Нов Български Университет

Департамент Информатика

Невяна Димитрова Георгиева

МРЕЖОВО КОДИРАНЕ И АНАЛОЗИ НА ДИЗАЙНИ

Дисертационен труд

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

Научен ръководител: проф. дмн Иван Ланджев

София, 2022 г.

Съдържание

Глава 1

Увод

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, 54, 55]

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 [79]. 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 [81]). 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 "поточно съответствие с физическата реалност" [31, 32, 33]. 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 [54, 55], Клайнфелд [53], Дрейк [15, 16, 17], Дембовски [13] 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 [77] – се представят като двоични образи на кодове над $\mathbb{Z}_4$ [71, 26]. С работите на А. А. Нечаев и Джей Ууд [70, 71, 72, 74, 75, 82, 83, 84, 85] 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 [38, 39, 40].

Случайното мрежово кодиране възниква от една работа на Р. Кьотер и Ф. Кшишанг от 2008 г. [56]. 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 [48] чрез изпозването 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 [66] (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 [80] и Ердьош-Ко-Радо [18] имат своите q-аналози [23, 47, 66]. 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 [8, 19, 20, 22]. 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 $M = {}_RR^n$ 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 [57, 58, 59, 60, 61], 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 [67, 68]. 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 ${}_RR^n$ 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) $a_{ij_i} = \theta^{m-t_i}$, $t_i \in \{0, \ldots, m\}$;

(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) $j_1 < j_2 < j_3 < \ldots$.

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 3.8. 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 $1 + a_1 + \ldots + a_{m-1} = \frac{n}{h}$, 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.

Резултатите от този дисертационен труд са публикувани в три научни статии [24, 25, 64]:

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

Глава 3 е написана по [25]. Описаните алгоритми са представени в [24]. Глава 4 е написана въз основа на [64] и на някои непубликувани резултати.

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

- Пролетна научна сесия на ФМИ, 2014;
- 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.

Считам за мое приятно задължение да изкажа най-дълбока благодарност на проф. дмн Иван Ланджев. Признателна съм му за безценните съвети и дискусии при съвместната ни работа и за техническата помощ при оформяне на този труд. Благодаря на колегите от катедра “Геометрия” на ФМИ към СУ “Св. Кл. Охридски”, които искрено са ме подкрпяли през годините и ме подкрепят в тези необичайни времена. Специално благодаря на колегите от департамент “Информатика” на Нов Български Университет , както и на колегите от групата по кодиране за подкрепата и критичното отношение към работата ми.

Глава 2

Основни дефиниции и резултати

В тази глава представяме основните понятия и факти за крайни верижни пръстени, крайно-породени модули над верижни пръстени и свързаните с тях геометрии на Йелмслев. Голяма част от изложените резултати се съдържат в класическите книги [13, 29, 62, 63, 65, 69, 81]. Най-новите резултати в тези области се съдържат в работите [45, 46, 73].

2.1 Крайни верижни пръстени

Един асоциативен пръстен с единица, $1 \neq 0$, наричаме *ляв (десен) верижен пръстен*, ако решетката от левите (десните) му идеали образува верига. Следващата теорема описва някои свойства на крайните верижни пръстени [11, 69, 70].

Теорема 2.1. Нека R е краен пръстен с радикал на Джейкъбсън $\operatorname{rad} R \neq 0$. Следните условия са еквивалентни:

(i) R е ляв верижен пръстен;

(ii) левите идеали на R образуват верига по включване;

(iii) R е локален пръстен и $\operatorname{rad} R = R\theta$, за всеки елемент $\theta \in \operatorname{rad}\mathbb{R}/\operatorname{rad}\mathbb{R}^2$;

(iv) R е десен верижен пръстен.

Ако R удовлетворява горните условия, то всеки собствен ляв (десен) идеал на R е от вида $(\operatorname{rad} R)^i = R\theta^i = \theta^i\mathbb{R}$ за някое естествено число i.

По-нататък ще използваме термина верижен пръстен за означаване на ляв и следователно и десен, верижен пръстен. Наймалкото естествено число m, за което $(\operatorname{rad} R)^m = (0)$ наричаме индекс на нилпотентност на R или още *дължина на* R. Така решетката на левите (десните) идеали на верижен пръстен R има вида:

$$R > R\theta > R\theta^2 > \cdots > R\theta^{m-1} > R\theta^m = (0).$$

Факторпръстенът $R/R\theta$ е поле. Ако $R/\operatorname{rad} R \cong \mathbb{F}_q$, то $\mathbb{F}_q$ наричаме *остатъчно поле* на R и мощността му ще бележим с $q = p^r$. За всяко $0 \leq i \leq m-1$ модулът $(\operatorname{rad} R)^i/(\operatorname{rad} R)^{i+1}$ е векторно пространство с размерност 1 над $R/\operatorname{rad} R$, откъдето следва, че $\left|(\operatorname{rad} R)^i/(\operatorname{rad} R)^{i+1}\right| = q$ и, следователно, $|R| = q^m$. Навсякъде оттук нататък с θ ще бележим произволен фиксиран пораждащ елемент на радикала на R, с m - дължината на пръстена, а с $q = p^r$ – реда на остатъчното поле. Характеристиката на верижен пръстен R очевидно е степен на p. Навсякъде по-нататък тя ще е $\operatorname{char} R = p^s$.

По-долу са представени примери за някои важни класове верижни пръстени.

1) Крайните полета могат да се разглеждат като тривиални верижни пръстени с $m = 1$. По-нататък ще изключваме крайните полета от нашите разглеждания и под верижен пръстен ще разбираме такъв с дължина $m \geq 2$.

2) Пръстените от остатъци по модул степен на просто число са верижни пръстени. Това са пръстените $\mathbb{Z}_{p^m} = \mathbb{Z}/(p^m)$, където

p е просто число. Очевидно за тях $\operatorname{rad} R = (p)$ и пораждащ θ на радикала на R може да бъде всеки елемент, който се дели на p, но не се дели на p^2. Остатъчното поле е $\mathbb{F}_p \cong \mathbb{Z}_p$.

3) Нека $\mathbb{F}_q$ е крайно поле и нека σ е автоморфизъм на $\mathbb{F}_q$. С $\mathbb{F}[X;\sigma]$ означаваме пръстена от полиноми от вида $f(X) = a_0 + a_1X + \cdots + a_kX^k$ с умножение, зададено с

$$Xa = a^\sigma X, \quad a \in \mathbb{F}_q.$$

Пръстенът $R = \mathbb{F}[X;\sigma]/(X^m)$, $m > 1$, е нетривиален верижен пръстен, за който веригата от вложени идеали е

$$R > (X) > (X^2) > \cdots > (X^{m-1}) > (X^m) = (0).$$

В случая $\sigma \neq id$ тези пръстени са некомутативни.

4) Един важен клас верижни пръстени са т.нар. *пръстени на Галоа*. Те се строят по следния начин. Нека p е просто число, а s – естествено число. Пръстен на Галоа наричаме всеки пръстен от вида

$$R = \mathbb{Z}_{p^s}[x]/(f)$$

където $f \in \mathbb{Z}_{p^s}[x]$ е със старши коефициент 1, $\deg f = r$ и f е базово неразложим. Казваме, че един полином f над R ($f \in R[x]$) е *базово неразложим*, ако ηf е неразложим над остатъчното поле K. Тук с η означаваме естествения хомоморфизъм

$$\eta : \ R \longrightarrow K = R/\operatorname{rad} R.$$

Този пръстен бележим с $\mathrm{GR}(q^s, p^s)$, където $q = p^r$. В литературата няма единно означение за пръстените на Галоа. Така например в [69] за същия пръстен се използва означението $\mathrm{GR}(p^s, r)$. От дефиницията е ясно, че $\mathrm{GR}(q^s, p^s)$ е комутативен пръстен с p^{rs} елемента и характеристика p^s. Ясно е, че при $s = 1$ имаме $\mathrm{GR}(p^r, p) \cong \mathrm{GF}(p^r)$, както и че $\mathrm{GR}(p^s, p^s) \cong \mathbb{Z}_{p^s}$.

Следващата теорема от [70] описва най-общата структура на краен верижен пръстен. От нея става ясно, че всеки верижен пръстен е факторпръстен на пръстен от полиноми над някакъв пръстен на Галоа.

Теорема 2.2. Нека R е краен верижен пръстен с индекс на нилпотентност m, характеристика p^s и остатъчно поле от ред $q = p^r$. Нека $S = GR(q^s, p^s)$. Съществуват единствени цели числа k, t, удовлетворяващи $m = (s-1)k + t,\ 1 \leq t \leq k\ (k = m = t,\ s = 1)$, както и автоморфизъм $\sigma \in \operatorname{Aut} S$ и полином на Айзенщайн $g(X) \in S[X;\sigma]$ от степен k (не непременно единствен), за който

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

Тук полином на Айзенщайн наричаме всеки полином $g(X)$ от пръстена $S[X;\sigma]$, имащ вида $g(X) = X^k + p(g_{k-1}X^{k-1} + \cdots + g_0)$, където $g_0 \in S \backslash pS = S^*$.

Най-простите нетривиални верижни пръстени R са тези от ред q^2 с $R/\operatorname{rad} R \cong \mathbb{F}_q$. Те са класифицирани от Кронхайм [12]. Ако $q = p^r$, съществуват точно $r+1$ такива пръстени с точност до изоморфизъм.

(1) Пръстени на σ-дуалните числа $R_\sigma = \mathbb{F}_q[X;\sigma]/(X^2)$, където $\mathbb{F}_q$ е поле с $q = p^r$ елемента, $\sigma \in \operatorname{Aut} \mathbb{F}_q$, а $\mathbb{F}_q[X;\sigma]$ е пръстенът от полиномите на Оре, в който умножението е зададено с $Xa = a^\sigma X$. Броят на тези пръстени е равен на r – броя на автоморфизмите на остатъчното поле. За всеки автоморфизъм $\sigma \in \operatorname{Aut}(\mathbb{F}_q)$ тези пръстени се представят като $R_\sigma = \mathbb{F}_q \oplus \mathbb{F}_q X$. Събирането и уможението се задават чрез:

$$(a_0 + a_1X) + (b_0 + b_1X) = (a_0 + b_0) + (a_1 + b_1)X;$$
$$(a_0 + a_1X)(b_0 + b_1X) = a_0b_0 + (a_0b_1 + a_1\sigma(b_0))X.$$

Всички тези пръстени са некомутативни с изключение на този, получен при $\sigma = id$. Характеристиката на всички пръстени в този клас е p.

(2) Един (с точност до изоморфизъм) пръстен на Галоа

$$GR(q^2, p^2) = (\mathbb{Z}/p^2\mathbb{Z})[X]/(f(X)),$$

където полиномът $f(X) \in (\mathbb{Z}/p^2\mathbb{Z})[X]$ е от степен r, със старши коефициент 1 и е неразложим по модул p. Този пръстен е комутативен с характеристика p^2.

Пример 2.3. Съществуват три неизоморфни пръстена с 16 елемента и остатъчно поле от ред 4. Това са:

(1) $\mathbb{F}_4[X]/(X^2)$;

(2) $\mathbb{F}_4[X;\sigma]/(X^2)$;

(3) $\mathbb{Z}_4[X]/(X^2 - X - 1)$;

Разбира се, съществуват и други верижни пръстени с 16 елемента, но при тях остатъчното поле е $\mathbb{F}_2$. Такива например са $\mathbb{Z}_{16}$, $\mathbb{F}_2[X]/(X^4)$. $\square$

Нека $\Gamma = \{\gamma_0 = 0, \gamma_1 = 1, \gamma_2, \dots \gamma_{q-1}\}$ е множество от елементи на R, никои два от които не са сравними по модул $\operatorname{rad} R$, т.е. $\gamma_i \not\equiv \gamma_j \pmod{\operatorname{rad} R}$ за всички i, j, $0 \le i < j \le q-1$. Лесно се показва, че всеки елемент $r \in R$ се представя по единствен начин като:

$$r = r_0 + r_1\theta + \cdots + r_{m-1}\theta^{m-1},$$

където $r_i \in \Gamma$, а θ е фиксиран пораждащ на R. Да фиксираме линейна наредба на елементите на Γ:

$$\gamma_0 \prec \gamma_1 \prec \cdots \prec \gamma_{m-1}.$$

Продължаваме тази наредба и върху елементите на R по следния начин: за елементи $a = a_0 + \cdots + a_{m-1}\theta^{m-1}$ и $b = b_0 + \cdots + b_{m-1}\theta^{m-1}$, $a_i, b_i \in \Gamma$ ще казваме, че a предхожда b, което записваме като $a \prec b$, тогава и само тогава, когато

$$a_{m-1} = b_{m-1}, \dots, a_{j+1} = b_{j+1}, a_j \prec b_j$$

за някое $0 \le j \le m-1$.

Множеството Γ получава структурата на поле, ако въведем следните операции:

$$\gamma_i + \gamma_j = \gamma_k, \text{ ако } (\gamma_i + \operatorname{rad} R) + (\gamma_j + \operatorname{rad} R) = \gamma_k + \operatorname{rad} R;$$

$$\gamma_i \cdot \gamma_j = \gamma_k, \text{ ако } (\gamma_i + \operatorname{rad} R) \cdot (\gamma_j + \operatorname{rad} R) = \gamma_k + \operatorname{rad} R.$$

Да дефинираме биекция $\varphi : R \to \{0, 1, \cdots, q^m - 1\}$, която запазва линейната наредба на елементите на R, въведена по-горе. Нека $\varphi(\gamma_i) = i$. Освен това за елемента $a = a_0 + \cdots + a_{m-1}\theta^{m-1}$, $a_i \in \Gamma$ нека $\varphi(a) = \sum_{i=0}^{m-1} \varphi(a_i)q^i$. В следващата лема се описват някои свойства на φ, които се получават непосредствено от дефиницията.

Лема 2.4. *(1)* $a \in \Gamma$ тогава и само тогава, когато $\varphi(a) < q$;

(2) за всяко $i \in \mathbb{N}$, $a \in (\operatorname{rad} R)^i$, т.е. $a = b\theta^i$, $b \in R^*$ тогава и само тогава, когато q^i дели $\varphi(a)$;

(3) ако q^i дели $\varphi(b)$, то $b = a\theta^i$ като $a = \varphi^{-1}\left(\dfrac{\varphi(b)}{q^i}\right)$.

Доказателство. (1) Очевидно.

(2) Ако $a \in (\mathrm{Rad}\ \ R)^i$, то $a - b\theta^i$, $b \in R^*$, т.е.

$$b = \beta_0 + \beta_1\theta + \ldots + \beta_{m-1}\theta^{m-1},\ \beta_i \in \Gamma, \beta_0 \neq 0.$$

Тогава очевидно $a = \beta_0\theta^i + \beta_1\theta^{i+1} + \ldots + \beta_{m-i-1}\theta^{m-1}$ и

$$\varphi(a) = \varphi(\beta_0)q^i + \varphi(\beta_1)q^{i+1} + \ldots + \varphi(\beta_{m-i-1})q^{m-1}.$$

Обратно, ако q^i дели $\varphi(a)$, то $\varphi(a) = a_0q^i + a_1q^{i+1} + \ldots$, $a_j \in \{0, \ldots, q-1\}$, и $a = \varphi^{-1}(a_0)\theta^i + \varphi^{-1}(a_1)\theta^{i+1} + \ldots$. Сега е ясно, че $a \in (\operatorname{rad} R)^i$.

(3) Първата част на твърдението повтаря едната посока на (2). Ако q^i дели $\varphi(b)$, то

$$\begin{aligned} b &= b_0\theta^i + b_1\theta^{i+1} + \ldots + b_{m-i+1}\theta^{m-1},\ \ b_i \in \Gamma, \\ \varphi(b) &= \varphi(b_0)q^i + \varphi(b_1)q^{i+1} + \ldots + \varphi(b_{m-i+1})q^{m-1}, \\ &\qquad\qquad\qquad\qquad\qquad\qquad \varphi(b_i) \in \{0, \ldots, q-1\}. \end{aligned}$$

Оттук

$$\frac{\varphi b}{q^i} = \varphi(b_0) + \varphi(b_1)q + \ldots + \varphi(b_{m-i+1})q^{m-i+1}$$

и

$$a = \varphi^{-1}\left(\frac{\varphi(b)}{q^i}\right) = b_0 + b_1\theta + \ldots + b_{m-i+1}\theta^{m-i+1}.$$

Сега лесно се проверява, че $b = a\theta^i$. $\square$

Ще демонстрираме въведените понятия с един пример.

Пример 2.5. Следният пример илюстрира Лема 2.4 върху пръстена $\mathrm{GR}(16,4)$. Пръстена $\mathrm{GR}(4^2,2^2)$ представяме във вида $R=\mathrm{GR}(4^2,2^2)\cong \mathbb{Z}_4[X]/(X^2-X-1)$. Елементите на R са

$$\begin{array}{rrrr} 0 & 1 & 2 & 3 \\ X & X+1 & X+2 & X+3 \\ 2X & 2X+1 & 2X+2 & 2X+3 \\ 3X & 3X+1 & 3X+2 & 3X+3 \end{array}$$

$\operatorname{rad} R=\{0,2,2X,2X+2\},\ \theta=2;$
$\Gamma = 0\prec 1\prec X\prec X+1$

$$\begin{array}{rcrcrr} r & & & & & \varphi(r) \\ 0 & = & 0 & \longrightarrow & (0,0) & 0 \\ 1 & = & 1 & \longrightarrow & (1,0) & 1 \\ 2 & = & 0.1+1.2 & \longrightarrow & (0,1) & 4 \\ 3 & = & 1.1+1.2 & \longrightarrow & (1,1) & 5 \\ X & = & X & \longrightarrow & (X,0) & 2 \\ X+1 & = & X+1 & \longrightarrow & (X+1,0) & 3 \\ X+2 & = & X.1+1.2 & \longrightarrow & (X,1) & 6 \\ X+3 & = & (X+1).1+1.2 & \longrightarrow & (X+1,1) & 7 \\ 2X & = & 0.1+X.2 & \longrightarrow & (0,X) & 8 \\ 2X+1 & = & 1.1+X.2 & \longrightarrow & (1,X) & 9 \\ 2X+2 & = & 0.1+(X+1).2 & \longrightarrow & (0,X+1) & 12 \\ 2X+3 & = & 1.1+(X+1).2 & \longrightarrow & (1,X+1) & 13 \\ 3X & = & X.1+X.2 & \longrightarrow & (X,X) & 10 \\ 3X+1 & = & (X+1).1+X.2 & \longrightarrow & (X+1,X) & 11 \\ 3X+2 & = & X.1+(X+1).2 & \longrightarrow & (X,X+1) & 14 \\ 3X+3 & = & (X+1).1+(X+1).2 & \longrightarrow & (X+1,X+1) & 15 \end{array}$$

Наредбата в $\mathrm{GR}(4^2,2^2)$ е следната:

$$\begin{aligned} &(0,0)\prec(1,0)\prec(X,0)\prec(X+1,0)\prec(0,1)\prec(1,1)\prec(X,1)\prec \\ &\quad(X+1,1)\prec(0,X)\prec(1,X)\prec(X,X)\prec(X+1,X)\prec \\ &\qquad(0,X+1)\prec(1,X+1)\prec(X,X+1)\prec(X+1,X+1) \end{aligned}$$

$$0 \prec 1 \prec X \prec X+1 \prec 2 \prec 3 \prec X+2 \prec X+3 \prec 2X \prec$$
$$2X+1 \prec 3X \prec 3X+1 \prec 2X+2 \prec 2X+3 \prec 3X+2 \prec 3X+3$$

2.2 Модули над крайни верижни пръстени

Нека са дадени пръстен R и адитивна абелева група M. Ще казваме, че M е *ляв R-модул*, ако за всеки два елемента $r \in R$ и $m \in M$ е определен еднозначно елемент $rm \in M$, изпълняващ условията:

(1) $r(m+n) = rm + rn$;

(2) $(rs)(m) = r(sm)$;

(3) $(r+s)(m) = rm + sm$;

(4) $1m = m$

където $r, s \in R$ и $m, n \in M$.

Дефиниция 2.6. Нека ${}_RM$ е ляв R-модул. Елементите $x_1, \ldots, x_r$ от модула M наричаме *независими* или *свободни*, ако от $a_1x_1 + \cdots + a_rx_r = 0$ следва, че $a_jx_j = 0$ за всяко $j = 1, \ldots, r$. Редицата $x_1, \ldots, x_r$ от елементи на модула M наричаме *линейно независима*, ако от $a_1x_1 + \cdots + a_rx_r = 0$ следва, че $a_j = 0$ за всяко $j = 1, \ldots, r$. *Базис* на M наричаме всяка независима редица от пораждащи елементи.

Модула ${}_RM$ наричаме *свободен*, ако той е изоморфен на директна сума на копия на ${}_RR$. Нека ${}_RM$ е краен ляв модул и нека θ е пораждащият елемнт на $\operatorname{rad} R$. Ще казщаме, че елементът $x \in {}_RM$ има период θ^i, ако $i \in \{0, 1, \ldots, m\}$ е най-малкото неотрицателно цяло число, удовлетворяващо условието $\theta^i x = 0$. Казваме, че x има височина i, ако $i \in \{0, 1, \ldots, m\}$ е най-голямото цяло число, за което $x = \theta^i y$ за някое $y \in M$.

Нека ${}_RM$ е лях R модул. Дефинираме следните множества:

$$M^* = \{x \in M;\ x \text{ има период } \theta^m\} = \{x \in M; Rx \cong \mathbb{R}\}; \tag{2.1}$$

$$\theta^i M = \{\theta^i x; x \in M\}; \tag{2.2}$$

$$M[\theta^i] = \{x \in M; \theta^i x = 0\} \tag{2.3}$$

Нека $\mathbb{R}$ е краен верижен пръстен. Горен ред на Льови за левия $\mathbb{R}$-модул M наричаме веригата от подмодули:

$$M = \theta^0 M \supseteq \theta^1 M \supseteq \cdots \supseteq \theta^{m-1} M \supseteq \theta^m M = 0. \tag{2.4}$$

Тук, очевидно, $\theta^i M = (\operatorname{rad} R)^i M \leq {}_RM$. Всеки фактормодул в горния ред $\theta^{i-1}M/\theta^i M, i \geq 1$ е векторно пространство над полето $R/\operatorname{rad} R \cong \mathbb{F}_q$. Аналогично долен ред на Льови на ${}_RM$ наричаме веригата от подмодули

$$M = M[\theta^m] \supseteq \cdots \supseteq M[\theta^2] \supseteq M[\theta] \supseteq M[1] = 0. \tag{2.5}$$

Тук $M[\theta^i] = \{x \in M; \theta^i x = 0\}$. Фактормодулите $M[\theta^i]/M[\theta^{i-1}]$ също са векторни пространства над полето $R/\operatorname{rad} R \cong \mathbb{F}_q$.

За всяко $i \in \mathbb{N}$ полагаме $\mu_i = \dim_{R/\operatorname{rad} R}(\theta^{i-1}M/\theta^i M)$. Умножението с θ индуцира R-изоморфизъм

$$\theta^{i-1}M/(M[\theta] + \theta^i M) \cong \theta^i M/\theta^{i+1}M. \tag{2.6}$$

Оттук получаваме, че $\log_q |M| = \mu_1 + \mu_2 + \cdots + \mu_m,\ \mu_i \geq \mu_{i+1}$, т.е. $\mu = (\mu_1, \mu_2, \dots)$ е разбиване на $\log_q |M|$ (на най-много m части), което ще означаваме с $\mu \vdash \log_q |M|$. По-нататък ще пишем $\mu = (\mu_1, \mu_2, \dots, \mu_r)$ тогава и само тогава, когато $\mu_r \geq 1$ и $\mu_i = 0,\ i > r$ и понякога $\mu = 1^{s_1}2^{s_2}3^{s_3}\cdots$, ако точно s_j части на μ са равни на j.

Следващата теорема характеризира структурата на крайните R-модули.

Теорема 2.7. Нека R е краен верижен пръстен. За всеки краен модул ${}_RM$ съществува еднозначно определено разбиване $\lambda = (\lambda_1, \dots, \lambda_k) \vdash \log_q |M|$ на такива части $1 \le \lambda_i \le m$, за които

$$ {}_RM \cong R/(\operatorname{rad} R)^{\lambda_1} \oplus \cdots \oplus R/(\operatorname{rad} R)^{\lambda_k}. $$

Частите на спрегнатото разбиване $\lambda' = (\lambda'_1, \lambda'_2, \dots) \vdash \log_q |M|$ са инвариантите на Улм-Капландски $\lambda'_i = \dim_{R/\operatorname{rad} R}(M[\theta] \cap \theta^{i-1}M)$.

Разбиването $\lambda = (\lambda_1, \dots, \lambda_k) \vdash \log_q |M|$ наричаме *тип* на крайния R-модул M, а разбиването λ', което е спрегнато на λ – *спрегнат тип* на M. Цялото число

$$ k = \lambda'_1 = \dim_{R/\operatorname{rad} R}(M/\theta M) = \dim_{R/\operatorname{rad} R} M[\theta], $$

задаващо броя на ненулевите събираеми в разлагането на ${}_RM$ в директна сума на циклични модули, наричаме *ранг* на M и означаваме с $\operatorname{rk} M$. Цялото число λ'_m, което е равно на броя на свободните събираеми в същото разлагане на ${}_RM$, наричаме *свободен ранг* на ${}_RM$.

Нека ${}_RM$ е ляв модул над верижния пръстен R. Ако S е множество от елементи на M, със $\operatorname{Ann}(S)$ бележим анихилатора на S, т.е. $\operatorname{Ann}(S) = \{r \in R | rm = 0, \forall\ m \in S\}$. Един елемент $m \in M$ наричаме *неторзионен*, ако $\operatorname{Ann}(m) \neq 0$. Множеството от всички неторзионни елементи на M означаваме с M^*. С други думи, $M^* = \{x \in M;\ x \text{ има период } \theta^m\}$.

Известно е, че броят на k мерните подпространства на n мерно векторно пространство над крайното поле $\mathbb{F}_q$ е равен на

$$ \begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{(q^n-1)(q^{n-1}-1)\dots(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1)\dots(q-1)}. \tag{2.7} $$

Числата, дефинирани с тази формула, наричаме *гаусови коефициенти*. Съществува подобна формула, задаваща броя на подмодулите от фиксиран тип, съдържащи се в даден модул над краен верижен пръстен. Нека ${}_RM$ е модул от тип λ. Модулът ${}_RM$ съдържа подмодул от тип μ тогава и само тогава, когато $\mu \le \lambda$, т.е. $\mu_i \le \lambda_i$ за всяко i. Тогава очевидно е изпълнено и $\mu' \le \lambda'$. В сила е следната теорема [40].

Теорема 2.8. Нека R е краен верижен пръстен с остатъчно поле от ред q. Нека ${}_RM$ е краен R-модул от тип λ. За всякà рàäèöà μ, удовлетворяващо условието $\mu \leq \lambda$ модулът ${}_RM$ съдържа точно

$$\begin{bmatrix}\lambda\\ \mu\end{bmatrix}_{q^m} := \prod_{i=1}^{\infty} q^{\mu'_{i+1}(\lambda'_i-\mu'_i)} \begin{bmatrix}\lambda'_i-\mu'_{i+1}\\ \mu'_i-\mu'_{i+1}\end{bmatrix}_q . \tag{2.8}$$

подмодула от тип μ. В частност, броят на свободните подмодули от ранг s на краен модул ${}_RM$ от тип λ е

$$q^{s(\lambda'_1-s)+\cdots+s(\lambda'_{m-1}-s)} \cdot \begin{bmatrix}\lambda'_m\\ s\end{bmatrix}_q . \tag{2.9}$$

Доказателство. Нека $U \leq {}_RM$ е подмодул от тип μ. Нека $M_j = M[\theta] \cap \theta^{j-1}M, 1 \leq j \leq m$ и по подобен начин $U_j = U[\theta] \cap \theta^{j-1}U$. Тогава $U_j \geq U_{j+1}$, U_j е подпространство на $R/\operatorname{rad} R$ - пространството M_j и $\dim_{R/\operatorname{rad} R} M_j = \lambda'_j$, $\dim_{R/\operatorname{rad} R} U_j = \mu'_j$. Обратно, съществуват точно

$$\prod_{j=1}^{m} \left[\begin{array}{c}\lambda'_j-\mu'_{j+1}\\ \mu'_j-\mu'_{j+1}\end{array}\right]_q \tag{2.10}$$

вериги $U_1 \geq \cdots \geq U_m$ от подпространства $U_j \leq M[\theta]$, удовлетворяващи допълнителното условие $U_j \leq M_j$. При зададена такава верига ще пресметнем броя на подмодулите U на M, за които $U[\theta] \cap \theta^{j-1}U = U_j$, $1 \leq j \leq m$. Нека $y_1, \ldots, y_{\mu'_1}$ е такава редица от елементи на $M[\theta]$, че за всяко $j \in \{1, \ldots, m\}$ подредицата $y_1, \ldots, y_{\mu'_1}$ е базис на $R/\operatorname{rad} R$-пространството U_j. Всеки разглеждан подмодул U има базис $x_1, \ldots, x_{\mu'_1}$, изпълняващ условието $y_s = \theta^{\mu_s-1}x_s$ за $1 \leq s \leq \mu'_1$. Броят на тези редици $x_1, \ldots, x_{\mu'_1}$ е

$$\prod_{1\leq s\leq \mu'_1} \left|M[\theta^{\mu_s-1}]\right| = \prod_{1\leq s\leq \mu'_1} q^{\sum_{1\leq s\leq \mu'_s} \lambda'_j} = \prod_{j\geq 1} q^{\lambda'_j\cdot|\{s|\mu_s>j\}|} = q^{\sum_{j\geq 1}\lambda'_j\mu'_{j+1}}.$$

Две редици $x_1, \ldots, x_{\mu'_1}$ и $x'_1, \ldots, x'_{\mu'_1}$ пораждат един и същ подмодул U тогава и само тогава, когато $x'_s = x_s u_s$, за някое $u_s \in M[\theta^{\mu_s-1}] \cap U = U[\theta^{\mu_s-1}]$ $(1 \leq s \leq \mu'_1)$. Оттук броят на подмодулите,

принадлежащи на веригата $U_1 \geq \cdots \geq U_m$, е

$$\frac{\prod\limits_{1\leq s\leq \mu_1'} \left|M[\theta^{\mu_s-1}]\right|}{\prod\limits_{1\leq s\leq \mu_1'} \left|U[\theta^{\mu_s-1}]\right|} = q^{\sum_{j\geq 1}(\lambda_j'-\mu_j')\mu_{j+1}'},$$

което искахме да покажем. □

Следствие 2.9. Нека $\boldsymbol{m} = (\underbrace{m,\ldots,m}_{n})$ и нека $\mu = (\mu_1,\ldots,\mu_n)$, където $m \geq \mu_1 \geq \cdots \geq \mu_n \geq 0$. Тогава

$$\begin{bmatrix}\boldsymbol{m}\\ \mu\end{bmatrix}_q = \begin{bmatrix}\boldsymbol{m}\\ \overline{\mu}\end{bmatrix}_q,$$

където $\overline{\mu} = (m-\mu_n,\ldots,m-\mu_1)$.

Формулата от Следствие 2.9 може да се разглежда като аналог на класическото биномно равенство за гаусови коефициенти

$$\begin{bmatrix}n\\ k\end{bmatrix}_q = \begin{bmatrix}n\\ n-k\end{bmatrix}_q.$$

Нека R е краен верижен пръстен. Разглеждаме левия R-модул ${}_RM$. За два вектора $\boldsymbol{x} = (x_1,\ldots,x_n)$ и $\boldsymbol{y} = (y_1,\ldots,y_n)$ дефинираме тяхното скаларно произведение по следния начин

$$\mathbf{xy} = x_1y_1 + \cdots + x_ny_n.$$

Дефинираме десен ортогонален модул на модула ${}_RM$ като

$$M_R^{\perp} = \{\mathbf{y} \in R^n |\ \mathbf{xy} = 0, \ \text{ за всяко } \ \mathbf{x} \in {}_RM\}.$$

Ще отбележим, че ортогоналният модул на ляв (респ, десен) модул е десен (респ. ляв) модул. Следната добре известна теорема представя някои от по-важните свойства на ортогоналния модул на даден модул.

Теорема 2.10. Нека R е верижен пръстен с $|R| = q^m$, $R/\operatorname{rad} R \cong \mathbb{F}_q$ и нека ${}_RM \leq {}_RR^n$ е ляв подмодул от тип $\lambda = (\lambda_1, \ldots, \lambda_n)$.

(1) Десният модул $M_R^\perp$ е от тип $\overline{\lambda} = (m - \lambda_n, \ldots, m - \lambda_1)$. В частност, $|M||M^\perp| = |R^n|$;

(2) ${}^\perp(M^\perp) = M$;

(3) Изображението $M \to M^\perp$ задава антиизоморфизъм между решетките на левите (съотв. десните) подмодули на R^n и, следователно,

$$(M_1 \cap M_2)^\perp = M_1^\perp + M_2^\perp;\ (M_1 + M_2)^\perp = M_1^\perp \cap M_2^\perp.$$

2.3 Проективни пространства на Йелмслев

Нека $\mathcal{P}$ и $\mathcal{L}$ са две непразни множества, които ще наричаме съответно множество от точки и множество от прави. Освен това е дадена и инцидентност $I \subseteq \mathcal{P} \times \mathcal{L}$. Тройката $(\mathcal{P}, \mathcal{L}, I)$ наричаме структура на инцидентност. Нека върху всяко от множествата $\mathcal{P}$ и $\mathcal{L}$ е дефинирана релация *съседство* $\bigcirc$ чрез следните условия:

(N1) $\forall\, X, Y \in \mathcal{P} : X \bigcirc Y \Longleftrightarrow \exists s, t \in \mathcal{L},\ s \neq t :\ X\ Is,\ X\ It, Y\ Is,\ Y\ It$;

(N2) $\forall\ s, t \in \mathcal{L} : s \bigcirc t \Longleftrightarrow$ за всяка точка $X : X\ Is$ съществува точка $Y :\ Y\ It$ такава, че $X \bigcirc Y$ и обратно, за всяка точка $Y :\ Y\ It$ съществува точка $X :\ X\ Is$ такава, че $Y \bigcirc X$.

Нека $(\mathcal{P}, \mathcal{L}, I)$ е структура на инцидентност, в която е зададена релация на съседство, удовлетворяваща (N1) и (N2). За всеки две точки X, Y, за които $X \not\bigcirc Y$ означаваме с XY единствената права, инцидентна с X и Y, ако такава права съществува. Понататък ще разглеждаме структури, в които всеки две точки са инцидентни с поне една права. Нека разгледаме точка X и права s. Ще пишем $X \bigcirc s$ и ще казваме, че X *е съседна на правата* s, ако съществува точка Y върху s, $Y \neq X$, за която $X \bigcirc Y$.

Проективно пространство на Йелмслев ще наричаме всяка структура на инцидентност $\Pi = (\mathcal{P}, \mathcal{L}, I)$ с релация на инцидентност $\bigcirc$, удовлетворяваща аксиомите:

(H1) За всеки две точки $X, Y \in \mathcal{P}$ съществува права s, за която $X\ Is$, $Y\ Is$.

(H2) Всяка права $s \in \mathcal{L}$ е инцидентна с поне три точки, които са две по две несъседни.

(H3) Две прави s и t, за които $s \cap t \neq \emptyset$ са съседни тогава и само тогава, когато $|s \cap t| \geq 2$.

(H4) За всеки три точки $X, Y, Z \in \mathcal{P}$, за които $X \bigcirc Y$ и $Y \bigcirc Z$, е изпълнено $X \bigcirc Z$.

(H5) За всеки две прави $s, t \in \mathcal{L}$ и всеки три точки X, Y, Z, за които XIs, YIs, XIt, ZIt, $X \not\bigcirc Y$, $X \not\bigcirc Z$, $Y \bigcirc Z$ е изпълнено $s \bigcirc t$.

(H6) За всяка точка X, която не е инцидентна, но е съседна на правата $s \in \mathcal{L}$, съществуват $Y, Z \in \mathcal{P}$, за които $Y \not\bigcirc s$, $Z\ Is$ и $X\ I\ \overline{Y, Z}$.

(H7) Нека $X \in \mathcal{P}$, $s \in \mathcal{L}$ като $X \not\bigcirc s$ и нека $Y, Z \in s$. За всеки две точки $Y'\ I\ \overline{X, Y}$ и $Z'\ I\ \overline{X, Z}$ съществува права t, за която $Y'\ It$, $Z'\ It$ и $s \cap t \neq \emptyset$.

Един важен клас от проективни пространства на Йелмслев се получава от крайно породени модули над крайни верижни пръстени. Да разгледаме верижен пръстен R, за който $|R| = q^m$, $R/\operatorname{rad} R \cong \mathbb{F}_q$, $q = p^r$. Нека $M = {}_R R^n$ и $M^* = M \backslash \theta M$, където θ е фиксиран елемент пораждащ на $\operatorname{rad} R$. Нека множеството $\mathcal{P} = \{Rx \mid x \in M^*\}$ е множеството на всички свободни подмодули на M от ранг 1, и нека $\mathcal{L} = \{Rx + Ry \mid x, y \text{ линейно независими}\}$ е множеството на всички свободни подмодули на M от ранг 2.

Инцидентността I се задава с теоретико-множествено включване. Така получената структура на инцидентност $(\mathcal{P}, \mathcal{L}, I)$, заедно с релацията на съседство $\bigcirc$, зададена чрез (N1) и (N2), удовлетворява аксиомите (H1)–(H7) е проективно пространство на Йелмслев, което ще означаваме с $\mathrm{PHG}({}_R R^n)$. Пространството $PHG({}_R R^n)$ наричаме още *лява геометрия на Йелмслев над верижния пръстен* R. Ако R е комутативен, то лявата и дясната геометрии над R съвпадат и ще използваме означението $\mathrm{PHG}(n-1, R)$.

Едно множество от точки $\mathcal{T}$ в $\mathrm{PHG}\,({}_R R^n)$ наричаме *подпространство на Йелмслев*, ако за всеки две точки $X, Y \in \mathcal{T}$ съществува поне една права, инцидентна с X и Y, която се съдържа изцяло в $\mathcal{T}$. Еквивалентно, множеството от точки (свободни подмодули от ранг 1) $\mathcal{T}$ е подпространство на Йелмслев, ако съвпада с множеството на всички свободни подмодули от ранг 1, съдържащи се в някакъв свободен подмодул на ${}_R R^n$ от ранг 2. Всяко подпространство на Йелмслев е проективно пространство на Йелмслев. Казваме, че едно множество от точки $\mathcal{S}$ е *подпространство* в $\mathrm{PHG}({}_R R^n)$, ако то е сечение на подпространства на Йелмслев. Ясно е, че едно подпространство не е непременно подпространство на Йелмслев, тъй като сечението на свободни подмодули на ${}_R R^n$ не е непременно свободен подмодул. Все пак сечението на свободни подмодули е подмодул на ${}_R R^n$. Типът на този подмодул наричаме *тип на подпространството* $\mathcal{S}$.

За всяко множество от точки $\mathcal{X} \subseteq \mathcal{P}$ дефинираме *обвивка* на $\mathcal{X}$ кото сечението на всички подпространства на Йелмслев, които съдържат $\mathcal{X}$:

$$\langle \mathcal{X} \rangle = \cap_{\mathcal{X} \subset \mathcal{T}} \mathcal{T}.$$

Множеството $\mathcal{X} \subset \mathcal{P}$ ще наричаме *независимо*, ако за всяка точка $X \in \mathcal{X}$ е изпълнено $X \not\subset \langle \mathcal{X} \backslash \{X\} \rangle$. Множеството от точки $\mathcal{B}$ ще наричаме *базис* на Π, ако $\langle \mathcal{B} \rangle = \mathcal{P}$ и $\mathcal{B}$ е независимо множество от точки. *Размерност* на проективното пространство на Йелмслев Π дефинираме като $\dim \Pi := |\mathcal{B}| - 1$.

Релацията $\bigcirc$ е релация на еквивалентност както върху $\mathcal{P}$, така и върху $\mathcal{L}$. Множеството на всички точки, които са съседни на точката X ще бележим с $[X]$. Аналогично, множеството на всички прави, съседни на правата s ще означаваме със $[s]$. Класовете $[X]$ и $[s]$ наричаме класове на съседство, съответно, на точката X и на правата s. Множеството на всички класове на съседство в $\mathcal{P}$ (съотевтно в $\mathcal{L}$) означаваме с $\mathcal{P}^{(1)}$ (съответно $\mathcal{L}^{(1)}$).

За координатни геометрии на Йелмслев над верижни пръстени с височина $m > 2$ можем да въведем по-фини релации на съседство. Да разгледаме $\mathrm{PHG}({}_R R^n)$, където R е верижен пръстен с $|R| = q^m$, $R/\operatorname{rad} R \cong \mathbb{F}_q$. Ще казваме че точките $X = R\boldsymbol{x}$ и $Y = R\boldsymbol{y}$ са *i-съседни* или *i-ти съседи*, $i \in \{0, \ldots, m\}$, ако $|X \cap Y| \geq q^i$. Това ще записваме като $X \bigcirc_i Y$. Еквивалентно, точките X и Y са i-съседни, ако модулът $Rx+Ry$ е от тип $(m, m-i)$, $i \in \{0, 1, \ldots, m\}$. Точката X е i-съседна на подпространството S, ако съществува точка Y от S, за която $X \bigcirc_i Y$. Две прави $s, t \in \mathcal{L}$ са *i-съседни*, ако за всяка точка XIs съществува точка YIt, за която $X \bigcirc_i Y$ и за всяка точка YIt съществува точка XIs, за която $Y \bigcirc_i X$. Фактът, че правите s и t са i-ти съседи означаваме със $s \bigcirc_i t$. По-общо едно подпространство S е i-съседно на подпространство T, ако всяка точка от S има i-съсед в T. Това означаваме отново с $S \bigcirc_i T$. Така въведената релация $\bigcirc_i$ е релация на еквивалентност, ако бъде разгледана върху множеството от подпространства от един и същи тип. Да отбележим, че всеки две точки (прави) са 0-съседи и всяка точка (права) е m-съсед единствено на себе си.

Да означим с $\pi^{(i)}$, $i \in \{0, \ldots, m\}$ естествения хомоморфизъм $\pi^{(i)} : R^n \longrightarrow R^n/\theta^i R^n$. За всяка точка $X \in \mathcal{P}$ и всяка права $s \in \mathcal{L}$ дефинираме i-тия клас на съседство за X по следния начин:

$$\begin{aligned} [X]_i &= \{Y \in \mathcal{P} \mid \pi^{(i)}(X) = \pi^{(i)}(Y)\}; \\ [s]_i &= \{t \in \mathcal{L} \mid \pi^{(i)}(s) = \pi^{(i)}(t)\}. \end{aligned}$$

С $\mathcal{P}^{(i)}$ и $\mathcal{L}^{(i)}$ означаваме, съответно, множеството от всички i-ти класове на съседство от точки и прави в $(\mathcal{P}, \mathcal{L}, I)$. Две точки (прави) са i-съседни тогава и само тогава, когато техните

образи под действието на $\pi^{(i)}$ съвпадат. Следователно, класът $[X]_i$ (съответно, $[s]_i$) е класът на еквивалентност на X (съответно, на s) относно релацията на еквивалентност $\bigcirc_i$. Класът $[R\boldsymbol{x}]_i$ съвпада с множеството на всички свободни подмодули от ранг 1 на $R\boldsymbol{x}+\theta^i R^n$. Аналогично, класът на съседство $[R\boldsymbol{x}+R\boldsymbol{y}]_i$ съвпада с множеството на всички свободни подмодули от ранг 2 на $R\boldsymbol{x}+R\boldsymbol{y}+\theta^i R^n$.

Теорема 2.11. Нека $(\mathcal{P},\mathcal{L},I)=\mathrm{PHG}({}_R R^n)$, където R е верижен пръстен. Тогава структурата на инцидентност $(\mathcal{P}^{(i)},\mathcal{L}^{(i)},I')$, където I' се дефинира чрез

$$[X]_i I'[s]_i \Longleftrightarrow \exists s' \in [s]_i : X' I s',$$

е изоморфна на $\mathrm{PHG}({}_{\widetilde{R}}\widetilde{R}^n)$, където $\widetilde{R}=R/(\operatorname{rad} R)^i$. В частност, $(\mathcal{P}^{(1)},\mathcal{L}^{(1)},I')$ е изоморфна на проективната геометрия $\mathrm{PG}(n-1,q)$.

Точките на произволно подпространство в $\mathrm{PHG}({}_R R^n)$ могат да се представят като решения на някаква система от линейни уравнения над R. Ако две подпространства са i-ти съседи, то съответните системи линейни уравнения могат да бъдат избрани по такъв начин, че да съдържат едни и същи уравнения по модул $(\operatorname{rad} R)^i$.

Теорема 2.12. Нека $\Pi=\mathrm{PHG}({}_R R^n)$ и нека Δ_1 и Δ_2 са подпространства на Йелмслев за Π с $\dim\Delta_1\le\dim\Delta_2$ и $\Delta_1\bigcirc_i\Delta_2$. Нека освен това Δ_2 е множество от точки $R(x_1,\ldots,x_u)$, удовлетворяващи линейната система

$$\sum_{l=1}^{n} a_{jl}x_l=0,\ \ j=1,\ldots,n-u.$$

Тогава съществуват такива елементи $b_{js}\in(\operatorname{rad} R)^i,\ \ j=1,\ldots,n-u,\ \ s=1,\ldots,n$, че Δ_1 може да се представи като множество от точки, които са решения на системата

$$\sum_{l=1}^{n}(a_{jl}+b_{jl})x_l=0,\ \ j=1,\ldots,n-u.$$

Нека R е верижен пръстен, за който $|R| = q^m$ и $R/\operatorname{rad} R \cong \mathbb{F}_q$. Ако ${}_RM$ е R-модул от тип λ, то броят на подмодулите на M от тип μ, $\mu \leq \lambda$ се задава с числа, които могат да се разглеждат като обобщение на гаусовите коефициенти и формула за които е дадена в Теорема 2.8. Този резултат позволява да се определят редица числови характеристики на геометриите $\mathrm{PHG}({}_RR^n)$. Така като частен случай получаваме следната теорема.

Теорема 2.13. Нека $\Pi = \mathrm{PHG}({}_RR^n)$, където R е верижен пръстен, за който $|R| = q^m$, $R/\operatorname{rad} R \cong \mathbb{F}_q$. Тогава

(a) броят на точките в Π е $\begin{bmatrix} n \\ 1 \end{bmatrix}_{q^m} = q^{(n-1)(m-1)} \dfrac{q^n - 1}{q - 1}$;

(b) броят на точките в един i-ти клас на съседство е $q^{(n-1)(m-i)}$ за $1 \leq i \leq m$;

(c) броят на класовете на i-съседство е равен на $q^{(n-1)(i-1)} \begin{bmatrix} n \\ 1 \end{bmatrix}_q$;

(d) броят на подпространствата на Йелмслев с проективна размерност $s-1$ е равен на $\begin{bmatrix} n \\ s \end{bmatrix}_{q^m} = q^{s(n-s)(m-1)} \dfrac{q^n - 1}{q - 1}$;

(e) броят на $(s-1)$-мерните подпространства на Йелмслев, съдържащи фиксирано $(t-1)$-мерно подпространство на Йелмслев, $t \leq s \leq n$, е равен на

$$q^{(s-t)(n-s)(m-1)} \begin{bmatrix} n-t \\ s-t \end{bmatrix}_q .$$

Ще разгледаме една специална подструктура на инцидентност, съдържаща се в $\Pi = \mathrm{PHG}({}_RR^n)$. Да фиксираме подпространство на Йелмслев S в Π с проективна размерност $\dim S = s-1$. Нека $[S]^{(i)}$ е множеството на точките от $\mathcal{P}$, които са i-ти

съседи на S (за които съществува точка върху S, която е техен i-ти съсед). Дефинираме ново множество от точки

$$\mathfrak{P} = \left\{ U \cap [P]^{m-i} \mid P \in \mathcal{P}_i(S),\ \dim U = s-1,\ U \bigcirc_i S,\ U \cap [P]^{m-i} \neq 0 \right\}.$$

С други думи новото множество от точки се състои от сеченията на $(s-1)$-мерните подпространства на Йелмслев с класовете от $(m-i)$-вите съседи. Лесно се доказва, че множествата $U \cap [P]^{m-i}$ или съвпадат или не се пресичат. Така точките са подпространства от тип $m^1 i^{s-1}$. По-нататък дефинираме множеството от прави

$$\mathfrak{L} = \left\{ V \mid V < R^q,\ V \subseteq [S]^{(i)},\ V \ \text{ от тип } \ m^2 i^{k-2} \right\}.$$

Инцидентност $\mathfrak{I} \subseteq \mathfrak{P} \times \mathfrak{L}$ се задава стандартно с теоретико-множествено включване. Така дефинираната структура на инцидентност $(\mathfrak{P}, \mathfrak{L}, \mathfrak{I})$ може да се вложи в подходящо избрана геометрия на Йелмслев. Това е съдържанието на следната теорема (вж. [35, 40]).

Теорема 2.14. Структурата на инцидентност $(\mathfrak{P}, \mathfrak{L}, \mathfrak{I})$ може да се вложи изоморфно в $\mathrm{PHG}\,({}_{R'}R')^n$, където $R' = R/(\mathrm{rad}\, R)^{m-i}$. Липсващата част съдържа точките на $(n-s-2)$-мерно подпространство на Йелмслев и всички нетривиално пресичащи го прави.

Нека $\Pi = (\mathcal{P}, \mathcal{L}, I)$ е проективно пространство на Йелмслев. Нека H е фиксирана хиперравнина. Структурата на инцидентност $(\mathcal{P}_0, \mathcal{L}_0, I)$, където $\mathcal{P}_0 = \mathcal{P} \backslash [H]$, $\mathcal{L}_0 = \{L \backslash [H] \mid L \in \mathcal{L}\}$, а I_0 е инцидентността, наследена от Π, наричаме *афинно пространство на Йелмслев*. Ако $\Pi = \mathrm{PHG}({}_R R^n)$, то афинната геометрия, получена по описания начин бележим с $\mathrm{AHG}({}_R R^{n-1})$. В този случай $\mathcal{P}_0$ се състои от всички елелменти на ${}_R R^{n-1}$, а $\mathcal{L}_0$ - от всички съседни класове на свободни подмодули от ранг 1. Ако в Теорема 2.14 изберем пространство S с проективна размерност 0, т.е. S е точка, то получената структура е афинна геометрия на Йелмслев.

Следствие 2.15. Нека R е верижен пръстен с индекс на нилпотентност m и остатъчно поле от ред q. Нека P е точка от геометрията $\mathrm{PHG}({}_R R^n) = (\mathcal{P}, \mathcal{L}, I)$ и нека $i \in \{1, 2, \ldots, m-1\}$. Структурата на инцидентност, състояща се от всички точки в $[P]^{(m-i)}$ заедно с правите $L \cap [P]^{(m-i)}$ и с инцидентност, наследена от $\mathrm{PHG}({}_R R^n)$, е изоморфна на $\mathrm{AHG}({}_{R_0} {R_0}^n)$, където $R_0 \cong R/(\mathrm{rad}\, R)^i$.

Друг специален случай се получава когато S е хиперравнина. Тогава структурата на инцидентност от Теорема 2.14 е изоморфна на $\mathrm{PHG}\,({}_{R'} R'^n)$, където $R' = R/(\mathrm{rad}\, R)^{m-i}$, като липсващата част е съседен клас от точки.

Строги доказателства на тези факти се съдържат в [35, 40].

Глава 3

Стандартна форма на матрица над верижен пръстен

Обектите, които изследваме в тази работа, са множества от подпространства в геометрии на Йелмслев. В тази връзка централен е въпросът за представянето на подмодулите на ${}_RR^n$. То трябва да бъде избрано така, че да е възможно ефективно сравняване на подмодули, ефективно намиране на обединение, сечение, и ортогонално допълнение, ефективно решаване на въпроса дали даден подмодул се включва в друг подмодул, както и ефективно генериране на всички подмодули от даден тип, съдържащи се във фиксиран подмодул. Това е изключително важно, ако при изследването на аналози на мрежови кодове над пръстени и свързаните с тях комбинаторни конфигурации се използват компютри. В този раздел ще въведем т.нар. стандартна форма на матрица над верижен пръстен, която представя едно възможно решение за тези проблеми.

Нека R е краен верижен пръстен с индекс на нилпотентност m и остатъчно поле $R/\operatorname{rad} R \cong \mathbb{F}_q$, $q = p^r$, където p е просто число. Фиксираме по произволен начин пораждащ на радикала $\theta \in \operatorname{rad} R \setminus \operatorname{rad}^2 R$. Нека M е подмодул на ${}_RR^n$. Ясно е, че M е краен, а следователно и крайно породен. Целта ни ще бъде да изберем такава система от пораждащи за M, която е еднозначно определена от модула и с която може да се работи ефективно.

Еквивалентно, при зададена $k \times n$-матрица A, чиито редове пораждат M, нашата цел ще бъде да определим такава матрица B, която е от някакъв специален вид, редовете ѝ пораждат модула, породен от редовете на A и освен това е единствената матрица от този вид, която поражда въпросния модул M.

Да означим с $\mathfrak{M}_{k,n}(R)$ множеството на всички $k \times n$ матрици над R. Когато пръстенът R е ясен от контекста, ще пишем само $\mathfrak{M}_{k,n}$.

Дефиниция 3.1. Казваме, че матрицата $A = (a_{ij}) \in \mathfrak{M}_{k,n}(R)$ е в *стандартна форма*, ако изпълнява 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) $j_1 < j_2 < j_3 < \dots$.

Нека $\boldsymbol{a} = (a_1, \dots, a_n) \in {}_RR^n$. Най-малкото число $i \in \{0, \dots, m\}$, за което $\theta^i \boldsymbol{a} = \mathbf{0}$, наричаме *тип* на $\boldsymbol{a}$. Следователно съществува поне една компонента на $\boldsymbol{a}$, която се съдържа във фактора $(\operatorname{rad} R)^{m-i} \backslash (\operatorname{rad} R)^{m-i+1}$. Тази компонента a_j, за която j е минимално, наричаме *водеща компонента* или *водещ елемент* на $\boldsymbol{a}$. Нека $A \in \mathfrak{M}_{k,n}(R)$. В дефиницията по-горе с t_i означаваме типа на реда i в матрицата A, $i = 1, \dots, k$, а с j_i номера на водещия елемент в този ред. Множеството на координатните позиции на водещите елементи на редовете от A ще бележим с $J(A)$, т.е. $J(A) = \{j_1, j_2, \dots, j_k\}$.

Лема 3.2. Нека ${}_RM$ е ляв подмодул на ${}_RR^n$ и нека A е матрица в стандартна форма, чиито редове пораждат ${}_RM$. Нека $s \in \{1, \dots, n\}$ е позицията на водещия елемент на $\boldsymbol{v} \in {}_RM$. Тогава $s \in J(A)$.

Доказателство. Нека редовете на A са $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_k$. Нека освен това $J(A) = \{j_1, \ldots, j_k\}$ и съответните водещи елементи са

$$\theta^{m-t_1}, \theta^{m-t_2}, \ldots, \theta^{m-t_k}.$$

Без ограничение на общността ще предполагаме, че $t_1 \geq t_2 \geq \ldots \geq t_k \geq 1$. От тези неравенства и от свойства (2) и (4) в дефиницията за стандартна форма на матрица следва, че всички елементи в стълба с номер j_s, $s = 1, \ldots, k$, намиращи се под водещия елемент на ред s, са нули.

Да разгледаме $\boldsymbol{v} = \lambda_1 \boldsymbol{v}_1 + \boldsymbol{v}_2 + \ldots + \lambda_k \boldsymbol{v}_k \in {}_R M$. Нека водещата компонента на $\boldsymbol{v}$ е в позиция l. Ще разгледаме три случая за l.

(1) Нека $l < j_1$. Да допуснем, че $s \in \{1, \ldots, k\}$ е такова число, че типът на $\lambda_s \boldsymbol{v}_s$ е най-големият между типовете на векторите $\lambda_i \boldsymbol{v}_i$, $i = 1, \ldots, k$. Ако $\lambda_s \in (\operatorname{rad} R)^{\tau_s}$, то типът на $\boldsymbol{v}$ е най-много $t_s - 1 - \tau_s$. От друга страна елементът в позиция j_s на $\boldsymbol{v}$ е

$$\lambda_s + (\text{членове, които са линейна комбинация на } 1, \theta, \ldots, \theta^{m-t_s-1}).$$

Тогава типът на $\boldsymbol{v}$ е най-малко $t_s - \tau_s$, което е противоречие.

(2) Нека $j_{i-1} < l < j_i$. Да допуснем, че $\lambda_s \neq 0$ за някое $s \leq i-1$ и $\lambda_s \boldsymbol{v}_s$ е най-голям тип на вектор измежду векторите $\{\lambda_1 \boldsymbol{v}_1, \ldots, \lambda_i \boldsymbol{v}_i\}$. Ако $\lambda_s \in (\operatorname{rad} R)^{\tau_s}$, този най-голям тип е най-много $t_s - \tau_s$. От друга страна в позиция j_s векторът $\boldsymbol{v}$ има елемент

$$\lambda_s \theta^{m-t_s} + (\text{ линейна комбинация на } 1, \theta, \ldots, \theta^{m-t_s-1}).$$

Първият член е от $R\theta^{m-t_s+\tau_s}$, но той е вляво от водещия елемент, което е противоречие. Дотук показахме, че $\lambda_j = 0$ за всички $j \leq i-1$. Сега можем да използваме аргументите от (1), за да получим противоречие.

(3) Ако $l > j_k$ можем да повторим аргументацията от първата част на (2).

От (1)–(3) следва, че l трябва да е в координатна позиция, която е от $J(A)$. $\square$

Теорема 3.3. За всеки модул ${}_RM \leq {}_RR^n$ съществува единствена матрица B в стандартна форма, редовете на която пораждат M.

Доказателство. (1) *Съществуване.* Ще докажем съществуването на матрицата B чрез индукция по $k = \operatorname{rk} M$. За $k = 1$ няма какво да се доказва. Ще отбележим само, че чрез подходящо умножение можем да направим така, че водещият елемент да е от вида θ^{m-t} за някое t.

Нека $\boldsymbol{v}_1' \in M$ е елемент с възможно най-голям тип в M, например $m - t_1$. Без ограничение на общността можем да предположим, че водещата компонента е в позиция j_1 и се намира най-вляво измежду всички водещи компоненти на векторите на M. Чрез подходящо умножение можем да направим този водещ елемент равен на θ^{m-t_1}. Сега ${}_RM = R\boldsymbol{v}_1' \oplus {}_RM'$, където ${}_RM'$ има ранг $k-1$ и е подмодулът на ${}_RM$, състоящ се от елементи, които имат 0 в позиция j_1. Това следва от факта, че за всеки вектор $\boldsymbol{v} \in {}_RM$ можем да намерим такова $\lambda \in R$, че $\boldsymbol{v} - \lambda_1 \boldsymbol{v}_1'$ да има нула в позиция j_1.

От индукционната хипотеза следва, че съществува матрица B в стандартна форма, чийто редове пораждат ${}_RM'$. Ще означим тези редове с $\boldsymbol{v}_2, \ldots, \boldsymbol{v}_k$. Нека $J(B) = \{j_2, \ldots, j_k\}$. Освен това нека j_s-тата компонента на $\boldsymbol{v}_1'$ е $\alpha_s + \beta_s \theta^{m-t_s}$, $\beta_s = y_0 + \cdots + y_{t_s-1}$, $x_i, y_i \in \Gamma$.

Елементът $\boldsymbol{v}_1 = \boldsymbol{v}_1' - \beta_2 \boldsymbol{v}_2 - \ldots - \beta_k \boldsymbol{v}_k$ има свойството, че елементът на позиция j_s е по-малък (по отношение на наредбата $\prec$) от θ^{m-t_s} за всяко $s = 2, \ldots, k$. Ясно е още, че компонентите на $\boldsymbol{v}_1$, които се намират наляво от водещия елемент, принадлежат на $\operatorname{rad} R^{m-t+1}$ (тъй като i-тата компонента, $i < j_1$, на всеки един от векторите $\boldsymbol{v}_1', \boldsymbol{v}_2, \ldots, \boldsymbol{v}_k$ е от $\operatorname{rad} R^{m-t+1}$). Следователно матрицата A с редове векторите $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_k$ е търсената матрица.

(2) *Единственост* Да предположим, че съществуват матрици

$$A' = (\boldsymbol{v}_1', \boldsymbol{v}_2', \ldots, \boldsymbol{v}_k')^T \text{ и } A'' = (\boldsymbol{v}_1'', \boldsymbol{v}_2'' \ldots, v_k'')^T$$

в стандартна форма, чиито редове пораждат един и същи модул ${}_RM$. Съгласно лема 3.2 имаме $J(A') = J(A'') = \{j_1, \ldots, j_k\}$. Нека водещият елемент на $\boldsymbol{v}_i'$ (съответно, $\boldsymbol{v}_i''$) е $\theta^{m-t_i'}$ (съответно, $\theta^{m-t_i''}$). Без ограничение на общността можем да считаме, че $t_1' \geq t_2' \geq$

$\cdots \geq t'_k$. В частност това означава, че всички елементи на A' в стълбове $j_1, \ldots, j_k$, намиращи се под водещия елемент на съответния ред са нули, т.е. имаме

$$\begin{array}{rcccccccccc}
v'_1 & = & (\ldots & \theta^{m-t_1} & v'_{1j_2} & \ldots & v'_{1j_i} & \ldots & v'_{1j_k} & \ldots) \\
v'_2 & = & (\ldots & 0 & \theta^{m-t_2} & \ldots & v'_{2j_i} & \ldots & v'_{2j_k} & \ldots) \\
\vdots & & & \vdots & \vdots & & \vdots & & \vdots & \\
v'_i & = & (\ldots & 0 & 0 & \ldots & \theta^{m-t'_i} & \ldots & v'_{ij_k} & \ldots) \\
\vdots & & & \vdots & \vdots & & \vdots & & \vdots & \\
v'_k & = & (\ldots & 0 & 0 & \ldots & 0 & \ldots & \theta^{m-t'_k} & \ldots)
\end{array}$$

Сега можем да изразим $\boldsymbol{v}''_i$ като $\boldsymbol{v}''_1 = \lambda_1 v'_1 + \cdots + \lambda_k v'_k$. Тъй като водещият елемент на $\boldsymbol{v}''_i$ се намира на позиция j_i имаме, че

$$\theta^{m-t''_i} = \lambda_i \theta^{m-t'_i} + \sum_{s=1}^{i-1} \lambda_s v'_{sj_s}.$$

Ще отбележим, че $\lambda_s = 0$ за всяко $s < i$, в противен случай водещият елемент на $\boldsymbol{v}''_i$ ще е в позиция с по-малък номер от j_i. Следователно горното равенство ще се опрости до $\theta^{m-t''_i} = \lambda_i \theta^{m-t'_i}$, откъдето следва, че $m - t'_i \leq m - t''_i$, т.е. $t'_i \geq t''_i$ за всяко $i = 1, \ldots, k$. Тъй като множествата $\{t'_i\}$ и $\{t''_i\}$, взети в ненарастващ ред, задават типа на ${}_RM$ имаме, че $\{t'_i\} = \{t''_i\}$, за всяко i.

Сега можем да заключим, че в позиции $j_1, \ldots, j_{k-1}$ $\boldsymbol{v}_k$ има нули и $\theta^{m-t'_k} = \theta^{m-t''_k}$ в позиция j_k. Тогава $\boldsymbol{v}'_k - \boldsymbol{v}''_k$ има нули на позиции $j_1, \ldots, j_k$. Нека $\boldsymbol{v}'_k - \boldsymbol{v}''_k \neq 0$. Тогава неговият водещ елемент е на позиция, различна от $j_1, \ldots, j_k$, което е противоречие с лема 3.2. Следователно, $\boldsymbol{v}'_k = \boldsymbol{v}''_k$ и доказателството се завършва чрез индукция по ранга на ${}_RM$. $\square$

Следствие 3.4. Нека A е $(k \times n)$-матрица в стандартна форма над верижен пръстен R. Съществуват пермутационни матрици

T_1 с размер $k \times k$ и T_2 с размер $n \times n$ такива, че

$$T_1 A T_2 = \begin{pmatrix} I_{k_0} & A_{01} & A_{02} & \dots & A_{0,m-1} & A_{0,m} \\ 0 & \theta I_{k_1} & \theta A_{12} & \dots & \theta A_{1,m-1} & \theta A_{1,m} \\ 0 & 0 & \theta^2 I_{k_2} & \dots & \theta^2 A_{2,m-1} & \theta^2 A_{2,m} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & \theta^{m-1} I_{k_{m-1}} & \theta^{m-1} A_{m-1,m} \end{pmatrix}. \quad (3.1)$$

Нека е дадена матрица A, чийто редове пораждат левия подмодул ${}_RM$ на ${}_RR^n$. Ще представим алгоритъм за генерирането на матрица A в стандартна форма, чиито редове, пораждат модула ${}_RM$.

Алгоритъм 3.5. Получаване на матрица в стандартна форма

Вход: $k \times n$ матрица A с елементи от пръстена R
Изход: матрица B в стандартна форма, чийто редове пораждат ${}_RM$

1: ***set*** $B = \varnothing$

2: ***for*** $t = m, ..., 1$ ***do***

3: ***for*** всеки ред $\boldsymbol{r}$ на матрицата A ***do***

4: ***if*** не всички елементи на $\boldsymbol{r}$ са кратни на θ^{m-t+1} ***then***

5: Намери най-лявата позиция i на $\boldsymbol{r}$, която не е кратна на θ^{m-t+1}

6: Умножи отляво всички елементи на $\boldsymbol{r}$ с $\left(\varphi^{-1}\left(\frac{\varphi(r_i)}{q^{m-t}}\right)\right)^{-1}$

7: Нека $C = B \cup A \setminus \{\boldsymbol{r}\}$

//C е обединението на редовете на B и A минус ред $\boldsymbol{r}$

8: ***for*** всеки ред $\boldsymbol{r}'$ на C ***do***

9: ***set*** $c = \varphi^{-1}\left(\left\lfloor \frac{\varphi(r_i)}{q^{m-t}} \right\rfloor\right)$

10: $\boldsymbol{r}' \longleftarrow \boldsymbol{r}' - c \cdot \boldsymbol{r}$

11: ***if*** $r' = 0$ ***then*** $A \longleftarrow A \setminus \boldsymbol{r}'$

// $\boldsymbol{r}'$ се изтрива от A

12: ***endfor***

13: $\boldsymbol{r}$ се поставя като i-ти ред на B и се изтрива от A

14: ***endif***

15: ***endfor***

16: ***endfor***

17: ***for*** всеки ред $\boldsymbol{b}$ на матрицата B

18: Нека j е най лявата ненулева позиция в $\boldsymbol{b}$

19: За всеки ред c от $B \setminus \{\boldsymbol{b}\}$, който предхожда $\boldsymbol{b}$

20: ***if*** $c_j \geq b_j$ ***do***

21: ***set*** $d_1 = \left\lceil \frac{q^m - c_j}{b_j} \right\rceil$

22: $\boldsymbol{b} \longleftarrow \boldsymbol{c} + c_1 \cdot \boldsymbol{b}$

23: ***endif***

24: ***endfor***

25: ***return*** B

Използвайки Алгоритъм 3.5 лесно можем да получим най-малкия модул, съдържащ два зададени подмодула. С други думи това е подмодулът, породен от обединението на двата подмодула. Двата подмодула са породени от редовете на две матрици A_1 и A_2. Достатъчно е да образуваме нова матрица $\left(\frac{A_1}{A_2}\right)$ и да я приведем в стандартна форма чрез Алгоритъм 3.5.

Алгоритъм 3.6. Модул, породен от обединението на подмодули

Вход: матрици A_1 и A_2 с размери, съответно $k_1 \times n$ *i* $k_2 \times n$

Изход: матрица B в стандартна форма, чиито редове пораждат модула, породен от редовете на A_1 и A_2.

1: ***set*** $A = \left(\frac{A_1}{A_2}\right)$

2: Прилагаме Алгоритъм 3.5 за полуване на стандартна форма B на матрицата A

3: ***return*** B

Алгоритъм 3.5 може да се използва и за проверка на това дали даден подмодул се съдъжа в друг даден подмодул.

Алгоритъм 3.7. Тест за включване

Вход: Матрици A и B в стандартна форма с един и същ брой стълбове

Изход: ***Yes*** - ако модулът, породен от редовете на матрицата B се съдържа в модула, породен от редовете на A;
No - в противен случай

1: Създава се матрицата $C = \left(\dfrac{A}{B}\right)$

2: Чрез Алгоритъм 3.5 се намира матрицата D – стандартна форма на C

3: ***If*** $D = A$ ***then*** B се съдържа в A;

4: ***return*** *Yes*

5: ***else return*** *No*

По-нататък ще се спрем на получаването на десния ортогонален модул на ляв модул над краен верижен пръстен. Да разгледаме левия R-модул ${}_RM$ над крайния верижен пръстен R. Да означим с A матрицата в стандартна форма, чиито редове пораждат ${}_RM$. По-долу ще получим в явен вид матрица B, чиито редове пораждат ортогоналния модул $M_R^{\perp}$. Матрицата B ще бъде също във вид близък до стандартна форма. За да получим стандартна форма на B, отговаряща на дефиницията от началото на тази глава, ще е достатъчно да вземем стълбовете от получената блочна форма в обратен ред.

Теорема 3.8. Нека ${}_RM$ е подмодул на ${}_RR^n$, породен от редовете на матрицата A, която има вида (3.1). Тогава, $M_R^{\perp}$ се поражда от матрицата

$$B = \begin{pmatrix} B_{0,m} & B_{1,m} & B_{2,m} & \cdots & B_{m-2,m} & B_{m-1,m} & I_{k_m} \\ B_{0,m-1}\theta & B_{1,m-1}\theta & B_{2,m-1}\theta & \cdots & B_{m-2,m-1}\theta & I_{k_{m-1}}\theta & 0 \\ B_{0,m-2}\theta^2 & B_{1,m-2}\theta^2 & B_{2,m-2}\theta^2 & \cdots & 0I_{k_{m-2}}\theta^2 & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ B_{02}\theta^{m-2} & B_{12}\theta^{m-2} & I_{k_2}\theta^{m-2} & \cdots & 0 & 0 & 0 \\ B_{01}\theta^{m-1} & I_{k_1}\theta^{m-1} & 0 & \cdots & 0 & 0 & 0 \end{pmatrix}, \tag{3.2}$$

където $k_m = n - k_0 - \ldots - k_{m-1}$ и

$$B_{ij} = -(A_{ij} - \sum_{1<k<j+1} A_{ik}A_{k,j+1} + \sum_{i<k<l<j+1} A_{ik}A_{kl}A_{l,j+1} - \cdots + (-1)^{j-i+1}A_{i,i+1}A_{i+1,i+2}\ldots A_{j,j+1})^T. \quad (3.3)$$

Доказателство. Типът на модула ${}_RM$ е $m^{k_0}(m-1)^{k_1}\ldots 2^{k_{m-2}}1^{k_{m-1}}$. Да положим $k_m = n - k_0 - k_1 - \ldots - k_{m-1}$. Тогава ортогоналният модул $M_R^\perp$ е от тип $m^{k_m}(m-1)^{k_{m-1}}\ldots 2^{k_2}1^{k_1}$. Ще търсим матрицата B, чийто редове пораждат $M_R^\perp$ във вида (3.2). Матриците A_{ij} са индексирани така, че размерът им е $k_i \times k_j$; за матриците B_{ij} индексацията е такава, че размерът им е $k_j \times k_i$. Тогава B_{ij}^T е с размери $k_i \times k_j$.

Сега условието за вида на матриците B_{ij}, $i < j$, от условието на теоремата $AB^T = \mathbf{0}$, където $\mathbf{0}$ е нулевата матрица с размер $(n-k_m)\times(n-k_0)$. Ще използваме индукция по $j - i$.

Нека $j - i = 1$, т.е. $j = i + 1$. От произведението на $(i+1)$-вия ред на A и $(m-i)$-тия стълб на B^T получаваме

$$\theta^i I_{k_i} B_{i,i+1}^T \theta^{m-1-i} + \theta^i A_{i,i+1}\theta^{m-1-i} = \mathbf{0},$$

което следва от $B_{i,i+1} = -A_{i,i+1}^T$. По-нататък нека да разгледаме произведението на $(i+1)$-вия ред на A и $(m+1-j)$-тия стълб на B^T за някакви i, j, $j > i$. Получаваме

$$\theta^i I_{k_i} B_{i,j}^T \theta^{m-j} + \theta^i A_{i,i+1} B_{i+1,j}^T \theta^{m-j} + \ldots + \theta^i A_{i,j} I_{k_j} \theta^{m-j} = \theta^i (B_{i,j} + A_{i,i+1}^T B_{i+1,j} + \ldots + A_{i,j}^T)\theta^{m-j},$$

за което, използвайки (3.3), лесно се проверява, че е нулевата матрица. □

Забележка 3.9. Теорема 3.8 може да се разглежда като обобщение на следния добре известен факт. Ако векторното пространство над крайното поле $\mathbb{F}_q$ е породено от редовете на матрица $A \in \mathfrak{M}_{k,n}(\mathbb{F}_q)$ от вида

$$A = (I_k|X),$$

то ортогоналното пространство $V^{\perp}$ се поражда от редовете на

$$B = (-X^T | I_{n-k}).$$

Следствие 3.10. Нека $A \in \mathfrak{M}_{k,n}$ е матрица над верижния пръстен R, чийто редове пораждат модула ${}_RM$. Нека $A' = T_1 A T_2$, е матрица от вида (3.1), където T_1 и T_2 са пермутационни матрици с размери, съответно, $(n-k_m) \times (n-k_m)$ и $n \times n$. Тогава редовете на матрицата

$$B = T_1 B' T_2^T,$$

където B' е матрицата, зададена чрез (3.2), пораждат модула $M_R^{\perp}$.

Доказателство. От $A'B'^T = \mathbf{0}$ получаваме

$$T_1 A T_2 B' = \mathbf{0} \implies A(T_2 B'^T T_1^T),$$

откъдето $B^T = T_2 B''^T T_1^T$ и $B = T_1 B' T_2^T$. □

Доколкото Теорема 3.8 и Следствие 3.10 представят в явен вид матрица, чиито редове пораждат ортогоналния модул $M_R^{\perp}$, то алгоритъмът, който при заден модул пресмята ортогоналния му, е очевиден.

Алгоритъм 3.11. Намиране на ортогоналния модул $M^{\perp}$

Вход: матрица A, чийто редове пораждат левия модул ${}_RM$

Изход: матрица C, чиито редове пораждат десния модул $M_R^{\perp}$, ортогонален на ${}_RM$

1: Намират се пермутационни матрици T_1 и T_2, които пробразуват A до вида (3.1)

2: Изчисляват се матриците B_{ij} чрез (3.3)

3: Пресмята се матрицата B чрез (3.2)

4: Пресмята се $C = T_1^T B T_2^T$

5: ***return*** C

Сечението на два модула може да се получи от Теорема 2.10(3), от която имаме, че

$$M_1 \cup M_2 =^{\perp} (M_1^{\perp} + M_2^{\perp}),$$

Така получаването на матрица, чийто редове пораждат сечението на два дадени модула, се свежда до изпълнението на следния алгоритъм.

Алгоритъм 3.12. Сечение на модули

Вход: Матрици A и B в стандартна форма,
чиито редове пораждат,
съответно, модулите M и N.
Изход: Матрица C, чийто редове пораждат сечението
на M и N.

1: Използваме Алгоритъм 3.11 за намиране на матриците $A^{\perp}$ и $B^{\perp}$, пораждащи десните ортогонални модули $M^{\perp}$ и $N^{\perp}$, съответно.

2: Образуваме $U = \left(\dfrac{A^{\perp}}{B^{\perp}}\right)$

3: Прилагаме Алгоритъм 3.11 за построяване на матрицата ${}^{\perp}U$, ляво ортогонална на U.

4: ***return*** $C = {}^{\perp}U$

При компютърни пресмятания често се налага генерирането на всички подмодули от даден тип на фиксиран модул ${}_RM$. Нека ${}_RM \leqq_R R^n$ е модул от тип λ, където

$$\lambda = (\underbrace{m,\ldots,m}_{k_0},\underbrace{m-1,\ldots,m-1}_{k_1},\ldots,\underbrace{1,\ldots,1}_{k_{m-1}}) =$$

$$(\lambda_1,\lambda_2,\ldots,\lambda_k) = m^{k_0}(m-1)^{k_1}\ldots 1^{k_{m-1}},\ k = \sum_{i=0}^{m-1} k_i.$$

Нека ${}_RN$ е подмодул на ${}_RM$ от тип $\mu = (\mu_1,\mu_2,\ldots,\mu_l)$, където $\mu \prec \lambda$. Нека редовете на матрицата A с размери $k \times m$, която е в стандартна форма, пораждат ${}_RM$. Без ограничение на общността може да считаме, че A е от вида (3.1). Нека освен това е дадена $l \times n$ - матрица B в стандартна форма, чийто редове пораждат ${}_RN$. Редовете на B са линейни комбинации на редовете на A. Следователно съществува такава матрица C, също в стандартна форма, за която матрицата B се изразява във вида $B = CA$. Освен това матрицата C трябва да има следните свойства:

(1) ако водещият елемент в ред i на матрицата B е в позиция j_i, то водещият елемент на ред i в матрицата C се намира в позиция $l_i \geqq j_i$;

(2) елементите на C, намиращи се в стълб j, където

$$k_0 + \cdots + k_{s-1} + 1 \leq j \leq k_0 + \cdots + k_{s-1} + k_s,\ k_{-1} = 0,$$

са от $\Gamma + \theta\Gamma + \cdots + \theta^{m-s-1}\Gamma$.

Горното наблюдение ни позволява да конструираме всички подмодули от даден тип на модул ${}_RM$, породен от редовете на дадена матрица A. Пораждането на всички подмодули от фиксиран тип е еквивалентно на конструирането на всички матрици C, които притежават свойствата (1) и (2). Тъй като типът на

модула, породен от редовете на матрицата B не следва директно от вида на матрицата C, то той трябва да бъде проверен в отделна стъпка. По-долу представяме алгоритъм за генерирането на всички подмодули от даден тип, а след това и пример, който илюстрира алгоритъма.

Алгоритъм 3.13. Пораждане на всички подмодули от даден тип

Вход: матрица A в стандартна форма, чиито редове пораждат модул от тип $\lambda = (\lambda_1, \ldots, \lambda_k)$; фиксиран тип $\mu = (\mu_1, \ldots, mu_k) \prec \lambda$

Изход: множество от матрици, чиито редове пораждат всички подмодули на M от тип μ.

1: Намират се матрици T_1 и T_2, за да се трансформира A до матрица A', която е от вида *(3.1)*

2: ***for*** всяка k-орка $\{j_1, \ldots, j_l\} \subseteq \{1, \ldots, k\}$ ***do***

3: ***for*** всяка l-орка $(t_1, \ldots, t_l)$, $t_i \in \{0, \ldots, m-1\}$

4: Нека $c_{ij_i} = \theta^{t_i}$, $i = 1, \ldots, l$

5: ***for*** всеки избор на останалите елементи на C, изпълняващи (1) и (2)

6: конструираме матрицата C

7: ***if*** типът на CA е μ ***then print:*** C

8: конструират се всички матрици

Ще отбележим, че проверката в стъпка [7 :] може да бъде пропусната, ако в стъпка [3 :] генерираме само онези l-орки, които пораждат подмодул от тип μ.

Пример 3.14. Нека $R = \mathbb{Z}_4$ и нека

$$A = \begin{pmatrix} 1 & 0 & 1 & 1 & 2 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 2 & 2 \end{pmatrix}.$$

Модулът M породен от редовете на A е от тип $\lambda = (2, 2, 1, 1)$. Ще конструираме всички подмодули $N \leq M$ от тип $\mu = (2, 1)$. Съгласно Теорема 2.8 имаме, че броят на всички подмодули N на M от указания тип е

$$\begin{bmatrix} \lambda \\ \mu \end{bmatrix}_{2^2} = 2^{1(4-2)} \begin{bmatrix} 4-1 \\ 2-1 \end{bmatrix}_2 \cdot 2^{0(2-0)} \begin{bmatrix} 2-0 \\ 1-0 \end{bmatrix}_2 = 2^2(2^2+2+1)(2+1) = 84.$$

Ще конструираме всички матрици C, удовлетворяващи горните условия, които водят до подмодули от тип μ. Матрицата A е вече от необходимия вид, така че пропускаме стъпка 1. В стъпка 2 генерираме всички възможни позиции за водещите елементи на редовете на C.

$$\begin{pmatrix} \bullet & \circ & \circ & \circ \\ \circ & \bullet & \circ & \circ \end{pmatrix}, \begin{pmatrix} \bullet & \circ & \circ & \circ \\ \circ & \circ & \bullet & \circ \end{pmatrix}, \begin{pmatrix} \bullet & \circ & \circ & \circ \\ \circ & \circ & \circ & \bullet \end{pmatrix}$$

$$\begin{pmatrix} \circ & \bullet & \circ & \circ \\ \circ & \circ & \bullet & \circ \end{pmatrix}, \begin{pmatrix} \circ & \bullet & \circ & \circ \\ \circ & \circ & \circ & \bullet \end{pmatrix}, \begin{pmatrix} \circ & \circ & \bullet & \circ \\ \circ & \circ & \circ & \bullet \end{pmatrix}$$

В стъпка 3 пробваме всички възможности за водещите елементи. Някои от тях ще доведат до подмодули, които не са от тип μ. За водещите елементи имаме следните възможности:

$$\begin{pmatrix} 1 & \circ & \circ & \circ \\ \circ & 2 & \circ & \circ \end{pmatrix}, \begin{pmatrix} 2 & \circ & \circ & \circ \\ \circ & 1 & \circ & \circ \end{pmatrix}, \begin{pmatrix} 1 & \circ & \circ & \circ \\ \circ & \circ & 1 & \circ \end{pmatrix}$$

$$\begin{pmatrix} 1 & \circ & \circ & \circ \\ \circ & \circ & \circ & 1 \end{pmatrix}, \begin{pmatrix} \circ & 1 & \circ & \circ \\ \circ & \circ & 1 & \circ \end{pmatrix}, \begin{pmatrix} \circ & 1 & \circ & \circ \\ \circ & \circ & \circ & 1 \end{pmatrix}$$

Ще отбележим, че последните два стълба на C могат да съдържат само елементи от $\Gamma = \{0, 1\}$. Така имаме следните възмож-

ности да допълним елементите на матриците C.

$$\begin{pmatrix} 1 & \Gamma & \Gamma & \Gamma \\ 0 & 2 & 0 & 0 \end{pmatrix}, \qquad \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 1 & \Gamma & \Gamma \end{pmatrix}, \qquad \begin{pmatrix} 1 & R & 0 & \Gamma \\ 0 & \operatorname{rad} R & 1 & \Gamma \end{pmatrix}$$

$$\begin{pmatrix} 1 & R & \Gamma & 0 \\ 0 & \operatorname{rad} R & 0 & 1 \end{pmatrix}, \begin{pmatrix} \operatorname{rad} R & 1 & 0 & \Gamma \\ \operatorname{rad} R & 0 & 1 & \Gamma \end{pmatrix}, \begin{pmatrix} \operatorname{rad} R & 1 & \Gamma & 0 \\ \operatorname{rad} R & 0 & 0 & 1 \end{pmatrix}$$

Тук $R = \{0, 1, 2, 3\}$, $\Gamma = \{0, 1\}$ и $\operatorname{rad} \mathbb{R} = \{0, 2\}$. Следователно броят на матриците C от първия тип е 8, от втория тип – 4, от третия – 32 и т.н., което дава общо

$$8 + 4 + 32 + 16 + 16 + 8 = 84,$$

подмодула, което вече пресметнахме.

Глава 4

Спредове в проективни пространства на Йелмслев

4.1 R-аналози на дизайни

Нека R е краен верижен пръстен, за който $|R| = q^m$ и $R/\operatorname{rad} R \cong \mathbb{F}_q$. Да фиксираме естествено число n и ненарастваща редица от цели неотрицателни числа $(\kappa_1, \kappa_2, \ldots, \kappa_n)$, за която е изпълнено

$$m \geq \kappa_1 \geq \kappa_2 \geq \ldots \geq \kappa_n \geq 0.$$

Да означим с $\mathcal{G}_R^{(l)}(n, \kappa)$ (съответно с $\mathcal{G}_R^{(r)}(n, \kappa)$) множеството на всички подмодули на ${}_RR^n$ (съответно на R_R^n), имащи тип κ. Това множество наричаме *Грасманиан* на подмодулите от тип κ. Ясно е, че $\mathcal{G}_R^{(l)}(n, \kappa) = \mathcal{G}_{R^{\mathrm{opp}}}^{(r)}(n, \kappa)$, където R^{opp} е противоположният пръстен за R, който съдържа елементите на R и в който умножението $*$ се задава с $a*b := ba$. Освен това е очевидно, че за всеки комутативен верижен пръстен R е в сила $\mathcal{G}_R^{(l)}(n, \kappa) = \mathcal{G}_R^{(r)}(n, \kappa)$. Така оттук нататък, без ограничение на общността, ще разглеждаме само леви модули и ще изпускаме горния индекс в означенията.

В този раздел ще въведем R-аналози на дизайни. Много от резултатите, известни за класическите q-аналози на дизайни [19, 20, 21, 22] са в сила и за R-аналозите, но съществуват и някои разлики. В следващите няколко дефиниции n и l са цели

положителни числа, а $\tau = (\tau_1, \ldots, \tau_n)$ и $\kappa = (\kappa_1, \ldots, \kappa_n)$ са ненарастващи редици с дължина n, за които е изпълнено

$$\tau \leq \kappa \leq (\underbrace{m, m, \ldots, m}_{n}).$$

Ще повторим, че с $\tau \leq \kappa$ означаваме, че $\tau_i \leq \kappa_i$ за всяко $i = 1, \ldots, n$.

Дефиниция 4.1. Едно семейство D от елементи на $\mathcal{G}_R(n, \kappa)$ наричаме *R-дизайн* с параметри τ-(n, κ, ℓ), ако всеки подмодул от $\mathcal{G}_R(n, \tau)$ се съдържа в точно ℓ подмодула от D. В случая, когато $\ell = 1$, дизайнът D се нарича *Щайнерова система* и се означава със $S_R(\tau, \kappa, n)$.

Дефиниция 4.2. Едно семейство C от елементи на $\mathcal{G}_R(n, \kappa)$ наричаме *покриващ R-дизайн* $C_R(n, \kappa, \tau)$, ако всеки елемент от $\mathcal{G}_R(n, \tau)$ се съдържа в поне един подмодул от C.

Дефиниция 4.3. Едно семейство T от елементи на $\mathcal{G}_R(n, \kappa)$ наричаме *Туранов R-дизайн* $T_R(n, \kappa, \tau)$, ако всеки подмодул от $\mathcal{G}_R(n, \kappa)$ съдържа поне един елемент от T.

С други думи подмодулите от T блокират модулите от $\mathcal{G}_R(n, \kappa)$. Някои класически обекти от крайните геометрии могат да се разглеждат като Туранови дизайни. Така например, блокиращите множества по отношение на хиперравнините в $\mathrm{PHG}(n-1, R)$ могат да се разглеждат като Туранови R-дизайни с $\kappa = m^{n-1}$ и $\tau = m^1$.

Нека S е множество от подмодули от Грасманиана $\mathcal{G}_R^{(l)}(n, \kappa)$. Да означим със $S^\perp$ множеството от ортогоналните модули на модулите от S:

$$S^\perp := \{X^\perp \mid X \in S\}.$$

Ясно е, че $S^\perp \subseteq \mathcal{G}_R^{(r)}(n, \overline{\kappa})$, където

$$\overline{\kappa} = (m - \kappa_1, m - \kappa_2, \ldots, m - \kappa_n).$$

Теорема 4.4. Множеството от подмодули $S \subseteq \mathcal{G}_R^{(l)}(n,\kappa)$ е покриващ R-дизайн с параметри $C_R(n,\kappa,\tau)$ тогава и само тогава, когато $S^\perp$ е Туранов R-дизайн с параметри $T_R(n,\overline{\tau},\overline{\kappa})$ в $\mathcal{G}_R^{(r)}(n,\overline{\kappa})$.

Доказателство. Нека $S \subseteq \mathcal{G}_R^{(l)}(n,\kappa)$ е покриващ R-дизайн с параметри $C_R(n,\kappa,\tau)$. За всеки модул $Y \in \mathcal{G}_R^{(r)}(n,\overline{\tau})$ ортогоналният модул $Y^\perp$ е елемент на $\mathcal{G}_R^{(l)}(n,\tau)$. Следователно съществува елемент X от R-дизайна S, който съдържа $Y^\perp$, т.е. $X^\perp \subset Y$ и X е от тип κ. Оттук получаваме, че $(Y^\perp)^\perp = Y \supset X^\perp$ като $X^\perp \in \mathcal{G}_R^{(r)}(n,\overline{\kappa})$. С други думи, показахме, че всеки подмодул Y от $\mathcal{G}_R^{(r)}(n,\overline{\tau})$ съдържа поне един подмодул от $S^\perp$. Следователно $S^\perp$ е Туранов R-дизайн с параметри $T_R(n,\overline{\tau},\overline{\kappa})$.

Обратната посока на твърдението се доказва аналогично. $\square$

Следващата теорема е необходимо условие за съществуване на τ-(n,κ,ℓ)-дизайни.

Теорема 4.5. Нека D е R-дизайн с параметри τ-(n,κ,ℓ). Тогава

$$|D| = \ell \cdot \frac{\begin{bmatrix} \boldsymbol{m} \\ \tau \end{bmatrix}_{q^m}}{\begin{bmatrix} \kappa \\ \tau \end{bmatrix}_{q^m}}.$$

В частност, $\begin{bmatrix} \kappa \\ \tau \end{bmatrix}_{q^m}$ дели $\ell \cdot \begin{bmatrix} \boldsymbol{m} \\ \tau \end{bmatrix}_{q^m}$.

Доказателство. Да преброим по два начина двойките (X,Y), където $X \in D$ е подмодул от тип κ в ${}_RR^n$, а Y е подмодул на ${}_RR^n$ от тип τ, който се съдържа в X.

От една страна X може да се избере по $|D|$ начина и за всеки избор на X съществуват $\begin{bmatrix} \kappa \\ \tau \end{bmatrix}_{q^m}$ възможности за избор на Y, тъй като този обобщен гаусов коефициент задава броя на подмодулите от тип τ, съдържащи се в модул от тип κ. От друга страна Y може да се избере по $\begin{bmatrix} \boldsymbol{m} \\ \tau \end{bmatrix}_{q^m}$ начина, а за всеки избор Y имаме ℓ възможности за X, тъй като D е τ-(n,κ,ℓ) R-дизайн.

Следователно,

$$|D| \cdot \begin{bmatrix} \kappa \\ \tau \end{bmatrix}_{q^m} = \ell \cdot \begin{bmatrix} \boldsymbol{m} \\ \tau \end{bmatrix}_{q^m},$$

което трябваше да се докаже. □

Теорема 4.6. Нека S е покриващ R-дизайн с параметри $C_R(n, \kappa, \tau)$. Тогава

$$|S| \geq \frac{\begin{bmatrix} \boldsymbol{m} \\ \tau \end{bmatrix}_{q^m}}{\begin{bmatrix} \kappa \\ \tau \end{bmatrix}_{q^m}}.$$

Доказателство. Всеки подмодул от тип κ покрива $\begin{bmatrix} \kappa \\ \tau \end{bmatrix}_{q^m}$ подмодула от тип τ. От друга страна, съществуват точно $\begin{bmatrix} \boldsymbol{m}^n \\ \tau \end{bmatrix}_{q^m}$ подмодула от тип τ в ${}_R R^n$, откъдето следва желаният резултат. □

Важен и централен за този дисертационен труд е случаят на τ-дизайни, за които $\tau = (m, 0, \ldots, 0)$. За тези τ един τ-(n, κ, ℓ)-дизайн е множество от подпространства от тип κ в $\mathrm{PHG}({}_R R^n)$, които съдържат всяка точка ℓ пъти. В случая $\ell = 1$ въпросните дизайни са семейства от подпространства от тип κ, покриващи всички точки на геометрията точно веднъж. Такива семейства от точки се наричат *спредове*.

В класическите геометрии $\mathrm{PG}(n, q)$ е известно необходимо и достатъчно условие за съществуване на спред от r-мерни подпространства: такъв спред съществува тогава и само тогава, когато $r + 1$ дели $n + 1$ [5, 29, 49]. В едната посока това твърдение е очевидно и следва от факта, че броят на точките в r-мерно подпространство трябва да дели броя на всички точки в $\mathrm{PG}(n, q)$. То следва и от Теорема 4.5, в която крайното поле $\mathbb{F}_q$ се разглежда като тривиален верижен пръстен без собствени идеали. В другата посока доказателството е нетривиално и се основава на факта, че всяко поле е векторно подпространство над всяко свое подполе.

4.2 Необходими условия за съществуване на спредове

Да фиксираме краен верижен пръстен R с индекс на нилпотентност m и остатъчно поле от ред q. Нека $\Pi = \mathrm{PHG}({}_R R^{n+1})$ е n-мерната проективна геометрия на Йелмслев над R. По-нататък $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_{n+1})$ е ненарастващата редица, за която

$$m = \lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_n \geq \lambda_{n+1} \geq 0.$$

Едно множество $\mathcal{S}$ от подпространства на Π, всяко от които е от тип λ, се нарича *λ-спред* в Π, ако то е разбиване на множеството от точки на Π. Това означава, че всяка точка от геометрията се съдържа в точно едно подпространство от $\mathcal{S}$. Едно очевидно необходимо условие е Теорема 4.5, съгласно която броят на точките в подпространство от тип λ трябва да дели броя на точките в цялата геометрия. Както в случая на геометриите $\mathrm{PG}(n, q)$, това условие се оказва и достатъчно, когато

$$\lambda = (\underbrace{m, m, \ldots, m}_{k}, \underbrace{0, \ldots, 0}_{n-k+1}) = m^k,$$

т.е. подпространствата в спреда са подпространства на Йелмслев и асоциирани със свободни подмодули на ${}_R R^n$. Доказателството на този факт обобщава класическото доказателство за съществуване на спредове в геометриите $\mathrm{PG}(n, q)$.

Теорема 4.7. *[52]* Нека R е верижен пръстен, за който $|R| = q^m$, $R/\operatorname{rad} R \cong \mathbb{F}_q$. Спред от r-мерни подпространства на Йелмслев в n-нерната геометрия $\mathrm{PHG}({}_R R^{n+1})$ съществува тогава и само тогава, когато $r + 1$ дели $n + 1$.

Доказателство. Необходимост. Броят на точките в подпространство на Йелмслев от спреда трябва да дели броя на точките в $\mathrm{PHG}({}_R R^{n+1})$. От Теорема 2.13 следва, че $\begin{bmatrix} r+1 \\ 1 \end{bmatrix}_{q^m}$ дели

$\begin{bmatrix} n+1 \\ 1 \end{bmatrix}_{q^m}$. Оттук получаваме, че $q^{r(m-1)}\dfrac{q^{r+1}-1}{q-1}$ дели $q^{n(m-1)}\dfrac{q^{n+1}-1}{q-1}$, т.е. $\dfrac{q^{r+1}-1}{q-1}$ дели $\dfrac{q^{n+1}-1}{q-1}$, т.е. $r+1$ дели $n+1$.

Достатъчност. Ще докажем, че условието $r+1$ да дели $n+1$ е и достатъчно за съществуване на спред. Да допуснем, че то е изпълнено, т.е. $n+1=(r+1)(l+1)$ за някакво цяло число l.

Съгласно характеризационната теорема за верижни пръстени (Теорема 2.2) $R \cong S[X;\sigma]/(g(X), p^{s-1}X^t)$ за някой полином на Айзенщайн $g(X)$ от степен k, където $m=(s-1)k+t$. Да разгледаме разширение T на S от степен $r+1$, т.е. $T=S[Y]/(f(Y))$ за някакъв полином $f(Y)$ от степен $r+1$, който е неразложим по модул p. По-нататък да разгледаме пръстена

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

в който $\alpha X = X\alpha^\sigma$ за всеки елемент $\alpha \in T$. Пръстенът R_{r+1} може да се разглежда като свободен модул от ранг $r+1$ над R. Така всеки елемент b от R_{r+1} може да бъде записан като

$$b=b_0+b_1Y+\ldots+b_rY^r, \quad b_i \in R.$$

Ясно е, че R_{r+1}^{l+1} и R^{n+1} са изоморфни като модули над R. Така всяка точка от $\mathrm{PHG}(R_R^{n+1})$ може да се разглежда като $(l+1)$-орка от елементи на R_{r+1}. Обратно, всяка наредена $(l+1)$-орка над R_{r+1}, в която поне една компонента е обратим елемент, може да се разглежда като точка в $\mathrm{PHG}(R_{r+1}^{l+1})$.

Нека $\gamma=(\gamma_0,\ldots,\gamma_l)$ е неторзионен вектор в R_{r+1} и да допуснем, че γ_0 е обратим елемент в R. Изборът на позиция, в която γ да съдържа обратим елемент е несъществен. Да разгледаме системата

$$\left|\begin{array}{lllllll} -\gamma_1x_0 & +\gamma_0x_1 & & & & = & 0 \\ -\gamma_2x_0 & & +\gamma_0x_2 & & & = & 0 \\ & & & \ddots & & = & \vdots \\ -\gamma_kx_0 & & & & +\gamma_0x_k & = & 0 \end{array}\right. . \tag{4.1}$$

Решенията на (4.1) образуват свободен подмодул от ранг 1 в R_{r+1}^{k+1}. Този подмодул може да се разглежда като свободен подмодул от ранг $r+1$ в R^{n+1}, т.е. като r-мерно подпространство на Йелмслев. Лесно се проверява, че два подмодула от ранг $r+1$ в ${}_RR^{n+1}$, получени от различни подмодули от ранг 1 на ${}_RR_{r+1}^{k+1}$, не могат да имат общ неторзионен вектор. Следователно подпространствата на Йелмслев, представени от тях, образуват разбиване на множеството от точки на $\mathrm{PHG}({}_RR^{n+1})$, а с това и спред. □

В общия случай от Теорема 2.8 получаваме следното необходимо условие за съществуване на спред.

Теорема 4.8. Нека в $\Pi = \mathrm{PHG}({}_RR^{n+1})$ съществува λ-спред, където $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_k)$ и $m = \lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_k > 0$. Тогава λ'_m дели $n+1$, където λ'_m е свободният ранг на подмодул от тип λ (т.е. най-малкият член в дуалното разбиване на λ).

Доказателство. Тъй като по условие съществува λ-спред, то броят на точките в подпространство от тип λ трябва да дели броя на точките в цялата геометрия. Броят на точките в подпространство от тип λ е

$$q^{\sum_{i=1}^{m-1}(\lambda'_i-1)} \begin{bmatrix} \lambda'_m \\ 1 \end{bmatrix}_{q^m},$$

а броят на точките в геометрията е $q^{(m-1)(n-1)} \begin{bmatrix} n \\ 1 \end{bmatrix}_{q^m}$. Ясно е, че $q^{\sum_{i=1}^{m-1}(\lambda'_i-1)} \begin{bmatrix} \lambda'_m \\ 1 \end{bmatrix}_{q^m}$ дели $q^{(m-1)(n-1)} \begin{bmatrix} n \\ 1 \end{bmatrix}_{q^m}$ тогава и само тогава, когато $q^{\lambda'_m} - 1$ дели $q^n - 1$, което от своя страна е в сила тогава и само тогава, когато λ'_m дели n. □

За спредове от подпространства на Йелмслев това условие е и достатъчно съгласно Теорема 4.7. както ще демонстрираме по-късно за спредове от подпространства (асоциирани с несвободни подмодули на ${}_RR^{n+1}$), това комбинаторно условие не е

достатъчно. Първият такъв пример е представен в [52]. Там е показано, че за всеки верижен пръстен R с индекс на нилпотентност 2 е невъзможно да разбием тримерната геометрия на Йелмслев $\mathrm{PHG}({}_R R^4)$, на ленти от съседни прави, т.е. на подпространства от тип $2^2 1^1$.

В следващия раздел ще конструираме широк спектър от типове λ, за които необходимото условие от Теорема 4.8 се удовлетворява, но въпреки това не съществува λ-спред. Най-напред ще разрешим някои типове от специален вид. Следващата лема се получава лесно от Теорема 2.11.

Лема 4.9. Нека R е верижен пръстен, за който $|R| = q^m$, $R/\operatorname{rad} R \cong \mathbb{F}_q$. Нека S е подпространство в $\mathrm{PHG}({}_R R^{n+1})$, от тип $\lambda = (\lambda_1, \ldots, \lambda_{n+1})$, където $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_{n+1} > 0$. Тогава множеството $\widetilde{S}$, съдържащо всички $(m-1)$-съседни класове от точки, съдържащи се в S е подпространство в $\mathrm{PHG}({}_{\widetilde{R}}\widetilde{R}^n)$, $\widetilde{R} = R/(\operatorname{rad} R)^{m-1}$, от тип $\mu = (\lambda_1 - 1, \lambda_2 - 1, \ldots, \lambda_{n+1} - 1)$.

Доказателство. Нека S е подпространство тип λ, а $[P]^{(m-1)}$ е $(m-1)$-ви съседен клас от точки. От $\lambda_n > 0$ следва, че $[P]^{(m-1)}$ или се съдържа изцяло в S или няма общи точки с това подпространство. Оттук лесно се получава, че множеството на $(m-1)$-съседните класове в S образуват подпространство във фактор-геометрията $\mathrm{PHG}({}_{\widetilde{R}}\widetilde{R}^n)$. $\square$

От Лема 4.9 получаваме следния резултат.

Теорема 4.10. Нека R е верижен пръстен с индекс на нилпотентност m. Ако съществува λ-спред в $\mathrm{PHG}({}_R R^{n+1})$, където $\lambda = (\lambda_1, \ldots, \lambda_{n+1})$, $\lambda_1 \geq \ldots \geq \lambda_{n+1} > 0$, то съществува и μ-спред в $\mathrm{PHG}({}_{\widetilde{R}}\widetilde{R}^{n+1})$, $\widetilde{R} = R/(\operatorname{rad} R)^{m-\lambda_{n+1}}$, където

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

Сега ще опишем конструкция на спредове от подпространства, които не са подпространства на Йелмслев. Доказателството следва стандартната схема за доказване на съществуване на спредове в проективни геометрии над крайни полета. Накратко

тя може да бъде описана по следния начин. За даден верижен пръстен R с индекс на нилпотентност m дефинираме разширение Q от степен h със същия индекс на нилпотентност m. След това разглеждаме $(l-1)$-мерна геометрия на Йелмслев над Q и дефинираме изображение $\widetilde{\psi}$ от $\mathrm{PHG}({}_QQ^l)$ в $\mathrm{PHG}({}_RR^{hl})$. Всяко разбиване на $\mathrm{PHG}({}_QQ^l)$ на подпространства от даден тип $\lambda = m^{a_1}(m-1)^{a_2}\ldots$ индуцира μ-спред в $\mathrm{PHG}({}_RR^{hl})$, който е от тип $\mu = m^{a_1h}(m-1)^{a_2h}\ldots$.

Да припомним, че R е фиксиран верижен пръстен, за който $|R| = q^m$, $R/\operatorname{rad} R \cong \mathbb{F}_q$. Приемаме, че $q = p^r$ и $\operatorname{char} R = p^s$. Да запишем m във вида $m = (s-1)l + t$. Съгласно 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 разглеждаме пръстена

$$Q = T[X;\sigma]/(g(X), p^{s-1}X^t). \tag{4.2}$$

Очевидно е изпълнено $|Q| = q^{mh}$ и $|T/\operatorname{rad} T| = q^h$. Елементите на Q могат да се представят във вида

$$a_0 + a_1Y + \ldots + a_{h-1}Y^{h-1},\ a_i \in R.$$

Лесно се забелязва, че всички елементи, за които всички a_i от горното представяне са в $\operatorname{rad} R$, се съдържат в радикала на Q. Следователно,

$$\{a_0 + a_1Y + \ldots + a_{h-1}Y^{h-1} \mid a_i \in \operatorname{rad} R\} \subseteq \operatorname{rad} Q, \tag{4.3}$$

откъдето $|\operatorname{rad} Q| \geq |\operatorname{rad} R|^h = q^{(m-1)h}$. Тъй като радикалът е максимален идеал за всеки верижен пръстен, то $T/\operatorname{rad} T$ и $Q/\operatorname{rad} Q$ са полета, като при това $T/\operatorname{rad} T$ е подполе на $Q/\operatorname{rad} Q$. Следователно $|Q/\operatorname{rad} Q| \geq |T/\operatorname{rad} T| = q^h$, и освен това

$$q^{mh} = |Q| = |Q/\operatorname{rad} Q||\operatorname{rad} Q| \geq q^h \cdot q^{(m-1)h} = q^{mh}.$$

Оттук следва, че $|\operatorname{rad} Q| = q^{(m-1)h}$ и от (4.3) получаваме, че

$$\operatorname{rad} Q = \{a_0 + a_1 Y + \ldots + a_{h-1} Y^{h-1} \mid a_i \in \operatorname{rad} R\}. \tag{4.4}$$

В следващата теорема пръстените R, Q, S се използват в смисъла, изяснен в горните редове.

Теорема 4.11. Нека R е верижен пръстен, за който е изпълнено $|R| = q^m$, $R/\operatorname{rad} R \cong \mathbb{F}_q$. Нека по-нататък Q е разширението на R, дефинирано в (4.2). Нека $n = hl$ и да предположим, че съществува λ-спред в $\mathrm{PHG}({}_Q Q^l)$, 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 $\mathrm{PHG}({}_R R^n)$, за който

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

Доказателство. Да дефинираме изображението $\psi : Q \to R^h$ по следния начин: ако $\alpha = a_0 + a_1 Y + \ldots + a_{h-1} Y^{h-1}$, $a_i \in R$, то

$$\psi(\alpha) = (a_0, a_1, \ldots, a_{h-1}).$$

Това изображение може да бъде продължено по естествен начин и върху Q^l чрез

$$\widetilde{\psi} : \left\{ \begin{array}{ccc} Q^l & \to & R^{hl} \\ (\alpha_0, \alpha_1, \ldots, \alpha_{l-1}) & \to & (\psi(\alpha_0), \psi(\alpha_1), \ldots, \psi(\alpha_{l-1})) \end{array} \right. .$$

да отбележим, че ако $x = (x_0, x_1, \ldots, x_{l-1})$ е торзионен вектор, т.е. $x_i \in \operatorname{rad} Q$ за всички $i = 0, \ldots, l-1$, то $\widetilde{\psi}(x)$ също е торзионен вектор над R, т.е. $\widetilde{\psi}(x) \in (\operatorname{rad} R)^{hl}$ (вж. (4.4)).

Нека M_1 и M_2 са подмодули на ${}_Q Q^l$, чието сечение $M_1 \cap M_2$ не съдържа неторзионен елемент. С други думи предполагаме, че M_1 и M_2 не съдържат общ свободен подмодул от ранг 1. Геометрично това означава, че подпространствата M_1 и M_2 нямат

обща точка. Тогава съгласно (4.4) и образите $\widetilde{\psi}(M_1)$ и $\widetilde{\psi}(M_2)$ също нямат обща точка. Ако

$$\boldsymbol{x} = (x_{0,0}, \ldots, x_{0,h-1}, x_{1,0}, \ldots, x_{1,h-1}, \ldots, x_{l-1,0}, \ldots, x_{l-1,h-1})$$

е вектор над R, имащ поне една обратима компонента, то тогава той е образ $\widetilde{\psi}(\boldsymbol{y})$ на вектор

$$\boldsymbol{y} = (y_0, y_1, \ldots, y_{l-1})$$

над Q, за който $y_i = x_{i,0} + x_{i,1}Y + \ldots + x_{i,h-1}Y^{h-1}$. Следователно, ако множеството $\mathcal{S} = \{S_1, S_2, \ldots\}$ от подпространства на $\mathrm{PHG}({}_QQ^l)$ е разбиване на точките на $\mathrm{PHG}({}_QQ^l)$, то тогава и

$$\mathcal{S}' = \{\widetilde{\psi}(S_1), \widetilde{\psi}(S_2), \ldots\}$$

е разбиване на точките на $\mathrm{PHG}({}_RR^n)$.

Сега, ако $\mathcal{S}$ се състои от подпространства от тип λ, то всяко $S \in \mathcal{S}$ се представя като

$$S = \theta^{m-\lambda_1}\boldsymbol{e}_1 + \theta^{m-\lambda_2}\boldsymbol{e}_2 + \ldots + \theta^{m-\lambda_l}\boldsymbol{e}_l,$$

където $\boldsymbol{e}_i$ е неторзионен вектор над Q, т.е. всяко $\boldsymbol{e}_i$ поражда подмодул на Q^l от тип m^1. Тъй като Q е свободен модул от ранг h над R, то векторите $\widetilde{\psi}(\boldsymbol{e}_iY^j)$, $j = 0, \ldots, h-1$, пораждат свободен модул от тип m^h. Оттук следва, че ако $\mathcal{S}$ е спред от подпространства от тип λ на $\mathrm{PHG}({}_QQ^l)$, то

$$\mathcal{S}' = \{\widetilde{\psi}(S) \mid S \in \mathcal{S}\}$$

е μ-спред на $\mathrm{PHG}({}_RR^{hl})$, където $\mu = \lambda_1^h\lambda_2^h \ldots$. $\square$

Нека $[P]$ е съседен клас от точки в $\mathrm{PHG}({}_RR^n)$, където, както и по-горе, R е верижен пръстен, за който $|R| = q^m$, $R/\operatorname{rad} R \cong \mathbb{F}_q$. Съседният клас $[P]$ е подмодул от тип $m^1(m-1)^{n-1}$ и е изоморфен на афинната геометрия $\mathrm{AHG}((R/(\operatorname{rad} R)^{m-1})^n)$. Твърдим, че за всяка $(n-1)$-орка $(\lambda_1, \ldots, \lambda_{n-1})$, за която $m-1 \geq \lambda_1 \geq \ldots \geq \lambda_{n-1} \geq 0$, съществува разбиване на $[P]$ на подпространства от тип $(m, \lambda_1, \ldots, \lambda_{n-1})$.

Този факт може да се докаже чрез двойна индукция по m и n. Фактът е очевиден за $m = 1$ и всички n (това е случаят, когато R е крайно поле), както и за $n = 2$ и всички m (това е случаят, когато геометрията е проективна права).

Нека $\lambda_{n-1} > 0$ и да разгледаме индуцираната геометрия, която се получава от $(m-1)$-вите класове на съседство, състоящи се от точки в $[P]$. Съществуването на желаното разбиване следва по индукция от съществуването на разбиване от тип $(m-1, \lambda_1 - 1, \ldots, \lambda_{n-1} - 1)$ в $\mathrm{AHG}((R/(\operatorname{rad} R)^{m-2})^n)$. Ако $\lambda_{n-1} = 0$, разглеждаме разбиването на $[P] \cong \mathrm{AHG}((R/(\operatorname{rad} R)^{m-1})^n)$ на успоредни хиперравнини, изоморфни на $\mathrm{AHG}((R/(\operatorname{rad} R)^{m-1})^{n-1})$ и използваме още веднъж индукционното допускане във всяка от тях.

Това наблюдение заедно с Теорема 4.11 води до следното достатъчно условие за съществуване на спредове.

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

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

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

Един важен въпрос, който възниква е дали съществуват λ-спредове за типове, които не се покриват от онези, характеризирани с условията в Теорема 4.12. Ако не съществуват други спредове, то бихме получили следното необходимо и достатъчно условие за съществуване на λ-спред:

В $\mathrm{PHG}({}_R R^n)$ съществува λ-спред тогава и само тогава, когато λ'_m дели n, както и всички λ'_i за $i = 1, \ldots, m$. Както навсякъде дотук $\lambda' = (\lambda'_1, \ldots, \lambda'_m)$ е дуалното разбиване на λ.

Това, че подпространствата в един спред не се пресичат не означава, че асоциираните с тях модули се пресичат само в нулевия вектор. Всъщност може да се докаже, че в конструкцията, представена в доказателството на Теорема 4.7, се получават модули с голямо непразно сечение (което обаче не съдържа

свободни подмодули). Може да се зададе въпрос за съществуването на спредове, в които сечението на всеки два подмодула в спреда е минимално. За спредове от прави в $\mathrm{PHG}({}_RR^4)$ това означава, че никои две от правите не са съседи.

За верижни пръстени с индекс на нилпотентност 2 такива спредове са конструирани с помощта на компютър за пръстените с четири и девет елемента. Лесно се получава, че в първия случай такъв спред съществува: 20 прави (за пръстени с 4 елемента) и 90 прави (за пръстени с 9 елемента). Важна нерешена задача е проблемът за съществуване на такива спредове за всеки верижен пръстен с индекс на нилпотентност 2.

По-долу са представени спредове от прави в $\mathrm{PHG}({}_RR^4)$, за двата верижни пръстена с $|R| = 4$. Правите в спреда са представени с матрици в стандартна форма.

За пръстена $\mathbb{Z}_4$ спредът съдържа следните прави:

$$\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 2 & 0 \\ 2 & 1 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 & 3 \\ 2 & 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 2 \\ 0 & 2 & 1 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 & 3 \\ 0 & 1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 3 & 0 & 2 \\ 0 & 2 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 3 & 0 \\ 0 & 1 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 3 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 0 & 2 \\ 0 & 0 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 2 & 1 \\ 0 & 1 & 2 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 1 & 0 & 3 \\ 0 & 0 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 & 0 \\ 2 & 2 & 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 2 & 3 \\ 0 & 1 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 0 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 3 & 3 & 0 \\ 0 & 2 & 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 1 & 0 & 2 \\ 0 & 2 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 3 & 2 \\ 0 & 1 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 & 3 \\ 0 & 1 & 0 & 2 \end{pmatrix}$$

За другия верижен пръстен с четири елелмента, $\mathbb{F}_2/(X^2)$ спредът съдъжа следните прави:

$$\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & X & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1+X & 0 & X \\ 0 & 0 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix},$$

$$\begin{pmatrix} X & 0 & 1 & 0 \\ X & X & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 0 & X \\ 0 & 0 & 1 & X \end{pmatrix}, \begin{pmatrix} X & 1 & 0 & 1+X \\ X & 0 & 1 & 1 \end{pmatrix},$$

$$\begin{pmatrix} 1 & 0 & X & 1+X \\ 0 & 1 & 1+X & 1 \end{pmatrix}, \begin{pmatrix} 1 & X & 0 & X \\ 0 & 0 & 1 & 1+X \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 & 1+X \\ 0 & 0 & 1 & 0 \end{pmatrix},$$

$$\begin{pmatrix} 1 & 0 & 1 & X \\ 0 & 1 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & X & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & X \\ 0 & X & 1 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 & 1+X \\ 0 & 1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1+X & 1 & 0 \\ 0 & X & X & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1+X & X \end{pmatrix},$$

$$\begin{pmatrix} X & 1 & 1+X & 0 \\ 0 & 0 & X & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & X & X \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1+X & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

$$\begin{pmatrix} 1 & 0 & X & 1 \\ 0 & 1 & X & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 & 1+X \\ 0 & 1 & 0 & X \end{pmatrix}$$

4.3 Несъществуване на спредове от определен тип

Известно е, че в геометриите $\mathrm{PHG}({}_R R^n)$, където $n \geq 4$ е четно число и R е верижен пръстен с индекс на нилпотентност 2, не съществуват λ-спредове, за които $\lambda = 2^{n/2}1^{n/2-1}$ ([52], Теорема 14). Този резултат може да се обобщи за верижни пръстени с произволен индекс на нилпотентност m: не съществуват λ-спредове с $\lambda = m^{n/2}(m-1)^{n/2-1}$ в проективните геометрии на

Йелмслев $\mathrm{PHG}({}_RR^n)$, където R е верижен пръстен с индекс на нилпотентност m. Доказателството на този факт повтаря стъпките на това, което е приведено в [52].

В този раздел ще обобщим Теорема 14 от [52] в малко поразлична посока. Ще докажем, че в геометрии с нечетна (проективна) размерност над верижни пръстени с индекс на нилпотентност 2 не съществуват λ-спредове с $\lambda = 2^{n/2}1^a$, където a е произволно цяло число, за което $1 \leq a \leq \frac{n}{2} - 1$. Да отбележим, че съгласно Теорема 4.12 съществуват λ-спредове при $\lambda = 2^{n/2}$ и $\lambda = 2^{n/2}1^{n/2}$. Следователно доказателството за несъществуване може да се разглежда като стъпка в посока на доказване на хипотезата, изказана в края на предния раздел.

Теорема 4.13. Нека R е краен верижен пръстен с индекс на нилпотентност 2 и нека $\Pi = \mathrm{PHG}({}_RR^n)$, $n \geq 4$ четно число, е проективна геометрия на Йелмслев над R. Тогава за никое a, $1 \leq a \leq n/2$, в геометриите $\Pi = \mathrm{PHG}({}_RR^n)$ не съществува λ-спред за $\lambda = 2^{n/2}1^a$.

Доказателство. Да допуснем, че съществува λ-спред $\mathcal{S}$ с подпространства от тип λ, като λ е от вида, указан в условието на теоремата. Броят на точките в подпространство от тип λ е равен на

$$q^{\frac{n}{2}+a-1}\frac{q^{\frac{n}{2}}-1}{q-1}$$

(съгласно Теорема 2.8). Следователно броят на подпространствата в $\mathcal{S}$ е равен на

$$\frac{q^{n-1}\frac{q^n-1}{q-1}}{q^{\frac{n}{2}+a-1}\frac{q^{\frac{n}{2}}-1}{q-1}} = q^{\frac{n}{2}-a}(q^{\frac{n}{2}}+1).$$

Нека сега разгледаме подпространство S от тип λ и нека $[H]$ е съседен клас от хиперравнини, т.е. подпространство от тип $2^{n-1}1$. Възможните типове на сеченията на S със съседния клас $[H]$, т.е. възможните типове на модула $S \cap [H]$ са следните:

(a) $2^{\frac{n}{2}}1^a$ – това се случва, когато S се съдържа в съседния клас $[H]$;

(b) $2^{\frac{n}{2}-1}1^{a+1}$.

Отново съгласно Теорема 2.8 получаваме, че в случай (a) сечението $S \cap [H]$ съдържа $q^{n-a-1}(q^{n/2}-1)/(q-1)$ точки, докато в случая (b) същото сечение има $q^{n-a-1}(q^{n/2-1}-1)/(q-1)$ точки. Да означим с x броя на подпространствата $S \in \mathcal{S}$, които пресичат $[H]$ в подпространство от тип (a); аналогично с y означаваме броя на подпространствата от $\mathcal{S}$, имащи тип (b). Тъй като ограниченията на подмножествата от $\mathcal{S}$ върху $[H]$ образуват разбиване на $[H]$, получаваме следната система:

$$\begin{array}{rcrcl} x & + & y & = & q^{n/2-a}(q^{n/2}+1) \\ q^{n/2+a-1}\frac{q^{n/2}-1}{q-1}x & + & q^{n/2+a-1}\frac{q^{n/2-1}-1}{q-1}y & = & q^{n-1}\frac{q^{n/2}-1}{q-1} \end{array}.$$

Тази система има единствено решение

$$x = q^{n/2-a}, y = q^{n-a}. \tag{4.5}$$

Оттук следва, че всеки съседен клас от хиперравнини съдържа точно $q^{n/2-a}$ подпространства от спреда.

Да изследваме възможните сечения на произволно подпространство от тип λ и хиперравнина Π. Тъй като хиперравнините са подпространства от тип 2^{n-1}, то съществуват четири възможни типа за сеченията $S \cap H$:

(c) $2^{n/2}1^a$ като в този случай $S \cap H$ съдържа $q^{n/2+a-1}(q^{n/2}-1)/(q-1)$ точки;

(d) $2^{n/2}1^{a-1}$ като в този случай $S \cap H$ съдържа $q^{n/2+a-2}(q^{n/2}-1)/(q-1)$ точки;

(e) $2^{n/2-1}1^{a+1}$ като в този случай $S \cap H$ съдържа $q^{n/2+a-1}(q^{n/2-1}-1)/(q-1)$ точки;

(f) $2^{n/2-1}1^a$ като в този случай $S \cap H$ съдържа $q^{n/2+a-2}(q^{n/2-1}-1)/(q-1)$ точки.

Да означим с u, v, w и t броя на подпространствата от $\mathcal{S}$, пресичащи H в подпространство от тип, съответно, (c), (d), (e) и (f). Нека отбележим, че ако $S \cap H$ е от тип (c), (d) или (e), то $S \subseteq [H]$. От това наблюдение получаваме

$$u + v + w = q^{n/2-a},\ t = q^{n-a}.$$

Сега, преброявайки точките в H, получаваме:

$$q^{n/2+a-1}\frac{q^{n/2}-1}{q-1}u + q^{n/2+a-2}\frac{q^{n/2}-1}{q-1}v + q^{n/2+a-1}\frac{q^{n/2-}-1}{q-1}w + \\ q^{n/2+a-2}\frac{q^{n/2-1}-1}{q-1} = q^{n-2}\frac{q^{n-1}-1}{q-1},$$

откъдето

$$q(q^{n/2}-1)u + (q^{n/2}-1)v + q(q^{n/2-1}-1)w = q^{n/2-a}(q^{n/2}-1). \qquad (4.6)$$

Очевидно имаме $(q, q^{n/2}-1) = 1$ и $(q^{n/2-1}-1, q^{n/2}-1) = (n/2-1, n/2) = 1$ откъдето следва, че $q^{n/2}-1$ дели w. Тъй като

$$w \leq u + v + w = q^{n/2-a} < q^{n/2} - 1,$$

получаваме $w = 0$. Оттук следва, че

$$\begin{array}{rcrcl} u & + & v & = & q^{n/2-a} \\ qu & + & v & = & q^{n/2-a} \end{array}.$$

което има единствено решение $u = 0$, $v = q^{n/2-a}$. Това е изпълнено за всеки избор на хиперравнина H. Но H може да се избере по такъв начин, че да съдържа подпространство от спреда. Оттук получаваме желаното противоречие. $\square$

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] A. Betten, M. Braun, H. Fripertinger, A. Kerber, A. Kohnert, A. Wassermann, *Error-Correcting Linear Codes. Classification by Isometry and Applications*, Springer Verlag, 2006.

[5] M. Bilioti, N. Johnson, V. Zha, Foundation of translation planes, CRC Press, 2001.

[6] I.F. Blake, Codes over certain rings, *Information and Control* **20**(1972), 396–404.

[7] I.F. Blake, Codes over integer residue rings, *Information and Control* **29** (1975), 295–300.

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

[9] E. Byrne, M. Greferath, T. Honold, Ring geometries, two-weight codes, and strongly regular graphs, *Designs, Codes and Cryptography* **48**(2008), 1–16.

[10] C. Carlet, $\mathbb{Z}_{2^k}$-linear codes, *IEEE Transactions on Information Theory* **IT-44** (1998), no. 4, 1543–1547.

[11] W.E. Clark, D.A. Drake, Finite chain rings, *Abhandlungen aus dem mathematischen Seminar der Universität Hamburg* **39** (1974), 147–153.

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

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

[14] S. Dodunekov, J. Simonis, Codes and projective multisets, *Electronic Journal of Combinatorics* **5** (1998), no. #R37.

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

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

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

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

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

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

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

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

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

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

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

[26] 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.

[27] W. Heise, P. Quattrocchi, Informations- und Codierungstheorie, Springer Verlag, Berlin, 3rd Edition, 1995.

[28] L. Hemme, T. Honold, I. Landjev, Arcs in projective Hjelmslev spaces obtained from Teichmüller sets, in: Proc. Seventh Int. Workshop on ACCT (ACCT-7), Bansko, 2000, 177–182.

[29] J.W.P.Hirschfeld, Projective Geometries over Finite Fields, Clarendon Press, Oxford, 1979; Second edition: Oxford University Press, 1998.

[30] J.W.P. Hirschfeld, Finite projective spaces of three dimensions, Oxford Univ. Press, 1985.

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

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

[33] 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.

[34] T. Honold, M. Kiermaier, Classification of maximal arcs in small projective Hjelmslev geometries,in: Proc. Tenth Int. Workshop on ACCT (ACCT-10), Zvenigorod, 2006, 112–117.

[35] T. Honold, I. Landjev, Projective Hjelmslev geometries, Optimal Codes and Related Topics (Sozopol, Bulgaria), 1998, pp. 97–115.

[36] T. Honold, I. Landjev, Linear codes over finite chain rings, Optimal Codes and Related Topics (Sozopol, Bulgaria), 1998, pp. 116-126.

[37] T. Honold, I. Landjev, Linearly representable codes over chain rings, Algebraic and Combinatorial Coding Theory (ACCT-6) (Pskov, Russia), 1998, pp. 135–141.

[38] 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.

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

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

[41] T. Honold, I. Landjev, On arcs in projective Hjelmslev planes, *Discrete Mathematics*, textbf231(2001), 265–278.

[42] T. Honold, I. Landjev, Arcs in projective Hjelmslev planes, *Discrete Math. and Appl.* **11**(2001), 265–278.

[43] T. Honold, I. Landjev, On maximal arcs in projective Hjelmslev planes, *Finite Fields and Their Applications* **11**(2005), 292–304.

[44] T. Honold, I. Landjev, Caps in projective Hjelmslev spaces over finite chain rings of nilpotency index 2, *Innovations in Incidence geometry* **4**(2006), 13–25.

[45] T. Honold, I. Landjev, Linear codes over finite chain rings and projective Hjelmslev geoemtries, in: Codes over Rings (ed. P. Solé), World Scientific, 2009, 60–123.

[46] T. Honold, I. Landjev, Codes over Rings and Ring Geometries, in: Current Research Topics in Galois Geometry (eds. L. Storme, J. De Beule), NOVA Science Publishers, 2012, 161–187.

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

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

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

[50] M. Kiermaier, Arcs und Codes über endlichen Kettenringen, Diplomarbeit, Technische Universität München, April 2006.

[51] M. Kiermaier, A. Kohnert, New arcs in projective Hjelmslev planes over Galois rings, In : *Optimal Codes and Related Topics*, Proc. Int. Conf. on Optimal Codes and Related Topics, White Lagoon, 2007, 112-119.

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

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

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

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

[56] 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.

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

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

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

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

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

[62] T. Y. Lam, Lectures on Modules and Rings, GTM, Springer, 1991, 2001.

[63] T. Y. Lam, A First Course in Non-Commutative Rings, GTM, Springer, 1999.

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

[65] S. Lang, Algebra, 2nd ed., Addison-Wesley Publishing Company, 1984.

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

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

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

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

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

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

[72] 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.

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

[74] 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.

[75] 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.

[76] G. Norton, On minimal realization over a finite chain ring, *Designs, Codes and Cryptography* **16**(1999), 161–178.

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

[78] R. Raghavendran, Finite associative rings, *Compositio Mathematica* **21**(1969), 195–229.

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

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

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

[82] 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.

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

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

[85] 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.