Ph.D. DISSERTATION

New Protograph-Based Construction of GLDPC Codes for Binary Erasure Channel and LDPC Codes for Block Fading Channel

프로토그래프 기반의 이진 소실 채널에서의 GLDPC 부호 및 블록 페이딩 채널에서의 LDPC 부호 설계

BY

KIM JAEWHA

FEBRUARY 2022

DEPARTMENT OF ELECTRICAL ENGINEERING AND
COMPUTER SCIENCE
COLLEGE OF ENGINEERING
SEOUL NATIONAL UNIVERSITY

Ph.D. DISSERTATION

New Protograph-Based Construction of GLDPC Codes for Binary Erasure Channel and LDPC Codes for Block Fading Channel

프로토그래프 기반의 이진 소실 채널에서의 GLDPC 부호 및 블록 페이딩 채널에서의 LDPC 부호 설계

BY

KIM JAEWHA

FEBRUARY 2022

DEPARTMENT OF ELECTRICAL ENGINEERING AND
COMPUTER SCIENCE
COLLEGE OF ENGINEERING
SEOUL NATIONAL UNIVERSITY

New Protograph-Based Construction of GLDPC Codes for Binary Erasure Channel and LDPC Codes for Block Fading Channel

프로토그래프 기반의 이진 소실 채널에서의 GLDPC 부호 및 블록 페이딩 채널에서의 LDPC 부호 설계

지도교수 노 종 선

이 논문을 공학박사 학위논문으로 제출함

2022년 2월

서울대학교 대학원

전기 컴퓨터 공학부

김 재 화

김재화의 공학박사 학위 논문을 인준함

2022년 2월

위 원 장: _____
부위원장: _____
위 원: _____
위 원: _____
위 원: _____

Abstract

In this dissertation, two main contributions are given as: i) new construction methods for protograph-based generalized low-density parity-check (GLDPC) codes for the binary erasure channel using partial doping technique and ii) new design of protograph-based low-density parity-check (LDPC) codes for the block fading channel using resolvable block design.

First, a new code design technique, called partial doping, for protograph-based GLDPC codes is proposed. While the conventional construction method of protograph-based GLDPC codes is to replace some single parity-check (SPC) nodes with generalized constraint (GC) nodes applying to multiple connected variable nodes (VNs) in the protograph, the proposed technique of partial doping can select any number of partial VNs in the protograph to be protected by GC nodes. In other words, the partial doping technique enables finer tuning of doping, which gives higher degrees of freedom in the code design and enables a sophisticated code optimization. The proposed partially doped GLDPC (PD-GLDPC) codes are constructed using the partial doping technique and optimized by the protograph extrinsic information transfer (PEXIT) analysis. In addition, the condition guaranteeing the linear minimum distance growth of the PD-GLDPC codes is proposed and analytically proven so that the PD-GLDPC code ensembles satisfying this condition have the typical minimum distance. Consequently, the proposed PD-GLDPC codes outperform the conventional GLDPC codes with a notable improvement in the waterfall performance and without the error floor phenomenon. Finally, the PD-GLDPC codes are shown to achieve a competitive performance compared to the existing state-of-the-art block LDPC codes.

Second, the protograph-based LDPC codes constructed from resolvable balanced incomplete block design (RBIBD) are designed and proposed for block fading (BF) channel. In order to analyze the performance of the proposed LDPC codes, the upper

bounds on bit error rate (BER) using the novel method called gamma evolution are derived. In addition, the numerical analysis shows that the upper bound and the frame error rate (FER) of the proposed LDPC codes approach the channel outage probability in a finite signal-to-noise ratio (SNR) region.

keywords: Binary erasure channel (BEC), block fading (BF) channel, diversity order, error correcting codes, generalized low-density parity-check (GLDPC) codes, low-density parity-check (LDPC) codes, partial doping, partially doped GLDPC (PD-GLDPC) codes, resolvable block design, resolvable balanced incomplete design (RBIBD), typical minimum distance.

student number: 2016-20878

Contents

List of Tables

List of Figures

Chapter 1

INTRODUCTION

1.1 Background

In the field of digital communication, the fundamental goal is the *reliable transmission* of information from the transmission node (source) to the receiver node (sink), where there exists a noisy channel. The digital communications systems are divided into three major roles: source coding, channel coding, and modulation (demodulation), which is shown in Fig. 1.1 [2], [3]. It was proven by Claude E. Shannon in 1948 that a *reliable communication* from noisy channel is possible via error correcting codes as long as the code rate of the transmitted information is less than the capacity of the given channel. Since then, the study of error correcting codes have been essential in the field of digital communication systems. The transmitter converts the information into a stream of binary information bits by using the source encoder. Further, new redundant bits are added to the information bits using the channel encoder to guarantee the *reliable transmission* of the information bits via noisy channel.

Shannon proposed the capacity achieving channel coding scheme, however, a random coding approach was used, which is impractical to implement. Also, no practical candidates of error correcting code schemes were neither proposed nor found at that time. Since then, the search of capacity approaching error correcting codes with prac-

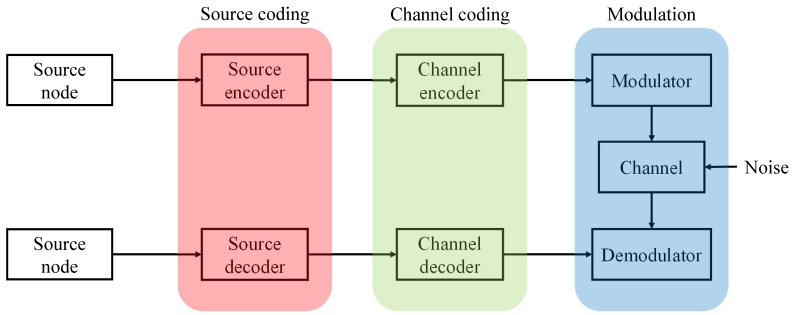


Figure 1.1: Block diagram of a point-to-point digital communication system.

tical encoding and decoding algorithms was one of the major goal in the field of digital communication systems [2]–[7]. The initial approach for the first 50 years was based on error correcting codes using the *algebraic codes*: Hamming codes [8], Golay codes [9], Reed-Muller codes [10], [11], Bose-Chaudhuri-Hocquenghem (BCH) codes [12], [13], and Reed-Solomon (RS) codes [14]. New approach for error correcting codes was made via *probabilistic coding*. Codes such as convolutional codes [15], turbo codes [16], and low-density parity-check (LDPC) codes [17] are constructed using the *probabilistic coding*. LDPC codes are considered as the major topic in this dissertation since the codes possess both the capacity approaching performance capability and practical algorithms for encoding and decoding.

LDPC codes were initially proposed by Gallager at 1963 [17]. However, due to the difficulty of practical implementation of LDPC codes, they did not receive much attention at 1960s. For nearly 30 years, LDPC codes were forgotten until the advent of turbo codes which were proposed by Berrou, Glavieus, and Thitimajshima [16]. Turbo codes showed the potential of codes with probabilistic decoding since they had capacity approaching performance with relatively low complexity iterative decoding. Since then, codes with probabilistic decoding received much attention and thus, LDPC codes were rediscovered by MacKay and Neal, showing that LDPC codes also have the potential to have excellent performance with low decoding complexity [18], [19].

Since the rediscovery of MacKay and Neal, LDPC codes have been a major re-

search topic in the field of error correcting codes. Many attempts have been made to construct LDPC codes with capacity approaching performance. Initially, Luby constructed irregular random LDPC codes with excellent error correcting capabilities over the binary erasure channel (BEC) [20]. The channel was extended to all classes of binary memoryless channel by Richardson and Urbanke, where the capacity approaching LDPC codes were constructed [21]. It was proven by them that LDPC codes with message passing decoding can asymptotically approach the Shannon capacity of the channel. Also, they showed that the performance of LDPC codes can be asymptotically analyzed by the tool called *density evolution*. Since then, LDPC codes were utilized in many communication systems and standards such as wireless local area network (WLAN) and digital video broadcasting [22]-[24].

1.2 Overview of Dissertation

This dissertation is organized as follows. In Chapter 2, the notation and review of LDPC codes are introduced. Section 2.1 presents basic descriptions of LDPC codes such as Tanner graph representation of LDPC codes and irregular LDPC ensembles. In Section 2.2, decoding algorithms of LDPC codes are illustrated and their decoding complexities are discussed. In Section 2.3, density evolution of LDPC codes and an optimization method of irregular LDPC ensembles are briefly described.

In Chapter 3, new construction methods for protograph-based generalized LDPC (GLDPC) codes are proposed. Section 3.1 introduces the code structures for conventional protograph-based GLDPC ensembles and the analysis using the protograph extrinsic information transfer (PEXIT). In Section 3.2, new construction method of the protograph-based GLDPC codes and the analysis tools for the codes are given including the PEXIT and the typical minimum distance. The optimization of the proposed GLDPC codes is given in Section 3.3. Finally, the numerical results of the proposed GLDPC codes are given in Section 3.4.

In Chapter 4, new construction of protograph-based LDPC codes from resolvable block designs is proposed. In Section 4.1, a brief problem formulation of the channel and performance metrics are presented. The construction and evaluation of the proposed protograph-based LDPC codes are given in Section 4.2.

Chapter 2

Overview of LDPC Codes

In this chapter, we introduce some preliminaries for LDPC codes. First, the basic notations of LDPC codes are introduced. Then, the decoding algorithms and analysis tools for LDPC codes are provided. Finally, protograph-based LDPC codes are introduced.

2.1 LDPC Codes

In this section, basic concepts of LDPC codes are given. An LDPC code is a linear block code defined by a parity-check matrix (PCM) $\mathbf{H}$ of size $m \times n$. Then, there exists a set of binary codewords, where each codeword c in the set of length n satisfies $\mathbf{H}c^{\mathrm{T}} = 0^{\mathrm{T}}$. The term low-density is derived from the sparseness of the matrix $\mathbf{H}$, where the number of 1's in the matrix increases linearly with the code length. The sparseness of $\mathbf{H}$ shows that the decoding complexity linearly grows with n when the message passing decoding is used. On the other hand, an LDPC code can be expressed in terms of a Tanner graph, which is is bipartite graph consisting of n variable nodes, m check nodes, and edges connecting both types of nodes. The variable nodes represent the column of the PCM whereas the check nodes represent the row of the PCM. Also, there exists an edge between a variable node v and check node c if the entry of the PCM is one. An example of a Tanner graph is in Fig. 2.1, where the variable nodes

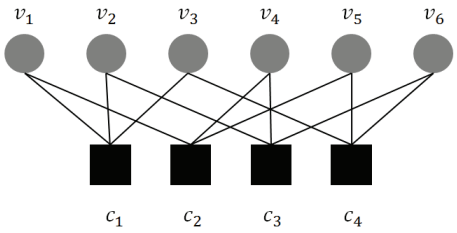


Figure 2.1: A tanner graph of an LDPC code.

are drawn in circles and check nodes are drawn in squares. The PCM representing the Tanner graph in Fig. 2.1 is

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

Let the degree of a node be the number of edges incident to the node. A (d_v, d_c) regular LDPC code is defined as an LDPC code where degree of all variable nodes are d_v and degree of all check nodes are d_c. The LDPC code in Fig. 2.1 is a $(2, 3)$ regular LDPC code. The LDPC code is called irregular if not all variable nodes or check nodes have the same degrees.

A class of irregular LDPC codes can be expressed in terms of degree distributions. Let (Λ, P) be the pair of degree distributions

$$\Lambda(x) = \sum_j \Lambda_j x^j, \mathrm{P}(x) = \sum_i \mathrm{P}_i x^i,$$

where Λ_j is the portion of variable nodes with degree-j and P_i is the portion of check nodes with degree-i. In the aspect of the portion of edges, a class of LDPC codes can be expressed as $\lambda(x) = \sum_i \lambda_i x^{i-1}$, $\rho(x) = \sum_i \rho_i x^{i-1}$, where λ_j (ρ_i) is the portion of edges incident to variable (check) nodes with degree j (i). For the same code ensemble,

the relationship between (Λ, P) and (λ, ρ) is derived as

$$\Lambda(x) = \frac{\int_0^x \lambda(t)dt}{\int_0^1 \lambda(t)dt},$$
$$\mathrm{P}(x) = \frac{\int_0^x \rho(t)dt}{\int_0^1 \rho(t)dt}.$$

2.2 Decoding of LDPC Codes in the BEC

In this section, some decoding schemes of LDPC codes are shown. The main focus in this section is the binary erasure channel (BEC). For an ith binary bit x_i, the output of BEC is $y_i \in \{0, 1, *\}$, where $*$ indicates that the corresponding bit is erased. For erasure probability ϵ, the input binary bit is either erased with probability ϵ or transmitted correctly with probability $1 - \epsilon$. The main goal of the decoding is to minimize the number of resulting erasures. It is noteworthy that the channel capacity of the BEC with erasure probability ϵ is $1 - \epsilon$.

The decoding for LDPC codes, in general, is done by the BP decoding algorithm, where its operation can be represented by passing messages along edges in a Tanner graph. The message passing decoding is done iteratively, which means that the messages are sent between variable nodes and check nodes iteratively. The process is terminated when the messages of the variable nodes satisfy the parity-check equations or the iteration reaches the predetermined iterations of the decoder. The BP decoding algorithm is an iterative decoding algorithm in the sense that the decoding algorithm proceeds iteratively. The decoder stops until it finds a valid codeword satisfying parity-check equations or the number of iterations reaches the predetermined number.

Suppose that a sequence $\mathbf{y} = \{y_1, \ldots, y_n\}$ is received from the channel. Also, let $M_{i,j}$ ($E_{j,i}$) be the extrinsic message from the ith (jth) variable (check) node to the jth (ith) check (variable) node. At first, the variable nodes do not receive any messages from the check nodes. Hence, ith variable nodes send $M_{i,j} = y_i$ to jth check node at the first iteration. At the check node side, by letting the degree of jth check node be d_j, each extrinsic message $E_{j,i}$ is computed by summing up d_j messages except $M_{i,j}$.

At the variable node side, for any erased messages, $M_{i,j}$ is recovered if any of the incoming messages except $E_{j,i}$ is a non-erased message. The decoder computes and sends extrinsic messages iteratively between variable nodes and check nodes until all variable nodes recover the messages from erasures or terminate if the decoder reaches the predetermined iteration.

2.3 Analysis tool for LDPC Codes

2.3.1 Density Evolution

The performance analysis of LDPC codes can be made through the density evolution. Richardson and Urbanke proposed the that by using density evolution, the asymptotic performance of the LDPC codes can be evaluated [21]. In other words, for a given degree distribution of the LDPC codes, the performance limit of the codes can be computed under the assumption that both the code length and the decoding iteration is infinity. Using this tool, the optimization of degree distribution can be made, which enables the construction of LDPC code ensemble with capacity approaching performance. The density evolution tracks down the evolution of messages in a probabilistic manner. In BEC, the probability of erasure is tracked down for all extrinsic messages and a posteriori messages of the variable nodes.

For an irregular LDPC code ensemble with degree distributions $(\lambda(x), \rho(x))$, $x^{(\ell)}$ is extrinsic erasure probability of variable nodes at iteration ℓ. Then, $x^{(\ell)}$ is computed as

$$x^{(\ell)} = \epsilon\lambda(1 - \rho(1 - x^{(\ell-1)})),$$

where $x^{(0)} = \epsilon$. It is clear that the density evolution follows the decoding algorithm of the given message passing decoder. The density evolution tracks down whether $x^{(\ell)}$ approaches to zero as the iteration reaches infinity for a given channel erasure probability ϵ, which implies that the decoder has successfully removed all the erasure. The threshold ϵ^* of the given code ensemble by using the belief propagation decoder is

the minimum ϵ that the $x^{(\ell)}$ approaches to zero, which is the asymptotic performance of the code ensemble.

2.4 Protograph-Based LDPC Codes

LDPC codes can also be constructed by a small building unit called a protograph. A protograph is a small bipartite graph that consists of N variable nodes, M check nodes, and a set of edges connecting both types of nodes. An LDPC code can be constructed from the protograph by the lifting operation, which we call the ensemble of the constructed codes as protograph-based LDPC codes. The lifting operation proceeds by copy-and-permute operation which the protograph is copied Z times and the edges are permuted among the Z replicas, where Z is called as a lifting factor. This implies that each of Z replicas of a variable node in the protograph should be connected to one of Z replicas of the check node which is connected to that variable node in the protograph. Although each code instance is obtained via different permutations, each code maintains the original graph structure of the protograph. Hence, a protograph represents an LDPC code ensemble. A protograph can also be expressed in terms of $M \times N$ base matrix $\mathbf{B}$, where each entry $b_{i,j}$ refers to the number of edges incident to ith variable node and the jth check node. In terms of the base matrix, the lifting operation is replacing each scalar value $b_{i,j}$ by the sum of $b_{i,j}$ distinct $Z \times Z$ permutation matrices, which constructs the parity-check matrix of the protograph-based LDPC code.

The density evolution equations of the protograph-based ensembles can also be described over the BEC. The messages for an edge between ith variable node and the jth check node are defined in terms of the directed edges. Such two types of directed edges are defined as follows: $e_{i \to j}$ is the directed edge from variable node v_i to check node c_j and $e_{i \leftarrow j}$ is the directed edge from check node c_j to variable node v_i. Let $p^{(l)}(e_{i \to j})$ be the erasure probability of the message sent along edge $e_{i \to j}$ in decoding iteration l. Likewise, let $q^{(l)}(e_{i \leftarrow j})$ be the erasure probability of the message sent along

edge $e_{i\leftarrow j}$ in decoding iteration l. At iteration l, the variable nodes first send messages to their neighborhood check nodes and then each check node sends an erasure message if at least one of the incoming messages is an erasure. Secondly, each variable node collects the messages from the neighborhood check nodes and sends a correct message if any of the incoming messages is not an erasure. Thus, the erasure probabilities of messages are computed as

$$\begin{aligned} q^{(l)}(e_{i\leftarrow j}) &= 1 - \prod_{k\in\mathcal{N}(c_j)\setminus\{i\}} \Big(1 - p^{(l-1)}(e_{k\rightarrow j})\Big), \\ p^{(l)}(e_{i\rightarrow j}) &= \epsilon \prod_{k\in\mathcal{N}(v_i)\setminus\{j\}} q^{(l)}(e_{i\leftarrow k}), \end{aligned} \tag{2.1}$$

where $\mathcal{N}(w)$ is the set of neighborhood nodes of the node w. The density evolution equation is initialized as $p^{(0)}(e_{i\rightarrow j}) = 1$. Note that the channel parameter ϵ is omitted in (2.1) for the punctured variable nodes.

Similar to the random-based ensembles, the BP threshold ϵ^* of the protograph-based ensemble is defined as the supremum value of ϵ for which $p^{(l)}(e_{i\rightarrow j})$ converges to zero as l goes to infinity for all i and $j \in \mathcal{N}(v_i)$. Thus, the performance of the protograph ensemble can also be analyzed in terms of the density evolution.

Chapter 3

Construction of Protograph-Based Partially Doped Generalized LDPC Codes

As a generalized class of LDPC codes, generalized LDPC (GLDPC) codes were introduced in [25], which are constructed by replacing some SPC nodes with generalized constraint (GC) nodes. GC nodes are defined by code constraints of a linear code with a larger minimum distance [26], which makes GLDPC codes have a larger minimum distance [27]. In addition, GLDPC codes have several advantages over LDPC codes such as faster decoding convergence [28] and a better asymptotic threshold at the cost of the additional decoding complexity and redundancy introduced by GC nodes [29]. Many types of linear codes for GC nodes, also called as the component codes, are used in the GLDPC codes such as Hamming codes [30], Hadamard codes [31], Bose–Chaudhuri–Hocquenghem codes, and Reed-Solomon codes [32]. The research on GLDPC codes is extended to spatially coupled LDPC (SC-LDPC) codes [33, 34, 35] and doubly GLDPC (DGLDPC) codes [36, 37, 38]. Moreover, some capacity approaching GLDPC codes were constructed using irregular random GLDPC codes [29, 39].

For the structured GLDPC codes, protograph-based GLDPC codes can be constructed from a small protograph [40] using so called doping technique [41]. Doping a

GC node, defined by a (μ, κ) linear code of length μ and dimension κ, means the replacement of an SPC node by the GC node with $\mu - \kappa$ constraints, which causes a rate loss. In the perspective of VNs, μ VNs are selected to be doped by a GC node. Thus, the smallest unit of doping, also called the doping granularity, is μ for the conventional protograph doping technique. In other words, the conventional doping technique has two limitations: i) the degree of the SPC node to be replaced should be μ, which means the doping operation is dependent on the underlying protograph and the parameter of component codes and ii) one cannot choose a finer doping granularity less than μ and thus the code design cannot be sophisticated. Due to the limited design flexibility, there has been little works on the well-designed optimization for protograph-based GLDPC codes, especially for medium to high code rates.

In this section, I propose a new doping technique, called partial doping, to minimize the doping granularity and enlarge the code design freedom. In detail, the partial doping involves the following three steps: i) A VN to be doped is selected in the protograph. ii) The Tanner graph is obtained by the lifting operation [40] from the protograph with a lifting factor N. iii) Additional GC nodes are connected to the lifted N VNs in the Tanner graph. The main difference from the conventional protograph doping technique is that the partial doping operation is conducted on the Tanner graph instead of the protograph. Thus, it is possible to dope even a single VN in the protograph and the doping granularity becomes one, which is independent of μ. In other words, the partial doping enables fine tuning of the code structure regardless of the underlying protograph and the parameter of component codes. Specifically, the selection of VNs to be protected by GC nodes and the rate loss can be adjusted in a more flexible manner.

I denote the proposed protograph-based GLDPC codes constructed using the partial doping as partially doped GLDPC (PD-GLDPC) codes. The structural characteristics of the PD-GLDPC codes have several advantages. First, the PD-GLDPC codes are structurally adequate to adopt the puncturing technique that compensates the rate-

loss. Since the partially doped VNs are highly and locally protected by GC nodes, the performance loss occurred by puncturing the doped VNs is relatively small while attaining the code rate gain. Second, the asymptotic performance of the PD-GLDPC codes can be analyzed by the low-complexity extrinsic information transfer (EXIT) analysis. For the conventional protograph doped GLDPC codes [41], the exact EXIT analysis is provided in [42], where the topology for the a priori and extrinsic mutual information of GC nodes is considered. Since the cases of the topology grows exponentially with the component code length μ, the computational complexity is too high to design a fast optimization algorithm. On the contrary, GC nodes in the PD-GLDPC codes can be analyzed by an average manner EXIT analysis in [43] because GC nodes in the PD-GLDPC codes are incident to VNs lifted from a single VN in the protograph. The a priori and extrinsic mutual information of GC nodes can be evaluated by a single value, which facilitates a fast optimization algorithm. Using this advatage, I propose an efficient optimization algorithm for the PD-GLDPC codes.

In addition, I propose the condition guaranteeing the linear minimum distance growth of the PD-GLDPC codes. I analytically prove that the PD-GLDPC code ensembles satisfying the condition have the typical minimum distance and use this condition for the constructions of PD-GLDPC codes in this dissertation. Also, utilizing the advantages of PD-GLDPC codes, I propose novel optimization methods to construct the proposed PD-GLDPC codes using the protograph EXIT (PEXIT) analysis [44] and genetic algorithm for code rates $1/2$ and $2/3$. Thus, optimized PD-GLDPC code ensembles are made while satisfying the typical minimum distance condition to have a minimum distance that grows linearly with the block length of the code. Comparison of the PD-GLDPC codes is made with the existing state-of-the-art protograph-based LDPC codes and conventional GLDPC codes [39]. Threshold results for both code rates show that the proposed PD-GLDPC codes outperform the well known protograph-based LDPC codes and have a competitive asymptotic performance compared to optimized protograph-based LDPC codes. In a same manner, the frame error

rate (FER) results show tangible gain in the waterfall performance compared to the existing protograph-based LDPC codes in [45] without the error floor phenomenon. Thus, well constructed protograph-based GLDPC codes can also have the competitive performance in the medium to high code rate regime by using the proposed partial doping technique.

I list the following contributions for this chapter: i) I propose a new method of doping, where the constraints of GC nodes are employed to specific VNs lifted from single protograph node, i.e., partial doping of a protograph node. ii) I propose two evaluation criteria for the proposed PD-GLDPC codes: the EXIT analysis of PD-GLDPC codes and the condition for the existence of the typical minimum distance for the PD-GLDPC code ensemble. iii) I propose the optimization method for the PD-GLDPC codes. iv) I show the finite-length performance gain of the optimized PD-GLDPC codes over some well known LDPC and GLDPC codes.

The rest of the chapter is organized as follows. In Section 3.1, I introduce some preliminaries on conventional protograph GLDPC codes. Section 3.2 illustrates the proposed PD-GLDPC code structure and derives its PEXIT analysis and the condition for the typical minimum distance. In addition, comparison with the protograph doped GLDPC codes is given. The optimization algorithms of PD-GLDPC codes are given in Section 3.3. Section 3.4 shows the error correcting performance of the proposed codes compared with other well known protograph-based LDPC codes. Section 3.5 shows the proof of the typical minimum distance of PD-GLDPC codes.

3.1 Code Structure of Protograph-Based GLDPC Ensembles

3.1.1 Construction of Protograph Doped GLDPC Codes

Conventionally, a protograph doped GLDPC code ensemble is constructed by replacing (doping) a CN of a protograph with a GC node that has a parity-check constraint

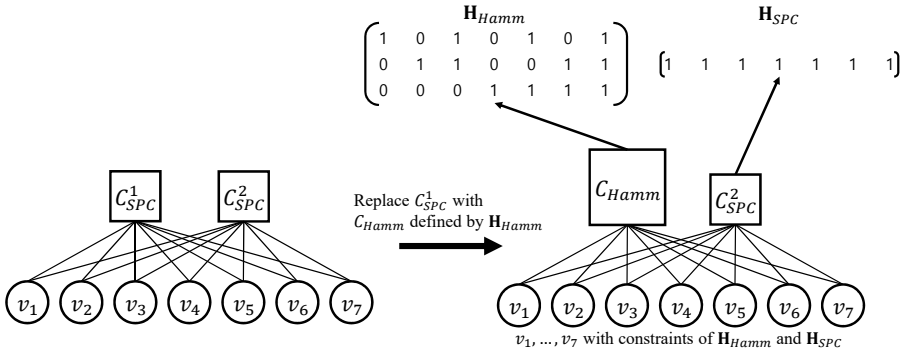


Figure 3.1: An example of protograph doped GLDPC code construction following [41] by replacing an SPC node with a GC node using the $(7, 4)$ Hamming code as the component code.

from an (n_i, k_i, d_{min}^i) linear code (component code), where n_i (k_i) is the code length (dimension) and d_{min}^i is the minimum distance of the component code for a CN c_i [41]. The condition for replacement is that the CN degree should be exactly equal to the length of the component code, i.e., $deg(c_i) = n_i$. Note that the original CN has the parity-check constraint of an $(n_i, k_i) = (deg(c_i), deg(c_i) - 1)$ SPC code. The code rate R of protograph doped GLDPC codes is $R = 1 - \frac{m_{proto}}{n_v}$, where $m_{proto} = \sum_{i=1}^{n_c}(n_i - k_i)$. While the minimum distance of an SPC node is 2, the VNs connected to the GC node will be protected by parity-check constraints of the component code with the minimum distance larger than two. Fig. 3.1 is the protograph doped GLDPC code of the code rate $3/7$ by replacing an SPC node with the $(7, 4)$ Hamming code constraints.

3.1.2 PEXIT Analysis and Decoding Process of Protograph Doped GLDPC Codes

The asymptotic performance of the protograph doped GLDPC codes is evaluated by the PEXIT analysis. The PEXIT analysis tracks down the mutual information of extrinsic messages and a priori error probabilities of the VNs, CNs, and GC nodes

Algorithm 3.1 The PEXIT analysis of a protograph doped GLDPC code [46]

1: **Step 1) Initialization**

Initialize $I_{ch}(j) = 1 - \epsilon$ for $j \in [n_v]$.

2: **Step 2) Message update from VN to CN**

Update $I_{EV}(i,j) = 1 - \epsilon \prod_{t \in N(v_j)} \big(1 - I_{AV}(t,j)\big)^{\delta(t,j)}$ for all $j \in [n_v]$, where $\delta(t,j) = b_{t,j}$ for $t \neq i$ and $\delta(t,j) = b_{t,j} - 1$ for $t = i$. Further, $I_{EV}(i,j) = 0$ if $b_{i,j} = 0$. If c_i is an SPC node, $I_{AV}(i,j) = I_{EC}(i,j)$ and if c_i is a GC node, $I_{AV}(i,j) = I_{EGC}(i,j)$.

3: **Step 3) Message update from CN to VN**

For all i, if c_i is an SPC node, go to **Step 3-1)** and if c_i is a GC node, go to **Step 3-2)**.

Step 3-1) $I_{EC}(i,j) = \prod_{t \in N(c_i)} I_{AC}(i,t)^{\delta(i,t)}$, where $\delta(i,t) = b_{i,t}$ for $t \neq i$ and

$\delta(i,t) = b_{i,t} - 1$ for $t = j$. Further, $I_{AC}(i,t) = I_{EV}(i,t)$.

Step 3-2) For all $j \in N(c_i)$, compute

$$I_{EGC}(i,j) = \frac{1}{n_i} \sum_{h=1}^{n_i} \big(1 - I_{AGC}(i)\big)^{h-1} \big(I_{AGC}(i)\big)^{n_i - h} [h\tilde{e}_h - (n_i - h + 1)\tilde{e}_{h-1}], \tag{3.1}$$

where $I_{AGC}(i) = \frac{1}{n_i} \sum_{j \in N(c_i)} b_{i,j} \times I_{EV}(i,j)$.

4: **Step 4) APP mutual information computation**

For all $j \in [n_v]$, $I_{APP}(j) = 1 - \epsilon \prod_{t \in N(v_j)} \big(1 - I_{AV}(t,j)\big)^{b_{t,j}}$. If c_t is an SPC node, $I_{AV}(t,j) = I_{EC}(t,j)$ and if c_t is a GC node, $I_{AV}(t,j) = I_{EGC}(t,j)$.

5: **Step 5) Convergence check of VNs**

Repeat **Step 2)–4)** until $I_{APP}(j) = 1$, for all $j \in [n_v]$.

of protograph GLDPC codes. For an exact PEXIT analysis, tracking down each mutual information corresponding to edges of the component code is needed, i.e., multi-dimensional EXIT computation [42]. However, in terms of code optimization, where lots of EXIT computation is required, it is beneficial to reduce the complexity of the EXIT computation in GC nodes by averaging the a priori and extrinsic mutual information of the GC nodes. The EXIT and PEXIT analyses of the protograph doped GLDPC codes over the BEC in terms of average mutual information are given in [46, 43, 44].

The PEXIT process is given in Algorithm 3.1. Let $I_{ch}(j)$ be the channel information from the erasure channel for the protograph VN v_j. In addition, $I_{EV}(i,j)$ ($I_{EC}(i,j)$) is the extrinsic information sent from v_j (c_i) to c_i (v_j) and $I_{AV}(i,j)$ ($I_{AC}(i,j)$) is the a priori mutual information of v_j (c_i) sent from c_i (v_j), where c_i is an SPC node. For GC nodes, I use the notations $I_{AGC}(i)$ and $I_{EGC}(i,j)$ for a priori and extrinsic information. Let $N(c_i)$ ($N(v_j)$) be a set of variable (check) nodes incident to c_i (v_j), i.e., neighborhood of c_i (v_j). Finally, $I_{APP}(j)$ is a posteriori probability of v_j. To explain (3.1) in Algorithm 3.1, if c_i is a GC node with the (n_i, k_i) Hamming code, the PEXIT of the GC node is computed from a closed form using the property of the simplex code, which is the dual code of a Hamming code. Also, $I_{AGC}(i) = \frac{1}{n_i}\sum_{j\in N(c_i)} b_{i,j} \times I_{EV}(i,j)$ is the average a priori mutual information for a GC node to compute the PEXIT message. In (3.1), I have

$$\tilde{e}_h = \sum_{t=1}^{h} t \sum_{u=0}^{t-1} (-1)^u 2^{\binom{u}{t}} \begin{bmatrix} k_i \\ t \end{bmatrix} \begin{bmatrix} t \\ u \end{bmatrix} \binom{2^{t-u}}{h}.$$

For two positive integers a and b, I also have $\binom{a}{b} = \prod_{i=0}^{b-1} \frac{a-i}{b-i}$ and $\begin{bmatrix} a \\ b \end{bmatrix} = \prod_{i=0}^{b-1} \frac{2^a - 2^i}{2^b - 2^i}$, where $\binom{a}{0} = 1$ and $\begin{bmatrix} a \\ 0 \end{bmatrix} = 1$. The PEXIT process searches for the minimum ϵ to successfully decode, i.e., $I_{APP}(j) = 1$, for all $j \in [n_v]$, in an asymptotic sense.

Now, I briefly explain the decoding process of GLDPC codes over the BEC [35]. The VNs process the conventional message-passing decoding over the BEC by sending correct extrinsic messages to the CNs if any of the incoming bits from their neighborhood is not erased. The SPC nodes send correct extrinsic messages to the VNs if all

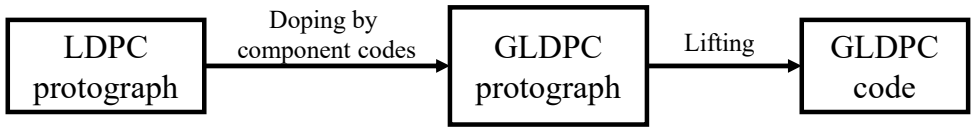
of their incoming messages are correctly received, and send erasure messages otherwise. In this dissertation, the decoding of GC nodes is processed by the maximum likelihood (ML) decoder. For each iteration, a GC node c_i with the (n_i, k_i) component code receives the set of erasure locations $\{e_i\}$ from $N(c_i)$. Let H_{GC} be the PCM of the component code and H_e be the submatrix of H_{GC} indexed with $\{e_i\}$. The decoder computes the Gaussian-elimination operation of H_e, making it into a reduced row echelon form $H_e^{reduced}$. If rank($H_e^{reduced}$)= $|\{e_i\}|$, the GC node solves all the input erasures and otherwise, the decoder corrects the erasures corresponding to the rows with weight one from $H_e^{reduced}$. The decoding complexity can be further reduced if the GC node exploits bounded distance decoding; however, the degradation of asymptotic performance is not negligible, as shown in [29].

3.2 The Proposed PD-GLDPC Codes

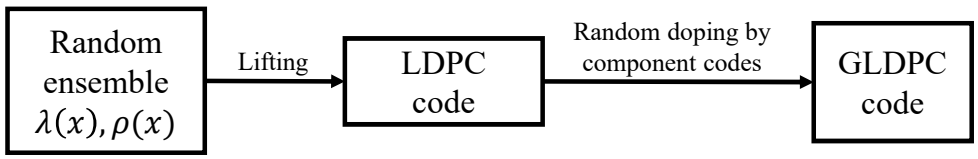
In this section, a new construction method of protograph-based GLDPC codes is proposed. While the protograph doped GLDPC codes are constructed by replacing some protograph SPC nodes in the original protograph by GC nodes using the component code, the proposed PD-GLDPC codes are constructed by adding GC nodes for the subset of VNs using component codes after the lifting process of the original protograph, where each GC node is connected to the VNs copied from single protograph VN. A block diagram of the construction process of both codes together with the conventional random GLDPC code is given in Fig. 3.2.

3.2.1 Construction Method of PD-GLDPC Codes

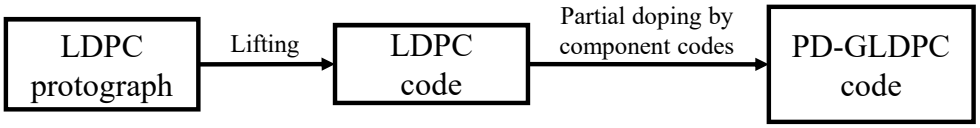
First, I define the partial doping for VNs using additional GC nodes to a lifted protograph, that is, the addition of rows for the PCM by the component code, where each GC node is incident to VNs copied from single protograph VN. Also, I define a partially doped protograph VN as the aforementioned single protograph VN for the GC node.



(a) Protograph doped GLDPC codes [41]



(b) Random GLDPC codes through doping



(c) Proposed PD-GLDPC codes

Figure 3.2: A block diagram of the construction process of protograph doped GLDPC codes [41], randomly doped GLDPC codes, and the proposed PD-GLDPC codes.

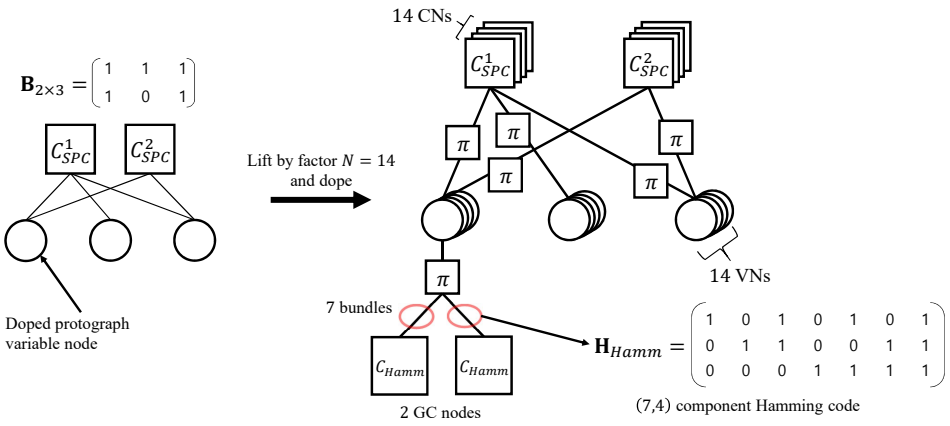
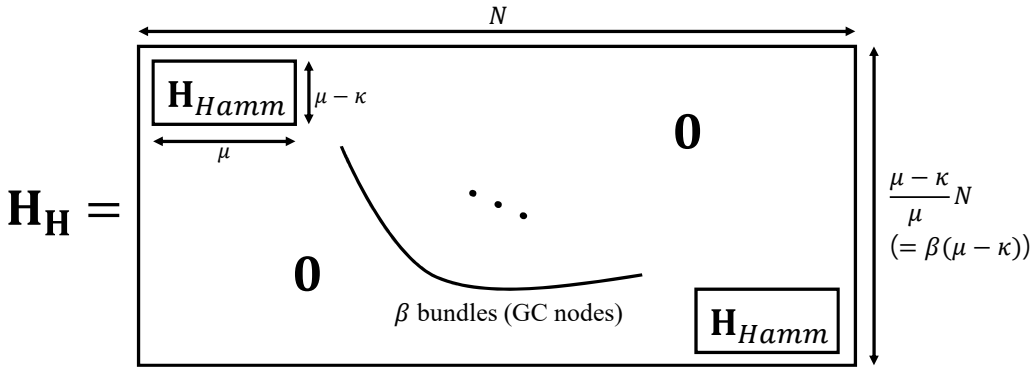


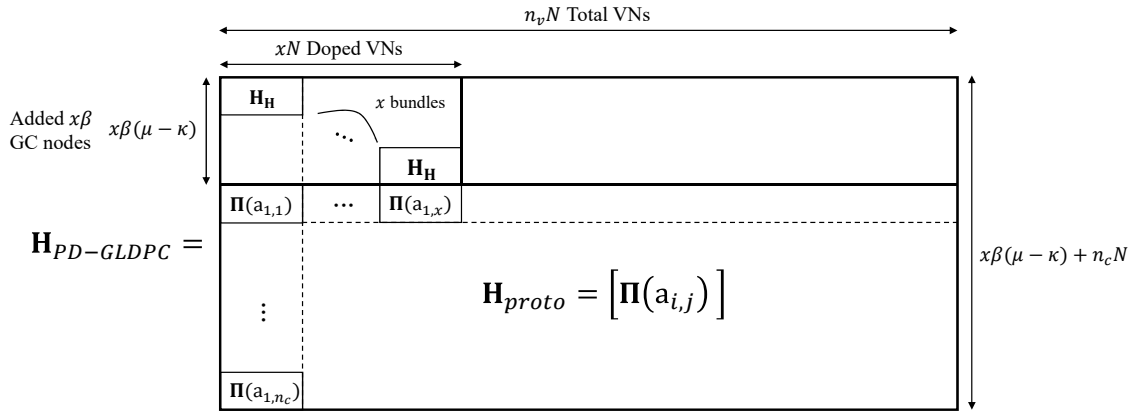
Figure 3.3: An example of a proposed $(\mathbf{B}_{2\times3}, 7, 4, \mathcal{X} = \{1\})$ PD-GLDPC code construction, where $\mathbf{B}_{2\times3} = [1\,1\,1; 1\,0\,1]$ and π is the 14×14 sized permutation matrix.

While the term doping in protograph doped GLDPC codes is used in the perspective of CNs, I use the term partial doping in the perspective of VNs. Let $\mathbf{B}_{n_c \times n_v}$ be an $n_c \times n_v$ base matrix, where some protograph VNs are partially doped with a (μ, κ) component code after the lifting process. Let $\mathcal{X}$ be a set that contains indices of protograph VNs that are partially doped, where each partially doped protograph VN is randomly doped by N/μ component codes after the lifting process. Then, the proposed PD-GLDPC codes are defined with the parameters $(\mathbf{B}_{n_c \times n_v}, \mu, \kappa, \mathcal{X})$. Although any component code can be used, I restrict the component code used in the dissertation as the (μ, κ) Hamming code and assume that μ divides the lifting factor N such that $N = \mu\beta$, where β is a positive integer. The VNs copied from $|\mathcal{X}|$ protograph VNs in the base matrix are partially doped by GC nodes. That is, in the proposed PD-GLDPC code construction, the N/μ GC nodes are randomly connected to N VNs lifted from each partially doped protograph VN. Thus, the proposed construction method can choose any protograph VNs to protect by partial doping. The code rate of the PD-GLDPC code ensemble with $(\mathbf{B}_{n_c \times n_v}, \mu, \kappa, \mathcal{X})$ is $1 - \frac{n_c + |\mathcal{X}| \cdot (\mu - \kappa)/\mu}{n_v}$. An example of the proposed construction is given in Fig. 3.3, which illustrates the doping process by a $(7, 4)$ component Hamming code over a 2×3 base matrix.

The basic concept of the proposed construction is to focus on the protection of VNs lifted from single protograph VN. Since N is the multiple of the component code length, all the VNs lifted from single protograph VN can be protected by using β GC nodes. A simple example for the PCM for β GC nodes, connected to the VNs lifted from single protograph VN, $\mathbf{H_H}$ is shown in Fig. 3.4(a), where $\mathbf{H}_{Hamm}$ is the PCM of the Hamming code. Although the PCM of the Hamming code can be applied randomly, a trivial representation of applying generalized constraints sequentially is given. The constructed PD-GLDPC code has a PCM $\mathbf{H}_{PD\text{-}GLDPC}$ as in Fig. 3.4(b), where the upper part is the PCM of the added βx GC nodes and the lower part $\mathbf{H}_{proto}$ refers to the PCM of the LDPC code lifted from the original protograph. Intuitively, $\mathbf{H_H}$ represents the PCM for each partially doped VN in the protograph and thus, the $x = |\mathcal{X}|$ bundles



(a) A PCM of β GC nodes doped for single protograph VN assuming a trivial permutation.



(b) A PCM of the PD-GLDPC code for the first $x = |\mathcal{X}|$ partially doped protograph VNs.

Figure 3.4: An exemplary PCM of a PD-GLDPC code.

of matrices are diagonally appended to the PCM of the PD-GLDPC code. Since the doping proceeds after the lifting process, PD-GLDPC codes cannot be expressed in terms of a protograph. I define the doping granularity as the minimum number of protograph VNs needed for doping. For the protograph doped GLDPC codes with (μ, κ) component code, the doping granularity is μ, whereas the proposed PD-GLDPC code has doping granularity one. The finer doping granularity of the PD-GLDPC codes allows the construction of protograph-based GLDPC codes with the higher rate.

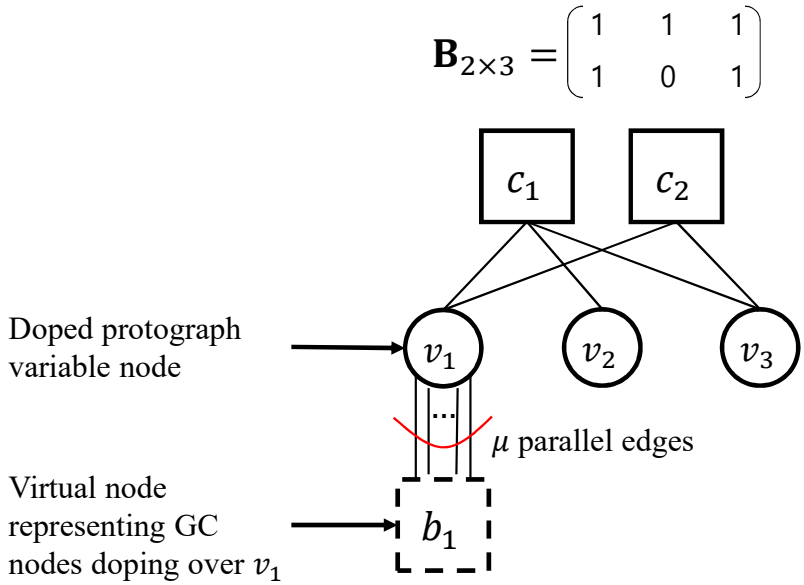


Figure 3.5: An example of the Tanner graph representation of the proposed PD-GLDPC code from the base matrix $\mathbf{B}_{2\times3} = [1\,1\,1; 1\,0\,1]$, where $\mathcal{X} = \{1\}$.

3.2.2 PEXIT Analysis of PD-GLDPC Codes

The PEXIT of the proposed PD-GLDPC codes is similar to that of the protograph doped GLDPC codes in Algorithm 3.1 except for the EXIT of a GC node. Since the incoming mutual information of each GC node is obtained from only a single protograph VN in the proposed code, the average mutual information sent to each GC node is the same as the extrinsic message of the protograph VN connected to the GC node. Let $b_j, j \in \mathcal{X}$ be the virtual node representing the set of β GC nodes connected to the protograph VN v_j. An example of the representation of a virtual node over a protograph is given in Fig. 3.5. Note that although b_j is not a protograph node itself, it is possible to compute the PEXIT of a PD-GLDPC code. Also, let $I_{EV}^{(b_j)}(j)$ be the extrinsic information from v_j to b_j expressed as

$$I_{EV}^{(b_j)}(j) = 1 - \epsilon \prod_{t \in N(v_j)} (1 - I_{AV}(t,j))^{b_{t,j}}, j \in \mathcal{X}.$$

Since b_j is solely connected to v_j, the index term for the extrinsic information from v_j to b_j is expressed by the notation of j only. In order to compute the EXIT of b_j, let $I_{AGC}^{(b_j)}(j)$ and $I_{EGC}^{(b_j)}(j)$ be the a priori and extrinsic mutual informations of b_j, respectively. Note that in an average sense, the EXIT of each GC node is computed from a single a priori mutual information to process the single value of the extrinsic mutual information for the neighboring VNs. Since b_j receives the extrinsic mutual information of v_j only, it is clear that $I_{AGC}^{(b_j)}(j) = I_{EV}^{(b_j)}(j),\ j \in \mathcal{X}$. I also compute the extrinsic mutual information from b_j to v_j denoted as $I_{EGC}^{(b_j)}(j)$ using (3.1), given the a priori mutual information $I_{AGC}^{(b_j)}(j)$, which is given as

$$I_{EGC}^{(b_j)}(j) = \frac{1}{\mu}\sum_{h=1}^{\mu}\big(1 - I_{AGC}^{(b_j)}(j)\big)^{h-1}\big(I_{AGC}^{(b_j)}(j)\big)^{\mu-h}[h\tilde{e}_h - (\mu - h + 1)\tilde{e}_{h-1}]. \quad (3.2)$$

Note that for the proposed PD-GLDPC codes, the a priori (extrinsic) EXIT of the GC node is computed from the extrinsic (a priori) EXIT of single protograph VN. While the EXIT of VNs and SPC nodes for the proposed PD-GLDPC codes is the same as that of the protograph doped GLDPC codes described in Algorithm 3.1, the EXIT of the GC nodes in the proposed codes is changed to (3.2) whereas the protograph doped GLDPC codes use (3.1) from Algorithm 3.1.

3.2.3 Condition for the Existence of the Typical Minimum Distance of the PD-GLDPC Code Ensemble

The existence of a typical minimum distance in the given LDPC code ensemble defined in [47] guarantees that the minimum distance of its corresponding code grows linearly with the block length in an asymptotic sense [17]. To express it formally, if there exists a small number $\delta^* > 0$ such that the weight enumerators for a given code ensemble with weights less than or equal to $\delta^* n$ vanish as $n \to \infty$, then δ^* is the typical minimum distance of the code ensemble. It was proved in [48] that a protograph-based LDPC code ensemble has a typical minimum distance if there is no cycle consisting

of only degree-2 VNs in the protograph. Furthermore, in [49], the condition for the existence of the typical minimum distance of the protograph-based GLDPC code ensembles was given.

The proposed PD-GLDPC codes also have a similar approach to that of the protograph doped GLDPC codes in [49]. However, since a GC node of the proposed PD-GLDPC codes is not well defined by a protograph node, the derivation of the weight enumerator of the proposed codeword is quite different from that of the protograph doped GLDPC code. Thus, the condition for the existence of the typical minimum distance of the proposed PD-GLDPC code ensemble is slightly different from that of the protograph doped GLDPC code ensemble. In fact, the degree-2 VNs can be regarded as the partially doped VNs with higher degrees. The detailed explanation for the existence of the typical minimum distance of the PD-GLDPC code ensemble is given in Section 3.5. Then, the following theorem for the proposed PD-GLPDC codes is proved.

Theorem 1. *For the PD-GLDPC code ensemble of* $(\mathbf{B}_{n_c \times n_v}, \mu, \kappa, \mathcal{X})$ *without degree-1 VNs in* $\mathbf{B}_{n_c \times n_v}$*, the property of the typical minimum distance holds if the undoped degree-2 VNs in the protograph have no cycles among themselves.*

Proof. The proof is given in Section 3.5.

The existence of the typical minimum distance of the proposed PD-GLDPC code ensemble guarantees that the minimum distance of the proposed code grows linearly with the code length, and thus the proposed code is expected to have the low error floor for the large code length. In the next section, I use Theorem 1 as the constraint to optimize the protograph in order to guarantee the existence of the typical minimum distance of the proposed PD-GLDPC code ensemble.

3.2.4 Comparison between Proposed PD-GLDPC Codes and Protograph Doped GLDPC Codes

The main difference between the proposed PD-GLDPC codes and the protograph doped GLDPC codes is the perspective of doping. While the protograph doped GLDPC codes replace an entire row in the protograph, i.e., a protograph CN by the PCM of the component code, the proposed PD-GLDPC codes append some rows incident to the VNs copied from single protograph VN. The focus of the protograph doped GLDPC codes is to choose a certain protograph CN to be replaced, whereas the PD-GLDPC codes focus on choosing which protograph VNs are further protected by partial doping. The constraint for the protograph doped GLDPC code is that the CNs to be replaced should have the degree equal to the component code length, while the constraint for the proposed PD-GLDPC codes is that the lifting size of a protograph should be the multiple of the component code length.

Furthermore, compared to the proposed PD-GLDPC codes, the protograph doped GLDPC codes have large doping granularity. By generalizing a single CN by a component code with parameters (μ, κ), the μ protograph VNs are doped assuming that the corresponding base entries are all ones for the protograph check node. Whereas, for every partial doping of β GC nodes in the proposed PD-GLDPC code, VNs copied from single protograph VN are partially doped. In other words, the doping granularity is one, which is smaller than that of the protograph doped GLDPC codes. Since the doping granularity of protograph doped GLDPC codes is large, construction of the small protograph with capacity approaching performance is very difficult. In Section 3.3, I propose the construction method of PD-GLDPC codes with partial doping of $|\mathcal{X}|$ protograph VNs.

3.3 Optimization of PD-GLDPC Codes

In this section, I illustrate two optimization methods for the construction of PD-GLDPC codes. The first subsection illustrates the construction method of protographs from the degree distribution of a random LDPC code ensemble in order to conduct comparison between LDPC codes and PD-GLDPC codes under the same degree distribution. The second subsection shows the optimization method of the protograph using the differential evolution algorithm in order to conduct comparison between LDPC codes and PD-GLDPC codes without any constraints.

3.3.1 Construction of PD-GLDPC Codes from Regular Protographs

I define a variable node regular protograph as a protograph, where all of its variable nodes have the same degree. Similar to the conventional protograph GLDPC code construction, I introduce the construction process of a proposed protograph-based PD-GLDPC code from a regular protograph. In this dissertation, I have strictly satisfied the variable node regularity for the protograph while making the check nodes as regular as possible using the progressive edge-growth (PEG) algorithm [53]. Since the PEG algorithm is a random construction method, I have considered doping for variable nodes from the left part of the base matrix, i.e., doping for v_j, $j = 1, 2, \cdots, y\mu$. After lifting by N, the number of partially doped variable nodes is $\mu y N$ and each subset of size μ variable nodes lifted from a protograph variable node constitutes a Hamming code with PCM $\mathbf{H}_{Hamm}$ as a component code. Note that the number of dopings for the protograph variable nodes should be sufficient enough to satisfy the constraint for the existence of the typical minimum distance. The necessary condition of y for the typical minimum distance condition is that the number of undoped degree-2 variable nodes is less than the number of check nodes of the original protograph, that is,

$$n_v - \mu y \leq n_c - 1 \leftrightarrow y \geq \frac{n_v - n_c + 1}{\mu}.$$

Algorithm 3.2 The construction method of a protograph-based PD-GLDPC code from a variable node regular protograph

Input: w_r, μ, κ, n_v, R

Output: y, $\mathbf{B}_{n_c \times n_v}$

Step 1) Initialization

For each y in $\lceil \frac{n_v - n_c + 1}{\mu} \rceil \leq y \leq \lfloor \frac{n_v}{\mu} \rfloor$, construct a variable node regular base matrix $\mathbf{B}$ of size $n_c \times n_v$ using the PEG method, where each variable node has degree-w_r and $n_c = n_v(1 - R) - (\mu - \kappa)y$.

Step 2) Construction of the candidate protograph-based PD-GLDPC code

For each y, partially dope (μ, κ) Hamming codes on $y\mu$ blocks of variable nodes in the base matrix.

Step 3) Check the existence of the typical minimum distance

For each y, $\lceil \frac{n_v - n_c + 1}{\mu} \rceil \leq y \leq \lfloor \frac{n_v}{\mu} \rfloor$, if there exists any cycle for the submatrix induced by only undoped variable nodes of degree 2, re-initialize the base matrix as in **Step 1)** for that y.

Step 4) Selection of the optimal protograph-based PD-GLDPC code

For each y, compute the PEXIT threshold of the constructed protograph-based PD-GLDPC code and find y with the best threshold.

Furthermore, in order to satisfy the sufficient condition for the typical minimum distance, I make sure that the undoped degree-2 variable nodes do not form a protograph cycle among themselves. The code rate R of the proposed protograph-based PD-GLDPC is derived as $R = 1 - \frac{n_c + (\mu - \kappa)y}{n_v}$, where for a given code rate and n_v, a protograph-based PD-GLDPC code is constructed. The construction of a protograph-based PD-GLDPC code from a regular protograph is summarized in Algorithm 3.2.

3.3.2 Differential Evolution-Based Code Construction from the Degree Distribution of Random LDPC Code Ensembles

In general, as the portion of degree-2 VNs in the LDPC codes increases, the asymptotic performance is enhanced [50], but their minimum distance decreases and then the error floor becomes worse. For the construction of PD-GLDPC codes in this subsection, I exploit the balance of the portion of degree-2 VNs, where I focus on the partial doping only for degree-2 VNs. The brief construction method is as follows. First, I construct the original base matrix $\mathbf{B}_{n_c \times n_v}$ with the large portion of degree-2 VNs. Then, I partially dope some of the protograph VNs of degree-2 to increase the minimum distance and improve their performance. Thus, irregular protographs with several degree-2 VNs are used for the construction of the proposed PD-GLDPC codes. In terms of irregular LDPC code ensembles, a large portion of degree-2 VNs enables the LDPC code to achieve the capacity approaching performance [51]. On the other hand, by reasonably selecting the number of partially doped VNs of degree-2, the property of the linear minimum distance growth with the length of the LDPC code can be guaranteed. Thus, when designing the proposed PD-GLDPC codes, balancing the partial doping over degree-2 VNs enables both the existence of a typical minimum distance and a good asymptotic performance. Optimization of irregular protograph-based LDPC code ensembles is made by initially obtaining the degree distribution of the random LDPC code ensemble using differential evolution [52] and constructing the protograph via the progressive edge growth (PEG) [53] algorithm for the construction of the proposed PD-GLPDC codes from irregular protographs. In this subsection, in order to make the CN degrees as even as possible, I try to construct the protograph from the degree distribution of a random LDPC code ensemble. I define G_c as the optimized protograph of the conventional LDPC code and G_p as the initial irregular protograph that is used to construct the PD-GLDPC code. That is, G_p can be regarded as the protograph corresponding to H_{proto} in Fig. 3.4. In order to compare FER performances of the conventional LDPC code and the proposed PD-GLDPC code under the

same degree distribution, G_c is constructed to have the same VN degree distribution as the PD-GLDPC code constructed from G_p after lifting by N.

Let $\lambda_{G_c}(x)$ and $\rho_{G_c}(x)$ be the VN and CN degree distributions of an irregular LDPC code ensemble to construct G_c, which is the optimized protograph for the conventional LDPC codes. In this subsection, I assume the degree distributions $\lambda_{G_c}(x) = \lambda_2 x + \lambda_3 x^2 + \lambda_4 x^3 + \lambda_5 x^4 + \lambda_6 x^5 + \lambda_l x^{l-1}$ and $\rho_{G_c}(x) = \rho_{r-1} x^{r-2} + \rho_r x^{r-1}$, where λ_i and ρ_i are the portions of edges of VNs and CNs of degree-i. Using the optimized degree distributions of $\lambda_{G_c}(x)$ and $\rho_{G_c}(x)$, a protograph G_c is constructed by the PEG algorithm. For the description of the protographs that construct the conventional LDPC codes and the proposed PD-GLDPC codes, let $\mathbf{D^{dv}} = (a_1, \cdots, a_{max})$ be a $|\mathbf{dv}|$-sized vector defining the numbers of protograph VNs, where a_i is the number of protograph VNs of degree l_i and $\mathbf{dv} = \{l_1, l_2, \cdots, l_{max}\}$ is a set of VN degrees that exist in the protograph.

In order to make the same VN degree distributions of the LDPC codes constructed from G_c and the PD-GLDPC codes constructed from G_p after lifting by N, optimization of $\lambda_{G_c}(x)$ and $\rho_{G_c}(x)$ should be constrained by y_{max}, which is the maximum number of bulks of protograph VNs allowed to be partially doped in G_p. Although doping granularity for the proposed PD-GLDPC code is one, I consider doping for bulks of protograph VNs in order to easily match the code rate and degree distribution because the purpose of this subsection is comparing FER performances between the conventional LDPC code and the proposed PD-GLDPC code under the same degree distribution. A PD-GLDPC code is constructed by partially doping μy protograph VNs in G_p. Construction of a PD-GLDPC code from G_p is optimized by ranging the doping bulk y, $1 \leq y \leq y_{max}$. That is, I search for the optimal value y which maximizes the coding gain between the PD-GLDPC codes constructed from G_p and the conventional protograph-based LDPC codes constructed from G_c.

Conditions for the degree distributions in order to construct G_c are derived as follows. The conditions need to guarantee two criteria: i) the VN degree distributions

Algorithm 3.3 Construction of G_c and the PD-GLDPC code

Input: μ, κ, n_v, n_c, R, l, r, y_{max}

Output: y^{opt}, G_c, G_p

1: **Step 1) Optimize degree distribution of** G_c

Optimize $\lambda_{G_c}(x) = \lambda_2 x + \lambda_3 x^2 + \lambda_4 x^3 + \lambda_5 x^4 + \lambda_6 x^5 + \lambda_l x^{l-1}$ and $\rho_{G_c}(x) = \rho_{r-1} x^{r-2} + \rho_r x^{r-1}$ using differential evolution under constraints (a)∼(c): (a) rate constraint $R = 1 - \frac{\int_0^1 \rho_{G_c}(x)dx}{\int_0^1 \lambda_{G_c}(x)dx}, 0 \leq \lambda_i \leq 1, 0 \leq \rho_i \leq 1$, (b) typical minimum distance constraint $\frac{\lambda_2/2}{\Sigma} \times n_v \leq n_c - 1 - y_{max}(\mu - \kappa) \leftrightarrow \lambda_2 \leq \frac{2\Sigma\{n_c - 1 - y_{max}(\mu-\kappa)\}}{n_v}$, and (c) G_p existence constraint $\lambda_3 \geq \frac{12\Sigma y_{max}}{n_v}, \lambda_4 \geq \frac{24\Sigma y_{max}}{n_v}, \lambda_5 \geq \frac{20\Sigma y_{max}}{n_v}, \lambda_6 \geq \frac{6\Sigma y_{max}}{n_v}$.

2: **Step 2) Construction of** G_c

From the optimized degree distribution and the random PEG algorithm, construct G_c defined as $\mathbf{D}^{(2,3,4,5,6,l)} = (a, b, c, d, e, f)$ guaranteeing a typical minimum distance.

3: **Step 3) Optimization of** G_p

For each $y = 1, 2, \cdots, y_{max}$, construct G_p defined as $\mathbf{D}^{(2,3,4,5,6,l)} = (a + 15y, b - 4y, c - 6y, d - 4y, e - y, f)$ and choose $y^{opt} \in \{y\}$ with the best threshold.

4: **Step 4) Typical minimum distance check of the PD-GLDPC code**

For the chosen y^{opt} and G_p, if there exists any cycle for the submatrix induced by undoped VNs of degree-2, go to **Step 2)**. Otherwise, output y^{opt} and G_p.

of the protograph-based LDPC code constructed from G_c and the PD-GLDPC code constructed from G_p after lifting by N are the same and ii) a typical minimum distance exists for both code ensembles. In this subsection, I assume that partial doping is conducted for the first μy degree-2 protograph VNs without loss of generality due to randomness of the PEG algorithm. For the y bulks of partially doped protograph VNs using the PCM of the $(15, 11)$ Hamming code, the numbers of protograph VNs in G_p

should be

$$\mathbf{D}^{(2,3,4,5,6,l)} = (a + 15y, b - 4y, c - 6y, d - 4y, e - y, f).$$

Given that G_c is represented as $\mathbf{D}^{(2,3,4,5,6,l)} = (a, b, c, d, e, f)$, for the existence constraint, each element of $\mathbf{D}^{(2,3,4,5,6,l)}$ should be non-negative. The parameters $a{\sim}f$ are approximated by the PEG construction as

$$a \approx \left\lfloor n_v \frac{\lambda_2/2}{\Sigma} \right\rfloor, b \approx \left\lfloor n_v \frac{\lambda_3/3}{\Sigma} \right\rfloor, c \approx \left\lfloor n_v \frac{\lambda_4/4}{\Sigma} \right\rfloor,$$

$$d \approx \left\lfloor n_v \frac{\lambda_5/5}{\Sigma} \right\rfloor, e \approx \left\lfloor n_v \frac{\lambda_6/6}{\Sigma} \right\rfloor, \text{ and } f \approx \left\lfloor n_v \frac{\lambda_l/l}{\Sigma} \right\rfloor$$

where $\Sigma = \int_0^1 \lambda_{G_c}(x)dx$. For the realization of the protograph from the degree distribution using the PEG algorithm, if the summation $a+b+c+d+e+f$ is lower than n_v, the values of $a{\sim}f$ are added by one in order starting from the lowest VN degree until the summation is equal to n_v.

If G_c is determined for a given y_{max} as $\mathbf{D}^{(2,3,4,5,6,l)} = (a, b, c, d, e, f)$, where $a+b+c+d+e+f = n_v$, G_p defined by $\mathbf{D}^{(2,3,4,5,6,l)} = (a+15y, b-4y, c-6y, d-4y, e-y, f)$ can be constructed for $y = 1, \cdots, y_{max}$. By allowing the PEG algorithm of the VN degree distribution over a base matrix with size $\{n_c - (\mu - \kappa)y\} \times n_v$, both the code rate and the VN degree distributions for the LDPC codes constructed from G_c and the proposed PD-GLDPC codes constructed from G_p after lifting by N are matched. I search for the value of y, which has the best PEXIT threshold while having a typical minimum distance. The optimized doping value is denoted as y^{opt}. The construction of G_c and the PD-GLDPC code is described in Algorithm 3.3.

The protograph of the conventional protograph-based LDPC code, G_c is made for $y_{max} = 5, 10, 15$ for the half-rate protograph-based LDPC code ensemble. The numerical results are summarized in Table 3.1, where the coding gain given for the proposed PD-GLDPC code is compared to the conventional protograph-based LDPC code with the equal degree distribution.

Table 3.1: Simulation results for optimized PD-GLDPC codes from irregular protographs using Algorithm 3.2, where $l = 20, n_v = 400$, and $R = 1/2$

y_{max}	$\lambda_{G_c}(x), \rho_{G_c}(x)$ (threshold)	G_c protograph $\mathbf{D}^{(2,3,4,5,6,20)}$ / G_c threshold	G_p protograph $\mathbf{D}^{(2,3,4,5,6,20)}$, y^{opt} / PD-GLDPC threshold	Coding gain
5	$\lambda_{G_c}(x) = 0.2049x + 0.2489x^2 + 0.1150x^3 + 0.074x^4 + 0.0210x^5 + 0.3363x^{19}$ $\rho_{G_c}(x) = 0.9735x^7 + 0.0265x^8$ (0.4815)	$(165, 134, 47, 23, 5, 26)$ / 0.4620	$(240, 114, 17, 3, 0, 26)$, $y^{opt} = 5$ / 0.4699	0.0079
10	$\lambda_{G_c}(x) = 0.1894x + 0.2255x^2 + 0.1431x^3 + 0.1191x^4 + 0.0357x^5 + 0.2872x^{19}$ $\rho_{G_c}(x) = 0.9908x^7 + 0.0012x^8$ (0.4696)	$(152, 121, 57, 38, 9, 23)$ / 0.4523	$(287, 85, 3, 2, 0, 23)$, $y^{opt} = 9$ / 0.4638	0.0115
15	$\lambda_{G_c}(x) = 0.1632x + 0.1758x^2 + 0.2143x^3 + 0.1827x^4 + 0.0543x^5 + 0.2098x^{19}$ $\rho_{G_c}(x) = 0.9940x^7 + 0.0060x^8$ (0.4476)	$(131, 94, 86, 59, 14, 16)$ / 0.4352	$(341, 38, 2, 3, 0, 16)$, $y^{opt} = 14$ / 0.4534	0.0182

3.3.3 Optimization of PD-GLDPC Codes Using Protograph Differential Evolution

In this subsection, I propose the optimization method of the protograph for the proposed PD-GLDPC codes using the differential evolution algorithm. Similar to the differential evolution algorithm in [50], I use the differential evolution algorithm to find the protograph with the optimized BEC threshold. The parameters for the differential evolution are as follows. The number of generations of the algorithm g is set to 6000. Each entry of the base matrix can have the integer value varying from 0 to a positive integer t. The number of base matrices examined for each generation instance is defined as N_p. For a given base matrix size $n_c \times n_v$, I fix $N_p = 10 \cdot n_c n_v$. The mutation parameter F is fixed to 0.5 and α is a uniform random variable with the domain $[0, 1]$. Lastly, the crossover probability p_c is fixed to 0.88 in this dissertation. I define the optimized PD-LDPC code ensemble as C_1 and the optimization algorithm is given in Algorithm 3.4. It is clear that while the optimization process is the same as that of the protograph-based LDPC codes, the indices of the partial doping represented by $\mathcal{X}$ are included, which show the protograph VNs that are doped by GC nodes. Also, the criterion for the existence of the typical minimum distance derived in Theorem 1 is

Algorithm 3.4 Differential evolution algorithm to design the base matrix of the PD-GLDPC codes

Input: μ, κ, n_c, n_v, $\mathcal{X}$, g, t, N_p, p_c, F, α

Output: $\mathbf{B}_{n_c \times n_v}$

1: **Initialization:** Set the initial base matrices $(\mathbf{B}_1, \ldots, \mathbf{B}_{N_p})$ each with size $n_c \times n_v$ randomly, where each entry is chosen from $\{0, \ldots, t\}$.

2: **for** $m = 1 : g$ **do**

3: **Mutation:** For each $k \in \{1, \ldots, N_p\}$, the mutation matrices are created through the interpolation as follow:

$$[\mathbf{M}_k]_{i,j} = [\mathbf{B}_{r_1}]_{i,j} + (F + \alpha(1 - F))([\mathbf{B}_{r_2}]_{i,j} - [\mathbf{B}_{r_3}]_{i,j})$$

where $[\mathbf{A}]_{i,j}$ is the (i, j) element of the matrix $\mathbf{A}$ and indices $r_i \in [N_p], i = 1, 2, 3$ are distinct and randomly selected. Each entry of $\mathbf{M}_k$ is replaced with the nearest integer in $\{0, \ldots, t\}$.

4: **Crossover:** For each $k \in \{1, \ldots, N_p\}$, create the trial matrices $\mathbf{M'}_k$ such that $[\mathbf{M'}_k]_{i,j} = [\mathbf{M}_k]_{i,j}$ with a probability p_c and $[\mathbf{M'}_k]_{i,j} = [\mathbf{B}_k]_{i,j}$ with probability $1 - p_c$. If $\mathbf{M'}_k$ contains any cycles only consisting of undoped degree-2 protograph VNs, $\mathbf{M'}_k$ is regenerated.

5: **Selection:** The base matrices for $(m + 1)$th generation are chosen between $\mathbf{B}_k$ and $\mathbf{M'}_k$. If the threshold of $\mathbf{B}_k$ is larger than $\mathbf{M'}_k$, no update is made. Otherwise, update $\mathbf{B}_k$ to $\mathbf{M'}_k$.

6: **end for**

7: From $\mathbf{B}_k, k \in [N_p]$, choose the matrix with the best threshold value and output $\mathbf{B}_{n_c \times n_v}$.

used during the construction of new trial matrices for the proposed PD-GLDPC codes. The component code used in the following optimization is a $(15, 11)$ Hamming code.

I optimize the protograph for the PD-GLDPC codes for base matrices with size 8×16 and 4×12. I set $\mathcal{X} = \{1, 2\}$ and $t = 5$ for $\mathbf{B}_{8\times16}$, $\mathcal{X} = \{1\}$ and $t = 3$ for $\mathbf{B}_{4\times12}$. Let the resulting base matrix of the optimization be $\mathbf{B}^{C_1}_{n_c\times n_v}$ for both cases. The optimized base matrix results are

$$\mathbf{B}^{C_1}_{8\times16} = \begin{bmatrix} \mathbf{5} & \mathbf{2} & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ \mathbf{4} & \mathbf{0} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ \mathbf{5} & \mathbf{5} & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ \mathbf{5} & \mathbf{0} & 1 & 0 & 2 & 1 & 5 & 5 & 0 & 0 & 5 & 5 & 0 & 5 & 0 & 3 \\ \mathbf{5} & \mathbf{3} & 0 & 1 & 1 & 1 & 5 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 2 & 0 \\ \mathbf{0} & \mathbf{0} & 1 & 0 & 0 & 0 & 0 & 1 & 4 & 1 & 3 & 0 & 0 & 2 & 1 & 0 \\ \mathbf{4} & \mathbf{0} & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ \mathbf{0} & \mathbf{5} & 0 & 0 & 0 & 0 & 1 & 0 & 3 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{bmatrix}, \tag{3.3}$$

$$\mathbf{B}^{C_1}_{4\times12} = \begin{bmatrix} \mathbf{3} & 0 & 0 & 3 & 1 & 3 & 0 & 1 & 2 & 2 & 3 & 0 \\ \mathbf{3} & 0 & 1 & 3 & 1 & 0 & 0 & 0 & 1 & 2 & 0 & 1 \\ \mathbf{3} & 1 & 0 & 3 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 2 \\ \mathbf{3} & 3 & 3 & 3 & 0 & 0 & 3 & 1 & 0 & 1 & 0 & 0 \end{bmatrix}. \tag{3.4}$$

The base matrix for $\mathbf{B}^{C_1}_{8\times16}$ is in (3.3), which has the BEC threshold 0.5227 with the code rate 0.4667 and the base matrix for $\mathbf{B}^{C_2}_{4\times12}$ is given in (3.4), which has the BEC threshold of 0.5227 with the code rate 0.6444. The bolded parts in the matrix represent VNs that are partialy doped. The results show that the VN with the highest degree is partially doped. From these optimization results, I can expect that partially doping high degree VNs and puncturing some portion of them for rate matching can improve the performance of the proposed PD-GLDPC codes.

The approach of partially doping and puncturing is a similar techique to the precoding and puncturing. Precoding and puncturing high degree VNs in a protograph is a well known technique in order to enhance the threshold of protograph-based LDPC codes [54]. Precoding takes place by placing a CN between a degree-1 VN and a high

degree VN. In order to compensate for the rate loss, the high degree VN is punctured. From some intuition of our optimization results and well known concepts of precoding, I apply a similar approach of the precoding technique for the proposed PD-GLDPC codes.

I first define ρ_d as the portion of random puncturing for VNs that are doped. For the BEC, I use the concept in [55] to derive ρ_d. For a target code rate R^*, the random puncturing ratio ρ is $1 - \frac{R}{R^*}$. Thus, ρ_d is derived as $\rho_d = \rho \cdot \frac{n_v}{|\mathcal{X}|}$ and I use it for the computation of the EXIT during the optimization algorithm. The channel values for the partially doped VNs become $I_{ch}(j) = 1 - \{\rho_d + (1-\rho_d)\epsilon\}$, $j \in \mathcal{X}$. Thus, it is possible to construct the PD-GLDPC codes for the target code rate by using the random puncturing method.

For the construction of PD-GLDPC codes with the target code rate $R^* = 1/2$, the base matrix $\mathbf{B}_{8\times 16}$ is optimized using Algorithm 3.4 for $\mathcal{X} = \{1, 2\}$, $\rho_d = 0.5333$, and $t = 5$. Likewise, for the target code rate $R^* = 2/3$, the base matrix $\mathbf{B}_{4\times 12}$ is optimized for $\mathcal{X} = \{1\}$, $\rho_d = 0.4058$, and $t = 3$. Let the resulting base matrix be $\mathbf{B}^{C_2}_{n_c\times n_v}$ for the optimized results of the protographs constructed by puncturing partially doped VNs. The optimized base matrices for both code rates are

$$\mathbf{B}^{C_2}_{8\times 16} = \begin{bmatrix} \mathbf{2} & \mathbf{0} & 5 & 2 & 1 & 3 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ \mathbf{2} & \mathbf{0} & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ \mathbf{1} & \mathbf{2} & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ \mathbf{1} & \mathbf{0} & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 2 & 1 & 0 & 2 & 1 & 2 & 0 \\ \mathbf{2} & \mathbf{0} & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ \mathbf{1} & \mathbf{1} & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 2 & 1 & 1 & 0 \\ \mathbf{0} & \mathbf{0} & 0 & 1 & 2 & 0 & 4 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 3 & 1 \\ \mathbf{3} & \mathbf{1} & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}, \tag{3.5}$$

$$\mathbf{B}^{C_2}_{4\times 12} = \begin{bmatrix} \mathbf{2} & 0 & 0 & 1 & 0 & 0 & 3 & 2 & 1 & 0 & 2 & 2 \\ \mathbf{2} & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 2 & 2 \\ \mathbf{3} & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\ \mathbf{2} & 1 & 2 & 0 & 3 & 2 & 0 & 0 & 1 & 3 & 0 & 3 \end{bmatrix}, \tag{3.6}$$

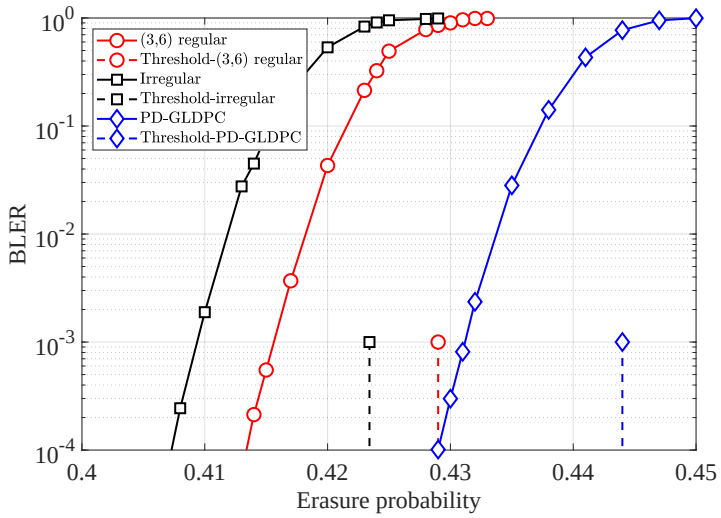
where the resulting base matrix for $R^* = 1/2$ is given in (3.5) and the resulting base matrix for $R^* = 2/3$ is given in (3.6). The resulting thresholds of the optimized base matrices are 0.486 and 0.319 for target code rates $R^* = 1/2$ and $R^* = 2/3$, respectively. The optimization results show that the constructed PD-GLDPC codes have capacity approaching performances and the average VN density is reduced by huge amount compared to $\mathbf{B}^{C_1}_{n_c \times n_v}$. Since the base matrix $\mathbf{B}^{C_2}_{n_c \times n_v}$ is driven from the random puncturing of partially doped VNs, I define the constructed PD-GLDPC code ensemble with parameters $(\mathbf{B}^{C_2}_{n_c \times n_v}, \mu, \kappa, \mathcal{X}, \rho_d)$.

3.4 Numerical Results and Analysis

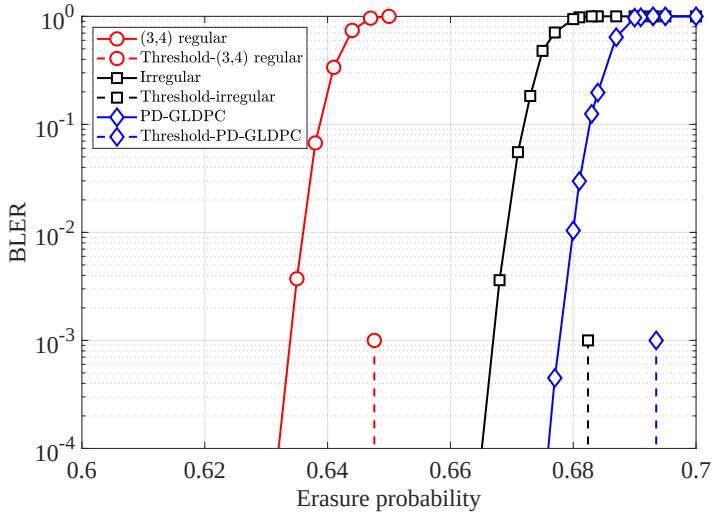
In this section, I propose the optimized protograph design and show the FER of the proposed PD-GLDPC codes. The performance of the conventional protograph-based LDPC code is compared with that of the proposed PD-GLDPC code. Two methods of comparison are conducted. The first subsection compares them under the same degree distribution using Algorithm 3.2 and Algorithm 3.3 for both regular and irregular protographs, respectively. The second subsection compares the performance of the PD-GLDPC codes constructed without the degree distribution constraints using Algorithm 3.4 to the state-of-the-art protograph-based LDPC codes.

3.4.1 Simulation Result for Optimized PD-GLDPC Code from Regular and Irregular Random LDPC Code Ensembles

For numerical analysis, I use a $(15, 11)$ systematic Hamming code as the component code. For a half-rate code, I construct a $(\mathbf{B}_{\{200-4y\}\times 400}, 15, 11, 75, 15y)$ protograph-based PD-GLDPC code, for a given y. Since the doping of single protograph variable node requires $\mu - \kappa = 4$ additional protograph rows, the original protograph should have a total of $200 - 4y$ rows to construct a half-rate protograph-based PD-GLDPC code. In order to satisfy the typical minimum distance property for the proposed PD-



(a) $R = \frac{1}{2}$



(b) $R = \frac{1}{4}$

Figure 3.6: Comparison of threshold and BLER for the regular LDPC codes, irregular protograph-based LDPC codes, and the protograph-based PD-GLDPC codes from a regular protograph for code rates $1/2$ and $1/4$.

GLDPC code, I make sure that there are no cycles among the undoped degree-2 variable nodes if $y \geq \frac{400-(200-4y)+1}{15} \leftrightarrow y \geq \frac{400-200+1}{11} \approx 18.27$ during the PEG process of regular base matrix construction. For $y = 19, 20, \cdots$, the best threshold is when $y = 19$, having a BEC threshold of 0.444. For comparison, I construct a $(3, 6)$ regular protograph with size 200×400 and lift it by 75, which has a threshold of 0.429. Also, by comparing an irregular protograph-based LDPC code that has the same degree distribution as the constructed protograph-based PD-GLDPC code, I can find the performance gain from BP decoding to MAP decoding over GC nodes. Since the doping of protograph variable nodes in the proposed protograph-based PD-GLDPC codes occurs only over degree-2 variable nodes, the degrees of $y\mu$ protograph variable nodes will change. Since the PCM of a $(15, 11)$ systematic Hamming code has 4 degree-1 columns, 6 degree-2 columns, 4 degree-3 columns, and 1 degree-4 column, the conventional irregular LDPC protograph without doping having the same variable node degree distribution with the proposed protograph-based PD-GLDPC code is defined as $\mathbf{D}^{(2,3,4,5,6)} = (115, 76, 114, 76, 19)$. Irregular protograph-based LDPC code and the (3,6) regular protograph-based LDPC code are constructed from the 200×400 protograph and the protograph-based PD-GLDPC code is constructed from the 124×200 protograph with $x = y\mu = 285$. The irregular protograph-based LDPC code also has the same variable node degree distribution as the proposed protograph-based PD-GLDPC code, where it is defined by $\mathbf{D}^{(2,3,4,5,6)} = (115, 76, 114, 76, 19)$. Using the PEG algorithm, I construct the irregular protograph-based LDPC code, having a threshold of 0.4234. The BLER performances of the constructed irregular protograph-based LDPC code, protograph-based PD-GLDPC code, and a $(3, 6)$ regular code with $(n, k) = (30000, 15000)$ are shown in Fig. 3.6(a), where all three codes are half rate LDPC codes constructed by $N = 75$. The coding gain of the constructed protograph-based PD-GLDPC code is 0.021 and 0.015 compared to irregular protograph-based LDPC code and $(3, 6)$ regular protograph-based LDPC code, respectively.

Similarly, I construct a $(\mathbf{B}_{\{300-4y\}\times 400}, 15, 11, 105, 15y)$ protograph-based PD-GLDPC code for code rate $1/4$. For $y \geq \frac{400-(300-4y)+1}{15} \leftrightarrow y \geq \frac{400-300+1}{11} \approx 9.18$, the optimized threshold is the highest value 0.6935 at $y = 10$. Similar to the half-rate case, I construct a $(3, 4)$ regular protograph-based LDPC code using the PEG algorithm to have a threshold of 0.647. The irregular protograph ensemble has a variable degree distribution of $\mathbf{D}^{(2,3,4,5,6)} = (250, 40, 60, 40, 10)$ and the threshold is 0.6883. The irregular protograph-based LDPC code and the $(3, 4)$ regular protograph-based LDPC code are constructed from the 300×400 protograph and the protograph-based PD-GLDPC code is constructed from the 260×400 protograph with $x = y\mu = 150$. The irregular protograph also has the same variable node degree distribution as the protograph-based PD-GLDPC code, where it is defined by $\mathbf{D}^{(2,3,4,5,6)} = (250, 40, 60, 40, 10)$. All the codes are lifted by 105 to make $(42000, 10500)$ codes and the numerical results are in Fig. 3.6(b). The coding gain of the constructed protograph-based PD-GLDPC code is 0.0052 and 0.0465 compared to irregular protograph-based LDPC code and $(3, 4)$ regular protograph-based LDPC code, respectively.

As the performance comparison with the existing GLDPC codes, I use the random GLDPC code ensemble with the threshold 0.466 in [39] that is represented as $\lambda(x) = 0.8x^2 + 0.01x^3 + 0.01x^5 + 0.18x^7$ and a doping portion of 40% by the Hamming code. Fig. 3.7 shows performance comparison of three half-rate codes which are the random ensemble-based GLDPC code in [39], the irregular protograph-based LDPC code constructed from G_c, and the proposed PD-GLDPC code constructed from G_p in Table 3.1, where $y_{max} = 5$. All three codes in Fig. 3.7 are $(n, k) = (30000, 15000)$ codes of the half-rate, where G_c is defined as $\mathbf{D}^{(2,3,4,5,6,20)} = (165, 134, 47, 23, 5, 26)$ and has the same VN degree distribution as the PD-GLDPC code after lifting by $N = 75$. $x = \mu y = 75$ protograph VNs are partially doped in the PD-GLDPC code. The constructed PD-GLDPC code for $y_{max} = 5$ has a coding gain of 0.0079 and 0.0039 compared to the GLDPC code in [39] and the irregular protograph-based LDPC code from G_c, respectively.

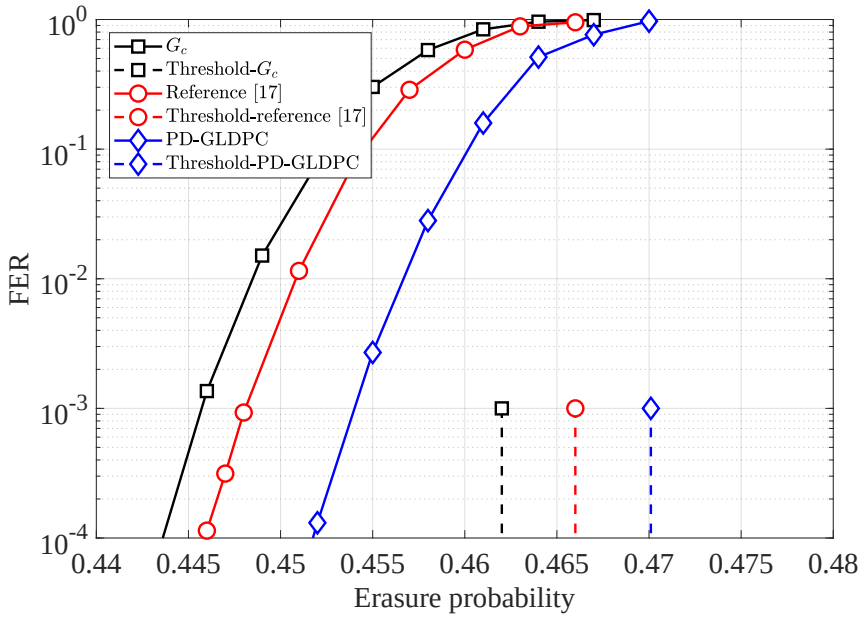


Figure 3.7: Comparison of the BEC threshold and FER for the irregular protograph-based LDPC code from G_c, the conventional random GLDPC code from the ensemble in [39], and the PD-GLDPC code from G_p for the code rate $1/2$.

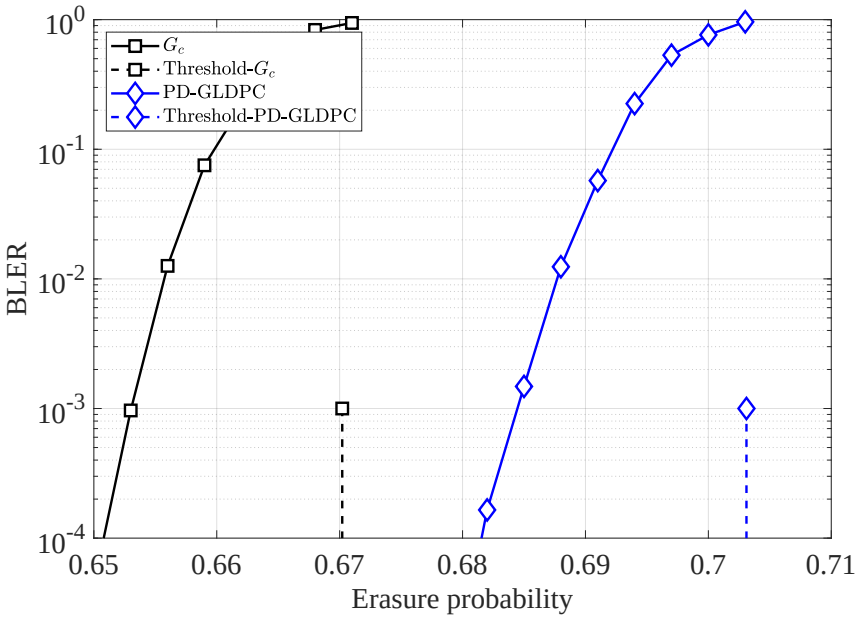


Figure 3.8: Comparison of threshold and BLER for the irregular protograph-based LDPC code from G_c and the proposed protograph-based PD-GLDPC code from G_p for code rate $1/4$.

Similarly, the construction of G_c is made for the code rate $1/4$ case. I simulate the proposed protograph-based PD-GLDPC with the small doping case, where the optimization of random ensemble for G_c is done under the constraint $y_{max} = 3$. The degree distribution of the optimized results is obtained as

$$\lambda_{G_c}(x) = 0.2858x + 0.1218x^2 + 0.0533x^3 + 0.0369x^4 + 0.0095x^5 + 0.4927x^{29},$$

$$\rho_{G_c}(x) = 0.9995x^5 + 0.0005x^6,$$

which makes G_c with $\mathbf{D}^{(2,3,4,5,6,30)} = (258, 74, 24, 13, 2, 29)$ via the PEG algorithm. The threshold of the proposed protograph-based PD-GLDPC code is best when $y = 2$ and for this instance, G_p is then defined as $\mathbf{D}^{(2,3,4,5,30)} = (288, 66, 12, 5, 29)$. Both codes are $(n, k) = (42000, 10500)$ codes of code rate $1/4$, where G_c is defined as $\mathbf{D}^{(2,3,4,5,6,30)} = (258, 74, 24, 13, 2, 29)$ and has the same variable node degree distribution as G_p after lifting by $N = 105$. $x = y\mu = 30$ protograph variable nodes are partially doped in the protograph-based PD-GLDPC code. The simulation result of both the irregular protograph-based LDPC code and the proposed protograph-based PD-GLDPC code are shown for the same variable node degree distribution in Fig. 3.8. The thresholds of G_c and the proposed PD-GLDPC code are 0.6702 and 0.7031, respectively, where the coding gain is 0.0329 compared to the irregular protograph-based LDPC code. Figs. 3.7 and 3.8 show that the proposed PD-GLDPC code has a good performance both in the waterfall and the low error floor region due to the fact that the code is optimized by increasing the doping as much as possible, and at the same time, the typical minimum distance constraint is satisfied. In terms of the asymptotic analysis, increasing the portion of degree-2 VNs increases the possibility of the code to approach the channel capacity [51]. However, the existence of a typical minimum distance of the protograph is also important, which upper bounds the portion of degree-2 VNs in the LDPC code. Thus, balancing the portion of degree-2 VNs is needed in order to satisfy both a typical minimum distance condition and a good threshold. The proposed PD-GLDPC code guarantees the balance of the degree-2 VNs by carefully

Table 3.2: Comparison for thresholds and average VN degrees of protographs for the BEC

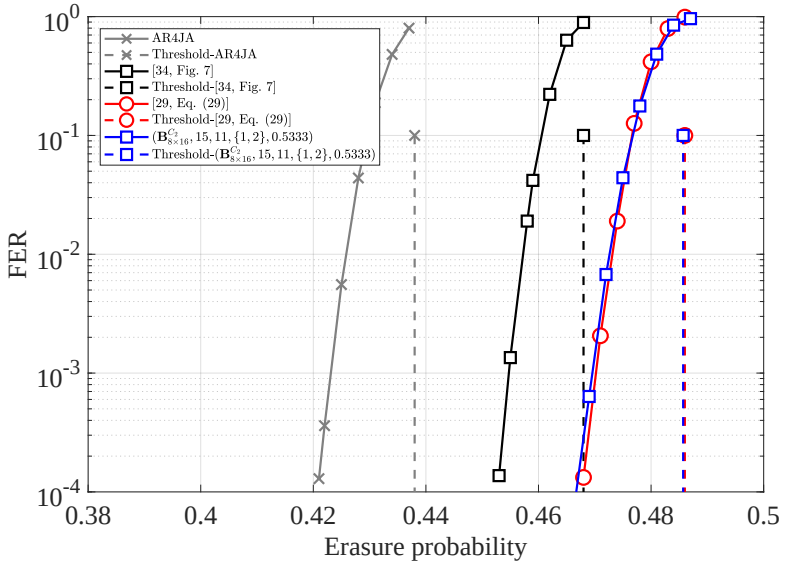
Code type	Code rate	Protograph size	Threshold	Average variable node degree	Gap to capacity
AR4JA [45]	0.5	3×5	0.438	3	0.062
Protograph [34, Fig. 7]	0.5	4×8	0.468	4.25	0.032
Protograph [50]	0.5	8×16	0.486	5.25	0.014
PD-GLDPC	0.5	8×16	0.4857	4.58	0.0143
AR4JA [45]	0.67	3×7	0.287	3.29	0.046
Protograph [34, Fig. 7]	0.67	2×6	0.292	5	0.041
Protograph [50]	0.67	4×12	0.320	5.08	0.013
PD-GLDPC	0.67	4×12	0.319	4.09	0.014

choosing the rate of the protograph code and the number of doping on degree-2 VNs.

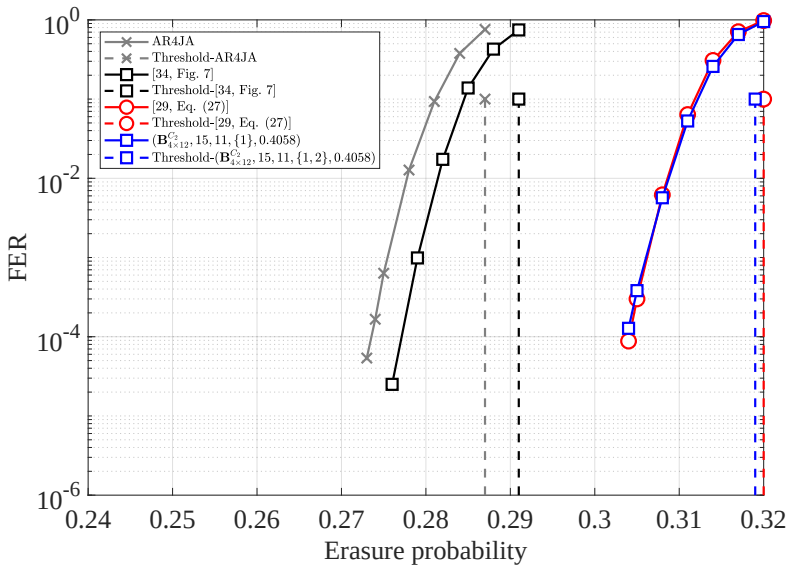
3.4.2 Simulation Result for PD-GLDPC Code from Optimized Protograph

The proposed PD-GLDPC codes for $R^* = 1/2$ and $R^* = 2/3$ are constructed from the ensembles $(\mathbf{B}^{C_2}_{8\times16}, 15, 11, \{1, 2\}, 0.5333)$ and $(\mathbf{B}^{C_2}_{4\times12}, 15, 11, \{1\}, 0.4058)$, respectively. The protographs are shown in (3.5) and (3.6). The AR4JA [45] and block protograph codes in [45, 50] of the same code rate are used for performance comparison. I first compare the threshold and average VN degree between the proposed PD-GLDPC code ensemble and the aforementioned protograph-based LDPC code ensembles in Table 3.2. The average VN degree of the PD-GLDPC code considers both the base matrix and the edges added from the partial doping. The results show that the asymptotic performance of the proposed PD-GLDPC code ensemble outperforms the AR4JA and block protograph introduced in [45]. The average VN degree of the PD-GLDPC codes is low while having the asymptotic performance comparable to the capacity approaching protographs introduced in [50].

By using the PEG algorithm, the protographs are lifted to construct $(48000, 24000)$



(a) $R^* = \frac{1}{2}$



(b) $R^* = \frac{2}{3}$

Figure 3.9: FER comparison for the constructed protograph-based LDPC codes from AR4JA [45], protograph [34, Fig. 7], protograph [50], and the proposed ensemble $(\mathbf{B}^{C_2}_{n_c\times n_v}, 15, 11, \mathcal{X}, \rho_d)$.

PD-GLDPC code for $R^* = 1/2$. The protograph AR4JA and LDPC protographs in [45, 50] are lifted to the same code length. The FER results are shown in Fig. 3.9(a). Likewise, the protograph of the PD-GLDPC and the protographs of AR4JA and [45, 50] are lifted to construct $(45000, 30000)$ codes for $R^* = 2/3$. The FER results are shown in Fig. 3.9(b). For both code rates $R^* = 1/2$ and $R^* = 2/3$, the FER of the proposed PD-GLDPC code shows tangible gain compared to the AR4JA code and protograph code in [45]. Also, the performance is comparable to the capacity approaching block LDPC code in [50]. The partial doping and puncturing technique, which is similar to the precoding techinique, shows that the capacity approaching PD-GLDPC codes can be constructed with the relatively low average VN degree.

3.5 Proof of Theorem 1: The Constraint for the Existence of the Typical Minimum Distance of the Proposed Protograph-Based PD-GLDPC Codes

A proof for the constraint of the existence of a typical minimum distance for the proposed protograph-based PD-GLDPC codes is given in this section. Similar to that in [49], a typical minimum distance is driven by the weight enumerator analysis over the lifted protograph. In order to use the notations in [49], I've distinguished the indexing notations during the enumeration for the partially doped variable nodes using $'$. Also, the c_j and v_i notations are used for the check nodes and the variable nodes, respectively. Suppose that the proposed protograph-based PD-GLDPC code is constructed from the protograph defined by $G = (V, C, E)$ and the x variable nodes are partially doped, where component codes are identical with the parameters (μ, κ). A variable node set $V = \{v_1, \cdots, v_{n_v}\}$ and a check node set $C_{PD\text{-}GLDPC} = B_{Hamm} \cup C = \{b_1, \cdots, b_x\} \cup \{c_1, \cdots, c_{n_c}\}$ are given for the protograph. It is important to note that the GC node set B_{Hamm} is not defined over a protograph. However, the

codeword enumeration can be made when the protograph is lifted, where $b_{i'}, i' \in [x]$ is a virtual check node that represents the Hamming check nodes used for partial doping for $v_{i'}$ in the original protograph. Although $b_{i'}$ is not a protograph check node, I define it for the enumeration of the partially doped protograph variable nodes. The protograph-based PD-GLDPC code is constructed by lifting the graph G by N times and permuting the replicated edges. Each v_i (c_j) has degree q_{v_i} (q_{c_j}) and each $b_{i'}$ has degree μ. For the enumeration of the GC node $b_{i'}$, it can be thought as a protograph node of degree μ that is lifted by a factor of $\frac{N}{\mu}$. The upper bound of the weight enumerator of the proposed protograph-based PD-GLDPC code with weight d, denoted as $A_d^{PD\text{-}GLDPC}$ is derived as follows.

Let $w_{m,u}, u \in [q_{v_m}]$ be the uth edge weight from a variable node v_m. For a partially doped variable node $v_m, m \in [x]$, there are μ weights sent towards the incident GC node, where the uth weight is defined as $w'_{m,u}, u \in [\mu]$. For a given input weight vector $\mathbf{d} = (d_1, \cdots, d_{n_v})$, I need to calculate $A^{PD\text{-}GLDPC}(\mathbf{d})$ and sum it over every instance of $\mathbf{d}$ that satisfies $d = d_1 + \cdots + d_{n_v}$. For input $d_{i'}, i' \in [x]$, it is clear that $\sum_{i=1}^{\mu} w'_{m,i} = d_{i'}$ because the extrinsic weight $w'_{m,i}$ consists of weights solely from v_m. I introduce the following notations:

- $A_{d_i}^{v_i}(\mathbf{w}_i) = \binom{N}{d_i}\delta_{d_i,w_{i,1}}, \cdots, \delta_{d_i,w_{i,q_{v_i}}} = \begin{cases} \binom{N}{d_i}, & \text{if } w_{i,j} = d_i, \forall j \in [q_{v_i}] \\ 0, & \text{otherwise} \end{cases}$ is the vector weight enumerator for a variable node v_i of the protograph [49].

- $A^{c_j}(\mathbf{z}_j)$ is the vector weight enumerator for a check node c_j of the original protograph, for the incoming weight vector $\mathbf{z}_j = [z_{j,1}, \cdots, z_{j,q_{c_j}}]$ [49].

- $B_{d_{i'}}^{v_{i'}}(\mathbf{w}'_{i'}) = \begin{cases} 1, & \text{for } w'_{i',1} + \cdots + w'_{i',\mu} = d_{i'} \\ 0, & \text{otherwise} \end{cases}$ is the vector weight enumerator for partially doped variable nodes $v_{i'}$, $i' \in [x]$.

- $B^{b_{i'}}(\mathbf{w}'_{i'})$ is the vector weight enumerator for check nodes that are created during the lifting process given the weight vector $\mathbf{w}'_{i'}$. $A^{b_{i'}}(d_{i'})$ is the summation

of enumerators over all possible $\mathbf{w}'_{i'}$ values given that $w'_{i',1} + \cdots + w'_{i',\mu} = d_{i'}$ satisfying

$$A^{b_{i'}}(d_{i'}) = \sum_{\mathbf{w}'} B^{b_{i'}}(\mathbf{w}'_{i'}) = \sum_{\mathbf{w}'} \sum_{\{\mathbf{m}\}} C(\frac{N}{\mu}; m_1, \cdots, m_K),$$

where $\mathbf{w}' = (w'_1, \cdots, w'_\mu)$ such that $\sum_{i=1}^{\mu} w'_1 = d'_k,\ w'_i \leq \frac{N}{\mu}$.

Then, the weight enumerator is given as

$$A_d^{PD-GLDPC} = \sum_{\{\mathbf{d}\}} A^{PD-GLDPC}(\mathbf{d})$$

where

$$\begin{aligned} A^{PD\text{-}GLDPC}(\mathbf{d}) &= \frac{\prod_{i=1}^{n_v} A_{d_i}^{v_i}(\mathbf{w}_i) \prod_{j=1}^{n_c} A^{c_j}(\mathbf{z}_j) \times \prod_{i'=1}^{x} B_{d_{i'}}^{v_{i'}}(\mathbf{w}'_{i'}) B^{b_{i'}}(\mathbf{w}'_{i'})}{\prod_{s=1}^{n_v} \prod_{r=1}^{q_{v_s}} \binom{N}{w_{s,r}} \times \prod_{s'=1}^{x} \prod_{r'=1}^{\mu} \binom{\frac{N}{\mu}}{w'_{s',r'}}} \\ &= \sum_{\{\mathbf{w}'_{i'}: w'_{i',1} + \cdots + w'_{i',\mu} = d_{i'}\}} \frac{\prod_{j=1}^{n_c} A^{c_j}(\mathbf{d}_j) \times \prod_{i'=1}^{x} B^{b_{i'}}(\mathbf{w}'_{i'})}{\prod_{i=1}^{n_v} \binom{N}{d_i}^{q_{v_i}-1} \times \prod_{s'=1}^{x} \prod_{r'=1}^{\mu} \binom{\frac{N}{\mu}}{w'_{s',r'}}}. \end{aligned}$$

The solution to the equation $\mathbf{w}' = \mathbf{m}\mathbf{M}^{\mathbf{C}}$ is given as $\mathbf{m} = \{m_1, \cdots, m_K\}$. The term $\binom{\frac{N}{\mu}}{w'_{s',r'}}$ is lower bounded by $(\frac{N}{\mu})^{w'_{s',r'}} e^{-w'_{s',r'} \cdot \ln w'_{s',r'}}$. Then, $A^{PD-GLDPC}(\mathbf{d})$ can be upper bounded as

$$\begin{aligned} A^{PD\text{-}GLDPC}(\mathbf{d}) &\leq \sum_{\{\mathbf{w}'_{i'}: w'_{i',1} + \cdots + w'_{i',\mu} = d_{i'}\}} \frac{\prod_{j=1}^{n_c} A^{c_j}(\mathbf{d}_j) \times \prod_{i'=1}^{x} B^{b_{i'}}(\mathbf{w}'_{i'})}{\prod_{i=1}^{n_v} \binom{N}{d_i}^{q_{v_i}-1} \times \prod_{s'=1}^{x} \prod_{r'=1}^{\mu} (\frac{N}{\mu})^{w'_{s',r'}} e^{-w'_{s',r'} \cdot \ln w'_{s',r'}}} \\ &\leq \sum_{\{\mathbf{w}'_{i'}: w'_{i',1} + \cdots + w'_{i',\mu} = d_{i'}\}} \frac{\prod_{j=1}^{n_c} A^{c_j}(\mathbf{d}_j) \times \prod_{i'=1}^{x} B^{b_{i'}}(\mathbf{w}'_{i'})}{\prod_{i=1}^{n_v} \binom{N}{d_i}^{q_{v_i}-1} \times \prod_{s'=1}^{x} (\frac{N}{\mu})^{d_{s'}} e^{-d_{s'} \cdot \ln d_{s'}}} \\ &\leq \sum_{\{\mathbf{w}'_{i'}: w'_{i',1} + \cdots + w'_{i',\mu} = d_{i'}\}} \frac{\prod_{j=1}^{n_c} A^{c_j}(\mathbf{d}_j) \times \prod_{i'=1}^{x} B^{b_{i'}}(\mathbf{w}'_{i'})}{\prod_{i=1}^{n_v} \binom{N}{d_i}^{q_{v_i}-1} \times (\frac{N}{\mu})^{P} e^{-P \cdot \ln P}} \\ &= \frac{\prod_{j=1}^{n_c} A^{c_j}(\mathbf{d}_j) \times \prod_{i'=1}^{x} \sum_{\{\mathbf{w}'_{i'}: w'_{i',1} + \cdots + w'_{i',\mu} = d_{i'}\}} B^{b_{i'}}(\mathbf{w}'_{i'})}{\prod_{i=1}^{n_v} \binom{N}{d_i}^{q_{v_i}-1} \times (\frac{N}{\mu})^{P} e^{-P \cdot \ln P}} \\ &= \frac{\prod_{j=1}^{n_c} A^{c_j}(\mathbf{d}_j) \times \prod_{i'=1}^{x} A^{b_{i'}}(d_{i'})}{\prod_{i=1}^{n_v} \binom{N}{d_i}^{q_{v_i}-1} \times (\frac{N}{\mu})^{P} e^{-P \cdot \ln P}} \end{aligned} \tag{3.7}$$

where $P = \sum_{s'=1}^{x} d_{s'}$ is the total weight of the x partially doped variable nodes. Then $\sum_t (t \cdot \ln t) \leq (\sum_t t) \cdot \ln (\sum_t t)$ is used for the second and the third inequalities in (3.7). It was shown in (18) of [49] that the inequality

$$\frac{\prod_{j=1}^{n_c} A^{c_j}(\mathbf{d}_j)}{\prod_{i=1}^{n_v} \binom{N}{d_i}^{q_{v_i}-1}} \leq \prod_{i=1}^{n_v} e^{(q_{v_i}-1-\frac{q_{v_i}}{d_{min}^{(c)}})d_i \ln \frac{d_i}{N} + \frac{q_{v_i}(2+k_{max}^{(c)} \ln 2)}{d_{min}^{(c)}} d_i}$$

holds, where $d_{min}^{(c)}$ is the minimum distance of an SPC component code for the original protograph and $k_{max}^{(c)}$ is the maximum number of codewords of an SPC component code. Using the similar notations in [49], let $d_{min}^{(b)}$ and $k^{(b)}$ be the minimum distance and the number of codewords of the (μ, κ) component code for the GC nodes. Then, $\prod_{i'=1}^{x} A^{b_{i'}}(d_{i'})$ is upper bounded as

$$\begin{aligned}
\prod_{i'=1}^{x} A^{b_{i'}}(d_{i'}) &\leq \prod_{i'=1}^{x} \sum_{\{\mathbf{w}'_{i'}: w'_{i',1}+\cdots+w'_{i',\mu}=d_{i'}\}} \prod_{i=1}^{\mu} (\frac{N}{\mu})^{\frac{1}{d_{min}^{(b)}} w'_{i',i}} e^{\frac{(2+k'_{i'} ln\, 2)}{d_{min}^{(b)}} w'_{i',i} - \frac{1}{d_{min}^{(b)}} w'_{i',i} \ln w'_{i',i}} \\
&= \prod_{i'=1}^{x} \sum_{\{\mathbf{w}'_{i'}: w'_{i',1}+\cdots+w'_{i',\mu}=d_{i'}\}} (\frac{N}{\mu})^{\frac{1}{d_{min}^{(b)}} d_{i'}} e^{\frac{(2+k'_{i'} \ln 2)}{d_{min}^{(b)}} d_{i'} - \sum_{i=1}^{\mu} \frac{1}{d_{min}^{(b)}} w'_{i',i} \ln w'_{i',i}} \\
&\leq \prod_{i'=1}^{x} \sum_{\{\mathbf{w}'_{i'}: w'_{i',1}+\cdots+w'_{i',\mu}=d_{i'}\}} (\frac{N}{\mu})^{\frac{1}{d_{min}^{(b)}} d_{i'}} e^{\frac{(2+k'_{i'} \ln 2)}{d_{min}^{(b)}} d_{i'} - \frac{1}{d_{min}^{(b)}} d_{i'} \ln \frac{d_{i'}}{\mu}} \\
&\leq \prod_{i'=1}^{x} \binom{d_{i'}+\mu-1}{d_{i'}} (\frac{N}{\mu})^{\frac{1}{d_{min}^{(b)}} d_{i'}} e^{\frac{(2+k'_{i'} \ln 2)}{d_{min}^{(b)}} d_{i'} - \frac{1}{d_{min}^{(b)}} d_{i'} \ln \frac{d_{i'}}{\mu}}. \qquad (3.8)
\end{aligned}$$

For the inequality in the third line of (3.8), I use the fact that $\sum_{i=1}^{p} t_i \ln t_i \leq s \cdot \ln \frac{s}{p}$ with $s = t_1 + \cdots + t_p$, which is clear by using the derivative on the multivariable function that consists of independent t_i's. The equality is satisfied when all t_i values are the same. Going back to (3.7), let $f(P) = \frac{1}{\binom{N}{\mu}^P e^{-P \ln P}}$ for convenience. Then I

have

$$
\begin{aligned}
A^{\text{PD-GLDPC}}(\mathbf{d}) \leq & \prod_{i=1}^{n_v} e^{(q_{v_i}-1-\frac{q_{v_i}}{d_{min}^{(c)}})d_i \ln \frac{d_i}{N} + \frac{q_{v_i}(2+k_{max}^{(c)} \ln 2)}{d_{min}^{(c)}} d_i} \\
& \times \prod_{i'=1}^{x} e^{d_{i'}+\mu-1} (\frac{N}{\mu})^{\frac{1}{d_{min}^{(b)}} d_{i'}} e^{\frac{(2+k'_{i'} \ln 2)}{d_{min}^{(b)}} d_{i'} - \frac{1}{d_{min}^{(b)}} d_{i'} \ln \frac{d_{i'}}{\mu}} \times f(P) \\
\leq & \prod_{i=1}^{n_v} e^{(q_{v_i}-1-\frac{q_{v_i}}{d_{min}^{(c)}})d_i \ln \frac{d_i}{N} + \frac{q_{v_i}(2+k_{max}^{(c)} \ln 2)}{d_{min}^{(c)}} d_i} \\
& \times e^{x(\mu-1)} e^{P} \prod_{i'=1}^{x} (\frac{N}{\mu})^{\frac{1}{d_{min}^{(b)}} d_{i'}} e^{\frac{(2+k^{(b)} \ln 2)}{d_{min}^{(b)}} d_{i'} - \frac{1}{d_{min}^{(b)}} d_{i'} \ln \frac{d_{i'}}{\mu}} \times f(P).
\end{aligned}
\tag{3.9}
$$

I classify the variable nodes in the protograph into three groups before doping:

- Protograph variable nodes of degrees higher than two
- Protograph variable nodes of degree-2 to be partially doped
- Protograph other variable nodes of degree-2.

I also separate the weights of codewords after lifting into three parts according to the three groups of variable nodes: u_i, p_z, and l_j, where u_i is the weight of the sub-codeword corresponding to a protograph variable node v_i of degree higher than two and p_z and l_j are the weights of codewords of each partially doped and undoped protograph variable node v_z and v_j of degree 2 from the protograph, respectively. The sum of sub-codeword weights for each group of variable nodes is given as $U = \sum_i u_i$, $P = \sum_z p_z$, and $L = \sum_j l_j$. It is clear that for the total codeword weight d, $d = U + P + L$. Then, the upper bound of the first term in (3.9) is written as

$$
\begin{aligned}
\prod_{i=1}^{n_v} e^{(q_{v_i}-1-\frac{q_{v_i}}{d_{min}^{(c)}})d_i \ln \frac{d_i}{N} + \frac{q_{v_i}(2+k_{max}^{(c)} \ln 2)}{d_{min}^{(c)}} d_i} \leq & e^{(2-\frac{3}{d_{min}^{(c)}})(d-P-L) \ln \frac{d-P-L}{N} + \frac{3(2+k_{max}^{(c)})}{d_{min}^{(c)}} \cdot (d-P-L)} \\
& \times e^{\frac{2(2+k_{max}^{(c)})}{d_{min}^{(c)}} \cdot L} \cdot e^{\frac{2(2+k_{max}^{(c)})}{d_{min}^{(c)}} \cdot P},
\end{aligned}
\tag{3.10}
$$

which is derived by using three weight groups of codewords similar to (20) of [49]. The same inequality $u_i < Ne^{-\frac{(2+k^{(c)}_{max}\ln 2)}{d^{(c)}_{min}-1}}$ is shared over the given codeword weight d as in [49]. Using the derivation in [49], the upper bound of the second term of (3.9) can be derived as

$$\prod_{i'=1}^{x}(\frac{N}{\mu})^{\frac{1}{d^{(b)}_{min}}d_{i'}}e^{\frac{(2+k^{(b)}\ln 2)}{d^{(b)}_{min}}d_{i'}-\frac{1}{d^{(b)}_{min}}d_{i'}\ln\frac{d_{i'}}{\mu}} = \prod_{i'=1}^{x}e^{\frac{1}{d^{(b)}_{min}}d_{i'}\ln\frac{N}{\mu}}e^{\frac{(2+k^{(b)}\ln 2)}{d^{(b)}_{min}}d_{i'}-\frac{1}{d^{(b)}_{min}}d_{i'}\ln\frac{d_{i'}}{\mu}}$$
$$= \prod_{i'=1}^{x}e^{\frac{1}{d^{(b)}_{min}}d_{i'}\ln\frac{N}{d_{i'}}}e^{\frac{(2+k^{(b)}\ln 2)}{d^{(b)}_{min}}d_{i'}} = \prod_{z=1}^{x}e^{\frac{1}{d^{(b)}_{min}}p_z\ln\frac{N}{p_z}}e^{\frac{(2+k^{(b)}\ln 2)}{d^{(b)}_{min}}p_z}$$
$$\leq e^{\frac{1}{d^{(b)}_{min}}P\cdot\ln\frac{Nx}{P}}e^{\frac{(2+k^{(b)}\ln 2)}{d^{(b)}_{min}}P}. \tag{3.11}$$

Using (3.10) and (3.11), the upper bound of $A^{PD\text{-}GLDPC}(\mathbf{d})$ is derived in terms of $E(d,P,L)$ as follows:

$$A^{PD\text{-}GLDPC}(\mathbf{d}) \leq e^{\frac{1}{d^{(b)}_{min}}P\cdot\ln\frac{Nx}{P}}e^{\frac{(2+k^{(b)}\ln 2)}{d^{(b)}_{min}}P}\cdot e^{(2-\frac{3}{d^{(c)}_{min}})(d-P-L)\ln\frac{d-P-L}{N}+\frac{3(2+k^{(c)}_{max})}{d^{(c)}_{min}}\cdot(d-P-L)}$$
$$\times e^{\frac{2(2+k^{(c)}_{max})}{d^{(c)}_{min}}\cdot(P+L)}\cdot e^{x(\mu-1)}e^{P}\cdot f(P). \tag{3.12}$$

Let $E(d,P,L)$ be the parameter satisfying $A^{PD\text{-}GLDPC}(\mathbf{d}) \leq e^{x(\mu-1)}\cdot e^{E(d,P,L)}$. Then, from the upper bound in (3.12), $E(d,P,L)$ is given as

$$E(d,P,L) = \frac{1}{d^{(b)}_{min}}P\cdot\ln\frac{Nx}{P}+\frac{(2+k^{(b)}\ln 2)}{d^{(b)}_{min}}P+(2-\frac{3}{d^{(c)}_{min}})(d-P-L)\ln\frac{d-P-L}{N}$$
$$+\frac{3(2+k^{(c)}_{max})}{d^{(c)}_{min}}\cdot(d-P-L)+\frac{2(2+k^{(c)}_{max})}{d^{(c)}_{min}}\cdot(P+L)+P+P\ln P-P\ln\frac{N}{\mu}.$$

Assuming that there are no type 1 degree-2 variable nodes defined in [49] and there are no cycles consisting only of undoped variable nodes of degree-2, I use the result of (22) in [49] such that the inequality $l^{(c_j)}_{2,k} \leq \frac{1}{d^{(c_j)}_{min}}(L^{(c_j)}_2+\sum_i w^{(c_j)}_i)$ is satisfied for all $j\in[n_c]$, where $l^{(c_j)}_{2,k}$ is the weight of the degree-2 undoped variable node of G_p and the total weight of them is denoted as $L^{(c_j)}_2$ for check node c_j. Similar to the result in [49], I can derive the upper bound $L \leq \gamma(U+P)$, which is the same as $L \leq \frac{\gamma}{1+\gamma}d$.

Now, the upper bound of $E(d,P,L)$ needs to be derived for independent values L and P. The first and second partial derivatives of $E(d,P,L)$ by P are given as

$$\begin{aligned}\frac{dE}{dP} =& \frac{1}{d_{min}^{(b)}} \cdot \ln \frac{Nx}{eP} + \frac{(2+k^{(b)}\ln 2)}{d_{min}^{(b)}} - (2-\frac{3}{d_{min}^{(c)}})\ln \frac{e(d-P-L)}{N} - \frac{(2+k_{max}^{(c)}\ln 2)}{d_{min}^{(c)}} \\ & + 1 + \ln P + 1 - \ln \frac{N}{\mu} < 0, \\ \frac{d^2E}{dP^2} =& -\frac{1}{d_{min}^{(b)}P} + (2-\frac{3}{d_{min}^{(c)}}) \cdot \frac{1}{d-P-L} + \frac{1}{P} > 0.\end{aligned}$$

Since the first derivative over P is negative and the second derivative is positive, $E(d,P,L)$ is upper bounded by

$$\lim_{P\to 0+} E(d,P,L) = (2-\frac{3}{d_{min}^{(c)}})(d-L)\ln \frac{d-L}{N} + \frac{3(2+k_{max}^{(c)})}{d_{min}^{(c)}} \cdot (d-L) + \frac{2(2+k_{max}^{(c)}\ln 2)}{d_{min}^{(c)}} L.$$

Since the resulting upper bound of $E(d,L)$ is the same as (37) in [49], the rest of the proof is the same as that in [49] and thus the proposed constraint guarantees the existence of typical minimum distance of the proposed protograph-based PD-GLDPC code.

Chapter 4

Design of Protograph-Based LDPC Code Using Resolvable Block Design for Block Fading Channel

Block fading (BF) channel has been considered as an effective and simple channel model that captures the fundamental characteristics of current communication systems such as orthogonal frequency divison multiplexing (OFDM), 5G new radio (5G NR) standards, and frequency hopping spread spectrum. Obtaining diversity order of such communication systems in the BF channel draw an attention for the researchers since it offers many advantages in terms of the robustness of data from errors in the deep fading channel. Here, the corresponding measure can be analyzed through the diversity order, which is the asymptotic slope of the error rate. Therefore, numerous high diversity-obtaining schemes such as space-time codes, maximum ratio combining (MRC), and channel coding approach have been developed.

Protograph-based LDPC codes are known to achieve the capacity approaching performance from low design complexity [40]. LDPC codes are designed according to the characteristics of the channel and the decoding algorithm of the code. In the case of BF channel, Root LDPC code has been thought to be a promising code to achieve full diversity order [56, 57]. Also, in order to enhance the performance of the BP decoding of the LDPC code, there were studies on the construction of high girth LDPC codes

from block design theory [58]. For this, in [59], a new progressive edge growth method was proposed to construct a structured root LDPC code.

Also in [60], high rate protograph-based LDPC code achieving diversity order two was proposed. Both root LDPC and generalized root protograph-based LDPC codes are designed to achieve the theoretical upper bound of diversity order using maximum and minimum parity block, respectively. So far, the existing works of LDPC codes for block fading channel has limited construction parameters in terms of code rate.

In this chapter, a new method for the construction of regular protograph-based LDPC codes for the BF channel with new parameters is given. I show that the constructed code has error performance that approaches the slope of the theoretical outage bound in the finite signal-to-noise ratio (SNR) regime for the new BF channel parameters. For this, I derive a novel theoretical analysis called gamma evolution, which tracks the instantaneous SNR values of the variable nodes in the LDPC code. Using gamma evolution, I can derive the upper bound of bit error rate (BER) of the proposed codes in the BF channel. Numerical simulation shows that the the decoding performance of the proposed LDPC codes approaches the theoretical bound.

The rest of the chapter is organized as follows. In Section 4.1, the system model is introduced. Section 4.2 introduces some existing class of resolvable block design (RBD) and the construction method of protograph-based LDPC codes using RBD. Furthermore, in Section 4.2, gamma evolution of the constructed codes are proposed to explain the upper bound of BER. Finally the numerical results and their analyses are included.

4.1 Problem Formulation

4.1.1 BF Channel Model

A BF channel with L blocks is considered in this dissertation. First, a binary information vector of K bits are encoded into N bits using (N,K) binary linear code with

code rate $r = K/N$, which is denoted as a codeword $\mathbf{c} = (c_1, c_2, \ldots, c_N), c_i \in \{0, 1\}$. The encoded bits undergo binary phase shift keying (BPSK) modulation and become $\mathbf{x} = (x_1, x_2, \ldots, x_N), x_i \in \{\pm 1\}$. The modulated codeword passes through fading blocks with block length $B = N/L$. Each block experience a fading gain $\alpha_i, i \in [L]$, where the expectation value of fading gain squared is one. Here, α_i is assumed to follow an independent and identically distributed (i.i.d.) Rayleigh probability density function (PDF). Let N_0 be the noise power spectral density and $\lceil x \rceil$ be the smallest integer greater than or equal to $x \in \mathbb{R}$. Then, the received signal $\mathbf{r} = (r_1, r_2, \ldots, r_N)$ is given as

$$r_j = \alpha_{\lceil j/B \rceil} \cdot x_j + n_j, j \in [N] \tag{4.1}$$

where n_i is the additive Gaussian noise with variance $\sigma^2 = N_0/2$. The instantaneous SNR of each signal in the block $i \in [L]$, denoted as γ_i, is defined as $\gamma_i = R(E_b/N_0)\alpha_i^2$ for BPSK modulation, where $r = K/N$ is the code rate and E_b is the average energy of an information bit. The average SNR $\overline{\gamma}$ is defined as $\overline{\gamma} = \mathbb{E}_{\gamma_i}[\gamma_i]$.

4.1.2 Performance Metrics of BF Channel

While, the BF channel can be analyzed by each γ_i, it can also be analyzed by the random variables derived from ordered statistics. In [61], the *spacing* concept can be applied in the realization of instantaneous SNRs using ordered statistics. Here, the instantaneous SNRs $\gamma_1, \gamma_2, \ldots, \gamma_N$ are reordered to $\gamma_{1:L}, \gamma_{2:L}, \ldots, \gamma_{L:L}$ such that $\gamma_{1:L} \geq \gamma_{2:L} \geq \ldots \geq \gamma_{L:L} \geq 0$. The *spacing* is defined in [62] as a random variable $\Delta_L = \gamma_{L:L}$ and $\Delta_i = \gamma_{i+1} - \gamma_i, i \in [L-1]$. Then, the PDF of each spacing is given as

$$p_{\Delta_i}(x) = \frac{i}{\overline{\gamma}} \cdot e^{-(ix/\overline{\gamma})} \tag{4.2}$$

for Rayleigh fading [61]. It is derived in [60] that the linear sum of Δ_i, i.e., $\gamma_\Delta = \sum_{i \in [L]} a_i \Delta_i$, has moment generating function as

$$M_{\gamma_\Delta}(s) = \prod_{i \in [L]} (1 - \frac{a_i \overline{\gamma} s}{i})^{-1}.$$

For BPSK modulation, its BER for r_Δ, denoted as $P_{\gamma_\Delta}(E)$, is computed as in [61]

$$P_{\gamma_\Delta}(E) = \frac{1}{\pi}\int_0^\infty M_{\gamma_\Delta}(-\frac{1}{2\sin^2\phi})d\phi.$$

Let $I_{AWGN}(\overline{\gamma}\alpha_i^2)$ be the input-output mutual information of AWGN channel for fading block with fading coefficient α_i. For BPSK modulation, it is given as

$$I_{AWGN}(\overline{\gamma}\alpha_i^2) = 1 - E_{X,Z}[\log_2(\sum_{x\in\{0,1\}} e^{-|\sqrt{\gamma_i}(X-x)+Z|^2+|Z|^2})]$$

where X is a random variable distributed uniformly over $\{0,1\}$ and Z is a normal distribution with zero mean with variance σ^2 [63]. In this dissertation, the main goal is to construct an LDPC code having the error performance approaching the theoretical bound for a given code rate r and the number of blocks L. For the theoretical lower bound of the FER of the channel, the channel outage probability is use, which is defined as

$$P_{out} = \text{Prob}\{I(\overline{\gamma}, \boldsymbol{\alpha}) < r\} \tag{4.3}$$

where $I(\overline{\gamma}, \boldsymbol{\alpha}) = (1/L)\sum_{i=i}^{L} I_{AWGN}(\overline{\gamma}\alpha_i^2)$ is the average mutual information between transmitted symbol and BF channel. Let $G_i = \sum_{j=1}^{L-i} A_j$ be the summation of random variables $A_j = \log_2\{1+\gamma_j\overline{\gamma}\}$ with the condition that $\gamma_j \leq 1/\overline{\gamma}$ and let p be defined as $\text{Prob}\{\gamma_j > 1/\overline{\gamma}\}$. I define $F_{G_i}(\cdot)$ as the cumulative density function (cdf) of G_i. In order to reduce the computational complexity of (4.3), I use the outage lower bound in [63]. The lower bound of the channel outage probability $P_{out}^{low}(\overline{\gamma}, r)$ is given as

$$P_{out}^{low}(\overline{\gamma}, r) = \sum_{i=0}^{L} F_{G_i}(Lr-t)\binom{L}{i}p^i(1-p)^{L-i}. \tag{4.4}$$

In Fig. 4.1, for a given L, I briefly illustrate the target code rate and outage probability that the proposed LDPC code tries to approach compared to the target code rate of the conventional LDPC codes.

In order to evaluate the asymptotic performance of the constructed code for a given

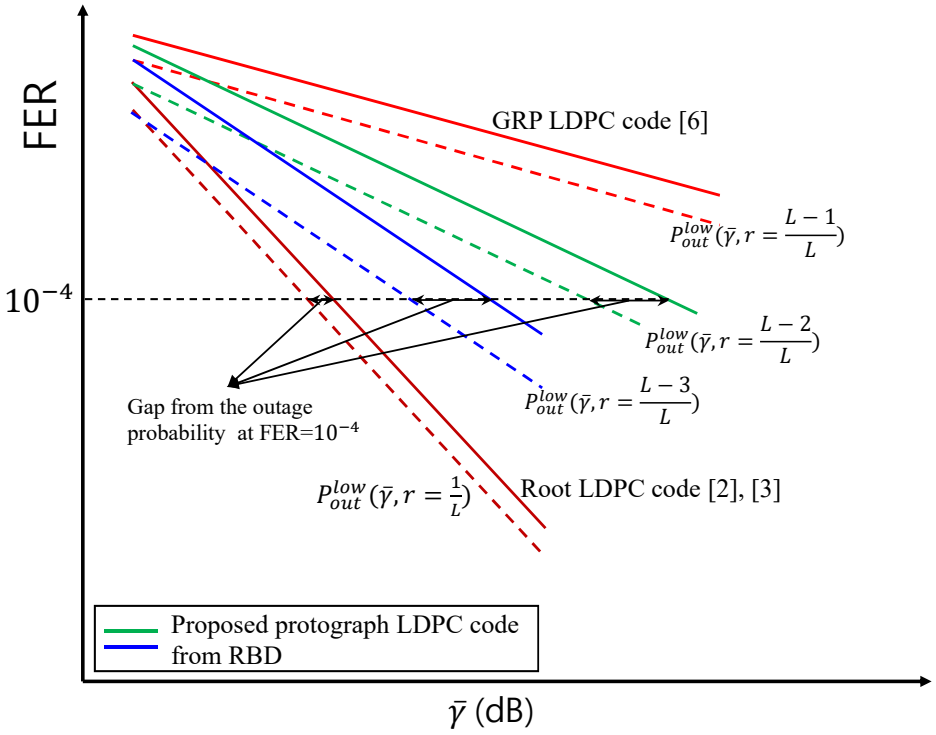


Figure 4.1: The illustration of the comparison between FER performance and outage probabaility of conventional root LDPC, GRP LDPC, and the proposed protograph-based LDPC codes.

decoder, the diversity order metric is used. The diversity order for a given (N, K) linear code with code rate $r = K/N$ is defined as

$$d_c = -\lim_{\overline{\gamma}\to\infty} \log \frac{P_F(\overline{\gamma}, r)}{\log \overline{\gamma}}$$

where $P_F(\overline{\gamma}, r)$ is the FER of the given code. For a given value of L and r, the upper bound of diversity order, which is also called as the Singleton-like bound, is given in [64].

$$d_c \leq 1 + \lfloor L(1-r) \rfloor. \tag{4.5}$$

For a given code rate r and belief propagation (BP) decoder, there were construc-

tions of LDPC codes with $r = 1/L$ and $r = (L-1)/L$ in a block fading channel with L fading blocks, where the the achieved diversity order is L and 2, respectively. For the code rates in between $r = 1/L$ and $r = (L-1)/L$, the construction of the channel outage probability approaching LDPC codes is unknown.

4.1.3 Protograph-Based LDPC Codes and QC LDPC Codes

A protograph-based LDPC code is built from a Tanner graph defined by an $M \times N$ base matrix $\mathbf{B} = [b_{ij}], i \in [M], j \in [N]$ [40], where rows represent the check nodes and the columns represent the variable nodes. The entry b_{ij} of each matrix decides the number of edges connecting ith check node and jth variable node. If each row has K number of ones and each column has J number of ones, it is called (J, K)-regular protograph-based LDPC code. The protograph-based LDPC code is constructed by the copy-and-permute operation from the protograph [40]. For a lifting factor Z, the entry $b_{ij} = 0$ becomes a zero matrix and $b_{ij} = 1$ becomes a permutation matrix with size $Z \times Z$ in the PCM of the protograph-based LDPC code. If the permutation matrix is a cyclic shifted version of an identity matrix, the code becomes a QC LDPC code.

4.2 New Construction of Protograph-Based LDPC Codes from Resolvable Block Designs

In this section, some basic concepts of RBD schemes and construction of the protograph from RBD to construct the proposed protograph-based LDPC code are introduced.

4.2.1 Resolvable Block Designs

I first introduce some definitions on the existing block designs that are used to construct the proposed protograph-based LDPC code in this dissertation. First, the definition of

BIBD is given as follows.

Definition 4.1 (Balanced incomplete block design [65]). *A balanced incomplete block design (BIBD) is a pair (V, B) where V is a v-set and B is a collection of b k-subsets of V (blocks) such that each element of V is contained in exactly r blocks and any 2-subset of V is contained in exactly λ blocks. The numbers $v, b, r, k,$ and λ are parameters of the BIBD.*

In this dissertation, I only focus on the resolvable block designs. The resolvable BIBD (RBIBD) is defined as follows.

Definition 4.2 (Resolvable BIBD (RBIBD) [65]). *A BIBD is resolvable if there exists a partition R of its set of blocks B into parallel classes, each of which in turn partitions the set V; R is a resolution.*

For $k = 2$, an RBIBD can be constructed from 1-factorization of $K_{2n}, n \in \mathbb{N}$, where K_{2n} is a complete graph with $2n$ vertices [65]. It is known in [65] that the columns of a using balanced tournament design of size n, i.e., BTD(n), construct a 1-factorization of a complete graph with $2n$ vertices, i.e., K_{2n}, making an RBIBD with $\lambda = 1, k = 2$. BTD(n) is defined as follows.

Definition 4.3 (Balanced tournament design [65]). *A balanced tournament design of order n, BTD(n), defined on a $2n$-set V is an arrangement of the $\binom{2n}{2}$ distinct unordered pairs of the elements of V into an $n \times (2n-1)$ array such that*

i) Every element of V is contained in precisely one cell of each column, and

ii) Every element of V is contained in at most two cells of any row.

For $k = 3$, Steiner triple system with order v, denoted as STS(v), refers to a BIBD with $k = 3, \lambda = 1$. An RBIBD with $k = 3$ is constructed using resolvable Steiner triple system, also known as *Kirkman triple system*, defined in the following definition. It is known that *Kirkman triple system* KTS(v) exists when $v \equiv 3 (mod\, 6)$ in STS(v). Another resolvable design with $k = 3$ is constructed from λ-configuration, which is defined as follows.

Table 4.1: Parameters for configuration and KTS(v)

	K	RC	K	RC	K
v	9	14	15	18	21
b	12	28	35	48	70
(k, r)	(3,4)	(3,6)	(3,7)	(3,9)	(3,10)

K: Kirkman triple system

RC: Resolvable configuration

Definition 4.4 (λ-configuration [65])**.** *A λ-configuration (v_r, b_k) is an incidence structure of v points and b blocks such that each block contains k points, each point belongs to r blocks, and any two different points are contained in at most λ blocks.*

When $\lambda = 1$, I denote the λ-configuration design as configuration (v_r, b_k). Using the result in [58], a configuration can be constructed by deleting a row and $r = (v - 1)/(k - 1) = (v - 1)/2$ columns incident to the deleted row in the STS(v). Likewise, a resolvable configuration can be made by deleting exactly one column from each resolution of KTS(v). Thus, some examples of resolvable block design (RBD) for $k = 2, 3$ are introduced. The RBDs for $k = 3$ are summarized as Table 4.1. In the table, the parameters v, b, k, and r are summarized for KTS(v) and resolvable configuration.

4.2.2 Construction of the Proposed Protograph-Based LDPC Codes

In this dissertation, I set the incidence matrix of RBD as the base matrix of the protograph-based LDPC code and define the base matrix as RBD base matrix. Also, I define the protograph of the RBD base matrix as the RBD protograph. In [58], the incidence matrix of incomplete block design with $\lambda = 1$ makes the base matrix of girth 6 makes it possible to construct a QC LDPC code with girth $g \geq 18$. This implies that it is possible to construct high girth LDPC code from the RBD protograph.

For a base matrix constructed from RBD, I assume that each resolution undergoes different fading coefficient α_i. I construct RBD base matrix for $k = 2, 3$ in this

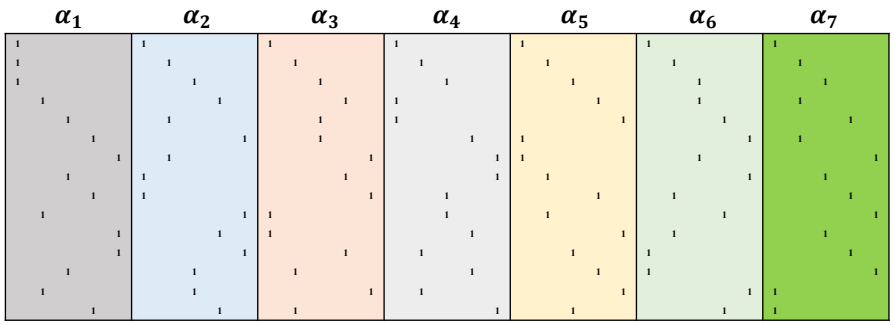


Figure 4.2: A 15×35 base matrix constructed from the incidence matrix of KTS(15).

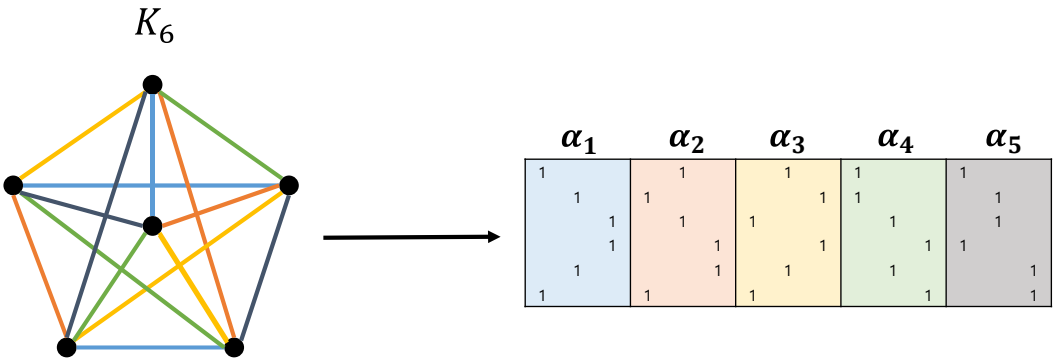


Figure 4.3: Example of the construction of the base matrix from 1-factorization of K_6 using BTD(3).

dissertation.

Let B_k be the base matrix of RBD base matrix from RBD with parameter k introduced in Section III.A for $k = 2, 3$. For B_2, a base matrix with code rate $r = \frac{L-2}{L}$ is constructed. Likewise, an RBD base matrix is constructed with code rate $r = \frac{L-3}{L}$ for B_3. I define each resolution in B_k as $R_i, i \in [r]$ and assume that each resolution undergoes different α_i. Thus, I assume the situation where the number of resolutions in the RBD is equal to the block number, i.e., $r = L$.

Definition 4.5 ($x^{(R)}$-shortened RBD)**.** *An $x^{(R)}$-shortened RBD$(v, b - xR, k, r - x)$ is an RBD such that x resolutions of size R are removed from the original RBD(v, b, r, k).*

Proposition 4.1. *An $x^{(R)}$-shortened RBD achieves diversity order 2 over block fading channel with $L - x$ blocks.*

Using the Proposition 4.1, I can construct an RBD-based base matrix of diversity order 2 over various L parameters of block fading channel by removing certain number of resolutions from RBD. For the construction of $x^{(R)}$-shortened RBD with $k = 2$, $(2, L)$-regular protograph with code rate $(L-2)/L$ is shortened into $(2, L-x)$-regular code ($x \in [L-2]$), with code rate $(L-2-x)/(L-x)$, which undergoes channel with $L-x$ fading blocks. Likewise, for $k = 3$, $(L-3)/L$ is shortened into $(3, L-x)$-regular protograph with code rate $(L-3-x)/(L-x)$ undergoing channel with $L-x$ fading blocks.

4.2.3 Theoretical Analysis of the Proposed Protograph-Based LDPC Code from RBD

In this subsection, since BER curve has similar slope as that of the FER curve, I explain how the proposed protograph-based LDPC codes has FER slope approaching the channel outage probability in the finite SNR regime in terms of BER. I first show how the instantaneous SNRs of a posteriori messages of variable nodes evolve during the message passing decoding of the proposed protograph-based LDPC code. As mentioned earlier in Section II, I order the instantaneous SNRs as $\gamma_{1:L}, \gamma_{2:L}, \ldots, \gamma_{L:L}$. I focus on the behavior of the APP message evolution during min-sum decoding process in terms of instantaneous SNRs since the diversity order of the code with of min-sum decoding is worse than that of the sum product decoding for the proposed protograph-based LDPC codes.

Remark 1. *Using [60], it is clear that the diversity order of $\gamma_\Delta = a\Delta_i + b\Delta_j$ is 2, where a, b, i, and j are positive integer and $i \neq j$.*

I define the density evolution in terms of instantaneous SNRs as gamma evolution.

First, gamma evolution is made for protograph-based LDPC code constructed from RBD with $k = 3$, which has code rate $(L-3)/L$. I assume that the constructed RBD has L resolutions undergoing block fading channel with L blocks. Since I focus on the gamma evolution of the two blocks with worst realization of fading coefficients, it is sufficient to evaluate the error performance of the code assuming that that code constructed from RBD with $k = 3$ undergoes a block fading channel with the ordered SNR vector $(\gamma_{L:L}, \gamma_{L-1:L}, \ldots, \gamma_{1:L})$. In order to evaluate the degree that the error performance of the code is approaching Singleton-like bound, it is sufficient to show the upper bound of BER of the block with the worst realized fading coefficient, i.e., the first fading block undergoing $\gamma_{L:L}$, reach the BER with fading vector $\gamma_{L-3:L}$.

In an average sense, the a posteriori message of variable node of the first resolution is lower bounded by $\gamma_{L:L} + 3\gamma_{L-1:L}$ at the first iteration of min-sum decoding, assuming that the message from the second resolution has the minimum LLR value of extrinsic message. Likewise, the second resolution has lower bounded a posteriori messages of $\gamma_{L:L} + 3\gamma_{L-1:L}$. Using the Remark, the achieved diversity order of the proposed protograph-based LDPC code is 2. However, I try to show that the proposed protograph-based LDPC code constructed from RBD has error performance approaching the diversity of 3 or higher for further iterations. Let $a^{(l)}$ and $b^{(l)}$ be the coefficient for the $\gamma_{L:L}$ and $\gamma_{L-1:L}$ at iteration l, respectively. The coefficients $a^{(l)}$ and $b^{(l)}$ of the a posteriori messages of the first resolution resulting from min-sum decoding is shown in Table 4.2. Assuming that the LDPC code constructed from RBD has girth g, due to the resolvable characteristic of RBD, gamma evolution will occur with independent path until $(g/2-1)$th iterations. In other words, the lower bound of a posteriori messages up to $g/2-1$ iterations are tractable.

For iteration $i \leq \lfloor g/2 \rfloor - 1$, I track down the coefficients $a^{(l)}$ and $b^{(l)}$ of a posteriori messages of the variable nodes of the protograph-based LDPC code in the first resolution: $a^{(l)}\gamma_{L:L} + b^{(l)}\gamma_{L-1:L}$. Comparison is made between the channel message $\gamma_{L-3:L}$ and the protograph-based LDPC code constructed from RBD. From [60], it is clear

Table 4.2: Coefficients of gamma evolution of BIBD with $k = 3$ and $k = 2$

	Iteration 1	Iteration 2	Iteration $l = 2t, t = 1, 2, \ldots$	Iteration $l = 2t + 1, t = 0, 1, \ldots, \ldots$
BIBD with $k = 3$ $(a^{(l)}, b^{(l)})$	(1,3)	(7,3)	$(2^{l+1} - 1, 2^l - 1)$	$(2^l - 1, 2^{l+1} - 1)$
BIBD with $k = 2$ $(c^{(l)}, d^{(l)})$	(1,2)	(3,2)	$(l + 1, l)$	$(l, l + 1)$

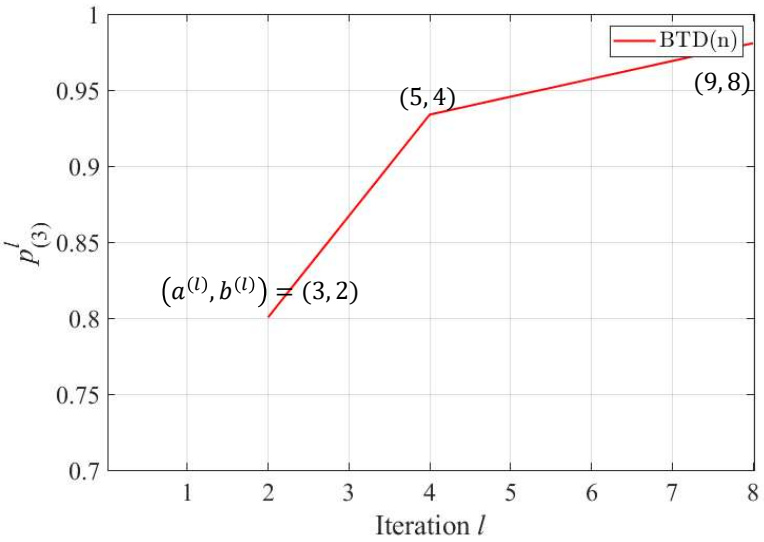


Figure 4.4: Gamma evolution of BTD(n) at $\overline{\gamma} = 16$ dB.

that $\gamma_{L-3:L}$ has diversity order 4 and $\gamma_{L-2:L}$ has diversity order 3. For a given channel SNR, I track down the probability that the linear sum of gamma values exceeds the value $\gamma_{L-3:L}$. Conversion to spacing of gamma values, I can track the probability that the given variable node exceeds $\gamma_{L-3:L}$ or $\gamma_{L-2:L}$ for the following two probabilistic events

$$\begin{aligned} A_1: \; p_1 =& P\{a^{(l)}\gamma_{L:L} + b^{(l)}\gamma_{L-1:L} \geq \gamma_{L-3:L}\} \\ =& P\{(a^{(l)} + b^{(l)} - 1)\Delta_{L:L} + (b^{(l)} - 1)\Delta_{L-1:L} \\ & - \Delta_{L-2:L} - \Delta_{L-3:L} \geq 0\}, \end{aligned} \tag{4.6}$$

$$A_2: \; p_2 = P\{a^{(l)}\gamma_{L:L} + b^{(l)}\gamma_{L-1:L} \geq \gamma_{L-2:L} | \overline{A_1}\}. \tag{4.7}$$

The probability p_1 in (4.6) can be computed as follows. Let Z be the random

variable of the linear sum of $\Delta_{L:L}$ and $\Delta_{L-1:L}$, i.e., $Z = a\Delta_{L:L} + b\Delta_{L-1:L}$. Then, it is clear that $p_1 = 1 - \int_{x\in\{\Delta_{L-2}\}} f_{\Delta_{L-2}}(x)(1 - F_Z(x))dx$, where

$$f_z(z) = \frac{1}{|a-1|}\int f_{\Delta_L}(\frac{z-(b-1)\Delta L - 1}{a-1}) f_{\Delta_{L-1}}(\Delta_{L-1})d\Delta_{L-1}$$

and $F_Z(z) = \int F_{\Delta_L}(\frac{z-(b-1)\Delta_{L-1}}{a-1}) f_{\Delta_{L-1}}(\Delta_{L-1})d\Delta_{L-1}$. Likewise, the probability p_2 in (4.7) can be computed as

$$p_2 = \int_{x=0}^{\infty}\int_{y=x}^{\infty} p_{\Delta_{L-2}}(x) p_{\Delta_{L-3}+\Delta_{L-2}}(y)(F(y) - F(x))dydx.$$

Using (4.6) and (4.7), the upper bound of BER of the proposed protograph-based LDPC code constructed from RBD with $k = 3$ at iteration l, i.e., $P_b^{(l)}(\mathrm{RBD}_{k=3})$ is computed as

$$\begin{aligned} P_b^{(l)}(\mathrm{RBD}_{k=3}) \leq & p_1 P_{\gamma_{L-3:L}}(E) + p_2 P_{\gamma_{L-2:L}}(E) \\ & + (1 - p_1 - p_2) P_{\gamma_{L-1:L}}(E), \end{aligned} \tag{4.8}$$

because the BER is upper bounded by $\gamma_{L-1:L}$ for any resolution in the RBD. Since the equation of gamma evolution for RBD with $k = 3$ is the same, the upper bound of BER is identical for any protograph-based LDPC code constructed from Table 4.1. For the upper bound of BER for K_{2n}, i.e., $P_b^{(l)}(\mathrm{BTD}(n))$, let $c^{(l)}$ and $d^{(l)}$ be the coefficients for the $\gamma_{L:L}$ and $\gamma_{L-1:L}$ at iteration l, respectively. Then, the upper bound of BER is computed as

$$P_b^{(l)}(\mathrm{BTD}(n)) \leq p_3^{(l)} P_{\gamma_{L-2:L}}(E) + (1 - p_3^{(l)}) P_{\gamma_{L-1:L}}(E), \tag{4.9}$$

where $p_3^{(l)} = P\{c^{(l)}\gamma_{L:L} + d^{(l)}\gamma_{L-1:L} \geq \gamma_{L-2:L}\}$, which is the probability that the a posteriori message of the first resolution exceeds that of $\gamma_{2:4}$. Thus, using the upper bound of BER, I can evaluate the BER slope through the probabilistic sum of random variables of instantaneous SNRs for a given iteration of min-sum decoding. I plot the probability of $P_b^{(l)}$ for each iteration at $\overline{\gamma} = 16$ dB, which is given in Fig. 4.4.

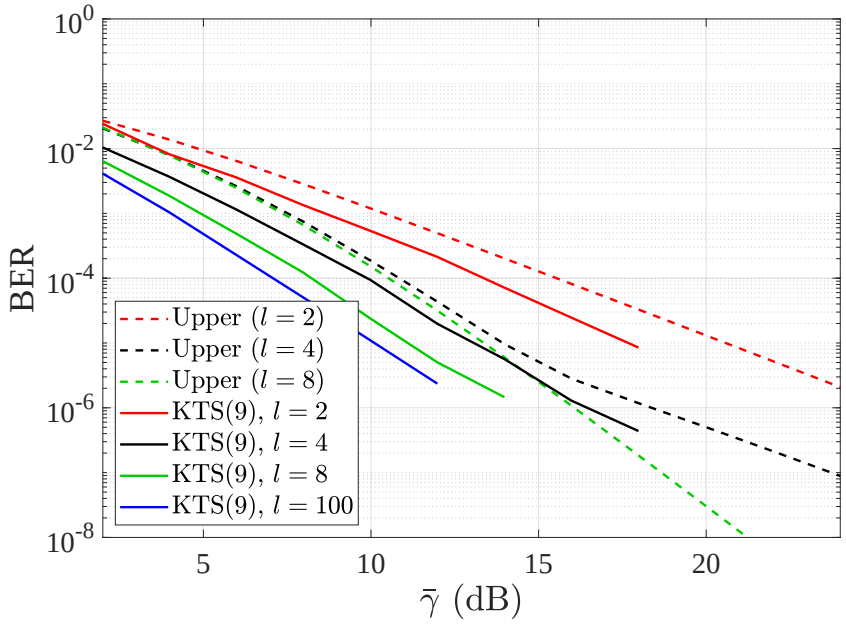


Figure 4.5: BER comparison between protograph-based LDPC constructed from KTS(9) and the upper bound of BER.

4.2.4 Numerical Analysis of the Proposed Protograph-Based LDPC Code Codes for BF Channel

In this section, I numerically show the upper bound of BER of RBD with $k = 3$ and $k = 2$. Also, the frame error rate (FER) performance of the proposed QC-LDPC codes constructed from RBDs are compared to that of the channel outage probability.

4.2.5 BER Comparison with Analytical Results from Gamma Evolution

Using the result in Table 4.2, (4.8), and (4.9), I plot the upper bound of BER for a BIBD for a given channel SNR. For $k = 3$, I construct a QC-LDPC code from KTS(9) with the lifting size $Z = 200$ and girth $g = 14$. The constructed QC-LDPC code is a $(2400, 600)$ linear code. For each given SNR and given decoding iteration,

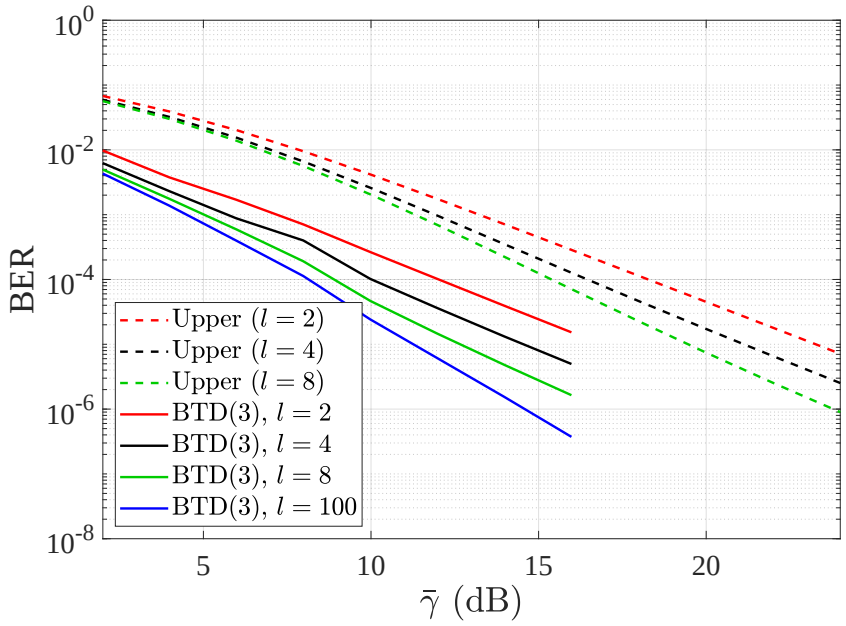


Figure 4.6: BER comparison between QC-LDPC constructed from BTD(3) and the upper bound of BER.

I numerically compute the upper bound of BER. The simulation results are shown in Fig. 4.5, where the channel has $L = 4$ fading blocks. Likewise, for BIBD with $k = 2$, I construct QC-LDPC code from $2^{(R)}$-shortened BTD(3), which makes protograph with size 6×12. The protograph is lifted by 200 with girth $g = 14$, which makes a $(2400, 1200)$ half rate linear code. The simluation results are shown in Fig. 4.6, where the channel has $L = 4$ fading blocks. Both results of KTS(9) and BTD(3) show that the slope of upper bound of BER corresponds well to the actual BER performance of the proposed protograph-based LDPC code. Also, as the decoding iteration proceeds, the slope becomes steeper due to gradually increasing a posteriori messages from the resolvable structure of RBIBD.

4.2.6 FER Comparison with Channel Outage Probability

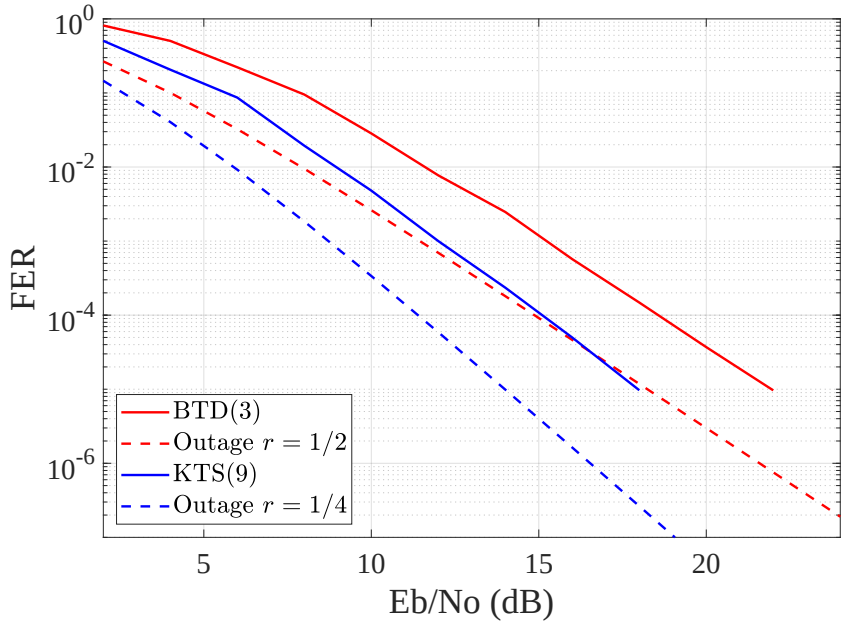


Figure 4.7: FER result of KTS(9) and BTD(3) compared to the channel outage probability.

In this subsection, I plot the FER performance of the proposed protograph-based LDPC constructed from RBIBD with $k = 3$ and $k = 2$. For each $k = 3$ and $k = 2$, I use the same code that is constructed from the previous subsection. The performance of the code is compared to that of the channel outage probability for $L = 4$ and code rate $r = 1/4$ for KTS(9) and $r = 1/2$ for BTD(3), respectively. The result is given in Fig. 4.7. The constructed protograph-based LDPC code has FER performance having slope as steep as the outage probability in the high SNR regime. Although in asymptotic sense, the LDPC code constructed from RBD has diversity order 2, in finite high SNR regime, the performance of the constructed codes approaches the Singleton-like bound.

Chapter 5

Conclusions

In this dissertation, research on the new design methods of protograph-based GLDPC and LDPC codes were presented.

In Chapter 2, a brief introduction of LDPC codes and protograph-based LDPC codes were briefly overviewed. Preliminaries for the channel, decoding of LDPC codes, and asymptotic analysis of LDPC codes were presented.

In Chapter 3, I proposed a new construction method of a PD-GLDPC code that has advantages of a finer granularity of the protograph node doping compared to the protograph doped GLDPC codes in the BEC. Also, I proposed two optimization algorithms for the PD-GLDPC codes: protographs constructed from random LDPC code ensembles and protograph-based LDPC code ensembles constructed from genetic algorithms. Furthermore, I proposed the partially doping and puncturing technique, which is similar to the well known precoding technique. Using the proposed technique, the constructed PD-GLDPC codes have good FER performances compared to the popular protograph-based LDPC codes. Since it is possible to partially dope the protograph VNs with a granularity 1, the rate loss is reduced from partial doping, and thus, GLDPC codes can have capacity approaching performance in the medium to high code rate regime. For future work, use of other component codes can be considered. Furthermore, since our doping technique is suitable for protecting certain VNs,

protection of VNs of degree-1 has to be studied.

In Chapter 4, I proposed the design of protograph-based LDPC codes in the BF channel constructed from RBDs with $k = 3$ and $k = 2$, which have good performance approaching the Singleton-like bound in the finite channel SNR. The proposed upper bound of BER analytically showed that the BER slope of the proposed codes became steeper as the iteration proceeded due to the resolvable structure of the RBD. As a future work, new constructions of protograph-based LDPC codes for different parameters in the Singleton-like bound will be considered.

Bibliography

[1] C. E. Shannon, "A mathematical theory of communications," *Bell Syst. Tech. J.*, vol. 27, pp. 379–423, Jul. 1948.

[2] S. Haykin, *Communication Systems*. 4th Ed. NY, NY, USA: John Wiley & Sons, Inc., 2001.

[3] J. G. Proakis and M. Salehi, *Digital Communications*, 5th Ed. NY, NY, USA: MacGraw-Hill, 2008..

[4] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes.* Amsterdam, The Netherlands: North-Holland, 1977.

[5] R. E. Blahut, *Algebraic Codes for Data Transmission.* NY, NY, USA: Cambridge University Press, 2003.

[6] S. Lin and D. J. Costello, Jr., *Error Control Coding*. 2nd Ed., Upper Saddle River, NJ, USA: Prentice Hall, 2004.

[7] T. J. Richardson and R. L. Urbanke, *Modern Coding Theory*. NY, NY, USA: Cambridge University Press, 2008.

[8] R. W. Hamming, "Error detecting and error correcting codes," *Bell Syst. Tech. J.,* vol. 26, no. 2, pp. 147–160, 1950.

[9] M. J. E. Golay, "Notes on digital coding," *Proc. IRE*, vol. 37, pp. 657–657, Jun. 1949.

[10] I. S. Reed, “A class of multiple-error-correcting codes and the decoding scheme,” *IRE Trans. Inf. Theory*, vol. PGIT-4, pp. 38–49, 1954.

[11] R. E. Muller, “Application of boolean algebra to switching circuit design and to error detection,” *IRE Trans. Electron. Comput.,* vol. EC-3, pp. 6–12, 1954.

[12] A. Hocquenghem, “Codes correcteurs d’erreurs,” *Chiffres*, vol. 2, pp. 147–156, 1959.

[13] R. C. Bose and D. K. Ray-Chaudhuri, “On a class of error-correcting binary group codes,” *Inf. Control*, vol. 3, pp. 68–79, Mar. 1960.

[14] I. S. Reed and G. Solomon, “Polynomial codes over certain finite fields,” *SIAM J.,* vol. 8, no. 2, pp. 300–304, Jun. 1960.

[15] P. Elias, “Coding for noisy channels,” *IRE Int. Convent. Record*, Mar. 1955, pp. 37–46.

[16] C. Berrou, A. Glavieux, and P. Thitimajshima, “Near Shannon limit error-correcting coding and decoding,” in *Proc. IEEE Int. Conf. Commun.*, Geneva, Switzerland, May 1993, pp. 1064–1070.

[17] R. G. Gallager, *Low-Density Parity-Check Codes*. Cambridge, MA, USA: MIT Press, 1963.

[18] D. J. C. MacKay and R. M. Neal, “Near Shannon limit performance of low density parity check codes,” *Electron. Lett.,* vol. 32, no. 18, pp. 1645–1646, Aug. 1996.

[19] D. J. C. MacKay, “Good error correcting codes based on very sparse matrices,” *IEEE Trans. Inf. Theory*, vol. 45, no. 2, pp. 399–431, Mar. 1999.

[20] M. Luby, M. Mitzenmacher, A. Shokrollahi, and D. A. Spielman, “Improved low-density parity-check codes using irregular graphs,” *IEEE Trans. Inf. Theory*, vol. 47, no. 2, pp. 585–598, Feb. 2001.

[21] T. Richardson and R. Urbanke, "The capacity of low-density parity check codes under message-passing decoding," *IEEE Trans. Inf. Theory,* vol. 47, no. 2, pp. 599–618, Feb. 2001.

[22] IEEE, "IEEE standards for information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements. Part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications. Amendment 5: Enhancement for higher throughput," *IEEE Std 802.11n-2009*, Oct. 2009.

[23] IEEE, "IEEE standards for information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements. Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specification. Amendment 1: Physical layer and management parameters for 10 Gb/s operation, type 10GBASE-T," *IEEE Std 802.3an-2006*, Sep. 2006.

[24] ETSI, "Digital video broadcasting (DVB): Second generation framing structure, channel coding and modulation systems for broadcasting, interactive services, news gathering and other broadband satellite applications (DVB-S2)," *EN 302 307 v1.2.1*, Aug. 2009.

[25] R. M. Tanner, "A recursive approach to low complexity codes," *IEEE Trans. Inf. Theory*, vol. 27, no. 5, pp. 533–547, Sep. 1981.

[26] G. Liva and W. E. Ryan, "Short low-error-floor Tanner codes with Hamming nodes," in *Proc. IEEE MILCOM*, 2005.

[27] S. Abu-Surra, D. Divsalar, and W. E. Ryan, "Enumerators for protograph-based ensembles of LDPC and generalized LDPC codes," *IEEE Trans. Inf. Theory*, vol. 57, no. 2, pp. 858–886, Feb. 2011.

[28] I. P. Mulholland, E. Paolini, and M. F. Flanagan, "Design of LDPC code ensembles with fast convergence properties," in *Proc. IEEE BlackSeaCom*, 2015.

[29] Y. Liu, P. M. Olmos, and T. Koch, "A probabilistic peeling decoder to efficiently analyze generalized LDPC codes over the BEC," *IEEE Trans. Inf. Theory*, vol. 65, no. 8, pp. 4831–4853, Aug. 2019.

[30] M. Lentmaier and K. S. Zigangirov, "On generalized low-density parity-check codes based on Hamming component codes," *IEEE Commun. Lett.*, vol. 3, no. 8, pp. 248–250, Aug. 1999.

[31] G. Yue, L. Ping, and X. Wang, "Generalized low-density parity-check codes based on Hadamard constraints," *IEEE Trans. Inf. Theory*, vol. 53, no. 3, pp. 1058–1079, Mar. 2007.

[32] N. Miladinovic and M. Fossorier, "Generalized LDPC codes with Reed-Solomon and BCH codes as component codes for binary channels," in *Proc. IEEE GLOBECOM*, 2005.

[33] D. G. M. Mitchell, M. Lentmaier, and D. J. Costello, "On the minimum distance of generalized spatially coupled LDPC codes," in *Proc. IEEE ISIT*, Jul. 2013.

[34] P. M. Olmos, D. G. M. Mitchell, and D. J. Costello, "Analyzing the finite-length performance of generalized LDPC codes," in *Proc. IEEE ISIT*, Jun. 2015.

[35] D. G. M. Mitchell, P. M. Olmos, M. Lentmaier, and D. J. Costello, "Spatially coupled generalized LDPC codes: Asymptotic analysis and finite length scaling," *IEEE Trans. Inf. Theory*, vol. 67, no. 6, pp. 3708–3723, Jun. 2021.

[36] E. Paolini, M. P. C. Fossorier, and M. Chiani, "Generalized and doubly generalized LDPC codes with random component codes for the binary erasure channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 4, pp. 1651–1672, Apr. 2010.

[37] Y. Wang and M. Fossorier, "Doubly generalized LDPC codes," in *Proc. IEEE ISIT*. 2006.

[38] Y. Wang and M. Fossorier, "Doubly generalized LDPC codes over the AWGN channel," *IEEE Trans. Commun.*, vol. 57, no. 5, pp. 1312–1319, May 2009.

[39] R. Guan and L. Zhang, "Hybrid Hamming GLDPC codes over the binary erasure channel," in *Proc. IEEE ASID*, 2017.

[40] J. Thorpe, "Low-density parity-check (LDPC) codes constructed from protographs," Jet Propulsion Lab., Pasadena, CA, INP Progress Rep. 42–154, 2003.

[41] G. Liva, W. E. Ryan, and M. Chiani, "Quasi-cyclic generalized LDPC codes with low error floors," *IEEE Trans. Commun.*, vol. 56, no. 1, pp. 49–57, Jan. 2008.

[42] M. Lentmaier, M. B. S. Tavares, and G. P. Fettweis, "Exact erasure channel density evolution for protograph-based generalized LDPC codes," in *Proc. IEEE ISIT*, 2009.

[43] A. Ashikhmin, G. Kramer, and S. ten Brink, "Extrinsic information transfer functions: Model and erasure channel properties," in *IEEE Tran. Inf. Theory*, vol. 50, no. 11, pp. 2657–2673, Nov. 2004.

[44] G. Liva and M. Chiani, "Protograph LDPC codes design based on EXIT analysis," in *Proc. IEEE GLOBECOM*, 2007.

[45] D. Divsalar, S. Dolinar, and C. Jones, "Construction of protograph LDPC codes with linear minimum distance," in *Proc. IEEE ISIT*, 2006.

[46] Y. Yu, Y. Han, and L. Zhang, "Hamming-GLDPC codes in BEC and AWGN channel," in *Proc. IEEE ICWMMN*, 2015.

[47] C. Di, A. Montanari, and R. Urbanke, "Weight distributions of LDPC code ensembles: Combinatorics meets statistical physics," in *Proc. ISIT*, 2004.

[48] S. Abu-Surra, D. Divsalar, and W. E. Ryan, "On the existence of typical minimum distance for protograph-based LDPC codes," in *Proc. IEEE ITA*, 2010.

[49] S. Abu-Surra, D. Divsalar, and W. E. Ryan, "On the typical minimum distance of protograph-based generalized LDPC codes," in *Proc. IEEE ISIT*, 2010,

[50] A. K. Pradhan, A. Thangaraj, and A. Subramanian, "Construction of near-capacity protograph LDPC code sequences with block-error thresholds," *IEEE Trans. Commun.*, vol. 64, no. 1, pp. 27–37, Jan. 2016.

[51] C. Di, T. J. Richardson, and R. L. Urbanke, "Weight distribution of low-density parity-check codes," *IEEE Trans. Inf. Theory*, vol. 52, no. 11, pp. 4839–4855, Nov. 2006.

[52] A. Shokrollahi and R. Storn, "Design of efficient erasure codes with differential evolution," in *Proc. IEEE ISIT*, 2000.

[53] Xiao-Yu Hu, E. Eleftheriou, and D. M. Arnold, "Regular and irregular progressive edge-growth Tanner graphs," *IEEE Trans. Inf. Theory*, vol. 51, no. 1, pp. 386–398, Jan. 2005.

[54] D. Divsalar, C. Jones, S. Dolinar, and J. Thorpe, "Protograph based LDPC codes with minimum distance linearly growing with block size," in *Proc. IEEE GLOBECOM*, 2005.

[55] D. G. M. Mitchell, M. Lentmaier, A. E. Pusane, and D. J. Costello, "Randomly punctured LDPC codes," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 2, pp. 408–421, Feb. 2016.

[56] J. J. Boutros, A. Guillén i Fàbregas, E. Biglieri, and G. Zémor, "Low-density parity-check codes for nonergodic bock-fading channels," *IEEE Trans. Inf. Theory*, vol. 56, no. 9, pp. 4286–4300, Aug. 2010.

[57] Y. Fang, G. Bi, and Y. L. Guan, "Design and analysis of root-protograph LDPC codes for non-ergodic block-fading channels," *IEEE Trans. Wireless Commun.*, vol. 14, no. 2, pp. 738–749, Feb. 2015.

[58] S. Kim, J.-S. No, H. Chung, and D. Shin, "Quasi-cyclic low-density parity-check codes with girth larger than 12," *IEEE Trans. Inf. Theory*, vol. 53, no. 8, pp. 2885–2891, Aug. 2007.

[59] C. T. Healy and R. C. de Lamare, "Design of LDPC codes based on multipath EMD strategies for progressive edge growth," *IEEE Trans. Commun.*, vol. 64, no. 8, pp. 3208–3219, Aug. 2016.

[60] C. Kim, S.-H. Kim and J.-S. No, "New GRP LDPC codes for H-ARQ-IR over the block fading channel", *IEEE Trans. Commun.*, vol. 68, no. 11, pp. 6642–6656, Nov. 2020.

[61] M. -S. Alouini and M. K. Simon, "An MGF-based performance analysis of generalized selection combining over Rayleigh fading channels," *IEEE Trans. Commun.*, vol. 48, no. 3, pp. 401–415, Mar. 2000.

[62] P. V. Sukhatme, "Tests of significance for samples of the χ^2 population with two degrees of freedom," *Ann. Eugenics*, vol. 8, pp. 52–56, 1937.

[63] K. D. Nguyen, A. G. i. Fabregas, and L. K. Rasmussen, "Analysis and computation of the outage probability of discrete-input block-fading channels," in *Proc. IEEE ISIT*, Nice, France, Jun. 2007.

[64] R. Knopp and P. A. Humblet, "On coding for block fading channels," *IEEE Trans. Inf. Theory*, vol. 46, no. 1, pp. 189–205, Jan. 2000.

[65] C. J. Colbourn and J. H. Dinitz, *The CRC Handbook of Combinatorial Designs*. Boca Raton, FL: CRC, 1996.

초 록

이 학위 논문에서는 다음 두 가지의 연구가 이루어졌다: i) 이진 소실 채널에서 새로운 구조의 프로토그래프 기반 generalized low-density parity-check (GLDPC) 부호의 설계 방법 ii) 블록 페이딩 채널을 위한 프로토그래프 기반의 LDPC 부호 설계.

첫 번째로, 이진 소실 채널에서 새롭게 제안된 부분적 도핑 기법을 이용한 프로토그래프 기반의 GLDPC 부호가 제안되었다. 기존의 프로토그래프 기반의 GLDPC 부호의 경우 프로토그래프 영역에서 single parity-check (SPC) 노드를 generalized constraint (GC) 노드로 치환(도핑)하는 형태로 부호가 설계되어 여러 변수 노드 걸쳐 GC 노드가 연결되는 형태를 가진다. 반면, 제안된 부분적 도핑 기법은 한 개의 변수 노드에 GC 노드를 연결하도록 만들 수 있다. 바꿔 말하면, 제안된 부분적 도핑 기법은 더 세밀한 도핑이 가능해서 결과적으로 부호 설계에 있어 높은 자유도를 가지고 더 세련된 부호 최적화가 가능하다. 본 학위 논문에서는 부분적 도핑과 PEXIT 분석을 이용하여 partially doped GLDPC (PD-GLDPC) 부호를 설계하고 최적화 하였다. 더불어, PD-GLDPC 부호의 일반적 최소 거리를 가지는 조건을 제시하였고 이를 이 론적으로 증명하였다. 결과적으로, 제안된 PD-GLDPC 부호는 현존하는 GLDPC 부호의 성능보다 유의미하게 워터플 성능이 좋았고 동시에 오류 마루가 없었다. 마지막으로, 최적화된 PD-GLDPC 부호는 현존하는 최신 블록 LDPC 부호들에 근접한 성능을 가짐을 보여주었다.

두 번째로, 블록 페이딩 (BF) 채널에서 resolvable block design (RBD)를 이용한 프로토그래프 LDPC 부호 설계가 이루어졌다. 제안된 부호의 성능을 확인하기 위한 비트 오류율의 상한을 감마 진화라는 제안된 기법을 이용해 유도하였다. 또한, 시뮬레이션을 통해 유도된 오류율 상한과 부호의 프레임 오류율이 높은 SNR 영역에서

채널 outage 확률에 근접함을 알 수 있다.

주요어: 블록 페이딩 채널, 오류 정정 부호, 일반적 저밀도 패리티 체크 부호, 저밀도 패리티 체크 부호, 부분 도핑, 부분 도핑된 일반적 저밀도 패리티 체크 부호, resolvable 블록설계, resolvable 균형불완비블록설계, 일반적 최소 거리
학번: 2016-20878