Canad. J. Math. Vol. **51** (2), 1999 pp. 326–346

Association Schemes for Ordered Orthogonal Arrays and (T, M, S)-Nets

W. J. Martin and D. R. Stinson

Abstract. In an earlier paper [10], we studied a generalized Rao bound for ordered orthogonal arrays and (T, M, S)-nets. In this paper, we extend this to a coding-theoretic approach to ordered orthogonal arrays. Using a certain association scheme, we prove a MacWilliams-type theorem for linear ordered orthogonal arrays and linear ordered codes as well as a linear programming bound for the general case. We include some tables which compare this bound against two previously known bounds for ordered orthogonal arrays. Finally we show that, for even strength, the LP bound is always at least as strong as the generalized Rao bound.

1 Association Schemes

In 1967, Sobol' introduced an important family of low discrepancy point sets in the unit cube $[0, 1)^S$. These are useful for quasi-Monte Carlo methods such as numerical integration. In 1987, Niederreiter [13] significantly generalized this concept by introducing (T, M, S)-*nets*, which have received considerable attention in recent literature (see [3] for a survey). In [7], Lawrence gave a combinatorial characterization of (T, M, S)-nets in terms of objects he called *generalized orthogonal arrays*. Independently, and at about the same time, Schmid defined *ordered orthogonal arrays* in his 1995 thesis [15] and proved that (T, M, S)-nets can be characterized as (equivalent to) a subclass of these objects. Not surprisingly, generalized orthogonal arrays and ordered orthogonal arrays are closely related. In this paper, we are interested in ordered orthogonal arrays and a dual concept, *ordered codes*. The latter turn out to be equivalent to what Rosenbloom and Tsfasman recently introduced as *codes for the m-metric* in [14].

An ordered orthogonal array is an array A having $s\ell$ columns, partitioned into s groups of size ℓ and satisfying certain balance conditions (to be specified later) based on this partition. The rows of an ordered orthogonal array form a set C of $s\ell$-tuples over an alphabet of size v whose coordinates are partitioned into s groups of size ℓ. In this initial section, we define an association scheme which, for fixed v, ℓ and s, contains each such set C as a subset of its vertices. Having done this, we will be able to apply Delsarte's theory of codes and designs in association schemes to derive new results about ordered orthogonal arrays and ordered codes.

1.1 Definitions and Basic Theory

Let X be a non-empty finite set. Let $G_1, G_2, \ldots, G_d$ be a set of undirected graphs whose edge sets partition the edge set of the complete graph on X. Define G_0 to be the identity relation. For $a, b \in X$, we say *a is k-related to b* and write $a \overset{k}{\sim} b$ to indicate that (a, b)

Received by the editors June 9, 1997; revised April 23, 1999.
AMS subject classification: Primary: 05B15; secondary: 05E30, 65C99.

https://doi.org/10.4153/CJM-1999-017-5 Published online by Cambridge University Press

is an edge of G_k. If $\mathcal{A} = \{G_0, \ldots, G_d\}$, we say the ordered pair $(X, \mathcal{A})$ is a (symmetric) *association scheme* provided the following condition holds:

- for each i, j and k satisfying $0 \leq i, j, k \leq d$, there exists a constant p_{ij}^k such that, whenever $a \overset{k}{\sim} b$, the number of $c \in X$ satisfying $c \overset{i}{\sim} a$ and $c \overset{j}{\sim} b$ is exactly p_{ij}^k.

The parameters p_{ij}^k are called the *intersection numbers* of the association scheme. Elements of X are referred to as *vertices* of the scheme.

Let $(X, \mathcal{A})$ be an association scheme. For $0 \leq i \leq d$, let A_i denote the adjacency matrix of graph G_i. Then we have a set of $d + 1$ symmetric 01-matrices satisfying the conditions

- $A_0 = I$;
- $\sum_{i=0}^{d} A_i = J$, the all-ones matrix;
- for $0 \leq i, j \leq d$, $A_i A_j$ belongs to the linear span of $\{A_0, \ldots, A_d\}$.

This gives an equivalent definition of an association scheme. In this paper, we use graph and matrix language interchangeably. Let A denote the vector space spanned by $\mathcal{A} = \{A_0, \ldots, A_d\}$. The last condition above states that A is closed under matrix multiplication. This is called the *Bose-Mesner algebra* of the association scheme.

The algebra A has a basis, $E_0, E_1, \ldots, E_d$ say, of primitive idempotents. These satisfy $E_i E_j = \delta_{i,j} E_i$. As $J \in \mathrm{A}$, one of these is a multiple of J. By convention, we take $E_0 = \frac{1}{n} J$ where n is the dimension of the matrices A_i. (In graph language, $n = |X|$.) If we let $\circ$ denote entrywise multiplication of matrices, it is easy to see that $A_i \circ A_j = \delta_{i,j} A_i$. It follows that there exist constants q_{ij}^k such that

$$E_i \circ E_j = \frac{1}{n} \sum_{k=0}^{d} q_{ij}^k E_k, \quad (0 \leq i, j \leq d).$$

These are the *Krein parameters* of the association scheme.

The transition matrices between the bases $\{A_0, \ldots, A_d\}$ and $\{E_0, \ldots, E_d\}$ are important for us. The *first eigenmatrix*, P, of the association scheme is defined by the equations

$$A_i = \sum_{j=0}^{d} P_{ji} E_j, \quad (0 \leq i \leq d).$$

The *second eigenmatrix*, Q, is defined by the equations

$$E_j = \frac{1}{n} \sum_{i=0}^{d} Q_{ij} A_i, \quad (0 \leq j \leq d)$$

and satisfies $PQ = nI$.

All relevant background material on association schemes can be found in the references. See [2, Chapter 2], [4] and [5, Chapter 12].

https://doi.org/10.4153/CJM-1999-017-5 Published online by Cambridge University Press

1.2 The Kernel Scheme

Let V be an alphabet of size v. For our purposes, it is convenient to choose $V = \mathbb{Z}_v$, but the analysis can be done using any abelian group and most of the results will hold for any alphabet.

Let $\hat{\mathbb{Z}}_v$ denote the group of characters of $\mathbb{Z}_v$. We will often use the isomorphism

$$a \mapsto \left(\hat{a} \colon \mathbb{Z}_v \to \mathbb{C} \text{ via } \hat{a}(b) = \omega^{ab}\right)$$

where ω is a primitive v-th root of unity in $\mathbb{C}$. The above isomorphism extends to an isomorphism from $\mathbb{Z}_v^\ell$ to its group of characters associating to $a = a_1 a_2 \cdots a_\ell \in \mathbb{Z}_v^\ell$ the character

$$\chi_a \colon \mathbb{Z}_v^\ell \to \mathbb{C} \text{ via } \chi_a(b_1 b_2 \cdots b_\ell) = \omega^{a_1 b_1 + \cdots + a_\ell b_\ell}.$$

Let $X = \mathbb{Z}_v^\ell$. For $1 \le k \le \ell$, define a graph G_k having X as vertex set. For $a = a_1 \cdots a_\ell$ and $b = b_1 \cdots b_\ell$ in X, we will say a is adjacent to b in G_k if $a_k \ne b_k$ but $a_j = b_j$ for all $j > k$. The edge sets of the graphs $G_1, \ldots, G_\ell$ partition the edge set of the complete graph on X. As usual, we let G_0 denote the identity relation.

Lemma 1.1 *Let i, j, and k be integers between 0 and ℓ, inclusive. For any given pair of k-related vertices $a, b \in X$, the number of vertices c which are i-related to a and j-related to b is a constant p_{ij}^k. For $k > 0$,*

$$p_{ij}^k = \begin{cases} 1, & \text{if } i = 0 \text{ and } j = k, \text{ or } j = 0 \text{ and } i = k; \\ (v-1)v^{i-1}, & \text{if } 0 \ne i < j = k \text{ or } k < i = j; \\ (v-1)v^{j-1}, & \text{if } 0 \ne j < i = k; \\ (v-2)v^{k-1}, & \text{if } i = j = k; \\ 0, & \text{otherwise.} \end{cases} \tag{1}$$

We also have $p_{ij}^0 = \delta_{i,j}(v-1)v^{i-1}$ for $i > 0$ and $p_{00}^0 = 1$. ■

As the numbers p_{ij}^k are independent of the choice of vertices a and b, the next theorem follows immediately from the definitions.

***Theorem 1.2* (cf. [16])** *The set $\mathcal{A} = \{G_0, \ldots, G_\ell\}$ forms an association scheme on X.* ■

In fact, this scheme belongs to a class (so-called "N_m-type association schemes") introduced by Yamamoto, Fujii and Hamada in 1965 [16]. We call this the *kernel scheme* and denote it by $\overleftarrow{k(\ell, v)}$. We will also be interested in the isomorphic scheme $\overrightarrow{k(\ell, v)}$ whose graph G_k contains all pairs (a, b) where $a_{\ell+1-k} \ne b_{\ell+1-k}$ but $a_j = b_j$ for all $j < \ell + 1 - k$; *i.e.*, we reverse the order of the coordinates. In fact, we will view an ordered orthogonal array as a collection of tuples of vertices of $\overrightarrow{k(\ell, v)}$. Although this association scheme is not P-polynomial, many of its intersection numbers vanish as indicated in the following corollary to Lemma 1.1.

Corollary 1.3 *For $k > \max(i, j)$, $p_{ij}^k = 0$.* ■

https://doi.org/10.4153/CJM-1999-017-5 Published online by Cambridge University Press

Each graph in $\mathcal{A}$ is a Cayley graph for the group $(\mathrm{Z}_v)^\ell$: if a is i-related to b and $c \in X$, then $a + c$ is i-related to $b + c$. Hence the characters of this group yield a complete set of eigenvectors for each graph G_i in $\mathcal{A}$ (see Lemma 12.9.2 in [5]).

We now compute the eigenvalues of the graphs G_i belonging to a particular character χ_a. Let $a = a_1 a_2 \cdots a_\ell \in \mathrm{Z}_v^\ell$. Let A_i denote the adjacency matrix of G_i in $\overrightarrow{k(\ell, v)}$. The system of equations

$$A_i \chi_a = \theta_i \chi_a, \quad (0 \leq i \leq \ell)$$

implies the following:

$$\sum_{i \leq k} \sum_{c \overset{i}{\sim} b} \chi_a(c) = (\theta_0 + \cdots + \theta_k)\chi_a(b), \quad (0 \leq k \leq \ell, b \in X).$$

The left-hand side evaluates to

$$\omega^{a_1 b_1 + \cdots + a_{\ell-k} b_{\ell-k}} \prod_{j=\ell+1-k}^{\ell} \Big(\sum_{c_j=0}^{v-1} \omega^{a_j c_j} \Big).$$

So we find

$$(\theta_0 + \cdots + \theta_k)\chi_a(b) = \begin{cases} v^k \chi_a(b), & \text{if } a_j = 0 \text{ for all } j > \ell - k; \\ 0, & \text{otherwise.} \end{cases} \tag{2}$$

Define $\mathrm{top}(a) = \max\{ j : a_j \neq 0\}$ and $\mathrm{top}(0) = 0$. The character corresponding to the all-zero tuple is the trivial character. The corresponding eigenvalues are the valencies of the graphs G_i, namely $k_0 = 1$ and $k_i = v^i - v^{i-1}$ for $i > 0$. For $a \neq 0$ having $\mathrm{top}(a) = \ell - k$, the eigenvalues are easily derived from Equation (2): they are

$$\theta_0 = 1, \theta_1 = v - 1, \ldots, \theta_k = v^k - v^{k-1}, \theta_{k+1} = -v^k, \theta_{k+2} = \cdots = \theta_\ell = 0.$$

Example For $\ell = 3$ and $v = 2$, we have

$$X = \{000, 001, 010, 011, 100, 101, 110, 111\}.$$

The adjacency matrices of $\overrightarrow{k(3, 2)}$—with the elements of X in the above order—are

$$A_0 = \begin{pmatrix} 1&0&0&0&0&0&0&0 \\ 0&1&0&0&0&0&0&0 \\ 0&0&1&0&0&0&0&0 \\ 0&0&0&1&0&0&0&0 \\ 0&0&0&0&1&0&0&0 \\ 0&0&0&0&0&1&0&0 \\ 0&0&0&0&0&0&1&0 \\ 0&0&0&0&0&0&0&1 \end{pmatrix}, \; A_1 = \begin{pmatrix} 0&1&0&0&0&0&0&0 \\ 1&0&0&0&0&0&0&0 \\ 0&0&0&1&0&0&0&0 \\ 0&0&1&0&0&0&0&0 \\ 0&0&0&0&0&1&0&0 \\ 0&0&0&0&1&0&0&0 \\ 0&0&0&0&0&0&0&1 \\ 0&0&0&0&0&0&1&0 \end{pmatrix},$$

https://doi.org/10.4153/CJM-1999-017-5 Published online by Cambridge University Press

$$A_2 = \begin{pmatrix} 0&0&1&1&0&0&0&0\\ 0&0&1&1&0&0&0&0\\ 1&1&0&0&0&0&0&0\\ 1&1&0&0&0&0&0&0\\ 0&0&0&0&0&0&1&1\\ 0&0&0&0&0&0&1&1\\ 0&0&0&0&1&1&0&0\\ 0&0&0&0&1&1&0&0 \end{pmatrix}, \; A_3 = \begin{pmatrix} 0&0&0&0&1&1&1&1\\ 0&0&0&0&1&1&1&1\\ 0&0&0&0&1&1&1&1\\ 0&0&0&0&1&1&1&1\\ 1&1&1&1&0&0&0&0\\ 1&1&1&1&0&0&0&0\\ 1&1&1&1&0&0&0&0\\ 1&1&1&1&0&0&0&0 \end{pmatrix}.$$

The characters are the columns of the Hadamard matrix

$$C = \begin{pmatrix} 1&1&1&1&1&1&1&1\\ 1&-1&1&-1&1&-1&1&-1\\ 1&1&-1&-1&1&1&-1&-1\\ 1&-1&-1&1&1&-1&-1&1\\ 1&1&1&1&-1&-1&-1&-1\\ 1&-1&1&-1&-1&1&-1&1\\ 1&1&-1&-1&-1&-1&1&1\\ 1&-1&-1&1&-1&1&1&-1 \end{pmatrix}.$$

The matrix M below has (a,i) entry equal to the eigenvalue of A_i belonging to the character χ_a:

$$M = \begin{pmatrix} 1&1&2&4\\ 1&-1&0&0\\ 1&1&-2&0\\ 1&-1&0&0\\ 1&1&2&-4\\ 1&-1&0&0\\ 1&1&-2&0\\ 1&-1&0&0 \end{pmatrix}. \qquad \blacksquare$$

We summarize the general situation in the following

Lemma 1.4

1. *For $a, b \in X$, write*
$$A_i\chi_a = \theta_i\chi_a \quad \text{and} \quad A_i\chi_b = \tau_i\chi_b$$
for $0 \le i \le \ell$. Then $\theta_i = \tau_i$ for all i if and only if $\operatorname{top}(a) = \operatorname{top}(b)$.
2. *The primitive idempotents [2, p. 45] of the association scheme $\overrightarrow{k(\ell, v)}$ are*
$$E_j = \frac{1}{v^\ell} \sum_{\operatorname{top}(a)=j} \chi_a\chi_a^T, \quad (0 \le j \le \ell).$$
3. *The first eigenmatrix P of $\overrightarrow{k(\ell, v)}$ is given by*
$$P_{ji} = \begin{cases} 1, & \text{if } i = 0;\\ v^i - v^{i-1}, & \text{if } 0 < i \le \ell - j;\\ -v^{i-1}, & \text{if } i + j = \ell + 1;\\ 0, & \text{if } i + j > \ell + 1. \end{cases} \qquad \blacksquare$$

https://doi.org/10.4153/CJM-1999-017-5 Published online by Cambridge University Press

For example, for $\overrightarrow{k(3,5)}$, we have

$$P = \begin{pmatrix} 1 & 4 & 20 & 100 \\ 1 & 4 & 20 & -25 \\ 1 & 4 & -5 & 0 \\ 1 & -1 & 0 & 0 \end{pmatrix}.$$

The i-th column of P lists the eigenvalues of graph G_i. As each G_i ($i \neq 0$) can be expressed as a disjoint union of pairwise isomorphic complete multipartite graphs, the eigenvalues of G_i are its valency, zero, and the negative of the size of a maximal coclique in one of its components (see [2, Thm. 1.3.1(v)]).

The number of tuples a satisfying $\mathrm{top}(a) = j$ is $v^j - v^{j-1}$ (except when $j = 0$). Using Lemma 1.4(2), rank E_j is thus given by

$$m_j = v^j - v^{j-1}$$

and $m_0 = 1$. These are the *multiplicities* of the association scheme. We see that the j-th multiplicity is equal to the j-th valency. In fact, we have

Lemma 1.5 *The association scheme $\overrightarrow{k(\ell,v)}$ is formally self-dual.*

Proof Let K denote the $(\ell+1) \times (\ell+1)$ diagonal matrix with i-th diagonal entry equal to k_i and let M denote the diagonal matrix with j-th diagonal entry equal to m_j. A well-known formula for the second eigenmatrix $Q = |X|P^{-1}$ of the association scheme (see, *e.g.*, Lemma 2.2.1(iv) in [2] or p. 226 in [5]) is

$$MP = Q^T K.$$

Using the above, it is easy to prove that

$$m_j P_{ji} = P_{ij} k_i,$$

showing $Q = P$. That is, the scheme $(X, \mathcal{A})$ is formally self-dual [2, p. 49]. ■

In fact, the pair $\overrightarrow{k(\ell,v)}$ and $\overleftarrow{k(\ell,v)}$ form a pair of dual association schemes (see Theorem 2.9 in [4]). This will allow us to extend concepts from linear coding theory to these schemes.

1.3 The Ordered Hamming Scheme

We now construct the ordered Hamming scheme as a symmetrization of the s-fold product of the scheme $(X, \mathcal{A}) = \overrightarrow{k(\ell,v)}$.

In [4, Section 2.5], Delsarte makes the following observation. If $(X, \mathcal{A})$ is a d-class association scheme, then, for any positive integer s, we may build an association scheme on X^s

https://doi.org/10.4153/CJM-1999-017-5 Published online by Cambridge University Press

as follows. For vertices $a = (a^{(1)}, \ldots, a^{(s)})$ and $b = (b^{(1)}, \ldots, b^{(s)})$, the relation joining a to b in the new scheme is the $(d+1)$-tuple $e = (e_0, e_1, \ldots, e_d)$ defined by

$$e_j = |\{k : 1 \le k \le s, a^{(k)} \overset{j}{\sim} b^{(k)}\}|.$$

Delsarte calls this the *extension of length s* of the scheme $\overrightarrow{k(\ell, v)}$ and observes that it forms an association scheme. In [6], a proof of this result is given which provides extra information needed for our application.

We now apply this construction to the kernel scheme $\overrightarrow{k(\ell, v)}$. For an s-tuple $\mathbf{i} = (i_1, i_2, \ldots, i_s)$ over $\{0, 1, \ldots, \ell\}$, define the *shape* of $\mathbf{i}$ by

$$\mathrm{shape}(\mathbf{i}) = (e_0, e_1, \ldots, e_\ell)$$

where $e_j = |\{k : i_k = j\}|$. For each $\mathbf{i}$, $\mathrm{shape}(\mathbf{i})$ is an ordered $(\ell+1)$-tuple whose entries sum to s. Our new association scheme has 01-basis $\mathcal{A}_s$ consisting of matrices

$$\mathsf{A}_e := \sum_{\mathrm{shape}(\mathbf{i})=e} A_{i_1} \otimes A_{i_2} \otimes \cdots \otimes A_{i_s}$$

where e is any ordered $(\ell+1)$-tuple of non-negative integers whose entries sum to s. Since the kernel scheme is self-dual, Godsil's refinement of Delsarte's observation gives us

***Theorem 1.6* ([6])** *$(Y, \mathcal{A}_s)$ is an association scheme which is also formally self-dual.* ■

We call this the *ordered Hamming scheme* and denote it as $\overrightarrow{H}(s, \ell, v)$. The first eigenmatrix P of this scheme is obtained from the s-fold Kronecker product $P^{\otimes s}$ by summing columns indexed by tuples of equal shape and subsequently deleting repeated rows. Concretely, if e and f are ordered $(\ell+1)$-tuples summing to s and if $\mathbf{j} = (j_1, \ldots, j_s)$ has shape f, we have

$$\mathsf{P}_{fe} = \sum_{\mathrm{shape}(\mathbf{i})=e} \prod_{k=1}^{s} P_{j_k i_k}. \tag{3}$$

A more efficient way to generate P is as follows. Let $\mathbf{z} = [z_0, z_1, \ldots, z_\ell]^T$. Then $P\mathbf{z}$ is the vector of length $\ell + 1$ having entries

$$z_0 + (v-1)z_1 + \cdots + (v^\ell - v^{\ell-1})z_\ell, \ldots,$$
$$z_0 + (v-1)z_1 + \cdots + (v^j - v^{j-1})z_j - v^j z_{j+1}, \ldots,$$
$$z_0 - z_1.$$

It is straightforward to see that

$$\mathsf{P}_{fe} = [z_0^{e_0} \cdots z_\ell^{e_\ell}] \prod_{k=1}^{s} (P\mathbf{z})_{j_k}, \tag{4}$$

https://doi.org/10.4153/CJM-1999-017-5 Published online by Cambridge University Press

where $[m(\mathbf{z})]g(\mathbf{z})$ denotes the coefficient of the monomial $m(\mathbf{z})$ in the polynomial $g(\mathbf{z})$.

The vertex set Y of $\overrightarrow{H}(s,\ell,v)$ consists of all s-tuples of ℓ-tuples over Z_v; *i.e.*, $(s\ell)$-tuples partitioned into s groups size ℓ. If $a=(a^{(1)},a^{(2)},\ldots,a^{(s)})$ belongs to Y with each $a^{(i)}\in\mathrm{Z}_v^{\ell}$ now, we define

$$\mathrm{profile}(a) := \bigl(\mathrm{top}(a^{(1)}),\ldots,\mathsf{top}(a^{(s)})\bigr),$$

and we define

$$\mathrm{shape}(a) := \mathrm{shape}\bigl(\mathrm{profile}(a)\bigr).$$

Each shape e is an ordered partition of s. It is straightforward to check that, for $a,b\in Y$, $a\overset{e}{\sim}b$ in $\overrightarrow{H}(s,\ell,v)$ if and only if $\mathrm{shape}(a-b)=e$.

Let $a\in Y$ and let ψ_a be the corresponding character of Y. Then, for $b\in Y$,

$$\psi_a(b)=\prod_{i=1}^{s}\prod_{j=1}^{\ell}\omega^{a_j^{(i)}b_j^{(i)}}.$$

Using these characters, we now compute the eigenvalues of the ordered Hamming scheme.

Theorem 1.7

1. *Let $a\in Y$ and let e be an ordered $(\ell+1)$-tuple of non-negative integers summing to s. Then*

$$\mathsf{A}_e\psi_a=\mathsf{P}_{fe}\psi_a$$

   where $f=\mathrm{shape}(a)$.
2. *Two $(s\ell)$-tuples have identical shape if and only if the corresponding characters give rise to identical eigenvalues.*
3. *The primitive idempotents for the Bose-Mesner algebra of $(Y,\mathcal{A}_s)$ are*

$$\mathsf{E}_f=\frac{1}{v^{s\ell}}\sum_{\mathrm{shape}(a)=f}\psi_a\psi_a^T,$$

   as f ranges over the $(\ell+1)$-tuples of non-negative integers summing to s. ∎

In fact, the association scheme $\overrightarrow{H}(s,\ell,v)$ has a dual: it is simply the group of characters of Y with relations determined by the behaviour of the various eigenvectors (see Section 2.6 in [4]). This scheme also has one relation for each shape e. Specifically, if χ is the character corresponding to the $(s\ell)$-tuple a and ψ is the character corresponding to the $(s\ell)$-tuple b, we have $\chi\overset{e}{\sim}\psi$ if $\mathrm{shape}(a-b)=e$ where we redefine top to count coordinate positions from right to left. Aside from the ordering of the coordinates within each group of ℓ coordinates, this second scheme, $\overleftarrow{H}(s,\ell,v)$, is identical to the ordered Hamming scheme $\overrightarrow{H}(s,\ell,v)$.

https://doi.org/10.4153/CJM-1999-017-5 Published online by Cambridge University Press

2 Ordered Codes and Ordered Orthogonal Arrays

Let us briefly recall the classical concepts on which these extensions are based.

For codes, we are interested in the minimum distance. Let C be a v-ary code of length k having m elements. View these as rows of an $m \times k$ array A. We say C has minimum distance d if d is the smallest number of columns of A we must delete in order that the resulting subarray has repeated rows.

Let A be an $m \times k$ array over V. If R is a subset of the columns of A, we say A is *balanced* with respect to R if the subarray obtained by restricting to those columns in R contains every $|R|$-tuple of symbols exactly $m/v^{|R|}$ times as a row. We say A is an *orthogonal array* (OA) of strength *at least* t if A is balanced with respect to any subset of t of its columns.

The following standard lemma will be useful to us.

Lemma 2.1 **(*cf.* [4, Theorem 4.4])** *Let A be an array over $\mathbb{Z}_v$ with k columns and let C denote the set of rows of A, viewed as a subset of $\mathbb{Z}_v^k$. For a subset R of $\{1, \ldots, k\}$, A is balanced with respect to R if and only if*

$$\sum_{c \in C} \chi_a(c) = 0$$

for every non-trivial character χ_a of $\mathbb{Z}_v^k$ such that the support of a is contained in R. ■

Let A be an $m \times s\ell$ array over V which satisfies the following properties:

1. The columns are partitioned into s groups of ℓ columns, denoted $G_1, \ldots, G_s$ (each G_i consists of ℓ columns);
2. Let $(t_1, \ldots, t_s)$ be an s-tuple of non-negative integers such that

$$0 \leq t_i \leq \ell \text{ for } 1 \leq i \leq s, \quad \text{and} \quad \sum_{i=0}^{s} t_i = t.$$

   If R is the set of columns of A obtained by taking the first t_i columns within each group G_i ($1 \leq i \leq s$), then A is balanced with respect to R.

Then we say that A is an *ordered orthogonal array* of strength at least t. Clearly $m = \lambda v^t$. We use the notation $\mathrm{OOA}_\lambda(t, s, \ell, v)$. The *ordered strength* of a subset C of Y is the largest integer t for which these conditions hold when C is viewed as the set of rows of an array.

Let $C \subseteq Y$ with m elements. Associate to C, in the natural way, an $m \times s\ell$ array A over V. Suppose A satisfies property (1) above and:

3. Let $(d_1, \ldots, d_s)$ be an s-tuple of non-negative integers such that

$$0 \leq d_i \leq \ell \text{ for } 1 \leq i \leq s, \quad \text{and} \quad \sum_{i=0}^{s} d_i < d.$$

   If B is the subarray of A obtained by restricting, within each group G_i of columns, to the first $\ell - d_i$ columns of G_i ($1 \leq i \leq s$), then the rows of B are all distinct.

Then we say that C is an *ordered code* with *ordered minimum distance at least d*. Thus, the *ordered distance* of C is the smallest number, d, of coordinates (right-justified within each group) we are required to delete in order to obtain repeated rows. Independently, Rosenbloom and Tsfasman defined *codes for the m-metric* which are equivalent to what we are calling ordered codes. See [14] for a definition as well as an application to shared communication channels.

It is easy to see from the definitions that $d+t \le s\ell$ if $m > v^t$ and $d+t \le s\ell+1$ if $m = v^t$.

Observe that the classical objects reviewed at the start of this section are obtained by taking $\ell = 1$ in these definitions.

Let C be an additive subgroup of $Y = (\mathrm{Z}_v^\ell)^s$ (*i.e.*, a v-ary additive code of length $s\ell$). The *dual code* of C is the subgroup $C^\perp$ of $(\hat{\mathrm{Z}}_v^\ell)^s$ given by

$$C^\perp = \{\chi \in (\hat{\mathrm{Z}}_v^\ell)^s : \chi(c) = 1, \forall c \in C\}.$$

2.1 The Connection with (T, M, S)-Nets

Let $S \ge 1$ and $v \ge 2$ be integers. An *elementary interval* in base v is a subset of $[0,1)^S$ of the form

$$E = \prod_{i=1}^{S} \left[a_i v^{-d_i}, (a_i + 1) v^{-d_i}\right),$$

where a_i and d_i are non-negative integers such that $a_i < v^{d_i}$ for $1 \le i \le S$. The *volume* of E is

$$\prod_{i=1}^{S} v^{-d_i} = v^{-\sum_{i=1}^{S} d_i}.$$

For integers $0 \le T \le M$, a (T, M, S)-*net* in base v is a set $\mathcal{N}$ of v^M points in $[0,1)^S$ such that every elementary interval E in base v having volume v^{T-M} contains exactly v^T points of $\mathcal{N}$. Since their introduction by Niederreiter [13] in 1987, there has been a considerable amount of research done on (T, M, S)-nets. For a good summary of known results, see [12] and [3]. The key result for us is the following theorem, due to Schmid [15] (*cf.* Lawrence [7]), which shows that (T, M, S)-nets correspond to ordered orthogonal arrays with $t = \ell$.

***Theorem 2.2* (Lawrence/Schmid)** *There exists a (T, M, s)-net in base v if and only if there exists an* $\mathrm{OOA}_\lambda(t, s, \ell, v)$ *where $\ell = t = M - T$ and $\lambda = v^T$.* ∎

The basic idea is to transform an OOA into a net by placing decimal points at the beginning of each group of ℓ columns in each row and interpreting each ℓ-tuple as a real number in $[0,1)$ in radix v notation.

On the other hand, an ordered code $C \subseteq (\mathrm{Z}_v^\ell)^s$ corresponds in the same way to a (T, M, s)-*packing* in base v: a subset $\mathcal{P} \subseteq I^s$ of v^M points such that any elementary interval J of volume at most v^{T-M} contains at most one point of $\mathcal{P}$.

Theorem 2.3 *There exists a (T, M, s)-packing in base v if and only if there exists an ordered code C in $\overrightarrow{H}(s, M - T, v)$ having $|C| = v^M$ and ordered distance $d > (s-1)(M-T)$.* ∎

https://doi.org/10.4153/CJM-1999-017-5 Published online by Cambridge University Press

In the language of nets and packings, we have obvious bounds on these objects. Since I^S can be partitioned into v^k elementary intervals of volume v^{-k}, we must have $|\mathcal{N}| \geq v^{M-T}$ and $|\mathcal{P}| \leq v^{M-T}$ for a (T, M, S)-net $\mathcal{N}$ and a (T, M, S)-packing $\mathcal{P}$.

3 MacWilliams Theorem

A recent result of Godsil [6] enables us to write down MacWilliams-type identities for any association scheme constructed in the manner described in Section 1.3. In our case, the kernel scheme, $\overrightarrow{k(\ell, v)}$, has a dual scheme and each additive code has a dual as well. The results of [6] are particularly suited to this case.

The association scheme $(Y, \mathcal{A}_s)$ has one relation for each shape $e = [e_0, \ldots, e_\ell]$ where each $e_i \geq 0$ and $\sum e_i = s$. Similarly, we have one primitive idempotent for each such $(\ell + 1)$-tuple e. Let $C \subseteq Y$ have characteristic vector $x = x_C$, a 01-vector of length $|Y|$. To C we associate the multivariate *weight enumerator* (or "distance enumerator")

$$W_C(\mathbf{z}) = \frac{1}{|C|} \sum_e (x^T \mathsf{A}_e x) z_0^{e_0} z_1^{e_1} \cdots z_\ell^{e_\ell}.$$

This sum is taken over all monomials

$$m(\mathbf{z}) = z_0^{e_0} z_1^{e_1} \cdots z_\ell^{e_\ell}$$

of total degree s in the variables $\mathbf{z} = [z_0, z_1, \ldots, z_\ell]^T$. In the special case when C is an additive subgroup of Y, the coefficient of $m(\mathbf{z})$ is the number of elements a of C satisfying $\operatorname{shape}(a) = e$. We also have a *dual weight enumerator*

$$W_C^\perp(\mathbf{z}) = \frac{v^{s\ell}}{|C|^2} \sum_f (x^T \mathsf{E}_f x) z_0^{f_0} z_1^{f_1} \cdots z_\ell^{f_\ell}.$$

Let P be the first eigenmatrix of the association scheme $\overrightarrow{k(\ell, v)}$, given in Lemma 1.4.

Proposition 3.1 **(Godsil)**

$$W_C^\perp(\mathbf{z}) = \frac{1}{|C|} W_C(P\mathbf{z}). \qquad \blacksquare$$

(We are using the fact that the association scheme $(X, \mathcal{A})$ is formally self-dual and hence $P^{-1} = (1/v^\ell)P$.) Observe that, since $x^T \mathsf{E}_f x \geq 0$ for each shape f, the coefficients of the polynomial $W_C^\perp(\mathbf{z})$ must all be non-negative. This is equivalent to the linear programming bound which will be investigated in the next section.

Now suppose C is an additive code in Y. Then, as noted earlier, we have a dual code $C^\perp$ which is a subgroup of the group of characters of Y. We can view $C^\perp$ as a code in $\overleftarrow{H}(s, \ell, v)$. So we have a weight enumerator for $C^\perp$ as well, where top is redefined to count from right to left. Applying Theorem 4.1 in [6] (*cf.* Theorem 2.10.12 in [2]), we have

Proposition 3.2 *If $C \subseteq Y$ is an additive code in $\overrightarrow{H}(s, \ell, v)$ and $C^\perp$ is the dual code in $\overleftarrow{H}(s, \ell, v)$, then*

$$W_C^\perp(\mathbf{z}) = W_{C^\perp}(\mathbf{z}). \qquad \blacksquare$$

https://doi.org/10.4153/CJM-1999-017-5 Published online by Cambridge University Press

This answers a question posed by Adams [1, p. 69].

Recall that the ordered distance of C in $\overrightarrow{H}(s,\ell,v)$ (resp., $\overleftarrow{H}(s,\ell,v)$) is the largest integer d such that upon deletion of any $d-1$ coordinates right-justified within each group G_i (resp., left-justified), the rows of the resulting subarray remain pairwise distinct. For a monomial $m(\mathbf{z}) = z_0^{e_0}\cdots z_\ell^{e_\ell}$ and for the corresponding shape $e = (e_0, e_1, \ldots, e_\ell)$, define the *height* as follows:

$$\operatorname{height}\bigl(m(\mathbf{z})\bigr) = \operatorname{height}(e) = \sum_{i=0}^{\ell} i e_i.$$

We pause here to remark that, in [14], Rosenbloom and Tsfasman observe that the function $\partial(a,b) = \operatorname{height}\bigl(\operatorname{shape}(a-b)\bigr)$ defines a metric on Y.

The next two results apply to arbitrary subsets C of Y, not just to additive subgroups.

Lemma 3.3 *Let C be any non-empty subset of $\overleftarrow{H}(s,\ell,v)$. Then C has minimum distance at least d if and only if its weight enumerator includes no monomials of non-zero height less than d.*

Proof Suppose there is such a monomial with a non-zero coefficient. Then there exist a pair $a, b \in C$ such that $a \overset{e}{\sim} b$. So the tuple $a-b$ has profile $\mathbf{i} = (i_1, i_2, \ldots, i_s)$ for some $\mathbf{i}$ such that

$$\operatorname{shape}(\mathbf{i}) = (e_0, e_1, \ldots, e_\ell).$$

Hence upon deletion of the last i_j coordinates from the j-th group ($j = 1, 2, \ldots, s$), the remaining coordinates of $a-b$ are all zero. That is, the resulting subarray has two identical rows. But we have deleted fewer than d coordinates in total. This contradicts our hypothesis. The proof of the converse is left to the reader. ■

Using Lemma 2.1, we obtain a similar characterization of ordered orthogonal arrays.

Theorem 3.4 *Let A be an array with m distinct rows and $s\ell$ columns, partitioned into s groups $G_1, G_2, \ldots, G_s$ of size ℓ. Let $C \subseteq Y$ be the set of rows of A. Then C is an ordered orthogonal array of strength at least t if and only if its dual weight enumerator includes no monomials of non-zero height less than or equal to t.*

Proof Suppose A has ordered strength strictly less than t. Then there is a set $R = R_1 \cup \cdots \cup R_s$ of t columns where: (1) each R_i consists of the first $|R_i|$ columns of G_i, and (2) A is *not* balanced with respect to R. By Lemma 2.1, there exists a non-trivial character $\psi = \psi_a$ with support contained in R such that $x_C^T\psi \neq 0$ (ψ is an eigenvector of $\overrightarrow{H}(s,\ell,v)$). If

$$\operatorname{shape}(a) = (f_0, f_1, \ldots, f_\ell),$$

then by Theorem 1.7 the idempotent E_f can be expressed as $\mathsf{E}_f = \psi\psi^T + \mathsf{F}$ where F is a positive semidefinite matrix. Therefore, as $x^T\psi\psi^T x > 0$, we have $x^T\mathsf{E}_f x > 0$ and $0 < f_0 + f_1 + \cdots + f_\ell < t$. The proof of the converse is left to the reader. ■

Corollary 3.5 *Let C be an additive code in $\overrightarrow{H}(s,\ell,v)$ and let $C^{\perp}$ be its dual code in $\overleftarrow{H}(s,\ell,v)$. Then C has ordered strength at least t if and only if $C^{\perp}$ has ordered distance at least $t+1$.* ■

Example Below is an additive code C in $(\mathbb{Z}_2^2)^2$ and its dual, $C^{\perp}$. In $\overrightarrow{H}(s,\ell,v)$, C forms an ordered orthogonal array of strength two and in $\overleftarrow{H}(s,\ell,v)$, $C^{\perp}$ has ordered distance three.

$$C = \begin{array}{|cc|cc|} \hline 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ \hline \end{array} \qquad C^{\perp} = \begin{array}{|cc|cc|} \hline 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ \hline \end{array}$$

In $\overrightarrow{H}(s,\ell,v)$, we have

$$W_C(\mathbf{z}) = z_0^2 + 2z_1z_2 + z_2^2.$$

The MacWilliams transform of Proposition 3.1 gives

$$W_C^{\perp}(\mathbf{z}) = z_0^2 + 2z_1z_2 + z_2^2,$$

which is identical to $W_{C^{\perp}}(\mathbf{z})$ in $\overleftarrow{H}(s,\ell,v)$. If one accounts for the reordering of coordinates, C is a "self-dual" code. ■

Example The following is an $\mathrm{OOA}_1(3,3,3,2)$:

$$A = \begin{array}{|ccc|ccc|ccc|} \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ \hline \end{array}$$

It can be viewed as a binary linear code of length nine with generator matrix

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

If C denotes the set of rows of A, then C as a subset of $\overrightarrow{H}(3,3,2)$ has weight enumerator

$$W_C(\mathbf{z}) = z_0^3 + 3z_1z_3^2 + 3z_2^2z_3 + z_3^3.$$

The MacWilliams transform of Proposition 3.1 is

$$W_C^{\perp}(\mathbf{z}) = z_0^3 + z_2^3 + 8z_3^3 + 6z_0z_1z_3 + 6z_0z_2z_3 + 6z_1z_2z_3 + 3z_0z_2^2 \\ + 6z_0z_3^2 + 3z_1^2z_2 + 6z_1z_3^2 + 6z_2^2z_3 + 12z_2z_3^2.$$

https://doi.org/10.4153/CJM-1999-017-5 Published online by Cambridge University Press

By Proposition 3.2, this is also the weight enumerator of $C^{\perp}$, namely, the row space of the matrix

$$H = \begin{pmatrix} 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Since $W_C(\mathbf{z})$ includes no monomial of (non-zero) height less than seven, C has ordered distance seven (Lemma 3.3). That is, we must delete seven or more right-justified columns in order to obtain repeated rows. Since $W_C^{\perp}(\mathbf{z})$ includes no monomial of non-zero height less than four, Theorem 3.4 guarantees that C has ordered strength 3. We have $d = 7$ and $t = 3$, so C achieves the bound $t + d \leq s\ell + 1$ with equality.

4 Linear Programming Bounds

Let C be a non-empty subset of $Y = (\mathbb{Z}_v^{\ell})^s$ with characteristic vector x. Then

$$x^T \mathsf{E}_f x \geq 0 \tag{5}$$

for each shape f since each E_f is a symmetric idempotent matrix. This is the standard approach to Delsarte's linear programming bound [4, Thm. 3.3].

Let $\mathbf{a}$ be the *inner distribution* vector of C. This is simply the vector of coefficients of the weight enumerator. We have

$$a_e = \frac{1}{|C|} x^T \mathsf{A}_e x.$$

Since the association scheme is formally self-dual,

$$\mathsf{E}_f = \frac{1}{|Y|} \sum_e \mathsf{P}_{fe} \mathsf{A}_e \tag{6}$$

where e and f are $(\ell + 1)$-tuples of non-negative integers summing to s. Putting Equations (5) and (6) together, we have the constraints for our linear program:

$$\begin{aligned} \mathbf{a}\mathsf{P} &\geq 0, \\ \mathbf{a} &\geq 0. \end{aligned} \tag{7}$$

The entries of P are computed using the formulas in Equations (3) and (4).

Now suppose one wishes to find the largest ordered code with a given ordered distance d. Then by Lemma 3.3, one has the additional constraints

$$a_e = 0 \quad \text{for all shapes } e \text{ with } 0 < \text{height}(e) < d. \tag{8}$$

If zero is used to denote the index $e = [s, 0, \ldots, 0]$ of the identity relation, one would then set $a_0 = 1$ and maximize $|C|$ (*i.e.*, the sum of the entries of $\mathbf{a}$) subject to these constraints together with those in (7).

On the other hand, one might want to use (7) to obtain bounds on the size of an ordered orthogonal array with a given ordered strength t. In this case, Theorem 3.4 gives the additional constraints

$$(\mathbf{a}\mathsf{P})_e = 0 \quad \text{for all shapes } e \text{ with } 0 < \text{height}(e) \leq t. \tag{9}$$

One then sets $a_0 = 1$ and minimizes the sum of the entries of $\mathbf{a}$.

We now present two new bounds that we proved using this linear programming approach.

Theorem 4.1 *The largest value of s for which a ternary $(1,5,s)$-net exists is $s = 8$.*

Proof In [3], it is indicated that a ternary $(1,5,8)$-net exists and that no ternary $(1,5,11)$-net exists. The results in our paper [10] show that no ternary $(1,5,10)$-net exists. The only value remaining, therefore, is $s = 9$. If a ternary $(1,5,9)$-net exists, then by Theorem 2.2 there also exists an $\mathrm{OOA}_3(4,9,4,3)$. Such an array would have $3^5 = 243$ rows. The linear programming approach outlined above gives us a lower bound of 245.25 on the number of rows in such an array. Thus, no ternary $(1,5,9)$-net exists. (The computation, performed by R. Bixby at Rice University, involves a linear program having 714 variables and constraints.) ■

Theorem 4.2 *The largest value of s for which a ternary $(1,7,s)$-net exists is $s = 7$.*

Proof From the tables in [3], we know that a ternary $(1,7,7)$-net exists and that no ternary $(1,7,9)$-net exists. While the generalized Rao bound only tells us that $s \leq 9$ in this case, the linear programming bound rules out a ternary $(1,7,8)$-net. ■

In general, the linear program for an $\mathrm{OOA}(t,s,\ell,v)$ involves $\binom{s+\ell}{\ell} - 1$ variables and constraints. Let $LP^*(t,s,\ell,v)$ denote the optimal value of this linear program. Clearly, by simply deleting columns, one may transform an $\mathrm{OOA}(t,s,\ell,v)$ into an $\mathrm{OOA}(t,s,\ell',v)$ for any ℓ' satisfying $1 \leq \ell' \leq \ell$. The following inequality is a bit more subtle, yet intuitively obvious.

Proposition 4.3 *$LP^*(t,s,\ell',v) \;\leq\; LP^*(t,s,\ell,v)$ for $1 \leq \ell' \leq \ell$.*

Proof If P is the first eigenmatrix for the kernel scheme $\overrightarrow{k(\ell,v)}$, then, by Lemma 1.4, $P_{0i} = P_{1i}$ for all $i < \ell$. Now consider the first eigenmatrix P for the ordered Hamming scheme $\overrightarrow{H}(s,\ell,v)$. Suppose e, f and g are $(\ell+1)$-tuples of non-negative integers summing to s such that $e_\ell = 0$, and $f_k = g_k$ for all $k \geq 2$. Then, from Equation (3),

$$\mathsf{P}_{fe} = \mathsf{P}_{ge}. \tag{10}$$

The first eigenmatrix P' for $\overrightarrow{H}(s,\ell-1,v)$ is a submatrix of P which can be obtained by deleting all rows indexed by shapes f having $f_0 > 0$ and all columns indexed by shapes e

https://doi.org/10.4153/CJM-1999-017-5 Published online by Cambridge University Press

having $e_\ell > 0$. (See Lemma 1.4 and the example following it.) Specifically, for an $(\ell + 1)$-tuple e, define

$$e_* = [e_1, e_2, \ldots, e_\ell] \quad \text{and} \quad e^* = [e_0, e_1, \ldots, e_{\ell-1}].$$

Then, for $f_0 = 0$ and $e_\ell = 0$, we have

$$\mathsf{P}'_{f_* e^*} = \mathsf{P}_{fe}.$$

As an example, we give the P matrix for $\overrightarrow{H}(2,3,5)$ with the corresponding matrix P' for $\overrightarrow{H}(2,2,5)$ highlighted:

$$\begin{pmatrix}
1 & 8 & 40 & 200 & 16 & 160 & 800 & 400 & 4000 & 10000 \\
1 & 8 & 40 & 75 & 16 & 160 & 300 & 400 & 1500 & -2500 \\
1 & 8 & 15 & 100 & 16 & 60 & 400 & -100 & -500 & 0 \\
1 & 3 & 20 & 100 & -4 & -20 & -100 & 0 & 0 & 0 \\
\mathbf{1} & \mathbf{8} & \mathbf{40} & -50 & \mathbf{16} & \mathbf{160} & -200 & \mathbf{400} & -1000 & 625 \\
\mathbf{1} & \mathbf{8} & \mathbf{15} & -25 & \mathbf{16} & \mathbf{60} & -100 & \mathbf{-100} & 125 & 0 \\
\mathbf{1} & \mathbf{3} & \mathbf{20} & -25 & \mathbf{-4} & \mathbf{-20} & 25 & \mathbf{0} & 0 & 0 \\
\mathbf{1} & \mathbf{8} & \mathbf{-10} & 0 & \mathbf{16} & \mathbf{-40} & 0 & \mathbf{25} & 0 & 0 \\
\mathbf{1} & \mathbf{3} & \mathbf{-5} & 0 & \mathbf{-4} & \mathbf{5} & 0 & \mathbf{0} & 0 & 0 \\
\mathbf{1} & \mathbf{-2} & \mathbf{0} & 0 & \mathbf{1} & \mathbf{0} & 0 & \mathbf{0} & 0 & 0
\end{pmatrix}.$$

The indices of the rows and columns are ordered as follows:

[2000], [1100], [1010], [1001], [0200], [0110], [0101], [0020], [0011], [0002].

Let $\mathbf{a}$ be any feasible solution to the linear program given by (7) and (9). Define a new vector $\mathbf{a}'$ whose entries are indexed by the ℓ-tuples of non-negative integers summing to s. For such a shape $f = [f_0, f_1, \ldots, f_{\ell-1}]$, define

$$a'_f = \sum_{e=[e_0,e_1,f_1,\ldots,f_{\ell-1}]} a_e.$$

Continuing with the above example, the vector

$$\mathbf{a} = [1\ \ 4\ \ 4\ \ 20\ \ 0\ \ 16\ \ 80\ \ 0\ \ 0\ \ 0]$$

which satisfies (7) for $\overrightarrow{H}(2,3,5)$ is sent under this mapping to

$$\mathbf{a}' = [5\ \ 20\ \ 100\ \ 0\ \ 0\ \ 0]$$

which satisfies (7) for $\overrightarrow{H}(2,2,5)$.

In general, Equation (10)—together with the relationships between P and P' and between $\mathbf{a}$ and $\mathbf{a}'$—implies that $\mathbf{a}'\mathsf{P}' \geq 0$ and $(\mathbf{a}'\mathsf{P}')_e = 0$ for all shapes e of non-zero height at most t. Clearly, $\mathbf{a}' \geq 0$. Now $a'_0 \geq 1$ and if $a'_0 \neq 1$, we may divide all entries by a'_0 preserving the other three properties. In this way, we obtain from any feasible solution $\mathbf{a}$ to

https://doi.org/10.4153/CJM-1999-017-5 Published online by Cambridge University Press

the linear program for an $\mathrm{OOA}(t,s,\ell,v)$ a feasible solution $\mathbf{a}'$ to the linear program for an $\mathrm{OOA}(t,s,\ell-1,v)$ having the property that the sum of the entries of $\mathbf{a}'$ is less than or equal to the sum of the entries of $\mathbf{a}$. Minimizing this sum over the two solution spaces, we obtain the desired inequality for $\ell' = \ell - 1$. By induction, we are done. ■

This result tells us that we can use a smaller value of ℓ to obtain a smaller (and hence easier to solve) LP, which in general will yield a weaker bound. For example, by reducing ℓ to 1, we end up with the usual linear programming bound for (ordinary) orthogonal arrays. This observation was employed to obtain the bounds in [3], among other techniques. In fact, the bounds in [3] are the result of a complex and lengthy process.

It is an interesting question to ask how the LP bounds vary as ℓ is decreased. As an example relating to Theorem 4.1, we used MAPLE to show that $LP^*(4,9,2,3) = 245.25$. Thus, it happens that $LP^*(4,9,2,3) = LP^*(4,9,4,3)$, so the LP bound does not change when ℓ is reduced from 4 to 2. Note that the smaller LP has only 54 variables and constraints, as compared to 714 in the larger one.

In Table 1, we compare three lower bounds on the number of rows in an ordered orthogonal array. The first bound is the standard LP bound for orthogonal arrays. The second bound is the generalized Rao bound from [10]. The third column lists the bound $LP^*(t,s,\ell,v)$ developed above. (Restricting to computations which can be done in exact arithmetic in reasonable time, we have limited the number of variables to 200.) The inequality above shows that the new bound is always at least as strong as the LP bound for OAs. As we shall prove below, the new bound is at least as strong as the generalized Rao bound when t is even. When $\ell = 2$, the generalised Rao bound gives mixed results, but for larger values such as $\ell = 4$, it outperforms the first bound for the values computed with only four exceptions. This small data set suggests that, while the new bound is strongest, the generalized Rao bound remains valuable because it is a closed form expression and easy to compute.

Although the main motivation for developing these tools is their relevance to the study of (T,M,S)-nets, we have limited data for our new bound in these cases due to the large size of the linear programs involved. However, at least one entry in Table 1 is relevant here. Since $LP^*(8,10,2,2) > 2^{11}$, we may conclude that there is no $\mathrm{OOA}_8(8,10,2,2)$, hence no $\mathrm{OOA}_8(8,10,8,2)$ exists. Using Theorem 2.2, this implies that there is no binary $(3,11,10)$-net, thus improving the bounds given in [3] and [10].

Our last result shows that, for t even, the linear programming bound is always at least as strong as the generalized Rao bound proved in [10]. The argument we use is a straightforward adaptation of the proof of Theorem 5.2 in [8]. First we prove

Proposition 4.4 *If e, f, and g are compositions of s in $\ell + 1$ non-negative parts, then the Krein parameter q^g_{ef} for scheme $(Y, \mathcal{A}_s)$ is zero whenever* $\mathrm{height}(g) > \mathrm{height}(e) + \mathrm{height}(f)$.

Proof Since the association scheme is formally self-dual we have $p^g_{ef} = q^g_{ef}$, so we need only verify this for the intersection number p^g_{ef} for $(Y, \mathcal{A}_s)$. Suppose e, f, and g are $(\ell+1)$-tuples of non-negative integers summing to s and that $p^g_{ef} > 0$. Let x, y, z be $s\ell$-tuples over $\mathbb{Z}_v$ with x g-related to y and z e-related to x and f-related to y. Consider tuples x, y and z in the s-fold product scheme $(Y, \mathcal{A}^{\otimes s})$ of the kernel scheme $(X, \mathcal{A})$. Suppose z is $\mathbf{i}$-related to x and $\mathbf{j}$-related to y and that x and y are $\mathbf{k}$-related in $(Y, \mathcal{A}^{\otimes s})$. Write $\mathbf{i} = (i_1, \ldots, i_s)$,

https://doi.org/10.4153/CJM-1999-017-5 Published online by Cambridge University Press

$\mathbf{j} = (j_1, \ldots, j_s)$, and $\mathbf{k} = (k_1, \ldots, k_s)$. Since height($\mathbf{k}$) $>$ height($\mathbf{i}$) + height($\mathbf{j}$), there exists a coordinate h in which $k_h > \max(i_h, j_h)$. Thus, in the kernel scheme, the intersection number $p^{k_h}_{i_h j_h}$ is zero (Corollary 1.3), yielding a contradiction. ∎

Now let M be any matrix in the Bose-Mesner algebra of $(Y, \mathcal{A}_s)$. We may write

$$\mathsf{M} = \sum_e \alpha_e \mathsf{A}_e = v^{s\ell} \sum_f \beta_f \mathsf{E}_f,$$

where, in both cases, the sum is over all compositions of s into $\ell + 1$ non-negative parts. If M satisfies the three conditions

1. M is non-negative;
2. $\beta_f \leq 0$ for all f having height $> t$;
3. $\beta_0 = 1$

(where the subscript 0 denotes the $(\ell + 1)$-tuple $(s, 0, \ldots, 0)$ corresponding to the identity relation in $(Y, \mathcal{A}_s)$), then it is known [8] that α_0 provides a lower bound on the optimal value of the above linear program. In fact, this is essentially the linear programming dual to Delsarte's inequalities for designs.

***Theorem 4.5* (*cf.* Theorem 3.5, [10])** *If C is the set of rows of an* $\mathrm{OOA}_\lambda(t, s, \ell, v)$*, and $D \subseteq Y$ is defined by*

$$D = \{a \in (\mathrm{Z}_v^\ell)^s : \mathrm{height}(a) \leq \lfloor t/2 \rfloor\},$$

then $|C| \geq |D|$.

Proof Define

$$\mathcal{E} = \Big\{(e_0, \ldots, e_\ell) : \sum_{i=0}^{\ell} e_i = s, \sum_{i=0}^{\ell} i e_i \leq \lfloor t/2 \rfloor \Big\}.$$

The rank of E_f is equal to the number of tuples $a = (a^{(1)}, \ldots, a^{(s)})$ having shape f. This follows from Theorem 1.7(3). Let

$$\mathsf{N} = \sum_{f \in \mathcal{E}} \mathsf{E}_f,$$

$$\gamma = \frac{v^{2s\ell}}{\sum_{f \in \mathcal{E}} \mathrm{rank}\, \mathsf{E}_f},$$

and define

$$\mathsf{M} = \gamma(\mathsf{N} \circ \mathsf{N})$$

where $\circ$ denotes entrywise product of matrices. Then M satisfies condition (1) since $\gamma > 0$ and $\mathsf{N} \circ \mathsf{N}$ is obviously non-negative. We leave it to the reader to check that condition (3) is also satisfied. By definition of the Krein parameters, we have

$$\mathsf{N} \circ \mathsf{N} = \Big(\sum_{f \in \mathcal{E}} \mathsf{E}_f\Big) \circ \Big(\sum_{f \in \mathcal{E}} \mathsf{E}_f\Big) = \frac{1}{v^{s\ell}} \sum_g \Big(\sum_{e \in \mathcal{E}} \sum_{f \in \mathcal{E}} q^g_{ef}\Big) \mathsf{E}_g.$$

Therefore, using the previous proposition, we have $\beta_g = 0$ for any composition g having height greater than t. Thus M also satisfies condition (2). Now we may compute

$$\alpha_0 = \sum_{f \in \mathcal{E}} \operatorname{rank} \mathsf{E}_f.$$

Observe that any tuple a of height less than or equal to $\lfloor t/2 \rfloor$ has shape f for some $f \in \mathcal{E}$. So $\alpha_0 = |D|$. As α_0 is a lower bound on the optimal value of the linear program for our array, this gives the desired bound. ■

t	**s**	ℓ	**v**	OA LP bound	GR bound	OOA LP bound
3	3	2	2	8	8	8
3	4	2	2	8	10	12
3	5	2	2	12	12	16
3	6	2	2	16	14	16
3	7	2	2	16	16	16
3	8	2	2	16	18	20
3	9	2	2	20	20	24
3	10	2	2	24	22	24
4	3	2	2	8	13	16
4	4	2	2	16	19	26.3
4	5	2	2	16	26	32
4	6	2	2	26.6	34	36.9
4	7	2	2	42.6	43	48.7
4	8	2	2	64	53	64
4	9	2	2	85.3	64	85.3
4	10	2	2	85.3	76	85.3
5	3	2	2	8	22	32
5	4	2	2	16	34	51.2
5	5	2	2	32	48	64
5	6	2	2	32	64	64
5	7	2	2	53.3	82	102.9
5	8	2	2	85.3	102	136.6
5	9	2	2	128	124	170.3
5	10	2	2	170.6	148	191.8
6	3	2	2	8	26	64
6	4	2	2	16	47	96
6	5	2	2	32	76	128
6	6	2	2	64	114	179.2
6	7	2	2	64	162	240
6	8	2	2	112	221	256
6	9	2	2	192	292	387.4
6	10	2	2	320	376	475.8
7	4	2	2	16	78	128

https://doi.org/10.4153/CJM-1999-017-5 Published online by Cambridge University Press

t	s	ℓ	v	OA LP bound	GR bound	OOA LP bound
7	5	2	2	32	132	256
7	6	2	2	64	204	332.8
7	7	2	2	128	296	477.8
7	8	2	2	128	410	682.6
7	9	2	2	224	548	896
7	10	2	2	384	712	1024
8	4	2	2	16	96	256
8	5	2	2	32	181	384
8	6	2	2	64	309	682.6
8	7	2	2	128	491	944.3
8	8	2	2	256	739	1331.0
8	9	2	2	256	1066	2012.6
8	10	2	2	460.8	1486	2633.1
4	3	4	2	8	13	16
4	4	4	2	16	19	26.6
4	5	4	2	16	26	32
5	3	4	2	8	26	32
5	4	4	2	16	38	53.3
5	5	4	2	32	52	64
6	3	4	2	8	38	64
6	4	4	2	16	63	106.6
6	5	4	2	32	96	128
7	3	4	2	8	76	128
7	4	4	2	16	126	213.3
7	5	4	2	32	192	256
8	3	4	2	8	104	256
8	4	4	2	16	192	426.6
8	5	4	2	32	321	512

Key Each of the three columns provides lower bounds on the number of rows in an ordered orthogonal array with the given parameters.

OA bound: linear programming bound for orthogonal array formed by the set of first columns of an OOA.

GR bound: Generalized Rao bound derived in [10].

OOA LP bound: Our linear programming bound $LP^*(t,s,l,v)$ for ordered orthogonal arrays, executed in exact arithmetic in MAPLE.

Acknowledgements This research was carried out while the second author was on sabbatical with the Department of Computer Science at the University of Manitoba. He would like to thank the department for its hospitality.

The authors' research is supported as follows: NSERC grant OGP 0155422 (WJM), and NSERC grant RGPIN #203114-98 (DRS).

We are grateful to Bob Bixby for his assistance in solving a large linear program using the CPLEX software. We have benefited from comments from a variety of readers; we wish to thank Phillippe Delsarte, Mark Lawrence, Vladimir Levenshtein and Wolfgang Schmid.

Note added in proof Since this paper was submitted for publication, more linear programming bounds have been computed (in exact arithmetic) using the software packages MAPLE and CPLEX. The results are reported in [9].

References

[1] M. J. Adams, *Generalized Orthogonal Arrays and Related Structures.* Ph.D. thesis, Department of Mathematics, University of Wyoming, Laramie, Wyoming, May 1997.

[2] A. E. Brouwer, A. M. Cohen and A. Neumaier, *Distance-Regular Graphs.* Springer-Verlag, Berlin, 1989.

[3] A. T. Clayman, K. M. Lawrence, G. L. Mullen, H. Niederreiter and N. J. A. Sloane, *Updated tables of parameters of* (T, M, S)*-nets.* J. Combin. Des., to appear.

[4] P. Delsarte, *An algebraic approach to the association schemes of coding theory.* Philips Res. Rep. Suppl. **10**(1973).

[5] C. D. Godsil, *Algebraic Combinatorics.* Chapman and Hall, New York, 1993.

[6] ———, *MacWilliams theorem for product schemes.* Preprint.

[7] K. M. Lawrence, *A combinatorial interpretation of* (t, m, s)*-nets in base b.* J. Combin. Des. **4**(1996), 275–293.

[8] W. J. Martin, *Designs in product association schemes.* Designs, Codes and Cryptography, **16**(1999) 271–289.

[9] ———, *Linear programming bounds for ordered orthogonal arrays and* (t, m, s)*-nets.* Proceedings of the Third International Conference on Monte Carlo and Quasi-Monte Carlo Methods in Scientific Computing. Lect. Notes Comput. Sci. Eng., Springer-Verlag, to appear.

[10] W. J. Martin and D. R. Stinson, *A generalized Rao bound for ordered orthogonal arrays and* (t, m, s)*-nets.* Canad. Math. Bull., to appear.

[11] G. L. Mullen and G. Whittle, *Point sets with uniformity properties and orthogonal hypercubes.* Monatsh. Math. **113**(1992), 265–273.

[12] G. L. Mullen, A. Mahalanabis and H. Niederreiter, *Tables of* (T, M, S)*-net and* (T, S)*-sequence parameters.* In: Monte Carlo and Quasi-Monte Carlo Methods in Scientific Computing (eds. H. Niederreiter and P. Shiue), Lecture Notes in Statist. **106**, Springer, New York, 1995, pp. 58–86.

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

[14] M. Yu. Rosenbloom and M. A. Tsfasman, *Codes for the m-metric.* Problems Inform. Transmission (1) **33**(1997), 45–52.

[15] W. Ch. Schmid, (t, m, s)*-nets: Digital Constructions and Combinatorial Aspects.* Ph.D. thesis, Institute of Mathematics, University of Salzburg, Salzburg, Austria, May 1995.

[16] S. Yamamoto, Y. Fujii and N. Hamada, *Computation of some series of association algebras.* J. Sci. Hiroshima University (2) **29**(1965), 181–215.

Mathematics and Statistics
University of Winnipeg
Winnipeg, Manitoba R3B 2E9
email: William.Martin@UWinnipeg.ca

Combinatorics and Optimization
University of Waterloo
Waterloo, Ontario, N2L 3G1
email: dstinson@cacr.math.uwaterloo.ca