SHONAN INSTITUTE OF
TECHNOLOGY JOURNAL
Vol. 53, No. 1, 2019

多レベル不均一誤り訂正符号の線形計画限界

齋藤 友彦*

Linear programming bounds for multi-level unequal protection codes

Tomohiko SAITO

Abstract: In coding theory, it is important to find upper bounds for the code size given a code length and minimum distance. The Hamming bounds and Linear Programming (LP) bounds were proposed in previous works. On the other hand, Masnick et al. proposed Unequal Error Protection (UEP) codes and modified Hamming bounds as upper bounds for the code size of UEP codes. In our previous work, we defined 2-level UEP codes as a subclass of UEP codes, and derived LP bounds for 2-level UEP codes. In this paper, we define multi-level UEP codes by extending 2-level UEP codes, and derive LP bounds for multi-level UEP codes. Moreover, we show that LP bounds for UEP codes are tighter upper bound than modified Hamming bounds.

KEYWORDS: Unequal Error Protection Code, Linear Programming Bound, Inner Distribution

要旨 符号長 n と最小距離 d の誤り訂正符号に対し，符号語数の上界として，ハミング限界や線形計画 (Linear Programming: LP) 限界が知られている．一方，Masnick らによって不均一誤り訂正 (Unequal Error Protection: UEP) 符号が提案された．UEP 符号においても，符号語数の上界として，ハミング限界を拡張した修正ハミング限界が示されている．従来，著者らは UEP 符号のサブクラスとして 2-レベル UEP 符号を定義し，その LP 限界を示した．本論文では，2-レベル UEP 符号を拡張した，多レベル UEP 符号を定義し，その LP 限界を導出する．更に，多レベル UEP 符号の LP 限界が修正ハミング限界よりも優れていることを示す．

キーワード： 不均一誤り訂正符号，線形計画限界，内部分布

1 はじめに

符号長 n と最小距離 d の誤り訂正符号に対し，符号語数の上界として，ハミング限界 [1] や線形計画 (Linear Programming: LP) 限界 [2] が知られている．

一方，Masnick らによって不均一誤り訂正 (Unequal Error Protection: UEP) 符号が提案された [3]．この符号は符号語シンボルごとに訂正能力が異なるものである[2]．UEP 符号の応用として，例えば数値データの送信が挙げられる [3]．正負や上位桁に対応するシンボルの誤りは下位桁のそれよりも深刻である場合が多く，より高い訂正能力が求められる．なお，UEP 符号においても，符号語数の上界として，ハミング限界を拡張した修正ハミング限界が示されている [3]．

従来研究において，著者らは UEP 符号のサブクラスである，2-レベル UEP を定義し，その LP 限界を提案した [9]．本論文では，まず 2-レベル UEP 符号を拡張した多レベル UEP 符号を定義する．そして，多レベル UEP 符号の LP 限界を導出する．更に，提案した LP 限界と Masnick らによって提案された修正ハミング限界 [3] との比較を行う．

*湘南工科大学 工学部 情報工学科 講師

[2]UEP 符号には符号化する前のメッセージのシンボルごとに訂正能力を変えた符号がある [6, 7]．本研究では，符号語のシンボルごとに訂正能力が異なる UEP 符号を扱うことに注意されたい [8, 3]．なお，後者は組織符号化することで，メッセージシンボルごとに訂正能力を変えた UEP 符号として利用することができる [8]．

2　準備

$\mathbb{F}_2 = \{0,1\}$ を 2 元有限体とする．$\mathbb{F}_2$ 上長さ n (n は正整数) の全てのベクトルから成る集合を $\mathbb{F}_2^n$ とする．$\boldsymbol{x}$ がベクトルであるとき，x_i を $\boldsymbol{x}$ の i 番目の要素とする．任意の $\boldsymbol{x}$, $\boldsymbol{y} \in \mathbb{F}_2^n$ に対して，$\boldsymbol{x}+\boldsymbol{y} = (x_1+y_1, x_2+y_2, \ldots, x_n+y_n)$ とし，$w_h(\boldsymbol{x})$ を $\boldsymbol{x}$ のハミング重み，$d_h(\boldsymbol{x},\boldsymbol{y})$ を $\boldsymbol{x}$ と $\boldsymbol{y}$ のハミング距離とする．また，有限集合 A に対し，$|A|$ を A のサイズ (要素数) とする．

$\mathbb{F}_2^n$ の部分集合 $C(|C| = M)$ を符号長 n，符号語数 M の 2 元符号，もしくは 2 元 (n, M) 符号と呼ぶ．本論文では 2 元符号を扱うため，以下では 2 元 (n, M) 符号を単に (n, M) 符号と呼ぶ．また，符号 C に含まれる長さ n の系列 $\boldsymbol{x} \in C$ を符号語と呼ぶ．このとき，x_i は $\boldsymbol{x}$ の i 番目の符号語シンボルであり，i を符号語シンボルのインデックスと呼ぶ．また，(n, M) 符号 C の最小距離 d を

$$d = \min\{d_h(\boldsymbol{x},\boldsymbol{y}) | \boldsymbol{x},\boldsymbol{y} \in C, \boldsymbol{x} \neq \boldsymbol{y}\} \tag{1}$$

と定義する．このとき，最小距離 d の (n, M) 符号を (n, M, d) 符号と呼ぶ [1, p.38].

任意の実数 x に対し，

$$\binom{x}{m} = \begin{cases} \frac{x(x-1)\ldots(x-m+1)}{m!} & (m \text{ が正整数}) \\ 1 & (m=0) \\ 0 & (\text{上記以外}) \end{cases} \tag{2}$$

とする [1, p.13]. 但し，$m! = 1{\cdot}2{\cdot}3{\cdot}\ldots(m-1)m$, $0! = 1$ とする．また，任意の正整数 N に関して，Krawtchouk 多項式 $P_k(x; N)$ を

$$P_k(x;N) = \sum_{j=0}^{k} (-1)^j \binom{x}{j}\binom{N-x}{k-j}, \quad k = 0, 1, 2, \ldots \tag{3}$$

と定義する [1, p.130]. すると，$P_k(x; N)$ は変数 x，次数 k の多項式である．また，i, N が $0 \leq i \leq N$ を満たす整数のとき，以下に示す z の多項式が 2 項定理より成り立つ [1, Ch.5 式 (16)].

$$(1+z)^{N-i}(1-z)^i = \sum_{k=0}^{N} P_k(i;N) z^k. \tag{4}$$

3　μ-レベル不均一誤り訂正符号

3.1　μ-レベル不均一誤り訂正符号

3.1 節では，文献 [3] に従い，セパレーション及び UEP 符号を定義する．更に本研究で対象とする μ-レベル UEP 符号を定義する．

本論文全体を通じ，n, n_1, n_2, $\cdots$, n_μ, d, d_1, d_2, $\cdots$, d_μ を以下を満たす正整数とする．

$$n = n_1 + n_2 + \cdots + n_\mu, \tag{5}$$

$$d_1 > d_2 > \cdots > d_\mu = d. \tag{6}$$

セパレーション及び UEP 符号を次のように定義する．

Definition 1. (n, M) 符号 C に対して，C のセパレーション $\boldsymbol{s} = (s_1, s_2, \ldots, s_n)$ を次のように定義する．

$$s_\ell = \min\{d_h(\boldsymbol{x},\boldsymbol{y}) | \boldsymbol{x},\boldsymbol{y} \in C, x_\ell \neq y_\ell\}, \quad \ell = 1, 2, \ldots, n. \tag{7}$$

このとき，$s_\ell \neq s_{\ell'}$ を満たす ℓ, ℓ' が存在するならば，C を *UEP* 符号と呼ぶ[3]. □

式 (7) の s_ℓ は，任意の符号語 $\boldsymbol{x} = (x_1, x_2, \ldots, x_n)$ の位置 ℓ，すなわち x_ℓ の誤り訂正能力を表す評価尺度である．(n, M) 符号 C の最小距離 d とセパレーション $\boldsymbol{s}$ は $d = \min\{s_\ell | \ell = 1, 2, \ldots, n\}$ の関係を満たす．

UEP 符号のサブクラスとして，次の μ-レベル UEP 符号を定義する．

Definition 2. C を次のセパレーション $\boldsymbol{s}$ を持つ $(n, M,$

[3] 文献 [3] を初め，UEP 符号に関する多くの文献では，線形 UEP(Linear UEP: LUEP) 符号を対象にしている．しかし，本論文では非線形符号も対象とするため，式 (7) をセパレーションの定義として用いる．また，LUEP 符号は大きく二つに分類され，一つは符号語シンボルごと [8, 3]，もう一つはメッセージシンボルごと [6, 7] に訂正能力が異なる符号である．本研究では前者と対応している．後者では，(n, M) 線形符号 $\mathcal{C}$(生成行列を G とする) のセパレーション $\boldsymbol{s}$ の定義として，

$s_\ell = \min\{w_h(\boldsymbol{m}G) | \boldsymbol{m} \in \mathbb{F}_2^k, m_\ell \neq 0\}, \ell = 1, 2, \ldots, k$

が用いられる．但し，$k = \log_2 M$ である．

d) 符号とする．

$$s_i \geq \begin{cases} d_1 \ (1 \leq i \leq n_1), \\ d_2 \ (n_1+1 \leq i \leq n_1+n_2), \\ \vdots \\ d_\mu \ (\sum_{k=1}^{\mu-1} n_k + 1 \leq i \leq \sum_{k=1}^{\mu} n_k), \end{cases} \tag{8}$$

このとき，C を $((n_1,\cdots,n_\mu),M,(d_1,\cdots,d_\mu))$ *UEP* 符号，もしくは μ-レベル *UEP* 符号と呼ぶ． □

以下では，対象を μ-レベル UEP 符号に限定し，その LP 限界を導出する．

3.2 内部分布

3.2 節では，文献 [10] に従い，内部分布を定義する．更に，μ-レベル UEP 符号の内部分布の性質についても述べる．

C を (n,M) 符号とする．このとき，$(n_1,n_2,\cdots,n_\mu)$ 分割 $\mathcal{T}$ を

$$\mathcal{T} = \{T_1, T_2, \cdots, T_\mu\}, \tag{9}$$

$$T_1 = \{1, 2, \ldots, n_1\}, \tag{10}$$

$$T_2 = \{n_1+1, n_1+2 \ldots, n_2\}, \tag{11}$$

$$\vdots \tag{12}$$

$$T_\mu = \left\{ \sum_{i=1}^{\mu-1} n_i + 1, \cdots \sum_{i=1}^{\mu} n_i \right\}. \tag{13}$$

と定義する．$T_1, T_2, \cdots, T_\mu$ は μ 個に分割した符号語シンボルのインデックスの集合である．

$\boldsymbol{x} \in \mathbb{F}_2^n$ に対して $\mathrm{supp}(\boldsymbol{x}) = \{i | x_i \neq 0\}$ とする．このとき，

$$w_{\mathcal{T}}(\boldsymbol{x}) = \Big(|\mathrm{supp}(\boldsymbol{x}) \cap T_1|, |\mathrm{supp}(\boldsymbol{x}) \cap T_2|, \cdots, |\mathrm{supp}(\boldsymbol{x}) \cap T_\mu| \Big) \in \mathbb{N}^\mu \tag{14}$$

を $\boldsymbol{x}$ の $\mathcal{T}$ 重み ($\mathcal{T}$-weight) と呼ぶ．但し，$\mathbb{N}$ は非負整数の集合である．ハミング重み $w_h(\boldsymbol{x})$ と $\mathcal{T}$ 重み $w_{\mathcal{T}}(\boldsymbol{x}) = (w_{\mathcal{T}}(\boldsymbol{x})_1, w_{\mathcal{T}}(\boldsymbol{x})_2, \cdots, w_{\mathcal{T}}(\boldsymbol{x})_\mu)$ は $w_h(\boldsymbol{x}) = w_{\mathcal{T}}(\boldsymbol{x})_1 + w_{\mathcal{T}}(\boldsymbol{x})_2 + \cdots + w_{\mathcal{T}}(\boldsymbol{x})_\mu$ を満たす．また，

$$W(\mathcal{T}) = \Big\{ \boldsymbol{i} = (i_1, i_2, \cdots, i_\mu) \ \Big| \ i_1 \leq |T_1| = n_1, i_2 \leq |T_2| = n_2, \cdots, i_\mu \leq |T_\mu| = n_\mu \Big\} \tag{15}$$

を $\mathcal{T}$ の重み集合 (weight set) と呼ぶ．このとき，(n,M) 符号の分割 $\mathcal{T}$ における内部分布を次のように定義する [10, p.90]．

Definition 3. $\boldsymbol{i} \in W(\mathcal{T})$ に関して，

$$A_{\boldsymbol{i}} = \frac{1}{M} \Big| \Big\{ (\boldsymbol{x}, \boldsymbol{y}) \in C \times C \Big| w_{\mathcal{T}}(\boldsymbol{y} - \boldsymbol{x}) = \boldsymbol{i} \Big\} \Big| \tag{16}$$

を C の分割 $\mathcal{T}$ における内部分布と呼ぶ． □

次に，3.1 節で述べた $((n_1,\cdots,n_\mu),M,(d_1,\cdots,d_\mu))$ UEP の内部分布の性質をまとめる．

Lemma 1. C を $((n_1,\cdots,n_\mu),M,(d_1,\cdots,d_\mu))$ *UEP* 符号，$\mathcal{T}$ を $(n_1,n_2,\cdots,n_\mu)$ 分割とする．$A_{\boldsymbol{i}}, \boldsymbol{i} \in W(\mathcal{T})$ が C の $\mathcal{T}$ における内部分布であるならば，

$$M = \sum_{\boldsymbol{i} \in W(\mathcal{T})} A_{\boldsymbol{i}}, \tag{17}$$

$$A_{(0,0,\cdots,0)} = 1, \tag{18}$$

$$A_{\boldsymbol{i}} = 0, \boldsymbol{i} \in \mathcal{D} \setminus \{(0,0,\cdots,0)\}, \tag{19}$$

$$A_{\boldsymbol{i}} \geq 0, \boldsymbol{i} \notin \mathcal{D}, \tag{20}$$

が成り立つ．但し，

$$\begin{aligned} \mathcal{D} = & \left\{ \boldsymbol{i} \in W(\mathcal{T}) \Big| i_1 \neq 0, \sum_{j=1}^{\mu} i_j \leq d_1 - 1 \right\} \\ & \cup \left\{ \boldsymbol{i} \in W(\mathcal{T}) \Big| i_2 \neq 0, \sum_{j=1}^{\mu} i_j \leq d_2 - 1 \right\} \\ & \vdots \\ & \cup \left\{ \boldsymbol{i} \in W(\mathcal{T}) \Big| \sum_{j=1}^{\mu} i_j \leq d_\mu - 1 \right\} \end{aligned} \tag{21}$$

とする．

Proof:

式 (17), (18), (20) は内部分布の定義より明らかである．式 (19) は次の通りである．$((n_1,\cdots,n_\mu),M,(d_1,\cdots,d_\mu))$ UEP 符号の定義から，$\boldsymbol{x},\boldsymbol{y} \in C, w_{\mathcal{T}}(\boldsymbol{x}-\boldsymbol{y})_j \neq 0, 1 \leq j \leq \mu$ ならば，$d_h(\boldsymbol{x},\boldsymbol{y}) \geq d_j$ が成り立つ．但し，$w_{\mathcal{T}}(\boldsymbol{e}) = (w_{\mathcal{T}}(\boldsymbol{e})_1, w_{\mathcal{T}}(\boldsymbol{e})_2, \cdots, w_{\mathcal{T}}(\boldsymbol{e})_\mu)$ としている．以上から，式 (19) が成り立つ． □

更に，文献 [10, Proposition 5] から次の補題が容易に得られる．

Lemma 2. C を $((n_1,\cdots,n_\mu),M,(d_1,\cdots,d_\mu))$ *UEP* 符号，$\mathcal{T}$ を $(n_1,n_2,\cdots,n_\mu)$ 分割とする．$A_{\boldsymbol{i}}, \boldsymbol{i}\in W(\mathcal{T})$ が C の $\mathcal{T}$ における内部分布であるならば，任意の $\boldsymbol{i}\in W(\mathcal{T})$ について

$$\sum_{\boldsymbol{j}\in W(\mathcal{T})} A_{\boldsymbol{j}} \prod_{\ell=1}^{\mu} P_{i_\ell}(j_\ell;n_\ell)\geq 0 \tag{22}$$

が成り立つ．

Proof: 証明は A1. を参照． □

ここで，$((n_1,\cdots,n_\mu),M,(d_1,\cdots,d_\mu))$UEP 符号が存在するためには，補題 1 及び補題 2 を満たすことが必要条件となることに注意されたい．4 ではこれらの必要条件を用いて，μ-レベル UEP 符号における LP 限界の定式化を行う．

3.3 μ-レベル不均一誤り訂正符号の限界式

μ-レベル UEP 符号において正整数 $n_1,n_2\cdots,n_\mu$, $d_1,d_2\cdots,d_\mu$ が与えられた下で，符号語数 M の上界を求めることは重要である．UEP 符号の上界として，ハミング限界を拡張した修正ハミング限界が知られている [3]．修正ハミング限界を，μ-レベル UEP 符号に限定したとき，次のように書ける．

Lemma 3. $((n_1,\cdots,n_\mu),M,(d_1,\cdots,d_\mu))$ *UEP* 符号が存在するとき，

$$M\leq M_{HB}(n_1,\cdots,n_\mu;d_1,\cdots,d_\mu) \tag{23}$$

$$M_{HB}(n_1,\cdots,n_\mu;d_1,\cdots,d_\mu)=\frac{2^n}{|E|} \tag{24}$$

$$\begin{aligned} E=\Bigg\{\boldsymbol{e}\in\mathbb{F}_2^n \Big| &\sum_{i=1}^{\mu} w_{\mathcal{T}}(\boldsymbol{e})_i \leq \lfloor\frac{d_1-1}{2}\rfloor,\\ &\sum_{i=2}^{\mu} w_{\mathcal{T}}(\boldsymbol{e})_i \leq \lfloor\frac{d_2-1}{2}\rfloor\\ &\qquad\vdots\\ &w_h(\boldsymbol{e})_\mu \leq \lfloor\frac{d_\mu-1}{2}\rfloor\Bigg\} \end{aligned} \tag{25}$$

が成り立つ．但し $w_{\mathcal{T}}(\boldsymbol{e})=(w_{\mathcal{T}}(\boldsymbol{e})_1,w_{\mathcal{T}}(\boldsymbol{e})_2,\cdots,w_{\mathcal{T}}(\boldsymbol{e})_\mu)$ とする．

Proof: 証明は A2. を参照． □

4 μ-レベル不均一誤り訂正符号の線形計画限界

4 節では，μ-レベル UEP 符号の LP 限界 (UEP-LPB) を導出する．まず，次の LP 問題とその最適値 $M_{LP}(n_1,n_2,\cdots,n_\mu;d_1,d_2,\cdots,d_\mu)$ を定義する．

Definition 4. $\mathcal{D}$ は式 *(21)* であるとする．*Let* $\mathcal{D}$ *be defined by Eq. (21).* このとき，$M_{LP}(n_1,n_2,\cdots,n_\mu;d_1,d_2,\cdots,d_\mu)$ を次の *LP* 問題の最適値 *(*$\sum_{\boldsymbol{i}\in W(\mathcal{T})} A_{\boldsymbol{i}}$ の最大値*)* とする．

最大化：

$$\sum_{\boldsymbol{i}\in W(\mathcal{T})} A_{\boldsymbol{i}} \tag{26}$$

制約条件：

$$A_{(0,0,\cdots 0)}=1, \tag{27}$$

$$A_{\boldsymbol{i}}=0, \boldsymbol{i}\in\mathcal{D}\setminus\{(0,0,\cdots 0)\} \tag{28}$$

$$A_{\boldsymbol{i}}\geq 0, \boldsymbol{i}\notin\mathcal{D}, \tag{29}$$

$$\sum_{\boldsymbol{j}\in W(\mathcal{T})} A_{\boldsymbol{j}} \prod_{\ell=1}^{\mu} P_{i_\ell}(j_\ell;n_\ell)\geq 0, \boldsymbol{i}\in W(\mathcal{T}). \tag{30}$$

□

式 (26)-(30) は，式 (17)-(20) 及び，式 (22) と対応している．このとき，次の UEP-LPB が得られる．

Theorem 1. $((n_1,\cdots,n_\mu),M,(d_1,\cdots,d_\mu))$ *UEP* 符号が存在するとき，

$$M\leq M_{LP}(n_1,\cdots,n_\mu;d_1,\cdots,d_\mu) \tag{31}$$

が成り立つ． □

また，UEP-LPB と修正ハミング限界の間には次の関係が成り立つ．

Theorem 2. $((n_1,\cdots,n_\mu),M,(d_1,\cdots,d_\mu))$ *UEP* 符号が存在するとき，

$$\begin{aligned} M&\leq M_{LP}(n_1,\cdots,n_\mu;d_1,\cdots,d_\mu)\\ &\leq M_{HB}(n_1,\cdots,n_\mu;d_1,\cdots,d_\mu) \end{aligned} \tag{32}$$

が成り立つ． □

Theorem 2 より，UEP-LPB は修正ハミング限界よりも強い上界であることを示している．以下では，Theorem 2 を証明する．その準備として次の三つの補題を述べる．

Lemma 4. *[1, Ch.5 Theorem 16]* 任意の $a, b \in \{0, 1, \ldots, N\}$ について，

$$\sum_{c=0}^{N} \binom{N}{c} P_a(c;N) P_b(c;N) = 2^N \binom{N}{a} \delta_{a,b} \tag{33}$$

が成り立つ．但し，$\delta_{a,b}$ をクロネッカーのデルタ記号とする．すなわち，$a = b$ のとき $\delta_{a,b} = 1$，$a \neq b$ のとき $\delta_{a,b} = 0$ となる． □

Lemma 5. *[1, Ch.5 Theorem 17]* 任意の $a, b \in \{0, 1, \ldots, N\}$ について，

$$\binom{N}{a} P_b(a;N) = \binom{N}{b} P_a(b;N) \tag{34}$$

が成り立つ． □

Lemma 6. $h + i < j$ を満たす任意の $h, i, j \in \{0, 1, \ldots, N\}$ について，次式が成り立つ．

$$\sum_{l=0}^{N} \binom{N}{l} P_h(l;N) P_i(l;N) P_j(l;N) = 0. \tag{35}$$

Proof: 式 (4) から，式 (35) の左辺は次式の $x^h y^i z^j$ の係数と一致する．

$$\sum_{l=0}^{N} \binom{N}{l} (1+x)^{N-l}(1-x)^l (1+y)^{N-l}(1-y)^l \times (1+z)^{N-l}(1-z)^l \tag{36}$$

$$= \Big\{(1+x)(1+y)(1+z) + (1-x)(1-y)(1-z)\Big\}^N \tag{37}$$

$$= 2^N (1 + xy + yz + zx)^N. \tag{38}$$

但し，式 (37) は 2 項定理から得られる．ここで，$h+i < j$ であるとき，式 (38) における $x^h y^i z^j$ の係数は 0 となる．従って，式 (35) が得られる． □

Proof of Theorem 2 : まず，Definition 4 で示した LP 問題の双対問題を示す．

最小化：

$$\sum_{\boldsymbol{i} \in W(\mathcal{T})} \binom{n_1}{i_1} \binom{n_2}{i_2} \cdots \binom{n_\mu}{i_\mu} \alpha_{\boldsymbol{i}} \tag{39}$$

制約条件：

$$\alpha_{(0,0)} = 1, \tag{40}$$

$$\alpha_{\boldsymbol{i}} \geq 0, \boldsymbol{i} \in W(\mathcal{T}), \tag{41}$$

$$\sum_{\boldsymbol{i} \in W(\mathcal{T})} \prod_{\ell=1}^{\mu} P_{i_\ell}(j_\ell; n_\ell) \alpha_{\boldsymbol{i}} \leq 0, \quad \forall \boldsymbol{j} \in W(\mathcal{T}) \setminus \mathcal{D}. \tag{42}$$

LP 問題の双対定理 [1, Ch.17 Theorem 15, 16] より，双対問題の実行可能解の目的関数値 (式 (39) の値) は Definition 4 で示した主問題の最適解 $M_{LP}(n_1, n_2, \cdots, n_\mu; d_1, d_2, \cdots, d_\mu)$ の上界になる．ここで，

$$\alpha_{\boldsymbol{i}} = \left\{ \frac{\sum_{\boldsymbol{a} \in \mathcal{E}} \prod_{\ell=1}^{\mu} P_{a_\ell}(i_\ell; n_\ell)}{|E|} \right\}^2 \tag{43}$$

と置く．但し，

$$\mathcal{E} := \Big\{ \boldsymbol{i} \in W(\mathcal{T}) \Big| \sum_{j=1}^{\mu} i_j \leq \lfloor \frac{d_1 - 1}{2} \rfloor, \sum_{j=2}^{\mu} i_j \leq \lfloor \frac{d_2 - 1}{2} \rfloor \vdots \; i_\mu \leq \lfloor \frac{d_\mu - 1}{2} \rfloor \Big\} \tag{44}$$

とする．

以下では，式 (43) が式 (40)-(42) の制約条件を満たすことを示す．更に，式 (43) を式 (39) に代入すると，式 (23) の右辺になることを示す．すなわち，式 (43) が双対問題の実行可能解であり，式 (23) の右辺がそのときの目的関数値であることを示す．

明らかに，$\alpha_{(0,0,\cdots,0)} = 1$, $\alpha_{\boldsymbol{i}} \geq 0$, $\boldsymbol{i} \in W(\mathcal{T})$ なので，式 (40), (41) が成立する．式 (42) については次の

通りである．任意の $\boldsymbol{j} \in W(\mathcal{T}) \setminus \mathcal{D}$ について，

$$\sum_{\boldsymbol{i}\in W(\mathcal{T})} \prod_{\ell=1}^{\mu} P_{i_\ell}(j_\ell; n_\ell) \left\{ \frac{\sum_{\boldsymbol{a}\in\mathcal{E}} \prod_{\ell=1}^{\mu} P_{a_\ell}(i_\ell; n_\ell)}{|E|} \right\}^2$$

$$= \frac{1}{|E|^2} \sum_{\boldsymbol{i}\in W(\mathcal{T})} \sum_{\boldsymbol{a}\in\mathcal{E}} \sum_{\boldsymbol{b}\in\mathcal{E}} \times \prod_{\ell=1}^{\mu} P_{a_\ell}(i_\ell; n_\ell) \prod_{\ell=1}^{\mu} P_{b_\ell}(i_\ell; n_\ell) \prod_{\ell=1}^{\mu} P_{i_\ell}(j_\ell; n_\ell) \quad (45)$$

$$= \frac{1}{|E|^2 \prod_{\ell=1}^{\mu} \binom{n_\ell}{j_\ell}} \sum_{\boldsymbol{i}\in W(\mathcal{T})} \prod_{\ell=1}^{\mu} \binom{n_\ell}{i_\ell} \sum_{\boldsymbol{a}\in\mathcal{E}} \sum_{\boldsymbol{b}\in\mathcal{E}} \times \prod_{\ell=1}^{\mu} P_{a_\ell}(i_\ell; n_\ell) \prod_{\ell=1}^{\mu} P_{b_\ell}(i_\ell; n_\ell) \prod_{\ell=1}^{\mu} P_{j_\ell}(i_\ell; n_\ell) \quad (46)$$

$$= 0 \quad (47)$$

となる．なお，式 (46) は Lemma 5 を，式 (47) は Lemma 6 を用いた．従って，式 (43) は式 (40)-(42) を満たしている．そして，式 (43) を式 (39) に代入すると

$$\sum_{\boldsymbol{i}\in W(\mathcal{T})} \binom{n_1}{i_1} \binom{n_2}{i_2} \cdots \binom{n_\mu}{i_\mu} \times \left\{ \frac{\sum_{\boldsymbol{a}\in\mathcal{E}} \prod_{\ell=1}^{\mu} P_{a_\ell}(i_\ell; n_\ell)}{|E|} \right\}^2$$

$$= \frac{1}{|E|^2} \sum_{\boldsymbol{a}\in\mathcal{E}} \sum_{\boldsymbol{b}\in\mathcal{E}} \sum_{\boldsymbol{i}\in W(\mathcal{T})} \binom{n_1}{i_1} \binom{n_2}{i_2} \cdots \binom{n_\mu}{i_\mu} \times \prod_{\ell=1}^{\mu} P_{a_\ell}(i_\ell; n_\ell) \prod_{\ell=1}^{\mu} P_{b_\ell}(i_\ell; n_\ell) \quad (48)$$

$$= \frac{1}{|E|^2} \sum_{\boldsymbol{a}\in\mathcal{E}} \sum_{\boldsymbol{b}\in\mathcal{E}} 2^n \binom{n_1}{a_1} \binom{n_2}{a_2} \cdots \binom{n_\mu}{a_\mu} \times \delta_{a_1,b_1} \delta_{a_2,b_2} \cdots \delta_{a_\mu,b_\mu} \quad (49)$$

$$= \frac{2^n}{|E|^2} \sum_{\boldsymbol{a}\in\mathcal{E}} \binom{n_1}{a_1} \binom{n_2}{a_2} \cdots \binom{n_\mu}{a_\mu} \quad (50)$$

$$= \frac{2^n}{|E|} \quad (51)$$

となる．なお，式 (49) は Lemma 4 を用いた．以上から，式 (23) の右辺は実行可能解の目的関数値であり，Definition 4 の主問題の上界であることが示された．□

5　おわりに

本論文では，まず μ-レベル UEP 符号を定義し，μ-レベル UEP の LP 限界 (UEP-LPB) を導出した．更に，UEP-LPB と修正ハミング限界を比較し，UEP-LPB が修正ハミング限界よりも強い上界であることを示した．

参考文献

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

[2] P.Delsarte, “An algebraic approach to the association schemes of coding theory, ” Philips Res. Repts. Suppl., no.10, 1973.

[3] B. Masnick and J. Wolf, “On linear unequal error protection codes,” IEEE Trans. Inform. Theory, vol.IT-3, no.4, pp. 600-607, 1967.

[4] 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, no.5, pp.1307-1315, 2006.

[5] Tomohiko Saito, Hiroshige Inazumi, Toshiyasu Matsushima and Shigeichi Hirasawa, “Disk Allocation Methods for Cartesian Product Files Using Unequal Error Protection Codes,” Proceedings of IEEE International Conference on Systems, Man, and Cybernetics, pp.2437-2442, 2011.

[6] 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.

[7] W. J. van Gils, “Two topics on linear unequal error protection codes: bounds on their length and cyclic code classes,” IEEE Trans. Inf. Theory, vol. IT-29, pp. 866-876, 1983.

[8] I. M. Boyarinov, and G. L. Katsman, "Linear Unequal Error Protection Codes," IEEE Trans. Inf. Theory, vol.IT-27, no.2, pp.168-175, 1981.

[9] 齋藤友彦, 新家稔央, 浮田善文, 松嶋敏泰, 平澤茂一, "2-レベル不均一誤り訂正符号の線形計画限界," 電子情報通信学会論文誌 A, vol.J100-A, no.9, pp.316-324, 2017.

[10] J. Simonis, "MacWilliams Identities and Coordinate Partitions," Linear Algebra and Its Applications 216, pp.81-91, 1995.

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

付 録

A1. Proof of Lemma 2

i, j, N が $0 \le i, j \le N$ を満たす整数のとき，$w_h(\boldsymbol{v}) = j$ を満たす任意の $\boldsymbol{v} \in \mathbb{F}_2^n$ について，

$$P_i(j;n) = \sum_{\substack{\boldsymbol{u} \in \mathbb{F}_2^n, \\ w_h(\boldsymbol{u}) = i}} (-1)^{\boldsymbol{uv}} \tag{52}$$

が成り立つ [11, Theorem 4.10]．但し，$\boldsymbol{uv}$ は $\boldsymbol{u}$ と $\boldsymbol{v}$ の内積とする．従って，$w_h(\boldsymbol{v}_1) = j_1 \cdots, w_h(\boldsymbol{v}_\mu) = j_\mu$ を満たす任意の $\boldsymbol{v}_1 \in \mathbb{F}_2^{n_1}, \cdots, \boldsymbol{v}_\mu \in \mathbb{F}_2^{n_\mu}$ について，

$$\prod_{\ell=1}^{\mu} P_{i_\ell}(j_\ell; n_\ell) \tag{53}$$

$$= \sum_{\substack{\boldsymbol{u}_1 \in \mathbb{F}_2^{n_1}, \\ w_h(\boldsymbol{u}_1) = i_1}} \cdots \sum_{\substack{\boldsymbol{u}_\mu \in \mathbb{F}_2^{n_\mu}, \\ w_h(\boldsymbol{u}_\mu) = i_\mu}} (-1)^{\boldsymbol{u}_1\boldsymbol{v}_1 + \cdots + \boldsymbol{u}_\mu\boldsymbol{v}_\mu} \tag{54}$$

$$= \sum_{\substack{\boldsymbol{u} \in \mathbb{F}_2^n, \\ w_{\mathcal{T}}(\boldsymbol{u}) = (i_1, \cdots, i_\mu)}} (-1)^{\boldsymbol{uv}} \tag{55}$$

が成り立つ．但し，$\boldsymbol{v} \in \mathbb{F}_2^n$ は $w_{\mathcal{T}}(\boldsymbol{v}) = (j_1, \cdots, j_\mu)$ を満たす任意のベクトルである．従って，

$$\sum_{\boldsymbol{j} \in W(\mathcal{T})} A_{\boldsymbol{j}} \prod_{\ell=1}^{\mu} P_{i_\ell}(j_\ell; n_\ell) \tag{56}$$

$$= \frac{1}{M} \sum_{\boldsymbol{j} \in W(\mathcal{T})} \sum_{\substack{\boldsymbol{x}, \boldsymbol{y} \in C, \\ w_{\mathcal{T}}(\boldsymbol{y}-\boldsymbol{x}) = \boldsymbol{j}}} \sum_{\substack{\boldsymbol{u} \in \mathbb{F}_2^n, \\ w_{\mathcal{T}}(\boldsymbol{u}) = \boldsymbol{i}}} \times (-1)^{\boldsymbol{u}(\boldsymbol{y}-\boldsymbol{x})} \tag{57}$$

$$= \frac{1}{M} \sum_{\substack{\boldsymbol{u} \in \mathbb{F}_2^n, \\ w_{\mathcal{T}}(\boldsymbol{u}) = \boldsymbol{i}}} \left(\sum_{\boldsymbol{x} \in C} (-1)^{\boldsymbol{ux}} \right)^2 \ge 0 \tag{58}$$

となる． □

A2. Proof of Lemma 3

$((n_1, \cdots, n_\mu), M, (d_1, \cdots, d_\mu))$ 符号 C を仮定する．まず，任意の $\boldsymbol{x}, \boldsymbol{x}' \in C$ $(\boldsymbol{x} \ne \boldsymbol{x}')$, $\boldsymbol{e}, \boldsymbol{e}' \in E$ について，

$$\boldsymbol{x} + \boldsymbol{e} \ne \boldsymbol{x}' + \boldsymbol{e}' \tag{59}$$

が成り立つことを示す．式 (59) の右辺を左辺に移項した

$$(\boldsymbol{x} - \boldsymbol{x}') + (\boldsymbol{e} - \boldsymbol{e}') \tag{60}$$

を考えたとき，

$$w_h(\boldsymbol{x} - \boldsymbol{x}') \ge \begin{cases} d_1 \ (w_{\mathcal{T}}(\boldsymbol{x} - \boldsymbol{x}')_1 > 0) \\ d_2 \ (w_{\mathcal{T}}(\boldsymbol{x} - \boldsymbol{x}')_2 > 0) \\ \quad \vdots \\ d_\mu \ (w_{\mathcal{T}}(\boldsymbol{x} - \boldsymbol{x}')_\mu > 0) \end{cases} \tag{61}$$

が $((n_1, \cdots, n_\mu), M, (d_1, \cdots, d_\mu))$ 符号の定義より明らかである．ここで，$w_{\mathcal{T}}(\boldsymbol{x} - \boldsymbol{x}')_1 > 0$ であるとき，

$$w_h(\boldsymbol{e} - \boldsymbol{e}') \le w_h(\boldsymbol{e}) + w_h(\boldsymbol{e}') \le d_1 - 1 \tag{62}$$

なので，$(\boldsymbol{x} - \boldsymbol{x}') + (\boldsymbol{e} - \boldsymbol{e}') \ne \boldsymbol{0}$ である．更に，$w_{\mathcal{T}}(\boldsymbol{x} - \boldsymbol{x}')_1 = \cdots = w_{\mathcal{T}}(\boldsymbol{x} - \boldsymbol{x}')_{i-1} = 0$, $w_{\mathcal{T}}(\boldsymbol{x} - \boldsymbol{x}')_i > 0$ $(i = 2, \cdots, \mu)$ の場合を考える．$1 \le j \le i$ and $w_{\mathcal{T}}(\boldsymbol{e} - \boldsymbol{e}')_j \ne 0$ を満たす j が存在するとき，明らかに $(\boldsymbol{x} - \boldsymbol{x}') + (\boldsymbol{e} - \boldsymbol{e}') \ne \boldsymbol{0}$ が成り立つ．一方，$w_{\mathcal{T}}(\boldsymbol{e} - \boldsymbol{e}')_1 = \cdots = w_{\mathcal{T}}(\boldsymbol{e} - \boldsymbol{e}')_{i-1} = 0$ であるとき，

$$w_h(\boldsymbol{e} - \boldsymbol{e}') \le \sum_{\ell=i}^{\mu} w_{\mathcal{T}}(\boldsymbol{e} - \boldsymbol{e}')_\ell \le d_i - 1 \tag{63}$$

から，$(\boldsymbol{x}-\boldsymbol{x}')+(\boldsymbol{e}-\boldsymbol{e}') \neq \boldsymbol{0}$ が成り立つ．従って，式 (59) が証明された．

次に，式 (23) を証明する．ここで，$C=\{\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_M\}$，$B(\boldsymbol{x}_i)=\{\boldsymbol{x}_i+\boldsymbol{e} | \boldsymbol{e} \in E\}$，$i=1,2,\ldots,M$ とする．式 (59) から，任意の i, j $(i,j \in \{1,2,\ldots,M\}$, $i \neq j)$ について，$B(\boldsymbol{x}_i) \cap B(\boldsymbol{x}_j)=\phi$ が成り立つ．従って，$B(\boldsymbol{x}_1) \cup B(\boldsymbol{x}_2) \cup \cdots \cup B(\boldsymbol{x}_M) \subseteq \mathbb{F}_2^n$ であり，

$$|B(\boldsymbol{x}_1) \cup B(\boldsymbol{x}_2) \cup \cdots \cup B(\boldsymbol{x}_M)| = M|E| \leq 2^n \quad (64)$$

が示された．　□