二元対称消失通信路におけるビット反転型アルゴリズムの改善

1X07C015-2　石橋想太郎
指導教員　後藤正幸

1　研究目的

近年，情報化社会における情報通信技術の発達に伴い，情報伝送に対する信頼性の確保が不可欠となっており，誤り訂正符号と復号技術の果たす役割が重要になっている．

誤り訂正符号の中でも低密度パリティ検査 (LDPC) 符号は，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，確率伝搬 (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．BF 復号法は Gallager によって考案され，Gallager Algorithm A [1](以下 Gallager A) や，Gallager Algorithm B [1](以下 Gallager B) といった代表的な方法がある．Gallager A は $\{0,1\}$ 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，復号中の誤り確率を扱う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]．Gallager B は，Gallager A を改良した BF 復号法であり，その密度発展法によって予め計算した誤り確率に応じて復号中に訂正条件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 Gallager B は Gallager E [1] 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 と同様に訂正条件を変化させることで，Gallager B と同様に高い復号性能を示す．しかし，一般的に消失訂正により復元されたビットがもつ情報の信頼度は消失していないビットに比べて低いと考えられる．そのため，消失訂正により復元されたビットがもつ情報をそのまま利用して誤り訂正を行う Gallager E では，その情報が復号性能に悪い影響を与えると考えられる．

そこで本研究では，Gallager E の列処理に着目し，信頼度が確保できたと考えられる情報のみを利用する 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 [1]．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)2 元正則 LDPC 符号と呼ぶ．2 元 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．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，$x_n = (-1)^{c_n}$ 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 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．

[1] $[a,b]$ は自然数 a から b までの集合を表す．

3　従来手法

3.1　Gallager E [1]

以下に Gallager E のアルゴリズムを示す．

[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．

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

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 のいずれかを計算する．以下では $s_{1,j} = |\{m' : U_{m'n}^{(i)} = j, m' \in \mathcal{M}(n) \setminus m\}|$，$j \in \{1,-1\}$，$k_1 = s_{1,1} + s_{1,-1}$ とし，$b_{i,k}$ は密度発展法による評価式によって求める．

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 のいずれかを計算する．以下では $s_{2,j} = |\{m' : U_{m'n}^{(i)} = j, m' \in \mathcal{M}(n)\}|$，$j \in \{1,-1\}$，$k_2 = s_{2,1} + s_{2,-1}$ とし，$b_{i,k}$ は密度発展法による評価式によって求める．

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

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

step4) 符号語判定

$\hat{x}_n \in \{1,-1\}$ を $\hat{c}_n \in \{0,1\}$ 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

Algorithm 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度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，信頼度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，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度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 通りの方法を構成できる．提案手法 1 は正しく誤り訂正が行われなかった場合を想定する改善方法，提案手法 2 は誤り訂正が正しく行われるように想定した改善方法とそれぞれみなすことができる．アルゴリズムにおける Gallager E からの変更部分を以下に示す．

[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．$W_{mn}^{(1)} := y_n$ とする．それ以外の step は Gallager E と同様．

step2-1) $y_n = 0$ の場合

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

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

step2-2) $y_n \neq 0$ の場合

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

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

[提案手法 2]

$i \geq 2$ のとき，$n \in [1, N]$ において $H_{mn} = 1$ となる (m, n) に対し，step2-2 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．

step2-2) $y_n \neq 0$ の場合

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

ここで，$s'_{1,j} = |\{m' : U_{m'n}^{(i)} = U_{m'n}^{(i-1)} = j, m' \in \mathcal{M}(n) \setminus m\}|$, $j \in \{1, -1\}$, $k'_1 = s'_{1,1} + s'_{1,-1}$ である．

step3-2) $y_n \neq 0$ の場合

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

ここで，$s'_{2,j} = |\{m' : U_{m'n}^{(i)} = U_{m'n}^{(i-1)} = j, m' \in \mathcal{M}(n)\}|$, $j \in \{1, -1\}$, $k'_2 = s'_{2,1} + s'_{2,-1}$ である．

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 2 元正則 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，10^6 個の符号語を送信する．ここで，通信路の消失確率は $q_0 = 0.1$ とし，誤り確率 p_0 を変化させる．

5.2　結果及び考察

図 1 に復号のシミュレーション結果を示す．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．

(1) 提案手法 1,2 ともに p_0 が低いところで Gallager E よりも BER が低減している．これにより，信頼度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．

(2) 提案手法 2 は p_0 が低い場合，提案手法 1 よりも優れた復号性能を示す．これは提案手法 2 はより受信値をメッセージとして送信する可能性を上げているアルゴリズムになっているため，p_0 が低い場合は正しいメッセージが送信される可能性がより高まり，正しく復号される可能性も高まるためだと考えられる．

(3) p_0 が高い場合，提案手法 1 が提案手法 2 よりも優れた復号性能を示している．これは提案手法 1 は受信値よりも反復中のメッセージを重要視しているアルゴリズムになっており，p_0 が高まり受信値が誤っている割合が増えたとしても，その誤っているメッセージを繰り返し送信する可能性が低く，正しく復号される可能性が高まるためだと考えられる．

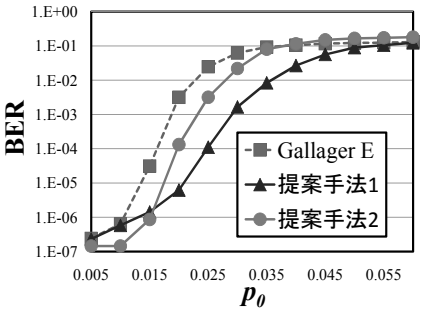

図 1．復号結果

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，信頼度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，p_0 が低い場合におい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の提案を試みる．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も今後の課題である．

参考文献

[1] 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.

[2] 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.