact value of $m'(k,q)$.

2020 Mathematics Subject Classification: 94B05, 51E20, 51E21, 94B65.

Key words: near-MDS codes, MDS codes, elliptic curves, $(n,3)$-arcs, n-tracks, projective geometries, designs.

1 Introduction. Near-MDS codes have been introduced in 1995 in [13]. They are defined by weakening some restrictions in the definition of the MDS codes. The most popular definition is via generalized Hamming weights. The r-th generalized Hamming weight $d_r(C)$ of a linear code C is defined as the size of the smallest support of an r-dimensional subcode of C. A linear $[n,k]_q$-code C is called a near-MDS code if

$$d_i(C) = n-k+i \text{ for } i = 2,\ldots,k, \;\; d_1(C) = n-k.$$

Of course, it is enough to require $d_1(C) = n-k$ and $d_2(C) = n-k+2$. The remaining conditions for $i = 3,\ldots,k$ are satisfied automatically. From the properties of the generalized Hamming weights one can easily deduce that the dual of a near-MDS code is again a near-MDS code. This follows immediately from the fact that for every linear code

$$\{d_i(C) \mid i = 1,\ldots,k\} \cup \{d_j(C^{\perp}) \mid j = 1,\ldots,n-k\} = \{1,\ldots,n\}.$$

The following propositions characterize near-MDS codes and can serve as alternative definitions. The proofs can be found in [13].

Proposition 1.1. *A linear $[n,k]_q$-code C is a near-MDS code if and only if any parity-check matrix H_C of C satisfies the conditions:*

[1]The research of the first author was supported by by the Bulgarian National Science Research Fund under Contract KP-06-N72/6-2023. The second author was supported by the Research Fund of Sofia University under Contract 80-10-14/21.05.2025

https://doi.org/10.55630/mem.2026.55.405-413

(1) any $n-k-1$ columns of H_C are linearly independent;

(2) there exist $n-k$ linearly dependent columns;

(3) any $n-k+1$ columns of H_C are of rank $n-k$.

Proposition 1.2. *A linear $[n,k]_q$-code C is near-MDS if and only if any generator matrix G_C of C satisfies the conditions:*

(1) any $k-1$ columns of G_C are linearly independent;

(2) there exist k linearly dependent columns;

(3) any $k+1$ columns of G_C are of rank k.

Proposition 1.3. *A linear $[n,k]_q$ code is a near-MDS code if and only if $d(C)+d(C^\perp)=n$.*

Closely related to near-MDS codes are the so-called almost-MDS codes introduced by de Boer [11, 12]. Almost-MDS codes are defined as $[n,k]_q$-codes with minimum distance $d=n-k$, or, in other words, as codes with Singleton defect 1. Not every almost-MDS code is near-MDS, which is demonstrated by the following example.

Consider a MDS-code C with parameters $[n,k]_q$ defined by a parity-check matrix H. Extend H by a row of weight less than $k-1$. Clearly, this row is not a linear combination of the rows of H. Denote the obtained matrix by H' and let C' be the code having H' as a parity=check matrix. By construction, the code C' has parameters $[n',k',d']$ where $n'=n$, $k'=k-1$, $d'\geq n'-k'$. The last inequality follows from the fact that every $d'-1=n'-k'-1=n-k$ columns of H' are linearly independent. Obviously, $d(C'^\perp)<k-1=k'$ and C' is not an MDS-code. Hence $d(C')=n'-k'$ and C' is an $[n',k',n'-k']$-code which is not a near-MDS code.

However, for large n every almost-MDS code is also a near-MDS code.

Proposition 1.4. *If $n>k+q$ every $[n,k,n-k]_q$-code is a near-MDS code.*

The weight distribution of a near-MDS code can be determined up to a single parameter. In the theorem below this parameter is taken to be the number of words of minimal weight.

Theorem 1.5. *Let C be an $[n,k]_q$ near-MDS code. Let (A_i) and (A'_i) be the spectra of C and $C^\perp$, respectively. Then*

$$A_{n-k+s}=\binom{n}{k-s}\sum_{j=0}^{s-1}(-1)^j\binom{n-k+s}{j}(q^{s-j}-1)+(-1)^s\binom{k}{s}A_{n-k},$$

where $s=1,\ldots,k$, and

$$A'_{k+s}=\binom{n}{k+s}\sum_{j=0}^{s-1}(-1)^j\binom{k+s}{j}(q^{s-j}-1)+(-1)^s\binom{n-k}{s}A'_k,$$

where $s=1,\ldots,n-k$.

For almost-MDS codes the situation is more complicated. The numbers of the parameters depends on the Singleton defect of the orthogonal code (cf. [18]). Theorem 1.5 gives a simple upper bound on the number of words of minimal weight.

Corollary 1.6. *For an $[n,k]_q$ near-MDS code*

$$A_{n-k} \le \binom{n}{k-1}\frac{q-1}{k},$$

with equality if and only if $A_{n-k+1}=0$. By duality,

$$A'_k \le \binom{n}{k+1}\frac{q-1}{n-k},$$

with equality if and only if $A'_{k+1}=0$.

It is interesting to find near-MDS codes with $A_{n-k+1}=0$. In such a case it is easy to see that the existence of an $[n,k,n-k]$ near-MDS code is equivalent to that of a $(k-1)$-$(n,k,1)$-design or a Steiner system $S(k-1,k,n)$. Apart from the ternary Golay code, there are just a few examples of such near-MDS codes. All of them are of dimension $k=3$. It looks likely that for $k>3$, $q>3$, such near-MDS codes do not exist.

2 The geometric view at near-MDS codes. It is known that with every $[n,k,d]_q$-code of full length one can associate a multiset of points in $\mathrm{PG}(k-1,q)$ (possibly in a non-unique way) so that isomorphic codes are associated with projectively equivalent multisets (cf. [16]). This implies that the existence of an $[n,k]_q$ near-MDS code is equivalent to that of a set $\mathcal{K}$ of points in $\mathrm{PG}(k-1,q)$ with the following properties:

(1) every $k-1$ points from $\mathcal{K}$ are in general position (generate a hyperplane);

(2) there exist k points from $\mathcal{K}$ that lie in a hyperplane;

(3) every $k+1$ points from $\mathcal{K}$ generate $\mathrm{PG}(k-1,q)$.

In particular, if $k=3$ a near-MDS code is equivalent to an $(n,3)$-arc in $\mathrm{PG}(2,q)$. The nonexistence of maximal $(n,3)$-arcs, i.e. arcs with $n=2q+3$ for $q>3$ was ruled out originally by Thas [28]. This result is a part of a more general theorem about the nonexistence of maximal arcs in $\mathrm{PG}(2,q)$ for odd q proved by Ball, Blokhuis and Mazzocca [4, 5]. Since every $(2q+2,3)$-arc is extendable one gets that the size of an $(n,3)$-arc is bounded by $n\le 2q+1$. This provides the best upper bound on the length of a near-MDS code (cf. Theorem 4.1(vi)).

This bound is attained only for $q=4,5,7$. For $q=4$ there exist three non-equivalent $(9,3)$-arcs: the complement of a triangle, the complement of an oval and two secants, and the Hermitian curve, or, equivalently, a triangle without the vertices. For $q=5$ there exist two non-equivalent $(11,3)$-arcs: the complement of four lines in general position and two additional points (for which there are two non-equivalent choices) (cf. [22]). For $q=7$ there exists exactly one $(15,3)$-arc which is obtained as the intersection points of the ten lines in the Desarguesian configuration that are not from the configuration (cf. also [26]). For larger values of q we have strict inequality. It is conjectured that

q	4	5	7	8	9	11	13
n	9	11	15	15	17	21	23
q	17	19	23	25	27	29	31
n	28–33	31–39	37–47	38–51	42–55	44–59	46–63

Table 1: Lower and upper bounds on the size of an $(n, 3)$-arc in $\mathrm{PG}(2, q)$

$q = 4, 5, 7$ are the only values of q for which $(2q + 1, 3)$-arcs in $\mathrm{PG}(2, q)$ are known. The largest known sizes for $(n, 3)$-arcs in $\mathrm{PG}(2, q)$, as well as upper bounds are given in the table below (cf. also [7, 10]).

Almost-MDS codes are equivalent to so-called n-tracks. An n-track is a set of points in $\mathrm{PG}(r, q)$ such that every r of them are in general position. Tables containing exact values and bounds on the maximal size of an n-track are contained in [3, 11, 12, 21].

3 Near-MDS codes over small fields. With no loss of generality, we consider only codes with $k \leq n/2$. Near-MDS codes of dimension greater than $n/2$ are obtained as orthogonal to near-MDS codes with $k \leq n/2$. This implies that from now on we can assume that $k \leq 2q$ and $n \geq 2q$.

It is known that all binary MDS codes are trivial. For near-MDS codes we have some non-trivial examples, but in fact we can list all near-MDS codes. These are the extended Hamming $[8, 4, 4]$-code, the simplex $[7, 3, 4]$-code, the $[6, 3, 3]$-codes obtained by shortening the Hamming code of length 7, as well as, several trivial codes of dimensions one and two.

In the ternary case, we have one $[9, 3, 6]_3$-code associated with the affine plane $\mathrm{AG}(2, 3)$, one $[10, 4, 6]_3$-code, one $[11, 5, 6]_3$-code (the orthogonal to the Golay code) and one $[12, 6, 6]_3$-code (the extended ternary Golay code).

For codes over $\mathbb{F}_4$, there exist three non-isomorphic $[9, 3, 6]_4$-codes, associated with the three non-equivalent $(9, 3)$-arcs in $\mathrm{PG}(2, 4)$, two $[10, 4, 6]_4$-codes, exactly one $[11, 5, 6]_4$-code and exactly one $[12, 6, 6]_4$-code [14, 15]. It should be noted that the $[12, 6, 6]_4$ code was constructed by Dumer and Zinoviev in [17] as the first member of an infinite family of uniformly packed codes. Remarkably, this code yields a cascade representation of the extended binary Golay code.

There exist two non-isomorphic $[11, 3, 8]_5$ codes associated with the two $(11, 3)$-arcs in $\mathrm{PG}(2, 5)$. One of them extends to a $[12, 4, 8]_5$ code which cannot be further extended. A $[12, 6, 6]_5$-code does exist. It was constructed in [9] using a computer. Later on, Abatangelo and Larato [2] constructed six non-isomorphic codes with these parameters. They extended by two points the elliptic curve Γ_6 of degree 6 in $\mathrm{PG}(5, q)$ arising from a non-singular cubic curve of $\mathrm{PG}(2, q)$ via the canonical Veronese embedding

$$\nu : (X : Y : Z) \to (X^2 : XY : Y^2 : XZ : YZ : Z^2).$$

In [27] the authors determine the maximal length of $[n, 4, n - 4]_{11}$-code which turns out to be 20. For $[n, 3, n - 3]_{11}$ the maximal length is 21 and is equal to the maximal size of an $(n, 3)$-arc in $\mathrm{PG}(2, 11)$. In the same paper the authors investigate also NMDS

codes with parameters

$$[13,5,8]_7,\ [14,5,9]_8,\ [15,4,11]_9.$$

4 Near-MDS codes of maximal length. As with MDS-codes, the main problem for near-MDS codes is to determine the maximal length of such a code for a fixed dimension k and a fixed ground field $\mathbb{F}_q$. In analogy with MDS codes, we denote by $m'(k,q)$ the maximum possible length for which there exists a $[n,k]_q$ near-MDS code. The following theorem summarizes some straightforward observations about $m'(k,q)$.

Theorem 4.1. *Let k be a positive integer and let q be a prime power. Then*

(i) $m'(2,q) = 2q+2$;

(ii) $m'(k,q) \leq m'(k-\alpha,q)+\alpha$, *for every positive integer* α *with* $\alpha \leq k$;

(iii) $m'(k,q) = k+1$ *for* $k > 2q$;

(iv) $m'(2q,q) = 2q+2$;

(v) $m'(2q-1,q) = 2q+1$;

(vi) $m'(k,q) \leq 2q+k-2$.

Near-MDS codes with parameters $[n,k]_q$ can be constructed from elliptic curves over $\mathbb{F}_q$ having exactly n rational points [29] (cf. also [1, 2, 19, 20]). Such codes are referred to as elliptic codes. For every prime power $q = p^r$, p a prime, near-MDS codes exist for lengths up to $N_q(1)$, where $N_q(1)$ denotes the maximum number of $\mathbb{F}_q$-rational points an elliptic curve defined over $\mathbb{F}_q$ can have. By a result of Waterhouse [30], we know that for every $q = p^e$

$$N_q(1) = \begin{cases} q + \lfloor 2\sqrt{q} \rfloor & \text{for } p \mid \lceil 2\sqrt{q} \rceil \text{ and odd } e, \\ q + \lfloor 2\sqrt{q} \rfloor + 1 & \text{otherwise.} \end{cases}$$

This gives a lower bound on $m'(k,q)$: $m'(k,q) \geq N_q(1)$. Due to extensive computational work by Bartoli, Marcugini, Milani and Pambianco [8, 15, 25, 27], the exact values of $m'(k,q)$ were determined for all fields of order $q \leq 9$, as well as lower and upper bounds on the size of the longest near-MDS code for some larger fields. In particular, in [25] the authors determine the three exact values

$$m'(5,8) = 15,\ \ m'(4,9) = 16, m'(5,9) = 16.$$

By duality, they also determine the values of $m'(k,8)$ for $k = 10,11,12$, and of $m'(k,9)$ for $k = 12,13,14$. Even more results were obtained for the case of dimension three, which corresponds to the problem of the maximal size of an $(n,3)$-arc in $\mathrm{PG}(2,q)$ (cf. [10, 23, 26, 24]). These results are summarized in the table below.

q / k	2	3	4	5	7	8	9	11	13
2	6	8	10	12	16	18	20	24	28
3	7	9	9	11	15	15	17	21	23
4	8	10	10	12	14	16	16	20-21	21-24
5		11	11	11	13	15	16	18-22	21-25
6		12	12	12	13	14	16	18-23	21-26
7			9	11	14	15	17	18-24	21-27
8			10	12	13	16	18	18-25	21-28
9				11	13	14	19	19-26	21-29
10				12	14	15	20	20-27	21-30
11					14	15	16	18-28	21-31
12					15	16	16	18-29	21-32
13					15	15	16	18-30	21-33
14					16	16	17	18-31	21-34
15						17	17	18-32	21-35
16						18	18	18-33	21-36

Table 2: Exact values and bounds on $m'(k,q)$ for small fields $\mathbb{F}_q$, $q \leq 13$

5 An upper bound on the maximal length of a near-MDS code. According to Theorem 4.1(vi), we have $m'(k,q) \leq 2q+k-2$. It can be seen from the table above that equality is achieved just for several pairs (k,q). The following theorem gives an improvement over Theorem 4.1(vi) for sufficiently large dimensions.

Theorem 5.1. *There exist no $[2q+k-2,k]_q$ near-MDS codes for $k \geq q+2$ and $q \geq 7$.*

Proof. We are going to use the geometric interpretation of near-MDS codes. Fix an integer $k > q+2$. Let $\mathcal{K}$ be an arc with $2q+k-2$ points in $\mathrm{PG}(k-1,q)$, associated with a $[2q+k-2,k]_q$ near-MDS code. Furthermore, let $P_1,\ldots,P_{k-2}$ be points from $\mathcal{K}$. By the properties of the arcs associated with near-MDS codes, these $k-2$ points are in general position. Without loss of generality we can take $P_i = (0,\ldots,1,0,\ldots,0)$, where the only unit is in position i. Set

$$\begin{aligned} S &= \langle P_1, P_2, \ldots, P_{k-2}\rangle, \\ S_i &= \langle P_1,\ldots,P_{i-1},P_{i+1},\ldots,P_{k-2}\rangle, \quad i=1,\ldots,k-2. \end{aligned}$$

Clearly S is the hyperline defined by $x_{k-1} = x_k = 0$, and S_i are the subspaces defined by $x_i = x_{k-1} = x_k = 0$, $i = 1,\ldots,k-2$. Obviously, $\dim S = k-3$, and $\dim S_i = k-4$. There exists a point Q that is not contained in any of the subspaces S_i, for example $Q = (1,\ldots,1,0,0)$.

There exists a plane π which meets S only in the point Q, i.e. $\pi \cap S = \{Q\}$ (in fact, there exist many such planes). It is clear that $\pi \cap S_i = \varnothing$. Note that from the properties of the near-MDS codes and the arcs associated with them it follows that $|\mathcal{K} \cap \pi| \leq 3$.

Now consider projections φ_i, $i = 1, \ldots, k-2$, from each S_i to π given by

$$\varphi_i \colon \begin{cases} \mathcal{P} \setminus S_i & \to \quad \pi \\ P & \to \quad \langle S_i, P \rangle \cap \pi, \end{cases}$$

where $\mathcal{P}$ is the set of points of $\mathrm{PG}(k-1,q)$. Obviously, all induced arcs $\mathcal{K}^{\varphi_i}$ are plane arcs with parameters $(2q+1, 3)$.

The arcs $\mathcal{K}^{\varphi_i}$ are projective; otherwise, we easily get a contradiction since there exists a subspace of projective dimension $k-3$ (a hyperline) containing $k-1$ points.

If $P \in \mathcal{K} \cap \pi$, then P is contained in all induced arcs. Obviously $Q = S \cap \pi$ is also contained in all arcs $\mathcal{K}^{\varphi_i}$. Note that there are at most three such points. If R is a point from π which is contained neither in $\mathcal{K}$ nor in S, then it is contained in at most two of $\mathcal{K}^{\varphi_i}$ (since a hyperplane contains at most k points from $\mathcal{K}$). Counting the pairs $(P, \mathcal{K}^{\varphi_i})$ with $P \in \mathcal{K}^{\varphi_i}$ in two possible ways, we get

$$(k-2)(2q+1) \leq 2(q^2+q-3) + 4(k-2),$$

whence $k \leq q+4$, a contradiction. Now it remains to use Theorem 4.1(ii) to obtain the nonexistence for all dimensions $k > q+4$. □

Let us note that the proof of the nonexistence of $(2q+1, 3)$-arcs would immediately imply the nonexistence of $[2q+k-2, k]_q$ near-MDS codes. All numerical evidence suggests that this is true for all $q \geq 8$, but no proof of the nonexistence of $(2q+1, 3)$-arcs in $\mathrm{PG}(2,q)$ for large q seems to be known for the time being. There is a problem for $(n, 3)$-arcs in $\mathrm{PG}(2,q)$ suggested by A. Blokhuis asking to determine a constant c such that $n/q < c < 2$ for q large enough, or a construction where $n/q > c > 1$ [6].

We finish with two conjectures for near-MDS codes that are similar to the famous Main Conjecture for MDS codes.

Conjecture 5.2 (Weak Main Conjecture for NMDS codes)**.** *For all positive integers k and all prime powers $q \geq 5$ it holds that $m'(k,q) \leq 2(q+1)$.*

Conjecture 5.3 (Strong Main Conjecture for NMDS codes)**.** *There exists a universal constant c (not depending on q) such that $m'(k,q) \leq N_q(1) + c$.*

REFERENCES.

[1] V. ABATANGELO and B. LARATO. Near-MDS codes arising from algebraic curves. *Discrete Mathematics*, 301(1):5–19, 2005.

[2] V. ABATANGELO and B. LARATO. Elliptic near-MDS codes. *Designs, Codes and Cryptography*, 46:167–174, 2008.

[3] T. I. ALDERSON and A. A. BRUEN. Maximal AMDS codes. *Applicable Algebra in Engineering, Communication and Computing*, 19(2):87–98, 2008.

[4] S. BALL and A. BLOKHUIS. An easier proof of the maximal arcs conjecture. *Proceedings of the American Mathematical Society*, 126:3377–3380, 1998.

[5] S. BALL, A. BLOKHUIS, and F. MAZZOCCA. Maximal arcs in desarguesian planes of order q do not exist. *Combinatorica*, 17:31–47, 1997.

[6] S. BALL and J. W. P. HIRSCHFELD. Bounds on (n,r)-arcs and their application to linear codes. *Finite Fields and Their Applications*, 11:326–336, 2005.

[7] SIMEON BALL. Table of bounds on three dimensional linear codes or (n,r)-arcs in $\mathrm{PG}(2,q)$. URL: `https://web.mat.upc.edu/simeon.michael.ball/codebounds.html`.

[8] D. BARTOLI, S. MARCUGINI, and F. PAMBIANCO. The non-existence of some NMDS codes and the extremal sizes of complete $(n, 3)$-arcs in $PG(2, 16)$. *Designs, Codes and Cryptography*, 72(1):129–134, 2014.
[9] I. BOUYUKLIEV and J. SIMONIS. Some new results on optimal codes over $\mathbb{F}_5$. *Designs, Codes and Cryptography*, 30:97–111, 2003.
[10] M. BROWN. New lower bounds on the size of (n, r)-arcs in PG$(2, q)$. *Journal of Combinatorial Designs*, 27:682–687, 2019.
[11] M. de BOER. Almost MDS codes. *Designs, Codes and Cryptography*, 9(2):143–155, 1996.
[12] M. de BOER. *Codes: Their Parameters and Geometry*. PhD thesis, Eindhoven University of Technology, 1997.
[13] S. DODUNEKOV and I. LANDJEV. On near-MDS codes. *Journal of Geometry*, 54:30–43, 1995.
[14] S. DODUNEKOV and I. LANDJEV. On the quaternary $[11, 6, 5]$ and $[12, 6, 6]$ codes. In D. GOLLMANN, editor, *Applications of Finite Fields*. Volume 59, IMA Conference Series, pages 75–84. Clarendon Press, Oxford, 1996.
[15] S. DODUNEKOV and I. LANDJEV. Near-MDS codes over some small fields. *Discrete Mathematics*, 213:55–65, 2000.
[16] S. DODUNEKOV and J. SIMONIS. Codes and projective multisets. *Electronic Journal of Combinatorics*, 5:R37, 1998.
[17] I. I. DUMER and V. A. ZINOVIEV. Some new maximal codes over GF(4). *Problems of Information Transmission*, 14:24–34, 1978.
[18] A. FALDUM and W. WILLEMS. Codes of small defect. *Designs, Codes and Cryptography*, 10:341–350, 1997.
[19] M. GIULIETTI. On the extendability of near-MDS elliptic codes. *Applicable Algebra in Engineering, Communication and Computing*, 15(1):1–11, 2004.
[20] M. GIULIETTI and F. PASTICCI. On the completeness of certain n-tracks arising from elliptic curves. *Finite Fields and Their Applications*, 13:988–1000, 2007.
[21] J. W. P. HIRSCHFELD and L. STORME. The packing problem in statistics, coding theory and finite projective spaces: update 2001. In *Finite Geometries: Proceedings of the Fourth Isle of Thorns Conference*, volume 3 of *Developments in Mathematics*, pages 201–246. Kluwer Academic Publishers, 2001.
[22] I. LANDJEV. The geometry $(n, 3)$-arcs in the projective plane of order 5. In *Proc. Sixth Workshop on ACCT*, pages 170–175, Sozopol, 1996.
[23] S. MARCUGINI, A. MILANI, and F. PAMBIANCO. Maximal $(n, 3)$-arcs in PG$(2, 11)$. *Discrete Math.*, 208/209:421–426, 1999.
[24] S. MARCUGINI, A. MILANI, and F. PAMBIANCO. Maximal $(n, 3)$-arcs in PG$(2, 13)$. *Discrete Math.*, 294:139–145, 1999.
[25] S. MARCUGINI, A. MILANI, and F. PAMBIANCO. NMDS codes of maximal length over F_q, $8 \leq q \leq 11$. *IEEE Transactions on Information Theory*, 48(4):963–966, 2002.
[26] S. MARCUGINI, A. MILANI, and F. PAMBIANCO. Classification of the $(n, 3)$-arcs in PG$(2, 7)$. *J. Geometry*, 80:179–184, 2004.
[27] S. MARCUGINI, A. MILANI, and F. PAMBIANCO. Classification of linear codes exploiting an invariant. *Contributions to Discrete Math.*, 1(1):1–7, 2006.
[28] J. A. THAS. Some results concerning $\{(q+1)(n-1); n\}$-arcs in finite projective planes of order q. *Journal of Combinatorial Theory, Series A*, 19:228–232, 1975.
[29] M. A. TSFASMAN and S. G. VLADUT. *Algebraic-Geometric Codes*. Kluwer Academic Publishers, Amsterdam, 1991.
[30] W. C. WATERHOUSE. Abelian varieties over finite fields. *Annales Scientifiques de l'École Normale Supérieure*, 2:521–560, 1969.

Ivan Landjev
Institute of Mathematics and Informatics
Bulgarian Academy of Sciences
Acad. G. Bonchev Str., Bl. 8
1113 Sofia, Bulgaria
e-mail: ivan@math.bas.bg

Assia Rousseva
Sofia University "St. Kliment Ohridski"
Faculty of Mathematics and Informatics,
James Bourchier Blvd, 5
1126 Sofia, Bulgaria
e-mail: assia@fmi.uni-sofia.bg

ВЪРХУ МАКСИМАЛНАТА ДЪЛЖИНА НА ПОЧТИ-МДР КОДОВЕ

Иван Ланджев и Ася Русева

Абстракт

В тази статия правим обзор на резултатите за почти-МДР кодове, получени през последните 30 години. Фокусът е поставен върху задачата за определяне на точната стойност на функцията $m'(k,q)$, дефинирана като максималната дължина на почти-МДР код с размерност k над поле с q елемента. За размерности $k > q+2$ ние подобряваме горната граница $m'(k,q) \leq 2q+k-2$, която следва от несъществуването на максимални арки над полета с нечетна характеристика. Подобно на основната хипотеза за МДР кодове, ние формулираме няколко хипотези за точната стойност на функцията $m'(k,q)$.

Ключови думи: почти-МДР кодове, МДР кодове, елиптични криви, $(n,3)$-арка, проективни геометрии, дизайни.

МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2026
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2026
Proceedings of the Fifty-Fifth Spring Conference
of the Union of Bulgarian Mathematicians
Tryavna, Bulgaria, April 5–9, 2026

GABIDULIN CODES BASED POST-QUANTUM ENCRYPTION SCHEMES

Pierre Loidreau

Abstract

In this paper we make a historic survey of GPT-like encryption schemes, and show that there are new promising directions in the design of encryption schemes inspired from the pioneering works.

2020 Mathematics Subject Classification: 94A60, 94-02.

Key words: Gabidulin codes, McEliece cryptosystem.

1 Introduction. The principle of rank-metric code based cryptography relying on Gabidulin codes is over 30 years old. It dates back to the seminal GPT scheme [15], built upon distorting the so-called Gabidulin codes. The original intention of the authors was to propose an encryption scheme with a public-key size one order of magnitude smaller than that of the original McEliece cryptosystem [21].

Since 2017 and the call for standardisation of Post-Quantum resistant cryptography by NIST, this subject has become of tremendous interest. Unfortunately, the original scheme and all of its evolutions up to 2017 were severely broken, making it useless for cryptography.

The seminal weakness which has been again and again exploited is the fact that Gabidulin codes are almost *Galois stable*. For short, a Gabidulin code contains a huge ($(k-2)$-dimensional were k is the dimension) vector space which is invariant under the action of the Frobenius automorphism generating the Galois group. All the proposals have been carefully attacked in [24] and in [22], for essentially all the most recent evolutions up to 2017.

So was this the end of the story? Many could have thought that it was indeed impossible to repair it. However, a paper first published at ACCT in 2016, and then at PQCrypto 2017, proposed a new method to distort the structure of Gabidulin code, such that all the preceding attacks cannot be applied, [18, 19]. This idea uses an idea developed in the design of LRPC codes, that is to know the use of a rank multiplier [16]. It consists in taking the coefficients of the inverse of the right scrambler in a fixed secret subspace of sufficiently small dimension to keep polynomial-time decoding, and sufficiently large to break the stability of the Gabidulin code through the Frobenius action.

https://doi.org/10.55630/mem.2026.55.414-422

Up to now this approach has revealed to be resistant to all the attempted cryptanalysis and permits the design of public-keys within one and two orders of magnitude shorter than that of McEliece.

The goal of this paper is to present, the masking principle and some schemes using these properties together with briefly describing the most recent approaches supporting security claims around the schemes.

2 Preliminaries on the rank metric. Rank-metric cryptography relies on codes which are $\mathbb{F}_{q^m}$-linear, where $\mathbb{F}_{q^m}$ is the finite field with q^m elements, an extension of degree m over $\mathbb{F}_q$. In this context, the *rank* (or *weight*) of a vector $\mathbf{a} = (a_1, \ldots, a_n) \in (\mathbb{F}_{q^m})^n$ denoted by $\mathrm{Rk}(\mathbf{a})$ is the dimension of the $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^m}$ generated by the components of $\mathbf{a}$, *i.e.*

$$\mathrm{Rk}(\mathbf{a}) \stackrel{def}{=} \dim\langle a_1, \ldots, a_n\rangle_{\mathbb{F}_q}.$$

Gabidulin codes were first constructed by Delsarte as extremal object in a Bose–Mesner combinatorial algebra [12]. Some years later, Gabidulin presented an algebraic theory as well as a polynomial-time decoding algorithm [14]. These codes can be viewed as analogues of Reed–Solomon codes in the rank metric, where polynomials are replaced by linearized polynomials.

Definition 2.1. *Let integers $k \leq n \leq m$ and let $\mathbf{g} = (g_1, \ldots, g_m) \in (\mathbb{F}_{q^m})^n$ such that $Rk(\mathbf{g}) = n$. The k-dimensional Gabidulin code with support vector $\mathbf{g}$ denoted by $\mathcal{G}_k(\mathbf{g})$ is defined as*

$$\mathcal{G}_k(\mathbf{g}) \stackrel{def}{=} \left\{ \mathbf{x} \left(g_j^{[i]} \right)_{i=0,j=1}^{k-1,n} \mid \mathbf{x} \in (\mathbb{F}_{q^m})^k \right\},$$

where $[i] \stackrel{def}{=} q^i$, stands for the ith power of the Frobenius automorphism.

There are many different types of polynomial-time algorithms enabling to decode errors up to a rank of $\lfloor (n-k)/2 \rfloor$. In the rest of the paper we select any of them and define

$$\forall \mathbf{c} \in \mathcal{G}_k(\mathbf{g}), \mathbf{e} \in (\mathbb{F}_{q^m})^n, \begin{cases} \mathtt{Decode}(\mathbf{y} = \mathbf{c} + \mathbf{e}, \mathcal{G}_{\mathtt{k}}(\mathbf{g})) = \mathbf{c}, \text{ if } \mathrm{Rk}(\mathbf{e}) \leq \lfloor (\mathtt{n} - \mathtt{k})/2 \rfloor \\ \mathtt{Decode}(\mathbf{y}, \mathcal{G}_{\mathtt{k}}(\mathbf{g})) = *, \text{ else} \end{cases}$$

Finally, the following proposition shows that the dual of a Gabidulin code is a Gabidulin code.

Proposition 2.2 ([14])**.** *Let $\mathcal{G}_k(\mathbf{g}) \subset \mathbb{F}_{q^m}^n$, then there exists $\mathbf{h} \in \mathbb{F}_{q^m}^n$ of rank n such that $\mathcal{G}_{n-k}(\mathbf{h}) = \mathcal{G}_k(\mathbf{g})^\perp$ for the usual scalar product in $\mathbb{F}_{q^m}$.*

Remark 2.3. *Note that Gabidulin codes are defined with the help of the Frobenius, but one obtains the same properties by replacing it by any other generator of the Galois group of $\mathbb{F}_{q^m}/\mathbb{F}_q$, see* [3].

3 Rise and fall of GPT code based-cryptography. To be employed in the design of encryption schemes, GPT cryptosystem must be an OW-CPA encryption scheme. OW stands for one-way and CPA for *chosen plaintext attack*. This simply means that without

the secret part which is the secret key, a given ciphertext cannot be inverted to recover the corresponding plaintext in a complexity which less than exponential in the plaintext size and depending on the required security level.

Let $\mathcal{G}_k(\mathbf{g})$ be a Gabidulin code over $(\mathbb{F}_{q^m})^n$ with generator matrix $\mathbf{G} = (g_j^{[i]})$. In [22], the authors show that all the proposed evolutions of original GPT can be synthetised under the following form:

- `KeyGen` — generation of the public key ($\mathbf{pk}$) and secret key ($\mathbf{sk}$) pair
  - Pick randomly a matrix $\mathbf{X} \in (\mathbb{F}_{q^m})^{k\times \ell}$, for some integer ℓ;
  - Pick randomly $\mathbf{S} \in GL_k(\mathbb{F}_{q^m})$;
  - Pick randomly $\mathbf{P} \in GL_n(\mathbb{F}_q)$;
  - Return $\mathbf{pk} = \mathbf{G}_{pub} = \mathbf{S}(\mathbf{X}|\mathbf{G})\mathbf{P}$ and $\mathbf{sk} = (\mathbf{S}, \mathbf{P})$.
- `Encrypt`($\mathbf{G}_{pub}$, $\mathbf{x}$, $t \leq \lfloor (n-k)/2 \rfloor$)
  - Pick randomly $\mathbf{e} \in (\mathbb{F}_{q^m})^n$ of rank t;
  - Compute $\mathbf{y} = \mathbf{x}\mathbf{G}_{pub} + \mathbf{e}$;
  - Return $\mathbf{y}$.
- `Decrypt`($\mathbf{y}$,$\mathbf{sk} = (\mathbf{S}, \mathbf{P})$):
  - Compute $\mathbf{yP} = \mathbf{xSG} + \mathbf{eP}$.
  - Remove the first ℓ coordinates of $\mathbf{yP} \mapsto \widehat{\mathbf{yP}}$
  - Now $\mathrm{Rk}(\widehat{\mathbf{eP}}) \leq \mathrm{Rk}(\mathbf{eP})$, and since $\mathbf{P} \in GL_n(\mathbb{F}_q)$ we have $\mathrm{Rk}(\mathbf{eP}) = \mathrm{Rk}(\mathbf{e})$ therefore
    $$\mathtt{Decode}(\widehat{\mathbf{yP}}, \mathcal{G}_{\mathtt{k}}(\mathbf{g})) = \mathbf{xS}$$
  - Compute $\mathbf{xS} \overset{\mathbf{S^{-1}}}{\longmapsto} \mathbf{x}$
  - Return $\mathbf{x}$.

The security of encryption schemes using GPT like systems is related to the complexity of solving two different problems.

1. Distinguish the code generated by $\mathbf{G}_{pub}$ from random;
2. Decode $\mathbf{y}$ in the code generated by $\mathbf{G}_{pub}$. This problem is usually called Rank Syndrome Decoding problem (RSD).

The Rank Syndrome decoding problem is a generic problem, since it applies with sometimes some variants to the so-called rank-metric based cryptography.

It was first seriously considered in 1996 in [8], then some improvement was made in [23], then later improved in [17].

More recently, significant breakthroughs were done in the analysis of the problem in [6, 5]. Thus, it was necessary to reconsider all of the proposed parameters until now for a given security. However, in essence this implied a moderate increase of the parameters. Since the complexity studies are kind of *ad hoc*, it is hard to present a closed formula for

estimating this complexity. However, given parameters it is not very difficult to program estimations of the complexity.

Concerning GPT-like encryption schemes, the first problem appeared to be more serious. Indeed, let us denote by $\mathcal{C}_{pub}$ the code generated by $\mathbf{G}_{pub}$ and by $\mathcal{C}_{pub}^{[i]}$ the code obtained by elevating the codewords of $\mathcal{C}_{pub}$ to the ith power of the Frobenius automorphism. A generator of $\mathcal{C}_{pub}^{[i]}$ is

$$\mathbf{G}_{pub}^{[i]} = \mathbf{S}^{[i]}(\mathbf{X}^{[i]} \mid \mathbf{G}^{[i]})\mathbf{P},$$

where $[i]$ is applied coefficientwise on the matrix elements. Then the dimension of the intersection

$$\mathcal{C}_{pub}^{\perp} \cap \left(\mathcal{C}_{pub}^{[1]}\right)^{\perp} \cap \cdots \cap \left(\mathcal{C}_{pub}^{[i]}\right)^{\perp},$$

is at least the dimension of $\mathcal{G}_k(\mathbf{g})^{\perp} \cap \cdots \cap \left(\mathcal{G}_k(\mathbf{g})^{[i]}\right)^{\perp}$, that is at least $n-k-i-1$, due to the particular structure of the underlying Gabidulin code. If the codes were randomly chosen one would expect the dimension to be $\max(n-ik, 0)$. Hence one obtains a polynomial-time distinguisher for GPT cryptosystem. Even worse, if i is sufficiently large, we generally obtain

$$\mathcal{C}_{pub}^{\perp} \cap \cdots \cap \left(\mathcal{C}_{pub}^{[i]}\right)^{\perp} = \left(\mathcal{G}_k(\mathbf{g})^{\perp} \cap \cdots \cap \left(\mathcal{G}_k(\mathbf{g})^{[i]}\right)^{\perp}\right)\mathbf{P}.$$

And provided that the codes are non-trivial some elementary linear algebra operations enable to recover a polynomial-time decoder for $\mathcal{C}_pub$ with a large probability.

More elaborate forms of right scrambler were proposed, see for instance in [13, 25]. Unfortunately for the conceivers, the former point remains true. That is, $\mathbf{G}_{pub}$ can always be rewritten under the form

$$\mathbf{G}_{pub} = \mathbf{S}^*(\mathbf{X}^* \mid \mathbf{G}^*)\mathbf{P}^*, \tag{1}$$

where $\mathbf{P}^*$ has coefficients in $\mathbb{F}_q$, and $\mathbf{G}^*$ a generator matrix for a Gabidulin code of smaller length. This nice result comes from the paper [22].

4 Rank multipliers. Relaxing optimality on the code by scrambling the columns with a non-isometry of the metric is not new. This was done for Hamming metric in the case of GRS codes [4], by using an almost permutation matrix $\mathbf{P}$ and tolerating few rows and columns to have Hamming weight 2. This property was crucial to increase the Hamming weight of the errors that one could add, but not too much so as to be in the decoding region of the parent code. However this scheme and reparations was broken in [10], by designing a distinguisher on the Hamming weight of the rows of the scrambler.

We can also adapt similar transformations to the case of rank metric: let $\alpha_1, \ldots, \alpha_\lambda \in \mathbb{F}_{q^m}$, be $\mathbb{F}_q$-linearly independent. Let

$$\mathcal{V} = \langle \alpha_1, \ldots, \alpha_\lambda \rangle_{\mathbb{F}_q}$$

be the $\mathbb{F}_q$-linear subspace generated by $\alpha_1, \ldots, \alpha_\lambda$. Let $\mathbf{P} \in GL_n(\mathcal{V})$, be a $n \times n$-non singular matrix with coefficients taken in $\mathcal{V}$. Then

Proposition 4.1 (Rank multiplication)**.** *For all* $\mathbf{x} \in (\mathbb{F}_{q^m})^n$,

$$Rk(\mathbf{xP}) \leq \lambda Rk(\mathbf{x})$$

Proof. Consider $\mathbf{x} = (x_1, \ldots, x_n) \in (\mathbb{F}_{q^m})^n$ of rank r. Let $\langle x_1, \ldots, x_n \rangle_{\mathbb{F}_q}$ be generated by $(y_1, \ldots, y_r)$. Suppose $\mathcal{V} = \langle \alpha_1, \ldots, \alpha_\lambda \rangle$, then the components of $\mathbf{xP}$, belong to the $\mathbb{F}_q$-vector space generated by $(y_i \alpha_j)_{i,j}$. It has dimension at most λr. □

The concept of *rank multiplication* can be found in [16]. The paper also introduces the notion of *Low Rank Parity-Check* codes *a.k.a* LRPC codes for cryptographic purposes. This family of codes aims at being the equivalent of LDPC codes, but for rank metric.

An immediate corollary of the proposition is

Corollary 4.2. *Let* $\mathcal{C}$ *be a* $[n, k, d]_r$ *code over* $\mathbb{F}_{q^m}$*. Let* $\mathcal{V}$ *be a* λ*-dimensional subspace of* $\mathbb{F}_{q^m}$ *seen as an* $\mathbb{F}_q$*-vector space. And let* $\mathbf{P} \in M_n(\mathcal{V})$*. Then*

$$\mathcal{C}\mathbf{P}^{-1} \stackrel{def}{=} \{\mathbf{c}\mathbf{P}^{-1} \mid \mathbf{c} \in \mathcal{C}\}$$

has dimension k *and minimum rank distance* d'*, where* $d' \geq \lfloor d/\lambda \rfloor$*.*

Proof. Since $\mathbf{P}$ is invertible, $\mathcal{C}$ and $\mathcal{C}\mathbf{P}^{-1}$ have the same dimension. Concerning the minimum distance, suppose that $d' < d/\lambda$. Then let $\mathbf{c} \in \mathcal{C}\mathbf{P}^{-1} \neq \mathbf{0}$ with rank distance d'. By construction $\mathbf{cP} \in \mathcal{C}$. But from Proposition 4.1, $\mathrm{Rk}(\mathbf{cP}) \leq d'\lambda < d$, which implies that $\mathbf{cP} = \mathbf{0}$. Thus $\mathbf{c} = \mathbf{0}$, which contradicts the hypothesis. □

Now, with this notion of rank multiplication we are able to modify the GPT encryption scheme accordingly.

- `KeyGen` — generation of the public key ($\mathbf{pk}$) and secret key ($\mathbf{sk}$) pair
  - Pick randomly $\mathbf{S} \in GL_k(\mathbb{F}_{q^m})$;
  - Pick randomly $\mathcal{V} \subset \mathbb{F}_{q^m}$, $\mathbb{F}_q$-linear of dimension λ;
  - Pick randomly $\mathbf{P} \in GL_n(\mathcal{V})$;
  - Return $\mathbf{pk} = \mathbf{G}_{pub} = \mathbf{SGP}^{-1}$ and $\mathbf{sk} = (\mathbf{S}, \mathbf{P})$
- `Encrypt`($\mathbf{G}_{pub}$, $\mathbf{x}$, $t \leq \lfloor (n-k)/(2\lambda) \rfloor$)
  - Pick randomly $\mathbf{e} \in (\mathbb{F}_{q^m})^n$ of rank t;
  - Compute $\mathbf{y} = \mathbf{xG}_{pub} + \mathbf{e}$;
  - Return $\mathbf{y}$.
- `Decrypt`($\mathbf{y}$,$\mathbf{sk} = (\mathbf{S}, \mathbf{P})$):
  - Compute $\mathbf{yP} = \mathbf{xSG} + \mathbf{eP}$.
  - Now $\mathrm{Rk}(\mathbf{eP}) \leq \lambda \mathrm{Rk}(\mathbf{e}) \leq \lfloor (n-k)/2 \rfloor$, therefore

$$\mathtt{Decode}(\mathbf{yP}, \mathcal{G}_{\mathtt{k}}(\mathbf{g})) = \mathbf{xS}$$

– Compute $\mathbf{xS} \overset{\mathbf{S}^{-1}}{\longmapsto} \mathbf{x}$

– Return $\mathbf{x}$.

A Niederreiter form can be obtained similarly to the Niederreiter idea, enabling to reduce the public-key size and the ciphertext size without losing security.

The next question to investigate is how we dimension the encryption scheme for a given security. As stated in previous section there are two types of attacks to consider:

- Concerning the decoding of $\mathbf{y}$ in the code generated by $\mathbf{G}_{pub}$, the standard approach of [6, 5] is applied;
- The problem of distinguishing the public code from random, on which we will elaborate.

In 2019 it was shown in [9] that provided

$$\lambda(n-k+1) < n,$$

the public code can be polynomially distinguished from random, by simple linear algebra techniques. It is the so-called Coggia–Couvreur distinguisher.

In the other case however whenever $\lambda(n-k+1) \geq n$, we do have only attacks exponential in essence. A first basic analysis was presented in [19], and was further improved in [20] and finally, the most up-to-date attack is [7]. The most up-to-date complexity is thus

$$P(m,n,k)q^{(\lambda-1)m-\lambda n(1-R)R}$$

where $R = k/n$ is the rate of the code, and P is a degree 5 polynomial counting the complexity of linear algebra operations. Note, that since the systems are sparse we use the complexity given by Wiedemann's algorithm.

With all the latest improvements, the parameters for 128 bits of security are given by

$m = n$	k	λ	t	**pk**	**y**
128	20	3	18	34 kB	1.8 kB
128	42	3	7	58 kB	1.3 kB

For an equivalent security if one compares with the ClassicMcEliece NIST submission for an equivalent security, then the parameters are the following, [1]:

- **pk**: 260 kB;
- **y**: 0.13 kB.

So, concerning the public-key size the gain is between 5 and 8 times. Note that in this case the parameters are computed by considering the public-key under a systematic matrix form that is to know the size is $mk(n-k)/8$ kBytes.

5 Most recent evolutions. In this section we present two recent evolutions of the system which enable to consider a wider range of parameters, still with the intention to reduce the parameters by keeping the same security.

5.1 Direct generalisation. The first approach has been presented in 2009 in [13]. The idea is to combine the use of rank multipliers with Gabidulin, Rashwan and Honary approach. It consists in multiplying on the right by a matrix $\mathbf{Q} = (\mathbf{Q}_1|\mathbf{Q}_2)$, such that $\mathbf{Q}_2 \in \mathbb{F}_q^{n\times(n-\gamma)}$ has coefficients in the base field. With this modification, the public code can be decoded up to $\lfloor (n-k-\gamma)/(2\lambda)\rfloor$.

Coggia-Couvreur distinguisher can be extended accordingly and it happens that provided

$$\lambda(n-k+1)+\gamma < n,$$

the public code can be polynomially distinguished from a random code. Moreover, if one wants to generalize the attack in [7], then this adds a significant complexity, which becomes

$$P'(m,n,k)q^{(\lambda-1)m-\lambda[n(1-R)R-\gamma R]},$$

which is $q^{\lambda\gamma R}$ more complex than the original scheme.

Thanks to this generalisation, we obtain much more interesting parameters than for the original scheme. Namely one obtains the following figures:

m	n	k	λ	γ	t	**pk**	**y**
128	89	10	2	11	17	9.5 kB	0.94 kB

5.2 Multidimensional approach. A different type of approach was published in [2]. To sum up rather than decoding one ciphertext $\mathbf{y}$, we will consider ℓ such ciphertexts $\mathbf{y}_1,\ldots,\mathbf{y}_\ell$ with the property that the coefficients of the corresponding $\mathbf{e}_1,\ldots,\mathbf{e}_\ell$ lie all in the same t-dimensional vector-space. Roughly speaking, this reduces to decode in an ℓ-interleaved Gabidulin code for which there are polynomial-time algorithms decoding errors up to a rank of

$$\left\lfloor \frac{\ell}{\ell+1}(n-k)\right\rfloor.$$

This however changes the problems that we have to consider for security.

- The RSD problem is now replaced by the so-called RSL problem (Rank Syndrome Learning with errors). The latter problem consists to decode an increasing number ℓ of codewords corrupted by errors taken all in the same t dimensional vector-space. However, ℓ has to remain rather small. Namely, [11]
  - if $\ell \geq nt$, then the problem can be solved in probabilistic polynomial-time;
  - if $\ell \geq kt$, then the problem can be solved probabilistically in subexponential-time.

  This is the reason why one has to choose $\ell < kt$.
- The decoding algorithm is probabilistic with a failure probability p_f of

  $$p_f \approx 3.5q^{-m[\ell(n-k)-(\ell+1)\lambda t+1]}.$$

  This fact has to be taken into account when designing an encryption scheme.

This gives for a security of 128 bits:

m	n	k	λ	ℓ	t	**pk**	**y**	p_f
61	50	25	3	6	7	4.8 kB	1.2 kB	2^{-242}

6 Perspectives. In this paper we only considered evolutions of the use of Gabidulin codes to design encryption schemes based on the RSD, or RSL problems. However, one can use other types of codes such as QC-LRPC codes which are structured quasi-cyclic codes with a decoding algorithm. Concerning the problem of distinguishability relative to a random quasi-cyclic codes, this raises other types of concerns. Equally, since the decoder is in essence probabilistic, then there is a failure probability that has to be taken into account in security reductions.

Another potential perspective to improve parameters consists in using an extension of rank metric such as sum-rank metric. Such a proposal is made with the use of linearized Reed–Solomon codes.

REFERENCES.

[1] M. ALBRECHT, D. J. BERNSTEIN, T. CHOU, C. CID, J. GILCHER, T. LANGE, V. MARAM, I. von MAURICH, R. MIZOCZKI, R. NIEDERHAGEN, E. PERSICHETTI, K. PATERSON, C. PETERS, P. SCHWABE, N. SENDRIER, J. SZEFER, C. J. TJHAI, M. TOMLINSON, and WANG WEN. Classic McEliece (merger of Classic McEliece and NTS-KEM. `https://classic.mceliece.org`, October 2020. Third round finalist of the NIST post-quantum cryptography call.

[2] N. ARAGON, V. DYSERYN, PH. GABORIT, P. LOIDREAU, J. RENNER, and A. WACHTER-ZEH. LowMS: a new rank metric code-based KEM without ideal structure. *Des. Codes Cryptogr.*, 92(4):1075–1093, 2024.

[3] D. AUGOT, P. LOIDREAU, and G. ROBERT. Generalized Gabidulin codes over fields of any characteristic. *Des. Codes Cryptogr.*, 86(8):1807–1848, 2018.

[4] M. BALDI, M. BIANCHI, F. CHIARALUCE, J. ROSENTHAL, and D. SCHIPANI. Enhanced public key security for the McEliece cryptosystem. *J. Cryptology*, 29(1):1–27, 2016.

[5] M. BARDET, P. BRIAUD, M. BROS, PH. GABORIT, and J.-P. TILLICH. Revisiting algebraic attacks on minrank and on the rank decoding problem. *Des. Codes Cryptogr.*, 91(11):3671–3707, 2023.

[6] M. BARDET, M. BROS, D. CABARCAS, PH. GABORIT, R. PERLNER, D. SMITH-TONE, J.-P. TILLICH, and J. VERBEL. Improvements of algebraic attacks for solving the rank decoding and minrank problems. In *Advances in Cryptology - ASIACRYPT 2020*, pages 507–536, 2020.

[7] P. BRIAUD and P. LOIDREAU. Cryptanalysis of Rank-Metric Schemes Based on Distorted Gabidulin Codes. In T. JOHANSSON and D. SMITH-TONE, editors, *Post-Quantum Cryptography 2023*, volume 14154 of *LNCS*, pages 38–56, 2023.

[8] F. CHABAUD and J. STERN. The cryptographic security of the syndrome decoding problem for rank distance codes. In *Advances in Cryptology - ASIACRYPT 1996*, volume 1163 of *LNCS*, pages 368–381, Kyongju, Korea. Springer, November 1996.

[9] D. COGGIA and A. COUVREUR. On the security of a Loidreau rank metric code based encryption scheme. *Des. Codes Cryptogr.*, 88(9):1941–1957, 2020.

[10] A. COUVREUR, A. OTMANI, J.-P. TILLICH, and V. GAUTHIER-UMAÑA. A polynomial-time attack on the BBCRS scheme. In J. KATZ, editor, *Public-Key Cryptography - PKC 2015*, volume 9020 of *LNCS*, pages 175–193. Springer, 2015.

[11] T. DEBRIS-ALAZARD and J.-P. TILLICH. Two attacks on rank metric code-based schemes: ranksign and an identity-based-encryption scheme. In *Advances in Cryptology - ASIACRYPT 2018*, volume 11272 of *LNCS*, pages 62–92, Brisbane, Australia. Springer, December 2018.

[12] PH. DELSARTE. Bilinear forms over a finite field, with applications to coding theory. *J. Comb. Theory, Ser. A*, 25(3):226–241, 1978.

[13] E. GABIDULIN, H. RASHWAN, and B. HONARY. On improving security of GPT cryptosystems. In *Proc. IEEE Int. Symposium Inf. Theory - ISIT*, pages 1110–1114. IEEE, 2009.

[14] E. M. GABIDULIN. Theory of codes with maximum rank distance. *Problemy Peredachi Informatsii*, 21(1):3–16, 1985.

[15] E. M. GABIDULIN, A. V. PARAMONOV, and O. V. TRETJAKOV. Ideals over a non-commutative ring and their applications to cryptography. In *Advances in Cryptology - EUROCRYPT'91*, number 547 in LNCS, pages 482–489, Brighton, April 1991.

[16] PH. GABORIT, G. MURAT, O. RUATTA, and G. ZÉMOR. Low rank parity check codes and their application to cryptography. In *Proceedings of the Workshop on Coding and Cryptography WCC'2013*, Bergen, Norway, 2013. URL: `www.selmer.uib.no/WCC2013/pdfs/Gaborit.pdf`.
[17] PH. GABORIT, O. RUATTA, and J. SCHREK. On the complexity of the rank syndrome decoding problem. *IEEE Trans. Information Theory*, 62(2):1006–1019, 2016.
[18] P. LOIDREAU. An evolution of GPT cryptosystem. In *Proceedings of the 15th Algebraic and Combinatorial Theory, Albena, Bulgaria*, pages 215–220, 2016.
[19] P. LOIDREAU. A new rank metric codes based encryption scheme. In *Post-Quantum Cryptography 2017*, volume 10346 of *LNCS*, pages 3–17. Springer, 2017.
[20] P. LOIDREAU. Analysis of a public-key encryption scheme based on distorted gabidulin codes. In *Twelfth International Workshop on Coding and Cryptography, WCC 2022*, 2022. URL: `https://www.wcc2022.uni-rostock.de`.
[21] R. J. MCELIECE. *A public-key system based on algebraic coding theory.* In DSN Progress Report 44. Jet Propulsion Lab, 1978, pages 114–116.
[22] A. OTMANI, H. TALÉ-KALACHI, and S. NDJEYA. Improved cryptanalysis of rank metric schemes based on Gabidulin codes. *Des. Codes Cryptogr.*, 86(9):1983–1996, 2018.
[23] A. V. OURIVSKI and T. JOHANSSON. New technique for decoding codes in the rank metric and its cryptography applications. English. *Problems of Information Transmission*, 38(3):237–246, 2002.
[24] R. OVERBECK. Structural attacks for public key cryptosystems based on Gabidulin codes. *J. Cryptology*, 21(2):280–301, 2008.
[25] H. RASHWAN, E. GABIDULIN, and B. HONARY. A smart approach for GPT cryptosystem based on rank codes. In *Proc. IEEE Int. Symposium Inf. Theory - ISIT*, pages 2463–2467. IEEE, 2010.

Pierre Loidreau
DGA MI and IRMAR, CNRS
Université de Rennes, France
e-mail: `pierre.loidreau@univ-rennes.fr`

ПОСТКВАНТОВИ КРИПТОГРАФСКИ СХЕМИ, БАЗИРАНИ НА КОДОВЕТЕ НА ГАБИДУЛИН

Pierre Loidreau

Абстракт

В тази статия правим исторически обзор на шифрови схеми от типа GPT и показваме, че съществуват нови обещаващи направления при проектирането на шифрови схеми, вдъхновени от пионерските разработки.

Ключови думи: кодове на Габидулин, криптосистема на McEliece.

МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2026
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2026
Proceedings of the Fifty-Fifth Spring Conference
of the Union of Bulgarian Mathematicians
Tryavna, Bulgaria, April 5–9, 2026

A CONJECTURE ON THE MINIMUM LENGTH OF BINARY LINEAR CODES [1]

T. Maruta, T. Tochiyama, and K. Yasufuku

Abstract

We give a new conjecture on $D_{2,k}$, where $D_{q,k}$ denotes the largest d such that a linear code of dimension k with minimum weight d meeting the Griesmer bound does not exist. We also prove that $D_{2,11} = 1632$, which yields that our conjecture is valid for dimensions $k \leq 11$.

2020 Mathematics Subject Classification: 94B05, 94B27, 94B65.

Key words: Griesmer bound, optimal code, divisible code.

1 Introduction. Let $\mathbb{F}_q^n$ denote the vector space of n-tuples over $\mathbb{F}_q$, the field of order q. An $[n,k,d]_q$ code $\mathcal{C}$ is a k-dimensional subspace of $\mathbb{F}_q^n$ with minimum Hamming weight $d = \min\{wt(c) \mid c \in \mathcal{C}, c \neq (0,\ldots,0)\}$, where $wt(c)$ is the number of non-zero entries in c. A fundamental problem in coding theory is to find $n_q(k,d)$, the minimum length n for which an $[n,k,d]_q$ code exists [6]. The Griesmer bound [5, 6] gives a lower bound on the length n:

$$n \geq g_q(k,d) := \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil, \tag{1}$$

where $\lceil x \rceil$ denotes the smallest integer greater than or equal to x. An $[n,k,d]_q$ code $\mathcal{C}$ is called *Griesmer* if it attains the Griesmer bound, i.e., $n = g_q(k,d)$. It is known that $n_q(k,d) = g_q(k,d)$ for $k = 1,2$ and all d. So, we assume $k \geq 3$. For fixed q and k, it is also known that the Griesmer bound is attained for all sufficiently large d [6]. A natural question arises.

Problem. For fixed q and k, find the integer $D_{q,k}$ such that $n_q(k,d) = g_q(k,d)$ for all $d > D_{q,k}$ and $n_q(k,d) > g_q(k,d)$ for $d = D_{q,k}$. Then, determine $n_q(k, D_{q,k})$.

As for the value $D_{q,k}$, Kawabata et al. [11] posed the following conjecture.

Conjecture 1.1 ([11])**.** (a) $D_{q,k} = B_{q,k}$ *for* $q \geq k \geq 3$*;*

(b) $D_{q,k} = C_{q,k}$ *for* $3 \leq q < k$*;*

[1]The work of T. Maruta is supported by JSPS KAKENHI Grant Number 24K06850
https://doi.org/10.55630/mem.2026.55.423-432

(c) $n_q(k, D_{q,k}) = g_q(k, D_{q,k}) + 1$,
where

$$B_{q,k} = (k-2)q^{k-1} - (k-1)q^{k-2},$$

$$C_{q,k} = q^{k-2-l}(((q-1)l + \alpha - 3)q^{l+1} + q^{k-\beta} + q - \alpha) \text{ for } \beta \le k \le \beta + l,$$

with integers l, α *and* β *satisfying* $l \ge 1$, $1 \le \alpha \le q-1$ *and*

$$\beta = \beta_{l,\alpha} = (q-1)\binom{l+1}{2} + (l+1)\alpha - l.$$

Note for $q = 2$ with $l \ge 2$ that $\beta = \binom{l+1}{2} + 1$ and

$$C_{2,k} = (l-2)2^{k-1} + 2^{k+\tau-l-2} + 2^{k-l-2}, \tag{2}$$

where $\tau = k - \beta$ with $0 \le \tau \le l$. As for binary linear codes, the following is known.

Theorem 1.2 ([2, 11, 16])**.** (a) $n_2(k, d) = g_2(k, d)$ *for all* d *for* $1 \le k \le 4$.

(b) $n_2(k, d) = g_2(k, d)$ *for all* $d > C_{2,k}$ *for* $k \ge 5$.

(c) $D_{2,k} = C_{2,k}$ *for* $k = 5, 6, 9, 10$.

(d) $D_{2,7} = 44 < C_{2,7} = 72$, $D_{2,8} = 104 < C_{2,8} = 152$.

(e) $D_{2,11} < C_{2,11}$.

So, Conjecture 1 excludes the case $q = 2$. Let

$$\tilde{C}_{2,k} = (l-2)2^{k-1} - (2^l - 1 - 2^{\tau+1})2^{k-l-2}. \tag{3}$$

We pose a new conjecture for binary codes as follows.

Conjecture 1.3. (a) $D_{2,k} = \tilde{C}_{2,k}$ *for* $k = \beta, \beta + 1$, $l \ge 3$*;*

(b) $D_{2,k} = C_{2,k}$ *for* $k = \beta + l - 1, \beta + l$, $l \ge 2$.

Since $\tilde{C}_{2,7} = 44$ and $\tilde{C}_{2,8} = 104$, Conjecture 2 is valid for $5 \le k \le 10$ ($\beta = 2, 3$). In this paper, we prove that Conjecture 2 is also valid for $k = 11$:

Theorem 1.4. $D_{2,11} = \tilde{C}_{2,11}$.

2 Geometric preliminaries. In this section, we give the geometric methods to construct codes or to prove the non-existence of codes with certain parameters. We denote by $\mathrm{PG}(r, q)$ the projective geometry of dimension r over $\mathbb{F}_q$. A j-flat is a projective subspace of dimension j in $\mathrm{PG}(r, q)$. The 0-flats, 1-flats, 2-flats, 3-flats, $(r-2)$-flats and $(r-1)$-flats are called *points, lines, planes, solids, secundums* and *hyperplanes*, respectively. We denote by θ_j the number of points in a j-flat, i.e., $\theta_j = |\mathrm{PG}(j, q)| = (q^{j+1} - 1)/(q - 1)$, where $|T|$ denotes the number of elements in a set T.

Let $\mathcal{C}$ be an $[n, k, d]_q$ code having no coordinate which is identically zero. The columns of a generator matrix G of $\mathcal{C}$ can be considered as a multiset of n points in $\Sigma = \mathrm{PG}(k-1, q)$ denoted by $\mathcal{M}_{\mathcal{C}}$. A point P in Σ is called an *i-point* if it has multiplicity $m_{\mathcal{C}}(P) = i$ in

$\mathcal{M}_{\mathcal{C}}$ (in other words, an i-point appears exactly i times as a column of G). Denote by γ_0 the maximum multiplicity of a point from Σ in $\mathcal{M}_{\mathcal{C}}$ and let Λ_i be the set of i-points in Σ, $0 \le i \le \gamma_0$. We denote by $\Delta_1 + \cdots + \Delta_s$ the multiset consisting of the s sets $\Delta_1, ..., \Delta_s$ in Σ. We denote by $\Delta_2 = \Delta - \Delta_1$ when $\Delta = \Delta_1 + \Delta_2$. We write $s\Delta$ for $\Delta_1 + \cdots + \Delta_s$ when $\Delta_1 = \cdots = \Delta_s$. Then, $\mathcal{M}_{\mathcal{C}} = \sum_{i=1}^{\gamma_0} i\Lambda_i$. For any set S in Σ, the *multiplicity of S (with respect to $\mathcal{M}_{\mathcal{C}}$)*, denoted by $m_{\mathcal{C}}(S)$, is defined as

$$m_{\mathcal{C}}(S) = \sum_{P \in S} m_{\mathcal{C}}(P) = \sum_{i=1}^{\gamma_0} i \cdot |S \cap \Lambda_i|.$$

Then we obtain the partition $\bigcup_{i=0}^{\gamma_0} \Lambda_i$ of Σ such that $n = m_{\mathcal{C}}(\Sigma)$ and that

$$n - d = \max\{m_{\mathcal{C}}(\pi) \mid \pi \in \mathcal{F}_{k-2}\},$$

where $\mathcal{F}_j$ denotes the set of all j-flats in Σ. Such a partition of Σ is called an $(n, n-d)$-*arc* of Σ. Conversely an $(n, n-d)$-arc of Σ gives an $[n, k, d]_q$ code. A line ℓ with $t = m_{\mathcal{C}}(\ell)$ is called a *t-line*. A *t-hyperplane* and so on are defined similarly. Denote by a_i the number of i-hyperplanes in Σ. The list of a_i's is called the *spectrum* of $\mathcal{C}$. The spectrum can be calculated from the weight distribution of $\mathcal{C}$ by $a_i = A_{n-i}/(q-1)$ for $0 \le i \le n-d$, where A_w is the number of codewords of $\mathcal{C}$ with weight w. Let τ_j be the number of j-secundums in a fixed hyperplane Π of Σ. The list of τ_j's is called the *spectrum* of Π. We denote by λ_s the number of s-points in Σ. For an m-flat Π in Σ we define

$$\gamma_j(\Pi) = \max\{m_{\mathcal{C}}(\Delta) \mid \Delta \subset \Pi,\ \Delta \in \mathcal{F}_j\},\ 0 \le j \le m.$$

We write simply by γ_j for $\gamma_j(\Sigma)$. It holds that $\gamma_{k-2} = n - d$, $\gamma_{k-1} = n$. When $\mathcal{C}$ is Griesmer, the value γ_j is uniquely determined in [13] as follows:

$$\gamma_j = \sum_{u=0}^{j} \left\lceil \frac{d}{q^{k-1-u}} \right\rceil \quad \text{for } 0 \le j \le k-1. \tag{4}$$

Lemma 2.1 ([15]). *Put $\epsilon = (n-d)q - n$ and $t_0 = \lfloor (w+\epsilon)/q \rfloor$, where $\lfloor x \rfloor$ denotes the largest integer less than or equal to x. Let Π be a w-hyperplane through a t-secundum δ. Then $t \le (w+\epsilon)/q$ and the following holds.*

(i) *$a_w = 0$ if an $[w, k-1, d_0]_q$ code with $d_0 \ge w - t_0$ does not exist.*

(ii) *$\gamma_{k-3}(\Pi) = t_0$ if an $[w, k-1, d_1]_q$ code with $d_1 \ge w - t_0 + 1$ does not exist.*

Note that a w-hyperplane Π with $\gamma_{k-3}(\Pi) = t_0$ gives a $[w, k-1, w-t_0]_q$ code if and only if $t_0 < w$. An $[n, k, d]_q$ code is called *m-divisible* if all codewords have weights divisible by an integer $m > 1$.

Lemma 2.2 ([9, 10, 15]). *Let $\mathcal{C}$ be an m-divisible $[n, k, d]_q$ code with $q = p^h$, p prime, whose spectrum is*

$$(a_{n-d-(w-1)m}, a_{n-d-(w-2)m}, \ldots, a_{n-d-m}, a_{n-d}) = (\alpha_{w-1}, \alpha_{w-2}, \ldots, \alpha_1, \alpha_0),$$

where $m = p^e$ for some $1 \le e < h(k-2)$ satisfying $\lambda_0 > 0$ and $n(q-1) > dq$. Then there exists a t-divisible $[n^*, k, d^*]_q$ code $\mathcal{C}^*$ with

$$t = q^{k-2}/m,\ n^* = ntq - \frac{d}{m}\theta_{k-1},\ d^* = ((n-d)q - n)t \tag{5}$$

whose spectrum is

$$(a_{n^*-d^*-\gamma_0 t}, a_{n^*-d^*-(\gamma_0-1)t}, \ldots, a_{n^*-d^*-t}, a_{n^*-d^*}) = (\lambda_{\gamma_0}, \lambda_{\gamma_0-1}, \ldots, \lambda_1, \lambda_0).$$

$\mathcal{C}^*$ is called a *projective dual* of $\mathcal{C}$, see also [3] and [7]. Note that a generator matrix for $\mathcal{C}^*$ is given by considering $(n-d-jm)$-hyperplanes as j-points in the dual space Σ^* of Σ for $0 \le j \le w-1$ [15]. From the principle of projective geometry, $\mathcal{C}$ and $(\mathcal{C}^*)^*$ are equivalent, and $(n^*)^* = n$, $(d^*)^* = d$. Hence, the following holds.

Lemma 2.3. *Assume there exists a t-divisible $[n^*, k, d^*]_q$ code $\mathcal{C}^*$ satisfying (5) with $q = p^h$, p prime, $m = p^e$, $1 \le e < h(k-2)$, $\lambda_0(\mathcal{C}^*) > 0$. Then, so does an m-divisible $[n, k, d]_q$ code.*

Lemma 2.4 ([10])**.** *Let $\mathcal{C}$ be an $[n, k, d]_q$ code with multiset $\mathcal{M}_\mathcal{C}$ over $\Sigma = \mathrm{PG}(k-1, q)$. Assume $d > q^t$ and that $\mathcal{M}_\mathcal{C}$ contains a t-flat Δ with $1 \le t \le k-1$. Let $\mathcal{C}'$ be an $[n-\theta_t, k, d']_q$ code with multiset $\mathcal{M}_{\mathcal{C}'} = \mathcal{M}_\mathcal{C} - \Delta$. Then, $d' \ge d - q^t$.*

The method to construct new codes from a given $[n, k, d]_q$ code by deleting the coordinates corresponding to some geometric object in $\mathrm{PG}(k-1, q)$ is called *geometric puncturing*, see [14]. As a consequence for $q = 2$, we get the following lemma, which is employed in Section 4.

Lemma 2.5. *Assume that a Griesmer $[n, k, d]_2$ code with multiset $\mathcal{M}_\mathcal{C}$ over $\Sigma = \mathrm{PG}(k-1, 2)$ exists and that $d = s \cdot 2^{k-1} - (d_{k-2}2^{k-2} + d_{k-3}2^{k-3} + \cdots + d_{t+1}2^{t+1} + 2^t)$ with integer $t \ge 2$ and $d_i \in \mathbb{F}_2$ for $t+1 \le i \le k-2$. If $\mathcal{M}_\mathcal{C}$ contains a multiset $F_1 + F_2 + \cdots + F_{t-1}$, where F_j is a j-flat for $1 \le j \le t-1$, then, $n_2(k, d') = g_2(k, d')$ for $d - 2^t + 1 \le d' \le d$.*

For the divisibility of Griesmer codes, we need the following results.

Lemma 2.6 ([17])**.** *Let $\mathcal{C}$ be a Griesmer $[n, k, d]_p$ code with a prime p. If p^e divides d, then $\mathcal{C}$ is p^e-divisible.*

Lemma 2.7 ([11])**.** *If there exists no p^e-divisible $[n, k, d]_q$ code with $q = p^h$, p prime, $\frac{dq}{q-1} < n < \theta_{k-1}$ and $1 \le e < h(k-2)$, then neither does there exist a p^e-divisible $[n, k+1, d]_q$ code.*

Lemma 2.8 ([11])**.** *Let $\mathcal{C}$ be an m-divisible $[n, k, d]_q$ code. If $\mathcal{M}_\mathcal{C}$ has an s-point P with $s \ge 1$, then the projection of $\mathcal{M}_\mathcal{C} - sP$ from P onto a hyperplane Π with $P \notin \Pi$ gives an m-divisible $[n-s, k-1, d']_q$ code with $d' \ge d$.*

3 Dimension-optimal binary divisible codes. Let $q = p^h$, p prime. Assume that an m-divisible $[n, k, d]_q$ code $\mathcal{C}$ exists for some integer $m > 1$. We say that $\mathcal{C}$ is *dimension-optimal* if an m-divisible $[n, k', d]_q$ code does not exist for any $k' > k$. We mainly consider d-divisible dimension-optimal $[n, k, d]_2$ codes for $d = 2^t$ with a positive integer t. Denote

Table 1: $k_2(n,4)$

n	4	6	7	8	10	11	12	13	14	15	16	17	18	19	20
$k_2(n,4)$	1	2	3	4	4	4	5	5	6	7	8	8	8	8	9

Table 2: $k_2(n,8)$

n	8	12	14	15	16	20	22	23	24	26	27	28
$k_2(n,8)$	1	2	3	4	5	4	4	5	6	5	6	7
n	29	30	31	32	34	35	36	37	38	39	40	41
$k_2(n,8)$	7	8	9	10	8	8	9	8	9	10	11	9

by $k_q(n,d)$ the maximum dimension k such that a d-divisible $[n,k,d]_q$ code exists. Körner and Kurz [12] determined $k_2(n,4)$ for $n \le 20$, $k_2(n,8)$ for $n \le 41$ and $k_2(n,16)$ for $n \le 79$, see Tables 1-3.

For $i = 1,2$, let $\mathcal{C}_i$ be an $[n_i,k_i,d_i]_q$ code with generator matrix G_i. Then, their *direct sum* $\mathcal{C}_1 \oplus \mathcal{C}_2$ is the $[n_1+n_2, k_1+k_2, \min\{d_1,d_2\}]_q$ code with generator matrix $G_1 \oplus G_2 = \begin{bmatrix} G_1 & O \\ O & G_2 \end{bmatrix}$, see [8]. For the multisets $\mathcal{M}_{\mathcal{C}_1}$ and $\mathcal{M}_{\mathcal{C}_2}$ obtained from G_1 and G_2, respectively, we denote by $\mathcal{M}_{\mathcal{C}_1} \oplus \mathcal{M}_{\mathcal{C}_2}$ the multiset $\mathcal{M}_{\mathcal{C}_1 \oplus \mathcal{C}_2}$ of the direct sum $\mathcal{C}_1 \oplus \mathcal{C}_2$. The following is obvious.

Lemma 3.1. *Let $\mathcal{C}_i$ be an m-divisible $[n_i,k_i,d_i]_q$ code for $i = 1,2$. Then, their direct sum $\mathcal{C}_1 \oplus \mathcal{C}_2$ is also m-divisible.*

A code $\mathcal{C}$ is called an *s-fold simplex code* if $\mathcal{M}_{\mathcal{C}} = s\mathrm{PG}(k-1,q)$ for some positive integer s, whose parameters are $[s\theta_{k-1}, k, sq^{k-1}]_q$. $\mathcal{C}$ is sq^{k-1}-divisible since every non-zero codeword has weight sq^{k-1}. Taking $s = 2^{t+1-k}$ with $q = 2$, one can get the part (a) of the next lemma.

Let $q = 2$. We denote a j-flat in $\mathrm{PG}(k-1,2)$ by Π_j. So, Π_0 and Π_{k-1} stand for a point and the whole space, respectively. We denote by $\mathcal{E}_3$ an elliptic quadric in $\mathrm{PG}(3,2)$, which gives a 2-divisible $[5,4,2]_2$ code with spectrum $(a_1,a_3) = (5,10)$.

Lemma 3.2. *Let $\mathcal{C}$ be an $[n,k,d]_2$ code and let t be a positive integer.*

(a) *$\mathcal{C}$ is 2^t-divisible $[2^{t+1-k}\theta_{k-1}, k, 2^t]_2$ code if $\mathcal{M}_{\mathcal{C}} = 2^{t+1-k}\Pi_{k-1}$ for $t \ge k$.*

Table 3: $k_2(n,16)$

n	16	24	28	30	31	32	40	44	46	47	48	52	54	55	56	58
$k_2(n,16)$	1	2	3	4	5	6	4	4	5	6	7	5	6	7	8	7
n	59	60	61	62	63	64	68	70	71	72	74	75	76	77	78	79
$k_2(n,16)$	8	9	9	10	11	12	8	8	9	10	8	9	10	10	11	12

(b) $\mathcal{C}$ *is* 2^{k-2}*-divisible* $[2^{k-1}, k, 2^{k-1} - 2^{k-2}]_2$ *code if* $\mathcal{M}_{\mathcal{C}} = \Pi_{k-1} - \Pi_{k-2}$.

(c) $\mathcal{C}$ *is* 2^t*-divisible* $[5 \cdot 2^{t-1}, 4, 2^t]_2$ *code if* $\mathcal{M}_{\mathcal{C}} = 2^{t-1}\mathcal{E}_3$.

Körner and Kurz [12] proved the following with the aid of a computer.

Lemma 3.3. *Let* $\mathcal{C}$ *be an* $[n, k, d]_2$ *code. Then,* d*-divisible* $[n, k_2(n, d), d]_2$ *codes are unique up to equivalence for*

(a) $n = 4, 6\text{-}8, 10, 17$ *when* $d = 4$*;*

(b) $n = 8, 12, 14\text{-}16, 20, 22, 23, 24, 27\text{-}29, 31, 32, 34\text{-}37, 39, 40$ *when* $d = 8$*;*

(c) $n = 16, 24, 30\text{-}32, 40, 46\text{-}48, 54\text{-}56, 58\text{-}61, 63, 64, 68, 70\text{-}72, 74\text{-}77, 79$ *when* $d = 16$.

Table 4: 8-divisible $[n, k_2(n, 8), 8]_2$ codes

n	$k_2(n, 8)$	construction
22	4	$8\Pi_0 \oplus 2\Pi_2$
23	5	$8\Pi_0 \oplus \Pi_3$
24	6	$8\Pi_0 \oplus (\Pi_4 - \Pi_3)$
27	6	$4\Pi_1 \oplus \Pi_3$
28	7	$4\Pi_1 \oplus (\Pi_4 - \Pi_3)$
29	7	$2\Pi_2 \oplus \Pi_3$
31	9	$\Pi_3 \oplus (\Pi_4 - \Pi_3)$
32	10	$(\Pi_4 - \Pi_3) \oplus (\Pi_4 - \Pi_3)$
35	8	$4\mathcal{E}_3 \oplus \Pi_3$

Most of the dimension-optimal binary divisible codes in Lemma 3.3 can be constructed by Lemmas 3.1 and 3.2, see Table 4 and Table 5. In the tables, "construction" gives the multiset $\mathcal{M}_{\mathcal{C}}$ for the unique d-divisible $[n, k_2(n, d), d]_2$ code $\mathcal{C}$.

Table 5: 16-divisible $[n, k_2(n, 16), 16]_2$ codes

n	$k_2(n, 16)$	construction
72	10	$8\mathcal{E}_3 \oplus (\Pi_5 - \Pi_4)$
74	8	$16\Pi_0 \oplus 4\Pi_2 \oplus 2\Pi_3$
75	9	$16\Pi_0 \oplus 4\Pi_2 \oplus \Pi_4$
76	10	$16\Pi_0 \oplus 4\Pi_2 \oplus (\Pi_5 - \Pi_4)$
77	10	$16\Pi_0 \oplus 2\Pi_3 \oplus \Pi_4$
79	12	$16\Pi_0 \oplus \Pi_4 \oplus (\Pi_5 - \Pi_4)$

In this paper, the point P in $\mathrm{PG}(r, 2)$ with coordinate vector $(p_0, p_1, \ldots, p_r)$ is denoted by $(p_0, p_1, \ldots, p_r)$ or simply $p_0 p_1 \ldots p_r$, and the hyperplane defined by the equation $a_0 x_0 + a_1 x_1 + \cdots + a_r x_r = 0$ is denoted by $[a_0 a_1 \ldots a_r]$. For two distinct points $P(p_0, p_1, \ldots, p_r)$ and $Q(q_0, q_1, \ldots, q_r)$ in $\mathrm{PG}(r, 2)$, we denote the point $(p_0 + q_0, p_1 + q_1, \ldots, p_r + q_r)$ by $P + Q$.

Let $\boldsymbol{e}_i = 0 \cdots 010 \cdots 0$ be the point of $\mathrm{PG}(r, 2)$ the only i-th entry of which is 1. Note that $\mathcal{E}_3 = \{1000, 0100, 0010, 0001, 1111\}$ is an elliptic quadric in $\mathrm{PG}(3, 2)$.

Lemma 3.4 ([12]). *There are exactly 11* 16*-divisible* $[78, 10, 16]_2$ *codes up to equivalence, all of whose multisets contain a 1-point.*

Lemma 3.5 ([12]). *There are exactly 23* 16*-divisible* $[79, 10, 16]_2$ *codes up to equivalence, all of whose multisets contain a 1-point.*

4 Proof of Theorem 1.4. Let d be a positive integer and let $\mathcal{C}$ be an $[n, k, d]_q$ code with effective length n. Since $[g_q(k, sq^{k-1}), k, sq^{k-1}]_q$ codes (s-fold simplex codes) exist for any positive integer s, we assume that d is not divisible by q^{k-1}. Then, d can be uniquely expressed with $s = \lceil d/q^{k-1} \rceil$ as

$$d = sq^{k-1} - \sum_{j=1}^{r} q^{u_j - 1}, \tag{6}$$

where r and u_j's are integers satisfying

$$k - 1 \geq u_1 \geq u_2 \geq \cdots \geq u_r \geq 1 \text{ and } u_j > u_{j+q-1} \text{ for } 1 \leq j \leq r - q + 1. \tag{7}$$

The latter condition of (7) means that at most $q-1$ of $u_1, \ldots, u_r$ can take any given value. If $r \leq s$, it is easy to construct Griesmer codes from the multiset of an s-fold simplex code by deleting $F_1 + \cdots F_r$,where F_j denotes a $(u_j - 1)$-flat. In general, a Griesmer code which is obtained from an s-fold simplex code by deleting a union of disjoint flats (at most $q - 1$ of any given dimension) is called a *code of Belov type*.

Lemma 4.1. *There exists a* $[g_q(k, d), k, d]_q$ *code if* $r \leq s$.

Assume $r \geq s + 1$ and let $u = \sum_{i=1}^{s+1} u_i$. The following theorem was proved by Belov et al. [1] for binary linear codes and by Hill [6] and Dodunekov [4] for codes over $\mathbb{F}_q$.

Theorem 4.2 ([6]). *When* $r \geq s + 1$*, there exists a* $[g_q(k, d), k, d]_q$ *code of Belov type if and only if* $u \leq sk$.

Assume l, k, β, τ are integers with $l \geq 3$, $\beta = \binom{l+1}{2} + 1$, $\beta \leq k \leq \beta + l$, $\tau = k - \beta$. Recall that $C_{2,k} = (l-2)2^{k-1} + 2^{k+\tau-l-2} + 2^{k-l-2}$ from (2). A Griesmer $[g_2(k, d), k, d]_2$ code for $d = C_{2,k}$ is not of Belov type by Theorem 4.2 since $u = \sum_{i=1}^{s+1} u_i$ from (6) for $d = C_{2,k}$ satisfies $u = (l-1)k + 1$ with $s = l - 1$. Actually, $C_{2,k}$ is the largest value of d such that a Griesmer $[g_2(k, d), k, d]_2$ code of Belov type does not exist for given $k \geq 5$ [11].

Lemma 4.3. *Let* $\mathcal{C}$ *be a Griesmer* $[g_2(k, d), k, d]_2$ *code for* $d = C_{2,k}$ *and let* $\mathcal{C}^*$ *be a projective dual. Then,*

(a) $g_2(k, C_{2,k}) = (l-2)\theta_{k-1} + \theta_{k+\tau-l-2} + \theta_{k-l-2} + l + 1$.

(b) $\mathcal{C}^*$ *is a* 2^{l-1}*-divisible* $[(l-1)2^l + 1, k, 2^{l-1}]_2$ *code for* $\tau = 0$.

(c) $\mathcal{C}^*$ *is a* 2^l*-divisible* $[(l-1)2^{l+1} + 2^\tau + 1, k, 2^l]_2$ *code for* $\tau \geq 1$.

Proof. The part (a) is obtained from (1). Since $\mathcal{C}$ is 2^{k-l-1}-divisible (resp. 2^{k-l-2}-divisible) for $\tau = 0$ (resp. $\tau \geq 1$) by Lemma 2.6, one can get (b) and (c) applying Lemma 2.2. □

Lemma 4.4. *$n_2(k,d) = g_2(k,d)$ for $\tilde{C}_{2,k} < d \le (l-2)2^{k-1}$.*

Proof. Let $d = \tilde{C}_{2,k} + 1 = (l-2)2^{k-1} - (2^l - 1 - 2^{\tau+1})2^{k-l-2} + 1$ from (3). Since $(2^l - 1 - 2^{\tau+1})2^{k-l-2} - 1 = \theta_{k-3} - 2^{k-l+\tau-1} - 2^{k-l-2}$, we can calculate $u = \sum_{i=1}^{s+1} u_i$ from (6) for $d = \tilde{C}_{2,k} + 1$ as $u = (l-2)k$. Hence, there exists a Griesmer code of Belov type. One can prove similarly for other values of d with $\tilde{C}_{2,k} < d \le (l-2)2^{k-1}$. □

Lemma 4.5. *$n_2(11,d) = g_2(11,d)$ for $2^{11} = 2048 < d \le C_{2,11} = 2112$.*

Proof. Note that $l = 4$ for $k = 11$. Let $\mathcal{C}$ be an 8-divisible $[49, 11, 8]_2$ code with multiset $\mathcal{M}_{\mathcal{C}} = 4\mathcal{E}_3 \oplus 2\Pi_2 \oplus \Pi_3$. Then, the spectrum of $\mathcal{C}$ is $(a_{17}, a_{25}, a_{33}, a_{41}) = (525, 1160, 330, 32)$, and the projective dual $\mathcal{C}^*$ of $\mathcal{C}$ is a $[g_2(11, 2112), 11, C_{2,11} = 2112]_2$ code. Let Λ_0^* be the set of 0-points for $\mathcal{C}^*$, which corresponds to the set of 41-hyperplanes for $\mathcal{C}$. We shall find j-flats F_j, $j = 1, 2, \ldots, 5$ which are disjoint from Λ_0^*. We take $\mathcal{E}_3$, Π_2 and Π_3 in $\Pi_{10} = \mathrm{PG}(10, 2)$ as

$$\mathcal{E}_3 = \{\boldsymbol{e}_1, \boldsymbol{e}_2, \boldsymbol{e}_3, \boldsymbol{e}_4, \sum_{i=1}^{4} \boldsymbol{e}_i\}, \quad \Pi_2 = \langle \boldsymbol{e}_5, \boldsymbol{e}_6, \boldsymbol{e}_7 \rangle, \quad \Pi_3 = \langle \boldsymbol{e}_8, \boldsymbol{e}_9, \boldsymbol{e}_{10}, \boldsymbol{e}_{11} \rangle.$$

Let Δ be the solid containing $\mathcal{E}_3$ and let H be a hyperplane of Π_{10}. Then, $m_{\mathcal{C}}(H) = 41$ if and only if either H contains Δ and one of Π_2, Π_3, or H contains $\Pi_2 \cup \Pi_3$ and $H \cap \Delta$ is a 12-plane. So, we get the 32-set $\Lambda_0^* = \mathcal{T}_3 \cup \Pi_2^* \cup \Pi_3^*$ with

$$\begin{aligned} \mathcal{T}_3 &= \{\boldsymbol{e}_1, \boldsymbol{e}_2, \boldsymbol{e}_3, \boldsymbol{e}_4\} \cup \{\boldsymbol{e}_i + \boldsymbol{e}_j \mid 1 \le i < j \le 4\}, \\ \Pi_2^* &= \langle \boldsymbol{e}_5, \boldsymbol{e}_6, \boldsymbol{e}_7 \rangle, \quad \Pi_3^* = \langle \boldsymbol{e}_8, \boldsymbol{e}_9, \boldsymbol{e}_{10}, \boldsymbol{e}_{11} \rangle. \end{aligned}$$

We take $F_1, F_2, \ldots, F_5$ as

$$\begin{aligned} F_1 &= \langle \boldsymbol{e}_i + \boldsymbol{e}_{i+8} \mid i = 1, 2 \rangle, \ F_2 = \langle \boldsymbol{e}_i + \boldsymbol{e}_{i+7} \mid i = 1, 2, 3 \rangle, \\ F_3 &= \langle \boldsymbol{e}_i + \boldsymbol{e}_{i+4} \mid i = 1, 2, 3, 4 \rangle, \ F_4 = \langle \boldsymbol{e}_i + \boldsymbol{e}_{i+6} \mid i = 1, 2, \ldots, 5 \rangle, \\ F_5 &= \langle \boldsymbol{e}_i + \boldsymbol{e}_{i+5} \mid i = 1, 2, \ldots, 6 \rangle. \end{aligned}$$

Then, it can be checked that $F_i \cap F_j = \emptyset$ for $1 \le i < j \le 5$ except for $(i, j) = (4, 5)$ and that $\Lambda_0^* \cap (F_1 \cup F_2 \cup \cdots \cup F_5) = \emptyset$. Since $F_4 \cap F_5 = \{Q := 11111011111\}$ and Q is a 3-point for $\mathcal{C}^*$, $\mathcal{M}_{\mathcal{C}^*}$ contains the multiset $F_1 + F_2 + \cdots + F_5$. Hence, our assertion follows from Lemma 2.5 since $2112 = 3 \cdot 2^{10} - (2^9 + 2^8 + 2^7 + 2^6)$. □

The following lemma can be confirmed by the exhaustive computer search.

Lemma 4.6. *There exists no 16-divisible $[n, 10, 32]_2$ code for $n = 72, 76, 77, 78$.*

Lemma 4.7. *A $[g_2(11,d), 11, d]_2$ code does not exist for $d = \tilde{C}_{2,11}$.*

Proof. Assume $\mathcal{C}$ is a putative $[g_2(11,d), 11, d]$ code with $d = \tilde{C}_{2,11}$, which is a 32-divisible $[3265, 11, 1632]_2$ code by Lemma 2.6. Then, its projective dual $\mathcal{C}^*$ is a 16-divisible $[83, 11, 16]_2$ code. If there exists a t-point Q with $t > 16$ in $\mathcal{M}_{\mathcal{C}^*}$, then the multiset $\mathcal{M}_{\mathcal{C}^*} - 16Q$ over $\Pi_{10} = \mathrm{PG}(10, 2)$ gives a 16-divisible $[67, 11, d']_2$ code $\mathcal{C}'$. But such a code does not exist for $d' \ge 48$ by the Griesmer bound. For $d' = 16, 32$, the projective

dual of $\mathcal{C}'$ does not exist by the Griesmer bound. Hence, $\mathcal{C}^*$ has at most 16-points, and the spectrum of $\mathcal{C}$ satisfies $a_i = 0$ for any $i \notin \{1633 - 32j \mid 0 \leq j \leq 16\}$. Suppose $a_{1121} > 0$. Then, by Lemma 2.1, a 1121-hyperplane gives a $[1121, 10, 560]_2$ code, which does not exist by the Griesmer bound. Suppose $a_{1153} > 0$. Then, by Lemma 2.1, a 1153-hyperplane gives a Griesmer $[1153, 10, 576]_2$ code whose projective dual is a 4-divisible $[17, 10, 4]_2$ code, which does not exist since $k_2(17, 4) = 8$. In this way, one can prove that $a_{1633-32j} = 0$ for $j = 1, 2, 8, 9, 10, 12, 13, 14, 15, 16$. So, the possible t-points in $\mathcal{M}_{\mathcal{C}^*}$ satisfy

$$t \in \{3, 4, 5, 6, 7, 11\}. \tag{8}$$

Suppose $\mathcal{M}_{\mathcal{C}^*}$ has a 11-point P. By Lemmas 2.8, 4.6 and the Griesmer bound, the projection of $\mathcal{M}_{\mathcal{C}^*} - 11P$ from P onto a hyperplane Π with $P \notin \Pi$ gives a 16-divisible $[72, 10, 16]_2$ code. On the other hand, 16-divisible $[72, 10, 16]_2$ codes are unique up to equivalence by Lemma 3.3 and the multiset of such a code consists of five 8-points and 32 1-points from Table 5, which contradicts (8). Hence, $\mathcal{M}_{\mathcal{C}^*}$ has no 11-point. Using Lemmas 3.3, 3.4, 3.5 and Table 5, one can vanish possible t-points of $\mathcal{M}_{\mathcal{C}^*}$ for $t = 4, 5, 6, 7$, similarly. Then, $\mathcal{M}_{\mathcal{C}^*}$ consists only of 3-points, which is impossible. This completes the proof. □

Now, Theorem 1.4 follows from Lemmas 4.4, 4.5 and 4.7.

REFERENCES.

[1] B. I. BELOV, V. N. LOGACHEV, and V. P. SANDIMIROV. Construction of a class of linear binary codes achieving the Varshamov–Griesmer bound. *Problems of Information Transmission*, 10(3):211–217, 1974.

[2] I. BOUYUKLIEV, D. B. JAFFE, and V. VAVREK. The smallest length of eight-dimensional binary linear codes with prescribed minimum distance. *IEEE Transactions on Information Theory*, 46:981–985, 2002.

[3] A. E. BROUWER and M. van EUPEN. The correspondence between projective codes and 2-weight codes. *Designs, Codes and Cryptography*, 11:261–266, 1997.

[4] S. M. DODUNEKOV. *Optimal Linear Codes*. PhD thesis, Bulgarian Academy of Sciences, Sofia, 1985.

[5] J. H. GRIESMER. A bound for error-correcting codes. *IBM Journal of Research and Development*, 4:532–542, 1960.

[6] R. HILL. Optimal linear codes. In CHRIS MITCHELL, editor, *Cryptography and Coding II*, pages 75–104. Oxford University Press, Oxford, 1992.

[7] R. HILL and E. KOLEV. A survey of recent results on optimal linear codes. In F. C. HOLROYD, K. A. S. QUINN, C. ROWLEY, and B. S. WEBB, editors, *Combinatorial Designs and their Applications*, Research Notes in Mathematics, pages 127–152. Chapman and Hall/CRC, Boca Raton, 1999.

[8] W. C. HUFFMAN and V. PLESS. *Fundamentals of Error-Correcting Codes*. Cambridge University Press, Cambridge, 2003.

[9] Y. INOUE and T. MARUTA. Construction of new Griesmer codes of dimension 5. *Finite Fields and Their Applications*, 55:231–237, 2019.

[10] A. KATO, T. MARUTA, and K. NOMURA. On the construction of optimal linear codes of dimension four. *Bulletin of the Korean Mathematical Society*, 60:1237–1252, 2023.

[11] D. KAWABATA, T. MARUTA, and K. YASUFUKU. A conjecture on the minimum length of linear codes over finite fields. *Designs, Codes and Cryptography*, 93:5039–5054, 2025.

[12] T. KÖRNER and S. KURZ. Lengths of divisible codes with restricted column multiplicities. *Advances in Mathematics of Communications*, 18(2):505–534, 2024.

[13] T. MARUTA. On the nonexistence of q-ary linear codes of dimension five. *Designs, Codes and Cryptography*, 22:165–177, 2001.

[14] T. MARUTA. Construction of optimal linear codes by geometric puncturing. *Serdica Journal of Computing*, 7:73–80, 2013.
[15] M. TAKENAKA, K. OKAMOTO, and T. MARUTA. On optimal non-projective ternary linear codes. *Discrete Mathematics*, 308:842–854, 2008.
[16] H. van TILBORG. The smallest length of binary 7-dimensional linear codes with prescribed minimum distance. *Discrete Mathematics*, 33:197–207, 1981.
[17] H. N. WARD. Divisibility of codes meeting the Griesmer bound. *Journal of Combinatorial Theory, Series A*, 83:79–93, 1998.

Tatsuya Maruta, Taiki Tochiyama and Keita Yasufuku
Department of Mathematics
Osaka Metropolitan University
3-3-138 Sugimoto, Sumiyoshi-ku
Osaka 558-8585 Japan
e-mail: maruta@omu.ac.jp, tt1816@icloud.com, keita0125sve@icloud.com

ХИПОТЕЗА ЗА МИНИМАЛНАТА ДЪЛЖИНА НА БИНАРНИ ЛИНЕЙНИ КОДОВЕ

T. Maruta, T. Tochiyama и K. Yasufuku

Абстракт

Даваме нова хипотеза за $D_{2,k}$, където $D_{q,k}$ означава най-голямото d, за което не съществува линеен код с размерност k и минимално тегло d, удовлетворяващ границата на Griesmer. Също така доказваме, че $D_{2,11} = 1632$, откъдето следва, че нашата хипотеза е вярна за размерности $k \leq 11$.

Ключови думи: граница на Грийсмър, оптимален код, делим код.

МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2026
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2026
Proceedings of the Fifty-Fifth Spring Conference
of the Union of Bulgarian Mathematicians
Tryavna, Bulgaria, April 5–9, 2026

ON THE STRUCTURE OF CYCLIC STEINER TRIPLE SYSTEMS OF SMALL ORDER [1]

Antoaneta Tsvetanova and Stela Zhelezova

Abstract

An n-configuration is a collection of n blocks of a particular STS(v). An n-configuration is full if none of its points occur in just one block. Of special interest for understanding the structure of an STS(v) is the number of its full configurations with no more than $n+2$ points. An STS(v) is n-sparse if every set of i blocks covers more than $i+2$ points, $4 \leq i \leq n$. The first examples of 6-sparse STS(v)s were presented by Forbes, Grannell and Griggs in 2007. The smallest known 6-sparse STS(v) is of order 139. Recently the properties of all STS(19)s were analyzed by Colbourn and coauthors, 2010 and of STS(21)s with nontrivial automorphisms by Erskine, Griggs, 2024 and 6-sparse STS(v)s were not found among them. It is not known if there exists a 6-sparse STS(v) for some order smaller than 139. In an attempt to answer this question we count the number of the full 6-configurations with 8 points in cyclic STS(v)s of small order. There are no 6-sparse ones but we find some examples of STS(v)s, $25 \leq v \leq 63$ with interesting structure.

2020 Mathematics Subject Classification: 05B07, 51E10.

Key words: combinatorial design; Steiner Triple system; configuration.

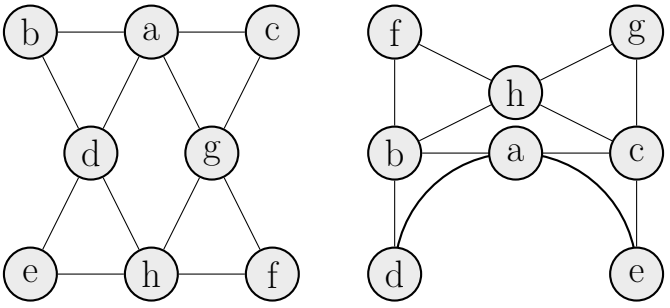
1 Introduction. Let V be a finite set of v *points*, and $\mathcal{B} = \{B_j\}_{j=1}^{b}$ a finite collection of k-element subsets of V, called *blocks*. $D = (V, \mathcal{B})$ is a 2-(v,k,λ) *design* if any 2-element subset of V is contained in exactly λ blocks of $\mathcal{B}$. Designs with $k = 3$ and $\lambda = 1$ are usually called *Steiner triple systems* and denoted by STS(v). Two designs $D_1 = (V_1, \mathcal{B}_1)$ and $D_2 = (V_2, \mathcal{B}_2)$ are *isomorphic* if there is a bijection from V_1 to V_2 which maps each block of D_1 to a block of D_2. A permutation of the design points which maps each block to a block of the same design is an *automorphism*. All the automorphisms of a design form its *full automorphism group* G under composition of permutations. If the automorphism group G contains a cycle of length v the design is *cyclic*. In what follows we denote cyclic STS(v)s by CSTS(v)s. CSTS(v)s have been classified up to order 69 in a series of papers [2, 6, 20]. More details on STS(v)s and CSTS(v)s can be found in [4, 7].

[1] The work is partially supported by the Bulgarian National Science Fund under Contract No KP-06-H62/2-2022.

https://doi.org/10.55630/mem.2026.55.433-441

An *n-configuration* is a collection of n blocks of a particular STS(v), $n < b$. Next we only use the term *configuration* if the number of the involved blocks is not important. The configurations in an STS(v) can be viewed as partial STS(v)s. The *degree* of a configuration point is the number of blocks which contain it. A configuration is *full* if the degree of each of its points is at least two. Two n-configurations are *isomorphic* if there exists a bijection on their point sets which maps each block of the first configuration to a block of the second one. Nonisomorphic full n-configurations are enumerated up to $n \leq 13$ [10, 19].

Next we are interested in the number of occurrences of some configurations in a particular CSTS(v) in connection with their applicability. Of special interest for understanding the structure of an STS(v) is the frequency of appearance of the full configurations with no more than $n + 2$ points. These with small number of blocks are well-known in the literature under special names. The unique up to isomorphism full 4-configuration covers 6 points and is known as *Pasch configuration* (quadrilateral) [3, 16, 25]. The full 5-configuration with $5 + 2 = 7$ points is called the *mitre configuration*, and is unique too [3, 6]. Up to isomorphism there are five full 6-configurations. They are first presented in [21]. Only two of them have $6 + 2 = 8$ points. Two of their points are of degree 3, the other 6 points are of degree 2. If the points of degree 3 are on two disjoint blocks, the *hexagon* configuration is obtained (Fig. 1a). In the other case the two points of degree 3 are in one and the same block and the *crown* configuration arises (Fig. 1b).



a) hexagon configuration b) crown configuration

Figure 1: Full 6-configurations with 8 points

The STS(v)s with lack of Pasch or mitre configurations are intensively studied. An STS(v) is *anti-Pasch* (*anti-mitre*) if it comprises no Pasch (mitre) configurations respectively. In the same manner we can call the STS(v)s missing the hexagon (crown) configuration *anti-hexagon* (*anti-crown*). An STS(v) is *n-sparse* if every set of i blocks covers more than $i + 2$ points, $4 \leq i \leq n$. Every n-sparse STS(v) is also $(n - 1)$-sparse. Hence the anti-Pasch STS(v)s are *4-sparse*. Anti-Pasch and simultaneously anti-mitre STS(v)s are *5-sparse*. For an STS(v) to be *6-sparse* it is enough besides Pasch and mitre configurations not to contain hexagon and crown configurations.

Next in our investigations we will denote by P the number of occurrences of Pasch configurations and by $P_{max}(v)$ the maximal number of Pasch configurations for the CSTS(v) of a particular order. We use respectively M and $M_{max}(v)$ for the number of mitre configurations; H and $H_{max}(v)$ for the hexagon configurations and C and $C_{max}(v)$ for the

crown configurations. Thus to each CSTS(v) we can associate a *configuration vector*. It comprises 4 nonnegative integers, namely (P, M, H, C). A 6-sparse STS(v) should be characterized with an all zero vector. The results for P, $P_{max}(v)$, M and $M_{max}(v)$, $v \leq 61$ are known in advance [3, 6, 25, 26]. In this research we add the results for CSTS(63) and count the frequency of occurrences of hexagon and crown configurations in CSTS(v), $25 \leq v \leq 63$ seeking 6-sparse CSTS(v)s.

For more details on configurations in STS(v)s and on n-sparse STS(v)s we refer to [7, 14, 16, Chapter 13].

2 Preliminary results and motivation. The research on configurations in STS(v)s and on n-sparse STS(v)s was started long ago. There is a conjecture of Erdös [8] that there exists an n-sparse STS(v) for every integer $n \geq 4$ and $v > v_0(n)$, where v_0 is some order of an STS(v). The existence question of 4-sparse (anti-Pasch) STS(v)s is completely settled [17]. They exist for every $v \equiv 1, 3 \pmod 6$, $v \notin \{7, 13\}$.

The 5-sparse STS(v)s have been intensively studied too. The results show that 5-sparse STS(v)s exist for almost all possible orders [13, 28, 29]. Examples of 5-sparse CSTS(v)s up to order $v \leq 97$ are provided in [6, Table 3]. The presented there 5-sparse cyclic STS(19) is unique. The properties of all STS(19)s are studied in [5] by Colbourn and coauthors, and the absence of 6-sparse STS(19)s is reported. Recently all 4-sparse STS(21)s have been cataloged by Kokkala and Östergård [22]. There are three 5-sparse STS(21)s and none of them is 6-sparse. The next 5-sparse CSTS(v)s occur for $v = 33$ and hence give the possibility of searching for 6-sparse CSTS(v)s. But we start our investigations from CSTS(25)s to find out what their structure looks like in connection with 6-configurations.

The first examples of 6-sparse STS(v)s are presented by Forbes, Grannell and Griggs in 2007 [11]. The same authors in their next paper [12] give a construction of 6-sparse STS(v)s for $v = 3p$, $p \equiv 3 \pmod 4$ and large enough. The smallest known 6-sparse STS(v) is of order 139. It is not known if there exists a 6-sparse STS(v) for some smaller order. In [15, Corollary 2.4] Fujiwara shows that a cyclic n-sparse STS(v) does not exist for $n \geq 10$. However no n-sparse STS(v) is known for $n \geq 7$ up to now.

The sparse property of STS(v)s is valuable for their applications in coding theory. An incidence matrix of an STS(v) can be considered as a parity-check matrix of a regular LDPC code [1, 27]. The LDPC codes constructed from CSTS(v)s are especially advantageous. They are well structured and therefore suitable for a hardware implementation with simple shift registers. The CSTS(v)s can ensure low-complexity encoding and good performance with iterative decoding of the associated LDPC codes [18]. It is known that short cycles affect significantly the decoding performance of the LDPC codes regarding the iterative decoding [23]. In [24] the authors propose a modification of the incidence matrix of a CSTS(v) to be used as parity-check matrix of an LDPC code in order to avoid cycles of length 6 (full 6-configurations with 8 points). High sparseness of an STS(v) results in an LDPC code without short cycles and thus of better performance.

Next we will test the CSTS(v)s, $25 \leq v \leq 63$ for 6-sparseness. We count the number of hexagon and crown configurations in CSTS(v)s, $25 \leq v \leq 63$. We do not find 6-sparse CSTS(v)s, but some examples of CSTS(v)s with interesting structure follow.

3 Counting hexagon and crown configurations. We consider the nonisomorphic CSTS(v)s with point set $V = \{1, 2, \ldots, v\}$. They are presented by sets of base blocks.

The collection of blocks of the CSTS(v) can be obtained by the action of the mapping $j \to j+1$, $1 \le j < v$ and $v \to 1$ on the points of the given base blocks. Next we use the design blocks in a lexicographic order defined by the numbers of the points they comprise. This gives us the opportunity to consider the configuration blocks in lexicographic order too. We count only the number of configurations which comprise different blocks by searching over the design blocks. In [19] the authors use a different algorithm for counting the number of n-configurations based on search over the points.

We are interested in the number of copies of two full 6-configurations on 8 points. For both of them two of the points have degree 3. These configurations differ by the place of their degree three points. The hexagon configuration is the unique one for which these two points are in two disjoint blocks. An example is presented graphically in Fig. 1a. It is defined by the following 6 blocks:

$$\{a,b,c\},\{a,d,e\},\{a,f,g\},\{b,d,h\},\{c,g,h\},\{e,f,h\}.$$

The points a and h are of degree 3 and the blocks $\{a,b,c\}$ and $\{e,f,h\}$ are disjoint. To count the number of all copies of the hexagon configuration in a CSTS(v) we consider all pairs of disjoint blocks.

The crown configuration is the unique one for which the two degree three points are in one and the same design block. Fig. 1b illustrates graphically an example of the crown configuration. It comprises the next six blocks:

$$\{a,b,c\},\{a,d,e\},\{b,d,f\},\{b,g,h\},\{c,e,g\},\{c,f,h\}.$$

The points of degree 3 are c and b, and are together in block $\{a,b,c\}$. In order to count the number of all copies of the crown configuration in a CSTS(v) we check all pairs of blocks with a common point as $\{a,b,c\}$ and $\{a,e,d\}$.

4 Results. The most studied configuration in the STS(v)s is the Pasch configuration. It is the smallest one. In comparison with the number of other configurations in consideration, it seems that the number of Pasch configurations is the smallest one and the smallest number of different values for P appears in a CSTS(v) for particular v . There are upper and lower bounds on the maximal number of Pasch configurations [25] and on the number of mitre configurations in an STS(v) [6]. The mitre and especially hexagon and crown configurations are less investigated. In Table 1 we present the maximal values for the number of hexagon and crown configurations in CSTS(v)s, $25 \le v \le 63$. Almost all CSTS(v)s with H_{max} or C_{max} are unique. All the data obtained as a result of this research is available upon request.

v	25	27	31	33	37	39	43	45	49	51	55	57	61	63
H_{max}	100	189	837	330	1443	3159	2322	990	3675	1479	1430	10260	7137	2646
C_{max}	425	486	930	825	1332	1794	2021	2070	2646	2856	3410	4788	4758	5733

Table 1: The values of H_{max} and C_{max} in CSTS(v)s, $25 \le v \le 63$

4.1 Anti-hexagon and anti-crown CSTS(v)s. The number of CSTS(v)s, $25 \le v \le 63$ with lack of hexagon and crown configurations is presented in Table 2. Just for comparison, the number of all CSTS(v)s obtained in [2, 6, 20] is presented in the second

row and the number of 5-sparse CSTS(v)s [6, 26] in the last row of Table 2. One of the new results in this paper is the number of 5-sparse CSTS(63)s (7730). Also we found that 2700317 CSTS(63)s are anti-Pasch and 191313 CSTS(63)s are anti-mitre.

The number of CSTS(v)s without any crown configuration is less than 1% except for CSTS(31)s. The CSTS(27)s are the only ones without any hexagon configuration. The STS(v)s avoiding simultaneously some of these configurations can be of interest too. There are a few examples of STS(v)s with lack of three of the configurations in consideration. We use a generalized configurations vector for a set of CSTS(v)s with the same value for three of the four indicators P, M, H or C. For example $(*, 0, 0, 0)$ denotes the set of all CSTS(v)s with $M = H = C = 0$. The value of P for these CSTS(v)s is different hence we choose to denote it by *. The number of CSTS(v)s with the corresponding generalized configurations vector can be seen in the 5th, 6th and 7th row of Table 2. A vector $(0, *, 0, 0)$ is not mentioned because such CSTS(v)s are not found.

v	25	27	31	33	37	39	43	45	49	51	55	57	61	63
|CSTS(v)|	12	8	80	84	820	798	9508	11616	157340	139828	3027456	2353310	42373196	49526744
anti-hexagon	2	0	12	8	44	22	301	204	2576	1433	29845	14617	245539	190914
anti-crown	0	0	2	0	1	0	1	0	16	1	0	8	5	5
$(*, 0, 0, 0)$	0	0	1	0	0	0	0	0	0	0	0	0	0	5
$(0, 0, *, 0)$	0	0	0	0	0	0	1	0	0	0	0	0	0	0
$(0, 0, 0, *)$	0	0	0	1	0	0	2	0	2	0	7	4	36	11
5-sparse	0	0	0	1	4	1	28	13	155	104	1197	843	9309	**7730**

Table 2: The number of anti-hexagon and anti-crown CSTS(v)s, $25 \leq v \leq 63$

4.2 CSTS(v)s without a crown configuration. Cyclic STS(v)s without crown configurations seem to be very rare (Table 2). Six of them are included in the generalized configurations vector $(*, 0, 0, 0)$ (5th row in Table 2) and appear for two of the considered CSTS(v) orders only. The one is a CSTS(31) isomorphic to the unique design derived from PG$(4, 2)$. Its configurations vector is $(1085, 0, 0, 0)$. The other five are CSTS(63)s (Table 3) one of which is isomorphic to the point-line design of PG$(5, 2)$.

P	2079	3717	4347	6237	9765
|STS(63)|	1	1	1	1	1

Table 3: Properties of STS(63)s with $(*, 0, 0, 0)$ vectors

The upper bound on the number of Pasch configurations in an STS(v) is settled in [25, Theorem 3.1] $P_{max}(v) = v(v-1)(v-3)/24$. It is attained for the point-line STS(v) of the projective space PG$(n, 2)$, $n \geq 2$, $v = 2^{n+1} - 1$. Following this bound $P_{max}(31) = 1085$. The result which we obtain by our program for CSTS(63) is $P_{max}(63) = 9765$ and it coincides with the value calculated by the theorem. We also check the configuration vector of the CSTS(15) connected to PG$(3, 2)$ and get $(105, 0, 0, 0)$. It can be conjectured that the STS(v) corresponding to PG$(n, 2)$ must have the $(P_{max}(v), 0, 0, 0)$ configurations vector.

Despite the relatively large number of CSTS(v)s with lack of hexagon configurations

there is only one example of CSTS(v), $v \leq 63$ with $(0,0,*,0)$ (6th row in Table 2). It is a CSTS(43) with $H = 1806$. The properties of the remaining 32 STS(v)s with $C = 0$ are presented in Table 4. For all of them $H \neq 0$, nine are with generalized configurations vector $(0,*,*,0)$, 14 with $(*,0,*,0)$ and 9 with $(*,*,*,0)$. In the sets with $M \neq 0$ there are CSTS(v)s for which the maximal value of mitre configurations is reached, namely $M_{max}(49) = 1764$ and $M_{max}(57) = 5130$.

v	31	37	49	51	57	61
$(0,*,*,0)$	0	0	0	1	8	0
$(*,0,*,0)$	1	1	8	0	0	4
$(*,*,*,0)$	0	0	0	0	8	1

Table 4: Number of CSTS(v)s with $C = 0$ and at most one other missing configuration

4.3 CSTS(v)s with crown configurations only. Almost all the CSTS(v)s of the considered orders contain many crown configurations and for them the number of the other investigated configurations is not zero. Only 63 CSTS(v)s, $33 \leq v \leq 63$ have generalized configurations vector $(0,0,0,*)$ (7th row in Table 2). Next in Tables 5, 6 and 7 these 63 CSTS(v)s are presented depending on their order. In Table 5 the number of crown configurations for each CSTS(v), $33 \leq v \leq 57$ is given. For each instance of the CSTS(v)s in the table, C is different and less than $C_{max}(v)$ except for CSTS(33) where $C_{max}(33) = 825$ appears.

v	33	43	49	55	57
$(0,0,0,*)$	1	2	2	7	4
C	**825**	1419	1323	1540	1539
		1677	1764	1650	1653
				1870	1881
				1925	2223
				2035	
				2145	
				2255	

Table 5: Properties of CSTS(v)s with $(0,0,0,*)$ vector, $33 \leq v \leq 57$

The properties of CSTS(v)s of the next two orders are presented in Tables 6 and 7 in detail. They comprise 3/4 of all investigated CSTS(v)s with the $(0,0,0,*)$ generalized configurations vector. Here CSTS(v)s with equal values of C occur.

C	1464	1525	1647	1830	1891	1952	2013	2074	2135	2196	2257	2318	2379	2440	2501	2562	2623
|STS(61)|	3	1	1	2	3	2	5	1	1	4	3	1	3	2	1	2	1

Table 6: Properties of CSTS(61)s with the $(0,0,0,*)$ vector

4.4 Conclusion remarks. Before the present work the number of crown and hexagon configurations was known only for STS(19)s [5], and for STS(21)s with nontrivial automorphism groups [9]. Now we know a bit more about the structure of cyclic STS(v)s.

C	1575	1890	1953	2016	2079	2457
|STS(63)|	1	3	1	2	2	2

Table 7: Properties of CSTS(63)s with $(0, 0, 0, *)$ vector

This is especially important in connection with their applications in Coding Theory. The question of the existence of a 6-sparse STS(v) of order less than 139 remains open. Recently the CSTS(v)s with $v = \{67, 69\}$ have been classified [20], but their number is more than 20 times bigger than the number of the nonisomorphic CSTS(63)s. To investigate their structure one should use parallel algorithms.

Our results are computer-aided and that is why mistakes are always possible. We partially verify them in the following ways. We obtain the number of crown and hexagon configurations in a particular CSTS(v) by two different software implementations of both authors. We obtain the same results for the examples of STS(21) presented by Erskine, Griggs [9]:

- three 5-sparse STS(21);
- an STS(21) with no hexagons;
- a cyclic STS(21) with no mitres, no crowns and $H_{max}(21) = 441$ with automorphism group 882;
- two STS(21) with $M_{max}(21) = 252$, each with $H = 252$ and $C = 0$, they are cyclic, with automorphism groups 504 and 1008;
- an STS(21) with $C_{max}(21) = 396$.

REFERENCES.

[1] M. ASIF, W. ZHOU, M. AJMAL, Z. UL A. AKHTAR, and N. A. KHAN. A construction of high performance quasicyclic LDPC codes: a combinatoric design approach. *Wireless Communications and Mobile Computing*:7468792, 2019.

[2] T. BAICHEVA and S. TOPALOVA. Classification results for $(v, k, 1)$ cyclic difference families with small parameters. In M. DEZA, M. PETITJEAN, and K. MARKOV, editors, *Mathematics of Distances and Applications*. Volume 25, Information Science and Computing, pages 24–30. 2012.

[3] A. E. BROUWER. Steiner Triple Systems without Forbidden Subconfigurations. Technical report ZW104/77, Mathematisch Centrum Amsterdam, 1977.

[4] C. J. COLBOURN and J. H. DINITZ, editors. *Handbook of Combinatorial Designs*. CRC Press, Boca Raton, 2nd edition, 2007.

[5] C. J. COLBOURN, A. D. FORBES, M. J. GRANNELL, T. S. GRIGGS, P. KASKI, P. R. J. ÖSTERGÅRD, D. A. PIKE, and O. POTTONEN. Properties of the Steiner triple systems of order 19. *Electronic Journal of Combinatorics*, 17:R98, 2010.

[6] C. J. COLBOURN, E. MENDELSOHN, A. ROSA, and J. ŠIRÁŇ. Anti-mitre Steiner triple systems. *Graphs and Combinatorics*, 10:215–224, 1994.

[7] C. J. COLBOURN and A. ROSA. *Triple Systems*. Clarendon Press, Oxford, 1999.

[8] P. ERDŐS. Problems and results in combinatorial analysis. *Colloquia Mathematica Societatis János Bolyai*, 9:25, 1976.

[9] G. ERSKINE and T. S. GRIGGS. Properties of Steiner triple systems of order 21. *Discrete Mathematics*, 347(11):114–158, 2024.

[10] A. D. FORBES, M. J. GRANNELL, and T. S. GRIGGS. Configurations and trades in Steiner triple systems. *Australasian Journal of Combinatorics*, 29:75–84, 2004.

[11] A. D. FORBES, M. J. GRANNELL, and T. S. GRIGGS. On 6-sparse Steiner triple systems. *Journal of Combinatorial Theory, Series A*, 114(2):235–252, 2007.
[12] A. D. FORBES, M. J. GRANNELL, and T. S. GRIGGS. Further 6-sparse Steiner triple systems. *Graphs and Combinatorics*, 25:49–64, 2009.
[13] Y. FUJIWARA. Infinite classes of anti-mitre and 5-sparse Steiner triple systems. *Journal of Combinatorial Designs*, 14:237–250, 2006.
[14] Y. FUJIWARA. Sparseness of triple systems: a survey. In *Theory and Applications of Combinatorial Designs with Related Field*, volume 1465 of *RIMS Kokyuroku*, pages 173–185, Kyoto, 2006.
[15] Y. FUJIWARA. Nonexistence of sparse triple systems over abelian groups and involutions. *Journal of Algebraic Combinatorics*, 26(4):495–506, 2007.
[16] M. J. GRANNELL and T. S. GRIGGS. Configurations in Steiner triple systems. In F. C. HOLROYD, K. A. S. QUINN, C. ROWLEY, and B. S. WEBB, editors, *Combinatorial Designs and Their Applications*, pages 103–126. Chapman and Hall/CRC, Boca Raton, 1999.
[17] M. J. GRANNELL, T. S. GRIGGS, and C. A. WHITEHEAD. The resolution of the anti-Pasch conjecture. *Journal of Combinatorial Designs*, 8(4):300–309, 2000.
[18] A. GRUNER and M. HUBER. New combinatorial construction techniques for low-density parity-check codes and systematic repeat-accumulate codes. *IEEE Transactions on Communications*, 60(9):2387–2395, 2012.
[19] D. HEINLEIN and P. R. J. ÖSTERGÅRD. Algorithms and complexity for counting configurations in Steiner triple systems. *Journal of Combinatorial Designs*, 30:527–546, 2022.
[20] I. HETMAN, T. BAICHEVA, and S. TOPALOVA. Construction of $(v, k, 1)$ cyclic difference families with small parameters. *Journal of Algebra, Combinatorics, Discrete Structures and Applications*, 13(1):111–119, 2026.
[21] P. HORAK, N. K. C. PHILLIPS, W. D. WALLIS, and J. L. YUCAS. Counting frequencies of configurations in Steiner triple systems. *Ars Combinatoria*, 46:65–75, 1997.
[22] J. I. KOKKALA and P. R. J. ÖSTERGÅRD. Sparse Steiner triple systems of order 21. *Journal of Combinatorial Designs*, 29(2):75–83, 2021.
[23] D. J. C. MACKAY. Good error-correcting codes based on very sparse matrices. *IEEE Transactions on Information Theory*, 45(2):399–431, 1999.
[24] H. PARK, S. HONG, J.-S. NO, and D.-J. SHIN. Design of multiple-edge protographs for QC LDPC codes avoiding short inevitable cycles. *IEEE Transactions on Information Theory*, 59(7):4598–4614, 2013.
[25] D. R. STINSON and Y. J. WEI. Some results on quadrilaterals in Steiner triple systems. *Discrete Mathematics*, 105(1–3):207–219, 1992.
[26] A. TSVETANOVA and S. ZHELEZOVA. Useful configurations in cyclic Steiner triple systems of small order, 2025. To appear in Studies in Computational Intelligence.
[27] B. VASIC and O. MILENKOVIC. Combinatorial constructions of low-density parity-check codes for iterative decoding. *IEEE Transactions on Information Theory*, 50:1156–1176, 2004.
[28] A. WOLFE. The resolution of the anti-mitre Steiner triple system conjecture. *Journal of Combinatorial Designs*, 14:229–236, 2006.
[29] A. WOLFE. The existence of 5-sparse Steiner triple systems of order $n \equiv 3 \pmod 6$, $n \neq \{9, 15\}$. *Journal of Combinatorial Theory, Series A*, 115(8):1487–1503, 2008.

Antoaneta Tsvetanova, Stela Zhelezova
Institute of Mathematics and Informatics
Bulgarian Academy of Sciences
78 Nikola Gabrovski Street, P.O. box 323
5000 Veliko Tarnovo
e-mail: a.cvetanova@math.bas.bg, stela@math.bas.bg

ЗА СТРУКТУРАТА НА ЦИКЛИЧНИТЕ ЩАЙНЕРОВИ СИСТЕМИ ОТ ТРОЙКИ МАЛЪК РЕД

Антоанета Цветанова и Стела Железова

Абстракт

Колекция от n блока в Щайнерова система от тройки от ред v (STS(v)) се нарича n-конфигурация. Една n-конфигурация е пълна, ако никоя от точките ѝ не участва само в един блок. От специален интерес за разбиране на структурата на STS(v) е броят на пълните конфигурации с не повече от $n+2$ точки, които тя притежава. STS(v) е n-sparse, ако всяко множество от i блока е инцидентно с повече от $i+2$ точки, $4 \leq i \leq n$. Първите примери на 6-sparse STS(v) са публикувани от Forbes, Grannell и Griggs през 2007. Най-малката известна 6-sparse STS(v) е от ред 139. Свойствата на всички STS(19) са анализирани през 2010 от Colbourn и съавтори и на STS(21) с нетривиални групи от автоморфизми от Erskine, Griggs, 2024. Не са намерени 6-sparse STS(v) между тях. Не се знае съществуват ли 6-sparse STS(v) от редове по-малки от 139. В опит да отговорим на този въпрос, изследваме броя на пълните 6-конфигурации с 8 точки в цикличните STS(v) от малък ред. Не намираме 6-sparse циклични STS(v), $25 \leq v \leq 63$, но представяме някои примери с интересна структура.

Ключови думи: комбинаторен дизайн; Щайнерова система от тройки; конфигурация.

МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2026
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2026
Proceedings of the Fifty-Fifth Spring Conference
of the Union of Bulgarian Mathematicians
Tryavna, Bulgaria, April 5–9, 2026

ON THE TERNARY EXTENDED PERFECT GOLAY CODE BY THE MODIFIED GC-CONSTRUCTION

D. V. Zinoviev and V. A. Zinoviev

Abstract

It is shown that the ternary extended perfect Golay $[12, 6, 6]_3$-code can be constructed by the modified GC-construction. For the binary Golay $[24, 12, 8]$-code this has been shown by us earlier. In particular, the Golay $[12, 6, 6]_3$-code can be constructed using the GC-construction with the inner codes of length 3 and the outer codes of length 4.

2020 Mathematics Subject Classification: 94B60, 94B25.

Key words: the ternary extended perfect Golay code, modified generalised concatenation construction.

1 Introduction. Let $E_q = \{0, 1, \ldots, q-1\}$ be the alphabet of size q. A q-ary block code C is an arbitrary nonempty subset of E_q^n. We say that C is an $(n, N, d)_q$-code, where n is the *length* of the code, $N = |C|$ is the number of codewords, i.e. the *cardinality* of C, and d is the *minimum Hamming distance*. A linear code C over the Galois field $\mathbb{F}_q$ of order q with parameters $(n, N = q^k, d)_q$ is denoted by $[n, k, d]_q$. Let $J = \{1, 2, \ldots, n\}$ be the coordinate set of E_q^n. For any vector $\mathbf{x} = (x_1, \ldots, x_n) \in E_q^n$, we denote by $\mathrm{supp}(\mathbf{x})$ its support, i.e.

$$\mathrm{supp}(\mathbf{x}) = \{i \in J : \ x_i \neq 0\}.$$

Let $\mathrm{wt}(\mathbf{x})$ be the weight of vector $\mathbf{x}$, i.e. the cardinality of its support: $\mathrm{wt}(\mathbf{x}) = |\mathrm{supp}(\mathbf{x})|$. The *parity* of any vector is the sum of its coordinates (in the field $\mathbb{F}_3$). In this case, the parity of any vector can be 0, 1 or 2.

Here, we restrict ourselves to the ternary codes. Thus, throughout the whole paper, we drop the size of the alphabet and use $[n, k, d]$ to denote a $[n, k, d]_3$-code over $\mathbb{F}_3$.

In the recent publication [6], we showed that the extended perfect $[24, 12, 8]_2$ Golay code can be constructed using the GC-construction (see [2] for the details on the Golay code). The goal of this work is to prove a similar result for the ternary extended perfect Golay $[12, 6, 6]_3$-code. In particular, this code is obtained using the modified GC-construction.

It is necessary to mention that the interest in cascade and generalized cascade codes is caused by the possibility of cascade decoding, which realizes the code distance by decoding short inner and outer codes (see [1, 9, 8] and the references therein). Consequently, the soft decoding is possible [4].

https://doi.org/10.55630/mem.2026.55.442-447

2 Preliminary results. In order to make this paper more self-sufficient, following [6, 7, 5], we repeat the well known generalized concatenation (GC) construction for the ternary codes. This construction is based on a nested family of inner codes of a fixed length n_b. In this paper, we need the inner codes of length $n_b = 3$ that we are going to introduce in the next section. Here we provide several trivial statements.

Lemma 2.1. *(i) If code C of length n consists of all vectors of length n of parity 0, then it is linear.*

(ii) Let C be an arbitrary linear code and let C_1 and C_2 be its cosets, given by

$$C_1 = C + \mathbf{b}_1, \;\; C_2 = C + \mathbf{b}_2.$$

If the vectors $\mathbf{b}_1$ and $\mathbf{b}_2$ are such that $\mathbf{b}_1 + \mathbf{b}_2$ is the zero vector, then, the code $C \bigcup C_1 \bigcup C_2$ is also linear.

Proof. (i) By construction, the set C is closed under the addition. Indeed, the sum of two words of parity 0, has parity 0, and the statement follows.

(ii) It is easy to verify that the code $C \cup C_1 \cup C_2$ is closed under the addition of its codewords, thus the statement follows. □

2.1 Inner codes of length 3. Consider the inner codes of length $n_b = 3$ over the field $\mathbb{F}_3$. These codes are denoted by B_i with some index i which represents the subdivision step and the tuple of i indices $(j_1, j_2, \ldots, j_i)$. Let B be the $[3, 3, 1]$-code, i.e. the set of all ternary vectors of length 3. This code can be subdivided into three $(3, 9, 2)$ subcodes: the linear $[3, 2, 2]$-code $B_1(0)$ and its cosets, the $(3, 9, 2)$ codes $B_1(1)$ and $B_1(2)$. The code $B_1(0)$ contains the trivial $[3, 1, 3]$-code $B_2(0, 0)$, which partitions the code $B_1(0)$ into the cosets of $B_2(0, 0)$, i.e.

$$B_1(0) = B_2(0,0) \bigcup B_2(0,1) \bigcup B_2(0,2) = \bigcup_{t=0}^{2} B_2(0,t).$$

We write out these codes explicitly

$$B_2(0,0) = \begin{bmatrix} (000) \\ (111) \\ (222) \end{bmatrix}, B_2(0,1) = \begin{bmatrix} (012) \\ (120) \\ (201) \end{bmatrix}, B_2(0,2) = \begin{bmatrix} (021) \\ (102) \\ (210) \end{bmatrix}.$$

Thus, we have defined a nested chain of codes of length 3:
the trivial $[3, 3, 1]_3$-code $B_0 = B$,
the trivial $[3, 2, 2]_3$-code $B_1(0)$,
the trivial $[3, 1, 3]_3$-code $B_2(0, 0)$.
These codes induce the following alphabets sizes of the outer codes:

$$q_1 = q_2 = q_3 = 3.$$

Recall that the sum of a matrix $B = [\mathbf{b}_i]$ (here $\mathbf{b}_i$ is the i-th row) and vector $\mathbf{x}$ is defined as $B + \mathbf{x} = [\mathbf{b}_i + \mathbf{x}]$, where the vector $\mathbf{x}$ is added to every row.

Thus, we have subdivided the set of all vectors of length 3 into $[3,1,3]$-codes $B_2(i,j)$. Every such code B can be presented as: $B = B_2(0,0) + \mathbf{b}$ for some vector $\mathbf{b}$. This presentation defines the following additive operation of two different codes $B = B_2(0,0) + \mathbf{b}$ and $B' = B_2(0,0) + \mathbf{b}'$. The sum $B'' = B + B'$ of two codes is defined as $B'' = B_2(0,0) + \mathbf{b}''$, where $\mathbf{b}'' = \mathbf{b} + \mathbf{b}'$.

Enumerate all ternary vectors of length 3. Assume that the s-th row $\mathbf{b} \in \mathbb{F}_3^3$ of the above matrices $B_2(i,j)$ is the s-th codeword of the corresponding code. In particular, if the word $\mathbf{b}$ belongs to the code $B_2(i,j)$ then, it is assigned index (i,j,s), and we write $\mathbf{b} = \mathbf{b}(i,j,s)$. So, any vector $\mathbf{b}(i,j,s) \in \mathbb{F}_3^3$ is the s-th codeword of the code $B_2(i,j)$.

The introduced enumeration of the ternary vectors of length 3 is linear in all three indices under the addition of codes as well as vectors. Thus it is useful to define a map μ from the set of vectors $\mathbf{x} = (x_1, x_2, x_3)$ of length 3 over $\mathbb{F}_3$ into the ring $\mathbb{Z}_{3^3}$ of integers

$$\mu(x_1, x_2, x_3) = \sum_{t=1}^{3} x_t 3^{t-1}.$$

The following statement is obvious:

Lemma 2.2. *Let $B_2(i,j)$ and $B_2(i',j')$ be two arbitrary codes of length 3, and let $\mathbf{b}(i,j,s) \in B_2(i,j)$ and $\mathbf{b}(i',j',s') \in B_2(i',j')$ be two arbitrary codewords of these codes. The sum of these codes*

$$B'' = B_2(i,j) + B_2(i',j')$$

and its codewords are such that

$$\mathbf{b} = \mathbf{b}(i,j,s) + \mathbf{b}(i',j',s').$$

Then

(i) The code B'' has index (i'',j'') equal to the coordinate-wise sum (in the field $\mathbb{F}_3$) of the corresponding indices, i.e.

$$i'' = i + i', \quad j'' = j + j'.$$

(ii) The code B'' is equal to

$$B = B_2(0,0) + \mathbf{b}'',$$

where the vector $\mathbf{b}''$ is the sum of two vectors $\mathbf{b}'' = \mathbf{b} + \mathbf{b}'$.

(iii) The vector $\mathbf{b}''$ is of the form $\mathbf{b}''(i'',j'',s'')$, whose indices i'', j'' and s'' are the sums (in the field $\mathbb{F}_3$) of indices of the corresponding terms, i.e.

$$i'' = i + i', \quad j'' = j + j', \quad s'' = s + s'.$$

(iv) The codeword $\mathbf{b}(i'',j'',s'')$, which is the sum of two codewords $\mathbf{b}(i,j,s)$ and $\mathbf{b}(i',j',s')$ of the codes $B_2(i,j)$ and $B_2(i',j')$ respectively, can be presented as $\mathbf{b}(i'',j'',s'')$ of the code $B_2(i'',j'')$, which is the sum of the codes $B_2(i,j)$ and $B_2(i',j')$ with these codewords.

Our construction consists of the following steps. First, using the standard *GC*-construction we construct the linear $[12, 5, 6]_3$-code C_0. Then, we find two cosets C_1 and C_2 of this code at distance 6 from the code C_0, and also $d(C_1, C_2) = 6$, so that the union of three codes C_0, C_1 and C_2 is the code with the minimum Hamming distance 6. Thus, using the classical GC-construction construct the $[12, 5, 6]$-code C_0. Here, we use only two outer codes instead of (according to the nested chain of the inner codes) the possible three. Indeed, there is no code A_1 with distance 6, since the length is 4.

Outer codes A_i for the construction of the code C_0: The ternary perfect $[4, 2, 3]$-Hamming code A_2, the ternary $[4, 3, 2]$-code A_3 with parity check.

We will provide these codes explicitly. The outer $[4, 2, 3]_3$-Hamming code A_2 is the union of three subcodes $A_{2,0}$, $A_{2,1}$ and $A_{2,2}$ listed below

$$A_{2,0} = \begin{bmatrix} (0000) \\ (0111) \\ (0222) \end{bmatrix}, \; A_{2,1} = \begin{bmatrix} (1012) \\ (1201) \\ (1120) \end{bmatrix}, \; A_{2,2} = \begin{bmatrix} (2021) \\ (2102) \\ (2210) \end{bmatrix}.$$

We also list below the outer code A_3 which is the union of three subcodes $A_{3,0}$, $A_{3,1}$ and $A_{3,2}$:

$$A_{3,0} = \begin{bmatrix} (0000) \\ (0012) \\ (0021) \\ (0102) \\ (0111) \\ (0120) \\ (0201) \\ (0210) \\ (0222) \end{bmatrix}, \; A_{3,1} = \begin{bmatrix} (1002) \\ (1011) \\ (1020) \\ (1102) \\ (1111) \\ (1120) \\ (1201) \\ (1210) \\ (1222) \end{bmatrix}, \; A_{3,2} = \begin{bmatrix} (2001) \\ (2010) \\ (2022) \\ (2100) \\ (2112) \\ (2121) \\ (2202) \\ (2211) \\ (2220) \end{bmatrix}.$$

Now we construct the linear $[12, 5, 6]$-code C_0 using the standard GC-construction with the given inner and outer codes. Lemma 2.1 implies that this code is linear. We are interested in the distance between the code C_0 and its cosets C_1 and C_2.

3 Ternary extended perfect Golay code. We want to find two vectors $\mathbf{b}_1$ and $\mathbf{b}_2$ so that the union of three codes

$$C = C_0 \bigcup C_1 \bigcup C_2,$$

where $C_1 = C_0 + \mathbf{b}_1$ and $C_2 = C_0 + \mathbf{b}_2$ is the ternary Golay code $\mathcal{G}_{12}$.

Lemma 3.1. *Consider the following two vectors $\mathbf{b}_1$ and $\mathbf{b}_2$*

$$\mathbf{b}_1 = (001, 001, 010, 211), \;\; \mathbf{b}_2 = (002, 002, 020, 122),$$

which satisfy $\mathbf{b}_1 + \mathbf{b}_2 = \mathbf{0}$. Then

(i) The minimal weight of the codewords of C_1 and C_2 is equal to 6.

(ii) The $[12, 6, 6]$-code C, obtained as the union of codes C_0, C_1 and C_2 is linear and has the minimal distance 6.

Proof. By Lemma 2.1 and direct verification. □

The following is the main theorem.

Theorem 3.2. *The code C, defined above as the union of codes C_0, C_1, and C_2, has parameters $[12, 6, 6]$. Then it is the ternary extended perfect Golay $[12, 6, 6]$-code $\mathcal{G}_{12}$.*

Proof. Lemma 2.1 and Lemma 3.1 imply that the code C is the ternary linear $[12, 6, 6]$-code. It follows from the classical result of Vera Pless [3] that the constructed $[12, 6, 6]$-code is the ternary extended perfect Golay code. □

Acknowledgements. The research of the second author of the paper was carried out at the Institute for Information Transmission Problems of the Russian Academy of Sciences within the program of fundamental research on the topic "Mathematical Foundations of the Theory of Error-Correcting Codes" and was also partly supported by the Higher School of Modern Mathematics MIPT, Moscow College of Physics and Technology, 1 Klimentovskiy per., Moscow, Russia.

REFERENCES.

[1] I. DUMER, V. ZINOVIEV, and V. ZYABLOV. Concatenated decoding according to minimal generalized distance. *Problems of Control and Information Theory*, 10(1):3–19, 1981.
[2] F. J. MACWILLIAMS and N. J. A. SLOANE. *The theory of Error Correcting Codes*. North-Holland, 1986.
[3] V. PLESS. On the uniqueness of the golay codes. *J. Comb. Theory*, 5:215–228, 1968.
[4] V. ZINOVIEV, V. ZYABLOV, and N. VVEDENSKAYA. Comparizon of some algorithms of concatenated decoding. In *Proc. of 8-th All-Union Conf. on Coding Theory and Inform. Transm.* Pages 13–18, Moscow-Kuibyshev, 1981.
[5] V. A. ZINOVIEV. Generalized concatenated codes. *Problems of Information Transmission*, 12(1):5–15, 1976.
[6] V. A. ZINOVIEV and D. V. ZINOVIEV. On generalized concatenated construction of Nordstrom–Robinson code and binary Golay code. *Problems of Information Transmission*, 57(4):34–44, 2021.
[7] V. A. ZINOVIEV and D. V. ZINOVIEV. On binary self-dual extremal double-even codes of length 80. *Proc. Of Moscow Inst. Phys.-Tech.*, 14(2):85–94, 2022.
[8] V. A. ZINOVIEV and V. V. ZYABLOV. Codes with unequal protection of information symbols. *Problems of Information Transmission*, 15(3):50–60, 1979.
[9] V. A. ZINOVIEV and V. V. ZYABLOV. Correction of error bursts and independent errors using generalized concatenated codes. *Problems of Information Transmission*, 15(2):58–70, 1979.

Dimitrii Victorovich Zinoviev
e-mail: dvzinov@gmail.com

Victor Alexandrovich Zinoviev
A.A. Kharkevich Institute for Information Transmission Problems
Russian Academy of Sciences
Bol'shoi Karetnyi 19, Moscow, Russia
Russia and Higher School of Modern
Mathematics of the Moscow College of Physics and Technology in Dolgoprudny,
1 Klimentovskiy per., Moscow, Russia
e-mail: vazinov@iitp.ru

ЗА ТРОИЧНИЯ РАЗШИРЕН СЪВЪРШЕН КОД НА ГОЛЕЙ ЧРЕЗ МОДИФИЦИРАНАТА GC-КОНСТРУКЦИЯ

Д. В. Зиновьев и В. А. Зиновьев

Абстракт

Показано е, че троичният разширен съвършен код на Голей $[12, 6, 6]_3$ може да бъде конструиран чрез модифицираната GC-конструкция, като за бинарния код на Голей $[24, 12, 8]$ това беше доказано от нас по-рано. В частност, кодът на Голей $[12, 6, 6]_3$ може да бъде конструиран с GC-конструкция с вътрешни кодове с дължина 3 и външни кодове с дължина 4.

Ключови думи: троичен разширен съвършен код на Голей, модифицирана обобщена конкатенационна конструкция.

CONTENTS

INTRODUCTION 317

T. Alexandrova, H. Kostadinov, N. L. Manev. Integer codes and their applications: an overview 320

T. Baicheva, S. Topalova. New optimal $(v, k, 1)$ optical orthogonal codes with $k = 3, 5, 6$ 329

Y. Borissov, M. Markov. Verifying the computed weight distribution for the binary Reed–Muller Code R(4,9) 340

J. Borges, J. Rifà, V. A. Zinoviev. On maximum distance separable and completely regular codes 350

S. Boumova, V. Drensky. On cyclic invariants of the free associative algebra . . . 357

S. Bouyuklieva, I. Bouyukliev. Griesmer codes, Grey–Rankin bound and the projective dual transform 370

P. Boyvalenkov, D. Cherkashin, P. Dragnev, D. Yorgov, V. Yorgov. On T-avoiding spherical codes and designs in 32-dimensional Euclidean space 382

M. Grassl, D. Krotov, L. Sok, P. Solé. The punctured dodecacode is unique 393

I. Landjev, A. Rousseva. On the maximal length of near-MDS codes 405

P. Loidreau. Gabidulin codes based post-quantum encryption schemes 414

T. Maruta, T. Tochiyama, K. Yasufuku. A conjecture on the minimum length of binary linear codes 423

A. Tsvetanova, S. Zhelezova. On the structure of cyclic Steiner triple systems of small order 433

D. V. Zinoviev, V. A. Zinoviev. On the ternary extended perfect Golay code by the modified GC-construction 442

СЪДЪРЖАНИЕ

ПРЕДГОВОР 317

Т. Александрова, Х. Костадинов, Н. Л. Манев. Кратък обзор на целочислените кодове и техните приложения 320

Ц. Байчева, С. Топалова. Нови оптимални $(v, k, 1)$ оптични ортогонални кодове с $k = 3, 5, 6$ 329

Ю. Борисов, М. Марков. Верификация на изчисленото разпределение на теглата за двоичния код на Рийд-Малер R(4,9) 340

J. Borges, J. Rifà, V. A. Zinoviev. За максимално раздалечими и напълно регулярни кодов 350

С. Бумова, В. Дренски. За цикличните инварианти на свободната асоциативна алгебра 357

С. Буюклиева, И. Буюклиев. Грийсмърови кодове, граница на Грей-Ранкин и проективно-дуална трансформация 370

П. Бойваленков, Д. Черкашин, П. Драгнев, Д. Йоргов, В. Йоргов. Върху T-избягващи сферични кодове и дизайни в 32-мерното Евклидово пространство 382

M. Grassl, D. Krotov, L. Sok, P. Solé. Скъсеният додекакод е единствен 393

И. Ланджев, А. Русева. Върху максималната дължина на почти-МДР кодове 405

P. Loidreau. Постквантови криптографски схеми, базирани на кодовете на Габидулин 414

T. Maruta, T. Tochiyama, K. Yasufuku. Хипотеза за минималната дължина на бинарни линейни кодове 423

А. Цветанова, С. Железова. За структурата на цикличните Щайнерови системи от тройки малък ред 433

Д. В. Зиновьев, В. А. Зиновьев. За троичния разширен съвършен код на Голей чрез модифицираната GC-конструкция 442