Bounds on ordered codes and orthogonal arrays

Alexander Barg
Dept. of ECE and Institute for Systems Research
University of Maryland, College Park, MD 20742
abarg@umd.edu

Punarbasu Purkayastha
Dept. of ECE
University of Maryland, College Park, MD 20742
ppurka@umd.edu

***Abstract*— We prove several new bounds on ordered codes and ordered orthogonal arrays. We also show that the eigenvalues of the ordered Hamming scheme are the multivariable Krawtchouk polynomials and establish some of their properties.**

I. Introduction

A. The NRT metric space. Let $\mathcal{Q}$ be a finite alphabet of size q viewed as an additive group mod q. Consider the set $\mathcal{Q}^{r,n}$ of vectors of dimension rn over $\mathcal{Q}$. A vector $\boldsymbol{x}$ will be written as a concatenation of n blocks of length r each, $\boldsymbol{x} = \{x_{11}, \dots, x_{1r}; \dots; x_{n1}, \dots, x_{nr}\}$. For a given vector $\boldsymbol{x}$ let $e_i, i = 1, \dots, r$ be the number of r-blocks of $\boldsymbol{x}$ whose rightmost nonzero entry is in the ith position counting from the beginning of the block. The r-vector $e = (e_1, \dots, e_r)$ will be called the *shape* of $\boldsymbol{x}$. For two vectors $\boldsymbol{x}, \boldsymbol{y} \in \mathcal{Q}^{r,n}$ let us write $\boldsymbol{x} \sim_e \boldsymbol{y}$ if $\operatorname{shape}(\boldsymbol{x} - \boldsymbol{y}) = e$. A shape vector $e = (e_1, \dots, e_r)$ defines a partition of a number $N \le n$ into a sum of r nonnegative parts. Let $\Delta_{n,r} = \{e \in (\mathbb{Z}_+ \cup \{0\})^r : \sum_i e_i \le n\}$ be the set of all such partitions. For brevity we write

$$|e| = \sum_i e_i, \quad |e|' = \sum_i i e_i, \quad e_0 = n - |e|.$$

Let $\boldsymbol{x} \in \mathcal{Q}^{r,n}$ be a vector of shape e. Define a weight function (norm) on $\mathcal{Q}^{r,n}$ by setting $\mathrm{w}(\boldsymbol{x}) = |e|'$ and let $d_r(\boldsymbol{x}, \boldsymbol{y}) = \mathrm{w}(\boldsymbol{x} - \boldsymbol{y})$ denote the metric induced by this norm. We call the function d_r the *ordered weight*. It was first introduced by Niederreiter [13] and later, independently, by Rosenbloom and Tsfasman [15]. The set $\mathcal{Q}^{r,n}$ together with this metric will be called the *ordered Hamming space* (the *NRT space*) and denoted by $\overrightarrow{H} = \overrightarrow{H}(q, n, r)$. Note that the case $r = 1$ corresponds to the usual Hamming distance on $\mathcal{Q}^n$. Below the value of r is assumed to be fixed.

B. Ordered codes and ordered orthogonal arrays (OOAs). An (n, M, d) *ordered code* $C \subset \overrightarrow{H}$ is an arbitrary subset of M vectors in $\mathcal{Q}^{r,n}$ such that the minimum ordered distance between any two distinct vectors in C is d. The number $R = \log_q M / rn$ is called the *rate* of the code C. In the asymptotic results below we assume that $n \to \infty$ and $d/n \to r\delta$.

Let us call a subset of coordinates $\mathcal{I} \subset \{1, \dots, rn\}$ *left-adjusted* if with any coordinate $ir+j, 0 \le i \le n-1, 1 \le j \le r$ it also contains all the coordinates $(ir+1, \dots, ir+j-1)$ of the same block. A subset $C \subset \mathcal{Q}^{r,n}, |C| = M$ is called a (t, n, r, q) *ordered orthogonal array* (OOA) of strength t if its projection on any left-adjusted set of t coordinates contains all the q^t rows an equal number, say λ, of times. The parameter λ is called the *index* of C. It follows that $M = \lambda q^t$. Sometimes OOAs are also called hypercubic designs.

The study of OOAs is motivated by the problem of designing uniformly distributed sets of points in the n-dimensional unit cube K_n for use in numerical integration. For a continuous function f of bounded variation, the error of replacing the integral over K_n with the sum $M^{-1} \sum_{x \in \mathcal{N}} f(x)$ over a set $\mathcal{N}$ of M points in K_n (a "net") can be bounded via the deviation of $\mathcal{N}$ from the uniform distribution. Low-discrepancy point sets [13] give rise to the notion of a (t, m, s)-net which can be equivalently defined as an $\mathrm{OOA}(m-t, s, m-t, q)$ with $\lambda = q^t$ (see, e.g., [12]). Therefore bounds on OOAs are of interest for estimating the error of Monte-Carlo integration on K_n. In this context ordered codes arise as a dual object of OOAs within the frame of Delsarte's theory [6], although [15] defined them independently of other problems.

Apart from the combinatorial motivation, ordered codes figure in recent algebraic list decoding algorithms of Reed-Solomon codes [14].

C. Notation. Let $v_e = |\{\boldsymbol{x} \in \overrightarrow{H} : \operatorname{shape}(\boldsymbol{x}) = e\}|$. We have

$$v_e = \binom{n}{e_0, e_1, \dots, e_n} (q-1)^{|e|} q^{|e|' - |e|}. \tag{1}$$

Let $A(z) = (q-1)z(z^r - 1)/(q(z-1))$ and let $z_0 = z_0(x)$ satisfy the equation $xr(1 + A(z)) = \frac{q-1}{q} \sum_i i z^i$. Define the function

$$H_{q,r}(x) = x(1 - \log_q z_0) + \frac{1}{r} \log_q(1 + A(z_0)).$$

In the case $r = 1$ we write $h_q(x)$ instead of $H_{q,1}(x)$, where $h_q(x) = -x \log_q \frac{x}{q-1} - (1-x) \log_q(1-x)$. Let

$$\delta_{\text{crit}} = 1 - \frac{1}{r} \sum_{i=1}^{r} q^{-i} = 1 - \frac{1}{rq^r} \frac{q^r - 1}{q - 1}. \tag{2}$$

Let S_d be a sphere of radius $d = \delta rn$ in $\overrightarrow{H}$. Its volume equals $|S_d| = \sum_{e:|e|'=d} v_e$. By [15], this quantity satisfies

$$\lim_{n \to \infty} (nr)^{-1} \log_q |S_d| = \begin{cases} H_{q,r}(\delta) & 0 \le \delta \le \delta_{\text{crit}} \\ 1 & \delta_{\text{crit}} < \delta \le 1. \end{cases} \tag{3}$$

D. Bounds on ordered codes and OOAs. A number of bounds on the size of ordered codes and OOAs were established in [15], [9], [11], [5], [12]. By the Gilbert-Varshamov bound [15] there exists an (n, M) code $C \in \overrightarrow{H}$ with NRT distance d whose parameters satisfy $M \sum_{i=0}^{d-1} |S_i| \ge q^{nr}$. Asymptotically, we obtain $R \ge 1 - H_{q,r}(\delta)$ for $0 \le \delta \le \delta_{\text{crit}}$. The same paper also proves the Plotkin bound

$$M \le \frac{d}{d - nr\delta_{\text{crit}}}$$

and the Singleton bound.

Dual bounds (i.e., lower bounds on the size of OOAs) were established in [11], [12]. In particular, let C be a (t, n, r, q) OOA. If $t + 1 \geq nr\delta_{\text{crit}}$ then

$$|C| \geq q^{nr}\Big(1 - \frac{nr\delta_{\text{crit}}}{t+1}\Big)$$

(dual Plotkin bound, [12]). A dual Hamming bound (Rao bound) on OOAs was proved in [11].

II. A Bassalygo-Elias bound on codes

Theorem 2.1: Let C be an (n, M, d) code. Then

$$M \leq q^{rn} dn \min_{0 \leq w \leq rn} \frac{1}{|S_w|(dn - 2wn + \frac{w^2}{r\delta_{\text{crit}}})}.$$

Proof : We will rely upon the next lemma.

Lemma 2.2: Let $C \subset \overrightarrow{H}, |C| = M$ be a code all of whose vectors have weight w and are at least distance d apart. Then

$$M \leq \frac{dn}{dn - 2wn + \frac{w^2}{r\delta_{\text{crit}}}}.$$

Proof : Let C^i be a projection of C on the ith block of coordinates. For a vector $\boldsymbol{z} \in \mathcal{Q}^r$ let $\boldsymbol{z}^h = (z_{r-h+1}, \dots, z_r)$ be its suffix of length h. Given $\boldsymbol{x} \in C$, we denote by $\boldsymbol{x}^i \in C^i$ its ith block and write $\boldsymbol{x}^{i,h}$ to refer to the h-suffix of $\boldsymbol{x}^i$. For $i = 1, \dots, n; h = 1, \dots, r; \boldsymbol{c} \in \mathcal{Q}^h$ let $\lambda^h_{i,\boldsymbol{c}} = |\{\boldsymbol{x}^i \in C^i : \boldsymbol{x}^{i,h} = \boldsymbol{c}\}|$. We have

$$d_r(\boldsymbol{x}^i, \boldsymbol{y}^i) = r - \sum_{h=1}^{r} \sum_{\boldsymbol{c} \in \mathcal{Q}^h} \delta(\boldsymbol{x}^{i,h}, \boldsymbol{c})\delta(\boldsymbol{y}^{i,h}, \boldsymbol{c}). \qquad (4)$$

Compute the sum of all distances in the code as follows:

$$\sum_{\boldsymbol{x},\boldsymbol{y} \in C} d_r(\boldsymbol{x}, \boldsymbol{y}) = nrM^2 - \sum_{i,\boldsymbol{x}^i,\boldsymbol{y}^i} \sum_{h=1}^{r} \sum_{\boldsymbol{c} \in \mathcal{Q}^h} \delta(\boldsymbol{x}^{i,h}, \boldsymbol{c})\delta(\boldsymbol{y}^{i,h}, \boldsymbol{c})$$
$$= nrM^2 - \sum_{i=1}^{n} \sum_{h=1}^{r} \sum_{\boldsymbol{c} \in \mathcal{Q}^h} (\lambda^h_{i,\boldsymbol{c}})^2. \qquad (5)$$

To bound above the right-hand side, we need to find the minimum of the quadratic form

$$F = \sum_{i=1}^{n} \sum_{h=1}^{r} \sum_{c \in \mathcal{Q}^h \backslash \{0\}} (\lambda^h_{i,c})^2 + \sum_{i=1}^{n} \sum_{h=1}^{r} (\lambda^h_{i,0})^2$$

under the constraints

$$\begin{array}{l} \sum_{i=1}^{n} \sum_{h=1}^{r} \lambda^h_{i,0} = M(nr - w) \\ \sum_{c \in \mathcal{Q}^h} \lambda^h_{i,c} = M \quad (1 \leq h \leq r,\ 1 \leq i \leq n) \end{array} \qquad (6)$$

Critical points of F in the intersection of these hyperplanes, together with (6), satisfy the equations

$$\begin{array}{ll} 2\lambda^h_{i,c} + \beta_{i,h} = 0 & 1 \leq i \leq n; 1 \leq h \leq r; c \in \mathcal{Q}^h \backslash \{0\} \\ 2\lambda^h_{i,0} + \alpha + \beta_{i,h} = 0 & 1 \leq i \leq n; 1 \leq h \leq r \\ & \alpha, \beta_{i,h} \in \mathbb{R}. \end{array} \qquad (7)$$

The system (6)-(7) has a unique solution for the variables $\lambda^h_{i,c}, \beta_{i,h}, \alpha$; in particular,

$$\lambda^h_{i,0} = M\Big[\Big(\frac{1}{q^h} - 1\Big)\frac{w}{nr\delta_{\text{crit}}} + 1\Big], \quad h = 1, \dots, r, i = 1, \dots, n$$

$$\lambda^h_{i,c} = \frac{Mw}{q^h nr\delta_{\text{crit}}}, \qquad h = 1, \dots, r, i = 1, \dots, n, c \in F_q^h \backslash \{0\}.$$

To verify that this critical point is in fact a minimum, observe that the form F is convex because its Hessian matrix is $2I$ and is positive definite (both globally and restricted to the intersection of the hyperplanes (6)). Substituting these values of the λs and taking account of the fact that $\sum_h q^{-h} = r(1 - \delta_{\text{crit}})$, we get

$$F \geq M^2 n\Big(\frac{w^2}{n^2 r\delta_{\text{crit}}} - \frac{2w}{n} + r\Big).$$

Then from (5) we obtain

$$dM(M-1) \leq \sum_{\boldsymbol{x},\boldsymbol{y} \in C} d_r(\boldsymbol{x}, \boldsymbol{y}) \leq \frac{M^2}{n}\Big(2wn - \frac{w^2}{r\delta_{\text{crit}}}\Big)$$

which gives the result. ∎

The proof of the theorem is completed as follows. Let S_w be a sphere of radius w around zero. Clearly,

$$|C||S_w| = \sum_{x \in \overrightarrow{H}} |(C - x) \cap S_w| \leq q^{nr} A_q(n, d, w),$$

where $A_q(n, d, w)$ is the maximum size of a distance-d code in S_w. With the previous lemma, this gives the result. ∎

Using (3), the asymptotic version of the BE bound is

$$R \leq 1 - H_{q,r}(\delta_{\text{crit}}(1 - \sqrt{1 - \delta/\delta_{\text{crit}}})).$$

III. The ordered Hamming scheme

An association scheme that describes the combinatorics of the NRT space was constructed in [10]. Define an r-class "kernel scheme" $\mathcal{K}(\mathcal{Q}^{r,1}, \mathcal{D} = (D_0, D_1, \dots, D_r))$ with the relations

$$D_i = \{(\boldsymbol{x}_1, \boldsymbol{x}_2) \in \mathcal{Q}^{r,1} \times \mathcal{Q}^{r,1} : d_r(\boldsymbol{x}_1, \boldsymbol{x}_2) = i\} \quad (0 \leq i \leq r).$$

The next theorem uses the notion of Delsarte extension of association schemes [6, p.17]. (We refer to [6], [3] for general combinatorial background.)

Theorem 3.1: [10] The space $X = \mathcal{Q}^{r,n}$ together with the relations

$$R_e = \{(\boldsymbol{x}, \boldsymbol{y}) \in X \times X : \boldsymbol{x} \sim_e \boldsymbol{y}\} \quad (e \in \Delta_{n,r})$$

forms a formally self-dual association scheme $\overrightarrow{\mathcal{H}}$, called the r-Hamming scheme. In can be constructed as an n-fold Delsarte extension of $\mathcal{K}$.

This implies in particular that the first and second eigenvalues of $\overrightarrow{\mathcal{H}}$ coincide. In this section we establish properties of the eigenvalues for later use in bounding the size of codes and OOAs. We remark that the valences of the scheme are equal to its multiplicities, and both are given by $v_e, e \in \Delta_{n,r}$.

In the conventional case of $r = 1$, eigenvalues of the Hamming scheme are given by the Krawtchouk polynomials

$$k_i(n, x) = \sum_{l=0}^{i} (-1)^l (q-1)^{k-l} \binom{x}{l} \binom{n-x}{k-l} \qquad (8)$$

which form a family of polynomials of one discrete variable orthogonal on $\{0,1,\dots,n\}$ with weight $\alpha(i)=\binom{n}{i}2^{-n}$, i.e., the binomial probability distribution. Here we are interested in their multivariable generalization.

Let $V=V_{r,n}$ be the space of real polynomials of r discrete variables $x=(x_1,x_2,\dots x_r)$ defined on $\Delta_{n,r}$. Let us define a bilinear form acting on the space V by

$$\langle\varphi,\psi\rangle=\sum_{e\in\Delta_{n,r}}\varphi(e)\psi(e)w(e) \tag{9}$$

where $w(e)=q^{-nr}v_e$. By Delsarte, the eigenvalues of $\overrightarrow{\mathcal{H}}$ are orthogonal, namely $\langle P_e,P_f\rangle=\delta_{e,f}v_e$. Let

$$p_i=q^{i-r-1}(q-1), i=1,\dots,r;\quad p_0=q^{-r}.$$

The numbers $p_i, i=0,\dots,r$ define a multinomial probability distribution on the set of partitions according to

$$\Pr(e)=n!\prod_{i=0}^{r}\frac{p_i^{e_i}}{e_i!},$$

and $\Pr(e)=w(e)$. With this, we recognize the eigenvalues P_e as a particular case of multivariable Krawtchouk polynomials [16] which form an orthogonal basis of the space $V=L_2(\Delta_{n,r})$ of real polynomials of r discrete variables. For a partition $f\in\Delta_{n,r}$ denote by

$$K_f(x)=K_{f_1,\dots,f_r}(x_1,\dots,x_r)$$

the Krawtchouk polynomial that corresponds to it. Let $\kappa=|f|$ be the degree of K_f.

Properties of the polynomials K_f. The next properties follow from the general theory of [6].

(i) $K_e(x)$ is a polynomial in the variables $x_1,\dots,x_r$ of degree $\kappa=|e|$. There are $\binom{\kappa+r-1}{r-1}$ different polynomials of the same degree, each corresponding to a partition of κ.

(ii) (*Orthogonality*)

$$\langle K_f,K_g\rangle=v_f\delta_{f,g},\quad \|K_f\|=\sqrt{v_f}. \tag{10}$$

In particular, let $F_i=(0^{i-1}10^{r-i-1}), i=1,\dots,r$ be a partition with one part. We have

$$\|K_{F_i}\|^2=\langle K_{F_i},K_{F_i}\rangle=n(q-1)q^{i-1}\quad i=1,\dots,r. \tag{11}$$

(iii) (*Linear polynomials*) For $i=1,\dots,r$,

$$K_{F_i}(x)=q^{i-1}(q-1)(n-x_r-\dots-x_{r-i+2})-q^ix_{r-i+1}. \tag{12}$$

This can be computed by Gram-Schmidt starting with $K_{0,\dots,0}=1$ and using (11).

(iv)

$$v_eK_f(e)=v_fK_e(f)\quad (e,f\in\Delta_{n.r}).$$

In particular, $K_f(0)=v_f$.

(v) For any $e,f\in\Delta_{n,r}$

$$K_f(e)K_g(e)=\sum_{h\in\Delta_{n,r}}p^h_{f,g}K_h(e) \tag{13}$$

where the linearization coefficients $p^h_{f,g}=|\{\boldsymbol{z}\in\mathcal{Q}^{r,n}:\boldsymbol{z}\sim_f\boldsymbol{x},\boldsymbol{z}\sim_g\boldsymbol{y};\boldsymbol{x}\sim_h\boldsymbol{y}\}|$ are the intersection numbers of the scheme. In particular, $p^h_{f,g}\ge 0$.

(vi) (*Three-term relation*) Let $\mathbb{K}_\kappa$ be a column vector of the polynomials K_f ordered lexicographically with respect to all f that satisfy $|f|=\kappa$. The three-term relation is obtained by expanding the product $P(e)\mathbb{K}_\kappa(e)$ in the basis $\{K_f\}$, where $P(e)$ is a first-degree polynomial. By orthogonality, the only nonzero terms in this expansion will be polynomials of degrees $\kappa+1,\kappa,\kappa-1$ [8, p.75].

We establish an explicit form of the three-term relation for $P(e)=\delta_{\text{crit}}rn-|e|'$. We have

$$P(e)\mathbb{K}_\kappa(e)=a_\kappa\mathbb{K}_{\kappa+1}(e)+b_\kappa\mathbb{K}_\kappa(e)+c_\kappa\mathbb{K}_{\kappa-1}(e) \tag{14}$$

where $a_\kappa,b_\kappa,c_\kappa$ are matrices of order $\binom{\kappa+r-1}{r-1}\times\binom{\kappa+t+r-1}{r-1}$, where $t=1,0,-1$ respectively. The nonzero elements of these matrices have the following form:

$$\begin{aligned}
a_\kappa[f,h]&=L_i(f_i+1)\\
&\qquad\text{if } h=(f_1,\dots,f_i+1,\dots,f_r)\\
c_\kappa[f,h]&=L_i(n-\kappa+1)q^{i-1}(q-1)\\
&\qquad\text{if } h=(f_1,\dots,f_i-1,\dots,f_r)
\end{aligned}$$

$$b_\kappa[f,h]=\begin{cases}L_if_iq^{i-1}(q-2)\quad\text{if } h=f\\ L_i(f_k+1)q^{i-1}(q-1)\\ \qquad\text{if } h=(f_1,\dots,f_k+1,\dots,f_i-1,\dots,f_r),\\ \qquad\qquad 1\le k<i\\ L_i(f_i+1)q^{k-1}(q-1)\\ \qquad\text{if } h=(f_1,\dots,f_k-1,\dots,f_i+1,\dots,f_r),\\ \qquad\qquad 1\le k<i\end{cases}$$

where $L_i=\frac{q^{r-i+1}-1}{q^r(q-1)}$.

Along with the polynomials K_e below we use their normalized version $\widetilde{K}_e=K_e/\sqrt{v_e}$. The polynomials $\{\widetilde{K}_e,e\in\Delta_{n,r}\}$ form an orthonormal basis of V. The matrices a,b,c in the orthonormal basis will be denoted by A,B,C respectively.

Let $V_\kappa\subset V$ be the set of polynomials of total degree $\le\kappa$. Let E_κ be the orthogonal projection from V on V_κ. Define the operator

$$\begin{aligned}S_\kappa:&V_\kappa\to V_\kappa\\ &\varphi\mapsto E_\kappa(P(e)\varphi).\end{aligned}$$

Its matrix in the orthonormal basis has the form

$$\widetilde{\mathbf{S}}_\kappa=\begin{bmatrix}B_0&A_0&0&\dots&0\\ C_1&B_1&A_1&\dots&0\\ 0&C_2&B_2&\dots&0\\ \vdots&\vdots&\vdots&\ddots&\vdots\\ 0&0&\dots&C_\kappa&B_\kappa\end{bmatrix}$$

where the B_is are symmetric and $C_i=A^T_{i-1}, i=1,\dots,\kappa$. On account of property (v) and the fact that $P(e)=\sum_{i=1}^rL_iK_{F_i}(e)$, the matrix elements of $\widetilde{\mathbf{S}}_\kappa$ are nonnegative.

The matrix of S_κ in the basis $\{K_e\}$ has the property

$$v_h\mathbf{S}_\kappa[f,h]=v_f\mathbf{S}_\kappa[h,f]\quad (f,h\in\Delta_{n,r}). \tag{15}$$

(vii) (*Explicit expression*)

$$K_f(x)=q^{|f|'-|f|}\prod_{i=1}^rk_{f_i}(n_i,x_{r-i+1}) \tag{16}$$

where k_{f_i} is a univariate Krawtchouk polynomial (8), $n_i = \sum_{j=0}^{r-i+1} x_j - \sum_{j=i+1}^{r} f_j$, and $f, x \in \Delta_{n,r}$. This form of the polynomial $K_f(x)$ was obtained in [5] (various other forms were found in [10], [7]).

(viii) (*Christoffel-Darboux*). Let $L \subset \Delta_{n,r}$ and define

$$U_L(a,e) \triangleq \sum_{f\in L} v_f^{-1} K_f(a) K_f(e) \quad (a,e\in\Delta_{n,r}).$$

The action of $P(e)$ on U_L is described as follows:

$$\begin{aligned}&(P(e)-P(a))U_L(a,e)\\ &=\sum_{f\in L} v_f^{-1} \sum_{h\in\Delta_{n,r}\setminus L} \mathbf{S}_\kappa[f,h](K_h(e)K_f(a)-K_h(a)K_f(e)),\end{aligned}$$

A particular case of the above is obtained when $L=\{f : |f|\le\kappa\}$. The kernel U_L, denoted in this case by U_κ, equals $U_\kappa = \sum_{s=0}^{\kappa} \widetilde{\mathbb{K}}_s(e)^T \widetilde{\mathbb{K}}_s(a)$, and we obtain

$$(P(e)-P(a))U_\kappa(a,e) = \sum_{f:|f|=\kappa} Q_f(e)\widetilde{K}_f(a) - \widetilde{K}_f(e)Q_f(a) \tag{17}$$

where $Q_f(e) = \sum_{h:|h|=\kappa+1} \widetilde{K}_h(e) A_\kappa[f,h]$. This relation is called the Christoffel-Darboux formula.

IV. An LP bound on codes and OOAs

The next result is a particular case of Delsarte's bound (see also [9]).

Theorem 4.1: Let $F(x) = F_0 + \sum_{e\ne 0} F_e K_e(x)$ be a polynomial that satisfies

$$F_0>0,\;\; F_e\ge 0\;\;(e\ne 0);\quad F(e)\le 0\;\;(|e|'\ge d). \tag{18}$$

Then any (n,M,d) code satisfies

$$M \le F(0)/F_0. \tag{19}$$

Any OOA of strength $t=d-1$ and size M' satisfies

$$M' \ge q^{nr} F_0/F(0). \tag{20}$$

We use this result to prove the next

Theorem 4.2: Let $C\subset \overrightarrow{H}$ be an (n,M,d) code and let λ_κ denote the maximum eigenvalue of S_κ. Then

$$M \le \frac{4r\delta_{\text{crit}}(n-\kappa)(q^r-1)^\kappa}{\delta_{\text{crit}} rn - \lambda_\kappa}\binom{n}{\kappa} \tag{21}$$

where κ is any degree such that $P(e)\le\lambda_{\kappa-1}$ for all shapes e with $|e|'\ge d$.

Proof : Consider the operator T_κ that equals S_κ on $V_{\kappa-1}$ and acts on a function $\varphi\in V_\kappa\setminus V_{\kappa-1}$ by

$$T_\kappa(\varphi) := S_\kappa\varphi - \sum_{f:|f|=\kappa} \varepsilon_f \varphi_f \widetilde{K}_f,$$

where $\varepsilon_f>0$ are some constants indexed by the partitions of weight κ (their values will be chosen later). The matrix of T_κ in the orthonormal basis equals

$$\widetilde{\mathbf{T}}_\kappa = \widetilde{\mathbf{S}}_\kappa - \begin{bmatrix} 0 & 0\\ 0 & E\end{bmatrix}$$

where $E=\operatorname{diag}(\varepsilon_f, |f|=\kappa)$ is a matrix of order $\binom{\kappa+r-1}{r-1}$. Let m be such that $\widetilde{\mathbf{T}}_\kappa + mI > 0$. By Perron-Frobenius, the spectral radius $\rho(T_\kappa+mI)$ is well-defined and is an eigenvalue of (algebraic and geometric) multiplicity one of $T_\kappa+mI$. Moreover, again using Perron-Frobenius,

$$\rho(S_{\kappa-1}+mI) < \rho(T_\kappa+mI) < \rho(S_\kappa+mI).$$

Then

$$\lambda_{\kappa-1} < \theta_\kappa < \lambda_\kappa \tag{22}$$

where $\theta_\kappa = \rho(T_\kappa)$. Let $G>0$ be the eigenfunction of T_κ with eigenvalue θ_κ. Let us write out the product $P(e)G$ in the orthonormal basis:

$$\begin{aligned}P(e)G &= G\widetilde{\mathbf{S}}_\kappa + G_\kappa A_\kappa \widetilde{\mathbb{K}}_{\kappa+1}\\ &= \theta_\kappa G + \sum_{f:|f|=\kappa} \varepsilon_f G_f \widetilde{K}_f + G_\kappa A_\kappa \widetilde{\mathbb{K}}_{\kappa+1}.\end{aligned}$$

where G_κ is a projection of the vector G on the space $V_\kappa\setminus V_{\kappa-1}$. This implies the equality

$$G = \frac{\sum_{|f|=\kappa} G_f(\varepsilon_f\widetilde{K}_f + Q_f)}{P(e)-\theta_\kappa},$$

where $Q_f(e)$ is defined after (17). Now take $F(e)=(P(e)-\theta_\kappa)G^2(e)$. Let us verify (18). Since multiplication by a function is a self-adjoint operator, we obtain

$$F_0 = \langle F,1\rangle = \langle \sum_{|f|=\kappa} G_f(\varepsilon_f\widetilde{K}_f+Q_f), G\rangle = \sum_{|f|=\kappa} G_f^2\varepsilon_f > 0.$$

By (13), $F_e\ge 0$ for $e\ne 0$. The assumption of the theorem together with (22) implies that $F(e)\le 0$ for $|e|'\ge d$. Hence

$$\begin{aligned}M &\le \frac{F(0)}{F_0} = \frac{\Big(\sum_{|f|=\kappa} G_f(\varepsilon_f\widetilde{K}_f(0)+Q_f(0))\Big)^2}{(P(0)-\theta_\kappa)\sum_{|f|=\kappa} G_f^2\varepsilon_f}\\ &\le \sum_{|f|=\kappa} \frac{(\varepsilon_f\widetilde{K}_f(0)+Q_f(0))^2}{(P(0)-\lambda_\kappa)\varepsilon_f} \le \frac{4\sum_{|f|=\kappa} Q_f(0)\sqrt{v_f}}{P(0)-\lambda_\kappa}\end{aligned} \tag{23}$$

where in the third step we used the Cauchy-Schwarz inequality and in the last step computed the minimum on ε_f. Next,

$$\sum_{|f|=\kappa} Q_f(0)\sqrt{v_f} = \sum_{f:|f|=\kappa}\sqrt{v_f}\sum_{h:|h|=\kappa+1} A_\kappa[f,h]\sqrt{v_h}.$$

Let $h=(f_1,\dots,f_i+1,\dots,f_r)$ for some $i, 1\le i\le r$. Then using (1) we find

$$A_\kappa[f,h]\sqrt{v_h} = \Big(1-\frac{1}{q^{r-i+1}}\Big)(n-\kappa)\sqrt{v_f},$$

Thus we have

$$\begin{aligned}\sum_{|f|=\kappa} Q_f(0)\sqrt{v_f} &= \sum_{|f|=\kappa}\sum_{i=1}^{r}(n-\kappa)\Big(1-\frac{1}{q^{r-i+1}}\Big)v_f\\ &= (n-\kappa)r\delta_{\text{crit}}\sum_{|f|=\kappa} v_f = (n-\kappa)r\delta_{\text{crit}}\binom{n}{\kappa}(q^r-1)^\kappa.\end{aligned}$$

Substitution of this into (23) concludes the proof. ∎

Remark: The proof uses a "spectral method" first employed in [2] for the Grassmannian space and later used in [4] to prove classical asymptotic bounds of coding theory. The gist of the method can be explained as follows. The polynomial $F(e)$ is sought in the form $F(e) = u(e)G^2(e)$ where $u(e)$ is a linear function that assures that $F(e) \le 0$ in (18) and $G(e)$ is a function that maximizes the Fourier transform $\widehat{F}(0)$. It turns out that a good choice for G is a delta-function at (or near) d. An approximation of the delta-function is given by the (Dirichlet) kernel U_κ which is its projection on V_κ. We therefore seek to modify the operator S_κ so that U_κ becomes its eigenfunction with eigenvalue θ_κ, express the bound of Theorem 4.1 as a function of θ_κ and optimize on κ within the limits (18). The reader is advised to consult the univariate case [4] for which these ideas become more apparent.

Next we estimate the spectral radius of S_κ using some combinatorics of partitions and prove the following asymptotic result.

Theorem 4.3: Let $R_{LP}(\delta)$ be the function defined by

$$R(\tau) = \tfrac{1}{r}(h_q(\tau) + \tau \log_q((q^r-1)/(q-1))), \quad 0 \le \tau \le 1;$$
$$\delta(\tau) = \delta_{\text{crit}} - \tfrac{1}{r}\max\Big\{\textstyle\sum_{i=1}^r L_i\Big(2\sqrt{(1-\tau)(q-1)\tau_i q^{i-1}}$$
$$+(q-2)\tau_i q^{i-1}(q^{r-i+1}-1) + 2\tfrac{q-1}{q}\textstyle\sum_{k=1}^{i-1}\sqrt{\tau_k\tau_i q^{i+k}}\Big)\Big\}$$

where the maximum is taken over $\{\tau_i \ge 0;\ \sum_{i=1}^l \tau_i = \tau\}$. Then the asymptotic rate of any code family of relative distance δ satisfies $R \le R_{LP}(\delta)$ and the rate of any family of OOAs of relative strength δ satisfies $R \ge 1 - R_{LP}(\delta)$.

V. An improved bound for $r = 2$

In this section we prove a bound for codes in $\overrightarrow{H}(q,n,2)$ which improves upon the general result of the previous section. The improvement is due to the fact that in the case $r = 2$ it is possible to work with the polynomials $K_f(e)$ in their explicit form, and base the bound on the behavior of their zeros instead of the spectral radius of the operator S_κ. Namely, let $f = (f_1, f_2), e = (e_1, e_2)$. From (16) we have

$$K_f(e) = q^{f_2} k_{f_2}(n - e_2, e_1) k_{f_1}(n - f_2, e_2).$$

We use the polynomial $F(a,e) = (P(e) - P(a))U_L^2(a,e)$ with a specially designed set L in Theorem 4.1. The analysis relies on the ideas of [1], leading to

Theorem 5.1: The asymptotic rate of any family of codes of relative distance δ satisfies $R \le \Phi(\delta)$, where

$$\Phi(\delta) = \min_{\tau_1,\tau_2} {}^1\!/_2\Big\{\tau_2 + h_q(\tau_1) + (1-\tau_1)h_q\Big(\frac{\tau_2}{1-\tau_1}\Big)\Big\},$$

where the minimum is taken over all τ_1, τ_2 that satisfy

$$0 \le \tau_1 \le (q-1)/q^2, \quad 0 \le \tau_2 \le (q-1)/q$$
$$\gamma(\tau_2) + (2 - \gamma(\tau_2))(1-\tau_2)\gamma(\tau_1) \le 2\delta$$

where

$$\gamma(x) = \frac{q-1}{q} - \frac{q-2}{q}x - \frac{2}{q}\sqrt{(q-1)x(1-x)}.$$

The asymptotic rate of any family of OOAs of relative strength δ satisfies $R \ge 1 - \Phi(\delta)$.

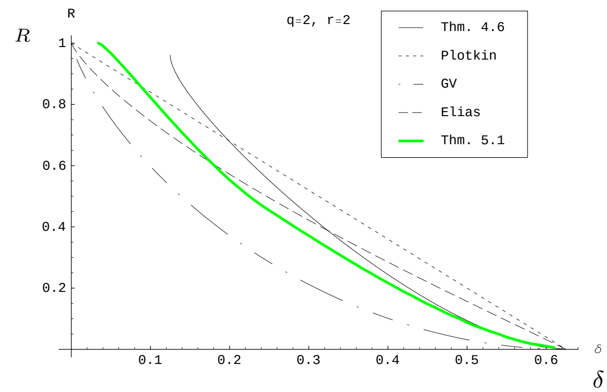

Fig. 1. Bounds for $r = 2, q = 2$

The bound of Theorem 5.1 is better than the result of Theorem 4.3 for all but large δ. For $r \ge 2$ Theorem 4.3 gives the best result for δ in this region.

Acknowledgment: A.B. is grateful to William J. Martin for calling his attention to the problem of code bounds for the NRT space.

Research supported in part by NSF grants CCF0515124, CCF0635271, and by NSA grant H98230-06-1-0044.

References

[1] M. Aaltonen, *A new upper bound on nonbinary block codes*, Discrete Mathematics **83** (1990), no. 2-3, 139–160.
[2] C. Bachoc, *Linear programming bounds for codes in Grassmannian spaces*, IEEE Trans. Inform. Theory **52** (2006), 2111–2126.
[3] E. Bannai and T. Ito, *Algebraic combinatorics I. Association schemes*, Benjamen/Cummings, London e. a., 1984.
[4] A. Barg and D. Nogin, *Spectral approach to linear programming bounds on codes*, Problems of Information Transmission **42** (2006), 12–25.
[5] J. Bierbrauer, *A direct approach to linear programming bounds*, preprint, 2006.
[6] P. Delsarte, *An algebraic approach to the association schemes of coding theory*, Philips Research Repts Suppl. **10** (1973), 1–97.
[7] S. T. Dougherty and M. M. Skriganov, *MacWilliams duality and the Rosenbloom-Tsfasman metric*, Mosc. Math. J. **2** (2002), no. 1, 81–97, 199.
[8] C. P. Dunkl and Y. Xu, *Orthogonal polynomials of several variables*, Cambridge University Press, 2001.
[9] W. J. Martin, *Linear programming bounds for ordered orthogonal arrays and (T,M,S)-nets*, Monte Carlo and quasi-Monte Carlo methods 1998 (Claremont, CA), Springer, Berlin, 2000, pp. 368–376.
[10] W. J. Martin and D. R. Stinson, *Association schemes for ordered orthogonal arrays and (T,M,S)-nets*, Canad. J. Math. **51** (1999), no. 2, 326–346.
[11] ———, *A generalized Rao bound for ordered orthogonal arrays and (t,m,s)-nets*, Canad. Math. Bull. **42** (1999), no. 3, 359–370.
[12] W. J. Martin and T. I. Visentin, *A dual Plotkin bound for (T,M,S)-nets*, IEEE Trans. Inform. Theory **53** (2007), no. 1, 411–415.
[13] H. Niederreiter, *Low-discrepancy point sets*, Monatsh. Math. **102** (1986), no. 2, 155–167.
[14] R. R. Nielsen, *A class of Sudan-decodable codes*, IEEE Trans. Inform. Theory **46** (2000), no. 4, 1564–1572.
[15] M. Yu. Rosenbloom and M. A. Tsfasman, *Codes for the m-metric*, Problems of Information Transmission **33** (1997), no. 1, 45–52.
[16] M. V. Tratnik, *Multivariable Meixner, Krawtchouk, and Meixner-Pollaczek polynomials*, J. Math. Phys. **30** (1989), no. 12, 2740–2749.