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.
IT2003-32 (2003-07)

確率伝播型復号法に適した低密度パリティ検査符号
—巡回型LDPC符号の短縮化法—

贄田 里詩† 細谷 剛† 八木 秀樹† 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
E-mail: †{nieda,hosoya,yagi,hirasawa}@hirasa.mgmt.waseda.ac.jp

あらまし LDPC符号の代表的復号法である確率伝播型復号法は事後確率(APP)復号に基づいて雑音が混入した受信系列に対して復号を行う．その際，符号のパリティ検査行列中に存在する短いループによってその復号性能が悪化することが知られており，検査行列中に長さ4のループの存在しないLDPC符号の構成法が提案されている．本論文では，長さ4のループが持たない符号のうち巡回型のLDPC符号に対して，長さ6のループを多く取り除く短縮化法を提案する．また，提案した短縮化法によって得られたLDPC符号がsum-productアルゴリズムによる復号で優れた性能を持つことをシミュレーションにより示す．

キーワード LDPC符号，確率伝播型復号法，sum-productアルゴリズム，巡回符号，有限幾何符号，短縮化

Low-Density Parity-Check Codes for Decoding Algorithm based on Belief Propagation
— A shortening method for cyclic LDPC codes —

Satoshi NIEDA†, Gou HOSOYA†, Hideki YAGI†, and Shigeichi HIRASAWA†

† School of Science and Engineering, Waseda University Okubo 3-4-1, Shinjuku-ku, Tokyo, 169-8555 Japan
E-mail: †{nieda,hosoya,yagi,hirasawa}@hirasa.mgmt.waseda.ac.jp

Abstract Decoding algorithms based on belief propagation, which iteratively compute a posteriori probability of received symbols, are well-known as decoding methods for Low-Density Parity-Check (LDPC) codes. It is known that decoding algorithms based on belief propargation, such as sum-product algorithm, does not work well when there exist loops of short length in the parity-check matrix. For this problem, several researchers have proposed construction methods of LDPC codes whose parity-check matrices have no loops of length 4. In this paper, we devise a shortening method for cyclic LDPC codes. We show by computer simulations that shortened codes obtained by the devised method have good performances.

Key words LDPC code, algorithm based on belief propagation, sum-product algorithm, cyclic code, finite-geometry code, shortening method

1. はじめに

低密度パリティ検査（以下LDPC）符号[1]は，1960年にR.G.Gallagerによって提案され，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符号は確率伝播型復号法を繰り返し行うことにより，高い復号性能を得るという特徴を持つ．中でもsum-productアルゴリズム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計算機シミュレーションによって示されている[1]．

しかし，高い復号性能を得ることが示されている一方，その確定的な方法による構成方法は見出されていない．Gallagerは擬似ランダムに構成されるLDPC符号を提案しているが，今日までに見出されている高い復号性能を持つLDPC符号の多くは計算機により探索されており，符号長が大きいものは特に計算機によるところが大きい．擬似ランダムに構成されたLDPC符号は巡回性や擬巡回性といった代数的構造を持たないため，その符号化に大きな計算量が必要となる．さらに，最小Hamming距離の算出も困難である[2]．

また，LDPC符号の代表的復号法である確率伝播型復号法は，符号のパリティ検査行列を2部グラフとして表現したとき，ノードが情報を交換しながらシンボルの事後確率を計算していく復号法である．検査行列に短いループが存在するとき，ノード間で十分な情報交換がなされず，良い復号性能を示さないこ

とが知られている．特に，最も短い長さ4のループは復号性能に致命的な影響を与える[3]．

このような問題に対しては，T.Shibuyaらによるidempotentに基づいて構成される巡回符号[2]や，Y.Kouらによる有限幾何符号[4]といった代数的な試みによるLDPC符号の構成法が見出されている．この2つの構成法によって得られるLDPC符号は巡回符号であり，この巡回型LDPC符号の符号化は線形時間で行うことができる．さらに，長さ4のループが存在しない検査行列の構成法もそれぞれShibuyaら及びKouらによって与えられている．しかし，この2つの構成法によって得られる巡回型LDPC符号の検査行列には必ず長さ6のループが存在しており，長さ6のループが存在しない検査行列を得ることはできない．

本論文では，確率伝播型復号法を考慮した巡回型LDPC符号の短縮化法を提案する．まず，長さ4のループが存在しない巡回型LDPC符号に対して，その検査行列に存在する長さ6のループの構造を解析する．その解析に基づき，より多く長さ6のループを消去する符号の短縮化法を提案する．復号法としてsum-productアルゴリズムを仮定したシミュレーションを行うことにより，提案した短縮化法は削除した列数によらず有効であることを示す．

2. 準　　備

2.1 通信路モデル

符号長n，情報記号数k，最小距離dのパラメータを持つ2元線形(n,k,d)符号Cを考える．符号Cが与えられたとき，任意の符号語$\boldsymbol{c}\in C$に対して$\boldsymbol{cH}^{\boldsymbol{T}}=\boldsymbol{0}$を満たす行列$\boldsymbol{H}$をパリティ検査行列という(注1)．また，符号語$\boldsymbol{c}=(c_1,c_2,\ldots,c_N)$はガウス雑音通信路を介して送信される際に雑音系列$\boldsymbol{e}$の影響を受け，復号器側では受信語$\boldsymbol{y}=(y_1,y_2,\ldots,y_N)$を受け取る．このとき，通信路として2元対称通信路(BSC)や加法的白色ガウス雑音(AWGN)通信路を仮定すると，発生する雑音系列$\boldsymbol{e}$は要素ごとに独立である．また，復号器では$\boldsymbol{y}$から送信された符号語を推定する．

2.2 LDPC符号

本論文では2元LDPC符号について取り扱う．2元LDPC符号は，検査行列に含まれる要素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で構成されている．ここで，各列の重みと各行の重みがそれぞれ一定となるように構成されるLDPC符号をregular LDPC符号と呼び，重みが一定でない符号をirregular LDPC符号と呼ぶ．また，LDPC符号のパリティ検査行列において，1である行列要素を全ての行，列ごとにpathでつなげた際にできる閉路をループといい，閉路が持つ辺の数が$q=4,6,8,\ldots,$のループをループqと呼ぶ．

2.3 sum-productアルゴリズム[5]

LDPC符号の代表的な復号アルゴリズムであるsum-productアルゴリズムは，2部グラフ上における確率伝播型復号法であり，各シンボルに対して事後確率(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(AWGN)通信路など，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．

[定義1]　符号語$\boldsymbol{c}$が与えられたとき，受信語$\boldsymbol{y}$の各時点$i=1,2,\cdots,n$に対して対数尤度比(LLR)を

$$\lambda_i \stackrel{\text{def}}{=} \ln\frac{\Pr(y_i|c_i=0)}{\Pr(y_i|c_i=1)}. \tag{1}$$

と表わす．パリティ検査行列$\boldsymbol{H}$に対して次式を定義する．

$$A(i)\stackrel{\text{def}}{=}\{j|H_{ij}=1\},\quad B(j)\stackrel{\text{def}}{=}\{i|H_{ij}=1\}.$$

さらに，次式を定義する．

$$\mathrm{sign}(x)\stackrel{\text{def}}{=}\begin{cases}1, & x\geqq 0;\\ -1, & x<0,\end{cases}\qquad f(x)\stackrel{\text{def}}{=}\ln\frac{e^x+1}{e^x-1}.$$

□

以下にsum-productアルゴリズムを示す．ここで，繰り返し数の最大値をt_{max}で表す．

[sum-productアルゴリズム]

s1) 初期化

$H_{ij}=1$の(i,j)に対して，$\beta_{ij}:=0$とする．繰り返し数$t:=1$とする．

s2) 行処理

$H_{ij}=1$の(i,j)に対して，次式でα_{ij}を求める．

$$\alpha_{ij}:=\prod_{j'\in A(i)\backslash j}\mathrm{sign}(\lambda_{j'}+\beta_{ij'})\times f\left(\sum_{j'\in A(i)\backslash j}f(|\lambda_{j'}+\beta_{ij'}|)\right). \tag{2}$$

s3) 列処理

$H_{ij}=1$の(i,j)に対して，次式でβ_{ij}を求める．

$$\beta_{ij}:=\sum_{i'\in B(j)\backslash i}\alpha_{i'j}. \tag{3}$$

s4) 推定符号語の計算

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

$$\hat{c}_j:=\begin{cases}0, & \lambda_j+\sum_{i\in B(j)}\alpha_{ij}>0\ ;\\ 1, & \text{otherwise}\ .\end{cases} \tag{4}$$

s5) 終了条件

$t=t_{max}$または$\hat{\boldsymbol{c}}\boldsymbol{H}^{\mathbf{T}}=\boldsymbol{0}$ならば，推定系列$\hat{\boldsymbol{c}}$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，$t:=t+1$としてs2)へ行く．□

sum-productアルゴリズムにおいて良い復号性能を得るためには，2部グラフ上のノード間で十分な信頼度情報の交換を行うことが必要となる．そのため，パリティ検査行列に短い長さのループが存在するとき，十分な情報交換がなされず良い復号性能を示さないことが知られている[3]．

また，確率伝播に基づく反復復号法は，多くの場合，sum-productアルゴリズム，もしくはその近似アルゴリズムとみなすことができる[5]．

3. 巡回型LDPC符号

巡回符号であるLDPC符号を巡回型LDPC符号と呼ぶ．巡回型LDPC符号の検査行列は，各行がそれぞれ巡回置換関係にある．

3.1 idempotentに基づく巡回符号[2][6]

$GF(2)$上のidempotent $e(x)=e_0+e_1x+\ldots+e_{n-1}x^{n-1}$は，$e(x)\equiv\{e(x)\}^2\equiv e(x^2)\ (\mathrm{mod}\ x^n-1)$を満たす$n-1$次

(注1)：ここでTは行列の転置を示す

多項式である．ここで，$e_i \in GF(2), i = 0, 1, \ldots, n-1$，である．idempotent $e(x)$ の求め方を以下に述べる．n を正奇数，p を n 未満の非負整数とするとき，以下で定義される集合を巡回コセットと呼ぶ．

$$C_p^n \stackrel{\text{def}}{=} \{p2^i \bmod n \mid i = 0, 1, \ldots, m_p - 1\}. \tag{5}$$

但し，m_p は $p2^{m_p} \equiv p \pmod{n}$ を満たす最小の正整数で，要素の同じ C_p^n は p の値の小さい C_p^n を残し，残された p の集合を $P^n = \{p_1, p_2, \ldots\}$ と定義する．このとき $e(x)$ は以下のように表現される．

$$e(x) = \sum_{p \in P} \sum_{i \in C_p^n} x^i. \tag{6}$$

ここで，P は P^n の部分集合である．式 (6) で得られる idempotent $e(x)$ から，巡回符号 C のパリティ検査行列 $\boldsymbol{H}$ を以下のように構成できる．

$$\boldsymbol{H} = \begin{bmatrix} e_0 & e_1 & e_2 & \cdots & e_{n-1} \\ e_{n-1} & e_0 & e_1 & \cdots & e_{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ e_1 & e_2 & e_3 & \cdots & e_0 \end{bmatrix}. \tag{7}$$

3.2 有限幾何 LDPC 符号 [7]

有限幾何符号は有限幾何学の性質に基づいて構成される符号で，有限幾何 $\boldsymbol{G}$ は N 個の点，J 本の線と次のような構造を持つ空間として定義される．

（1） 全ての線は ρ 個の点を持つ．

（2） 点と点は必ず唯一の線で接続される．

（3） 全ての点は γ 本の線と交差する．

（4） 線と線は平行であるか，唯一の点で交差する．

$GF(2^s)$ 上の m 次元 Euclid 幾何を $EG(m, 2^s)$ で表わす．$EG(m, 2^s)$ は 2^{ms} 個の点と $2^{(m-1)s}(2^{ms}-1)/(2^s-1)$ 本の線から構成されており，それぞれの線は 2^s 個の点から成る．また，点は $GF(2^s)$ 上の m 次元ベクトルで，点 $\mathbf{0} = (0, 0, \ldots, 0)$ を origin と呼ぶ．それゆえ，$EG(m, 2^s)$ は $GF(2^s)$ 上の m 次元ベクトル空間であり，$GF(2^s)$ の m 次拡大体 $GF(2^{ms})$ と見なすことができる．また，線を成す 2^s 個の点は $EG(m, 2^s)$ の 1 次元部分空間 $EG(1, 2^s)$ を構成する．Kou らは [4] において，$EG(m, 2^s)$ に基づく regular LDPC 符号である EG-LDPC 符号について述べている．

いま，$\boldsymbol{v} = (v_0, v_1, \ldots, v_{2^{ms}-2})$ を $GF(2)$ 上の $(2^{ms}-1)$ 次元ベクトルとし，α を $GF(2^{ms})$ の原始元とする．ここで，$GF(2^{ms})$ を $EG(m, 2^s)$ とみなすことにより，$\boldsymbol{v}_L = (v_0, v_1, \ldots, v_{2^{ms}-2})$ は $EG(m, 2^s)$ の線 L が点 α^i を含むとき $v_i = 1$，点 α^i を含まないとき $v_i = 0$ とする．このとき，$\boldsymbol{v}_L$ を線 L の付随ベクトルといい，付随ベクトルを行とするパリティ検査行列によって定義される符号を $EG(m, 2^s)$ 符号といい，その符号長は 2^{ms} である．パリティ検査行列の列数は $\boldsymbol{v}$ の次元数であり origin 以外の点の総数である $2^{ms}-1$ となる．また，行数は origin を含む線以外の線の総数であり，$(2^{(m-1)s}-1)(2^{ms}-1)/(2^s-1)$ となる．

$m = 2$ のとき，$EG(m, 2^s)$ 符号のパリティ検査行列は行数，列数ともに $2^{2s}-1$ となり，各行は $EG(2, 2^s)$ の任意の線の付随ベクトル $\boldsymbol{v}$ の巡回置換により構成することができる．$EG(2, 2^s)$ 符号のパリティ検査行列は巡回性をもった $(2^{2s}-1) \times (2^{2s}-1)$ 正方行列となり，$EG(2, 2^s)$ 符号を 2-D EG 符号と呼ぶ．2-D EG 符号のパリティ検査行列は行重みが 2^s，列重みが 2^s となる．従ってパリティ検査行列は s の値が大きくなるにしたがって疎な行列となり，2-D EG 符号は巡回型 LDPC 符号となる．これを 2-D EG-LDPC 符号と呼ぶ．

3.3 有限幾何符号の短縮化法 [4]

有限幾何符号についての短縮化法が Kou らによって提案されている．いま，(n, k) 2-D EG-LDPC 符号について考える．このとき，2-D EG-LDPC 符号のパリティ検査行列から 1 次元部分空間 $EG(1, 2^s)$ を構成する点に対応する列を削除する．また，$EG(1, 2^s)$ の 2^s 個の点が成す線を L とすると，L の付随ベクトル $\boldsymbol{v}_L$ に対応する行の重みは 0 となるのでパリティ検査行列から対応する行を取り除くことにより，$(2^{2s}-1) \times (2^{2s}-2^s-1)$ 行列を得る．この短縮化法によって得られる短縮符号のパラメータは $(n-2^s, k-2^s+1)$ である．短縮符号のパリティ検査行列の行重みは，L と平行である線の付随ベクトルに対応する行の重みは 2^s であり，L と交差する線の付随ベクトルに対応する行の重みは 2^s-1 となる．また，列重みは 2^s のままで一定となる．短縮化された 2-D EG-LDPC 符号は irregular LDPC 符号となるが，その行重み，列重みはほぼ一定である．

4. 巡回 LDPC 符号の短縮化法

符号長や情報記号数といったパラメータの限られてくる巡回符号に対して，任意に設定したパラメータを得るために検査行列の列削除による短縮化を行うことが多い．本節では，巡回符号のループ 6 の構造を解析し，より多くのループ 6 を削除できる列の選定法を示す．削除する列数を Y とおくと，この選定法における Y の値は符号長 n 未満の任意の値をとることができる．(n, k, d) 符号のパリティ検査行列を Y 列削除することにより $(n-Y, k-Y, D)$ 符号が得られる．但し，$d \leq D$ である [8]．

4.1 巡回型 LDPC 符号の検査行列に存在するループ 6

パリティ検査行列の任意の行において，要素が 1 である列番号の集合を E で定義する．$\forall u, v \in E$ に対し，その差集合 L を次式で定義する．

$$L \stackrel{\text{def}}{=} \left\{ l_i \;\middle|\; l_i \equiv u - v \pmod{n},\ i \leqq 2\binom{\|E\|}{2} \right\}. \tag{8}$$

ただし，$\|E\|$ は集合 E の要素数を表わす．

巡回型 LDPC 符号の検査行列の各行はおのおの巡回置換の関係であるため，得られる差集合 L は行番号に依存しない．

[補題 1] [2] 巡回型 LDPC 符号のパリティ検査行列にループ 4 が存在する必要十分条件は，差集合 L に同じ値の要素が存在することである． □

[補題 2] 巡回型 LDPC 符号のパリティ検査行列にループ 6 が存在する必要十分条件は，$x, y, z \in L$ に対し，

$$x + y = z \tag{9}$$

が成り立つことである． □

式 (9) を満たす x, y, z の関係は図 1 のように表せる．式 (3)

$$\boldsymbol{H} = \left[\begin{array}{c} \overset{z}{\overbrace{\qquad\qquad}} \\ \underset{x}{\underbrace{\qquad\qquad}} \qquad \underset{y}{\underbrace{\qquad\qquad}} \end{array} \right]$$

図 1 ループ 6 の一般表現

よりパリティ検査行列の各行はそれぞれ巡回置換関係にあるため，ある (x,y,z) の組から形成されるループ 6 は符号長 n の数だけ存在する．

[定理 1] idempotent に基づく巡回符号の検査行列中には必ずループ 6 が存在する． □

(証明) 式 (6) において $\|P\|=1$ である $e(x)$ を $e_1(x)$ とおく．すなわち，

$$e_1(x)=\sum_{i\in C_p^n} x^i. \tag{10}$$

である．さらに，$\|P\|\geqq 2$ である $e(x)$ を $e_2(x)$ とおく．このとき，式 (6) より，全ての $e_1(x)$ から構成される検査行列にループ 6 が存在するならば，$e_2(x)$ から構成される検査行列にも必ずループ 6 が存在する．以下で $e_1(x)$ から構成される検査行列にはループ 6 が存在することを示す．

i) $\|C_p^n\|=1$ の場合

式 (5) より，$2p\equiv p \pmod n$ が成り立つ．また，n が正奇数，p が n 未満の非負整数であるため，唯一 $p=0$ のときのみ $\|C_p^n\|=1$ となるが，$p=0$ のとき $e_1(x)$ は構成できない．

ii) $\|C_p^n\|=2$ の場合

このとき，$2^2p\equiv p \pmod n$ が成り立つ．これを満たすのは $p=n/3$，または $n=3$ のときである．$p=n/3$ のとき，$C_p^n=\{n/3,2n/3\}$ となり，$e_1(x)$ の差集合が $L=\{n/3,2n/3\}$ となるので，$x=n/3, y=n/3, z=2n/3$ のとき，補題 2 よりループ 6 が存在する．また，$n=3$ のとき巡回コセットは C_1^3 のみ存在しており，$p=n/3$ であるので同様にループ 6 が存在する．従って $\|C_p^n\|=2$ のとき $e_1(x)$ から構成される検査行列にはループ 6 が存在する．

iii) $\|C_p^n\|\geqq 3$ の場合

$C_p^n=\{p,2p,4p,\ldots\}$ であり，$e(x)$ の差集合は $L=\{p,2p,\ldots\}$ となるので，$x=p$, $y=p3$, $z=2p$ のとき，補題 2 よりループ 6 が存在することがわかる．

i)，ii)，iii) より，$e_1(x)$ から構成される検査行列には必ずループ 6 が存在することがわかり，ゆえに $e_2(x)$ から構成される検査行列にも必ずループ 6 が存在する． □

また，有限幾何符号に対しては，Kou らが [4] において，有限幾何符号の検査行列にループ 6 が必ず存在することを示している．

4.2 ループ 6 の構造解析

ループ 4 が存在しないパリティ検査行列を $\boldsymbol{M}$ と表わすとき，補題 1 より $\boldsymbol{M}$ から得られる集合 L に同じ値の要素は存在しない．このとき，L の要素を考慮することによって，$\boldsymbol{M}$ に存在するループ 6 の構造の解析ができる．

ここで，2-D EG-LDPC 符号のパリティ検査行列の各行の関係も，$i=0,1,\ldots,n-2$ に対し $i+1$ 行目は i 行目の 1 ビット巡回置換であると仮定しても一般性は失われないことに注意されたい．

[定義 2] 検査行列において，式 (2) を満たす 3 要素 $l_1,l_2,l_3\in L$ から形成されるループ 6 と，そのループ 6 を巡回置換したループ 6 は等価であるという． □

[定義 3] 式 (2) を満たす 3 要素を $l_1,l_2,l_3\in L$ とする．$j\in\{1,2,3\}$ に対し，$\Omega_j=\{l_j,n-l_j\}$ を定義し，その要素を $\omega_j\in\Omega_j$ と表わす．このとき，式 (11), (12) を同時に満たす $\omega_{\tau_1},\omega_{\tau_2},\omega_{\tau_3}\in\{\omega_1,\omega_2,\omega_3\}$, $\tau_1\neq\tau_2\neq\tau_3$, が存在する

$$\min_{\omega_j\in\Omega_j}\sum_{j=1}^{3}\omega_j \tag{11}$$

$$\omega_{\tau_1}=\omega_{\tau_2}+\omega_{\tau_3}. \tag{12}$$

l_1,l_2,l_3 が形成するループ 6 と等価なループ 6 の集合をループ 6 の規則といい，その規則を $F(\omega_{k_1},\omega_{k_2},\omega_{\tau_1})$, $k_1,k_2\in\{\tau_2,\tau_3\}$, $k_1\neq k_2$, で表わす． □

規則 $F(\omega_{k_1},\omega_{k_2},\omega_{\tau_1})$ とは，図 1 において $x=\omega_{k_1}$, $y=\omega_{k_2}$, $z=\omega_{\tau_1}$ であるループ 6 の巡回置換による集合である．

また，定義 3 より $l_1,l_2,l_3\in L$ が形成するループ 6 は $F(\omega_{\tau_2},\omega_{\tau_3},\omega_{\tau_1})$ と $F(\omega_{\tau_3},\omega_{\tau_2},\omega_{\tau_1})$ の 2 つの規則に属することがある．この 2 つの規則を区別する方法を以下の補題 3 で述べる．ここで，ω_{τ_2}, ω_{τ_3} は差集合 L の要素であるため，おのおの集合 E の 2 要素からなる．いま，$\omega_{\tau_2}\equiv u_{\tau_2}-v_{\tau_2} \pmod n$ かつ，$\omega_{\tau_3}\equiv u_{\tau_3}-v_{\tau_3} \pmod n$, $u_{\tau_2},v_{\tau_2},u_{\tau_3},v_{\tau_3}\in E$, と仮定する．

[補題 3] l_1,l_2,l_3, が形成するループ 6 は，

i) もし $v_{\tau_2}=u_{\tau_3}$ ならば，$F(\omega_{\tau_2},\omega_{\tau_3},\omega_{\tau_1})$ に属する．

ii) もし $v_{\tau_3}=u_{\tau_2}$ ならば，$F(\omega_{\tau_3},\omega_{\tau_2},\omega_{\tau_1})$ に属する．

iii) $v_{\tau_2}\neq u_{\tau_3}$ または $v_{\tau_3}\neq u_{\tau_2}$ ならば 2 つの規則 $F(\omega_{\tau_2},\omega_{\tau_3},\omega_{\tau_1})$ と $F(\omega_{\tau_3},\omega_{\tau_2},\omega_{\tau_1})$ に属する． □

[補題 4] $l=3/n$, となる要素 $l\in L$ が存在するならば，ループ 6 の規則 $F\left(\frac{n}{3},\frac{n}{3},\frac{2n}{3}\right)$ が存在する．この規則に属するループ 6 は互いに $l=n/3$ ビット巡回置換の関係となる． □

4.3 ループ 6 の規則に基づく手法

ループ 4 が存在しないパリティ検査行列 $\boldsymbol{M}$ において，規則 $F\left(\frac{n}{3},\frac{n}{3},\frac{2n}{3}\right)$ 以外のループ 6 の規則数を θ とし，この θ の規則を F_i, $i=1,2,\ldots,\theta$, と表し，規則 $F\left(\frac{n}{3},\frac{n}{3},\frac{2n}{3}\right)$ を $F_{\theta+1}$ と表す．また変数 η を規則 $F_{\theta+1}$ が存在するとき $\eta=1$，存在しないとき $\eta=0$ とすると，検査行列 $\boldsymbol{M}$ には $n(\theta+\frac{1}{3}\eta)$ 個のループ 6 が存在する．

ループ 6 は 3 列から成るため，検査行列の任意の列に対して各規則 F_i, $i=1,2,\ldots,\theta$, に属するループ 6 が必ず 3 つずつ依存している．従って検査行列の 1 列を削除すると 1 規則につき 3 つのループ 6 が除かれる．しかし，ある 3 列に依存するループ 6 に対して，その 3 列のうちの 2 列を削除してもその規則に属するループ 6 は高々5 つしか削除することができない．また，規則 $F_{\theta+1}$ については 1 列に依存するループ 6 は必ず 1 つであり，ある 3 列に依存するループ 6 において，その 3 列のうちの 2 列を削除しても規則 $F_{\theta+1}$ のループ 6 は 1 つしか削除することはできない．このことにより，検査行列 $\boldsymbol{M}$ から 1 列を削除するならばどの列を選んでも削除されるループ 6 の数は $3\theta+\eta$ であるが，2 列目以降を削除する際は，選択する列によりループ 6 の削除される数が変わる．

[定義 4] 規則 $F(l_1,l_2,l_3)$, $l_1,l_2,l_3\in L$, は図 1 において $x=l_1$, $y=l_2$, $z=l_3$ であるループ 6 の巡回置換による集合である．このとき $x=l_1$ の左端点と $z=l_3$ の左端点が依存する列を $F(l_1,l_2,l_3)$ の左列，$x=l_1$ の右端点と $y=l_2$ の左端

点が依存する列を中央列，$y = l_2$ の右端点と $z = l_3$ の右端点が依存する列を右列と呼ぶ． □

[定義 5] 規則 F_i $i = 1, 2, \ldots, \theta + 1$, に対して，左列が検査行列 $\boldsymbol{M}$ の j 列目にあるループ 6 を $Loop6(F_i, j)$ と表わす． □

以下で提案する短縮化法では，各列に依存するループ 6 を表すリストを用意し，1 列を削除する度に各列に依存するループ 6 の数を求め，値が大きい列を次に削除していく．

まず，各列に対しメモリサイズ $3 \times \theta + \eta$ のリストを用意する．$j = 1, 2, \ldots, n$, $i = 1, 2, \ldots, \theta + \eta$, それぞれについて，$Loop6(F_i, j)$ が依存する列のリストに対し，$Loop6(F_i, j)$ を登録する．

[提案アルゴリズム]

(1) $t := 0$ とする．

(2) もし $t = 1$ ならば，任意の列を削除する．そうでないならば，リストに基づいてループ 6 が依存する数が最も多い列を ξ_t 列目として削除する．

(3) ξ_t 列目と共に削除されたループ 6 が依存している他の列に対し，その列が持つリストを更新する．

(4) $t = t_{max}$ ならば，アルゴリズムを終了する．そうでないならば，(2) へ行く． □

この提案した短縮化法によって得られる検査行列は，削除する列数 Y に対して一意に定まる．

5. シミュレーションによる評価および考察

本節では計算機シミュレーションを行い，結果の考察を行う．

5.1 シミュレーション条件

巡回型 LDPC 符号を C，パリティ検査行列を $\boldsymbol{M}$，符号化比率を R とする．また，$\boldsymbol{M}$ の Y 列を削除することにより得られるパリティ検査行列，短縮化符号とその符号化比率をそれぞれ $\boldsymbol{M}^{(Y)}$, $C^{(Y)}$, $R^{(Y)}$ と表わす．

1)idempotent に基づく巡回符号の短縮化

2 つの idempotent に基づく巡回符号 (n=255, k=127) 符号 C_a と (1023, 511) 符号 C_b を短縮化する．C_a に対して，$Y = 42$, 72, とすることにより，$R_a^{(42)} = 0.4$, $R_a^{(72)} = 0.3$ である $C_a^{(42)}$, $C_a^{(72)}$ を得る．このとき，提案短縮化法によって Y 列を削除した検査行列をそれぞれ 1 つ (a-提案-$R_a^{(Y)}$)，ランダムに Y 列を削除して得られる検査行列をそれぞれ 3 つずつ用意する．C_b についても同様に，$Y = 170, 292$, とすることにより，$R_b^{(170)} = 0.4$, $R_b^{(292)} = 0.3$ である $C_b^{(170)}$, $C_b^{(292)}$ を得る．提案短縮化法によって Y 列を削除した検査行列をそれぞれ 1 つ (b-提案-$R_b^{(Y)}$)，ランダムに Y 列を削除して得られる検査行列をそれぞれ 3 つずつ用意する．

2)EG-LDPC 符号の短縮化

2-D EG-LDPC 符号について，$s = 4$ の (255,175) 符号 C_c と，$s = 5$ の (1023,781) 符号 C_d を短縮化する．C_c に対しては，$Y = 2^s = 16$ と定めることにより Kou らの短縮化法によって短縮化符号が得られる．このとき，提案短縮化法によって 16 列を削除した検査行列を 1 つ (c-提案)，Kou らの短縮化法によって得られる検査行列を 1 つ (c-Kou) 用意する．C_d に対しては，$Y = 2^s = 32$ と定めることにより Kou らの短縮化法によって短縮化符号が得られる．提案短縮化法によって $Y = 32$ 列を削除した検査行列を 1 つ (d-提案)，Kou らの短縮化法によって得られる検査行列を 1 つ (d-Kou) 用意する．

3) 短縮化符号に対するシミュレーション条件

通信路として加法的白色ガウス雑音通信路を仮定し，それぞれの短縮化符号に対し，sum-product アルゴリズムによる復号を行う．この際，繰り返し回数を $t_{max} = 200$ とする．また，評価尺度を bit error rate とする．

5.2 結　　果

表 1 から表 4 に，C_a, C_b, C_c, C_d の列削除前と列削除後のループ 6 の数を示し，表 5 と表 6 に，C_c, C_d の列削除後の行重みの分布を示す．また，復号後の bit error rate を図 2, 3, 4 に示す．表及び図中では，idempotent に基づく巡回符号をもとにし，ランダムに列を削除して得られる 3 つの短縮化符号に対する平均の値を示している．符号 C_a に対する結果を Ave(a-R-$R_a^{(Y)}$)，符号 C_b に対する結果を Ave(b-R-$R_b^{(Y)}$) で表わす．

表 1. 符号 C_a とその短縮化符号におけるループ 6 の数

列削除前	列削除後		
M_a		a-提案-$R_a^{(Y)}$	Ave(a-R-$R_a^{(Y)}$)
3.162×10^4	$Y = 42, R_a^{(42)} = 0.4$	1.742×10^4	1.838×10^4
	$Y = 72, R_a^{(72)} = 0.3$	1.032×10^4	1.147×10^4

表 2. 符号 C_b とその短縮化符号におけるループ 6 の数

列削除前	列削除後		
M_b		b-提案-$R_b^{(Y)}$	Ave(b-R-$R_b^{(Y)}$)
2.405×10^5	$Y = 170, R_b^{(170)} = 0.4$	1.335×10^5	1.391×10^5
	$Y = 292, R_b^{(292)} = 0.3$	7.962×10^4	8.695×10^5

表 3. 符号 C_c とその短縮化符号におけるループ 6 の数

列削除前	列削除後		
M_c		c-提案	c-Kou
2.152×10^6	$Y = 16$	1.750×10^6	1.770×10^6

表 4. 符号 C_d とその短縮化符号におけるループ 6 の数

列削除前	列削除後		
M_d		d-提案	d-Kou
1.575×10^6	$Y = 32$	1.427×10^6	1.432×10^6

表 5. 符号 C_c の短縮化符号における行重みの分布

行重み		c-提案	c-Kou
14		15	0
15		226	240
16		14	14

表 6. 符号 C_d の短縮化符号における行重みの分布

行重み		d-提案	d-Kou
30		31	0
31		962	992
32		30	30

5.3 考　　察

表 1 から 4 より，提案短縮化法により列削除をした場合，ランダムに列削除した場合や，Kou らの短縮化法により短縮化した場合に比べ，より多くのループ 6 を削除できていることがわかる．また，図 2, 3, 4 から，提案短縮化法により得られた短縮化符号は，ランダムに列を削除した短縮化符号に比べ復号性能が優れており，Kou らの短縮化法によって得られた短縮化符号と同程度の復号性能を示すことがわかる．

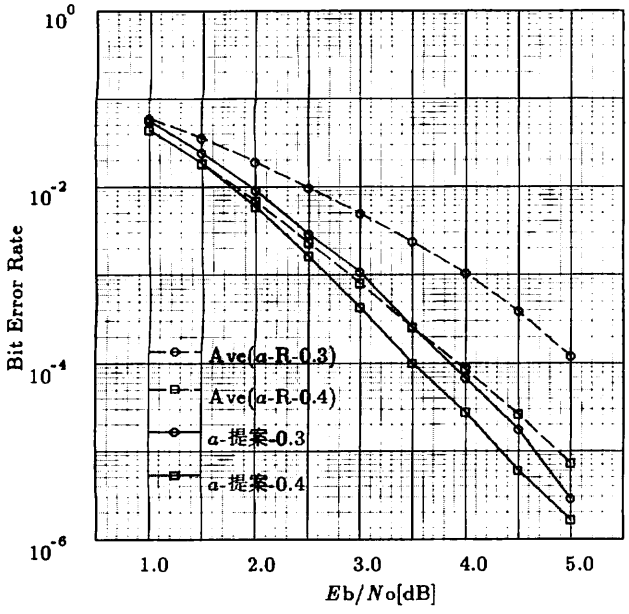

図 2　符号 C_a の短縮化符号の復号性能

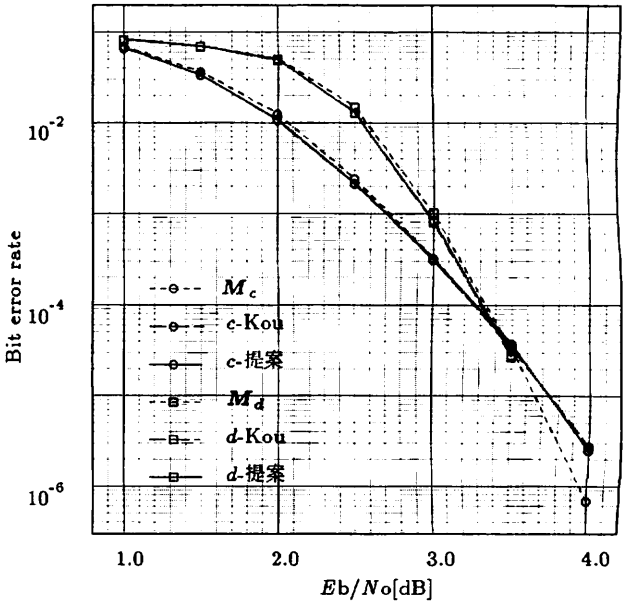

図 4　符号 C_c, C_d とその短縮化符号の復号性能

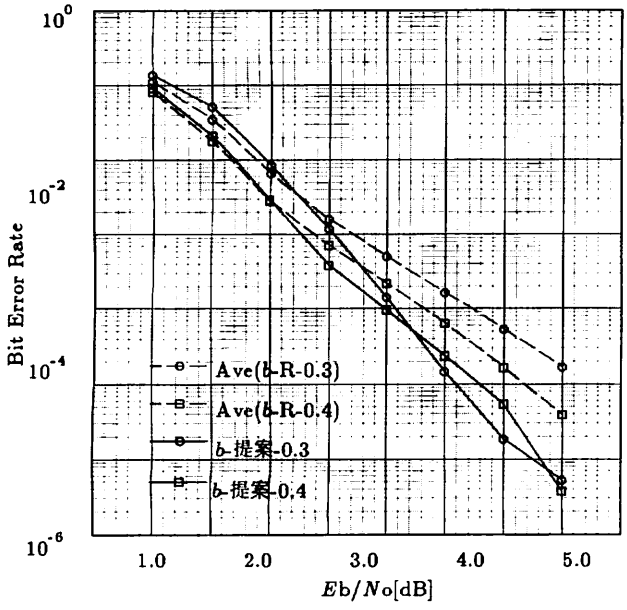

図 3　符号 C_b の短縮化符号の復号性能

列削除による最小距離の変化は基本的に起こらないことより，ランダムに列を削除した短縮化符号と提案短縮化法により列を削除した短縮化符号の復号性能はループ 6 の数に大きく依存しているためと考えられる．また表 5, 6 より，ほぼ regular な Kou らの短縮化法によって得られた短縮化符号と提案短縮化法によって得られた短縮化符号が同程度の復号性能を示したことについてもループ 6 の数に起因しているためと考えられる．

6. まとめと今後の課題

本論文では，巡回型 LDPC 符号の検査行列に存在するループ 6 の構造を解析し，ループ 6 を数多く取り除く短縮化法を提案した．また，提案短縮化法により得られた短縮化符号は sum-product アルゴリズムで復号する際に良い性能を達成すること示した．

提案短縮化法では，必ずしも短縮化された検査行列に存在するループ 6 の数を最小化する保証はなく，短縮化された検査行列に存在するループ 6 の数を最小化する最適探索法を開発することが今後の課題として挙げられる．また，重みの分布と短い長さのループの関係が復号性能に対してどのように影響するか解析することも今後の課題として挙げられる．

7. 謝　　辞

本研究を行うにあたり，数多くのご助言，ご支援を賜わりました，早稲田大学 李相協先生，石田崇氏，若狭心司氏，並びに早稲田大学平澤研究室の各氏に感謝いたします．

文　　献

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

[2] T.Shibuya and K.Sakaniwa, "Factor graphs for cyclic codes with no cycles of length four", *Proceedings of the 24th Symposium on Information Theory and Its Applications*, Kobe, Hyogo, Japan, December 4–7, 2001.

[3] F.R.Kschischang, B.J.Frey, and H.-A.Loeliger, "Factor graphs and the sum-product algorithm", *IEEE Trans. Inform. Theory*, vol. 47, pp. 489–519, Feb. 2001.

[4] Y.Kou, S.Lin, and M.P.C.Fossorier, "Low-Density Parity-Check Codes Based on Finite Geometries: A Rediscovery and New Results", *IEEE Trans. Inform. Theory*, vol. 47, pp. 2711-2736, Nov. 2001.

[5] 和田山正, 低密度パリティ検査符号とその復号法, トリケップス社, p43-94, 2002.

[6] F.J.MacWilliams and N.J.A.Sloane, *The Theory of Error-Correcting Codes*, North-Holland Publishing Company, 1977.

[7] S.Lin and D.J.Costello,Jr, *Error Control Coding:Fundamentals and Applications*, Prentice-Hall,Inc., 1983.

[8] 今井秀樹, 符号理論, 電子情報通信学会, p36-93, 1990.