Институт по Математика и Информатика
Българска Академия на Науките

Секция "Математически Основи на Информатиката"

КОНСТАНТИН ВАСИЛЕВ ДЕЛЧЕВ

Кодове и дизайни в полиномиални метрични пространства

автореферат на дисертация
за получаване на образователната и научна степен доктор
професионално направление 4.6
информатика и компютърни науки

научен ръководител: проф. дмн Петър Бойваленков
ИМИ-БАН

София
2 0 2 1

В дисертацията се разглеждат кодове и дизайни с малък брой разстояния в някои метрични пространства. Най-простите такива кодове, тези с едно и също разстояние между всеки два елемента се наричат **еквидистантни** и са сред първите обекти, изследвани в областта. Допускането на две и повече разстояния, обаче, позволява много по-голямо богатство от структури. Пространствата, които се разглеждат, са единичната сфера в n-мерното Евклидово пространство $\mathbb{R}^n$ и някои крайни линейни пространства с Хемингова метрика.

Глава 1. Увод

Първата глава на дисертацията въвежда основни понятия от теория на кодирането и класически резултати за сферични кодове и дизайни, получени чрез метода на линейното програмиране.

Дефиниция 1.1 **Код** ще наричаме всяко крайно непразно множество от точки в метрично пространство.

Дефиниция 1.2 Ако един код е подпространство в съответното пространство, то той се нарича **линеен**.

Дефиниция 1.3 **Минимално разстояние** на код ще наричаме минималното разстояние между две различни точки на кода.

От тези дефиниции, по естествен начин възникват и основните параметри на един код C – мощност, $M = |C|$, размерност n на разглежданото пространство и разстоянията между точките в C, като в частност най-голямо значение има минималното разстояние d. Понякога, вместо с минималното разстояние ще работим с максималното скаларно произведение s от съображения за удобство. Кодове с тези параметри ще наричаме (n, M, d) или (n, M, s)-кодове. Първият и най-естествен въпрос, който възниква, е какви са взаимовръзките между тези параметри, т.нар. **основна задача на теория на кодирането**.

Задача 1.1 При фиксирани n и d, да се намери $M(n, d)$, най-голямото естествено число M, за което съществува (n, M, d)-код.

Задача 1.2 При фиксирани n и M, да се намери $d(n, M)$, най-голямото число d, за което съществува (n, M, d)-код.

Нека $\mathbb{M}$ е метрично пространство с краен диаметър $D_{\mathbb{M}}$ и крайна мярка $\mu_{\mathbb{M}}$. Нека Хилбертовото пространство $\mathcal{L}_2(\mathbb{M})$ е директна сума от изброимо много взаимно-ортогонални подпространства V_i:

$$\mathcal{L}_2(\mathbb{M}) = V_0 \oplus V_1 \oplus ...$$

Нека $r_i = dim(V_i)$ и V_i са такива, че съществуват полиноми с реални коефициенти G_i от степен i, за които е изпълнено

$$G_i(t_{\mathbb{M}}(d_{\mathbb{M}}(x, y))) = \frac{1}{r_i} \sum_{j=1}^{r_i} v_{ij} \overline{v_{ij}},$$

където полиномите v_{ij} формират ортонормиран базис на V_i и $t_{\mathbb{M}}$ е непрекъсната намаляваща функция, за която $t_{\mathbb{M}}(0) = 1$ и $t_{\mathbb{M}}(D_{\mathbb{M}}) = -1$. Тогава ще наричаме $\mathbb{M}$ **полиномиално метрично пространство**, а G_i - **зонални сферични функции** [11].

Тази дефиниция е неконструктивна, но описва добре свойствата, които са необходими, за да бъде приложим метода на линейното програмиране. Безкрайните пространства, които я удовлетворяват са евклидовата сфера и някои проективни пространства. Крайните не са напълно класифицирани.

Нека разгледаме стандартното n-мерно евклидово пространство $\mathbb{R}^n$ с разстояние и скаларно произведение за произволни точки $x = (x_1, ..., x_n)$ и $y = (y_1, ..., y_n)$ съответно:

$$d(x, y) = \sqrt{\sum_{i=1}^{n} (x_i - y_i)^2},$$

$$\langle x, y \rangle = \sum_{i=1}^{n} x_i y_i.$$

С $\mathbb{S}^{n-1}$ ще бележим единичната сфера в $\mathbb{R}^n$,

$$\mathbb{S}^{n-1} = \{x = (x_1, x_2, ..., x_n) \in \mathbb{R}^n \quad | \quad x_1^2 + x_2^2 + ... + x_n^2 = 1\}.$$

Върху нея скаларното произведение и разстоянието са свързани с равенствата

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

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

Дефиниция 1.4 Нека $C \in \mathbb{S}^{n-1}$ е непразно множество с мощност M, като най-голямото скаларно произведение между различни точки на C е равно на s. Тогава C е (n, M, s)-сферичен код.

Основната задача на теорията на кодирането, във формулировката си за сферични кодове, цели намирането на величините $A(n, s)$ и $s(n, M)$, където

$$A(n, s) = \max\{M : \exists (n, M, s) - \text{сферичен код}\},$$

$$s(n, M) = \min\{s : \exists (n, M, s) - \text{сферичен код}\}.$$

Величината $A(n, s)$ е известна за неположителни s, където тя се реализира от класически конструкции ([43, 44], виж книгите [25, **?**, 48] и референциите там). За положителни стойности на s са известни само отделни частни случаи.

Дефиниция 1.5 [27] Един n-мерен сферичен код C се нарича сферичен τ-дизайн, ако за всеки полином на n променливи от степен най-много τ е изпълнено равенството

$$\int_{\mathbb{S}^{n-1}} f(x) d\mu(x) = \frac{1}{|C|} \sum_{x \in C} f(x).$$

Тук $\mu(x)$ е стандартната лебегова мярка, нормирана с $\mu(\mathbb{S}^{-1}) = 1$.

Точките на C да бъдат разглеждани като върхове на квадратурна формула върху $\mathbb{S}^{n-1}$ с равни тегла $1/|C|$ и с алгебрична степен на точност τ, а скаларните произведения дефинират квадратурна формула върху интервала $[-1, 1]$, също с алгебрична степен на точност τ. Това показва важността на параметъра τ и търсенето на кодове с по-голямо τ.

Дефиниция 1.8 Максималното τ, за което даден сферичен код е и сферичен τ-дизайн се нарича **сила** на дизайна.

За фиксирана размерност n полиномите на Гегенбауер се дефинират чрез следната тричленна рекурентна връзка

$$(i + n - 2)P_{i+1}^{(n)}(t) = (2i + n - 2)tP_i^{(n)} - iP_{i-1}^{(n)}$$

с начални условия $P_0^{(n)}(t) = 1$ и $P_1^{(n)}(t) = t$.

Полиномите на Гегенбауер са ортогонални върху интервала $[-1, 1]$ спрямо скаларното произведение

$$\langle f, g\rangle = c_n \int_{-1}^{1} f(t)g(t)(1 - t^2)^{\frac{n-3}{2}} dt,$$

като можем да изкажем следната релация на ортогоналност в явен вид:

$$\left\langle P_i^{(n)}(t), P_j^{(n)}(t)\right\rangle = \delta_{ij}\frac{\Gamma(n-1)}{2^{n-2}\Gamma(\frac{n-1}{2})^2} = \frac{\delta_{ij}}{c_n},$$

където δ_{ij} е символът на Кронекер. Константата c_n е нормираща. Ако

$$f(t) = \sum_{i=0}^{k} a_i t^i \in \mathbb{R}[t],$$

то $f(t)$ се представя по единствен начин (поради ортогоналността) и като

$$f(t) = f_0 P_0^{(n)}(t) + f_1 P_1^{(n)}(t) + \cdots + f_k P_k^{(n)}(t).$$

Тогава за коефициентите в това развитие имаме

$$f_i = c_n \int_{-1}^{1} f(t)P_i^{(n)}(t)(1 - t^2)^{\frac{n-3}{2}} dt. \tag{1}$$

За коефициентите f_0 в развитието на полиномите t^k, $k \geq 0$ въвеждаме следното означение:

$$t^k = b_k + \sum_{i=1}^{k} P_i^{(n)}(t).$$

Те имат следния явен вид:

$$b_{2j} = \frac{(2j-1)!!}{n(n+2)\cdots(n+2j-2))},$$

За нечетни k коефициентът е 0 и това следва директно от формулата (1).

Полиномите на Гегенбауер са зонални сферични функции т.е. за тях е в сила следното равенство (вж. например [41])

$$P_i^{(n)}(\langle x, y\rangle) = \frac{1}{r_i}\sum_{j=1}^{r_i} v_{ij}(x)v_{ij}(y), \tag{2}$$

където $x, y \in \mathbb{S}^{n-1}$ и $r_i = \dim(Harm(i))$ е размерността на пространство на хомогенните хармонични полиноми (разглеждани върху $\mathbb{S}^{n-1}$) от степен i, а $v_{ij}(x)$, $j = 1, 2, \ldots, r_i$, съставляват негов ортонормиран базис. Класически резултат [46] ни дава

$$r_i = \left(\begin{array}{c} n+i-1 \\ i \end{array}\right) - \left(\begin{array}{c} n+i-3 \\ i-2 \end{array}\right) = \frac{n+2i-2}{i}\left(\begin{array}{c} n+i-3 \\ i-1 \end{array}\right).$$

За методите, които ползваме, от голямо значение са броят и подредбата на корените на полиномите на Гегенбауер и близки до тях полиноми.

Лема 1.1 Полиномът $P_k^{(n)}(t)$ има точно k различни реални нули, които се намират в интервала $[-1, 1]$.

Тези нули ще означаваме по следния начин:

$$-1 < t_{k,1} < t_{k,2} < \cdots < t_{k,k} = 1.$$

Полиномите на Гегенбауер всъщност са частен случай на полиномите на Якоби $P_i^{(\alpha,\beta)}(t)$ с параметри $\alpha = \beta = (n-3)/2$ [45]. Заедно с тях, за получаване и изследване на граници ще използваме и т.нар. съседни полиноми:

$$P_i^{a,b}(t) = \frac{P_i^{(a+(n-3)/2, b+(n-3)/2)}(t)}{P_i^{(a+(n-3)/2, b+(n-3)/2)}(1)}.$$

Те също са ортогонални в интервала $[-1, 1]$ относно тегловата функция

$$(1-t)^{a+(n-3)/2}(1+t)^{b+(n-3)/2}.$$

Също така, $P_i^{1,1}(t)$ всъщност е полином на Гегенбауер за размерност $n+2$:

$$P_i^{1,1}(t) = \frac{P_i^{1+(n-3)/2, 1+(n-3)/2}(t)}{P_i^{1+(n-3)/2, 1+(n-3)/2}(1)} = P_i^{(n+2)}(t).$$

Нека $t_k^{a,b}$ е най-голямата нула на $P_k^{a,b}(t)$, като $t_0^{-1,1} := -1$. В сила е следната лема:

Лема 1.2 [37, 38] За всяко k са в сила следните неравенства

$$t_{k-1}^{1,1} < t_k^{1,0} < t_k^{1,1} < t_{k-1}^{0,1}, \quad t_{k,k}^{1,0} < t_{k,k}.$$

Събирателната формула (2), която свързва полиномите на Гегенбауер и хармоничните полиноми, ни дава възможност да докажем следната основна теорема [38].

Теорема 1.1 За всеки сферичен код $C \in \mathbb{S}^{n-1}$ и за всеки полином с реални коефициенти $f(t) = \sum_{i=0}^{k} f_i P_i^{(n)}(t)$ е в сила равенството:

$$|C|f(1) + \sum_{x,y\in C, x\neq y} f(\langle x,y\rangle) = |C|^2 f_0 + \sum_{i=1}^{k} \frac{f_i}{r_i} \sum_{j=1}^{r_i} \left(\sum_{x\in C} v_{ij}(x) \right)^2. \tag{3}$$

Сумите от квадрати в дясната част на тъждеството (3) са особено важни инварианти на сферичните кодове.

Дефиниция 1.9 [12, 20] За код $C \in \mathbb{S}^{n-1}$ и естествени числа i,

$$M_i(C) = \frac{1}{r_i} \sum_{j=1}^{r_i} \left(\sum_{x\in C} v_{ij}(x) \right)^2$$

се наричат $i-$ти **моменти** на C. Ще отбележим, че $M_i \geq 0$ за всяко $i \geq 1$. В сила е следното свойство на сферичните дизайни:

Теорема 1.2 [12] Един код $\subset \mathbb{S}^{n-1}$ е сферичен τ-дизайн, $\tau \geq 1$, тогава и само тогава, когато $M_i(C) = 0$ за $i = 1, 2, \ldots, \tau$.

Тук следва да отбележим, че ако един код C е **антиподален**, т.е. $C = -C$, то $M_{2i-1}(C) = 0$ за всяко i.

Освен това работата с моментите понякога може да даде лесни доказателства за границите на линейното програмиране, както ще видим във втора глава.

Границата на линейното програмиране за сферични кодове се основава на търсене на подходящи полиноми за следната теорема, чието доказателство се получава директно от (3).

Теорема 1.3 [27, 33] Нека C е (n, M, s) сферичен код, за който $n \geq 3$, $s \in [-1, 1)$ и полиномът $f(t) = \sum_{i=0}^{k} f_i P_i^{(n)}(t)$ е такъв, че

- $f(t) \leq 0 \quad \forall t \in [-1, s]$,
- $f_0 > 0$ и $f_i \geq 0 \quad \forall i > 0$.

Тогава

$$A(n,s) \leq \frac{f(1)}{f_0}.$$

Аналогично, (3) и Теорема ни позволяват за получим обща оценка за минималната възможна мощност на сферичен τ-дизайн при фиксирани n и τ,

$$B(n,\tau) := \min\{|C| : C \subset \mathbb{S}^{n-1} \text{ е сферичен } \tau\text{-дизайн}\}.$$

Теорема 1.4 [27] Нека $C \subset \mathbb{S}^{n-1}$ е сферичен τ-дизайн, за който $n \geq 3$, $\tau \geq 1$ и полиномът $f(t) = \sum_{i=0}^{k} f_i P_i^{(n)}(t)$ е такъв, че:

- $f(t) \geq 0 \quad \forall t \in [-1, 1]$,
- $f_0 > 0$ и $f_i \leq 0 \quad \forall i > \tau$.

Тогава $|C| \geq \frac{f(1)}{f_0}$ и следователно:

$$B(n, \tau) \geq \frac{f(1)}{f_0}.$$

Отново, по подобен начин, Юдин получава и граници за енергии на сферични кодове и дизайни. Прецизирана версия на теоремата на Юдин е представена в глава 3. Потенциал наричаме:

Дефиниция 1.10 За дадена функция (потенциал) $h : [-1, 1] \to [0, +\infty]$, ще наричаме *енергия* (или потенциална енергия; също h-енергия) на сферичен код (или τ-дизайн) $C \subset \mathbb{S}^{n-1}$ следната сума

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

Следвайки [24] и [20, 19] ще разглеждаме само абсолютно монотонни потенциали h, т.е. $h^{(k)}(t) \geq 0$ за всяко $k \geq 0$ и $t \in [-1, 1)$. Класическият пример за такъв потенциал е s-потенциалът на Рис $h(t) = 1/(2(1-t))^s$. Други често използвани потенциали в литературата са

- Нютонов потенциал - $h(t) = (2 - 2t)^{\frac{-(n-2)}{2}}$;
- Логаритмичен потенциал - $h(t) = \log(2 - 2t)$;
- Гаусов потенциал - $h(t) = e^{2(1-t)}$.

За фиксирани n и τ Делсарт, Гьоталс и Зайдел [27] използват границата на линейното програмиране с полиномите

$$d_\tau^{(n)}(t) = \begin{cases} (t+1)\left(P_{k-1}^{1,1}(t)\right)^2, & \text{ако } \tau = 2k-1, \\ \left(P_k^{1,0}(t)\right)^2, & \text{ако } \tau = 2k. \end{cases}$$

Това води до получаването на следната граница:

$$B(n, \tau) \geq D(n, \tau) = \begin{cases} 2\binom{n+k-2}{n-1}, & \text{ако } \tau = 2k-1, \\ \binom{n+k-1}{n-1} + \binom{n+k-2}{n-1}, & \text{ако } \tau = 2k. \end{cases} \tag{4}$$

Дизайните, които достигат тази граница, се наричат плътни. Границата (4) се достига във всички размерности в следните малки случаи: при $\tau = 1$ от двойка антиподални точки, при $\tau = 2$ от 2-дизайна, образуван от върховете ($n + 1$ на брой) на правилния n-мерен симплекс, при $\tau = 3$ от 3-дизайна, образуван от върховете на ортонормирана координатна система и техните антиподални точки. Освен тези случаи са известни само осем плътни дизайна (с $n \geq 3$ и $\tau \geq 4$).

Всички тези случаи са описани от Делсарт-Гьоталс-Зайдел [27] и са единствени с точност до изометрия. Резултати за несъществуване и класификация са получени от Банай-Дамерел [4, 5], Банай-Слоен [6] и Бойваленков [1, 10] (вж. също обзорните статии [2, 3]).

Границата на Левенщейн използва серии от полиноми в различни подинтервали на $[-1, 1]$ по следния начин. Нека:

$$I_m = \begin{cases} \left[t_{k-1}^{1,1}, t_k^{1,0}\right], & \text{ако } m = 2k-1, \\ \left[t_k^{1,0}, t_k^{1,1}\right], & \text{ако } m = 2k. \end{cases}$$

и нека:

$$f_m^{(n,s)}(t) = \begin{cases} (t-s)\left(T_{k-1}^{1,0}(t,s)\right)^2, & \text{ако } m = 2k-1, \\ (t+1)(t-s)\left(T_{k-1}^{1,1}(t,s)\right)^2, & \text{ако } m = 2k. \end{cases}$$

Тук $T_k^{a,b}(t,s)$ са т.нар. **ядра на съседните полиноми** или **ядра на Кристофел-Дарбу**

$$T_k^{a,b}(t,s) = \sum_{i=0}^{k} r_i^{a,b} P_i^{(a+(n-3)/2, b+(n-3)/2)}(t) P_i^{(a+(n-3)/2, b+(n-3)/2)}(s)$$

където:

$$r_i^{a,b} = \frac{2i+a+b+n-2}{i+a+b+n-2} \cdot \frac{\binom{i+a+b+n-2}{i}\binom{i+a+(n-3)/2}{i}}{\binom{i+b+(n-3)/2}{i}}.$$

Това води до следната граница:

$$A(n,s) \leq L(n,s) = \begin{cases} L_{2k-1}(n,s) = \begin{pmatrix} k+n-3 \\ k-1 \end{pmatrix} \left[\frac{2k+n-3}{n-1} - \frac{P_{k-1}^{(n)}(s) - P_k^{(n)}(s)}{(1-s)P_k^{(n)}(s)}\right] \\ \text{за } s \in I_{2k-1}, \\ L_{2k}(n,s) = \begin{pmatrix} k+n-2 \\ k \end{pmatrix} \left[\frac{2k+n-1}{n-1} - \frac{(1+s)\left(P_k^{(n)}(s) - P_{k+1}^{(n)}(s)\right)}{(1-s)\left(P_k^{(n)}(s) + P_{k+1}^{(n)}(s)\right)}\right] \\ \text{за } s \in I_{2k}. \end{cases}$$

Функцията $L(n, s)$ е непрекъсната по s, а в краищата на интервалите I_m са в сила равенства, които я свързват с границите на Делсарт-Гьоталс-Зайдел по следния начин:

$$L_{2k-2}\left(n, t_{k-1}^{1,1}\right) = L_{2k-1}\left(n, t_{k-1}^{1,1}\right) = D(n, 2k-1) = 2\begin{pmatrix} n+k-2 \\ n-1 \end{pmatrix}, \tag{5}$$

$$L_{2k-1}\left(n,t_k^{1,0}\right)=L_{2k}\left(n,t_k^{1,0}\right)=D(n,2k)= \\ =\left(\begin{array}{c}n+k-1\\ n-1\end{array}\right)+\left(\begin{array}{c}n+k-2\\ n-1\end{array}\right). \tag{6}$$

За нас е важна разбивката на $[-1,1)$ на интервали и свързаните с нея квадратурни формули. Нека $\alpha_0,\dots,\alpha_{k-1}$ са корените на уравнението

$$P_k^{1,0}(t)P_{k-1}^{1,0}(s)-P_k^{1,0}(s)P_{k-1}^{1,0}(t)=0$$

и $\beta_0=-1$, а $\beta_1,\dots,\beta_k$ са корените на

$$P_k^{1,1}(t)P_{k-1}^{1,1}(s)-P_k^{1,1}(s)P_{k-1}^{1,1}(t)=0.$$

Левенщейн доказва [39, 41], че те са различни и се намират в интервала $[-1,1]$. Нещо повече, пак там той доказва и следната формула от тип на Гаус-Якоби:

$$f_0=\begin{cases}\dfrac{f(1)}{L_{2k-1}(n,s)}+\displaystyle\sum_{i=0}^{k-1}\rho_i f(\alpha_i), & \text{ако } m=2k-1,\\ \dfrac{f(1)}{L_{2k}(n,s)}+\displaystyle\sum_{i=0}^{k}\gamma_i f(\beta_i), & \text{ако } m=2k.\end{cases} \tag{7}$$

за всеки полином от степен, ненадминаваща m.

Глава 2. Максимални антиподални кодове с малък брой разстояния

Методът на линейното програмиране е по същество алгебричен. Изучаването на комбинаторните свойства, представлява независим от него подход, който играе важна роля в изследването на кодове и дизайни с параметри близки до оптималните. В глава 2 на дисертацията разглеждаме антиподални кодове, за които тези комбинаторни свойства носят допълнителна информация. Резултатите, в нея са публикувани в [13] и са получени посредством класическия подход чрез изследване на производните кодове.

Дефиниция 2.1 С $A(C)$ ще бележим множеството от скаларните произведения между различни елементи на сферичния код C.

Дефиниция 2.2 За фиксирана точка $x\in C$ и $t\in[-1,1)$ означаваме

$$A_t(x)=|\{y\in C:\langle x,y\rangle=t\}|.$$

Ще наричаме **спектър на C относно x** системата от естествени числа

$$(A_t(x):t\in[-1,1)\,,\exists y\in C,\langle x,y\rangle=t),$$

а самите числа $A_t(x)$ наричаме **елементи на спектъра**.

В случая na антиподален код (такъв код C за който $C=-C$) директно получаваме свойствата:

$$A_{-1}(x)=1\quad\forall x\in C,$$

$$A_t(x) = A_{-t}(x) \quad \forall x \in C, \quad \forall t \in [-1,1],$$
$$\sum_{t\in(-1,1)} A_t(x) = |C| - 2 \quad \forall x \in C.$$

Дефиниция 2.3 Нека $C \in \mathbb{S}^{n-1}$ е сферичен код, $x \in C$ и α е такова число, за което $A_\alpha(x) > 0$. Тогава множеството

$$C_\alpha(x) = \{y \in C : \langle x, y\rangle = \alpha\}$$

се нарича производен код на C.

Ясно е, че след подходяща хомотетия $C_\alpha(x)$ става $(n-1, |C_\alpha(x)|, s')$-код, където s' ще бъде определено по-долу.

Теорема 2.1 [27] Всички скаларни произведения на $C_\alpha(x)$ принадлежат на множеството

$$I_{\alpha,x} = \left\{\frac{\beta - \alpha^2}{1-\alpha^2} : \beta \in A(C)\right\} \cap [-1,1).$$

В частност, максималното скаларно s' произведение на $C_\alpha(x)$ е най-голямото число в $I_{\alpha,x}$, т.е. $s' = \frac{s-\alpha^2}{1-\alpha^2}$.

Други свойства на производните кодове са:

Теорема 2.2 [27] Ако C е сферичен τ-дизайн, то $C_\alpha(x)$ е сферичен $(\tau - \ell + 1)$-дизайн, където $\ell = |I_{\alpha,x}|$.

Теорема 2.3[27] Нека C е сферичен τ-дизайн с мощност $|C| = M$ и нека броят на различните скаларни произведения между различни точки на C е q. Тогава, ако $q \leq \tau+1$, то елементите на спектъра $A_t(x)$ не зависят от x и могат да бъдат представени като функции на n, M и стойностите на скаларните произведения.

Кодове и дизайни с това свойство ще наричаме **регулярни** и ще изпускаме аргумента x при означенията на елементите на спектъра A_t, които наричаме спектър на кода.

Антиподалните кодове, които имат само скаларни произведения -1 и $\pm s$, където $s \in (0,1)$ дефинират множества от прави (по една през всяка двойка антиподални точки), които се наричат **равноъгълни прави** (equiangular lines). Те са въведени за първи път през 1948 г. от Хаантьес [30]. Наричат се още и "плътни рамки" (tight frames), а техен частен случай са т.нар. SIC-POVM (симетрични, информационно-пълни, положителни операторнозначни мерки), които имат приложение в квантовата криптография [28].

Дефиниция 2.4 За дадени $n \geq 3$ и $s \in (0,1)$ означаваме

$$M_n(s) := \max\{|C| : C \subset \mathbb{S}^{n-1} \text{ е антиподален и } A(C) = \{-1, \pm s\}\}.$$

Един от класическите резултати за равноъгълни прави е т.нар. теорема от тип на Лойд [8], която твърди, че ако $C \subset \mathbb{S}^{n-1}$ е антиподален код, $A(C) = \{-1, \pm s\}$ и мощност $|C| > 2n$ (т.е. $M_s(n) > 2n$), то $s = \frac{1}{2\ell+1}$, където ℓ е естествено число.

Граници за линейното програмиране за равноъгълни прави са получени от Барг и Ю [8]. Ние получаваме един от тяхните резултати с директно доказателство, базирано на целочислеността на спектъра.

Теорема 2.4 Ако n, k и ℓ са такива, че

$$P_{2k}^{(n)}(\frac{1}{2\ell+1}) < 0,$$

то

$$M_{2\ell+1}(n) \leq 2 - \frac{2}{P_{2k}^{(n)}(\frac{1}{2\ell+1})}.$$

При $k = 1$ имаме $P_2^{(n)}(t) = \frac{nt^2-1}{n-1}$, откъдето следва границата

$$M_{2\ell+1}(n) \leq \frac{8n\ell(\ell+1)}{(2\ell+1)^2 - n}, \tag{8}$$

валидна при $n < (2\ell+1)^2$. Границата (8) е известна с името "относителна граница" [42].

При $k = 2$ имаме $P_4^{(n)}(t) = \frac{(n+2)(n+4)t^4-6(n+2)t^2+3}{n^2-1}$, откъдето получаваме

$$M_{2\ell+1}(n) \leq \frac{2(n-2)((2\ell+1)^4(n+2)+6(2\ell+1)^2-n-4)}{6(2\ell+1)^2(n+2)-3(2\ell+1)^4-(n+2)(n+4)},$$

като тази граница е в сила, когато

$$6(2\ell+1)^2(n+2) - 3(2\ell+1)^4 - (n+2)(n+4) > 0.$$

Тази граница е по-добра от относителната за $n \geq 96$ и всички ℓ. Може да се предположи, че тази тенденция ще продължи, с по-високи степени, подобряващи границата за по-високи размерности, но числените експерименти показват, че границата, получена при $k = 2$, остава оптимална (в рамките на Теорема) поне до $n = 900$.

Първото от двете естествени продължения на изследването на равноъгълните прави е да разгледаме антиподален код $C \subset \mathbb{S}^{n-1}$ с мощност $M = |C|$ и скаларни произведения -1, $\pm s$ и 0, т.е. $A(C) = \{-1, 0, \pm s\}$.

За тези кодове получаваме следният резултат:

Теорема 2.5 Нека C е антиподален (n, M, s)-сферичен код със скаларни произведения -1, $\pm s$ и 0, като $s^2 < 3/(n+2)$. Тогава

$$M \leq \frac{2n(n+2)(1-s^2)}{3-s^2(n+2)}.$$

Доказателството се получава посредством основното тъждество и полинома $f(t) = t^2(t^2 - s^2)$. Чрез изследване на спектъра, получаваме следните теореми:

Теорема 2.6 Ако C е антиподален (n, M, s)-сферичен код със скаларни произведения -1, $\pm s$ и 0, който достига границата от **Теорема 2.5**, то s е рационално число.

Теорема 2.7 Нека C е антиподален (n, M, s)-сферичен код със скаларни произведения -1, $\pm s$ и 0, който е сферичен 3-дизайн, и $k \geq 2$ е такова, че

$$P_{2k}^{(n)}(s) + (ns^2 - 1)P_{2k}^{(n)}(0) < 0.$$

Тогава

$$M \leq \frac{n\left(2ns + (1-2s^2)P_{2k}^{(n)}(0) - P_{2k}^{(n)}(s)\right)}{\left|P_{2k}^{(n)}(s) + (ns^2-1)P_{2k}^{(n)}(0)\right|}. \tag{9}$$

Второто естествено продължение на изследването на равноъгълните прави е да се добави втори ъгъл, т.е. да разгледаме "двуъгълни прави". Те също представляват интерес от инженерна гледна точка и на тяхното изследване има посветени няколко публикации, като например [29, 32].

В този случай аналогът на относителната граница има следната форма:

Теорема 2.8 Нека $C \subset \mathbb{S}^{n-1}$ е антиподален (n, M, s_2)-код със скаларни произведения -1, $\pm s_1$ and $\pm s_2$, където $0 < s_1 < s_2 < 1$. Нека са изпълнени неравенствата

$$s_1^2 s_2^2 + \frac{3 - (n+2)(s_1^2 + s_2^2)}{n(n+2)} > 0,$$

$$6 - (n+4)(s_1^2 + s_2^2) > 0.$$

Тогава

$$M \leq \frac{n(n+2)(1-s_1^2)(1-s_2^2)}{n(n+2)s_1^2 s_2^2 - (n+2)(s_1^2+s_2^2) + 3}.$$

Както в предния случай, можем да построим граница, базирана на ъглите.

Теорема 2.9 Ако $C \subset \mathbb{S}^{n-1}$ е антиподален (n, M, s_2)-код със скаларни произведения -1, $\pm s_1$ and $\pm s_2$, където $0 < s_1 < s_2 < 1$, който е сферичен 5-дизайн, $k \geq 2$ и

$$(1 - ns_1^2)P_{2k}^{(n)}(s_1) + (1 - ns_2^2)P_{2k}^{(n)}(s_2) < 0.$$

Тогава

$$M \leq \frac{2n\left((1-s_1^2)P_{2k}^{(n)}(s_1) + (1-s_2^2)P_{2k}^{(n)}(s_2) + s_2^2 - s_1^2\right)}{\left|(1-ns_1^2)P_{2k}^{(n)}(s_1) + (1-ns_2^2)P_{2k}^{(n)}(s_2)\right|}.$$

Глава 3. Горни граници за енергиите на сферични дизайни със сравнително малка мощност

В трета глава разглеждаме задачата за намиране на горни граници за h-енергията на сферични τ-дизайни с M точки върху $\mathbb{S}^{n-1}$, където M е близко до границата на Делсарт, Гьоталс и Зайдел (4), като се базираме и правим паралели с резултатите за енергиите на сферични дизайни на Бойваленков и съавтори в [19, 20]. Представените резултати са публикувани оригинално в [14].

Основният ни резултат показва, че сферичните дизайни са, в известен смисъл, енергийно ефективни, т.е. всички дизайни със сравнително малка мощност имат h-енергия в много тесен интервал. Не на последно място, резултатите ни за горните граници са изключително близки до получените в [19, 20] и също са валидни за всички абсолютно монотонни потенциали.

В [11] Бойваленков, Бумова и Данев отбелязват, че формулата на Левенщейн за f_0 може да бъде използвана за изследването на сферични дизайни като $L_\tau(n,s)$ се замени с мощността M на предполагаем сферичен τ-дизайн. Това позволява да се разглежда $M = L_\tau(n,s)$, като функция на точките и коефициентите във формулата, ако τ се избере такова, че $M \in (D(n,\tau), D(n,\tau+1))$.

Да означим:

$$u(n,M,\tau) := \sup\{u(C) : C \subset \mathbb{S}^{n-1} \text{ е } \tau\text{-дизайн}, |C| = M\},$$

където $u(C) := \max\{\langle x,y\rangle : x,y \in C, x \neq y\}$, и

$$\ell(n,M,\tau) := \inf\{\ell(C) : C \subset \mathbb{S}^{n-1} \text{ е } \tau\text{-дизайн}, |C| = M\},$$

където $\ell(C) := \min\{\langle x,y\rangle : x,y \in C, x \neq y\}$.

За всеки n, τ и $M \in (D(n,\tau), D(n,\tau+1))$ съществуват нетривиални граници за $u(n,M,\tau)$, получени от Бойваленков, Бумова и Данев [11] и Бумова, Бойваленков, Кулина и Стоянова [9].

Бойваленков и съавтори в [19] предлагат следната обща техника за получаване на горни граници на енергията на сферични кодове при дадени размерност, мощност и сила чрез линейно програмиране.

Теорема 3.2 [19] Нека n, τ, и $M \geq D(n,\tau)$ са естествени числа. Нека $h : [-1,1] \to [0,+\infty]$ и $I \in [-1,1)$ и $g(t) = \sum_{i=0}^{\deg(g)} g_i P_i^{(n)}(t)$ е полином с реални коефициенти, за който:

(D1) $g(t) \geq h(t)$ за $t \in I$;

(D2) Коефициентите на $g(t)$ в развитието по Гегенбауер удовлетворяват условията $g_i \leq 0$ за $i \geq \tau+1$.

Нека $C \subset \mathbb{S}^{n-1}$ е сферичен τ-дизайн, за който $|C| = M$ и $\langle x,y\rangle \in I$ за всеки две различни точки $x,y \in C$. Тогава $E(n,C;h) \leq M(g_0 M - g(1))$. В частност, ако $[\ell(n,M,\tau), u(n,M,\tau)] \subseteq I$, то

$$\mathcal{U}(n,M,\tau;h) \leq M(g_0 M - g(1)). \tag{10}$$

Доказателството на теоремата е сходно с доказателството на класическите граници на линейното програмиране.

В [20] и [19] Бойваленков и съавтори получават долна граница за енергията на сферични кодове и дизайни, която е универсална, в смисъла на Левенщейн [41]. За сферични дизайни границата изглежда по следния начин. Нека въведем следното означение:

$$\mathcal{L}(n,M,\tau;h) := \inf\{E(n,C;h) : |C| = M,\ C \subset \mathbb{S}^{n-1} \text{ е } \tau\text{-дизайн}\}. \tag{11}$$

Тогава имаме теоремата:

Теорема 3.3 [19] Нека $n \geq 3$, τ, и $M \in [D(n,\tau), D(n,\tau+1))$ са естествени числа и $h : [-1,1] \to [0,+\infty]$ е абсолютно монотонна. Тогава:

$$\mathcal{L}(n,M,\tau;h) \geq \begin{cases} M^2 \displaystyle\sum_{i=0}^{k-1} \rho_i h(\alpha_i), & \text{ако } \tau = 2k-1, \\ M^2 \sum_{i=0}^{k} \gamma_i h(\beta_i), & \text{ако } \tau = 2k \end{cases} . \qquad (12)$$

Нека $n \geq 3$, τ, и $M \in (D(n,\tau), D(n,\tau+1))$ са естествени числа, а $h : [-1,1] \to [0,+\infty]$ е абсолютно монотонна. В настоящата дисертация представяме две конструкции на полиноми, които удовлетворяват условията (D1) и (D2) на Теорема и следователно предлагат валидни граници за $\mathcal{U}(n,M,\tau;h)$.

За да подобрим границите, използваме Ермитова интерполация не в пълния интервал $[-1,1]$, а в интервал $[-1,u]$, където u е валидна горна граница за максималното скаларно произведение.

Случай 1. $\tau = 2k-1$ Разглеждаме полинома $g(t)$, резултат от Ермитовата интерполация на h в корените -1 и $t_{k-1,i}^{1,1}$, $i = 1,2,\ldots,k-1$, на полинома $d_{2k-1}^{(n)}(t)$ (полином на Делсарт-Гьоталс-Зайдел 4)

Случай 2. $\tau = 2k$. Ще разгледаме полинома $g(t)$, резултат от Ермитовата интерполация на h в корените $t_{k-1,i}^{1,1}$, $i = 1,2,\ldots,k-1$, на полинома $d_{2k}^{(n)}(t)$

Така получените граници могат да бъдат записани като сума (с тегла) от стойности на потенциала $h(t)$, като за целта ползваме квадратурата на Левенщейн.

Теорема 3.4 Нека $n \geq 3$, τ и $M \in (D(n,\tau), D(n,\tau+1))$ са естествени числа и $h : [-1,1] \to [0,+\infty]$ е абсолютно монотонна. Тогава:

$$\frac{\mathcal{U}(n,M,\tau;h)}{M^2} \leq \begin{cases} g_0\left(1 - \dfrac{D(n,2k-1)}{M}\right) + \dfrac{D(n,2k-1)}{M} \displaystyle\sum_{i=0}^{k-1} \gamma_i h(t_{k-1,i}^{1,1}), & \tau = 2k-1 \\ g_0\left(1 - \dfrac{D(n,2k)}{M}\right) + \dfrac{D(n,2k)}{M} \displaystyle\sum_{i=0}^{k-1} \rho_i h(t_{k,i+1}^{1,0}), & \tau = 2k \end{cases} \qquad (13)$$

(полагаме $t_{k-1,0}^{1,1} := -1$ за нечетно τ).

Първият от двата начина за представяне на границата използва стойностите на потенциала в границите на интервалите на Левенщейн. Вторият я представя посредством универсалната долна граница и параметрите $\rho_i, \alpha_i, \gamma_i$ и β_i.

Теорема 3.5 Нека $n \geq 3$, τ, и $M \in (D(n,\tau), D(n,\tau+1))$ са естествени числа, а h :

$[-1,1] \to [0,+\infty]$ е абсолютно монотонна. Тогава е в сила:

$$\frac{\mathcal{U}(n,M,\tau;h)}{M^2} \leq \begin{cases} \dfrac{ULB}{M^2} + \displaystyle\sum_{i=0}^{k-1} \rho_i(g(\alpha_i) - h(\alpha_i)), & \text{ако } \tau = 2k-1 \\ \dfrac{ULB}{M^2} + \displaystyle\sum_{i=0}^{k} \gamma_i(g(\beta_i) - h(\beta_i)), & \text{ако } \tau = 2k, \end{cases} \tag{14}$$

където ULB е съответната универсална долна граница (12) и ρ_i, α_i, γ_i, and β_i са същите като в (12).

Извеждаме и асимптотичен резултат за поведението на границата.

Теорема 3.8 Нека n и M клонят към безкрайност със следната връзка $M = \lambda n + o(1)$, където $\lambda \in (1,2)$ е константа. Тогава:

$$h(0) + \frac{h(1-\lambda) - \lambda h(0)}{M(\lambda-1)} \leq \frac{\mathcal{L}(n,M,2;h)}{M^2} \leq \frac{\mathcal{U}(n,M,2;h)}{M^2}$$
$$\leq h(0) + \frac{h(\lambda-1) + (\lambda-2)h(0) - (\lambda^2 - 3\lambda + 3)h'(0)}{M(\lambda-1)} + o(M^{-2}).$$

Доказателството се получава с директни изчисления.

Глава 4. Върху q-ични кодове с две съседни разстояния

Четвърта и пета глава представят резултатите от работата с Д.В. Зиновиев и В.А. Зиновиев [15, 17], върху q-ични кодове в Хемингово пространство с две разстояния, като особен фокус се поставя върху кодовете с две близки или съседни разстояния и в линейния и в общия случай. Разглеждат се фамилии такива кодове, базирани на връзки с класически обекти като еквидистантни кодове и се дават граници за тяхната мощност.

Мотивацията за разглеждане на кодове с две съседни разстояния произлиза от две причини. Първо, интересен е въпросът до колко би била по-богата структурата на тези кодове спрямо добрите еквидистантни кодове в същите пространства. Също така, поради близките си разстояния, те ще бъдат кодове с почти константна енергия при амплитудно фазова модулация, което може да бъде потенциално практическо приложение.

В предните глави използвахме значимо полиномите на Гегенбауер и техните свойства, които позволяват извеждането на граници за кодове и дизайни, базирани на връзката им с хармоничните полиноми и основното равенство на границите на линейното програмиране. Те, обаче, са конкретно свързани с n-мерната сфера. За q-ичните кодове аналогична функция имат полиномите на Кравчук, които имат практически аналогични свойства.

За фиксирани n и q, нормализираните полиноми на Кравчук се дефинират като

$$Q_i^{(n,q)}(t) = \frac{1}{r_i} K_i^{(n,q)}(d),\ d = \frac{n(1-t)}{2},\ r_i = (q-1)^i \binom{n}{i},$$

където

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

са стандартните полиноми на Кравчук [34, 45]; вж. също [40]. В дисертацията работим с $Q_i^{(n,q)}(t)$.

Разгледани са два типа граници - граници, идващи от метода на линейното програмиране и граници, идващи от едно биективно съответствие между кодове в $\mathbb{Q}^n$ и $\mathbb{S}^{n(q-1)-1}$. В четвърта глава разглеждаме първо случая, когато разстоянията са съседни , а в следващата глава - по-общия случай, на разстояния d и $d+\delta$.

Нека

$$A_q(n; \{d, d+1\}) = \max\{|C| : C \text{ е } (n, |C|, \{d, d+1\})\text{-код}\},$$

максималната мощност на код в Q^n с две разстояния d и $d+1$.

Класическите резултати за кодове с две разстояния са хармоничната граница на Делсарт [26] и нейното подобрение от Барг и Мусин [7]. И двете, обаче, не отразяват добре спецификата на съседните разстояния и са сравнително неточни в разглеждания случай.

Класическата граница на линейното програмиране за q-ични кодове [26, 40], в частния случай за две съседни разстояния има следния вид.

Теорема 4.6 Нека $n \geq q \geq 2$ и $f(t)$ е полином с реални коефициенти от степен наймного $m \leq n$ за който са изпълнени следните условия:

(A1) $f(t) \leq 0$ за всяко $t \in \{1 - 2d/n, 1 - 2(d+1)/n\}$;

(A2) Коефициентите на Кравчук в развитието $f(t) = \sum_{i=0}^{m} f_i Q_i^{(n,q)}(t)$ са неотрицателни за всяко i.

Тогава $A_q(n; \{d, d+1\}) \leq f(1)/f_0$. Ако границата се достига от $(n, N, \{d, d+1\})_q$-код C и полином $f(t)$, то тогава $f(1 - 2(d+i)/n) = 0$, $i = 0, 1$, и $f_i M_i(C) = 0$.

Тук отново

$$M_i(C) = \sum_{x,y \in C} Q_i^{(n,q)}(1 - 2d(x,y)/n)$$

е i-ия момент на C, но дефиниран за q-ични кодове по аналогичен начин.

Ако използваме $f(t) = t - 1 + 2d/n$, в Теорема получаваме

$$\frac{f(1)}{f_0} = \frac{2d}{2d-n},$$

като тази граница е валидна при $f_0 > 0$. Това представлява класическата граница на Плоткин. Ако използваме полиноми от втора степен, получаваме следната теорема:

Теорема 4.8 Нека $d \geq (n-1)(q-1)/q$, тогава е изпълнено

$$A_q(n; \{d, d+1\}) \leq \frac{q^2 d(d+1)}{n^2(q-1)^2 - n(q-1)(2dq + q - 1) + dq^2(d+1)}. \tag{15}$$

Ако границата (22) се достига от $(n, N, \{d, d+1\})_q$-код C, то $M_2(C) = 0$ и $M_1(C)(dq-(n-1(q-1))) = 0$.

Границата е точна за някои стойности на параметрите. Например

$$A_q(n; \{d, d+1\}) \leq q^2$$

за $d = n-1$ се достига при $(q, n) = (3,3), (3,4), (4,5)$, и $(5,6)$. Всички подобни случаи са маркирани с $d2$ в приложените таблици. Аргументи за моментите позволяват допълнителни подобрения. Тези случаи са отбелязани с n в таблиците към дисертацията.

Други полиноми също дават добри граници, като например $f(t) = 1+(q-1)nQ^{(n,q)}_{(n(q-1)+1)/q}(t)$ и $f(t) = 1 + \frac{n+2}{2}Q^{(n,2)}_{n/2}(t) + \frac{n}{2}Q^{(n,2)}_{1+n/2}(t)$. Този тип случаи ще бележим с a в таблиците със събраните резултати за долни и горни граници.

За конструирането на добри кодове с две съседни разстояния основна роля играят еквидистантните кодове. Те са един от класическите обекти на теория на кодирането, върху който са натрупани голям брой резултати, като например границата на Джонсън и много конструкции на кодове с добри параметри.

Следвайки [17] можем да опишем следните видове конструкции:

- Сфера с радиус 1 с или без проверка за четност
- Еквидистантен код с премахнат или добавен стълб
- Слепвания на еквидистантен код с код с две разстояния
- Кодове, базирани на латински квадрати
- Кодове, базирани на разностни матрици

Интересен начин за получаване на граници за q-ични кодове е посредством изображение на q-ичен код върху $\mathbb{S}^{(q-1)n-1}$. Тази биекция е добре известна и чрез нея и резултатите на Ларман, Роджърс и Зайдел [36] можем да изведем следната горна граница за $A_q(n, \{d, d+1\})$.

Теорема 4.13 Ако $d > (\sqrt{2(q-1)n} - 1)/2$, то

$$A_q(n, \{d, d+1\}) \leq 2(q-1)n + 1.$$

Границата от нея обикновено е по-добра от симплекс метода за достатъчно големи n и d в средата на интервала. Най-малкият пример за това са случаите $(q, n, d) = (2, 13, 4)$, $(q, n, d) = (3, 9, 3)$, $(q, n, d) = (4, 8, 3)$ и $(q, n, d) = (5, 7, 4)$.

В дисертацията са обобщени резултатите за долните граници за $q = 2, 3, 4, 5$, като долните граници предлагат по-добрият резултат измежду компютърно-генерирани кодове и конструкциите, описани в тази глава.

Горните граници са най-доброто измежду линейните граници получени чрез симплекс метод, чрез ad-hoc полиноми (където са отбелязани с $d2$, n и a, съответно), чрез най-добрата известна граница за $A_q(n,d)$, взета от [23] (отбелязани с $*$), и чрез сферични кодове (Теорема - отбелязни с sc).

Компютърно-генерираните кодове са получени посредством случайна разходка с връщане назад, като за $q = 2$ това позволи получаване на резултати до $n = 26$, а за $q = 3$ - до $n = 14$ и $q = 4$ - до $n = 12$.

Глава 5. Горни граници на линейното програмиране за кодове с две несъседни разстояния

Глава 5 представлява своеобразно разширение на предната, като вместо съседни, се разглеждат разстояния d и $d + \delta$ за малки стойности на δ. Получените кодове наричаме $(n, N, \{d, d + \delta\})_q$-кодове. Изложените резултати са публикувани за първи път в [16, 18].

Границата на линейното програмиране има следния вид:

Теорема 5.1 Нека $n \geq q \geq 2$ и $f(t)$ е полином с реални коефициенти, който изпълнява следните условия:

(A1) $f(t) \leq 0$ for $t \in \{1 - 2d/n, 1 - 2(d + \delta)/n\}$;

(A2) Коефициентите на Кравчук f_i са неотрицателни за всяко $i \geq 1$.

Тогава

$$A_q(n; \{d, d + \delta\}) \leq \frac{f(1)}{f_0}. \tag{16}$$

Ако един $(n, N, \{d, d+\delta\})_q$ код C достига границата за даден полином $f(t)$, то $f(1-2(d+i)/n) = 0$, $i = 0, \delta$, ако има елементи на C на разстояние $d + i$, $i = 0, \delta$, и $f_i M_i(C) = 0$, където M_i е i-я момент на C.

Доказателството е аналогично на предните теореми от този тип.

Отново, при $f(t) = t-1+2d/n$ получаваме границата на Плоткин, която се достига за множество случаи при голямо d. Използвайки полином от втора степен можем да получим следната връзка между параметрите на q-ичен двутегловен код.

Теорема 5.2 Нека C е q-ичен двутеглови $(n, N, \{w_1, w_2\})_q$-код, който е и ортогонален масив със сила $t \geq 2$, т.е. M е кратно на q^2. Тогава ако $u_i = n - w_i,\ i = 1, 2$ е в сила:

- Дължината n удовлетворява следното уравнение от втора степен:

$$n^2 - n\left(Q_1(u_1 + u_2 - 1) + 1\right) + Q_2 u_1 u_2 = 0, \tag{17}$$

$$Q_1 = q\,\frac{N - q}{N - q^2},\ \ Q_2 = q^2\,\frac{N - 1}{N - q^2}. \tag{18}$$

- Ако $w_2 = n$ (т.е. ако $u_2 = 0$), то дължината n на C удовлетворява

$$n = \frac{Q_1(d + 1) - 1}{Q_1 - 1}, \tag{19}$$

където $d = w_1$ е минималното разстояние на C.

Тази теорема има и комбинаторно доказателство, предложено от Д. Зиновиев и В. Зиновиев.

С помощта на полином от втора степен можем да получим и граница, която съвпада с границата на Хелесет-Кльове-Левенщейн за кодове с известно максимално и минимално разстояние [31], а също така и с границата за $k = 1$ в Теорема 5.2 в [22].

Теорема 5.3 Ако

$$q(2d+\delta) \geq 2nq + 2 - 2n - q, \tag{20}$$

$$n(q-1)(nq-n+1) + nq(2d+\delta) > q^2(2nd + n\delta - d^2 - d\delta), \tag{21}$$

то

$$A_q(n, \{d, d+\delta\}) \leq \frac{d(d+\delta)q^2}{n(q-1)(nq-n+1) - q^2(2nd+n\delta-d^2-d\delta) + nq(2d+\delta)}. \tag{22}$$

Ако даден код C с параметри $(n, N, \{d, d+\delta\})_q$ достига границата, то кодът е и ортогонален масив със сила 2.

Както във втора глава, ако дясната част на (22) е цяло число, можем да намерим спектъра на C, което дава няколко нови резултата за несъществуване, като например: $A_2(12, \{6, 10\}) \leq 19$ вместо 20, $A_2(20, \{10, 14\}) \leq 27$ вмсто 28, и $A_2(16, \{8, 14\}) \leq 27$ вместо 28. Тези случаи ще бележим с (22).

Аналогично на случая $\delta = 1$, можем да изкажем следната теорема, взимайки предвид връзката със сферични кодове:

Теорема 5.4 Нека отношението между двете разстояния се представя като несъкратима дроб по следния начин $\frac{d}{d+\delta} = \frac{r}{s}$. Тогава ако е изпълнено $s - r \geq 2$ (в частност, когато $\mathrm{GCD}(d, d+\delta) = 1$), то

$$A_q(n, \{d, d+\delta\}) \leq 2(q-1)n + 1.$$

За няколко безкрайни серии кодове можем да докажем резултати за несъществуване или да намерим тяхната мощност по сравнително директен начин, чрез комбинаторни аргументи и неравенство на триъгълника.

Лема 5.1 Не съществуват кодове $C \subset E_2^n$ с разстояния d and $d+\delta$ когато:

(a) d и $d+\delta$ са едновременно нечетни;

(b) d е нечетно, $d+\delta$ е четно и $n < (3d-\delta)/2$;

(c) d е нечетно, $d+\delta$ е четно и $d < \delta$;

(d) $d+\delta = n$ и $n \neq 2d$;

(e) $d+\delta = n-1$ и $2d > n+1$.

Лема 5.2 За $q = 2$, ако d е нечетно и $|C| > 4$, то

$$A_2(n, \{d, 2d\}) = 1 + \left[\frac{n}{d}\right].$$

Лема 5.3 $A_3(n, \{1,3\}) = 6$ за всяко $n \geq 4$.

Както в случая с две съседни разстояния, получени и обобщени в таблици са резултати за $q = 2,3,4,5$, като долните граници предлагат по-добрият резултат измежду компютърно-генерираните кодове и описаните конструкции.

Компютърно-генерираните кодове са получени с модификация на описания в предната глава софтуер.

Горните граници са най-доброто измежду линейните граници получени чрез общият симплекс метод (отбелязано чрез lp), чрез съображения за спектъра (отбелязано с dd), чрез ad-hoc полиноми (където са отбелязани с $d2$), чрез най-добрата известна граница за $A_q(n,d)$, взета от [23] (отбелязани с $*$), и чрез теоремата за сферични кодове (отбелязни с sc).

Благодарности

Изразявам най-дълбоката си благодарност към моят научен ръководител, проф. Петър Бойваленков за възможността, която ми предостави да стана част от уважаваната българска школа по теория на кодирането и за огромното му внимание и търпение.

Благодаря на доц. Тодорка Александрова, за нейните ведри и винаги точни съвети. На доц. Христо Костадинов, проф. Емил Колев и всички останали колеги от секция МОИ благодаря за работната атмосфера и оказаната подкрепа, както при работата върху настоящия труд, така и при цялата ми останала дейност в рамките на ИМИ-БАН.

Константин Делчев

Библиография

[1] Бойваленков П., Граници на линейното програмиране за сферични кодове и дизайни, ИМИ-БАН, София 2003г.

[2] Bannai Ei., Bannai Et., A survey on spherical designs and algebraic combinatorics on spheres, *European Journal of Combinatorics* 30, 2009, P. 1392-1425.

[3] Bannai Ei., Bannai Et., Tanaka H., Zhu Y., Design theory from the viewpoint of Algebraic Combinatorics, *Graphs and combinatorics* 33, 2017, P. 1-41.

[4] Bannai Ei., Damerell R. N., Tight spherical designs I, *J. Math. Soc. Japan* 31, 1979, P. 199-207.

[5] Bannai Ei., Damerell R. N., Tight spherical designs II, *J. London Math. Soc.* 21, 1980, P. 13-30.

[6] Bannai Ei., Sloane N. J. A., Uniqueness of certain spherical codes, *Canad. J. Math.* 33, 1981, P. 437-449.

[7] Barg A., Musin O., Bounds on sets with few distances, *Journ. Combin. Theory* Ser. A. 118, 2011, P. 1465-1474.

[8] Barg A., Yu W-H., New bounds on equiangular lines, in Discrete Geometry and Algebraic Combinatorics, A. Barg and O. Musin, eds., *Contemporary Mathematics* vol. 625, Amer. Math. Soc., Providence, RI, 2014, P. 111-121.

[9] Boumova S., Boyvalenkov P., Kulina H., Stoyanova M., Polynomial techniques for investigation of spherical designs, *Des., Codes Crypt.* 51, 2009, P. 275-288.

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

[11] Boyvalenkov P., Boumova S., Danev D., Necessary conditions for existence of some designs in polynomial metric spaces, *Europ. J. Combin.* 20, 1999, P. 213-225.

[12] Boyvalenkov P., Danev D., Kazakov P., Indexes of spherical codes, *DIMACS Ser. Disc. Math. & Theor. Comp. Sci.* 56, 2001, P. 47-57.

[13] Boyvalenkov, P., Delchev, K., On maximal antipodal spherical codes with few distances. *Electronic Notes in Discrete Mathematics* 57, Elsevier, 2017, P. 85-90.

[14] Boyvalenkov, P., Delchev, K., Jourdain, M., Upper energy bounds for spherical designs of relatively small cardinalities. *Discrete and Computational Geometry* 65, 1, Springer, 2021, P. 244–260.

[15] Boyvalenkov P., Delchev K., Zinoviev D. V., Zinoviev V. A., Codes with two distances: d and $d+1$, *Proc. 16th International Workshop on Algebraic and Combinatorial Coding Theory*, Svetlogorsk (Kaliningrad region, Russia, 2-8 September 2018).

[16] Boyvalenkov P., Delchev K., Zinoviev D. V., Zinoviev V. A., , On two-weight (linear and nonlinear) codes, *Proc. 17th International Workshop on Algebraic and Combinatorial Coding Theory*, Bulgaria, 11-17 October 2020.

[17] Boyvalenkov, P., Delchev, K., Zinoviev, D., Zinoviev, V.. On q-ary codes with two distances d and $d+1$, *Problems of Information Transmission* 56, 1, Springer, 2020, P. 33-44.

[18] Boyvalenkov, P., Delchev, K., Zinoviev, D., Zinoviev, V.. On two-weight codes. *Discrete Mathematics*, 344, 5, paper no. 112318, Elsevier, 2021.

[19] Boyvalenkov P., Dragnev P., Hardin D., Saff E., Stoyanova M., Universal upper and lower bounds for potential energy of spherical designs, *Dolom. Res. Notes Approx.* 8, 2015, P. 51-65.

[20] Boyvalenkov P., Dragnev P., Hardin D., Saff E., Stoyanova M., Universal lower bounds for potential energy of spherical codes, *Constr. Approx.* 44, 2016, P. 385-415.

[21] Boyvalenkov P., Dragnev P., Hardin D., Saff E., Stoyanova M., Energy bounds for codes in polynomial metric spaces, Analysis and Mathematical Physics 9, 2019, P. 781-808.

[22] Boyvalenkov P., Dragnev P., Hardin D., Saff E., Stoyanova M., Universal bounds for size and energy of codes of given minimum and maximum distances, to appear in IEEE Trans. Inform. Theory, 2021, arxiv:910.07274.

[23] Brouwer A. E., Tables of bounds for q-ary codes, http:www.win.tue.nl/˜aeb/ .

[24] Cohn H., Kumar A. Universally optimal distribution of points on spheres, *Journal of the American Mathematical Society* 20 (2007), P. 99-148.

[25] Conway J. H., Sloane N. J. A., *Sphere Packings, Lattices and Groups*, Springer-Verlag, New York, 1988.

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

[27] Delsarte P, Goethals J.-M., Seidel J.J., Spherical codes and designs, *Geom. Dedicata* 6, 1977, P. 363-388.

[28] Fuchs C. A., Sasaki M., Squeezing quantum information through a classical channel: measuring the 'quantumness' of a set of quantum states, *Quant. Info. Comp.* 3, 2003, P. 377-404.

[29] Ganzhinov M., Szöllősi F., Biangular lines revisited, arxiv.org/abs/1910.05950 (Submitted on 14 Oct 2019).

[30] Haantjes J., Equilateral point-sets in elliptic two- and three-dimensional spaces, *Nieuw Arch. Wisk.* 22, 1948, P. 355–362.

[31] Helleseth T., Kløve T., Levenshtein V. I., A bound for codes with given minimum and maximum distances, *Proc. IEEE Intern. Symp. on Inform. Theory*, 2006, P. 292-296.

[32] Holzmann W. H., Kharaghani H., Suda S., Mutually unbiased biangular vectors and association schemes. In: C. J. Colbourn (ed.) *Algebraic Design Theory and Hadamard Matrices*, 2015, P. 149-157.

[33] Kabatianskii G. A., Levenshtein V. I., Bounds for packings on a sphere and in space, *Probl. Inform. Transm.* 14, 1978, P. 1-17.

[34] Krawtchouk M., Sur une généralisation des polynômes d'Hermite, *Comptes Rendus* 189 (1929) 620-622.

[35] Landjev I., Rousseva A., Storme L., On linear codes of almost constant weight and the related arcs, manuscript, 2019.

[36] Larman D. G., Rogers C. A., Seidel J. J., On two distance sets in Euclidean space, *Bull. London Math. Soc.* 1977, 9, P. 261-267.

[37] Levenshtein V. I., On bounds for packings in n-dimensional Euclidean space, *Soviet Math. Dokl.* 20, 1979, P. 417-421.

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

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

[40] Levenshtein V. I., Krawtchouk polynomials and universal bounds for codes and designs in Hamming spaces, *IEEE Trans. Infor. Theory.* 41., 1995, P. 1303-1321.

[41] Levenshtein V. I. Universal bounds for codes and designs, Handbook of Coding Theory, Elsevier Science B.V. 1998, chapter 6.

[42] van Lint J. H., Seidel J. J., Equilateral point sets in elliptic geometry, *Indag. Math.* 28, 1966, P. 335-348.

[43] Rankin R. A., The closest packing of spherical caps in n dimensions, *Proc. Glasgow Math. Assoc.* 2, 1955, P. 139-144.

[44] Rogers C. A., *Packing and Covering*, Cambridge University Press, 1964.

[45] Szegő G., *Orthogonal polynomials*, AMS Col. Publ. 23, 1939.

[46] Vilenkin N. Y., *Special functions and theory of group representations*, Providence, RI, 1968.

[47] Yudin V. A., The minimum for the potential energy of a system of point charges, *Diskret. Mat. [Discrete Math. Appl.]* 4, 1992, P 115–121; English translation: *Discr. Math. Appl.* 3, 1993, P. 75-81.

[48] Zong C., *Sphere packings*, Springer-Verlag, New York, 1999.

Научни приноси

В настоящия дисертационен труд са получени следните нови резултати:

- Нови граници за мощността на антиподални сферични кодове с малък брой разстояния, мотивирани от изучаването на равноъгълни прави.
- Резултати от тип на Лойд за рационалност на скаларните произведения на максимални антиподални сферични кодове с малък брой разстояния.
- Горни граници за енергиите на сферични дизайни с мощност близка до границата на Делсарт-Гьоталс-Зайдел
- Асимптотични ограничения за енергиите на сферични 2-дизайни.
- Алгоритъм за конструкции на кодове с две съседни или близки разстояния, посредством случайни разходки с връщане назад.
- Конструкции за q-ични кодове с две съседни разстояния, базирани на алгебрични и комбинаторни обекти
- Конструкции за q-ични кодове с две близки разстояния, базирани на алгебрични и комбинаторни обекти
- Граници за мощността и резултати за несъществуване на q-ични кодове с две съседни разстояния, базирани на линейно програмиране, връзка със сферични кодове и др.
- Граници за мощността и резултати за несъществуване на q-ични кодове с две съседни разстояния, базирани на линейно програмиране, геометрични съображения и др.

Публикации на автора по темата на дисертацията

1. Boyvalenkov, P., Delchev, K.. On maximal antipodal spherical codes with few distances. *Electronic Notes in Discrete Mathematics* 57, Elsevier, 2017, P.85-90. SJR (Scopus): 0.262

2. Boyvalenkov, P., Delchev, K., Zinoviev, D., Zinoviev, V.. Codes with two distances: d and $d+1$. *Proceedings of 16th International workshop on Algebraic and Combinatorial Coding Theory*, Kaliningrad, Russia, Sep 2-8, 2018, P. 40-45, 2018.

3. Boyvalenkov, P., Delchev, K., Zinoviev, D., Zinoviev, V.. On q-ary codes with two distances d and $d+1$. *Problems of Information Transmission* 56, 1, Springer, 2020, 33-44. SJR (Scopus): 0.506, JCR-IF (Web of Science): 0.593

4. Boyvalenkov, P., Delchev, K., Zinoviev, D., Zinoviev, V.. On two-weight codes. *Discrete Mathematics*, 344, 5, paper no. 112318, Elsevier, 2021, SJR (Scopus): 0.824, JCR-IF (Web of Science): 0.77

5. Boyvalenkov, P., Delchev, K., Jourdain, M.. Upper energy bounds for spherical designs of relatively small cardinalities. *Discrete and Computational Geometry* 65, 1, Springer, 2021, P. 244–260, SJR (Scopus): 0.611, JCR-IF (Web of Science): 0.621

6. Boyvalenkov, P., Delchev, K., Zinoviev, D., Zinoviev, V.. On two-weight (linear and non-linear) codes, *Proceedings of 17th International workshop on Algebraic and Combinatorial Coding Theory*, Bulgaria (on-line), Oct 11-17, 2020, 40-45

Цитирания на публикациите по темата на дисертацията

1. Boyvalenkov, P., Delchev, K.. On maximal antipodal spherical codes with few distances. *Electronic Notes in Discrete Mathematics* 57, Elsevier, 2017.

е цитирана в:

1 Womersly, R., "Efficient Spherical Designs with Good Geometric Properties In: Dick J., Kuo F., Woźniakowski H. (eds) *Contemporary Computational Mathematics - A Celebration of the 80th Birthday of Ian Sloan*, Springer, Cham, 2018, P. 1243-1285.

2 Ganzhinov, M., Szöllősi, F., Biangular lines revisited, 2019 https://arxiv.org/abs/1910.05950, accessed: 02.02.2021.

2. Boyvalenkov, P., Delchev, K., Zinoviev, D., Zinoviev, V.. Codes with two distances: d and d+1. *Proceedings of 16th International workshop on Algebraic and Combinatorial Coding Theory, Kaliningrad, Russia, Sep 2-8, 2018*, 40-45, 2018.

е цитирана в:

3 Landjev, I., Rousseva, A., Storme, L., On linear codes of almost constant weight and the related arcs, *Comp. Rend. Acad. Bulg. Sci.* 72(12), 2019, P. 1626-1633.

3. Boyvalenkov, P., Delchev, K., Zinoviev, D., Zinoviev, V.. On q-ary codes with two distances d and d+1. *Problems of Information Transmission* 56, 1, Springer, 2020, 33-44.

е цитирана в:

4 Landjev, I., Rousseva, A., Storme, L., On linear codes of almost constant weight and the related arcs, *Comp. Rend. Acad. Bulg. Sci.* 72(12), 2019, P. 1626-1633.