

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: доц. д-р Ася Петрова Русева

Дисертационният труд е посветен на няколко актуални проблема от теория на кодирането. Разглежданите задачи са от различни направления и нямат голяма връзка помежду си. Общото между тях е че те третираат различни страни на теория на кодирането, разбираана като използване на алгебрични и комбинаторни структури за защита на данни. Накратко основните проблеми, разгледани в дисертационния труд могат да бъдат формулирани така:

- (1) определяне на радиуса на покритие на класове линейни кодове; в частност, определяне на стойностите на $t_q[n, k]$ за различни стойности на параметрите q, n и k ;
- (2) изследване на поведението на шумозащитни кодове при откриване и поправяне на грешки;
- (3) конструиране и изследване на нови скъсени циклични кодове;
- (4) изследване на специални характеристики на шумозащитни кодове;
- (5) конструиране на оптични ортогонални кодове и изследване на връзките им с класически комбинаторни конфигурации.

Дисертационният труд е в обем от 216 страници и е структуриран в увод, седем глави, осем приложения и списък на използваната литература, включващ 235 заглавия. Първите две глави носят уводен характер. В глава 1 са представени някои дефиниции и факти от теория на кодирането. В глава 2 се обсъждат изчислителните аспекти на задачите, разглеждани в останалата част на дисертационния труд. Направен е кратък увод в теория на NP -пълните задачи. Представено е и подробно описание на конкретни алгоритми: генериране на q -ичен отразен код на Грей, намиране на разпределението на теглата на q -ичен линеен

код, намиране на радиуса на покритие на линеен код. Оригиначните приноси се съдържат в глави 3 – 7.

Глава 3 е посветена на задачата за намиране на радиуса на покритие на линеен код. Тази задача е добила голяма популярност в средата на 80-те години с обзора на Коен, Карповски, Метсън и Шатц и е във фокуса на изследванията и до наши дни. Основните резултати се състоят в определяне на точната стойност на функцията $t_q[n, k]$ (дефинирана като минималния радиус на покритие на q -ичен $[n, k]$ -код) за различни стойности на параметрите q, n и k . Тези резултати включват:

- точните стойности на $t_3[n, k]$ за всички $n \leq 26$ (тук са получени и някои интересни резултати за квазисъвършени кодове);

- точната стойност на $t_2[n, k]$ в шест важни специални случая: $(n, k) = (17, 6), (17, 8), (18, 7), (19, 7), (20, 8), (21, 7)$, които са анонсирани като открити в монографията на Коен, Хонкала, Лицин и Лобстейн;

- $t_2[n, 6]$ за всички дължини n ;

- $t_3[n, 4]$ за $5 \leq n \leq 40$.

По мое мнение особен интерес представляват резултатите от раздел 3.2, отнасящи се до квазисъвършени кодове. Макар да има много примери на такива кодове, смислена класификация в смисъла на направената от Титавайнен (и независимо от Зиновьев и Леонтиев) за съвършени кодове, изглежда недостъпна към настоящия момент. Все пак в таблици 3.2.3 – 3.2.5 са дадени някои интересни за параметри на квазисъвършени кодове, за които е направена пълна класификация. Във връзка с това има известна неяснота с едно твърдение на стр. 51, ред 16 отдолу, където се отбелязва, че квазисъвършените кодове с параметри $[n, n-4, 5]_q$ съответстват на “пълни арки в ... $PG(3, q)$ ”. Ако приемем, че пълна арка, е арка, която не може да бъде разширена, запазвайки максималния брой точки на права, то горното твърдение не изглежда смислено. По-скоро дисертантът има предвид пълни шапки и дори по-общо ρ -насищащи множества ρ -saturating sets.

Много приятно впечатление прави раздел 3.4, в който са определени минималните радиуси на покритие за всички двоични линейни кодове с размерност 6. Това продължава изследванията на Коен, Карповски, Метсън, Шатц, Греъм, Слоен, които в няколко публикации решават тази задача за размерност 5. Резултатът се опира на една оценка на Греъм и Слоен, съгласно която

$$t_2[n, 6] \leq \lfloor \frac{n-8}{2} \rfloor, \quad n \geq 18.$$

Основният резултат тук е теорема 3.4.1, в която се твърди, че в горната оценка всъщност се достига равенство. За получаване на този резултат е определен радиуса на покритие на над четвърт милиард кода, което изисква големи по обем компютърни пресмятания.

Глава 4 е посветена на един проблем, който има смисъл при q -ични симетрични канали с променлива вероятност ε за сгрешен символ: подходящ код за откриване на грешки. Очакваното поведение на един код при нарастване на ε е да нараства и вероятността $P_{ue}(C, \varepsilon)$ за неоткрита грешка при декодиране. Оказва се, че далеч не всички кодове имат това свойство. Казваме, че кодът C е подходящ, ако функцията $P_{ue}(C, \varepsilon)$ е монотонно растяща по ε в интервала $[0, (q-1)/q]$. В работата се изследва поведението на тази функция за двоични и троични кодове с дължина до 33.

Особена ценност представлява изследването на троичния квадратично-остатъчен $[13, 7, 5]$ -код в раздел 4.3 и предложените два алгоритъма за декодирането му. Квадратично остатъчните кодове се считат за особено добри при поправяне на грешки и поради добрата си структура допускат ефективни алгоритми за декодиране. Те удовлетворяват т.нар. граница на квадратния корен, $d \geq \sqrt{n}$, която в много от случаите се надхвърля (както и при горния код). Така, квадратично остатъчният $[13, 7]_3$ -код се оказва с минимално разстояние 5 и може да поправи две грешки.

Любопитно е, че в тази глава е даден отговор на един въпрос (Проблем (5.1)) от монографията на МакУилямс и Слоан за кодове, поправящи грешки. Кандидатът успява да конструира пример на двойка линейни кодове със съвпадащи спектри на лидерите на съседни класове, чиито ортогонални са с различни спектри на лидерите. Бих отбелязала, че проблемите, поставени като открити в книгата на МакУилямс и Слоан, са разглеждани като трудни задачи, чието решаване е престижно и определят за дълго време насоката на изследванията в теория на кодирането.

Бих направила малка бележка по обсъждането на различните оптимизационни задачи в раздел 4.4, стр 93. Прието е минималната дължина на линеен $[n, k, d]_q$ -код с фиксирани q, k, d да себележи $n_q(k, d)$ (а не с голямо N). Въпрос 1 за това как се отнасят една спрямо друга оптималностите спрямо различните параметри е изяснен още през 60-те години (от Левенщайн). Освен това въпрос 2 може да бъде преформулиран така: вярно ли е, че всички пунктирани кодове на код с делител $\Delta > 1$ са изоморфни (еквивалентни). Става ясно, че отговорът на въпрос 2 е: “не винаги добавянето на проверка за четност на нееквивалентни кодове води до нееквивалентни кодове”.

Глава 5 носи по-приложен характер. В нея се изследват скъсени циклични кодове (CRC-кодове). Тези кодове намират широко приложение при съхраняване на данни върху различни памети и затова са обект на интензивни изследвания. Тук се сравнява поведението на функцията $P_{ue}(C, \varepsilon)$ за различни CRC-кодове, което позволява да се избере най-добрият код за конкретни приложения. Оказва се, че редица стандартизирани CRC-кодове имат по лошо поведение от не-стандартизирани CRC-кодове. Подробно са изследвани (раздели 5.2 и 5.3) CRC-кодове с 8 и 16 проверочни бита и са намерени тези, които са най-подходящи

за приложенията.

Глава 6 е посветена на три по мое мнение несвързани теми: Нютонов радиус на покритие на кодове, кодове с неравна защита на символите и нормализирани линейни кодове. Последните са ценни с това, че могат да бъдат използвани в една специална конструкция на Грѐм и Слоан, наречена *amalgamated direct sum*, позволяваща конструиране на линейни кодове с “голям” радиус на покритие. В раздел 6.1 е пресметнат т.нар. Нютонов радиус 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. Раздел 6.2 е посветен на линейни 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, ненадхвърлящи 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 и свързаните с тях комбинаторни конфигурации. Централни за тази глава са двете класификации на $OOC(v, 4, 2, 1)$ за $v \leq 75$, $v \neq 71$, и $OOC(v, 5, 2, 1)$, $v \leq 114$. Конструирани са и оптимални ортогонални кодове за някои по-големи стойности на v . По мое мнение ценност представляват и комбинаторните резултати, получени при изследването на оптичните ортогонални кодове. Така например авторът конструира 42373196 неизоморфни Шайнерови системи от тройки от ред 61. Самата задача за разделяне на Шайнеровите системи от тройки от ред 61 в такъв голям брой класове на изоморфизъм е нетривиална изчислителна задача. Това предполага, че броят на първоначално генерираните Шайнерови системи е много по-голям, което от своя страна повдига редица технически въпроси като този за кодирането им, съхранението им, тестовите за изоморфизъм и т.н. По нататък в главата са класифицирани и разностни множества с параметри $(71, 4, 1)$, $(76, 4, 1)$, $(81, 5, 1)$, $(85, 5, 1)$, което от своя страна води до класификационни резултати за дизайни с циклична група от автоморфизми от ред v (където v е броят на точките в дизайна).

По мое мнение най-стойностни в дисертационния труд са глави 3 и 7, където са направени важни класификационни резултати, съизмерими с най-добрите изследвания в настоящия момент. Приносите на този дисертационен труд могат да бъдат характеризирани така:

- Определени са радиусите на покритие на класове от линейни кодове. Намемена е точната стойност на функцията $t_q[n, k]$ за $q = 2, 3$ и различни стойности на n и k .
- Характеризирани са класове от линейни кодове, които не са подходящи за откриване или поправяне на грешки.

- Намерен е ефективен алгебричен алгоритъм за декодиране на троичния квадратично-остатъчен код с дължина 13.
- Направена е класификация на скъсените циклични кодове с малък брой проверочни символи.
- Конструирани и класифицирани са линейни квазисъвършени кодове с минимално разстояние, надхвърлящо 5.
- Определени са Нютоновите радиуси на покритие за двоични и троични кодове с малка дължина.
- Класифицирани са оптични ортогонални кодове с параметри $(v, 4, 2, 1)$ за $v \leq 75$, $v \neq 71$, и $(v, 5, 2, 1)$ за $v \leq 114$.
- Класифицирани са $(v, k, 1)$ -циклични константно тегловни кодове за $v \leq 61$, както и циклични разностни множества с параметри $(61, 3, 1)$, $(73, 4, 1)$, $(76, 4, 1)$, $(81, 5, 1)$, $(85, 5, 1)$.

Дисертационният труд е написан въз основа на 25 статии (16 в реферирани научни списания и 9 в сборници с доклади на конференции). Поне осем от статиите са публикувани в списания с импакт-фактор: IEEE Transactions on Information Theory (4), IEEE Transactions on Communications (1), Advances in Mathematics of Communication (1), Journal of Combinatorial Designa (1), AAECC (1). Седем от статиите са самостоятелни; останалите са с един или повече съавтори. Приемам, че приносът на дисертанта е равностоеен с този на останалите автори. В материалите е приложен и списък от 116 цитирания на резултати на кандидата. Това показва, че резултатите, представени в настоящия труд, са сериозно апробирани и добре приети от международната колегия. Споменатите по-горе количествени показатели надхвърлят значително изискванията, поставени в Правилника за условията и реда за придобиване на научни степени и за заемане на академични длъжности в ИМИ на БАН.

Заклучение. Имайки предвид гореизложеното, препоръчвам на уважаемото Жури да присъди на проф. д-р Цонка Стефанова Байчева научната степен “доктор на математическите науки” по научната специалност 01.01.12 “Информатика”.

София, 16.08.2015 г.

Рецензент:

(доц. д-р Ася Русева)