Софийски Университет "св. Климент Охридски"
Факултет по Математика и Информатика

Иван Бойчев Маринов

Дзета функции на линейни кодове и локално крайни модули

АВТОРЕФЕРАТ

за получаване на образователна и научна степен
“доктор”
по професионално направление 4.5 “Математика”
(Алгебра и теория на числата)

научен ръководител: проф. д-р Азнив Киркор Каспарян

София
2 0 1 8

Дисертацията съдържа 169 страници и се състои от 6 глави и литература, включваща 16 заглавия.

Дисертантът работи като старши програмист в Бош Софтуер Иновейшънс

Защитата на дисертационния труд ще се състои на .... от .... часа в аудитория .... на Факултета по математика и информатика на Софийски университет "Св. Климент Охридски",бул. "Джеймс Баучер" № 5, София 1164л

Настоящият дисертационен труд решава някои комбинаторни задачи чрез пораждащи функции на една променлива, използвайки идеи от алгебричната геометрия. От една страна са развити резултати на Дуурсма за изучаване на тегловото разпределение на линеен код C чрез неговата ζ-функция. От друга страна се определя ζ-функция на локално краен модул M над абсолютната група на Галоа $\mathfrak{G} = Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ на крайно поле $\mathbb{F}_q$ и се намира достатъчно условие, при което M изпълнява аналога на хипотезата на Риман относно проективната права $\mathbb{P}^1(\overline{\mathbb{F}_q})$. Разглежданията за линейни кодове установяват, че тъждествата на Мак Уилямс за тегловото разпределение на линеен код C и неговия дуален $C^{\perp}$ са поляризирано обобщение на Теоремата на Риман-Рох за криви. Нека $C \subset \mathbb{F}_q^n$ е $\mathbb{F}_q$-линеен код с дължина n и размерност $k = \dim_{\mathbb{F}_q}(C)$, а $C^{\mathrm{MDS}} \subset \mathbb{F}_q^n$ е MDS-код със същата дължина n и размерност $k = \dim_{\mathbb{F}_q}(C^{\mathrm{MDS}})$ като C. Коефициентите на редуцирания полином на Дуурсма, който изучаваме се оказват удобни параметри за броя на думите с фиксирано тегло, които трябва да отстраним, съответно, да присъединим към C^{MDS}, за да получим C (или код със същото теглово разпределение като C). Известно е, че от аналога на хипотезата на Риман за гладка неприводима крива X следва границата на Хасе-Вайл за броя на рационалните точки на

X. Получените в дисертацията резултати разкриват, че основните предпоставки за изпълнение на аналога на хипотезата на Риман за локално крайни модули M са границата на Хасе-Вайл и наличието на неразклонено покритие $M_o \rightarrow L_o$ с обвивка на Галоа за подмодули $M_o \subseteq M$ и $L_o \subseteq \mathbb{P}^1(\overline{\mathbb{F}_q})$ с най-много крайни допълнения.

Ако $X \subset \mathbb{P}^n(\overline{\mathbb{F}_q})$ е гладка неприводима проективна крива $X \subset \mathbb{P}^n(\overline{\mathbb{F}_q})$, определена над крайно поле $\mathbb{F}_q$ и $N_m := |X \cap \mathbb{P}^n(\mathbb{F}_{q^m})|$ е броят на $\mathbb{F}_{q^m}$-рационалните точки на X, то формалният степенен ред

$$\zeta_X(t) = \exp\left(\sum_{m=0}^{\infty} N_m \frac{t^m}{m}\right),$$

се нарича ζ-функция на X. Проективната права $\mathbb{P}^1(\overline{\mathbb{F}_q})$ има ζ-функция

$$\zeta_{\mathbb{P}^1(\overline{\mathbb{F}_q})}(t) = \frac{1}{(1-t)(1-qt)}.$$

Ако $F = \mathbb{F}_q(X)$ е функционалното поле на X над $\mathbb{F}_q$, то

$$\zeta_X(t) = L_F(T)\zeta_{\mathbb{P}^1(\overline{\mathbb{F}_q})}(t) = \frac{L_F(t)}{(1-t)(1-qt)}$$

за полином $L_F(t) \in \mathbb{Z}[t]$, който се нарича ζ-полином на кривата. По определение, ζ-полиномът и ζ-функцията на крива X съдържат пълна информация за броя на рационалните точки на X.

Изследванията на настоящата дисертационна работа са силно повлияни и вдъхновени от трудовете на Иван Дуурсма [Duursma1] и [Duursma2]. В тези статии той въвежда и изучава ζ-полинома на линеен код C, който задава еднозначно тегловото разпределение на кода. Чрез алгебро-геометрична реализация на C като код на Гоппа върху крива X, Дуурсма свързва ζ полинома на C с този на X. Той представя тегловия полином на линеен код C като линейна комбинация на тегловите полиноми на подходящи MDS-кодове с рационални коефициенти $a_i,\ \ 0 \leq i \leq r$. Дуурсма определя ζ-полинома на C като

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

и ζ-функцията на C като

$$\zeta_C(t) = \frac{P_C(t)}{(1-t)(1-qt)}.$$

Той доказва, че ζ-полиномът $P_C(t)$ на линеен код C е свързан с ζ-полинома $P_{C^\perp}(t)$ на неговия дуален $C^\perp$ посредством функционалното уравнение

$$P_{C^\perp}(t) = P_C\left(\frac{1}{qt}\right) q^g t^{g+g^\perp},$$

което заедно с условието $P_C(1) = P_{C^\perp}(1) = 1$ еквивалентно на тъждествата на Мак Уилямс за тегловото разпределение на C и на $C^\perp$. В частност,

$$P_C\left(\frac{1}{q}\right) = P_{C^\perp}(1)q^{-g} = \frac{1}{q^g}$$

и полиномът $P_C(t) - t^g \in \mathbb{Q}[t]$ се анулира за $t = 1$ и $t = \frac{1}{q}$. Дуурсма забелязва, че

$$D_C(t) := \frac{P_C(t) - t^g}{(1-t)(1-qt)} \in \mathbb{Q}[t]$$

е полином с рационални коефициенти, но не използва този полином за изучаване на тегловото разпределение на C и $C^\perp$. Някои ключови резултати от глави 4 и 5 са свързани със свойствата на $D_C(t)$, който наричаме редуциран полином на Дуурсма.

Мотивацията, както и терминологията на настоящия дисертационен труд са отражение на свойствата на проективните криви, определени над крайно поле. Съгласно статията [PShW] на Пеликаан, Шен и ван Уи, всеки линеен код може да се реализира като алгеброгеометричен код на Гопа, т.е. като множество от стойности на пространство на Риман-Рох на дивизор върху крива в краен брой точки на тази крива. При такава реализация, точките от проективизацията на кода могат да се разглеждат като ефективни дивизори от фиксиран клас на линейна еквивалентност. Затова сумата на ζ-функциите на алгебро-геометричните кодове, отговарящи на пълна система представители на класовете на линейна еквивалентност на дивизорите от фиксирана степен, се оказва равна на ζ-функцията на кривата.

Статията [KM1] изучава тегловото разпределение на линеен код C чрез редуцирания полином на Дуурсма $D_C(t)$ на C. Тя установява, че коефициентите на $D_C(t)$ изразяват разликата на тегловия полином на C и тегловия полином на MDS-код C^{MDS} със същата дължина и размерност като C относно мономи на хомогенните линейни полиноми $x - y$ и y. С помощта на $D_C(t)$, работата [KM2] доказва, че тъждествата на Мак Уилямс за тегловото разпределение на C и $C^{\perp}$ са еквивалентни на поляризирани условия на Риман-Рох.

В светлината на [PShW], линейните кодове могат да се разглеждат като комбинаторни разновидности на линейните системи от дивизори върху алгебрична крива X. Абстрахирайки някои свойства на действието на абсолютната група на Галоа $\mathfrak{G} = Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ на крайно поле $\mathbb{F}_q$ върху гладка неприводима крива $X \subset \mathbb{P}^n(\overline{\mathbb{F}_q})$, определена над $\mathbb{F}_q$, въвеждаме понятието локално краен модул M над $\mathfrak{G} = Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$. Наличието на взаимно еднозначно съответствие между $\mathfrak{G} = Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-орбитите върху X и класовете дискретни нормирания на функционалното поле $F = \mathbb{F}_q(X)$ на X позволява определянето на ζ-функция $\zeta_M(t)$ на M. Съгласно Теоремата на Хасе-Вайл, частното

$$L_F(t) := \frac{\zeta_X(t)}{\zeta_{\mathbb{P}^1(\overline{\mathbb{F}_q})}(t)} = (1-t)(1-qt)\zeta_X(t)$$

на ζ-функцията $\zeta_X(t)$ на X и ζ-функцията $\zeta_{\mathbb{P}^1(\overline{\mathbb{F}_q})}(t)$ на проективната права $\mathbb{P}^1(\overline{\mathbb{F}_q})$ е полином, чиито корени са с модул $\frac{1}{\sqrt{q}}$. Този резултат е еквивалентен на $\mathrm{Re}(s_o) = \frac{1}{2}$ за комплексните корени $s_o \in \mathbb{C}$ на функцията $L_F(q^{-s})$ на комплексна променлива $s \in \mathbb{C}$ и се нарича аналог на хипотезата на Риман. Статията [KM3] доказва достатъчно условие, при което локално краен $\mathfrak{G} = Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-модул M изпълнява аналога на хипотезата на Риман относно $\mathbb{P}^1(\overline{\mathbb{F}_q})$. Споменатото достатъчно условие се състои от три предположения. Първото предположение е, че частното

$$P_M(t) := \frac{\zeta_M(t)}{\zeta_{\mathbb{P}^1(\overline{\mathbb{F}_q})}(t)}$$

на ζ-функцията $\zeta_M(t)$ на M и ζ-функцията $\zeta_{\mathbb{P}^1(\overline{\mathbb{F}_q})}(t)$ на проективната права е полином $P_M(t)$ с цели коефициенти. Второто предположение изисква съществуването на $\mathfrak{G}$-подмодули $M_o \subseteq M$, съответно, $L_o \subseteq \mathbb{P}^1(\overline{\mathbb{F}_q})$ с най-много крайни допълнения $M \setminus M_o$, $\mathbb{P}^1(\overline{\mathbb{F}_q}) \setminus L_o$, които са свързани с крайно неразклонено покритие $\xi : M_o \to L_o$, притежаващо обвивка на Галоа. Третото изискване е аналог на границата на Хасе-Вайл за броя на рационалните точки на крива X и се формулира като неравенство между порядъка на Хасе.Вайл на M и $\lambda := \log_q \sqrt[d]{|LC(P_M(t))|} \in \mathbb{R}^{\geq 0}$, където $LC(P_M(t)) \in \mathbb{Z} \setminus \{0\}$ е старшият коефициент на $P_M(t)$.

Накратко за съдържанието на настоящия дисертационен труд. Следващите две глави се състоят от предварителни сведения. Глави 4, 5 и 6 отразяват, съответно, резултатите на публикациите [KM1], [KM2] и [KM3].

Глава 2 съдържа предварителни сведения от областта на алгебричната геометрия. Първият параграф е посветен на взаимно еднозначното съответствие между класовете дискретни нормирания ν на функционалните полета $\mathbb{F}_q(X)$ на алгебричните криви X и техните локални пръстени $\mathcal{O}_\nu$. Напомня се класификацията на дискретните нормирания ν на чисто трансцендентно разширение $\mathbb{F}_q(x)$ на полето от коефициенти $\mathbb{F}_q$ и техните пръстени $\mathcal{O}_\nu$. Доказва се, че всички нормирания на функционално поле $\mathbb{F}_q(X)$ на крива X са дискретни и съответните им полета от остатъци $\mathcal{O}_\nu / \mathfrak{M}_\nu$ са крайни разширения на $\mathbb{F}_q$. Подробно се дискутира Апроксимационната теорема за краен брой дискретни нормирания и краен брой елементи, както и наличието на разлагане в Лоранов ред на произволна рационална функция $f \in \mathbb{F}_q(X)$ относно локален параметър t на $\mathcal{O}_\nu$. Тези факти се използват във втората част на параграф 3 за извеждане на съответствието между пръстените на дискретно нормиране на $\mathbb{F}_q(X)$ и орбитите на $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$, в четвъртия параграф за изучаване на дивизорите на рационални функции върху крива, както и в параграф 5 за получаване на горна граница върху броя на рационалните точки на крива. Вторият параграф на глава 2 разглежда някои свойства на действието на абсолютната група на Галоа $\mathfrak{G} = Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ на крайно поле $\mathbb{F}_q$ върху афинно или проективно пространство или многообразие. Дискутира се топологията на Зариски, структурата на Зариски затворената обвивка и неприводимостта на многообразие. Третият параграф на глава 2 обяснява подробно съответствието между гладките точки на неприводима крива $X \subset \mathbb{P}^n(\overline{\mathbb{F}_q})$, определена над $\mathbb{F}_q$ и пръстените на дискретно нормиране на $\overline{\mathbb{F}_q}(X)$, както и съответствието между $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-орбитите върху X и пръстените на дискретно нормиране на $\mathbb{F}_q(X)$. Напомнени са основните свойства на дивизорите върху крива $X \subset \mathbb{P}^n(\overline{\mathbb{F}_q})$ и техните пространства на Риман-Рох. Изложено е доказателството на Теоремата на Риман за дивизор върху крива. Детайлно е разгледан случаят на равенство и е формулирана Теоремата на Риман-Рох. Последният, пети параграф на глава 2 излага доказателството на горна граница върху броя на рационалните точки на гладка неприводима крива $X \subset \mathbb{P}^n(\overline{\mathbb{F}_q})$, която мотивира даденото в [KM3] определение за порядъка на Хасе-Вайл на локално краен $\mathfrak{G} = Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-модул относно проективната права $\mathbb{P}^1(\overline{\mathbb{F}_q})$.

В глава 3 са събрани някои предварителните сведения от теория на кодирането, които се концентрират около тъждествата на Мак Уилямс. Първият параграф напомня основни определения за линейни кодове и алгебро-геометричните кодове на Гопа. Вторият параграф дискутира тъждествата на Мак Уилямс за тегловото разпределение на двойка дуални линейни кодове в техния класически вид. Последните два параграфа са посветени на резултати на Дуурсма от [Duursma1], [Duursma2] и [Duursma3]. Третият параграф дава две еквивалентни определения за ζ-полинома $P_C(t)$ на линеен код $C \subset \mathbb{F}_q^n$. Четвъртият параграф доказва връзката между ζ-полиномите $P_{C_i}(t)$ на алгебро-геометричните кодове на Гопа, асоциирани с пълна система представители G_i на класовете на линейна еквивалентност на дивизорите от подходяща фиксирана степен върху крива X с ζ-полинома $L_{\mathbb{F}_q(X)}$ на X. Тя изрязява тъждествата на Мак Уилямс за C и $C^\perp$ във вид на функционално уравнение на техните ζ-полиноми $P_C(t)$, съответно, $P_{C^\perp}(t)$.

Глава 4 отразява резултатите на статията [KM1]. Тя е посветена на редуцирания полином на Дуурсма

$$D_C(t) := \frac{P_C(t) - t^g}{(1-t)(1-qt)} \in \mathbb{Q}[t]$$

на линеен код C от род g с ζ-полином $P_C(t)$. В своята статия [Duursma3] Дуурсма забелязва съществуването на $D_C(t)$, но не използва този полином за описание на тегловото разпределение на C. Нека C е $\mathbb{F}_q$-линеен код от род g с дуален $C^\perp$ от род $g^\perp$, $\mathcal{W}_C(x,y) \in \mathbb{Z}[x,y]$ е тегловият полином на C, а $\mathcal{M}_{n,n+1-k}(x) \in \mathbb{Z}[x,y]$ е тегловият полином на MDS-код със същата дължина n и размерност k като C. Първият параграф на глава 4 използва коефициентите на редуцирания полином на Дуурсма $D_C(t) \in \mathbb{Q}[t]$ на C за изразяване на $\mathcal{W}_C(x,y) - \mathcal{M}_{n,n+1-k}(x,y) \in \mathbb{Z}[x,y]$ като хомогенен полином на $x-y$ и y от степен n. В резултат, $D_C(t)$ определя еднозначно броя на думите с фиксирано тегло, които трябва да се присъединят, съответно, отстранят от MDS-код C^{MDS} със същата дължина n и размерност k като C, за да се получи C (или код със същото теглово разпределение като C). Във втория параграф се проверява, че линейните кодове C, изпълняващи аналога на хипотезата на Риман са формално самодуални. Тегловото разпределение на формално самодуален код C от род g се характеризира чрез половината на коефициентите на редуцирания полином на Дуурсма $D_C(t)$ на C.

Установено е, че тегловото разпределение на формално самодуален код с размерност k и минимално разстояние d се определя напълно от броя на думите на C с тегло $d \leq w \leq k$. Ако C е формално самодуален код от род g,то редуцираният полином на Дуурсма $D_C(t) \in \mathbb{Q}[t]$ на C е от степен $\deg(D_C(t)) = 2g - 2$. Кодовете с постоянен редуциран полином на Дуурсма $D_C(t) = c_o \in \mathbb{Q}$ са почти MDS-кодовете, изучени от Додунеков и Ланджев в [Додунеков, Ланджев]. Резултатите на Ким и Хюн от [Kim, Hyun] характеризират почти MDS-кодовете, изпълняващи аналога на хипотезата на Риман. Параграф 2 от глава 4 дава необходимо и достатъчно условие, при което формално самодуален код с квадратичен полином на Дуурсма изпълнява аналога на хипотезата на Риман. Третият параграф на глава 4 изучава редуцирания полином на Дуурсма, $D_{\mathbb{F}_q(X)}(t) \in \mathbb{Z}[t]$ на функционално поле $\mathbb{F}_q(X)$ на гладка неприводима крива $X \subset \mathbb{P}^n(\overline{\mathbb{F}_q})$ от род g, определена над $\mathbb{F}_q$. Той доказва, че коефициентите на $D_{\mathbb{F}_q(X)}(t)$ се определят еднозначно от броя на ефективните дивизори върху X от степен $\leq g - 1$. Частното

$$\frac{D_{\mathbb{F}_q(X)}(t)}{(1-t)(1-qt)}$$

се характеризира с редица свойства на ζ-функцията на гладка неприводима проективна крива от род $g - 1$, определена над $\mathbb{F}_q$.

Петата глава на настоящия дисертационен труд е посветена на еквивалентностата на тъждествата на Мак Уилямс за тегловото разпределение на линеен код C и неговия дуален $C^{\perp}$ с поляризираните условия на Риман-Рох за техните ζ-функции

$$\zeta_C(t) := \frac{P_C(t)}{(1-t)(1-qt)}, \quad \text{съответно,}$$

$$\zeta_{C^{\perp}}(t) := \frac{P_{C^{\perp}}(t)}{(1-t)(1-qt)}.$$

Този резултат разкрива общата природа на споменатите класически резултати от теория на кодирането и алгебричната геометрия. Той позволява разглеждането на тъждествата на Мак Уилямс като поляризиран вариант на Теоремата на Риман-Рох и двойствеността на Сер върху гладка неприводима крива X. Първият параграф на глава 5 въвежда поляризираните условия на Риман-Рох за двойка формални степенни редове и мотивира тяхното определение с условията на Риман-Рох върху крива. Той изразява тъждествата на Мак Уилямс за двойка дуални линейни кодове C, $C^{\perp}$ чрез поляризираните условия на Риман-Рох за съответните ζ-функции $\zeta_C(t)$, $\zeta_{C^{\perp}}(t)$. Вторият параграф на глава 5 предоставя усредняващи и вероятностни интерпретации на коефициентите на редуцирания полином на Дуурсма $D_C(t)$ на линеен код C.

Последната глава 6 дава достатъчно условие за изпълнение на аналога 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 $\mathbb{F}_q$. Нейните разглеждания обобщават хипотезите на Вайл за гладка неприводима проективна крива X, определена над $\mathbb{F}_q$. Исторически, ζ-функцията $\zeta_X(t)$ на X е въведена от Артин през 1923 г. Теоремата на Хасе-Вайл за X гласи, че

$$\zeta_X(t) = \frac{L_{\mathbb{F}_q(X)}(t)}{(1-t)(1-qt)}$$

за полином $L_{\mathbb{F}_q(X)}(t) \in \mathbb{Z}[t]$, чиито корени се намират върху окръжността в комплексната равнина $\mathbb{C}$ с начало $0 \in \mathbb{C}$ и радиус $\frac{1}{\sqrt{q}}$. Случаят на елиптична крива X е доказан от Хасе през 1936 г. Андре Вайл установява верността на теоремата за произволна гладка неприводима проективна крива X през 1940 г. Разглежданията от глава 6 обобщават доказателството на Бомбиери от [Bombieri] на Теоремата на Хасе-Вайл. Те предоставят критерий или достатъчно условие за изпълнение на аналога на хипотезата на Риман за локално краен $\mathfrak{G} = Gal(\overline{\mathbb{F}_q}/\mathbb{F}_Q)$-модул M относно проективната права $\mathbb{P}^1(\overline{\mathbb{F}_q})$. Критерият се състои от три предположения.

Първо изискваме частното

$$P_M(t) := \frac{\zeta_M(t)}{\zeta_{\mathbb{P}^1(\overline{\mathbb{F}_q})}(t)}$$

на ζ-функцията $\zeta_M(t)$ на M и ζ-функцията $\zeta_{\mathbb{P}^1(\overline{\mathbb{F}_q})}(t)$ на $\mathbb{P}^1(\overline{\mathbb{F}_q})$ да е полином $P_M(t) = \sum\limits_{i=0}^{d} a_i t^i$. Второ, предполагаме съществуването на покритие $\xi : M \dashrightarrow \mathbb{P}^1(\overline{\mathbb{F}_q})$ с обвивка на Галоа. Дефиниционната област M_o на ξ и областта от стойности $\xi(M_o)$ са с крайно допълнение в M, съответно, в $\mathbb{P}^1(\overline{\mathbb{F}_q})$. Обвивката на Галоа се състои от локално краен $\mathfrak{G}_m = Gal(\overline{\mathbb{F}_q}/\mathbb{F}_{q^m})$-модул N за някакво крайно разширение $\mathbb{F}_{q^m} \supset \mathbb{F}_q$ и крайни групи $H_1 < H$ от $\mathfrak{G}_m$-еквивариантни биекции $N \to N$ без фиксирани точки, така че изображението $\xi_H : N \to N/H = \xi(M_o)$, $\xi_H(z) = \mathrm{Orb}_H(z)$, съпоставящо на точка $z \in N$ нейната H-орбита се пропуска през $\xi_{H_1} : N \to N/H_1 = M_o$ и неразклоненото покритие $\xi : M_o \to \xi(M_o)$. Третото предположение на критерия за изпълнение на аналога на хипотезата на Риман относно $\mathbb{P}^1(\overline{\mathbb{F}_q})$ е горна граница върху относителната скорост на растене на броя на рационалните точки на M относно броя на рационалните точки на $\mathbb{P}^1(\overline{\mathbb{F}_q})$. Споменатата граница зависи от степента и старшия коефициент на ζ-полинома $P_M(t)$. Тя може да се разглежда като обобщение на класическата граница на Хасе-Вайл за броя на рационалните точки върху гладка неприводима проективна крива, определена над $\mathbb{F}_q$. Конструиран е пример за локално краен модул M над $\mathfrak{G} = Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$, изпълняващ предположенията на дискутирания критерий, а оттам и аналога на хипотезата на Риман относно $\mathbb{P}^1(\overline{\mathbb{F}_q})$, който не е изоморфен като $\mathfrak{G}$-модул на гладка неприводима проективна крива X, определена над $\mathbb{F}_q$. Установено е, че от аналога на хипотезата на Риман за локално краен $\mathfrak{G} = Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-модул M относно $\mathbb{P}^1(\overline{\mathbb{F}_q})$ следва функционалното уравнение за ζ-полинома $P_M(t)$ на M.

Публикации във връзка с дисертацията

1. Duursma's reduced polynomial, A. Kasparian, I. Marinov, Advances in Mathematics of Communication, vol. 11, № 4, November 2017.

2. Mac Williams identities and polarized Riemann-Roch conditions, A. Kasparian, I. Marinov, Electronic Notes in Discrete Mathematics, vol. 57, 2017.

3. Riemann Hypothesis Analogue for locally finite modules over the absolute Galois group of a finite field, A. Kasparian, I. Marinov, accepted for a publication in Annuaire de l'Université de Sofia "St. Kl. Ohridski"

Апробация на резултатите

Резултатите на дисертацията са докладвани на следните научни форуми:

1. ”Tangent codes”, A. Kasparian, E. Velikova, I. Marinov, Международна конференция ”Дни на математиката в София”, 7 - 10 юли 2014 г.

2. ”Някои интерпретации на тегловия полином на линеен код”, А. Каспарян, И. Маринов, Национален семинар по кодиране ”Акад. Стефан Додунеков”, 20-23 ноември 2014г.

3. ”Редуциран полином на Дуурсма”, А. Каспарян, И. Маринов, Юбилейна конференция ”125 години математика и природни науки в Софийски университет "Св. Климент Охридски”, 5 - 7 декември 2014 г.

4. ”Фамилии на Гоппа от линейни кодове”, А. Каспарян, И. Маринов, Пролетна научна сесия на Факултета по математика и информатика на Софийски университет ”Св. Климент Охридски”, 28 март 2015 г.

5. ”Нелинейни кодове на Гоппа”, А. Каспарян, И. Маринов, Национален семинар по кодиране ”Акад. Стефан Додунеков”, 19-22 ноември 2015 г.

6. ”Mac Williams identities for linear codes as Riemann-Roch conditions”, A. Kasparian, I. Marinov, 18-24 юни 2016 г.

7. ”Локално крайни модули над топологично циклична про-крайна група”, А. Каспарян, И. Маринов, Пролетна научна сесия на Факултета по математика и информатика на Софийски университет ”Св. Климент Охридски”, 26 март 2016 г.

8. ”Riemann Hypothesis Analogue for locally finite modules over the absolute Galois group of a finite field”, A. Kasparian, I. Marinov, International Conference ”Groups and Rings - Theory and Applications”, (GRiTA 2016), 11-15 юли 2016 г.

9. ”Унитарни симетрии на локално крайни модули”, А. Каспарян, И. Маринов, Пролетна научна сесия на Факултета по математика и информатика на Софийски университет ”Св. Климент Охридски”, 25 март 2017 г.

Докладите с номера 4, 5, 6, 7, и 9 са изнесени от Иван Маринов, а тези с номера 1, 2, 3 и 8 са изнесени от Азнив Каспарян.

Библиография

[Bombieri] E. Bombieri, Counting Points on Curves over Finite Fields, Sém. Bourbaki, No. 430, 1972/73.

[Додунеков, Ланджев] S. Dodunekov and I. Landgev, Near MDS-codes, *Journal of Geometry*, **54** (1995), 30–43.

[Duursma1] I. Duursma, From weight enumerators to zeta functions, *Discrete Applied Mathematics*, **111** (2001), 55—73.

[Duursma2] I. Duursma, Weight distribution of geometric Goppa codes, *Transections of the American Mathematical Society*, **351** (1999), 3609–3639.

[Duursma3] I. Duursma Combinatorics of the two-variable zeta function in *In: Mullen G.L., Poli A., Stichtenoth*

H. (eds) Finite Fields and Applications. Lecture Notes in Computational Sciences **2948**, Springer, Berlin, Heidelberg (2004), 109–136.

[KM1] A. Kasparian, I. Marinov, Duursma's reduced polynomial, Advances in Mathematics of Communication, vol. 11, № 4, November 2017.

[KM2] A. Kasparian, I. Marinov, Mac Williams identities and polarized Riemann-Roch conditions, Electronic Notes in Discrete Mathematics, vol. 57, 2017.

[KM3] A. Kasparian, I. Marinov, Riemann Hypothesis Analogue for locally finite modules over the absolute Galois group of a finite field, accepted for a publication in Annuaire de l'Université de Sofia "St. Kl. Ohridski"

[Kim, Hyun] D. Ch. Kim and J. Y. Hyun, A Riemann hypothesis analogue for near-MDS codes, *Discrete Applied Mathematics*, **160** (2012), 2440–2444.

[Mustaţă] M. Mustaţă, *Zeta Functions in Algebraic Geometry*, Lecture Notes of Mihnea Popa.

[Niederreiter, Xing] Niederreiter H., Xing Ch., *Algebraic Geometry in Coding Theory And Cryptography*, Princeton University Press, 2009

[PShW] R. Pellikaan, B.-Z. Shen, G. J. M. van Wee, Which linear codes are algebraic geometric?, IEEE Trans. Inform. Theory **IT-37** (1991), 583-602.

[Shafarevich] Shafarevich, I.R., *Basics of Algebraic Geometry*, (Science, Moscow, 1988).

[Stichtenoth] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer, 1993.

[Tsafman, Vladut, Nogin] M. Tsfasman, S. Vlădut, D. Nogin, *Algebraic Geometry Codes: Basic Notions,* Providence, RI: American Mathematical Society, 2007

[Ward] H. K. Ward, The Mac Williams Identity, Preprint.