A-007

二元対称消失通信路におけるビット反転復号法の改善

Improved Bit-flipping Decoding Algorithms over the Binary Symmetric Erasure Channel

石橋想太郎† Sotaro Ishibashi　長田佳史† Keishi Osada
細谷剛‡ Gou Hosoya　後藤正幸§ Masayuki Goto

1 はじめに

誤り訂正符号の 1 つである低密度パリティ検査 (LDPC) 符号 [1] は，繰り返し復号を行うことで優れた復号性能を示すことが知られている．繰り返し復号法には，確率伝播型 (BP) 復号法とビット反転 (BF) 復号法がある．BP 復号法は優れた復号性能を持つが，計算コストが BF 復号法よりも高く実装の際に問題となる恐れがある [2]．BF 復号法は Gallager によって考案され，Gallager Algorithm A [3](以下 Gallager A) や，Gallager Algorithm B [3](以下 Gallager B) といった代表的な方法がある．Gallager A は $\{-1,1\}$ の 2 値のメッセージを扱う最も一般的な BF 復号法で，計算コストが低い．また Gallager A はそのアルゴリズムの簡便さから解析が容易であり，復号中に更新されるメッセージの誤り確率を計算する密度発展法によって様々な理論的解析がなされている [1], [3], [4]．Gallager B は，Gallager A を改良した BF 復号法であり，密度発展法によって予め計算したメッセージの誤り確率に応じて復号中で用いるパラメータを変化させることで，高い復号性能を示す．

一方，二元対称消失通信路を対象とした BF 復号法は Gallager E [3], [5] と呼ばれる．Gallager E は，通信路で発生する誤りと消失の確率に応じて Gallager B と同様にパラメータを変化させることで Gallager B よりも高い復号性能を示す．しかし消失から復元されたビットがもつメッセージの信頼性は消失していないビットに比べて低い可能性がある．そのため，消失から復元されたビットがもつメッセージをそのまま利用して誤り訂正を行う Gallager E では，そのメッセージが復号性能に悪い影響を与える可能性がある．

そこで本研究では，Gallager E の列処理に着目し，信頼性が確保できたと考えられるメッセージのみを利用する BF 復号法を提案する．また，計算機シミュレーションによる実験結果から，提案手法の有効性を示す．

2 LDPC 符号と通信路モデル

LDPC 符号は非零要素が非常に少ない M 行 N 列のパリティ検査行列 H により定義される符号である．検査行列 H の 第 m 行第 n 列の要素を H_{mn}，$m \in [1,M]$，$n \in [1,N]$ とする *．本研究では 2 元 LDPC 符号を対象とし，ある m 行中の 1 の数を行重み d_c とし，ある n 列中の 1 の数を列重み d_v とする．全ての行と列で重みが等しい場合，その LDPC 符号を (N, d_v, d_c) 正則 LDPC 符号と呼ぶ．LDPC 符号の符号語 $\boldsymbol{c} = (c_1, c_2, \cdots, c_N) \in F_2^N$ は $\boldsymbol{c}H^{\mathrm{T}} = \boldsymbol{0}$ を満たす．ここで F_2 はガロア体上の要素 $\{0,1\}$ を，T は行列の転置を表す．

検査行列 H は，タナーグラフとして表現することができる．タナーグラフは検査行列 H の列に対応する N 個のノードをビットノード，行に対応する M 個のノードをチェックノードとし，非零要素の位置に対応するノード同士を枝で結んだ 2 部グラフである．

†早稲田大学大学院創造理工学研究科
‡早稲田大学理工学総合研究所
§早稲田大学理工学術院
*$[a,b]$ は自然数 a から b までの集合を表す．

また，検査行列 H に対して，$\mathcal{N}(m) \triangleq \{n : H_{mn} = 1\}$，$\mathcal{M}(n) \triangleq \{m : H_{mn} = 1\}$ を定義する．本研究では誤り確率 p_0，消失確率 q_0 の二元対称消失通信路を仮定する．符号語の各ビット c_n は，$x_n = 2c_n - 1$ と写像した系列 $\boldsymbol{x} := (x_1, x_2, \cdots, x_N)$ を送信する．雑音 $\boldsymbol{e} = (e_1, e_2, \cdots, e_N)$ と消失が加わった受信語 $\boldsymbol{y} = (y_1, y_2, \cdots, y_N)$ を受信するものとし，受信語の n ビット目が消失している場合，$y_n := 0$ とする．また受信側では受信語 $\boldsymbol{y}$ から推定系列 $\hat{\boldsymbol{x}} = (\hat{x}_1, \hat{x}_2, \cdots, \hat{x}_N)$ に復号する．

3 Gallager E [3], [5]

[Gallager E]

初期設定) $H_{mn} = 1$ となる (m,n) に対し $V_{mn}^{(0)} := y_n$ とする．$i := 1$ とし，最大繰り返し回数 $I_{\max}$ を適当な定数に設定する．

step1) 行処理

$m \in [1,M]$ において，$H_{mn} = 1$ となる (m,n) に対し次式を計算する．

$$U_{mn}^{(i)} := \prod_{n' \in \mathcal{N}(m) \setminus n} V_{mn'}^{(i-1)} \tag{1}$$

step2) 列処理

$n \in [1,N]$ において，$H_{mn} = 1$ となる (m,n) に対し step2-1 と 2-2 のいずれかを実行する．ここで $s_{1,j} = |\{m' : U_{m'n}^{(i)} = j, m' \in \mathcal{M}(n) \setminus m\}|$，$j \in \{1,-1\}$，$k_1 = s_{1,1} + s_{1,-1}$ とし，b_{i,k_1} は，密度発展法 [3] により決定される．

step2-1) $y_n = 0$ の場合

$$V_{mn}^{(i)} := \begin{cases} 1, & \text{if } s_{1,1} \geq \lceil k_1/2 \rceil; \\ -1, & \text{if } s_{1,-1} \geq \lceil k_1/2 \rceil; \\ 0, & \text{otherwise.} \end{cases} \tag{2}$$

step2-2) $y_n \neq 0$ の場合

$$V_{mn}^{(i)} := \begin{cases} 1, & \text{if } s_{1,1} \geq b_{i,k_1}; \\ -1, & \text{if } s_{1,-1} \geq b_{i,k_1}; \\ y_n, & \text{otherwise.} \end{cases} \tag{3}$$

step3) 推定系列の算出

$n \in [1,N]$ において，$H_{mn} = 1$ となる (m,n) に対し step3-1 と 3-2 のいずれかを実行する．ここで $s_{2,j} = |\{m' : U_{m'n}^{(i)} = j, m' \in \mathcal{M}(n)\}|$，$j \in \{1,-1\}$，$k_2 = s_{2,1} + s_{2,-1}$ とし，b_{i,k_2} は密度発展法によって決定される．

step3-1) $y_n = 0$ の場合

$$\hat{x}_n := \begin{cases} 1, & \text{if } s_{2,1} \geq \lceil k_2/2 \rceil; \\ -1, & \text{if } s_{2,-1} \geq \lceil k_2/2 \rceil; \\ y_n, & \text{otherwise.} \end{cases} \tag{4}$$

step3-2) $y_n \neq 0$ の場合

$$\hat{x}_n := \begin{cases} 1, & \text{if } s_{2,1} \geq b_{i,k_2}; \\ -1, & \text{if } s_{2,-1} \geq b_{i,k_2}; \\ y_n, & \text{otherwise.} \end{cases} \quad (5)$$

step4) 符号語判定

$\hat{x}_n \in \{1,-1\}$ を $\hat{c}_n = (1-x_n)/2$ に変換し，$\hat{\boldsymbol{c}}H^{\mathrm{T}} = \boldsymbol{0}$ または $i = I_{\max}$ ならば，$\hat{\boldsymbol{c}}$ を符号語として出力し復号を終了する．それ以外の場合，$i := i+1$ として step1 へ戻る．□

4 提案手法

Gallager E では消失訂正により復元されたビットがもつメッセージの信頼性は低いと考えられるが，そのようなメッセージが存在する場合，正しく誤り訂正が行われない可能性がある．そこで本研究では，誤り訂正の行われる Gallager E の列処理に着目し，前回の反復時のメッセージと値が変わらないメッセージのみを利用し，値が変わったメッセージは次回の反復では利用せず消失メッセージと同等に扱う．このような更新ルールに変更することで，信頼性が確保できたと思われるメッセージのみを利用する復号法を提案する．

ここで，i 回目の更新において列処理に関わるメッセージには，ビットノードからチェックノードへ送られるメッセージ $V_{mn}^{(i)}$ と，チェックノードからビットノードへ送られるメッセージ $U_{mn}^{(i)}$ の 2 通りがある．そのため，前者のメッセージに関して信頼性の確保を考えた提案手法 1 と後者に関して同様の改善を加えた提案手法 2 の 2 つの復号法を述べる．

[提案手法 1]

$i \geq 2$ のとき，$n \in [1,N]$ において $H_{mn} = 1$ となる (m,n) に対し，step2-1 と 2-2 を以下のように変更する．なお $W_{mn}^{(1)} := y_n$ とする．それ以外の step は Gallager E と同様である．

step2-1) $y_n = 0$ の場合

$$W_{mn}^{(i)} := \begin{cases} 1, & \text{if } s_{1,1} \geq \lceil k_1/2 \rceil; \\ -1, & \text{if } s_{1,-1} \geq \lceil k_1/2 \rceil; \\ 0, & \text{otherwise.} \end{cases} \quad (6)$$

$$V_{mn}^{(i)} := \begin{cases} 1, & \text{if } s_{1,1} \geq \lceil k_1/2 \rceil, W_{mn}^{(i-1)} = 1; \\ -1, & \text{if } s_{1,-1} \geq \lceil k_1/2 \rceil, W_{mn}^{(i-1)} = -1; \\ 0, & \text{otherwise.} \end{cases} \quad (7)$$

step2-2) $y_n \neq 0$ の場合

$$W_{mn}^{(i)} := \begin{cases} 1, & \text{if } s_{1,1} \geq b_{i,k_1}; \\ -1, & \text{if } s_{1,-1} \geq b_{i,k_1}; \\ 0, & \text{otherwise.} \end{cases} \quad (8)$$

$$V_{mn}^{(i)} := \begin{cases} 1, & \text{if } s_{1,1} \geq b_{i,k_1}, W_{mn}^{(i-1)} = 1; \\ -1, & \text{if } s_{1,-1} \geq b_{i,k_1}, W_{mn}^{(i-1)} = -1; \\ 0, & \text{otherwise.} \end{cases} \quad (9)$$

[提案手法 2]

$i \geq 2$ のとき step2-2 と 3-2 を以下のように変更する．それ以外の step は Gallager E と同様である．

step2-2) $y_n \neq 0$ の場合

$$V_{mn}^{(i)} := \begin{cases} 1, & \text{if } s'_{1,1} \geq b_{i,k'_1}; \\ -1, & \text{if } s'_{1,-1} \geq b_{i,k'_1}; \\ y_n, & \text{otherwise.} \end{cases} \quad (10)$$

ここで，$s'_{1,j} = |\{m' : U_{m'n}^{(i)} = U_{m'n}^{(i-1)} = j, m' \in \mathcal{M}(n) \setminus m\}|$, $j \in \{1,-1\}$, $k'_1 = s'_{1,1} + s'_{1,-1}$ とし，b_{i,k'_1} は，密度発展法により決定される¶．

¶密度発展法による計算は Gallager E のときと同じ方法で行う．

step3-2) $y_n \neq 0$ の場合

$$\hat{x}_n := \begin{cases} 1, & \text{if } s'_{2,1} \geq b_{i,k'_2}; \\ -1, & \text{if } s'_{2,-1} \geq b_{i,k'_2}; \\ y_n, & \text{otherwise.} \end{cases} \quad (11)$$

ここで，$s'_{2,j} = |\{m' : U_{m'n}^{(i)} = U_{m'n}^{(i-1)} = j, m' \in \mathcal{M}(n)\}|$, $j \in \{1,-1\}$, $k'_2 = s'_{2,1} + s'_{2,-1}$ とし，b_{i,k'_2} は，密度発展法により決定される．

5 計算機シミュレーションによる評価

提案手法の有効性を検証するために計算機によるシミュレーションを行い，評価を行った．

5.1 シミュレーション条件

実験にはランダムに構成した $(1000,4,8)$ の正則 LDPC 符号に対し，提案手法 1,2 と Gallager E を実行したときの推定系列のビット誤り率 (BER) で評価した．通信路は二元対称消失通信路を仮定し，10^8 個の符号語を送信する．ここで，通信路の誤り確率 p_0 を変化させる．

5.2 実験結果及び考察

図 1 に実験結果を示す．ここで縦軸は BER を表し，横軸は通信路の誤り確率 p_0 を表す．

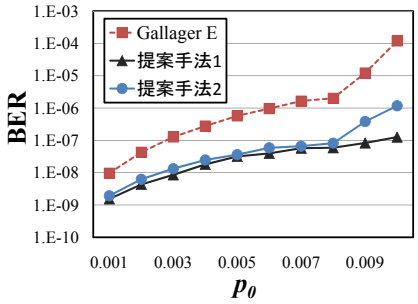

図 1．復号結果 ($(1000,4,8)$ 符号, $q_0 = 0.1$)

提案手法 1,2 ともに Gallager E よりも BER が低減している．これにより，信頼性が確保できたと思われるメッセージのみを利用する復号法は効果があると考えられる．

6 まとめと今後の課題

本稿では，消失訂正により復元されたビットがもつ情報に着目し，信頼性が確保できたと考えられる場合のみ，その情報を利用する BF 復号法を 2 つ提案した．実験結果より，提案手法はいずれも Gallager E に比べて復号性能が向上することを示した．

今後は対象を正則 LDPC 符号ではなく，非正則 LDPC 符号に拡張した復号法を検討する．また提案復号法に対する復号性能を理論的に解析をすることや，提案手法の計算量を考察することも今後の課題である．

参考文献

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

[2] J. Chen, A. Dholakia, E. Eleftheriou, M.P.C. Fossorier, X.-Y. Hu, "Reduced-complexity decoding of LDPC codes," *IEEE Trans. Commun.*, vol. 53, pp. 1288–1299, Aug. 2005.

[3] T. J. Richardson and R. L. 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.

[4] L. Bazzi, T. J. Richardson, and R. L. Urbanke, "Exact thresholds and optimal codes for the binary-symmetric channel and Gallager's decoding algorithm A," *IEEE Trans. Inform. Theory*, Vol. 50, No. 9, pp. 2010–2021, Sep. 2004.

[5] M. Mitzenmacher, "A note on low density parity check codes for erasures and errors," *SRC Technical Note, 1998-017*, Dec. 1998.