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.
IT2003-20 (2003-07)

バースト誤り通信路に適した低密度パリティ検査符号の構成法

細谷 剛† 八木 秀樹† 小林 学†† 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
†† 湘南工科大学工学部情報工学科 〒251-8511 神奈川県藤沢市辻堂西海岸 1-1-25
E-mail: †{hosoya,yagi,hirasawa}@hirasa.mgmt.waseda.ac.jp, ††kobayasi@info.shonan-it.ac.jp

あらまし 低密度パリティ検査 (LDPC) 符号の代表的な復号法である sum-product 復号法は，ランダム誤りに対するビット単位の事後確率 (APP) 復号法であるため，バースト誤り通信路など記憶のある通信路に対する LDPC 符号の復号法に関する研究が，近年盛んに行われている．本研究ではバースト誤りに適した LDPC 符号の構成法について検討を行う．まず，従来から用いられている構成法ではバースト誤りに対する復号性能が悪化する点を指摘する．さらにバースト誤りに適した構成法を提案する．その結果，ランダム誤りに対する復号性能を劣化させることなく，バースト誤りに対する復号性能が向上することをシミュレーションにより示す．

キーワード 低密度パリティ検査符号，sum-product 復号法，バースト誤り通信路

Construction Methods of Low-Density Parity-Check Codes for Burst Error Channels

Gou HOSOYA†, Hideki YAGI†, Manabu KOBAYASHI††, and Shigeichi HIRASAWA†

† Department of Industrial and Management Systems Engineering, School of Science and Engineering, Waseda University Okubo 3-4-1, Shinjuku-ku, Tokyo, 169-8555 Japan
†† Faculty of Engineering, Shonan Institute of Technology Tsujido Nishikaigan 1-1-25, Fujisawa-shi, Kanagawa, 251-8511 Japan
E-mail: †{hosoya,yagi,hirasawa}@hirasa.mgmt.waseda.ac.jp, ††kobayasi@info.shonan-it.ac.jp

Abstract The sum-product algorithm, a well-known decoding algorithm of Low-Density Parity-Check (LDPC) codes, is a bit-by-bit a posteriori probability decoding and assumes channels as memoryless. Iterative decoding algorithms of LDPC codes for channels with memory such as burst error channels have been widely studied in recent years. In this paper, we study construction methods of LDPC codes for burst error channels. We first point out that some conventional construction methods have weakness in error performance for burst error channels. Assuming the sum-prduct algorithm, we propose new construction methods of LDPC codes for burst error channels. We show by simulation results that codes constructed by proposed methods have robustness in error performance for burst error channels, compared to codes constructed by conventional methods. We show the proposed methods do not cause any degradation in error performance for memoryless channels.

Key words Low-Density Parity-Check codes, sum-product decoding algorithm, burst error channels

1. まえがき

低密度パリティ検査 (以下 LDPC) 符号 [2] [3] [6] は，1962 年に R.G.Gallager によって提案された後，長い間その存在が忘れられていたが，最近その復号性能が見直されて盛んに研究されている．LDPC 符号に対する代表的な復号法である sum-product 復号法は，LDPC 符号に対し確率的復号を繰り返し行うことにより，復号誤り確率を低減できる特徴を持つ．そのため，長い符号長の LDPC 符号に対して sum-product 復号法を用いることにより，Shannon 限界に迫る結果を達成できることが示されている [2] [3] [6] [8]．また，その復号計算量は符号長 N に対して $O(N)$ という高速性を併せ持つ [2] [3] [6]．

sum-product 復号法における復号過程では，通信路で発生する雑音は各ビットごとに独立であるランダム誤り，すなわち通信路が無記憶であることを仮定している．記憶のある通信路を仮定した場合，通信路の記憶を考慮した符号化・復号化が必要となる．記憶のある通信路の代表的な例として，Gilbert-Elliot 通信路 [7] など隠れマルコフモデルに基づくバースト誤り通信路が挙げられる．バースト誤りに対しては交錯法で雑音を無相関化し，ランダムな雑音として扱う復号法が一般的である．しかし，一般に同じ定常誤り確率のバースト誤り通信路とランダム誤り通信路では，バースト誤り通信路の方が通信路容量が大きいことが知られている [7]．そのため，バースト誤り通信路の雑音の相関性を利用することでより高い復号性能が期待できる．バースト誤りとして隠れマルコフ型雑音通信路を仮定し，その通信路に適した sum-product 復号法は [4] [5] [9] [11] において提案されている．これらの研究によってバースト誤りに適した復号法が提案されたが，雑音の生起が異なるランダム誤りとバースト誤りに対し，依然として同じ LPDC 符号の構成法が仮定されている．そこで本研究ではバースト誤りを考慮した LDPC 符号の構成法を提案する．提案する符号の構成法がランダム誤りに対する復号性能が劣化させることなくバースト誤りに対する復号性能の向上することを，シミュレーションにより示す．

2. 準 備

2.1 LDPC 符号 [2] [3] [6]

本論文では 2 元 LDPC 符号について考える．2 元 LDPC 符号は，検査行列 H に含まれる要素 1 が非常に少ない (疎な) 符号であり，検査行列の要素は殆ど 0 で構成され，要素 1 は確率的に配置される．ここで検査行列とは長さ N の任意の符号語 $\boldsymbol{c} = (c_1, c_2, \ldots, c_N) \in \{0,1\}^N$ に対し

$$\boldsymbol{c}H^{\mathrm{T}} = \boldsymbol{0}, \tag{1}$$

を満たす行列であり，符号を一意に定める†．疎な検査行列の

† T は転置を表す．

各行の重みと各列の重みがそれぞれ一定となるように構成される符号を正則 LDPC 符号という．本研究では正則 LDPC 符号のみを対象とし，以降単に LDPC 符号と呼ぶことにする．(N, w_r, w_c) LDPC 符号は符号長 N，行重み w_r，列重み w_c を持つ $M \times N$ の検査行列 H によって定義される．よって，式 (1) は LDPC 符号の任意の符号語が M 個の方程式 (以下パリティ検査方程式) を同時に満たさなければならないことを示している．ここで，$\rho \triangleq N/w_r$ と定義すると，$\rho = M/w_c$ が成り立つ．さらに，符号化率 R は $R \geq 1 - w_c/w_r$，検査行列 H の行数 M は $M = w_c\rho$ である．また，$w_c \geq 3, w_r > w_c$，$Nw_c \bmod w_r = 0$，を満足するようにパラメータ (N, w_r, w_c) は決定される．行列内のある要素 1 から行方向・列方向を交互に移動して自分自身に戻るまでの閉路をループといい，その移動回数 l をループの長さという．従って，長さ l は $l = 4, 6, 8, \cdots$，の値をとる．また，検査行列 H に存在する最小ループの長さを内径 g と呼ぶ．LPDC 符号は 2.2 節で述べる sum-product 復号法で復号を行う際に 2 部グラフの構造によって復号性能の良し悪しが左右される．検査行列 H が多数の短いループを持つ場合，復号性能に悪影響を及ぼすことが知られている．そこで，LDPC 符号を構成する際には検査行列 H の任意の 2 列に対し要素 1 の重なり個数が多くても 1 であるという制約を設ける．この制約により，長さ 4 のループが形成されることを回避できる [3] [6].

2.2 sum-product 復号法 [3]

sum-product 復号法は LDPC 符号の代表的な復号法であり，各ビットに対して事後確率 (APP) 復号を行う．この復号法は 2 元対称通信路 (BSC) や加法的白色ガウス雑音通信路 (AWGNC) など，通信路から発生する雑音系列は要素ごとに独立であることを仮定している．

受信語 $\boldsymbol{y} = (y_1, y_2, \ldots, y_N)$ の各時点 $n = 1, 2, \cdots, N$ に対して尤度 $\lambda_n(a)$ を

$$\lambda_n(a) = \Pr(y_n | c_n = a), a \in \{0, 1\}, \tag{2}$$

と表す．また，検査行列 $H = [H_{mn}]$ に対して次の 2 つの集合を定義する．

$$\mathcal{A}(m) \triangleq \{n : H_{mn} = 1\},\ \mathcal{B}(n) \triangleq \{m : H_{mn} = 1\}.$$

以下に sum-product 復号法を示す．ここで，最大繰り返し回数を l_{max} とおいている．

[sum-product 復号法]

s1) 初期化

$H_{mn} = 1$ の (m, n) に対して $r_{mn}(a) := 0.5, a \in \{0, 1\}$，とする．繰り返し数 $l := 1$ とする．

s2) 行処理

$H_{mn} = 1$ の (m, n) に対して，次式で外部値 $v_{mn}(a), a \in \{0, 1\}$，を更新する．

$$v_{mn}(a) := \sum_{\substack{c_{n'} \in \{0,1\}, n' \in \mathcal{A}(m) \backslash n, \\ \sum c_{n'} = a}} \prod_{n' \in \mathcal{A}(m) \backslash n} r_{mn'}(c_{n'}). \tag{3}$$

s3) 列処理

$H_{mn} = 1$ の (m, n) に対して，次式で事前値 $r_{mn}(a), a \in \{0, 1\}$，を更新する．

$$r_{mn}(a) := K_{mn}\ \lambda_n(a) \prod_{m' \in \mathcal{B}(n) \backslash m} v_{m'n}(a). \tag{4}$$

ここで K_{mn} は $\sum_{a \in \{0,1\}} r_{mn}(a) = 1$ を満たすように決められる正規化定数である．

s4) 推定符号語の計算

$\hat{\boldsymbol{c}} = (\hat{c}_1, \hat{c}_2, \cdots, \hat{c}_N)$ を以下のように求める．

$$\hat{c}_n = \arg \max_{a \in \{0,1\}} \lambda_n(a) \prod_{m \in \mathcal{B}(n)} v_{mn}(a), \quad n \in [1, N]. \tag{5}$$

s5) 終了条件

$l = l_{max}$ または $\hat{\boldsymbol{c}} H^{\mathrm{T}} = \boldsymbol{0}$ ならば，$\hat{\boldsymbol{c}}$ を復号語として出力し，アルゴリズムを終了する．それ以外の場合は，$l := l + 1$ として s2) へ行く． □

2.3 隠れマルコフ型雑音通信路

隠れマルコフ型雑音通信路は記憶のある通信路であり，バースト誤りを発生する．本論文では LDPC 符号の符号語 $\boldsymbol{c} = (c_1, c_2, \ldots, c_N) \in \{0, 1\}^N$ が通信路を介して送信されると仮定する．また $\boldsymbol{c}$ に隠れマルコフモデルに従う加法的雑音 $\boldsymbol{z} = (z_1, z_2, \ldots, z_N) \in \{0, 1\}^N$ が加わり，受信側において受信語 $\boldsymbol{y} = \boldsymbol{c} \oplus \boldsymbol{z}$ を受けとるものとする[†]．受信側では受信語 $\boldsymbol{y}$ から送信された符号語 $\boldsymbol{c}$ を推定する．隠れマルコフ型雑音通信路のパラメータを以下の 4 つ (状態数，出力記号，状態遷移確率，各記号の出力確率) により定義する．また，状態集合 $\mathcal{S}$ は L 状態から成り，$\mathcal{S} = \{S_1, S_2, \ldots, S_L\}$ で表される．出力記号の集合 $\mathcal{Z}$ は $\mathcal{Z} = \{0, 1\}$ とする．状態 $r \in \mathcal{S}$ から $s \in \mathcal{S}$ に遷移する状態遷移確率を $p(s|r)$ とする．定常性を仮定したとき，この隠れマルコフモデルは定常分布 $\boldsymbol{\pi} = (\pi_{S_1}, \pi_{S_2}, \ldots, \pi_{S_L})$ を持つ．π_r は状態 $r \in \mathcal{S}$ に滞在する平均の確率を表している．時点 $n = 1, 2, \cdots, N$ で状態遷移系列 $\boldsymbol{s} = (s_0, s_1, \cdots, s_N)$ に従い $z_n \in \mathcal{Z}$ が出力される．ただし，初期状態分布は定常分布とする．すなわち，$\Pr(s_0) = \pi_{s_0}$ である．状態 s_{n-1} から状態 s_n に遷移するとき，記号 $z_n \in \mathcal{Z}$ が出力される確率を $q_{s_n}(z_n)$ とする．このような記憶のある通信路を仮定することで，ある時点で滞在している状態によって，記号出力 (雑音発生) 確率が変化する．

また，隠れマルコフ型雑音通信路の平均誤り確率 p_{ave} は以下の式で求めることができる．

$$p_{ave} = \sum_{r \in \mathcal{S}} \pi_r q_r(1). \tag{6}$$

3. LDPC 符号の構成法

3.1 MacKay による構成法 [6]

D.J.C.MacKay による LDPC 符号の構成法は，全ゼロの行列に対して以下で述べる制約を付加して検査行列 H_M を構成する方法である．

m1) $M \times N$ の全零の行列 H_M に対し，w_c 個の列の要素を 1 に変換する．

m2) できる限り一定に w_r 個の行の要素を 1 に変換する．

m3) 任意の 2 列間の要素 1 の重なり個数は多くとも 1 とする．

m4) 内径 g をできる限り大きくする．

m5) $H_M = [H_M^{(1)} | H_M^{(2)}]$ と表す．ここで $H_M^{(1)}$ は $M \times (N - M)$ 行列，$H_M^{(2)}$ は $M \times M$ 行列とする．生成行列を構成するため，$H_M^{(2)}$ が正則となるよう構成する． □

ここで述べた制約は，符号化ができることかつ復号性能が良好な LDPC 符号を構成するための指標であるが，上の制約を満足する効率的な構成方法は知られていない．

3.2 Gallager による構成法 [2]

次に述べる Gallager による構成法 [2] は行重みと列重みが一定になるような構成法である．Gallager による構成法によって得られる検査行列 $H_G = [H_{Gmn}]$, $m \in [1, M]$, $n \in [1, N]$, は w_c 個の $\rho \times N$ 部分行列 $H_G^{(i)}, i = 1, 2, \cdots, w_c$, から成り，次式のように構成される．ここで，$N \bmod w_r = 0$ とする．

$$H_G = \begin{bmatrix} H_G^{(1)} \\ H_G^{(2)} \\ \vdots \\ H_G^{(w_c)} \end{bmatrix}. \tag{7}$$

それぞれの部分行列 $H_G^{(i)}$ の各列重みを 1，また各行重みを w_r に固定する．結果として H_G の各列の重みは w_c となる．部分行列 $H_G^{(1)}$ において，1 行目の 1 列目から w_r 列目までの要素を 1 とする．2 行目に対しては，$w_r + 1$ 列目から $2w_r$ 列目までの要素を 1 とする．同様に ρ 行目には，$(\rho - 1)w_r + 1$ 列目から ρw_r 列目までの要素を 1 とする．すなわち，$H_G^{(1)}$ の i 行 j 列成分を $H_{G_{ij}}^{(1)}$ で表すと，

$$H_{G_{ij}}^{(1)} \triangleq \begin{cases} 1, & j \in [(i-1)w_r + 1, iw_r]; \\ 0, & \text{otherwise}, \end{cases} \tag{8}$$

[†] $\oplus$ は排他的論理和を表す．

となる．部分行列 $H_G^{(i)}, 2 \leq i \leq w_c$, は，部分行列 $H_G^{(1)}$ の列を置換することにより得られる．

3.3 Poisson 構成法 [3]

Poisson 構成法 [3] は sum-product 復号法で復号する際，特に復号性能に悪影響を及ぼす短いループが発生しないよう比較的容易に構成することが可能な方法である．LDPC 符号の検査行列は確率的に構成するが，一般に (1) 行重みと列重みを一定にしつつ，(2) ループ 4 が発生しないという 2 つの制約を課して検査行列を構成することは難しい．Poisson 構成法は，Gallager の構成法と比較すると比較的容易に上記の制約 (1),(2) を満足する検査行列を構成することができる．

Poisson 構成法による (N, w_r, w_c) 正則 LDPC 符号の検査行列 $H_P = [H_{Pmn}]$, $m \in [1, M]$, $n \in [1, N]$, は，$w_r w_c$ 個の $\rho \times \rho$ 部分行列 $H_P^{(i,j)}$, $i \in [1, w_r]$, $j \in [1, w_c]$, から成る．ただし，$N \bmod w_r = 0$ とする．ここで $H_P^{(i,j)}$ の各行各列の重みは 1 である．検査行列 H_P は次式のように構成されるので，行重み w_r，列重み w_c の (N, w_r, w_c) LDPC 符号となることが保証される．

$$H_P = \begin{bmatrix} H_P^{(1,1)} & H_P^{(1,2)} & \cdots & H_P^{(1,w_r)} \\ H_P^{(2,1)} & H_P^{(2,2)} & \cdots & H_P^{(2,w_r)} \\ \vdots & \vdots & \ddots & \vdots \\ H_P^{(w_c,1)} & H_P^{(w_c,2)} & \cdots & H_P^{(w_c,w_r)} \end{bmatrix}. \quad (9)$$

4. バースト誤り通信路に適した LDPC 符号の構成法

近年，記憶のある通信路に適した LDPC 符号の復号法の研究が盛んに行われてきたことによって，ランダム誤り通信路と同様，マルコフ性を仮定したバースト誤り通信路に適した復号を行うことが可能になった [4][5][9][11]．ランダム誤り通信路に対する復号法とバースト誤り通信路に対する復号法は通信路雑音の尤度計算の方法が異なるだけであり，sum-proudct 復号法の部分は同じである．

ここで，sum-product 復号法の **s2) 行処理**に注目する．この処理では，あるパリティ検査方程式の注目するビット以外のビットに対して事前値を利用してその行が偶数重みと奇数重みである確率を計算している．ランダム誤りの場合，雑音の発生は i.i.d. であるため，パリティ検査方程式のビット位置（検査行列で行方向の要素 1 の位置）に注意する必要はない．一方バースト誤りは連続したビットに集中して誤りが発生するため，Gallager による構成法の第 1 部分行列 $H_G^{(1)}$ のように，各行の要素 1 同士が比較的近い距離にある各々のパリティ検査方程式には多くの誤りが発生する．MacKay による構成法 [6] で述べられている通り，LDPC 符号を構成する際に要素 1 同士の距離を考慮に入れる必要はない．しかし，バースト誤り通信路に対して LDPC 符号を用いる場合は，内径と同時にパリティ検査方程式の要素 1 同士の距離を考慮に入れて構成する必要がある．

本節では検査行列に対してバースト誤り通信路を考慮した LDPC 符号の構成法を提案する．

4.1 要素間距離を考慮した LDPC 符号

ここで検査行列 H の列番号インデックス $\mathcal{A}(m)$, $m = 1, 2, \cdots, M$, と行番号インデックス $\mathcal{B}(n)$, $n = 1, 2, \cdots, N$, を次式のように定義する．

$$\mathcal{A}(m) \triangleq \{n : H_{mn} = 1\} = \{n_{m,1}, n_{m,2}, \ldots, n_{m,w_r}\},$$

$$\mathcal{B}(n) \triangleq \{m : H_{mn} = 1\} = \{m_{n,1}, m_{n,2}, \ldots, m_{n,w_c}\}. \quad (10)$$

ただし，$n_{m,1} < n_{m,2} < \ldots < n_{m,w_r}$, $m_{n,1} < m_{n,2} < \ldots < m_{n,w_c}$ とする．

[定義 4.1] 検査行列の各行における隣り合う要素 1 同士の距離を要素間距離と呼ぶ．$\forall m \in [1, M]$, $\forall \gamma \in [1, w_r - 1]$ に対し，要素間距離 $D_{m\gamma}$ を次式で定義する．

$$D_{m\gamma} \triangleq n_{m,\gamma+1} - n_{m,\gamma}. \quad (11)$$

$D = [D_{m\gamma}]$ は検査行列 H の要素間距離を表す $M \times w_r$ 行列であり，要素間行列と呼ぶ． □

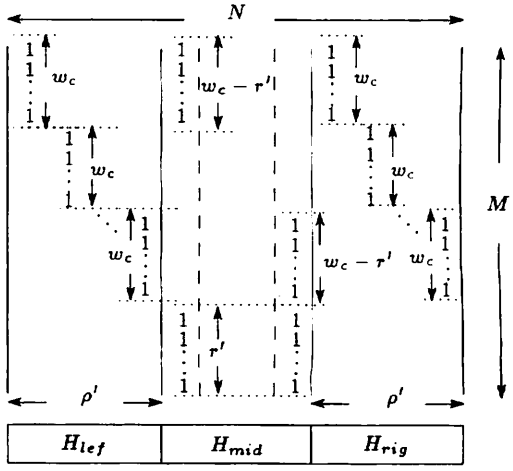

図 1 式 (14) が表す検査行列の構造の一例

要素間距離を大きくするためには，(1) 要素間行列 D の全要素の平均値 D_{ave} を大きく取ること，(2) 各々の要素間距離 $D_{m\gamma}$ がある閾値 δ 以上にすることの 2 通りのアプローチが考えられる．

[定義 4.2] D_{ave} を要素間行列 D の平均要素間距離と呼び，D の平均要素間距離と呼ぶ．D_{ave} は次式により定義する．

$$D_{ave} \triangleq \frac{1}{M(w_r - 1)} \sum_{m=1}^{M} \sum_{\gamma=1}^{w_r-1} D_{m\gamma}. \quad (12)$$

□

式 (11), (12) より次式が成り立つ．

$$\sum_{\gamma=1}^{w_r-1} D_{m\gamma} = n_{m,w_r} - n_{m,1}. \quad (13)$$

従って，D_{ave} は検査行列の各行の左端の要素 1 と右端の要素 1 の距離で決定される．平均要素間距離を大きくするには式 (13) を大きくするとよい．そこで，できる限り検査行列の各行の左端の要素 1 の列番号は小さく，右端の要素 1 の列番号は大きくすることを考える．今，検査行列 H が，

$$H \triangleq [H_{lef}, H_{mid}, H_{rig}], \quad (14)$$

の形であると仮定する．H_{lef}, H_{rig} は $M \times \rho'$ 行列であり，これらの部分行列の r' 行は行重みが 0，$M - r'$ 行は行重みが 1 であり，列重みは w_c であるとする．ただし，$M \bmod w_c \triangleq r'$, $\rho' \triangleq \frac{M - r'}{w_c} = \frac{N}{w_r} - \frac{r'}{w_c}$, とする．図 1 は，式 (14) の構造をもつ検査行列を表した一例である．行列 H_{lef} は検査行列 H の左から ρ' 列を成す．H_{lef} の左から ρ' 列には H の列番号インデックス $\mathcal{A}(m)$, $m = 1, 2, \cdots, M$, のうち，$n_{m,1}$ 列目のみが含まれると仮定する．同様に行列 H_{rig} は検査行列 H の右から ρ' 列を成す．H_{rig} の右から ρ' 列には H の列番号インデックス $\mathcal{A}(m)$, $m = 1, 2, \cdots, M$, のうち，n_{m,w_r} 列目のみが含まれると仮定する．ここで次の補題が成立する．

[補題 4.1] 式 (14) の構造をもつ検査行列は，式 (12) を最大にする． □

D_{ave} と符号のパラメータ (N, w_r, w_c) の間には次の定理が成り立つ．

[定理 4.1] (N, w_r, w_c) LPDC 符号の検査行列 H に対し D_{ave} は，次式を満足する．

$$D_{ave} \leq \rho. \quad (15)$$

(証明) 検査行列 H が D_{ave} を最大にする，式 (??) の形で構成できると仮定する．$\nu \in [1, \rho']$ に対し，

$$\#\{n_{m,1} = \nu\} = w_c, \quad (16)$$

となる[†††]．$\rho' + 1$ 列目には $n_{m,1} = \rho' + 1$ となる行が r' 行含ま

[†††] $\#\{\cdot\}$ は集合 $\{\cdot\}$ 要素数を表す．

れるため，

$$\#\{n_{m,1} = \rho' + 1\} = r', \tag{17}$$

が成り立つ．

また，検査行列 H の右端から $\rho'+1$ 列を成している H_{rig} にも同様のことが成り立つため，$\xi \in [N-\rho'+1, N]$ に対し，

$$\#\{n_{m,w_r} = \xi\} = w_c, \tag{18}$$

$$\#\{n_{m,w_r} = N - \rho'\} = r', \tag{19}$$

である．式 (13) に式 (12) を代入すると，

$$\begin{aligned} M(w_r-1)D_{ave} &= \sum_{m=1}^{M}\sum_{\gamma=1}^{w_r-1} D_{m\gamma}, \\ &= \sum_{m=1}^{M}(n_{m,w_r} - n_{m,1}), \\ &= \sum_{m=1}^{M} n_{m,w_r} - \sum_{m=1}^{M} n_{m,1}, \end{aligned}$$

となる．ここで，式 (16) ~ (19) より

$$\begin{aligned} &\sum_{m=1}^{M} n_{m,w_r} - \sum_{m=1}^{M} n_{m,1} \\ &= w_c\Big(\sum_{n\in[N-\rho'+1,N]} n - \sum_{n\in[1,\rho']} n\Big) \\ &\quad + r'\{(N-\rho') - (\rho'+1)\}, \\ &= w_c\rho'(N-\rho') + r'(N-2\rho'-1), \\ &= M(w_r-1)\times\rho + r'(\rho-\rho'-1), \\ &= M(w_r-1)\times\rho + r'\Big(\frac{r'}{w_c} - 1\Big). \end{aligned} \tag{20}$$

$M \bmod w_c = 0$ の場合は $r' = 0$ となるため，

$$D_{ave} = \rho, \tag{21}$$

が成り立つ．$M \bmod w_c \neq 0$ の場合は $w_c - r' > 0$ より式 (20) の第 2 項は負となるため，

$$D_{ave} < \rho, \tag{22}$$

となる．検査行列 H が式 (14) の形に構成できないときは，補題 4.1 より式 (22) となる．従って，式 (21), (22) より式 (15) が成立する． □

平均要素間距離は最小要素間距離の上界であるため，バースト誤りに適した検査行列は可能な限り式 (14) の形で検査行列を構成することが望ましい．

4.2 列置換を施した置換検査行列

LDPC 符号の性能はランダム性に依るところが大きいため，大きい要素間距離をもつという制約を付加して構成することでランダム性が失われる可能性がある．その結果，ランダム誤り通信路に対する性能が劣化する可能性がある．そこで，本研究ではランダム誤り通信路に対する性能が劣化させることなく大きい要素間距離の符号を構成する．要素間距離を変化させる方法として検査行列に対して列置換を施す手法が考えられる．検査行列 H に対して適当な列置換を施すことで等価かつ大きい要素間距離をもつ置換検査行列 $\tilde{H}$ が得られる．置換検査行列 $\tilde{H}$ は，もとの検査行列 H と比較した場合同じ符号語空間をもつため，ランダム誤りに対する最尤復号性能は変わらない．また，置換検査行列 $\tilde{H}$ は内径や 2 部グラフの構造に関して次の補題が成り立つ．

[補題 4.2] 検査行列 H に列置換を施した置換検査行列 $\tilde{H}$ の 2 部グラフの構造は，検査行列の H の 2 部グラフの構造と同じである．従って内径も同じである． □

検査行列の 2 部グラフの構造は sum-product 復号法での復号性能に大きな影響を与える．従って，列置換を施すことによってランダム誤り通信路に対する sum-product 復号法の復号結果に大きな影響を与える 2 部グラフの構造や最小距離は変化しない．

[定義 4.3] 検査行列 $H = [\boldsymbol{h}_1, \boldsymbol{h}_2, \ldots, \boldsymbol{h}_N]$ に対して，適当な列置換の結果得られた検査行列を $\tilde{H}$ とする．ここで，$\boldsymbol{h}_n$, $n = 1, 2, \cdots, N$, は n 列目の列ベクトルを表す．列置換後の検査行列を置換検査行列 $\tilde{H}$ とし，次式で定義する．

$$\tilde{H} = [\tilde{\boldsymbol{h}}_1, \tilde{\boldsymbol{h}}_2, \ldots, \tilde{\boldsymbol{h}}_N] \triangleq [\boldsymbol{h}_{\theta(1)}, \boldsymbol{h}_{\theta(2)}, \ldots, \boldsymbol{h}_{\theta(N)}]. \tag{23}$$

ただし，$\theta(n)$ は置換関数である．

置換検査行列 $\tilde{H}$ の行インデックス $\tilde{\mathcal{A}}(m)$, $m = 1, 2, \cdots, M$, と列インデックス $\tilde{\mathcal{B}}(n)$, $n = 1, 2, \cdots, N$, を次式で定義する．

$$\begin{aligned} \tilde{\mathcal{A}}(m) &\triangleq \{n : \tilde{H}_{mn} = 1\} = \{\tilde{n}_{m,1}, \tilde{n}_{m,2}, \ldots, \tilde{n}_{m,w_r}\}, \\ \tilde{\mathcal{B}}(n) &\triangleq \{m : \tilde{H}_{mn} = 1\} = \{\tilde{m}_{n,1}, \tilde{m}_{n,2}, \ldots, \tilde{m}_{n,w_c}\}. \end{aligned} \tag{24}$$

D_{ave} を大きくするため，列置換を行うことで検査行列を式 (14) の形に置換することが望ましいが，任意の LDPC 符号の検査行列が正確に式 (14) の形に構成できるとは限らない．式 (14) に近い形であり，最小要素間距離が大きい置換検査行列は以下の制約を満足するように構成することができる．

[要素間距離を考慮した列置換法]

最小要素間距離 δ を設定する．ただし，$\delta \leq \rho$ である．

C1) 式 (14) の形，または式 (14) 近い形になるよう検査行列に対して列置換を行う．

C2) $\forall m \in [1, M]$, $\forall \gamma \in [1, w_r - 1]$ に対して $D_{m,\gamma} \geq \delta$ となるように列置換を行う． □

上記の制約の困難さは **C2),C1)** の順となる．

4.3 Poisson 構成法に対する列置換手法

Poisson 構成法によって構成される検査行列 H_P は式 (14) の形になるため，必ず全要素の平均値 D_{ave} が与えられた (N, w_r, w_c) に対して最大の ρ になる．これは，Gallager による構成法や MacKay による構成法では必ずしも保証されない．そこで，H_P に対しては式 (14) の形を保ったまま列置換を行うことで，比較的容易に要素間距離が大きい検査行列を構成することができる．

[Poisson 構成法に対する列置換法]

I1) $i := 2$ とする．$n = 1, 2, \cdots, \rho$ に対して $\theta(n) := n$, $n = \rho+1, \rho+2, \cdots, N$ に対して $\theta(n) := 0$ とする．

I2) $n = \rho(i-1)+1, \rho(i-1)+2, \cdots, \rho i$, それぞれに対して **a), b)** を計算する．

- **a)** $\mathcal{B}(n) = \{m_{n,j}\}$ を満足する $j = 1, 2, \cdots, w_c$ に対して $\delta_{n,j} := \rho(i-1) + 1 - \tilde{n}_{m_{n,j},i-1}$ とする．
- **b)** $\delta_{min}(n) := \min_{j\in[1,w_c]} \delta_{n,j}$ とする．
- **c)** $n := \rho(i-1)+1$ とする．

I3) $\theta(n) := \arg\max_{n'\in[\rho(i-1)+1,ni]\setminus\theta(n')} \delta_{min}(n')$ とおく．

I4) $n = \rho i$ ならば $i := i+1$ として I2) へ行く．それ以外の場合は，$n := n+1$ として I3) へ行く． □

5. シミュレーションによる評価

5.1 評価条件

提案構成法に基づく LDPC 符号のバースト誤りに対する性能を評価するために，符号のパラメータが $(N, w_r, w_c) = (2040, 6, 3)$ の符号を用いてシミュレーションを行った．また，実験で用いる LDPC 符号の検査行列は内径 $g = 6$ とする．MacKay による構成法，Gallager による構成法，Poisson 構成法をもとに 3 種類の LDPC 符号を構成した．おのおのの構成法では 3 パターンの符号を構成し，復号結果にはその結果の平均をのせた．さらにその 3 種類の LDPC 符号に対してそれぞれ

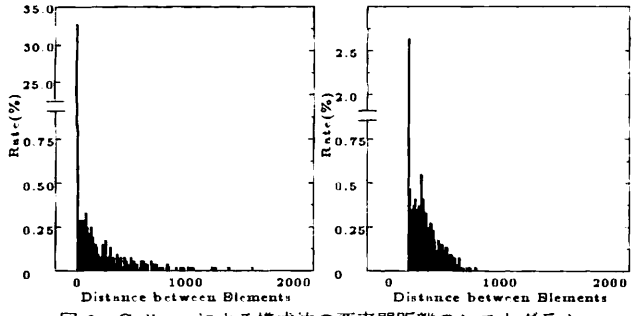

図 2 Gallagr による構成法の要素間距離のヒストグラム
左図は列置換前，右図は列置換後のヒストグラムである．

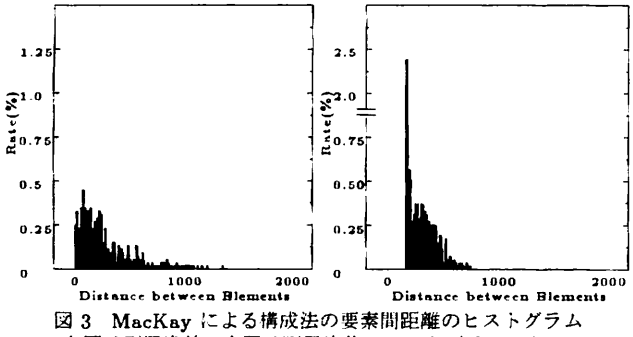

図 3 MacKay による構成法の要素間距離のヒストグラム
左図は列置換前，右図は列置換後のヒストグラムである．

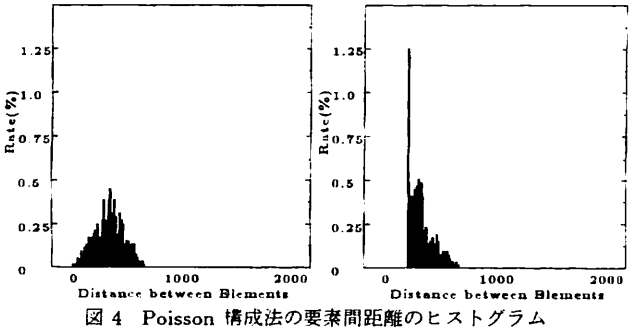

図 4 Poisson 構成法の要素間距離のヒストグラム
左図は列置換前，右図は列置換後のヒストグラムである．

列置換を行うことで置換検査行列を生成した．まず，MacKay による構成法と Gallager による構成法の検査行列は 4.2 節の列置換法を行う際に最小要素間距離 $\delta = 181$ とした．Poisson 構成法の検査行列に対しては 4.3 節の列置換法を行うことでそれぞれ最小要素間距離 $\delta = 202, 203, 207$ を得た．また，図 3 ～ 図 4 に 3 種類の構成法の要素間距離のヒストグラムを列置換前と列置換後に分けて示す．

隠れマルコフ型雑音通信路の状態数を 2 状態 $\mathcal{S} = \{S_1, S_2\}$ とする．各状態での誤り確率を $0 \leqq q_{S_1}(1) < q_{S_2}(1) \leqq 0.5$ とすることで，状態 S_1 は雑音の発生が少ない状態（以下 Good 状態），状態 S_2 は雑音の発生が多い状態（以下 Bad 状態）を表すことになる．

sum-product 復号法の最大繰り返し回数を $l_{max} := 200$ とする．復号後の符号語の復号誤り率 (WER) を評価尺度とする．

5.2 ランダム誤り通信路に対する復号結果

本研究で提案された LDPC 符号の構成法により得られる符号の性能がランダム誤り通信路に対して劣化しないことを計算機シミュレーションによって検証した．MacKay の構成法に基づく LDPC 符号を AWGNC に対して sum-product 復号法で復号した結果を図 5 に示す．3 パターンの符号それぞれについて全零の符号語を 10^6 個送信し，50 回復号に失敗した時点でシミュレーションを停止した．

図 5 より，列置換前と列置換後の符号の性能は同等であることが確認できる．

5.3 バースト誤り通信路に対する復号結果

隠れマルコフ型雑音通信路のパラメータはそれぞれ $q_{S_1}(1) = 0.01, q_{S_2}(1) = 0.5, p(S_1|S_2) = 0.025$ の場合について $p(S_2|S_1)$ を変化させることで定常誤り確率を変化させる．ここで平均バースト長 L_{burst} を次式で定義する[iii]．

$$L_{burst} = \sum_{n=1}^{\infty} n \times p(S_1|S_2)p(S_2|S_2)^{n-1} = \frac{1}{p(S_1|S_2)} \quad (25)$$

そのため，平均バースト長は 40 となる．

sum-product 復号法を用いて復号を行う際に 2 つの場合を仮定して尤度計算を行う．

復号法 A) 状態遷移系列が未知で状態推定を行わない
復号法 B) 状態遷移系列が既知

3 パターンの符号それぞれについて全零の符号語を 2×10^5 個送信し，50 回復号に失敗した時点でシミュレーションを停止した．

列置換を行うことにより，3 種類の構成法をもとにした LDPC 符号は列置換前と比較して全て性能が向上したことが確認された．また，復号法 A), 復号法 B) のそれぞれで列置換を行うことにより性能が向上した．列置換前と列置換後の性能の向上の度合いは，Gallager による構成法，MacKay による構成法，Poisson 構成法の順である．

図 2 に示す通り，Gallager による構成法は最小要素間距離が 1 であること，また図 2 からも確認できるように要素間距離が小さい値に分布が集中していることから，バースト誤り通信路には脆弱である．そのため，列置換を行うことで性能が大幅に向上した．図 3 に示す通り，MacKay による構成法は Gallager による構成法と比較して要素間距離が大きい．そのため，列置換を行うことで性能がある程度に向上した．図 4 に示す通り，Poisson 構成法はその他の構成法と比較して要素間距離の分布が平均して大きく，バースト誤りに対する性能が頑健であるためと考えられる．Poisson 構成法は列置換を行うことによる性能の差は殆ど確認することができなかった．

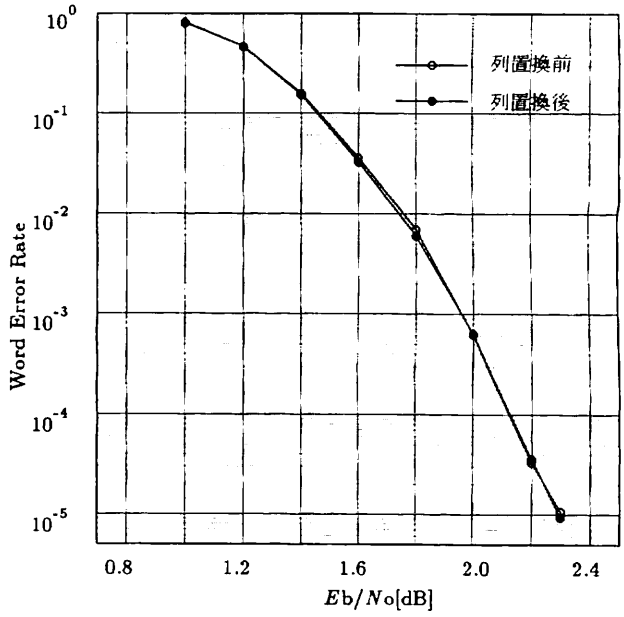

図 5 AWGNC に対する復号結果

6. まとめと今後の課題

バースト誤り通信路に対して頑健である LDPC 符号を構成するため，検査行列に対して要素間距離を考慮して列置換を行う構成法を提案した．さらにシミュレーションにより，提案した構成法の有効性を示した．

今後の課題として，列置換を行うことによるバースト誤り通

[iii] 本論文では，状態 S_2 (Bad 状態) に滞在する平均の長さを平均バースト長 L_{burst} と定義している．

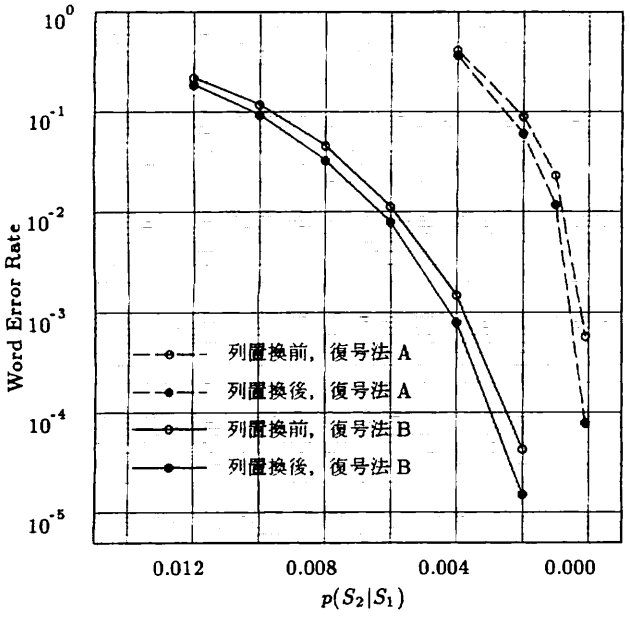

図 6 MacKay による構成法に対する復号結果
通信路は隠れマルコフ型雑音通信路を仮定する.

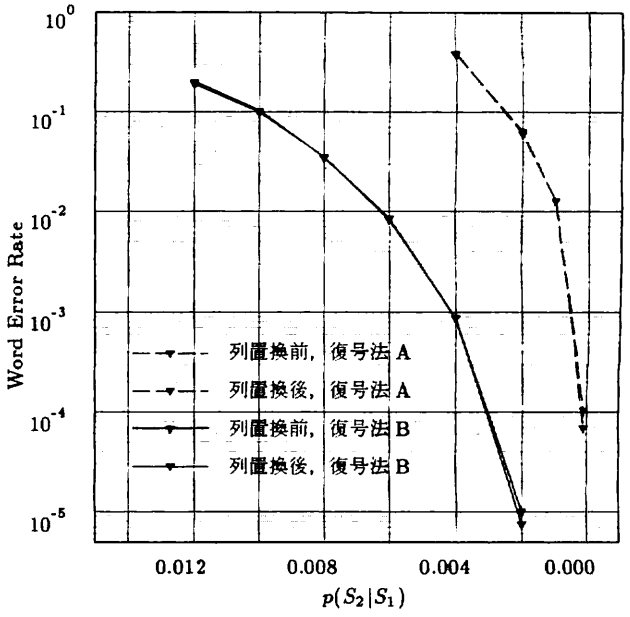

図 8 Poisson 構成法に対する復号結果
通信路は隠れマルコフ型雑音通信路を仮定する.

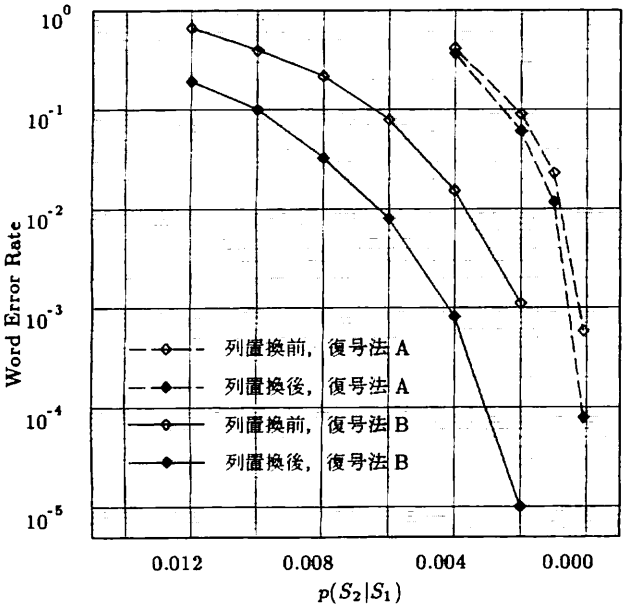

図 7 Gallager による構成法に対する復号結果
通信路は隠れマルコフ型雑音通信路を仮定する.

信路に対する性能の詳細な解析が挙げられる. また, バースト誤り通信路に適した LDPC 符号の復号法[4][5][9][11] に対して本研究で提案した符号が適していることを検証する必要がある. さらに, 要素間距離を考慮した構成法を行重みと列重みが不均一な非正則 LDPC 符号へ拡張することが挙げられる.

謝辞 著者の一人細谷は本研究を進めるにあたって有益なコメントを頂いた早稲田大学の松嶋敏泰教授, 平澤研究室の石田崇氏, 若狭心司氏をはじめ諸氏に深く感謝いたします. 本研究の一部は文部省科学研究費 (基礎研究 No.1576-0281) の助成による.

文 献

[1] L.R.Bahl, J.Coche, F.Jelinek,and J.Raviv, "Optimal decoding of linear codes for minimizing symbol error rate," *IEEE Trans. Inform. Theory*, vol.5, pp.284–287, Mar. 1974.

[2] R.G.Gallager, "Low density parity check codes," *IRE Trans. Inform. Theory*, vol.8, pp.21–28, Jan. 1962.

[3] R.G.Gallager, *Low density parity check codes*, MIT Press, 1963.

[4] J.Garcia-Frias, "Decoding of low-density parity check codes over finite-state binary Markov channels," *Proceeding of IEEE International Symposium on Information Theory*, Washington D.C., U.S.A., June 2001.

[5] 細谷 剛, 八木 秀樹, 小林 学, 平澤 茂一, "隠れマルコフ型雑音通信路に対する低密度パリティ検査符号の復号に関する一考察, パラメータ未知の通信路に対する一復号法, " 信学技報, IT2002-23, pp.19–24, 7 月, 2002.

[6] D.J.C.MacKay, "Good error-correcting codes based on very sparse matrices," *IEEE Trans. Inform. Theory*, vol.45, No.2, pp.399–431, March. 1999.

[7] M.Mushkin and I.Bar-David, "Capacity and coding for the Gilbert-Elliot channels," *IEEE Trans. Inform. Theory*, vol.35, No.6, pp.1277–1290, Nov. 1989.

[8] T.Richardson and R.Urbanke, "The capacity of low-density parity-check codes under message-passing decoding," *IEEE Trans. Inform. Theory*, vol.47, No.2, pp.599–618, Feb. 2001.

[9] T.Wadayama, "An iterative decoding algorithm of low density parity check codes for hidden Markov noise channels," *Proceeding of International Symposium on Information Theory and its Applications*, Honolulu, Hawaii, U.S.A, Nov. 2000.

[10] N.Wiberg, "Codes and decoding on general graphs," Ph.D.dissertation, Linköping Univ., Sweden, 1996.

[11] A.P.Worthen and W.E.Stark, "Low-density parity check codes for fading channels with memory," *Proceeding of the 36th Annual Allerton Conference on Communications, Control, and Computing*, 1998.

[12] A.P.Worthen and W.E.Stark, "Unified design of iterative raceivers using factor graphs," *IEEE Trans. Inform. Theory*, vol.47, No.2, pp.843–849, Feb. 2001.