Софийски университет „Св. Климент Охридски”
Факултет по математика и информатика

Таня Тодорова Маринова

АЛГОРИТМИ ЗА ХАРАКТЕРИЗИРАНЕ НА ОРТОГОНАЛНИ МАСИВИ

АВТОРЕФЕРАТ

на дисертация
за присъждане на образователна и научна степен
„ДОКТОР”

по Професионално направление 4.5. Математика
Докторска програма „Алгебра, топология и приложения”

научен ръководител:
доц. д-р Мая Митева Стоянова

София
2 0 2 1

Дисертацията съдържа 115 страници и се състои от увод, четири глави и използвана литература с 59 заглавия.

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

В дисертационния труд е изследвана структурата на някои класове от ортогонални масиви в Хеминговото пространство $H(n,q)$. Ортогоналните масиви имат редица приложения в различни области на математиката като статистика [30, 48, 56], теория на кодирането [1, 2, 20, 29], криптографията [4, 36, 57], а също така и в областта на компютърните науки за тестване на софтуери и в областта на физиката.

Изследванията в дисертационния труд се извършват в Хеминговото пространство $H(n,q)$, разглеждано като крайномерно полиномиално метрично пространство. Използвани са полиномиални техники [21, 37, 38, 13] за изследване на спектрите на ортогоналните масиви и за получаване на някои ограничения върху структурата на масивите.

Хеминговото пространство е пространството от всички наредени n-орки над азбука (поле) Q с q елемента. Размерността на $H(n,q)$ е точно n. В $H(n,q)$ се въвежда метрика, използвайки разстоянието $d(x,y)$ между две думи от пространството $x,y \in H(n,q)$, което се определя като броят на различните координати, в които две думи се различават. Въвежда се скаларно произведение по следното правило

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

Обратимата функция $\sigma(d) = 1 - \frac{2d}{n}$, благодарение на която преминаваме от разстояния към скаларни произведения и обратно, се нарича стандартна субституция.

В първа глава на дисертационния труд са представени подробно полиномите на Кравчук и нормализираните полиноми на Кравчук, които се явяват зонални полиноми на крайномерното метрично пространство $H(n,q)$.

Всяко непразно (крайно) подмножество $C \subset H(n,q)$ се нарича код. Най-важните параметри на един код са неговите размерност n, мощност $M = |C|$, както и минималното разстояние между две различни думи $d = d(C) = \min\{\ d(x,y)\ :\ x,y \in C, x \neq y\}$.

Фазекаш и Левенщейн [26] въвеждат понятието τ-дизайн в $H(n,q)$.

Определение 1.1.1 *Един код $C \subset H(n,q)$ се нарича τ-дизайн тогава и само тогава, когато за всеки полином с реални коефициенти $f(t)$ от степен k, ненадминаваща τ, и за всяка точка $y \in H(n,q)$ 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. $f(t) = \sum\limits_{i=0}^{n} f_i Q_i^{(n)}(t)$.

Максималното цяло неотрицателно число $\tau \leq n$, за което C е τ-дизайн, се нарича сила на дизайна. Разглеждани като комбинаторни структури, за τ-дизайните е показано, че са точно ортогоналните масиви в $H(n,q)$.

Определение 1.2.1 *Нека Q е произволна азбука (поле) с q елемента, а C е матрица с M реда и n стълба с елементи от Q. Ще казваме, че C е 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 (n, M, q, τ).*

В параграф 1.2. са представени основни свойства на ортогоналните масиви. Въведени са техните характеристики като основната характеристика, която е обект на анализиране в този дисертационен труд е понятието спектър на ортогонален масив относно точка от пространството.

Определение 1.2.2 *На всеки (n, M, q, τ) ортогонален масив $C \subset H(n, q)$ и фиксирана точка $c \in H(n, q)$ съпоставяме $(n+1)$-орката от цели неотрицателни числа*

$$W = W(c) = (w_0(c), w_1(c), \ldots, w_n(c)),$$

където

$$w_i(c) = |\{x \in C | d(x, c) = i\}|,$$

за $i = 0, \ldots, n$. Ще наричаме $W = W(c)$ спектър на ортогоналния масив C относно точката c (или спектър на точката c, ако C се подразбира).

За удобство в настоящата работа ще използваме различни означения в зависимост от това дали точката c принадлежи на масива C или не. По-точно, за вътрешна за масива точка $c \in C$ ще означаваме спектъра на C по отношение на точката c с

$$P = P(c) = (p_0 \geq 1, p_1, \ldots, p_n),$$

докато за външна за масива точка $c \in H(n, q) \setminus C$ ще означаваме спектъра на C относно точката c с

$$Q = Q(c) = (q_0 = 0, q_1, \ldots, q_n).$$

В дисертационния труд се разглеждат ортогонални масиви с техните комбинаторни свойства, като се използват известни полиномиални техники върху τ-дизайни в полиномиални метрични пространства.

Основна задача от теорията на кодирането, която се разглежда в дисертационния труд е следната:

Задача 1.3.1 *За фиксирани сила τ, брой стълбове n и азбука с q елемента да се намери минималната възможна мощност M, за която съществува (n, M, q, τ) ортогонален масив в $H(n, q)$, т.е. да се оцени величината*

$$B(n, q, \tau) = \min\{M = |C| \ : \ \text{съществува } (n, M, q, \tau) \text{ ортогонален масив в } H(n, q)\}.$$

Известно е, че индексът λ на даден ортогонален масив може да бъде пресметнат посредством зависимостта $\lambda = M/q^\tau$. По този начин получаваме следната еквивалентна задача.

Задача 1.3.2 *За фиксирани сила τ, брой стълбове n и азбука с q елемента да се намери минималният възможен индекс λ, за който съществува (n, M, q, τ) ортогонален масив в $H(n, q)$, т.е. да се оцени величината*

$$\Lambda(n, q, \tau) := min\{\lambda = |C|/q^\tau \ : \ \text{съществува } \ (n, M, q, \tau) \text{ ортогонален масив}\}.$$

В Параграф 1.3. са описани известни граници за мощността на един ортогонален масив $C \in H(n, q)$. Това са границите на линейното програмиране (или граница

на Делсарт)[24], също така границите на Рао и Хеминг [49], [39], които в Хеминговото пространство $H(n,q)$ съвпадат. Въведени са още границата на Сингълтън [53] и границата на Плоткин [47], като последната е валидна за двоичното Хемингово пространство $H(n,2)$. Подробно са описани универсалните граници (горна и долна) на Левенщейн [38].

Намирането на всички възможности за различни характеристики на един код е стандартен похват в теория на кодирането и в комбинаториката. Идеята за намирането на спектрите на оптималните кодове и дизайни е въведена за пръв път от Делсарт в неговата дисертация [21]. Ние ще приложим един от начините за пресмятане на всички възможности за спектри на (n, M, q, τ) ортогонален масив, който е следствие от по-общ подход, предложен от Бойваленков [9].

По-точно следващата теорема дава необходимия апарат за първоначално намиране на всички възможности за спектри относно вътрешна или външна точка за даден ортогонален масив (виж [13], [14]).

Теорема 1.4.1 *Нека $C \subset H(n,q)$ е (n, M, q, τ) ортогонален масив и $c \in H(n,q)$ е фиксирана точка. Тогава:*

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

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

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

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

където b_k е първият коефициент в развитието на полинома t^k по нормализираните полиноми на Кравчук, т.е. $t^k = b_k + \sum_{i=1}^{k} P_i^{(n)}(t)$.

Благодарение на **Теорема 1.4.1** успяваме да намерим множествата от всички възможни спектри спрямо вътрешни и външни точки на масива. За фиксирани n, M, $\tau \leq n$ и q бележим множеството от всички възможни спектри спрямо коя да е вътрешна точка с $P(n, M, q, \tau)$, а множеството от възможните спектри спрямо произволна външна за масива точка - $Q(n, M, q, \tau)$. Множеството от всички възможни точки независимо от избраната точка бележим с

$$W(n, M, q, \tau) = P(n, M, q, \tau) \cup Q(n, M, q, \tau).$$

Следващата теорема ни дава възможност да фиксираме точка от пространството и да работим спрямо нея без да губим ограничение на общността.

Теорема 1.4.4 *Множеството $W(n, M, q, \tau)$ е точно множеството от спектри на ортогонални масиви с параметри (n, M, q, τ) спрямо точката $\mathbf{0} \in H(n,q)$.*

Доказани са още **Теорема 1.4.6** и **Теорема 1.4.8**, както и техни непосредствени следствия, които ни дават възможност да разглеждаме спектрите на ортогонални масиви спрямо коя да е фиксирана точка от пространството $H(n,q)$.

Във втора глава се разглеждат ортогонални масиви в двоичното Хемингово пространство $H(n,2)$. Да отбележим, че $H(n,2)$ е антиподално метрично пространство, т.е. за всека точка $x \in H(n,2)$ съществува единствена точка $\bar{x} \in H(n,2)$, за която е изпълнено условието $d(x,\bar{x}) = n$. Използвайки този факт, в [28] е доказано, че ортогонални масиви с параметри $(n, M, 2, 2k)$ и $(n+1, 2M, 2, 2k+1)$ съществуват едновременно.

В дисертационния труд се използват две основни конструкции за изследването на ортогоналните масиви. При първата конструкция за ортогонален масив с фиксирани параметри $(n, M, 2, \tau)$ се отрязва произволен стълб и се анализират връзките между спектрите с новополучените производни масиви. При тази конструкция се получават производни ортогонални масива съответно с параметри $(n-1, M, 2, \tau)$ и $(n-1, M/2, 2, \tau-1)$. Конструкцията има следния вид.

$$\begin{array}{c} \overbrace{\begin{array}{c} C' - (n-1, M, 2, \tau) \\ W' = (w'_0, w'_1, \ldots, w'_{n-1}) \end{array}} \\ \left.\begin{array}{|c|c|} \hline 0 & \\ 0 & Y = (y_0, y_1, \ldots, y_{n-1}) \\ \vdots & C_0 - (n-1, M/2, 2, \tau-1) \\ 0 & \\ \hline 1 & \\ 1 & X = (x_1, x_2, \ldots, x_n) \\ \vdots & C_1 - (n-1, M/2, 2, \tau-1) \\ 1 & \\ \hline \end{array}\right\} \\ \underbrace{\begin{array}{c} C - (n, M, 2, \tau) \\ W = (w_0, w_1, \ldots, w_n) \end{array}} \end{array}$$

Конструкция 2.3.

В параграф 2.3. е разгледано само множеството от спектри относно вътрешна за масива точка $P(n, M, 2, \tau)$. Благодарение на **Теорема 2.3.1**, **Теорема 2.3.3**, **Теорема 2.3.4** и **Теорема 2.3.6** е организиран алгоритъм за редуцирането на броя на елементите в множеството от спектри $P(n, M, 2, \tau)$.

При работа единствено с вътрешни точки, част от получените в Конструкция 2.2 ортогонални масиви не могат да бъдат изследвания. Затова в Параграф 2.4. са обобщени теоремите от Параграф 2.3. върху множеството от спектри $W(n, M, 2, \tau)$ относно коя да е произволна точка от пространството $H(n,2)$. В допълнение са представени в явен спектрите на новополучените ортогонални масиви с параметри $(n-1, M/2, 2, \tau-1)$.

Теорема 2.3.4 *Нека $C \subset H(n,2)$ е $(n, M, 2, \tau)$ двоичен ортогонален масив, за който $W \in W(n, M, \tau, 2)$ е спектър на C спрямо произволна точката $c \in H(n,2)$. Нека $c' \in H(n-1, 2)$ и C' са получени съответно от c и C съгласно Конструкция 2.3, а $W' \in W(n-1, M, 2, \tau)$ е спектър на масива C' относно точката c'. Тогава*

системата линейни уравнения

$$\left|\begin{array}{l} x_i + y_i = w_i,\ i = 1, 2, \ldots, n-1 \\ x_{i+1} + y_i = w'_i,\ i = 0, 1, \ldots, n-1 \\ y_0 = w_0 \\ x_n = w_n \\ x_i, y_i \in \mathbb{Z},\ x_i \geq 0,\ y_i \geq 0,\ i = 0, 1, \ldots, n \end{array}\right. . \tag{3}$$

с неизвестни $X = (x_1, x_2, \ldots, x_{n-1}, x_n)$ *и* $Y = (y_0, y_1, \ldots, y_{n-1})$ *има единствено решение от вида*

$$X = (w'_0 - w_0, \sum_{j=0}^{1}(w'_j - w_j), \ldots, \sum_{j=0}^{n-2}(w'_j - w_j), w_n),$$

$$Y = (w_0, w_1 - (w'_0 - w_0), w_2 - \sum_{j=0}^{1}(w'_j - w_j), \ldots, w_{n-1} - \sum_{j=0}^{n-2}(w'_j - w_j)).$$

В същия параграф, използвайки антиподалността, достигнахме до редица теореми и следствия, благодарение на които доказахме важната за изследванията ни **Теорема 2.4.16**, която за даден спектър (относно произволна точка x от пространството) задава вида на спектър спрямо точката x на друг ортогонален масив със същите параметри, изоморфен на изходния масив. Така спектърът на новополучения изоморфен ортогонален масив трябва да принадлежи отново на множеството $W(n, M, 2, \tau)$. По този начин за пръв път достигаме до извода, че даден спектър на масива, т.е. елемент на множеството $W(n, M, 2, \tau)$ зависи от друг спектър (елемент) на същото множество.

Реализиран е втори алгоритъм, който се използва за редуциране на множеството от спектри спрямо произволна точка от пространството $W(n, M, 2, \tau)$. Този алгоритъм е доста по-мощен от Алгоритъм 1., но като недостатък трябва да се отбележи, че мощността на $W(n, M, 2, \tau)$ е доста по-голяма от мощността на $P(n, M, 2, \tau)$ за големи стойности на n.

В Параграф 2.5 е разгледана втората конструкция, при която се отрязват два стълба от фиксирания ортогонален масив C. Получават се редица произволни ортогонални масиви с различни параметри: $(n-1, M, 2, \tau)$, $(n-2, M, 2, \tau)$, $(n-1, M/2, 2, \tau)$, $(n-2, M/2, 2, \tau)$, като и още няколко новополучени ортогонални масиви с параметри като изходния $(n, M, 2, \tau)$ ортогонален масив. Подробно са доказани в Теореми 2.5.3 - 2.5.28 различните връзки между техните спектри. Където е възможно, са предоставени в явен вид някои от спектрите. Създаден е трети алгоритъм, който подобрява резултатите за редуциране на множеството от спектри $W(n, M, 2, \tau)$.

Трябва да се отбележи, че резултатите в дисертационния труд зависят от реализацията на алгоритмите. Затова са описани редица оптимизации, които сме приложили, за да могат програмите да имат по-добро бързодействие. Описани са също и някои по-любопитни моменти от алгоритмите, тъй като за част от тях се налага използването на рекурсия.

В последния параграф 2.8 са формулирани всички резултати за несъществуване, които се получили благодарение на гореописаните алгоритми.

Благодарение на Алгоритъм 1. и като използваме известни граници за минималното разстояние на даден код, достигаме до следващите две теореми

Теорема 2.8.1 *Не съществува двоичен ортогонален масив с параметри* $(4, 96, 11)$.

Теорема 2.8.2 *Не съществува двоичен ортогонален масив с параметри* $(4, 96, 10)$.

Получени са и следните резултати.

Следствие 2.8.3 *Не съществуват двоични ортогонални масиви (съответно) с параметри* $(11, 192, 5)$ *и* $(12, 192, 5)$.

С използването на Алгоритъм 2. се достига до подобряване на горните резултати.

Теорема 2.8.4 *Двоичен ортогонален масив с параметри* $(9, 96, 2, 4)$ *не съществува.*

Следствие 2.8.5 *Двоичен ортогонален масив с параметри* $(10, 192, 2, 5)$ *не съществува.*

Друга редица, върху която са приложени алгоритмите, е $(13, 224, 2, 5)$. Върху нея Алгоритъм 1. дава следния резултат.

Теорема 2.8.6 *Двоичен ортогонален масив с параметри* $(13, 224, 2, 5)$ *не съществува.*

Следствие 2.8.7 *Двоичен ортогонален масив с параметри* $(12, 112, 2, 4)$ *не съществува.*

Когато приложим Алгоритъм 2. се получава следната теорема и нейните следствия.

Теорема 2.8.8 *Двоичен ортогонален масив с параметри* $(10, 112, 2, 4)$ *не съществува.*

Следствие 2.8.9 *Двоичен ортогонален масив с параметри* $(11, 112, 2, 4)$ *не съществува.*

Следствие 2.8.10 *Двоичен ортогонален масив с параметри* $(11, 224, 2, 5)$ *не съществува.*

Следствие 2.8.11 *Двоичен ортогонален масив с параметри* $(12, 224, 2, 5)$ *не съществува.*

За да получим пълен резултат върху разглежданата редица, се налага да се използва най-мощният, но и най-бавен от описаните алгоритми, а именно Алгоритъм 3. След прилагането му са получени следните резултати.

Теорема 2.8.12 *Двоичен ортогонален масив с параметри* $(9, 112, 2, 4)$ *не съществува.*

Следствие 2.8.13 *Двоичен ортогонален масив с параметри* $(10, 224, 2, 5)$ *не съществува.*

Показани са също и някои известни вече резултати. По този начин достигнахме до точни граници за $\Lambda(n, 2, \tau)$ в следните случаи:

$$\Lambda(9, 2, 4) = \Lambda(10, 2, 5) = 8, \quad \Lambda(9, 2, 4) = \Lambda(10, 2, 5) = 8,$$

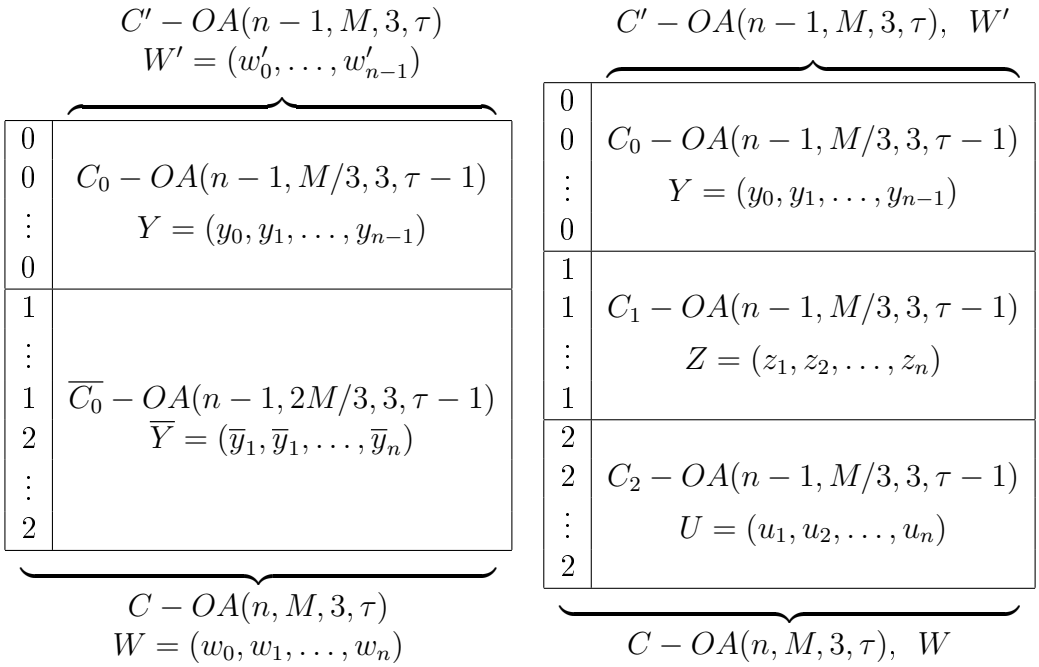
$$\Lambda(11, 2, 4) = \Lambda(12, 2, 5) = 8 \quad \Lambda(12, 2, 5) = \Lambda(13, 2, 5) = 8.$$

На база на разработените от нас алгоритми успяхме да достигнем и до други вече известни резултати за несъществуване, описани накрая на Параграф 2.8. От своя

страна за редица параметри на ортогонални масиви, въпреки, че не сме достигнали до резултат за съществуване или несъществуване, сме получили значително редуциране на броя на елементите в множеството $W(n, M, 2, \tau)$ от възможности за спектри за изследвания ортогонален масив.

Втора глава е написана въз основа на следните три публикации [16], [17] и [43].

В трета глава се разглеждат ортогонални масиви над троичното Хемингово пространство $H(n, 3)$. Анализирани са съответно множествата от спектри $W(n, M, 3, \tau)$ и $P(n, M, 3, \tau)$. Приложена е аналогична (на първата в двоичния случай) конструкция с отрязване на един стълб от троичен ортогонален масив C с фиксирани параметри $(n, M, 3, \tau)$. По-долу тази конструкция е илюстрирана, при отрязване на $\ell = 1$ стълб, за да може да се придобие по-ясна представа за новообразуваните производни ортогонални масиви.



Конструкция 3.2 (Фигура 1).

Както може да се забележи, от ортогоналния масив C се получават няколко производни ортогонални масива с параметри $(n-1, M, 3, \tau)$, $(n-1, M/3, 3, \tau-1)$ и $(n-1, 2M/3, 3, \tau-1)$. За тези ортогонални масиви могат да се намерят връзки между техните спектри и спектъра на началния ортогонален масив C. Теорема 3.2.2 ни дава в явен вид спектрите на някои от изследваните ортогонални масиви, докато Теорема 3.2.6 задава система, на която трябва да отговарят спектрите на ортогоналните масиви с параметри $(n-1, M/3, 3, \tau-1)$ и $(n-1, 2M/3, 3, \tau-1)$.

Нека да означим трите транспозиции от симетричната група S_3 съответно със $\sigma_0 = (12)$, $\sigma_1 = (20)$ и $\sigma_2 = (01)$, а двата тройни цикъла съответно с $\rho = (012)$ и $\rho^2 = (021)$. От свойствата на ортогоналните масиви знаем, че при пермутация на елементите във фиксиран стълб, отново се получава ортогонален масив с параметри $(n, M, 3, \tau)$. Ако извършим първо трите транспозиции върху фиксирания ℓ-ти стълб

на ортогоналния масив C със спектър $W \in W(n, M, 3, \tau)$ относно произволна точка $c \in H(n, 3)$, получаваме три, изоморфни на масива C, ортогонални масива с параметри $(n, M, 3, \tau)$. Означаваме тези масиви съответно с C^{σ_0}, C^{σ_1} и C^{σ_2}. Всъщност резултатът от приложението на пермутацията $\sigma_0 = (12)$ върху C води до ортогонален масив, чиито спектър спрямо точката c съвпада със спектъра W на C. Спектрите на другите два ортогонални масива, получени при пермутациите σ_1, σ_2 са означени съответно с W^{σ_1} и W^{σ_2}. При извършване на някой двата тройни цикъла от S_3 върху ℓ-тия стълб на ортогоналния масив C бихме получили ортогонални масиви, които са изоморфни на вече намерените ортогонални масиви. Следващата теорема ни задава вида на новополучените ортогонални масиви.

Теорема 3.2.7 *Нека $C \subset H(n, 3)$ е (n, M, τ) троичен ортогонален масив, за който*

$$\begin{aligned} W &= (w_0, w_1, \ldots, w_n) = (y_0, y_1 + \overline{y}_1, \ldots, y_{n-1} + \overline{y}_{n-1}, \overline{y}_n) \\ &= (y_0, y_1 + z_1 + u_1, \ldots, y_{n-1} + z_{n-1} + u_{n-1}, z_n + u_n) \in W(n, M, \tau), \end{aligned}$$

е спектърът на C спрямо произволна точка $c \in H(n, 3)$. Тогава:

(а) Спектърът $W^{\sigma_1} \in W(n, M, \tau)$ на троичния ортогонален масив C^{σ_1} относно точката с има вида

$$W^{\sigma_1} = (u_1, y_0 + z_1 + u_2, \ldots, y_{n-2} + z_{n-1} + u_n, y_{n-1} + z_n);$$

(б) Спектърът $W^{\sigma_2} \in W(n, M, \tau)$ на троичния ортогонален масив C^{σ_2} относно точката с има вида

$$W^{\sigma_2} = (z_1, y_0 + u_1 + z_2, \ldots, y_{n-2} + u_{n-1} + z_n, y_{n-1} + u_n).$$

Формулирана и доказана е **Теорема 3.2.10**, която е аналог на доказаната в двоичния случай **Теорема 2.4.18**. Въз основа на **Теореми 3.2.2-3.2.10** в Параграф 3.2 е организиран алгоритъм за редуциране на елементите на множеството $W(n, M, 3, \tau)$. При опит да се генерира множеството $W(n-1, 2M/3, 3, \tau-1)$, се установява, че то дори за относително малки параметри има много голяма мощност. Дори множеството $P(n-1, 2M/3, 3, \tau-1)$ се състои от прекалено много елементи. Това е причината в Параграф 3.3 да бъде описан алгоритъм, който работи единствено върху множеството от вътрешни за ортогоналния масив точки $P(n, M, 3, \tau)$. Благодарение на него е доказана следната теорема.

Теорема 3.3.1 *Троичен ортогонален масив с параметри $(17, 108, 3, 3)$ не съществува.*

По този начин получаваме, че в троичния случай имаме $5 \leq \Lambda(17, 3, 3)$.

Трета глава е написана въз основа на следните две публикации: [6] и [7].

В последната *четвърта глава* е въведено понятието енергия на ортогонален масив в пространството $H(n, q)$.

Определение 4.0.2 *Нека C е ортогонален масив (дизайн) в $H(n, q)$ с параметри (n, M, q, τ). За всяка функция (потенциал) $h(t) : [-1, 1] \to (0, +\infty)$ ще дефинираме h-енергията (или потенциалната енергия) на ортогоналния масив C по следния*

начин:

$$\mathcal{E}(n, C; h) := \frac{1}{|C|} \sum_{x,y \in C, x \neq y} h(\langle x, y \rangle).$$

Двете основни задачи при работата с енергии на ортогонални масиви целят при фиксирана функция h да се намерят минималната и максималната стойност на енергията.

Задача 4.0.3 *За фиксирани потенциал h, дължина на векторите n, сила τ и мощност $|C| = M = \lambda q^\tau$ да се намери минималната възможна енергия $\mathcal{L}(n, M; \tau; h)$, за която съществува (n, M, q, τ) ортогонален масив (τ-дизайн) C в $H(n, q)$, т.е. да се оцени величината*

$$\mathcal{L}(n, M; \tau; h) := \min\{\mathcal{E}(n, C; h) \ : \ |C| = M, \ C \subset H(n, q) \text{ е } \tau\text{-дизайн}\}.$$

Задача 4.0.4 *За фиксирани потенциал h, дължина на векторите n, сила τ и мощност $|C| = M = \lambda q^\tau$ да се намери максималната възможна енергия $\mathcal{U}(n, M; \tau; h)$, за която съществува (n, M, q, τ) ортогонален масив (τ-дизайн) C в $H(n, q)$, т.е. да се оцени величината*

$$\mathcal{U}(n, M; \tau; h) := \max\{\mathcal{E}(n, C; h) \ : \ |C| = M, \ C \subset H(n, q) \text{ е } \tau\text{-дизайн}\}.$$

Използваме комбинаторни похвати, за да остойностим горните проблеми. За целта е необходимо да въведем следната дефиниция.

Определение 4.1.1 *Нека $C \subset H(n, q)$ е (n, M, q, τ) ортогонален масив и $x \in C$ е точка относно която масивът C има спектър $P(x) = (p_0(x), p_1(x), \ldots, p_n(x))$. Енергия на спектъра $P(x)$ на даден ортогонален масив C, относно вътрешната му точка x ще наричаме стойността*

$$\mathcal{E}(x, C; h) := \frac{1}{|C|} \sum_{i=1}^{n} p_i(x) h(t_i),$$

където $t_i = 1 - \frac{2i}{n}$, т.е. t_i пробягва множеството T_n от скаларни произведения в $H(n, q)$. Тази енергия понякога ще наричаме също енергия на точката $x \in C$.

Нека $C = (n, M, \tau)$ е ортогонален масив в $H(n, q)$, а $P_1(x_1), P_2(x_2), \ldots, P_s(x_s)$ са различните спектри на един ортогонален масив спрямо всички вътрешни точки с кратности $k_1, k_2, \ldots, k_s$, съответно. Тогава е в сила следната теорема.

Теорема 4.1.2 *Нека C е (n, M, q, τ) ортогонален масив в $H(n, q)$, за който $P_1(x_1)$, $P_2(x_2)$, ..., $P_s(x_s)$ са всички различни спектри за някоя вътрешна точка на C, които се появяват с кратности $k_1, k_2, \ldots, k_s$ пъти, съответно. Тогава енергията на ортогоналния масив C може да се пресметне по следния начин:*

$$\mathcal{E}(n, C; h) = \sum_{i=1}^{s} k_i \mathcal{E}(x_i, C; h).$$

По-точно в сила е следното равенството

$$\mathcal{E}(n, C; h) \in \mathcal{E}(M) := \Big\{ \sum_{k_1+k_2+\cdots+k_s=M} k_i \mathcal{E}(x_i, C; h) \Big\}.$$

Ако имаме генерирането множеството $P(n, M, q, \tau)$ от всички възможни спектри на вътрешни точки и то има вида $P(n, M, \tau) = \{P_1(x_1), P_2(x_2), \ldots, P_s(x_s)\}$. Означаваме най-малката и най-голямата енергия на точките от това множество

$$p = \min\{E(x_i, C; h) : s = 1, 2, \ldots, s\}$$

и

$$P = \max\{E(x_i, C; h) : s = 1, 2, \ldots, s\}.$$

Получени са следните комбинаторни граници за енергията на точка x от (n, M, q, τ) ортогонален масив C.

Теорема 4.2.1 *Нека p и P са съответно минималната и максималната възможна енергия на точка x от (n, M, q, τ) ортогонален масив (τ-дизайн) $C \subset H(n, q)$. Тогава са в сила следните зависимости*

$$Mp \leq \mathcal{L}(n, M, \tau; h) \leq \mathcal{U}(n, M, \tau; h) \leq MP.$$

Важно следствие от тези теореми представлява частният случай, когато ортогоналния масив C притежава единствен спектър. Тогава можем да пресметнем точната на енергия на ортогоналния масив.

Следствие 4.2.3 *Нека параметрите q, n, M и τ са такива, че всеки (n, M, q, τ) ортогонален масив в $H(n, q)$ има единствен възможен спектър $P = P(x)$, относно вътрешна за него точка, което е еквивалентно на факта, че за всяко $x \in C$ енергия на точката x от дизайна C е точно $ME(x, C; h)$. Тогава за всеки потенциал h такива ортогонални масиви притежават оптимална енергия, т.е.*

$$\mathcal{E}(n, C; h) = \mathcal{L}(n, M, \tau; h) = \mathcal{U}(n, M, \tau; h) = M\mathcal{E}(x, C; h).$$

Важно е да отбележим, че в [20, 10] е необходимо разглежданите потенциали да са абсолютно монотонни функции в интервала $[-1, 1)$, докато комбинаторните граници, получени от нас са валидни за произволен потенциал.

За пълнота на изложението е показана Универсалната граница за енергии на ортогонални масиви [12] и е направено сравнение между двете граници. В някои случаи комбинаторната граница дава по-добри резултати, докато в други случаи универсалната граница се оказва по-мощна.

Четвърта глава е написана въз основа на следната публикация [18].

Всички изчисления и алгоритми, направени за целите на настоящия труд, са реализирани на Maple. Актуалните резултати се поддържат и могат да бъдат намерени на следния адрес [59], а кодът на алгоритмите може да бъде предоставен при поискване.

Научни приноси

По преценка на автора основните приноси на дисертационния труд са следните:

1. Разработен е и е приложен алгоритъм (Алгоритъм 1) за редуциране на множеството от спектри $P(n, M, \tau)$ относно вътрешни точки на двоичен ортогонален (n, M, τ) масив;

2. Разработен е и е приложен алгоритъм (Алгоритъм 2 - основен алгоритъм) за редуциране на множеството от спектри $W(n, M, \tau)$ на двоичен ортогонален (n, M, τ) масив;

3. Разработен е и е приложен алгоритъм (Алгоритъм 3 - обобщен алгоритъм) за редуциране на множеството от спектри $W(n, M, \tau)$ на двоичен ортогонален (n, M, τ) масив чрез премахване на два стълба;

4. Намерена е точна стойност на минималния възможен индекс на даден ортогонален масив за следните параметри

$$\Lambda(9, 4, 2) = \Lambda(10, 4, 2) = \Lambda(11, 4, 2) = \Lambda(12, 4, 2) = 8 \text{ и}$$

$$\Lambda(10, 5, 2) = \Lambda(11, 5, 2) = \Lambda(12, 5, 2) = \Lambda(13, 5, 2) = 8;$$

5. Разработен е и е приложен алгоритъм (Алгоритъм 5 - основен алгоритъм) за редуциране на множеството от спектри $W(n, M, \tau)$ на троичен ортогонален (n, M, τ) масив;

6. Разработен е и е приложен алгоритъм (Алгоритъм 6) за редуциране на множеството от спектри $P(n, M, \tau)$ относно вътрешни точки на (n, M, τ) троичен ортогонален масив;

7. Подобрена е долната граница за минималния възможен индекс на $(17, 108, 3, 3)$ ортогонален масив т.е. доказано е, че $\Lambda(17, 3, 3) \geq 5$;

8. Разработен е и е приложен алгоритъм (Алгоритъм 7) за пресмятане границите за енергиите на ортогоналните масиви при фиксиран потенциал;

9. Намерена ни са следните комбинаторни граници за стойността на енергията на (n, M, q, τ) ортогонален масив

$$Mp \leq L(n, M, \tau; h) \leq U(n, M, \tau; h) \leq MP.$$

Апробация на резултатите

Резултатите, които са описани в настоящия труд, са публикувани в следните 6 статии:

[16] Boyvalenkov P., Kulina H., Marinova T., Stoyanova M., Nonexistence of binary orthogonal arrays via their distance distributions, *Problems of Information Transmission*, Vol. 51(4), pages: 326–334 (2015), (Original Russian Text Published in Problemy Peredachi Informatsii, Vol. 51(4), pages: 23–31 (2015), ISSN: 0555-2923), Print ISSN: 0032-9460, Online ISSN: 1608-3253, https://doi.org/10.1134/S003294601504002X, Ref Web of Science, Impact Factor: 0.632 (2015), Quartile: Q_3 (2015).

[18] Peter Boyvalenkov, Tanya Marinova, Maya Stoyanova, Mila Sukalinska, Distance distributions and energy of designs in Hamming spaces, *Serdica Journal of Computing*, Vol. 9, No. 2, pages: 139–150 (2015), ISSN: 1314-7897 (Online), ISSN: 1312-6555 (Print), Ref zbMATH (Zbl 1387.94112).

[17] Peter Boyvalenkov, Tanya Marinova, Maya Stoyanova, Nonexistence of a few binary orthogonal arrays, *Discrete Applied Mathematics*, Vol. 217(2), pages: 144–150 (2017), ISSN: 0166-218X, https://doi.org/10.1016/j.dam.2016.07.023, Ref Web of Science, Impact Factor: 0.932 (2017), Quartile: Q_3 (2017).

[43] Tanya Marinova, Maya Stoyanova, Nonexistence of $(9, 112, 4)$ and $(10, 224, 5)$ binary orthogonal arrays, *Electronic Notes in Discrete Mathematics (containing the Proceedings of ACCT XV)*, Vol. 57, pages: 153-159 (March 2017), ISSN: 1571-0653, Ref Scopus, SJR: 0.262 (2017), SNIP 0.401 (2017), http://doi.org/10.1016/j.endm.2017.02.026.

[7] Boumova S., Marinova T., Ramaj T., Stoyanova M., Nonexistence of (17, 108, 3) ternary orthogonal array, *Ann. Sofia Univ., Fac. Math and Inf.*, Vol. 106, pages: 117-126 (2019), ISSN: 1313-9215 (print), ISSN: 2603-5529 (online), Ref MathSciNet (MR4125835).

[6] Boumova S., Marinova T., Stoyanova M., On ternary orthogonal arrays, *Proceedings Sixteenth International Workshop on Algebraic and Combinatorial Coding Theory*, ACCT XVI, September 2-9, 2018, Svetlogorsk (Kaliningrad region), Russia, pages: 102-105 (2018).

Резултатите от публикации [17] и [43] са анонсирани на Fifteenth International Workshop on Algebraic and Combinatorial Coding Theory, ACCT–15, June 18-24, 2016, Albena, Bulgaria.

Две от публикациите са с импакт фактор ([16],[17]), една е с SJR ([43]), а две са реферирани в научните бази от данни ZbMath и MathSciNet ([18], [7]).

Публикациите са цитирани 12 пъти, като 10 от тези цитати са в Web of Science или Scopus, т.е. в реферирани и индексирани издания.

Във всички публикации съавтор е моят научен ръководител - доц. д-р Мая Стоянова. В публикации [16], [17] и [18] съавтор е също и проф. дмн Петър Бойваленков. Със съавтор доц. д-р Силвия Бумова са статиите [6] и [7], като в последната съавтор е също така докторант Тедис Рамай. Работата по статиите [16] е в съавторство и с доц. д-р Христина Кулина, а в [18] съавтор е и Мила Сукалинска.

Резултатите в настоящия труд са докладвани от мен на

- Юбилейна конференция 125 години математика и природни науки в СУ "Св. Климент Охридски", София, Декември 2014,

- Национален семинар по теория на кодирането "Проф. Стефан Додунеков", Велико Търново, Ноември 2014,
- Национален семинар по теория на кодирането "Проф. Стефан Додунеков", Чифлик, Ноември 2015,
- Пролетна научна сесия на ФМИ-СУ, Секция "Алгебра, Геометрия и Топология", София, Март 2015,
- Пролетна научна сесия на ФМИ-СУ, Секция "Алгебра, Геометрия и Топология", София, Март 2016,
- Семинар към секция Математически основи на информатиката на ИМИ-БАН, София, Декември 2015,
- 15та Международна конференция по Алгебрична и комбинаторна теория на кодирането, Албена, Юни 2016,
- Национален семинар по теория на кодирането "Проф. Стефан Додунеков", Чифлик, Ноември 2019.

Декларация за оригиналност на резултатите

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

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

Подпис:

Благодарности

Бих искала да изкажа голямата си благодарност към научния си ръководител доц. д-р Мая Стоянова за ценните съвети, напътствията и оказаната подкрепа. Благодаря на проф. дмн Петър Бойваленков за доверието, което ми оказа и за идеите и знанията, които успя да ми предаде. Благодарна съм на всеки един мой съавтор - доц. д-р Силвия Бумова, доц. д-р Христина Кулина, Мила Сукалинска и Тедис Рамай, за различните гледни точки и чудесната работа в екип.

Благодаря на всички колеги от катедра Алгебра за вярата в мен и окуражителните думи, които получавах от тях.

Не на последно място искам да благодаря на моя съпруг за безрезервната подкрепа, която ми оказваше във всеки един момент, за грижите за децата ни, докато пишех тази дисертация, и за факта, че винаги е бил мое вдъхновение и опора.

Библиография

[1] Abramowitz M., Stegun I.A., Handbook of Mathematical Functions, with Formulas, Graphs, and Mathematical Tables, *National Bureau of Standards*, Applied Mathematics Series, Vol. 55 (1964).

[2] Angelopoulos P., Evangalaras H., Koukouvinos C.,Lappas E., An effective step-down algorithm for the construction and the identification of non-isomorphic orthogonal arrays, *Metrika*, Vol. 66 (2), 139-149 (2007).

[3] Alon N., Goldreich O., Hastad J., Peralta R., Simple construction of almost k-wise independent random variables, *Random Struct. Algor.*, Vol. 3, 289-304 (1992).

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

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

[6] Boumova S., Marinova T., Stoyanova M., On ternary orthogonal arrays, *Proc. Sixteenth International Workshop on Algebraic and Combinatorial Coding Theory, ACCT–16*, September 2-9, 2018, Svetlogorsk (Kaliningrad region), Russia, 102-105 (2018).

[7] Boumova S., Marinova T., Ramaj T., Stoyanova M., Nonexistence of $(17, 108, 3)$ ternary orthogonal array, *Ann. Sofia Univ., Fac. Math and Inf.*, Vol. 106, 117-126 (2019).

[8] Boumova S., Ramaj T., Stoyanova M., Computing distance distributions of ternary orthogonal arrays, *Compt. rend. Acad. bulg. Sci.*, 2020, accepted.

[9] Boyvalenkov P., Computing distance distributions of spherical designs, *Linear Algebra and Its Applications*, Vol. 226/228, 277-286 (1995).

[10] P. G. Boyvalenkov, P. D. Dragnev, D. P. Hardin, E. B. Saff, M. M. Stoyanova, Energy bounds for codes and designs in Hamming spaces, *Designs, Codes and Cryptography*, Vol. 82, Issue I, pp. 411–433 (2017).

[11] P. Boyvalenkov, D. Danev, On linear programming bounds for codes in polynomial metric spaces, *Problems of Information Transmission*, Vol. 34, No. 2, pp. 108-120 (1998).

[12] Peter Boyvalenkov, Danyo Danev, Maya Stoyanova, Refinements of Levenshtein bounds in q-ary Hamming spaces, *Problems of Information Transmission*, Vol. 54, No. 4, pp. 329–342 (2018).

[13] Boyvalenkov P., Kulina H., Computing distance distributions of orthogonal arrays, *Proc. Intern. Workshop ACCT2010*, Novosibirsk, Sept., 82-85 (2010).

[14] Boyvalenkov P., Kulina H., Investigation of binary orthogonal arrays via their distance distributions, *Problems of Information Transmission*, Vol. 49(4), 320-330 (2013). (Original Russian text: Problemy Peredachi Informatsii, Vol. 49, No. 4, 28–40, 2013).

[15] Boyvalenkov P., Kulina H., Stoyanova M., Nonexistence of certain binary orthogonal arrays, *Proc. 7th Intern. Workshop on Optimal Codes and Related Topics*, Sep. 6-12, 2013, Albena, Bulgaria, 65-70 (2013).

[16] Boyvalenkov P., Kulina H., Marinova T., Stoyanova M., Nonexistence of binary orthogonal arrays via their distance distributions, *Problems of Information Transmission*, Vol. 51(4), 326-334 (2015).

[17] Boyvalenkov P., Marinova T., Stoyanova M., Nonexistence of a few binary orthogonal arrays, *Discrete Applied Mathematics*, Vol. 217(2), 144-150 (2017).

[18] Peter Boyvalenkov, Tanya Marinova, Maya Stoyanova, Mila Sukalinska, Distance distributions and energy of designs in Hamming spaces, *Serdica Journal of Computing*, Vol. 9, No. 2, 139–150 (2015).

[19] Bulutoglu D.A., Margot F., Classification of orthogonal arrays by integer programming, *Jornal of Statistical Planning and Inference*, Vol. 138, 654-666 (2008).

[20] Cohn H., Zhao Y., Energy-minimizing error-correcting codes, *IEEE Transactions on Information Theory*, Vol. 60, 7442-7450. (2014).

[21] Delsarte P., An Algebraic Approach to the Association Schemes in Coding Theory, *Philips Res. Rep. Suppl.*, Vol. 10, 1973.

[22] Delsarte P., Four fundamental parameters of a code and their combinatorial signficance, *Information and Control*, Vol. 23, 407-438 (1973).

[23] Delsarte P., Levenshtein L.I., Association schemes and coding theory, *IEEE Transactions on Information Theory*, Vol. 44, 2477-2504 (1998).

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

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

[26] Fazekas G., Lenvestein V.I., On Upper Bounds for Code Distance and Covering Radius of Designs in Polynomial Metric Spaces, *Journal of combinatorial theory*, Series A, Vol. 70, 267-288 (1995).

[27] Hamming, R. W., Error detecting and error correcting codes, *Bell System Technical Journal*, Vol. 29, 147–160 (1950).

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

[29] Helleseth T., Kløve T., Lenvestein V.I., A bound for codes with given minimum and maximum distances,' *IEEE International Symposium on Information Theory* Seattle, USA, 292–296 (2006).

[30] Jackson W. A., Martin K., A combinatorial interpretation of ramp schemes, *Australasian Journal of Combinatorics*, Vol. 14, 51–60 (1996).

[31] Petteri Kaski, Patric R.J. Östergård, Classification Algorithms for Codes and Designs, *Springer Verlag*, Berlin Heidelberg (2006).

[32] Khalyavin A. V., Estimates of the capacity of orthogonal arrays of large strength, *Moscow Univ. Math. Bull.*, Vol. 65, 130-131 (2010).

[33] Kleinberg, Jon; Tardos, Éva, Algorithm Design (2nd ed.), *Addison-Wesley*, ISBN 0-321-37291-3 (2006).

[34] I.Krasikov, S.Litsyn, On integral zeros of Krawtchouk polynomials, Journal of Combinatorial Theory, *Ser. A*, 74(1), 71-99 (1996).

[35] I.Krasikov, S.Litsyn, Linear programming bounds for codes of small codes, *Europ. J. Comb.*, Vol.18, 647-656 (1997).

[36] Kurosawa K., Johannsson T., Stinson D. R., Almost k-wise independent sample spaces and their cryptologic applications, *Journal of Cryptology*, Vol. 14, 231–253 (2001).

[37] Levenshtein V.I., Krawtchouk polynomials and universal bounds for codes and designs in Hamming spaces, *IEEE Transactions on Information Theory*, Vol. 41, 1303-1321 (1995).

[38] Levenshtein V.I., Universal bounds for codes and designs, *Handbook of Coding Theory*, V. S. Pless and W. C. Huffman, Eds., Elsevier, Amsterdam, Ch. 6, 499-648 (1998).

[39] Levenshtein V.I., Designs as maximum codes in polynomial metric spaces, *Acta Applicandae Mathematica*, Vol. 29, 1-82 (1992).

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

[41] MacWilliams F. J. , Sloane N. J. A., The Theory of Error-Correcring Codes, Amsterdam, The Netherlands: North Holland, 1977.

[42] Manev, N. L., On the distance distributions of Orthogonal Arrays, *Problems of Information Transmission*, Vol. 56, 45–55 (2020).

[43] Marinova T., Stoyanova M., Nonexistence of $(9, 112, 4)$ and $(10, 224, 5)$ binary orthogonal arrays, *Electronic Notes in Discrete Mathematics*, containing the Proceedings of ACCT XV, Vol. 57, 153–159 (2017).

[44] Nikiforov A. F., Suslov S. K., Uvarov V. B. , Classical Orthogonal Polynomials of a Discrete Variable *Springer Series in Computational Physics*, Berlin: Springer-Verlag (1991).

[45] Ostergard P.R.J., Baicheva T., Kolev E., Optimal binary one-error-correcting codes of length 10 have 72 codewords, *IEEE Transactions on Information Theory*, Vol. 45, 1229-1231 (1999).

[46] A. Perttula, Bounds for binary and nonbinary codes slightly outside of the Plotkin range, *Tampere University of Technology Publ.*, 14 (1982).

[47] Plotkin M., Binary codes with specified minimum distance, *IRE Transactions on Information Theory*, Vol. 6, 445–450 (1960).

[48] Raghavarao D., Constructions and Combinatorial Problems in Design of Experiments, New York : Wiley, 1971.

[49] Rao C. R., Factorial experiments derivable from combinatorial arrangements of arrays, *J. Royal Stat. Soc.*, Vol. 89, 128-139 (1947).

[50] A. Samorodnitsky, On the optimum of Delsarte's linear program, *J. Combin. Theory*, Ser. A 96, 261-287 (2001).

[51] Schoen E. D., Eendebak P. T., Nguyen M. V. M., Complete enumeration of pure-level and mixed-level orthogonal arrays, *Journal of Combinatorial Designs*, Vol. 18, 123-140 (2009).

[52] Seiden E., Zemach R., On orthogonal arrays, *Ann. Math. Statist.*, Vol. 37, 1355-1370 (1996).

[53] Singleton R. C., Maximum distance q-ary codes, *IEEE Transactions on Information Theory*, Vol. 10, 116-118 (1964).

[54] J. Stuffken, B. Tang, Complete enumeration of two-level orthogonal arrays of strength d, *The Annals of Statistics*, Vol. 35, 793–814 (2007).

[55] Szegő G., *Orthogonal Polynomials*, American Mathematical Society Colloquium Publications 23, Providence, RI, 1939.

[56] Taguchi, G., System of Experimental Design: Engineering Methods to Optimize Quality and Minimize Costs, *UNIPUB/Kraus International Publications*, 1987.

[57] Vaudenay S., Decorrelation: A theory for block cipher security, *Journal of Cryptology*, Vol. 16, 249–286 (2003).

[58] http://neilsloane.com/oadir/index.html

[59] https://store.fmi.uni-sofia.bg/fmi/algebra/mstoyanova.shtml