Софийски Университет "Св. Климент Охридски"

Факултет по Математика и Информатика

Tedis Ramaj

Алгебрични методи за изучаване на някои комбинаторни конфигурации и техните приложения

Автореферат

на дисертация

за присъждане на образователна и научна степен

" ДОКТОР "

по Професионално направление 4.5. Математика

Докторска програма " Алгебра, топология и приложения "

Научни ръководители:

доц. д-р Силвия Първанова Бумова

доц. д-р Мая Митева Стоянова

София, 2021

Дисертацията съдържа 88 страници и се състои от увод три глави и използвана литература с 45 заглавия.

Номерацията на дефинициите, теоремите и следствията в автореферата съответства точно на номерацията им в дисертационния труд.

През 1940 г. Рао въвежда комбинаторни стуктури, наречени ортогонални масиви. Те играят важна роля в статистиката (използвана при проектирането на експерименти), компютърните науки и криптографията. Ортогоналните масиви са свързани с комбинаториката, крайните полета, геометрията и кодовете за изправяне (коригиране) на грешки. Въпреки че в тази област е направено много, все още има много нерешени проблеми. [17]

Дефиниция 0.0.1. *(**Дефиниция 1.1.1**) Нека $\mathcal{A}$ е азбука с q символи.* ***Ортогонален масив*** $OA(M, n, q, t)$ ***от сила*** t ***с*** M ***реда,*** n ***стълба*** $(n \geq t)$***, и*** q ***нива*** *е $M \times n$ матрица с елементи от $\mathcal{A}$ такава, че всяка подматрица $M \times t$ съдържа всички възможни q^t, t-орки еднакъв брой пъти (да кажем λ пъти).*

Очевидно $M = \lambda q^t$ и ортогоналния масив със сила t е също и със сила t', за стойности $t' < t$. Числото λ се нарича ***индекс*** на ортогоналния масив.

Често се използва означението $OA(M, n, q, t)$, както и $OA(M, q^n, t)$ или $t - (q, n, \lambda)$.

Ето пример за $OA(4, 3, 2, 2)$:

$$\begin{matrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{matrix}$$

Корените на ортогоналните масиви са в експериментална статистика. C. R. Rao ([30, 31, 32]) ги въвежда за използване във fractional factorial experiments. След въвеждането им много изследователи, идващи от различни научни области, започват да допринасят по темата. Разнообразието от техния произход е довело до използването на различни термини за едни и същи понятия. Ето най-използваните термини за основните параметри на $OA(M, n, q, t)$:

$\mathcal{A}^n$**:** пълен факториален дизайн;

$OA(M, n, q, t)$**:** фрационален факториален дизайн;

M**:** брой реда, брой експерименти;

n**:** брой стълба, фактори;

q**:** брой нива или символи;

t**:** сила;

λ**:** индекс; index;

По принцип $OA(M, n, q, t)$ е мулти-подмножество от $\mathcal{A}^n$, т.е. може да има повтарящи се редове, но всичките му различни редове образуват подмножество от $\mathcal{A}^n$. Ортогонален масив без повтарящи се редове се нарича ***прост***.

Например $t-(q, t, \lambda)$, т.е. $OA(\lambda q^t, t, q, t)$ е тривиален пример за ортогонален масив: всеки елемент от $\mathcal{A}^t$ се повтаря λ пъти.

Обикновено $\mathcal{A} = \mathbb{Z}_q$, адитивната група от цели числа по модул q или крайното поле $GF(q)$, когато q е степен на просто число. Използването на крайното поле $GF(q)$ като азбука позволява да се извлекат резултати от теорията на кодирането за решаване на проблеми, свързани с ортогонални масиви. Но има изследователи, които разглеждат ортогонални масиви над $\mathbb{C}_q$, мултипликативната група от q -корени на единицата в $\mathbb{C}$ ($\mathbb{Z}_q \cong \mathbb{C}_q$) или други специфични азбуки.

Понятието ортогонален масив може да бъде обобщено до така наречения **em смесен ортогонален масив**. Нека $\mathcal{A}_1, \mathcal{A}_2,\ ldots, \mathcal{A}_n$ е набор от азбуки с мощност $q_1, q_2, \ldots, q_n$, съответно. Смесеният ортогонален масив се дефинира като мулти-подмножество $\mathcal{A}_1 \times \mathcal{A}_2 \times \cdots \times \mathcal{A}_n$, удовлетворяващо свойствата, дадени в Определение 1.1.1.

Някои приложения на ортогоналните масиви в медицината са в:

- **фармацевтични компании**. Въз основа на ортогонални масиви те провеждат проучвания за стабилността и срока на годност на лекарствата, което включва много различни фактори.
- **множествена (многократна) лекарствена терапия**. Ортогоналните масиви могат да помогнат на лекарите да регулират нивата на дозата, за да се избегнат или минимизират взаимодействията при използване на множество лекарства.
- **клинични изпитвания**, за да се изследва как лекарствата се абсорбират, разпределят, метаболизират и ограничават от организма, особено за да се изследват ефектите на множество фактори върху тези лекарствени характеристики.

В експериментите се изследва съвместното въздействие на няколко фактора върху свойствата на даден продукт или процес. И обикновено те се провеждат според ортогонален масив. Използваната терминология е следната: всяка колона съответства на фактор n, символите са нивата на фактора q и всеки ред представлява комбинация от нива на фактора, наречени "runs" (изпълнения).

Броят на редовете M (който представлява броя на изпълненията в експеримента и може да изисква твърде много ресурси) трябва да бъде намален. Това ни води до следните проблеми:

1. за намиране на възможно най-малкия брой редове на ортогонален масив;
2. за даден брой изпълнения, за да се знае най-големият брой колони, които могат да се използват в ортогонален масив.

Или по-общо това са проблеми на

⋆ **Съществуване:** за кои стойности на броя редове, колони, сила и нива съществува ортогонален масив?

⋆ **Конструкция:** как можем да изградим масив, ако такъв съществува.

⋆ **Неизоморфни класове:** намерете броя на неизоморфните ортогонални масиви за дадени параметри.

По-нататък продължаваме с по-подробно описание на резултатите в главите. Дефиниции, понятия и теореми са въведени, за да опишат резултатите, получени в докторската дисертация. Дадени са и съответните им номера в дисертационния труд.

В Глава 1 даваме някои обозначения и свойства на ортогоналните масиви.

Proposition 0.0.2. *(**Твърдение 1.2.1, [17]**) За $OA(M, n, q, t)$ са в сила следните свойства*

(i) $\lambda = \frac{M}{q^t}$

(ii) Пермутация на символите (нива q) на всеки фактор (стълб n) в $OA(M, n, q, t)$ води до ортогонален масив със същите параметри.

(iii) Пермутацията на редовете (изпълнения) или факторите (стълбовете n) в $OA(M, n, q, t)$ води до ортогонален масив със същите параметри.

(iv) Всеки $M \times k$ подмасив на $OA(M, n, q, t)$ е $OA(M, k, q, t')$, където $t' = \min\{t, k\}$.

(v) Ако $A = \begin{bmatrix} A_1 \\ A_2 \end{bmatrix}$ е $OA(M, n, q, t)$, където A_1 е $OA(M_1, n, q, t_1)$, тогава A_2 е $OA(M - M_1,\, n,\, q,\, t_2)$ като $t_2 \geq \min\{t, t_1\}$.

Определенията за кодове и връзките им с ортогонални масиви са дадени в раздел 1.3.

Специално внимание е обърнато на полиномите на Krawtchouk, които са въведени през 1929 г. от украинския математик Krawtchouk като обобщение на полиномите на Хермит (Hermite). Те играят важна роля в теорията на кодирането и също са полезни в теорията на графовете и теорията на числата (вижте например [22, 15], [19], [41] и [25]) .

Нека евклидовото пространство E е линейно пространство над полето на реалните числа $\mathbb{R}$, снабдено с обичайното скаларно произведение.

Нека $E \subset \mathbb{R}[x]$ е линейното пространство на полиноми със степен ненадминаваща n. Билинейното изображение, дефинирано от

$$\langle f, g\rangle \stackrel{def}{=} \sum_{i=0}^{n} k_i f(x_i) g(x_i), \quad k_i \geq 0,$$

където $(x_0, x_1, \ldots, x_n) \in \mathbb{R}^{n+1}$ са фиксирана $(n+1)$ -орка от различни реални числа, наречени ***апроксимацинните точки (approximation points)***, удовлетворява аксиомите за скаларно произведение. ***Тегловият вектор*** $(k_0, k_1, \ldots, k_n)$ е избран така, че да удовлетворява условието $\sum_{i=0}^{n} k_i = 1$, за да се гарантира, че нормата е 1.

Нека $q \geq 2$ е цяло число, $(0, 1, \ldots, n)$ са апроксимацинните точки и

$$\langle f, g\rangle \stackrel{def}{=} \frac{1}{q^n} \sum_{i=0}^{n} \binom{n}{i} (q-1)^i f(i) g(i). \tag{1}$$

Тегловият вектор е

$$\frac{1}{q^n}\left(1, \ \binom{n}{1}(q-1), \ \ldots, \ \binom{n}{n}(q-1)^n\right)$$

и удовлетворява

$$\sum_{i=0}^{n} \binom{n}{i} \frac{(q-1)^i}{q^n} = 1.$$

Дефиниция 0.0.3. *(**Дефиниция 1.4.1**) **Полином на Кравчук** е полином, дефиниран по следния начин*

$$K_k(x;\, n, q) = \sum_{j=0}^{k} (-1)^j \binom{x}{j} \binom{n-x}{k-j} (q-1)^{k-j}, \quad k = 0, 1 \ldots n.$$

Параметрите n и q са вече фиксирани или техните стойности са известни от

контекста. Затова често пропускаме n и q и пишем само $K_k(x)$.

Полиномът на Кравчук $K_k(x;\, n, q)$ е полином на степен k на променливата x със старши коефициент $(-q)^k/k!$. Ето първите три полинома:

$$
\begin{aligned}
&K_0(x) = 1;\\
&K_1(x) = -qx + n(q-1);\\
&K_2(x) = \frac{1}{2}\Big[q^2x^2 - \big((2n-1)(q-1)+1\big)x + n(n-1)(q-1)^2\Big].
\end{aligned}
$$

Производящата функция на полиномите на Кравчук е

$$\sum_{k=0}^{n} K_k(x;\, n, q) z^k = \Big(1 + (q-1)z\Big)^{n-x} (1-z)^x. \tag{2}$$

Proposition 0.0.4. *(**Твърдение 1.4.2**)Полиномите на Кравчик удовлетворяват съотношенията (the relations???)*

$$(q-1)^i \binom{n}{i} K_k(i) = (q-1)^k \binom{n}{k} K_i(k). \tag{3}$$

Lemma 0.0.5. *(**Лема 1.4.3**) Полиномите на Кравчук $K_0(x), K_1(x), \ldots, K_n(x)$ образуват ортогонална система относно скаларното произведение (1), а именно*

$$\langle K_k, K_l \rangle = \frac{1}{q^n} \sum_{i=0}^{n} \binom{n}{i} (q-1)^i K_k(i) K_l(i) = \binom{n}{k} (q-1)^k \, \delta_{kl} \tag{4}$$

за $k, l = 0, 1, \ldots, n$, където δ_{kl} е символа на Кронекер.

Второто съотношение за ортогоналност е както следва.

Corollary 0.0.6. *(**Следствие 1.5**)*

$$\sum_{i=0}^{n} K_k(i) K_i(l) = q^n \delta_{kl} \tag{5}$$

Theorem 0.0.7. *(**Теорема 1.4.5**) За всеки полином $f(x) \in \mathbb{R}[x]$ от степен $\leq n$ съществува единствено развитие (представяне) по полиномите на Кравчук*

$$f(x) = \sum_{k=0}^{n} f_k K_k(x), \qquad \textit{where}$$

$$f_k = \frac{1}{q^n \binom{n}{k}(q-1)^k} \sum_{i=0}^{n} \binom{n}{i}(q-1)^i f(i) K_k(i) = \frac{1}{q^n} \sum_{i=0}^{n} f(i) K_i(k).$$

Ортогоналните полиноми имат много интересни свойства (вижте [41]). Следващата теорема дава някои от тях.

Theorem 0.0.8. *(**Теорема 1.4.10**) В сила са следните равенства???*

(i) $K_k(x;\, n) = (q-1)K_{k-1}(x;\, n-1) + K_k(x;\, n-1)$;

(ii) $(q-1)K_k(x;\, n) + K_k(x-1;\, n) = qK_k(x-1;\, n-1)$;

(iii) $\sum_{k=0}^{n} \binom{n-k}{n-j} K_k(x) = q^j \binom{n-x}{j}$;

(iv) $\sum_{k=0}^{m} K_k(x; n) = K_m(x-1; n-1)$.

Използвайки привлекателните и красиви свойства на адитивните характери (раздел 1.4.4), можем да докажем теореми, които да помогнат при нашите изследвания в областта на ортогоналните масиви.

Дефиниция 0.0.9. *(**Дефиниция 1.5.1**) Нека C е $OA(M, n, q, t)$ (или подмножество на $\mathcal{A}^n$) и $\mathbf{x} \in \mathcal{A}^n$ е фиксиран вектор. Множеството от цели числа $\mathbf{p}(\mathbf{x}) = (p_0, p_1, \ldots, p_n)$, дефинирано чрез*

$$p_i = |\{\mathbf{u} \in C \mid d(\mathbf{x}, \mathbf{u}) = i\}|$$

*се нарича **разпределение на разстоянията на C относно $\mathbf{x}$**.*

Лемата по-долу е доказана от Delsart ([14, 13])

Lemma 0.0.10. *(**Лема 1.5.2, Делсарт[14, 13]**) Нека C е $OA(M, n, q, t)$ и $\mathbf{x} \in \mathcal{A}^n(\mathbb{F}_q^n)$. Ако $\mathbf{p}(\mathbf{x}) = (p_0, p_1, \ldots, p_n)$ е разпределение на разстоянията на C относно $\mathbf{x}$, то*

$$\sum_{i=0}^{n} p_i K_k(i) = 0 \qquad \text{for } k = 1, \ldots, t. \tag{6}$$

Theorem 0.0.11. *(**Теорема 1.5.3**) Нека C ее $OA(M, n, q, t)$ и $\mathbf{v} \in \mathbb{F}_q^n$. Ако $\mathbf{p}(\mathbf{v}) = (p_0, p_1, \ldots, p_n)$ е разпределение на разстоянията на C относно $\mathbf{v}$, тогава за всеки полином $f(x)$ от степен $\deg f \le t$ е в сила*

(a)

$$\sum_{i=0}^{n} p_i f(i) = f_0 M, \qquad f_0 = \frac{1}{q^n} \sum_{i=0}^{n} f(i) K_i(0) = \frac{1}{q^n} \sum_{i=0}^{n} \binom{n}{i}(q-1)^i f(i) \tag{7}$$

където $f(x) = f_0 + \sum_{j=1}^{t} f_j K_j(x)$.

(b)

$$\sum_{i=0}^{n} p_i f(t_i) = a_0 M, \qquad a_0 = \frac{1}{q^n}\sum_{i=0}^{n}\binom{n}{i}(q-1)^i f(t_i) = \frac{1}{q^n}\sum_{i=0}^{n} K_i(0) f(t_i) \quad (8)$$

където $f(x) = a_0 + \sum_{j=1}^{t} a_j Q_j(x)$ *и* $t_i = 1 - \frac{2i}{n}$.

В Глава 2 са използвани полиномни и комбинаторни техники [13, 23, 17], за да се изчислят всички възможни разпределения на разстоянията на тройчнини ($q = 3$) ортогонални масиви със съответно малки дължини и сила. Предлагаме метод за изчисляване и намаляване на възможностите за разпределения на разстоянията на дадени ортогонални масиви. Използваме свойства на ортогонални масиви (с дадени параметри) и някои връзки с техните производни ортогонални масиви, за да намалим възможните разпределения на разстоянието. За да се решат въпроси относно съществуването и класификацията, е важно да се знаят възможните разпределения на разстояние на ортогонален масив по отношение на която и да е точка. Разполагайки с тази информация, можем да получим знания за нейната структура.

Подобряваме познатите методи [7, 8, 2] за изчисляване и намаляване на възможностите за разпределение на разстоянието на ортогонални масиви. След това приламе новите условия, които ортогоналните масиви трябва да изпълняват. Ако не, тогава получаваме резултат от несъществуване, и пример за това е $OA(108, 16, 3, 3)$ и потвърждаваме резултата за несъществуване за $OA(108, 17, 3, 3)$ ([2]).

Нека C е $OA(M, n, q, t)$ и $\mathbf{x} \in \mathcal{A}^n$ е фиксиран вектор. Множеството от цели положителни числа $\mathbf{p}(\mathbf{x}) = (p_0, p_1, \ldots, p_n)$, определено чрез

$$p_i = |\{\mathbf{u} \in C \mid \mathrm{d}(\mathbf{x}, \mathbf{u}) = i\}|$$

се нарича **разпределение на разстоянието на** C **относно** $\mathbf{x}$.

Бойваленков и съавтори ([7, 8, 3]) посочват, че в общия случай всички възможни разпределения на разстояния могат да бъдат изчислени като неотрицателни целочислени решения на определена система от линейни уравнения с матрица на Вандермонд (t_j^i) , където $t_j = 1 - \frac{2j}{n}, j = 0, \ldots, n$.

Наскоро резултатите на Босе и Буш ([1]) бяха доказани от Манев ([26]) по различен начин. Резултатите на Манев са обобщени в теорема 2.1.2. Тази теорема може да улесни бързото изчисляване на разпределенията на разстоянието.

Theorem 0.0.12 (**Теорема 2.1.2, [26]**). *Нека* C *е* $OA(M, n, q, t)$ *и* $\mathbf{v} \in \mathcal{A}^n$. *Ако* $\mathbf{p}(\mathbf{v}) = (p_0, p_1, \ldots, p_n)$ *е разпределение на разстоянията на* C *относно* $\mathbf{v}$,

тогава за $m = 0, 1, \ldots, t$ *и* $s = 1, \ldots, t+1$, $\mathbf{p}(\mathbf{v})$ *удовелтворява следните системи:*

(i)

$$\sum_{i=0}^{n} \binom{n-i}{m} p_i = \frac{M}{q^m} \binom{n}{m} = \lambda q^{t-m} \binom{n}{m};$$

(ii)

$$\sum_{i=0}^{n} p_i i^m = \frac{M}{q^n} \sum_{i=0}^{n} \binom{n}{i} i^m (q-1)^i;$$

(iii)

$$\sum_{i=0}^{n} p_i (n-i)^m = \frac{M}{q^n} \sum_{i=0}^{n} \binom{n}{i} (n-i)^m (q-1)^i;$$

(iv)

$$\sum_{i=0}^{n} \binom{i-s}{m} p_i = \frac{M}{q^n} \sum_{i=0}^{n} \binom{n}{i} \binom{i-s}{m} (q-1)^i.$$

Тези системи (Теорема 2.1.2 (i), (ii), (iii), (iv)) показват, че $(p_0, p_1, ..., p_n)$ е решение на еквавалентни линейни системи с неотрицателни целочислени коефициенти. За да се намерят разпределенията на разстоянията трябва да се намерят всичките им неотрицателни целочислени решения, тоест да избере неотрицателното измежду всички целочислени решения.

В раздел 2.2 представяме алгоритъм за определяне на възможни вектори $\mathbf{p}$. Оказва се, че намирането на възможно най-добрия вектор на горната граница u за векторите p е много важно. Това увеличава ефективността на изчисленията.

Разглеждаме система (iv) на Теорема 2.1.2 подробно.

$$A_s p^\tau = a, \tag{9}$$

където

$$A_s = (a_{kl}) = \left(\binom{l-s}{k} \right)$$

е $(t+1) \times (n+1)$ матрица. Векторът $a = (a_0, a_1, \ldots, a_t)^\tau$, е определен от

$$a_k = \frac{M}{q^n} \sum_{i=0}^{n} \binom{n}{i} \binom{i-s}{k} (q-1)^i,$$

където $k = 0, \ldots, t$. ???Стълбовете на A съответно на $l = s, \ldots, s+t$ образуват $(t+1) \times (t+1)$ матрица $R_t = (r_{ij}) = (\binom{j}{i})$. Умножавайки системата (9) с R_t^{-1}

получаваме $Bp^\tau = b$, където $B = R_t^{-1}A = (b_{ml})$ и $b = (b_0, \ldots, b_t)^\tau$, т.е.

$$b_{ml} = (-1)^m \sum_{j=0}^{t} (-1)^j \binom{j}{m} \binom{l-s}{j}, \quad m = 0, 1, \ldots, t,\ l = 0, 1, \ldots, n$$

и

$$b_m = (-1)^m \lambda q^{t-n} \sum_{i=0}^{n} \left(\binom{n}{i} (q-1)^i \sum_{j=0}^{t} \binom{j}{m} \binom{i-s}{j} \right), \quad m = 0, 1, \ldots, t.$$

В следващата теорема получихме преобразуваната матрица в аналитичен вид. Това много помага при изчисленията.

Theorem 0.0.13. *(**Теорема 2.3.1**) В сила е:*

(a) $b_{ml} = (-1)^{2m} \binom{l-s}{m} \binom{t-l-s}{t-m} = \binom{l-s}{m} \binom{t-l-s}{t-m}$;

(b) $$b_{ml} = \begin{cases} (-1)^{m+t} \dfrac{l-s-t}{l-s-m} \binom{t}{m} \binom{l-s}{t}, & l \neq s+m \\ 1, & l = s+m \end{cases}$$

Оказва се, че b_m няма добро изразяване като цяло, само в специални случаи. След опростяване (подробно описано в глава 2) получаваме

$$b_m = (-1)^m \lambda q^{t-n} \sum_{i=0}^{n} \binom{n}{i} (q-1)^i (-1)^m \binom{i-s}{m} \binom{t+s-i}{t-m}$$

или еквивалентно

$$b_m = (-1)^{m+t} \lambda q^{t-n} \binom{t}{m} \sum_{i=0}^{n} \binom{n}{i} \binom{i-s}{t} \frac{i-s-t}{i-s-m} (q-1)^i,$$

където $m = 0, 1, \ldots, t$.

Някои граници могат да бъдат намерени, когато силата t е четно число. Ситуацията, когато t е нечетно число, е по-сложна.

Corollary 0.0.14. *(**Следствие 2.3.3**) За t четно число е изпълнено неравенството:*

$$p_l \leq \left\lfloor \frac{b_m}{b_{ml}} \right\rfloor,\ \textit{for } l = 0, 1, ..s-1, s+t+1, \ldots, n$$

В раздел 2.4. ние изучаваме ортогонални масиви, прилагайки знанията за възможни разпределения на разстояние и извличаме информация за неговата структура.

Нека C е $OA(M,n,q,t)$ и можем да приемем, че C съдържа нулевия вектора. Нека C' е ортогоналният масив, получен от C чрез изтриване на първия стълб. Обозначаваме с $C_i,\ i=0,1,\ldots,q-1$ множеството, получено чрез вземане на всички редове на C с i -тия елемент на $\mathcal{A}$ в първия стълб и след това изтриваме първия стълб. (C_0 съответства на 0 в първия стълб.) Съгласно Твърдение 1.2.1

$$C' \text{ is } OA(M,n-1,q,t) \qquad \text{and} \qquad C_i \text{ is } OA(M/q,n-1,q,t-1).$$

Изчисляваме всички възможни разпределения на разстоянията на C', C_i, C използвайки описания алгоритъм и за всички други необходими ортогонални масиви, получени от C.

Нека $\mathbf{c}=(c_1,c_2,\ldots,c_n)\in C$, т.е., $\mathbf{c}_0=(c_2,\ldots,c_n)\in C_0$ or C_i. Разпределение на разстоянието на C относно $\mathbf{c}$ е $\mathbf{p}(\mathbf{c})=(p_0,p_1,\ldots,p_n)$ и $\mathbf{p}^0(\mathbf{c}_0)=(p_0^0,p_1^0,\ldots,p_{n-1}^0)$ на C_0 (или C_i) относно $\mathbf{c}_0$, съответно.

Вектор $\mathbf{a}=(a_1,a_2,\ldots,a_n)$ ***доминира*** друг вектор $\mathbf{b}=(b_1,b_2,\ldots,b_n)$ ако $a_i\geq b_i$ за всички $i=1,\ldots,n$.

Corollary 0.0.15. *(**Следствие 2.4.1**) Ако векторът $p=(p_0,p_1,\ldots,p_n)$ е разпределение на разстоянията на ортогонален масив $OA(M,n,q,t)$ - C, тогава удовлетворява следните условия*

(i) $(p_0,p_1,\ldots,p_{n-1})$ *доминира* $(p_0^0,p_1^0,\ldots,p_{n-1}^0)$, *когато* $p_0^0\geq 1$;

(ii) $(p_1,p_2,\ldots,p_n)$ *доминира* $(p_0^0,p_1^0,\ldots,p_{n-1}^0)$ *когато* $p_0^0=0$;

(iii) *разликата*

$$\overline{p}(c_0)=(\bar{p}_0,\bar{p}_1,\ldots,\bar{p}_{n-1})=(p_1-p_1^0,\ldots,p_{n-1}-p_{n-1}^0,p_n)$$

има разпределение на разстоянията на $C_1\cup\cdots\cup C_{q-1}$ относно външна точка c_0;

(iv) $\overset{\text{v}}{p}(c_0)=\overline{p}(c_0)+p^0(c_0)$ *е разпределение на разстоянията на* $\overset{\text{v}}{C}$ *относно c_0.*

Изтривайки различни стълбове, можем да получим не само различни C_i, но различни стойности за bp, $overline\ bp(\ bc)$, bp^0. Следният резултат е валиден

Theorem 0.0.16. *(**Теорема 2.4.2 [[7, 26]]**) Нека $\overline{p}^{(1)},\overline{p}^{(2)},\ldots,\overline{p}^{(s)}$ са всички възможни наследници на p и нека $\overline{p}^{(i)}$ да бъде получено в k_i случаи на изтриване*

на стълб, $i = 1, 2, \ldots, s$. *Тогава целите числа* k_i *удовлетворяват*

$$\begin{cases} k_1 + k_2 + \cdots + k_s = n \\ k_1\overline{p}^{(1)} + k_2\overline{p}^{(2)} + \cdots + k_s\overline{p}^{(s)} = (p_1, 2p_2, \ldots, np_n) \\ k_i \geq 0 \end{cases}$$

В раздел 2.5 доказваме, че

Theorem 0.0.17. *(**Теорема 2.5.1**) Минималният индекс на тройчен ортогонален масив със сила* $t = 3$ *и брой фактори 17 и 16 е* $\lambda = 5$.

Някои резултати, даващи ограничения върху структурата са показани в раздел 2.5.1.

textbf Забележка: Всички изчисления са направени на Maple.

В Глава 3 разглеждаме друга връзка между кодовете и ортогоналните масиви, т.е. **радиус на покритие** ([5]). Радиусът на покритие на ортогонален масив C е минимумът от числата ρ, така че всяка точка от пространството на Хаминг $H(n, q)$ е на разстояние ρ от поне една точка в C; тоест, това е най-малкият радиус, такъв, че описаните сферите с този радиус и центрове точките на C, имат всички точки от $H(n, q)$ като обединение.

Получаваме аналитични горни граници за радиус на покритие на даден ортогонален масив в зависимост от неговите параметри. Правим това чрез изследване на множеството от всички възможни разпределения на разстоянието от съответния ортогонален масив и свързани с него ортогонални масиви.

За да докажем нашите граници за радиус на покриване, избираме да работим с $s = n - t$. Това улеснява ситуацията, т.е.

$$Bp^\tau = b, \text{ and } B = (UI_{t+1}) = (b_{ml}),$$

където $b = (b_m),\ m = 0, 1, \ldots, t,\ l = 0, 1, \ldots, n.$

Коефициентите b_0 и b_1 могат да бъдат изразени.

Corollary 0.0.18. *(**Следствие 3.2.1**) За дадени параметри* M, n, q, t, $s = n - t$, *и* $\lambda = M/q^t$ *е в сила:*

(i) $b_0 = \lambda\binom{n}{t}$;

(ii) $b_1 = -\lambda\binom{n}{t-1}(n - t - q + 1)$.

Следващата теорема дава граници на радиус на покритие за даден ортогонален масив.

Разпределение на разстоянията с максимален брой нули в началото	$\rho(C)$	Теореми 3.2.2, 3.2.3
$OA(54, 5, 3, 3)$ $(0, 0, 20, 0, 30, 4)$ **страницата на Sloane** [40]	2	$\rho(C)$ $\leq 5 - 3 = 2$ $n - t = q - 1$
$OA(18, 7, 3, 2)$ $(0, 0, 0, 0, 14, 0, 0, 4)$ **Evangelaras, Koukouvinos, Lappas** [16] **Schoen, Eendebak, Nguyen**[34]	4	$\rho(C)$ $\leq 7 - 2 - 1 = 4$ $n - t > q - 1$

Таблица 1: Примери за радиус на покритие на ортогонални масиви, които достигат границите от Теоремите 3.2.2, 3.2.3.

Theorem 0.0.19. *(**Теорема 3.2.2**) Нека C е $OA(M, n, q, t)$, имащ радиус на покритие $\rho(C)$. Тогава*

$$\rho(C) \leq n - t.$$

Единствеността на решението в доказателството на теорема 3.2.2 позволява да направим допълнителни подобрения.

Theorem 0.0.20. *(**Теорема 3.2.3**) Нека C е $OA(M, n, q, t)$, имащ радиус на покритие $\rho(C)$. Ако $n - t > q - 1$, то*

$$\rho(C) \leq n - t - 1.$$

Използвайки процедура за намаляване на възможните разпределения на разстояние от ортогонален масив, ние подобряваме границата с 1 при определени предположения.

Theorem 0.0.21. *(**Теорема 3.2.3**) Нека C е $OA(M, n, q, t)$ с радиус на покритие $\rho(C)$. Ако $n > 2(t + q - 1)$, то*

$$\rho(C) \leq n - t - 2.$$

Посочени са някои примери, които достигат границите.

Разпределение на разстоянията с максимален брой нули в началото, страницата на Sloane [40]	$\rho(C)$	Теорема 3.3.1
$OA(27, 13, 3, 2)$ $[0, 0, 0, 0, 0, 0, 0, 13, 0, 0, 13, 0, 0, 1]$	7	$\rho(C)$ $\leq 13 - 2 - 2 = 9$
$OA(36, 13, 3, 2)$ $[0, 0, 0, 0, 0, 0, 0, 10, 14, 0, 6, 4, 0, 2]$	7	$\rho(C)$ $\leq 13 - 2 - 2 = 9$
$OA(729, 14, 3, 4)$ $[0, 0, 0, 0, 0, 14, 42, 42, 133, 126, 210, 70, 84, 0, 8]$	5	$\rho(C)$ $\leq 14 - 4 - 2 = 8$

Таблица 2: Примери за радиус на покритие на ортогонални масиви

Благодарности

Бих искал да изкажа своята благодарност на моите ръководители доц. д-р Силвия Бумова и доц. д-р Мая Стоянова за техните ценни съвети, насоки и помощ.

Бих искал да благодаря на всички колеги от Катедрата по алгебра на Факултет по математика и информатика, СУ "Св. Климент Охридски" за приятната и стимулираща атмосфера по време на подготовката на дисертацията.

Научни приноси

По преценка на автора основните приноси на дисертационния труд са следните

1. Разработен е комбинаторен метод за изчисляване и намаляване на възможностите за разпределение на разстоянията на тройчен ортогонален масив от зададени параметри $OA(M, n, q, t)$.

2. Получаваме аналитичен израз на матрицата от (теорема 2.3.1), използвана за оценка на разпределение на разстоянията на даден ортогонален масив. Това помага много за по-бързо изчисляване на разпределенията на разстоянията.

3. Основен резултат е несъществуването на $OA(108, 18, 3, 3)$ и $(108, 17, 3, 3)$ тройчни ортогонални масиви. Резултатът от несъществуването на $OA(108, 18, 3, 3)$ вече е получен от М. Стоянова и Т. Маринова, но го получихме независимо, използвайки друг подход. Заедно написахме статия [2].

4. Получаваме аналитично горни граници за радиус на покритие на ортогонални масиви.

5. Прилагаме процедура за намаляване на възможните разпределения на разстояния на ортогонален масив, за да подобрим границата за радиус на покритие с едно, при определени предположения.

Апробация на резултатите

Резултатите, описани в дисертацията, са публикувани в следващите статии.

1. ([6]) **S. Boumova, T. Ramaj, M. Stoyanova**, *Computing distance distributions of ternary orthogonal arrays. Comptes rendus de l'Académie bulgare des Sciences, 2020, ISSN (print):1310–1331 , ISSN (online):2367–5535, to appear.* (*SJR (Scopus):0.218, JCR-IF (Web of Science):0.343*).

2. ([2]) **S. Boumova, T. Marinova, T. Ramaj, M. Stoyanova**, Nonexistence of (17, 108, 3) ternary orthogonal array, *Annual of Sofia University "St. Kliment Ohridski", Faculty of Mathematics and Informatics, vol:106, 2019, pages:117-126, ISSN (print):1313-9215, ISSN (online):2603-5529, Ref, MathSciNet.*

3. ([5]) **S. Boumova, T. Ramaj, M. Stoyanova**, On Covering Radius of Orthogonal Arrays, *Proceedings of Seventeenth International Workshop on Algebraic and Combinatorial Coding Theory ACCT 2020, October 11-17, 2020, Bulgaria* (accsepted in IEEE Xplore),

Всички статии са в съавторство със С. Бумова и М. Стоянова. Единият от тях е в съавторство на С. Бумова, М. Стоянова и Т. Маринова.

Резултатите са представени на международни и национални конференции и форуми, както следва

Conference talks

1. ([5]) **S. Boumova, T. Ramaj, M. Stoyanova**, On Covering Radius of Orthogonal Arrays, *Proceedings of Seventeenth International Workshop on Algebraic and Combinatorial Coding Theory, October 11-17, 2020, Bulgaria (online).*

2. **S. Boumova, P. Boyvalenkov, T. Ramaj, M. Stoyanova**, Some bounds for Covering Radius of Orthogonal Arrays, *Annual Workshop on Coding Theory "Prof. Stefan Dodunekov October 8-11, 2020, Bulgaria (online).*

3. ([4]) **S. Boumova, P. Boyvalenkov, T. Ramaj, M. Stoyanova**, Computing distance distributions of ternary orthogonal arrays, *The 14th Annual Meeting of the Bulgarian Section of SIAM, 2019, December 17-19, Bulgaria.*

4. **S. Boumova, T. Ramaj, M. Stoyanova**, Distance distributions of ternary orthogonal arrays, *Spring Science Session FMI, 2019.*

5. **S. Boumova, T. Ramaj, M. Stoyanova**, Computing distance distributions of ternary orthogonal arrays, *Annual Workshop on Coding Theory "Prof. Stefan Dodunekov November 21-24, 2019, Troyan, Bulgaria.*

6. **S. Boumova, T. Ramaj, M. Stoyanova**, Orthogonal Arrays and Related Objects I, *Annual Workshop on Coding Theory "Prof. Stefan Dodunekov November 8-11, 2018, Veliko Turnovo, Bulgaria.*

Декларация за оригиналност на резултатите

Декларирам, че настоящият дисертационен труд съдържа оригинални резултати, получени при проведени от мен научни изследвания, с подкрепата на научите ми ръководители и съавтори. Резултатите, които са получени, описани и/или публикувани от други учени са надлежно и подробно цитирани в библиографията.

Настоящата работа не е прилага за придобиване на научна степен в друго висше училище, университет или научен институт.

Библиография

[1] Bose, R., and Bush, K. Orthogonal arrays of strength two and three. *Ann. Math.Stat. 23* (1952), 508–524.

[2] Boumova, S., Marinova, T., Ramaj, T., and Stoyanova, M. Nonexistence of (17, 108, 3) ternary orthogonal array. *Annuaire de l'Université se Sofia "St. Kl. Ohridski" Faculté de Mathématiques et Informatique, Ann. Sofia Univ., Fac. Math and Inf. 106* (2019), 117–126.

[3] Boumova, S., Marinova, T., and Stoyanova, M. On ternary orthogonal arrays. *Proceedings of 17th International Workshop on Algebraic and Combinatorial Coding Theory* (2018), 102–105.

[4] Boumova, S., Ramaj, T., and Stoyanova, M. Computing distance distributions of ternary orthogonal arrays. *BGSIAM* (2019).

[5] Boumova, S., Ramaj, T., and Stoyanova, M. On covering radius of orthogonal arrays. *Proceedings of 16th International Workshop on Algebraic and Combinatorial Coding Theory* (2020).

[6] Boumova, S., Ramaj, T., and Stoyanova, M. Computing distance distributions of ternary orthogonal arrays. *Comptes rendus de l'Académie bulgare des Sciences* (to appear).

[7] Boyvalenkov, P., and Kulina, H. Investigation of binary orthogonal arrays via their distance distributions. *Problems of Information Transmission 14* (1998), 97–107.

[8] Boyvalenkov, P., Marinova, T., and Stoyanova, M. Nonexistence of a few binary orthogonal arrays. *Discrete Applied Mathematics 2* (2017), 144–150.

[9] Bush, K. A. *Orthogonal arrays.* PhD thesis, University of North Carolina, 1950.

[10] Cohen, G., Honkala, I., Litsyn, D., and Lobstain, A. *Covering codes.* North-Holland Mathematical Library, vol. 54, ELSEVIAR, 1997.

[11] Cohen, G., Karpovsky, M., Matson, H., and Schatz, J. Covering radius – survey and recent results. *IEEE Trans. Infor. Theory IT-311* (May 1985), no 3.

[12] Delsarte, P. Bounds for unrestricted codes by linear programming. *Philips Research Reports 27* (1972), 272–289.

[13] Delsarte, P. An algebraic approach to the association schemes of coding theory. *Philips Research Reports Supplements 10* (1973).

[14] Delsarte, P. Four fundamental parameters of a code and their combinatorial significance. *Inform. Contr. 23* (1973), 407–438.

[15] Delsarte, P., and Levenstein, V. Association schemes and coding theory. *IEEE Trans. on Inform. Theory 44*, 6 (1998), 2477–2504.

[16] Evangelaras, H., Koukouvinos, C., and Lappas, E. 18-run nonisomorphic three level orthogonal arrays. *Metrika 66* (2007), 437–449.

[17] Hedayat, A., Sloane, N., and Stufken, J. *Orthogonal Arrays: Theory and Applications.* Springer-Verlag, New York, 1999.

[18] James, G., and Liebeck, M. *Representations and Characters of Groups (2nd ed.).* Cambridge University Press.

[19] Krawtchouk, M. Sur une généralisation des polynômes d' hermite. *Compt.rend. 189*.

[20] Laihonen, T., and Litsyn, S. On upper bounds for minimum distance and covering radius of non-binary codes. *Designs, Codes, Crypt.. 14* (1998), 71–80.

[21] Laihonen, T., and Litsyn, S. New bounds on covering radius as a function of dual distance. *SIAM J. Discrete Math 12* (1999), 243–251.

[22] Levenshtein, V. I. Krawtchouk polynomials and universal bounds for codes and designs in hamming spaces. *IEEE Trans. Inform. Theory 41, no 5* (1995), 1303–1321.

[23] Levenshtein, V. I. Universal bounds for codes and design in *handbook of coding theory, eds. v.pless and w.c.huffman.* Elsevier Science B.V. *(1998), 499–648.*

[24] Levenshtein, V. I., and G., F. *On upper bounds for code distance and covering radius of designs in polynomial metric spaces.* Journal of Combinatorial Theory Series A 70 *(1995), 267–288.*

[25] MacWilliams, F. J., and Sloane, N. J. A. *The theory of error-correcting codes.* Amsterdam, The Netherlands: North Holland *(1997).*

[26] Manev, N. L. *On the distance distributions of orthogonal arrays.* Problems of Information Transmission 56*, 5 (2020).*

[27] Panario, D., Saaltink, M., Stevens, B., and Wevrick, D. *A general construction of ordered orthogonal arrays using lfsrs.* IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 65, NO. 7 *(JULY 2019), 4316– 4326.*

[28] Pless, V., and Huffman, W. Handbook of Coding Theory*. North-Holland, 1998.*

[29] Raghavarao, D. Constructions and Combinatorial Problems in Design of Experiments*. Wiley, 1st Edition, 1971.*

[30] Rao, C. R. *Hypercubes of strength d leading to confounded designs in factorial experiments.* Bull. Calcutta Math. Soc. 38 *(1946), 67–78.*

[31] Rao, C. R. *Factorial experiments derivable from combinatorial arrangements of arrays.* Royal Statist. Soc. (Suppl.) 9 *(1947), 128–139.*

[32] Rao, C. R. *On a class of arrangements.* Proc. Edinburgh Math. Soc. 8 *(1949), 119–125.*

[33] Riordan, J. *Combinatorial identities.* John Wiley& Sons, Inc. *(1968).*

[34] Schoen, E. D., Eendebak, P., and Nguyen, M. *Complete enumeration of pure-level and mixed-level orthogonal arrays.* Journal of Combinatorial Designs 18, Issue 2 *(2010), 123–140.*

[35] Seiden, E. *On the problem of construction of orthogonal arrays.* Ann. Math. Statist. 25 *(1954), 151–156.*

[36] Seiden, E. *On the maximum number of constraints of an orthogonal array.* he Annals of Mathematical Statistics, 26 *(1955), 132–135.*

[37] Shahriari, S. Algebra in Action, A course in groups, rings, and fields. *American Mathematical Society.*

[38] Shannon, C. E. *A mathematical theory of communication.* Bell. Syst. Tech. J. 27 *(1948), 374–423, 623–656.*

[39] Shannon, C. E. *Collected papers.* New York: IEEE Press. Edited by Sloane, N. J. A. and Wyner, A. D. *(1992).*

[40] Sloane, N. J. A. *http://neilsloane.com/oadir/index.html.*

[41] Szego, G. Orthogonal polynomials. *Providence, AMS col. publ., 1939.*

[42] Tang, Y., Xu, H., and Lin, D. K. J. *Uniform fractional factorial designs.* Annals of Statistics 40*, 2 (04 2012), 891–907.*

[43] Tietäväinen, A. *Covering radius and dual distance. Des. Codes Cryptogr (May 1991), 1:31–46.*

[44] Tietäväinen, A. *An upper bound on the covering radius as a function of the dual distance. IEEE Trans. Inform. Theory 36(6) (Nov 1990), 1472–1474.*

[45] Torres-Jimenez, J., Avila-George, H., Rangel-Valdez, N., and Gonzalez-Hernandez, L. *Construction of orthogonal arrays of index unity using logarithm tables for galois fields.* Cryptography and Security in Computing, Ch. 4*, 71–90.*