Efficiently Encodable Low-Density Codes and Generalization of Tanner’s Bounds

by

Min-Ho Shin

A Dissertation Submitted to the Graduate School of Yonsei University in partial fulfillment of the requirements for the degree of Doctor of Philosophy

Supervised by Professor Hong-Yeop Song, Ph.D.

Department of Electrical and Electronic Engineering The Graduate School

YONSEI University

December 2004
Contents

List of Figures v

List of Tables vi

Abstract vii

1 Introduction 1

1.1 Motivation .................................. 1
1.2 Overview ................................... 4

2 Properties of Circulant Matrices and Design Criteria for LDPC Codes 5

2.1 Properties of Circulant Matrices .................... 5
2.2 Known Design Criteria ........................... 8
2.3 Construction Methods so far .......................... 10

2.3.1 Density Evolution .......................... 10
2.3.2 Efficient Encoding Algorithm ................... 11
2.3.3 Stair case Codes ............................ 12
2.3.4 PEG Algorithm ............................. 15
3 Construction of QC-LDPC Codes from \(q\)-th Power Residues

3.1 QC-LDPC Codes ........................................... 20
3.2 QC-LDPC codes from Power Residue .......................... 21
3.3 Regular Constructions and Simulations ......................... 26
3.4 Irregular Constructions using block-PEG Algorithm .............. 30
3.5 Remarks .................................................. 35

4 Irregular Concatenated LDGM Codes by LLR Analysis

4.1 Low-Density Generator Codes ............................... 37
4.2 Irregular Concatenated LDGM Codes by LLR analysis ........   39
4.3 Simulation Results ......................................... 41
4.4 Remarks .................................................. 45

5 Generalization of Tanner’s Minimum Distance Bounds for LDPC Codes

5.1 Tanner’s Minimum Distance Bounds ........................... 48
5.2 Generalization of the bounds .................................. 50
5.3 Code Construction Examples ................................ 55
5.4 Remarks .................................................. 60

6 Concluding Remarks

6.1 Summary .................................................. 64
6.2 Future Directions ......................................... 66
List of Figures

2.1 Binary circulant matrix. ........................................... 6
2.2 Richardson’s parity-check matrix form and its encoder structure. .... 13
2.3 Encoder structure for staircase codes. .......................... 14
2.4 Neighbor $\mathcal{N}_{b_i}$ within depth $l$ of bit node $b_i$. ................. 16

3.1 A rate-1/2 QC-LDPC code from two circulant matrices. ................. 22
3.2 A [39,4,6]-regular LDPC code from power residue. ..................... 24
3.3 Six basic types for 6-cycle and an example of 6-cycle. ................... 25
3.4 Encoder structure of QC-LDPC code. .............................. 26
3.5 Encoder structure of shortened QC-LDPC code. ....................... 27
3.6 Parity-check matrix of rate-1/2 [1002,3,6] QC-LDPC code. ................. 28
3.7 Flow chart of construction process for QC-LDPC codes. ................. 29
3.8 Simulation results of regular QC-LDPC codes. ........................ 30
3.9 Block-PEG algorithm .............................................. 31
3.10 Parity-check matrices of rate-1/2 irregular QC-LDPC codes. ............. 33
3.11 BER/FER simulation results of irregular QC-LDPC codes. ............... 34

4.1 Generator matrix, parity-check matrix and the associated bipartite graph. 38
<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2</td>
<td>Graph representation of concatenated LDGM codes</td>
<td>40</td>
</tr>
<tr>
<td>4.3</td>
<td>Parity check matrices of concatenated LDGM codes</td>
<td>42</td>
</tr>
<tr>
<td>4.4</td>
<td>Average LLRs of concatenated LDGM codes</td>
<td>43</td>
</tr>
<tr>
<td>4.5</td>
<td>BER/FER simulation results of concatenated LDGM codes</td>
<td>46</td>
</tr>
<tr>
<td>5.1</td>
<td>Parity-check matrix and the associated bipartite graph</td>
<td>51</td>
</tr>
<tr>
<td>5.2</td>
<td>BER performance of QC-LDPC codes compared with that of randomly constructed ones</td>
<td>58</td>
</tr>
<tr>
<td>5.3</td>
<td>BER performance comparison of QC-LDPC codes</td>
<td>62</td>
</tr>
</tbody>
</table>
List of Tables

2.1 Design criteria for LDPC constructions .................................. 10
2.2 Construction methods so far .................................................. 18
3.1 Search results for [1002,3,6] QC-LDPC codes in Example 3.3 ...... 28
5.1 Weight enumeration of LDPC codes in Example 5.2 ................. 57
5.2 Search Results of Optimized QC-LDPC Codes ....................... 61
ABSTRACT

Efficiently Encodable Low-Density Codes and Generalization of Tanner’s Bounds

Min-Ho Shin
Department of Electrical and Electronic Eng.
The Graduate School
Yonsei University

Codes on graphs such as low-density parity check (LDPC) codes and turbo codes, together with the associated iterative decoding algorithms, are now known as practical and capacity-approaching coding schemes. Since one major drawback of LDPC codes is their high encoding complexity it is worth investigating to design efficiently encodable low-density codes.

We first consider quasi-cyclic LDPC (QC-LDPC) codes that have efficient encoder structure. So far QC-LDPC codes have mostly regular structure with weight-1 circulants, while we consider QC-codes from residue number systems with weight 0, 1, and 2 circulant matrices. QC-LDPC codes from residue number system have an advantages over other schemes that they admit a structure that does not excessively increase the number of short cycles while they give benefits to construct higher degree bit nodes with improved performance. We propose the algebraic construction of QC-LDPC codes us-
ing residue number systems for regular codes. To design irregular QC-LDPC codes, we suggest a block progressive edge growth (block-PEG) algorithm by modifying the original PEG algorithm. We construct block-wise irregular QC-LDPC codes using this algorithm and compare the performance of the codes with that of other coding schemes that have similar structure.

Another class of linear codes with iterative decoding algorithm is low-density generator matrix (LDGM) codes that have extremely efficient encoder structure. Recently it has been shown that this coding scheme approaches the Shannon limit by concatenation of two systematic regular LDGM codes. The problem of this coding scheme is the presence of degree-1 bit nodes which deteriorates the overall performance during a message-passing decoding process. To solve this problem we propose an irregular concatenated LDGM coding scheme. Proposed construction method increases the reliability of degree-1 nodes using irregular graphs by analysis on the log-likelihood ratio (LLR) values of bit nodes.

In the last, we derive a bit-oriented bound and a parity-oriented bound on the minimum distance of both regular and block-wise irregular LDPC codes using the relationship between nodes on the graph and a minimum-weight codeword. We generalize Tanner’s results and set up a heuristic rule that a code with a smaller ratio of second to first eigenvalue would have a good distance property. We construct various example codes and show that the proposed design criteria work well in designing block-wise irregular LDPC codes.

**Key words:** Low-density parity-check codes, quasi-cyclic codes, power residue, block-PEG algorithm, irregular low-density generator matrix codes, minimum distance bound
Chapter 1

Introduction

1.1 Motivation

In the half century since Shannon derived the capacity of ergodic channels, the construction of capacity-achieving coding schemes has been the supreme goal of coding research. Now we know that all revealed practical capacity-achieving coding schemes, such as low-density parity-check codes (LDPC) and turbo codes, are understood to be codes defined on graphs, combined with the associated iterative decoding algorithm called sum-product decoding.

LDPC codes were originally invented by Gallager [1] at 1961 but were subsequently neglected by the coding community since Gallager’s codes were simply considered impractical. Recent research concentration upon codes on graphs and sum-product decoding was ignited in the mid-1990s by the advent of turbo codes of Berrou et. al [2] and the rediscovery on Gallager codes by MacKay and Neal [3]. In many ways LDPC codes are thought to be intense competitors to turbo codes. Especially LDPC codes exhibit an asymptotically better performance than turbo codes, and they admit a various code rates and wide range of tradeoffs between performance and decoding complexity.
One major drawback of LDPC codes is their high encoding complexity. While turbo codes are linear time encodable with shift-registers, encoders for LDPC codes in general are considered to be performed by matrix multiplication which has complexity quadratic in the block length. Therefore it is worth while to

- design LDPC codes with efficient encoder structure.

LDPC codes approaches to the Shannon limit by the random property of the encoder structure with iterative decoding. Actually pseudorandom constructions of codes on graphs work well, in particular for long block lengths. However more structured algebraic constructions are especially desirable both in order to describe codes concisely and to investigate their distance property and graph-theoretic characteristics more precisely. That is why we are interested in

- algebraic construction of LDPC codes.

Luby et al. introduced LDPC codes with highly non-uniform column-weight distributions which give improved performance [4]. The capacity of LDPC codes with sum-product decoding has been determined by an algorithm called density evolution [5]. The approach of this algorithm has been made concerning the asymptotics of ensembles of codes, i.e., randomly chosen codes from a given class. This algorithm considers the distribution of the messages on graphs, and is parameterized in terms of degree distribution sequences. Consequently, many capacity-approaching degree distribution sequences of irregular LDPC codes have been found in terms of the threshold calculated by this algorithm [6]. However the irregular codes are mostly constructed via a pseudo-random
process which merely involves discarding codes which contain 4-cycles. Henceforth it is a challengeable work

- to explicitly find the best possible irregular Tanner graphs with given degree distribution sequences with an appropriate optimization algorithm.

In practical applications, capacity approaching channel coding schemes such as turbo codes and LDPC codes present either a high encoding or high decoding complexity. One class of channel coding schemes with iterative decoding algorithm to solve this complexity issues is LDGM codes consist of systematic linear codes. Since the parity check matrices of systematic LDGM codes are also sparse, they are in fact a subset of LDPC codes and can be decoded in the same manner as general LDPC codes. Garcia et al. introduced concatenated regular LDGM codes whose performance approaches the Shannon limit. One weakness point of LDGM codes is the existence of degree-1 bit nodes at the parity parts due to systematic structure. Since sum-product algorithm updates each bit node reliability via iterative decoding for the successful process of message-passing algorithm it will be a good construction method

- to increase the reliability of degree-1 bit nodes of LDGM codes and thus improve the overall performance.

Finally we mention that although much characteristics of LDPC codes are now unveil, whereas, relatively few researches have been conducted on the distance property of the LDPC codes. Tanner [7] derived minimum distance bounds on the regular LDPC codes in terms of the eigenvalues of the associated graph by using the relationship be-
tween nodes on the graph and a minimum-weight codeword. Since codes on irregular
graphs perform better than a regular one, it is quite desirable

- to derive the minimum distance bounds on both regular and irregular LDPC codes.

1.2 Overview

In chapter 2, we explain some definitions and properties of circulant matrices. In addi-
tion, we introduce design criteria and construction methods for LDPC codes so far.
In chapter 3, we propose construction of quasi-cyclic LDPC codes with circulant matri-
ces. Here circulant matrices are obtained using power residues/non-residues. In addi-
tion, an efficient encoder structure of the proposed codes is described. For the irregular
QC-LDPC codes we derive block-progressive edge growth (block-PEG) algorithm that
constructs QC-codes block-by-block basis. We construct some irregular QC-codes and
compare the performance with other codes. In chapter 4, we introduce efficiently en-
codable concatenated LDGM codes. By analysis on the log-likelihood ratios (LLRs) of
bit nodes we propose irregular LDGM codes with improved performance. In chapter 5
we derive a bit-oriented bound and a parity-oriented bound on the minimum distance
of both regular and block-wise irregular LDPC codes. Finally all those results of this
dissertation are summarized and some discussions follow.
Chapter 2

Properties of Circulant Matrices and Design Criteria for LDPC Codes

In this chapter we first introduce some basic properties of circulant matrices that will be used throughout the dissertation. Next, we summarize and explain known design criteria for the construction of LDPC codes. We investigate various construction methods for LDPC codes that have been published so far.

2.1 Properties of Circulant Matrices

We consider square circulant matrices of order \( p \) with coefficients \( a_i \) in the binary field \( \text{GF}(2) \) in which each row is the previous one shifted once to the right.

Rows and columns are numbered from 0 to \( p - 1 \) as shown in Fig.2.1. Any element \( a_{ij} \) is entirely determined by \( j - i \). It is well known that circulants are entirely characterized by the polynomials formed on their top rows:

\[
a(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{p-1} x^{p-1} \mod x^p - 1.
\]  

(2.1)
Figure 2.1: Binary circulant matrix.

This isomorphism between the algebra of polynomials \( a(x) \mod x^p - 1 \) and the circulants is quite complete, i.e., the multiplication of two polynomials \( a(x)b(x) \mod x^p - 1 \) is identical to the leading row polynomial of circulant product \( AB = BA \).

**Definition 2.1** A polynomial \( a(x) \) will be called nonsingular, or invertible, if there is a polynomial \( a(x)^{-1} \) such that
\[
a(x)a(x)^{-1} = 1 \mod x^p - 1.
\]

**Definition 2.2** The transpose polynomial \( a(x)^T \) corresponding to column 0 of (2.1) can be defined as
\[
a(x)^T = \sum_{i=0}^{p-1} a_i x^{i-1} \mod x^p - 1.
\]

**Definition 2.3** The rank over the binary field of an \( p \times p \) circulant \( A \), is the dimension of the ideal generated by \( a(x) \) in the ring of binary polynomials \( \mod x^p - 1 \).
Definition 2.4 The weight of a polynomial, denoted \( w(a(x)) \), is the number of nonzero terms in \( a(x) \). This is also called the weight of circulant matrix \( A \).

Definition 2.5 A symmetric polynomial is defined by \( s(x) = s(x)^T \), and a nonsingular symmetric polynomial by \( h(x) = h(x)^T \) with \( h(x)h(x)^{-1} = 1 \).

Definition 2.6 A 1-generator quasi-cyclic code of dimension \( p \) and length \( n = mp \) is a linear code \( C \) with generator matrix

\[
G = [G_1, G_2, G_3, \cdots, G_m],
\]

where each \( G_j, 1 \leq j \leq m \), is a \( p \times p \) circulant matrix.

This matrix \( G \) generates a quasi-cyclic code iff \( \text{rank } G = p \).

Theorem 2.1 [8] Let \( G = [G_1, G_2, \cdots, G_m] \) where \( G_j, 1 \leq j \leq m \), are \( p \times p \) circulants associated with polynomials \( g_j(x) \) by (2.1). Then

\[
\text{rank } G = k \iff \gcd(g_1(x), g_2(x), \cdots, g_m(x), x^p - 1) \quad (2.2)
\]

is a nonzero constant.

In this dissertation, all these definitions and theorems will be widely used in designing LDPC codes based on circulant matrices.
2.2 Known Design Criteria

The recent literature in coding has seen an explosion of papers surrounding the design of LDPC codes. We first introduce basic design criteria for LDPC codes.

- **Sparsity**: The sparsity non-zero elements in the parity check matrix is a key to success of LDPC codes for practical error correcting codes. Since in the decoder, the information for a particular check or bit node depends on the nodes that are connected to it. Therefore the lower the density of the code, the simpler the calculations. Note that, however, sparsity alone does not guarantee a good LDPC code.

- **Large minimum distance** Gallager showed that a randomly generated LDPC codes have good minimum distances for long block lengths [1]. So far codes defined randomly rather than with a simple structure seem to have better distance properties. It is generally known that the large minimum distance relieves error-floors in high SNR. However the distance properties of LDPC codes are quite unveil possibly except algebraic constructions based on finite geometries by S. Lin et.al [9].

- **Large girth** It is well known that with a cycle-free Tanner graph, the message-passing decoding algorithm terminates naturally in a finite number of steps and yields optimal decoding in the sense that the frame error probability is minimized [10]. The girth of an LDPC code is defined as the length of the smallest cycle in the tanner graph representation of the parity check matrix. Hence the
girth determines the smallest number of iterations for a message sent by a node in the shortest cycle of the graph to propagate back to the node itself. This causes loss of independence in the extrinsic information merged on a node in the iterative decoding through the successive iterations. Therefore large girth is important to the message-passing decoding algorithm because it speeds the convergence of iterative decoding and improves the performance at least in the high SNR range.

- **Algebraic constructions** Algebraic constructions have their own merits over randomly constructed codes that they can be easily described with good theoretical properties and have comparable performances. The performance of regular LDPC codes can be enhanced in a third manner with algebraic properties. That is to design a code to have redundant sparse constraints. One example of such code is a difference-set cyclic code [3]. The difference-set cyclic code performs about 0.7dB better than an equivalent random LDPC code.

- **Regularity and irregularity** The main advantages of regular LDPC codes are their simple representation and easiness of implementation. So far algebraically describable LDPC codes are mostly regular codes, e.g., finite geometry-based codes [9], balanced incomplete block designs [11] [12] [13] [14], and so on. The most powerful way of improving LDPC codes, introduced by Luby et al. is to make their Tanner graphs irregular [4]. Methods for optimizing the degree distribution sequences of an LDPC code have been developed by Richardson et al., and have led to irregular LDPC codes whose performance, when decoded with sum-product algorithm, approaches the Shannon limit within hundredths of a decibel.
Table 2.1: Design criteria for LDPC constructions

<table>
<thead>
<tr>
<th>Design Criteria</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sparsity</td>
<td>need to practical iterative decoding</td>
</tr>
<tr>
<td>Large minimum distance</td>
<td>to avoid error-floor at high SNR</td>
</tr>
<tr>
<td>Large girth</td>
<td>need to decode with independency</td>
</tr>
<tr>
<td>Algebraic constructions</td>
<td>easy to describe specific code, easy to analyze</td>
</tr>
<tr>
<td>Regularity</td>
<td>easy to implement but relatively poor performance</td>
</tr>
<tr>
<td>Irregularity</td>
<td>difficult to implement but better performance</td>
</tr>
</tbody>
</table>

2.3 Construction Methods so far

So far, various construction methods for LDPC codes have been presented. In this section we summarize and explain some major construction methods for LDPC codes.

2.3.1 Density Evolution

Richardson et al. demonstrated that the average asymptotic behavior of a sum-product decoding for LDPC codes is numerically computable by using an algorithm called *density evolution* [5]. They also showed that for various channels, including additive white Gaussian noise (AWGN) channels, one can calculate a *threshold* value for the ensemble of randomly constructed LDPC codes which asymptotically determines the boundary of the error-free region with the assumption of infinite block length. Density evolution can efficiently be computed by means of Fourier transform based methods.

**Theorem 2.2 (Density Evolution [5])** Let $P_0$ denote the initial message distribution, under the assumption that the all-one codeword was transmitted, of a LDPC code spec-
ified by degree distributions $\sum_i \lambda_i x^{i-1}$ and $\sum_i \rho_i x^{i-1}$. If $R_l$ denotes the density of the messages passed from the check nodes to the variable nodes at round $l$ of the belief propagation, with $R_0 := \triangle_0$, then we have

$$R_l = \Gamma^{-1} \rho(\Gamma(P_0 \otimes \lambda(R_{l-1}))).$$

Many capacity-approaching degree sequences are found in terms of density evolution using numerical optimization techniques.

### 2.3.2 Efficient Encoding Algorithm

Richardson et al. demonstrated an elegant method by which the encoding cost of any LDPC code with $n \times m$ parity check matrix can be reduced from the $m^2$ to a cost of $n + g^2$, where $g$, is a small small fraction of $n$.

In the first step, the parity-check matrix is rearranged into the approximate lower-triangular form shown in Fig. 2.2(a), where the matrix $T$ is lower triangular and has 1s along the diagonal.

$$H = \begin{bmatrix} A & B & C \\ D & E & F \end{bmatrix}$$

Consider modified matrix $H'$ by making the matrix $E$ in $H$ to zero-matrix.

$$H' = \begin{bmatrix} A & B & C \\ D & E & F \end{bmatrix} \times \begin{bmatrix} I & 0 \\ -ET^{-1} & I \end{bmatrix}$$

$$= \begin{bmatrix} A \\ -ET^{-1}A+C \\ -ET^{-1}B+D \end{bmatrix} \begin{bmatrix} B \\ 0 \\ T \end{bmatrix}$$

Let a codeword be $c = [u | p_1 | p_2]$, then the codeword $c$ satisfies the following equations

$$Au^T + Bp_1^T + TP_2^T = 0^T,$$

$$(-ET^{-1}A+C)u^T + (-ET^{-1}B+D)p_1^T = 0^T.$$
Let $\phi = -ET^{-1}B + D$ and assume that $\phi$ is nonsingular. Then we can obtain parity bits as following equations,

$$p_1^T = -\phi^{-1}(-ET^{-1}A + C)u^T,$$
$$p_2^T = -T^{-1}(Au^T + Bp_1^T).$$

The overall complexity of this encoding algorithm is determined as $O(n + g^2)$. The encoder structure for this algorithm is shown in Fig. 2.2(b). Lots of efficiently encodable LDPC codes are constructed based on this structure, especially optional B-LDPC [15] simplifies the encoding process one step more by making the matrix $\phi = I$.

### 2.3.3 Stair case Codes

Certain low-density parity check matrices with $m$ columns of weight 2 or less can be encoded easily in linear time, especially when the parity part of the matrix is staircase structure [16].

Let a parity check matrix be

$$H = [H_1 H_2],$$

where $H_1$ and $H_2$ correspond to information bits and parity bits respectively. Let $H_2$ be a full-rank $m \times m$ matrix as follows.

$$H_2 = \begin{bmatrix}
1 \\
1 & 1 \\
1 & 1 \\
\vdots \\
1 & 1 \\
1 & 1
\end{bmatrix}$$
(a) Parity-check matrix in approximate lower-triangular form

(b) Encoder structure

Figure 2.2: Richardson’s parity-check matrix form and its encoder structure.
If the information bits $u = [u_1 u_2 \cdots u_k]$ are encoded, the parity bits $p = [p_1 p_2 \cdots p_m]$ can be computed recursively as follows.

$$
\begin{align*}
p_1 &= \sum_{i=1}^{k} H_{1i} u_i \\
p_2 &= p_1 + \sum_{i=1}^{k} H_{2i} u_i \\
p_3 &= p_2 + \sum_{i=1}^{k} H_{3i} u_i \\
\vdots \\
p_m &= p_{m-1} + \sum_{i=1}^{k} H_{mi} u_i
\end{align*}
$$

An alternative way to look at encoding for this class of codes is as follows. The systematic generator matrix $G$ for the code of (2.4) is given by

$$
G = [IP] = [IH_1^T H_2^{-T}]
$$

And it is easy to check that the transpose of $H_2^{-1}$ is

$$
H_2^{-T} = \begin{bmatrix}
1 & 1 & \cdots & 1 & 1 \\
1 & \cdots & 1 & 1 \\
\vdots & \vdots & \vdots & \vdots & \vdots \\
1 & 1 & \cdots & 1 & 1 \\
1 & 1 & \cdots & 1 & 1
\end{bmatrix}.
$$

This matrix is precisely the transformation matrix corresponding to a differential encoder whose transfer function is $1/1 \oplus D$. Hence the encoder for this class of LDPC codes exploits efficiently encodable structure as shown in Fig. 2.3.
2.3.4 PEG Algorithm

Hu et al. introduced edge-by-edge girth conditioning algorithm called progressive edge-growth (PEG) construction which tries to remove as many short cycles as possible [17]. To explain the PEG algorithm we first introduce some definitions and notations. An LDPC code with \(m \times n\) sparse parity check matrix can be thought as a bipartite graph with \(n\) bit nodes and \(m\) check nodes. A Tanner graph is \(G = (V_b \cup V_c, E)\), where \(V_b = \{b_0, b_1, \ldots, b_{n-1}\}\), \(V_c = \{c_0, c_1, \ldots, c_{m-1}\}\) and the edge set \(E\) consists of edge \((c_i, b_j)\) in \(V_c \times V_b\) corresponds to nonzero \(h_{ij}\) in \(H\). Denote the bit degree sequence by \(D_b = \{d_{b_0}, d_{b_1}, \ldots, d_{b_{n-1}}\}\), and the parity-check degree sequence by \(D_c = \{d_{c_0}, d_{c_1}, \ldots, d_{c_{m-1}}\}\). Let \(E_{b_i}\) be the edge set consists all edges incident on the bit node \(b_i\) and \(E_{b_i}^k\) be the \(k\)-th edge incident on \(b_i\), \(0 \leq k \leq d_{b_i} - 1\).

For a given bit node \(b_i\), define its neighbor within depth \(l\), \(N^l_{b_i}\), as the set consisting of all incident check nodes supported by tree expansion from bit node \(b_i\) within depth \(l\) as shown in Fig. 2.4. Its complementary set, \(\bar{N}^l_{b_i}\), is defined as \(V_c \setminus N^l_{b_i}\).

In graph theory, girth \(g\) refers to the length of the shortest cycle in a graph. For each bit node \(b_i\), define a local girth \(g_{b_i}\) as the length of the shortest cycle passing through the bit node \(b_i\). The set of local girths \(\{g_{b_i}\}\) is defined as girth histogram. It follows that the girth of a graph \(g\) is the minimum local girth \(g_{b_i}\), i.e., \(g = \min\{g_{b_i}\}\)

The PEG algorithm is girth conditioning algorithm which makes the local girth of a bit node to be maximized whenever a new edge is added to the node. After having finished constructing edges of the first \(i\) bit nodes on a Tanner graph, let \(g^t\) be a temporary girth under the current graph, i.e., \(g^t = \min\{g_{b_0}, g_{b_1}, \ldots, g_{b_{i-1}}\}\). Then the next step is
Figure 2.4: Neighbor $N_{b_i}^l$ within depth $l$ of bit node $b_i$.

how to select the edge set $E_{b_i}$ such that adding these new edges to the current graph does not exceedingly decrease the current $g^t$. Optimizing the current edge set incident on $b_i$ means maximizing the local girth $g_{b_i}$, because adding $E_{b_i}$ to the current graph results in a cycle shorter than $g^t$. The PEG algorithm adds $d_{b_i}$ edges of $E_{b_i}$ to the current graph on an edge-by-edge basis, and makes the length of the shortest cycle passing through the bit node $b_i$ to be maximized whenever a new edge incident on $b_i$ is being added. During
each optimizing process, the tree originated from the bit node $b_i$ is expanded up to depth $l$ such that $\tilde{N}_{b_i}^l \neq \emptyset$ but $\tilde{N}_{b_i}^{l+1} = \emptyset$ or the cardinality of $\tilde{N}_{b_i}^l$ stops increasing. Then a new edge incident on both $b_i$ and a check node selected from $\tilde{N}_{b_i}^l$ is determined. This algorithm guarantees that the shortest cycle passing through this new edge is not shorter than $2(l + 2)$.

### 2.4 Remarks

So far we have investigated some algebraic properties of circulant matrices that will be widely used throughout this dissertation. We also introduced design criteria for the construction of LDPC codes and explained some important known construction methods for LDPC codes. More construction methods for LDPC codes are summarized in Table 2.2.
<table>
<thead>
<tr>
<th>Construction Methods</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Random Construction [3]</td>
<td>• by superposing permutation matrices without 4-cycle</td>
</tr>
<tr>
<td></td>
<td>• easy to construct</td>
</tr>
<tr>
<td></td>
<td>• encoding is complex</td>
</tr>
<tr>
<td>EG/PG LDPC [9]</td>
<td>• cyclic structure (simple encoder structure)</td>
</tr>
<tr>
<td></td>
<td>• good distance property</td>
</tr>
<tr>
<td></td>
<td>• algebraic construction</td>
</tr>
<tr>
<td></td>
<td>• complexity increases as block length increases</td>
</tr>
<tr>
<td></td>
<td>• fixed code rate</td>
</tr>
<tr>
<td>Based on Combinatorics</td>
<td>• Balanced incomplete block design [18]</td>
</tr>
<tr>
<td></td>
<td>• Kirkman triple system [11] [12]</td>
</tr>
<tr>
<td></td>
<td>• Partial geometry [13]</td>
</tr>
<tr>
<td>Density Evolution [6]</td>
<td>• irregular construction</td>
</tr>
<tr>
<td></td>
<td>• optimized degree distribution sequences</td>
</tr>
<tr>
<td>Array-based LDPC [19]</td>
<td>• efficient encoder structure</td>
</tr>
<tr>
<td></td>
<td>• easy to analyze</td>
</tr>
</tbody>
</table>
Chapter 3

Construction of QC-LDPC Codes from \( q \)-th Power Residues

One of main disadvantages in the implementation of LDPC codes is the encoding complexity since encoding is generally performed by the matrix multiplication. A class of LDPC codes having some cyclic structure, e.g., Euclidian Geometry(EG) LDPC codes and Projective Geometry(PG) LDPC codes, has very low encoding complexity, but they exist over only a small range of code lengths and rates [9]. In this chapter we consider quasi-cyclic LDPC (QC-LDPC) codes which have encoding complexity almost as low as cyclic codes. The parity check matrix of QC-code comprises of circulant matrices, and each circulant matrix can be described by equivalent polynomial. We first design regular QC-LDPC codes using \( q \)-th power residues. Further we propose block-PEG algorithm by modifying the original PEG algorithm and then construct irregular QC-LDPC codes with better performance.
3.1 QC-LDPC Codes

A parity check matrix $H$ of QC-LDPC code is composed of $m \times n$ block matrices given by

$$H = \begin{bmatrix}
H_{11} & H_{12} & \cdots & H_{1m} & \cdots & H_{1,m+1} & \cdots & H_{1n} \\
H_{21} & H_{22} & \cdots & H_{2m} & \cdots & H_{2,m+1} & \cdots & H_{2n} \\
\vdots & \vdots & \ddots & \vdots & \cdots & \vdots & \cdots & \vdots \\
H_{m1} & H_{m2} & \cdots & H_{mm} & \cdots & H_{m,m+1} & \cdots & H_{mn}
\end{bmatrix},$$  \tag{3.1}

where each $H_{ij}$ for $1 \leq i \leq m, 1 \leq j \leq n$ is a $p \times p$ circulant matrix. The algebra of $p \times p$ circulant matrices over GF(2) is isomorphic to the algebra of polynomials modulo $x^p - 1$ with coefficients over GF(2). Thus each circulant matrix $H_{ij}$ is completely described by the associated polynomial $h_{ij}(x)$ corresponding to the top row of $H_{ij}$. More precisely, we have

$$h_{ij}(x) = \sum_{k=0}^{p-1} (H_{ij})_{0k}x^k. \tag{3.2}$$

For the polynomial $h(x) = h_0 + h_1x + \cdots + h_{p-1}x^{p-1}$, its transpose is defined as

$$h(x)^T = \sum_{k=0}^{p-1} h_kx^{n-k}.$$

We define the weight of polynomial $h(x)$ as the number of nonzero coefficients of $h(x)$. Using an equivalent polynomial representation, we can rewrite the matrix $H$ in 3.1 as the following

$$H(x) := \begin{bmatrix}
h_{11}(x) & h_{12}(x) & \cdots & h_{1m}(x) & \cdots & h_{1,m+1}(x) & \cdots & h_{1n}(x) \\
h_{21}(x) & h_{22}(x) & \cdots & h_{2m}(x) & \cdots & h_{2,m+1}(x) & \cdots & h_{2n}(x) \\
\vdots & \vdots & \ddots & \vdots & \cdots & \vdots & \cdots & \vdots \\
h_{m1}(x) & h_{m2}(x) & \cdots & h_{mm}(x) & \cdots & h_{m,m+1}(x) & \cdots & h_{mn}(x)
\end{bmatrix}. \tag{3.3}$$

For general LDPC codes, encoding is performed by matrix multiplication and so complexity is quadratic in the code length. QC-LDPC codes are linear time encodable since encoding process can be performed by polynomial multiplication using shift registers.
**Example 3.1** Consider a rate-1/2 QC-LDPC consists of two $5 \times 5$ circulant matrices. The first circulant is described by $h_1(x) = 1 + x + x^4$, and the second one is described by $h_2(x) = 1 + x^2$. Note $h_1(x)$ is invertible

$$h_1^{-1}(x) = 1 + x^2 + x^3.$$ 

The generator matrix can be put into a systematic form, thus contains $5 \times 5$ identity matrix and the $5 \times 5$ circulant matrix described by the polynomial

$$(h_1^{-1}(x) \ast h_2(x))^T = ((1 + x^2 + x^3) \ast (1 + x^2))^T = (x^3 + x^4)^T = x + x^2.$$ 

Fig. 3.1 shows the parity-check matrix, systematic generator matrix and corresponding Tanner graph of this code. For this example the code is not 4-cycle free. To construct a QC-LDPC code for sum-product decoding we require that the parity check matrix $H$ is sparse and the corresponding Tanner graph of the code is free of short cycles. In the next section we present constructions for such codes using polynomials from power residues.

### 3.2 QC-LDPC codes from Power Residue

Power residues modulo a prime $p$ have applications throughout the fields of number theory, combinatorics, and the theory of block codes. Let $p$ be an odd prime and $q$ be a divisor of $p - 1$. Let $t = (p - 1)/q$ and $\alpha$ be a primitive element mod $p$. Then the nonzero integers mod $p$ can be partitioned into $q$ cosets $C_i$, $0 \leq i \leq q - 1$, where $C_0$ is the set of $q$-th power residues mod $p$, and the remaining $C_i$ are sets of non-residues and formed as $\alpha^i \cdot C_0$. Each $C_i$ has exactly $t$ elements since $C_0$ has $t$ elements and the size of $C_i$ is the same with that of $C_0$ for $1 \leq i \leq q - 1$. 

21
(a) Parity-check matrix with two circulants
\[
H = \begin{bmatrix}
1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 \\
\end{bmatrix}
\]

(b) Systematic generator matrix form
\[
G = \begin{bmatrix}
1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 \\
\end{bmatrix}
\]

(c) Tanner graph representation

Figure 3.1: A rate-1/2 QC-LDPC code from two circulant matrices.
In this work we are interested in the case $q = \frac{p-1}{2}$ because it is favorable to the short cycle problem. Then the $q$-th power residue is $\{\alpha^{\frac{p-1}{2}}, \alpha^{p-1}\}$. Since $\alpha^{\frac{p-1}{2}} = -1 \mod p$, the $q$-th power residue is always $C_0 = \{1, -1\}$. The proposed construction of QC-LDPC using power residues and non-residues has the following base structure.

$$H(x) := \begin{bmatrix}
(1,1) & (\alpha, \alpha) & \cdots & (\alpha^{m-1}, \alpha^{m-1}) \\
(\alpha^n, -\alpha^n) & (\alpha^{n+1}, -\alpha^{n+1}) & \cdots & (\alpha^{2n-1}, -\alpha^{2n-1}) \\
\vdots & \vdots & \ddots & \vdots \\
(\alpha^{(m-1)n}, -\alpha^{(m-1)n}) & (\alpha^{(m-1)n+1}, -\alpha^{(m-1)n+1}) & \cdots & (\alpha^{mn-1}, -\alpha^{mn-1})
\end{bmatrix},$$

where $(a, a)$ denotes $x^a + x^{-a}$. The corresponding codes are $[np, 2m, 2n]$-regular LDPC codes.

**Example 3.2** Let $p = 13$, $m = 2$ and $n = 3$. These parameters set up a [39,4,6]-regular LDPC code. The number of primitive elements in the nonzero integer multiplicative group $\mathbb{Z}^*_13$ is $\phi(12) = 4$. We choose $\alpha = 2$, and the parity-check matrix of this code is shown in the Fig. 3.2. Note this code is free of 4-cycle.

Cycles in Tanner graphs are equivalently analyzed in view of geometrical diagrams in the parity-check matrix. As an example, if bit nodes $b_i, b_j$ and check nodes $c_k, c_l$ form a 4-cycle, we can figure out a rectangle with four vertices $(b_i, c_k), (b_i, c_l), (b_j, c_k)$ and $(b_j, c_l)$ in the parity-check matrix. Longer cycles in the Tanner graphs can be thought as similar. Fig. 3.3 shows six basic types of 6-cycles in view of geometrical diagrams in the parity-check matrix. It is easy to check that a circulant matrix with both column and row weight greater than or equal to 3 will always have 6-cycles as depicted in Fig 3.3. To avoid occurrence of such short cycles we have focused on the case that the weight of each circulant matrix is less than or equal to 2. Method of difference is well used to analyze the distribution of cycles. Here, difference is measured by the distance between any two
non-zeros in the same row or column in the parity-check matrix. Let a weight-2 circulant block in the QC-LDPC code have ones in positions $a$ and $b$ in the first row. Then to make a graph free of 4-cycle we should avoid the occurrence of differences $a + b, a - b, -a + b$ and $-a - b \mod p$ in the remaining blocks with the same column index. On the contrary, we need only to avoid differences $\pm a$ if we are making a circulant block using a power residue. Thus randomness property of power residues/non-residues and the advantage of cycle avoidance are major reason to use circulant blocks from power residues.

For regular LDPC codes it is known that parity check matrices with column weight-3 perform better than the others in the middle range of code rates. Henceforth we modify the matrix in (3.3) so that the resulting code has column weight 3 as shown in the
Figure 3.3: Six basic types for 6-cycle and an example of 6-cycle.
following form.

\[
H(x) := \begin{bmatrix}
  h_{11}(x) & 0 & 0 & \cdots & h_{1m}(x) & h_{1,m+1}(x) & \cdots \\
  h_{21}(x) & h_{22}(x) & 0 & \cdots & 0 & h_{2,m+1}(x) & \cdots \\
  0 & h_{32}(x) & h_{33}(x) & \cdots & 0 & 0 & \cdots \\
  \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \cdots \\
  0 & 0 & 0 & \cdots & h_{m,m}(x) & 0 & \cdots
\end{bmatrix}, \tag{3.4}
\]

where 0 denotes zero polynomial and each weight of the rest polynomial \(h_{ij}\) is

\[
w(h_{ij}(x)) = \begin{cases}
  2 & \text{if } i = j, j + m, j + 2m, \cdots, (1 \leq i \leq m) \\
  1 & \text{otherwise}
\end{cases}
\]

### 3.3 Regular Constructions and Simulations

The encoder structure of the proposed code is shown in Fig. 3.4. The encoding process can be performed with \(p\)-interval since the process can be fully in parallel with \(m \times (n - m) p\)-stage Linear Feedback Shift Register (LFSRs). Further the structure makes it possible to be applicable to various code rates and frame lengths with minimal hardware change, as shown in Fig. 3.5.

\[
c(x) = m(x)G(x) = [p(x), m(x)] = [p_1(x), p_2(x), \ldots, p_a(x), m_1(x), m_2(x), \ldots, m_k(x)]
\]

Figure 3.4: Encoder structure of QC-LDPC code.
This overall systematic procedure for the construction of QC-LDPC code with column weight-3 is described in Fig. 3.7. The following example presents a QC-LDPC code generated by the proposed construction method.

Example 3.3 Let \( m = 3, n = 6 \) and \( p = 167 \). Then we can construct a rate-1/2 \([1002, 3, 6]\) regular QC-LDPC code by proposed construction method. There are \( \phi(166) = 82 \) primitive elements in the nonzero multiplicative group \( \mathbb{Z}_{167}^* \). By applying different primitive elements we generate ensembles of Tanner graphs and then calculate the girth and the number of short cycles of corresponding graphs. An optimized primitive element \( \alpha = 123 \) is chosen by this cycle analysis. Table 3.1 summarizes the search results for QC-LDPC codes of this example with different primitive elements, and Fig. 3.6 shows the parity-check matrix of QC-LDPC code and its systematic form.
Table 3.1: Search results for [1002,3,6] QC-LDPC codes in Example 3.3

<table>
<thead>
<tr>
<th>Primitive</th>
<th># of 4-cycle</th>
<th># of 6-cycle</th>
<th># of 8-cycle</th>
<th>etc</th>
</tr>
</thead>
<tbody>
<tr>
<td>158</td>
<td>0</td>
<td>167</td>
<td>3,151</td>
<td>Minimum number of 6-cycles</td>
</tr>
<tr>
<td>103</td>
<td>0</td>
<td>835</td>
<td>7,301</td>
<td>Maximum number of 6-cycles</td>
</tr>
<tr>
<td>123</td>
<td>0</td>
<td>0</td>
<td>835</td>
<td>Minimum number of 8-cycles</td>
</tr>
<tr>
<td>46</td>
<td>0</td>
<td>0</td>
<td>2,672</td>
<td>Maximum number of 8-cycles</td>
</tr>
</tbody>
</table>

Figure 3.6: Parity-check matrix of rate-1/2 [1002,3,6] QC-LDPC code.
Decide Code Rate/Code length

(Code Rate) = \((n-m)/n\)
(Code length) = \(np\)

Decide \(n, m, p\)

Construction of Circulant matrix

Using \((p-1)/2\)-th residue/nonresidue

Reconstruct the matrix

Make Column weight 3 by Weight Puncturing

Select \(\alpha\) and determine \(H\)

Minimized Short cycle?

Construct Systematic \(H', G\) matrix

Using Row operation
\(H'=[I|P], G=[P^T|I]\)

Cycle analysis by varying \(\alpha\)

Figure 3.7: Flow chart of construction process for QC-LDPC codes.
Simulation results for the codes in Table 3.1 are shown in Fig. 3.8. Sum-product decoding with maximum 80 iterations is applied over an AWGN channel. Performance of QC-LDPC codes is compared with that of MacKay’s random LDPC codes with the same code structure. The best code of Example 3.3 performs slightly better than the MacKay’s code at high SNR. In addition the advantage of encoder implementation makes it worth investigating the proposed construction.

Figure 3.8: Simulation results of regular QC-LDPC codes.

3.4 Irregular Constructions using block-PEG Algorithm

We extend the proposed construction to irregular QC-LDPC codes. For the given code rate, we first determine the number of row blocks and column blocks of the QC-codes. We then obtain an optimized degree distribution sequence using density evolution technique. To find a specific QC-LDPC code corresponding to the degree distribution se-
quence, we modify the PEG algorithm introduced in Chap. 2 such that the algorithm works in block wise sense. We call this algorithm as block-PEG algorithm.

\begin{verbatim}
for i = 1 to N_col blks do
    STEP1
    Find the circulant $C_{ij}$ having the lowest check degree under the current graph setting.
    STEP2
    Choose nonzero position of the left most column of $C_{ij}$, either 0 or by random.
    STEP3
    Construct $C_{ij}$ by cyclic shifts. Set current graph by updating $C_{ij}$.
    for k = 1 to $d_{b_i} - 1$ do
        STEP4
        Tree expansion from bit node $b_i$ up to depth $l$ such that $\bar{N}_l^{b_i - 1} \neq \emptyset$ but $\bar{N}_l^{b_i} = \emptyset$ or the cardinality of $\bar{N}_l^{b_i}$ stops decreasing.
        STEP5
        Find the circulant $C_{ij}$ corresponding to the edge $(b_i, c_k)$ from the set $\bar{N}_l^{b_i - 1}$ which has the lowest check degree under the current graph setting.
        STEP6
        Construct $C_{ij}$ by cyclic shifts. Set current graph by updating $C_{ij}$.
    end for
end for
\end{verbatim}

Figure 3.9: Block-PEG algorithm

Block-PEG algorithm selects a new edge to the current symbol node on a block-by-block basis. It is enough to consider just a left most column of each circulant block for the current symbol node being determined. This makes the algorithm work in efficiency on the order of circulant size. The algorithm produces each circulant block with weight 0, 1, and 2. We put a constraint on the weight-2 circulants that they should form a residue/non-residue pair. Once an appropriate circulant block is chosen, and the lowest edge has been determined, we make a full circulant matrix by shifting a non-zero element corresponding to the lowest edge determined in the left most column of the block.
We then set the current graph by considering all the edges contained in the currently constructed circulant block. All this procedures are summarized in Fig. ??.

**Example 3.4** In this example we design a rate-1/2 irregular QC-LDPC code consists of $12 \times 24$ circulant blocks. We set the order of circulant size to 43 and thus the frame length of this code is 1032. A code of these parameters generated by the proposed block-PEG algorithm is shown as following matrix. We compare the performance of this code with that of Samsung’s BLDPC code [15]. Parity check matrices of both codes are shown in Fig. 3.10(a) and 3.10(b). Here $\pm a$ denotes $h(x) = x^a + x^{-a}$.

\[
\begin{bmatrix}
-11 & 0 & -20 & 18 & 19 & 0 & \pm6 \\
7 & 0 & 5 & 1 & 20 & -16 & \pm9 \\
-17 & 9 & 3 & 17 & 8 & -11 & -19 \\
7 & -5 & -16 & -20 & 16 & -17 & 11 \\
-7 & 5 & -6 & -17 & -15 & -4 & 0 \\
-18 & 21 & 13 & 20 & -6 & 3 & 14 \\
-6 & 19 & 4 & -16 & -20 & 21 & \pm4 \\
-20 & -3 & 20 & 0 & 11 & -15 & 17 \\
2 & -17 & -12 & -2 & -16 & -16 & 13 \\
10 & -15 & 1 & -9 & -1 & \pm5 & 18 \\
-14 & 18 & 4 & 15 & 14 & \pm2 & 10 \\
-19 & -9 & -8 & 14 & & \pm17 & 4 \\
\end{bmatrix}
\]

**Example 3.5** A rate-2/3 irregular QC-LDPC code consists of $12 \times 36$ circulant blocks is constructed by the proposed algorithm. We set the order of circulant size to 29 and thus the frame length of this code is 1044. We compare the performance of this code with that of Samsung’s BLDPC code [15].
(a) A rate-1/2 QC-LDPC code in Example 3.4

(b) A rate-1/2 B-LDPC code with frame length 1032 [15].

Figure 3.10: Parity-check matrices of rate-1/2 irregular QC-LDPC codes.
Figure 3.11: BER/FER simulation results of irregular QC-LDPC codes.
3.5 Remarks

We have proposed design of QC-LDPC codes using residue number system (residues/non-residues). The proposed codes are linear time encodable since we can use polynomial multiplication instead of matrix multiplication. In addition, algebraic structure of the QC-LDPC codes admits wide range of code rates and block lengths by applying conventional modification schemes, e.g. shortening and lengthening, of linear block codes. This new QC-LDPC codes from residue number system have advantages over other schemes that they admit a structure that does not excessively increase the number of short cycles while they give benefits to construct higher degree bit nodes with improved performance. For the regular codes we proposed algebraically describable QC codes using residue number systems. For the irregular constructions, we suggest a block progressive edge growth (block-PEG) algorithm by modifying the original PEG algorithm. We have constructed block-wise irregular QC-LDPC codes using this algorithm and compared the performance of the codes with that of other codes with similar structure.
Chapter 4

Irregular Concatenated LDGM Codes by LLR Analysis

During past 10 years research concentration on codes on graphs and message-passing decoding algorithm has been focused on capacity-achieving error-correcting codes such as low-density parity check (LDPC) codes and the Turbo codes. However in practical applications, both coding schemes reveal either high encoding complexity or decoding complexity problems. As an alternative coding scheme without complexity issues, low-density generator matrix (LDGM) codes are recently investigated by [20] [21]. Though LDGM codes are very efficiently encodable and decodable, performance of an LDGM code is asymptotically bad as mentioned in [3]. LDGM codes are sparse systematic linear codes and thus the presence of degree-1 bit nodes and the poor distance properties cause error floors during message passing decoding process.

To control the error floor of LDGM codes, Garcia-Frias proposed concatenation of very high rate outer LDGM code with properly chosen inner LDGM code and showed this coding scheme approaches Shannon performance [20]. However in the application of moderate length of codes, higher rate outer codes inevitably contain lots of short
cycles resulting performance degradation. Henceforth we have to lower the code rate of outer codes in such cases. The problem here is that increased portion of degree 1-bit nodes in outer code will again causes error floors during message-passing decoding process due to their low log-likelihood ratio (LLR) values.

In this chapter we present improved irregular concatenated LDGM codes by increasing the reliability of degree-1 bit nodes using analysis on the LLRs of inner code and outer code.

4.1 Low-Density Generator Codes

Low-density generator (LDG) codes are defined by a bipartite graph \( B = (X \cup C, E) \) consists of set of information nodes \( X \) and set of parity check nodes \( C \). The values of parity check nodes in \( C \) are defined by those in \( X \) and the set of edges \( E \). The \( k \times n \) generator matrix of a LDG code has systematic form of \( G = [I_k|P] \), where \( P \) is a \( k \times r \) sparse matrix with \( r = n - k \). The corresponding adjacency matrix of \( B \) has the form

\[
\begin{bmatrix}
0 & P \\
P^T & 0
\end{bmatrix}.
\]

Let the information message vector be \( \mathbf{m} = [m_0, m_1, \ldots, m_{k-1}] \) and \( r \)-redundant parity bits be \( c_0, c_1, \ldots, c_{r-1} \), then the encoding process is as follows.

\[
\mathbf{c} = \mathbf{m}G = [m_0, m_1, \ldots, m_{k-1}] [I_k|P] = [m_0, m_1, \ldots, m_{k-1} | c_0, c_1, \ldots, c_{r-1}]
\]

Given a systematic generator matrix of the form as above, a corresponding parity check matrix can be expressed as \( H = [P^T|I_r] \). Note that the parity-check matrix of LDG
code is still sparse, and thus LDG codes can be decoded with the same algorithm as that of general LDPC codes. Fig. 4.1 shows an example of generator matrix, parity-check matrix and the corresponding bipartite graph.

If a graph has every information node with degree X and every parity check node with degree Y then we call the corresponding code as a regular (X,Y)-LDGM code. We
denote the degree distribution sequence pair of (X,Y)-LDGM code as \( \lambda(x) = x^{X-1} \) and \( \rho(x) = x^{Y-1} \). It is known that the LDGM codes are asymptotically bad, since the existence of degree-1 bit nodes corresponding to the parity bit nodes causes error floors during message-passing decoding process.

To reduce the error floors due to degree-1 bit nodes, Garcia-Frias proposed proper concatenation of two regular LDGM codes [20]. Fig. 4.2 shows a general graph representation of concatenated LDGM codes. He gave an example of a rate-1/2 regular (6,6) inner LDGM code concatenated with very high rate regular outer code, e.g. a rate-19/20 (3,57) outer code. Note in this example degree-1 bit nodes in the outer code still suffers from low LLRs but since the portion of degree-1 nodes is sufficiently small their effects on the overall performance is negligible.

### 4.2 Irregular Concatenated LDGM Codes by LLR analysis

In some practical applications, one need to design a moderate length \( 10^3 < n < 10^4 \) of codes, however in such cases higher rate outer codes will inevitably contain lots of short cycles. For example, to randomly make a rate-19/20 outer code without 4-cycles, the block length of the outer code would be greater than 6800 in terms of girth bound presented in [17]. Further if we concatenate a rate-1/2 inner code with such outer code the overall block length of the concatenated code would be greater than 13600. Since increased short cycles deteriorate the performance of codes on graph, one need to reduce the outer code rate to avoid short cycles. The problem here is that as the outer code rate reduces the portion of degree-1 bit nodes increases and consequently the insufficient LLRs in such nodes will deteriorate overall performance of concatenated coded system.
Figure 4.2: Graph representation of concatenated LDGM codes.
To solve this problem we consider irregular design of LDGM codes. The idea is that we adopt higher degree nodes in the inner code corresponding to the degree-1 bit nodes of the outer code. Then the higher bit degrees in the inner code will produce increased LLRs during message-passing decoding process, and since outer code initializes the messages produced by the inner code, the degree-1 bit nodes of the outer code with increased reliability will not any more be a dominant factor for performance degradation. Fig. 4.3 shows examples of parity-check matrices for regular and irregular concatenated LDGM codes respectively. The maximum left degree of inner code is empirically chosen to compensate the LLR loss corresponding to degree-1 nodes in the outer code. Other bit degrees are determined by adjusting the average right degrees of inner code and to make the overall average LLR values of the outer code equalized as possible. Fig. 4.4 shows examples of average LLRs of overall coding system measured in the bit (or left) nodes of regular and irregular outer code.

4.3 Simulation Results

In this section we provide two examples of irregular concatenated LDGM codes comparing with other coding schemes.

Example 4.1 (Rate-9/20 concatenated LDGM codes) The first example is a rate-1/2 irregular inner LDGM code with frame length 1580 concatenated with a rate-9/10 irregular outer LDGM code with frame length 790. For this parameter, we first determine the degree distribution sequences using LLR analysis. Left(bit) degree distribution sequence
(a) Parity check matrices of regular LDGM codes

(b) Parity check matrices of irregular LDGM codes

Figure 4.3: Parity check matrices of concatenated LDGM codes.
Figure 4.4: Average LLRs of concatenated LDGM codes.
for inner code and outer code is determined as

$$\lambda_{\text{inner}}(x) = 0.526316 x^4 + 0.315789 x^5 + 0.157895 x^8,$$

$$\lambda_{\text{outer}}(x) = 0.272727 x^2 + 0.727273 x^3.$$  

To generate specific LDGM codes corresponding to above degree distribution sequences, we used progressive edge growth (PEG) algorithm in [17]. The parity check matrices of inner code and outer code are shown in Fig. 4.3 compared with regular concatenated LDGM codes with same frame structure. For the regular concatenated code, we used a rate-1/2 (6,6) inner LDGM code with a rate-9/10 (3, 27) outer LDGM code. Fig. 4.5(a) shows simulation results of both coding schemes over AWGN channel. We applied maximum iteration number 50 to the inner code and 20 to the outer code. We compare the performance of the proposed code with that of regular concatenated LDGM codes. Simulation results show that the proposed scheme has meaningful coding gain over the regular codes.

**Example 4.2** [Rate-15/32 concatenated LDGM codes] In this example we consider concatenated LDGM codes composed of a rate-1/2 inner code with frame length 4096 and a rate-15/16 outer code with frame length 2048. Degree distribution sequence for inner code is chosen as

$$\lambda_{\text{inner}}(x) = 0.260417 x^4 + 0.625 x^5 + 0.114583 x^10,$$

$$\lambda_{\text{outer}}(x) = 0.6 x^2 + 0.4 x^3.$$  

For comparison, we used a rate-1/2 (6,6) inner LDGM code with a rate-15/16 (3, 45)
outer LDGM code. Fig. 4.5(b) shows simulation results of proposed irregular concatenated LDGM codes compared with regular ones.

4.4 Remarks

Design of irregular concatenated LDGM codes using LLR analysis has been proposed. Proposed coding scheme is useful for the concatenated LDGM codes of moderate block length where higher rate outer code seems to be difficult to apply due to short cycle problems. However as shown in Example 4.2 the higher the code rate of outer code becomes, attainable coding gain over regular concatenated system decreases. This is because degree-1 parts of outer code becomes relatively small and thus the poor reliability of degree-1 bit nodes does not affect the overall performance of the concatenated coding system. For future work, it is desirable to find and analyze the proper coding scheme applicable to higher-rate outer coded concatenated system.
(a) Performance of a rate-9/20 concatenated LDGM codes

(b) Performance of a rate-15/32 concatenated LDGM codes

Figure 4.5: BER/FER simulation results of concatenated LDGM codes.
Chapter 5

Generalization of Tanner’s Minimum Distance Bounds for LDPC Codes

LDPC codes with iterative decoding were first invented by Gallager in 1962 and recently much attention has been paid since they have been rediscovered to perform very close to the theoretical limit [1], [3], [4], [6]. Especially Luby et al. [4] introduced irregular LDPC codes with improved performances and Richardson et al. [5] presented near capacity achieving irregular LDPC codes by introducing density evolution technique which analyzes the asymptotic performance of the codes.

However, relatively few papers have been presented on the distance property of the LDPC codes. Tanner [7] derived minimum distance bounds on the regular LDPC codes in terms of the eigenvalues of the associated graph by using the relationship between nodes on the graph and a minimum-weight codeword.

In this chapter we generalize the Tanner’s results. We derive a bit-oriented bound and a parity-oriented bound on the minimum distance of both regular and block-wise
irregular LDPC codes. We present some examples of codes and discuss the usefulness of the bounds.

5.1 Tanner’s Minimum Distance Bounds

An LDPC code with an \(m \times n\) parity check matrix \(H\) can be thought of as a bipartite graph with \(m\) check nodes and \(n\) bit nodes [7]. A bipartite graph is \(B = (V_b \cup V_c, E)\), where \(V_b = \{b_1, b_2, \ldots, b_n\}\), \(V_c = \{c_1, c_2, \ldots, c_m\}\) and the edge set \(E\) consists of edge \((c_i, b_j)\) in \(V_c \times V_b\) corresponds to nonzero \(h_{ij}\) in \(H\) [22]. The connectivity of the graph is described by an \((m + n) \times (m + n)\) real-valued adjacency matrix with entry \(a_{ij} = 1\) if and only if the \(i\)th node is connected by an edge to the \(j\)th node [22]. Thus with an appropriate labelling of the nodes, \(A\) has the form

\[
A = \begin{bmatrix}
0 & H \\
H^T & 0
\end{bmatrix}.
\]

It follows from the following Lemma that the nonzero eigenvalues of \(H^T H\) and \(H H^T\) are the same [22].

**Lemma 5.1** Let \(M\) be an real matrix. If \(e\) is an eigenvector of \(M^T M\) with nonzero eigenvalue \(\lambda\), then \(e' = Me\) is an eigenvector of \(MM^T\) with the same eigenvalue \(\lambda\).

The following Lemma indicates the relationship between the eigenvalues of the adjacency matrix \(A\) and the nonzero eigenvalues of \(H H^T\) [22].

**Lemma 5.2** Let \(A\) be the adjacency matrix of a connected bipartite graph. The eigenvalues of \(A\) are \(\pm \sqrt{\mu_i}\) or 0, where \(\mu_i, 1 \leq i \leq s\) are the distinct eigenvalues of \(H H^T\).
Proof: Let $e = [e_p^T, e_b^T]^T$ be any nonzero eigenvector of $A$ with eigenvalue $\lambda$. Then

$$\lambda^2 e_p = H H^T e_p$$

and

$$\lambda^2 e_b = H^T H e_b.$$ 

Thus either $\lambda^2 = 0$ or $\lambda^2 = \mu_i$ for some $i$, and the result follows. ■

In terms of matrix terminology the connectedness of the graph is equivalent to the irreducibility of the adjacent matrix.

**Definition 5.1** A symmetric matrix $M$ is called reducible, if there exists a permutation matrix $P$ such that $P^{-1}MP$ has the block-diagonal form

$$
\begin{bmatrix}
M_1 & 0 \\
0 & M_2
\end{bmatrix},
$$

where $M_1$ and $M_2$ are symmetric matrices. Otherwise $M$ is called irreducible.

Tanner [7] derived minimum distance bounds by analyzing the properties of the sub-graph of $B$ related to a minimum-weight word. He defined active bit nodes as bit nodes corresponding to non-zeros in a minimum-weight word, active edges as the edges incident on active bit nodes, and active check nodes as the check nodes with at least one active incident edge. Fig.5.1 shows an example of regular LDPC code with length 9, fixed column weight 2 and fixed row weight 3. Active bit nodes and active check nodes are shown corresponding to a minimum-weight word (110101000).

Tanner presented the following bounds on the minimum distance $d$ of a code with an $m \times n$ regular parity check matrix $H$ with connected associated graph. Let $\gamma$ be the fixed column weight and $\rho$ be the fixed row weight of $H$ and $\mu_1, \mu_2$ be the largest and the second largest eigenvalues of $HH^T$ respectively. Then we have the *bit-oriented*
bound [7, Theorem 3.1]
\[ d \geq \frac{n(2\gamma - \mu_2)}{\mu_1 - \mu_2}, \]
and the parity-oriented bound [7, Theorem 4.1]
\[ d \geq \frac{2n(2\gamma + \rho - 2 - \mu_2)}{\rho(\mu_1 - \mu_2)}. \]

Using these bounds, Tanner set up a heuristic rule that a code with a smaller ratio of second to first eigenvalues will have a good distance property [7].

5.2 Generalization of the bounds

Tanner’s bounds are applicable only to regular LDPC codes. In this section we generalize Tanner’s results. To prove the main theorem we need the following lemma.

Lemma 5.3 Let \( H \) be a parity-check matrix of a bipartite graph \( B \), then the graph \( B \) is connected if and only if \( HH^T \) is irreducible.

Proof: If the graph is not connected then after some ordering of the nodes, the parity-check matrix \( H \) reduces to the form
\[
\begin{bmatrix}
H_1 & 0 \\
0 & H_2
\end{bmatrix}.
\]
(5.1)
Then it is easy to check the resulting \( HH^T \) is reducible. Second, if \( HH^T \) is reducible \( H \) should be in the form of (5.1) since \( H \) is non-negative binary matrix.

It follows from the Perron-Frobenius theory of matrices that if a graph \( G \) is connected, then its largest eigenvalue is a simple eigenvalue. A complete proof may be found in [23]. Here we present simplified proof of the Perron-Frobenius theorem for non-negative symmetric matrices.
Figure 5.1: Parity-check matrix and the associated bipartite graph.
**Theorem 5.1** Let $M$ be an $n \times n$ irreducible symmetric matrix with elements $m_{ij} \geq 0$, $\lambda$ be the largest eigenvalue. Then there exists a corresponding eigenvector $e$ with every entry $e_i > 0$ and this eigenvector is unique.

**Proof:** Let $v$ be any real normalized eigenvector corresponding to $\lambda$ then
\[ \lambda v_i = \sum_{j=0}^{n-1} m_{ij} v_j, \quad i = 0, 1, \ldots, n - 1. \] (5.2)

Set $e_i = |v_i|$ then
\[ \lambda = \sum_{i,j=0}^{n-1} m_{ij} v_i v_j \leq \sum_{i,j=0}^{n-1} m_{ij} e_i e_j. \] (5.3)

Since $\lambda$ is assumed to be the largest eigenvalue the right-hand side is less than or equal to $\lambda$ with equality if and only if $e$ is an eigenvector belonging to $\lambda$. If $e_i = 0$ for some $i$ then by permutation of coordinates we can write
\[
\begin{cases}
    e_i > 0, & \text{for } i = 0, 1, \ldots, m - 1, \\
    e_i = 0, & \text{for } i \geq m.
\end{cases}
\] (5.4)

It follows from above that
\[ \sum_{j=0}^{m-1} m_{ij} e_j = 0 \text{ if } i \geq m. \] (5.5)

Therefore we have $m_{ij} = 0$ for $i \geq m > j$ and $M$ is reducible. This proves the existence of positive-definite eigenvector $e$ corresponding to the largest eigenvalue $\lambda$.

Now if there exists two real orthonomal eigenvectors $u$ and $v$ corresponding to $\lambda$. From (5.2), (5.3) we write $\lambda(u_i + |u_i|) = \sum_{j=0}^{n-1} m_{ij}(u_i + |u_i|)$, which implies either $u_i + |u_i| = 0$ for all $i$ or $u_i + |u_i| > 0$ for all $i$. The same applies to $v$ and thus $u$ and $v$ cannot be orthogonal.

The bit-oriented bound is derived by considering the relationship between bit nodes in a minimum-weight word.
Theorem 5.2 (Bit-oriented bound) Let $\mu_1 > \mu_2 > \cdots > \mu_s$ be the ordered distinct eigenvalues of real valued matrix $H^T H$, where the parity check matrix $H$ of a linear block code is in the form of $H = [H_1, H_2, \ldots, H_p]$. We assume that the associated graph of the code is connected. Let each $H_i$, $(1 \leq i \leq p)$ be an $m \times l$ matrix with fixed column weight $\gamma_i$ and fixed row weight $\rho_i$ with the assumption $\gamma_1 \leq \gamma_2 \leq \cdots \leq \gamma_p$.

Then the minimum distance $d$ of the code satisfies

$$d \geq (2\gamma_1 - \mu_2) l \sum_{i=1}^{p} \frac{\gamma_i^2}{\gamma_p^2 (\sum_{i=1}^{p} \gamma_i \rho_i - \mu_2)}.$$  

Proof: Let $c$ be a real-valued vector of length-$pl$ corresponding to a minimum-weight codeword with ones in every nonzero positions and zeros elsewhere. The first eigenvector of $H^T H$ can be taken to be $e_1 = (\gamma_1, \ldots, \gamma_1, \gamma_2, \ldots, \gamma_2, \ldots, \gamma_p, \ldots, \gamma_p)^T / \sqrt{l \sum_{i=1}^{p} \gamma_i^2}$ with the corresponding eigenvalue $\mu_1 = \sum_{i=1}^{p} \gamma_i \rho_i$. Lemma 5.3 and theorem 5.1 provides that this eigenvalue is unique since the graph is assumed to be connected. Let $d_i$ be the number of nonzeros of $c$ in each $l$-portion corresponding to $H_i$, and let $c_i$ be the projection of $c$ onto the $i$th eigenspace. Clearly

$$c^T c = \|c\|^2 = d, \quad (5.6)$$

$$\|c_1\|^2 = \frac{(\sum_{i=1}^{p} d_i \gamma_i)^2}{l \sum_{i=1}^{p} \gamma_i^2} \leq \frac{d^2 \gamma_p^2}{l \sum_{i=1}^{p} \gamma_i^2}. \quad (5.7)$$

Let $x_i$ be the weight on the $i$th check defined by $Hc$. Since each nonzero $x_i$ must be even and at least two, we have

$$\|Hc\|^2 = \sum_{i=1}^{m} x_i^2 \geq 2 \sum_{i=1}^{m} x_i = 2 \sum_{i=1}^{p} d_i \gamma_i \geq 2 \gamma_1 d. \quad (5.8)$$

53
Using the eigenspace representation we get
\[ \| Hc \|^2 = \sum_{i=1}^{s} \mu_i \| c_i \|^2 \leq (\mu_1 - \mu_2) \| c_1 \|^2 + \mu_2 \| c \|^2. \] (5.9)

Then substituting (5.6), (5.7), (5.8) into (5.9) gives the desired bound for \( d \).

The second bound considers the connectivity between parity nodes adjacent to any nonzero bit in a minimum-weight word.

**Theorem 5.3 (Parity-oriented bound)** Let \( \mu_1 > \mu_2 > \cdots > \mu_s \) be the ordered distinct eigenvalues of real valued matrix \( HH^T \), where the parity check matrix \( H \) of a linear block code is in the form of \( H = [H_1, H_2, \ldots, H_p] \). We assume that the associated graph of the code is connected. Let each \( H_i, (1 \leq i \leq p) \) be an \( m \times l \) matrix with fixed column weight \( \gamma_i \) and fixed row weight \( \rho_i \) with the assumption \( \gamma_1 \leq \gamma_2 \leq \cdots \leq \gamma_p \).

Then the minimum distance \( d \) of the code satisfies
\[ d \geq \frac{2m(2\gamma_1 + \sum_{i=1}^{p} \rho_i - 2 - \mu_2)}{\gamma_p(\sum_{i=1}^{p} \gamma_i \rho_i - \mu_2)}. \]

**Proof:** Let \( p \) be a length-\( m \) real-valued vector that has a 1 in every active check node position and 0 elsewhere, and let \( p_i \) be the projection of \( p \) onto the \( i \)th eigenspace of \( HH^T \). The first eigenvector can be taken to be \( e_1 = (1, 1, \ldots, 1)^T / \sqrt{m} \) with \( \mu_1 = \sum_{i=1}^{p} \gamma_i \rho_i \). Lemma 5.3 and theorem 5.1 provides that this eigenvalue is unique since the graph is assumed to be connected. If \( \eta \) is the number of 1’s in \( p \), then \( p^T p = \| p \|^2 = \eta \) and \( \| p_1 \|^2 = \eta^2 / m. \) Observe that \( H^T p \) assigns an integer weight distribution to bit nodes in \( H \). Let \( y_i \) be the weight on the \( i \)th bit node so that
\[ \| H^T p \|^2 = \sum_{i=1}^{p} y_i^2. \] (5.10)
Each active check node is adjacent to an even number of nonzero bit nodes. For the $j$th active check node, let $u_j(w)$ be the number of adjacent nodes with weight $w$ in $H^T p$, $0 \leq w \leq \gamma_p$. The squared weight counted at the $j$th active check node is

$$
\sum_{w=1}^{\gamma_p} (1/w) u_j(w) w^2 \geq 2\gamma_1 + \sum_{i=1}^{p} \rho_i - 2.
$$

(5.11)

Then since there are $\eta$ active check nodes,

$$
\sum_{i=1}^{\eta} y_i^2 \geq \eta(2\gamma_1 + \sum_{i=1}^{p} \rho_i - 2).
$$

(5.12)

Using eigenspace representation we get

$$
\|H^T p\|^2 = \sum_{i=1}^{s} \mu_i \|p_i\|^2 \leq (\mu_1 - \mu_2)\|p_1\|^2 + \mu_2\|p\|^2.
$$

(5.13)

Substituting from above gives

$$
\eta \geq m(2\gamma_1 + \sum_{i=1}^{p} \rho_i - 2 - \mu_2)/(\mu_1 - \mu_2)
$$

(5.14)

and $\eta \gamma_p \geq 2\eta$ gives the desired bound.

\[\blacksquare\]

**Corollary 5.3** Tanner’s bounds are obtained by setting $p = 1$ or by setting $\gamma_1 = \gamma_2 = \cdots = \gamma_p$ and $\rho_1 = \rho_2 = \cdots = \rho_p$ in Theorems 1 and 2.

### 5.3 Code Construction Examples

To illustrate the use of the theorems, we calculate the bounds of the code in Fig.5.1 and present examples of quasi-cyclic LDPC (QC-LDPC) codes. The parity check matrix of a quasi-cyclic code is in the form of a block matrix consists of $m \times m$ circulant matrices.
as blocks, where \( m \) is the order of circulant matrix. Each circulant matrix \( H_{ij} \) in \( H \) is completely described by the associated polynomial \( h_{ij}(x) \) corresponding to the top row of \( H_{ij} \) \cite{8, 24, 25}. More precisely, we have

\[
h_{ij}(x) = \sum_{k=0}^{m-1} (H_{ij})_{0k} x^k.
\]  \( 5.15 \)

We call the number of nonzero coefficients of the polynomial the weight of the polynomial.

**Example 5.1** The code in Fig. 5.1 is a rate-4/9 [9,2,3]-regular LDPC code with \( \mu_1 = 6 \) and \( \mu_2 = 3 \). Note that non-zero eigenvalues of \( H^T H \) and \( HH^T \) are the same \cite{7, 22}. Hence the bit-oriented bound gives \( d \geq 3 \) and the parity-oriented bound gives \( d \geq 4 \). The actual minimum distance found through an exhaustive search is 4. Thus the parity-oriented bound gives the true minimum distance.

**Example 5.2** Let \( H = [H_1, H_2] \) with \( h_1(x) = 1+x+x^8, h_2(x) = 1+x^2+x^6+x^{16} \) and \( m = 19 \). Then \( \mu_1 = 25 \) and \( \mu_2 = 6 \). In this example the bound from Theorem 1 becomes zero since \( \mu_2 = 2 \gamma_1 \), whereas the bound from Theorem 2 gives \( d \geq 2.5 \). The actual minimum distance found through an exhaustive search is 7. One of the worst connected graphs with these code parameters is \( H = [H_1, H_2] \) with \( h_1(x) = 1+x^5+x^{12}, h_2(x) = 1+x^2+x^7+x^{14} \). This code has \( \mu_1 = 25 \) and \( \mu_2 = 22.29 \) with the true minimum distance 4. The complete weight distributions of the codes in this example are listed in Table 5.1.
Table 5.1: Weight enumeration of LDPC codes in Example 5.2

<table>
<thead>
<tr>
<th>Weight</th>
<th>Multiplicity</th>
<th>Weight</th>
<th>Multiplicity</th>
<th>Weight</th>
<th>Multiplicity</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>19</td>
<td>70016</td>
</tr>
<tr>
<td>7</td>
<td>38</td>
<td>4</td>
<td>19</td>
<td>20</td>
<td>66443</td>
</tr>
<tr>
<td>8</td>
<td>190</td>
<td>6</td>
<td>38</td>
<td>21</td>
<td>56962</td>
</tr>
<tr>
<td>11</td>
<td>4636</td>
<td>7</td>
<td>95</td>
<td>22</td>
<td>41230</td>
</tr>
<tr>
<td>12</td>
<td>10260</td>
<td>8</td>
<td>266</td>
<td>23</td>
<td>27227</td>
</tr>
<tr>
<td>15</td>
<td>58938</td>
<td>9</td>
<td>399</td>
<td>24</td>
<td>16682</td>
</tr>
<tr>
<td>16</td>
<td>85044</td>
<td>10</td>
<td>1045</td>
<td>25</td>
<td>9405</td>
</tr>
<tr>
<td>19</td>
<td>134920</td>
<td>11</td>
<td>2774</td>
<td>26</td>
<td>5453</td>
</tr>
<tr>
<td>20</td>
<td>127832</td>
<td>12</td>
<td>4826</td>
<td>27</td>
<td>2546</td>
</tr>
<tr>
<td>23</td>
<td>58938</td>
<td>13</td>
<td>9823</td>
<td>28</td>
<td>1216</td>
</tr>
<tr>
<td>24</td>
<td>37050</td>
<td>14</td>
<td>17670</td>
<td>29</td>
<td>551</td>
</tr>
<tr>
<td>27</td>
<td>4636</td>
<td>15</td>
<td>28044</td>
<td>30</td>
<td>190</td>
</tr>
<tr>
<td>28</td>
<td>1748</td>
<td>16</td>
<td>41344</td>
<td>31</td>
<td>114</td>
</tr>
<tr>
<td>31</td>
<td>38</td>
<td>17</td>
<td>54169</td>
<td>32</td>
<td>19</td>
</tr>
<tr>
<td>32</td>
<td>19</td>
<td>18</td>
<td>65702</td>
<td>33</td>
<td>19</td>
</tr>
</tbody>
</table>
Example 5.3 Consider QC-LDPC codes with $H = [H_1, H_2, H_3]$ with $m = 64$. Let the weights of the associated polynomials are 3, 3, and 4 respectively. Then the largest eigenvalue is $\mu_1 = 34$. With this structure one of the best codes with girth 6 in terms of the theorems is $h_1(x) = 1 + x^5 + x^{56}, h_2(x) = 1 + x^{16} + x^{47}$ and $h_3(x) = 1 + x^2 + x^{30} + x^{57}$. The second largest eigenvalue of this code is $\mu_2 = 13.67$. Whereas one of the worst codes without 4-cycle is $h_1(x) = 1 + x + x^{18}, h_2(x) = 1 + x^{12} + x^{36}$ and $h_3(x) = 1 + x^5 + x^{11} + x^{34}$ with $\mu_2 = 28.19$.

Figure 5.2: BER performance of QC-LDPC codes compared with that of randomly constructed ones.
Example 5.4 In this example we construct rate-3/4 QC-LDPC codes from a (217,7,1) cyclic difference family. A (217, 7, 1) difference family has five base blocks as base blocks as follows [26]:

\[ B_1 = \{0, 1, 37, 67, 88, 92, 149\}, \]
\[ B_2 = \{0, 15, 18, 65, 78, 121, 137\}, \]
\[ B_3 = \{0, 8, 53, 79, 85, 102, 107\}, \]
\[ B_4 = \{0, 11, 86, 100, 120, 144, 190\}, \]
\[ B_5 = \{0, 29, 64, 165, 198, 205, 207\}. \] (5.16)

Using this difference family we design rate 3/4 QC-LDPC codes. We first construct regular QC-LDPC codes applying the Taner’s simple bounds. For a design of irregular QC-LDPC codes, the main problem is to select the required circulant matrices. That is, we must choose nonzero coefficients of each polynomial \( h_i(x) \) from the base blocks which could lead to seemingly the best QC-code. The first step to solve this problem is deciding an appropriate weight distribution of the polynomials. This corresponds to deciding a degree distribution pair of the code. One strategy would be to use density evolution technique [5]. In this case we optimize degree distribution for AWGN channel and find a distribution pair \( \lambda(x) := 0.1333x + 0.400x^2 + 0.4667x^6 \) and \( \rho(x) := x^{14} \) which has an approximate threshold \( \sigma^* = 0.6462 \). Once the degree distribution is determined the largest eigenvalue is fixed to be \( \mu_1 = \sum_{i=1}^{t} \gamma_i^2 \), and the remaining step is to find a code from every possible candidates which minimizes the second largest eigenvalue.

Example 5.5 In this example, we construct rate 2/3 QC-LDPC codes of length 501 whose parity check matrix consists of three circulant matrices of length 167. We first
find an optimized weight distribution pair \( \lambda(x) := 0.18182x + 0.27273x^2 + 0.54545x^5 \)

and \( \rho(x) := x^{10} \) which has an approximate threshold \( \sigma^* = 0.722465 \). We consider all the possible candidates \( h_i(x) \) to directly construct a code using an exhaustive search. Some combinatorial symmetric properties and 4-cycle free condition are used to reduce the search complexity. The remaining step is similar to the previous example.

Table 5.2. presents search results of QC-LDPC code examples described in subsection A and B. For the random LDPC code in the Table 5.2, we used Mackay’s construction and we also presented the number of 6-cycles of each code. In case of regular QC-LDPC codes the best case is when a ratio \( \mu_1/\mu_2 \) is 0.5469 and this code outperforms the worst one about 0.4dB at BER \( 10^{-3} \) as shown in . Interestingly codes that have smaller eigenvalue ratio have smaller number of short cycles as shown in the Table 5.2. We obtain similar results in case of irregular QC-LDPC codes.

### 5.4 Remarks

The derived bounds have weak points due to some approximations used in the derivation. First if there are parity check equations in the minimum-weight word satisfied by four or more nonzero bits in the code, the inequality (5.8) will not be tight. Second, replacing all the smaller eigenvalues by \( \mu_2 \) results in the loss of tightness. Third, replacing all the other weights into the maximum(or minimum) weight in (5.7), (5.8), (5.11) does the same. We observe that the bit-oriented bound becomes trivial as \( p \) increases both in regular and irregular cases, whereas the parity-oriented bound becomes meaningful for larger column and row weights.
Table 5.2: Search Results of Optimized QC-LDPC Codes

<table>
<thead>
<tr>
<th>Code Description</th>
<th>Eigen-value ratio</th>
<th>Number of 6-cycles</th>
</tr>
</thead>
<tbody>
<tr>
<td>[868,3,12] Random LDPC code</td>
<td>0.5926</td>
<td>1,792</td>
</tr>
<tr>
<td>$h_1(x) = x^{78} + x^{121} + x^{137}$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$h_2(x) = 1 + x^8 + x^{107}$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$h_3(x) = 1 + x^{11} + x^{86}$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$h_4(x) = x^{29} + x^{64} + x^{198}$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rate 3/4 regular QC-LDPC from CDF</td>
<td>0.9543 (max.)</td>
<td>6,727</td>
</tr>
<tr>
<td>$h_1(x) = 1 + x^{121} + x^{137}$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$h_2(x) = 1 + x^{8} + x^{79} + x^{85}$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$h_3(x) = 1 + x^{11} + x^{100}$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$h_4(x) = x^{29} + x^{165} + x^{207}$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rate 3/4 irregular QC-LDPC from CDF</td>
<td>0.5469 (min.)</td>
<td>1,085</td>
</tr>
<tr>
<td>$h_1(x) = x^{67} + x^{88}$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$h_2(x) = x^{18} + x^{78} + x^{121}$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$h_3(x) = 1 + x^{11} + x^{144}$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$h_4(x) = x^{B_5a}$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rate 2/3 irregular QC-LDPC</td>
<td>0.3830 (min.)</td>
<td>23,002</td>
</tr>
<tr>
<td>$h_1(x) = 1 + x^{149}$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$h_2(x) = 1 + x^{18} + x^{137}$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$h_3(x) = 1 + x^{144} + x^{190}$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$h_4(x) = x^{B_5a}$</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

$^{a}x^{B_5}$ comes from (5.16)
Figure 5.3: BER performance comparison of QC-LDPC codes.
The bounds, though might not be tight sometimes, still give a heuristic indicator for the distance property of an associated code. For an example, the weight enumerator of the first code in Example 5.2 is \( A(z) = 1 + 38z^7 + 190z^8 + 4636z^{11} + \cdots \), while \( A(z) = 1 + 19z^4 + 38z^6 + 95z^7 + 266z^8 + \cdots \) for the second one. Empirical results indicate the bounds give a heuristic rule that a code with a smaller ratio of second to first eigenvalue would have a good distance property as expected by Tanner in his analysis on the case of regular LDPC codes. This rule is also in accord with other criteria related to expander graphs [27]. Simulation results show that the derived bounds work well as a design criterion for the construction of irregular LDPC codes.
Chapter 6

Concluding Remarks

6.1 Summary

In this dissertation, we have proposed construction methods for efficiently encodable low-density codes and derived minimum distance bounds of codes on graphs. In chapter 2, we have reviewed some basic properties of circulant matrices and design criteria for the construction of LDPC codes. Subsequently, we have summarized the existing construction methods so far.

One major drawback of LDPC codes is their high encoding complexity. Encoding is, in general, performed by matrix multiplication and so complexity is quadratic in the block length. In chapter 3, we have considered design of QC-LDPC codes using residue number system (residues/non-residues). The proposed codes are linear time encodable since we can use polynomial multiplication instead of matrix multiplication. In addition, algebraic structure of the QC-LDPC codes admits wide range of code rates and block lengths by applying conventional modification schemes, e.g. shortening and lengthening, of linear block codes. Previous published constructions of QC-LDPC codes have mostly regular structure consists of weight-1 circulants, while we considered QC-codes from
residue number system consist of weight 0, 1, and 2 circulant blocks. This new QC-LDPC codes from residue number system have advantages over other schemes that they admit a structure that does not excessively increase the number of short cycles while they give benefits to construct higher degree bit nodes with improved performance. For the regular codes we proposed algebraically describable QC codes using residue number systems. For the irregular constructions, we suggest a block progressive edge growth (block-PEG) algorithm by modifying the original PEG algorithm. We have constructed block-wise irregular QC-LDPC codes using this algorithm and compared the performance of the codes with that of other codes with similar structure.

We have investigated another class of linear codes with iterative decoding algorithm called LDGM codes that have extremely efficient encoder structure. LDGM codes are relatively new research topic and recently it has been shown that this coding scheme approaches the Shannon limit by concatenation of two systematic regular LDGM codes. We observed one weak point of this coding scheme is the presence of the degree-1 bit nodes correspond to the parity parts of the LDGM codes which deteriorates the overall performance during the message-passing decoding process. Henceforth we proposed an irregular concatenated LDGM code scheme that improves the reliability of degree-1 bit nodes. Proposed construction method increases the reliability of degree-1 node by increasing the density of bit degrees of the inner code correspond to the degree-1 parts of outer code. To this end we analyzed the LLR messages of the bit nodes and make them equalized over all bit nodes by conditioning the degree distribution of the inner code and outer code.

Finally, in chapter 5, we derive a bit-oriented bound and a parity-oriented bound
on the minimum distance of both regular and block-wise irregular LDPC codes using the relationship between nodes on the graph and a minimum-weight codeword. We generalized Tanner’s results and set up a heuristic rule that a code with a smaller ratio of second to first eigenvalue would have a good distance property. We presented simulation results that the derived bounds work well as a design criterion in designing irregular LDPC codes.

6.2 Future Directions

Throughout this dissertation, we have proposed some efficiently encodable low-density codes and derived the minimum distance bounds on LDPC codes. In the further research, the following unsolved problems are desired to be studied.

1. Algebraic cycle analysis on the proposed QC-LDPC codes from power residues.

2. Related to irregular QC-LDPC codes we proposed block-PEG algorithm that fulfills the local girth maximization. For the construction of ensembles of codes that have lower error-floor, we need to develop local connectivity maximization criterion.

3. In chapter 4, we introduced simple degree distribution sequence pair for inner code and outer code of the concatenated LDGM codes in order to improve the reliability of degree-1 bit nodes. We need algebraic analysis on the capacity achieving degree distribution sequences for LDGM codes especially for higher-rate outer code.

4. In chapter 5, we need to specify and analyze the class of codes that achieves the derived bounds.
Bibliography


국문 요약

효율적인 부호화가 가능한 Low-Density 부호의 설계와 Tanner 바운드의 일반화

반복 부호 알고리즘을 이용한 그래프상에서 해석되는 부호는 Shannon의 이론적 인 채널 용량 한계에 근접하는 설용적인 부호로 연구되어 오고 있다. 특히 LDPC 부호의 커다란 단점으로 알려진 부호화 과정의 복잡도를 줄임으로써 효율적인 부호화가 가능한 LDPC 부호의 설계가 매우 중요하다.

본 논문에서는 먼저 행렬 곱셈 대신 다항식 곱셈을 수행함으로써 효율적인 부호화가 가능한 QC-LDPC 부호에 대해 연구한다. 기존에 알려진 QC-LDPC 부호는 대부분 균일한 구조를 가지고 있으며, 각 순환 행렬의 무게가 0 또는 1로 구성된 것에 반해 본 연구에서는 순환 행렬의 무게가 0, 1 또는 2가 되는 덱임여류로부터 생성된 QC-LDPC 부호를 제안한다. 덱임여류로부터 생성된 QC-LDPC 부호는 최소 사이클의 개수를 줄이는 데 유리한 구조를 가지고 있으며, 비균일한 부호를 성 상할 때 있어서 높은 무게도 갖는 비트 노드를 쉽게 구성할 수 있는 장점이 있고 이를 통하여 보다 우수한 성능을 나타내는 부호를 설계할 수 있다. 본 논문에서는 균일 부호의 경우 덱임여류의 특성을 이용하여 대수학적 구조를 갖는 부호를 설 계하며, 비균일 부호의 생성을 위해 기존의 비트 단위 최소 사이클 조정 알고리즘인 PEG 알고리즘을 변경하여 블록 단위의 설계에 적용 가능하도록 재구성한 블록 PEG 알고리즘을 제안한다. 제안한 블록 PEG 알고리즘을 이용하여 매우 우수
한 성능을 나타내는 비균일 QC-LDPC 부호를 예시하고 기존의 유사한 구조를 갖는 부호와 비교함으로써 그 성능을 검증한다.

LDPC 부호화 둔연한 반복 부호 알고리즘을 사용하는 LDGM 부호는 구조적 형태를 갖는 저밀도 생성행렬로서 매우 효율적인 부호화기 구조를 갖고 있다. LDGM 부호는 LDPC 부호에 비해 상대적으로 최근에 연구가 시작되고 있으며, 두개의 구조적 LDGM 부호의 연결 부호 방식을 통해 우수한 성능을 나타낸다. 하지만 LDGM 부호는 검사행렬의 패러미터 부분이 단위 행렬로 이루어져 있어 이에 해당하는 비트들의 무게가 1이기 때문에 메시지 전달 방식의 반복 부호를 수행함에 있어서 성능 연화의 요인이 된다. 본 논문에서는 무게가 1인 비트들의 신뢰도 를 높일 수 있는 비균일한 LDGM 부호를 새롭게 설계한다. 제안하는 부호는 외부 부호의 무게 1인 비트에 메시지를 전달하게 되는 내부 부호의 비트들의 업무게를 높여 외부 부호의 전체적인 신뢰도가 극단하게함으로써 성능의 향상을 가져온다.

LDPC 부호의 최소 거리 부호에 대한 연구는 상대적으로 어렵기 때문에 많은 연구 결과가 발표되지 못하였다. 이에 본 논문에서는 그래프상의 노드들과 최소 거리 부호여와의 관계를 통하여, 균일 및 불복 구조를 갖는 비균일 LDPC 부호에 적용 가능한 비트 노드 기반 하한식과 검사 노드 기반 하한식을 유도한다. 본 논문에서 유도한 일반화된 하한식은 Tanner의 결과를 확장한 것이며, 이를 통하여 LDPC 부호의 거리 특성을 그래프상의 고유값으로 표현할 수 있다. 다양한 예제 부호를 통하여 본 논문에서 유도한 하한식이 불복 구조를 갖는 비균일 LDPC 부호를 생성함에 있어서 설계 적도로 쓸어 수 있음을 보인다.

핵심되는 말: LDPC 부호, LDGM 부호,의 사전부호, 역행렬 수열, 불복 PEG 알고리즘, 비균일 LDGM 부호, 최소 거리 하한식

72