A dual Plotkin bound for (T, M, S)-nets

William J. Martin[1]
Terry I. Visentin[2]

[1]Department of Mathematical Sciences
Worcester Polytechnic Institute
Worcester, Massachusetts 01609
martin@wpi.edu

[2]Department of Mathematics and Statistics
University of Winnipeg
Winnipeg, Canada R3B 2E9
visentin@UWinnipeg.ca

Keywords: linear programming bound, (t, m, s)-nets, Plotkin bound, association scheme

Abstract. The effectiveness of Quasi-Monte Carlo methods for numerical integration has led to the study of (T, M, S)-nets, which are uniformly distributed point sets in the Euclidean unit cube. A recent result, proved independently by Schmid/Mullen and Lawrence, establishes an equivalence between (T, M, S)-nets and ordered orthogonal arrays. In a paper of Martin and Stinson, a linear programming technique is described which gives lower bounds on the size of an ordered orthogonal array and, hence, on the quality parameter T of a (T, M, S)-net. In this paper, we use these ideas to derive a dual Plotkin bound for ordered orthogonal arrays. For a (T, M, S)-net in base b, this bound implies

$$T \geq M + 1 - \frac{S}{1 - b^{M-S\ell}} \left(\ell - \frac{1}{b} - \frac{1}{b^2} - \cdots - \frac{1}{b^\ell} \right),$$

where $\ell = 1 + \lfloor \frac{M-T}{S} \rfloor$. We end the paper with an exploration of the implications of this bound relative to known tables and examples.

1 Introduction

Low-discrepancy point sets in the Euclidean unit cube $[0,1)^S$ are important in several quasi-Monte Carlo methods in scientific computing. In applications such as numerical integration, pseudo-random number generation and simulation, it is desirable to have a good supply of "small" subsets $\mathcal{N} \subseteq [0,1)^S$ which evenly sample a prespecified collection of subregions of the cube. The following concept is due to Niederreiter [8] but is based on earlier ideas of Sobol' [13].

Consider a base $b \geq 2$. An elementary interval in base b is a region of the form

$$E = \prod_{i=1}^{S} \left[\frac{a_i}{b^{d_i}}, \frac{a_i+1}{b^{d_i}} \right)$$

where the integers a_i satisfy $0 \leq a_i < b^{d_i}$ for each i. Observe that $\mathrm{Vol}(E) = b^{-\sum d_i}$. A (T,M,S)-net in base b is a subset $\mathcal{N}$ of $[0,1)^S$ of size b^M such that every elementary interval in base b having volume b^{T-M} contains exactly b^T points of $\mathcal{N}$. While much recent research focuses on the construction of such point sets (see, e.g., [9,11]), our aim is to provide good lower bounds on the size of such a set. For such bounds in the case of small dimensions S, see [1,7]. An analogue of the Rao bound for orthogonal arrays was obtained in [5]; this applies to all dimensions S and is strongest for $M-T$ small. By contrast, our main result — which also applies for all dimensions S — is most useful when $M-T$ is large. The main result of this paper is the following lower bound on T as a function of M, S and b.

Theorem 1 (Dual Plotkin Bound for T). *If a (T,M,S)-net exists in base b, then*

$$T \geq M + 1 - \frac{S}{1-b^{M-S\ell}} \left(\ell - \frac{1}{b} - \frac{1}{b^2} - \cdots - \frac{1}{b^\ell} \right),$$

where $\ell = 1 + \lfloor \frac{M-T}{S} \rfloor$.

We now outline a translation of these structures into the language of combinatorial designs. Let F be an alphabet composed of b symbols. Let A be an array with entries from F whose $s\ell$ columns are indexed by the set

$$\mathcal{C} = \{(i,j) : \ 1 \leq i \leq s, \ 1 \leq j \leq \ell\}.$$

The parameter i will be referred to as a *coordinate*. The motivation for this suggestive notation will be clear after the next theorem. We say that A is *balanced* with respect to $R \subseteq \mathcal{C}$ provided the array obtained by restricting A to only those columns in R contains each $|R|$-tuple over F as a row exactly λ times for some positive integer λ. We say that a set R of columns is *left-justified* provided, for all i and all $j > 1$, if $(i,j) \in R$, then $(i,j-1) \in R$. An *ordered orthgonal array* (OOA) with parameters t, s, ℓ and b is an array A with entries from F and columns indexed by $\mathcal{C}$ having the property that A is balanced with respect to every left-justified set R consisting of t columns. If this condition holds, we will call A an $OOA_\lambda(t,s,\ell,b)$ where λb^t is the number of rows of A, and we refer to t as the *strength* of the array.

Theorem 2 (Mullen/Schmid, Lawrence). *There exists a (T, M, S)-net in base b if and only if there exists an $OOA_{b^T}(M-T, S, M-T, b)$.*

If b is a prime power and F is the finite field of order b, it may happen that the rows of A form a linear subspace of $F^{s\ell}$. Such an array is called a *linear OOA*. More generally, we may impose the structure of an abelian group on F and require the rows of A to form a subgroup of $F^{s\ell}$. These *additive OOA's* are connected via the above correspondence to the so-called *digital nets*.

Henceforth, a tuple $\mathbf{x}$ in $F^{s\ell}$ will be written

$$\mathbf{x} = \left(\ \mathbf{x}^{(1)}; \ \mathbf{x}^{(2)}; \ \cdots; \ \mathbf{x}^{(s)} \right) = \left(x_1^{(1)}, \ldots, x_\ell^{(1)}; \ x_1^{(2)}, \ldots, x_\ell^{(2)}; \ \cdots; \ x_1^{(s)}, \ldots, x_\ell^{(s)} \right).$$

In [10], Rosenbloom and Tsfasman define the following metric on $F^{s\ell}$:

$$\rho(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^{s} \left(\ell - \max(j : x_k^{(i)} = y_k^{(i)} \text{for all } k < j) \right)$$

where the maximum is taken to be zero when $x_1^{(i)} \neq y_1^{(i)}$. We will refer to this as the *RT metric*. A nonempty subset C of $F^{s\ell}$ is said to have minimum distance d in the RT metric provided $\rho(\mathbf{x}, \mathbf{y}) \geq d$ for all pairs $\mathbf{x}$, $\mathbf{y}$ of distinct elements in C and $\rho(\mathbf{x}, \mathbf{y}) = d$ for some $\mathbf{x}$ and $\mathbf{y}$ in C. We define *linear RT code* and *additive RT code* the same way we did for ordered orthgonal arrays.

Theorem 3 (Martin/Stinson [6]). *Suppose F is an abelian group. Let C be an additive subset of $F^{s\ell}$ and let $C^\perp$ denote its dual. Then C has minimum distance d as an RT code if and only if $C^\perp$ has strength $d-1$ as an ordered orthogonal array.*

2 The Plotkin Bound

We begin with an elementary proof of an upper bound of Rosenbloom and Tsfasman [10] on the size of an RT code. This is a straightforward extension of the Plotkin bound familiar to coding theorists (cf. [14]).

Let C be an RT code of size M with minimum distance at least d. Then we clearly have

$$dM(M-1) \leq \sum_{\mathbf{x} \in C} \sum_{\mathbf{y} \in C} \rho(\mathbf{x}, \mathbf{y}). \tag{1}$$

Observe that

$$\rho(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^{s} \rho(\mathbf{x}^{(i)}, \mathbf{y}^{(i)}) \tag{2}$$

where, on the right, the metric ρ is the Rosenbloom-Tsfasman metric specialized to the case $s = 1$. Fix a coordinate i $(1 \leq i \leq s)$. For each $\mathbf{c} \in F^h$ $(1 \leq h \leq \ell)$, define

$$m_{\mathbf{c}} := \left| \left\{ \mathbf{x} \in C : x_j^{(i)} = c_j \quad \text{for} \quad 1 \leq j \leq h \right\} \right|$$

and note that, for any $1 \le h \le \ell$, $\sum_{\mathbf{c}\in F^h} m_{\mathbf{c}} = M$. For this coordinate i, we may write

$$\sum_{\mathbf{x}\in C}\sum_{\mathbf{y}\in C}\rho(\mathbf{x}^{(i)},\mathbf{y}^{(i)}) = \sum_{\mathbf{u}\in F^\ell}\sum_{\mathbf{v}\in F^\ell}\rho(\mathbf{u},\mathbf{v})m_{\mathbf{u}}m_{\mathbf{v}}. \tag{3}$$

Let $\theta = \ell - \frac{1}{b} - \frac{1}{b^2} - \cdots - \frac{1}{b^\ell}$. We claim the following

Lemma 1.

$$\sum_{\mathbf{u}\in F^\ell}\sum_{\mathbf{v}\in F^\ell}\rho(\mathbf{u},\mathbf{v})m_{\mathbf{u}}m_{\mathbf{v}} \le \theta M^2.$$

Proof. Let X denote the quantity on the left-hand side. For $\mathbf{c}\in F^h$, $\mathbf{u}\in F^\ell$, write $\mathbf{c}\preceq\mathbf{u}$ when $u_j = c_j$ for $1\le j\le h$. Then, for any $\mathbf{u}$ and $\mathbf{v}$ in F^ℓ,

$$\rho(\mathbf{u},\mathbf{v}) = \ell - \sum_{\substack{\mathbf{c}\preceq\mathbf{u}\\ \mathbf{c}\preceq\mathbf{v}}} 1$$

since $\mathbf{u}$ and $\mathbf{v}$ have one common prefix of length h for each $h = 1,\ldots,\ell-\rho(\mathbf{u},\mathbf{v})$. We therefore have

$$X = \ell M^2 - \sum_{h=1}^{\ell}\sum_{\mathbf{c}\in F^h} m_{\mathbf{c}}^2.$$

Now apply the Cauchy-Schwarz inequality: for $\mathbf{c}\in F^h$

$$\sum_{\substack{\mathbf{c}'\in F^{h+1}\\ \mathbf{c}\preceq\mathbf{c}'}} m_{\mathbf{c}'}^2 \ge \frac{1}{b}m_{\mathbf{c}}^2, \quad \text{which gives} \quad \sum_{\mathbf{c}'\in F^{h+1}} m_{\mathbf{c}'}^2 \ge \frac{1}{b}\sum_{\mathbf{c}\in F^h} m_{\mathbf{c}}^2,$$

after summing over all $\mathbf{c}\in F^h$. In fact, we may apply Cauchy-Schwarz repeatedly to obtain the inequalities

$$\begin{aligned}
X &= \ell M^2 - \sum_{h=1}^{\ell-1}\sum_{\mathbf{c}\in F^h} m_{\mathbf{c}}^2 - \sum_{\mathbf{c}\in F^\ell} m_{\mathbf{c}}^2\\
&\le \ell M^2 - \sum_{h=1}^{\ell-2}\sum_{\mathbf{c}\in F^h} m_{\mathbf{c}}^2 - \left(1+\frac{1}{b}\right)\sum_{\mathbf{c}\in F^{\ell-1}} m_{\mathbf{c}}^2\\
&\;\;\vdots\\
&\le \ell M^2 - \left(1+\frac{1}{b}+\cdots+\frac{1}{b^{\ell-1}}\right)\sum_{c\in F} m_c^2\\
&\le \ell M^2 - \left(1+\frac{1}{b}+\cdots+\frac{1}{b^{\ell}}\right)M^2 = \theta M^2.
\end{aligned}$$

□

With equation (3), this gives the following inequality for each coordinate i:

$$\sum_{\mathbf{x}\in C}\sum_{\mathbf{y}\in C}\rho(\mathbf{x}^{(i)},\mathbf{y}^{(i)}) \le \theta M^2. \tag{4}$$

Summing over all s coordinates and using equations (1) and (2), we obtain

$$dM(M-1) \leq \sum_{\mathbf{x}\in C}\sum_{\mathbf{y}\in C}\rho(\mathbf{x},\mathbf{y}) \leq s\theta M^2,$$

which completes our proof of the bound of Rosenbloom and Tsfasman [10].

Theorem 4 (Plotkin Bound). *If a code C has minimum distance $d > s\theta$, then $M = |C|$ satisfies*

$$M \leq \frac{d}{d-s\theta}.$$

In view of Theorems 2 and 3, this implies a dual Plotkin bound for digital (T, M, S)-nets. In order to establish such a bound for arbitrary (T, M, S)-nets, we now turn to the linear programming method from the theory of association schemes.

3 Linear Programming

In [6], Martin and Stinson derived a linear programming bound for ordered orthogonal arrays. This is a special case of a general result of Delsarte [2].

Let positive integers s, ℓ, and $b \geq 2$ be given. Let $\mathbf{z} = (z_0, \ldots, z_\ell)$ be a vector of indeterminates. Define polynomials

$$p_i(\mathbf{z}) = \left(\sum_{h=0}^{\ell-i}\lceil b^h - b^{h-1}\rceil z_h\right) \; - \; b^{\ell-i}z_{\ell+1-i}$$

where the ceiling function $\lceil\cdot\rceil$ is used simply to round up the coefficient of z_0 and we introduce the constant $z_{\ell+1} = 0$ for convenience.

Now if $\mathbf{f} = (f_0, \ldots, f_\ell)$ is any $(\ell+1)$-tuple of nonnegative integers summing to s we define

$$P_{\mathbf{f}}(\mathbf{z}) = \prod_{i=0}^{\ell} p_i(\mathbf{z})^{f_i}.$$

Our linear program has $\binom{\ell+s}{s}$ variables and constraints, one of each for every $(\ell+1)$-tuple $\mathbf{f}$ of nonnegative integers summing to s. We will henceforth refer to these tuples as "shapes".

For a shape $\mathbf{e} = (e_0, \ldots, e_\ell)$, we write

$$\mathbf{z}^{\mathbf{e}} = z_0^{e_0}\cdots z_\ell^{e_\ell}.$$

Now we define the constraint matrix P. For shapes $\mathbf{e}$ and $\mathbf{f}$, the entry $\mathsf{P}_{\mathbf{f},\mathbf{e}}$ in row $\mathbf{f}$ and column $\mathbf{e}$ is defined to be the coefficient of $\mathbf{z}^{\mathbf{e}}$ in the polynomial $P_{\mathbf{f}}(\mathbf{z})$. We have one variable $A_{\mathbf{f}}$ for each shape $\mathbf{f}$, but the variable $A_{\mathbf{0}}$ will be treated in a special manner by putting $A_{\mathbf{0}} = 1$ where the zero shape is $\mathbf{0} \equiv (s, 0, \ldots, 0)$.

We define the "height" of a shape $\mathbf{e}$ as follows:

$$\mathsf{ht}(\mathbf{e}) = e_1 + 2e_2 + \cdots + \ell e_\ell.$$

Let $\mathbf{A}$ denote the row vector whose entries are the variables $A_{\mathbf{f}}$. We are now prepared to give a concise description of the linear program obtained by Martin and Stinson [6]. For any ordered orthogonal array OOA(t, s, ℓ, b), the number of rows is bounded below by the optimal objective value of the following LP:

$$\begin{array}{rl}
\textbf{minimize} & \sum_{\mathbf{f}} A_{\mathbf{f}} \\
\text{subject to} & \\
(\mathbf{A}\mathsf{P})_{\mathbf{e}} = 0 & \text{for } 0 < \mathsf{ht}(\mathbf{e}) \leq t \\
(\mathbf{A}\mathsf{P})_{\mathbf{e}} \geq 0 & \text{for } \mathsf{ht}(\mathbf{e}) > t \\
A_{\mathbf{f}} \geq 0 & \text{for all } \mathbf{f} \\
A_{\mathbf{0}} = 1 &
\end{array}$$

We can rephrase this by replacing the rows of P by the corresponding multivariate polynomials $P_{\mathbf{f}}(\mathbf{z})$ and setting $g(\mathbf{z}) = \sum A_{\mathbf{f}} P_{\mathbf{f}}(\mathbf{z})$. If $[\mathbf{z}^{\mathbf{e}}]g(\mathbf{z})$ is used to denote the coefficient of the monomial $\mathbf{z}^{\mathbf{e}}$ in the polynomial $g(\mathbf{z})$, then we have

$$\begin{array}{rl}
\textbf{minimize} & [z_0^s]g(\mathbf{z}) \\
\text{subject to} & \\
[\mathbf{z}^{\mathbf{e}}]g(\mathbf{z}) = 0 & \text{for } 0 < \mathsf{ht}(\mathbf{e}) \leq t \\
[\mathbf{z}^{\mathbf{e}}]g(\mathbf{z}) \geq 0 & \text{for } \mathsf{ht}(\mathbf{e}) > t \\
g(\mathbf{z}) = \sum_{\mathbf{f}} A_{\mathbf{f}} P_{\mathbf{f}}(\mathbf{z}) & \text{with all } A_{\mathbf{f}} \geq 0 \\
A_{\mathbf{0}} = 1 &
\end{array}$$

Since only the minimum feasible solution provides a lower bound and solving this LP to optimality does not seem practicable asymptotically, we pass to the dual linear program for which each feasible solution is a valid lower bound on the number of rows in our OOA. The dual linear program can be formulated as follows:

$$\begin{array}{rl}
\textbf{maximize} & [z_0^s]g(\mathbf{z}) \\
\text{subject to} & \\
[\mathbf{z}^{\mathbf{e}}]g(\mathbf{z}) \geq 0 & \text{for all } \mathbf{e} \neq 0 \\
g(\mathbf{z}) = \sum_{\mathbf{e}} B_{\mathbf{e}} P_{\mathbf{e}}(\mathbf{z}) & \text{with} \\
B_{\mathbf{e}} \leq 0 & \text{whenever } \mathsf{ht}(\mathbf{e}) > t \\
B_{\mathbf{0}} = 1 &
\end{array} \qquad (\dagger)$$

For a given set of parameters t, s, ℓ, and b, let $LP^*(t, s, \ell, b)$ denote the optimal objective value of this linear program. The case $\ell = 1$ corresponds to the ordinary linear programming bound for error-correcting codes and orthogonal arrays. Quite a bit is known in this case (see, e.g., [4]), but almost nothing is known for the cases $\ell \geq 2$.

4 Proof of the Main Theorem

We begin with a technical lemma.

Lemma 2.

$$\sum_{j=1}^{\ell} j \left(b^j - b^{j-1}\right) p_j = b^\ell \theta z_0 - \sum_{j=1}^{\ell} \left(b^\ell - b^{j-1}\right) z_j.$$

Proof. Let $U(\mathbf{z}) = \sum_{j=1}^{\ell} j\left(b^j - b^{j-1}\right)p_j = \sum_{k\geq 0} u_k z_k$. Proving this lemma is now a matter of computing the u_k. For $j \geq 1$,

$$p_j = z_0 + \sum_{i=1}^{\ell-j}(b^i - b^{i-1})z_i - b^{\ell-j}z_{\ell-j+1}.$$

Concentrating first on the coefficient of z_0 in $U(\mathbf{z})$, we have

$$\begin{aligned} u_0 &= \sum_{j=1}^{\ell} j(b^j - b^{j-1}) = \sum_{j=1}^{l} jb^j - \sum_{j=0}^{\ell-1}(j+1)b^j = \ell b^\ell - 1 - \sum_{j=1}^{l-1} b^j \\ &= b^\ell\left(\ell - \tfrac{1}{b^\ell} - \tfrac{1}{b^{\ell-1}} - \cdots - \tfrac{1}{b}\right) = b^\ell\theta. \end{aligned}$$

Now if $k \geq 1$, the coefficient of z_k in $U(\mathbf{z})$ is

$$\begin{aligned} u_k &= \sum_{j=1}^{\ell-k} j(b^j - b^{j-1})(b^k - b^{k-1}) - (\ell-k+1)(b^{\ell-k+1} - b^{\ell-k})b^{k-1} \\ &= (b^k - b^{k-1})\left\{\sum_{j=1}^{\ell-k} jb^j - \sum_{j=0}^{\ell-k-1}(j+1)b^j\right\} - (\ell-k+1)(b^\ell - b^{\ell-1}) \\ &= (b^k - b^{k-1})\left\{(\ell-k)b^{\ell-k} - \sum_{j=0}^{\ell-k-1} b^j\right\} - (\ell-k)b^\ell + (\ell-k)b^{\ell-1} - b^\ell + b^{\ell-1} \\ &= -\sum_{j=0}^{\ell-k-1} b^{j+k} + \sum_{j=0}^{\ell-k-1} b^{j+k-1} - b^\ell + b^{\ell-1} = -b^{\ell-1} + b^{k-1} - b^\ell + b^{\ell-1} \\ &= -(b^\ell - b^{k-1}), \end{aligned}$$

which completes the proof. □

The following theorem will lead to the dual Plotkin bound by giving a particular feasible solution to the dual LP (†).

Theorem 5. *For $t > s\theta - 1$, we have $LP^*(t, s, \ell, b) \geq b^{s\ell}\left(1 - \dfrac{s\theta}{t+1}\right)$.*

Proof. Let $\alpha = \frac{s}{t+1}$ and consider the solution defined by

$$B_{\mathbf{f}} = \left(1 - \frac{\mathsf{ht}(\mathbf{f})}{t+1}\right)\binom{s}{f_0, \ldots, f_\ell}\prod_{i=1}^{\ell}\left(b^i - b^{i-1}\right)^{f_i}.$$

In view of our linear programming formulation (†), it suffices to establish the following four claims:

Claim 1:

$$\sum_{\mathbf{f}} B_{\mathbf{f}}P_{\mathbf{f}}(\mathbf{z}) = (b^\ell z_0)^{s-1}\left[b^\ell(1-\alpha\theta)z_0 + \alpha\sum_{j=1}^{\ell}\left(b^\ell - b^{j-1}\right)z_j\right].$$

Claim 2: All coefficients on the right-hand side of Claim 1 are nonnegative.

Claim 3: $B_{\mathbf{f}} \le 0$ whenever $\mathsf{ht}(\mathbf{f}) > t$.

Claim 4: $\sum_{\mathbf{f}} B_{\mathbf{f}} = b^{s\ell}(1 - \alpha\theta)$.

Claim 3 follows immediately from the definition. Let us prove Claim 1 next.

$$\begin{aligned}
\sum_{\mathbf{f}} B_{\mathbf{f}} P_{\mathbf{f}}(\mathbf{z}) &= \sum_{\mathbf{f}} \left(1 - \alpha \frac{\mathsf{ht}(\mathbf{f})}{s}\right) \binom{s}{f_0, \ldots, f_\ell} \prod_{i=0}^{\ell} \left(\lceil b^i - b^{i-1} \rceil p_i\right)^{f_i} \\
&= \sum_{\mathbf{f}} \binom{s}{f_0, \ldots, f_\ell} \prod_{i=0}^{\ell} \left(\lceil b^i - b^{i-1} \rceil p_i\right)^{f_i} \; - \\
&\quad \alpha \sum_{j=1}^{\ell} \frac{j}{s} \sum_{\mathbf{f}} \binom{s}{f_0, \ldots, f_\ell} f_j \prod_{i=0}^{\ell} \left(\lceil b^i - b^{i-1} \rceil p_i\right)^{f_i} \\
&= \left(\sum_{i=0}^{\ell} \lceil b^i - b^{i-1} \rceil p_i\right)^s - \left(\alpha \sum_{j=1}^{\ell} \frac{j p_j}{s}\right) \times \\
&\quad \sum_{\mathbf{f}} \binom{s}{f_0, \ldots, f_\ell} f_j (b^j - b^{j-1}) \left[(b^j - b^{j-1}) p_j\right]^{f_j - 1} \prod_{i \neq j} \left(\lceil b^i - b^{i-1} \rceil p_i\right)^{f_i} \\
&= \left(\sum_{i=0}^{\ell} \lceil b^i - b^{i-1} \rceil p_i\right)^s \; - \; \alpha \sum_{j=1}^{\ell} \frac{j p_j}{s} \cdot \frac{\partial}{\partial p_j} \left(\sum_{i=0}^{\ell} \lceil b^i - b^{i-1} \rceil p_i\right)^s \\
&= \left(b^\ell z_0\right)^s \; - \; \alpha \sum_{j=1}^{\ell} j p_j (b^j - b^{j-1}) \left(b^\ell z_0\right)^{s-1} \\
&= \left(b^\ell z_0\right)^{s-1} \left[b^\ell z_0 - \alpha \sum_{j=1}^{\ell} j p_j (b^j - b^{j-1}) \right] \\
&= \left(b^\ell z_0\right)^{s-1} \left[b^\ell z_0 - \alpha \left(b^\ell \theta z_0 - \sum_{j=1}^{\ell} \left(b^\ell - b^{j-1}\right) z_j \right) \right] \\
&= (b^\ell z_0)^{s-1} \left[b^\ell (1 - \alpha\theta) z_0 + \alpha \sum_{j=1}^{\ell} \left(b^\ell - b^{j-1}\right) z_j \right].
\end{aligned}$$

Thus Claim 1 holds. Now, since $0 \le \alpha < 1/\theta$, all coefficients of the resulting polynomial are easily seen to be nonnegative, and Claim 2 holds. Finally, we compute the sum of the $B_{\mathbf{f}}$ by setting $z_0 = 1$ and $z_j = 0$ for all $j \neq 0$ in Claim 1 and Claim 4 is proven. This completes the proof of the theorem. $\square$

By a result of Levenshtein [4], any linear programming bound for designs, such as the above, yields a corresponding bound for codes. Without going into details, we remark that, in this case, we obtain a third proof of the Plotkin bound for RT codes.

The translation into a bound for (T, M, S)-nets is now immediate.

Proof of Theorem 1: Let $\mathcal{N}$ be a (T, M, S)-net in base b. Then, by Theorem 2, there exists an $OOA(M-T, S, M-T, b)$ having b^M rows. Theorem 5 then implies that

$$b^M \geq b^{S\ell}\left(1 - \frac{S\theta}{M-T+1}\right)$$

where ℓ and $\theta = \ell - \frac{1}{q} - \cdots - \frac{1}{q^\ell}$ satisfy $M - T > S\theta - 1$. Taking $\ell = 1 + \lfloor \frac{M-T}{S} \rfloor$, we obtain

$$b^{M-S\ell} \geq 1 - \frac{S\theta}{M-T+1}$$

which is easily manipulated to give the desired result. $\square$

5 Impact of our results

We observe that the Plotkin bound gives the optimal solution to the linear program (†) for several infinite families of parameter sets.

$$LP^*(5u-1, 3u, 2, 2) = 2^{6u-2} \qquad (u = 1, 2, 3, \ldots)$$

$$LP^*(4u-1, 3u, 2, 2) = 2^{6u-4} \qquad (u = 1, 2, 3, \ldots)$$

$$LP^*(10u-1, 7u, 2, 2) = 2^{14u-3} \qquad (u = 1, 2, 3, \ldots)$$

Now we give lower bounds $T(M, S)$ on T for (T, M, S)-nets in base b for sufficiently large M. These are important because they give lower bounds on T for structures called (T, S)-sequences [9]. Niederreiter showed that every (T, S)-sequence in base b yields a $(T, M, S+1)$-net in base b for all $M \geq T$ [8, Lemma 5.15]. Thus the bounds below, obtained via the propagation rules

$$T(M+1, S) \geq T(M, S), \qquad T(M, S+1) \geq T(M, S),$$

for $M = 500$ and $\ell \leq 50$ yield new information about the existence of such sequences. For comparison, the reader should consult `http://mint.sbg.ac.at/` [12] where an elegant and regularly updated web tool gives the best known information on both nets and sequences.

Lower bounds on T for (T, S)-sequences in bases $b = 2, 3, 5$

$b\backslash S$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
2	0	0	1	1	2	3	3	4	5	6	7	7	8	9	10	11	12	13	14	14	15	16	17	18	19
3	0	0	0	1	1	1	2	2	2	3	3	3	4	4	5	5	6	6	6	7	7	8	8	9	9
5	0	0	0	0	0	1	1	1	1	1	1	2	2	2	2	2	3	3	3	3	3	4	4	4	4

$b\backslash S$	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50
2	20	21	22	23	24	25	26	27	28	29	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43
3	10	10	11	11	11	12	12	13	13	14	14	15	15	16	16	17	17	18	18	19	19	20	20	20	21
5	5	5	5	5	5	6	6	6	6	7	7	7	7	8	8	8	8	8	9	9	9	9	10	10	10

Acknowledgements

During the time that this research was carried out, WJM's work was supported through NSERC and by the NSF through ITR. TIV's research was supported by an NSERC Discovery Grant. WJM wishes to thank CACR for its support and the Department of Combinatorics and Optimization at the University of Waterloo for its hospitality during the period this work was carried out. In particular, Doug Stinson provided helpful ideas. We are also grateful to Rudolf Schürer at the University of Salzburg for corrections and helpful comments.

References

1. 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. Designs* **7** (1999), 381–393.
2. P. Delsarte, An algebraic approach to the association schemes of coding theory, *Philips Res. Reports Suppl.* **10** (1973).
3. K. M. Lawrence, A combinatorial interpretation of (t, m, s)-nets in base b, *J. Combin. Designs* **4** (1996), 275–293.
4. V. I. Levenshtein, Krawtchouk polynomials and universal bounds for codes and designs in Hamming spaces, *IEEE Trans. Inform. Theory* **41** (no. 5) (1995), 1303–1321.
5. W. J. Martin and D. R. Stinson, A generalized Rao bound for ordered orthogonal arrays and (t, m, s)-nets, *Canad. Math. Bull.* **42** (no. 3) (1999), 359–370.
6. W. J. Martin and D. R. Stinson, Association schemes for ordered orthogonal arrays and (t, m, s)-nets, *Canad. J. Math.* **51** (no. 2) (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-Verlag, Berlin, 2000.
8. H. Niederreiter, Point sets and sequences with small discrepancy, *Monatsh. Math.* **104** (1987), 273–337.
9. H. Niederreiter, Constructions of (t, m, s)-nets, Monte Carlo and Quasi-Monte Carlo Methods 1998 (H. Niederreiter and J. Spanier, eds.), pp. 70–85, Springer-Verlag, Berlin, 2000.
10. M. Yu. Rosenbloom and M. A. Tsfasman, Codes for the m-metric, *Problems of Information Transmission* **33** (no. 1) (1997), 45–52.
11. W. Schmid, (t, m, s)-nets: Digital constructions and combinatorial aspects, Doctoral Dissertation, University of Salzburg, (1995).
12. R. Schürer and W. Schmid, MinT: A database for optimal net parameters, Monte Carlo and Quasi-Monte Carlo Methods 2004 (H. Niederreiter and D. Talay, eds.), Springer-Verlag, 2005 (to appear).
13. I. M. Sobol', Distribution of points in a cube and approximate evaluation of integrals, *U.S.S.R. Comput. Math. and Math. Phys.* **7** (1967), 784–802.
14. J. H. van Lint, Introduction to Coding Theory (2nd ed.), Graduate Texts in Mathematics #86, Springer-Verlag, Berlin (1992).