РЕЦЕНЗИЯ
от д-р Никола Петков Зяпков,
професор във ФМИ при ШУ „Еп. Константин Преславски”

на дисертационния труд на тема „Крайни геометрии и кодове” с автор Ася Петрова Русева за придобиване на научната степен “доктор на науките” в област на висше образование: 4. Природни науки, математика и информатика, професионално направление: 4.5. Математика, докторска програма „Геометрия”.

Общо описание на представените материали

Със заповед № Р 38-186/ 14.05.2020 на Ректора на Софийския университет „Св. Климент Охридски“, съм определен за член на научното жури във връзка с процедурата за защита на дисертационния труд на тема „Крайни геометрии и кодове ” с автор доц. д-р Ася Петрова Русева за придобиване на научната степен „доктор на науките” в област на висше образование 4. Природни науки, математика и информатика, професионално направление 4.5. Математика, докторска програма „Геометрия” .
Представеният от доц. Русева комплект материали е в съответствие с Правилника на СУ за прилагане на ЗРАСРБ .

Актуалност на тематиката и целесъобразност на поставените цели и задачи

Дисертационният труд е посветен на изследвания в областта на крайните геометрии, имащи връзка с теорията на шумозащитните кодове. Съвременната теория на кодирането започва с основополагащата статия на Шенон от 1948 г.
C. E. Shannon, A mathematical theory of communication,
Bell Syst. Tech. J., 27 (1948), 379-423, 623-656.

Тя възниква като опит да се реши следният Основен проблем при предаването на информация на разстояние:

Появяване на грешки в резултат на смущения по канала.

В годините след появяването на работата на Shannon линейните кодове се превръщат в най-изследвания клас блокови кодове. Наличието на хубава математическа структура ги прави лесни за описание и анализ и води до ефективни алгоритми за декодиране. Линейните кодове над крайно поле с q елемента имат три основни параметра дължина n, размерност k и минимално разстояние d и се записват така: $(n,k,d)_q$. Най-добрите кодове измежду всички с фиксирани два от тези параметри са тези, за които третият параметър е оптимален. Естествена долна граница за дължината n е т. нар. граница на Griesmer . Една от основните задачи на теорията на кодирането е намиране на кодове, които достигат известните граници,

а когато такива кодове не съществуват, подобряване на съществуващите граници и намиране на кодовете с най-добри параметри.

През 80-те и 90-те години на XX век се изяснява, че основната задача на теория на кодирането има геометрична природа и може да се формулира естествено като задача за разполагане на точки в проективна геометрия над крайно поле.

През последните години бяха доказани няколко важни резултата за оптимални кодове над крайни полета. Всички те се получават като резултати за специални множества от точки в крайни геометрии. Тези резултати са получени от S. Ball, H. N. Ward, A. Bruen, A. Blokhuis, F. Mazzocca и др.

Характеристика и оценка на дисертационния труд

Дисертационният труд е структуриран в увод (даден е като глава първа), четири глави, и цитирана литература с общ обем 180 стр. Списъкът от цитирана литература включва 201 заглавия на статии и монографии.

В увода е даден кратък исторически преглед на резултатите ,получени за оптимални кодове над крайни полета които са получени като твърдения за специални множества от точки в крайни геометрии.

Също така накратко е направен кратък преглед на съдържанието на дисертацията.

Втора глава има важно място в представения труд. Дадени са основни понятия и предварителни резултати , необходими в следващите глави. В §2.1 са въведени координатните проективни пространства PG(r, q) над полетата F_q и са формулирани фундаментални теореми на проективната геометрия. Въведени са арки и блокиращи множества като специални мултимножества от точки в PG(r, q). Представени са специални конструкции на арки, най-важните от които са проектиране от подпространство и конструиране на σ-дуална арка. В §2.2 са описани редица класове от арки и е представена класификацията на арки в малки проективни равнини. § 2.3 е посветен на линейни кодове над крайни полета. Въведени са основните понятия и са представени някои класически граници: границите на Singleton, Gilbert-Varshamov, обобщената граница на Singleton и границата на Griesmer. В § 2.4 е описана връзката между линейните кодове имултимножествата от точки в геометриите PG(r, q). Изложени са геометричните версии на принципни резултати като теоремата на Ward за делимост на кодове, лежащи на границата на Griesmer и теоремата за разширимост на Hill и LlZAK. Описани са и подобрения на теоремата на Hill-Lizak, следващи от един резултат на Beutelspacher за блокиращи множества. В края на раздела е представено съответствие между някои понятия от теория на кодирането и крайните геометрии.

§ 2.3 е посветен на линейни кодове над крайни полета. Въведени са основните понятия и са представени някои класически граници: границите на Singleton, Gilbert-Varshamov, обобщената граница на Singleton и границата на Griesmer. В раздел 2.4 е описана връзката между линейните кодове

мултимножествата от точки в геометриите PG(r, q). Изложени са геометричните версии на принципни резултати като теоремата на Ward за делимост на кодове, лежащи на границата на Griesmer и теоремата за разширимост на Hill и Lizak. Описани са и подобрения на теоремата на Hill-Lizak, следващи от един резултат на Beutelspacher за блокиращи множества. В края на раздела е представено съответствие между някои понятия от теория на кодирането и крайните геометрии.

В следващите три глави се съдържат оригиналните резултати в дисертационния труд.

Основна тема в трета глава е достижимостта на границата на Griesmer

$$n > g_q(k,d) := \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil$$

и геометрична характеризация на кодовете, които лежат на нея.

Кодове, лежащи на тази граница се наричат кодове на Griesmer, а асоциираните с тях арки — арки на Griesmer.

От съществено значение е да се изследва поведението на функцията $t_q(k)$, задаваща отклонението на оптималната дължина на код от стойността, зададена от границата на Griesmer:

$$t_q(k) := \max(n_q(k,d) - g_q(k,d)).$$

Стефан Додунеков първи доказва, че ако се фиксира d и k расте неограничено, то $(n_q(k,d) - g_q(k,d)) \to \infty$, откъдето и $t_q(k) \to \infty$. В § 3.1.-3.3 се изследва скоростта на това нарастване.

В началото на §3.1 е приведено ново доказателство на теоремата на Додунеков за неограниченото нарастване на $t_q(k)$ като функция на k. След това са представени няколко резултата, опростяващи изследването на $t_q(k)$. Най-важен от тях е следният.

Лема 3.6. *Ако nq(k, d) = gq(k, d) +t, то nq(k, d + qk-1) < gq(k, d + qk-1) +t.*

Основен резултат в § 3.2 е Теорема 3.10, която може да се разглежда като обобщение на конструкцията на Белов, Логачев и Сандимиров.

Важен резултат в §3.3 е доказателство на хипотезата на Ball за арки в дезаргови равнини от четен ред.

В § 3.4 са намерени нови точни стойности на $n_q(k, d)$ за $q = 4$, $k = 5$. За кодове над F_4, $k = 5$ е най-малката размерност, при която съществуват минимални разстояния d, за които точната стойност на $n_4(5, d)$ не е намерена. Характеризацията на арките с параметри (118, 30) се съдържа в Леми 3.20-3.25 Една (118, 30)-арка в PG(3, 4) е от един от следните типове (а) K = 2 — F, където F е (52,12)-блокиращо множество, а F е сума на две равнини и две прави, взети така, че максималната кратност на точка да бъде 2. Описани са двата възможни спектъра.

Доказани са и следните твърдения:

- Всяка (117, 30)-арка в PG(3, 4) е разширима.
- Неразширимата (100, 26)-арка в PG(3, 4) е единствена.

До края на главата са изложени доказателства за несъществуване на арки, които се асоциират с грийсмърови кодове.

От тези резултати са получени точната стойност на $n_4(5,d)$ за десет минимални разстояния d = 295, 296, 297, 298, 347,..., 352. В края на глава 3 е представена таблица на всички стойности на d, за които въпросът за точната стойност на $n_4(5,d)$ е открит към настоящия момент.

Глава 4 е посветена на изследване на условия за разширимост на арки и, еквивалентно на условия за разширимост на асоциираните с тях линейни кодове. Изследванията по разширимост на арки предхождат тези по разширимост на кодове и протичат независимо от тях. В тази глава е предложен нов геометричен подход към задачата за разширимост, разбирана като формулиране на условия, при които (n,w)-арка в PG(r, q) е разширима до (n+1, w)-арка чрез увеличаване на кратността на една точка. Прави се връзка между разширимостта на дадена арка K със структурата на специална арка K в дуалната геометрия.

В §4.1 се въвеждат (t mod q)-арки. Те се получават при подходящо дуализиране на арки със свойството t-квазиделимост, които на свой ред са асоциирани с кодове на Griesmer с минимално разстояние

$d \equiv -t \pmod q$.Основен резултата в този параграф е следният: Достатъчно условие за с-кратна разширимост на t-квазиделима арка K е дуалната арка K да е сума на c хиперравнини и някоя друга арка(следва от Т4.3)

В § 4.2 се изследва структурата на (t mod q)-арки без връзка със задачата за разширимост. Основен резултат в този параграф е

Теорема 4.12. *Векторното пространство на всички* (0 mod p)*-арки в* PG(r,p) *се поражда от допълненията на хиперравнините.*

§ 4.3 е посветен на изследване на (t mod q)-арки, в които максималната кратност на точка е t. Основен резултат в този параграф е:

Теорема 4.21. *Всяка* (3 mod 5)*-арка F в* PG(3, 5) *с мощност* $|F| < 158$ *е получена чрез лифтинг от 3-точка. По-специално,* $|F| = 93,118$ *или* 143.

Този резултат се използва по-нататък за доказване на несъществуването на (104, 22)-арки в PG(3, 5) в § 4.5.

В § 4.4 се изследва разширимост на грийсмърови арки, имащи свойството t-квазиделимост по модул q. Основният резултат е доказан в Т4.27, който за линейни кодове се формулира по следния начин:

Нека C е код на Griesmer *с параметри* $[n, k, d]_q$*, притежаващ свойството t-квазиделимост. Нека d е представен във вида*

$$d = sq^{k-1} - \sum_{i=0}^{k-2} \varepsilon_i q^i,$$

където $0 \le \varepsilon_i < q$ *за всички* $i = 0, \ldots, k-2$. *Ако за числата* ε_i *са изпълнени неравенствата*

$$t = \varepsilon_0 < \sqrt{q}, \varepsilon_1 < \sqrt{q}, \ldots, \varepsilon_{k-2} < \sqrt{q},$$

то C е t-разрешим, т.е. съществува линеен код с параметри $[n+t, k, d+t]_q$.

В § 4.5 е доказано несъществуването на (104, 22)-арки в PG(3, 5) и на асоциираните с тях $[104, 4, 82]_5$-кодове.

Глава 5 е посветена на конструирането на афинни блокиращи множества. Изследва се задачата за намиране на минималната мощност на афинно блокиращо множество по отношение на хиперравнините. Тази задача има връзка с теория на кодирането: съществуването на афинни блокиращи множества е еквивалентно на съществуването на думи с голямо тегло (близко да дължината на кода) в линейни кодове над крайни полета.

§ 5.1 съдържа обзор на известните долни граници за мощността на блокиращо множество в AG(n,q).

В §5.2 е описана нова обща конструкция, даваща афинни блокиращи множества, които са оптимални или близки до оптималните. Тази конструкция е направена в Т5.6.

В раздел 5.3 са представени редица приложения на общата конструкция от Теорема 5.6 и следствията от нея, даващи добри блокиращи множества. Така например, като специален случай на следствие 5.7 се получава и Теорема 5.12, в която се получава нов клас от афинни блокиращи множества, лежащи на границата на Bruen.

Приноси на дисертационния труд

След запознаване с дисертационния труд, констатирам, че основните цели и задачи на дисертацията са изпълнени. Приемам приносите, описани в заключението на дисертационния труд, а именно:

- Изследвано е нарастването на функцията $t_q(k)$, дефинирана като максималното отклонение от границата на GRIESMER на оптимален q-ичен код с размерност k. Доказано е, че за четни размерности е в сила $t_q(k) \leq q^{k/2}$. В случая k = 4 е доказано неравенството $t_q(4) \leq q - 1$.

- Доказано е неравенството $t_q(3) < \log_2 q$ — 1 в случая, когато q е четно число. Това решава частично една хипотеза на S. Ball за равнинни арки (тримерни кодове). За четни степени на нечетни прости числа q е доказано по-слабото неравенство $t_q(3) < \sqrt{q} - 1$.

- Доказано е несъществуване на хипотетични грийсмърови арки (и грийсмърови кодове) в случая q = 4, k = 5 за следните стойности на минималното разстояние d:

d = 295, 296, 297, 298, 347, 348, 349.

- Тези резултати решават 10 случая на задачата за определяне на точната стойност на $n_4(5,d)$ и свежда броя на откритите случаи до 98.

- Въведен е нов геометричен обект (t mod q)-арки (или арки със свръхделимост). Доказано е, че разширимостта на една t-квазиделима арка K е еквивалентна на наличието на хиперравнина в носителя на специална дуална арка K, която е (t mod q)-арка.

- Доказано е, че всяка (0 mod p)-арка, p просто число, е сума на допълненията на хиперравнини. В частност, всяка (t mod p)-арка е сума на арки, получени чрез лифтинг от арки в по-малка размерност. В случая на равнинни арки е доказано, че всяка (t mod p)- арка е сума на не повече от p арки, получени чрез лифтинг.

-Направена е частична характеризация на (3 mod 5)-арки в PG(2, 5) и PG(3,5)

- Доказано е несъществуването на (104, 22)-арки в PG(3,5) и, еквивалентно, на линейни кодове с параметри $[104,4,82]_5$. С това е решен един от четирите открити случая за определяне на точната стойност на $n_5(4,d)$.

- Намерена е обща конструкция за афинни блокиращи множества. Като специален случай е построен нов безкраен клас t-блокиращи множества с $t = q-n+2$, лежащи на границата на Bruen. Това е едва третият пример за блокиращи множества, достигащи границата на Bruen след тривиалните блокиращи множества с t =1 и класа на S. BALL с t = 2. Този клас дава и нови оптимални блокиращи множества за $t = q - n +1$, които лежат на първата граница на S. Ball от 2000 г.

- Построени са пет примера на блокиращи множества, лежащи на границата на S. Ball от 2014 г.: (28, 4) в AG(5,4), (40,4) в AG(9,4), (52,4) в AG(13,4), (64, 4) в AG(17,4), (120,8) в AG(9,8).

Това са първите известни примери, за които тази граница се достига.

Преценка на публикациите по дисертационния труд

Резултатите от дисертацията са публикувани в 7 научни публикации (излезли от печат 6 публикации и една е приета за печат).

Те са представени в следните научни списания:

- [131] *Designs, Codes and Cryptography* , IF 1,224 , Q2.
- [130] *Adv. Math. Comm.* ,IF 0,8 ; Q3.
- [164] *Compt. Rend. Acad. Bulg. des Sciences*,IF 0,321, Q4
- [129] *Ann. de l'Univ. de Sofia* ,Ref: Zhl-MATH
- [127] *Probl. Inf. Transmission*
- [128] *Advances in Mathematics of Communications*
- [165] *Ann. de l'Univ de Sofia (to appear),* Ref: Zhl-MATH
- Самостоятелните публикации на доц. Русева са 2 Останалите са в съавторство с Иван Ланджев.

Представени са 13 цитирания на научните публикации по проблемите на дисертационния труд, от които 11 са в научни статии с импакт фактор.

Публикациите и цитиранията по дисертационния труд удовлетворяват минималните национални изисквания за научната степен „доктор на науките" в професионално направление 4.5. Математика (показател 7-177т. и показател 11-104 т.).

Резултатите от дисертацията са докладвани в голям брой научни конференции у нас и чужбина (това е отразено в дисертацията на стр.15).

Автореферат

Авторефератът е на 28 страници и съдържа основните резултати, получени в дисертационния труд. Той отразява достатъчно пълно съдържанието на дисертационния труд и основните приноси на дисертанта. Авторефератът дава пълна представа за изследваните проблеми, получените резултати и тяхната апробация.

Заключение

Дисертационният труд ***съдържа научни и научно-приложни резултати, които представляват оригинален принос в математиката*** и отговарят на изискванията на Закона за развитие на академичния (ЗРАСРБ) , Правилника за прилагане на ЗРАСРБ и съответния Правилник на СУ „Св. Кл. Охридски“ за научната степен „доктор на науките“ в професионално направление 4.5. Математика.

Представените материали и дисертационни резултати **напълно** съответстват на специфичните изисквания на ФМИ на СУ, приети във връзка с Правилника за прилагане на ЗРАСРБ на СУ.

Поради гореизложеното, давам своята ***положителна оценка*** за проведеното изследване, представено от рецензираните по-горе дисертационен труд, автореферат, постигнати резултати и приноси, и ***предлагам на почитаемото научно жури да присъди научната степен „доктор на науките“*** на доц. д-р Ася Петрова Русева в област на висше образование: 4. *Природни науки, математика и информатика*, професионално направление 4.5. *Математика*, научна специалност *Геометрия.*

Рецензент:

17.06.2020г