Нов Български Университет

Департамент Информатика

Невяна Димитрова Георгиева

МРЕЖОВО КОДИРАНЕ И АНАЛОЗИ НА ДИЗАЙНИ

Автореферат

на дисертация
за присъждане на образователната и научна степен
"доктор"
по професионално направление
4.6. Информатика

Научен ръководител: проф. дмн Иван Ланджев
София, 2022 г.

Дисертационният труд е в обем от 78 страници и се състои от увод, три глави и литература, включваща 85 заглавия.

Настоящият дисертационен труд е посветен на задачата за съществуване на дизайни в проективни координатни геометрии над крайни верижни пръстени. Тези геометрии са известни като геометрии на Йелмслев. Изучаването им започва още в началото на XX век от датския математик Йоханес Йелмслев, но сериозен напредък в разбирането им е направен с работите на Барбилиан, Клингенберг, Артман [1, 2, 3, 29, 30]

В класическите координатни геометрии координатите на точките са елементи на поле или тяло. Първата стъпка в разглеждането на геометрии над пръстени е направена от Корадо Сегре през 1911 г. в [49]. Той разглежда тримерна проективна геометрия над пръстена на дуалните числа $\mathbb{R}[\varepsilon]$ с $\varepsilon^2 = 0$, както и над някои други разширения на $\mathbb{R}$. По това време верижни пръстени над реалните числа вече са разглеждани и в геометриите на Грюнвелд, Петерсен, Щуди и Оскар Клайн (виж литературата в [51]). Появяването им не е изненадващо и вече се е случило в механиката. В периода 1929-1949 г. Й. Йелмслев предлага "по-естествен поглед към геометрията", който е в "по-точно съответствие с физическата реалност" [19, 20, 21]. Систематично изследване на проективни равнини над широк клас асоциативни пръстени е предприето от Д. Барбилиан (1940-1941) [3]. Получената от него аксиоматика е неудовлетворителна, защото е отчасти с геометрична и отчасти с алгебрична природа, отнасяща се до координатния пръстен.

Изследванията на Сегре и Йелмслев са продължени от Клингенберг [29, 30], Клайнфелд [28], Дрейк [7, 8, 9], Дембовски [6], Кронхайм [5] и други автори, които представят аксиоматика за проективни и афинни равнини над пръстени на Йелмслев и описват основните им свойства. Това са локални пръстени, удовлетворяващи някои допълнителни условия.

Задачата за съществуване, която изследваме в този дисертационен труд, макар и да представя чисто геометричен проблем, се мотивира най-вече от връзката с теория на кодирането. В края на XX век беше доказано, че две известни семейства нелинейни кодове – тези на Кердок и Препарата [48] – се представят като двоични образи на кодове

над $\mathbb{Z}_4$ [43, 18]. С работите на А. А. Нечаев и Джей Ууд [42, 43, 44, 46, 47, 52, 53, 54, 55] бе поставено началото на изследването на линейни кодове над крайни пръстени. По същото време изследването на линейни кодове беше свързано с това на специални множества от точки в геометрии на Йелмслев. В работите на Т. Хонолд и И. Ланджев беше доказана еквивалентността на линейните кодове с пълна дължина над крайни верижни пръстени и мултимножествата от точки в координатните геометрии над тези пръстени [22, 23, 24].

Случайното мрежово кодиране възниква от една работа на Р. Кьотер и Ф. Кшишанг от 2008 г. [31]. Нека $\mathbb{F}_q$ е крайното поле от ред q и нека $\mathcal{P}_q(n)$ е множеството на всички подпространства на $\mathbb{F}_q^n$ – векторното пространство на всички n-орки над $\mathbb{F}_q$. Код от подпространства Ω с дължина на пакета n над $\mathbb{F}_q$ наричаме всяко непразно множество от елементи на $\mathcal{P}_q(n)$. Еквивалентно, един код от подпространства може да се разглежда като множество от подпространства в $\mathrm{PG}(n-1,q)$. Код Ω, в който всички подпространства са с една и съща размерност, се нарича код с постоянна размерност. Такъв код е например:

$$\Omega = \left\{ \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix} \right\}$$

Това е двоичен код от подпространства с постоянна размерност 2 и дължина на пакета 4. В същото време двумерните подпространства, породени от редовете на тези матрици, могат да се разглеждат като прави в $\mathrm{PG}(3,2)$. Нещо повече – тези прави образуват специална конфигурация, наречена спред от прави в $\mathrm{PG}(3,2)$, т.е. множество от прави което представлява разбиване на точковото множество на $\mathrm{PG}(3,2)$. Така всяка дума на кода е права от $\mathrm{PG}(3,2)$.

В $\mathcal{P}_q(n)$ се въвежда специална метрика, наречена рангова метрика, която задава разстоянията между кодовите думи на код от подпространства. За $U, V \in \mathcal{P}_q(n)$ дефинираме:

$$\begin{aligned} d_S(U,V) &= \dim(U+V) - \dim(U \cap V) \\ &= \dim U + \dim V - 2\dim(U \cap V) \\ &= 2\dim(U+V) - \dim U - \dim V. \end{aligned}$$

Минималното разстояние на код от подпространства се задава чрез

$$d_S(\Omega) = \min\left\{d_S(U,V) |\ U, V \in \Omega, U \neq V\right\}.$$

Нека предаването на данни се извършва по т.нар. операторен канал [26] чрез използването на код от подпространства Ω с дължина на пакета n. Нека при изпращане на думата U са възникнали ρ изтривания и t грешки като в резултат е получена думата V. Ако $2(\rho + t) < d_S(\Omega)$, то декодер, работещ по принципа за декодиране в най-близкия съсед (в смисъл на ранговата метрика), възстановява изпратената дума U. За кодове в рангова метрика съществуват аналози на всички класически граници като границата на сферичната опаковка, границата на Сингълтън, границата на Джонсън, границата на Варшамов-Джилберт и т.н.

Както в класическата теория на кодирането двете основни посоки на изследване са:

- Конструиране на оптимални мрежови кодове (например с максимален брой думи при зададени други параметри).
- Създаване на алгоритми за ефективно декодиране на зададени мрежови кодове.

Настоящият дисертационен труд може да се разглежда като принос към първата задача. Интересът към кодове от подпространства се появява и преди приложението им в мрежовото кодиране. Задачата за намиране и характеризиране на q-аналози на класически комбинаторни конфигурации е значително по стара [38] (Глава 24). Теория на дизайните е добре развита област, която има очевидни връзки с теория на кодирането. Много известни комбинаторни резултати като теоремите на Шпернер [50] и Ердьош-Ко-Радо [10] имат своите q-аналози

[15, 25, 38]. В последните няколко години изключително се увеличи броят на изследванията по q-аналози на дизайни като някои задачи се радваха на голяма популярност – такава е задачата за съществуване на q-аналози на Щайнерови системи [4, 11, 12, 14]. Резултатите от тази дисертация могат да се разглеждат и като принос към този кръг задачи, при които крайното поле се заменя с краен верижен пръстен.

Настоящият дисертационен труд се състои от увод, три глави и списък на използваната литература.

В **глава 2** са въведени основните обекти, изследвани в този дисертационен труд и са формулирани някои от по-важните резултати, отнасящи се до тях. В раздел 2.1 са въведени верижните пръстени с условието техните идеали да образуват верига по включване. Представени са примери за някои важни класове верижни пръстени като пръстените на σ-дуалните числа и пръстените на Галоа. Формулирана е основната характеризационна теорема за верижни пръстени, съгласно която всеки верижен пръстен се представя като факторпръстен на пръстен от полиноми. По-нататък е въведено канонично представяне на елементите на произволен пръстен, както и линейна наредба върху тях, която се използва при компютърното представяне на елементите на такива пръстени и в алгоритмите за работа с модули в **глава 3**. Изложените дефиниции са демонстрирани върху примера на пръстен на Галоа с 16 елемента над $\mathbb{F}_4$.

В раздел 2.2 са изложени някои фундаментални факти за модули над крайни верижни пръстени. Формулирана е основната структурна теорема за модули над верижни пръстени, която е следствие на общата теорема на Крул-Шмид. Дефинирани са понятия като тип на модул, ранг и свободен ранг на модул, дуален тип. По-нататък е изложен основният комбинаторен резултат на този раздел, определящ броя на подмодулите от даден тип μ, съдържащи се във фиксиран R-модул от тип λ. Този брой се оказва произведение на Гаусови коефициенти. В края на раздел 2.2 е формулирана теорема, която характеризира ортогоналния модул $M_R^{\perp}$ на фиксиран модул ${}_RM$.

В раздел 2.3 са представени някои важни дефиниции за проективни геометрии на Йелмслев. Тези геометрии се въвеждат по аналогичен

начин с класическите геометрии $\mathrm{PG}(n-1,q)$ като в дефиницията крайното поле $\mathbb{F}_q$ се заменя с верижен пръстен R. При зададен свободен модул $M = {}_R R^n$ множеството от точки се състои от всички свободни подмодули на M от ранг 1, прави са свободните подмодули на M от ранг 2 като инцидентност се дефинира чрез теоретико-множествено включване. Разликата с класическия случай се състои в това, че две точки са инцидентни с *поне една* права; две точки, които са едновременно инцидентни с повече от една права се наричат съседни. Геометриите на Йелмслев могат да се въведат и аксиоматично. Известно е [32, 33, 34, 35, 36], че при определени естествени условия, те се координатизират с верижни пръстени. Редица резултати за класически геометрии над крайни полета имат свои аналози за геометрии на Йелмслев [39, 40]. В тази работа се разглеждат само координатни геометрии на Йелмслев.

Релацията на съседство може да се продължи върху прави и въобще върху подпространства от произволен тип. Тя се оказва релация на еквивалентност върху подпространствата от един и същи тип. Класовете на еквивалентност се оказват добре структурирани. Те могат да бъдат вложени в геометрии на Йелмслев над верижни пръстени с по-нисък индекс на нилпотентност. Този важен структурен резултат е формулиран в раздел 2.3.

Оригиналните приноси на дисертационния труд се съдържат в глави 3 и 4.

Глава 3 е посветена на намирането на стандартна форма на матрица над верижен пръстен R. Този въпрос е от голяма практическа важност поради необходимостта от ефективен начин за представяне на подмодулите на ${}_R R^n$ и операциите с тях в компютърни пресмятания. Казваме, че матрицата $A = (a_{ij})_{k\times n}$, $a_{ij} \in R$, $\operatorname{rad} R = R\theta$ е в стандартна форма, ако са изпълнени условията:

(1) $a_{ij_i} = \theta^{m-t_i}$, $t_i \in \{0, \dots, m\}$;
(2) $a_{is} = \theta^{m-t_i+1}\beta$, $\beta \in R$, за всяко $s < j_i$;
(3) $a_{is} = \theta^{m-t_i}\beta$, $\beta \in R$, за всяко $s > j_i$;
(4) $a_{sj_i} \prec a_{ij_i}$ за всяко $s \neq i$ (тук $\prec$ е лексикографската наредба, въведена в раздел 2.1);
(5) $j_1 < j_2 < j_3 < \dots$.

Основният резултат тук се съдържа в следната теорема:
Теорема 3.3. За всеки R-модул ${}_RM \leq {}_RR^n$ съществува единствена матрица в стандартна форма, чиито редове го пораждат.
До края на главата са описани алгоритми за работа с модули. Те включват:

(A) Привеждане на матрица в стандартна форма;
(B) намиране на матрица, пораждаща обединението на два зададени модула;
(C) проверка дали даден модил U е подмодул на друг модул V.

След това формулираме резултат, с който се получава ортогоналния модул $M_R^{\perp}$ на даден модул ${}_RM$, породен от редовете на матрица в стандартна форма. Ортогоналният модул се поражда от редовете на матрица над R, която е зададена експлицитно.
Теорема 21. Нека ${}_RM$ е подмодул на ${}_RR^n$, породен от редовете на матрицата A, която има вида

$$\begin{pmatrix} I_{k_0} & A_{01} & A_{02} & \dots & A_{0,m-1} & A_{0,m} \\ 0 & \theta I_{k_1} & \theta A_{12} & \dots & \theta A_{1,m-1} & \theta A_{1,m} \\ 0 & 0 & \theta^2 I_{k_2} & \dots & \theta^2 A_{2,m-1} & \theta^2 A_{2,m} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & \theta^{m-1} I_{k_{m-1}} & \theta^{m-1} A_{m-1,m} \end{pmatrix}.$$

Тогава, $M_R^{\perp}$ се поражда от матрицата

$$B = \begin{pmatrix} B_{0,m} & B_{1,m} & B_{2,m} & \cdots & B_{m-2,m} & B_{m-1,m} & I_{k_m} \\ B_{0,m-1}\theta & B_{1,m-1}\theta & B_{2,m-1}\theta & \cdots & B_{m-2,m-1}\theta & I_{k_{m-1}}\theta & 0 \\ B_{0,m-2}\theta^2 & B_{1,m-2}\theta^2 & B_{2,m-2}\theta^2 & \cdots & I_{k_{m-2}}\theta^2 & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ B_{02}\theta^{m-2} & B_{12}\theta^{m-2} & I_{k_2}\theta^{m-2} & \cdots & 0 & 0 & 0 \\ B_{01}\theta^{m-1} & I_{k_1}\theta^{m-1} & 0 & \cdots & 0 & 0 & 0 \end{pmatrix},$$

където $k_m = n - k_0 - \ldots - k_{m-}$ и

$$B_{ij} = -(A_{ij} - \sum_{1<k<j+1} A_{ik}A_{k,j+1} + \sum_{i<k<l<j+1} A_{ik}A_{kl}A_{l,j+1} - \cdots + (-1)^{j-i+1} A_{i,i+1}A_{i+1,i+2}\ldots A_{j,j+1})^T.$$

По-нататък са представени и алгоритми за:

(D) намиране на ортогоналния модул $M_R^{\perp}$ на даден модул ${}_RM$;
(E) алгоритъм за намиране на сечението на два модула ${}_RM$ и ${}_RN$;
(F) пораждане на всички подмодули от фиксиран тип на даден модул ${}_RM$.

Глава 4 е посветена на намирането на необходими и достатъчни условия за съществуване на спредове в проективни геометрии на Йелмслев. В раздел 4.1 са въведени R-аналози (аналози над верижни пръстени R) за различни типове дизайни. Най-напред е дефиниран Грасманианът $\mathcal{G}_R(n,\kappa)$ като множеството на всички леви подмодули на ${}_RR^n$ от тип κ, където $\kappa = (k_1,\ldots,k_n)$, $m \geq k_1 \geq \ldots \geq k_n \geq 0$. Демонстрирана е връзката между R-покриващите дизайни и Турановите R-дизайни (Теорема 4.4). Намерено е необходимо и достатъчно условие за съществуване на τ-(n,κ,l) дизайни – аналози на класическите t-(v,k,λ) дизайни. Геометричните спредове са специален случай на τ-дизайни с $\tau = (m,0,\ldots,0)$.

В раздел 4.2 се изследва въпросът за намиране на необходими и достатъчни условия за съществуване на спредове в проективни геометрии на Йелмслев. В класическия случай на спредове от r-мерни подпространства в $\mathrm{PG}(n,q)$ комбинаторното необходимо условие – броят на точките в r-мерно подпространство да дели броя на всички точки в $\mathrm{PG}(n,q)$ – се оказва и достатъчно. В случая на верижни пръстени ситуацията е по-сложна. Известно е, че в класическия случай на спредове от свободни подмодули комбинаторното необходимо условие се оказва и достатъчно. Основните резултати от този раздел се съдържат в теореми 4.10–4.12, които формулираме по-долу.

Теорема 4.10 Нека R е верижен пръстен с дължина m. Ако съществува λ-спред $\mathrm{PHG}({}_RR^n)$, където $\lambda = (\lambda_1,\ldots,\lambda_n)$, $\lambda_1 \geq \ldots \geq \lambda_n > 0$, то тогава съществува и μ-спред в геометрията $\mathrm{PHG}({}_{\widetilde{R}}\widetilde{R}^n)$, $\widetilde{R} = R/(\operatorname{rad} R)^{m-\lambda_n}$, за който

$$\mu = (\lambda_1 - \lambda_n, \lambda_2 - \lambda_n, \ldots, \lambda_{n-1} - \lambda_n, 0).$$

Нека отново R е фиксиран верижен пръстен, за който $|R| = q^m$, $R/\operatorname{rad} R \cong \mathbb{F}_q$. Нека освен това $q = p^r$ и $\operatorname{char} R = p^s$. Да запишем m във вида $m = (s-1)l + t$. Пръстенът R може да се представи като (Теорема 2.2)

$$R = S[X;\sigma]/(g(X), p^{s-1}X^t),$$

където $S = \mathrm{GR}(q^s, p^s)$ и σ е автоморфизъм на S. Ясно е, че $S/\operatorname{rad} S \cong \mathbb{F}_q$. Дефинираме разширение на Галоа $T = S[Y]/(f(Y))$ за пръстена S, където f е базово неразложим полином над S от степен h. Сега дефинираме пръстена

$$Q = T[X;\sigma]/(g(X), p^{s-1}X^t).$$

Теорема 4.11 Нека R е верижен пръстен, за който $|R| = q^m$, $R/\operatorname{rad} R \cong \mathbb{F}_q$. Нека по-нататък Q е разширението на R, дефинирано по-горе. Нека $n = hl$ и да допуснем, че съществува λ-спред в $\mathrm{PHG}({}_QQ^l)$, за който

$$\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_l), \;\; m = \lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_l \geq 0.$$

Тогава съществува μ-спред в $\mathrm{PHG}({}_RR^n)$, където

$$\mu = (\underbrace{\lambda_1, \ldots, \lambda_1}_{h}, \underbrace{\lambda_2, \ldots, \lambda_2}_{h}, \ldots, \underbrace{\lambda_l, \ldots, \lambda_l}_{h}).$$

Теорема 4.12 Нека R е произволен верижен пръстен, за който $|R| = q^m$, $R/\operatorname{rad} R \cong \mathbb{F}_q$, и нека n е естествено число. За всеки делител h на n и за всеки тип λ от вида

$$\lambda = m^h (m-1)^{a_{m-1}h} (m-2)^{a_{m-2}h} \ldots 1^{a_1 h},$$

където $a_i \geq 0$ и $1 + a_1 + \ldots + a_{m-1} = \dfrac{n}{h}$, съществува λ-спред в $\mathrm{PHG}({}_RR^n)$.

Интересен е въпросът дали съществуват спредове от подмодули от типове, които са различни от тези, описани в теореми 4.10–4.12. В раздел 4.3 са намерени типове на подмодули, за които комбинаторното необходимо условие е изпълнено, но въпреки това спредове не съществуват. Това е съдържанието на Теорема 4.13.

Научни приноси

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

(1) Намерена е стандартна форма за матрици над краен верижен пръстен R със свойството, че за всеки крайно породен модул ${}_RM$ съществува единствена матрица в стандартна форма, чийто редове пораждат ${}_RM$.
(2) За даден десен модул ${}_RM$, породен от матрица в стандартна форма, е намерена матрица в стандартна форма, чийто редове пораждат ортогоналния модул $M_R^{\perp}$.
(3) Представени са алгоритми за работа с модули: намиране на матрица в стандартна форма, пораждаща даден модул, получаване на модул, породен от дадени подмодули, алгоритъм за проверка на принадлежност към модул, генериране на ортогоналния модул, намиране на сечение на два модула, генериране на всички подмодули от фиксиран тип за даден модул.
(4) Доказани са достатъчни условия за съществуване на спредове от несвободни подмодули.
(5) Конструирани са примери на типове λ, за които комбинаторното необходимо условие за съществуване не е достатъчно.

Публикации по дисертационния труд

(1) N. Georgieva, Basic algorithms for manipulation of modules over finite chain rings, *Serdica J. Computing* **10**(2016), No. 3-4, 285–297. [24]
(2) N. Georgieva, I. Landjev, On the representation of modules over finite chain rings, *Ann. Sofia Univ. Math. and Inf.* **104**(2017), 89–98. [25]
(3) I. Landjev, N. Georgieva, Conditions for the existence of spreads in prijective Hjelmslev geometries, *Des. Codes Cryptogr.* **87**(2019), 785-794. (IF 1.524; Q2) [64]

Резултатите от този дисертационен труд са докладвани на следните научни конференции:

- Пролетна научна сесия на ФМИ;
- Computer Science and Education in Computer Science, Fulda, Germany 2016;
- Computer Science and Education in Computer Science, Boston University, 2018;
- Computer Science and Education in Computer Science, Fulda, Germany, 2019
- International Workshop on Algebraic and Combinatorial Coding Theory, Pomorie 2012;
- International Workshop on Algebraic and Combinatorial Coding Theory, Svetlogorsk 2014, Russia;
- International Workshop on Algebraic and Combinatorial Coding Theory, Albena 2016;
- International Workshop on Algebraic and Combinatorial Coding Theory, Svetlogorsk 2018.

Литература

[1] B. Artmann, Hjelmslev-Ebenen mit verfeinerten Nachbarschaftsrelationen, *Mathematische Zeitschrift* **112** (1969), 163–180.

[2] B. Artmann, Desarguessche Hjelmslev-Ebenen n-ter Stufe, *Mitt. Math. Sem. Gießen* **91**(1971), 1–19.

[3] D. Barbilian, Zur Axiomatik der projektiven ebenen Ringgeometrien I und II, *Jahresbericht der DMV* **50**(1940) 179–229 und **51**(1941) 34–76.

[4] M. Braun, T. Etzion, P. Östergard, A. Vardy, A. Wasserman, Existence of q-analogs of Steiner systems, *Forum of Math.*, Pi, **4**(2016), E7.

[5] A. Cronheim, Dual numbers, Witt vectors, and Hjelmslev planes, *Geometriae Dedicata* **7** (1978), 287–302.

[6] P. Dembowski, *Finite Geometries*, Springer Verla, Berlin-Heidelberg-New York, 1968.

[7] D.A Drake, Projective extension of uniform affine Hjelmslev planes, *Math. Zeitschrift* **105**(1968), 196–207.

[8] D.A. Drake, On n-uniform Hjelmslev planes, *Journal of Combinatorial Theory* **9** (1970), 267–288.

[9] D.A. Drake, Nonexistence results for finite Hjelmslev planes, *Abh. Math. Sem. der Univ. Hamburg* **40**(1974), 100–110.

[10] P. Erdős, C. Ko, R. Rado, Intersection theorems for systems of finite sets, *Quarterly J. Math.* **12**(1961), 313-320.

[11] T. Etzion, A new approach to examining q-Steiner systems, *Electronic J. Combin.* **25**(2)(2018), #P 2.8.

[12] T. Etzion, S. Kurz, K. Otal, F. Özbudak, Subspace packings: constructiuons and bounds, *Des. Codes Cryptogr.* **88**(9)(2020), 1781–1810.

[13] T. Etzion, N. Silberstein, Codes and designs relkated to lifted MRD-codes, *IEEE Trans. Inf. Theory* **59**(2013), 1004-1017.

[14] T. Etzion, A. Vardy, On q-analogs of Steiner systems and covering designs, *Adv. Math. Comm.* **5**(2)(2011).

[15] P. Frankl, R. M. Wilson, The Erdős-Ko-Rado theorem for vector spaces, *J. Combin. Theory* Ser. A **43**(1986), 228–236.

[16] N. Georgieva, Basic algorithms for manipulation of modules over finite chain rings, *Serdica J. Computing* **10**(2016), No. 3-4, 285–297.

[17] N. Georgieva, I. Landjev, On the representation of modules over finite chain rings, *Ann. Sofia Univ. Math. and Inf.* **104**(2017), 89–98.

[18] A.R. Hammons, Jr., P.V. Kumar, A.R. Calderbank, N.J.A. Sloane, P. Sole, The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes, *IEEE Trans. Inform. Theory* **IT-40**(1994), 301–319.

[19] J. Hjelmslev, Geometrie der Wirklichkeit, *Acta Mathematica* **40**(1916), 33-66.

[20] J. Hjelmslev, Die natürliche Geometrie, *Abh. des Math. Sem. der Univ. Hamburg* **2**(1923), 1–36.

[21] J. Hjelmslev, Einleitung in die allgemeine Kongruenzlehre I-VI, alles in *KGI Dansk. Vid. Selsk. Math. Fys. Medd.*, I. Mitt. **8**(1929); II. Mitt. **10**(129); III. Mitt. **19**(1942) no.12; IV. Mitt. **22**(1945) no.6; V. Mitt. **22**(1945) no.13; VI. Mitt. **25**(1949) no.10.

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

[23] T. Honold, I. Landjev, Linearly representable codes over chain rings, *Abh. aus dem Math. Seminar der Universität Hamburg* **69**(1999), 187–203.

[24] T. Honold, I. Landjev, *Electronic Journal of Combinatorics*, **7**(2000), No. 11.

[25] W. N. Hsieh, Intersection theorems for systems for systems for finite vector spaces, *Discrete Matrh.* **12**(1975), 1–16.

[26] W. Cary Huffman, Jon-Lark KIm, Patrick Solé, Concise Encyclopaediae of Coding Theory, Chapman and Hall/CRC, 2021.

[27] N. Johnson, V. Zha, M. Bilioti, Handbook of finite translation planes, Chapman & Hall/CRC, 2007.

[28] E. Kleinfeld, Finite Hjelmslev planes, *Illinois Journal of Mathematics* **3** (1959), 403–407.

[29] W. Klingenberg, Projektive und affine Ebenen mit Nachbarelementen, *Math. Zetschrift* **60**(1954), 384–406.

[30] W. Klingenberg, Desarguessche Ebenen mit Nachbarelementen, *Abh. Math. Sem. der Univ. Hamburg* **20**(1955), 97–111.

[31] R. Koetter, F. Kschischang, Coding for Errors and Erasures in Random Network Coding, *IEEE Trans. Inform. Theory* 54(8)(2008), 3579-3591. doi: 10.1109/TIT.2008.926449.

[32] A. Kreuzer, *Hjelmslev-Räume*, *Resultate der Mathematik* **12** (1987), 148–156.

[33] A. Kreuzer, Projektive Hjelmslev-Räume, Dissertation, Technische Universität München, 1988.

[34] A. Kreuzer, Hjelmslevsche Inzidenzgeometrie - ein Bericht, Bericht TUM-M9001, Technische Universität München, January 1990, Beiträge zur Geometrie und Algebra Nr. 17.

[35] A. Kreuzer, Fundamental theorem of projective Hjelmslev spaces, *Mitteilungen der Mathematischen Gesellschaft in Hamburg* **12** (1991), no. 3, 809–817.

[36] A. Kreuzer, A system of axioms for projective Hjelmslev spaces, *Journal of Geometry* **40**(1991), 125–147.

[37] I. Landjev, N. Georgieva, Conditions for the existence of spreads in prijective Hjelmslev geometries, *Des. Codes Cryptogr.* **87**(2019), 785-794.

[38] J. H. van Lint, R. M. Wilson, A Course in Combinatorics, Cambridge University Press, 1992, 2001.

[39] K. Mathiak, Ein Beweis der Dimensionsformel in projektiven Hjelmslevschen Räumen, *J. für die reine u. angew. Mathematik* **256**(1972), 215–220.

[40] K. Mathiak, Valuations of skew-fields and projective Hjelmslev spaces, Lecture Notes in Mathematics no.1175, 1986, Springer-Verlag.

[41] B.R. McDonald, Finite rings with identity, Marcel Dekker, New York, 1974.

[42] A.A. Nechaev, Finite principal ideal rings, *Russian Academy of Sciences. Sbornik. Mathematics* **20** (1973), 364–382.

[43] A.A. Nechaev, Kerdock code in a cyclic form, *Discr. Math. and Appl.* **1**no.4(1991), 365-384.

[44] A.A. Nechaev, Linear codes over modules and over spaces. MacWilliams'identity, Proceedings of the 1996 IEEE Int. Symp. Inf. Theory and Appl. (Victoria B.C., Canada), 1996, pp. 35–38.

[45] A.A. Nechaev, Finite rings with applications, in: handbook of Algebra vol. 5 (ed. M. Hazewinkel), Elsevier-North Holland, 2008, 217–319.

[46] A.A. Nechaev, A.S. Kuzmin, Linearly presentable codes, Proceedings of the 1996 IEEE Int. Symp. Inf. Theory and Appl. (Victoria B.C., Canada), 1996, pp. 31–34.

[47] A.A. Nechaev, A.S. Kuzmin, V.T. Markov, Linear codes over finite rings and modules, Preprint N 1995-6-1, Center of New Information Technologies, Moscow State University, 1995.

[48] F.P. Preparata, A class of optimum nonlinear double-error correcting codes, *Information and Control* **13**(1968), 378-400.

[49] C. Segre, La geometrie proiettive nei campi di numeri duali, *Atti Acad. Sci. Torino* **47**(1911), 114–133; 164–185.

[50] E. Sperner, Ein Satz über Untermengen einer endlichen Menge, *math. Z.* **27**(11)(1928), 544–548.

[51] F.D. Veldkamp, Geometry over rings, Handbook of Incidence Geometry – Buildings and Foundations (Francis Buekenhout, ed.), Elsevier Science Publishers, 1995, pp. 1033–1084.

[52] J.A. Wood, Extension theorems for linear codes over finite rings, Applied Algebra, Algebraic Algorithms and Error-Correcting Codes (AAECC) 12 (Teo Mora and Harold F. Mattson, Jr., eds.), Lecture Notes in Computer Science, no. 1255, Springer-Verlag, 1997, pp. 329–340.

[53] J.A. Wood, Duality for modules over finite rings and applications to coding theory, *American Journal of Mathematics* **121**(3) (1999), 555–575.

[54] J.A. Wood, Weight functions and the extension theorem for linear codes over finite rings, *Contemporary Mathematics*, vol. 225, American Mathematical Society, 1999.

[55] J. A. Wood, Foundation of linear codes over finite modules: the extension theorem and the MacWilliams identities, in: Codes over Rings (ed. P. Solé), World Scientific, 2009, 124–190.