2007 Hawaii and SITA Joint Conference on Information Theory, HISC2007
Hawaii, USA, May 29–31, 2007

An Adaptive Decoding Algorithm of LDPC Codes over the Binary Erasure Channel

Gou HOSOYA*, Hideki YAGI†, Toshiyasu MATSUSHIMA‡, and Shigeichi HIRASAWA††

* Graduate School of Science and Engineering
Waseda University
Ookubo 3-4-1, Shinjuku-ku, Tokyo 169-8555, Japan
E-mail: hosoya@hirasa.mgmt.waseda.ac.jp

† Media Network Center
Waseda University
Totsuka-Machi 1–104, Shinjuku-ku, Tokyo
169–8050, Japan

‡ School of Fundamental Science and Engineering
Waseda University
Ookubo 3-4-1, Shinjuku-ku, Tokyo 169-8555, Japan

†† School of Creative Science and Engineering
Waseda University
Ookubo 3-4-1, Shinjuku-ku, Tokyo 169-8555, Japan

Abstract

Two decoding algorithms of LDPC codes over the binary erasure channel are presented. These algorithms continue the decoding procedure after the BP decoding algorithm fails. Since the proposed decoding algorithms also use the sparse structure of the parity-check matrix of LDPC codes, the increase of decoding complexity of these algorithms is slightly larger compared to that of the BP decoding algorithm. We show by simulation results that the performance of the proposed decoding algorithms is much superior to that of the BP decoding algorithm.

1. Introduction

The combination of the LDPC codes with the belief propagation (BP) decoding algorithm has high performance with low decoding complexity [1], [2]. It is well known that the BP decoding over the binary erasure channel (BEC) cannot decode whenever a subset of the erased bit positions contains a stopping set [3]. To overcome a decoding failure caused by a stopping set, two approaches have been studied by many researchers. The first approach is adding the redundant rows and columns for a given parity-check matrix of the code to improve the performance of the BP decoding. This approach is taken by K. Kasai et al. [6], S. Sankaranarayanan and B. Vasic [8], and N. Kobayashi et al. [9]. The second one is performing the additional procedure after the BP decoding algorithm fails in decoding. This approach is taken by H. Pishro-Nik and F. Fekri [4], the present authors [7], and B. N. Vellambi and F. Fekri [10]. The decoding algorithms in [4] and [10] guess the erased bits for some value to correct erased bits. The decoding algorithm in [7] needs to substitute the equation which requires only small increament of the docoding complexity.

The main difference of these two approaches is as follows: The first approach needs to perform the additions of redundant rows and columns for the parity-check matrix, so it needs the procedure of constructing the redundant parity-check matrix only one time before transmitting the codewords. The performance of the BP decoding algorithm by using the redundant parity-check matrix is better than by using the original one, but it is only effective for codes with short length. On the other hand, the second approach needs to perform additional decoding procedure, so this procedure is always needed for each received sequence. The performance of these improved BP decoding algorithms are significantly superior to that of the BP decoding algorithm [2] for codes with various length.

In this paper, we propose two decoding algorithms of LDPC codes over the binary erasure channel (BEC) which do not need the guessing procedures. The proposed decoding algorithms are also an iterative one using the sparse structure of the parity-check matrix of LDPC codes. We show by simulation results that the proposed decoding algorithms can attain a smaller bit erasure rate than the BP decoding algorithm with a little increase of the decoding complexity.

This paper is organized as follows. In Section 2, we describe LDPC codes, decoding for the BEC, and the BP decoding algorithm. In Section 3, we describe the proposed decoding algorithms. We mention the related works of the proposed decoding algorithms in Section 3.1. An overview and procedure of the decoding algorithm A are presented in Section 3.2 and we give some correctable condition of the decoding algorithm A in Section 3.3. The decoding algorithm B is presented in Section 3.4. Finally, some simulation results and discussions are presented in Section 4 and concluding remarks are given in Section 5.

This work is partially supported by Waseda University Grant for Special Research Project No. 2005B-189 and No. 2006B-293.

2. Preliminaries

2.1. LDPC Codes

Let $\boldsymbol{c} = (c_1, c_2, \ldots, c_N) \in \{0,1\}^N$ be a codeword of LDPC codes and $H = [H_{mn}]$, $m \in [1, M]$, $n \in [1, N]$, $\boldsymbol{c}H^{\mathrm{T}} = \boldsymbol{0}$, be a parity-check matrix whose row and column lengths are M and N, respectively[1]. In this paper, we consider binary LDPC codes for simplify the discussion. Let λ_i and ρ_i denote the fraction of element ones in H which are in columns and rows for weight i, respectively, and $\lambda(x) \triangleq \sum_{i=2}^{\infty} \lambda_i x^{i-1}$ and $\rho(x) \triangleq \sum_{i=2}^{\infty} \rho_i x^{i-1}$ be weight distributions of rows and columns of ones in H, respectively. LDPC codes are characterized by $\mathcal{C}\big(N, \lambda(x), \rho(x)\big)$. The number of rows M is given by $M = N\frac{\int_0^1 \rho(x)dx}{\int_0^1 \lambda(x)dx}$ and designed rate R' is given by $R' = 1 - \frac{M}{N}$. The rate of the codes R satisfies $R \leq R'$ since H is not guaranteed to be a full rank matrix.

We define a loop of length $2L$, $L \geq 2$ in H as a closed path consitituting of the elments 1 in H at the positions (m_1, n_1), (m_1, n_2), (m_2, n_2), $\ldots$, (m_L, n_L), and (m_L, n_1) where $m_1 \neq m_2 \neq \ldots \neq m_L$ and $n_1 \neq n_2 \neq \ldots \neq n_L$. For an example, the element ones at the positions (m_1, n_1), (m_1, n_2), (m_2, n_2), and (m_2, n_1) form a loop of length 4.

2.2. Decoding for the BEC

We assume a codeword $\boldsymbol{c}$ is transmitted through the BEC. $\boldsymbol{c}$ is disturbed by the sequence from the channel $\boldsymbol{e} = (e_1, e_2, \ldots, e_N) \in \{0, \epsilon\}^N$ where ϵ denotes an erasure, and the decoder receives a sequence $\boldsymbol{y} = \boldsymbol{c} + \boldsymbol{e}$. The addition of a binary bit and the erasure bit are defined as $0 + \epsilon = \epsilon$ and $1 + \epsilon = \epsilon$. Therefore, the received bits are either erased or known bits.

Let $\mathcal{N} \in [1, N]$ be an index set of the codeword bits or these of the columns in H. And let $\mathcal{E} \in \mathcal{N}$ and $\bar{\mathcal{E}} = \mathcal{N} \setminus \mathcal{E}$ be the index sets of the erased bits and the known bits, respectively. From the definition of a parity-check matrix H, we can write

$$\boldsymbol{c}H^{\mathrm{T}} = \boldsymbol{c}_{\mathcal{E}}H_{\mathcal{E}}^{\mathrm{T}} + \boldsymbol{c}_{\bar{\mathcal{E}}}H_{\bar{\mathcal{E}}}^{\mathrm{T}} = \boldsymbol{0}, \tag{1}$$

where $\boldsymbol{c}_{\mathcal{E}}$ is a subvector of $\boldsymbol{c}$ whose elements are indexed by $\mathcal{E}$, and $H_{\mathcal{E}}^{\mathrm{T}}$ is asubmatrix whose column positions are indexed by $\mathcal{E}$. Since $\boldsymbol{c}_{\bar{\mathcal{E}}}H_{\bar{\mathcal{E}}}^{\mathrm{T}}$ is known to a receiver and from Eq.(1),

$$\boldsymbol{c}_{\mathcal{E}}H_{\mathcal{E}}^{\mathrm{T}} \quad = \quad \boldsymbol{c}_{\bar{\mathcal{E}}}H_{\bar{\mathcal{E}}}^{\mathrm{T}} = \boldsymbol{s}^E, \tag{2}$$

where $\boldsymbol{s}^E = (s_1^E, s_2^E, \ldots, s_M^E) \in \{0,1\}^M$ is a syndrome sequence calculated by $\boldsymbol{c}_{\bar{\mathcal{E}}}H_{\bar{\mathcal{E}}}^{\mathrm{T}}$. Therefore, decoding for the BEC is to solve the erased (unknown) sequence $\boldsymbol{c}_{\mathcal{E}}$ from the simultaneous equations $\boldsymbol{c}_{\mathcal{E}}H_{\mathcal{E}}^{\mathrm{T}} = \boldsymbol{s}^E$. Since $\boldsymbol{c}$ is a codeword, $\boldsymbol{c}_{\mathcal{E}}$ has at least one solution. If $\boldsymbol{c}_{\mathcal{E}}$ has multiple solutions, then it cannot be corrected which causes to decoding failure.

2.3. BP Decoding Algorithm [2]

We define the following sets for all (m, n) such that $H_{mn} = 1$.

$$\mathcal{A}(m) \triangleq \{n \mid H_{mn} = 1\}, \ \mathcal{B}(n) \triangleq \{m \mid H_{mn} = 1\}.$$

Let $\mathcal{A}_{\mathcal{E}}(m) = \{\mathcal{A}(m) \cap \mathcal{E}\}$, $m \in [1, M]$ be an index set of the erased bit positions at row m in $H_{\mathcal{E}}$. Therefore, we can rewrite $\boldsymbol{c}_{\mathcal{E}}H_{\mathcal{E}}^{\mathrm{T}} = \boldsymbol{s}^E$ as

$$\sum_{i \in \mathcal{A}_{\mathcal{E}}(m)} c_i = s_m^E, \qquad m \in [1, M]. \tag{3}$$

Note that c_i, $i \in \mathcal{A}_{\mathcal{E}}(m)$ are not known to the receiver and from Eq. (2), s_m^E is obtained by calculating

$$s_m^E = \sum_{i \in \mathcal{A}(m) \setminus \mathcal{A}_{\mathcal{E}}(m)} c_i. \tag{4}$$

From Eq. (4), BP decoding algorithm can correct the erased bit c_i, $i \in \mathcal{A}_{\mathcal{E}}(m)$ if $|\mathcal{A}_{\mathcal{E}}(m)| = 1$. The algorithm can continue the above procedure until all erased bits are corrected or there is no m satisfying $|\mathcal{A}_{\mathcal{E}}(m)| = 1$.

The BP decoding algorithm over the BEC is constituted by the following procedures:

[BP Decoding Algorithm over the BEC]

B1) For $m \in [1, M]$, set $\Psi_B(m) := \mathcal{A}_{\mathcal{E}}(m)$ and $s_B(m) = s_m^E$. $\mathcal{E}_B := \mathcal{E}$.

B2) If there exists $m \in [1, M]$ satisfying $|\Psi_B(m)| = 1$, then go to B3). Otherwise the algorithm fails to stop.

B3) For $m \in [1, M]$ such that $|\Psi_B(m)| = 1$, perform the followings.

B3-1) Set $c_i := s_B(m)$ and $\mathcal{E}_B := \mathcal{E}_B \setminus i$.

B3-2) For $m' \in \mathcal{B}(i) \setminus m$, set

$$\Psi_B(m') := \Psi_B(m') \setminus i,$$
$$s_B(m') := s_B(m') + s_B(m).$$

B4) If $\mathcal{E}_B \neq \phi$, then go to B2). Otherwise the algorithm successfully finishes to decode. □

The BP decoding algorithm on the BEC fails when a subset of the erased bit positions contains a stopping set.

Definition 1. [Stopping set [3]] Choose some columns of H to make a submatrix. A stopping set $\mathcal{S} \in \mathcal{E}$ is a subset of the erased bit positions such that the weights of all rows in the submatrix $H_{\mathcal{S}}$ of H, whose column positions are indexed by $\mathcal{S}$, are at least two[2]. □

---

[1] For two integers i and j $(i \leq j)$, $[i, j]$ denotes the set of integers from i to j.

[2] Notice that we do not consider the rows of weight zero.

In the procedure B2) at the BP decoding algorithm, the algorithm stops when there does not exist $m \in [1, M]$ satisfying $\Psi_B(m) = 1$. At this time, all rows of the submatrix of H whose column postions are indexed by $\mathcal{E}_B$, are at least two. Threfore $\mathcal{E}_B$ contains a stopping set[3] $\mathcal{S}$.

3. Proposed Decoding Algorithms

In this section, we propose two decoding algorithms of LDPC codes over the BEC which utilize the decoding procedure after the BP decoding algorithm fails.

3.1. Relation with Other Methods

To overcome a decoding failure caused by a stopping set, two approaches have been studied.

The first approach is adding the redundant rows and columns for a given parity-check matrix of the code to improve the performance of the BP decoding [6], [8], [9]. The second one is performing the additional procedure after the BP decoding algorithm fails [4], [7], [10].

The first approach needs to add the redundant rows or columns for the parity-check matrix before transmition, therefore it needs only once. The key idea is to make the small size of the stopping set be a large value by adding rows or columns for H. When adding rows or columns, this method needs to investigate the loops in H as possible. And its computational complexity is large when we look for large length of loops. Therefore it usually take into account only the loops with short length and the performance by this method can be improved only for the codes only with short length.

On the other hand, the second approach needs to perform additional decoding procedure, therefore this procedures are always needed for each received sequence. The decoding performance of these improved BP decoding algorithms are significantly better than that of the ordinaly BP decoding algorithm for codes with various length. The decoding algorithms by Pishro-Nik and Fekri [4] and Vellambi and Fekri [10] guess the values of erased bits (0 or 1) which are not corrected by the BP decoding algorithm. Clearly the performance of these algorithms depends on the number of guessed bits and the way of choosing these bits.

In this section, we propose two decoding algorithms which do not need the guessing procedures.

3.2. Decoding Algorithm A

The decoding algorithm A continues the decoding procedure after the BP decoding algorithm fails.

Let $\boldsymbol{c}_{\mathcal{E}_B}$ is a subvector of $\boldsymbol{c}$ whose elements are indexed by $\mathcal{E}_B$, and $H_{\mathcal{E}_B}$ is a submatrix whose column positions are indexed by $\mathcal{E}_B$. Let $\boldsymbol{s}^P = \boldsymbol{c}_{\overline{\mathcal{E}}_B} H^{\mathrm{T}}_{\overline{\mathcal{E}}_B}$ where $\boldsymbol{s}^P = (s^P_1, s^P_2, \ldots, s^P_M) \in \{0,1\}^M$. The decoding algorithm A tries to solve a simultaneous equation $\boldsymbol{c}_{\mathcal{E}_B} H^{\mathrm{T}}_{\mathcal{E}_B} = \boldsymbol{s}^P$. From the Definition 1, weights of all rows in $H_{\mathcal{E}_B}$ are at least two since $\mathcal{E}_B$ contains a stopping set $\mathcal{S}$. Let $\mathcal{A}_{\mathcal{P}}(m) = \{\mathcal{A}(m) \cap \mathcal{E}_B\}$, $m \in [1, M]$, be an index set of erased bit positions at row m in $H_{\mathcal{E}_B}$. The inequality $|\mathcal{A}_{\mathcal{P}}(m)| \geq 2$ always holds from the Definition 1.

At first, we choose row m satisfying $|\mathcal{A}_{\mathcal{P}}(m)| = 2$. We here assume that $\mathcal{A}_{\mathcal{P}}(m) = \{i_1, i_2\}$ where $\mathcal{B}(i_1) \geq \mathcal{B}(i_2)$. Notice that choosing either i_1 or i_2 does not influence on the decoding result. In a view-point of the simultaneous equation $\boldsymbol{c}_{\mathcal{E}_B} H^{\mathrm{T}}_{\mathcal{E}_B} = \boldsymbol{s}^P$, the equaiton we choose can be written as follows:

$$c_{i_2} = c_{i_1} + s^P_m.$$

Next, we substitute the above equation to the other equations that have element at i_2. The equation that we used to substitute will never be used in a substitution procedure. This substitution procedure sometimes makes an erased bit to a known bit. The procedure continues until all erased bits are corrected or the number of elements in all the equations that are not used in substitution procedures, are at least three.

The decoding algorithm A is constituted by the following procedures after the BP decoding algorithm fails:

[Decoding Algorithm A]

P1) For any $m \in [1, M]$, set $\Psi_P(m) := \mathcal{A}_{\mathcal{P}}(m)$ and $s_P(m) := s^P_m$. For $n \in \mathcal{E}_B$, set $\Delta_P(n) := \mathcal{B}(n)$. Set $\mathcal{E}_P := \mathcal{E}_B$, $\mathcal{M}_P :\in \{m \mid m = [1, M], |\Psi_P(m)| \geq 2\}$.

P2) If there does not exist $m \in \mathcal{M}_P$ satisfying $|\Psi_P(m)| = 2$ or $|\Psi_P(m)| = 1$, then the algorithm fails. If there exists $m \in \mathcal{M}_P$ satisfying $|\Psi_P(m)| = 1$, then go to P4). Otherwise (If there exists $m \in \mathcal{M}_P$ satisfying $|\Psi_P(m)| = 2$), go to P3).

P3) For $m \in \mathcal{M}_P$ satisfying $|\Psi_P(m)| = 2$, perform the followings:

P3-1) For $m' \in \Delta_P(j)$ where $\Psi_P(m) = \{i, j\}$, $|\Delta_P(i)| \geq |\Delta_P(j)|$, set

$$\Psi_P(m') := \{\Psi_P(m') \setminus j\} \cup i,$$
$$s_P(m') := s_P(m') + s_P(m).$$

.

P3-2) Set $\Delta_P(i) := \{\Delta_P(i) \setminus m\} \cup \{\Delta_P(j) \setminus m\}$ and set $\mathcal{M}_P := \mathcal{M}_P \setminus m$. If $\Delta_P(i)$ has the same elements, then remove all of them from $\Delta_P(i)$.

P4) For $m \in [1, M]$ such that $|\Psi_P(m)| = 1$, perform the followings.

---

[3] Note that at this time, $\mathcal{E}_B$ equals to the set of erased bit positions which cannot be corrected by the BP decoding algorithm.

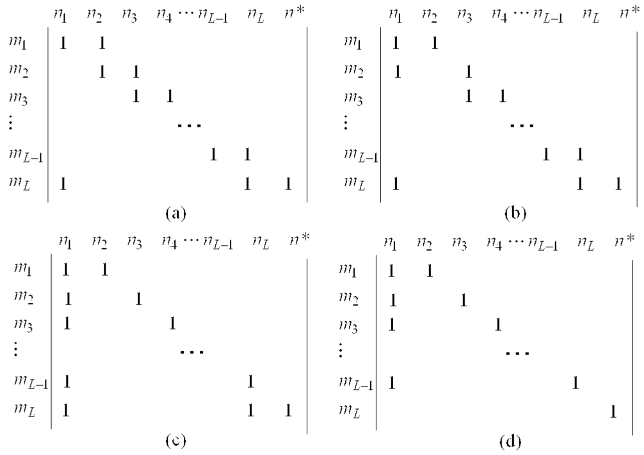

Figure 1: An example of the assumption in the proof of Theorem 1. **(a):** The positions (m_1, n_1), (m_1, n_2), (m_2, n_2), …, (m_L, n_L), and (m_L, n_1) form a loop of length $2L$. **(b):** The result after substituting the equation m_1. **(c):** The result before substituting the equation m_{L-1}. **(d):** The result after substituting equation m_{L-1}. We can obtain erased bit at position n^*.

- **P4-1)** Set $c_i := s_P(m)$ and $\mathcal{E}_P := \mathcal{E}_P \setminus i$ where $i = \Psi_P(m)$.
- **P4-2)** For $m' \in \mathcal{P}(i) \setminus m$, set

$$\Psi_P(m') := \Psi_P(m') \setminus i,$$
$$s_P(m') := s_P(m') + s_P(m).$$

P5) If $\mathcal{E}_P \neq \emptyset$, then go to P2). Otherwise the algorithm successfully finishes. ☐

3.3. Correctable Condition for an Erased Bit by the Decoding Algorithm A

In this section, we show the condition that the proposed decoding algorithm can correct an erased bit.

Lemma 1. ([5]) The submatrix $H_{\mathcal{S}}$ of a parity-check matrix H has at least one loop when $w_c \geq 2$. ☐

The above lemma shows that if there is no loops in a submatrix of H, then the index set of bit postions of this submatrix is not a stopping set. Therefore the key idea of the proposed decoding algorithm is to eliminate loops in $H_{\mathcal{S}}$. The substituition procedure sometimes makes $|\Psi_P(m)| = 1$ and we calculate an erased bit at position $i = \Psi_P(m)$. The condition of the proposed decoding algorithm can produce a known bit, which is not corrected by the BP decoding algorithm, is shown by the following Theorem.

Theorem 1. Assume that a loop of length $2L$, $L \geq 2$, is contained in $H_{\mathcal{S}}$. Let the positions of this loop be (m_1, n_1), (m_1, n_2), (m_2, n_2), …, (m_L, n_L), and (m_L, n_1). We set $\mathcal{M}_L = \{m_1, m_2, \ldots, m_L\}$ and $\mathcal{N}_L = \{n_1, n_2, \ldots, n_L\}$. The decoding algorithm A can correct an erased bit n^* iff there exist only one $m' \in \mathcal{M}_L$ such that $|\Psi_P(m') = 3|$, $\Psi_P(m') \setminus n^* \subseteq \mathcal{N}_L$, and $n^* \in \Psi_P(m')$ and other $m \in \mathcal{M}_L \setminus m'$ satisfy $|\Psi_P(m) = 2|$, $m \in \mathcal{M}_L$, and $\Psi_P(m) \subseteq \mathcal{N}_L$.

Proof. We assume that $m' = m_L$. Therefore $|\Psi_P(m_L)| = 3$, $|\Psi_P(m)| = 2$, $m \in \mathcal{M}_L \setminus m_L$, and $\Psi_P(m_L) \in \{n_1, n_L, n^*\}$ hold. An example of the above assumption is shown in Fig. 1 (a). This assumption is valid even if m' is other value choosen from $\mathcal{M}_L$.

We substitute equation m_1 to the other equations having element at position $j = n_2$ and $\Psi_P(m_2)$ is rewritten from $\{n_2, n_3\}$ to $\{n_1, n_3\}$. We can see this result in Fig. 1 (b). We subsitute equations m_2, m_3, …, m_{L-1} in order and obtain $\Psi_P(m_L) = n^*$. Therefore we calculate an erased bit at position n^*. We can see the result before substituting m_{L-1}th equation in Fig. 1 (c) and after substituting it in Fig. 1 (d).

Conversely, we consider the situation that the substituting the equation (with two elements) can produce the resulting equation with one bit. We assume that the erased bit at position n^* in the equation m_L is corrected by substituting the equation m_{L-1}. Therefore $|\Psi_P(m_{L-1})| = 2$ and $|\Psi_P(m_L)| \geq 3$ are always hold before substituiting the equation m_L. But $|\Psi_P(m_L)| = 3$ holds since it must become $|\Psi_P(m_L)| = 1$ after substituiting the equation m_L. An example of this situation can be seen in Fig. 1 (c) where this is the case of $L = 2$. The cases of $L \geq 3$ are obviously proven. ☐

3.4. Decoding Algorithm B

The decoding algorithm B continues the decoding procedure after the algorithm A fails. At this time, we set $\Psi_P(m) := \Psi_Q(m)$ and $\mathcal{M}_Q := \mathcal{M}_P$. The matrix H_Q whose row index sets are $\Psi_P(m)$, $m \in \mathcal{M}_P$, contains many short loops in common. The size of the matrix H_Q is $|\mathcal{M}_P| \times | \cup_{m \in \mathcal{M}_P} \Psi_P(m)|$.

First the algorithm investigates the loops of short length in the matrix H_Q, then the row index sets for each loop are obtained. Next the set of row vectors H_{Q_1} are produced by linearly combiding the row vectors of H_Q indexed by the above row index sets. These rows are concatenated to H_Q and we obtain a new matrix H_Q^1 such that

$$H_Q^1 = \left[\frac{H_Q}{H_{Q_1}} \right]. \tag{5}$$

If H_Q^1 has a row of weight two, then we go back to the decoding algorithm A for H_Q^1. If the decoding algorithm A stops in failure, we again proceed the same procedure. These procedures continues until all the erased bits are corrected. If the algorithm cannot produce a new row vector or the number of iterations of the above procedures reaches pre-determined value, then the algorithm fails.

4. Simulation Results

4.1. Conditions for Simulation

In order to show the performance of the proposed decoding algorithms, we show the simulation results. We construct codes $\mathcal{C}_1$ and $\mathcal{C}_2$ which are denoted by $\mathcal{C}_1\big(N_1, \lambda_1(x), \rho_1(x)\big)$ and $\mathcal{C}_2\big(N_2, \lambda_2(x), \rho_2(x)\big)$ such that

$$N_1 = 1000,\ \lambda_1(x) = x^2,\ \rho_1(x) = x^5, \qquad (6)$$

$$N_2 = 1000,\ \lambda_2(x) = 0.0769x + 0.6923x^2 + 0.2308x^5,$$
$$\rho_2(x) = 0.46135x^5 + 0.53865x^6. \quad (7)$$

The designed rate of these codes are one half.

We compare the BP decoding algorithm [2] (denoted by "BP"), the decoding algorithm A (denoted by "PropA"), and the decoding algorithm B (denoted by "PropB"). For each decoding algorithm, we transmit at least 10^8 codewords over the BEC with channel erasure probability p until 50 codewords are failed in decoding. In "PropB" we repeate the procedure of investigating the loops of length 4 twice for each received sequence.

We evaluate them by (i) decoding performance as bit erasure rate (BER) and (ii) decoding complexity as the number of Exclusive OR operations needed for decoding.

4.2. Decoding Results and Discussions

4.2.1. Decoding Performance

Figs. 2 and 3 show the decoding performance for the Code $\mathcal{C}_1$ and the $\mathcal{C}_2$, respectively. The horizontal axis and the vertical axis represent the erasure probability of the BEC and BER, respectively.

From Figures. 2 and 3, the performance of both proposed decoding algorithms are superior to that of the "BP". In Fig. 3 at $p = 0.36$, the BER of the "PropA" is 100 times smaller than that of the "BP" and that of the "PropB" is 1000 times smaller than that of the "BP", respectively.

We confirm that there is no significant difference of behavior between BER and the word erasure rate.

4.2.2. Decoding Complexity

The "PropB" can be divided into the following parts of the procedures.

(A) The procedure of computing $\boldsymbol{s}_E$ by $\boldsymbol{c}_{\bar{\mathcal{E}}} H_{\bar{\mathcal{E}}}^{\mathrm{T}}$

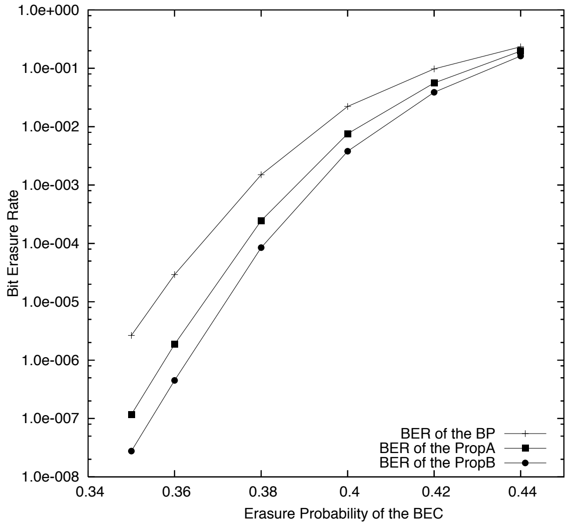

Figure 2: Decoding result of the Code $\mathcal{C}_1$

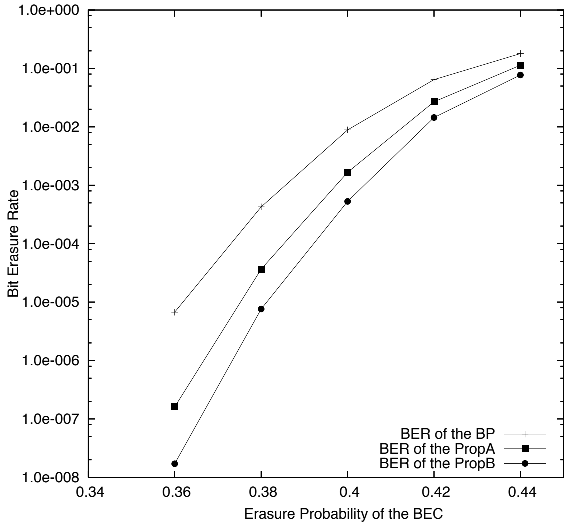

Figure 3: Decoding result of the Code B

(B) The procedure of the "BP"

(C) The procedure of the "PropA" after the "BP" fails

(D) The procedure of the "PropB" after the "PropA" fails except finding the loops of length 4

(E) The procedure of finding the loops in the "PropB"

Clearly the combination of the procedures (A) and (B) equals to the "BP" and the combination of the procedures (A) $\sim$ (C) equals to the "PropA".

Tables 1 and 3 show the average number of decoding operations of decoding procedures (A) $\sim$ (E) for the Code $\mathcal{C}_1$ and the Code $\mathcal{C}_2$, respectively. Tables 2 and 4 show the average number of Exclusive OR operations needed for decoding algorithms of the Code $\mathcal{C}_1$ and the Code $\mathcal{C}_2$, respectively. Notice that we here average the number of computational operations of decoding algorithms over all the transmitted sequences.

Table 1: The number of Exclusive OR operations of each procedure for the Code $\mathcal{C}_1$

p	(A)	(B)	(C)	(D)	(E)
0.35	700	700	948.7	1312.3	3675.7
0.36	719.9	719.9	975	1281.5	3616.8
0.38	757	757	1010.8	1187.2	3661.4
0.4	755.5	755.2	1003.9	1006.1	3725.9
0.42	643.4	641	980.3	799.4	3698.1
0.44	420.9	412.1	828.5	540.8	3652.2

Table 2: The average number of Exclusive OR operations needed by both decoding algorithms for the Code $\mathcal{C}_1$

p	BP	PropA	PropB
0.35	1399.9	1400	1400
0.36	1439.8	1440	1440
0.38	1514	1520.8	1525.4
0.4	1510.7	1604.4	1737.2
0.42	1284.4	1647.7	2535.2
0.44	833	1477.4	4145.7

From these tables, "PropA" and "PropB" need slightly more operations than "BP". Both of these algorithms need much more operations than "BP" as p takes large value. From Tables 1 and 3, the procedure (E) dominates much times in the "PropB". In procedure (E), we only invesitagate the loops of length 4. The computational complexity of the procedure (E) is $O(\{d_{max}c_{max}\}^l)$ where d_{max} and c_{max} represent the maximum weights of rows and columns, respectively if we look for the loops of length l. Therefore the computational complexity of the "PropB" grows large if we look for loops with long length.

5. Concluding Remarks

We have proposed new iterative decoding algorithms of LDPC codes over the BEC. From simulation results, BER of the proposed decoding algorithms are much lower than that of the BP decoding algorithm. They have a favorable trade-off between BER and complexity when the channel erasure probability is a small value.

Table 3: The number of Exclusive OR operations of each procedure for the Code $\mathcal{C}_2$

p	(A)	(B)	(C)	(D)	(E)
0.36	810	810	1014.5	2139.4	7109.1
0.38	854.1	854.1	1071.5	1978.4	6630.1
0.4	881.4	881.4	1095.4	1725.8	6224.7
0.42	809.1	808.3	1059.4	1443.3	6363.9
0.44	610.7	606	981.5	1268.7	6901.1

Table 4: The average number of Exclusive OR operations needed by both decoding algorithms for the Code $\mathcal{C}_2$

p	BP	PropA	PropB
0.36	1619.9	1620	1620
0.38	1708.1	1710	1711.1
0.4	1762.8	1799.8	1845.1
0.42	1617.5	1855.1	2526.5
0.44	1216.7	1782	4590.3

References

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

[2] M. Luby, M. Mitzenmacher, M. A. Shokrollahi, and D. A. Spielman, "Efficient erasure correcting codes," *IEEE Trans. Inform. Theory*, vol. 47, no.2, pp.569–584, Feb. 2001.

[3] C. Di, D. Proietti, I. E. Telatar, T. J. Richardson, and R. L. Urbanke, "Finite-length analysis of low-density parity-check codes on the binary erasure channel," *IEEE Trans. Inform. Theory*, vol. 48, no. 6, pp. 1570–1579, June 2002.

[4] H. Pishro-Nik and F. Fekri, "On decoding of low-density parity-check codes over the binary-erasure channel," *IEEE Trans. Inform. Theory*, vol. 50, no.3, pp.439–454, March 2004.

[5] T. Tian, C. Jones, J. D. Villasenor, and R. D. Wesel, "Selective avoidance of cycles in irregular LDPC code construction," *IEEE Trans. Commun.*, vol. 52, no. 8, pp. 1242–1247, Aug. 2004.

[6] K. Kasai, T. Shibuya, and K. Sakaniwa, "A code-equivalent transformation removing cycles of lenght four in Tanner graphs," (in Japanese) *IEICE Technical Report*, vol.104, no.302, IT2004-42, pp.25–30, Sept. 2004.

[7] G. Hosoya, T. Matsushima, and S. hirasawa, "A decoding method of low-density parity-check codes over the binary erasure channel," *Proc. 27th Symposium on Information Theory and its Applications* (SITA2004), pp. 263-266, Gero, Japan, Dec. 2004.

[8] S. Sankaranarayanan and B. Vasic, "Iterative decoding of linear block codes: A parity-check orthogonalization approach," *IEEE Trans. Inform. Theory*, vol. 51, no.9, pp.3347–3353, Sept. 2005.

[9] N. Kobayashi, T. Matsushima, and S. Hirasawa, "Transformation of a parity-check matrix for a message-passing algorithm over the BEC," *IEICE Trans. Fundamentals*, vol.E89-A, no.5, pp.1299–1306, May 2006.

[10] B. N. Vellambi and F. Fekri, "Results on the improved decoding algorithm for low-density parity-check codes over the binary erasure channel," *IEEE Trans. Inform. Theory*, vol. 53, no.4, pp.1510–1520, April 2007.