Results on codes with few distances

Alexander Barg University of Maryland, College Park
Oleg Musin University of Texas, Brownsville

D. Ray-Chaudhuri and R. Wilson (1975):

Let $\mathcal{F}=\{F_1,F_2,\dots, F_m\}$ be a family of w-subsets of [n] such that $|F_i \cap F_j| \in \{p_1,p_2,\dots,p_s\}$, $i \neq j$

Then $m \leq \binom{n}{s}$

Consider $\mathcal{F}$={all w-subsets of [n] }, then s=w, so this estimate is tight

P. Delsarte, J.-M.Goethals, J. Seidel (1977):

Let $C \subset S^{n-1}$ be a set of points $(x_1,x_2,\dots,x_m)$ such that $(x_i,x_j) \in \{t_1,t_2,\dots,t_s\}$, $i \neq j$

Then $m \leq \binom{n+s-1}{s} + \binom{n+s-2}{s-1}$

s=1 : the bound $m \leq n$ is attained by the C={n vertices of a regular simplex}

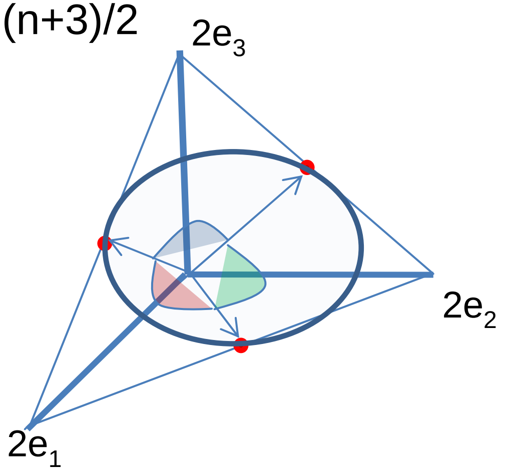
In this talk we will provide a general improvement of these theorems, together with some other results

Some improvements are known:

e.g., take $X=S^{n-1}$, s=2, then the bound gives $|C|\leq n(n+3)/2$

Take $e_1,\ldots,e_{n+1}$ to be the standard basis;

$C=\{e_i+e_j,\ 1\leq i < j \leq n+1\}$



Scalar products 1 or 0, so C is a sperical 2-distance set

$|C|=n(n+1)/2$

Larger codes with distances t_1,t_2 such that $t_1+t_2>0$ do not exist since in this case the DGS bound can be improved to

$m \leq n(n+1)/2$ (Musin, 2008)

Harmonic analysis on homogeneous spaces

X compact metric space, d(.,.) - distance

Harmonic analysis on X:
Let G be the isometry group of X which acts transitively on it
H -- subgroup that fixes a point x_0
$X \cong G/H$

$$L_2(G,d\text{æ})=\oplus_{i=0} V_i$$

$$V_i=(\varphi_{i,1},\ldots,\varphi_{i,h_i})$$

There is a unique H-invariant function Φ_i
$\Phi_i(x,y)=\sum_{j=1}^{h_i}\varphi_{i,j}(x)\,\varphi_{i,j}(y)$

$$\Phi_0=1$$

G acts *distance-transitively*:
$p_i(d(x,y))=\Phi_i(x,y)$ $\quad p_0(x)=1$

$$xp_i(x)=a_ip_{i+1}(x)+b_ip_i(x)+c_ip_{i-1}(x)$$

$X=\{0,1\}^n$, $d_H(x,y)=\#\{i: x_i\neq y_i\}$

$G=S_n \ltimes Z_2^n$

$H=S_n$

$\varphi_{i,j}(x)=(-1)^{x_{i_1}+\ldots+x_{i_l}}$

$h_i=\binom{n}{i}$

$K_i(d(x,y))=\sum_{j=1}^{h_i}\varphi_{i,j}(x)\,\varphi_{i,j}(y)$

$K_0(x)=1$, $K_1(x)=n-2x$
$K_2(x)=2x^2-2nx+½n(n-1)$, …

$xK_i=-((i+1)/2)K_{i+1}+(n/2)K_i-((n-i+1)/2)K_{i+1}$

Theorem (Delsarte; DGS, 73-77): Let $C\subset X$ be a code with s distances (s-code). Then

$$|C|\leq h_0+h_1+\ldots+h_s$$

Later proofs of particular cases and generalizations obtained by
Frankl-Wilson ('85), Alon-Babai-Suzuki ('91), Babai-Snevily-Wilson ('95) and others.

Parameters of metric space of coding theory

X	H_n	$J^{n,w}$	S^{n-1}
$d\mu$	$2^{-n}\binom{n}{i}$	$\frac{\binom{w}{i}\binom{n-w}{i}}{\binom{n}{w}}$	$\frac{n-2}{\omega_n}(1-x^2)^{(n-3)/2}dx$
h_i	$\binom{n}{i}$	$\binom{n}{i}-\binom{n}{i-1}$	$\binom{n+i-2}{i}+\binom{n+i-3}{i-1}$
a_i	$-\frac{i+1}{2}$	$-\frac{(i+1)(w-i)(n-w-i)}{(n-2i-1)(n-2i)}$	$\frac{n-2+i}{n-2+2i}$
b_i	$\frac{n}{2}$	$\frac{(n+2)w(n-w)-ni(n-i+1)}{(n-2i)(n-2i+2)}$	0
c_i	$-\frac{n-i+1}{2}$	$-\frac{(w-i+1)(n-w-i+1)(n-i+2)}{(n-2i+2)(n-2i+3)}$	$\frac{i}{n-2+2i}$

Hahn polynomials:

$$Q_i(x) = \left(\binom{n}{i} - \binom{n}{i-1}\right) \sum_{j=0}^{i} (-1)^j \frac{\binom{i}{j}\binom{n+1-i}{j}}{\binom{w}{j}\binom{n-w}{j}} \binom{x}{j}.$$

Nozaki's theorem (2008)

Theorem 1 *Let $C \subset X$ be an s-code with distances $d_1, \dots, d_s$. Consider the polynomial $f(x) = \prod_{i=1}^{s}(d_i - x)$ and suppose that its expansion in the basis $\{p_i\}$ has the form $f(x) = \sum_i f_i p_i(x)$. Then*

$$|C| \le \sum_{i: f_i > 0} h_i.$$

Proof: Consider the matrix H_l given by $(H_l)_{i,j} = \phi_{l,j}(\mathbf{x}_i)$. Let $\mathscr{H} = (H_1, \dots, H_s)$ and

$$F = \operatorname{diag}(f_0, f_1, \dots, f_1, \dots, \underbrace{f_i, \dots, f_i}_{h_i}, \dots, f_s).$$

$$\begin{aligned} A_{p,r} := \mathscr{H} F \mathscr{H}^t &= \sum_{i=0}^{s} f_i \sum_{j=1}^{h_i} \phi_{i,j}(\mathbf{x}_p)\phi_{i,j}(\mathbf{x}_r) = \sum_i f_i p_i(d(\mathbf{x}_p, \mathbf{x}_r)) \\ &= f(d(\mathbf{x}_p, \mathbf{x}_r)) = \delta_{p.r} f(0), \qquad 1 \le p, r \le |C|, \end{aligned}$$

so $A = f(0) I_{|C|}$.

We have found $|C|$ vectors $\mathbf{z}_i = ((H_l)_{i,j}, j = 1, \dots, \sum_{p=0}^{s} h_p)$ that lie in the positive subspace of the quadratic form F and satisfy $(F\mathbf{z}_u, \mathbf{z}_v) = 0$ for $u \ne v$.

It follows that the $\mathbf{z}_i$ are linearly independent

$\Rightarrow$ their number $\le$ the number of positive eigenvalues of F

Polynomials $\{p_i, i=0,1,\ldots\}$

$L(g)=\int g\,d\mu$ – linear functional that controls orthogonality

$r_i\, L(p_i\, p_j)=\delta_{ij}$ $\qquad r_i=1/h_i$

$L(x^k\, p_m)=0$ for any $k<m$

$p_0(x)=1$

$$xp_i(x)=a_i p_{i+1}(x)+b_i p_i(x)+c_i p_{i-1}(x)$$

Lemma: Consider the polynomial $f(x)=\prod_{i=1}^{s}(d_i-x)=\sum_{i=0}^{s} f_i p_i(x)$.
Then

$$f_s=(-1)^s r_s\, c_1 c_2\ldots c_s$$

$$f_{s-1}=(-1)^s\, r_{s-1}\sum_{j=1}^{s}(b_{j-1}-d_j)\prod_{i=1}^{s-1}c_i \qquad (s\geq 2)$$

For instance,

$$(-1)^s\, f_s=r_s L(x^s\, p_s)=r_s L[x^{s-1}(a_s p_{s+1}+b_s p_s+c_s p_{s-1})]=r_s\, c_s L[x^{s-1} p_{s-1}]$$

Theorem: Let C be a code with distances $d_1, \ldots, d_s$. Let

$$D = b_0 + \cdots + b_{s-1} - d_1 - \cdots - d_s.$$

(a) Suppose that $c_i < 0, i = 1, 2, \ldots$ and $D > 0$. Then

$$|C| \leq h_0 + h_1 + \cdots + h_{s-2} + h_s.$$

(b) Suppose that $c_i > 0, i = 1, 2, \ldots$. Then

$$|C| \leq \begin{cases} h_0 + h_1 + \cdots + h_{s-2} & s \equiv 1 \pmod 2 \text{ and } D > 0 \\ h_0 + h_1 + \cdots + h_{s-1} & s \equiv 1 \pmod 2 \text{ and } D < 0 \\ h_0 + h_1 + \cdots + h_{s-2} + h_s & s \equiv 0 \pmod 2 \text{ and } D < 0. \end{cases}$$

Applications: Intersecting families

Family $\mathcal{F} = \{F_1, F_2, \dots\}$ of subsets of an n-element set is called

w-*uniform* if $\forall_i |F_i| = w$

s-*intersecting* if $\forall_{F_i,F_j} |F_i \cap F_j| \in \{w, t_1, \dots, t_s\}$ for some $t_1, \dots, t_s, 0 < t_i < w$.

Theorem 1 (Ray-Chaudhuri–Wilson, 1975)

Let $\mathcal{F}$ be a w-uniform s-intersecting family. Then $|\mathcal{F}| \le \binom{n}{s}$.

The indicator vectors of a w-uniform s-intersecting family $\mathcal{F}$ form an s-code C in $J^{n,w}$.

Johnson space $J^{n,w}=\{x\in\{0,1\}^n\text{: wt}(x)=w\}$

$\{p_i(x), i=0,1,\dots,w\}$ – discrete dual Hahn polynomials

For instance, let n=13, w=5, $t_1=3$, $t_2=4$, then we obtain $|\mathcal{F}| \le 78$

Delsarte LP bound: $|C| \le \max\{1+a_1+a_2+\dots+a_s : a_i\ge 0, \sum_{i=1}^s a_i p_k(i) \ge -1, 0\le k\le \text{diam}(X)\}$

$$|\mathcal{F}|=1+\max\{a+b,\ aQ_4(1)+bQ_4(2) \ge -Q_4(0);\ aQ_5(1)+bQ_5(2) \ge -Q_5(0);\ a,b \ge 0\ \}$$

$Q_1(1)=27/40$ $Q_1(2)=7/20$
$Q_2(1)=2/5$ $Q_2(2)=1/28$
$Q_3(1)=7/40$ $Q_3(2)=-17/280$
$Q_4(1)=0$ $Q_4(2)=-1/28$
$Q_5(1)=-1/8$ $Q_5(2)=-1/28$

$(1/28)b \le 1$
$(1/8)a+(1/28)b \le 1$
$a=16, b=28$
$|\mathcal{F}|\le 45$

Theorem: Let $\mathcal{F}$ be a w-uniform s-intersecting family. Suppose that

$$p_1 + \cdots + p_s > ws - \sum_{i=0}^{s-1} \frac{(n+2)w(n-w) - ni(n-i+1)}{(n-2i)(n-2i+2)},$$

then $|\mathcal{F}| \leq \binom{n}{s} - \binom{n}{s-1} + \binom{n}{s-2} = \binom{n}{s}\left(1 - \frac{s}{n-s+1}\frac{n-2s+3}{n-s+2}\right)$.

For instance, let s=2
Consider codes (intersecting family) with distances (intersections) 1,2 (w-1,w-2) between distinct codewords. Make a code as follows

1111111000000000000
1111100110000000000 |C|=½(n-w+2)(n-w+1)

In many cases for $6 \leq$ n $\leq$ 46 we establish maximality of this code:

n,w								
	6	3	10	3	12	5	……..	
	7	3	10	4	……..		35	3
	8	3	11	3	18	3	35	4
	9	3	11	4	18	4	35	5
	9	4	12	3	18	5	35	6
	10	3	12	4	18	6	etc.	

Generally for 2-distance constant-weight codes (intersecting families) we obtain

Proposition: Suppose that $d_1+d_2 \leq (2w(n-w)-n)/(n-2)$ $(p_1+p_2 \geq 2w-(2w(n-w)-n)/(n-2)$. Then

$$|C| \text{ or } |\mathcal{F}| \leq \tfrac{1}{2}(n-1)(n-2)$$

Similarly, for 3-intersecting w-uniform families the bounding condition on the distances is computed to be

$$\frac{w(n-w)(n^2+4n-8)-n(2n^2-n-4)}{n(n-2)(n-4)}$$

Applications: Binary codes

Let $C \subset H_n = \{0,1\}^n$ be a binary code with distances $d_1, d_2, \ldots, d_s$

Theorem: Suppose that $d_1 + \cdots + d_s < sn/2$. Then

$$|C| \le 1 + n + \binom{n}{2} + \cdots + \binom{n}{s-2} + \binom{n}{s}.$$

Theorem: (a) Let $C \subset H_n$ be a binary code in which the distances between distinct codewords are d_1, d_2. If $d_1 + d_2 < n$ then $|C| \le M_2 := 1/2(n^2 - n + 2)$.

(b) If $6 \le n \le 46, 48 \le n \le 52$, $n = 54, 55, 57, 58, 60, 61, 62, 63, 64, 66, 67, 69, 72$, then the size of a maximal code with 2 distances equals M_2.

Code C={00…000,110..00, 0110…0,….,00…011} has $\{d_1,d_2\}=\{2,4\}$; is optimal

To prove that even if $d_1+d_2 \ge n$, no larger code exists for small n, compute the Delsarte LP bound.

$$|C| \le \max\{1+a_1+a_2+\ldots+a_s : a_i \ge 0, \textstyle\sum_{i=1}^{s} a_i p_k(i) \ge -1, 0 \le k \le n\}$$

Theorem: (a) Let $C \subset H_n$ be a binary code in which the distances between distinct codewords are d_1, d_2, d_3. If $d_1+d_2+d_3 < 3/2n$, then $|C| \le M_3 := n+\binom{n}{3}$.

(b) If $8 \le n \le 22$ or $n = 24, 25$ then then the size of a maximal code with 3 distances equals M_3.

Code C={all wt 1; all wt. 3} has $\{d_1,d_2,d_3\}$={2,4,6}; is optimal

To prove that even if $d_1+d_2+d_3 \ge n$, no larger code exists for small n, compute the Delsarte LP bound

Theorem: (a) Let $C \subset H_n$ be a binary 4-distance code with distances d_1, d_2, d_3, d_4. If $d_1+d_2+d_3+d_4 < 2n$, then $|C| \le M_4 := 1+\binom{n}{2}+\binom{n}{4}$.

(b) For $10 \le n \le 24$ the maximum size of a 4-distance binary code equals M_4.

Applications: Spherical codes

Let

$$M_s := \binom{n+s-1}{s} + \binom{n+s-2}{s-1}.$$

P. Delsarte, J.-M.Goethals, J. Seidel (1977):

Theorem: Let $C \subset S^{n-1}$ be a set of points $(x_1,x_2,\ldots,x_m)$ such that $(x_i,x_j) \in \{t_1,t_2,\ldots,t_s\}$

Then $m \leq M_s$

O.R.Musin (2008): For s=2, $t_1+t_2>0$ $m \leq \frac{1}{2}n(n+1)$

More generally:

Theorem: Suppose that s is even and $t_1+t_2+\cdots+t_s>0$, then

$$|C| \leq M_{s-2} + \binom{n-2+s}{s} + \binom{n+s-3}{s-1}.$$