The 24th Symposium on Information Theory
and Its Applications (SITA2001)
Kobe, Hyogo, Japan, Dec. 4 - 7, 2001

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
On the Construction of an Interleaver for Block Turbo Codes and Minimum Distance

小林 学* 松嶋 敏泰† 平澤 茂一†
Manabu KOBAYASHI Toshiyasu MATSUSHIMA Shigeichi HIRASAWA

Abstract— In 1993 C. Berrou et. al. have proposed turbo codes which achieved low BER with a SNR per information bit close to Shannon's theoretical limit on AWGN channel. H. Hagenauer et. al. also have proposed block turbo codes which consist of two systematic block codes concatenated in parallel. In this paper we show the lower bound of minimum distance by restricting an interleaver. Furthermore we propose an algorithm to construct the component codes and an interleaver which maximize its lower bound. Finary we show that the minimum distance of block turbo codes increases in comparison with conventional one.

Keywords—Block turbo codes, Minimum distance, Generator matrix, Interleaver

1 まえがき

1993 年 C.Berrou らは，AWGN 通信路に対し単位情報記号あたりの信号対雑音比 (E_b/N_0) に対する Shannon 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持つ 2 つの組織畳込み符号器を並列に連接した符号である [1]．さらに要素符号に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 [2, 4]．

本稿では H.Hagenauer らの提案したブロックターボ符号 [2] に対しインタリーバに制限を加えることにより，情報記号の重みが 1 および 2 のときのブロックターボ符号の符号語に対する Hamming 重みの下界を求める．さらにこの下界を大きくするインタリーバの構成手法を示し，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およびインタリーバを用いることにより，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 Hagenauer 型ブロックターボ符号

H.Hagenauer らにより提案されたブロックターボ符号 C_H は，2 つの要素符号の検査記号が情報記号にのみ依存し，互いの検査記号には影響を受けない構成となっている．ここでは (n_1, k_1, d_1) 組織ブロック符号 C_1 と (n_2, k_2, d_2) 組織ブロック符号 C_2 を要素符号としたときのブロックターボ符号の符号化について述べる．まず k_1k_2 シンボルの情報記号 $\boldsymbol{u}$ を k_1 シンボル毎に k_2 個のベクトルに分割する．すなわち $\boldsymbol{u} = (\boldsymbol{u}_1^{(1)}, \boldsymbol{u}_2^{(1)}, \cdots, \boldsymbol{u}_{k_2}^{(1)})$, $\boldsymbol{u}_i^{(1)} = (u_{i,1}^{(1)}, u_{i,2}^{(1)}, \cdots, u_{i,k_1}^{(1)}), i = 1, 2, \ldots, k_2$, と置く．それぞれのベクトル $\boldsymbol{u}_i^{(1)}$ を情報記号とみなし，組織符号を用いて符号化を行う．本稿では簡単のため，それぞれを同一の C_1 を用いて符号化を行うものと仮定する[1]．また C_1 の生成行列を G_1 と表すとこの符号化により $\boldsymbol{c}^{(1)} = (\boldsymbol{c}_1^{(1)}, \boldsymbol{c}_2^{(1)}, \ldots, \boldsymbol{c}_{k_2}^{(1)})$, $\boldsymbol{c}_i^{(1)} = (\boldsymbol{u}_i^{(1)}, \boldsymbol{x}_i^{(1)})$, $\boldsymbol{x}_i^{(1)} = (x_{i,1}, x_{i,2}, \ldots, x_{i,n_1-k_1})$, が得られる．ただし $\boldsymbol{c}_i^{(1)} = \boldsymbol{u}_i^{(1)} G_1$ であり，$G_1 = [I_{k_1}, Q_1]$ 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．

さらにインタリーバにより $\boldsymbol{u}$ を置換し，今度はこれを k_2 シンボル毎に k_1 個のベクトルに分割する．これを $\boldsymbol{u}' = (\boldsymbol{u}_1^{(2)}, \boldsymbol{u}_2^{(2)}, \ldots, \boldsymbol{u}_{k_1}^{(2)})$, $\boldsymbol{u}_i^{(2)} = (u_{i,1}^{(2)}, u_{i,2}^{(2)}, \ldots, u_{i,k_2}^{(2)}), i = 1, 2, \ldots, k_1$, と表す．このそれぞれのベクトルに対し同一の C_2 を用いて符号化を行う．C_2 の生成行列を G_2 と表すと結果的に $\boldsymbol{c}^{(2)} = (\boldsymbol{c}_1^{(2)}, \boldsymbol{c}_2^{(2)}, \ldots, \boldsymbol{c}_{k_1}^{(2)})$, $\boldsymbol{c}_i^{(2)} = \boldsymbol{u}_i^{(2)} G_2$, が得られる．最終的に Hagenauer 型のブロックターボ符号の符号語 $\boldsymbol{c}_H$ は次式で表すことができる．

$$\boldsymbol{c}_H = (\boldsymbol{c}_1^{(2)}, \boldsymbol{c}_2^{(2)}, \ldots, \boldsymbol{c}_{k_1}^{(2)}, \boldsymbol{x}_1^{(1)}, \boldsymbol{x}_2^{(1)}, \ldots, \boldsymbol{x}_{k_2}^{(1)}). \quad (1)$$

さてこの Hagenauer 型のブロックターボ符号の生成行列を示す．$\boldsymbol{u}$ から $\boldsymbol{c}^{(1)}$ を求めるためには，$k_1k_2 \times k_2n_1$ 行列 $G_H^{(1)}$ を

$$G_H^{(1)} = \begin{bmatrix} G_1 & & & \mathbf{O} \\ & G_1 & & \\ & & \ddots & \\ \mathbf{O} & & & G_1 \end{bmatrix}, \quad (2)$$

と置くと $\boldsymbol{c}^{(1)} = \boldsymbol{u} G_H^{(1)}$ となる．次にインタリーバを $k_2n_1 \times k_2n_1$ 置換行列 $P_H = [p_{a,b}]$ により表現する．置換行列とは各行，各列の Hamming 重みが 1 の行列である．ここで C_1 の検査記号の各ベクトルを後ろへ置換するために P_H を次のように制限する．

$$p_{(i-1)n_1+k_1+j, k_1k_2+(i-1)(n_1-k_1)+j} = 1, \quad \forall i \in [1, k_2], \forall j \in [1, n_1 - k_1], \quad (3)$$

ただし整数 r, s に対し $[r, s] = \{r, r+1, \ldots, s\}$ と定義する．これにより

$$\boldsymbol{u} G_H^{(1)} P_H = (\boldsymbol{u}', \boldsymbol{x}_1^{(1)}, \boldsymbol{x}_2^{(1)}, \ldots, \boldsymbol{x}_{k_2}^{(1)}), \quad (4)$$

とすることができる．最後に式 (4) を符号化して式 (1) とするためには，$k_2n_1 \times \{k_1n_2 + (n_1 - k_1)k_2\}$ 行列 $G_H^{(2)}$ を

$$G_H^{(2)} = \begin{bmatrix} \overbrace{G_2}^{k_1\text{個}} & & & \mathbf{O} \\ & G_2 & & \\ & & \ddots & \\ & & & G_2 \\ \mathbf{O} & & & I_{(n_1-k_1)k_2} \end{bmatrix}, \quad (5)$$

と置けばよい．結果的に Hagenauer 型のブロックターボ符号 C_H の生成行列 G_H は式 (2),(3),(5) を用いて $G_H = G_H^{(1)} P_H G_H^{(2)}$ となる．

* 早稲田大学理工総合研究所，〒169-8555 新宿区大久保 3-4-1, School of Science and Engineering, Waseda University, 3-4-1 Ohkubo Shinjyuku-ku, Tokyo, 169-8555 Japan, E-mail:manabu@hirasa.mgmt.waseda.ac.jp
† 早稲田大学理工学部経営システム工学科，同上．
1 より一般に可変符号化に拡張することは容易である．

$P_H=[p_{a,b}]$ に式(3)以外の制約を次のように設ける．

$$\sum_{a=(i-1)n_1+1}^{(i-1)n_1+k_1}\ \sum_{b=(j-1)k_2+1}^{jk_2} p_{a,b} = 1, \qquad (6)$$
$$\forall i\in[1,k_2], \qquad \forall j\in[1,k_1],$$

ただし式(6)の和は通常の整数の加算を表す．置換行列により $u^{(1)}_{i_1,y_1}, u^{(1)}_{i_2,y_2}$ がそれぞれ $u^{(2)}_{j_1,z_1}, u^{(2)}_{j_2,z_2}$ に置換されたとすると，式(6)の制約により $i_1=i_2$ ならば $j_1\neq j_2$ となる．本稿では式(6)を満足する置換行列 P_H を持つ Hagenauer 型ブロックターボ符号 C^*_H を対象とする．

定義 1 ある符号 C に対し情報記号の Hamming 重みが w でかつ検査記号の Hamming 重みが z の符号語数を $A^C_{w,z}$ とする．また $W^C_{min}(w)=\min_z\{w+z|A^C_{w,z}>0\}$ と定義する． □

このとき次の定理が成り立つ．

定理 1 $d_1=d_2$ のとき $H(w)$ を次式で定義する．

$$H(w)=\begin{cases}(2\lceil\sqrt{w}\rceil-1)d_1-\lceil\sqrt{w}\rceil(\lceil\sqrt{w}\rceil-1), \\ \qquad\qquad \text{if } (\lceil\sqrt{w}\rceil-1)\lceil\sqrt{w}\rceil\geq w \\ 2\lceil\sqrt{w}\rceil d_1-\lceil\sqrt{w}\rceil^2, \qquad \text{otherwise}\end{cases} \qquad (7)$$

ただし $\lceil a\rceil$ は a 以上の最小の整数を表す．このとき

$$\min_{w'\geq w} W^{C^*_H}_{min}(w')\geq H(w), \qquad (8)$$

が成り立つ．

(証明) 文献[5]定理5,7参照． □

3 低重み情報に対する符号語の重みの下界

本節では情報記号の Hamming 重み $w=1,2$ それぞれに対する C^*_H の符号語の最小 Hamming 重み $W^{C^*_H}_{min}(w)$ の厳しい下界を示す．まずインタリーバ（置換行列）P_H にさらなる制限を加え，$W^{C^*_H}_{min}(w), w=1,2,$ の下界を示す．次に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．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．

定義 2 ある正定数 x_{max} に対し $F:[1,x_{max}]\to[1,x_{max}]$ を $F^{-1}(i)=F(i), i\in[1,x_{max}]$, を満たす全単射の関数とする．生成行列 G_1 の各行を $\boldsymbol{g}_i, i=1,2,\ldots,k_1$, と表し，$X_1,X_2,\ldots,X_{x_{max}}$ を

$$\bigcup_{i=1}^{x_{max}} X_i=[1,k_1], \qquad X_i\cap X_j=\phi,\ i\neq j,$$
$$|X_j|=|X_{F(j)}|\neq 0, \qquad j=1,2,\ldots,x_{max}, \qquad (9)$$

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．ただし $|X|$ は集合 X の要素数を表す．さらに関数 $J(y)$ を $y\in X_i\Leftrightarrow J(y)=i$ と定義し，$P(y)$ を次式で定義する．

$$P(y)=\min_{j\in X_{F(J(y))}}\{w_H(\boldsymbol{g}_j)-1\}. \qquad (10)$$

ただし $w_H(\boldsymbol{a})$ は $\boldsymbol{a}$ の Hamming 重みとする． □

このとき置換行列 $P_H=[p_{a,b}]$ に対し式(3),(6)に加え，さらに次のような制約を設ける．

$$(a \bmod n_1)\in X_i \text{ and } p_{a,b}=1$$
$$\Rightarrow (b-1 \bmod k_2)+1\in X_{F(i)}. \qquad (11)$$

すなわち，C_1 における X_i の要素の情報記号は C_2 における $X_{F(i)}$ の要素の情報記号へと置換する．このとき $W^{C^*_H}_{min}(1)$ に関して次の補題が成り立つ．

補題 1 式(3),(6),(11)を満足するように置換行列に制限を加えた時，次式を満足する定数 D_1 が存在するならば $W^{C^*_H}_{min}(1)\geq D_1$ が成り立つ．

$$P(y)+w_H(\boldsymbol{g}_y)\geq D_1,\ \forall y\in[1,k_1]. \qquad (12)$$

(証明) $w_H(\boldsymbol{u})=1$ を満たす $\boldsymbol{u}$ について考える．ある i,y に対し $\boldsymbol{u}^{(1)}_i=(u^{(1)}_{i,1},u^{(1)}_{i,2},\ldots,u^{(1)}_{i,k_1})$, $u^{(1)}_{i,y}=1$ とすると $G^{(1)}_H$ による符号化により $\boldsymbol{c}^{(1)}_i=\boldsymbol{g}_y$ となる．また $a=(i-1)n_1+y$ に対し $p_{a,b}=1$ とすると，$u^{(1)}_{i,y}$ は置換行列により $u^{(2)}_{j,z}$, $j=\lceil b/k_2\rceil$, $z=(b-1 \bmod k_2)+1$ へ置換される．従って $u^{(2)}_{j,z}=1$ より $\boldsymbol{c}^{(2)}_j=\boldsymbol{g}_z$ となる．ここで式(11)より $z\in X_{F(J(y))}$ であるから，式(10)の定義より $\boldsymbol{c}^{(2)}_j$ の検査記号の Hamming 重みについて $w_H(\boldsymbol{g}_z)-1\geq P(y)$ が成り立つ．従って

$$w_H(\boldsymbol{c}_H)=w_H(\boldsymbol{c}^{(1)}_i)+w_H(\boldsymbol{c}^{(2)}_j)-1\geq w_H(\boldsymbol{g}_y)+P(y), \qquad (13)$$

である．$u^{(1)}_{i,y}=1$ の i,y は任意として式(13)は成り立つので，補題が成り立つ． □

次にある正定数 D_1 に対し式(12)を満足するような集合 $X_1,X_2,\ldots,X_{x_{max}}$ を求める．そのために $Q(y):=\min_j\{j\geq D_1-w_H(\boldsymbol{g}_y)|A^{C_1}_{1,j}>0\}, y\in[1,k_1]$, $S_z:=\{y\in[1,k_1]|\ w_H(\boldsymbol{g}_y)-1=z\}, z\in[d_1-1,n_1-k_1]$, $x_{max}:=0$ とし，次のアルゴリズムを実行する．ただし $\lfloor a\rfloor$ は a 以下の最大の整数とする．

[探索アルゴリズム1]

(1) $z=d_1-1,d_1,\ldots,\lfloor\frac{D_1-2}{2}\rfloor$ について以下を行う．

(i) $S_z\neq\phi$ ならば以下を行う．

(ii) もし $q_i=z,\exists i\in[1,x_{max}]$ ならば $m:=i$, $flag:=0$ とする．そうでなければ $x_{max}:=x_{max}+2$, $F(x_{max}-1)=x_{max}$, $F(x_{max})=x_{max}-1$, $X_{x_{max}-1}=X_{x_{max}}:=\phi$, $m:=x_{max}-1$, $flag:=1$ とする．

(iii) 適当な $y\in S_z$ 1個に対し $X_m:=X_m\cup\{y\}$, $S_z:=S_z\setminus\{y\}$. また $t\geq Q(y)$ に対し $l\in S_t$ とし $X_{F(m)}:=X_{F(m)}\cup\{l\}$, $S_t:=S_t\setminus\{l\}$. もし $flag=1$ ならば $q_{x_{max}-1}:=z$, $q_{x_{max}}:=Q(y)$ とする．(i)へ．

(2) $Z:=\left\{z\geq\lceil\frac{D_1-1}{2}\rceil|S_z\neq\phi\right\}$ とし，もし $Z\neq\phi$ ならば $x_{max}:=x_{max}+1$, $X_{x_{max}}:=\bigcup_{z\in Z}S_z$, $F(x_{max}):=x_{max}$ とする．$X_1,X_2,\ldots,X_{x_{max}}$ を出力して終了． □

定理 2 正定数 D_1 に対して

$$\sum_{i=d_1-1}^{z}A^{C_1}_{1,i}\leq\sum_{i=D_1-z-1}^{n_2-k_2}A^{C_2}_{1,i},\ \forall z\in[d_1-1,n_1-k_1], \qquad (14)$$

が成り立つならば式(12)を満足する $X_1,X_2,\ldots,X_{x_{max}}$ が存在し，探索アルゴリズム1により得られる．

(証明) 探索アルゴリズム1のステップ(iii)における z に対し，式(14)を満足するならば $y\in S_z$ に対し $S_t\neq\phi$ を満たす $t\geq Q(y)$ が必ず存在する．従って式(14)が成り立つときアルゴリズム1は正常に終了する．次に，ステップ(iii)において $y\in X_m$ に対し $w_H(\boldsymbol{g}_y)-1=z$ であり，かつ $l\in X_{F(m)}$ に対し $w_H(\boldsymbol{g}_l)-1\geq Q(y)$ であるから $P(y)\geq Q(y)$ が成り立つ．また $w_H(\boldsymbol{g}_l)-1\geq Q(y)\geq D_1-w_H(\boldsymbol{g}_y)=D_1-(z+1)$ より $P(l)=z\geq D_1-w_H(\boldsymbol{g}_l)$ も成り立つ．

さらにステップ (2) において $z \geq \lceil \frac{D_1-1}{2} \rceil, z \in Z$, であるから，$y \in X_{x_{max}}$ に対し $P(y) \geq \lceil \frac{D_1-1}{2} \rceil$ である．従って $w_H(\boldsymbol{g}_y)+P(y) \geq 2\lceil \frac{D_1-1}{2} \rceil + 1 \geq D_1$ が成り立つ．以上より定理が成り立つ． □

次に $W_{min}^{C_H^*}(2)$ の下界に関して次の補題が成り立つ．

補題 2 式(3),(6),(11)を満足するように置換行列に制限を加えた時，次式を満足する定数 $D_2, 2D_1 \geq D_2$, が存在するならば $W_{min}^{C_H^*}(2) \geq D_2$ が成り立つ．

$$P(y)+P(z)+w_H(\boldsymbol{g}_y+\boldsymbol{g}_z) \geq D_2, \quad \forall y,z \in [1,k_1], y \neq z. \tag{15}$$

(証明) $w_H(\boldsymbol{u})=2$ を満たす $\boldsymbol{u}$ について考える．$i_l, y_l, l = 1,2,$ に対し $u_{i_l,y_l}^{(1)} = 1$ とし，また $a_l = (i_l-1)n_1 + y_l$ について $p_{a_l,b_l} = 1$ とする．このとき補題1の証明と同様 $u_{i_l,y_l}^{(1)}$ は置換行列により $u_{j_l,z_l}^{(2)}$, $j_l = \lceil b_l/k_2 \rceil$, $z_l = (b_l - 1 \bmod k_2)+1$ へ置換される．まず $i_1 = i_2$ を仮定すると $\boldsymbol{c}_{i_1}^{(1)} = \boldsymbol{g}_{y_1} + \boldsymbol{g}_{y_2}$ となる．また式(6)の制限より $j_1 \neq j_2$ であるから

$$\begin{aligned} w_H(\boldsymbol{c}_H) &= w_H(\boldsymbol{c}_{i_1}^{(1)}) + w_H(\boldsymbol{c}_{j_1}^{(2)}) - 1 + w_H(\boldsymbol{c}_{j_2}^{(2)}) - 1 \\ &\geq w_H(\boldsymbol{g}_{y_1}+\boldsymbol{g}_{y_2}) + P(y_1) + P(y_2), \end{aligned} \tag{16}$$

が成り立つ．次に $i_1 \neq i_2$ を仮定する．もし $j_1 \neq j_2$ ならば

$$\begin{aligned} w_H(\boldsymbol{c}_H) &= w_H(\boldsymbol{c}_{i_1}^{(1)}) + w_H(\boldsymbol{c}_{i_2}^{(1)}) + w_H(\boldsymbol{c}_{j_1}^{(2)}) - 1 \\ &\quad + w_H(\boldsymbol{c}_{j_2}^{(2)}) - 1 \\ &\geq w_H(\boldsymbol{g}_{y_1}) + w_H(\boldsymbol{g}_{y_2}) + P(y_1) + P(y_2), \end{aligned} \tag{17}$$

が成り立つ．ここで $y_1 \neq y_2$ ならば

$$\text{式(17)の最右辺} \geq w_H(\boldsymbol{g}_{y_1}+\boldsymbol{g}_{y_2}) + P(y_1) + P(y_2), \tag{18}$$

であり，$y_1 = y_2$ ならば

$$\text{式(17)の最右辺} \geq 2D_1, \tag{19}$$

となる．また $j_1 = j_2$ ならば

$$\begin{aligned} w_H(\boldsymbol{c}_H) &= w_H(\boldsymbol{c}_{i_1}^{(1)}) + w_H(\boldsymbol{c}_{i_2}^{(1)}) + w_H(\boldsymbol{c}_{j_1}^{(2)}) - 2 \\ &\geq P(z_1) + P(z_2) + w_H(\boldsymbol{g}_{z_1}+\boldsymbol{g}_{z_2}), \end{aligned} \tag{20}$$

が成り立つ．式(20)の最後の不等式は関数 $F = F^{-1}$ の対称性からなる．以上より，補題が成り立つ． □

次に符号 $C_1(=C_2)$ が式(14)を満足しているとき，式(15)を満足するような集合 $X_1, X_2, \ldots, X_{x_{max}}$ を探索により求めるアルゴリズムを以下に示す．

[探索アルゴリズム 2]

(初期化)

(1) $y = 1,2,\ldots,k_1$ に対し $Q(y) := \min_j\{j \geq D_1 - w_H(\boldsymbol{g}_y) | A_{1,j}^{C_1} > 0\}$.

(2) $z = d_1-1, d_1, \ldots, n_1-k_1$ に対し $S_z := \{y \in [1,k_1] | w_H(\boldsymbol{g}_y) - 1 = z\}$, $\Delta_z := \sum_{i=D_1-z-1}^{n_1-k_1} A_{1,i}^{C_1} - \sum_{i=d_1-1}^{z} A_{1,i}^{C_1}$.

(3) $M := \{\{y,z\} | Q(y)+Q(z)+w_H(\boldsymbol{g}_y+\boldsymbol{g}_z) < D_2, 1 \leq y < z \leq k_1\}$, $E := \phi$, $x_{max} := 0$.

(探索)

(4) もし $M = \phi$ ならば (12) へ．

(5) $y = 1,2,\ldots,k_1$ に対し $M_y := \{\{y,z\} \in M\}$.

(6) $L := \{y \in [1,k_1] | M_y \neq \phi\}$.

(7) もし任意の $y,z \in E$, に対し，ある $\{y,z\} \in M$ が存在するならば探索失敗として終了．

(8) $l := \arg\max_{y \in L \setminus (E \cap L)} |M_y|$, $t_0 := \max_{y|\{l,y\} \in M_l}\{D_2 - Q(y) - w_H(\boldsymbol{g}_y + \boldsymbol{g}_l)\}$, $t_1 := \min\{y \geq t_0 | S_y \neq \phi\}$.

(9) もし $i = Q(l), Q(l)+1, \ldots, t_1-1$ 全てに対し $\Delta_i > 0$ ならば $i = Q(l), Q(l)+1, \ldots, t_1-1$ それぞれについて $\Delta_i := \Delta_i - 1$. $Q(l) := t_1$, $M := M \setminus M_l$ とし，(10)へ．そうでなければ $E := E \cup \{l\}$ とし，(7)へ．

(10) もし $q_i = Q(l), \exists i \in [1, x_{max}]$ ならば $m := i$, $flag := 0$ とする．そうでなければ $x_{max} := x_{max} + 2$, $F(x_{max}-1) = x_{max}$, $F(x_{max}) = x_{max}-1$, $X_{x_{max}-1} = X_{x_{max}} := \phi$, $m := x_{max}-1$, $flag := 1$ とする．

(11) 適当な $y \in S_{Q(l)} \setminus (S_{Q(l)} \cap L)$ 1個に対し $X_m := X_m \cup \{y\}$, $S_{Q(l)} := S_{Q(l)} \setminus \{y\}$. $X_{F(m)} := X_{F(m)} \cup \{l\}$, $S_{w_H(\boldsymbol{g}_l)-1} := S_{w_H(\boldsymbol{g}_l)-1} \setminus \{l\}$. もし $flag = 1$ ならば $q_{x_{max}-1} := Q(l)$, $q_{x_{max}} := Q(y)$ とする．(4)へ．

(12) 探索アルゴリズム 1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 3 探索アルゴリズム 2 により得られた $X_1, X_2, \ldots, X_{x_{max}}$ は式(12),(15)を満足する．

(証明) 探索アルゴリズム2において，$\forall (y,z) \in M$ に対し $P(y) = Q(y)$, $P(z) = Q(z)$ とすると式(15)を満足しない．そこでステップ (8) から (11) において $P(l) = t_1$ を満足するように X_m および $X_{F(m)}$ を生成している．これにより $\forall (l,y) \in M_l$ に対し $P(l)+P(y)+w_H(\boldsymbol{g}_l+\boldsymbol{g}_y) \geq D_2$ が成り立つため，$M := M \setminus M_l$ として繰り返している．また明らかにこの $P(l)$ は式(12)を満足している．以上よりステップ (12) が行われる時は式(15)を満足している．ここでステップ (12) においては定理2の証明と同様式(12)を満足するように X_m および $X_{F(m)}$ が作成される．しかしステップ (12) を行う場合式(14)と同様に

$$\begin{aligned} \Delta_z &= \sum_{i=D_1-z-1}^{n_1-k_1} |S_i| - \sum_{i=d_1-1}^{z} |S_i| \geq 0, \\ &\qquad \forall z \in [d_1-1, n_1-k_1], \end{aligned} \tag{21}$$

を満足している必要がある．そこでステップ (9) において l に対し $P(l) = t_1$ としたとき式(21)が成り立つかどうかをチェックしている．もし式(21)が成り立たないなら $P(l) \leq t_1$ とせざるを得ないため $E := E \cup \{l\}$ とする．従ってステップ (7) において $y,z \in E$ に対し $\exists (y,z) \in M$ ならば $P(y)+P(z)+w_H(\boldsymbol{g}_y+\boldsymbol{g}_z) < D_2$ となってしまうため，アルゴリズム失敗として終了となる．以上よりアルゴリズムが正常に終了した場合，生成された $X_1, X_2, \ldots, X_{x_{max}}$ に対し式(12),(15)が成り立つ． □

以上より，与えられた符号 C_1 と生成行列 G_1 に対し，式(14)を満たす最大の D_1 を求め，また D_2 を適当な値から始めて探索アルゴリズム 2 を適用し，$X_1, X_2, \ldots, X_{x_{max}}$ 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．このとき定理2,3より低重み情報記号に対する符号語の Hamming 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．

4 最小距離の最大化

本節では C_H^* を構成したとき，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2および探索アルゴリズム 2 を用

表 1: D_1 および D_2 を最大とする $(n_1 = 2^m - 1, k_1, d_1 = 5)$ BCH 符号の生成行列 G_1^* の例

(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

いることにより，補題1，2を満足する最も大きい D_1 および D_2 を持つ C_H^* 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^*, $X_1^*, X_2^*, \ldots, X_{x_{max}^*}^*$, 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，その行列のはじめの k 列を線形独立となるように列置換する．さらに，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 と表す．

(4) G_1 より $A_{1,i}^{C_1}$ を求め，定理2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 $X_1, X_2, \ldots, X_{x_{max}}$ を求める．

(6) $D_2 > D_2^*$ ならば $G_1^* := G_1$, $x_{max}^* := x_{max}$, $X_i^* := X_i, i \in [1, x_{max}]$, $D_1^* := D_1$, $D_2^* := D_2$ とする．$repeat := repeat + 1$ として(2)へ． □

上のアルゴリズムで C に $n_1 = 2^m - 1, d_1 = 5$ を満たす (n_1, k_1, d_1) 原始 BCH 符号を用いた時の結果を表1に示す．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，さらに 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ビット毎に区切り，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．

表から，符号長 n_1 が増加するに従い D_1 および 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_H^* の最小距離に関する定理を以下に示す．

定理 4 式(3),(6),(11)を満足するインタリーバ（置換行列）を用いて構成した C_H^* の最小距離 D_H^* について

$$D_H^* \geq \min\{D_1, D_2, H(3)\}, \tag{22}$$

が成り立つ．

(証明) 補題1より $W_{min}^{C_H^*}(1) \geq D_1$, 補題2より $W_{min}^{C_H^*}(2) \geq D_2$, 定理1より $w \geq 3$ に対し $W_{min}^{C_H^*}(w) \geq H(3)$ が成り立つ．明らかに $D_H^* = \min_w W_{min}^{C_H^*}(w)$ 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_H^* では $D_H^* \geq D_1$ となる．また定理1から明らかな通り，$H(3) = 4d_1 - 4$ は d_1 が増加するに従い線形に増加する．このとき定理4より最小距離は D_1 あるいは D_2 に大きく依存する．従って本節で述べた生成行列生成アルゴリズムは C_H^* を設計する上で重要な役割を演ずる．

従来の置換行列に式(6),(11)の制約を課さないインタリーバを用いた場合，ブロックターボ符号 C_H の最小距離の下界は $d_1 (= d_2)$ である[5]．さらに式(6)の制約を課すと最小距離の下界は $2d_1 - 1$ となる[5]．表1を見ると D_1 はこれらに対し十分大きくなっている．従って本稿で示したインタリーバの構成法および要素符号 C_1 の生成手法は有効であると考えられる．

5 むすび

本稿では H.Hagenauer らの提案したブロックターボ符号に対し，最小距離を大きくする要素符号の探索アルゴリズムおよ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は従来より大きな最小距離を持つことを示した．

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する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(14)を満足する符号を生成する手法を開発する必要がある．また，得られたブロックターボ符号 C_H^* に対する重み分布の導出なども今後の課題である．

謝辞

本研究の一部は文部科学省平成12・13年度科学研究費補助金(課題番号12875072)の助成による．

参考文献

[1] C.Berrou, A.Glavieux and P.Thitimajshima, "Near Shannon limit error-correcting Coding and Decoding: Turbo-codes(1), " in IEEE Int. Conf. Communications ICC'93, Vol.2/3, pp.1064-1071, May 1993.

[2] H.Hagenauer, E.Offer and L.Papke, "Iterative Decoding of Binary Block and Convolutional Codes, " IEEE Trans. Inform. Theory, Vol. IT-42, No.2, pp.429-445, March 1996.

[3] C.Heegard and S.B.Wicker, TURBO CODING, Kluwer Academic Publishers, 1999.

[4] R.M.Pyndiah, "Near-Optimum Decoding of Product Codes: Block Turbo Codes, " IEEE Trans. Commun. Vol.46, No.8, pp.1003-1010, August 1998.

[5] 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," 電子情報通信学会研究技術報告,IT2001-11, pp.1-6, July 2001.