論　文

ブロックターボ符号のインタリーバ構成法と最小距離

小林　学[†a)]　松嶋　敏泰[††]　平澤　茂一[††]

On the Interleaver Design Method for Block Turbo Codes and Its Minimum Distance

Manabu KOBAYASHI[†a)], Toshiyasu MATSUSHIMA[††], and Shigeichi HIRASAWA[††]

あらまし　1993 年，C. Berrou らは加法的白色ガウス雑音（AWGN）通信路に対し 1 情報記号当りの信号対雑音比 (E_b/N_0) に対するシャノン限界に近いビット誤り確率（BER）を達成するターボ符号を提案した．その後 S. Benedetto ら及び J. Hagenauer らにより，構成符号にブロック符号を用いるブロックターボ符号が提案されている．本論文では S. Benedetto らにより提案された PCBC（Parallel Concatenated Block Codes）型ブロックターボ符号を一次元の符号とみなしたときの性能の解析を行い，大きな最小距離をもつインタリーバの構成法を提案する．まずとり得るインタリーバに制約を加えることにより，各情報記号のハミング重み（情報重み）に対応する符号語のハミング重み（符号語重み）の下界を導出する．更に情報重みが 1 及び 2 のときの符号語重みに対する下界を大きくするインタリーバの構成手法を示し，最小距離を大きくすることが可能な要素符号を探索により求めるアルゴリズムを提案する．結果的に得られる要素符号及びインタリーバを用いることにより，従来より大きな最小距離を保証するブロックターボ符号を設計することが可能となる．

キーワード　ブロックターボ符号，Parallel Concatenated Block Codes，インタリーバ，Code-Matched Interleaver，最小距離

1. まえがき

1993 年 C. Berrou らは，加法的白色ガウス雑音（AWGN）通信路に対し単位情報記号当りの信号対雑音比 (E_b/N_0) に対するシャノン限界に近いビット誤り確率（BER）を達成するターボ符号を提案した．C. Berrou らにより提案されたターボ符号は帰還回路をもつ二つの組織的畳込み符号器を並列に連接した符号である [1]〜[3]．復号にはこれらの要素符号それぞれに対し最大事後確率（MAP）復号を用い，それぞれの情報ビットごとに信頼度情報（外部情報と呼ばれる）を生成する．このターボ復号では，一方の復号器のこの外部情報を他方の復号器に対する情報の事前確率とみなし，MAP 復号を互いに繰り返すことにより，最終的に送られた情報を推定する．また要素符号の外部情報を生成する手法や，厳密な MAP 復号を行わずにこれを近似する復号法など種々研究されている [2]〜[4]．更に要素符号に組織的畳込み符号を用いたターボ符号に対し，その要素符号の特性を考慮したインタリーバの構成法が提案されており，復号誤り確率を大幅に低減させることに成功している [3], [6]〜[8]．このインタリーバは CMI（Code-Matched Interleaver）と呼ばれる．

一方，要素符号に組織ブロック符号を用いたブロックターボ符号も提案されている [4], [9]〜[12]．ブロックターボ符号の利点としては，復号の際に各ブロック符号を並列に処理することにより復号遅延を少なくできること，符号化率を高くすることが可能なことなどが挙げられる．

本論文ではブロックターボ符号の中でも S.Benedetto らにより提案された PCBC（Parallel Concatenated Block Codes）型ブロックターボ符号 [9] を対象とする．PCBC の有効性については，例えば論文 [10], [11]

† 湘南工科大学情報工学科，藤沢市
Department of Information Science, Shonan Institute of Technology, 1–1–25 Tsujido-Nishikaigan, Fujisawa-shi, 251–8511 Japan
†† 早稲田大学理工学部経営システム工学科，東京都
School of Science and Engineering, Waseda University, 3–4–1 Okubo, Shinjyuku-ku, Tokyo, 169–8555 Japan
a) E-mail: kobayasi@info.shonan-it.ac.jp

において要素符号に (1023,1013) ハミング符号を用いてターボ復号を行った場合，10^{-5} のビット誤り確率においてシャノン限界からの距離が約 0.28 dB 以下であることがシミュレーションにより確かめられている．また PCBC についてターボ復号の特性を考慮し，与えられた受信語に対して各情報ビットの外部情報の収束性に関する解析も行われている [13]．また要素符号の符号化率に依存するが，PCBC は積符号よりも符号化率が高くなる．

そこで本論文では積符号ではないブロックターボ符号として PCBC を対象とし，一次元の符号とみなしたときの性能の解析を行い，大きな最小距離をもつインタリーバの構成法を提案する．

まずインタリーバに制限を加えることにより，最小距離の下界を大きくすることが可能となることを示す．更にこの制限により，各情報記号のハミング重みに対応する符号語のハミング重みの下界も導出される．その結果，与えられたインタリーバに対しある範囲の低域重み分布を少ない計算量で厳密に求めることが可能となる．これは種々のインタリーバに対する平均的な重み分布を求めるのではなく，与えられた生成行列及びインタリーバに対し，正確な低域重み分布を探索により求めることを意味している．

また情報記号のハミング重みが 1 及び 2 のときの符号語のハミング重みに対する下界を大きくするインタリーバの構成手法を示す．このようにして得られるインタリーバは，ブロックターボ符号に対する CMI に相当する．更にブロックターボ符号の最小距離を大きくすることが可能な要素ブロック符号を探索により求めるアルゴリズムを提案する．結果的に得られる要素符号及びインタリーバを用いることにより，従来より大きな最小距離を保証するブロックターボ符号を設計することが可能となる．

2. PCBC 型ブロックターボ符号

S. Benedetto らにより提案された PCBC（Parallel Concatenated Block Codes）型ブロックターボ符号（以下 PCBC と略す）C_B は，各要素符号の検査記号が情報にのみ依存し，互いの検査記号には影響を受けない構成となっている [9]．今正整数 k_1, k_2, l_1, l_2 に対し $k_1 l_1 (= k_2 l_2)$ ビットの 2 元情報 $\boldsymbol{u}$ を k_1 ビットごとに l_1 個のブロック（ベクトル）に分割する．すなわち $\boldsymbol{u} = (\boldsymbol{u}_1^{(1)}, \boldsymbol{u}_2^{(1)}, \cdots, \boldsymbol{u}_{l_1}^{(1)})$, $\boldsymbol{u}_i^{(1)} = (u_{i,1}^{(1)}, u_{i,2}^{(1)}, \cdots, u_{i,k_1}^{(1)}), i \in [1, l_1]$, とおく．ただし整数 x, y に対し $[x, y] = \{x, x+1, \cdots, y\}$ と定義する．このそれぞれのベクトル $\boldsymbol{u}_i^{(1)}$ を情報とみなし，(n_1, k_1, d_1) 組織符号 C_1 を用いて符号化を行う．また C_1 の生成行列を G_1 と表し，一般性を失うことなく $G_1 = [I_{k_1}, Q_1]$ の形式をしているものとする．ここで I_a は $a \times a$ 単位行列を表し，Q_1 は $k_1 \times (n_1 - k_1)$ 行列である．この G_1 を用いて $\boldsymbol{c}^{(1)} = (\boldsymbol{c}_1^{(1)}, \boldsymbol{c}_2^{(1)}, \cdots, \boldsymbol{c}_{l_1}^{(1)})$, $\boldsymbol{c}_i^{(1)} = \boldsymbol{u}_i^{(1)} G_1 = (\boldsymbol{u}_i^{(1)}, \boldsymbol{v}_i^{(1)})$, $\boldsymbol{v}_i^{(1)} = (v_{i,1}^{(1)}, v_{i,2}^{(1)}, \cdots, v_{i,n_1-k_1}^{(1)})$, が得られる．

更に $k_1 l_1 \times k_2 l_2$ 置換行列 P_B により $\boldsymbol{u}$ を置換し，$\boldsymbol{u}' = \boldsymbol{u} P_B$ を得る(注1)．置換行列はインタリーバの役割を果たす．今度はこれを k_2 ビットごとに l_2 個のブロック（ベクトル）に分割し，$\boldsymbol{u}' = (\boldsymbol{u}_1^{(2)}, \boldsymbol{u}_2^{(2)}, \cdots, \boldsymbol{u}_{l_2}^{(2)})$, $\boldsymbol{u}_i^{(2)} = (u_{i,1}^{(2)}, u_{i,2}^{(2)}, \cdots, u_{i,k_2}^{(2)}), i \in [1, l_2]$, と表す．このそれぞれのベクトル $\boldsymbol{u}_i^{(2)}, i \in [1, l_2]$, に対し (n_2, k_2, d_2) 組織符号 C_2 を用いて符号化を行う．C_2 の生成行列を $G_2 = [I_{k_2}, Q_2]$ と表すと結果的に $\boldsymbol{c}^{(2)} = (\boldsymbol{c}_1^{(2)}, \boldsymbol{c}_2^{(2)}, \cdots, \boldsymbol{c}_{l_2}^{(2)})$, $\boldsymbol{c}_i^{(2)} = \boldsymbol{u}_i^{(2)} G_2$, が得られる．最終的に C_B の符号語 $\boldsymbol{c}_B$ は次式で表すことができる．

$$\boldsymbol{c}_B = (\boldsymbol{c}_1^{(2)}, \boldsymbol{c}_2^{(2)}, \cdots, \boldsymbol{c}_{l_2}^{(2)}, \boldsymbol{v}_1^{(1)}, \boldsymbol{v}_2^{(1)}, \cdots, \boldsymbol{v}_{l_1}^{(1)}). \tag{1}$$

C_1, C_2 ともに組織符号であること，及び式 (1) から明らかに C_B は組織符号である．

J. Hagenauer らの論文 [4] に示されているブロックターボ符号は，上の C_B の構成法において $l_1 = k_2$ とした特別の場合である．

これ以降情報記号のハミング重みを情報重み，検査記号のハミング重みを検査重み，更に符号語のハミング重みを符号語重みと呼ぶことにする．

3. インタリーバの制限及び情報重みに対する符号語重みの下界

本章では，前章で定義した PCBC の最小距離の下界を求める．また置換行列（すなわちインタリーバ）を制限することにより，最小距離の下界を大きくすることができることを示す．更にこの置換行列の制限から，情報重みごとの符号語重みの下界を求める．

3.1 インタリーバの制限

まず PCBC の最小距離の下界を示す．

(注1)：ここで置換行列 P_B はその各行及び各列のハミング重みが厳密に 1 の行列である．

［定理 1］ C_B の最小距離 D_B は $D_B \geq \max\{d_1, d_2\}$ を満たす．
（証明） 符号の構成法から明らかである． □

定理 1 は C_B に任意の置換行列を用いたときの最小距離の下界を示している．そこでこの下界と一致する P_B 及び C_B が存在することを示す．

［定義 1］ 任意の符号 C に対し情報重みが w でかつ検査重みが z の符号語数を $A^C_{w,z}$ と表記する．また $w_H(\boldsymbol{x})$ をベクトル $\boldsymbol{x}$ のハミング重みを表すものとする． □

［定理 2］ $d_1 \leq d_2$ である C_1, C_2 について

$$A^{C_1}_{w,0} > 0 \ \text{ and } \ A^{C_2}_{w,d_2-w} > 0, \tag{2}$$

を満たす $d_1 \leq w \leq d_2$ が存在するとき，$D_B = d_2$ を満たす P_B 及び C_B が存在する．
（証明） 式 (2) より $w_H(\boldsymbol{u}) = w_H(\boldsymbol{u}^{(1)}_i) = w_H(\boldsymbol{c}^{(1)}_i) = w$ を満足する $\boldsymbol{u}$ 及び i が存在する．またある j に対し $w_H(\boldsymbol{u}') = w_H(\boldsymbol{u}^{(2)}_j) = w$ 及び $w_H(\boldsymbol{c}^{(2)}_j) = d_2$ を満たす $\boldsymbol{u}'$ を考えると，$w_H(\boldsymbol{u}) = w_H(\boldsymbol{u}') = w$ であるため $\boldsymbol{u}' = \boldsymbol{u}P_B$ を満たす P_B は必ず存在する．このとき結果的に得られる符号語重みは d_2 となり，定理 1 より結局 $D_B = d_2$ となる． □

（注意） もし $d_1 > d_2$ ならば符号化の順序を変更し，C_1 の代わりに C_2 を，C_2 の代わりに C_1 を用い，置換行列を適当に変更することにより同値な符号ができる．したがって $d_1 > d_2$ の場合も定理 2 と同様のことがいえる．

定理 2 は最小距離が最も小さくなる最悪の P_B が存在するための十分条件を示しているにすぎない(注2)．しかし定理 2 の証明から分かることは，置換前のあるブロック $\boldsymbol{u}^{(1)}_i$ の情報記号にのみ 1 があり，これらの 1 をもつ情報記号が置換後にやはり同一のブロック $\boldsymbol{u}^{(2)}_j$ に置換されてしまうと，小さな符号語重みを与えてしまう可能性があることである．

そこでまず最小距離の下界を大きくするために，情報 $\boldsymbol{u}$ における同一ブロック $\boldsymbol{u}^{(1)}_i$ 中の任意の 2 ビットが，置換後の情報 $\boldsymbol{u}'$ 中の同一ブロックへ置換されることはないように P_B に制約を設ける．ここで $u^{(1)}_{i,x}$ が置換行列 $P_B = [p_{a,b}]$, $a, b \in [1, k_1 l_1]$, により $u^{(2)}_{j,y}$ に置換されるのは，$p_{(i-1)k_1+x,(j-1)k_2+y} = 1$ のときであることに注意すると，P_B に対するこの制約は次式で表される．

$$\sum_{a=(i-1)k_1+1}^{ik_1} \ \sum_{b=(j-1)k_2+1}^{jk_2} p_{a,b}=1, \qquad \forall i \in [1, l_1], \ \ \forall j \in [1, l_2], \tag{3}$$

ただし式 (3) の和は通常の整数の加算を表す．

この制約により，置換前のあるブロックの情報記号にのみ 1 がある場合，これらの 1 をもつ情報記号は置換後に必ず別のブロックに置換されることになり，それぞれが非ゼロの符号語に符号化され，符号語重みを大きくすることができる．以下で詳しく述べるが，これにより定理 1 よりも最小距離の下界を大きくすることができる．

式 (3) を満足する置換行列 P_B をもつ PCBC をこれ以降 C^*_B と表す．

（注意） 式 (3) の制約を満たすためには $l_1 \geq k_2$ であることが必要となる．そこで本論文ではこれ以降 $l_1 \geq k_2$ であるものとして議論を進める．

3.2 情報重みに対する符号語重みの下界

ここでは C^*_B に対して，各情報重みに対応する符号語重みの最小値を評価し，その下界を求める．

［定義 2］ 情報 $\boldsymbol{u} = (\boldsymbol{u}^{(1)}_1, \boldsymbol{u}^{(1)}_2, \cdots, \boldsymbol{u}^{(1)}_{l_1})$, $\boldsymbol{u}^{(1)}_i \in \{0,1\}^{k_1}$, に対し $S^{(1)}(\boldsymbol{u}) = \{i \in [1, l_1] | w_H(\boldsymbol{u}^{(1)}_i) > 0\}$ と定義する．また $\boldsymbol{u}' = (\boldsymbol{u}^{(2)}_1, \boldsymbol{u}^{(2)}_2, \cdots, \boldsymbol{u}^{(2)}_{l_2}) = \boldsymbol{u}P_B$, $\boldsymbol{u}^{(2)}_i \in \{0,1\}^{k_2}$, に対し $S^{(2)}(\boldsymbol{u}) = \{i \in [1, l_2] | w_H(\boldsymbol{u}^{(2)}_i) > 0\}$ と定義する． □

この定義を用いると次の補題が成り立つ．

［補題 1］ 情報 $\boldsymbol{u}$ に対応する C_B の符号語 $\boldsymbol{c}_B$ は次式を満足する．

$$w_H(\boldsymbol{c}_B) \geq d_2 |S^{(2)}(\boldsymbol{u})| + d_1 |S^{(1)}(\boldsymbol{u})| - w_H(\boldsymbol{u}), \tag{4}$$

ただし集合 X に対し $|X|$ は X の要素数を表す．
（証明） 式 (1) 及び定義 2 より次式が成り立つ．

$$w_H(\boldsymbol{c}_B) = \sum_{i=1}^{l_2} w_H(\boldsymbol{c}^{(2)}_i) + \sum_{i=1}^{l_1} w_H(\boldsymbol{v}^{(1)}_i)$$

(注2)：実際に $D_B = d_2$ となる P_B がどの程度存在するかは確率的に評価する必要があるが，ここでは議論の対象外とする．

$$= \sum_{i=1}^{l_2} w_H(\boldsymbol{c}_i^{(2)}) + \sum_{i=1}^{l_1} \left(w_H(\boldsymbol{c}_i^{(1)}) - w_H(\boldsymbol{u}_i^{(1)}) \right)$$
$$= \sum_{i \in S^{(2)}(\boldsymbol{u})} w_H(\boldsymbol{c}_i^{(2)}) + \sum_{i \in S^{(1)}(\boldsymbol{u})} w_H(\boldsymbol{c}_i^{(1)}) - w_H(\boldsymbol{u})$$
$$\geq d_2 |S^{(2)}(\boldsymbol{u})| + d_1 |S^{(1)}(\boldsymbol{u})| - w_H(\boldsymbol{u}). \quad (5)$$

以上より補題が証明された. □

［補題 2］ C_B^* に対し $S^{(1)}(\boldsymbol{u}), S^{(2)}(\boldsymbol{u})$ は次式を満たす.

$$|S^{(1)}(\boldsymbol{u})||S^{(2)}(\boldsymbol{u})| \geq w_H(\boldsymbol{u}). \quad (6)$$

（証明） ある i に対し $w_H(\boldsymbol{u}_i^{(1)}) = a$ とすると，この a ビットの非ゼロの情報は式 (3) の制約から，$\boldsymbol{u}' = (\boldsymbol{u}_1^{(2)}, \boldsymbol{u}_2^{(2)}, \cdots, \boldsymbol{u}_{l_2}^{(2)}) = \boldsymbol{u}P_B$ において必ず互いに異なるブロックに置換される．すなわち $|S^{(2)}(\boldsymbol{u})| \geq a$ となる．また

$$\max_{i \in [1,l_1]} \left\{ w_H(\boldsymbol{u}_i^{(1)}) \right\} \geq \frac{w_H(\boldsymbol{u})}{|S^{(1)}(\boldsymbol{u})|} \quad (7)$$

である．したがって補題が成り立つ. □

［定義 3］ 正整数 w と $i \in [1, w]$ に対し

$$W_{(d_1,d_2)}(i, w) = d_2 \left\lceil \frac{w}{i} \right\rceil + d_1 i - w, \quad (8)$$
$$W_{(d_1,d_2)}(w) = \min_{i \in [1,w]} W_{(d_1,d_2)}(i, w), \quad (9)$$

と定義する．ただし $\lceil a \rceil$ は a 以上の最小の整数を表す．また d_1 と d_2 に関して混同のおそれがないときは式 (8)，(9) をそれぞれ $W(i, w), W(w)$ と略記する．更に C_B, C_B^* の生成行列をそれぞれ G_B, G_B^* と表す. □

［定義 4］ 任意の符号 C に対し情報重みが w の符号語中で最小の符号語重みを D_w^C と表記する．すなわち C の生成行列を G としたとき

$$D_w^C = \min_{\boldsymbol{u} | w_H(\boldsymbol{u}) = w} w_H(\boldsymbol{u}G), \quad (10)$$

と定義する. □

これらの定義と補題 1，2 より次の補題が即座に導かれる.

［補題 3］ 任意の $w \in [1, k_1 l_1]$ に対し

$$D_w^{C_B^*} \geq W(w), \quad (11)$$

が成り立つ. □

［定理 3］ C_B^* の最小距離 D_B^* は $D_B^* \geq W(1,1) = d_1 + d_2 - 1$ が成り立つ.

（証明） $w_H(\boldsymbol{u}) \geq W(1,1)$ に関しては明らかに $w_H(\boldsymbol{u}G_B^*) \geq W(1,1)$ であるから $w_H(\boldsymbol{u}) = w < W(1,1)$ を仮定する．ここで任意の $i \in [1, w]$ に対して $W(i, w) \geq W(1,1)$ であるから，これと補題 3 より

$$D_B^* = \min_{\boldsymbol{u} \neq \boldsymbol{0}} \{ w_H(\boldsymbol{u}G_B) \} \geq W(1,1), \quad (12)$$

となり定理が成り立つ. □

次に $d_1 = d_2$ としたとき，情報重み w に対する符号語重みの下界 $W(w)$ を求める.

［定理 4］ $d_1 = d_2$ のとき次式が成り立つ.

$$W_{(d_1,d_2)}(w) = \begin{cases} (2\lceil \sqrt{w} \rceil - 1)d_1 - w, \\ \qquad \text{if } (\lceil \sqrt{w} \rceil - 1)\lceil \sqrt{w} \rceil \geq w, \\ 2\lceil \sqrt{w} \rceil d_1 - w, \qquad \text{otherwise.} \end{cases} \quad (13)$$

（証明） 付録 **1.** 参照. □

さて，C_B^* の最小距離 D_B^* の下界は定理 3 で述べたとおり $d_1 + d_2 - 1$ であるが，今 $d_1 + d_2 - 1$ を一定として考えると次の定理が成り立つ.

［定理 5］ $d_1 + d_2 - 1$ を一定の奇数としたとき，それぞれの w に対し $W_{(d_1,d_2)}(w)$ を最大にする d_1, d_2 の組は $d_1 = d_2$ である.

（証明） 付録 **2.** 参照. □

補題 3 と定理 5 より，PCBC C_B^* では $d_1 = d_2$ とすることにより，最小距離の下界 $d_1 + d_2 - 1$ を一定に保ったもとで情報重みに対する検査重みの下界を最も大きくすることができる．したがって以下では $d_1 = d_2$ を仮定する.

［定義 5］ $H(w)$ 及び $U(w)$ を次式で定義する.

$$H(w) = \min_{w \leq w' \leq d_1^2} W_{(d_1,d_1)}(w'), \quad (14)$$

$$U(w) = \begin{cases} \lceil \sqrt{w} \rceil (\lceil \sqrt{w} \rceil - 1), \\ \qquad \text{if } (\lceil \sqrt{w} \rceil - 1)\lceil \sqrt{w} \rceil \geq w, \\ \lceil \sqrt{w} \rceil^2, \qquad \text{otherwise.} \end{cases} \quad (15)$$

ここで $H(w)$ は情報重みが w 以上 d_1^2 以下の符号語重みの下界を表している. □

［補題 4］ $U(w)$ に対し $\lceil\sqrt{U(w)}\rceil = \lceil\sqrt{w}\,\rceil$ が成り立つ．
（証明） $U(w) = \lceil\sqrt{w}\,\rceil^2$ ならば明らかなので，$U(w) = \lceil\sqrt{w}\,\rceil(\lceil\sqrt{w}\,\rceil - 1)$ を仮定する．もし $\lceil\sqrt{U(w)}\rceil \geq \lceil\sqrt{w}\,\rceil + 1$ ならば

$$\begin{aligned}&\lceil\sqrt{w}\,\rceil(\lceil\sqrt{w}\,\rceil - 1)\\ &\quad\leq (\lceil\sqrt{U(w)}\rceil - 1)(\lceil\sqrt{U(w)}\rceil - 2)\\ &\quad< \sqrt{U(w)}(\sqrt{U(w)} - 1) < U(w),\end{aligned} \tag{16}$$

となり仮定と矛盾する．同様に $\lceil\sqrt{U(w)}\rceil \leq \lceil\sqrt{w}\,\rceil - 1$ とすると

$$\begin{aligned}&\lceil\sqrt{w}\,\rceil(\lceil\sqrt{w}\,\rceil - 1)\\ &\quad\geq (\lceil\sqrt{U(w)}\rceil + 1)\lceil\sqrt{U(w)}\rceil > U(w),\end{aligned} \tag{17}$$

となり仮定と矛盾する．したがって補題が成り立つ．
□

［補題 5］ $d_1 = d_2$ かつ $w < w' \leq d_1^2$ に対し $W_{(d_1,d_1)}(U(w)) \leq W_{(d_1,d_1)}(U(w'))$ が成り立つ．
（証明） 付録 **3.** 参照 □

定理 4，補題 4，5 より次の定理が成り立つ．

［定理 6］ $d_1 = d_2$ のとき次式が成り立つ．

$$H(w) = \begin{cases} (2\lceil\sqrt{w}\,\rceil - 1)d_1 - \lceil\sqrt{w}\,\rceil(\lceil\sqrt{w}\,\rceil - 1), \\ \qquad\qquad \text{if } (\lceil\sqrt{w}\,\rceil - 1)\lceil\sqrt{w}\,\rceil \geq w, \\ 2\lceil\sqrt{w}\,\rceil d_1 - \lceil\sqrt{w}\,\rceil^2, \qquad \text{otherwise.} \end{cases} \tag{18}$$

（証明） 定義より $w \leq U(w)$ でかつ補題 4 より $\lceil\sqrt{w}\,\rceil = \lceil\sqrt{U(w)}\rceil$ であるから，定理 4 より

$$W_{(d_1,d_1)}(w) \geq W_{(d_1,d_1)}(U(w)), \tag{19}$$

である．これと補題 5 より $W_{(d_1,d_1)}(U(w))$ は w に関して単調非減少であるから $H(w) = W_{(d_1,d_1)}(U(w))$ となる．したがって定理が成り立つ． □

$H(d_1^2) = d_1^2$ で，$w_H(\boldsymbol{u}) > d_1^2$ に対しては明らかに $w_H(\boldsymbol{u}G_B^*) > d_1^2$ である．したがってある $w_{max} \leq d_1^2$ を選び $w_H(\boldsymbol{u}) \leq w_{max}$ を満たすすべての $\boldsymbol{u}$ について $w_H(\boldsymbol{u}G_B^*)$ を求めたとき，符号語重みが $H(w_{max}+1)$ 未満の低域重み分布が厳密に求まる．すなわち

$$\{A_{w,z}^{C_B^*} | w + z < H(w_{max} + 1)\}, \tag{20}$$

が求まる．

［例 1］ $d_1 = d_2 = 4$ とすると定理 6 より $H(1) = 7, H(2) = 10, H(3) = H(4) = 12$，である．したがって $w_{max} = 2$ としてハミング重みが 2 以下の情報をすべて符号化し，符号語重みを調べると，ハミング重みが $H(w_{max}+1) - 1 = 11$ 以下の符号語数及び重み分布が求められる．同様に $d_1 = d_2 = 6$ とすると $H(1) = 11, H(2) = 16, H(3) = H(4) = 20$，であるから，$w_{max} = 2$ とすると符号語重みが 19 以下の重み分布が求められる． □

3.3 S-ランダムインタリーバとの関係

ここでは，式 (3) の制約を満たすインタリーバと，よく知られている S-ランダムインタリーバ [3], [5] との関係について述べる．今置換行列 $P_B = [p_{a,b}]$ に対し，$\pi(a)$ を $p_{a,b} = 1 \Leftrightarrow \pi(a) = b$ と定義する．これは情報 $\boldsymbol{u}$ 中の位置 a にある情報記号は，置換後の情報 $\boldsymbol{u}'$ 中の位置 $\pi(a)$ に置換されることを意味する．このとき S-ランダムインタリーバはある定数 s_1, s_2 に対して次式を満たすような制約をもつインタリーバである．

$$0 < |a - a'| \leq s_1 \Rightarrow |\pi(a) - \pi(a')| > s_2. \tag{21}$$

すなわち置換前の情報 $\boldsymbol{u}$ 中の任意の二つの情報記号の位置 a, a' が定数 s_1 以下の距離にある場合，情報 $\boldsymbol{u}'$ 中の置換後の二つの情報記号の位置 $\pi(a), \pi(a')$ の距離は定数 s_2 より大きくする．

さてこの S-ランダムインタリーバに対し，定数を

$$s_1 \geq k_1 - 1, \quad s_2 \geq k_2 - 1, \tag{22}$$

となるように設定すると，式 (3) の制約を満足する．なぜならば，$|a - a'| \leq k_1 - 1$ を満たす二つの情報記号の位置 a, a' は置換前の情報 $\boldsymbol{u}$ 中の同一情報ブロックに存在する可能性があるが，そのとき条件より $|\pi(a) - \pi(a')| > k_2 - 1$ であるから置換後の位置 $\pi(a), \pi(a')$ は $\boldsymbol{u}'$ 中の同一ブロックとはならないからである．したがって，本章で述べた C_B^* に対する補題や定理は，式 (22) を満足する S-ランダムインタリーバに対してもすべて成り立つ．

以上の考察から，式 (3) の制約をもつインタリーバは，本章の補題や定理を満足する意味で式 (21)，(22) の制約よりも若干緩いが，考え方は PCBC に対する S-ランダムインタリーバに対応している．

4. インタリーバの構成

前章で示したように，小さな符号語重みを与える情

報は情報重み w が小さい場合（特に $w=1,2$ の場合）である．そこで本章ではインタリーバ（置換行列）P_B に更なる制限を加え，情報重み $w=1,2$ それぞれに対する C_B^* の符号語重みの最小値 $D_w^{C_B^*}$ のより厳しい下界を求める．またこの下界を大きくするインタリーバの構成法について述べる．具体的には，要素符号の生成行列 G_1 の検査重みが小さな行に対応する情報記号は，置換後に G_2 の検査重みが大きな行に対応する位置へ置換する．この考え方により小さな重みの情報に対してなるべく大きな符号語重みを出力し，下界を大きくすることが可能となる．

以降簡単のため要素符号を $C_1=C_2$ とし，かつその生成行列を $G_1=G_2$ とする．

4.1 情報重み 1 に対するインタリーバ構成法

［定義 6］ ある正定数 M に対し $F:[1,M]\to[1,M]$ を $F^{-1}(i)=F(i), i\in[1,M]$, を満たす全単射の関数とする．生成行列 G_1 の各行を $\boldsymbol{g}_i, i\in[1,k_1]$, と表し，$X_1, X_2, \cdots, X_M$ を

$$\bigcup_{i=1}^{M} X_i=[1,k_1], \qquad X_i\cap X_j=\phi,\ \ i\neq j,$$
$$|X_j|=|X_{F(j)}|\neq 0,\ \ j\in[1,M], \tag{23}$$

を満たすように G_1 の行番号の集合を分割したものとする． □

このような $X_1, X_2, \cdots, X_M$ 及び関数 $F(i), i\in[1,M]$, が与えられたとき，置換行列 $P_B=[p_{a,b}]$, $a,b\in[1,k_1l_1]$, に対し式 (3) に加え，更に次のような制約を設ける．

$$(a-1 \bmod k_1)+1\in X_i \ \text{ and } \ p_{a,b}=1$$
$$\Rightarrow (b-1 \bmod k_2)+1\in X_{F(i)}. \tag{24}$$

すなわち情報 $\boldsymbol{u}=(\boldsymbol{u}_1^{(1)}, \boldsymbol{u}_2^{(1)}, \cdots, \boldsymbol{u}_{l_1}^{(1)})$, $\boldsymbol{u}'=(\boldsymbol{u}_1^{(2)}, \boldsymbol{u}_2^{(2)}, \cdots, \boldsymbol{u}_{l_2}^{(2)})=\boldsymbol{u}P_B$ とすると，$\forall j$ に対し置換前の情報ブロック $\boldsymbol{u}_j^{(1)}\in\{0,1\}^{k_1}$ 中の X_i の要素の情報記号は，$\exists j'$ に対し置換後の情報ブロック $\boldsymbol{u}_{j'}^{(2)}\in\{0,1\}^{k_2}$ 中の $X_{F(i)}$ の要素の情報記号へと置換する．

この制約を用いて最小距離を大きくする方針を述べる．今情報 $\boldsymbol{u}$ の重みを 1 と仮定する．ある X_i の要素 x に 1 をもつ情報ブロックを G_1 で符号化すると $\boldsymbol{g}_x$ となる．またこの情報記号を置換したブロック内の位置を $y\in X_{F(i)}$ とすると，符号語は $\boldsymbol{g}_y$ である．そこでもし $\boldsymbol{g}_x$ の検査重みが小さいときは，$\boldsymbol{g}_y$ の検査重みが大きくなるように $X_{F(i)}$ を選ぶ．このときブロックターボ符号の符号語重みは明らかに $\boldsymbol{g}_x+\boldsymbol{g}_y-1$ であるから，これにより定理 3 よりも最小距離の下界を大きくすることが可能となる．

［定義 7］ 関数 $J(x)$ を $x\in X_i \Leftrightarrow J(x)=i$ と定義し，$Z(x)$ を

$$Z(x)=\min_{j\in X_{F(J(x))}} w_H(\boldsymbol{g}_j)-1, \tag{25}$$

と定義する． □

このとき $D_1^{C_B^*}$ に関して次の補題が成り立つ．

［補題 6］ 与えられた X_i, $F(i)$, $i\in[1,M]$, に対し式 (3)，(24) を満足するように置換行列に制限を加えたとき，次式を満足する定数 D_1 が存在するならば $D_1^{C_B^*}\geq D_1$ が成り立つ．

$$\min_{x\in[1,k_1]}\{Z(x)+w_H(\boldsymbol{g}_x)\}\geq D_1. \tag{26}$$

（証明） $w_H(\boldsymbol{u})=1$ を満たす $\boldsymbol{u}=(\boldsymbol{u}_1^{(1)}, \boldsymbol{u}_2^{(1)}, \cdots, \boldsymbol{u}_{l_1}^{(1)})$ と $\boldsymbol{u}'=(\boldsymbol{u}_1^{(2)}, \boldsymbol{u}_2^{(2)}, \cdots, \boldsymbol{u}_{l_2}^{(2)})=\boldsymbol{u}P_B$ について考える．ある i,x に対し $\boldsymbol{u}_i^{(1)}=(u_{i,1}^{(1)}, u_{i,2}^{(1)}, \cdots, u_{i,k_1}^{(1)})$, $u_{i,x}^{(1)}=1$ とすると G_1 による符号化により $\boldsymbol{c}_i^{(1)}=\boldsymbol{u}_i^{(1)}G_1=\boldsymbol{g}_x$ となる．また $p_{(i-1)k_1+x,b}=1$ を満たす b に対し，$\boldsymbol{u}_j^{(2)}=(u_{j,1}^{(2)}, u_{j,2}^{(2)}, \cdots, u_{j,k_2}^{(2)}), j=\lceil b/k_2\rceil$ とすると，$u_{i,x}^{(1)}$ は置換行列により $u_{j,y}^{(2)}, y=(b-1 \bmod k_2)+1$, へ置換される．したがって $u_{j,y}^{(2)}=1$ より $\boldsymbol{c}_j^{(2)}=\boldsymbol{u}_j^{(2)}G_2=\boldsymbol{g}_y$ となる．ここで式 (24) より $y\in X_{F(J(x))}$ であるから，式 (25) の定義より $w_H(\boldsymbol{g}_y)-1\geq Z(x)$ が成り立つ．したがって $\boldsymbol{c}_B=\boldsymbol{u}G_B^*$ について式 (5) より

$$w_H(\boldsymbol{c}_B)=w_H(\boldsymbol{c}_i^{(1)})+w_H(\boldsymbol{c}_j^{(2)})-1$$
$$\geq w_H(\boldsymbol{g}_x)+Z(x), \tag{27}$$

である．$u_{i,x}^{(1)}=1$ の i,x は任意として式 (27) は成り立つので，補題が成り立つ． □

前章の議論より，$D_1\geq 2d_1-1$ とできることは明らかである．そこである正定数 $D_1(\geq 2d_1-1)$ に対し式 (26) を満足するような X_i, $F(i)$, $i\in[1,M]$, の一つを求めるアルゴリズムを以下に示す．

［探索アルゴリズム 1］
（初期化）
(1) $i=d_1-1, d_1, \cdots, n_1-k_1$ に対し

$S_i := \{x \in [1,k_1] |\ w_H(\boldsymbol{g}_x) - 1 = i\}$.
$M := 0$, $z := d_1 - 1$.
(探索)
(2) (i)$z = \left\lceil \frac{D_1-1}{2} \right\rceil$ ならば (3) へ.
(ii) $S_z = \phi$ ならば $z := z+1$ として (i) へ.
(iii) もし $r_i = z, i \in [1,M]$, なる i 及び r_i が存在するならば $m := i$.
そうでなければ $M := M+2$, $F(M-1) := M$, $F(M) := M-1$, $X_{M-1} = X_M := \phi$, $m := M-1$, $r_{M-1} := z$, $r_M := D_1 - (z+1)$.
(iv) 適当な $x \in S_z$ を選び $X_m := X_m \cup \{x\}$, $S_z := S_z \setminus \{x\}$.
$S_t \neq \phi, t \geq D_1 - w_H(\boldsymbol{g}_x)$, を満たす S_t から $l \in S_t$ を一つ選び, $X_{F(m)} := X_{F(m)} \cup \{l\}$, $S_t := S_t \setminus \{l\}$. (ii) へ.
もしそのような S_t が存在しなければアルゴリズムは失敗として終了.
(3) $B := \left\{ z \geq \left\lceil \frac{D_1-1}{2} \right\rceil | S_z \neq \phi \right\}$ とし, もし $B \neq \phi$ ならば $M := M+1$, $X_M := \bigcup_{z \in B} S_z$, $F(M) := M$.
(4) $X_i, F(i), i \in [1,M]$, を出力して終了. □
この探索アルゴリズム 1 に対して次の定理が成り立つ.

[定理 7] 正定数 D_1 に対し, すべての $z \in [d_1 - 1, n_1 - k_1]$ について

$$\sum_{i=d_1-1}^{z} A_{1,i}^{C_1} \leq \sum_{i=D_1-z-1}^{n_1-k_1} A_{1,i}^{C_1}, \tag{28}$$

が成り立つならば式 (26) を満足する X_i, $F(i)$, $i \in [1,M]$, が存在し, 探索アルゴリズム 1 によりその一つが得られる.
逆に式 (28) が成り立たない z が存在するならば, 式 (26) を満足する $X_i, F(i), i \in [1,M]$, は存在しない.
(証明) 付録 **4.** 参照. □

この定理より式 (28) を満たす最大の D_1 をあらかじめ求め, その D_1 について探索アルゴリズム 1 を行うことにより補題 6 を満たす最大の D_1 と $X_i, F(i)$, $i \in [1,M]$, が得られる.

4.2 情報重み 2 に対するインタリーバ構成法

次に情報 $\boldsymbol{u}$ の重みが 2 の場合に, 符号語の最小重みを大きくする方針を述べる. 置換前のある情報ブロックの要素 x, y にそれぞれ 1 がある場合, このブロックを G_1 で符号化すると $\boldsymbol{g}_x + \boldsymbol{g}_y$ となる. またこれらの情報記号を置換したブロック内の位置をそれぞれ x', y' とするとこれらは別のブロックに置換され, それぞれの符号語は $\boldsymbol{g}_{x'}, \boldsymbol{g}_{y'}$ となる. そこでもし $\boldsymbol{g}_x + \boldsymbol{g}_y$ の検査重みが小さいときは, $\boldsymbol{g}_{x'}$ 及び $\boldsymbol{g}_{y'}$ の検査重みが大きくなるように $X_i, X_{F(i)}$ を作成する.
ここで $D_2^{C_B^*}$ の下界に関して次の補題が成り立つ.

[補題 7] 与えられた X_i, $F(i)$, $i \in [1,M]$, に対し式 (3), (24) を満足するように置換行列に制限を加え, また D_1 は式 (26) を満たすとする. このとき, 次式を満足する定数 $D_2, 2D_1 \geq D_2$, が存在するならば $D_2^{C_B^*} \geq D_2$ が成り立つ.

$$\min_{1 \leq x < y \leq k_1} \{Z(x) + Z(y) + w_H(\boldsymbol{g}_x + \boldsymbol{g}_y)\} \geq D_2, \tag{29}$$

(証明) 付録 **5.** 参照. □

次に符号 $C_1 (= C_2)$ がある D_1 に対し式 (28) を満足しているとき, 与えられた D_2 について式 (29) を満足するような集合 X, $F(i), i \in [1,M]$, の一つを求めるアルゴリズムを以下に示す. ただし集合 A, B に対し $A \setminus (A \cap B)$ を簡単に $A \setminus B$ と表す.

[探索アルゴリズム 2]
(初期化)
(1) $x = 1, 2, \cdots, k_1$ に対し
$T_x := \min_j \{j \geq D_1 - w_H(\boldsymbol{g}_x) | A_{1,j}^{C_1} > 0\}$.
(2) $j = d_1 - 1, d_1, \cdots, n_1 - k_1$ に対し
$S_j := \{x \in [1,k_1] |\ w_H(\boldsymbol{g}_x) - 1 = j\}$.
(3) $L := \left\{ \{x,y\} | T_x + T_y + w_H(\boldsymbol{g}_x + \boldsymbol{g}_y) < D_2, 1 \leq x < y \leq k_1 \right\}$, $E := \phi$, $M := 0$.
(探索)
(4) もし $L = \phi$ ならば (12) へ.
(5) $x = 1, 2, \cdots, k_1$ に対し $L_x := \{\{x,y\} \in L\}$.
(6) $Y := \{x \in [1,k_1] | L_x \neq \phi\}$.
(7) もし任意の $x, y \in E$, に対し, ある $\{x,y\} \in L$ が存在するならば探索失敗として終了.
(8) $x^* := \arg \max_{x \in Y \setminus E} |L_x|$,
$\zeta := \max_{y | \{x^*, y\} \in L_{x^*}} \{D_2 - T_y - w_H(\boldsymbol{g}_y + \boldsymbol{g}_{x^*})\}$,
$z^* := \min\{z \geq \zeta | S_z \setminus Y \neq \phi\}$.
もし z^* が存在しないならば $E := E \cup \{x^*\}$ とし, (7) へ.
(9) $j = d_1 - 1, d_1, \cdots, n_1 - k_1$ に対し $s_j := |S_j|$ とおく. 更に $s_{z^*} := s_{z^*} - 1$, $s_{w_H(\boldsymbol{g}_{x^*})-1} := s_{w_H(\boldsymbol{g}_{x^*})-1} - 1$ と更新する.

もし次式を満足するならば (10) へ．そうでなければ $E := E \cup \{x^*\}$ とし，(7) へ．

$$\sum_{i=d_1-1}^{j} s_i \leq \sum_{i=D_1-j-1}^{n_1-k_1} s_i,\ \forall j \in [d_1-1, n_1-k_1], \tag{30}$$

(10) もし $r_j = z^*, j \in [1, M]$, なる j 及び r_j が存在するならば $m := j$.

そうでなければ $M := M+2$, $F(M-1) := M$, $F(M) := M-1$, $X_{M-1} = X_M := \phi$, $m := M-1$, $r_{M-1} := z^*$, $r_M := D_1 - (z^*+1)$.

(11) 適当な $x \in S_{z^*} \setminus Y$ を選択し $X_m := X_m \cup \{x\}$, $S_{z^*} := S_{z^*} \setminus \{x\}$, $X_{F(m)} := X_{F(m)} \cup \{x^*\}$, $S_{w_H(\boldsymbol{g}_{x^*})-1} := S_{w_H(\boldsymbol{g}_{x^*})-1} \setminus \{x^*\}$, $L := L \setminus L_{x^*}$. (4) へ．

(12) $z := d_1 - 1$ とし，探索アルゴリズム 1 の探索（ステップ (2)，(3)，(4)）を行い終了． □

この探索アルゴリズム 2 に対し次の定理が成り立つ．

［定理 8］ 与えられた D_1, D_2 に対し探索アルゴリズム 2 を実行した結果 X_i ,$F(i)$, $i \in [1, M]$, が得られるならば，これらは式 (26)，(29) を満足する．
(証明) 付録 **6.** 参照． □

以上より，与えられた符号 C_1 と生成行列 G_1 に対し，式 (28) を満たす最大の D_1 を求め，また D_2 を $H(2) = 3d_1 - 2$ から始めて探索アルゴリズム 2 を適用し，X_i, $F(i)$, $i \in [1, M]$ が得られるたびに D_2 を上昇させることを繰り返し，探索アルゴリズム 2 が失敗するまで続ける．結果的に得られた X_i ,$F(i)$, $i \in [1, M]$, に対して式 (3)，(24) の制約を満たすインタリーバ（置換行列）を生成する．このとき定理 7，8 より低重み情報記号に対する符号語重みの下界を大きくするインタリーバの構成が得られる．

探索アルゴリズム 2 を行う際，最も計算量を要するのはステップ (3) において $\forall x, y \in [1, k_1], x \neq y$, に対し $w_H(\boldsymbol{g}_x + \boldsymbol{g}_y)$ を求める作業である．これは $O((n_1-k_1)k_1^2)$ の計算量である．しかし同一の C_1 に対し D_2 を変えて探索アルゴリズム 2 を複数回行う場合も，この作業は 1 回のみ行えばよい．したがって結果的に探索アルゴリズム 2 は高速である．

5. 最小距離の最大化

5.1 要素符号の探索アルゴリズム

本節では C_B^* を構成するとき，最小距離が大きくなる要素符号 $C_1 (= C_2)$ を見つけることを考える．そのために任意のブロック符号 C の生成行列を列置換した符号を $R_{\max}$ 回生成し，定理 7 及び探索アルゴリズム 2 を繰り返し用いることにより，補題 6,7 を満足するなるべく大きな D_1 及び D_2 をもつ C_B^* の構成を求めるアルゴリズムを以下に示す．

［生成行列生成アルゴリズム］

(1) (n_1, k_1, d_1) 符号 C に対する生成行列 G を求め，$D_1^* := 0$, $D_2^* := 0$, $repeat := 0$ とする．

(2) $repeat = R_{\max}$ ならば G_1^*, X_i^*, $F^*(i)$, $i \in [1, M^*]$, D_1^*, D_2^* を出力して終了．

(3) G の列をランダムに置換した行列を作成し，更にその行列のはじめの k_1 列を線形独立となるように列置換する．またこの行列に対しはじめの k_1 列が単位行列となるように行基本操作を施し，これを G_1 とする．またこの符号を C_1 とする(注3)．

(4) G_1 より $A_{1,i}^{C_1}$ を求め，定理 7 を用いて最大の D_1 を求める．$D_1 \geq D_1^*$ ならば (5) へ．そうでなければ $repeat := repeat + 1$ として (2) へ．

(5) 探索アルゴリズム 2 を繰り返し用いて最大の D_2 とそのときの X_i, $F(i)$, $i \in [1, M]$ を求める．

(6) $D_1 > D_1^*$ あるいは $D_2 > D_2^*$ ならば $G_1^* := G_1$, $M^* := M$, $X_i^* := X_i$, $F^*(i) := F(i)$, $i \in [1, M]$, $D_1^* := D_1$, $D_2^* := D_2$ とする．$repeat := repeat + 1$ として (2) へ． □

上のアルゴリズムで C に $n_1 = 2^m - 1, m \in [4, 7]$, $d_1 = 5$ を満たす (n_1, k_1, d_1) 原始 BCH 符号を用いたときの結果を表 1 に示す．ただし $R_{\max} = 10^6$ とした．アルゴリズムで得られた生成行列を $G_1^* = [I_{k_1}, Q_1^*]$ と表し，更に Q_1^* の各行を $\boldsymbol{q}_i^* \in \{0,1\}^{n_1-k_1}, i \in [1, k_1]$, と表す．表 1 にはこの $\boldsymbol{q}_i^* \in \{0,1\}^{n_1-k_1}$ を下位から 3 ビットごとに区切り，8 進数として表示している．例えば表 1 の (15, 7) 符号における $\boldsymbol{q}_1^* = (0,1,0,1,0,1,1,1)$ は 127 と表記する．

表 1 から，符号長 n_1 が増加するに従い D_1 及び D_2 を大きくすることが可能であることが分かる．これは d_1 一定のもとで符号長が増加すると $n_1 - k_1$ も増加するため，$A_{1,i}^{C_1} > 0$ なる i が $d_1 - 1$ から $n_1 - k_1$ の間に広く分布する傾向があるからである．

ここでブロックターボ符号 C_B^* の最小距離に関する定理を以下に示す．

(注3)：C_1 は C と同値な符号であるから，基本的に同一の復号法を用いることが可能である．

表 1　D_1 及び D_2 が大きな $(n_1 = 2^m - 1, k_1, d_1 = 5)$ BCH 符号の生成行列 G_1^* の例
Table 1　Generator matrix examples with large D_1 and D_2 for $(n_1 = 2^m - 1, k_1, d_1 = 5)$ BCH codes.

(n_1, k_1)	D_1	D_2	Q_1^* の各行 $\boldsymbol{q}_i^*, i \in [1, k_1]$，（8 進数表示）
(15,7)	10	14	127,074,057,352,266,225,162
(31,21)	13	14	0773,1535,1766,0075,1315,1716,1267,1770,1443,1557,1341,1623,0524,1405,0567,1454,0635,1651,1106,0607,1037
(63,51)	15	16	2151,6165,0275,6267,1721,7373,4273,3407,5511,3625,1633,3715,7471,3544,2745,1364,6462,7703,7345,7366,1263,1461,5354,3162,7041,6143,7734,5457,7533,5516,5574,3577,6777,5771,7032,0770,4530,6527,5732,3327,2626,3752,7550,3466,6721,1072,0766,1757,7124,1335,2137
(127,113)	16	16	03650,03154,32370,26077,07071,07673,03227,14752,07563,21166,05316,15636,11647,12361,24570,27605,05037,30474,23273,10633,23744,16105,26774,26355,03766,33141,01142,00374,27416,02350,32057,37153,22356,33646,27211,26635,33634,23330,05577,02037,06236,05622,21703,16534,05531,17056,23561,36433,31052,35751,02772,23427,32237,37454,33733,00453,12630,36614,16741,13176,06366,36273,00216,01326,07160,31276,27727,17217,27103,25333,12112,32672,37323,10455,25655,26034,14661,24314,20652,27336,35245,13345,34070,37354,33431,32547,34236,17760,20223,27460,24720,05054,13006,36352,36224,31125,24676,06223,20071,27447,31615,14315,05502,27346,35660,37477,17704,12677,13252,35765,06713,16337,30706

［定理 9］ 式 (3)，(24) を満足するインタリーバ（置換行列）を用いて構成した C_B^* の最小距離 D_B^* について

$$D_B^* \geq \min\{D_1, D_2, H(3)\}, \tag{31}$$

が成り立つ．
（証明） 補題 6 より $D_1^{C_B^*} \geq D_1$，補題 7 より $D_2^{C_B^*} \geq D_2$，定理 6 より $w \geq 3$ に対し $D_w^{C_B^*} \geq H(3)$ が成り立つ．明らかに $D_B^* = \min_{w>0} D_w^{C_B^*}$ であるから定理が成り立つ． □

$d_1 = 5$ の場合 $H(3) = 16$ であるから，表 1 の符号を要素符号としたブロックターボ符号 C_B^* では $D_B^* \geq D_1$ となる．また定理 6 から明らかなとおり，$H(3) = 4d_1 - 4$ は d_1 が増加するに従い線形に増加する．このとき定理 9 より最小距離は D_1 あるいは D_2 に大きく依存する．したがって本節で述べた生成行列生成アルゴリズムは C_B^* を設計する上で重要な役割を演ずる．

5.2　他のインタリーバとの比較

次に提案インタリーバ構成法と他のインタリーバとの比較を行う．ここではランダムインタリーバ及び式 (3) の制約のみをもつインタリーバを対象とする(注4)．要素符号は表 1 と同じ $n_1 = 2^m - 1, m \in [4, 7]$, $d_1 = 5$ を満たす (n_1, k_1, d_1) 原始 BCH 符号を用いる．また BCH 符号を列置換及び行基本操作した要素符号 C_1 を 10^3 個用い，更にそれぞれについて 10^3 回インタリーバを構成する(注5)．ランダムインタリーバを用いた符号 C_B 及び式 (3) の制約のみをもつ符号 C_B^* それぞれについて，情報重み $w = 1, 2$ に対応する符号語を発生させ，$D_w^{C_B}, D_w^{C_B^*}, w = 1, 2,$ を求めた結果をそれぞれ表 2，表 3 に示す．表中 $N_{C_B}, N_{C_B^*}$ はそれぞれ $D_w^{C_B}, D_w^{C_B^*}, w = 1, 2,$ の値をもつ符号 C_B, C_B^* の数を表す．なお情報重み $w = 1, 2$ に対応するすべての符号語に対して符号語重みを求めるのは計算量がかかるため，符号語重みの下界と一致した符号語が見つかった時点でその符号の探索は終了させて求めた．それでもなおランダムインタリーバに対して要素符号を (127,113) 符号とした場合は多くの計算量を必要とするため，インタリーバの構成回数を 10^2 回とした．

表 2 の結果を見ると，ランダムインタリーバでは $D_1^{C_B} > D_2^{C_B}$ となる場合が多い．これは情報重みが 2 の場合に，置換前の同一ブロック中の情報記号が，置換後にやはり同一ブロックへ置換されることにより小さな符号語重みが発生しているためである．これに対し，情報重みが 2 の場合について表 3 の結果は表 2 よりもかなり改善されている．また表 3 から，定理 6 の $D_1^{C_B^*}, D_2^{C_B^*}$ の下界 $H(1) = 9, H(2) = 13$ よりも若干大きな値をもつ符号 C_B^* が得られていることが分かる．ただし，そのような符号が得られる確率はさほど高くない．なお，表 2，表 3 の要素符号が (63,51), (127,113) 符号の場合において，$D_1^{C_B} = D_1^{C_B^*} = 11$ となる符号が数多く得られている．これはある要素符号 C_1 において，情報重み 1 に対する符号語重みの最

(注4)：**3.3** で述べたように，式 (3) の制約は式 (21)，(22) の制約をもつ S-ランダムインタリーバよりも制約が若干緩い．したがって式 (22) の制約をもつ S-ランダムインタリーバもこの中に含まれる．
(注5)：後述する理由のためランダムインタリーバに対する (127,113) 符号についてのみインタリーバの構成回数は 10^2 回とする．

表 2 ランダムインタリーバに対する $D_1^{C_B}, D_2^{C_B}$ の分布

Table 2 A distribution of $D_1^{C_B}$ and $D_2^{C_B}$ for C_B with the random interleaver.

(n_1, k_1)	$D_1^{C_B}$	$D_2^{C_B}$	N_{C_B}
(15,7)	9	8	829171
	9	9	144870
	9	10	25441
	9	11	8
	10	8	493
	10	9	17
(31,21)	9	8	958254
	9	9	40519
	10	8	1225
	10	9	2
(63,51)	9	8	982922
	9	9	15908
	10	8	168
	10	9	2
	11	8	999
	11	9	1
(127,113)	9	8	96191
	9	9	3699
	10	8	10
	11	8	99
	11	9	1

表 3 式 (3) の制約をもつインタリーバに対する $D_1^{C_B^*}, D_2^{C_B^*}$ の分布

Table 3 A distribution of $D_1^{C_B^*}$ and $D_2^{C_B^*}$ for C_B^* with the interleaver constrained by Eq. (3).

(n_1, k_1)	$D_1^{C_B^*}$	$D_2^{C_B^*}$	$N_{C_B^*}$
(15,7)	9	13	975508
	9	14	24003
	10	13	489
(31,21)	9	13	998727
	9	14	49
	10	13	1194
	10	14	30
(63,51)	9	13	998842
	10	13	158
	11	15	1000
(127,113)	9	13	998881
	10	13	119
	11	15	1000

小値が 6（すなわち $D_1^{C_1} = 6$）であったときに起こっている．この要素符号を用いたときは，すべてのインタリーバに対して $D_1^{C_B} = D_1^{C_B^*} \geq 11$ 及び $D_2^{C_B^*} \geq 15$ となる．そこでこの要素符号に対してのみインタリーバ構成回数を 10^4 回に増やしてみたが，表 2，表 3 よりも大きな値をもつ符号を得ることはできなかった．

さて表 1 と表 3 の結果を比較すると，表 1 の方が大きな値をとっていることが分かる．表 3 の分布から，要素符号及びインタリーバの構成回数を大きくしても，式 (3) の制約のみでは表 1 と同じ最小距離をもつ符号を構成することが困難であることは想像にかたくない(注6)．またその場合，インタリーバを構成するたびに $D_1^{C_B^*}, D_2^{C_B^*}$ を求める必要があるため，多くの計算量を必要とする．以上の結果を踏まえると，**4.** で提案したインタリーバの構成法及び本節で示した要素符号 C_1 の生成手法は有効であると考えられる．

5.3 PCBC の構成

最後に，提案インタリーバを用いた PCBC の構成について考える．まず PCBC の符号長は $l_1 n_1 + l_2(n_2 - k_2)$，情報記号数は $k_1 l_1$ である．また要素符号を $C_1 = C_2$ として C_1 の符号化率を $r = k_1/n_1$ と表すと，PCBC の符号化率 R_B はすぐ分かるように $R_B = r/(2-r)$ となる．すなわち PCBC の符号化率は l_1, l_2 に依存しない．また **4.** で提案した探索アルゴリズム 1, 2 は明らかに要素符号にのみ依存し，やはり l_1, l_2 に依存しない．すなわち最小距離のタイトな下界も残念ながら l_1, l_2 に依存しない(注7)．この事実は，要素符号を決めたときに PCBC のインタリーバサイズを十分に大きくしても，復号誤り確率の減少分がさほど増えないという論文 [9] の結果と符合する．したがって，実際には $l_1 \geq k_2 = k_1$ を満たす中で都合の良い情報記号数や符号長を選択すればよく，むやみに大きなインタリーバを利用する必要はない．

ただし PCBC に用いる要素符号は，上で述べてきたように PCBC の最小距離に大きな影響を与える．そこで最小距離の観点から要素符号について考えるとまず，定理 9 から $H(3)$ がある程度大きくなるように要素符号の最小距離 d_1 を選ぶ必要がある．また上で考察したように，d_1 一定のもとで符号長 n_1 を大きくした方が D_1 及び D_2 を大きくすることが可能である．ここで実際的な PCBC を考えると，ターボ復号を行うためには要素符号の MAP 復号あるいはその近似復号を繰り返し行う必要があるため，符号の種類にもよるが一般的には大きな符号長をもつブロック符号 C_1 を要素符号として選ぶことが難しい．したがって復号の計算量も含めた適切な要素符号を選択する必要がある(注8)．

(注6)：表 1 で得られている要素符号に対しても式 (3) の制約のみをもつ符号 C_B^* を 10^4 回構成してみたが，表 3 よりも大きな $D_1^{C_B^*}, D_2^{C_B^*}$ をもつ符号を得ることはできなかった．

(注7)：ただし式 (3) の制約を満足するために $l_1 \geq k_2 = k_1$ である必要がある．

(注8)：論文 [10], [11] では要素符号に (1023,1013) ハミング符号を用いている．したがって符号の種類や情報記号数にもよるが，要素符号の実用的な最大の符号長は 200〜1000 程度と思われる．

6. むすび

本論文ではS. Benedettoらの提案したブロックターボ符号の最小距離の下界を示し，更にその最小距離の下界を大きくする要素符号の探索アルゴリズム及びインタリーバの構成法を提案した．また結果的に得られるブロックターボ符号 C_B^* は従来の符号より大きな最小距離をもつことを示した．

更に例1で述べたように得られた C_B^* について，ある範囲の低域重み分布を少ない計算量で厳密に求めることが可能である．

4. で示したインタリーバの構成法は，要素符号の特性を利用してインタリーバに制約を課し，最小距離を大きくする点で，ブロックターボ符号に対するCMIに相当するものと考えることができる．ただし制約を課す方法が論文[3], [6]〜[8]で提案されている畳込みターボ符号用のCMIと異なるため，相互の関連に関しては今後の検討課題である．

5. で提案した生成行列生成アルゴリズムでは，与えられた符号の生成行列に対しランダムな列置換を施して候補符号を生成した．しかし構成的に式(28)を満足する符号を生成する手法を開発する必要がある．

本論文では最小距離が大きくなるようにブロックターボ符号のインタリーバを構成する手法について述べた．結果的に信号対雑音比（SNR）の大きな領域において，PCBCの復号誤り確率が改善されることが期待できる．しかし通信路の雑音が大きくなるに従い，復号誤り確率は最小距離だけでなく重み分布に大きな影響を受けることが知られている[2], [3], [9]．したがって今後，本論文の手法により得られたブロックターボ符号 C_B^* に対し，情報重みごとの符号語の最小重みだけでなく，重み分布を評価することが必要である．また，この重み分布まで考慮したインタリーバを構成することも今後の課題である．更に，提案したインタリーバに対する実際の復号特性並びにエラーフロアの改善の程度について，シミュレーションなどにより明らかにすることも今後の課題である．

謝辞　筆者らは非常に有益な御示唆と御指摘を頂きました査読者並びに編集委員の方々に深く感謝致します．本研究の一部は文部科学省科学研究費基盤研究C15560338及び若手研究B15760281，早稲田大学特定課題研究助成費2001A-566の助成による．

文　献

[1] C. Berrou, A. Glavieux, and P. Thitimajshima, “Near Shannon limit error-correcting coding and decoding: Turbo-codes(1),” IEEE Int. Conf. Communications ICC’93, vol.2/3, pp.1064–1071, May 1993.

[2] C. Heegard and S.B. Wicker, Turbo Coding, Kluwer Academic Publishers, 1999.

[3] B. Vucetic and J. Yuan, Turbo Codes : Principles and Applications, Kluwer Academic Publishers, 2000.

[4] J. Hagenauer, E. Offer, and L. Papke, “Iterative decoding of binary block and convolutional codes,” IEEE Trans. Inf. Theory, vol.42, no.2, pp.429–445, March 1996.

[5] S. Dolinar and D. Divsalar, “Weight distributions for turbo codes using random and nonrandom permutations,” JPL TDA Progr. Rep., 42-122, pp.56–65, Aug. 1995.

[6] J. Yuan, B. Vucetic, and W. Feng, “Combined turbo codes and interleaver design,” IEEE Trans. Commun., vol.47, no.4, pp.484–487, April 1999.

[7] W. Feng, J. Yuan, and B. Vucetic, “A code-matched interleaver design for turbo codes,” IEEE Trans. Commun., vol.50, no.6, pp.926–937, June 2002.

[8] H. Ogiwara and M. Kasawa, “Performance evaluation of turbo codes with code-matched interleaver over inter-symbol interference channel,” IEICE Trans. Fundamentals, vol.E85-A, no.10, pp.2203–2210, Oct. 2002.

[9] S. Benedetto and G. Montorsi, “Unveiling turbo codes: Some results on parallel concatenated coding schemes,” IEEE Trans. Inf. Theory, vol.42, no.2, pp.409–428, March 1996.

[10] J. Hagenauer, F. Burkert, and H. Nickl, “The race to Shannon’s limit: Discipline high-rate codes,” Proc., Int. Symp. on Turbo Codes and Related Topics, pp.239–242, Brest, France, Sept. 1997.

[11] H. Nickl, J. Hagenauer, and F. Burkert, “Approaching Shannon’s capacity limit by 0.27 dB using Hamming codes in a ‘turbo’ – decoding scheme,” Proc., IEEE Int. Symp. on Inform. Theory, p.12, Ulm, Germany, June 1997.

[12] R.M. Pyndiah, “Near-optimum decoding of product codes: Block turbo codes,” IEEE Trans. Commun., vol.46, no.8, pp.1003–1010, Aug. 1998.

[13] A. Sella and Y. Be’ery, “Convergence analysis of turbo decoding of product codes,” IEEE Trans. Inf. Theory, vol.47, no.2, pp.723–735, Feb. 2001.

[14] 小林　学，松嶋敏泰，平澤茂一，“ブロックターボ符号の生成行列と性能評価,” 信学技報，IT2001-11, July 2001.

[15] 小林　学，松嶋敏泰，平澤茂一，“ブロックターボ符号に対するインタリーバの構成法と最小距離,” 第24回情報理論とその応用シンポジウム予稿集，pp.95–98, Dec. 2001.

付　録

1. 定理4の証明

$f(i) = d_2\frac{w}{i} + d_1 i - w$ とおくと $f'(i) = -\frac{d_2 w}{i^2} + d_1 =$

0 より $i=\sqrt{\frac{d_2 w}{d_1}}$ のとき $f(i)$ は最小値をとる．$d_1=d_2$ より $W(i,w)$ は $i=\lceil\sqrt{w}\,\rceil$ あるいは $\lceil\sqrt{w}\,\rceil-1$ のとき最小となる．以下では場合分けをして証明する．

(1) $(\lceil\sqrt{w}\,\rceil-1)\lceil\sqrt{w}\,\rceil\geq w$ のとき
(1-i) $i=\lceil\sqrt{w}\,\rceil$ のとき

$$W(\lceil\sqrt{w}\,\rceil,w)=d_2\left\lceil\frac{w}{\lceil\sqrt{w}\,\rceil}\right\rceil+d_1\lceil\sqrt{w}\,\rceil-w, \tag{A·1}$$

について考える．まず $\lceil\sqrt{w}\,\rceil-2<\frac{w}{\lceil\sqrt{w}\,\rceil}$ を示す．これは

$$\begin{aligned}&w-(\lceil\sqrt{w}\,\rceil-2)\lceil\sqrt{w}\,\rceil\\&=(\sqrt{w}+\lceil\sqrt{w}\,\rceil)(\sqrt{w}-\lceil\sqrt{w}\,\rceil)+2\lceil\sqrt{w}\,\rceil\\&>0,\end{aligned} \tag{A·2}$$

と等価だが，$(\sqrt{w}+\lceil\sqrt{w}\,\rceil)\leq 2\lceil\sqrt{w}\,\rceil$ であり，かつ $-1<\sqrt{w}-\lceil\sqrt{w}\,\rceil\leq 0$ であるので式 (A·2) は成り立つ．
また (1) の仮定より $(\lceil\sqrt{w}\,\rceil-1)\lceil\sqrt{w}\,\rceil\geq w$ であるから $\frac{w}{\lceil\sqrt{w}\,\rceil}\leq\lceil\sqrt{w}\,\rceil-1$ が成り立つ．結局 $\lceil\sqrt{w}\,\rceil-2<\frac{w}{\lceil\sqrt{w}\,\rceil}\leq\lceil\sqrt{w}\,\rceil-1$ より $\left\lceil\frac{w}{\lceil\sqrt{w}\,\rceil}\right\rceil=\lceil\sqrt{w}\,\rceil-1$ である．したがって $W(\lceil\sqrt{w}\,\rceil,w)=(2\lceil\sqrt{w}\,\rceil-1)d_1-w$ となる．

(1-ii) $i=\lceil\sqrt{w}\,\rceil-1$ のとき
(1-i) と同様 $W(\lceil\sqrt{w}\,\rceil-1,w)$ について考える．$\frac{w}{\lceil\sqrt{w}\,\rceil-1}$ に対して

$$\begin{aligned}&w-(\lceil\sqrt{w}\,\rceil-1)^2\\&\quad=(\sqrt{w}+\lceil\sqrt{w}\,\rceil-1)(\sqrt{w}-\lceil\sqrt{w}\,\rceil+1)\\&\quad>0,\end{aligned} \tag{A·3}$$

であるから $\lceil\sqrt{w}\,\rceil-1<\frac{w}{\lceil\sqrt{w}\,\rceil-1}$ が成り立つ．また仮定 $(\lceil\sqrt{w}\,\rceil-1)\lceil\sqrt{w}\,\rceil\geq w$ より $\frac{w}{\lceil\sqrt{w}\,\rceil-1}\leq\lceil\sqrt{w}\,\rceil$ が成り立つ．したがって $\left\lceil\frac{w}{\lceil\sqrt{w}\,\rceil-1}\right\rceil=\lceil\sqrt{w}\,\rceil$ より $W(\lceil\sqrt{w}\,\rceil-1,w)=(2\lceil\sqrt{w}\,\rceil-1)d_1-w$ である．

(2) $(\lceil\sqrt{w}\,\rceil-1)\lceil\sqrt{w}\,\rceil<w$ のとき
(2-i) $i=\lceil\sqrt{w}\,\rceil$ のとき
仮定 $(\lceil\sqrt{w}\,\rceil-1)\lceil\sqrt{w}\,\rceil<w$ より $\lceil\sqrt{w}\,\rceil-1<\frac{w}{\lceil\sqrt{w}\,\rceil}$ でかつ $\frac{w}{\lceil\sqrt{w}\,\rceil}\leq\sqrt{w}$ であるから $\left\lceil\frac{w}{\lceil\sqrt{w}\,\rceil}\right\rceil=\lceil\sqrt{w}\,\rceil$ となる．したがって $W(\lceil\sqrt{w}\,\rceil,w)=2\lceil\sqrt{w}\,\rceil d_1-w$ である．
(2-ii) $i=\lceil\sqrt{w}\,\rceil-1$ のとき
仮定より $\lceil\sqrt{w}\,\rceil<\frac{w}{\lceil\sqrt{w}\,\rceil-1}$ が成り立ち，$\lceil\sqrt{w}\,\rceil$ は整数であるから $\left\lceil\frac{w}{\lceil\sqrt{w}\,\rceil-1}\right\rceil\geq\lceil\sqrt{w}\,\rceil+1$ である．したがって $W(\lceil\sqrt{w}\,\rceil-1,w)\geq 2\lceil\sqrt{w}\,\rceil d_1-w$ となる．

以上より定理が成り立つ．

2. 定理 5 の証明

$T=d_1+d_2$ を偶数の定数とし，定理 4 の証明と同様場合分けを行う．それぞれの場合に対し $d_1\neq d_2$ を仮定したとき $W_{(d_1,d_2)}(w)=\min_{i'\in[1,w]}W_{(d_1,d_2)}(i',w)\leq W_{(T/2,T/2)}(w)$ となることを示す．

(1) $(\lceil\sqrt{w}\,\rceil-1)\lceil\sqrt{w}\,\rceil\geq w$ のとき
$W_{(d_1,d_2)}(i,w)$ について $i=\lceil\sqrt{w}\,\rceil$ のとき $\left\lceil\frac{w}{\lceil\sqrt{w}\,\rceil}\right\rceil=\lceil\sqrt{w}\,\rceil-1$ より $W_{(d_1,d_2)}(i,w)=T\lceil\sqrt{w}\,\rceil-d_2-w$ となる．また $i=\lceil\sqrt{w}\,\rceil-1$ のときは $\left\lceil\frac{w}{\lceil\sqrt{w}\,\rceil-1}\right\rceil=\lceil\sqrt{w}\,\rceil$ より $W_{(d_1,d_2)}(i,w)=T\lceil\sqrt{w}\,\rceil-d_1-w$ である．ここで $d_1\neq d_2$ を仮定し $d_{max}=\max\{d_1,d_2\}$ とおくと定理 4 より

$$\begin{aligned}&\min_{i'\in[1,w]}W_{(d_1,d_2)}(i',w)\leq T\lceil\sqrt{w}\,\rceil-d_{max}-w\\&<T\lceil\sqrt{w}\,\rceil-\frac{T}{2}-w=W_{(T/2,T/2)}(w),\end{aligned} \tag{A·4}$$

となり，厳密に $d_1=d_2=\frac{T}{2}$ のときに $W_{(d_1,d_2)}(w)$ が最大となる．

(2) $(\lceil\sqrt{w}\,\rceil-1)\lceil\sqrt{w}\,\rceil<w\leq\lceil\sqrt{w}\,\rceil^2-1$ のとき
$W_{(d_1,d_2)}(i,w)$ について $i=\lceil\sqrt{w}\,\rceil-1$ のとき w の仮定より $\lceil\sqrt{w}\,\rceil<\frac{w}{\lceil\sqrt{w}\,\rceil-1}\leq\lceil\sqrt{w}\,\rceil+1$ であるから $\left\lceil\frac{w}{\lceil\sqrt{w}\,\rceil-1}\right\rceil=\lceil\sqrt{w}\,\rceil+1$ である．したがって

$$\begin{aligned}&W_{(d_1,d_2)}(\lceil\sqrt{w}\,\rceil-1,w)\\&\qquad=T\lceil\sqrt{w}\,\rceil+d_2-d_1-w,\end{aligned} \tag{A·5}$$

となる．
また $i=\lceil\sqrt{w}\,\rceil+1$ のとき (2) の仮定より $\frac{w}{\lceil\sqrt{w}\,\rceil+1}\leq\lceil\sqrt{w}\,\rceil-1$ である．次に $\lceil\sqrt{w}\,\rceil-2<\frac{w}{\lceil\sqrt{w}\,\rceil+1}$ を示す．これは $(\lceil\sqrt{w}\,\rceil-2)(\lceil\sqrt{w}\,\rceil+1)=(\lceil\sqrt{w}\,\rceil-1)\lceil\sqrt{w}\,\rceil-2<w$ と等価だが，(2) の仮定より明らかに成り立つ．以上より $\left\lceil\frac{w}{\lceil\sqrt{w}\,\rceil+1}\right\rceil=$

$\lceil\sqrt{w}\,\rceil-1$ である．したがって

$$W_{(d_1,d_2)}(\lceil\sqrt{w}\,\rceil+1,w) = T\lceil\sqrt{w}\,\rceil-d_2+d_1-w, \quad \text{(A·6)}$$

となる．結局定理 4，式 (A·5)，(A·6) より $d_1\neq d_2$ のとき

$$\min_{i'\in[1,w]} W_{(d_1,d_2)}(i',w) \le T\lceil\sqrt{w}\,\rceil-|d_2-d_1|-w < T\lceil\sqrt{w}\,\rceil-w = W_{(T/2,T/2)}(w), \quad \text{(A·7)}$$

が成り立つ．したがって厳密に $d_1=d_2=\frac{T}{2}$ のときに $W_{(d_1,d_2)}(w)$ が最大となる．

(3)　$w=\lceil\sqrt{w}\,\rceil^2$ のとき

$$\min_{i'\in[1,w]} W_{(d_1,d_2)}(i',w) \le W_{(d_1,d_2)}(\sqrt{w},w) = W_{(T/2,T/2)}(w) = T\sqrt{w}-w, \quad \text{(A·8)}$$

が成り立つ．

以上より定理が成り立つ．

3. 補題 5 の証明

$U(w)=U(w')$ のときは明らかであるから $U(w)<U(w')$ を仮定する．まず

$$V(w) = \begin{cases} 2\lceil\sqrt{w}\,\rceil-1, & \text{if } (\lceil\sqrt{w}\,\rceil-1)\lceil\sqrt{w}\,\rceil\ge w,\\ 2\lceil\sqrt{w}\,\rceil, & \text{otherwise,}\end{cases} \quad \text{(A·9)}$$

と定義する．ここで $U(w),V(w)$ について次の性質が成り立つ．

(i)　$U(w)=\lceil\sqrt{w}\,\rceil^2$ のとき
明らかに $\sqrt{U(w)}=\lceil\sqrt{U(w)}\rceil=\lceil\sqrt{w}\,\rceil$ である．したがって定義より $V(w)=2\lceil\sqrt{U(w)}\rceil$ である．

(ii)　$U(w)=\lceil\sqrt{w}\,\rceil(\lceil\sqrt{w}\,\rceil-1)$ のとき
補題 4 より $\lceil\sqrt{U(w)}\rceil=\lceil\sqrt{w}\,\rceil$ であるから $U(w)=\lceil\sqrt{U(w)}\rceil(\lceil\sqrt{U(w)}\rceil-1)$，$V(w)=2\lceil\sqrt{U(w)}\rceil-1$ である．

この性質と定理 4 と補題の条件 $w<w'\le d_1^2$ より

$$\begin{aligned} &W(U(w'))-W(U(w))\\ &=d_1\{V(w')-V(w)\}-\{U(w')-U(w)\}\\ &\ge\lceil\sqrt{U(w')}\rceil\{V(w')-V(w)\}-\{U(w')-U(w)\},\end{aligned} \quad \text{(A·10)}$$

が成り立つ．次に場合分けにより式 (A·10) の最右辺が非負であることを示す．

(1)　$U(w)=\lceil\sqrt{w}\,\rceil^2$ のとき
$U(w')=\lceil\sqrt{w'}\rceil^2$ あるいは $\lceil\sqrt{w'}\rceil(\lceil\sqrt{w'}\rceil-1)$ の場合の双方にそれぞれ上の (i)，(ii) の性質を用いて計算すると

式 (A·10) の最右辺

$$=\left\{\lceil\sqrt{U(w')}\rceil-\lceil\sqrt{U(w)}\rceil\right\}^2\ge 0, \quad \text{(A·11)}$$

が成り立つ．

(2)　$U(w)=\lceil\sqrt{w}\,\rceil(\lceil\sqrt{w}\,\rceil-1)$ のとき
同様に $U(w')=\lceil\sqrt{w'}\rceil^2$ あるいは $\lceil\sqrt{w'}\rceil(\lceil\sqrt{w'}\rceil-1)$ の場合の双方ともに

$$\text{式 (A·10) の最右辺}=\left\{\lceil\sqrt{U(w')}\rceil-\lceil\sqrt{U(w)}\rceil\right\}^2+\left\{\lceil\sqrt{U(w')}\rceil-\lceil\sqrt{U(w)}\rceil\right\}\ge 0, \quad \text{(A·12)}$$

が成り立つ．

以上より補題が示された．

4. 定理 7 の証明

まずすべての z に対して式 (28) が成り立つ場合を考える．探索アルゴリズム 1 のステップ (1) において S_i の与え方により，ステップ (1) の初期時点では $|S_i|=A_{1,i}^{C_1}$, $i\in[d_1-1,n_1-k_1]$, が成り立っている．次にステップ (iv) では $\forall z<\left\lceil\frac{D_1-1}{2}\right\rceil$ に対し $x\in S_z$ と $l\in S_t, t\ge D_1-w_H(\boldsymbol{g}_x)$, を選び，それぞれ X_m 及び $X_{F(m)}$ に含めており，$S_z:=S_z\setminus\{x\}$ 及び $S_t:=S_t\setminus\{l\}$ と更新される．ここでステップ (1) の S_z の与え方により $w_H(\boldsymbol{g}_x)-1=z$ であるから $t\ge D_1-(z+1)$ が成り立つ．仮定よりすべての z に対して式 (28) が成り立っているため，アルゴリズム中任意の $z<\left\lceil\frac{D_1-1}{2}\right\rceil$ に対するステップ (iv) において

$$\sum_{i=d_1-1}^{z}|S_i|=|S_z|\le\sum_{i=D_1-z-1}^{n_1-k_1}|S_i|, \quad \text{(A·13)}$$

が常に成り立つ．ただしステップ (ii) において $S_z=\phi$ のときに z を 1 増やしているため，式 (A·13) の左辺は $|S_z|$ となる．したがってステップ (iv) において $S_t\neq\phi, t\ge D_1-w_H(\boldsymbol{g}_x)$, を満たす S_t は必ず存在し，アルゴリズム 1 は正常に終了する．

またステップ (iii) の $r_m=z$ とステップ (iv) の S_z の関係から，ステップ (iv) で得られる X_m について $w_H(\boldsymbol{g}_x)-1=z, \forall x\in X_m$, なので任意の $l\in X_{F(m)}$ に対し

$$w_H(\boldsymbol{g}_l) - 1 \geq D_1 - (z+1) = r_{F(m)} = D_1 - w_H(\boldsymbol{g}_x), \quad \text{(A·14)}$$

である．したがって $Z(x) \geq D_1 - w_H(\boldsymbol{g}_x), x \in X_m$, が成り立つ．また逆に $l \in X_{F(m)}$ について $F(J(l)) = m$ より

$$Z(l) = \min_{j \in X_m} w_H(\boldsymbol{g}_j) - 1 = z \geq D_1 - w_H(\boldsymbol{g}_l), \quad \text{(A·15)}$$

であるから，$Z(l) + w_H(\boldsymbol{g}_l) \geq D_1$ となる．

更にステップ (3) において，もし $B \neq \phi$ ならば $z \geq \left\lceil \frac{D_1-1}{2} \right\rceil, z \in B$, であるから，最終的に $x \in X_M = \bigcup_{z \in B} S_z$ に対し $Z(x) \geq \left\lceil \frac{D_1-1}{2} \right\rceil$ である．したがって $w_H(\boldsymbol{g}_x) + Z(x) \geq 2\left\lceil \frac{D_1-1}{2} \right\rceil + 1 \geq D_1$ が成り立つ．以上よりすべての z に対し式 (28) が成り立つ場合の定理が証明された．

次にある z に対して式 (28) が成り立たない場合を考える．このとき式 (26) を満たす $X_i, F(i), i \in [1, M]$, が存在すると仮定して矛盾を示す．

まず $Y_z = \{x \in [1, k_1] | w_H(\boldsymbol{g}_x) - 1 \leq z\}$ とおくと

$$\left| \bigcup_{x \in Y_z} X_{J(x)} \right| \geq |Y_z| = \sum_{i=d_1-1}^{z} A_{1,i}^{C_1}, \quad \text{(A·16)}$$

が成り立つ．ここで定義 6，7 より

$$\left| \bigcup_{x \in Y_z} X_{J(x)} \right| = \left| \bigcup_{x \in Y_z} X_{F(J(x))} \right|, \quad \text{(A·17)}$$

である．また $X_i, F(i), i \in [1, M]$, は式 (26) を満たすと仮定しているので，$\forall x \in Y_z$ と $\forall x' \in X_{F(J(x))}$ に対し定義 7 と式 (26) より

$$w_H(\boldsymbol{g}_{x'}) - 1 \geq Z(x) \geq D_1 - w_H(\boldsymbol{g}_x) \geq D_1 - z - 1, \quad \text{(A·18)}$$

が成り立つ．これは

$$\left| \bigcup_{x \in Y_z} X_{F(J(x))} \right| \leq \sum_{i=D_1-z-1}^{n_1-k_1} A_{1,i}^{C_1}, \quad \text{(A·19)}$$

を意味するが，今 z は式 (28) を満たさないと仮定しているため

$$\left| \bigcup_{x \in Y_z} X_{J(x)} \right| \geq \sum_{i=d_1-1}^{z} A_{1,i}^{C_1} > \sum_{i=D_1-z-1}^{n_1-k_1} A_{1,i}^{C_1} \geq \left| \bigcup_{x \in Y_z} X_{F(J(x))} \right|, \quad \text{(A·20)}$$

となり式 (A·17) と矛盾する．したがってある z に対して式 (28) が成り立たないならば式 (26) を満たす $X_i, F(i), i \in [1, M]$, は存在しない．

以上より定理が示された．

5. 補題 7 の証明

$w_H(\boldsymbol{u}) = 2$ を満たす $\boldsymbol{u} = (\boldsymbol{u}_1^{(1)}, \boldsymbol{u}_2^{(1)}, \cdots, \boldsymbol{u}_{l_1}^{(1)})$ と $\boldsymbol{u}' = (\boldsymbol{u}_1^{(2)}, \boldsymbol{u}_2^{(2)}, \cdots, \boldsymbol{u}_{l_2}^{(2)}) = \boldsymbol{u}P_B$ について考える．ある $i_m, x_m, m = 1, 2,$ に対し $u_{i_m,x_m}^{(1)} = 1$ であったとし，$p_{(i_m-1)k_1+x_m,b_m} = 1$ を満たす $b_m, m = 1, 2,$ について $j_m = \lceil b_m/k_2 \rceil$ とおく．このとき補題 6 の証明と同様 $u_{i_m,x_m}^{(1)}$ は置換行列により $u_{j_m,y_m}^{(2)}$, $y_m = (b_m - 1 \bmod k_2) + 1$ へ置換される．いくつかの場合に分けて証明する．

(1) $i_1 = i_2$ のとき

このとき $\boldsymbol{c}_{i_1}^{(1)} = \boldsymbol{u}_{i_1}^{(1)} G_1 = \boldsymbol{g}_{x_1} + \boldsymbol{g}_{x_2}$ となる．また式 (3) の制限より $j_1 \neq j_2$ であるから $\boldsymbol{c}_B = \boldsymbol{u}G_B^*$ について

$$w_H(\boldsymbol{c}_B) = w_H(\boldsymbol{c}_{i_1}^{(1)}) + w_H(\boldsymbol{c}_{j_1}^{(2)}) + w_H(\boldsymbol{c}_{j_2}^{(2)}) - 2 \geq w_H(\boldsymbol{g}_{x_1} + \boldsymbol{g}_{x_2}) + Z(x_1) + Z(x_2), \quad \text{(A·21)}$$

が成り立つ．

(2) $i_1 \neq i_2$ のとき

(i) $j_1 \neq j_2$ のとき

$$w_H(\boldsymbol{c}_B) = \sum_{m=1}^{2} \Big(w_H(\boldsymbol{c}_{i_m}^{(1)}) + w_H(\boldsymbol{c}_{j_m}^{(2)}) \Big) - 2 \geq \sum_{m=1}^{2} \big(w_H(\boldsymbol{g}_{x_m}) + Z(x_m) \big) \geq 2D_1, \quad \text{(A·22)}$$

が成り立つ．

(ii) $j_1 = j_2$ のとき

$$w_H(\boldsymbol{c}_B) = w_H(\boldsymbol{c}_{i_1}^{(1)}) + w_H(\boldsymbol{c}_{i_2}^{(1)}) + w_H(\boldsymbol{c}_{j_1}^{(2)}) - 2 \geq Z(y_1) + Z(y_2) + w_H(\boldsymbol{g}_{y_1} + \boldsymbol{g}_{y_2}), \quad \text{(A·23)}$$

が成り立つ．式 (A·23) の最後の不等式は式 (3) の制限及び関数 $F(i) = F^{-1}(i), i \in [1, M]$, の性質からなる．

以上より，補題が成り立つ．

6. 定理 8 の証明

まず探索アルゴリズム 2 において得られる X_i, $F(i), i \in [1, M]$, に対し式 (26) が成立することを示す．そのためには定理 7 の証明と同様探索アルゴリズム 2 の任意の時点で，すべての $j \in [d_1 - 1, n_1 - k_1]$ に対し

$$\sum_{i=d_1-1}^{j} |S_i| \leq \sum_{i=D_1-j-1}^{n_1-k_1} |S_i|, \qquad \text{(A·24)}$$

を満足する必要がある．しかし式 (30) が成立した場合のみステップ (11) で更新を行うため，式 (A·24) は常に成り立つ．ここでステップ (8) で与えられる $x^* \in Y$ と z^* に対し，ステップ (11) で $x \in S_{z^*}$ と x^* をそれぞれ X_m 及び $X_{F(m)}$ に含めている．ステップ (5) の L_x の与え方及びステップ (8) より

$$\begin{aligned} z^* &\geq \max_{y|\{x^*,y\} \in L_{x^*}} \{D_2 - T_y - w_H(\boldsymbol{g}_y + \boldsymbol{g}_{x^*})\} \\ &> T_{x^*} \geq D_1 - w_H(\boldsymbol{g}_{x^*}), \end{aligned} \qquad \text{(A·25)}$$

であるから，ステップ (11) で得られる $\forall l \in X_{F(m)}$ について $Z(l) \geq D_1 - w_H(\boldsymbol{g}_l)$ であり，逆も成り立つため $Z(x) \geq D_1 - w_H(\boldsymbol{g}_x), \forall x \in X_m$, である．更にステップ (12) はすべての j に対し式 (A·24) が成立して行われるため，定理 7 の証明と同様，最終的に得られる X_i, $F(i), i \in [1, M]$, に対し式 (26) が成り立つ．ここでステップ (1) の T_x の与え方から，$Z(x) \geq T_x$ も成り立つことに注意されたい．

次に探索アルゴリズム 2 において得られる X_i, $F(i), i \in [1, M]$, について式 (29) が成り立つことを示す．ステップ (3) で与えられた L に対し $\forall \{x, y\} \in L$ について $Z(x) = T_x, Z(y) = T_y$ とするならば式 (29) を満足しない．そこでステップ (11) において $x \in S_{z^*}$ を X_m に含めることによって $Z(x^*) = z^*$ となる．また上で述べたように，任意の y に対し $Z(y) \geq T_y$ であるから，式 (A·25) より

$$\min_{y|\{x^*,y\} \in L_{x^*}} \{Z(x^*) + Z(y) + w_H(\boldsymbol{g}_{x^*} + \boldsymbol{g}_y)\} \geq D_2, \qquad \text{(A·26)}$$

が成り立つ．したがってステップ (11) において $L := L \setminus L_{x^*}$ と更新することができる．以上よりステップ (4) において $L = \phi$ となったとき，生成された $X_i, F(i), i \in [1, M]$, に対し式 (29) が成り立つ．

ステップ (8) において z^* が存在しないならば，式 (A·26) を保証するような $Z(x^*)$ を与えることができない．またステップ (9) においてもし式 (30) を満足しないとき，式 (A·24) の制約を保つために更新することができず，$Z(x^*) < z^*$ となってしまう．これらのとき $E := E \cup \{x^*\}$ となり，ステップ (7) において $\forall x, y \in E$ に対しある $\{x, y\} \in L$ が存在するならば

$$Z(x) + Z(y) + w_H(\boldsymbol{g}_x + \boldsymbol{g}_y) \geq D_2, \qquad \text{(A·27)}$$

を保証できないまま以降 $L = \phi$ となることはないため，アルゴリズム失敗として終了となる．

以上より定理が成り立つ．

（平成 16 年 3 月 19 日受付，17 年 5 月 31 日再受付，
10 月 3 日最終原稿受付）

小林　学　（正員）

平 6 早大・理工・工業経営卒．平 8 同大理工学研究科修士課程了．平 8 同大理工学研究科博士後期課程入学．平 14 湘南工科大学情報工学科講師，現在に至る．情報理論とその応用，並びにデータマイニングに関する研究に従事．博士（工学）．IEEE，情報理論とその応用学会，情報処理学会各会員．

松嶋　敏泰　（正員）

昭 53 早大・理工・工業経営卒．昭 55 同大大学院修士課程了．同年，日本電気（株）入社．昭 61 早大・理工学研究科・博士後期課程入学．平元横浜商科大学講師．平 3 同大助教授．平 4 早大・理工学部・工業経営学科（現在経営システム工学科）助教授．平 9 同大教授，現在に至る．知識情報処理及び情報理論とその応用に関する研究に従事．博士（工学）．IEEE，情報理論とその応用学会，人工知能学会，情報処理学会，OR 学会，日本経営工学会等各会員．

平澤　茂一　（正員：フェロー）

昭 36 早大・理工・数学卒．昭 38 同電気通信卒．同年三菱電機（株）入社．昭 56 早大・理工・工業経営学科（現在経営システム工学科）教授，現在に至る．情報理論とその応用，データ伝送方式，並びに計算機応用システムの開発などの研究に従事．工学博士．昭 54 UCLA 計算機科学科客員研究員．昭 60 ハンガリー科学アカデミー，昭 61 伊トリエステ大学客員研究員．平 5 本会小林記念特別賞，業績賞受賞．IEEE Fellow，情報理論とその応用学会，人工知能学会，情報処理学会，OR 学会，日本経営工学会等各会員．