The 32nd Symposium on Information Theory
and its Applications (SITA2009)
Yuda-Onsen, Yamaguchi, Japan, Dec. 1–4, 2009

A Linear Programming Bound for Unequal Error Protection Codes

Tomohiko Saito* Yoshifumi Ukita† Toshiyasu Matsushima‡ Shigeichi Hirasawa§

Abstract— In coding theory, it is important to calculate an upper bound for the size of codes given the length and minimum distance. The Linear Programing (LP) bound is known as a good upper bound for the size of codes. On the other hand, Unequal Error Protection (UEP) codes have been studied in coding theory. In UEP codes, a codeword has special bits which are protected against a greater number of errors than other bits. In this paper, we propose a LP bound for UEP codes. Firstly, we generalize the distance distribution (or weight distribution) of codes. Under the generalization, we lead to the LP bound for UEP codes. Lastly, we compare the proposed bound with a modified Hamming bound.

Keywords— Linear Programing, Hamming bound, Unequal Error Protection Codes,

1 Introduction

One of the most basic problem in coding theory is to find the largest code given the length n and minimum distance d. And it is also important to calculate an upper bound for the size of codes, in order to evaluate codes found by certain methods.

Many upper bounds have been proposed, for example the Hamming bound, the Singleton bound and so on [6]. Delsarte proposed the Linear Programming (LP) bound [1]. It is known that the LP bound is better upper bound than most of the other bounds in many parameters.

On the other hand, Unequal Error Protection (UEP) codes were proposed by Masnick and Wolf [7]. UEP codes are divided to two types. The one is bit-wise UEP codes [7], and the other is message-wise UEP codes [2], [3]. In this paper, we focus on bit-wise UEP codes.

In UEP codes, a codeword has special bits which are protected against a greater number of errors than other bits. Thus a criterion different from the *minimum distance* is needed to evaluate UEP codes.

In this paper, we propose a LP bound for UEP codes. Firstly, we generalize the distance distribution (or weight distribution) of codes. Under the generalization, we lead to the LP bound for UEP codes. Lastly, we compare the proposed bound with a modified Hamming bound.

This paper is organized as follows. In Section 2, we describe some basic notations and definitions. Especially, we describe the definition of UEP codes. Also, we show the Hamming bound in Section 2. In Section 3, we show the LP bound proposed by Delsarte. In Section 4, we propose a LP bound for UEP codes. Most of the proof of theorems in Section 4 are described in Section 5. Lastly, we conclude our research in Section 6.

2 Preliminary

For any $\boldsymbol{x} \in \{0,1\}^n$, let $\mathrm{wt}(\boldsymbol{x})$ be the Hamming weight of $\boldsymbol{x}$. Let $\oplus$ be the exclusive-or operation, and $\cdot$ be the and operation. For any $\boldsymbol{x} = (x_1, x_2, \ldots, x_n)$, $\boldsymbol{y} = (y_1, y_2, \ldots, y_n) \in \{0,1\}^n$, let $\boldsymbol{x} \oplus \boldsymbol{y} = (x_1 \oplus y_1, x_2 \oplus y_2, \ldots, x_n \oplus y_n)$, and $\boldsymbol{x} \cdot \boldsymbol{y} = x_1 \cdot y_1 \oplus x_2 \cdot y_2 \oplus \cdots \oplus x_n \cdot y_n$. For any set A, let $|A|$ be the number of elements of A. The binomial coefficient $\left(\begin{array}{c} x \\ m \end{array} \right)$ is defined by

$$\left(\begin{array}{c} x \\ m \end{array} \right) = \begin{cases} \frac{x(x-1)\cdots(x-m+1)}{m!}, & \\ & \text{if } m \text{ is a positive integer }, \\ 1 & \text{if } m = 0 \ , \\ 0 & \text{otherwise }, \end{cases} \tag{1}$$

where x is any real number, and $m! = 1 \cdot 2 \cdot \cdots \cdot (m-1) \cdot m$, $0! = 1$.

Definition 1 ((n, M, D) binary code) *Let n be any positive integer and $D \subseteq \{0,1\}^n$. If a subset $C \subseteq \{0,1\}^n$ satisfies*

$$|C| = M, \tag{2}$$

$$\forall \boldsymbol{x}, \boldsymbol{y} \in C, \forall \boldsymbol{z} \in D, \quad \boldsymbol{x} \oplus \boldsymbol{y} \neq \boldsymbol{z}, \tag{3}$$

then C is called an (n, M, D) binary code.

In this paper, we consider only binary codes, so we omit the word “binary” in the following. If a code C is a linear vector space, then C is called a *linear code.*

If

$$D = \{\boldsymbol{z} \in \{0,1\}^n | wt(\boldsymbol{z}) \leq d-1\}, \tag{4}$$

then an (n, M, D) code has the *minimum distance d*, and this code is also called an *(n, M, d) code.*

Next, we define UEP codes.

Definition 2 (unequal error protection code) *An (n, M, D) code is called an $((n_1, n_2), M, (d_1, d_2))$ unequal error protection* (UEP) *code, if*

$$D = \{\boldsymbol{z} = (\boldsymbol{z}_1, \boldsymbol{z}_2) \in \{0,1\}^{n_1} \times \{0,1\}^{n_2} | \\ (\boldsymbol{z}_1 \neq \boldsymbol{0}, wt(\boldsymbol{z}) \leq d_1 - 1) \text{ or } \\ (wt(\boldsymbol{z}) \leq d_2 - 1)\}, \tag{5}$$

where $n = n_1 + n_2$ and $d_1 \geq d_2$.

[*] College of Science and Engineering, Aoyama Gakuin University, Sagamihara, Kanagawa 229-8558, Japan.

[†] Department of Management Information, Yokohama College of Commerce, Kanagawa 230-8577, Japan.

[‡] School of Fundamental Science and Engineering, Waseda University, Tokyo 169-8555, Japan.

[§] Research Institute for Science and Engineering, Waseda University, Tokyo 169-8555, Japan, and Cyber University, Tokyo 162-0853, Japan.

In this paper, we consider UEP codes which have only two error protection levels, d_1 and d_2, for simplicity. An $((n_1, n_2), M, (d_1, d_2))$ UEP code can correct errors included in an error pattern E,

$$E = \{\boldsymbol{e} = (\boldsymbol{e}_1, \boldsymbol{e}_2) \in \{0,1\}^{n_1} \times \{0,1\}^{n_2} | \\ (\boldsymbol{e}_1 \neq \boldsymbol{0}, wt(\boldsymbol{e}) \leq t_1) \text{ or} \\ (wt(\boldsymbol{e}) \leq t_2)\}, \quad (6)$$

where $t_i = \lfloor \frac{d_i - 1}{2} \rfloor$, $i = 1, 2$.

Next, we show one of upper bounds for (n, M, D) codes. Later, this bound is compared with the LP bound.

Theorem 1 *Let $E \subseteq \{0,1\}^n$ and let $D = \{\boldsymbol{e}_1 \oplus \boldsymbol{e}_2 | \boldsymbol{e}_1, \boldsymbol{e}_2 \in E\}$. Then any (n, M, D) codes satisfy*

$$M \leq \frac{2^n}{|E|}. \quad (7)$$

If $E = \{\boldsymbol{e} \in \{0,1\}^n | wt(\boldsymbol{e}) \leq t\}$ and $D = \{\boldsymbol{z} \in \{0,1\}^n | wt(\boldsymbol{z}) \leq 2t\}$, then Eq. (7) becomes

$$M \leq \frac{2^n}{\sum_{i=0}^{t} \binom{n}{i}}. \quad (8)$$

Eq. (8) is called the Hamming bound [6, Ch.1 Theorem 6].

3 LP bounds

In this section, we show the LP bound for (n, M, d) codes proposed by Delsarte [1]. In Section 3.1, we show some definitions and theorems, which are used to show the LP bound. In Section 3.2, we show the LP bound.

3.1 Basic Theorems

Definition 3 ($W_i^{(n)}$) *For any positive integer n, $W_i^{(n)}$ $(= W_i)$, $i = 0, 1, \ldots n$, are defined by*

$$W_i^{(n)} := \{\boldsymbol{w} \in \{0,1\}^n | wt(\boldsymbol{w}) = i\}. \quad (9)$$

If there is no danger of confusion we omit the n.

The *distance distribution of a code* $C(\subseteq \{0,1\}^n)$ is $(n+1)$-tuple $(A_0, A_1, \ldots, A_n)$, where

$$A_i = \frac{1}{|C|} \sum_{\boldsymbol{x} \in C} \Big| \{\boldsymbol{y} \in C | \boldsymbol{x} \oplus \boldsymbol{y} \in W_i\} \Big|, i = 0, 1, \ldots, n. \quad (10)$$

If C is a linear code, the distance distribution A_i is equal to the *weight distribution* A'_i, that is

$$A_i = A'_i \left(= \Big| \{\boldsymbol{y} \in C | \boldsymbol{y} \in W_i\} \Big| \right), i = 0, 1, \ldots, n. \quad (11)$$

Definition 4 (Krawtchouk polynomial) *For any positive integer n, the Krawtchouk polynomial $P_i(z; n)(= P_i(z))$ is defined by*

$$P_i(z; n) := \sum_{k=0}^{i} (-1)^k \binom{z}{k} \binom{n-z}{i-k}, \\ i = 0, 1, \ldots n, \quad (12)$$

where z is an indeterminate. If there is no danger of confusion we omit the n.

The next Theorem 2, 3, and 4, give properties of the Krawtchouk polynomial.

Theorem 2 [4, Theorem 4.10] *If $\boldsymbol{v} \in W_j$, then*

$$\sum_{\boldsymbol{u} \in W_i} (-1)^{\boldsymbol{u} \cdot \boldsymbol{v}} = P_i(j). \quad (13)$$

where $i, j \in \{0, 1, \ldots, n\}$.

Theorem 3 [6, Ch.5 Theorem 16] *For any $a, b \in \{0, 1, \ldots, n\}$,*

$$\sum_{i=0}^{n} \binom{n}{i} P_a(i) P_b(i) = 2^n \binom{n}{a} \delta_{a,b}, \quad (14)$$

where $\delta_{a,b} = 1$, if $a = b$, $\delta_{a,b} = 0$, if $a \neq b$ is the Kronecker symbol.

Theorem 4 [6, Ch.5 Theorem 17] *For any $a, b \in \{0, 1, \ldots, n\}$,*

$$\binom{n}{a} P_b(a) = \binom{n}{b} P_a(b). \quad (15)$$

The next Theorem 5 is called the MacWilliams theorem. This theorem shows a relationship between a code C and the dual code $C^\perp$.

Theorem 5 [6, Ch.5 Theorem 1] *Let $C(\subseteq \{0,1\}^n)$ be a linear code, and $C^\perp$ be the dual code of C. Let A_i and $A_i^\perp$, $i = 0, 1, \ldots, n$, be the distance distribution of C and $C^\perp$. Then,*

$$A_i^\perp = \frac{1}{|C|} \sum_{j=0}^{n} A_j P_i(j), i = 0, 1, \ldots, n. \quad (16)$$

In Theorem 5, C is constrained to a linear code. But, even if C is a nonlinear code, the MacWilliams theorem holds [6, Ch.5 Sec.5].

The next theorem 6 is proposed by Delsarte. This theorem is especially important in the LP bound.

Theorem 6 [6, Ch.5 Theorem 6] *Let $C(\subseteq \{0,1\}^n)$ be a code, and $A_i, i = 0, 1, \ldots, n$ be the distance distribution of C. Then,*

$$\frac{1}{|C|} \sum_{j=0}^{n} A_j P_i(j) \geq 0, \quad i = 0, 1, \ldots, n. \quad (17)$$

The left-hand side of Eq. (17) is equal to the right-hand side of Eq. (16). Thus, we can see that the distance distribution of the dual code is non-negative.

3.2 LP Bounds

Definition 5 ($M_{LP}(n; d)$) *$M_{LP}(n; d)$ is defined by the solution to the following linear programming problem: choose real numbers $A_0, A_1, \ldots, A_n$ so as to*

$$\textit{maximize} \quad \sum_{i=0}^{n} A_i \quad (18)$$

subject to the constraints

$$A_0 = 1, \tag{19}$$

$$A_i = 0, i = 1, 2, \ldots, d-1, \tag{20}$$

$$A_i \geq 0, i = d, d+1, \ldots, n, \tag{21}$$

$$\sum_{j=0}^{n} A_j P_i(j) \geq 0, i = 0, 1, \ldots n. \tag{22}$$

The next Theorem 7 gives the LP bound.

Theorem 7 *[6, Ch.17 Theorem 18] Any (n, M, d) codes satisfy*

$$M \leq M_{LP}(n; d). \tag{23}$$

The next Theorem 8 compares the LP bound with the Hamming bound, Eq. (8).

Theorem 8 [6, Ch.17 Problem(16)] *Let $d = 2t+1$. Then*

$$M_{LP}(n; d) \leq \frac{2^n}{\sum_{i=0}^{t} \left(\begin{array}{c} n \\ i \end{array} \right)}. \tag{24}$$

Theorem 8 means that the LP bound is a better upper bound than the Hamming bound.

4 LP Bounds for UEP Codes

In this section, we propose a LP bound for UEP codes. In Section 4.1, we generalize the definitions and theorems in Section 3.1. In Section 4.2, we show the LP bound for UEP codes.

4.1 Generalization of Basic Theorems

Definition 6 ($W_{i,j}^{(n_1,n_2)}$) *Let n, n_1 and n_2 be any positive integers, where $n = n_1 + n_2$. Then $W_{i,j}^{(n_1,n_2)}(= W_{i,j})$, $i = 0, 1, \ldots, n_1$, $j = 0, 1, \ldots, n_2$ are defined by*

$$W_{i,j}^{(n_1,n_2)} := \{\boldsymbol{w} = (\boldsymbol{w}_1, \boldsymbol{w}_2) \in \{0,1\}^{n_1} \times \{0,1\}^{n_2} | \\ wt(\boldsymbol{w}_1) = i, wt(\boldsymbol{w}_2) = j\}. \tag{25}$$

And, we let

$$W_U := \{W_{i,j}^{(n_1,n_2)} | i = 0, 1, \ldots, n_1, j = 0, 1, \ldots, n_2\}. \tag{26}$$

If there is no danger of confusion we omit the n_1, n_2.

If $n_1 = n$ and $n_2 = 0$, then $W_{i,j}$ is equal to W_i, defined by Eq. (9).

The *distribution based on W_U of a code $C (\subseteq \{0,1\}^n)$* is $(n_1+1) \times (n_2+1)$ array $(B_{i,j})_{i=0,1,\ldots n_1, j=0,1,\ldots n_2}$, where

$$B_{i,j} = \frac{1}{|C|} \sum_{\boldsymbol{x} \in C} \left| \{\boldsymbol{y} \in C | \boldsymbol{x} \oplus \boldsymbol{y} \in W_{i,j}\} \right|, \\ i = 0, 1, \ldots, n_1, j = 0, 1, \ldots, n_2. \tag{27}$$

Like the distance distribution, if C is a linear code, the distribution $B_{i,j}$ based on W_U is equal to the *weight distribution $B'_{i,j}$ based on W_U* , that is

$$B_{i,j} = B'_{i,j} \left(= \left| \{\boldsymbol{y} \in C | \boldsymbol{y} \in W_{i,j}\} \right| \right), \\ i = 0, 1, \ldots, n_1, j = 0, 1, \ldots, n_2. \tag{28}$$

Definition 7 ($Q_{i,j}(z_1, z_2; n_1, n_2)$) *For any positive integers n_1, n_2, a polynomial $Q_{i,j}(z_1, z_2; n_1, n_2)$ $(= Q_{i,j}(z_1, z_2))$ is defined by*

$$Q_{i,j}(z_1, z_2; n_1, n_2) := P_i(z_1; n_1) P_j(z_2; n_2), \\ i = 0, 1, \ldots, n_1, j = 0, 1, \ldots, n_2. \tag{29}$$

where z_1, z_2 are indeterminate, and $P_i(z_1; n_1)$, $P_j(z_2; n_2)$ are the Krawtchouk polynomials. If there is no danger of confusion we omit the n_1, n_2.

The next Theorem 9, 10, and 11 correspond to Theorem 2, 3, and 4, respectively.

Theorem 9 *If $\boldsymbol{v} \in W_{k,l}$, then*

$$\sum_{\boldsymbol{u} \in W_{i,j}} (-1)^{\boldsymbol{u} \cdot \boldsymbol{v}} = Q_{i,j}(k, l). \tag{30}$$

where $i, k \in \{0, 1, \ldots, n_1\}$, $j, l \in \{0, 1, \ldots, n_2\}$.

Proof: See Section 5.1.

Theorem 10 *For any $a_1, b_1 \in \{0, 1, \ldots, n_1\}$, $a_2, b_2 \in \{0, 1, \ldots, n_2\}$,*

$$\sum_{c_1=0}^{n_1} \sum_{c_2=0}^{n_2} \left| W_{c_1,c_2} \right| \; Q_{a_1,a_2}(c_1, c_2) \; Q_{b_1,b_2}(c_1, c_2) \\ = 2^n \left| W_{a_1,a_2} \right| \; \delta_{a_1,b_1} \delta_{a_2,b_2}, \tag{31}$$

where δ_{a_1,b_1} and δ_{a_2,b_2} are the Kronecker symbols.

Proof: See Section 5.2.

Theorem 11 *For any $a_1, b_1 \in \{0, 1, \ldots, n_1\}$, $a_2, b_2 \in \{0, 1, \ldots, n_2\}$,*

$$\left| W_{b_1,b_2} \right| \; Q_{a_1,a_2}(b_1, b_2) = \left| W_{a_1,a_2} \right| \; Q_{b_1,b_2}(a_1, a_2). \tag{32}$$

Proof: See Section 5.3.

The next Theorem 12 corresponds to Theorem 5.

Theorem 12 *Let $C (\subseteq \{0,1\}^n)$ be a linear code, and $C^\perp$ be the dual code of C. Let $B_{i,j}$ and $B_{i,j}^\perp$, $i = 0, 1, \ldots, n_1$, $j = 0, 1, \ldots, n_2$, be the distribution based on W_U of C and $C^\perp$. Then,*

$$B_{i,j}^\perp = \frac{1}{|C|} \sum_{k=0}^{n_1} \sum_{l=0}^{n_2} B_{k,l} Q_{i,j}(k, l), \\ i = 0, 1, \ldots, n_1, j = 0, 1, \ldots, n_2. \tag{33}$$

Proof: See Section 5.4.

The next Theorem 13 corresponds to Theorem 6.

Theorem 13 *Let $C (\subseteq \{0,1\}^n)$ be a code, and $B_{i,j}$, $i = 0, 1, \ldots, n_1$, $j = 0, 1, \ldots, n_2$ be the distribution based on W_U of C. Then,*

$$\frac{1}{|C|} \sum_{k=0}^{n_1} \sum_{l=0}^{n_2} B_{k,l} Q_{i,j}(k, l) \geq 0, \\ i = 0, 1, \ldots, n_1, j = 0, 1, \ldots, n_2. \tag{34}$$

Proof: See Section 5.5.

4.2 LP Bounds for UEP Codes

In what follows, let

$$\Delta := \{(i,j) \in \{0,1,\ldots,n_1\} \times \{0,1,\ldots,n_2\}| \\ (i \neq 0, i+j \leq d_1 - 1) \text{ or } \\ (i+j \leq d_2 - 1)\}. \quad (35)$$

For any $(i,j) \in \Delta$, $W_{i,j} \in D$, if D satisfies Eq. (5).

Definition 8 ($M_{LP}(n_1,n_2;d_1,d_2)$) *$M_{LP}(n_1,n_2;d_1,d_2)$ is defined by the solution to the following linear programming problem: choose real numbers $B_{i,j}$, $i = 0,1,\ldots,n_1$, $j = 0,1,\ldots,n_2$, so as to*

$$\textit{maximize} \quad \sum_{i=0}^{n_1}\sum_{j=0}^{n_2} B_{i,j} \quad (36)$$

subject to the constraints

$$B_{0,0} = 1, \quad (37)$$

$$B_{i,j} = 0, \forall (i,j) \in \Delta, \quad (38)$$

$$B_{i,j} \geq 0, \\ \forall (i,j) \in \{0,1,\ldots,n_1\} \times \{0,1,\ldots,n_2\} \setminus \Delta, \quad (39)$$

$$\sum_{k=0}^{n_1}\sum_{l=0}^{n_2} B_{k,l} Q_{i,j}(k,l) \geq 0, \\ i = 0,1,\ldots,n_1, j = 0,1,\ldots,n_2. \quad (40)$$

The next Theorem 14 corresponds to Theorem 7.

Theorem 14 *Any $((n_1,n_2),M,(d_1,d_2))$ codes satisfy*

$$M \leq M_{LP}(n_1,n_2;d_1,d_2). \quad (41)$$

Proof: This is obvious from Theorem 13. □

The next Theorem 15 corresponds to Theorem 8.

Theorem 15 *Let D satisfy Eq. (5). And, we assume that E ($\subseteq \{0,1\}^n$) satisfies*

$$D = \{\boldsymbol{e}_1 \oplus \boldsymbol{e}_2 | \boldsymbol{e}_1, \boldsymbol{e}_2 \in E\}, \quad (42)$$

$$\bigcup_{(i,j)\in\Gamma} W_{i,j} = E, \\ \exists \Gamma \subseteq \{0,1,\ldots,n_1\} \times \{0,1,\ldots,n_2\}. \quad (43)$$

Then

$$M_{LP}(n_1,n_2;d_1,d_2) \leq \frac{2^n}{|E|}. \quad (44)$$

Proof: See Section 5.6.

In the last of this section, we briefly note Theorem 15. Theorem 15 corresponds to Theorem 8 in Section 3. But, different from Theorem 8, assumptions in Theorem 15, that is Eq. (42), (43), rarely hold completely. Thus, Theorem 15 is not a pure generalization of Theorem 8. This is because that $((n_1,n_2),M,(2t_1+1,2t_2+1))$ UEP codes are a sufficient condition to correct all errors in E defined by Eq. (6), while $(n,M,2t+1)$ codes are a necessary and sufficient condition to correct all errors in E, defined by

$$E = \{\boldsymbol{e} \in \{0,1\}^n | wt(\boldsymbol{e}) \leq t\}. \quad (45)$$

5 Proofs of Theorems

In this section, we prove the theorems in Section 4.

5.1 Proof of Theorem 9

Let $\boldsymbol{v} \in W_{k,l}$. Then we can write $v = (\boldsymbol{v}_1,\boldsymbol{v}_2) \in W_k^{(n_1)} \times W_l^{(n_2)}$. Therefore,

$$\begin{aligned} &\sum_{\boldsymbol{u}\in W_{i,j}} (-1)^{\boldsymbol{u}\cdot\boldsymbol{v}} \\ &= \sum_{(\boldsymbol{u}_1,\boldsymbol{u}_2)\in W_i^{(n_1)}\times W_j^{(n_2)}} (-1)^{(\boldsymbol{u}_1,\boldsymbol{u}_2)\cdot(\boldsymbol{v}_1,\boldsymbol{v}_2)} && (46)\\ &= \sum_{\boldsymbol{u}_1\in W_i^{(n_1)}} \sum_{\boldsymbol{u}_2\in W_j^{(n_2)}} (-1)^{(\boldsymbol{u}_1\cdot\boldsymbol{v}_1)\oplus(\boldsymbol{u}_2\cdot\boldsymbol{v}_2)} && (47)\\ &= \sum_{\boldsymbol{u}_1\in W_i^{(n_1)}} (-1)^{\boldsymbol{u}_1\cdot\boldsymbol{v}_1} \sum_{\boldsymbol{u}_2\in W_j^{(n_2)}} (-1)^{\boldsymbol{u}_2\cdot\boldsymbol{v}_2} && (48)\\ &= P_i(k;n_1)P_j(l;n_2) && (49)\\ &= Q_{i,j}(k,l). && (50) \end{aligned}$$

where Eq. (49) is from Theorem 2.

5.2 Proof of Theorem 10

For any $a_1, b_1 \in \{0,1,\ldots,n_1\}$, $a_2, b_2 \in \{0,1,\ldots,n_2\}$,

$$\begin{aligned} &\sum_{c_1=0}^{n_1}\sum_{c_2=0}^{n_2} |W_{c_1,c_2}|\, Q_{a_1,a_2}(c_1,c_2) Q_{b_1,b_2}(c_1,c_2) \\ &= \sum_{c_1=0}^{n_1}\sum_{c_2=0}^{n_2} \binom{n_1}{c_1}\binom{n_2}{c_2} \\ &\quad \times P_{a_1}(c_1;n_1)P_{a_2}(c_2;n_2)P_{b_1}(c_1;n_1)P_{b_2}(c_2;n_2) && (51)\\ &= 2^{n_1}\binom{n_1}{a_1}\delta_{a_1,b_1} \times 2^{n_2}\binom{n_2}{a_2}\delta_{a_2,b_2} && (52)\\ &= 2^n |W_{a_1,a_2}|\, \delta_{a_1,b_1}\delta_{a_2,b_2}, && (53) \end{aligned}$$

where Eq. (52) is from Theorem 3.

5.3 Proof of Theorem 11

For any $a_1, b_1 \in \{0,1,\ldots,n_1\}$, $a_2, b_2 \in \{0,1,\ldots,n_2\}$,

$$\begin{aligned} &|W_{b_1,b_2}|\, Q_{a_1,a_2}(b_1,b_2) \\ &= \binom{n_1}{b_1}\binom{n_2}{b_2} P_{a_1}(b_1;n_1)P_{a_2}(b_2;n_2) && (54)\\ &= \binom{n_1}{a_1}\binom{n_2}{a_2} P_{b_1}(a_1;n_1)P_{b_2}(a_2;n_2) && (55)\\ &= |W_{a_1,a_2}|\, Q_{b_1,b_2}(a_1,a_2), && (56) \end{aligned}$$

where Eq. (55) is from Theorem 4.

5.4 Proof of Theorem 12

Before the proof of Theorem 12, we show the next Lemma 1. In Lemma 1, let f be any mapping defined on $\{0,1\}^n$, and $\hat{f}$ be the Hadamard transform of f, that is

$$\hat{f}(\boldsymbol{u}) = \sum_{\boldsymbol{v}\in\{0,1\}^n} (-1)^{\boldsymbol{u}\cdot\boldsymbol{v}} f(\boldsymbol{v}), \boldsymbol{u} \in \{0,1\}^n. \quad (57)$$

Lemma 1 [6, Ch.5 Lemma 2] *Let C be a linear code, and $C^\perp$ be the dual code of C. Then*

$$\sum_{\boldsymbol{u}\in C^\perp} f(\boldsymbol{u}) = \frac{1}{|C|}\sum_{\boldsymbol{u}\in C}\hat{f}(\boldsymbol{u}). \tag{58}$$

Proof of Theorem 12: Let the mapping $f_{W_{i,j}}$ be

$$f_{W_{i,j}}(\boldsymbol{u}) = \begin{cases} 0, & \boldsymbol{u}\notin W_{i,j}, \\ 1, & \boldsymbol{u}\in W_{i,j}. \end{cases}$$
$$i = 0,1,\dots n_1, j = 0,1,\dots n_2, \tag{59}$$

If Eq. (59) is used as the mapping f in Eq. (58), the left-hand side of Eq. (58) is

$$\sum_{\boldsymbol{u}\in C^\perp} f_{W_{i,j}}(\boldsymbol{u}) = B^\perp_{i,j}, \tag{60}$$

because $C^\perp$ is a linear code.

And, the right-hand side of Eq. (58) is

$$\begin{aligned}
&\frac{1}{|C|}\sum_{\boldsymbol{u}\in C}\hat{f}_{W_{i,j}}(\boldsymbol{u}) \\
&= \frac{1}{|C|}\sum_{\boldsymbol{u}\in C}\sum_{\boldsymbol{v}\in\{0,1\}^n}(-1)^{\boldsymbol{u}\cdot\boldsymbol{v}} f(\boldsymbol{v}) && (61)\\
&= \frac{1}{|C|}\sum_{\boldsymbol{u}\in C}\sum_{\boldsymbol{v}\in W_{i,j}}(-1)^{\boldsymbol{u}\cdot\boldsymbol{v}} && (62)\\
&= \frac{1}{|C|}\sum_{k=0}^{n_1}\sum_{l=0}^{n_2}\sum_{\boldsymbol{u}\in C\cap W_{k,l}}\sum_{\boldsymbol{v}\in W_{i,j}}(-1)^{\boldsymbol{u}\cdot\boldsymbol{v}} && (63)\\
&= \frac{1}{|C|}\sum_{k=0}^{n_1}\sum_{l=0}^{n_2} B_{k,l}Q_{i,j}(k,l), && (64)
\end{aligned}$$

where Eq. (64) is from Theorem 9. Thus we can get Eq. (33). □

5.5 Proof of Theorem 13

For $i = 0,1,\dots,n_1, j = 0,1,\dots,n_2$,

$$\begin{aligned}
&\frac{1}{|C|}\sum_{k=0}^{n_1}\sum_{l=0}^{n_2} B_{k,l}Q_{i,j}(k,l) \\
&= \frac{1}{|C|^2}\sum_{k=0}^{n_1}\sum_{l=0}^{n_2}\sum_{\substack{(\boldsymbol{x},\boldsymbol{y})\in C^2,\\ \boldsymbol{x}\oplus\boldsymbol{y}\in W_{k,l}}} Q_{i,j}(k,l) && (65)\\
&= \frac{1}{|C|^2}\sum_{k=0}^{n_1}\sum_{l=0}^{n_2}\sum_{\substack{(\boldsymbol{x},\boldsymbol{y})\in C^2,\\ \boldsymbol{x}\oplus\boldsymbol{y}\in W_{k,l}}}\sum_{\boldsymbol{u}\in W_{i,j}}(-1)^{\boldsymbol{u}\cdot(\boldsymbol{x}\oplus\boldsymbol{y})} && (66)\\
&= \frac{1}{|C|^2}\sum_{\boldsymbol{x}\in C}\sum_{\boldsymbol{y}\in C}\sum_{\boldsymbol{u}\in W_{i,j}}(-1)^{\boldsymbol{u}\cdot\boldsymbol{x}}(-1)^{\boldsymbol{u}\cdot\boldsymbol{y}} && (67)\\
&= \sum_{\boldsymbol{u}\in W_{i,j}}\left(\frac{1}{|C|}\sum_{\boldsymbol{x}\in C}(-1)^{\boldsymbol{u}\cdot\boldsymbol{x}}\right)^2 && (68)\\
&\geq 0, && (69)
\end{aligned}$$

where Eq. (66) is from Theorem 9.

5.6 Proof of Theorem 15

Before the proof of Theorem 15, we show some lemmas and definitions.

Lemma 2 *If $i+j<k$, then*

$$\sum_{l=0}^{n}\binom{n}{l}P_i(l)P_j(l)P_k(l) = 0. \tag{70}$$

Proof: The left-hand side of Eq. (70) is the coefficient of $x^iy^jz^k$ in

$$\begin{aligned}
&\sum_{l=0}^{n}\binom{n}{l}(1+x)^{n-l}(1-x)^l \\
&\qquad (1+y)^{n-l}(1-y)^l(1+z)^{n-l}(1-z)^l && (71)\\
&= \sum_{l=0}^{n}\binom{n}{l}\{(1+x)(1+y)(1+z)\}^{n-l} \\
&\qquad \{(1-x)(1-y)(1-z)\}^l && (72)\\
&= \{(1+x)(1+y)(1+z) + \\
&\qquad (1-x)(1-y)(1-z)\}^n && (73)\\
&= 2^n(1+xy+yz+za)^n, && (74)
\end{aligned}$$

where Eq. (73) is from binomial theorem. If $i+j<k$, the coefficient of $x^iy^jz^k$ in Eq. (74) is 0. Thus we get Eq. (70). □

Next, we show the dual problem to the linear programming problem defined in Definition 8.

Problem 1 *Choose real numbers $\beta_{i,j}$, $i=0,1,\dots,n_1$, $j=0,1,\dots,n_2$, so as to*

$$\textit{minimize} \quad \sum_{i=0}^{n_1}\sum_{j=0}^{n_2}\binom{n_1}{i}\binom{n_2}{j}\beta_{i,j} \tag{75}$$

subject to the constraints

$$\begin{aligned}
&\beta_{0,0} = 1, && (76)\\
&\beta_{i,j}\geq 0, i=0,1,\dots,n_1, j=0,1,\dots,n_2, && (77)\\
&\sum_{i=0}^{n_1}\sum_{j=0}^{n_2}\beta_{i,j}Q_{i,j}(k,l)\leq 0, \\
&\qquad \forall(k,l)\in\{0,1,\dots,n_1\}\times\{0,1,\dots,n_2\}\setminus\Delta. && (78)
\end{aligned}$$

From the duality theorem of linear programming [6, Ch.17 Theorem 15, 16], it follows that any feasible solution to the dual problem gives an upper bound on the optimal solution to the primal problem.

Proof of Theorem 15: In Problem 1, let

$$\beta_{i,j} = \left\{\frac{\sum_{(p,q)\in\Gamma}Q_{p,q}(i,j)}{|E|}\right\}^2. \tag{79}$$

Then

$$\begin{aligned}
&\beta_{0,0} = 1, && (80)\\
&\beta_{i,j}\geq 0, i=0,1,\dots,n_1, j=0,1,\dots,n_2. && (81)
\end{aligned}$$

And, for any $(k,l) \in \{0,1,\ldots,n_1\} \times \{0,1,\ldots,n_2\} \setminus \Delta$,

$$\begin{aligned}
&\sum_{i=0}^{n_1}\sum_{j=0}^{n_2}\beta_{i,j}Q_{i,j}(k,l) \\
&= \sum_{i=0}^{n_1}\sum_{j=0}^{n_2}\left\{\frac{\sum_{(p,q)\in\Gamma}Q_{p,q}(i,j)}{|E|}\right\}^2 Q_{i,j}(k,l) \qquad (82)\\
&= \frac{1}{|E|^2}\sum_{i=0}^{n_1}\sum_{j=0}^{n_2}\sum_{(p,q)\in\Gamma}\sum_{(r,s)\in\Gamma} \\
&\quad \times Q_{p,q}(i,j)Q_{r,s}(i,j)Q_{i,j}(k,l) \qquad (83)\\
&= \frac{1}{|E|^2\cdot|W_{k,l}|}\sum_{(p,q)\in\Gamma}\sum_{(r,s)\in\Gamma}\sum_{i=0}^{n_1}\sum_{j=0}^{n_2}|W_{i,j}| \\
&\quad \times Q_{p,q}(i,j)Q_{r,s}(i,j)Q_{k,l}(i,j) \qquad (84)\\
&= \frac{1}{|E|^2\cdot|W_{k,l}|}\sum_{(p,q)\in\Gamma}\sum_{(r,s)\in\Gamma}\sum_{i=0}^{n_1}\sum_{j=0}^{n_2}|W_{i,j}| \\
&\quad \times P_p(i;n_1)P_q(j;n_2)P_r(i;n_1)P_s(j;n_2) \\
&\quad \times P_k(i;n_1)P_l(j;n_2) \qquad (85)\\
&= \frac{1}{|E|^2\cdot|W_{k,l}|}\sum_{(p,q)\in\Gamma}\sum_{(r,s)\in\Gamma} \\
&\quad \times \left\{\sum_{i=0}^{n_1}|W_i^{(n_1)}|P_p(i;n_1)P_r(i;n_1)P_k(i;n_1)\right\} \\
&\quad \times \left\{\sum_{j=0}^{n_2}|W_j^{(n_2)}|P_q(j;n_2)P_s(j;n_2)P_l(j;n_2)\right\} \qquad (86)\\
&= 0. \qquad (87)
\end{aligned}$$

where Eq. (84) is from Theorem 11, and Eq. (87) is from Lemma 2.

Thus, the following is a feasible solution to Problem 1.

$$\begin{aligned}
&\sum_{i=0}^{n_1}\sum_{j=0}^{n_2}\binom{n_1}{i}\binom{n_2}{j}\left\{\frac{\sum_{(p,q)\in\Gamma}Q_{p,q}(i,j)}{|E|}\right\}^2 \\
&= \frac{1}{|E|^2}\sum_{i=0}^{n_1}\sum_{j=0}^{n_2}\binom{n_1}{i}\binom{n_2}{j} \\
&\qquad \sum_{(p,q)\in\Gamma}\sum_{(r,s)\in\Gamma}Q_{p,q}(i,j)Q_{r,s}(i,j) \qquad (88)\\
&= \frac{1}{|E|^2}\sum_{(p,q)\in\Gamma}\sum_{(r,s)\in\Gamma}2^n\binom{n_1}{p}\binom{n_2}{q}\delta_{p,r}\delta_{q,s} \qquad (89)\\
&= \frac{2^n}{|E|^2}\sum_{(p,q)\in\Gamma}|W_{p,q}| \qquad (90)\\
&= \frac{2^n}{|E|}, \qquad (91)
\end{aligned}$$

where Eq. (89) is from Theorem 10. We can get Eq. (44), because any feasible solution to the dual problem is upper bound on the optimal solution to the primal problem. □

6 Conclusion

In this paper, we proposed the LP bound for UEP codes. Firstly, we generalized the distance distribution, to the distribution based on W_U. Under the generalization, we led to some theorems and the LP bound for UEP codes. Lastly, we compared the proposed bound with the modified Hamming bound.

In future work, we will actually calculate bounds for UEP codes in some parameters by solving the LP problems. And, we will compare these bounds with codes found by certain methods.

Acknowledgment

The authors would like to thank all members of Matsushima Lab. in Waseda Univ. for their helpful suggestions to this work. This research was partially supported by Grant-in-Aid for Scientific Research on Innovative Areas of Japan Society for the Promotion of Science (No:20200044), Waseda University Grant for Special Research Project No:2009A-058.

References

[1] P.Delsarte, "An algebraic approach to the association schemes of coding theory, " *Philips Res. Repts. Suppl.* , No.10, 1973.

[2] L. A. Dunning and W. E. Robbins, "Optimal encodings of linear block codes for unequal error protection, " *Inform. Contr.* , vol. 37, pp.150-177, 1978.

[3] W. J. van Gils, "Two topics on linear unequal error protection codes: bounds on their length and cyclic code classes," *IEEE Trans. Inform. Theory,* vol. IT-29, pp. 866-876, Sept. 1983.

[4] A. S. Hedayat, N. J. A. Sloane and J. Stufken, *Orthogonal Arrays: Theory and Applications*, Springer, New York, 1999.

[5] S. Hirasawa and T. Nishijima, *Introduction to coding theory* (in Japanese), Baifukan, 1999.

[6] F. J. MacWilliams and N. J. A. Sloane, *The theory of Error-Correcting Codes*, Amsterdam: North-Holland Publishing Co., 1977.

[7] B. Masnick and J. Wolf, "On linear unequal error protection codes," *IEEE Trans. Inform. Theory,* vol. IT-3, pp. 600-607, Oct. 1967.

[8] T. Saito, T. Matsushima and S. Hirasawa, "A Note on Construction of Orthogonal Arrays with Unequal Strength from Error-Correcting Codes," *IEICE Trans. Fundamentals*, Vol.E89-A, pp.1307-1315, May 2006.

[9] Y. Ukita, T. Matsushima and S. Hirasawa, "A Note on Learning Boolean Functions Using Orthogonal Designs" (in Japanese), *IEICE Trans. Fundamentals*, Vol.J86-A, no.4, pp.482-490, Apr. 2003.