ON UNIVERSAL LDPC CODE ENSEMBLES OVER MEMORYLESS SYMMETRIC CHANNELS

BOAZ SHUVAL

ON UNIVERSAL LDPC CODE ENSEMBLES OVER MEMORYLESS SYMMETRIC CHANNELS

RESEARCH THESIS

SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE DEGREE OF MASTER OF SCIENCE
IN ELECTRICAL ENGINEERING

BOAZ SHUVAL

SUBMITTED TO THE SENATE OF THE TECHNION — ISRAEL INSTITUTE OF TECHNOLOGY
Shebat 5771 HAIFA FEBRUARY 2011

THIS RESEARCH THESIS WAS SUPERVISED BY PROF. IGAL SASON UNDER THE AUSPICES OF THE ELECTRICAL ENGINEERING DEPARTMENT

ACKNOWLEDGMENT

First and foremost, I would like to express my gratitude to my supervisor, Prof. Igal Sason, without whom this work will not have been possible. His assistance, support, and guidance throughout this research work have been invaluable.

I would also like to thank my family for being supportive of me during my research and for always being there for me.

THE GENEROUS FINANCIAL HELP OF THE TECHNION IS GRATEFULLY ACKNOWLEDGED

To my family.

Contents

List of Figures

List of Tables

Abstract

Traditionally, low-density parity-check (LDPC) code ensembles are designed using numerical methods suited to the channel on which they are to be used. In practice, the actual channel statistics are hardly ever known in advance. Moreover, even if the channel statistics were known, it is desirable to design universal codes that will be robust enough to perform well on a range of channels, rather than a specific channel only. Therefore, a universal design of LDPC code ensembles that enables to operate reliably over various channels is of great theoretical and practical interest.

In this thesis we consider the universality of LDPC code ensembles over families of memoryless binary-input output-symmetric (MBIOS) channels, both under belief propagation (BP) decoding and maximum-likelihood (ML) decoding.

For the BP decoding case, we rely on the density evolution approach, to derive an analytical method for universal LDPC code design over various families of MBIOS channels. We analyze this regime for several families of MBIOS channels. The density evolution approach also enables us to derive a necessary condition for universality of LDPC code ensembles under BP decoding. This necessary condition sits at the heart of an LP bound on the universal achievable fraction of capacity. It also enables us to provide analytical and easy-to-calculate bounds on the threshold of LDPC code ensembles under BP decoding that are based on the Bhattacharyya parameter of the channel. The results for LDPC code ensembles are also extended to irregular repeat-accumulate (IRA) code ensembles under BP decoding.

For the ML decoding case, we prove that properly selected regular LDPC code ensembles are universally capacity-achieving for the set of equi-capacity MBIOS channels. We extend this result also to prove that punctured regular LDPC code ensembles are also universally capacity-achieving for the set of equi-capacity MBIOS channels.

List of notation and Abbreviations

AWGN	Additive White Gaussian Noise
BIAWGNC	Binary Input Additive White Gaussian Noise Channel
BEC	Binary Erasure Channel
BER	Bit Error Rate
BP	Belief Propagation
B-Parameter	Bhattacharyya Parameter
BSC	Binary Symmetric Channel
DE	Density Evolution
GEXIT	Generalized Extrinsic Information Transfer
IRA	Irregular Repeat Accumulate
LDPC	Low Density Parity Check
LLR	Log-Likelihood Ratio
LP	Linear Programming
MAP	Maximum A-Posteriori
MBIOS	Memoryless, Binary-Input, Output-Symmetric
pdf	probability density function

$\circledast$	Convolution in the L-domain
$\boxast$	Convolution in the G-domain
a_{R}	Average right degree of and LDPC code ensemble
$\mathcal{A}$	A set of channels (L-densities)
B	Bhattacharyya Parameter
$\mathcal{B}(\cdot)$	Bhattacharyya functional
$C(\cdot)$	Capacity Functional
C	Capacity
d_{c}	Fixed right degree of a right-regular LDPC code
$d_{\mathrm{v}}^{\max}$	Maximal left degree of an LDPC code ensemble
$\mathcal{E}(\cdot)$	Bit error probability functional
$h_2(\cdot)$	Binary entropy function on base 2
$h_2^{-1}(\cdot)$	Inverse of the binary entropy function on base 2
n	Length of a block code
$Q(\cdot)$	The Q-function
R_{d}	Design rate of an LDPC code ensemble
γ	Euler's constant ($\gamma \approx 0.5772$)
Γ	Mapping of densities from the L-domain to the G-domain
Γ^{-1}	Mapping of densities from the G-domain to the L-domain
λ	Left-degree distribution from the edge perspective of an LDPC code ensemble
ρ	Right-degree distribution from the edge perspective of an LDPC code ensemble
σ	Standard deviation of the noise for a BIAWGNC

Chapter 1

Introduction

The inception of information theory began with Shannon's seminal paper [38] in which he showed that it is possible to transmit information reliably over noisy channels at a positive rate, so long as the information transmission rate is below the channel capacity. The mechanism by which this reliable transmission was made possible is coding. Shannon's proof of existence of such transmission schemes relied on using random block codes; while this made for a particularly elegant proof, it is of little practical use in the *design* of actual codes that can be used. Shannon's decoding scheme is a joint-typicality decoding scheme, in which the decoder must compare the received word with each of the possible codewords. This results in an impractical amount of time and memory even for modest code rates if the code is long enough.

This motivated the search for "good" practical codes. Researchers sought codes that could be used to reliably transmit information in as high a rate as possible, all the while enabling practical decoding. One ripe family of codes considered is linear block codes. Linear block codes have a special structure that dramatically reduces the memory requirements of the encoder and decoder. Each of the valid codewords is constructed by means of the code's generator matrix. In the binary setting, a row-vector containing the k information bits is right-multiplied by the generator matrix to become an n-vector which represents the codeword to be transmitted. Thus, the code can be seen as the row-space of the generator matrix. An alternative representation of the code is via its parity-check matrix, whose row-space is orthogonal to the code. A column-vector of length n is left-multiplied by the parity-check matrix; the result is the zero vector if the column-vector represents a valid codeword. In this thesis we will consider a particular subset of codes within this family, the subset of Low-density parity-check (LDPC) codes.

1.1 LDPC Codes

Low-density parity-check (LDPC) codes were first introduced by Gallager [8] [1]. These codes are linear block codes that can be represented by a sparse parity-check matrix. This sparse structure enables to decode these codes using suboptimal iterative decoding algorithms. These algorithms are of low-complexity, thus enabling practical decoding. Even though these algorithms are suboptimal, they are remarkable in that they enable reliable communication at rates close to capacity for properly designed LDPC code ensembles (see , e.g., [5], [1], [20], [26] and [28]).

Gallager's construction of LDPC codes is based on a parity-check matrix with a constant number of non-zero elements in each row and each column of the matrix. Today, such codes are termed *regular*. Gallager not only described a method of constructing these codes, but he also analyzed their weight distribution and their performance under optimal maximum-likelihood (ML) decoding. Gallager's analysis was for a somewhat idealized yet highly useful class of channels, the class of memoryless, binary-input, output-symmetric (MBIOS) channels. These channels are memoryless, receive a binary input (either 0 or 1), and are symmetric in the sense that the channel outputs can be paired in such a way that the probability of the channel producing one output given input 0 is equal to the probability of it producing the other output given input 1. Common examples of such channels are the Binary Erasure Channel (BEC), the Binary Symmetric Channel (BSC), and the Binary-Input Additive White Gaussian Noise Channel (BIAWGNC). Recognizing that ML decoding is not practical, Gallager also suggested and analyzed the performance of his regular LDPC codes under several iterative decoding algorithms.

The concept behind the iterative decoding algorithms is to use the channel information received for each code variable (i.e., each element of the transmitted word) and compute "messages" that are sent to the various parity-checks. Each parity-check receives messages from the code variables that participate in it and computes

[1] This paper is actually an expanded and revised version of Gallager's PhD dissertation, in which the study of LDPC codes was first done.

a return message to each code variable, based on the other received messages. The code variables then return a message to the parity-checks, based on the other incoming messages and the channel input. These iterations continue until some stopping criterion occurs and then a decision is made. The iterative decoding algorithms differ in the data carried by the messages as well as the way messages are computed at each iteration. A major iterative decoding algorithm, in which the messages that are sent by code variables are confidence levels in the value of the code variable, is called the *Belief Propagation* (BP) algorithm (see [29, Chapter 2]). The decoding criterion for which the message update rules of this algorithm were derived is minimum bit-error probability.

A natural extension of regular LDPC codes is to have a non-constant number of non-zero elements in each row or column of the parity-check matrix. These LDPC codes are called *irregular*, and in [28] were shown to operate well at rates close to capacity, under suboptimal BP decoding. In paritcular, in [5] the authors have constructed LDPC codes that operate very close to capacity for a BIAWGNC. The mechanism which enabled this analysis and design is a tool called *density evolution*, which enables to numerically calculate whether, for a given channel, a randomly constructed LDPC code with a certain structure will asymptotically achieve vanishing bit-error probability under BP decoding. When the channel exhibits degradation based on a certain channel parameter, this gives rise to a threshold value on the channel parameter. This thershold value determines the range of channel parameter values for which the randomly constructed code will asympotically exhibit error-free performance.

The structure of an ensemble of irregular LDPC codes can be described using bipartite graphs. The code variables form variable nodes, on the left-hand-side of the graph, and the parity-checks form the parity-check nodes on the right-hand-side of the graph. The non-zero elements of the parity-check matrix are the graph's edges; each edge connects a variable node to a parity-check node in which it participates. For analysis of LDPC code, it is useful to define their degree distributions. A node (either variable or parity-check) is called of degree i if there are i edges emanating from it. The fraction of edges connected to variable nodes of degree i is denoted λ_i. The left-degree distribution λ consists of the set of fractions $\{\lambda_2, \lambda_3, \dots \lambda_{d_{\mathrm{v}}^{\max}}\}$, where $d_{\mathrm{v}}^{\max}$ is the maximal degree of the variable nodes. Similarly, the fraction of edges connected to parity-check nodes of degree i is denoted ρ_i, and the right-degree distribution ρ consists of the set $\{\rho_2, \rho_3, \ldots \rho_{d_{\mathrm{c}}^{\max}}\}$, where $d_{\mathrm{c}}^{\max}$ is the maximal degree of the parity-check nodes. Often, codes in which all parity-check nodes are of the same degree are considered; such codes are called *right-regular* or *check-regular*. Based on these degree distributions, the polynomials $\lambda(x) = \sum_i \lambda_i x^{i-1}$ and $\rho(x) = \sum_i \rho_i x^{i-1}$ are defined.

The density evolution approach serves as a main tool for the asymptotic analysis of the performance of LDPC code ensembles under iterative message-passing decoding [28]. Using this approach, it is possible to numerically optimize LDPC codes for specific MBIOS channels. The goal is to find degree distributions that asymptotically ensure convergence to error-free communications for a given channel model, and that are optimal in the sense of either achieving maximal rate for specific channel parameters, or exhibiting the best threshold for a specific chosen rate or other constraints on the degree distributions (depending on the threshold parameter considered, "the best" threshold could be either "maximum," as in the crossover probability of a binary symmetric channel, or "minimum," as in the noise variance of a binary-input additive white Gaussian noise channel). Another consequence of density evolution is the stability condition which forms a necessary condition for an LDPC code ensemble to asymptotically achieve vanishing bit error probability under message-passing decoding for a given channel model. Density evolution is a powerful tool for numerical optimization of degree distributions, but it does not lend itself, in general, for the *analytical* design of degree distributions. An exception to this is the case of the binary erasure channel (BEC), where density evolution is greatly simplified to a single-dimensional equation. Based on this, several explicit expressions of capacity-approaching sequences for the BEC have been derived (see, e.g. [24] and [40]). So far, no explicit expressions for capacity-approaching code ensembles under iterative decoding for other MBIOS channel models have been found.

We note that while ML decoding is impractical, explicit expressions for capacity-approaching codes for any MBIOS channel under ML decoding have been derived (see [12] and [33, Theorem 2.2]). The analysis under ML decoding relies on upper bounds on the decoding error probability based on the average weight distribution of the ensemble (see [22] and [35]).

1.2 Universal Codes

It is of great interest, both practically and theoretically, to design a code that will operate reliably over a range of channels. Such robust codes are termed *universal.* There are many different notions of universality, and many approaches to the design of universal codes. An excellent survey on the matter can be found in [18], where the authors have concentrated on the problem of communicating reliably when there is channel uncertainty. The authors introduced several models of channel uncertainty, and discussed several universality strategies for these models, both in terms of encoder and decoder design.

The subject of universal LDPC codes has been addressed in several recent studies. In this setting, the goal is to design an LDPC code ensemble that will perform well in terms of error probability over a family of channels, using a standard decoder for LDPC codes, such as a belief propagation decoder. This is in contrast to traditional methods of LDPC code design, in which knowledge of the channel model affords the use of numerical methods such as density evolution, as described in Section 1.1, to design the code.

One approach is to find so-called "extreme" channels that can be used to predict the LDPC code ensemble's performance under iterative decoding. Khandekar [16] showed that a code's behavior on the BEC can be used to predict its behavior on other channels. In particular, he showed that if for a BEC, the bit erasure probability of an LDPC code ensemble converges to zero under iterative message-passing decoding then the bit error probability will also converge to zero on any other MBIOS channel with the same Bhattacharyya parameter (B-parameter). Among the family of equi-capacity MBIOS channels, the BEC exhibits the smallest B-parameter whereas the binary symmetric channel (BSC) exhibits the greatest B-parameter [4]. Based on this observation, it was suggested that it may be possible to design a code for an arbitrary MBIOS channel by designing it for a BEC with a matching B-parameter. Further evidence of the extremality of the BEC and BSC can be found, e.g., in a study by Sutskover et al. (see [41] and [42]), which is based on an information-combining approach ([17]) to predict the behavior of LDPC code ensembles over various channels; they showed that the behavior of an LDPC code ensemble over a BEC and BSC can be used to provide bounds on its behavior over other MBIOS channels under iterative message-passing decoding. These works all use bounds that stem from the reduction of the density evolution equation to a single parameter. Such bounds first appeared in [3], albeit not from a universality standpoint.

Several researchers have noticed that LDPC codes exhibit similar performance under iterative message-passing decoding over a set of channels with similar parameters. Numerical evidence that equi-capacity and equi-B-parameters exhibit similar thresholds is provided in [4], and thus it was conjectured that the performance of an LDPC code over one MBIOS channel can be approximated by its performance on a different MBIOS channel but with the same capacity or B-parameter. Franceschini et al. ([7]), also provide supporting numerical evidence that LDPC code ensembles behave similarly on equi-capacity MBIOS channels. In [25], the authors conjecture that it is possible to design good LDPC codes based on a so-called "surrogate" channel, such as the BEC, so that they will exhibit good performance over other channels. Recently, Sanaei et al. ([31]) numerically designed some universal LDPC code ensembles that achieve high fraction of capacity for a set of equi-capacity MBIOS channels. In addition, based on some practical experiments, they have conjectured that an LDPC code ensemble designed for two equi-capacity MBIOS channels will also converge under iterative message-passing decoding over any convex combination of these two channels[2].

We briefly mention several other avenues of research regarding universal LDPC codes; these works present approaches that are quite removed from the approach to universality of this thesis, and are presented here for the sake of completeness. Duyck, et al. [6] numerically optimized LDPC code ensembles to be universal over Ricean multiple-access channels for all k-factors. Miyake and Maruyama [23] study universal properties of fixed length LDPC codes under the minimum-entropy decoding scheme. Universal codes with finite block lengths are addressed in [39]; that study concentrates on the performance of such code ensembles, in terms of bounds on the probability of error (and error exponents), for a class of channels the authors call "periodic erasure channels." Factor-graph decoding over a family of channels related by some unknown parameters was considered in [45], in which several factor-graph based decoding schemes over channels with unknown parameters were defined and applied

[2] I.e., a channel formed by using one of these channels with probability θ, $0 \leq \theta \leq 1$, and the other channel with probability $1 - \theta$.

to codes that can be represented by factor graphs, not necessarily LDPC codes. Finally, Yedla, et al. [48] consider the problem of universal joint source-channel coding; in their setting, there are two correlated sources transmitting over two channels with unknown parameters, to be jointly decoded by a single receiver.

1.3 This work

In this work, we consider the universality of LDPC code ensembles under both iterative message-passing decoding and ML decoding over MBIOS channels. For the iterative (belief propagation) decoding case, we use density evolution to derive some conditions for universality of LDPC code ensembles over various MBIOS channels. These results serve to formulate an approach for the *analytical* design of universal LDPC code ensembles. Moreover, a necessary condition for universality enables us to formulate linear-programming upper bounds on the universal achievable rate of LDPC code ensembles over families of MBIOS channels. Furthermore, we show that for any code ensemble, one can classify channels as "good" or "bad" (in the sense of asymptotically achieving vanishing bit-error-probability under belief propagation decoding) based on the value of the B-parameter of the channel. This, in turn, leads to bounds on the threshold of the code ensemble. Some of these results are also extended for the family of irregular, repeat-accumulate (IRA) code ensembles. For the ML decoding case, we show that the regular LDPC code ensembles can be made universally capacity achieving both with and without puncturing over equi-capacity MBIOS channels.

This thesis is structured as follows: Chapter 2 provides some preliminary material and notation. Chapter 3 explores the universality of LDPC code ensembles under belief propagation decoding, and Chapter 4 extends these results to IRA codes. Universality results for LDPC code ensembles under ML decoding are considered in Chapter 5. Finally, in Chapter 6 we present a summary of this thesis and some directions for future research.

The results in this research work are also presented in [36], which was recently accepted for publication in the *IEEE Trans. on Information Theory* (as a full paper).

Chapter 2

Preliminaries

This Chapter follows the notation in [29, Chapter 4], and briefly introduces some preliminaries on memoryless binary-input output-symmetric (MBIOS) channels that are relevant for the analysis in this research work.

Consider an MBIOS channel whose input and output are designated by X and Y, respectively, and let $p_{Y|X}(\cdot|\cdot)$ be its transition probability. The associated log-likelihood ratio (LLR) $l(y)$ when the channel output is $Y = y$ is given by

$$l(y) = \ln\left(\frac{p_{Y|X}(y|0)}{p_{Y|X}(y|1)}\right).$$

The LLR associated with the random variable Y is defined as $L = l(Y)$. Let a designate the conditional probability density function (*pdf*) of the random variable L given that the channel input is $X = 0$ (to be referred to as the L-density function). This density function satisfies the symmetry property $a(x) = e^x \, a(-x)$ for every $x \in \mathbb{R}$ (see [29, Theorem 4.26]).

The following three functionals serve at the heart of the analysis presented in this work (various other functionals are presented in [29, Section 4.1]).

Proposition 2.1 [Capacity functional] Consider an MBIOS channel whose symmetric L-density function is denoted by a. The capacity of this channel in units of bits per channel use, $C \triangleq C(a)$, is given by

$$C = \int_{-\infty}^{\infty} a(x)\big(1 - \log_2(1 + e^{-x})\big)\,\mathrm{d}x. \tag{2.1}$$

This proposition is proved in [29, p. 193].

Definition 2.1 [**The Bhattacharyya functional**] The Bhattacharyya parameter (B-parameter), $B \triangleq \mathcal{B}(a)$ that is associated with the symmetric L-density function a, is given by

$$B = \int_{-\infty}^{\infty} a(x) e^{-\frac{x}{2}} \, \mathrm{d}x. \tag{2.2}$$

Definition 2.2 [**The error probability functional**] The bit error probability that is associated with a symmetric L-density function a is given by

$$\begin{aligned} \mathcal{E}(a) &= \int_{-\infty}^{0^-} a(x) \, \mathrm{d}x + \frac{1}{2} \int_{0^-}^{0^+} a(x) \, \mathrm{d}x \\ &= \frac{1}{2} \int_{-\infty}^{+\infty} a(x) \, e^{-(|\frac{x}{2}| + \frac{x}{2})} \, \mathrm{d}x. \end{aligned}$$

The following propositions and inequalities establish some relationships between the capacity, B-parameter, and the bit error probability associated with the same symmetric L-density.

The following proposition relates the capacity with the B-paremeter of an MBIOS channel. It is a direct consequence[1] of a proposition that was introduced in [2, Proposition 1] (for a proof see [2, Appendix A]).

Proposition 2.2 For every MBIOS channel, let a be the L-density of the LLR at the channel output for an equi-probable binary input, and let B and C designate the B-parameter and channel capacity, respectively. Then, the following inequality holds:

$$\log_2 \left(\frac{2}{1+B} \right) \leq C \leq \sqrt{1 - B^2}. \tag{2.3}$$

Proposition 2.2 implies that for a perfect MBIOS channel, whose capacity, C, approaches 1 bit per channel use, the corresponding B-parameter tends to zero. On

[1] [2, Proposition 1] is specified for a general binary-input, discrete memoryless channel, and it relates between the symmetric capacity and the B-Parameter. The extension for MBIOS channels that are not necessarily discrete is immediate. MBIOS channels are symmetric, for which the symmetric capacity is indeed the channel capacity; changing summations to integrals extends the proof to possibly continuous channels.

the other hand, for a very noisy channel, whose capacity is close to zero, we have that the B-parameter tends to 1. This is consistent with the interpretation that the B-parameter forms an upper bound on the error probability under ML decoding when the channel is used only once to transmit a zero or a one.

Another property that relates the channel capacity and the B-parameter of an MBIOS channel is presented in the following proposition, which was introduced in [32, Lemma 8] (for a proof see [32, Appendix IV]). This proposition improves upon the lower bound in Proposition 2.2.

Proposition 2.3 For every MBIOS channel, the sum of its channel capacity and its B-parameter is greater than or equal to 1, i.e.,

$$B + C \geq 1$$

and equality is achieved for a BEC.

Note that Proposition 2.3 implies that among all equi-capacity MBIOS channels, the BEC possesses the minimal B-parameter.

Remark 2.1 From the lower bound of 2.2, it is implied that $C+B \geq 1+(B-\log_2(1+B))$. It can easily be verified that $f(B) \triangleq 1 + (B - \log_2(1 + B)) \leq 1$ for $B \in [0, 1]$, with equality only at the end points, i.e., $B = 0$ or $B = 1$. To see this, we first note that indeed $f(0) = f(1) = 1$. The derivative of f is $f'(B) = 1 - ((1 + B) \ln 2)^{-1}$, which has only one zero, at $B = -1 + 1/\ln 2 \approx 0.4427$. This is easily determined to be a minimum point of f, implying that $f(B) \leq 1$ for $B \in [0, 1]$. On the other hand, proposition 2.3 states that $B + C \geq 1$, thereby improving the lower bound in Proposition 2.2.

The following inequalities relate the Bhattacharyya and error probability functionals. Based on [29, Lemma 4.64], for an arbitrary symmetric L-density a we have

$$2\mathcal{E}(a) \leq \mathcal{B}(a) \leq 2\sqrt{\mathcal{E}(a)\big(1 - \mathcal{E}(a)\big)}. \tag{2.4}$$

Note that the lower and upper bounds on the B-parameter, as given in (2.4), are satisfied with equality for a BEC and BSC, respectively.

Convolutions of densities in the so-called L-domain and G-domain[2] are presented in [29, p. 181], and are denoted by $\circledast$ and $\boxast$, respectively. Using the density evolution approach for the asymptotic analysis of LDPC code ensembles over MBIOS channels, where we let the block length tend to infinity, the $\circledast$ convolution describes how the distribution of the (statistically independent) messages changes at the variable node side under BP decoding at every single iteration, whereas the $\boxast$ convolution describes the change of this distribution at the parity-check node side.

A consequence of density evolution is the *stability condition* for LDPC code ensembles under belief propagation (BP) decoding. This condition applies to the asymptotic case where we let the block length tend to infinity, and it forms a necessary condition for successful BP decoding in the sense that it requires that the fixed point of zero bit error rate be stable. Consider an LDPC code ensemble with a pair of degree distributions (λ, ρ) whose transmission takes place over an MBIOS channel, characterized by its L-density function a. Then, the stability condition under BP decoding assumes the form (see [29, Theorem 4.125])

$$\mathcal{B}(a)\lambda'(0)\rho'(1) < 1. \tag{2.5}$$

The reader is referred to [29, Section 4.9] for a proof.

[2] As mentioned at the beginning of this chapter, an L-density is the pdf of the LLR $l(Y)$ given that the channel input is $X = 0$. A G-density is the result of the transformation $l(Y) \rightarrow (\operatorname{sgn} l(Y), \log\coth(|l(Y)|/2))$. The L and G-domains are, respectively, the domains of the L and G densities.

Chapter 3

Universality under Belief Propagation Decoding

In this chapter we consider universality under BP decoding. In Section 3.1 we derive a condition for a sequence of LDPC code ensembles to asymptotically achieve vanishing bit-error-probability under BP decoding. Using this condition we show that it is possible to design LDPC code ensembles that will operate reliably over a range of channels. We study this approach for two particular families of channels. In Section 3.2 we use the condition developed in Section 3.1 to derive a necessary condition for universality of LDPC code ensembles under BP decoding. Using this condition, we derive universal lower bounds on the achievable gap to capacity based on linear-programming. We conclude this chapter with Section 3.3, in which we show that the B-parameter of the channel can be used as a universal condition for "good" or "bad" communications under BP decoding.

3.1 Universal Achievability Results

In the following, we consider the suitability of LDPC code ensembles to operate reliably over a set of MBIOS channels under BP decoding. We rely here on the density evolution approach, and our goal is to construct LDPC code ensembles that achieve vanishing bit error probability, in the asymptotic case where the block length tends to infinity, uniformly over a set of MBIOS channels.

To this end, let us consider first an arbitrary MBIOS channel, and let a_0 denote the *pdf* of the LLR at the channel output given that the channel input is zero. Let λ and ρ designate the degree distributions of the variable and parity-checks, respectively, from the edge perspective. Based on density evolution, the densities at every iteration of the BP decoder satisfy the recursive equation

$$a_l = a_0 \circledast \lambda\Biggl(\Gamma^{-1}\Bigl(\rho\bigl(\Gamma(a_{l-1})\bigr)\Bigr)\Biggr), \quad l = 1, 2, \ldots \tag{3.1}$$

where the mapping Γ and its inverse Γ^{-1} are introduced in [28, p. 627], and denote the transformation of densities from the L-domain to the G-domain and vice-versa. The densities a_l are symmetric functions for every $l \geq 0$, i.e., $a_l(x) = e^x a_l(-x)$ for all $x \in \mathbb{R}$. Let $x_l = \mathcal{B}(a_l)$ for $l \geq 0$ where $\mathcal{B}(a)$ designates the B-parameter that is associated with the L-density a. Based on the proof of sufficiency in the stability condition (see [29, p. 234]), it follows that

$$x_l \leq \mathcal{B}(a_0)\,\lambda\bigl(1 - \rho(1 - x_{l-1})\bigr), \quad l = 1, 2, \ldots \tag{3.2}$$

This inequality is proved directly in [11, Theorem 4.2] and also in [15, Theorem 2]. From (2.4), a necessary and sufficient condition for an LDPC code ensemble to asymptotically obtain vanishing bit error probability as the number of iterations grows is that $\lim_{l \to \infty} x_l = 0$.

Let us now consider an arbitrary set of MBIOS channels, and let $\mathcal{A}$ designate the corresponding set of its L-densities. Suppose that one wishes to design an LDPC code ensemble with degree distributions (λ, ρ) in order to asymptotically achieve vanishing bit error probability under BP decoding for every channel in this set. Let us designate by B the maximal B-parameter over the MBIOS channels of the considered set, i.e.,

$$B \triangleq \max_{a \in \mathcal{A}} \mathcal{B}(a). \tag{3.3}$$

Let us consider the recursive equation

$$y_l = B\,\lambda\bigl(1 - \rho(1 - y_{l-1})\bigr), \quad l = 1, 2, \ldots \tag{3.4}$$

with the initial value $y_0 = B$. This recursive equation refers to the density evolution of a BEC whose erasure probability is equal to B. By comparing (3.2) and (3.4), it is straightforward to show (e.g., by induction) that $0 \leq x_l \leq y_l$ for every $l \geq 0$ and $a \in \mathcal{A}$. If the pair of degree distributions (λ, ρ) is selected in a way where

$\lim_{l\to\infty} y_l = 0$, then we get that $\lim_{l\to\infty} x_l = 0$ in (3.2) for *every MBIOS channel* from the set $\mathcal{A}$. Hence, the universality of the LDPC code ensemble whose degree distribution is (λ, ρ) follows with respect to the considered set of channels.

One can thus rely on (3.4) to construct a sequence of LDPC code ensembles which achieves vanishing bit error probability, under BP decoding, for all the MBIOS channels of the considered set. In particular, to this end one can use the well-known explicit constructions of capacity-achieving sequences of LDPC code ensembles for the BEC (see, e.g., [24] and references therein). By this approach, the asymptotic design rate of this capacity-achieving sequence of LDPC code ensembles is equal to the capacity of the BEC,

$$R_{\mathrm{d}} = 1 - B \tag{3.5}$$

where B is given in (3.3). We study the following particular cases of this approach.

3.1.1 Universal LDPC Code Ensembles for Equi-Capacity MBIOS Channels

Among all MBIOS channels which exhibit a given capacity C, the B-parameter that is associated with the L-densities of this set of channels attains its maximal and minimal values for the BSC and BEC, respectively (this follows readily from (2.4)). The B-parameter of a BSC whose crossover probability is p is equal to $\sqrt{4p(1-p)}$, and the capacity of this channel is equal to $C = 1 - h_2(p)$. By referring to the of set all equi-capacity MBIOS channels, one therefore gets from (3.3) that the maximal B-parameter over this set, B, is given by

$$B = \sqrt{4h_2^{-1}(1-C)\left(1 - h_2^{-1}(1-C)\right)} \tag{3.6}$$

where h_2^{-1} designates the inverse of the binary entropy function on base 2. From (3.5), the asymptotic design rate of the corresponding sequence of LDPC code ensembles is equal to $R_{\mathrm{d}} = 1 - B$. As a consequence of Proposition 2.3, it follows that indeed $R_{\mathrm{d}} \leq C$, which is necessary for reliable communication. The fraction of the channel capacity that is achievable by this approach,

$$\mu_1(C) \triangleq \frac{R_{\mathrm{d}}}{C},$$

is therefore equal to

$$\mu_1(C) = \frac{1 - \sqrt{4h_2^{-1}(1-C)\big(1 - h_2^{-1}(1-C)\big)}}{C}. \tag{3.7}$$

Lemma 3.1 The function μ_1 is monotonic increasing over the interval $(0, 1]$, and

$$\lim_{C \to 0} \mu_1(C) = \ln 2 \approx 69.3\%, \qquad \lim_{C \to 1} \mu_1(C) = 1.$$

Proof: See Appendix A. ■

This implies that as the value of the capacity is increased, a larger fraction of the channel capacity is achievable uniformly for the entire considered set of equi-capacity MBIOS channels, and the two extremes are 69.3% and 100% when the capacity varies between zero and 1 bits per channel use. For a value of the channel capacity which approaches 1, the channels are almost noiseless, so almost no coding is required. Hence, the uniform attainment of nearly 100% of the capacity for the entire set of channels is well expected. However, as evidenced in Fig. 3.1, this convergence of the achievable fraction of capacity is rather slow as we let the code rate tend to 1. To see this, note that if C is close to 1

$$\mu_1(C) \approx \frac{1 - 2\sqrt{h_2^{-1}(1-C)}}{C}$$

which tends to 1 quite slowly (e.g., for $C = 0.95$ bits per channel use, this approximation is equal to 0.895 which indeed coincides with Fig. 3.1).

The above analysis implies that at least 69.3% of the capacity of any MBIOS channel can be achieved by designing a capacity-achieving sequence of LDPC code ensembles for a BEC; the erasure probability of this BEC is set to be equal to the B-parameter of a BSC whose capacity matches our channel.

This presents an analytical approach for the design of universal LDPC code ensembles for equi-capacity MBIOS channels where a provable (non-vanishing) fraction of capacity is universally achieved, and the value of this fraction gets larger as the value of capacity is increased. We note, however, that numerical optimization via density evolution enables to design universal LDPC code ensembles in [31] achieving a significantly larger fraction of the channel capacity, though the approach considered here is purely analytical, and it is not subject to numerical optimizations.

3.1.2 Universal LDPC Code Ensembles for BEC and BIAWGNC with the Same Capacity

We consider here the achievable fraction of capacity when one wishes to design an LDPC code ensemble which asymptotically achieves vanishing bit error probability under BP decoding for both the BEC and the binary-input AWGN channel (BIAWGNC) with the same capacity. Since among all equi-capacity MBIOS channels, the BEC possesses the minimal B-parameter (see Proposition 2.3), then the parameter B in (3.3) corresponds to the B-parameter of the BIAWGNC. The conversion from the channel capacity to the B-parameter for this channel is done numerically by first calculating the noise variance σ^2 via the following expression for its capacity, which is based on (2.1) (see [29, p. 194]):

$$C = 1 + \frac{1}{\ln 2}\left[\left(\frac{2}{\sigma^2} - 1\right) Q\!\left(\frac{1}{\sigma}\right) - \sqrt{\frac{2}{\pi\sigma^2}}\, e^{-\frac{1}{2\sigma^2}} + \sum_{i=1}^{\infty} \frac{(-1)^i}{i(i+1)}\, e^{\frac{2i(i+1)}{\sigma^2}} Q\!\left(\frac{1+2i}{\sigma}\right)\right],$$

and then substituting the value of σ^2 to obtain the B-parameter $B = e^{-\frac{1}{2\sigma^2}}$ (based on (2.2)). From (3.5), the asymptotic achievable fraction of the capacity is equal to

$$\mu_2(C) = \frac{1-B}{C}. \tag{3.8}$$

Since the universality in this example applies to a subset of the equi-capacity MBIOS channels, the inequality $\mu_2(C) \geq \mu_1(C)$ is expected to hold for $0 \leq C \leq 1$. This is exemplified in Fig. 3.1. Our results so far are summarized in the following theorem. To this end, we denote by BEC(ε) the binary erasure channel whose erasure probability is ε:

Theorem 3.1 [Universality of LDPC Codes under BP Decoding for Equi-Capacity MBIOS Channels] Consider a set $\mathcal{A}$ of MBIOS channels that exhibit a given capacity C, and let B denote the maximal B-parameter over this set (see (3.3)). Let $\{(n, \lambda, \rho)\}$ form a capacity-achieving sequence of LDPC code ensembles for BEC(B), achieving vanishing bit erasure probability under BP decoding. Then, this sequence universally achieves vanishing bit error probability under BP decoding for the entire set $\mathcal{A}$, and the design rate of this sequence forms a fraction that is at least $\frac{1-B}{C}$ of the channel capacity. As a consequence, the following results hold:

- For the entire set of equi-capacity MBIOS channels, the universal achievable design rate forms at least a fraction $\mu_1(C)$ of capacity (see (3.7)). Moreover, μ_1 forms a monotonic increasing function of the capacity C (see Fig. 3.1), getting the extreme values $\ln 2 \approx 69.3\%$ and 100% at the endpoints where $C \to 0$ or $C \to 1$, respectively.

- For some sub-classes of equi-capacity MBIOS channels, the results for the universal achievable design rate significantly improve (see, e.g., (3.8) and μ_2 in Fig. 3.1).

Fig. 3.1 compares the achievable fractions of capacity, μ_1 and μ_2 as a function of the channel capacity.

3.2 Universal Lower Bound on the Achievable Gap to Capacity

The stability condition $\mathcal{B}(a)\lambda'(0)\rho'(1) < 1$ forms a necessary condition for asymptotically achieving vanishing bit error probability under BP decoding when the transmission takes place over an MBIOS channel.

We wish to find an upper bound on the achievable design rate of universal LDPC code ensembles over a set $\mathcal{A}$ of MBIOS channels, or alternatively, a universal lower bound on the achievable gap (in rate) to capacity. From the stability condition in (2.5) and also from (3.3), the inequality

$$B\lambda'(0)\rho'(1) \leq 1 \tag{3.9}$$

forms a necessary condition for achieving this goal universally over the set $\mathcal{A}$.

We consider in the following *right-regular* LDPC code ensembles, where d_{c} designates the degree of the parity-check nodes (i.e., $\rho(x) = x^{d_{\mathrm{c}}-1}$).

Following the notation in [29, p. 181], let $a \boxast b$ denote the density which is the result of transforming both a and b from the L-domain to the G-domain, then performing the convolution in the G-domain, and then transforming the outcome back to the L-domain. As mentioned in Chapter 2, the operator $\boxast$ describes the change of the distributions at the check node side under BP decoding.

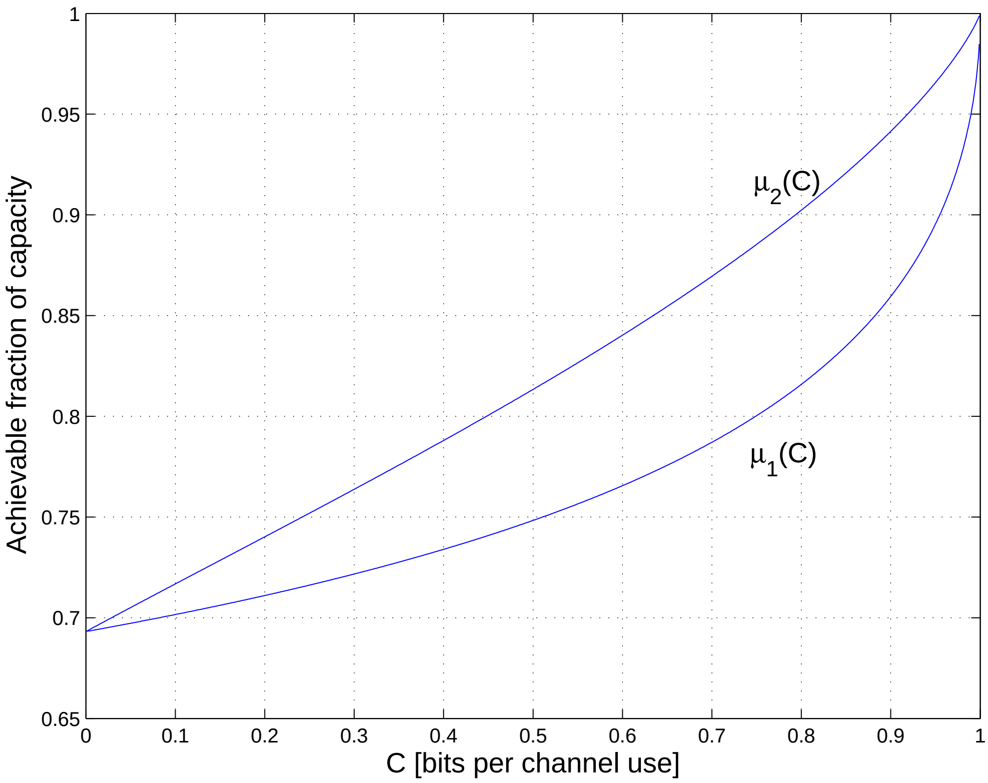

Figure 3.1: Universal achievable fraction of capacity under BP decoding for two sets of MBIOS channels which exhibit a given capacity (see Theorem 3.1). The values of μ_1 in (3.7) and μ_2 in (3.8) correspond, respectively, to the entire set of equi-capacity MBIOS channels, and the subset of a BEC and BIAWGNC with capacity C bits per channel use.

In the following, we introduce an additional necessary condition for universally achieving vanishing bit error probability under BP decoding with respect to a set $\mathcal{A}$ of MBIOS channels.

Theorem 3.2 [A Necessary Condition for Universality of LDPC Code Ensembles under BP Decoding] Let $\{(n, \lambda, \rho)\}$ be a right-regular sequence of LDPC code ensembles, universally achieving vanishing bit error probability under BP decoding for a set of MBIOS channels $\mathcal{A}$. Then, the following condition holds

$$B\lambda\big(\sqrt{1-\rho(1-x^2)}\big) < x, \quad \forall\, x \in (0, B] \tag{3.10}$$

where B designates the maximal B-parameter over the set $\mathcal{A}$.

Proof: For the derivation of this condition, we rely on the following inequality:

Lemma 3.2 Let $a^{\boxast k} \triangleq a \boxast a \boxast \cdots \boxast a$ denote the operator where a is convolved by itself $k-1$ times (i.e., a appears k times on the right-hand side of this equality), where the convolution here is in the G-domain (see [29, p. 181]). Then, for a symmetric L-density a with $\mathcal{B}(a) = \beta_a$

$$\mathcal{B}(a^{\boxast k}) \geq \sqrt{1-(1-\beta_a^2)^k} \tag{3.11}$$

for any integer $k \geq 2$.

Proof: Let a and b denote two symmetric L-densities with $\mathcal{B}(a) = \beta_a$ and $\mathcal{B}(b) = \beta_b$, then from [29, Problem 4.62]

$$\sqrt{\beta_a^2 + \beta_b^2 - \beta_a^2\beta_b^2} \leq \mathcal{B}(a \boxast b) \leq \beta_a + \beta_b - \beta_a\beta_b \tag{3.12}$$

where the upper and lower bounds are achieved with equality if a and b are from the family BEC or BSC, respectively. By setting $a = b$, we get the inequality in (3.11) for $k = 2$. The proof for a general $k \geq 2$ is completed by mathematical induction. Let us assume that (3.11) holds for a certain $k \geq 2$, then from (3.12)

$$\begin{aligned}
\mathcal{B}(a^{\boxast k+1}) &= \mathcal{B}(a^{\boxast k} \boxast a) \\
&\geq \sqrt{\mathcal{B}(a^{\boxast k})^2 + \mathcal{B}(a)^2 - \mathcal{B}(a^{\boxast k})^2\,\mathcal{B}(a)^2} \\
&= \sqrt{1-\big(1-\mathcal{B}(a^{\boxast k})^2\big)\big(1-\mathcal{B}(a)^2\big)} \\
&= \sqrt{1-\big(1-\mathcal{B}(a^{\boxast k})^2\big)(1-\beta_a^2)} \\
&\geq \sqrt{1-(1-\beta_a^2)^{k+1}}
\end{aligned}$$

which then implies that (3.11) also holds for $k+1$. ■

Corollary 3.1 For a right-regular LDPC code ensemble

$$\mathcal{B}\Big(\Gamma^{-1}\Big(\rho\big(\Gamma(a)\big)\Big)\Big) \geq \sqrt{1-\rho\big(1-\mathcal{B}(a)^2\big)}. \tag{3.13}$$

Hence, by defining $x_l \triangleq \mathcal{B}(a_l)$ for all l in the density evolution equation in (3.1), we get the following chain of equalities and inequalities

$$\begin{aligned} x_l &= \mathcal{B}(a_l) \\ &\overset{\text{(a)}}{=} \mathcal{B}(a_0)\,\mathcal{B}\Bigg(\lambda\Big(\Gamma^{-1}\Big(\rho\big(\Gamma(a_{l-1})\big)\Big)\Big)\Bigg) \\ &\overset{\text{(b)}}{=} \mathcal{B}(a_0)\,\lambda\Bigg(\mathcal{B}\Big(\Gamma^{-1}\Big(\rho\big(\Gamma(a_{l-1})\big)\Big)\Big)\Bigg) \\ &\overset{\text{(c)}}{\geq} \mathcal{B}(a_0)\,\lambda\Big(\sqrt{1-\rho\big(1-\mathcal{B}(a_{l-1})^2\big)}\,\Big) \\ &= \mathcal{B}(a_0)\,\lambda\Big(\sqrt{1-\rho\big(1-x_{l-1}^2\big)}\,\Big) \end{aligned} \tag{3.14}$$

where equality (a) follows from the recursive density evolution equation in (3.1) and since for two symmetric L-densities a and b

$$\mathcal{B}(a \circledast b) = \mathcal{B}(a)\,\mathcal{B}(b), \tag{3.15}$$

equality (b) follows since the linearity of the convolution operator and the last equality yield that

$$\mathcal{B}(\lambda(a)) = \mathcal{B}\left(\sum_i \lambda_i a^{\circledast(i-1)}\right) = \sum_i \lambda_i \mathcal{B}\left(a^{\circledast(i-1)}\right) = \sum_i \lambda_i \mathcal{B}(a)^{i-1} = \lambda\left(\mathcal{B}(a)\right), \tag{3.16}$$

and inequality (c) follows from (3.13). By definition, the initial value x_0 is equal to the B-parameter of the symmetric L-density of the MBIOS channel. From (3.14), it follows that if the sequence $\{x_l\}$ tends asymptotically to zero, then the sequence

$$z_l = \mathcal{B}(a_0)\,\lambda\left(\sqrt{1-\rho(1-z_{l-1}^2)}\right), \quad l = 1, 2, \ldots \tag{3.17}$$

with the initial value $z_0 = \mathcal{B}(a_0)$, should also tend to zero. Note that the sequence $\{z_l\}$ is not the same as $\{x_l\}$: the sequence $\{x_l\}$, as shown in (3.14), is *greater than or equal* *to* the right-hand-side of (3.17). Further note that from (2.4), the convergence of the sequence $\{x_l\}$ forms a necessary and sufficient condition for achieving vanishing bit error probability as we let the number of iterations grow (recall that by the density evolution approach, we first let the block length tend to infinity, so that the tree assumption holds with probability 1 for any fixed number of iterations, and then we let the number of iterations grow).

Consider a sequence of right-regular LDPC code ensembles that universally achieves vanishing bit error probability under BP decoding over a set $\mathcal{A}$ of MBIOS channels. Let B be the maximal B-parameter over the entire set $\mathcal{A}$ (see (3.3)), then we obtain from (3.17) that the sequence defined recursively by

$$z_l = B\,\lambda\left(\sqrt{1-\rho(1-z_{l-1}^2)}\,\right), \quad l = 1, 2, \ldots \tag{3.18}$$

with the initial value $z_0 = B$ tends asymptotically to zero. Therefore, the satisfiability of the condition in (3.10) forms a necessary condition for universality. This completes the proof of Theorem 3.2. ■

For an extension of condition (3.10) for general LDPC code ensembles (not necessarily right-regular), see Appendix B.

In order to relate the condition in Theorem 3.2 to the stability condition, we calculate the derivative of the left-hand side of (3.10)

$$\begin{aligned}&\frac{\mathrm{d}}{\mathrm{d}x}\left\{B\,\lambda\left(\sqrt{1-\rho(1-x^2)}\right)\right\}\\ &\quad = B\,\lambda'\left(\sqrt{1-\rho(1-x^2)}\right)\,x\left(1-\rho(1-x^2)\right)^{-\frac{1}{2}}\rho'(1-x^2)\end{aligned}$$

and then require that this derivative be strictly less than 1 at the fixed point $x = 0$. Since d_c designates the fixed right degree of the right-regular LDPC code ensemble,

$$\begin{aligned}\lim_{x\to 0} x\left(1-\rho(1-x^2)\right)^{-\frac{1}{2}} &= \lim_{x\to 0}\frac{x}{\sqrt{1-(1-x^2)^{d_\mathrm{c}-1}}}\\ &= \frac{1}{\sqrt{d_\mathrm{c}-1}}\end{aligned}$$

and therefore one gets the condition

$$\frac{B\lambda'(0)\rho'(1)}{\sqrt{d_\mathrm{c}-1}} < 1. \tag{3.19}$$

Interestingly, this coincides with the stability condition (2.5) up to a scaling factor that is equal to the reciprocal of the square root of $d_{\text{c}} - 1$; this scaling factor in (3.19) yields a weaker condition as compared to the stability condition. However, the condition in (3.10) provides a constraint on the interval $(0, B]$, and not just at a neighborhood of the fixed point at zero.

Let $d_{\text{v}}^{\max}$ designate the maximal degree of the variable nodes. Since the design rate of the right-regular LDPC code ensemble is equal to

$$R_{\text{d}} = 1 - \frac{1}{d_{\text{c}} \sum_{i=2}^{d_{\text{v}}^{\max}} \frac{\lambda_i}{i}} \tag{3.20}$$

then the maximization of R_{d} is equivalent to maximizing $\sum_{i=2}^{d_{\text{v}}^{\max}} \frac{\lambda_i}{i}$.

Suppose that it is required to universally achieve vanishing bit error probability under BP decoding as the block length tends to infinity over a set $\mathcal{A}$ of equi-capacity MBIOS channels with capacity C. This requirement also implies that the bit error probability under MAP decoding vanishes. Thus, by combining [32, Eqs. (43), (44) and (53)], it follows that the design rate satisfies the inequality

$$0 \leq R_{\text{d}} \leq 1 - \frac{1 - C}{h_2\left(\frac{1 - C^{\frac{d_{\text{c}}}{2}}}{2}\right)} \tag{3.21}$$

and therefore, as the parity-check degree (d_{c}) is decreased, R_{d} becomes more bounded away from capacity. Combining (3.20) and (3.21) gives that

$$\frac{1}{d_{\text{c}}} \leq \sum_{i=2}^{d_{\text{v}}^{\max}} \frac{\lambda_i}{i} \leq \frac{1}{(1 - C)\, d_{\text{c}}} \cdot h_2\left(\frac{1 - C^{\frac{d_{\text{c}}}{2}}}{2}\right). \tag{3.22}$$

By a maximization of $\sum\limits_{i=2}^{d_{\text{v}}^{\max}} \frac{\lambda_i}{i}$ subject to

1. the necessary condition for vanishing bit error probability in Theorem 3.2,

2. the satisfiability of the stability condition for all the MBIOS channels in the set $\mathcal{A}$ (see (3.9)),

3. the inequality constraints in (3.22) that follow from the information-theoretic bounds in [32],

one obtains a linear programming (LP) universal upper bound on the achievable rate of LDPC code ensembles over the set $\mathcal{A}$ of equi-capacity MBIOS channels with capacity C under BP decoding. This gives the following LP bound where, practically, the values of $x \in (0, B]$ in the first inequality constraint are quantized uniformly over this interval in order to get a finite number of inequality constraints in the LP problem (to be referred to as the 'LP1 bound'):

$$\boxed{\begin{array}{l}
\text{maximize } \sum_{i=2}^{d_{\text{v}}^{\max}} \frac{\lambda_i}{i} \\
\text{subject to} \\
\begin{cases}
B\lambda\big(\sqrt{1-\rho(1-x^2)}\big) < x, \quad \forall\, x \in (0, B] \\[2ex]
B\lambda_2 \rho'(1) \le 1 \\[2ex]
\sum_{i=2}^{\infty} \lambda_i = 1 \\[2ex]
\lambda_i \ge 0, \quad i = 2, 3, \ldots \\
\frac{1}{d_{\text{c}}} \le \sum_{i=2}^{d_{\text{v}}^{\max}} \frac{\lambda_i}{i} \le \frac{1}{(1-C)\, d_{\text{c}}} \cdot h_2\left(\frac{1-C^{\frac{d_{\text{c}}}{2}}}{2}\right)
\end{cases}
\end{array}}$$

Due to (3.20), LP1 also defines an upper bound on the design rate. This upper bound can also be translated into a universal lower bound on the achievable gap to capacity, $\varepsilon = 1 - R_{\text{d}}/C$.

This LP problem is solved numerically with the aid of the CVX Matlab-based modeling system for convex optimization (see [9]). Numerical results for the lower bound on the achievable gap to capacity are provided in Table 3.1 for the cases where $\rho(x) = x^7, x^9$, and x^{11} (i.e., the parity-check degree is fixed to 8, 10, and 12, respectively), and the maximal degree of the variable nodes is set to $d_{\text{v}}^{\max} = 200$.

In order to possibly improve the bound, let us consider the particular case where the set $\mathcal{A}$ forms a set of equi-capacity MBIOS channels that also includes the BEC. However, in this case, the LDPC code ensembles are not restricted to be right-regular. For a BEC, the condition for vanishing bit erasure probability under BP decoding assumes the form

$$(1-C)\lambda\big(1-\rho(1-x)\big) < x, \quad \forall\, 0 < x \le 1-C. \tag{3.23}$$

This condition is used instead of the necessary condition (3.10)[1]. Since in this LP the LDPC code ensemble is not assumed to be right-regular, the condition (3.22) that is a result of combining [32, Eqs. (43), (44) and (53)] and (3.20) assumes the form

$$\frac{1}{a_{\text{R}}} \leq \sum_{i=2}^{d_{\text{v}}^{\max}} \frac{\lambda_i}{i} \leq \frac{1}{(1-C)\, a_{\text{R}}} \cdot h_2\left(\frac{1-C^{\frac{a_{\text{R}}}{2}}}{2}\right),$$

where a_{R} is the average right degree of the LDPC code ensemble.

In this particular case where the set $\mathcal{A}$ includes the BEC, one gets the following LP problem (to be referred to as the 'LP2 bound'):

$$\boxed{\begin{array}{l} \text{maximize } \sum_{i=2}^{d_{\text{v}}^{\max}} \frac{\lambda_i}{i} \\ \text{subject to} \\ \begin{cases} (1-C)\lambda\big(1-\rho(1-x)\big) < x, \quad \forall\, 0 < x \leq 1-C \\[1em] B\lambda_2\rho'(1) \leq 1 \\[1em] \sum_{i=2}^{\infty} \lambda_i = 1 \\[1em] \lambda_i \geq 0, \quad i = 2, 3, \dots \\ \frac{1}{a_{\text{R}}} \leq \sum_{i=2}^{d_{\text{v}}^{\max}} \frac{\lambda_i}{i} \leq \frac{1}{(1-C)\, a_{\text{R}}} \cdot h_2\left(\frac{1-C^{\frac{a_{\text{R}}}{2}}}{2}\right) \end{cases} \end{array}}$$

where the values of $x \in (0, 1-C]$ are quantized uniformly over this interval in order to get a finite number of inequality constraints in the LP problem; our implementation converts the first inequality constraint above to 1000 inequality constraints where x is equally spaced, and it gets the values $x_k = 0.001(1-C)k$ for $k = 1, \dots, 1000$ (it was verified numerically that increasing the number of inequality constraints beyond one thousand, by a more refined uniform quantization of x over the interval $(0, 1-C]$, does not affect the numerical results of the LP2 bound). Numerical results for the lower bound on the achievable gap to capacity are provided in Table 3.2 for the same setting as in Table 3.1[2].

[1] It was verified numerically that adding condition (3.10) to the LP does not change the result. Thus, this condition is conjectured to be redundant in light of (3.23).

[2] Even though in the LP2 bound the LDPC code ensembles are not restricted to be right regular,

By comparing Tables 3.1 and 3.2, the values of the LP1 and LP2 bounds coincide for large values of the capacity C, whereas the LP2 bound shows an improved (larger) lower bound as compared to the LP1 bound for lower values of C. Note also that the two lower bounds become more significant (i.e., they become greater) as the value of capacity is increased. It is mentioned that the possible improvement in the LP2 bound stems from the fact that it applies to a set of equi-capacity MBIOS channels that includes the BEC, whereas the LP1 bound applies to any set of equi-capacity MBIOS channels.

It was observed numerically that the LP2 bound on the achievable gap to capacity is sensitive the value of $d_{\text{v}}^{\max}$, especially for large values of d_{c}. For example, for $C = \frac{1}{2}$ and $d_{\text{c}} = 12$, when $d_{\text{v}}^{\max} = 200$, the LP2 lower bound is equal to $1.94 \cdot 10^{-2}$ if , but when $d_{\text{v}}^{\max} = 500$ the LP2 lower bound becomes $7.38 \cdot 10^{-3}$.

for the purpose of comparing the results of the LP2 bound with those of the LP1 bound, we provide the numerical results for the same setting as for the LP1 bound.

Capacity	Set of all Equi-Capacity Channels			BEC + BIAWGNC			BEC		
(C)	$d_{\mathrm{c}} = 8$	$d_{\mathrm{c}} = 10$	$d_{\mathrm{c}} = 12$	$d_{\mathrm{c}} = 8$	$d_{\mathrm{c}} = 10$	$d_{\mathrm{c}} = 12$	$d_{\mathrm{c}} = 8$	$d_{\mathrm{c}} = 10$	$d_{\mathrm{c}} = 12$
$\frac{1}{2}$	$2.83 \cdot 10^{-3}$	$7.05 \cdot 10^{-4}$	$1.76 \cdot 10^{-4}$	$2.83 \cdot 10^{-3}$	$7.05 \cdot 10^{-4}$	$1.76 \cdot 10^{-4}$	$2.83 \cdot 10^{-3}$	$7.05 \cdot 10^{-4}$	$1.76 \cdot 10^{-4}$
$\frac{3}{4}$	$9.09 \cdot 10^{-2}$	$1.79 \cdot 10^{-2}$	$7.84 \cdot 10^{-3}$	$7.90 \cdot 10^{-2}$	$1.43 \cdot 10^{-2}$	$7.84 \cdot 10^{-3}$	$5.56 \cdot 10^{-2}$	$1.43 \cdot 10^{-2}$	$7.84 \cdot 10^{-3}$
$\frac{9}{10}$	$2.06 \cdot 10^{-1}$	$1.57 \cdot 10^{-1}$	$1.20 \cdot 10^{-1}$	$1.73 \cdot 10^{-1}$	$1.33 \cdot 10^{-1}$	$1.03 \cdot 10^{-1}$	$1.67 \cdot 10^{-1}$	$1.11 \cdot 10^{-1}$	$7.99 \cdot 10^{-2}$

Table 3.1: Lower bound on the universal achievable gap to capacity ($\varepsilon \triangleq 1 - \frac{R_{\mathrm{d}}}{C}$) for equi-capacity MBIOS channels under BP decoding; the degree of the parity-check nodes is fixed (d_{c}), and the maximal degree of the variable nodes is set to $d_{\mathrm{v}}^{\max} = 200$. These numerical results refer to the LP1 bound.

Capacity	Set of all Equi-Capacity Channels			BEC + BIAWGNC			BEC		
(C)	$d_{\mathrm{c}} = 8$	$d_{\mathrm{c}} = 10$	$d_{\mathrm{c}} = 12$	$d_{\mathrm{c}} = 8$	$d_{\mathrm{c}} = 10$	$d_{\mathrm{c}} = 12$	$d_{\mathrm{c}} = 8$	$d_{\mathrm{c}} = 10$	$d_{\mathrm{c}} = 12$
$\frac{1}{2}$	$1.50 \cdot 10^{-2}$	$9.01 \cdot 10^{-3}$	$1.94 \cdot 10^{-2}$	$1.25 \cdot 10^{-2}$	$6.76 \cdot 10^{-3}$	$1.73 \cdot 10^{-2}$	$7.34 \cdot 10^{-3}$	$1.79 \cdot 10^{-3}$	$1.22 \cdot 10^{-2}$
$\frac{3}{4}$	$9.09 \cdot 10^{-2}$	$4.24 \cdot 10^{-2}$	$2.75 \cdot 10^{-2}$	$7.90 \cdot 10^{-2}$	$3.99 \cdot 10^{-2}$	$2.42 \cdot 10^{-2}$	$6.59 \cdot 10^{-2}$	$3.56 \cdot 10^{-2}$	$1.93 \cdot 10^{-2}$
$\frac{9}{10}$	$2.06 \cdot 10^{-1}$	$1.57 \cdot 10^{-1}$	$1.20 \cdot 10^{-1}$	$1.73 \cdot 10^{-1}$	$1.33 \cdot 10^{-1}$	$1.03 \cdot 10^{-1}$	$1.67 \cdot 10^{-1}$	$1.11 \cdot 10^{-1}$	$7.99 \cdot 10^{-2}$

Table 3.2: Lower bound on the universal achievable gap to capacity ($\varepsilon \triangleq 1 - \frac{R_{\mathrm{d}}}{C}$) for equi-capacity MBIOS channels under BP decoding; the degree of the parity-check nodes is fixed (d_{c}), and the maximal degree of the variable nodes is set to $d_{\mathrm{v}}^{\max} = 200$. These numerical results refer to the LP2 bound.

3.3 Universal Conditions for Reliable Communications under Belief Propagation Decoding

We prove in this section the following theorem and exemplify its use:

Theorem 3.3 [Universal Conditions on the B-parameter for Good/ Bad Communications under BP Decoding] Let $\{(n, \lambda, \rho)\}$ be a sequence of LDPC code ensembles whose block lengths tend to infinity. The following universal properties hold under BP decoding:

- This sequence achieves vanishing bit error probability under BP decoding for *every* MBIOS channel whose B-parameter is less than

$$B_0(\lambda, \rho) \triangleq \inf_{x \in (0,1]} \frac{x}{\lambda\big(1 - \rho(1-x)\big)}. \tag{3.24}$$

- For a *right-regular* sequence, it does not achieve reliable communications over *any* MBIOS channel whose B-parameter is greater than

$$B_1(\lambda, \rho) \triangleq \inf_{x \in (0,1]} \frac{x}{\lambda\big(\sqrt{1 - \rho(1-x^2)}\big)}. \tag{3.25}$$

  For every MBIOS channel whose B-parameter B satisfies $B > B_1(\lambda, \rho)$, BP decoding is not reliable in the sense that the left-to-right message error probability (i.e., the average probability of error for a message emanating from a variable node to a parity-check node) is greater than the positive value

$$\left(\frac{1}{2} \max\left\{x \in (0,1] : \frac{x}{\lambda\big(\sqrt{1-\rho(1-x^2)}\big)} \leq B\right\}\right)^2 \tag{3.26}$$

  irrespective of the number of iterations performed by the BP decoder.

Proof: We start by proving the first part of the theorem. Let $\{a_l\}$ be the sequence of symmetric L-densities that are obtained from the density evolution equation (3.1) (where $l \geq 0$ denotes the number of iterations). From (2.4), it follows that a necessary and sufficient condition for obtaining vanishing bit error probability under BP decoding is that the B-parameter that is associated with the *pdf* a_l tends to zero, i.e.,

$$\lim_{l \to \infty} \mathcal{B}(a_l) = 0. \tag{3.27}$$

From (3.2), it follows that if the sequence $\{y_l\}$ as defined in (3.4) by the recursive equation

$$y_l = B\lambda\big(1 - \rho(1 - y_{l-1})\big), \quad l = 1, 2, \ldots$$

with the initial condition $y_0 = B$ tends to zero, then also the sequence $\{x_l\}$ where

$$x_l = \mathcal{B}(a_l)$$

tends to zero (since $0 \leq x_l \leq y_l$ for every integer $l \geq 0$, see (3.4) and the paragraph that follows). The sequence $\{y_l\}$ refers to the density evolution analysis for a BEC whose channel erasure probability is B. The threshold value, which determines a necessary and sufficient condition for the convergence of the sequence $\{y_l\}$ to zero, yields that if $B < B_0(\lambda, \rho)$ then $\lim_{l\to\infty} y_l = 0$ (this follows from [29, Theorem 3.59]). Hence, for every MBIOS channel, if the B-parameter is less than $B_0(\lambda, \rho)$, then the property in (3.27) is satisfied, and therefore the bit error probability vanishes under BP decoding. This completes the proof of the first part.

In order to prove the second part of the theorem, which refers to a sequence of right-regular LDPC code ensembles, we rely on inequality (3.14). If the equality in (3.27) holds, then it follows from (3.14) that the sequence $\{z_l\}$ in (3.18) should necessarily tend to zero. Hence, from (2.4), if the sequence that is defined in (3.18) via the recursive equation

$$z_l = B\lambda\Big(\sqrt{1 - \rho(1 - z_{l-1}^2)}\Big), \quad l = 1, 2, \ldots$$

stays bounded away from zero, with the initial value $z_0 = B$, then the communication is not reliable. More explicitly, for every MBIOS channel whose B-parameter is greater than $B_1(\lambda, \rho)$, the sequence $\{\mathcal{E}(a_l)\}$ that represents the left-to-right message error probabilities under BP decoding stays bounded away from zero (irrespective of the number of iterations). In order to proceed, the following lemma considers the convergence of the sequence $\{z_l\}$.

Lemma 3.3 Let $B_1(\lambda, \rho)$ be defined as in (3.25). If $B < B_1(\lambda, \rho)$ then the sequence $\{z_l\}$ in (3.18) tends to zero, and if $B > B_1(\lambda, \rho)$ then the sequence $\{z_l\}$ is lower bounded by the positive constant

$$x(B) \triangleq \max\left\{ x \in (0, 1] : \frac{x}{\lambda\Big(\sqrt{1 - \rho(1 - x^2)}\Big)} \leq B \right\}. \tag{3.28}$$

Proof: See Appendix C. ■

From (3.14),

$$\mathcal{B}(a_l) \triangleq x_l \geq z_l, \quad l = 0, 1, \ldots$$

and therefore it follows from Lemma 3.3 that for every MBIOS channel whose B-parameter is greater than $B_1(\lambda, \rho)$

$$\mathcal{B}(a_l) \geq x(B), \quad l = 0, 1, \ldots .$$

From (2.4),

$$\mathcal{B}(a_l) \leq 2\sqrt{\mathcal{E}(a_l)(1 - \mathcal{E}(a_l))} \leq 2\sqrt{\mathcal{E}(a_l)}$$
$$\Rightarrow \mathcal{E}(a_l) \geq \left(\frac{\mathcal{B}(a_l)}{2}\right)^2 \geq \left(\frac{x(B)}{2}\right)^2$$

and therefore the left-to-right message error probability cannot be reduced below the positive value as above, irrespective of the number of iterations of the BP decoder. This completes the proof of Theorem 3.3. ■

Corollary 3.2 For every MBIOS channel with B-parameter $B > B_1(\lambda, \rho)$, let $x(B)$ be defined as in (3.28). Then, the (average) left-to-right message error probability is bounded away from zero by the universal bound

$$\eta \triangleq \lim_{B \to B_1(\lambda,\rho)^+} \left(\frac{x(B)}{2}\right)^2 \tag{3.29}$$

irrespective of the number of iterations of the BP decoder.

Proof: By definition, $x(B)$ in (3.28) is an increasing function of B, and therefore we take the limit $B \to B_1(\lambda, \rho)$, where the limit is from the right side, in order to obtain a lower bound on the left-to-right message error probability for the case where $B > B_1(\lambda, \rho)$. ■

Corollary 3.3 Let $\{(n, \lambda, \rho)\}$ be a sequence of right-regular LDPC code ensembles whose block lengths tend to infinity. Then, the left-to-right message error probability stays bounded away from zero under BP decoding for every MBIOS channel whose B-parameter is greater than

$$B_2(\lambda, \rho) \triangleq \min\left\{B_1(\lambda, \rho), \frac{1}{\lambda'(0)\rho'(1)}, \sqrt{1 - R_{\mathrm{d}}^2}\right\} \tag{3.30}$$

where B_1 is introduced in (3.25), and

$$R_{\mathrm{d}} \triangleq 1 - \frac{\int_0^1 \rho(x)\,\mathrm{d}x}{\int_0^1 \lambda(x)\,\mathrm{d}x}$$

designates the design rate.

Proof: If the B-parameter B is greater than $B_1(\lambda, \rho)$, then the statement follows from the second part of Theorem 3.3. Also, if $B > \frac{1}{\lambda'(0)\rho'(1)}$, then the communication under BP decoding is not reliable because the stability condition is not satisfied. Finally, if $B > \sqrt{1 - R_{\mathrm{d}}^2}$ then it follows from the right-hand side of (2.3) that $R_{\mathrm{d}} > C$ and error-free communication cannot be achieved when the design rate exceeds the channel capacity. Therefore, BP decoding is not reliable for any MBIOS channel whose B-parameter is greater than B_2 in (3.30). ■

Remark 3.1 In essence, the results of this chapter stem from one dimensional bounds based on the density evolution equation that utilize the B-parameter (namely, inequalities (3.2) and (3.14)). This approach is not new, and was introduced in [3]. In that paper, the authors derived iterative bounds on the expectation of messages transferred in BP decoding. These bounds enabled them to lower- and upper-bound the performance of BP decoding.

Remark 3.2 Inequalities (3.2) and (3.14) were first proved by Wang, et al. in [46]. They mention that these inequalities can be used iteratively to derive upper and lower bounds on the decoding threshold based on the initial Bhattacharyya parameter of the channel, and that closed-form solutions for these bounds can be obtained, but do not derive them explicitly. In this work, we have independently shown these inequalities and have also explicitly derived a closed-form solution of the bounds. Moreover, we have shown a lower bound on the decoding error probability when the Bhattacharyya parameter of the channel exceeds the value in (3.30).

Although here we concentrate only on channels with symmetric outputs, we note that [46, Theorem 4] extended inequalities (3.2) and (3.14) also to memoryless channels with binary input and non-symmetric output, under the assumption that the input distribution is uniform.

Remark 3.3 Note that if the B-parameter is above $B_2(\lambda, \rho)$ (see (3.30)), then Corollary 3.3 does not specify an explicit positive lower bound on the left-to-right message error probability under BP decoding. However, if $B > B_1(\lambda, \rho)$ (where it readily follows from (3.30) that $B_1(\lambda, \rho) \geq B_2(\lambda, \rho)$), then the second part of Theorem 3.3 determines an explicit positive lower bound on the left-to-right message error probability that is valid universally for all MBIOS channels. As shown in Examples 3.1 and 3.2 that follow, the value of this lower bound η (see (3.29)) is typically large, irrespective of the number of iterations of the BP decoder, and this lower bound holds for all MBIOS channels whose B-parameter is above $B_1(\lambda, \rho)$.

Remark 3.4 All channels in the convex hull[3] of equi-capacity MBIOS channels have the same capacity. Similarly, all channels in the convex hull of equi-B-parameter MBIOS channels have the same B-parameter. This is due to the linearity of the capacity and Bhattacharyya functionals in the L-density function, see (2.1) and (2.2). Therefore, the condition for good channels, under BP decoding, in the sense that $B < B_0(\lambda, \rho)$ (see the first part of Theorem 3.3) or the condition for bad channels in the sense that $B > B_2(\lambda, \rho)$ (see the second part of Theorem 3.3 and Corollaries 3.2 and 3.3) are both preserved, respectively, for the convex hull of good or bad channels. Although this conclusion does not prove [31, Conjecture 1] for equi-capacity MBIOS channels (since it does not cover the case where B is between B_0 and B_2 in case that $B_0 < B_2$), it supports this conjecture in the cases where $B < B_0$ or $B > B_2$.

Remark 3.5 From the two parts of Theorem 3.3, it follows directly that for right-regular codes, $B_1(\lambda, \rho) \geq B_0(\lambda, \rho)$. For a direct proof of this inequality, see Appendix D.

In the following, we exemplify the use of Theorem 3.3 and its corollaries:

Example 3.1 [Regular LDPC Code Ensembles] In Table 3.3, we show the numerical values of B_0 and B_1 in Theorem 3.3, and the value of η in Corollary 3.2 for some regular LDPC code ensembles whose design rate is one-half. The value of B_0 corresponds to the threshold for the BEC under BP decoding, and the value of B_1

[3] The convex hull of a set $\mathcal{A}$ of channels consists of all the channels that are convex combinations of channels in $\mathcal{A}$. A convex combination of several channels is the result of using each channel with probability θ_i, $0 \leq \theta_i \leq 1$, such that $\sum_i \theta_i = 1$.

(see (3.25)) refers to the value of the B-parameter where above it, the left-to-right message error probability is at least η, no matter how many iterations of the BP decoder are performed. For these regular LDPC code ensembles, $\lambda_2 = 0$, and therefore the stability condition is useless. Also, since the design rate of these ensembles is equal to one-half, then $\sqrt{1 - R_{\mathrm{d}}^2} = \frac{\sqrt{3}}{2} \approx 0.8660$, hence the values of B_2 in (3.30) coincide with B_1 for these ensembles.

LDPC	B_0	B_1	η
(3,6)	0.4294	0.6553	$6.50 \cdot 10^{-2}$
(4,8)	0.3834	0.6192	$6.58 \cdot 10^{-2}$
(5,10)	0.3416	0.5884	$6.18 \cdot 10^{-2}$

Table 3.3: The numerical values of B_0 and B_1 in Theorem 3.3, and the value of η in Corollary 3.2 for some regular LDPC code ensembles whose design rate is one-half.

Example 3.2 [Optimized Right-Regular LDPC Code Ensembles for the BEC, and their Universal Properties] In Table 3.4, right-regular LDPC code ensembles are optimized for the BEC under BP decoding; to this end, a linear program is solved as described in [29, Section 3.18] for a design rate of one-half ($R_{\mathrm{d}} = \frac{1}{2}$) and for a maximal degree of the variable nodes of one hundred ($d_{\mathrm{v}}^{\max} = 100$).

$\lambda(x) = \sum_i \lambda_i x^{i-1}$	$\rho(x) = \sum_i \rho_i x^{i-1}$	B_0	B_2	B_1	η
$\lambda_2 = 0.4127,\ \lambda_3 = 0.1762$ $\lambda_4 = 0.1177,\ \lambda_7 = 0.1202$ $\lambda_8 = 0.1731$	$\rho_6 = 1$	0.4816	0.4846	0.7066	$8.45{\cdot}10^{-2}$
$\lambda_2 = 0.2879,\ \lambda_3 = 0.1222$ $\lambda_4 = 0.0905,\ \lambda_6 = 0.1174$ $\lambda_7 = 0.0300,\ \lambda_{12} = 0.0807$ $\lambda_{13} = 0.0831,\ \lambda_{32} = 0.0050$ $\lambda_{33} = 0.1831$	$\rho_8 = 1$	0.4962	0.4962	0.7146	$1.02{\cdot}10^{-1}$
$\lambda_2 = 0.2226,\ \lambda_3 = 0.1013$ $\lambda_4 = 0.0504,\ \lambda_5 = 0.0646$ $\lambda_6 = 0.0445,\ \lambda_{10} = 0.1219$ $\lambda_{11} = 0.0117,\ \lambda_{24} = 0.0903$ $\lambda_{25} = 0.0678,\ \lambda_{100} = 0.2248$	$\rho_{10} = 1$	0.4988	0.4992	0.7123	$1.08{\cdot}10^{-1}$

Table 3.4: The degree distributions (from the edge perspective), numerical values of B_0 and B_1 in Theorem 3.3, the value of η in Corollary 3.2, and the value of B_2 in Corollary 3.3 for some optimized right-regular LDPC code ensembles whose design rate is one-half with a maximal degree of the variable nodes that is set to 100.

We observe from Table 3.4 that for these ensembles, $B_0 \approx B_2$. Hence, for these optimized LDPC code ensembles, the first part of Theorem 3.3 states that these LDPC code ensembles are reliable under BP decoding, in the sense of achieving vanishing bit error probability, for every MBIOS channel whose B-parameter is below B_0; on the other hand, Corollary 3.3 implies that these code ensembles are not reliable under BP decoding for every MBIOS channel whose B-parameter is slightly above B_0 or greater than this value. This is a universal result that applies to all MBIOS channels, and it separates them into two sets of "good" or "bad" channels for which the reliability of these code ensembles under BP decoding solely depends on the B-parameter of the communication channel *without any relevance to its channel model* (as long as it is MBIOS, and it exhibits a given B-parameter).

In contrast to the results in Table 3.3 that apply to regular LDPC code ensembles, for the right-regular LDPC code ensembles studied in this example, the value of B_1 is significantly greater than B_2, which here is given by the stability condition. In continuation to Remark 3.3, the lower bound on the left-to-right message error probabilities when the B-parameter is greater than B_1 is rather large (around 0.1), whereas such a measure is not provided here for the unreliability of the messages when the B-parameter is between B_1 and B_2.

The results of this thesis imply that a family of degraded channels can be parameterized by the B-parameter. This is also supported by [29, Theorem 4.76], which states that a degraded channel has a higher B-parameter than the original (see also Proposition 2.2 in this thesis). Moreover, in many cases there is a simple one-to-one correspondence between the channel parameter and the B-parameter. For example, for a BEC with erasure probability ϵ, we have $B = \epsilon$; for a BSC with crossover probability p, we have $B = \sqrt{4p(1-p)}$; and for a BIAWGN channel with noise variance σ^2, we have $B = e^{-\frac{1}{2\sigma^2}}$.

In order to obtain bounds on any LDPC code ensemble, not necessarily right-regular, a simple modification of Theorem 3.3 and Corollary 3.3 yields the following:

Corollary 3.4 Let $\{(n, \lambda, \rho)\}$ be a sequence of (not necessarily right-regular) LDPC code ensembles whose block lengths tend to infinity. Then

- This sequence achieves vanishing bit error probability under BP decoding for *every* MBIOS channel whose B-parameter is less than

$$B_0(\lambda,\rho) \triangleq \inf_{x\in(0,1]} \frac{x}{\lambda\big(1-\rho(1-x)\big)}.$$

- The left-to-right message error probability of this sequence stays bounded away from zero under BP decoding for every MBIOS channel whose B-parameter is greater than

$$B_3(\lambda,\rho) \triangleq \begin{cases} \min\left\{B_1(\lambda,\rho), \dfrac{1}{\lambda'(0)\rho'(1)}, \sqrt{1-R_{\mathrm{d}}^2}\right\}, & \\ \qquad\qquad\qquad\qquad \text{if the sequence is right-regular} & \\ \min\left\{\dfrac{1}{\lambda'(0)\rho'(1)}, \sqrt{1-R_{\mathrm{d}}^2}\right\}, & \\ \qquad\qquad\qquad\qquad \text{if the sequence is not right-regular} & \end{cases}$$

  where B_1 is introduced in (3.25), and R_{d} designates the design rate.

It follows that for any family of MBIOS channels there exists a B_{th} between B_0 and B_3 (its exact value is dependent on the family) such that BP converges for all channels of this family with $B < B_{\mathrm{th}}$ and does not converge for channels of the family with $B > B_{\mathrm{th}}$. Hence, $B_0(\lambda,\rho)$ and $B_3(\lambda,\rho)$ provide universal lower and upper bounds on the threshold B-parameter. In general, different channel families will have different thresholds. It should be noted that the lower bound is tight for the BEC. Furthermore, this universal bound is non-iterative, simple, and easy to compute.

Similar bounds on the Bhattacharyya parameters have been derived in [46]. In that paper, the authors have derived the same inequalities on the Bhattacharyya parameter evolution during BP decoding that have led to the bounds on the threshold in this section. Therefore, the lower bound $B_0(\lambda,\rho)$ and the upper bound $B_1(\lambda,\rho)$ are not new. In this thesis, however, we have combined the upper bound $B_1(\lambda,\rho)$ with other upper bounds, such as the stability condition, to arrive at a tighter upper bound in some cases. Moreover, we have also demonstrated that these bounds can be tight in some cases, as shown in Table 3.4.

Other works, such as [17], [29, Section 4.10.2], and [41] used an information-combining approach to also provide universal bounds on the threshold. These bounds give upper and lower bounds on the capacity of the channel, another natural parameter for channel degradation (a degraded channel has lower capacity). These bounds are significantly more difficult to compute, requiring either an iterative process or involving computations that are numerically unstable for high left degrees.

In Table 3.5, we compare the bounds suggested by this approach with the bounds of [41] for some of the ensembles considered in this thesis. In order to make the comparison, we translate the bounds on the B-parameter to bounds on the channel parameters for a BSC and a BIAWGN channel. It is exemplified that the bounds in [41] are superior for the regular LDPC code ensembles, but the bounds of the approach presented here are more informative for the irregular LDPC code ensembles shown in Table 3.5.

$\lambda(x) = \sum_i \lambda_i x^{i-1}$	$\rho(x) = \sum_i \rho_i x^{i-1}$		Bounds based on B	Bounds based on C
$\lambda_3 = 1$	$\rho_6 = 1$		$0.4294 < B < 0.6553$	$0.4744 < C < 0.6350$
		BSC:	$0.0485 < p < 0.1223$	$0.0698 < p < 0.1187$
		BIAWGN:	$0.7691 < \sigma < 1.0877$	$0.8026 < \sigma < 1.0180$
$\lambda_4 = 1$	$\rho_8 = 1$		$0.3834 < B < 0.6192$	$0.5160 < C < 0.6630$
		BSC:	$0.0382 < p < 0.1074$	$0.0624 < p < 0.1048$
		BIAWGN:	$0.7222 < \sigma < 1.0214$	$0.7707 < \sigma < 0.9553$
$\lambda_5 = 1$	$\rho_{10} = 1$		$0.3416 < B < 0.5844$	$0.5564 < C < 0.6970$
		BSC:	$0.0301 < p < 0.0943$	$0.0540 < p < 0.0921$
		BIAWGN:	$0.6822 < \sigma < 0.9648$	$0.7333 < \sigma < 0.8996$
$\lambda_2 = 0.4127,\ \lambda_3 = 0.1762$ $\lambda_4 = 0.1177,\ \lambda_7 = 0.1202$ $\lambda_8 = 0.1731$	$\rho_6 = 1$		$0.4816 < B < 0.4846$	$0.4147 < C < 0.8980$
		BSC:	$0.0618 < p < 0.0626$	$0.0133 < p < 0.1404$
		BIAWGN:	$0.8272 < \sigma < 0.8308$	$0.5182 < \sigma < 1.1209$
$\lambda_2 = 0.2879,\ \lambda_3 = 0.1222$ $\lambda_4 = 0.0905,\ \lambda_6 = 0.1174$ $\lambda_7 = 0.0300,\ \lambda_{12} = 0.0807$ $\lambda_{13} = 0.0831,\ \lambda_{32} = 0.0050$ $\lambda_{33} = 0.1831$	$\rho_8 = 1$		$0.4962 \leq B \leq 0.4962$	$0.3989 < C < 0.8910$
		BSC:	$0.0659 \leq p \leq 0.0659$	$0.0144 < p < 0.1465$
		BIAWGN:	$0.8446 \leq \sigma \leq 0.8447$	$0.5265 < \sigma < 1.1513$

Table 3.5: Comparison of universal bounds on thresholds for various LDPC code ensembles. The bounds based on the B-parameter are computed based on the approach presented in this thesis; the bounds based on the capacity are computed according to [41].

Comparing these information-combining results by Land et al. [17], and by Sutskover et al. ([41, 42]) with our bounds, there is one conceptual difference: for $B > B_1$, Theorem 3.3 and Corollary 3.2 provide an explicit lower bound on the left-to-right message error probability that is irrespective of the number of iterations, whereas this is not the case in these related works. Secondly, for the regular LDPC code ensembles, for which we have $B_3 = B_1$, we also have an explicit positive lower bound on the left-to-right message error probability for the case where the B-parameter is larger than B_3 (e.g., as shown in Table 3.3, for the (3,6) LDPC code ensemble, a lower bound on the left-to-right message error probability around 6.5% applies to the cases where $p > 0.1223$ or $\sigma > 1.088$ for the BSC and the binary-input AWGN channel, respectively).

The observation made in Example 3.2, regarding the reliability of the optimized right-regular LDPC code ensembles over the entire set of MBIOS channels where this result solely depends on the B-parameter of the communication channel (but not on the specific channel model of the MBIOS channel) calls for analysis. Since these LDPC code ensembles were optimized numerically (via linear programming), closed forms for the degree distributions are not available, and we turn instead to consider the sequences of right-regular LDPC code ensembles as suggested by Shokrollahi [40]. In this respect, the following theorem demonstrates a universality property under BP decoding with respect to the entire set of MBIOS channels that exhibit a given B-parameter; the following theorem shows that not only the stability condition is common for the considered set of channels, but also a universality property exists for this set.

Theorem 3.4 [Universality of LDPC Code Ensembles under BP Decoding for MBIOS Channels with a Fixed B-Parameter] Consider the set of MBIOS channels that exhibit a fixed B-parameter (B). Then:

- Every capacity-achieving sequence designed for BEC(B), universally achieves the following fraction of capacity for the considered set of channels:

$$\mu_3(B) \triangleq \frac{1-B}{1-h_2\left(\frac{1-\sqrt{1-B^2}}{2}\right)}, \tag{3.31}$$

  where h_2 denotes the binary entropy function to the base 2. The function μ_3 is monotonic decreasing in B; it gets the values $\ln 2 \approx 69.3\%$ and 100% for the extreme cases where $B \to 1$ (i.e., a very noisy channel) and $B \to 0$ (i.e., a perfect channel), respectively.

- There exists an explicit construction of a sequence of right-regular LDPC code ensembles for which B satisfies

$$B \leq B_0 \leq B_2 \leq 1 - \left(\frac{d_{\text{c}} - 2}{d_{\text{c}} - 1}\right)^{\frac{\pi^2}{6}} e^{\frac{1}{d_{\text{c}}-1}\left(\frac{\pi^2}{6} - \gamma\right)} (1 - B) \tag{3.32}$$

  so B_0 and B_2 can be made arbitrarily close to B for large d_{c}. Here d_{c} denotes the fixed degree of parity-check nodes, B_0 and B_2 are introduced in (3.24) and (3.30) respectively, and $\gamma \approx 0.5772$ denotes Euler's constant.

Proof: Among all MBIOS channels which exhibit a given B-parameter B, the capacity is maximized or minimized for a BSC and BEC, respectively. For a BEC, $C = 1 - B$, and therefore the capacity is achieved (i.e., $R_{\text{d}} = C$) because of (3.5). For a BSC whose crossover probability is p,

$$C = 1 - h_2(p), \quad B = \sqrt{4p(1-p)}$$

and therefore

$$C = 1 - h_2\left(\frac{1 - \sqrt{1 - B^2}}{2}\right).$$

From (3.5), the fraction of capacity that is universally achieved for the entire set of MBIOS channels which exhibit a given B-parameter B satisfies

$$\frac{1 - B}{1 - h_2\left(\frac{1-\sqrt{1-B^2}}{2}\right)} \leq \frac{R_{\text{d}}}{C} \leq 1 \tag{3.33}$$

where the upper and lower bounds are obtained, respectively, for a BEC and BSC with a B-parameter B. Let us check the two extreme cases where $B = 0$ and $B \to 1$ (referring, respectively, to an ideal channel and a very noisy channel). In the case where $B = 0$, the upper and lower bounds coincide, and are equal to 1; hence, capacity is achievable. For examining the case where $B \to 1$, we rely on the following Taylor series expansion of the binary entropy function around $x = \frac{1}{2}$ (see [47, p. 575]):

$$h_2(x) = 1 - \frac{1}{2 \ln 2} \sum_{q=1}^{\infty} \frac{(1-2x)^{2q}}{q(2q-1)}, \quad 0 \leq x \leq 1 \tag{3.34}$$

which enables to calculate the limit of the left-hand side in (3.33) when $B \to 1$ (from below). This gives

$$\begin{aligned}
&\lim_{B \to 1^-} \frac{1-B}{1-h_2\left(\frac{1-\sqrt{1-B^2}}{2}\right)} \\
&= \lim_{B \to 1^-} \frac{1-B}{\frac{1}{2\ln 2}\sum_{q=1}^{\infty}\frac{(1-B^2)^q}{q(2q-1)}} \\
&= \lim_{B \to 1^-} \frac{1-B}{\left(\frac{1-B^2}{2\ln 2}\right)} \\
&= \ln 2.
\end{aligned}$$

Moreover, it is easy to verify with (3.34) that the lower bound on $\frac{R_{\mathrm{d}}}{C}$ in (3.33) forms a monotonic decreasing function of B (where $0 \leq B < 1$); it varies from 1 to $\ln 2 \approx 0.693$ as the value of B is increased from zero to 1 bit per channel use. This shows that, for the entire set of MBIOS channels which exhibit a given B-parameter B, the achievable fraction (3.5) of capacity is at least 69.3%; this result is obtained by designing a capacity-achieving sequence of LDPC code ensembles for a BEC whose B-parameter matches our channel (as above). Interestingly, these two extreme values (i.e., 69.3% and 100%) coincide with those obtained in Theorem 3.1 for the entire set of equi-capacity MBIOS channels.

To prove the second part of the Theorem, we consider a sequence of right-regular LDPC code ensembles with a fixed right-degree d_{c}, and parameters of the degree distributions that are selected according to [33, Theorem 2.3] for a BEC with channel erasure probability B (see also [29, Section 3.15] and [32, Appendix VI]). These sequences are capacity-achieving as we let the right degree d_{c} tend to infinity. From [33, Theorems 2.1 and 2.3], this sequence is constructed to achieve at least a fraction $1-\varepsilon$ of the capacity of the BEC under BP decoding with a right degree d_{c} that scales logarithmically with the reciprocal of the gap to capacity, i.e., it behaves like $\log \frac{1}{\varepsilon}$.

For a BEC, the B-parameter of the channel is equal to the channel erasure probability. The sequence of right-regular LDPC code ensembles is designed to achieve vanishing bit erasure probability under BP decoding for a BEC whose channel erasure probability is set to B (since, by assumption, the parameters (α and N) of its degree distributions are selected according to [33, Theorem 2.3]). Hence, the threshold of this sequence, B_0, under BP decoding is greater than or equal to B. This proves the left-hand side of inequality (3.32).

We derive in the following the upper bound on B_2 in this inequality, based on [32, Appendix VI]. More explicitly, let $c(\alpha, N)$ be the function (see [32, Eq. (116)])

$$c(\alpha, N) \triangleq (1-\alpha)^{\frac{\pi^2}{6}} \; e^{\alpha\left(\frac{\pi^2}{6}-\gamma+\frac{1}{2N}\right)} \, . \tag{3.35}$$

for $0 < \alpha < 1$ and an integer $N \geq 1$ (on the right-hand side of this equality, $\gamma \approx 0.5772$ denotes Euler's constant). The fraction of edges attached to degree-2 variable nodes, for this right-regular sequence, satisfies (see [32, Eq. (117)])

$$\frac{\alpha}{1 - c(\alpha, N)\,(1-B)} < \lambda_2 \leq \frac{\alpha}{B} \tag{3.36}$$

where $\alpha \triangleq \frac{1}{d_{\rm c}-1}$. From (3.30), (3.35) and (3.36)

$$\begin{aligned} B_2 &\leq \frac{1}{\lambda'(0)\rho'(1)} \\ &= \frac{\alpha}{\lambda_2} \\ &\leq 1 - c(\alpha, N)(1-B) \\ &= 1 - (1-\alpha)^{\frac{\pi^2}{6}} e^{\alpha\left(\frac{\pi^2}{6}-\gamma+\frac{1}{2N}\right)} (1-B) \\ &\leq 1 - (1-\alpha)^{\frac{\pi^2}{6}} e^{\alpha\left(\frac{\pi^2}{6}-\gamma\right)} \, (1-B) \\ &= 1 - \left(\frac{d_{\rm c}-2}{d_{\rm c}-1}\right)^{\frac{\pi^2}{6}} \, e^{\frac{1}{d_{\rm c}-1}(\frac{\pi^2}{6}-\gamma)} \, (1-B). \end{aligned}$$

This completes the proof of (3.32). Following the first part of Theorem 3.3 and Corollary 3.3, it follows that in the limit where $d_{\rm c} \to \infty$, $B_2 \leq 1 - (1-B) = B$, so that (3.32) yields that $B_0 = B_2 = B$. Hence,

- the BP decoder achieves vanishing bit error probability for every MBIOS channel whose B-parameter is less than B,
- it is unreliable (i.e., the left-to-right message error probability is bounded away from zero) for every MBIOS channel whose B-parameter is greater than B.

This completes the proof of Theorem 3.4. ■

Remark 3.6 Another way to prove the first part of the above theorem is via use of the approach of sub-section 3.1. In the setting of Theorem 3.4, the family of MBIOS channels being considered is the one that exhibits the same B-parameter (regardless of capacity). Over this family, the BSC and BEC exhibit the maximal and minimal capacities, respectively. Following the approach of sub-section 3.1, we construct a capacity-achieving sequence of LDPC ensembles for a BEC with erasure probability B. The design rate of this ensemble is $R_{\text{d}} = 1 - B$. Since the BSC exhibits the maximal capacity over this set of MBIOS channels, the universally achievable fraction of capacity is $\frac{R_{\text{d}}}{C}$, where C is the capacity of a BSC with B-parameter B. Using the expressions for R_{d} and C we obtain that the universally achievable fraction of capacity is indeed $\mu_3(B)$.

Table 3.6 shows the resulting achievable fraction of capacity in (3.31) as a function of the B-parameter of the considered set of MBIOS channels.

B	$\mu_3(B)$
0	100%
0.250	85.0%
0.333	82.0%
0.500	77.5%
0.750	72.7%
1.000	69.3%

Table 3.6: Universal achievable fraction of capacity under BP decoding for the entire set of MBIOS channels which exhibit a given B-parameter B (see Theorem 3.4).

Corollary 3.5 In the limit where $d_{\text{c}} \to \infty$, the BP decoder in Theorem 3.4 achieves vanishing bit error probability for all MBIOS channels whose B-parameter is less than B, and it is unstable for every MBIOS channel whose B-parameter is greater than B. For finite d_{c}, the values of B_0 and B_2 differ from B by at most

$$(1-B)\left(\frac{\gamma}{d_{\text{c}}-1} + \left(\frac{\pi^2}{6} - \gamma\right)\frac{\pi^2/6}{(d_{\text{c}}-1)^2}\right),$$

and this difference tends uniformly to zero for $0 \le B \le 1$ as we let d_{c} tend to infinity.

Proof: The first part of this corollary, for infinite d_{c}, is immediate from (3.32). For finite d_{c}, subtracting B from (3.32) yields

$$0 \leq B_0 - B \leq B_2 - B \leq (1-B)\left(1 - \left(\frac{d_{\mathrm{c}}-2}{d_{\mathrm{c}}-1}\right)^{\frac{\pi^2}{6}} e^{\frac{1}{d_{\mathrm{c}}-1}\left(\frac{\pi^2}{6}-\gamma\right)}\right). \tag{3.37}$$

Bernoulli's inequality states that $(1+x)^r \geq 1+rx$ for $x > -1$, $r \geq 1$. Thus,

$$\left(\frac{d_{\mathrm{c}}-2}{d_{\mathrm{c}}-1}\right)^{\frac{\pi^2}{6}} = \left(1 - \frac{1}{d_{\mathrm{c}}-1}\right)^{\frac{\pi^2}{6}} \geq 1 - \frac{\pi^2/6}{d_{\mathrm{c}}-1} \tag{3.38}$$

Moreover, for every $y > 0$ we have $e^y \geq 1+y$, so that

$$e^{\frac{1}{d_{\mathrm{c}}-1}\left(\frac{\pi^2}{6}-\gamma\right)} \geq 1 + \frac{\pi^2/6-\gamma}{d_{\mathrm{c}}-1}. \tag{3.39}$$

Using (3.37)–(3.39) gives

$$\begin{aligned}0 \leq B_0 - B \leq B_2 - B &\leq (1-B)\left(1 - \left(1 - \frac{\pi^2/6}{d_{\mathrm{c}}-1}\right)\left(1 + \frac{\pi^2/6-\gamma}{d_{\mathrm{c}}-1}\right)\right) \\ &= (1-B)\left(\frac{\gamma}{d_{\mathrm{c}}-1} + \left(\frac{\pi^2}{6}-\gamma\right)\frac{\pi^2/6}{(d_{\mathrm{c}}-1)^2}\right).\end{aligned}$$

From the above inequality it is clear that as we let $d_{\mathrm{c}} \to \infty$, the differences $B_0 - B$ and $B_2 - B$ tend to zero uniformly. ■

Example 3.3 For ensemble no. 2 in Table 3.4, whose design rate is $R_{\mathrm{d}} = \frac{1}{2}$ bits per channel use, the threshold under BP decoding corresponds *uniformly* to the B-parameter $B = 0.4962$ for every MBIOS channel. For the BEC, this corresponds to capacity of $C = 1 - B = 0.5038$ bits per channel use, and therefore 99.3% of the capacity of the BEC is achieved under BP decoding with vanishing bit erasure probability. For the BIAWGN channel, this corresponds to channel capacity $C = 0.5977$ bits per channel use, and therefore this code ensemble achieves 83.4% of the capacity for this channel. The smallest fraction of capacity under BP decoding is achieved for the BSC. The B-parameter $B = 0.4962$ corresponds to $C = 0.6496$ for the BSC, which means that 77.0% of capacity is achieved under BP decoding.

Example 3.4 In this example, we consider a right-regular LDPC code ensemble, whose design rate is $R_\mathrm{d} = 0.9$ bits per channel use, and which closely approaches the capacity of the BEC under BP decoding. To this end, we set the degree of the parity-check nodes to be 40, and the maximal variable node degree is set to 200. The following degree distributions are obtained by linear programming with the approach in [29, Section 3.18]:

$$\begin{aligned}\lambda(x) =& 0.2638x + 0.1259x^2 + 0.1088x^3 + 0.0551x^5 + 0.1589x^6 + 0.0278x^{15} \\ & + 0.2598x^{16}\ , \\ \rho(x) =& \, x^{39}.\end{aligned}$$

From (3.24), (3.25), and (3.30)

$$B_0 = 0.0972, \quad B_1 = 0.3185, \quad B_2 = 0.0972$$

and therefore, since $B_0 = B_2$, then for every MBIOS channel, this LDPC code ensemble achieves vanishing bit error probability under BP decoding if the B-parameter is below $B = 0.0972$, and it is unstable if the B-parameter exceeds this value. This enables to calculate the threshold under BP decoding by transforming the B-parameter to the proper channel parameter. For the BEC, this corresponds to capacity of $C = 1 - B = 0.9028$ bits per channel use, and therefore 99.7% of the capacity of the BEC is asymptotically obtained under BP decoding with vanishing bit erasure probability. For the BIAWGN channel, this corresponds to channel capacity $C = 0.9400$ bits per channel use, and therefore this code ensemble achieves 95.7% of the capacity for this channel. The smallest fraction of capacity under BP decoding is achieved for the BSC, and it coincides with the lower bound $\mu_3(B) = 92.5\%$ as given in (3.31).

Example 3.5 We note that the approach presented in the examples above is not necessarily the best approach for obtaining universal LDPC code ensembles. Numerically optimized code ensembles may lead to better performance under BP over some channels. To demonstrate this, we consider the following LDPC code ensemble, obtained using [1]:

$$\begin{aligned}\lambda(x) =& 0.244022x + 0.224973x^2 + 0.0476526x^5 + 0.225756x^6 + 0.0270727x^{18} \\ & + 0.173877x^{19} + 0.0515554x^{20} + 0.00509134x^{22}\ , \\ \rho(x) =& x^8.\end{aligned}$$

This code is numerically optimized for the BIAWGN channel, with a design rate of one-half; its threshold under BP decoding is $\sigma = 0.966293$. This corresponds to capacity of $C = 0.5084$ bits per channel use. Therefore, this code achieves 98.35% of the capacity of the BIAWGN channel. The threshold of this code under BP decoding for the BEC computes to be $B = 0.4741$, which corresponds to a capacity of $C = 1 - B = 0.5259$ bits per channel use. I.e., this code achieves 95.08% of the capacity for the BEC.

The ensemble above and the ensemble considered in Example 3.3 share the same design rate. We see that the code ensemble considered here, when used over a BI-AWGN channel, is superior to the ensemble of example 3.3, achieving a much higher fraction of capacity. The performance of the two ensembles over the BEC, however, is similar, with a slight advantage to the ensemble of Example 3.3, recognizing that it was designed for a BEC.

This observation is also supported by the numerical results presented in [25]. In that work, the authors compared how LDPC code ensembles designed for one MBIOS channel performed over other MBIOS channels. The channels considered there were the BEC, the BIAWGN, and the flat-fading binary input Rayleigh channel. Their results show that the BEC can indeed be used as a so-called "surrogate" channel for the design of good LDPC code ensembles, while recognizing that better results can be obtained, at the expense of a higher computational load, with numerical optimization for the desired channel.

While the approach presented here may not be the optimal approach, it is *analytical and easy to compute*, and thus provides insight. For instance, we have shown how this approach can be used to obtain bounds on the thresholds of ensembles under BP decoding over *any* channel, which, as exemplified in Examples 3.3 and 3.4 above, are tight for some ensembles.

Remark 3.7 Universality results for LDPC code ensembles have been derived in this chapter with vanishing *bit* error probability under BP decoding. An extension of these results for vanishing *block* error probability can be made based on the results of [15] and [19]. These works showed that for a specific MBIOS channel, an LDPC code ensemble with $\lambda_2 = 0$ has the same threshold under vanishing block and bit error probabilities[4]. The threshold for vanishing block error probability, similar to

[4] In fact, [15] gives a stronger condition, also enabling $\lambda_2 > 0$ for ensembles with certain structures.

the threshold for vanishing bit error probability, is defined as the maximal channel parameter for which the block error probability will converge to zero. This result is based on the union bound, $P_B \leq nP_b$, where P_B is the block error probability, P_b is the bit error probability, and n is the block length. The conditions on λ_2 ensure that the bit error probability decays fast enough, thus causing the block error probability to vanish as well.

An extension of this result to universality over a multitude of MBIOS channels is now straightforward. As an example, let us demonstrate this by extending the results of Theorem 3.1. In the setting of this theorem, we consider a set $\mathcal{A}$ of MBIOS channels exhibiting the same capacity, C, and maximal B-parameter B. If the capacity-achieving sequence of LDPC code ensembles $\{(n, \lambda, \rho)\}$ for BEC(B) also satisfies the above-mentioned condition on λ_2, then this sequence is not only universal over this set in terms of vanishing *bit* error probability, but also in terms of vanishing *block* error probability.

Similarly, by imposing on λ_2 the conditions from [15] and [19], the other results of this chapter can be extended in a straight-forward manner for universality under vanishing *block* error probability.

Chapter 4

Universality for Irregular Repeat-Accumulate Codes

Irregular Repeat-Accumulate (IRA) code ensembles were introduced in [13], [14] as a family of code ensembles defined on graphs that have a natural linear-time encoding algorithm. This family is, in fact, a special subclass of irregular LDPC code ensembles, and was shown to achieve capacity under BP decoding over the BEC (see, e.g., [14], [26], [34]).

In this Chapter we use the approach of Chapter 3 to derive universality results for IRA code ensembles. This is made possible due to the fact that the density-evolution approach can also be used to analyze IRA code ensembles. In Section 4.1 we introduce IRA code ensembles and present the density evolution equations for them. Then, in Sections 4.2 and 4.3 we extend some of the results of Chapter 3 to IRA code ensembles.

4.1 Definition of IRA code ensembles

Figure 4.1 shows a Tanner graph of an IRA code with repetition profile $\{f_2, f_3, \ldots, f_J\}$ and right degree a, where $f_i \geq 0$, $\sum_i f_i = 1$, and a is a positive integer. A Tanner graph has two types of nodes: variable nodes, which are marked with circles, and check nodes, which are marked with squares. In an IRA code, the variable nodes are further divided into two types: *information nodes* on the left-hand side and *parity nodes* on the right-hand side. For a systematic IRA code, both the information bits and the parity bits are submitted over the channel. When the IRA code is non-systematic, only the parity bits are submitted; we can view this as puncturing all of the information bits of a systematic IRA code. Another way to view non-systematic IRA codes is to think of them as if the information bits are transmitted over a channel with capacity zero whereas the parity bits are transmitted over the actual channel (i.e., we can view this is a change in the channel rather than a change in the code).

An IRA code has k information nodes and r parity nodes. Each information node is connected to a number of check nodes; the fraction of information nodes connected to i check nodes is f_i. There are r check nodes, each connected to a information nodes. Each check node is further connected to two parity nodes (the parity node x_0 is virtual and does not constitute part of the code. We set it to 0 for the reason explained below).

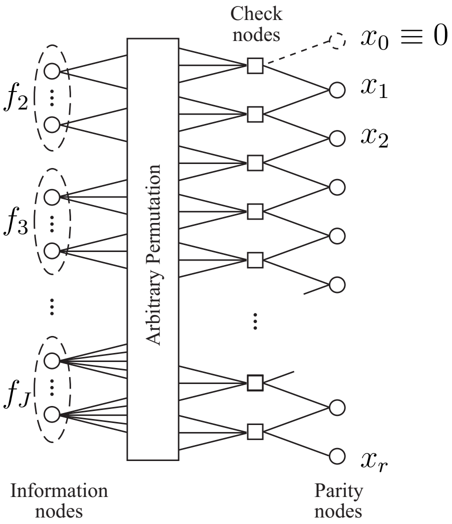

Figure 4.1: Tanner graph for an IRA code with repetition profile $\{f_2, f_3, \ldots, f_J\}$ and right degree a.

For a fixed permutation, the Tanner graph represents a systematic binary linear code. The k information bits, $(u_1, u_2, \ldots, u_k)$, are represented by the information nodes, and the r parity nodes are $(x_1, x_2, \ldots, x_r)$. The parity bits are computed as follows. First, we set $x_0 \equiv 0$. The information bits are repeated a number of times, based on the repetition profile. They are then interleaved according to the permutation, and are fed into an accumulator, initialized with $x_0 = 0$, that outputs one bit for every a input symbols. The accumulator outputs, $x_i, i = 1, \ldots, r$ are given by

$$x_i = x_{i-1} + \sum_{j=1}^{a} v_{(i-1)a+j}, \quad i = 1, 2, \ldots, r$$

where $v_j, j = 1, 2, \ldots, k$ are the information nodes. The design rate of a systematic IRA code is $R_{\text{d}}^{\text{s}} = a/(a + \sum_i if_i)$. In the non-systematic case, the information bits are not transmitted, so the design rate of the code becomes $R_{\text{d}}^{\text{ns}} = a/\sum_i if_i$.

The code is decoded using Belief-Propagation decoding. The nodes transfer messages over the graph edges, based on the messages received from their neighbors; the messages represent log-likelihood ratios. An iteration consists of all variable nodes (information and parity nodes) sending their messages over the graph edges to the check nodes, and then the check nodes sending their messages over the graph back to the variable nodes. In each iteration, therefore, all variable nodes and all check nodes are activated alternately and in parallel. The initial messages sent by the variable nodes represent the received symbols from the channel. The computation of the messages is precisely the same as for BP of standard LDPC codes (see [29, section 2.5.2]). The same decoder is used for the systematic and non-systematic cases. In the non-systematic case, the information bits are not transmitted over the channel, so they are initialized with zero LLRs. As above, we can also think of the non-systematic case as if the information bits are transmitted over a channel with zero capacity, which leads to the same conclusion about the initialization of the decoder.

The density evolution technique enables to calculate the BER performance of BP decoding averaged over the IRA code ensemble for MBIOS channels. In fact, the derivation of the density evolution equations for IRA code ensembles parallels that of standard LDPC code ensembles. Let λ_i be the fraction of edges between the information and check nodes that are adjacent to an information node of degree i (i.e., we momentarily ignore the parity nodes, and view the remaining graph as a standard LDPC code, and define λ_i as usual), and further define $\lambda(x) = \sum_i \lambda_i x^{i-1}$. The relationship between f_i and λ_i is given by [14]

$$f_i = \frac{\lambda_i / i}{\sum_j \lambda_j / j}.$$

Denote by a_l ($\tilde{a}_l$) the L-density of the messages transferred from the information nodes (parity nodes) to the check nodes at the l^{th} iteration, and by b_l ($\tilde{b}_l$) the L-density of the messages transferred from the check nodes to the information nodes (parity nodes) at the l^{th} iteration. Let a_0 be the L-density of the channel observation messages. Under these definitions, the density evolution equations for systematic IRA code ensembles are ([30]):

$$\begin{aligned} a_l &= a_0 \circledast \lambda(b_l) && (4.1)\\ \tilde{a}_l &= a_0 \circledast \tilde{b}_l && (4.2)\\ b_l &= \Gamma^{-1}\left(\Gamma(\tilde{b}_{l-1})^{\boxast 2} \boxast \Gamma(a_{l-1})^{\boxast (a-1)}\right) && (4.3)\\ \tilde{b}_l &= \Gamma^{-1}\left(\Gamma(\tilde{b}_{l-1}) \boxast \Gamma(a_{l-1})^{\boxast a}\right), && (4.4) \end{aligned}$$

where $\circledast$ and $\boxast$ represent convolutions of distributions in the L and G domains, respectively, and Γ and Γ^{-1} are the transformations from the L to the G domain and vice versa.

In the non-systematic case, there are no received channel symbols entering the information nodes, so equation (4.1) becomes:

$$a_l = \lambda(b_l). \tag{4.5}$$

The remaining density evolution equations for non-systematic IRA codes are the same as for the systematic case.

Remark 4.1 Both systematic and non-systematic IRA codes have been shown to be capacity-achieving when their degree distributions are properly chosen. However, as shown in [26] and [34], non-systematic IRA codes are superior to systematic IRA codes in that bounded decoding and encoding complexity per information bit for message-passing iterative decoding over the BEC is possible for non-systematic capacity-achieving IRA codes but not for systematic capacity-achieving IRA codes. Therefore, in this chapter we develop results both for the systematic and non-systematic cases.

4.2 Universal Achievability for IRA Codes

We now follow in the footsteps of section 3.1 in order to obtain parallel results on the universal achievability of IRA code ensembles over various families of MBIOS channels. First, let us derive a necessary and sufficient condition for convergence of a sequence of IRA code ensembles. To this end, we apply the Bhattacharyya functional $\mathcal{B}$ in (2.2) onto the density evolution equations (4.1) – (4.4). Denoting

$$\begin{aligned} x_l &\triangleq \mathcal{B}(a_l), \\ \tilde{x}_l &\triangleq \mathcal{B}(\tilde{a}_l) \end{aligned}$$

and using the multiplicativity of the B-parameter functional for a convolution of densities in the L-domain, (3.15), and the right-hand side of (3.12) for convolution of densities in the G-domain, we obtain for the systematic case:

$$\begin{aligned} x_l &= B_0\,\lambda(\mathcal{B}(b_l)) \\ \tilde{x}_l &= B_0\,\mathcal{B}(\tilde{b}_l) \\ \mathcal{B}(b_l) &\leq 1 - (1-\tilde{x}_{l-1})^2(1-x_{l-1})^{a-1} \\ \mathcal{B}(\tilde{b}_l) &\leq 1 - (1-\tilde{x}_{l-1})(1-x_{l-1})^{a}, \end{aligned}$$

where $B_0 \triangleq \mathcal{B}(a_0)$. These equations also apply to the non-systematic case, with the topmost equation replaced with

$$x_l = \lambda(\mathcal{B}(b_l)).$$

Adopting the notation

$$\hat{B}_0 \triangleq \begin{cases} B_0 & \text{systematic case} \\ 1 & \text{non-systematic case,} \end{cases}$$

we can address both cases jointly using

$$x_l = \hat{B}_0\lambda(\mathcal{B}(b_l)).$$

Note that $\tilde{x}_0 = \mathcal{B}(a_0) = B_0$, and similarly $x_0 = \hat{B}_0$. The left degree polynomial λ is monotone increasing; therefore, we can replace $\mathcal{B}(b_l)$ and $\mathcal{B}(\tilde{b}_l)$ with their upper bounds in the expressions for x_l and $\tilde{x}_l$, to obtain

$$x_l \leq \hat{B}_0\lambda\left(1-(1-\tilde{x}_{l-1})^2(1-x_{l-1})^{a-1}\right) \tag{4.6}$$

$$\tilde{x}_l \leq B_0\left(1-(1-\tilde{x}_{l-1})(1-x_{l-1})^{a}\right). \tag{4.7}$$

Recall that a necessary and sufficient condition for BP decoding to achieve vanishing bit error probability is that $x_l \to 0$, $\tilde{x}_l \to 0$ (see (3.27)). Since the information nodes represent the actual decoded message, it is, in fact, sufficient that only $x_l \to 0$ in order to achieve vanishing bit-error probability under BP decoding. This holds both for the systematic and non-systematic cases.

As in Section 3.1, let us now consider an arbitrary set of MBIOS channels, with L-densities in some set $\mathcal{A}$. The goal is to design an IRA code ensemble with right-degree a and left degree distribution λ that will achieve vanishing bit error probability over every channel in the set. Let us define B as in (3.3), i.e., B designates the maximal B-parameter over the MBIOS channels in the set. Consider the sequences y_l, $\tilde{y}_l$ $(l = 1, 2, \ldots)$, defined by the recursion

$$y_l = \hat{B}\,\lambda\left(1 - (1 - \tilde{y}_{l-1})^2(1 - y_{l-1})^{a-1}\right) \tag{4.8}$$

$$\tilde{y}_l = B\,\left(1 - (1 - \tilde{y}_{l-1})(1 - y_{l-1})^{a}\right) \tag{4.9}$$

with initial conditions $\tilde{y}_0 = B$, $y_0 = \hat{B}$, and where

$$\hat{B} \triangleq \begin{cases} B & \text{systematic case} \\ 1 & \text{non-systematic case.} \end{cases}$$

Note that this recursion refers to the density evolution equations for an IRA code ensemble used over a BEC (both for the systematic and non-systematic cases). Comparing (4.6) and (4.7) with (4.8) and (4.9), it is clear that $0 \le x_l \le y_l$, $0 \le \tilde{x}_l \le \tilde{y}_l$ for every $l \ge 0$ and any MBIOS channel in $\mathcal{A}$. Therefore, if λ and a are selected such that $y_l \to 0$ then we will also have $x_l \to 0$ for every channel in the set $\mathcal{A}$, making the code universal over this set of MBIOS channels.

Since capacity-achieving sequences of degree distributions of IRA ensembles over the BEC are known (see, e.g., [13], [14] for the systematic case, and [26] for the non-systematic case), a capacity-achieving sequence of IRA code ensembles designed for a BEC with erasure probability B will be universal under BP decoding for every channel in the considered set of MBIOS channels. The asymptotic design rate of this capacity-achieving sequence of IRA codes ensembles is equal to $R_{\mathrm{d}} = 1 - B$. Therefore, in a matter completely analogous to Section 3.1, by considering sets of MBIOS channels that exhibit the same capacity, we obtain the following theorem:

Theorem 4.1 [Universality of IRA Codes under BP Decoding for Equi-Capacity MBIOS Channels] Consider a set $\mathcal{A}$ of MBIOS channels that exhibit a given capacity C, and let B denote the maximal B-parameter over this set (see (3.3)). Let $\{(n, \lambda(x), \rho(x) = x^{a-1})\}$ form a capacity-achieving sequence of (systematic or non-systematic) IRA code ensembles for BEC(B), achieving vanishing bit erasure probability under BP decoding. Then, this sequence universally achieves vanishing bit error probability under BP decoding for the entire set $\mathcal{A}$, and the design rate of this sequence forms a fraction that is at least $\frac{1-B}{C}$ of the channel capacity.

Remark 4.2 As in Section 3.1, we can compute the universal achievable fraction of capacity using this approach for specific families of equi-capacity MBIOS channels. Comparing Theorems 4.1 and 3.1, we see that the universal achievable fraction of capacity for IRA code ensembles is the same as that for LDPC code ensembles. Therefore, Fig. 3.1 applies here as well.

Remark 4.3 The results above can also be extended to IRA code ensembles that do not have a constant right degree. The analysis follows in the same vein, but the resulting density evolution equations are somewhat more cumbersome, involving right degree polynomials both from the node and the edge perspectives. Since IRA codes are often designed with a constant right degree[1], we have opted to provide here the analysis only for this case. The derivation of the more general case is similar and is left to the interested reader.

4.3 Bounds on the Bhattacharyya Parameter for Convergence of a sequence of IRA code ensembles

The following theorem is analogous to Theorem 3.3 for LDPC code ensembles.

Theorem 4.2 Let $\{(n, \lambda(x), \rho(x) = x^{a-1})\}$ be a sequence of (systematic or non-systematic) IRA code ensembles with right degree a and left degree distribution λ

[1] Some explicit constructions of capacity-achieving check-regular IRA code ensembles for the BEC are provided in the literature (see, e.g., [26, Theorem 2]).

whose block lengths tend to infinity. The following universal properties hold under BP decoding:

- This sequence achieves vanishing bit error probability under BP decoding for *every* MBIOS channel whose B-parameter is less than

$$\begin{aligned} B_0(\lambda, a) \triangleq \sup_{B \in (0,1]} \Bigg\{ y = \hat{B}\lambda \left(1 - \left(\frac{1-B}{1-B(1-y)^a}\right)^2 (1-y)^{a-1}\right) \\ \text{has no solution } y \text{ in } (0,1]. \Bigg\} \end{aligned} \tag{4.10}$$

- This sequence does not achieve reliable communications over any MBIOS channels whose B-parameter is greater than

$$\begin{aligned} B_1(\lambda, a) \triangleq \sup_{B \in (0,1]} \Bigg\{ z = \hat{B}\lambda \left(\sqrt{1 - \left(\frac{1-B^2}{1-B^2(1-z^2)^a}\right)^2 (1-z^2)^{a-1}}\right) \\ \text{has no solution } z \text{ in } (0,1], \Bigg\} \end{aligned} \tag{4.11}$$

where

$$\hat{B} \triangleq \begin{cases} B & \text{systematic case} \\ 1 & \text{non-systematic case.} \end{cases}$$

Proof: To prove the first part of the theorem, consider the recursion given by (4.6) and (4.7). Let $B \geq B_0$; clearly,

$$\begin{aligned} x_l &\leq \hat{B}\lambda \left(1 - (1-\tilde{x}_{l-1})^2 (1-x_{l-1})^{a-1}\right), \\ \tilde{x}_l &\leq B \left(1 - (1-\tilde{x}_{l-1})(1-x_{l-1})^a\right). \end{aligned}$$

Observe that $0 \leq x_l \leq y_l$ and $0 \leq \tilde{x}_l \leq \tilde{y}_l$ where y_l and $\tilde{y}_l$ are defined according to (4.8) and (4.9), with B denoting any B-parameter greater than or equal to B_0 and initial conditions $\tilde{y}_0 = B$, $y_0 = \hat{B}$. Thus, if $\{y_l, \tilde{y}_l\}$ converge to 0 then also $x_l \to 0$ and the sequence of IRA code ensembles converges for any MBIOS channel with B-parameter less than or equal to B. Therefore, if we denote by $B_0(\lambda, a)$ the maximal B-parameter such that the recursion defined by (4.8) and (4.9) with initial condition

$\tilde{y}_0 = B_0(\lambda, a)$, $y_0 = \hat{B}_0(\lambda, a)$ converges to 0, then the sequence of IRA code ensembles $\{(n, \lambda(x), \rho(x) = x^{a-1})\}$ will converge for any MBIOS channel whose B-parameter is less than or equal to $B_0(\lambda, a)$.

The expression in (4.10) for $B_0(\lambda, a)$ stems from a fixed-point characterization of (4.8) and (4.9), as derived in appendix E. This completes the proof of the first part of the theorem.

To prove the second part, we rely on the inequality (3.13). Applying the B-parameter functional onto (4.3) and (4.4) and using (3.13) we obtain

$$\begin{aligned}\mathcal{B}(b_l) &\geq \sqrt{1-(1-\tilde{x}_{l-1}^2)^2(1-x_{l-1}^2)^{a-1}},\\ \mathcal{B}(\tilde{b}_l) &\geq \sqrt{1-(1-\tilde{x}_{l-1}^2)(1-x_{l-1}^2)^{a}},\end{aligned}$$

where, as above, we have defined $x_l \triangleq \mathcal{B}(a_l)$ and $\tilde{x}_l \triangleq \mathcal{B}(\tilde{a}_l)$. Applying the B-parameter functional onto (4.1) and (4.2) (and (4.5) for the non-systematic case) and using these inequalities, we obtain:

$$\begin{aligned}x_l &\geq \hat{B}_0\lambda\left(\sqrt{1-(1-\tilde{x}_{l-1}^2)^2(1-x_{l-1}^2)^{a-1}}\right),\\ \tilde{x}_l &\geq B_0\sqrt{1-(1-\tilde{x}_{l-1}^2)(1-x_{l-1}^2)^{a}},\end{aligned}$$

where $B_0 = \mathcal{B}(a_0)$. It therefore follows that if the sequences $\{x_l, \tilde{x}_l\}$ tend asymptotically to zero, then the sequences

$$z_l = \hat{B}_0\lambda\left(\sqrt{1-(1-\tilde{z}_{l-1}^2)^2(1-z_{l-1}^2)^{a-1}}\right), \tag{4.12}$$

$$\tilde{z}_l = B_0\sqrt{1-(1-\tilde{z}_{l-1}^2)(1-z_{l-1}^2)^{a}}, \tag{4.13}$$

with initial value $\tilde{z}_0 = B_0$ and $z_0 = \hat{B}_0$ should also tend to zero. Recall that $x_l \to 0$ forms a necessary and sufficient condition for achieving vanishing bit error probability under BP as we let the number of iterations grow. Therefore, the convergence of $\{z_l, \tilde{z}_l\}$ to zero forms a necessary condition for the sequence of IRA code ensembles to achieve vanishing bit error probability under BP decoding. Hence, if $\{z_l, \tilde{z}_l\}$ does not converge to zero, then x_l is bounded away from zero. The expression in (4.11) for $B_1(\lambda, a)$ stems from a fixed-point characterization of (4.12) and (4.13); its derivation is completely analogous to the derivation in appendix E, and is thus omitted here.

This completes the proof of the theorem. ■

Corollary 4.1 Let $\{(n, \lambda(x), \rho(x) = x^{a-1})\}$ be a sequence of systematic IRA code ensembles whose block lengths tend to infinity. Then, the message error probability stays bounded away from zero under BP decoding for every MBIOS channel whose B-parameter is greater than

$$B_2(\lambda, a) \triangleq \min\left\{ B_1(\lambda, a), \frac{-(1+\lambda_2(a-1)) + \sqrt{(1+\lambda_2(a-1))^2 + 4(1+\lambda_2(a+1))}}{2\lambda_2(a+1)}, \right.$$
$$\left. \sqrt{1-R_{\mathrm{d}}^2} \right\} \tag{4.14}$$

where B_1 is introduced in (4.11), and R_{d} designates the design rate.

Proof: If the parameter B is greater than $B_1(\lambda, a)$ the statement follows from the second part of Theorem 4.2. The stability condition for systematic IRA ensembles, which is another necessary condition for convergence, is given by

$$\lambda_2 < \frac{B^{-1}(B^{-1}-1)}{a+1+B^{-1}(a-1)},$$

as proved in [30, Theorem 1]. Rearranging this inequality yields that a necessary condition for convergence is that

$$(a+1)\lambda_2 B^2 + (1+\lambda_2(a-1))B - 1 < 0. \tag{4.15}$$

The left-hand-side is a convex quadratic polynomial in B with zeros

$$Z_{1,2} = \frac{-(1+\lambda_2(a-1)) \pm \sqrt{(1+\lambda_2(a-1))^2 + 4(1+\lambda_2(a+1))}}{2\lambda_2(a+1)}$$

Therefore, the condition (4.15) is equivalent to $Z_1 < B < Z_2$, where Z_1 is the zero with the negative sign in front of the square root, and Z_2 is the other zero; in particular, $Z_1 < 0$ and $Z_2 > 0$. Since $B > 0$ by definition, an equivalent condition is that $B < Z_2$. Therefore, the stability condition can be written as

$$B < \frac{-(1+\lambda_2(a-1)) + \sqrt{(1+\lambda_2(a-1))^2 + 4(1+\lambda_2(a+1))}}{2\lambda_2(a+1)},$$

and when this condition is violated, the message error probability stays bounded away from zero. Finally, the case where $B > \sqrt{1-R_{\mathrm{d}}^2}$ is the same as in Corollary 3.3. ■

Chapter 5

Universality under Maximum-Likelihood Decoding

In Chapter 3 we considered the universality of LDPC code ensembles under BP decoding. Though maximum-likelihood (ML) decoding is in general prohibitively complex, we show in the following that universality can be achieved under ML decoding for the entire set of equi-capacity MBIOS channels. The universality results proved in Chapter 3 under BP decoding automatically hold under ML decoding, but the universality results that are proved in this chapter under ML decoding are stronger in the sense that capacity can be approached *arbitrarily closely* for the entire set of channels under consideration with vanishing *block* error probability. In Section 5.1 we show that Gallager's regular LDPC code ensembles can be made universal under ML decoding. In Section 5.2 we show that randomly punctured regular LDPC code ensembles can also be made universal.

5.1 Universality of Gallager's Regular LDPC Code Ensembles

In his monograph, Gallager introduced ensembles of regular LDPC codes, and also considered their performance under ML decoding via their distance properties (see [8, Chapters 2 and 3]). In the following, we rely on [33], and demonstrate that a proper selection of Gallager's regular LDPC code ensembles can be made to approach arbitrarily closely the channel capacity for the entire set of equi-capacity MBIOS channels with vanishing block error probability.

Theorem 5.1 [Universality of Regular LDPC Code Ensembles under ML Decoding for Equi-Capacity MBIOS Channels] Under ML decoding, Gallager's regular LDPC code ensembles can be made universal for the set $\mathcal{A}$ of MBIOS channels that exhibit a given capacity C. More explicitly, for any $\varepsilon > 0$ (that can be made arbitrarily small), there exists a sequence of these code ensembles whose design rate forms at least a fraction $1 - \varepsilon$ of the channel capacity with vanishing block error probability for the entire set $\mathcal{A}$. Moreover, the asymptotic parity-check density of this sequence scales like $\log \frac{1}{\varepsilon}$.

Proof: The proof of the first part of this theorem follows along the lines of the proof of [33, Theorem 2.2] by noticing that the way where the capacity-approaching sequence of regular LDPC code ensembles is determined only depends on the channel capacity. This therefore makes this sequence universal for the entire set of equi-capacity MBIOS channels $\mathcal{A}$, and it asymptotically achieves (as we let the block length of this sequence tend to infinity) vanishing block error probability under ML decoding with a design rate that is at least a fraction $1 - \varepsilon$ of the channel capacity. The asymptotic parity-check density scales like $\log \frac{1}{\varepsilon}$, which is a consequence of the upper and lower bounds on the parity-check density in [33, Theorem 2.2] and [33, Theorem 2.1], respectively, which both scale like $\log \frac{1}{\varepsilon}$. ■

Example 5.1 In order to exemplify Theorem 5.1, consider lower bounds on the error exponents of some expurgated Gallager's regular LDPC code ensembles under ML decoding. Figure 5.1 shows lower bounds on the error exponent for several expurgated Gallager's LDPC code ensembles of length $n = 100000$ and design rate $\frac{1}{2}$. The expurgation followed the approach in [8, Chapter 2]. The bounds were computed for three MBIOS channels of different capacities. For the BSC and BEC, the Shulman-Feder bound was used (see [35, section 4.4.1]). For the BIAWGN channel, the error exponent was computed based on [44, Theorem 3.1]. The distance spectra of the ensembles were computed according to the asymptotic results in [8, Chapter 2]. It is noted that for this block length, the asymptotic results are very close to the exact distance spectra (see [43]). It is evident from Figure 5.1 that as we increase the degrees of the variable and check nodes while maintaining a constant design rate, the point where the error exponent vanishes gets closer to the channel capacity, regardless of the MBIOS channel in question. Thus, this demonstrates that this sequence of ensembles becomes universal under maximum-likelihood decoding for equi-capacity MBIOS channels.

For short block lengths, we compare the lower bound for the expurgated $(6, 12)$ ensemble and block length $n = 1008$ computed using the exact distance spectrum [43] and the upper bound from [8, Chapter 2]. Figure 5.2 shows the comparison. Clearly, the vanishing point of the error exponent is closer to capacity when computed using the exact distance spectrum. The calculation of the lower bound on the error exponent that uses the upper bound on the distance spectrum provides, however, a reasonable estimate of the lower bound on the error exponent that is calculated via the exact distance spectrum.

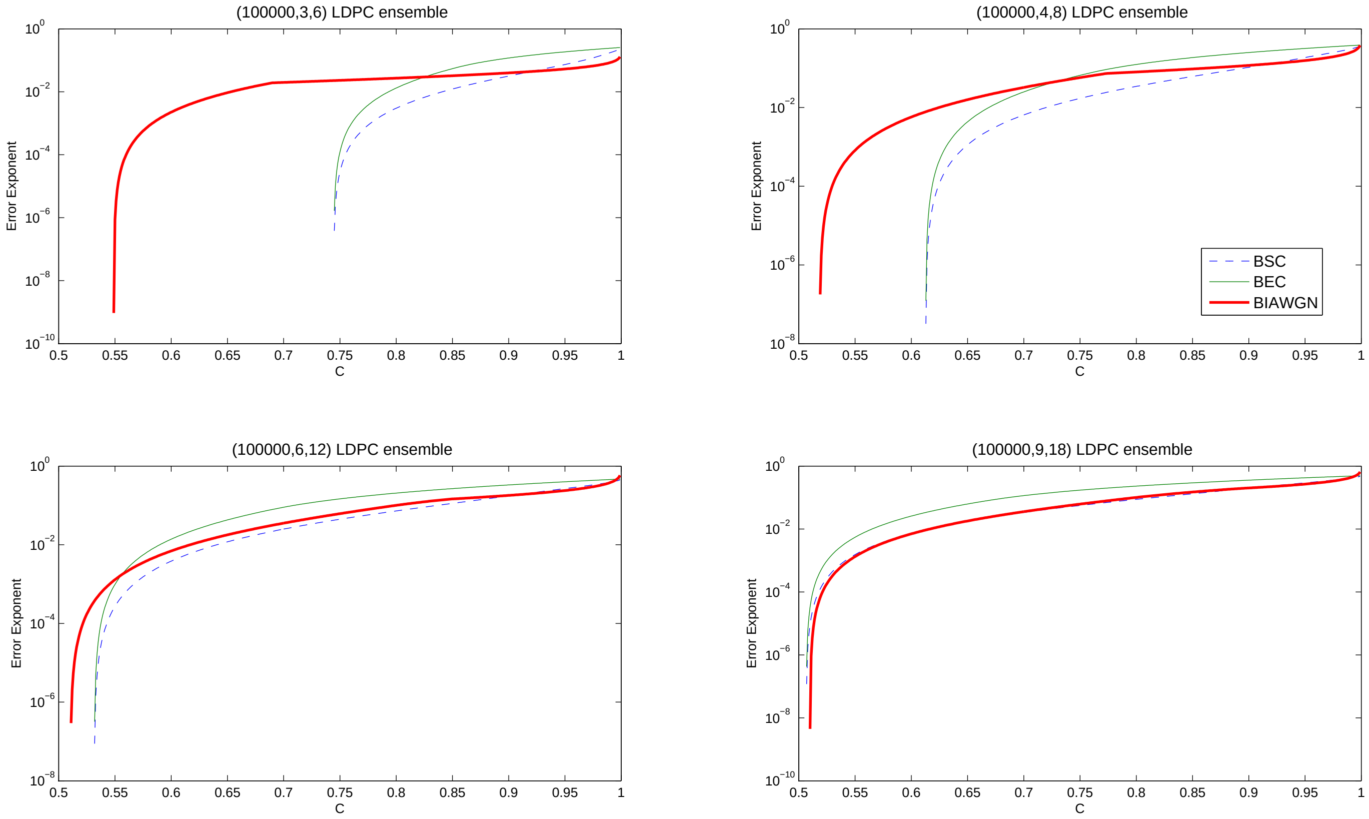

Figure 5.1: Lower bounds on the error exponent for expurgated Gallager's LDPC code ensembles on various MBIOS channels. The results were computed for block length $n = 100000$, and for codes with constant design rate 1/2 and increasing variable and check node degrees.

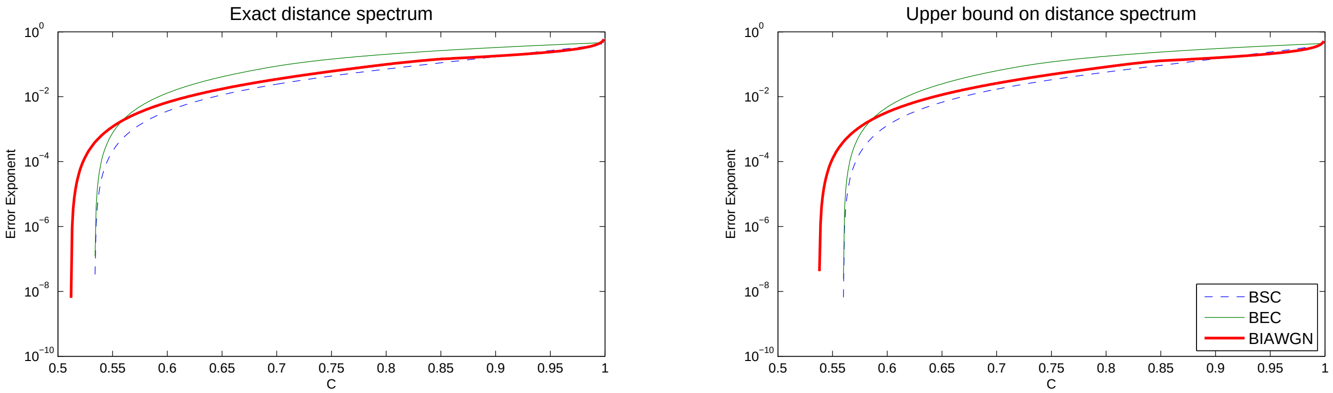

Figure 5.2: A comparison of the lower bounds on the error exponent of some expurgated Gallager's LDPC code ensembles for various MBIOS channels. The results were computed for the expurgated $(6, 12)$ ensemble with block length $n = 1008$, using both the exact distance spectrum as found in [43] (left-hand plot) and the upper bound from [8, Chapter 2] (right-hand plot).

5.2 Universality of Punctured Regular LDPC Code Ensembles

The performance of punctured LDPC code ensembles under BP decoding was addressed extensively (see, e.g., in [10] and [27]). The potential performance of punctured LDPC code ensembles under ML decoding was studied, e.g., in [12] and [37]. These works show the remarkable performance of some punctured LDPC code ensembles for various channel models. In the following, we rely on [12], and consider the universality of some randomly punctured regular LDPC code ensembles under ML decoding over the set of equi-capacity MBIOS channels.

Consider a linear block code, which will be referred to as a mother code. By introducing the option of possibly puncturing various fractions of the code bits of the mother code, one generates a set of new linear block codes with some higher rates. The advantage of puncturing lies in the flexibility of the selected rates of the punctured codes, and in the ability to use the same decoder as for the mother code to decode all of these punctured codes. Specifically, by puncturing nq bits of a mother code of length n and rate R, one obtains a punctured code of length $n(1-q)$ and rate at most $\frac{R}{1-q}$. A lower rate occurs whenever at least two different codewords of the mother code are mapped to the same codeword after puncturing; this phenomenon is called *rate reduction* (see [12, Section III]).

In [12], the authors analyze the performance of punctured LDPC code ensembles under ML decoding. Specifically, they consider puncturing Gallager's ensemble of regular (n, j, k) LDPC codes, and provide conditions on the original ensemble (before puncturing) for asymptotically obtaining zero rate reduction with probability 1 as we let the block length n tend to infinity. Consider an ensemble whose design rate is R_{d}, then in the case where there is no rate reduction due to puncturing, the design rate of the punctured ensemble is $\frac{R_{\text{d}}}{1-q}$. It is also shown in [12] that under the condition of zero rate reduction, if the original sequence of code ensembles achieves a fraction $1-\varepsilon$ of capacity (note that Theorem 5.1 ensures the existence of such a sequence), then so does the sequence of punctured code ensembles. This leads to the following theorem:

Theorem 5.2 [Universality of Punctured Regular LDPC Code Ensembles

under ML Decoding for Equi-Capacity MBIOS Channels] Under ML decoding, punctured regular LDPC code ensembles can be made universal for the set of MBIOS channels that exhibit a given capacity. More explicitly, let $\varepsilon > 0$ (which can be set arbitrarily close to zero), and consider a sequence of regular (n, j, k) LDPC code ensembles whose design rate R_{d} forms a fraction of at least $1 - \varepsilon$ of the capacity C. Assume that this sequence achieves vanishing block error probability under ML decoding for the entire set of MBIOS channels $\mathcal{A}$ which exhibit a channel capacity C. Random puncturing of a fraction q of code bits from this sequence of ensembles produces a new sequence of punctured code ensembles with any desired design rate $R'_{\text{d}} > R_{\text{d}}$ with the following properties:

- It achieves vanishing block error probability under ML decoding over the entire set of equi-capacity MBIOS channels with capacity $C' = \frac{C}{1-q}$.
- It achieves a fraction of at least $1 - \varepsilon$ of the capacity C'.

Proof: From Theorem 5.1, there exists a sequence of regular LDPC code ensembles that universally achieves, under ML decoding, a fraction $1 - \varepsilon$ of the channel capacity with vanishing block error probability for the entire set $\mathcal{A}$. The idea is to first construct such a sequence with a low enough design rate, and then increase the design rate via (random) puncturing to obtain the new universal code ensemble. More specifically, according to [12, Theorem 1], if the design rate of the mother ensemble is low enough, then the rate reduction due to puncturing is zero. Note that the proof of this theorem is based solely on the distance properties of the original (mother) code ensemble and the desired design rate. Since the proofs of [12, Theorems 2 and 3] rely only on the capacity of the MBIOS channel and the condition for zero rate reduction, this implies that the new sequence of punctured LDPC code ensembles has vanishing block error probability under ML decoding over all MBIOS channels with capacity $C' = \frac{C}{1-q}$. Note that since

$$\frac{R'_{\text{d}}}{1-\varepsilon} = \frac{R_{\text{d}}}{(1-\varepsilon)(1-q)} \geq \frac{C}{1-q} = C'$$

then this new sequence of punctured LDPC code ensembles has a design rate that is at least a fraction $1 - \varepsilon$ of C'. ■

Chapter 6

Summary and Outlook

6.1 Contribution of this Thesis

In this thesis, we have considered the universality of LDPC code ensembles under both BP and ML decoding over families of MBIOS channels. We have focused on obtaining closed-form analytical results, even though better performance can be obtained by numerical design of LDPC code ensembles (see, e.g. [4], [7], [25], [31] and also the discussion in Example 3.5 of this thesis).

Under BP decoding we derived an analytical method to design LDPC code ensembles that achieve vanishing bit error probability over every channel in a family of MBIOS channels. This method is based on a necessary and sufficient condition for an LDPC code ensemble to achieve vanishing bit error probability under BP decoding; this condition is a consequence of applying the $\mathcal{B}$ functional (2.2) to the density evolution equation (3.1). We derived an expression for the universal achievable fraction of capacity over the family obtained using this method, ans applied it to several families of MBIOS channels, such as the family of equi-capacity MBIOS channels. Thus, we showed that at least 69.3% of capacity is uniformly achievable for these families.

We also derived a necessary condition for a sequence of LDPC code ensembles to universally achieve vanishing bit error probability under BP decoding over an arbitrary set of MBIOS channels. This condition forms the basis for a linear programming universal upper bound on the achievable rate of LDPC code ensembles over a set of equi-capacity MBIOS channels. This bound can also be translated into a lower bound on the achievable gap to capacity. Additionally, by considering sets of

MBIOS channels that also include the BEC, we were able to improve the bound in some cases.

The analytical design method and the necessary condition above were then used to derive universal conditions for reliable communication under BP decoding. In particular, we showed that an LDPC code ensemble will achieve vanishing bit error probability under BP decoding when used over any MBIOS channel whose B-parameter is less than a certain value, and will achieve a positive bit error probability when the B-parameter exceeds a certain (other) value. These bounds support [31, Conjecture 1], yet due to the gap between the two bounds, they do not prove it. Although a form of these bounds was previously published in [46], they were independently derived here in an easy-to-compute closed form, and the lower bound on the bit error probability when the B-parameter exceeds the bound in (3.30) is new. We computed these bounds for several LDPC code ensembles, both regular and irregular, and showed that in some cases they coincide. We also showed that these bounds can be translated into bounds on the threshold under BP decoding, and compared them to previously published bounds based on an information combining approach [41]. In some cases, our bounds were more informative. In addition to analyzing the numerically designed degree distributions, we also computed the bounds for the family of analytically designed capacity-approaching right-regular degree distributions on the BEC in [29, Example 3.88], and showed that these LDPC code ensembles can achieve universality over the set of MBIOS channels with the same B-parameter. Although numerically designed LDPC code ensembles can achieve better performance than the codes designed using our approach (see, e.g., [7], [25], and [31]), our approach is analytical, easily computable, and guarantees universality. The universality results that were derived for vanishing bit error probability can be extended to universally achieving vanishing block error probability subject to the conditions on the degree distributions in [15] and [19].

The universality results of LDPC codes under BP decoding can be extended to other families of codes defined on graphs that can be analyzed using density evolution type equations. We demonstrated this by considering the family of IRA code ensembles ([13], [14]). As for LDPC code ensembles, we derived an analytical method to design IRA code ensembles that will universally achieve vanishing bit error probability over a set of MBIOS channels, and determined the universally achievable fraction of capacity obtained using this method. Then, we derived conditions on the B-parameter for reliable communication under BP decoding that are analogous to the ones for LDPC code ensembles.

Universality under ML decoding was also considered. We used the results of [33] to show that Gallager's regular LDPC code ensembles can be made universally capacity achieving over the set of equi-capacity MBIOS channels (in the sense of vanishing block error probability). It is noted that the ML decoding results are an improvement over the BP decoding case, where the universally achievable fraction of capacity over the family of equi-capacity MBIOS channels depended on the channel capacity and could be as low as 69.3%. We exemplified this result for a particular sequence of expurgated regular LDPC code ensembles by showing that as the right degree is increased, all the while maintaining the same design rate, the point where the error exponent vanishes approaches capacity for different MBIOS channels. Finally, we used [12] to extend this result to randomly punctured LDPC code ensembles as well.

The results in this research work are also presented in [36], which was recently accepted for publication in the *IEEE Trans. on Information Theory* (as a full paper).

6.2 Topics for Future Research

In this section, we propose some directions for future research:

- The LP bounds derived in Section 3 are not tight in general, since the universal achievable gap to capacity does not always decrease for increasing values of d_{c} (contrary to the expected experimental behavior of optimized LDPC code ensembles under BP decoding). Finding some new constraints in these optimization problems may enhance the tightness of these bounds. Moreover, our bounds refer to fixed right-degree ensembles (note that typically LDPC code ensembles are designed to be right-regular or almost right-regular). Extending the bounds to the case where the parity-check degree is not fixed is also of interest.

- The Bhattacharyya parameter (B-parameter) for equi-capacity MBIOS channels can vary in a large range. As a result, the universal LDPC code ensembles designed in this work achieve, e.g., 75% of capacity if the channel capacity is 0.5

bit per channel use (see Fig. 3.1). Nonetheless, the fact that these ensembles are provably universal and are designed by simple analytical tools is important. Since, in practice, numerical optimizations enable to design LDPC code ensembles which universally achieve a larger fraction of capacity for some classes of equi-capacity MBIOS channels (see [31]), further analysis in this direction is of interest.

- The ideas of universality in this paper can be developed to consider other sets of communication channels (for example, the universality of LDPC code ensembles for the set of MBIOS channels with the same uncoded bit error probability is considered in Appendix F).

- The approach for universality in Section 3 of this paper stems on the asymptotic analysis of BP decoding via density evolution; it has resulted in an analytical design of a universal decoder that is based on code design for a BEC. This universal LDPC code ensemble converges but does not achieve full capacity when used over other channels in the family it was designed for, as Fig. 3.1 demonstrates. That said, one should not infer that this is the penalty of universality, as these results are merely an artifact of the approach presented here. Numerical evidence in [7] and [25] suggests that better results are possible (see also Example 3.5 in this paper). One possible approach to obtain better analytical results may rely on analytic properties of GEXIT charts [21], instead of the suggested approach in this paper that relies on density evolution for the BEC as a starting point for the analysis. Another possible approach may be to investigate universal LDPC code ensemble design under other suboptimal decoding methods for LDPC codes (e.g., a study of the universality of LDPC code ensembles under LP decoding).

- Although ML decoding is prohibitively complex for codes of large blocklength, the fact that (regular) LDPC code ensembles are capacity-achieving under ML decoding for the set of equi-capacity MBIOS channels is interesting (see Theorems 5.1 and 5.2). As a continuation of the previous item, it would be interesting to investigate the tradeoff between performance and complexity for some near-ML decoding algorithms that provide a better tradeoff between performance and complexity than the ML decoding algorithm.

Appendix A

Proof of Lemma 3.1

In the following, we prove the monotonicity of μ_1 (see (3.7)) over the interval $[0, 1)$, and then calculate the limits of $\mu_1(C)$ as the channel capacity C tends either to zero or 1 bit per channel use.

Let $x \triangleq h_2^{-1}(1-C)$, then we get from (3.7) that

$$\mu_1(C) = \frac{1-\sqrt{4x(1-x)}}{1-h_2(x)}.$$

We note that μ_1, as a function of x, monotonically decreases when $0 \leq x \leq \frac{1}{2}$. This is readily seen by taking the derivative of μ_1 with respect to x, which remains negative when $0 \leq x \leq \frac{1}{2}$. The substitution of the Taylor series expansion of the binary entropy function around $x = \frac{1}{2}$ (see [47, p. 575])

$$h_2(x) = 1 - \frac{1}{2\ln 2}\sum_{q=1}^{\infty}\frac{(1-2x)^{2q}}{q(2q-1)}, \quad 0 \leq x \leq 1$$

in the denominator gives

$$\begin{aligned}
\mu_1(C) &= \frac{1-\sqrt{1-(1-2x)^2}}{\frac{1}{2\ln 2}\displaystyle\sum_{q=1}^{\infty}\frac{(1-2x)^{2q}}{q(2q-1)}} \\
&= \frac{(1-2x)^2}{1+\sqrt{1-(1-2x)^2}}\;\frac{2\ln 2}{\displaystyle\sum_{q=1}^{\infty}\frac{(1-2x)^{2q}}{q(2q-1)}} \\
&= \frac{2\ln 2}{1+\sqrt{1-(1-2x)^2}}\;\frac{1}{\displaystyle\sum_{q=1}^{\infty}\frac{(1-2x)^{2(q-1)}}{q(2q-1)}}\,.
\end{aligned}$$

If C is increased from 0 to 1, then x, which was defined above as $x \triangleq h_2^{-1}(1-C)$, decreases from $\frac{1}{2}$ to 0 and therefore $\mu_1(C)$ is increasing with C, and

$$\lim_{C\to 1}\mu_1(C) = 1.$$

On the other hand, the limit of $\mu_1(C)$ when we let the capacity tend to zero is equal to

$$\begin{aligned}
\lim_{C\to 0}\mu_1(C) &= \lim_{x\to\frac{1}{2}}\frac{2\ln 2}{1+\sqrt{1-(1-2x)^2}}\;\frac{1}{\displaystyle\sum_{q=1}^{\infty}\frac{(1-2x)^{2(q-1)}}{q(2q-1)}} \\
&= \ln 2\;\lim_{x\to\frac{1}{2}}\frac{1}{\displaystyle\sum_{q=1}^{\infty}\frac{(1-2x)^{2(q-1)}}{q(2q-1)}} \\
&= \ln 2.
\end{aligned}$$

This completes the proof of Lemma 3.1.

Appendix B

Extension of (3.10) for general LDPC code ensembles

The condition in (3.10) is stated for a right-regular channel. For a general right-degree distribution

$$\rho(x) = \sum_i \rho_i x^{i-1}.$$

This condition can be readily extended to the case at hand, although it takes a more involved form. As in (3.14) we begin with (3.1) to obtain

$$\begin{aligned}
x_l &\triangleq \mathcal{B}(a_l) \\
&\overset{(a)}{=} \mathcal{B}(a_0)\, \mathcal{B}\Bigg(\lambda\Big(\Gamma^{-1}\Big(\rho\big(\Gamma(a_{l-1})\big)\Big)\Big)\Bigg) \\
&\overset{(b)}{=} \mathcal{B}(a_0)\, \lambda\Bigg(\mathcal{B}\Big(\Gamma^{-1}\Big(\rho\big(\Gamma(a_{l-1})\big)\Big)\Big)\Bigg) \\
&\overset{(c)}{=} \mathcal{B}(a_0)\, \lambda\left(\sum_i \rho_i \mathcal{B}\left(a_{l-1}^{\boxast i-1}\right)\right) \\
&\overset{(d)}{\geq} \mathcal{B}(a_0)\, \lambda\left(\sum_i \rho_i \sqrt{1 - \big(1 - \mathcal{B}(a_{l-1})^2\big)^{i-1}}\right),
\end{aligned} \tag{B.1}$$

where equality (a) follows from the recursive density evolution equation in (3.1) and the multiplicativity of the B-functional over convolution in the L-domain (3.15), equalities (b) and (c) follow from the linearity of the convolution operator and of the

B-functional (see (3.16)), and inequality (d) follows from (3.13).

The extension of (3.10) for a general LDPC code ensemble readily follows by replacing z_l in (3.17) with

$$z'_l = \mathcal{B}(a_0)\,\lambda\left(\sum_i \rho_i \sqrt{1-\big(1-\mathcal{B}(z'_{l-1})^2\big)^{i-1}}\right).$$

Thus, the extended (3.10) assumes the form

$$B\,\lambda\left(\sum_i \rho_i \sqrt{1-\big(1-x^2\big)^{i-1}}\right) \leq x, \quad \forall x \in (0, B]. \tag{B.2}$$

Appendix C

Proof of Lemma 3.3

Let us consider the sequence

$$z_l = z_0 \lambda\big(\sqrt{1-\rho(1-z_{l-1}^2)}\big), \quad l = 1, 2, \ldots$$

for $z_0 < B_1(\lambda, \rho)$ where

$$B_1(\lambda, \rho) \triangleq \inf_{x \in (0,1]} \frac{x}{\lambda\big(\sqrt{1-\rho(1-x^2)}\big)}$$

is introduced in (3.25). By substituting $x = 1$ on the right-hand side above, it follows readily that $B_1(\lambda, \rho) \leq 1$ and therefore $z_0 < 1$. In the following, it is proved by induction that the sequence is monotonic decreasing and bounded between 0 and 1: let us assume that $0 \leq z_{l-1} < 1$ holds for a specific $l \geq 1$, then

$$\begin{aligned} z_l &= z_0 \lambda\big(\sqrt{1-\rho(1-z_{l-1}^2)}\big) \\ &\leq B_1(\lambda, \rho)\ \lambda\big(\sqrt{1-\rho(1-z_{l-1}^2)}\big) \\ &\leq z_{l-1} \end{aligned}$$

where the last inequality follows from the definition of B_1 and the above assumption for z_{l-1}. It therefore follows by induction that the sequence $\{z_l\}$ is monotonic decreasing and bounded between 0 and 1, hence it is a convergent sequence. Let $z^* \in [0, 1]$ denote the limit of this sequence, then due to the continuity of λ and ρ over the interval $[0, 1]$, it follows (by letting l tend to infinity in the recursive equation for the sequence $\{z_l\}$) that the limit $z = z^*$ satisfies the equation

$$z = z_0 \lambda\big(\sqrt{1-\rho(1-z^2)}\big).$$

For $z \in (0,1]$

$$\begin{aligned} z_0 < B_1 &\le \frac{z}{\lambda\big(\sqrt{1-\rho(1-z^2)}\big)} \\ &\Rightarrow z_0 \lambda\big(\sqrt{1-\rho(1-z^2)}\big) < z \end{aligned}$$

and therefore the limit z should be necessarily zero for the case where the initial value z_0 is less than $B_1(\lambda, \rho)$.

For the proof of the second part of the lemma, we consider the case where $B_1(\lambda, \rho) < z_0 \le 1$. From the way B_1 is defined in (3.25), it follows that the set

$$\mathcal{F}_{z_0} \triangleq \left\{ x \in (0,1] : \frac{x}{\lambda\big(\sqrt{1-\rho(1-x^2)}\big)} \le z_0 \right\} \tag{C.1}$$

is non-empty. Let $x(z_0)$ designate the maximal value of this set (note that $0 < x(z_0) \le 1$).

Let us define the function $g(u,v) \triangleq u\lambda\big(\sqrt{1-\rho(1-v^2)}\big)$ over the square $\{(u,v) : 0 \le u \le 1, 0 \le v \le 1\}$. Note that the function g is monotonic increasing in its two variables; the monotonicity in u is due to its linearity in u and since λ is non-negative, and the monotonicity in v is due to the monotonicity of the degree distribution λ and ρ over the interval $[0,1]$ and since they are mapped to the same interval. We show in the following, by induction, that $z_l \in [x(z_0), z_0]$ for every integer $l \ge 0$. For $l = 0$, the inequality $x(z_0) \le z_0 \le 1$ holds since for $x \in (z_0, 1]$

$$\frac{x}{\lambda\big(\sqrt{1-\rho(1-x^2)}\big)} \ge x > z_0.$$

Let us assume that $z_{l-1} \in [x(z_0), z_0]$ for a specific $l \ge 1$ then

$$\begin{aligned} z_l &= g(z_0, z_{l-1}) \\ &\overset{\text{(a)}}{\ge} g(z_0, x(z_0)) \\ &= z_0 \lambda\big(\sqrt{1-\rho(1-x(z_0)^2)}\big) \\ &\overset{\text{(b)}}{\ge} x(z_0) \end{aligned}$$

where inequality (a) is due to the monotonicity of g, and inequality (b) follows from the way $x(z_0)$ is defined above (or, more generally, this inequality holds for every

$x \in \mathcal{F}_B$ where the set $\mathcal{F}_{z_0}$ is defined in (C.1)). Also, from the above assumption for z_{l-1}

$$\begin{aligned} z_l &= g(z_0, z_{l-1}) \\ &\leq g(z_0, 1) \\ &= z_0 \end{aligned}$$

and therefore, it follows by induction that

$$x(z_0) \leq z_l \leq z_0, \quad l = 0, 1, \ldots$$

and the sequence $\{z_l\}$ is bounded away from zero (since $x(z_0) > 0$). This completes the proof of Lemma 3.3.

Appendix D

Proof of the Inequality in Remark 3.5

From the definitions of B_0 and B_1 in (3.24) and (3.25), respectively, in order to prove that $B_1(\lambda, \rho) \geq B_0(\lambda, \rho)$, it is sufficient to show that

$$\lambda\big(\sqrt{1-\rho(1-x^2)}\big) \leq \lambda\big(1-\rho(1-x)\big), \quad \forall\, x \in [0,1].$$

Since $\lambda(0) = 0$, $\lambda(1) = 1$, and λ is monotonic increasing over the interval [0, 1], then this inequality is equivalent to

$$\sqrt{1-\rho(1-x^2)} \leq 1-\rho(1-x), \quad \forall\, x \in [0,1].$$

By squaring and rearranging terms, we need to prove that

$$h(x) \triangleq \rho(1-x^2) + \rho^2(1-x) - 2\rho(1-x) \geq 0, \quad \forall\, x \in [0,1].$$

Note that h is zero at the endpoints of this interval (since $\rho(0) = 0$ and $\rho(1) = 1$). From the assumption of right-regularity then $\rho(x) = x^{d_{\mathrm{c}}-1}$. Let $\gamma \triangleq d_{\mathrm{c}} - 1$ (where $\gamma \geq 1$), then

$$\begin{aligned} h(x) &= (1-x^2)^\gamma + (1-x)^{2\gamma} - 2(1-x)^\gamma \\ &= 2(1-x)^\gamma \left[\frac{(1+x)^\gamma + (1-x)^\gamma}{2} - 1\right] \\ &\geq 0 \end{aligned}$$

where the last transition follows from the non-negativity of both terms over the interval $x \in [0,1]$ (the second term is non-negative due to the convexity of the function

$f(x) = x^\gamma$ for $x \geq 0$ (note that $\gamma \geq 1$)). This completes the proof of the inequality in Remark 3.5.

Appendix E

Fixed Point Analysis of (4.8) and (4.9)

At a fixed point of (4.8) and (4.9), $y_l = y_{l-1} \equiv y$ and $\tilde{y}_l = \tilde{y}_{l-1} \equiv \tilde{y}$. Rearranging (4.9) at the fixed point yields

$$1 - \tilde{y} = \frac{1-B}{1-B(1-y)^a}.$$

Plugging this into (4.8) yields the fixed-point equation

$$y = \hat{B}\lambda\left(1 - \left(\frac{1-B}{1-B(1-y)^a}\right)^2 (1-y)^{a-1}\right). \tag{E.1}$$

Convergence to zero is obtained if and only if the equation above has no solution y in $(0,1]$. Denote

$$f(y,B) \triangleq 1 - \left(\frac{1-B}{1-B(1-y)^a}\right)^2 (1-y)^{a-1},$$

so that (E.1) becomes $y = \hat{B}\lambda(f(y,B))$. This is a non-decreasing function in both y and B, since

$$\begin{aligned}\frac{\partial f(y,B)}{\partial B} &= \frac{2(1-B)\left(1-(1-y)^a\right)(1-y)^{a-1}}{\left(1-B(1-y)^a\right)^3} \geq 0,\\ \frac{\partial f(y,B)}{\partial y} &= \frac{(1-B)^2\left(a-1+B(a+1)(1-y)^a\right)(1-y)^{a-2}}{\left(1-B(1-y)^a\right)^3} \geq 0,\end{aligned}$$

where the inequalities are due to $0 \leq y, B \leq 1$ and $a \geq 1$. One solution of (E.1) is $y = 0$. If this is the only solution y in $[0,1]$ for some B, then, since $\lambda(\cdot)$ is monotone increasing, this will also be the only solution of (E.1) for any smaller B.

Appendix F

Universality for MBIOS channels with the same uncoded bit error probability

In this appendix we show how the approach of Section 3.1 can be used for the set $\mathcal{A}$ of MBIOS channels that exhibit the same uncoded bit probability of error, $\mathcal{E}$.

It readily follows from (2.4) that over $\mathcal{A}$, the BSC exhibits the maximal B-parameter and the BEC exhibits the minimal B-parameter. Therefore, here B in (3.3) assumes the form

$$B = \sqrt{4\mathcal{E}(1-\mathcal{E})}.$$

We design a capacity-achieving sequence of LDPC code ensembles for a BEC with erasure probability B, so that the design rate of this ensemble is $R_{\mathrm{d}} = 1 - B$. Over this set, the channel with the maximal capacity is the BSC, with $C = 1 - h_2(\mathcal{E})$. Therefore, the universally achievable fraction of capacity over this set following the approach of Section 3.1 is given by

$$\mu_4(\mathcal{E}) \triangleq \frac{1 - 2\sqrt{\mathcal{E}(1-\mathcal{E})}}{1 - h_2(\mathcal{E})}.$$

Let us analyze the achievable fraction of capacity for the extreme cases of a noiseless channel ($\mathcal{E} = 0$ or $\mathcal{E} = 1$, where in the latter case we simply flip the detections) and very noisy channel ($\mathcal{E} \to 0.5$). Clearly, when $\mathcal{E} = 0$ or $\mathcal{E} = 1$, we have $\mu_4 = 1$, meaning that capacity is achievable. When $\mathcal{E} \to 0.5$, we have

$$\begin{aligned}\lim_{\mathcal{E}\to 0.5} \frac{1-2\sqrt{\mathcal{E}(1-\mathcal{E})}}{1-h_2(\mathcal{E})} &= \ln 2 \lim_{\mathcal{E}\to 0.5} \frac{1-2\mathcal{E}}{\sqrt{\mathcal{E}(1-\mathcal{E})}\ln\left(\frac{1-\mathcal{E}}{\mathcal{E}}\right)} \\ &= \ln 2 \lim_{\mathcal{E}\to 0.5} \frac{-2}{\left(\frac{-2+(1-2\mathcal{E})\ln((1-\mathcal{E})/\mathcal{E})}{2\sqrt{\mathcal{E}(1-\mathcal{E})}}\right)} \\ &= \ln 2.\end{aligned}$$

Thus, over this set of channels, the extreme values of $\mu_4(\mathcal{E})$ are 1 for a noiseless channel and 69.3% for a very noisy channel. We note that this coincides with the extreme values of the achievable fraction of capacity for the two other families considered in Chapter 3 of this thesis: the family of equi-capacity MBIOS channels and the family of equi-B-parameter MBIOS channels (see Theorems 3.1 and 3.4).

References

[1] A. Amraoui, "LDPCopt – a fast and accurate degree distribution optimizer for ldpc code ensembles." [Online]. Available: http://ipgdemos.epfl.ch/ldpcopt/

[2] E. Arikan, "Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels," *Information Theory, IEEE Transactions on*, vol. 55, no. 7, pp. 3051 – 3073, July 2009.

[3] D. Burshtein and G. Miller, "Bounds on the performance of belief propagation decoding," *Information Theory, IEEE Transactions on*, vol. 48, no. 1, pp. 112 – 122, January 2002.

[4] S. Y. Chung, "On the construction of some capacity-approaching coding schemes," Ph.D. dissertation, MIT, 2000. [Online]. Available: http://wicl.kaist.ac.kr/pdf/sychungphdthesis.pdf

[5] S. Y. Chung, D. Forney, T. Richardson, and R. Urbanke, "On the design of low-density parity-check codes within 0.0045 db of the shannon limit," *Communications Letters, IEEE*, 2001.

[6] D. Duyck, M. H. Azmi, J. Yuan, J. J. Boutros, and M. Moeneclaey, "Universal LDPC codes for cooperative communications," in *Proceedings 6th International Symposium on Turbo Codes and Iterative Information Processing*, Brest, France, September 2010, pp. 83 – 87.

[7] M. Franceschini, G. Ferrari, and R. Raheli, “Does the performance of LDPC codes depend on the channel?” *Communications, IEEE Transactions on*, vol. 54, no. 12, pp. 2129 – 2132, December 2006.

[8] R. G. Gallager, *Low-Density Parity-Check Codes*. Cambridge, MA, USA: MIT Press, 1963. [Online]. Available: http://web.mit.edu/gallager/www/pages/ldpc.pdf

[9] M. Grant and S. Boyd, “CVX: Matlab software for disciplined convex programming,” June 2009. [Online]. Available: http://stanford.edu/~boyd/cvx

[10] J. Ha, D. Klinc, J. Kwon, and S. W. McLaughlin, “Layered BP decoding for rate-compatible punctured LDPC codes,” *Communications Letters, IEEE*, vol. 11, no. 5, pp. 440 – 442, May 2007.

[11] C. H. Hsu, “Design and analysis of capacity-achieving codes and optimal receivers with low complexity,” Ph.D. dissertation, University of Michigan, USA, 2006. [Online]. Available: http://www.eecs.umich.edu/~anastas/docs/chunhao_thesis.pdf

[12] C. H. Hsu and A. Anastasopoulos, “Capacity achieving LDPC codes through puncturing,” *Information Theory, IEEE Transactions on*, vol. 54, no. 10, pp. 4698 – 4706, October 2008.

[13] H. Jin, “Analysis and design of turbo-like codes,” Ph.D. dissertation, Caltech, Pasadena, CA, USA, 2001. [Online]. Available: http://resolver.caltech.edu/CaltechETD:etd-08222001-151244

[14] H. Jin, A. Khandekar, and R. McEliece, “Irregular repeat-accumulate codes,” in *Proceedings 2nd International Conference on Turbo Codes and Related Topics*, Brest, France, September 2000, pp. 1 – 8.

[15] H. Jin and T. Richardson, “Block error iterative decoding capacity for LDPC codes,” in *Proceedings of 2005 International Symposium on Information Theory*, September 2005, pp. 52 – 56.

[16] A. Khandekar, “Graph-based codes and iterative decoding,” Ph.D. dissertation, Caltech, Pasadena, CA, USA, 2002. [Online]. Available: http://resolver.caltech.edu/CaltechETD:etd-06202002-170522

[17] I. Land and J. Huber, “Information combining,” *Found. Trends Commun. Inf. Theory*, vol. 3, no. 3, pp. 227 – 330, 2006.

[18] A. Lapidoth and P. Narayan, “Reliable communication under channel uncertainty,” *Information Theory, IEEE Transactions on*, vol. 44, no. 6, pp. 2148 – 2177, October 1998.

[19] M. Lentmaier, D. V. Truhachev, K. S. Zigangirov, and D. J. Costello, “An analysis of the block error probability performance of iterative decoding,” *Information Theory, IEEE Transactions on*, vol. 51, no. 11, pp. 3834 – 3855, November 2005.

[20] M. G. Luby, M. Mitzenmacher, A. Shokrollahi, and D. A. Spielman, “Efficient erasure correcting codes,” *Information Theory, IEEE Transactions on*, vol. 47, no. 2, pp. 569 – 584, February 2001.

[21] C. Measson, A. Montanari, T. Richardson, and R. Urbanke, “The generalized area theorem and some of its consequences,” *Information Theory, IEEE Transactions on*, vol. 55, no. 11, pp. 4793 – 4821, November 2009.

[22] G. Miller and D. Burshtein, “Bounds on the maximum-likelihood decoding error probability of low-density parity-check codes,” *Information Theory, IEEE Transactions on*, vol. 47, no. 7, pp. 2696 – 2710, November 2001.

[23] S. Miyake and M. Maruyama, “Construction of universal codes using LDPC matrices and their error exponents,” *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.*, vol. E90-A, no. 9, pp. 1830 – 1839, September 2007.

[24] P. Oswald and A. Shokrollahi, “Capacity-achieving sequences for the erasure channel,” *Information Theory, IEEE Transactions on*, vol. 48, no. 12, pp. 3017 – 3028, December 2002.

[25] F. Peng, W. E. Ryan, and R. D. Wesel, "Surrogate-channel design of universal LDPC codes," *Communications Letters, IEEE*, vol. 10, no. 6, pp. 480 – 482, June 2006.

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

[27] H. Pishro-Nik and F. Fekri, "Results on punctured low-density parity-check codes and improved iterative decoding techniques," *Information Theory, IEEE Transactions on*, vol. 53, no. 2, pp. 599 – 614, February 2007.

[28] T. Richardson, A. Shokrollahi, and R. Urbanke, "Design of capacity-approaching irregular low-density parity-check codes," *Information Theory, IEEE Transactions on*, vol. 47, no. 2, pp. 619 – 637, February 2001.

[29] T. Richardson and R. Urbanke, *Modern Coding Theory.* Cambridge University Press, March 2008.

[30] A. Roumy, S. Guemghar, G. Caire, and S. Verdú, "Design methods for irregular repeat-accumulate codes," *Information Theory, IEEE Transactions on*, vol. 50, no. 8, pp. 1711 – 1727, August 2004.

[31] A. Sanaei, M. Ramezani, and M. Ardakani, "Identical-capacity channel decomposition for design of universal LDPC codes," *Communications, IEEE Transactions on*, vol. 57, no. 7, pp. 1972 – 1981, July 2009.

[32] I. Sason, "On universal properties of capacity-approaching LDPC code ensembles," *Information Theory, IEEE Transactions on*, vol. 55, no. 7, pp. 2956 – 2990, July 2009.

[33] I. Sason and R. Urbanke, "Parity-check density versus performance of binary linear block codes over memoryless symmetric channels," *Information Theory, IEEE Transactions on*, vol. 49, no. 7, pp. 1611 – 1635, July 2003.

[34] ——, "Complexity versus performance of capacity-achieving irregular repeat-accumulate codes on the binary erasure channel," *Information Theory, IEEE Transactions on*, vol. 50, no. 6, pp. 1247 – 1256, June 2004.

[35] I. Sason and S. Shamai, “Performance analysis of linear codes under maximum-likelihood decoding: a tutorial,” *Found. Trends Commun. Inf. Theory*, vol. 3, no. 1/2, pp. 1–222, 2006.

[36] I. Sason and B. Shuval, “On universal LDPC code ensembles over memoryless symmetric channels,” *Information Theory, IEEE Transactions on*, Accepted for publication.

[37] I. Sason and G. Wiechman, “On achievable rates and complexity of LDPC codes over parallel channels: Bounds and applications,” *Information Theory, IEEE Transactions on*, vol. 53, no. 2, pp. 580 – 598, February 2007.

[38] C. E. Shannon, *A Mathematical Theory of Communication.* CSLI Publications, 1948. [Online]. Available: http://cm.bell-labs.com/cm/ms/what/shannonday/paper.html

[39] J. Shi and R. D. Wesel, “A study on universal codes with finite block lengths,” *Information Theory, IEEE Transactions on*, vol. 53, no. 9, pp. 3066 – 3074, September 2007.

[40] A. Shokrollahi, “Capacity-achieving sequences,” *IMA volumes in Mathematics and its Applications*, vol. 123, pp. 153 – 166, 2000.

[41] I. Sutskover, S. Shamai, and J. Ziv, “Extremes of information combining,” *Information Theory, IEEE Transactions on*, vol. 51, no. 4, pp. 1313 – 1325, April 2005.

[42] ——, “Constrained information combining: Theory and applications for LDPC coded systems,” *Information Theory, IEEE Transactions on*, vol. 53, no. 5, pp. 1617 – 1643, May 2007.

[43] S. Tong, “Tangential sphere bounds on the ensemble performance of ML decoded gallager codes via their exact ensemble distance spectrum,” in *Proceedings of 2008 IEEE International Conference on Communications*, May 2008, pp. 1150 – 1154.

[44] M. Twitto and I. Sason, “On the error exponents of improved tangential sphere bounds,” *Information Theory, IEEE Transactions on*, vol. 53, no. 3, pp. 1196 – 1210, March 2007.

[45] P. O. Vontobel, “A factor-graph approach to universal decoding,” in *Proceedings 44th Annual Allerton Conference on Communication, Control, and Computing*, Monticello, Illinois, USA, September 2006, pp. 23 – 30.

[46] C.-C. Wang, S. R. Kulkarni, and H. V. Poor, “Finite-dimensional bounds on $\mathbb{Z}_m$ and binary LDPC codes with belief propagation decoders,” *Information Theory, IEEE Transactions on*, vol. 53, no. 1, pp. 56 – 81, Januray 2007.

[47] G. Wiechman and I. Sason, “Parity-check density versus performance of binary linear block codes: New bounds and applications,” *Information Theory, IEEE Transactions on*, vol. 53, no. 2, pp. 550 – 579, February 2007.

[48] A. Yedla, H. D. Pfister, and K. R. Narayanan, “Can iterative decoding for erasure correlated sources be universal?” *Forty-Seventh Annual Allerton Conference on Communication, Control and Computing*, September 2009. [Online]. Available: http://arxiv.org/abs/0910.1123

על אנסמבלים אוניברסליים של קודי LDPC
מעל ערוצים סימטריים וחסרי זיכרון

בועז שובל

על אנסמבלים אוניברסליים של קודי LDPC
מעל ערוצים סימטריים וחסרי זיכרון

חיבור על מחקר

לשם מילוי חלקי של הדרישות לקבלת תואר
מגיסטר למדעים
הנדסת חשמל

בועז שובל

הוגש לסנט הטכניון — מכון טכנולוגי לישראל

שבט תשע"א	חיפה	פברואר 2011

חיבור על מחקר נעשה בהדרכת פרופ' יגאל ששון
בפקולטה להנדסת חשמל

הכרת תודה

ראשית, ברצוני להודות למנחה שלי, פרופ' יגאל ששון, שבלעדיו עבודה זו לא היתה מתאפשרת. תמיכתו וסיועו במהלך המחקר לא יסולאו בפז.

ברצוני גם להודות למשפחתי על תמיכתם בי לאורך המחקר ועל כך שתמיד הם שם עבורי.

אני מודה לטכניון על התמיכה הכספית הנדיבה בהשתלמותי

למשפחתי.

תקציר

בשנים האחרונות, השימוש בקודי LDPC הולך וגובר עקב יכולתם להתקרב לקיבול הערוץ גם תחת אלגוריתמי פענוח איטרטיביים תת אופטימליים בעלי סיבוכיות נמוכה. אלגוריתמים אלה מבוססים על ייצוג גרפי של הקוד, בו משתני הקוד ובדיקות הזוגיות מהווים קודקודים, והקשתות בגרף מייצגות את משתני הקוד המשתתפים בבדיקות הזוגיות השונות. בתהליך הפענוח, הקודקודים מעבירים הודעות זה לזה על גבי קשתות הגרף, המחושבות על בסיס ההודעות הקודמות שהתקבלו וכן הקלט מהערוץ. הודעות אלה מהוות "רמת סמך" לגבי ערך המשתנה.

ביצועי אלגוריתם הפענוח האיטרטיבי ניתנים להערכה באופן אסימפטוטי עבור צביר קודי LDPC באמצעות שיטה נומרית הנקראת density evolution. בשיטה זו, אנו מחשבים כיצד מתעדכן פילוג ההודעות העוברות במהלך אלגוריתם הפענוח האיטרטיבי, עבור אורך קוד אינסופי. כך, ניתן להסיק האם הפענוח האיטרטיבי מביא באופן אסימפטוטי להסתברות שגיאה מתאפסת לביט או לא. שיטה זו מהווה גם כלי מרכזי בתכן צבירים של קודי LDPC. המטרה בתכן קודים בשיטה זו היא לתכנן צביר קודי LDPC אשר באופן אסימפטוטי יבטיח תקשורת ללא שגיאות עבור מודל ערוץ מסוים, ואשר הינו אופטימלי במובן של השגת קצב מירבי עבור פרמטרי ערוץ מסוימים או אילוצים אחרים על מבנה הקוד. אחת מהתוצאות הנגזרות משיטת ה־density evolution הינה תנאי היציבות שהינו תנאי הכרחי לכך שצביר מסוים ישיג הסתברות שגיאה מתאפסת לביט באופן אסימפטוטי תחת פענוח איטרטיבי עבור מודל ערוץ מסוים. אף על פי ששיטת ה־density evolution מאפשרת תכן נומרי של צבירים של קודי LDPC, באופן כללי היא איננה מאפשרת תכן אנליטי של צבירים כאלה. מקרה יוצא דופן הינו תכן קודים עבור ערוץ המחיקה הבינארי, שכן עבורו משוואות ה־density evolution ניתנות לפישוט למשוואה חד מימדית בודדת. ואכן, עבור ערוץ המחיקה פותחו שיטות אנליטיות לתכן צבירים של קודי LDPC משיגי קיבול. נכון להיום, עדיין לא נמצאו ביטויים אנליטיים עבור קודי LDPC משיגי קיבול עבור ערוצים חסרי זיכרון אחרים שהינם בינאריים במבוא וסימטריים במוצא.

שיטת פענוח אחרת לקודי LDPC הינה פענוח סבירות מירבית (Maximum Likelihood). זוהי, למעשה, שיטת פענוח אופטימלית, אך שיטה זו איננה מעשית בשל מורכבות הפענוח שלה. עם זאת, יש לציין כי עבור שיטת פענוח זו נמצאו באופן אנליטי ביטויים לצבירים של קודי LDPC

המשיגים את הקיבול עבור ערוצים חסרי זיכרון שהינם בינאריים במבוא וסימטריים במוצא (ולאו דווקא עבור ערוץ המחיקה הבינארי). האנליזה במקרה זה מבוססת על חסמים עליונים על שגיאת הפענוח המשתמשים בחסמים הדוקים על פילוג המשקלים הממוצע של האנסמבל.

תכן נומרי של צבירים של קודי LDPC מבוצע בדרך כלל עבור ערוץ מסוים. אך סטטיסטיקת הערוץ בו נפעיל לבסוף את הקוד בדרך כלל תהא שונה מזו שעבורה הוא תוכנן. ישנו עניין רב, איפוא, הן במישור התיאורטי והן במישור המעשי, בתכן קוד אשר יהא אמין, כלומר ישיג הסתברות שגיאה מתאפסת, עבור משפחה של ערוצים. קודים כאלה נקראים אוניברסליים. ישנן גישות רבות ומגוונות לתכן קודים אוניברסליים, הן מבחינת תכן המקודד והן מבחינת תכן המפענח. המיקוד בעבודה זו הינו בקודי LDPC אוניברסליים, כאשר כאן האוניברסליות משמעה שהקוד ישיג ביצועים טובים מבחינת הסתברות השגיאה עבור משפחה של ערוצים, וזאת תוך כדי שימוש במפענח סטנדרטי עבור קודי LDPC, כדוגמת המפענח האיטרטיבי שתואר בקצרה לעיל.

המיקוד בעבודה זו הינו האוניברסליות של צבירים של קודי LDPC, הן תחת פענוח איטרטיבי תת אופטימלי והן תחת פענוח סבירות מירבית עבור משפחות של ערוצים חסרי זיכרון, בינאריים במבוא, וסימטריים במוצא (ערוצי MBIOS).

בפרק 3 אנו בוחנים את האוניברסליות של קודי LDPC תחת פענוח איטרטיבי. בהתבסס על שיטת ה־ density evolution אנו מפתחים תנאים לאוניברסליות של צבירים של קודי LDPC מעל משפחות של ערוצי MBIOS. תוצאות אלה מאפשרות לנו לפתח גישה אנליטית לתכן של צבירים אוניברסליים של קודי LDPC. לפי גישה זו, על מנת לתכנן קוד LDPC אשר יתכנס עבור כל ערוץ מתוך משפחה של ערוצי MBIOS עלינו לתכנן קוד LDPC עבור ערוץ מחיקה בינארי בעל קבוע Bhattacharyya הזהה לקבוע ה Bhattacharyya המקסימלי במשפחת הערוצים. אנו מראים כי קוד זה משיג הסתברות שגיאה מתאפסת לביט עבור כל ערוץ במשפחה. אנו מפעילים גישה זו על מספר משפחות ערוצים, כדוגמת משפחות של ערוצי MBIOS שווי קיבול, ומחשבים את אחוז הקיבול שניתן להשיג באופן אוניברסלי על גבי המשפחה. אמנם הצבירים משיגים הסתברות שגיאה מתאפסת לביט עבור כל ערוץ במשפחה, אך הם אינם משיגים את הקיבול באופן אוניברסלי עבור כל הערוצים במשפחה.

תנאי האוניברסליות אותם אנו מפתחים מאפשרים לנו למצוא חסמים עליונים על הקצב של צבירי קודי LDPC בעלי דרגה ימנית קבועה אותו ניתן להשיג באופן אוניברסלי על פני משפחת ערוצי MBIOS שווי קיבול. חסמים אלה מבוססים על תנאי הכרחי לאוניברסליות אותו אנו מפתחים, המאפשר לנו להגדיר באמצעותו בעית תכנות לינארי מתאימה. פתרון בעית התכנות הלינארי הינו קצב הקוד המקסימלי שניתן להשיג באופן אוניברסלי ולכן מהווה חסם עליון על הקצב שניתן להשגה. חסם עליון זה מאפשר לנו לתת גם חסם תחתון על הפער לקיבול שניתן להשיג. אנו מראים גם כי ניתן לקבל חסם משופר באמצעות התבוננות במשפחות ערוצי MBIOS שוות קיבול הכוללות גם את ערוץ המחיקה.

יתר על כן, התנאים האנליטיים אותם אנו מפתחים מאפשרים לנו להראות שניתן עבור כל צביר קודי LDPC לסווג את הערוצים ל"טובים" ו"רעים" (במובן של השגת הסתברות שגיאה מתאפסת לביט באופן אסימפטוטי תחת פענוח איטרטיבי), בהתבסס על קבוע Bhattacharyya של הערוץ. כלומר, הקוד ישיג הסתברות שגיאה מתאפסת על גבי כל ערוץ MBIOS בעל קבוע Bhattacharyya הקטן מערך סף מסוים, ומאידך ישיג הסתברות שגיאה חיובית ממש על גבי כל ערוץ MBIOS בעל קבוע Bhattacharyya הגדול מערך סף אחר. אנו גם נותנים ביטוי עבור החסם התחתון להסתברות השגיאה במקרה ה"רע". ערכי הסף האלה מבוססים על מאפייני הקוד בלבד והינם נתונים באמצעות נוסחאות סגורות וקלות לחישוב. בפרט, אנו מראים כיצד ניתן להמיר את החסמים הללו לחסמים תחתונים ועליונים על הסף להתכנסות של קוד LDPC כלשהו. אנו מראים גם כי עבור צבירים מסוימים, חסמים אלה הדוקים.

בפרק 4 אנו מרחיבים את התוצאות של פרק 3 עבור משפחת קודים אחרת שניתנת לייצוג על גבי גרפים, משפחת ה־ Irregular Repeat Accumulate codes. גם משפחת קודים זו ניתנת לניתוח באמצעות density evolution, אם כי הנוסחאות עצמן שונות. את ההרחבה אנו מבצעים באמצעות הפעלת הכלים שפותחו בפרק 3 על משוואות ה־ density evolution המתאימות למשפחה זו.

בפרק 5 אנו דנים באוניברסליות של צבירים של קודי LDPC תחת פענוח סבירות מירבית. התוצאות מהפרקים הקודמים, עבור אלגוריתם הפענוח התת־אופטימלי belief propagation, תקפים כמובן גם תחת פענוח סבירות מירבית (שהוא אופטימלי). אך תחת פענוח סבירות מירבית ניתן לקבל תוצאות חזקות יותר, ובפרט, אנו מראים כי הצביר של גלגר של קודי LDPC רגולריים, תחת תנאים מסויימים, יכול להשיג את הקיבול באופן אוניברסלי עבור משפחת ערוצי ה־ MBIOS שווי הקיבול. כאשר כאן אנו מתקרבים לקיבול כרצוננו לכל ערוצי ה־ MBIOS שווי הקיבול, ובנוסף משיגים הסתברות שגיאה מתאפסת לבלוק (לעומת הסתברות שגיאה מתאפסת לביט תחת פענוח איטרטיבי). אנו גם מרחיבים תוצאה זו עבור קודי LDPC המנוקבים באופן אקראי.

סיכום העבודה והצעת נושאים להמשך מחקר מופיעים בפרק 6.