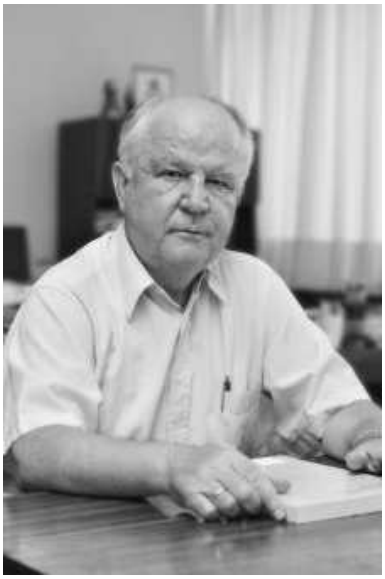
МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2020
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2020
Proceedings of the Forty-ninth Spring Conference
of the Union of Bulgarian Mathematicians
2020

75 ГОДИНИ ОТ РОЖДЕНИЕТО НА АКАД. СТЕФАН ДОДУНЕКОВ*

Цонка Байчева, Петър Бойваленков, Илия Буюклиев



На 5 август 2012 г. завинаги ни напусна нашият учител, колега и приятел академик Стефан Додунеков. Той щеше да навърши 67 години само месец по-късно, а през тази година се навършват 75 години от рождението му. В спомените на голяма част от колегията Стефан Додунеков е учен – специалист по теория на кодирането, администратор – директор на ИМИ–БАН, председател на СМБ, председател на БАН (уви, за кратко), преподавател, приятел. За нас обаче Стефан Додунеков е преди всичко Учител с главна буква – създател на българската школа по теория на кодирането, станала известна в целия свят.

Създадената от Стефан Додунеков школа в областта на Алгебричната и комбинаторна теория на кодирането не е формална структура. През годините в нея

*Тази статия е частично подкрепена от Национална научна програма „Информационни и комуникационни технологии за единен цифров пазар в науката, образованието и сигурността (ИКТвНОС)“ на МОН и проект 12/8 от 15.12.2017 на ФНИ.

се включваха учени от различни институции – ИМИ–БАН, ФМИ–СУ, НБУ, ФМИ–ВТУ, ФМИ–ШУ, ТУ Габрово, ЮЗУ, БСУ, РУ. По традиция, веднъж годишно се събираме на националния семинар по теория на кодирането, където всеки представя резултати, получени през годината, обменят се мнения, представят се докторантите, набелязват се и се координират планове и проекти. Семинарът през ноември 2019 г. беше с рекорден брой участници – над 50. Програмата зае плътно два работни дни, като се обсъдиха и три проекта за дисертации.

По инициатива на Стефан Додунеков са създадени и се провеждат и до днес две серии от международни конференции – българо-руската (започнала като българо-съветска, но винаги с английския като единствен официален език) *Algebraic and Combinatorial Coding Theory* (ACCT) и организираната от ИМИ *Optimal Codes and Related Topics* (OCRT). На тези конференции идват изявени учени от областта, представят се млади колеги, които тепърва започват изследователската си кариера, и българските учени получават прекрасна възможност да обсъдят с чуждестранните колеги актуални и нововъзникващи теми.

Основните инициатори на ACCT са Стефан Додунеков и Леонид Бассалыго от Института по проблеми на предаването на информацията на РАН. Те са и съпредседатели на организационния комитет на първите 13 издания на конференцията, а проф. Бассалыго, който е ученик на Колмогоров, неведнъж е подчертавал, че отдавна вече не ходи на други конференции, освен на ACCT.

Стефан Додунеков инициира работата по много от тематиките, по които изследователите, работещи в областта на теорията на кодирането в България, работиха, а по някои от тях и продължават да се работят – оптимални линейни кодове, самодуални кодове, CRC кодове, near-MDS кодове (въведени от него и Ланджев), добри и точни кодове, сферични кодове[1].

Ще завършим този кратък обзор на наследството на Стефан Додунеков с неговия индивидуален подход към всеки от групата. Съдействаше или организираше различни специализации, обмени за повишаване на квалификацията (в България и чужбина), настояваше и поощряваше да се кандидатства за проекти и стипендии, да се участва в конференции. Ще отбележим няколко цитата: „Колеги, в нашата работа се искат три неща – конструктивизъм, позитивизъм и добронамереност“, „Срещу заобикалящата ни посредственост може да се борим само с професионализъм“, „От наука не се забогатява, но се оцелява, при това интересно“, „Където отивате – гледайте внимателно и „купувайте“, та като се върнете да има на какво да научите и другите“.

На следващите страници ще се спрем накратко на някои резултати, свързани с изследвания на оптимални кодове, тематика, която Стефан Додунеков разви с учениците си в България.

1. Оптимални кодове. Една от сферите, в които Додунеков има важни научни постижения, се отнася до възможните параметри и някои основни свойства на оптималните линейни кодове спрямо някои от познатите граници.

[1] В интерес на истината, Стефан Додунеков смяташе, че един от авторите на тези редове ще работи успешно в областта на конструирането на добри сферични кодове. Но нещата се завъртяха – получиха се резултати за несъществуване, универсални граници, необходими и достатъчни условия за тяхната оптималност и т.н., и при всички случаи помощта на Додунеков беше навременна и изключително важна.

Нека F_q е крайно поле с q елемента, където q е степен на просто число. Да означим n-мерното векторно пространство над това поле с F_q^n. Разстояние по Хеминг между два вектора x и y от F_q^n се дефинира като брой на позициите, в които те се различават. Тегло (по Хеминг) $wt(x)$ на вектор $x \in F_q^n$ ще наричаме броя на ненулевите координати на x. Подпространство C с размерност k на линейното пространство F_q^n ще наричаме линеен код с дължина n и размерност k. Минимално разстояние (минимално тегло) на линеен код ще наричаме най-малкото измежду теглата на ненулевите вектори на кода. С $[n, k, d; q]$ ще означаваме линеен код с дължина n, размерност k и минимално разстояние d над поле с q елемента.

Една от основните задачи на теорията на кодирането е оптимизирането на един от параметрите n, k и d на линеен код над крайно поле по зададени другите два. С параметрите n и d при фиксирано k се свързват следните две функции:

$n_q(k, d)$ – минималното n, за което съществува $[n, k, d; q]$ код при зададени k и d;

$d_q(n, k)$ – максималното d, за което съществува $[n, k, d; q]$ код при зададени n и k.

Намирането на точните стойности на тези функции се свежда до:

– конструиране на кодове с фиксирани параметри;

– доказване несъществуването на кодове с определени параметри.

Кодовете с параметри $[n_q(k, d), k, d; q]$ и $[n, k, d_q(n, k); q]$ се наричат оптимални.

Първите оптимални линейни кодове са конструирани със самото зараждане на теорията на кодирането. Една част от известните оптимални двоични линейни кодове с голямо практическо и теоретично значение са описани от МакУйлямс и Слоен [5] и др.

В [25] е получена следната оценка отдолу за $n_q(k, d)$:

$$n_q(k, d) \geq g_q(k, d) = \sum_{i=0}^{k-1} \lceil d/q^i \rceil.$$

Тази граница е известна като *граница на Грийсмър*. Кодове, за които тя се достига, се наричат *Грийсмърови*.

Границата на Грийсмър има особена роля поради факта, че за фиксирани k всички оптимални кодове с достатъчно големи d я достигат [3, 4], т.е. има само краен брой оптимални кодове, които не са Грийсмърови. В тази посока Додунеков доказва следните твърдения:

Теорема 1 ([2]). *Нека* $d = s(q-1)q^{k-1} - \sum_{i=0}^{p} a_i q^{u_i - 1}$, *където* $s = \lceil d/(q-1)q \rceil$, $k = u_0 > u_1 > \cdots > u_p \geq 1$, $0 \leq a_0 \leq q-2$, $1 \leq a_i \leq q-1$ *за* $i = 1, 2, \ldots, p$. *Код с параметри* $[g_q(k, d), k, d; q]$ *съществува тогава и само тогава, когато* $\sum_{i=1}^{\min(s+1,p)} u_i \leq sk$.

Следствие от теорема 1 е:

Теорема 2 ([2, 26]). *За всяка размерност* k *съществува константа* $D(k)$, *такава, че* $n_q(k, d) = g_q(k, d)$ *при* $d \geq D(k)$.

Следното твърдение дава съществена информация за вида на пораждащата матрица на Грийсмърови кодове.

Теорема 3 ([2, 15]). *Ако* $d \leq sq^{k-1}$, *то всяка пораждаща матрица на* $[g_q(k, d) + t, k, d; q]$ *код* C *не съдържа повече от* $t + s$ *еквивалентни помежду си стълба.*

С други думи, всеки Грийсмъров код с $(s-1)q^{k-1} \leq d \leq sq^{k-1}$ може да се конструира чрез изтриване на подходящи координати от код, представляващ s копия на симплексния код на размерност k и при $d \leq q^{k-1}$ Грийсмъровите кодове нямат пропорционални координати (наричат се проективни кодове).

Тези твърдения поставят следните естествени въпроси.

Има ли Грийсмърови кодове с d по-малко от D?

С какви параметри са останалите, *негрийсмърови*, оптимални кодове за дадено k и d?

Отговорите на тези въпроси отварят нови или дават друго развитие на вече известни изследователски направления. Такива са изследванията върху възможните теглови разпределения на линейните кодове [18],[19]. Класификацията (или намирането на точно един представител от клас на еквивалентност) на кодове с фиксирани параметри води до характеризация на структурите и в частност до доказване на несъществуване на кодове с дадени параметри. Геометричната интерпретация на кодовете над крайни полета се оказа много уместна и резултатна. Благодарение на тази интерпретация стана възможно използване на методи за редуциране на параметрите на кодове, като например, базиран на проективно дуалната трансформация.

Ще се спрем по-подробно на един пример, който се отнася до доказване на съществуване и класификация на оптималните $[162, 8, 80; 2]$ кодове и се основава на този метод, поради няколко причини. Една от причините е, че това е последното конструктивно уточнение на $n_2(8, d)$ (за останалите няколко отворени случая впоследствие беше доказано несъществуване), а Додунеков и неговите ученици имат основни заслуги при намирането на точните стойности на $n_2(8, d)$. Друга причина е, че този пример провокира интереса на Додунеков към теоретично обобщение на проективно дуалната трансформация. Такова обобщение беше развито заедно със Симонис в класическата статия [20]. В тази разработка се дава нов аналитичен поглед на връзката между линейни кодове и мултимножества от точки в проективни геометрии. Представя се добре известната още от Делсарт (преразгледана в друга светлина от Брауер) трансформация като частен случай на много по-общо изображение, позволяващо линейност, лифтинг и др.

Брауер и Ван Ойпън [11] установяват следното съответствие между двойнотегловни и проективни кодове.

Нека C е $[n, k, d; q]$ код с пораждаща матрица G и нека $\gamma^j = (\gamma_1^j, \gamma_2^j, \ldots, \gamma_k^j)$ са представители на точките от $PG(k-1, q)$ за $j = 1, 2, \ldots, (q^k - 1)/(q-1)$.

Нека кодът C да има ненулеви тегла $w_1, w_2, \ldots, w_t$. Всеки подкод B на C с размерност $k-1$ има ненулеви тегла $w_1, w_2, \ldots, w_t$ с кратности съответно $f_1, f_2, \ldots, f_t$.

Да изберем α и β такива, че всички числа $\alpha w_i + \beta$ да са цели и неотрицателни. Нека матрицата G_X да съдържа всяко γ^j като стълб $\alpha w_j + \beta$ пъти, където $w_j = wt(\gamma^j.G)$ за $j = 1, 2, \ldots, (q^k - 1)/(q-1)$.

Броят на всички γ^j, включени в G_X, за които $\gamma^j.G \in B$, е

$$\sum(\alpha w_i + \beta) f_i)/(q-1) = \alpha n_B q^{k-2} + \beta(q^{k-1} - 1)/(q-1)q,$$

където n_B е ефективната дължина на кода. Да разгледаме кода X, породен от G_X. Лесно се проверява, че X е $[n', k', d'; q]$ код с параметри:

$$n' = \beta(q^k - 1)/(q-1) + \alpha q^{k-1} n, k' \leq k, d' = |X| - \beta\frac{q^{k-1} - 1}{q-1} - q^{k-2}.\max(\alpha n, \alpha(n-1)).$$

Аналогично съответствие е в сила за непроективни кодове, но тогава полученият код ще има повече от две тегла, защото n_B ще приема повече от две стойности.

Възможен е и обратният преход от X към C. При избор на подходящи α и β от X може да се конструира C.

В по-нататъшните разсъждения използваме Теорема 3 и представената по-долу Теорема 4, доказана в общия случай от Додунеков и отнасяща се до параметрите на остатъчния линеен код.

Дефиниция. *Остатъчен код на кода C относно кодовата дума $x \in C$ ще наричаме кода, който се получава от рестрикцията на C върху стълбовете, в които x има нули. Остатъчният код на кода C относно кодовата дума $x \in C$ ще означаваме с $Res(C, x)$.*

Ако не се интересуваме от вектора x, относно който образуваме остатъчния код, а само от неговото тегло $w = wt(x)$, ще записваме $Res(C, w)$.

Теорема 4 ([1]). *Нека C е $[n, k, d; q]$ код, $x \in C$, $wt(x) = w$ и $w < d + \lceil w/q \rceil$. Тогава $Res(C; w)$ има параметри $[n - w, k - 1, d_\mu]$, където $d_\mu \geq d - w + \lceil w/q \rceil$.*

Известно е от [17], че $n_2(8, 78) = 159$ или 160; $n_2(8, 80) = 162$ или 163. Ще разгледаме остатъчния код $Res(162, 112)$, който е $[50, 7, 24; 2]$ код.

Теорема 5. *Съществува единствен с точност до еквивалентност $[50, 7, 24; 2]$ код.*

Доказателство. Използвайки Теорема 4 и резултатите за оптимални двоични линейни кодове, се установява, че [50,7,24;2] код може да има кодови думи с ненулеви тегла 24, 32, 46, 48, 50.

Нека x е кодова дума с тегло 24 и $y \in C$. Ако $wt(y) = 50$, то $wt(x + y) = 26$ – противоречие. Ако $wt(y) = 48$, то $wt(x + y) = 24, 26$ или 28. Поради това, че в кода няма кодова дума с тегло 26 и 28, то $wt(x + y) = 24$ и $wt(v + y) = 24$ за всички вектори $v \in C$ с тегла 24. Това е невъзможно, защото от теорема 3 имаме, че кодът $[50, 7, 24; 2]$ се генерира от пораждаща матрица с редове с тегло 24. Тогава за някой вектор c от пораждащата матрица ще е изпълнено $c + y \neq 48$, защото в противен случай ще има две позиции, в които всички кодови думи ще имат нули.

Нека $wt(y) = 46$. Да допуснем, че $y = (11 \ldots 10000)$. Знаейки, че в C няма кодови думи с тегла 22, 26, 28 и 30, то $wt(x + y) = 24$ за всички $x \in C$ с тегло 24. За векторите $u = (u_1, 1000)$ и $v = (v_1, 0100)$ от C с тегла 24 имаме $wt(u + v + y) = 46 - wt(u_1 + v_1) + 2 = 50 - wt(u + v) = 4, 12$ или 26, което е невъзможно.

Тогава от уравненията на МакУйлямс лесно се получава, че за $[50, 7, 24; 2]$ кодовете има единствена възможност за теглови спектър: $A_0 = 1$, $A_{24} = 108$, $A_{32} = 19$, $B_2 = 1$.

В [16] е показано, че съществува единствен [19,7,8;2] код с теглови спектър $A_0 = 1$, $A_8 = 78$, $A_{12} = 48$ и $A_{16} = 1$. От този $[19, 7, 8; 2]$ код, използвайки съответствието между проективни и двойнотегловни кодове за $\alpha = 1/4$ и $\beta = -2$, се получава $[50, 7, 24; 2]$ код. Обратният преход от $[50, 7, 24; 2]$ код към $[19, 7, 8; 2]$ код имаме при $\alpha = 1/8$ и $\beta = -3$. От това, че кодът с параметри [19,7,8;2] е единствен, а $[50, 7, 24; 2]$ има единствен теглови спектър и съответствието е взаимно еднозначно, следва, че двойнотегловният непроективен $[50, 7, 24; 2]$ код е също единствен. □

Сега ще докажем, че има две възможности за тегловия спектър на кодовете с параметри $[162, 8, 80; 2]$:

(*i*) $A_0 = 1$, $A_{80} = 234$, $A_{96} = 21$, (*ii*) $A_0 = 1$, $A_{80} = 235$, $A_{96} = 19$, $A_{112} = 1$.

Използвайки Теорема 4 и резултатите за оптимални двоични линейни кодове, установяваме, че в $[162, 8, 80; 2]$ код C може да има кодови думи с ненулеви тегла 80, 96, 98, 100, 112, 160, 162. Ако има кодова дума с тегло 162, тогава би трябвало също да има кодова дума с тегло 82. Ако има кодова дума с тегло 160, тогава би трябвало да има кодова дума с тегло 82, защото векторите с тегла 80 генерират кода. Следва, че $A_{160} = A_{162} = 0$. С използване на уравненията на МакУйлямс се елиминира и възможността да има кодови думи с тегло 98 и 100. Следователно в кода C може да има само кодови думи с тегла 80, 96, 112.

Сега ще докажем, че $A_{112} \leq 1$. Нека v_1 и v_2 са различни кодови думи с тегло 112 и нека $v_2 = (v_2', v_2'')$, където $v_2'' \in Res(C, v_1)$. Според Теорема 4 теглата на v_2'' са 24 или 32 и оттук получаваме, че теглата на $v_1 + v_2$ са 64 или 48, което е невъзможно. Ако $A_{112} = 0$, тегловият спектър на C е $A_0 = 1$, $A_{80} = 234$, $A_{96} = 21$ и ако $A_{112} = 1$, тегловият спектър е $A_0 = 1$, $A_{80} = 235$, $A_{96} = 19$, $A_{112} = 1$.

Теорема 6. *Съществуват* $[162, 8, 80; 2]$ *кодове с теглови спектър* (i) *и* (ii) *и те са единствени с точност до еквивалентност.*

Доказателство. В [27] Джафе характеризира всички [21,8,8;2] кодове и доказва единствеността на [21,8,8;2] кодовете със спектри

1) $A_0 = 1$, $A_8 = 102$, $A_{12} = 144$, $A_{16} = 9$; 2)$A_0 = 1$, $A_8 = 106$, $A_{12} = 136$, $A_{16} = 13$.

По метода, описан в [11], на [162,8,80;2] кодовете с теглови спектър от вида (i) и (ii) за $\alpha = 1/16$ и $\beta = -5$ съответстват [21,8,8;2] кодовете с теглови спектър 1) и 2) съответно. Обратният преход се получава при $\alpha = 1/4$ и $\beta = -2$. От единствеността на [21,8,8;2] кодовете с теглови спектър 1) и 2) следва единствеността на [162,8,80;2] кодовете със спектри (i) и (ii). Поради това, че в дуалните кодове на кодовете, конструирани в горното доказателство, има вектори с тегло 3, следва, че съществува $[159, 8, 78; 2]$ код и оттам $n_2(8, 78) = 159$. $\square$

2. Двоични и троични квази-съвършени кодове с малки размерности. Когато се интересуваме от възможността на един шумозащитен код да коригира определен брой грешки, са важни следните понятия.

Дефиниция. *Радиус на покритие* $R = R(C)$ *на код* C *се нарича максималното измежду разстоянията на вектор от пространството* F_q^n *до кода* C, *т.е.* $R(C) = \max\{d(x, C) \mid x \in F_q^n\}$.

Ще означаваме с $[n, k, d; q]R$ линеен $[n, k, d; q]$ код с радиус на покритие R.

Дефиниция. *Радиус на сферичната опаковка* $e(C) = \left\lfloor \dfrac{d-1}{2} \right\rfloor$.

Радиусът на сферичната опаковка ни дава теглото на най-тежкия еднозначно коригируем вектор-грешка, докато радиусът на покритие на кода е мярката за максималното тегло на коригируем (еднозначно или не) вектор-грешка.

Оптимални по отношение на максималния брой коригирани грешки са *съвършените кодове*, за които $R(C) = e(C)$. Проблемът за намиране на всички съвършени кодове е поставен от Golay през 1949 и е напълно решен през 1973 от Зиновиев и Леонтиев [29] (и независимо от Tietäväinen [28]).

Следващата стъпка в тази посока е да се разглеждат квази-съвършени кодове, т.е. кодове, за които радиусът на сферичната опаковка и радиусът на покритие се различават с 1. Един съвсем естествен въпрос е: *Кои кодове са квази-съвършени?* Ясно е, че всеки код с радиус на покритие 1 и минимално разстояние 1 или 2 е

квази-съвършен. В тази работа ще представим резултати на Додунеков за кодове с радиус на покритие поне 2.

Квази-съвършените кодове с радиуси на покритие 2 и 3 са изследвани от различни автори. В частност, кодовете с параметри $[n, k, d; q]2$, $d = 3, 4$ са квази-съвършени. Тези кодове са свързани с *1-saturating* множества в проективните пространства $PG(n-k-1, q)$ и в литературата са описани много такива кодове. Направени са и изследвания на $[n, n-4, 5; q]3$ квази-съвършените кодове, които съответстват на пълни арки в проективното пространство $PG(3, q)$.

Значително по-малко е известно за q-ичните квази-съвършени кодове с $q > 2$. Една безкрайна фамилия от троични квази-съвършени кодове е известна от работата на Гашков и Сидельников [23]. Членове на фамилията са $[(3^s+1)/2, (3^s+1)/2 - 2s, 5; 3]3$ кодовете. Две фамилии от четвъртични кодове $[(4^s-1)/3, (4^s-1)/3-2s, 5; 4]3$ и $[(2^{2s+1}+1)/3, (2^{2s+1}+1)/3-2s-1, 5; 4]3$ са представени в [21] и [24], а Додунеков показва, че техните членове са квази-съвършени кодове [13, 1].

Тегловните разпределения и поведението при откриване на грешки на троичния $[13, 7, 5]$ квадратично-остатъчен код са изследвани в [6]. Показано е, че радиусът на покритие на кода е три, т.е. той е квази-съвършен. По-късно Додунеков и Данев [12] доказват, че този код е първият член на фамилия от троични квази-съвършени кодове с параметри $[(3^s-1)/2, (3^s-1)/2 - 2s, 5]$ за всички нечетни $s \geq 3$.

Представените до тук резултати водят до следния въпрос: *Колко рестриктивно е свойството на един код да е квази-съвършен, т.е. има ли неекивалентни квази-съвършени кодове със зададени параметри (тъй като всички посочени примери съдържат само по един код за съответните параметри)?*

За да се отговори на този въпрос, в [8] са класифицирани кодове със зададени параметри. Първо се фиксира размерността на кода и за тази размерност се определят възможните дължини и минимални разстояния на кодовете, които биха могли да са квази-съвършени, като се вземе предвид, че минималното разстояние на тези кодове може да има само две стойности: $2e+1$ или $2e+2$. По-конкретно, определят се параметрите, за които е възможно да съществуват двоични квази-съвършени кодове с размерности до 14 и троични квази-съвършени кодове с размерности до 13. След това се класифицират всички такива кодове, като се прилагат две основни техники. Първата се основава на съкращаване, а втората – на скъсяване на кодове. При съкращаване на кода изтриваме една или няколко негови позиции от всяка кодова дума. При скъсяване на кода фиксираме една негова позиция, избираме кодовите думи, които имат 0 в тази позиция, изтриваме тази позиция и получаваме скъсения $[n-1, k-1]$ код на $[n, k]$ кода.

За класификацията на част от кодовете, обект на това изследване, са използвани и вече известни класификации. Тъй като се разглеждат кодове с радиус на покритие, по-голям от 1, то минималното им разстояние трябва да е поне 3. Тогава дуалните им кодове трябва да са проективни кодове, т.е. такива, чието дуално минимално разстояние е поне 3. Двоичните проективни кодове с размерности до 6 са класифицирани от Илия Буюклиев в [10]. Те са използвани като основа за класифицирането на двоичните кодове с ко-размерности $n-k$ до 6, като измежду класифицираните в [10] проективни кодове се разглеждат само тези, които имат необходимото дуално разстояние. Например, за да класифицираме всички двоични $[8, 2, 5]$ кодове, се разглеждат 14-те $[8, 6]$ проективни кода. Само един от тях има дуално разстояние

5 и следователно има единствен $[8, 2, 5]$ код. По същия начин класификацията на троичните проективни кодове с размерности до 4 [7] е използвана, за да бъдат класифицирани троичните кодове с ко-размерности до 4, които биха могли да бъдат квази-съвършени.

След класифицирането на кодовете, които биха могли да са квази-съвършени, са пресметнати радиусите им на покритие. За целта последователно се разглеждат всички вектори с дължина n от вида $(\underbrace{0, \ldots, 0}_{k}, a)$, $a \in F_q^{n-k}$ за $q = 2$ или $q = 3$ и с тегло $\geq e$, тъй като всеки вектор с тегло по-малко или равно на e е единствен лидер на съседен клас. Пресмята се тяхното разстояние до кода. Ако се намери вектор, който е на разстояние от кода, по-голямо от $e+1$, търсенето се преустановява, защото радиусът на покритие на съответния код е поне $e + 2$, а ние търсим кодове с радиус на покритие $e + 1$.

С помощта на представения подход са класифицирани всички двоични и троични квази-съвършени кодове с размерности съответно до 9 и до 6. Получени са и частични резултати за двоичните квази-съвършени кодове с размерности до 14 и за троичните квази-съвършени кодове с размерности до 13.

В следващата теорема е показана конструкция на последователност от квази-съвършени кодове.

Теорема 7 ([8]). *Да приемем, че съществува $[n, k, d; q]2$ квази-съвършен код с $n \leq \dfrac{q^{n-k} - 1}{q - 1} - 2$ и $3 \leq d \leq 4$. Тогава съществува и $[n+1, k+1, 3; q]2$ квази-съвършен код.*

Като се приложи Теорема 7 към кодовете, получени в настоящата класификация, се получават следните вериги от параметри на квази-съвършени кодове.
$[5, 2, 3; 2]2 \to [6, 3, 3; 2]2$
$[8, 4, 4; 2]2 \to \cdots \to [14, 10, 3; 2]2$
$[9, 4, 4; 2]2 \to \cdots \to [30, 25, 3; 2]2$
$[13, 7, 4; 2]2 \to \cdots \to [\mathbf{18}, \mathbf{12}, \mathbf{3}; \mathbf{2}]\mathbf{2} \to [19, 13, 3; 2]2 \to [\mathbf{20}, \mathbf{14}, \mathbf{3}; \mathbf{2}]\mathbf{2} \to \ldots$
$\to [\mathbf{62}, \mathbf{56}, \mathbf{3}; \mathbf{2}]\mathbf{2}$
$[5, 2, 3; 3]2 \to [12, 3, 3; 3]2;$
$[8, 4, 4; 3]2 \to \cdots \to [17, 13, 3; 3]2 \to [\mathbf{18}, \mathbf{14}, \mathbf{3}; \mathbf{3}]\mathbf{2} \to \cdots \to [\mathbf{40}, \mathbf{36}, \mathbf{3}; \mathbf{3}]\mathbf{2}$
$[12, 7, 3; 3]2 \to [\mathbf{13}, \mathbf{8}, \mathbf{3}; \mathbf{3}]\mathbf{2} \to \cdots \to [\mathbf{121}, \mathbf{116}, \mathbf{3}; \mathbf{3}]\mathbf{2}$.

Кодовете, които не са били известни преди тази класификация, са дадени в получерен шрифт.

До тази работа, единствените известни примери на квази-съвършени кодове с минимално разстояние, по-голямо от 5, бяха двоичните кодове с повторение, $[22, 12, 6; 2]3$ съкратеният код на Golay, $[7, 1, 7; 3]4$ и $[8, 1, 8; 2]4$ кодовете с повторение. С намерените примери на още такива кодове се дава отговор на отворения проблем, поставен в статията на Etzion и Mounits [22], където се предлага да се намерят нови или да се докаже несъществуването на квази-съвършени кодове с $d > 5$. Най-интересни са $[24, 12, 7; 2]4$ и $[25, 12, 8; 2]4$, които са първите примери на квази-съвършени кодове с $R = 4$ извън споменатите по-горе.

Получените в това изследване резултати показват, че има само по няколко дължини, за които е възможно да съществуват квази-съвършени кодове за всяка размерност. За някои от параметрите са намерени стотици и хиляди квази-съвършени

кодове, което показва че това не е чак толкова рестриктивно свойство за кода. Намирането на квази-съвършени кодове с минимално разстояние, по-голямо от 5, ни дава основание да считаме, че за по-големи размерности ще съществуват квази-съвършени кодове с по-големи радиуси на покритие.

ЛИТЕРАТУРА

[1] С. М. Додунеков. Минимальная блоковая длина линейного q-ичного кода с заданными размерностью и кодовым расстоянием. *Проблемы передачи информации*, **20** (1984), No 4, 11–22.

[2] С. М. Додунеков. Оптимални линейни кодове. Дисертация за присъждане на научната степен „доктор на математичските науки“, София, 1985.

[3] С. М. Додунеков, Н. Л. Манев. Характеризация двух классов кодов, достигающих границ Грайсмера. *Проблемы передачи информации,* **19**, *4* (1983), 3–10.

[4] С. М. Додунеков, Н. Л. Манев. Уточнение границы Грайсмера для некоторых классов расстояний. *Проблемы передачи информации*, **23** (1987), No 1, 47–56.

[5] Ф. Дж. МакУилямс, Н. Дж. А. Слоен. Теория кодов исправляющих ошибки, Москва, Связь, 1979.

[6] T. Baicheva, S. Dodunekov, R. Kötter. On the Performance of the Ternary [13,7,5] Quadratic-Residue Codes. *IEEE Trans. Inform. Theory*, **48** (2002), No 2, 562–564.

[7] T. Baicheva, I. Boyukliev. On the ternary projective codes with dimensions 4 and 5. Proc of the International Workshop on Algebraic and Combinatorial Coding Theory, Kranevo, Bulgaria, 2004, 34–39.

[8] T. Baicheva, I. Bouyukliev, S. Dodunekov, V. Fack. Binary and Ternary Quasi-perfect Codes with Small Dimensions. *IEEE Trans. Inform. Theory*, **54** (2008), No 9, 4335–4339.

[9] I. Bouyukliev. What is Q-extension? *Serdica J. Computing*, **1** (2007), No 2, 115–130.

[10] I. Bouyukliev. On the binary projective codes with dimension 6. *Discrete Applied Mathematics*, **154** (2006) 1693–1708.

[11] A. E. Brouwer, M. van Eupen. The corespondence between projective codes and 2-weight codes. *Designs, Codes and Cryptography*, **11** (1997), No 3, 261–266.

[12] D. Danev, S. Dodunekov. A family of ternary quasi-perfect codes. Proc. International workshop on coding and cryptograph, Versailles, France, 2007.

[13] S. M. Dodunekov. The optimal double-error correcting codes of Zetterberg and Dumer-Zinov'ev are quasiperfect. *C. R. Acad. Bulgare Sci*, **38** (1985), No 9, 1121–1123.

[14] S. M. Dodunekov. Some quasiperfect double error correcting codes, *Problems Control Inform. Theory/Problemy Upravlen. Teor. Inform.*, **15** (1986), No 5, 367–375.

[15] S. M. Dodunekov. A remark on the weight structure of generating matrices of linear codes. *Problems Inform. Transmission*, **26** (1990), No 2, 173–176.

[16] S. M. Dodunekov, S. B. Encheva. On the uniqueness of some linear subcodes of the binary extended Golay code. Proc. of the Int. Workshop Algebraic and Combinatorial Coding Theory, Varna, Bulgaria, 1988, 38–40.

[17] S. M. Dodunekov , T. Helleseth, N. L. Manev, Ø. Ytrehus. New bounds on binary linear codes of dimension eight. *IEEE Trans. Inform. Theory*, **33** (1987), No 6, 917–919.

[18] S. M. Dodunekov, N. L. Manev. An improvement of the Griesmer bound for some small minimum distances. *Discrete Appl. Math.*, **12** (1985), No 2, 103–114.

[19] S. M. Dodunekov, N. L. Manev. An improvement of the Griesmer bound for some classes of distances. IEEE Conf. on Inf. Theory, Brightion, 1985.

[20] S. Dodunekov, J. Simonis. Codes and projective multisets. *Electron. J. Combin.*, **5** (1998), No 1, Research Paper 37, 23 pp.
[21] I. I. Dumer, V. A. Zinov'ev. Some new maximal codes over $GF(4)$, *Problems of Information Transmission*, **14** (1978), No 3, 174–181.
[22] T. Etzion, B. Mounits. Quasi-perfect codes with small distance. *IEEE Trans. Inf. Theory*, **51** (2005), No 11, 3938–3946.
[23] I. B. Gashkov, V. M. Sidel'nikov. Linear ternary quasiperfect codes correcting double errors. *Problems of Information Transmission*, **22** (1986), No 4, 284–288.
[24] D. N. Gevorkijan, A. M. Avetisjan, G. A. Tigranjan. On the construction of codes correcting two errors in Hamming's metric over Galois field. *Vichislitel'naja tehnika*, **3** (1975) 19–21 (in Russian).
[25] J. H. Griesmer. A bound for error-correcting codes. *IBM J Res. Develop.*, **4** (1960), 532-542.
[26] R. Hill. Optimal linear codes. In: Cryptography and Coding II (ed. C. Mitchell), Oxford, Oxford University Press, 1992, 75–104.
[27] D. Jaffe. Binary linear codes: new results on nonexistence. Manuscript, Department of mathematics and statistics, University of Nebraska.
[28] A. Tietäväinen. On the nonexistence of perfect codes over finite fields. *SIAM J. Appl. Math.*, **24** (1973), 88–96.
[29] V. A. Zinov'ev, V. K. Leont'ev. On non-existence of perfect codes over Galois fields. *Probl. Control Inf. Theory*, 2 (1973), 16–24; translation from *Probl. Upravl. Teor. Inform.* **2** (1973), No 2, 123–132.

Цонка Байчева
e-mail: tsonka@math.bas.bg
Петър Бойваленков
e-mail: peter@math.bas.bg
Илия Буюклиев
e-mail: iliyab@math.bas.bg
Институт по математика и информатика
Българска академия на науките
ул. „Акад. Г. Бончев“, блок 8
1113 София, България

STEFAN DODUNEKOV'S 75th BIRTHDAY

T. Baicheva, P. Boivalenkov, I. Bouyukliev

This year marks the 75th anniversary of Stefan Dodunekov's birth - a world-renowned scientist, founder of the Coding theory group in Bulgaria, of two international scientific conferences, former Director of the Institute of Mathematics and Informatics, Academician and President of the Bulgarian Academy of Sciences, but most of all a great teacher, friend and person. In this work we present some results on optimal error-correcting codes obtained by Stefan Dodunekov.