The 29th Symposium on Information Theory
and its Applications (SITA2006)
Hakodate, Hokkaido, Japan, Nov. 28 – Dec. 1, 2006

信頼度更新を用いたLDPC符号のBit-Flipping復号法の改良
Improved Bit-Flipping Decoding Algorithms of Low-Density Parity-Check Codes with Updating Reliabilities

長谷川 裕* 細谷 剛* 八木秀樹† 平澤茂一*
Yu HASEGAWA Gou HOSOYA Hideki YAGI Shigeichi HIRASAWA

Abstract— Bit-flipping-based decoding algorithms for low-density parity-check (LDPC) codes, such as modified weighted bit-flipping (MWBF) and reliability-ratio based weighted bit-flipping (RRWBF) algorithms, provide good trade-off between error-correcting performance and decoding complexity. Recently it has been shown that a decoding algorithm which updates bit reliabilities in every iteration achieves good error performance. In this paper, we propose improved bit-flipping decoding algorithms which updates symbol reliabilities. We show from simulation results that the proposed decoding algorithms have good trade-off between performance and decoding complexity.

Keywords— low-density parity-check code, reliability-ratio based weighted bit-flipping decoding, modified weighted bit-flipping decoding.

1 はじめに

低密度パリティ検査 (以下 LDPC) 符号 [1][2] は 1960 年代に R.G.Gallager によって提案された誤り訂正符号であり，1990 年代に D.J.C.Mackay らによって再発見されてから大きな注目を集め実用化に向けた動きも活発になっている．

LPDC 符号は繰り返し復号法との組み合わせにより優れた誤り訂正能力を示すことが知られており，多くの繰り返し復号法が提案されてきた．bit-flipping (以下 BF) 復号法もそのひとつで，BF 復号法を基礎として様々な改良復号法が提案されている．中でも，weighted bit-flipping (以下 WBF) 復号法 [3] を改良した，modified weighted bit-flipping (以下 MWBF) 復号法 [4]，および，reliability-ratio based weighted bit-flipping (以下 RRWBF) 復号法 [5][6] は誤り訂正能力と計算量の優れたトレードオフを示すことで知られている．

また，近年，各繰り返し毎に判定されたビットの信頼度を更新する MWBF 復号法が提案された [7]．この信頼度更新を用いた MWBF 復号法は，信頼度を更新しない MWBF 復号法より優れた訂正能力を持つことが示されている．しかし [7] で提案された信頼度の更新式は，更新前の信頼度と大きく離れた値に更新される可能性があり，更新したことにより信頼度が下がってしまう可能性もある．また，RRWBF 復号法には適応しにくい．

そこで本研究では，新しい信頼度更新式を提案し，従来の更新式よりも優れた誤り訂正能力を持つことを計算機シミュレーションにより示す．また，RRWBF 復号法に適した信頼度更新式も提案し，提案した復号法が RRWBF 復号法と比較して優れた誤り訂正能力を持つことも示す．

2 準備

2.1 LDPC 符号

本研究では符号長 N，情報記号数 K の 2 元 LDPC 符号を考える．LDPC 符号は，要素 1 が非常に少ない N 行 $M(M > N-K)$ 列の検査行列 H によって定義される符号であり，検査行列 H の要素は殆ど 0 となる．また，検査行列の各行における 1 の数 ρ を行重み，各列における 1 の数 γ を列重みと呼ぶ．検査行列により構成される符号 C は，

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

を満たす任意のベクトル $\boldsymbol{c} = (c_1, c_2, \cdots, c_N) = \{0,1\}^N$ を符号語とし，これはまた各符号語が検査行列の各行 $h_j, j \in [1, M]$. に対応する検査方程式 Φ_j において $c_{j_1} \oplus c_{j_2} \oplus \cdots \oplus c_{j_\rho} = 0$ を満たすことを表す．ここで，$\oplus$ は排他的論理和を表し，また $j_1, j_2, \cdots, j_\rho$ は検査行列の j 行目において 1 が生起している列番号を表す．

2.2 通信路のモデル

2 元 LDPC 符号の符号語 $\boldsymbol{c}$ の各符号ビットを $1 \rightarrow 1, 0 \rightarrow -1$ と変調し，加法的白色ガウス雑音 (AWGN) 通信路を介して送信する．通信路では雑音 $\boldsymbol{e} = (e_1, e_2, \cdots, e_N)$ が加わり，受信側では受信語 $\boldsymbol{y} = (y_1, y_2, \cdots, y_N)$ を受け取る．受信側は次式より硬判定系列 $\boldsymbol{z} = (z_1, z_2, \cdots, z_N)$，

$$z_i = \begin{cases} 1, & \text{if} \quad y_i > 0 \\ 0, & \text{otherwise.} \end{cases} \tag{2}$$

を生成する．最終的に推定系列 $\hat{\boldsymbol{c}} = (\hat{c}_1, \hat{c}_2, \cdots, \hat{c}_N)$, $\hat{\boldsymbol{c}}\boldsymbol{H}^{\mathrm{T}} = 0$ に復号する．

3 従来手法

本節では，LDPC 符号の復号法として従来提案されているいくつかの手法について説明する．

* 〒 169–8555 東京都新宿区大久保 3–4–1 早稲田大学理工学部経営システム工学科，School of Science and Engineering,Waseda University, Okubo 3–4–1, Shinjuku-ku, Tokyo, 169–8555 Japan. E-mail: hasegawa@hirasa.mgmt.waseda.ac.jp
† 〒 169–8050 東京都新宿区西早稲田 1–6–1 早稲田大学メディアネットワークセンター，Media Network Center,Waseda University, Nishi Waseda 1–6–1, Shinjuku-ku, Tokyo, 169–8050 Japan.

3.1 MWBF 復号法 [4]

MWBF 復号法は，硬判定ビット自身の信頼度と検査方程式の信頼度を用いる復号法であり，誤り訂正能力と計算量の良いトレードオフを達成する．

硬判定ビット $z_m, m \in [1, N]$ の信頼度 r_m には受信ビット y_m の絶対値 $|y_m|$ を用いる．

また，検査方程式 $\Phi_j, j \in [1, M]$ の信頼度は「硬判定ビット $z_{j_1}, z_{j_2}, \cdots, z_{j_\rho}$ が全て信頼できる場合には，検査方程式 Φ_j に対応するシンドローム s_j の値も信頼できるが，硬判定ビット $z_{j_1}, z_{j_2}, \cdots, z_{j_\rho}$ の中に一つでも信頼出来ないものがある時，検査方程式 Φ_j に対応するシンドローム s_j の値も信頼できなくなる」という考えに基づき，チェックする硬判定ビットの信頼度の中で最も小さい値とおく．

以下に MWBF 復号法のアルゴリズムを示す．なお，繰り返し i 回目の硬判定系列を $z^{(i)}$，繰り返し i 回目のシンドローム系列を $s^{(i)}$，最大繰り返し回数を L とし，硬判定ビット z_m をチェックする検査方程式の組を $\Phi_{m_1}, \Phi_{m_2}, \cdots, \Phi_{m_\gamma}$ とする．ここで $m_1, m_2, \cdots, m_\gamma$ は検査行列の m 列目において 1 が生起している行を表す．

[MWBF 復号法]

m1) 繰り返し回数 $i := 1$ とする．

m2) 各検査方程式 $\Phi_j, j \in [1, M]$ において，チェックする硬判定ビットの信頼度の中で最も小さい値

$$r_{\min-j} = \min_{1 \le n \le \rho} r_{j_n} \tag{3}$$

を求める．

m3) 硬判定系列 $z^{(i)}$ よりシンドローム系列 $s^{(i)} = \left(s_1^{(i)}, s_2^{(i)} \cdots, s_M^{(i)}\right)$ を次式により求める．

$$s^{(i)} = z^{(i)} \boldsymbol{H}^{\mathrm{T}}. \tag{4}$$

m4) $s^{(i)} = 0$ もしくは $i = L$ ならば $z^{(i)}$ を出力し復号を終了する．それ以外の場合は $i := i + 1$ として，次へ行く．

m5) それぞれの硬判定ビットにおいて，その硬判定ビット自身の信頼度と重み付けされた検査方程式の信頼度から得られる値

$$E_m^{(i)} = \sum_{1 \le n \le \gamma} \{2s_{m_n}^{(i)} - 1\} \cdot r_{\min-m_n} - \alpha_1 \cdot r_m \tag{5}$$

を求める．但し $\alpha_1 (> 0)$ はある定数である．

m6) $E_m^{(i)}$ を最大にする硬判定ビットを反転して $z^{(i)}$ を生成し，m3) に行く． □

3.2 RRWBF 復号法 [5][6]

RRWBF 復号法は「ある検査方程式においては，絶対値 $|y_m|$ が高い受信ビットの方が絶対値 $|y_{m'}|$ が低い受信ビットよりも検査方程式を乱す確率が低い」という考えから信頼度比を次式により定義し，これを復号に用いる．

$$R_{j,m} = \beta \frac{|y_m|}{|y_{\max-j}|} \tag{6}$$

但し，$|y_{\max-j}|$ は，検査方程式 Φ_j に含まれる受信ビット $y_{j_1}, y_{j_2} \cdots, y_{j_\rho}$ の中で最も大きい絶対値とし，β は $\sum_{1 \le n \le \rho} R_{j,j_n} = 1$ を満たす正規化係数とする．

[5] で提案された RRWBF 復号法は式 (6) を用いて復号するが，[6] では式を変形した全く同等のアルゴリズムが提案されている．この復号アルゴリズムは，式 (6) を用いる代わりに式 (7) を用いることによって，[5] のアルゴリズムを効率化したものであり，本研究では [6] の RRWBF 復号法を用いる．

以下に RRWBF 復号法 [6] のアルゴリズムを示す．

[RRWBF 復号法]

r1) m1) と同様．

r2) 各検査方程式において，以下の式で与えられる T_j を求める．

$$T_j = \sum_{1 \le n \le \rho} r_{j_n} \tag{7}$$

r3) m3)～ m4) と同様．

r4) それぞれの硬判定ビットにおいて，

$$E_m^{(i)} = \frac{1}{r_m} \sum_{1 \le n \le \gamma} (2s_{m_n}^{(i)} - 1) T_{m_n} \tag{8}$$

を求める．

r5) $E_m^{(i)}$ を最大にする硬判定ビットを反転して $z^{(i)}$ を生成し，r3) に行く． □

3.3 信頼度更新を用いた MWBF 復号法 [7]

MWBF 復号法において「復号の繰り返しが進むと，反転した硬判定ビットの信頼度に受信ビットの絶対値を用いるのは妥当ではない」という考えから，繰り返し毎に反転された硬判定ビットの信頼度を更新する手法である．MWBF 復号法の m5) で求められる値 $E_m^{(i)}$ は z_m の信頼できない度合を表すことから，更新に $E_m^{(i)}$ を用いる．

i 回目の繰り返しで反転した硬判定ビット z_m の信頼度 $r_m^{(i+1)}$ を以下のように与える．

$$r_m^{(i+1)} = \alpha_2 \cdot \left| E_m^{(i)} \right|. \tag{9}$$

但し，$\alpha_2 (> 0)$ はある定数である．

以下に信頼度更新を用いた MWBF 復号法のアルゴリズムを示す．

[信頼度更新を用いた MWBF 復号法]

u1) m1) と同様．

u2) m3)～ m4) と同様．

u3) $i = 2$ の場合は全ての検査方程式において，それ以外の場合には i 回目に反転した硬判定ビット z_m をチェックする検査方程式 $\Phi_{m_1}, \Phi_{m_2}, \cdots, \Phi_{m_\gamma}$ において，チェックする硬判定ビットの信頼度の中で最も小さい値

$$r_{\min-j}^{(i)} = \min_{1 \le n \le \rho} r_{j_n}^{(i)} \tag{10}$$

を求める．

u4) それぞれの硬判定ビットにおいて，その硬判定ビット自身の信頼度と重み付けされた検査方程式の信頼度から得られる値

$$E_m^{(i)} = \sum_{1\le n\le\gamma} \{2s_{m_n}^{(i)} - 1\} \cdot r_{\min - m_n}^{(i)} - \alpha_1 \cdot r_m^{(i)} \quad (11)$$

を求める．但し $\alpha_1(>0)$ はある定数である．

u5) $E_m^{(i)}$ を最大にする硬判定ビットを反転して $z^{(i)}$ を生成する．

u6) 反転した硬判定ビットの信頼度を式 (9) を用いて更新し，u2) へ行く． □

4 提案手法

4.1 信頼度更新を用いた MWBF 復号法の改良

更新式 (9) は定数倍をおこなっている為，更新前の信頼度と大きく離れた値に更新される可能性がある．また，最も信頼できないと判断されたビットを反転するにも関わらず，反転後に更新式 (9) を用いることにより，反転された硬判定ビットの信頼度が下がることもあるが，これは直感に合わない．そこで i 回目の繰り返しで反転した硬判定ビット z_m の信頼度 $r_m^{(i+1)}$ を以下のように与える．

$$r_m^{(i+1)} = r_m^{(i)} + \alpha_3 \cdot \left| E_m^{(i)} \right|. \quad (12)$$

但し，$\alpha_3(>0)$ はある定数である．

これにより，(i) 更新前後で信頼度が大きく離れた値に更新されること，(ii) 更新後に硬判定ビットの信頼度が下がることを防ぐ．

4.2 信頼度更新を用いた RRWBF 復号法

信頼度を更新するという考え方は RRWBF 復号法にも適応できる．しかし更新として式 (9) を用いると，RRWBF 復号法に対しては適切な更新ができない．これは $E_m^{(i)}$ を式 (8) で計算するため，r_m が小さい値をとる時に $E_m^{(i)}$ がとても大きな値になるためである．一方，定数 α_2 の値を小さくとれば，$E_m^{(i)}$ が大きな値をとる場合には対応できるが，$E_m^{(i)}$ が比較的小さい値の場合，更新された r_m はほぼ 0 になってしまう．

そこで RRWBF 復号法に対しても式 (12) のように，信頼度 $r_m^{(i+1)}$ が繰り返し 1 回前の信頼度 $r_m^{(i)}$ から大きく離れた値に更新されないようにする．また，適切な更新を妨げている r_m の除算を更新式には含めない．このように修正しても式 (8) の $\sum_{1\le n\le\gamma}(2s_{m_n}^{(i)} - 1) \cdot T_{m_n}$ が式 (7) から得られるため，$\sum_{1\le n\le\gamma}(2s_{m_n}^{(i)} - 1) \cdot T_{m_n}$ の値を更新式に用いれば，r_m の情報も含んでいると考えられるからである．

以上の議論により RRWBF 復号法に対しては，次式を用いて信頼度更新を行う．

$$r_m^{(i+1)} = r_m^{(i)} + \alpha_4 \cdot \left| \sum_{1\le n\le\gamma} (2s_{m_n}^{(i)} - 1) \cdot T_{m_n} \right|. \quad (13)$$

但し，$\alpha_4(>0)$ はある定数である．

以下に信頼度更新を用いた RRWBF 復号法のアルゴリズムを示す．

[信頼度更新を用いた RRWBF 復号法]

d1) r1) と同様．

d2) r3) と同様．

d3) $i=2$ の場合は全ての検査方程式において，それ以外の場合には i 回目に反転した硬判定ビット z_m をチェックする検査方程式 $\Phi_{m_1}, \Phi_{m_2}, \cdots, \Phi_{m_\gamma}$ において，以下の式で与えられる $T_j^{(i)}$ を求める．

$$T_j^{(i)} = \sum_{1\le n\le\rho} r_{j_n}^{(i)}. \quad (14)$$

d4) それぞれの硬判定ビットにおいて，

$$E_m^{(i)} = \frac{1}{r_m^{(i)}} \sum_{1\le n\le\gamma} (2s_{m_n}^{(i)} - 1) T_{m_n}^{(i)} \quad (15)$$

を求める．

d5) $E_m^{(i)}$ を最大にする硬判定ビットを反転して $z^{(i)}$ を生成する．

d6) 反転した硬判定ビットの信頼度を (13) 式を用いて更新し，d2) へ行く． □

5 シミュレーションによる評価と考察

5.1 評価条件

提案復号法の性能を評価するため，符号長 $N=1000$，情報記号数 $K=500$，行重み $\rho=6$，列重み $\gamma=3$ の 2 元 LDPC 符号 C を用い実験を行う．

評価尺度には，(1) 誤り訂正能力 (BER) (2) 計算量 を用いる．なお，ここで計算量は実数演算回数により評価した．各復号法において全 0 の符号語を 10^6 回送信し，100 回復号に失敗した時点で終了する．また，最大繰り返し回数を 100 回とする．定数 α_1, α_4 については最も優れた誤り訂正能力を示す値を予備実験により求める．定数 α_2, α_3 は最適な α_1 のもとで予備実験により求めることとする．

5.2 結果と考察

(1) 誤り訂正能力について

図 1，図 2 に復号結果を示す．提案した更新式は優れた誤り訂正能力を持つことが分かる．符号長 $N=2000$ でも同様に計算シミュレーションを行い，提案手法は優れた誤り訂正能力を示すことが確認している．

これはループと呼ばれる状態になっても，正しい復号が行われる可能性があるからである．ここでループとは，$z^{(i_1)} = z^{(i_0)}, (i_1 > i_0)$ となる現象を指す．この状態に陥ると信頼度更新のない MWBF 復号法や RRWBF 復号法では，必ず無限ループとなり誤りが生じる．しかし信頼度更新を用いる場合，ループから脱出して正しい符号語に復号できる可能性がある．一度ループになっても，ループから脱出して正しく復号できた割合を表 1 に示す．

(2) 計算量について

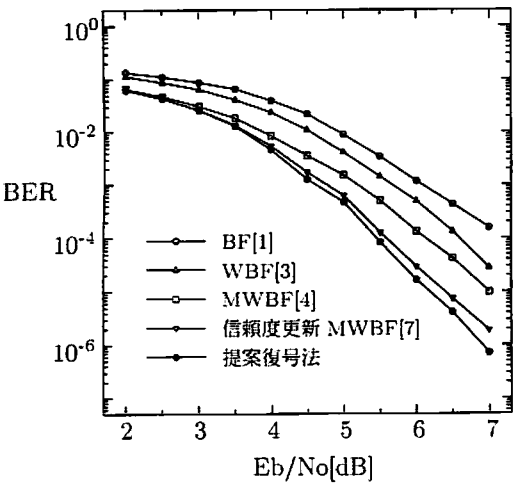

図 1: 各 WBF 復号法の BER 特性

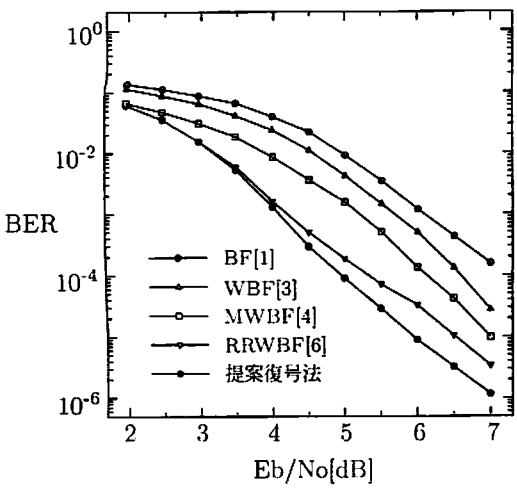

図 2: 各 RRWBF の BER 特性

従来の信頼度更新を用いた MWBF 復号法のアルゴリズムと提案手法の計算量について，式 (9),(12) を比べれば，実数演算の加算が $(i-1)$ 回増えるのみである．

一方，RRWBF 復号法と提案手法を比べると，更新の為に，加算が $\{1+(\rho-1)\times\gamma\}\times(i-1)$ 回，乗算が $(i-1)$ 回増える．しかし提案手法の方が少ない繰り返し回数で復号できる為，特に高い SN 比において，シミュレーション 1 回あたりに増加する計算量は僅かである．図 3 にシミュレーション 1 回あたりに行った演算回数を示す．

6 まとめと今後の課題

本研究では，MWBF 復号および RRWBF 復号法に対して，更新前後で大きく信頼度が変わることのない新しい信頼度更新式を提案した．またシミュレーションにより，この新しい更新式が従来の更新式よりも優れた誤り訂正能力をもつことを示した．

今後の課題としては，解析的な性能評価，本研究では予備実験によって決定した定数 $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ の自動的

表 1: ループから脱出し，正しく復号した割合

	更新 MWBF[7]	提案 MWBF	提案 RRWBF
6.0[dB]	82.67 %	91.82 %	79.67 %
6.5[dB]	87.78 %	93.08 %	79.96 %
7.0[dB]	88.17 %	95.58 %	79.04 %

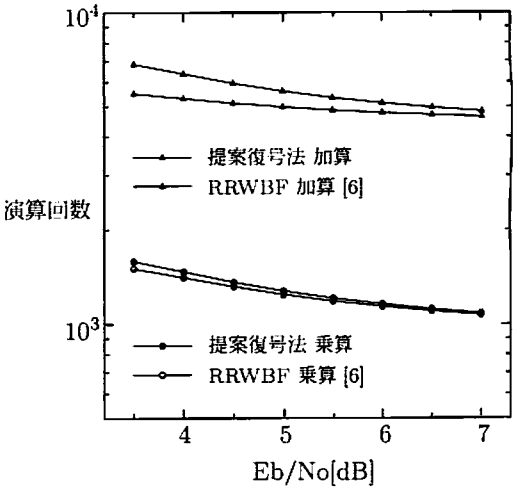

図 3: RRWBF 復号法と提案 RRWBF 復号法の計算量の評価

決定アルゴリズムの検討等が挙げられる．

7 謝辞

著者の一人である長谷川は，本研究を行うにあたり，数多くのご助言，ご支援を賜りました早稲田大学平澤研究室の各氏に感謝いたします．

参考文献

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

[2] D.J.C. MacKay, "Good error-correcting codes based on very sparse matrices," *IEEE Trans. Inform. Theory*, vol.45, pp. 399-432, Mar. 1999.

[3] 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.

[4] J. Zhang and M.P.C. Fossorier, "A modified weighted bit-flipping decoding of low-density parity-check codes," *IEEE Commun. Lett.*, vol.8, pp. 165–167. Mar. 2004.

[5] F. Guo and L. Hanzo, "Reliability ratio based weighted bit-flipping decoding for low-density parity-check codes," *IEEE Electronics Lett.*, vol.40, pp. 1356–1358. Oct. 2004.

[6] C. -H. Lee and W. Wolf, "Implementation-efficient reliability ratio based weighted bit-flipping decoding for LDPC codes." *IEEE Electronics Lett.*, vol.41, pp. 755–757. Jun. 2005.

[7] 佐藤匡，細谷剛，八木秀樹，平澤茂一，"信頼度更新を用いた LDPC 符号の Weighted Bit-Flipping 復号法，" 第 28 回情報理論とその応用学会シンポジウム予稿集，pp. 9–12，2005 年 11 月．