A note on the duality of linear programming bounds for orthogonal arrays and codes

Jürgen Bierbrauer
Department of Mathematical Sciences
Michigan Technological University
Houghton, MI 49931

K. Gopalakrishnan
Department of Computer Science
Wichita State University
Wichita, KS 67260

D. R. Stinson
Department of Computer Science and Engineering
University of Nebraska - Lincoln
Lincoln, NE 68588

September 6, 2001

Abstract

In this brief note, we exhibit a duality between linear programming bounds for codes and orthogonal arrays. This duality is based on the elementary observation that the same linear program can be used to obtain bounds for both codes and orthogonal arrays. Whenever a linear programming bound for a code is derived, a corresponding bound for orthogonal arrays is obtained "for free", and vice versa.

Keywords: code, orthogonal array, linear programming bounds

1 Basic results

In this section, we review the basic results pertaining to linear programming bounds that we need. This theory is due to Delsarte, and can be found in standard textbooks such as MacWilliams and Sloane [6].

An (n, M) *binary code* is a set $\mathcal{C}$ of M binary vectors of length n. The *distance distribution* of $\mathcal{C}$ is defined to be the sequence $(A_0, A_1, \ldots, A_n)$, where

$$A_i = \frac{1}{M}|\{(u,v) : u, v \in \mathcal{C}, d(u,v) = i\}|,$$

$i = 0, \ldots, n$, and $d(u,v)$ denotes the Hamming distance between the two vectors u and v. The following properties are easily verified:

$$A_0 = 1, \tag{1}$$

$$A_i \geq 0 \quad \text{for } 0 \leq i \leq n, \quad \text{and} \tag{2}$$

$$A_0 + A_1 + \ldots + A_n = M. \tag{3}$$

$\mathcal{C}$ is said to have *distance* d provided that $A_i = 0$ for $1 \leq i \leq d-1$, and $A_d > 0$.

Let k be a non-negative integer, and let $P_k(x)$ be the *Krawtchouk polynomial* defined as follows:

$$P_k(x) = \sum_{j=0}^{k} (-1)^j \binom{x}{j} \binom{n-x}{k-j}.$$

The *dual distance distribution* of the code $\mathcal{C}$ is defined to be the sequence $(A_0^{'}, A_1^{'}, \ldots, A_n^{'})$, where

$$A_i^{'} = \frac{1}{M} \sum_{j=0}^{n} A_j P_i(j),$$

$i = 0, \ldots, n$. We will express this notationally as

$$(A_0^{'}, A_1^{'}, \ldots, A_n^{'}) = \mathsf{Kr}(A_0, A_1, \ldots, A_n).$$

The following properties, analogous to (1), (2) and (3), were proved by Delsarte:

$$A_0^{'} = 1, \tag{4}$$

$$A_i^{'} \geq 0 \quad \text{for } 0 \leq i \leq n, \quad \text{and} \tag{5}$$

$$A_0^{'} + A_1 + \ldots + A_n = \frac{2^n}{M}. \tag{6}$$

Delsarte further showed that Kr is an involutory transformation:

$$\mathsf{Kr}(A_0^{'}, A_1^{'}, \ldots, A_n^{'}) = (A_0, A_1, \ldots, A_n). \tag{7}$$

If $A_i^{'} = 0$ for $1 \le i \le d^{'} - 1$ and $A_{d'}^{'} > 0$, then $d^{'}$ is called the *dual distance* of the code $\mathcal{C}$. If we write the vectors in $\mathcal{C}$ as rows of an $M \times n$ array, then Delsarte showed that any set of $r \le d^{'} - 1$ columns contains each r-tuple exactly $M/2^r$ times. In other words $\mathcal{C}$ is a *binary orthogonal array* of *strength* $d^{'} - 1$.

2 The linear programming approach

Let d and n be positive integers such that $d \le n$. We employ the following linear program, $\mathsf{L}(n, D)$, which is identical to the one considered in [7].

$$\boxed{\begin{array}{ll}
\multicolumn{2}{l}{\text{Maximize } S = x_0 + x_1 + \cdots + x_n \text{ subject to}} \\
& \\
x_0 = 1 & \\
x_i = 0 & \text{for } 1 \le i \le D - 1 \\
x_i \ge 0 & \text{for } D \le i \le n \\
\sum_{j=0}^{n} x_j P_i(j) \ge 0 & \text{for } 0 \le i \le n.
\end{array}}$$

Theorem 2.1 *Suppose that $\mathcal{C}$ is an (n, M) binary code. Then the following hold:*

1. *Let S_{opt} be the optimal solution to $\mathsf{L}(n, d)$. If $\mathcal{C}$ has distance d, then $M \le S_{\mathsf{opt}}$.*

2. *Let S_{opt} be the optimal solution to $\mathsf{L}(n, d^{'})$. If $\mathcal{C}$ has dual distance $d^{'}$, then $M \ge 2^n / S_{\mathsf{opt}}$.*

Proof. Let $(A_0, A_1, \ldots, A_n)$ be the distance distribution of an (n, M) binary code $\mathcal{C}$ having distance d, and let $(A_0^{'}, A_1^{'}, \ldots, A_n^{'})$ be the dual distance distribution of $\mathcal{C}$.

The first assertion is proved in [7], as follows. We claim that $(A_0, \ldots, A_n)$ is a feasible solution for $\mathsf{L}(n, d)$. That the constraints of $\mathsf{L}(n, d)$ are satisfied follows immediately from (1), (2) and (5), and the fact that $\mathcal{C}$ is assumed to have distance d. Then, from (3), the resulting value of the objective function is M, so the first assertion follows.

To prove the second assertion, we show that $(A_1^{'}, \ldots, A_n^{'})$ is a feasible solution for $\mathsf{L}(n, d^{'})$. This follows in a similar way from (2), (4), (5) and (7). Then, from (6), the resulting value of the objective function is $2^n/M$, so the second assertion follows, as well. $\square$

Bounds on the optimal solution S_{opt} for the LP $\mathsf{L}(n, D)$ are usually obtained by finding a feasible solution in the dual LP, $\mathsf{L}^*(n, D)$. If S^* is the value of the objective function at any feasible solution of $\mathsf{L}^*(n, D)$, then $S^* \geq S_{\mathsf{opt}}$. Now, applying Theorem 2.1, we see that any such value S^* simultaneously yields an upper bound on the size of a binary code with distance $d = D$ and a lower bound on the size of a binary orthogonal array with strength $D - 1$ (i.e., dual distance $d^{'} = D$). We give several examples of pairs of bounds obtained in this way in the next section.

3 Some pairs of dual bounds

Let $M(n, d)$ denote the maximum M such that an (n, M) binary code with distance d exists. Let $N(n, d^{'})$ denote the minimum M such that an (n, M) binary code with dual distance distance d' exists (i.e., $N(n, d^{'})$ is the minimum number of rows in a binary orthogonal array of strength $d^{'} - 1$ having n columns).

We now proceed to state various bounds which follow from Theorem 2.1, using known upper bounds on $S_{\mathsf{opt}}(n, D)$ (all of which can be found in [6], unless otherwise indicated). We start with the Singleton bounds.

Theorem 3.1 (Singleton bounds) *The following bounds hold:*

$$M(n, d) \leq 2^{n-d+1} \qquad \textit{and} \qquad N(n, d^{'}) \geq 2^{d^{'}-1}.$$

The Singleton bound is the really the code bound; the orthogonal array bound is completely trivial

Let us turn now to the Plotkin bounds.

Theorem 3.2 (Plotkin bounds) *Suppose that $d > n/2$ and $d^{'} > n/2$. Then the following bounds hold:*

$$M(n, d) \leq \frac{2d}{2d - n} \qquad \textit{and} \qquad N(n, d^{'}) \geq 2^n - \frac{n2^{n-1}}{d^{'}}.$$

It is interesting to note that, although the Plotkin bound for codes has been known for many years, the corresponding orthogonal array bound was only proved quite recently, by Friedman [3].

We can say a bit more about the Plotkin bounds. In [1], a simple formula for the optimal solution of the LP $\mathsf{L}(n, D)$ was obtained for a large class of parameters. To be precise, if D is even and $D \leq n \leq 2D-1$, then it was proved in [1, Theorem 8.1] that $S_{\mathsf{opt}}(n,D) = 2D/(2D-n)$. This means that the bounds of Theorem 3.2 are equivalent to the linear programming bounds in these parameter situations.

We proceed to the Hamming and Rao bounds. The Hamming bound refers to codes while the Rao bound [8] is the corresponding bound for orthogonal arrays.

Theorem 3.3 (Hamming-Rao bounds) *Suppose that d and d' are odd, $d = 2e+1$ and $d' = 2e'+1$. Then the following bounds hold:*

$$M(n,d) \leq \frac{2^n}{\sum_{i=0}^{e} \binom{n}{i}} \qquad \text{and} \qquad N(n,d') \geq \sum_{i=0}^{e'} \binom{n}{i}.$$

Finally, we look at the MRRW bounds, due to McEliece, Rodemich, Rumsey and Welch [7]. First, we consider the explicit version of their bounds, which derive from a bound on $S_{\mathsf{opt}}(n,D)$ given as [7, Eq. (3.13)].

Theorem 3.4 (MRRW bounds) *Suppose that $d, d' \geq x_1^{(s)}$, where $x_1^{(s)}$ is the smallest root of $P_s(x)$, and suppose that $s < n/2$. Then the following bounds hold:*

$$M(n,d) \leq \binom{n}{s} \frac{(n+1)^2}{2(s+1)} \qquad \text{and} \qquad N(n,d') \geq \frac{2^{n+1}(s+1)}{\binom{n}{s}(n+1)^2}.$$

Further study of the values of the smallest roots of the Krawtchouk polynomials leads to asymptotic bounds, which we describe now. For a real number δ such that $0 < \delta < 1$, define the binary entropy function

$$h(x) = -x \log_2(x) - (1-x)\log_2(1-x).$$

For $0 < \delta < 1$, define

$$R(\delta) = \limsup_{n\to\infty} \frac{\log_2 M(n,\delta n)}{n},$$

and for $0 < \delta' < 1$, define

$$R'(\delta') = \liminf_{n\to\infty} \frac{\log_2 N(n,\delta n)}{n}.$$

We now state the bound for codes proved in [7], and the corresponding result for orthogonal arrays, which appears to be new.

Theorem 3.5 (Asymptotic MRRW bounds) *Let* $0 < \delta < 1$ *and* $0 < \delta^{'} < 1$. *Then the following bounds hold:*

$$R(\delta) \leq h\left(\frac{1}{2} - \sqrt{\delta(1-\delta)}\right) \qquad \textit{and} \qquad R^{'}(\delta^{'}) \geq 1 - h\left(\frac{1}{2} - \sqrt{\delta^{'}(1-\delta^{'})}\right).$$

4 Comments

This research first appeared in the PhD thesis of the second author [4]. Similar results have also been proved by Levenshtein [5]; however, our approach is more elementary.

References

[1] J. Bierbrauer, K. Gopalakrishnan and D. R. Stinson. Orthogonal arrays, resilient functions, error-correcting codes and linear programming bounds. *SIAM J. Discrete Math.* **9** (1996), 424–452.

[2] P. Delsarte. An algebraic approach to the association schemes of coding theory. *Philips Research Reports Supplements*, #10, 1973.

[3] J. Friedman. On the bit extraction problem. In "Proceedings of the 33rd IEEE Symposium on the Foundations of Computer Science", 1992, pp. 314–319.

[4] K. Gopalakrishnan. *A Study of Correlation-immune, Resilient and Related Cryptographic Functions*, PhD Thesis, University of Nebraska-Lincoln, 1994.

[5] V. I. Levenshtein. Krawtchouk polynomials and universal bounds for codes and designs in Hamming spaces. *IEEE Transactions on Information Theory* **41** (1995), 1303–1321.

[6] F. J. MacWilliams and N. J. A. Sloane. *The theory of error-correcting codes*, North-Holland, 1977.

[7] R. J. McEliece, E. R. Rodemich, H. Rumsey and L. R. Welch. New upper bounds on the rate of a code via the Delsarte-MacWilliams inequalities. *IEEE Transactions on Information Theory* **23** (1977), 157–166.

[8] C. R. Rao. Factorial experiments derivable from combinatorial arrangements of arrays. *J. Royal Stat. Soc.* **9** (1947), 128–139.