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.

[招待講演] 多元LDPC符号とその応用

笠井　健太†

† 東京工業大学 大学院理工学研究科集積システム専攻
E-mail: †kenta@comm.ss.titech.ac.jp

あらまし　近年，中程度の符号長の復号性能が高いことから，多元 LDPC 符号が注目されている．本稿では多元 LDPC 符号の研究を概観し，可変符号化率符号化，レートレス符号，量子誤り訂正符号への応用を紹介する．
キーワード　多元 LDPC 符号，可変符号化率符号，レートレス符号，量子誤り訂正符号

Non-binary LDPC Codes and Their Applications

Kenta KASAI†

† Dept. of Communications and Integrated Systems, Tokyo Institute of Technology
E-mail: †kenta@comm.ss.titech.ac.jp

Abstract　Recently, non-binary LDPC codes attract much attention for their decoding performance for moderate code length. We review the known results on non-binary LDPC codes, and the applications to rate-compatible coding, rateless coding and quantum error correction.
Key words　non-binary LDPC codes, rate-compatible codes, rateless codes, quantum error correcting codes

1. はじめに

通信路容量に任意に近い符号化率で，任意に低い誤り率かつ現実的な計算量で通信を行うことは，誤り訂正技術に携わる者にとって，かつては実現不可能とも思われていた究極の目標であった．この目標は，非正則 LDPC 符号 [1] によって現実的に満足され，Polar 符号 [2] によって達成可能であることが厳密に証明された．Polar 符号は，符号化が構成的で復号が驚くほど単純であるにも関わらず，広い範囲の応用問題に対して最適な符号化と低い計算量の復号法を与えることができる．LDPC 符号および Polar 符号によって，無限の符号長では最適な符号を手に入れられるようになった．しかし，有限の符号長の場合にはどうだろう．

Polyanskiy らは，符号長 n で，ブロック誤り率 P_{B} を達成可能な符号の最大符号語数 $M^*(n, P_{\mathrm{B}})$ が漸近的に

$$\log M^*(n, P_{\mathrm{B}}) = nC(\epsilon) - \sqrt{nV(\epsilon)}Q^{-1}(P_{\mathrm{B}}) + O(\log n)$$

と近似できる事を示した [3]．ここで，ϵ は通進路を規定するパラメータ，$V(\epsilon)$ は例えば，クロスオーバー確率 ϵ の BSC なら $V = \epsilon(1-\epsilon)+\log^2\left(\frac{1-\epsilon}{\epsilon}\right)$，消失確率 ϵ の BEC なら $V = \epsilon(1-\epsilon)$ と与えられる．上の式を書き換えると，

$$P_{\mathrm{B}} = Q\left(\frac{\sqrt{n}(C(\epsilon) - R^*)}{\sqrt{V}(\epsilon)}\right)(1 + o(1)) \qquad (1)$$

となる．ただし，$R^* := \frac{1}{n}\log M^*(n, P_{\mathrm{B}})$ である．図 1 に，通信路容量 $C = 1/2$ の Binary Symmetric Channel (BSC) と Binary Erasure Channel (BEC) で，ブロック誤り率 10^{-3} を達成する最適な符号の符号化率 $R^* = \frac{1}{n}\log M^*$ と符号長 n をプロットした．あるブロック誤り率 P_{B} を保ったまま，ギャップ $C(\epsilon) - R^*$ を半分にするためには，最適な符号を使ったとしても符号長を 4 倍にしなければならないことを，式 (1) は表している．ある程度低いブロック誤り率 P_{B} に対して，高いスループット $R^*(1 - P_{\mathrm{B}})$ を達成するためには，符号化率 R^* を大きくすればよい．符号化・復号化にかかるレイテンシ・計算複雑度・回路規模は符号長に対して少なくとも線形に増えてしまう．ある程度の長さの十分に最適化された効率的に復号可能な符号があれば，それ以上符号長を数倍に伸ばしてスループットを数%増やそうとすることは現実的ではない．有限長の最適な復号性能に，有限長の LDPC 符号はどの程度接近しているのだろうか．

今までと視点を変えて，符号化率 R のある符号が，ブロック誤り率 P_{B} を達成することが可能な通信路容量 $C(\epsilon)$ の最小値を考えよう．式 (1) から，最適な符号に対するこの値を計算することができる．BEC において，符号化率 1/2 の各種符号が，ブロック誤り率 10^{-3} を達成することが可能な通信路容量 $C(\epsilon)$ の最小値をプロットした．有限長の 2 元 (3,6) 正則 LDPC 符号に関する，ウォータフォール領域のブロック誤り率は，次の様に書けることが予想されており，BEC では厳密に証明されている [4].

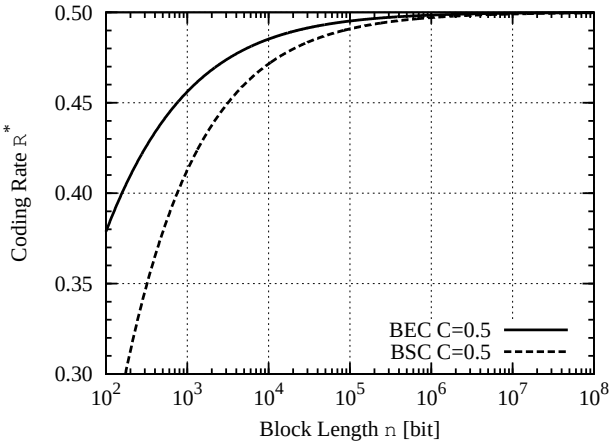

図 1　通信路容量 $C = 1/2$ の通信路で，ブロック誤り率 10^{-3} を達成する最適な符号の符号化率 $R^* = \frac{1}{n}\log M^*$ と符号長 n の関係

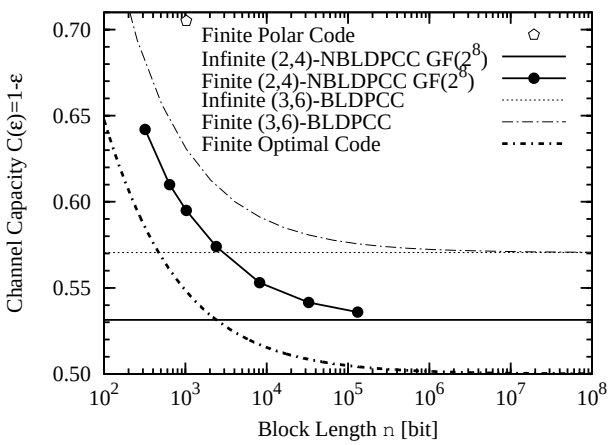

図 2　BEC において，符号化率 1/2 の符号が，ブロック誤り率 10^{-3} を達成するために耐えられる通信路容量 $C(\epsilon)$ の最小値

$$P_{\mathrm{B}} = Q\left(\frac{\sqrt{n}(C(\epsilon) - C(\epsilon^*))}{\alpha}\right)(1 + o(1)) \qquad (2)$$

ただし，ϵ^* は LDPC 符号の閾値 [5]，α は LDPC 符号の次数分布から決まる定数である．ギャップ $C(\epsilon) - C(\epsilon^*)$ を半分にするために支払うこの符号長の交換レートは，最適な符号と同じように，LDPC 符号に対しても 4 倍になっている(注1)．非正則 LDPC 符号は，高い閾値を有しているが符号長が数千より短い符号では高いエラーフロアが現れてしまう傾向がある．公平な比較のため，および筆者の実験データ収集能力の限界から，低いエラーフロアを有する符号のみを対象に比較している．短い符号長で最適な符号に近い復号性能を示している点列が，本稿で扱う多元 LDPC 符号によるものである．

多元 LDPC 符号は Gallager によって発明され [7]，Davey と MacKay [8] によって 2 元 LDPC 符号を凌ぐ復号性能を有すことが発見された．近年短い符号長から高い復号性能を有する符号として注目されている．本稿では，近年開発された多元 LDPC 符号に関する構成法，復号法，解析法，多種問題への応用を紹介する．

2. 多元 LDPC 符号とその構成および復号法

多値の変調方式に応用するという自然な使われ方 [9] ばかりでなく，2 元入力通信路に対しても，多元 LDPC 符号は 2 元 LDPC 符号に比べて優れた復号性能を有している．

符号化，復号に必要な演算を簡単にするために，多元 LDPC 符号はガロア体 GF(2^m) 上で定義することが一般的であるが，本稿では，代数に不慣れな読者のために，2 元 $m \times m$ 部分行列からなる行列 $H \in (\{0,1\}^{m\times m})^{M\times N}$ によって定義される $\{0,1\}^m$ 上の 2^m 元 LDPC 符号 C_1 を扱うこととする．

$$C_1 = \{(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_N) \mid H(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_N)^T = \boldsymbol{0}\},$$

(注1)：通信路容量を達成する Polar 符号列に対して，逐次除去復号法によって復号されたあるブロック誤り率 P_{B} を保ったまま，符号化率と通信路容量の間のギャップを半分にするためには BEC では 12.35 倍，2 元入力 AWGN 通信路では 16.08 倍の符号長が必要なことが経験的に知られている [6].

$$H = \begin{pmatrix} A_{1,1} & \cdots & A_{1,N} \\ \vdots & \ddots & \vdots \\ A_{M,1} & \cdots & A_{M,N} \end{pmatrix} \in \{0,1\}^{mM\times mN},$$

$$\boldsymbol{x}_v = (x_{v,1}, \ldots, v_{v,m})^T \in \{0,1\}^m, v = 1, \ldots, N$$

ただし $A_{c,v} \in \{0,1\}^{m\times m}$ はサイズ $m \times m$ の正則行列または 0 行列である．ビット $x \in \{0,1\}$ に対して，$\boldsymbol{x} \in \{0,1\}^m$ を多元シンボル，または単にシンボルと呼ぶこととする．非零部分行列の数によって H の列重みと行重みを定義する．

2 元 LDPC 符号の場合，パリティ検査行列の列重みを非正則なものにすることで，その復号性能を大幅に改善することが可能であった．しかし多元 LDPC 符号の場合には，この列重みの非正則化による効果がほとんどないことが知られている．2^m 元 LDPC 符号では $m \geqq 6$ なら，列重みが 2 であるパリティ検査行列を有するものが最良であることが知られている [10]．つまり，2 元 LDPC 符号に対しては復号性能の向させていたパリティ検査行列の列重み分布の非正則化，および Multi-edge type LDPC 符号 [11] や Protograph LDPC 符号 [12] などによるタナーグラフの構造化が，$m \geqq 6$ の多元 LDPC 符号に対してはほとんど効果がない．多元 LDPC 符号では $m < 6$ なら，パリティ検査行列の列重み分布の非正則化によって復号性能をある程度改善することができる [10, Fig. 3.5]．しかし本稿では，その復号性能の高さを理由に，$m \geqq 6$ である $(2, d_{\mathrm{c}})$-正則 2^m 元 LDPC 符号のみを扱うこととする．

2.1 符号の構成法

2 元 LDPC 符号の設計とは，パリティ検査行列の非零成分，つまり 1 の位置を決めることとみなすことができる．一方，多元 LDPC 符号の設計には，非零部分行列 $A_{c,v} \neq 0$ の位置 (c, v) だけではなく，その値 $A_{c,v} \in \{0,1\}^{m\times m}$ のとりかたにも自由度がある．

まず，タナーグラフのサイクルの最小サイズができるだけ大きく，かつ列重みが 2 であり行重みが d_{c} となるようにパリティ検査行列の非零部分行列の位置を定める．非零部分行列の値 $A_{c,v} \in \{0,1\}^{m\times m}$ を定める方法として，次の方法が知られて

いる．

Davey ら [8] と Poulliat ら [13] は，多元 LDPC 符号を構成する各単一パリティ検査符号のビットを単位とする最小ハミング距離を最大にするような非零成分の組み合わせを，各行の非零成分として用いると，ウォータフォール領域の復号性能が改善できることを発見した．

パリティ検査行列の中で列重みと行重みが共に 2 であるような小さな部分行列が非正則となると，小さな重みの符号語が存在する様な符号になってしまう．Poulliat ら [13] は，この様な小さな部分行列が正則になる様に非零行列を選ぶことで，エラーフロア領域の復号性能が改善できることを発見した．

しかし，これらの符号の最適化法も $m \geqq 7$ に対しては，有意な改善が見られなくなり，ランダムに非零部分行列の値を決定すれば，十分良い性能を引き出すことができる．列重みが 2 であるが，部分行列のサイズ m を大きくするにしたがって，エラーフロアが深くなる傾向があり，$m \geqq 8$ では情報ビット数 $k \geqq 1024$，符号化率 1/2 の多元 LDPC 符号では，AWGN 通信路に対して少なくともブロック誤り率 10^{-7} までエラーフロアを観測することがきない．

2.2 復号アルゴリズム

多元 LDPC 符号の復号法である Sum-Product 復号法は，行処理と列処理によってサイズ 2^m の各反復段階 $\ell \geqq 0$ で対応するタナーグラフが木である時に，シンボル MAP 復号 $\hat{\boldsymbol{x}}_v = \mathrm{argmax}_{\boldsymbol{x}\in\{0,1\}^m} \Pr(X_v = \boldsymbol{x}|Y_1, \ldots, Y_N)$ となるアルゴリズムとなっている．$v = 1, \ldots, N$, $c = 1, \ldots, M$ に対して $V_c := \{v \mid A_{c,v} \neq 0\}$, $C_v := \{c \mid A_{c,v} \neq 0\}$ とする．$A_{c,v} \neq 0$ である c, v に対して，メッセージと呼ばれる確率ベクトル $p_{vc}^{(\ell)}$ と $p_{cv}^{(\ell)}$ を更新していく．

初期化: $v = 1, \ldots, N$, $c = 1, \ldots, M$, $\boldsymbol{x} \in \{0,1\}^m$ に対して

$$p_{vc}^{(0)}(\boldsymbol{x}) = p_v^{(0)}(\boldsymbol{x}) = \Pr(X_v = \boldsymbol{x}|Y_v = y_v)$$

y_v は $\boldsymbol{x}_v$ に対応する通信路からの出力であり，ビット毎に無記憶な通信路に対しては，$\boldsymbol{x} = (x_1, \ldots, x_m)$ と $y_v = (y_{v,1}, \ldots, y_{v,m})$ を用いて次のように書くことができる．

$$\Pr(X_v = \boldsymbol{x}|Y_v = y_v) = \prod_{i=1}^{m} \Pr(X_{v,i} = x_i|Y_{v,i} = y_{v,i})$$

行処理: $v = 1, \ldots, N$, $c = 1, \ldots, M$, $\boldsymbol{x} \in \{0,1\}^m$ に対して

$$\tilde{p}_{vc}^{(\ell-1)}(A_{vc}\boldsymbol{x}) = p_{vc}^{(\ell-1)}(\boldsymbol{x}),$$
$$\tilde{q}_{cv}^{(\ell)} = \bigotimes_{v'\in V_c\setminus\{v\}} \tilde{p}_{v'c}^{(\ell-1)},$$
$$q_{cv}^{(\ell)}(\boldsymbol{x}) = \tilde{q}_{cv}^{(\ell)}(A_{vc}\boldsymbol{x})$$

ただし，$\otimes$ は畳み込みを表す．正確に書くと，

$$(p_1 \otimes p_2)(\boldsymbol{x}) = \sum_{\boldsymbol{y},\boldsymbol{z}\in\{0,1\}^m : \boldsymbol{x}=\boldsymbol{y}+\boldsymbol{z}} p_1(\boldsymbol{y})p_2(\boldsymbol{z}).$$

となり，これは m 次元 DFT $\mathcal{F}[p](\boldsymbol{z}) = \sum_{\boldsymbol{x}\in\{0,1\}^m} p(\boldsymbol{x})(-1)^{\boldsymbol{x}\cdot\boldsymbol{z}}$, と IDFT $\mathcal{F}^{-1}[P](\boldsymbol{x}) = 2^{-m}\sum_{\boldsymbol{z}\in\{0,1\}^m} P(\boldsymbol{z})(-1)^{\boldsymbol{x}\cdot\boldsymbol{z}}$, $\boldsymbol{x}\cdot\boldsymbol{z} = (x_1, \ldots, x_m)\cdot(z_1, \ldots, z_m) = \sum_{i=1}^m x_i z_i$ を使ってフーリエ領域で次のように書くことができる．

$$\mathcal{F}[p_1 \otimes p_2](\boldsymbol{z}) = \mathcal{F}[p_1](\boldsymbol{z})\mathcal{F}[p_2](\boldsymbol{z})$$

これは FFT によって，$O(m2^m)$ 回の加算と乗算によって高速に計算可能である [14].

列処理: $v = 1, \ldots, N$, $c = 1, \ldots, M$, $\boldsymbol{x} \in \{0,1\}^m$ に対して

$$p_{vc}^{(\ell)}(\boldsymbol{x}) = \mu p_v^{(0)}(\boldsymbol{x}) \prod_{c'\in C_v\setminus\{c\}} q_{cv'}^{(\ell)}(\boldsymbol{x}) \text{ for } x \in \{0,1\}^m$$

ただし，μ は $\sum_{\boldsymbol{x}\in\{0,1\}^m} p_{vc}^{(\ell)}(\boldsymbol{x}) = 1$ となるように決められた定数である．

シンボル判定: $v = 1, \ldots, N$, $\boldsymbol{x} \in \{0,1\}^m$ に対して

$$\hat{\boldsymbol{x}}_v^{(\ell)} = \mathop{\mathrm{argmax}}_{\boldsymbol{x}\in\{0,1\}^m} p_v^{(0)}(\boldsymbol{x}) \prod_{c'\in C_v} q_{c'v}^{(\ell)}(\boldsymbol{x})$$

$c = 1, \ldots, M$ に対して，$(\hat{\boldsymbol{x}}_1, \ldots, \hat{\boldsymbol{x}}_N) \in C_1$ となるまで，行処理と列処理を繰り返す．

並列処理ができるものの，1 回の行処理と列処理にかかる計算量は $O(Nm2^m)$ であり，この復号法は，サイズ 2^m の確率ベクトルを更新していくので，$O(N2^m)$ のメモリが必要となってしまう．Declercq らは [14] 確率ベクトルの要素のうち，有意なものだけを扱うことにより必要なメモリを削減した復号法を提案している．対数領域の Sum-Product 復号法 [15] を用いることにより，量子化レベルを低く抑えることができるが，FFT による行処理の高速計算ができなくなってしまう．そこで，筆者らは [16]，フーリエ対数領域でベクトルを更新していくことにより，行処理と列処理の関係を逆転させ，復号計算の並列性を高めた復号アルゴリズムを提案している．これらの低計算量のアルゴリズムを以ってしても，低い量子化レベル，少ないメモリ，少ない計算量，高い復号性能に同時を満たす復号アルゴリズムの要求に対する，十分な答えにはなっていない．

2.3 性能解析

2 元 LDPC 符号の漸近的なウォータフォール領域の性能解析法として開発された密度発展法は，多元 LDPC 符号にも原理的には拡張することができる [9]．2 元消失通信路に対しては，漸近的な性能を厳密に評価すること [17] が可能となっているが，一般の 2 元入力無記憶通信路では，現実的には計算量が多く困難であり，漸近的な復号性能を量るためには，木アンサンブルに対するモンテカルロ法 [10] に頼らざるを得ない．性能解析の目的が符号化システムの最適化である場合，最適な次数分布を探索しても，$m \geqq 6$ で $(2,d_c)$ 正則多元 LDPC 符号が最適であるという，性能解析をした甲斐がない結果を得ることはよくあることである．

$m \geqq 3$ ならば，多元 LDPC 符号のブロック誤り率は式 (2) に従うことが経験的に知られており，特に BEC の場合には，筆者らによって [18] パラメータ α が厳密に求められている．Gallager [7] によって多元シンボル単位の重み分布が，筆者らによってビット単位の重み分布が導出されている．

3. 可変符号化率符号化

時間と共に変化するような通信路の場合には，通信路に応じ

て符号化率を変更して，できるだけ通信路容量に近い符号化率で信頼できる通信を行うことが望ましい．多くの通信システムに対して，符号化率が可変な符号化システムが求められている．異なる符号化率の複数の符号を用意して，通信路の状況が変わる度に符号を変更することは，符号化システムを複雑にしてしまうので，1 組の符号器と復号器だけで，多くの符号化率での通信できる，符号化率が可変な符号化システムが望まれている．さらに，可変符号化率符号化システムでは，復号に失敗した際に，パケットをすべて送り直さずに，付加的にパリティビットを送信して復号するという，ハイブリッド自動再送要求を実現することも可能である．

低い符号化率の符号をパンクチャして高い符号化率の符号を作ることが，符号化率が可変な誤り訂正符号を実現する一般的な方法である．しかしながら，低い符号化率の LDPC 符号を構成することは，高い符号化率の符号に比べて難しいこと [11] が，報告されている．このため，従来提案されていた可変符号化率符号化法は，低い符号化率に対応しているものがなかった．符号化率 1/6 の Accumulate Repeat Accumulate (ARA) 符号 [19, Tabel. 1] と，符号化率 1/10 の Multi-Edge Type LDPC 符号 [11, Table. X] はパンクチャビットを含む構造化された LDPC 符号であり，現在知られている低い符号化率で最良の LDPC 符号として知られている．しかし，これらの符号のパリティ検査行列の最大行重みはそれぞれ 11 と 28 と高く，このため比較的高いエラーフロアを有し，短い符号長での復号性能を引き出すことができなかった．LDPC 符号の復号にかかる行処理は，復号処理の中で最も計算複雑度が高い計算を要する．この処理は行単位で行われるためパリティ検査行列の行数が多いほど復号に必要な計算量が多くなる．情報シンボルの数を K とすると，パリティ検査行列の行数 M は符号化率 R を用いて $M = K(1-R)/R$ と書け，低い R の場合には M，つまり復号にかかる計算量が非常に大きくなることが分かる．

低い符号化率の LDPC 符号の設計と復号法に関する，上記の問題点は以下の様にまとめられる．

問題 1: 高い計算量が必要な，行処理を多く必要とする．

問題 2: 最適化されたパリティ検査行列の行重みが高くなる傾向があり，短い符号長では復号性能を引き出すことができず，エラーフロアも高い．

問題 3: パンクチャビットを多く含んでいるため，復号にかかる多くの反復回数が必要である．

筆者らはこれらの問題を解決する符号化法を [20] で提案している．

符号化率 1/3 の (2,3)-正則多元 LDPC 符号 C_1 を母符号として，低い符号化率の $C_2, C_3, \ldots$ を次の様に構成する．まず，N 個の 2 元 $m \times m$ 正則行列 $F_{(T-1)N+1}, \ldots, F_{TN}$ と C_{T-1} をランダムに選ぶ．C_{T-1} の各シンボルに $F_{(T-1)N+1}, \ldots, F_{TN}$ と C_{T-1} をそれぞれかけて C_{T-1} に繋げたものを C_T とする．

$$C_T = \{(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_{TN}) | \boldsymbol{x}_{(T-1)N+v} = F_{(T-1)N+v}\boldsymbol{x}_v, \\ \text{for } v = 1, \ldots, N, (\boldsymbol{x}_1, \ldots, \boldsymbol{x}_{(T-1)N}) \in C_{T-1}\}.$$

C_T は符号長 TN シンボル，符号化率 $1/(3T)$ の符号となる．

この符号の構成法は，2 元 LDPC 符号 $m = 1$ の場合には，単に LDPC 符号の符号語を T 回送信している符号とみなすことができる．この繰り返し送るという符号化は，Eb/No 対ブロック誤り率曲線を改善せず，ただ符号長を無駄に消費するだけなので，低符号化率の符号を作る最も効率の悪い方法である．しかし，多元 LDPC 符号 $m \geqq 2$ の場合には，単なる繰り返しではなくシンボルごとにランダムな $m \times m$ 正則行列が乗算されていることで，各シンボル $\boldsymbol{x}_v$ を仮想的な通信路 $\Pr(Y_v, \ldots, Y_{(T-1)N+v} | X_v)$ を通して送信していると考えることができる．

C_T の復号に必要な初期メッセージは次のように計算される．$v = 1, \ldots, N$，$\boldsymbol{x} \in \{0,1\}^m$ に対して，

$$p_v^{(0)}(\boldsymbol{x}) = \mu \Pr(X_v = \boldsymbol{x} | Y_v = y_v) \times \\ \prod_{t=1}^{T-1} \Pr(X_{tN+v} = F_{tN+v}\boldsymbol{x} | Y_{tN+v} = y_{tN+v})$$

初期メッセージを計算した後は，C_1 のパリティ検査行列の列 $v = 1, \ldots, N$ と行 $c = 1, \ldots, M$ に対して，行処理と列処理を行う．初期メッセージの計算以外は，前節で定義した C_1 の復号法とまったく同じ復号処理がなされる．従来は符号化率が低いほどパリティ検査行列の数が多くなり，復号にかかる計算量が増えてしまっていたが，C_T の符号化率を小さく (T を大きく) しても，C_T の復号に必要な計算量は C_1 と同じであり，T によらないことが分かる．さらに，C_T は符号化法，復号法が単純であるにも関わらず，今まで知られている短い符号長の最良の誤り訂正符号に比べて，優れた復号性能を有することが実験で確かめられている [20].

4. レートレス符号化への応用

レートレス符号は噴水 (Fountain) 符号とも呼ばれる，従来のブロック符号とは異なるブロードキャスト通信のための符号化法である．ブロック符号の目的は，通信路容量 C の通信路で，できるだけ少ない $n > k/C$ ビットの系列に符号化し，n 個の通信路出力を受信した受信者に k ビットの情報を確実に送り届けることであった．一方，レートレス符号化では，ある特定の通信路を想定しないで，不特定多数の受信者にそれぞれ異なる通信路容量 C の通信路を通じて，k ビットの情報を確実に送り届けることを目的としている．具体的には，送信者は k ビットの情報を無限長の系列に符号化 $\mathcal{C}_\infty : \{0,1\}^k \to \{0,1\}^\infty$ し，各受信者はこの無限の長さの符号化ビット系列の中から，できるだけ少ない任意の $n > k/C$ 個の通信路出力を受信し，確実に k ビットの情報ビットを復元することがレートレス符号化の目的である．言い換えると，ある復号誤り率を達成するオーバヘッド $\epsilon = nC/k - 1$ の平均をできるだけ小さくするように，レートレス符号化法 $\mathcal{C}_\infty$ を設計することが望まれている．

レートレス符号化では，任意の位置の n 個の通信路出力から元の k ビットを復元することが要請されているので，$C = 1$ であるようなノイズのない通信路に対しても自明な解があるわけではない．このノイズのない通信路に対して，LT 符号 [21] と Raptor 符号 [22] は，情報長 k の極限で，オーバヘッド $\epsilon \to 0$

を達成するレートレス符号となっている. [23] において Etesami らは $C+1$ となる一般の通信路での Raptor 符号の利用を提案している．Raptor 符号は高い符号化率の 2 元 LDPC 符号と確率 Ω_d で選ばれる長さ $d+1$ の単一パリティ検査符号の連接符号とみなすことができる．Venkiah らは [24]，一般通信路に対して，この連接符号の最適化法を提案し，元の Raptor 符号よりも優れた復号性能を引き出すことに成功している．

一般通信路に適した Raptor 符号の，設計と復号に関する問題点として次の 4 つを挙げることができる．

問題 1: 各情報長 k に対して確率分布 Ω_d を最適化する必要がある．

問題 2: 最適化された Raptor 符号は，最大の単一パリティ検査符号の長さ $\max_d\{d \mid \Omega_d \neq 0\}$ が大きくなる傾向があり，復号に大きな計算量が必要となる．

問題 3: 単一パリティ検査符号の数 $(1+\epsilon)k/C$ は，通信路容量 C が小さな通信路では多くなってしまう．

問題 4: 短い情報ビット数 k では，低いオーバヘッドと誤り率で情報ビットを送ることができない．

(2,3) 正則多元 LDPC 符号 C_1 を用いたレートレス符号化法 [25] はこれらの問題を一挙に解決するものとなっている．次の様なレートレス符号化 $\mathcal{C}_\infty : \{0,1\}^k \to \{0,1\}^\infty$ を考える．

（1） k 個の情報ビット $s_1, \ldots, s_k \in \{0,1\}$ を $K := k/m$ 個の多元情報シンボル $\boldsymbol{s}_1, \ldots, \boldsymbol{s}_K \in \{0,1\}^m$ とみなす．

（2） C_1 を用いて K 個の多元情報シンボル $\boldsymbol{s}_1, \ldots, \boldsymbol{s}_K$ を N 個の多元符号化シンボル $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_N \in \{0,1\}^m$ に符号化する．

（3） 次の (a),(b) を時刻 $i = 1 \ldots, \infty$ に対して行う．

（a） ランダムに $v_i \in [1,N]$ と $w_i \in [1,m]$ と正則な 2 元 $m \times m$ 行列 $F_i \in \{0,1\}^{m\times m}$ を選択する．

（b） $F_i \boldsymbol{x}_{v_i} \in \{0,1\}^m$ の第 w_i ビットを第 i レートレス符号化ビット y_i として送信する．

このレートレス符号 $\mathcal{C}_\infty$ は (2,3) 正則多元 LDPC 符号 C_1 と長さ 2 の多元単一パリティ検査符号の連接符号である Raptor 符号とみなすことができる．

受信者は通信路の出力 $y_1, \ldots, y_\infty$ のうち任意の $n = (1+\epsilon)k/C$ 個の出力アルファベット $\{y_i\}_{i\in I}, \#I = n$ を集める．多元符号化シンボル $\boldsymbol{x}_v$ から生成されたレートレス符号化ビットが送信された時刻の集合 $I_v := \{i \in I \mid v_i = v\}$ を定義する．このとき，$I = \cup_{v=1}^N I_v$ が成り立つ．復号に使われる初期メッセージ $p_v^{(0)}(\boldsymbol{x})$, $\boldsymbol{x} \in \{0,1\}^m$ は，次のように計算される．

$$p_v^{(0)}(\boldsymbol{x}) = \mu \prod_{i\in I_v} \tilde{p}_i^{(0)}(F_i\boldsymbol{x}) \tag{3}$$

$$\tilde{p}_i^{(0)}(\boldsymbol{x}) = \begin{cases} \Pr(X=0|Y=y_i) & \boldsymbol{x} \text{ の第 } w_i \text{ ビットが } 0 \\ \Pr(X=1|Y=y_i) & \boldsymbol{x} \text{ の第 } w_i \text{ ビットが } 1, \end{cases}$$

ここで，μ は $\sum_{\boldsymbol{x}\in\{0,1\}^m} p_v^{(0)}(\boldsymbol{x}) = 1$ となるような定数，X, Y はそれぞれ通信路の入力と出力である．ブロック符号とは異なりレートレス符号では，通信路出力を $n \geqq k/C$ 個集めなければならず，通信路容量 C が小さい通信路では多くの通信路出力を集めなければならなくなり，復号にかかる計算量が C に大きく依存していた．一方，上で紹介した多元 LDPC 符号を用いたレートレス符号の復号は，初期メッセージの計算法が異なるだけで，他の復号処理は第 2.2 節で定義された行処理と列処理を繰り返すだけである．つまり，復号に必要な計算量は C_1 の復号に必要な計算量と同じであり，通信路容量に依存しない．さらに，少ない情報ビット数 k に対しても，少ないオーバヘッドで最適化された Raptor 符号よりも低いブロック誤り率を達成できることが実験により確かめられている [25].

5. 量子誤り訂正符号への応用

量子誤り訂正は，量子状態を確実に保存し高信頼度で通信すること，つまり量子計算および量子通信を実現するために必要な技術である．量子 LDPC 符号は，疎なパリティ検査方程式によって定義された，古典 LDPC 符号に対応する量子誤り訂正符号である．CSS (Calderbank, Shor and Steane) 符号 [26], [27] は, 量子誤り訂正符号の重要な符号クラスである．CSS 符号 $CSS(C,D)$ は $H_C H_D^T = 0$ となる 2 元パリティ検査行列 H_C と H_D を有する，符号化率 1/2 以上の，2 つの 2 元古典符号 C と D によって定義される量子誤り訂正符号である．通信路にも依存するが，古典符号としての C と D の誤り訂正性能が高いほど，CSS 符号 $CSS(C,D)$ の量子誤り訂正性能も高くなる．

LDPC-CSS 符号は拘束条件 $H_C H_D^T = 0$ を満たす疎なパリティ検査行列 H_C と H_D によって定義される CSS 符号である．LDPC 符号の設計に詳しい読者は，少し考えてみると分かることだが，拘束条件 $H_C H_D^T = 0$ を満たし，タナーグラフに小さなサイクルを含まないような，疎なパリティ検査行列のペア H_C, H_D を見つけることは容易ではない．ランダムに構成した疎行列が拘束条件 $H_C H_D^T = 0$ を満たす確率を MacKay が計算しているが，符号長を大きくすると速く 0 に収束してしまう．有限幾何符号をそのまま使った LDPC-CSS 符号が Postol [28] によって初めて提案され，その後，MacKay らによって自転車符号 [29]，ケイリーグラフに基づいた符号 [30] が，提案されている．さらに，Poulin らによってターボ符号を用いた CSS 符号 [31] が提案されている．筆者の知る限りでは，これらの CSS 符号 [29]〜[31] が，今まで知られている最良の量子誤り訂正符号である．萩原と今井 [32] は，quasi-cyclic (QC) LDPC 符号を用いた LDPC-CSS 符号を提案している．この LDPC-CSS 符号のパリティ検査行列は任意の偶数の行重み $L \geqq 4$ と列重み $J(L/2 \geqq J \geqq 2)$ を有するように設計可能である．

筆者らによって [33]，萩原と今井の LDPC-CSS 符号の構成法が多元 LDPC 符号に拡張されている．この方法では，列重みが 2 であり行重みが L であり，$H_\Gamma H_\Delta^T = 0$ となるパリティ検査行列 H_Γ と H_Δ を，次の手順によって構成している．まず萩原と今井の方法により，$\hat{H}_C \hat{H}_D^T = 0$ となる，列重みが 2 であり行重みが L である 2 元 $M \times N$ パリティ検査行列 $\hat{H}_C$ と $\hat{H}_D$ を構成する．$\hat{H}_C$ と $\hat{H}_D$ の非零成分を，GF(2^m) 上の非零要素をとる変数と置き換えて，新たに列重み 2，行重み L の GF(2^m) 上の $M \times N$ 行列 H_Γ と H_Δ を考える．次に $H_\Gamma H_\Delta^T = 0$ となるように H_Γ と H_Δ の非零成分を決定する．この問題は一般には極めて難しい問題として知られている GF(2^m) 上の連立 2 次多変数方程式となってしまう．しかし，幸運なことに列重み

$L = 2$ の萩原と今井の構成法から得られた $\hat{H}_C$ と $\hat{H}_D$ から作られた H_Γ と H_Δ に対しては，この問題を $\mathbb{Z}_{2^m-1}$ 上の線形連立方程式に帰着させることができる．

最後に，自然な GF(2^m) から $\{0,1\}^{m\times m}$ への写像 [34] を使って，H_Γ と H_Δ をそれぞれ 2 元 $mM \times mN$ パリティ検査行列とみなすことで，多元 LDPC-CSS 符号を得ることができる．この多元 LDPC-CSS 符号は，今まで知られている最良の CSS 符号 [29]〜[31] の 2 倍以上の誤りを訂正することが可能となっている．さらに従来の LDPC-CSS 符号では，大きな問題となっていた小さな最小距離のために引き起こされていた高いエラーフロアも，部分行列のサイズ $m \times m$ を大きくすることにより解消できることが観測されている．

6. ま と め

多元 LDPC 符号は，2 元 LDPC 符号の自然な一般化であるにもかかわらず，構成法や最適な符号の性質は全く異なっており，2 元非正則 LDPC 符号の最適化で得られた知見があまり役に立たないこと，正則なものが最良の性能を有するという美しい性質を有していることを見た．紹介しきれなかったが，他の多くの問題に対して，従来の 2 元非正則 LDPC 符号を凌ぐ性能を発揮している．計算量・メモリを削減した復号アルゴリズムの開発が重要な課題であり，今後の研究の発展が期待されている．

文　献

[1] T. Richardson and R. Urbanke, Modern Coding Theory, Cambridge University Press, March 2008.

[2] E. Arikan, “Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels,” IEEE Trans. Inf. Theory, vol.55, no.7, pp.3051–3073, July 2009.

[3] Y. Polyanskiy, H. Poor, and S. Verdu, “Channel coding rate in the finite blocklength regime,” IEEE Trans. Inf. Theory, vol.56, no.5, pp.2307 –2359, May 2010.

[4] A. Amraoui, Asymptotic and finite-length optimization of LDPC codes, Ph.D. thesis, EPFL, Lausanne, 2006.

[5] T.J. Richardson, M.A. Shokrollahi, and R.L. Urbanke, “Design of capacity-approaching irregular low-density parity-check codes,” IEEE Trans. Inf. Theory, vol.47, pp.619–637, Feb. 2001.

[6] S.B. Korada, A. Montanari, E. Telatar, and R. Urbanke, “An empirical scaling law for polar codes,” Proc. 2010 IEEE Int. Symp. Inf. Theory(ISIT), pp.884 –888, June 2010.

[7] R.G. Gallager, Low Density Parity Check Codes, in Research Monograph series, MIT Press, Cambridge, 1963.

[8] M. Davey and D. MacKay, “Low-density parity check codes over GF(q),” IEEE Commun. Lett., vol.2, no.6, pp.165–167, June 1998.

[9] A. Bennatan and D. Burshtein, “Design and analysis of nonbinary LDPC codes for arbitrary discrete-memoryless channels,” IEEE Trans. Inf. Theory, vol.52, no.2, pp.549 – 583, Feb. 2006.

[10] M. Davey, Error-correction using low-density parity-check codes, Ph.D. thesis, Univ. Cambridge, Cambridge, U.K, Dec. 1999.

[11] T. Richardson and R. Urbanke, “Multi-edge type LDPC codes,” 2003.

[12] J. Thorpe, “Low-density parity-check (LDPC) codes constructed from protographs,” IPN Progress Report, pp.42–154, Aug. 2003.

[13] C. Poulliat, M. Fossorier, and D. Declercq, “Design of regular (2,d_c)-LDPC codes over GF(q) using their binary images,” IEEE Trans. Commun., vol.56, no.10, pp.1626–1635, Oct. 2008.

[14] D. Declercq and M. Fossorier, “Decoding algorithms for nonbinary LDPC codes over GF(q),” IEEE Trans. Commun., vol.55, no.4, pp.633–643, April 2007.

[15] H. Wymeersch, H. Steendam, and M. Moeneclaey, “Log-domain decoding of LDPC codes over GF(q),” Communications, 2004 IEEE International Conference on, pp.772–776 Vol.2, June 2004.

[16] K. Kasai and K. Sakaniwa, “Fourier domain decoding algorithm of non-binary LDPC codes for parallel implementation,” IEICE Trans. Fundamentals, vol.E93-A, no.11, Nov. 2010.

[17] V. Rathi and R. Urbanke, “Density Evolution, Threshold and the Stability Condition for non-binary LDPC Codes,” IEE Proceedings - Communications, vol.152, no.6, pp.1069–1074, 2005.

[18] I. Andriyanova and K. Kasai, “Finite-length scaling of non-binary (c, d) LDPC codes for the BEC,” Proc. 2010 IEEE Int. Symp. Inf. Theory(ISIT), pp.714 –718, June 2010.

[19] D. Divsalar, S. Dolinar, and C. Jones, “Low-rate LDPC codes with simple protograph structure,” Proc. 2005 IEEE Int. Symp. Inf. Theory(ISIT), pp.1622–1626, Sept. 2005.

[20] K. Kasai, D. Declercq, C. Poulliat, and K. Sakaniwa, “Multiplicatively repeated non-binary LDPC codes,” submitted for publication, `http://arxiv.org/abs/1004.5367`, 2010.

[21] M. Luby, “LT codes,” Proc. 40th Annual Allerton Conf. on Commun., Control and Computing, pp.271 – 280, 2002.

[22] A. Shokrollahi, “Raptor codes,” IEEE Trans. Inf. Theory, vol.52, no.6, pp.2551–2567, June 2006.

[23] O. Etesami and A. Shokrollahi, “Raptor codes on binary memoryless symmetric channels,” IEEE Trans. Inf. Theory, vol.52, no.5, pp.2033 – 2051, May 2006.

[24] A. Venkiah, C. Poulliat, and D. Declercq, “Jointly decoded raptor codes: analysis and design for the BIAWGN channel,” EURASIP J. Wirel. Commun. Netw., vol.2009, pp.1–11, 2009.

[25] K. Kasai and K. Sakaniwa, “Fountain codes with multiplicatively repeated non-binary LDPC codes,” Proc. 6th Int. Symp. on Turbo Codes and Related Topics, Sept. 2010.

[26] A.R. Calderbank and P.W. Shor, “Good quantum error-correcting codes exist,” Phys. Rev. A, vol.54, no.2, pp.1098–1105, Aug. 1996.

[27] A.M. Steane, “Error correcting codes in quantum theory,” Phys. Rev. Lett. , vol.77, no.5, pp.793–797, July 1996.

[28] M.S. Postol, “A proposed quantum low density parity check code,” http://arxiv.org/abs/quant-ph/0108131v1, 2001.

[29] D. MacKay, G. Mitchison, and P. McFadden, “Sparse-graph codes for quantum error correction,” IEEE Trans. Inf. Theory, vol.50, no.10, pp.2315 – 2330, Oct. 2004.

[30] D.J.C. MacKay, A. Shokrollahi, O. Stegle, and G. Mitchison, “More sparse-graph codes for quantum error-correction,” http://www.inference.phy.cam.ac.uk/mackay/QECC.html, June 2007.

[31] D. Poulin, J.P. Tillich, and H. Ollivier, “Quantum serial turbo codes,” IEEE Trans. Inf. Theory, vol.55, no.6, pp.2776 –2798, June 2009.

[32] M. Hagiwara and H. Imai, “Quantum quasi-cyclic LDPC codes,” Proc. 2007 IEEE Int. Symp. Inf. Theory(ISIT), pp.806–810, June 2007.

[33] K. Kasai, M. Hagiwara, H. Imai, and K. Sakaniwa, “Quantum error correction beyond the bounded distance decoding limit,” http://arxiv.org/abs/1007.1778, July 2010.

[34] F.J. MacWilliams and N.J.A. Sloane, The Theory of Error-Correcting Codes, Elsevier, Amsterdam, 1977.