PROPERTIES OF LDGM-LDPC CODES WITH APPLICATIONS TO SECRECY CODING

By

MANIK RAINA

A thesis submitted to the

Graduate School—New Brunswick

Rutgers, The State University of New Jersey

in partial fulfillment of the requirements

For the degree of

Master of Science

Graduate Program in Electrical and Computer Engineering

written under the direction of

Professor Predrag Spasojević

and approved by

_____

_____

_____

_____

New Brunswick, New Jersey

May, 2010

ABSTRACT OF THE THESIS

Properties of LDGM-LDPC codes With Applications to Secrecy Coding

by Manik Raina

Thesis Directors: Professor Predrag Spasojević

The ensemble of low-density generator-matrix/low-density parity-check (LDGM-LDPC) codes has been proposed in literature. In this thesis, an irregular LDGM-LDPC code is studied as a sub-code of an LDPC code with some randomly *punctured* output-bits. It is shown that the LDGM-LDPC codes achieve rates arbitrarily close to the channel-capacity of the binary-input symmetric-output memoryless (BISOM) channel with a finite lower-bound on the *complexity*. The measure of complexity is the average-degree (per information-bit) of the check-nodes for the factor-graph of the code. A lower-bound on the average degree of the check-nodes of the irregular LDGM-LDPC codes is obtained. The bound does not depend on the decoder used at the receiver. The stability condition for decoding the irregular LDGM-LDPC codes over the binary-erasure channel (BEC) under iterative-decoding with message-passing is described. The LDGM-LDPC codes are capacity achieving with bounded complexity and possess natural binning/nesting structure. These codes are applied to secrecy coding. The problem of secrecy coding for the type-II binary symmetric memoryless wiretap channel is studied. In this model, the main channel is binary-input and noiseless and the eavesdropper channel is binary-symmetric memoryless. A coding strategy based on *secure nested codes* is proposed. A capacity achieving length-n code for the eavesdropper

channel bins the space $\{0,1\}^n$ into co-sets which are used for secret messaging. The resulting co-set scheme achieves secrecy capacity of the type-II binary symmetric memoryless channel. As an example, the ensemble of capacity-achieving regular low-density generator-matrix/low-density parity-check (LDGM-LDPC) codes is studied as a basis for binning. The previous result is generalized to the case of a noisy main-channel. The problem of secrecy-coding for a specific type-I wiretap channel is studied. In the type-I wiretap channel under consideration, the main channel is a binary-input symmetric-output memoryless (BISOM) channel and the eavesdropper channel is a binary-symmetric channel (BSC). A secure-nested-code that achieves perfect-secrecy for the above type-I channel is proposed. The secure-nested-code is based on a nested regular LDGM-LDPC code construction.

Acknowledgements

I am most grateful to my advisor Professor Predrag Spasojević for guiding my research, for his patience and kindness. I would like to thank Dr. Ruoheng Liu for his meticulous comments on our paper.

The course on "Probability theory and Stochastic Processes" forms the foundation for most of the work at Winlab. I would like to thank Professor Christopher Rose for teaching that course with great panache. That course was an unforgettable experience. I benefited greatly from Professor Roy Yates' course on "Information Theory and Coding". I would like to thank him for teaching the course. I would like to thank Professor Predrag Spasojević and Dr. Silvija D. Filipović for teaching the course "Advanced Topics in Communications Engineering" that foccused on LDPC codes, it greatly benefited in my research. I would like to thank the department of Electrical and Computer Engineering for financial support. A special thanks to Lynn Ruggiero, Barbara Klimkiewicz, Dianne Coslit, Noreen DeCarlo and Elaine Connors. A "thank you" to Devan, Michelle, Yao and Gautam.

I am grateful to my family: Rekha for her patience, love and support; Mihir, for being the most adorable little baby in the world; and my parents. Perhaps my greatest debt is to Viswanath Ganapathy for introducing me to the problems in channel coding and for just being one of the nicest people I have met. Thank you Viswa.

Table of Contents

List of Tables

List of Figures

Chapter 1

Introduction

The foundation of channel coding theory was laid by the pioneering work of Shannon [1]. Shannon showed that for a given channel, there existed a highest rate of information transmission called the *channel capacity* (C), below which information could be transmitted at arbitrarily low error-probability. Conversely, it was shown that for rates at or higher than capacity, the error-probability was bounded away from zero. Shannon's theory was *non-constructive* in that it showed what rates of communication were possible for large block lengths without indicating which specific coding schemes could be used to achieve those rates. However, Shannon showed that, asymptotically, almost all codes chosen randomly were *reliable* in the sense that if the transmission rate $R < C$, arbitrarily low error-probability was achievable.

Taking a cue from Shannon's random code construction, Gallager [2] proposed the *low-density parity-check* codes or LDPC codes. The LDPC codes were constructed by randomly choosing a sparse parity-check matrix. The purpose of a sparse parity-check matrix was to use the iterative decoder (using message passing). With the introduction of irregular LDPC codes, rates very close to the capacity of the binary-erasure channel were reached. After the discovery of LDPC codes, more complex codes like Turbo codes, Repeat-accumulate (RA) codes and Irregular repeat-accumulate (IRA) codes have been proposed and studied. More recently, the ensemble of low-density generator-matrix/low-density parity-check (LDGM-LDPC) codes has been proposed in literature. This thesis attempts to understand the properties of the ensemble of LDGM-LDPC codes and applies nested code constructions based on LDGM-LDPC codes to secrecy.

1.1 Outline of the Thesis

In Chapter 2, it is shown that irregular LDGM-LDPC codes achieve capacity of the binary-input symmetric-output memoryless (BISOM) channel with a finite lower-bound on complexity. Further, the performance of irregular LDGM-LDPC codes under iterative decoding is studied and the stability condition for zero error probability is given. Subsequent chapters study the applications of LDGM-LDPC codes to secrecy.

In Chapter 3, regular LDGM-LDPC codes are used to partition the set of vectors $\{0,1\}^n$ and the resulting coset coding scheme is shown to achieve the secrecy-capacity of a type-II binary symmetric wiretap channel.

In Chapter 4, regular LDGM-LDPC codes are used to achieve perfect-secrecy of the type-I wiretap channel with a BISOM main channel and a binary symmetric wiretap channel such that the main channel is less noisy compared to the eavesdropper channel.

Chapter 2

Decoding Complexity of Irregular LDGM-LDPC Codes Over BISOM Channels

2.1 Introduction

Two questions guide much of the research in channel-coding: the construction of codes that achieve rates arbitrarily close to the capacity of a given channel and efficient decoding of these codes. The decoding of error-correcting-codes using message-passing over sparse-graphs is considered the state-of-the-art. An example of a sparse-graph code is the ensemble of low-density parity-check codes [2]. Consider a binary-input symmetric-output memoryless (BISOM) channel with channel-capacity C. Suppose a code is chosen at random from a given code-ensemble and achieves a rate $(1-\epsilon)C$, where $\epsilon \in (0,1]$ is the multiplicative gap-to-capacity. The study of the encoding and decoding complexity of code-ensembles in terms of the capacity-gap ϵ was proposed by Khandekar and McElice [3].

Low-density parity-check (LDPC) codes exhibit remarkable performance under message-passing decoding. This performance is attributed to the sparseness of the parity-check matrices of these codes. The *density* of a parity-check matrix is the number of ones in the parity-check matrix per-information-bit. The density is proportional to the number of messages passed in one round of iterative-decoding. A lower-bound on the density of a parity-check matrix in terms of the multiplicative-capacity-gap ϵ was obtained in [4] and later tightened in [8]. For a code defined by a full-rank parity-check matrix, the lower-bound on the density is $\frac{K_1+K_2\log\frac{1}{\epsilon}}{1-\epsilon}$, where K_1 and K_2 depend on the channel and not on code parameters. As the rate of code approaches the channel-capacity ($\epsilon \to 0$), the density of the parity-check matrix becomes unbounded. The authors of [5] showed that non-systematic irregular-repeat-accumulate (NSIRA) codes could achieve

rates arbitrarily close to the channel-capacity of a BISOM channel with bounded complexity. The rates close to channel-capacity were achieved by randomly puncturing the information bits of the NSIRA codes indepedently with a probability that depended on the gap to capacity. Recently, the authors of [15], [10] modeled several communication scenarios using parallel channels. This model enables (among other things) the investigation of the performance of punctured LDPC codes. The effect of random-puncturing on the ensemble of (j, k) regular LDPC codes was studied in [11]; where an upper-bound on the weight spectrum of the ensemble of LDPC codes in question was obtained. The ensemble of low-density generator-matrix/low-density parity-check (LDGM-LDPC) codes was studied in [6], [20]. This ensemble results on compounding the LDGM and LDPC codes. Hsu [6] proved that codes from the *regular* LDGM-LDPC ensemble could achieve rates arbitrarily close to the channel-capacity of the BISOM channel with bounded graphical complexity. However, the proof of [6] assumed: a regular LDGM code with rate 1; a regular LDPC code; and, a maximum-likelihood (ML) decoder. No puncturing was employed. Pfister and Sason [12] studied capacity achieving degree-distributions for the accumulate-repeat-accumulate (ARA) codes over the BISOM channel. Using a technique called *graph-reduction*, some capacity-achieving degree-distributions for accumulate LDPC (ALDPC) codes were proposed. ALDPC codes were shown to be LDGM-LDPC codes with a 2-regular LDGM code. In this work, the upper LDGM code can have any rate $R_G \in (0, 1]$. Further, the LDPC and LDGM codes can be irregular and the requirement for ML decoding is removed.

This chapter obtains lower-bounds on the complexity of the ensemble of irregular LDGM-LDPC codes at rates arbitrarily close to the capacity of the binary-input symmetric-output memoryless channel for asymptotic block-lengths. The information-theoretic bounds obtained in this chapter do not depend on the type of decoder. The LDGM-LDPC codes are studied as sub-codes of *constrained punctured LDPC codes*. It is shown that if some variable nodes of the constrained punctured LDPC codes are punctured independently with probability $p = 1 - \kappa\epsilon$ (for some constant κ), the ensemble achieves rates arbitrarily close to channel capacity of the BISOM channel with

a finite lower-bound on the *complexity*. Further, it is shown that that the LDGM-LDPC codes are equivalent to the constrained punctured LDPC codes when $\epsilon \to 0$ (or $p \to 1$). The performance of the constrained punctured LDPC codes are studied over the binary-erasure channel under iterative-decoding using message-passing. The stability conditions are derived.

This chapter is organized as follows. Some preliminary topics are introduced in Section 2.2. LDGM-LDPC codes are modeled as sub-codes of constrained punctured LDPC codes in Section 2.3. Performance of the constrained punctured LDPC codes and bounds on the average degrees of the factor graph are studied in Section 2.4. The stability condition for these codes over the binary-erasure channel under message-passing decoding is studied in Section 2.5. The chapter is concluded in Section 2.6.

2.2 Preliminaries

In this chapter, uppercase, lowercase and bold-uppercase variables represent random-variables, realization of random variables and random-vectors respectively. For example, X is a random-variable with a realization x while $\mathbf{X}$ is a random-vector.

2.2.1 LDGM-LDPC Codes

Regular LDGM-LDPC codes were studied in [6, 20]. In this chapter, irregular LDGM-LDPC codes are studied. Consider the binary random vectors $\mathbf{X_1}, \mathbf{X_2}$ of length $n^{[1]}$ and $n^{[2]}$ respectively. The LDGM-LDPC code is defined as follows:

$$\mathcal{C} \triangleq \{\mathbf{X_1} : \mathbf{X_1} = \mathbf{X_2}G, \mathbf{X_2}H^T = \mathbf{0}\} \tag{2.1}$$

where H and G are the random low-density parity-check (LDPC) matrix and random low-density generator-matrix (LDGM) respectively (Figure 2.1). Consider the factor-graphs $\mathcal{G}_\mathcal{H}$ and $\mathcal{G}_\mathcal{G}$ represented by the matrices H and G respectively. Let $\mathcal{G}_\mathcal{H}$ be a $(n^{[2]}, \lambda_H(x), \rho_H(x))$ factor-graph with $n^{[2]}$ variable-nodes where we define the following generating-functions:

$$\lambda_H(x) = \sum_i \lambda_{H,i} x^{i-1}, \qquad \rho_H(x) = \sum_i \rho_{H,i} x^{i-1} \tag{2.2}$$

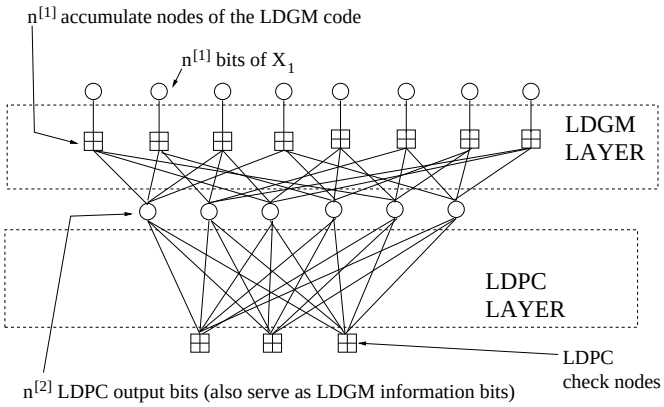

Figure 2.1: The LDGM-LDPC Code

where $\lambda_{H,i}$ ($\rho_{H,i}$) is the probability of a randomly chosen edge in $\mathcal{G}_{\mathcal{H}}$ being connected to a variable (check) node of degree i. Similarly, Let $\mathcal{G}_{\mathcal{G}}$ be a $(n^{[1]}, \lambda_G(x), \rho_G(x))$ factor-graph with $n^{[1]}$ accumulated-nodes where we define the following generating-functions:

$$\lambda_G(x) = \sum_i \lambda_{G,i} x^{i-1}, \qquad \rho_G(x) = \sum_i \rho_{G,i} x^{i-1} \tag{2.3}$$

where $\lambda_{G,i}$ ($\rho_{G,i}$) is the probability of a randomly chosen edge in $\mathcal{G}_{\mathcal{G}}$ being connected to a information (accumulate) node of degree i. The two factor graphs $\mathcal{G}_{\mathcal{G}}$ and $\mathcal{G}_{\mathcal{H}}$ are compounded to form the LDGM-LDPC code as shown in Figure 2.1.

2.3 LDGM-LDPC Codes As a LDPC Sub-Code

In this section, the LDGM-LDPC code as defined in (2.1) is shown to be a sub-code of an LDPC code. Consider the binary vector $\mathbf{X} = (\mathbf{X_1 X_2})$ that results on the concatenation of the two binary vectors $\mathbf{X_1}$ and $\mathbf{X_2}$ (of lengths $n^{[1]}$ and $n^{[2]}$ respectively), which satisfy (2.1). A new constraint-matrix is defined as follows:

$$\mathcal{H} = \begin{pmatrix} I & 0 \\ \\ G & H^T \end{pmatrix}^T \tag{2.4}$$

where I is the $n^{[1]} \times n^{[1]}$ identity matrix, G and H are the random LDGM generator-matrix and LDPC parity-check matrix of the LDGM-LDPC code (defined in (2.1)). The following lemma holds.

Lemma 1. *The code* $\mathcal{C}_{\mathcal{H}} \stackrel{\Delta}{=} \{\mathbf{X} : \mathbf{X}\mathcal{H}^T = \mathbf{0}\}$ *is a parity-check code with parity-check matrix* $\mathcal{H}$ *which is a* mother code *of the LDGM-LDPC code defined in* (2.1).

Proof. It follows from (2.4) that

$$\{(\mathbf{X_1}\mathbf{X_2})\mathcal{H}^T = \mathbf{0}\} \iff \{\mathbf{X_1} = \mathbf{X_2}G \text{ and } \mathbf{X_2}H^T = \mathbf{0}\}$$

where all arithmetic is over GF(2). The bits $\mathbf{X_1}$ are identical to the code bits of the LDGM-LDPC code in (2.1). Thus, the code in (2.1) is a sub-code of the code $\mathcal{C}_{\mathcal{H}}$. The vector $\mathbf{X}$ is a length n parity-check code with a sparse parity-check matrix $\mathcal{H}$. $\mathcal{H}$ is the parity-check matrix of a randomly chosen code from the ensemble $(n, \lambda_G(x), \rho_G(x), \lambda_H(x), \rho_H(x))$. □

2.4 Puncturing the Mother Code $\mathcal{C}_{\mathcal{H}}$

In this section, a random puncturing scheme is introduced for the code $\mathcal{C}_{\mathcal{H}}$ that was defined in Lemma 1. Further, the lower-bound on the average density of the irregular LDGM-LDPC ensemble is obtained. Consider a length n codeword $\mathbf{X} = \{X_1, \ldots, X_n\}$ that is transmitted over a BISOM channel. A code bit of $\mathbf{X}$ is punctured if the output at the BISOM channel corresponding to the said code bit is 0. Some puncturing schemes for codes were proposed in [13], which include random puncturing (codeword bits were punctured independently with some probability p) or intentional-puncturing (code bits were divided into classes and each class had its own puncturing probability).

Remark 1. *The codeword* $\mathbf{X}$ *is assumed to be uniformly chosen from the code* $\mathcal{C}_{\mathcal{H}}$*. It is assumed in this chapter that all the bits of the codeword are equally likely to be* 0 *or* 1.

The result [10, Proposition 2.1] is now restated. It is assumed that every codeword bit in $\mathbf{X}$ is transmitted though one of the J statistically independent BISOM channels, where C_j is the capacity of the jth channel (in bits per channel use) and $p_{Y|X}(.|.; j)$ is the transition probability of the jth channel. Let the received message at the channel output be $\mathbf{Y}$. The conditional probability-density of the log-likelihood ratio $\log \frac{p_{Y|X}(Y=y|0;j)}{p_{Y|X}(Y=y|1;j)}$ at the output of the jth channel given the input is 0 is denoted by $a(.; j)$. Let $\mathcal{I}(j)$ be the

set of indices of the code bits transmitted over the jth channel, $n^{[j]} \triangleq |\mathcal{I}(j)|$ be the size of this set, and $p_j = \frac{n^{[j]}}{n}$ be the fraction of bits transmitted over the jth channel. For an arbitrary $c \times n$ parity-check matrix H of the code $\mathcal{C}$, let $\beta_{j,m}$ designate the number of indices in $\mathcal{I}(j)$ referring to bits which are involved in the mth parity-check equation of H and let $R_d = 1 - \frac{c}{n}$ be the design rate of $\mathcal{C}$.

Proposition 1. *Let $\mathcal{C}$ be a binary linear block code of length n, and assume that its transmission takes place over a set of J statistically independent BISOM channels. Let $\mathbf{X} = \{X_1, \ldots, X_n\}$ and $\mathbf{Y} = \{Y_1, \ldots, Y_n\}$ designate the transmitted codeword and received sequence respectively. Then, the average conditional entropy of the transmitted codeword given the received sequence satisfies*

$$\begin{aligned} \frac{1}{n} H(\mathbf{X}|\mathbf{Y}) \geq 1 - \sum_{j=1}^{J} p_j C_j - (1 - R_d) \\ \cdot \left(1 - \frac{1}{2n(1-R_d)\log 2} \right. \\ \left. \sum_{p=1}^{\infty} \left\{ \frac{1}{p(2p-1)} \sum_{m=1}^{n(1-R_d)} \prod_{j=1}^{J} (g_{j,p})^{\beta_{j,m}} \right\} \right) \end{aligned}$$

where

$$\begin{aligned} g_{j,p} \triangleq \int_0^{\infty} a(l;j)(1+e^{-l}) \tanh^{2p}\Big(\frac{l}{2}\Big) dl, \\ j \in \{1, \ldots, J\}, p \in \mathbb{N}. \end{aligned} \tag{2.5}$$

Definition 1. Constrained punctured LDPC code $\mathcal{C}_{\mathcal{H}}(p)$*: Let $\mathcal{C}_{\mathcal{H}}$ be a parity-check code defined in Lemma 1. If the first $n^{[1]}$ bits of this code $\mathbf{X_1}$ pass through the channel without puncturing and the last $n^{[2]}$ bits of the code $\mathbf{X_2}$ are punctured independently with probability p, the punctured mother code is denoted by $\mathcal{C}_{\mathcal{H}}(p)$.*

The following remark explains why the above punctured LDPC codes are termed "constrained."

Remark 2. *Let k_m be a random variable representing the number of edges involved in the mth parity-check of a given parity-check code. In the bound derived in proposition 1, $\beta_{j,m}$ refers to the number of code bits from the jth class that are connected to the*

mth parity-check. For every m, it follows that:

$$k_m = \sum_{j \in [1,\ldots,J]} \beta_{j,m}$$

where J is the number of parallel, statistically independent channels. When discussing the code $\mathcal{C}_{\mathcal{H}}(p)$*,* $J = 2$*. The case* $j = 1$ *corresponds to the* $n^{[1]}$ *un-punctured bits (variable nodes)* $\mathbf{X_1}$ *and* $j = 2$ *corresponds to the* $n^{[2]}$ *bits (variable nodes) of* $\mathbf{X_2}$ *that are independently punctured with probability p. From the structure of the code* $\mathcal{C}_{\mathcal{H}}(p)$*, each of the first* $n^{[1]}$ *parity-checks are connected to exactly one variable node from the first class (bits of* $\mathbf{X_1}$*), i.e* $\beta_{1,m} = 1$*, if* $m \in [1, n^{[1]}]$*. The number of variable nodes connected to the first* $n^{[1]}$ *check nodes from* $j = 2$ *is* $\beta_{2,m} = k_m - 1$*, where* k_m *is distributed as per* $\rho_G(.)$ *of* (2.3) *(see Figure 2.1 and 2.2). The remaining parity-checks of the code* $\mathcal{C}_{\mathcal{H}}(p)$ *are connected to variables nodes from the second class (bits of* $\mathbf{X_2}$*) only. Thus if* $m \geq n^{[1]}$*,* $\beta_{1,m} = 0$ *and* $\beta_{2,m} = k_m$*, where* k_m *is distributed as per* $\rho_H(.)$ *of* (2.2)*. To summarize:*

$$\begin{aligned} \beta_{1,m} &= \begin{cases} 1, m \in [1, n^{[1]}], \\ 0, \ \textit{otherwise} \end{cases} \\ \beta_{2,m} &= \begin{cases} k_m - 1, m \in [1, n^{[1]}] \\ k_m, \ \textit{otherwise} \end{cases} \end{aligned} \tag{2.6}$$

In parallel LDPC codes of [10], the members of the sequence $\{\beta_{1,m}, \ldots, \beta_{J,m}\}$ *take on all possible values between* 1 *and* k_m *such that* $\sum_j \beta_{j,m} = k_m$*. On the other hand, for the code* $\mathcal{C}_{\mathcal{H}}(p)$*,* $\beta_{1,m}$ *takes values* 0 *or* 1 *only. This follows from: the structure of the parity-check matrix* $\mathcal{H}$ *of the code* $\mathcal{C}_{\mathcal{H}}$ *(and of* $\mathcal{C}_{\mathcal{H}}(p)$*); and, the assignment of* $\mathbf{X_1}$ *and* $\mathbf{X_2}$ *to the two classes of parallel channels.*

Claim 1. *Let* $\mathcal{C}$ *and* $\mathcal{C}_{\mathcal{H}}(p)$ *represent the codes defined in* (2.1) *and definition 1 respectively. Then,*

$$\lim_{p \to 1} \mathcal{C}_{\mathcal{H}}(p) = \mathcal{C}$$

The above claim follows from (2.1) and definition 1 because in the limit $p \to 1$, all

the bits of the lower LDPC code $\mathbf{X_2}$ are punctured. The codewords of $\mathcal{C}_{\mathcal{H}}(p)$ are $\mathbf{X_1}$, which is identical to the codewords of $\mathcal{C}$ of (2.1).

The following lemma relates the code rate and the conditional entropy $H(\mathbf{X}|\mathbf{Y})$ of the code defined in definition 1.

Lemma 2. *Let $\mathcal{C}_{\mathcal{H}}(p)$ be a code of length n as defined in definition 1. Let $\mathbf{X}$ be a binary codeword from $\mathcal{C}_{\mathcal{H}}(p)$. Let $\mathbf{Y}$ be a vector sequence of length n at the output of the BISOM channel upon transmission of $\mathbf{X}$. Then, the following inequality holds:*

$$\frac{1}{n}H(\mathbf{X}|\mathbf{Y}) \leq \frac{n^{[2]}}{n}H(P_b) \tag{2.7}$$

where P_b is the average bit-error probability of decoding the lower LDPC code $\mathbf{X_2}$, $n^{[2]}$ is the length of the lower LDPC code $\mathbf{X_2}$, as defined in (2.1).

Proof.

$$\begin{aligned}\frac{1}{n}H(\mathbf{X}|\mathbf{Y}) &\overset{a}{=} \frac{1}{n}H(\mathbf{X_1},\mathbf{X_2}|\mathbf{Y}) \\ &\overset{b}{=} \frac{1}{n}H(\mathbf{X_2}|\mathbf{Y}) + \frac{1}{n}H(\mathbf{X_1}|\mathbf{Y},\mathbf{X_2}) \overset{c}{=} \frac{1}{n}H(\mathbf{X_2}|\mathbf{Y})\end{aligned} \tag{2.8}$$

where $\overset{a}{=}$ follows from the definition of $\mathbf{X}$, $\overset{b}{=}$ follows from the chain rule of entropy and $\overset{c}{=}$ follows because for a given code $\mathcal{C}_{\mathcal{H}}(p)$, the entropy of $\mathbf{X_1}$ is zero if $\mathbf{X_2}$ is known (this follows from $\mathbf{X_1} = \mathbf{X_2}G$). Further,

$$\begin{aligned}\frac{1}{n}H(\mathbf{X_2}|\mathbf{Y}) &\overset{d}{\leq} \frac{1}{n}\sum_{i=1}^{n^{[2]}} h_2(p_e^i) = \frac{n^{[2]}}{n}\frac{1}{n^{[2]}}\sum_{i=1}^{n^{[2]}} h_2(p_e^i) \\ &\overset{e}{\leq} \frac{n^{[2]}}{n}h_2\Big(\frac{1}{n^{[2]}}\sum_{i=1}^{n^{[2]}} p_e^i\Big) \overset{f}{=} \frac{n^{[2]}}{n}h_2(P_b)\end{aligned} \tag{2.9}$$

where $\overset{d}{\leq}$ follows from the Fano's inequality for binary valued random variables and where p_e^i is the bit error probability for the ith bit of $\mathbf{X_2}$, $\overset{e}{\leq}$ follows from the concavity of the binary entropy function and $\overset{f}{=}$ follows from the definition of the average bit-error probability of $\mathbf{X_2}$. (2.7) follows from (2.8) and (2.9). □

In the following theorem, it is assumed that the code length $n \to \infty$ and $P_b \to 0$. An upper-bound on the design-rate for the ensemble of parity-check codes defined in Lemma 1 is obtained.

Theorem 1. *Consider a $(n, \lambda_G(x), \rho_G(x), \lambda_H(x), \rho_H(x))$ ensemble as defined in Lemma 1. Let $\mathbf{X}$ be a codeword from the code $\mathcal{C}_{\mathcal{H}}(p)$ that is chosen uniformly from this ensemble. Let the first $n^{[1]}$ bits of $\mathbf{X}$ pass through a BISOM channel with capacity C without puncturing. The last $n^{[2]}$ bits of $\mathbf{X}$ pass through the BISOM channel after being punctured independently with probability p. Let $p_1 = \frac{n^{[1]}}{n}$, $p_2 = \frac{n^{[2]}}{n}$ (where $p_1 + p_2 = 1$) and let R_H be the design-rate of the lower LDPC code in the LDGM-LDPC code. Further, let a_L and a_R be the average degrees of the accumulate nodes of the LDGM codes and check nodes of the LDPC nodes respectively. Then, the design rate R_d of the ensemble is upper-bounded as:*

$$R_d \leq 1 - \frac{1 - (p_1 + (1-p)p_2)C}{1 - \frac{1}{2\log 2}\frac{g_{1,1}p_1 + (1-R_H)p_2}{p_1 + (1-R_H)p_2} g_{2,1}^{\frac{g_{1,1}p_1 a_L + (1-R_H)p_2 a_R}{g_{1,1}p_1 + (1-R_H)p_2}}}$$

where $g_{1,1}$ and $g_{2,1}$ are defined as per (2.5).

The above theorem is proved in the appendix. The above upper-bound on the design-rate of punctured $(n, \lambda_G(x), \rho_G(x), \lambda_H(x), \rho_H(x))$ ensembles (as defined in Lemma 1) can be used to obtain a lower-bound on the asymptotic complexity of the code. In the following theorem, the lower-bound is obtained.

Corollary 1. *In the limiting case of $n \to \infty$, puncturing the last $n^{[2]}$ bits of a codeword (independently with probability p) results in a channel capacity $\bar{C} = (1 - p_2 p)C$, where C is the capacity of the BISOM channel under consideration. Let a_L and a_R be the average degrees of the LDGM accumulate nodes and the LDPC check nodes. Let R_H be the rate of the lower LDPC code. Then, if the design rate of the ensemble $R_d = (1-\epsilon)\bar{C}$, the following lower-bound on a_L and a_R holds:*

$$\frac{p_1 g_{1,1} a_L + (1 - R_H)p_2 a_R}{p_1 g_{1,1} + (1 - R_H)p_2} \geq \frac{\log\left(\frac{1}{2\log 2}\frac{p_1 g_{1,1} + (1-R_H)p_2}{p_1 + (1-R_H)p_2}\frac{1-(1-\epsilon)\bar{C}}{\epsilon\bar{C}}\right)}{\log(\frac{1}{g_{2,1}})}$$

Proof. The design-rate R_d is set to $(1 - \epsilon)\bar{C}$ in the upper-bound of Theorem 1 and obtain the above bound. □

A direct consequence of the above result is that rates arbitrarily close to channel capacity are possible with finite complexity.

Lemma 3. *Consider a code $\mathcal{C}_{\mathcal{H}}(p)$ discussed in corollary 1. Then, in the limit $\epsilon \to 0$, the lower-bound on the average-degrees is finite if the puncturing probability $p = 1 - \kappa\epsilon$, for some constant κ.*

Proof. Since the last $n^{[2]}$ bits of the code $\mathcal{C}_{\mathcal{H}}(p)$ are punctured independently with probability p, the probability density of the log-likelihood ratio (LLR) of those bits is:

$$a(l;2) = p\delta_0(l) + (1-p)a(l) \tag{2.10}$$

where $\delta_0(l)$ is the Dirac delta function at $l = 0$ and $a(l)$ is the density of the LLR over the original (un-punctured) BISOM channel. First, $g_{2,1}$ is simplified. As per (2.5),

$$\begin{aligned} g_{2,1} &\triangleq \int_0^\infty a(l;2)(1+e^{-l})\tanh^2\Big(\frac{l}{2}\Big)dl \\ &\stackrel{a}{=} \int_0^\infty [p\delta_0(l) + (1-p)a(l)](1+e^{-l})\tanh^2\Big(\frac{l}{2}\Big)dl \\ &= (1-p)g_1 \end{aligned}$$

where $\stackrel{a}{=}$ follows from (2.10) and where

$$g_1 = \int_0^\infty a(l)(1+e^{-l})\tanh^2\Big(\frac{l}{2}\Big)dl.$$

In the limit $\epsilon \to 0$, the lower-bound on the complexity in corollary 1 is finite if and only if $(1-p)g_1 = \eta\epsilon$ for some constant η. Thus, it follows that $p = 1 - \kappa\epsilon$, where $\kappa = \frac{\eta}{g_1}$. □

Lemma 4. *The lower-bound on the average degrees of the LDGM-LDPC code defined in* (2.1) *is finite for a BISOM channel.*

Proof. Let $\mathbf{X} = (\mathbf{X_1}\mathbf{X_2})$ represent a randomly chosen codeword from the code $\mathcal{C}_{\mathcal{H}}(p)$. It follows from Lemma 3 that if the design rate of this ensemble R_d approaches capacity ($\epsilon \to 0$) and the puncturing probability p of the LDPC code bits $\mathbf{X_2}$ approaches 1, the average lower-bound on the complexity is bounded. In the limit $n \to \infty$ and $p \to 1$, the code words of the code $\mathcal{C}_{\mathcal{H}}(p)$ are $\mathbf{X_1}$ as all the bits of $\mathbf{X_2}$ are punctured. Thus, the code words of the code $\mathcal{C}_{\mathcal{H}}(p)$ are identical to the LDGM-LDPC code defined in (2.1). □

2.5 Stability Condition for Message Passing Decoding of Punctured LDGM-LDPC Codes Over BEC

In this section, the decoding of the ensemble of $(n, \lambda_G(x), \rho_G(x), \lambda_H(x), \rho_H(x))$ codes is studied. The channel is assumed to be a binary erasure channel (BEC) with an erasure probability of δ. It is assumed that the decoder employs iterative-decoding using message-passing. The density-evolution technique of [14] is employed in this work. The main assumption in density-evolution is that the message on an edge of the factor-graph of a randomly chosen code is independent of the messages on all other edges. This assumption is justified because in the asymptotic case $n \to \infty$, the fraction of bits involved in finite-length cycles vanishes. The density-evolution (DE) equations are obtained for the lth stage of decoding. The fixed-point analysis is performed on the DE equations and the stability-condition for DE is derived.

Consider the factor-graph of the LDGM-LDPC code in fig. 2.2. The lth iteration of DE is considered. Let x_1^l (y_1^l) be the erasure probability along a random edge from (to) the $n^{[1]}$ un-punctured LDGM channel bit nodes to (from) the LDGM accumulate nodes in the lth iteration of message-passing. Further, let x_2^l (y_2^l) be the erasure probability along a random edge from (to) the $n^{[2]}$ punctured LDPC variable bit nodes to (from) the LDGM accumulate nodes. Similarly, let x_3^l (y_3^l) be the erasure probability along a random edge from (to) the $n^{[2]}$ punctured LDPC variable bit nodes to (from) the LDPC check nodes. Consider the $n^{[1]}$ LDGM variable nodes. The message from the LDGM variable nodes to the LDGM accumulate constraints is an erasure if the original channel symbol that was received was an erasure and the message from the accumulate constraint to the LDGM node in the $l-1$th erasure was an erasure. This observation is formalized as:

$$x_1^l = \delta y_1^{l-1} \tag{2.11}$$

Consider the message on a random edge from an LDGM accumulate node to a LDGM variable node. An erasure results when at least one message from the LDPC variable

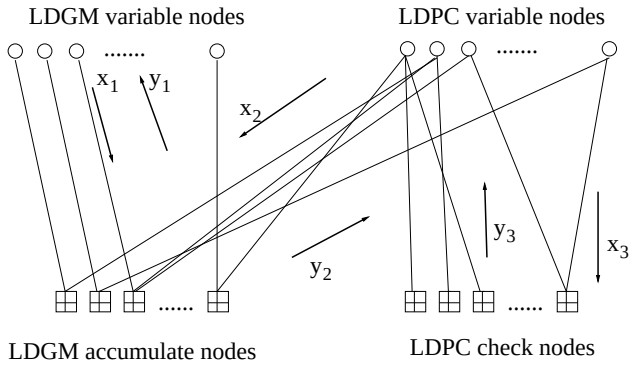

Figure 2.2: The erasure probabilities for LDGM-LDPC codes

nodes in the previous iteration were erasures.

$$y_1^l = 1 - R_{\mathrm{G}}(1 - x_2^{l-1}) \tag{2.12}$$

where $R_{\mathrm{G}}(x) = \frac{\int_0^x \rho_{\mathrm{G}}(t)dt}{\int_0^1 \rho_{\mathrm{G}}(t)dt}$. Consider a random edge from an LDPC variable node to the LDGM accumulate node. An erasure results on this edge during the lth iteration if all the incoming edges are erasures and the variable node was erased or punctured. Thus,

$$x_2^l = (1 - (1-\delta)(1-p))\lambda_G(y_2^{l-1})L_H(y_3^{l-1}) \tag{2.13}$$

where p is the puncturing probability and $L_{\mathrm{H}}(x) = \frac{\int_0^x \lambda_{\mathrm{H}}(t)dt}{\int_0^1 \lambda_{\mathrm{H}}(t)dt}$. The probability along a random edge from a LDGM accumulate node to a LDPC variable node in the lth iteration happen if any of the channel outputs are erased in the previous iteration.

$$y_2^l = 1 - (1 - x_1^{l-1})\rho_G(1 - x_2^{l-1}) \tag{2.14}$$

Along the lines of (2.13), a randomly chosen edge from an LDPC variable node to an LDPC check-node has an erasure in the lth iteration if the variable node experienced an erasure and all incoming edges carried erasure messages in the $l-1$th iteration.

$$x_3^l = (1 - (1-\delta)(1-p))L_G(y_2^{l-1})\lambda(1 - y_3^{l-1}) \tag{2.15}$$

An erasure along a randomly chosen edge from an LDPC check node to an LDPC variable node happens if any incoming edge has an erasure.

$$y_3^l = 1 - \lambda_H(1 - x_3^{l-1}) \tag{2.16}$$

Definition 2. *The* fixed-points *of density-evolution described in (2.11-2.16) are defined as*

$$\lim_{l\to\infty} x_i^l = x_i \text{ and } \lim_{l\to\infty} y_i^l = y_i, \qquad \forall i \in \{1,2,3\}$$

We solve for x_2 and x_3 from (2.11-2.16) and obtain,

$$\begin{aligned} x_2 &= [1-(1-\delta)(1-p)]. \\ &\quad \lambda_G(1-(1-\delta(1-R_G(1-x_2)))\rho_G(1-x_2)). \\ &\quad L_H(1-\rho_H(1-x_3)) \\ x_3 &= [1-(1-\delta)(1-p)]. \\ &\quad L_G(1-(1-\delta(1-R_G(1-x_2)))\rho_G(1-x_2)). \\ &\quad \lambda_H(1-\rho_H(1-x_3)) \end{aligned} \tag{2.17}$$

Theorem 2. *Consider the LDGM-LDPC code ensemble as defined in Lemma 1. The point $x_2 = 0$ is stable during density-evolution if*

$$(1-(1-\delta)(1-p))^2 \lambda_G(0) L_G^{'}(0) \rho_H^{'}(1) \lambda_H(0) L_H^{'}(0) \tag{2.18}$$

$$.[\delta L_G^{'}(1) + \rho_G^{'}(1)] < 1 \tag{2.19}$$

The theorem is proved in the appendix.

As per Lemma 3, at rates very close to capacity, if the puncturing rate $p = 1-\kappa\epsilon$, the lower-bound on the complexity is finite as the rates are arbitrarily close to capacity. We study the stability condition when the rates are chosen very close to capacity.

Lemma 5. *When the code rate of the LDGM-LDPC code is arbitrarily close to capacity i.e. $\epsilon \to 0$, and $p = 1-\kappa\epsilon$, the stability condition for iterative decoding is*

$$\lambda_G(0) L_G^{'}(0) \rho_H^{'}(1) \lambda_H(0) L_H^{'}(0) [\delta L_G^{'}(1) + \rho_G^{'}(1)] < 1$$

Proof. Substituting $p = 1-\kappa\epsilon$ and $\epsilon \to 0$ in (2.18) proves the above lemma. □

2.6 Chapter Summary

Irregular LDGM-LDPC codes have been shown to be the sub-codes of LDPC codes with some randomly punctured bits. The ensemble of irregular LDGM-LDPC codes have

been shown to achieve the capacity of the BISOM channel with a finite lower-bounded on the complexity. The stability condition for the punctured LDGM-LDPC codes over the BEC under message-passing decoding was obtained.

2.7 Appendix

2.7.1 Proof of Theorem 1

Proof. From Lemma 2, proposition 1, setting $n \to \infty$ and $P_b \to 0$,

$$0 \geq 1 - \sum_{j=1}^{J} p_j C_j - (1 - R_d)\Bigg(1 - \frac{1}{2n(1-R_d)\log 2} \cdot \sum_{p=1}^{\infty}\Bigg\{\frac{1}{p(2p-1)} \sum_{m=1}^{n(1-R_d)} \prod_{j=1}^{J} (g_{j,p})^{\beta_{j,m}}\Bigg\}\Bigg) \tag{2.20}$$

By considering the first term of the sum in p in the above equation, the above equation can be bounded as follows:

$$0 \geq 1 - \sum_{j=1}^{J} p_j C_j - (1 - R_d)\Bigg(1 - \frac{1}{2n(1-R_d)\log 2} \cdot \Bigg\{\sum_{m=1}^{n(1-R_d)} \prod_{j=1}^{J} (g_{j,1})^{\beta_{j,m}}\Bigg\}\Bigg) \tag{2.21}$$

Since the first $n^{[1]}$ bits pass through the BISOM channel without puncturing, $C_1 = C$. Further, since the last $n^{[2]}$ bits of the codeword are punctured, $C_2 = (1-p)C$. Let c be the number of parity checks in the matrix (2.4). Then, $c = n(1 - R_d)$. Due to the structure of the code, from (2.6) and (2.4), for $m \in [1, n^{[1]}]$, $\beta_{1,m} = 1$ and $\beta_{2,m}$ is distributed as $\rho_G(x)$, (defined in (2.3)). Further, for $m \in [n^{[1]} + 1, c]$, $\beta_{1,m} = 0$ and $\beta_{2,m}$ is distributed as $\rho_H(x)$ (defined in (2.2)). We compute the expectation of (2.21) over the distributions $\rho_G(.)$ and $\rho_H(.)$. The expectation $\mathbf{E}\Big[\sum_{m=1}^{n(1-R_d)} \prod_{j=1}^{J} (g_{j,p})^{\beta_{j,m}}\Big]$ is computed as follows:

$$\mathbf{E} \sum_{m=1}^{n(1-R_d)} \prod_{j=1}^{J} (g_{j,p})^{\beta_{j,m}} = \mathbf{E} \sum_{m=1}^{n^{[1]}} \prod_{j=1}^{J} (g_{j,p})^{\beta_{j,m}} + \mathbf{E} \sum_{m=n^{[1]}+1}^{c} \prod_{j=1}^{J} (g_{j,p})^{\beta_{j,m}} \tag{2.22}$$

$\mathbf{E}\sum_{m=1}^{n^{[1]}}\prod_{j=1}^{J}(g_{j,p})^{\beta_{j,m}}$ is evaluated as follows:

$$\begin{aligned}\mathbf{E}\sum_{m=1}^{n^{[1]}}\prod_{j=1}^{J}(g_{j,p})^{\beta_{j,m}} &\overset{a}{=} n^{[1]}\mathbf{E}_{\beta_{2,m}}[g_{1,p}g_{2,p}^{\beta_{2,m}}]\\ &\overset{b}{=} n^{[1]}g_{1,p}\mathbf{E}_{\beta_{2,m}}[g_{2,p}^{\beta_{2,m}}] \overset{c}{\geq} n^{[1]}g_{1,p}g_{2,p}^{\mathbf{E}_{\beta_{2,m}}\beta_{2,m}}\end{aligned} \tag{2.23}$$

where $\overset{a}{=}$ follows because $\beta_{1,m}=1$, $\overset{b}{=}$ follows because $g_{1,p}$ is a constant as the expectation is w.r.t. $\beta_{2,m}$, $\overset{c}{\geq}$ follows from the convexity of the function $g_{2,p}^{\beta_{2,m}}$ and the Jensen's inequality. $\mathbf{E}\sum_{m=n^{[1]}+1}^{c}\prod_{j=1}^{J}(g_{j,p})^{\beta_{j,m}}$ is evaluated as follows:

$$\mathbf{E}\sum_{m=n^{[1]}+1}^{c}\prod_{j=1}^{J}(g_{j,p})^{\beta_{j,m}} \overset{d}{=} c_H\mathbf{E}_{\beta_{2,m}}[g_{2,p}^{\beta_{2,m}}] \overset{e}{\geq} c_H g_{2,p}^{\mathbf{E}_{\beta_{2,m}}\beta_{2,m}} \tag{2.24}$$

where $c_H = c - n^{[1]}$ is the number of parity-checks in the lower LDPC layer of the LDGM-LDPC code, where $\overset{d}{=}$ follows because $\beta_{1,m}=0$, $\overset{e}{\geq}$ follows from the convexity of the function $g_{2,p}^{\beta_{2,m}}$ and the Jensen's inequality. From (2.23) and (2.24), the sum in (2.22) becomes

$$\begin{aligned}\mathbf{E}\sum_{m=1}^{n(1-R_d)}\prod_{j=1}^{J}(g_{j,p})^{\beta_{j,m}} &\geq n^{[1]}g_{1,p}g_{2,p}^{\mathbf{E}_{\beta_{2,m}}\beta_{2,m}} + c_H g_{2,p}^{\mathbf{E}_{\beta_{2,m}}\beta_{2,m}}\\ &\overset{f}{=} n^{[1]}g_{1,p}g_{2,p}^{a_L} + c_H g_{2,p}^{a_R}\end{aligned} \tag{2.25}$$

where $\overset{f}{=}$ results by replacing the average number of edges to the LDGM accumulate nodes and LDPC check nodes by a_L and a_R respectively. The right hand side of (2.25) is further simplified as follows.

$$\begin{aligned}n^{[1]}g_{1,p}g_{2,p}^{a_L} + c_H g_{2,p}^{a_R} &= (n^{[1]}g_{1,p}+c_H)\Big[\frac{n^{[1]}g_{1,p}}{n^{[1]}g_{1,p}+c_H}g_{2,p}^{a_L}\\ &\quad + \frac{c_H}{n^{[1]}g_{1,p}+c_H}g_{2,p}^{a_R}\Big]\\ &\overset{g}{\geq} (n^{[1]}g_{1,p}+c_H)g_{2,p}^{\frac{n^{[1]}g_{1,p}}{n^{[1]}g_{1,p}+c_H}a_L+\frac{c_H}{n^{[1]}g_{1,p}+c_H}a_R}\end{aligned} \tag{2.26}$$

$\overset{f}{\geq}$ is explained as follows. Consider a random-variable B with a probability distribution defined as:

$$P_B(b) = \begin{cases}\frac{n^{[1]}g_{1,p}}{n^{[1]}g_{1,p}+c_H}, & b=a_L\\ \frac{c_H}{n^{[1]}g_{1,p}+c_H}, & b=a_R\end{cases}$$

Consider $f(B) = g_{2,p}^{B}$. As $f(B)$ is convex in B, from the Jensen's inequality, $\overset{f}{\geq}$ follows. From (2.21-2.26), and substituting $n(1-R_d) = c = n^{[1]} + c_H$,

$$0 \geq 1 - \sum_{j=1}^{J} p_j C_j - (1-R_d)\Bigg(1 - \frac{1}{2\log 2} \cdot \Bigg\{ \frac{n^{[1]} g_{1,1} + c_H}{n^{[1]} + c_H} g_{2,1}^{\frac{n^{[1]} g_{1,1}}{n^{[1]} g_{1,1} + c_H} a_L + \frac{c_H}{n^{[1]} g_{1,1} + c_H} a_R} \Bigg\} \Bigg) \tag{2.27}$$

We make the following substitutions in the above equations $c_H = (1-R_H)n^{[2]}$, $n^{[1]} = p_1 n$ and $n^{[2]} = p_2 n$, where R_H is the rate of the lower LDPC code:

$$0 \geq 1 - \sum_{j=1}^{J} p_j C_j - (1-R_d)\Bigg(1 - \frac{1}{2\log 2} \cdot \Bigg\{ \frac{p_1 g_{1,1} + (1-R_H)p_2}{p_1 + (1-R_H)p_2} g_{2,1}^{\frac{p_1 g_{1,1} a_L + (1-R_H)p_2 a_R}{p_1 g_{1,1} + (1-R_H)p_2}} \Bigg\} \Bigg) \tag{2.28}$$

By replacing $C_1 = C$, $C_2 = (1-p)C$ and solving for R_d in the above equation, we obtain the desired bound. □

2.7.2 Proof of Theorem 2

Proof. The equations (2.17) can be represented as

$$x_2 = \psi_A(x_2, x_3), \qquad\qquad x_3 = \psi_B(x_2, x_3)$$

Consider a fixed point in the density-evolution $(x_2, x_3) = (x_2^o, x_3^o)$. The above functions can be linearly approximated in the neighbor of the fixed point as follows,

$$\psi_A(x_2, x_3) = x_2^o + \left[\frac{\partial \psi_A}{\partial x_2} + \frac{\partial \psi_A}{\partial x_3}\frac{dx_3}{dx_2}\right](x_2 - x_2^o) + o(x_2 - x_2^o)^2 \tag{2.29}$$

Since $x_3 = \psi_B(x_2, x_3)$, taking derivatives on both sides,

$$\frac{dx_3}{dx_2} = \frac{\partial \psi_B}{\partial x_2} + \frac{\partial \psi_B}{\partial x_3}\frac{dx_3}{dx_2} \tag{2.30}$$

Substituting $\frac{dx_3}{dx_2}$ from (2.30) into (2.29),

$$\psi_A(x_2, x_3) = x_2^o + \left[\frac{\partial \psi_A}{\partial x_2} + \frac{\partial \psi_A}{\partial x_3}\frac{\frac{\partial \psi_B}{\partial x_2}}{1 - \frac{\partial \psi_B}{\partial x_3}}\right](x_2 - x_2^o)$$

$$+ o(x_2 - x_2^o)^2$$

For stability, $\left[\frac{\partial \psi_A}{\partial x_2} + \frac{\partial \psi_A}{\partial x_3} \frac{\frac{\partial \psi_B}{\partial x_2}}{1-\frac{\partial \psi_B}{\partial x_3}}\right] < 1$. Evaluating the derivatives and substituting $x_2^o = x_3^o = 0$, the result is obtained. □

Chapter 3

Applications of Regular LDGM-LDPC Codes to the Type-II Binary Symmetric Wiretap Channel

3.1 Introduction

The popularity of wireless communications has led to new security issues. Wireless devices have numerous applications: communications, health care, computer peripherals, home automation, gaming, etc. The broadcast nature of wireless devices makes them vulnerable to eavesdropping. Traditionally, cryptographic mechanisms are used to solve this problem. Cryptographic mechanisms require infrastructure to support passwords and key exchange. In this chapter, we study techniques that use error-correcting codes to provide secrecy without requiring cryptographic infrastructure. These techniques achieve secrecy by exploiting the statistical properties of the noise in the channel between the transmitter and the eavesdropper [17].

The information theoretic approach to secrecy was pioneered by Shannon [16]. Wyner [18] proposed the *wiretap channel* model to study data transmission in the presence of an eavesdropper. In this model, discrete memoryless channels were used to model communication links from the transmitter to the legitimate receiver and the eavesdropper. Wyner determined the rates at which information could be transmitted to the receiver while keeping the eavesdropper completely ignorant. Wyner and Ozarow [19] considered a special case of the wiretap channel model in which the channel between the transmitter and the legitimate receiver was noiseless. This model was called the type-II wiretap channel.

Low density parity check codes were used for secure code design in type-II binary erasure wiretap channels in [25]. In that work, error detection codes were also used for secure code design of type-II binary symmetric wiretap channels. The authors of [24]

solved the problem of secure coding for a general class of type-II wiretap channels, in which the main channel was noiseless and the eavesdropper channel was a binary input symmetric output memoryless (BISOM) channel. The problem was solved by proving that a BISOM channel was a degraded version of a binary erasure channel. Secure codes were then designed to achieve perfect secrecy for the binary erasure channel. It was shown that this secure code design achieved perfect secrecy of the type-II BISOM wiretap channel.

More recently, low-density generator-matrix/low-density parity-check (LDGM-LDPC) codes have been studied in [6] and [20]. This code ensemble results from compounding factor graphs of randomly chosen regular LDGM and LDPC codes. These codes are shown to achieve the capacity of the binary symmetric channel under typical-pairs decoding. While previous works [24] and [25] have proposed approaches to achieve perfect secrecy, there is a gap between the achieved transmission rates and the secrecy capacity.

This chapter focuses on designing secure codes to achieve the secrecy capacity of the type-II binary symmetric wiretap channel. To achieve that goal, we construct secure nested codes based on regular LDGM-LDPC codes of [20]. In this approach, the space of vectors, $\{0,1\}^n$ is partitioned by a sub-code and its corresponding cosets. The sub-code is an LDGM-LDPC code sequence that achieves the capacity of the eavesdropper channel. A scheme to transmit confidential messages using this partition is proposed. It is shown that the proposed coding scheme achieves the secrecy capacity of the type-II binary symmetric wiretap channel. Finally, we choose specific LDGM-LDPC codes and compute their noise thresholds using typical-pairs decoding. These results demonstrate how such codes can be used to achieve rates on the secrecy capacity curve. The chapter is organized as follows. We introduce some definitions and background concepts in Section 3.2. An approach for secure nested codes for the type-II binary symmetric wiretap channel is studied in Section 3.3. This is followed by a discussion of the performance of the proposed approach in Section 3.4. The equivocation rate is compared to the transmission rate and the cross-over probability of the eavesdropper channel.

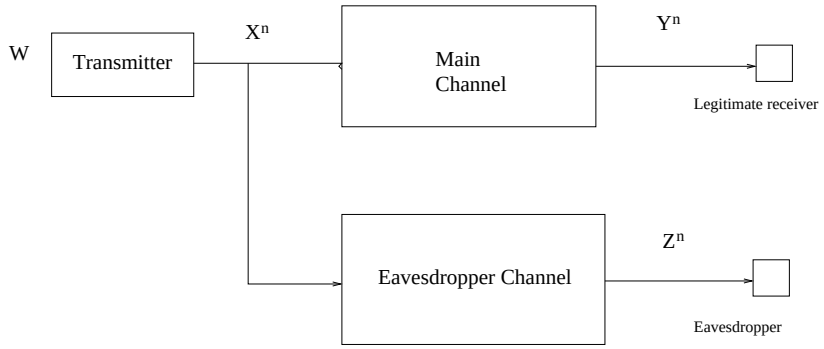

Figure 3.1: The wiretap channel model

3.2 Preliminaries

3.2.1 Wiretap Channels and Secrecy Coding

As shown in Fig. 3.1, the wiretap channel model consists of the transmitter, the legitimate receiver, and an eavesdropper. The transmitter sends a confidential message W to the legitimate receiver. The confidential message W is chosen uniformly from the set of all messages, $\{1, \ldots, M\}$. The transmitter encodes the message W into a binary sequence $X^n = \{X_1, \ldots, X_n\}$. Let Y^n and Z^n be the received sequences at the legitimate receiver and the eavesdropper, respectively, given that X^n was transmitted. The goal of secrecy coding is two fold. The transmitter must be able to communicate with the legitimate receiver at rate R such that the messages can be decoded by the legitimate receiver with error probability $P_e \to 0$ as code length $n \to \infty$ (*reliability*). The uncertainty about the message at the eavesdropper $\frac{H(W|Z^n)}{n}$ must be larger than or equal to the design *equivocation rate* R_e, i.e. $\lim_{n\to\infty} \frac{H(W|Z^n)}{n} \geq R_e$ (*confidentiality*). If the above two conditions are satisfied, the rate pair (R, R_e) is said to be achievable. If $R = R_e$, the eavesdropper is completely ignorant about the transmitted message. We say that the encoding scheme achieves perfect secrecy.

3.2.2 Random Bins and Secure Nested Codes

Wyner [18] proposed a solution to the secrecy coding problem for wiretap channels. A code C was randomly partitioned into *bins* $\{C_1, \ldots, C_M\}$. To transmit a message $W = i$, a codeword was uniformly chosen from the bin C_i and transmitted. The code

C had enough redundancy to defeat the noise in the main channel (Fig. 3.1). On the other hand, the noise in the eavesdropper channel prevented the eavesdropper from determining which bin the transmitted codeword came from. Structured codes which solve the problem of secure code design over wiretap channels are based on the intuitions provided by Wyner's random binning scheme. Let $\{C(n)\}$ denote a sequence of binary linear codes, where $C(n)$ is a (n, k_n) code having a common rate $R_c = \frac{k_n}{n}$. Following [24], we define a secure code sequence as follows:

Definition 3. *Secure Code Sequence:* $\{C_0(n), C_1(n)\}$ *is a secure nested code sequence if* $C_0(n)$ *is a fine code of rate* R_0 *and* $C_1(n)$ *is a coarse code of rate* R_1 *so that* $C_1(n) \subseteq C_0(n)$ *and* $R_1 \leq R_0$*. The information rate of this code sequence is* $R_0 - R_1$*.*

The secure code sequence is chosen such that it satisfies the *confidentiality* and *reliability* requirements (Section 3.2.1).

Definition 4. Type-II Binary Symmetric Wiretap Channel*: Consider a wiretap channel (Fig. 3.1). If the main channel is noiseless and the eavesdropper channel is a binary-symmetric memoryless channel with crossover probability* p*, the resulting channel is a type-II binary symmetric wiretap channel.*

Definition 5. Secrecy Capacity*: The secrecy capacity is the maximum possible rate at which the transmitter can communicate with the legitimate receiver (with arbitrarily low probability of error) such that the eavesdropper is completely ignorant of the transmitted message.*

The secrecy capacity for the wiretap channel was established in [26] as

$$C_s = \max_{p(X)}[I(X;Y) - I(X;Z)]$$

For the type-II binary symmetric wiretap channel, $C_s = h_2(p)$, where $h_2(.)$ is the binary entropy function:

$$h_2(p) = -p\log_2 p - (1-p)\log_2(1-p).$$

Similarly, $h(p) = -p\log p - (1-p)\log(1-p)$.

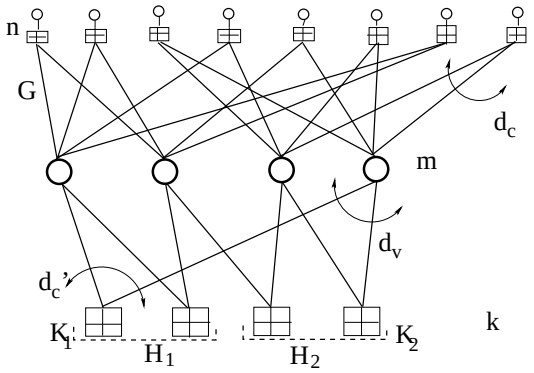

Figure 3.2: The regular LDGM-LDPC compound construction

3.2.3 LDGM-LDPC Codes

LDGM-LDPC codes were proposed in [6] and [20]. This code ensemble is based on compounding the factor graph of a randomly-chosen regular low-density generator-matrix (LDGM) code, with a randomly-chosen regular low-density parity-check (LDPC) code (Fig. 3.2). We now discuss the nesting properties of the LDGM-LDPC codes.

Let x^n be a codeword of the LDGM-LDPC code C; then

$$\begin{aligned} C = \{x^n \in \{0,1\}^n : x^n = Gy^m \text{ for some} \\ y^m \in \{0,1\}^m \text{ such that } Hy^m = 0\}. \end{aligned} \tag{3.1}$$

where G and H denote the generator-matrix of the LDGM layer and the parity-check matrix of the LDPC layer, respectively. Partition the k lower parity checks into two sets K_1 and K_2 (Fig. 3.2). The number of parity checks in K_1 and K_2 are k_1 and k_2, respectively. Let the parity check matrices for K_1 and K_2 be H_1 and H_2, respectively. Then, the code $C(G, H_1)$ is defined as follows:

$$\begin{aligned} C(G,H_1) = \{x^n \in \{0,1\}^n : x^n = Gy^m \text{ for some} \\ y^m \in \{0,1\}^m \text{ such that } H_1 y^m = 0\}. \end{aligned} \tag{3.2}$$

This code consists of codewords which satisfy the parity checks in K_1 alone. For a sequence $r \in \{0,1\}^{k_2}$, the code $C(r)$ is defined as follows:

$$\begin{aligned} C(r) = \{x^n \in \{0,1\}^n : x^n = Gy^m \text{ for some} \\ y^m \in \{0,1\}^m \text{ such that } \begin{pmatrix} H_1 \\ H_2 \end{pmatrix} y^m = \begin{pmatrix} 0 \\ r \end{pmatrix}\}. \end{aligned} \tag{3.3}$$

$C(r)$ satisfies all the parity checks in K_1 and leaves a syndrome with the parity checks in K_2. Clearly, $C(r) \subseteq C(G, H_1)$ as codewords in $C(r)$ satisfy *at least* all the constraints of K_1. $C(r)$ forms partitions of $C(G, H_1)$ such that $C(G, H_1) = \cup_{r \in \{0,1\}^{k_2}} C(r)$.

3.3 Secure code design for Type-II Binary symmetric wiretap channel

In this section, we study secure codes for a type-II binary symmetric wire-tap channel based on the LDGM-LDPC code sequence. Let $C_0(n) = \{0, 1\}^n$ and let $C_1(n)$ be a sequence of LDGM-LDPC codes which achieve the capacity of the binary symmetric channel with cross-over probability p. The set of vectors $\{0, 1\}^n$ is partitioned into sub-codes $\{C_1, \ldots, C_M\}$ by $C_1(n)$ and its co-sets. To transmit the confidential message $W = i$, the transmitter chooses a codeword uniformly from the co-set $C_i(n)$ and transmits it. Now we have the following result:

Theorem 3. *Consider a sequence of secure nested codes $\{C_0(n), C_1(n)\}$, where $C_0(n) = \{0, 1\}^n$ and $C_1(n)$ is an LDGM-LDPC code sequence achieving the capacity of the binary symmetric channel with cross-over probability p (the eavesdropper channel). Suppose that the secure code sequence $\{C_0(n), C_1(n)\}$ is transmitted over the type-II binary symmetric wiretap channel, then, the rate-equivocation pair*

$$(R, R_e) = (h_2(p), h_2(p)) \tag{3.4}$$

is achievable.

Proof. The secrecy capacity of the type-II binary symmetric wiretap channel is shown in [26] to be $h_2(p)$. We need to prove that the rate-equivocation pair $(R, R_e) = (h_2(p), h_2(p))$ is achievable. Following the approach of [24, Appendix A], we compute

$H(W|Z^n)$, the equivocation of the transmitted message at the eavesdropper:

$$\begin{aligned} H(W|Z^n) &= H(W, Z^n) - H(Z^n) \\ &= H(W, X^n, Z^n) - H(Z^n) - H(X^n|W, Z^n) \\ &= H(X^n) + H(W, Z^n|X^n) - H(Z^n) \\ &\quad - H(X^n|W, Z^n) \\ &\geq H(X^n) + H(Z^n|X^n) - H(Z^n) \\ &\quad - H(X^n|W, Z^n) \\ &= H(X^n) - I(X^n; Z^n) - H(X^n|W, Z^n) \\ &\geq n - nC_{\text{BSC}} - H(X^n|W, Z^n) \end{aligned} \tag{3.5}$$

where $C_{\text{BSC}} = 1 - h_2(p)$ is the capacity of the binary symmetric channel. Consider the term $H(X^n|W, Z^n)$. Suppose the transmitted message is $W = w$. Based on the encoding procedure described in Section 3.3, X^n is uniformly chosen from the co-set C_w. By applying Fano's inequality, we obtain

$$H(X^n|W = w, Z^n) \leq 1 + nP_e(w)R_1 = n\epsilon \tag{3.6}$$

where $P_e(w)$ denotes the average probability of error under Maximum-likelihood (ML) decoding at the eavesdropper incurred by using coset C_w and ϵ is small when n is large. Since the co-set C_w shares the same Hamming distance properties of C_1, we have $P_e(W = w) = P_e(W = 1) = \lim_{n\to\infty} 0$, i.e., the probability of error vanishes to 0 where n is large. Now, we have

$$H(X^n|W, Z^n) = \frac{1}{M}\sum_{w=1}^{M} H(X^n|W = w, Z^n) \leq n\epsilon. \tag{3.7}$$

Substituting this result into (3.5), we get $H(W|Z^n) \geq n - nC_{BSC} = nh_2(p)$. Hence, the rate pair $(R, R_e) = (h_2(p), h_2(p))$ is achievable. □

3.4 Numerical Examples

In this section, the performance of the proposed secure code sequence for the Type-II binary symmetric wiretap channel is discussed. We look at specific examples of

LDGM-LDPC codes and determine the secrecy rates they achieve. Towards that end, we determine the *noise thresholds* these codes achieve. Consider a channel characterized by one parameter. The noise threshold of a code over this channel is the worst value of the channel noise parameter at which decoding of the given code is possible at arbitrarily small error probability. We consider the crossover probability of the binary symmetric channel as the channel noise parameter. Using typical-pair decoding [22, Chapter 6], we numerically calculate the noise thresholds for some regular LDGM-LDPC codes based on the weight spectrum of the LDGM-LDPC code ensemble. The weight spectrum of the LDGM-LDPC ensemble is described in the Appendix. As shown in Table 3.1, we derive the noise thresholds of several LDGM-LDPC code ensembles. In particular, we choose LDGM-LDPC codes with LDGM degree $d_c = 2$. The LDPC degrees are varied to get different rates. In Table 3.1, we compare the Shannon threshold p_{sh} with the noise threshold $p_{2,j,k}$ of the LDGM-LDPC codes for the binary symmetric channels. It is observed that the achieved noise threshold $p_{2,j,k}$ achieves the Shannon limit. The

$(2, j, k)$	R	p_{sh}	$p_{2,j,k}$
$(2, 2, 8)$	0.75	0.0416	0.0416
$(2, 2, 7)$	0.714	0.0498	0.0498
$(2, 2, 5)$	0.6	0.0793	0.0793
$(2, 4, 8)$	0.5	0.11	0.11
$(2, 3, 5)$	0.4	0.1461	0.1461
$(2, 4, 6)$	0.33	0.17395	0.17395
$(2, 3, 4)$	0.25	0.2145	0.2145

Table 3.1: Noise thresholds of some regular LDGM-LDPC codes

secrecy capacity is plotted as a function of the crossover probability of the eavesdropper channel in Fig. 3.3. Also shown are the highest achievable rates with the best known techniques. The use of error detection codes [23] gives a best secrecy rate of $-\log(1-p)$ as shown in the figure. Using a degraded erasure channel [24] gives a best secrecy rate of $2p$. The secure coding sequence proposed in this chapter (Theorem 3) achieves a secrecy rate of $h_2(p)$. The secrecy rates that the $(2, j, k)$ LDGM-LDPC codes achieve are shown in Fig. 3.3. The rate achieved by each code is marked on the secrecy capacity curve. The secrecy capacity curve for the type-II binary symmetric wiretap channel in Fig. 3.3 overlaps with the secrecy rate achieved by the proposed coding scheme.

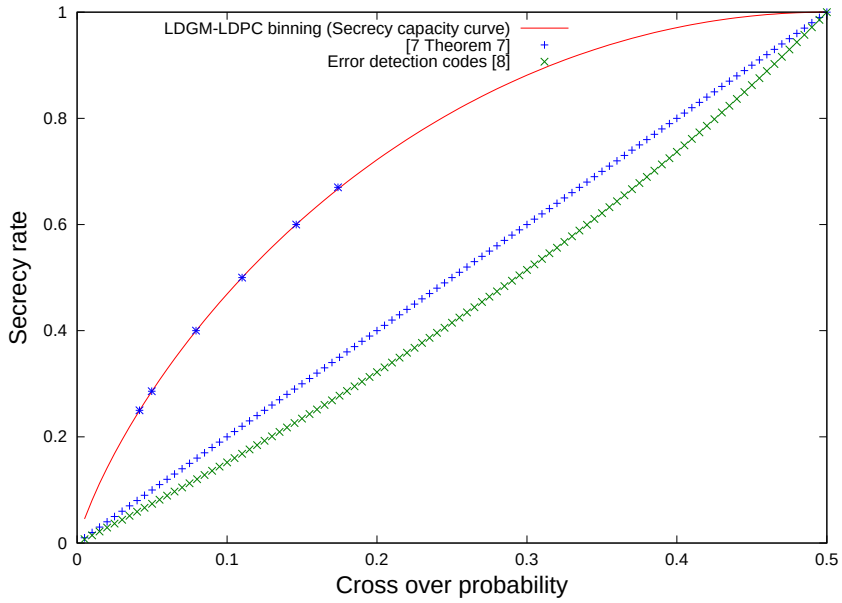

Figure 3.3: Secrecy rate that can be achieved using LDGM-LDPC binning

The boundaries of the equivocation rate vs. the transmission rate for the type-II binary symmetric(0.214) wiretap channel are shown in Fig. 3.4. At $p = 0.214$, the equivocation rate rises linearly with transmission rate till the rate is 0.75. This rate pair $(R_e, R) = (0.75, 0.75)$ can be achieved by a $(2, 3, 4)$ LDGM-LDPC code. The rate pair $(R_e, R) = (0.42, 0.42)$ can be achieved by using a dual of a good code for the binary erasure channel as shown in [24]. Any point (R_e, R) on the straight line between $(0.42, 0.42)$ and $(0.75, 0.75)$ can be achieved by time-sharing. The capacity equivocation region [18] for the type-II binary symmetric wiretap channel $X \rightarrow (Y, Z)$ with cross-over probability p consists of transmission-equivocation rate pairs (R, R_e) satisfying

$$R_e \leq R \leq \max_{p(X)} I(X;Y) = 1$$
$$0 \leq R_e \leq \max_{p(X)} I(X;Y) - I(X;Z) = h_2(p).$$

For our example above, that means $0 \leq R_e \leq 0.75$ and $R_e \leq R \leq 1$. The transmission-equivocation region achieved by LDGM-LDPC secure code sequences is identical to the region achievable in Wyner's random binning scheme.

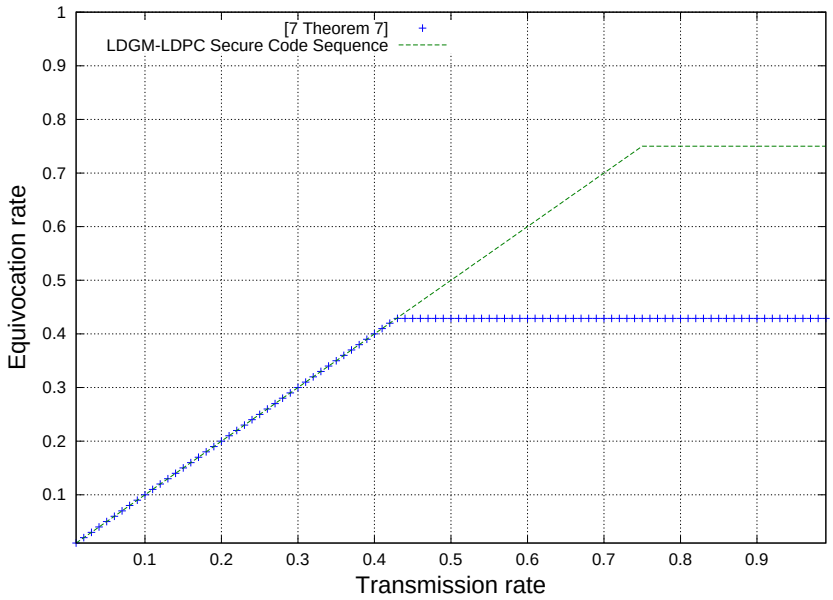

Figure 3.4: Rate, equivocation region which can be achieved for the type-II BSWT(0.214) channel

3.5 Chapter Summary

This chapter has used capacity achieving LDGM-LDPC codes as coarse codes to partition the space of binary vectors $\{0,1\}^n$. It has been seen that this results in a secure nested code which achieves the secrecy capacity of the type-II binary symmetric wiretap channel. We have compared the performance of the scheme with previous results. Further, we have demonstrated this result using some specific LDGM-LDPC codes.

3.6 Appendix

3.6.1 Spectrum of regular LDGM-LDPC Codes

An upper-bound on the weight-spectrum of the LDGM-LDPC codes was derived in [6, Section 3.3]. However, [6] assumed a (d, c) LDGM upper-code, i.e. both the check-nodes and variable-nodes in the factor-graph of the upper LDGM code were assumed to be regular. Further, the upper LDGM code was assumed to be rate-1, i.e. $d = c$. An upper-bound on the asymptotic-spectrum of the LDGM-LDPC codes is derived in this

section after relaxing the above two conditions. The upper-bound on the asymptotic-spectrum is used to calculate the noise-thresholds of the LDGM-LDPC codes over the binary-symmetric-memoryless channel. Consider a regular LDGM-LDPC code ensemble with a randomly-chosen LDGM generator-matrix G and a randomly-chosen parity-check matrix H respectively (as defined in Section 3.2.3). Let X^n and V^m denote the LDGM-LDPC codeword and the lower LDPC code-word respectively, such that $X^n = V^m G$ and $V^m H^T = 0$, where H^T is the transpose of the matrix H. Let $A_{\text{LDGM-LDPC}}(n\delta)$ denote the ensemble-averaged LDGM-LDPC weight-enumerator of the above code, where $\delta \in [0, 1]$. Then, the ensemble-averaged weight-enumerator can be upper-bounded as follows:

$$A_{\text{LDGM-LDPC}}(n\delta) \leq \sum_{l=0}^{m} \frac{A_{\text{LDPC}}(l)}{\binom{m}{l}} Z(n\delta, l). \tag{3.8}$$

where $A_{\text{LDPC}}(l)$ is the ensemble-averaged weight-enumerator of the lower LDPC code (determined by Litsyn et. al. in [28]) and $Z(n\delta, l)$ is the number of LDGM code-words with input-weight l and output-weight $n\delta$ for a randomly chosen LDGM code. The equation (3.8) is an inequality because different LDPC code-words could result in the same LDGM-LDPC code-word (leading to an over-count). Following [33], we have

$$Z(n\delta, l) = \binom{m}{l} P(\text{wt}(X^n) = n\delta | \text{wt}(V^m) = l) \tag{3.9}$$

Thus,

$$\begin{aligned} A_{\text{LDGM-LDPC}}(n\delta) \leq & \sum_{l=0}^{m} A_{\text{LDPC}}(l) \\ & P(\text{wt}(X^n) = n\delta | \text{wt}(V^m) = l). \end{aligned} \tag{3.10}$$

If the weight of the input sequence applied to a randomly chosen LDGM code is l, then by [21, Appendix A], $X^n = \{X_1, \ldots, X_n\}$ is a sequence of independent and identically distributed, binary, Bernoulli random variables with parameter $\delta^*(l) = \frac{1}{2}(1-(1-\frac{2l}{m})^{d_c})$, where d_c is the degree of the upper, regular, LDGM check-nodes. Furthermore, applying the method of types [27, Chapter 12], we obtain

$$P(\text{wt}(X^n) = n\delta | \text{wt}(V^m) = l) = \binom{n}{n\delta} e^{-n(h(\delta)+D(\delta||\delta^*(l))} \tag{3.11}$$

where $D(.)$ is the Kullback-Leibler distance between two probability distributions. By substituting $P(\mathrm{wt}(X^n) = n\delta|\mathrm{wt}(V^m) = l)$ into (3.10),

$$A_{\text{LDGM-LDPC}}(n\delta) \leq \binom{n}{n\delta} \sum_{l=0}^{m} A_{\text{LDPC}}(l). \\ e^{-n(h(\delta)+D(\delta||\delta^*(l))}. \tag{3.12}$$

In the limiting case of $n \to \infty$,

$$A_{\text{LDGM-LDPC}}(n\delta) \leq \sum_{l=0}^{m} A_{\text{LDPC}}(l) e^{-n(D(\delta||\delta^*(l))}. \tag{3.13}$$

The upper-bound on the spectrum of the LDGM-LDPC code is:

$$r(\delta) = \lim_{n\to\infty} \frac{1}{n} \log A_{\text{LDGM-LDPC}}(n\delta). \tag{3.14}$$

Then, the upper-bound on the weight-spectrum of the regular LDGM-LDPC code ensemble is given by

$$r(\delta) \leq \lim_{n\to\infty} \frac{1}{n} \log \sum_{l=0}^{m} A_{\text{LDPC}}(l) e^{-n(D(\delta||\delta^*(l))} \tag{3.15}$$

Using the bound on the weight-spectrum, the noise thresholds of these codes over a binary-symmetric channel with cross-over probability p are determined. The noise-thresholds are obtained using the typical-pairs approach of [22], which assumes that the weight-spectrum of the code in question satisfies assumptions 1 and 2 of [22, Section 6.4.1]. Two lemmas are presented to prove this to be true for the LDGM-LDPC codes.

Lemma 6. *Consider the upper-bound on the LDGM-LDPC weight-spectrum in (3.15). There exists a $\delta_0 \in (0, 1)$ such that $r(\delta) < 0$ for all $\delta \leq \delta_0$. (The quantity $n\delta_0$ is the minimum-distance of the code).*

Proof. From (3.15), $r(\delta) \leq R_G \max_{l\in[0,\ldots,m]} r^{\text{LDPC}}(\frac{l}{m}) - D(\delta||\delta * (\frac{l}{m}))$, where R_G is the upper LDGM rate and $r^{\text{LDPC}}(\frac{l}{m})$ is the asymptotic weight-spectrum of the lower LDPC code. Let $x = \frac{l}{m}$. We upper-bound $r^{\text{LDPC}}(x)$ from [33, Lemma 1] and expand the term $D(\delta||\delta * (\frac{l}{m}))$ to obtain,

$$r(\delta) \leq h(\delta) + \max_x R_G((1 - R_H + 1 - \delta) \log(1 + (1 - 2x)^{d_c'}) + \\ h(x) + (1 - R_H) \log 2) + \delta \log \delta^*(x) + (1 - \delta) \log(1 - \delta^*(x))$$

By using the definition of $\delta^*(x)$ and the observation that $\delta^*(x) \leq 0 \leq 1 - \delta^*(x)$, the above upper-bound simplifies to:

$$r(\delta) \leq h(\delta) + R_G h(x) - \log 2(R_G R_H + 1) + \\ (R_G(1 - R_H) + (1 - \delta)) \log(1 + (1 - 2x)^{\max(d_c^{'}, d_c)})$$

It is shown in [33, Theorem 1] that the above expression has a maxima at $x = \frac{1}{2}$ for a sufficiently large (but finite) $d_c^{'}$ or d_c. Substituting $x = \frac{1}{2}$ in the above equation, we obtain the bound $r(\delta) \leq h(\delta) - (1 - R_G R_H) \log 2$. From the previous bound, $\delta_0 = h^{-1}(1 - R_G R_H \log 2)$. □

Lemma 7. *Let $r_n(\delta)$ and $r(\delta)$ be the weight-spectrum and asymptotic weight-spectrum of the regular LDGM-LDPC codes. Then $r_n(\delta) - r(\delta) \leq \theta_n$ for a non-negative θ_n such that $\lim_{n\to\infty} \frac{n\theta_n}{d_n} = 0$, where d_n is the minimum-distance.*

Proof. From (3.12),

$$\begin{aligned} r_n(\delta) &\leq \frac{1}{n}(\log \binom{n}{n\delta} + R_G \max_{l \in [0,\ldots,m]} r_{\text{LDPC}}(\frac{l}{m}) - h(\delta) \\ &\quad - D(\delta || \delta^*(\frac{l}{m})) + \frac{\log m}{n} \\ &\leq \frac{1}{n}(\log \binom{n}{n\delta}) - h(\delta) + \frac{\log m}{n} + r(\delta) \end{aligned}$$

Clearly, as $n \to \infty$, $r_n(\delta) - r(\delta) = 0$. □

Chapter 4

Applications of Regular LDGM-LDPC Codes to Type-I Channels With a Binary Symmetric Eavesdropper

4.1 Introduction

This chapter focuses on designing secure codes to achieve perfect-secrecy of the type-I wiretap channel with an eavesdropper's channel that is a binary-symmetric channel (BSC). The main channel is assumed to be any BISOM channel. To achieve that goal, we construct secure nested codes based on regular LDGM-LDPC codes of [20]. In this approach, a regular LDGM-LDPC code is partitioned by a sub-code and its corresponding co-sets. The sub-code is another regular LDGM-LDPC code sequence that achieves the capacity of the eavesdropper channel. A scheme to transmit confidential messages using this partition is proposed. It is shown that the proposed coding scheme achieves the perfect secrecy of the type-I channel in question.

4.2 Preliminaries

Definition 6. *Binary-input symmetric-output memoryless (BISOM) channel: Consider a channel with binary-input:*

$$X \in \mathcal{X} \triangleq \{0, 1\}. \tag{4.1}$$

Let $\mathbb{R}$ be the set of real numbers. Let the output of the channel be $Y \in \mathcal{Y} \subseteq \mathbb{R}$, and let the channel transition probability be $P_{Y|X}(.|.)$. A channel is symmetric if:

$$P_{Y|X}[Y = y|X = 0] = P_{Y|X}[Y = -y|X = 1], \forall y \in \mathcal{Y}. \tag{4.2}$$

All memoryless channels satisfying (4.1) *and* (4.2) *are called BISOM channels.*

Definition 7. *Bhattacharrya parameter of a BISOM channel: Consider a BISOM channel (as per definition 6). The Bhattacharyya noise parameter of the above channel is defined as*

$$\gamma \triangleq \int_{y\in\mathcal{Y}} \left\{\sqrt{P_{Y|X}[Y=y|X=0]P_{Y|X}[Y=y|X=1]}\right\}dy \tag{4.3}$$

Definition 8. *Type-I (γ, p) wiretap channel: The type-I (γ, p) wiretap channel has a main channel that is a BISOM channel with Bhattacharrya noise parameter γ; the eavesdropper channel is a binary-symmetric channel (BSC) with cross-over probability p.*

4.3 Regular LDGM-LDPC Codes Achieve Capacity of the BSC

Theorem 4. *The ensemble of regular $(d_c, d_v, d_{c'})$ LDGM-LDPC codes achieves the capacity of the BSC with finite degrees under typical-pairs decoding.*

This theorem is proved in the appendix.

4.4 Cutoff Rates for Regular LDGM-LDPC Codes Over BISOM Channels

We now restate [31, Thm 5.1] for completeness. Let D_n be a sequence of integers such that

$$\frac{D_n}{n^\epsilon} \to 0, \qquad \frac{\log n}{D_n} \to 0, \qquad \forall \epsilon > 0 \tag{4.4}$$

Further,

$$c_0^{(n)} \triangleq \sup_{\frac{D_n}{n}<\delta\leq 1} \frac{r_n(\delta)}{\delta}, \qquad c_0 \triangleq \limsup_{n\to\infty} c_0^{(n)} \tag{4.5}$$

where $r_n(\delta)$ is the spectrum of the length n code under discussion.

Theorem 5. *[31, Thm. 5.1] : Suppose the ensemble threshold c_0 (defined in (4.5)) is finite and $\alpha = -\log\gamma$ such that $\alpha > c_0$. Then if $\bar{P}_W^{(n)}$ denotes the ensemble averaged maximum-likelihood (ML) decoder error probability, there exists an integer n_0 and*

positive constants K and ϵ such that for $n > n_0$,

$$\bar{P}_W^{(n)} \leq Z^{(n)}(D_n) + Ke^{-\epsilon D_n}$$

where $Z^{(n)}(D) \triangleq \sum_{h=1}^{D} \bar{A}_h^{(n)}$, where $\bar{A}_h^{(n)}$ is the ensemble averaged weight enumerator of the code in question.

An upper bound on the asymptotic spectrum of the regular LDGM-LDPC codes is derived in (4.11) in the Appendix as

$$r(\delta) \leq H(\delta) - \log 2(1 - R) \tag{4.6}$$

where R is the rate of the code. Using (4.6) and (4.5), the following result is proved.

Lemma 8. *For a regular LDGM-LDPC code with rate R, the ensemble threshold c_0 is bounded as:*

$$c_0 \leq \log \frac{1}{2^{1-R} - 1}$$

This lemma is proved in the appendix.

Theorem 6. *Consider a regular LDGM-LDPC code with c_0 satisfying Lemma 8. Then, if $\alpha = -\log \gamma > \log \frac{1}{2^{1-R}-1}$, the ensemble maximum-likelihood decoder error probability $\bar{P}_W^{(n)}$ goes to 0 for large code-lengths n.*

Proof. If $\alpha = -\log \gamma > \log \frac{1}{2^{1-R}-1} \implies \alpha > c_0$ as $c_0 \leq \log \frac{1}{2^{1-R}-1}$, which follows from Lemma 8. From Theorem 5, $\bar{P}_W^{(n)}$ goes to 0 as $n \to \infty$. □

Lemma 9. *Consider a regular LDGM-LDPC code transmitted over the BISOM with Bhattacharrya noise-parameter γ. If $R < 1 - \log_2(1 + \gamma)$, $\bar{P}_W^{(n)}$ goes to 0 as $n \to \infty$ under maximum likelihood decoding.*

Proof. The lemma follows from Theorem 6. □

We observe that the upper-bound on the rate in Lemma 9 is identical to the *cut-off rate* for the BISOM channel [31].

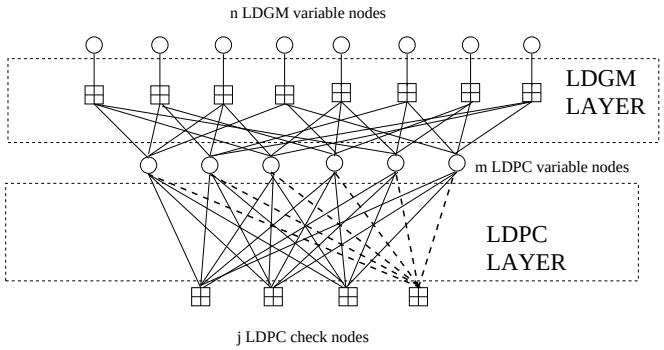

Figure 4.1: A nested regular LDGM-LDPC construction

4.5 A Nested Code Construction Based on LDGM-LDPC Codes

A nested LDGM-LDPC construction is proposed in this section. First, a regular LDGM-LDPC code is defined.

Definition 9. $(d_c, d_v, d_{c'})$ *regular LDGM-LDPC code: In this code, each of the* n *accumulate nodes (the parity-checks) connected to the* n *LDGM variable nodes are connected to* d_c *LDPC variable nodes. Further, each LDPC variable node is connected to* d_v *LDPC check nodes; each LDPC check-node is connected to* $d_{c'}$ *LDPC variable nodes.*

As an example, a $(3, 4, 6)$ regular LDGM-LDPC code is shown in Figure 4.1.

Definition 10. *Nested* $(d_c, d_v, d_{v_2}, d_{c'})$ *regular LDGM-LDPC code: Consider a* $(d_c, d_v, d_{c'})$ *regular LDGM-LDPC code as defined in definition 9. The above code is a nested* $(d_c, d_v, d_{v_2}, d_{c'})$ *regular LDGM-LDPC code if removing a given set of LDPC parity-checks results in a* $(d_c, d_{v_2}, d_{c'})$ *regular LDGM-LDPC code.*

As an example, consider the $(3, 4, 6)$ regular LDGM-LDPC code illustrated in Figure 4.1. Removing the last LDPC parity-check (and the corresponding edges connected to the removed parity-check) results in a $(3, 3, 6)$ regular LDGM-LDPC code. Thus, as per definition 10, the code in Figure 4.1 is a nested $(3, 4, 3, 6)$ regular LDGM-LDPC code. This chapter assumes that the rate of the lower LDPC code R_H of the nested regular LDGM-LDPC codes agrees with the design rate $1 - \frac{d_v}{d_{c'}}$. A similar assumption is made about the rate of the randomly chosen lower LDPC code (after removal of the LDPC checks) $R_{H'}$, and its design rate $1 - \frac{d_{v_2}}{d_{c'}}$. This assumption is justified for codes

with large block-lengths by [30, lemma 3.27] which is re-stated for completeness.

Lemma 10. *[30, Lemma 3.27]: Consider the $(d_v, d_{c'})$ regular LDPC code with length m and with $2 \leq d_v < d_{c'}$. Let the design rate of the ensemble be $r(d_v, d_{c'}) = 1 - \frac{d_v}{d_{c'}}$. Let H be the parity-check matrix of a randomly chosen code from this ensemble with rate $r(H)$. Then,*

$$P\Big[r(H) = r(d_v, d_{c'}) + \frac{\nu}{m}\Big] = 1 - o_m(1)$$

where $\nu = 1$ if d_v is even and 0 otherwise.

Note 1. *Rank of the parity-check matrix of the lower LDPC code: Consider the length m lower LDPC code in the nested $(d_c, d_v, d_{v_2}, d_{c'})$ regular LDGM-LDPC code. It follows from Lemma 10 that the parity-check matrix H of the lower $(d_v, d_c^{'})$ LDPC code is full rank with probability 1 for $m \to \infty$. Removal of parity-checks from the factor graph of the LDPC code (as shown in fig. 4.1) involves removal of the corresponding rows of the full-rank matrix H. The resulting matrix is also full rank with probability 1 for $m \to \infty$.*

4.6 Secure Code Sequence for the Type-I Wiretap (WT) Channel

In this section, a secure code sequence for the type-I (γ, p) wiretap channel is proposed.

Lemma 11. *Consider a type-I (γ, p) WT channel where the main and eavesdropper channels are BISOM channels with capacities C_M and C_E respectively. Let the main channel be less noisy than the eavesdropper channel. Then, the secrecy capacity of such a type-I channel is*

$$C_s = C_M - C_E$$

Proof. Since both the main and eavesdropper channels are BISOM channels, the input distribution that maximizes the mutual information $I(X;Y)$ and $I(X;Z)$ is the uniform distribution. As per [32], since the main channel is less noisy than the eavesdropper channel and the same (uniform) distribution on X maximizes $I(X^n;Y^n)$ and $I(X^n;Z^n)$, the secrecy capacity of such a wiretap channel is the difference between the capacities of the main channel channel and eavesdropper channels respectively. Thus, the result. □

The main theorem of the chapter is now stated.

Theorem 7. *Consider a regular nested $(d_c, d_v, d_{v_2}, d_{c'})$ LDGM-LDPC code. Further, consider a type-I (γ, p) wiretap channel such that the main channel is a BISOM channel with Bhattacharrya noise-parameter γ and the eavesdropper channel is a BSC with cross-over probability p. Let $C_1(n)$ be the regular $(d_c, d_v, d_{c'})$ LDGM-LDPC code that achieves the capacity of the eavesdropper's channel. Further, Let $C_0(n)$ be the nested regular $(d_c, d_{v_2}, d_{c'})$ LDGM-LDPC code that results on removing a specific number of LDPC check nodes. Then, the secure code sequence $(C_0(n), C_1(n))$ has the following properties.*

- *The proposed secure code sequence achieves perfect secrecy.*
- *The maximum information rate of the resulting secure code sequence is $h_2(p) - \log_2(1+\gamma)$ under maximum likelihood decoding, where $h_2(.)$ is the binary entropy function such that $h_2(x) = x\log_2\frac{1}{x} + (1-x)\log_2\frac{1}{1-x}$ and γ is the Bhattacharrya noise parameter of the main channel.*

Proof. For asymptotic code lengths, it follows from Lemma 10 that a randomly chosen LDPC code has rate that equals the design rate with probability $1 - o_m(1)$. Assuming a full rank LDGM generator matrix G, the fine code is chosen to achieve the capacity of the eavesdropper's channel (this is possible as per Theorem 4). As the code $C_1(n)$ is capacity achieving for the eavesdropper channel, as per [25, Theorem1], the secure code sequence achieves perfect secrecy of the type-I (γ, p) wiretap channel. As per Lemma 9, the nested regular LDGM-LDPC code can achieve a rate upto the cut-off rate $R_0 \leq 1 - \log_2(1+\gamma)$ and still be decoded by the receiver with an arbitrarily low error-probability under maximum-likelihood decoding. Thus, from definition 3, the rate of the secure code sequence is upper-bounded by $(1 - \log_2(1+\gamma)) - (1 - h_2(p)) = h_2(p) - \log_2(1+\gamma)$. □

4.7 Chapter Summary

A type-I wiretap channel was studied in this chapter with a BISOM main channel and a binary symmetric eavesdropper channel. A secure code sequence for this channel was proposed using a special construction of the regular LDGM-LDPC codes. It was shown that this construction achieved perfect secrecy.

4.8 Appendix

4.8.1 Proof of Theorem 4

Proof. An upper bound on the asymptotic-spectrum of the regular $(d_c, d_v, d_{c'})$ LDGM-LDPC codes was determined in [29] as:

$$r(\delta) = \max_{\frac{l}{m}\in(0,1)} \Big\{ R_G \; r_L\Big(\frac{l}{m}\Big) - D\Big(\delta||\delta^*\Big(\frac{l}{m}\Big)\Big)\Big\} \tag{4.7}$$

where R_G is the rate of the upper LDGM code, $r_L(.)$ is the asymptotic spectrum of the lower $(d_v, d_{c'})$ LDPC code, m is the code-length of the lower LDPC code, $D(.||.)$ is the Kullback-Leibler divergence between two distributions and $\delta^*(\frac{l}{m}) = \frac{1}{2}(1-(1-2\frac{l}{m})^{d_c})$. As per [33, lemma 1], for $x \in [0,1]$, the LDPC spectrum can be upper-bounded as,

$$\begin{aligned} r_L(x) \leq (1-R_H)\log(1+(1-2x)^{d_{c'}}) + H(x) \\ - (1-R_H)\log 2 \end{aligned} \tag{4.8}$$

where R_H is the rate of the lower LDPC code and $H(.)$ is the entropy function. The term $D(\delta||\delta^*(x))$ can be written as:

$$\begin{aligned} D(\delta||\delta^*(x)) &= \delta \log \frac{2\delta}{(1-(1-2x)^{d_c})} + \\ &\quad (1-\delta)\log\frac{2(1-\delta)}{(1+(1-2x)^{d_c})} \\ &= \log 2 - H(\delta) - \delta\log(1-(1-2x)^{d_c}) \\ &\quad - (1-\delta)\log(1+(1-2x)^{d_c}) \end{aligned} \tag{4.9}$$

Substituting (4.9) and (4.8) into (4.7),

$$\begin{aligned} r(\delta) &= \max_{x\in(0,1)}\{R_G(1-R_H)\log(1+(1-2x)^{d_{c'}})+ \\ &\quad R_G H(x) - R_G(1-R_H)\log 2 - \log 2 + H(\delta)+ \\ &\quad \delta\log(1-(1-2x)^{d_c}) - (1-\delta)\log(1+(1-2x)^{d_c})\} \\ &\overset{a}{\leq} \max_{x\in(0,1)}\{R_G(1-R_H)\log(1+(1-2x)^{d_{c'}})+ \\ &\quad R_G H(x) - R_G(1-R_H)\log 2 - \log 2 + H(\delta)+ \\ &\quad -(1-\delta)\log(1+(1-2x)^{d_c})\} \end{aligned} \tag{4.10}$$

where $\overset{a}{\leq}$ results because $\log(1-(1-2x)^{d_c}) \leq 0$, for $x \in [0,1]$. By choosing a large enough d_c and $d_{c'}$, the terms $\log(1+(1-2x)^{d_c})$ and $\log(1+(1-2x)^{d_{c'}})$ can be made as small as possible. Thus, (4.11) simplifies to,

$$\begin{aligned} r(\delta) &= \max_{x\in(0,1)}\{R_G H(x) - R_G(1-R_H)\log 2 - \log 2 + \\ &\quad H(\delta)\} = R_G\log 2 - R_G(1-R_H)\log 2 - \log 2 + H(\delta) \\ &= R_G R_H \log 2 - \log 2 + H(\delta) = H(\delta) - \log 2(1-R) \end{aligned} \tag{4.11}$$

where $R = R_G R_H$. A sufficient condition for the code with a spectrum bounded as in (4.11) to achieve arbitrarily small error-probability under typical-pair decoding was proved in [22] as

$$r(\delta) < H(\delta) - pH(\frac{\delta}{2p}) - (1-p)H(\frac{\delta}{2(1-p)}) \tag{4.12}$$

Substituting (4.11) into (4.12),

$$\begin{aligned} H(\delta) - \log 2(1-R) &< H(\delta) - pH(\frac{\delta}{2p}) - (1-p)H(\frac{\delta}{2(1-p)}) \\ \implies pH(\frac{\delta}{2p}) + (1-p)H(\frac{\delta}{2(1-p)}) &< \log 2(1-R) \end{aligned} \tag{4.13}$$

As per [22, (6.31)], the function $pH(\frac{\delta}{2p}) + (1-p)H(\frac{\delta}{2(1-p)})$ over $\delta \in [0, 2p]$ is maximized at $\delta = 2p(1-p)$. The maximum value of the function is $H(p)$. Thus,

$$H(p) < \log 2(1-R) \implies R < 1 - \frac{H(p)}{\log 2} \tag{4.14}$$

□

4.8.2 Proof of Lemma 8

Proof. By the definition of C_0 in (4.5),

$$c_0 = \sup_{0<\delta\leq 1} \frac{r(\delta)}{\delta} \overset{a}{\leq} \sup_{0<\delta\leq 1} \frac{H(\delta) - \log 2(1-R)}{\delta}$$

where $\overset{a}{\leq}$ follows from (4.11). The function $f(\delta) = \frac{H(\delta)-\log 2(1-R)}{\delta}$ is maximized with respect to δ by setting the first derivative to 0 as follows.

$$\begin{aligned} f^{'}(\delta) = \frac{H^{'}(\delta)}{\delta} - \frac{H(\delta) - \log 2(1-R)}{\delta^2} &= 0 \\ \overset{b}{\Longrightarrow} \frac{\log \frac{1-\delta}{\delta}}{\delta} - \frac{H(\delta) - \log 2(1-R)}{\delta^2} &= 0 \\ \overset{c}{\Longrightarrow} \log(1-\delta) + (1-R)\log 2 &= 0 \\ \Longrightarrow \delta = 1 - 2^{-(1-R)} & \end{aligned}$$

where $\overset{b}{\Longrightarrow}$ follows because $H^{'}(\delta) = \frac{1-\delta}{\delta}$, $\overset{c}{\Longrightarrow}$ follows by replacing $H(\delta)$ by $-\delta\log\delta - (1-\delta)\log(1-\delta)$. The value of $f(\delta)$ at $\delta = 1 - 2^{-(1-R)}$ is computed as follows.

$$\begin{aligned} f(1-2^{-(1-R)}) = \frac{H(1-2^{-(1-R)}) - (1-R)\log 2}{1-2^{-(1-R)}} \\ \log \frac{2^{-(1-R)}}{1-2^{-(1-R)}} = \log \frac{1}{2^{1-R}-1} \end{aligned}$$

□

References

[1] C.E. Shannon, "A Mathematical Theory of Communication", *Bell System Tech. J.*, vol. 27, pp. 379-423, 623-656, July, October, 1948.

[2] R. G. Gallager, *Low-density Parity-Check Codes.* Cambridge, MA: MIT Press, 1963.

[3] A. Khandekar and R. J. McElice, "Typical pairs decoding on the AWGN channel," in *Proc. IEEE Int. Symp. Information Theory*, pp. 180-183, Hawaii, USA, Nov. 2000.

[4] I. Sason and R. Urbanke, "Parity-check density versus performance of binary linear block codes over memoryless symmetric channels," in *IEEE Trans. Inf. Theory,* vol. 49, no. 7, pp. 1611-1635, Jul. 2003.

[5] H. D. Pfister, I. Sason and R. Urbanke, "Capacity-achieving ensembles for the binary erasure channel with bounded complexity", in *IEEE Trans. on Info. Theory*, vol. 51, no. 7, pp. 2352- 2379, July, 2005.

[6] C. H. Hsu, *Design and Analysis of Capacity-Achieving Codes and Optimal Receivers with Low Complexity,* PhD. Thesis, University of Michigan, MI, 2006.

[7] M.J. Wainwright and E. Martinian, "Low-density graph codes that are optimal for source/channel coding and binning", *arXiv Technical report* , April 2007. [ONLINE] . Available: *http://arxiv.org/abs/0704.1818.*

[8] G. Wiechman and I. Sason, "Parity-Check Density Versus Performance of Binary Linear Block Codes: New Bounds and Applications," in *IEEE Trans. Info. Th.*, vol. 53, no. 2, pp. 550-579, Feb. 2007.

[9] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. W. McLaughlin and J-M. Merolla, "Applications of LDPC Codes To the Wiretap Channel,", *IEEE Trans. Inf. Theory*, vol. 53, no. 8, pp. 2933–2945, Aug. 2007.

[10] I. Sason and G. Wiechman, "On Achievable Rates and Complexity of LDPC Codes Over Parallel Channels: Bounds and Applications," *IEEE Trans. Inf. Th.*, vol. 53, no. 2, pp. 580-598, Feb. 2007.

[11] C. H. Hsu and A. Anastasopoulos, "Capacity Achieving LDPC Codes Through Puncturing," *IEEE Trans. Inf. Th.*, vol. 54, no. 10, pp. 4698-4706, Oct. 2008.

[12] H. D. Pfister and I. Sason, "Accumulate-Repeat-Accumulate Codes: Capacity-Achieving Ensembles of Systematic Codes for the Erasure Channel With Bounded Complexity," *IEEE Trans. Info. Th.*, vol. 53, no. 6, pp. 2088-2115, June, 2007.

[13] J. Ha and S. W. McLaughlin, "Rate-compatible puncturing of low-density parity-check codes," *IEEE Trans. on Inf. Th.*, vol. 50, no. 11, pp. 28242836, November 2004.

[14] T. Richardson and R. Urbanke, "The capacity of low-density parity-check codes under message-passing decoding," *IEEE Trans. Inf. Th.*, vol. 50, no. 2, pp. 599-618, Feb. 2001.

[15] R. Liu, P. Spasojević and E. Soljanin, "Reliable channel regions for good codes transmitted over parallel channels," *IEEE Trans. Inf. Th.*, vol. 52, no. 4, pp. 1405-1424, April 2006.

[16] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, pp. 656-715, Oct. 1975.

[17] Y. Liang, H. V. Poor and S. Shamai (Shitz), "Information Theoretic Security," *Foundations and Trends in Communications and Information Theory*, Vol. 5, nos. 4-5, pp. 355-580, 2008.

[18] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 135-138, Oct. 1975.

[19] L. H. Ozarow and A. D. Wyner, "Wire-tap channel II," *Bell Syst. Tech. J.*, vol. 63, no. 10, pp. 2135-2157, Dec. 1984.

[20] M. J. Wainwright and E. Martinian, "Low-density graph codes that are optimal for source/channel coding and binning." *IEEE Trans. Inf. Theory*, vol. 55, no. 3, pp.1061-1079, March, 2009.

[21] M. J. Wainwright and E. Martinian, "Low-density Graph Codes That Are Optimal for Source/Channel Coding and Binning," arXiv technical report, April 2007, http://arxiv.org/abs/0704.1818.

[22] H. Jin, *Analysis and Design of Turbo-like Codes,* PhD. Thesis, California Institute of Technology, Pasadena, CA, 2001, http://resolver.caltech.edu/CaltechETD:etd-08222001-151244 .

[23] A. Khandekar, *Graph Based Codes and Iterative Decoding,* PhD. Thesis, California Institute of Technology, Pasadena, CA, 2002, http://resolver.caltech.edu/CaltechETD:etd-06202002-170522.

[24] R. Liu, Y. Liang, H. V. Poor and P. Spasojevic, "Secure Nested Codes for Type-II Wiretap Channels," *Proc. IEEE Information Theory Workshop*, Lake Tahoe, CA, 2007 pp. 337 – 342.

[25] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. W. McLaughlin and J-M. Merolla, "Applications of LDPC Codes To the Wiretap Channel," *IEEE Trans. Inf. Theory*, vol. 53, no. 8, pp. 2933–2945, Aug. 2007.

[26] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339-348, May 1978.

[27] T. M. Cover and J. A. Thomas, "Elements of Information Theory," John Wiley and Sons, New York, 1991.

[28] S. Litsyn and V. Shevelev, "On Ensembles of Low-Density Parity-Check Codes: Asymptotic Distance Distributions," *IEEE Transactions on Information Theory*, vol. 48, no. 4, pp. 887-908, 2002.

[29] M. Raina, R. Liu, P. Spasojević, H. V. Poor, "Application of LDGM-LDPC Codes to Secrecy Coding for the Type-II Binary Symmetric Wiretap Channel," *Proc. of IEEE Info. Th. Workshop* , Cairo, Egypt, Jan. 2010.

[30] T. Richardson and R. Urbanke, *Modern Coding Theory*, Cambridge University Press, New York, 2008.

[31] H. Jin and R. J. McEliece, "Coding theorems for turbo code ensembles," *IEEE Trans. Inf. Th.* , vol.48, no.6, pp.1451-1461, Jun 2002.

[32] M. van Dijk, "On a special class of broadcast channels with confidential messages," *IEEE Trans. on Info. Theory*, vol. 43, no. 2, pp. 712714, Mar. 1997.

[33] C. H. Hsu and A. Anastasopoulos, "Capacity-Achieving Codes with Bounded Graphical Complexity on Noisy Channels," *Proc. 43rd Ann. Allerton Conf. Communication, Control and Computing*, pp. 1825-1834, Monticello, IL, Sep. 2005.