社団法人 電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
TECHNICAL REPORT OF IEICE.
IT 2001-11 (2001-7)

ブロックターボ符号の生成行列と性能評価

小林 学　　松嶋 敏泰　　平澤 茂一

早稲田大学 理工学部 経営システム工学科
〒169-8555 東京都新宿区大久保3-4-1
tel.03-5286-3290
fax.03-5273-7215
E-mail: manabu@hirasa.mgmt.waseda.ac.jp

あらまし　1993 年，C.Berrou らは AWGN 通信路に対し 1 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．その後 H.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．本稿ではブロックターボ符号を 1 次元の符号とみなした時の性能の解析を行うことを目的とする．そのためにブロックターボ符号の生成行列を求め，置換行列に制約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．また Hagenauer らの提案したブロックターボ符号に対し，置換行列に制約を加えることにより低域重み分布を少ない計算量で厳密に求めることができることを示し，BER の近似式とシミュレーションの結果を比較する．さらに，まったくランダムに選ばれた置換行列よりも，制約を加えた置換行列を用いたブロックターボ符号はその BER も小さくなることをシミュレーションにより示す．

キーワード　ブロックターボ符号，生成行列，最小距離，重み分布，最尤復号法

Generator Matrices of Block Turbo Codes and Their Performance Analysis

Manabu KOBAYASHI　　Toshiyasu MATSUSHIMA　　Shigeichi HIRASAWA

Dep. of Industrial and Management Systems Engineering
Waseda University
3-4-1 Ohkubo, Shinjuku-ku, Tokyo 169-8555
tel.03-5286-3290
fax.03-5273-7215
E-mail: manabu@hirasa.mgmt.waseda.ac.jp

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 analyze the performance of the block turbo codes by considering them as one-dimensional codes. At first we find generator matrices of block turbo codes. We show that it is possible to increase the lower bound of minimum distance by restricting permutation matrices. Furthermore we propose a method to calculate low weight distribution with low complexity. Simulation results show that block turbo codes achieve low BER by restricting permutation matrices.

key words　Block turbo codes, Generator matrix, Minimum distance, Weight distribution, MLD

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]．復号にはこれらの要素符号の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を生成する．ターボ復号では，一方の復号器のこの信頼度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．また要素符号の情報に対する信頼度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 [3]．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 [3, 6]．

本稿ではこのブロックターボ符号を 1 次元の符号とみなした時の性能の解析を行うことを目的とする．そのためにまずブロックターボ符号の生成行列を求める．また置換行列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．この制限を加えると，H.Hagenauer らの提案したブロックターボ符号 [3] (以降 Hagenauer 型と呼ぶ) に対しては与えられた置換行列に対し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 (ユニバーサルインターリーバのような) 置換の取りうるすべて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置換に対し，正確な重み分布を探索により求めることを考えている．これによりビット誤り確率を低減するための決定的な (ランダムでない) 置換行列を求める指針を導き出せる可能性がある．さらにブロックターボ符号に対し，この低域重み分布から BER の近似式とシミュレーションの結果を比較し，考察を加える．また，まったくランダムに選ばれた置換行列よりも，制限を加えた置換行列を用いたブロックターボ符号はその復号誤り確率も小さくなることをシミュレーションにより明らかにする．

2 ブロックターボ符号の生成行列

2.1 一般のブロックターボ符号に対する生成行列

2 つの要素符号をそれぞれ $C^{(1)}, C^{(2)}$ と表し，$C^{(i)}, i = 1, 2,$ はそれぞれ符号長 N_i, 情報記号数 K_i の組織ブロック符号とする．またそれぞれの生成行列を $G^{(i)}$ で表し，$N_1 \times K_2$ 置換行列を P とする．置換行列 P は各行，各列の Hamming 重みが厳密に 1 の行列である．ここで本稿では符号長 N_2，情報記号数 K_1 のブロックターボ符号を次のように定義する．ただし $K_2 = N_1$ とする．

[ブロックターボ符号の符号化]

(Step 1) K_1 ビットの情報を $G^{(1)}$ により符号化する．

(Step 2) N_1 ビットの $C^{(1)}$ の符号語を置換行列 P により置換する．

(Step 3) 置換後の $K_2 = N_1$ ビットの系列を $G^{(2)}$ により符号化する．

(Step 4) 得られた符号語がブロックターボ符号の符号語である． □

この符号に対する生成行列 G が $G = G^{(1)} P G^{(2)}$ となることは明らかであろう[1]．またこの G からパリティ検査行列を求めることも容易である．この符号化では $C^{(1)}$ の符号語のパリティビットも $G^{(2)}$ で符号化していることに注意する必要がある．次節で述べるように，パリティビットを符号化する必要がなければ，置換行列において $C^{(1)}$ の符号語のパリティビットの部分を後にまとめ，$G^{(2)}$ においてこの部分をそのまま出力するようにすればよい．従ってこの表記はかなり広い符号のクラスを含む．また通常の組織畳込み符号を用いたターボ符号も，終端まで考慮すると上で述べた生成行列により表現可能である．任意の線形ブロック符号に対し生成行列が既知であれば，その最小トレリスを作成することが可能である [5] ため，ターボ符号のトレリスを作成することができ，またそのトレリスは状態数最小のトレリスとして表現できる．従って M.Breiling らにより提案されたターボ符号のトレリス [2] より状態数を小さくすることが可能である．

2.2 Hagenauer 型ブロックターボ符号の生成行列

H.Hagenauer らにより提案されたブロックターボ符号 C_H は，2 つの要素符号のパリティビットが情報にのみ依存し，互いのパリティビットには影響を受けない構成となっている．今 K_1 ビットの情報 $\boldsymbol{u}$ を k_1 ビット毎に $k_2 = K_1/k_1$ 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．このそれぞれのベクトル $\boldsymbol{u}_i^{(1)}$ を情報とみなし，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 (n_1, k_1, d_1) 組織符号 C_1 を用いて符号化を行うものと仮定する[2]．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 $\boldsymbol{u}$ を置換し，今度はこれを k_2 ビット毎に 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 (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 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求めよう．$\boldsymbol{u}$ から $\boldsymbol{c}^{(1)}$ を求めるためには，$k_1 k_2 \times k_2 n_1$ 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 $k_2 n_1 \times k_2 n_1$ 置換行列 $P_H = [p_{a,b}]$ を次のように制限する．

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

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．すなわち式 (3) はパリティビットを後ろへ置換している．最後に式 (4) を符号化して式 (1) と

[1] ここでは最終的な符号語のビットの並び順については考慮していない．もし考慮する必要がある場合には最後に符号語に対し別の置換を施せばよい．これは結局生成行列 G の列に対しこの置換を施せば良いことに対応する．

[2] より一般に可変符号化に拡張することは容易である．

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

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

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．

2.3 積型ブロックターボ符号の生成行列

本節では従来の積符号を含む，積型のブロックターボ符号 C_P についてその生成行列 G_P を導き出す．ここでも Hagenauer 型と同じく (n_i, k_i, d_i) 組織符号 $C_i, i = 1, 2$, とその生成行列 G_i を用いるものと仮定する．まず符号化は2.2節の $c^{(1)}$ まで同一である．従って $G_P^{(1)} = G_H^{(1)}$ とする．積型では $C^{(1)}$ の符号語 $c^{(1)}$ のパリティビットに対しても符号化を施す点が Hagenauer 型と異なる点である．従って $k_2n_1 \times k_2n_1$ 置換行列 P_P は式(3)のような制限を設けず，任意の置換行列とする．さらにこの置換行列に従って $c^{(1)}$ を置換し，k_2 ビットずつ分割したベクトルを $v = (v_1, v_2, \ldots, v_{n_1})$, $v_i = (v_{i,1}, v_{i,2}, \ldots, v_{i,k_2})$, と表す．すなわち $v = c^{(1)} P_P$ である．v_i をそれぞれ G_2 により符号化し，積型ブロックターボ符号の符号語 c_P は

$$c_P = (c'^{(2)}_1, c'^{(2)}_2, \ldots, c'^{(2)}_{n_1}), \quad (6)$$

となる．ただし $c'^{(2)}_i = v_i G_2$ である．これは $k_2n_1 \times n_1n_2$ 行列 $G_P^{(2)}$ を

$$G_P^{(2)} = \begin{bmatrix} G_2 & & \mathbf{O} \\ & G_2 & \\ & & \ddots \\ \mathbf{O} & & G_2 \end{bmatrix}, \quad (7)$$

としていることに他ならない．結局積型ブロックターボ符号 C_P の生成行列 G_P は $G_P = G_P^{(1)} P_P G_P^{(2)}$ となる．

3 置換の制限および最小距離の下界

本節では，前節までに定義した Hagenauer 型および積型のブロックターボ符号の最小距離の下界を求める．さらに置換行列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．

3.1 Hagenauer 型ブロックターボ符号の最小距離

定義 1 生成行列 G_H の部分行列を次のように定義する．

$$G_H = [G^{(2)}_{H,1}, G^{(2)}_{H,2}, \ldots, G^{(2)}_{H,k_1}, G^{(1)}_{H,1}, G^{(1)}_{H,2}, \ldots, G^{(1)}_{H,k_2}], \quad (8)$$

ただし $G^{(2)}_{H,i}$ は $k_1k_2 \times n_2$ 行列，$G^{(1)}_{H,i}$ は $k_1k_2 \times (n_1-k_1)$ 行列とする．また $G^{(2)}_{H,i}$ の非全零の行の番号の集合を $F_i \subset [1, k_1k_2]$ と定義する． □

このとき $G_H = G_H^{(1)} P_H G_H^{(2)}$ から次の補題が成り立つ．

補題 1 式(8)の生成行列 G_H に対して次が成り立つ．

(1) $G^{(2)}_{H,i}$ はその行に G_2 の各行をただ 1 回ずつ必ず含み，かつその他の行は全零ベクトルである $(|F_i| = k_2)$.

(2) $G^{(1)}_{H,i}$ ははじめの $(i-1)k_1$ 行は全零ベクトルであり，続く k_1 行の部分に G_1 の部分行列 Q_1 が現れ，終わりの $(k_2-i)k_1$ 行はまた全零ベクトルである．

(3) $F_i \bigcap F_j = \emptyset, i \neq j$, である． □

定理 1 Hagenauer 型ブロックターボ符号 C_H の最小距離 D_H は $D_H \geq \max\{d_1, d_2\}$ が成り立つ．

(証明) $G_H^{left} = [G^{(2)}_{H,1}, G^{(2)}_{H,2}, \ldots, G^{(2)}_{H,k_1}]$, $G_H^{right} = [G^{(1)}_{H,1}, G^{(1)}_{H,2}, \ldots, G^{(1)}_{H,k_2}]$ と置く．このとき G_H^{left} は補題1の(1),(3)より任意の行の和の Hamming 重みは d_2 以上であることが保証される．さらに G_H^{left} の中で情報位置に対応する Hamming 重みが 1 の列のみを並べた G_H^{left} の部分行列を G_H^{info} とすると，補題1の(2)より行列 $[G_H^{info}, G_H^{right}]$ の任意の行の和は Hamming 重み d_1 以上となる．以上より定理が成り立つ． □

さて最小距離の下界を大きくするために，$P_H = [p_{a,b}]$ に式(3)以外の制約を次のように設ける．

$$\sum_{a=(i-1)n_1+1}^{(i-1)n_1+k_1} \sum_{b=(j-1)k_2+1}^{jk_2} p_{a,b} = 1, \quad (9)$$
$$\forall i \in [1, k_2], \qquad \forall j \in [1, k_1],$$

ただし式(9)の和は通常の整数の加算を表す．これは補題1に加え次の補題を導く．

補題 2 P_H に式(9)の条件を加えたとき，式(8)の生成行列 G_H に対し，$|F_i \bigcap [(j-1)k_1+1, jk_1]| = 1, \forall i \in [1, k_1]$, $\forall j \in [1, k_2]$, が成り立つ． □

式(9)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をこれ以降 C_H^* と表す．

定義 2 情報 $u = (u_1, u_2, \ldots, u_{k_1k_2})$ に対し $S(u) = \{i | u_i = 1\}$ と定義し，その逆写像を $S^{-1}(\ )$ で表す．また $S^{(2)}(u) = \{i \in [1, k_1] | F_i \bigcap S(u) \neq \emptyset\}$, $S^{(1)}(u) = \{i \in [1, k_2] | [(i-1)k_1+1, ik_1] \bigcap S(u) \neq \emptyset\}$ と定義する．さらに情報 u に対応する符号語のパリティビットの Hamming 重みを $Z(u) = w_H(uG_H) - w_H(u)$ と定義する．ここで $w_H(x)$ は x の Hamming 重みを表す． □

この定義を用いると次の補題が成り立つ．

補題 3 情報 u に対応する C_H の符号語のパリティビットの Hamming 重みは次式を満足する．

$$Z(u) \geq d_2 |S^{(2)}(u)| + d_1 |S^{(1)}(u)| - 2w_H(u). \quad (10)$$

(証明) $i \in S^{(2)}(u)$ に対し $c_i^{(2)} = S^{-1}(F_i \bigcap S(u))$ $G^{(2)}_{H,i}$ は補題1の(1)より C_2 の符号語であるから，$w_H(c_i^{(2)}) \geq d_2$ が成り立つ．また $i \in S^{(1)}(u)$ に対し $x_i^{(1)} = S^{-1}([(i-1)k_1+1, ik_1] \bigcap S(u)) G^{(1)}_{H,i}$ は補題1の(2)より C_1 の符号語のパリティビットであるから $w_H(x_i^{(1)}) + |[(i-1)k_1+1, ik_1] \bigcap S(u)| \geq d_1$ が成り立つ．従って

$$\sum_{i \in S^{(1)}(u)} \left\{ w_H(x_i^{(1)}) + \left| [(i-1)k_1+1, ik_1] \bigcap S(u) \right| \right\}$$
$$= \sum_{i \in S^{(1)}(u)} w_H(x_i^{(1)}) + w_H(u) \geq |S^{(1)}(u)| d_1, \quad (11)$$

であるから，以上より補題が成り立つ． □

補題 4 C_H^* に対し $S^{(2)}(u), S^{(1)}(u)$ は次式を満たす．

$$|S^{(2)}(u)||S^{(1)}(u)| \geq w_H(u). \quad (12)$$

(証明) 補題2より明らか． □

$$W(i,w) = d_2\left\lceil \frac{w}{i} \right\rceil + d_1 i - w, \quad i \in [1,w], \qquad (13)$$

と定義すると次の定理が導かれる．

定理 2 C_H^* の最小距離 D_H^* は $D_H^* \geq W(1,1) = d_1 + d_2 - 1$ が成り立つ．

(証明) 補題 3 , 4 より任意の $w \in [1, k_1k_2]$ に対し

$$\min_{u|w_H(u)=w} \{w_H(u) + Z(u)\} \geq \min_{i\in[1,w]} W(i,w), \qquad (14)$$

が成り立つ．もし $\lceil \frac{w}{i} \rceil = 1$ ならば $i = w$ より $W(w,w) \geq W(1,1)$，同様に $W(1,w) \geq W(1,1)$ が成り立つ．結局任意の $w < W(1,1)$ と $i \in [1,w]$ に対して $W(i,w) \geq W(1.1)$ である．以上より

$$D_H^* = \min_{u\neq 0} \{w_H(u) + Z(u)\} \geq W(1,1), \qquad (15)$$

となり定理が成り立つ． □

3.2 積型ブロックターボ符号の最小距離

いま簡単のため $d_1 \leq k_2$ とする．このとき積型ブロックターボ符号 C_P の最小距離 D_P に関して次の定理が成り立つ．

定理 3 積型ブロックターボ符号 C_P の最小距離 D_P は $D_P \geq \max\{d_1, d_2\}$ が成り立つ．

(証明) C_1 の最小距離が d_1 であるから，非零の情報に対し $w_H(\boldsymbol{c}^{(1)}) \geq d_1$ が成り立つ．いま $w_H(\boldsymbol{c}^{(1)}) = d_1$ の時を考える．またこの $\boldsymbol{c}^{(1)}$ を置換したベクトル $\boldsymbol{v} = (v_1, v_2, \ldots, v_{n_1})$ が，ある j に対し $w_H(v_i) = 0, i \neq j$，かつ $w_H(v_j) = d_1$ を満たす置換 P_P が存在する．このとき式(6)より C_2 は組織符号であるから，明らかに $w_H(\boldsymbol{c}_P) \geq d_1$ である．また C_2 の最小距離は d_2 であるから，同様に $w_H(\boldsymbol{c}_P) \geq d_2$ が成り立つ．$w_H(\boldsymbol{c}^{(1)}) > d_1$ のときも同様である．以上より定理が成り立つ． □

定理 3 の最小距離の下界が定理 1 の Hagenauer 型と同一であることは興味深い．

さて Hagenauer 型と同様最小距離の下界を大きくするために，$P_P = [p_{a,b}]$ に次の制約を設ける．

$$\sum_{a=(i-1)n_1+1}^{in_1} \sum_{b=(j-1)k_2+1}^{jk_2} p_{a,b} = 1, \qquad (16)$$
$$\forall i \in [1,k_2], \qquad \forall j \in [1,n_1],$$

ただし式(16)の和は通常の整数の加算を表す．このとき次の定理が成り立つ．

定理 4 P_P に式(16)の条件を加えた積型ブロックターボ符号 C_P^* の最小距離 D_P^* は $D_P^* \geq d_1d_2$ が成り立つ．

(証明) 非零の情報に対し $w_H(\boldsymbol{c}^{(1)}) \geq d_1$ が成り立つ．またこの $\boldsymbol{c}^{(1)}$ を置換したベクトル $\boldsymbol{v} = (\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_{n_1})$ は，式(16)の条件のため $w_H(\boldsymbol{v}_i) \neq 0$ なる i が必ず d_1 以上存在する．また $w_H(\boldsymbol{v}_i) \neq 0$ に対し $\boldsymbol{c}'^{(2)}_i = \boldsymbol{v}_i G_2$ より $w_H(\boldsymbol{c}'^{(2)}_i) \geq d_2$ であるから定理が成り立つ． □

従来の積符号が積型ブロックターボ符号として記述できることは明らかであろう．またそのときの置換行列 P_P は式(16)を満足する．従って式(16)を満足する置換行列を用いた積型ブロックターボ符号は，積符号の自然な拡張と考えることができる．しかし従来の積符号はその最小距離が厳密に d_1d_2 であるのに対し，C_P^* の中にはその最小距離 D_P^* が $D_P^* > d_1d_2$ となるものが存在する．$D_P^* > d_1d_2$ となる符号 C_P^* の例は論文[7]を参照されたい．

定理 2 と定理 4 を比較すると，Hagenauer 型と積型ではその最小距離のオーダが異なることが分かる．最小距離の観点からすると，積型のブロックターボ符号が優れていることが分かる．

4 情報に対する符号語の Hamming 重み

本節では式(9)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^* を対象とし，情報の Hamming 重みに対する符号語の Hamming 重みの下界を求める．これにより符号 C_H^* に対する小さい Hamming 重みを持つ符号語数を求めることが可能な条件が明らかとなる．従って最尤復号法を行ったときのビット誤り確率の近似式が得られる．本稿では（ユニバーサルインターリーバのような）P_H の取りうるすべて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 G_1, G_2, P_H に対し正確な重み分布を探索により求めることを考える．

定義 3 符号 C_H^* に対し情報記号の Hamming 重みが w でかつパリティビットの Hamming 重みが z の符号語数を $A_{w,z}$ とする．また $Z_{min}^{C_H^*}(w) = \min\{z | A_{w,z} > 0\}$ と定義する． □

定理 5 $d_1 = d_2$ のとき次式が成り立つ．

$$\min_i W(i,w) = \begin{cases} (2\lceil\sqrt{w}\rceil - 1)d_1 - w, \\ \qquad \text{if } (\lceil\sqrt{w}\rceil - 1)\lceil\sqrt{w}\rceil \geq w \\ 2\lceil\sqrt{w}\rceil d_1 - w, \qquad \text{otherwise} \end{cases} \qquad (17)$$

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

(証明) 付録A参照． □

系 1 $Z_{min}^{C_H^*}(w) \geq \min_i W(i,w) - w$ である．もし $d_1 = d_2$ ならば $\min_i W(i,w)$ は式(17)で与えられる． □

さて，C_H^* の最小距離 D_H^* の下界は定理 2 で述べた通り $d_1 + d_2 - 1$ であるが，いま $d_1 + d_2 - 1$ を一定として考えると次の重要な定理が成り立つ．

定理 6 $d_1 + d_2 - 1$ を一定の奇数としたとき，それぞれの w に対し $\min_i W(i,w)$ を最大にする d_1, d_2 の組は $d_1 = d_2$ である．

(証明) 付録B参照． □

系 1 と定理 6 より，Hagenauer 型のブロックターボ符号 C_H^* では $d_1 = d_2$ とすることにより，最小距離の下界を一定に保ったもとで情報の Hamming 重みに対するパリティビットの Hamming 重みの下界を最も大きくすることができる．

定義 4 $H(w)$ および $U(w)$ を次式で定義する．

$$H(w) = \min_{w\leq w'\leq d_1^2} \min_i W(i,w'), \qquad (18)$$

$$U(w) = \begin{cases} \lceil\sqrt{w}\rceil(\lceil\sqrt{w}\rceil - 1), \\ \qquad \text{if } (\lceil\sqrt{w}\rceil - 1)\lceil\sqrt{w}\rceil \geq w \\ \lceil\sqrt{w}\rceil^2, \qquad \text{otherwise} \end{cases} \qquad (19)$$

□

補題 5 $U(w)$ に対し $\lceil\sqrt{U(w)}\rceil = \lceil\sqrt{w}\rceil$ が成り立つ．

(証明) $U(w) = \lceil\sqrt{w}\rceil^2$ なら明らか．いま $U(w) = \lceil\sqrt{w}\rceil(\lceil\sqrt{w}\rceil - 1)$ を仮定する．もし $\lceil\sqrt{U(w)}\rceil \geq \lceil\sqrt{w}\rceil + 1$ ならば $\lceil\sqrt{w}\rceil(\lceil\sqrt{w}\rceil - 1) \leq (\lceil\sqrt{U(w)}\rceil - 1)(\lceil\sqrt{U(w)}\rceil - 2) < U(w)$ となり矛盾する．従って補題が成り立つ． □

補題 6 $d_1 = d_2$ かつ $w < w' \leq d_1^2$ に対し $\min_i W(i, U(w)) \leq \min_i W(i, U(w'))$ が成り立つ．

(証明) 付録C参照 □

補題 5 , 6 より次の定理が成り立つ．

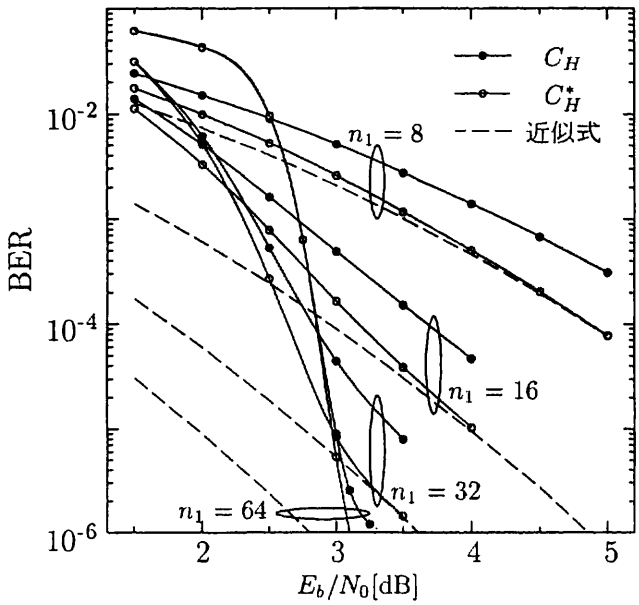

図 1: Hagenauer 型ブロックターボ符号のビット誤り確率

定理 7 $d_1 = d_2$ のとき次式が成り立つ.

$$H(w) = \begin{cases} (2\lceil\sqrt{w}\rceil - 1)d_1 - \lceil\sqrt{w}\rceil(\lceil\sqrt{w}\rceil - 1), \\ \qquad \text{if } (\lceil\sqrt{w}\rceil - 1)\lceil\sqrt{w}\rceil \geq w \\ 2\lceil\sqrt{w}\rceil d_1 - \lceil\sqrt{w}\rceil^2, \qquad \text{otherwise} \end{cases} \tag{20}$$

(証明) まず補題 5 より $w \leq U(w)$ かつ $\lceil\sqrt{w}\rceil = \lceil\sqrt{U(w)}\rceil$ であるから

$$\min_i W(i,w) \geq \min_i W(i,U(w)), \tag{21}$$

である. これと補題 6 より定理が成り立つ. □

$H(d_1^2) = d_1^2$ で, $w_H(\boldsymbol{u}) > d_1^2$ に対しては明らかに $w_H(\boldsymbol{u}G_H) > d_1^2$ であるから, ある $w_{max} \leq d_1^2$ を選び $w_H(\boldsymbol{u}) \leq w_{max}$ を満たす全ての $\boldsymbol{u}$ について $w_H(\boldsymbol{u}G_H)$ を全て求めたとき, $\{A_{w,z} | w \leq w_{max}, w+z < H(w_{max}+1)\}$ が求まる.

例 1 $d_1 = d_2 = 4$ とすると定理 7 より $H(1) = 7, H(2) = 10, H(3) = H(4) = 12$, である. 従って $w_{max} = 2$ とすると Hamming 重み 11 以下の符号語数が求められる. 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 Hamming 重み 19 以下の符号語数が求められる. □

5 シミュレーションによる評価

本節では, 3節で述べた置換に式 (9) の制約を設ける Hagenauer 型ブロックターボ符号 C_H^* に対し, 制約を設けない符号 C_H との比較をシミュレーションにより評価する. ブロックターボ符号を構成する要素符号 C_1, C_2 は共に同じ符号長を持つ拡大 Hamming 符号を用い, 符号長をそれぞれ $n_1 = n_2 = 8, 16, 32, 64$ とする.

ターボ復号は要素符号 C_1, C_2 それぞれに対し MAP 復号を用い, 一方の符号の外部情報から他方の情報の事前確率を求める Hagenauer らの復号 [3] を行う.

図 1に結果を示す. 置換の種類はそれぞれの符号に対し 10 通りを (制約を満足する中で) ランダムに生成し, ビット誤り確率はその平均を示した. MAP 復号の繰り返し数は C_1, C_2 それぞれに対し $n_1 = 8, 16, 32$ では 6 回ずつ, $n_1 = 64$ では 15 回ずつ行っている.

また図 1では参考のため 4節で提案した条件を用いて C_H^* に対する低域重み分布を求め, 次式のビット誤り確率 P_b の近似式 [4] を用いた結果も併せて示している. ただし $R = k_1 k_2 / \{k_1 n_2 + k_2(n_1 - k_1)\}$ は C_H^* の符号化率である.

$$P_b \approx \frac{e^{D_H^* R E_b/N_0}}{k_1 k_2} Q\left(\sqrt{2D_H^* R E_b/N_0}\right) \cdot \left(\sum_{w=1}^{w_{max}} \sum_{z=0}^{H(w_{max}+1)-1-w} w A_{w,z} e^{-(w+z)RE_b/N_0}\right), \tag{22}$$

$$Q(x) \equiv \frac{1}{\sqrt{2\pi}} \int_x^\infty e^{-\frac{y^2}{2}} dy,$$

ただし $w_{max} = 2, H(w_{max}+1) = 12$ とし, $\{A_{w,z} | w \leq 2, w+z < 12\}$ を求めた.

図 1より以下のことが分かる.

(1) C_H^* のビット誤り確率は, 置換に制約を課さない符号 C_H のそれよりかなり小さい.

(2) 近似式 (22) は最尤復号を行ったときの近似値を表しているため, ターボ復号の結果がこの近似式と近い領域ではターボ復号と最尤復号の差が小さいことを示す. 従って少なくとも SN 比が (3.5dB 程度以上) 高くなるとターボ復号はほぼ最尤復号と同等の性能を示す[3].

(3) (2) より, SN 比が (3.5dB 程度以上) 高くなると P_b の近似式 (22) がかなり良い精度となる.

6 むすび

本稿ではブロックターボ符号の生成行列を求めた. またブロックターボ符号の最小距離の下界を示し, 置換行列に制約を加えるとこれを改善することが可能であることを示した. さらにこの制約を加えると, Hagenauer 型のブロックターボ符号 C_H^* に対しては, 与えられた置換行列に対し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ことを示した. 結果的にまったくランダムに選ばれた置換行列よりも, 制約を加えた置換行列を用いたブロックターボ符号はその復号誤り確率も小さくなる. さらにブロックターボ符号に対しこの低域重み分布から BER の近似式とシミュレーションの結果を比較し, 近似式がかなり良い値を示すことを明らかにした.

本稿で述べた通り, 符号 C_H^* では情報記号の Hamming 重みが 1 のときに符号語の最小 Hamming 重みの下界がでてくるため, G_1 の最小重みの行に対応する情報はなるべく G_2 の最大重みの行に置換されるように置換行列を作成することにより, C_H^* の最小距離の下界をさらに大きくすることが可能である.

積型ブロックターボ符号のシミュレーションによる性能評価は論文 [7] を参照されたい. その他補題 3 , 4 を用いて, $H(w_{max}+1)$ 未満の Hamming 重みを持つ符号語数を高速に求めるアルゴリズムを導出することが今後の課題である.

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] M.Breiling and L.Hanzo, "The Super-Trellis Structure of Turbo Codes, " IEEE Trans. Inform. Theory, Vol. IT-46, No.6, pp.2212-2228, Sep. 2000.

[3] これより SN 比が小さいところでは近似式の精度が良くないため, ターボ復号と最尤復号の比較は図 1からは述べることができない.

[3] 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.

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

[5] S.Lin, T.Kasami, T.Fujiwara and M.Fossorier, TRELLISES AND TRELLIS-BASED DECODING ALGORITHMS FOR LINEAR BLOCK CODES, Kluwer Academic Publishers, 1998.

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

[7] 大島 英明, 小笠原 尚徳, 小林 学, 平澤 茂一 "ブロックターボ符号の生成行列を用いた一復号法." 信学技報, this issue, July 2001.

A 定理 5 の証明

$f(i) = d_2\frac{w}{i} + d_1 i - w$ と置くと $f'(i) = -\frac{d_2 w}{i^2} + d_1 = 0$ 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．

(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

$$w - (\lceil\sqrt{w}\rceil - 2)\lceil\sqrt{w}\rceil = (\sqrt{w} + \lceil\sqrt{w}\rceil)(\sqrt{w} - \lceil\sqrt{w}\rceil) + 2\lceil\sqrt{w}\rceil, \quad (23)$$

が成り立つが，$(\sqrt{w} + \lceil\sqrt{w}\rceil) \leq 2\lceil\sqrt{w}\rceil$，であり，かつ $-1 < \sqrt{w} - \lceil\sqrt{w}\rceil \leq 0$ であるので式(23)は 0 より大きい．従って $\lceil\sqrt{w}\rceil - 2 < \frac{w}{\lceil\sqrt{w}\rceil} \leq \lceil\sqrt{w}\rceil - 1$ が成り立つので $\left\lceil\frac{w}{\lceil\sqrt{w}\rceil}\right\rceil = \lceil\sqrt{w}\rceil - 1$ である．従って $W(\lceil\sqrt{w}\rceil, w) = (2\lceil\sqrt{w}\rceil - 1)d_1 - w$ となる．

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

$w - (\lceil\sqrt{w}\rceil - 1)^2 = (\sqrt{w} + \lceil\sqrt{w}\rceil - 1)(\sqrt{w} - \lceil\sqrt{w}\rceil + 1) > 0$ であるから $\lceil\sqrt{w}\rceil - 1 < \frac{w}{\lceil\sqrt{w}\rceil - 1} \leq \lceil\sqrt{w}\rceil$ が成り立つ．従って $\left\lceil\frac{w}{\lceil\sqrt{w}\rceil - 1}\right\rceil = \lceil\sqrt{w}\rceil$ 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

$\lceil\sqrt{w}\rceil - 1 < \frac{w}{\lceil\sqrt{w}\rceil} \leq \sqrt{w}$ であるから $\left\lceil\frac{w}{\lceil\sqrt{w}\rceil}\right\rceil = \lceil\sqrt{w}\rceil$ となる．従って $W(\lceil\sqrt{w}\rceil, w) = 2\lceil\sqrt{w}\rceil d_1 - w$ である．

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

$\lceil\sqrt{w}\rceil < \frac{w}{\lceil\sqrt{w}\rceil - 1}$ が成り立つので，$\left\lceil\frac{w}{\lceil\sqrt{w}\rceil - 1}\right\rceil \geq \lceil\sqrt{w}\rceil + 1$ である．従って $W(\lceil\sqrt{w}\rceil - 1, w) \geq 2\lceil\sqrt{w}\rceil d_1 - w$ となる．

以上より定理が成り立つ．

B 定理 6 の証明

表記のあいまいさをなくすため，式(13)を改めて $W_{(d_1,d_2)}(i,w)$ と書くことにする．また $T = d_1 + d_2$ を偶数の定数とする．定理 5 の証明と同様場合分けを行う．

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

$i = \lceil\sqrt{w}\rceil$ 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 $d_{max} = \max\{d_1, d_2\}$ と置くと

$$\min_i W_{(d_1,d_2)}(i,w) \leq T\lceil\sqrt{w}\rceil - d_{max} - w < \min_i W_{(T/2,T/2)}(i,w) = T\lceil\sqrt{w}\rceil - \frac{T}{2} - w, \quad (24)$$

となり，厳密に $d_1 = d_2 = \frac{T}{2}$ のときに $\min_i W_{(d_1,d_2)}(i,w)$ 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

$i = \lceil\sqrt{w}\rceil - 1$ のとき $\frac{w}{\lceil\sqrt{w}\rceil - 1} \leq \lceil\sqrt{w}\rceil + 1$ であるから $\left\lceil\frac{w}{\lceil\sqrt{w}\rceil - 1}\right\rceil = \lceil\sqrt{w}\rceil + 1$ である．従って

$$W_{(d_1,d_2)}(\lceil\sqrt{w}\rceil - 1, w) = T\lceil\sqrt{w}\rceil + d_2 - d_1 - w, \quad (25)$$

となる．また $i = \lceil\sqrt{w}\rceil + 1$ のとき $\lceil\sqrt{w}\rceil - 2 < \frac{w}{\lceil\sqrt{w}\rceil + 1} \leq \lceil\sqrt{w}\rceil - 1$ より

$$W_{(d_1,d_2)}(\lceil\sqrt{w}\rceil + 1, w) = T\lceil\sqrt{w}\rceil - d_2 + d_1 - w, \quad (26)$$

である．結局式(25),(26)より $d_1 \neq d_2$ のとき

$$\min_i W_{(d_1,d_2)}(i,w) \leq T\lceil\sqrt{w}\rceil - |d_2 - d_1| - w, < \min_i W_{(T/2,T/2)}(i,w) = T\lceil\sqrt{w}\rceil - w, \quad (27)$$

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

(3) $w = \lceil\sqrt{w}\rceil^2$ のとき

$$\min_i W_{(d_1,d_2)}(i,w) \leq W_{(d_1,d_2)}(\sqrt{w}, w) = T\sqrt{w} - w = \min_i W_{(T/2,T/2)}(i,w), \quad (28)$$

が成り立つ．

以上より定理が成り立つ．

C 補題 6 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．ここで

$$V(w) = \begin{cases} 2\lceil\sqrt{w}\rceil - 1, & \text{if } (\lceil\sqrt{w}\rceil - 1)\lceil\sqrt{w}\rceil \geq w \\ 2\lceil\sqrt{w}\rceil, & \text{otherwise} \end{cases} \quad (29)$$

と定義すると，補題 5 と補題の条件より

$$\begin{aligned} &\min_i W(i, U(w')) - \min_i W(i, U(w)) \\ &= d_1\{V(w') - V(w)\} - \{U(w') - U(w)\} \\ &\geq \lceil\sqrt{U(w')}\rceil\{V(w') - V(w)\} - \{U(w') - U(w)\}, \end{aligned} \quad (30)$$

が成り立つ．

(1) $U(w) = \lceil\sqrt{w}\rceil^2$ のとき

$$\text{式(30)の最右辺} = \left\{\lceil\sqrt{U(w')}\rceil - \lceil\sqrt{U(w)}\rceil\right\}^2 \geq 0, \quad (31)$$

(2) $U(w) = \lceil\sqrt{w}\rceil(\lceil\sqrt{w}\rceil - 1)$ のとき

$$\text{式(30)の最右辺} = \left\{\lceil\sqrt{U(w')}\rceil - \lceil\sqrt{U(w)}\rceil\right\}^2 + \left\{\lceil\sqrt{U(w')}\rceil - \lceil\sqrt{U(w)}\rceil\right\} \geq 0, \quad (32)$$

が成り立つので，補題が成り立つ．