PAPER Special Section on Information Theory and Its Applications

Analysis of Error Floors for Non-binary LDPC Codes over General Linear Group through q-Ary Memoryless Symmetric Channels*

Takayuki NOZAKI[†a)], **Kenta KASAI**[†b)], ***Members***, ***and*** **Kohichi SAKANIWA**[†c)], ***Fellow***

SUMMARY In this paper, we compare the decoding error rates in the error floors for non-binary low-density parity-check (LDPC) codes over general linear groups with those for non-binary LDPC codes over finite fields transmitted through the q-ary memoryless symmetric channels under belief propagation decoding. To analyze non-binary LDPC codes defined over both the general linear group $\mathrm{GL}(m, \mathbb{F}_2)$ and the finite field $\mathbb{F}_{2^m}$, we investigate non-binary LDPC codes defined over $\mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}})$. We propose a method to lower the error floors for non-binary LDPC codes. In this analysis, we see that the non-binary LDPC codes constructed by our proposed method defined over general linear group have the same decoding performance in the error floors as those defined over finite field. The non-binary LDPC codes defined over general linear group have more choices of the labels on the edges which satisfy the condition for the optimization.

key words: *non-binary LDPC code, error floor, q-ary memoryless symmetric channel, belief propagation*

1. Introduction

Gallager invented low-density parity-check (LDPC) codes [1]. Due to the sparseness of the parity check matrices, LDPC codes are efficiently decoded by the belief propagation (BP) decoder. Optimized LDPC codes can exhibit performance very close to the Shannon limit [2]. Davey and MacKay [3] have found that non-binary LDPC codes can outperform binary ones.

The finite field of order 2^m is denoted by $\mathbb{F}_{2^m}$. The general linear group of degree m_3 over $\mathbb{F}_{2^{m_4}}$ is the set of $m_3 \times m_3$ invertible matrices over $\mathbb{F}_{2^{m_4}}$ with the operation of ordinary matrix multiplication and matrix inversion, and denoted by $\mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}})$. The finite field $\mathbb{F}_{2^m}$ and the general linear group $\mathrm{GL}(m, \mathbb{F}_2)$ are special cases of $\mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}})$ with $m_3 = 1, m_4 = m$ and $m_3 = m, m_4 = 1$, respectively.

A Tanner graph for a non-binary LDPC code over the general linear group $\mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}})$ is represented by a bipartite graph with variable nodes, check nodes and edges *labeled* by elements in the general linear group $\mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}})$. The v-th variable node and the c-th check node are connected with an edge labeled by $h_{c,v} \in \mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}})$. To simplify the notation, $h_{c,v} = 0 \in \mathbb{F}_{2^{m_3}}^{m_4 \times m_4}$ if the v-th variable node and the c-th check node are not connected. For a given Tanner graph, the code represented by the Tanner graph is given by $\{(\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_N) \in (\mathbb{F}_{2^{m_4}}^{m_3})^N \mid \sum_{j=1}^{N} h_{j,i} \boldsymbol{x}_i^T = \boldsymbol{0}^T \in \mathbb{F}_{2^{m_4}}^{m_3} \ \forall j \in \{1, 2, \ldots, M\}\}$, where N and M are the number of the variable nodes and the check nodes in the Tanner graph, respectively.

It is known that the decoding complexity of non-binary LDPC codes over the general linear group $\mathrm{GL}(m, \mathbb{F}_2)$ is larger than that of non-binary LDPC codes over finite field $\mathbb{F}_{2^m}$ for $m \geq 2$. On the other hand, the decoding error rates in the waterfall region for optimized non-binary LDPC codes over the general linear group $\mathrm{GL}(m, \mathbb{F}_2)$ is lower than those for optimized non-binary LDPC codes over the finite field $\mathbb{F}_{2^m}$ [4].

The error floors are mainly caused by small weight errors. *Zigzag cycles* in the Tanner graphs degrade the error floors since zigzag cycles cause small weight errors. Hence, we are able to lower the error floors if we reduce the decoding errors in the zigzag cycles. To reduce the decoding errors in the zigzag cycles, we need to optimize both the structures of Tanner graphs and the labels on the edges in zigzag cycles. The progressive edge-growth algorithm [5] is a method to optimize the structure of the Tanner graph for the binary and non-binary LDPC codes. This algorithm constructs Tanner graphs which have a large girth, i.e., which do not contain zigzag cycle of small weight. In [6], the authors proposed a method to optimize the labels on the edges in zigzag cycles for non-binary LDPC codes over finite field. This method selects the labels in zigzag cycles to lower the decoding error rates caused by the zigzag cycles.

However, it has been not proposed to select the labels for lowering the decoding error rates in error floors for non-binary LDPC codes over general linear groups $\mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}})$ and $\mathrm{GL}(m, \mathbb{F}_2)$. Moreover, the decoding error rates in the error floors for non-binary LDPC codes over the general linear group $\mathrm{GL}(m, \mathbb{F}_2)$ have not been compared with those for non-binary LDPC codes over the finite field $\mathbb{F}_{2^m}$.

In this paper, we define non-binary LDPC codes over the general linear group $\mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}})$ and BP decoding algorithm to analyze the non-binary LDPC codes over both the finite field $\mathbb{F}_{2^m}$ and the general linear group $\mathrm{GL}(m, \mathbb{F}_2)$. We assume q-ary memoryless symmetric (q-MS) channels [7] for the generality of the channels. We extend the label optimization and analysis method in [6] to the non-binary LDPC codes over the general linear groups $\mathrm{GL}(m, \mathbb{F}_2)$ and $\mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}})$ transmitted through the q-MS channels. More

Manuscript received February 10, 2012.
Manuscript revised June 23, 2012.

[†]The authors are with the Dept. of Communications and Integrated Systems, Tokyo Institute of Technology, Tokyo, 152-8550 Japan.

*The material in this paper was presented in part at IEEE International Symposium on Information Theory (ISIT2012).

a) E-mail: nozaki@comm.ss.titech.ac.jp
b) E-mail: kenta@comm.ss.titech.ac.jp
c) E-mail: sakaniwa@comm.ss.titech.ac.jp

DOI: 10.1587/transfun.E95.A.2113

precisely, first, we derive the condition for successful decoding of zigzag cycle code. Next, we propose a method to lower the decoding error rates in the error floors for non-binary LDPC codes over $\mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}})$. Moreover, we show lower bounds on the symbol error rates in the error floors for non-binary LDPC codes over $\mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}})$. Furthermore, some simulation results show that the lower bounds on symbol error rates in the error floors are tight for the non-binary LDPC codes constructed by our proposed method.

This paper is organized as follows: In Sect. 2, we define non-binary LDPC code and introduce the q-MS channel. In Sect. 3, we propose a method to lower the error floors by analyzing the zigzag cycles. In Sect. 4, we derive lower bounds for symbol error rates in the error floors for non-binary LDPC codes.

2. Preliminaries

In this section, we define the non-binary LDPC code over $\mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}})$ and recall the 2^{m_1}-MS channel [7]. Moreover, we introduce BP decoding algorithm for the non-binary LDPC codes over $\mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}})$ through the 2^{m_1}-MS channels.

2.1 Non-binary LDPC Code over $\mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}})$

For the non-binary LDPC codes over $\mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}})$, the Tanner graphs are represented by sparse bipartite graphs with variable nodes, check nodes and edges labeled by elements in $\mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}})$. Let N and M be the number of variable nodes and check nodes, respectively. We denote the label on the edge adjacent to the v-th variable node and the c-th check node, by $h_{c,v} \in \mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}})$. To simplify the notation, $h_{c,v} = 0 \in \mathbb{F}_{2^{m_3}}^{m_4 \times m_4}$ if the v-th variable node and the c-th check node are not connected. Define $[a, b] := \{n \in \mathbb{Z} \mid a \le n \le b\}$ for the integers $a, b \in \mathbb{Z}$. Note that $[a, b] = \emptyset$ if $a > b$. For a given Tanner graph, the code represented by the Tanner graph is given by $\{(\boldsymbol{x}_i)_{i\in[1,N]} \in (\mathbb{F}_{2^{m_4}}^{m_3})^N \mid \sum_{i=1}^{N} h_{j,i}\boldsymbol{x}_i^T = \boldsymbol{0}^T \in \mathbb{F}_{2^{m_4}}^{m_3} \ \forall j \in [1, M]\}$, where $(\boldsymbol{x}_i)_{i\in[1,N]}$ represents the vector $(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_N)$.

Let α be a primitive element $\mathbb{F}_{2^{m_4}}$. Once a primitive element α is fixed, each element in $\mathbb{F}_{2^{m_4}}$ is given by an m_4-bit representation [8, p.110]. Since $\gamma \in \mathbb{F}_{2^{m_4}}^{m_3}$ is represented by $m_3 m_4$ bits as $(\gamma_i)_{i\in[1,m_3m_4]}$, the codeword $(\boldsymbol{x}_i)_{i\in[1,N]} \in (\mathbb{F}_{2^{m_4}}^{m_3})^N$ is represented as a binary codeword $(x_{i,j})_{i\in[1,N],j\in[1,m_3m_4]}$.

Note that the non-binary LDPC codes over $\mathbb{F}_{2^m} = \mathrm{GL}(1, \mathbb{F}_{2^m})$ and over $\mathrm{GL}(m, \mathbb{F}_2)$ are special case for the non-binary LDPC codes over $\mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}})$ with $m_3 = 1, m_4 = m$ and $m_3 = m, m_4 = 1$, respectively.

2.2 2^{m_1}-Ary Memoryless Symmetric Channel [7]

In this paper, we consider the q-MS channel, where $q = 2^{m_1}$. For the 2^{m_1}-ary channel, the number of input alphabet $\mathcal{X}$ is 2^{m_1}. We assume $\mathcal{X} = \mathbb{F}_2^{m_1}$. Let $\mathcal{Y}$ be a given continuous (or discrete) output alphabet. We denote the channel transition probability by $p(y \mid x)$, where $x \in \mathcal{X}$ and $y \in \mathcal{Y}$. The q-ary memoryless channel is *symmetric* if there exists a function $\mathcal{T} : \mathcal{Y} \times \mathcal{X} \to \mathcal{Y}$ satisfying the following properties:

1. For every $x \in \mathcal{X}$, the function $\mathcal{T}(\cdot, x) : \mathcal{Y} \to \mathcal{Y}$ is bijective.
2. For every $x_1, x_2 \in \mathcal{X}$ and $y \in \mathcal{Y}$, $p(y \mid x_1) = p(\mathcal{T}(y, x_2 - x_1) \mid x_2)$ holds.
3. For channels whose output alphabet $\mathcal{Y}$ is continuous, the mapping $\mathcal{T}$ is that its Jacobian is equal to 1.

We denote $a \mid b$ if a divides b. We assume $m_1 \mid m_3 m_4$ and denote $m_2 = m_3 m_4 / m_1$. Then, the symbol $\boldsymbol{x}_v \in \mathbb{F}_{2^{m_4}}^{m_3}$ in the v-th variable node is represented as m_2 channel inputs to the 2^{m_1}-MS channel for all $v \in [1, N]$. For a given codeword, we denote the channel outputs by $(y_{i,j})_{i\in[1,N],j\in[1,m_2]} \in \mathcal{Y}^{Nm_2}$.

Example 1: The 2^{m_1}-ary symmetric channel (2^{m_1}-SC) is an example of the 2^{m_1}-MS channel. For the 2^{m_1}-SC, the input and output alphabets are $\mathcal{X} = \mathcal{Y} = \mathbb{F}_2^{m_1}$ and transition probability function is

$$p(y \mid x) = \begin{cases} 1 - \epsilon, & x = y, \\ \epsilon/(2^{m_1} - 1), & x \neq y, \end{cases}$$

where ϵ is referred as *channel error probability*.

The memoryless binary-input output-symmetric (MBI-OS) channel is also an example of the 2^{m_1}-MS channel [7, Example 1].

2.3 Belief Propagation Decoder

BP decoding proceeds by sending *messages* along the edges in the Tanner graph. The messages arising in the BP decoder for LDPC codes over $\mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}})$ are vectors of length 2^m, where $m = m_3 m_4$. Let $\Psi_{v,c}^{(\ell)}$ (resp. $\Phi_{c,v}^{(\ell)}$) be the message from the v-th variable node (resp. c-th check node) to the c-th check node (resp. v-th variable node) at the ℓ-th iteration.

2.3.1 Initialization

Set $\ell = 0$. For $v \in [1, N]$, let $C_v = (C_v(x))_{x\in\mathbb{F}_{2^{m_4}}^{m_3}}$ denote the initial message of the v-th variable node. For $\gamma \in \mathbb{F}_{2^{m_4}}^{m_3}$, the element of the initial message $C_v(\gamma)$ is given from the channel outputs as follows:

$$C_v(\gamma) = \textstyle\prod_{i=1}^{m_2} p(y_{v,i} \mid (\gamma_j)_{j\in[m_1(i-1)+1,m_1 i]}).$$

Let $\mathcal{N}_{\mathrm{c}}(c)$ (resp. $\mathcal{N}_{\mathrm{v}}(v)$) be the set of the positions of the variable nodes (resp. check nodes) connecting to the c-th check node (resp. v-th variable node). Set $\Phi_{c,v}^{(0)} = (2^{-m}, 2^{-m}, \ldots, 2^{-m})$ for all $c \in [1, M]$ and $v \in \mathcal{N}_{\mathrm{c}}(c)$.

2.3.2 Iteration

Iteratively repeat the following two steps for $\ell \in \{0, 1, \ldots\}$.

(1) Variable node calculation

The message $\Psi_{v,c}^{(\ell)}$ is given by the component-wise multiplication of the initial message C_v and the incoming messages

$\Phi^{(\ell)}_{c',v}$ from check nodes whose positions c' are in $\mathcal{N}_{\mathrm{v}}(v) \setminus \{c\}$, i.e., for $x \in \mathbb{F}_{2^{m_4}}^{m_3}$

$$\Psi^{(\ell)}_{v,c}(x) = \xi^{-1} C_v(x) \prod_{c' \in \mathcal{N}_{\mathrm{v}}(v)\setminus\{c\}} \Phi^{(\ell)}_{c',v}(x),$$

where ξ is a normalization factor such that $1 = \sum_{x \in \mathbb{F}_{2^{m_4}}^{m_3}} \Psi^{(\ell)}_{v,c}(x)$.

(2) Check node calculation

The convolution of two vectors Ψ_1 and Ψ_2 is given by

$$[\Psi_1 \oplus \Psi_2](x) = \sum_{y,z \in \mathbb{F}_{2^{m_4}}^{m_3} : x = y+z} \Psi_1(y)\Psi_2(z),$$

where $\sum_{y,z \in \mathbb{F}_{2^{m_4}}^{m_3} : x=y+z} \Psi_1(y)\Psi_2(z)$ is the sum of $\Psi_1(y)\Psi_2(z)$ over all $y, z \in \mathbb{F}_{2^{m_4}}^{m_3}$ such that $x = y + z$. To simplify the notation, we define $\bigoplus_{i \in [1,k]} \Psi_i := \Psi_1 \oplus \Psi_2 \oplus \cdots \oplus \Psi_k$. The message $\Phi^{(\ell+1)}_{c,v}$ is given as, for $x \in \mathbb{F}_{2^{m_4}}^{m_3}$

$$\check{\Psi}^{(\ell)}_{v,c}(x) = \Psi^{(\ell)}_{v,c}\left(h^{-1}_{c,v} x\right),$$
$$\check{\Phi}^{(\ell+1)}_{c,v} = \bigoplus_{v' \in \mathcal{N}_{\mathrm{c}}(c)\setminus\{v\}} \check{\Psi}^{(\ell)}_{v',c},$$
$$\Phi^{(\ell+1)}_{c,v}(x) = \check{\Phi}^{(\ell+1)}_{c,v}(h_{c,v} x).$$

2.3.3 Decision

Define

$$\mathrm{argmax}_{x \in \mathbb{F}_{2^{m_4}}^{m_3}} \Psi := \{x \in \mathbb{F}_{2^{m_4}}^{m_3} \mid \forall y \in \mathbb{F}_{2^{m_4}}^{m_3}, \Psi(x) \geq \Psi(y)\},$$

and for $x \in \mathbb{F}_{2^{m_4}}^{m_3}$

$$D^{(\ell)}_v(x) := \xi^{-1} C_v(x) \prod_{c \in \mathcal{N}_{\mathrm{v}}(v)} \Phi^{(\ell)}_{c,v}(x),$$

where ξ is a normalization factor such that $1 = \sum_{x \in \mathbb{F}_{2^{m_4}}^{m_3}} D^{(\ell)}_v(x)$. For $v \in [1, N]$, let $\hat{x}^{(\ell)}_v \in \mathbb{F}_{2^{m_4}}^{m_3}$ be the decoding output of the v-th variable node. Define $\mathcal{D}^{(\ell)}_v := \mathrm{argmax}_{x \in \mathbb{F}_{2^{m_4}}^{m_3}} D^{(\ell)}_v(x)$. We denote the cardinality of the set $\mathcal{D}$, by $|\mathcal{D}|$. If $|\mathcal{D}^{(\ell)}_v| = 1$, the decoding output $\hat{x}^{(\ell)}_v$ is the unique element of $\mathcal{D}^{(\ell)}_v$. If $|\mathcal{D}^{(\ell)}_v| > 1$, the decoder chooses $\hat{x}^{(\ell)}_v \in \mathcal{D}^{(\ell)}_v$ with probability $1/|\mathcal{D}^{(\ell)}_v|$.

2.4 Decoding Failure and All-Zero Codeword Assumption

The v-th symbol is *eventually correct* [9] if there exists L_v such that for all $\ell > L_v$, $\hat{x}^{(\ell)}_v = \boldsymbol{x}_v$. The symbol error rate is defined by the fraction of the symbol which is not eventually correct.

The following lemma shows that *all-zero codeword assumption* holds for non-binary LDPC code over $\mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}})$ transmitted through the 2^{m_1}-MS channel under BP decoding.

Lemma 1: For the non-binary LDPC codes over $\mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}})$ transmitted through the 2^{m_1}-MS channel under BP decoding, the symbol error probability is independent of the transmitted codeword.

The proof of this lemma is in Appendix A. From this lemma, we are able to assume that the all-zero codewords are sent without loss of generality to analyze the decoding error probability.

3. Zigzag Cycle Code Analysis

A zigzag cycle is a *circuit* [10] such that the degrees of all the variable nodes in the circuit are two. A zigzag cycle of weight w consists of w variable nodes of degree two. The zigzag cycle code is defined by a Tanner graph which forms a single zigzag cycle. Figure 1 shows a zigzag cycle code of symbol code length w.

In this section, we give a condition for successful decoding for the zigzag cycle codes through the 2^{m_1}-MS channels under BP decoding and introduce Bhattacharyya functional for the 2^{m_1}-MS channels.

3.1 Condition for Successful Decoding

We consider the zigzag cycle code of symbol code length w with labels $h_{1,1}, h_{1,2}, \ldots, h_{w,w}, h_{w,1} \in \mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}})$ as shown in Fig. 1. For any $m_3 \times m_3$ matrices $A_1, A_2, \ldots, A_k$, we denote $\prod_{i=1}^{k} A_k := A_1 A_2 \cdots A_k$. We define $\iota_i := h^{-1}_{i,i} h_{i,i+1}$, where $h_{w,w+1} := h_{w,1}$. Define $\chi := \sum_{i=1}^{w} \iota_i \in \mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}})$.

Definition 1: Let $\langle \chi \rangle$ be the cyclic subgroup generated by χ, i.e., $\langle \chi \rangle := \{\chi^j \mid j = 0, 1, 2, \ldots\}$. The relation $\sim$ on $\mathbb{F}_{2^{m_4}}^{m_3}$ defined by $x \sim y$ is an equivalence relation on $\mathbb{F}_{2^{m_4}}^{m_3}$, if and only if there exists $g \in \langle \chi \rangle$ such that $gx = y$. The equivalence class of $x \in \mathbb{F}_{2^{m_4}}^{m_3}$ under this relation is $\langle \chi \rangle x = \{gx \mid g \in \langle \chi \rangle\}$, and is called the *orbit* of x under $\langle \chi \rangle$. The set of orbits of $x \in \mathbb{F}_{2^{m_4}}^{m_3} \setminus \{0\}$ under $\langle \chi \rangle$ forms a *partition* of $\mathbb{F}_{2^{m_4}}^{m_3} \setminus \{0\}$, i.e., every element in $\mathbb{F}_{2^{m_4}}^{m_3} \setminus \{0\}$ belongs exactly one of equivalence classes. A set of class representatives S_χ is a subset of $\mathbb{F}_{2^{m_4}}^{m_3} \setminus \{0\}$ which contains exactly one elements from each equivalent class.

The following lemma gives the condition for successful decoding for zigzag cycle codes under BP decoding by a set of class representatives S_χ and the initial messages.

Lemma 2: We consider a zigzag cycle code of symbol code length w labeled by $h_{1,1}, h_{1,2}, \ldots, h_{w,w}, h_{w,1} \in \mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}})$ transmitted through the 2^{m_1}-MS channel. Assume that the all-zero codewords are sent without loss of generality. Let $\iota_i = h^{-1}_{i,i} h_{i,i+1}$ for $i \in [1, w]$, where $h_{w+1,w} = h_{1,w}$. The matrix χ is given by $\chi = \prod_{i=1}^{w} \iota_i \in \mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}})$.

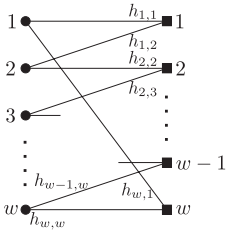

Fig. 1 A zigzag cycle code of symbol code length w.

Define S_χ as in Definition 1. In the limit of large ℓ, all the symbols in the zigzag cycle code are eventually correct under BP decoding if and only if for all $x \in S_\chi$,

$$\prod_{t=0}^{|\langle\chi\rangle x|-1} \prod_{s=1}^{w} C_s(0) > \prod_{t=0}^{|\langle\chi\rangle x|-1} \prod_{s=1}^{w} C_s\left(\left(\prod_{j=s}^{w} \iota_j\right)\chi^t x\right).$$

Moreover, in the limit of large ℓ, no symbols in the zigzag cycle code are eventually correct under BP decoding if and only if there exists $x \in S_\chi$ such that

$$\prod_{t=0}^{|\langle\chi\rangle x|-1} \prod_{s=1}^{w} C_s(0) \le \prod_{t=0}^{|\langle\chi\rangle x|-1} \prod_{s=1}^{w} C_s\left(\left(\prod_{j=s}^{w} \iota_j\right)\chi^t x\right).$$

The proof of this lemma is in Appendix B. By using Lemma 2, we have the following theorem.

Theorem 1: Define S_χ as in Definition 1. For a fixed channel output, if the zigzag cycle with a matrix χ such that $|S_\chi| > 1$ is successfully decoded, the zigzag cycle with a matrix $\tilde{\chi}$ such that $|S_{\tilde{\chi}}| = 1$ is also successfully decoded.

proof: We consider a zigzag cycle of symbol code length w. Since the channel output is fixed, the initial messages C_i for $i \in [1, w]$ are also fixed. From Lemma 2, if the zigzag cycle with a matrix χ such that $|S_\chi| > 1$ is successfully decoded, for all $x \in S_\chi$

$$\prod_{s=1}^{w} C_s(0)^{|\langle\chi\rangle x|} > \prod_{t=0}^{|\langle\chi\rangle x|-1} \prod_{s=1}^{w} C_s\left(\left(\prod_{j=s}^{w} \iota_j\right)\chi^t x\right).$$

Since the set of the orbits $\langle\chi\rangle x$ forms a partition of $\mathbb{F}_{2^{m_4}}^{m_3} \setminus \{0\}$, $\cup_{x\in S_\chi}\langle\chi\rangle x = \mathbb{F}_{2^{m_4}}^{m_3} \setminus \{0\}$ holds. From the product of the above equation over all $x \in S_\chi$, we have

$$\begin{aligned}
&\prod_{x\in S_\chi} \prod_{s=1}^{w} C_s(0)^{|\langle\chi\rangle x|} \\
&\quad > \prod_{x\in S_\chi} \prod_{t=0}^{|\langle\chi\rangle x|-1} \prod_{s=1}^{w} C_s\left(\left(\prod_{j=s}^{w} \iota_j\right)\chi^t x\right) \\
&\iff \prod_{s=1}^{w} C_s(0)^{2^{m_3m_4}-1} > \prod_{x\in\mathbb{F}_{2^{m_4}}^{m_3}} \prod_{s=1}^{w} C_s(x). \qquad (1)
\end{aligned}$$

Similarly, for a matrix $\tilde{\chi}$ such that $|S_{\tilde{\chi}}| = 1$ and $x \in S_{\tilde{\chi}}$, $\langle\tilde{\chi}\rangle x = \mathbb{F}_{2^{m_4}}^{m_3} \setminus \{0\}$. Hence, from Lemma 2, if the zigzag cycle with a matrix $\tilde{\chi}$ such that $|S_{\tilde{\chi}}| = 1$ is successfully decoded,

$$\prod_{s=1}^{w} C_s(0)^{2^{m_3m_4}-1} > \prod_{x\in\mathbb{F}_{2^{m_4}}^{m_3}} \prod_{s=1}^{w} C_s(x).$$

Since this condition coincides with Eq. (1), the zigzag cycle with a matrix $\tilde{\chi}$ such that $|S_{\tilde{\chi}}| = 1$ is also successfully decoded. □

Theorem 1 shows that a condition for lowering the error floor depends on the cardinality of a set of class representatives S_χ. The order σ_χ of the matrix χ is the smallest positive integer satisfying that χ^{σ_χ} is $m_3 \times m_3$ identity matrix. The following lemma gives a relation between the cardinality of a set of class representatives and the order of χ.

Lemma 3: The order of the matrix χ is $2^{m_3m_4} - 1$ if and only if $|S_\chi| = 1$.

This lemma is proved in Appendix C.

Discussion 1: By combining Theorem 1 and Lemma 3, we see that the zigzag cycles with the matrices χ of the order $2^{m_3m_4} - 1$ have the best decoding performance. By using this condition, we propose a method to lower the error floors for non-binary LDPC codes as follows: designing the labels in the zigzag cycles of small weight as the order of χ satisfies $2^{m_3m_4} - 1$.

The log-likelihood ratio for the 2^{m_1}-ary channels are defined in [11]. For $\gamma \in \mathbb{F}_2^{m_1}$, let $Z_{v,i}(Y_{v,i}, \gamma)$ denote the log-likelihood ratio corresponding to the i-th channel output $y_{v,i}$ in the v-th variable node, i.e.,

$$Z_{v,i}(y_{v,i}, \gamma) := \log \frac{p(y_{v,i} \mid 0)}{p_i(y_{v,i} \mid \gamma)}. \qquad (2)$$

The following corollary gives the condition for successful decoding for the zigzag cycle codes with the matrices χ of the order $2^{m_3m_4} - 1$ through the 2^{m_1}-MS channel by using the log-likelihood ratio.

Corollary 1: We consider the zigzag cycle codes of symbol code length w with the matrices χ of the order $2^{m_3m_4} - 1$ through the 2^{m_1}-MS channel. For $\gamma \in \mathbb{F}_2^{m_1}$, $i \in [1, m_2]$ and $v \in [1, N]$, let $Z_{v,i}(Y_{v,i}, \gamma)$ define as in Eq. (2). In the limit of large ℓ, all the symbols in the zigzag cycle code are eventually correct if and only if

$$\sum_{v=1}^{w} \sum_{i=1}^{m_2} \sum_{\gamma\in\mathbb{F}_2^{m_1}\setminus\{0\}} Z_{v,i}(Y_{v,i}, \gamma) > 0.$$

Moreover, in the limit of large ℓ, no symbols in the zigzag cycle code are eventually correct if and only if

$$\sum_{v=1}^{w} \sum_{i=1}^{m_2} \sum_{\gamma\in\mathbb{F}_2^{m_1}\setminus\{0\}} Z_{v,i}(Y_{v,i}, \gamma) \le 0.$$

proof: The initial messages are represented as $C_v(\gamma) = \prod_{i=1}^{m_2} p(y_{v,i} \mid \underline{\gamma}_i)$, where $\underline{\gamma}_i := (\gamma_j)_{j\in[m_1(i-1)+1, m_1 i]}$ for $\gamma \in \mathbb{F}_{2^{m_4}}^{m_3}$ and $i \in [1, m_2]$. Hence, we have for $v \in [1, w]$,

$$\begin{aligned}
&C_v(0) = \prod_{i=1}^{m_2} p(y_{v,i} \mid 0), \\
&\prod_{\gamma\in\mathbb{F}_{2^{m_4}}^{m_3}} C_v(\gamma) = \prod_{i=1}^{m_2} \prod_{x\in\mathbb{F}_2^{m_1}} p(y_{v,i} \mid x)^{2^{m-m_1}}.
\end{aligned}$$

Hence, from Theorem 1, all the symbols in the zigzag cycles are eventually correct if and only if

$$\begin{aligned}
&\prod_{v=1}^{w} C_v(0)^{2^m-1} > \prod_{v=1}^{w} \prod_{x\in\mathbb{F}_{2^{m_4}}^{m_3}\setminus\{0\}} C_v(x) \\
&\iff \prod_{v=1}^{w} \prod_{i=1}^{m_2} \prod_{x\in\mathbb{F}_2^{m_1}\setminus\{0\}} \frac{p(y_{v,i} \mid 0)^{2^{m-m_1}}}{p(y_{v,i} \mid x)^{2^{m-m_1}}} > 1 \\
&\iff \sum_{v=1}^{w} \sum_{i=1}^{m_2} \sum_{x\in\mathbb{F}_2^{m_1}\setminus\{0\}} Z(y_{v,i}, x) > 0.
\end{aligned}$$

Similarly, we derive the necessary and sufficient condition for which no symbols in the zigzag cycles are eventually correct from Theorem 1. This concludes the proof. □

3.2 Bhattacharyya Functional and Decoding Error Rate

We define the random variable $L(Y)$ as

$$L(Y) := \sum_{\gamma\in\mathbb{F}_2^{m_1}\setminus\{0\}} \log \frac{p(Y \mid 0)}{p(Y \mid \gamma)}.$$

Let a denote the conditional probability density function of

the random variable $L(Y)$ given that the corresponding channel input is zero. We refer the function a as *L-density*. Note that in the case for the MBIOS channels, i.e., $m_1 = 1$, L-density defined in the above gives the definition of the L-density in [12, p.178].

Definition 2: For a L-density a, the *Bhattacharyya functional* $\mathfrak{B}(\mathsf{a})$ is defined as $\mathfrak{B}(\mathsf{a}) := \int_{-\infty}^{\infty} \mathsf{a}(x)\exp[-x/2]\mathrm{d}x$.

In Definition 2, we assume not only *symmetric* L-density [12] but also *asymmetric* L-density. The following facts show the properties of the Bhattacharyya functional.

Fact 1: For L-density a_1 and a_2, $\mathfrak{B}(\mathsf{a}_1 * \mathsf{a}_2) = \mathfrak{B}(\mathsf{a}_1)\mathfrak{B}(\mathsf{a}_2)$ holds, where $*$ denotes the convolution, i.e., $(\mathsf{a}_1 * \mathsf{a}_2)(x) := \int_{-\infty}^{\infty} \mathsf{a}_1(x-y)\mathsf{a}_2(y)\mathrm{d}y$.

Fact 2: Let Z denote the random variable with L-density a. Then, $\Pr(Z \le 0) \le \mathfrak{B}(\mathsf{a})$.

The following corollary gives the decoding error rates for zigzag cycle codes with the matrices χ of the order $2^{m_3m_4} - 1$.

Corollary 2: Denote $m = m_1m_2$. Let $\mathrm{P}_{zz}(w, m_1, m_2, \mathsf{a})$ be the symbol error rate for the zigzag cycle codes defined over $\mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}})$ of symbol code length w with matrices χ such that $\sigma_\chi = 2^m - 1$, through the 2^{m_1}-MS channel with L-density a under BP decoding. Let $Z_1, Z_2, \ldots, Z_k$ denote independent and identically distributed random variables with L-density a. Define $Z^{(k)} := \sum_{v=1}^{k} Z_v$. The Bhattacharyya functional is defined in Definition 2. We have the symbol error rates of the zigzag cycle codes is given by

$$\mathrm{P}_{zz}(w, m_1, m_2, \mathsf{a}) = \Pr(Z^{(m_2w)} \le 0) \le \mathfrak{B}(\mathsf{a})^{m_2w}. \tag{3}$$

proof: Corollary 1 implies that $\mathrm{P}_{zz}(w, m_1, m_2, \mathsf{a}) = \Pr(Z^{(m_2w)} \le 0)$. From Fact 1 and 2, we have $\Pr(Z^{(m_2w)} \le 0) \le \mathfrak{B}(\mathsf{a})^{m_2w}$. □

Corollary 2 shows that for a fixed weight w and $m = m_3m_4$, the decoding error rate of the zigzag cycle code does not depend on m_3 or m_4. In other words, the decoding error rates for the zigzag cycles over the general linear group $\mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}})$ are equal to those for the zigzag cycles over the finite field $\mathbb{F}_{2^m}$ for a fixed weight w and $m = m_3m_4$.

4. Analysis of Error Floors

In the previous section, we give the decoding error rates for the zigzag cycle codes. By using this result, in this section, we give lower bounds on the symbol error rates in the error floors for the non-binary LDPC code ensembles through the 2^{m_1}-MS channels under BP decoding.

First, we define the expurgation ensembles for non-binary LDPC codes over $\mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}})$.

Definition 3: Let $\mathrm{LDPC}(N, \mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}}), \lambda, \rho)$ denote the LDPC code ensemble of symbol code length N over $\mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}})$ defined by Tanner graphs with a degree distribution pair (λ, ρ) [12] and elements in $\mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}})$ are chosen as the labels on edges with equal probability. Let $w_\mathrm{g} \in \mathbb{N} := \{1, 2, \ldots\}$ be an expurgation parameter. The expurgated ensemble $\mathrm{ELDPC}(N, \mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}}), \lambda, \rho, w_\mathrm{g})$ consists of the subset of codes in $\mathrm{LDPC}(N, \mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}}), \lambda, \rho)$ which contain no stopping sets of weight in $[1, w_\mathrm{g} - 1]$. Let $w_\mathrm{c} \in \mathbb{N}$ be an expurgation parameter for labeling in the Tanner graph, where $w_\mathrm{g} \le w_\mathrm{c}$. Define the expurgated ensemble $\mathrm{ELDPC}(N, \mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}}), \lambda, \rho, w_\mathrm{g}, w_\mathrm{c}, \mathcal{H})$ as the subset of codes in $\mathrm{ELDPC}(N, \mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}}), \lambda, \rho, w_\mathrm{g})$ which contain no zigzag cycles of weight in $[w_\mathrm{g}, w_\mathrm{c}-1]$ with the matrix $\chi \in \mathcal{H}$.

Define

$$\mathcal{H}^*_{m_3,m_4} := \{\chi \in \mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}}) \mid \sigma_\chi < 2^{m_3m_4} - 1\}.$$

From Discussion 1, to lower the error floors, we need to avoid the zigzag cycles with the matrices $\chi \in \mathcal{H}^*_{m_3,m_4}$. Since $|\mathrm{GL}(m, \mathbb{F}_2)\backslash\mathcal{H}^*_{m,1}| \ge |\mathbb{F}_{2^m}\backslash\mathcal{H}^*_{1,m}|$, the non-binary LDPC codes defined over the general linear group $\mathrm{GL}(m, \mathbb{F}_2)$ have more choices of the labels on the edges which satisfy the condition for the optimization.

4.1 Analysis of Error Floors

In this section, we analyze the symbol error rates in the error floors for the expurgated ensembles defined in Definition 3. The following theorem gives a lower bound on the symbol error rate under BP decoding for the expurgated ensemble $\mathrm{ELDPC}(N, \mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}}), \lambda, \rho, w_\mathrm{g}, w_\mathrm{c}, \mathcal{H}^*_{m_3,m_4})$.

Theorem 2: Denote $m = m_1m_2 = m_3m_4$. Let $\mathrm{P_s}(\mathrm{ELDPC}, \mathsf{a}, m_1, m_2)$ be the symbol error rate of the expurgated ensemble $\mathrm{ELDPC}(N, \mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}}), \lambda, \rho, w_\mathrm{g}, w_\mathrm{c}, \mathcal{H}^*_{m_3,m_4})$ through the 2^{m_1}-MS channel characterized by its L-density a under BP decoding. Define $Z^{(k)}$ as in Corollary 2. For sufficiently large N and $\mathfrak{B}(\mathsf{a}) < \mu^{-1/m_2}$, the symbol error rate is lower bounded by

$$\mathrm{P_s}(\mathrm{ELDPC}, \mathsf{a}, m_1, m_2) \ge \frac{1}{2N}\sum_{w=w_\mathrm{g}}^{\infty} \mu^w \Pr(Z^{(m_2w)} \le 0). \tag{4}$$

proof: Corollary 2 shows that the symbol error rates of the zigzag cycles of weight w with matrices χ such that $\sigma_\chi = 2^m - 1$ are $\Pr(Z^{(m_2w)} \le 0)$. Moreover, by combining Discussion 1 and Corollary 2, we see that the symbol error rates of the zigzag cycles of weight w with matrices χ such that $\sigma_\chi \ne 2^m - 1$ are lower bounded by $\Pr(Z^{(m_2w)} \le 0)$. By using technique in the proof of Theorem 2 in [6], we have Eq. (4). From Corollary 2, we get

$$\textstyle\sum_{w=w_\mathrm{g}}^{\infty} \mu^w \Pr(Z^{(m_2w)} \le 0) \le \sum_{w=w_\mathrm{g}}^{\infty} \mu^w \mathfrak{B}(\mathsf{a})^{m_2w}.$$

Thus, for sufficiently large N and $\mathfrak{B}(\mathsf{a}) < \mu^{-1/m_2}$, the left hand side of this inequality converges. □

For a given channel and a fixed μ, m, the decoding error rate for the non-binary LDPC code ensemble over finite field $\mathbb{F}_{2^m}$ is same as that for the non-binary LDPC code ensemble over $\mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}})$ such that $m = m_3m_4$.

4.2 Simulation Results

In this section, we compare the symbol error rates in the error floors for the expurgated ensembles constructed by proposed method with that for non-optimized ensembles. In the simulation results of this section, we do not employ the methods which reduce the decoding error rates in waterfall regions [4], [13]. Hence, there are no gains in the waterfall regions for non-binary LDPC codes over general linear groups.

Figure 2 shows the symbol error rates for the expurgated ensembles ELDPC$(315, \mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}}), x, x^2, 1, 8, \mathcal{H})$ transmitted through the binary additive white Gaussian noise channel for $m_3 = 1, m_4 = 4, \mathcal{H} = \mathcal{H}^*_{1,4}$ ($\mathbb{F}_{2^4}$ Proposed), for $m_3 = 4, m_4 = 1, \mathcal{H} = \emptyset$ ($\mathrm{GL}(4, \mathbb{F}_2)$ Random) and for $m_3 = 4, m_4 = 1, \mathcal{H} = \mathcal{H}^*_{4,1}$ ($\mathrm{GL}(4, \mathbb{F}_2)$ Proposed). The lower bound is derived from Eq. (4). Figure 3 shows the symbol error rates for the expurgated ensemble ELDPC$(315, \mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}}), x, x^2, 1, 8, \mathcal{H})$ transmitted through the 2^4-SC for $m_3 = 1, m_4 = 4, \mathcal{H} = \emptyset$ ($\mathbb{F}_{2^4}$ Random), for $m_3 = 1, m_4 = 4, \mathcal{H} = \mathcal{H}^*_{1,4}$ ($\mathbb{F}_{2^4}$ Proposed), for $m_3 = 4, m_4 = 1, \mathcal{H} = \emptyset$ ($\mathrm{GL}(4, \mathbb{F}_2)$ Random) and for $m_3 = 4, m_4 = 1, \mathcal{H} = \mathcal{H}^*_{4,1}$ ($\mathrm{GL}(4, \mathbb{F}_2)$ Proposed). The lower bound is given by Eq. (4). From Figs. 2 and 3, we see that the proposed codes exhibit better decoding performance than non-optimized codes. The lower bound Eq. (4) gives tight lower bounds for the symbol error rates to the proposed codes. Moreover, we see that the decoding performance in the error floors for codes constructed by proposed method depend only on the size of $m_3 m_4$.

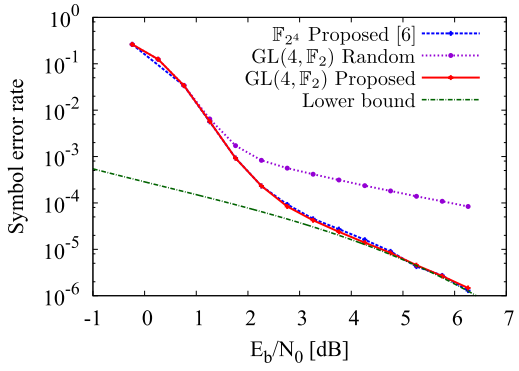

Fig. 2 The symbol error rates for the expurgated ensembles ELDPC$(315, \mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}}), x, x^2, 1, 8, \mathcal{H})$ transmitted through the binary additive white Gaussian noise channel for $m_3 = 1$, $m_4 = 4$, $\mathcal{H} = \mathcal{H}^*_{1,4}$ ($\mathbb{F}_{2^4}$ Proposed), for $m_3 = 4$, $m_4 = 1$, $\mathcal{H} = \emptyset$ ($\mathrm{GL}(4, \mathbb{F}_2)$ Random), and for $m_3 = 4$, $m_4 = 1$, $\mathcal{H} = \mathcal{H}^*_{4,1}$ ($\mathrm{GL}(4, \mathbb{F}_2)$ Proposed). The lower bound is given by Eq. (4).

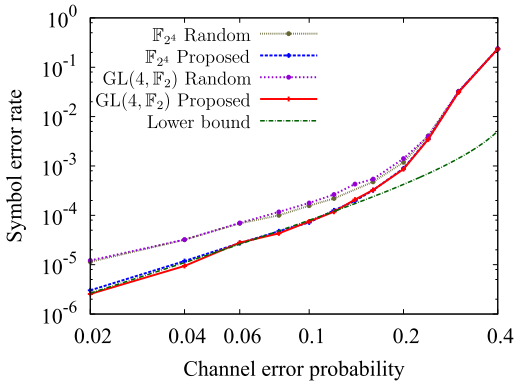

Fig. 3 The symbol error rates for the expurgated ensembles ELDPC$(315, \mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}}), x, x^2, 1, 8, \mathcal{H})$ transmitted through the 2^4-SC for $m_3 = 1$, $m_4 = 4$, $\mathcal{H} = \emptyset$ ($\mathbb{F}_{2^4}$ Random), for $m_3 = 1$, $m_4 = 4$, $\mathcal{H} = \mathcal{H}^*_{1,4}$ ($\mathbb{F}_{2^4}$ Proposed), for $m_3 = 4$, $m_4 = 1$, $\mathcal{H} = \emptyset$ ($\mathrm{GL}(4, \mathbb{F}_2)$ Random) and for $m_3 = 4$, $m_4 = 1$, $\mathcal{H} = \mathcal{H}^*_{4,1}$ ($\mathrm{GL}(4, \mathbb{F}_2)$ Proposed). The lower bound is given by Eq. (4).

5. Conclusion

In this paper, we derived the condition for successful decoding for zigzag cycle codes through the q-MS channels. We proved the relation between a set of class representatives and the order of general linear group. Moreover, we proposed a method to lower the error floors for non-binary LDPC codes. This analysis shows that the constructed non-binary LDPC codes defined over general linear group exhibits have the same decoding performance in the error floors as those defined over finite field. The non-binary LDPC codes defined over general linear group have more choices of the labels on the edges which satisfy the condition for the optimization.

As a future work, we will lower the decoding error rates in the waterfall for the non-binary LDPC codes.

Acknowledgment

The authors are so grateful to anonymous reviewers for their valuable comments. This work was supported by Grant-in-Aid for JSPS Fellows. The work of K. Kasai was supported by the grant from the Storage Research Consortium.

References

[1] R.G. Gallager, Low Density Parity Check Codes, in Research Monograph series, MIT Press, Cambridge, 1963.
[2] T. Richardson, M.A. Shokrollahi, and R. Urbanke, "Design of capacity-approaching irregular low-density parity-check codes," IEEE Trans. Inf. Theory, vol.47, no.2, pp.619–637, Feb. 2001.
[3] 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.
[4] W. Chen, C. Poulliat, D. Declercq, L. Conde-Canencia, A. Al-Ghouwayel, and E. Boutillon, "Non-binary LDPC codes defined over the general linear group: Finite length design and practical implementation issues," Proc. IEEE 69th Vehicular Technology Conference, pp.1–5, April 2009.
[5] X.Y. Hu, E. Eleftheriou, and D. Arnold, "Regular and irregular progressive edge-growth tanner graphs," IEEE Trans. Inf. Theory, vol.51, no.1, pp.386–398, Jan. 2005.
[6] T. Nozaki, K. Kasai, and K. Sakaniwa, "Analysis of error floors of non-binary LDPC codes over MBIOS channel," IEICE Trans. Fundamentals, vol.94-A, no.11, pp.2144–2152, Nov. 2011.
[7] E. Hof, I. Sason, and S. Shamai, "Performance bounds for non-binary linear block codes over memoryless symmetric channels," IEEE Trans. Inf. Theory, vol.55, no.3, pp.977–996, March 2009.
[8] F.J. MacWilliams and N.J.A. Sloane, The Theory of Error-Correcting Codes, Elsevier, Amsterdam, 1977.
[9] T.J. Richardson, "Error floors of LDPC codes," Proc. 41st Annual

Allerton Conf. on Commun., Control and Computing, pp.1426–1435, Oct. 2003.
[10] W. Mayeda, Graph Theory, Wiley-Interscience, 1972.
[11] G. Li, I. Fair, and W. Krzymien, "Density evolution for nonbinary LDPC codes under Gaussian approximation," IEEE Trans. Inf. Theory, vol.55, no.3, pp.997–1015, March 2009.
[12] T. Richardson and R. Urbanke, Modern Coding Theory, Cambridge University Press, March 2008.
[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] R. Lidl and H. Niederreiter, Introduction to finite fields and their applications, Cambridge University Press, New York, NY, USA, 1986.
[15] M. Darafsheh, "Order of elements in the groups related to the general linear group," Finite Fields and Their Applications, vol.11, no.4, pp.738–747, 2005.

Appendix A: Proof of Lemma 1

proof: Fix a Tanner graph $\mathtt{G}$ of a LDPC code over $\mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}})$. We will compare the decoding process when the all-zero codeword and a codeword $\boldsymbol{x} \neq \boldsymbol{0}$ are transmitted. We assume that the noise realizations are the same in both all-zero codeword and a codeword $\boldsymbol{x}$ case. To simplify the notation, we denote $\underline{\gamma}_i := (\gamma_j)_{j\in[m_1(i-1)+1,m_1 i]}$ and $\underline{x}_{v,i} := (x_{v,j})_{j\in[m_1(i-1)+1,m_1 i]}$ for $i \in [1, m_2]$ and $v \in [1, N]$. From the channel symmetry for the q-MS channel, the same noise realizations are for $i \in [1, m_2]$ and $v \in [1, N]$

$$p(y_{v,i} \mid 0) = p(z_{v,i} \mid 0),$$
$$p(y_{v,i} \mid \underline{x}_{v,i}) = p(\mathcal{T}(z_{v,i}, \underline{x}_{v,i}) \mid \underline{x}_{v,i}).$$

Let $C_v, \Phi_{c,v}^{(\ell)}, \Psi_{v,c}^{(\ell)}, D_v^{(\ell)}$ be the messages in the BP decoder for the all-zero codeword and $\dot{C}_v, \dot{\Phi}_{c,v}^{(\ell)}, \dot{\Psi}_{v,c}^{(\ell)}, \dot{D}_v^{(\ell)}$ be the messages in the BP decoder for the codeword $\boldsymbol{x}$.

(1) Initial message

For the codeword $\boldsymbol{x}$, the initial message under BP decoding is $\dot{C}_v(\gamma) = \prod_{i=1}^{m_2} p\big(\mathcal{T}(z_{v,i}, \underline{x}_{v,i}) \mid \underline{\gamma}_i\big)$, for $v \in [1, N]$ and $\gamma \in \mathbb{F}_{2^{m_4}}^{m_3}$. Hence, we get for $\gamma \in \mathbb{F}_{2^{m_4}}^{m_3}$,

$$\begin{aligned} C_v(\gamma) &= \prod_{i=1}^{m_2} p\big(z_{v,i} \mid \underline{\gamma}_i\big) = \prod_{i=1}^{m_2} p\big(\mathcal{T}(z_{v,i}, \underline{x}_{v,i}) \mid \underline{\gamma}_i + \underline{x}_{v,i}\big) \\ &= \dot{C}_v(\gamma + x_v). \end{aligned} \tag{A·1}$$

(2) Iteration

We derive the following equations by mathematical induction for all $\gamma \in \mathbb{F}_{2^{m_4}}^{m_3}$, $v \in [1, N]$, $c \in \mathcal{N}_{\mathtt{v}}(c)$ and $\ell \in \{0, 1, \dots\}$:

$$\Psi_{v,c}^{(\ell)}(\gamma) = \dot{\Psi}_{v,c}^{(\ell)}(\gamma + x_v), \tag{A·2}$$
$$\check{\Psi}_{v,c}^{(\ell)}(\gamma) = \dot{\check{\Psi}}_{v,c}^{(\ell)}(\gamma + h_{c,v} x_v), \tag{A·3}$$
$$\check{\Phi}_{c,v}^{(\ell)}(\gamma) = \dot{\check{\Phi}}_{c,v}^{(\ell)}(\gamma + h_{c,v} x_v), \tag{A·4}$$
$$\Phi_{c,v}^{(\ell)}(\gamma) = \dot{\Phi}_{c,v}^{(\ell)}(\gamma + x_v). \tag{A·5}$$

First, we consider the basis of the mathematical induction. In the variable node calculation, the messages are

$$\Psi_{v,c}^{(0)}(\gamma) = C_v(\gamma), \qquad \dot{\Psi}_{v,c}^{(0)}(\gamma) = \dot{C}_v(\gamma), \tag{A·6}$$

for $\gamma \in \mathbb{F}_{2^{m_4}}^{m_3}$, $v \in [1, N]$ and $c \in \mathcal{N}_{\mathtt{v}}(v)$. From Eqs. (A·1) and (A·6), we get the basis of Eq. (A·2) for all $\gamma \in \mathbb{F}_{2^{m_4}}^{m_3}$, $v \in [1, N]$, $c \in \mathcal{N}_{\mathtt{c}}(c)$ and $\ell = 0$. The messages $\check{\Psi}$ and $\dot{\check{\Psi}}$ are given as $\check{\Psi}_{v,c}^{(0)}(\gamma) = \Psi_{v,c}^{(0)}(h_{c,v}^{-1}\gamma)$ and $\dot{\check{\Psi}}_{v,c}^{(0)}(\gamma) = \dot{\Psi}_{v,c}^{(0)}(h_{c,v}^{-1}\gamma)$, respectively, for $\gamma \in \mathbb{F}_{2^{m_4}}^{m_3}$, $v \in [1, N]$ and $c \in \mathcal{N}_{\mathtt{v}}(v)$. Hence, we have

$$\begin{aligned} \check{\Psi}_{v,c}^{(0)}(\gamma) &= \Psi_{v,c}^{(0)}(h_{c,v}^{-1}\gamma) \\ &= \dot{\Psi}_{v,c}^{(0)}(h_{c,v}^{-1}\gamma + x_v) = \dot{\check{\Psi}}_{v,c}^{(0)}(\gamma + h_{c,v} x_v). \end{aligned} \tag{A·7}$$

This leads the basis of Eq. (A·3). Denote $\Gamma_{c,v} = \{(\gamma_{v'})_{v'\in\mathcal{N}_{\mathtt{c}}(c)\setminus\{v\}} \mid \gamma = \sum_{v'\in\mathcal{N}_{\mathtt{c}}(c)\setminus\{v\}} \gamma_{v'}\}$. The message $\dot{\check{\Phi}}_{c,v}^{(1)}$ is given as

$$\dot{\check{\Phi}}_{c,v}^{(1)}(\gamma) = \sum_{\boldsymbol{\gamma}\in\Gamma_{c,v}} \prod_{v'\in\mathcal{N}_{\mathtt{c}}(c)\setminus\{v\}} \dot{\check{\Psi}}_{v',c}^{(0)}(\gamma_{v'}). \tag{A·8}$$

The message $\check{\Phi}_{c,v}^{(1)}$ is transformed as follows:

$$\begin{aligned} \check{\Phi}_{c,v}^{(1)}(\gamma) &= \sum_{\boldsymbol{\gamma}\in\Gamma_{c,v}} \prod_{v'\in\mathcal{N}_{\mathtt{c}}(c)\setminus\{v\}} \check{\Psi}_{v',c}^{(0)}(\gamma_{v'}) \\ &= \sum_{\boldsymbol{\gamma}\in\Gamma_{c,v}} \prod_{v'\in\mathcal{N}_{\mathtt{c}}(c)\setminus\{v\}} \dot{\check{\Psi}}_{v',c}^{(0)}(\gamma_{v'} + h_{c,v'} x_{v'}) \\ &= \dot{\check{\Phi}}_{c,v}^{(1)}(\gamma + \sum_{v'\in\mathcal{N}_{\mathtt{c}}(c)\setminus\{v\}} h_{c,v'} x_{v'}) \\ &= \dot{\check{\Phi}}_{c,v}^{(1)}(\gamma + h_{c,v} x_v), \end{aligned}$$

where in the second equality we use Eq. (A·7), in the third equality we use Eq. (A·8) and in the fourth equality we use the parity check constraint $h_{c,v} x_v = \sum_{v'\in\mathcal{N}_{\mathtt{c}}(c)\setminus\{v\}} h_{c,v'} x_{v'}$. Hence, we get the basis of Eq. (A·4). The message $\dot{\Phi}_{c,v}^{(1)}$ is written as $\dot{\Phi}_{c,v}^{(1)}(\gamma) = \dot{\check{\Phi}}_{c,v}^{(1)}(h_{c,v}\gamma)$. Hence, the message $\Phi_{c,v}^{(1)}$ is represented as

$$\Phi_{c,v}^{(1)}(\gamma) = \check{\Phi}_{c,v}^{(1)}(h_{c,v}\gamma) = \dot{\check{\Phi}}_{c,v}^{(1)}(h_{c,v}\gamma + h_{c,v} x_v) = \dot{\Phi}_{c,v}^{(1)}(\gamma + x_v).$$

This derives the basis of Eq. (A·5).

Next, we consider the induction step of the mathematical induction. By using induction hypothesis Eq. (A·5) for $\ell = \ell'$, the message $\Phi_{c,v}^{(\ell)}$ is represented as

$$\begin{aligned} \Psi_{v,c}^{(\ell')}(\gamma) &= \frac{\prod_{c'\in\mathcal{N}_{\mathtt{c}}(c)\setminus\{c\}} \Phi_{c',v}^{(\ell')}(\gamma)}{\sum_{\gamma\in\mathbb{F}_{2^{m_4}}^{m_3}} \prod_{c'\in\mathcal{N}_{\mathtt{c}}(c)\setminus\{c\}} \Phi_{c',v}^{(\ell')}(\gamma)} \\ &= \frac{\prod_{c'\in\mathcal{N}_{\mathtt{c}}(c)\setminus\{c\}} \dot{\Phi}_{c',v}^{(\ell')}(\gamma + x_v)}{\sum_{\gamma\in\mathbb{F}_{2^{m_4}}^{m_3}} \prod_{c'\in\mathcal{N}_{\mathtt{c}}(c)\setminus\{c\}} \dot{\Phi}_{c',v}^{(\ell')}(\gamma + x_v)} \\ &= \dot{\Psi}_{v,c}^{(\ell')}(\gamma + x_v). \end{aligned}$$

Hence, we get Eq. (A·2) for $\ell = \ell'$. The following three statements are derived from a way similar to the basis steps:

1. If Eq. (A·2) holds for $\ell = \ell'$, Eq. (A·3) holds for $\ell = \ell'$.
2. If Eq. (A·3) holds for $\ell = \ell'$, Eq. (A·4) holds for $\ell = \ell' + 1$.
3. If Eq. (A·4) holds for $\ell = \ell' + 1$, Eq. (A·5) holds for $\ell = \ell' + 1$.

(3) Decision

For $\gamma \in \mathbb{F}_{2^{m_4}}^{m_3}$ and $v \in [1, N]$, we have

$$\begin{aligned} D_v^{(\ell)}(\gamma) &= \frac{C_v(\gamma)\prod_{c\in\mathcal{N}_v(v)}\Phi_{c,v}^{(\ell)}(\gamma)}{\sum_{\gamma\in\mathbb{F}_{2^{m_4}}^{m_3}} C_v(\gamma)\prod_{c\in\mathcal{N}_v(v)}\Phi_{c,v}^{(\ell)}(\gamma)} \\ &= \frac{\dot{C}_v(\gamma+x_v)\prod_{c\in\mathcal{N}_v(v)}\dot{\Phi}_{c,v}^{(\ell)}(\gamma+x_v)}{\sum_{\gamma\in\mathbb{F}_{2^{m_4}}^{m_3}} \dot{C}_v(\gamma+x_v)\prod_{c\in\mathcal{N}_v(v)}\dot{\Phi}_{c,v}^{(\ell)}(\gamma+x_v)} \\ &= \dot{D}_v^{(\ell)}(\gamma+x_v). \end{aligned}$$

Hence, there is a bijection from the message $D_v^{(\ell)}(\gamma)$ to the message $\dot{D}_v^{(\ell)}(\gamma)$. Thus, both decoding have the same number of symbol errors. Therefore, the symbol error probability is independent of the transmitted codeword. □

Appendix B: Proof of Lemma 2

proof: First, we write the messages $D_v^{(\ell)}$ by the initial messages C_v for the zigzag cycle code of symbol code length w with the matrix χ. Let $\tilde{\Psi}_{v,c}^{(\ell)}$ be the *unnormalized* message from the v-th variable node to the c-th check node at the ℓ-th iteration. For all $x \in \mathbb{F}_{2^{m_4}}^{m_3}$ and $i \in [1, w]$, the unnormalized messages for the zigzag cycle code of symbol code length w are written as follows:

$$\tilde{\Psi}_{i,i-1}^{(0)}(x) := C_i(x), \qquad \tilde{\Psi}_{i,i}^{(0)}(x) := C_i(x), \tag{A·9}$$

$$\tilde{\Psi}_{i,i-1}^{(\ell+1)}(x) := C_i(x)\tilde{\Psi}_{i+1,i}^{(\ell)}(\iota_i^{-1}x), \tag{A·10}$$

$$\tilde{\Psi}_{i,i}^{(\ell+1)}(x) := C_i(x)\tilde{\Psi}_{i-1,i-1}^{(\ell)}(\iota_{i-1}x), \tag{A·11}$$

$$\tilde{D}_i^{(\ell+1)}(x) := C_i(x)\tilde{\Psi}_{i-1,i-1}^{(\ell)}(\iota_{i-1}x)\tilde{\Psi}_{i+1,i}^{(\ell)}(\iota_i^{-1}x), \tag{A·12}$$

where $\tilde{\Psi}_{0,0}^{(\ell)} = \tilde{\Psi}_{w,w}^{(\ell)}$, $\tilde{\Psi}_{1,0}^{(\ell)} = \tilde{\Psi}_{w+1,w}^{(\ell)} = \tilde{\Psi}_{1,w}^{(\ell)}$, $\tilde{\Psi}_{w+1,w+1}^{(\ell)} = \tilde{\Psi}_{1,1}^{(\ell)}$ and $\iota_0 = \iota_w$. Then, for the zigzag cycle code, the message $D_i^{(\ell)}$ is written as follows:

$$D_i^{(\ell)}(x) = \tilde{D}_i^{(\ell)}(x) \Big/ \sum_{x'\in\mathbb{F}_{2^{m_4}}^{m_3}} \tilde{D}_i^{(\ell)}(x'). \tag{A·13}$$

From Eqs. (A·9), (A·10), (A·11) and (A·12), we have

$$\begin{aligned} \tilde{D}_i^{(\ell)}(x) = C_i(x)\prod_{k=1}^{\ell}\Big\{ & C_{i-k}\left(\left(\prod_{j=1}^{k}\iota_{i+j-k-1}\right)x\right) \\ & C_{i+k}\left(\left(\prod_{j=1}^{k}\iota_{i-j+k}^{-1}\right)x\right)\Big\}, \end{aligned} \tag{A·14}$$

where $C_{i+nw}(x) = C_i(x)$ and $\iota_{i+nw} = \iota_i$ for $n \in \mathbb{Z}$. For $x \in \mathbb{F}_{2^{m_4}}^{m_3}$, Eq. (A·14) gives the following equation

$$\begin{aligned} \tilde{D}_i^{(\ell+\sigma_\chi w)}(x) = \tilde{D}_i^{(\ell)}(x)\prod_{k=1}^{\sigma_\chi w}\Big\{ & C_{i-k}\left(\left(\prod_{j=1}^{k}\iota_{i+j-k-1}\right)x\right) \\ & C_{i+k}\left(\left(\prod_{j=1}^{k}\iota_{i-j+k}^{-1}\right)x\right)\Big\}. \end{aligned} \tag{A·15}$$

where σ_χ is the order of the matrix χ, i.e., σ_χ is the smallest positive integer satisfying that χ^{σ_χ} is $m_3 \times m_3$ identity matrix. The production of Eq. (A·15) are transformed as follows:

$$\begin{aligned} &\prod_{k=1}^{\sigma_\chi w} C_{i-k}\left(\left(\prod_{j=1}^{k}\iota_{i+j-k-1}\right)x\right) C_{i+k}\left(\left(\prod_{j=1}^{k}\iota_{i-j+k}^{-1}\right)x\right) \\ &= \prod_{t=0}^{\sigma_\chi-1}\prod_{s=1}^{w} C_s\left(\left(\prod_{j=s}^{w}\iota_j\right)\chi^t\left(\prod_{j=[1,i-1]}\iota_j\right)x\right)^2. \end{aligned}$$

Notice that $\prod_{j\in\emptyset}\iota_j$ is equal to $m_3 \times m_3$ identity matrix. Define $\kappa_i := \prod_{j\in[1,i-1]}\iota_j$ and for $x \in S_\chi$

$$B(x) := \prod_{t=0}^{|\langle\chi\rangle x|-1}\prod_{s=1}^{w} C_s\left(\left(\prod_{j=s}^{w}\iota_j\right)\chi^t x\right).$$

Then, Eq. (A·14) are rewritten as for $x \in S_\chi$ and $i \in [1, w]$

$$\tilde{D}_i^{(\ell+\sigma_\chi w)}(x) = B(\kappa_i x)^{2\sigma_\chi/|\langle\chi\rangle x|}\tilde{D}_i^{(\ell)}(x).$$

For all $x \in S_\chi$, $x' \in \langle\chi\rangle x$, $B(\kappa_i x) = B(\kappa_i x')$ holds. By combining this equation and Eq. (A·13), we have

$$\begin{aligned} &D_i^{(\sigma_\chi\ell_1 w+\ell_2)}(0) \\ &= \frac{\tilde{D}_i^{(\ell_2)}(0)}{\tilde{D}_i^{(\ell_2)}(0) + \sum_{x\in S_\chi}\left\{\frac{B(\kappa_i x)}{B(0)}\right\}^{2\sigma_\chi\ell_1/|\langle\chi\rangle x|}\sum_{x'\in\langle\chi\rangle x}\tilde{D}_i^{(\ell_2)}(x')}. \end{aligned}$$

Hence, we have $\lim_{\ell\to\infty} D_i^{(\ell)}(0) = 1$ for all $i \in [1, w]$, i.e., the decoding is successful, if $B(0) > B(x)$ for all $x \in S_\chi$. Similarly, we have $\lim_{\ell\to\infty} D_i^{(\ell)}(0) = 0$ for all $i \in [1, w]$, i.e., no symbols are eventually correct, if there exists $x \in S_\chi$ such that $B(0) < B(x)$. Finally, we claim that no symbols are eventually correct, if there exists $x \in S_\chi$ such that $B(0) = B(x)$. Note that for all $\ell_1 \geq 1$, $x \in S_\chi$ and $i \in [1, w]$,

$$\begin{aligned} \tilde{D}_i^{(\sigma_\chi\ell_1 w)}\left(\kappa_i^{-1}x\right) &= B(x)^{2\sigma_\chi\ell_1/|\langle\chi\rangle x|}C_i\left(\kappa_i^{-1}x\right), \\ \tilde{D}_i^{(\sigma_\chi\ell_1 w-1)}\left(\kappa_i^{-1}x\right) &= B(x)^{2\sigma_\chi\ell_1/|\langle\chi\rangle x|}C_i\left(\kappa_i^{-1}x\right)^{-1}. \end{aligned}$$

Hence for $\ell_1 \geq 1$ and $i \in [1, w]$,

$$\begin{aligned} &\tilde{D}_i^{(\sigma_\chi\ell_1 w)}\left(\kappa_i^{-1}x\right)\tilde{D}_i^{(\sigma_\chi\ell_1 w-1)}\left(\kappa_i^{-1}x\right) \\ &\quad = B(x)^{4\sigma_\chi\ell_1/|\langle\chi\rangle x|} \\ &\quad = B(0)^{4\sigma_\chi\ell_1/|\langle\chi\rangle x|} = \tilde{D}_i^{(\sigma_\chi\ell_1 w)}(0)\tilde{D}_i^{(\sigma_\chi\ell_1 w-1)}(0). \end{aligned} \tag{A·16}$$

Recall that the i-th symbol is eventually correct if there exists L such that $\tilde{D}_i^{(\ell)}(0) > \tilde{D}_i^{(\ell)}(x)$ for $\ell > L$ and $x \in \mathbb{F}_{2_4^m}^{m_3} \setminus \{0\}$. However, from Eq. (A·16), for all $i \in [1, w]$, if $\tilde{D}_i^{(\sigma_\chi\ell_1 w-1)}(0) > \tilde{D}_i^{(\sigma_\chi\ell_1 w-1)}(\kappa_i^{-1}x)$, then $\tilde{D}_i^{(\sigma_\chi\ell_1 w)}(0) < \tilde{D}_i^{(\sigma_\chi\ell_1 w)}(\kappa_i^{-1}x)$. Thus, no symbols are eventually correct. □

Appendix C: Proof of Lemma 3

To prove Lemma 3, we recall the order of polynomial [14, Definition 3.2].

Definition 4: For polynomials $f(x)$ over $\mathbb{F}_{2^{m_4}}$ such that $f(0) \neq 0$, the least positive integer e for which $f(x)$ divides $x^e - 1$ is called the *order* of polynomial $f(x)$ and is denoted by $\mathrm{ord}(f)$.

We use the following lemma to prove Lemma 3.

Lemma 4: The *characteristic polynomial* $f_\chi(x)$ of the matrix $\chi \in \mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}})$ is defined by $\det(xI - \chi)$ with I being $m_3 \times m_3$ identity matrix over $\mathbb{F}_{2^{m_4}}$. If the order σ_χ of the matrix χ is $2^{m_3m_4-1}$, then the order $\mathrm{ord}(f_\chi)$ of the characteristic polynomial $f_\chi(x)$ is also $2^{m_3m_4-1}$.

proof: Since χ is an $m_3 \times m_3$ nonsingular matrix, $f_\chi(0) \neq 0$. By the Cayley-Hamilton theorem, $f_\chi(\chi) = 0$. From Definition 4, we have $f_\chi(x) \mid x^{\mathrm{ord}(f_\chi)} - 1$. Since $f_\chi(\chi) \mid \chi^{\mathrm{ord}(f_\chi)} - 1$ and $f_\chi(\chi) = 0$, we have $\chi^{\mathrm{ord}(f_\chi)} - 1 = 0$. Hence, we get $\sigma_\chi \mid \mathrm{ord}(f_\chi)$. Since $\mathrm{ord}(f_\chi) \leq 2^{m_3 m_4} - 1$ from [14, Corollary 3.4], $\mathrm{ord}(f_\chi) = 2^{m_3 m_4} - 1$ if $\sigma_\chi = 2^{m_3 m_4} - 1$. □

Lemma 3 is derived from this lemma as follows.

proof of Lemma 3: Firstly, we assume $|S_\chi| = 1$. We denote the first column of χ^j, by χ_1^j. Since $|S_\chi| = 1$,

$$\begin{aligned}\mathbb{F}_{2^{m_4}}^{m_3} \setminus \{0\} &= \{\chi^j(1, 0, 0, \ldots, 0)^T \mid j \in [0, 2^{m_3 m_4} - 2]\} \\ &= \{\chi_1^j \mid j \in [0, 2^{m_3 m_4} - 2]\}.\end{aligned}$$

This equation asserts that $\chi_1^i \neq \chi_1^j$ for $i, j \in [0, 2^{m_3 m_4} - 2]$ with $i \neq j$. Hence, $\chi^i \neq \chi^j$ for $i, j \in [0, 2^{m_3 m_4} - 2]$ with $i \neq j$. Thus, the order of χ is equal to or greater than $2^{m_3 m_4} - 1$. For all $\chi \in \mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}})$, the order of χ is equal to or lower than $2^{m_3 m_4} - 1$, i.e., $\sigma_\chi \leq 2^{m_3 m_4} - 1$ [15, Corollary 2]. Therefore, $\sigma_\chi = 2^{m_3 m_4} - 1$ if $|S_\chi| = 1$.

Secondly, we assume $\sigma_\chi = 2^{m_3 m_4 - 1}$. By Lemma 4, the order of the characteristic polynomial $f_\chi(x)$ is $2^{m_3 m_4} - 1$. Since $\mathrm{ord}(f_\chi) = 2^{m_3 m_4} - 1$, $f_\chi(0) \neq 0$ and $f_\chi(x)$ is a *monic polynomial* [14, Definition 1.49], the characteristic polynomial $f_\chi(x)$ is a *primitive polynomial* [14, Theorem 3.16]. Hence, the field $\mathbb{F}_{2^{m_3 m_4}}$ is represented in $\{0\} \cup \{\chi^i \mid i \in [0, 2^{m_3 m_4} - 2]\}$. Thus, for all $i, j \in [0, 2^{m_3 m_4} - 2]$ with $i \neq j$, there exists a $k \in [0, 2^{m_3 m_4} - 2]$ such that $\chi^i + \chi^j = \chi^k$. This implies that $\chi_1^i \neq \chi_1^j$ for all $i, j \in [0, 2^{m_3 m_4} - 2]$ with $i \neq j$. Therefore, $|S_\chi| = 1$ since $\mathbb{F}_{2^{m_4}}^{m_3} \setminus \{0\} = \langle \chi \rangle (1, 0, \ldots, 0)^T$. □

Takayuki Nozaki received B.E. M.E. and D.E. degrees from Tokyo Institute of Technology in 2008, 2010 and 2012, respectively. He has a Research Fellow of the Japan Society for the Promotion of Science since April 2010. His research interests are codes on graph and iterative decoding algorithm. He is a member of IEEE.

Kenta Kasai received B.E., M.E. and Ph.D. degrees from Tokyo Institute of Technology in 2001, 2003 and 2006, respectively. Since April 2012, he has been an associate professor in the Department of Communications and Integrated Systems, Graduate School of Science and Engineering, Tokyo Institute of Technology. His current research interests include codes on graphs and iterative decoding algorithms.

Kohichi Sakaniwa received B.E., M.E., and Ph.D. degrees all in electronic engineering from Tokyo Institute of Technology, Tokyo Japan, in 1972, 1974 and 1977, respectively. He joined Tokyo Institute of Technology in 1977 as a research associate and served as an associate professor from 1983 to 1991. Since 1991 he has been a professor in the Department of Electrical and Electronic Engineering, and since 2000 in the Department of Communication and Integrated Systems, Graduate School of Science and Engineering, both in Tokyo Inst. of Tech. From November 1987 to July 1988, he stayed at the University of Southwestern Louisiana as a Visiting Professor. He received the Excellent Paper Award from the IEICE of Japan in 1982, 1990, 1992 and 1994. His research area includes Communication Theory, Error Correcting Coding, (Adaptive) Digital Signal Processing and so on. Dr. Sakaniwa is a member of IEEE, Information Processing Society of Japan, and Institute of Image Information and Television Engineers of Japan.