Софийски Университет “Св. Климент Охридски”

Факултет по Математика и Информатика

Ася Петрова Русева

КРАЙНИ ГЕОМЕТРИИ И КОДОВЕ

Автореферат

на дисертация
за присъждане на научната степен
“доктор на науките”
по професионално направление
4.5. Математика

София, 2020 г.

Дисертационният труд е в обем от 180 страници и се състои от увод, четири глави и литература, включваща 201 заглавия.

Настоящият дисертационен труд съдържа изследвания по няколко задачи от областта на крайните геометрии, имащи връзка с теория на шумозащитните кодове. Тези два дяла на математиката възникват почти едновременно и независимо един от друг в средата на XX век. За рождена дата на теория на кодирането се приема публикуването на забележителната статия на C.Shannon [50], в която той доказва, че за всяка скорост по-малка от капацитета на използвания канал съществуват блокови кодове, както и правило за декодирането им, за които грешката при декодиране на произволна кодова дума е по-малка от всяка предварително зададена константа. За съжаление, въведените в тази статия стохастични кодове са с такава голяма дължина, че практическото им използване е невъзможно. Така изключително значение придобива обратната теорема: в случаите, когато скоростта на използваните кодове е по-голяма от капацитета на използвания канал, не е възможно предаване на данни с произволно малка грешка при декодиране. От практическа гледна точка изключително важна е задачата за построяване на "добри" кодове и на алгоритми за декодирането им. За "добри" обикновено се считат кодове с параметри, които лежат или са близо до известните теоретични граници.

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. Следва да отбележим, че макар общата задача за декодиране на линеен код по принципа на максималното правдоподобие да е NP-пълна [12], това не изключва наличието на кодове, за които съществува ефективно декодиране.

Активното изследване на крайни геометрични структури започва също около 1950 г., макар отделни разултати да се появяват и по-рано. Така в своята работа [20] по доказване на независимостта на аксиомите за проективно пространство G. Fano изследва възможността четвъртата хармонична точка да съвпада със спрегнатата си. Това води до конструиране на тримерното пространство от 15 точки, 35 прави и 15 равнини, известно днес като $\mathrm{PG}(3,2)$. През 1955 г. B. Segre

доказва в [49], че всяко множество от $q+1$ точки в $\mathrm{PG}(2,q)$, q нечетно, никои три от които не са колинеарни, е коника. В следващите години започва интензивно изследване на крайните геометрии. Същевременно проучванията в теория на кодирането протичат независимо от изследванията в крайните геометрии, което води до пресичане и дори до преоткриване на резултати. През 70-те години на миналия век става все по-забележима дълбоката връзка между определени задачи от теория на кодирането и крайните геометрии. Централни резултати, които повлияват в значителна степен на изследванията са откриването на алгебро-геометричните кодове от В. Гоппа [22, 23, 24], конструирането на 56-шапка в $\mathrm{PG}(5,3)$ от R. Hill [28, 29], както и конструирането от M. Tsfasman, S. Vladut и Th. Zink [54] на алгебро-геометрични кодове, подобряващи границата на Gilbert-Varshamov [21, 55].

През 80-те и 90-те години на XX век се изясни, че т. нар. основна 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. В най-популярния си вид тя се формулира като задача за минимизиране на дължината на линеен код при фиксирани размерност и минимално разстояние. Естествена долна граница за тази дължина е т. нар. граница на Griesmer [26, 51]. От принципно значение е характеризирането на кодовете, лежащи на тази граница. Въпреки значителния напредък, постигнат в работите на Б. И. Белов, В. Н. Логачев, В. П. Сандимиров, С. Додунеков, Н. Манев, И. Буюклиев, N. Hamada, R. Hill, T. Helleseth, H. van Tilborg, T. Maruta, L. Storme и др., решението на тази задача над произволни полета към настоящия момент изглежда недостъпно.

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. Най-важните от тях са следните:

- доказателството на S. Ball за максималната мощност на множество от точки в $\mathrm{PG}(r,p)$, p просто число, намиращи се в общо положение

[2, 8]; това е еквивалентно на прочутата MDS-хипотеза от теория на кодирането за максималната възможна дължина на MDS-код;
- теоремата на H. N. Ward за делимостта на кодове над просто поле, лежащи на границата на Griesmer [56];
- намирането на долна граница за мощността на афинно блокиращо множество в афинните геометрии $\mathrm{AG}(n,q)$ от A. Bruen [15], както и подобряването ѝ от S. Ball и A. Blokhuis [3, 6];
- доказателството на теоремата за несъществуване на максимални арки в равнини от нечетен ред на S. Ball, A. Blokhuis, и F. Mazzocca [5, 7].

В настоящия труд са решени задачи от крайните геометрии, имащи пряко отношение към теория на кодирането. Макар резултатите да са представени като геометрични, те допускат и ясни формулировки в термините на линейни кодове. По-долу ще опишем накратко съдържанието на този труд.

Глава 1. Увод. Първата глава е уводна. Тя съдържа кратки исторически сведения за тематиката, с която се занимаваме. Също така, тук е представен обзор на най-съществените резултати от дисертационния труд.

Глава 2. Предварителни сведения. Тази глава съдържа дефиниции и резултати за множества от точки в крайни геометрии и линейни кодове над крайни полета. Раздел 2.1 е посветен на проективни геометрии над крайни полета. В него се въвеждат координатните проективни пространства $\mathrm{PG}(r,q)$ над полетата $\mathbb{F}_q$ и се формулират т.нар. фундаментални теореми на проективната геометрия. По-нататък се дефинират и понятията арка и блокиращо множество като специални мултимножества от точки в $\mathrm{PG}(r,q)$, в които кратността на хиперравнина е ограничена отгоре (съответно отдолу). Представени са специални конструкции на арки и блокиращи множества, най-важните от които са проектиране от подпространство и конструиране на σ-дуална арка. В раздел 2.2 са описани важни мултимножества от точки като n-арки, (n,w)-арки и n-шапки. Представена е класификацията на някои арки в

малки проективни равнини, които се използват многократно в дисертационния труд. Раздел 2.3 е посветен на линейни кодове над крайни полета. Дефинирани са основни понятия като линеен код, ортогонален код, пораждаща и проверочна матрици, спектър на код. Представени са няколко класически граници за параметрите на линеен код: границите на SINGLETON, GILBERT-VARSHAMOV, обобщената граница на SINGLETON и границата на GRIESMER. В раздел 2.4 се описва връзката между линейните кодове и мултимножествата от точки в геометриите $\mathrm{PG}(r,q)$. Изложени са геометричните версии на важни резултати за линейни кодове като теоремата на H. N. 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 [13] за блокиращи множества. В края на раздела е представено съответствие между някои понятия от теория на кодирането и крайните геометрии.

Следващите три глави съдържат оригиналните резултати в дисертационния труд.

Глава 3. Арки и оптимални кодове. Основна тема в тази глава е достижимостта на границата на GRIESMER и геометричната характеризация на кодовете, които лежат на нея. Съгласно тази граница за всеки линеен код с параметри $[n,k,d]_q$ е изпълнено:

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

Кодове, лежащи на тази граница се наричат кодове на GRIESMER, а асоциираните с тях арки – арки на GRIESMER. Широк клас от кодове на GRIESMER е построен от БЕЛОВ, ЛОГАЧЕВ и САНДИМИРОВ в [11]. Тяхната конструкцията се състои в изтриване на симплекс кодове с малки размерности от конкатенация на симплекс-кодове с размерност k. Геометрично тази конструкция е по-естествена: тя се състои в изтриване на блокиращо множество от определен брой копия на $\mathrm{PG}(k-1,q)$. Най-малката дължина n, за която съществува $[n,k,d]_q$-код при фиксирани k, d и q бележим с $n_q(k,d)$. Много полезно за по-нататъшните изследвания

се оказва представянето на d във вида

$$d = sq^{k-1} - \lambda_{k-2}q^{k-2} - \ldots - \lambda_1 q - \lambda_0, \tag{2}$$

където $0 \leq \lambda_i \leq q-1$. Тогава

$$g_q(k,d) = sv_k - \lambda_{k-2}v_{k-1} - \ldots \lambda_1 v_2 - \lambda_0 v_1, \tag{3}$$

където $v_i = (q^i - 1)/(q-1)$.

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

$$t_q(k) := \max_{0 \leq d < \infty} (n_q(k,d) - g_q(k,d)). \tag{4}$$

Тук полето $\mathbb{F}_q$ е фиксирано. Известно е [30], че за всяка фиксирана размерност k съществува константа $\delta(k,q)$, такава че $n_q(k,d) = g_q(k,d)$ за всички $d \geq \delta_q(k,d)$. Ако фиксираме d и оставим k да расте неограничено, то $(n_q(k,d) - g_q(k,d)) \to \infty$, откъдето и $t_q(k) \to \infty$. Този нетривиален факт е забелязан за пръв път от Додунеков в [18]. В раздели 3.1–3.3 изследваме въпроса за скоростта на това нарастване.

В раздел 3.1 излагаме три еквивалентни формулировки на задачата за определяне на максималното отклонение от границата на Griesmer на най-добрите кодове от фиксирана размерност над дадено поле. Формално, това е еквивалентно на намирането на скоростта на нарастване на функцията $t_q(k)$, зададена с (4). Трите формулировки са съответно в термините на линейни кодове, на арки и на блокиращи множества (или минихипери) в $\mathrm{PG}(k-1,q)$.

Задача A. *Нека са дадени степен на просто число q и цяло положително число k. Да се намери минималната стойност на t, за която съществуват $[g_q(k,d)+t,k,d]_q$-кодове за всички d.*

Задача B. *Нека са фиксирани степен на просто число q и цяло положително число k. Да се намери минималната стойност на t, за която съществува арка в $\mathrm{PG}(k-1,q)$ с параметри $(g_q(k,d)+t, w_q(k,d)+t)$ за всички d.*

Задача С. *Да се намери максималната стойност на t такава, че за всички d, зададени с (2), съществува минихипер в* $\mathrm{PG}(k-1,q)$ *с параметри*

$$(\sigma v_k + \lambda_{k-2}v_{k-1} + \lambda_1 v_2 + \lambda_0 v_1 - t, \sigma v_{k-1} + \lambda_{k-2}v_{k-2} + \lambda_1 v_1 - t),$$

с кратност на точките, ненадхвърляща $\sigma + s$.

В началото на раздела 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, упростяващи изследването на $t_q(k)$. Най-важен от тях е следният.

Лема 3.6. *Ако $n_q(k,d) = g_q(k,d) + t$, то $n_q(k, d+q^{k-1}) \le g_q(k, d+q^{k-1}) + t$.*

От тази лема следва, че максимумът в (4) може да бъде взет само по краен брой стойности на d:

$$t_q(k) := \max_{0 \le d < q^{k-1} - q^{k-2}} (n_q(k,d) - g_q(k,d)). \tag{5}$$

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

Теорема 3.10. *Нека $d = sq^{k-1} - \lambda_{k-2}q^{k-2} - \ldots - \lambda_1 q - \lambda_0$, и нека мултимножеството $\mathcal{F}$ е минихипер в* $\mathrm{PG}(k-1,q)$ *с параметри*

$$(\sigma v_k + \lambda_{k-2}v_{k-1} + \ldots + \lambda_0 v_1 - \tau_1, \sigma v_{k-1} + \lambda_{k-2}v_{k-2} + \ldots + \lambda_1 v_1 - \tau_1).$$

Дефинираме мултимножеството $\mathcal{F}'$ по следния начин:

$$\mathcal{F}'(x) = \begin{cases} \mathcal{F}(x), & \text{ако } \mathcal{F}(x) \le \sigma + s, \\ \sigma + s, & \text{ако } \mathcal{F}(x) > \sigma + s. \end{cases}$$

Нека $N = |\mathcal{F}|$ и $N' = |\mathcal{F}'|$. Ако $\mathcal{F} - \mathcal{F}'$ е $(N - N', \tau_2)$-арка, то съществува $(g_q(k,d) + t, w_q(k,d) + t)$-арка в $\mathrm{PG}(k-1,q)$*, или, еквивалентно, линеен код с параметри $[g_q(k,d) + t, k, d]_q$, където $t = \tau_1 + \tau_2$.*

На геометричен език тя се състои в изтриване на блокиращо множество, получено като сума на подпространства с дадени размерности, от s-кратна сума на $\mathrm{PG}(k-1,q)$. Проблемът е, че при конструирането

на блокиращото множество могат да се появят точки с кратност по-голяма от s. Идеята на Теорема 3.10 се състои в изглаждане на точките с кратности, надхвърлящи s, и заменянето им с точки с максималната допустима кратност. По този начин някои хиперравнини се оказват блокирани недостатъчен брой пъти и трябва да бъдат компенсирани с допълнителни, подходящо избрани точки.

В конструкцията от Теорема 3.10 има голяма свобода при избора на подпространства, които формират търсеното блокиращо множество. За геометрии с нечетна размерност $\mathrm{PG}(2l-1,q)$ съществува спред от $(l-1)$-мерни подпространства, които могат да се използват за конструиране на подходящи блокиращи множества. Използвайки тази идея, доказваме оценка за $t_q(k)$ в случая на четна размерност $k=2l$.

Теорема 3.13. *Ако $k=2l$, то*

$$t_q(k) \le 2\frac{q^l-1}{q-1} - (2l+q-1).$$

Асимптотично имаме $t_q(k) \lesssim q^{k/2}$. По-специално за $k=4$ получаваме

Следствие 3.14. $t_q(4) \le q-1$.

Този резултат дава частичен отговор на въпроса за нарастването на $t_q(4)$ като функция на q. Това е интересна модификация на основния въпрос за поведението на функцията $t_q(k)$. В случая на равнинни арки проблемът за определяне на асимптотиката на $t_q(3)$ като функция на q е поставен от S. Ball [4]. Той изказа хипотезата, че

$$t_q(3) \le \log q.$$

В раздел 3.3 изследваме задачата за скоростта на нарастване на $t_q(3)$. Най-напред доказваме, че ако в $\mathrm{PG}(2,q)$ съществува (n,w)-арка, за която $n=(w-1)q+w-\alpha$, то съществува $[n,3,d]_q$-код с $d=n-w$, за който $n=t+g_q(3,d)$ с $t=\lfloor \alpha/q \rfloor$ (Лема 3.15). Това свързва тривиалната горна граница за мощността на арка с отклонението от границата на Griesmer за асоциирания код.

Основен резултат в този раздел е доказателство на хипотезата на Ball за арки в дезаргови равнини от четен ред. В доказателството на този резултат използваме следните две леми.

Лема 3.16. *Нека $q = 2^h$ и нека $\mathcal{K}_i$, $i = 1, \ldots, r$, са максимални арки. Дефинираме арката $\mathcal{K} = \sum_{i=1}^{r} \mathcal{K}_i$. Ако кодът $C_{\mathcal{K}}$, асоцииран с $\mathcal{K}$ има параметри $[n, 3, d]_q$, то $n = g_q(3, d) + (r - 1)$.*

Лема 3.17. *Нека $q = 2^h$. Всяко цяло число $m \leq q$ може да се представи във вида $m = 2^{a_1} + \ldots + 2^{a_r} - r$, където $a_i \in \{1, \ldots, h - 1\}$ и $r \leq h$.*

Като резултат получаваме следната горна граница за $t_q(3)$ в случая на четно q.

Теорема 3.18. *Ако $q = 2^h$, то $t_q(3) \leq \log_2 q - 1$.*

Тъй като доказателството на тази теорема използва съществуването на максимални арки в равнини от четен ред [17, 46, 52, 53], то тези аргументи са неприложими за нечетни q. Въпреки това, за равнини от редове, които са четна степен на нечетно просто число, можем да използваме един резултат на R. Hill и J. Mason [33] за да докажем малко по-слаба оценка.

Теорема 3.19. *Ако q е четна степен на просто число, то $t_q(3) \leq \sqrt{q} - 1$.*

В раздел 3.4 са намерени нови точни стойности на $n_q(k, d)$ за $q = 4$, $k = 5$. За кодове над $\mathbb{F}_4$ $k = 5$ е най-малката размерност, при която съществуват минимални разстояния d, за които точната стойност на $n_4(5, d)$ не е намерена. В началото на този раздел (подраздели 3.4.1 и 3.4.2) е направена характеризация на арките с параметри $(100, 26)$, $(117, 30)$ и $(118, 30)$ в $\mathrm{PG}(3, 4)$. Тя се използва по-нататък в доказателствата за несъществуване, но представлява и самостоятелен интерес.

Характеризацията на арките с параметри $(118, 30)$ се съдържа в Леми 3.20-3.25 Една $(118, 30)$-арка в $\mathrm{PG}(3, 4)$ е от един от следните типове

(α) $\mathcal{K} = 2 - \mathcal{F}$, където $\mathcal{F}$ е $(52, 12)$-блокиращо множество, а $\mathcal{F}$ е сума на две равнини и две прави, взети така, че максималната кратност на точка да бъде 2. Възможни са два спектъра:

$$a_{14}=2, a_{22}=0, a_{26}=10, a_{30}=73, \quad \lambda_0=9, \lambda_1=34, \lambda_2=42;$$
$$a_{14}=2, a_{22}=1, a_{26}=8, a_{30}=74, \quad \lambda_0=10, \lambda_1=32, \lambda_2=43$$

(β) $\mathcal{K}=2-\chi_{\pi_0\cup\pi_1}+\chi_L-\mathcal{F}$, където π_i са равнините през фиксирана права L, а $\mathcal{F}$ е $(15,3)$-блокиращо множество, съдържащо се в $\pi_2\cup\pi_3\cup\pi_4$. Съществуват точно две такива арки. Те се получават, ако блокиращото множество $\mathcal{F}$ е сума на три кръстосани прави, или подгеометрията $\mathrm{PG}(3,2)$. И в двата случая получаваме един и същ спектър:

$$a_{18}=2, a_{22}=0, a_{26}=12, a_{30}=71, \lambda_0=3, \lambda_1=46, \lambda_2=36.$$

(γ) $\mathcal{K}$ е дуална на мултимножество с мощност 18 и максимална кратност на точка 2 и числа на пресичане 2, 6, 10. Съществуват три такива мултимножества, които дават два възможни спектъра за $\mathcal{K}$:

$$(\gamma') \quad a_{22}=5, a_{26}=8, a_{30}=73, \quad \lambda_0=2, \lambda_1=48, \lambda_2=35;$$
$$(\gamma'') \quad a_{22}=9, a_{26}=0, a_{30}=76, \quad \lambda_0=6, \lambda_1=40, \lambda_2=39.$$
$$(\gamma''') \quad a_{22}=9, a_{26}=0, a_{30}=76, \quad \lambda_0=6, \lambda_1=40, \lambda_2=39.$$

(γ') Двете 0-точки са инцидентни с 6-права; равнините през тази 6-права са с кратности съответно 22, 30, 30, 30, 30.
(γ'') Съществува 30-равнина, съдържаща всичките шест 0-точки като пет от тях са колинеарни. Равнините през образуваната 0-права имат кратности 30, 22, 22, 22, 22. Точките с кратност 2, нележащи в тази 30-равнина образуват конус с връх шестата 0-точка и хиперовал като управителна крива.
(γ''') Съществува 22-равнина със седем 2-точки. През всяка от четирите и́ 2-прави минават две 22- и две 30-равнини, като всяка от тези 22-равнини съдържа четири 2-точки (за характеризацията на $(q^2+q+2, q+2)$-арките вж. [9]).

Това характеризира и арките с параметри $(117,30)$ в $\mathrm{PG}(3,4)$.

Лема 3.26. *Всяка* $(117,30)$*-арка в* $\mathrm{PG}(3,4)$ *е разширима.*

Арките с параметри $(100,26)$ могат да се получат от $(102,26)$-арката с изтриване на две точки. Последната е сума на 17-шапка и цялото пространство. Особено интересна е конструкцията на неразширимата $(100,26)$-арка в $\mathrm{PG}(3,4)$, която се окзва и единствена.

Теорема 3.34. *Нека $\mathcal{K}$ е $(100, 26)$-арка в $\mathrm{PG}(3, 4)$. Тогава $\mathcal{K}$ е от един от следните два типа:*

(1) *сума на шапка и цялото пространство минус две точки;*
(2) *конус, без върха, с управителна крива хиперовал плюс цялото пространство минус симетричната разлика на хиперовала и образуваща на конуса.*

До края на главата са изложени доказателства за несъществуване на арки, които се асоциират с грийсмърови кодове, чието съществуване беше под въпрос.

Теорема 3.35. *В $\mathrm{PG}(4, 4)$ не съществуват арки с параметри $(467, 118)$.*

Следствие 3.36. *Не съществуват кодове с параметри $[467, 5, 349]_4$. Това определя точните стойности $n_4(5, 349 + i) = 468 + i$ за $i = 0, 1, 2, 3$.*

Теорема 3.37. *В $\mathrm{PG}(4, 4)$ не съществуват арки с параметри $(465, 117)$.*

Теорема 3.38. *В $\mathrm{PG}(4, 4)$ не съществуват арки с параметри $(464, 117)$.*

Следствие 3.39. *Не съществуват кодове с параметри $[464, 5, 347]_4$. Това определя точните стойности $n_4(5, 347 + i) = 465 + i$ за $i = 0, 1$.*

Теорема 3.40. *Не съществуват $(398, 101)$-арки в $\mathrm{PG}(4, 4)$.*

Следствие 3.41. *Не съществуват кодове с параметри $[398, 5, 297]_4$ и $[399, 5, 298]_4$. Следователно, $n_4(5, 297) = 399$ и $n_4(5, 298) = 400$.*

Теорема 3.42. *Не съществуват $(396, 100)$-арки в $\mathrm{PG}(4, 4)$.*

Теорема 3.43. *Не съществуват $(395, 100)$-арки в $\mathrm{PG}(4, 4)$.*

Следствие 3.44. *Не съществуват кодове с параметри $[395, 5, 295]_4$ и $[396, 5, 296]_4$. Следователно, $n_4(5, 295) = 396$ и $n_4(5, 296) = 397$.*

От тези резултати получаваме точната стойност на $n_4(5, d)$ за десет минимални разстояния $d = 295, 296, 297, 298,\ 347, \ldots, 352$. 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. Разширимост на арки и кодове. Глава 4 е посветена на изследване на условия за разширимост на арки и, еквивалентно на условия за разширимост на асоциираните с тях линейни кодове.

Добре известен факт е, че всеки двоичен $[n, k, d]$-код с нечетно минимално разстояние е разширим до $[n+1, k, d+1]$-код. Това наблюдение е обобщено от R. Hill и P. Lizak в [31, 32]. Те доказват, че всеки q-ичен $[n, k, d]_q$-код с $(d, q) = 1$, в който всяка дума е с тегло сравнимо с 0 или d по модул q, е разширим до $[n+1, k, d+1]_q$-код. Типичен случай при изследване на достижимостта на границата на Griesmer е $d \equiv -1 \pmod{q}$. Тази линия на изследване е продължена от T. Maruta, който доказа нови резултати за разширимост [40, 42, 43, 44]. Най-интересен за нас е резултатът от [43], съгласно който за нечетни $q \geq 5$ всеки $[n, k, d]_q$-код с $d \equiv -2 \pmod{q}$, имащ тегла $\equiv -2, -1, 0 \pmod{q}$, е разширим.

Изследванията по разширимост на арки предхождат тези по разширимост на кодове и протичат независимо от тях. Може би първият такъв резултат е теоремата на A. Barlotti [10], съгласно която всяка $((w-1)(q+1), w)$-арка в $\mathrm{PG}(2, q)$ е разширима до максимална $((w-1)(q+1)+1, w)$-арка. Резултатите за разширимост са специален случай на широк клас от резултати, известни като теореми за стабилност.

В тази глава е предложен нов геометричен подход към задачата за разширимост, разбирана като формулиране на условия, при които (n, w)-арка в $\mathrm{PG}(r, q)$ е разширима до $(n+1, w)$-арка чрез увеличаване на кратността на една точка. Основната идея е да се свърже разширимостта на дадена арка $\mathcal{K}$ със структурата на специална арка $\widetilde{\mathcal{K}}$ в дуалната геометрия. От особен интерес е въпросът за разширимостта на т.нар. арки с t-квазиделимост. Такива арки се появяват при разглеждане на кодове на Griesmer с $d \equiv -t \pmod{q}$, $t < q$.

В раздел 4.1 въвеждаме т.нар. $(t \mod q)$-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 $d \equiv -t \pmod{q}$. Нека $\mathcal{K}$ е (n, w)-арка в $\Sigma = \mathrm{PG}(r, q)$ със спектър $(a_i)_{i \geq 0}$ и $w \equiv n + t \pmod{\Delta}$, $1 \leq t < \Delta$. Казваме, че $\mathcal{K}$ притежава свойството *t-квазиделимост* с делител Δ, ако $a_i = 0$, за всяко $i \not\equiv n, n+1, \ldots, n+t \pmod{\Delta}$. За $\mathcal{K}$ дефинираме арка $\widetilde{\mathcal{K}}$ в дуалната геометрия $\widetilde{\Sigma}$, с множество от точки $\widetilde{\mathcal{H}} = \{\widetilde{H} | H -$ хиперравнина в $\Sigma\}$, по следното

правило:

$$\widetilde{\mathcal{K}} : \begin{cases} \widetilde{\mathcal{H}} & \to & \{0,1,\ldots,t\} \\ \widetilde{H} & \to & \widetilde{\mathcal{K}}(H) \equiv n+t-\mathcal{K}(H) \pmod q \end{cases}, \tag{6}$$

Теорема 4.1. *Нека $\mathcal{K}$ е (n,w)-арка в $\Sigma = \mathrm{PG}(r,q)$, която притежава свойството t-квазиделимост по модул q като $t < q$. Тогава за всяко подпространство $\widetilde{S}$ на $\widetilde{\Sigma}$, с размерност $\dim \widetilde{S} \geq 1$, е изпълнено*

$$\widetilde{\mathcal{K}}(\widetilde{S}) \equiv t \pmod q.$$

Направеното наблюдение оправдава следната дефиниция. Нека t е цяло неотрицателно число. Една арка $\mathcal{K}$ в Σ наричаме $(t \mod q)$-арка, ако за кратността на всяко подпространство S с (проективна) размерност $\dim S \geq 1$ е изпълнено $\mathcal{K}(S) \equiv t \pmod q$. Основен резултат в този раздел е следната теорема.

Теорема 4.3. *Нека $\mathcal{K}$ е (n,w)-арка в $\Sigma = \mathrm{PG}(r,q)$, която е t-квазиделима по модул q като $t < q$. Нека $\widetilde{\mathcal{K}}$ е дуалната на $\mathcal{K}$, дефинирана чрез (6). Ако $\widetilde{\mathcal{K}}$ се представя във вида*

$$\widetilde{\mathcal{K}} = \sum_{i=1}^{c} \chi_{\widetilde{P}_i} + \mathcal{K}'$$

където $\mathcal{K}'$ е някаква арка в $\widetilde{\Sigma}$, а $\widetilde{P}_1, \ldots, \widetilde{P}_c$ са с не непременно различни хиперравнини в $\widetilde{\Sigma}$, то $\mathcal{K}$ е c-кратно разширима. По-специално, ако $\widetilde{\mathcal{K}}$ съдържа в носителя си хиперравнина, то $\mathcal{K}$ е разширима.

Съгласно тази теорема достатъчно условие за c-кратна разширимост на t-квазиделима арка $\mathcal{K}$ е дуалната арка $\widetilde{\mathcal{K}}$ да е сума на c хиперравнини и някоя друга арка. В частност, една арка $\mathcal{K}$ с t-квазиделимост е 1-разширима (или просто разширима), ако носителят ѝ $\operatorname{Supp}\mathcal{K} = \{X \mid \mathcal{K}(X) > 0\}$ съдържа хиперравнина. Това обуславя и важността на задачата за определяне на структурата на $(t \mod q)$-арките.

В раздел 4.2 се изследва структурата на $(t \mod q)$-арки без връзка със задачата за разширимост. В началото представяме една нетривиална конструкция, която от $(t \mod q)$-арки в $\mathrm{PG}(r-1,q)$ дава такива арки в $\mathrm{PG}(r,q)$.

Теорема 4.6. *Нека $\mathcal{F}_0$ е ($t \mod q$)-арка в хиперравнината $H \cong \mathrm{PG}(r-1,q)$ на $\Sigma = PG(r,q)$. Нека точката $P \in \Sigma \setminus H$ е фиксирана. Арката $\mathcal{F}$ в Σ, дефинирана по следния начин:*

– $\mathcal{F}(P) = t$;

– за всяка точка $Q \neq P$: $\mathcal{F}(Q) = \mathcal{F}_0(R)$, където $R = \langle P, Q\rangle \cap H$.

е ($t \mod q$)-арка с мощност $q|\mathcal{F}_0| + t$.

Най-важен тук е въпросът за структурата на ($0 \mod q$)-арките, т.е. тези арки, за които всяка хиперравнина е с кратност $\equiv 0 \pmod q$. Изследването ни е ограничено само до геометриите $\mathrm{PG}(r,p)$ от прост ред p. В този случай кратностите на точките могат да се разглеждат като елементи на $\mathbb{F}_p$ и всички ($0 \mod p$)-арки образуват векторно пространство над $\mathbb{F}_p$. Основен резултат в този раздел е Теорема 4.12.

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

Този резултат се получава с използване на класическата формула на N. Hamada [27] за p-ранга на матрицата на инцидентност на $\mathrm{PG}(r,q)$, в която редовете са индексирани с точките, а стълбовете – с правите на тази геометрия. Затворен вид на формулата за ранга е получен от J. van Lint като доказателството се съдържа в работата на P. V. Ceccherini и J. Hirschfeld [16]. От Теорема 4.12 следва, че всяка ($0 \mod p$)-арка, а оттук и всяка ($t \mod p$)-арка за $t < p$ е сума на арки, получени чрез лифтинг (Следствие 4.13 и Следствие 4.14). Теорема 4.12 не отговаря на въпроса какъв е броят на събираемите в тази сума. В Теорема 4.15 даваме оценка за този брой.

Теорема 4.15. *Нека $P_1, \ldots, P_{p+1}$ са точките на коника в $\mathrm{PG}(2,p)$. Да означим с V_i векторното пространство на всички ($0 \mod p$)-арки, получени чрез лифтинг от P_i, $i = 1, \ldots, p+1$, а с V – векторното пространство на всички ($0 \mod p$)-арки. Тогава*

$$V = V_1 + V_2 + \cdots + V_p.$$

Изглежда правдоподобно, че аналогично твърдение е в сила и за геометрии от всяка размерност. Доказателството на това твърдение

зависи от проверката на условие, което гарантира валидността на формулата за включване и изключване за размерностите на подпространства. Известно е, че тази формула не е вярна в общия случай.

Раздел 4.3 е посветен на изследване на $(t \mod q)$-арки, в които максималната кратност на точка е t. Разделът започва с теорема, в която доказваме, че ако една $(t \mod q)$-арка има допълнителното свойство, че ограничението ѝ върху всяка равнина е получена чрез лифтинг, то и самата арка е получена чрез лифтинг.

Теорема 4.18. *Нека $\mathcal{K}$ е $(t \mod q)$-арка в $\mathrm{PG}(r,q)$ и нека ограничението ѝ върху всяка хиперравнина H, $\mathcal{K}|_H$, е получено чрез лифтинг от точка. Тогава и арката $\mathcal{K}$ е получена чрез лифтинг от точка.*

В равнинния случай $(t \mod q)$-арки с ограничена кратност на точките се получават като σ-дуални на блокиращи множества, при които кратностите на правите се съдържат в интервал с дължина t.

Теорема 4.19. *Необходимо и достатъчно условие за съществуването на $(t \mod q)$-арка в $\mathrm{PG}(2,q)$ с мощност $mq+t$ и максимална кратност на точка t е съществуването на блокиращо множество в същата равнина с параметри $((m-t)q+m, m-t)$ и с кратности на правите, принадлежащи на множеството $\{m-t, m-t+1, \ldots, m\}$.*

В края на раздела са характеризирани $(3 \mod 5)$-арките в $\mathrm{PG}(2,5)$ с малък брой точки: 18, 23, 28 и 33. От тази характеризация получаваме частичен резултат за $(3 \mod 5)$-арки в $\mathrm{PG}(3,5)$.

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

Този резултат се използва по-нататък за доказване на несъществуването на $(104,22)$-арки в $\mathrm{PG}(3,5)$ в раздел 4.5.

В следващия раздел 4.4 изследваме разширимост на грийсмърови арки, имащи свойството t-квазиделимост по модул q. В случаите, когато минималното разстояние d на асоциирания с такава арка код

удовлетворява $d \equiv -t \pmod q$, тези арки притежават свойството t-квазиделимост с $t \equiv -d \pmod q$. Така за тях могат да бъдат използвани резултатите от предните три раздела. Нека $\mathcal{K}$ е грийсмърова (n, w)-арка в $\mathrm{PG}(k-1, q)$, която е t-квазиделима за някое $t < q$. Нека $C_{\mathcal{K}}$ е линейният код, асоцииран с арката $\mathcal{K}$. Тогава $C_{\mathcal{K}}$ има параметри $[n, k, d]_q$, където $d = n - w$. Да запишем d във вида:

$$d = sq^{k-1} - \sum_{i=0}^{k-2} \varepsilon_i q^i, \tag{7}$$

където $0 \leq \varepsilon_i < q$ за всички $i = 0, \ldots, k-2$.

В следващите няколко леми установяваме важни свойства на арката $\widetilde{\mathcal{K}}$, дефинирана в (6). Първата от тях дава връзка между кратността на хиперправите (подпространства с коразмерност 2), съдържащи се в дадена хиперравнина и съответната им кратност по отношение на дуалната арка $\widetilde{\mathcal{K}}$.

Лема 4.22. *Нека $\mathcal{K}$ е грийсмърова арка в $\Sigma = \mathrm{PG}(k-1, q)$ с параметри $(n, n-d)$, която има свойството t-квазиделимост. Нека d е представено във вида (7) и нека S е подпространство с коразмерност 2, съдържащо се в хиперравнина H_0 с кратност $\mathcal{K}(H_0) = w_{k-2} - aq$ за някое цяло число $a \geq 0$.*

(i) *Ако $\mathcal{K}(S) = w_{k-3} - a - b$, $0 \leq b \leq t-2$, то $\widetilde{\mathcal{K}}(\widetilde{S}) \leq t + bq$;*

(ii) *Ако $\mathcal{K}(S) = w_{k-3} - a - b$, $b \geq t-1$, то $\widetilde{\mathcal{K}}(\widetilde{S}) \leq t + (t-1)q$.*

Следващите резултати дават оценка за кратността на равнините в дуалното пространство, съответстващи на максимални (по отношение на $\mathcal{K}$) подпространства в Σ с различна коразмерност.

Лема 4.23. *Нека $\mathcal{K}$ е грийсмърова $(n, n-d)$-арка в $\mathrm{PG}(k-1, q)$, притежаваща свойството t-квазиделимост. Нека d е представено във вида (7) и нека $\widetilde{\mathcal{K}}$ е дуална на $\mathcal{K}$, получена по начина, описан в (6). Нека T е подпространство на $\mathrm{PG}(k-1, q)$ с коразмерност 3 и максимална кратност $\mathcal{K}(T) = w_{k-4}$. Тогава*

$$\widetilde{\mathcal{K}}(\widetilde{T}) \leq t(q+1) + \varepsilon_1 q.$$

Лема 4.24. *Нека $\mathcal{K}$ е грайсмърова $(n, n-d)$-арка в $\mathrm{PG}(k-1,q)$, $q \geq 3$, притежаваща свойството t-квазиделимост, като d е представено във вида (7). Нека $\widetilde{\mathcal{K}}$ е дуалната на $\mathcal{K}$, зададена с (6). Накрая нека $\varepsilon_0, \varepsilon_1 < \sqrt{q}$. Тогава за всяко подпространство T в $\mathrm{PG}(k-1,q)$ с коразмерност 3, за което $\mathcal{K}(T) = w_{k-4}$, е в сила*

$$\widetilde{\mathcal{K}}(\widetilde{T}) = t(q+1).$$

Лема 4.25. *Нека $\mathcal{K}$ е грайсмърова (n, w)-арка в $\mathrm{PG}(k-1,q)$, $q \geq 3$, имаща свойството квазиделимост, за която $d = n - w$ е представено във вида (7). Нека $\widetilde{\mathcal{K}}$ е дуална на $\mathcal{K}$, дефинирана чрез (6). Нека U е подпространство в $\mathrm{PG}(k-1,q)$ с коразмерност – $\operatorname{codim} U = r$, $1 \leq r \leq k$, имащо максимална мощност w_{k-1-r} (ако $U = \varnothing$, приемаме, че $\operatorname{codim} U = k$). Тогава, ако $\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_{r-2} < \sqrt{q}$, то е изпълнено*

$$\widetilde{\mathcal{K}}(\widetilde{U}) = \varepsilon_0 v_{r-1}.$$

Основен резултат в 4.4 е следната теорема, която е получена като резултат за разширимост на арки.

Теорема 4.26. *Нека $\mathcal{K}$ е грайсмърова $(n, n-d)$-арка в $\mathrm{PG}(k-1,q)$, която притежава свойството t-квазиделимост. Нека d е представено във вида*

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

където $0 \leq \varepsilon_i < q$ 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 $\mathcal{K}$ е t-разширима.

Този резултат е формулиран за разширимост на линейни кодове в следната теорема.

Теорема 4.27. *Нека C е код на* Griesmer *с параметри $[n,k,d]_q$, притежаващ свойството t-квазиделимост. Нека d е представено във вида*

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

където $0 \leq \varepsilon_i < q$ 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-разширим, т.е. съществува код с параметри $[n+t, k, d+t]_q$.

В общия случай параметрите на една арка $\mathcal{K}$ с t-квазиделимост не определят параметрите на дуалната ѝ арка $\widetilde{\mathcal{K}}$. Все пак в случаите, когато е известен спектърът на рестрикцията на $\mathcal{K}$ върху максимална хиперравнина, то мощността на $\widetilde{\mathcal{K}}$ може да бъде ограничена. В редица случаи това позволява да се докаже разширимостта на $\mathcal{K}$. Един такъв резултат представлява Теорема 4.28, която дава достатъчно условие за разширимост, зависещо от спектъра на $\mathcal{K}|_H$, където H е максимална хиперравнина.

Теорема 4.28. *Нека $\mathcal{K}$ е грайсмърова арка в $\mathrm{PG}(k-1,q)$ с параметри (n,w), $w = n-d$, която е t-квазиделима по модул q. За фиксирана хиперравнина H_0 с кратност w нека $(a_i)_{i\geq 0}$ е спектърът на арката $\mathcal{K}|_{H_0}$. Да означим с A най-голямото цяло число, за което всяко блокиращо множество с параметри $(tv_{k-1} + A, tv_{k-2})$ съдържа хиперравнина в носителя си. Тогава, ако*

$$(8)\quad qa_{w-\lceil d/q\rceil-1} + 2qa_{w-\lceil d/q\rceil-2} + \ldots + (t-2)qa_{w-\lceil d/q\rceil-t+2} + (t-1)q \sum_{u \leq w-\lceil d/q\rceil-t+1} a_u \leq A,$$

то $\mathcal{K}$ е разширима.

В края на раздел 4.4 са представени два примера, в които се прилагат получените резултати за разширимост. В първия пример се изследва клас от хипотетични арки в $\mathrm{PG}(3,q)$ с параметри $(q^3 - 3q - 6, q^2 - 3)$. Оказва се, че всички те са разширими до несъществуващите (q^3-3q-3, q^2-3)-арки. За $q \geq 11$ този резултат следва от Теорема 4.29.

В случаите $q = 5, 7, 8, 9$ хипотетичните арки с параметри (q^3-3q-6, q^2-3) са отново разширими, но доказателството изисква и допълнителни геометрични аргументи. Във втория пример е доказана t-разширимостта на (q^2+1-t)-шапки в $\mathrm{PG}(3,q)$ за всяко $t < \sqrt{q}$.

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

Теорема 4.36. *Не съществува* $(104, 22)$*-арка в* $\mathrm{PG}(3,5)$.

Това решава един от четирите открити случая за кодове с $k = 4, q = 5$ [45]. Идеята е, че ако съществува такава арка $\mathcal{K}$, то тя има свойството 3-квазиделимост и е неразширима. Така дуалната арка $\widetilde{\mathcal{K}}$ не съдържа в носителя си равнина и има допълнителното свойство, че не съществува 18-равнина, съдържаща 18-права. Като се използва характеризацията на равнинните $(3 \mod 5)$-арки и априорните наблюдения за спектъра на хипотетична $(104, 22)$-арка $\mathcal{K}$ в $\mathrm{PG}(3,5)$ (подраздел 4.5.1) се стига до противоречие.

Глава 5. Афинни блокиращи множества. Глава 5 е посветена на конструирането на афинни блокиращи множества. Едно множество $\mathcal{B}$ от точки в $\mathrm{AG}(n,q)$ наричаме афинно t-кратно блокиращо множество, ако всяка хиперравнина на $\mathrm{AG}(n,q)$ съдържа поне t точки от $\mathcal{B}$.

Раздел 5.1 съдържа обзор на известните долни граници за мощността на блокиращо множество в $\mathrm{AG}(n,q)$. Границата за минималната мощност на 1-блокиращо множество е доказана независимо от R. Jamison [34] и A. Brouwer и A. Schrijver [14]:

$$|\mathcal{B}| \geq n(q-1)+1.$$

Тази граница е точна за всички размерности n и всички полета $\mathbb{F}_q$. Един пример за такова блокиращо множество са n конкурентни прави, никои три от които не лежат в една равнина. Значително обобщение на тази граница е направено от A. Bruen [15], който доказа, че ако $\mathcal{B}$ е t-кратно блокиращо множество, то за мощността му е в сила неравенството:

$$|\mathcal{B}| \geq (n+t-1)(q-1)+1.$$

Тази граница е нетривиална за $1 \leq t \leq (n-1)(q-1)$, тъй като за стойности на t извън този интервал тя става по-слаба от тривиалната

$$|\mathcal{B}| \geq tq.$$

За големи стойности на t границата на Bruen не се достига. C. Zanella [57] доказа, че за стойности на t, за които

$$t > \frac{(n-1)(q-1)+1}{2}$$

не съществуват блокиращи множества, удовлетворяващи границата на Bruen. Границата на Bruen е съществено подобрена за някои специални стойности на t и n. S. Ball [1] доказа, че за $t < q$ едно t-кратно блокиращо множество $\mathcal{B}$ в $\mathrm{AG}(n,q)$, $q = p^h$, е с мощност поне $(n+t-1)(q-1)+k$ при условие, че съществува цяло число j, за което е изпълнено

$$\binom{k-n-t}{j} \not\equiv \pmod{p}.$$

По-специално, ако $\binom{-n}{t-1} \not\equiv 0 \pmod{p}$, то

$$|\mathcal{B}| \geq (n+t-1)q - n + 1.$$

В същата работа [1] S. Ball конструира и блокиращи множества в $\mathrm{AG}(n,q)$ с параметри $((n+t-1)q-n+\varepsilon, 2)$, където

$$\varepsilon = \begin{cases} 1, & \text{за } n \not\equiv 0 \pmod{p}, \\ 0, & \text{за } n \equiv 0 \pmod{p}. \end{cases}$$

В случаите, когато $\varepsilon = 0$ конструираните блокиращи множества достигат границата на Bruen. Независимо един от друг, C. Zanella [57] и S. Ball [1] отбелязват, че ако от хиперболичната квадрика в $\mathrm{PG}(3,q)$ се изтрие равнина, минаваща по две нейни прави, то резултатът е $(q^2, q-1)$-блокиращо множество в $\mathrm{AG}(3,q)$, лежащо на границата на Bruen. Така известните класове от блокиращи множества, достигащи границата на Bruen се получават в следните случаи:

(1) $t = 1$ за всички n и q;
(2) $t = 2$ за всяко $n \equiv 0 \pmod{p}$ и всяко $q = p^h$;
(3) $t = q-1$, $n = 3$ за всяко $q = p^h$.

В раздел 5.2 е изложен основният резултат на тази глава. Това е Теорема 5.6, в която е представена нова обща конструкция на афинни блокиращи множества.

Теорема 5.6. *Нека $n \geq 3$ е цяло число и нека $q = p^h$ е степен на просто число. Ако съществуват*

- *арка с параметри (M, w) в $\mathrm{PG}(r, q)$, където $2 \leq r \leq n-2$, и*
- *блокиращо множество с параметри (M', u) в $\mathrm{AG}(n-r-1, q)$,*

то съществува (N, t)-блокиращо множество в $\mathrm{AG}(n, q)$ с параметри

$$N = qM, \;\; t = \min\{M - w, aqu\},$$

където $a = \lfloor M/M' \rfloor$.

В няколко следствия са описани важни специални случаи на прилагане на Теорема 5.6.

Следствие 5.7. *Нека $n \geq 3$ е цяло число и нека $q = p^h$ е степен на просто число. Ако съществуват*

- *(M, w)-арка в $\mathrm{PG}(r, q)$, $1 \leq r \leq n-2$, и*
- *(M, u)-блокиращо множество в $\mathrm{AG}(n-r-1, q)$,*

то съществува и (N, t)-блокиращо множество в $\mathrm{AG}(n, q)$ с параметри $N = qM$ и $t = \min\{M - w, qu\}$.

Следствие 5.8. *Нека $n \geq 4$ е цяло число и нека $q = p^h$ е степен на просто число. Ако съществува арка с параметри (M, w) в $\mathrm{PG}(n-2, q)$, то съществува и (N, t)-блокиращо множество в $\mathrm{AG}(n, q)$ с параметри*

$$N = qM, \; t = \min\{M - w, q\lfloor M/q \rfloor\}.$$

Следствие 5.9. *Нека $n \geq 3$ е цяло число и нека $q = p^h$ е степен на просто число. Ако съществува (M, w)-арка в $\mathrm{PG}(n-1, q)$, то съществува и $(qM, M - w)$-блокиращо множество в $\mathrm{AG}(n, q)$.*

Следствие 5.10. *Нека $n \geq 3$ е цяло число и нека $q = p^h$ е степен на просто число. Ако съществуват*

- *(M, w)-арка в $\mathrm{PG}(r, q)$, където $1 \leq r \leq n-2$, и*
- *(M', u)-блокиращо множество в $\mathrm{AG}(n-r-1, q)$,*

то за всяко $i \geq 1$ *и всички* $\alpha \in \{1, \ldots, q-1\}$ *съществува* (N,t)*-блокиращо множество в* $\mathrm{AG}(n,q)$ *с параметри*

$$N = qM - i\alpha, \;\; t = \min\{M - w - i, aqu - b\alpha\},$$

където $a = \lfloor M/M' \rfloor$ *и* $b = \lfloor i/M' \rfloor$.

В раздел 5.3 представяме 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.

Теорема 5.12. *За всяко* n*, за което* $3 \leq n \leq q-1$*, в геометрията* $\mathrm{AG}(n,q)$ *съществува блокиращо множество с параметри* $(q^2, q-n+2)$.

Този клас включва хиперболичните квадрики от (3), които се получават при $n = 3$. Така конструираният клас се използва по-нататък за получаване на нови примери на оптимални блокиращи множества, имащи минимална мощност при фиксирани t, n и q.

Теорема 5.13. *За всяко* $s = 0, 1, \ldots, q+1-n$ *в* $\mathrm{AG}(n,q)$, $3 \leq n \leq q-1$, *съществува блокиращо множество с параметри* $(q^2 - s(n-2+s), q-(n-2+s))$.

Теорема 5.14. *За всяко* $n \geq 2$ *и всяка степен на просто число* $q = p^h$ *съществува афинно блокиращо множество в* $\mathrm{AG}(n,q)$ *с параметри* $(q^2 - n+1, q-n+1)$. *Блокиращите множества с тази мощност са оптимални.*

Следствие 5.15. *За всяка степен на просто число* $q = p^h$ *съществува афинно блокиращо множество в* $\mathrm{AG}(n,q)$, $3 \leq n \leq q-1$, *с параметри* $(q^2 - 2n, q-n)$. □

Теорема 5.16. *Съществуват* $(q^2+2q-1, q-n+3)$*-блокиращи множества в* $\mathrm{AG}(n,q)$ *за* $3 \leq n \leq q-1$.

По-нататък, като използваме Теорема 5.6, конструираме блокиращи множества със следните параметри:

$(28, 4)$ в $\mathrm{AG}(5, 4)$; $(40, 4)$ в $\mathrm{AG}(9, 4)$;
$(52, 4)$ в $\mathrm{AG}(13, 4)$; $(64, 4)$ в $\mathrm{AG}(17, 4)$;
$(120, 8)$ в $\mathrm{AG}(9, 8)$.

Тези пет блокиращи множества са оптимални и лежат на границите на Ball от [3] и Ball-Blokhuis от [6]. Освен, че са първите примери въобще на блокиращи множества, за които тези граници се достигат, те са и единствените известни примери към настоящия момент.

В раздел 5.4 представяме две таблици. Първата от тях е таблица за блокиращи множества в $\mathrm{AG}(n, 4)$, получени от конструкцията в Теорема 5.6, които са сравнени с долните граници от работите [3, 6]. Втората таблица съдържа долни и горни граници за мощността на 3-кратни и 4-кратни блокиращи множества в малки афинни геометрии $\mathrm{AG}(n, q)$, за $n = 3, 4, 5$, $q = 5, 7, 8, 9, 11, 13$.

Научни приноси

Основните научни приноси в настоящия дисертационен труд по преценка на автора са следните:

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

(2) Доказано е неравенството $t_q(3) \leq \log_2 q - 1$ 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 $t_q(3) \leq \sqrt{q} - 1$.

(3) 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.

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

(5) 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.

(6) Направена е частична характеризация на $(3 \mod 5)$-арки в $\mathrm{PG}(2, 5)$ и $\mathrm{PG}(3, 5)$.

(7) Доказано е несъществуването на $(104, 22)$-арки в $\mathrm{PG}(3, 5)$ 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 $n_5(4, d)$.

(8) 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.

(9) Построени са пет примера на блокиращи множества, лежащи на границата на S. Ball от 2014 г.:

$(28, 4)$ в $\mathrm{AG}(5, 4)$, $(40, 4)$ в $\mathrm{AG}(9, 4)$, $(52, 4)$ в $\mathrm{AG}(13, 4)$,
$(64, 4)$ в $\mathrm{AG}(17, 4)$, $(120, 8)$ в $\mathrm{AG}(9, 8)$.

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

Публикации по дисертационния труд

(1) I. Landjev, A Rousseva, An extension theorem for arcs and linear codes, *Probl. Inf. Transmission* **42**(2006), 65–76.

(2) I. Landjev, A. Rousseva, Characterization of some optimal arcs, *Adv. Math. Comm.* **5**(2)(2011), 317–331.

(3) I. Landjev, A. Rousseva, On the extendability of Griesmer arcs, *Ann. de l'Univ. de Sofia* **101**(2013/14), 183–191.

(4) I. Landjev, A. Rousseva, The Nonexistence of (104,22;3,5)-Arsc, *Advances in Mathematics of Communications* **10**(3)(2016), 601–611.

(5) I. Landjev, A. Rousseva, Linear codes close to the Griesmer bound and the related geometric structures, *Designs, Codes and Cryptography* **87**(4)(2019), 841-854.

(6) A. Rousseva, A General construction for blocking sets in finite affine geometries, *Compt. Rend. Acad. Bulg. des Sciences* **71**(4)(2018), 460-466.

(7) A. Rousseva, On the structure of some arcs related to caps and the nonexistence of some optimal codes, *Ann. de l'Univ de Sofia*, 2020, to appear.

Литература

[1] S. Ball, On intersection sets in Desarguesian affine spaces, *European J. Comb.* **21**(2000), 441-446.

[2] S. Ball, On sets of vectors of a finite vector space in which every subset of basis size is a basis, *J. Eur. Math. Soc.* **14** (2012) 733–748.

[3] S. Ball, A p-adic condition on the weight of a codeword of a linear code, *Des. Codes Cryptogr.* **72** (2014) 177–183.

[4] S. Ball, Table of bounds on three dimensional linear codes or (n, r)-arcs in PG$(2, q)$, `https://mat-web.upc.edu/people/simeon.michael.ball/codebounds.html`

[5] S. Ball, A. Blokhuis, An easier proof of the maximal arcs conjecture, *Proc. Amer. Math. Soc.* **126** (1998) 3377–3380.

[6] S. Ball, A. Blokhuis, A bound for the maximum weight of a linear code, *SIAM J. Discrete Math.* **27** (2013) 575–583.

[7] S. Ball, A. Blokhuis, F. Mazzocca, Maximal arcs in Desarguesian planes of odd order do not exist, *Combinatorica*, **17** (1997) 31–41.

[8] S. Ball, J. De Beule, On sets of vectors of a finite vector space in which every subset of basis size is a basis II, *Des. Codes Cryptogr.* **65** (2012) 5–14.

[9] S. Ball, R. Hill, I.Landjev, H. N. Ward, On $(q^2+q+2, q+2)$-arcs in the projective plane $PG(2, q)$, *Designs, Codes and Cryptography*, **24**, 2001, 205–224.

[10] A. Barlotti, Su $\{k; n\}$-archi di un piano lineare finito, *Boll. Un. Mat. Ital.* **1**(1956), 553–556.

[11] B. I. Belov, V. N. Logachev, V. P. Sandimirov, Construction of a class of linear binary codes achieving the Varshamov-Griesmer bound, *Probl. Inf. Transm.* **10**(3)(1974), 211–217.

[12] E. R. Berlekamp, R. C. McEliece, H. C. van Tilborg, On the inherent intractability of certain coding theoretic problems, *IEEE Trans. Inf. Theory* **IT-24**(1978), 384-386.

[13] A. Beutelspacher, Blocking sets and partial spreads in finite projective spaces, *Geom. Dedicata* 9(1980), 130–157.

[14] A. E. Brouwer, A. Schrijver, The blocking number of an affine space, *J. Combin. Th. Ser. A* **24**(1978), 251–253.

[15] A. A. Bruen, Polynomial multiplicities over finite fields and intersection sets, *J. Comb. Th. Ser. A* **60**(1992), 19–33.

[16] P. V. Cechherini, J. W. P Hirschfeld, The dimension of projective geometry code, *Discrete Math.* **106/107**(1992), 117–126.

[17] R.H.F.Denniston, Some maximal arcs in finite projective planes, *J. Comb. Theory* Ser. A, **6**(1969), 317–319.

[18] S. Dodunekov, Optimal Codes, DSc Thesis, Institute of Mathematics, Sofia, 1985.

[19] S.Dodunekov, I.Landjev, On Near-MDS Codes, *Journal of Geometry*, **54**(1995), 30–43.

[20] G. Fano, Sui postulati fondamentali della geometria proiettiva, *Giornale di Matematiche* **30**(1892), 106–132.

[21] E.N. Gilbert, A comparisonof sigmaling alphabets, *Bell System Tech. J.* **31**(1952), 504–522.

[22] V. D. Goppa, A new class of linear error-correcting codes, *Probl. Peredach. Inform.* **6**(3)(1970), 24–30.
[23] V. D. Goppa, Rational representation of codes and (L, g) codes, *Probl. Peredach. Inform.* **7**(3)(1971), 41–49.
[24] V. D. Goppa, Some codes constructed on the basis of (L, g) codes, *Probl. Peredach. Inform.* **8**(2)(1972), 107–109.
[25] M. Grassl, Code Tables: Bounds on the parameters of various types of codes. `http://codetables.markus-grassl.de`
[26] J.H. Griesmer, A bound for error-correcting codes, *IBM J. Res. Develop.* 4, 1960, 532–542.
[27] N. Hamada, The Rank of the Incidence Matrix of Points and d-Flats in Finite Geometries, *J. Sci. Hiroshima Univ.* Ser. A-I 32(1968), 381–396.
[28] R. Hill, On the largest size of cap in $S_{5,3}$, *Atti Accad. Naz. Linzei Rend.* **54** (1973), 378–384.
[29] R. Hill, Caps and codes, *Discrete Math.* **22** (1978), 111–137.
[30] R. Hill, Optimal Linear Codes, Cryptography and Coding II (C. Mitchell ed.), Oxford Univ. Press (1992), 75–104.
[31] R. Hill, P. Lizak, Extensions of linear codes, in: *Proc. Int. Symp. on Inf. Theory*, Whistler, Canada, 1995, 345.
[32] R. Hill, An extension theorem for linear codes, *Des. Codes and Cryptogr.* **17**(1999), 151–157.
[33] R. Hill, J. R. M. Mason, On (k, n)-arcs and the falsity of the Lunelli-Sce conjecture, "Finite Geometries and Designs", London Math. Soc. Lecture Note Series 49, cambridge Univ. Press, cambridge, 1981, 153–168.
[34] R. Jamison, Covering finite fields with cosets of subspaces, *J. Comb. Th. Ser. A* **22**(1977), 253–256.
[35] I. Landjev, A Rousseva, An extension theorem for arcs and linear codes, *Probl. Inf. Transmission* **42**(2006), 65–76.
[36] I. Landjev, A. Rousseva, Characterization of some optimal arcs, *Adv. Math. Comm.* **5**(2)(2011), 317–331.
[37] I. Landjev, A. Rousseva, On the extendability of Griesmer arcs, *Ann. de l'Univ. de Sofia* **101**(2013/14), 183–191.
[38] I. Landjev, A. Rousseva, The Nonexistence of (104,22;3,5)-Arsc, *Advances in Mathematics of Communications* **10**(3)(2016), 601–611.
[39] I. Landjev, A. Rousseva, Linear codes close to the Griesmer bound and the related geometric structures, *Designs, Codes and Cryptography* **87**(4)(2019), 841-854.
[40] T. Maruta, On the extendability of linear codes, *Finite Fields Appl.* **7**(2001), 350–354.
[41] T. Maruta, The nonexistence of some quaternary linear codes of dimension 5, *Discrete Mathematics* 238(2001), 99–113.
[42] T. Maruta, Extendability of linear codes over GF(q) with minimum distance d, $\gcd(d, q) = 1$, *Discrete Math.* **266**(2003), 377–385.
[43] T. Maruta, A new extension theorem for linear codes, *Finite Fields and Appl.* **10**(2004), 674–685.

[44] T. Maruta, Extension theorems for linear codes over finite fields, *J. of Geom.* **101**(2011), 173–183.
[45] T. Maruta, `http://www.mi.s.oskafu-u.ac.jp/ maruta/griesmer.htm`
[46] R. Mathon, New maximal arcs in Desarguesian planes, *j. Combin. theory*, Ser A, **97**(2002), 353–368.
[47] A. Rousseva, A General construction for blocking sets in finite affine geometries, *Compt. Rend. Acad. Bulg. des Sciences* **71**(4)(2018), 460-466.
[48] A. Rousseva, On the structure of some arcs related to caps and the non-existence of some optimal codes, *Ann. de l'Univ de Sofia*, 2020, to appear.
[49] B. Segre, Ovals in a finite projective plane, *Can. J. Math.* **7**(1955), 414–416.
[50] C. Shannon, A mathematical theory of communication, *Bell Systems Technical Journal* **27**(1948), 379–423.
[51] G. Solomon, J. J. Stiffler, Algebraically punctured cyclic codes, *Inf. and Control* **8**(1965), 170–179.
[52] J. Thas Construction of maximal arcs and partial geoemtries, *Geom. Dedicata* **3**(1974), 61–64.
[53] J.Thas, Constructions of maximal arcs and dual ovals in translation planes, *Eurpean J. Comb* **1**(1980), 189–192.
[54] M. A. Tsfasman, S. G. Vladut, Th. Zink, Modular curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound, *Mth. Nachr.* **109**(1982), 21–28.
[55] R. R. Varshamov, Estimate of the number of signals in error-correcting codes, *Dokl. Akad. Nauk SSSR* **117**(1957), 739–741.
[56] H.N. Ward, Divisibility of codes meeting the Griesmer bound, *Journal of Combinatorial Theory*, Ser. A, **83**(1998), 79–93.
[57] C. Zanella, Intersection sets in $AG(n,q)$ and a characterization of the hyperbolic quadric in $\mathrm{PG}(3,q)$, *Discrete Math.* **255**(2002), 381–386.