Linear programming bounds for (T, M, S)-nets

William J. Martin
Departments of Mathematical Sciences and Computer Science
Worcester Polytechnic Institute
Worcester, Massachusetts
martin@wpi.edu

October 21, 2005

1 Statement of the problem

Extending earlier ideas of Sobol' [11], Niederreiter [6] introduced the following definition. A (T, M, S)-*net in base* b is a subset $\mathcal{N}$ of the Euclidean unit cube $[0,1)^S$ of size b^M enjoying the property that each *elementary interval* in base b

$$E = \prod_{i=1}^{S} \left[\frac{a_i}{b^{d_i}}, \frac{a_i + 1}{b^{d_i}} \right), \qquad 0 \leq a_i < b^{d_i}$$

of volume b^{T-M} contains exactly b^T points of the net. (Note that $Vol(E) = b^{-\sum d_i}$.) These deterministic low-discrepancy point sets have proven powerful in the estimate of high-dimensional integrals. The goal is to make the *quality parameter* T as close to zero as possible.

Some researchers work on constructions of such nets and ideas from coding theory have led to very powerful examples [7]. But, in many cases, we do not know if these constructions are optimal. Therefore a theory of bounds is needed. The problem addressed here is that of obtaining provable lower bounds on the parameter T in terms of M, S and the base b. The theoretical breakthrough came in several stages. First, Mullen/Schmid [9] and Lawrence [2] independently proved an equivalnce between the Euclidean (T, M, S)-nets and combinatorial objects call *ordered orthogonal arrays*. Based on these ideas, Martin and Stinson [3] constructed a family of association schemes analogous to the Hamming schemes used in coding theory and established a linear programming bound for (T, M, S)-nets. Finally, we need to apply this bound.

2 Importance of the problem

This problem is of interest to combinatorialists dealing with combinatorial designs and orthogonal arrays because, for them, a (T, M, S)-net is an unusual ana-

log of an orthogonal array and we are interested in how constructions and bounds can be adapted to this new situation. The problem is of interest to coding theorists not only because of the similarity between error-correcting codes and the duals of (T, M, S)-nets (which we won't define here), but because these may be useful in digital communications under a new error model, the "synchronization channel". But, most importantly, the constructions and bounds for (T, M, S)-nets are of great importance to practitioners in Monte Carlo and Quasi-Monte Carlo methods (numerical integration, simulation, global optimization). The practitioner must choose which net to implement in complex software packages and knowing that a given net is optimal will affect the longevity of the code and the user's confidence in its efficiency.

3 Contribution to the problem

In this talk, we bridge the gap between numerical finite bounds obtained using floating point software (in this case, CPLEX, a powerful optimization package) and publishable bounds in exact arithmetic and (hopefully) analytic bounds valid for all dimensions. The problems in making this leap are many-fold. First, the optimization software reports questionable data which cannot be trusted enough for publication purposes. On the other hand, going directly to a computer algebra system working in exact arithmetic is not feasible since linear programming problems with tens of thousands of variables seem to be beyond the reach of MAPLE, etc.

Once this hurdle is conquered and provable bounds are obtained for small dimensions, the next contribution is to extrapolate these results to obtain bounds for all dimensions. We sought patterns in solution families and conjectured that this behavior continues. In some cases, we applied ideas from formal power series to prove such bounds for an infinite family of linear programming problems of this type. These are the first ever analytic solutions to the linear programming problem for (T, M, S)-nets.

4 Originality of the contribution

An *ordered orthogonal array* $\mathrm{OOA}_\lambda(t, s, \ell, b)$ is a $\lambda b^t \times s\ell$ array over an alphabet of size b with the property that for any "left-justified" set $A = \{(i, j) : 1 \leq i \leq s, 1 \leq j \leq t_i, \sum t_i = t\}$ of t columns, the subarray restricted to columns in A contains each t-tuple over b exactly λ times as a row. Mullen/Schmid and Lawrence proved that a (T, M, S)-net in base b exists if and only if an $\mathrm{OOA}_\lambda(M - T, S, M - T, b)$ exists with $\lambda = b^T$.

In [3], Martin and Stinson derived a linear programming bound for ordered orthogonal arrays. This is a special case of a general result of Delsarte [1].

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 $z_{\ell+1} = 0$.

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:

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

In our approach, we express the dual of the linear program of Martin and Stinson in terms of multivariate polynomials.

For any ordered orthogonal array $\mathrm{OOA}(t, s, \ell, b)$, the number of rows is bounded below by the objective value of any feasible solution to the following LP:

maximize		$[z_0^s] g(\mathbf{z})$
subject to		
$[\mathbf{z}^{\mathbf{e}}] g(\mathbf{z})$	$\geq$	0 for all $\mathbf{e} \neq 0$
$g(\mathbf{z})$	$=$	$\sum_{\mathbf{e}} B_{\mathbf{e}} P_{\mathbf{e}}(\mathbf{z})$ with
$B_{\mathbf{e}}$	$\leq$	0 whenever $\mathsf{ht}(\mathbf{e}) > t$
$B_{\mathbf{0}}$	$=$	1

Our approach is then to find families of polynomials $g(\mathbf{z})$ feasible for this problem and thereby give lower bounds for the quality parameter T of a (T, M, S)-net for $S \to \infty$.

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, but almost nothing is known for the cases $\ell \geq 2$.

5 Non-triviality of the contribution

The solution presented here involved months of computing just to get the numerical data from CPLEX. Next, a continued fractions technique was used to help

MAPLE guess various rational solutions to the optimization problem. With this rational data in hand, we were able to make several conjectures as to what the asymptotic behavoir should be. The most difficult step, in collaboration with Terry Visentin at the University of Winnipeg, was to derive algebraic proofs of these bounds. So the overall solution required tools from coding theory, optimization, numerical analysis, number theory, algebra and combinatorics. As well, the theory of association schemes and ideas from combinatorial design theory played a crucial role in the development of the theory that made this result possible.

References

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

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

[3] 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.

[4] 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.

[5] W. J. Martin and T. I. Visentin. A dual Plotkin bound for (T, M, S)-nets. Submitted, *IEEE Trans. Info. Theory* (2005).

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

[7] 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.

[8] M. Yu. Rosenbloom and M. A. Tsfasman, Codes for the m-metric, *Problems of Information Transmission* **33** (no. 1) (1997), 45–52.

[9] W. Schmid, (t, m, s)-nets: Digital constructions and combinatorial aspects, Doctoral Dissertation, University of Salzburg, (1995).

[10] 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, ed s.), Springer-Verlag, 2005 (to appear).

[11] 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.