СПЕЦИАЛИЗИРАН НАУЧЕН СЪВЕТ ПО
ИНФОРМАТИКА И ПРИЛОЖНА МАТЕМАТИКА
ПРИ ВАК

Радка Пенева Русева

ЕКСТРЕМАЛНИ САМОДУАЛНИ КОДОВЕ НАД GF(2) И GF(4)

АВТОРЕФЕРАТ

НА

ДИСЕРТАЦИЯ

за присъждане на научната и образователна степен

"доктор"

Научна специалност 01.01.12

НАУЧЕН КОНСУЛТАНТ: доц.д-р Васил Йоргов

РЕЦЕНЗЕНТИ: ст.н.с.I ст. дмн Веселин Дренски

доц. д-р Никола Зяпков

София, 2000

Дисертацията съдържа 73 страници, от които 65 основен текст и 6 страници литература на кирилица и латиница със 79 заглавия. Публикации по дисертацията - 8 бр.

Дисертационният труд е обсъден и насочен за защита на заседание на Националния семинар по Теория на кодирането, проведено на 11.12.1999г.

Докторантът работи като главен асистент в катедра "Алгебра и геометрия", ФМИИ на Шуменския Университет "Еп. Константин Преславски".

Защитата на дисертацията ще се състои на заседание на СНС по информатика и приложна математика при ВАК на 26.06.2000г. от 14.30 часа в Заседателната зала на Института по математика и информатика при БАН. Материалите по защитата са на разположение на интересуващите се в библиотеката на ИМИ – БАН.

Автор: Радка Пенева Русева

Заглавие: Екстремални самодуални кодове над GF(2) и GF(4).

Теорията на кодирането се занимава със създаване на ефективни методи за бързо, удобно и защитено от странични шумове предаване на съобщения. Теоретичните основи на тази наука се поставят в средата на нашия век от Клод Шенон. Съвременната теория на кодирането е дисциплина с прецизен апарат, който използва методи от различни области на математиката - алгебра, геометрия, теория на вероятностите, комбинаторика и др.

Нека F_q^n е n-мерното векторно пространство над крайно поле $F_q = GF(q)$ с характеристика p. Всяко непразно подмножество на F_q^n се нарича код с дължина n и елементи - кодови думи. Броя на ненулевите координати на вектор $v \in F_q^n$ наричаме тегло (на Хеминг) за този вектор и бележим с $wt(v)$.

Казваме, че C е $[n, k, d]$ код над полето F_q, ако C е линейно подпространство на F_q^n, с размерност k, и d е минималното измежду теглата на ненулевите кодови думи. Броя на векторите с тегло i от кода бележим с $A_i, i = 0, 1, \ldots, n$. Полинома

$$W(y) = A_0 + A_1 y + A_2 y^2 + \cdots + A_n y^n$$

наричаме тегловна функция на кода.

Нека M_n е групата на всички мономиални матрици от ред n над F_q. С $Gal(F_q)$ означаваме групата на Галоа за F_q над простото му подполе F_p, съдържаща всички автоморфизми на полето, които фиксират елементите от F_p. Нека M_n^* е полудиректното произведение на M_n, разширена чрез $Gal(F_q)$. Тогава всеки елемент $T \in M_n^*$ може да се представи във вида $T = PD\nu$, където P е пермутационна матрица, D е диагонална матрица с ненулеви диагонални елементи, а $\nu \in Gal(F_q)$. Когато действаме с елемент $T = PD\nu \in M_n^*$ върху произволен вектор $v \in F_q^n$, първо разместваме координатите му с пермутацията P, след това умножаваме полученият вектор с D и накрая прилагаме автоморфизма ν върху всяка координата от получения резултат.

Два линейни кода C и C' над полето F_q се наричат еквивалентни, ако единия код може да се получи от другия след прилагането на елемент $T \in M_n^*$. Групата от автоморфизми $Aut(C)$ на кода C съдържа множеството от онези елементи от M_n^*, които изобразяват всяка кодова дума на C в кодова дума на същия код. Можем да разглеждаме и подгрупите на пермутационните и мономиалните автоморфизми на кода.

Код, който съвпада с ортогоналното си допълнение при въведено скаларно произведение във векторното пространство F_q^n, ще наричаме самодуален. Всеки самодуален код над полето F_q е с четна дължина n и има размерност $\frac{n}{2}$.

Самодуалните кодове предизвикват интерес, тъй като много от най-добрите известни кодове са от този вид и те са широко изс-

ледвани. Има съществена връзка между самодуалните кодове и някои видове дизайни, графи, решетки, адамарови матрици и други комбинаторни структури [4], [5]. Голям принос за развитието на тази област от теорията на кодирането имат Вера Плес, Мак Уилямс, Слоен, Конуей, Хафмън, Тончев, Йоргов и др. Най-пълна и актуална информация за изследванията до момента върху самодуалните кодове може да се намери в [49].

В дисертацията се изследват самодуални кодове над полето F_2 относно скаларно произведение

$$(u,v) = \sum_{i=1}^{n} u_i v_i \quad u,v \in F_2^n$$

и самодуални кодове над $F_4 = \{0,1,\omega,\bar{\omega}\}$, $\bar{\omega} = \omega + 1$ относно скаларно произведение

$$(u,v) = \sum_{i=1}^{n} u_i v_i^2 = \sum_{i=1}^{n} u_i \bar{v}_i \quad u,v \in F_4^n.$$

В тези случаи кодовете съдържат само четно тегловни вектори. Оказва се, че броят на самодуалните кодове расте бързо с нарастването на дължината им. Затова интерес представляват предимно екстремалните самодуални кодове, т.е. кодовете с най-голямо възможно минимално тегло измежду кодовете с дадена дължина.

Най-пълно изследвани и класифицирани са двоичните кодове. Построени са всички неекивалентни самодуални кодове с дължина до 32 [17],[21],[44],[46],[58]. Двоичните самодуални кодове се разделят на два основни типа - двойночетни, в които теглата на всички кодови вектори са кратни на 4 (с дължина кратна на 8), и едночетни, в противен случай.

Нова горна граница за минималното тегло на двоичните самодуални кодове дават Конуей и Слоен в работата си от 1990 година [22]. Известен е списък на всички възможни тегловни функции на екстремалните самодуални кодове с дължина до 100 [22], [23]. Изследванията са насочени в две посоки: 1) попълване на празните места в таблицата на кодовете, реализиращи всяка една от посочените тегловни функции и 2) пълна класификация на екстремалните самодуални кодове с фиксирана дължина.

Разработени са различни методи за конструиране на двоични самодуални кодове. Нови кодове са получени от симетрични дизайни [50], [51] и от Адамарови матрици [10],[11],[28],[42]. Много двойноциркулантни кодове се оказват самодуални [55]. По метода на пълното изчерпване Гъливер, Харада и Кимура намират всички неекивалентни двойноциркулантни екстремални самодуални кодове с дължина, ненадминаваща 72 [25],[26]. Бруалди, Плес и Тцаи

построяват нови едночетни екстремални кодове, използвайки вече известни самодуални кодове със същата или близка дължина [9],[53],[54]. Буюклиева разработи нов метод за конструиране на двоични самодуални кодове, притежаващи автоморфизъм от ред 2, чрез използване на самоортогонални и квазициклични кодове с по-малка дължина [13],[14],[15].

Метод за конструиране на двоични самодуални кодове чрез използване на автоморфизъм от нечетен прост ред е предложен от Хафмън [31], Конуей и Плес [18],[45] и доразвит от Йоргов [1],[57]. За пръв път тази идея е използвана в работата [6] за търсене на проективна равнина от ред 10. Методът дава възможност за пълна характеризация на самодуалните кодове, притежаващи автоморфизъм от нечетен прост ред p. По този начин са намерени всички неекивалентни двойночетни и едночетни кодове с автоморфизъм от ред $p \geq 5$ с параметри [40,20,8] [1],[16],[62]. Хафмън доказва, че всеки екстремален двойночетен код с дължина 48, притежаващ нетривиален автоморфизъм от нечетен ред, е еквивалентен на разширения квадратично-остатъчен код q_{48} [31]. Чрез автоморфизми от нечетен прост ред са класифицирани някои класове екстремални двойночетни кодове за дължини 56 и 64. [2],[57] и екстремални кодове с дължини 52, 44, 42, 38, 36, 34 [39],[48],[60],[61],[64]. Намерени са и много нови екстремални самодуални кодове с дължини 40, 42, 44, 52, 54, 58 [12],[52],[53],[59] и др. Все още остава открит въпросът за съществуването на двойночетни $[72, 36, 16]$ и едночетни $[72, 36, 14]$ кодове, но е доказано, че ако съществуват самодуални кодове с тези параметри, те нямат автоморфизми от прост ред, поголям от 7 [40],[63].

Известна е пълна класификация за самодуалните кодове над F_4 с дължина, ненадминаваща 16 [20],[56]. За по-големи дължини n се изследват само екстремалните кодове, за които минималното разстояние удовлетворява равенството $d = 2[n/6] + 2$. Хафмън доказва, че съществуват: единствен [18,9,8] самодуален код и точно два [20,10,8] самодуални кода с точност до еквивалентност[38]. Екстремални самодуални кодове съществуват и за дължини 22, 28 и 30 [56],[36], но Лем и Плес в [41] доказват, че не съществува самодуален [24,12,10] код над F_4. Самодуални кодове над полето F_4 могат да се получат отново чрез използване на автоморфизми. Класифицирани са евентуалните екстремални самодуални кодове за дължини от 18 до 28, притежаващи мономиален автоморфизъм от прост ред $r \geq 3$ или 9 [33],[35],[36],[37]. Не са намерени до сега екстремални кодове над F_4 за $n = 26, 32, \ldots$.

Хафмън предлага обща теория за конструиране на самодуални кодове над крайно поле F_q с пермутационен автоморфизъм от ред взаимно прост с характеристиката на полето (тя обобщава резултатите за конструиране на нееквивалентни самодуални двоични кодове, притежаващи автоморфизъм от нечетен прост ред) и метод за конструиране на самодуални кодове над F_4 с мономиален автоморфизъм от ред степен на 3 [34],[35],[36] и [37]. Общото при тях е, че всеки код, за който са приложими, се разлага в директна сума на подкодове, които свеждаме до кодове с по-малка дължина над разширения на основното поле с интересни свойства. Проблемите при реализирането на тези методи възникват при избора на подходящи пораждащи матрици за съкратените кодове, с точност до еквивалентност. Използваме необходими и достатъчни условия за еквивалентност на конструираните чрез автоморфизми кодове и специфичните свойства на съкратените кодове във всеки отделен случай.

В този дисертационен труд са получени и класифицирани нови екстремални двоични самодуални кодове с дължини 36, 38, 42 и 44. Конструирани са всички нееквивалентни самодуалени [24,12,8] кодове над F_4, притежаващи мономиален автоморфизъм от прост ред $r \geq 3$. Изследването на самодуални кодове с тези параметри е интересно, понеже те имат най-голямо възможно минимално тегло за тази дължина, не бяха класифицирани до сега и са тясно свързани с хипотетичния двойночетен $[72, 36, 16]$ двоичен код. Използвани са методите за конструиране на самодуални кодове над крайно поле, притежаващи автоморфизъм от нечетен ред.

Дисертацията се състои от увод и три глави.

Глава 1 е помощна и в нея са изложени известни необходими сведения от алгебричната теория на кодирането. Използваните означения са аналогични на тези от [3],[43]. Особено полезна се оказва следната лема:

Лема 1.1.2. *Нека C е линеен код над F_q с дължина n, притежаващ мономиален автоморфизъм $M = PD$ от прост ред r, където r не дели $q-1$. Тогава C е еквивалентен на код C' с пермутационен автоморфизъм P.*

В частния случай за линейни кодове над F_4 тази лема е доказана в [19].

В част 1.2. са представени основните дефиниции и твърдения, отнасящи се до самодуалните кодове.

Нека C е линеен $[n, k]$ код, над полето F_q с характеристика p и r е положително цяло число, взаимно просто с p. Предполагаме,

че C притежава пермутационен автоморфизъм σ от ред r, който се представя като произведение на c независими r-цикъла и оставя неподвижни $f = n - cp$ точки. В такъв случай казваме, че σ е от тип $r(c, f)$. С точност до еквивалентност можем да считаме, че

$$\sigma = (1, 2, \ldots, r)(r+1, r+2, \ldots, 2r)\ldots((c-1)r+1, \ldots, cr)$$

Общият метод за конструиране на самодуални кодове над крайно поле с пермутационен автоморфизъм σ е подробно описан в част 1.3. и 1.4. Доказани са основните твърдения, върху които се гради тази теория и е изследвано приложението ѝ върху кодове над F_2 и F_4. Тя е приложима за самодуални кодове над F_2, притежаващи автоморфизъм от нечетен прост ред и съгласно Лема 1.1.2., за самодуални кодове над F_4 с мономиален автоморфизъм от прост ред $r \geq 5$.

Във втора глава конструираме нови екстремални двоични самодуални кодове чрез метода, описан в Глава 1.

В част 2.2. изследваме самодуални [36,18,8] екстремални кодове. Съществуват две възможности за тегловната им функция [22]:

(3) $$W(y) = 1 + 225y^8 + 2016y^{10} + 9555y^{12} + 28800y^{14} + \ldots$$

(4) $$W(y) = 1 + 289y^8 + 1632y^{10} + 10387y^{12} + 28288y^{14} + \ldots$$

Преди нашата разработка бяха известни само два самодуални кода с тези параметри: код $R2$ с тегловна функция от вида (3) (неговата структура не е описана подробно) и двойно циркулантния код $D3$ с тегловна функция от втория вид, представени от Конуей и Слоен в [22]. Ние доказваме твърденията:

Теорема 2.2.1. *Нека C е самодуален* $[36, 18, 8]$ *код с автоморфизъм от нечетен прост ред r и тип (c, f). Тогава единствените възможности за $r(c, f)$ са следните: 17(2, 2), 7(5, 1), 5(6, 6), 3(12, 0), 3(10, 6) , 3(8, 12) и 3(6, 18).*

Изследваме случаите за $r = 17$ и $r = 7$ и получаваме.

Теорема 2.2.3. *Съществува единствен самодуален* $[36, 18, 8]$ *двоичен код с автоморфизъм от ред 17.*

Следствие 2.2.4. *Двойноциркулантният код $D3$ е единствен с точност до еквивалентност самодуален* $[36, 18, 8]$ *код, притежаващ автоморфизъм от ред 17.*

Теорема 2.2.5. *Съществуват точно 3 неекивалентни самодуални [36,18,8] кода, притежаващи автоморфизъм от ред 7.*

Конструираните от нас кодове с автоморфизъм от ред 7 са с тегловна функция от вида (4). Доказваме, че те са неекивалентни на кода $R2$ и следователно са нови кодове.

По-късно, случаят $r = 5$ е изчерпан от Йоргов и Янков в [64]. Самодуални [36,18,8] кодове, притежаващи автоморфизъм от ред

3, са конструирани от Йоргов, Зяпков и Радева в [48].

В част 2.3. се изследват самодуални [38,19,8] двоични кодове. Съществуват две възможности за тегловната им функция [22]:

(5) $$W(y) = 1 + 171y^8 + 1862y^{10} + 10374y^{12} + \dots$$

(6) $$W(y) = 1 + 203y^8 + 1702y^{10} + 10598y^{12} + \dots$$

Известни са ни три самодуални кода с тези параметри. Конуей и Слоен в [22] представят два кода с тегловна функция от вида (5): двойно циркулантния код $D4$ и код $R3$ (неговата структура не е описана подробно). Харада и Кимура в [29] намират код с тегловна функция (6), като използват цикличен 2-(19,9,4) дизайн.

Ние доказваме, че нечетните прости делители на реда на групата от автоморфизми за самодуалните [38,19,8] кодове са числата 19, 7, 5 и 3 (Теорема 2.3.1). Конструираме, с точност до еквивалентност, всички кодове с автоморфизъм от ред 7.

Теорема 2.3.2. *Съществуват точно 7 самодуални [38,19,8] двоични кода с автоморфизъм от ред 7.*

Единият от конструираните кодове е с тегловна функция от вида (5), неекивалентен на $D4$ и $R3$ и шест кода с тегловна функция от вида (6). Така поне 6 от конструираните от нас кодове са нови.

Има два типа тегловна функция за самодуалните екстремални кодове с дължина 42 [22]:

(7) $W(y) = 1 + (84 + 8\beta)y^8 + (1449 - 24\beta)y^{10} + (10640 - 16\beta)y^{12} + \dots$ или $W(y) = 1 + 164y^8 + 697y^{10} + 15088y^{12} + \dots$.

За самодуалните $[44, 22, 8]$ кодове имаме следните възможности:

$W(y) = 1 + (44 + 4\beta)y^8 + (976 - 8\beta)y^{10} + (12289 - 20\beta)y^{12} + \dots$ или

(8) $W(y) = 1 + (44 + 4\beta)y^8 + (1232 - 8\beta)y^{10} + (10241 - 20\beta)y^{12} + \dots$

Първите известни екстремални кодове с тези параметри са посочени в [22]. Там са представени самодуални $[42, 21, 8]$ кодове с тегловна функция (7) с $\beta = 0, 1, \dots, 7$ и самодуални $[44, 22, 8]$ кодове с тегловна функция от първия вид за $\beta = 14, 17$ и от втория вид (8) за $\beta = 4, 5, \dots, 15$. Самодуални $[42, 21, 8]$ кодове с тегловна функция от втория вид са конструирани от Тцаи [53], Спенс и Тончев [50].

В част 2.4. изследваме самодуални [42,21,8] и [44,22,8] кодове, притежаващи автоморфизъм от нечетен прост ред. Доказваме твърденията:

Теорема 2.4.1. *Нека C е двоичен самодуален $[42, 21, 8]$ код с автоморфизъм от нечетен прост ред r и тип (c, f). Единствените възможности за $r(c, f)$ са следните: 7(3, 21), 7(6, 0), 5(4, 22), 5(8, 2), 3(6, 24), 3(8, 18), 3(10, 12), 3(12, 6) и 3(14, 0).*

Теорема 2.4.4. *Нека C е двоичен самодуален $[44, 22, 8]$ код с автоморфизъм от нечетен прост ред r и тип (c, f). Единствените възможности за $r(c, f)$ са следните: 11(2, 22), 11(4, 0), 5(4, 24), 3(6, 26), 3(8, 20), 3(10, 14), 3(12, 8) и 3(14, 2).*

Конструираме самодуален $[42, 21, 8]$ код с автоморфизъм от тип 7(3, 21) и самодуален $[44, 22, 8]$ код с автоморфизъм от тип 11(2, 22). Тези кодове са тясно свързани с разширения код на Голей g_{24}, описан в Глава 1. Те са първите известни екстремални кодове с дължини 42 и 44 с тегловни функции от вида (7) за $\beta = 42$ и (8) за $\beta = 154$ съответно. Построяването на екстремални кодове с дължини 42 и 44 с възможните тегловни функции за нови стойности на параметрите представлява интерес и за други автори [9],[12],[24],[26],[27],[29],[59] и др.
При получаване на резултатите от части 2.2 и 2.4 сме използвали и програмната система GFQ за пресмятания над крайно поле [7].

В глава 3 разглеждаме самодуални [24,12,8] кодове над поле с четири елемента. Известно ни е съществуването на два самодуални кода с такива параметри: разширението над F_4 на кода g_{24} и неекивалентен на него код, с пермутационен автоморфизъм от ред 7, построен от Конуей и Плес в [19].

Намираме тегловната функция на самодуален [24,12,8] код. Тя има вида:

$$W(y) = 1 + \alpha y^8 + (18216 - 8\alpha)y^{10} + +(156492 + 28\alpha)y^{12} +$$
$$(1147608 - 56\alpha)y^{14} + (3736557 + 70\alpha)y^{16} + (6248088 - 56\alpha)y^{18} + \quad (9)$$
$$(4399164 + 28\alpha)y^{20} + (1038312 - 8\alpha)y^{22} + (32778 + \alpha)y^{24},$$

където $\alpha = A_8$ е параметър. В част 3.1. са класифицирани всички кодове с мономиален автоморфизъм от прост ред $r \geq 5$. Възможностите за r - 23, 11, 7 и 5 и цикличната структура на автоморфизмите са определени в Теорема 3.1.2. Изследваме всички случаи. Доказваме, че с точност до еквивалентност съществуват:

единствен самодуален [24,12,8] код с автоморфизъм от ред 23, който е еквивалентен на разширението над F_4 на кода g_{24} и притежава също автоморфизми от редове 11, 7 и 5,

точно 2 кода с автоморфизъм от ред 11,

точно 6 кода с автоморфизъм от ред 7,

и точно 12 кода с автоморфизъм от ред 5.

Получените самодуални кодове имат 12 различни тегловни функции за 12 стойности на $\alpha = 513, 522, 630, 657, 702, 756, 792, 837, 1089, 1197, 1242, 2277$. Тези резултати са съвместни с В. Йоргов [70],[73].

В част 3.2.1. е разяснен методът за конструиране на самодуални кодове над F_4 с дължина n, притежаващи мономиален автоморфизъм $M = PD$, където за неотрицателни цели числа c, f_0, f_1, f_2, удовлетворяващи равенството $n = 3c + f_0 + f_1 + f_2$,
$P = (1,2,3)\ldots(3c-2, 3c-1, 3c)$ и

$$D = diag(d_1, \ldots, d_n) \text{ за } d_i = \begin{cases} 1 & \text{при } 0 \leq i \leq 3c + f_0 \\ \omega & \text{при } 3c + f_0 + 1 \leq i \leq 3c + f_1 \\ \bar{\omega} & \text{при } 3c + f_1 + 1 \leq i \leq 3c + f_2 \end{cases}$$

M наричаме автоморфизъм от I тип.

В Лема 3.2.2. доказваме, че всеки самодуален [24,12,8] код с мономиален автоморфизъм от ред 3 е еквивалентен на код с автоморфизъм от I тип и можем да използваме метода от част 3.2.

В част 3.3. класифицираме самодуалните [24,12,8] кодове, притежаващи нетривиален автоморфизъм от ред 3. Намираме структурата на техните автоморфизми.

Теорема 3.3.1. *Нека C е самодуален [24,12,8] код над F_4 с с автоморфизъм M от* I *тип. В сила е една от следните възможности: 1) $c = 6, f_0 = 6, f_1 = f_2 = 0$; 2) $c = 6, f_0 = 4, f_1 = 2, f_2 = 0$; 3) $c = 6, f_0 = f_1 = f_2 = 2$; 4) $c = 7, f_0 = f_1 = f_2 = 1$; 5) $c = 8, f_0 = f_1 = f_2 = 0$.*

Изследвани са всички възможности за M. В част 3.3.1. са получени, с точност до еквивалентност, всички самодуални [24,12,8] кодове, притежаващи пермутационен автоморфизъм от ред 3.

Теорема 3.3.8. *Съществуват точно 52 неекивалентни самодуални [24,12,8] кода над F_4, притежаващи пермутационен автоморфизъм от ред 3.*

В част 3.3.2. са конструирани кодовете с непермутационен автоморфизъм от ред 3, с точност до еквивалентност. Доказваме, че:

не съществува самодуален [24,12,8] код над F_4 с автоморфизъм от I Тип със $c = 7$, $f_0 = f_1 = f_2 = 1$.

съществува единствен самодуален [24,12,8] код над F_4 с автоморфизъм от I Тип със $c = 6$, $f_0 = f_1 = f_2 = 2$.

съществуват точно 153 самодуални [24,12,8] кода над F_4 с автоморфизъм от I Тип , за $c = 6, f_0 = 4, f_1 = 2, f_2 = 0$.

Установяваме, че само един от кодовете построени в част 3.3.2. притежава и пермутационен автоморфизъм от ред 3. В част 3.3. получаваме кодове с тегловна функция за 9 нови стойности на $\alpha =$ 594, 684, 738, 765, 846, 900, 954, 981 и 1413. За резултатите от тази част сме използвали и системата за компютърна алгебра GAP.

Резултатите, включени в дисертацията, са публикувани или представени за публикуване в [66], [67], [68], [69], [70], [71], [72], [73]. Докладвани са на ежегодните сбирки на Националния семинар по

кодиране към секция МОИ на ИМИ - БАН; на Международните семинари по Алгебрична и комбинаторна теория на кодирането, В. Вода 1992, Созопол 1996г.; на Международния семинар "Optimal Codes and Related Topics" Созопол през 1995, на Пролетните конференции на СМБ 1996, 1998 и 1999 г. и на Международния семинар по компютърна алгебра с приложение в кодирането и криптографията, София 1999.

Накрая бих искала да благодаря на всички, които ми помагаха по време на подготовката на тази дисертация.

Считам за свой приятен дълг да изразя дълбоката си признателност към моя научен консултант доц. д-р Васил Йоргов, който насочи интересите ми към алгебричната теория на кодирането, за всестранната помощ, интерес и внимание към моята работа. Благодаря на проф. дмн Стефан Додунеков за моралната подкрепа и предоставените възможности за изява. Използвам случая да благодаря на д-р Стефка Буюклиева и на доц. д-р Стоян Капралов за отзивчивостта, помощта и ценните съвети. В заключение изказвам благодарност на колегите ми от катедра Алгебра и геометрия към Факултета по математика и информатика на Шуменския Университет и на всички участници в Семинара по кодиране за подкрепата и проявеното внимание към работата ми. Искам сърдечно да благодаря и на моето семейство за обичта и подкрепата им.

Литература

[1] В.Й.Йоргов, "Двоичные самодуальные коды с автоморфизмом нечетного порядка", Проблемы передачи информации, вып. **4** (1983), стр. 11-24.

[2] В.Й.Йоргов, "Дважды четные экстремальные коды длины 64", Проблемы передачи информации, вып. **4** (1986), стр. 35-42.

[3] Ф. Дж. Мак-Вильямс, Н.Дж.А. Слоэн, "Теория кодов, исправляющих ошибки", Москва, "Связь", 1979.

[4] Владимир Тончев, "Комбинаторни конфигурации. Дизайни, кодове, графи", София, изд. "Наука и изкуство" (1984).

[5] Владимир Тончев, "Комбинаторни структури и кодове", София, Университетско издателство "Климент Охридски" (1988).

[6] R.Anstee, M.Hall Jr. and J.G.Thompson, "Planes of order 10 do not have a collineation of order 5", J. Combin. Theory, ser. A, vol. **29** (1980) pp.39-58.

[7] Ts. Baicheva, G. Bogdanova, S. Ilieva and Sv. Topalova, Object-oriented C++ library for computations in and over finite fields of characteristic 2 , *Mathematics and Education in Mathematics* 23, Stara Zagora, April 1–4, pp. 227-230, 1994.

[8] I. Boukliev and St.Buyuklieva, "Some new extremal self-dual codes of lengths 44, 50, 54 and 58", IEEE Trans. Inform. Theory, vol. **44** (1998), 809-812.

[9] R.A.Brualdi and V.Pless, "Weight enumerators of self-dual codes", IEEE Trans. Inform. Theory, vol.**37** (1991) pp. 1222-1225.

[10] F.C.Bussemaker and V.D.Tonchev, "New extremal doubly-even codes of length 56 derived from Hadamard matrices of order 28", Discrete Math., vol.**76** (1989) pp. 45-49.

[11] F.C.Bussemaker and V.D.Tonchev, "Extremal doubly-even codes of length 40 derived from Hadamard matrices of order 20", Discrete Math., vol. **82** (1990) pp. 317-321.

[12] St.Buyuklieva, "New extremal self-dual codes of lengths 42 and 44", IEEE Trans. Inform. Theory, vol. **43** (1997), 1607-1612.

[13] St.Buyuklieva, "On the binary self-dual codes with an automorphism of order 2", Designs, Codes and Cryptography. vol. **12** (1997) 39-48.

[14] St.Buyuklieva, "A method for constructing self-dual codes with application to length 64", Proceedings of the International Workshop ACCT, Sozopol, Bulgaria (1996) pp. 81-85.

[15] St.Buyuklieva and I. Boukliev, "Extremal self-dual codes with an automorphism of order 2", IEEE Trans. Inform. Theory, vol. **44** (1998), 323-328.

[16] St.Buyuklieva and V.Yorgov, "Singly-even self-dual codes of length 40", Designs, Codes and Cryptography, vol.**9** (1996) pp. 131-141.

[17] J.H.Conway and V.Pless, "On the enumeration of self-dual codes", J. Combin. Theory, ser. A, vol. **28** (1980) pp. 26-53.

[18] J.H.Conway, V.Pless, "On primes dividing the group order of a doubly-even (72, 36, 16) code and the group order of a quaternary (24, 12, 10) code", Discrete Math., vol.**38**, pp. 143-156, 1982.

[19] J.H.Conway, V.Pless, "Monomials of orders 7 and 11 cannot be in the group of a [24, 12, 10] self-dual quaternary code", IEEE Trans. Info. Theory **IT-29** (1983), pp. 137-140.

[20] J.H.Conway, V.Pless and N.J.A.Sloane, "Self-dual codes over GF(3) and GF(4) of length not exceeding 16", IEEE Trans. Inform. Theory, vol. **25** (1979) pp.312-322.

[21] J.H.Conway, V.Pless and N.J.A.Sloane, "The binary self-dual codes of length up to 32: a revised enumeration", J. Combin. Theory, ser. A, vol. **60** (1992) pp.183-195.

[22] J.H.Conway and N.J.A.Sloane, "A new upper bound on the minimal distance of self-dual codes", IEEE Trans. Inform. Theory, vol. **36** (1991) pp. 1319-1333.

[23] S.T.Dougherty, T.A.Gulliver and M.Harada, "Extremal binary self-dual codes", IEEE Trans. Inform. Theory, vol. **43**, No. 6, (1997), 2036-2047.

[24] T.A.Gulliver and M.Harada, "Weight enumerators of double circulant codes and new extremal self-dual codes", Designs,Codes and Cryptography, vol. **11** (1997) pp. 141-151.

[25] T.A.Gulliver and M.Harada, "Classification of extremal double circulant self-dual codes of length 64 to 72", Designs,Codes and Cryptography, vol. **13** (1998) pp. 257-269.

[26] M.Harada,T.A.Gulliver and H.Kaneta, "Classification of extremal double circulant self-dual codes of length up to 62", preprint.

[27] M.Harada, "Existence of new extremal double-even codes and extremal singly-even codes", Designs,Codes and Cryptography, vol.**8** (1996) pp. 1-12.

[28] M.Harada and H.Kimura, "New extremal doubly-even [64,32,12] codes", Designs,Codes and Cryptography, vol.**6** (1995) pp.91-96.

[29] M.Harada and H.Kimura, "On extremal self-dual codes", Math. J. Okayama Univ. **37**. (1995), 1-14.

[30] M.Harada and V.D.Tonchev, "Singly-even self-dual codes and Hadamard matrices", Lecture Notes in Computer Science, vol. **948** (1995) pp. 279-284.

[31] W.C.Huffman, "Automorphisms of codes with application to extremal doubly-even codes of lenght 48", IEEE Trans. Inform. Theory, vol. **28** (1982) pp. 511-521.

[32] W.C.Huffman, "Decomposing and shortening codes using automorphisms", IEEE Trans. Inform. Theory, vol. **IT-32** (1986) pp. 833-836.

[33] W.C.Huffman, " On the [24,12,10] quaternary code and binary codes with an automorphism having two cycles", IEEE Trans. Inform. Theory, vol. **34** (1988) pp. 486-493.

[34] W.C.Huffman, "On the equivalence of codes and codes with an automorphism having two cycles", Discrete Math. vol.**83** (1990) 265-283.

[35] W.C.Huffman, "On extremal self-dual quaternary codes of length 18 to 28, I", IEEE Trans. Info. Theory **IT-36** (1990), 651-660.

[36] W.C.Huffman, "On 3-elements in Monomial Automorphism Groups of Quaternary Codes, and the group of a [24, 12, 10] Code ", IEEE Trans. Info. Theory **IT-36** (1990), 660-664.

[37] W.C.Huffman, "On extremal self-dual quaternary codes of length 18 to 28, II", IEEE Trans. Info.Theory **IT-37** (1991), 1206-1216.

[38] W.C.Huffman, "Characterisation of Quaternary Extremal Codes of Lengths 18 and 20", IEEE Trans. Info.Theory vol.**43** (1997), 1613-1616.

[39] W.C.Huffman and V.D.Tonchev, "The [52,26,10] binary self-dual codes with an automorphism of order 7", Proceedings of the International Workshop OCRT, Sozopol, Bulgaria (1998) pp. 127-136.

[40] W.C.Huffman and V.Y.Yorgov, "A [72,36,16] doubly-even code does not have an automorphism of order 11", IEEE Trans. Theory, vol.**33** (1987) pp. 749-752.

[41] C.W.H.Lam and V.Pless, "There is no [24,12,10] self-dual quaternary code", IEEE Trans.Inform.Theory vol.**36**, pp. 1153-1156, 1990.

[42] M.Ozeki, "Hadamard matrices and doubly even self-dual error-correcting codes", J. Combin. Theory, ser. A, vol.**44** (1987) pp. 274-287.

[43] V.Pless, "Introduction to the theory of error-correcting codes", John Wiley and sons: New York, 1989.

[44] V.Pless, "A classification of self-orthogonal codes over GF(2)", Discrete Math., vol. **3** (1972) pp. 209-246.

[45] V.Pless, "23 does not divide the order of the group of a (72,36,16) doubly-even code", IEEE Trans. Inform. Theory, vol. **28** (1982) pp. 113-117.

[46] V.Pless and N.J.A.Sloane, "On the classification and enumeration of self-dual codes", J. Combin. Theory, ser. A, vol. **18** (1975) pp. 313-335.

[47] V.Pless, V.Tonchev and J.Leon, "On the existence of a certain [64,32,12] extremal code", IEEE Trans. Inform. Theory, vol.**39** (1993) pp. 214-215.

[48] V.Radeva, V.Yorgov, N.Ziapkov, "Some new extremal binary codes of length 36", Proceedings of the International Workshop ACCT, Sozopol, Bulgaria (1996) pp. 245-251.

[49] E.M.Rains and N.J.A.Sloane,"Handbook of coding theory, Self-Dual Codes", Elsevier Science Publishers, Amsterdam: 1998.

[50] E.Spence and V.D.Tonchev, "Extremal self-dual codes from symmetric designs", Discrete Math., vol.**110** (1992) pp. 265-268.

[51] V.D.Tonchev, "Self-orthogonal designs and extremal doubly-even codes", J. Combin. Theory, Ser. A, vol. **52** (1989) pp. 197-205.

[52] V.Tonchev and V.Yorgov, "The existence of certain extremal [54,27,10] self-dual codes", Proceedings of the International Workshop ACCT, Sozopol, Bulgaria (1996) pp. 280-287.

[53] H.P.Tsai, "Existence of certain extremal self-dual codes," IEEE Trans. Inform. Theory vol.**38**, pp. 501-504, 1992.

[54] H.P.Tsai, "Existence of some extremal self-dual codes," IEEE Trans. Inform. Theory vol. **38**, pp. 1829-1833, 1992.

[55] M.Ventou and C.Rigoni, "Self-dual doubly circulant codes", Discrete Math., vol.**56** (1985) pp. 291-298.

[56] F.J.Mac Williams, A.M.Odlyzko, N.J.A.Sloane, and H.N.Ward, "Self-dual codes over GF(4)", Journ. Combin. Theory **A25** (1978), 288-318.

[57] V.Y.Yorgov, "A method for constructing inequivalent self-dual codes with applications to length 56", IEEE Trans. Inform. Theory, vol.**33** (1987) pp. 77-82.

[58] V.Y.Yorgov, "On the extremal binary codes of length 32", Proceedings of the Fourth Joint Swedish-Russian International Workshop on Information Theory, Sweden (1989) pp. 275-279.

[59] V.Y.Yorgov, "New extremal singly-even self-dual codes of length 44", Proceedings of the Sixth Joint Swedish-Russian International Workshop on Information Theory, Sweden, (1993), pp. 372-375.

[60] V.Y.Yorgov, "The extremal codes of length 42 with automorphism of order 7", Discrete Math. vol. **190** (1998), 201-213.

[61] V.Y.Yorgov, R.A.Dontcheva, "Binary self-dual [34,17,6] codes with automorphism of odd prime order greater than 3", Математика и математическо образование (1998).

[62] V.Y.Yorgov and N.P.Ziapkov, "Doubly-even self-dual [40,20,8] codes with an automorphism of odd order", (in Russian) Probl. Pered. Inform., vol. **32** (1996), pp. 41-46; English translation in Prob. Inform. Trans. **32** (1996), pp. 253-257.

[63] V.Y.Yorgov and N.P.Ziapkov, "On the group of a [72,36,14] self-dual code", Proceedings of the International Workshop OCRT, Sozopol, Bulgaria (1995), pp. 143-145.

[64] V.Y.Yorgov and N.Yankov, "On the extremal binary codes of lengths 36 and 38 with an automorphism of order 5", Proceedings of the International Workshop ACCT, Sozopol, Bulgaria (1996), pp. 307-312.

[65] http://www-gap.dcs.st-and.ac.uk

Публикации по дисертацията

[66] R.P.Russeva and V.Y.Yorgov, "Two extremal codes of length 42 and 44", (in Russian) Probl. Pered. Inform., vol. **29** (1993) pp. 99-103. English translation in Prob. Inform. Trans. **29** (1994), pp. 385-388.

[67] R.P.Russeva, "Uniqueness of the [36,18,8] double circulant code", Proceedings of the International Workshop on Optimal Codes and Related Topics, Sozopol, Bulgaria (1995) pp.126-129.

[68] R.P.Russeva, "On the extremal self-dual binary codes of length 38 with an automorphism of order 7", Proceedings of the Fifth International Workshop on Algebraic and Combinatorial Coding Theory, Sozopol, Bulgaria (1996), pp. 239-244.

[69] Р.П.Русева, "Нови екстремални самодуални кодове с дължина 36", Математика и математическо образование,(1996), стр.150-153.

[70] V.Y.Yorgov and R.P.Russeva, "On the [24,12,8] quaternary self-dual codes", Mathematics and Education in Mathematics, (1998), 167-172.

[71] R.P.Russeva, "Self-dual [24,12,8] quaternary codes with a permutation automorphism of order 3", Mathematics and Education in Mathematics, (1999), 154-159.

[72] R.P.Russeva, "Self-dual [24,12,8] quaternary codes with a nontrivial automorphism of order 3", submitted to Finite Fields and Their Applications.

[73] V.Y.Yorgov and R.P.Russeva, "On the [24,12,8] quaternary self-dual codes", submitted to Journal of Combinatorial Mathematics and Combinatorial Computing.

Авторска справка

Основна цел на този дисертационен труд е построяването и класифициране на нови екстремални самодуални кодове над $GF(2)$ и $GF(4)$. Използвани са: метод за конструиране на самодуални кодове над крайно поле, притежаващи пермутационен автоморфизъм от ред взаимно прост с характеристиката на полето и метод за конструиране на нееквивалентни самодуални кодове над $GF(4)$ с мономиален автоморфизъм от ред степен на 3.

Разгледани са екстремални двоични самодуални кодове с параметри [36,18,8], [38,19,8], [42,21,8] и [44,22,8]. Намерена е цикличната структура за техните автоморфизми от нечетен прост ред. Построени са всички нееквивалентни [36,18,8] самодуални кодове с автоморфизъм от ред 7. Те са точно 3 на брой и са нови, нееквивалентни на известните самодуални кодове с тези параметри. Доказваме, че двойно-циркулантния [36,18,8] код е единствения , с точност до еквивалентност, самодуален [36,18,8] код с автоморфизъм от ред 17. Класифицирани са всички самодуални [38,19,8] кодове с автоморфизъм от ред 7. Те са точно 7 на брой и поне 6 от тях са нови. Построени са два нови [42,21,8] и [44,22,8] самодуални кода, тясно свързани с разширения двоичен код на Голей. Тези кодове са първите известни кодове за получените тегловни функции.

Изследвани са самодуалните [24,12,8] кодове над $GF(4)$. Те са с най-добрите възможни параметри за дължина 24. Намерен е вида на тегловната им функция. Тя зависи от един параметър. Конструирани са всички нееквивалентни самодуални [24,12,8] кодове с мономиален автоморфизъм от прост ред r, по-голям или равен на 3. За случая $r = 3$ е използван вторият посочен метод. Построените самодуални [24,12,8] кодове са с 21 различни тегловни функции.

СПЕЦИАЛИЗИРАН НАУЧЕН СЪВЕТ ПО ИНФОРМАТИКА
И ПРИЛОЖНА МАТЕМАТИКА ПРИ ВАК

ДАНИЕЛА АНАНИЕВА ЛАНГОВА-ОРОЗОВА

ИНТЕЛИГЕНТНИ БАЗИ ОТ ДАННИ И СИСТЕМИ ЗА ОБУЧЕНИЕ

АВТОРЕФЕРАТ НА ДИСЕРТАЦИЯ
за присъждане на образователната и научна степен "доктор"

Научен ръководител:
доц. д-р Павел Азълов

София, 2001 г.

Дисертационният труд "Интелигентни бази от данни и системи за обучение" съдържа 165 страници в основен текст и 59 страници в приложенията. Състои се от четири глави, заключение и приложения. В основния текст са включени 27 фигури. Използвани са 131 литературни източника, от които 106 на латиница и 25 на кирилица. Резултатите са представени в 10 научни публикации.

Дисертационният труд е обсъден и насочен за защита от разширен съвет на катедра "Компютърна информатика" при Факултет по математика и информатика на СУ "Св. Кл.Охридски".

Защитата ще се състои на 19.03.2001г. от 13:30 часа на разширено заседание на СНС по ИПМ при ВАК, в заседателната зала на Институт по матаматика и информатика при БАН, ул. „Акад. Г. Бончев“, бл. 8.