A simple proof of the main inequalities for parameters of codes in polynomial association schemes

Vladimir Levenshtein

INRIA

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

A simple proof of the main inequalities for parameters of codes in polynomial association schemes

Vladimir LEVENSHTEIN

N° 2347
Septembre 1994

PROGRAMME 2

A simple proof of the main inequalities for parameters of codes in polynomial association schemes

Une preuve simple des principales inégalités sur les paramètres des codes dans des schémas d'association polynomiaux

Vladimir Levenshtein*

Abstract

Codes in P- and Q-polynomial association schemes are considered. A simple proof of seven main inequalities for such code parameters as the minimal distance, the dual distance, the number of distances, the external distance and the covering radius is given. It is based in essential only on the annihilating and dual-annihilating polynomials for a code and on orthogonality conditions for system P and Q and for certain adjacent systems as well. All these inequalities are attained for some codes in some spaces, in particular, for some codes in the Hamming space.

*Keldysh Institute for Applied Mathematics, Russian Academy of Sciences, Miusskaya sq. 4, 125047 Moscow, Russia. **Invité au projet CODES du 01.04. au 30.04.94**

Résumé

On considère des codes dans des schémas d'association P et Q-polynomiaux. On donne une preuve simple de sept inégalités importantes sur les paramètres de tels codes comme la distance minimale, la distance duale, le nombre de distances, la distance externe et le rayon de recouvrement. Cette preuve est essentiellement basée sur les polynômes annulateurs du code et de son dual, et sur des conditions d'orthogonalité des systèmes P et Q et d'autres systèmes adjacents. Toutes ces inégalités sont atteintes pour des codes dans certains espaces, en particulier pour des codes dans l'espace de Hamming.

1 Introduction. Polynomial association schemes

We consider codes and designs in metric spaces which are P- and Q-polynomial association schemes [6, 11, 1, 4]. In this connection we use a definition association schemes which is close to the definition of metric space.

A (symmetrical) *association scheme* (with D classes) $\{X, d(x,y)\}$ is a finite set X with a given function $d(x,y)$ which is defined for any $x, y \in X$, takes values $0, 1, \ldots, D$ and has following properties :

1. $d(x,y) = 0$ if and only if $x = y$;
2. $d(x,y) = d(y,x)$ for any $x, y \in X$;
3. for any $x, y \in X$ and any $i, j \in \{0, 1, \ldots, D\}$, the number of points z such that $d(x,z) = i, d(z,y) = j$ depends on $d(x,y)$ only (this number is denoted by p_{ij}^k, where $k = d(x,y)$.

In particular, for association schemes $p_{ij}^k = p_{ji}^k$ and for any x the number p_{ii}^0 of points $y \in X$ such that $d(x,y) = i$ does not depend on x. This number is denoted by ν_i and is called *valency*. Notice that in general the function $d(x,y)$ does not satisfy the triangle inequality : $d(x,y) \leq d(x,z) + d(z,y)$. However, for many significant examples of association schemes the function $d(x,y)$ posseses this property and is a metric. In particular, the Hamming space $H(n,q), q = 2, 3, \ldots$, consisting of q^n vectors $x = (x_1, \ldots, x_n)$ where $x_i \in \{0, 1, \ldots, q-1\}$ with the metric $d(x,y)$ being equal to the number of

places where x and y differ, forms an association scheme with $D = n$ classes. As another example of an association scheme with $D = \min(w, n-w)$ classes we consider the Johnson space $J(n,w)$ consisting of $\begin{pmatrix} n \\ w \end{pmatrix}$ w-subsets of a n-set with the metric $d(x,y) = w - |x \cap y|$. Notice that $J(n,w)$ can be considered as subset of $H(n,2)$ consisting of characteristic vectors of w-subsets of a n-set (that is, of binary vectors of length n and weight w) with the metric being equal to half of the Hamming distance.

Using the adjacency matrices $A_i, i = 0, 1, \ldots, D$, of order $|X|$ defined by

$$(A_i)_{x,y} = \begin{cases} 1 & \text{if } d(x,y) = i, \\ 0 & \text{otherwise,} \end{cases} \tag{1.1}$$

the definition of association scheme can be expressed by

$$A_0 = I, \quad \sum_{i=0}^{D} A_i = J, \quad A_i = A_i^T, \quad A_i A_j = \sum_{k=0}^{D} p_{ij}^k A_k, \tag{1.2}$$

where I is the unit matrix, J is the matrix the entries of which are all equal to one and A^T is the transpose of A.

The matrices A_i are linearly independent and generate a $(D+1)$-dimensional (over $\mathbb{R}$) commutative algebra $\mathcal{A}$ of symmetrical matrices, which is called the Bose-Mesner algebra. We consider $|X|$-dimensional space $V = \{f(x) : X \Rightarrow \mathbb{R}\}$ of real functions on X with the inner product

$$< u, v >= \frac{1}{|X|} \sum_{x \in X} u(x)v(x).$$

It is known [6, 1, 4] that for an association scheme with D classes (as for $(D+1)$-dimensional commutative algbera of symmetrical matrices) there exists a decomposition

$$V = V_0 + \ldots + V_D$$

of V into a direct sum of pairwise orthogonal subspaces V_i, where V_i is a maximal common eigenspace of $A_0, A_1, \ldots, A_D$. We can assume that V_0 consists of constants only since eigenvector from all units can belong only to an one-dimensional common eigenspace.

Let $m_i = \dim V_i, i = 0, 1, \ldots, D, m_0 = 1$, and $\{v_{ij}(x), j = 1, \ldots, m_i\}$ be any orthonormal basis of V_i. The matrices

$$E_i(x,y) = \frac{1}{|X|} \sum_{j=1}^{m_i} v_{ij}(x) v_{ij}(y), \quad i = 0, 1, \ldots, D, \tag{1.3}$$

do not depend on the choice of the bases of V_i, possess the properties

$$E_i E_j = E_i \delta_{ij}, \quad E_0 = \frac{1}{|X|} J, \quad \sum_{i=0}^{D} E_i = I, \tag{1.4}$$

and hence form the basis of irreducible idempotents of $\mathcal{A}$. It follows that there exist two non-degenerate matrices $P = (P_{ij})$ and $Q = (Q_{ij})$ of order $D + 1$ such that

$$A_j = \sum_{i=0}^{D} P_{ij} E_i, \quad j = 0, 1, \ldots, D, \tag{1.5}$$

$$E_j = \frac{1}{|X|} \sum_{i=0}^{D} Q_{ij} A_i, \quad j = 0, 1, \ldots, D. \tag{1.6}$$

(1.3)-(1.5) show that the column space of E_i is an eigenspace of each A_j, and the corresponding eigenvalue P_{ij} has the *multiplicity* $m_i = \text{rank } E_i = tr\ E_i$. In particular, by (1.1), (1.4)-(1.5) P_{0i} is equal to the valency $v_i = p^0_{ii}$, and by (1.3) and (1.6) $Q_{0i} = m_i$. From (1.5) and (1.6) it follows that

$$PQ = QP = \frac{1}{|X|} I \tag{1.7}$$

where I here is the unit matrix of order $D + 1$. Considering $tr\ (A_j E_i)$ and using that $tr\ (A_i A_j) = v_i |X| \delta_{ij}$ by (1.1) and (1.2), we get also that

$$P_{ij} m_i = Q_{ji} v_j. \tag{1.8}$$

It is clear that an association scheme is a metric space with distance $d(x,y)$ when for this function the triangle inequality holds. Delsarte proved [6] that it holds if there exists polynomials $p_j(\sigma)$ of degree $j, j = 1, \ldots, D$, of a real variable σ such that $A_j = p_j(A_1)$ or, other words (see (1.5)),

$$P_{ij} = p_j(P_{i1}), \quad i = 0, 1, \ldots, D \tag{1.9}$$

Such an association scheme is called *P-polynomial* or *metric.*

There is another description of metric association schemes in terms of graphs. The vertex set X of any undirected graph G can be considered as a metric space with metric $d_G(x,y)$ equal to the number of edges in the shortest path from x to y. An undirected connected graph G with the vertex set X is called *distance-regular* if for any $x,y \in X$ the number of vertices z such that $d_G(x,z) = 1, d_G(y,z) = d_G(x,y) - 1$ and the number of vertices z such that $d_G(x,z) = 1, d_G(y,z) = d_G(x,y) + 1$ depend on $d_G(x,y)$ only Delsarte [6] proved that for any distance-regular graph G with vertex set $X, \{X, d_G(x,y)\}$ is a metric association scheme, and for any metric association scheme $\{X, d(x,y)\}$ the graph G with the vertex set X and the adjacency matrix A_1 is a distance-regular graph, and $d(x,y) = d_G(x,y)$. Thus, there is one-to-one correspondence between metric association schemes with D classes and distance-regular graphs of diameter D.

An association scheme $\{X, d(x,y)\}$ with D classes is called *Q-polynomial,* or *cometric,* if there exist polynomials $q_j(\sigma)$ of degree $j, j = 0,1,\ldots,D$, of a real variable σ such that

$$Q_{ij} = q_j(Q_{i1}), \quad i = 0,1,\ldots,D. \tag{1.10}$$

Hereafter we consider P- and Q-polynomial association schemes (or Q-polynomial distance-regular graphs [4]) which are refered to as *polynomial association schemes.* It is known that Q_{i1} (and P_{i1}) are different for different $i, i = 0,1,\ldots,D$. We introduce an additional restriction that they decrease, which is fulfilled for many polynomial association schemes. Let $\sigma_Q(z)$ and $\sigma_P(z)$ be increasing functions in a real variable z (the *substitutions*) such that for any $i = 0,1,\ldots,D$,

$$\sigma_Q(i) = \frac{m_1 - Q_{i1}}{m_1 - Q_{D1}}, \quad \sigma_P(i) = \frac{v_1 - P_{i1}}{v_1 - P_{D1}}$$

By the construction and the assumption

$$\sigma_Q(0) = 0 \le \sigma_Q(i) \le \sigma_Q(D) = 1, \ \sigma_P(0) = 0 \le \sigma_P(i) \le \sigma_P(D) = 1. \tag{1.11}$$

The following results are well known [5-8]. For the Hamming space $H(n,q)$:

$$\begin{aligned} & D = n \\ v_i \quad & = m_i = \binom{n}{i}(q-1)^i, \quad i = 0,1,\ldots,n, \end{aligned}$$

$$Q_{ik} \quad = P_{ik} = K_k^n(i), \qquad\qquad i,k = 0,1,\ldots,n,$$

where $K_k^n(z) = \sum_{j=0}^{k}(-1)^j(q-1)^{k-j}\binom{z}{j}\binom{n-z}{k-j}$ is the Krawtchouk polynomial of degree k, in particular,

$$Q_{i1} = P_{i1} = (q-1)n - qi$$

and hence $H(n,q)$ is a polynomial association scheme with

$$\sigma_Q(z) = \sigma_P(z) = \frac{z}{n}.$$

For the Johnson space $J(n,w)$ with $1 \le w \le n/2$:

$$\begin{aligned} & D = w \\ v_i \quad & = \sum_{j=0}^{i}\binom{w}{j}\binom{n-w}{j}, \quad i = 0,1,\ldots,w \end{aligned}$$

$$m_i \quad = \binom{n}{i} - \binom{n}{i-1}, \qquad i = 1,\ldots,w \quad (m_0 = 1),$$

$$Q_{ik} \quad = m_k\sum_{j=0}^{k}(-1)^j\frac{\binom{k}{j}\binom{n+1-k}{j}}{\binom{w}{j}\binom{n-w}{j}}\binom{i}{j},$$

$$P_{ik} \quad = \sum_{j=0}^{k}(-1)^{k-j}\binom{w-j}{k-j}\binom{w-i}{j}\binom{n-w+j-i}{j},$$

in particular,

$$\begin{aligned} Q_{i1} \quad & = \quad n\left(1 - \frac{ni}{w(n-w)}\right), \\ P_{i1} \quad & = \quad w(n-w) - i(n+1-i) \end{aligned}$$

and hence $J(n,w)$ is a polynomial association scheme with

$$\sigma_Q(z) = \frac{z}{w}, \quad \sigma_P(z) = \frac{z(n+1-z)}{w(n+1-w)}.$$

Now we introduce systems $\{Q_i(z)\}$ and $\{P_i(z)\}$ of polynomials in a real z, $0 \le z \le 1$, which are obtained from polynomials (1.10) and (1.09) by change the variables as follows

$$\begin{aligned} m_j Q_j(z) &= q_j(z(Q_{D1} - m_1) + m_1), \\ v_j P_j(z) &= p_j(z(P_{D1} - v_1) + v_1), \end{aligned}$$

and hence for any $i, j = 0, 1, \ldots, D$,

$$m_j Q_j(\sigma_Q(i)) = Q_{ij}, \quad v_j P_j(\sigma_P(i)) = P_{ij}. \tag{1.12}$$

By (1.5)-(1.12) we have the following equalities

$$m_i \sum_{d=0}^{D} Q_i(\sigma_Q(d)) Q_j(\sigma_Q(d)) v_d = \delta_{ij}|X|, \quad Q_i(0) = 1, \tag{1.13}$$

$$v_i \sum_{d=0}^{D} P_i(\sigma_P(d)) P_j(\sigma_P(d)) m_d = \delta_{ij}|X|, \quad P_i(0) = 1, \tag{1.14}$$

$$Q_i(\sigma_Q(d)) = P_d(\sigma_P(i)). \tag{1.15}$$

Furthermore from (1.3), (1.6) and (1.12) it follows that

$$Q_i(\sigma_Q(d(x,y))) = \frac{1}{m_i} \sum_{j=1}^{m_i} v_{ij}(x) v_{ij}(y). \tag{1.16}$$

Notice also the following formulae for coefficients of expansions of an arbitrary polynomial $f(z) = \sum_{i=0}^{D} f_i(Q) Q_i(z) = \sum_{i=0}^{D} f_i(P) P_i(z)$:

$$f_i(Q) = \frac{m_i}{|X|} \sum_{d=0}^{D} f(\sigma_Q(d)) Q_i(\sigma_Q(d)) v_d, \tag{1.17}$$

$$f_i(P) = \frac{v_i}{|X|} \sum_{d=0}^{D} f(\sigma_P(d)) P_i(\sigma_P(d)) m_d. \tag{1.18}$$

In particular,

$$f_0(Q) = \frac{1}{|X|}\sum_{d=0}^{D} f(\sigma_Q(d))v_d \quad ; \quad f_0(P) = \frac{1}{|X|}\sum_{d=0}^{D} f(\sigma_P(d))m_d. \qquad (1.19)$$

Below we shall also use the following equality

$$P_{ki}P_{kj} = \sum_{d=0}^{D} p_{ij}^{d} P_{kd} \qquad (1.20)$$

which follows from (1.2), (1.4) and (1.5).

2 Parameters of codes in polynomial association schemes

We fix a code C in a polynomial association scheme X of diameter D (or with D classes). For any point $x \in X$ we consider vector

$$\mathbf{B}(x) = (B_0(x), B_1(x), \ldots, B_D(x)) \qquad (2.1)$$

where

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

which is called the *outer distribution* of C.

The vector

$$\mathbf{B} = \frac{1}{|C|}\sum_{x \in C} \mathbf{B}(x) = (B_0, B_1, \ldots, B_D) \qquad (2.2)$$

is called the *inner distribution* of C. A code C is referred to as *regular* if $\mathbf{B}(x) = \mathbf{B}(y)$ for any $x, y \in C$ (and hence $\mathbf{B}(x) = \mathbf{B}$ for any $x \in C$) and referred to as *completely regular* if $\mathbf{B}(x) = \mathbf{B}(y)$ when $d(x,C) = d(y,C)$ (here $d(x,C)$ is the minimum distance between x and points of C).

For any vector $\mathbf{a} = (a_0, a_1, \ldots, a_D)$ such that not all $a_1, \ldots, a_D$ are equal to 0 (in particular, for $\mathbf{a} = \mathbf{B}$ and $\mathbf{a} = \mathbf{B}(x)$) we introduce the following

parameters (cf. [5]) :

$$\begin{aligned} d(\mathbf{a}) &= \min\{i : i = 1, \ldots, D, \quad a_i \neq 0\}, \\ s(\mathbf{a}) &= |\{i : i = 1, \ldots, D, a_i \neq 0\}|, \\ \alpha(\mathbf{a}) &= \begin{cases} 0 & \text{if } a_0 = 0, \\ 1 & \text{otherwise,} \end{cases} \\ \beta(\mathbf{a}) &= \begin{cases} 0 & \text{if } a_D = 0, \\ 1 & \text{otherwise,} \end{cases} \end{aligned}$$

Values $d(\mathbf{a}), s(\mathbf{a}), \beta(\mathbf{a})$ for the vector $\mathbf{a} = \mathbf{B}$ have a significant sense for a code C. They are denoted by $d(C), s(C), \beta(C)$ and characterize the *minimal distance*, the *number of* (non-zero) *distances* and the *diametrality* of a code C (that is, whether or not the diameter of C coincides with the diameter of the whole space X). These values for the vector $\mathbf{a} = \mathbf{B}(x)$ have a similar sense and are denoted by $d(x, C), s(x, C), \beta(x, C)$ ($d(\mathbf{B}(x))$ is really equal to $d(x, C)$). The values $\alpha(\mathbf{a})$ have an auxiliary character. They are introduced to investigate simultaneously both cases because

$$\alpha(\mathbf{B}(x)) = \begin{cases} 1 & \text{if } x \in C, \\ 0 & \text{if } x \notin C. \end{cases} \tag{2.3}$$

Now for any vector $\mathbf{a} = (a_0, a_1, \ldots, a_D)$ we consider a vector $\mathbf{a}' = (a'_0, a'_1, \ldots, a'_D)$ defined by

$$a'_i = m_i \sum_{d=0}^{D} a_d Q_i(\sigma_Q(d)), \quad i = 0, 1, \ldots, D. \tag{2.4}$$

The vector $\mathbf{a}'$ is called by the *MacWilliams transform* of $\mathbf{a}$ [17], and allow us to determine dual parameters $d'(\mathbf{a}) = d(\mathbf{a}'), s'(\mathbf{a}) = s(\mathbf{a}'), \alpha'(\mathbf{a}) = \alpha(\mathbf{a}'), \beta'(\mathbf{a}) = \beta(\mathbf{a}')$ of the vector $\mathbf{a}$. In particular, parameters $d'(\mathbf{a}), s'(\mathbf{a}), \beta'(\mathbf{a})$ for the vector $\mathbf{a} = \mathbf{B}$ have a significant sense for a code C as well and denoted by $d'(C), s'(C), \beta'(C)$. The value $d'(C)$ is called the *dual distance*. If $t(C)$ is the *maximum strength of design* formed by C, that is, the maximum integer t such that

$$\sum_{x,y \in C} Q_i(\sigma_Q(d(x, y))) = 0 \quad \text{for } i = 1, \ldots, t, \tag{2.5}$$

then from (2.4) it follows that $d'(C) = t(C) + 1$. The parameters $d'(\mathbf{a}), s'(\mathbf{a}), \beta'(\mathbf{a})$ for $\mathbf{a} = \mathbf{B}(x)$ we denote $d'(x, C), s'(x, C), \beta'(x, C)$ respectively. Notice that $a'_0 = |C|$ and hence

$$\alpha'(\mathbf{a}) = 1 \quad \text{for } \mathbf{a} = \mathbf{B} \text{ and } \mathbf{a} = \mathbf{B}(x) \text{ for each } x \in X. \tag{2.6}$$

A polynomial $f(z)$ is called *annihilating* or *dual-annihilating* for $\mathbf{a} = (a_0, a_1, \ldots, a_D)$ (and for a code C if $\mathbf{a} = \mathbf{B}$) if respectively

$$a_i f(\sigma_Q(i)) = 0, \quad i = 1, \ldots, D, \tag{2.7}$$
$$a'_i f(\sigma_P(i)) = 0, \quad i = 1, \ldots, D. \tag{2.8}$$

Annihilating and dual-annihilating polynomials for $\mathbf{a}$ of minimum degree (that is, $s(\mathbf{a})$ and $s'(\mathbf{a})$) are called respectively *minimal* and *dual-minimal.*

The following two theorems follow respectively from (1.13)-(1.15) and (2.4).

Theorem 2.1 *For any vector* $\mathbf{a} = (a_0, a_1, \ldots, a_D)$,

$$a_i = \frac{v_i}{|X|} \sum_{d=0}^{D} a'_d P_i(\sigma_P(d)), \quad i = 0, 1, \ldots, D. \tag{2.9}$$

Theorem 2.2 *For any vector* $\mathbf{a} = (a_0, a_1, \ldots, a_D)$ *and any polynomial* $f(z) = \sum_{i=0}^{D} f_i(Q) Q_i(z) = \sum_{i=0}^{D} f_i(P) P_i(z)$,

$$\sum_{i=0}^{D} a_i f(\sigma_Q(i)) = \sum_{j=0}^{D} a'_j \frac{f_j(Q)}{m_j}, \tag{2.10}$$

$$\sum_{i=0}^{D} a_i \frac{f_i(P)}{v_i} = \frac{1}{|X|} \sum_{j=0}^{D} a'_j f(\sigma_P(j)). \tag{2.11}$$

Thus we introduced for a code C six parameters $d(C), s(C), \beta(C), d'(C), s'(C), \beta'(C)$. One more parameter, the *covering radius* $\rho(C)$of a code C, is defined as follows :

$$\rho(C) = \max_{x \in X} d(x, C). \tag{2.12}$$

We know also that it is the maximum $d(\mathbf{a})$ over all $\mathbf{a} = \mathbf{B}(x), x \in X$. A code C is called the *uniformly packed* [2] if there exist real numbers $\alpha_0, \alpha_1, \ldots, \alpha_{\rho(C)}$ such that

$$\sum_{i=0}^{\rho(C)} \alpha_i B_i(x) = 1 \quad \text{for any } x \in C. \tag{2.13}$$

In the next section we prove some inequalities for the parameters. The main tool is to use equalities (2.10) and (2.11) for annihilating and dual-annihilating polynomials and also to use the following adjacent systems of orthogonal polynomials.

For an arbitrary $a \in \{0,1\}$ and $b \in \{0,1\}$ we consider polynomials $Q_j^{a,b}(z)$ and $P_j^{a,b}(z)$ in a real z of degree $j, j = 0, 1, \ldots, D - \delta_{a,1} - \delta_{b,1}$, which are determined up to a constant factor by the following orthogonality relations :

$$\sum_{d=0}^{D} Q_i^{a,b}(\sigma_Q(d)) Q_j^{a,b}(\sigma_Q(d))(\sigma_Q(d))^a (1-\sigma_Q(d))^b v_d = 0, \quad i \neq j, \tag{2.14}$$

$$\sum_{d=0}^{D} P_i^{a,b}(\sigma_P(d)) P_j^{a,b}(\sigma_P(d))(\sigma_P(d))^a (1-\sigma_P(d))^b m_d = 0, \quad i \neq j. \tag{2.15}$$

Let $z_j^{a,b}(Q)$ and $z_j^{a,b}(P)$ be the smallest roots of polynomials $Q_j^{a,b}(z)$ and $P_j^{a,b}(z)$ respectively. Using that $\sigma_Q(z)$ and $\sigma_P(z)$ increase we can determine values $d_j^{a,b}(Q)$ and $d_j^{a,b}(P)$ as follows

$$\sigma_Q(d_j^{a,b}(Q)) = z_j^{a,b}(Q), \quad \sigma_P(d_j^{a,b}(P)) = z_j^{a,b}(P). \tag{2.16}$$

In particular, for the Hamming space $H(n,q), d_k^{0,0}(Q) = d_k^{0,0}(P)$ equals to the smallest root $d_k(n)$ of the Krawtchouk polynomial

$$K_k^n(z)\left(d_1(n) = \frac{q-1}{q}n, d_2(n) = \frac{2(q-1)n - q + 2 - \sqrt{4(q-1)n + (q-1)^2}}{2q}\right)$$

and (see [16])

$$d_k^{a,b}(Q) = d_k^{a,b}(P) = d_k(n-a-b) + a.$$

Apply these orthogonality conditions to find the free coefficient $f_0(Q)$ of the polynomial

$$f(z) = z^a(1-z)^b \frac{(Q_j^{a,b}(z))^2}{z - z_j^{a,b}(Q)}. \tag{2.17}$$

Using (1.19) and the fact that by (2.14) $Q_j^{a,b}(z)$ is orthogonal with respect to $(\sigma_Q(d))^a(1-\sigma_Q(d))^b v_d$ to any polynomial of degree at most $j-1$, we obtain

$$f_0(Q) = \frac{1}{|X|}\sum_{d=0}^{D} f(\sigma_Q(d))v_d = 0. \tag{2.18}$$

3 Inequalities for code parameters based on annihilating polynomials

Now we obtain a number of inequalities for parameters of an arbitrary code C using (2.10) and (2.11) for annihilating and dual-annihilating polynomials for $\mathbf{a} = \mathbf{B}$ and $\mathbf{a} = \mathbf{B}(x)$. We take into account that by (2.2), (2.4) and (1.16)

$$B_i' = \frac{m_i}{|C|}\sum_{x,y\in C} Q_i(\sigma(d(x,y))) = \frac{1}{|C|}\sum_{j=1}^{m_i}\left(\sum_{x\in C} v_{ij}(x)\right)^2. \tag{3.1}$$

It follows that the vector $\mathbf{B}'$ is non-negative (that is, it consists of non-negative coordinates). Furthermore by (1.16), (2.1) and (2.4) for the vector $\mathbf{a} = \mathbf{B}(x)$ we have

$$B_i'(x) = m_i\sum_{j=1}^{m_i} v_{ij}(x)\sum_{y\in C} v_{ij}(y)$$

and hence

$$B_i' = 0 \quad \text{implies that } B_i'(x) = 0 \text{ for any } x \in X. \tag{3.2}$$

Notice also that

$$B_i = 0 \quad \text{implies that } B_i(x) = 0 \text{ for any } x \in C. \tag{3.3}$$

Theorem 3.1 *For any code C in a polynomial association scheme of diameter D the following inequalities hold :*

1. $d(C) + d'(C) \le D + 2$,
2. $d'(C) \le 2s(C) - \beta(C) + 1$,
3. $d(C) \le 2s'(C) - \beta'(C) + 1$,

4. *If* $d'(C) \geq 2k - \sigma + 1$ *where* k *is an integer and* $\sigma \in \{0,1\}$, *then*

$$d(C) \leq d^{1,\sigma}_{k-\sigma}(Q)$$

with equality if and only if $k = s(C), \sigma = \beta(C)$ *and* $(1-z)^\sigma Q^{1,\sigma}_{k-\sigma}(z)$ *is minimal for* C.

5. *If* $d(C) \geq 2k - \sigma + 1$ *where* k *is an integer and* $\sigma \in \{0,1\}$, *then*

$$d'(C) \leq d^{1,\sigma}_{k-\sigma}(P)$$

with equality if and only if $k = s'(C), \sigma = \beta'(C)$ *and* $(1-z)^\sigma P^{1,\sigma}_{k-\sigma}(z)$ *is dual-minimal for* C.

Remark 3.1 *The first inequality of Theorem seems to be new although it is well known for Hamming and Johnson spaces and is attained for MDS-codes and Steiner systems respectively [17]. The second and third inequalities improve the corresponding Delsarte's results when* $\beta(C) = 1$ *and* $\beta'(C) = 1$ *and are attained only for tight designs and perfect codes respectively [6, 17, 13-16]. The fourth inequality follows from the author's work [12-13] as it was noticed in [9], and is attained again for the tight designs. The last inequality seems to be new and is attained only for perfect codes. It was proved in [16] for the case of the Hamming space.*

A proof of Theorem based on some auxiliary statements on vectors $\mathbf{a} = (a_0, a_1, \ldots, a_D)$.

Lemma 3.1 *Let* $g(z)$ *be annihilating for* $\mathbf{a}, \alpha'(\mathbf{a}) = 1$ *and* $g(\sigma_Q(i)) \geq 0$ *for* $i = 1, 2, \ldots, D$. *Then*

$$d'(\mathbf{a}) \leq \deg g(z) + \alpha(\mathbf{a}).$$

Proof. One can assume that $h = \deg g + \alpha(\mathbf{a}) \leq D$ because otherwise the statement is trivial. Since $a'_0 \neq 0$ and for the annihilating polynomial $f(z) = z^{\alpha(\mathbf{a})} g(z)$ of degree at most D it holds $f_0(Q) = \dfrac{1}{|X|} \sum\limits_{d=0}^{D} f(\sigma_Q(d)) v_d > 0$ we get from (2.10) that

$$\sum_{j=1}^{h} a'_j \frac{f_j(Q)}{m_j} \neq 0.$$

This completes the proof, since not all $a'_j, j = 1, \ldots, h$ are equal to zero, and hence $d'(\mathbf{a}) \leq h$.

Corollary 3.1 *If* $\alpha'(\mathbf{a}) = 1$ *then* $d'(\mathbf{a}) + d(\mathbf{a}) \le D + 1 + \alpha(\mathbf{a})$.

Proof. Use Lemma 3.1 for the polynomial $g(z) = \prod_{i=d(\mathbf{a})}^{D} (\sigma_Q(i) - z)$ satisfying the required properties.

Corollary 3.2 *If* $\alpha'(\mathbf{a}) = 1$ *then* $d'(\mathbf{a}) \le 2s(\mathbf{a}) + \alpha(\mathbf{a}) - \beta(\mathbf{a})$.

Proof. Use Lemma 3.1 for the polynomial $g(z) = (f(z))^2/(1-z)^{\beta(a)}$, where $f(z)$ is minimal for $\mathbf{a}$, satisfying the required properties as well.

Lemma 3.2 *Let* $\mathbf{a}$ *be non-negative,* $\alpha'(\mathbf{a}) = 1$ *and* $d'(\mathbf{a}) \ge 2k - \sigma + \alpha(\mathbf{a})$ *where* k *is an integer and* $\sigma \in \{0, 1\}$. *Then* $d(\mathbf{a}) \le d_{k-\sigma}^{\alpha(\mathbf{a}),\sigma}(Q)$ *with equality if and only if* $k = s(\mathbf{a}), \sigma = \beta(\mathbf{a})$ *and* $(1-z)^{\beta(\mathbf{a})} Q_{s(\mathbf{a})-\beta(\mathbf{a})}^{\alpha(\mathbf{a}),\beta(\mathbf{a})}(z)$ *is minimal for* $\mathbf{a}$.

Proof. Consider the polynomial $f(z) = z^{\alpha(\mathbf{a})}(1-z)^{\sigma} \dfrac{(Q_{k-\sigma}^{\alpha(\mathbf{a}),\sigma}(z))^2}{z - z_{k-\sigma}^{\alpha(\mathbf{a}),\sigma}(Q)}$ of degree $h = 2k - \sigma + \alpha(\mathbf{a}) - 1$ and notice that $f_0(Q) = 0$ by (2.18). Using (2.10) we get

$$\sum_{i=1}^{D} a_i f(\sigma_Q(i)) = 0. \tag{3.4}$$

By Corollary 3.2 $\quad 2k - \sigma + \alpha(\mathbf{a}) \le d'(\mathbf{a}) \le 2s(\mathbf{a}) + \alpha(\mathbf{a}) - \beta(\mathbf{a})$ and hence $s(\mathbf{a}) \ge k$. All $a_i, i = 1, \ldots, D$, are non-negative and exactly $s(\mathbf{a})$ among them are positive. Since $f(\sigma_Q(i)) \ge 0$ for $i \ge d_{k-\sigma}^{\alpha(\mathbf{a}),\sigma}$ it follows that (3.4) implies $d(\mathbf{a}) \le d_{k-\sigma}^{\alpha(\mathbf{a}),\sigma}$ with equality if and only if $k = s(\mathbf{a})$, $\sigma = \beta(\mathbf{a})$ and the polynomial $(1-z)^{\beta(\mathbf{a})} Q_{s(\mathbf{a})-\beta(\mathbf{a})}^{\alpha(\mathbf{a}),\beta(\mathbf{a})}(z)$ is minimal for $\mathbf{a}$.

Remark 3.2 *By Theorems 2.1 and 2.2, Lemmas 3.1, 3.2 and Corollaries 3.1, 3.2 will be valid if we replace in their formulations* $\mathbf{a}$ *by* $\mathbf{a}'$, *and* Q *by* P.

Proof of Theorem 3.1. We can use Corollaries 3.1, 3.2 and Lemma 3.2 for the vector $\mathbf{a} = \mathbf{B}$ (see (2.2)) for which $\alpha(\mathbf{a}) = 1$ and $\alpha'(\mathbf{a}) = 1$ by (2.6). It gives the statements 1, 2 and 4. The statements 3 and 5 follow from dual analogues of Corollary 3.2 and Lemma 3.2 (see Remark 3.2).

For any vector $\mathbf{a} = \mathbf{B}(x)$ where $x \notin C$ according to (2.3) and (2.6) we have $\alpha'(\mathbf{a}) = 1, \alpha(\mathbf{a}) = 0$. Therefore we can use only Corollaries 3.1, 3.2 and Lemma 3.2 and obtain the following results for an arbitrary point $x \in X$ and an arbitrary code C :

1. $d(x,C) + d'(x,C) \leq D+2$,

2. $d'(x,C) \leq 2s'(x,C)+1 - \beta'(x,C)$,

3. If $d'(x,C) \geq 2k - \sigma$ where k is an integer and $\sigma \in \{0,1\}$ then

$$d(x,C) \leq d^{0,\sigma}_{k-\sigma}(Q)$$

with equality if and only if $k = s(x,C), \sigma = \beta(x,C)$ and $(1-z)^\sigma Q^{0,\sigma}_{k-\sigma}(z)$ is minimal for $\mathbf{B}(x)$.

Since by (3.2) $d'(C) \leq d'(x,C)$ for any $x \in X$, the last statement gives rise to the following

Theorem 3.2 *If $d'(C) \geq 2k - \sigma$ where k is an integer and $\sigma \in \{0,1\}$ then*

$$\rho(C) \leq d^{0,\sigma}_{k-\sigma}(Q)$$

with equality if and only if there exists a point $x \in X$ such that $(1-z)^\sigma Q^{0,\sigma}_{k-\sigma}(z)$ is minimal for $\mathbf{B}(x)$.

The inequality of Theorem 3.2 for the Hamming space belongs to Tietäväinen [18-20]. For arbitrary polynomial association schemes it was proven together with necessary and sufficient conditions of its attainability in [9]. In particular, it is attained for all binary tight designs of even strength, for example, for tight 6-design formed by the Golay [23, 11, 8] code.

We consider $B_i(x)$ (see (2.1)) as an entry of a matrix of size $|X| \times (D+1)$ with rows $\mathbf{B}(x)$ numerated by $x \in X$ and columns $\mathbf{B}_i$ numerated by i, $i = 0, 1, \ldots, D$.

Theorem 3.3 *For any code C there exists $x \in X$ such that $d(x,C) \leq s'(C)$, and*

$$\rho(C) \leq s'(C) \tag{3.5}$$

with equality if and only if C is uniformly packed. The column $\mathbf{B}_{s'}$ where $s' = s'(C)$ is a linear combination of columns $\mathbf{B}_0, \ldots, \mathbf{B}_{s'-1}$ and of column from all units. Any column $\mathbf{B}_i, s' < i \leq D$, is a linear combination of preceding columns, any row $\mathbf{B}(x)$ is determined uniquely by its s' coordinates, the columns $\mathbf{B}_0, \ldots, \mathbf{B}_{s'}$ are linearly independent.

Proof. Let $f(z)$ be a dual-minimal polynomial of degree $s' = s'(C)$ for C such that $f(0) = 1$. Using (3.2) and (2.11) for $\mathbf{a} = \mathbf{B}(x)$ we have for any $x \in X$

$$\frac{|X|}{|C|} \sum_{i=0}^{s'} B_i(x) \frac{f_i(P)}{v_i} = 1 \quad \text{where } f_{s'}(P) \neq 0. \tag{3.6}$$

This proves two first statements of Theorem except that $\rho(C) = s'(C)$ for an uniformly packed code. The statement on $\mathbf{B}_i$, $s' < i \leq n$, is obtained by analogy using dual-annihilating polynomial $z^{i-s'} f(z)$ of degree i. Therefore any row $\mathbf{B}(x)$ is determined uniquely by its s' coordinates. The linear independence of the first $s' + 1$ columns is a consequence of the Delsarte equality

$$\sum_{x \in X} B_i(x) B_j(x) = |C| \sum_{d=0}^{D} B_d p_{ij}^d = \frac{|C|}{|X|} \sum_{k=0}^{D} B'_k P_{ki} P_{kj}$$

which follows from definitions of $B_i(x), B_d, p_{ij}^d$ and from (2.9), (1.12), (1.20) and shows that rank of the matrix under consideration equals $s' + 1$. Since $\mathbf{B}_{s'}$ is not a linear combination of preceding columns from (2.13) and (3.6) it follows that for any uniformly packed code the inequality (3.5) cannot be strong.

Theorem 3.3 belongs to Delsarte [6] except for the necessary and sufficient conditions of the equality in (3.5) which were obtained in [3]. Uniformly packed code were investigated in [2, 10, 3].

In conclusion we derive from Theorem 3.3 one more Delsarte's result.

Corollary 3.3 *A code C is completely regular if $d(C) \geq 2s'(C) - 1$.*

Proof. For any $x \in X$ it holds $\sum_{i=0}^{s'-1} B_i(x) \leq 1$ (where $s' = s'(C)$), because otherwise, by the triangle axiom, there exist two code points at distance at most $2s' - 2$. Furthermore by Theorem 3.3 any row $\mathbf{B}(x)$ is determined uniquely by its first s' coordinates. This completes the proof.

References

[1] E. Bannai, T. Ito, "Algebraic combinatorics. I. Association schemes", *Benjamin/Cummings*, London, 1984.

[2] L.A. Bassalygo, G.V. Zaitsev, V.A. Zinoviev, "On uniformly packed codes", *Problems of Inform. Transmission*, Vol. 10 (1974), **n. 1**, pp. 9–14.

[3] L.A. Bassalygo, V.A. Zinoviev, "Remark on uniformly packed codes", *Problems of Inform. Transmission*, Vol. 13 (1977), **n. 3**, pp. 22–25.

[4] A.E. Brouwer, A.M. Cohen, A. Neumaier, "Distance-regular graphs", *Springer Verlag*, Berlin, 1989.

[5] Ph. Delsarte, "Four fundamental parameters of a code and their combinatorial significance", *Info. and Control* **23** (1973), 407–438.

[6] Ph. Delsarte, "An algebraic approach to the association schemes of coding theory", *Philips Res. Reports, Suppl.* **10** (1973).

[7] Ph. Delsarte, "Associations schemes and t-design in regular semilattices", *J. Combin. Th. (A)* **20** (1976), 230–273.

[8] Ph. Delsarte, "Hahn poliominals, discrete harmonics and t-designs", *SIAM J. Appl. Math.* **34** (1978), 157–166.

[9] G. Fazekas, V.I. Levenshtein, "On upper bounds for code distance and covering radius of designs in polynomial metric spaces", *Fifth Joint Soviet-Swedish Intern. Workshop on Information Theory*, (1990), Moscow, 65–68. Full text was submitted to *J. Comb. Th. (A)*.

[10] J.M. Goethals, H.C.A. van Tilborg, "Uniformly packed codes", *Philips Res. Reports*, **30, 1** (1975), 9–36.

[11] G.A. Katabiansky, V.I. Levenshtein, "Bounds for packings on a sphere and in space", *Problems of Information Transmission* **14 : (1)** (1978), 1–7.

[12] V.I. Levenshtein, "On choosing polynomials to obtain bounds in packing problems", *In : Proc. Seventh All-Union Conf. on Coding Theory and Information Transmission*, **Part II**, Moscow, Vilnius, (1978), pp. 103–108 (in Russian).

[13] V.I. Levenshtein, "Bounds for packings of metric spaces and some their applications", *In : Probl. Cybern.* **40**, Nauka, Moscow, (1983), pp. 43-110 (in Russian).

[14] V.I. Levenshtein, "Designs as maximum codes in polynomial metric spaces", *Acta Applicandae Mathematicae* **29** (1992), 1–82.

[15] V.I. Levenshtein, "Packing and decomposition problems for polynomial association schemes", *Europ. J. Combinatorics* **14** (1993), 461–477.

[16] V.I. Levenshtein, "Krawtchouk polynomials and universal bounds for codes and designs in Hamming spaces", submitted to *IEEE Trans. on Information Theory.*

[17] F.J. MacWilliams, N.J.A. Sloane, "The theory of error-correcting codes", *North Holland*, Amsterdam, 1977.

[18] A. Tietäväinen, "Covering radius problems and character sums", *Fourth Joint Swedish-Soviet International Workshop on Information Theory*, (1989), Gotland, Sweden, 196–198.

[19] A. Tietäväinen, "An upper bound on the covering radius of codes as a function of the dual distance", *IEEE Trans. Inform. Theory* **IT-36 (6)** (1990), 1472–1474.

[20] A. Tietäväinen, "Covering radius and dual distance", *Designs, Codes and Cryptography* **1** (1991), 31–46.

Unité de recherche INRIA Rocquencourt
Domaine de Voluceau - Rocquencourt - B.P. 105 - 78153 Le Chesnay Cedex (France)

Unité de recherche INRIA Lorraine - Technopôle de Nancy-Brabois - Campus scientifique
615, rue du Jardin Botanique - B.P. 101 - 54602 Villers lès Nancy Cedex (France)
Unité de recherche INRIA Rennes - IRISA, Campus universitaire de Beaulieu 35042 Rennes Cedex (France)
Unité de recherche INRIA Rhône-Alpes 46, avenue Félix Viallet - 38031 Grenoble Cedex 1 (France)
Unité de recherche INRIA Sophia Antipolis - 2004, route des Lucioles - B.P. 93 - 06902 Sophia Antipolis Cedex (France)

Éditeur
INRIA - Domaine de Voluceau - Rocquencourt - B.P. 105 - 78153 Le Chesnay Cedex (France)

ISSN 0249 - 6399