論文 / 著書情報
Article / Book Information

題目(和文)	有限長の低密度パリティ検査符号の復号誤り率の解析
Title(English)	Analysis of decoding error probability for finite length LDPC codes
著者(和文)	野崎隆之
Author(English)	Takayuki Nozaki
出典(和文)	学位:博士(工学), 学位授与機関:東京工業大学, 報告番号:甲第8726号, 授与年月日:2012年3月26日, 学位の種別:課程博士, 審査員:坂庭 好一
Citation(English)	Degree:Doctor (Engineering), Conferring organization: Tokyo Institute of Technology, Report number:甲第8726号, Conferred date:2012/3/26, Degree Type:Course doctor, Examiner:
学位種別(和文)	博士論文
Type(English)	Doctoral Thesis

Analysis of Decoding Error Probability for Finite Length LDPC Codes

A Dissertation

Submitted to Department of

Communications And Integrated Systems

Graduate School of Science and Engineering

Tokyo Institute of Technology

In Partial Fulfillment of The Requirements

for The Degree of

Doctor of Engineering

Takayuki Nozaki

March 2012

Abstract

Low-density parity-check (LDPC) codes are linear codes defined by sparse parity check matrices. Due to the sparseness of the parity check matrices, LDPC codes are efficiently decoded by the belief propagation (BP) decoder. It is known that non-binary LDPC codes can outperform binary ones. However, the decoding complexity grows with the size of non-binary alphabets. Hence, there is a trade-off between performance and complexity. In this dissertation, we focus on both binary and non-binary LDPC codes.

We analyze the decoding error probability for *finite length* LDPC codes under BP decoding. The curve of the decoding error probability for finite length LDPC codes, as a function of channel error probability, is divided into two regions called *waterfall region* and *error floor region.* We analyze the decoding error probability in the waterfall region for binary LDPC codes and in the error floor region for non-binary LDPC codes.

The main results of this dissertation are summarized as follows:

- We analyze the decoding erasure probabilities of waterfall regions for binary LDPC codes over binary erasure channels (BECs) without any assumptions by analytically solving the covariance evolution.

- We propose a method to lower the decoding error rates in the error floors of non-binary LDPC codes defined over Galois field and general linear group transmitted over the BEC, the memoryless binary-input output-symmetric (MBIOS) channel and q-ary memoryless symmetric (q-MS) channel. Simulation results show that the decoding error rates of the codes designed by the proposed method outperform those of the codes designed by the conventional method proposed by Poulliat et al.

- We give lower bounds of decoding error rates in the error floor regions for non-binary LDPC codes over the BEC, MBIOS channel and q-MS channel. Simulation results show that those lower bounds are tight. Moreover, we show that the decoding error rates for non-binary LDPC codes defined over general linear group have same decoding performance in the error floor regions with that for non-binary LDPC codes defined over Galois field. Furthermore, we show that this tight lower bound monotonically decreases, as the order of Galois field of non-binary LDPC code increases in the BEC and binary additive white Gaussian noise channel.

- We derive the weight distribution of the decoding error patterns in the BP decoder for non-binary LDPC codes defined over general linear group transmitted over the BEC.

Acknowledgments

I would like to express my deepest gratitude to my adviser, Professor Kohichi Sakaniwa of Tokyo Institute of Technology. He have supervised me for 5 years, from the 4th grade of undergraduate course to the doctoral course. Without his immense help, support, encouragement and guidance, this dissertation would not have been completed.

I would like to thank referees, Professor Yoshinori Sakai of Tokyo Institute of Technology, Professor Hiroshi Suzuki of Tokyo Institute of Technology, Professor Tomohiko Uyematsu of Tokyo Institute of Technology, Professor Isao Yamada of Tokyo Institute of Technology, Professor Tadashi Wadayama of Nagoya Institute of Technology and Associate Professor Tomoharu Shibuya of Sophia University, for there comments and advisement to the dissertation.

I would like to thank Assistant Professor Kenta Kasai of Tokyo Institute of Technology for his unflagging support and interesting discussions about low-density parity-check codes. His comments have improved my presentation and this dissertation so much.

My deep thanks are also addressed to all the members of the Sakaniwa Laboratory, who I met these years, for their friendship. In particular, Ms. Hiroko Ota has taken care of a lot of paperwork. I really appreciate her help.

This work was partially supported by Grant-in-Aid for Japan Society for the Promotion of Science (JSPS) Fellows.

Symbols and Abbreviations

$\mathbb{R}$	the set of real number
$\mathbb{N}$	the set of natural number including 0 (non-negative integer)
$\mathbb{F}$	field
$\mathbb{F}_{2^m}$	the finite field of order 2^m
$\mathrm{GL}(m, \mathbb{F})$	general linear group of degree m over $\mathbb{F}$
$\mathbb{F}^{M \times N}$	the set of $M \times N$ matrices over $\mathbb{F}$
$\#A$	the number of elements in (cardinality of) the set A
$\|A\|$	the number of elements in (cardinality of) the set A
$\mathbb{E}[X]$	mean (expected value) of random variable X
$\mathrm{Cov}[X, Y]$	covariance of X and Y

LDPC	low-density parity-check (code)
BP	belief propagation
PA	peeling algorithm
CE	covariance evolution
BEC	binary erasure channel
BSC	binary symmetric channel
BAWGN	binary additive white Gaussian noise (channel)
MBIOS	memoryless binary-input output-symmetric (channel)
q-SC	q-ary symmetric channel
q-MS	q-ary memoryless symmetric (channel)

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Background

Reliable communications can be possible by *channel codes* or *error correcting codes.* In channel coding, an appropriate amount of redundancy is added to the information bits to protect them against the errors or the erasures in the channel. Then, the receiver decodes the received bits to determine the information bits. Shannon's channel coding theorem [1] asserts the existence of a maximum rate, called the *channel capacity* or simply *capacity*, at which information can be transmitted with vanishing error probability over a given channel.

A *Linear code* is an error correcting code such that any linear combination of codewords is a codeword of the code. Each linear code is defined by *Tanner graphs* or a *parity check matrix.* More precisely, a Tanner graph represents a parity check matrix and a parity check matrix defines a linear code. For a given N and M, a linear code over a finite field $\mathbb{F}_q$ is defined by an $M \times N$ matrix $H = (h_{i,j})$, called parity check matrix, as follows:

$$\left\{ \boldsymbol{x} \in \mathbb{F}_q^N \mid H\boldsymbol{x}^{\mathrm{T}} = \mathbf{0}^{\mathrm{T}} \in \mathbb{F}_q^M \right\},$$

where $\boldsymbol{x}^{\mathrm{T}}$ represents the transpose of row vector $\boldsymbol{x} = (x_1, x_2, \dots, x_N)$. A Tanner graph for a *binary* linear code, i.e., a linear code over $\mathbb{F}_2$, is represented by a bipartite graph with variable nodes and check nodes. If the v-th variable node and the c-ch check node are connected, then $h_{c,v} = 1$, otherwise $h_{c,v} = 0$. For a non-binary linear code, i.e., a linear code over $\mathbb{F}_q$ where $q > 2$, the Tanner graph is represented by a bipartite graph with variable nodes, check nodes and labeled edges. If the v-th variable node and the c-ch check node are connected with an edge labeled $h_{c,v} \in \mathbb{F}_q \setminus \{0\}$, then $h_{c,v} \neq 0$.

Low-density parity-check (LDPC) codes, invented by Gallager [2], are linear codes defined by *sparse* parity check matrices. 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 [3]. Davey and MacKay [4] found that non-binary LDPC codes can outperform binary ones. However, it is known that the decoding complexity grows with the non-binary alphabet size [5]. Hence, there is a trade-off between performance

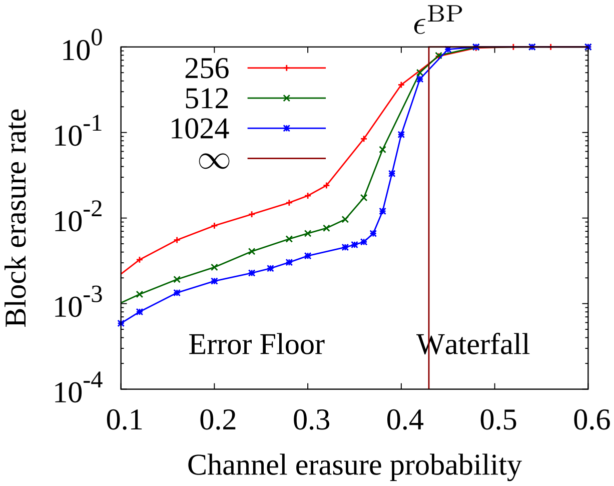

Figure 1.1: Block erasure rates for the (3,6)-regular binary LDPC code ensembles of code length $256, 512, 1024, \infty$.

and complexity. In this dissertation, we focus on both binary and non-binary LDPC codes.

To construct codes which have good decoding performances, it is important to analyze the decoding error rates of LDPC codes. It is known that the decoding error probability of the individual elements of an ensemble close to *ensemble average* with high probability [6]. More precisely, all except an exponentially small fraction of codes behave within an arbitrarily small value from the ensemble average. Hence, in this dissertation, we analyze the ensemble average of decoding error probability.

The LDPC codes defined by Tanner graphs with the variable nodes of degree d_{v} and the check nodes of degree d_{c} are called $(d_{\mathrm{v}}, d_{\mathrm{c}})$-regular LDPC codes. Figure 1.1 shows that the decoding erasure rates[1] for (3,6)-regular binary LDPC code ensembles over the binary erasure channel (BEC) under BP decoding.

The BP *threshold* is denoted by ϵ^{BP} in Figure 1.1. For the BEC, the BP threshold is defined by the supremum of the channel erasure probability such that the decoding error probability is equal to 0. For the LDPC codes of infinite code length, the decoding erasure probabilities are determined by the BP threshold. The BP threshold is analyzed by the *density evolution* [3].

On the other hand, there is room for further research for the LDPC codes of finite code length, or simply *finite length* LDPC codes. Hence, we analyze the decoding error probability for finite length LDPC codes. The curve of the decoding error probability for finite length LDPC codes is divided into two regions which called *waterfall region* and *error floor region*. In the waterfall region, the decoding error probability drops off steeply as the function of channel error probability as in Figure 1.1. The waterfall region is mainly caused by the decoding errors of large weights. In the error floor region, the decoding error probability has a gentle slope as in Figure 1.1. The error floor region is mainly caused by the decoding errors of small weights. In the analysis of decoding error rate for finite length LDPC codes, we analyze both the waterfall

[1] For the BEC, the error rate in the decoding is called *decoding erasure rate*.

Table 1.1: Dissertation contribution.

	Waterfall region		Error floor region	
	Finite-length scaling	Rigorous derivation of scaling parameter	Error floor analysis	Stopping constellation (set) distribution
Binary LDPC code ensemble	Amraoui et al. [7]	Chapter 3	Di et al. [8]	Orlitsky et al. [9]
Non-binary LDPC code ensemble	Kasai et al. [10]		Chapter 4,5	Chapter 6

region and the error floor region.

1.2 Objectives of Dissertation

Table 1.1 shows that the works about analysis of decoding error probability for finite-length LDPC code ensembles. The first and second columns represent the analysis of the waterfall regions. *Finite-length scaling* is a method to analyze the waterfall regions. By the finite-length scaling, the decoding erasure probabilities in the waterfall regions for binary and non-binary LDPC code ensembles were analyzed by Amraoui et al. [7] and Kasai et al. [10], respectively. However, those analyze use unproved assumptions. Hence, we should analyze the waterfall regions without assumptions. The third and fourth columns represent the analysis of the error floor regions. For the binary case, decoding error probability of error floors and weight distribution of decoding error patterns (stopping set distributions) are derived by Di et al. [8] and Orlitsky et al. [9]. However, the error floors for non-binary LDPC codes has not been done so far.

Thus, we should solve the following problems to analyze the decoding error probabilities.

1. Rigorous derivation of scaling parameter for binary LDPC code ensembles

2. Rigorous derivation of scaling parameter for non-binary LDPC code ensembles

3. Analysis of decoding error probability in the error floors for non-binary LDPC code ensembles

4. Analysis of weight distribution of decoding error patterns (stopping constellation distributions)

The dissertation solves the problems 1, 3 and 4 in Chapter 3, Chapter 4,5 and Chapter 6, respectively. The Dissertation does not deal the problem 2. This problem will be solved in future works.

1.3 Main Results and Organization of Dissertation

The main contributions of this dissertation are analysis of decoding error rate for finite-length LDPC code ensembles. The contributions and Organization of the dissertation are the following:

Preliminaries

Chapter 2 We introduce several definitions and basic facts on finite length LDPC codes.

Rigorous derivation of scaling parameter for binary LDPC code ensemble

Chapter 3 We derive the scaling parameter rigorously for the binary irregular LDPC code ensembles.

Error floor analysis for non-binary LDPC code ensemble

Chapter 4 We give lower bounds of bit and symbol error rates in the error floor regions for the non-binary regular and irregular LDPC code ensembles over the BEC. Furthermore, we propose a design method to lower the error floors for the non-binary irregular LDPC code ensembles over the BEC.

Chapter 5 We extends the results in Chapter 4 to the generalized non-binary LDPC codes over the q-ary memoryless symmetric (q-MS) channels. We give lower bounds of symbol error rates in the error floor regions for the non-binary regular and irregular LDPC code ensembles over the q-MS channel. Next, we propose a design method to lower the error floors for the non-binary LDPC codes over the q-MS channel. Moreover, we compare the decoding error rates in the error floors for non-binary LDPC codes over the general linear group with those for non-binary LDPC codes over finite field transmitted over the q-MS channel under BP decoding.

Stopping constellation distribution for the non-binary LDPC code ensembles

Chapter 6 We derive the stopping constellation distributions for the non-binary regular and irregular LDPC code ensembles.

Conclusion

Chapter 7 We conclude the dissertation.

Chapter 2

Preliminaries

In this chapter, we review LDPC codes and basic facts related to this dissertation. We also introduce some notations used throughout this dissertation.

2.1 Mathematical Preliminaries

2.1.1 Finite Field of Order 2^m

A *finite field* or *Galois field* is a field that contains a finite number of elements. The number of elements in a finite field is called its *order*. Denote a finite field of order 2^m, by $\mathbb{F}_{2^m}$.

Let α be a primitive element of $\mathbb{F}_{2^m}$. Once a primitive element α of $\mathbb{F}_{2^m}$ is fixed, each symbol is given by an m-bit (vector) representation [11, p. 110]. We denote the m-bit representation of $\gamma \in \mathbb{F}_{2^m}$, by $b(\gamma)$. We denote the i-th bit of $b(\gamma)$, by $b_i(\gamma)$.

Example 1 With a primitive element $\alpha \in \mathbb{F}_{2^3}$ such that $\alpha^3 + \alpha + 1 = 0$, each symbol is represented as $b(0) = (0,0,0)$, $b(1) = (1,0,0)$, $b(\alpha) = (0,1,0)$, $b(\alpha^2) = (0,0,1)$, $b(\alpha^3) = (1,1,0)$, $b(\alpha^4) = (0,1,1)$, $b(\alpha^5) = (1,1,1)$ and $b(\alpha^6) = (1,0,1)$.

2.1.2 General Linear Group

For an non-negative integer m and a field $\mathbb{F}$, the set of $m \times m$ invertible matrices over $\mathbb{F}$, i.e., $\mathbb{F}^{m\times m}$, is called the *general linear group* over $\mathbb{F}$ and is denoted by $\mathrm{GL}(m, \mathbb{F})$. In this dissertation, we consider $\mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}})$. The number of elements in $\mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}})$ is given by

$$[m_3]_{2^{m_4}} := \begin{cases} 1 & m_3 = 0, \\ \prod_{i=1}^{m_3}(2^{im_4} - 1) & m_3 \geq 1. \end{cases}$$

In particular, the number of elements in $\mathrm{GL}(m, \mathbb{F}_2)$ is

$$[m]_2 := \begin{cases} 1 & m = 0, \\ \prod_{i=1}^{m}(2^{i} - 1) & m \geq 1. \end{cases}$$

To simplify the notation, we denote the number of elements in $\mathrm{GL}(m, \mathbb{F}_2)$, by $[m]$.

2.2 LDPC Codes

Gallager invented LDPC codes [2]. Binary and non-binary LDPC codes are defined by $M \times N$ sparse parity check matrices. For the binary LDPC codes, each entry of parity check matrices is an element in $\mathbb{F}_2$. For the non-binary LDPC codes over group (or field) G, each entry of parity check matrices is an element in G.

The *Tanner graph* for a binary LDPC code is represented by a bipartite graph with variable nodes, check nodes and edges. For the non-binary LDPC codes over group (or field) G, the Tanner graphs are represented by bipartite graphs with variable nodes, check nodes and edges *labeled* by non-zero elements in G.

The details are in the following sections.

2.2.1 Binary LDPC Code

A binary LDPC code is defined by the null space of an $M \times N$ sparse parity check matrix $H = (h_{i,j}) \in \mathbb{F}_2^{M \times N}$ as follows:

$$\left\{ \boldsymbol{x} \in \mathbb{F}_2^N \mid H\boldsymbol{x}^{\mathrm{T}} = \mathbf{0}^{\mathrm{T}} \in \mathbb{F}_2^M \right\}.$$

Note that N is called *bit code length* or simply code length. The parity check matrices are represented by Tanner graphs as the following: If the v-th variable node and the c-th check node are connected with an edge, $h_{c,v} = 1$, otherwise $h_{c,v} = 0$.

Example 2 Figure 2.1 shows an example of Tanner graph. The circles and squares in the Tanner graph represent variable nodes and check nodes, respectively. Tanner graph in Fig. 2.1 represents the following matrix:

$$H = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}.$$

2.2.2 Non-Binary LDPC Code over Galois Field

A non-binary LDPC code defined over Galois field $\mathbb{F}_{2^m}$ is defined by the null space of an $M \times N$ sparse parity check matrix $H = (h_{i,j}) \in \mathbb{F}_{2^m}^{M \times N}$ as follows:

$$\left\{ \boldsymbol{x} \in \mathbb{F}_{2^m}^N \mid H\boldsymbol{x}^{\mathrm{T}} = \mathbf{0}^{\mathrm{T}} \in \mathbb{F}_{2^m}^M \right\}.$$

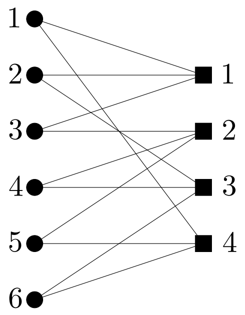

Figure 2.1: An example of Tanner graph. The circles and squares represent variable nodes and check nodes, respectively.

Note that N is called *symbol code length.* The bit code length n is given by mN. The parity check matrices for non-binary LDPC codes are also represented by Tanner graphs as the following: If the v-th variable node and the c-th check node are connected with an edge labeled $h_{c,v} \in \mathbb{F}_{2^m} \setminus \{0\}$, $h_{c,v} \neq 0$ $h_{c,v} = 1$, otherwise $h_{c,v} = 0$.

2.2.3 Non-Binary LDPC Code over General Linear Group

A non-binary LDPC code defined over general linear group $\mathrm{GL}(m, \mathbb{F}_2)$ is defined by the null space of an $M \times N$ sparse parity check matrix $H = (h_{i,j}) \in \mathrm{GL}(m, \mathbb{F}_2)^{M \times N}$ as follows:

$$\left\{ (\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_N) \in (\mathbb{F}_2^m)^N \mid \sum_{j=1}^{N} h_{i,j} \boldsymbol{x}_j^{\mathrm{T}} = \mathbf{0}^{\mathrm{T}} \in \mathbb{F}_2^m \quad \forall i \in [1, M] \right\},$$

where we denote $[k_1, k_2] := \{k \in \mathbb{N} \mid k_1 \leq k \leq k_2\}$ for $k_1 \leq k_2$. The bit code length n is given by mN. The parity check matrices for non-binary LDPC codes are also represented by Tanner graphs as the following: If the v-th variable node and the c-th check node are connected with an edge labeled $h_{c,v} \in \mathrm{GL}(m, \mathbb{F}_2) \setminus \{\mathbf{0}\}$, $h_{c,v} \neq \mathbf{0}$, otherwise $h_{c,v} = \mathbf{0}$.

2.2.4 Generalized Non-Binary LDPC Code

In the similar way, we define the non-binary LDPC codes over general linear group $\mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}})$. Non-binary LDPC codes over general linear group $\mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}})$ are defined by the null space of $M \times N$ sparse parity check matrix $H = (h_{i,j}) \in \mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}})^{M \times N}$ as follows:

$$\left\{ (\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_N) \in (\mathbb{F}_{2^{m_4}}^{m_3})^N \mid \sum_{j=1}^{N} h_{i,j} \boldsymbol{x}_j^{\mathrm{T}} = \mathbf{0}^{\mathrm{T}} \in \mathbb{F}_{2^{m_4}}^{m_3} \quad \forall i \in [1, M] \right\}.$$

We refer the number of variable node N, as symbol code length of non-binary LDPC code over $\mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}})$. The bit code length is $m_3 m_4 N$. The parity check matrices for non-binary LDPC codes are also represented by Tanner graphs as the following: If the v-th variable node and the c-th check node are connected with an edge labeled $h_{c,v} \in \mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}}) \setminus \{\mathbf{0}\}$, $h_{c,v} \neq \mathbf{0}$, otherwise $h_{c,v} = \mathbf{0}$.

Since 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 cases for the non-binary LDPC codes over $\mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}})$, we refer the non-binary LDPC codes over $\mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}})$ as *generalized* non-binary LDPC codes.

2.3 LDPC Code Ensembles

It is known that the decoding error probability of the individual elements of an ensemble close to *ensemble average* with high probability [6]. More precisely, all except an exponentially small fraction of codes behave within an arbitrarily small value from the ensemble average. Hence, in this dissertation, we analyze the ensemble average of decoding error probability.

2.3.1 Binary Irregular LDPC Code Ensemble

Let λ_i and ρ_i be the fractions of the edges connected to variable nodes and check nodes of degree i, respectively. Let $\mathcal{L}$ and $\mathcal{R}$ be the sets of degrees of variable nodes and check nodes, i.e. $\mathcal{L} := \{i \mid \lambda_i \neq 0\}$ and $\mathcal{R} := \{i \mid \rho_i \neq 0\}$, respectively. Each irregular LDPC code ensemble [12] is characterized with the number of variable nodes N and a pair of *degree distribution*, $\lambda(x) = \sum_{i \in \mathcal{L}} \lambda_i x^{i-1}$ and $\rho(x) = \sum_{i \in \mathcal{R}} \rho_i x^{i-1}$.

The total number of edges in the Tanner graph is

$$\xi := \frac{N}{\int_0^1 \lambda(x)dx}.$$

Let L_i and R_j be the fraction of the variable nodes of degree i and the check nodes of degree j, respectively, i.e.,

$$L_i := \frac{\lambda_i}{i \int_0^1 \lambda(x)dx}, \qquad R_j := \frac{\rho_j}{j \int_0^1 \rho(x)dx}.$$

Define the *design rate* r as follows:

$$r := 1 - \frac{\int_0^1 \rho(x)dx}{\int_0^1 \lambda(x)dx}.$$

The number of check node M is $M = (1-r)N$. The average variable node degree is expressed as

$$\Lambda_{\mathrm{ave}} := \frac{1}{\int_0^1 \lambda(x)dx}.$$

Assume that the number of variable nodes N and the degree distribution pair $\lambda(x), \rho(x)$ are given. A binary irregular LDPC code ensemble $\mathrm{E}(N, \lambda, \rho)$ is defined in the following way. There exist $L_i N$ variable nodes of degree i and $R_j N(1-r)$ check nodes of degree j. A node of degree i has i sockets for its connected edges. Consider a permutation π on the number of edges ξ.

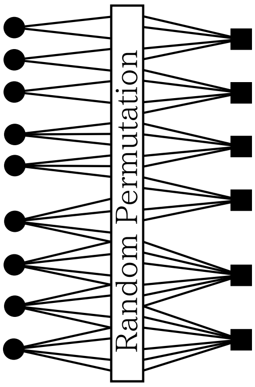

Figure 2.2: The irregular binary LDPC code ensemble $\mathrm{E}(9, \lambda, \rho)$, where $\lambda(x) = \frac{3}{14}x + \frac{3}{14}x^2 + \frac{4}{7}x^3$ and $\rho(x) = \frac{4}{7}x^3 + \frac{3}{7}x^5$.

Join the i-th socket on the variable node side to the $\pi(i)$-th socket on the check node side. The bipartite graphs are chosen with equal probability from all the permutations on the number of edges.

Example 3 Figure 2.2 shows the irregular LDPC codes ensemble $\mathrm{E}(9, \lambda, \rho)$, where

$$\lambda(x) = \frac{3}{14}x + \frac{3}{14}x^2 + \frac{4}{7}x^3, \qquad \rho(x) = \frac{4}{7}x^3 + \frac{3}{7}x^5.$$

The number of variable nodes is $N = 6$. The sets of degrees of variable nodes and check nodes are $\mathcal{L} = \{2, 3, 4\}$ and $\mathcal{R} = \{4, 6\}$. The total number of edges is $\xi = 28$. The fraction of the variable nodes and check nodes are

$$L_2 = \frac{1}{3}, \quad L_3 = \frac{2}{9}, \quad L_4 = \frac{4}{9}, \qquad\qquad R_4 = \frac{2}{3}, \quad R_6 = \frac{1}{3}.$$

The design rate is $r = \frac{1}{3}$. The number of check nodes is given by $M = 4$.

Discussion 1 A $(d_\mathrm{v}, d_\mathrm{c})$-*regular* LDPC code is a binary LDPC code such that every variable node has degree d_v and every check node has degree d_c. Figure 2.1 shows a (2,3)-regular LDPC code. The $(d_\mathrm{v}, d_\mathrm{c})$-regular LDPC code ensemble is denoted by $\mathrm{E}(N, x^{d_\mathrm{v}-1}, x^{d_\mathrm{c}-1})$.

2.3.2 Non-Binary Irregular LDPC Code Ensemble

The non-binary LDPC code ensembles are defined in an analogous way as in the binary case. Firstly, we define the non-binary irregular LDPC code ensemble defined over $\mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}})$. For a given number of variable nodes N, Galois field $\mathbb{F}_{2^m}$ and degree distribution pair $\lambda(x), \rho(x)$, a non-binary irregular LDPC code ensemble $\mathrm{LDPC}(N, \mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}}), \lambda, \rho)$ is defined in the following way. There exist $L_i N$ variable nodes of degree i and $R_j N(1-r)$ check nodes of degree j. A node of degree i has i sockets for its connected edges. Consider a permutation π on the number of edges. Join the i-th socket on the variable node side to the $\pi(i)$-th socket on the check node side. The bipartite graphs are chosen with equal probability from all the permutations on the number of edges. Each label in an edge is chosen as an element from $\mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}}) \setminus \{\mathbf{0}\}$ with equal probability.

To simplify the notation, we denote the non-binary LDPC code ensemble over $\mathrm{GL}(m, \mathbb{F}_2)$ and over $\mathbb{F}_{2^m}$, by $\mathrm{EGL}(N, m, \lambda, \rho)$ and $\mathrm{EGF}(N, \mathbb{F}_{2^m}, \lambda, \rho)$, respectively.

Discussion 2 The regular non-binary LDPC code ensemble is defined in a way similar to the binary case. The $(d_{\mathrm{v}}, d_{\mathrm{c}})$-regular non-binary LDPC code ensemble is denoted by $\mathrm{LDPC}(N, \mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}}), x^{d_{\mathrm{v}-1}}, x^{d_{\mathrm{c}-1}}, \rho)$.

For the non-binary defined over Galois field case, it is empirically known that $(2, d_{\mathrm{c}})$-regular non-binary LDPC codes exhibit good decoding performance among other LDPC codes for $m \geq 6$ [13]. However, this is not the case for $m < 6$. In this dissertation, we consider the irregular non-binary LDPC codes which contain variable nodes of degree two for the generality of code ensemble.

2.4 Channel Models

In this section, we introduce channel models used in this dissertation.

To simplify the notation, the input alphabet is $\{+1, -1\}$ indeed of $\{0, 1\}$. The mapping is the following:

$$\begin{aligned} 0 &\longleftrightarrow +1, \\ 1 &\longleftrightarrow -1. \end{aligned}$$

With some abuse of notation, we make no distinction between $\{+1, -1\}$ and $\{0, 1\}$.

We regard the codewords in the non-binary LDPC codes as binary codewords $(x_1, x_2, \ldots, x_N)$, i.e., the codewords $\boldsymbol{x}$ are represented by $(x_{1,1}, x_{1,2}, \ldots, x_{N,m})$, where $x_{i,j} = b_j(x_i)$ for $i \in [1, N], j \in [1, m]$. Hence, the codewords in the non-binary LDPC codes can be transmitted by *binary* channels. We denote the received word as $(y_{1,1}, y_{1,2}, \ldots, y_{N,m})$.

2.4.1 Binary Erasure Channel (BEC)

Let X and Y be the channel input and the channel output, respectively. For the BEC, the channel input and channel output take value in the alphabet $X \in \{+1, -1\}$ and $Y \in \{+1, -1, ?\}$, respectively, where ? indicates an erasure. Each channel input is either erased with probability ϵ or received correctly with probability $1 - \epsilon$, where ϵ is referred to as *channel erasure probability.* Figure 2.3 depicts the BEC with channel erasure probability ϵ.

2.4.2 Binary Symmetric Channel (BSC)

For the BSC, the channel input and channel output take value in the alphabet $\{+1, -1\}$. Each channel input is either error with probability ϵ or received correctly with probability $1 - \epsilon$, where ϵ is referred to as *crossover probability.* Figure 2.4 depicts the BSC with crossover probability ϵ.

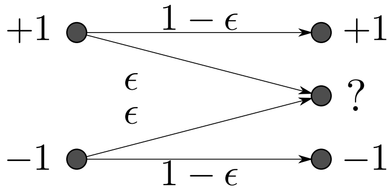

Figure 2.3: The BEC with channel erasure probability ϵ.

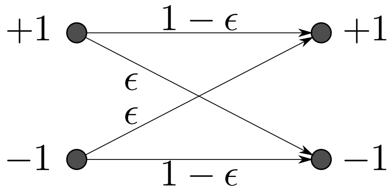

Figure 2.4: The BSC with crossover probability ϵ.

2.4.3 Binary Additive White Gaussian Noise (BAWGN) Channel

Each channel inputs and channel outputs of the BAWGN channel are $X \in \{+1, -1\}$ and $Y \in \mathbb{R}$, respectively, where $\mathbb{R}$ is the set of real number. More precisely, $Y = X + Z$, where Z is a Gaussian random variable with zero mean and variance σ^2. In other words, the transition probability density function for the BAWGN channel with noise variance σ^2 is written as

$$p_{Y|X}(y \mid x) = \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left[-\frac{(y-x)^2}{2\sigma^2}\right],$$

where $\exp[x]$ is the exponential function. The signal to noise ratio (SNR) of the BAWGN channel with noise variance σ^2 is σ^{-2}.

2.4.4 Memoryless Binary-Input Output-Symmetric (MBIOS) Channel

For the binary channel, we denote the channel input $\boldsymbol{x} := (x_{1,1}, x_{1,2}, \ldots, x_{N,m-1}, x_{N,m})$ and the channel output $\boldsymbol{y} = (y_{1,1}, y_{1,2}, \ldots, y_{N,m-1}, y_{N,m})$. A channel is called *memoryless* binary-input channel if

$$p(\boldsymbol{y} \mid \boldsymbol{x}) = \prod_{i=1}^{N} \prod_{j=1}^{m} p(y_{i,j} \mid x_{i,j}).$$

A memoryless binary-input channel is called *output-symmetric* if

$$p(y \mid x) = p(-y \mid -x).$$

The MBIOS channels are characterized by its L-density a [5]. Examples of the MBIOS channels include the BEC, the BSC and the BAWGN channel.

2.4.5 q-ary Memoryless Symmetric (q-MS) Channel

The cardinality of an input alphabet $\mathcal{X}$ of a q-ary channel is q i.e., $|\mathcal{X}| = q$. For the q-ary channel, we denote the channel input $\boldsymbol{x} := (x_{1,1}, x_{1,2}, \ldots, x_{N,m_2-1}, x_{N,m_2})$ and the channel output $\boldsymbol{y} = (y_{1,1}, y_{1,2}, \ldots, y_{N,m_2-1}, y_{N,m_2})$ for a fixed positive integer m_2. A q-ary channel is called *memoryless* if

$$p(\boldsymbol{y} \mid \boldsymbol{x}) = \prod_{i=1}^{N} \prod_{j=1}^{m_2} p(y_{i,j} \mid x_{i,j}).$$

The channel symmetry for a q-ary memoryless channel is given in the following definition.

Definition 1 [14, Definition 1] A q-ary memoryless channel which is characterized by a transition probability $p(\cdot \mid \cdot)$, an input alphabet $\mathcal{X}$, and an output alphabet $\mathcal{Y}$ is *symmetric* if there exists a function $\mathcal{T} : \mathcal{Y} \times \mathcal{X} \to \mathcal{Y}$ which satisfies 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 $y \in \mathcal{Y}$, the following equality holds:

$$p(y \mid x_1) = p(\mathcal{T}(y, x_2 - x_1) \mid x_2)$$

3. For channels whose output alphabet $\mathcal{Y}$ is continuous, the mapping $\mathcal{T}$ is that its Jacobian is equal to 1.

Example 4 The q-ary symmetric channel (q-SC) is an example of the q-MS channel. We consider 2^m-SC in this dissertation. The input alphabet is $\mathcal{X} = \mathbb{F}_{2^m}$ and the output alphabet is $\mathcal{Y} = \mathbb{F}_{2^m}$ for the 2^m-SC. The transition probability function is

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

If we set $\mathcal{X} = \mathbb{F}_{2^m}$, $\mathcal{Y} = \mathbb{F}_{2^m}$ and

$$\mathcal{T}(y, x) = y + x,$$

then Definition 1 holds the 2^m-SC.

Example 5 The MBIOS channel is also an example of the q-MS channel. If we set the input alphabet $\mathcal{X} = \mathbb{F}_2$, the output alphabet is $\mathcal{Y}$ and

$$\mathcal{T}(y, x) = \begin{cases} y & x = 0, \\ -y & x = 1, \end{cases}$$

then Definition 1 holds the MBIOS channel.

2.5 Decoding Algorithms

In this section, we review decoding algorithms and several properties about decoding algorithms.

2.5.1 Belief Propagation Decoder for Binary LDPC Codes

BP decoding proceeds by sending messages along the edges in the Tanner graph. The messages arising in the BP decoder for binary LDPC codes are vectors of length 2. Let $\Psi_{v,c}^{(\ell)}$ be the message from the v-th variable node to the c-th check node at the ℓ-th iteration. Let $\Phi_{c,v}^{(\ell)}$ be the message from the c-th check node to the v-th variable node at the ℓ-th iteration.

Initialization

Set $\ell = 0$. Recall that N and M are the number of variable nodes and check nodes in a Tanner graph, respectively. For $v \in [1, N]$, let $C_v = (C_v(0), C_v(1))$ denote the initial message of the v-th variable node. The initial message C_v is given from the channel outputs as follows:

$$\begin{aligned}C_v(0) =&\Pr\bigl(Y_v = y_v \mid X_v = 0\bigr),\\ C_v(1) =&\Pr\bigl(Y_v = y_v \mid X_v = 1\bigr).\end{aligned}$$

Let $\mathcal{N}_{\mathsf{c}}(c)$ be the set of the indices of the variable nodes connecting to the c-th check node. Set for all $c = [1, M]$ and $v \in \mathcal{N}_{\mathsf{c}}(c)$,

$$\Phi_{c,v}^{(0)} = \left(\frac{1}{2}, \frac{1}{2}\right).$$

Iteration

Iteratively perform the following actions for $\ell = 1, 2, \ldots$.

Variable node action Let $\mathcal{N}_{\mathsf{v}}(v)$ be the set of the indices of the check nodes connected to the v-th variable node. The message $\Psi_{v,c}^{(\ell)}$ is given by the component-wise multiplication of the initial message C_v and the incoming messages $\Phi_{c',v}^{(\ell)}$ from check nodes whose indices c' are in $\mathcal{N}_{\mathsf{v}}(v) \setminus \{c\}$, i.e., for $x \in \mathbb{F}_2$

$$\Psi_{v,c}^{(\ell)}(x) = \frac{1}{\zeta} C_v(x) \prod_{c' \in \mathcal{N}_{\mathsf{v}}(v) \setminus \{c\}} \Phi_{c',v}^{(\ell)}(x),$$

where ζ is the normalization factor such that $1 = \Psi_{v,c}^{(\ell)}(0) + \Psi_{v,c}^{(\ell)}(1)$.

Check node action The convolution of two vectors Ψ_1 and Ψ_2 is given by

$$[\Psi_1 \oplus \Psi_2](x) = \sum_{y,z \in \mathbb{F}_2 : x = y + z} \Psi_1(y)\Psi_2(z),$$

where $\sum_{y,z\in\mathbb{F}_2:x=y+z}\Psi_1(y)\Psi_2(z)$ is the sum of $\Psi_1(y)\Psi_2(z)$ over all $y,z\in\mathbb{F}_2$ such that $x=y+z$. To simplify the notation, we define

$$\bigoplus_{i\in\{1,2,\dots,k\}}\Psi_i := \Psi_1\oplus\Psi_2\oplus\cdots\oplus\Psi_k.$$

The message $\Phi_{c,v}^{(\ell+1)}$ is given as, for $x\in\mathbb{F}_2$

$$\Phi_{c,v}^{(\ell+1)} = \bigoplus_{v'\in\mathcal{N}_\mathrm{c}(c)\setminus\{v\}}\Psi_{v',c}^{(\ell)}.$$

Decision

For $x\in\mathbb{F}_2$

$$D_v^{(\ell)}(x) := \frac{1}{\zeta}C_v(x)\prod_{c\in\mathcal{N}_\mathrm{v}(v)}\Phi_{c,v}^{(\ell)}(x),$$

where ζ is the normalization factor such that $1=D_v^{(\ell)}(0)+D_v^{(\ell)}(1)$. The decoding output $\hat{x}_v^{(\ell)}$ given as the following:

$$\hat{x}_v^{(\ell)} = \begin{cases} 0 & D_v^{(\ell)}(0) > D_v^{(\ell)}(1),\\ 1 & D_v^{(\ell)}(0) < D_v^{(\ell)}(1),\\ ? & D_v^{(\ell)}(0) = D_v^{(\ell)}(1),\end{cases}$$

where ? represents that the v-th symbol is not recovered.

2.5.2 Peeling Decoder for Binary LDPC Codes

The peeling algorithm [15] is a sequential iterative decoding algorithm for the BEC. As the PA proceeds, edges and nodes are progressively removed from the original Tanner graph and the so-called *residual graph* is left at each iteration. The residual graph at each iteration consists of the variable nodes that are still unknown and the check nodes and the edges connecting to those variable nodes. The decoding process successfully stops if and only if the residual graph vanishes.

Peeling decoding proceeds as follows.

Initialization Variable nodes receive the channel outputs. The variable nodes receiving the known values send their values to the check nodes connected to them. Then the variable nodes sending their values and edges connecting to those variable nodes are removed from the graph.

Iteration The decoder uniformly chooses a check node of degree one in the residual graph. The chosen check node sends the value computed from the received values to the adjacent variable node. The variable node propagates this value to all adjacent check nodes. The variable node is removed together with its edges.

Decision If the decoder does not find any check nodes of degree one in the residual graph, then the decoding process stops. If the residual graph is empty, then the decoding process succeeds, otherwise it fails.

Discussion 3 For the BEC and sufficiently large number of iterations, the BP decoder stops in a fixed point of decoding. It is known that the BP decoder and the peeling decoder stop in the same decoding results [15]. Hence, we are able to analyze the decoding performance under BP decoding by analyzing peeling decoder.

2.5.3 BP Decoder for Non-Binary LDPC Codes

The BP decoder for the non-binary LDPC codes is an extension of the BP decoder for binary LDPC codes. 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 $m = m_3 m_4$. Recall $\Psi_{v,c}^{(\ell)}$ is the message from the v-th variable node to the c-th check node at the ℓ-th iteration and $\Phi_{c,v}^{(\ell)}$ is the message from the c-th check node to the v-th variable node at the ℓ-th iteration.

Once a primitive element of $\mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}})$ is fixed, each symbol in $\mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}})$ is represented as the m-bits. We assume that the codewords are transmitted over the 2^{m_1}-MS channels such that $m_1 \mid m$. Then, each symbol $\boldsymbol{x}_i$ of the codeword $(\boldsymbol{x}_1, \boldsymbol{x}_2, \dots, \boldsymbol{x}_N)$ is represented as m_2 channel inputs to the 2^{m_1}-SC channel, where $m_2 = m/m_1$. We denote the channel outputs by $(y_{1,1}, y_{1,2}, \dots, y_{N,m_2}) \in \mathcal{Y}^{Nm_2}$.

In the case for $m_1 = 1$, the 2^{m_1}-MS channels represent the MBIOS channels.

Initialization

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

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

Set for all $c \in [1, M]$ and $v \in \mathcal{N}_{\mathsf{c}}(c)$,

$$\Phi_{c,v}^{(0)} = \left(\frac{1}{2^m}, \frac{1}{2^m}, \dots, \frac{1}{2^m}\right).$$

Iteration

Iteratively perform the following actions for $\ell = 1, 2, \dots$.

Variable node action The message $\Psi_{v,c}^{(\ell)}$ is given by the component-wise multiplication of the initial message C_v and the incoming messages $\Phi_{c',v}^{(\ell)}$ from check nodes whose positions c' are in $\mathcal{N}_{\mathsf{v}}(v)$, i.e., for $x \in \mathbb{F}_{2^{m_4}}^{m_3}$

$$\Psi_{v,c}^{(\ell)}(x) = \zeta^{-1} C_v(x) \prod_{c' \in \mathcal{N}_{\mathsf{v}}(v) \setminus \{c\}} \Phi_{c',v}^{(\ell)}(x),$$

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

Check node action 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 $\bigoplus_{i \in \{1,2,\dots,k\}} \Psi_i := \Psi_1 \oplus \Psi_2 \oplus \cdots \oplus \Psi_k$. The message $\Phi_{c,v}^{(\ell+1)}$ is given as, for $x \in \mathbb{F}_{2^{m_4}}^{m_3}$

$$\begin{aligned}
\check{\Psi}_{v,c}^{(\ell)}(x) &= \Psi_{v,c}^{(\ell)}\left(h_{c,v}^{-1} x\right), \\
\check{\Phi}_{c,v}^{(\ell+1)} &= \bigoplus_{v' \in \mathcal{N}_{\mathsf{c}}(c) \setminus \{v\}} \check{\Psi}_{v',c}^{(\ell)}, \\
\Phi_{c,v}^{(\ell+1)}(x) &= \check{\Phi}_{c,v}^{(\ell+1)}(h_{c,v} x).
\end{aligned}$$

Decision

Define

$$\operatorname*{arg\,max}_{x \in \mathbb{F}_{2^{m_4}}^{m_3}} \Psi := \left\{ x \mid \forall y \in \mathbb{F}_{2^{m_4}}^{m_3}, \Psi(x) \geq \Psi(y) \right\},$$

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

$$D_v^{(\ell)}(x) := \zeta^{-1} C_v(x) \textstyle\prod_{c \in \mathcal{N}_{\mathsf{v}}(v)} \Phi_{c,v}^{(\ell)}(x),$$

where ζ is the normalization factor such that $1 = \sum_{x \in \mathbb{F}_{2^{m_4}}^{m_3}} D_v^{(\ell)}(x)$. For $v \in [1, N]$, let $\hat{x}_v^{(\ell)}$ be the decoding output of the v-th variable node. Define

$$\mathcal{D}_v^{(\ell)} := \operatorname*{arg\,max}_{x \in \mathbb{F}_{2^{m_4}}^{m_3}} D_v^{(\ell)}(x).$$

If $|\mathcal{D}_v^{(\ell)}| = 1$, the decoding output $\hat{x}_v^{(\ell)}$ is the element of $\mathcal{D}_v^{(\ell)}$. If $|\mathcal{D}_v^{(\ell)}| > 1$, the decoder chooses $\hat{x}_v^{(\ell)} \in \mathcal{D}_v^{(\ell)}$ with probability $1/|\mathcal{D}_v^{(\ell)}|$.

Example 6 In the case for non-binary LDPC code defined over general linear group $\mathrm{GL}(3, \mathbb{F}_2)$, the messages are represented by vectors of length 2^3 as follows:

$$C_v = (C_v(000), C_v(100), C_v(010), C_v(110), C_v(001), C_v(101), C_v(011), C_v(111)).$$

In the case for non-binary LDPC code defined over Galois field $\mathbb{F}_{2^3}$, the messages are represented by vectors of length 2^3 as follows:

$$C_v = \big(C_v(0), C_v(1), C_v(\alpha^1), C_v(\alpha^2), C_v(\alpha^3), C_v(\alpha^4), C_v(\alpha^5), C_v(\alpha^6)\big),$$

where α is a primitive element of $\mathbb{F}_{2^3}$.

2.5.4 Peeling Decoder for Non-Binary LDPC Codes

We assume transmitted over the BEC. The peeling decoder assigns a set of candidate symbols for the decoding result to each variable node. Such a set is referred to as state of the v-th variable node and denoted by E_v, where $E_v \subseteq \mathbb{F}_{2^m}$. Initially, for all $v \in [1, N]$, the peeling decoder assigns the state

$$\begin{aligned} E_v = \{\gamma \in \mathbb{F}_{2^m} \mid b_i(\gamma) = 0 \text{ (for } i \text{ s.t. } y_{v,i} = 0), b_i(\gamma) = 1 \text{ (for } i \text{ s.t. } y_{v,i} = 1), \\ b_j(\gamma) \in \{0, 1\} \text{ (for } j \text{ s.t. } y_{v,j} =?)\} \end{aligned} \tag{2.1}$$

to the v-th variable node. In words, the peeling decoder assigns the states corresponding to the channel outputs to the variable nodes. For any subsets $A_1, A_2, \dots, A_k \subseteq \mathbb{F}_{2^m}$, we denote

$$\sum_{i=1}^{k} A_i := \left\{ \sum_{i=1}^{k} a_i \mid a_j \in A_j \ (j = 1, 2, \dots, k) \right\}.$$

To simplify the notation, for $\gamma \in \mathbb{F}_{2^m}$ and $E \subseteq \mathbb{F}_{2^m}$, we define $\gamma E := \{\gamma e \mid e \in E\}$. If $E_v \cap h_{c,v}^{-1}\big(\sum_{i \in \mathcal{N}_c(c)\setminus\{v\}} h_{c,i} E_i\big)$ is a proper subset of E_v, then (v, c) is said to be an *active pair.* The peeling decoder involves the following 3 steps:

1. Initially the peeling decoder assigns the states corresponding to the channel outputs to the variable nodes.

2. The peeling decoder chooses an active pair (v, c) uniformly at random. The peeling decoder assigns $E_v \leftarrow E_v \cap h_{c,v}^{-1}\big(\sum_{i \in \mathcal{N}_c(c)\setminus\{v\}} h_{c,i} E_i\big)$ to the v-th variable node.

3. If there is no active pair, then the peeling decoder stops. Otherwise repeat step 2.

Note that the cardinality of the states of the variable nodes do not increase as decoding proceeds.

Discussion 4 All the nonzero entries in a message arising in the BP decoder are equal [16, Lemma 2]. For the BEC and sufficiently large number of iterations, the BP decoder stops in a fixed point of decoding. In [17], Rathi et al. proved that the BP decoder and the peeling decoder stop in the same fixed point of decoding. More precisely, $\{\mathcal{D}_v^{(\ell)}\}_{v \in [1,N]}$ for sufficiently large ℓ is equal to $\{E_v\}_{v\in[1,N]}$ in the same channel outputs. Thus, if we analyze the fixed point of peeling decoder, we are able to analyze the condition of successful decoding under BP decoding.

2.6 Analysis of Decoders

2.6.1 All-zero Codeword Assumption

For binary LDPC codes over the MBIOS channel under BP decoding, the bit error probability is independent of the transmitted codeword. Hence we are able to assume that all-zero codewords are sent without loss of generality to analyze the decoding error rate [6] for binary LDPC codes over the MBIOS channel under BP decoding. This assumption is referred to as the *all-zero codeword assumption*. In the case for non-binary LDPC codes over the MBIOS channel under BP decoding, all-zero codeword assumption also holds [16, Lemma 1].

In this section, we prove that all-zero codeword assumption also holds for non-binary LDPC codes defined over $\mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}})$ transmitted over the 2^{m_1}-MS channel under BP decoding.

Lemma 1 For non-binary LDPC codes over $\mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}})$ transmitted over the 2^{m_1}-MS channel under BP decoding, the symbol error probability is independent of the transmitted codeword. In other words, all-zero codeword assumption holds for non-binary LDPC codes defined over $\mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}})$ over the 2^{m_1}-MS channel under BP decoding.

The proof of Lemma 1 is in Appendix 2.A.

2.6.2 Decoding Failure

Firstly, we consider the non-binary case. Recall that we are able to assume that all-zero codewords are sent without loss of generality. The v-th symbol is *eventually correct* [18] if there exists L_v such that for all $\ell > L_v$, $\hat{x}_v^{(\ell)} = 0$. The block is eventually correct if and only if all the symbols are eventually correct. The i-th bit in the v-th symbol is eventually correct if there exists L_v such that for all $\ell > L_v$, $b_i(\gamma) = 0$ for all $\gamma \in \mathcal{D}_v^{(\ell)}$. The block erasure rate, the symbol erasure rate and the bit erasure rate are defined by the fraction of the blocks, the symbols and the bits which are not eventually correct, respectively.

Next, we consider the binary case. The v-th bit is eventually correct if there exists L_v such that for all $\ell > L_v$, $\hat{x}_v^{(\ell)} = 0$. The bit error rate is defined by the fraction of the bits error bits which are not eventually correct.

2.6.3 State of Non-binary Peeling Decoder

Closure under Linear Subspace for State

Recall that we are able to assume that all-zero codewords are sent without loss of generality. The states of peeling decoder for non-binary LDPC codes are represented by linear subspaces [16, Lemma 2], [19, Lemma 2] as follows:

$$\{b(w) \in \mathbb{F}_2^m \mid w \in E_v \subset \mathbb{F}_{2^m}\}$$

In other words, the set of the m-bit representations for the indices corresponding to nonzero entries of a message arising in the BP decoder forms a linear subspace of $\mathbb{F}_2^m$ [16, Lemma 2], [19, Lemma 2].

Closure under Additive of Galois Field for State

The states are the subsets in $\mathbb{F}_{2^m}$ which are closed under the addition in $\mathbb{F}_{2^m}$. From (2.1), initially, the states are subset in $\mathbb{F}_{2^m}$ which is closed under the addition in $\mathbb{F}_{2^m}$. We claim that if the subset $E \subseteq \mathbb{F}_{2^m}$ is closed under the addition, the subset γE is also closed under the addition for $\gamma \in \mathbb{F}_{2^m} \setminus \{0\}$. For all $e_1', e_2' \in \gamma E$, there exist $e_1, e_2 \in E$ such that $e_1' = \gamma e_1$ and $e_2' = \gamma e_2$. For all $e_1', e_2' \in \gamma E$, we see that

$$e_1' + e_2' = \gamma e_1 + \gamma e_2 = \gamma(e_1 + e_2) \in \gamma E.$$

Hence, the subset $\gamma E \subseteq \mathbb{F}_{2^m}$ is closed under the addition if $E \subseteq \mathbb{F}_{2^m}$ is closed under the addition. We claim that the subset $E_1 \cap E_2 \subseteq \mathbb{F}_{2^m}$ is closed under the addition if the subsets $E_1, E_2 \subseteq \mathbb{F}_{2^m}$ are closed under the addition. For all $e_1, e_2 \in E_1 \cap E_2$, we see that $e_1 + e_2 \in E_1$ and $e_1 + e_2 \in E_2$ since $e_1, e_2 \in E_1$ and $e_1, e_2 \in E_2$. Since $e_1 + e_2 \in E_1 \cap E_2$, the subset $E_1 \cap E_2 \subseteq \mathbb{F}_{2^m}$ is closed under the addition if the subsets $E_1, E_2 \subseteq \mathbb{F}_{2^m}$ are closed under the addition. Obviously, if the subsets $E_1, E_2, \dots, E_k \in \mathbb{F}_{2^m}$ are closed under the addition, $\sum_{i=1}^{k} E_1$ is closed under the addition. Hence $E_v \cap h_{c,v}^{-1}\big(\sum_{i \in \mathcal{N}_\mathsf{c}(c) \setminus \{v\}} h_{c,i} E_i\big)$ is closed under the addition, if E_i is closed under the addition for $i \in \mathcal{N}_\mathsf{c}(c) \setminus \{v\}$. Recall that initially the states are subset in $\mathbb{F}_{2^m}$ which is closed under the addition in $\mathbb{F}_{2^m}$. Thus, all the states are closed under the addition in $\mathbb{F}_{2^m}$.

2.7 Tools for Performance Analysis

2.7.1 Threshold and Density Evolution

In this section, we review the BP *threshold* and *density evolution* for the binary LDPC codes. For $a < b$, define $\overline{[a,b]} := \{x \in \mathbb{R} \mid a \le x \le b\}$ and $\overline{(a,b]} := \{x \in \mathbb{R} \mid a < x \le b\}$. Let $P_\mathrm{B}(\epsilon, N)$ be the block erasure probability under BP decoding for channel erasure probability ϵ and the bit code length N. The BP threshold is defined by

$$\epsilon_\mathrm{BP} := \sup_{\epsilon \in \overline{[0,1]}} \left\{ \lim_{N \to \infty} P_\mathrm{B}(\epsilon, N) = 0 \right\},$$

and characterized via density evolution [3] as follows:

$$\epsilon_\mathrm{BP} = \sup_{\epsilon \in \overline{(0,1]}} \{y = 1 - \rho(1 - \epsilon\lambda(y)) \text{ has no solution } y \in (0,1]\}.$$

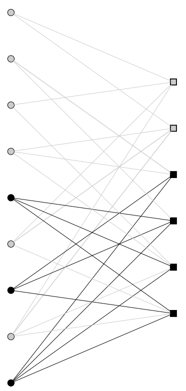

Figure 2.5: An example of stopping set.

2.7.2 Waterfall Region and Error Floor Region

The block error probability is represented by the sum of two contributions, the decoding error of large weight (of order $O(N)$) and the decoding error of small weight (of order $o(N)$). The curve of the block error probability for finite length LDPC codes is divided two regions which called *waterfall region* and *error floor region.* In the waterfall region, the block error probability drops off steeply as the function of channel parameter. The curve of the block error probability in the waterfall region is represented by Q-function, where

$$Q(z) = \frac{1}{\sqrt{2\pi}} \int_{z}^{\infty} \exp\left[-\frac{x^2}{2}\right] dx.$$

The waterfall region is mainly caused by the decoding erasures of large weights (of order $O(N)$). In the error floor region, the block erasure probability has a gentle slope. The curve of the block error probability in the error floor region is represented by a polynomial. The error floor region is mainly caused by the decoding erasures of small weights (of order $o(N)$).

2.7.3 Stopping Set

A *stopping set* $\mathcal{S}$ is a set of variable nodes such that all the neighbors of $\mathcal{S}$ are connected to $\mathcal{S}$ at least twice. With some abuse of notation, we make no distinction between the set of the variable nodes and the set of the position of the variable nodes.

Example 7 Figure 2.5 shows an example of stopping set. The 5th, 7th and 9th variable nodes forms a stopping set since all the neighbors of those variable nodes are connected to those variable nodes at least twice.

For the binary LDPC code over the BEC, the stopping sets are the fixed points of the BP decoder. It is known that BP decoding is failure if a stopping set is included in the set of position $i \in [1, N]$ such that the channel output $y_i =?$. Hence, the stopping sets are important to characterize the decoding erasures.

Since the definition of stopping sets depends only on structure of a Tanner graph, we extend the definition of the stopping set for the non-binary LDPC codes.

2.7.4 Stopping Constellation

Definition 2 [17] A *stopping constellation* $\{E_v\}_{v\in[1,N]}$ is defined as an assignment of the states such that

$$E_v \subseteq h_{c,v}^{-1}\left(\sum_{i\in\mathcal{N}_c(c)\setminus\{v\}} h_{c,i}E_i\right), \tag{2.2}$$

for any $v \in [1, N]$ and all the check nodes connecting to the v-th variable node.

It is known that stopping constellations are fixed points of the peeling decoder and the BP decoder [17]. In this chapter for a given stopping constellation we refer to the number of states whose dimensions are not equal to 0 as the *weight* of the stopping constellation.

2.7.5 Stopping Constellation and Stopping Set

In this section, we show the relationship between the stopping constellation and the stopping set. For a given stopping constellation $\{E_v\}_{v\in[1,N]}$, let $\tilde{\mathcal{S}}$ be the set of variable nodes such that the dimensions of the corresponding states are not 0, i.e.,

$$\tilde{\mathcal{S}} := \{v \in [1, N] \mid E_v \neq \{\mathbf{0}\}\}.$$

Lemma 2 For a fixed $\mathtt{G} \in \mathrm{LDPC}(N, \mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}}), \lambda, \rho)$ and a given stopping constellation, the set of variable nodes $\tilde{\mathcal{S}}$ for the stopping constellation forms a stopping set.

proof: If there exists a check node in c which connects to $\tilde{\mathcal{S}}$ once, then for the variable node in $v \in \tilde{\mathcal{S}}$ such that $E_v \neq \{\mathbf{0}\}$ and $h_{c,v}^{-1}\sum_{i\in\mathcal{N}_c(c)\setminus\{v\}} h_{c,i}E_i = \{\mathbf{0}\}$. Hence, the assignment of the states $\{E_v\}_{v\in[1,N]}$ is not a stopping constellation if there exists a check node which connects to $\tilde{\mathcal{S}}$ once. Thus, all the neighbors of $\tilde{\mathcal{S}}$ are connected to $\tilde{\mathcal{S}}$ at least twice. Therefore, the set of variable nodes $\tilde{\mathcal{S}}$ for the stopping constellation forms a stopping set. (Q.E.D.)

Lemma 3 For a fixed $\mathtt{G} \in \mathrm{LDPC}(N, \mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}}), \lambda, \rho)$ and a given stopping set $\mathcal{S}$, there exist at least one stopping constellation with the set of variable nodes $\tilde{\mathcal{S}}$ such that $\tilde{\mathcal{S}} = \mathcal{S}$.

proof: For a given stopping set $\mathcal{S}$, the assignment of state $\{E_v\}_{v\in[1,N]}$ such that $E_v = \mathbb{F}_2^m$ for all $v \in \mathcal{S}$ and $E_v = \{\mathbf{0}\}$ for all $v \in [1, N] \setminus \mathcal{S}$ is a stopping constellation. (Q.E.D.)

The stopping constellations of small weight degrade the decoding erasure rates of non-binary LDPC codes. From those lemmas, we see that in order to get a code which does not contain the stopping constellation of small weight, we need to eliminate the stopping sets of small weight.

2.8 Summary

In this chapter, we have reviewed LDPC codes and basic facts related to this dissertation. We have also introduced some notations used throughout this dissertation. We have proved the all-zero codeword assumption for non-binary LDPC codes over the q-MS channel under BP decoding. Moreover, we have shown the relationship between the stopping sets and stopping constellations.

Appendix 2.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 $\boldsymbol{x} \neq \mathbf{0}$ are transmitted. We assume that the noise realizations are the same in the both all-zero codeword and a codeword $\boldsymbol{x}$ case. To simplify the notation, we denote $\underline{\gamma}_i := (b_j(\gamma))_{j\in[m_1(i-1)+1,m_1 i]}$ 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 $v \in [1, N]$ and $i \in [1, m_2]$

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

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

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 $\gamma \in \mathbb{F}_{2^{m_4}}^{m_3}$,

$$C_v(\gamma) = \prod_{i=1}^{m_2} p\Big(z_{v,i} \mid \underline{\gamma}_i\Big) = \prod_{i=1}^{m_2} p\Big(\mathcal{T}(z_{v,i}, \underline{x}_{v,i}) \mid \underline{\gamma}_i + \underline{x}_{v,i}\Big) = \dot{C}_v(\gamma + x_v). \tag{2.3}$$

Iteration We derive the following equations by mathematical induction for all ℓ, $\gamma \in \mathbb{F}_{2^{m_4}}^{m_3}$ and $v \in [1, N]$:

$$\begin{aligned} \Psi^{(\ell)}_{v,c}(\gamma) =& \dot{\Psi}^{(\ell)}_{v,c}(\gamma + x_v), & (2.4) \\ \check{\Psi}^{(\ell)}_{v,c}(\gamma) =& \dot{\check{\Psi}}^{(\ell)}_{v,c}(\gamma + h_{c,v}x_v), & (2.5) \\ \check{\Phi}^{(\ell)}_{c,v}(\gamma) =& \dot{\check{\Phi}}^{(\ell)}_{c,v}(\gamma + h_{c,v}x_v), & (2.6) \\ \Phi^{(\ell)}_{c,v}(\gamma) =& \dot{\Phi}^{(\ell)}_{c,v}(\gamma + x_v). & (2.7) \end{aligned}$$

Firstly, we consider the basis of the mathematical induction. In the variable node action, the messages are

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

for $\gamma \in \mathbb{F}_{2^{m_4}}^{m_3}$, $v \in [1,N]$ and $c \in \mathcal{N}_{\mathsf{v}}(v)$. Hence, from (2.3), we get the basis of (2.4) for $\ell = 0$, $\gamma \in \mathbb{F}_{2^{m_4}}^{m_3}$ and $v \in [1,N]$. 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 $c \in \mathcal{N}_{\mathsf{v}}(v)$. Hence, we have

$$\begin{aligned}\check{\Psi}_{v,c}^{(0)}(\gamma) =&\Psi_{v,c}^{(0)}(h_{c,v}^{-1}\gamma)\\ =&\dot{\Psi}_{v,c}^{(0)}(h_{c,v}^{-1}\gamma + x_v) = \dot{\check{\Psi}}_{v,c}^{(0)}(\gamma + h_{c,v}x_v).\end{aligned} \tag{2.8}$$

This leads the basis of (2.5). The message $\dot{\check{\Phi}}_{c,v}^{(1)}$ is given as

$$\dot{\check{\Phi}}_{c,v}^{(1)}(\gamma) = \sum_{\substack{\gamma\in\{(\gamma_{v'})_{v'\in\mathcal{N}_{\mathsf{c}}(c)\setminus\{v\}}\mid\\ \gamma=\sum_{v'\in\mathcal{N}_{\mathsf{c}}(c)\setminus\{v\}}\gamma_{v'}\}}} \prod_{v'\in\mathcal{N}_{\mathsf{c}}(c)\setminus\{v\}} \dot{\check{\Psi}}_{v',c}^{(0)}(\gamma_{v'}) \tag{2.9}$$

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

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

where in the second equality we use (2.8), in the third equality we use (2.9) and in the fourth equality we use the parity check constraint $h_{c,v}x_v = \sum_{v'\in\mathcal{N}_{\mathsf{c}}(c)\setminus\{v\}} h_{c,v'}x_{v'}$. Hence, we get the basis of (2.6). 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 derive the basis of (2.7).

Next, we consider the induction step of the mathematical induction. By using induction hypothesis (2.7) for $\ell = \ell'$, the message $\Phi_{c,v}^{(\ell)}$ is represented as

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

Hence, we get (2.4) for $\ell = \ell'$. The following three statements are derived from a way similar to the basis steps:

1. If (2.4) holds for $\ell = \ell'$, (2.5) holds for $\ell = \ell'$.

2. If (2.5) holds for $\ell = \ell'$, (2.6) holds for $\ell = \ell' + 1$.

3. If (2.6) holds for $\ell = \ell' + 1$, (2.7) holds for $\ell = \ell' + 1$.

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

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

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 errors. Therefore, the symbol error probability is independent of the transmitted codeword. (Q.E.D.)

Chapter 3

Analytical Solution of Covariance Evolution for Irregular Binary LDPC Codes

The scaling law developed by Amraoui et al. is a powerful method to estimate the block erasure probabilities in the waterfall regions of finite-length LDPC codes. Solving a system of differential equations called covariance evolution, one can obtain the scaling parameter. However, the covariance evolution has not been analytically solved. In this chapter, we present the analytical solutions of the covariance evolution for the irregular LDPC code ensembles.

3.1 Introduction

The *scaling law* developed by Amraoui et al. [7] is a powerful method to estimate the block and bit erasure probabilities in the waterfall regions of finite length LDPC codes transmitted over the BEC. Let r_i and l_j be random variables representing the number of edges connecting to the check nodes of degree i and to the variable nodes of degree j, respectively, in the residual graph. Then, the *scaling parameter* is obtained from the mean and the variance of r_1. The means of r_i and l_j are determined from a system of differential equations which was derived and analytically solved by Luby et al. [15]. The covariances of r_i and l_j also satisfy a system of differential equations called *covariance evolution* which was derived by Amraoui et al. [7]. However, the analytical solution of the covariance evolution has not been known. Therefore, one had to resort to numerical computation to solve the covariance evolution.

In [20], Amraoui et al. proposed an alternative way to determine the variance of r_1, though only at the decoding threshold. Thereby they have given the analytic expression for the scaling parameters without using the covariance evolution. They used BP decoding instead of the PA. This method was applied to irregular repeat-accumulate codes [21] and to turbo-like codes [22] and was extended to the binary memoryless symmetric channels [23, 24].

Denote by ξ the total number of edges in the Tanner graph. For $i = 1, 2, \ldots, \xi$, let μ_i

be the random variable which is 1 if the edge i conveys an erasure message from a variable node to a check node, and 0 otherwise, in BP decoding. In [20], Amaroui et al. analyzed the random variable $\sum_{i=1}^{\xi} \mu_i$ in decoding and derived the analytical expression for the variance of this random variable. Finally, they made an unproved assumption that the random variable $r_1 - \mathbb{E}[r_1]$ in the PA is proportional to the random variable $\sum_{i=1}^{\xi} \mu_i - \mathbb{E}[\sum_{i=1}^{\xi} \mu_i]$ in BP decoding and under this assumption they have given the analytical solution for the variance of r_1.

However, no such assumption is needed if the covariance evolution is solved analytically. Moreover, we obtain the variance of r_1 at any channel erasure probability. In this chapter. we present the analytical solution of the covariance evolution for irregular LDPC code ensembles.

This chapter is organized as follows. In Section 3.2, we recall some basic facts on the finite length analysis of LDPC codes under iterative decoding. In Section 3.3, we present the analytical solution of the covariance evolution for the irregular LDPC code ensembles. In Section 3.4, we analytically solve the covariance evolution for the irregular LDPC code ensembles.

3.2 Residual Graph and Finite-Length Scaling

In this section, we recall the analysis of the residual graphs and the finite-length scaling for the irregular LDPC code ensembles. We also introduce some notations used throughout this chapter.

3.2.1 Analysis of Residual Graph

Denote the iteration round of the PA by ℓ. Let $l_{k,\ell}$ and $r_{i,\ell}$ denote random variables representing the number of edges connecting to the variable nodes of degree k and to the check nodes of degree i, respectively, in the residual graph at the iteration round ℓ. Let d_{c} be the maximum degree of check nodes. We define $\bar{\mathcal{R}} := \{1, 2, \dots, d_{\mathrm{c}} - 1\}$. We also define a set of random variables

$$\mathcal{D}_\ell := \{l_{k,\ell} \mid k \in \mathcal{L}\} \cup \{r_{k,\ell} \mid k \in \bar{\mathcal{R}}\}.$$

Since the total number of edges connecting to variable nodes is equal to the total number of edges connecting to check nodes in each residual graph, we have

$$\sum_{i \in \mathcal{L}} l_{i,\ell} = \sum_{j \in \bar{\mathcal{R}} \cup \{d_{\mathrm{c}}\}} r_{j,\ell}.$$

This equation gives

$$r_{d_{\mathrm{c}},\ell} = \sum_{i \in \mathcal{L}} l_{i,\ell} - \sum_{j \in \bar{\mathcal{R}}} r_{j,\ell}.$$

Hence, we see that the random variable $r_{d_{\mathrm{c}},\ell}$ depends on the random variables in $\mathcal{D}_\ell$. Hence, we drop $r_{d_{\mathrm{c}},\ell}$ as in [25]. To simplify the notation, we drop the subscript ℓ.

For $X \in \mathcal{D} \cup \{r_{d_c}\}$, we define the *normalized* expectation of X as

$$\bar{X} := \frac{\mathbb{E}[X]}{\xi}.$$

Let e be the expectation of the fraction of the edges in the residual graph, i.e.,

$$e := \sum_{i \in \mathcal{L}} \bar{l}_i.$$

We define

$$\tau := \frac{\ell}{\xi}. \tag{3.1}$$

Define a parameter y such that $y = 1$ at $\tau = 0$ and

$$\frac{dy}{d\tau} = -\frac{y}{e}.$$

Hence, we see that the iteration round ℓ is parameterized by y.

Let $I_{\{\cdot\}}$ be the indicator function which is 1 if the condition inside the braces is fulfilled and 0 otherwise. Define

$$a := \frac{1}{e} \sum_{i \in \mathcal{L}} i\bar{l}_i.$$

For $i \in \mathcal{L}$ and $j \in \bar{\mathcal{R}} \cup \{d_c\}$ in the limit of large block length, Luby et al. [15] showed that $\bar{X}(y)$ satisfies the following system of differential equations

$$\frac{d\bar{l}_i}{d\tau} = \hat{f}^{(l_i)} = -\frac{i\bar{l}_i}{e}, \qquad \frac{d\bar{r}_j}{d\tau} = \hat{f}^{(r_j)} = j(\bar{r}_{j+1} - \bar{r}_j)\frac{a-1}{e} - I_{\{j=1\}}.$$

We define the binomial coefficient [26] for non-negative integer n, k as

$$\binom{n}{k} := \begin{cases} \frac{n!}{k!(n-k)!} & 0 \le k \le n, \\ 0 & k > n. \end{cases}$$

Recall that the channel erasure probability is ϵ. By using the parameter y, for $i \in \mathcal{L}$ and $j \in \{2, \ldots, d_c\}$, this system of differential equation are solved as:

$$\bar{l}_i(y) = \epsilon\lambda_i y^i, \qquad \bar{r}_j(y) = \sum_{i \in \mathcal{R}} \rho_i \binom{i-1}{j-1} x^j \tilde{x}^{i-j}, \qquad \bar{r}_1(y) = x(y - 1 + \rho(\tilde{x})),$$

where $x := \epsilon\lambda(y)$ and $\tilde{x} := 1 - x$. Define $x' := dx/dy$. From this result, we see that

$$e = xy, \qquad a = \frac{x'y + x}{x}.$$

For $X, Y \in \mathcal{D}$, we define the *normalized* covariance of X and Y by

$$\delta^{(X,Y)} := \frac{\mathrm{Cov}[X,Y]}{\xi}.$$

Unless otherwise specified, we drop y to simplify the notation. In [7,25], Amraoui et al. showed that $\delta^{(X,Y)}$ satisfies the following system of differential equations for the irregular LDPC code ensembles in the limit of large block length:

$$\frac{d\delta^{(X,Y)}}{dy} = -x \sum_{Z\in\mathcal{D}} \left(\frac{\partial \hat{f}^{(X)}}{\partial \bar{Z}} \delta^{(Y,Z)} + \frac{\partial \hat{f}^{(Y)}}{\partial \bar{Z}} \delta^{(X,Z)} \right) - x\hat{f}^{(X,Y)}, \tag{3.2}$$

and this system of the differential equation is referred to as the covariance evolution. Define $x'' := d^2x/dy^2$ and

$$G_j(y) := \begin{cases} j(\bar{r}_{j+1} - \bar{r}_j)/x & j \in \bar{\mathcal{R}}, \\ -d_{\mathrm{c}}\bar{r}_{d_{\mathrm{c}}}/x & j = d_{\mathrm{c}}. \end{cases}$$

The terms in the covariance evolution are given by the following for $k, s \in \mathcal{L}$, $i \in \bar{\mathcal{R}}$ and $j \in \bar{\mathcal{R}} \setminus \{d_{\mathrm{c}} - 1\}$

$$\begin{aligned}
\frac{\partial \hat{f}^{(l_s)}}{\partial \bar{l}_k} &= \frac{s\bar{l}_s}{e^2} - I_{\{k=s\}}\frac{s}{e}, & \frac{\partial \hat{f}^{(l_s)}}{\partial \bar{r}_i} &= 0, \\
\frac{\partial \hat{f}^{(r_j)}}{\partial \bar{l}_k} &= -\frac{2a-k-1}{e}\frac{G_j}{y}, & \frac{\partial \hat{f}^{(r_j)}}{\partial \bar{r}_i} &= j\frac{a-1}{e}\left(I_{\{i=j+1\}} - I_{\{i=j\}}\right), \\
\frac{\partial \hat{f}^{(r_{d_{\mathrm{c}}-1})}}{\partial \bar{l}_k} &= (d_{\mathrm{c}}-1)\frac{a-1}{e} - \frac{2a-k-1}{e}\frac{G_{d_{\mathrm{c}}-1}}{y}, \\
\frac{\partial \hat{f}^{(r_{d_{\mathrm{c}}-1})}}{\partial \bar{r}_i} &= -(d_{\mathrm{c}}-1)\frac{a-1}{e}\left(1 + I_{\{i=d_{\mathrm{c}}-1\}}\right),
\end{aligned}$$

and for $k, s \in \mathcal{L}$ and $i, j \in \bar{\mathcal{R}}$

$$\begin{aligned}
\hat{f}^{(l_k,l_s)} &= ks\frac{\bar{l}_k}{e}\left(I_{\{k=s\}} - \frac{\bar{l}_s}{e}\right), \\
\hat{f}^{(l_k,r_i)} &= (a-k)\frac{k\bar{l}_k}{e}\frac{G_i}{y}, \\
\hat{f}^{(r_i,r_j)} &= \frac{x''x - (x')^2}{x^2}G_iG_j + ij\frac{x'}{x^2}\left\{I_{\{i=j\}}(\bar{r}_{j+1} + \bar{r}_j) - I_{\{i=j+1\}}\bar{r}_i - I_{\{j=i+1\}}\bar{r}_j\right\}.
\end{aligned}$$

Initial conditions of the covariance evolution are also given by Amraoui et al. [7,25]. For $i, j \in \bar{\mathcal{R}}$ and $k, s \in \mathcal{L}$, the initial conditions of the covariance evolution are derived as follows:

$$\begin{aligned}
\delta^{(l_k,l_s)}(1) &= I_{\{k=s\}}\epsilon\tilde{\epsilon}\lambda_k k, \\
\delta^{(l_k,r_i)}(1) &= -\epsilon\tilde{\epsilon}\lambda_k k G_i(1), \\
\delta^{(r_i,r_j)}(1) &= I_{\{i=j\}}i\bar{r}_i(1) - V_{i,j}(1) + \epsilon\tilde{\epsilon}\lambda'(1)G_i(1)G_j(1),
\end{aligned}$$

Table 3.1: Summary of intermediate variables defined in Section 3.2.1.

$x = \epsilon\lambda(y)$
$x' = dx/dy = \epsilon\lambda'(y)$
$x'' = d^2x/dy^2 = \epsilon\sum_{i\in\mathcal{L}}(i-1)(i-2)\lambda_i y^{i-3}$
$\tilde{x} = 1 - x$
$\tilde{\epsilon} = 1 - \epsilon$
$a = e^{-1}\sum_{i\in\mathcal{L}} i\bar{l}_i = (x'y + x)/x$
$G_j(y) = \begin{cases} j(\bar{r}_{j+1} - \bar{r}_j)/x & j \in \bar{\mathcal{R}} \\ -d_{\mathrm{c}}\bar{r}_{d_{\mathrm{c}}}/x & j = d_{\mathrm{c}} \end{cases}$
$V_{i,j}(y) = \sum_{s\in\mathcal{R}} \rho_s s \binom{s-1}{i-1}\binom{s-1}{j-1} x^{i+j}\tilde{x}^{2s-i-j} \quad i,j \in \bar{\mathcal{R}} \cup \{d_{\mathrm{c}}\}$

Table 3.2: Summary of notations in Section 3.2.1.

$\bar{l}_i = \epsilon\lambda_i y^i$	The expectation of the fraction of the edges connecting to the variable nodes of degree i in the residual graph
$\bar{r}_j = \sum_{i\in\mathcal{R}} \rho_i \binom{i-1}{j-1} x^j \tilde{x}^{i-j}$	The expectation of the fraction of the edges connecting to the check nodes of degree $j \in \{2, \ldots, d_{\mathrm{c}}\}$ in the residual graph
$\bar{r}_1 = x(y - 1 + \rho(\tilde{x}))$	The expectation of the fraction of the edges connecting to the check nodes of degree 1 in the residual graph
$e = \sum_{i\in\mathcal{L}} \bar{l}_i = xy$	The expectation of the fraction of the edges in the residual graph

where $\tilde{\epsilon} := 1 - \epsilon$ and

$$V_{i,j}(y) := \sum_{s\in\mathcal{R}} \rho_s s \binom{s-1}{i-1}\binom{s-1}{j-1} x^{i+j}\tilde{x}^{2s-i-j}.$$

The summary of intermediate variables and notations are in Table 3.1 and Table 3.2, respectively.

3.2.2 Scaling Law

The *scaling law* is a method which allows us to estimate the decoding erasure probability caused by the decoding erasures of large weight. In other words, the scaling law is a method to estimate the waterfall region. The scaling law is based on the analysis of the residual graphs.

In [7], the block erasure probability $P_{\mathrm{B}}(N, \epsilon)$ is given by

$$P_{\mathrm{B}}(N, \epsilon) = Q\left(\frac{\sqrt{N}(\epsilon^{\mathrm{BP}} - \epsilon)}{\alpha}\right) + o(1),$$

where α is *slope scaling parameter* depending on the ensemble and the Q-function is defined as

$$Q(z) := \frac{1}{\sqrt{2\pi}} \int_z^\infty \exp\left[-\frac{x^2}{2}\right] dx.$$

In [20], the slope scaling parameter is derived as

$$\alpha = -\sqrt{\Lambda_{\text{ave}}\ \delta^{(r_1,r_1)}\big|_{\epsilon^{\text{BP}};y^*}}\left(\frac{\partial \bar{r}_1}{\partial \epsilon}\bigg|_{\epsilon^{\text{BP}};y^*}\right)^{-1} \tag{3.3}$$

where y^* is the nonzero solution of $\bar{r}_1(y) = 0$ at the threshold, i.e., define y^* such that $y^* = 1 - \rho(1 - \epsilon^* \lambda(y^*))$.

3.3 Main Results

We show, in the following theorem, the analytical solution of the covariance evolution, for the irregular LDPC code ensembles. The proof shall be given in Section 3.4.

Theorem 1 Consider the irregular binary LDPC code ensemble $\mathrm{E}(N, \lambda, \rho)$ transmitted over the BEC with channel erasure probability ϵ. Let τ be the normalized iteration round of the PA as defined in (3.1). A parameter y is defined by $dy/d\tau = -1/(\epsilon\lambda(y))$ and $y = 1$ at $\tau = 0$. The intermediate variables are defined in Table 3.1 and Table 3.2. For the irregular LDPC code ensemble, $i, j \in \bar{\mathcal{R}}$ and $k, s \in \mathcal{L}$, in the limit of the bit length N, we obtain the following.

$$\begin{aligned}
\delta^{(l_k,l_s)} =& -\frac{ks\bar{l}_k\bar{l}_s}{e^2}F + \frac{\epsilon\bar{l}_k\bar{l}_s}{e}\left\{k\left(y^s-1\right) + s\left(y^k-1\right)\right\} + I_{\{k=s\}}k\bar{l}_k(1-\epsilon y^k), && (3.4)\\
\delta^{(l_s,r_j)} =& \left\{\frac{s\bar{l}_s}{e}F - \epsilon\bar{l}_s\left(y^s-1\right)\right\}\left(\frac{x'}{x}G_j - I_{\{j=1\}}\right) - \frac{s\bar{l}_s}{e}G_j\left(\frac{F'+x}{2} - \epsilon x y^s\right), && (3.5)\\
\delta^{(r_i,r_j)} =& -F\left(\frac{x'}{x}G_i - I_{\{i=1\}}\right)\left(\frac{x'}{x}G_j - I_{\{j=1\}}\right) + G_iG_j\left(\frac{x'}{x}F' - \epsilon^2\sum_{s\in\mathcal{L}}\lambda_s s y^{2s-2} + x^2\right)\\
& - V_{i,j} + \left(I_{\{j=1\}}G_i + I_{\{i=1\}}G_j\right)\left\{x(e-x) - \frac{F'-x}{2}\right\} + I_{\{i=j\}}i\bar{r}_i\\
& + I_{\{i=j=1\}}(e-x)^2, && (3.6)
\end{aligned}$$

where

$$\begin{aligned}
F :=& \sum_{i\in\mathcal{L}}\frac{\lambda_i}{i}\left\{\epsilon^2\left(y^i-1\right)^2 + \epsilon\left(y^i-1\right)\right\}, && (3.7)\\
F' :=& \frac{dF}{dy} = 2\epsilon^2\sum_{i\in\mathcal{L}}\lambda_i y^{2i-1} + (1-2\epsilon)x. && (3.8)
\end{aligned}$$

Using Theorem 1, we obtain the following corollary.

Corollary 1 Let ϵ^{BP} be the threshold of the ensemble under BP decoding, N be the symbol code length and ξ be the total number of edges in the original graph. Denote the nonzero solution of $\bar{r}_1(y) = 0$ at the threshold, by y^*. Define $x^* := \epsilon^*\lambda(y^*)$ and $\tilde{x}^* := 1 - x^*$. For the irregular

LDPC code ensembles $\mathrm{E}(N,\lambda,\rho)$, the slope scaling parameter α is given by

$$\alpha = \Bigg\{ \frac{\rho(\tilde{x}^*)^2 - \rho\big(\tilde{x}^{*2}\big) - \tilde{x}^{*2}\rho'\big(\tilde{x}^{*2}\big)}{\rho'(\tilde{x}^*)^2} + \frac{1-2x^*\rho(\tilde{x}^*)}{\rho'(\tilde{x}^*)} \\ + x^{*2} - \left(\epsilon^{\mathrm{BP}}\right)^2\lambda\big(y^{*2}\big) - \left(\epsilon^{\mathrm{BP}}\right)^2 y^{*2}\lambda'\big(y^{*2}\big)\Bigg\}^{\frac{1}{2}} \sqrt{\Lambda_{\mathrm{ave}}}\frac{1}{\lambda(y^*)}. \tag{3.9}$$

proof: Since $\bar{r}_1|_{\epsilon^{\mathrm{BP}};y^*} = 0$ and $\frac{\partial \bar{r}_1}{\partial y}\Big|_{\epsilon^{\mathrm{BP}};y^*} = 0$, we see that

$$1 - y^* = \rho(\tilde{x}^*), \qquad \epsilon^{\mathrm{BP}}\lambda'(y^*)\rho'(\tilde{x}^*) = 1.$$

Combining those equations, we have from (3.6),

$$\delta^{(r_1,r_1)}\Big|_{\epsilon^{\mathrm{BP}};y^*} = x^{*2}\big(\rho(\tilde{x}^*)^2 - \tilde{x}^{*2}\rho'\big(\tilde{x}^{*2}\big) - \rho\big(\tilde{x}^{*2}\big)\big) + x^{*2}\rho'(\tilde{x}^*)(1-2x^*\rho(\tilde{x}^*)) \\ + (x^*\rho'(\tilde{x}^*))^2\big(x^{*2} - \epsilon^{*2}y^{*2}\lambda'\big(y^{*2}\big) - \epsilon^{*2}\lambda\big(y^{*2}\big)\big).$$

Recall that $\bar{r}_1 = x(y - 1 + \rho(\tilde{x}))$. We see that

$$\frac{\partial \bar{r}_1}{\partial \epsilon}\Big|_{\epsilon^{\mathrm{BP}};y^*} = -x^*\lambda(y^*)\rho'(\tilde{x}^*).$$

From (3.3), we obtain (3.9). (Q.E.D.)

The result of Corollary 1 coincides with the result in [20] for the irregular LDPC code ensembles. We rigorously obtain the slope scaling parameter. Hence, we can optimize the pair of degree distributions without any assumptions by this result.

3.4 Lemmas and Proofs

In this section, we prove Theorem 1. To prove Theorem 1, we state three lemmas. We use Lemma 4, 5 and 6 to prove (3.4), (3.5) and (3.6), respectively.

From the covariance evolution (3.2), we have the following equations for $k, s \in \mathcal{L}$ and $i, j \in \bar{\mathcal{R}}$:

$$\frac{d\delta^{(l_k,l_s)}}{dy} = -x\sum_{i\in\mathcal{L}}\left(\frac{\partial \hat{f}^{(l_k)}}{\partial \bar{l}_i}\delta^{(l_i,l_s)} + \frac{\partial \hat{f}^{(l_s)}}{\partial \bar{l}_i}\delta^{(l_i,l_k)}\right) - x\hat{f}^{(l_k,l_s)}, \tag{3.10}$$

$$\frac{d\delta^{(l_k,r_i)}}{dy} = -x\sum_{s\in\mathcal{L}}\left(\frac{\partial \hat{f}^{(l_k)}}{\partial \bar{l}_s}\delta^{(l_s,r_i)} + \frac{\partial \hat{f}^{(r_i)}}{\partial \bar{l}_s}\delta^{(l_s,l_k)}\right) - x\sum_{j\in\bar{\mathcal{R}}}\frac{\partial \hat{f}^{(r_i)}}{\partial \bar{r}_j}\delta^{(l_k,r_j)} - x\hat{f}^{(l_k,r_i)}, \tag{3.11}$$

$$\frac{d\delta^{(r_i,r_j)}}{dy} = -x\sum_{s\in\mathcal{L}}\left(\frac{\partial \hat{f}^{(r_i)}}{\partial \bar{l}_s}\delta^{(l_s,r_j)} + \frac{\partial \hat{f}^{(r_j)}}{\partial \bar{l}_s}\delta^{(l_s,r_i)}\right) - x\sum_{k\in\bar{\mathcal{R}}}\left(\frac{\partial \hat{f}^{(r_i)}}{\partial \bar{r}_k}\delta^{(r_k,r_j)} + \frac{\partial \hat{f}^{(r_j)}}{\partial \bar{r}_k}\delta^{(r_k,r_i)}\right) \\ - x\hat{f}^{(r_i,r_j)}. \tag{3.12}$$

To simplify the notation, we drop some subscripts in this paragraph. Those equations assert

Table 3.3: Definitions of intermediate variables used in Section 3.4.1.

$U^{(l_k;l_s)} := \frac{1}{(k\bar{l}_k)^2}\delta^{(l_k,l_k)} - \frac{1}{(s\bar{l}_s)^2}\delta^{(l_s,l_s)}$	$k, s \in \mathcal{L}$
$\delta^{(l_k,l_\Sigma)} := \sum_{s\in\mathcal{L}} \delta^{(l_k,l_s)}$	$k \in \mathcal{L}$

- The differential equations $\frac{d}{dy}\delta^{(l,l)}$ only involve $\delta^{(l,l)}$
- The differential equations $\frac{d}{dy}\delta^{(l,r)}$ involve $\delta^{(l,l)}$ and $\delta^{(l,r)}$
- The differential equations $\frac{d}{dy}\delta^{(r,r)}$ involve $\delta^{(l,r)}$ and $\delta^{(r,r)}$

Since the differential equation $\frac{d}{dy}\delta^{(l,l)}$ only involves $\delta^{(l,l)}$, firstly, we solve $\delta^{(l,l)}$ in Section 3.4.1. If $\delta^{(l,l)}$ is known function, we are able to solve the differential equation $\frac{d}{dy}\delta^{(l,r)}$. Hence, secondly, we solve $\delta^{(l,r)}$ in Section 3.4.2. Similarly, if $\delta^{(l,r)}$ is known function, we are able to solve the differential equation $\frac{d}{dy}\delta^{(r,r)}$. Thus, finally, we give $\delta^{(r,r)}$ in Section 3.4.3.

3.4.1 Lemma and Proof of (3.4)

In this section, we give a lemma to prove (3.4) and we prove (3.4). Table 3.3 gives the definitions of intermediate variables which are used in this section.

Lemma to Prove (3.4)

Lemma 4 We define $U^{(l_k;l_s)}$ as in Table 3.3. The intermediate variables are defined in Table 3.1. For $k, s \in \mathcal{L}$, we have the following equations.

$$\sum_{k,s\in\mathcal{L}} \frac{\delta^{(l_k,l_s)}}{ks} = \epsilon\tilde{\epsilon}\sum_{i\in\mathcal{L}} \frac{\lambda_i}{i}, \tag{3.13}$$

$$2\frac{\delta^{(l_k,l_s)}}{ks\bar{l}_k\bar{l}_s} - \frac{\delta^{(l_k,l_k)}}{(k\bar{l}_k)^2} - \frac{\delta^{(l_s,l_s)}}{(s\bar{l}_s)^2} = \left(\frac{\epsilon y^k - 1}{k\bar{l}_k} + \frac{\epsilon y^s - 1}{s\bar{l}_s}\right) I_{\{k\neq s\}}, \tag{3.14}$$

$$U^{(l_k;l_s)} = -\frac{\epsilon y^k - 1}{k\bar{l}_k} + \frac{\epsilon y^s - 1}{s\bar{l}_s} + \frac{2\epsilon}{e}\left(\frac{y^k - 1}{k} - \frac{y^s - 1}{s}\right). \tag{3.15}$$

proof: Define $\delta^{(l_k,l_\Sigma)}$ as in Table 3.3. From (3.10), we get

$$\frac{d\delta^{(l_k,l_s)}}{dy} = -\frac{s\bar{l}_s}{ey}\delta^{(l_k,l_\Sigma)} - \frac{k\bar{l}_k}{ey}\delta^{(l_s,l_\Sigma)} + \frac{k+s}{y}\delta^{(l_k,l_s)} - x\hat{f}^{(l_k,l_s)}. \tag{3.16}$$

Proof of (3.13) From (3.16), we have the following equation:

$$\sum_{k,s\in\mathcal{L}} \frac{1}{ks}\frac{d\delta^{(l_k,l_s)}}{dy} = 0.$$

From the initial conditions, we obtain

$$\sum_{k,s\in\mathcal{L}} \frac{1}{ks}\delta^{(l_k,l_s)} = \epsilon\tilde{\epsilon}\sum_{i\in\mathcal{L}}\frac{\lambda_i}{i}.$$

This leads to (3.13).

Proof of (3.14) Obviously, the left hand side of (3.14) is equal to 0 for $k = s$. Hence, we get (3.14) for $k = s$. Next, we consider the case for $k \neq s$. From (3.16), we have

$$\begin{aligned}\frac{d}{dy}\left(\frac{\delta^{(l_k,l_s)}}{ks\bar{l}_k\bar{l}_s}\right) &= \frac{1}{ks\bar{l}_k\bar{l}_s}\frac{d\delta^{(l_k,l_s)}}{dy} - \frac{k+s}{ks\bar{l}_k\bar{l}_s y}\delta^{(l_k,l_s)} \\ &= -x\left(\frac{\hat{f}^{(l_k,l_s)}}{ks\bar{l}_k\bar{l}_s} + \frac{\delta^{(l_k,l_\Sigma)}}{k\bar{l}_k e^2} + \frac{\delta^{(l_s,l_\Sigma)}}{s\bar{l}_s e^2}\right). \qquad (3.17)\end{aligned}$$

For $k \neq s$, (3.17) gives the following equation:

$$\frac{d}{dy}\left[2\frac{\delta^{(l_k,l_s)}}{ks\bar{l}_k\bar{l}_s} - \frac{\delta^{(l_k,l_k)}}{(k\bar{l}_k)^2} - \frac{\delta^{(l_s,l_s)}}{(s\bar{l}_s)^2}\right] = -2\frac{x\hat{f}^{(l_k,l_s)}}{ks\bar{l}_k\bar{l}_s} + \frac{x\hat{f}^{(l_k,l_k)}}{k^2\bar{l}_k^2} + \frac{x\hat{f}^{(l_s,l_s)}}{s^2\bar{l}_s^2} = \frac{1}{y}\left(\frac{1}{\bar{l}_k} + \frac{1}{\bar{l}_s}\right).$$

The solution of this differential equation is

$$2\frac{\delta^{(l_k,l_s)}}{ks\bar{l}_k\bar{l}_s} - \frac{\delta^{(l_k,l_k)}}{(k\bar{l}_k)^2} - \frac{\delta^{(l_s,l_s)}}{(s\bar{l}_s)^2} = -\frac{1}{k\bar{l}_k} - \frac{1}{s\bar{l}_s} + C_{l_k,l_s},$$

where C_{l_k,l_s} is a constant determined from the initial conditions. The initial conditions gives

$$C_{l_k,l_s} = \frac{1}{k\lambda_k} + \frac{1}{s\lambda_s}.$$

Thus, we have for $k \neq s$

$$2\frac{\delta^{(l_k,l_s)}}{ks\bar{l}_k\bar{l}_s} - \frac{\delta^{(l_k,l_k)}}{(k\bar{l}_k)^2} - \frac{\delta^{(l_s,l_s)}}{(s\bar{l}_s)^2} = \frac{\epsilon y^k - 1}{k\bar{l}_k} + \frac{\epsilon y^s - 1}{s\bar{l}_s}.$$

Hence, we obtain (3.14).

Proof of (3.15) The equation (3.14) is rewritten for all $k, s \in \mathcal{L}$

$$\delta^{(l_k,l_s)} = \left[\frac{s\bar{l}_s}{2}\left(\epsilon y^k - 1\right) + \frac{k\bar{l}_k}{2}\left(\epsilon y^s - 1\right)\right]I_{\{k\neq s\}} + \frac{s\bar{l}_s}{2k\bar{l}_k}\delta^{(l_k,l_k)} + \frac{k\bar{l}_k}{2s\bar{l}_s}\delta^{(l_s,l_s)}.$$

The sum of this equation over all $s \in \mathcal{L}$ is written as follows:

$$\delta^{(l_k,l_\Sigma)} = \frac{ae}{2}\left(\epsilon y^k - 1\right) + \frac{k\bar{l}_k}{2}\sum_{s\in\mathcal{L}}\left(\epsilon y^s - 1\right) - k\bar{l}_k\left(\epsilon y^k - 1\right) + \frac{ae}{2k\bar{l}_k}\delta^{(l_k,l_k)} + k\bar{l}_k\sum_{s\in\mathcal{L}}\frac{\delta^{(l_s,l_s)}}{2s\bar{l}_s}.$$

Combining (3.17) with this equation, we have

$$\begin{aligned}\frac{d}{dy}\left[\frac{\delta^{(l_k,l_k)}}{(k\bar{l}_k)^2}\right] &= -x\frac{\hat{f}^{(l_k,l_k)}}{k^2\bar{l}_k^2} - 2\frac{\delta^{(l_k,l_\Sigma)}}{k\bar{l}_k ey} \\ &= K^{(l_k,l_k)} - \frac{a}{y}\frac{\delta^{(l_k,l_k)}}{(k\bar{l}_k)^2} - \frac{1}{ey}\sum_{s\in\mathcal{L}}(\epsilon y^s - 1) - \frac{1}{ey}\sum_{s\in\mathcal{L}}\frac{\delta^{(l_s,l_s)}}{s\bar{l}_s},\end{aligned}$$

where

$$K^{(l_k,l_k)} := -x\frac{\hat{f}^{(l_k,l_k)}}{(k\bar{l}_k)^2} - \frac{a}{k\bar{l}_k y}\big(\epsilon y^k - 1\big) + \frac{2}{ey}\big(\epsilon y^k - 1\big).$$

From this equation and the definition of $U^{(l_k;l_s)}$ in Table 3.3, we have

$$\frac{dU^{(l_k;l_s)}}{dy} = \frac{d}{dy}\left[\frac{\delta^{(l_k,l_k)}}{(k\bar{l}_k)^2}\right] - \frac{d}{dy}\left[\frac{\delta^{(l_s,l_s)}}{(s\bar{l}_s)^2}\right] = K^{(l_k,l_k)} - K^{(l_s,l_s)} - \frac{a}{y}U^{(l_k;l_s)}. \tag{3.18}$$

Note that

$$\int \frac{a}{y}dy = \ln e.$$

Since (3.18) is a first order differential equation, it is solved as follows:

$$U^{(l_k;l_s)} = \frac{1}{e}\int e\Big(K^{(l_k,l_k)} - K^{(l_s,l_s)}\Big)dy + \frac{1}{e}C_{l_k;l_s},$$

with a constant $C_{l_k;l_s}$ which is determined from the initial conditions. The integration of the part of this equation is

$$\begin{aligned}\int eK^{(l_k,l_k)}dy &= \int\left[-\frac{x'y+x}{k\lambda_k} + \frac{x'y-(k-1)x}{k\bar{l}_k} + 2\epsilon y^{k-1} - \frac{1}{y}\right]dy \\ &= -\frac{e}{k\lambda_k} + \sum_{i\in\mathcal{L}}\frac{\bar{l}_i}{k\bar{l}_k}I_{\{i\neq k\}} + \frac{2\epsilon y^k}{k} - \ln y \\ &= -\frac{\epsilon y^k - 1}{k\bar{l}_k}e + \frac{2\epsilon y^k - 1}{k} - \ln y.\end{aligned}$$

Hence, we get

$$U^{(l_k;l_s)} = -\frac{\epsilon y^k - 1}{k\bar{l}_k} + \frac{\epsilon y^s - 1}{s\bar{l}_s} + \frac{1}{e}\left(\frac{2\epsilon y^k - 1}{k} - \frac{2\epsilon y^s - 1}{s} + C_{l_k;l_s}\right).$$

From the initial conditions, we have

$$U^{(l_k;l_s)}(1) = \frac{\tilde{\epsilon}}{\epsilon}\left(\frac{1}{k\lambda_k} - \frac{1}{s\lambda_s}\right).$$

Hence, the constant $C_{l_k;l_s}$ is derived as

$$C_{l_k;l_s} = \frac{1-2\epsilon}{k} - \frac{1-2\epsilon}{s}.$$

Therefore, we have

$$U^{(l_k;l_s)} = -\frac{\epsilon y^k - 1}{k\bar{l}_k} + \frac{\epsilon y^s - 1}{s\bar{l}_s} + \frac{2\epsilon}{e}\left(\frac{y^k-1}{k} - \frac{y^s-1}{s}\right).$$

Thus, (3.15) holds. (Q.E.D.)

Proof of (3.4)

Here, by using Lemma 4, we prove (3.4). Firstly, we consider $\delta^{(l_s,l_s)}$. By transforming $U^{(l_k;l_s)}$, we have

$$\frac{\bar{l}_k}{e}\delta^{(l_s,l_s)} = \frac{(s\bar{l}_s)^2}{e}\left(\frac{\delta^{(l_k,l_k)}}{k^2\bar{l}_k} - \bar{l}_k U^{(l_k;l_s)}\right).$$

The sum of this equation over all $k \in \mathcal{L}$ is written as follows:

$$\delta^{(l_s,l_s)} = \frac{(s\bar{l}_s)^2}{e}\sum_{k\in\mathcal{L}}\frac{\delta^{(l_k,l_k)}}{k^2\bar{l}_k} - \frac{(s\bar{l}_s)^2}{e}\sum_{k\in\mathcal{L}}\bar{l}_k U^{(l_k;l_s)}. \tag{3.19}$$

Now, we consider the first term of (3.19). By transforming (3.14), we see that for all $k, s \in \mathcal{L}$

$$\frac{1}{2}\frac{\bar{l}_s}{k^2\bar{l}_k}\delta^{(l_k,l_k)} + \frac{1}{2}\frac{\bar{l}_k}{s^2\bar{l}_s}\delta^{(l_s,l_s)} = \frac{1}{ks}\delta^{(l_k,l_s)} - \frac{\bar{l}_s}{2}\frac{\epsilon y^k-1}{k}I_{\{k\neq s\}} - \frac{\bar{l}_k}{2}\frac{\epsilon y^s-1}{s}I_{\{k\neq s\}}.$$

The sum of this equation over all $k, s \in \mathcal{L}$ is written as follows:

$$e\sum_{k\in\mathcal{L}}\frac{\delta^{(l_k,l_k)}}{k^2\bar{l}_k} = \sum_{k,s\in\mathcal{L}}\frac{\delta^{(l_k,l_s)}}{ks} + \sum_{k\in\mathcal{L}}(\bar{l}_k - e)\frac{\epsilon y^k - 1}{k}. \tag{3.20}$$

Combining (3.20) with (3.13), we have

$$\sum_{k\in\mathcal{L}}\frac{\delta^{(l_k,l_k)}}{k^2\bar{l}_k} = \frac{\epsilon\tilde{\epsilon}}{e}\sum_{k\in\mathcal{L}}\frac{\lambda_k}{k} + \sum_{k\in\mathcal{L}}\frac{\bar{l}_k - e}{e}\frac{\epsilon y^k - 1}{k}. \tag{3.21}$$

Next, we consider the second term of (3.19). From (3.15), we have

$$\sum_{k\in\mathcal{L}}\bar{l}_k U^{(l_k;l_s)} = \frac{e}{s\bar{l}_s}\big(\epsilon y^s - 1\big) - 2\epsilon\frac{y^s-1}{s} - \sum_{k\in\mathcal{L}}\frac{\epsilon y^k - 1}{k} + \frac{2\epsilon}{e}\sum_{k\in\mathcal{L}}\frac{\bar{l}_k\big(y^k-1\big)}{k}. \tag{3.22}$$

Combining (3.19) with (3.21) and (3.22), we obtain

$$\delta^{(l_s,l_s)} = -\frac{(s\bar{l}_s)^2}{e^2}F + 2\epsilon\frac{s\bar{l}_s^2}{e}\big(y^s - 1\big) + s\bar{l}_s\big(1 - \epsilon y^s\big). \tag{3.23}$$

Table 3.4: Definitions of intermediate variables used in Section 3.4.2.

$\delta^{(l_\Sigma,r_j)} := \sum_{k\in\mathcal{L}} \delta^{(l_k,r_j)}$	$j \in \bar{\mathcal{R}}$
$\delta^{(l_k,r_\Sigma)} := \sum_{j\in\bar{\mathcal{R}}} \delta^{(l_k,r_j)}$	$k \in \mathcal{L}$
$\delta^{(l_k,r_{d_c})} := \delta^{(l_k,l_\Sigma)} - \delta^{(l_k,r_\Sigma)}$	$k \in \mathcal{L}$
$A^{(l_\Sigma,r_j)} := \sum_{i\in\mathcal{L}} i^{-1}\delta^{(l_i,r_j)}$	$j \in \bar{\mathcal{R}}$
$A^{(l_\Sigma,r_\Sigma)} := \sum_{j\in\bar{\mathcal{R}}} A^{(l_\Sigma,r_j)}$	
$A^{(l_\Sigma,r_{d_c})} := \sum_{i\in\mathcal{L}} i^{-1}\delta^{(l_i,r_{d_c})}$	
$S^{(l_i,l_s;r_j)} := \frac{1}{i\bar{l}_i}\delta^{(l_i,r_j)} - \frac{1}{s\bar{l}_s}\delta^{(l_s,r_j)}$	$i,s \in \mathcal{L}$, $j \in \bar{\mathcal{R}}$
$S^{(l_i,l_s;r_\Sigma)} := \sum_{j\in\bar{\mathcal{R}}} S^{(l_i,l_s;r_j)}$	$i,s \in \mathcal{L}$
$S^{(l_i,l_s;r_{d_c})} := \frac{1}{i\bar{l}_i}\delta^{(l_i,r_{d_c})} - \frac{1}{s\bar{l}_s}\delta^{(l_s,r_{d_c})}$	$i,s \in \mathcal{L}$
$S^{(l_k,l_s;l_i)} := \frac{1}{k\bar{l}_k}\delta^{(l_k,l_i)} - \frac{1}{s\bar{l}_s}\delta^{(l_s,l_i)}$	$k,s,i \in \mathcal{L}$
$S^{(l_k,l_s;l_\Sigma)} := \sum_{i\in\mathcal{L}} S^{(l_k,l_s;l_i)}$	$k,s \in \mathcal{L}$
$G_\Sigma := \sum_{j\in\bar{\mathcal{R}}} G_j = x^{-1}(d_\mathrm{c}\bar{r}_{d_\mathrm{c}} - e)$	
$D^{(l_k,r_j)} := 2\frac{x'}{e}G_j\delta^{(l_k,l_\Sigma)} - x\hat{f}^{(l_k,r_j)} - \frac{1}{y^2}G_j\sum_{i\in\mathcal{L}}(i-1)\delta^{(l_k,l_i)}$	$k \in \mathcal{L}$, $j \in \mathcal{R}$
$D^{(l_k,r_\Sigma)} := \sum_{j\in\bar{\mathcal{R}}} D^{(l_k,r_j)}$	$k \in \mathcal{L}$

Secondly, we consider $\delta^{(l_k,l_s)}$ for $k \neq s$. From (3.14), we see that for $k \neq s$

$$\delta^{(l_k,l_s)} = \frac{s\bar{l}_s}{2k\bar{l}_k}\delta^{(l_k,l_k)} + \frac{k\bar{l}_k}{2s\bar{l}_s}\delta^{(l_s,l_s)} + \frac{\epsilon y^k - 1}{2s\bar{l}_s} + \frac{\epsilon y^s - 1}{2k\bar{l}_k}.$$

Combining this equation with (3.23), we obtain (3.4) for $k, s \in \mathcal{L}$.

3.4.2 Lemma and Proof of (3.5)

In this section, we introduce a lemma to prove (3.5) and we prove (3.5). The definitions of intermediate variables used in this section are summarized in Table 3.4.

Lemma to Prove (3.5)

Lemma 5 We define $A^{(l_\Sigma,r_j)}$, $A^{(l_\Sigma,r_\Sigma)}$, $S^{(l_i,l_s;r_j)}$, $S^{(l_i,l_s;r_\Sigma)}$ and G_Σ as in Table 3.4. The intermediate variables are defined in Table 3.1. For $j \in \bar{\mathcal{R}}$ and $k, s \in \mathcal{L}$, we have the following equations.

$$A^{(l_\Sigma,r_\Sigma)} = \epsilon\tilde{\epsilon}\left(\frac{x'}{x}G_\Sigma - 1\right)\sum_{i\in\mathcal{L}}\frac{\lambda_i}{i}\left(y^i - 1\right) - \tilde{\epsilon}xG_\Sigma, \tag{3.24}$$

$$A^{(l_\Sigma,r_j)} = \epsilon\tilde{\epsilon}\left(\frac{x'}{x}G_j - I_{\{j=1\}}\right)\sum_{i\in\mathcal{L}}\frac{\lambda_i}{i}\left(y^i - 1\right) - \tilde{\epsilon}xG_j, \tag{3.25}$$

$$S^{(l_k,l_s;r_\Sigma)} = -\epsilon\left(\frac{x'}{x}G_\Sigma - 1\right)\left(\frac{y^k-1}{k} - \frac{y^s-1}{s}\right) + \epsilon G_\Sigma\big(y^{k-1} - y^{s-1}\big), \tag{3.26}$$

$$S^{(l_k,l_s;r_j)} = -\epsilon\left(\frac{x'}{x}G_j - I_{\{j=1\}}\right)\left(\frac{y^k-1}{k} - \frac{y^s-1}{s}\right) + \epsilon G_j\big(y^{k-1} - y^{s-1}\big). \tag{3.27}$$

We use (3.24) and (3.26) to prove the basis of the mathematical induction in the proof of (3.25) and (3.27), respectively.

proof: We will derive the differential equations. Firstly, we consider $A^{(l_\Sigma,r_j)}$ for $j \in \bar{\mathcal{R}}$. We define $\delta^{(l_\Sigma,r_j)}$, $\delta^{(l_k,r_\Sigma)}$ and $\delta^{(l_k,r_{d_c})}$ as in Table 3.4. From (3.11) we have for $j \in \bar{\mathcal{R}}$ and $k \in \mathcal{L}$

$$\frac{d\delta^{(l_k,r_j)}}{dy} = D^{(l_k,r_j)} - \frac{k\bar{l}_k}{ey}\delta^{(l_\Sigma,r_j)} + \frac{k}{y}\delta^{(l_k,r_j)} - j\frac{x'}{x}\Big(\delta^{(l_k,r_{j+1})} - \delta^{(l_k,r_j)}\Big), \tag{3.28}$$

where a known function $D^{(l_k,r_j)}$ is defined as for $k \in \mathcal{L}$ and $j \in \mathcal{R}$

$$D^{(l_k,r_j)} := 2\frac{x'}{e}G_j\delta^{(l_k,l_\Sigma)} - x\hat{f}^{(l_k,r_j)} - \frac{G_j}{y^2}\sum_{i\in\mathcal{L}}(i-1)\delta^{(l_k,l_i)}.$$

From (3.28), we have for $k \in \bar{\mathcal{R}}$

$$\frac{dA^{(l_\Sigma,r_j)}}{dy} = \sum_{k\in\mathcal{L}}\frac{1}{k}\frac{d\delta^{(l_k,r_j)}}{dy} = \sum_{k\in\mathcal{L}}\frac{D^{(l_k,r_j)}}{k} - j\frac{x'}{x}\Big(A^{(l_\Sigma,r_{j+1})} - A^{(l_\Sigma,r_j)}\Big). \tag{3.29}$$

From this equation, we see that $A^{(l_\Sigma,r_j)}$ is solved if $A^{(l_\Sigma,r_{j+1})}$ is a known function. Moreover, we see that $A^{(l_\Sigma,r_{d_c-1})}$ is solved if $A^{(l_\Sigma,r_\Sigma)}$ is a known function.

Secondly, we consider $A^{(l_\Sigma,r_\Sigma)}$. The sum of (3.29) over all $j \in \bar{\mathcal{R}}$ gives $\frac{d}{dy}A^{(l_\Sigma,r_\Sigma)}$ as follows:

$$\frac{dA^{(l_\Sigma,r_\Sigma)}}{dy} = \sum_{k\in\mathcal{L}}\frac{D^{(l_k,r_\Sigma)}}{k} - (d_\mathrm{c}-1)\frac{x'}{x}\sum_{k\in\mathcal{L}}\frac{1}{k}\delta^{(l_k,l_\Sigma)} + d_\mathrm{c}\frac{x'}{x}A^{(l_\Sigma,r_\Sigma)}. \tag{3.30}$$

Since this equation is a first order differential equation and the first and second terms of this equation are known function, we are able to solve this equation. The derivation of $A^{(l_\Sigma,r_\Sigma)}$ is written in Section 3.4.2.

Next, we derive the differential equation of $S^{(l_k,l_s;r_j)}$ for $k,s \in \mathcal{L}$ and $j \in \bar{\mathcal{R}}$. By using (3.28), we get

$$\begin{aligned}\frac{d}{dy}\left(\frac{\delta^{(l_k,r_j)}}{k\bar{l}_k}\right) &= \frac{1}{k\bar{l}_k}\frac{d\delta^{(l_k,r_j)}}{dy} - \frac{1}{\bar{l}_k y}\delta^{(l_k,r_j)} \\ &= \frac{D^{(l_k,r_j)}}{k\bar{l}_k} - \frac{1}{ey}\delta^{(l_\Sigma,r_j)} - \frac{j}{k\bar{l}_k}\frac{x'}{x}\Big(\delta^{(l_k,r_{j+1})} - \delta^{(l_k,r_j)}\Big).\end{aligned} \tag{3.31}$$

Define $S^{(l_k,l_s;r_j)}$, $S^{(l_k,l_s;l_i)}$ and $S^{(l_k,l_s;l_\Sigma)}$ as in Table 3.4. From (3.31), we have

$$\frac{dS^{(l_k,l_s;r_j)}}{dy} = \frac{D^{(l_k,r_j)}}{k\bar{l}_k} - \frac{D^{(l_s,r_j)}}{s\bar{l}_s} - j\frac{x'}{x}\Big(S^{(l_k,l_s;r_{j+1})} - S^{(l_k,l_s;r_j)}\Big), \tag{3.32}$$

for $k, s \in \mathcal{L}$ and $j \in \bar{\mathcal{R}}$. From this equation, we see that we obtain $S^{(l_k,l_s;r_j)}$ if the function $S^{(l_k,l_s;r_{j+1})}$ is known. Moreover, we see that we obtain $S^{(l_k,l_s;r_{d_\mathrm{c}-1})}$ if the function $S^{(l_k,l_s;r_\Sigma)}$ is known.

Finally, we consider $S^{(l_k,l_s;r_\Sigma)}$. From the sum of (3.32) over all $j \in \bar{\mathcal{R}}$, we obtain

$$\frac{dS^{(l_k,l_s;r_\Sigma)}}{dy} = \frac{D^{(l_k,r_\Sigma)}}{k\bar{l}_k} - \frac{D^{(l_s,r_\Sigma)}}{s\bar{l}_s} - (d_\mathrm{c}-1)\frac{x'}{x}S^{(l_k,l_s;l_\Sigma)} + d_\mathrm{c}\frac{x'}{x}S^{(l_k,l_s;r_\Sigma)}. \tag{3.33}$$

Since this equation is a first order of differential equation, we are able to solve this equation. we will derive $S^{(l_k,l_s;r_\Sigma)}$ in Section 3.4.2.

Proof of (3.24) Since (3.30) is a first order differential equation, it is solved as follows[1]:

$$\begin{aligned} A^{(l_\Sigma,r_\Sigma)} &= x^{d_\mathrm{c}} \int \frac{1}{x^{d_\mathrm{c}}} \left[\sum_{k\in\mathcal{L}} \frac{D^{(l_k,r_\Sigma)}}{k} - (d_\mathrm{c}-1)\frac{x'}{x} \sum_{k\in\mathcal{L}} \frac{\delta^{(l_k,l_\Sigma)}}{k} \right] dy + C_{l_\Sigma,r_\Sigma} x^{d_\mathrm{c}} \\ &= \epsilon\tilde{\epsilon}\left(\frac{x'}{x}G_\Sigma - 1\right) \sum_{k\in\mathcal{L}} \frac{\lambda_k}{k}\big(y^k - 1\big) + \tilde{\epsilon}xy + C_{l_\Sigma,r_\Sigma} x^{d_\mathrm{c}}, \end{aligned}$$

with a constant C_{l_Σ,r_Σ} which is derived from the initial conditions. From the initial conditions, we see that

$$A^{(l_\Sigma,r_\Sigma)}(1) = \epsilon\tilde{\epsilon}\big(1 - \epsilon^{d_\mathrm{c}-1}\rho_{d_\mathrm{c}} d_\mathrm{c}\big).$$

From this equation, we determine $C_{l_\Sigma,r_\Sigma} = -d_\mathrm{c}\rho_{d_\mathrm{c}}\tilde{\epsilon}$. Thus, we find

$$A^{(l_\Sigma,r_\Sigma)} = \epsilon\tilde{\epsilon}\left(\frac{x'}{x}G_\Sigma - 1\right) \sum_{k\in\mathcal{L}} \frac{\lambda_k}{k}\big(y^k - 1\big) - \tilde{\epsilon}xG_\Sigma.$$

Hence, we have (3.24).

Proof of (3.25) Since (3.29) is a first order differential equation, the solution of (3.29) is

$$A^{(l_\Sigma,r_j)} = x^j \int \frac{1}{x^j} \left(\sum_{k\in\mathcal{L}} \frac{D^{(l_k,r_j)}}{k} - j\frac{x'}{x}A^{(l_\Sigma,r_{j+1})} \right) dy + C_{l_\Sigma,r_j} x^j, \tag{3.34}$$

where C_{l_Σ,r_j} is a constant derived from the initial conditions.

We solve (3.34) by mathematical induction for $j \in \bar{\mathcal{R}} \setminus \{1\}$. Firstly, we derive $A^{(l_\Sigma,r_{d_\mathrm{c}-1})}$. Using (3.4), (3.24) and the definition of $A^{(l_\Sigma,r_{d_\mathrm{c}})}$ and $A^{(l_\Sigma,r_\Sigma)}$, we have

$$A^{(l_\Sigma,r_{d_\mathrm{c}})} = \sum_{i\in\mathcal{L}} \frac{\delta^{(l_i,l_\Sigma)} - \delta^{(l_i,r_\Sigma)}}{i} = \sum_{i\in\mathcal{L}} \frac{\delta^{(l_i,l_\Sigma)}}{i} - A^{(l_\Sigma,r_\Sigma)} = \epsilon\tilde{\epsilon}\frac{x'}{x}G_{d_\mathrm{c}} \sum_{i\in\mathcal{L}} \frac{\lambda_i}{i}(y^i - 1) - \tilde{\epsilon}xG_{d_\mathrm{c}}. \tag{3.35}$$

[1] In a way similar to the derivation of $A^{(l_\Sigma,r_{d_\mathrm{c}})}$ we perform this calculation in Section 3.4.2. More precisely, we use integration by parts to integrate (3.30).

Note that for $j \in \bar{\mathcal{R}} \setminus \{1\}$

$$\sum_{k \in \mathcal{L}} \frac{D^{(l_k, r_j)}}{k} = \tilde{\epsilon} x' G_j + \epsilon\tilde{\epsilon} \frac{x''}{x} G_j \sum_{i \in \mathcal{L}} \frac{\lambda_i}{i} \big(y^i - 1\big) - 2\epsilon\tilde{\epsilon} \frac{(x')^2}{x^2} G_j \sum_{i \in \mathcal{L}} \frac{\lambda_i}{i} \big(y^i - 1\big). \tag{3.36}$$

The combination of (3.34), (3.35) and (3.36) gives

$$\begin{aligned}
A^{(l_\Sigma, r_{d_c - 1})} =& \; x^{d_c - 1} \int \frac{1}{x^{d_c - 1}} \sum_{k \in \mathcal{L}} \frac{D^{(l_k, r_{d_c - 1})}}{k} dy - x^{d_c - 1} \int \frac{x'}{x^{d_c}} (d_c - 1) A^{(l_\Sigma, r_{d_c})} dy + C_{l_\Sigma, r_{d_c}} x^{d_c - 1} \\
=& x^{d_c - 1} \int \frac{G_{d_c - 1}}{x^{d_c - 1}} \left\{ \tilde{\epsilon} x' - 2\epsilon\tilde{\epsilon} \frac{(x')^2}{x^2} \sum_{i \in \mathcal{L}} \frac{\lambda_i}{i} \big(y^i - 1\big) \right\} dy \\
&+ x^{d_c - 1} \int \epsilon\tilde{\epsilon} \frac{x''}{x^{d_c}} G_{d_c - 1} \sum_{i \in \mathcal{L}} \frac{\lambda_i}{i} \big(y^i - 1\big) dy \\
&- x^{d_c - 1} \int \epsilon\tilde{\epsilon} (d_c - 1) \frac{(x')^2}{x^{d_c + 1}} G_{d_c} \sum_{i \in \mathcal{L}} \frac{\lambda_i}{i} \big(y^i - 1\big) dy \\
&+ x^{d_c - 1} \int \tilde{\epsilon} (d_c - 1) \frac{x'}{x^{d_c - 1}} G_{d_c} dy + C_{l_\Sigma, r_{d_c - 1}} x^{d_c - 1}.
\end{aligned} \tag{3.37}$$

Using integration by parts, the second term of (3.37) is written as follows:

$$\begin{aligned}
&x^{d_c - 1} \int \epsilon\tilde{\epsilon} \frac{x''}{x^{d_c}} G_{d_c - 1} \sum_{i \in \mathcal{L}} \frac{\lambda_i}{i} \big(y^i - 1\big) dy \\
&\quad = \epsilon\tilde{\epsilon} \frac{x'}{x} G_{d_c - 1} \sum_{i \in \mathcal{L}} \frac{\lambda_i}{i} \big(y^i - 1\big) - x^{d_c - 1} \int \epsilon\tilde{\epsilon} \left\{ \frac{G_{d_c - 1}}{x^{d_c}} \sum_{i \in \mathcal{L}} \frac{\lambda_i}{i} \big(y^i - 1\big) \right\}' x' dy.
\end{aligned}$$

Hence, we have

$$\begin{aligned}
&x^{d_c - 1} \int \epsilon\tilde{\epsilon} \frac{x''}{x^{d_c}} G_{d_c - 1} \sum_{i \in \mathcal{L}} \frac{\lambda_i}{i} \big(y^i - 1\big) dy + x^{d_c - 1} \int \epsilon\tilde{\epsilon} \left\{ \frac{G_{d_c - 1}}{x^{d_c}} \sum_{i \in \mathcal{L}} \frac{\lambda_i}{i} \big(y^i - 1\big) \right\}' x' dy \\
&\quad = \epsilon\tilde{\epsilon} \frac{x'}{x} G_{d_c - 1} \sum_{i \in \mathcal{L}} \frac{\lambda_i}{i} \big(y^i - 1\big).
\end{aligned} \tag{3.38}$$

Since $G_j' = -j \frac{x'}{x} G_{j+1} + (j-1) \frac{x'}{x} G_j$ for $j \in \bar{\mathcal{R}} \setminus \{1\}$, the second term of left hand side of (3.38) are transformed as follows:

$$\begin{aligned}
&x^{d_c - 1} \int \epsilon\tilde{\epsilon} \left\{ \frac{G_{d_c - 1}}{x^{d_c}} \sum_{i \in \mathcal{L}} \frac{\lambda_i}{i} \big(y^i - 1\big) \right\}' x' dy \\
&\quad = x^{d_c - 1} \int \frac{G_{d_c - 1}}{x^{d_c - 1}} \left\{ \tilde{\epsilon} x' - 2\epsilon\tilde{\epsilon} \frac{(x')^2}{x^2} \sum_{i \in \mathcal{L}} \frac{\lambda_i}{i} \big(y^i - 1\big) \right\} dy \\
&\qquad - x^{d_c - 1} \int \epsilon\tilde{\epsilon} (d_c - 1) \frac{(x')^2}{x^{d_c + 1}} G_{d_c} \sum_{i \in \mathcal{L}} \frac{\lambda_i}{i} \big(y^i - 1\big) dy.
\end{aligned}$$

The first and second terms of this equation coincide with the first and third term of (3.37), respectively. In other words, the sum of the first three terms of (3.37) is equal to the right hand side of (3.38). The fourth term of (3.37) is transformed as follows:

$$\int \frac{1}{x^{d_\mathrm{c}-1}}\tilde{\epsilon}(d_\mathrm{c}-1)x' G_{d_\mathrm{c}} dy = -\tilde{\epsilon}\frac{1}{x^{d_\mathrm{c}-2}} G_{d_\mathrm{c}-1}.$$

Thus, we obtain

$$A^{(l_\Sigma, r_{d_\mathrm{c}-1})} = \epsilon\tilde{\epsilon}\frac{x'}{x} G_{d_\mathrm{c}-1} \sum_{i\in\mathcal{L}} \frac{\lambda_i}{i}\big(y^i - 1\big) - \tilde{\epsilon} x G_{d_\mathrm{c}-1} + C_{l_\Sigma, r_{d_\mathrm{c}-1}} x^{d_\mathrm{c}-1}.$$

The initial conditions give

$$A^{(l_\Sigma, r_{d_\mathrm{c}-1})}(1) = -\epsilon\tilde{\epsilon} G_j(1).$$

Hence, we get $C_{l_\Sigma, r_{d_\mathrm{c}-1}} = 0$. Thus, we show that $A^{(l_\Sigma, r_{d_\mathrm{c}-1})}$ fulfills (3.25). Now, we consider the induction step. In other words, we show that if $A^{(l_\Sigma, r_{j+1})}$ fulfills (3.25), then $A^{(l_\Sigma, r_j)}$ also fulfills (3.25). Using the induction hypothesis, the first term of (3.34) is written as follows:

$$\begin{aligned}
&x^j \int \frac{1}{x^j}\left(\sum_{k\in\mathcal{L}} \frac{D^{(l_k, r_j)}}{k} - j\frac{x'}{x} A^{(l_\Sigma, r_{j+1})}\right) dy \\
&= x^j \int \frac{1}{x^j}\left\{\tilde{\epsilon} x' G_j - 2\epsilon\tilde{\epsilon}\frac{(x')^2}{x^2} G_j \sum_{i\in\mathcal{L}} \frac{\lambda_i}{i}\big(y^i - 1\big)\right\} dy + x^j \int \epsilon\tilde{\epsilon}\frac{x''}{x^{j+1}} G_j \sum_{i\in\mathcal{L}} \frac{\lambda_i}{i}\big(y^i - 1\big) dy \\
&\quad - x^j \int \epsilon\tilde{\epsilon} j \frac{(x')^2}{x^{j+2}} G_{j+1} \sum_{i\in\mathcal{L}} \frac{\lambda_i}{i}\big(y^i - 1\big) dy + x^j \int \tilde{\epsilon} j \frac{x'}{x^j} G_{j+1} dy \\
&= \epsilon\tilde{\epsilon}\frac{x'}{x} G_j \sum_{i\in\mathcal{L}} \frac{\lambda_i}{i}\big(y^i - 1\big) - \tilde{\epsilon} x G_j.
\end{aligned}$$

Here, the last step is derived from a similar way to $A^{(l_\Sigma, r_{d_\mathrm{c}-1})}$. Hence, we get

$$A^{(l_\Sigma, r_j)} = \epsilon\tilde{\epsilon}\frac{x'}{x} G_j \sum_{i\in\mathcal{L}} \frac{\lambda_i}{i}\big(y^i - 1\big) - \tilde{\epsilon} x G_j + C_{l_\Sigma, r_j} x^j.$$

From the initial conditions, we have

$$A^{(l_\Sigma, r_j)}(1) = -\epsilon\tilde{\epsilon} G_j(1).$$

Hence, we have $C_{l_\Sigma, r_j} = 0$. Thus, we find

$$A^{(l_\Sigma, r_j)} = \epsilon\tilde{\epsilon}\frac{x'}{x} G_j \sum_{i\in\mathcal{L}} \frac{\lambda_i}{i}\big(y^i - 1\big) - \tilde{\epsilon} x G_j.$$

This leads to (3.25) for $j \in \bar{\mathcal{R}} \setminus \{1\}$.

Next, we consider $A^{(l_\Sigma,r_1)}$. Since $A^{(l_\Sigma,r_1)} = A^{(l_\Sigma,r_\Sigma)} - \sum_{j=2}^{d_c-1} A^{(l_\Sigma,r_j)}$, we have

$$A^{(l_\Sigma,r_1)} = \epsilon\tilde{\epsilon}\biggl(\frac{x'}{x}G_1 - 1\biggr)\sum_{i\in\mathcal{L}}\frac{\lambda_i}{i}\bigl(y^i - 1\bigr) - \tilde{\epsilon}xG_1.$$

Hence, we obtain (3.25).

Proof of (3.26) Since (3.33) is a first order differential equation, it is solved as follows:

$$S^{(l_k,l_s;r_\Sigma)} = x^{d_c}\int\frac{1}{x^{d_c}}\left[\frac{D^{(l_k,r_\Sigma)}}{k\bar{l}_k} - \frac{D^{(l_s,r_\Sigma)}}{s\bar{l}_s} - (d_c-1)\frac{x'}{x}S^{(l_k,l_s;l_\Sigma)}\right]dy + C_{l_k,l_s;r_\Sigma}x^{d_c}.$$

Note that

$$\frac{D^{(l_k,r_\Sigma)}}{k\bar{l}_k} - \frac{D^{(l_s,r_\Sigma)}}{s\bar{l}_s} - (d_c-1)\frac{x'}{x}S^{(l_k,l_s;l_\Sigma)} = K^{(l_k,r_\Sigma)} - K^{(l_s,r_\Sigma)},$$

where

$$\begin{aligned}K^{(l_k,r_\Sigma)} = {} & \epsilon G_\Sigma\left[-2\frac{x'}{x}y^{k-1} + (k-1)y^{k-2} + \frac{2(x')^2 - x''x}{x^2}\frac{y^k-1}{k}\right]\\ & + \epsilon(d_c-1)\frac{x'}{x}\biggl(y^k - \frac{x'y+x}{x}\frac{y^k-1}{k}\biggr).\end{aligned}$$

By using integration by parts, we have

$$x^{d_c}\int\frac{1}{x^{d_c}}K^{(l_k,r_\Sigma)}dy = -\epsilon\biggl(\frac{x'}{x}G_\Sigma - 1\biggr)\frac{y^k-1}{k} + \epsilon G_\Sigma y^{k-1}.$$

Thus, we have

$$S^{(l_k,l_s;r_\Sigma)} = -\epsilon\biggl(\frac{x'}{x}G_\Sigma - 1\biggr)\biggl(\frac{y^k-1}{k} - \frac{y^s-1}{s}\biggr) + \epsilon G_\Sigma\bigl(y^{k-1} - y^{s-1}\bigr) + C_{l_k,l_s;r_\Sigma}x^{d_c}.$$

The initial covariance leads $S^{(l_i,l_s;r_\Sigma)}(1) = 0$ and $C_{l_k,l_s;r_\Sigma} = 0$. Hence (3.26) holds.

Proof of (3.27) In a way similar to Section 3.4.2, i.e., by mathematical induction for $j \in \bar{\mathcal{R}}\backslash\{1\}$ and $S^{(l_k,l_s;r_1)} = S^{(l_k,l_s;r_\Sigma)} - \sum_{i=2}^{d_c-1} S^{(l_k,l_s;r_i)}$, we obtain (3.27). (Q.E.D.)

Proof of (3.5)

From definitions of $S^{(l_k,l_s;r_j)}$ and $A^{(l_\Sigma,r_j)}$, we see that

$$\begin{aligned}\delta^{(l_s,r_j)} = {} & \frac{s\bar{l}_s}{e}\biggl(A^{(l_\Sigma,r_j)} - \sum_{k\in\mathcal{L}}\bar{l}_kS^{(l_k,l_s;r_j)}\biggr)\\ = {} & \left[\frac{s\bar{l}_s}{e}F - \epsilon\bar{l}_s(y^s-1)\right]\biggl(\frac{x'}{x}G_j - I_{\{j=1\}}\biggr) - \frac{s\bar{l}_s}{e}G_j\biggl(\frac{F'+x}{2} - \epsilon xy^s\biggr).\end{aligned}$$

Thus, we obtain (3.5).

Table 3.5: Definitions of intermediate variables used in Section 3.4.3.

$\delta^{(r_j,r_\Sigma)} := \sum_{k\in\bar{\mathcal{R}}} \delta^{(r_j,r_k)}$	$j \in \bar{\mathcal{R}}$
$\delta^{(r_\Sigma,r_\Sigma)} := \sum_{j\in\bar{\mathcal{R}}} \delta^{(r_j,r_\Sigma)}$	
$\delta^{(r_{d_\mathrm{c}},r_j)} := \delta^{(l_\Sigma,r_j)} - \delta^{(r_\Sigma,r_j)}$	$j \in \bar{\mathcal{R}}$
$D^{(r_i,r_j)} := \sum_{k\in\mathcal{L}} y^{-2}(2a-k-1)\big(\delta^{(l_k,r_j)}G_i + \delta^{(l_k,r_i)}G_j\big) - x\hat{f}^{(r_i,r_j)}$	$i,j \in \bar{\mathcal{R}}$
$D^{(r_i,r_\Sigma)} := \sum_{j\in\bar{\mathcal{R}}} D^{(r_i,r_j)}$	$i \in \mathcal{R}$
$D^{(r_\Sigma,r_\Sigma)} := \sum_{i\in\bar{\mathcal{R}}} D^{(r_i,r_\Sigma)}$	

3.4.3 Lemma and Proof of (3.6)

In this section, we introduce a lemma to prove (3.6) and we prove (3.6). Table 3.5 gives the definitions of intermediate variables which are used in this section.

Lemma to Prove (3.6)

Lemma 6 Define $\delta^{(r_j,r_\Sigma)}$ and $\delta^{(r_\Sigma,r_\Sigma)}$ as in Table 3.5. The intermediate variables are defined in Table 3.1. Define F and F' as in (3.7) and (3.8). For $j \in \bar{\mathcal{R}}$, the following equations hold.

$$\begin{aligned}
\delta^{(r_\Sigma,r_\Sigma)} =& -F\left(\frac{x'}{x}G_\Sigma - 1\right)^2 + F'G_\Sigma\left(\frac{x'}{x}G_\Sigma - 1\right) - \epsilon^2 G_\Sigma^2 \sum_{i\in\mathcal{L}} \lambda_i i y^{2i-2} + d_\mathrm{c}^2 \bar{r}_{d_\mathrm{c}}^2 \\
& - V_{d_\mathrm{c},d_\mathrm{c}}, \qquad (3.39)\\
\delta^{(r_j,r_\Sigma)} =& -F\left(\frac{x'}{x}G_\Sigma - 1\right)\left(\frac{x'}{x}G_j - I_{\{j=1\}}\right) + F'G_j\left(\frac{x'}{x}G_\Sigma - 1\right) - \epsilon^2 G_\Sigma G_j \sum_{i\in\mathcal{L}} \lambda_i i y^{2i-2} \\
& + d_\mathrm{c}\bar{r}_{d_\mathrm{c}} x G_j + V_{j,d_\mathrm{c}} + \frac{F'-x}{2}\big(G_j - I_{\{j=1\}}G_\Sigma\big) + I_{\{j=1\}} d_\mathrm{c}\bar{r}_{d_\mathrm{c}}(e-x). \qquad (3.40)
\end{aligned}$$

We use (3.39) to prove of the basis for the mathematical induction in the proof of (3.40). Similarly, we use (3.40) to prove of the basis for the mathematical induction in the proof of (3.6).

proof: Firstly, we derive the differential equations. We define $\delta^{(r_{d_\mathrm{c}},r_j)}$ as in Table 3.5. From (3.12), we get

$$\frac{d\delta^{(r_i,r_j)}}{dy} = -\frac{x'}{x}\left[i\delta^{(r_{i+1},r_j)} + j\delta^{(r_{j+1},r_i)} - (i+j)\delta^{(r_j,r_i)}\right] + D^{(r_i,r_j)}, \qquad (3.41)$$

where $D^{(r_i,r_j)}$ is defined in Table 3.5. From this equation, we have $\delta^{(r_i,r_j)}$ if $\delta^{(r_{i+1},r_j)}$ and $\delta^{(r_i,r_{j+1})}$ are known functions. Moreover, to solve $\delta^{(r_i,r_{d_\mathrm{c}-1})}$, we need to obtain $\delta^{(r_i,r_\Sigma)}$ and $\delta^{(r_{i+1},r_{d_\mathrm{c}-1})}$. From the sum of this equation over all $j \in \bar{\mathcal{R}}$, the differential equation for $\delta^{(r_i,r_\Sigma)}$ is written as follows:

$$\frac{d\delta^{(r_i,r_\Sigma)}}{dy} =-\frac{x'}{x}\Big[i\delta^{(r_{i+1},r_\Sigma)}-(d_\mathrm{c}+i)\delta^{(r_i,r_\Sigma)}\Big]-\frac{x'}{x}(d_\mathrm{c}-1)\delta^{(l_\Sigma,r_i)}+D^{(r_i,r_\Sigma)}.$$

Similarly, we see that to solve $\delta^{(r_i,r_\Sigma)}$, we need to obtain $\delta^{(r_{i+1},r_\Sigma)}$. Moreover, if we obtain $\delta^{(r_\Sigma,r_\Sigma)}$, we are able to solve $\delta^{(r_{d_\mathrm{c}-1},r_\Sigma)}$. The sum of this equation over all $i\in\bar{\mathcal{R}}$ is written as follows:

$$\frac{d\delta^{(r_\Sigma,r_\Sigma)}}{dy} =-2\frac{x'}{x}\big[(d_\mathrm{c}-1)\delta^{(l_\Sigma,r_\Sigma)}-d_\mathrm{c}\delta^{(r_\Sigma,r_\Sigma)}\big]+D^{(r_\Sigma,r_\Sigma)}. \tag{3.42}$$

Proof of (3.39) The solution of (3.42) is given by

$$\begin{aligned}\delta^{(r_\Sigma,r_\Sigma)} =&x^{2d_\mathrm{c}}\int\frac{1}{x^{2d_\mathrm{c}}}\Big[D^{(r_\Sigma,r_\Sigma)}-2(d_\mathrm{c}-1)\frac{x'}{x}\delta^{(l_\Sigma,r_\Sigma)}\Big]dy+x^{2d_\mathrm{c}}C_{r_\Sigma,r_\Sigma}\\ =&-F\left(\frac{x'}{x}G_\Sigma-1\right)^2+G_\Sigma\left(\frac{x'}{x}G_\Sigma-1\right)F'-\epsilon^2G_\Sigma^2\sum_{i\in\mathcal{L}}i\lambda_iy^{2i-2}+C_{r_\Sigma,r_\Sigma}x^{2d_\mathrm{c}},\end{aligned}$$

where C_{r_Σ,r_Σ} is a constant determined from the initial conditions. The initial conditions give

$$\delta^{(r_\Sigma,r_\Sigma)}(1) =\epsilon\tilde{\epsilon}\lambda'(1)(\epsilon^{d_\mathrm{c}-1}\rho_{d_\mathrm{c}}d_\mathrm{c}-1)^2+\epsilon\tilde{\epsilon}-2\epsilon^{d_\mathrm{c}}\tilde{\epsilon}\rho_{d_\mathrm{c}}d_\mathrm{c}+\epsilon^{d_\mathrm{c}}\rho_{d_\mathrm{c}}d_\mathrm{c}-\epsilon^{2d_\mathrm{c}}\rho_{d_\mathrm{c}}d_\mathrm{c}$$

and $C_{r_\Sigma,r_\Sigma}=\rho_{d_\mathrm{c}}^2d_\mathrm{c}^2-\rho_{d_\mathrm{c}}d_\mathrm{c}$. Thus, we obtain

$$\delta^{(r_\Sigma,r_\Sigma)} =-F\left(\frac{x'}{x}G_\Sigma-1\right)^2+G_\Sigma\left(\frac{x'}{x}G_\Sigma-1\right)F'-\epsilon^2G_\Sigma^2\sum_{i\in\mathcal{L}}\lambda_iiy^{2i-2}+d_\mathrm{c}^2r_{d_\mathrm{c}}^2-V_{d_\mathrm{c},d_\mathrm{c}}.$$

This leads to (3.39).

Proof of (3.40) In a way similar to Section 3.4.2, we find (3.40). (Q.E.D.)

Proof of (3.6)

(3.41) is solved as follows:

$$\delta^{(r_i,r_j)}=x^{i+j}\int\frac{1}{x^{i+j}}\left(D^{(r_i,r_j)}-i\frac{x'}{x}\delta^{(r_{i+1},r_j)}-j\frac{x'}{x}\delta^{(r_i,r_{j+1})}\right)dy+C_{r_i,r_j}x^{i+j}. \tag{3.43}$$

This equation is solved by mathematical induction for $i,j\in\bar{\mathcal{R}}\backslash\{1\}$. Firstly, we consider $\delta^{(r_j,r_{d_\mathrm{c}})}$ for $j\in\bar{\mathcal{R}}\setminus\{1\}$. From (3.5), $\delta^{(l_\Sigma,r_j)}$ is given by

$$\delta^{(l_\Sigma,r_j)}=a\frac{x'}{x}FG_j-F'G_j\left(a-\frac{1}{2}\right)-\frac{1}{2}xG_j+\epsilon^2G_j\sum_{s\in\mathcal{L}}\lambda_ssy^{2s-1}$$

Combining with this equation, the definition of $\delta^{(r_{d_c},r_j)}$ and (3.40), we have

$$\delta^{(r_j,r_{d_c})} = \delta^{(l_\Sigma,r_j)} - \delta^{(r_\Sigma,r_j)} = G_j G_{d_c}\left[-\frac{(x')^2}{x^2}F + \frac{x'}{x}F' - \epsilon^2\sum_{s\in\mathcal{L}}\lambda_s s y^{2s-2} + x^2\right] - V_{j,d_c},$$

for $j \in \bar{\mathcal{R}} \setminus \{1\}$. Hence, in the case for $\delta^{(r_{d_c-1},r_{d_c-1})}$, (3.43) is transformed to

$$\begin{aligned}\delta^{(r_{d_c-1},r_{d_c-1})} &= x^{2d_c-2}\int\frac{1}{x^{2d_c-2}}D^{(r_{d_c-1},r_{d_c-1})}dy - 2(d_c-1)x^{2d_c-2}\int\frac{x'}{x^{2d_c-1}}\delta^{(r_{d_c},r_{d_c-1})}dy\\ &\quad + C_{r_{d_c-1},r_{d_c-1}}x^{2d_c-2}\\ &= G_{d_c-1}^2\left[-\frac{(x')^2}{x^2}F + \frac{x'}{x}F' - \epsilon^2\sum_{s\in\mathcal{L}}\lambda_s s y^{2s-2} + x^2\right] - V_{d_c-1,d_c-1}\\ &\quad + (d_c-1)\bar{r}_{d_c-1} + C_{r_{d_c-1},r_{d_c-1}}x^{2d_c-2}.\end{aligned}$$

The initial condition gives $C_{r_{d_c-1},r_{d_c-1}} = 0$. Thus, we see that $\delta^{(r_{d_c-1},r_{d_c-1})}$ fulfills (3.6). We show that if all the elements in $\{\delta^{(r_i,r_j)} \mid i,j \in \bar{\mathcal{R}}\setminus\{1\}, i+j = k+1\}$ fulfill (3.6), then all the elements in $\{\delta^{(r_i,r_j)} \mid i,j \in \bar{\mathcal{R}}\setminus\{1\}, i+j = k\}$ fulfill (3.6). Using the induction hypothesis, we solve (3.43) as follows:

$$\begin{aligned}\delta^{(r_i,r_j)} &= G_i G_j\left[-\frac{(x')^2}{x^2}F + \frac{x'}{x}F' - \epsilon^2\sum_{s\in\mathcal{L}}\lambda_s s y^{2s-2} + x^2\right] - V_{i,j}\\ &\quad + I_{\{i=j\}} i \sum_{s\in\mathcal{R}}\rho_s\binom{s-1}{i-1}\left[x^i\tilde{x}^{s-i} - \binom{s-i}{i}x^i(-x)^i\right] + C_{r_i,r_j}x^{i+j}.\end{aligned}$$

The constant C_{r_i,r_j} is derived from the initial condition and given by

$$C_{r_i,r_j} = I_{\{i=j\}} i \sum_{s\in\mathcal{R}}\rho_s\binom{s-1}{i-1}\binom{s-i}{i}(-1)^i.$$

Thus, we have (3.6) for $i,j \in \bar{\mathcal{R}}\setminus\{1\}$.

Since $\delta^{(r_i,r_1)} = \delta^{(r_i,r_\Sigma)} - \sum_{j=2}^{d_c-1}\delta^{(r_i,r_j)}$, we show that $\delta^{(r_i,r_1)}$ fulfills (3.6) for $i \in \bar{\mathcal{R}}$. Hence we obtain (3.6).

3.5 Summary

In this chapter, we have analytically solved the covariance evolution for irregular LDPC code ensembles. We have also obtained the slope scaling parameter without assumptions.

Chapter 4

Analysis of Error Floors of Non-Binary LDPC Codes over Binary Erasure Channels

In this chapter, we investigate the error floors of the non-binary LDPC codes transmitted over the BEC under BP decoding. We propose a method to improve the decoding erasure rates in the error floors by optimizing labels in zigzag cycles in the Tanner graphs of codes. Furthermore, we give lower bounds on the bit and the symbol erasure rates in the error floors. The simulation results show that the presented lower bounds are tight for the codes designed by the proposed method.

4.1 Introduction

The error floors of non-binary LDPC codes decoded by the BP decoder are mainly caused by *nonzero* codewords or stopping constellations of small weight. We focus on nonzero codewords at first. A zigzag cycle is a cycle such that the degrees of all the variable nodes in the cycle are two. A zigzag cycle of weight w consists of w variable nodes of degree two. It is known that the set of variable nodes in a zigzag cycle forms a stopping set. For the binary LDPC codes, small zigzag cycles always yield nonzero codewords which result in serious degradation of the decoding performance. On the other hand, zigzag cycles in the non-binary codes do not always yield nonzero codewords. Let $H_q^{(w)}$ denote the submatrix over $\mathbb{F}_q$ corresponding to a zigzag cycle of weight w with labels $h_{1,1}, h_{1,2}, \dots, h_{w,w}, h_{w,1}$ in the Tanner graph. For example, the submatrix $H_q^{(4)}$ is written as

$$H_q^{(4)} = \begin{pmatrix} h_{1,1} & h_{1,2} & 0 & 0 \\ 0 & h_{2,2} & h_{2,3} & 0 \\ 0 & 0 & h_{3,3} & h_{3,4} \\ h_{4,1} & 0 & 0 & h_{4,4} \end{pmatrix}.$$

To simplify notation, we define $h_{w,w+1} := h_{w,1}$. The zigzag cycle corresponding to $H_q^{(w)}$ yields nonzero codeword iff $H_q^{(w)}$ is singular, i.e.,

$$\det H_q^{(w)} = \prod_{i=1}^{w} h_{i,i} + \prod_{i=1}^{w} h_{i,i+1} = 0,$$

which is equivalent to

$$\chi := \prod_{i=1}^{w} h_{i,i}^{-1} h_{i+1,i} = 1.$$

It can be seen that zigzag cycles in the Tanner graphs for the binary LDPC codes always yield nonzero codewords since $\det H_2^{(w)} = 0$. On the other hand, for the non-binary case, zigzag cycles in the Tanner graphs do not yield nonzero codewords if the corresponding submatrices are nonsingular.

To lower the error floors of codes under maximum likelihood decoding, Poulliat et al. proposed *cycle cancellation* [27]. The cycle cancellation is a method to design the edge labels in zigzag cycles so that the corresponding submatrices are nonsingular. We see that from the simulation result [27] the resulting codes have lower error floors under BP decoding. However, it is found in our analyses that some zigzag cycles, even if their submatrices are nonsingular, can cause decoding failures under BP decoding over the BEC, i.e., some zigzag cycles yield stopping constellations.

In this chapter, we analyze *nonsingular* zigzag cycles which cause the decoding failures under BP decoding. We clarify that the condition for successful decoding of zigzag cycles over the BEC depends on the parameter χ. More precisely, if the parameter χ is not a nonzero element of proper subfields of $\mathbb{F}_q$, the zigzag cycles do not yield stopping constellations. Based on this fact, we propose a design method of selecting labels so as to eliminate small zigzag cycles which yield stopping constellations.

For the binary LDPC code ensembles over the BEC, a closed-form expression for the bit erasure rate in the error floors was given in [5, p. 155]. However, for the non-binary LDPC code ensembles, no closed-form expressions or bounds for the bit and the symbol erasure rates in the error floors have been given. In this chapter, we give lower bounds on the bit and the symbol erasure rates in the error floors for the non-binary LDPC code ensembles. More precisely, those lower bounds are derived from the decoding erasures caused by the zigzag cycles. Furthermore, the simulation results show that the lower bounds on the bit and the symbol erasure rates are tight for the expurgated ensemble constructed by our proposed method over the BEC.

This chapter is organized as follows. In Section 4.2, we investigate BP decoding of zigzag cycles over the BEC and propose the improved cycle cancellation. In Section 4.3, we give lower bounds on the bit and the symbol erasure rates in the error floors for expurgated ensembles.

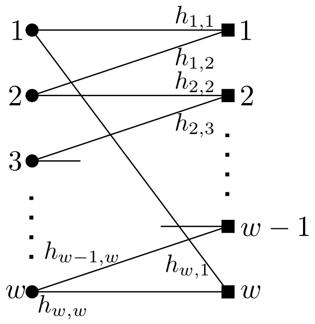

Figure 4.1: A zigzag cycle of weight w with labels $h_{1,1}, h_{2,1}, \dots, h_{w,w}, h_{w,1}$.

4.2 Zigzag Cycle Code Analysis

A zigzag cycle is a cycle such that the degrees of all the variable nodes in the cycle are two. The zigzag cycle code is defined by a Tanner graph which forms a single zigzag cycle as shown in Fig. 4.1. In this section, we investigate the zigzag cycle codes to clarify a condition for decoding failures on the zigzag cycles in Tanner graphs. We also show the decoding performance for zigzag cycle codes under BP decoding.

4.2.1 Condition for Successful Decoding

In the following theorem, we clarify a necessary condition for successful decoding of the zigzag cycle codes over the BEC by the BP decoder.

Theorem 2 Consider zigzag cycle codes of length w with labels $h_{1,1}, h_{1,2}, \dots, h_{w,w}, h_{w,1} \in \mathbb{F}_{2^m} \setminus \{0\}$ over the BEC. Let α be the primitive element of $\mathbb{F}_{2^m}$. Define

$$\mathcal{H}_m^* := \bigcup_{r>0:r|m,r\neq m} \Big\{\alpha^{i(2^m-1)/(2^r-1)} \mid i = 0, 1, \dots, 2^r - 2\Big\}. \tag{4.1}$$

All the symbols in a zigzag cycle code are correct unless all the bits are erased, if

$$\prod_{i=1}^{w} h_{i,i+1}^{-1} h_{i,i} = \chi \notin \mathcal{H}_m^*.$$

Specifically, $\{1\} = \mathcal{H}_m^* \subseteq \mathbb{F}_{2^m}$ for a prime m.

The proof of Theorem 2 shall be shown in Appendix 4.A. Note that $\{\alpha^{i(2^m-1)/(2^r-1)} \mid i = 0, 1, \dots, 2^r - 2\}$ forms the set of the nonzero elements of the proper subfield of order 2^r for $r \mid m$. In other words, $\mathcal{H}_m^*$ consists of the nonzero elements of the proper subfields of $\mathbb{F}_{2^m}$.

We refer to χ as the *cycle parameter* of the zigzag cycle code. Theorem 2 shows that the condition of successful decoding under BP decoding for the zigzag cycle codes over the BEC depends on the cycle parameter χ. In Table 4.1, we list the cycle parameters in $\mathcal{H}_m^* \subseteq \mathbb{F}_{2^m}$ for m = 4,6,8 and 9. It follows from Theorem 2 that it is desired to avoid the zigzag cycle codes

Table 4.1: The elements of $\mathcal{H}_m^*$ over $\mathbb{F}_{2^m}$ for $m = 4, 6, 8, 9$.

Field	The elements of $\mathcal{H}_m^*$
$\mathbb{F}_{2^4}$	$1, \alpha^5, \alpha^{10}$
$\mathbb{F}_{2^6}$	$1, \alpha^9, \alpha^{18}, \alpha^{21}, \alpha^{27}, \alpha^{36}, \alpha^{42}, \alpha^{45}, \alpha^{54}$
$\mathbb{F}_{2^8}$	$1, \alpha^{17}, \alpha^{34}, \alpha^{51}, \alpha^{68}, \alpha^{85}, \alpha^{102}, \alpha^{119}, \alpha^{136}, \alpha^{153}, \alpha^{170}, \alpha^{187}, \alpha^{204}, \alpha^{221}, \alpha^{238}$
$\mathbb{F}_{2^9}$	$1, \alpha^{73}, \alpha^{146}, \alpha^{219}, \alpha^{292}, \alpha^{365}, \alpha^{438}$

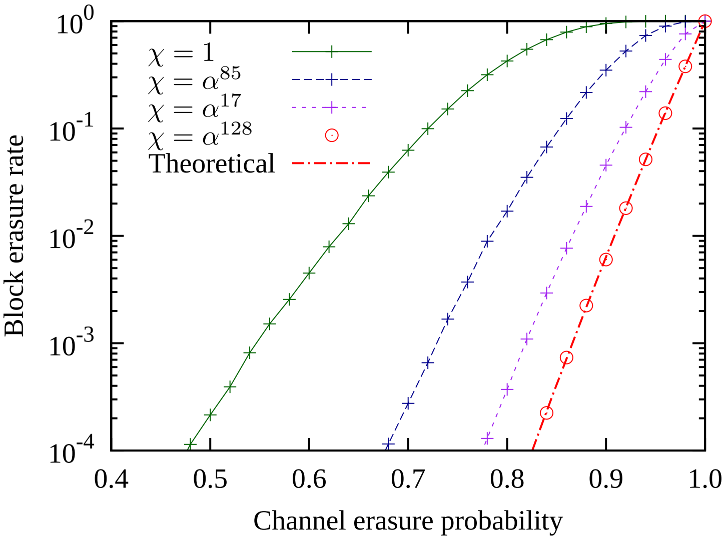

Figure 4.2: The block erasure rates for zigzag cycle codes with the cycle parameter $\chi = 1, \alpha^{85}, \alpha^{17}, \alpha^{128}$ over the BEC under BP decoding. The zigzag cycle codes are of weight 6 over $\mathbb{F}_{2^8}$. Let ϵ be the channel erasure probability. The solid curve shows the theoretical block erasure rate ϵ^{48} of zigzag cycle codes with the cycle parameter $\chi \notin \mathcal{H}_8^*$.

with the cycle parameter $\chi \in \mathcal{H}_m^*$, since those codes can cause decoding failures even if not all the bits are erased.

We propose an *improved cycle cancellation* to get lower error floors. The improved cycle cancellation is a method to design the labels in Tanner graphs so that zigzag cycles of small weight satisfy $\chi \notin \mathcal{H}_m^*$. The zigzag cycles designed by the improved cycle cancellation are successfully decoded under BP decoding unless all the bits are erased. Hence, zigzag cycles designed by the improved cycle cancellation recover more erasures than those designed by the cycle cancellation [27].

We compare the block erasure rates of zigzag cycle codes designed by the improved cycle cancellation with that of zigzag cycle codes satisfying $\chi \in \mathcal{H}_m^*$ in Section 4.2.2.

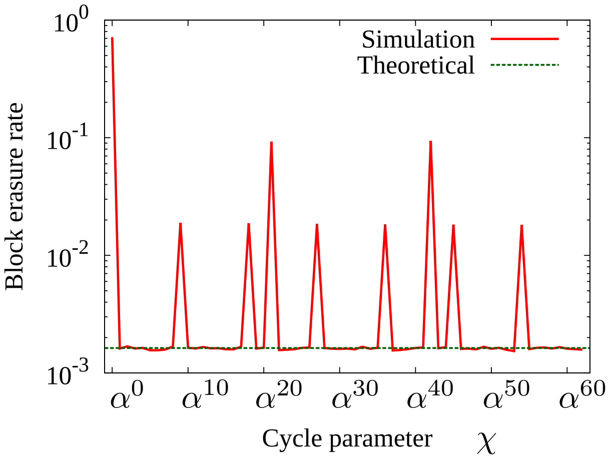

Figure 4.3: The block erasure rates for zigzag cycle codes over the BEC with channel erasure probability 0.7 under BP decoding. The zigzag cycle codes are weight 3 over $\mathbb{F}_{2^6}$. We see that the zigzag cycle codes with the cycle parameter $\chi \notin \mathcal{H}_6^*$ exhibit good decoding performance, where $\mathcal{H}_6^* = \{1, \alpha^9, \alpha^{18}, \alpha^{21}, \alpha^{27}, \alpha^{36}, \alpha^{42}, \alpha^{45}, \alpha^{54}\}$.

4.2.2 Simulation Results

Figure 4.2 shows the block erasure rates of zigzag cycle codes over the BEC under BP decoding. Each curve of $\chi = \alpha^j$ in Fig. 4.2 shows the block erasure rates of zigzag cycle codes of weight 6 over $\mathbb{F}_{2^8}$ with the cycle parameter $\chi = 1, \alpha^{17}, \alpha^{85} \in \mathcal{H}_8^*$. The circles in Fig. 4.2 show the block erasure rate of zigzag cycles with the cycle parameter $\chi = \alpha^{128} \notin \mathcal{H}_8^*$.

The solid curve in Fig. 4.2 shows the theoretical block erasure rate of zigzag cycle codes with the cycle parameter $\chi \notin \mathcal{H}_8^*$. A zigzag cycle code is *recoverable* if all the symbols in the zigzag cycle code are correct by the BP decoder. The zigzag cycle codes with the cycle parameter $\chi \notin \mathcal{H}_8^*$ are recoverable unless all the bits are erased. All the bits are erased with probability ϵ^{48} for the BEC with channel erasure probability ϵ since the bit code length is 6 symbols or equivalently 6×8=48 bits. Hence, the theoretical block erasure rate of zigzag cycle codes designed by the improved cycle cancellation is given by ϵ^{48}.

The cycle cancellation avoids only the zigzag cycles with the cycle parameter $\chi = 1$. In other words, the cycle cancellation cannot avoid the zigzag cycles with the cycle parameter $\chi = \alpha^{17}$ and $\chi = \alpha^{85}$. On the other hand, the improved cycle cancellation avoids the zigzag cycles with the cycle parameter not only $\chi = 1$ but also $\chi = \alpha^{17}$ and $\chi = \alpha^{85}$ since $1, \alpha^{17}, \alpha^{85} \in \mathcal{H}_8^*$.

The smallest stopping state is defined in Appendix 4.A.3. The smallest stopping state containing 1 for $\chi = \alpha^{85}$ is given by $\{0, 1, \alpha^{85}, \alpha^{170}\}$. Then, the cardinality of this stopping state is 4. On the other hand, the smallest stopping state containing 1 for $\chi = \alpha^{17}$ is given by $\{0\} \cup \{\alpha^{17i} \mid i = 0, 1, \ldots, 14\}$. Then, the cardinality of this stopping state is 16. We see that from Fig. 4.2 the block erasure rate increases as the cardinality of the smallest stopping state decreases.

Figure 4.3 shows the block erasure rates of zigzag cycle codes over the BEC with channel erasure probability 0.7 under BP decoding. The zigzag cycle codes are weight 3 over $\mathbb{F}_{2^6}$. From Fig. 4.3, we see that the zigzag cycle codes with the cycle parameter $\chi \notin \mathcal{H}_6^*$ exhibit good decoding performance.

4.3 Error Floor Analysis

From Theorem 2, we see that no zigzag cycles designed by the improved cycle cancellation are recoverable iff all the bits in the zigzag cycles are erased. From Appendix 4.A.2, we see that all the zigzag cycles are not recoverable if all the bits are erased. By using this result, in this section, we give lower bounds on the bit and the symbol erasure rates under BP decoding for an expurgated ensembles. More precisely, those lower bounds are derived from the decoding erasures caused by the zigzag cycles. Simulation results show that those lower bounds are tight bounds on the bit and the symbol erasure rates in the error floors for the expurgated ensembles designed by our proposed method.

4.3.1 Code Ensemble

Since all the neighbors of the set $\mathcal{Z}$ of the variable nodes in a zigzag cycle are connected to $\mathcal{Z}$ exactly twice, the set $\mathcal{Z}$ of the variable nodes in a zigzag cycle forms a stopping set.

To analyze the bit and the symbol erasure rates in the error floors of the non-binary LDPC codes, we consider the following expurgated ensemble.

Definition 3 Recall that $\mathrm{EGF}(N, \mathbb{F}_{2^m}, \lambda, \rho)$ denote the non-binary LDPC code ensemble over $\mathbb{F}_{2^m}$. Let $w_{\mathrm{g}} \in \mathbb{N} \setminus \{1\}$ be an expurgation parameter. The expurgated ensemble $\mathrm{ELDPC}(N, \mathbb{F}_{2^m}, \lambda, \rho, w_{\mathrm{g}})$ consists of the subset of codes in $\mathrm{EGF}(N, \mathbb{F}_{2^m}, \lambda, \rho)$ which contain no stopping sets of size in $\{1, \dots, w_{\mathrm{g}} - 1\}$. Note that the expurgated ensemble $\mathrm{ELDPC}(N, \mathbb{F}_{2^m}, \lambda, \rho, 1)$ is equivalent to $\mathrm{EGF}(N, \mathbb{F}_{2^m}, \lambda, \rho)$. Let $w_{\mathrm{c}} \in \mathbb{N}$ be an expurgation parameter for labeling in the Tanner graph, where $w_{\mathrm{g}} < w_{\mathrm{c}}$. Define expurgated ensemble $\mathrm{ELDPC}(N, \mathbb{F}_{2^m}, \lambda, \rho, w_{\mathrm{g}}, w_{\mathrm{c}}, \mathcal{H})$ as the subset of codes in $\mathrm{ELDPC}(N, \mathbb{F}_{2^m}, \lambda, \rho, w_{\mathrm{g}})$ which contain no zigzag cycles of weight in $\{w_{\mathrm{g}}, \dots, w_{\mathrm{c}} - 1\}$ with the cycle parameter $\chi \in \mathcal{H}$.

Since the sets of the variable nodes in zigzag cycles form stopping sets, the codes in the expurgated ensemble $\mathrm{ELDPC}(N, m, \lambda, \rho, w_{\mathrm{g}})$ contain no zigzag cycles of weight in $\{1, 2, \dots, w_{\mathrm{g}} - 1\}$.

Example 8 The codes in the expurgated ensemble $\mathrm{ELDPC}(N, \mathbb{F}_{2^m}, \lambda, \rho, w_{\mathrm{g}}, w_{\mathrm{c}}, \{1\})$ contain no stopping sets of size in $\{1, 2, \dots, w_{\mathrm{g}} - 1\}$ and no zigzag cycles with the cycle parameter $\chi = 1$ of weight in $\{w_{\mathrm{g}}, \dots, w_{\mathrm{c}} - 1\}$. In other words, the expurgated ensemble $\mathrm{ELDPC}(N, \mathbb{F}_{2^m}, \lambda, \rho, w_{\mathrm{g}}, w_{\mathrm{c}}, \{1\})$ is constructed by the cycle cancellation. Since the sets of the variable nodes in zigzag cycles form stopping sets, the codes in $\mathrm{ELDPC}(N, \mathbb{F}_{2^m}, \lambda, \rho, w_{\mathrm{g}}, w_{\mathrm{c}}, \{1\})$ contain no zigzag cycles of weight in $\{1, 2, \dots, w_{\mathrm{g}} - 1\}$.

Recall that $\mathcal{H}_m^*$ is defined as in (4.1). Similarly, the expurgated ensemble $\mathrm{ELDPC}(N, \mathbb{F}_{2^m}, \lambda, \rho, w_{\mathrm{g}}, w_{\mathrm{c}}, \mathcal{H}_m^*)$ is constructed by the improved cycle cancellation.

4.3.2 Analysis of Error Floors

The following theorem gives lower bounds on the bit and the symbol erasure rates under BP decoding for the expurgated ensemble ELDPC$(N, \mathbb{F}_{2^m}, \lambda, \rho, w_{\mathrm{g}}, w_{\mathrm{c}}, \mathcal{H}_m^*)$.

Theorem 3 Let $P_{\mathrm{b}}(N, \mathbb{F}_{2^m}, \lambda, \rho, w_{\mathrm{g}}, w_{\mathrm{c}}, \mathcal{H}_m^*, \epsilon)$ and $P_{\mathrm{s}}(N, \mathbb{F}_{2^m}, \lambda, \rho, w_{\mathrm{g}}, w_{\mathrm{c}}, \mathcal{H}_m^*, \epsilon)$ be the bit and the symbol erasure rates, respectively, for the expurgated ensemble ELDPC$(N, \mathbb{F}_{2^m}, \lambda, \rho, w_{\mathrm{g}}, w_{\mathrm{c}}, \mathcal{H}_m^*)$ by the BP decoder over the BEC with channel erasure probability ϵ. Define $\mu := \lambda'(0)\rho'(1)$ and

$$\epsilon_m^* := \begin{cases} 1, & \mu \leq 1, \\ \mu^{-\frac{1}{m}}, & \mu > 1. \end{cases} \tag{4.2}$$

For sufficiently large N, the bit and the symbol erasure rates for $\mu > 0$ and $\epsilon < \epsilon_m^*$ are bounded by

$$P_{\mathrm{b}}(N, \mathbb{F}_{2^m}, \lambda, \rho, w_{\mathrm{g}}, w_{\mathrm{c}}, \mathcal{H}_m^*, \epsilon) \geq \frac{1}{2N} \frac{(\mu\epsilon^m)^{w_{\mathrm{g}}}}{1-\mu\epsilon^m} + o\left(\frac{1}{N}\right), \tag{4.3}$$

$$P_{\mathrm{s}}(N, \mathbb{F}_{2^m}, \lambda, \rho, w_{\mathrm{g}}, w_{\mathrm{c}}, \mathcal{H}_m^*, \epsilon) \geq \frac{1}{2N} \frac{(\mu\epsilon^m)^{w_{\mathrm{g}}}}{1-\mu\epsilon^m} + o\left(\frac{1}{N}\right). \tag{4.4}$$

proof: First, we will consider the symbol erasure rate. The symbol erasure rate is represented by the sum of two contributions, the symbol erasures caused by the stopping constellations from the zigzag cycles and from the stopping sets other than the zigzag cycles[1]. Let $\tilde{P}_{\mathrm{z}}(N, \mathbb{F}_{2^m}, \lambda, \rho, w_{\mathrm{g}}, w_{\mathrm{c}}, \mathcal{H}_m^*, \epsilon)$ and $\tilde{P}_{\mathrm{ss}}(N, \mathbb{F}_{2^m}, \lambda, \rho, w_{\mathrm{g}}, w_{\mathrm{c}}, \mathcal{H}_m^*, \epsilon)$ be the contributions of the zigzag cycles and of the stopping sets other than the zigzag cycles, respectively, for the symbol erasure rates of the ensemble ELDPC$(N, \mathbb{F}_{2^m}, \lambda, \rho, w_{\mathrm{g}}, w_{\mathrm{c}}, \mathcal{H}_m^*)$ over the BEC with channel erasure probability ϵ. Then, we have

$$\begin{aligned} P_{\mathrm{s}}(N, \mathbb{F}_{2^m}, &\lambda, \rho, w_{\mathrm{g}}, w_{\mathrm{c}}, \mathcal{H}_m^*, \epsilon) \\ &= \tilde{P}_{\mathrm{z}}(N, \mathbb{F}_{2^m}, \lambda, \rho, w_{\mathrm{g}}, w_{\mathrm{c}}, \mathcal{H}_m^*, \epsilon) + \tilde{P}_{\mathrm{ss}}(N, \mathbb{F}_{2^m}, \lambda, \rho, w_{\mathrm{g}}, w_{\mathrm{c}}, \mathcal{H}_m^*, \epsilon) \\ &\geq \tilde{P}_{\mathrm{z}}(N, \mathbb{F}_{2^m}, \lambda, \rho, w_{\mathrm{g}}, w_{\mathrm{c}}, \mathcal{H}_m^*, \epsilon). \end{aligned}$$

In words, the symbol erasure rate is lower bounded by the contribution of the zigzag cycles for the symbol erasure rate.

We will consider $\tilde{P}_{\mathrm{z}}(N, \mathbb{F}_{2^m}, \lambda, \rho, w_{\mathrm{g}}, w_{\mathrm{c}}, \mathcal{H}_m^*, \epsilon)$. Let $\tilde{P}_{1}(N, w, \mathbb{F}_{2^m}, \lambda, \rho, w_{\mathrm{g}}, w_{\mathrm{c}}, \mathcal{H}_m^*, \epsilon)$ be the symbol erasure rate caused by the stopping constellations from zigzag cycles of weight w under BP decoding over the BEC with channel erasure probability ϵ for ELDPC$(N, \mathbb{F}_{2^m}, \lambda, \rho, w_{\mathrm{g}}, w_{\mathrm{c}}, \mathcal{H}_m^*)$. From Definition 3, codes in the expurgated ensemble ELDPC$(N, \mathbb{F}_{2^m}, \lambda, \rho, w_{\mathrm{g}}, w_{\mathrm{c}}, \mathcal{H}_m^*)$ contain no zigzag cycles of weight in $\{1, 2, \ldots, w_{\mathrm{g}} - 1\}$. Hence, we consider the symbol erasure rate caused by stopping constellation from zigzag cycles of weight

[1] For a fixed Tanner graph and a given stopping set $\mathcal{S}$, there exist at least one stopping constellation $\{E_v\}_{v \in [1,N]}$ such that the set of variable nodes in $\{v \mid E_v \neq \{0\}\}$ is $\mathcal{S}$ from Lemma 3. In this proof, we refer to those stopping constellations as stopping constellations from stopping set $\mathcal{S}$.

at least w_{g}. If we fix a finite W and let N tend to infinity, the zigzag cycles of weight at most W become asymptotically non-overlapping with high probability [5, p. 155]. Thus, for a fixed W and sufficiently large N we have

$$\tilde{P}_{\mathrm{z}}(N, \mathbb{F}_{2^m}, \lambda, \rho, w_{\mathrm{g}}, w_{\mathrm{c}}, \mathcal{H}_m^*, \epsilon) \geq \sum_{w=w_{\mathrm{g}}}^{W} \tilde{P}_1(N, w, \mathbb{F}_{2^m}, \lambda, \rho, w_{\mathrm{g}}, w_{\mathrm{c}}, \mathcal{H}_m^*, \epsilon).$$

In Section 4.2.2, zigzag cycle codes designed by the improved cycle cancellation can not be recovered iff all the bits are erased. From this result, we see that zigzag cycles with the cycle parameter $\chi \notin \mathcal{H}_m^*$ in a Tanner graph can not be recovered iff all the bits in the cycle are erased, which happens with probability ϵ^{mw}. In other words, symbols in zigzag cycles of weight $w \in \{w_{\mathsf{g}}, \ldots, w_{\mathsf{c}} - 1\}$ are not recovered with probability ϵ^{mw}. From Appendix 4.A.2, no symbols in the zigzag cycle of weight w with the cycle parameter $\chi \in \mathcal{H}_m^*$ are correct if all the bits in the zigzag cycle are erased. Hence, all the zigzag cycles are not recovered with probability at least ϵ^{mw}. In other words, the zigzag cycles of weight $w \in \{w_{\mathsf{c}}, \ldots, W\}$ are not recovered with probability at least ϵ^{mw}. By [5, C. 37] for a fixed W, the expectation of the number of zigzag cycles of weight $w \leq W$ in the expurgated ensemble ELDPC$(N, \mathbb{F}_{2^m}, \lambda, \rho, s_{\mathrm{g}}, s_{\mathrm{c}}, \mathcal{H}_m^*)$ is given by

$$\frac{\mu^w}{2w},$$

for sufficiently large N. From Appendix 4.A.3, if all the bits in the zigzag cycle are erased, no symbols in zigzag cycle are correct. Hence, iff all the bits in the zigzag cycle of weight w are erased, the zigzag cycle causes w symbol erasures. Since w symbols are in the zigzag cycles of weight w, the zigzag cycles of weight w cause a symbol erasure rate of w/N if the bits in the zigzag cycles of weight w are erased. Therefore, for sufficiently large N, we have for $w \in \{w_{\mathsf{g}}, \ldots, w_{\mathsf{c}} - 1\}$,

$$\tilde{P}_1(N, w, \mathbb{F}_{2^m}, \lambda, \rho, w_{\mathrm{g}}, w_{\mathrm{c}}, \mathcal{H}_m^*, \epsilon) = \frac{1}{2N} \mu^w \epsilon^{mw} + o\left(\frac{1}{N}\right),$$

and for $w \in \{w_{\mathsf{c}}, \ldots, W\}$

$$\tilde{P}_1(N, w, \mathbb{F}_{2^m}, \lambda, \rho, w_{\mathrm{g}}, w_{\mathrm{c}}, \mathcal{H}_m^*, \epsilon) \geq \frac{1}{2N} \mu^w \epsilon^{mw} + o\left(\frac{1}{N}\right).$$

Thus, we have

$$\tilde{P}(N, \mathbb{F}_{2^m}, \lambda, \rho, w_{\mathrm{g}}, w_{\mathrm{c}}, \mathcal{H}_m^*, \epsilon) \geq \frac{1}{2N} \sum_{w=w_{\mathrm{g}}}^{W} \mu^w \epsilon^{mw} + o\left(\frac{1}{N}\right).$$

If $\epsilon < \epsilon_m^*$, for sufficiently large N and W, we see that

$$\tilde{P}(N, \mathbb{F}_{2^m}, \lambda, \rho, w_{\mathrm{g}}, w_{\mathrm{c}}, \mathcal{H}_m^*, \epsilon) \geq \frac{1}{2N} \frac{(\mu \epsilon^m)^{s_{\mathrm{g}}}}{1 - \mu \epsilon^w} + o\left(\frac{1}{N}\right).$$

Hence, for sufficiently large N, the symbol decoding erasure rate is bounded by

$$\mathrm{P}_{\mathrm{s}}(N, \mathbb{F}_{2^m}, \lambda, \rho,_{\mathrm{g}}, w_{\mathrm{c}}, \mathcal{H}_m^*, \epsilon) \geq \frac{1}{2N} \frac{(\mu\epsilon^m)^{w_{\mathrm{g}}}}{1-\mu\epsilon^w} + o\left(\frac{1}{N}\right).$$

We will consider the bit erasure rate. The proof is similar to the proof for the symbol erasure rate. From Appendix 4.A.3, if all the bits in the zigzag cycle are erased, all the states of the variable nodes in the zigzag cycle are equal to $\mathbb{F}_{2^m}$. Hence, if all the bits in the zigzag cycle are erased, no bits in the zigzag cycle are correct. Note that the bit code length is Nm. Since mw bits are in the zigzag cycles of weight w, the zigzag cycles of weight w cause a bit erasure rate of w/N if all the bits in the zigzag cycles of weight w are erased. Thus, the bit erasure rate caused by zigzag cycles is lower bounded by

$$\frac{1}{2N} \sum_{w=w_{\mathrm{g}}}^{W} \mu^w \epsilon^{mw} + o\left(\frac{1}{N}\right).$$

By using this result, we obtain a lower bound on the bit erasure rate for the expurgated ensemble similarly. (Q.E.D.)

Discussion 5 Since the symbol and the bit erasure rates of all the zigzag cycles of weight w are lower bounded by ϵ^{mw}, the bit and the symbol erasure rates do not depend on the parameter w_{c} and the subset $\mathcal{H}_m^*$. Hence, (4.3) and (4.4) do not depend on the parameter w_{c} and the subset $\mathcal{H}_m^*$.

4.3.3 Simulation Results

Figure 4.4 compares the symbol erasure rate for the expurgated ensemble constructed by the improved cycle cancellation ELDPC$(315, \mathbb{F}_{2^4}, x, x^2, 1, 8, \mathcal{H}_4^*)$ with that for the expurgated ensemble constructed by the cycle cancellation ELDPC$(315, \mathbb{F}_{2^4}, x, x^2, 1, 8, \{1\})$, where $\mathcal{H}_4^* = \{1, \alpha^5, \alpha^{10}\}$. It can be seen that our proposed codes exhibit a better decoding performance than codes designed by the cycle cancellation. Figure 4.4 also shows the lower bound on the symbol erasure rate which is given by (4.4). We see that (4.4) is a tight lower bound on the symbol erasure rate for the expurgated ensemble ELDPC$(315, \mathbb{F}_{2^4}, x, x^2, 1, 8, {\mathcal{H}_4}^*)$ in the error floor.

Figure 4.5 compares the symbol erasure rate for the expurgated ensemble constructed by the improved cycle cancellation ELDPC$(600, \mathbb{F}_{2^4}, x, x^2, 2, 12, \mathcal{H}_4^*)$ with that for the expurgated ensemble constructed by the cycle cancellation ELDPC$(600, \mathbb{F}_{2^4}, x, x^2, 2, 12, \{1\})$. The lower bound on the symbol erasure rate is given by (4.4). This is the case for $w_{\mathsf{g}} \geq 2$. Figure 4.6 compares the symbol erasure rate for the expurgated ensemble constructed by the improved cycle cancellation ELDPC$(2000, \mathbb{F}_{2^4}, \lambda, \rho, 1, 8, \mathcal{H}_4^*)$ with that for the expurgated ensemble constructed by the cycle cancellation ELDPC$(2000, \mathbb{F}_{2^4}, \lambda, \rho, 1, 8, \{1\})$ where $\lambda = 0.5x + 0.5x^2$ and $\rho = 0.5x^3 + 0.5x^5$. The lower bound on the symbol erasure rate is given by (4.4). This is the case for an irregular non-binary LDPC code ensemble. From Fig. 4.5 and 4.6, we see that (4.4) is a tight lower bound on the symbol erasure rate of the expurgated ensemble constructed by the

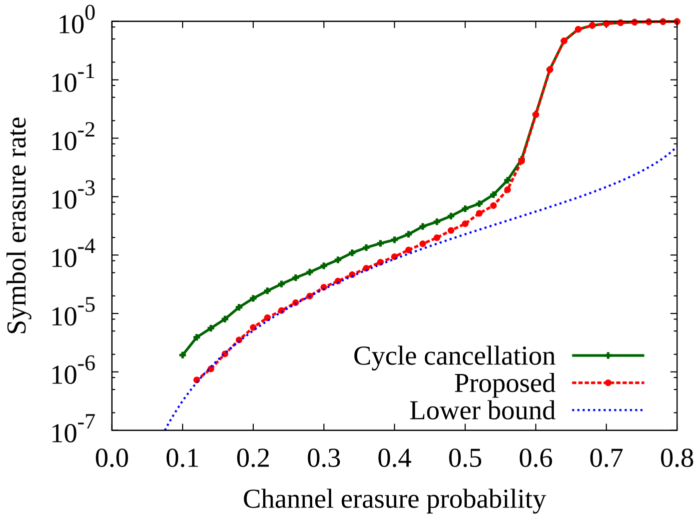

Figure 4.4: Comparison of the symbol erasure rate for the expurgated ensemble $\mathrm{ELDPC}(315, \mathbb{F}_{2^4}, x, x^2, 1, 8, \mathcal{H}_4^*)$ (proposed) with that for the expurgated ensemble $\mathrm{ELDPC}(315, \mathbb{F}_{2^4}, x, x^2, 1, 8, \{1\})$ (cycle cancellation). The lower bound is given by (4.4). It can be seen that our proposed codes exhibit a better decoding performance than the cycle cancellation. It can be seen that (4.4) is a tight lower bound on the symbol erasure rate for the expurgated ensemble $\mathrm{ELDPC}(315, \mathbb{F}_{2^4}, x, x^2, 1, 8, \mathcal{H}_4^*)$ for small ϵ.

improved cycle cancellation in the error floor and our proposed codes exhibit a better decoding performance than codes designed by the cycle cancellation.

Figure 4.7 compares the bit erasure rate for the expurgated ensemble constructed by the improved cycle cancellation $\mathrm{ELDPC}(315, \mathbb{F}_{2^4}, x, x^2, 1, 8, \mathcal{H}_4^*)$ with that for the expurgated ensemble constructed by the cycle cancellation $\mathrm{ELDPC}(315, \mathbb{F}_{2^4}, x, x^2, 1, 8, \{1\})$. It can be seen that our proposed codes exhibit a better decoding performance than codes designed by the cycle cancellation. Figure 4.7 also shows the lower bound on the bit erasure rate which is given by (4.3). We see that (4.3) is a tight lower bound on the bit erasure rate for the expurgated ensemble $\mathrm{ELDPC}(315, \mathbb{F}_{2^4}, x, x^2, 1, 8, \mathcal{H}_4^*)$ in the error floor.

4.3.4 Monotonicity of Error Floor

In Section 4.3.3, we see that the lower bound given by (4.3) is a tight lower bound on the bit erasure rate in the error floor for the expurgated ensemble constructed by the improved cycle cancellation. It is empirically known that the error floors for the non-binary LDPC codes decrease as the size of Galois field increases [13]. In this subsection, we show the monotonicity of the error floor by using the lower bound given by (4.3).

Let n be the bit code length, i.e., $n = mN$. From (4.3), we have

$$\lim_{n\to\infty} n\mathrm{P}_{\mathrm{b}}(n, \mathbb{F}_{2^m}, \lambda, \rho, w_{\mathrm{g}}, w_{\mathrm{c}}, \mathcal{H}_m^*, \epsilon) \geq \frac{m}{2}\frac{(\mu\epsilon^m)^{w_{\mathrm{g}}}}{1-\mu\epsilon^m} =: f(m, \epsilon, w_{\mathrm{g}}). \tag{4.5}$$

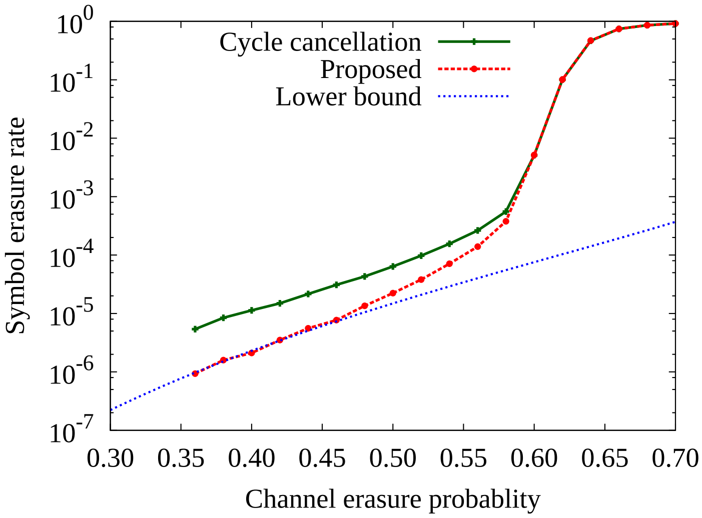

Figure 4.5: Comparison of the symbol erasure rate for the expurgated ensemble $\mathrm{ELDPC}(600, \mathbb{F}_{2^4}, x, x^2, 2, 12, \mathcal{H}_4^*)$ (proposed) with that for the expurgated ensemble $\mathrm{ELDPC}(600, \mathbb{F}_{2^4}, x, x^2, 2, 12, \{1\})$ (cycle cancellation). The lower bound is given by (4.4). This is the case for $w_g > 1$.

The following lemma shows that for a fixed large bit code length, the lower bound on the bit erasure rate is decreasing in m, i.e., $f(m, \epsilon, w_\mathrm{g})$ is decreasing in m.

Lemma 7 Define $f(m, \epsilon, w_\mathrm{g})$ as in (4.5). Define ϵ_m^* as in (4.2). Then $f(m, \epsilon, w_\mathrm{g}) > f(m + 1, \epsilon, w_\mathrm{g})$ for $\mu \geq 1$ and $0 < \epsilon < \min\{\epsilon_m^*, \epsilon_{m+1}^*\} = \epsilon_m^*$.

Proof: From (4.5), we have

$$f(m, \epsilon, w_\mathrm{g}) - f(m + 1, \epsilon, w_\mathrm{g}) = \frac{(\mu\epsilon^m)^{w_\mathrm{g}} g(m, \epsilon, w_\mathrm{g})}{2(1 - \mu\epsilon^{m+1})(1 - \mu\epsilon^m)},$$

where

$$g(m, \epsilon, w_\mathrm{g}) := m(1 - \mu\epsilon^{m+1}) - (m + 1)\epsilon^{w_\mathrm{g}}(1 - \mu\epsilon^m).$$

For $\epsilon < \epsilon_m^*$, $g(m, \epsilon, w_\mathrm{g})$ is increasing in w_g. Hence, we have $g(m, \epsilon, w_\mathrm{g}) \geq g(m, \epsilon, 1)$. For $\epsilon < \epsilon_m^*$, $g(m, \epsilon, 1)$ is decreasing in ϵ. Note that $\min\{\epsilon_m^*, \epsilon_{m+1}^*\} < \mu^{-\frac{1}{m}}$. Thus, we see that for $\epsilon < \mu^{-\frac{1}{m}}$ and $\mu \geq 1$

$$g(m, \epsilon, w_\mathrm{g}) \geq g(m, \epsilon, 1) > g(m, \mu^{-\frac{1}{m}}, 1) = m(1 - \mu^{-\frac{1}{m}}) > 0.$$

Therefore, we have $f(m + 1, \epsilon, w_\mathrm{g}) - f(m, \epsilon, w_\mathrm{g}) < 0$ for $\mu \geq 1$ and $0 < \epsilon < \min\{\epsilon_m^*, \epsilon_{m+1}^*\}$. (Q.E.D)

Figure 4.8 shows curves given by (4.5) for $\mu = 2$, $w_\mathrm{g} = 1$ and $m = 1, 2, \ldots, 9$. We see that the lower bound decreases as the order of the Galois field increases.

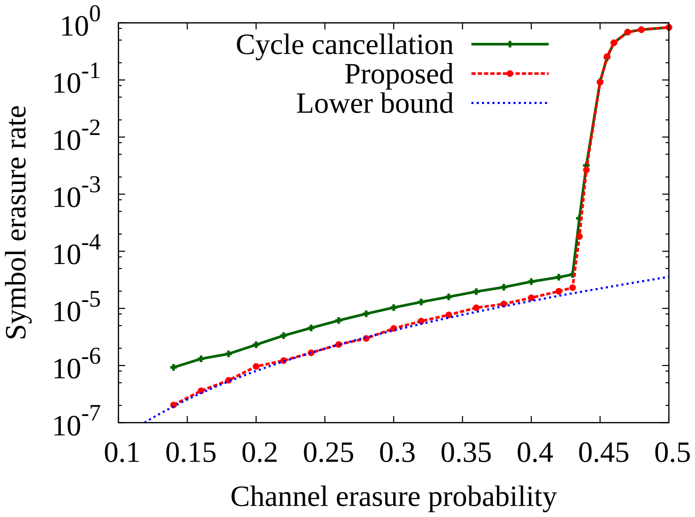

Figure 4.6: Comparison of the symbol erasure rate for the expurgated ensemble $\mathrm{ELDPC}(2000, \mathbb{F}_{2^4}, \lambda, \rho, 1, 8, \mathcal{H}_4^*)$ (proposed) with that for the expurgated ensemble $\mathrm{ELDPC}(2000, \mathbb{F}_{2^4}, \lambda, \rho, 1, 8, \{1\})$ (cycle cancellation), where $\lambda = 0.5x + 0.5x^2$ and $\rho = 0.5x^3 + 0.5x^5$. The lower bound is given by (4.4). This is the case for an irregular LDPC code ensemble case.

4.4 Summary

In this chapter, we have proposed a method to improve the error floors for the non-binary LDPC codes which contain the variable nodes of degree two over the BEC under BP decoding. We have derived lower bounds on the bit and the symbol erasure rates in the error floors for the expurgated ensembles under BP decoding. From the simulation results, the lower bounds are tight for the bit and the symbol erasure rates for the expurgated ensembles constructed by the proposed method over the BEC under BP decoding.

Appendix 4.A Proof of Theorem 2

In this section, we prove Theorem 2. To prove Theorem 2, we give several lemmas in the following sections.

4.A.1 Analysis of Stopping Constellation for Zigzag Cycle Codes

Consider zigzag cycle codes of weight w with labels $h_{1,1}, h_{1,2}, \dots, h_{w,w}, h_{w,1} \in \mathbb{F}_{2^m} \setminus \{0\}$ as depicted in Fig. 4.1. Let $E_1, \dots, E_w \subseteq \mathbb{F}_{2^m}$ be the states of the variable nodes.

Lemma 8 For any zigzag cycles of weight w with labels $h_{1,1}, h_{1,2}, \dots, h_{w,w}, h_{w,1} \in \mathbb{F}_{2^m} \setminus \{0\}$, an assignment of states $\{E_i\}_{i=1}^{w}$ forms a stopping constellation if and only if for $i = 1, \dots, w$:

$$E_i = h_{i,i}^{-1} h_{i+1,i} E_{i+1}, \qquad E_i = h_{i-1,i}^{-1} h_{i-1,i-1} E_{i-1},$$

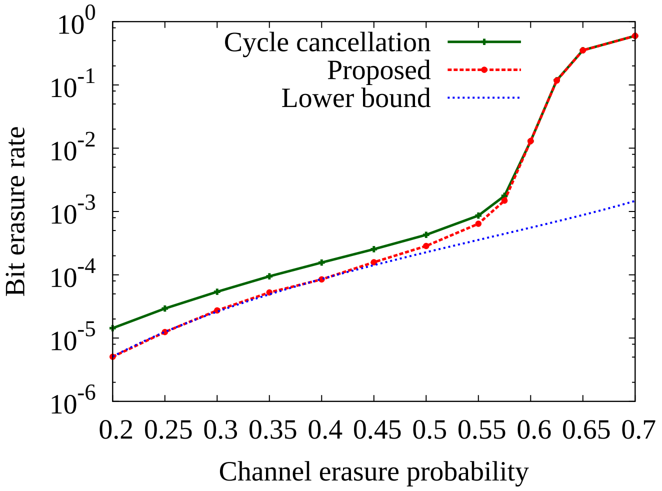

Figure 4.7: Comparison of the bit erasure rate for the expurgated ensemble ELDPC$(315, \mathbb{F}_{2^4}, x, x^2, 1, 8, \mathcal{H}_4^*)$ (proposed) with that for the expurgated ensemble ELDPC$(315, \mathbb{F}_{2^4}, x, x^2, 1, 8, \{1\})$ (cycle cancellation). The lower bound is given by (4.3). It can be seen that our proposed codes exhibit a better decoding performance than the cycle cancellation. It can be seen that (4.3) is a tight lower bound on the symbol erasure rate for the expurgated ensemble ELDPC$(315, \mathbb{F}_{2^4}, x, x^2, 1, 8, \mathcal{H}_4^*)$ for small ϵ.

where

$$E_0 := E_w, \quad E_{w+1} := E_1, \quad h_{0,0} := h_{w,w} \quad h_{0,1} := h_{w,1}.$$

Proof: From the definition of stopping constellation, it holds that for $i = 1, \dots, w$

$$E_i \subseteq h_{i,i}^{-1} h_{i+1,i} E_{i+1}, \qquad E_i \subseteq h_{i-1,i}^{-1} h_{i-1,i-1} E_{i-1}.$$

From those equations, we have

$$E_1 \subseteq h_{1,1}^{-1} h_{2,1} E_2 \subseteq h_{1,1}^{-1} h_{2,1} h_{2,2}^{-1} h_{3,2} E_3 \subseteq \cdots \subseteq \chi E_1. \tag{4.6}$$

Similarly, we have $E_1 \subseteq \chi^{-1} E_1$. Note that $E_1 \subseteq \chi^{-1} E_1$ iff $\chi E_1 \subseteq E_1$, and we have $\chi E_1 \subseteq E_1 \subseteq \chi E_1$. Thus, we have

$$E_1 = \chi E_1. \tag{4.7}$$

From (4.6) and (4.7), we get $E_1 = h_{1,1}^{-1} h_{2,1} E_2$. Similarly, we have $E_i = h_{i,i}^{-1} h_{i+1,i} E_{i+1}$ and $E_i = h_{i-1,i}^{-1} h_{i-1,i-1} E_{i-1}$ for $i = 1, 2, \dots, w$. The converse is clear from the definition. (Q.E.D.)

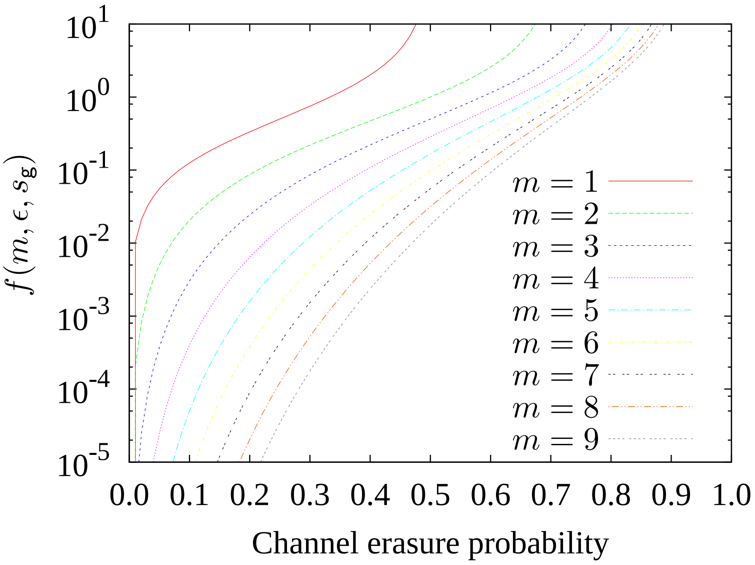

Figure 4.8: Curves given by (4.5) for $\mu = 2$, $w_{\mathrm{g}} = 1$ and $m = 1, 2, \dots, 9$.

4.A.2 The Condition of Successful Decoding for Zigzag Cycle Codes

From Lemma 8, for all the stopping constellations $\{E_i\}_{i=1}^{w}$ of zigzag cycle codes, we see that E_j for $j = 2, \dots, w$ depends only on E_1, i.e.,

$$E_j = \prod_{i=1}^{j-1} h_{i,i}^{-1} h_{i+1,i} E_1$$

for $j = 2, \dots, w$. Hence, in order to clarify the stopping constellation for zigzag cycle codes, without loss of generality, we may focus on analyzing the state E_1. From Lemma 8, we see that $E_1 = \chi E_1$. A *stopping state* for $\chi \in \mathbb{F}_{2^m} \setminus \{0\}$ is defined as a subset $E \subseteq \mathbb{F}_{2^m}$ such that

$$E = \chi E.$$

Let $\mathcal{E}_\chi$ denote the set of all the stopping states for χ.

A zigzag cycle code is *recoverable* if all the symbol in the zigzag cycle code are correct by the BP decoder. From the definition, it is clear that the assignment of states such that $E_i = \mathbb{F}_{2^m}$ for $i = 1, 2, \dots, w$ forms a stopping constellation for any zigzag cycle code of weight w. Note that $\mathbb{F}_{2^m}$ is a subset of $\mathbb{F}_{2^m}$. Thus, no zigzag cycle codes over the BEC are recoverable if all the bits are erased, i.e., $\mathbb{F}_{2^m} \in \mathcal{E}_\chi$ for all $\chi \in \mathbb{F}_{2^m} \setminus \{0\}$. More precisely, if all the bits are erased, no symbols and no bits in the zigzag cycle are correct. Similarly, the assignment of states such that $E_i = \{0\}$ for $i = 1, 2, \dots, w$ also forms a stopping constellation for any zigzag cycle code of weight w, i.e., $\{0\} \in \mathcal{E}_\chi$ for all $\chi \in \mathbb{F}_{2^m} \setminus \{0\}$. Such a stopping constellation corresponds to the case that all the bits are correct by the BP decoder.

Hence, the zigzag cycle codes with labels $h_{1,1}, h_{1,2}, \dots, h_{w,w}, h_{w,1}$ are recoverable unless all the bits are erased if $\mathcal{E}_\chi = \{\{0\}, \mathbb{F}_{2^m}\}$. In other words, whether the zigzag cycle codes with labels $h_{1,1}, h_{1,2}, \ldots, h_{w,w}, h_{w,1}$ are recoverable unless all the bits are erased, depends only on the cycle parameter $\chi = \prod_{i=1}^{w} h_{i,i}^{-1} h_{i+1,i}$.

4.A.3 Analysis of Stopping States

In this subsection, we clarify the condition of χ such that $\mathcal{E}_\chi = \{\{0\}, \mathbb{F}_{2^m}\}$.

For $\chi \in \mathbb{F}_{2^m} \setminus \{0\}$, let $\mathcal{E}_\chi^{(\alpha^i)}$ denote the set of the stopping states containing α^i, i.e., $\alpha^i \in E$ for all $E \in \mathcal{E}_\chi^{(\alpha^i)}$. The *smallest* stopping state containing α^i for χ, denoted by $E_\chi^{(\alpha^i)}$, is the stopping state for χ such that $E_\chi^{(\alpha^i)} \subseteq E$ for all $E \in \mathcal{E}_\chi^{(\alpha^i)}$ and $\alpha^i \in E_\chi^{(\alpha^i)}$. It is clear $E_\chi^{(\alpha^i)}$ equals

$$\bigcap_{E \in \mathcal{E}_\chi^{(\alpha^i)}} E. \tag{4.8}$$

Since $\alpha^i \in E$ for all $E \in \mathcal{E}_\chi^{(\alpha^i)}$, we have α^i is in (4.8). We show the closure of (4.8) under the addition. If γ_1, γ_2 are in (4.8), γ_1, γ_2 are in E for all $E \in \mathcal{E}_\chi^{(\alpha^i)}$. Since γ_1, γ_2 are in E for all $E \in \mathcal{E}_\chi^{(\alpha^i)}$, $\gamma_1 + \gamma_2$ is in E for all $E \in \mathcal{E}_\chi^{(\alpha^i)}$. Hence $\gamma_1 + \gamma_2$ is in (4.8). Obviously (4.8) is a subset of E for all $E \in \mathcal{E}_\chi^{(\alpha^i)}$. Note that

$$\chi \bigcap_{E \in \mathcal{E}_\chi^{(\alpha^i)}} E = \bigcap_{E \in \mathcal{E}_\chi^{(\alpha^i)}} \chi E = \bigcap_{E \in \mathcal{E}_\chi^{(\alpha^i)}} E.$$

Therefore, $E_\chi^{(\alpha^i)}$ is the smallest stopping state containing α^i for χ.

Next, we show the uniqueness of the smallest stopping state containing α^i for χ. Let E^* be another smallest stopping state for χ containing α^i. The existence of a stopping state E^* contradicts the definition of (4.8), since the intersection of E^* and (4.8) contains α^i and is a stopping state for χ.

Lemma 9 The smallest stopping state containing $\alpha^0 = 1$ for $\chi \in \mathbb{F}_{2^m} \setminus \{0\}$ is a subfield of $\mathbb{F}_{2^m}$.

Proof: For all $E \in \mathcal{E}_\chi^{(1)}$, since $1 \in E$ and $E = \chi E$, we have $\chi \in E$. Hence, we have $\chi \in E_\chi^{(1)}$. Recursively, $\chi^j \in E_\chi^{(1)}$ for $j = 0, 1, \ldots, \sigma - 1$, where σ is the order of χ, i.e, σ is the smallest positive integer such that $\chi^\sigma = 1$. Since $E_\chi^{(1)}$ is closed under the addition, we have $\sum_{j=0}^{\sigma-1} a_j \chi^j \in E_\chi^{(\alpha^i)}$, where $a_0, a_1, \ldots, a_{\sigma-1} \in \{0, 1\}$. Hence, we have

$$E_\chi^{(1)} \supseteq \mathcal{A} := \left\{ \sum_{j=0}^{\sigma-1} a_j \chi^j \mid a_0, a_1, \ldots, a_{\sigma-1} \in \{0, 1\} \right\}.$$

Note that $\mathcal{A} = \chi \mathcal{A}$ and $\mathcal{A}$ is closed under the addition. Thus, we have $E_\chi^{(1)} = \mathcal{A}$.

We claim that $E_\chi^{(1)}$ is a subfield of $\mathbb{F}_{2^m}$. Obviously, we have the closure of $E_\chi^{(1)}$ under addition and multiplication. The additive identity is 0 and the multiplicative identity is 1. The additive inverse for $\gamma \in E_\chi^{(1)}$ is γ. For $\gamma \in E_\chi^{(1)}$, γ^{2^m-2} is in $E_\chi^{(1)}$ since the closure of $E_\chi^{(1)}$ under multiplication. The multiplicative inverse for $\gamma \in E_\chi^{(1)} \setminus \{0\}$ is γ^{2^m-2} (Note that $\gamma \in \mathbb{F}_{2^m} \setminus \{0\}$). We are able to check that all field axioms are satisfied. Therefore, $E_\chi^{(1)}$ is a subfield of $\mathbb{F}_{2^m}$. (Q.E.D.)

Lemma 10 Define $\mathcal{H}_m^*$ as in (4.1). If $\chi \notin \mathcal{H}_m^* \cup \{0\}$, it holds that $E_\chi^{(1)} = \mathbb{F}_{2^m}$.

Proof: From Lemma 9, $E_\chi^{(1)}$ is a subfield of $\mathbb{F}_{2^m}$. Note that the order of proper subfield of $\mathbb{F}_{2^m}$ is 2^r [28, p. 45], where r is a positive integer such that $r \mid m$ and $r \neq m$. We will prove $E_\chi^{(1)}$ is not equal to any proper subfields of order 2^r. Define $g := \frac{2^m-1}{2^r-1}$. From $\chi \notin \mathcal{H}_m^* \setminus \{0\}$, we have $\chi = \alpha^{ig+j}$, where $j \in \{1, 2, \dots, g-1\}$. If χ is a member of the proper subfield of order 2^r, then $\chi^{2^r} - \chi = 0$ [28, p. 45]. However,

$$\chi^{2^r} - \chi = \chi(\alpha^{j(2^r-1)} - 1) \neq 0.$$

Hence, χ is not a member of the proper subfield of order 2^r. Thus, we have $E_\chi^{(1)}$ is not equal to the proper subfield of order 2^r for any positive integer r such that $r \mid m$ and $r \neq m$. Therefore, we obtain $E_\chi^{(1)} = \mathbb{F}_{2^m}$. (Q.E.D.)

Lemma 11 Let $\mathcal{E}_\chi$ denote the set of stopping states for χ. Define $\mathcal{H}_m^*$ as in (4.1). If $\mathcal{E}_\chi \setminus \{\{0\}, \mathbb{F}_{2^m}\} \neq \emptyset$, then $\chi \in \mathcal{H}_m^*$.

Proof: Let E be an element of $\mathcal{E}_\chi \setminus \{\{0\}, \mathbb{F}_{2^m}\}$. Note that $\alpha^i E \in \mathcal{E}_\chi \setminus \{\{0\}, \mathbb{F}_{2^m}\}$ for $i = 0, 1, \dots, 2^m-2$. If E contains α^i, then 1 is an element of $\alpha^{-i}E \in \mathcal{E}_\chi \setminus \{\{0\}, \mathbb{F}_{2^m}\}$. Hence, without loss of generality, we assume that $E \in \mathcal{E}_\chi \setminus \{\{0\}, \mathbb{F}_{2^m}\}$ and 1 is an element of E, i.e., $E \in \mathcal{E}_\chi^{(1)}$. Since $E_\chi^{(1)} \neq \mathbb{F}_{2^m}$ and $\chi \neq 0$, we have $\chi \in \mathcal{H}_m^*$ from Lemma 10. (Q.E.D.)

Lemma 12 Define $\mathcal{H}_m^*$ as in (4.1). If $\chi \in \mathcal{H}_m^*$ then $\mathcal{E}_\chi \setminus \{\{0\}, \mathbb{F}_{2^m}\} \neq \emptyset$.

Proof: If $\chi \in \mathcal{H}_m^*$, there exists a positive integer r such that $r \mid m$, $r \neq m$ and $\chi \in \{\alpha^{i(2^m-1)/(2^r-1)} \mid i = 0, 1, \dots, 2^r-2\}$. Then, a stopping state for χ is written as the following:

$$E = \{0\} \cup \left\{\alpha^{j(2^m-1)/(2^r-1)} \mid j = 0, 1, \dots, 2^r-2\right\},$$

in fact $E = \chi E$ and E is a subfield of $\mathbb{F}_{2^m}$ of order 2^r. Hence, we have $E \in \mathcal{E}_\chi \setminus \{\{0\}, \mathbb{F}_{2^m}\} \neq \emptyset$. (Q.E.D.)

4.A.4 Proof of Theorem 2

Note that $\{\{0\}, \mathbb{F}_{2^m}\} \subseteq \mathcal{E}_\chi$ for all $\chi \in \mathbb{F}_{2^m} \setminus \{0\}$. Hence, we have $\mathcal{E}_\chi = \{\{0\}, \mathbb{F}_{2^m}\}$ iff $\mathcal{E}_\chi \setminus \{\{0\}, \mathbb{F}_{2^m}\} = \emptyset$. Define $\mathcal{H}_m^*$ as in (4.1). From Lemma 11 and 12, we have that $\chi \notin \mathcal{H}_m^*$ is a necessary and sufficient condition for $\mathcal{E}_\chi = \{\{0\}, \mathbb{F}_{2^m}\}$. From Appendix 4.A.2, we see that the zigzag cycle codes with labels $h_{1,1}, h_{2,1}, \dots, h_{w,w}, h_{w,1}$ are recoverable unless all the bits are erased if $\mathcal{E}_\chi = \{\{0\}, \mathbb{F}_{2^m}\}$, where $\chi = \prod_{i=1}^{w} h_{i,i}^{-1} h_{i+1,i}$. Hence, we obtain that the zigzag cycle codes with labels $h_{1,1}, h_{1,2}, \dots, h_{w,w}, h_{w,1}$ are recoverable unless all the bits are erased, if $\chi \notin \mathcal{H}_m^*$.

Chapter 5

Analysis of Error Floors of Generalized Non-Binary LDPC Codes over Binary and Non-Binary Memoryless Symmetric Channels

In this chapter, we investigate the error floors of non-binary LDPC codes over $\mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}})$ transmitted over the q-MS channels. We provide a necessary and sufficient condition for successful decoding of zigzag cycle codes over the q-MS channel by the BP decoder. We consider an expurgated ensemble of non-binary LDPC codes by using the above necessary and sufficient condition, and hence exhibit lower error floors. Next, we show lower bounds of the error floors for the expurgated LDPC code ensembles over the q-MS channels. Moreover, we compare the decoding error rates in the error floors for non-binary LDPC codes over the general linear group with those for non-binary LDPC codes over finite field transmitted over the q-MS channel under BP decoding. In this analysis, we see that the optimized non-binary LDPC codes defined over general linear group have the same decoding performance in the error floors as those defined over finite field.

5.1 Introduction

In this chapter, we extend to the results in Chapter 4 to the non-binary LDPC codes defined over $\mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}})$ transmitted over the q-MS channels.

More precisely, we analyze a condition for successful decoding of zigzag cycles under BP decoding over the q-MS channel. Based on this condition, we propose a design method of selecting labels so as to eliminate small zigzag cycles which degrade decoding performance. Moreover, we analyze the error floors of non-binary LDPC codes over the q-MS channel. In other words, we show lower bounds for the symbol error rates in the error floors of the expurgated LDPC code ensembles over the q-MS channel. More precisely, those lower bounds are derived from the decoding errors caused by the zigzag cycles. Furthermore, simulation results show that the lower bounds on symbol error rates are tight for the expurgated ensembles constructed by our proposed method over the q-MS channels.

It is known that the decoding complexity of non-binary LDPC codes over 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 general linear group is lower than those for optimized non-binary LDPC codes over finite field [29]. However, no methods to lower the decoding error rates in error floors for non-binary LDPC codes over general linear group have been proposed. Moreover, the decoding error rates in the error floor region for optimized non-binary LDPC codes over general linear group have not been compared with those for optimized non-binary LDPC codes over finite field.

In this chapter, we define non-binary LDPC codes over general linear group $\mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}})$ and decoding algorithm to analyze the non-binary LDPC code over both finite field $\mathbb{F}_{2^m}$ and general linear group $\mathrm{GL}(m, \mathbb{F}_2)$. We assume the q-MS channels [14] for the generality. We extend the optimization and analysis method in Chapter 4 to the non-binary LDPC codes over general linear group transmitted over the q-MS channels. More precisely, firstly, 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 code 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 code 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 optimized non-binary LDPC codes.

This chapter is organized as follows: In Section 5.2, we propose a method to lower the error floors by analyzing the zigzag cycles. In Section 5.3, we derive lower bounds for symbol error rates in the error floors for non-binary LDPC codes.

5.2 Zigzag Cycle Code Analysis

A zigzag cycle is a cycle such that the degrees of all the variable nodes in the cycles 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 4.1 shows a zigzag cycle code of symbol code length w. In this section, we give a condition for successful decoding of the zigzag cycle codes over the 2^{m_1}-MS channels under BP decoding.

5.2.1 Condition for Successful Decoding

We consider the zigzag cycle code of symbol code length w with labels $h_{1,1}, h_{1,2}, \dots, h_{w,w}, h_{w,1} \in \mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}}) \setminus \{0\}$ as shown in Fig. 4.1. For any $m_3 \times m_3$ matrices $A_1, A_2, \dots, A_k$, we define $\prod_{i=1}^{k} A_k := A_1 A_2 \cdots A_k$. We define $\chi := h_{1,1}^{-1} h_{1,2} h_{2,2}^{-1} h_{2,3} \cdots h_{w,w}^{-1} h_{w,1} \in \mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}}) \setminus \{0\}$.

Definition 4 Let $\langle \chi \rangle$ be the cyclic subgroup generated by χ, i.e., $\langle \chi \rangle := \{\chi^j \mid j = 0, 1, 2, \dots\}$. 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 shows that the decoding error rates depend on a set of class representatives S_χ, i.e., the matrix $\chi \in \mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}}) \setminus \{0\}$, for a fixed channel and weight of zigzag cycle code.

Lemma 13 We consider a zigzag cycle code of symbol code length w labeled by $h_{1,1}, h_{1,2}, \ldots, h_{w,w}, h_{w,1} \in \mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}}) \setminus \{0\}$ transmitted over the 2^{m_1}-MS channel. The matrix χ is given by $\chi = h_{1,1}^{-1} h_{1,2} h_{2,2}^{-1} h_{2,3} \cdots h_{w,w}^{-1} h_{w,1} \in \mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}}) \setminus \{0\}$. Define $\iota_i = h_{i,i}^{-1} h_{i,i+1}$ for $i \in [1, w]$, where $h_{w+1,w} = h_{1,w}$. Define S_χ as in Definition 4. 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 $x \in \tilde{S}_\chi$ such that

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

The proof of this lemma is in Appendix 5.A.

By Using Lemma 13, we have the following Theorem.

Theorem 4 Define S_χ as in Definition 4. For a fixed channel output, if the zigzag cycle with the matrix χ such that $|S_\chi| > 1$ is successfully decoded, the zigzag cycle with the matrix χ such that $|S_\chi| = 1$ is also successfully decoded.

proof: We consider 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 13, if the zigzag cycle with the matrix χ such that $|S_\chi| > 1$ is successfully decoded, for all $x \in S_\chi$

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

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

$$\begin{aligned} &\prod_{x\in S_\chi}\prod_{k=1}^{w} C_k(0)^{|\langle\chi\rangle x|} > \prod_{x\in S_\chi}\prod_{t=0}^{|\langle\chi\rangle x|-1}\prod_{s=1}^{w} C_s\left(\left(\prod_{j=s}^{w}\iota_j\right)\chi^t x\right) \\ \iff &\prod_{k=1}^{w} C_k(0)^{2^{m_3m_4}-1} > \prod_{x\in\mathbb{F}_{2^{m_4}}^{m_3}}\prod_{s=1}^{w} C_s\left(x\right). \end{aligned} \tag{5.1}$$

Similarly, for the matrix χ such that $|S_\chi| = 1$ and $x \in S_\chi$, $\langle\chi\rangle x = \mathbb{F}_{2^{m_4}}^{m_3}$. Hence, from Lemma 13, if the zigzag cycle with the matrix χ such that $|S_\chi| = 1$ is successfully decoded,

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

Since this condition coincides with (5.1), the zigzag cycle with the matrix χ such that $|S_\chi| = 1$ is also successfully decoded. (Q.E.D.)

Theorem 4 shows a condition for lowering the error floor. The order σ_χ of the matrix χ is the smallest positive integer such that χ^{σ_χ} is $m_3 \times m_3$ identity matrix. The following lemma asserts that the condition for successful decoding in the case for $|S_\chi| = 1$ is simplified by the order of the matrix χ.

Lemma 14 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 5.B.

Discussion 6 By combining Theorem 4 and Lemma 14, we see that the zigzag cycles with the matrix χ such that the order of χ is $2^{m_3m_4} - 1$ have the best decoding performance. By using this condition, we propose a method to lower the error floors for generalized non-binary LDPC codes as follows: Designing the labels in the zigzag cycles of small weight as the order of χ satisfies $2^{m_3m_4} - 1$.

Discussion 7 From Discussion 6, in the case for the non-binary LDPC codes over Galois field $\mathbb{F}_{2^m}$, the condition for the zigzag cycles which have the best decoding performance can be simplified. We claim that for the non-binary LDPC codes over $\mathbb{F}_{2^m}$ the order of χ is $2^m - 1$ if and only if $\chi \notin \mathcal{H}_{1,m}$, where

$$\mathcal{H}_{1,m} := \bigcup_{0<r<2^m-1:r|2^m-1}\left\{\alpha^{i\frac{2^m-1}{r}} \mid i = 0, \ldots, r-1\right\}.$$

Firstly, we show that the order of χ is $2^m - 1$ if $\chi \notin \mathcal{H}_{1,m}$. For $r < 2^m - 1$, we define

$$\mathcal{H}_{1,m}^{(r)} := \left\{\alpha^{i\frac{2^m-1}{r}} \mid i = 0, \ldots, r-1\right\}.$$

Table 5.1: The elements in $\mathcal{H}_{1,m}$ for $m = 2, 3, \ldots, 9$.

Field	The elements of $\mathcal{H}_{1,m}$
$\mathbb{F}_{2^2}$	1
$\mathbb{F}_{2^3}$	1
$\mathbb{F}_{2^4}$	$1, \alpha^3, \alpha^5, \alpha^6, \alpha^9, \alpha^{10}, \alpha^{12}$
$\mathbb{F}_{2^5}$	1
$\mathbb{F}_{2^6}$	$1, \alpha^3, \alpha^6, \alpha^7, \alpha^9, \alpha^{12}, \alpha^{14}, \alpha^{15}, \alpha^{18}, \alpha^{21}, \alpha^{24}, \alpha^{25}, \alpha^{27}, \alpha^{28}, \alpha^{30}, \alpha^{33}, \alpha^{35}, \alpha^{36}, \alpha^{39}, \alpha^{42},$ $\alpha^{45}, \alpha^{48}, \alpha^{49}, \alpha^{51}, \alpha^{54}, \alpha^{56}, \alpha^{57}, \alpha^{60}$
$\mathbb{F}_{2^7}$	1
$\mathbb{F}_{2^8}$	$1, \alpha^3, \alpha^5, \alpha^6, \alpha^9, \alpha^{10}, \alpha^{12}, \alpha^{15}, \alpha^{17}, \alpha^{18}, \alpha^{20}, \alpha^{21}, \alpha^{24}, \alpha^{25}, \alpha^{27}, \alpha^{30}, \alpha^{33}, \alpha^{34}, \alpha^{35}, \alpha^{36},$ $\alpha^{39}, \alpha^{40}, \alpha^{42}, \alpha^{45}, \alpha^{48}, \alpha^{50}, \alpha^{51}, \alpha^{54}, \alpha^{55}, \alpha^{57}, \alpha^{60}, \alpha^{63}, \alpha^{65}, \alpha^{66}, \alpha^{68}, \alpha^{69}, \alpha^{70}, \alpha^{72}, \alpha^{75},$ $\alpha^{78}, \alpha^{80}, \alpha^{81}, \alpha^{84}, \alpha^{85}, \alpha^{87}, \alpha^{90}, \alpha^{93}, \alpha^{95}, \alpha^{96}, \alpha^{99}, \alpha^{100}, \alpha^{102}, \alpha^{105}, \alpha^{108}, \alpha^{110}, \alpha^{111},$ $\alpha^{114}, \alpha^{115}, \alpha^{117}, \alpha^{119}, \alpha^{120}, \alpha^{123}, \alpha^{125}, \alpha^{126}, \alpha^{129}, \alpha^{130}, \alpha^{132}, \alpha^{135}, \alpha^{136}, \alpha^{138}, \alpha^{140},$ $\alpha^{141}, \alpha^{144}, \alpha^{145}, \alpha^{147}, \alpha^{150}, \alpha^{153}, \alpha^{155}, \alpha^{156}, \alpha^{159}, \alpha^{160}, \alpha^{162}, \alpha^{165}, \alpha^{168}, \alpha^{170}, \alpha^{171},$ $\alpha^{174}, \alpha^{175}, \alpha^{177}, \alpha^{180}, \alpha^{183}, \alpha^{185}, \alpha^{186}, \alpha^{187}, \alpha^{189}, \alpha^{190}, \alpha^{192}, \alpha^{195}, \alpha^{198}, \alpha^{200}, \alpha^{201},$ $\alpha^{204}, \alpha^{205}, \alpha^{207}, \alpha^{210}, \alpha^{213}, \alpha^{215}, \alpha^{216}, \alpha^{219}, \alpha^{220}, \alpha^{221}, \alpha^{222}, \alpha^{225}, \alpha^{228}, \alpha^{230}, \alpha^{231},$ $\alpha^{234}, \alpha^{235}, \alpha^{237}, \alpha^{238}, \alpha^{240}, \alpha^{243}, \alpha^{245}, \alpha^{246}, \alpha^{249}, \alpha^{250}, \alpha^{252}$
$\mathbb{F}_{2^9}$	1

If $\chi \notin \mathcal{H}_{1,m}^{(r)}$, there exist integers $i \in \{0, 1, \ldots, r-1\}$ and $j \in \{1, \ldots, (2^m - 1)/r - 1\}$ such that $\chi = \alpha^{i(2^m-1)/r+j}$. Hence, we have

$$\chi^r = \alpha^{\{i(2^m-1)/r+j\}r} = \alpha^{jr}.$$

Since $jr < 2^m - 1$, we get $\chi = \alpha^{jr} \neq 1$. Thus, we have the order of χ is not r if $\chi \notin \mathcal{H}_{1,m}^{(r)}$. Since the order of χ is less than or equal to $2^m - 1$ for $\chi \in \mathbb{F}_{2^m} \setminus \{0\}$, the order of χ is $2^m - 1$ if $\chi \notin \mathcal{H}_{1,m}$. Secondly, we show that $\chi \notin \mathcal{H}_{1,m}$ if the order of χ is $2^m - 1$. Obviously, the order of $\chi \in \mathcal{H}_{1,m}^{(r)}$ is less than or equal to r. Hence, the order of $\chi \in \mathcal{H}_{1,m}$ is less than $2^m - 1$. From the contraposition, $\chi \notin \mathcal{H}_{1,m}$ if the order of χ is $2^m - 1$. Therefore, we see that the order of χ is $2^m - 1$ if and only if $\chi \notin \mathcal{H}_{1,m}$.

Thus, the zigzag cycles with the cycle parameter $\chi \notin \mathcal{H}_{1,m}$ have the best decoding performance. Note that $\{\alpha^{i(2^m-1)/r} \mid i = 0, \ldots, r-1\}$ represents a proper subgroup of $\mathbb{F}_{2^m}$. Table 5.1 shows the elements in $\mathcal{H}_{1,m}$ for $m = 2, 3, \ldots, 9$. Figure 5.1 shows the symbol error rate for the zigzag cycle code define over $\mathbb{F}_{2^4}$ of symbol code length 3 over the BAWGN channel with channel variance $\sigma^2 = 1$. From Figure 5.1, we see that the zigzag cycle codes with the cycle parameter $\chi \notin \mathcal{H}_{1,4}$ have the best decoding performance.

The log-likelihood ratio for the 2^{m_1}-ary channels are defined in [30]. 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

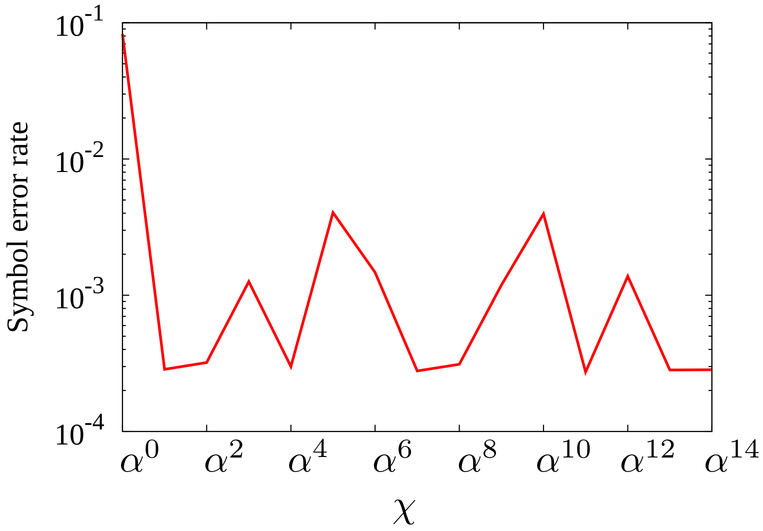

Figure 5.1: The symbol error rate for the zigzag cycle code defined over $\mathbb{F}_{2^4}$ of symbol code length 3 over the BAWGN channel with channel variance $\sigma^2 = 1$. The horizontal line corresponds to the cycle parameter.

v-th variable node, i.e.,

$$Z_{v,i}(y_{v,i}, \gamma) := \log \frac{p(y_{v,i} \mid 0)}{p_i(y_{v,i} \mid \gamma)}. \tag{5.2}$$

By using the log-likelihood ratio, the condition for successful decoding of the zigzag cycle codes with the matrix χ of the order $2^{m_3 m_4} - 1$ over the 2^{m_1}-MS channel is given as the following corollary.

Corollary 2 We consider the zigzag cycle codes of symbol code length w with the matrix χ of the order $2^{m_3 m_4} - 1$ over the 2^{m_1}-ary input memoryless symmetric channel. For $\gamma \in \mathbb{F}_2^{m_1}$, let $Z_{v,i}(Y_{v,i}, \gamma)$ define as in (5.2). In the limit of large ℓ, no symbols in the zigzag cycle code are eventually correct if and only if

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

Moreover, in the limit of large ℓ, all the symbols in the zigzag cycle code are eventually correct if and only if

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

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

$$C_v(0) = \prod_{i=1}^{m_2} p(y_{v,i} \mid 0),$$

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

Hence, from Theorem 4, no symbols in the zigzag cycles are eventually correct if and only if

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

Similarly, we have that all the symbols in the zigzag cycle code are eventually correct if and only if

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

This concludes the proof. (Q.E.D.)

5.2.2 Bhattacharyya Functional and Error Probability

We define distributions of log-likelihood ratios associated with 2^{m_1}-ary channels as follows:

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

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 [5, p. 178].

Definition 5 For a L-density a, the *Bhattacharyya functional* $\mathfrak{B}(\mathsf{a})$ is defined as

$$\mathfrak{B}(\mathsf{a}) := \int_{-\infty}^{\infty} \mathsf{a}(x)\exp[-x/2]dx.$$

In this definition, we assume not only *symmetric* L-density [5] but also *asymmetric* L-density. In the case for the MBIOS channel, Definition 5 holds [5, Definition 4.61]. 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.,

$$(\mathsf{a}_1 * \mathsf{a}_2)(x) := \int_{-\infty}^{\infty} \mathsf{a}_1(x-y)\mathsf{a}_2(y)dy.$$

Fact 2 Let Z denote the random variable with L-density a. Then,

$$\Pr(Z \leq 0) \leq \mathfrak{B}(\mathsf{a}).$$

Corollary 2 gives the decoding error probability of zigzag cycle with the matrix χ of the order σ_χ as the following corollary.

Corollary 3 Denote $m = m_1 m_2 = m_3 m_4$. Let $\mathrm{P}_{\mathrm{zz}}(w, m, \mathsf{a})$ 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 the matrix χ such that $\sigma_\chi = 2^m - 1$, over 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 5. We have the symbol error rates of the zigzag cycle codes is given by

$$\mathrm{P}_{\mathrm{zz}}(w, m, \mathsf{a}) = \Pr\bigl(Z^{(wm_2)} \leq 0\bigr) \leq \mathfrak{B}^{wm_2}(\mathsf{a}).$$

proof: Corollary 2 implies that $\mathrm{P}_{\mathrm{zz}}(w, m, \mathsf{a}) = \Pr(Z^{(wm_2)} \leq 0)$. From Fact 1 and 2, we have $\Pr(Z^{(wm_2)} \leq 0) \leq \mathfrak{B}^{wm_2}(\mathsf{b})$. (Q.E.D.)

Corollary 3 shows that for a fixed weight w and $m = m_3 m_4$, the decoding error rate of the zigzag cycle code does not depend on m_3 or m_4. In other words, the decoding error rate of the zigzag cycle over general linear group is equal to that of the zigzag cycle over finite field for a fixed weight w and $m = m_3 m_4$.

Figure 5.2 shows the symbol error rate for the zigzag cycle code defined over $\mathbb{F}_{2^4}$ of symbol code length 3 with the cycle parameter $\chi \notin \mathcal{H}_{1,4}$ over the BAWGN channel. The circles in Figure 5.2 show the simulation results. The solid curve the theoretical symbol error rate. For the BAWGN channel with channel variance σ, the theoretical symbol error rate of the zigzag cycle codes defined over $\mathbb{F}_{2^4}$ of symbol code length w with cycle parameter $\chi \notin \mathcal{H}_{1,m}$ is given by

$$Q\left(\frac{\sqrt{mw}}{\sigma}\right),$$

where $Q(y) = \frac{1}{\sqrt{2\pi}} \int_y^\infty \exp[-\frac{x^2}{2}]dx$. From Figure 5.2, we see that the theoretical result gives the symbol error rate of zigzag cycle code with the cycle parameter $\chi \notin \mathcal{H}_{1,m}$.

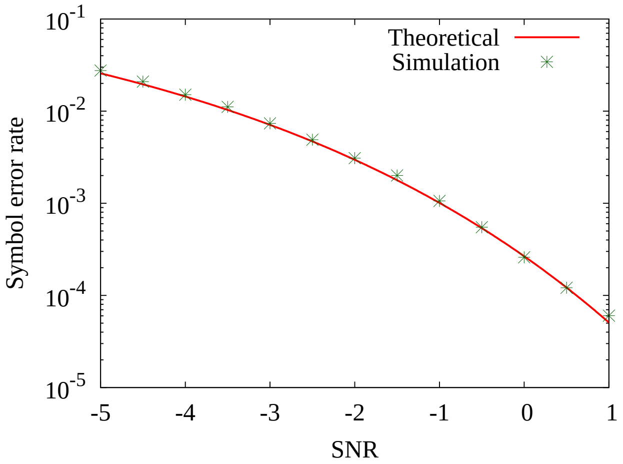

Figure 5.2: Symbol error rate of zigzag cycle codes defined over $\mathbb{F}_{2^4}$ of symbol code length 3 with cycle parameter $\chi \notin \mathcal{H}_{1,4}$. The solid curve shows the theoretical symbol error rate. The circles show the simulation result.

5.3 Analysis of Error Floors

In the previous section, we give a condition for the decoding error to the zigzag cycle code. By using this result, in this section, we give lower bounds of the symbol error rates in the error floors of the non-binary LDPC code ensembles over the 2^{m_1}-MS channel under BP decoding.

Definition 6 Recall that $\mathrm{LDPC}(N, \mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}}), \lambda, \rho)$ 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) [5] over $\mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}}) \setminus \{0\}$. Let $w_\mathrm{g} \in \mathbb{N} \setminus \{1\}$ 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 $\{1, \dots, w_\mathrm{g} - 1\}$. Note that the expurgated ensemble $\mathrm{ELDPC}(N, \mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}}), \lambda, \rho, 1)$ is equivalent to $\mathrm{LDPC}(N, \mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}}), \lambda, \rho)$. Let $w_\mathrm{c} \in \mathbb{N}$ be an expurgation parameter for labeling in the Tanner graph, where $w_\mathrm{g} < w_\mathrm{c}$. 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 $\{w_\mathrm{g}, \dots, w_\mathrm{c} - 1\}$ with the cycle parameter $\beta \in \mathcal{H}$.

Define

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

From Discussion 6, to lower the error floors, we need to avoid the zigzag cycles with the matrices $\chi \in \mathcal{H}_{m_3,m_4}$. Note that $|\mathcal{H}_{m,1}| \geq |\mathcal{H}_{1,m}|$. Hence, the non-binary LDPC codes defined over general linear group have more choices of the labels in the edges which satisfy the condition for the optimization.

5.3.1 Analysis of Error Floors

In this section, we analyze the symbol error rates in the error floors for the expurgated ensembles defined in Definition 6. The following theorem gives a lower bound on the symbol error rate under BP decoding for the expurgated ensemble $\mathrm{ELDPC}(N, \mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}}), \lambda, \rho, w_{\mathsf{g}}, w_{\mathsf{c}}, \mathcal{H}_{m_3,m_4})$.

Theorem 5 Let $\mathrm{P_s}(\mathrm{ELDPC}, \mathsf{a}, m_1)$ be the symbol error rate of the expurgated ensemble $\mathrm{ELDPC}(N, \mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}}), \lambda, \rho, w_{\mathsf{g}}, w_{\mathsf{c}}, \mathcal{H}_{m_3,m_4})$ over the 2^{m_1}-MS channel characterized by its L-density a under BP decoding. Define $m := m_3 m_4$. Define $Z^{(km)}$ as in Corollary 3. For sufficiently large N and $\mathfrak{B}(\mathsf{b}) < \mu^{-1/m}$ the symbol error rate is bounded by

$$\mathrm{P_s}(\mathrm{ELDPC}, \mathsf{a}, m_1) \geq \frac{1}{2N} \sum_{w=w_{\mathsf{g}}}^{\infty} \mu^w \Pr\bigl(Z^{(wm_2)} \leq 0\bigr) + o\Bigl(\frac{1}{N}\Bigr). \tag{5.3}$$

proof: From Corollary 3 show that the symbol error rates of the zigzag cycles of weight w with the matrix χ such that $\sigma_\chi = 2^m - 1$ are $\Pr(Z^{(wm_2)} \leq 0)$. Moreover, by combining Discussion 6 and Corollary 3, we see that the symbol error rates of the zigzag cycles of weight w with the matrix χ such that $\sigma_\chi \neq 2^m - 1$ are lower bounded by $\Pr(Z^{(wm_2)} \leq 0)$. By using technique in the proof of Theorem 3, we have (5.3). From Corollary 3, we get

$$\sum_{w=w_{\mathsf{g}}}^{\infty} \mu^w \Pr\bigl(Z^{(wm_2)} \leq 0\bigr) \leq \sum_{w=w_{\mathsf{g}}}^{\infty} \mu^w \mathfrak{B}(\mathsf{b})^{wm_2}.$$

Thus, for sufficiently large N and $\mathfrak{B}(\mathsf{b}) < \mu^{-1/m}$, the left hand side of this inequality converges. (Q.E.D.)

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

Corollary 4 Define

$$\epsilon_m^* := \begin{cases} \frac{1}{2} & \text{for } \mu \leq 1, \\ \frac{1-\sqrt{1-\mu^{-2/m}}}{2} & \text{for } \mu > 1. \end{cases}$$

For the BSC with crossover probability ϵ and $\epsilon < \epsilon_m^*$, the symbol error rate is lower bounded by

$$\mathrm{P_s}(\mathrm{ELDPC}, \mathsf{a}) \geq \frac{1}{2N} \sum_{w=w_{\mathsf{c}}}^{\infty} \mu^w \sum_{i \leq mw/2} \binom{mw}{i} \epsilon^{mw-i} (1-\epsilon)^i + o\Bigl(\frac{1}{N}\Bigr). \tag{5.4}$$

Corollary 5 Define

$$\sigma_m^* := \begin{cases} \infty & \text{for } \mu \leq 1, \\ \sqrt{\frac{m}{2 \ln \mu}} & \text{for } \mu > 1. \end{cases}$$

For the BAWGN channel with channel variance σ^2 and $\sigma < \sigma_m^*$, the symbol error rate is lower bounded by

$$\mathrm{P_s}(\mathrm{ELDPC}, \mathsf{a}) \geq \frac{1}{2N} \sum_{w=w_\mathsf{g}}^{\infty} \mu^w Q\left(\frac{\sqrt{mw}}{\sigma}\right) + o\left(\frac{1}{N}\right), \tag{5.5}$$

where $Q(y) = \frac{1}{\sqrt{2\pi}} \int_y^\infty \exp[-\frac{x^2}{2}]dx$.

Let $\mathrm{P_b}(\mathrm{ELDPC}, \mathsf{a})$ be the the bit error rate for the non-binary LDPC code ensemble $\mathrm{ELDPC}(N, \mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}}), \lambda, \rho, w_\mathsf{g}, w_\mathsf{c}, \mathcal{H}_{m_3,m_4})$ over the MBIOS channel characterized by its L-density a under BP decoding. The expected value the number of bit errors in a symbol which is caused error is $\frac{m2^{m-1}}{2^m-1}$. Let n be the bit code length, i.e., $n = m_3 m_4 N$. Hence, the bit error rate is bounded by

$$\mathrm{P_b}(\mathrm{ELDPC}, \mathsf{a}) \geq \frac{1}{2n} \frac{m2^{m-1}}{2^m - 1} \sum_{w=w_\mathsf{g}}^{\infty} \mu^w Q\left(\frac{\sqrt{mw}}{\sigma}\right) + o\left(\frac{1}{N}\right). \tag{5.6}$$

Discussion 8 Let $I_{\{\cdot\}}$ be the indicator function which is 1 if the condition inside the braces is fulfilled and 0 otherwise. Consider the q-SC with channel error probability ϵ, where $q = 2^m$. From the definition of q-SC, the zigzag cycle cause the decoding error if the number of changed symbols in zigzag cycle is more than $q-1$ times the number of the correct symbols in zigzag cycle. Thus, we have that

$$\Pr(Z^{(w)} \leq 0) = \sum_{k=0}^{w} \binom{w}{k} (1-\epsilon)^k \epsilon^{w-k} I_{\{w \geq kq\}}.$$

From Theorem 5, the symbol error rate of the expurgated LDPC code ensemble is given by

$$\mathrm{P_s}(\mathrm{ELDPC}, \mathsf{a}) \geq \frac{1}{2N} \sum_{w=w_\mathsf{g}}^{\infty} \mu^w \sum_{k=0}^{w} \binom{w}{k} (1-\epsilon)^k \epsilon^{w-k} I_{\{w \geq kq\}} + o\left(\frac{1}{N}\right).$$

Note that $\Pr(Z^{(w)} \leq 0) \geq \epsilon^w$, and that equality holds if and only if $w \leq q$. For $w_\mathsf{g} < q$, we have

$$\begin{aligned} P_\mathrm{s}(\mathrm{ELDPC}, \mathsf{a}) \geq & \frac{1}{2N} \sum_{w=w_\mathsf{g}}^{\infty} \mu^w \Pr(Z^{(w)} \leq 0) + o\left(\frac{1}{N}\right) \\ \geq & \frac{1}{2N} \sum_{w=w_\mathsf{g}}^{q} \mu^w \epsilon^w + o\left(\frac{1}{N}\right) \\ \geq & \frac{1}{2N} \frac{(\mu\epsilon)^{w_\mathsf{g}} - (\mu\epsilon)^{q+1}}{1-\mu\epsilon}. \end{aligned}$$

For sufficient large q, the left hand side of this equation is written as follows:

$$\frac{1}{2N} \frac{(\mu\epsilon)^{w_\mathsf{g}}}{1-\mu\epsilon}. \tag{5.7}$$

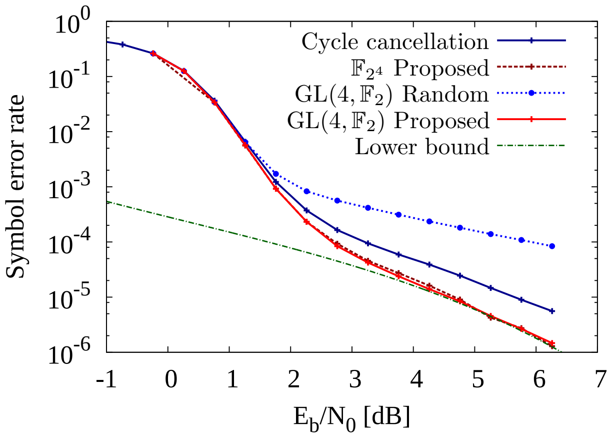

Figure 5.3: The symbol error rates for the expurgated ensemble ELDPC(315, GL($m_3, \mathbb{F}_{2^{m_4}}$), $x, x^2, 1, 8, \mathcal{H}$) transmitted over the BAWGN channel for $m_3 = 1, m_4 = 4, \mathcal{H} = \{1\}$ (Cycle cancellation), for $m_3 = 1, m_4 = 4, \mathcal{H} = \mathcal{H}_{1,4}$ ($\mathbb{F}_{2^4}$ Proposed), for $m_3 = 4, m_4 = 1, \mathcal{H} = \{\}$ (GL(4, $\mathbb{F}_2$) Random) and for $m_3 = 4, m_4 = 1, \mathcal{H} = \mathcal{H}_{4,1}$ (GL(4, $\mathbb{F}_2$) Proposed). The lower bound is given by (5.5).

5.3.2 Monotonicity of Error floors for MBIOS Channel

We denote the lower bound of decoding error rate for the expurgated ensemble ELDPC(N, GL($m_3, \mathbb{F}_{2^{m_4}}$), $\lambda, \rho, w_\mathrm{g}, w_\mathrm{c}, \mathcal{H}_{m_3,m_4}$) by $f(m, w_\mathrm{g})$, i.e.,

$$f(m, w_\mathrm{g}) := \frac{1}{2n}\frac{m2^{m-1}}{2^m - 1}\sum_{w=w_\mathrm{g}}^{\infty} \mu^w Q\left(\frac{\sqrt{mw}}{\sigma}\right). \tag{5.8}$$

The following lemma shows that for a fixed large bit code length, the lower bound on the bit error rate is decreasing in m, i.e., $f(m, w_\mathrm{g})$ is decreasing in m.

Lemma 15 Define $f(m, w_\mathrm{g})$ as in (5.8). Then $f(m, w_\mathrm{g}) > f(m+1, w_\mathrm{g})$ for $\mu = \lambda'(0)\rho'(1) > 1$ and $0 < \sigma < \sqrt{\frac{1}{2\ln\mu}}$.

The proof of this lemma is in Appendix 5.C.

5.3.3 Simulation Results

In this section, we compare the symbol error rate in the error floor for the expurgated ensemble constructed by our proposed method with (i) that constructed by the cycle cancellation [27] and non-optimized ensemble, and (ii) that constructed by the combination of the cycle cancellation and the stopping set mitigation [27].

BAWGN Channel Case

Figure 5.3 shows the symbol error rates for the expurgated ensemble ELDPC(315, GL($m_3, \mathbb{F}_{2^{m_4}}$), $x, x^2, 1, 8, \mathcal{H}$) transmitted over the BAWGN channel for $m_3 = 1, m_4 = 4, \mathcal{H} = \{1\}$ (Cycle cancellation), for $m_3 = 1, m_4 = 4, \mathcal{H} = \mathcal{H}_{1,4}$ ($\mathbb{F}_{2^4}$), for $m_3 = 4, m_4 = 1, \mathcal{H} = \{\}$ (GL(4, $\mathbb{F}_2$)

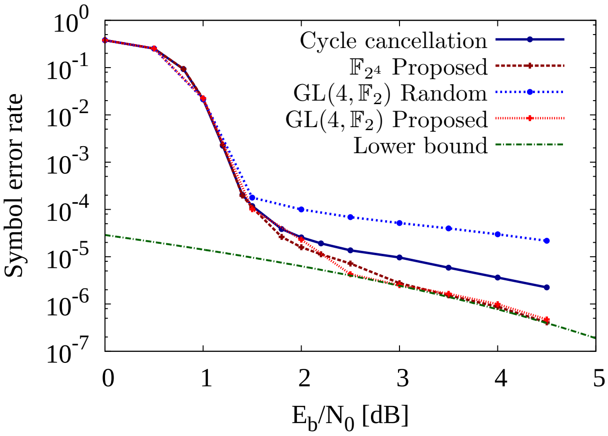

Figure 5.4: The symbol error rates for the expurgated ensemble $\mathrm{ELDPC}(1000, \mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}}), \lambda, \rho, 1, 8, \mathcal{H})$ transmitted over the BAWGN channel for $m_3 = 1, m_4 = 4, \mathcal{H} = \{1\}$ (Cycle cancellation), for $m_3 = 1, m_4 = 4, \mathcal{H} = \mathcal{H}_{1,4}$ ($\mathbb{F}_{2^4}$ Proposed), for $m_3 = 4, m_4 = 1, \mathcal{H} = \{\}$ (GL(4, $\mathbb{F}_2$) Random) and for $m_3 = 4, m_4 = 1, \mathcal{H} = \mathcal{H}_{4,1}$ (GL(4, $\mathbb{F}_2$) Proposed). The lower bound is given by (5.5).

Random) and for $m_3 = 4, m_4 = 1, \mathcal{H} = \mathcal{H}^*_{4,1}$ GL(4, $\mathbb{F}_2$) Proposed). Figure 5.4 shows that the symbol error rates for the expurgated ensemble $\mathrm{ELDPC}(1000, \mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}}), \lambda, \rho, 1, 8, \mathcal{H})$ transmitted over the BAWGN channel for $m_3 = 1, m_4 = 4, \mathcal{H} = \{1\}$ (Cycle cancellation), for $m_3 = 1, m_4 = 4, \mathcal{H} = \mathcal{H}_{1,4}$ ($\mathbb{F}_{2^4}$ Proposed), for $m_3 = 4, m_4 = 1, \mathcal{H} = \{\}$ (GL(4, $\mathbb{F}_2$) Random) and for $m_3 = 4, m_4 = 1, \mathcal{H} = \mathcal{H}_{4,1}$ (GL(4, $\mathbb{F}_2$) Proposed). The lower bounds in Figure 5.3 and 5.4 are derived from (5.5). Figure 5.3 and 5.4 show that the proposed codes exhibit better decoding performance than the codes designed cycle cancellation and non-optimized codes. We see that the lower bounds (5.5) give tight lower bounds for the symbol error rates to the proposed codes. Moreover, the decoding performance in the error floors for optimized LDPC codes over general linear group is the same as that for optimized LDPC codes over Galois field.

Figure 5.5 shows bit error rates of $\mathrm{ELDPC}(N, \mathbb{F}_{2^m}, x, x^2, 1, 6, \mathcal{H}_{1,m})$ for $(N, m) = (2520, 1), (1260, 2), (630, 4)$. The bit code length n of those ensemble is 2520. The lower bounds are given by (5.6). We see that (5.6) gives tight lower bound for bit error rate of the expurgated ensemble $\mathrm{ELDPC}(N, \mathbb{F}_{2^m}, x, x^2, 1, 6, \mathcal{H}_{1,m})$. Moreover, Figure 5.5 implies that for a fixed bit code length n, the bit error rate decreases as the order of field increases.

BSC Case

Figure 5.6 shows the symbol error rates for the expurgated ensemble $\mathrm{ELDPC}(315, \mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}}), x, x^2, 1, 8, \mathcal{H})$ transmitted over the BSC for $m_3 = 1, m_4 = 4, \mathcal{H} = \{1\}$ (Cycle cancellation), for $m_3 = 1, m_4 = 4, \mathcal{H} = \mathcal{H}_{1,4}$ ($\mathbb{F}_{2^4}$), for $m_3 = 4, m_4 = 1, \mathcal{H} = \{\}$ (GL(4, $\mathbb{F}_2$) Random) and for $m_3 = 4, m_4 = 1, \mathcal{H} = \mathcal{H}_{4,1}$ (GL(4, $\mathbb{F}_2$) Proposed). For the expurgated ensemble with the expurgated parameter $w_{\mathrm{g}} = 1$, predominant contributions to the symbol error rate are caused by zigzag cycles of weight 1. For the BSC, the decoding error rate for zigzag cycle codes of symbol code over $\mathbb{F}_{2^4}$ with length 1 is the same for all cycle parameter χ. Hence, the decoding

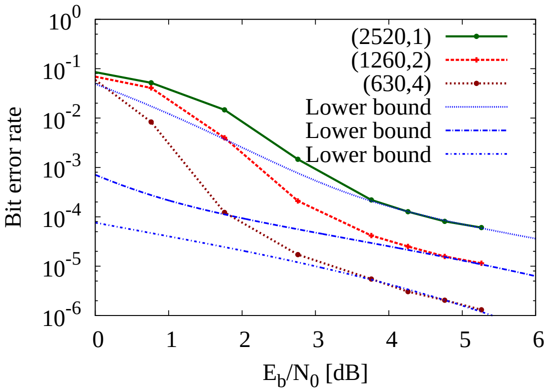

Figure 5.5: Bit error rates of $\mathrm{ELDPC}(N, \mathbb{F}_{2^m}, x, x^2, 1, 6, \mathcal{H}_{1,m})$ for $(N, m) = (2520, 1), (1260, 2), (630, 4)$. The bit code length n of those ensemble is 2520. The lower bounds are given by (5.6).

performance in the error floor for the code designed by our proposed method is same as that in the error floor for the code designed by cycle cancellation in Figure 5.6. The lower bound in Figure 5.6 is given by (5.4). We see that (5.4) gives tight lower bounds for the symbol error rates to the expurgated ensembles constructed by our proposed method in the error floor.

Figure 5.6 shows the symbol error rates for the expurgated ensemble with $s_{\mathrm{g}} > 1$. More precisely, Figure 5.6 shows the symbol error rates for the expurgated ensemble ELDPC(315, $\mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}}), x, x^2, 2, 8, \mathcal{H})$ transmitted over the BSC for $m_3 = 1, m_4 = 4, \mathcal{H} = \{1\}$ (Cycle cancellation), for $m_3 = 1, m_4 = 4, \mathcal{H} = \mathcal{H}_{1,4}$ ($\mathbb{F}_{2^4}$), for $m_3 = 4, m_4 = 1, \mathcal{H} = \{\}$ ($\mathrm{GL}(4, \mathbb{F}_2)$ Random) and for $m_3 = 4, m_4 = 1, \mathcal{H} = \mathcal{H}_{4,1}$ ($\mathrm{GL}(4, \mathbb{F}_2)$ Proposed). The lower bounds for the symbol error rates are given by (5.4). From Figure 5.7, we see that our proposed codes exhibit better decoding performance than codes designed by the cycle cancellation. Moreover the decoding error rate in the error floor for the optimized code over general linear group is same as that for the optimized code over Galois field.

2^m-SC Case

Figure 5.8 shows the symbol error rates for the expurgated ensemble $\mathrm{ELDPC}(315, \mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}}), x, x^2, 2, 8, \mathcal{H})$ transmitted over the 2^4-SC for $m_3 = 1, m_4 = 4, \mathcal{H} = \{\}$ ($\mathbb{F}_{2^4}$ Random), for $m_3 = 1, m_4 = 4, \mathcal{H} = \mathcal{H}_{1,4}$ ($\mathbb{F}_{2^4}$ Proposed), for $m_3 = 4, m_4 = 1, \mathcal{H} = \{\}$ ($\mathrm{GL}(4, \mathbb{F}_2)$ 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 (5.7). From Figure 5.8, we see that the proposed codes exhibit better decoding performance than non-optimized code. The lower bound (5.7) 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 optimized codes depend only on the size of $m_3 m_4$.

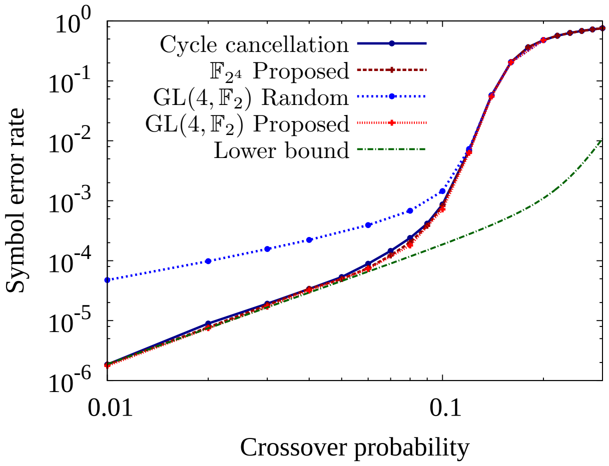

Figure 5.6: The symbol error rates for the expurgated ensemble ELDPC(315, GL($m_3, \mathbb{F}_{2^{m_4}}$), $x, x^2, 1, 8, \mathcal{H}$) transmitted over the BSC for $m_3 = 1, m_4 = 4, \mathcal{H} = \{1\}$ (Cycle cancellation), for $m_3 = 1, m_4 = 4, \mathcal{H} = \mathcal{H}_{1,4}$ ($\mathbb{F}_{2^4}$ Proposed), for $m_3 = 4, m_4 = 1, \mathcal{H} = \{\}$ (GL(4, $\mathbb{F}_2$) Random) and for $m_3 = 4, m_4 = 1, \mathcal{H} = \mathcal{H}_{4,1}$ (GL(4, $\mathbb{F}_2$) Proposed). The lower bound is given by (5.4).

Comparison with Stopping Set Mitigation

In [27], Poulliat et al. also proposed the *stopping set mitigation*. To lower the error floor further, Poulliat et al. proposed to use both the cycle cancellation and the stopping set mitigation. We refer to the Hamming weight of the binary represented non-binary codeword as binary weight. The stopping set mitigation is a method to design the labels on the edges, which are connecting to the nodes in the smallest stopping set, so that the binary minimum distance in the stopping sets takes the maximum value.

Figure 5.9 compares the symbol error rate for the codes designed by the proposed method and the codes designed by the method which uses both the cycle cancellation and the stopping set mitigation [27]. In order to make the stopping set mitigation work effectively, we employ as the base codes the codes whose Tanner graphs include many small stopping sets. For example, this condition is met by the code ensemble ELDPC($60, \mathbb{F}_{2^4}, x, x^3, 3$). By applying our proposed method and the method which uses both the cycle cancellation and stopping set mitigation, we get resulting codes which are the subsets of ELDPC($60, \mathbb{F}_{2^4}, x, x^3, 3$). We see Figure 5.9 that the symbol error rate for our proposed method is lower than that for the method using both the cycle cancellation and the stopping set mitigation.

5.4 Summary

We prove the relation between the orbit and the order of general linear group. In this chapter, we propose a method to lower the error floors for non-binary LDPC codes. The decoding error rates of the optimized codes is lower than that of the code optimized by cycle cancellation. We

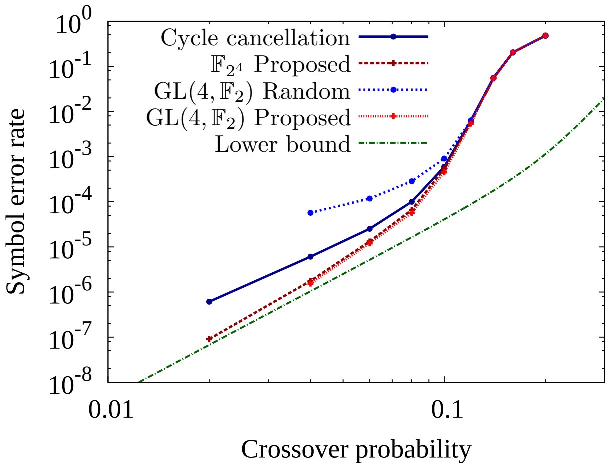

Figure 5.7: The symbol error rates for the expurgated ensemble ELDPC(315, GL$(m_3, \mathbb{F}_{2^{m_4}}), x, x^2, 2, 8, \mathcal{H})$ transmitted over the BSC for $m_3 = 1, m_4 = 4, \mathcal{H} = \{1\}$ (Cycle cancellation), for $m_3 = 1, m_4 = 4, \mathcal{H} = \mathcal{H}_{1,4}$ ($\mathbb{F}_{2^4}$ Proposed), for $m_3 = 4, m_4 = 1, \mathcal{H} = \{\}$ (GL$(4, \mathbb{F}_2)$ Random) and for $m_3 = 4, m_4 = 1, \mathcal{H} = \mathcal{H}_{4,1}$ (GL$(4, \mathbb{F}_2)$ Proposed). The lower bound is given by (5.4).

have shown lower bounds of the error floors for the expurgated LDPC code ensembles over the q-MS channel. In this analysis, we see that the optimized 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 in the edges which satisfy the condition for the optimization.

Appendix 5.A Proof of Lemma 13

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. To simplify the notations, we define $\iota_i := h_{i,i+1} h_{i,i}^{-1}$ for $i \in [1, w]$, where $h_{w+1,w} = h_{1,w}$. For all $x \in \mathbb{F}_{2^{m_4}}^{m_3}$ and $i \in [1, w]$, the unnormalized message for the zigzag cycle code of symbol code length w is written as follows:

$$\begin{aligned}
&\tilde{\Psi}_{i,i-1}^{(0)}(x) := C_i(x), \qquad \tilde{\Psi}_{i,i-1}^{(\ell+1)}(x) := C_i(x)\tilde{\Psi}_{i+1,i}^{(\ell)}\big(\iota_i^{-1}x\big),\\
&\tilde{\Psi}_{i,i}^{(0)}(x) := C_i(x), \qquad \tilde{\Psi}_{i,i}^{(\ell+1)}(x) := C_i(x)\tilde{\Psi}_{i-1,i-1}^{(\ell)}\big(\iota_{i-1}x\big),\\
&\tilde{D}_i^{(\ell+1)}(x) := C_i(x)\tilde{\Psi}_{i-1,i-1}^{(\ell)}\big(\iota_{i-1}x\big)\tilde{\Psi}_{i+1,i}^{(\ell)}\big(\iota_i^{-1}x\big),
\end{aligned}$$

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 $\gamma_0 = \gamma_w$. Then, for the zigzag cycle code, the message $D_i^{(\ell)}$ are written as follows:

$$D_i^{(\ell)}(x) = \frac{\tilde{D}_i^{(\ell)}(x)}{\sum_{x' \in \mathbb{F}_{2^{m_4}}^{m_3}} \tilde{D}_i^{(\ell)}(x')}.$$

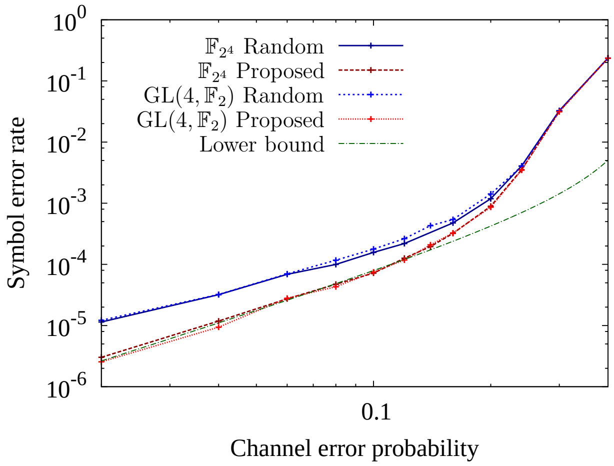

Figure 5.8: The symbol error rates for the expurgated ensemble ELDPC(315, GL($m_3, \mathbb{F}_{2^{m_4}}$), $x, x^2, 2, 8, \mathcal{H}$) transmitted over the 2^4-SC for $m_3 = 1, m_4 = 4, \mathcal{H} = \{\}$ ($\mathbb{F}_{2^4}$ Random), for $m_3 = 1, m_4 = 4, \mathcal{H} = \mathcal{H}_{1,4}$ ($\mathbb{F}_{2^4}$ Proposed), for $m_3 = 4, m_4 = 1, \mathcal{H} = \{\}$ (GL($4, \mathbb{F}_2$) Random) and for $m_3 = 4, m_4 = 1, \mathcal{H} = \mathcal{H}_{4,1}$ (GL($4, \mathbb{F}_2$) Proposed). The lower bound is given by (5.7).

From the definition, we have

$$\tilde{D}_i^{(\ell)}(x) = C_i(x) \prod_{k=1}^{\ell} \Big\{ C_{i-k}\left(\left(\prod_{j=1}^{k} \iota_{i+j-k-1}\right) x\right) C_{i+k}\left(\left(\prod_{j=1}^{k} \iota_{i-j+k}^{-1}\right) x\right)\Big\}, \tag{5.9}$$

where $C_{i+nw}(x) = C_i(x)$ and $\gamma_{i+nw} = \gamma_i$ for $n = 0, \pm 1, \dots$. For $x \in \mathbb{F}_{2^{m_4}}^{m_3}$, (5.9) gives the following equation

$$\tilde{D}_i^{(\ell + w\sigma_\chi)}(x) = \tilde{D}_i^{(\ell)}(x) \prod_{k=1}^{w\sigma_\chi} \Big\{ C_{i-k}\left(\left(\prod_{j=1}^{k} \iota_{i+j-k-1}\right) x\right) C_{i+k}\left(\left(\prod_{j=1}^{k} \iota_{i-j+k}^{-1}\right) x\right)\Big\}. \tag{5.10}$$

where σ_χ is the order of the matrix χ, i.e., σ_χ is the smallest positive integer such that χ^{σ_χ} is $m_3 \times m_3$ identity matrix. The the production of (5.10) are transformed as follows:

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

Note that $B(\kappa_i x) = B(\kappa_i x')$ holds for $\forall x \in S_\chi, \forall x' \in \langle \chi \rangle x$. Define

$$\kappa_i = \begin{cases} 1 & i = 1 \\ \prod_{j=1}^{i-1} \iota_j & i = 2, 3, \dots, w \end{cases},$$

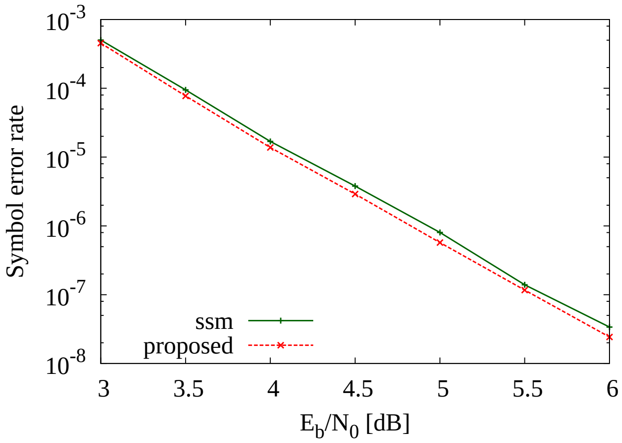

Figure 5.9: Comparison of the symbol error rate for the codes designed by the proposed method and the codes designed by the method which uses both the cycle cancellation and the stopping set mitigation. The base code ensemble is ELDPC$(60, \mathbb{F}_{2^4}, x, x^3, 3)$. The solid curve (proposed) shows the symbol error rate for the codes designed by our proposed method. The dotted curve (ssm) shows the symbol error rate for the codes designed by the method which uses both the cycle cancellation and the stopping set mitigation.

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, (5.9) are rewritten as for $x \in S_\chi$ and $i \in [1, w]$

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

For $\forall x \in S_\chi, \forall x' \in \langle\chi\rangle x$, $B(\kappa_i x) = B(\kappa_i x')$ holds. By using this equation, we have

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

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 $i \in [1, w]$,

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

Hence for $\ell_1 \geq 1$ and $i \in 1, 2, \ldots, w$

$$\begin{aligned}\tilde{D}_i^{(w\sigma_\chi \ell_1)}\left(\kappa_i^{-1}x\right)\tilde{D}_i^{(w\sigma_\chi \ell_1-1)}\left(\kappa_i^{-1}x\right) &= B(x)^{4\ell_1\sigma_\chi/|\langle\chi\rangle x|}\\ &= B(0)^{4\ell_1\sigma_\chi/|\langle\chi\rangle x|} = \tilde{D}_i^{(w\sigma_\chi \ell_1)}(0)\tilde{D}_i^{(w\sigma_\chi \ell_1-1)}(0). \quad (5.11)\end{aligned}$$

The i-th symbol is eventually correct if there exist L such that $\tilde{D}_i^{(\ell)}(0) > \tilde{D}_i^{(\ell)}(x)$ for $\ell > L$ and $x \in \mathbb{F}_{2^m_4}^{m_3} \setminus \{0\}$. However, from (5.11), for all $i \in [1, w]$, if $\tilde{D}_i^{(w\sigma_\chi \ell_1-1)}(0) > \tilde{D}_i^{(w\sigma_\chi \ell_1-1)}(\kappa_i^{-1}x)$, then $\tilde{D}_i^{(w\sigma_\chi \ell_1)}(0) < \tilde{D}_i^{(w\sigma_\chi \ell_1)}(\kappa_i^{-1}x)$. Thus, no symbols are eventually correct. (Q.E.D.)

Appendix 5.B Proof of Lemma 14

We use the following lemma in order to prove Lemma 14.

Lemma 16 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 $\mathbb{F}_{2^{m_4}}$. 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 $\mathrm{ord}(f)$. 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 $m_3 \times m_3$ nonsingular matrix, $f_\chi(0) \neq 0$. By the Cayley-Hamilton theorem, $f_\chi(\chi) = 0$. The definition of the order $\mathrm{ord}(f_\chi)$ of polynomial f_χ gives $f_\chi(x) \mid x^{\mathrm{ord}(f_\chi)} - 1$. 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 $\mathrm{ord}(f_\chi) \leq 2^{m_3m_4} - 1$ by using [28, Corollary 3.4], $\mathrm{ord}(f_\chi) = 2^{m_3m_4} - 1$ if $\sigma_\chi = 2^{m_3m_4} - 1$. (Q.E.D.)

By using this lemma, the proof of Lemma 14 is given as follows.

proof of Lemma 14: Firstly, we assume $|S_\chi| = 1$. We denote the first column of χ^j, by χ_1^j. Since $|S_\chi| = 1$,

$$\begin{aligned}\mathbb{F}_{2^{m_4}}^{m_3} \setminus \{0\} =& \{\chi^j(1, 0, 0, \ldots, 0)^T \mid j = 0, 1, \ldots, 2^{m_3m_4} - 2\}\\ =& \{\chi_1^j \mid j = 0, 1, \ldots, 2^{m_3m_4} - 2\}.\end{aligned}$$

This equation asserts that $\chi_1^i \neq \chi_1^j$ for $i \neq j$ and $i, j \in [0, 2^{m_3m_4} - 2]$. Hence, for $i \neq j$ and $i, j \in [0, 2^{m_3m_4} - 2]$, $\chi^i \neq \chi^j$. Thus, the order of χ is equal to or greater than $2^{m_3m_4} - 1$. For $\forall\chi \in \mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}})$, the order of χ is equal to or lower than $2^{m_3m_4} - 1$, i.e., $\sigma_\chi \leq 2^{m_3m_4} - 1$ [31, Corollary 2]. Therefore, $\sigma_\chi = 2^{m_3m_4} - 1$ if $|S_\chi| = 1$.

Secondly, we assume $\sigma_\chi = 2^{m_3m_4-1}$. By Lemma 16, the order of characteristic polynomial $f_\chi(x)$ is $2^{m_3m_4} - 1$. Since $\mathrm{ord}(f_\chi) = 2^{m_3m_4} - 1$, $f(0) \neq 0$ and $f(x)$ is *monic polynomial* [28, Definition 1.49], the characteristic polynomial $f_\chi(x)$ is a *primitive polynomial* [28, Theorem 3.16]. Hence, the field $\mathbb{F}_{2^{m_3 m_4}}$ is represented in $\{0\} \cup \{\chi^i \mid i = 0, 1, \ldots, 2^{m_3 m_4} - 2\}$. Thus, if $\forall i, j \in [0, 2^{m_3 m_4} - 2]$ and $i \neq j$, there exists a $k \in [0, 2^{m_3 m_4} - 2]$ such that $\chi^i + \chi^j = \chi^k$. This implies that $\chi_1^i \neq \chi_1^j$ if $\forall i, j \in [0, 2^{m_3 m_4} - 2]$ and $i \neq j$. Therefore, $|S_\chi| = 1$ since $\mathbb{F}_{2^{m_4}}^{m_3} \setminus \{0\} = \langle \chi \rangle (1, 0, \ldots, 0)^T$. (Q.E.D.)

Appendix 5.C Proof of Lemma 15

proof: The Q-function is represented as follows [32]:

$$Q(x) = \frac{1}{\pi} \int_0^{\frac{\pi}{2}} \exp\left[-\frac{x^2}{2\sin^2\theta}\right] d\theta.$$

By using this equation, (5.8) is rewritten by

$$f(m, w_{\mathrm{g}}) = \frac{1}{2n} \frac{m 2^{m-1}}{2^m - 1} \sum_{w = w_{\mathrm{g}}}^{\infty} \mu^w \frac{1}{\pi} \int_0^{\frac{\pi}{2}} \exp\left[-\frac{mw}{2\sigma^2 \sin^2\theta}\right] d\theta.$$

To simplify notation, we define the following substitution:

$$\tau_{\theta,\sigma} := \exp\left[-\frac{1}{2\sigma^2 \sin^2\theta}\right].$$

Note that

$$\mu\tau_{\theta,\sigma} \leq \mu \exp\left[-\frac{1}{2\sigma^2}\right] < 1,$$

since $\sigma < \sqrt{\frac{1}{2\ln\mu}}$ holds for $m = 1, 2, \ldots$. This substitution simplifies $f(m, w_{\mathrm{g}})$ as

$$\begin{aligned}
f(m, w_{\mathrm{g}}) =& \frac{1}{2n} \frac{m 2^{m-1}}{2^m - 1} \sum_{w = w_{\mathrm{g}}}^{\infty} \mu^w \frac{1}{\pi} \int_0^{\frac{\pi}{2}} \tau_{\theta,\sigma}^{mw} d\theta \\
=& \frac{1}{2n} \frac{m 2^{m-1}}{2^m - 1} \frac{1}{\pi} \int_0^{\frac{\pi}{2}} \sum_{w = w_{\mathrm{g}}}^{\infty} \mu^w \tau_{\theta,\sigma}^{mw} d\theta \\
=& \frac{1}{2n} \frac{m 2^{m-1}}{2^m - 1} \frac{1}{\pi} \int_0^{\frac{\pi}{2}} \frac{\mu^{w_{\mathrm{g}}} \tau_{\theta,\sigma}^{m w_{\mathrm{g}}}}{1 - \mu \tau_{\theta,\sigma}^m} d\theta.
\end{aligned}$$

This equation leads the following:

$$f(m, w_{\mathrm{g}}) - f(m+1, w_{\mathrm{g}}) = \frac{1}{2n} \frac{\mu^{w_{\mathrm{g}}}}{\pi} \int_0^{\frac{\pi}{2}} \frac{2^{m-1} \tau_{\theta,\sigma}^{m w_{\mathrm{g}}}}{(2^m - 1)(1 - \mu \tau_{\theta,\sigma}^m)} \frac{g(m, w_{\mathrm{g}}, \tau_{\theta,\sigma})}{(2^{m+1} - 1)(1 - \mu \tau_{\theta,\sigma}^{m+1})} d\theta,$$

where

$$g(m, w_{\mathrm{g}}, \tau_{\theta,\sigma}) := m(2^{m+1} - 1)(1 - \mu \tau_{\theta,\sigma}^{m+1}) - 2(m+1) \tau_{\theta,\sigma}^{w_{\mathrm{g}}} (2^m - 1)(1 - \mu \tau_{\theta,\sigma}^m).$$

Note that $(1-\mu\tau_{\theta,\sigma}^{m+1}) > 0$ and $(1-\mu\tau_{\theta,\sigma}^{m}) > 0$, since $\tau_{\theta,\sigma} < 1$ and $\mu\tau_{\theta,\sigma} < 1$. Since $g(m, w_{\mathtt{g}}, \tau_{\theta,\sigma})$ increases in $w_{\mathtt{g}}$, $g(m, w_{\mathtt{g}}, \tau_{\theta,\sigma}) > g(m, 1, \tau_{\theta,\sigma})$ holds. For $\tau < \mu^{-1/m}$, $g(m, 1, \tau_{\theta,\sigma})$ decreases in $\tau_{\theta,\sigma}$. Hence, the function $g(m, w_{\mathtt{g}})$ is bounded as

$$g(m, w_{\mathtt{g}}, \tau_{\theta,\sigma}) \geq g(m, 1, \tau_{\theta,\sigma}) > g(m, 1, \mu^{-1/m}) = m(2^{m+1} - 1)(1 - \mu^{-1/m}) > 0.$$

Thus, we get $f(m, w_{\mathtt{g}}) > f(m+1, w_{\mathtt{g}})$. (Q.E.D.)

Chapter 6

Analysis of Stopping Constellation Distribution for Irregular Non-Binary LDPC Code Ensemble

The fixed points of the belief propagation decoder for non-binary LDPC codes are referred to as stopping constellations. In this chapter, we give the stopping constellation distributions for the irregular non-binary LDPC code ensembles defined over the general linear group. Moreover, we derive the exponential growth rate of the average stopping constellation distributions in the limit of large codelength.

6.1 Introduction

In this chapter, we consider the non-binary LDPC codes defined over general linear group. It is known that LDPC codes defined over the general linear groups outperform LDPC codes defined over finite fields in terms of the decoding performance [29].

The block and the bit erasure probabilities for binary LDPC codes over the BEC are determined by the size of the maximal stopping set [33]. The fixed points of the BP decoder for non-binary LDPC codes are referred to as stopping constellations [17]. Hence, the stopping constellations for the non-binary LDPC codes correspond to the stopping sets for the binary LDPC codes. To analyze the decoding erasure probabilities of the non-binary LDPC codes over the BEC by the BP decoder, we need to analyze the stopping constellation. In this chapter, Moreover, we derive the stopping constellation distribution. In this chapter, we also give the exponential growth rates of the average stopping constellation distributions in the limit of large code length.

The remainder of this chapter is organized as follows. In Section 6.2, we derive the stopping constellation distributions for irregular non-binary LDPC code ensembles. In Section 6.3, we derive the exponential growth rates of the average stopping constellation distributions in the limit of large code length. In Section 6.4, we show the numerical examples for the exponential growth rates of the average number of stopping constellation distributions.

6.2 Stopping Constellation Distribution for Non-Binary LDPC Codes

In this section, we derive the stopping constellation distributions for irregular non-binary LDPC code ensembles. We give some lemmas to count constellations of the linear subspaces satisfying the stopping constellation constraints (2.2) for check nodes.

6.2.1 Number of Linear Subspaces

It is known that the number of distinct subspaces of dimension k of the vector space $\mathbb{F}_2^m$ is given by the Gaussian binomial coefficient [11, p. 443]. The Gaussian binomial coefficient $\begin{bmatrix} m \\ k \end{bmatrix}$ is given by

$$\begin{bmatrix} m \\ k \end{bmatrix} = \frac{[m]}{[m-k][k]},$$

where $[m]$ is defined in Section 2.1.2. We denote the dimension of V_i, by $\dim V_i$. The following lemma gives the number of the sets of linear subspaces $\{V_i\}_{i=1}^k$ for a given condition for the dimension of $\{V_i\}_{i=1}^k$.

Lemma 17 Assume that two non-negative integers k, m are given. For a given set of non-negative integers $\boldsymbol{a}_k = \{a_k(S)\}_{S\subseteq[1,k]}$ such that $\sum_{S\subseteq[1,k]} a_k(S) = m$, let $B_k(\boldsymbol{a}_k)$ be the number of the sets of linear subspaces $\{V_i\}_{i=1}^k$ in $\mathbb{F}_2^m$ which satisfy

$$\dim\left(\bigcap_{i\in S} V_i\right) = \sum_{\tilde{S}\subseteq[1,k]:S\subseteq\tilde{S}} a_k(\tilde{S}), \tag{6.1}$$

where $\sum_{\tilde{S}\subseteq[1,k]:S\subseteq\tilde{S}} a_k(\tilde{S})$ is the sum of $a_k(\tilde{S})$ over all $\tilde{S} \subseteq [1,k]$ such that $S \subseteq \tilde{S}$. Then, we have

$$B_k(\boldsymbol{a}_k) = \frac{[m]}{\prod_{S\subseteq[1,k]}[a_k(S)]} 2^{T_k}, \tag{6.2}$$

where

$$T_k := \frac{1}{2} \sum_{\substack{S_1,S_2\subseteq[1,k]: \\ S_1\not\subseteq S_2, S_1\not\supseteq S_2}} a_k(S_1)a_k(S_2).$$

The proof of this lemma is in Appendix 6.A.

Lemma 18 Assume that two non-negative integers k, m are given. Define $B_k(\boldsymbol{a}_k)$ as in (6.2). For a given set of non-negative integers $\boldsymbol{v} = \{v_i\}_{i=1}^k$ where $v_i \in [0,m]$ for all $i \in [1,k]$, we denote the number of the sets of linear subspaces $\{V_i\}_{i=1}^k$ such that $V_i \supseteq \bigcap_{j\in[1,k]\setminus\{i\}} V_j$ and $\dim V_i = v_i$ for all $i \in [1,k]$, by $\tilde{h}_k(\boldsymbol{v})$, i.e.,

$$\tilde{h}_k(\boldsymbol{v}) := \#\left\{ \{V_i\}_{i=1}^k \mid V_i \supseteq \bigcap_{j\in[1,k]\setminus\{i\}} V_j \ \forall i \in [1,k], \dim V_i = v_i \ \forall i \in [1,k] \right\}.$$

Then,

$$\tilde{h}_k(\boldsymbol{v}) = \sum_{\boldsymbol{a}_k \in \mathcal{W}_k'} B_k(\boldsymbol{a}_k),$$

where

$$\mathcal{W}_k' := \left\{ \boldsymbol{a}_k \mid \sum_{S:i\in S} a_k(S) = \dim V_i \quad \forall i \in [1,k], \sum_{S\subseteq[1,k]} a_k(S) = m, \right.$$
$$\left. a_k([1,k]\setminus\{i\}) = 0 \quad \forall i \in [1,k] \right\}.$$

The proof is in Appendix 6.B.

Discussion 9 Assume that two non-negative integers k, m are given. For a given $\boldsymbol{d} = (d_0, \ldots, d_m)$ such that $\sum_{i=0}^m d_i = k$ and $d_i \geq 0$ for $i \in [0,m]$, we denote the number of the sets of linear subspaces $\{V_i\}_{i=1}^k$ such that $V_i \supseteq \bigcap_{j\in[1,k]\setminus\{i\}} V_j$ for all $i \in [1,k]$ and the number of subspaces in $\{V_j\}_{j=1}^k$ with dimension $m-i$ is d_i, by $h_k(\boldsymbol{d})$, i.e.,

$$h_k(\boldsymbol{d}) := \#\left\{ \{V_j\}_{j=1}^k \mid V_i \supseteq \bigcap_{j\in[1,k]\setminus\{i\}} V_j \ \forall i \in [1,k], \#\{i \mid \dim V_i = j\} = d_j \ \forall j \in [1,m] \right\}.$$

There are $\binom{k}{d_0, d_1, \ldots, d_m}$ choices to the dimensions of $\{V_i\}_{i=1}^k$, where

$$\binom{k}{d_0, d_1, \ldots, d_m} := \frac{k!}{\prod_{i=0}^m d_i!}, \quad k = \sum_{i=0}^m d_i,$$

is known as the multinomial coefficient [34]. From Lemma 18, we have for any permutation π on k and $\{v_i\}_{i=1}^k$

$$\tilde{h}_k(\{v_i\}_{i=1}^k) = \tilde{h}_k(\{v_{\pi(i)}\}_{i=1}^k).$$

For $j \in [1,m]$, let p_j be the smallest integer such that $j \leq \sum_{i=0}^{p_j} d_i$. Hence, we get

$$h_k(\boldsymbol{d}) = \binom{k}{d_0, d_1, \ldots, d_m} \tilde{h}_k(\{v_i\}_{i=1}^k),$$

where $v_i = m - p_i$ for all $i \in [i, k]$. Thus, we obtain

$$h_k(\boldsymbol{d}) = \binom{k}{d_0, d_1, \dots, d_m} \sum_{\boldsymbol{a}_k \in \mathcal{W}_k} B_k(\boldsymbol{a}_k),$$

where

$$\mathcal{W}_k := \Bigg\{ \boldsymbol{a}_k \mid \sum_{S: i \in S} a_k(S) = m - p_i \quad \forall i \in [1,k], \sum_{S \subseteq [1,k]} a_k(S) = m,$$
$$a_k([1,k] \setminus \{i\}) = 0 \quad \forall i \in [1,k] \Bigg\}.$$

We denote $\boldsymbol{d} \geq \boldsymbol{0}$ if $d_i \geq 0$ for all $i \in [0, m]$. The generator function of $h_k(\boldsymbol{d})$ is written as follows:

$$f_k(\boldsymbol{u}) := \sum_{\boldsymbol{d} \geq \boldsymbol{0} : \sum_{i=0}^m d_i = k} h_k(\boldsymbol{d}) \prod_{i=1}^m u_i^{d_i}. \tag{6.3}$$

Since d_0 depends on $d_1, d_2, \dots, d_m$, i.e., $d_0 = k - \sum_{i=1}^m d_i$, we drop u_0 from (6.3).

6.2.2 Stopping Constellation Distributions for Non-Binary LDPC Codes

Recall that for a given stopping constellation we refer to the number of the states whose dimensions are not equal to 0 as the weight of the stopping constellation. For a given Tanner graph $\mathtt{G} \in \mathrm{EGL}(N, m, \lambda, \rho)$, we denote the number of stopping constellations of weight w in $\mathtt{G}$ by $\Omega^{\mathtt{G}}(w)$. For the ensemble $\mathrm{EGL}(N, m, \lambda, \rho)$, let $\Omega(w)$ be the average stopping constellations of weight w. Since each code is chosen with equal probability from $\mathrm{EGL}(N, m, \lambda, \rho)$, we get

$$\Omega(w) = \sum_{\mathtt{G} \in \mathrm{EGL}(N,m,\lambda,\rho)} \frac{\Omega^{\mathtt{G}}(w)}{|\mathrm{EGL}(N, m, \lambda, \rho)|}.$$

The following theorem gives the average stopping constellations for irregular non-binary LDPC code ensembles.

Theorem 6 Define $f_k(\boldsymbol{u})$ as in (6.3). The average stopping constellations $\Omega(w)$ of weight w for the non-binary LDPC code ensemble $\mathrm{EGL}(N, m, \lambda, \rho)$ is given by

$$\Omega(w) = \sum_{\boldsymbol{b} \geq \boldsymbol{0} : \sum_{i=0}^m b_i = \xi} \frac{\mathrm{coef}\big((Q(\boldsymbol{s}, t) P(\boldsymbol{u}))^N, t^w \prod_{i=1}^m s_i^{b_i} u_i^{b_i}\big)}{\binom{\xi}{b_0, b_1, \dots, b_m} \prod_{k=1}^m \begin{bmatrix} m \\ k \end{bmatrix}^{b_k}}, \tag{6.4}$$

$$Q(\boldsymbol{s}, t) := \prod_{j \in \mathcal{L}} \left\{ 1 + t \sum_{i=1}^m \begin{bmatrix} m \\ i \end{bmatrix} s_i^j \right\}^{L_j},$$

$$P(\boldsymbol{u}) := \prod_{k \in \mathcal{R}} \{ f_k(\boldsymbol{u}) \}^{R_k(1-r)},$$

where $\mathrm{coef}(g(\boldsymbol{s},t,\boldsymbol{u}), t^w \prod_{i=1}^m s_i^{b_i} u_i^{b_i})$ is the coefficient of the term $t^w \prod_{i=1}^m s_i^{b_i} u_i^{b_i}$ in the polynomial $g(\boldsymbol{s},t,\boldsymbol{u})$.

proof: First, we count constellations of the linear subspaces satisfying the stopping constellation constraint (2.2) for all check nodes. Consider a check node $\mathtt{c}$ of degree k. We say that the check node $\mathtt{c}$ satisfies the decoding failure criterion with respect to the state assignment $\{E_{\mathtt{v}}\}_{\mathtt{v}\in\mathcal{V}}$ if

$$E_{\mathtt{v}} \subseteq h_{\mathtt{c},\mathtt{v}}^{-1} \left(\sum_{i\in\mathcal{N}_{\mathtt{c}}(\mathtt{c})\setminus\{\mathtt{v}\}} h_{\mathtt{c},i} E_i \right), \qquad \forall \mathtt{v} \in \mathcal{N}_{\mathtt{c}}(\mathtt{c}).$$

Substituting $\tilde{E}_i = h_{\mathtt{c},i}E_i$ to this, we have

$$\tilde{E}_{\mathtt{v}} \subseteq \left(\sum_{i\in\mathcal{N}_{\mathtt{c}}(\mathtt{c})\setminus\{\mathtt{v}\}} \tilde{E}_i \right), \qquad \forall \mathtt{v} \in \mathcal{N}_{\mathtt{c}}(\mathtt{c}).$$

For a linear subspace V, denote its dual subspace by $V^{\perp}$, i.e.,

$$V^{\perp} := \{\beta \mid \langle \alpha, \beta \rangle = 0 \ \forall \alpha \in V\},$$

where $\langle \alpha, \beta \rangle$ denotes the inner product of α and β. Using the dual subspaces, we have

$$\tilde{E}_{\mathtt{v}}^{\perp} \supseteq \left(\bigcap_{i\in\mathcal{N}_{\mathtt{c}}(\mathtt{c})\setminus\{\mathtt{v}\}} \tilde{E}_i^{\perp} \right), \qquad \forall \mathtt{v} \in \mathcal{N}_{\mathtt{c}}(\mathtt{c}).$$

We refer to the edges adjacent to the variable node assigned to state of dimension i as the edges of dimension i. Let d_i be the number of edges of dimension i which are adjacent to the check node $\mathtt{c}$. From Discussion 9, for a given $(d_0,\dots,d_m)$ such that $\sum_{i=0}^m d_i = k$ and $d_i \geq 0$ for all $i \in [0,m]$, the number of the constellations that satisfy the decoding failure criterion for the check node $\mathtt{c}$ is written as

$$\mathrm{coef}\left(f_k(\boldsymbol{u}), \prod_{i=1}^m u_i^{d_i} \right).$$

Let b_i be the total number of edges of dimension i. Since there are $R_k(1-r)N$ check nodes of degree k, the number of the constellations that satisfy the stopping constellation constraints for the $N(1-r)$ check nodes for a given $\boldsymbol{b} = (b_0,\dots,b_m)$ such that $\sum_{i=0}^m b_i = \xi$ and $b_i \geq 0$ for all $i \in [0,m]$, is

$$\mathrm{coef}\left(\prod_{k\in\mathcal{R}} (f_k(\boldsymbol{u}))^{R_k(1-r)N}, \prod_{i=1}^m u_i^{b_i} \right). \tag{6.5}$$

Secondly, we count constellations of linear subspaces satisfying the constraints of the variable nodes. Consider a variable node $\mathtt{v}$ of degree k. If the variable node $\mathtt{v}$ is assigned to state of dimension i, the k edges adjacent to $\mathtt{v}$ are of dimension i. Define the parameter w as 1 if the dimension of the state of the variable node $\mathtt{v}$ is not 0, and otherwise 0. Denote the number of edges of dimension i adjacent to the variable node $\mathtt{v}$, by d_i. For a given $w \in \{0,1\}$ and $\boldsymbol{d} = (d_0, \dots, d_m)$ such that $\sum_{i=0}^m d_i = k$ and $d_i \geq 0$ for all $i \in [0, m]$, let $g_k(w, \boldsymbol{d})$ be the number of constellations of linear subspaces satisfying a constraint of variable node of degree k. Since the number of states of dimension i is $\begin{bmatrix} m \\ i \end{bmatrix}$, we have

$$g_k(w, \boldsymbol{d}) = \begin{cases} 1 & w = 0, d_0 = k, d_j = 0 \ \forall j \in [1, m], \\ \begin{bmatrix} m \\ i \end{bmatrix} & w = 1, d_i = k, d_j = 0 \ \forall j \in [0, m] \setminus \{i\}, \\ 0 & \text{otherwise.} \end{cases}$$

The generator function of $g_k(w, \boldsymbol{d})$ is written as follows:

$$\sum_{w, \boldsymbol{d}} g_k(w, \boldsymbol{d}) t^w \prod_{i=1}^m s_i^{d_i} = 1 + t \sum_{i=1}^m \begin{bmatrix} m \\ i \end{bmatrix} s_i^k.$$

Since there are $L_k N$ variable nodes of degree k, for a given w and $\boldsymbol{b}$ such that $\sum_{i=0}^m b_i = \xi$ and $b_i \geq 0$ for all $i \in [0, m]$, the number of constellations of linear subspaces satisfying constraints of the N variable nodes is given by

$$\operatorname{coef}\left(\prod_{k \in \mathcal{L}} \left(1 + t \sum_{i=1}^m \begin{bmatrix} m \\ i \end{bmatrix} s_i^k \right)^{L_k N}, t^w \prod_{i=1}^m s_i^{b_i} \right). \tag{6.6}$$

Thirdly, we count the edge permutation and the edge labels which satisfy the constellation. For a given $\boldsymbol{b}$ such that $\sum_{i=0}^m b_i = \xi$ and $b_i \geq 0$ for all $i \in [0, m]$, the number of permutations of edges is given by $\prod_{i=0}^m b_i!$ and the number of edge labels is equal to $\prod_{i=0}^m ([m-i][i])^{b_i}$. Hence, for a given $\boldsymbol{b}$ such that $\sum_{i=0}^m b_i = \xi$ and $b_i \geq 0$ for all $i \in [0, m]$, the number of choices for the permutations of edges and edge labels is

$$\prod_{i=0}^m b_i! ([m-i][i])^{b_i}. \tag{6.7}$$

Finally, the number of Tanner graphs in $\mathrm{EGL}(N, m, \lambda, \rho)$ is given by $\xi! [m]^\xi$. From (6.5), (6.6) and (6.7) and the number of Tanner graphs, the average stopping constellation distribution for a given w and $\boldsymbol{b}$ such that $\sum_{i=0}^m b_i = \xi$ and $b_i \geq 0$ for all $i \in [1, m]$, is given by

$$\Omega(w, \boldsymbol{b}) = \frac{\operatorname{coef}\Big((Q(\boldsymbol{s}, t) P(\boldsymbol{u}))^N, t^w \prod_{i=1}^m s_i^{b_i} u_i^{b_i} \Big)}{\binom{\xi}{b_0, b_1, \dots, b_m} \prod_{k=1}^m \begin{bmatrix} m \\ k \end{bmatrix}^{b_k}}.$$

Since

$$\Omega(w) = \sum_{\boldsymbol{b} \geq \boldsymbol{0} : \sum_{i=0}^m b_i = \xi} \Omega(w, \boldsymbol{b}),$$

we get Theorem 6. (Q.E.D.)

6.3 Asymptotic Analysis

In this section, we investigate the asymptotic behavior of the average stopping constellation distributions of non-binary LDPC code ensembles in the limit of large code length. Define the *normalized* weight ω by $\omega := w/N$. We define

$$\Gamma_m(\omega) := \lim_{N\to\infty} \frac{1}{N} \log_2 \Omega(\omega N),$$

and refer to this as the *exponential growth rate* or simply *growth rate* of the average stopping constellation distribution. To simplify the notation, we denote logarithms to base 2 as log.

With the growth rate, we can roughly estimate the number of stopping constellations by

$$\Omega(\omega N) \sim 2^{\Gamma_m(\omega)N},$$

where $a_N \sim b_N$ means that $\lim_{N\to\infty} \frac{1}{N} \log \frac{a_N}{b_N} = 0$.

The number of the terms in (6.4) is at most $(\xi+1)^m$. Hence, from (6.4) we have

$$\max_{\boldsymbol{b}\geq\boldsymbol{0}:\sum_{i=0}^{m} b_i=\xi} \Omega(w,\boldsymbol{b}) \leq A(w) \leq (\xi+1)^m \max_{\boldsymbol{b}\geq\boldsymbol{0}:\sum_{i=0}^{m} b_i=\xi} \Omega(w,\boldsymbol{b}).$$

Therefore, we get

$$\lim_{N\to\infty} \frac{1}{N} \log \Omega(w) = \lim_{N\to\infty} \frac{1}{N} \log \max_{\boldsymbol{b}\geq\boldsymbol{0}:\sum_{i=0}^{m} b_i=\xi} \Omega(w,\boldsymbol{b}).$$

To calculate this equation, we introduce the following lemma.

Lemma 19 [35, Theorem 2] Let $\gamma > 0$ be some rational number and let $p(x_1, x_2, \ldots, x_m)$ be a function such that $p(x_1, x_2, \ldots, x_m)^\gamma$ is a multivariate polynomial with non-negative coefficients. Let $\alpha_k > 0$ be some rational numbers for $k \in [1, m]$ and let n_i be the series of all indices j such that j/γ is an integer and $\mathrm{coef}(p(x_1,\ldots,x_m)^j, x_1^{\alpha_1 j}\cdots x_m^{\alpha_m j}) \neq 0$. Then

$$\lim_{i\to\infty} \frac{1}{n_i} \log \mathrm{coef}(p(x_1,\ldots,x_m)^{n_i}, (x_1^{\alpha_1}\cdots x_m^{\alpha_m})^{n_i}) = \inf_{x_1,\ldots,x_m>0} \log \frac{p(x_1,\ldots,x_m)}{x_1^{\alpha_1}\cdots x_m^{\alpha_m}}.$$

A point $(x_1, \ldots, x_m)$ achieves the minimum of the function

$$\frac{p(x_1,\ldots,x_m)}{(x_1^{\alpha_1}\ldots x_m^{\alpha_m})},$$

if and only if it satisfies the following equation for all $k \in [1, m]$:

$$x_k \frac{\partial p(x_1,\ldots,x_m)^\gamma}{\partial x_k} - \gamma\alpha_k p(x_1,\ldots,x_m)^\gamma = 0.$$

Define $\beta_i := b_i/N$ for $i \in [0, m]$. Note that $\Lambda_{\mathrm{ave}} = \xi/N$. We denote $\boldsymbol{s} > \mathbf{0}$ if $s_i > 0$ for all $i \in [1, m]$. From Theorem 6 and Lemma 19, we obtain the following theorem.

Theorem 7 The growth rate $\Gamma_m(\omega)$ of the average stopping constellation distributions for the irregular non-binary LDPC code ensemble $\mathrm{EGL}(N, m, \lambda, \rho)$ is given by

$$\begin{aligned}\Gamma_m(\omega) = &\sup_{\substack{\boldsymbol{\beta}>\mathbf{0}:\\ \sum_{i=0}^m \beta_i=\Lambda_{\mathrm{ave}}}} \inf_{\substack{\boldsymbol{s}>\mathbf{0},t>0,\\ \boldsymbol{u}>\mathbf{0}}} \Bigg\{ \log Q(\boldsymbol{s}, t) - \omega \log t + \log P(\boldsymbol{u}) - \sum_{i=1}^m \beta_i \log \begin{bmatrix} m \\ i \end{bmatrix} s_i u_i \\ &\qquad\qquad + \sum_{i=0}^m \beta_i \log \frac{\beta_i}{\Lambda_{\mathrm{ave}}} \Bigg\} \qquad (6.8) \\ =: &\sup_{\boldsymbol{\beta}>\mathbf{0}:\sum_{i=0}^m \beta_i=\Lambda_{\mathrm{ave}}} \inf_{\boldsymbol{s}>\mathbf{0},t>0,\boldsymbol{u}>\mathbf{0}} \hat{\Gamma}_m(\omega, \boldsymbol{\beta}, \boldsymbol{s}, t, \boldsymbol{u}) \\ =: &\sup_{\boldsymbol{\beta}>\mathbf{0}:\sum_{i=0}^m \beta_i=\Lambda_{\mathrm{ave}}} \tilde{\Gamma}_m(\omega, \boldsymbol{\beta}).\end{aligned}$$

A point $(\boldsymbol{u}, t, \boldsymbol{s})$ which achieves the minimum of the function $\hat{\Gamma}_m(\omega, \boldsymbol{\beta}, \boldsymbol{s}, t, \boldsymbol{u})$ is given in a solution of the following equations for all $i \in [1, m]$:

$$\beta_i = \frac{s_i}{Q}\frac{\partial Q}{\partial s_i} = \sum_{j \in \mathcal{L}} L_j \frac{j \begin{bmatrix} m \\ i \end{bmatrix} t s_i^j}{1 + t \sum_{k=1}^m \begin{bmatrix} m \\ k \end{bmatrix} s_k^j}, \qquad (6.9)$$

$$\omega = \frac{t}{Q}\frac{\partial Q}{\partial t} = \sum_{j \in \mathcal{L}} L_j \frac{t \sum_{i=1}^m \begin{bmatrix} m \\ i \end{bmatrix} s_i^j}{1 + t \sum_{k=1}^m \begin{bmatrix} m \\ k \end{bmatrix} s_k^j}, \qquad (6.10)$$

$$\beta_i = \frac{u_i}{P}\frac{\partial P}{\partial u_i} = \sum_{k \in \mathcal{R}} R_k (1-r) \frac{u_i}{f_k(\boldsymbol{u})}\frac{\partial f_k}{\partial u_i}, \qquad (6.11)$$

where

$$\frac{\partial f_k}{\partial u_i} = \sum_{\boldsymbol{d}\geq\mathbf{0}:\sum_j d_j = k} \binom{k}{d_0, \ldots, d_k} \frac{d_i}{u_i} \prod_{j=1}^m u_j^{d_j} \sum_{\boldsymbol{a}_k \in D_k} B_k(\boldsymbol{a}_k).$$

The point $\boldsymbol{\beta}$ which gives the maximum of $\Gamma_m(\omega, \boldsymbol{\beta})$ needs to satisfy the stationary condition

$$s_k u_k \begin{bmatrix} m \\ k \end{bmatrix} \left(\Lambda_{\mathrm{ave}} - \sum_{i=1}^m \beta_i \right) = \beta_k, \qquad (6.12)$$

for $k = 1, 2, \ldots, m$.

Lemma 20 For a given degree distribution pair (λ, ρ), we have $\Gamma_m(\omega) \geq \Gamma_1(\omega)$.

proof: We consider a fixed ω. Define β^* such that $\Gamma_1(\omega) = \tilde{\Gamma}_1(\omega, \beta^*)$. Note that

$$\begin{aligned}\tilde{\Gamma}_1(\omega, \beta^*) = \inf_{\substack{s_1>0,t>0,\\ u_1>0}} \Bigg[& \sum_{j\in\mathcal{L}} \log\Big(1+ts_1^j\Big)^{L_j} + \sum_{j\in\mathcal{R}} \log\Big\{\tilde{f}_k^{(1)}(u_1)\Big\}^{R_j(1-r)} \\ & + \Lambda_{\text{ave}} \log\frac{\Lambda_{\text{ave}}-\beta^*}{\Lambda_{\text{ave}}} - \beta^* \log\frac{s_1u_1(\Lambda_{\text{ave}}-\beta^*)}{\beta^*} - \omega\log t\Bigg],\end{aligned} \tag{6.13}$$

where $\tilde{f}_k^{(1)}(u_1) = \{(1+u_1)^j - ju_1\}$. For $m > 1$, define $\boldsymbol{\beta}^{(m)}(\delta) := (\delta, \ldots, \delta, \beta^* - (m-1)\delta)$. For any $\delta > 0$, we have

$$\Gamma_m(\omega) \geq \tilde{\Gamma}_m\big(\omega, \boldsymbol{\beta}^{(m)}(\delta)\big).$$

Now, we consider $\tilde{\Gamma}_m(\omega, \boldsymbol{\beta}^{(m)}(\delta))$ for $\delta \to 0$. For $\delta \to 0$, we have $s_i \to 0$ and $u_i \to 0$ for $i \in [1, m-1]$ from (6.9) and (6.11). Note that $f_k(\boldsymbol{u}) = (1+u_m)^k - ku_m = f_k^{(1)}(u_m)$ for $u_i \to 0$ $\forall i \in [1, m-1]$. Hence we have

$$\begin{aligned}&\lim_{\delta\to 0} \tilde{\Gamma}_m(\omega, \boldsymbol{\beta}^{(m)}(\delta)) \\ &\quad = \inf_{\substack{s_m>0,t>0,\\ u_m>0}} \Bigg\{ \sum_{j\in\mathcal{L}} \log\Big(1+ts_m^j\Big)^{L_j} + \sum_{j\in\mathcal{R}} \log\Big\{\tilde{f}^{(1)}(u_m)\Big\}^{R_j(1-r)} \\ &\qquad\qquad + \Lambda_{\text{ave}} \log\frac{\Lambda_{\text{ave}}-\beta^*}{\Lambda_{\text{ave}}} - \beta^* \log\frac{s_mu_m(\Lambda_{\text{ave}}-\beta^*)}{\beta^*} - \omega\log t\Bigg\}.\end{aligned}$$

This equation coincides with (6.13). Hence, we have $\Gamma_m(\omega) \geq \Gamma_1(\omega)$. (Q.E.D.)

Lemma 21 For t such that $t > 0$, (6.9), (6.10) and (6.11) hold, we have

$$\frac{d\Gamma_m(\omega)}{d\omega} = -\log t.$$

proof: Consider $\frac{d\Gamma_m(\omega)}{d\omega}$. From (6.8), we have

$$\begin{aligned}\frac{d\Gamma_m(\omega)}{d\omega}\ln 2 = & -\ln t + \frac{1}{P}\frac{dP}{d\omega} - \frac{\omega}{t}\frac{dt}{d\omega} + \frac{1}{Q}\frac{dQ}{d\omega} - \sum_{i=1}^m \frac{\beta_i}{s_i}\frac{ds_i}{d\omega} - \sum_{i=1}^m \frac{\beta_i}{u_i}\frac{du_i}{d\omega} \\ & - \sum_{i=1}^m \frac{d\beta_i}{d\omega} \ln s_iu_i \begin{bmatrix} m \\ i \end{bmatrix} \frac{\Lambda_{\text{ave}} - \sum_{i=1}^m \beta_i}{\beta_i}.\end{aligned}$$

From (6.12), we have

$$\ln\left\{ s_iu_i \begin{bmatrix} m \\ i \end{bmatrix} \frac{\Lambda_{\text{ave}} - \sum_{i=1}^m \beta_i}{\beta_i} \right\} = 0.$$

From (6.11), we have

$$\frac{1}{P}\frac{\partial P}{\partial \omega} = \frac{1}{P}\sum_{i=1}^{m}\frac{\partial P}{\partial u_i}\frac{du_i}{d\omega} = \sum_{i=1}^{m}\frac{\beta_j}{u_j}\frac{du_j}{d\omega}.$$

Similarly, from (6.9) and (6.10), we get

$$\frac{1}{Q}\frac{\partial Q}{\partial \omega} = \frac{\omega}{t}\frac{dt}{d\omega} + \sum_{i=1}^{m}\frac{\beta_i}{s_i}\frac{ds_i}{d\omega}.$$

Hence, we have

$$\frac{d\Gamma_m(\omega)}{d\omega} = -\log t.$$

This concludes the proof. (Q.E.D.)

The following theorem shows the growth rate of the average stopping constellation distributions for small ω.

Theorem 8 For the irregular non-binary LDPC code ensemble $\mathrm{EGL}(N, m, \lambda, \rho)$ with $\lambda'(0) > 0$, the growth rate of the average stopping constellation distributions of normalized weight ω, in the limit of large symbol code length for $\omega \to 0$, is given by

$$\Gamma_m(\omega) = \log[\lambda'(0)\rho'(1)]\omega + o(\omega).$$

proof: From the definition of stopping constellation, we get $\Omega(0) = 1$ and $\Gamma_m(0) = 0$. From Lemma 21, we have for $\omega \to 0$

$$\Gamma_m(\omega) = -\omega \log t(\omega) + o(\omega).$$

Recall that t satisfies (6.8), (6.9), (6.10) and (6.11). From (6.10), for $\omega \to 0$, it holds that $t_i s_i^j \to 0$ for $i \in [1, m]$ and $j \in \mathcal{L}$. By using this and (6.9), we have $\beta_i \to 0$ for $i \in [1, m]$. Note that

$$f_k(\boldsymbol{u}) = 1 + \sum_{i=1}^{m}\binom{k}{2}\begin{bmatrix} m \\ i \end{bmatrix} u_i^2 + o\left(\left(\sum_{i=1}^{m} u_i\right)^2\right). \tag{6.14}$$

Since $\beta_i \to 0$ for $i \in [1, m]$, from (6.11) we have $u_i \to 0$ for $i \in [1, m]$. From (6.11) and (6.14) we get

$$\beta_i = \sum_{k \in \mathcal{R}} R_k (1 - r) 2 \binom{k}{2}\begin{bmatrix} m \\ i \end{bmatrix} u_i^2 + o\left(\left(\sum_{i=1}^{m} u_i\right)^2\right).$$

Substituting this equation into (6.12), we have

$$s_i = u_i\rho'(1) + o\left(\sum_{i=1}^{m} u_i\right). \tag{6.15}$$

Since $u_i \to 0$ for $i \in [1,m]$, we get $s_i \to 0$ for $i \in [1,m]$. From (6.9), it holds that

$$\beta_i = 2L_2\begin{bmatrix} m \\ i \end{bmatrix} ts_i^2 + o\left(\left(\sum_{i=1}^{m} s_i\right)^2\right).$$

Substituting this equation into (6.12), we get

$$u_i = \lambda'(0)ts_i + o\left(\sum_{i=1}^{m} s_i\right). \tag{6.16}$$

From (6.15) and (6.16), we have for $\omega \to 0$

$$1 = \lambda'(0)\rho'(1)t(\omega).$$

Hence, we obtain this theorem. (Q.E.D.)

Discussion 10 From Theorem 8, the growth rate for $\omega \to 0$ does not depend on m. The result of Theorem 8 coincides with the result for the weight distribution of non-binary LDPC code ensemble [36]. More precisely, the growth rates of the stopping constellation distributions and that of the weight distributions are the same for $\omega \to 0$. The techniques used in the proofs of Theorem 8 and Lemma 21 are originally developed in [37].

Define the *critical exponent stopping ratio* [9] as

$$\theta_m^* := \inf\{\omega > 0 \mid \Gamma_m(\omega) \geq 0\}, \quad \text{for} \ \ m = 1, 2, \ldots.$$

From Lemma 20 and Theorem 8, we have the following corollary.

Corollary 6 For a given degree distribution pair (λ, ρ) which satisfies $\lambda'(0)\rho'(1) < 1$, the critical exponent stopping ratio θ_1^* is larger than others, namely, $\theta_1^* \geq \theta_m^*$ for $m > 1$.

Recall that the average stopping constellation of weight ωN is approximated by $\Omega(\omega N) \sim 2^{\Gamma_m(\omega)N}$. Since $\Gamma_m(\omega) < 0$ for $\omega \in (0, \theta_m^*)$, there are exponentially few stopping constellations of weight ωN for $\omega \in (0, \theta_m^*)$. It is known that the decoding erasure rate for the BEC with small channel erasure probability is caused by the stopping constellations of small weight. Therefore among LDPC codes with the degree distribution pair (λ, ρ) such that $\lambda'(0)\rho'(1) < 1$ over the BEC, we see from Corollary 6 that the *binary* ($m = 1$) LDPC code ensemble is the best in the sense that there are exponentially few stopping constellations of weight ωN for ω within the widest range $(0, \theta_1^*) \supseteq (0, \theta_m^*)$.

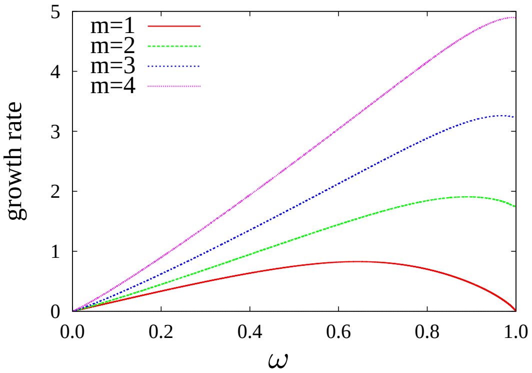

Figure 6.1: The growth rates of the average stopping constellation distributions for the (2,4)-regular non-binary LDPC code ensembles defined over $\mathrm{GL}(m, \mathbb{F}_2)$, where $m = 1, 2, 3, 4$.

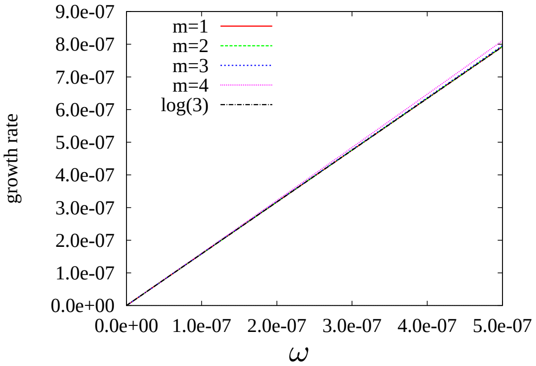

Figure 6.2: The growth rates for $\omega \in [0, 5 \times 10^{-7}]$ of the average stopping constellation distributions for the (2,4)-regular non-binary LDPC code ensembles defined over $\mathrm{GL}(m, \mathbb{F}_2)$, where $m = 1, 2, 3, 4$.

6.4 Numerical Examples

In this section, we give some numerical examples of growth rate which illustrate the statement of Theorem 8 and Corollary 6.

Figure 6.1 and 6.2 show the growth rates of the average number of stopping constellations for the (2,4)-regular non-binary LDPC code ensembles defined over $\mathrm{GL}(m, \mathbb{F}_2)$, where $m = 1, 2, 3, 4$. From these figures, especially from Figure 6.2, we see that the growth rate for small ω does not depend on the dimension m. Moreover, we see that the gradient of the growth rate for small ω is $\log 3$. Similarly, Figure 6.3 and 6.4 show the growth rates for the (3,6)-regular non-binary LDPC code ensembles. From these figures, especially from Figure 6.4, we see that the growth rate for small ω does not depend on the dimension m even if $\lambda'(0) = 0$.

Figure 6.5 shows the critical exponent stopping ratio for the (3,6)-regular non-binary LDPC code ensembles defined over $\mathrm{GL}(m, \mathbb{F}_2)$, where $m = 1, 2, 3, 4, 5$. We see that the critical exponent stopping ratio monotonically decreases as the dimension m increases.

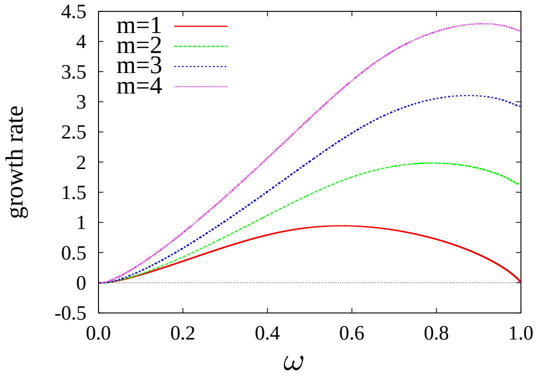

Figure 6.3: The growth rates of the average stopping constellation distributions for the (3,6)-regular non-binary LDPC code ensembles defined over $\mathrm{GL}(m, \mathbb{F}_2)$, where $m = 1, 2, 3, 4$.

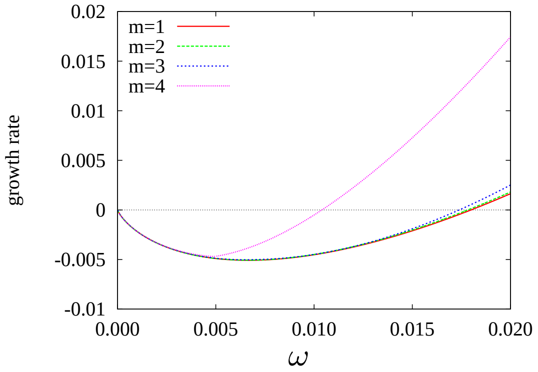

Figure 6.4: The growth rates for $\omega \in [0, 0.02]$ of the average stopping constellation distributions for the (3,6)-regular non-binary LDPC code ensembles defined over $\mathrm{GL}(m, \mathbb{F}_2)$, where $m = 1, 2, 3, 4$.

6.5 Summary

In this chapter, we have derived the stopping constellation distribution and growth rate for non-binary LDPC code ensembles over general linear groups. We have shown that the growth rate does not depend on the dimension of the general linear group for small normalized weight. Moreover, we have shown that the binary LDPC code ensemble is the best in terms of the critical exponent ratio for $\lambda'(0)\rho'(1) < 1$.

Appendix 6.A Proof of Lemma 17

To prove Lemma 17, we use mathematical induction. For $k = 1$, we see that $\dim V_1 = a_1(\{1\})$ and $T_k = 0$. The number of distinct subspaces V_1 of dimension $a_1(\{1\}) = \dim V_1$ is equal to $\left[{m \atop a_1(\{1\})}\right] = \frac{[m]}{[a_1(\{1\})][a_1(\{\})]}$. Hence, (6.2) holds for $k = 1$.

We will show that if (6.2) holds for $k = k' - 1$, then (6.2) also holds for $k = k'$. From the

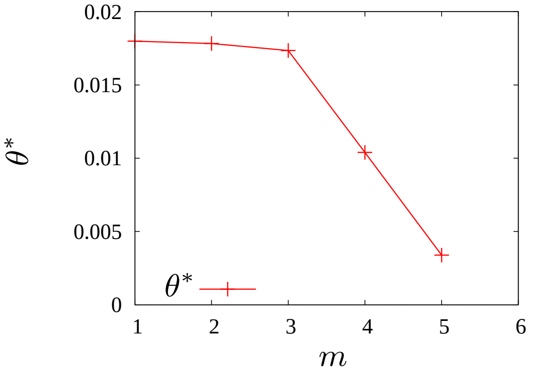

Figure 6.5: The critical exponent stopping ratio of the average stopping constellation distributions for the (3,6)-regular non-binary LDPC code ensembles defined over $\mathrm{GL}(m, \mathbb{F}_2)$, where $m = 1, 2, 3, 4, 5$.

induction hypothesis, we have

$$\begin{aligned} &B_{k'-1}\Big(\big\{a_{k'}(S) + a_{k'}(S \cup \{k'\})\big\}_{S\subseteq[1,k'-1]}\Big) \\ &\quad= \frac{[m]}{\prod_{S\subseteq[1,k'-1]}[a_{k'}(S) + a_{k'}(S \cup \{k'\})]} 2^{T_{k'-1}}, \end{aligned} \tag{6.17}$$

where

$$T_{k'-1} = \frac{1}{2} \sum_{\substack{S_1,S_2\subseteq[1,k'-1]:\\ S_1\not\subseteq S_2, S_1\not\supseteq S_2}} (a_{k'}(S_1) + a_{k'}(S_1 \cup \{k'\}))(a_{k'}(S_2) + a_{k'}(S_2 \cup \{k'\})).$$

If we fix $A_{k'}(S' \cup \{k'\})$ for all $S' \supsetneq S$, then the number of $A_{k'}(S \cup \{k'\})$ is given by

$$\begin{bmatrix} a_{k'}(S) + a_{k'}(S \cup \{k'\}) \\ a_{k'}(S \cup \{k'\}) \end{bmatrix} 2^{T_{k'}(S)}, \tag{6.18}$$

where

$$T_{k'}(S) = a_{k'}(S \cup \{k'\}) \sum_{\tilde{S}\subseteq[1,k'-1]:\tilde{S}\supsetneq S} a_{k'}(\tilde{S}).$$

From (6.17) and (6.18), $B_{k'}(\boldsymbol{a}_{k'})$ is given by

$$\begin{aligned} &\frac{[m]}{\prod_{S\subset[1,k']}[a_{k'}(S)]} 2^{T_k} \prod_{S\subset[1,k']} \begin{bmatrix} a_{k'}(S) \\ a_{k'+1}(S \cup \{k'+1\}) \end{bmatrix} 2^{T_{k'+1}(S)} \\ &\quad= \frac{[m]}{\prod_{S\subseteq[1,k']}[a_{k'}(S)]} 2^{T_{k'-1}+\sum_{S\subseteq[1,k'-1]} T_{k'}(S)}. \end{aligned}$$

The exponential part is written as follows:

$$\begin{aligned}T_{k'-1}+\sum_{S\subseteq[1,k'-1]}T_{k'}(S)=&T_{k'-1}+\frac{1}{2}\sum_{S\subseteq[1,k'-1]}a_{k'}(S\cup\{k'\})\sum_{\tilde{S}:\tilde{S}\supsetneq S}a_{k'}(\tilde{S})\\&+\frac{1}{2}\sum_{S\subseteq[1,k'-1]}a_{k'}(S)\sum_{\tilde{S}:\tilde{S}\subsetneq S}a_{k'}(\tilde{S}\cup\{k'\})\\=&T_{k'}.\end{aligned}$$

This concludes the proof.

Appendix 6.B Proof of Lemma 18

From (6.1), we have $\sum_{S:i\in S}a_k(S)=\dim V_i$ and $\sum_{S\subseteq[1,k]}a_k(S)=m$. From (6.1), we have

$$\dim\left(\bigcap_{j\in[1,k]}V_j\right)=a([1,k])$$

and

$$\dim\left(\bigcap_{j\in[1,k]\setminus\{i\}}V_j\right)=a([1,k])+a([1,k]\setminus\{i\})$$

for $i\in[1,k]$. From those equations, we have

$$\dim\left(\bigcap_{j\in[1,k]\setminus\{i\}}V_j\right)=\dim\left(\bigcap_{j\in[1,k]}V_j\right)+a([1,k]\setminus\{i\}).\tag{6.19}$$

Since $a([1,k]\setminus\{i\})\geq 0$, we have

$$\dim\left(\bigcap_{j\in[1,k]\setminus\{i\}}V_j\right)\leq\dim\left(\bigcap_{j\in[1,k]}V_j\right).\tag{6.20}$$

First, we claim that for all $i\in[1,k]$, $V_i\supseteq\bigcap_{j\in[1,k]\setminus\{i\}}V_j$ if $a_k([1,k]\setminus\{i\})=0$. Since $a_k([1,k]\setminus\{i\})=0$, we have

$$\dim\left(\bigcap_{j\in[1,k]\setminus\{i\}}V_j\right)=\dim\left(\bigcap_{j\in[1,k]}V_j\right),$$

from (6.19). If $V_i\not\supseteq\bigcap_{j\in[1,k]\setminus\{i\}}V_j$, then

$$\dim\left(\bigcap_{j\in[1,k]\setminus\{i\}}V_j\right)>\dim\left(\bigcap_{j\in[1,k]}V_j\right).$$

By using this equation and (6.20), we see that $V_i \supseteq \bigcap_{j\in[1,k]\setminus\{i\}} V_j$ if

$$\dim\left(\bigcap_{j\in[1,k]\setminus\{i\}} V_j\right) = \dim\left(\bigcap_{j\in[1,k]} V_j\right).$$

Thus, for all $i \in [1,k]$, $V_i \supseteq \bigcap_{j\in[1,k]\setminus\{i\}} V_j$ if $a_k([1,k]\setminus\{i\}) = 0$.

Next, we claim that for all $i \in [1,k]$, $a_k([1,k]\setminus\{i\}) = 0$ if $V_i \supseteq \bigcap_{j\in[1,k]\setminus\{i\}} V_j$. If $a_k([1,k]\setminus\{i\}) \neq 0$, we have

$$\dim\left(\bigcap_{j\in[1,k]\setminus\{i\}} V_j\right) > \dim\left(\bigcap_{j\in[1,k]} V_j\right)$$

from (6.19). If $V_i \supseteq \bigcap_{j\in[1,k]\setminus\{i\}} V_j$, then

$$\dim\left(\bigcap_{j\in[1,k]\setminus\{i\}} V_j\right) = \dim\left(\bigcap_{j\in[1,k]} V_j\right).$$

By using this equation and (6.20), we see that $V_i \not\supseteq \bigcap_{j\in[1,k]\setminus\{i\}} V_j$ if

$$\dim\left(\bigcap_{j\in[1,k]\setminus\{i\}} V_j\right) > \dim\left(\bigcap_{j\in[1,k]} V_j\right).$$

Thus, for all $i \in [1,k]$, $V_i \not\supseteq \bigcap_{j\in[1,k]\setminus\{i\}} V_j$ if $a_k([1,k]\setminus\{i\}) \neq 0$. Therefore, we have for all $i \in [1,k]$, $a_k([1,k]\setminus\{i\}) = 0$ if $V_i \supseteq \bigcap_{j\in[1,k]\setminus\{i\}} V_j$. Thus, this concludes the proof.

Chapter 7

Conclusions

To make codes which have good decoding performance, it is important to analyze the decoding error rate for LDPC codes. In this dissertation, we have analyzed the decoding error probability for finite length LDPC codes.

In Chapter 2, we have proved the all-zero codeword assumption for no-binary LDPC codes over the q-MS channel under BP decoding. Moreover, we have shown the relationship between the stopping sets and stopping constellations. The relationship between the stopping sets and stopping sets implies that a way to optimize the non-binary LDPC codes.

In Chapter 3, we have analyzed the decoding erasure probability in the waterfall region for binary LDPC code ensemble over the BEC. We have analytically solved the covariance evolution for the binary irregular LDPC code ensemble. We have also obtained the slope scaling parameter without assumptions.

In Chapter 4, we have analyzed the decoding erasure probability in the error floor region for the non-binary LDPC codes which contain the variable nodes of degree two over the BEC under BP decoding. We have shown that the decoding performances of the zigzag cycles only depend on the cycle parameter. For the non-binary LDPC code over $\mathbb{F}_{2^m}$ we have also shown that cycle parameters which have bad decoding performances are in the proper subfields of the field $\mathbb{F}_{2^m}$. We have proposed a method to improve the error floors for the non-binary LDPC codes which contain the variable nodes of degree two over the BEC under BP decoding. The codes which optimized by proposed method are outperform the existing design methods. Moreover, we have derived lower bounds on the bit and the symbol erasure rates in the error floors for the expurgated ensembles under BP decoding. Simulation results have shown that the lower bounds are tight for the bit and the symbol erasure rates for the expurgated ensembles. Furthermore, we show that this tight lower bound monotonically decrease, as the order of Galois field of non-binary LDPC code increase in the case for the BEC.

In chapter 5, we have extended the results in Chapter 4 to the generalized non-binary LDPC codes over the q-MS channels. For the non-binary LDPC code defined over $\mathrm{GL}(m_3, \mathbb{F}_{2^{m_4}})$ over the q-MS channels, we have shown that the cycles which have bad decoding performances are characterized by the matrices defined by the labels in the cycles. Furthermore, we show that this tight lower bound monotonically decrease, as the order of Galois field of non-binary LDPC code increase in the case for the BEC and BAWGN channel. Moreover, we compare the decoding error rates in the error floors for non-binary LDPC codes over the general linear group with those for non-binary LDPC codes over finite field transmitted over the q-MS channel under BP decoding. In this analysis, we see that the optimized non-binary LDPC codes defined over general linear group have the same decoding performance in the error floors as those defined over finite field.

In Chapter 6, we have derived the stopping constellation distribution and growth rate for non-binary LDPC code ensembles over general linear groups. We have shown that the growth rate does not depend on the dimension of the general linear group for small normalized weight. Moreover, we have shown that the binary LDPC code ensemble is the best in terms of the critical exponent ratio for $\lambda'(0)\rho'(1) < 1$.

By results in the dissertation, (i) we rigorously analyze the waterfall regions for binary LDPC codes and (ii) we are able to optimize the non-binary LDPC codes. The result (i) gives the optimized degree distribution pair without any assumptions and another method to obtain the scaling parameter. If we can extend this result to multi-edge type LDPC code [5], we can optimize the multi-edge type LDPC codes by solving the covariance evolution [38]. The result (ii) help us to make a good performance non-binary LDPC codes.

As a future work, we will analyze the decoding error rate in the water fall region for non-binary LDPC code. More precisely, we will derive the scaling parameters for non-binary LDPC codes. By combining the this result, we will optimized the non-binary LDPC codes. Moreover, we will analyze the decoding error rates for the binary and non-binary multi-edge type LDPC codes.

Bibliography

[1] C. Shannon, "A mathematical theory of communication," The Bell System Technical Journal, vol.27, pp.379–423, 623–656, July, Oct. 1948.

[2] R.G. Gallager, Low Density Parity Check Codes, in Research Monograph series, MIT Press, Cambridge, 1963.

[3] T. Richardson, M.A. Shokrollahi, and R. Urbanke, "Design of capacity-approaching irregular low-density parity-check codes," IEEE Transactions on Information Theory, vol.47, pp.619–637, Feb. 2001.

[4] M. Davey and D. MacKay, "Low-density parity check codes over GF(q)," IEEE Communications Letters, vol.2, no.6, pp.165–167, June 1998.

[5] T. Richardson and R. Urbanke, Modern Coding Theory, Cambridge University Press, March 2008.

[6] T. Richardson and R. Urbanke, "The capacity of low-density parity-check codes under message-passing decoding," IEEE Transactions on Information Theory, vol.47, no.2, pp.599–618, Feb. 2001.

[7] A. Amraoui, A. Montanari, T. Richardson, and R. Urbanke, "Finite-length scaling for iteratively decoded LDPC ensembles," IEEE Transactions on Information Theory, vol.55, no.2, pp.473–498, Feb. 2009.

[8] C. Di, T. Richardson, and R. Urbanke, "Weight distribution of low-density parity-check codes," IEEE Transactions on Information Theory, vol.52, no.11, pp.4839–4855, Nov. 2006.

[9] A. Orlitsky, K. Viswanathan, and J. Zhang, "Stopping set distribution of LDPC code ensembles," IEEE Transactions on Information Theory, vol.51, no.3, pp.929–953, March 2005.

[10] I. Andriyanova and K. Kasai, "Finite-length scaling of non-binary (c, d) LDPC codes for the BEC," Proc. 2010 IEEE Int. Symp. Inf. Theory(ISIT), pp.714–718, June 2010.

[11] F.J. MacWilliams and N.J.A. Sloane, The Theory of Error-Correcting Codes, Elsevier, Amsterdam, 1977.

[12] M. Luby, M. Mitzenmacher, A. Shokrollahi, and D. Spielman, “Improved low-density parity-check codes using irregular graphs,” IEEE Transactions on Information Theory, vol.47, no.2, pp.585–598, Feb. 2001.

[13] X.Y. Hu, E. Eleftheriou, and D. Arnold, “Regular and irregular progressive edge-growth tanner graphs,” IEEE Transactions on Information Theory, vol.51, no.1, pp.386–398, Jan. 2005.

[14] E. Hof, I. Sason, and S. Shamai, “Performance bounds for nonbinary linear block codes over memoryless symmetric channels,” IEEE Transactions on Information Theory, vol.55, no.3, pp.977–996, March 2009.

[15] M. Luby, M. Mitzenmacher, M.A. Shokrollahi, D.A. Spielman, and V. Stemann, “Practical loss-resilient codes,” Proc. the 29th annual ACM Symposium on Theory of Computing, pp.150–159, 1997.

[16] V. Rathi and R. Urbanke, “Density evolution, thresholds and the stability condition for non-binary LDPC codes,” IEE Communications Proceedings, vol.152, no.6, pp.1069–1074, Dec. 2005.

[17] V. Rathi, “Conditional entropy of non-binary LDPC codes over the BEC,” Proc. 2008 IEEE Int. Symp. Inf. Theory(ISIT), pp.945–949, July 2008.

[18] T.J. Richardson, “Error floors of LDPC codes,” Proc. 41th Annual Allerton Conf. on Commun., Control and Computing, pp.1426–1435, Oct. 2003.

[19] V. Rathi, Non-binary LDPC codes and EXIT like functions, Ph.D. thesis, EPFL, Lausanne, 2008.

[20] A. Amraoui, A. Montanari, and R. Urbanke, “How to find good finite-length codes: from art towards science,” European Transactions on Telecommunications, vol.18, no.5, pp.491–508, 2007.

[21] I. Andriyanova, “Finite-length scaling of repeat-accumulate codes on the BEC,” Proc. 2008 IEEE Int. Zurich Seminar on Communications, pp.64–67, March 2008.

[22] I. Andriyanova, “Finite-length scaling of turbo-like code ensembles on the binary erasure channel,” IEEE Journal on Selected Areas in Communications, vol.27, no.6, pp.918–927, Aug. 2009.

[23] J. Ezri, A. Montanari, S. Oh, and R. Urbanke, “The slope scaling parameter for general channels, decoders, and ensembles,” Proc. 2008 IEEE Int. Symp. Inf. Theory(ISIT), pp.1443–1447, July 2008.

[24] J. Ezri, Finite-length scaling laws for iterative coding systems, Ph.D. thesis, EPFL, 2011.

[25] A. Amraoui, R. Urbanke, and A. Montanari, “Finite-length scaling of irregular LDPC code ensembles,” Proc. 2005 IEEE Inform. Theory Workshop, Sept. 2005.

[26] R. Graham, D. Knuth, and O. Patashnik, Concrete mathematics: a foundation for computer science, A foundation for computer science, Addison-Wesley, 1994.

[27] C. Poulliat, M. Fossorier, and D. Declercq, "Design of regular $(2,d_c)$-LDPC codes over GF(q) using their binary images," IEEE Transactions on Communications, vol.56, no.10, pp.1626–1635, Oct. 2008.

[28] R. Lidl and H. Niederreiter, Introduction to finite fields and their applications, Cambridge University Press, New York, NY, USA, 1986.

[29] 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.

[30] G. Li, I. Fair, and W. Krzymien, "Density evolution for nonbinary LDPC codes under Gaussian approximation," IEEE Transactions on Information Theory, vol.55, no.3, pp.997–1015, March 2009.

[31] 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.

[32] J. Craig, "A new, simple and exact result for calculating the probability of error for two-dimensional signal constellations," Military Communications Conference, 1991. MILCOM '91, Conference Record, 'Military Communications in a Changing World'., IEEE, pp.571 –575 vol.2, Nov. 1991.

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

[34] D.E. Knuth, The Art of Computer Programming; Vol. 1: Fundamental Algorithms, Addison-Wesley, Reading, Massachusetts, 1973.

[35] D. Burshtein and G. Miller, "Asymptotic enumeration methods for analyzing LDPC codes," IEEE Transactions on Information Theory, vol.50, no.6, pp.1115–1131, June 2004.

[36] K. Kasai, C. Poulliat, D. Declercq, and K. Sakaniwa, "Weight distribution of non-binary LDPC codes," IEICE Trans. Fundamentals, vol.E94-A, no.4, pp.1106–1115, April 2011.

[37] K. Kasai, T. Awano, D. Declercq, C. Poulliat, and K. Sakaniwa, "Weight distribution of multi-edge type LDPC codes," IEICE Trans. Fundamentals, vol.E93-A, no.11, pp.1942–1948, Nov. 2010.

[38] R. Hinton, S. Wilson, and R. Urbanke, "Finite-length scaling for multi-edge type LDPC ensembles," in preparation.

Publications

Journals

- **T. Nozaki**, K. Kasai, and K. Sakaniwa, "Analysis of error floors of generalized non-binary LDPC codes over q-ary memoryless symmetric channels," **submitted to** *IEICE Transaction on Fundamentals,*
- **T. Nozaki**, K. Kasai, and K. Sakaniwa, "Analytical solution of covariance evolution for irregular LDPC codes," **accepted to** *IEEE Transaction on Information Theory,*
- **T. Nozaki**, K. Kasai, and K. Sakaniwa, "Analysis of error floors of non-binary LDPC codes over BEC," *IEICE Transaction on Fundamentals,* vol. 95-A, no. 1, pp. 381–390, Jan. 2012
- **T. Nozaki**, K. Kasai, and K. Sakaniwa, "Analysis of Stopping Constellation Distribution for Irregular Non-binary LDPC code ensemble," *IEICE Transaction on Fundamentals,* vol. E94-A, no. 11, pp. 2153–2160, Nov. 2011.
- **T. Nozaki**, K. Kasai, and K. Sakaniwa, "Analysis of Error Floors of Non-Binary LDPC Codes over MBIOS Channel," *IEICE Transaction on Fundamentals,* vol. E94-A, no. 11, pp.2144–2152, Nov. 2011.
- **T. Nozaki**, K. Kasai, T. Shibuya, and K. Sakaniwa, "Detailed evolution of degree distributions in residual graphs with joint degree distributions," *IEICE Transaction on Fundamentals,* vol. E91-A, no. 10, pp. 2737–2744, Oct. 2008.

International Conferences

- K. Kasai, **T. Nozaki**, and K. Sakaniwa, "Spatially-Coupled Binary MacKay-Neal Codes for Channels with Non-Binary Inputs and Affine Subspace Outputs" **submitted to** IEEE ISIT 2012.
- **T. Nozaki**, K. Kasai, and K. Sakaniwa, "Analysis of error floors of generalized non-binary LDPC codes over q-ary memoryless symmetric channels," **submitted to** IEEE ISIT 2012.
- **T. Nozaki**, K. Kasai, and K. Sakaniwa, "Analysis of Stopping Constellation Distribution for Irregular Non-binary LDPC code ensemble," in *Proc. IEEE International Symposium on Information Theory 2011,* Saint Petersburg, Russia, pp. 1106–1110, Aug. 2011

- **T. Nozaki**, K. Kasai, and K. Sakaniwa, "Analysis of error floors of non-binary LDPC codes over MBIOS channel," in *Proc. International Conference on Communication 2011,*

- **T. Nozaki**, K. Kasai and K. Sakaniwa, "Error floors of non-binary LDPC codes," in *Proc. IEEE International Symposium on Information Theory 2010,* Austin, Texas, pp. 729–733, June 2010.

- **T. Nozaki**, K. Kasai, and K. Sakaniwa, "Analytical solution of covariance evolution for regular LDPC codes," in *Proc. IEEE International Symposium on Information Theory 2009,* Seoul, Korea, pp. 2649–2653, July 2009.

- **T. Nozaki**, K. Kasai, T. Shibuya, and K. Sakaniwa, "Detailed evolution of degree distributions on residual graphs with joint degree distributions," in *Proc. IEEE International Symposium on Information Theory 2008,* Toronto, Canada, pp. 1438–1442, July 2008.

Domestic Conferences

- **T. Nozaki**, K. Kasai, and K. Sakaniwa, "Optimization Method to Lower Error Floors for Generalized Non-binary LDPC Codes over Non-binary Input Memoryless Symmetric Channels," IEICE General Conference 2012, Okayama, Mar. 2012.

- **T. Nozaki**, K. Kasai, and K. Sakaniwa, "Monotonicity of error floors for non-binary LDPC codes over AWGN channels," IEICE General Conference 2011, Tokyo, Mar. 2011

- **T. Nozaki**, K. Kasai, and K. Sakaniwa, "Analysis of error floors of non-binary LDPC codes over q-ary discrete memoryless symmetric channel," in *Proc. 33rd Symposium on Information Theory and its Application,* Matsushiro, Nagano, pp. 13–18, Dec. 2010.

- **T. Nozaki**, K. Kasai, and K. Sakaniwa, "Analysis of stopping constellation distribution for irregular non-binary LDPC code ensemble," in *Proc. 33rd Symposium on Information Theory and its Application,* Matsushiro, Nagano, pp. 7–12, Dec. 2010.

- **T. Nozaki**, K. Kasai, and K. Sakaniwa, "Analysis of error floors of non-binary LDPC codes over MBIOS channel," LDPC workshop, Tagajo, Miyagi, Sep. 2010

- **T. Nozaki**, K. Kasai, and K. Sakaniwa, "Modified cancellation for non-binary LDPC codes," IEICE General Conference 2010, p. 124, Sendai, Miyagi, Mar. 2010

- **T. Nozaki**, K. Kasai, and K. Sakaniwa, "Analytical solution of covariance evolution for irregular LDPC codes," in *Proc. 32nd Symposium on Information Theory and its Application,* Yuda-Onsen, Yamaguchi, pp. 88–93, Dec. 2009.

- **T. Nozaki**, K. Kasai, and K. Sakaniwa, "Analytical solution of covariance evolution for regular LDPC codes," in *Proc. 31st Symposium on Information Theory and its Application,* Kinugawa, Tochigi, pp. 504–509, Oct. 2008.

- **T. Nozaki**, K. Kasai, T. Shibuya, and K. Sakaniwa, "A note on analytical solution of covariance evolution for regular LDPC codes," LDPC workshop, Okinawa, Sep. 2008
- **T. Nozaki**, K. Kasai, T. Shibuya, and K. Sakaniwa, "Evolution of degree distribution of residual graphs for detailedly represented irregular LDPC code ensembles," in *Proc. 30th Symposium on Information Theory and its Applications,* Kashikojima, Mie, pp. 774–779, Nov. 2007.