

РЕЦЕНЗИЯ

на дисертационен труд

за придобиване на научна степен “Доктор на математическите науки”

по научната специалност 01.01.12 “Информатика”

Тема: “Оптимални кодове за контрол на грешки и оптични комуникации”

Автор: Цонка Стефанова Байчева

Рецензент: проф. д.м.н. Иван Николов Ланджев

Тема на дисертационния труд

Дисертационният труд е посветен на конструиране и изследване на шумозащитни кодове и свързаните с тях комбинаторни структури. В работата се разглеждат от една страна линейни кодове над крайни полета, а от друга оптични ортогонални кодове. Тези части от теория на кодирането са във фокуса на изследванията на много автори поради богатата структура на разглежданите обекти и разнообразните им връзки с други дялове на математиката.

Главните задачи, които са обект на изследване в настоящия дисертационен труд, са следните:

- намиране на радиуса на покритие на класове линейни кодове;
- изследване на поведението на шумозащитни кодове при използването им за откриване и поправяне на грешки;
- конструиране на нови скъсени циклични кодове;
- изследване на специални характеристики на шумозащитни кодове, свързани с възможността им за контрол на грешки;
- конструиране на оптични ортогонални кодове и изследване на свързаните с тях комбинаторни конфигурации.

Литературен обзор

Общото ми впечатление е, че дисертантката познава задълбочено съвременното състояние на разглеждания проблем. Част от изследванията ѝ са върху задачи и

хипотези, формулирани от значими специалисти от теория на кодирането. Дисертацията включва решения на редица открити случаи, както и подобрения на известни резултати. С това дисертантката демонстрира дълбоко познаване на областта и възможности творчески да я развива. Дисертантката показва отлична информираност по разглежданите проблеми.

Методика

В изследванията си дисертантката използва методи от линейната алгебра, елементарната комбинаторика както и компютърни пресмятания.

Съдържание и резултати на дисертационния труд

Дисертационният труд е в обем от 216 нестандартни машинописни страници и се състои от увод, седем глави, осем приложения и списък на използваната литература, включващ 235 заглавия.

Глава 1 съдържа основните дефиниции и резултати за линейни кодове над крайни полета, които се използват по нататък в дисертацията. Раздел 1.1 и 1.2 са въведени основите на теория на линейните кодове над крайни полета. Въведени са понятията спектър на линеен код, еквивалентност на кодове, цикличен код, ортогонален код, дуален код, спектър на линеен код, лидер на съседен клас, спектър на лидерите, пораждаща и проверочна матрица t -подходящ и t -добър код за поправяне на грешки. В раздели 1.3 и 1.4 се въвеждат циклични скъсени циклични кодове. Формулирани са класически резултати за скъсени циклични кодове от дисертацията на Питерсън. В раздел 1.5 и 1.6 се дефинира параметърът радиус на покритие на код. Представена е границата на Делсарт, както и граници за радиуса на покритие на кодовете, получени от кодове с известни радиуси при различни стандартни конструкции. Въведена е функцията $t_q[n, k]$ като минималния радиус на покритие на q -ичен $[n, k]$ -код за фиксирани стойности на q, n и k . Представени са и някои известни неравенства за $t_q[n, k]$. Глава 1 не съдържа оригинални резултати.

Глава 2 е посветена на някои изчислителни аспекти на задачите от дисертационния труд. В раздел 2.1 се дефинират понятията код откриващ t грешки и код поправящ t грешки. Формулирани са добре известните резултати, че тези свойства на един код са свързани с параметрите на кода, както и с със спектъра и спектъра на лидерите на съседни класове.

В раздел 2.2 се въвеждат някои понятия от теория на алгоритмите като сложност на алгоритъм, класовете P , NP и $NP - c$. Представен е списък на някои NP -пълни задачи, имащи отношение към теория на кодирането. Всички задачи, разглеждани в дисертационния труд – определяне на минималното разстояние на код, определяне на радиуса на покритие на код, определяне на спектъра на код, определяне на спектъра на лидерите на съседни те класове – се оказват с експоненциална сложност. В раздел 2.3 са представени реализации на алгоритмите за пресмятане на разпределението на теглата и на радиуса на покритие на код.

Основна тема на глава 3 е определянето на радиуса на покритие на специални класове линейни кодове. Раздел 3.1 е посветен на негациклични кодове с дължина, ненадхвърляща 26. Ще отбележим, че констацикличните кодове (и в частност негацикличните кодове) възникват като естествено обобщение на цикличните кодове. Основен резултат е твърдение 3.1.1, където се поучени точните стойности на $t_3[n, k]$ за дължини, ненадхвърлящи 26. Някои от кодовете, получени в този раздел са квазисъвършени, което представлява особен интерес. Двоични и троични квазисъвършени кодове са разгледани подробно в следващия раздел 3.2. Тези кодове представляват особен интерес като обобщение на съвършените кодове, при които радиуса на покритие съвпада с радиуса на сферичната опаковка. За квазисъвършените кодове тези числа се различават с 1. Докато за съвършените кодове имаме характеристика (направена от Титавайнен и независимо от Зиновьев и Леонтиев), то такава липсва (и изглежда малковероятна поне за малки радиуси на покритие) за квазисъвършените кодове. Главният резултат на този раздел е представен в таблици 3.2.3-3.2.5, където са описани параметрите на двоични и троични квази съвършени линейни кодове, за които е направена пълна класификация. Резултатите в този раздел, разглеждани от гледна точка на евентуална характеристика на квазисъвършените кодове, са по-скоро обезкуражаващи. Такава едва ли е възможна във вида, който е известен за съвършените кодове.

В раздел 3.3 са решени шест открити случая за определяне на точната стойност на $t_2[n, k]$ от класическата книга на Кoen, Хонкала, Лидин и Лобстейн. Това са точните стойности:

$$t_2[17, 6] = 5, t_2[17, 8] = 4, t_2[18, 7] = 5, t_2[19, 7] = 5, t_2[20, 8] = 5, t_2[21, 7] = 6.$$

В раздел 3.4 е определена точната стойност на функцията $t_2[n, k]$ за $k = 6$ и всички дължини. Този резултат се основава на оценката $t_2[n, 6] \leq \lfloor (n-8)/2 \rfloor$ и наблюдението, че тя е точна за $n \geq 64$. В настоящата работа е доказано, че тази граница е всъщност точна и за всички $n \geq 18$. Подобно изследване за троични кодове с размерност 4 проведено в раздел 3.5. Основните резултати тук са обобщени в таблицата на стр. 79, в която са дадени точни стойности и граници за $t_3[n, 4]$ за $5 \leq n \leq 40$.

Глава 4 е посветена на поведението на линейни кодове при промяна на параметрите на канала. Предполага се, че разглеждаме q -ичен симетричен канал с вероятност за преминаване на символ в различен символ $\epsilon \in [0, (q-1)/q]$. При използване на конкретен код C вероятността за неоткрита грешка при декодиране $P_{ue}(C, \epsilon)$ се задава като функция спектъра и ϵ . Един код е подходящ, ако тази функция е монотонна (растяща) по ϵ в целия интервал на изменение на ϵ . В раздел 4.1 е изследвано поведението на тази функция за всички двоични и троични кодове с дължини до 33. В раздел 4.2 е представен ефективен начин за пресмятане на спектъра на лидерите на съседни класове за циклични кодове. Раздел 4.3 представлява детайлно изследване на троичния квадратично остатъчен $[13, 7, 5]$ -код. Предложен е алгебричен алгоритъм за декодиране на тези кодове. В раздел 4.4. е направено сравнение на поведението

на различни класове линейни кодове при контролиране на грешки. Тук е даден и негативен отговор на една открита задача от класическата книга на Мак-Уилямс и Слоан. Известно е, че спектърът на един линейен код определя еднозначно спектъра на ортогоналния му (посредством тъждествата на МакУилямс). Въпросът зададен от МакУилямс и Слоан е доколко спектърът на лидерите на линейен код определя спектъра на лидерите на ортогоналния му. В раздел 4.4 са приведени примери на кодове с параметри $[15, 3, 7]$, които имат еднакви спектри на лидерите, но за които ортогоналните са с различни спектри на лидерите.

В глава 5 се изследват скъсени циклични кодове и поведението им при откриване и поправяне на грешки.

В трите раздела на глава 6 са разгледани някои характеристики на шумозащитни кодове, между които не можах да установя особена връзка: Нютонов радиус на покритие, възможност за неравна защита на символите, нормализираност на линейни кодове. Последното свойство се изисква за да може един код да се използва в една специална конструкция на Грем и Слоан, даваща кодове с възможно малък радиус на покритие. В раздел 6.1 са пресметнати Нютоновите радиуси на покритие на всички двоични циклични кодове с дължини до 31, на оптималните двоични кодове с дължина до 33 и на всички троични циклични и негациклични кодове с дължини до 22. В раздел 6.2 се разглеждат кодове с неравномерна защита на символите. Предложен е алгоритъм за определяне на възможностите за неравномерна защита на символите на всички троични циклични и негациклични кодове с дължини до 26 и минимално разстояние поне 3. В раздел 6.3 е доказано, че всички двоични кодове с дължини 16, 17 и 18 и коразмерност 10 са нормализирани.

Глава 7 е посветена на оптични ортогонални кодове, както и на свързани с тях комбинаторни конфигурации. Казваме, че семейството $\{C_i\}$ от k -елементни подмножества на $\mathbb{Z}_v$ е $(v, k, \lambda_a, \lambda_c)$ оптичен ортогонален код, ако две различни трансляции на всяка кодова дума имат най-много λ_a общи елементи, а произволни трансляции на две различни кодови думи имат най-много λ_c общи елемента. В раздел 7.1 е предприета класификация на оптични ортогонални кодове с параметри $(v, 4, 2, 1)$ за $v \leq 76$, $v \neq 71$, и $(v, 5, 2, 1)$ за $v \leq 114$. Получените резултати са представени в таблиците от Приложение 3. Там са представени конструкции на оптични ортогонални кодове с параметри $(v, 4, 2, 1)$ и $(v, 5, 2, 1)$ и за по-големи стойности на v от 76 (респ. 114). Освен конструктивните резултати е доказано и несъществуване на оптичен ортогонален код, достигащ границата на Бурати-Пасоти-Ву с параметри $(154, 5, 2, 1)$.

Раздел 7.2 е посветен на класификация на $(v, 3, 1)$ циклично пермутационни кодове с $v \leq 61$. В случаите, когато получените кодове са свършени се получават класификационни резултати за Шайнерови системи от тройки, които представляват независим интерес. Така например, от класификацията на $(61, 3, 1)$ циклично-пермутационните константно-тегловни кодове се получава, че съществуват поне 42 373 196 нееквивалентни $STS(61)$ с цикличен автоморфизъм.

Последният раздел 7.3 е посветен на класификацията на $(v, k, 1)$ циклични разностни множества за относително малки стойности на v . Нови резултати в тази глава са

класификациите на цикличните разностно множества с параметри $(61, 3, 1)$, $(73, 4, 1)$, $(76, 4, 1)$, $(81, 5, 1)$, $(85, 5, 1)$ както и няколко множества от параметри с $k \geq 7$.

Приноси на дисертационния труд

По мое мнение по-важните приноси в дисертационния труд се свеждат до следното:

- (1) Определени са радиусите на покритие на класове от кодове, както и на отделни кодове. Намерена е точната стойност на $t_q[n, k]$ за $q = 2, 3$ и различни стойности на n и k .
- (2) Определени са класове от кодове, които не са подходящи за контрол на грешки.
- (3) Предложен е алгоритъм за декодиране на троичния квадратично-остатъчен код с дължина 13.
- (4) Класифицирани са скъсените циклични кодове с относително малък брой проверочни символи.
- (5) Разрешен е проблем 5.1 от монографията на МакУилямс и Слоан.
- (6) Решена е задача на Туви Етцион за намиране на квазисвършени кодове с минимално разстояние, надхвърлящо 5.
- (7) Определени са Нютоновите радиуси на покритие за двоични и троични кодове с малка дължина.
- (8) Класифицирани са оптични ортогонални кодове с параметри $(v, 4, 2, 1)$ за $v \leq 75$, $v \neq 71$, и $(v, 5, 2, 1)$ за $v \leq 114$.
- (9) Класифицирани са $(v, k, 1)$ -циклични константно тегловни кодове за $v \leq 61$, както и циклични разностни множества с параметри $(61, 3, 1)$, $(73, 4, 1)$, $(76, 4, 1)$, $(81, 5, 1)$, $(85, 5, 1)$.

Забележки по дисертационния труд

Във връзка с дисертационния труд имам следните забележки, въпроси и коментари:

- (1) Раздел 1.1 е е странно къс.
- (2) На стр. 21: по-коректно е да се говори за векторното пространство на всички наредени n -орки над F вместо за " n -мерното векторно пространство".
- (3) На стр. 24: не е дефинирано какво се рабира под комуникационна система и комуникационен канал.

- (4) На стр. 33: дефиниции 2.1.1 и 2.1.3 са неясни. За мен дефинициите на код поправящ (откриващ) t грешки са по-скоро Теорема 2.1.2 и теорема 2.1.4.
- (5) На стр.48: означението $t_3[20, 6] = 7 - 8$ е неудачно. По-добре би било $7 \leq t_3[20, 6] \leq 8$.
- (6) На стр.50: пропуснато е да се каже, че става дума за линейни свършени кодове. Класификация на всички нелинейни свършени кодове е малко вероятна.
- (7) Дават ли резултатите от последната таблица в глава 7 някави подобрения на таблиците на Матон и Роса?
- (8) На стр. 143: защо се използва думата колекция в дефиницията на оптичен ортогонален код (а и на други места)? Не е ли по-добре да се използва просто "множество от подмножества"? Очевидно е от (7.2), че C_i -тата са различни освен ако не вземем $\lambda_c = k$, което пък е безсмислено. Пак там: вместо размер на код е по-добре да се използва мощност на код.
- (9) На стр.144: вместо насочен граф е по-добре ориентиран граф.

Публикации по дисертационния труд

Резултатите от дисертационния труд са публикувани в 25 статии: 16 от тях са публикувани в чуждестранни и наши научни списания, а 9 – в сборници с доклади от конференции и симпозиуми. Статиите са публикувани както следва:

- IEEE Transaction on Information Theory - 4;
- Computer Communications - 1;
- IEE Proc. Communications - 1;
- IEEE Transactions on Communications - 1;
- Advances in Mathematics of Communication - 1;
- Journal of Combinatorial Designs - 1;
- AAECC - 1
- Mathematica Balkanica - 3;
- Serdica J. Computing - 1;
- Годишник на СУ - 1;
- Proceedings of the Int. Workshop on ACCT - 5;

- Proceedings of the Int. Conference on Appl. of Computer Algebra - 1;
- Proceedings of the ITHEA - 1;
- Proc. Workshop Mathematics, Informatics and Comp. Sciences -1;
- Enhancing cryptographic primitives (IOS Press) - 1.

Пет от тези списания – IEEE Trans. Inf. Theory, IEEE Trans. on Communications, AMC, JCD, AAЕСС имат импакт фактор. Бих желал да отбележа, че при цялата условност на импакт-фактора на изданията, където са публикувани работите по дисертационния труд, той все пак е индикатор за това, че тематиката е актуална и резултатите на дисертантката са значими.

Авторство на получените резултати

Авторството на публикациите е следното: 7 са самостоятелни, 13 са с един, 3 са с двама и 2 с трима съавтори. Тъй като през последните години следя отблизо развитието на областта, в която е написан дисертационния труд, за мен няма съмнение, че във въпросните работи приносът на дисертантката е равностоеен с този на останалите автори.

Цитирания на публикациите от дисертационния труд

Дисертантката е приложила списък от 116 цитиранията на нейни резултати, включени в дисертацията. Голяма част от тях са в международни научни списания и монографии, което показва, че резултатите ѝ са широко известни и добре приети от математическата общност. Сред цитираните работи изпъкват [213] с 53 цитирания и [211] с 22 цитирания.

Автореферат и авторска справка

Авторефератът и авторската справка са направени съгласно изискванията и отразяват правилно резултатите и приносите в дисертационния труд.

Заклучение

Дисертацията е посветена на един кръг от интересни и актуални проблеми от теория на кодирането. Направено е задълбочено изследване на няколко важни задачи от теорията на шумозащитните кодове. С това е постигнат е сериозен напредък в актуални дялове на теорията на кодирането. Изложените по-горе количествени показатели за брой статии (25), брой статии в списания с импакт фактор (8), брой статии в рецензирани издания (25) и цитирания (116), надхвърлят значителни изискванията, поставени в чл. 6(2) на Правилника за условията и реда за придобиване на научни степени и за заемане на академични длъжности в ИМИ на БАН.

Считам, че представеният дисертационен труд "Оптимални кодове за контрол на грешки и оптични комуникации" с автор Цонка Стефанова Байчева съдържа научни резултати, които са съизмерими със съвременните постижения в теория на кодирането и представляват значителен и оригинален принос в науката. Дисертантът показва задълбочени теоретични знания в областта на теория на кодирането, както и способност за самостоятелни научни изследвания. С това считам, че той отговаря на изискванията на Закона за научните степени и звания за даване на научната степен "Доктор на математическите науки". Гореизложеното ми дава основание да препоръчам на Уважаемото Жури да излезе с положително становище на дисертационния труд на Цонка Стефанова Байчева за получаване на научната степен степен "Доктор на математическите науки" по научната специалност 01.01.12 "Информатика".

София, 10.08.2015 г.

Рецензент: