Софийски Университет "Св. Климент Охридски"
Факултет по Математика и Информатика

ДИПЛОМНА РАБОТА

на тема

СПЕКТРИ НА ОРТОГОНАЛНИ МАСИВИ

за присъждане на образователно-квалификационната степен

"магистър"

по магистърска програма

Дискретни и алгебрични структури

на

Таня Тодорова Маринова

Научен ръководител: гл. ас. д-р Мая Митева Стоянова

София, 2013 г.

Съдържание

Увод

Настоящата дипломна работа съдържа резултати, получени при изследване на някои класове ортогонални масиви. Състои се от увод, четири глави и списък с използвана литература.

Ортогонален масив е матрица с M реда и n стълба с елементи от някакво множество Q (най-често полето с q елемента). Елементите на Q ще означаваме с числата от 0 до $q-1$. Матрицата $M \times n$ има свойството, че ако вземем кои да са нейни τ стълба и разгледаме подматрицата, състояща се само от тях, в нейните редове ще се съдържат всички възможни наредени τ-орки над азбуката Q еднакъв брой пъти. Ортогонален масив с тези параметри ще бележим с $\tau - (n, M, q)$.

Хемингово пространство с размерност n над азбука Q (поле с q елемента) се нарича пространството от всички наредени n-орки над Q, което ще означаваме с $\mathbb{H}(n, q)$. Ще разглеждаме ортогоналните масиви като непразно подмножество на Хеминговото пространство с размерност n над азбуката Q.

Едно непразно подмножество C на $\mathbb{H}(n, q)$ е *τ-дизайн*, ако за всеки полином с реални коефициенти $f(t)$ от степен $k \leq \tau$ и за всяка точка y от $\mathbb{H}(n, q)$ е изпълнено, че $\sum_{x \in C} f(\langle x, y \rangle) = f_0|C|$, където f_0 е първият коефициент в развитието на полинома $f(t)$ по нормализираните полиноми на Кравчук.

Всеки ортогонален масив в $\mathbb{H}(n, q)$ може да се разгледа като τ-дизайн. Благодарение на този факт във втора и трета глави на дипломната работа са използвани полиномиални техники, с помощта на които са получени всички възможни спектри на ортогонален масив в $\mathbb{H}(n, 2)$ с фиксирани τ, n и M.

В първа глава на дипломната работа са въведени всички основни понятия, дефиниции и известни резултати, необходими за по-нататъшното изложение. Дефинирани са полиномите на Кравчук, използвани съществено в прилаганите в дипломната работа полиномиални техники. Описани са няколко основни граници върху характеристиките на ортогоналните масиви в $\mathbb{H}(n, 2)$ - граница на линейното програмиране за τ-дизайни, горна и долна граница за мощността на даден ортогонален масив на Рао и Хеминг, както и границата на Сингълтън за кодове. Известните до този момент граници за τ-дизайни в $\mathbb{H}(n, 2)$ са обобщени от Слоен. В края на първа глава е представена таблица с тези граници.

Във втора глава са изследвани ортогонални масиви в $\mathbb{H}(n, 2)$ с цел да се намерят всички спектри на вътрешна точка на даден ортогонален масив, разгледан

като τ-дизайн. *Спектър на τ-дизайн* относно точка $y \in \mathbb{H}(n,2)$ наричаме наредената $(n+1)$-орка, чиято i-та координата съответства на броя на думите в дизайна, които се намират на разстояние i от точката y. Основната техника за изследване на структурата на τ-дизайните се базира на така наречения полиномиален подход. Намирането на всички възможни спектри на вътрешна или външна точка се свежда до решаването на система линейни уравнения. Изложени са примери, които са пресметнати с помощта на компютърна програма, реализирана на Maple 15.

В трета глава е предложен метод за редуциране на възможностите за спектър на вътрешна точка на ортогонални масиви в $\mathbb{H}(n,2)$, който ще наричаме *теглови алгоритъм*. Той се основава на зависимостите между спектрите на ортогонални масиви със дължини n и $n-1$, представени в §3.1. Този подход не се оказва достатъчно силен, за да докажем несъществуване за някой открит случай, но редуцира доста от възможностите за спектри. За някои съществуващи ортогонални масиви прилагането на тегловия алгоритъм води до единствения възможен спектър за тяхна вътрешна точка.

В Глава 4 са представени някои приложения на ортогоналните масиви в различни области на математиката. По-подробно, разгледани са приложенията на ортогоналните масиви в криптографията при криптиране с кодове за автентичност и универсални хеш функции. Представени са също основни зависимости между кодове и ортогонални масиви. Благодарение на тези връзки, голяма част от свойствата на кодовете и известните за тях граници могат да бъдат пренесени директно върху разглежданите от нас ортогонални масиви. В дипломната работа са дадени конструкции на ортогонални масиви с помощта на разностни схеми и матрици на Адамар. В последния параграф накратко е показано приложението на ортогоналните масиви в статистиката.

Резултатите, представени в дипломната работа, са докладвани на Семинар по дискретни и алгебрични структури на магистърска програма „Дискретни и алгебрични структури“, ФМИ, СУ "Св. Кл. Охридски".

Благодарности

Преди всичко искам да изкажа благодарност на научния си ръководител гл. ас. д-р Мая Стоянова за многобройните напътствия, полезните съвети и безрезервната подкрепа, оказана по време на работата ми.

Благодаря на всички колеги от катедра Алгебра към Факултета по Математика и Информатика на Софийски Университет за създадената творческа атмосфера за работа и за подкрепата, препоръките и помощта, оказана по време на работата ми, като специално искам да отбележа помощта на ръководителя на катедрата и завеждащ магистърската програма доц. д-р Евгения Великова.

Глава 1

Ортогонални масиви

В тази глава са представени основни дефиниции, свойства и факти, които са необходими за по-нататъшните изследвания на ортогонални масиви в настоящата дипломна работа.

1.1 Хемингово пространство $\mathbb{H}(n,q)$. Двоично Хемингово пространство

Дефиниция 1.1.1. *Хемингово пространство с размерност n наричаме векторното пространство от всички n-орки над фиксирано поле Q (азбука с q елемента, $Q = \{0, 1, \ldots, q-1\}$). Ще го означаваме с $\mathbb{H}(n,q)$, а неговите елементи ще наричаме точки (думи). Разстояние на Хеминг между две точки в $\mathbb{H}(n,q)$ определяме с функцията:*

$$d : \begin{cases} \mathbb{H}(n,q) \times \mathbb{H}(n,q) & \to \mathbb{Z} \\ (x,y) & \to d(x,y), \end{cases}$$

където

$$d(x,y) = |\{\ i \mid x_i \neq y_i, x = (x_1, x_2, \ldots, x_n), y = (y_1, y_2, \ldots, y_n), x_i, y_i \in Q\ \}|.$$

По-точно, разстоянието $d(x,y)$ е броят на координатите, в които x и y се различават. В частност, диаметър на пространството $\mathbb{H}(n,q)$ означаваме с D и определяме като $D = \max\{\ d(x,y) \mid x,y \in \mathbb{H}(n,q)\ \}$.

Твърдение 1.1.2. *Хеминговото разстоянието удовлетворява следните зависимости:*

1. *$d(x,y) \geq 0$ като равенство се достига само когато $x = y$;*
2. *$d(x,y) = d(y,x)$;*

3. $d(x,y) + d(y,z) \geq d(x,z)$,

където x, y *и* z *са три произволни точки от* $\mathbb{H}(n,q)$.

Доказателство:

Първите две условия са следствие от Дефиниция 1.1.1.

3. Нека $x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n), z = (z_1, \ldots, z_n)$ са три точки от $\mathbb{H}(n,q)$. Да разгледаме разстоянието $d(x,z) = |\{i, x_i \neq z_i\}|$. За фиксиран елемент $i \in \{1, \ldots, n\}$ $x_i \neq z_i$ точно когато поне едното от двете е различно от y_i. Формално записано $\{i, x_i \neq z_i\} \subset \{i, x_i \neq y_i\} \cup \{i, y_i \neq z_i\}$. Като вземем предвид равенството за мощността на обединение на две множества A и B: $|A \cup B| = |A| + |B| - |A \cap B| \leq |A| + |B|$ и дефиницията за разстояние на Хеминг, то можем да заключим, че $d(x,z) \leq |\{i, x_i \neq y_i\} \cup \{i, y_i \neq z_i\}| \leq |\{i, x_i \neq y_i\}| + |\{i, y_i \neq z_i\}| = d(x,y) + d(y,z)$, с което доказателството е завършено. □

Да отбележим, че разстоянието $d(x, \mathbf{0})$ задава броя на ненулевите позиции в точката $x \in \mathbb{H}(n,q)$. Наричаме това разстояние тегло на точката x и го означаваме с $wt(x)$. За всеки две точки $x, y \in \mathbb{H}(n,q)$ е в сила зависимостта: $d(x,y) = wt(x) + wt(y) - 2wt(x * y)$, където $wt(x * y)$ е броят на еднаквите ненулеви позиции на x и y.

От Твърдение 1.1.2 следва, че Хеминговото разстояние е метрика. Това позволява да въведем скаларно произведение в $\mathbb{H}(n,q)$ по следното правило:

$$\langle x, y \rangle = 1 - \frac{2d(x,y)}{n}.$$

Връзката между скаларното произведение и разстоянието ще използваме и в следния еквивалентен вид:

$$d(x,y) = \frac{n(1 - \langle x, y \rangle)}{2}.$$

Ясно е, че разстоянията в n-мерното Хемингово пространство са краен брой, а именно $0, 1, \ldots, n$. Тогава всички възможности за скаларно произведение също са краен брой и те са $1, 1 - \frac{2}{n}, \ldots, 1 - \frac{2n-2}{n}, -1$.

В настоящата дипломна работа ще работим основно в двоично Хемингово пространство, което ще означаваме с $\mathbb{H}(n,2)$, т.е. азбуката е полето с два елемента $Q = \{0,1\}$.

1.2 Свойства на ортогоналните масиви

Ортогоналните масиви в Хемингово пространство (не само двоично) са разгледани за пръв път през четиридесетте години на двадесети век като комбинаторни структури с приложения в статистиката.

Дефиниция 1.2.1. *Нека азбуката е полето* $Q = \{0, 1, \ldots, q-1\}$ *и* C *е матрица с* M *реда и* n *стълба с елементи от* Q. C *се нарича ортогонален масив с* q *нива, сила*

τ и индекс λ, където $0 \leq \tau \leq n$, ако всяка $M \times \tau$ подматрица на C съдържа всички τ-орки над Q точно λ пъти като редове. Такъв ортогонален масив C ще бележим с $\tau - (n, M, q)$. Лесно се забелязва, че $\lambda = M/q^\tau$, поради което ще изпускаме λ в означението на ортогонален масив.

Ще разглеждаме ортогоналните масиви като непразно подмножество на Хеминговото пространство $\mathbb{H}(n, q)$, в което допускаме повторения на елементи. Важна характеристика на един ортогонален масив C е минималното разстояние между две различни точки от масива, което ще означаваме с $d(C)$, т.е.

$$d(C) = \min\{\ d(x, y) \mid x, y \in C, x \neq y\ \}.$$

По-надолу са представени някои основни свойства на ортогоналните масиви над $\mathbb{H}(n, q)$.

1. Всеки ортогонален масив със сила τ е ортогонален масив със сила τ' за всяко цяло $0 \leq \tau' < \tau$.

2. Нека $C_i, i = 1, \ldots, r$ са ортогонални масиви с параметри $\tau_i - (n, M_i, q)$. Тогава масивът C, получен по следния начин:

$$C = \begin{bmatrix} C_1 \\ C_2 \\ \vdots \\ C_r \end{bmatrix},$$

   е ортогонален $\tau - (n, M, q)$ масив, където $M = M_1 + M_2 + \cdots + M_r$, а силата $\tau \geq \min\{\tau_1, \ldots, \tau_r\}$. Освен това, ако $r = q$ и C_i са ортогонални $\tau - (n, M, q)$ масиви, $i = 1, \ldots, r$, след добавяне на 0 на всеки ред на C_1, 1 на всеки ред на C_2 и прочее, ще получим ортогонален масив с параметри $\tau - (n + 1, qM, q)$.

3. При пермутация на редове или стълбове в един ортогонален масив се получава ортогонален масив със същите параметри.

4. При пермутация на нивата на някой стълб в ортогонален масив се получава ортогонален масив със същите параметри.

5. Всеки $M \times n'$ подмасив на един ортогонален масив $\tau - (n, M)$ е ортогонален масив с параметри $\tau' - (n', M)$, където $\tau' = \min\{n', \tau\}$.

6. Ако вземем редовете на един $\tau - (n, M, q)$ ортогонален масив, които започват с фиксиран елемент (например 0), и изпуснем първия стълб, остава ортогонален масив с параметри $(\tau - 1) - (n - 1, M/q, q)$. По-точно:

0 0 ⋮ 0	$(\tau-1)-(n-1,M/q,q)$
1 1 ⋮ 1	$(\tau-1)-(n-1,M/q,q)$
⋮	
q - 1 q - 1 ⋮ q - 1	$(\tau-1)-(n-1,M/q,q)$

7. Нека

$$C=\begin{bmatrix} C_1 \\ C_2 \end{bmatrix}$$

е ортогонален $\tau-(n,M,q)$ масив, а C_1 е ортогонален масив с параметри $\tau_1-(n,M_1,q)$. Тогава C_2 е ортогонален масив с параметри $\tau_2-(n,M-M_1,q)$, където $\tau_2\geq\min\{\tau,\tau_1\}$.

Дефиниция 1.2.2. *Два ортогонални масива се наричат изоморфни, ако могат да се получат един от друг чрез последователност от пермутации на стълбове, редове или нива на някой ред.*

Както вече споменахме, в двоичното Хемингово пространство $\mathbb{H}(n,2)$ имаме, че азбуката е полето с два елемента $Q=\{0,1\}$. В този случай за ортогонален масив C индексът е $\lambda=M/2^\tau$. Затова тези два параметъра ще бъдат изпускани в означенията по-нататък.

Дефиниция 1.2.3. *Ортогонален масив $C\subset\mathbb{H}(n,2)$ ще означаваме с $\tau-(n,M)$.*

За двоичния случай е в сила следната теорема.

Теорема 1.2.4. *Един ортогонален масив с параметри $2u-(n,M)$ съществува точно когато съществува ортогонален $(2u+1)-(n+1,2M)$ масив.*

Доказателство:

От свойство 6. на ортогоналните масиви знаем как от един $(2u+1)-(n+1,2M)$ ортогонален масив да получим $2u-(n,M)$ ортогонален масив.

Обратно, нека C е ортогонален масив с параметри $2u-(n,M)$ и индекс λ. Строим масив B по следния начин: поставяме масива C, следван от 0, заедно с допълнението $\bar{C}$, като към него е добавен стълб от единици. Ще покажем, че получената матрица е $(2u+1)-(n+1,2M)$ масив. За целта нека означим с $\tau=2u+1$ и да

разгледаме произволни τ стълба на B. Всяка двоична τ-орка се среща точно λ пъти като редове в избрания $2M \times \tau$ подмасив. Наистина, ако последният стълб участва в избраните τ стълба, то горният факт е налице (C има сила $2u$).

В противен случай е ясно, че $n \geq \tau$ и нека изберем произволни τ стълба от първите n. За удобство ще считаме, че това са първите τ стълба. За всяка τ-орка $c = c_1, c_2, \ldots, c_\tau$ да означим с $v(c)$ броя на редовете от C, които започват с c. Тогава броят на редовете на B, започващи с c, е $v(c) + v(\bar{c})$. Целта е да покажем, че този брой е точно λ за всяко c.

Ако c се различава от c' в точно една позиция, то

$$v(c) + v(c') = \lambda.$$

Следва от факта, че C е със сила $\tau - 1$. Ако вземем дума c'', която се различава от c в две позиции, то за нея имаме:

$$v(c) - v(c'') = v(c) + v(c') - v(c') - v(c'') = (v(c) + v(c')) - (v(c') + v(c'')) = \lambda - \lambda = 0,$$

където c' е дума, която се намира на разстояние 1 както от c, така и от c''. Повтаряйки това наблюдение, забелязваме, че когато думата d се намира на четно разстояние от думата c, то $v(c) - v(d) = 0$ или с други думи $v(c) = v(d)$. От друга страна, c и $\bar{c}$ се намират на разстояние $\tau = 2u+1$, а c' и $\bar{c}$ на разстояние $2u$. Следователно $v(c') = v(\bar{c})$ и

$$v(c) + v(\bar{c}) = v(c) + v(c') = \lambda$$

за всяка дума c. С това теоремата е доказана. □

1.3 Полиноми на Кравчук

Изследванията в следващата глава се базират на факта, че можем да разглеждаме ортогоналните масиви като τ-дизайни ([8]). За целта се използва системата от ортогонални полиноми на Кравчук [17]. В този параграф са представени основни свойства и характеристики на тези полиноми.

За фиксирани елементи n и q, за $i = 0, 1, 2, \ldots$ дефинираме полиномите на Кравчук по следния начин:

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

В частност при $q = 2$ имаме:

$$K_i(x) = \sum_{j=0}^{i} (-1)^j \binom{x}{j} \binom{n-x}{i-j} = (-1)^i K_i(n-x).$$

Полиномите на Кравчук удовлетворяват и следната рекурентна зависимост

$$(i+1)K_{i+1}(x) = [i + (q-1)(n-i) - qx]K_i(x) - (q-1)(n-i+1)K_{i-1}(x),$$
$$K_0(x) = 1,\ K_1(x) = n(q-1) - qx.$$

В двоичния случай:

$$(i+1)K_{i+1}(x) = (n-2x)K_i(x) - (n-i+1)K_{i-1}(x),$$
$$K_0(x) = 1,\ K_1(x) = n - 2x.$$

Не е трудно да се докаже, че $K_i(x)$ е полином от степен i със старши коефициент $\frac{(-q)^i}{i!}$. Ортогоналното съотношение се задава със следната формула

$$\sum_{k=0}^{n} \binom{n}{k} (q-1)^k K_i(k) K_j(k) = \delta_{ij} q^n (q-1)^i \binom{n}{i},$$

от което може да се изведе и второто ортогонално съотношение

$$\sum_{k=0}^{n} K_i(k) K_j(k) = \delta_{ij} q^n.$$

Тогава *нормализираните полиноми на Кравчук* (зоналните сферични функции на Хеминговото пространство [25]) са:

$$Q_i^n(t) = \frac{1}{r_i} K_i^n \left(\frac{n}{2}(1-t) \right),$$

където константите $r_i = \binom{n}{i}(q-1)^i$, $i = 0, 1, \ldots, N = D+1$. В двоичния случай нормализираните полиноми на Кравчук са:

$$Q_0^n(t) = 1,\quad Q_1^n(t) = t,\quad Q_2^n(t) = \frac{nt^2 - 1}{n-1},\quad Q_3^n(t) = \frac{n^2t^3 + (2-3n)t}{(n-1)(n-2)},\quad \ldots$$

В сила са следните две свойства.

Лема 1.3.1. *[18] Всеки полином $Q_i(t)$, $1 \le i < N$, има i различни корена в интервала $[-1, 1]$, т.е. $-1 < z_{i,1} < z_{i,2} < \ldots < z_{i,i} < 1$.*

Да отбележим още, че $Q_i(t)$ са четни и нечетни функции съответно за четно и нечетно i, т.е. $Q_i(t) = (-1)^i Q_i(-t)$ за всяко i и t.

Лема 1.3.2. *[18] За всеки две фиксирани числа i и j, ако $1 \le j \le i < N$ са изпълнени неравенствата $z_{i+1,j} < z_{i,j} < z_{i+1,j+1}$.*

Важна роля в намирането на границите на линейното програмиране играе *ядрото* на полиномите на Кравчук, означено с $T_k(x, y)$, за $0 \le k < N$, и дефинирано чрез равенството

$$T_k(x, y) = \sum_{i=0}^{k} r_i Q_i(x) Q_i(y).$$

Дефиниция 1.3.3. *За всеки две цели неотрицателни числа a и b системата от ортогонални полиноми $\{Q_i^{a,b}(t)\}_{i=0}^N$ се нарича присъединена на основната система $\{Q_i(t)\}_{i=0}^N$.*

По-точно:

$$Q_k^{0,0}(t) = Q_k^{(n)}(t), \qquad Q_k^{0,1}(t) = \frac{K_k^{n-1}(d)}{\binom{n-1}{k}(q-1)^k},$$

$$Q_k^{1,0}(t) = \frac{K_k^{n-1}(d-1)}{\sum\limits_{i=0}^{k}\binom{n}{i}(q-1)^i}, \quad Q_k^{1,1}(t) = \frac{K_k^{n-2}(d-1)}{\sum\limits_{i=0}^{k}\binom{n-1}{i}(q-1)^i}$$

На присъединените полиноми $Q_i^{a,b}(t)$ също се съпоставят ядра

$$T_k^{a,b}(x,y) = \sum_{i=0}^{k} r_i^{a,b} Q_i^{a,b}(x) Q_i^{a,b}(y).$$

(Тук a и $b \in \{0,1\}$, а константите $r_i^{a,b}$ са естествени числа).

За всяко естествено i най-голямата нула на полинома $Q_i^{a,b}(t)$ ще означаваме с $z_i^{a,b}$, $a,b \in \{0,1\}$. В сила са следните зависимости.

Лема 1.3.4. *[16] За всяко естествено число $1 \le i < N$ са изпълнени неравенствата*

$$z_{i-1}^{1,1} < z_i^{1,0} < z_i^{1,1} < z_i^{0,1},$$

$z_0^{1,1} = -1$ *по дефиниция.*

Всеки полином $f(x)$ с реални коефициенти от степен k може да запишем по единствен начин като линейна комбинация (развитие на Фурие) по нормализираните полиноми на Кравчук $f(x) = \sum\limits_{i=0}^{k} f_i Q_i(x)$. За всяко фиксирано k е удобно да означим с b_k коефициентите f_0 в горното развитие за полиномите t^k.

За константите b_i, $i \le n$, в двоичния случай имаме следните равенства:

$$b_0 = 1; \quad b_{2j+1} = 0; \quad b_{2j} = \frac{1}{2^n}\sum_{d=0}^{n}\left(1 - \frac{2d}{n}\right)^{2j}\binom{n}{d}.$$

Дефиниция 1.3.5. *[15] Нека C е непразно мултимножество, $C \subset \mathbb{H}(n,q)$. C е τ-дизайн, ако за всеки полином с реални коефициенти $f(t)$ от степен k, ненадминаваща τ, и за всяка точка $y \in \mathbb{H}(n,q)$ е в сила равенството*

$$\sum_{x \in C} f(\langle x,y\rangle) = f_0|C|,$$

където f_0 е първият коефициент в развитието на полинома $f(t)$ по нормализираните полиноми на Кравчук, т.е. $f(t) = \sum\limits_{i=0}^{n} f_i Q_i(t)$, а $\langle x,y\rangle = 1 - \dfrac{2d(x,y)}{n}$. Максималното цяло неотрицателно число τ, за което C е τ-дизайн, се нарича сила на дизайна.

Някои автори разглеждат τ-дизайните като τ-независими множества [1]. Ако C е τ-дизайн, $\tau \geq 1$, то C е τ'-дизайн за всяко $\tau' \in \{0, 1, \ldots, \tau - 1\}$.

1.4 Основни граници за ортогонални масиви в $\mathbb{H}(n, 2)$

Една от важните задачи в изучаването на ортогоналните масиви е следната.

Проблем 1.4.1. *За фиксирани сила τ и брой стълбове n да се намери минималната възможна мощност M, за която съществува $\tau - (n, M)$ ортогонален масив в $\mathbb{H}(n, 2)$, т.е. да се оцени величината*

$$B(n, \tau) = min\{M = |C| : \text{ съществува } \tau - \text{дизайн } C \subset \mathbb{H}(n, 2)\}.$$

От тъждеството $M = \lambda 2^\tau$, горната задача е еквивалентна с намирането на минимален индекс λ на ортогонален масив с фиксирани сила τ и n стълба.

Универсални долни граници за минималната възможна мощност (величината $B(n, \tau)$) на ортогонален масив с параметри $\tau - (n, M)$ в $\mathbb{H}(n, 2)$ (Проблем 1.4.1) са получени от редица автори [2, 3, 7, 8, 10]. В този параграф са представени някои от тези граници в двоичния случай като първа е разгледана границата на линейното програмиране за дизайни в крайни полиномиални метрични пространства.

Теорема 1.4.2. *(Граница на линейното програмиране за дизайни [7]) Нека $C \subset \mathbb{H}(n, 2)$ е τ-дизайн, $\tau \geq 1$ е цяло число. Нека $f(t)$ е полином с реални коефициенти от степен k, за който за изпълнени условията*

1. *$f(t) \geq 0$ за всяко $t \in [-1, 1]$,*
2. *Коефициентите в развитието на полинома $f(t)$ по нормализираните полиноми на Кравчук $f(t) = \sum_{i=1}^{n} f_i Q_i(t)$ удовлетворяват неравенствата $f_0 > 0, f_i \leq 0$ за $i = \tau + 1, \ldots k$.*

Тогава $B(n, \tau) \geq f(1)/f_0$.

Следващите две двойки граници могат да се получат с помощта на комбинаторни методи, а също така могат да се докажат, използвайки методите на линейното програмиране. Да отбележим, че в общия случай границата на линейното програмиране (границата на Делсарт) е по-силна от представената по-долу граница на Рао, но в двоичния случай тези две граници съвпадат.

Теорема 1.4.3. *(Граници на Рао [20] и Хеминг) Параметрите $\tau - (n, M)$ на един ортогонален масив C в $\mathbb{H}(n, 2)$ удовлетворяват следните неравенства*

$$D(n, \tau) \leq |C| \leq \frac{2^n}{D(n, d(C) - 1)},$$

където за $D(n,\tau)$ *имаме*

$$D(n,\tau) = \begin{cases} \sum_{i=0}^{n} \binom{n}{i}, & \text{ако } \tau = 2u, \\ \sum_{i=0}^{n} \binom{n}{i} + \binom{n-1}{u}, & \text{ако } \tau = 2u+1. \end{cases}$$

Кодовете, които достигат лявата или дясната граница в Теорема 1.4.3, се наричат съответно плътни дизайни и съвършени кодове.

Следващата двойка са границите на Сингълтън за код $C \subset \mathbb{H}(n,2)$.

Теорема 1.4.4. *Нека* C *е крайно непразно подмножество (код) на* $\mathbb{H}(n,2)$. *Тогава за мощността на* C *са в сила следните граници:*

$$2^{d'-1} \leq |C| \leq 2^{n-d(C)+1},$$

като всяка от границите се достига тогава и само тогава когато $d(C)+\tau = n+1$. *Да уточним, че* $\tau = d'-1$, *т.е. при равенство имаме* $d+d' = n+2$.

Границите за τ-дизайни в $\mathbb{H}(n,2)$ са обобщени от Слоен [13] и са представени по-долу в Таблица 1.1. За всяко n от 4 до 32 и всяко τ от 2 до 10 са дадени минималните възможни индекси λ, за които съществуват τ-дизайни. От таблицата е ясно, че минималните възможни стойности за 2-дизайни и 3-дизайни са известни са всяко разгледано n.

Означението $\lambda_0 - \lambda_1$ показва, че τ-дизайн със съответните n и τ трябва да има индекс не по-малък от λ_0, а τ-дизайн с индекс λ_1 съществува. Например, за $n = 10$ и $\tau = 6$ в таблицата е записано $6-8$, което означава, че 6-дизайни с размерност 10 имат мощност не по-малка от 6.2^6, а дизайн с параметри $6-(10, 8.2^6)$ е известен. С други думи все още стои открит въпросът дали съществуват 6-дизайни съответно с параметри $6-(10, 6.2^6)$ и $6-(10, 7.2^6)$.

n \ τ	2^{Hd}	3^{Hd}	4	5	6	7	8	9	10
4	2	1	1						
5	2	2	1	1					
6	2	2	2	1	1				
7	2	2	$^{SZ}4$	2	1	1			
8	3	2	4^{c}	$^{SZ}4$	2	1	1		
9	3	3	6–8	4^{c}	4	2	1	1	
10	3	3	6–8	6–8	$^{SZ}6$–8	4	2	1	1
11	3	3	6–8	6–8	8^{c}	$^{SZ}6$–8	4	2	1
12	4	3	7–8	6–8	12–16	8^{c}	6–8	4	2
13	4	4	8	7–8	16	12–16	10–16	6–8	4
14	4	4	8	8	16	16	16^{c}	10–16	6–8
15	4	4	8^{NR}	8	16^{RH}	16	26–32	16^{c}	11–16
16	5	4	10–16	8^{NR}	21–32	16^{RH}	39–64	26–32	19–32
17	5	5	12–16	10–16	26–32	21–32	52–64^{jx}	39–64	32^{c}
18	5	5	13–16	12–16	29–32	26–32	52–128	52–64^{jx}	54–64
19	5	5	14–16^{X4}	13–16	29–32	29–32	52–128	52–128	86–128
20	6	5	15–32	14–16^{X4}	29–32	29–32	64–128^{c}	52–128	128^{c}
21	6	6	17–32	15–32	32	29–32	86–256	64–128^{c}	171–256
22	6	6	20–32	17–32	32	32	108–256	86–256	171–256
23	6	6	22–32^{W}	20–32	32^{Go}	32	118–256^{HP}	108–256	171–256^{uv}
24	7	6	22–64	22–32^{W}	41–64	32^{Go}	119–512	118–256^{HP}	219–512
25	7	7	23–64	22–64	51–128	41–64	127–512	119–512	290–512
26	7	7	26–64	23–64	58–128	51–128	149–512	127–512	384–512^{re}
27	7	7	29–64	26–64	66–128^{Ka}	58–128	164–512^{Pi}	149–512	456–1024
28	8	7	29–64	29–64	73–256	66–128^{Ka}	165–1024	164–512^{Pi}	458–1024
29	8	8	29–64	29–64	74–256	73–256	168–1024	165–1024	464–1024
30	8	8	33–64	29–64	87–256	74–256	189–1024	168–1024	570–1024
31	8	8	37–64	33–64	96–256^{CS}	87–256	199–1024^{Sh}	189–1024	681–1024^{BC}
32	9	8	37–64^{BC}	37–64	108–512	96–256^{CS}	209–2048	199–1024^{Sh}	721–2048

Таблица 1.1. Минимален възможен индекс на τ-(n, M) дизайн в $H(n, 2)$.

Легенда:

BC	БЧХ код
c	цикличен код
CS	код на Ченг и Слоен (1989)
Go	код на Голей
HP	код на Хашим и Поздняков (1976)
jx	слепваща конструкция
Ka	код на Карлин (1969)
NR	код на Нордстром-Робинсън (1967)
Pi	код на Пирет (1980)
re	конструкция на остатъците (Хелгерт и Щинаф, 1973)
RH	конструкция на Рао-Хеминг
Sh	код на Шиърър (1988)
SZ	граница на Зайден и Земаш (1966)
uv	(u,u+v) конструкция
W	код на Вагнер (1965)
$X4$	конструкция X4

Глава 2

Спектри на ортогонални масиви в $\mathbb{H}(n,2)$

Изследването на дадена характеристика на един обект е често срещана практика. В тази и следващата глава ще обърнем специално внимание на спектрите на даден дизайн в $\mathbb{H}(n,2)$, намирането на всички възможности и анализ на резултатите.

2.1 Намиране спектрите на вътрешна точка на τ-дизайн

Дефиниция 2.1.1. *Нека $C \subset \mathbb{H}(n,2)$ е $\tau-(n,M)$-дизайн. Разглеждаме масива C като подпространство на двоичното Хеминтово пространство $\mathbb{H}(n,2)$ с размерност n. На всяка точка $y \in \mathbb{H}(n,2)$ съпоставяме $(n+1)$-орка $(q_0(y), q_1(y), \ldots, q_n(y))$, където*

$$q_i(y) = |\{x \in C | d(x,y) = i\}|,$$

за $i = 0, \ldots, n$. Тази $(n+1)$-орка се нарича спектър на C по отношение на елемента y. С други думи $q_i(y)$ е броят на редовете на C, които се намират на разстояние i от фиксирания елемент y.

За удобство ще използваме две различни означения в зависимост от това дали елемента y принадлежи на дизайна или не. За думите от дизайна числата от спектъра ще бележим с $p_i(y), i = 0, 1, \ldots, n$, докато за тези извън C ще оставим означението от дефиницията - $q_i(y)$. Да отбележим специално, че в тази глава допускаме повторение на точките в разглежданите дизайни.
Освен това за всяка точка $y \in C$ имаме $p_0(y) \geq 1$, тъй като $p_0(y)$ показва броя на думите в дизайна C, съвпадащи с y (включително самата y). При това $p_n(y) = 0$ точно когато $-y \notin C$. От друга страна за всяка точка y извън дизайна C имаме $q_0(y) = 0$.

Нека $C \subset \mathbb{H}(n,2)$ е ортогонален масив. Винаги може да считаме, че C съдържа нулев ред. Това може да го осигурим с пермутиране на нивата на стълбовете, знаейки от Свойство 4., че ще получим ортогонален масив със същите параметри, изоморфен на първоначално дадения.

В такъв случай може да разгледаме спектъра на C относно елемента $\mathbf{0} = (0,0,\ldots,0)$. Този специален спектър на масива C ще бележим с $w(\mathbf{0}) = (w_0, w_1, \ldots, w_n)$ и ще наричаме *теглово разпределение* на ортогоналния масив.
От дефиницията на тегловото разпределение на C се вижда, че w_i е броят на точките в масива C, които имат тегло i за всяко $i = 0, \cdots, n$. Тъй като всеки елемент с подходящи пермутации може да бъде сведен до нулев, то всеки спектър на точка може да бъде разглеждан като негово теглово разпределение.

Един от начините за пресмятане на спектри на даден τ-дизайн е следствие от по-общ подход, предложен от Бойваленков в [4]. По-точно следващата теорема, следствие от [4, Теорема 3.2], дава необходимия апарат за намиране всички възможности за спектри на вътрешна точка или външна точка за даден ортогонален масив (вж. също [5], [14]).

Теорема 2.1.2. *Нека $C \subset \mathbb{H}(n,2)$ е τ-дизайн и $y \in \mathbb{H}(n,2)$ е фиксирана точка от разглежданото Хемингово пространство. Тогава*

(а) ако $y \in C$, спектърът на C относно точката y удовлетворява системата

$$\sum_{i=0}^{n} p_i(y) \left(1 - \frac{2i}{n}\right)^k = b_k|C|, k = 0, 1, \ldots, \tau, \tag{2.1.1}$$

(б) ако $y \notin C$, спектърът на C относно точката y удовлетворява системата

$$\sum_{i=1}^{n} q_i(y) \left(1 - \frac{2i}{n}\right)^k = b_k|C|, k = 0, 1, \ldots, \tau,$$

където b_k е първият коефициент в развитието на полинома t^k по нормализираните полиноми на Кравчук.

Системата (2.1.1) се състои от $\tau + 1$ реда и $n + 1$ стълба. Тя от Вандермондов тип с пълен ранг. Следователно пространството от решения на системата се определя от $(n+1) - (\tau+1) = n - \tau$ неизвестни параметъра. Тези параметри могат да пробягват множеството $\{0, \ldots, |C|\}$. По този начин може да намираме всички възможни спектри за вътрешни точки на ортогонален масив C с дадени параметри τ, n и M.

Следствие 2.1.3. *Нека C е ортогонален масив с параметри $\tau - (\tau, \lambda 2^\tau)$. Тогава има само един възможен спектър на вътрешна точка y на C като за тази единствена възможност $p_0(y) = \lambda$.*

Доказателство:

Тъй като системата (2.1.1) се състои от $n-\tau$ свободни параметъра, а $n=\tau$, всъщност имаме единствено решение. Това решение е търсеният спектър на точка от масива C.

От дефиницията на ортогонален $\tau-(n,M)$ масив знаем, че във всеки подмасив $M\times\tau$ всяка τ-орка се среща точно $\lambda=M/2^\tau$ пъти. От факта, че $n=\tau$ и $M=\lambda 2^\tau$, можем директно да покажем кое е това решение, а именно спектърът на C спрямо коя да е вътрешна точка $y\in C$ е:

$$p_i(y)=\lambda\binom{\tau}{i},\ i=0,\ldots,\tau.$$

В частност $p_0(y)=\lambda$. □

Следствие 2.1.4. *Нека C е ортогонален масив с параметри $\tau-(\tau+1,\lambda 2^\tau)$. Тогава възможностите за спектър на вътрешна точка за C са точно λ на брой.*

Доказателство:
Нека спрямо вътрешна точка y ортогоналният масив C има спектър $(p_0,p_1,\ldots,p_{\tau+1})$. От Свойство 5. на ортогоналните масиви следва, че при премахване на един стълб от масива C, ще получим масив C' с параметри $\tau-(\tau,\lambda 2^\tau)$. Нека C' спрямо вътрешна точка има спектър $(p'_0,p'_1,\ldots,p'_\tau)$. От една страна $p'_0\geq p_0$, а от Следствие 2.1.3 имаме $p'_0=\lambda$. Тогава $p_0\in\{1,2,\ldots,\lambda\}$. Заместваики p_0 с всяка една от тези стойности в система (2.1.1), получаваме системи от Вандермондов тип с $\tau+1$ реда и $\tau+1$ неизвестни. Всяка една от тези λ системи има единствено решение, следователно и всички възможни спектри на вътрешна точка на C за точно λ на брой. □

2.2 Примери за намерени спектри на вътрешна точка на някои ортогонални масиви

В този параграф ще илюстрираме техниката от §2.1 в няколко примера.

Пример 2.2.1. *Единственият спектър на вътрешна точка за ортогонален масив с параметри $6-(6,6.2^6)$ има вида $(p_0(y),p_1(y),\ldots,p_6(y))$, където $p_i(y)=6\binom{6}{i}, i=0,1,\ldots,6$. По-точно:*

$$p_0(y)=6,p_1(y)=36,p_2(y)=90,p_3(y)=120,p_4(y)=90,p_5(y)=36,p_6(y)=6.$$

Пример 2.2.2. *Нека C е $\tau-(\tau+1,2^\tau)$ ортогонален масив. От Следствие 2.1.4 е ясно, че системата има $\lambda=1$ решения. Всъщност този масив се конструира като към ортогоналния масив с параметри $\tau-(\tau,2^\tau)$ е добавена проверка за четност за всяка дума. Следователно не е необходимо да решаваме системата, за да научим*

това единствено решение. То се получава по следния начин:

$$\begin{aligned} p_0 &= 1 \\ p_{2i+1} &= 0, \qquad\qquad za\ i = 0,1,\ldots,\left[\frac{\tau}{2}\right] \\ p_{2i} &= \sum_{j=2i-1}^{min\{\tau,2i\}} \binom{\tau}{i}, \quad za\ i = 1,2,\ldots,\left[\frac{\tau+1}{2}\right]. \end{aligned}$$

Например, за $4-(4,16)$ *ортогонален масив имаме* $\lambda = 1$ *и от Следствие 2.1.3 получаваме*

$$p_0(y) = 1, p_1(y) = 4, p_2(y) = 6, p_3(y) = 4, p_4(y) = 1.$$

Откъдето за $4-(5,16)$ *ортогонален масив ще имаме*

$$p_0(y) = 1, p_1(y) = 0, p_2(y) = 10, p_3(y) = 0, p_4(y) = 10, p_5(y) = 0.$$

Да отбележим (вж. например [13]), че всеки два ортогонални масива (дизайна) с параметри $\tau-(\tau+1,2^\tau)$ са изоморфни помежду си.

По-надолу са представени няколко примера, в които спектрите на дизайните са пресметнати по Теорема 2.1.2 с помощта на компютърна програма на Maple 15. Тъй като пресметнатите спектри ще бъдат използвани за тегловия алгоритъм, изложен в следващата глава, тук при изследване на $\tau-(n,M)$ дизайн ще разглеждаме спектрите за следната редица от ортогонални масиви $\tau-(\tau,M), \tau-(\tau+1,M),\ldots,\tau-(n,M)$.

За по-голяма яснота на представената техника първо е разгледан един пример на известни (конструирани от Слоен) масиви. С този пример ще бъде добре илюстриран и тегловия алгоритъм в следващата глава. Самите масиви могат да бъдат намерени на web-страницата на Слоен: http://neilsloane.com/oadir/index.html.

Пример 2.2.3. *За редицата от ортогонални масиви* $5-(5,128)$, $5-(6,128)$, $5-(7,128)$, $5-(8,128)$, $5-(9,128)$ *прилагаме Теорема 2.1.2 за вътрешна точка от разглежданите дизайни. Резултатите са представени в съответни таблици по-долу. Спектърът на* $5-(5,128)$ *е:* $(p_0,p_1,p_2,p_3,p_4,p_5) = (4,20,40,40,20,4)$.

0	p_0	p_1	p_2	p_3	p_4	p_5	p_6
1	1	18	15	60	15	18	1
2	2	12	30	40	30	12	2
3	3	6	45	20	45	6	3
4	4	0	60	0	60	0	4

Таблица 2.1. Всички възможни спектри на вътрешна точка за ортогонален $5-(6,128)$ масив.

0	p_0	p_1	p_2	p_3	p_4	p_5	p_6	p_7
1	1	6	27	20	55	6	13	0
2	1	7	21	35	35	21	7	1
3	1	8	15	50	15	36	1	2
4	2	0	42	0	70	0	14	0
5	2	1	36	15	50	15	8	1
6	2	2	30	30	30	30	2	2

Таблица 2.2. Всички възможни спектри на вътрешна точка за ортогонален $5-(7,128)$ масив.

0	p_0	p_1	p_2	p_3	p_4	p_5	p_6	p_7	p_8
1	1	0	27	6	55	20	13	6	0
2	1	0	28	0	70	0	28	0	1
3	1	1	21	21	35	35	7	7	0
4	1	1	22	15	50	15	22	1	1
5	1	2	15	36	15	50	1	8	0
6	1	2	16	30	30	30	16	2	1
7	1	3	10	45	10	45	10	3	1

Таблица 2.3. Всички възможни спектри на вътрешна точка за ортогонален $5-(8,128)$ масив.

0	p_0	p_1	p_2	p_3	p_4	p_5	p_6	p_7	p_8	p_9
1	1	0	7	38	3	52	17	6	4	0
2	1	0	8	32	18	32	32	0	5	0
3	1	0	9	27	27	27	27	9	0	1
4	1	0	10	21	42	7	42	3	1	1
5	1	1	3	42	7	42	21	10	0	1
6	1	1	4	36	22	22	36	4	1	1

Таблица 2.4. Всички възможни спектри на вътрешна точка за ортогонален $5-(9,128)$ масив.

Пример 2.2.4. *Както вече споменахме в края на първа глава, за ортогонален масив с параметри* $6-(10,384)$ *нямаме информация нито за неговото съществуване, нито за неговото несъществуване. Той е един от основните обекти на нашите изследвания. Всички възможности за спектри на вътрешна точка на редицата* $6-(6,384), 6-(7,384), 6-(8,384), 6-(9,384), 6-(10,384)$ *са представени в съответни таблици по-долу. Спектърът на* $6-(6,384)$ *е:* $(p_0,p_1,p_2,p_3,p_4,p_5,p_6) = (6,36,90,120,90,36,6)$.

0	p_0	p_1	p_2	p_3	p_4	p_5	p_6	p_7
1	1	35	21	175	35	105	7	5
2	2	28	42	140	70	84	14	4
3	3	21	63	105	105	63	21	3
4	4	14	84	70	140	42	28	2
5	5	7	105	35	175	21	35	1
6	6	0	126	0	210	0	42	0

Таблица 2.5. Всички възможни спектри на вътрешна точка за ортогонален $6-(7,384)$ масив.

0	p_0	p_1	p_2	p_3	p_4	p_5	p_6	p_7	p_8
1	1	14	42	70	140	42	70	2	3
2	1	15	35	91	105	77	49	9	2
3	1	16	28	112	70	112	28	16	1
4	1	17	21	133	35	147	7	23	0
5	2	7	63	35	175	21	77	1	3
6	2	8	56	56	140	56	56	8	2
7	2	9	49	77	105	91	35	15	1
8	2	10	42	98	70	126	14	22	0
9	3	0	84	0	210	0	84	0	3
10	3	1	77	21	175	35	63	7	2
11	3	2	70	42	140	70	42	14	1
12	3	3	63	63	105	105	21	21	0

Таблица 2.6. Всички възможни спектри на вътрешна точка за ортогонален $6-(8,384)$ масив.

0	p_0	p_1	p_2	p_3	p_4	p_5	p_6	p_7	p_8	p_9
1	1	2	52	0	182	28	84	32	1	2
2	1	3	45	21	147	63	63	39	0	2
3	1	3	46	14	168	28	98	18	7	1
4	1	4	39	35	133	63	77	25	6	1
5	1	4	40	28	154	28	112	4	13	0
6	1	5	32	56	98	98	56	32	5	1
7	1	5	33	49	119	63	91	11	12	0
8	1	6	25	77	63	133	35	39	4	1
9	1	6	26	70	84	98	70	18	11	0
10	1	7	18	98	28	168	14	46	3	1

Таблица 2.7. Всички възможни спектри на вътрешна точка за ортогонален $6-(9,384)$ масив.

11	1	7	19	91	49	133	49	25	10	0
12	1	8	12	112	14	168	28	32	9	0
13	2	0	39	63	63	147	21	45	3	1
14	2	0	40	56	84	112	56	24	10	0
15	2	1	32	84	28	182	0	52	2	1
16	2	1	33	77	49	147	35	31	9	0
17	2	2	26	98	14	182	14	38	8	0

Таблица 2.7. Всички възможни спектри на вътрешна точка за ортогонален $6-(9,384)$ масив. (Продължение)

0	p_0	p_1	p_2	p_3	p_4	p_5	p_6	p_7	p_8	p_9	p_{10}
1	1	0	23	54	28	182	0	82	11	2	1
2	1	0	24	47	49	147	35	61	18	1	1
3	1	0	25	40	70	112	70	40	25	0	1
4	1	0	25	41	63	133	35	75	4	7	0
5	1	0	26	34	84	98	70	54	11	6	0
6	1	0	27	27	105	63	105	33	18	5	0
7	1	0	28	20	126	28	140	12	25	4	0
8	1	1	17	68	14	182	14	68	17	1	1
9	1	1	18	61	35	147	49	47	24	0	1
10	1	1	18	62	28	168	14	82	3	7	0
11	1	1	19	55	49	133	49	61	10	6	0
12	1	1	20	48	70	98	84	40	17	5	0
13	1	1	21	41	91	63	119	19	24	4	0
14	1	2	11	82	0	182	28	54	23	0	1
15	1	2	12	76	14	168	28	68	9	6	1
16	1	2	13	69	35	133	63	47	16	5	0
17	1	2	14	62	56	98	98	26	23	4	0
18	1	2	15	55	77	63	133	5	30	3	0
19	1	3	6	90	0	68	42	54	15	5	0
20	1	3	7	83	21	133	77	33	22	4	0
21	1	3	8	76	42	98	112	12	29	3	0
22	1	4	1	97	7	133	91	19	28	3	0

Таблица 2.8. Всички възможни спектри на вътрешна точка за ортогонален $6-(10,384)$ масив.

Пример 2.2.5. *Последният пример, който ще изложим в тази глава, е за ортогонален масив с параметри* $6-(11,512)$. *Масивите от разгледаната по-долу редица съществуват (вж. web-страницата на Слоен). За ортогоналните масиви с параметри* $6-(6,512)$, $6-(7,512)$, $6-(8,512)$, $6-(9,512)$, $6-(10,512)$ *и*

$6-(11,512)$ *прилагаме Теорема 2.1.2 и получаваме в съответни таблици всички възможности за техните спектри. Спектърът на* $6-(6,512)$ *е:* $(p_0,p_1,p_2,p_3,p_4,p_5,p_6) = (8,48,120,160,120,48,8)$.

0	p_0	p_1	p_2	p_3	p_4	p_5	p_6	p_7
1	1	49	21	245	35	147	7	7
2	2	42	42	210	70	126	14	6
3	3	35	63	175	105	105	21	5
4	4	28	84	140	140	84	28	4
5	5	21	105	105	175	63	35	3
6	6	14	126	70	210	42	42	2
7	7	7	147	35	245	21	49	1
8	8	0	168	0	280	0	56	0

Таблица 2.9. Всички възможни спектри на вътрешна точка за ортогонален $6-(7,512)$ масив.

0	p_0	p_1	p_2	p_3	p_4	p_5	p_6	p_7	p_8
1	1	21	49	105	175	63	91	3	4
2	1	22	42	126	140	98	70	10	3
3	1	23	35	147	105	133	49	17	2
4	1	24	28	168	70	168	28	24	1
5	1	25	21	189	35	203	7	31	0
6	2	14	70	70	210	42	98	2	4
7	2	15	63	91	175	77	77	9	3
8	2	16	56	112	140	112	56	16	2
9	2	17	49	133	105	147	35	23	1
10	2	18	42	154	70	182	14	30	0
11	3	7	91	35	245	21	105	1	4
12	3	8	84	56	210	56	84	8	3
13	3	9	77	77	175	91	63	15	2
14	3	10	70	98	140	126	42	22	1
15	3	11	63	119	105	161	21	29	0
16	4	0	112	0	280	0	112	0	4
17	4	1	105	21	245	35	91	7	3
18	4	2	98	42	210	70	70	14	2
19	4	3	91	63	175	105	49	21	1
20	4	4	84	84	140	140	28	28	0

Таблица 2.10. Всички възможни спектри на вътрешна точка за ортогонален $6-(8,512)$ масив.

0	p_0	p_1	p_2	p_3	p_4	p_5	p_6	p_7	p_8	p_9
1	1	5	63	7	245	21	133	29	6	2
2	1	6	56	28	210	56	112	36	5	2
3	1	6	57	21	231	21	147	15	12	1
4	1	7	49	49	175	91	91	43	4	2
5	1	7	50	42	196	56	126	22	11	1
6	1	7	51	35	217	21	161	1	18	0
7	1	8	42	70	140	126	70	50	3	2
8	1	8	43	63	161	91	105	29	10	1
9	1	8	44	56	182	56	140	8	17	0
10	1	9	35	91	105	161	49	57	2	2
11	1	9	36	84	126	126	84	36	9	1
12	1	9	37	77	147	91	119	15	16	0
13	1	10	28	112	70	196	28	64	1	2
14	1	10	29	105	91	161	63	43	8	1
15	1	10	30	98	112	126	98	22	15	0
16	1	11	21	133	35	231	7	71	0	2
17	1	11	22	126	56	196	42	50	7	1
18	1	11	23	119	77	161	77	29	14	0
19	1	12	15	147	21	231	21	57	6	1
20	1	12	16	140	42	196	56	36	13	0
21	1	13	9	161	7	231	35	43	12	0
22	2	0	70	14	210	70	98	42	4	2
23	2	0	71	7	231	35	133	21	11	1
24	2	0	72	0	252	0	168	0	18	0
25	2	1	63	35	175	105	77	49	3	2
26	2	1	64	28	196	70	112	28	10	1
27	2	1	65	21	217	35	147	7	17	0
28	2	2	56	56	140	140	56	56	2	2
29	2	2	57	49	161	105	91	35	9	1
30	2	2	58	42	182	70	126	14	16	0
31	2	3	49	77	105	175	35	63	1	2
32	2	3	50	70	126	140	70	42	8	1
33	2	3	51	63	147	105	105	21	15	0
34	2	4	42	98	70	210	14	70	0	2
35	2	4	43	91	91	175	49	49	7	1
36	2	4	44	84	112	140	84	28	14	0

Таблица 2.11. Всички възможни спектри на вътрешна точка за ортогонален $6 - (9, 512)$ масив.

37	2	5	36	112	56	210	28	56	6	1
38	2	5	37	105	77	175	63	35	13	0
39	2	6	29	133	21	245	7	63	5	1
40	2	6	30	126	42	210	42	42	12	0
41	2	7	23	147	7	245	21	49	11	0
42	3	0	44	112	42	224	28	48	11	0
43	3	1	37	133	7	259	7	55	10	0

Таблица 2.11. Всички възможни спектри на вътрешна точка за ортогонален $6-(9,512)$ масив (Продължение).

0	p_0	p_1	p_2	p_3	p_4	p_5	p_6	p_7	p_8	p_9	p_{10}
1	1	0	38	48	70	224	0	112	17	0	2
2	1	0	39	42	84	210	0	126	3	6	1
3	1	0	40	35	105	175	35	105	10	5	1
4	1	0	41	28	126	140	70	84	17	4	1
5	1	0	42	21	147	105	105	63	24	3	1
6	1	0	42	22	140	126	70	98	3	10	0
7	1	0	43	14	168	70	140	42	31	2	1
8	1	0	43	15	161	91	105	77	10	9	0
9	1	0	44	7	189	35	175	21	38	1	1
10	1	0	44	8	182	56	140	56	17	8	0
11	1	0	45	0	210	0	210	0	45	0	1
12	1	0	45	1	203	21	175	35	24	7	0
13	1	1	33	56	70	210	14	112	9	5	1
14	1	1	34	49	91	175	49	91	16	4	1
15	1	1	35	42	112	140	84	70	23	3	1
16	1	1	35	43	105	161	49	105	2	10	0
17	1	1	36	35	133	105	119	49	30	2	1
18	1	1	36	36	126	126	84	84	9	9	0
19	1	1	37	28	154	70	154	28	37	1	1
20	1	1	37	29	147	91	119	63	16	8	0
21	1	1	38	21	175	35	189	7	44	0	1
22	1	1	38	22	168	56	154	42	23	7	0
23	1	1	39	15	189	21	189	21	30	6	0
24	1	2	27	70	56	210	28	98	15	4	1

Таблица 2.12. Всички възможни спектри на вътрешна точка за ортогонален $6-(10,512)$ масив.

25	1	2	28	63	77	175	63	77	22	3	1
26	1	2	28	64	70	196	28	112	1	10	0
27	1	2	29	56	98	140	98	56	29	2	1
28	1	2	29	57	91	161	63	91	8	9	0
29	1	2	30	49	119	105	133	35	36	1	1
30	1	2	30	50	112	126	98	70	15	8	0
31	1	2	31	42	140	70	168	14	43	0	1
32	1	2	31	43	133	91	133	49	22	7	0
33	1	2	32	36	154	56	168	28	29	6	0
34	1	2	33	29	175	21	203	7	36	5	0
35	1	3	20	91	21	245	7	105	14	4	1
36	1	3	21	84	42	210	42	84	21	3	1
37	1	3	21	85	35	231	7	119	0	10	0
38	1	3	22	77	63	175	77	63	28	2	1
39	1	3	22	78	56	196	42	98	7	9	0
40	1	3	23	70	84	140	112	42	35	1	1
41	1	3	23	71	77	161	77	77	14	8	0
42	1	3	24	63	105	105	147	21	42	0	1
43	1	3	24	64	98	126	112	56	21	7	0
44	1	3	25	57	119	91	147	35	28	6	0
45	1	3	26	50	140	56	182	14	35	5	0
46	1	4	14	105	7	245	21	91	20	3	1
47	1	4	15	98	28	210	56	70	27	2	1
48	1	4	15	99	21	231	21	105	6	9	0
49	1	4	16	91	49	175	91	49	34	1	1
50	1	4	16	92	42	196	56	84	13	8	0
51	1	4	17	84	70	140	126	28	41	0	1
52	1	4	17	85	63	161	91	63	20	7	0
53	1	4	18	78	84	126	126	42	27	6	0
54	1	4	19	71	105	91	161	21	34	5	0
55	1	4	20	64	126	56	196	0	41	4	0
56	1	5	9	112	14	210	70	56	33	1	1
57	1	5	9	113	7	231	35	91	12	8	0
58	1	5	10	105	35	175	105	35	40	0	1
59	1	5	10	106	28	196	70	70	19	7	0
60	1	5	11	99	49	161	105	49	26	6	0
61	1	5	12	92	70	126	140	28	33	5	0
62	1	5	13	85	91	91	175	7	40	4	0

Таблица 2.12. Всички възможни спектри на вътрешна точка за ортогонален $6-(10,512)$ масив (Продължение).

63	1	6	3	126	0	210	84	42	39	0	1
64	1	6	4	120	14	196	84	56	25	6	0
65	1	6	5	113	35	161	119	35	32	5	0
66	1	6	6	106	56	126	154	14	39	4	0
67	1	7	0	120	42	126	168	0	45	3	0
68	2	0	17	112	0	224	70	48	38	0	1
69	2	0	18	106	14	210	70	62	24	6	0
70	2	0	19	99	35	175	105	41	31	5	0
71	2	0	20	92	56	140	140	20	38	4	0
72	2	1	12	120	0	210	84	48	30	5	0
73	2	1	13	113	21	175	119	27	37	4	0
74	2	1	14	106	42	140	154	6	44	3	0
75	2	2	7	127	7	175	133	13	43	3	0

Таблица 2.12. Всички възможни спектри на вътрешна точка за ортогонален $6-(10,512)$ масив (Продължение).

0	p_0	p_1	p_2	p_3	p_4	p_5	p_6	p_7	p_8	p_9	p_{10}	p_{11}
1	1	0	10	77	10	168	140	10	93	0	2	1
2	1	0	10	78	3	189	105	45	72	7	1	1
3	1	0	11	71	24	154	140	24	79	6	1	1
4	1	0	11	72	17	175	105	59	58	13	0	1
5	1	0	11	74	4	210	56	94	51	6	5	0
6	1	0	12	64	45	119	175	3	86	5	1	1
7	1	0	12	65	38	140	140	38	65	12	0	1
8	1	0	12	67	25	175	91	73	58	5	5	0
9	1	0	12	68	18	196	56	108	37	12	4	0
10	1	0	12	69	11	217	21	143	16	19	3	0
11	1	0	13	58	59	105	175	17	72	11	0	1
12	1	0	13	60	46	140	126	52	65	4	5	0
13	1	0	13	61	39	161	91	87	44	11	4	0
14	1	0	13	62	32	182	56	122	23	18	3	0
15	1	0	13	63	25	203	21	157	2	25	2	0
16	1	0	14	53	67	105	161	31	72	3	5	0
17	1	0	14	54	60	126	126	66	51	10	4	0
18	1	0	14	55	53	147	91	101	30	17	3	0
19	1	0	14	56	46	168	56	136	9	24	2	0

Таблица 2.13. Всички възможни спектри на вътрешна точка за ортогонален $6-(11,512)$ масив.

20	1	0	15	46	88	70	196	10	79	2	5	0
21	1	0	15	47	81	91	161	45	58	9	4	0
22	1	0	15	48	74	112	126	80	37	16	3	0
23	1	0	15	49	67	133	91	115	16	23	2	0
24	1	0	16	40	102	56	196	24	65	8	4	0
25	1	0	16	41	95	77	161	59	44	15	3	0
26	1	0	16	42	88	98	126	94	23	22	2	0
27	1	0	16	43	81	119	91	129	2	29	1	0
28	1	0	17	33	123	21	231	3	72	7	4	0
29	1	0	17	34	116	42	196	38	51	14	3	0
30	1	0	17	35	109	63	161	73	30	21	2	0
31	1	0	17	36	102	84	126	108	9	28	1	0
32	1	0	18	27	137	7	231	17	58	13	3	0
33	1	0	18	28	130	28	196	52	37	20	2	0
34	1	0	18	29	123	49	161	87	16	27	1	0
35	1	0	19	22	144	14	196	66	23	26	1	0
36	1	0	19	23	137	35	161	101	2	33	0	0
37	1	0	20	16	158	0	196	80	9	32	0	0
38	1	1	5	85	10	154	154	10	85	5	1	1
39	1	1	5	86	3	175	119	45	64	12	0	1
40	1	1	6	79	24	140	154	24	71	11	0	1
41	1	1	6	81	11	175	105	59	64	4	5	0
42	1	1	6	82	4	196	70	94	43	11	4	0
43	1	1	7	72	45	105	189	3	78	10	0	1
44	1	1	7	74	32	140	140	38	71	3	5	0
45	1	1	7	75	25	161	105	73	50	10	4	0
46	1	1	7	76	18	182	70	108	29	17	3	0
47	1	1	7	77	11	203	35	143	8	24	2	0
48	1	1	8	67	53	105	175	17	78	2	5	0
49	1	1	8	68	46	126	140	52	57	9	4	0
50	1	1	8	69	39	147	105	87	36	16	3	0
51	1	1	8	70	32	168	70	122	15	23	2	0
52	1	1	9	61	67	91	175	31	64	8	4	0
53	1	1	9	62	60	112	140	66	43	15	3	0
54	1	1	9	63	53	133	105	101	22	22	2	0
55	1	1	9	64	46	154	70	136	1	29	1	0

Таблица 2.13. Всички възможни спектри на вътрешна точка за ортогонален $6-(11,512)$ масив (Продължение).

56	1	1	10	54	88	56	210	10	71	7	4	0
57	1	1	10	55	81	77	175	45	50	14	3	0
58	1	1	10	56	74	98	140	80	29	21	2	0
59	1	1	10	57	67	119	105	115	8	28	1	0
60	1	1	11	48	102	42	210	24	57	13	3	0
61	1	1	11	49	95	63	175	59	36	20	2	0
62	1	1	11	50	88	84	140	94	15	27	1	0
63	1	1	12	41	123	7	245	3	64	12	3	0
64	1	1	12	42	116	28	210	38	43	19	2	0
65	1	1	12	43	109	49	175	73	22	26	1	0
66	1	1	12	44	102	70	140	108	1	33	0	0
67	1	1	13	36	130	14	210	52	29	25	1	0
68	1	1	13	37	123	35	175	87	8	32	0	0
69	1	1	14	30	144	0	210	66	15	31	0	0
70	1	2	0	93	10	140	168	10	77	10	0	1
71	1	2	1	88	18	140	154	24	77	2	5	0
72	1	2	1	89	11	161	119	59	56	9	4	0
73	1	2	1	90	4	182	84	94	35	16	3	0
74	1	2	2	81	39	105	189	3	84	1	5	0
75	1	2	2	82	32	126	154	38	63	8	4	0
76	1	2	2	83	25	147	119	73	42	15	3	0
77	1	2	2	84	18	168	84	108	21	22	2	0
78	1	2	2	85	11	189	49	143	0	29	1	0
79	1	2	3	75	53	91	189	17	70	7	4	0
80	1	2	3	76	46	112	154	52	49	14	3	0
81	1	2	3	77	39	133	119	87	28	21	2	0
82	1	2	3	78	32	154	84	122	7	28	1	0
83	1	2	4	69	67	77	189	31	56	13	3	0
84	1	2	4	70	60	98	154	66	35	20	2	0
85	1	2	4	71	53	119	119	101	14	27	1	0
86	1	2	5	62	88	42	224	10	63	12	3	0
87	1	2	5	63	81	63	189	45	42	19	2	0
88	1	2	5	64	74	84	154	80	21	26	1	0
89	1	2	5	65	67	105	119	115	0	33	0	0
90	1	2	6	56	102	28	224	24	49	18	2	0
91	1	2	6	57	95	49	189	59	28	25	1	0
92	1	2	6	58	88	70	154	94	7	32	0	0

Таблица 2.13. Всички възможни спектри на вътрешна точка за ортогонален $6-(11,512)$ масив (Продължение).

93	1	2	7	50	116	14	224	38	35	24	1	0
94	1	2	7	51	109	35	189	73	14	31	0	0
95	1	2	8	44	130	0	224	52	21	30	0	0
96	1	3	0	70	88	28	238	10	55	17	2	0
97	1	3	0	71	81	49	203	45	34	24	1	0
98	1	3	0	72	74	70	168	80	13	31	0	0
99	1	3	1	64	102	14	238	24	41	23	1	0
100	1	3	1	65	95	35	203	59	20	30	0	0
101	1	3	2	58	116	0	238	38	27	29	0	0

Таблица 2.13. Всички възможни спектри на вътрешна точка за ортогонален $6-(11,512)$ масив (Продължение).

С помощта на илюстрираната в горните примери техника са пресметнати възможните спектри на всички ортогонални масиви от Таблица 1.1. за $n \leq 15$. Създадена е библиотека от резултати, която авторът е готов да предостави при поискване.

Глава 3

Метод за редуциране на възможните спектри на ортогонални масиви в $\mathbb{H}(n, 2)$

В тази глава са получени зависимости между спектрите на ортогонални масиви със съседни дължини. Намерените условия ще използваме в теглови алгоритъм, за да намалим броя на възможните спектри на даден дизайн. Ако за един $\tau - (n, M)$ ортогонален масив успеем да отхвърлим всички възможности за спектри, тогава разглежданият ортогонален масив не съществува. От Свойство 5. ще следва още, че няма да съществуват и ортогонални масиви с параметри $\tau - (n', M)$ за всяко $n' \geq n$. Също така, от Свойство 6. и Теорема 1.2.4 получаваме, че няма да съществуват и ортогонални $(\tau + 1) - (n', 2M)$ масиви, където $n' \geq n + 1$.
Един ортогонален масив с параметри $\tau - (n, M)$ и теглово разпределение $w(\mathbf{0}) = (w_0, w_1, \ldots, w_n)$ съществува точно когато съществува ортогонален $\tau - (n, M)$ масив с теглово разпределение $(w_n, w_{n-1}, \ldots, w_0)$. Това е ясно от Свойство 4. на ортогоналните масиви, когато на всеки стълб разменим нулите и единиците.
Да напомним, че разглеждаме само ортогонални масиви с поне един нулев ред, т.е. $w_0 \geq 1$.

3.1 Зависимости между спектрите на ортогонален масив с дължини n и $n - 1$

Нека C е ортогонален $\tau - (n, M)$ масив, където $\tau < n$. Нека C има теглово разпределение $w(\mathbf{0}) = (w_0, w_1, \ldots, w_n)$. От Свойство 5. на ортогоналните масиви следва, че при премахването на кой да е стълб на C ще получим масив с параметри $\tau-(n-1, M)$ и същия индекс $\lambda = \dfrac{M}{2^\tau}$ като на изходния дизайн. Новополучения масив

ще бележим с C', а неговото теглово разпределение с $w'(\mathbf{0}) = (w'_0, w'_1, \ldots, w'_{n-1})$. При тази конструкция е ясно, че $w'_0 \geq w_0 \geq 1$.

Дефиниция 3.1.1. *За всяко фиксирано число $i \in \{0, 1, \ldots, n\}$ ще наричаме i-блок подматрицата на C с размери $w_i \times n$, която се състои от всички редове на C с тегло i. За фиксиран стълб на матрицата C с x_i (y_i) ще означаваме броя на единиците (нулите) в този стълб, които принадлежат на i-блока.*

Теорема 3.1.2. *Нека $C \subset \mathbb{H}(n,2)$ е ортогонален масив с параметри $\tau - (n, M)$ и теглово разпределение $w(\mathbf{0}) = (w_0, w_1, \ldots, w_n)$. Нека C' е ортогонален масив с параметри $\tau-(n-1, M)$ и теглово разпределение $w'(\mathbf{0}) = (w'_0, w'_1, \ldots, w'_{n-1})$, получен при отрязването на кой да е стълб на C. В означенията на Дефиниция 3.1.1 да разгледаме системата линейни уравнения*

$$\left|\begin{array}{l} x_i + y_i = w_i, i = 1, 2, \ldots, n-1 \\ x_{i+1} + y_i = w'_i, i = 0, 1, \ldots, n-1 \\ y_0 = w_0 \\ x_n = w_n \\ x_i, y_i \in \mathbb{Z}, x_i \geq 0, y_i \geq 0, i = 0, \ldots, n \end{array}\right. \tag{3.1.1}$$

с неизвестни $x_i, y_i, i = 0, \ldots, n$. Ортогоналният масив C с параметри $\tau - (n, M)$ съществува, ако системата (3.1.1) има решение.

Нещо повече, нека $(x_0^{(r)} = 0, x_1^{(r)}, \ldots, x_n^{(r)}; y_0^{(r)}, y_1^{(r)}, \ldots, y_{n-1}^{(r)}, y_n^{(r)} = 0)$, $r = 1, \ldots, s$, са всички s решения на системата (3.1.1) за всички възможни C', получени от C при премахване на някой негов стълб. Тогава системата

$$\left|\begin{array}{llll} k_1 & +k_2 & +\ldots & +k_s & = n \\ k_1 x_1^{(1)} & +k_2 x_1^{(2)} & +\ldots & +k_s x_1^{(s)} & = w_1 \\ k_1 x_2^{(1)} & +k_2 x_2^{(2)} & +\ldots & +k_s x_2^{(s)} & = 2w_2 \\ \vdots & & & & \\ k_1 x_n^{(1)} & +k_2 x_n^{(2)} & +\ldots & +k_s x_n^{(s)} & = nw_n \\ k_j \in \mathbb{Z}, & k_j \geq 0, & j = 1, & \ldots, s & \end{array}\right. \tag{3.1.2}$$

спрямо неизвестните $k_1, k_2, \ldots, k_s$ има решение.

Доказателство:

От Дефиниция 3.1.1 са изпълнени следните тъждества:

$$x_i + y_i = w_i, \quad i = 1, \ldots, n-1, \quad x_n = w_n, \quad y_0 = w_0.$$

Вземайки предвид конструкцията на C', редовете на новополучения масив с тегло i са съвкупност от тези с тегло i в изходния масив и 0 на съответния отрязан стълб заедно с тези с тегло $i-1$ в изходния масив с 1 на премахнатия стълб. С други думи, в сила са равенствата $x_{i+1} + y_i = w'_i, i = 0, \ldots, n-1$.

Нека за всички възможни отрязвания на някой стълб, т.е. за всички възможни w', системата (3.1.1) има s решения, които съгласно условието са $(x_0^{(r)} = 0, x_1^{(r)}, \ldots, x_n^{(r)};$

$y_0^{(r)}, y_1^{(r)}, \ldots, y_{n-1}^{(r)}, y_n^{(r)} = 0)$, $r = 1, 2, \ldots, s$. Да означим с k_r броя на стълбовете, които съответстват на r-тото решение на системата, $r = 1, \ldots, s$. Нека за фиксирано i да разгледаме i-блока. Броят на единиците в него е точно iw_i. От друга страна, като вземем предвид, че x_i е точно броят на думите от i-блока, които имат 1 на съответния стълб, то броят на единиците в i-блока е равен също така на $k_1 x_i^{(1)} + k_2 x_i^{(2)} + \cdots + k_s x_i^{(s)}$. Следователно за всяко $i = 0, \ldots, s$ са изпълнени равенствата в система (3.1.2). □

Забележка 3.1.3. *Нека $C \subset \mathbb{H}(n, 2)$ е ортогонален масив с параметри $\tau - (n, M)$. От Свойство 6. на ортогоналните масиви имаме, че при премахване на един стълб на C ще получим два ортогонални масиви с параметри $(\tau - 1) - (n - 1, M/2)$. Първият масив ще се състои от редовете на C, в които на отрязания стълб са имали фиксиран елемент 0. Тогава съгласно означенията по-горе, тегловото разпределение на новополучения масив е точно $(y_0, y_1, \ldots, y_{n-1})$. Аналогично ако разгледаме редовете на C, които са имали 1 на премахнатия стълб, ще получим ортогонален масив с параметри $(\tau - 1) - (n - 1, M/2)$ и теглово разпределение $(x_1, x_2, \ldots, x_n)$. Лесно се проверява, че първият масив има поне толкова нулеви реда, колкото и оригиналният. За втория масив не може да сме сигурни дали ще има нулев ред, за сметка на това има поне толкова реда само с единици, колкото и в C.*

Тези нови ограничения върху тегловите разпределения на масива C и получените по-горе два масива от него с теглови разпределения съответно $(x_1, x_2, \ldots, x_n)$ и $(y_0, y_1, \ldots, y_{n-1})$ се оказва, че са изпълнени винаги за изследваните от нас масиви и не водят до по-силни резултати от изложените по-долу.

Забележка 3.1.4. *Ако C е $2u - (n, M)$ ортогонален масив, то от Теорема 1.2.4 следва, че масивът $\widetilde{C}$, получен от стълбовете на C с добавен нулев стълб, последвани от допълнението $\bar{C}$ на C с добавен стълб от единици, е ортогонален масив с параметри $(2u + 1) - (n + 1, 2M)$. Ако $w(\mathbf{0}) = (w_0, w_1, \ldots, w_n)$ е тегловото разпределение на C, съответно $(w_n, w_{n-1}, \ldots, w_0)$ е тегловото разпределение на $\bar{C}$, тогава тегловото разпределение на $\widetilde{C}$ е $(w_0, w_1 + w_n, w_2 + w_{n-1}, \ldots, w_{n-1} + w_2, w_n + w_1, w_0)$. В частност, ако изключим като възможност фиксирания спектър на $\widetilde{C}$, тогава и спектърът $w(\mathbf{0})$ на C няма да бъде възможен.*

Прилагането на получените зависимости между спектрите на масиви със съседни дължини (Теорема 3.1.2) ще доведе до редуциране на възможните спектри на даден $\tau - (n, M)$ ортогонален масив (дизайн) C. Тази техника е приложена в описания в следващия параграф теглови алгоритъм.

3.2 Теглови алгоритъм

Нека C е ортогонален $\tau - (n, M)$ масив. С помощта на Теорема 2.1.2 намираме всички възможни спектри за вътрешна точка за всички ортогонални масиви в редицата $\tau - (\tau, M), \tau - (\tau + 1, M), \ldots, \tau - (n, M)$. За всяка съседна двойка може

да приложим Теорема 3.1.2. За дадено теглово разпределение $w(\mathbf{0})$ на C и всички възможни теглови разпределения $w'(\mathbf{0})$ на C', получени от C, решаваме съответните системи (3.1.1). Ако за всички спектри $w'(\mathbf{0})$ горните системи нямат решение, то разглежданият $w(\mathbf{0})$ не е възможен спектър на масива C. Ако за някои спектри $w'(\mathbf{0})$ на C' системите от вида (3.1.1) имат решение, но съответната система (3.1.2) няма решение, то спектърът $w(\mathbf{0})$ на масива C отново се отхвърля. В противен случай спектърът $w(\mathbf{0})$ на C остава. Можем да започнем да прилагаме този алгоритъм от коя да е двойка съседни масиви, но за удобство ще започваме винаги от първата двойка масиви в редицата по-горе.

Забележка 3.2.1. *Ясно е, че системата (3.1.1) не е необходимо да се решава в случаите, когато* $w_0 > w'_0$ *или* $w_n > w'_{n-1}$, *тъй като тези неравенства са невъзможни в описаната конструкция.*

Както вече споменахме в предния параграф, подробно ще опишем представения теглови алгоритъм за ортогоналния масив с параметри $5-(9,128)$.

Пример 3.2.2. *(Продължение на Пример 2.2.3) Да напомним, че в Пример 2.2.3 вече са пресметнати всички възможни спектри на вътрешна точка за всеки масив от редицата* $5-(5,128), 5-(6,128), 5-(7,128), 5-(8,128), 5-(9,128)$. *Броят на възможните спектри за всеки един масив в горната редица е съответно* $1,4,6,7,6$. *Прилагайки тегловия алгоритъм, ще редуцираме този брой до* $1,4,6,7,1$. *На практика само на последната стъпка има редукция, но тя е достатъчно силна и води до спектъра на единствения съществуващ ортогонален масив с тези параметри.*

Ще илюстрираме тегловия алгоритъм върху последните две двойки от горната редица. Първо да разгледаме двойката $5-(7,128)$ и $5-(8,128)$. За всяка от седемте възможности на теглово разпределение за C проверяваме дали някой от шестте спектъра на C' няма да успее да удовлетвори Теорема 3.1.2.
Започваме с $w(\mathbf{0}) = (1,0,27,6,55,20,13,6,0)$ на масива $5-(8,128)$. За четири от шестте спектъра $w'(\mathbf{0})$ на C' системите от вида (3.1.1) нямат решение. В останалите два случая, а именно за спектър $w'(\mathbf{0}) = (1,6,27,20,55,6,13,0)$ на C' получаваме решение $(0,0,6,6,20,20,6,6,0;\ 1,0,21,0,35,0,7,0,0)$ и за $w'(\mathbf{0}) = (1,7,21,35,35,21,7,1)$ съответното решение е $(0,0,7,1,30,10,11,5,0;\ 1,0,20,5,25,10,2,1,0)$. Системата (3.1.2) изглежда по следния начин:

$$\left|\begin{array}{llll} k_1 & +k_2 & = & 8 \\ 0k_1 & +0k_2 & = & 0 \\ 6k_1 & +7k_2 & = & 54 \\ 6k_1 & +k_2 & = & 18 \\ 20k_1 & +30k_2 & = & 220 \\ 20k_1 & +10k_2 & = & 100 \\ 6k_1 & +11k_2 & = & 78 \\ 6k_1 & +5k_2 & = & 42 \\ 0k_1 & +0k_2 & = & 0 \\ k_j \in \mathbb{Z}, & k_j \geq 0, & j=1,2 & \end{array}\right.$$

Решението на тази система е единствено: $(2, 6)$. Това означава, че при рязането на стълбове на масива C два пъти ще получим масив със спектър $(1, 6, 27, 20, 55, 6, 13, 0)$. В останалите шест случая това ще бъде $5-(7, 128)$ дизайн с теглово разпределение $w'(\mathbf{0}) = (1, 7, 21, 35, 35, 21, 7, 1)$.
Да проследим още един случай за тази двойка. Нека $w(\mathbf{0}) = (1, 1, 21, 21, 35, 35, 7, 7, 0)$ е спектър на масива $5-(8, 128)$. В този случай системите от вида (3.1.1) имат решение за четири от шестте спектъра на C'. Съответните четири решения за $(x; y)$ са:

$(0, 0, 5, 11, 10, 30, 1, 7, 0; 1, 1, 16, 10, 25, 5, 6, 0, 0)$,

$(0, 0, 6, 6, 20, 20, 6, 6, 0; 1, 1, 15, 15, 15, 15, 1, 1, 0)$,

$(0, 1, 0, 21, 0, 35, 0, 7, 0; 1, 0, 21, 0, 35, 0, 7, 0, 0)$ и

$(0, 1, 1, 16, 10, 25, 5, 6, 0; 1, 0, 20, 5, 25, 10, 2, 1, 0)$.

С тях конструираме системата (3.1.2) от Теорема 3.1.2 относно неизвестните $k_i, i = 1, 2, 3, 4$.

$$\left|\begin{array}{lllll} k_1 & +k_2 & +k_3 & +k_4 & = 8 \\ 0k_1 & +0k_2 & +k_3 & +k_4 & = 1 \\ 5k_1 & +6k_2 & +0k_3 & +k_4 & = 42 \\ 11k_1 & +6k_2 & +21k_3 & +16k_4 & = 63 \\ 10k_1 & +20k_2 & +0k_3 & +10k_4 & = 140 \\ 30k_1 & +20k_2 & +35k_3 & +25k_4 & = 175 \\ k_1 & +6k_2 & +0k_3 & +5k_4 & = 42 \\ 7k_1 & +6k_2 & +7k_3 & +6k_4 & = 49 \\ 0k_1 & +0k_2 & +0k_3 & +0k_4 & = 0 \\ k_j \in \mathbb{Z}, & k_j \geq 0, & j = 1, 2, 3, 4 & & \end{array}\right.$$

Решението на тази система има параметричен вид: $(p, 7-p, 1-p, p)$, като възможностите за p са две: 0 и 1. Следователно не е еднозначно определено масиви C' с какви теглови разпределения ще се получат при премахването на някой стълб на разглеждания масив C със спектър $w(\mathbf{0}) = (1, 0, 27, 6, 55, 20, 13, 6, 0)$.
Останалите случаи няма да ги описваме подробно. За всяка разглеждана двойка $w(\mathbf{0})$ и $w'(\mathbf{0})$, спектри съответно на $5-(8, 128)$ и $5-(7, 128)$ системите от вида (3.1.1) имат поне едно решение, а оттам съответната система (3.1.2) от Теорема 3.1.2 има решение и следователно всички 7 спектъра на $5-(8, 128)$ остават.

Да продължим прилагането на алгоритъма за двойката C' с параметри $5-(8, 128)$ и C с параметри $5-(9, 128)$. Да отбележим, че ако на предишната стъпка бяхме успели да отсеем някои от възможностите за $5-(8, 128)$, щяхме да продължим работата с редуцираните възможности. В конкретния случай това не е така.
Първата възможна стойност за спектър на C е $w(\mathbf{0}) = (1, 0, 7, 38, 3, 52, 17, 6, 4, 0)$. Няма нито един спектър $w'(\mathbf{0})$ на C', за който системата от вида (3.1.1) да има неотрицателно решение. Следователно разглеждания спектър $w(\mathbf{0})$ на C го отхвърляме. Следващата възможност за спектър на C е $w(\mathbf{0}) = (1, 0, 8, 32, 18, 32, 32, 0, 5, 0)$. За този спектър и всички $w'(\mathbf{0})$ на C' системите от вида (3.1.1) са несъвместими.

Следващият разглеждан спектър на C е $w(\mathbf{0}) = (1,0,9,27,27,27,27,9,0,1)$. Получаваме три решения за $(x;y)$ на системите (3.1.1). С тях съставяме системата (3.1.2)

$$\left|\begin{array}{lll} k_1 & +k_2 & +k_3 = 9 \\ 0k_1 & +0k_2 & +0k_3 = 0 \\ k_1 & +2k_2 & +3k_3 = 18 \\ 14k_1 & +9k_2 & +4k_3 = 81 \\ 2k_1 & +12k_2 & +22k_3 = 108 \\ 25k_1 & +15k_2 & +5k_3 = 135 \\ 13k_1 & +18k_2 & +23k_3 = 162 \\ 8k_1 & +7k_2 & +6k_3 = 63 \\ 0k_1 & +0k_2 & +0k_3 = 0 \\ k_1 & +k_2 & +k_3 = 9 \\ k_j \in \mathbb{Z}, & k_j \geq 0, & j = 1,2,3 \end{array}\right.$$

Решението на тази система е $(p, 9-2p, p)$. Вижда се, че това решение има смисъл в неотрицателни числа, следователно този спектър остава като възможност.
За следващия спектър $w(\mathbf{0}) = (1,0,10,21,42,7,42,3,1,1)$ на C има единствен спектър $w'(\mathbf{0}) = (1,2,16,30,30,30,16,2,1)$ на C', за който системата (3.1.1) има решение. Системата (3.1.2) относно k_1 има вида:

$$\left|\begin{array}{ll} k_1 & = 9 \\ 0k_1 & = 0 \\ 2k_1 & = 20 \\ \vdots & \end{array}\right.$$

Очевидно тази система няма решение, така че и този спектър се отхвърля.
Разглеждаме спектъра $w(\mathbf{0}) = (1,1,3,42,7,42,21,10,0,1)$ на C. Отново само за един спектър $w'(\mathbf{0}) = (1,2,16,30,30,30,16,2,1)$ на C' системата (3.1.1) има решение и то е $(0,0,1,14,2,25,13,8,0,1;\ 1,1,2,28,5,17,8,2,0,0)$. Тогава системата (3.1.2) има вида:

$$\left|\begin{array}{ll} k_1 & = 9 \\ 0k_1 & = 1 \\ 1k_1 & = 6 \\ \vdots & \end{array}\right.$$

Тази система няма решение. Остава да разгледаме последната възможност за спектър на C, а именно $w(\mathbf{0}) = (1,1,4,36,22,22,36,4,1,1)$. В този случай имаме два спектъра $w'(\mathbf{0})$ на C', за които системите от вида (3.1.1) имат решение. Съответната система (3.1.2) има следния вид:

$$\left|\begin{array}{lll} k_1 & +k_2 & = 9 \\ 0k_1 & +0k_2 & = 1 \\ k_1 & +2k_2 & = 8 \\ \vdots & & \end{array}\right.$$

Ясно е, че тази възможност също отпада. Така получихме, че разглежданият $5-(9,128)$ ортогонален масив C има единствен възможен спектър и той е $w(\mathbf{0}) = (1,0,9,27,27,27,27,9,0,1)$. Масив с тези параметри е конструиран от Слоен и може да бъде видян на неговата web-страница.

3.3 Някои резултати от прилагането на тегловия алгоритъм

Ще разгледаме отново примерите от предишната глава и върху тях ще илюстрираме как прилагането на тегловия алгоритъм редуцира броя на възможните им спектри.

Пример 3.3.1. *(Продължение на Пример 2.2.4) Нека C е $6-(10,384)$ ортогонален масив. В Пример 2.2.4 получихме, че броят на възможните спектри за всеки един масив в редицата $6-(6,384), 6-(7,384), 6-(8,384), 6-(9,384), 6-(10,384)$ е съответно $1,6,12,17,22$. След прилагането на тегловия алгоритъм върху вече пресметнатите възможности за спектър на вътрешна точка, получаваме следната редица $1,6,12,9,8$. Все пак остават 8 спектъра, които трябва да бъдат изследвани по-детайлно, за да се определи дали ортогонален масив с такива параметри съществува. По-долу са изложени в табличен вид резултатите след прилагането на тегловия алгоритъм (като са представени само редуцираните таблици).*

0	p_0	p_1	p_2	p_3	p_4	p_5	p_6	p_7	p_8	p_9
1	1	3	45	21	147	63	63	39	0	2
2	1	4	39	35	133	63	77	25	6	1
3	1	5	32	56	98	98	56	32	5	1
4	1	6	25	77	63	133	35	39	4	1
5	1	6	26	70	84	98	70	18	11	0
6	1	7	19	91	49	133	49	25	10	0
7	2	0	39	63	63	147	21	45	3	1
8	2	0	40	56	84	112	56	24	10	0
9	2	1	33	77	49	147	35	31	9	0

Таблица 3.1. Редуцирани възможни спектри на вътрешна точка за ортогонален $6-(9,384)$ масив.

0	p_0	p_1	p_2	p_3	p_4	p_5	p_6	p_7	p_8	p_9	p_{10}
1	1	0	25	40	70	112	70	40	25	0	1
2	1	0	26	34	84	98	70	54	11	6	0
3	1	0	27	27	105	63	105	33	18	5	0
4	1	0	28	20	126	28	140	12	25	4	0
5	1	1	19	55	49	133	49	61	10	6	0
6	1	1	20	48	70	98	84	40	17	5	0
7	1	1	21	41	91	63	119	19	24	4	0
8	1	2	14	62	56	98	98	26	23	4	0

Таблица 3.2. Редуцирани възможни спектри на вътрешна точка за ортогонален $6-(10,384)$ масив.

Пример 3.3.2. *(Продължение на Пример 2.2.5) Нека* C *е ортогонален масив с параметри* $6-(11,512)$. *Както показахме в Пример 2.2.5 броят на възможните спектри за съответната редица от дизайни е* $1,8,20,43,75,101$. *След прилагане на тегловия алгоритъм редуцираме този брой до следната редица от възможности* $1,8,20,39,55,36$. *Резултатите са представени в таблици по-долу.*

0	p_0	p_1	p_2	p_3	p_4	p_5	p_6	p_7	p_8	p_9
1	1	6	56	28	210	56	112	36	5	2
2	1	6	57	21	231	21	147	15	12	1
3	1	7	49	49	175	91	91	43	4	2
4	1	7	50	42	196	56	126	22	11	1
5	1	7	51	35	217	21	161	1	18	0
6	1	8	42	70	140	126	70	50	3	2
7	1	8	43	63	161	91	105	29	10	1
8	1	8	44	56	182	56	140	8	17	0
9	1	9	35	91	105	161	49	57	2	2
10	1	9	36	84	126	126	84	36	9	1
11	1	9	37	77	147	91	119	15	16	0
12	1	10	28	112	70	196	28	64	1	2
13	1	10	29	105	91	161	63	43	8	1
14	1	10	30	98	112	126	98	22	15	0
15	1	11	21	133	35	231	7	71	0	2
16	1	11	22	126	56	196	42	50	7	1
17	1	11	23	119	77	161	77	29	14	0
18	1	12	15	147	21	231	21	57	6	1
19	1	12	16	140	42	196	56	36	13	0

Таблица 3.3. Редуцирани възможни спектри на вътрешна точка за ортогонален $6-(9,512)$ масив.

20	2	0	70	14	210	70	98	42	4	2
21	2	0	71	7	231	35	133	21	11	1
22	2	0	72	0	252	0	168	0	18	0
23	2	1	63	35	175	105	77	49	3	2
24	2	1	64	28	196	70	112	28	10	1
25	2	1	65	21	217	35	147	7	17	0
26	2	2	56	56	140	140	56	56	2	2
27	2	2	57	49	161	105	91	35	9	1
28	2	2	58	42	182	70	126	14	16	0
29	2	3	49	77	105	175	35	63	1	2
30	2	3	50	70	126	140	70	42	8	1
31	2	3	51	63	147	105	105	21	15	0
32	2	4	42	98	70	210	14	70	0	2
33	2	4	43	91	91	175	49	49	7	1
34	2	4	44	84	112	140	84	28	14	0
35	2	5	36	112	56	210	28	56	6	1
36	2	5	37	105	77	175	63	35	13	0
37	2	6	30	126	42	210	42	42	12	0
38	2	7	23	147	7	245	21	49	11	0
39	3	0	44	112	42	224	28	48	11	0

Таблица 3.3. Редуцирани възможни спектри на вътрешна точка за ортогонален $6-(9,512)$ масив. (Продължение)

0	p_0	p_1	p_2	p_3	p_4	p_5	p_6	p_7	p_8	p_9	p_{10}
1	1	0	40	35	105	175	35	105	10	5	1
2	1	0	41	28	126	140	70	84	17	4	1
3	1	0	42	21	147	105	105	63	24	3	1
4	1	0	42	22	140	126	70	98	3	10	0
5	1	0	43	14	168	70	140	42	31	2	1
6	1	0	43	15	161	91	105	77	10	9	0
7	1	0	44	7	189	35	175	21	38	1	1
8	1	0	44	8	182	56	140	56	17	8	0
9	1	0	45	0	210	0	210	0	45	0	1
10	1	0	45	1	203	21	175	35	24	7	0
11	1	1	34	49	91	175	49	91	16	4	1
12	1	1	35	42	112	140	84	70	23	3	1
13	1	1	35	43	105	161	49	105	2	10	0

Таблица 3.4. Редуцирани възможни спектри на вътрешна точка за ортогонален $6-(10,512)$ масив.

14	1	1	36	35	133	105	119	49	30	2	1
15	1	1	36	36	126	126	84	84	9	9	0
16	1	1	37	28	154	70	154	28	37	1	1
17	1	1	37	29	147	91	119	63	16	8	0
18	1	1	38	21	175	35	189	7	44	0	1
19	1	1	38	22	168	56	154	42	23	7	0
20	1	1	39	15	189	21	189	21	30	6	0
21	1	2	27	70	56	210	28	98	15	4	1
22	1	2	28	63	77	175	63	77	22	3	1
23	1	2	28	64	70	196	28	112	1	10	0
24	1	2	29	56	98	140	98	56	29	2	1
25	1	2	29	57	91	161	63	91	8	9	0
26	1	2	30	49	119	105	133	35	36	1	1
27	1	2	30	50	112	126	98	70	15	8	0
28	1	2	31	42	140	70	168	14	43	0	1
29	1	2	31	43	133	91	133	49	22	7	0
30	1	2	32	36	154	56	168	28	29	6	0
31	1	3	21	84	42	210	42	84	21	3	1
32	1	3	21	85	35	231	7	119	0	10	0
33	1	3	22	77	63	175	77	63	28	2	1
34	1	3	22	78	56	196	42	98	7	9	0
35	1	3	23	70	84	140	112	42	35	1	1
36	1	3	23	71	77	161	77	77	14	8	0
37	1	3	24	63	105	105	147	21	42	0	1
38	1	3	24	64	98	126	112	56	21	7	0
39	1	3	25	57	119	91	147	35	28	6	0
40	1	3	26	50	140	56	182	14	35	5	0
41	1	4	15	98	28	210	56	70	27	2	1
42	1	4	15	99	21	231	21	105	6	9	0
43	1	4	16	91	49	175	91	49	34	1	1
44	1	4	16	92	42	196	56	84	13	8	0
45	1	4	17	84	70	140	126	28	41	0	1
46	1	4	17	85	63	161	91	63	20	7	0
47	1	4	18	78	84	126	126	42	27	6	0
48	1	4	19	71	105	91	161	21	34	5	0
49	1	5	10	105	35	175	105	35	40	0	1
50	1	5	10	106	28	196	70	70	19	7	0

Таблица 3.4. Редуцирани възможни спектри на вътрешна точка за ортогонален $6-(10,512)$ масив. (Продължение)

51	1	5	11	99	49	161	105	49	26	6	0
52	1	5	12	92	70	126	140	28	33	5	0
53	1	6	6	106	56	126	154	14	39	4	0
54	2	0	19	99	35	175	105	41	31	5	0
55	2	0	20	92	56	140	140	20	38	4	0

Таблица 3.4. Редуцирани възможни спектри на вътрешна точка за ортогонален $6-(10,512)$ масив. (Продължение)

0	p_0	p_1	p_2	p_3	p_4	p_5	p_6	p_7	p_8	p_9	p_{10}	p_{11}
1	1	0	11	72	17	175	105	59	58	13	0	1
2	1	0	12	65	38	140	140	38	65	12	0	1
3	1	0	12	67	25	175	91	73	58	5	5	0
4	1	0	12	68	18	196	56	108	37	12	4	0
5	1	0	12	69	11	217	21	143	16	19	3	0
6	1	0	13	58	59	105	175	17	72	11	0	1
7	1	0	13	60	46	140	126	52	65	4	5	0
8	1	0	13	61	39	161	91	87	44	11	4	0
9	1	0	13	62	32	182	56	122	23	18	3	0
10	1	0	14	54	60	126	126	66	51	10	4	0
11	1	0	14	55	53	147	91	101	30	17	3	0
12	1	0	14	56	46	168	56	136	9	24	2	0
13	1	0	15	47	81	91	161	45	58	9	4	0
14	1	0	15	48	74	112	126	80	37	16	3	0
15	1	0	15	49	67	133	91	115	16	23	2	0
16	1	0	16	40	102	56	196	24	65	8	4	0
17	1	0	16	41	95	77	161	59	44	15	3	0
18	1	0	16	42	88	98	126	94	23	22	2	0
19	1	0	17	34	116	42	196	38	51	14	3	0
20	1	0	17	35	109	63	161	73	30	21	2	0
21	1	0	17	36	102	84	126	108	9	28	1	0
22	1	0	18	27	137	7	231	17	58	13	3	0
23	1	0	18	28	130	28	196	52	37	20	2	0
24	1	0	18	29	123	49	161	87	16	27	1	0
25	1	0	19	23	137	35	161	101	2	33	0	0
26	1	1	8	68	46	126	140	52	57	9	4	0
27	1	1	8	69	39	147	105	87	36	16	3	0
28	1	1	9	61	67	91	175	31	64	8	4	0

Таблица 3.5. Редуцирани възможни спектри на вътрешна точка за ортогонален $6-(11,512)$ масив.

29	1	1	9	62	60	112	140	66	43	15	3	0
30	1	1	9	63	53	133	105	101	22	22	2	0
31	1	1	10	55	81	77	175	45	50	14	3	0
32	1	1	10	56	74	98	140	80	29	21	2	0
33	1	1	10	57	67	119	105	115	8	28	1	0
34	1	1	11	49	95	63	175	59	36	20	2	0
35	1	1	11	50	88	84	140	94	15	27	1	0
36	1	1	12	43	109	49	175	73	22	26	1	0

Таблица 3.5. Редуцирани възможни спектри на вътрешна точка за ортогонален $6-(11,512)$ масив. (Продължение)

С помощта на тегловия алгоритъм са редуцирани възможностите за спектри на всички ортогонални масиви от Таблица 1.1. за $n \leq 15$. Създадена е библиотека от резултати, която при поискване авторът е готов да предостави.

Да отбележим, че такива техники са използвани от Бойваленков и Кулина в [5], [6], и [14].

Глава 4

Приложения на ортогоналните масиви в други области на математиката

Тъй като може да разглеждаме $\mathbb{H}(n,2)$ като n-дизайн, то произволен τ-дизайн в $\mathbb{H}(n,2)$ за $\tau < n$ е апроксимация на цялото пространство $\mathbb{H}(n,q)$. Това обяснява успешното приложение на ортогоналните масиви в статистиката [20], в теория на кодирането [19] и криптографията [13].

Основна връзка [9, 19] между кодовете, коригиращи грешки, и τ-дизайните в $\mathbb{H}(n,2)$ е, че за всеки линеен код C с максимална сила τ е изпълнено равенството $\tau = d^{\perp} - 1$, където $d^{\perp}$ е минималното разстояние на дулния код на C.

Нещо повече, в [13] са описани редица свойства и конструкции на ортогонални масиви, които показват връзките на ортогоналните масиви с комбинаториката, теория на крайните полета, теория на кодирането и криптографията.

По-подробно ще се спрем на зависимостите между кодове, разностни схеми, матрици на Адамар и ортогоналните масиви, тъй като тези обекти са по-широко изследвани, а някои техни свойства и конструкции могат да бъдат приложени за изследването на ортогоналните масиви. Накрая ще скицираме основната идея за използването на ортогонални масиви в статистиката, тъй като от там е тръгнало изследването на разглежданите от нас ортогонални масиви.

4.1 Използване на ортогонални масиви в криптографията

Основните приложения на ортогоналните масиви в криптографията са при дерандомизация на алгоритми, тестване на случайни модели на VLSI чипове, кодове за автентичност, универсални хеш функции, схеми за разпределяне на секретни данни

(threshold schemes) и други. В този параграф ще се спрем по-подробно на приложението на ортогоналните масиви в кодовете за автентичност и универсалните хеш функции.

Първият пример, който ще разгледаме, е публичен код за автентичност. Кодовете за автентичност са въведени за пръв път през 1974г. от Гилберт, МакУилямс и Слоен [11]. В обичайния модел има трима участници: Алис, Боб и противник (Оскар). Алис иска да размени информация с Боб, използвайки публичен канал. Целта на ауторизацията е да се запази цялостта на предадената информация. Когато Боб получи съобщение, той иска да е сигурен, че съобщението е наистина от Алис и не е подправено. От друга страна Оскар има способността да атакува канала като праща съобщения или променя съществуващи съобщения. За по-формално описание, въвеждаме следната дефиниция:

Дефиниция 4.1.1. *Публичен код за автентичност наричаме наредената четворка* $(\mathcal{S}, \mathcal{A}, \mathcal{K}, \mathcal{E})$*, такава че*

1. $\mathcal{S}$ *е крайно множество от входящи съобщения (source states) и нека* $|\mathcal{S}| = k$*.*
2. $\mathcal{A}$ *е крайно множество от* l *удостоверения (authenticators).*
3. $\mathcal{K}$ *е крайно множество от ключове.*
4. *За всеки ключ* $K \in \mathcal{K}$ *съществува правило за верификация (authentication rule)* $e_K \in \mathcal{E}, e_K : \mathcal{S} \to \mathcal{A}$*.*

Алис и Боб следват следните правила. Първо, заедно избират таен ключ $K \in \mathcal{K}$. По-късно Алис иска да изпрати някое входящо съобщение $s \in \mathcal{S}$ до Боб. Алис използва правилото за верификация e_K, за да създаде удостоверението $a = e_K(s)$ и изпраща съобщение $m = (s, a)$ по канала до Боб. Когато Боб получи съобщението m, проверява дали $a = e_K(s)$, и ако е така, приема, че Алис е изпратила входящото съобщение s. Тъй като всяко правило за верификация е функция от $\mathcal{S}$ към $\mathcal{A}$, то можем да представим кода за автентичност с една $|\mathcal{E}| \times |\mathcal{S}|$ матрица, в която редовете са индексирани от верифициращите правила, а стълбовете са входящите съобщения. Така даден елемент на ред e и стълб s е $e(s)$. Получената матрица наричаме матрица на истинност.

Когато Оскар реши да атакува съобщението на Алис, той изпаща свое съобщение или прави промяна в изпратеното от Алис съобщение. Изпратеното от Оскар съобщение е някое $m' = (s', a')$, което достига до Боб. Боб ще се заблуди, че това е оригиналното съобщение от Алис единствено когато Оскар (без да знае правилото за верификация e) е успял да удовлетвори условието $a' = e(s')$.

Предполагаме, че съществува вероятностно разпределение върху $\mathcal{S}$, което се знае от всички участници. Използвайки го, Алис и Боб ще изберат вероятностно разпределение за $\mathcal{E}$, което ще наричаме стратегия за истинност (authentication strategy). След като изберат своята стратегия, те могат да пресметнат вероятностите за измама P_{d_0} и P_{d_1}, съответни на Оскар да е заблудил Боб посредством свое съобщение или посредством промяна на част от изпратеното от Алис до Боб съобщение.

Не е трудно да се покаже, че $P_{d_0} \geq 1/|\mathcal{A}|$ и $P_{d_1} \geq 1/|\mathcal{A}|$ (вж. [21], [24]). Нашата основна цел е да минимизираме вероятностите за измама, както и броя на правилата за верификация, тъй като това определя количеството информация, което Алис и Боб могат да си предават по сигурен начин преди да използват кодове за автентичност. Основната връзката между публичните кодове за автентичност и ортогоналните масиви е представена в следната теорема.

Теорема 4.1.2. *[22] Нека са дадени публичен код за автентичност с k входящи съобщения и l удостоверения, като вероятностите за измама са съответно $P_{d_0} = P_{d_1} = 1/l$. Тогава*

1. *$|\mathcal{E}| \geq l^2$ като равенство се достига тогава и само тогава когато матрицата на истинност е ортогонален масив с параметри $2-(k, l^2, l)$ и индекс $\lambda = 1$.*
2. *$|\mathcal{E}| > k(l-1)1$ като равенство се достига тогава и само тогава когато матрицата на истинност е ортогонален масив с параметри $2-(k, \lambda l^2, l)$, където*

$$\lambda = \frac{k(l-1)+1}{l^2}.$$

Да отбележим, че в горните случаи правилата за верификация са използвани с еднаква вероятност.

Друга употреба на ортогоналните масиви в криптографията е създаването на добри хеш функции [12]. Нека A и B са крайни множества, за които мощността на A е по-голяма от тази на B. Всяка функция $h : A \to B$ се нарича *хеш функция*. Когато на един елемент от B са съпоставени повече от един елемента на A, казваме, че е настъпила колизия. Разглеждат се хеш функции, при които броят на колизиите е минимален.

Дефиниция 4.1.3. *Фамилия от хеш функции $H = \{h : A \to B\}$ се нарича универсална, ако за всеки два различни елемента $x \neq y \in A$, вероятността*

$$P(h(x) = h(y)) \leq \frac{1}{|B|},$$

т.е. вероятността за колизии е не повече от $1/|B|$.

Дефиниция 4.1.4. *Една крайна фамилия от хеш функции $H = \{h : A \to B\}$ ще наричаме силно универсална от втори род ($strongly - universal_2$) и ще означаваме с SU_2, ако за всеки два различни елемента $x_1 \neq x_2 \in A$ и за всеки два елемента $y_1, y_2 \in B$ е в сила*

$$|\{h \in H | h(x_1) = y_1, h(x_2) = y_2\}| = \frac{|H|}{|B|^2}.$$

За практически изследвания е важно фамилията да бъде с малко елементи. Това се налага поради необходимостта от $log_2|H|$ бита за определяне на дадена хеш функция от фамилията. Може да се покаже, че SU_2 хеш функциите са еквивалентни с ортогонални масиви.

Теорема 4.1.5. *[23] Ако съществува ортогонален масив с параметри* $2-(n,M,q)$ *и индекс* λ*, тогава съществува и* SU_2 *фамилия* H *от хеш функции от* A *към* B*, където* $|A|=n$*,* $|B|=q$ *и* $|H|=\lambda q^2$*. Обратно, ако съществува* SU_2 *фамилия* H *от хеш функции от* A *към* B*, то съществува ортогонален масив* $2-(|A|,M,|B|)$ *с индекс* $\lambda=|H|/|B|^2$*.*

4.2 Връзки между ортогонални масиви и кодове

Връзката между ортогоналните масиви и кодовете най-силно се илюстрира от факта, че кодовите думи на даден код могат да бъдат разгледани като редове на някой ортогонален масив и обратно. Основно предимство да сравняваме двата обекта е, че голяма част от границите, които са в сила за ортогонални масиви, са следствие от изследването на кодовете. Такава е например границата на Делсарт за линейното програмиране [7], която е не по-слаба от неравенството на Рао, дори в общия случай постига по-добри резултати. Теория на кодирането и теорията на ортогоналните масиви исторически погледнато започват сравнително по едно и също време. С кодове са се занимавали доста повече учени и някои добре известни резултати за кодове често се пренасят върху ортогоналните масиви за конструиране на редици от ортогонални масиви. В тази глава отново ще се върнем към дефиницията на ортогонален масив в общия случай, т.е. работим с масиви над някаква азбука $Q=\{0,1,\ldots,q-1\}$ с q елемента.

На всеки $\tau-(n,M,q)$ ортогонален масив може да съпоставим код, който се формира от неговите редове. Това ще бъде $(n,M,d)_q$ код за някое минимално разстояние d. Обратно, на всеки един $(n,M,d)_q$ код асоцииране $M\times n$ матрица, чиито редове представляват кодовите думи. Тогава за някое τ получената матрица ще се превърне в $\tau-(n,M,q)$ ортогонален масив.

За да се направи съпоставка между ортогонални масиви и линейни кодове, се въвежда и дефиницията за линеен ортогонален масив.

Дефиниция 4.2.1. *Нека* q *е просто число. Един ортогонален масив* C *с параметри* $\tau-(n,M,q)$ *и с елементи от полето* $GF(q)$ *(с* q *елемента) се нарича линеен, ако редовете му са неповтарящи се и разглеждайки ги като елементи на* $(GF(q))^n$*, всичките* M *реда формират линейно пространство над* $GF(q)$*. С други думи за всеки два реда* R_1 *и* R_2 *на масива* C*, елементът* $c_1R_1+c_2R_2$ *също е ред от масива за произволни елементи* c_1 *и* c_2 *от полето.*

Тъй като множеството от редовете на един линеен $\tau-(n,M,q)$ ортогонален масив C образуват линейно пространство над $GF(q)$, е ясно, че M трябва да бъде q^k за някое неотрицателно число k. Числото k се нарича *размерност* на ортогоналния масив.

Следващите 2 основни свойства на ортогоналните масиви с елементи от полето $GF(q)$, ще използваме по-нататък, за да покажем връзката между параметрите на даден ортогонален масив и линейните кодове.

Теорема 4.2.2. *Нека C е ортогонален $\tau - (n, M, q)$ масив с елементи от $GF(q)$. Тогава всеки τ стълба на C са линейно независими над $GF(q)$.*

Доказателство:

Нека $C_1, C_2, \ldots, C_\tau$ са τ стълба на C. Допускаме че са линейно зависими над полето с q елемента, т.е.

$$\alpha_1 C_1 + \alpha_2 C_2 + \cdots + \alpha_\tau C_\tau = \mathbf{0}.$$

за някои елементи $\alpha_1, \alpha_2, \ldots, \alpha_\tau \in GF(q)$. От дефиницията за ортогонален масив всяка наредена τ-орка се среща във всеки $M \times \tau$ подмасив на C. Използвайки последователно τ-орките $(1, 0, \ldots, 0), (0, 1, 0, \ldots, 0), (0, 0, \ldots, 0, 1)$, следва, че $\alpha_1 = \alpha_2 = \cdots = \alpha_\tau = 0$, т.е. кои да е τ стълба на C са линейно независими над $GF(q)$. □

Теорема 4.2.3. *Нека C е $M \times n$ матрица, чиито редове образуват линейно подпространство на $(GF(q))^n$. Ако всеки τ стълба на C са линейно независими над $GF(q)$, тогава C е $\tau - (n, M, q)$ ортогонален масив.*

Доказателство:

Нека $M = q^k$ за някое неотрицателно цяло число k. Нека G е пораждащата на C матрица с размери $(k \times n)$. C се състои от всички n-орки ξG, $\xi = (\xi_1, \xi_2, \ldots, \xi_n), \xi_i \in GF(q)$. Нека да изберем произволни τ стълба на C и нека G_1 да бъде съответната $k \times \tau$ подматрица на G. Тогава стълбовете на G_1 са линейно независими. Броят пъти, които τ-орката z се среща като ред в тези τ стълба, е равен на броя на елементите ξ, за които е изпълнено

$$\xi G_1 = z.$$

Тъй като G_1 има ранг τ, то този брой е точно $q^{k-\tau}$ за всяко z. Следователно C е ортогонален масив със сила τ. □

От дефинициите на линеен код и линеен ортогонален масив е в сила следната теорема.

Теорема 4.2.4. *Един ортогонален масив, съпоставен на даден код, е линеен точно когато самият код е линеен.*

Друг основен факт ни дава възможността да определяме силата на ортогонален масив, получен от даден код.

Теорема 4.2.5. *Ако C е $[n, M, d]_q$ линеен код над $GF(q)$ с минимално разстояние $d^\perp$ на дуалния код, тогава кодовите думи на C образуват ортогонален масив с параметри $d^\perp - (n, M, q)$ над $GF(q)$. Обратно, от редовете на линеен $\tau - (n, M, q)$ ортогонален масив над $GF(q)$ се получава линеен код над $GF(q)$ с параметри $[n, M, d]_q$ и минимално разстояние на дуалния код $d^\perp \geq \tau + 1$. Ако силата на масива е точно τ, но не е $\tau + 1$, то тогава и разстоянието на дуалния код е точно $\tau + 1$.*

Доказателство:

Нека C е $[n, M, d]_q$ линеен код над $GF(q)$ с минимално разстояние $d^\perp$ на дуалния си код. Нека A е масивът, състоящ се от кодовите думи на C като редове. Всеки $d^\perp - 1$ стълба на A трябва да бъдат линейно независими над $GF(q)$. Да допуснем противното, т.е. че някои $d^\perp - 1$ стълба на A са линейно зависими над $GF(q)$. Без ограничение на общността можем да считаме, че това са първите $d^\perp - 1$ стълба на A, които означаваме с $A_1, A_2, \ldots, A_{d^\perp - 1}$. Тогава съществуват елементи $\alpha_1, \alpha_2, \ldots, \alpha_{d^\perp - 1} \in GF(q)$, такива че $\alpha_1 A_1 + \alpha_2 A_2, \ldots, \alpha_{d^\perp - 1} A_{d^\perp - 1} = 0$. Да отбележим, че умножението на n-орката $(\alpha_1, \alpha_2, \ldots, \alpha_{d^\perp - 1}, 0, 0, \ldots, 0)$ с коя да е кодова дума е равно на нула, с други думи тя принадлежи на дуалния код. При това тази n-орка е дума с тегло по-малко от $d^\perp$, което е в противоречие с дефиницията на минимално разстояние. От Теорема 4.2.3 следва, че A е ортогонален $(d^\perp - 1) - (n, M, q)$ масив.

Обратно, нека A е ортогонален масив с параметри $\tau - (n, M, q)$. От Теорема 4.2.2 знаем, че всеки τ стълба на матрицата A са линейно независими над $GF(q)$. Следователно в $A^\perp$ не може да има дума с тегло по-малко или равно на τ. Ако силата на масива е точно τ, то някои негови $\tau + 1$ стълба са линейно зависими над $GF(q)$, следователно в дуалния код има дума с тегло $\tau + 1$, т.е. $d^\perp = \tau + 1$. □

Забележка 4.2.6. *Благодарение на резултатите на Делсарт [7, 8, 9] в горната теорема може да изпуснем линейността, което я превръща в основна връзка между кодовете и ортогоналните масиви.*

4.3 Ортогонални масиви и други алгебрични структури

Разностните схеми са също един мощен способ за конструиране на ортогонални масиви. Получените масиви са със сила 2.

В този параграф ще означаваме с $(G, +)$ или просто G крайна абелева адитивна група с q елемента. В повечето случаи това ще бъде адитивната група на полето $GF(q)$.

Дефиниция 4.3.1. *Нека D е $r \times c$ матрица с елементи от G. D се нарича разностна схема, основана на $(G, +)$, ако притежава следното свойство: за всяко i и j, $1 \leq i, j \leq c, i \neq j$ разликата (като вектори) между i-тия и j-тия стълб съдържа всеки елемент на G с еднаква честота.*

От дефиницията е ясно, че q трябва да дели r. Нека $r = \lambda q$, където λ е броят на повторенията на елементите на групата G, участващи в разликата между две колони. Ще означаваме разностната схема с $D(r, c, q)$.

По-долу са представени примери за разностни схеми.

1. Всеки ортогонален масив с параметри $\tau - (n, M, q)$ при $\tau \geq 2$ може да се разглежда като разностно множество $D(M, n, q)$.

2. Ако имаме две разностни схеми $D_1(r_1, c, q)$ и $D_2(r_2, c, q)$, то като добавим редовете на едната матрица към редовете на другата, ще получим ново разностно множество $D(r_1 + r_2, c, q)$.

3. Нека G е адитивната група на полето $GF(q)$, чиито елементи ще означаваме с $g_0, g_1, \ldots, g_{q-1}$. Нека D е таблицата на умножението на елементите на полето. Тогава D е разностна схема с параметри $D(q, q, q)$. Всъщност разликата между всеки две колони на D има вида

$$\begin{pmatrix} \alpha g_0 \\ \alpha g_1 \\ \vdots \\ \alpha g_{q-1} \end{pmatrix} - \begin{pmatrix} \beta g_0 \\ \beta g_1 \\ \vdots \\ \beta g_{q-1} \end{pmatrix} = (\alpha - \beta) \begin{pmatrix} g_0 \\ g_1 \\ \vdots \\ g_{q-1} \end{pmatrix},$$

   където α и β са различни елементи от полето. Тогава елементите $(\alpha - \beta)g_i, i = 0, 1, \ldots, q-1$ пробягват цялата група, т.е. всеки елемент на групата се среща точно веднъж.

4. Нека D е разностна схема над $G = \{g_0, g_1, \ldots, g_{q-1}\}$. С D_i означаваме масива, получен от D чрез добавяне на g_i към всеки елемент на разностната схема. Така получаваме D_i разностна схема с параметри като тези на D.

Лесно може да превърнем една разностна схема в ортогонален масив. За целта ще разчитаме на конструкцията от Пример 4. за разностни схеми.

Твърдение 4.3.2. *Нека D е разностна схема $D(r, c, q)$. Тогава*

$$A = \begin{bmatrix} D_0 \\ D_1 \\ \vdots \\ D_{q-1} \end{bmatrix}$$

е ортогонален масив с параметри $2 - (c, rq, qs)$.

Доказателство:

Нека вземем два различни стълба на матрицата A и ги означим с $F_1 \neq F_2$. Нека g и g' са два елемента на групата G, не задължително различни. Трябва да покажем, че броят на срещанията на g в F_1 е равен на срещанията на g' в F_2 и този брой е точно $rs/s^2 = \lambda$, (вж. Дефиниция 4.3.1).

Означаваме с C_1 и C_2 стълбове на D, съответстващи на F_1 и F_2. Знаем, че в $C_1 - C_2$ точно λ пъти се среща елемента $g - g'$. За всяко такова срещане съществува единствен ред в точно едно D_i, за което F_1 има елемента g, а F_2 съдържа елемента g'. Тогава от единствеността можем да заключим, че редове с g на F_1 и g' на F_2 са точно λ реда на матрицата A, което трябваше да покажем. □

Да разгледаме един пример как точно се използва конструкцията от Твърдение 4.3.2. Нека D е разностна схема с параметри $D(3,3,3)$, например

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

Тогава получаваме

$$D_0 = D+0 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 2 & 1 \end{pmatrix}, D_1 = D+1 = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 0 \\ 1 & 0 & 2 \end{pmatrix}, D_2 = D+2 = \begin{pmatrix} 2 & 2 & 2 \\ 2 & 0 & 1 \\ 2 & 1 & 0 \end{pmatrix},$$

а от Твърдение 4.3.2 конструираме ортогонален масив A с параметри $2-(3,9,3)$.

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

Разностни схеми $D(r,c,q)$, при които $r=c$, се наричат *генерализирани матрици на Адамар* от ред r над $(G,+)$. В частност, матриците на Адамар са разностни схеми с параметри $D(r,r,2)$.

Да напомним, че матрица на Адамар от ред n е квадратна $n \times n$ матрица H_n над множеството $\{-1,+1\}$, чиито редове са ортогонални, т.е. $H_n H_n^T = nE_n$.

Матриците на Адамар са най-важният пример на разностни схеми над множество 2 елемента. Те са изследвани обстойно и се използват за конструиране на различни кодове, ортогонални масиви и други. Освен това са изключително полезни при статистически изследвания.

Ако H_n е матрица на Адамар, тогава всяка матрица, която се получава при пермутация на редове или стълбове и при смяна на знака в някой ред или стълб, също е матрица на Адамар. Такива матрици се наричат *еквивалентни* на H_n. С такива трансформации винаги може да си осигурим първият ред и първият стълб на H_n да започват с $+1$ и казваме, че H_n е в нормализиран вид.

Лема 4.3.3. *Нека H_n е нормализирана матрица на Адамар от ред $n, n>2$. Нека $u=(u_1,u_2,\ldots,u_n)$ и $v=(v_1,v_2,\ldots,v_n)$ са два реда от матрицата H_n, различни от първия. Тогава*

(a) $n/2$ координати на u са +1 и $n/2$ координати са -1.

(б) има $n/4$ координати $u_i = v_i = +1$ и $n/4$ координати $u_i = +1, v_i = -1$, $n/4$ координати $u_i = v_i = -1$ и $n/4$ координати $u_i = -1, v_i = +1$.

(в) За стълбовете на матрицата H_n с изключение на първия могат да се изкажат аналогични на (а) и (б) твърдения.

Твърдение 4.3.4. *Ако матрица на Адамар от ред n съществува, то n е 1, 2 или се дели на 4.*

Една от връзките между матриците на Адамар и ортогоналните масиви е представена в следващата теорема.

Теорема 4.3.5. *Ортогонални масиви с параметри $2-(4\lambda-1, 4\lambda, 2)$ и $3-(4\lambda, 8\lambda, 2)$ съществуват точно когато съществува матрица на Адамар от ред 4λ.*

Доказателство:

От Теорема 1.2.4 знаем, че един ортогонален масив с параметри $2-(4\lambda-1, 4\lambda, 2)$ съществува точно когато съществува ортогонален масив с параметри $3-(4\lambda, 8\lambda, 2)$.

Нека $H_{4\lambda}$ е нормализирана матрица на Адамар. От Лема 4.3.3 е ясно, че при премахване на първия стълб на матрицата $H_{4\lambda}$, получаваме точно ортогонален масив с параметри $2-(4\lambda-1, 4\lambda, 2)$.

Обратно, нека C ортогонален $2-(4\lambda-1, 4\lambda, 2)$ масив над множеството $\{-1, 1\}$. От Дефиниция 1.2.1 на ортогонален масив следва, че след добавяне на стълб с $+1$ в матрицата C, новополучената матрица отговаря на условията от Лема 4.3.3, следователно е матрица на Адамар от ред 4λ. □

4.4 Ортогонални масиви и употребата им в статистиката

Рао въвежда ортогоналните масиви заради техните статистически свойства, наблюдавани при частични факторни експерименти. В този параграф ще спомена някои основни приложения на ортогоналните масиви като ги разглеждаме като статистически обекти. Под ортогонален масив ще разбираме следното по-общо понятие.

Дефиниция 4.4.1. *Обобщени (mixed) ортогонален масив с параметри $\tau - (q_1^{n_1}\ q_2^{n_2}\ \ldots\ q_\nu^{n_\nu}, M)$ наричаме матрица $M \times n$, където $n = n_1 + n_2 + \cdots + n_\nu$ като първите n_1 стълба са над азбуката $\{0, 1, \ldots, q_1 - 1\}$, следващите n_2 стълба са с елементи от $\{0, 1, \ldots, q_2 - 1\}$ и така нататък, със свойството че във всяка $M \times \tau$ подматрица всяка τ-орка се среща еднакъв брой пъти.*

Неравенството на Рао за ортогонални масиви лесно може да бъде пренесено и върху обобщени ортогонални масиви. За по-голяма яснота да въведем означението:

$$I_m(\nu) = \{(i_1, i_2, \ldots, i_\nu) \mid i_1 \geq 0, \ldots, i_\nu \geq 0, \sum_{k=1}^{\nu} i_k = m\},$$

където $m \geq 0$ и $\nu \geq 1$ са цели числа.

Теорема 4.4.2. *(Неравенство на Рао) Нека C е (обобщен) ортогонален масив с параметри $\tau-(q_1^{n_1}q_2^{n_2}\dots q_\nu^{n_\nu}, M)$. Без ограничение на общността можем да приемем, че $q_1 \leq q_2 \leq \dots \leq q_\nu$. Тогава за параметрите на масива C са в сила следните неравенства:*

(а) ако $\tau = 2u$, то

$$M \geq \sum_{m=0}^{u} \sum_{I_m(\nu)} \binom{n_1}{i_1}\binom{n_2}{i_2}\dots\binom{n_\nu}{i_\nu}(q_1-1)^{i_1}(q_2-1)^{i_2}\dots(q_\nu-1)^{i_\nu}.$$

(б) ако $\tau = 2u+1$, то

$$M \geq \sum_{m=0}^{u} \sum_{I_m(\nu)} \binom{n_1}{i_1}\binom{n_2}{i_2}\dots\binom{n_\nu}{i_\nu}(q_1-1)^{i_1}(q_2-1)^{i_2}\dots(q_\nu-1)^{i_\nu}+$$

$$\sum_{I_u(\nu)} \binom{n_1}{i_1}\dots\binom{n_{\nu-1}}{i_{\nu-1}}\binom{n_\nu-1}{i_\nu}(q_1-1)^{i_1}(q_2-1)^{i_2}\dots(q_{\nu-1}-1)^{i_{\nu-1}}(q_\nu-1)^{i_\nu+1}.$$

Да се върнем отново към статистическите наблюдения. Факторни експерименти обикновено изучават как промяната в нивата на различните фактори влияят върху крайния резултат. Факторите обикновено се разделят на два основни вида: качествени и количествени. Количествен фактор е например температурата, при която протича дадена химична реакция, докато пример за качествен фактор е типът катализатор, използван в съответната химична реакция.

Всеки от факторите, който се идентифицира с повече от две стойности, се наблюдава в експеримента. Изборът на възможни стойности при количествените фактори е далеч по-лесен от този при качествените. Едно от най-важните неща е да се определи оптималната стойност на минималната промяна в нивата, при която ще се промени крайният резултат.

След като са избрани факторите и нивата, се съставят всички техни възможни комбинации. При пълен факторен експеримент се правят изследвания на всяка такава възможна комбинация от стойности. Често обаче всички възможности са необозримо много. В този случай се прави подбор на комбинациите и се получава така наречения частичен факторен експеримент. При тези наблюдения ортогоналните масиви играят важна роля.

Нека означим с $A_1, A_2, \dots, A_n$ факторите, които ще бъдат включени в разглеждания експеримент. Възможните стойности за даден фактор A_i ще означаваме съответно с $q_i, i = 1, 2, \dots, n$. За удобство ще кодираме стойностите на съответния фактор с $0, 1, \dots, q_i - 1$, а комбинациите на нивата ще бележим като наредени n-орки $(j_1, j_2, \dots, j_n)$, където $0 \leq j_i \leq q_i - 1, i = 1, 2, \dots, n$. Множеството от всички комбинации бележим с L.

Да означим с M броя на експерименталните единици, които са възможни в разглеждания експеримент и нека $t \in L$ е една възможна комбинация. Означаваме

още с r_t броя на обектите, които са асоциирани с тази комбинация. При това, ако r_t е положителен, ще означаваме с Y_{tj}, $j = 1, 2, \ldots, r_t$ променливата, съответстваща на j-тата единица, асоциирана с комбинацията t. Често използван статистически модел за така определените непрекъснати зависими променливи Y_{tj} е следният:

$$Y_{tj} = \mu_t + \epsilon_{tj},$$

където μ_t означава определено очакване на популация за възможни наблюдения с комбинацията t, а ϵ_{tj} съответства на ненаблюдавано произволно отклонение от очакването μ_t за j-ия обект, получил комбинацията t. Параметър ϵ_{tj} се нарича произволна грешка и има очакване 0 и дисперсия σ^2, с други думи очакването и дисперсията за Y_{tj} са $E(Y_{tj}) = \mu_t$, $D(Y_{tj}) = \sigma^2$.

Удобно е този модел да се запише в следния матричен вид. Да означим с μ вектор стълба $|L|\times 1$ с очаквана популация μ_t, с Y вектор стълба $M\times 1$ от произволни променливи Y_{tj} и с ϵ вектор стълба $M \times 1$ от произволни грешки. Тогава моделът придобива следния вид:

$$Y = X\mu + \epsilon,$$

където X е матрица с размери $M \times |L|$, съставена от нули и единици по следното правило: елементът на позиция (tj, t') е 1, ако $t = t'$ и 0 в противен случай. Всеки ред на X съдържа точно една единица.

Контраст наричаме линейна комбинация на очакванията на популация с произволни коефициенти, чиято сума е равна на нула, т.е. за известен вектор стълб $N\times 1$, казваме, че $c^T\mu$ е контраст, ако $c^T N = 0$. Нека имаме даден фактор A и да разменим неговите нива, но да не променяме нивата на останалите фактори. Контрастът в този случай, сметнат средно върху нивата на останалите фактори, наричаме *главен ефект* на фактора A. Нека фиксираме две различни нива на фактора B, които да означим с 0 и 1 съответно. Сравняваме ефекта на фактор A в зависимост от фактора B с ниво 0 с ефекта на фактора A в зависимост от фактора B с ниво 1. Тогава контрастът, който се получава, се нарича ефект на взаимодействие между факторите A и B. Той показва дали ефектът на A зависи от нивата на B или обратното. Повечето анализи на частичните факторни експерименти са базирани на изучаването на главните контрасти и на ефектите на взаимодействие.

Броят на елементите в L може да бъде огромен при наличието на достатъчно много нива. Всяко собствено подмножество на L се нарича частично факторно множество, върху което се налага да наложим повече ограничения, за да може да се прилага в разглежданите наблюдения. За всяка комбинация $t \in L$ и за всеки главен ефект съществува поне една компонента на ефекта, при който коефициентът на μ_t е ненулев. В този случай разглеждаме модела

$$Y = XU\gamma + \epsilon, \tag{4.4.1}$$

където γ е вектор стълб от $R^{\text{-те}}$ ненулеви елемента на β (вектор стълб от контрасти), а U е подматрицата $N \times R$ на $N \times N$ матрицата, състояща се от R колони, които отговарят на $R^{\text{-те}}$ елемента на β, които остават в γ. Удобно е този модел да се раздели на следните две части:

$$Y = XU_1\gamma_1 + XU_2\gamma_2 + \epsilon, \tag{4.4.2}$$

където обединението на елементите на γ_1 и γ_2 е точно γ, а стълбовете на U_1 и U_2 са съответното разбиване на U.

При така определените по-горе модели един ортогонален масив с параметри $\tau - (q_1 q_2 \dots q_n, M)$ определя M комбинации на нивата за даден $q_1 q_2 \dots q_n$ частичен факторен експеримент.

Теорема 4.4.3. *[13] Нека един ортогонален масив с параметри* $\tau - (q_1 q_2 \dots q_k,), \tau \geq 2$ *се използва в частичен факторен експеримент.*

(i) Ако τ *е четно число,* γ_2 *липсва и* $\gamma = \gamma_1$ *се състои от параметъра на засичане, главните ефекти и всички ефекти на взаимодействие с най-много* $\tau/2$ *фактора, то всички елементи на* $\gamma = \gamma_1$ *са предвидими с модела (4.4.1).*

(ii) Ако τ *е нечетно число,* γ_1 *се състои от параметъра на засичане, главните ефекти и всички ефекти на взаимодействие с най-много* $(\tau - 1)/2$ *фактора, а* γ_2 *се състои от всички компоненти на взаимодействия с точно* $(\tau + 1)/2$ *фактора, тогава всички елементи на* γ_1 *са предвидими с модела (4.4.2).*

Приложенията на ортогоналните масиви в тази глава са една илюстрация на актуалността на изследваните в представената дипломна работа проблеми. Прилагането на ортогоналните масиви особено в статистиката и криптографията са част от мотивациите на много учени непрекъснато да се стремят да конструират такива масиви или да изучават техните свойства. В частност проблемът за намиране спектрите на даден ортогонален масив е важен аспект на тези изследвания.

Библиография

[1] N. Alon, O. Goldreich, J. Hastad, R. Peralta, Simple construction of almost k-wise independent random variables, Random Structions and Algoritms, 3, 1992, 289-304, *Regional Conf. Lect. Appl. Math.*, SIAM 21, 1975.

[2] J. Bierbrauer, K. Gopalakrishan, D. R. Stinson, Bounds for resilient functions and orthogonal arrays, *Lecture Notes in Computer Sciences*, 839, 1994, 247-256.

[3] J. Bierbrauer, K. Gopalakrishan, D. R. Stinson, Orthogonal arrays, resilient functions, error-correcting codes and linear programming bounds, *SIAM J. Discrete Math.*,9, 1996, 424-452.

[4] P. G. Boyvalenkov, Computing distance distributions of spherical designs, *Lin. Alg. Appl.*, 226/228, 1995, 277-286.

[5] P. Boyvalenkov, H. Kulina, Computing distance distributions of orthogonal arrays, Proc. Intern. Workshop ACCT2010, ISBN 978-5-86134-174-5, 85-85.

[6] P. Boyvalenkov, H. Kulina, Nonexistence of binary orthogonal arrays via their distance distributions, (submitted).

[7] P.Delsarte, Bounds for Unrestricted Codes by Linear Programming, *Philips Research Reports*, 27, 1972, 272-289.

[8] P.Delsarte, Four fundamental parameters of a code and their combinatorial significance, Inform. Contr., 23, 1973, 407-438.

[9] P.Delsarte, An Algebraic Approach to Association Schemes in Coding Theory, *Philips Research Report Suppl.*,10, 1993.

[10] C.F. Dunkl, Discrete quadrature and bounds on t-designs, *Michigan Math. J.*, 26, 1979, 81-102.

[11] E. N. Gilbert, F. J. MacWilliams, and N. J. A. Sloane, Codes which detect deception, Bell System Tech. Journal, 53 (1974), pp. 405–424.

[12] K. Gopalakrishnan, Douglas R. Stinson, Applications of Orthogonal Arrays to Computer Science, Proc. of ICDM 2006, Pages 149–164.

[13] A. S. Hedayat, N. J. A. Sloane, John Stufken, *Orthogonal arrays: Theory and Applications*, Spinger-Verlag New York, Inc., 1999.

[14] Х. Кулина, Кодове и дизайни в антиподални полиномиални метрични пространства, PhD Thesis, 2012

[15] V. I. Levenshtein, Bounds for packings in metric spaces and certain applications, *Probl. Kibern.* 40, 1983, 44-110 (in Russian).

[16] V. I. Levenshtein, Designs as maximum codes in polynomial metric spaces, *Acta Appl. Math.* 25, 1992, 1-82.

[17] V. I. Levenshtein, Krawchouk Polynomials and Universal Bounds for Codes and Designs in Hamming Spaces, IEEE Transactions on Information Theory, Vol.41, No. 5, 1995, 1303-1321.

[18] V. I. Levenshtein, Universal bounds for codes and designs, chapter 6 in *Handbook of Coding Theory*, V. Pless and W. C. Huffman, Eds., Elsevier Science B.V., 1998.

[19] F. J. MacWilliams, N. J. Sloane, *The Theory of Error-Correcting Codes*, Amsterdam, The Netherlands: North Holland, 1977.

[20] C. R. Rao, Factorial experiments derivable from combinatorial arrangements of arraya, J. Roy. Stat. Soc. 89, 1947, 128-139.

[21] G. J. Simmons, Message authentication: a game on hypergraphs, Congressus Numerantium, 45 (1984), pp. 161–192.

[22] D. R. Stinson, Combinatorial characterizations of authentication codes, Designs, Codes and Cryptography, 2 (1992), pp. 175–187.

[23] D. R. Stinson, Combinatorial techniques for universal hashing, Journal of Comp. and Sys. Sci., 48(2) (1994), pp. 337–346.

[24] D. R. Stinson, The combinatorics of authentication and secrecy codes, Journal of Cryptology, 2 (1990), pp. 23–49.

[25] G. Szegö, *Orthogonal polynomials*, AMS Col. Publ. Providence, RI, 1939.