# АВТОРСКА СПРАВКА

за резултатите в трудовете на
**проф. Иван Николов Ланджев**,
представени за участие в конкурса за избор на
член-кореспонденти
в направление "Математически науки"

Трудовете, представени за участие в конкурса са са обединени условно в четири групи. В някои случаи това разделение е условно поради вътрешните връзки, съществуващи между тези области.

1. Работи по теория на кодирането
   1.1. Почти-МДР кодове
   1.2. Кодове над крайни верижни пръстени
   1.3. Оптимални линейни кодове
   1.4. Тъждества на МакУилямс
   1.5. Други работи по теория на кодирането
2. Работи по крайни геометрии
   2.1. Арки в крайни геометрии
   2.2. Шапки в крайни геометрии
   2.3. Блокиращи множества
   2.4. Спредове
   2.5. Арки с делимост
3. Работи по теория на дизайните
   3.1. Квазиостатъчни дизайни
   3.2. Дизайни с повтарящи се блокове
   3.3. $R$-аналози на дизайни
   3.4. Други работи по дизайни
   3.5. Работи по екстремална теория на множествата
4. Обзори и глави от книги

# 1 Работи по теория на кодирането

Основният проблем на теория на кодирането е точното или приблизително възстановяване на съобщение, генерирано на друго място и/или в друг момент. Съгласно забележителната теорема на Клод Шенън от 1948 г., съществуват (блокови) кодове със скорост, лежаща произволно близо до капацитета на използвания канал, както и такова правило за декодиране, че вероятността за грешка при декодиране на произволна кодова дума е по-малка от предварително фиксирана положителна константа. Въведените за доказателството на тази теорема стохастични кодове са с толкова голяма дължина, че практическото им използване едва ли някога ще бъде възможно. В този смисъл изключителна роля за приложенията има обратната теорема: Не е възможно предаването на данни по канал с шум с произволно малка вероятност за грешка при декодиране, когато скоростта на използвания код е по-голяма от капацитета на канала. Така конструирането на оптимални от математическа гледна точка кодове, както и на ефективни алгоритми за тяхното декодиране, се превръща в централна задача в теория на кодирането.

## 1.1 Почти-МДР кодове **[7, 11, 20]**

Класическото семейството на МДР-кодовете, т.е. кодове лежащи на границата на Сингълтън, е сред най-използваните класове линейни кодове. Така например кодирането на данните върху компакт-дискове се осъществява с кодове на Рид-Соломон, които са МДР кодове. Задачата за намиране на максималната дължиина на МДР-код с фиксирана размерност над фиксирано поле е решена само за прости полета и е открита в общия случай. Тя е еквивалентна на класическата задача за намиране на максималния брой точки в общо положение, които могат да бъдат избрани в крайната геометрия PG$(k, q)$. Наличните горни граници показват, че най-добрите МДР-кодове имат същия порядък като мощността на полето, над което се конструират. В много случаи това е неудовлетворително. В работи [7, 11, 20] се въвежда и изследва нов клас от кодове, които се отклоняват "малко" от границата на Сингълтън, но запазват в достатъчна степен свойствата на МДР-кодовете. Това е класът на т.нар. почти-МДР кодове.

Статиите [7, 11, 20] са посветени на изследването на почти МДР-кодове. Този важен клас линейни кодове бе въведен от Додунеков и Ланджев [7] и веднага предизвика огромен интерес у специалистите по теория на кодирането. В тази първа работа са направени няколко характеризации на почти-МДР кодовете, пресметнат е точния им спектър и са доказани долни и горни граници за максималната дължина $m'(k,q)$ на почти-МДР код с размерност $k$ над поле с $q$ елемента. По-специално доказано е, че

$$q + \lceil 2\sqrt{q} \rceil \leq m'(k,q) \leq 2q + k - 2,$$

като долната граница се получава от алгебрични криви от род 1 в $\mathrm{PG}(k,q)$, а горната граница се получава от геометрични съображения. Тези оценки не са подобрени и до днес.

В [7] и [11] са изследвани са връзките на почти МДР-кодове със специални множества от точки в проективни геометрии над крайни полета. Така, използвайки класификацията на $(9,3)$-арките в $\mathrm{PG}(2,4)$, в [11] е доказана единствеността на почти-МДР кодовете с параметри $[11,6,5]_4$, $[11,5,6]_4$ и $[12,6,6]_4$. Ще отбележим, че използвайки последния код Думер и Зиновиев получиха каскадно представяне на класическия двоичен код на Голей с параметри $[24,12,8]$. Като междинен резултат е получена и класификацичта на кодове с параметри $[10,4,6]_4$ и $[10,6,4]_4$. В [11] е решена и задачата за намиране максималната дължина на почти-МДР код над поле с четири елемента и произволна размерност.

Всички известни резултати за максималната дължина на почти-МДР кодове над малки полета ($q \leq 13$) са представени в работата [20]. Задачата е окончателно решена за $q \leq 5$, като за останали полета максималната дължина е ограничена в относително тесни граници.

Най-важна в тази група от статии е [7], която има около 150 цитирания и е отбелязана във всички монографии по теория на кодирането и крайни геометрии, появили се след 1995 г.

## 1.2 Кодове над пръстени [16, 19, 44]

Една от най-изследваните области в теория на кодирането през последните 15 години е линейни кодове над пръстени. Първоначално фокусът на тези изследвания бе върху пръстени от остатъци и по-специално $\mathbb{Z}_4$. Този интерес се подхранваше от изненадващото откритие, че класически семейства от нелинейни кодове (като тези на Кердок и Препарата) са всъщност двоични образи на кодове, които са линейни над $\mathbb{Z}_4$. Постепенно бяха получени добри кодове и над други пръстени и възникна необходимост от създаване на обща теория на линейните кодове над подходящ клас от пръстени. Този клас трябваше да бъде избран така, че да включва важни семейства като пръстени на Галоа, пръстени от остатъци, пръстени на дуалните числа и пр. При това теорията на тези кодове трябваше да е смислена, т.е. да позволява доказването на аналози на най-важните резулати от теорията на линейните кодове над крайни полета (като теорема на МакУилямс за еквивалентност на кодове, тъждества на МакУилямс и др.). Не на последно място кодовете на този клас трябваше да допускат удовлетворителна геометрична интерпретация. В поредица от статии написани в съавторство с Т. Хонолд показваме, че най-подходящият клас от пръстени за такава теория е класът на крайните верижни пръстени; по дефиниция това са пръстени, за които решетката от левите (десните) идеали образува верига.

В статия [19] е развита достатъчно пълно теорията на линейните кодове над крайни верижни пръстени. Голяма част от теорията на линейните кодове над полета може да бъде пренесена относително безпроблемно, но все пак се забелязват трудности, свързани със съществуването на некомутативни верижни пръстени. Това налага особено внимание при дефиниране на понятията дуален и самодуален код (по-коректно би било ортогонален и самоортогонален код). Понятието размерност на код също трябва да бъде предефинирано така, че да носи информация за мощността на кода. Оказва се, че и Хеминговата метрика не е особено добре пригодена за представяне на шумозащитните свойства на линейните кодове над верижни пръстени. Правилната теглова функция тук е т.нар. хомогенно тегло, въведено от Хайзе и Константинеску, явяващо се обобщение на теглото на Ли. В статия в [19] всички тези трудности са преодолени по един удовлетворителен начин.

В [19] са доказани и аналози на някои важни резултати от теория на линейните кодове над крайни полета. Дадено е комбинаторно доказателство на тъждествата на МакУилямс, които са обобщени по-късно в [23] за произволни кодове над квазифробениусови пръстени (които тривиално включват верижните пръстени). Принципно най-важният резултат в [19] е доказателството, че с всеки ляв линеен код с пълна дължина [1] над краен верижен пръстен $R$ може да се свърже мултимножество от точки в дясната геометрия на Йелмслев $\mathrm{PHG}(R_R^n)$ и то по такъв начин, че два кода са изоморфни, когато свързаните с тях мултимножества са проективно еквивалентни. Това позволява въвеждането на аналози на важни класове от кодове: кодове на Хеминг, Симплекс кодове, кодове на МакДоналд.

Едно от предимствата на кодовете над пръстени е това, че те да-

[1] Казваме, че кодът $C$ е с пълна дължина, ако никоя координата, не се съдържа в $\mathrm{Rad}\, R$.

ват каскадно представяне не само на нелинейни кодове, но и на важни линейни кодове над крайни полета. Исторически това е и първата мотивация за разглеждане на тези кодове. В работа [17] се излага теория на линейната представимост на кодове над малка азбука чрез линейни кодове над верижен пръстен. Въведено е т.нар изображение на Рид-Соломон, което е обобщение на класическото изображение на Грей, изпращащо $\mathbb{Z}_4$ във $\mathbb{F}_2^2$. Доказано е, че в случая на верижни пръстени с индекс на нилпотентност 2 това изображение е дори изометрия между $R^n$ с хомогенна метрика и $\mathbb{F}_q^{qn}$ с Хемингова метрика. Друг интересен резултат в [17] е следният: ако азбуката, в която изобразяваме линеен код над верижен пръстен $R$ е крайно поле $\mathbb{F}_q$ и $\operatorname{char} R = \operatorname{char} \mathbb{F}_q$, то образът на кода може да бъде направен линеен. Доказано е, че голяма част от кодовете на МакДоналд са линейно представими над верижния пръстен на $\sigma$-дуалните числа.

Работа [16] е посветена на една задача за линейната представимост на кодовете на Рид-Малер. Както отбелязахме по-горе, задачата за линейната представимост (над верижен пръстен) на важни класове от линейни (над крайно поле кодове) е с голяма важност в теория на кодирането. Още в класическата работа на Хамънс, Кумар, Калдербанк, Слоан и Соле за линейната представимост на кодовете на Кердок и Препарата бе повдигнат и въпроса за линейната представимост на кодовете на Рид-Малер. Те успяха да покажат, че кодовете на Рид-Малер от първи и втори ред са линейно представими над $\mathbb{Z}_4$. По-късно Лоу, Кахтонен и Копонен показаха, че кодовете на Рид-Малер $\mathcal{R}(r, m)$, $3 \leq r \leq m$ не са линейно предствими над $\mathbb{Z}_4$. Резултатът, доказан в [16] е, че всички двоични кодове на Рид-Малер са линейно представими над другия верижен пръстен с четири елемента – $\mathbb{F}_2[X]/(X^2)$.

В [44] са представени две нови конструкции за $R$-линейни кодове, съдържащи подкод, асоцииран със симплекс кода над пръстена $R$. Симплекс кодовете се дефинират като кодове, породени от матрица, имаща за стълбове хомогенните координати на всички точки в проективната геометрия на Йелмлсев $\mathrm{PHG}(R^k)$. Първата конструкция обобщава един неотдавнашен резултат на Кирмайер и Цванцгер за кодове с прозволна размерност. Обобщението е възможно благодарение на геометричната интерпретация, която даваме на тяхната конструкция. Тя се състои в добавянето на "несвободни" редове и стълбове към пораждащата матрица, имащи нули в позиции, отговарящи на някаква хубава конфигурация от точки (хиперовал). Втората конструкция използва вместо симплекс код, произволен линеен код, асоцииран с хубава арка в $\mathrm{PHG}(R_R^k)$.

Конструкциите работят и с двата верижни пръстена с четири елемента, но по-добри двоични кодове се получават при $R = \mathbb{Z}_4$.

## 1.3 Оптимални линейни кодове [8, 12, 14, 15, 18, 29, 30, 32, 34, 36, 41, 46, 51]

Централна задача в теория на кодирането е оптимизиране на един от трите основни параметъра на линеен код – дължина $n$, размерност $k$, минимално разстояние $d$ – ако останалите два са фиксирани. Така се достига до три оптимизационни задачи, най-силната от които е задачата за намиране на минималната дължина $n_q(k,d)$ на линеен код с фиксирана размерност $k$ и фиксирано минимално разстояние $d$ над поле с $q$ елемента. Тази задача е известна като основна задача на теория на кодирането. Една класическа граница е границата на Грийсмър: за всеки $[n,k,d]_q$-код е изпълнено

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

Линеен код с параметри $[g_q(k,d),k,d]_q$, наричаме код на Грийсмър.

Известно е, че кодове на Грийсмър съществуват за всяко достатъчно голямо $d$. Следователно, задачата за намиране на точната стойност $n_q(k,d)$ при фиксирани $k,q$ и за всички $d$ е крайна. За големи $k$ границата на Грийсмър е доста неточна съгласно един резултат на Додунеков. Затова е прието задачата за намиране на точната стойност на $n_q(k,d)$ да се атакува над малки полета и малки размерности за всички стойности на $d$. Към настоящия момент точните стойности на $n_q(k,d)$ са известни за $q = 2, k \leq 8$, $q = 3, k \leq 5$, $q = 4, k \leq 4$ и $q = 5, k \leq 3$. Кръгът от проблеми, възникващ около основниата задача на теория на кодирането, има ясно изразен геометричен характер. Някои от тях (като тази за максималната дължина на МДР-код) са известни в геометрична формулировка без връзка с теория на кодирането. Работи [8, 12, 14, 15, 18, 29, 30, 32, 34, 36, 41, 46] са посветени на този кръг от проблеми. Тъй като използваните методи в горните статии са геометрични, всички те могат да бъдат разглеждани като чисто геометрични работи. Ние ги включваме в този раздел, тъй като са мотивирани от основната задача на теория на кодирането и решават по същество проблеми на шумозащитното кодиране.

В осемте статии [8, 12, 14, 15, 18, 29, 30, 41] са приведени доказателства за несъществуване на някои кодове над полетата $\mathbb{F}_3$, $\mathbb{F}_4$ и $\mathbb{F}_5$. Изборът на параметрите, които се атакуват, не е случаен. Всички те са се оказвали в някакъв момент във фокуса на изследванията по оптимални кодове. Така например, $[143, 5, 94]_3$ и $[147, 5, 97]_3$ бяха последните параметри на хипотетични троични кодове с размерност 5, чието съществуване бе под въпрос. Съществуването или несъществуването на тези кодове решаваше задачата за намиране на точната стойност на $n_3(5, d)$ за всички $d$. По подобен начин изясняването на въпроса за съществуването на кодове с параметри $[51, 4, 37]_4$, $[56, 4, 41]_4$ и $[104, 4, 77]_4$ решаваше същата задача за кодове над $\mathbb{F}_4$ с размерност 4. В някакъв смисъл това бяха "най-трудните" параметри за съответните размерности.

Подходът към изследването на тези параметри е геометричен. Задачата за съществуване на кодове се преформулира като задача за съществуване на мултимножество от точки в някаква проективна геометрия. Използвайки геометрични техники и опирайки се на известни структурни резултати за арки в по-малките размерности, се доказват резултати за несъществуване.

Така например в [8] е отхвърлена възможността за съществуване на $[51, 4, 37]_4$-код. В [12] и [14] е доказано несъществуването на кодове за други осем тройки от параметри. Тези две статии решават напълно основната задача на теория на кодирането за кодове с размерност $k = 4$ над поле с четири елемента.

В [15] е доказано несъществуването на троични линейни кодове с параметри $[143, 5, 94]$ и $[147, 5, 97]$. С това точната стойност на $n_3(5, d)$ беше определена за $d = 94, 95, 96, 97, 98$ и 99. Този резултат даде окончателно решение на основната задача на теория на кодирането за троични кодове с размерност $k = 5$.

Техниките от горните четири работи са доразвити в [29, 30] и [41]. Макар фокусът на работите да е върху кодове над полета с четири и пет елемента, използваните техники позволяват формулиране на резултатите над произволни крайни полета. Така например един от главните резултати в [30] е, че Грийсмерови кодове съществуват над всички крайни полета за всички размерности $k$ при стойности на $d$ зададени чрез $q^{k-1} - q^{k-2} - q + 1 \leq d \leq q^{k-1} - q^{k-2}$. По-нататък $n_q(k, d) = g_q(k, d) + 1$ за $q^{k-1} - q^{k-2} - (s+1)q \leq d \leq q^{k-1} - q^{k-2} - sq$, където $1 \leq s \leq \sqrt{q} - 1$, при $q \geq 4$, $k = 4$, и $1 \leq s \leq q - 1$ при $q \geq 3, q \geq 5$. Разултатите в тези работи са доказани частично с използването на минихипери, геометричен обект въбведен от Хамада, който е обобщение на блокиращите множества и който е особено удобен при изследване на кодове.

В [32] се доказва обобщение на една теорема на Хил и Лизак за разширяване на линейни кодове, която се формулира така: Ако един

$[n,k,d]_q$, $q=p^s$, $p$ просто число, не допуска разширение, то броят на думите с тегло $i \not\equiv 0, d \pmod{q}$ надхвърля $q^{k-2} \cdot r(q)$, където $q+r(q)+1$ е минималната мощност на нетривиално блокиращо множество в $\mathrm{PG}(2,q)$. Доказателството на този резултат е чисто геометрично и се опира на едно свойство на арката, образувана от немаксималните равнини в дуалното проективно пространство. Този резултат е удобен инструмент за доказване на несъществуването на Грийсмерови кодове. В статията са приведени няколко такива доказателства за несъществуване на кодове над поле с четири елемента.

Обща теория на разширимостта на линейни кодове над крайни полета (и еквивалентно на арки в крайни геометрии) е развита в [50]. До този момент съществуваха отделни резултати като лемата на Хил-Лизак и няколко теореми на Марута, които при наличието на определени условия за спектъра на кода (арката) гарантират разширимост. В [50] въвеждаме т.нар. арки (съотв. кодове) с квазиделимост. С всяка такава арка $\mathcal{K}$ свързваме специална арка $\widetilde{\mathcal{K}}$ в дуалната геометрия, която се оказв арка със свръхделимост: кратностите на всички подпространства с размерност поне 1 са сравними с константа по модул реда на полето. Арка $\mathcal{K}$ (и асоциирания с нея код) е разширима точно когато съществува хиперравнина относно $\widetilde{\mathcal{K}}$ без точки с кратност 0.

В статия [51] е доказано с геометрични методи (развити в [50]) несъществуването на линейни кодове с параметри $[104,4,82]$ над $\mathrm{GF}(5)$. Това бе един от четирите открити случая на кодове с размерност 4 над полето с пет елемента. Съвсем наскоро, използвайки същите методи, ни се удаде да решим още един от откритите случаи: доказахме несъществуването на $[204,4,162]_5$-кодове. Този резултат все още не е непубликуван.

Работите [34, 36, 46] са посветени на минихипери. Известните конструкции на Белов-Логачев-Сандимиров имат естествено описание в термините на минихипери. От гледна точка на теория на кодирането много важен се оказва въпроса за описание на параметрите на минихипери, които се представят като сума на подпространства. Тази задача има удовлетворително решение само в двоичния случай.

През 1985 г. Хамада успя да характеризира проективните минихипери (допустимите кратности на точка са 0 и 1) с параметри

$$(\sum_{i=1}^{h} v_{\lambda_i+1}, \sum_{i=1}^{h} v_{\lambda_i})$$

в $\mathrm{PG}(k-1,q)$, за които $k-1>\lambda_1>\ldots>\lambda_h\geq 0$ като обединение на $h$ подпространства с размерност съответно $\lambda_1,\ldots,\lambda_h$. Тук $v_t=(q^t-1)/(q-1)$. В

[34] е доказана непроективната версия на този резултат:всеки минихипер с горните параметри в $\mathrm{PG}(k-1,q)$, за който са изпълнени неравенствата $k-1 > \lambda_1 > \ldots > \lambda_h \geq 0$ се представя като сума на подпространства с размерности $\lambda_1, \ldots, \lambda_h$. Разбира се, допустимо е размерностите $\lambda_i$ да са такива, че подпространствата да се пресичат.

Работа [36] е продължение на една статия на Хил и Уорд и се отнася само до равнинни минихипери. Това са мултимножества от $x(q+1)$ точки в $\mathrm{PG}(2,q)$, пресичащи всяка права в поне $x$ точки. Разбира се сума на произволно избрани $x$ прави е минихипер с такива параметри, но това не изчерпва всички възможности. В статията доказваме, че макар $(x(q+1),x)$-минихипер да не е непременно целочислена сума от прави, то той е винаги положителна рационална сума от прави. Представени са няколко нови конструкции на минихипери. Особено интересна е конструкцията на двутегловен минихипер за $x = 3q/4$, както и т.нар. switching construction. Доказано е, че за големи стойности на $x$ не съществуват неразложими минихипери.

В статия [46] са изследвани минихипери с параметри $(xv_t, xv_{t-1})$ в геометриите $\mathrm{PG}(t,q)$. Тази минихипери са характеризирани като неотрицателни рационални суми като с това са подобрени по ранни резултати от [36]. Установени се някои дълбоки връзки с теория на кодирането, което позволява построяването на нови класове от минихипери, които не могат да бъдат получени като целочислена сума на хиперравнини.

## 1.4 Тъждества на МакУилямс [13, 23]

Класическите тъждества на МакУилямс са доказани през 1963 г. и дават връзка между спектъра на линеен код и спектъра на неговия ортогонален код. От появяването им и до днес те са обект на усилване, уточняване и обобщаване. Работи [13] и [23] са посветени на тъждествата на МакУилямс. Статията [13] съдържа ново комбинаторно доказателство на едно обобщение на тъждествата на МакУилямс. Единственото комбинаторно доказателство към момента на написване на статията е това на Бруалди и Плес, което се отнася за класическата версия на тъждествата, т.е. за спектър на линеен код над поле по отношение на тегло на Хеминг. Нашето доказателство се отнася до спектъра на линеен код по отношение на произволно регулярно разбиване и произволно скаларно произведение в основното пространство. Макар това доказателство да е направено за линейни кодове над крайно поле, то се обобщава и за линейни кодове над крайни верижни пръстени. Комбинаторното доказателство за кодове над верижни пръстени се съдържа в докторската ми дисертация и не е публикуван в журнална статия.

Работата [23] съдържа доказателство на тъждествата на МакУилямс за линейни кодове над Фробениусови пръстени и спектри по отношение на т.нар. $\mathcal{W}$-допустими разбивания. Това е може би най-широкото възможно обобщение на тъждествата на МакУилямс, известно към настоящия момент.

## 1.5 Други работи по теория на кодирането **[6, 27, 50, 59, 61]**

Работа [27] е на границата между теория на кодирането и крайните геометрии. В нея са са дадени геометрични доказателства за някои класически резултати от теория на кодирането. Геометричният подход позволява значително усилване на някои от тях. Първият резултат е теоремата на Хил и Лизак за разширяване на линеен код. Тази теорема изненадващо се оказва еквивалентна на добре известния факт от крайните геометрии (срв. теоремите на Боуз-Бъртън и Бойтелспахер-Хайм), а именно че блокиращо множество чиято мощност е близка до мощността на хиперравнина съдържа хиперравнина. Това позволява отслабване на някои условия в теоремата на Хил-Лизак. Изложената тук идея по-късно бе доразвита от Марута в поредица от статии. Вторият резултат е теоремата на Додунеков за ранга на системата от думи с "малко" тегло в линеен код. Третият резултат е теоремата на Уорд за делимост на кодове над прости полета, лежащи на границата на Грийсмер. Изложеното в работата доказателство е различно от това на Уорд и използва т.нар. полиномиален метод. Предимство на това доказателство е, че позволява установяване на свойството делимост и за някои негрийсмерови кодове, при наличието някои допълнителни условия. Към този раздел може да бъде отнесена и статията [50], която описахме по-горе.

В края на 70-те години бе доказано, че общата задача за декодиране на линейни блокови код е $NP$-трудна. От гледна точка на приложенията се предпочитат кодове, за които съществува бърз алгоритъм за декодиране, пред кодове, чиито параметри са оптимални. Тази идея е залегнала в концепцията за LDPC-кодове (low density parity check codes), открита от Галагър през 1963 г. и проткрита от МакКий през 1985. В работата [6] са въведени два такива класа линейни кодове, зададени чрез проверочната им матрица. Тази матрица е разредена и се получава от структури на инцидентност, дефинирани над крайни афинни пространства. За дефинираните класове са предствени алгоритми за декодиране, които са със сложност по отношение на дължината на кода.

В статия [59] са изследвани кодове от подпространства с постоыанна размерност на сечението на кодовите думи. Направена е оценка за максималната размерност на пространството, породено от такъв код, кой9то е различен от "слънчоглед" (подпространствата в кода не се пресичат канонично). намерен е широк интерва;лот размерности за пространството, породено от думите в кода. направено е подобрение на резултат на Е. Горла и А. Раваняни за броя на центровете в код от подпространства с постоянна размерност на сечението.

Статия [61] е посветена на изследването ан нелинейни двоични кодове с две възможни разстояния между кодовите думи. По-специално фокусът е върху задачата за намиране на максималната мощност на двоичен код с дължина $n$ и разстояния $d_1 < d_2$. Тази мощност се означава с $A_2(n, \{d_1, d_2\})$. Доказано е, че ако $d_2 > 2d_1$, то

$$A_2(n, \{d_1, d_2\}) \leq n + 1.$$

Подобна граница е в сила и за кодове с $d_1 \not\equiv d_2 \pmod 2$.

$$A_2(n, \{d_1, d_2\}) \leq \begin{cases} n+1 & \text{за } d_1 \text{ четно}, \\ n+2 & \text{за } d_2 \text{ нечетно}. \end{cases}$$

Решена е и задачата за намиране на точната стойност на $A_2(n, \{2, d\})$, която се оказа равна на

$$A_2(n, \{2, d\}) \leq \begin{cases} \binom{n}{2} + 1 & \text{за } d = r, n \geq 6; \\ n & \text{за } 4 < d < n-1, \\ n+1 & \text{за } d = n-1. \end{cases}$$

Доказана е и общата граница

$$A_2(n, \{d_1, d_2\}) = \binom{n+2}{2},$$

без ограничения върху $d_1$ и $d_2$. Наскоро тази обща граница бе подобрена от Барг и др. до

$$A_2(n, \{d_1, d_2\}) = \binom{n}{2} + 1.$$

# 2 Работи по крайни геометрии

Работите в тази група са мотивирани от геометрични задачи макар и да имат отношения към изследванията по теория на линейните кодове. В работите се разглеждат както множества то точки в класическите геометрии $\mathrm{PG}(n,q)$, така и в проективните геометрии на Йелмслев $\mathrm{PHG}(R^n)$. Макар въведени в началото на XX век, последните представляваха доскоро интерес само за геометрията. Нашите изследвания показват, че тези геометрии са удобен език за получаване на резултати от теория на кодирането.

## 2.1 Арки в крайни геометрии **[24, 25, 31, 37, 40, 55, 56, 57, 60]**

В статии [24, 25, 31, 37, 40] е изследвана задачата за намиране на максималната мощност $m_n(2,R)$ на $(k,n)$-арка в проективната равнина на Йелмлсев $\mathrm{PHG}(R^3)$. Същата задача, поставена за равнините $\mathrm{PG}(2,q)$, е една от най-популярните задачи в крайните геометрии. Точно решение съществува за равнините от ред ненадхвърлящ 11. Към 2000 г. съществуваха само откъслечни резултати за арки в проективни равнини на Йелмлсев.

Основните резултати за арки в $\mathrm{PHG}(R^3)$, където $R$ е верижен пръстен с индекс на нилпотентност 2, се съдържат в [24] и [25]. Поради по-сложната структура на проективните равнини на Йелмслев е трудно дори да се даде горна граница за броя на точките в $(k,n)$-арка. В [24] е доказано, че

$$\begin{aligned} m_n(2,R) \le \max_{1\le u\le q^2} \min\{&u(q^2+q+1),\\ &q^2(n-1)+q(n-u)+u, q(q+1)(n-\lceil u/q\rceil)+u\}, \end{aligned}$$

Особено интересна граница е получена при $n=2$; тук $m_2(2,R)\le q^2+q+1$ за четно $q$ и $m_2(2,R)\le q^2$ за нечетно $q$. При това всеки клас на съседство съдържа не повече от една точка, като за $q$ четно празните класове са колинеарни във фактор-равнината. Оказва се, че над някои пръстени тази граница се достига, а над други – не.

Във [24] бе решена задачата за намиране на мощността на максималната $(k,n)$-арка при стойности на $n$ близки до $q^2+q$. Доказано бе че $m_{q^2+s}(2,R) = q^4+q^2s+qs$ за всяко $s=0,\dots,q-1$. Доказани бяха горни граници за някои специални параметри и бяха дадени голям брой конструкции, което доведе до създавене на таблици с мощностите на най-добрите известни $(k, n)$-арки в равнините над пръстените с 4,9,16 и 25 елемента. През следващите години тези таблици бяха многократно подобрявани. В момента те се поддържат от групата по изчислителна математика на Университета в Байройт.

В [31] е доказано, че $(q^2+q+1, 2)$-арки в равнини на Йелмслев над верижни пръстени $R$ с индекс на нилпотентност 2 съществуват тогава и само тогава, когато $\operatorname{char} R = 4$. Конструкцията използва точките, свързани с Тайхмюлеровата група от единици на някакво разширение на основния пръстен. Доказателството използва изоморфизма между пръстените на Галоа и пръстените на т.нар вектори на Вит, въведени от Е. Вит през 1937 г. Ние наричаме конструираните арки хиперовали, тъй като, точно както в класическия случай на хиперовали, те нямат допирателни.

В [37] са представени конструкции и доказателства за несъществуване на арки с някои специални параметри, които позволяват установяването на точната стойност на $m_n(2, R)$ в следните случаи:

$$m_5(2, \mathbb{Z}_9) = 39, m_5(2, \mathbb{S}_3) = 38, m_8(2, \mathbb{Z}_9) = m_8(2, \mathbb{S}_3) = 69,$$

където $\mathbb{S}_3 = \mathbb{F}_3[X]/(X^2)$.

В [40] е представена дуална конструкция за мултиарки в равнини на Йелмлсев, аналогична на конструкцията на Брауер-ван Ойпен. Конструкцията зависи от подходящо избрана функция $\tau$. Ако $\tau$ е линейна функция, то е възможно да бъдат пресметнати параметрите на т.нар $\tau$-дуална мултиарка. С дуалната конструкция получаваме арки в дуалната равнина (която в случаите на верижни пръстени не съвпада непременно с изходната). В случай на комутативни пръстени такива трудности не възникват. Разгледани са някои примери, най-интересният от които са арките, получени като дуални на хиперовалите. Те имат параметри $((q^4 - q)/2, q^2/2)$, две числа на пресичане 0 и $q^2/2$ и са оптимални.

Работа [26] е посветена на арки в класическите Дезаргови равнини $\mathrm{PG}(2, q)$. Там се разглеждат арки с параметри $(q^2 + q + 2, q + 2)$. Задачата за класифициране на арки с такива параметри е важна за теория на кодирането. Те са еквивалентни на $[q^2+q+2, 3, q^2]_q$-кодове, които често се появяват като остатъчни при решаване на основната задача на кодирането. В [26] са предствени няколко конструкции на такива арки. Показано е, че тези конструкции дават всички арки в равнините от ред, ненадхвърлящ 7. За равнини от ред 8 и 9 пълна класификация бе направена преди няколко години от Хил и Уорд. За съжаление, към настоящия момент пълната класификация на $(q^2 + q + 2, q + 2)$-арки за равнини от произволен ред изглежда невъзможно. За равнинии от четен ред тази задача изглежда тясно свързана с класификацията на максималните арки, което също е класически открит проблем в крайните геометрии.

Намерена е горна граница за броя на двойните точки в $(q^2+q+2, q+2)$-арка и е доказано, че съществуват арки с такъв брой двойни точки. Доказано е, че ако броят на двойните точки надхвърля реда на равнината, то арката притежава свойството делимост: кратостта на всяка права е сравнима с 2 по модул някаква степен на характеристиката на основното поле. Доказателството се опира на т.нар. полиномиален метод. Основната му идея може да бъде използвана за доказване на калсическия резултат на Уорд за делимост на грийсмерови кодове над прости полета. Това е направено в [27].

В работата [55] са изследвани арки в $\mathrm{PG}(r, q)$, за които числата на пресичане се съдържат в относително тесен интерщал $[w, w+\alpha]$, където $\alpha < \operatorname{char} \mathbb{F}_q$. В случая $\alpha = 0$ е известно (А. Бонисоли), че това са арките, при които всички точки в пространството са с една и съща кратнопст. За случаите $\alpha = 1$ и 2 ние доказваме, че тези арки се получават от константно-тегловните арки чрез добавяне/изтриване на една или две точки. При $\alpha = 2$ този резултат е в сила за геометриите с размерност поне 3. В равнината са изверстни много примери на арки с числа на пресичане $w, w+1, w+2$, най-известни от които са овалите и хипероватите, ермитивите криви, беровата подравнина в $\mathrm{PG}(2,4)$, $(15,3)$-арката в $\mathrm{PG}(2,7)$, свързана с дезарговата конфигурация и др.

В [56]е изследвано поведението на функцията $t_q(k)$, дефинирана като максималното отклонение от границата на Грийсмър на оптималната дължина на линеен код с фиксирана рамерност $k$;

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

Тук $g_q(k,d)$ е изразът в границата на Грийсмър, а $n_q(k,d)$ е оптималната дължина на линеен код с размерност $k$ и минимално разстояние $d$. Доказана е общата оценка $t_q(k) =)(q^{k/2})$, както и няколко специални резултати за $k = 3$. Най-силният от тях е $t_q(3) = O(\log q)$ за $q$ четно, което доказва една хипотеза на Бол за частния случай на полета с четна характеристика.

В [57] е изследвана основната задача на теория на кодирането за кодове над $\mathbb{F}_4$ с размерност 5. Задачата е разгледана в геометричната ѝ формулировка като задача за съществуване на арки с определени параметри в геометрията $\mathrm{PG}(4,4)$. Доказано е несъществуването на арки с параметри

$$(395,100),(396,100),(448,113),(449,113),$$

което води до несъществуването на кодове с параметри

$$[395,5,295]_4,[396,5,296]_4,[448,5,335]_4,[449,5,336]_4.$$

Това подобрява таблицата на Марута в четири пункта. Съществен страничен резултат е характеризацията на $(100,26)$- и $(113,29)$-арките в $\mathrm{PG}(3,4)$, която е направена без помощтта на компютър.

В [60] е се разглеждат арки в проективни геометрии на Йелмслев по отношение на хомогенната метрика, въведена от Хайзе и Константинеску. Тези арки се асоциират с линейно представими кодве над верижни пръстени. Хомогенната метрика се счита за по-естествена, когато арките се разглеждат в контекста на теория на кодирането. В работата са намрени връзки между параметрите на линейни кодове и тези на хомогенните арки. Направена е оценка на максималното хомогенно тегло $W$ в хомогенна $(N,W)$-арка. Характеризирани са константно-тегловните хомогенни арки като сума на линейни класове от точки. Представена е дуална конструкция за хогенни арки, като е доказано, че дуалната на двутегловна хомогенна арка е отново двутегловна хомогенна арка. Характеризирани са нови калсове двутегловни хомогенни арки, някои от които водят до силно регулярни графи.

## 2.2 Шапки в крайни геометрии **[22, 28, 38]**

Шапка наричаме множество от точки в крайна геометрия (обикновено се иска тя да е с размерност поне 3), никои три от които не лежат на една права. Централна задача е определянето на максималната мощност $m_2(n,q)$ на шапка в $\mathrm{PG}(n,q)$. Тази задача е тривиална за $q=2$, където максималната мощност е $2^n$. Задачата е решена за $n=3$ за всички полета $\mathbb{F}_q$, $q\geq 3$. Тук максималната мощност е $q^2+1$; тя се достига от елиптичните квадрики и т.нар. овоиди на Титс. Извън тези стойности са известни решения за няколко спорадични двойки $(n,q)$: в $\mathrm{PG}(4,3)$ и $\mathrm{AG}(4,3)$ максималната мощност е 20 и се достига за шапките на Пелегрино; в $\mathrm{PG}(5,3)$ максимумът е 56 и се достига за шапката на Хил; в $\mathrm{PG}(4,4)$ и $\mathrm{AG}(4,4)$ максималните мощности са съответно 41 и 40 като конструкцията е дело на Талини, а горната граница е доказана от Бирбрауер и Едел.

За да може да бъде атакувана задачата за намиране на максималната мощност на шапка в $\mathrm{PG}(6,3)$ е необходимо да се знаят всички пълни шапки в по-долната размерност. Най-голямата известна пълна шапка в PG$(5,3)$, различна от шапката на Хил (към 1999 г.) бе с мощност 43. В [22] е конструирана пълна шапка с мощност 48 и е доказано, че всяка шапка с поне 53 точки се разширява до шапката на Хил. По-нататък е доказана горната граница $m_2(6,3) \leq 154$; към момента на написването на [22] беше известна само, че $m_2(6,3) \leq 164$. По-късно бе доказано от други автори, отчасти с комптърни пресмятания, че 48 е и максималната мощност на шапка в PG$(5,3)$, различна от шапката на Хил.

Работата [28] продължава изследванията от [22]. В нея е доказано, че максималната мощност на шапка в AG$(5,3)$ е 45, както и единствеността на такава шапка. Тя се получава от шапката на Хил чрез изтриване на произволна 11-равина. Това е последният точен резултат за шапки, получен в последните 15 години.

В работата [38] е разгледано едно естествено обобщение на класическите шапки. Едно множество от точки в PG$(n,q)$ е $(\kappa,\nu)$-шапка, ако всяка права го пресича в не повече от $\nu$ точки. В [38] е доказана горна граница за мощността на такава шапка и са предствени няколко общи конструкции. Разгледани са няколко специални случая за малки стойност на $\nu, n$ и $q$ и са предствени добри експлицитни конструкции. По-специално, опредлена е максималната мощност на $(\kappa,3)$ шапка в PG$(3,5)$, която се оказва 44. С помощта на този резултат в работа [38] се решават четири от осемте открити случая на основната задача на теория на кодирането за $q=5, k=4$.

## 2.3 Блокиращи множества в крайни равнини **[33, 39, 47, 52, 58]**

Едно мултимножецво $\mathcal{K}$ от точки в крайна проективна равнина на Йелмслев $\Pi = \mathrm{PHG}(R^3)$ с множество от точки $\mathcal{P}$ наричаме $(k,n)$-блокиращо множество, ако $\sum_{x\in\mathcal{P}}\mathcal{K}(x)=k$ и $\sum_{x\in L}\mathcal{K}(x)\leq n$ за всяка права $L$ от $\Pi$. В [33] и [39] се изследват блокиращи множества в проективна равнина над верижен пръстен $R$ с $|R|=q^m$, $R/\operatorname{Rad}R\cong\mathbb{F}_q$.

В [33] доказваме, че за всяко $(k,n)$-блокиращо мултимножество с $1\leq n\leq q$, е изпълнено $k\geq nq^{m-1}(q+1)$. За разлика от класическите равнини блокиращо множество, лежащо на тази граница, не е непременно сума от прави. Ние доказваме. че ако $n<\operatorname{char}R$ неговият образ под действието на каноничния епиморфизъм $\pi^{(1)}: R\to\mathbb{F}_q$ е сума от прави във фактор-равнината. По специално, при $n=1$ най-малкото блокиращо множество е права и има мощност $k=q^{m-1}(q+1)$. Както и в класическия случай, правите се разглеждат като тривиални блокиращи множества и смисленият въпрос е за най-малкото блокиращо множество, несъдържащо права. Ние доказваме, че ако $R$ има подпръстен $S$ със $\sqrt{|R|}$ елемента, такъв, че $R$ е свободен като модул над $S$, то подравнината $\mathrm{PHG}(S^3)$ е неразложимо блокиращо множество с $n = 1$.

В специалния случай на верижен пръстен $R$ със $|R| = q^2$, $R/\operatorname{Rad} R \cong \mathbb{F}_q$ и $n = 1$, показваме, че минималното нетривиално блокиращо множество е с мощност $q^2 + q + 1$. Ние класифицираме всички блокиращи множества с тази мощност. Оказва се, че при $\operatorname{char} R = p$, $p$ просто число, съществуват две такива множества; при $\operatorname{char} R = p^2$ имаме единствено неразложимо блокиращо множество. За равнини над такива пръстени представяме клас от неразложими блокиращи множества с всяка от мощностите $q^2 + q + s$, къдтео $s \in \{1, \ldots, q + 1\}$.

В [39] продължаваме изследването върху нетривиални блокиращи множества в равнини над верижни пръстени $R$ с индекс на нилпотентност 2. Задачата е смислена единствено за равнини над пръстени на Галоа, защото в тях не същецвуват Берови подравнини. Ние модифицираме конструкцията на Редеи за блокиращи множества в класическите проективни равнини за равнини на Йелмслев над верижен пръстен $R$ с описаните свойства. По-специално ние доказваме следния резултат:

Нека $U$ е множество от $q^2$ точки в $\mathrm{AHG}(R_R^2)$. Безкрайната точка $(a)$ е определена от $U$, ако съществуват различни точки $P, Q \in U$, такива че $P, Q$ и $(a)$ са колинеарни в $\mathrm{PHG}(R_R^3)$. Нека $D$ е множеството от безкрайни точки, определени от $U$, а $D^{(1)}$ е множеството от съседни класове върхиу безкрайната права във фактор-геометрията, съдържаща точки от $D$. Ако $|D| < q^2 + q$, то съществува неразложимо блокиращо множество в равнината $\mathrm{PHG}(R_R^3)$ с мощност $q^2 + q + 1 + |D| - |D^{(1)}|$, което съдържа $U$. Ако $D$ съдържа представители на всички съседни класове върху безкрайната права, то $B = U \cup D$ е неразложимо блокиращо множество с мощност $q^2 + |D|$.

В статията са разгледани примери, когато $U = \{(x, f(x)) \mid x \in R\}$. В работата са дадени някои специално функции $f$, за които мощността на $D$ и $D^{(1)}$ може да бъде изчислена.

Работа [47] е посветена на блокиращи множестща в крайни афинни пространства. През 1991 г. А. Бруен доказа забележително неравенство за минималната мощност на $t$-кратно блокиращо множестщо в $AG(n, q)$: тч не надхвърля $(t+n-1)(q-1)+1$. За $t = 1$ тази граница се достига тривиално. За $t = 2$ С. Бол построи безкраен клас от блокиращи мнжества, лежащи на границата на Бруен в произволна размерност. До написването на [47] не бяха известни други примери на блокиращи множества, достигащи границата на Бруен. В [47] ние построяваме нов безкраен клас от блокиращи множества, достигащи границата на Бруен за които $t = q - n + 2$. Тази конструкция е използвана по-нататък за определяне на минималната мощност на блокиращо множество в $t = n - q + 1$, както и за някои други конструкции, даващи блокиращи множества с мощности близки до оптималните.

Работа [52] е посветена на изследването на арки със свръхделимост или т.нар. $(t \mod q)$-арки. Структурата на тези арки е съществена при изследване на разширимоста на арки в крайни проективни геометрии или на кодове над крайни полета. В работата е представена обща обща конструкция за такива арки, т.нар. lifting construction. Доказано е, че всяка $(t \mod q)$-арка може да се предстви като сума на lift-вани арки. за равнини от прост ред броят на арките в такава сума не надхвърля реда на полето.

Статия [58] е продължение на [52]. В нея са представени нови конструкции на афинни блокиращи множества, лежащи на границата на Бол. Последната е усилване на класическата граница на Бруен.Това са първите примери на блокиращи множества достигащи тази граница. Представента обща конструкция използва арки в $r$-мерни подпространства на $\mathrm{PG}(n,q)$ и блокиращо множеств в афинната част на допълнението, изоморфна на $\mathrm{AG}(n-r-1,q)$. Като резултат се получава блокиращо множество в $\mathrm{AG}(n,q)$. Безкрайният клас от $t$-блокиращи множества с $t = q - n + 2$ , лежащи на границата на Бруен от [47] се получава като специален случай на тази конструкция. Получени са и много примери на блокиращи множества, лежащи близо до границите на Бруен, Бол-Блохаус и Бол.

## 2.4 Спредове **[53]**

Нека $R$ е верижен пръстен с индекс на нилпотентност $m$. Едно множество $\mathcal{S}$ от $r$-мерни пространства на Йелмслев на $\Gamma = \mathrm{PHG}({}_RR^{n+1})$ се нарича $r$-спред, ако всяка точка на геометрията се съдържа в точно едно подпростравнство от $\mathcal{S}$. В [53] се разглеждат спредове, съдържащи само подпространства на Йелмслев, т.е. такива, получени от свободни подмодули. Доказано е, че $r$-спред в $\Gamma$ съществува тогава и само тогава, когато $r+1$ дели $n+1$. По-нататък представяме обобщение на една конструкция на Андре за $r$-спредове в класическите геометрии $\mathrm{PG}(n,q)$. Тя позволява конструирането на проективни равнини на Йелмслев от висок ред от $(t-1)$-спредове в $\mathrm{PHG}({}_R R^{2t})$. Естествено е да се разглеждат спредове и от нейелсмлемови подпространства. В този случай класическото необходимо условие престава да бъде достатъчно.

По-нататък в тази работа е намерено достатъчно условие за съществуването на спредове. То е най-силното достатъчно услощие известно до момента. Съществува хипотеза, че то е и необходимо. По-специално, $\lambda$-спред в геометрията $\mathrm{PHG}({}_R R^n)$ над верижен пръстен $R$ с дължина $m$ същецвува тогава и само тогава, когато $\lambda'_i$ дели $n$ за всяко $i = 1, \ldots, m$. Тук $\lambda' = (\lambda'_1, \ldots, \lambda'_m)$ е дуалното разбиване на $\lambda = (\lambda_1, \ldots, \lambda_n)$.

## 2.5 Арки с делимост [52, 54, 62, 63]

В тези четири работи е развита обща теория на разширимостта на арки в $\mathrm{PG}(k-1, q)$. Всички получени резултати могат да се формулират и за линейни кодове като това позволява унифицирано доказателство на редица резултати за разширимост, като теоремите на Хил-Лизак, Марута и Канда. Основната идея е да се въведе специален клас от арки със свръхделимост (наречени $(t \mod q)$, от чиито структурни свойства може да се извлече информация за разширимост/неразширимост на изследваните обекти.

Работа [52] е първата статия от тази група, в която е въведен класът на $(t \mod q)$-арките и са изследвани фундаменталните им свойства. Представени са няколко общи конструкции, най-важната от които е т. нар. lifting construction. Доказано е, че всяка $(t \mod q)$-арка може да се представи като сума на лифтвани арки, като в равнината $\mathrm{PG}(2, q)$ броят на сумандите не надхвърля $q$.

В [54] е представен унифициран подход към задачата за реазширимост. Доказано е, че разширимостта на една арка $\mathcal{K}$ зависи от наличието на хиперравнина в носителя на специална дуална арка $\widetilde{\mathcal{K}}$. Доказано е, че множеството на $(0 \mod q)$ арките е векторно пространство, което се поражда от допълненията на хиперравнините. Изследвани са $(t \mod q)$-арки за малки $t$, като в случая $t = 2$ и геометрии с размерност поне 3 такива арки са винаги лифтвани. От този резултат следва непосредствено теоремата на Марута, доказана по-рано, съгласно която всяка $(n, w)$-арка с числа на пресичане $\equiv n, n+1, n+2 \mod q$, $q \geq 5$, $q$ нечетно, е двукратно разширима. Като приложение на тези резултати е доказано, че всяка шапка с мощност $q^2 + 1 - t$, $t < t_0$, е разширима до елиптична квадрика. Тук $t_0$ е най-малкото естествено число, за което съществува нетривиално блокиращо множество с мощност $q + 1 + t_0$.

В [62] е направена пълна класификация на силните (максимална кратност на точка 3) ($3 \mod 5$)-арки в PG$(2,5)$ и PG$(3,5)$. Това е необходимо за доказване на несъществуването на $(104,22)$-арки в PG$(3,5)$ (или, еквивалентно, на кодове с параметри $[104,4,82]_5$. Класификацията позволи да се попълни една празнина в доказателството от [51]. Построени са три примера на ($3 \mod 5$)-арки, които не са лифтвани или сума на лифтвани. Тези арки са с мощности, съответно, 128, 143 и 168 и имат големи групи от автоморфизми.

В [63] е представена геометрични конструкции за трите арки от [62]. Арка с 128 точки се получава от първата от двете пълни 20-шапки в PG$(3,5)$, конструирани от Абатанджел-Корчмарош-Ларато. Другите две ($3 \mod 5$)-арки с мощности 143 и 168 се получават от елиптичната и хиперболичната квадрика в PG$(3,5)$. Представена е и об]а конструкция на ($t \mod q$)-арки с $\frac{q+1}{2}$, която е възможна в геометрии от произволна размерност над поле с нечетна характеристика. Получените от тази конструкция ($t \mod q$)-арки не са лифтвани.

# 3 Работи по теория на дизайните

## 3.1 Квазиостатъчни дизайни [3, 4]

В края на 80-те години на миналия век една от най-атакуваните задачи за блок-дизайни бе тази за конструиране на дизайн с параметри 2-$(22,8,4)$. Това бяха най-малките неразрешени параметри в таблиците на Матон и Роса. Забележително е, че това са параметри на квазиостатъчен дизайн, който не се разширява до симетричен 2-$(43,12,4)$. Последният не съществува съгласно теоремата на Брук-Райзър-Човла. Тази задача е поставена още в монографията на М. Хол Combinatorial Theory (1967). Работи [3] и [4] са мотовирани от тази задача.

В [3] е доказано, че пълната група от автоморфизми на хипотетичния 2-$(22,8,4)$-дизаин е 2-група или тривиалната група. Доказателството на този резултат не включва компютърни пресмятания. Несъществуването на дизайн с параметри 2-$(22,8,4)$ бе окончателно доказано от Кл. Лам и др. с помощта на компютър през 2000 г. Ще отбележим, че същите автори отхвърлиха дванадесет години по-рано с подобни техники съществуването на проективна равнина от ред 10.

Развитите техники в тази работа позволиха построяването на дизайн с параметри 2-$(28,10,5)$. Забележително е, че това също са параметри на квазиостатъчен дизайн, чийто симетричен не съществува по теоремата на Брук-Райзър-Човла. Това бяха и вторите неразрешени параметри в таблиците на Матон и Роса (случай 100 в монографията на М. Хол). Такъв дизайн е построен в [4]. Допускането, че съществува автоморфизъм от ред 3, фиксиращ една точка, води до единствена орбитна структура на такъв дизайн, която от своя страна се разширява по единствен начин. Доказателството не използва компютърни пресмятания.

## 3.2 Дизайни с повтарящи се блокове **[1, 2, 5]**

Работи [1, 2, 5] се отнасят до дизайни с повтарящи се блокове. Тези комбинаторни конфигурации играят важна роля в планирането на експеримента. Важна характеристика на такива дизайни минималната мощност на носителя $b^*_{\min}$, дефинирана минималния брой блокове, които са различни като подмножества на множеството от точки. В [1] е доказана нова долна граница за мощността носителя на блок-дизайн, подобряваща почти два пъти известните към момента граници. В [1] и [2] е намерена минималната мощност на носителя за радица конкретни множества от параметри: $v = 8, k = 3,\ v = 11, k = 3,\ v = 12, k = 4,\ v = 8, k = 4$.

В [5] са представени нови конструкции на дизайни с повтарящи се блокове като е дадено и частично решение на една задача поставена от Хедаят за съществуване на дизайни, които имат мощност на носителя точно $\binom{v}{2}$.

## 3.3 $R$-аналози на дизайни **[45, 49, 48]**

През последните десетина години изключително се засили интересът към изучаването на аналози на дизайни във връзка с използването им в мрежовото кодиране. Тези дизайни са интересни и сами по себе си, тъй като представляват интерсно обобщение на класическите комбинаторни дизайни. В [45] ние въвеждаме и изследваме аналози на дизайни в Грасманиана на подмодулите от даден тип на свободния модул $_R R^n$. Доказани са аналози на резултати класически дизайни. Доказано е, че при допускането на повтарящи се блокове $\tau$-дизайни съществуват за произволен тип $\tau$. Даден е пример на параметри на спредове (които могат да бъдат разглеждани и като дизайни), при които комбинаторното необходимо условие не е достатъчно.

В работата [49] е доказан аналог на калсическата теорема на Кантор за ранга на матрицата на инцидентност, на подпространства на $\mathrm{PG}(n, q)$

с фиксирана размерност. Ние доказваме, че в случая на пространства на Йелмслев и матрици, при които редовете са индексирани с подпространства на Йелмслев (т.е. свободни подмодули), матрицата е от максимален ранг. За случая, когато редовете са индексирани с подпространства (несвободни подмодули), ние строим пример при който матрицата на инцидентност не е от максимален ранг.

В [48] е пресметната детерминантата на матрицата на инцидентност на равнини на Йелмслев над произволни верижни пръстени.

## 3.4 Други работи по дизайни [9, 10]

Работа [9] е гранична между теория на дизайните и теория на кодирането. В редица случаи двоичните кодове, породени от матрицата на инцидентност на дизайни, имат добри коригиращи свойства. В [9] се изследвани кодовете породени от матриците на Щайнерови системи от тройки. Изследван е интересния въпрос, доколко една Щайнерова система се характеризира от породения от нея код, или с други думи, възможно ли е един код да съдържа неизоморфни Щайнерови системи от тройки. Доказано е, че класическите Щайнерови системи, получени от правите в $\mathrm{PG}(n-1,2)$ или правите в $\mathrm{AG}(n,3)$, се характеризират от кодовете си.

В [10] са представени нови конструкции на разделими дизайни, използващи Кронекерово произведение частични разностни матрици. Конструкциите обобщават по-ранни резултати на К. Арасу, В. Хамерс, Д. Юнгникел и А. Пот.

## 3.5 Работи по екстремална теория на множествата [64]

В [64] е изследван въпросът за максималната мощност на антиверига в решетката на частично нареденото множество от всички подмодули на несвободен модул $_RM$ над верижен пръстен $R$. Доказано е, че за пръстени с индекс на нилпотентност 2 и модули от тип $2^1 1^n$ тази решетка не е непременно от шпернеров тип. Намерени са точните стойности за мощността на максималните антивериги. Тези резултати са обобщени за модули от тип $m^1 1^n$ над верижни пръстени с индекс на нилпотентност $m$.

# 4 Обзори и глави от книги

В публикациите, представени за участие в конкурса е представен обзорът [21], една глава от книгата "Codes over Rings" [35], както и две глави от книгата "Current research topics in Galois geometries" [42, 43].

По мое мнение най-значимите резултати от работите, представени за участие в конкурса са следните:

- въвеждане и изследване на класа на почти-МДР кодовете;
- доказване на съществуване на хиперовали в равнини на Йелмслев над верижни пръстени с характеристика 4;
- развиване на геометрична теория на конфигурациите от точки в проективни геометрии на Йелмслев;
- доказване на обобщение на тъждествата на МакУилямс;
- доказаване на линейната представимост на кодовете на Рид-Малер над верижен пръстен с 4 елемента;
- намиране на максималната мощност на шапка в $\mathrm{AG}(5,3)$;
- конструирането на 2-$(28,10,5)$ дизайн;
- намиране на аналог на блокиращите множества от тип Редеи в проективни равнини на Йелмслев;
- намиране на геометрично доказателство и обобщаване на теоремата за разширимост на линейни кодове над крайно поле;
- представяне на конструкция за несвободно разширяване на симплекс-кодовете над верижни пръстени;
- намиране на дуална конструкция на арки в геометрии на Йелмслев;
- конструиран е нов клас афинни блокиращи множества, достигащи границата на Бруен;
- конструирани са първите примери на блокиращи множества, лежащи на границата на Бол;
- доказан е аналог на теоремата на Кантор за ранга на матрицата на инцидентност подпространства на подпространства в проективни пространства на Йелмслев;
- развита е теория на разширимостта на арки и линейни кодове, обхващаща всички известни до момента резултати за разширимост;

- намерено е най-силното (към настоящия момент) условие за съществуване на спредове в геометрии на Йелмслев над крайни верижни пръстени с прозволна дължина;

- доказани са граници за мощността на нелинейни двоични кодове с две разстояния;

- намерено е геометрично описание на три компютърно генерирани (3 mod 5)-арки в PG(3, 5) с мощности 128, 143 и 168;

- решена е задачаыта за намиране на максималната мощност на антиверига в решетката на подмодулите на несвободен модул от тип $2^1 1^n$ над верижен пръстен с индекс на нилпотентност 2.

## References


[1] A. S. Hedayat. I. Landjev, V. Tonchev, Results on the support of BIB designs, *Journal of Statistical Planning and Inference*, **22**, 1989, 295–306. [MR 90d:05037][ZBl 674.05006]

[2] A. S. Hedayat, J. Stufken, I. Landjev, The possible support sizes for BIB designs with $v = 8$, $k = 4$, *Journal of Combinatorial Theory Ser. A*, **51**, 1989, 258–267. [MR 91g:05014]

[3] I. Landjev, V. Tonchev, Automorphisms of 2-(22,8,4) designs, *Discrete Mathematics*, **77**, 1989, 177–189. [MR 91a:05011]

[4] J. H. van Lint, V. Tonchev, I. Landjev, A new design, Coding Theory and Design Theory, Part II, The IMA Volumes in Mathematics and Its Applications, Vol. 21, Springer 1990, 251–256. [MR 91f:05018]

[5] I. Landjev, On block designs with repeated blocks, *Discrete Mathematics*, **106/107**, 1992, 317–328.

[6] I. Landjev, A family of codes derived from finite affine spaces, *Atti del Seminario Matematico e Fisico dell'Universita di Modena*, **XLII**, 1994, 455–466.

[7] S. Dodunekov, I. Landjev, On near-MDS codes, *Journal of Geometry*, **54**, 1995, 30–43.

[8] R. Hill, I. Landjev, T. Maruta, On the nonexistence of $[51, 4, 37]_4$ codes, *Finite Fields and Their Applications*, **2**, 1996, 96–110.

[9] A. Baartmans, I. Landjev, V. Tonchev, On the binary codes of Steiner Triple Systems, *Designs, Codes and Cryptography*, **8**(1996), 29–43.

[10] I. Landjev, Constructions of group divisible designs, *Designs, Codes and Cryptography*, **8**, 1996, 309–318.

[11] S. Dodunekov, I. Landjev, On the quaternary [11,6,5] and [12,6,6] codes, Applications of Finite Fields (ed. D. Gollmann), IMA Conference Series 59, Clarendon Press, Oxford, 1996, 75–84.

[12] R. Hill, I. Landjev, On the nonexistence of some quaternary codes, Applications of Finite Fields (ed. D. Gollmann), IMA Conference Series 59, Clarendon Press, Oxford, 1996, 85–98.

[13] I. Landjev, A note on the MacWilliams identities, *Compt. Rend. Bulg. Acad. Sci.*, **50**(9-10), 1997, 17–18.

[14] I. Landjev, Optimal linear codes of dimension 4 over $\mathbb{F}_5$, Lecture Notes in Comp. Science, **1255**, 1997, 212–220.

[15] I. Landjev, The nonexistence of some ternary optimal codes of dimension five, *Designs, Codes and Cryptography* **15**, 1998, 245–258.

[16] T. Honold, I. Landjev, All Reed-Muller codes are linearly representable over the ring of dual numbers over $\mathbb{Z}_2$, *IEEE Trans. on Information Theory*, **45**, 1999, 700-701.

[17] T. Honold, I. Landjev, Linearly representable codes over chain rings, *Abhandlungen des Mathematischen Seminars der Universität Hamburg*, **69**, 1999, 187–203.

[18] I. Landjev, T. Maruta, On the minimum length of quaternary linear codes of dimension five, *Discrete Mathematics*, **202**, 1999, 145–161.

[19] T. Honold, I. Landjev, Linear codes over finite chain rings, *Electronic Journal of Combinatorics*, **7**(1), 2000, R11.

[20] S. Dodunekov, I. Landjev, Near-MDS Codes over some small fields, *Discrete Mathematics*, **213**, 2000, 55–65.

[21] I. Landjev, Linear codes over finite fields and finite projective geometries, *Discrete Mathematics*, **213**, 2000, 211-214.

[22] R. Hill, C. Jones, I. Landjev, L. Storme, J. Barat, On complete caps in the projective geometries over $\mathbb{F}_3$, *Journal of Geometry*, **67**, 2000, 127-144.

[23] T. Honold, I. Landjev, MacWilliams identities for codes over finite Frobenius rings, In: *Finite Fields and Applications* (eds. D. Jungnickel, H. Niederreiter), Springer, 2000, 276–292.

[24] И. Н. Ланджев, Т. Хонольд, Дуги в проективных ельслемовых плоскостях, Дискретная Математика 13(1)(2001), 90-109. English translation: Arcs in projective Hjelmslev planes, *Discrete Mathematics and Applications* **11**, 2001, 53–70.

[25] T. Honold, I. Landjev, On arcs in projective Hjelmslev planes, *Discrete Mathematics*, **231**, 2001, 265–278.

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

[27] I. Landjev, The geometric approach to linear codes, in: *Finite Geometries* (eds. A. Blokhuis, J. Hirschfeld, D. Jungnickel, J. Thas), Ser. Developments in Mathematics, 2001, 247–257.

[28] Y. Edel, S. Ferret, I. Landjev, L. Storme, The classification of the largest caps in $AG(5,3)$, *Journal of Combinatorial Theory* Ser. A, 99(2002), 95–110.

[29] R. Hill, I. Landjev, A. Rousseva, T. Maruta, On optimal codes over the field with five elements, *Designs Codes and Cryptography*, 29(2003), 165–175.

[30] T. Maruta, I. Landjev, A. Rousseva, On the minimum size of some minihypers and related linear codes, *Designs, Codes and Cryptography* **34**(2005), 5–15.

[31] T. Honold, I. Landjev, On maximal arcs in projective Hjelmslev planes over chain rings of even characteristic, *Finite Fields and Their Applications* **11**(2005), 292–304.

[32] I. Landjev, A. Rousseva, An extension theorem for arcs and linear codes, *Problems of Information Transmission* 42(4)(2006), 65–76.(with A. Rousseva)

[33] I. Landjev, On blocking sets in projective Hjelmslev planes, *Advances in Mathematics of Communication* 1(2007), 65–82.

[34] I. Landjev, L. Storme, A weighted version of a result of Hamada on minihypers and on linear codes meeting the Griesmer bound, Designs, Codes and Cryptography 45 (2007), 123-138.

[35] T. Honold, I. Landjev, Linear codes over finite chain rings and projective Hjelmslev geometries, Codes over Rings, edited by Patrick Sole (CNRS, France) Series on Coding Theory and Cryptology - Vol. 6, World Scientific, 2009, 60-123. (ISBN 978-981-283-768-4; ISBN 981-283-768-X).

[36] I. Landjev, L. Storme, A study of $(x(q+1), x; 2, q)$-minhypers, Designs, Codes and Cryptography 54, No 2 (2010), 135-147.

[37] T. Honold, M. Kiermaier, I. Landjev, New arcs of maximal size in the projective Hjelmslev planes of order 9, *Compt. Rend. Acad. Bulg. Sci.* 63, No 2 (2010), 171-180.

[38] I. Edel, I. Landjev, On multiple caps in finite projective spaces, Designs Codes and Cryptography 56(2010), 163-175.

[39] I. Landjev, S. Boev, Blocking sets of Redei type in projective Hjelmslev planes, *Discrete Mathematics* 310(2010), 2061-2068.

[40] T. Honold, I. Landjev, The dual construction for arcs in projective Hjelmslev spaces, Advances in Matehmatics of Communications, 5(2011), 11-21.

[41] I. Landjev, A. Rousseva, Characterization of some optimal arcs, Advances in Matehmatics of Communications, 5(2011), 317-332.

[42] T. Honold, I. Landjev, Codes over rings and ring geometries, chapter 7 in: "Current research topics in Galois geometries" (eds. L.Storme and Jan De Beule) NOVA Publishers, 2012, 161-186. (ISBN 978-1-61209-523-3)

[43] I. Landjev, L. Storme, Linear codes and Galois geometries, chapter 8 in: "Current research topics in Galois geometries" (eds. L. Storme and J. De Beule), NOVA Publishers, 187-214. (ISBN 978-1-61209-523-3)

[44] T. Honold, I. Landjev, Non-free extensions of the Simplex codes over a chain ring with four elements, Designs, Codes and Cryptography 63(2012), to appear.

[45] M. Kiermaier, I. Landjev, Designs in projective Hjelmlsev spaces, in: Theory and Applications of Finite Fields (eds. M. Lavrauw et al.) Contemporary Mathematics vol. 579, 2012, 111-122.

[46] I. Landjev, P. Vanderdriesche, A note on $(xv_t, xv_{t-1})$-minihypers in PG$(t, q)$, Journal of Combinatorial Theory Ser. A 119(2012), 1123–1131. DOI: 10.1016/j-jcta.2012.02.009

[47] I. Landjev, A. Rousseva, On the sharpness of Bruen's bound for intersection sets in Desarguesian affine spaces, Designs, Codes and Cryptography 72(2014), 551–558.

[48] I. Landjev, P. Vandendriesche, On the point-by-subspace incidence matrices of projective Hjelmslev planes, Compt. Rend. Acad. Bulg des Sci. 67(11)(2014), 1485-1489.

[49] I. Landjev, P. Vandendriessche, On the rank of incidence matrices in projective Hjelmslev spaces, Designs, Codes and Cryptography 73(2014), 615–623.

[50] I. Landjev, A. Rousseva, L. Storme, On the extendability of quasidivisible Griesmer arcs, Designs, Codes and Cryptography 79(2016), 535-547.

[51] I. Landjev, A. Rousseva, The nonexistence of $(104, 22; 3, 5)$-arcs, Advances in Mathematics of Communications 10(3)(2016), 601–611.

[52] I. Landjev, A. Rousseva, A note on divisible arcs in projective spaces of prime order, *Compt. Rend. Acad. Bulg. des Sci.* **70**(2017), 13–20.

[53] I. Landjev, N. Georgieva, Conditions for the existence of spreads in projective Hjelmslev spaces, *Designs, Codes and Cryptography* **87**(4)(2019), 785–794.

[54] I. Landjev, A. Rousseva, Divisible arcs, divisible codes and the extension problem for arcs and codes, *Problems of Information Transmission* **55**(3)(2019), 226-240.

[55] I. Landjev, A. Rousseva, L. Storme, On Linear Codes of Almost Constant Weight and the Related Arcs, *Comptes rendus, de l'Academie Bulgare des Sciences* **72**(12)(2019), 1626-1633.

[56] 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.

[57] I. Landjev, A. Rousseva, The Geometric Approach to the Existence of Some Quaternary Griesmer Codes, *Designs, Codes and Cryptography* **88**(9)(2020), 1925-1940.

[58] I. Landjev, A. Rousseva, A General Construction for Blocking Sets in Finite Affine Geometries, *Results in Mathematics* **75** #142, 2020, 1-12,

[59] L. Hernandez-Lucas, I. Landjev, L. Storme, P. Vandendriessche, A stability result and a spectrum result on constant dimension codes, *Linear Algebra and its Applications* **621**(2021), 193–213.

[60] T. Honold, I. Landjev, On homogeneous arcs and linear codes over finite chain rings, *AAECC* **34**(3)(2023), 359–376.

[61] I. Landjev, A. Rousseva, K. Vorobev, Constructions of binary codes with two distances, *Discrete Mathematics* **346**(2023), 113337.

[62] S. Kurz, I. Landjev, A. Rousseva, Classification of (3 mod 5) arcs in PG(3,5), *Advances in Mathematics of Communications* **17**(1)(2023), 172-206.

[63] S. Kurz, I. Landjev, F. Pavese, A. Rousseva, The geometry of (t mod q)-arcs, *Designs, Codes and Cryptography*, 2024.

[64] I. Landjev, E. Rogachev, Sperner's theorem for non-free modules over finite chain rings, *Designs, Codes and Cryptography*, 2024.