A direct approach to linear programming bounds for codes and tms-nets

Jürgen Bierbrauer
Department of Mathematical Sciences
Michigan Technological University
Houghton, Michigan 49931 (USA)

September 21, 2006

Abstract

Based on a self-contained account of the classical linear programming bounds for codes and orthogonal arrays we give a simplified description of the linear programming bounds for ordered codes, ordered orthogonal arrays (OOA) and tms-nets. The main result is a description in terms of a family of polynomials which generalize the Kravchouk polynomials of coding theory. The Plotkin bound and the sphere packing bound for ordered codes are consequences. We also derive a quadratic bound and illustrate by giving some improvements for bounds on the parameters of tms-nets.

1 Introduction

Error-correcting block codes (codes) and orthogonal arrays (OA) live in Hamming space. Virtually all known general bounds on codes and OA are based on linear programming (LP). Ordered orthogonal arrays (OOA) and tms-nets are objects of fundamental importance for quasi-Monte Carlo methods of numerical integration. They generalize OA and live in an ambient space which generalizes Hamming space. A linear programming bound for OOA and nets has been described in [6, 7]. It is based on the structure of the ambient space seen as an association scheme.

The classical theory of LP-bounds for codes and orthogonal arrays is essentially due to Delsarte (see [2, 3, 4]). In the present paper we start from a self-contained account of the basics of this theory (Section 2). One of its advantages is that it generalizes in a natural way to the case of ordered codes and ordered orthogonal arrays, thus giving a simplified approach to the results of [6, 7]. The theory is developed in Section 3. The description is in terms of a family of polynomials which generalize the Kravchouk polynomials (Definition 6). The introduction of this class of polynomials is the most important new element in the present paper.

The classical Kravchouk polynomials are best understood as polynomials of two variables, see Definition 2. One of the basic parameters of the association scheme where ordered codes and OOA are defined is its depth l. In case $l = 1$ the Hamming scheme is obtained. The generalized Kravchouk polynomials have $l + 1$ variables, see Definition 6. The LP-bound is in terms of polynomials satisfying certain conditions, see Theorems 3 and 4. Special choices for this polynomial yield generalizations of the Plotkin/ dual Plotkin bound (Section 4) and of the sphere packing/ Rao bound (Section 5). These generalized bounds are known already, see [5, 9]. An advantage of our method is that we obtain characterizations of the cases of equality (see Section 6). In the case of the sphere packing bound equality is described in terms of a generalized Lloyd polynomial (Proposition 3). This is expected to facilitate an attack on the problem of classifying the ordered codes meeting the sphere packing bound or the Rao bound with equality (perfect ordered codes). Along the way we obtain generalizations of some of the fundamental parameters of coding theory (see [3]).

As the Plotkin bound of coding theory is obtained using polynomials of degree 1 it comes as no surprise that the generalization of the Plotkin bound for OOA is derived using linear polynomials of $l + 1$ variables. In the final section we derive a new bound, using quadratic polynomials. We close with a list of parameters of tms-nets which are excluded by the quadratic bound.

The best known net parameter bounds are to be found in the MinT data base maintained by the group in Salzburg, see http://mint.sbg.ac.at and the recent paper [11].

My thanks go to Wolfgang Schmid and the department of mathematics of the University of Salzburg (Austria) for their hospitality and the support provided in the framework of the Austrian Science Foundation FWF Grant S8311-MAT. The paper was sponsored by NSA grant H982300510088.

2 The case of codes and orthogonal arrays

We start with an elementary approach to the linear programming (LP) bound on codes and orthogonal arrays. Nothing in this section is new. The reason we include it is that in this form it generalizes to the case of ordered codes and ordered OA, as will be seen in Section 3. Also, it is felt that the classical LP bound for codes and OA is best understood and taught the way we describe it in the present section.

The ambient space is the space of v-ary n-tuples $V = Z_v^n$, where Z_v denotes the integers mod v. Equip V with the Hamming metric. A v-ary code of length n is a subset $C \subseteq V$. Let $g = v^n, |C| = M$ and $\zeta \in \mathbb{C}$ a primitive v-th root of unity. The main parameters of C are its minimum distance d and its strength t. They describe the properties of C as a code and as an orthogonal array, respectively. As a tool we use the distance distribution $(A_i), i = 0, \ldots, n$ defined by

$$A_i = |\{(x, y) \mid x, y \in C, d(x, y) = i\}|/M.$$

By definition the A_i are non-negative rational numbers and the minimum distance is the smallest $i > 0$ such that $A_i > 0$. Also $\sum A_i = M$. We wish to define a transform (A'_k) of the weight distribution which satisfies the following conditions:

- $A'_k \geq 0$ for all k, and
- C is an OA of strength t if and only if $A'_1 = \cdots = A'_t = 0$.

The fact that (A'_k) is a transform of (A_i) means that we can write

$$A'_k = \frac{1}{M} \sum_i A_i K_k(i)$$

for suitable coefficients $K_k(i)$. We define as follows:

Definition 1.

$$K_k(i) = \sum_{z: wt(z)=k} \zeta^{x \cdot z},$$

where x is a vector of weight i.

Here $x \cdot z$ is the dot product. It is rather obvious that this expression is indeed independent of the choice of x.

In order to check the desired properties we use basic properties of the Fourier transform: denote by $L^2(V)$ the space of complex-valued functions $f : V \longrightarrow \mathbb{C}$, with the scalar product $\langle , \rangle$, where

$$\langle f, h \rangle = \frac{1}{g} \sum_{x \in V} f(x) \cdot \overline{h(x)}.$$

The **characters** $\phi_z \in L^2(V)$ defined by

$$\phi_z(x) = \zeta^{x \cdot z}.$$

form an orthonormal basis of the g-dimensional vector space $L^2(V)$. The **Fourier transform** $\hat{f} \in L^2(V)$ is defined by

$$f = \sum_{z \in V} \hat{f}(z) \phi_z.$$

In other words, $\hat{f}(z)$ is the coefficient of ϕ_z when $f \in L^2(V)$ is expanded with respect to this basis. Because of the orthonormality of the characters the Fourier coefficients are given by

$$\hat{f}(z) = \langle f, \phi_z \rangle = \frac{1}{g} \sum_{x \in V} f(x) \zeta^{-x \cdot z}. \tag{1}$$

Lemma 1. *Let $f \in L^2(V)$. Then the following are equivalent:*

- *f is a constant function.*
- *$\hat{f}(z) = 0$ for all $z \neq 0$.*

Proof. One direction is obvious as the sum of all powers of ζ vanishes. Assume $\hat{f}(z) = 0$ for all $z \neq 0$. These conditions describe a 1-dimensional subspace of $L^2(G)$. $\square$

Lemma 2. *Let $C \subseteq V$. Identify C with its characteristic function. Then the following are equivalent:*

- *$\hat{C}(z) = 0$ for all z such that $0 < wt(z) \leq t$.*
- *C is an orthogonal array of strength t.*

Proof. Again one direction is obvious: if C has strength t then its restriction to any set of at most t coordinates is a constant function, so the preceding lemma applies. Assume now $\hat{C}(z) = 0$ for all z such that $0 < wt(z) \leq t$. Fix a set of t coordinates and let $\lambda(x)$ be the multiplicity, with which the t-tuple $x \in Z_v^t$ occurs in the projection of C. It follows from Equation 1 that λ satisfies $\hat{\lambda}(z) = 0$ for all $0 \neq z \in Z_v^t$. Lemma 1 implies that λ is a constant function thus verifying that C has strength t. $\square$

The justification for the transform is that we can immediately express A'_k in terms of Fourier coefficients and read off the desired properties:

$$A'_k = \frac{1}{M^2} \sum_i \sum_{a,b \in C, d(a,b)=i} \sum_{z: wt(z)=k} \zeta^{(a-b)\cdot z} =$$

$$= \frac{1}{M^2} \sum_{z: wt(z)=k} (\sum_{a \in C} \zeta^{a\cdot z})(\sum_{b \in C} \zeta^{-b \cdot z}) = \frac{g^2}{M^2} \sum_{z: wt(z)=k} |\hat{C}(z)|^2,$$

where $\hat{C}(z)$ is the Fourier coefficient of C when we identify it with its characteristic function. This shows that the A'_k have the desired properties. We need a combinatorial interpretation of the $K_k(i)$:

Lemma 3. *Let $x \in V$ of weight i. Then*

$$\sum_{z \in V, wt(z)=k} \zeta^{x \cdot z} = \sum_{j=0}^{k} (-1)^j (v-1)^{k-j} \binom{i}{j} \binom{n-i}{k-j}.$$

Proof. Without restriction $x = (x_1, \ldots, x_i, 0, 0, \ldots, 0)$. Choose k coordinates $h_1, \ldots, h_k$ such that $0 < h_1 < \ldots h_j \leq i < h_{j+1} < \cdots < h_k \leq n$, let D be the set of vectors of weight k having nonzero coordinates exactly at the h_j. Then $\sum_{z \in D} \zeta^{x\cdot z} = (v-1)^{k-j}(-1)^j$. Summing over all D we get our statement. $\square$

If we interpret i as a variable X the right side of the equation in Lemma 3 describes the Kravchouk polynomial $K_k(X)$. We find it best to work with two-variable K-polynomials as follows:

Definition 2. *The two-variable degree k Kravchouk polynomial is defined by*

$$K_k(X,Y) = \sum_{j=0}^{k} (-1)^j (v-1)^{k-j} \binom{X}{j} \binom{Y}{k-j}.$$

One advantage is that it does not involve the length explicitly. The one-variable K-polynomial is obtained by substituting $Y = n - X$. The fact that $M = \sum A_i$ suggests how to generalize the K-transform in a natural way:

Definition 3. *Let*

$$\mathcal{S} = \{x = (x_i) \mid x_i \in \mathbb{R}\}$$

and $\mathcal{S}_0 \subset \mathcal{S}$ *the subspace defined by* $x_0 = 1, \sum_j x_j \neq 0$. *Define the K-transform on* $\mathcal{S}_0$ *by* $x' = (x'_k)$, *where*

$$x'_k = \sum_i x_i K_k(i) / (\sum_j x_j)$$

Lemma 4.

$$x \in \mathcal{S}_0 \longrightarrow x' \in \mathcal{S}_0$$

Proof. Observe $K_0(i) = 1$. It follows $x'_0 = 1$. Definition 1 shows $\sum_k K_k(i) = 0$ if $i > 0$, whereas $\sum_k K_k(0) = g$. This shows $\sum_k x'_k = g x_0 (\sum x_i)$. □

In order to see what happens if the K-tranform is applied twice the following orthogonality relation is needed:

Lemma 5.

$$\sum_k K_k(i) K_j(k) = g \delta_{i,j}.$$

Proof. By Definition 1 we have to fix a vector x of weight i and obtain $\sum_k K_k(i) K_j(k) = \sum_{z:wt(z)=k} \zeta^{x \cdot z} \sum_{u:wt(u)=j} \zeta^{z \cdot u} = \sum_{z,u} \zeta^{z \cdot (x+u)}$. If $i \neq j$, then $x + u \neq 0$ and the sum vanishes. If $i = j$ we can choose $u = -x$ and obtain the value g. □

A routine calculation shows that the K-transform is involutorial on $\mathcal{S}_0$. The K-transform of the weight distribution of code C is a special case.

The duality of LP-bounds will be used in the following form:

Theorem 1. *Let* A *be a real* (n, m)*-matrix,* $b = (b_1, \ldots, b_m) \geq 0$ *and* $p = (p_1, \ldots, p_n)$. *The following LP-problems form a dual pair:*

- **The primal problem:** *Unknowns* $x = (x_1, \ldots, x_m)$, *restrictions:* $x \geq 0$ *and* $Ax \leq p$, *maximize* $x \cdot b$.

- **The dual problem:** *Unknowns* $y = (y_1, \ldots, y_n)$, *restrictions* $y \geq 0$ *and* $A^t y \geq b$, *minimize* $y \cdot p$.

Let now

$$\alpha = (\alpha_0 = 1, \alpha_1 = 0, \ldots, \alpha_{r-1} = 0, \alpha_r, \ldots, \alpha_n) \in \mathcal{S}$$

for some r which also satisfies $\alpha \geq 0$ and $\alpha' \geq 0$. Consider the primal problem of Theorem 1 with unknowns $(x_r, \ldots, x_n)$, matrix $A = (-K_k(i))$ for $k = 1, \ldots, n$ and $i = r, \ldots, n$, where $p_k = K_k(0)$ and b is constant 1. Then $(\alpha_r, \ldots, \alpha_n)$ is an instance of this problem and $\sum_{j=r}^n \alpha_j$ is bounded by its maximum. Instances of the dual problem are described by $(c_1, \ldots, c_n) \geq 0$ such that $\sum_{k \geq 1} c_k K_k(i) \geq 1$, the corresponding value being $\sum_{k \geq 1} c_k K_k(0)$. This can be conveniently expressed in terms of the polynomial $p(X) = \sum_{k=0}^n c_k K_k(X)$, where $c_0 = 1$. The conditions are $c_k \geq 0$ and $p(i) \leq 0$ for $i = r, r+1, \ldots, n$. The value is $p(0) - 1$. We obtain the following form of the LP-bound:

Theorem 2. *Let $p(X)$ be a real polynomial of degree $\leq n$ which satisfies the following conditions:*

- *If $p(X)$ is expressed in terms of the Kravchouk basis: $p(X) = \sum_{k=0}^n c_k K_k(X)$, then $c_0 = 1,\ c_k \geq 0$ for all k.*
- *$p(i) \leq 0,\ i = r, r+1, \ldots n$.*

Then for every $(n+1)$-tuple $(\alpha_0, \alpha_1, \ldots, \alpha_n)$ of non-negative real numbers with non-negative Kravchouk transform, satisfying $\alpha_0 = 1, \alpha_1 = \alpha_2 = \ldots \alpha_{r-1} = 0$ we have

$$\sum_{k=0}^n \alpha_k \leq p(0).$$

Application of Theorem 2 to the weight distribution of a code C of minimum distance r shows $|C| \leq p(0)$. Application to the dual distribution (the K-transform of the weight distribution) of an OA of strength $r-1$ shows $\sum_k A'_k = g/|C| \leq p(0)$.

3 The case of ordered codes and ordered OA

One advantage of the approach used in Section 2 is that it is elementary. For example, no a priori knowledge of the K-polynomials is needed. Another advantage is that it generalizes to ordered codes and ordered OA in a natural way. We need to introduce some notation.

The ambient space is $V = V_v^{(l,n)} = (Z_v)^{ln}$ with its ordered distance at depth l. Write $x = (x_{i,j}) \in V$ where $i = 1, \ldots, n; j = 1, \ldots, l$. Call n the **length** and l the **depth** of V. There are n **blocks** indexed by $i = 1, 2, \ldots, n$. The **ordered weight** of block i of x is the maximal index j such that $x_{i,j} \neq 0$. The **ordered weight** of x is the sum of the ordered weights over all blocks. The **ordered distance** $d(x, y)$ is the ordered weight of $x - y$.

We visualize vectors $x \in V_v^{(l,n)}$ as matrices with l rows and n columns, where in each column (corresponding to a block) we read from top to bottom. Instead of this stalactite notation the reader may as well use the stalagmite version where the ordering in the blocks is from bottom to top. We use the stalactite version here. As an example $x = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \in V_2^{(4,3)}$ has weight $1+2+3 = 6$. There is the structure of a poset on the ln coordinate positions. Cell (i, j) precedes (i', j') if $i = i'$ and $j < j'$. This poset is therefore the union of n chains, each of length l. An **ideal** of a poset is a set which is closed under predecessors. By definition a subset $C \subset V_v^{(l,n)}$ is an OOA of strength t if in the projection from C to any ideal of size t each t-tuple occurs equally often.

Large part of the interest in OOA stems from the link to the **nets,** point sets in Euclidean space which were defined by Niederreiter [10] in the context of quasi-Monte Carlo methods of numerical integration. This link has been explained in many places, see for example [1]. Here we ignore Euclidean space and use the following equivalent definition:

Definition 4. *A $(t, m, n)_v$-net is a subset $C \subseteq V_v^{(l,n)}$ of size v^m which is an OOA of strength $l = m - t$.*

Denote by $k = m - t$ the strength of the net. Observe that bounds on the parameters of strength k OOA of any depth $l \leq k$ imply bounds on the parameters of nets.

More notation will be needed. For $x \in V$ denote by $\overline{x}$ the vector obtained by reading the entries in each block in the reverse order. Each $x \in V$ generates a uniquely determined ideal in an obvious way. Each ideal has a **type.** The types are partitions of numbers $\leq ln$ into at most n parts, where each part is $\leq l$. Describe such a type e as $e = (e_0, \ldots, e_l)$, where e_j is the number of times part j is used. The number being partitioned is $s(e) = \sum j e_j$ (the

size of e), the number of different parts used is $b(e) = \sum_{j=1}^{l} e_j$ (the **breadth** of e). In the example above the ideal generated by x has type $(0, 1, 1, 1, 0)$. Write $x \sim_e y$ if the ideal generated by $x - y$ has type e.

Let $g = v^{ln}$. The **type distribution** of $C \subseteq V$ is defined as

$$A_e = \frac{1}{M} |\{(x, y) \mid x, y \in C, \overline{x} \sim_e \overline{y}\}|,$$

where $M = |C|$. Recall that $e = (e_0, \ldots, e_l)$ is the type of $\overline{x} - \overline{y}$. In our generalization the types take the role of the weight. Each vector has a well-defined type. In the special case $l = 1$ type $e = (e_0, e_1)$ corresponds to weight e_1. In general $\sum_i e_i = n$.

In comparison with the code case (corresponding to $l = 1$) we replaced x by $\overline{x}$. This will be justified a little later. It is consistent as $x = \overline{x}$ in case $l = 1$. As in Section 2 the definition of the transform (A'_f) is motivated by the desire to verify the following conditions:

- $A'_f \geq 0$ for all f, and
- C is an OOA of strength t if and only if $A'_f = 0$ for all types $f \neq 0$ of size at most t. Here $f = 0$ stands for $f = (n, 0, \ldots, 0)$.

The definition is motivated by the code case:

$$A'_f = \frac{1}{M} \sum_e A_e B_f(e),$$

where the coefficients $B_f(e)$ are defined as follows (see also [6]):

Definition 5.

$$B_f(e) = \sum_{z : z \sim_f 0} \zeta^{x \cdot z},$$

where $\overline{x} \sim_e 0$.

As in the code case we need to prove that this definition is indeed independent of the choice of x. Let us assume this is the case. The same summation as in Section 2 yields

$$A'_f = \frac{g^2}{M^2} \sum_{z : z \sim_f 0} |\hat{C}(z)|^2.$$

This verifies the desired properties of the transform.

We need to analyze the formula in Definition 5 in order to justify the definition and to obtain a combinatorial interpretation of the coefficients $B_f(e)$. This is not hard. Let $\overline{X}$ be the ideal (of type e) generated by $\overline{x}$. Just as in the proof of Lemma 3 fix an ideal $Z = (z_1, \ldots, z_s)$ of type f (depth z_i in block i) and sum over all z which generate Z. The trick is to write this sum as a product, the summation taking place seperately at each entry. Assume $x_{i,j} \neq 0$ for some $j < z_i$. As all entries are permitted in this cell the inner sum corresponding to cell (i,j) vanishes. We can therefore assume this situation never occurs. Let $y_i = l - wt(\overline{x}_i)$ be the number of leading zeroes in the i-th block of x. The excluded situation is $z_i > y_i + 1$. It follows that we can restrict to z such that for each block i we have $z_i \leq y_i + 1$. If the corresponding block of x has all entries 0 (case $y_i = l$), then this restriction is empty. The inner sum corresponding to block i is $(v-1)v^{z_i-1}$ if $z_i \leq y_i$, it is $-v^{z_i-1} = -v^{y_i}$ if $z_i = y_i + 1$. The total power of v is $v^{\sum(z_i-1)}$ where the sum is over $z_i > 0$, in other words $v^{s(f)-b(f)}$. Denote by $i(Y,Z)$ the number of blocks i where $z_i = y_i + 1$. The summand corresponding to ideal Z is then

$$(-1)^{i(Y,Z)}(v-1)^{b(Z)-i(Y,Z)}v^{s(Z)-b(Z)}.$$

This has to be summed over all ideals Z of type f. Observe that the numbers y_i depend only on the type of $\overline{x}$. This shows the desired independence of the choice. The type $(t_0, t_1, \ldots, t_l)$ of (y_i) is simply given by $t_k = e_{l-k}$ for $k = 0, 1, \ldots, l$. We obtain

$$B_f(e) = v^{s(f)-b(f)} \sum_{j_l=0}^{f_l} (-1)^{j_l}(v-1)^{f_l-j_l}\binom{t_{l-1}}{j_l}\binom{t_l}{f_l-j_l} \times$$

$$\sum_{j_{l-1}=0}^{f_{l-1}} (-1)^{j_{l-1}}(v-1)^{f_{l-1}-j_{l-1}}\binom{t_{l-2}}{j_{l-1}}\binom{t_{l-1}+t_l-f_l}{f_{l-1}-j_{l-1}} \cdots \times$$

$$\sum_{j_1=0}^{f_1} (-1)^{j_1}(v-1)^{f_1-j_1}\binom{t_0}{j_1}\binom{t_1+\cdots+t_l-(f_2+\cdots+f_l)}{f_1-j_1}$$

Each of the sums on the right side is recognized as an instance of the two-variables K-polynomials of Definition 2. This is best stated by using the following family of polynomials which may be called multivariate Kravchouk polynomials. Here we see the t_k above as variables X_k. Observe that f_0 is not used here.

Definition 6.

$$K_f(X_0,\dots,X_l) = v^{s(f)-b(f)} K_{f_l}(X_{l-1},X_l)\times K_{f_{l-1}}(X_{l-2},X_{l-1}+X_l-f_l)\times\dots$$
$$\dots\times K_{f_1}(X_0,X_1+\dots+X_l-(f_2+\dots+f_l)).$$

The coefficients $B_f(e)$ are obtained by evaluation (in reverse order):

$$B_f(e) = K_f(e_l,\dots,e_1,e_0) = K_f(\overline{e}).$$

Let us check at first that everything is OK in the familiar case $l=1$. We have

$$K_{f_1}(X_0,X_1) = \sum_j (-1)^j (v-1)^{f_1-j}\binom{X_0}{j}\binom{X_1}{f_1-j}$$

With $f_1 = k, X_0 = e_1 = i, X_1 = e_0 = n-i$ this yields

$$\sum_j (-1)^j (v-1)^{k-j}\binom{i}{j}\binom{n-i}{k-j},$$

as expected.

Proposition 1.

$$\sum_f B_f(e)B_h(f) = g\delta_{e,h}$$

Proof. Simply use Definition 5.

$$\sum_f B_f(e)B_h(f) = \sum_f \sum_{z\sim_f 0}\zeta^{x\cdot z}\sum_{w\sim_h 0}\zeta^{\overline{z}\cdot w}$$

where $\overline{x}\sim_e 0$. As $\overline{z}\cdot w = z\cdot\overline{w}$ we obtain

$$\sum_{w\sim_h 0}\sum_z \zeta^{(x+\overline{w})\cdot z}.$$

The inner sum vanishes unless $x=\overline{w}$, which is possible only if $h=e$. $\square$

Definition 3 generalizes in an obvious way.

Definition 7. *Let $P_{l,n}$ be the set of all partitions of numbers $\leq ln$ with highest part $\leq l$ and with $\leq n$ parts. Consider the space of real tuples*

$$S = \{(x_e)\mid e\in P_{l,n}\}$$

and its subspace S_0 defined by $x_0 = 1, \sum_e x_e \neq 0$.

Just as in the code case the orthogonality relation Proposition 1 shows that the transformation $(x_e) \mapsto (y_f)$ where $y_f = \sum_e x_e B_f(e)/(\sum_e x_e)$, is involutorial on $\mathcal{S}_0$. Also, $\sum_f y_f = g/(\sum x_e)$. In particular $\sum A'_f = g/M$. The same argument as in the case of codes and OA, using the duality of linear programming, shows the following generalization of Theorem 2.

Theorem 3. *Let $p(X) = \sum_f c_f K_f(X)$, where $X = (X_0, \ldots, X_l)$, $f = (f_0, f_1, \ldots, f_l), \sum f_k = n$ and $c_f \geq 0$ for all f, $c_0 = 1$. Here $0 = (n, 0, \ldots, 0)$. Assume $p(\overline{e}) \leq 0$ for all e such that $\sum e_k = n, s(e) \geq r$. Then the following hold:*
For all (α_e) such that $\alpha_0 = 1$, $\alpha_e = 0$ for $0 < s(e) < r$ and $\alpha_e \geq 0$ for all e we have $\sum \alpha_e \leq p(\overline{0})$.

As a consequence the following LP-bounds are obtained which, using Definition 6, is equivalent to the LP-bound derived in [9].

Theorem 4. *Let the polynomial $p(X)$ satisfy the conditions of Theorem 3. Then the following hold:*

- *$p(\overline{0})$ is an upper bound on the size of a code in $V_v^{(l,n)}$ of minimum ordered distance r.*
- *$g/p(\overline{0})$ is a lower bound on the size of an OOA of strength $r-1$ in the same space.*

4 The Plotkin bound

Just as in the case of codes and OA the idea is to use degree 1 polynomials. Let $P_i = K_{e_i}(X_0, \ldots, X_l)$, where e_i is the i-th elementary vector. We have

$$P_i = v^{i-1} K_1(X_{i-1}, X_i + \ldots, X_l) = v^{i-1}((v-1)(X_i + \cdots + X_l) - X_{i-1}).$$

Definition 8. *Let $\lambda(X) = lX_0 + (l-1)X_1 + \cdots + X_{l-1}$.*

The linear polynomial $\lambda(X)$ has the property $\lambda(\overline{e}) = s(e)$. If we work with it the non-positivity condition in Theorem 3 will be easy to control. After substitution of $e_0 = n - e_1 - \cdots - e_l$ we have

$$P_1 = (v-1)n - ve_l,\ P_2 = v\{(v-1)n - ve_{l-1} - (v-1)e_l\},$$

$$P_3 = v^2\{(v-1)n - ve_{l-2} - (v-1)e_{l-1} - (v-1)e_l\} \ldots,$$

$$P_l = v^{l-1}\{(v-1)n - ve_1 - (v-1)e_2 - \cdots - (v-1)e_l\}.$$

Solving for the e_i yields

$$e_l = qn - P_1/v,\ e_{l-1} = q(1-q) + qP_1/v - P_2/v^2,$$

$$e_{l-2} = q(1-q)^2 + q(1-q)P_1/v + qP_2/v^2 - P_3/v^3,$$

in general

$$e_i = nq(1-q)^{l-i} + q(1-q)^{l-i-1}P_1/v + \cdots + qP_{l-i}/v^{l-i} - P_{l+1-i}/v^{l+1-i}.$$

Here $q = (v-1)/v$. This simplifies:

Lemma 6.

$$e_i = \frac{1}{v^{l+1-i}}\{(v-1)(n + P_1 + \cdots + P_{l-i}) - P_{l+1-i}\}$$

Proposition 2. *The expression of λ in terms of generalized Kravchouk polynomials is $\sum_{i=1}^{l} ie_i = \sum_{k=1}^{l} d_k P_k + d_0,$ where*

$$d_k = -\frac{v^{l+1-k}-1}{(v-1)v^l} < 0 \text{ for } k \geq 1,$$

$$d_0 = ln - \frac{n}{v-1}(1 - 1/v^l) = \rho_l n,$$

and

$$\rho_l = l - 1/v - \cdots - 1/v^l = \{lv^l - (v^l - 1)/(v-1)\}/v^l.$$

Proof. Using Lemma 6 we obtain $d_l = -1/v^l, d_{l-1} = -2/v^{l-1} + (v-1)/v^l = -(v+1)/v^l$, by induction

$$d_k = -(1 + v + \cdots + v^{l-k})/v^l = -\frac{v^{l+1-k}-1}{(v-1)v^l}$$

for $k \geq 1$. In order to obtain d_0 we need the derivative of the geometric series:

$$\sum_{j=1}^{T-1}(T-j)x^{j-1} = \frac{T}{1-x} - \frac{1-x^T}{(1-x)^2}.$$

It follows

$$d_0 = ln - \frac{n}{v-1}(1 - 1/v^l) = \rho_l n$$

$\square$

Choose $p(X) = c(r - \lambda(X))$ for $c > 0$. The non-positivity condition of Theorem 3 is automatically satisfied. The coefficient at P_k for $k > 0$ is $-d_k > 0$ by Propositon 2. The constant coefficient is $c(r - d_0)$ We need it to be $= 1$. This is possible if $r > d_0$. The bound from Theorem 3 is then $p(\overline{0}) = cr = r/(r - d_0)$. We have proved the following:

Theorem 5. *Consider the problem of Theorem 3, where $r/n > \rho_l = l - 1/v - \cdots - 1/v^l$. A feasible value is $r/(r - n\rho_l)$.*

As usual application of Theorem 5 to the type distribution and its dual yields bounds on ordered codes and ordered orthogonal arrays:

Theorem 6. *A code $C \subset V_v^{(l,n)}$ of minimum distance d, where $d/n > \rho_l$, has at most $d/(d - n\rho_l)$ codewords.*

Codes $C \subset V_v^{(l,n)}$ of strength t, where $(t+1)/n > \rho_l$, have at least $v^{ln}(t + 1 - n\rho_l)/(t + 1)$ codewords.

This is the bound first described in [9].

The orthogonality relations

Theorem 7 (orthogonality relations).

$$B_f(0) = v^{s(f)-b(f)}(v-1)^{b(f)}\binom{n}{f_l, f_{l-1}, \ldots, f_0}$$

is the number of vectors of type f.

- $B_e(0)B_f(e) = B_f(0)B_e(f)$.
- $\sum_f B_f(e)B_h(f) = g\delta_{e,h}$
- $\sum_e B_e(0)B_f(e)B_h(e) = \delta_{f,h}B_f(0)g$.

Proof. The third item is Proposition 1. It is known as the second orthogonality relation in the case of Kravchouk polynomials. For the first statement evaluate K_f at $X_0 = \cdots = X_{l-1} = 0, X_l = n$.

In order to obtain the second claim evaluate

$$\sum_{z \sim_f 0} \sum_{x \sim_e 0} \zeta^{x \cdot \overline{z}}.$$

This equals the number of participating z times $P_e(f)$. The other expression is obtained by summing at first over x, observing $x \cdot \overline{z} = \overline{x} \cdot z$. The last claim (first orthogonality relation) is obtained by multiplying the left side of the third claim by $B_e(0)$, applying the second claim and using the second orthogonality relation. □

The first two statements of Theorem 7 are equivalent to results from [6]. In order to control the products $B_f(e)B_h(e)$ observe that for given types f, h, m there is a constant p_{fh}^m such that for each pair of vectors x, y such that $x \sim_m y$ there are exactly p_{fh}^m vectors z such that $x \sim_f z$ and $y \sim_g z$. This is equivalent with the statement, proved in [6], that the relations $\sim_e$ as defined in the section following Definition 4 form an association scheme.

Theorem 8. *There exist constants p_{fh}^m such that for each pair of vectors (x, y) such that $x \sim_m y$ there exist precisely p_{fh}^m vectors z such that $x \sim_f z$ and $y \sim_g z$. Then*

$$B_f(e)B_h(e) = \sum_m p_{fh}^m B_m(e).$$

Moreover $p_{fh}^m = 0$ if $s(m) > s(f) + s(h)$.

Proof. The product formula follows from the definition of the B-constants. □

5 The sphere-packing and Rao bound

Fix r and s such that $2s < r$. Define $\Psi_s(X) = \sum_{f:s(f)\leq s} K_f(X)$, where as usual $X = (X_0, \ldots, X_l)$. Then $V = \Psi_s(\overline{0}) = \sum_{f:s(f)\leq s} B_f(0)$ is the volume of the ball of radius s. Consider the polynomial

$$p(X) = \sum_f c_f K_f(X), \text{ where } c_f = (\Psi_s(\overline{f})/V)^2.$$

This has the advantage that the coefficients are non-negative and $c_0 = 1$, as required. We need to check the non-positivity conditions. Let e such that $s(e) \geq r$.

$$p(\overline{e}) = \frac{1}{V^2} \sum_f (\Psi_s(f))^2 B_f(e).$$

Here $\Psi_s(X)$ has degree $\leq s$, so its square has degree $\leq 2s < r$. It follows from Theorem 8 that $(\Psi_s(f))^2$ is a linear combination of the $B_h(f)$ for $s(h) < r$. The second orthogonality relation shows $p(\overline{e}) = 0$.

The bound is

$$p(\overline{0}) = \frac{1}{V^2}\sum_f B_f(0)\Psi_s(f) = \frac{1}{V^2}\sum_{e_1,e_2:s(e_i)\leq s}\sum_f B_f(0)B_{e_1}(f)B_{e_2}(f).$$

Fix e_1, e_2. By the first orthogonality relation the sum over f vanishes if $e_1 \neq e_2$. The result is $p(\overline{0}) = g/V$. This is the sphere-packing bound for ordered codes and the Rao bound for OOA, first derived from the LP-bound in [9]. The fact that those bounds can be derived from the LP bound implies that the case of equality (perfect codes) can be described in terms of a Lloyd polynomial. The case of equality in these bounds has also been considered in [8].

6 The case of equality

Let $c = (c_i) = (c_1, \ldots, c_n)$ be an admissible point for the dual problem of Theorem 1, and $d = (d_j) = (d_1, \ldots, d_m)$ admissible for the primal problem. They form an **optimal pair** if both yield the same value. Let z_i be row number i of A and s_j column number j, where $i = 1, \ldots n, j = 1 \ldots, m$. Then c, d form an optimal pair if and only if the following conditions are satisfied:

$$c_i(z_i \cdot d - b) = 0 \text{ and } d_j(s_j \cdot c - p) = 0$$

for all i, j as above.

We applied Theorem 1 in the following situation: $A = (-B_f(e))$, where $e = (e_0, \ldots, e_l)$ such that $s(e) \geq r$ and $f = (f_0, \ldots, f_l) \neq 0$. Here we see f as row index and e as column index. The variables are $x = (x_e) \geq 0$ for the primal and $y = (y_f) \geq 0$ for the dual problem. The side conditions for the dual problem are $(A^t y)_e = -\sum_f y_f B_f(e) \geq 1$ ($b = (b_e)$ is the constant 1 vector) which we expressed in terms of $p(X) = 1 + \sum_f y_f K_f(X)$ as $p(\overline{e}) \leq 0$. The vector p is $(p_f) = (B_f(0))$. The side conditions for the primal problem are $-\sum_e x_e B_f(e) \leq B_f(0)$. Using an orthogonality relation this is equivalent with $\sum_e x_e B_e(f)/B_e(0) + 1 \geq 0$. This can be expressed in terms of the polynomial $q(X) = 1 + \sum_e x_e K_e(X)/B_e(0)$ as $q(f) \geq 0$. We obtain the following complete description of the relation between primal end dual problem in the case of Theorem 3 as well as the characterization of the case of equality:

Theorem 9. *Let $f \in P_{l,n}$ (see Definition 7) and $e \in P_{l,n}$ such that $s(e) \geq r$.*

- *An instance of the dual problem is described by a polynomial $p(X) = \sum_f y_f K_f(X)$, where $y_f \geq 0$ for all $f, y_0 = 1$ and $p(\overline{e}) \leq 0$ for all e. The objective value is $p(\overline{0})$.*
- *An admissible value of the primal problem is described by a polynomial $q(X) = 1 + \sum_e x_e K_e(X)/B_e(0)$ where $x_e \geq 0$ for all e as usual, and $q(\overline{f}) \geq 0$ for all f. The objective value is $q(\overline{0}) = 1 + \sum_e x_e$.*
- *Let $p(X), q(X)$ describe instances of the dual and primal problem, respectively. We have $p(\overline{0}) = q(\overline{0})$ (the optimal values of the pair of linear programs, shifted by 1) if and only if the following hold:*

  $$y_f q(\overline{f}) = 0 \text{ and } x_e p(\overline{e}) = 0$$

  for all e, f as usual.

Let now C be a perfect code. This means that $x_e = A_e$ describes the coefficients of the optimal $q(X)$. By definition $q(\overline{f}) = A'_f$. We saw in the proof of the sphere packing bound that $p(\overline{e}) = 0$ is always satisfied. This verifies half of the optimality conditions of Theorem 9. The other half says that whenever $A'_f \neq 0$ then $y_f = 0$. As y_f was defined in terms of Ψ_s we arrive at the following description:

Proposition 3. *The code $C \subset V_v^{(l,n)}$ of minimum distance $d = 2s + 1$ is perfect if and only if we have $\Psi_s(\overline{f}) = 0$ for every $f \neq 0$ such that $A'_f \neq 0$.*

Proposition 3 may motivate us to call $\Psi_s(X)$ the generalized Lloyd polynomial.

Some fundamental parameters

Clearly the material in this subsection was inspired by Delsarte's fundamental paper [3]. Consider the space $\mathcal{S}$ and its subspace $\mathcal{S}_0$ as in Definition 7. Each element of $\mathcal{S}$ can also be interpreted as a polynomial in l variables $E_1, \ldots, E_l$. Here we identify $x = (x_e)$ with the polynomial having coefficient x_e at monomial $E_1^{e_1} \ldots E_l^{e_l}$. The B-functions B_f are polynomials if we read the $e_i = X_{l-i}, i = 1, \ldots, l$ as variables and substitute $e_0 = n - e_1 - \ldots, e_l$. In this natural way we have $B_f \in \mathcal{S}$. Moreover the B_f form a basis of $\mathcal{S}$. In fact we saw in Section 4 how to express the E_i in terms of the B-functions. Theorem 8 shows how products are handled. This shows that the B-functions generate $\mathcal{S}$. The orthogonality relations show linear independence.

The following lemma describes a relationship between the two ways of writing elements of $\mathcal{S}$.

Lemma 7. *Let $\alpha = (\alpha_e) \in \mathcal{S}_0$ and $p(E) \in \mathcal{S}$. Express $p = \sum_h c_h B_h$ in terms of the B-basis. Then the following holds:*

$$\sum_f \alpha'_f p(f) = \frac{g}{\sum \alpha_e} \sum_e \alpha_e c_e.$$

Proof. Simply write out the left side and use the orthogonality relations. $\square$

The basic parameters for codes and OA generalize in a natural way, compare [3].

Definition 9. *Let $\alpha \in \mathcal{S}$ and α' its B-transform. Denote by $d = d(\alpha)$ the smallest $i > 0$ such that there exists e with $s(e) = i$ and $\alpha_e \neq 0$. Similarly s is the number of different sizes i such that there exist e of size i with $\alpha_e \neq 0$. Also, $\delta(\alpha)$ is the maximal number i such that there exist partitions of sizes $ln, ln-1, \ldots, ln-i+1$ with nonzero coefficient in α. A $'$ means that we apply the parameter to α'.*

Proposition 4. *Let $\alpha \in \mathcal{S}_0$. Then*

$$1 + 2s' - \delta' \geq d.$$

Proof. Let $\lambda = E_1 + 2E_2 + \cdots + lE_l$ and consider the polynomial

$$\beta = \lambda(ln - \lambda) \ldots (ln - \delta' + 1 - \lambda) \prod_k (\lambda - k)^2,$$

where the product is over all integers k be 1 and $ln - \delta'$ such that $\alpha'_k \neq 0$. By definition $\beta(e) \geq 0$ for all $e \in P_{l,n}$ (observe $\lambda(e) = s(e)$), and β has degree $1 + 2s' - \delta'$. Assume this number is $< d$. Then $\beta = \sum_{h:s(h)<d} c_h B_h$. By definition of β we have $\sum_f \alpha'_f \beta(f) = 0$. It follows from Lemma 7 that $\sum_e \alpha_e c_e = 0$. By definition of d this implies $\alpha_0 c_0 = 0$, hence $c_0 = 0$. As $\beta(e) \geq 0$ for all e the orthogonality relations show $\beta(e) = 0$ for all e, contradiction. $\square$

In the case of perfect codes Proposition 4 shows that the dual type distribution has nonzero entries at $s' \geq (d-1)/2$ different types of different sizes. At these types the Lloyd polynomial has to vanish.

7 A quadratic bound

Let $p(X) = \alpha(\lambda(X) - r)(\lambda(X) - ln)$ for $\alpha > 0$ (see Definition 8). It satisfies the non-positivity conditions of Theorem 3. We know how λ is expressed in terms of the generalized Kravchouk basis, see Proposition 2.

In order to control the coefficients of $p(X)$ in terms of the generalized Kravchouk basis we need the structure constants p_{fh}^m from Theorem 8 when f, h correspond to elementary vectors. Denote p_{ij}^m those numbers where i corresponds to type $f_i = 1$ and j to $f_j = 1$. Given a vector y of type m, p_{ij}^m is the number of times y can be written in the form $y = z + z'$, where z has type i and z' has type j. We consider only those m for which $p_{ij}^m \neq 0$. Clearly we must have $b(m) \leq 2$. Consider at first case $i > j$. If $b(m) = 2$, then the type of m must be described by $f_i = f_j = 1$ and the representation is unique. As $i \neq j$ we have $b(m) \neq 0$. Let $b(m) = 1, m$ of type $f_k = 1$. Clearly $k = 1$. The nonzero entry at depth i of z is uniquely determined by y, entries below that are arbitrary. It follows $p_{ij}^i = (v-1)v^{j-1}$.

Lemma 8. *Let indices $i \geq 1$ stand for the partition with $f_i = 1, f_0 = n-1$, $\{i, j\}$ for $f_i = f_j = 1, f_0 = n-2$ when $i \neq j$ and $\{i, i\}$ for $f_i = 2, f_0 = n-2$. Index 0 stands for $f_0 = n$. Then the values of the relevant structure constants are*

$$p_{ij}^{\{i,j\}} = 2,\ p_{ij}^i = (v-1)v^{j-1},\ p_{ij}^k = 0 \text{ otherwise}$$

for $i > j$, and

$$p_{ii}^{\{i,i\}} = 2,\ p_{ii}^i = (v-2)v^{i-1},\ p_{kk}^i = (v-1)v^{k-1}, p_{ii}^0 = n(v-1)v^{i-1}$$

for $k > i$.

In particular

$$K_i K_j = 2K_{\{i,j\}} + (v-1)v^{j-1}K_i$$

and

$$K_i^2 = 2K_{\{i,i\}} + (v-2)v^{i-1}K_i + \sum_{0<j<i}(v-1)v^{i-1}K_j + n(v-1)v^{i-1}.$$

We have $p = \alpha(\sum ie_i - r)(\sum ie_i - ln) = \alpha(\sum_{k=1}^l d_k P_k + d_0 - r)(\sum_{k=1}^l d_k P_k + d_0 - n)$. Clearly the coefficients at quadratic terms are non-negative. Let c_i be the coefficient at $P_i, i > 0$. Then

$$c_i = \alpha(\sum_{j<i} 2d_i d_j (v-1)v^{j-1} + d_i^2(v-2)v^{i-1} + \sum_{k>i} d_k^2(v-1)v^{k-1} + d_i(2d_0 - r - ln)).$$

The constant coefficient is

$$c_0 = \alpha(\sum_k d_k^2 n(v-1)v^{k-1} + (d_0 - r)(d_0 - ln)).$$

It follows

$$c_0/\alpha = (d_0 - r)(d_0 - ln) + \frac{n}{(v-1)v^{2l}} \sum_k (v^{l+1-k} - 1)^2 v^{k-1} =$$

$$(d_0 - r)(d_0 - ln) + \frac{n}{(v-1)v^{2l}} \sum_k (v^{2l+1-k} - 2v^l + v^{k-1}) =$$

$$= (d_0 - r)(d_0 - ln) + \frac{n}{(v-1)v^{2l}}(v^{l+1} + \cdots + v^{2l} - 2lv^l + v^{l-1} + \cdots + 1) =$$

$$= (d_0 - r)(d_0 - ln) + \frac{n}{(v-1)v^{2l}}(-(2l+1)v^l + (v^{2l+1} - 1)/(v-1)).$$

For $r > \rho_l n$ this is not interesting as in this range the Plotkin bound applies. For $r = \rho_l n$ the conditions are clearly satisfied. Let now $r = \rho_l n - \epsilon$ for some $\epsilon > 0$. The conditions $c_i \geq 0$ for $i > 0$ are certainly satisfied as long as $2d_0 - r - ln \leq 0$. This is a wide range. The condition $c_0 > 0$ is sharpest. It reads

$$-\epsilon n \frac{v^l - 1}{(v-1)v^l} + n \frac{v^{2l+1} - (2l+1)(v-1)v^l - 1}{(v-1)^2 v^{2l}} > 0$$

equivalently

$$\epsilon < \frac{v^{2l+1} - (2l+1)(v-1)v^l - 1}{(v-1)v^l(v^l - 1)}.$$

We have to choose ϵ in this range such that $r = d_0 - \epsilon$ is integer. As $c_0 = 1$ this determines α. The upper bound is $\alpha l n r$.

Theorem 10. *Given v, n, l, let $d_0 = ln - \frac{n}{v-1}(1 - 1/v^l) = \rho_l n$ and*

$$0 < \epsilon < \frac{v^{2l+1} - (2l+1)(v-1)v^l - 1}{(v-1)v^l(v^l - 1)}$$

such that $r = d_0 - \epsilon$ is integer. Then

$$M = \frac{l(v-1)^2 v^{2l} r}{v^{2l+1} - (2l+1)(v-1)v^l - 1 - \epsilon(v-1)v^l(v^l - 1)}$$

is an upper bound on the size of a code with minimum distance r in $V_v^{(l,n)}$ and $M' = v^{ln}/M$ is a lower bound on the size of a strength $r-1$ OOA in the same space.

With $m = log_v(M')$ we have that no $(m-r, m-1, n)_v$-net exists.

Case $v = 2, l = 2$

The condition is $\epsilon < 11/12$. We have $d_0 = 5n/4$. Consider first case $n = 4n', \epsilon = 0$. Then $r = 5n', \alpha = 16/(11n)$ and the code bound is $M = 2n\alpha r = 160n'/11$. The bound on the OOA is $M' = 2^{2n-5}11/(5n')$. This excludes net parameters

$$(2, 11, 8)_2,\ (7, 26, 16)_2,\ (12, 41, 24)_2,\ (15, 49, 28)_2,\ (18, 57, 32)_2,$$

$$(20, 64, 36)_2,\ (23, 72, 40)_2,\ (26, 80, 44)_2.$$

Here are some new parameters excluded by the quadratic bound:

$$(9, 44, 17)_2,\ (13, 76, 21)_2,\ (14, 80, 22)_2,\ (17, 73, 27)_2,$$

$$(18, 57, 32)_2,\ (22, 91, 33)_2, (23, 94, 34)_2$$

and

$$(7, 43, 24)_3,\ (9, 53, 29)_3,\ (11, 90, 32)_3,\ (12, 67, 36)_3.$$

References

[1] J. Bierbrauer: *Introduction to Coding Theory,* Chapman&Hall/CRC Press 2004.

[2] P. Delsarte: *Bounds for unrestricted codes by linear programming, Philips Research Report* **27** (1972), 272-289.

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

[4] P. Delsarte: *An algebraic approach to the association schemes of coding theory, Philips Research Reports Supplements* **10** (1973).

[5] W. J. Martin and D. R. Stinson: *A generalized Rao bound for ordered orthogonal arrays and (t, m, s)-nets, Canadian Mathematical Bulletin* **42** (1999), 359-370.

[6] W. J. Martin and D. R. Stinson: *Association schemes for ordered orthogonal arrays and (t, m, s)-nets, Canadian Journal of Mathematics* **51** (1999), 326-346.

[7] W. J. Martin: *Linear programming bounds for ordered orthogonal arrays and* (t, m, s)*-nets,* Monte Carlo and Quasi-Monte Carlo methods 1998 (H. Niederreiter and J. Spanier, eds), pp. 368-376, Springer, Berlin, 2000.

[8] W. J. Martin: *Design systems: combinatorial characterizations of Delsarte T-designs via partially ordered sets,* in *Codes and Association Schemes, DIMACS Series in Discrete Mathematics and Theoretical Computer Science, vol. 56, (A. Barg and S. Litsyn, eds.), American Mathematical Society* (2001), 223-239.

[9] W. J. Martin and T. I. Visentin: *A dual Plotkin bound for* (t, m, s)*-nets,* manuscript.

[10] H. Niederreiter: *Point sets and sequences with small discrepancy, Monatsh. Math.* **104** (1987), 273–337.

[11] R. Schürer and W. Ch. Schmid: *MinT: A Database for Optimal Net Parameters,* in *Monte Carlo and Quasi-Monte Carlo Methods 2004, H. Niederreiter and D. Talay, editors* 457-469, Springer-Verlag, Berlin.