Journal of Combinatorial Theory, Series A 118 (2011) 1465–1474

Contents lists available at ScienceDirect

Journal of Combinatorial Theory, Series A

www.elsevier.com/locate/jcta

Bounds on sets with few distances

Alexander Barg [a,b,1], Oleg R. Musin [c,2]

[a] Dept. of Electrical and Computer Engineering and Institute for Systems Research, University of Maryland, College Park, MD 20742, USA
[b] Institute for Problems of Information Transmission, Russian Academy of Sciences, Moscow, Russia
[c] Department of Mathematics, University of Texas at Brownsville, 80 Fort Brown, Brownsville, TX 78520, USA

ARTICLE INFO

Article history:
Received 23 May 2009
Available online 20 January 2011

Keywords:
Distance transitive spaces
Binary codes
Intersecting families
Orthogonal polynomials
Spherical codes

ABSTRACT

We derive a new estimate of the size of finite sets of points in metric spaces with few distances. The following applications are considered:

- we improve the Ray-Chaudhuri–Wilson bound of the size of uniform intersecting families of subsets;
- we refine the bound of Delsarte–Goethals–Seidel on the maximum size of spherical sets with few distances;
- we prove a new bound on codes with few distances in the Hamming space, improving an earlier result of Delsarte.

We also find the size of maximal binary codes and maximal constant-weight codes of small length with 2 and 3 distances.

1. Introduction

We consider finite collections of points in a metric space X with distance function d. Following the terminology of coding theory we call such collections codes. We say that $\mathcal{C} \subset X$ is an s-code if the set of distances $d(\boldsymbol{x}_1, \boldsymbol{x}_2)$ between any two distinct points of $\mathcal{C}$ has size s. The subject of this paper is estimates for the size (the number of points) of s-codes.

The study of s-codes in $\mathbb{R}^n$ was initiated by Einhorn and Schoenberg [10]. Delsarte [5,6] obtained several classical results for s-codes in finite spaces, while for the case of the unit sphere $S^{n-1} \subset \mathbb{R}^n$ the problem of bounding the size of s-codes was first addressed by Delsarte, Goethals, and Seidel in [8]. Codes with few distances in finite spaces are closely related to the well-known combinatorial

E-mail addresses: abarg@umd.edu (A. Barg), omusin@gmail.com (O.R. Musin).
1 Research supported in part by NSF grants DMS0807411, CCF0635271, and CCF0830699.
2 Research supported in part by NSF grant DMS0807640 and NSA grant MSPF-08G-201.

0097-3165/$ – see front matter
doi:10.1016/j.jcta.2011.01.002

problem of bounding the size of families of sets with restricted intersections. Results of this kind are often called intersection theorems in combinatorial literature. They have been a subject of extensive studies beginning with the work of Ray-Chaudhuri and Wilson [22]. Their proofs are mostly based on two general methods, namely, the method of linearly independent polynomials, see e.g., Alon et al. [1], Blokhuis [4], Babai et al. [3], and on Delsarte's linear programming method [6,8].

Recently an improvement of the Delsarte–Goethals–Seidel bound on spherical s-codes for the case $s = 2$ was obtained in the second author's paper [20]. Following this result, Nozaki [21] proved a general bound on the size of spherical s-codes. We continue this line of work, employing Delsarte's ideas to derive a general improvement of the bound [8] for every even s as well as new estimates of the size of s-codes over a finite alphabet. The latter result also enables us to tighten the Ray-Chaudhuri–Wilson bound on the size of uniform s-intersecting families. Of course, both these bounds are known to be tight in general, so our improvements are only valid under some assumptions on the size of the intersections.

2. A bound on *s*-codes

In this section we present a general bound on the size of s-codes (Theorem 5). The bound is most conveniently described in the context of harmonic analysis. This approach to packings of metric spaces was introduced in [5,8] for finite spaces known as association schemes and the sphere S^{n-1} respectively. It was generalized in [15] to all distance transitive compact metric spaces. Under this approach the space X is viewed as a homogeneous space of its isometry group G. The space X is called distance transitive if G acts transitively on ordered pairs of points of X at a given distance. Denote by $d\alpha$ the normalized G-invariant measure on X. The space $L^2(X, d\alpha)$ of complex-valued square-integrable functions on X decomposes into a finite or countably infinite direct sum of pairwise orthogonal finite-dimensional linear spaces V_i of functions called (generalized) spherical harmonics. Let us fix a basis of spherical harmonics $(\phi_{i,1}, \dots, \phi_{i,h_i})$ in the space V_i, where $h_i = \dim V_i$. Since X is distance transitive, the function

$$P_i(\boldsymbol{x}, \boldsymbol{y}) = \sum_{j=1}^{h_i} \phi_{i,j}(\boldsymbol{x})\overline{\phi_{i,j}(\boldsymbol{y})} \tag{1}$$

depends only on the distance $d(\boldsymbol{x}, \boldsymbol{y})$. This expression is called the addition formula in the theory of special functions, and it is only this formula that we need in later derivations. Below we use small p to refer to functions obtained from the functions (1) once the pair of points $\boldsymbol{x}, \boldsymbol{y}$ is replaced by the distance between them, and use x to denote this distance. In particular, $p_i(x)$ is a univariate real polynomial of degree i. Without loss of generality we assume that $p_0 \equiv 1$.

In the cases of interest to us, the functions p_i form a family of classical orthogonal polynomials. Namely, consider the linear functional $\mathcal{L}(f) = \int f(x)\,d\mu(x)$, where $d\mu$ is the measure induced by $d\alpha$ on the set of possible values of the distance on X. Then $\mathcal{L}(p_i p_j) = 0$ for $i \neq j$, and

$$r_i \mathcal{L}\big(p_i^2\big) = 1, \quad \text{where } r_i = \frac{1}{h_i}.$$

As is well known (e.g., [2, p. 244]), the polynomials p_i satisfy a three-term recurrence of the form

$$xp_i = a_i p_{i+1} + b_i p_i + c_i p_{i-1}, \tag{2}$$

where the numbers a_i, b_i, c_i can be easily computed. Given a polynomial $f(x)$ of degree s we can compute its Fourier coefficients in the basis $\{p_i\}$ in a usual way, namely,

$$f_i = r_i \mathcal{L}(f p_i) \quad (0 \leqslant i \leqslant s). \tag{3}$$

Our primary examples will be the Hamming space $H_q^n = (Z_q)^n$ where Z_q is the set of integers $\operatorname{mod} q$, the binary Johnson space $J^{n,w}$ formed by the n-dimensional binary vectors with w ones, $w \leqslant n/2$, and the sphere S^{n-1}. The distance in H_q^n is defined as $d_H(\boldsymbol{x}_1, \boldsymbol{x}_2) = |\{i\colon\ x_{1i} \neq x_{2i}\}|$, the distance in $J^{w,n}$ is given by $d_J(\boldsymbol{x}_1, \boldsymbol{x}_2) = \frac{1}{2} d_H(\boldsymbol{x}_1, \boldsymbol{x}_2)$, and the distance on S^{n-1} is measured as the inner product between the vectors.

Table 1
Parameters of the metric spaces.

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

To illustrate the above ideas, let us consider the Hamming case $X = H_q^n$. A typical isometry of X is a permutation of coordinates followed by a permutation of symbols in every coordinate, i.e., $G = S_q \wr S_n$. An orthogonal basis of the space V_i is formed of functions $\phi_{i,j}(\boldsymbol{x}) = e^{\frac{2\pi i}{q}(\alpha_1 x_{l_1}+\cdots+\alpha_i x_{l_i})}$, where $1 \leqslant l_1 < \cdots < l_i \leqslant n$ is an i-subset of $[n]$ and $\alpha_m \in Z_q\backslash 0$, $m = 1, \ldots, i$. There are $h_i = \binom{n}{i}(q-1)^i$ linearly independent functions $\phi_{i,j}$ of this form. Then p_i is a Krawtchouk polynomial $K_i(x)$ of degree i whose explicit form can be found from (1). We have

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

In particular, $K_i(0) = \binom{n}{i}(q-1)^i$,

$$K_0(x) = 1, \qquad K_1(x) = n(q-1) - qx,$$
$$K_2(x) = \frac{1}{2}\left\{q^2x^2 - q(2qn - q - 2n + 2)x + (q-1)^2 n(n-1)\right\}. \tag{4}$$

For $X = J^{n,w}$ the polynomials p_i form a certain family of discrete Hahn polynomials [7]. The Hahn polynomial of degree i is given by

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

Finally, for S^{n-1} the functions p_i are given by the Gegenbauer polynomials $G_i(t)$. The explicit form and properties of these polynomials are well known. All the information about them that we need is listed in Table 1 together with the corresponding properties of K_i and Q_i. There is no single reference with the proofs of these formulas although they are mentioned in many places. The primary sources are Koekoek and Swarttouw [17] (or the recent book [16]) or Andrews et al. [2, Chapter 6], but the normalizations there are different from the ones used above. Hahn polynomials are also discussed by Delsarte in [5] (without being identified as such) and [7].

The following bound on s-codes is well known. It was proved by Delsarte [5,6] for codes in Q-polynomial association schemes which includes H_q^n and $J^{n,w}$, and by Delsarte et al. [8] for codes in S^{n-1}.

Theorem 1. *Let $\mathcal{C}$ be an s-code in a compact distance-transitive space X. Then*

$$|\mathcal{C}| \leqslant h_0 + h_1 + \cdots + h_s. \tag{5}$$

For $X = S^{n-1}$ and $s = 2$ this theorem gives the bound $|\mathcal{C}| \leqslant \frac{1}{2}n(n+3)$. This estimate was recently improved in [20] where it was shown that if the inner products between distinct code words take values t_1, t_2, and $t_1 + t_2 \geqslant 0$, then $|\mathcal{C}| \leqslant \frac{1}{2}n(n+1)$. The proof relies on the method of linearly independent polynomials. Subsequently, Nozaki [21] proved a general bound on spherical s-codes. His theorem builds upon Delsarte's ideas and is included here for completeness.

We will need a result in matrix analysis known as Ostrowski's theorem [14, pp. 224–225].

Theorem 2. *Let F, S be $N \times N$ real matrices, and let F be symmetric. Let the eigenvalues of F and SS^T be arranged in increasing order, i.e., $\lambda_i(F) \leqslant \lambda_j(F)$, $\lambda_i(SS^T) \leqslant \lambda_j(SS^T)$, $i < j$. For each $k = 1, \ldots, N$ there exists a real number θ_k, $0 \leqslant \theta_k \leqslant \lambda_N(SS^T)$ such that*

$$\lambda_k\big(SFS^T\big) = \theta_k \lambda_k(F).$$

Theorem 3. *(Nozaki [21].) Let $\mathcal{C} = \{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_M\} \subset X$ be an s-code with distances $d_1, \ldots, d_s$. 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*

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

Proof. Let $|\mathcal{C}| = M$ and consider the $M \times h_l$ matrix H_l given by $(H_l)_{i,j} = \phi_{l,j}(\boldsymbol{x}_i)$, where $i = 1, \ldots, M$; $j = 1, \ldots, h_l$. Let $\mathcal{H} = (H_0, H_1, \ldots, H_s)$ and consider the $M \times M$ matrix $A = \mathcal{H} F \mathcal{H}^t$ where

$$F = f_0 I_1 \oplus f_1 I_{h_1} \oplus \cdots \oplus f_s I_{h_s}$$

is a direct sum. By (1) the general entry of A equals $A_{\boldsymbol{x},\boldsymbol{y}} = f(d(\boldsymbol{x}, \boldsymbol{y}))$, which implies that $A = f(0) I_M$.

Here our arguments deviate from [21]. Let $S = \left[\begin{smallmatrix} \mathcal{H} \\ 0 \end{smallmatrix}\right]$ be an $N \times N$ matrix, $N = \sum_{i=0}^s h_i$, and let $A' = SFS^T$. The eigenvalues of A' are 0 and $f(0)$ with multiplicities $N - M$ and M, respectively. By Ostrowski's theorem, to every positive eigenvalue of A' there corresponds a positive eigenvalue of F, i.e.,

$$M = \big|\{k\colon \lambda_k\big(A'\big) > 0\}\big| \leqslant \big|\{k\colon \lambda_k(F) > 0\}\big|,$$

which was to be proved. $\square$

To apply this theorem let us compute some coefficients of the polynomial $f(x)$.

Lemma 4. *Let $f(x) = \prod_{i=1}^s (d_i - x) = \sum_{i=0}^s f_i p_i(x)$. Then*

$$f_s = (-1)^s r_s c_1 c_2 \cdots c_s \quad (s \geqslant 1),$$
$$f_{s-1} = (-1)^s r_{s-1} c_1 \cdots c_{s-1} \sum_{j=1}^s (b_{j-1} - d_j) \quad (s \geqslant 2).$$

Proof. We have

$$f(x) = (-1)^s \big(x^s - (d_1 + \cdots + d_s) x^{s-1}\big) + \cdots.$$

In the following we use the relation $\mathcal{L}(x^m p_k) = 0$, valid for all $0 \leqslant m < k$, and relations (2) and (3). We compute

$$\begin{aligned}(-1)^s f_s &= r_s \mathcal{L}\big(x^s p_s\big) = r_s \mathcal{L}\big(x^{s-1}(a_s p_{s+1} + b_s p_s + c_s p_{s-1})\big) \\ &= r_s c_s \mathcal{L}\big(x^{s-1} p_{s-1}\big) = \cdots = r_s c_1 c_2 \cdots c_s.\end{aligned}$$

Next we claim that

$$\mathcal{L}\big(x^s p_{s-1}\big) = c_1 c_2 \cdots c_{s-1}(b_0 + b_1 + \cdots + b_{s-1}), \quad s \geqslant 2.$$

Indeed, $\mathcal{L}(x^2 p_1) = \mathcal{L}(x(b_1 p_1 + c_1)) = b_1 c_1 + b_0 c_1$. Now let us assume that

$$\mathcal{L}\big(x^{s-1} p_{s-2}\big) = c_1 c_2 \cdots c_{s-2}(b_0 + b_1 + \cdots + b_{s-2}).$$

Then

$$\begin{aligned}\mathcal{L}\big(x^s p_{s-1}\big) &= \mathcal{L}\big(x^{s-1}(b_{s-1}p_{s-1}+c_{s-1}p_{s-2})\big)\\ &= b_{s-1}c_1c_2\cdots c_{s-1}+c_{s-1}\big(c_1c_2\cdots c_{s-2}(b_0+b_1+\cdots+b_{s-2})\big)\end{aligned}$$

as was to be proved. Next,

$$\begin{aligned}f_{s-1} &= r_{s-1}\mathcal{L}\big((-1)^s\big(x^s-(d_1+\cdots+d_s)x^{s-1}\big)p_{s-1}\big)\\ &= (-1)^s r_{s-1}\big(c_1c_2\cdots c_{s-1}(b_0+b_1+\cdots+b_{s-1})-(d_1+\cdots+d_s)c_1\cdots c_{s-1}\big)\\ &= (-1)^s r_{s-1}c_1\cdots c_{s-1}\big((b_0+b_1+\cdots+b_{s-1})-(d_1+\cdots+d_s)\big). \qquad \square\end{aligned}$$

The next theorem provides an improvement of the general bound (5). It will be used in subsequent sections to establish the main results of this paper.

Theorem 5. *Let $\mathcal{C}$ be a code in a compact distance-transitive space X with distances $d_1,\dots,d_s$. Let the numbers b_i, c_i, $i \geqslant 0$ be defined by* (2) *and let*

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

(a) *Suppose that $c_i<0$, $i=1,2,\dots$ and $D\geqslant 0$. Then*

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

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

$$|\mathcal{C}| \leqslant \begin{cases} h_0+h_1+\cdots+h_{s-2} & s\equiv 1(\operatorname{mod} 2) \text{ and } D\geqslant 0,\\ h_0+h_1+\cdots+h_{s-1} & s\equiv 1(\operatorname{mod} 2) \text{ and } D<0,\\ h_0+h_1+\cdots+h_{s-2}+h_s & s\equiv 0(\operatorname{mod} 2) \text{ and } D\leqslant 0.\end{cases}$$

Proof. The proof uses Theorem 3 and is completed by the analysis of the signs of f_s and f_{s-1} for the cases specified in the theorem. $\square$

Remark. It is possible to evaluate other coefficients of the polynomial $f(x)$ in Lemma 4 which will lead to further refinements of bound (5) from Theorem 3. However the conditions on the distances will involve higher-degree symmetric functions of them, which limits somewhat their usefulness.

Example 1. Consider the binary extended Golay code $\mathcal{G}_{24}$ of length $n=24$ and cardinality 4096. The distances between distinct codevectors of $\mathcal{G}_{24}$ are 8, 12, 16, and 24 [19, p. 67]. Since $\mathcal{G}_{24}$ is a linear code, it contains the all-zero vector and therefore also the vector $\mathbf{1}=1^{24}$ of all ones. Therefore, if $\boldsymbol{x}$ is a codevector then so is the vector $\mathbf{1}+\boldsymbol{x}$. Deleting one vector from each of such pairs, we obtain a code $\mathcal{G}_{24}^o$ of cardinality $2048=\binom{24}{1}+\binom{24}{3}$ with distances $d_1=8, d_2=12, d_3=16$. From Table 1, $b_i=12$ for all i, so $D=0$, and Theorem 5(a) implies that for any code $\mathcal{C}\in H_2^{24}$ with distances 8, 12, 16, we have $|\mathcal{C}|\leqslant h_0+h_1+h_3$. However,

$$(8-x)(12-x)(16-x)=\frac{3}{4}K_1(x)+\frac{3}{4}K_3(x),$$

meaning that $f_0=0$, so the bound can be tightened to $|\mathcal{C}|\leqslant h_1+h_3$. In other words, the Golay "half-code" $\mathcal{G}_{24}^o$ is an optimal 3-distance code of length 24. This example will be generalized in Section 4 below.

In the following sections we will use another general bound on codes known as Delsarte's "linear programming" bound [5]. For s-codes this bound gives

Theorem 6 *(Delsarte). Let $\mathcal{C}\subset X$ be an s-code with distances $d_1,\dots,d_s$. Then*

$$|\mathcal{C}| \leqslant \max\left\{1+\alpha_1+\cdots+\alpha_s\colon \sum_{i=1}^{s}\alpha_i p_k(d_i)\geqslant -p_k(\tau_0),\ k\geqslant 0;\ \alpha_i\geqslant 0,\ i=1,\dots,s\right\}.$$

Here $\tau_0 = 0$ for the Hamming and Johnson spaces and $\tau_0 = 1$ for the sphere S^{n-1}.

3. Constant weight codes and intersecting families

Call a family $\mathcal{F} = \{F_1, F_2, \ldots\}$ of subsets of an n-element set w-*uniform* if $|F_i| = w, i = 1, 2, \ldots,$ and call it s-*intersecting* if $\forall_{F_i,F_j} |F_i \cap F_j| \in \{w, \ell_1, \ldots, \ell_s\}$ for some $\ell_1, \ldots, \ell_s, 0 \leqslant \ell_i < w$. For two subsets F_1, F_2 with $|F_1 \cap F_2| = \ell$ the distance between their indicator vectors $\boldsymbol{x}_1, \boldsymbol{x}_2$ equals $d_J(\boldsymbol{x}_1, \boldsymbol{x}_2) = w - \ell$. Thus, the indicator vectors of $\mathcal{F}$ form an s-code $\mathcal{C}$ in $J^{n,w}$.

Theorem 7. *(Ray-Chaudhuri–Wilson [22].) Let $\mathcal{F}$ be a w-uniform s-intersecting family. Then*

$$|\mathcal{F}| \leqslant \binom{n}{s}. \tag{6}$$

Proof. Follows from (5) and Table 1. □

Deza, Erdös, and Frankl [9] showed that for $n \geqslant w\binom{3w}{w}$ this estimate can be improved to

$$|\mathcal{F}| \leqslant \prod_{i=1}^{s} \frac{n - \ell_i}{w - \ell_i}. \tag{7}$$

The particular case $\{\ell_1, \ldots, \ell_s\} = \{w - s, w - s + 1, \ldots, w - 1\}$ corresponds to the celebrated Erdös–Ko–Rado theorem [11]. According to it, if $n \geqslant (w - s + 1)(s + 1)$ then

$$|\mathcal{F}| \leqslant \binom{n - w + s}{s}.$$

Note also that generally (6) is best possible because the bound is met by $\mathcal{F} = \binom{[n]}{w}$. Several generalizations of Theorem 7 were obtained in [1,3,23]. We obtain the following general improvement of this theorem.

Theorem 8. *Let $\mathcal{F}$ be a w-uniform s-intersecting family. Suppose that*

$$\ell_1 + \cdots + \ell_s \geqslant \frac{s(w^2 - (s-1)(2w - n/2))}{n - 2(s-1)}. \tag{8}$$

Then

$$|\mathcal{F}| \leqslant \binom{n}{s} - \binom{n}{s-1} \frac{n - 2s + 3}{n - s + 2}. \tag{9}$$

Proof. The proof will follow from Theorem 5(a). For it to hold, we need that

$$\sum_{i=1}^{s} d_i = ws - \sum_{i=1}^{s} \ell_i \leqslant \sum_{i=0}^{s-1} b_i. \tag{10}$$

Now take the value of b_i from Table 1 and use induction to show that

$$\sum_{i=0}^{s-1} \frac{(n+2)w(n-w) - ni(n-i+1)}{(n-2i)(n-2i+2)} = \frac{ws(n-w) - \binom{s}{2}n}{n - 2(s-1)}.$$

The proof is concluded by substituting this expression for $\sum_{i=0}^{s-1} b_i$ in (10). □

Let us show that the region of ℓ_i's defined in (8) is not void. Write this inequality as

$$\sum \ell_i > ws - \frac{ws(n-w) - \binom{s}{2}n}{n - 2(s-1)}.$$

As $s \leqslant w \leqslant n/2$, the numerator of the fraction is nonnegative and $n-2(s-1) \leqslant n$. Thus (8) will hold if $\sum \ell_l > w^2 s/n - \binom{s}{2}$. This last inequality holds in turn if w is close to $n/2$ and the ℓ_is are large. For instance if $s=2$ then the Ray-Chaudhuri–Wilson bound can be tightened for all $\ell_1+\ell_2 > (2w(w-2)+n)/(n-2)$. See also the example in the end of this section. The bound (9) is not as good as (7) whenever the latter applies; on the other hand, (9) involves no restrictions on n.

Let us consider in more detail the case of 2- and 3-intersecting families, switching to the language of constant weight codes.

Corollary 9. *Let $\mathcal{C} \subset J^{n,w}$ be a code.*

(a) *Suppose that the distances between distinct vectors of $\mathcal{C}$ take values d_1, d_2. If*

$$d_1 + d_2 \leqslant \frac{2w(n-w)-n}{n-2} \tag{11}$$

then $|\mathcal{C}| \leqslant \frac{1}{2}(n-1)(n-2)$.

(b) *Suppose that the distances between distinct vectors in $\mathcal{C}$ take values d_1, d_2, d_3. If*

$$d_1 + d_2 + d_3 \leqslant \frac{3w(n-w)-3n}{n-4}$$

then $|\mathcal{C}| \leqslant \frac{n}{6}(n^2-6n+11)$.

We note that a 2-distance constant weight code can be constructed by taking the $\binom{n-w+2}{2}$ vectors with $w-2$ ones in the first coordinates and the remaining 2 ones anywhere outside them. This code attains the Erdös–Ko–Rado bound and in the case $w=3$ is extremal for Part (a) of the above corollary for all $n \geqslant 6$.

To establish the next result we will need the following result of Larman, Rogers, and Seidel [18], restated here in the form convenient to us: *Suppose that $\mathcal{C} \subset H_2^n$ is a binary code with distances $d_1 < d_2$, and $|\mathcal{C}| > 2n+3$. Then $d_1/d_2 = (k-1)/k$ where k is an integer satisfying $2 \leqslant k \leqslant \frac{1}{2} + \sqrt{n/2}$.* Below we call this relation for the numbers d_1, d_2 the LRS condition.

Proposition 10. (a) *For $6 \leqslant n \leqslant 44$ and $3 \leqslant w \leqslant n/2$ with the exception of the cases $(n,w) = (23,7), (44,17)$ the size of a 2-distance code $\mathcal{C} \subset J^{n,w}$ satisfies $|\mathcal{C}| \leqslant \frac{1}{2}(n-1)(n-2)$.*

(b) *If n and w satisfy any of the following conditions*:

$$6 \leqslant n \leqslant 8 \quad \textit{and} \quad w = 3;$$
$$9 \leqslant n \leqslant 11 \quad \textit{and} \quad 3 \leqslant w \leqslant 4;$$
$$12 \leqslant n \leqslant 14 \quad \textit{or} \quad 25 \leqslant n \leqslant 34 \quad \textit{and} \quad 3 \leqslant w \leqslant 5;$$
$$15 \leqslant n \leqslant 24 \quad \textit{or} \quad 35 \leqslant n \leqslant 46 \quad \textit{and} \quad 3 \leqslant w \leqslant 6,$$

then the maximum 2-distance code $\mathcal{C} \subset J^{n,w}$ satisfies $|\mathcal{C}| = \frac{1}{2}(n-w+1)(n-w+2)$.

Proof. Part (a). If the distances in $\mathcal{C}$ satisfy (11), then the upper bound in Part (a) follows from the previous corollary. Otherwise we examine every pair of distances d_1, d_2. If a given pair does not satisfy the LRS condition, then $|\mathcal{C}| \leqslant 2n+3$. If this condition is satisfied, we compute the Delsarte bound of Theorem 6. Together these arguments produced an upper bound $\binom{n-1}{2}$ on the code size for all the parameters in the statement.

Part (b). For all $n, w \leqslant n/2$ there exists a constant weight 2-distance code of size $\binom{n-w+2}{2}$. The matching upper estimates are established by computing the Delsarte bound. $\square$

As an example of the arguments involved in the proof, let $\mathcal{C}$ be a two-distance code in $J^{n,w}$ with $n=13, w=5$. There are 10 possibilities for the distances d_1, d_2. The LRS condition is fulfilled if $d_1/d_2=(k-1)/k, 2\leqslant k\leqslant 3$. Thus, the pairs $(1,3)$, $(1,4)$, $(1,5)$, $(2,5)$, $(3,4)$, $(3,5)$, $(4,5)$ do not satisfy it, so for all these cases $|\mathcal{C}|\leqslant 29$. Next we compute the Delsarte bound $D(d_1,d_2)$ for the 3 remaining cases, obtaining $D(1,2)=45$, $D(2,3)=33$, $D(2,4)=27$. This exhausts all the possible cases, so we conclude that $|\mathcal{C}|\leqslant 45$. As mentioned above, the extremal configuration has 45 vectors at distances 1 or 2. This code meets both the Delsarte bound and the Erdös–Ko–Rado bound. This establishes both parts of the last proposition in the case considered.

Likewise, if $n=18$, $w=8$, Corollary 9(a) applies whenever $d_1+d_2\leqslant 8$. For any such two-distance code we obtain $|\mathcal{C}|\leqslant 136$. The remaining possibilities for the distances are covered by the LRS condition or checked by computing the Delsarte bound. This establishes the corresponding case of Part (a) of the proposition.

Generally, the Delsarte bound is better than the other bounds for n up to about 45 and is rather loose (and difficult to compute) for greater n.

Note that the case $n=23$, $w=7$ is a true exception in Part (a) of Proposition 10. Indeed, the 253 vectors of weight 7 in the binary Golay code of length 23 have pairwise Johnson distances 4 and 6 [19, p. 69], which is greater than $\binom{23}{2}=231$.

4. s-codes in the Hamming space

Let $\mathcal{C}\subset H_q^n$ be a code in which the distances between distinct codewords are $d_1,d_2,\dots,d_s$. Theorem 5 implies the following bound.

Theorem 11. *Suppose that*

$$d_1+\dots+d_s\leqslant\frac{s}{q}\left[(q-1)n-\frac{1}{2}(q-2)(s-1)\right]\quad\left(\frac{1}{2}sn\quad \text{for } q=2\right).$$

Then

$$|\mathcal{C}|\leqslant 1+n(q-1)+\binom{n}{2}(q-1)^2+\dots+\binom{n}{s-2}(q-1)^{s-2}+\binom{n}{s}(q-1)^s. \tag{12}$$

This enables us to draw some conclusions for sets of binary vectors with few distances.

Theorem 12. (a) *Let $\mathcal{C}$ be a binary code in which the distances between distinct codewords are d_1, d_2. If $d_1+d_2\leqslant n$ then $|\mathcal{C}|\leqslant\frac{1}{2}(n^2-n+2)$.*

(b) *Let $\mathcal{C}$ be a binary code in which the distances between distinct codewords are d_1,d_2,d_3. If $d_1+d_2+d_3\leqslant 3n/2$ then*

$$|\mathcal{C}|\leqslant 1+n+\binom{n}{3}.$$

If in addition none or two of the three distances d_1,d_2,d_3 are $>n/2$ then

$$|\mathcal{C}|\leqslant n+\binom{n}{3}.$$

Proof. Part (a) follows from the previous theorem.

Part (b). Consider the annihilator polynomial $f(x)=(d_1-x)(d_2-x)(d_3-x)$ and let $f_0,\dots,f_3$ be its coefficients in the Krawtchouk basis. We know that under the assumption of the theorem, $f_2\leqslant 0$. This proves the first claim in Part (b). Further, by (3), the constant coefficient equals

$$f_0=-\left(\frac{n}{2}-d_1\right)\left(\frac{n}{2}-d_2\right)\left(\frac{n}{2}-d_3\right)+\frac{n}{4}(d_1+d_2+d_3)-\frac{3n^2}{8}.$$

If both assumptions in Part (b) of the theorem hold then $f_0\leqslant 0$. This proves the bound $|\mathcal{C}|\leqslant n+\binom{n}{3}$. $\square$

Proposition 13. (a) *If $6 \leqslant n \leqslant 74$ with the exception of the values $n = 47, 53, 59, 65, 70, 71$, or if $n = 78$, then the size of a maximal code with 2 distances equals $\frac{1}{2}(n^2 - n + 2)$.*

(b) *If $8 \leqslant n \leqslant 22$ or $n = 24$ then the size of a maximal code with 3 distances equals $n + \binom{n}{3}$.*

(c) *If $10 \leqslant n \leqslant 33$ then the size of a maximal code with 4 distances equals $1 + \binom{n}{2} + \binom{n}{4}$.*

Proof. Part (a). Observe that the size of the code $\mathcal{C}$ formed of all vectors of weight 2 and the all-zero vector equals $1 + \binom{n}{2}$ for all $n \geqslant 3$. It remains to show that even if $d_1 + d_2 \geqslant n + 1$, no two-distance code of length n for each value of n in the statement can have larger size. To establish this, for each n we compute the Delsarte bound of Theorem 6 for all the possible distance values $d_1, d_2, d_1 + d_2 \geqslant n + 1$ that satisfy the LRS condition $d_1/d_2 = (k-1)/k$. These computations show that in each case the Delsarte bound is less than or equal to $\frac{1}{2}(n^2 - n + 2)$. This establishes our claim.

Part (b). We proceed in a way analogous to Part (a). Note that the code $\mathcal{C}$ formed of all vectors of weights 1 and 3 has size $|\mathcal{C}| = n + \binom{n}{3}$ for all $n \geqslant 3$. We need to show that even if $d_1 + d_2 + d_3 \geqslant 3n/2 + 1$, no three-distance code of length $8 \leqslant n \leqslant 22$ or 24 can have larger size. To do this, we rely on Part (b) of the previous theorem. Namely, for each n in the range and for all d_1, d_2, d_3 such that $d_1 + d_2 + d_3 \geqslant 3n/2 + 1$ or that $f_0 > 0$, we compute the Delsarte bound of Theorem 6 and verify that it is less than or equal to the claimed code size.

Part (c). For $n \geqslant 6$, a 3-code of size $1 + \binom{n}{2} + \binom{n}{4}$ is formed of all vectors of weights 0, 2, 4. Therefore, if $f_1 \leqslant 0$ and $f_3 \leqslant 0$ in the expansion

$$\prod_{i=1}^{4}(d_i - x) = \sum_{i=0}^{4} f_i K_i(x),$$

then the claim holds true. Otherwise, for every $10 \leqslant n \leqslant 33$ and for every set of numbers d_1, d_2, d_3, d_4 that fails these conditions, we compute the Delsarte bound and verify that it is less than or equal to $1 + \binom{n}{2} + \binom{n}{4}$. $\square$

Example 1 above shows that an extremal 3-distance code $\mathcal{G}_{24}^o$ of length $n = 24$ can be obtained from the binary Golay code $\mathcal{G}_{24}$. A related example accounts for the omission of $n = 23$ from Part (b). Indeed, the even subcode of the Golay code $\mathcal{G}_{23}$ (i.e., the dual code $\mathcal{G}_{23}^{\perp}$) has distances 8, 16, 24, but its size 2048 is greater than $23 + \binom{23}{3} = 1794$, so this case is a true exception.

5. Spherical codes

Let $\mathcal{C} \subset S^{n-1}$ be a code such that the inner product of any two distinct code vectors takes one of the s values $t_1, \ldots, t_s$. Let

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

Theorem 14 *(Delsarte–Goethals–Seidel, 1977). $|\mathcal{C}| \leqslant M_s$.*

Proof. Follows from (5) and Table 1 by the identity $\sum_{k=0}^{p} \binom{m+k}{k} = \binom{m+p+1}{p}$. $\square$

This result was improved in [20] as follows: If $s = 2$ and $t_1 + t_2 \geqslant 0$ then $|\mathcal{C}| \leqslant \frac{1}{2}n(n+1)$. We now have the following general improvement.

Theorem 15. *Suppose that s is even and $t_1 + t_2 + \cdots + t_s \geqslant 0$, then*

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

Proof. Consider the polynomial $g(x) = \prod_{i=1}^{s}(x - t_i)$. By Lemma 4 its leading coefficients in the basis of Gegenbauer polynomials are

$$g_s = r_s c_1 c_2 \cdots c_s > 0, \qquad g_{s-1} = r_s(-t_1 - t_2 - \cdots - t_s)\prod_i c_i.$$

Thus, $g_{s-1} \leqslant 0$ if $t_1 + \cdots + t_s \geqslant 0$ (since $c_i > 0$ for all i). Then the last case of Theorem 5(b) applies, and the result follows from Table 1. □

Any binary code can be mapped to S^{n-1} by a distance-preserving mapping, so the bound for spherical codes implies bounds on binary codes (both constant weight and unrestricted). However the bounds thus obtained are generally inferior to the results derived in the corresponding discrete spaces. This is because the bounds become progressively stronger as we move from a space to its subspaces, so there is no gain in using the last theorem for binary codes.

The methods discussed in this paper are applicable to other distance-transitive spaces of interest to geometry and combinatorics. We point to one such class of spaces, namely, q-analogs of the Hamming and Johnson spaces, for which intersection theorems were studied in [12,13].

Acknowledgment

We are grateful to a reviewer for detailed and insightful comments on the first version of this paper.

References

[1] N. Alon, L. Babai, H. Suzuki, Multilinear polynomials and Frankl–Ray-Chaudhuri–Wilson type intersection theorems, J. Combin. Theory Ser. A 58 (1991) 165–180.
[2] G.E. Andrews, R. Askey, R. Roy, Special functions, Cambridge University Press, 1999.
[3] L. Babai, H. Snevily, R.M. Wilson, A new proof of several inequalities on codes and sets, J. Combin. Theory Ser. A 71 (1995) 148–153.
[4] A. Blokhuis, Polynomials in finite geometries and combinatorics, in: Surveys in Combinatorics, 1993, Keele, in: London Math. Soc. Lecture Note Ser., vol. 187, Cambridge Univ. Press, Cambridge, 1993, pp. 35–52.
[5] P. Delsarte, An algebraic approach to the association schemes of coding theory, Philips Res. Rep. Suppl. 10 (1973) 1–97.
[6] P. Delsarte, Four fundamental parameters of a code and their combinatorial significance, Inform. Control 23 (1973) 407–438.
[7] P. Delsarte, Hahn polynomials, discrete harmonics, and t-designs, SIAM J. Appl. Math. 34 (1) (1978) 157–166.
[8] P. Delsarte, J.M. Goethals, J.J. Seidel, Spherical codes and designs, Geom. Dedicata 6 (1977) 363–388.
[9] M. Deza, P. Erdös, P. Frankl, Intersection properties of systems of finite sets, Proc. London Math. Soc. 36 (3) (1978) 369–384.
[10] S.J. Einhorn, I.J. Schoenberg, On Euclidean sets having only two distances between points. I, Nederl. Akad. Wetensch. Proc. Ser. A 69, Indag. Math. 28 (1966) 479–488;
S.J. Einhorn, I.J. Schoenberg, On Euclidean sets having only two distances between points. II, Nederl. Akad. Wetensch. Proc. Ser. A 69, Indag. Math. 28 (1966) 489–504.
[11] P. Erdös, C. Ko, R. Rado, Intersection theorems for systems of finite sets, Q. J. Math. 12 (2) (1961) 313–320.
[12] P. Frankl, R.M. Wilson, The Erdős–Ko–Rado theorem for vector spaces, J. Combin. Theory Ser. A 43 (1986) 228–236.
[13] T.-S. Fu, Erdős–Ko–Rado-type results over $J_q(n,d)$, $H_q(n,d)$ and their designs, Discrete Math. 196 (1999) 137–151.
[14] R.A. Horn, C.R. Johnson, Matrix Analysis, Cambridge University Press, Cambridge, 1990.
[15] G. Kabatyansky, V.I. Levenshtein, Bounds for packings on the sphere and in the space, Probl. Inf. Transm. 14 (1) (1978) 3–25.
[16] R. Koekoek, P.A. Lesky, F. Swarttouw, Hypergeometric Orthogonal Polynomials and Their q-Analogues, Springer, 2010.
[17] R. Koekoek, F. Swarttouw, The Askey-scheme of hypergeometric orthogonal polynomials and its q-analogue, Technical Report 98-17, Department of Technical Mathematics and Informatics, Delft University of Technology, 1998, arXiv:math/9602214.
[18] D.G. Larman, C.A. Rogers, J.J. Seidel, On two-distance sets in Euclidean space, Bull. Lond. Math. Soc. 9 (1977) 261–267.
[19] F.J. MacWilliams, N.J.A. Sloane, The Theory of Error-Correcting Codes, North-Holland, Amsterdam, 1991.
[20] O.R. Musin, Spherical two-distance sets, J. Combin. Theory Ser. A 116 (4) (2009) 988–995.
[21] H. Nozaki, New upper bound for the cardinalities of s-distance sets on the unit sphere, arXiv:0906.0195.
[22] D.K. Ray-Chaudhuri, R.M. Wilson, On t-designs, Osaka J. Math. 12 (3) (1975) 737–744.
[23] H.S. Snevily, A generalization of the Ray-Chaudhuri–Wilson theorem, J. Combin. Des. 3 (5) (1995) 349–352.