Р Е Ц Е Н З И Я

на дисертационен труд
за придобиване на образователната и научна степен "Доктор"

по професионално направление 4.5 "Математика" (Алгебра и теория на числата)

Тема: "Дзета-функции на линейни кодове и локално крайни модули"

Автор: Иван Бойчев Маринов

Научни консултанти: проф. д-р Азнив Киркор Каспарян

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

Тема на дисертационния труд

В представения дисертационен труд са разгледани въпроси, отнасящи се до общата теория на линейните кодове над крайни полета, и по специално до въпроси за numerатора на теглата на линеен код и свързаните с него ζ-полином и редуциран полином на Дуурсма. Разгледана е и една алгебро-геометрична задача за модули над абсолютната група на Галоа в крайно поле. Целите, които дисертантът си поставя в настоящия труд са следните:

1) Намиране на numerатора на теглата на произволен линеен код чрез коефициентите на неговия полином на Дуурсма.

2) Намиране на условия за формална самодуалност на произволен линеен код от даден род.

3) Намиране на връзки между тъждествата на МакУилямс за линеен код и поляризираните условия на Риман-Рох за неговата ζ-функция.

4) Намиране на условия за изпълнение на аналога на хипотезата на Риман за локално крайни модули над абсолютната група на Галоа на крайно поле.

Литературен обзор

Общото ми впечатление е, че дисертантът познава много добре съвременното състояние на разглеждания проблем. Голяма част от изследванията му са върху един

кръг от задачи от теория на кодирането, причислявани обикновено към теорията на алгебро-геометричните кодове. Алгебро-геометричният подход към шумозащитното кодиране възниква през 70-те години на XX век с работите на Валерий Д. Гоппа и доведе до конструирането на класове от кодове, имащи голяма важност за приложенията.

Методика

В изследванията си дисертантът използва основно идеи и резултати от алгебричната геометрия, комутативната алгебра, линейната алгебра и теория на групите. На места дисертантът използва и комбинаторни разсъждения.

Съдържание и резултати на дисертационния труд

Представеният дисертационният труд е в обем от 169 нестандартни машинописни страници и се състои от шест глави и списък на използваната литература, включващ 16 заглавия.

По-долу ще изложа накратко съдържанието на отделните глави от дисертационния труд.

Глава 1 представлява увод в дисертацията. Докторантът излага целите, които си поставя с настоящия текст, както и основните идеи, заложени в него. Една от тях е намирането на връзка между тъждествата на МакУйлямс и поляризираните условия на Риман-Рох. Друг фокус на работата е дефинирането на ζ-функция на локално краен модул над абсолютната група на Галоа на крайно поле и изследване на въпроса за верността на аналога на хипотезата на Риман.

Глава 2, наречена "Предварителни сведения", съдържа доста подробен увод в алгебричната геометрия. Изложени са дискретните нормирания на функционално поле на една променлива, съответствието между пръстените на дискретното нормиране на $\mathbb{F}_q(X)$ и орбитите на абсолютната група на Галоа върху X. Изложени са свойствата на дивизорите върху крива, доказана е теоремата на Риман и е представена горна граница за броя на рационалните точки на крива X над $\mathbb{F}_q$. Изложението в тази глава следва монографиите на Шихтенот и Нидерайтер-Зинг.

В глава 3 са изложени някои важни сведения и резултати от теория на кодирането. В раздел 3.1 са въведени фундаментални понятия като линеен код, разстояние на Хеминг, пораждаща и проверочна матрица на линеен код, дуален код, граница на Сингълтън, род на линеен код, MDS-кодове. По-нататък се дефинират строго кодовете на Рид-Соломон и естественото им продължение - алгебро-геометричните кодове на Гоппа. Раздел 3.2 е посветен на тъждествата на МакУйлямс в частния случай, представящ връзката между нумераторите на теглата (на Хеминг) на двойка взаимноортогонални линейни кодове над крайно поле. Изложено е известното доказателство на Харълд Уорд на тъждествата на МакУйлямс за стандартния нумератор на теглата на линеен код.

В раздел 3.3 е въведен ζ-полином на произволен линеен $[n,k,d]_q$-код с пълна дължина (неизроден код в термините на дисертацията). Най-напред номераторът на теглата $W_C(x,y)$ се представя като линейна комбинация на номераторите на MDS-кодове с дължина n и минимално разстояние $d+i$ (които, както е добре известно са определени от параметрите на кода):

$$W_C(x,y) = \sum_{i=0}^{r} a_i M_{n,d+i}(x,y), \quad \sum a_i = 1,$$

а след това ζ-полиномът се дефинира като

$$P_C(t) = \sum_{i=0}^{r} a_i t^i.$$

Показана е връзка между номератора и ζ-полинома на линеен код. В раздел 3.4 са изложени някои важни резултати на Иван Дуурсма, описващи свойства на ζ-полинома на линеен код.

Следващите три глави са централни за дисертационния труд. В тях са изложени оригиналните резултати на докторанта.

В глава 4 е изследван редуцираният полином на Дуурсма на линеен код C от род g, дефиниран като

$$D_C(t) = \frac{P_C(t) - t^g}{(1-t)(1-qt)},$$

където $P_C(t)$ е ζ-полиномът на C. Съгласно Дуурсма линейният код $C \leq \mathbb{F}_q^n$ удовлетворява хипотезата на Риман, ако корените на $P_C(t) = \sum a_i t^i \in \mathbb{Q}[t]$ лежат върху окръжността

$$S\left(\frac{1}{\sqrt{q}}\right) = \{Z \in \mathbb{C} \mid |z| = \frac{1}{\sqrt{q}}\}.$$

Централният резултат в раздел 4.1 е Твърдение 101 (защо не Теорема?), в което е определено отклонението на номератора на теглата на произволен линеен $[n,k]$-код от номератора $M_{n,n-k+1}$ на линеен MDS-код със същата дължина. Оказва се, че това отклонение зависи от коефициентите в редуцирания полином на Дуурсма. Този резултат може да се разглежда и като обобщение на резултата на Додунеков-Ланджев за номератора на теглата на почти-MDS код.

Основният резултат на раздел 4.2 е твърдение 102, съгласно което ако един код C удовлетворява хипотезата на Риман за линейни кодове, то той е формално самодуален, или с други думи номераторът на теглата на C съвпада с номератора на C. Доказателството се основава на наблюдението, че един код е формално самодуален тогава и само тогава, когато неговият ζ-полином удовлетворява функционалното уравнение

$$P_C(t) = P_C\left(\frac{1}{qt}\right) q^g t^{2g}$$

на полинома на Хасе-Вейл на функционалното поле на крива от род g над $\mathbb{F}_q$. По-нататък в твърдение 103 са доказани различни еквивалентни условия за това един линеен код да е формално самодуален. В твърдение 104 са доказани условия за това един код от род 2 да е формално самодуален. Тези условия са формулирани в термините на коефициентите на редуцирания полином на Дуурсма, който в този случай е от степен 2.

В раздел 4.3 са получени резултати за редуцирания полином на Дуурсма на функционалното поле F на гладка неприводима крива X (твърдение 106). По-специално, доказано е, че редуцираният полином на Дуурсма $D_F(t)$ е еднозначно определен от броя на ефективните дивизори на F от степен i. Доказани са и неравенства за броя $h(F)$ на класовете на линейна еквивалентност на дивизорите на F от степен 0.

В глава 5 представлява един нов поглед към класическите тъждества на МакУилямс за numerатора на теглата на линеен код и неговия ортогонален. Основният резултат в първия раздел на тази глава е Теорема 110, съгласно която тъждествата на МакУйлямс за двойка взаимно-ортогонални кодове C и $C^\perp$ са еквивалентни на поляризираните условия на Риман-Рох за техните ζ-функции

$$\zeta_C(t) = \frac{P_C(t)}{(1-t)(1-qt)} \quad \text{и } \zeta_{C^\perp} = \frac{P_{C^\perp}(t)}{(1-t)(1-qt)}.$$

В раздел 5.2 е дадена кобинаторно-геометрична интерпретация на коефициентите c_i от редуцирания полином на Дуурсма като средно-аритметично на броя на точките в сечението на $n-d-i$ координатни хиперравнини в проективното пространство $\mathbb{P}(\mathbb{F}_q^n)$ (Твърдние 112). В Твърдение 113 е дадена и вероятностна интерпретация на коефициентите c_i от редуцирания полином на Дуурсма.

Резултатите в последната глава 6 не са пряко свързани с теория на кодирането. Нека $\mathfrak{G}$ е абсолютната група на Галоа на крайно поле $\mathbb{F}_q$. Казваме, че един безкраен локално краен модул M изпълнява аналога на хипотезата на Риман относно проективната права $\mathbb{P}^1(\overline{\mathbb{F}}_q)$, ако

$$P_M(t) = \frac{\zeta_M(t)}{\zeta_{\mathbb{P}^1(\mathbb{F}_q)}(t)} = \prod_{i=1}^{d}(1-\omega_i t)$$

е полином с $|\omega_1| = \cdots = |\omega_d| = \sqrt[d]{|a_d|}$ за всяко $1 \leq i \leq d$. Доказани са условия, при които локално краен модул M изпълнява аналога на хипотезата на Риман относно проективната права $\mathbb{P}^1(\mathbb{F}_q)$. Това е и съдържаниетио на теорема 142 от раздел 6.3. От този резултат са изведени интересни следствия като, например, Следствие 144, съгласно което ζ-частното $P_M(t)$ на безкраен локално краен модул M удовлетворява функционално уравнение, аналогично на уравнението за ζ-функцията на линеен код.

Приноси на дисертационния труд

По мое мнение по-важните приноси в дисертационния труд са следните:

(1) Намерена е формула, изразяваща номератора на теглата на произволен линеен код чрез коефициентите на неговия полином на Дуурсма.

(2) Доказано е. че всеки код, удовлетворяващ хипотезата на Риман е формално самодуален.

(3) Намерени са условия за това един линеен код от род 2 да бъде формално самодуален в термините на коефициентите на неговия редуциран полином на Дуурсма.

(4) Доказано е, че тъждествата на МакУилямс за номератора на теглата на линеен код са еквивалентни на поляризираните условия на Риман-Рох за ζ-функциите на линеен код C и неговия ортогонален $C^{\perp}$.

(5) Доказани са достатъчни условия за изпълнение на хипотезата на Риман за локално-крайни модули над абсолютната група на Галоа $\mathfrak{G} = Gal(\overline{\mathbb{F}}_q, \mathbb{F}_q)$ на крайно поле $\mathbb{F}_q$.

Забележки по дисертационния труд

Във връзка с дисертационния труд имам следните забележки и коментари:

(1) Работата е стегнато и ясно написана. Обемът ѝ от близо 170 страници надхвърля значително това, което читателят очква от докторска дисертация, но това се дължи на двете глави излагащи теоретичните основи (глави 2 и 3 с обем над 80 стр.). Ще отбележа, че не считам това за недостатък. Такава организация има предимстовото, че се спестява на читателя препратки към други текстове.

(2) Техническото оформление на работата е изпълнено на LaTeX. Появящите се на места печатни грешки не променят общото добро впечатление. Номерацията на резултатите е единна за целия труд. Това създава известни неудобства при локализиране на резултатите в доста обемния текст. Личните ми предпочитания са към двуцифрена номерация, първата цифра от която задава номера на главата.

(3) Макар библиографията да включва важни и централни за разглежданата тема публикации имам усещането, че са пропуснати важни за тематиката работи като статиите на Джей Ууд, Хайке Глюсинг-Люрсен, МакУйлямс, Бруалди-Плес съдържащи важни доказателства и обобщения на тъждествата на МакУйлямс.

(4) Имената на някои автори са изписани неправилно на български като Щихтенот, ван Вее, Андре Вейл (а не Вайл).

(5) Последният автор от библиографията е не H. K. Ward, а H. N. Ward (Harold Nathan Ward) и въпросната публикация е излязла от печат в Archiv der Mathematik (Basel) vol. 74, 2000, pp. 95–96.

(6) Можеше да бъде направено малко по-подробно проучване на литературата по теория на кодирането. Така например, тъждествата на МакУйлямс са в сила и в много по-общата ситуация на т.нар $\mathcal{W}$-регулярни разбивания на $\mathbb{F}_q^n$. Интересно би било да се изследва дали в този случай може да се дефинира аналог на полинома на Дуурсма и да се получат сходни резултати. Но това по-скоро са насоки за бъдещи изследвания.

Публикации по дисертационния труд

Резултатите от дисертационния труд са публикувани в 3 статии. Три от статиите са излезли от печат в Advances in Mathematics of Communications, Electronic Notes in Discrete Mathematics на Elsevier и Годишника на Софийския Университет.

Списанието Advances in Mathematics of Communications има импакт-фактор 0.8 за 2016 г. и е едно от водещите в областта на математическите методи в областта на теория на кодирането и криптографията.

Авторство на получените резултати

Представените три публикации са с един съавтор – научния ръководител на докторанта. Тъй като познавам научните интереси на докторанта и следя работата му в последните няколко години, за мен няма съмнение, че приносът му е равностоен на този на другия съавтор.

Цитирания на публикациите от дисертационния труд

Дисертантът не е приложил списък на цитирания на статиите, в които са публикувани резултатите от дисертационния труд. Не са ми известни цитирания на тези резултати.

Автореферат и авторска справка

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

Заключение

Дисертацията е посветена на един кръг от важни проблеми от теория на алгебро-геометричните кодове и алгебричната геометрия, представляващи значителен теоретичен интерес.

Считам, че представеният дисертационен труд "Дзета-функции на линейни кодове и локално крайни модули" с автор Иван Бойчев Маринов съдържа резултати, които представляват оригинален принос в теория на кодирането и алгебричната геометрия. Дисертантът показва задълбочени теоретични знания в областта на алгебричната

геометрия и в алгебро-геометричните методи в теория на кодирането, както и способност за самостоятелна научна работа. С това считам, че той отговаря напълно на изискванията на Закона за развитие на академичния състав в Република България за даване на научната степен "Доктор", както и на специфичните изисквания от Правилника за условията и реда за придобиване на научни степени и за заемане на академични длъжности във ФМИ на СУ. Гореизложеното ми дава основание да дам положителна оценка на представения дисертационен труд. Убедено препоръчвам на Уважаемото Жури да присъди на Иван Бойчев Маринов образователната и научна степен "Доктор".

София, 23.04.2018 г.

Рецензент:

(проф. д.м.н. Иван Ланджев)