# 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 Mathematics
East Carolina University
Greenville, NC 27858

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

October 13, 1997

**Abstract**

In this expository note, we exhibit a duality between linear programming bounds for codes and orthogonal arrays that was pointed out by Levenshtein in [7]. This duality implies that whenever a linear programming bound for a code is derived, a corresponding bound for orthogonal arrays is obtained "for free", and vice versa. We give an elementary proof of this result which follows from the observation that the same linear program can be used to obtain bounds for both codes and orthogonal arrays. Then we survey the dual pairs of bounds that can be obtained as a consequence.

## 1 Introduction

An $(n, M)$ *binary code* is a set $\mathcal{C}$ of $M$ binary vectors of length $n$. $\mathcal{C}$ is said to have *distance* $d$ if $d$ is the minimum hamming distance between any two distinct vectors in $\mathcal{C}$. The classical Hamming bound for binary codes [6] was proved in 1950. It states that

$$M \leq \frac{2^n}{\sum_{i=0}^{\frac{d-1}{2}} \binom{n}{i}}$$

if $\mathcal{C}$ is an $(n, M)$ binary code having odd distance $d$. This is easily proved by observing that the $M$ spheres of radius $(d-1)/2$, whose centres are the vectors in $\mathcal{C}$, are disjoint.

An $(n, N)$ *binary orthogonal array* of *strength* $t$ is an $N \times n$ binary array, $\mathcal{D}$, such that any set of $t$ (or fewer) columns of $\mathcal{D}$ contains each binary $t$-tuple exactly $N/2^t$ times, and $t$ is the largest integer having this property. The classical Rao bound for binary orthogonal arrays [10] was proved in 1947. It states that

$$N \geq \sum_{i=0}^{\frac{t}{2}} \binom{n}{i}$$

if $\mathcal{D}$ is an $(n, N)$ binary orthogonal array of even strength $t$.

We sketch a fairly easy proof of the Rao bound: First, replace every entry $i$ in $\mathcal{D}$ by $(-1)^i$ (hence 1 becomes $-1$ and 0 becomes 1). Now, let $D_1, \ldots, D_n$ be the columns of $\mathcal{D}$, considered as vectors in $\mathrm{R}^N$. Construct all the vectors that can be formed as the componentwise product of at most $t/2$ vectors chosen from $D_1, \ldots, D_n$. (This includes the all-ones vector, which is the componentwise product of none of these vectors.) The resulting set of $\sum_{i=0}^{\frac{t}{2}} \binom{n}{i}$ vectors can be shown to be mutually orthogonal, and hence they are linearly independent vectors in $\mathrm{R}^N$. The bound follows.

The Hamming and Rao bounds have an obvious similarity in form, though the proof methods given above seem to be completely different. The purpose of this note is to explore the relationship between these and other pairs of "dual bounds". The link is provided by the linear programming bounds due to Delsarte. We describe the basic theory we need in the next section. The main result on dual bounds is proved in Section 3, and a short survey of dual bounds is provided in Section 4.

## 2 Delsarte theory

In this section, we review the basic results of Delsarte theory [3] that will allow us to prove our results on linear programming bounds. This theory can be found in standard textbooks such as MacWilliams and Sloane [8].

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

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

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

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

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

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

Observe that $\mathcal{C}$ has 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 $\mathsf{Kr}$ 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 $1 \leq i \leq d^{'} - 1$ and $A_{d'}^{'} > 0$, then $d^{'}$ is called the *dual distance* of the code $\mathcal{C}$. Suppose we write the vectors in $\mathcal{C}$ as rows of an $M \times n$ array, $\mathcal{D}$. Delsarte showed that any set of $r \leq d^{'} - 1$ columns contains each $r$-tuple exactly $M/2^r$ times, and $d^{'}$ is the largest integer with this property. In other words $\mathcal{C}$ is an $(n, M)$ binary orthogonal array of strength $t = d^{'} - 1$. Thus, the strength of $\mathcal{D}$ (as an orthogonal array) is specified in terms of the dual distance of $\mathcal{C}$.

## 3 Linear programming bounds

Let $d$ and $n$ be positive integers such that $d \leq n$. We employ the following linear program, $\mathsf{L}(n, D)$, which is identical to the one considered in [9].

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

The following is our main result.

**Theorem 3.1** *Suppose that $\mathcal{C}$ is an $(n, M)$ binary code. Then the following hold:*

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

*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 [9], 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 $(A_0^{'}, \ldots, A_n^{'})$ 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. $\square$

In [7, Corollary 2.9], Levenshtein proves an equivalent result in a slightly different way. Levenshtein begins with two LPs, one for codes and one for orthogonal arrays (which are referred to as "designs"). Given a polynomial which provides an optimal solution for one LP, it is shown how to construct a *dual polynomial* which provides an optimal solution for the other one. From the way in which the dual polynomial is constructed, it can be verified that the product of the optimal solutions of the two LPs is $2^n$.

The novelty of our approach is in using the same LP for both codes and orthogonal arrays. As a consequence, the duality between the LP bounds for codes and orthogonal arrays becomes completely transparent.

Bounds on the optimal solution $S_{\mathsf{opt}}$ 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 3.1, 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.

## 4 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 3.1, using known upper bounds on $S_{\mathsf{opt}}(n, D)$. (All the upper bounds on

$S_{\mathsf{opt}}(n, D)$ that we use can be found in [8], unless otherwise indicated.) We start with the Singleton bounds.

**Theorem 4.1 (Singleton bounds)** *The following bounds hold:*

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

The term "Singleton bound" refers to the bound for codes. The corresponding orthogonal array bound is completely trivial.

Let us turn now to the Plotkin bounds.

**Theorem 4.2 (Plotkin bounds)** *Suppose that $d > n/2$ and $d^{'} > n/2$. Then the following bounds hold:*

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

It is interesting to note that, although the Plotkin bound for codes has been known since 1951 [8, p. 741], the corresponding orthogonal array bound was only proved quite recently, by Friedman [4]. We also observe that a simple formula for the optimal solution of the LP $\mathsf{L}(n, D)$ was obtained in [2] 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 [2, Theorem 8.1] that $S_{\mathsf{opt}}(n, D) = 2D/(2D-n)$. This means that the bounds of Theorem 4.2 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 [10] is the corresponding bound for orthogonal arrays.

**Theorem 4.3 (Hamming-Rao bounds)** *Suppose that $d$ and $d^{'}$ are odd, $d = 2e + 1$ and $d^{'} = 2e^{'} + 1$. Then the following bounds hold:*

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

This theorem can also be used to obtain bounds when $d$ or $d^{'}$ are even. It is well-known that

$$M(n, d) = M(n - 1, d - 1)$$

if $d$ is even; and

$$N(n,d') = 2N(n-1,d'-1)$$

if $d'$ is even. The bounds are obtained by applying these relations in conjunction with Theorem 4.3.

Finally, we look at the MRRW bounds, due to McEliece, Rodemich, Rumsey and Welch [9]. First, we consider the explicit version of their bounds, which derive from a bound on $S_{\mathsf{opt}}(n,D)$ given as [9, Eq. (3.13)].

**Theorem 4.4 (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:*

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

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 $\delta$ 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 [9], and the corresponding result for orthogonal arrays.

**Theorem 4.5 (Asymptotic MRRW bounds)** *Let $0 < \delta < 1$ and $0 < \delta' < 1$. Then the following bounds hold:*

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

Other examples of dual pairs of bounds can be found in the paper by Levenshtein [7]. As well, most of the bounds can be extended in a straightforward manner to codes and orthogonal arrays over non-binary alphabets.

## 5 Comments

Our approach to dual pairs of bounds first appeared in [5], the PhD thesis of the second author, in 1994 (see also Bierbrauer, Gopalakrishnan and Stinson [1, p. 253]). This exposition is based on the treatment in [5].

## References


[1] J. Bierbrauer, K. Gopalakrishnan and D. R. Stinson. Bounds for resilient functions and orthogonal arrays, *Lecture Notes in Computer Science* **839** (1994), 247–256 (Advances in Cryptology, Proceedings of CRYPTO '94).

[2] 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.

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

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

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

[6] R. W. Hamming. Error detecting and error correcting codes. *Bell Systems Technical Journal* **29** (1950), 147–160.

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

[8] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes*, North-Holland, 1977.

[9] 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.

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