ШУМЕНСКИ УНИВЕРСИТЕТ
"ЕПИСКОП КОНСТАНТИН ПРЕСЛАВСКИ"
ФАКУЛТЕТ ПО МАТЕМАТИКА И ИНФОРМАТИКА
КАТЕДРА "АЛГЕБРА И ГЕОМЕТРИЯ"

ДАМЯН СТЕФАНОВ АНЕВ

ИЗСЛЕДВАНЕ И КЛАСИФИКАЦИЯ НА САМОДУАЛНИ КОДОВЕ: ГРУПА ОТ АВТОМОРФИЗМИ, ЧЕТИРИ ЦИРКУЛАНТНА КОНСТРУКЦИЯ, СЪСЕДИ

А В Т О Р Е Ф Е Р А Т

на дисертация
за придобиване на образователната и научна степен
"доктор"
в докторска програма Алгебра и теория на числата;
професионално направление 4.5. Математика;
област на висше образование
4. Природни науки, математика и информатика;

Научен ръководител
проф. д.м.н. Николай Иванов Янков

Шумен
2018

Дисертационният труд е обсъден и предложен за защита на разширено заседание на катедра „Алгебра и геометрия“ към Факултет по математика и информатика на Шуменски университет „Епископ Константин Преславски“, проведено на 25.09.2018 г.

Дисертационният труд се състои от увод, четири глави, авторска справка, списък на публикациите включени в дисертацията, апробация на резултатите и списък на използваната литература. Използваната литература съдържа 83 заглавия. Общият обем на дисертационния труд е 94 страници.

Номерациите на определенията, теоремите и формулите, както и цитиранията в авторефератa съвпадат със съответните номерации на определения, теореми, формули и цитирания в дисертационния труд.

Публичната защита е насрочена на 14.12.2018 г. от 14 часа в Корпус 3, зала 214 (КЛ1) на Шуменски университет „Епископ Константин Преславски“ на открито заседание на научното жури.

Съдържание

Увод

Теорията на кодирането е динамична, бързо развиваща се математическа дисциплина, в която се прилагат идеи от алгебрата, комбинаториката, геометрията и дискретната математика. Тя води началото си от 1948 г., с издаването на статията на Claude Shannon „A mathematical theory of communication"[30], в която е представен модел на комуникационна система и се разглежда въпросът, свързан с измерване на капацитета на комуникационния канал. В същото изследване е въведена и единица за измерване на информацията *бит*. Самият автор е известен като „баща на теорията на информацията".

Основна част от тази теория са кодовете за коригиране на грешки. Истинските им корени, обаче, са още по-ранни - в комуникационните системи като телеграфа и телефона. Необходимостта от появата на такива кодове е продиктувана от възможностите им за откриване и коригиране на грешки. Кодовете също така се изучват от редица научни дисциплини - теория на информацията, електроинжинерство, лингвистика, математика и компютърни науки, като основната им цел е разработването на ефективни начини за сигурно предаване на данни.

Сред всички видове кодове най-изучавани са линейните кодове. Поради тяхната алгебрична структура, те са по-лесни за описване, кодиране и декодиране. Един клас кодове за коригиране на грешки, са линейните самодуални кодове, каквито най-често ще разглеждаме в настоящата дисертация. Самодуалните кодове представляват особено интересен клас кодове, поради факта, че теореми като тези, описващи разпределението на теглото, произтичат от строго дефинираната им структура. Тези кодове имат интересни връзки към групи и t-дизайни. Нещо повече, много самодуални кодове често се оказват „най-добри" или „оптимални" сред линейните кодове със същите параметри.

Нека $\mathbb{F}_q$ е крайно поле с q елемента, където q е степен на просто число. Всяко k-мерно подпространство $\mathcal{C}$ на n-мерното

линейното пространство $\mathbb{F}_q^n$ наричаме *линеен код* с дължина n и размерност k над $\mathbb{F}_q$. Елементите на кода C се наричат *кодови думи*.

Разстояние (по Hamming) между два вектора $x = (x_1, x_2, ..., x_n)$ и $y = (y_1, y_2, ..., y_n)$ от векторното пространство $\mathbb{F}_q^n$ наричаме броя на координатите, в които x и y се различават и означаваме с $d(x, y)$. *Минимално разстояние* $d(C)$ на кода C наричаме най-малкото разстояние между две различни кодови думи. *Тегло* $\mathrm{wt}(x)$ на вектора $x \in \mathbb{F}_q^n$ е броят на ненулевите координати на x. *Минимално тегло* d на C е най-малкото ненулево тегло на всяка кодова дума на C. За всеки линеен код е изпълнено, че минималното му разстояние съвпада с минималното тегло на ненулевите вектори.

$$\min\{d(x, y) \mid x, y \in C,\ x \neq y\} = \min\{\mathrm{wt}(x - y) \mid x, y \in C,\ x \neq y\}$$

Носител на вектора $x = (x_1, x_2, ..., x_n)$ от $\mathbb{F}_q^n$ наричаме множеството $\mathrm{supp}(x) = \{i \mid x_i \neq 0\}$ от координатни позиции, в които x има ненулева координата. Броят на елементите в $\mathrm{supp}(x)$ съвпада с теглото на вектора x.

Линеен код с дължина n, размерност k и минимално разстояние d, наричаме $[n, k, d]$ код над $\mathbb{F}_q$.

Всяка матрица G с k реда и n стълба с елементи от полето $\mathbb{F}_q$, чиито редове формират базис на C се нарича *пораждаща матрица* на този код.

За всеки два вектора $x = (x_1, \ldots, x_n)$ и $y = (y_1, \ldots, y_n)$ от $\mathbb{F}_q^n$, равенството $(x, y) = \sum_{i=1}^{n} x_i y_i$ задава стандартното *скаларно произведение* в $\mathbb{F}_q^n$. Ако $(x, y) = 0$ казваме, че векторите x и y са ортогонални. Ортогоналното допълнение на кода C

$$C^{\perp} = \{y \in \mathbb{F}_q^n \mid (x, y) = 0, \forall\, x \in C\}$$

наричаме *дуален код* на кода C. Ако $C \subseteq C^{\perp}$, линейният $[n, k, d]$ код C се нарича *самоортогонален код*, а ако $C = C^{\perp}$, C е *самодуален код*. Всеки самодуален код с дължина n над $\mathbb{F}_q$ има

размерност $k = \frac{n}{2}$, следователно самодуални кодове над дадено поле съществуват само за четни дължини.

Линеен код C, в който всички кодови думи имат четни тегла, наричаме *четнотегловен*. Ако всички кодови думи имат тегла кратни на 4, то C се нарича *двойночетен*. Над $\mathbb{F}_2$ и $\mathbb{F}_4$, всеки самодуален код е четнотегловен код. Двоичните самодуални кодове, които не са двойночетни, наричаме *едночетни*. Едночетните самодуални кодове са четнотегловни, но съдържат и ненулеви кодови думи $x \in C$, с тегла $\mathrm{wt}(x) \equiv 2 \pmod 4$. Двоичен двойночетен самодуален $[n, n/2]$ код съществува, тогава и само тогава, когато n се дели на 8.

Два линейни $[n, k, d]$ кода над $\mathbb{F}_q$ наричаме *еквивалентни*, ако единия може да се получи от другия, чрез композиция от следните трансформации:

1) пермутация на координати;

2) умножение на елементите във фиксирана координатна позиция с ненулев скалар;

3) прилагане на автоморфизъм на полето $\mathbb{F}_q$ към елементите във всички координатни позиции.

Понеже еквивалентните кодове имат едни и същи параметри $[n, k, d]$ и еднакви тегловни функции, те предлагат еднакви възможности за откриване и поправяне на грешки.

Под *тегловно разпределение* или *спектър* на линеен код C с дължина n разбираме наредената $n+1$ - орка $(A_0, A_1, ..., A_n)$, където цялото неотрицателно число A_i за $i = 0, 1, ..., n$ е броят на кодовите думи с тегло i в кода C. Полиномът $W(x, y) = \sum_{i=0}^{n} A_i x^{n-i} y^i$ наричаме *тегловна функция* на кода C.

Основна граница, на която отговаря минималното тегло на двоичните самодуални кодове е тази на Rains [29]. Нека C е двоичен самодуален $[n, n/2, d]$ код. Тогава

$$d \leq 4 \left\lfloor \frac{n}{24} \right\rfloor + 4, \quad n \not\equiv 22 \pmod{24},$$

$$d \leq 4 \left\lfloor \frac{n}{24} \right\rfloor + 6, \quad n \equiv 22 \pmod{24}.$$

Самодуален код, изпълняващ горната граница с равенство се нарича *екстремален*. Един самодуален код се нарича *оптимален*, ако не е екстремален, но има най-голямо минимално разстояние за дадената дължина.

Изучаването и класификацията на двоичните самодуалните кодове започва през 1972 г. със статията на Vera Pless „A classification of self-orthogonal codes over $GF(2)$" [28], където са класифицирани всички кодове с дължина $n \leq 20$. По-късно Pless, Conway и Sloane класифицират самодуалните кодове с дължина $n \leq 30$ [11]. Класификацията на кодове с дължина 32 е завършена от Bilous и Van Rees [5], а на кодове с дължина 34 от Bilous [4]. В [1] Melchor и Gaborit систематизират всички оптимални самодуални кодове с дължина 36, а Harada и Munemasa завършват класификацията на всички кодове за същата дължина [21].

Последните постижения на пълна класификация в това направление са за дължина 38 на Буюклиева и Буюклиев в [8] и за дължина 40 на Буюклиев, Джумалиева-Стоева и Монев [7]. При по-големи дължини нараства експоненциално броят на всички двоични самодуални кодове и дори класифицирането само на оптималните самодуални кодове е твърде сложно. Затова ефективен начин за намирането на нови оптимални кодове е въвеждането на ограничения, свързани с техните групи от автоморфизми.

Други методи за конструиране на самодуални кодове са четири циркулантни конструкции и съседи. Често се намират нови кодове и чрез скъсяване и разширяване на вече известни самодуални кодове. В настоящата дисертация използваме следните методи:

1. Huffman-Йоргов за конструиране на двоични самодуални кодове с автоморфизъм от нечетен прост ред в § 2 и § 3;

2. Четири циркулантна конструкция и разглеждане на са-

модуални съседи в § 4;

3. Разширяване на дължината на вече известни самодуални кодове в § 4;

4. Конструиране на нови двоични самодуални кодове чрез скъсяване на дължината им с 2 в § 2.

В [12] Conway и Sloane намират възможните тегловните функции на екстремални или оптимални двоични самодуални кодове с дължини до 72. По-късно Dougherty, Gulliver и Harada в [16] извеждат тегловните функции на кодове с дължини $72 \leq n \leq 100$, като в някои от случаите функциите зависят от един или два параметъра. Така за изследователите на самодуални кодове, една от основните цели е конструирането на кодове с тегловна функция, за която се предполага, че е възможна, но не е известно съществуването на такъв код.

Най-голямата дължина, за която са конструирани кодове за всички възможни стойности на параметрите в тегловната функция на оптимален едночетен двоичен самодуален код, е 52 [37]. В работата си [38] от 2015 г. Янков и Lee класифицират всички оптимални двоични самодуални кодове с автоморфизъм от нечетен прост ред с дължини до 50.

В този дисертационен труд при изследването на двоични самодуални кодове са приложени алгебрични и комбинаторни методи. При работа с голям брой кодове, изчисленията са извършени с помощта на компютърна техника. Използвани са системите за компютърна алгебра Magma; **GAP** и допълнителния пакет за кодове към него GUAVA; софтуерния пакет **Q-extension** на Буюклиев [6], както и собствени програми.

Обзор на дисертацията

Дисертацията се състои от увод и 4 глави. Накратко изследванията са организирани по следния начин:

Глава 1. Основни понятия и предварителни резултати

В първа глава са представени основни понятия и предварителни резултати, използвани в дисертационния труд. В § 1.3 е направен преглед на известните до момента тегловни функции и параметрите им на оптималните двоични самодуални кодове с дължини $58 \leq n \leq 64$ и $78 \leq n \leq 84$ или на кодове, които не са оптимални, но имат най-голямото минимално тегло за съответната дължина, което е известно към момента. Разгледани са известните тегловни функции на екстремалните едночетни самодуални кодове с дължини 64 и 66. Освен това е направен преглед и на намерените от нас нови стойности на параметрите.

В § 1.6 е описан метода на Huffman и Йоргов за конструиране на двоични самодуални кодове, притежаващи автоморфизъм от нечетен прост ред.

Нека C е двоичен самодуален код с дължина n с автоморфизъм σ от нечетен прост ред p с точно c независими p-цикъла и $f = n - pc$ неподвижни точки в разлагането му. Приемаме, че

$$\sigma = (1, 2, \ldots, p)(p+1, p+2, \ldots, 2p) \ldots (p(c-1)+1, \ldots, pc)$$

и казваме, че σ е от *тип* $p-(c,f)$.

Обозначаваме циклите на σ чрез $\Omega_1, \ldots, \Omega_c$ и неподвижните точки чрез $\Omega_{c+1}, \ldots, \Omega_{c+f}$. Нека

$$F_\sigma(C) = \{v \in C \mid v\sigma = v\},$$

$$E_\sigma(C) = \{v \in C \mid wt(v|\Omega_i) \equiv 0 \pmod 2, i = 1, \ldots, c+f\},$$

където $v|\Omega_i$ е ограничението на v върху цикъла Ω_i.

Теорема 1.6.1. (Huffman, [23]). *Нека C е самодуален код. Тогава кодът C е директна сума на подкодовете $F_\sigma(C)$ и $E_\sigma(C)$. Подкодовете $F_\sigma(C)$ и $E_\sigma(C)$ са подпространства с размерности съответно* $\dfrac{c+f}{2}$ *и* $\dfrac{c(p-1)}{2}$.

Имаме $v \in F_\sigma(C)$ тогава и само тогава, когато $v \in C$ и векторът v има еднакви координати във всеки цикъл. Нека $\pi : F_\sigma(C) \to \mathbb{F}_2^{c+f}$ е проективното изображение при което, ако $v \in F_\sigma(C)$, $(v\pi)_i = v_j$ за някое $j \in \Omega_i, i = 1, 2, \ldots, c+f$.

Отбелязваме с $E_\sigma(C)^*$ кодът $E_\sigma(C)$, от който са премахнати последните f координати. Така $E_\sigma(C)^*$ е самоортогонален двоичен код с дължина pc. Всеки вектор v от $E_\sigma(C)^*$ под действието на σ се разбива на c на брой вектора с дължина p. Тогава на всеки цикъл $v|\Omega_i = (v_0, v_1, \ldots, v_{p-1})$ от $E_\sigma(C)^*$ съпоставяме полиномът $v_0 + v_1 x + \cdots + v_{p-1}x^{p-1}$ от $\mathcal{P}$, където $\mathcal{P}$ е множеството от четнотегловни полиноми над факторпръстена $\mathbb{F}_2[x]/\langle x^p - 1\rangle$. Така получаваме изображението $\varphi : E_\sigma(C)^* \to \mathcal{P}^c$, където $\mathcal{P}$ е цикличен код с дължина p с пораждащ полином $x - 1$. Известно е, че $\varphi(E_\sigma(C)^*)$ е подмодул на $\mathcal{P}$-модула $\mathcal{P}^c$ [23], [40].

Прилагайки Теорема 1.6.1 можем да констуираме пораждаща матрица на кода C във вида

$$\operatorname{gen} C = \begin{pmatrix} \operatorname{gen} F_\sigma(C) & \\ \operatorname{gen} E_\sigma(C)^* & O \end{pmatrix},$$

където O е нулева матрица от тип $\dfrac{c(p-1)}{2} \times f$.

Така изборът на подкодове $F_\sigma(C)$ и $E_\sigma(C)$ определя целия код C. Следователно за дадена дължина могат да бъдат получени всички самодуални кодове с автоморфизъм σ.

Необходими и достатъчни условия за един двоичен код с автоморфизъм от тип $p - (c, f)$ да е самодуален дава следната теорема.

Теорема 1.6.2. (Йоргов, [40]). *Двоичен $[n, n/2]$ код C с ав-*

томорфизъм σ е самодуален тогава и само тогава, когато са в сила следните условия:

(i) $C_\pi = \pi(F_\sigma(C))$ *е двоичен самодуален код с дължина* $c+f$,

(ii) за всеки два вектора u, v *от* $C_\varphi = \varphi(E_\sigma(C)^*)$ *имаме*

$$u_1(x)v_1(x^{-1}) + \cdots + u_c(x)v_c(x^{-1}) = 0. \tag{1.11}$$

В случая, когато 2 е примитивен корен по модул p, $\mathcal{P}$ е поле с 2^{p-1} елемента. В този слечай е валидна следната теорема.

Теорема 1.6.3. (Йоргов, [40]). *Нека* 2 *е примитивен корен по модул* p. *Тогава двоичния код* C *с автоморфизъм* σ *е самодуален тогава и само тогава, когато са изпълнени следните две условия:*

(i) C_π *е двоичен самодуален код с дължина* $c+f$;

(ii) C_φ *е ермитово самодуален код с дължина* c *над полето* $\mathcal{P}$ *относно ермитовото скаларното произведение*

$$(u, v) = \sum_{i=1}^{c} u_i v_i^{2^{\frac{p-1}{2}}}.$$

За да класифицираме кодовете, които получаваме, се нуждаем от допълнителни условия за еквивалентност, дадени от следната теорема:

Теорема 1.6.4. (Йоргов, [41]). *Следните трансформации запазват разлагането на* C *и го изпращат в еквивалентен код:*

(i) пермутация на фиксираните координати;

(ii) пермутация на p*-цикличните координати;*

(iii) субституция $x \to x^2$ *в* C_φ;

(iv) умножение на j-тата координата на C_φ с x^{t_j} където t_j е цяло число, $0 \leq t_j \leq p-1$, $j = 1, 2, \ldots, c$.

Лема 1.6.5. (Йоргов, [40]). *Нека $M_j = \{u \in \varphi(E_\sigma(C)^*) | u_i \in I_j, i = 1, 2, \ldots, c\}$, $j = 1, 2, \ldots, s$. Тогава*

1) M_j е линейно пространство над полето I_j, $j = 1, 2, \ldots, s$;

2) $C_\varphi = \varphi(E_\sigma(C)^*) = M_1 \oplus M_2 \oplus \cdots \oplus M_s$ (директна сума на $\mathcal{P}$-подмодули);

3) Ако C е самодуален код, то $\sum_{j=1}^{s} \dim_{I_j} M_j = \frac{cs}{2}$.

В някои случаи, за да съществува оптимален самодуален код, има ограничения за броя на цикличните и фиксирани координати. Такива ограничения ни дава следната лема:

Лема 1.6.6. (Йоргов, [40]). *Нека σ е автоморфизъм на двоичен самодуален код C и този автоморфизъм има с цикъла и f фиксирани точни. Ако $g_2(k, d) = \sum_{i=0}^{k-1} \lceil \frac{d}{2^i} \rceil$, то:*

1) $pc \geq g_2(\frac{(p-1)c}{2}, d)$;

2) в случай че $f > c$, то $f \geq g_2(\frac{f-c}{2}, d)$.

Връзка между тегловните разпределения на двоичния самодуален код C и подкодовете $F_\sigma(C)$ и $E_\sigma(C)$ дава следната теорема:

Теорема 1.6.7. [14]. *Нека C е двоичен самодуален код с автоморфизъм σ. Ако A_i, B_i и D_i са съответно коефициентите в тегловните функции на C, $F_\sigma(C)$ и $E_\sigma(C)$, то:*

$$D_i \equiv 0 \pmod{p}, \quad A_i \equiv B_i \pmod{p}.$$

В § 1.7 разглеждаме четири циркулантна конструкция и самодуални съседи.

Определение 1.7.1. Циркулантна матрица от тип $n \times n$ има следният вид:

$$\begin{pmatrix} r_0 & r_1 & r_2 & \cdots & r_{n-1} \\ r_{n-1} & r_0 & r_1 & \cdots & r_{n-2} \\ \vdots & \vdots & \vdots & & \vdots \\ r_1 & r_2 & r_3 & \cdots & r_0 \end{pmatrix},$$

където всеки следващ ред е дясно циклично завъртане на предишния.

Нека A и B са $n \times n$ циркулантни матрици. Нека C е $[4n, 2n]$ код с пораждаща матрица от следният вид:

$$\begin{pmatrix} & & A & B \\ I_{2n} & & B^T & A^T \end{pmatrix}, \tag{1.13}$$

където с I_n е означена единичната квадратна матрица от тип $n \times n$, а с A^T транспонираната на A. Тогава C е самодуален код, ако

$$AA^T + BB^T = I_n.$$

Четири циркулантната конструкция е въведена в [3], впоследствие модифицирана в [27]. Въз основа на тази конструкция са получени много двоични кодове с добри параметри.

Определение 1.7.2. Кодовете с пораждащи матрици от вида (1.13) се наричат *четири циркулантни*.

Определение 1.7.3. Два самодуални кода C и C' с дължина n се наричат *съседи*, ако

$$\dim(C \cap C') = n/2 - 1.$$

Всеки самодуален код с дължина n може да бъде достигнат от всеки друг като се вземат последователни съседи (виж

[12]). Тъй като всеки самодуален код C с дължина n съдържа вектора с n единици $\mathbf{1}$, C има $2^{n/2-1}-1$ подкода D от коразмерност 1, съдържащи $\mathbf{1}$. Понеже $\dim(D^{\perp}/D) = 2$, има два самодуални кода, такива че C е между $D^{\perp}$ и D. Ако C е едночетен самодуален код с дължина, която се дели на 8, тогава C има два двойночетни самодуални съседа (виж [9]).

В [31] е представен метод за конструиране на едночетни самодуални кодове. Нека C е самодуален код с дължина n, а x е вектор с нечетно тегло. Означаваме с C^0 подкод на C, състоящ се от всички кодови думи, които са ортогонални на x. Тогава има съседни класове C^1, C^2, C^3 на C^0, такива че $C^{0^{\perp}} = C^0 \cup C^1 \cup C^2 \cup C^3$, където $C = C^0 \cup C^2$ и $x + C = C^1 \cup C^3$. Кодът

$$C(x) = (0, 0, C^0) \cup (1, 1, C^2) \cup (1, 0, C^1) \cup (0, 1, C^3)$$

е едночетен самодуален код с дължина $n+2$ [31].

Определение 1.7.4. *Радиус на покритие* на код C с дължина n и минимално разстояние d, наричаме най-малкото цяло число $R = R(C)$, такова че сферите с радиус R около кодовите думи на C покриват пространството $\mathbb{F}_q^n$.

Радиусът на покритие на линеен код е равен на теглото на най-тежкия лидер на съседен клас на кода.

Определение 1.7.5. Най-голямото цяло e, такова че кълбата с радиус e, описани около кодовите думи, не се пресичат, наричаме *радиус на сферичната опаковка.*

В сила е следната *граница на сферичната опаковка* за радиуса на покритие на код:

$$R \geq e = \left\lfloor \frac{d-1}{2} \right\rfloor .$$

Кълбата с радиус R покриват цялото пространство $\mathbb{F}_q^n$. Следователно за долна граница (*граница на сферичното пок-*

ритие) [32] имаме:

$$\sum_{i=0}^{R(C)} \binom{n}{i} (q-1)^i \geq q^{n-k}.$$

Горна граница за радиуса на покритие е получена в [13]:

$$R(C) \leq n - k.$$

Радиусът на покритие е основен и важен геометричен параметър на кода. В сила е следната граница за $R(C)$:

Теорема 1.7.6. (Граница на Delsarte, [13]). *Нека s' е общият брой на ненулевите тегла в $C^\perp$. Тогава*

$$R(C) \leq s'.$$

Глава 2. Самодуални кодове с автоморфизъм от пети ред

В настоящата глава разглеждаме структурата на оптималните двоични самодуални кодове $[n, n/2]$ с дължини $60 \leq n \leq 64$, притежаващи автоморфизъм от ред 5 с 12 независими цикъла и минимално тегло 12. Представяме пълна класификация на кодовете с дължини 60 и 62. Намираме някои нови $[64, 32, 12]$ и $[58, 29, 10]$ самодуални кодове. Кодовете с дължина 58 се получават чрез скъсяване на самодуалните $[60, 30, 12]$ кодове с автоморфизъм от тип 5-$(12, 0)$. Получаваме за първи път самодуален $[58, 29, 10]$ код с тегловна функция $W_{58,2}$ за $\beta = 0$, $\gamma = 132$. Използваме метода на Huffman и Йоргов за конструиране на двоични самодуални кодове, притежаващи автоморфизъм от нечетен прост ред, описан в § 1.6

Всички оптимални двоични самодуални кодове с дължини от 52 до 60 с автоморфизъм от ред 7 или 13 са класифицирани

в [39]. Наскоро, всички кодове с дължини $50 \leq n \leq 60$, притежаващи автоморфизъм от тип 5-$(10, f)$ за $f = 0, 2, 4, 6, 8$ и 10 са класифицирани с точност до еквивалентност в [33].

Според [25, Table 2] не са изследвани случаите за дължини $60 \leq n \leq 70$ и автоморфизъм от ред 5 с 12 цикъла.

Ще се съсредоточим върху оптималните самодуални кодове с дължини $60 \leq n \leq 64$ с автоморфизъм от ред 5 с 12 цикъла, които ще изследваме и ще класифицираме.

В § 2.1 разглеждаме структурата на подкода $E_\sigma(C)$.

Тъй като числото 2 е примитивен корен по модул 5, от Теорема 1.6.2, подкода C_φ е самодуален код с дължина c над полето $\mathcal{P}$ относно ермитовото скаларно произведение

$$(u, v) = \sum_{i=1}^{c} u_i v_i^4. \tag{2.1}$$

Освен това, $\mathcal{P}$ е крайно поле с 16 елемента, $\mathcal{P} \cong \mathbb{F}_{16} = \{0, e = \alpha^0, \alpha^k | k = 1, \ldots, 14\}$, където $e = x + x^2 + x^3 + x^4$, $\alpha = 1 + x$ е примитивен елемент на мултипликативен ред 15.Ако $\delta = \alpha^5$, то групата $\mathcal{P}^*$ може да се запише по следния начин: $\mathcal{P}^* = \{\alpha^{3t}\delta^l \mid 0 \leq t \leq 4, 0 \leq l \leq 2\}$.

Нека C е оптимален двоичен самодуален код с автоморфизъм от ред 5 с 12 цикъла и $f = 2t$, $t = 0, \ldots, 5$ фиксирани точки.

Твърдение 2.1.1. *Нека C_φ е ермитов самодуален код с дължина* 12 *над $\mathcal{P}$ относно ортогоналното условие (2.1), така че подкодът $E_\sigma(C)$ е код с минимално разстояние най-малко* 12. *Тогава пораждащата матрица на C_φ има вида*

$$\left(\begin{array}{c|cccccc} & t_{11} & t_{12} & t_{13} & t_{14} & t_{15} & t_{16} \\ & t_{21} & l_{22} & l_{23} & l_{24} & l_{25} & l_{26} \\ & t_{31} & l_{32} & l_{33} & l_{34} & l_{35} & l_{36} \\ eI_6 & t_{41} & l_{42} & l_{43} & l_{44} & l_{45} & l_{46} \\ & t_{51} & l_{52} & l_{53} & l_{54} & l_{55} & l_{56} \\ & t_{61} & l_{62} & l_{63} & l_{64} & l_{65} & l_{66} \end{array}\right), \tag{2.2}$$

където $t_{1j} \in \{0, e, \delta, \delta^2\}$ *за* $1 \leq j \leq 6$, $t_{j1} \in \{0, e, \delta, \delta^2\}$ *за* $1 \leq j \leq 6$ *и* $l_{ij} \in \mathcal{P}$. *Векторът* $(t_{11}, \ldots, t_{16})$ *е един от следните седем вектори:*
$(0, 0, e, e, \delta, \delta^2)$, $(0, e, \delta, \delta, \delta, \delta)$, $(0, e, \delta, \delta, \delta^2, \delta^2)$,$(0, e, e, e, e, e)$,
$(0, e, e, e, \delta, \delta)$, $(e, e, \delta, \delta, \delta, \delta^2)$, $(e, e, e, e, \delta, \delta^2)$.

Използвайки компютър за изчисляване на възможния втори ред на матрицата (2.2), получаваме 242 нееквивалентни кода.

След това, за всеки от тези 242 нееквивалентни кода, когато добавяме третия ред, проверяваме получените кодове за минимално разстояние и еквивалентност. Съществуват точно 35191 нееквивалентни кода с 3 реда. За всеки един от тези кодове добавяме четвърти ред и отново проверяваме получените кодове за минимално разстояние и еквивалентност. Така се оказва, че има точно 681862 нееквивалентни такива кодове.

След това добавяме пети и шести ред на матрицата и проверяваме получените кодове за еквивалентност и за минимално разстояние най-малко 12. Окончателно получаваме следния резултат.

Твърдение 2.1.2. *С точност до еквивалентност съществуват* 60467 *кода* C_φ *над* $\mathcal{P}$, *такива че кодът* $\varphi^{-1}(C_\varphi)$ *има минимално разстояние* 12.

В § 2.2 представяме пълна класификация на кодовете с дължина 60 и с автоморфизъм от тип 5-$(12, 0)$. Има две възможни тегловни функции за двоичен самодуален $[60, 30, 12]$ код. Известни са кодове и с двете тегловни функции (вж. § 1.3).

Нека C е двоичен самодуален $[60, 30, 12]$ код с автоморфизъм от тип $5 - (12, 0)$. Според Теорема 1.6.2, C_π е двоичен самодуален $[12, 6]$ код. Има точно три такива кода $6i_2$, $2i_2 + h_8$ и d_{12} (вж. [24]). Тъй като всеки вектор с тегло 2 в C_π ще доведе до вектор с тегло 10 в $F_\sigma(C)$, търсим $[12, 6, 4]$ код и единственият възможен такъв код е d_{12}. Нека да означим G_1 пораждаща матрица на този код. Конструираме всички кодове $C = G_1^\tau \oplus H_i$

за $1 \leq i \leq 60467$, $\tau \in T_1$ - дясна трансверзала на S_{12} породена от S_1 - групата от автоморфизми на кода, а след това ги изследваме за минимално тегло и за еквивалентност. Представяме следния резултат.

Теорема 2.2.1. *С точност до еквивалентност съществуват* 236 *оптимални двоични самодуални* $[60, 30, 12]$ *кодове с автоморфизъм от тип* 5-$(12, 0)$.

Забележка 2.2.2. Всички кодове, които получаваме, имат тегловна функция $W_{60,2}$. Сред кодовете, конструирани от нас, има 13 кода, еквивалентни на кодовете с автоморфизъм от ред 15, конструирани от Дончева и Harada в [14].

В § 2.3 правим пълна класификация на кодовете с дължина 62 и с автоморфизъм от тип 5-$(12, 2)$. За самодуалния $[62, 31, 12]$ код има две възможни тегловни функции. Съществуват кодове и с двете функции (вж. § 1.3).

Според Теорема 1.6.2, кодът C_π е двоичен самодуален и има параметри $[14, 7]$. Съществуват точно четири такива кода [24]: $7i_2$, $3i_2 \oplus e_8$, $i_2 \oplus d_{12}$ и $2e_7$. Ако имаме кодова дума с тегло 2 в C_π, то тогава минималното разстояние на C е $d \leq 10$. Следователно, само $[14, 7, 4]$ код може да породи C_π, което води до $C_\pi \cong 2e_7$. Избирайки всички $\binom{14}{2}$ разделяния на координатите $\{1, \ldots, 14\}$ в непресичащи се множества X_c на циклични и X_f – фиксирани координати, намираме два различни кода C_π, породени от $G_2 = (I_7|Z_2)$ и $G_3 = (I_7|Z_3)$, където

$$Z_2 = \begin{pmatrix} 1110000 \\ 0110111 \\ 1010111 \\ 1100111 \\ 0001011 \\ 0001101 \\ 0001110 \end{pmatrix}, Z_3 = \begin{pmatrix} 1100010 \\ 0101111 \\ 1001111 \\ 1101101 \\ 0010101 \\ 0011001 \\ 0011100 \end{pmatrix}$$

и пораждащите матрици са такива, че $X_f = \{13, 14\}$.

Въпреки че вече получихме всички случаи за двете директни събираеми за кода C, необходимо е да ги свържем заедно. Нека подкодът $F_\sigma(C)$ е фиксиран, породен от матрицата G_2 или G_3. Разглеждаме всички (дори и да са еквивалентни) възможности за втория подкод $E_\sigma(C)$.

Нека $S_i, i = 1, 2$ е подгрупа на групата автоморфизми на двоичния $[14, 7]$ код, породен от G_i, състояща се от автоморфизмите на този код, които разместват първите 12 координати (съответстващи на 5-циклите) помежду им и разместват последните 2 координати (съответстващи на координатите на фиксираните точки) помежду им. Нека $St_i, i = 1, 2$ е подгрупа на симетричната група S_{12}, състояща се от пермутациите в S_i, ограничени до първите 12 координати, игнорирайки действието върху фиксираните точки. Имаме:

$$St_1 = \langle (1,9,4,2)(3,8)(5,11), (1,10,9,4,2,8,3)(5,7)(6,11) \rangle,$$
$$St_2 = \langle (1,3,9)(2,4,8)(5,10)(6,7), (1,10,2,12,3,5)(4,7,9,11,8,6) \rangle,$$

$|St_1| = 1344$ и $|St_2| = 1152$.

За пермутация $\tau \in S_{12}$ означаваме с $C^\tau_{i,j}$, $i = 1, 2$, $j = 1, \ldots, 60467$, самодуалния $[62, 31]$ код, определен от матрицата G_i с колони, пермутирани от τ, като пораждащ за $F_\sigma(C)$ и H_j като пораждаща матрица за $E_\sigma(C)^*$. Ако τ_1 и τ_2 принадлежат към един и същ десен съседен клас на G_2 (или G_3) в S_{12}, тогава кодовете $C^{\tau_1}_{i,j}$ и $C^{\tau_2}_{i,j}$ са еквивалентни. По този начин можем да използваме само десните трансверзали T_2 и T_3 на S_{12} по отношение на G_2 и G_3. След изчисляване на всички кодове $C^\tau_{i,j}$, $i = 2, 3$, $j = 1, \ldots, 60467$ за $\tau \in T_i$, $i = 2, 3$ обобщаваме резултатите в следната теорема.

Теорема 2.3.1. *Съществуват точно* 4636 *неекивалентни двоични самодуални* $[62, 31, 12]$ *кодове с автоморфизъм от тип* 5-$(12, 2)$. *Съществуват двоични самодуални* $[62, 31, 12]$ *кодове с тегловна функция* $W_{62,2}$ *за* $\beta = 1, 5, 6, 11$ *и* 21.

В § 2.4 намираме нови $[64, 32, 12]$ самодуални кодове с автоморфизъм от тип 5-$(12, 4)$. За двоичните самодуални $[64, 32, 12]$ кодове има една възможна тегловна функция за двойночетния код и две възможни тегловни функции за екстремалния едночетен код. Конструирани са кодове и с трите тегловни функции (вж. § 1.3).

Според Теорема 1.6.2 имаме, че C_π е двоичен самодуален $[16, 8]$ код. Съществуват точно седем такива кода: пет едночетни $i_2 \oplus 2e_7$, $2i_2 \oplus d_{12}$, $4i_2 \oplus e_8$, $8i_2$, $2d_8$ и два двойночетни d_{16} и $2e_8$. Минималното разстояние $d = 12$ на кода C ограничава минималното разстояние на C_π до $d' \geq 4$, ефективно елиминирайки всички кодове със събираемо i_2. Използвайки кодовете $2d_8, d_{16}$ и $2e_8$ и всички възможни $\binom{16}{4}$ разделяния на координатите $\{1, \ldots, 16\}$ на множества X_c и X_f, намираме минималното тегло на кода $F_\sigma(C)$. За кода C_π получаваме общо 8 различни пораждащи матрици: една от $2e_8$, пораждаща двойночетен подкод $F_\sigma(C)$; шест едночетни кодове, породени от d_{16} и един двойночетен код от $2d_8$. Означаваме с $G_4, \ldots, G_{11}$ пораждащите матрици на тези 8 кода, като само матриците G_9 и G_{10} не са в стандартна форма. Трябва да отбележим, $\pi^{-1}(G_4)$ и $\pi^{-1}(G_{11})$ пораждат двойночетни подкодове $F_\sigma(C)$ и следователно само в тези два случая $[64, 32, 12]$ кодовете са двойночетни.

За $4 \leq i \leq 11$, използвайки двойната трансверзала T_i, за кода породен от G_i и означен с $C^\tau_{i,j}$ кода, определен от матрицата G_i, със стълбове пермутирани от τ, като пораждащ за $F_\sigma(C)$ и H_j, като пораждаща матрица за $E_\sigma(C)^*$, изчисляваме тегловното разпределение на всички кодове, с изключение на $C^\tau_{4,j}$ и $C^\tau_{11,j}$, където получените $[64, 32, 12]$ кодове са двойночетни. Поради необходимостта от много време за изчисляване на всички кодове, за кодовете $C^\tau_{4,j}$ и $C^\tau_{11,j}$, изчисляваме само тези, за които групата автоморфизми на H_j не е от ред 5, 10, 20 и 40.

Що се отнася до едночетните $[64, 32, 12]$ кодове с автоморфизъм от тип 5-$(12, 4)$, намираме техните тегловни функции и проверяваме кодовете за еквивалентност. Получаваме следни-

те резултати.

Теорема 2.4.1. *С точност до еквивалентност съществуват* 6834068 *двоични едночетни* $[64, 32, 12]$ *кодове с автоморфизъм от тип* 5-$(12, 4)$. *От тези кодове* 1469019 *и* 5365049 *имат съответно тегловна функция* $W_{64,1}$ *и* $W_{64,2}$. *Съществуват кодове с* $W_{64,1}$ *за* $\beta =$ 19, 49 *и* 54, *и* $W_{64,2}$ *за* $\beta =$ 31, 39, 46, 47, 49, 54, 55, 57, 60, 62 *и* 69.

В § 2.5, чрез скъсяване на дължината с 2 на самодуалните $[60, 30, 12]$ кодове с автоморфизъм от тип 5-$(12, 0)$, получаваме нови $[58, 29, 10]$ самодуални кодове, които притежават автоморфизъм от тип 5-$(10, 8)$. Има две възможни тегловни функции за самодуален $[58, 29, 10]$ код, като и двете зависят от параметри. През 2017 г. Harada в [19] доказа, че първата тегловна функция не зависи от параметър, т.к. има единствена възможност $\beta = 55$. Известни са кодове и с двете тегловни функции (вж. § 1.3).

Нека C е двоичен самодуален $[60, 30, 12]$ код. Избирайки двойка $1 \leq i_1 < i_2 \leq 60$ от координати, конструираме нов код:

$$C' = \{(x_1, \ldots, x_n) | (x_1, \ldots, x_{60}) \in C_{60,i}, x_{i_1} = x_{i_2}\}.$$

Известно е, че C' е самодуален код с дължина 58 и затова казваме, че C' се получава от C чрез скъсяване.

Да скъсим всички 315 двоични самодуални $[60, 30, 12]$ кодове с автоморфизъм от ред 5: 236 конструирани в § 2.2 и 79 с автоморфизъм от тип 5-$(10, 10)$ от [37]. Тъй като всички кодове, които скъсяваме имат минимално тегло 12, всички получени кодови думи ще имат минимално тегло 10, така че кодовете C' са оптимални самодуални $[58, 29, 10]$ кодове. Скъсявайки по всички възможни двойки $(i_1, i_2), 1 \leq i_1 < i_2 \leq 60$, получаваме следния резултат.

Твърдение 2.5.1. *С точност до еквивалентност съществуват* 53968 *двоични самодуални* $[58, 29, 10]$ *кодове, които се*

получават чрез скъсяване на самодуалните $[60, 30, 12]$ *кодове с автоморфизъм от тип* $5\text{-}(12, 0)$. 189 *кода имат тегловна функция* $W_{58,1}$ *и* 53779 *имат тегловна функция* $W_{58,2}$ *за* 80 *двойки* (β, γ) :

- $\beta = 0, \gamma = 2m, m \in \{0, 26, 29, \ldots, 64, 66\}$;
- $\beta = 1, \gamma = 2m, m \in \{39, \ldots, 55\}$;
- $\beta = 2, \gamma = 2m, m \in \{0, 26, 28, \ldots, 51\}$.

Забележка 2.5.2. Получаваме за първи път самодуален $[58, 29, 10]$ код с тегловна функция $W_{58,2}$ за $\beta = 0$, $\gamma = 132$. От конструираните от нас 3 такива кода, 2 имат група от автоморфизми с 4 елемента и 1 с 8. Всички кодове, за които $|\mathrm{Aut}(C)| \equiv 0 \pmod 5$ притежават автоморфизъм от тип $5\text{-}(10, 8)$ и са известни от [37]. Всички останали кодове са нови.

Глава 3. Самодуални кодове с автоморфизъм от тринадесети ред

В тази глава, използвайки метода на Huffman и Йоргов, описан в § 1.6, класифицираме всички двоични самодуални $[n, n/2]$ кодове с дължини $78 \leq n \leq 84$, притежаващи автоморфизъм от ред 13 с 6 независими цикъла. Някои от конструираните кодове с дължини 78, 80, 82 и 84 задават нови стойности на параметрите в тегловните функции. Получаваме двойночетни $[80, 40, 16]$ кодове с автоморфизъм от тип $13\text{-}(6, 2)$ и едночетни самодуални $[80, 40, 14]$ кодове с тегловна функция $W_{80,2}$. Отбелязваме, че съществуването на едночетни $[80, 40, 14]$ кодове с $W_{80,2}$ досега не бе известно. Доказваме, че не съществува двоичен самодуален $[82, 41, 16]$ код и двоичен самодуален $[84, 42, 16]$ код с автоморфизъм от ред 13.

Чрез O и J ще бележим матрици със съответните размери, който се състоят само от нули, респективно от единици. С I

обичайно бележим единична матрица от съответната степен.

Оптималните самодуални кодове с автоморфизъм от нечетен прост ред са предмет на обстойно изучаване. Всъщност всички такива кодове са класифицирани до дължина 50 [38]. Според Gulliver и Harada [18] съществуват 5 екстремални двойноциркулантни двойночетни самодуални кода с дължина 80, притежаващи автоморфизъм от ред 13. Редовете на групите от автоморфизми на тези кодове са: 246480 за един код ($P_{80,1} = B_{80,5}$), който е едновременно двойноциркулантен и граничен двойноциркулантен и четири кода ($B_{80,1}$–$B_{80,4}$), за които $|\mathrm{Aut}(C)| = 78$. В [17] Gaborit и Otmani конструират $[78, 39, 14]$ самодуален код с автоморфизъм от ред 13 с $W_{78,1}$ за $\alpha = 0$, $\beta = -26$.

Дончева и Harada в [15] класифицират всички двойночетни самодуални $[80, 40, 16]$ кодове с автоморфизъм от ред 19.

Екстремалните или оптимални двоични самодуални кодове с автоморфизъм от ред 13 с 4 цикъла са класифицирани от Янков и Русева в [39]. Продължаваме изследването на двоични самодуални кодове с автоморфизъм от ред 13 със следващия възможен случай, т.е. 6 независими цикъла. Трябва да отбележим, че Капралов, Русева и Радева в [26] конструират 35 двойночетни $[80, 40, 16]$ кода с автоморфизъм от тип 13-$(6, 2)$, но не дават класификация.

От границата на Rains (Теорема 1.2.13) имаме $d \leq 16$ за двоични самодуални кодове с дължини от 78 до 92. Нека C е оптимален двоичен самодуален $[2k, k, d]$ код за $39 \leq k \leq 46$, а минималното тегло на кода е $d = 16$ или 14. Предполагаме, че кодът C има автоморфизъм σ от ред 13 с $c = 6$ цикъла и f фиксирани точки за

$$0 \leq f = 78 - 2k \leq 14.$$

Според Теорема 1.6.4, ако $f > c = 6$ имаме

$$f \geq \sum_{k=0}^{(f-c)/2-1} \left\lceil \frac{d}{2^k} \right\rceil,$$

което за $d = 16$ и $k \geq 1$ дава границата $f \geq 16$. Следователно, имаме брой на фиксираните точки $f = 0,\ 2,\ 4,\ 6$ и съответно размерности $39 \leq k \leq 42$.

Възможните тегловни функции за екстремални и оптимални двоични самодуални кодове с дължини $72 \leq n \leq 100$ са изведени от Dougherty, Gulliver и Harada [16]. По-късно Harada в [20] доказва някои допълнителни ограничения за параметрите. Тъй като към настоящия момент в литературата няма конструирани едночетни $[2k, k, 16]$, $k = 39, 40, 41, 42$ кодове, то изчисляваме възможните тегловни функции за самодуални едночетни $[2k, k, 14]$ кодове, когато $k = 39, 40, 41, 42$.

В § 3.1 класифицираме ермитово самодуални кодове с дължина 6 над полето от всички четнотегловни полиноми в $\mathbb{F}_2[x]/\langle x^{13} - 1\rangle$.

Според [39], 2 е примитивен корен по модул 13, следователно $\mathcal{P}$ е поле с 2^{12} елемента и единица полинома $e(x) = x + \cdots + x^{12}$. Използваме елемента $\alpha = 1 + x + x^3 + x^5$, който е примитивен елемент в $\mathcal{P}$ [41]. Означаваме $\beta = \alpha^{13}$, който е елемент от мултипликативен ред 315 в $\mathcal{P}$. Може да запишем $\mathcal{P}^* = \{x^i\beta^j | 0 \leq i \leq 12, 0 \leq j \leq 314\}$.

След Гаусова елиминация можем да разгледаме пораждащата матрица на кода във вида $G = (I|Z)$, където Z е 3×3 матрица над $\mathcal{P}$. Използвайки Теорема 1.6.4, транформираме матрицата Z в следната матрица

$$Z = \begin{pmatrix} \beta^{i_1} & \beta^{i_2} & \beta^{i_3} \\ \beta^{i_4} & x^{l_5}\beta^{i_5} & x^{l_6}\beta^{i_6} \\ \beta^{i_7} & x^{l_8}\beta^{i_8} & x^{l_9}\beta^{i_9} \end{pmatrix},$$

където $i_1 \leq i_2 \leq i_3$, $0 \leq i_t \leq 314$, $0 \leq l_t \leq 12$ или някои от елементите на Z са нули. Използвайки условието за ортогоналност (1.11) и проверявайки, че $d = 16$ изчисляваме всички неекивалентни варианти за първият ред на Z и намираме 1676 възможни тройки (i_1, i_2, i_3). След това добавяме втория ред на Z и получаваме 4086196 различни 2×3 подматрици. Накрая, след добавяне на последния ред, получаваме точно 322103 не-

еквивалентни кода с минимално разстояние $d = 16$. В резултат получаваме следната теорема.

Теорема 3.1.1. *Съществуват точно* 322103 *неекивалентни кода* C_φ *с дължина* 6 *над множеството* $\mathcal{P}$ *от всички четнотегловни полиноми в* $\mathbb{F}_2[x]/\langle x^{13}-1\rangle$, *за които* $d(E_\sigma(C)^*) = 16$.

В § 3.2 извършваме пълна класификация на всички оптимални самодуални кодове с дължина 78 и с автоморфизъм от ред 13 с 6 цикъла. За самодуалните $[78, 39, 14]$ кодове има две възможни тегловни функции (вж. § 1.3).

Нека C е самодуален код с дължина 78 и с автоморфизъм от тип 13-$(6, 0)$. От Теорема 1.6.2, C_π е двоичен самодуален $[6, 3, 2]$ код. Има единствен такъв код: $3i_2$ ([24]) с пораждаща матрица $G_1 = (I_3|I_3)$. От Теорема 1.6.1, C е директна сума на $F_\sigma(C)$ и $E_\sigma(C)$. Определяме пораждащата матрица на $E_\sigma(C)$ да е пораждащата матрица на един от кодовете от Теорема 3.1.1. За всички пермутации $\tau \in S_6$ определяме пораждащата матрица на C_π да е $\tau(G_1)$. Обобщаваме резултатите в следното:

Твърдение 3.2.1. *Съществуват точно* 1592 *неекивалентни двоични самодуални* [78, 39, 14] *кодове с автоморфизъм от тип* 13-$(6, 0)$.

Всички кодове, които получаваме имат тегловна функция $W_{78,1}$ за $\beta = -117, -104, -78, -65, -52, -39, -26, -13, 0$. Всички стойности, освен $\beta = -78, -26$ и 0, са нови.

В § 3.3 правим пълна класификация на всички оптимални самодуални кодове с дължина 80 и с автоморфизъм от тип 13-$(6, 2)$. За двойночетни $[80, 40, 16]$ кодове има единствена възможна тегловна функция. Според теоремата на Assmus-Mattson (Теорема 1.1.25), кодовите думи с определено тегло в екстремален двойночетен $[80, 40, 16]$ код образуват 3-дизайн (вж. [15]). За тегловната функция на едночетни $[80, 40, 14]$ самодуални кодове съществува отново единствена възможност (вж. § 1.3).

Нека C е самодуален $[80, 40, d]$ код с автоморфизъм от тип 13-$(6, 2)$. От Теорема 1.6.2, C_π е двоичен самодуален $[8, 4, \geq 2]$ код. Има два такива кода ([24]): едночетният $4i_2$ и двойночетният h_8. Тъй като трябва да изберем 2 от 8 координатни позиции за множеството X_f от фиксирани точки, в случая $4i_2$, за да има $d \geq 14$ не е възможно целият носител на събираемото i_2 да е в X_f. Кодът h_8 има трикратно транзитивна група от автоморфизми, така че можем да изберем всяка двойка координати в X_f. Така получаваме следното:

Твърдение 3.3.1. *Съществуват две възможни пораждащи матрици за кода C_π за $[80, 40, d]$ самодуален код с автоморфизъм от тип* 13-$(6, 2)$*: $G_2 = (I_4|I_4)$ и $G_3 = (I_4|I_4 + J_4)$, където двете най-десни координати съответстват на множеството от фиксирани точки.*

Твърдение 3.3.2. *С точност до еквивалентност съществуват* 195 *двойночетни* $[80, 40, 16]$ *кода с автоморфизъм от тип* 13-$(6, 2)$*. Съществуват* 162696 *неекивалентни самодуални едночетни двоични* $[80, 40, 14]$ *кода, притежаващи автоморфизъм от тип* 13-$(6, 2)$*.*

Получените двойночетни $[80, 40, 16]$ кодове с $|\mathrm{Aut}(C)| = 13$ и 26 са нови. Едночетните $[80, 40, 14]$ самодуални кодове имат тегловна функция $W_{80,2}$ за $\beta = 0$ и $\alpha = -13k$, $k \in \{2, \ldots, 25, 27\}$. Отбелязваме, че за всички тези стойности в $W_{80,2}$ преди това няма известни кодове. Harada и Munemasa в [22] определят тегловните функции на предполагаем s-екстремален едночетен самодуален $[80, 40, 14]$ код, но нито един от кодовете, които получаваме не е s-екстремален ($W_{80,2}$ за $\alpha = \beta = 0$).

В § 3.4 представяме пълна класификация на двоичните самодуални $[82, 41, 14]$ кодове с автоморфизъм от тип 13-$(6, 4)$. За тях съществуват два възможни тегловни полинома. Известни са само кодове с тегловен полином $W_{82,1}$ (вж. § 1.3).

Нека C е самодуален $[82, 41, 14]$ код с автоморфизъм от тип

13-$(6,4)$. От Теорема 1.6.2, C_π е двоичен самодуален $[10,5,\geq 2]$ код. Има два такива кода ([24]): $5i_2$ и i_2+h_8. Чрез проверка на възможния избор на 10 координатни позиции от двата кода в подмножества X_c и X_f, откриваме 3 възможни пораждащи матрици за C_π:

$$G_4 = \begin{pmatrix} I_5 & I_5 \end{pmatrix}, G_5 = \begin{pmatrix} 1 & 1 & O & O \\ 0 & 0 & I_4 & I_4+J_4 \end{pmatrix},$$

$$G_6 = \begin{pmatrix} & 01000 \\ & 00111 \\ I_5 & 10011 \\ & 10101 \\ & 10110 \end{pmatrix},$$

където G_4 е получена от $5i_2$, а другите две са получени от i_2+h_8. Фиксираме $E_\sigma(C)$ и разглеждаме всички пермутации $\tau \in S_6$, действащи на множеството $X_c = \{1,\ldots,6\}$ от циклични позиции в G_i, $i=4,5,6$.

Твърдение 3.4.1. *Не съществува двоичен самодуален* $[82,41,16]$ *код с автоморфизъм от ред* 13. *Неекивалентните двоични самодуални* $[82,41,14]$ *кодове с автоморфизъм от тип* 13-$(6,4)$ *са:*

- $gen(C_\pi) = G_4$: 604992 *кода с тегловна функция* $W_{82,2}$*;*
- $gen(C_\pi) = G_5$: 164338 *кода с тегловна функция* $W_{82,2}$*;*
- $gen(C_\pi) = G_6$: 50989 *кода с тегловна функция* $W_{82,2}$.

Когато $C_\pi = G_4$ кодовете имат тегловна функция $W_{82,2}$ за 45 различни стойности на α и β.

Когато $C_\pi = G_5$ кодовете имат тегловна функция $W_{82,2}$ за 38 различни стойности на α и β.

В случая на $C_\pi = G_6$ има 50972 кода с група от автоморфизми от ред 13 и 17 кода с $|\mathrm{Aut}(C)| = 39$. Всички получени кодове имат $\alpha = -680$, $\beta = 170$ в $W_{82,2}$.

В § 3.5 класифицираме всички двоични самодуални $[84, 42, 14]$ кодове с автоморфизъм от тип 13-$(6, 6)$. Съществуват две възможности за тегловни функции. Известни до момента са само кодове с тегловна функция $W_{84,2}$ (вж. § 1.3).

Нека C самодуален е $[84, 42, 14]$ код с автоморфизъм от тип 13-$(6, 6)$. От Теорема 1.6.2, C_π е двоичен самодуален $[12, 6, \geq 2]$ код. Има три такива кода ([24]): $2i_2+h_8$, $6i_2$, и d_{12}. Чрез проверка на възможностите за избор на 12 координатни позиции от двата кода в подмножества X_c и X_f, получаваме 4 възможни пораждащи матрици за C_π:

$$G_7 = \begin{pmatrix} I_6 & I_2 & O \\ & O & I_4 + J_4 \end{pmatrix}, G_8 = \left(\begin{array}{c|c} I_6 & I_6 \end{array} \right),$$

$$G_9 = \left(\begin{array}{c|c} & 100110 \\ & 010110 \\ I_6 & 001110 \\ & 111101 \\ & 111011 \\ & 000111 \end{array} \right), G_{10} = \left(\begin{array}{c|c} 100001 & 010010 \\ 010001 & 001010 \\ 001001 & 000110 \\ 000100 & 011111 \\ 000001 & 111101 \\ 000011 & 000011 \end{array} \right),$$

където G_7 е получена от $2i_2 + h_8$, G_8 се получава от $6i_2$, а останалите две – от d_{12}. Нека да фиксираме $E_\sigma(C)$ и да разгледаме всички пермутации $\tau \in S_6$, действащи на цикличните позиции в G_i, $i = 7, \ldots, 10$.

Твърдение 3.5.1. *Не съществува двоичен самодуален* $[84, 42, 16]$ *код с автоморфизъм от ред* 13. *Неекивалентните двоични самодуални* $[84, 42, 14]$ *кодове с автоморфизъм от тип* 13-$(6, 6)$ *са:*

- $gen(C_\pi) = G_7$: 607773 *кода с тегловна функция* $W_{84,2}$;
- $gen(C_\pi) = G_8$: 113879 *кода с тегловна функция* $W_{84,1}$;
- $gen(C_\pi) = G_9$: 604064 *кода с тегловна функция* $W_{84,2}$;
- $gen(C_\pi) = G_{10}$: 113439 *кода с тегловна функция* $W_{84,1}$.

Когато $C_\pi = G_7$ кодовете имат тегловна функция $W_{84,2}$ за 26 различни стойности на α.

За матрицата G_8 кодовете имат тегловна функция $W_{82,1}$ за различни стойности на $\alpha = 2280 + 26l$, $l \in \{0, \ldots, 44, 54\}$ за $\beta = 18$, 31, 44 и 57. Общо 112449, 1403, 6 и 21 кода имат група от автоморфизми, съответно от ред 13, 26, 39 и 78.

В случая на $C_\pi = G_9$, кодовете имат тегловна функция $W_{84,2}$ за 28 различни стойности на α.

Когато $C_\pi = G_{10}$ кодовете имат тегловна функция $W_{82,1}$ за различни стойности на $\alpha = 2286 + 26l$, $l \in \{0, \ldots, 46, 48\}$ за $\beta = 18$, 31, 44 и 57. Общо 112005, 1401, 12 и 21 кода имат група от автоморфизми, съответно от ред 13, 26, 39 и 78.

Глава 4. Четири циркулантни самодуални $[64, 32, 12]$ кодове, съседи и кодове с дължина 66, получени чрез разширяване

В настоящата глава конструираме екстремални едночетни самодуални кодове с дължини 64 и 66 с неизвестни до този момент тегловни функции. Кодовете с дължина 64 конструираме като самодуални съседи на екстремалните четири циркулантни едночетни самодуални кодове. Използвайки метода, представен в [31], получаваме от кодове с дължина 64, кодове с дължина 66 чрез разширяване. Доказваме, че съществуват най-малко 44 нееквивалентни екстремални двойночетни самодуални $[64, 32, 12]$ кодове с радиус на покритие 12, достигащи границата на Delsarte (Теорема 1.7.6).

Нека C е едночетен самодуален код. Нека C_0 е подкода на C, състоящ се от кодови думи x с $\mathrm{wt}(x) \equiv 0 \pmod 4$. *Сянката* S на C е дефинирана чрез $C_0^\perp \setminus C$. Сенки за самодуални кодове са въведени от Conway и Sloane [12], за да се даде възможно най-голямото минимално тегло сред едночетните самодуални кодове и да се осигурят ограничения върху тегловните функции на тези кодове.

Най-големите възможни минимални тегла между едночет-

ните самодуални кодове с дължина n са дадени за $n \leq 72$ в [12]. Възможните тегловни функции на едночетни самодуални кодове с най-големите възможни минимални тегла са дадени в [12] и [16] за $n \leq 72$. Често е интересен въпросът за определяне на това кои от възможните тегловни функции всъщност възникват (вж. [12]), а също така и в случай, че тези функции зависят от параметри, кои стойности на параметрите реално се осъществяват.

Целта ни е да конструираме екстремални едночетни самодуални кодове с тегловни функции, неизвестни до този момент. По точно, показваме, че съществуват екстремални едночетни самодуални $[64, 32, 12]$ кодове с тегловни функции $W_{64,1}$ за $\beta = 35$ и $W_{64,2}$ за $\beta \in \{19, 34, 42, 45, 50\}$. Тези кодове са конструирани като самодуални съседи на екстремалните четири циркулантни едночетни самодуални кодове. В резултат конструираме екстремални едночетни самодуални $[66, 33, 12]$ кодове с тегловни функции $W_{66,1}$ за $\beta \in \{7, 58, 70, 91, 93\}$ и $W_{66,3}$ за $\beta \in \{22, 23\}$. Тези кодове са получени от екстремални едночетни самодуални $[64, 32, 12]$ кодове по метода, представен в [31].

В § 4.1 представяме възможните тегловни функции на екстремални едночетни самодуални кодове с дължини 64 и 66 и техните сенки. Както вече знаем, за екстремалните едночетни самодуални $[64, 32, 12]$ кодове има две възможни тегловни функции и кодове съществуват и с двете функции. Екстремални едночетни самодуални $[66, 33, 12]$ кодове са конструирани и с трите тегловни функции, които съществуват за тази дължина.

В § 4.2 правим класификация на екстремални четири циркулантни едночетни самодуални $[64, 32, 12]$ кодове. С пълно изчерпване, откриваме всички различни екстремални четири циркулантни едночетни самодуални $[64, 32, 12]$ кодове. След това тези кодове проверяваме допълнително за еквивалентност, с което завършваме класификацията.

За да намерим всички четирициркулантни кодове, разглеждаме всички двойки циркулантни матрици A и B от тип

16×16, удовлетворяващи условието

$$AA^T + BB^T = I_{16},$$

така че сумата от теглата на първите редове на A и B е сравнима с 1 (mod 4) и е по-голяма или равна на 13. Използвайки циклично завъртане на първите редове получаваме еквивалентен код и можем да приемем, без загуба на общност, че последният елемент на първия ред от матрицата B е 1. Нашите резултати, с помощта на компютър показват, че всички екстремални четири циркулантни едночетни самодуални $[64, 32, 12]$ кодове са разделени на 67 орбити.

Твърдение 4.2.1. *С точност до еквивалентност, съществуват* 67 *екстремални четири циркулантни едночетни самодуални* $[64, 32, 12]$ *кодове.*

Нека да означим тези 67 кода с $C_{64,i}$ $(i = 1, 2, \ldots, 67)$. Оказва се, че кодовете $C_{64,i}$ имат тегловна функция $W_{64,2}$ за 10 различни стойности на β.

В § 4.3 конструираме екстремални самодуални $[64, 32, 12]$ кодове чрез разглеждане на самодуални съседи.

Два самодуални кода C и C' с дължина n се наричат *съседи*, ако

$$\dim(C \cap C') = n/2 - 1.$$

Всеки самодуален код с дължина n може да бъде достигнат от всеки друг, като се вземат последователни съседи (вж. [12]). Тъй като всеки самодуален код C с дължина n съдържа вектора с n единици $\mathbf{1}$, C има $2^{n/2-1} - 1$ подкода D от коразмерност 1, съдържащи $\mathbf{1}$. Понеже $\dim(D^\perp/D) = 2$, има два самодуални кода, такива че C е между $D^\perp$ и D. Ако C е едночетен самодуален код с дължина, която се дели на 8, тогава C има два двойночетни самодуални съседа (вж. [9]). Ще конструираме екстремални самодуални $[64, 32, 12]$ кодове чрез разглеждане на самодуални съседи.

За $i = 1, 2, \ldots, 67$, намираме всички екстремални едночетни самодуални съседи на $C_{64,i}$, които не са еквивалентни на нито един от тези 67 кода. Получаваме, че тези кодове са разделени на 385 класа от нееквивалентни кода с представители кодовете $D_{64,i}$ $(i = 1, 2, \ldots, 385)$. Кодовете $D_{64,i}$ конструираме като

$$\langle (C_{64,j} \cap \langle x \rangle^{\perp}), x \rangle.$$

Така получаваме следният резултат.

Твърдение 4.3.1. *Съществува екстремален едночетен самодуален* $[64, 32, 12]$ *код с тегловна функция* $W_{64,1}$ *за* $\beta = 35$ *и* $W_{64,2}$ *за* $\beta \in \{19, 34, 42, 45, 50\}$.

Нека сега да разгледаме екстремалните двойночетни самодуални съседи на $C_{64,i}$ $(i = 1, 2, 3)$. Понеже сянката има минимално тегло 12, двата двойночетни самодуални съседа $\mathcal{C}^1_{64,i}$ и $\mathcal{C}^2_{64,i}$ са екстремалните двойночетни самодуални $[64, 32, 12]$ кодове с радиус на покритие 12 (вж. [10]). По този начин, конструираме 6 екстремални двойночетни самодуални $[64, 32, 12]$ кода с радиус на покритие 12. В допълнение, сред 385-те кода $D_{64,i}$ $(i = 1, 2, \ldots, 385)$ има 19 екстремални едночетни самодуални кода $D_{64,j}$, които имат сянка с минимално тегло 12, където

$$j \in \{1, 2, 12, 19, 22, 33, 44, 58, 66, 68, 84, 95, 108, 115, 136, 143, 191, 240, 254\}.$$

Кодовете $D_{64,j}$ имат два двойночетни самодуални съседа $\mathcal{D}^1_{64,j}$ и $\mathcal{D}^2_{64,j}$, които са екстремални двойночетни самодуални $[64, 32, 12]$ кодове с радиус на покритие 12. Проверяваме, че съществуват еквивалентни кодове сред четирите кода в [10], шестте кода $\mathcal{C}^1_{64,i}$ и $\mathcal{C}^2_{64,i}$, както и сред 38 кода $\mathcal{D}^1_{64,j}$ и $\mathcal{D}^2_{64,j}$, за които

$$\mathcal{D}^2_{64,22} \cong \mathcal{D}^2_{64,68}, \mathcal{D}^2_{64,33} \cong \mathcal{D}^2_{64,84}, \mathcal{D}^2_{64,44} \cong \mathcal{D}^2_{64,95}, \mathcal{D}^2_{64,136} \cong \mathcal{D}^2_{64,143},$$

където $C \cong D$ означава, че C и D са еквивалентни и няма друга двойка еквивалентни кодове. Резултатите обобщаваме в

следното твърдение.

Твърдение 4.3.2. *Съществуват поне* 44 *нееквивалентни екстремални двойночетни самодуални* $[64, 32, 12]$ *кодове с радиус на покритие* 12*, достигащи границата на Delsarte.*

Два двойночетни съседа $\mathcal{D}^1_{64,i}$ и $\mathcal{D}^2_{64,i}$ $(i = 68, 84, 95, 143)$ разграничаваме чрез носителя $\mathrm{supp}(x)$. Кодовете $\mathcal{D}^1_{64,i}$ и $\mathcal{D}^2_{64,i}$ са конструирани като $\langle (D_{64,i} \cap \langle x \rangle^{\perp}), x \rangle$.

В § 4.4 получаваме четири циркулантни едночетни самодуални $[64, 32, 10]$ кодове. Доказваме несъществуването на екстремален едночетен самодуален $[64, 32, 12]$ съсед на $E_{64,i}$ за $i = 1, 2, \ldots, 224$.

Използвайки подход, подобен на дадения в раздел 4.2, изследваме различните четири циркулантни едночетни самодуални $[64, 32, 10]$ кодове. С помощта на компютър получаваме, че различните четири циркулантни едночетни самодуални $[64, 32, 10]$ кодове са разделени на 224 класа от нееквивалентни кода.

Твърдение 4.4.1. *С точност до еквивалентност, съществуват* 224 *четири циркулантни едночетни самодуални* $[64, 32, 10]$ *кодове.*

Да означим тези 224 кода с $E_{64,i}$ $(i = 1, 2, \ldots, 224)$.

Методът за конструиране на самодуални съседи е представен в [10]. За $C = E_{64,i}$, $i = 1, 2, \ldots, 224$, нека M е матрица, чиито редове са кодовите думи с тегло 10 в C. Предполагаме, че има вектор x с четно тегло, така че

$$Mx^T = \mathbf{1}^T. \tag{4.1}$$

Тогава $C^0 = \langle x \rangle^{\perp} \cap C$ е подкод с индекс 2 в C. Имаме самодуални съседи $\langle C^0, x \rangle$ и $\langle C^0, x + y \rangle$ на C за някой вектор $y \in C \setminus C^0$, които нямат кодова дума с тегло 10 в C. Когато C има самодуален съсед C' с минимално тегло 12, има вектор x, удовлетворяващ (4.1) и така получаваме C'. За $i = 1, 2, \ldots, 224$, проверява-

ме, че има единствен вектор, удовлетворяващ (4.1) и C има два самодуални съседи, където C^0 е двойночетен $[64, 31, 12]$ код. В този случай двата съседни кода са двойночетни автоматично. Така получаваме следният резултат.

Твърдение 4.4.2. *Не съществува екстремален едночетен самодуален* $[64, 32, 12]$ *съсед на* $E_{64,i}$ *за* $i = 1, 2, \ldots, 224$.

В § 4.5 конструираме нови екстремални едночетни самодуални кодове с дължина 66.

Следващият метод за конструиране на едночетни самодуални кодове е представен в [31]. Нека C е самодуален код с дължина n. Нека x е вектор с нечетно тегло. Нека C^0 е подкод на C, състоящ се от всички кодови думи, които са ортогонални на x. Тогава има съседни класове C^1, C^2, C^3 на C^0, такива че $C^{0\perp} = C^0 \cup C^1 \cup C^2 \cup C^3$, където $C = C^0 \cup C^2$ и $x + C = C^1 \cup C^3$. Кодът

$$C(x) = (0, 0, C^0) \cup (1, 1, C^2) \cup (1, 0, C^1) \cup (0, 1, C^3) \tag{4.2}$$

е едночетен самодуален код с дължина $n + 2$ [31]. В този параграф конструираме нови екстремални едночетни самодуални кодове с дължина 66, използвайки екстремалните едночетни самодуални $[64, 32, 12]$ кодове, получени в § 4.2 и § 4.3.

Изчерпателното ни търсене показва, че съществуват 1166 нееквивалентни екстремални едночетни самадуални $[66, 33, 12]$ кодове, конструирани като кодовете $C(x)$ в (4.2) от кодовете $C_{64,i}$ $(i = 1, 2, \ldots, 67)$. 1157 кода от 1166 кода имат тегловна функция $W_{66,1}$ за $\beta \in \{7, 8, \ldots, 92\} \setminus \{9, 11\}$, 3 от тях имат тегловна функция $W_{66,3}$ за $\beta \in \{30, 49, 54\}$ и 6 от тях имат тегловна функция $W_{66,2}$. Екстремални едночетни самодуални $[66, 33, 12]$ кодове с тегловна функция $W_{66,1}$ за $\beta \in \{7, 58, 70, 91, 93\}$ досега не бяха известни.

Прилагайки конструкцията, дадена в (4.2) към $D_{64,i}$, откриваме екстремални едночетни самодуални $[66, 33, 12]$ кодове $D_{66,j}$ с тегловна функция $W_{66,3}$ за $\beta \in \{22, 23\}$, които са неизвестни до момента.

Получаваме следния резултат.

Твърдение 4.5.1. *Съществува екстремален едночетен самодуален* $[66, 33, 12]$ *код с тегловна функция* $W_{66,1}$ *за* $\beta \in \{7, 58, 70, 91, 93\}$ *и тегловна функция* $W_{66,3}$ *за* $\beta \in \{22, 23\}$.

Публикации включени в дисертацията

[2] D. Anev, M. Harada, and N. Yankov, New extremal singly even self-dual codes of lengths 64 and 66, *Journal of Algebra Combinatorics Discrete Structures and Applications (JACODESMATH)*, vol. 5, no. 3, pp. 143-151, 2018 (indexed in MathSciNet, Zentralblatt MATH, EBSCO), DOI: 10.13069/jacodesmath.458601

[34] N. Yankov, D. Anev, and M. Gürel, "Constructing the self-dual codes with an automorphism of order 13 with 6 cycles," *Advances in Mathematics of Communications*, vol. 11, no. 3, pp. 635–645, 2017, DOI: 10.3934/amc.2017047

[35] N. Yankov, D. Anev, "New self-dual $[78, 39, 14]$ codes with an automorphism of order 13," *Proceedings of Eighth International Workshop on Optimal Codes and Related Topics (OC2017)*, Sofia, July, 2017, pp. 128–133.

[36] N. Yankov, D. Anev, M.H. Lee, "On the even subcode of codes with an automorphism of order 5 with 12 cycles," *Proceedings of the XXIII-th International Workshop on Multimedia Signal Processing and Transmission (MSPT)*, p. 6, Youngil Publishing, Korea, ISSN 1975-5635, 2017.

Апробация на резултатите

Резултатите, които са включени в настоящата дисертация, са получени в съавторство с:

- Янков § 2;
- Янков и Gurel [34];
- Янков и Harada [2].

публикувани са в научното списание

- Advances in Mathematics of Communications (JCR 0.8) ISSN 1930-5346:
  N. Yankov, D. Anev, M. Gurel, Self-Dual Codes with an Automorphism of Order 13, Advances in Mathematics of Communications, vol. 11, no. 3, 2017, pp. 635-645, ISSN 1930-5346, DOI: 10.3934/amc.2017047
- Journal of Algebra Combinatorics Discrete Structures and Applications:
  D. Anev, M. Harada, and N. Yankov, New extremal singly even self-dual codes of lengths 64 and 66, Journal of Algebra Combinatorics Discrete Structures and Applications (JACODESMATH), vol. 5, no. 3, pp. 143-151, 2018 (indexed in MathSciNet, Zentralblatt MATH, EBSCO)

и в рецензирани сборници от конференции:

- N. Yankov, D. Anev, New self-dual [78, 39, 14] codes with an automorphism of order 13, Proceedings of Eighth International Workshop on Optimal Codes and Related Topics (OC2017), Sofia, July, 2017, pp. 128-133
- N. Yankov, D. Anev, M.H. Lee, On the even subcode of codes with an automorphism of order 5 with 12 cycles, Proceedings of the XXIII-th International Workshop on Multimedia Signal Processing and Transmission (MSPT), Youngil Publishing, Korea, p. 6, ISSN 1975-5635, 2017

Резултатите от дисертационния труд са докладвани на:

- Международна конференция по оптимални кодове и свързани теми (OCRT'17), Дни на математиката в София, София, 10 - 14 юли 2017
- Национален семинар по кодиране „Проф. Стефан Додунеков", Троян, 30 ноември - 3 декември 2017
- XXIII International Workshop on Multimedia Signal Processing and Transmission (MSPT), Jeonju, Korea, February 2017

Авторска справка

По мнение на автора, основните приноси на дисертационния труд са:
I. Използвайки метода на Huffman и Йоргов за конструиране на двоични самодуални кодове, притежаващи автоморфизъм от нечетен прост ред p:

1. Класифицирани са всички оптимални двоични самодуални кодове с дължини $60 \leq n \leq 64$, с автоморфизъм от ред 5 с 12 независими цикъла. Извършена е пълна класификация на кодовете с дължини 60 и 62.

Доказано е, съществуването на точно 60467 нееквивалентни кода C_φ с дължина 12 над множеството $\mathcal{P}$ от всички четнотегловни полиноми от $\mathbb{F}_2[x]/\langle x^5 - 1\rangle$, за които кодът $\varphi^{-1}(C_\varphi)$ има минимално разстояние 12. Резултатите за получените двоични самодуални кодове са следните:

- $[60, 30, 12]$: Конструирани са 223 нови двоични самодуални кодове с автоморфизъм от тип 5-$(12, 0)$ за 17 стойности на двойката $(\beta, |\mathrm{Aut}(C)|)$. Всички получени кодове имат тегловна функция $W_{60,2}$.

- $[62, 31, 12]$: Съществуват 4636 нееквивалентни двоични самодуални $[62, 31,$
  $12]$ кодове с автоморфизъм от тип 5-$(12, 2)$. Всички кодове имат тегловна функция $W_{62,2}$. Стойностите за $\beta = 1, 5, 6, 11$ и 21 са нови.

- $[64, 32, 12]$: Намерени са 6837749 нееквивалентни двоични самодуални кодове с автоморфизъм от тип 5-$(12, 4)$, от които:

  - при $\mathrm{gen}(C_\pi) = G_4$ и $\mathrm{gen}(C_\pi) = G_{11}$ са получени 3681 нови двойночетни кодове с W_{64}, за 12 различни стойности на $|\mathrm{Aut}(C)|$.

- при $\mathrm{gen}(C_\pi) = G_7$ и $\mathrm{gen}(C_\pi) = G_{10}$ има 1469019 едночетни кодове с $W_{64,1}$ за 12 различни стойности на β, като $\beta = 19, 49$ и 54 са нови.
- при $\mathrm{gen}(C_\pi) = G_5$, $\mathrm{gen}(C_\pi) = G_6$, $\mathrm{gen}(C_\pi) = G_8$ и $\mathrm{gen}(C_\pi) = G_9$ има 5365049 едночетни кодове с $W_{64,2}$ за 54 различни стойности на β, като 11 от тях са нови.

2. Направена е пълна класификация на всички двоични самодуални кодове с дължини $78 \leq n \leq 84$, с автоморфизъм от ред 13 с 6 независими цикъла. Доказано е, съществуването на точно 322103 нееквивалентни кода C_φ с дължина 6 над множеството $\mathcal{P}$ от всички четнотегловни полиноми в $\mathbb{F}_2[x]/\langle x^{13} - 1\rangle$, за които $d(E_\sigma(C)^*) = 16$. За тези кодове е получена следната информация:

- $[78, 39, 14]$: Получени са 1592 нееквивалентни двоични самодуални кодове с автоморфизъм от тип 13-$(6, 0)$. Всички кодове имат тегловна функция $W_{78,1}$ за 6 нови стойности на β.

- Кодове с дължина 80:

  - Конструирани са 195 двойночетни $[80, 40, 16]$ кода с автоморфизъм от тип 13-$(6, 2)$ и тегловна функция $W_{80,1}$. От тях 190 са нови.
  - Съществуват 162696 нееквивалентни самодуални едночетни двоични $[80, 40, 14]$ кода, притежаващи автоморфизъм от тип 13-$(6, 2)$. Тези кодове съществуват за тегловна функция $W_{80,2}$ за $\beta = 0$ и $\alpha = -13k$, $k \in \{2, \ldots, 25, 27\}$. Всички стойности на двойката параметри (α, β) са нови.

- $[82, 41, 14]$: Доказано е, че не съществува двоичен самодуален $[82, 41, 16]$ код с автоморфизъм от ред 13. За първи път са получени 820319 нееквивалентни двоични самодуални $[82, 41, 14]$ кодове с автоморфизъм от тип 13-$(6, 4)$ и

тегловна функция $W_{82,2}$. Намерени са 84 нови стойности на двойката параметри (α, β).

- $[84, 42, 14]$: Не съществува двоичен самодуален $[84, 42, 16]$ код с автоморфизъм от ред 13. Съществуват 1439155 нееквивалентни двоични самодуални кодове с автоморфизъм от тип 13-$(6, 6)$, от които:

  - при $\mathrm{gen}(C_\pi) = G_8$ и $\mathrm{gen}(C_\pi) = G_{10}$ има 227318 кодове с тегловна функция $W_{84,1}$, за 93 различни стойности на α и $\beta = 18, 31, 44$ и 57. За първи път са получени кодове с функцията $W_{84,1}$.
  - при $\mathrm{gen}(C_\pi) = G_7$ и $\mathrm{gen}(C_\pi) = G_9$ са получени 1211837 кодове с тегловна функция $W_{84,2}$, за 54 нови стойности на α.

II. Приложен е метод за конструиране на нови двоични самодуални кодове чрез скъсяване на дължината им с 2. Съществуват 53968 нееквивалентни двоични самодуални $[58, 29, 10]$ кодове, получени чрез скъсяване на самодуалните $[60, 30, 12]$ кодове с автоморфизъм от тип 5-$(12, 0)$. От тях 189 кода имат тегловна функция $W_{58,1}$, като 115 са нови за $|\mathrm{Aut}(C)| = 1, 2, 4, 8$ и 16, а 53779 кода имат тегловна функция $W_{58,2}$ за 80 двойки (β, γ). Получен е за първи път самодуален $[58, 29, 10]$ код с тегловна функция $W_{58,2}$ за $\beta = 0$, $\gamma = 132$.
III. Използван е метод за конструиране на самодуални съседи. Резултатите за получените кодове са следните:

- Намерени са 67 екстремални четири циркулантни едночетни самодуални $[64, 32, 12]$ кодове с тегловна функция $W_{64,2}$.

- Конструирани са нови екстремални едночетни самодуални $[64, 32, 12]$ кодове като самодуални съседи на екстремални четири циркулантни едночетни самодуални кодове. Стойностите на параметъра $\beta = 35$ в $W_{64,1}$ и $\beta = 19, 34, 42, 45$ и 50 в $W_{64,2}$ са нови.

- Доказано е, че съществуват поне 44 нееквивалентни екстремални двойночетни самодуални $[64, 32, 12]$ кодове с радиус на покритие 12, достигащи границата на Delsarte.

- Получени са 224 нееквивалентни четири циркулантни едночетни самодуални $[64, 32, 10]$ кодове. Не съществува екстремален едночетен самодуален $[64, 32, 12]$ съсед на $E_{64,i}$ за $i = 1, 2, \ldots, 224$.

IV. Приложен е метод за конструиране на нови едночетни самодуални кодове чрез разширяване на дължината им с 2.

- Конструирани са нови екстремални едночетни самодуални $[66, 33, 12]$ кодове с $W_{66,1}$ за $\beta \in \{7, 58, 70, 91, 93\}$ и тегловна функция $W_{66,3}$ за $\beta \in \{22, 23\}$.

V. Направен е преглед на известните до момента тегловни функции на оптималните двоични самодуални кодове с дължини $58 \leq n \leq 64$ и $78 \leq n \leq 84$ или на кодове, които не са оптимални, но имат най-голямото минимално тегло, известно до момента, за съответната дължина. Разгледани са също известните тегловни функции на екстремалните едночетни самодуални кодове с дължини 64 и 66. Направен е обзор на стойностите на параметрите известни до момента и на намерените от нас нови стойности.

Литература

[1] C. Aguilar Melchor and P. Gaborit, "On the Classification of Extremal [36,18,8] Binary Self-Dual Codes," *IEEE Transactions on Information Theory*, vol. 54, no. 10, pp. 4743–4750, 2008.

[2] D. Anev, M. Harada, and N. Yankov, "New extremal singly even self-dual codes of lengths 64 and 66," *Journal of Algebra Combinatorics Discrete Structures and Applications (JACODESMATH)*, vol. 5, no. 3, pp. 143–151, 2018.

[3] K. Betsumiya, S. Georgiou, T. Gulliver, M. Harada, and C. Koukouvinos, "On self-dual codes over some prime fields," *Discrete Mathematics*, vol. 262, no. 1-3, pp. 37–58, 2003.

[4] R. Bilous, "Enumeration of the binary self-dual codes of length 34," *Journal of Combinatorial Mathematics and Combinatorial Computing*, vol. 59, pp. 173–211, 2006.

[5] R. Bilous and G. V. Rees, "An enumeration of binary self-dual codes of length 32," *Designs, Codes and Cryptography*, vol. 26, pp. 61–86, 2002.

[6] I. Bouyukliev, *About the code equivalence in Advances in Coding Theory and Cryptography vol. 3.* World Scientific Publishing Company, 2007, pp. 126–151.

[7] I. Bouyukliev, M. Dzhumalieva-Stoeva, and V. Monev, "Classification of Binary Self-Dual Codes of Length 40," *IEEE Transactions on Information Theory*, vol. 61, pp. 4253–4258, 2015.

[8] S. Bouyuklieva and I. Bouyukliev, "An Algorithm for Classification of Binary Self-Dual Codes," *IEEE Transactions on Information Theory*, vol. 58, no. 6, pp. 3933–3940, 2012.

[9] R. Brualdi and V. Pless, "Weight enumerators of self-dual codes," *IEEE Transactions on Information Theory*, vol. 37, no. 4, pp.

1222–1225, 1991.

[10] N. Chigira, M. Harada, and M. Kitazume, "Extremal self-dual codes of length 64 through neighbors and covering radii," *Designs, Codes and Cryptography*, vol. 42, no. 1, pp. 93–101, 2007.

[11] J. Conway, V. Pless, and N. J. A. Sloane, "The binary self-dual codes of length up to 32: A revised enumeration," *Journal of Combinatorial Theory, Series A*, vol. 60, no. 2, pp. 183–195, 1992.

[12] J. Conway and N. J. A. Sloane, "A new upper bound on the minimal distance of self-dual codes," *IEEE Transactions on Information Theory*, vol. 36, no. 6, pp. 1319–1333, 1990.

[13] P. Delsarte, "Four fundamental parameters of a code and their combinatorial significance," *Information and Control*, vol. 23, no. 5, pp. 407–438, 1973.

[14] R. Dontcheva and M. Harada, "New extremal self-dual codes of length 62 and related extremal self-dual codes," *IEEE Transactions on Information Theory*, vol. 48, no. 7, pp. 2060–2064, 2002.

[15] R. Dontcheva and M. Harada, "Extremal doubly-even [80,40,16] codes with an automorphism of order 19," *Finite Fields and Their Applications*, vol. 9, no. 2, pp. 157–167, 2003.

[16] S. Dougherty, T. A. Gulliver, and M. Harada, "Extremal binary self-dual codes," *IEEE Transactions on Information Theory*, vol. 43, no. 6, pp. 2036–2047, 1997.

[17] P. Gaborit and A. Otmani, "Experimental constructions of self-dual codes," *Finite Fields and Their Applications*, vol. 9, no. 3, pp. 372–394, 2003.

[18] T. A. Gulliver and M. Harada, "Classification of extremal double circulant self-dual codes of lengths 74–88," *Discrete Mathematics*, vol. 306, no. 17, pp. 2064–2072, 2006.

[19] M. Harada, "Binary extremal self-dual codes of length 60 and related codes," *Designs, Codes and Cryptography*, vol. 86, no. 5, pp. 1085–1094, 2018.

[20] M. Harada and A. Munemasa, "Some restrictions on weight enumerators of singly even self-dual codes," *IEEE Transactions on Information Theory*, vol. 52, no. 3, pp. 1266–1269, 2006.

[21] M. Harada and A. Munemasa, "Classification of self-dual codes of length 36," *Advances in Mathematics of Communications*, vol. 6,

no. 2, pp. 229–235, 2012.

[22] M. Harada and A. Munemasa, "On s-extremal singly even self-dual $[24k + 8, 12k + 4, 4k + 2]$ codes," *Finite Fields and Their Applications*, vol. 48, pp. 306–317, 2017.

[23] W. C. Huffman, "Automorphisms of codes with applications to extremal doubly even codes of length 48," *IEEE Transactions on Information Theory*, vol. 28, no. 3, pp. 511–521, 1982.

[24] W. C. Huffman and V. S. Pless, *Fundamentals of Error-Correcting Codes*. Cambridge University Press, 2003.

[25] W. Huffman, "On the classification and enumeration of self-dual codes," *Finite Fields and Their Applications*, vol. 11, no. 3, pp. 451–490, 2005.

[26] S. Kapralov, R. Russeva, and V. Radeva, "New extremal doubly even $[80, 40, 16]$ codes with an automorphism of order 13," in *Proceedings of Eighth International Workshop on Algebraic and Combinatorial Coding Theory*, 2002, pp. 139–142.

[27] A. Kaya, B. Yildiz, and A. Pasa, "New extremal binary self-dual codes from a modified four circulant construction," *Discrete Mathematics*, vol. 339, no. 3, pp. 1086–1094, 2016.

[28] V. Pless, "A classification of self-orthogonal codes over $GF(2)$," *Discrete Mathematics*, vol. 3, no. 1-3, pp. 209–246, 1972.

[29] E. Rains, "Shadow bounds for self-dual codes," *IEEE Transactions on Information Theory*, vol. 44, no. 1, pp. 134–139, 1998.

[30] C. Shannon, "A mathematical theory of communication," *Bell System Tech. J.*, vol. 27, pp. 379–423, 1948.

[31] H. P. Tsai, "Existence of certain extremal self-dual codes," *IEEE Transactions on Information Theory*, vol. 38, no. 2, pp. 501–504, 1992.

[32] H. C. A. van Tilborg, "Uniformly packed codes," Ph.D. dissertation, Technische Hogeschool Eindhoven, 1976.

[33] N. Yankov, "New optimal $[52, 26, 10]$ self-dual codes," *Designs, Codes and Cryptography*, vol. 69, no. 2, pp. 151–159, 2013.

[34] N. Yankov, D. Anev, and M. Gürel, "Constructing the self-dual codes with an automorphism of order 13 with 6 cycles," *Advances in Mathematics of Communications*, vol. 11, no. 3, pp. 635–645, 2017.

[35] N. Yankov and D. Anev, "New self-dual [78, 39, 14] codes with an automorphism of order 13," in *Proceedings of Eighth*

International Workshop on Optimal Codes and Related Topics (OC2017), 2017, pp. 128–133.

[36] N. Yankov, D. Anev, and M. H. Lee, "On the even subcode of codes with an automorphism of order 5 with 12 cycles," in *Proceedings of the XXIII-th International Workshop on Multimedia Signal Processing and Transmission (MSPT)*, 2017, p. 6.

[37] N. Yankov and M. H. Lee, "New binary self-dual codes of lengths $50 - 60$," *Designs, Codes and Cryptography*, vol. 73, no. 3, pp. 983–996, 2014.

[38] N. Yankov and M. H. Lee, "Classification of self-dual codes of length 50 with an automorphism of odd prime order," *Designs, Codes and Cryptography*, vol. 74, no. 3, pp. 571–579, 2015.

[39] N. Yankov and R. Russeva, "Binary Self-Dual Codes of Lengths 52 to 60 With an Automorphism of Order 7 or 13," *IEEE Transactions on Information Theory*, vol. 57, no. 11, pp. 7498–7506, 2011.

[40] V. Yorgov, "Binary Self-Dual Codes with Automorphisms of Odd Order," *Problems of information transmission*, vol. 19, no. 4, pp. 260–270, 1983.

[41] V. Yorgov, "A method for constructing inequivalent self-dual codes with applications to length 56," *IEEE Transactions on Information Theory*, vol. 33, no. 1, pp. 77–82, 1987.

Благодарности

Бих искал да изразя искрената си благодарност към моя научен ръководител проф. дмн Николай Янков за непрестанната подкрепа през целия период на научната ми работа и разработването на настоящото изследване, за търпението му, мотивацията и готовността да предаде огромните си познания.

Благодаря на проф. д-р Никола Зяпков, който ме въведе в дисциплината „Алгебра и теория на числата", което впоследствие доведе до интереса ми към научна работа.

Благодарен съм на доц. д-р Радка Русева за ценните съвети и ползотворната съвместна дейност.

Изказвам благодарност и на колегите от катедра „Алгебра и геометрия" към Факултета по Математика и информатика на Шуменски университет за приятната творческа атмосфера.

Не на последно място сърдечно благодаря на моето семейство, чиято подкрепа, разбиране и съпричастност ми дава увереност във всяко мое начинание.