Coding Theorems via Jar Decoding

by

Jin Meng

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Doctor of Philosophy
in
Electrical and Computer Engineering

Waterloo, Ontario, Canada, 2013

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Abstract

In the development of digital communication and information theory, every channel decoding rule has resulted in a revolution at the time when it was invented. In the area of information theory, early channel coding theorems were established mainly by maximum likelihood decoding, while the arrival of typical sequence decoding signaled the era of multi-user information theory, in which achievability proof became simple and intuitive. Practical channel code design, on the other hand, was based on minimum distance decoding at the early stage. The invention of belief propagation decoding with soft input and soft output, leading to the birth of turbo codes and low-density-parity check (LDPC) codes which are indispensable coding techniques in current communication systems, changed the whole research area so dramatically that people started to use the term "modern coding theory" to refer to the research based on this decoding rule. In this thesis, we propose a new decoding rule, dubbed jar decoding, which would be expected to bring some new thoughts to both the code performance analysis and the code design.

Given any channel with input alphabet $\mathcal{X}$ and output alphabet $\mathcal{Y}$, jar decoding rule can be simply expressed as follows: upon receiving the channel output $y^n \in \mathcal{Y}^n$, the decoder first forms a set (called a jar) of sequences $x^n \in \mathcal{X}^n$ considered to be close to y^n and pick any codeword (if any) inside this jar as the decoding output. The way how the decoder forms the jar is defined independently with the actual channel code and even the channel statistics in certain cases. Under this jar decoding, various coding theorems are proved in this thesis. First of all, focusing on the word error probability, jar decoding is shown to be near optimal by the achievabilities proved via jar decoding and the converses proved via a proof technique, dubbed the outer mirror image of jar, which is also quite related to jar decoding. Then a Taylor-type expansion of optimal channel coding rate with finite block length is discovered by combining those achievability and converse theorems, and it is demonstrated that jar decoding is optimal up to the second order in this Taylor-type expansion. Flexibility of jar decoding is then illustrated by proving LDPC coding theorems via jar decoding, where the bit error probability is concerned. And finally, we consider a coding scenario, called interactive encoding and decoding, and show that jar decoding can be also used to prove coding theorems and guide the code design in the scenario of two-way communication.

Acknowledgements

Before a long list of people I owe my thanks to for making this thesis possible, my deepest gratitude and admiration is reserved for my supervisor, Professor En-Hui Yang, who has taught me to appreciate the beauty of information theory and data compression and constantly inspired me to think and work on exciting research topics in those areas. Moreover, his training of logic thinking, preciseness and rigour benefits me even beyond my academic career.

I am extremely grateful of the examining committee members, formed by distinguished scholars. I would like to thank Professor Liang-liang Xie, Professor Patrick Mitran, and Professor Alejandro Lopez-Ortiz for their valuable comments in my comprehensive exam and their commitment to my PH.D defense. And I would like to thank Professor Ning Cai from Xidian University for serving as my external examining committee member.

I am also greatly indebted to co-authors with whom I am honored to share papers during my PH.D. study. The list includes but is not limited to Professor Zhen Zhang from University of Southern California for teaching me to glimpse great knowledge of coding theory, Dr. Dake He from Research In Motion Limited for his help on academic writing and inspiring me to solve practical problem related to my research, and Professor Shenghao Yang in Tsinghua University for his friendship and willingness to share his research knowledge.

I would like to thank all the people with whom I am lucky to work in Multimedia Communication Lab during the past six years, including Dr. Xiang Yu, Professor Haiquan Wang, Dr. Wei Sun, Dr. Lin Zheng, Professor Yuan Luo, Dr. Mehdi Torbatian, Yuhan Zhou, Chang Sun, James Ho, Fei Teng, Jie Zhang, Krishna Rapaka, Krzysztof Michal Hebel, Mahshad Eslamifar, Nan Hu, Yueming Gao and Duo Xu, for their invaluable friendship.

Finally, my sincere gratitude goes to my family, to my father and mother, who always provide me great support and are the very motivation for any achievement I pursue, and to my wife Yan whose encouragement and consolation are the source of my strength.

To Yan

Table of Contents

List of Tables

List of Figures

List of Acronyms

AMC	adaptive modulation and coding
BEC	binary erasure channel
BIAGC	binary input additive Gaussian channel
BIMC	binary input memoryless channel with uniform capacity achieving distribution
BIMSC	binary input memoryless symmetric channel
BP	belief propagation
BSC	binary symmetric channel
DIMC	discrete input memoryless channel
IED	interactive encoding and decoding
LDPC	low density parity check
MAP	maximum a posteriori
MD	minimum distance
MIBOS	memoryless input binary output symmetric
ML	maximum likelihood
NEP	non-asymptotic equipartition property
SWC	Slepian-Wolf coding

Chapter 1

Introduction

1.1 Channel Decoding Rules

In the literature of channel coding so far, channel decoding is predominantly associated with maximum a posteriori (MAP) decoding, maximum likelihood (ML) decoding, minimum distance (MD) decoding, typical sequence decoding, and, more recently, message-passing decoding [1–5]. In MAP decoding and ML decoding, upon receiving a channel output sequence $y^n = y_1 y_2 \cdots y_n$, the MAP (ML, respectively) decoder examines each and every codeword, and then selects the one maximizing the a posteriori probability (likelihood, respectively) as the estimate of the transmitted codeword. Similarly, in MD decoding, the MD decoder examines each and every codeword, and then chooses the one closest to the received sequence y^n as the estimate of the transmitted codeword. In typical sequence decoding, the decoder examines each and every codeword, and chooses one jointly typical with y^n as the estimate of the transmitted codeword. All these decoding rules are more or less codebook centric. On the other hand, message passing decoding (including belief propagation (BP) decoding for low density parity check (LDPC) codes) is received sequence centric to some extent; upon receiving y^n, it updates and passes messages from one iteration to another until it finds a codeword or fails to converge.

All decoding rules mentioned above have their own advantages and limitations. MAP decoding is optimal in the sense of minimizing the word error probability; it is applicable to any code and channel in theory, and it is also widely adopted in the theoretic performance analysis of a coded communication system. However, MAP decoding has prohibitive computation complexity when the number of codewords is large, thus making it impractical. In addition, performance analysis under MAP decoding sometimes becomes

extremely difficult. For example, to the best of our knowledge, the performance analysis of random linear codes based on Gallager's parity check ensembles under MAP decoding for asymmetric memoryless channels is still unknown because codewords are generally not pairwisely independent. Since ML decoding and MD decoding are equivalent to MAP decoding under some conditions, they have the same advantages and limitations as does MAP decoding. Typical sequence decoding is a convenient information theoretic tool for proving asymptotic coding theorems in information theory. However, it is generally applicable only to Shannon random codes and also has prohibitive computation complexity. In addition, these decoding rules are generally concerned with the word error probability. In contrast, message passing decoding has low decoding complexity and is generally concerned with the bit error probability. However, message passing decoding is suboptimal in the sense of either minimizing the bit error probability or word error probability and is applicable only to certain types of codes such as LDPC codes and turbo codes; it is also difficult, if not impossible, to have a rigorous analysis of message passing decoding [5].

It would be desirable to develop a new decoding rule which can have all advantages of the above decoding rules. To this end, in this thesis, we propose a new decoding rule dubbed *jar decoding*. Given a channel, code, and channel output sequence y^n, jar decoding first forms a set of suitable size, called a jar, consisting of sequences from the channel input alphabet considered to be closely related to y^n, and then takes any codeword from the jar as the estimate of the transmitted codeword. If only the first order coding performance is concerned, given any transmission rate, discrete channel input alphabet, and discrete channel output alphabet, the jar corresponding to y^n can be even formed a priori without knowing either the code or the channel. In this sense, unlike MAP, ML, MD, and typical sequence decoding, but similar to message passing decoding, jar decoding is channel output sequence centric. In addition, jar decoding is flexible in the sense that it can handle both the word error probability and bit error probability and deal with coding problem in interactive information theory where the jar can change dynamically; it is also powerful in the sense that new coding theorems, which could not be or at least have not been proved with MAP, ML, or typical sequence decoding, can be established.

As evidenced by the evolution of digital communication and information theory over the past 60 years, different decoding rules bring in different perspectives not only on decoding itself, but also on how to design codes particularly suitable for the respective decoding rule. In the first 40 years or so after the birth of information theory, code design was predominantly on how to construct codes which can maximize the distance of the codes under some conditions due to the union bound analysis under ML decoding. With message passing decoding, however, code design was changed dramatically in recent 20 years or so. For example, with BP decoding for LDPC codes, code design was largely on how

to construct variable and check node degree distributions so that LDPC codes generated from these degree distributions are efficient under BP decoding. With jar decoding, it is expected that similar change would happen in code design, and we believe that there is ample room to design effective codes and jar decoding algorithms.

1.2 Jar Decoding

Consider a memoryless channel $\{p(y|x) : x \in \mathcal{X}, y \in \mathcal{Y}\}$, where $\mathcal{X}$ is the channel input alphabet, and $\mathcal{Y}$ is the channel output alphabet. In this thesis, we mainly consider the case where $\mathcal{X}$ is finite, but $\mathcal{Y}$ is arbitrary and could be discrete or continuous. Such a channel will be referred to as a discrete input memoryless channel (DIMC) . As such, for any $x \in \mathcal{X}$, $p(y|x)$ is a probability mass function (pmf) over $\mathcal{Y}$ if $\mathcal{Y}$ is discrete, and a probability density function (pdf) over $\mathcal{Y}$ if $\mathcal{Y}$ is the real line.

Given a DIMC $\{p(y|x) : x \in \mathcal{X}, y \in \mathcal{Y}\}$, its capacity is given by

$$C_{\text{DIMC}} \stackrel{\Delta}{=} \max_{X} I(X;Y) \tag{1.1}$$

where Y is the channel output in response to an input X, $I(X;Y)$ is the mutual information between X and Y, and the maximization is taken over all possible input random variables X. Of particular interest is the case where the maximum in (1.1) is achieved at the uniformly distributed random variable X. Such a DIMC is said to have the uniform capacity achieving distribution; in this case,

$$C_{\text{DIMC}} = \ln |\mathcal{X}| - H(X|Y) \tag{1.2}$$

where Y is the channel output in response to the uniform input random variable X, and $H(X|Y)$ is the conditional entropy of X given Y.

Two well known examples of a binary input memoryless channel with uniform capacity achieving distribution (BIMC) are the binary symmetric channel (BSC) and the binary input additive Gaussian channel (BIAGC) . For the BSC, its channel input and output relationship is described by

$$Y = X \oplus Z \tag{1.3}$$

where $\oplus$ denotes the modulo-2 addition, and Z is a binary random variable independent of the channel input X with $\Pr\{Z = 1\} = p$, $0 < p < 0.5$. The capacity of the BSC is equal to

$$C_{BSC} = \ln 2 - H(p) \tag{1.4}$$

where $H(p) = -p \ln p - (1-p)\ln(1-p)$ is the binary entropy function. For the BIAGC, its channel input and output relationship is described by

$$Y = X + W \tag{1.5}$$

where $X \in \{1, -1\}$, and W is a Gaussian random variable with zero mean and variance σ^2 and independent of X. Its capacity is equal to

$$C_{\text{BIAGC}} = \ln 2 - \frac{1}{2} - \int \frac{1}{2\sqrt{2\pi\sigma^2}} \left(e^{-\frac{(y-1)^2}{2\sigma^2}} + e^{-\frac{(y+1)^2}{2\sigma^2}} \right) \ln \left[e^{-\frac{(y-1)^2}{2\sigma^2}} + e^{-\frac{(y+1)^2}{2\sigma^2}} \right] dy \, . \tag{1.6}$$

1.2.1 Concept and Illustration of Jar Decoding

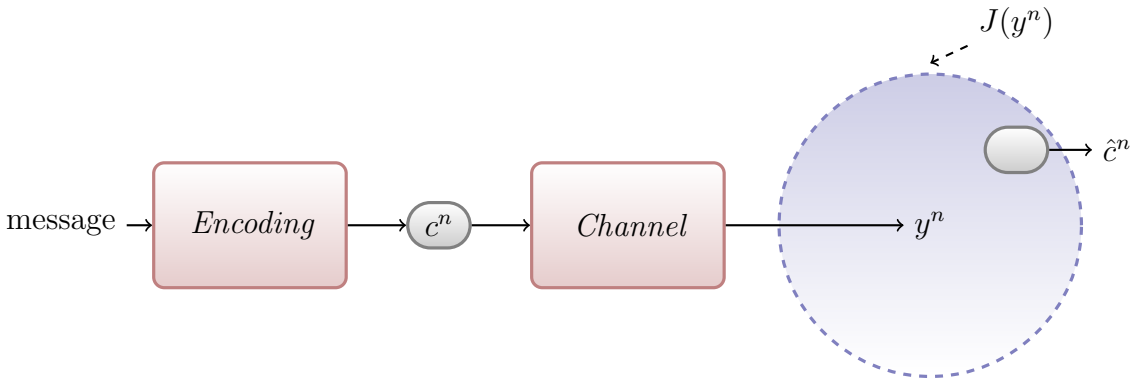


Figure 1.1: Jar Decoding

Definition 1.1 (Jar Decoding)**.** As illustrated in Figure 1.1, given any channel with input alphabet $\mathcal{X}$ and output alphabet $\mathcal{Y}$, which may not be necessarily memoryless, any code of block length n for the channel, and any channel output sequence $y^n \in \mathcal{Y}^n$, jar decoding first forms a set of suitable size (called a jar and denoted by $J(y^n)$) consisting of sequences $x^n \in \mathcal{X}^n$ believed to be closely related to y^n through the channel, and then picks any codeword (if any) from the jar $J(y^n)$ as the estimate of the transmitted codeword.

Discussion: For many channels including all binary input memoryless channels with uniform capacity achieving distribution, the jar $J(y^n)$ can be formed a priori without knowing the actual code to be used over the channels. When $\mathcal{Y}$ is also finite, the jar $J(y^n)$ can be even formed a priori without knowing either the actual code to be used over the

channel or the channel itself. In this sense, jar decoding is channel output y^n centric, in contrast with MAP, ML, MD, and typical sequence decoding, which are all codebook centric. Of course, in the final decoding stage, the knowledge of the channel and code is needed implicitly to pick a codeword from the jar $J(y^n)$ as the estimate of the transmitted codeword. This property is similar to the double universality of Yang-Kieffer lossy codes [6] as commented by Berger and Gibson in [7]. Below we will further illustrate this through examples.

Example 1 (Hamming Jar): Consider the BSC with cross-over probability $0 < p < 0.5$. No matter what the code of block length n used over the BSC is, the jar $J(y^n)$ for each $y^n \in \{0,1\}^n$ can be formed as

$$J(y^n) = \left\{ x^n \in \mathcal{X}^n : \frac{1}{n} wt(y^n - x^n) \leq p + \delta \right\} \tag{1.7}$$

where $wt(z^n)$ denotes the Hamming weight of z^n, i.e., the number of nonzero entries in z^n, and δ is a real number. For the obvious reasons, the jar defined in (1.7) will be referred to as a Hamming jar. The size of $J(y^n)$ is

$$\sum_{0 \leq w \leq n(p+\delta)} \left(\begin{array}{c} n \\ w \end{array} \right)$$

and upper bounded by $e^{nH(p+\delta)}$ whenever $p + \delta < 0.5$.

Let us now look at why jar decoding works effectively in this case. Let c^n be the codeword transmitted over the BSC, and Y^n the corresponding channel output. From the law of large numbers or the Chernoff bound, it is not hard to see that as long as δ is not too small, c^n is in the jar $J(Y^n)$ with high probability. Therefore, jar decoding would succeed if there is no other sequence in the jar $J(Y^n)$ which is also a codeword, which is generally true if the code used over the BSC is well designed. For example, for random linear codes, the probability that $x^n \in J(Y^n)$, $x^n \neq c^n$, is a codeword is upper bounded by $e^{-n[\ln 2 - R]}$, where R is the code rate in nats. This implies the probability that the jar $J(Y^n)$ contains another codeword is upper bounded by $e^{-n[\ln 2 - R - H(p+\delta)]}$. Therefore, jar decoding succeeds with high probability whenever $R < \ln 2 - H(p+\delta)$. Note that $\ln 2 - H(p+\delta)$ is close to the BSC capacity $C_{BSC} = \ln 2 - H(p)$. The argument presented here will be made rigorous in Section 2.1 to establish non-asymptotic linear coding theorems for the BSC.

Example 2 (BIAGC Jar): Consider now the BIAGC with $\mathcal{X} = \{1, -1\}$. For any $x^n = x_1 x_2 \cdots x_n \in \mathcal{X}^n$ and any real-valued sequence $y^n = y_1 y_2 \cdots y_n$, let

$$|y^n - x^n|^2 = \sum_{i=1}^{m} |y_i - x_i|^2 .$$

The jar $J(y^n)$ can be formed as

$$J(y^n) = \left\{ x^n \in \mathcal{X}^n : -\frac{1}{n} \ln \frac{e^{-\frac{|y^n - x^n|^2}{2\sigma^2}}}{\prod_{i=1}^n \left[e^{-\frac{(y_i-1)^2}{2\sigma^2}} + e^{-\frac{(y_i+1)^2}{2\sigma^2}} \right]} \leq H(X|Y) + \delta \right\} \tag{1.8}$$

where Y is the BIAGC output in response to the uniform input random variable X, and δ is a real number. It is not hard to verify that

$$|J(y^n)| \leq e^{n(H(X|Y)+\delta)}$$

for any y^n.

Example 3 (BIMC Jar): Consider now an arbitrary BIMC with binary alphabet $\mathcal{X} = \{0, 1\}$. As indicated in (1.2), its capacity is equal to

$$C_{\text{BIMC}} = \ln 2 - H(X|Y)$$

where Y is the BIMC output in response to the uniform input random variable X. For any $x^n \in \mathcal{X}^n$ and $y^n \in \mathcal{Y}^n$, let

$$p(y^n|x^n) = \prod_{i=1}^n p(y_i|x_i) \ .$$

Then given y^n,

$$\frac{p(y^n|x^n)}{\prod_{i=1}^n [p(y_i|0) + p(y_i|1)]}$$

is a pmf over $\mathcal{X}^n$. In this case, the jar $J(y^n)$ for y^n can be formed as

$$J(y^n) = \left\{ x^n \in \mathcal{X}^n : -\frac{1}{n} \ln \frac{p(y^n|x^n)}{\prod_{i=1}^n [p(y_i|0) + p(y_i|1)]} \leq H(X|Y) + \delta \right\} \tag{1.9}$$

where δ is a real number. Once again, one can verify that

$$|J(y^n)| \leq e^{n(H(X|Y)+\delta)} \tag{1.10}$$

for any y^n.

The reason why jar decoding works effectively in this case is similar to the BSC case. Let us look at linear block codes of block length n again. For any linear block code of

block length n with any rate $R > 0$, suppose we randomly pick its coset code for use over the BIMC. Then the transmitted codeword c^n takes any sequence in $\mathcal{X}^n$ equally likely. Let Y^n be the BIMC output in response to c^n. From the asymptotic equipartition property (AEP) [4] or the non-asymptotic equipartition property established in Appendix A, it follows that with high probability, c^n is in the jar $J(Y^n)$ as long as δ is not too small. Therefore, jar decoding would succeed if there is no other sequence in the jar $J(Y^n)$ which is also a codeword, which is generally true if the linear block code is well designed.

Example 4 (Empirical Conditional Entropy Jar): Suppose now that the channel output alphabet $\mathcal{Y}$ is finite, and the channel is memoryless, but otherwise unknown. For any $x^n \in \mathcal{X}^n$ and $y^n \in \mathcal{Y}^n$, let $h(x^n|y^n)$ be the normalized empirical conditional entropy of x^n given y^n, i.e.,

$$h(x^n|y^n) \triangleq \sum_{y\in\mathcal{Y}} \sum_{x\in\mathcal{X}} \frac{n(x,y)}{n} \left[-\ln \frac{n(x,y)}{n(y)} \right]$$

where $n(x,y)$ ($n(y)$, respectively) is the number of times (x,y) (y, respectively) appears in $(x^n,y^n) = \{(x_i,y_i)\}_{i=1}^n$ (y^n, respectively). In this case, the jar $J(y^n)$ for each y^n can be formed as

$$J(y^n) = \{x^n \in \mathcal{X}^n : h(x^n|y^n) \le T\} \tag{1.11}$$

where $T > 0$ generally depends on the targeted transmission rate. Using the standard type technique [4], one can verify that

$$|J(y^n)| \le \left[\binom{n+|\mathcal{X}|-1}{|\mathcal{X}|-1} \right]^{|\mathcal{Y}|} e^{nT} .$$

Example 5 (Jar from Classical Prefix Codes): Suppose now that the channel output alphabet $\mathcal{Y}$ is finite, and the channel is unknown and not necessarily memoryless, but ergodic. Let $\mathcal{S}_n$ denote a (classical) prefix code with side information available to both the encoder and decoder, where $\mathcal{S}_n$ is a mapping from $\mathcal{X}^n \times \mathcal{Y}^n$ to $\{0,1\}^*$ satisfying that for any $y^n \in \mathcal{Y}^n$, the set $\{\mathcal{S}_n(x^n,y^n) : x^n \in \mathcal{X}^n\}$ is a prefix set. (See, for example, [8–13], and the references therein for the existence of such universal prefix codes.) Let $h_n(\cdot|\cdot)$ denote its normalized length function such that $nh_n(x^n|y^n)$ is the number of nats resulting from applying $\mathcal{S}_n$ to encode x^n from $\mathcal{X}$ given the side information sequence y^n from $\mathcal{Y}$ available to both the encoder and decoder. In this case, the jar $J(y^n)$ for each y^n can be formed as

$$J(y^n) = \{x^n \in \mathcal{X}^n : h_n(x^n|y^n) \le T\} \tag{1.12}$$

where $T > 0$ generally depends on the targeted transmission rate. In view of the Kraft inequality, one can verify that

$$|J(y^n)| \le e^{nT}. \tag{1.13}$$

1.2.2 Connections with Old Decoding Rules

From the previous subsection, it is apparent that jar decoding is quite different from MAP, ML, MD, typical sequence, and BP decoding. In this section, we further demonstrate, by examples, that to a large extent, jar decoding indeed has advantages of all these old decoding rules.

Connection with MD decoding: Let us first look at the BSC. As discussed in Example 1, the jar $J(y^n)$ for each $y^n \in \{0,1\}^n$ in this case is the Hamming jar given in (1.7). Let $\mathcal{C}$ be the actual code of block length n used over the BSC, and $c^n \in \mathcal{C}$ the codeword transmitted over the BSC. Given a received sequence y^n, in minimum Hamming distance decoding, the decoder selects

$$\hat{c}^n \stackrel{\Delta}{=} \arg\min_{b^n \in \mathcal{C}} wt(y^n - b^n) \tag{1.14}$$

as the estimate of the transmitted codeword c^n. In view of (1.7), if the jar $J(y^n)$ contains a codeword, it must contain $\hat{c}^n$ too. Therefore, if the jar $J(y^n)$ contains only one codeword, which is true with high probability when the code $\mathcal{C}$ is well designed, then jar decoding and minimum Hamming distance decoding agree! Furthermore, one of many ways to pick a codeword from the jar $J(y^n)$ is to select

$$\tilde{c}^n \stackrel{\Delta}{=} \arg\min_{b^n \in \mathcal{C} \cap J(y^n)} wt(y^n - b^n) \tag{1.15}$$

as the estimate of the transmitted codeword c^n. Of course, behind this similarity and agreement is a striking difference. In minimum Hamming distance decoding, one always has to solve (1.14) and ends up with a codeword (right or wrong). On the other hand, in jar decoding, if the jar $J(y^n)$ does not contain a codeword, jar decoding may not produce a codeword, even though such probability is very small; if the jar $J(y^n)$ does contain a codeword, one does not have to solve (1.15) and picking up any codeword from the jar is just fine. This flexibility leaves ample room to reduce decoding complexity. The correctness of jar decoding is guaranteed by the fact that with high probability, the jar $J(y^n)$ contains one and only one codeword—the transmitted codeword c^n—in the case of word error probability or codewords very close (in Hamming distance) to c^n in the case of bit error probability, as shown in the proofs of our coding theorems in subsequent chapters.

The above analysis and comparison can be applied equally well to jar decoding and minimum Euclidean distance decoding in the case of BIAGC. As discussed in Example 2, the jar $J(y^n)$ for each real-valued sequence y^n in this case is the BIAGC jar given in (1.8). Let $\mathcal{C} \subset \mathcal{X}^n$ be the actual code of block length n used over the BIAGC, and $c^n \in \mathcal{C}$

the codeword transmitted over the BIAGC. Given a received real-valued sequence y^n, in minimum Euclidean distance decoding, the decoder selects

$$\hat{c}^n \stackrel{\Delta}{=} \arg\min_{b^n \in \mathcal{C}} |y^n - b^n| \tag{1.16}$$

as the estimate of the transmitted codeword c^n. In view of (1.8), if the jar $J(y^n)$ contains a codeword, it must contain $\hat{c}^n$ too. Therefore, if the jar $J(y^n)$ contains only one codeword, which is true with high probability when the code $\mathcal{C}$ is well designed, then jar decoding and minimum Euclidean distance decoding agree! Furthermore, one of many ways to pick a codeword from the jar $J(y^n)$ is to select

$$\tilde{c}^n \stackrel{\Delta}{=} \arg\min_{b^n \in \mathcal{C} \cap J(y^n)} |y^n - b^n| \tag{1.17}$$

as the estimate of the transmitted codeword c^n. The rest of comparison goes along the same way as in the case of BSC. As a final note, in both cases of BSC and BIAGC, since codewords are equally likely, minimum distance (Hamming or Euclidean as the case may be) is equivalent to MAP and ML decoding.

Connection with ML decoding: Consider an arbitrary BIMC $\{p(y|x) : x \in \mathcal{X}, y \in \mathcal{Y}\}$ with $\mathcal{X} = \{0, 1\}$. In this case, as discussed in Example 3, the jar $J(y^n)$ for each sequence $y^n \in \mathcal{Y}^n$ is the BIMC jar given in (1.9). Let $\mathcal{C} \subset \mathcal{X}^n$ be the actual code of block length n used over the BIMC, and $c^n \in \mathcal{C}$ the codeword transmitted over the BIMC. Given a received sequence $y^n \in \mathcal{Y}^n$, in ML decoding, the decoder selects

$$\hat{c}^n \stackrel{\Delta}{=} \arg\max_{b^n \in \mathcal{C}} p(y^n|b^n) \tag{1.18}$$

as the estimate of the transmitted codeword c^n. In view of (1.9), it is not hard to see that if the jar $J(y^n)$ contains a codeword, it must contain $\hat{c}^n$ too. Therefore, if the jar $J(y^n)$ contains only one codeword, which is true with high probability when the code $\mathcal{C}$ is well designed, then jar decoding and ML decoding agree! Furthermore, one of many ways to pick a codeword from the jar $J(y^n)$ is to select

$$\tilde{c}^n \stackrel{\Delta}{=} \arg\max_{b^n \in \mathcal{C} \cap J(y^n)} p(y^n|b^n) \tag{1.19}$$

as the estimate of the transmitted codeword c^n. The rest of comparison goes along the same way as in the case of BSC. Note that in the case of BIMC, since codewords are equally likely, MAP and ML decoding are identical.

Connection with typical sequence decoding: As mentioned early, typical sequence decoding is an information theoretic tool for proving asymptotic coding theorems in information theory; it is applicable only to Shannon random codes. By forming the jar $J(y^n)$ as

$$J(y^n) = \{x^n \in \mathcal{X}^n : x^n \text{ is jointly typical with } y^n\} \tag{1.20}$$

it is easy to see that typical sequence decoding is actually a special case of jar decoding. Of course, the jointly typical jar defined above is of limited practical use for several reasons including (1) it is asymptotic and (2) it rejects non-typical received sequences y^n from the outset. However, this connection does indicate the potential of applying jar decoding to multi-user communication problems as well.

Connection with Feinstein's threshold decoding: In [14], Feinstein proposed a decoding rule, called threshold decoding, in which the decoder selects a codeword whose likelihood passes certain threshold, declares an error if no such codeword exists and chooses the codeword with the lowest index if more than one codeword passes the likelihood threshold. As can be seen, threshold decoding is also a special case of jar decoding, where the jar consists of all sequences x^n passing the likelihood threshold given the channel output y^n. Moreover, threshold decoding specifies the tie-breaking rule when more than one codeword is inside the jar, in which case the one with the lowest index is selected.

Connection with BP decoding: For LDPC codes, BP decoding is one of many ways to pick up a codeword from the jar $J(y^n)$. This will be further confirmed by our simulation results in Section 5.5.

1.3 Organization and Main Contribution

The rest of this thesis is organized as follows.

In Chapter 2, non-asymptotic channel coding achievabilities proved via jar decoding are presented. In particular, it is shown that with jar decoding,

1) random linear codes of block length n can reach within

$$\sigma_H(X|Y)\sqrt{\frac{2\alpha \ln n}{n}} + \frac{(\alpha + 0.5)\ln n}{n} + O\left(\frac{\ln \ln n}{n}\right)$$

of the capacity of any binary input memoryless channel with uniform capacity-achieving input X and arbitrary (either discrete or continuous) channel output al-

phabet (BIMC) while maintaining the word error probability

$$\frac{n^{-\alpha}}{2\sqrt{\pi\alpha\ln n}}+O\left(n^{-\alpha}\frac{\ln^{3/2}n}{\sqrt{n}}\right),$$

and within

$$\frac{c}{\sqrt{n}}+\frac{\ln n}{2n}-\frac{1}{n}\ln\frac{(1-C_{BE})M_H(X|Y)}{\sigma_H^3(X|Y)}$$

of the capacity while maintaining the word error probability

$$Q\left(\frac{c}{\sigma_H(X|Y)}\right)+\frac{M_H(X|Y)}{\sigma_{\mathrm{H}}^3(X|Y)}\frac{1}{\sqrt{n}},$$

where $\sigma_H^2(X|Y)$ and $M_H(X|Y)$ are the conditional information variance and absolute third moment respectively of X given the channel output Y, $Q(z)=\frac{1}{\sqrt{2\pi}}\int_z^\infty e^{-t^2/2}dt$, and $C_{BE}<1$ is the universal constant in the Berry-Esseen central limit theorem;

2) the non-asymptotic achievable bound on random linear codes for BIMC (including BSC and BEC as special examples) is essentially identical with Dependence Testing Bound on Shannon random codes in [15], one of the tightest achievable bounds in literature;

3) and Shannon random codes of block length n and fixed codeword type t can achieve a similar tradeoff between the diminishing capacity gap and the word error probability for any DIMC.

Furthermore, compared to existing achievabilities applicable to random linear code ensembles or Shannon random code ensemble with a fixed codeword type from the previous literature, our achievabilities are shown to be new, very tight and easy to compute, which suggests that jar decoding, as a suboptimal decoding rule, does not lose much optimality to ML decoding, especially in the case of practical interest when the block length is not large and the channel coding rate is close to the capacity.

To confirm the near optimality of jar decoding, a proof technique of non-asymptotic channel coding converses, dubbed *the outer mirror image of jar*, is developed in Chapter 3. Using this proof technique, which is also quite related to the concept of jar as its name suggests, non-asymptotic channel coding converse theorems are derived, which show that

1) for BIMSC, a special class of BIMC, any channel code suffers at least

$$\sigma_H(X|Y)\sqrt{\frac{2\alpha\ln n}{n}}-O\left(\frac{\ln n}{n}\right)$$

rate penalty from channel capacity by maintaining word error probability

$$\frac{n^{-\alpha}}{2\sqrt{\pi\alpha \ln 2}}\left(1-\frac{1}{2\alpha \ln n}\right)$$

and

$$\frac{\sigma_H(X|Y)}{\sqrt{n}}Q^{-1}(\epsilon)-\frac{\ln n}{n}-O(n^{-1})$$

rate penalty from channel capacity by maintaining word error probability ϵ;

2) and similar upper bounds on trade-off between channel coding rate and the word error probability hold for DIMC in general.

Those converses are shown to be very tight compared to existing results from the previous literature, especially the non-asymptotic converses proved in [15]. Furthermore, combining those converses with the achievabilities in Chapter 2 implies that jar decoding achieves the first and second order of optimal channel coding rate with respect to block length n when the error probability ϵ is a constant or sub-exponentially decreasing function of n.

In the non-asymptotic regime when both n and ϵ are finite, however, treating ϵ as a constant or function of n is not convenient. Chapter 4 is then devoted to analyzing the second order channel coding performance and confirming the second order optimality of jar decoding in the non-asymptotic regime. Towards this, a quantity $\delta_{t,n}(\epsilon)$ is then defined to measure the relative magnitude of the error probability ϵ and block length n with respect to a given channel and an input distribution t. By combining the achievabilities of jar decoding in Chapter 2 and the converses in Chapter 3, it is demonstrated that when $\epsilon < 1/2$, the best channel coding rate $R_n(\epsilon)$ given n and ϵ has a "Taylor-type expansion" with respect to $\delta_{t,n}(\epsilon)$, where the first two terms of the expansion are $\max_t[I(t;P)-\delta_{t,n}(\epsilon)]$, which is equal to $I(t^*,P)-\delta_{t^*,n}(\epsilon)$ for some optimal distribution t^*, and the third order term of the expansion is $O(\delta^2_{t^*,n}(\epsilon))$ whenever $\delta_{t^*,n}(\epsilon)=\Omega(\sqrt{\ln n/n})$, thus implying the optimality of jar decoding up to the second order coding performance. Moreover, based on the Taylor-type expansion and the converses in Chapter 3, two approximation formulas for $R_n(\epsilon)$ (dubbed "SO" and "NEP") are provided; they are further evaluated and compared against some of the best bounds known so far, as well as the normal approximation of $R_n(\epsilon)$ revisited in the recent literature. It turns out that while the normal approximation is all over the map, i.e. sometime below achievable bounds and sometime above converse bounds, the SO approximation is much more reliable as it is always below converses; in the meantime, the NEP approximation is the best among the three and always provides an accurate estimation for $R_n(\epsilon)$. An important implication arising from the Taylor-type expansion

of $R_n(\epsilon)$ is that in the practical non-asymptotic regime, the optimal marginal codeword symbol distribution is not necessarily a capacity achieving distribution. In addition, to demonstrate the impact of this Taylor-type expansion on practical communication system design, a practical issue in adaptive modulation and coding, i.e. how to select constellation and coding rate according to channel condition, is considered. A selecting rule is then derived based on the Taylor-type expansion, and when applied to adaptive modulation and coding in the LTE system, reveals new combinations of constellation and coding rate which can improve the system throughput.

Besides its near optimality demonstrated above, jar decoding also has the flexibility to handle bit error probability and code ensembles much more complex than random linear code ensemble or Shannon random code ensemble with a fixed codeword type. In Chapter 5, we show that under jar decoding, the analysis of LDPC codes is much easier compared to that under MAP or ML and BP decoding, and new LDPC coding theorems, which have not been proved under ML or BP decoding to our best knowledge, can be established. Specifically, it is proved that LDPC codes with any variable node degree distribution $L(z^k)$ and check node degree distribution $R(z^k)$ can approach the capacity, with diminishing bit error probability, of any BIMC as k increases. As the assumption of uniform capacity-achieving distribution on channels is not essential to the proof of this coding theorem, it further demonstrates that LDPC codes can approach mutual information between a uniform random variable and its channel response whenever the degrees of the ensemble are large for general binary input memoryless channels. This achievability is very general as no symmetric property is required for channels. Moreover, simulation shows an interesting connection between jar decoding and BP decoding, i.e., BP decoding can be regarded as one of many ways to pick up a codeword from the jar for LDPC codes when it succeeds in outputting a codeword.

The demonstration of flexibility of jar decoding is further extended to interactive information and coding theory in Chapter 6. Specifically, a coding scenario, called interactive encoding and decoding for one way learning, is considered, in which the encoder transmits the source X to the decoder with some side information Y (correlated to X) available to the decoder but unknown to the encoder through a two-way noiseless channel. As can be seen, interactive encoding and decoding distinguishes itself from Slepian-Wolf coding by allowing two-way information flow. Under jar decoding with a dynamic jar, interactive encoding and decoding based on binary LDPC codes with syndrome accumulation (SA-LDPC-IED) is proposed and investigated. Assume that the source alphabet is $\mathbf{GF}(2)$, and the side information alphabet is finite. It is first demonstrated how to convert any classical universal lossless code $\mathcal{C}_n$ (with block length n and side information available to both the encoder and decoder) into a universal SA-LDPC-IED scheme. It is then shown that with the word error

probability approaching 0 sub-exponentially with n, the compression rate (including both the forward and backward rates) of the resulting SA-LDPC-IED scheme is upper bounded by a functional of that of $\mathcal{C}_n$, which in turn approaches the compression rate of $\mathcal{C}_n$ for each and every individual sequence pair (x^n, y^n) and the conditional entropy rate $H(X|Y)$ for any stationary, ergodic source and side information (X, Y) as the average variable node degree $\bar{l}$ of the underlying LDPC code increases without bound. When applied to the class of binary source and side information (X, Y) correlated through a BSC with the crossover probability unknown to either the encoder or decoder, the resulting SA-LDPC-IED scheme can be further simplified, yielding even improved rate performance versus the bit error probability when $\bar{l}$ is not large. Then the interesting connection between jar decoding and BP decoding discovered in Chapter 5 inspires us to implement SA-LDPC-IED schemes by modified BP decoding. And simulation results on binary source-side information pairs confirm the theoretic analysis, and further show that the SA-LDPC-IED scheme consistently outperforms the Slepian-Wolf coding scheme based on the same underlying LDPC code.

Finally, the conclusion of this thesis is drawn and future work is discussed in Chapter 7.

1.4 Definitions, Notations and Conventions

In this thesis, information quantities such as entropy, conditional entropy, mutual information, and divergence (or relative entropy) are measured in nats*, and ln stands for the logarithm with base e. For any set S, we use S^n to denote the set of all sequences of length n drawn from S. Let $|S|$ denotes the cardinality of a finite set S. Let $\mathbb{E}[\cdot]$, $\mathbb{VAR}[\cdot]$, $\mathbb{M}_3[\cdot]$, and $\hat{\mathbb{M}}_3[\cdot]$ be expectation, variance, third absolute central moment, and third central moment operators on random variables respectively. For any two sequences $\{a_i\}_{i=1}^n$ and $\{b_i\}_{i=1}^n$, we write $a_n \sim b_n$ if

$$\lim_{n\to\infty} \frac{a_n}{b_n} = 1 \ .$$

Furthermore, for any positive integer x, define

$$\pi(x) \triangleq \begin{cases} 0 & \text{if } x \text{ is even} \\ 1 & \text{otherwise.} \end{cases} \tag{1.21}$$

*Some exceptions, explicitly mentioned in their context, are seen in figures of simulation results with unit in bits.

As has been defined and used above, $H(\cdot)$, when taking a real number number as the only argument, is the binary entropy function. And define $H^{-1}(\cdot) : [0, \ln 2] \to [0, 0.5]$ as the inverse function of $H(\cdot)$ such that $x = H^{-1}(h)$ if and only if $h = H(x)$ for $x \in [0, 0.5]$ and $h \in [0, \ln 2]$. Moreover, for any set $\mathcal{X}$, $\int_{\mathcal{X}} f(x)dx$ is understood to be summation and integral over $x \in \mathcal{X}$ for discrete and continuous $\mathcal{X}$ respectively, and the subscript $\mathcal{X}$ is dropped when it is clear from context.

The proof of coding theorems via jar decoding in this thesis, especially non-asymptotic coding theorems, relies heavily on non-asymptotic equipartition property (NEP) in Appendix A. In particular, Theorems A.4 (Right NEP with respect to Conditional Entropy) and A.8 (Left NEP with respect to Relative Entropy) are extensively used, and therefore presented together with their related definitions in the next two subsections respectively for easy reference.

1.4.1 Definitions Related to Conditional Entropy

Let $\{p(x)p(y|x) : x \in \mathcal{X}, y \in \mathcal{Y}\}$ be a joint probability distribution where $p(x)$ is a p.m.f for discrete $\mathcal{X}$ and $p(y|x)$ is a p.m.f and p.d.f for discrete and continuous $\mathcal{Y}$ respectively, and (X, Y) be a random variable pair following this distribution. Define

$$\lambda^*(X|Y) \stackrel{\Delta}{=} \sup \left\{ \lambda \geq 0 : \int p(y) \left[\sum_{x \in \mathcal{X}} p^{-\lambda+1}(x|y) \right] dy < \infty \right\}. \tag{1.22}$$

Suppose that

$$\lambda^*(X|Y) > 0\,. \tag{1.23}$$

Define for any $\delta \geq 0$

$$r_{X|Y}(\delta) \stackrel{\Delta}{=} \sup_{\lambda \geq 0} \left[\lambda(H(X|Y) + \delta) - \ln \sum_{x \in \mathcal{X}} \int p(y) p^{-\lambda+1}(x|y) dy \right]. \tag{1.24}$$

For any $\lambda \in [0, \lambda^*(X|Y))$, let X_λ and Y_λ be random variables under joint distribution $p(x, y)f_\lambda(x, y)$ where

$$f_\lambda(x, y) \stackrel{\Delta}{=} \frac{p^{-\lambda}(x|y)}{\sum_{u \in \mathcal{X}} \int p(v) p^{-\lambda+1}(u|v) dv}. \tag{1.25}$$

Further define

$$\delta(\lambda) \stackrel{\Delta}{=} \mathbb{E}[-\ln p(X_\lambda|Y_\lambda)] - H(X|Y) \tag{1.26}$$

$$\Delta^*(X|Y) \triangleq \lim_{\lambda \uparrow \lambda^*(X|Y)} \delta(\lambda) \tag{1.27}$$

$$\sigma_H^2(X|Y,\lambda) \triangleq \mathbb{VAR}[-\ln p(X_\lambda|Y_\lambda)] = \mathbb{E}[|-\ln p(X_\lambda|Y_\lambda) - \mathbb{E}[-\ln p(X_\lambda|Y_\lambda)]|^2] \tag{1.28}$$

$$M_H(X|Y,\lambda) \triangleq \mathbb{M}_3[-\ln p(X_\lambda|Y_\lambda)] = \mathbb{E}[|-\ln p(X_\lambda|Y_\lambda) - \mathbb{E}[-\ln p(X_\lambda|Y_\lambda)]|^3] \tag{1.29}$$

and

$$\hat{M}_H(X|Y,\lambda) \triangleq \hat{\mathbb{M}}_3[-\ln p(X_\lambda|Y_\lambda)] = \mathbb{E}\left[-\ln p(X_\lambda|Y_\lambda) - \mathbb{E}[-\ln p(X_\lambda|Y_\lambda)]\right]^3 \tag{1.30}$$

and write $\hat{M}_H(X|Y,0)$ as $\hat{M}_H(X|Y)$, $M_H(X|Y,0)$ as $M_H(X|Y)$, and $\sigma_H^2(X|Y,0)$ as $\sigma_H^2(X|Y)$. Clearly, $\sigma_H^2(X|Y)$, $M_H(X|Y)$, and $\hat{M}_H(X|Y)$ are the variance, third absolute central moment, and third central moment of $-\ln p(X|Y)$. In particular, $\sigma_H^2(X|Y)$ is referred to as the conditional information variance of X given Y in Appendix A. Assume that

$$\sigma_H^2(X|Y) > 0 \text{ and } M_H(X|Y) = \mathbb{M}_3[-\ln p(X|Y)] < \infty. \tag{1.31}$$

Then it follows from Appendix A that $r_{X|Y}(\delta)$ is strictly increasing, convex, and continuously differentiable up to at least the third order inclusive over $\delta \in [0, \Delta^*(X|Y))$, and furthermore has the following parametric expression

$$r_{X|Y}(\delta(\lambda)) = \lambda(H(X|Y) + \delta(\lambda)) - \ln \sum_{x \in \mathcal{X}} \int p(y) p^{-\lambda+1}(x|y) dy \tag{1.32}$$

with $\delta(\lambda)$ defined in (1.26) and $\lambda = r'_{X|Y}(\delta)$. In addition, let

$$\begin{aligned} \bar{\xi}_H(X|Y,\lambda,n) \triangleq & \frac{2C_{BE} M_H(X|Y,\lambda)}{\sqrt{n}\sigma_H^3(X|Y,\lambda)} \\ & + e^{\frac{n\lambda^2\sigma_H^2(X|Y,\lambda)}{2}} \left[Q\left(\sqrt{n}\lambda\sigma_H(X|Y,\lambda)\right) - Q\left(\rho^* + \sqrt{n}\lambda\sigma_H(X|Y,\lambda)\right)\right] \end{aligned} \tag{1.33}$$

$$\underline{\xi}_H(X|Y,\lambda,n) \triangleq e^{\frac{n\lambda^2\sigma_H^2(X|Y,\lambda)}{2}} Q\left(\rho_* + \sqrt{n}\lambda\sigma_H(X|Y,\lambda)\right) \tag{1.34}$$

with $Q(\rho^*) = \frac{C_{BE} M_H(X|Y,\lambda)}{\sqrt{n}\sigma_H^3(X|Y,\lambda)}$ and $Q(\rho_*) = \frac{1}{2} - \frac{2C_{BE} M_H(X|Y,\lambda)}{\sqrt{n}\sigma_H^3(X|Y,\lambda)}$.

The significance of the above quantities can be seen from Theorem A.4 in A, summarized as below:

Result 1.1. (a) *There exists a $\delta^* > 0$ such that for any $\delta \in (0, \delta^*]$,*

$$r_{X|Y}(\delta) = \frac{1}{2\sigma_H^2(X|Y)}\delta^2 + O(\delta^3). \tag{1.35}$$

(b) *For any $\delta \in (0, \Delta^*(X|Y))$ and any positive integer n*

$$\begin{aligned} \bar{\xi}_H(X|Y,\lambda,n)e^{-nr_{X|Y}(\delta)} &\geq \Pr\left\{-\frac{1}{n}\ln p(X^n|Y^n) > H(X|Y)+\delta\right\} \\ &\geq \underline{\xi}_H(X|Y,\lambda,n)e^{-nr_{X|Y}(\delta)}, \end{aligned} \tag{1.36}$$

where $\lambda = r'_{X|Y}(\delta) > 0$. Moreover, when $\delta = o(1)$ and $\delta = \Omega(1/\sqrt{n})$,

$$\bar{\xi}_H(X|Y,\lambda,n) = e^{\frac{n\lambda^2\sigma_H^2(X|Y,\lambda)}{2}} Q\left(\sqrt{n}\lambda\sigma_H(X|Y,\lambda)\right)(1+o(1)) \tag{1.37}$$

$$\underline{\xi}_H(X|Y,\lambda,n) = e^{\frac{n\lambda^2\sigma_H^2(X|Y,\lambda)}{2}} Q\left(\sqrt{n}\lambda\sigma_H(X|Y,\lambda)\right)(1-o(1)) \tag{1.38}$$

and

$$e^{\frac{n\lambda^2\sigma_H^2(X|Y,\lambda)}{2}} Q\left(\sqrt{n}\lambda\sigma_H(X|Y,\lambda)\right) = \Theta\left(\frac{1}{\sqrt{n}\lambda}\right) \tag{1.39}$$

with $\lambda = r'_X(\delta) = \Theta(\delta)$.

(c) *For any $\delta \leq c\sqrt{\frac{\ln n}{n}}$, where $c < \sigma_H(X|Y)$ is a constant,*

$$\begin{aligned} Q\left(\frac{\delta\sqrt{n}}{\sigma_H(X|Y)}\right) - \frac{C_{BE}M_H(X|Y)}{\sqrt{n}\sigma_H^3(X|Y)} &\leq \Pr\left\{-\frac{1}{n}\ln p(X^n|Y^n) > H(X|Y)+\delta\right\} \\ &\leq Q\left(\frac{\delta\sqrt{n}}{\sigma_H(X|Y)}\right) + \frac{C_{BE}M_H(X|Y)}{\sqrt{n}\sigma_H^3(X|Y)}. \end{aligned} \tag{1.40}$$

where $0 < C_{BE} < 0.4784$ is the universal constant in the Berry-Esseen central limit theorem [16].

1.4.2 Definitions Related to Relative Entropy

Let $\mathcal{P}(\mathcal{X})$ represent the set of all probability distributions on $\mathcal{X}$. For any $t \in \mathcal{P}(\mathcal{X})$, $t(x)$ denotes the probability of x under t. The set of types $\mathcal{P}_n(\mathcal{X})$ is the subset of $\mathcal{P}(\mathcal{X})$ such that $t \in \mathcal{P}_n(\mathcal{X})$ if and only if $t(x)n$ is an integer for any $x \in \mathcal{X}$. And for any $t \in \mathcal{P}_n(\mathcal{X})$, let $\mathcal{T}_t^n \subset \mathcal{X}^n$ be the set of sequences with empirical distribution t. Moreover, let $\{p(y|x) : x \in \mathcal{X}, y \in \mathcal{Y}\}$ be a conditional probability distribution (p.m.f and p.d.f for discrete and continuous $\mathcal{Y}$ respectively).

For any $t \in \mathcal{P}$, define

$$H(t) \triangleq \sum_{x\in\mathcal{X}} -t(x)\ln t(x) \tag{1.41}$$

$$D(t,x) \stackrel{\Delta}{=} \int p(y|x) \ln \frac{p(y|x)}{q_t(y)} dy \tag{1.42}$$

$$I(t;P) \stackrel{\Delta}{=} \sum_{x \in \mathcal{X}} t(x) \int p(y|x) \ln \frac{p(y|x)}{q_t(y)} dy \tag{1.43}$$

where

$$q_t(y) \stackrel{\Delta}{=} \sum_{x \in \mathcal{X}} t(x) p(y|x) \tag{1.44}$$

$$q_t(y^n) \stackrel{\Delta}{=} \prod_{i=1}^{n} q_t(y_i), \tag{1.45}$$

and

$$\lambda_-^*(t;P) \stackrel{\Delta}{=} \sup \left\{ \lambda \geq 0 : \sum_{a \in \mathcal{X}} t(a) \int p(y|a) \left[\frac{p(y|a)}{q_t(y)} \right]^{-\lambda} dy < \infty \right\}. \tag{1.46}$$

It is easy to see that $\lambda_-^*(t;P)$ is the same for all $t \in \mathcal{P}$ with the same support set $\{a \in \mathcal{X} : t(a) > 0\}$. Suppose that

$$\lambda_-^*(t;P) > 0. \tag{1.47}$$

Define for any $t \in \mathcal{P}$ and any $\delta \geq 0$

$$r_-(t,\delta) \stackrel{\Delta}{=} \sup_{\lambda \geq 0} \left[\lambda(\delta - I(t;P)) - \sum_{x \in \mathcal{X}} t(x) \ln \int p(y|x) \left[\frac{p(y|x)}{q_t(y)} \right]^{-\lambda} dy \right] \tag{1.48}$$

and for any $t \in \mathcal{P}$ and any $\lambda \in [0, \lambda_-^*(t;P))$, random variables X_t and $Y_{t,\lambda}$ with joint distribution $t(x)p(y|x)f_{-\lambda}(y|x)$ where

$$f_{-\lambda}(y|x) \stackrel{\Delta}{=} \frac{\left[\frac{p(y|x)}{q_t(y)} \right]^{-\lambda}}{\int p(v|x) \left[\frac{p(v|x)}{q_t(v)} \right]^{-\lambda} dv}. \tag{1.49}$$

Then define

$$D(t,x,\lambda) \stackrel{\Delta}{=} \mathbb{E}\left[\ln \frac{p(Y_{t,\lambda}|X_t)}{q_t(Y_{t,\lambda})} \middle| X_t = x \right] \tag{1.50}$$

$$\delta_-(t,\lambda) \stackrel{\Delta}{=} \mathbb{E}\left[-\ln \frac{p(Y_{t,\lambda}|X_t)}{q_t(Y_{t,\lambda})} \right] + I(t;P) \tag{1.51}$$

$$\Delta_-^*(t) \stackrel{\Delta}{=} \lim_{\lambda \uparrow \lambda_-^*(t;P)} \delta_-(t,\lambda) \tag{1.52}$$

$$\sigma^2_{D,-}(t;P,\lambda) \stackrel{\Delta}{=}\mathbb{E}\left\{\mathbb{VAR}\left[\ln\frac{p(Y_{t,\lambda}|X_t)}{q_t(Y_{t,\lambda})}\middle| X_t\right]\right\} = \sum_{x\in\mathcal{X}} t(x)\mathbb{VAR}\left[\ln\frac{p(Y_{t,\lambda}|X_t)}{q_t(Y_{t,\lambda})}\middle| X_t = x\right] \tag{1.53}$$

$$M_{D,-}(t;P,\lambda) \stackrel{\Delta}{=}\mathbb{E}\left\{\mathbb{M}_3\left[\ln\frac{p(Y_{t,\lambda}|X_t)}{q_t(Y_{t,\lambda})}\middle| X_t\right]\right\} = \sum_{x\in\mathcal{X}} t(x)\mathbb{M}_3\left[\ln\frac{p(Y_{t,\lambda}|X_t)}{q_t(Y_{t,\lambda})}\middle| X_t = x\right] \tag{1.54}$$

and

$$\hat{M}_{D,-}(t;P,\lambda) \stackrel{\Delta}{=}\mathbb{E}\left\{\hat{\mathbb{M}}_3\left[\ln\frac{p(Y_{t,\lambda}|X_t)}{q_t(Y_{t,\lambda})}\middle| X_t\right]\right\} = \sum_{x\in\mathcal{X}} t(x)\hat{\mathbb{M}}_3\left[\ln\frac{p(Y_{t,\lambda}|X_t)}{q_t(Y_{t,\lambda})}\middle| X_t = x\right]. \tag{1.55}$$

Note that $\sigma^2_{D,-}(t;P,\lambda)$, $M_{D,-}(t;P,\lambda)$, and $\hat{M}_{D,-}(t;P,\lambda)$ are respectively the conditional variance, conditional third absolute central moment, and conditional third central moment of $\ln\frac{p(Y_{t,\lambda}|X_t)}{q_t(Y_{t,\lambda})}$ given X_t. Write $\sigma^2_{D,-}(t;P,0)$ simply as $\sigma^2_D(t;P)$, $M_{D,-}(t;P,0)$ as $M_D(t;P)$, and $\hat{M}_{D,-}(t;P,0)$ as $\hat{M}_D(t;P)$. Assume that

$$\sigma^2_D(t;P) > 0 \text{ and } M_D(t;P) < \infty. \tag{1.56}$$

Furthermore $r_-(t,\delta)$ has the following parametric expression

$$r_-(t,\delta_-(t,\lambda)) = \lambda(\delta_-(t,\lambda) - I(t;P)) - \sum_{x\in\mathcal{X}} t(x)\ln\int p(y|x)\left[\frac{p(y|x)}{q_t(y)}\right]^{-\lambda} dy \tag{1.57}$$

with $\lambda = \frac{\partial r_-(t,\delta)}{\partial\delta}$ satisfying $\delta_-(t,\lambda) = \delta$. In addition, let

$$\begin{aligned}\bar{\xi}_{D,-}(t;P,\lambda,n) \stackrel{\Delta}{=}& \frac{2C_{BE}M_{\mathrm{D},-}(t;P,\lambda)}{\sqrt{n}\sigma^3_{\mathrm{D},-}(t;P,\lambda)} \\ &+ e^{\frac{n\lambda^2\sigma^2_{D,-}(t;P,\lambda)}{2}}\left[Q(\sqrt{n}\lambda\sigma_{D,-}(t;P,\lambda)) - Q(\rho^* + \sqrt{n}\lambda\sigma_{D,-}(t;P,\lambda))\right] \qquad (1.58)\\ \underline{\xi}_{D,-}(t;P,\lambda,n) \stackrel{\Delta}{=}& e^{\frac{n\lambda^2\sigma^2_{D,-}(t;P,\lambda)}{2}}Q(\rho_* + \sqrt{n}\lambda\sigma_{D,-}(t;P,\lambda)) \qquad (1.59)\end{aligned}$$

with $Q(\rho^*) = \frac{C_{BE}M_{\mathrm{D},-}(t;P,\lambda)}{\sqrt{n}\sigma^3_{\mathrm{D},-}(t;P,\lambda)}$ and $Q(\rho_*) = \frac{1}{2} - \frac{2C_{BE}M_{\mathrm{D},-}(t;P,\lambda)}{\sqrt{n}\sigma^3_{\mathrm{D},-}(t;P,\lambda)}$.

Similar to the previous subsection, the purpose of introducing above definitions is to present the following result extensively used in this thesis, proved as Theorem A.8 in Appendix A, and valid for any $t \in \mathcal{P}_n$ satisfying (1.47) and (1.56).

Result 1.2. **(a)** *There exists a $\delta^* > 0$ such that for any $\delta \in (0, \delta^*]$*

$$r_-(t,\delta) = \frac{1}{2\sigma_D^2(t;P)}\delta^2 + O(\delta^3). \tag{1.60}$$

(b) *For any $\delta \in (0, \Delta_-^*(t))$, and any $x^n \in \mathcal{T}_t^n$,*

$$\begin{aligned} \underline{\xi}_{D,-}(t;P,\lambda,n)e^{-nr_-(t,\delta)} &\geq \Pr\left\{\frac{1}{n}\ln\frac{p(Y^n|X^n)}{q_t(Y^n)} \leq I(t;P) - \delta \middle| X^n = x^n\right\} \\ &\geq \underline{\xi}_{D,-}(t;P,\lambda,n)e^{-nr_-(t,\delta)} \end{aligned} \tag{1.61}$$

where $\lambda = \frac{\partial r_-(t,\delta)}{\partial \delta} > 0$, and $Y^n = Y_1Y_2\cdots Y_n$ is an independently distributed sequence with Y_i following the distribution $p(y_i|x_i)$. Moreover, when $\delta = o(1)$ and $\delta = \Omega(1/\sqrt{n})$,

$$\bar{\xi}_{D,-}(t;P,\lambda,n) = e^{\frac{n\lambda^2\sigma_{D,-}^2(t;P,\lambda)}{2}}Q\left(\sqrt{n}\lambda\sigma_{D,-}(t;P,\lambda)\right)(1+o(1)) \tag{1.62}$$

$$\underline{\xi}_{D,-}(t;P,\lambda,n) = e^{\frac{n\lambda^2\sigma_{D,-}^2(t;P,\lambda)}{2}}Q\left(\sqrt{n}\lambda\sigma_{D,-}(t;P,\lambda)\right)(1-o(1)) \tag{1.63}$$

and

$$e^{\frac{n\lambda^2\sigma_{D,-}^2(t;P,\lambda)}{2}}Q\left(\sqrt{n}\lambda\sigma_{D,-}(t;P,\lambda)\right) = \Theta\left(\frac{1}{\sqrt{n}\lambda}\right) \tag{1.64}$$

with $\lambda = r_X'(\delta) = \Theta(\delta)$.

(c) *For any $\delta \leq c\sqrt{\frac{\ln n}{n}}$, where $c < \sigma_D(t;P)$ is a constant, and $x^n \in \mathcal{X}_t^n$,*

$$\begin{aligned} Q\left(\frac{\delta\sqrt{n}}{\sigma_D(t;P)}\right) - \frac{C_{BE}M_D(t;P)}{\sqrt{n}\sigma_D^3(t;P)} &\leq \Pr\left\{\frac{1}{n}\ln\frac{p(Y^n|X^n)}{q_t(Y^n)} \leq I(t;P) - \delta \middle| X^n = x^n\right\} \\ &\leq Q\left(\frac{\delta\sqrt{n}}{\sigma_D(t;P)}\right) + \frac{C_{BE}M_D(t;P)}{\sqrt{n}\sigma_D^3(t;P)}. \end{aligned} \tag{1.65}$$

where $0 < C_{BE} < 0.56$ is the universal constant in the Berry-Esseen central limit theorem [17].

Chapter 2

Non-asymptotic Achievable Channel Coding Theorems

2.1 Non-asymptotic Linear Coding Theorem: BSC

In this section, we demonstrate how to use jar decoding to establish non-asymptotic coding results for random linear codes of block length n based on either Elias' generator ensemble or Gallager's parity check ensemble for the BSC.

Let $\mathfrak{C}_{n,k}$ be a linear code with block length n and with generator matrix $\mathbf{G}_{k\times n}$ or parity check matrix $\mathbf{H}_{(n-k)\times n}$. Assuming codewords are ordered in some manner, we shall refer to the q-th codeword in $\mathfrak{C}_{n,k}$ as $x^n(q)$. We say $\mathbf{H}_{(n-k)\times n}$ ($\mathbf{G}_{k\times n}$, respectively) is randomly picked from Gallager's parity check ensemble $\mathcal{H}_{n,k}$ (Elias' generator ensemble $\mathcal{G}_{n,k}$, respectively) if entries of $\mathbf{H}_{(n-k)\times n}$ ($\mathbf{G}_{k\times n}$, respectively) are independently and uniformly generated from $\mathcal{X} = \{0, 1\}$. Denote the ensemble of linear codes with their generator matrices from $\mathcal{G}_{n,k}$ by $\mathcal{C}_{n,k}^{(1)}$, and the ensemble of linear codes with their parity check matrices from $\mathcal{H}_{n,k}$ by $\mathcal{C}_{n,k}^{(2)}$. To facilitate our subsequent discussion, we also specify the encoding procedure (i.e. the mapping from messages to codewords) of $\mathcal{C}_{n,k}^{(1)}$ and $\mathcal{C}_{n,k}^{(2)}$:

$\mathcal{C}_{n,k}^{(1)}$: Given $\mathbf{G}_{k\times n}$, $x^n(q) = b(q)\mathbf{G}_{k\times n}$ where $b(q)$ is the binary representation of q using k bits for $0 \le q \le 2^k - 1$;

$\mathcal{C}_{n,k}^{(2)}$: Given $\mathbf{H}_{(n-k)\times n}$, $x^n(q)$ is the q-th vector in the null space of $\mathbf{H}_{(n-k)\times n}$ by lexicographical order for $0 \le q \le 2^{n-rank(\mathbf{H}_{(n-k)\times n})} - 1$.

By convention, we assume that all messages are equally likely. With slight abuse of notation, we shall use q to represent both the uniformly distributed random message and its specific realization; its exact meaning, however, will be clear from the context. Note that all codes in $\mathcal{C}_{n,k}^{(1)}$ and $\mathcal{C}_{n,k}^{(2)}$ have the channel coding rate greater than or equal to $\mathcal{R}(\mathcal{C}_{n,k}) \stackrel{\Delta}{=} \frac{k}{n} \ln 2$ (in nats).

Select δ in the Hamming jar (1.7) such that $p + \delta < 0.5$. Then we have the following non-asymptotic coding result with jar decoding.

Theorem 2.1. *Let $P_e(\mathcal{C}_{n,k}^{(i)})$, $i = 1, 2$, denote the average word error probability (under jar decoding) of $\mathcal{C}_{n,k}^{(i)}$ with respect to the random message q, the BSC, and the random linear code $\mathcal{C}_{n,k}^{(i)}$ itself. Then for any block length n, $i = 1, 2$ and any $\delta > 0$ with $p + \delta < 0.5$,*

$$P_e(\mathcal{C}_{n,k}^{(i)}) \leq \Pr\left\{\frac{1}{n} wt(W^n) > p + \delta\right\} + e^{-n\left(\ln 2 - \mathcal{R}(\mathcal{C}_{n,k})\right)} \sum_{0 \leq w \leq n(p+\delta)} \binom{n}{w} \tag{2.1}$$

where W^n is an i.i.d binary sequence with $\Pr\{W_1 = 1\} = p$. Moreover, for any block length $n$and $i = 1, 2$, the following hold:

1) For any $\delta > 0$ with $p + \delta < 0.5$

$$P_e(\mathcal{C}_{n,k}^{(i)}) \leq \left(1 + \frac{1}{\sqrt{n}}\right) e^{-nD(p+\delta||p)} \tag{2.2}$$

whenever

$$\mathcal{R}(\mathcal{C}_{n,k}) \leq C_{\text{BSC}} - (H(p+\delta) - H(p) + D(p+\delta||p)) - \frac{\ln n}{2n} \tag{2.3}$$

where

$$D(p+\delta||p) = (p+\delta) \ln \frac{p+\delta}{p} + (1-p-\delta) \ln \frac{1-p-\delta}{1-p}$$

is the divergence between $(p+\delta, 1-p-\delta)$ and $(p, 1-p)$.

2) For any $\alpha \geq 0.5$

$$P_e(\mathcal{C}_{n,k}^{(i)}) \leq n^{-\alpha} + O\left(n^{-\alpha} \frac{\ln^{3/2} n}{\sqrt{n}}\right) \tag{2.4}$$

whenever

$$\mathcal{R}(\mathcal{C}_{n,k}) \leq C_{\text{BSC}} - \left[\ln \frac{1-p}{p}\right] \sqrt{\frac{2p(1-p)\alpha \ln n}{n}} - O\left(\frac{\ln n}{n}\right). \tag{2.5}$$

3) For any real number c

$$P_e(\mathcal{C}_{n,k}^{(i)}) \le Q\left(\frac{c}{\sqrt{p(1-p)}\ln\frac{1-p}{p}}\right) + \frac{(1-p)^2+p^2}{\sqrt{p(1-p)}}\frac{1}{\sqrt{n}} \tag{2.6}$$

whenever

$$\mathcal{R}(\mathcal{C}_{n,k}) \le C_{\rm BSC} - \frac{c}{\sqrt{n}} - \frac{\ln n}{2n} + \frac{1}{n}\ln\frac{(1-C_{BE})((1-p)^2+p^2)}{\sqrt{p(1-p)}}. \tag{2.7}$$

Proof. For any linear block code $\mathfrak{C}_{n,k}$, we use $x^n \in \mathfrak{C}_{n,k}$ to represent that x^n is a codeword of $\mathfrak{C}_{n,k}$. It is not hard to see that for any $x^n \neq 0$,

$$\begin{aligned}
\Pr\left\{x^n \in \mathcal{C}_{n,k}^{(1)}\right\} &= \Pr\left\{\exists q \neq 0, b(q)\mathbf{G}_{k\times n} = x^n\right\} \\
&\le \sum_{q=1}^{2^k-1} \Pr\{b(q)\mathbf{G}_{k\times n} = x^n\} \\
&< 2^k 2^{-n} = 2^{-(n-k)} = e^{-(n-k)\ln 2} = e^{-n(\ln 2 - \mathcal{R}(\mathcal{C}_{n,k}))}
\end{aligned} \tag{2.8}$$

and

$$\Pr\left\{x^n \in \mathcal{C}_{n,k}^{(2)}\right\} = \Pr\left\{\mathbf{H}_{(n-k)\times n}x^n = 0^k\right\} = 2^{-(n-k)} = e^{-(n-k)\ln 2} = e^{-n(\ln 2 - \mathcal{R}(\mathcal{C}_{n,k}))}\ . \tag{2.9}$$

Now let

$$Y^n = X^n(q) + W^n$$

where W^n is the noise vector in the BSC, and the addition above is the binary addition. Note that Y^n is simply the output of the BSC in response to the transmitted codeword $X^n(q)$. From the description of jar decoding, we have

$$\begin{aligned}
P_e(\mathcal{C}_{n,k}^{(i)}) &\le \Pr\{X^n(q) \notin J(Y^n)\} \\
&\quad + \Pr\left\{\exists x^n \neq X^n(q), x^n \in J(Y^n), x^n \in \mathcal{C}_{n,k}^{(i)}, X^n(q) \in J(Y^n)\right\}
\end{aligned} \tag{2.10}$$

We next upper bound each term on the right side of (2.10). First we can verify that

$$\begin{aligned}
&\Pr\left\{\exists x^n \neq X^n(q), x^n \in J(Y^n), x^n \in \mathcal{C}_{n,k}^{(i)}, X^n(q) \in J(Y^n)\right\} \\
&\overset{1)}{\leq} \Pr\left\{\exists x^n \neq X^n(q), x^n \in J(X^n(q)+W^n), x^n - X^n(q) \in \mathcal{C}_{n,k}^{(i)}\right\} \\
&\overset{2)}{=} \Pr\left\{\exists x^n \neq X^n(q), x^n - X^n(q) \in J(W^n), x^n - X^n(q) \in \mathcal{C}_{n,k}^{(i)}\right\} \\
&= \Pr\left\{\exists z^n \neq 0, z^n \in J(W^n), z^n \in \mathcal{C}_{n,k}^{(i)}\right\} \\
&\overset{3)}{=} \sum_{w^n \in \mathcal{Y}^n} \Pr\{W^n = w^n\} \Pr\left\{\exists z^n \neq 0, z^n \in J(w^n), z^n \in \mathcal{C}_{n,k}^{(i)}\right\} \\
&\overset{4)}{\leq} \sum_{w^n \in \mathcal{Y}^n} \Pr\{W^n = w^n\} e^{-n(\ln 2 - \mathcal{R}(\mathcal{C}_{n,k}))} |J(w^n)| \\
&\leq e^{-n(\ln 2 - \mathcal{R}(\mathcal{C}_{n,k}))} \sum_{0 \leq w \leq n(p+\delta)} \binom{n}{w}
\end{aligned} \tag{2.11}$$

where the inequality 1) is due to the linearity of $\mathcal{C}_{n,k}^{(i)}$, the equality 2) follows from the Hamming jar definition in (1.7), the equality 3) is attributable to the fact that W^n and $\mathcal{C}_{n,k}^{(i)}$ are independent, the inequality 4) follows from (2.8) and (2.9), and finally, the last inequality is due to the jar size discussed in Example 1. On the other hand, it follows from (1.7) again that

$$\Pr\{X^n(q) \notin J(Y^n)\} = \Pr\left\{\frac{1}{n} wt(W^n) > p + \delta\right\} \tag{2.12}$$

which, coupled with (2.10) and (2.11), implies

$$P_e(\mathcal{C}_{n,k}^{(i)}) \leq \Pr\left\{\frac{1}{n} wt(W^n) > p + \delta\right\} + e^{-n(\ln 2 - \mathcal{R}(\mathcal{C}_{n,k}))} \sum_{0 \leq w \leq n(p+\delta)} \binom{n}{w}, \tag{2.13}$$

and consequently, (2.1) is proved.

Now applying the upper bound

$$\sum_{0 \leq w \leq n(p+\delta)} \binom{n}{w} \leq e^{nH(p+\delta)} \tag{2.14}$$

to (2.13) yields

$$P_e(\mathcal{C}_{n,k}^{(i)}) \leq \Pr\left\{\frac{1}{n} wt(W^n) > p + \delta\right\} + e^{-n\left(C_{\mathrm{BSC}} - (H(p+\delta) - H(p)) - \mathcal{R}(\mathcal{C}_{n,k})\right)} \tag{2.15}$$

where $C_{\rm BSC} = \ln 2 - H(p)$. The inequalities (2.2) to (2.7) can now be established by applying different bounds to (2.12) for different scales of δ. Applying Chernoff-Hoeffding's inequality to (2.12) yields

$$\Pr\left\{\frac{1}{n}wt(W^n) > p+\delta\right\} \le e^{-nD(p+\delta||p)}$$

which, combined with (2.15), implies (2.2) and (2.3).

Note that (2.2) and (2.3) are valid for any $\delta > 0$ with $p + \delta < 0.5$. By letting $\delta = \sqrt{\frac{2p(1-p)\alpha \ln n}{n}}$ in (2.2) and (2.3), it is not hard to see that (2.4) and (2.5) then follow from the facts that

$$D(p+\delta||p) = \frac{1}{2p(1-p)}\delta^2 + O\left(\delta^3\right)$$

and

$$H\left(p+\delta\right) - H(p) \le \left(\ln\frac{1-p}{p}\right)\delta.$$

Finally, letting $\delta = \frac{c}{\sqrt{n}\log_2\frac{1-p}{p}}$, and applying the central limit theorem of Berry and Esseen to (2.12) yields

$$\begin{aligned}
&\Pr\left\{\frac{1}{n}wt(W^n) > p + \frac{c}{\sqrt{n}\ln\frac{1-p}{p}}\right\} \\
&= \Pr\left\{\frac{1}{\sqrt{n}}\sum_{i=1}^{n}(wt(W_i)-p) > \frac{c}{\ln\frac{1-p}{p}}\right\} \\
&\le Q\left(\frac{c}{\sqrt{p(1-p)}\ln\frac{1-p}{p}}\right) + \frac{C_{BE}((1-p)^2+p^2)}{\sqrt{p(1-p)}}\frac{1}{\sqrt{n}}\,.
\end{aligned}$$

Then (2.6) follows from the fact that

$$\begin{aligned}
e^{-n\left(C_{\rm BSC}-\left(H\left(p+\frac{c}{\sqrt{n}\log_2\frac{1-p}{p}}\right)-H(p)\right)-\mathcal{R}(\mathcal{C}_{n,k})\right)} &\le e^{-n\left(C_{\rm BSC}-\frac{c}{\sqrt{n}}-\mathcal{R}(\mathcal{C}_{n,k})\right)} \\
&= \frac{(1-C_{BE})(1-p)^2+p^2}{\sqrt{p(1-p)}}\frac{1}{\sqrt{n}}
\end{aligned}$$

whenever (2.7) holds. This completes the proof of Theorem 2.1. □

Remark 2.1. *The inequalities (2.4) to (2.7) show that linear block codes of block length n can reach within*

$$\left[\ln\frac{1-p}{p}\right]\sqrt{\frac{2p(1-p)\alpha\ln n}{n}}+O\left(\frac{\ln n}{n}\right)$$

of the capacity of the BSC while maintaining the word error probability

$$n^{-\alpha}+O\left(n^{-\alpha}\frac{\ln^{3/2} n}{\sqrt{n}}\right),$$

and within

$$\frac{c}{\sqrt{n}}+\frac{\ln n}{2n}-\frac{1}{n}\ln\frac{(1-C_{BE})((1-p)^2+p^2)}{\sqrt{p(1-p)}}$$

of the capacity while maintaining the word error probability

$$Q\left(\frac{c}{\sqrt{p(1-p)}\ln\frac{1-p}{p}}\right)+\frac{(1-p)^2+p^2}{\sqrt{p(1-p)}}\frac{1}{\sqrt{n}}.$$

If the word error probability is kept slightly above 0.5*, the code rate can be even slightly above the capacity! Figure 2.1 shows the tradeoff between the word error probability and*

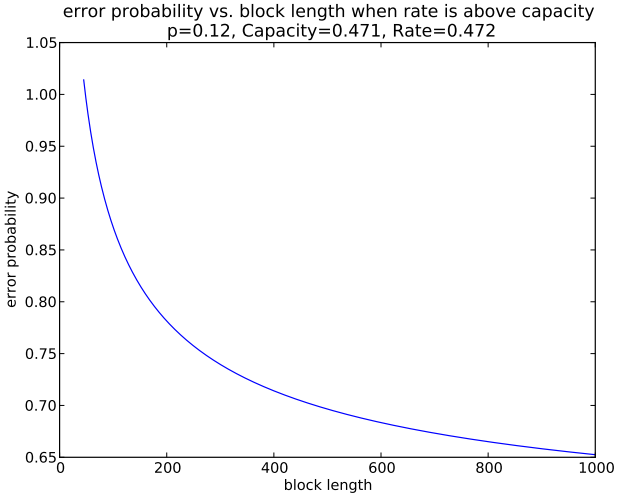


Figure 2.1: Tradeoff between the word error probability and block length when the code rate is above the capacity with $p = 0.12$.

block length when the code rate is 0.21% *above the capacity with* $p = 0.12$*, where in Figure 2.1, both the capacity and code rate are expressed in terms of bits. As can be seen from Figure 2.1, at the block length* 1000*, the word error probability is around* 0.65*, and the code rate is* 0.21% *above the capacity!*

Remark 2.2. *The bounds (2.2) and (2.3) are further improved in Theorem 2.2.*

2.2 Non-asymptotic Linear Coding Theorem: BIMC

In this section, we extend Theorem 2.1 to the case of BIMC. Consider an arbitrary BIMC $\{p(y|x) : x \in \mathcal{X}, y \in \mathcal{Y}\}$ with $\mathcal{X} = \{0, 1\}$. As discussed in Section 1.2, its capacity is equal to

$$C_{\text{BIMC}} = \ln 2 - H(X|Y)$$

where X is the uniform input random variable, and Y is the corresponding output of the BIMC. Let $p(y)$ be the pmf or pdf (as the case may be) of Y, and $p(x|y)$ the conditional pmf of X given by Y. It is easy to see that

$$p(y) = \frac{1}{2}[p(y|0) + p(y|1)]$$

and

$$p(x|y) = \frac{p(y|x)}{p(y|0) + p(y|1)} \ .$$

Recall definitions in Section 1.4.1, and further define

$$\begin{aligned}\zeta_H(X|Y, \lambda, n) \triangleq & \frac{2M_H(X|Y, \lambda)}{\sqrt{n}\sigma_H^3(X|Y, \lambda)} \\ & + e^{\frac{n\lambda^2\sigma_H^2(X|Y,\lambda)}{2}} \left[Q(\sqrt{n}\lambda\sigma_H(X|Y, \lambda)) - Q(\rho^* + \sqrt{n}\lambda\sigma_H(X|Y, \lambda))\right]\end{aligned}$$

where $Q(\rho^*) = \frac{C_{BE}M_H(X|Y,\lambda)}{\sqrt{n}\sigma_H^3(X|Y,\lambda)}$.

Puncture 0 from the message space and ignore the insignificant effect on the rate. With the BIMC jar specified in (1.9), we have the following non-asymptotic coding theorem with jar decoding.

Theorem 2.2. *Given a BIMC with* $C_{\text{BIMC}} \in (0, 1)$*, let* $P_e(\mathcal{C}_{n,k}^{(i)})$*,* $i = 1, 2$*, denote the average word error probability (under jar decoding) of* $\mathcal{C}_{n,k}^{(i)}$ *with respect to the random message* q*,*

the BIMC, and the random linear code $\mathcal{C}_{n,k}^{(i)}$ itself. Then for any block length n, $i = 1, 2$ and any $\delta \in (0, \Delta^*(X|Y))$,

$$P_e(\mathcal{C}_{n,k}^{(i)}) \leq C^{(i)} \Pr\left\{-\frac{1}{n}\sum_{i=1}^{n} \ln p(X_i|Z_i) > H(X|Y) + \delta\right\} + e^{-n\left(C_{\text{BIMC}} - \delta - \mathcal{R}(\mathcal{C}_{n,k})\right)} \tag{2.16}$$

where X^n is an independently, identically and uniformly distributed binary sequence, Z^n is the output of BIMC in response to X^n, and

$$C^{(i)} = \begin{cases} 1 & \text{if } i = 1 \\ \frac{1}{1-2^{-n}} & \text{otherwise.} \end{cases} \tag{2.17}$$

Moreover, for any block length n and $i = 1, 2$, the following hold:

1) For any $\delta \in (0, \Delta^*(X|Y))$

$$P_e(\mathcal{C}_{n,k}^{(i)}) \leq C^{(i)} \zeta_H(X|Y, \lambda, n) e^{-n r_{X|Y}(\delta)} \tag{2.18}$$

whenever

$$\mathcal{R}(\mathcal{C}_{n,k}) \leq C_{\text{BIMC}} - \delta - r_{X|Y}(\delta) + \frac{\ln \frac{2(1-C_{BE}) M_H(X|Y,\lambda)}{\sqrt{n}\sigma_H^3(X|Y,\lambda)}}{n} \tag{2.19}$$

where $\lambda = r'_{X|Y}(\delta)$.

2) For any $\alpha \geq 0.5$

$$P_e(\mathcal{C}_{n,k}^{(i)}) \leq \frac{C^{(i)} n^{-\alpha}}{2\sqrt{\pi \alpha \ln n}} + O\left(n^{-\alpha} \frac{\ln^{3/2} n}{\sqrt{n}}\right) \tag{2.20}$$

whenever

$$\mathcal{R}(\mathcal{C}_{n,k}) \leq C_{\text{BIMC}} - \sigma_H(X|Y)\sqrt{\frac{2\alpha \ln n}{n}} - \left(\alpha + \frac{1}{2}\right)\frac{\ln n}{n} - O\left(\frac{\ln \ln n}{n}\right). \tag{2.21}$$

3) For any real number c

$$P_e(\mathcal{C}_{n,k}^{(i)}) \leq C^{(i)} \left(Q\left(\frac{c}{\sigma_H(X|Y)}\right) + \frac{M_H(X|Y)}{\sigma_H^3(X|Y)} \frac{1}{\sqrt{n}}\right) \tag{2.22}$$

whenever

$$\mathcal{R}(\mathcal{C}_{n,k}) \leq C_{\text{BIMC}} - \frac{c}{\sqrt{n}} - \frac{\ln n}{2n} + \frac{1}{n} \ln \frac{C^{(i)}(1 - C_{BE}) M_H(X|Y)}{\sigma_H^3(X|Y)}. \tag{2.23}$$

Proof. Recall the encoding procedure of $\mathcal{C}_{n,k}^{(i)}$, $i = 1, 2$. Let $X^n(q)$ be the transmitted codeword, where q is distributed uniformly over the punctured message space with message 0 deleted. Let Y^n be the output of the BIMC in response to $X^n(q)$. In parallel with (2.8) and (2.9), it is not hard to verify that for any $z^n \neq x^n \in \mathcal{X}^n$,

$$\Pr\left\{ z^n \in \mathcal{C}_{n,k}^{(1)} \middle| X^n(q) = x^n \right\} < 2^k 2^{-n} = e^{-(n-k)\ln 2} \tag{2.24}$$

and

$$\Pr\left\{ z^n \in \mathcal{C}_{n,k}^{(2)} \middle| X^n(q) = x^n \right\} = 2^{-(n-k)} = e^{-(n-k)\ln 2} \,. \tag{2.25}$$

Similarly, in parallel with (2.10), we have

$$\begin{aligned} P_e(\mathcal{C}_{n,k}^{(i)}) &\leq \Pr\{X^n(q) \notin J(Y^n)\} \\ &\quad + \Pr\left\{ \exists z^n \neq X^n(q), z^n \in J(Y^n), z^n \in \mathcal{C}_{n,k}^{(i)}, X^n(q) \in J(Y^n) \right\} \\ &\leq \Pr\{X^n(q) \notin J(Y^n)\} + \Pr\left\{ \exists z^n \neq X^n(q), z^n \in J(Y^n), z^n \in \mathcal{C}_{n,k}^{(i)} \right\} \end{aligned} \tag{2.26}$$

where $J(Y^n)$ is the BIMC jar for Y^n. For any $x^n \in \mathcal{X}^n$ and $y^n \in \mathcal{Y}^n$, one can verify that

$$\begin{aligned} &\Pr\left\{ \exists z^n \neq X^n(q), z^n \in J(Y^n), z^n \in \mathcal{C}_{n,k}^{(i)} \middle| X^n(q) = x^n, Y^n = y^n \right\} \\ &= \Pr\left\{ \exists z^n \neq x^n, z^n \in J(y^n), z^n \in \mathcal{C}_{n,k}^{(i)} \middle| X^n(q) = x^n, Y^n = y^n \right\} \\ &\overset{1)}{\leq} \sum_{z^n \in J(y^n), z^n \neq x^n} \Pr\left\{ z^n \in \mathcal{C}_{n,k}^{(i)} \middle| X^n(q) = x^n \right\} \\ &\overset{2)}{\leq} |J(y^n)| e^{-(n-k)\ln 2} \\ &\leq e^{n(H(X|Y)+\delta)} e^{-(n-k)\ln 2} = e^{-n\left(C_{\mathrm{BIMC}} - \delta - \mathcal{R}(\mathcal{C}_{n,k})\right)} \end{aligned} \tag{2.27}$$

where the inequality 1) follows from the fact that given $X^n(q)$, Y^n and $\mathcal{C}_{n,k}^{(i)}$ are conditionally independent, the inequality 2) is due to (2.24) and (2.25), and finally the last inequality above is attributable to the upper bound on the size of the jar $J(y^n)$ in (1.10). Since (2.27) is valid for any $x^n \in \mathcal{X}^n$ and $y^n \in \mathcal{Y}^n$, it follows that

$$\Pr\left\{ \exists z^n \neq X^n(q), z^n \in J(Y^n), z^n \in \mathcal{C}_{n,k}^{(i)} \right\} \leq e^{-n\left(C_{\mathrm{BIMC}} - \delta - \mathcal{R}(\mathcal{C}_{n,k})\right)} \,. \tag{2.28}$$

To continue, let $X^n = X_1 X_2 \cdots X_n$ be a random variable taking values uniformly over $\mathcal{X}^n$. Let $Z^n = Z_1 Z_2 \cdots Z_n$ be the output of the BIMC in response to X^n. For the random

code $\mathcal{C}_{n,k}^{(1)}$, it is easy to see that $X^n(q)$ and X^n have the same distribution. So do $(X^n(q), Y^n)$ and (X^n, Z^n). Therefore, for $\mathcal{C}_{n,k}^{(1)}$, we have

$$\Pr\{X^n(q) \notin J(Y^n)\} = \Pr\{X^n \notin J(Z^n)\} \,. \tag{2.29}$$

For $\mathcal{C}_{n,k}^{(2)}$, one can verify that for any $x^n, x'^n \in \mathcal{X}^n/\{0^n\}$,

$$\begin{aligned}
\Pr\{X^n(q) = x^n\} &= \sum_{\mathbf{H}_{(n-k)\times n}:\mathbf{H}_{(n-k)\times n}x^n=0^{n-k}} \frac{2^{-(n-k)n}}{2^{(n-rank(\mathbf{H}_{(n-k)\times n}))}-1} \\
&= \sum_{\mathbf{H}_{(n-k)\times n}:\mathbf{H}_{(n-k)\times n}\mathbf{K}_{n\times n}x'^n=0^{n-k}} \frac{2^{-(n-k)n}}{2^{(n-rank(\mathbf{H}_{(n-k)\times n}))}-1} \\
&= \sum_{\mathbf{H}_{(n-k)\times n}:\mathbf{H}_{(n-k)\times n}\mathbf{K}_{n\times n}x'^n=0^{n-k}} \frac{2^{-(n-k)n}}{2^{(n-rank(\mathbf{H}_{(n-k)\times n}\mathbf{K}_{n\times n}))}-1} \\
&= \sum_{\mathbf{H}'_{(n-k)\times n}:\mathbf{H}'_{(n-k)\times n}x'^n=0^{n-k}} \frac{2^{-(n-k)n}}{2^{(n-rank(\mathbf{H}'_{(n-k)\times n}))}-1} \\
&= \Pr\{X^n(q) = x'^n\}
\end{aligned}$$

where $\mathbf{K}_{n\times n}$ is an invertible matrix such that $x^n = \mathbf{K}_{n\times n}x'^n$. This implies that for $\mathcal{C}_{n,k}^{(2)}$, $X^n(q)$ takes all sequences $x^n \in \mathcal{X}^n/\{0^n\}$ equally likely. Since the zero sequence is not allowed by way of puncturing, it follows that the distribution of $X^n(q)$ is the same as the conditional distribution of X^n given $X^n \neq 0^n$. Therefore, for $\mathcal{C}_{n,k}^{(2)}$, we have

$$\begin{aligned}
\Pr\{X^n(q) \notin J(Y^n)\} &= \Pr\{\, X^n \notin J(Z^n) |\, X^n \neq 0^n\} \\
&\leq \frac{1}{1-2^{-n}} \Pr\{X^n \notin J(Z^n)\} \,.
\end{aligned} \tag{2.30}$$

Putting (2.26) and (2.28)-(2.30) together yields

$$P_e(\mathcal{C}_{n,k}^{(i)}) \leq C^{(i)} \Pr\{X^n \notin J(Z^n)\} + e^{-n\left(C_{\text{BIMC}}-\delta-\mathcal{R}(\mathcal{C}_{n,k})\right)} \tag{2.31}$$

where $C^{(i)}$ is defined in (2.17), and (2.16) is proved by observing from (1.9) that

$$\Pr\{X^n \notin J(Z^n)\} = \Pr\left\{-\frac{1}{n}\sum_{i=1}^{n} \ln p(X_i|Z_i) > H(X|Y) + \delta\right\} \tag{2.32}$$

where $H(X_1|Z_1) = H(X|Y)$.

The inequalities (2.18) to (2.23) can now be established by applying different upper bounds to (2.32). At this point, we apply the non-asymptotic equipartition property with respect to $H(X|Y)$ and invoke Result 1.1 in Section 1.4.1, part (b) of which says

$$\Pr\left\{-\frac{1}{n}\sum_{i=1}^{n}\ln p(X_i|Z_i) > H(X|Y)+\delta\right\} \;\leq\; \bar{\xi}_H(X|Y,\lambda,n)e^{-nr_{X|Y}(\delta)}\,. \tag{2.33}$$

The inequalities (2.18) and (2.19) then follow from (2.31)-(2.33).

To show (2.20), let $\delta = \sigma_H(X|Y)\sqrt{\frac{2\alpha\ln n}{n}}$. Invoke Result 1.1 again, part (a) of which says

$$r_{X|Y}(\delta) = \frac{1}{2\sigma_H^2(X|Y)}\delta^2 + O(\delta^3) = \frac{\alpha\ln n}{n} + O\left(\sqrt{\frac{\ln^3 n}{n^3}}\right)$$

and

$$\lambda = \frac{\delta}{\sigma_H^2(X|Y)} + O(\delta^2) = \frac{1}{\sigma_H(X|Y)}\sqrt{\frac{2\alpha\ln n}{n}} + O\left(\frac{\ln n}{n}\right).$$

On the other hand, it is easy to see from the definition of $\bar{\xi}_H(X|Y,\lambda,n)$ that

$$\frac{(2-C_{BE})M_H(X|Y,\lambda)}{\sqrt{n}\sigma_H^3(X|Y,\lambda)} \leq \zeta_H(X|Y,\lambda,n) - e^{\frac{n\lambda^2\sigma_H^2(X|Y,\lambda)}{2}}Q(\sqrt{n}\lambda\sigma_H(X|Y,\lambda)) \leq \frac{2M_H(X|Y,\lambda)}{\sqrt{n}\sigma_H^3(X|Y,\lambda)} \tag{2.34}$$

while

$$-\frac{1}{2\pi n\lambda^2\sigma_H^2(X|Y,\lambda)} \leq e^{\frac{n\lambda^2\sigma_H^2(X|Y,\lambda)}{2}}Q(\sqrt{n}\lambda\sigma_H(X|Y,\lambda)) - \frac{1}{\sqrt{2\pi n}\lambda\sigma_H(X|Y,\lambda)} \leq 0. \tag{2.35}$$

This implies that

$$\zeta_H(X|Y,\lambda,n) = \Theta\left(\frac{1}{\sqrt{\ln n}}\right) \tag{2.36}$$

and

$$\zeta_H(X|Y,\lambda,n)e^{-nr_{X|Y}(\delta)} = \frac{n^{-\alpha}}{2\sqrt{\pi\alpha\ln n}} + O\left(n^{-\alpha}\frac{\ln^{3/2} n}{\sqrt{n}}\right)\,. \tag{2.37}$$

Therefore, in this case, we have

$$\Pr\left\{-\frac{1}{n}\sum_{i=1}^{n}\ln p(X_i|Z_i) > H(X|Y)+\delta\right\} \;\leq\; \frac{n^{-\alpha}}{2\sqrt{\pi\alpha\ln n}} + O\left(n^{-\alpha}\frac{\ln^{3/2} n}{\sqrt{n}}\right)\,. \tag{2.38}$$

The inequalities (2.20) and (2.21) then follow from (2.31), (2.32), (2.36) and (2.38).

Finally, let $\delta = \frac{c}{\sqrt{n}}$. Applying part (c) of Result 1.1, yields

$$\Pr\left\{-\frac{1}{n}\sum_{i=1}^{n}\ln p(X_i|Z_i) > H(X|Y)+\frac{c}{\sqrt{n}}\right\} \;\le\; Q\left(\frac{c}{\sigma_H(X|Y)}\right)+\frac{C_{BE}M_H(X|Y)}{\sigma_H^3(X|Y)}\frac{1}{\sqrt{n}}.$$

Then (2.22) follows from the fact that

$$e^{-n\left(C_{\mathrm{BMS}}-\frac{c}{\sqrt{n}}-\mathcal{R}(\mathcal{C}_{n,k})\right)} \le \frac{C^{(i)}(1-C_{BE})M_H(X|Y)}{\sigma_H^3(X|Y)}\frac{1}{\sqrt{n}}$$

whenever (2.23) holds. This completes the proof of Theorem 2.2. □

Remark 2.3. *The purpose of puncturing $q = 0$ from the message space is to make the proof a little bit simpler. From the proof, it can be seen that if we add $q = 0$ back, it only increases the error probability upper bound by $2^{-n\mathcal{R}(\mathcal{C}_{n,k})}$, and all the remaining statements in Theorem 2.2 still hold.*

Remark 2.4. *As can be seen, the fact that the uniform distribution is the capacity achieving distribution for BIMC is not essential in the proof of Theorem 2.2. Therefore, for general binary input memoryless channels, Theorem 2.2 still holds by replacing C_{BIMC} with the mutual information between a uniform random variable and its channel response. Moreover, Theorem 2.2 can be easily extended to the general case when $\mathcal{X}$ is a finite field.*

Remark 2.5. *The inequalities (2.20) to (2.23) show that linear block codes of block length n can reach within $\sigma_H(X|Y)\sqrt{\frac{2\alpha\ln n}{n}}+\left(\alpha+\frac{1}{2}\right)\frac{\ln n}{n}+O\left(\frac{\ln\ln n}{n}\right)$ of the capacity of any BIMC while maintaining the word error probability $\frac{n^{-\alpha}}{2\sqrt{\pi\alpha\ln n}}+O\left(n^{-\alpha}\frac{\ln^{3/2} n}{\sqrt{n}}\right)$, and within $\frac{c}{\sqrt{n}}+\frac{\ln n}{2n}-\frac{1}{n}\ln\frac{(1-C_{BE})M_H(X|Y)}{\sigma_H^3(X|Y)}$ of the capacity while maintaining the word error probability $Q\left(\frac{c}{\sigma_H(X|Y)}\right)+\frac{M_H(X|Y)}{\sigma_H^3(X|Y)}\frac{1}{\sqrt{n}}$. If the word error probability is kept slightly above 0.5, the code rate can be even slightly above the capacity of the BIMC!*

2.3 Non-asymptotic Coding Theorem: DIMC

Consider now an arbitrary DIMC $P = \{p(y|x) : x \in \mathcal{X}, y \in \mathcal{Y}\}$. Let X be the capacity achieving input random variable, i.e., X achieves the maximum in (1.1). Let Y be the output of the DIMC P in response to X. Then the capacity of the DIMC P is

$$C_{\mathrm{DIMC}} = I(X;Y)\,.$$

Without loss of generality, assume that the distribution p_X of X assigns a positive probability to each and every $x \in \mathcal{X}$.

Since X is not necessarily uniformly distributed, we now move away from linear codes in this section, and use random codes drawn from a particular type t instead. Recall definitions $I(t;P)$, $\sigma^2_{D,-}(t;P,\lambda)$, $M_{D,-}(t;P,\lambda)$, $\sigma^2_D(t;P)$ and $M_D(t;P)$ in Section 1.4.2. Due to the significance of p_X, write $\sigma^2_D(p_X;P)$ and $M_D(p_X;P)$ as $\sigma^2_D(X;Y)$ and $M_D(X;Y)$ respectively. In particular, it can be easily verified that

$$I(t;P) = C_{\text{DIMC}} + O(n^{-1}) \tag{2.39}$$

whenever

$$||t - p_X||_1 \leq \frac{|\mathcal{X}|}{n} \tag{2.40}$$

where $||\cdot||_1$ is the l_1-norm. Obviously, types t satisfying (2.40) exist.

Now let $\mathcal{C}_{t,n,k}$ denote the ensemble of channel codes from a type t with code length n and rate $\mathcal{R}(\mathcal{C}_{t,n,k}) = \frac{k}{n}\ln 2$, where a channel code from $\mathcal{C}_{t,n,k}$ is generated in such way that each codeword is uniformly picked from $\mathcal{T}^n_t$. At the decoder, the jar $J(y^n)$ for each sequence $y^n \in \mathcal{Y}^n$ is formed as

$$J(y^n) = \left\{ x^n \in \mathcal{T}^n_t : \frac{1}{n}\sum_{i=1}^{n} \ln \frac{p(y_i|x_i)}{q_t(y_i)} \geq I(t;P) - \delta \right\} \tag{2.41}$$

where δ is a real number. The jar defined in (2.41) will be referred to as the DIMC jar based on type t. Moreover, for any $x^n \in \mathcal{T}^n_t$,

$$P^-_{t,\delta} \triangleq \Pr\left\{ \frac{1}{n}\sum_{i=1}^{n} \ln \frac{p(Y_i|X_i)}{q_t(Y_i)} < I(t;P) - \delta \,\middle|\, X^n = x^n \right\} \tag{2.42}$$

where Y^n is the output of DIMC P in response to x^n. It is easy to verify that $P^-_{t,\delta}$ is well defined as the probability at the right hand side of (2.42) is the same for any $x^n \in \mathcal{T}^n_t$, and the upper bounds on

$$\Pr\left\{ \frac{1}{n}\sum_{i=1}^{n} \ln \frac{p(Y_i|X_i)}{q_t(Y_i)} \leq I(t;P) - \delta \,\middle|\, X^n = x^n \right\}$$

in Section 1.4.2 holds for $P^-_{t,\delta}$.

Recall definitions in Section 1.4.2, and define

$$\zeta_{D,-}(t;P,\lambda,n) \triangleq \frac{2M_{D,-}(t;P,\lambda)}{\sqrt{n}\sigma^3_{D,-}(t;P,\lambda)} + e^{\frac{n\lambda^2\sigma^2_{D,-}(t;P,\lambda)}{2}}\left[Q(\sqrt{n}\lambda\sigma_{D,-}(t;P,\lambda)) - Q(\rho^* + \sqrt{n}\lambda\sigma_{D,-}(t;P,\lambda))\right]$$

With the DIMC jar based on type t specified in (2.41), we have the following non-asymptotic coding theorem with jar decoding.

Theorem 2.3. *Given a DIMC P with $C_{\text{DIMC}} \in (0, |\mathcal{X}|)$, let $P_e(\mathcal{C}_{t,n,k})$ denote the average word error probability (under jar decoding) of $\mathcal{C}_{t,n,k}$ with respect to the DIMC and the random code $\mathcal{C}_{t,n,k}$ itself. Then for any block length n,*

$$P_e(\mathcal{C}_{t,n,k}) \le P^-_{t,\delta} + e^{-n\left[I(t;P)-\delta+\frac{\ln e^{-nH(t)}|\mathcal{T}^n_t|}{n}-\mathcal{R}(\mathcal{C}_{t,n,k})\right]}. \tag{2.43}$$

Moreover, for any block length n, the following hold:

1) *For any $\delta \in (0, \Delta^*_-(t))$*

$$P_e(\mathcal{C}_{t,n,k}) \le \zeta_{D,-}(t;P,\lambda,n)e^{-nr_-(t,\delta)} \tag{2.44}$$

whenever

$$\mathcal{R}(\mathcal{C}_{t,n,k}) \le I(t;P) - \delta - r_-(t,\delta) - \frac{|\mathcal{X}|\ln(n+1) - \ln\frac{2(1-C_{BE})M_{\text{D},-}(t;P,\lambda)}{\sqrt{n}\sigma^3_{\text{D},-}(t;P,\lambda)}}{n} \tag{2.45}$$

where $\lambda = \frac{\partial r_-(t,\delta)}{\partial\delta}$ satisfying $\delta_-(t,\lambda) = \delta$.

2) *For any $\alpha \ge 0.5$ and any t satisfying (2.40)*

$$P_e(\mathcal{C}_{t,n,k}) \le \frac{n^{-\alpha}}{2\sqrt{\pi\alpha\ln n}} + O\left(n^{-\alpha}\frac{\ln^{3/2} n}{\sqrt{n}}\right) \tag{2.46}$$

whenever

$$\mathcal{R}(\mathcal{C}_{t,n,k}) \le C_{\text{DIMC}} - \sigma_D(X;Y)\sqrt{\frac{2\alpha\ln n}{n}} - \frac{\left(\frac{1}{2}+\alpha+|\mathcal{X}|\right)\ln(n+1)}{n} - O\left(\frac{\ln\ln n}{n}\right). \tag{2.47}$$

3) For any t satisfying (2.40)

$$\begin{aligned} P_e(\mathcal{C}_{t,n,k}) &\leq Q\left(\frac{c}{\sigma_D(X;Y)}\right) + \frac{M_D(t;P)}{\sigma_D^3(t;P)}\frac{1}{\sqrt{n}} \\ &= Q\left(\frac{c}{\sigma_D(X;Y)}\right) + \frac{M_D(X;Y)}{\sigma_D^3(X;Y)}\frac{1}{\sqrt{n}} + O\left(n^{-1.5}\right) \end{aligned} \tag{2.48}$$

whenever

$$\begin{aligned} \mathcal{R}(\mathcal{C}_{t,n,k}) &\leq I(t;P) - \frac{\sigma_D(t;P)}{\sigma_D(X;Y)}\frac{c}{\sqrt{n}} - \frac{\left(\frac{1}{2}+|\mathcal{X}|\right)\ln(n+1) + \ln\frac{(1-C_{BE})M_D(t;P)}{\sigma_D^3(t;P)}}{n} \\ &= C_{\text{DIMC}} - \frac{c}{\sqrt{n}} - \frac{\left(\frac{1}{2}+|\mathcal{X}|\right)\ln(n+1) + \ln\frac{(1-C_{BE})M_D(X;Y)}{\sigma_D^3(X;Y)}}{n} - O\left(n^{-1}\right) \end{aligned} \tag{2.49}$$

for any real number c.

Proof. The proof is along the same way as in the proof of Theorems 2.1 and 2.2. Let $X^n(q)$ be the transmitted codeword, and Y^n the output of the DIMC P in response to $X^n(q)$. In parallel with (2.26), we have

$$P_e(\mathcal{C}_{t,n,k}) \leq \Pr\{X^n(q) \notin J(Y^n)\} + \Pr\left\{\exists z^n \neq X^n(q), z^n \in J(Y^n), z^n \in \mathcal{C}_{t,n,k}\right\} \tag{2.50}$$

where $J(Y^n)$ is the DIMC jar based on type t as defined in (2.41). Note that $X^n(q)$ is distributed uniformly over $\mathcal{T}_t^n$. For any $x^n \in \mathcal{T}_t^n$ and $y^n \in \mathcal{Y}^n$, one can verify that

$$\begin{aligned} &\Pr\left\{\exists z^n \neq X^n(q), z^n \in J(Y^n), z^n \in \mathcal{C}_{t,n,k} \middle| X^n(q) = x^n, Y^n = y^n\right\} \\ &\overset{(a)}{\leq} |J(y^n)||\mathcal{T}_t^n|^{-1}2^k \\ &\leq |J(y^n)|e^{k\ln 2 - nH(t) - \ln e^{-nH(t)}|\mathcal{T}_t^n|} \\ &\overset{(b)}{\leq} e^{n[H(t)-I(t;P)+\delta]}e^{n\left[\frac{k}{n}\ln 2 - H(t) - \frac{\ln e^{-nH(t)}|\mathcal{T}_t^n|}{n}\right]} \\ &\leq e^{-n\left[I(t;P)-\delta+\frac{\ln e^{-nH(t)}|\mathcal{T}_t^n|}{n} - \mathcal{R}(\mathcal{C}_{t,n,k})\right]} \end{aligned} \tag{2.51}$$

where (a) is due to the fact that all codewords in $\mathcal{C}_{t,n,k}$ are independent, and each is

distributed uniformly over $\mathcal{T}_t^n$, and (b) is verified by

$$\begin{aligned}
|J(y^n)|e^{-n(H(t)-I(t;P)+\delta)} &\le \sum_{z^n\in J(y^n)} e^{-nH(t)+\sum_{i=1}^n \ln\frac{p(y_i|z_i)}{q_t(y_i)}} \\
&= \sum_{z^n\in J(y^n)} \frac{e^{-nH(t)}\prod_{i=1}^n p(y_i|z_i)}{\prod_{i=1}^n q_t(y_i)} \\
&= \frac{\sum_{z^n\in J(y^n)} e^{-nH(t)}\prod_{i=1}^n p(y_i|z_i)}{\prod_{i=1}^n \sum_{x\in\mathcal{X}} t(x)p(y_i|x)} \\
&= \frac{\sum_{z^n\in J(y^n)} e^{-nH(t)}\prod_{i=1}^n p(y_i|z_i)}{\sum_{x^n\in\mathcal{X}^n}\prod_{i=1}^n t(x_i)p(y_i|x_i)} \\
&\le \frac{\sum_{z^n\in\mathcal{T}_t^n} e^{-nH(t)}\prod_{i=1}^n p(y_i|z_i)}{\sum_{x^n\in\mathcal{X}^n}\prod_{i=1}^n t(x_i)p(y_i|x_i)} \\
&= \frac{\sum_{z^n\in\mathcal{T}_t^n}\prod_{i=1}^n t(z_i)p(y_i|z_i)}{\sum_{x^n\in\mathcal{X}^n}\prod_{i=1}^n t(x_i)p(y_i|x_i)} \le 1
\end{aligned}$$

since for any $z^n \in \mathcal{T}_t^n$,

$$\prod_{i=1}^n t(z_i) = e^{-nH(t)}$$

and $\mathcal{T}_t^n$ is only a subset of $\mathcal{X}^n$. Since (2.51) is valid for any $x^n \in \mathcal{T}_t^n$ and $y^n \in \mathcal{Y}^n$, it follows that

$$\Pr\{\exists z^n \ne X^n(q), z^n \in J(Y^n), z^n \in \mathcal{C}_{t,n,k}\} \le e^{-n\left[I(t;P)-\delta+\frac{\ln e^{-nH(t)}|\mathcal{T}_t^n|}{n}-\mathcal{R}(\mathcal{C}_{t,n,k})\right]}. \tag{2.52}$$

On the other hand, in view of (2.41) and (2.42),

$$\Pr\{X^n(q) \notin J(Y^n)\} = P_{t,\delta}^-. \tag{2.53}$$

Putting (2.53), (2.52), and (2.50) together yields

$$P_e(\mathcal{C}_{t,n,k}) \le P_{t,\delta}^- + e^{-n\left[I(t;P)-\delta+\frac{\ln e^{-nH(t)}|\mathcal{T}_t^n|}{n}-\mathcal{R}(\mathcal{C}_{t,n,k})\right]} \tag{2.54}$$

and (2.43) is proved.

Applying the inequality

$$e^{-nH(t)}|\mathcal{T}_t^n| \ge (n+1)^{-|\mathcal{X}|}, \tag{2.55}$$

the inequalities (2.44)-(2.49) can now be established by applying different upper bounds to $P_{t,\delta}^{-}$. At this point, we apply the non-asymptotic equipartition property with respect to relative entropy and invoke Result 1.2 in Section 1.4.2, part (b) of which says

$$P_{t,\delta}^{-} \leq \bar{\xi}_{D,-}(t;P,\lambda,n)e^{-nr_{-}(t,\delta)} \ . \tag{2.56}$$

The inequalities (2.44) and (2.45) then follow from (2.54) and (2.56).

To show (2.46), let $\delta = \sigma_D(X;Y)\sqrt{\frac{2\alpha \ln n}{n}}$. Invoke Result 1.2 in Section 1.4.2 again, part (a) of which says

$$r_{-}(t,\delta) \ = \ \frac{1}{2\sigma_D^2(t;P)}\delta^2 + O(\delta^3)$$

and

$$\lambda = \frac{\delta}{\sigma_D^2(t;P)} + O(\delta^2),$$

which, together with (2.40), implies

$$\begin{aligned} r_{-}(t,\delta) \ &= \ \frac{\sigma_D^2(X:Y)}{\sigma_D^2(t;P)}\frac{\alpha \ln n}{n} + O\left(\sqrt{\frac{\ln^3 n}{n^3}}\right) \\ &= \ \frac{\alpha \ln n}{n} + O\left(\sqrt{\frac{\ln^3 n}{n^3}}\right) \end{aligned}$$

and

$$\lambda = \frac{\delta}{\sigma_D^2(X;Y)} + O(\delta^2).$$

Moreover, under the condition (2.40)

$$I(t;P) = C_{\mathrm{DIMC}} - O(n^{-1}) \ .$$

The inequality (2.46) under the condition (2.47) can then be established by following the respective argument in the proof of Theorem 2.2.

Finally, let $\delta = \frac{\sigma_{\mathrm{D}}(t;P)}{\sigma_{\mathrm{D}}(X;Y)}\frac{c}{\sqrt{n}}$. Applying part (c) of Result 1.2, we have

$$P_{t,\delta}^{-} \leq Q\left(\frac{c}{\sigma_{\mathrm{D}}(X;Y)}\right) + \frac{C_{BE}M_{\mathrm{D}}(t;P)}{\sigma_{\mathrm{D}}^3(t;P)}\frac{1}{\sqrt{n}} \ .$$

The inequality (2.48) then follows from the fact that

$$\frac{M_D(t;P)}{\sigma_D^3(t;P)} = \frac{M_D(X;Y)}{\sigma_D^3(X;Y)} + n^{-1}$$

for t satisfying (2.40), and

$$e^{-n\left[I(t;P)-\delta-\frac{|\mathcal{X}|\ln(n+1)}{n}-\mathcal{R}(\mathcal{C}_{t,n,k})\right]} \leq \frac{(1-C_{BE})M_{\mathrm{D}}(t;P)}{\sigma_{\mathrm{D}}^3(t;P)}\frac{1}{\sqrt{n}}$$

whenever (2.49) holds. This completes the proof of Theorem 2.3. □

Remark 2.6. *It is not hard to show that in the case of BIMC*

$$\sigma_D(X;Y) \leq \sigma_H(X|Y) \tag{2.57}$$

and the inequality (2.57) is strict in general unless the BIMC, such as the BSC and BIAGC, happens to have some symmetric properties, in which case (2.57) is the equality. Therefore, by comparing Theorem 2.3 with Theorem 2.2, we see that for a BIMC, Shannon random codes based on types are generally slightly better than random linear codes in terms of the tradeoff between the capacity gap and word error probability. In addition, since our bounds in Theorem 2.3 are valid for any n, t, and p_X achieving the capacity C_{DIMC}, in the case of DIMC where there are multiple input distributions p_X achieving the capacity C_{DIMC}, one can further optimize the bounds in Theorem 2.3 over all these capacity achieving input distributions. In particular, in (2.48) and (2.49), one should choose the minimum $\sigma_D(X;Y)$ over all capacity achieving inputs X when $c > 0$ and the maximum $\sigma_D(X;Y)$ over all capacity achieving inputs X when $c < 0$.

Remark 2.7. *Related to (2.48) and (2.49) is the second order coding rate analysis in [15, 18, 19] with a fixed word error probability $0 < \epsilon < 1$. All identify correctly the coefficient before the second order $\frac{1}{\sqrt{n}}$. The difference lies in that the works in [15, 18, 19] are asymptotic. On the other hand, (2.48) and (2.49) are are non-asymptotic. In addition, bounds in Theorem 2.3 also give a complete picture about the tradeoff between the capacity gap and word error probability when the word error probability goes to 0 with block length n at a sub-polynomial $n^{-\alpha}$, $0 < \alpha < 1$, polynomial $n^{-\alpha}$, $\alpha \geq 1$, or sub-exponential $e^{-n^{\alpha}}$, $0 < \alpha < 1$, speed. In particular, comments similar to Remarks 2.1 and 2.5 apply here too.*

2.4 Comparison with Existing Non-Asymptotic Achievability

There are tremendous achievable bounds [20,21] (and references therein) on channel coding rate in the prosperous literature of information theory, where various code ensembles and bounding techniques are used. Comparing our achievabilities with all of those achievabilities is analogous to brute-force implementation of ML decoding. At the same time, not all achievabilities are comparable with ours since the underlying code ensembles could be totally different. For example, some achievabilities are based on Shannon random code ensemble, where each symbol of any codeword is independently and identically generated. However, the ensembles used in our achievable bounds via jar decoding have some structures and/or constraints imposed, and consequently, achievabilities based on Shannon random code ensemble may not be applicable. Therefore, our comparison strategy adopts the idea of jar decoding, where we first form the jar of comparable achievabilities consisting of those applicable to code ensembles used by us, and then focus on those achievabilities inside the jar. Nevertheless, Gallager's Error Exponent Bound in [22] and non-asymptotic achievabilities in [15] are cited here as benchmarks for the comparison.

Result 2.1. *Given any channel* $\{p_{Y^n|X^n}(y^n|x^n) : x^n \in \mathcal{X}^n, y^n \in \mathcal{Y}^n\}$ *and Shannon random code ensemble* $\mathcal{C}_n$ *with* M *number of codewords and input distribution* $p_{X^n}(x^n)$ *for* $x^n \in \mathcal{X}^n$,

$$P_e(\mathcal{C}_n) \leq (M-1)^{\rho} \int \left(\int p_{X^n}(x^n)[p_{Y^n|X^n}(y^n|x^n)]^{\frac{1}{1+\rho}} dx^n \right)^{1+\rho} dy^n \tag{2.58}$$

for $0 \leq \rho \leq 1$. *When the channel is memoryless (i.e.* $p_{Y^n|X^n}(y^n|x^n) = \prod_{i=1}^n p(y_i|x_i)$*) and each symbol of any codeword is independently and identically generated (i.e.* $p_{X^n}(x^n) = \prod_{i=1}^n Q(x_i)$*),*

$$P_e(\mathcal{C}_n) \leq e^{-n(E(\rho,Q)-\rho\mathcal{R}(\mathcal{C}_n))} \tag{2.59}$$

for $0 \leq \rho \leq 1$, *where* $\mathcal{R}(\mathcal{C}_n) = \frac{1}{n} \ln M$ *and*

$$E(\rho, Q) = -\ln \int \left(\int Q(x)[p(y|x)]^{\frac{1}{1+\rho}} dx \right)^{1+\rho} dy.$$

Result 2.2 (Random Coding Union [15, Theorem 16])**.** *Given any channel* $\{p_{Y^n|X^n}(y^n|x^n) : x^n \in \mathcal{X}^n, y \in \mathcal{Y}^n\}$ *and Shannon random code ensemble* $\mathcal{C}_n$ *with* M *number of codewords and input distribution* $p_{X^n}(x^n)$ *for* $x^n \in \mathcal{X}^n$,

$$P_e(\mathcal{C}_n) \leq \mathbb{E}\left[\min\left\{1, (M-1)\Pr\left\{\ln\frac{p_{Y^n|X^n}(Y^n|\bar{X}^n)}{p_{Y^n}(Y^n)} \geq \ln\frac{p_{Y^n|X^n}(Y^n|X^n)}{p_{Y^n}(Y^n)} \middle| X^n, Y^n\right\}\right\}\right] \tag{2.60}$$

where $(X^n, Y^n, \bar{X}^n)$ *follows the distribution* $p_{X^n}(x^n)p_{Y^n|X^n}(y^n|x^n)p_{X^n}(\bar{x}^n)$ *for* $(x^n, y^n, \bar{x}^n) \in \mathcal{X}^n \times \mathcal{Y}^n \times \mathcal{X}^n$.

Result 2.3 (Dependence Testing [15, Theorem 17,18])**.** *Given any channel* $\{p_{Y^n|X^n}(y^n|x^n) : x^n \in \mathcal{X}^n, y \in \mathcal{Y}^n\}$ *and Shannon random code ensemble* $\mathcal{C}_n$ *with* M *number of codewords and input distribution* $p_{X^n}(x^n)$ *for* $x^n \in \mathcal{X}^n$,

$$P_e(\mathcal{C}_n) \leq \Pr\left\{\ln \frac{p(Y^n|X^n)}{p(Y^n)} \leq \ln \frac{M-1}{2}\right\} + \frac{M-1}{2} \Pr\left\{\ln \frac{p(\bar{Y}^n|X^n)}{p(\bar{Y}^n)} > \ln \frac{M-1}{2}\right\} \quad (2.61)$$

where $(X^n, Y^n, \bar{Y}^n)$ *follows the distribution* $p_{X^n}(x^n)p_{Y^n|X^n}(y^n|x^n)p_{Y^n}(\bar{y}^n)$ *for* $(x^n, y^n, \bar{y}^n) \in \mathcal{X}^n \times \mathcal{Y}^n \times \mathcal{Y}^n$ *and*

$$p_{Y^n}(y^n) = \int p_{X^n}(x^n)p_{Y^n|X^n}(y^n|x^n)dx^n.$$

Towards presenting another achievability in [15], called $\kappa\beta$ Bound, following definitions are needed. Let $q_1(w^n)$ and $q_2(w^n)$ for $w^n \in \mathcal{W}^n$ be some distributions on a sample space $\mathcal{W}^n$, and $p_{Z|W^n}(z|w^n)$ for $z \in \{0,1\}$ and $w^n \in \mathcal{W}^n$ be a conditional distribution on $\{0,1\} \times \mathcal{W}^n$. Then define for $\alpha \in [0,1]$

$$\beta_\alpha(q_1, q_2) \stackrel{\Delta}{=} \min_{p_{Z|W^n}: \int q_1(w^n)p_{Z|W^n}(1|w^n)dw^n \geq \alpha} \int q_2(w^n)p_{1|W^n}(1|w^n)dw^n. \quad (2.62)$$

In hypothesis testing, the minimizer $p^*_{Z|W^n}$ of the optimization above can be interpreted as the optimal randomized test function between q_1 (null) and q_2 (alternative). Now let $q_{Y^n}(y^n)$ and $p_{Y^n|X^n}(y^n|x^n)$ for $x^n \in \mathcal{X}^n$ and $y^n \in \mathcal{Y}^n$ be some distribution and conditional distribution on $\mathcal{X}^n$ and $\mathcal{X}^n \times \mathcal{Y}^n$ respectively. Further define $\alpha \in [0,1]$

$$\beta_\alpha(x^n, q_{Y^n}) \stackrel{\Delta}{=} \beta_\alpha(p_{Y^n|X^n=x^n}, q_{Y^n}) \quad (2.63)$$

where $p_{Y^n|X^n=x^n}(y^n) = p_{Y^n|X^n}(y^n|x^n)$ for all $y^n \in \mathcal{Y}^n$ given x^n. In addition, for $\mathcal{F} \subseteq \mathcal{X}^n$ and $\tau \in [0,1]$, define

$$\kappa_\tau(\mathcal{F}, q_{Y^n}) = \inf_{p_{Z|Y^n}: \inf_{x^n \in \mathcal{F}} \int p_{Y^n|X^n}(y^n|x^n)p(1|y^n)dy^n \geq \tau} \int q_{Y^n}(y^n)p_{Z|Y^n}(1|y^n)dy^n. \quad (2.64)$$

Again the minimizer $p^*_{Z|Y^n}$ (if exists) above can be interpreted as the optimal composite test function between $\{p_{Y^n|X^n=x^n}\}_{x^n \in \mathcal{F}}$ (null) and q_{Y^n} (alternative). Then the following result is proved in [15].

Result 2.4 ($\kappa\beta$ [15, Theorem 25])**.** *Given any channel* $\{p_{Y^n|X^n}(y^n|x^n) : x^n \in \mathcal{X}^n, y \in \mathcal{Y}^n\}$ *and* $\mathcal{F} \subseteq \mathcal{X}^n$*, a channel code* $\mathcal{C}_n$ *with its codewords from* $\mathcal{F}$ *and* M *number of codewords can be deterministically constructed, satisfying*

$$M \geq \sup_{0<\tau<P_e(\mathcal{C}_n)} \sup_{q_{Y^n}} \frac{\kappa_\tau(\mathcal{F}, q_{Y^n})}{\sup\limits_{x^n \in \mathcal{F}} \beta_{1-P_e(\mathcal{C}_n)+\tau}(x^n, q_{Y^n})}. \tag{2.65}$$

Moreover, considering that β and κ defined above are in general extremely difficulty to evaluate, upper and lower bounds on β and κ are provided in [15, Equations (103), (104), (106), (121) and (122)], and included here for easy reference.

$$\beta_\alpha(q_1, q_2) \leq \frac{1}{\sup\limits_{\gamma:\Pr\left\{\frac{q_1(W^n)}{q_2(W^n)} \geq \gamma\right\} \geq \alpha} \gamma} \tag{2.66}$$

where W^n follows the distribution q_1,

$$\beta_\alpha(x^n, q_{Y^n}) \geq \sup_{\gamma>0} \frac{1}{\gamma} \left(\alpha - \Pr\left\{ \frac{p_{Y^n|X^n}(Y^n|x^n)}{q_{Y^n}(Y^n)} \geq \gamma \right\} \right) \tag{2.67}$$

where Y^n follows the distribution $p_{Y^n|X^n=x^n}$ given x^n, and

$$\tau \int_{x^n \in \mathcal{F}} p_{X^n}(x^n) dx^n \leq \kappa_\tau(\mathcal{F}, q_{Y^n}) \leq \tau \tag{2.68}$$

where p_{X^n} satisfies

$$q_{Y^n}(y^n) = \int p_{X^n}(x^n) p_{Y^n|X^n}(y^n|x^n) dx^n.$$

2.4.1 Achievability on Random Linear Code Ensembles

In Sections 2.1 and 2.2, Gallager's parity check ensemble and Elias' generator ensemble are used. Unlike Shannon random code ensemble, codewords generated in Gallager's parity check ensemble are not pairwisely independent. Consequently, achievabilities, including Results 2.2 and 2.3, whose proof relies on pairwise independence of codewords, are ruled out in this subsection. Result 2.4 is not applicable either, as the deterministic construction used in its proof can not guarantee the linearity of the constructed code. Here we focus on those achievabilities applicable to random linear code ensemble. Furthermore, as some achievabilities are only applicable to special channels, we divide the discussion into four parts: 1) achievabilities on BSC; 2) achievabilities on binary erasure channel (BEC) ; 3) achievabilities on BIAGC ;and 4) achievabilities on Memoryless Input Binary Output Symmetric (MIBOS) channels.

BSC

To make comparison transparent, we rewrite Theorem 2.1. Let $M = 2^k$ be the number of codewords, and p be the crossover probability. By (2.1) in Theorem 2.1, it is not hard to verify that

$$P_e(\mathcal{C}_{n,k}^{(i)}) \leq \underbrace{\sum_{n(p+\delta)<w\leq n} \binom{n}{w} p^w(1-p)^{n-w}}_{\Pr\left\{\frac{1}{n}wt(W^n)>p+\delta\right\}} + \sum_{0\leq w\leq n(p+\delta)} \binom{n}{w} 2^{-n}M \tag{2.69}$$

for $i = 1, 2$, with δ defined in (1.7). Further optimizing δ implies that

$$P_e(\mathcal{C}_{n,k}^{(i)}) \leq \sum_{w=0}^{n} \binom{n}{w} \min\left\{p^w(1-p)^{n-w}, 2^{-n}M\right\} \tag{2.70}$$

and (2.70) is essentially the same (except for a minor difference*) as the Dependence Testing Bound recently established in [15, Theorem 34] (specifying Result 2.3 on BSC) for Shannon random code ensemble over the BSC.

As a candidate to be compared with Theorem 2.1 or (2.70), an achievable bound under ML decoding was proved in [23] by Poltyrev.

Result 2.5. *For BSC with cross-over probability p and a linear code $\mathfrak{C}_{n,k}$ with hamming weight profile $\{N(l)\}_{l=1}^n$, where $N(l)$ is the number of codewords with hamming weight l in $\mathfrak{C}_{n,k}$,*

$$\begin{aligned} P_e(\mathfrak{C}_{n,k}) \leq & \sum_{w=1}^{\lfloor \frac{n}{2} \rfloor} p^w(1-p)^{n-w} \min\left\{ \binom{n}{w}, \sum_{l=1}^{2w} N(l) \sum_{\eta=\lceil \frac{l}{2} \rceil}^{\min\{w,l\}} \binom{l}{\eta}\binom{n-l}{w-\eta} \right\} \\ & + \sum_{w=\lfloor \frac{n}{2} \rfloor+1}^{n} \binom{n}{w} p^w(1-p)^{n-w}. \end{aligned} \tag{2.71}$$

The result below immediately follows Result 2.5.

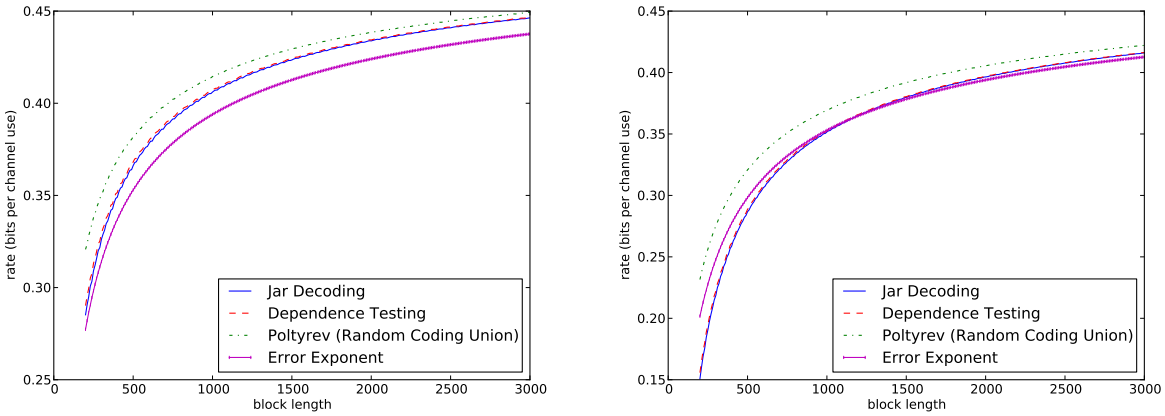
*Replacing M in (2.70) by $(M-1)/2$ yields exactly the Dependence Testing Bound [15, Theorem 34].

Result 2.6. *For BSC with cross-over probability p, $i = 1, 2$,*

$$\begin{aligned} P_e(\mathcal{C}_{n,k}^{(i)}) \quad \leq \quad & \sum_{w=1}^{\lfloor \frac{n}{2} \rfloor} p^w (1-p)^{n-w} \\ & \times \min \left\{ \binom{n}{w}, e^{-(1-\mathcal{R}(\mathcal{C}_{n,k}))n \ln 2} \sum_{l=1}^{2w} \binom{n}{l} \sum_{\eta=\lceil \frac{l}{2} \rceil}^{\min\{w,l\}} \binom{l}{\eta} \binom{n-l}{w-\eta} \right\} \\ & + \sum_{w=\lfloor \frac{n}{2} \rfloor + 1}^{n} \binom{n}{w} p^w (1-p)^{n-w}. \end{aligned} \tag{2.72}$$

It has been shown in [15] that Poltyrev's Bound in (2.72) is equivalent to Random-Coding Union Bound [15, Theorem 33] (by specifying Result 2.2 on BSC) proved on Shannon random code ensembles.

Another candidate for comparison is Error Exponent Bound. Although this bound was originally proved by Gallager on Shannon random code ensemble, it was shown to hold for Gallager's parity check and Elias' generator ensembles on MIBOS channels (discussed in the subsection of MIBOS channels in details), including BSC as a special case.



(a) $P_e = 10^{-3}$ (b) $P_e = 10^{-6}$

Figure 2.2: Comparison of Achievability for BSC with cross-over probability $p = 0.11$

Figure 2.2 shows the numerical comparison (with block length range $[200, 3000]$ and fixed word error probability 10^{-3} and 10^{-6}) among Theorem 2.1, Poltyrev's Bound (Ran-

dom Coding Union Bound) and Error Exponent Bound on a BSC with cross-over probability $p = 0.11$, where Dependence Testing Bound [15, Theorem 34] is also included for a benchmark. As can be seen, the numerical result confirms that Theorem 2.1 is essentially the same as Dependence Testing Bound and further shows that Poltyrev's Bound (Random Coding Union Bound) is better than Dependence Testing Bound and Theorem 2.1 by a small margin, while Dependence Testing Bound and Theorem 2.1 outperforms Error Exponent Bound when word error probability is relatively large with respect to block length, which is consistent with the observation in [15]. As Poltyrev's Bound is proved under ML decoding, this comparison demonstrates that the achievability via jar decoding is very sharp and jar decoding does not lose much optimality compared to ML decoding in the non-asymptotic regime.

BEC

Now let us focus on BEC, a special case of BIMC. It turns out that Theorem 2.2 on BEC can be further improved as follows. Let $M = 2^k$ be the number of codewords and p be the erasure probability. It is then easy to verify that

$$H(X|Y) = p \ln 2$$

and in this case, the BIMC jar reduces to

$$J(y^n) = \begin{cases} \{x^n : x_i = y_i \text{ if } y_i \neq e\} & \text{if } |\{i : y_i = e\}| \leq n\left(p + \frac{\delta}{\ln 2}\right) \\ \text{empty} & \text{otherwise} \end{cases}.$$

Following the argument in the proof of Theorem 2.2, it is not hard to show that

$$\begin{aligned} P_e(\mathcal{C}_{n,k}^{(i)}) &\leq \underbrace{\sum_{n(p+\frac{\delta}{\ln 2})<t\leq n} \binom{n}{t} p^t (1-p)^{n-t}}_{\Pr\{X^n(q)\notin J(Y^n)\}} \\ &\quad + \Pr\left\{\exists z^n \neq X^n(q), z^n \in J(Y^n), z^n \in \mathcal{C}_{n,k}^{(i)}\right\} \\ &\leq \sum_{n(p+\frac{\delta}{\ln 2})<t\leq n} \binom{n}{t} p^t (1-p)^{n-t} \\ &\quad + \sum_{1\leq t\leq n(p+\frac{\delta}{\ln 2})} \binom{n}{t} p^t (1-p)^{n-t} 2^t 2^{-n} M \end{aligned} \tag{2.73}$$

and optimizing δ yields

$$\begin{aligned} P_e(\mathcal{C}_{n,k}^{(i)}) &\leq \sum_{t=1}^{n} \binom{n}{t} p^t (1-p)^{n-t} \min\left\{1, 2^{-(n-t)} M\right\} \\ &= \sum_{t=1}^{n} \binom{n}{t} p^t (1-p)^{n-t} 2^{-[n-t-\log_2 M]^+} \end{aligned} \tag{2.74}$$

which is again essentially the same (except for a minor difference[†]) as the Dependence Testing Bound [15, Theorem 37] for Shannon random code ensemble and Elias' generator ensemble. Note that C^i in Theorem 2.2 is dropped here because of the symmetry of BEC where the technique used in the proof of Theorem 2.1 on BSC can be applied. Another improvement of (2.74) over Theorem 2.2 is due to a better bound on $|J(y^n)|$ given the channel output y^n. In particular, the size of jar $|J(y^n)|$ only depends on the number of erasures in y^n. In general, however, such the refinement is very difficult, as $|J(y^n)|$ may be different for each possible channel output y^n, and one of the best ways to bound $|J(y^n)|$ in order to yield a computable achievability result is to use (1.10), as we did in the proof of Theorem 2.2.

Because BEC is a special channel, exact calculation of word error probability under ML decoding is possible for some linear code ensembles. In particular, Ashikmin proved the following result, included in [15]. Note that the ensemble used by Ashikmin, in which the generator matrix of the code is uniformly picked from the set of full rank matrices, is neither Gallager's parity check ensemble nor Elias' generator ensemble. However, as the matrices in Gallager's parity check ensemble and Elias' generator ensemble are of full rank with high probability, Ashikmin's result is still a legitimate candidate to be compared with jar decoding achievability.

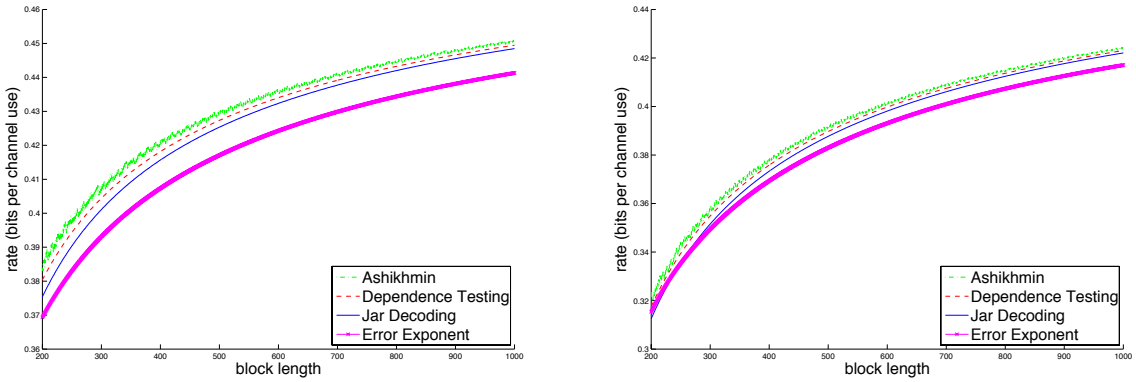
Result 2.7. *For BEC with erasure probability p and random linear code ensemble $\mathcal{C}_{n,k}^{(full)}$ in which the generator matrix is equiprobably selected among all full rank $k \times n$ matrices, the word error probability under ML decoding is given by*

$$\begin{aligned} &P_e(\mathcal{C}_{n,k}^{(full)}) \\ &\quad = \sum_{i=0}^{n} \binom{n}{i} p^{n-i} (1-p)^i \sum_{r=\max\{0,k-n+i\}}^{\min\{k,i\}} \begin{bmatrix} i \\ r \end{bmatrix} \begin{bmatrix} n-i \\ k-r \end{bmatrix} \begin{bmatrix} n \\ k \end{bmatrix}^{-1} 2^{r(n-i-k+r)} (1-2^{r-k}) \end{aligned} \tag{2.75}$$

[†]Replacing M by $(M-1)/2$, and then starting the summation from $t=0$ instead of $t=1$ in (2.74) yield exactly the Dependence Testing Bound [15, Theorem 37].

where

$$\left[\begin{array}{c} a \\ r \end{array} \right] = \left\{ \begin{array}{cc} \prod_{j=0}^{r-1} \frac{2^a - 2^j}{2^r - 2^j} & r > 0 \\ 1 & r = 0 \end{array} \right. .$$



(a) $P_e = 10^{-3}$ (b) $P_e = 10^{-6}$

Figure 2.3: Comparison of Achievability for BEC with erasure probability $p = 0.5$

As BEC is also MIBOS, Error Exponent Bound holds for Gallager's parity check and Elias' generator ensembles. Figure 2.3 shows the numerical comparison between (2.74), Ashikmin's Bound in Result 2.7 and Error Exponent Bound, where Dependence Testing Bound [15, Theorem 37] serves as a benchmark. Once again, our achievability via jar decoding outperforms Error Exponent Bound, and is worse than Ashikmin's Bound (the best achievability under ML decoding known so far) by a small margin.

BIAGC

Applying Theorem 2.2 to BIAGC, $C^{(i)}$ in (2.16) can be dropped for the same reason as that for BSC and BEC. Unfortunately, direct evaluation of (2.16) becomes infeasible, as the probability

$$\Pr\left\{ -\frac{1}{n} \sum_{i=1}^{n} \ln p(X_i|Z_i) > H(X|Y) + \delta \right\}$$

is an n-fold integral. Nevertheless, we can resort to (2.18) and (2.19) in part 1) of Theorem 2.2, which can be efficiently evaluated for any BIMC. Note that to yield the tightest bound, δ in (2.18) and (2.19) can be further optimized.

There is a rich literature about error probability bounds for linear codes on BIAGC, considering the practical impact of this research topic. One of the tightest bounds in this research area is the Tangential Sphere Bound (TSB), proved by Poltyrev in [23].

Result 2.8. *For BIAGC with noise variance σ^2 and a linear code $\mathfrak{C}_{n,k}$ with hamming weight profile $\{N(l)\}_{l=1}^{n}$,*

$$P_e(\mathfrak{C}_{n,k}) \leq \min_{r>0} \left\{ \int_{-\infty}^{+\infty} \frac{e^{-\frac{x^2}{2\sigma^2}}}{\sqrt{2\pi}\sigma} \left(1 - \gamma\left(\frac{n-1}{2}, \frac{(\sqrt{n}-x)^2 r^2}{2\sigma^2}\right)\right) dx \right.$$
$$\left. + \sum_{l=1}^{\left\lfloor \frac{r^2}{1+r^2} n \right\rfloor} N(l) \int_{-\infty}^{+\infty} \left| \int_{(\sqrt{n}-x)\sqrt{\frac{l}{n-l}}}^{(\sqrt{n}-x)r} \frac{e^{-\frac{x^2+y^2}{2\sigma^2}}}{2\pi\sigma^2} \gamma\left(\frac{n-2}{2}, \frac{|(\sqrt{n}-x)^2 r^2 - y^2|}{2\sigma^2}\right) dy \right| dx \right\} \tag{2.76}$$

where $\gamma(a,x)$ is the (normalized) incomplete gamma function defined as

$$\gamma(a,x) = \frac{1}{\Gamma(a)} \int_0^x t^{a-1} e^{-t} dt$$

and

$$\Gamma(a) = \int_0^{+\infty} t^{a-1} e^{-t} dt$$

is the gamma function.

For Elias' generator ensemble $\mathcal{C}_{n,k}^{(1)}$ and Gallager's parity check ensemble $\mathcal{C}_{n,k}^{(2)}$, (2.76) holds by replacing $N(l)$ with $2^{-n\left(1-\frac{k}{n}\right)} \binom{n}{l}$. It turns out that the proof technique of TSB is quite related to the idea of jar decoding. In fact, from jar decoding perspective, TSB is yielded by treating a n-dimensional circular cone with half-angle θ ($r = \tan\theta$ is subject to optimization as shown in (2.76)) as the jar and applying the union bound to the probability (conditioned on the radial component of the noise) that there exists a codeword in the jar closer to the channel output than the transmitted one in Euclidean distance. As the jar is a circular cone, the probability that the transmitted codeword is outside the jar can be exactly calculated with the help of integration and incomplete gamma function,

shown as the first term in (2.76). TSB was then improved by Yousefi and Khandani in [24], and Mehrabian and Yousefi in [25]. It is unclear, however, whether those two improved bounds can be efficiently evaluated for Elias' generator ensemble and Gallager's parity check ensemble.

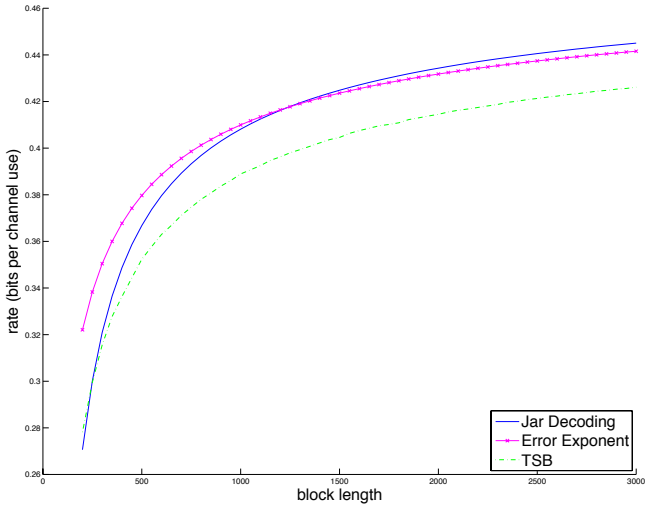


Figure 2.4: Comparison of Achievability for BIAGC with snr 0dB and word error probability $P_e = 10^{-2}$

As mentioned earlier, given any linear code, TSB is one of the tightest bounds on BIACG in terms of the hamming weight profile. However, for Elias' generator ensemble and Gallager's parity check ensemble, TSB fails to reproduce the Gallager's error exponent ([20] and references therein). On the other hand, Error Exponent Bound holds for Elias' generator ensemble and Gallager's parity check ensemble on BIAGC, due to that BIAGC is MIBOS. Therefore, we would like to numerically compare Theorem 2.2 ((2.18) and (2.19)) with TSB and Error Exponent Bound, shown in Figure 2.4, where the signal-to-noise ratio (snr) is 0dB and the word error probability is kept to be 10^{-2}. As can be seen, TSB is worse than Error Exponent Bound, while our jar decoding achievability is better than Error Exponent Bound in certain block length region.

General MIBOS Channel

A channel $\{p(y|x) : x \in \mathcal{X}, y \in \mathcal{Y}\}$ is MIBOS if $p(y|x)$ satisfies

$$p(y|0) = p(-y|1).$$

It is not hard to verify that any MIBOS channel is also a BIMC. In fact, it can be easily verified that

$$\text{MIBOS Channels} \subsetneq \text{BIMSC} \subsetneq \text{BIMC}\ .$$

To be more specific, the following venn diagram is provided, where weakly symmetric and strongly symmetric channels follow the definitions in [4]. As can be seen, BIMSC includes

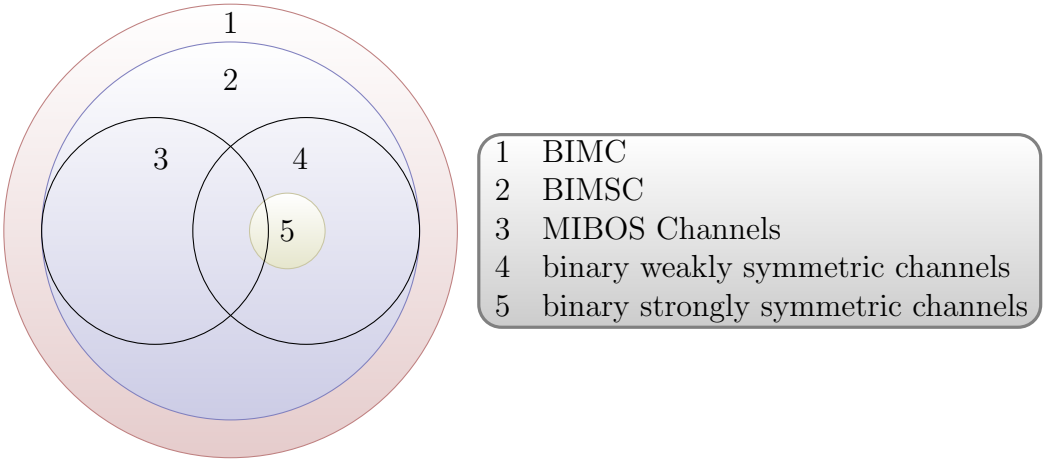


Figure 2.5: Venn Diagram of Symmetric Channels

both MIBOS channels and binary weakly symmetric channels, either of which can not include the other. Consequently, Theorem 2.2 can be applied. Moreover, for any MIBOS channel, by the same technique in the proof of Theorem 2.1, $C^{(i)}$ in Theorem 2.2 can be eliminated. On the other hand, although Poltyrev's Bound and Ashikhmin's Bound are very tight on BSC and BEC respectively, the extension of their proving technique on linear codes to general MIBOS channels is difficulty. Turning our attention to achievability of linear codes for general MIBOS channels, we see that Gallager [1] proved the following achievability result.

Result 2.9. *For any MIBOS channel, a linear code $\mathfrak{C}_{n,k}$ with hamming weight profile $\{N(l)\}_{l=1}^{n}$ and a function $f(y)$ satisfying $f(y) = f(-y)$ for any y and $f(y) > 0$ if $p(y|0) > 0$,*

$$P_e(\mathfrak{C}_{n,k}) \leq g(s)^n e^{-nsd} + e^{-nrd} \sum_{l=1}^{n} N(l)[h(r)]^l [g(r)]^{n-l} \tag{2.77}$$

for any $d \geq 0$, $s \geq 0$ *and* $r \leq 0$, *where*

$$g(s) = \int [p(y|0)]^{1-s}[f(y)]^s dy \tag{2.78}$$

$$h(r) = \int [p(y|0)p(-y|0)]^{\frac{1-r}{2}}[f(y)]^r dy. \tag{2.79}$$

Applying Result 2.9 to $\mathcal{C}_{n,k}^{(2)}$, Gallager [1] further obtained Result 2.10.

Result 2.10. *For any MIBOS channel,*

$$P_e(\mathcal{C}_{n,k}^{(2)}) \leq (1 + nC_n)e^{-n\left(E\left(\rho,\left(\frac{1}{2},\frac{1}{2}\right)\right)-\rho\mathcal{R}(\mathcal{C}_{n,k}^{(2)})\right)} \tag{2.80}$$

for $0 \leq \rho \leq 1$, *where* $\left(\frac{1}{2},\frac{1}{2}\right)$ *is the uniform distribution on binary alphabet and*

$$C_n = \max_{1\leq l\leq n} e^{-nH\left(\frac{l}{n}\right)} \begin{pmatrix} n \\ l \end{pmatrix}. \tag{2.81}$$

It can be easily verified that $E(\rho, Q) - \rho R$ achieves its maximum with respect to Q at the uniform distribution $\left(\frac{1}{2},\frac{1}{2}\right)$ when the channel is MIBOS. Result 2.10 was then improved by Shulman and Feder [26], who proved the result below.

Result 2.11. *For any MIBOS channel, a linear code* $\mathfrak{C}_{n,k}$ *with hamming weight profile* $\{N(l)\}_{l=1}^n$ *and* $0 \leq \rho \leq 1$,

$$P_e(\mathfrak{C}_{n,k}) \leq \left(\max_{1\leq l\leq n} \frac{N(l)2^n}{(2^k-1)\begin{pmatrix} n \\ l \end{pmatrix}} \right)^{\rho} e^{-n\left(E\left(\rho,\left(\frac{1}{2},\frac{1}{2}\right)\right)-\rho\mathcal{R}(\mathfrak{C}_{n,k})\right)}. \tag{2.82}$$

By observing x^ρ for $0 \leq \rho \leq 1$ is a concave function of x and therefore $\mathbb{E}[X^\rho] \leq (\mathbb{E}[X])^\rho$, the following result can be easily yielded from Result 2.11.

Result 2.12. *For any MIBOS channel,* $i = 1, 2$, *and* $0 \leq \rho \leq 1$,

$$P_e(\mathcal{C}_{n,k}^{(i)}) \leq e^{-n\left(E\left(\rho,\left(\frac{1}{2},\frac{1}{2}\right)\right)-\rho\mathcal{R}(\mathcal{C}_{n,k}^{(i)})\right)}. \tag{2.83}$$

Remark 2.8. *Strictly speaking, for* $1 \leq l \leq n$,

$$\mathbb{E}\left[\frac{N(l)2^n}{(2^k-1)\begin{pmatrix} n \\ l \end{pmatrix}}\right] = 1$$

for $\mathcal{C}_{n,k}^{(1)}$ *and*

$$\mathbb{E}\left[\frac{N(l)2^n}{(2^k-1)\begin{pmatrix} n \\ l \end{pmatrix}}\right] = \frac{1}{1-2^{-k}}$$

for $\mathcal{C}_{n,k}^{(2)}$. *However, the difference between* 1 *and* $\frac{1}{1-2^{-k}}$ *is numerically negligible in common settings of* k, *and therefore ignored here.*

Consequently, Gallager's Error Exponent Bound holds for Gallager's parity check and Elias' generator ensembles on MIBOS channels. It is worth mentioning that the symmetric property of MIBOS channel, i.e.

$$p(y|0) = p(-y|1)$$

is essential to the bounding techniques used in Result 2.9-2.12. To the our best knowledge, this is the best achievability in the literature for random linear code ensemble and general MIBOS channels. Meanwhile, on BSC, BEC and BIAGC, we have already shown that the achievability via jar decoding can be tighter than Error Exponent Bound.

Applicability (to ensembles and channels) and computational complexity of jar decoding achievability and existing achievability bounds on random linear coding ensembles in the literature are summerized in Table 2.1. Among all the listed results, Theorem 2.2 is the only achievability that can be applied to general BIMC and efficiently evaluated. Focusing on Gallager's ensemble, existing achievabilities only deal with MIBOS channels, which is a strict subset of BIMC. For some special MIBOS channels, e.g. BSC and BEC, there are bounds proved under ML decoding, which are better than the achievability under jar decoding in (2.70) and (2.74) by a small margin in the non-asymptotic regime. For general MIBOS channels, however, to the our best knowledge, Error Exponent Bound is best achievability result in the literature. And numerical calculation shows that the achievability in Theorem 2.2 can be tighter than Error Exponent Bound in the non-asymptotic regime.

Achievability		Applicability		Computational Complexity
		Linear Ensembles	BIMC	
Jar Decoding	(2.70)	$\surd$ Elias $\surd$ Gallager	BSC	$O(n)$
	(2.74)		BEC	$O(n)$
	Theorem 2.2		General	$O(1)$
Poltyrev	Result 2.5	$\surd$ Elias $\surd$ Gallager	BSC	$O(n)$
Ashikmin	Result 2.7	$\surd$ Elias $\surd$ Gallager (full rank)	BEC	$O(n^2)$
TSB	Result 2.8	$\surd$ Elias $\surd$ Gallager	BIAGC	$O(1)$
Error Exponent	Result 2.11	$\surd$ Elias $\surd$ Gallager	MIBOS	$O(1)$
RCU	[15, Theorem 33]	$\surd$ Elias $\times$ Gallager	BSC	$O(n)$
	Result 2.2		General	Unknown
DT	[15, Theorem 34]	$\surd$ Elias $\times$ Gallager	BSC	$O(n)$
	[15, Theorem 37]		BEC	$O(n)$
	Result 2.3		General	Unknown

Table 2.1: Achievabilities on Random Linear Codes and BIMC

2.4.2 Achievability on Shannon Random Code Ensemble With a Fixed Codeword Type

Technically speaking, when channel input is discrete, achievability on Shannon random code ensemble can be also applied to that with a fixed codeword type t, by restricting the input distribution in $\mathcal{T}_n^t$. In this case, however, neither input nor output distribution has the product form. Consequently, the evaluation of those achievable bounds becomes much more challenging. Taking Dependence Testing Bound in Result 2.3 as an example. When Shannon random code ensemble (without type constraint) is considered, the channel is memoryless (i.e. $p_{Y^n|X^n}(y^n|x^n) = \prod_{i=1}^n p(y_i|x_i)$ for some $p(y|x)$) and $p_{X^n}(x^n) = \prod_{i=1}^n p(x_i)$ for some $p(x)$, $p_{Y^n}(y^n) = \prod_{i=1}^n p(y_i)$ where $p(y) = \sum_{x\in\mathcal{X}} p(x)p(y|x)$. As a consequence, probabilities in (2.61) are probabilities of event of summation of an i.i.d sequences, which can be exactly evaluated with linear computation complexity with respect to n in certain special cases and estimated by certain bounds (e.g. NEP or Chernoff Bound) in general. Now applying Dependence Testing Bound to random coding ensemble with a fixed codeword type, let

$$p(x^n) = \begin{cases} \frac{1}{|\mathcal{T}_n^t|} & t(x^n) = t \\ 0 & \text{otherwise} \end{cases}.$$

It is then clear that the evaluation of probabilities in (2.61) becomes prohibitive as the computation complexity scales exponentially with respect to n. It is even hard to find a bound for those probabilities which can be easily computed, as they are no longer probabilities of event of summation of an i.i.d sequence. Similar discussion applies to Random Coding Union Bound in Result 2.2. In contrast, our achievability in Theorem 2.3 can be always easily computed. Therefore, in this subsection, we focus on those achievabilities on random code ensemble with a fixed codeword type, which allow easy evaluation.

First of all, let us compare Theorem 2.3 and Result 2.4. Strictly speaking, Result 2.4 is not applicable to random code ensemble with a fixed codeword type, as its proof uses deterministic construction of the channel code. Nevertheless, Result 2.4 can be used to show the existence of a code in this ensemble achieving the rate and the word error probability bound. Specifically, give a type t, let $\mathcal{F} = \mathcal{T}_t^n$ and $q_{Y^n}(y^n) = q_t(y^n) = \prod_{i=1}^n q_t(y_i)$. It is then easy to verify that $\beta_\alpha(x^n, q_t)$ is a constant (denoted by $\beta_\alpha(q_t)$) for any $x^n \in \mathcal{F}$. Consequently, the bound (2.65) reduces to

$$M \geq \sup_{0<\tau<P_e(\mathcal{C}_{t,n,k})} \frac{\kappa_\tau(\mathcal{T}_t^n, q_t)}{\beta_{1-P_e(\mathcal{C}_{t,n,k})+\tau}(q_t)}. \tag{2.84}$$

As $\kappa_\tau(\mathcal{T}_t^n, q_t)$ and $\beta_{1-\epsilon+\tau}(x^n, q_t)$ can not be efficiently evaluated in general, bounds on κ and β in (2.68) and (2.66) respectively are applied, yielding

$$\kappa_\tau(\mathcal{T}_t^n, q_t) \geq \tau e^{-nH(t)} |\mathcal{T}_t^n| \tag{2.85}$$

and $\forall x^n \in \mathcal{T}_t^n$,

$$\begin{aligned} \frac{1}{\beta_{1-P_e(\mathcal{C}_{t,n,k})+\tau}(x^n, q_t)} &\geq \sup\left\{\gamma : \Pr\left\{\frac{p(Y^n|x^n)}{q_t(Y^n)} \geq \gamma\right\} \geq 1 - P_e(\mathcal{C}_{t,n,k}) + \tau\right\} \\ &= \sup\left\{e^\gamma : \Pr\left\{\ln\frac{p(Y^n|x^n)}{q_t(Y^n)} < \gamma\right\} \leq P_e(\mathcal{C}_{t,n,k}) - \tau\right\} \\ &= \sup_{\delta: P_{t,\delta}^- \leq P_e(\mathcal{C}_{t,n,k})-\tau} e^{I(t;P)-\delta} \end{aligned} \tag{2.86}$$

where Y^n is the channel response to x^n. Now plug (2.85) and (2.86) into (2.84), take

logarithm and divide n on both sides, and we yield

$$\begin{aligned}\mathcal{R}(C_{t,n,k}) &\geq \sup_{0<\tau<P_e(\mathcal{C}_{t,n,k})} \sup_{\delta:P^-_{t,\delta}\leq P_e(\mathcal{C}_{t,n,k})-\tau} I(t;P) - \delta + \frac{\ln\tau + \ln e^{-nH(t)}|\mathcal{T}^n_t|}{n} \\ &= \sup_{\delta:P^-_{t,\delta}<P_e(\mathcal{C}_{t,n,k})} \sup_{0<\tau\leq P_e(\mathcal{C}_{t,n,k})-P^-_{t,\delta}} I(t;P) - \delta + \frac{\ln\tau + \ln e^{-nH(t)}|\mathcal{T}^n_t|}{n} \\ &= \sup_{\delta:P^-_{t,\delta}<P_e(\mathcal{C}_{t,n,k})} I(t;P) - \delta + \frac{\ln\left(P_e(\mathcal{C}_{t,n,k}) - P^-_{t,\delta}\right) + \ln e^{-nH(t)}|\mathcal{T}^n_t|}{n} \quad (2.87)\end{aligned}$$

which is equivalent to (2.43) in Theorem 2.3. Consequently, both Result 2.4 and Theorem 2.3 imply the existence of a channel code with a fixed codeword t achieving the trade-off between the rate and the word error probability in (2.43). And both of the results go beyond this existence in their own ways. Result 2.4 holds for maximal error probability, and the achievability (2.65) is tighter than (2.43) in general, although the evaluation of β and κ is quite challenging. Theorem 2.3, on the other hand, shows that the average coding performance (the rate and the word error probability) of random coding ensemble with a fixed codeword type can achieve (2.43), which implies the existence result, but not vice versa.

Next, we move on to the error exponent result, proved by Fano in [27].

Result 2.13. *For any discrete (input and output) memoryless channel* $P = \{p(y|x) : x \in \mathcal{X}, y \in \mathcal{Y}\}$ *and any* $t \in \mathcal{P}_n$,

$$P_e(\mathcal{C}_{t,n,k}) \leq \begin{cases} \left[1 + e^{nH(t)}|\mathcal{T}^n_t|^{-1}\right] e^{-na(t,s(t,\mathcal{R}(\mathcal{C}_{t,n,k})))} & R(t,0.5) < \mathcal{R}(\mathcal{C}_{t,n,k}) < I(t;P) \\ e^{nH(t)}|\mathcal{T}^n_t|^{-1} e^{-n(a(t,0.5)+R(t,0.5)-\mathcal{R}(\mathcal{C}_{t,n,k}))} & 0 \leq \mathcal{R}(\mathcal{C}_{t,n,k}) \leq R(t,0.5) \end{cases} \quad (2.88)$$

where

$$a(t,s) = \sum_{x\in\mathcal{X},y\in\mathcal{Y}} t(x)Q_s(y|x)\ln\frac{Q_s(y|x)}{p(y|x)} \text{ for } 0 \leq s \leq 0.5 \quad (2.89)$$

$$R(t,s) = \sum_{x\in\mathcal{X},y\in\mathcal{Y}} t(x)Q_s(y|x)\ln\frac{Q_s(y|x)}{Q_s(y)} \text{ for } 0 \leq s \leq 0.5 \quad (2.90)$$

$s(t,R)$ is the solution of s to $R(t,s) = R$ given t, and $Q_s(y)$ and $Q_s(y|x)$ are unconditional

and conditional probability distributions satisfying

$$Q_s(y|x) = \frac{[p(y|x)]^{1-s}[Q_s(y)]^s}{\sum_{y\in\mathcal{Y}}[p(y|x)]^{1-s}[Q_s(y)]^s} \tag{2.91}$$

$$Q_s(y) = \sum_{x\in\mathcal{X}} t(x)Q_s(y|x). \tag{2.92}$$

In the orignal version of Result 2.13, the term $e^{nH(t)}|\mathcal{T}_t^n|^{-1}$ is further upper bounded by $(2\pi n)^{|\mathcal{X}|/2}e^{|\mathcal{X}|/2}$. By defining

$$E_t(R) = \begin{cases} a(t, s(t, \mathcal{R}(\mathcal{C}_{t,n,k}))) & R(t,0.5) < \mathcal{R}(\mathcal{C}_{t,n,k}) < I(t;P) \\ a(t,0.5) + R(t,0.5) - \mathcal{R}(\mathcal{C}_{t,n,k}) & 0 \le \mathcal{R}(\mathcal{C}_{t,n,k}) \le R(t,0.5) \end{cases}, \tag{2.93}$$

it can be verified that

$$E_t(R) = \max_{0\le\rho\le 1} \max_{\substack{Q(y|x):\ \sum_y Q(y|x)=1 \\ Q(y|x)=0 \text{ if } p(y|x)=0}} -\sum_x t(x) \ln \left\{ \sum_y [p(y|x)]^{\frac{1}{1+\rho}} [Q(y)]^{\frac{\rho}{1+\rho}} \right\}^{1+\rho} - \rho R \tag{2.94}$$

where $Q(y) = \sum_x t(x)Q(y|x)$. Fano [27] then showed that

$$\max_t E_t(R) = \max_{0\le\rho\le 1} \max_Q E(\rho, Q) - \rho R \tag{2.95}$$

for $0 \le R < \max_t I(t;P)$ and

$$E_t(R) \ge \max_{0\le\rho\le 1} E(\rho, t) - \rho R \tag{2.96}$$

for general type t.

Towards numerical comparison between Result 2.13 and Theorem 2.3, we consider a special DIMC with discrete output, Z channel, shown in Figure 2.6. As can be seen, Z channel and BEC share some common properties. Consequently, the achievability via jar decoding in Theorem 2.3 can be further improved by providing a better bound on the size of jar $|J(y^n)|$ given a channel output y^n. Given a type t, the improved jar decoding achievability is shown below

$$P_e(\mathcal{C}_{t,n,k}) \le \sum_{i=0}^{m} \binom{m}{i} (1-p)^{m-i} p^i \min\left\{1, (M-1)\frac{\binom{n-m+i}{i}}{\binom{n}{m}}\right\} \tag{2.97}$$

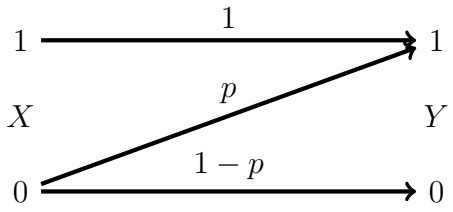
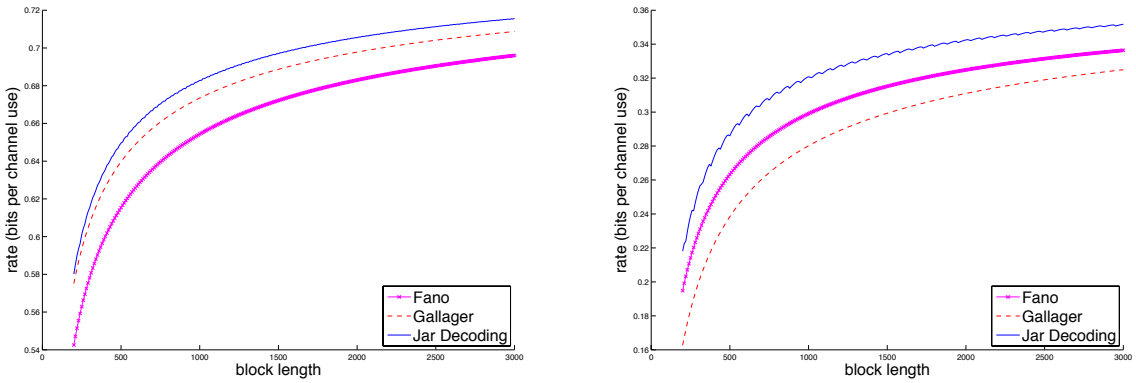


Figure 2.6: Z Channel

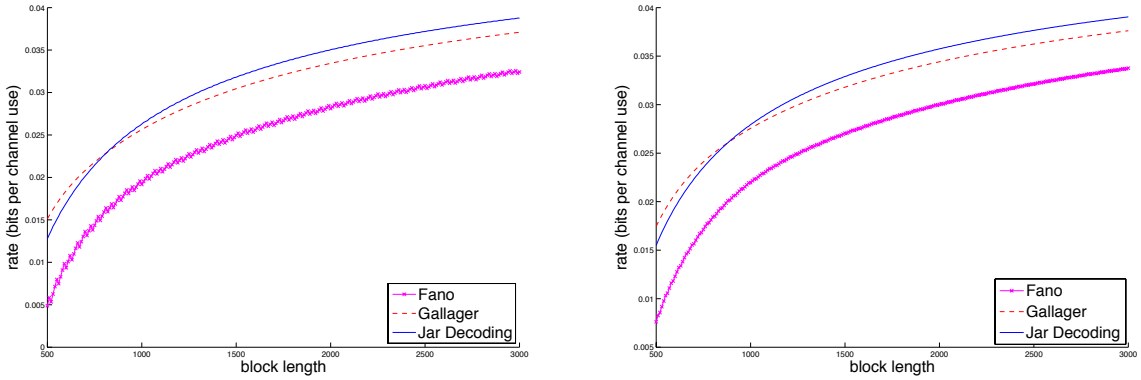
where $M = 2^{n\mathcal{R}(\mathcal{C}_{t,n,k})}$ and $m = t(0)n$. Then (2.97) (Jar Decoding) is numerically compared with Result 2.13 (Fano) on Z channel with different channel parameters p and input types t, where Result 2.1 (Gallager) on Shannon random code ensemble with input distributions corresponding to t serves as a benchmark.



(a) $t = (0.5, 0.5)$ (b) $t = (0.1, 0.9)$

Figure 2.7: Comparison of Achievability for Z Channel with $p = 0.5$ and $P_e = 10^{-3}$

As shown in Figures 2.7 and 2.8, jar decoding achievability constantly outperforms Fano's error exponent result. In addition, Figure 2.7 shows that due to the non-exponential term $\left[1 + e^{nH(t)}|\mathcal{T}_t^n|^{-1}\right]$ or $e^{nH(t)}|\mathcal{T}_t^n|^{-1}$, Fano's result could be worse than Gallager's, despite the relation of Fano's and Gallager's error exponent functions in (2.96). Meanwhile, in Figure 2.8, p_X represents the capacity achieving type, while t^* is some type calculated in a way specified in Chapter 4. A close look at Figure 2.8 then reveals that curves in (b) are above their counterparts in (a), which suggests that capacity achieving input type or distribution is not necessarily optimal in the non-asymptotic regime. Detailed discussion on this issue is delayed to Chapter 4.



(a) $t = p_X$ (b) $t = t^*$

Figure 2.8: Comparison of Achievability for Z Channel with $p = 0.9$ and $P_e = 10^{-3}$

To summarize, we compare the achievability via jar decoding for general DIMC with $\kappa\beta$ bound and Fano's Error Exponent Bound. As discussed above, $\kappa\beta$ bound, as an existence result, implies Theorem 2.3. However, since $\kappa\beta$ bound uses some deterministic construction of the channel codes in its proof, Theorem 2.3 is new on Shannon random code ensemble with a fixed codeword type. On the other hand, numerical calculation on Z channel shows that the achievability via jar decoding (an improved version of Theorem 2.3) is tighter than Fano's Error Exponent Bound in the non-asymptotic regime. Moreover, Fano's Error Exponent Bound is only applicable to the channel with discrete input and output, while Theorem 2.3 can be applied to channels with arbitrary (discrete or continuous) output as long as the input is discrete.

2.5 Summary

In this chapter, we establish several achievable channel coding theorems via jar decoding. In comparison with old decoding rules, jar decoding really makes the proof of achievable channel coding theorems simpler and easier. Given a channel and a code $\mathcal{C}_n$ of block length n for the channel, let X^n be the transmitted random codeword, and Y^n the corresponding channel output. Let $J(Y^n)$ be the jar formed for Y^n. The word error probability $P_e(\mathcal{C}_n)$ is

conveniently upper bounded by

$$\begin{aligned} P_e(\mathcal{C}_n) &\leq \Pr\{X^n \notin J(Y^n)\} \\ &\quad + \Pr\left\{\exists x^n \neq X^n, x^n \in J(Y^n), x^n \in \mathcal{C}_n, X^n \in J(Y^n)\right\} . \end{aligned} \tag{2.98}$$

For most codes, the first probability on the right side of (2.98) is actually independent of the codes themselves and can be nicely upper bounded for any n by using non-asymptotic equipartition properties with respect to different information quantities from [28]. For random linear codes based on either Elias' generator ensembles or Gallager's parity check ensembles and for Shannon random codes, the second probability on the right side of (2.98) is negligible in comparison with the first one when the code rate is very close to the channel capacity. With this, we have established non-asymptotic coding theorems for any block length n for random linear codes based on either Elias' generator ensembles or Gallager's parity check ensembles and for Shannon random codes, which reveal a complete picture about the tradeoff between the capacity gap and word error probability when the word error probability is a constant, or goes to 0 with block length n at a sub-polynomial $n^{-\alpha}$, $0 < \alpha < 1$, polynomial $n^{-\alpha}$, $\alpha \geq 1$, or sub-exponential $e^{-n^{\alpha}}$, $0 < \alpha < 1$, speed. For example, this complete tradeoff picture tells us that random linear codes of block length n can reach within $\sigma_H(X|Y)\sqrt{\frac{2\alpha \ln n}{n}} + \left(\alpha + \frac{1}{2}\right)\frac{\ln n}{n} + O\left(\frac{\ln \ln n}{n}\right)$ of the capacity of any BIMC while maintaining the word error probability $\frac{n^{-\alpha}}{2\sqrt{\pi \alpha \ln n}} + O\left(n^{-\alpha}\frac{\ln^{3/2} n}{\sqrt{n}}\right)$, and within $\frac{c}{\sqrt{n}} + \frac{\ln n}{2n} - \frac{1}{n}\ln\frac{(1-C_{BE})M_H(X|Y)}{\sigma_H^3(X|Y)}$ of the capacity while maintaining the word error probability $Q\left(\frac{c}{\sigma_H(X|Y)}\right) + \frac{M_H(X|Y)}{\sigma_H^3(X|Y)}\frac{1}{\sqrt{n}}$, where $\sigma_H^2(X|Y)$ is the conditional information variance of X given the channel output Y, $M_H(X|Y)$ is another parameter related to the channel, $Q(z) = \frac{1}{\sqrt{2\pi}}\int_z^{\infty} e^{-t^2/2}dt$, and $C_{BE} < 1$ is the universal constant in the Berry-Esseen central limit theorem. If the word error probability is kept slightly above 0.5, the code rate can be even slightly above the capacity! In the case of BSC with cross over probability $p = 0.12$, at the block length 1000, the word error probability is around 0.65, and the code rate is 0.21% above the capacity!

Those achievabilities in this chapter are shown to be surprisingly sharp in certain scenarios, considering the fact that jar decoding is not the optimal decoding rule. For example, we compare our achievable bounds based on random linear code ensembles with Dependent Testing bounds (one of the best achievable bounds in channel coding literature) based on Shannon random code ensemble in [15] for BSC and BEC channels, and the difference is quit insignificant. In addition, compared with asymptotic achievable and converse results in [15, 18, 19] when the error probability is fixed to be a constant, our achievable results based on random linear code ensemble for BIMC and Shannon random code ensemble with

a fixed codeword type for DIMC coincide with the optimal channel coding rate up to the second order ($\frac{1}{\sqrt{n}}$) with respect to n asymptotically. Therefore, it would be interesting to show how far the achievabilities proved via jar decoding is from the optimal channel coding rate in general settings. In the next chapter, we will attempt this problem by providing non-asymptotic converse coding theorems using the concept of jar.

Chapter 3

Non-asymptotic Converse Channel Coding Theorems

In this chapter, towards investigating the sharpness of achievabilities via jar decoding, we prove non-asymptotic converse theorems using the concept of jar. Specifically, we present a new converse proof technique dubbed *the outer mirror image of jar* and use the technique to establish new non-asymptotic converse coding theorems for any binary input memoryless symmetric channel (BIMSC) and any DIMC respectively.

3.1 Non-Asymptotic Converse Theorems: BIMSC

Consider a BIMC $\{p(y|x) : x \in \mathcal{X}, y \in \mathcal{Y}\}$, where $\mathcal{X} = \{0, 1\}$ is the channel input alphabet, and $\mathcal{Y}$ is the channel output alphabet, which is arbitrary and could be discrete or continuous. Throughout this section, let X denote the uniform random variable on $\mathcal{X}$ and Y the corresponding channel output of the BIMC in response to X. Then the capacity (in nats) of the BIMC is calculated by

$$C_{\text{BIMC}} = \ln 2 - H(X|Y) \tag{3.1}$$

where $H(X|Y)$ is the conditional entropy of X given Y. Further assume that the random variable $-\ln p(0|Y)$ given $X = 0$ and the random variable $-\ln p(1|Y)$ given $X = 1$ have the same distribution, where $p(0|Y)$ ($p(1|Y)$, respectively) denotes the conditional probability of $X = 0$ ($X = 1$, respectively) given Y. Such a BIMC is called a BIMSC. (It can be

verified that BSC, BEC, BIAGC, and general MBIOS channels all belong to the class of BIMSC.) Under this assumption, we have

$$\Pr\left\{-\frac{1}{n}\ln p(X^n|Y^n) > H(X|Y)+\delta \middle| X^n = x^n\right\} = \Pr\left\{-\frac{1}{n}\ln p(X^n|Y^n) > H(X|Y)+\delta\right\} \tag{3.2}$$

for any $x^n \in \mathcal{X}^n$, where Y^n is the output of the BIMSC in response to X^n, the n independent copies of X.

To present the converse theorems in this section, recall definitions in Section 1.4.1. In addition, following definitions are needed. Define for any $x^n \in \mathcal{X}^n$,

$$B(x^n,\delta) \stackrel{\Delta}{=} \left\{y^n : \infty > -\frac{1}{n}\ln p(x^n|y^n) > H(X|Y)+\delta\right\} \tag{3.3}$$

and

$$B_{n,\delta} \stackrel{\Delta}{=} \cup_{x^n\in\mathcal{X}^n} B(x^n,\delta). \tag{3.4}$$

Since for any $y^n \in \mathcal{Y}^n$, the following set

$$\left\{x^n \in \mathcal{X}^n : -\frac{1}{n}\ln p(x^n|y^n) \le H(X|Y)+\delta\right\} \tag{3.5}$$

is referred to as a BIMC jar for y^n in Chapters 1 and 2, we shall call $B(x^n,\delta)$ the *outer mirror image of jar* corresponding to x^n. Moreover, define for any set $B \subseteq \mathcal{Y}^n$,

$$P(B) \stackrel{\Delta}{=} \Pr\{Y^n \in B\} \tag{3.6}$$

$$P_{x^n}(B) \stackrel{\Delta}{=} \Pr\{Y^n \in B | X^n = x^n\}. \tag{3.7}$$

It is easy to see that

$$\begin{aligned} P_{x^n}(B(x^n,\delta)) &= \Pr\left\{-\frac{1}{n}\ln p(X^n|Y^n) > H(X|Y)+\delta \middle| X^n = x^n\right\} \\ &= \Pr\left\{-\frac{1}{n}\ln p(X^n|Y^n) > H(X|Y)+\delta\right\} \end{aligned} \tag{3.8}$$

where the last equality is due to (3.2).

We are now ready to state our non-asymptotic converse coding theorem for BIMSCs.

Theorem 3.1. *Given a BIMSC, for any channel code $\mathcal{C}_n$ of block length n with average word error probability $P_e(\mathcal{C}_n) = \epsilon_n$ and any $\beta_n > 0$,*

$$\mathcal{R}(\mathcal{C}_n) \leq C_{\text{BIMSC}} - \delta - \frac{\ln \epsilon_n + \ln \beta_n - \ln P(B_{n,\delta})}{n} \tag{3.9}$$

where δ is the largest number such that

$$(1+\beta_n)\,\epsilon_n \leq \Pr\left\{-\frac{1}{n}\ln p(X^n|Y^n) > H(X|Y) + \delta\right\}. \tag{3.10}$$

Moreover, the following hold:

1)

$$\mathcal{R}(\mathcal{C}_n) \leq C_{\text{BIMSC}} - \delta - \frac{\ln \epsilon_n - \ln P(B_{n,\delta}) + \frac{1}{2}\ln \frac{-2\ln \epsilon_n}{\sigma_H^2(X|Y)n}}{n} \tag{3.11}$$

where δ is the solution to

$$\left(1 + \frac{1}{\sigma_H(X|Y)}\sqrt{\frac{-2\ln \epsilon_n}{n}}\right)\epsilon_n = \underline{\xi}_H(X|Y,\lambda,n)e^{-nr_{X|Y}(\delta)} \tag{3.12}$$

with $\delta(\lambda) = \delta$.

2) When $\epsilon_n = \frac{e^{-n^\alpha}}{2\sqrt{\pi n^\alpha}}\left(1 - \frac{1}{2n^\alpha}\right)$ for $\alpha \in (0,1)$,

$$\mathcal{R}(\mathcal{C}_n) \leq C_{\text{BIMSC}} - \sqrt{2}\sigma_H(X|Y)n^{-\frac{1-\alpha}{2}} + O(n^{-(1-\alpha)}). \tag{3.13}$$

3) When $\epsilon_n = \frac{n^{-\alpha}}{2\sqrt{\pi\alpha\ln n}}\left(1 - \frac{1}{2\alpha\ln n}\right)$ for $\alpha > 0$,

$$\mathcal{R}(\mathcal{C}_n) \;\leq\; C_{\text{BIMSC}} - \sigma_H(X|Y)\sqrt{\frac{2\alpha\ln n}{n}} + O\left(\frac{\ln n}{n}\right). \tag{3.14}$$

4) When $\epsilon_n = \epsilon$ satisfying $\epsilon + \frac{1}{\sqrt{n}}\left(\frac{2\sqrt{-2\ln\epsilon}}{\sigma_H(X|Y)}\epsilon + \frac{C_{BE}M_H(X|Y)}{\sigma_H^3(X|Y)}\right) < 1$,

$$\begin{aligned}\mathcal{R}(\mathcal{C}_n) \;&\leq\; C_{\text{BIMSC}} - \frac{\ln\epsilon + \frac{1}{2}\ln\frac{-2\ln\epsilon}{\sigma_H^2(X|Y)n}}{n} \\ &\quad - \frac{\sigma_H(X|Y)}{\sqrt{n}}Q^{-1}\left(\epsilon + \frac{1}{\sqrt{n}}\left(\frac{\sqrt{-2\ln\epsilon}}{\sigma_H(X|Y)}\epsilon + \frac{C_{BE}M_H(X|Y)}{\sigma_H^3(X|Y)}\right)\right) \qquad (3.15)\\ &=\; C_{\text{BIMSC}} - \frac{\sigma_H(X|Y)}{\sqrt{n}}Q^{-1}(\epsilon) + \frac{\ln n}{2n} + O(n^{-1}). \qquad (3.16)\end{aligned}$$

Proof. Assume that the message M is uniformly distributed in $\mathcal{M} = \{1, 2, \ldots, e^{n\mathcal{R}(\mathcal{C}_n)}\}$, $x^n(m)$ is the codeword corresponding to the message m, and $\epsilon_{m,n}$ is the conditional error probability given message m. Then

$$\epsilon_n = \mathbb{E}[\epsilon_{M,n}] = e^{-n\mathcal{R}(\mathcal{C}_n)} \sum_{m=1}^{e^{n\mathcal{R}(\mathcal{C}_n)}} \epsilon_{m,n}. \tag{3.17}$$

Denote the decision region for message m as D_m. Then

$$\begin{aligned} P_{x^n(m)}(B(x^n(m),\delta) \cap D_m) &= P_{x^n(m)}(B(x^n(m),\delta)) - P_{x^n(m)}(B(x^n(m),\delta) \cap D_m^c) \\ &\geq P_{x^n(m)}(B(x^n(m),\delta)) - P_{x^n(m)}(D_m^c) \\ &= P_{x^n(m)}(B(x^n(m),\delta)) - \epsilon_{m,n} \\ &= \Pr\left\{-\frac{1}{n}\ln p(X^n|Y^n) > H(X|Y) + \delta\right\} - \epsilon_{m,n} \end{aligned} \tag{3.18}$$

where the last equality is due to (3.8). At this point, we select δ such that

$$\Pr\left\{-\frac{1}{n}\ln p(X^n|Y^n) > H(X|Y) + \delta\right\} \geq \epsilon_n(1+\beta_n). \tag{3.19}$$

By the fact that D_m are disjoint for different m and

$$\cup_{m\in\mathcal{M}} \left(B(x^n(m),\delta) \cap D_m\right) \subseteq B_{n,\delta}, \tag{3.20}$$

we have

$$
\begin{aligned}
P(B_{n,\delta}) &= \int_{B_{n,\delta}} p(y^n)dy^n \\
&\geq \sum_{m=1}^{e^{\mathcal{R}(\mathcal{C}_n)}} \int_{B(x^n(m),\delta)\cap D_m} p(y^n)dy^n \\
&= \sum_{m=1}^{e^{\mathcal{R}(\mathcal{C}_n)}} \int_{B(x^n(m),\delta)\cap D_m} \frac{p(y^n|x^n(m))p(x^n(m))}{p(x^n(m)|y^n)}dy^n \\
&\overset{1)}{\geq} \sum_{m=1}^{e^{\mathcal{R}(\mathcal{C}_n)}} \int_{B(x^n(m),\delta)\cap D_m} p(y^n|x^n(m))e^{n(-C_{\text{BIMSC}}+\delta)}dy^n \\
&= \sum_{m=1}^{e^{\mathcal{R}(\mathcal{C}_n)}} e^{n(-C_{\text{BIMSC}}+\delta)} \int_{B(x^n(m),\delta)\cap D_m} p(y^n|x^n(m))dy^n \\
&= e^{n(-C_{\text{BIMSC}}+\delta)} \sum_{m=1}^{e^{\mathcal{R}(\mathcal{C}_n)}} P_{x^n(m)}(B(x^n(m),\delta)\cap D_m) \\
&\overset{2)}{\geq} e^{n(-C_{\text{BIMSC}}+\delta)} \sum_{m=1}^{e^{\mathcal{R}(\mathcal{C}_n)}} \left[\Pr\left\{-\frac{1}{n}\ln p(X^n|Y^n) > H(X|Y)+\delta\right\} - \epsilon_{m,n}\right] \\
&\overset{3)}{=} e^{n(-C_{\text{BIMSC}}+\delta+\mathcal{R}(\mathcal{C}_n))} \left[\Pr\left\{-\frac{1}{n}\ln p(X^n|Y^n) > H(X|Y)+\delta\right\} - \epsilon_n\right] \\
&\overset{4)}{\geq} e^{n(-C_{\text{BIMSC}}+\delta+\mathcal{R}(\mathcal{C}_n))}\beta_n\epsilon_n
\end{aligned} \tag{3.21}
$$

where the inequality 1) is due to the definition of $B(x^n,\delta)$ given in (3.3), the inequality 2) follows from (3.18), the equality 3) comes from (3.17), and the inequality 4) is yielded by substituting (3.19). From (3.21), it follows that

$$
\mathcal{R}(\mathcal{C}_n) \leq C_{\text{BIMSC}} - \delta - \frac{\ln\beta_n + \ln\epsilon_n - \ln P(B_{n,\delta})}{n}, \tag{3.22}
$$

and therefore (3.9) and (3.10) are proved. Now let $\beta_n = \frac{1}{\sigma_H(X|Y)}\sqrt{\frac{-2\ln\epsilon_n}{n}}$.

1) By Result 1.1 in Section 1.4.1, part (b) of which says

$$\Pr\left\{-\frac{1}{n}\ln p(Y^n|X^n) > H(X|Y)+\delta\right\} \geq \underline{\xi}_H(X|Y,\lambda,n)e^{-nr_{X|Y}(\delta)}, \tag{3.23}$$

selecting δ to be the solution to (3.12) will make (3.19) satisfied, and therefore (3.11) is proved.

2) Towards proving (3.13), we want to show that by making $\delta = \sqrt{2}\sigma_H(X|Y)n^{-\frac{1-\alpha}{2}} - \eta n^{-(1-\alpha)}$ for some constant η,

$$\Pr\left\{-\frac{1}{n}p(X^n|Y^n) > H(X|Y)+\delta\right\} \geq \left(1+\frac{1}{\sigma_H(X|Y)}\sqrt{\frac{-2\ln\epsilon_n}{n}}\right)\epsilon_n \tag{3.24}$$

with $\epsilon_n = \frac{e^{-n^\alpha}}{2\sqrt{\pi n^\alpha}}\left(1-\frac{1}{2n^\alpha}\right)$. Then the proof follows essentially the same approach as that of (3.14), shown below in details.

3) Apply the trivial bound $P(B_{n,\delta}) \leq 1$. Then to show (3.14), we only have to show that $\delta = \sigma_H(X|Y)\sqrt{\frac{2\alpha\ln n}{n}} - \frac{\eta\ln n}{n}$ for some constant η can make

$$\begin{aligned}
&\Pr\left\{-\frac{1}{n}p(X^n|Y^n) > H(X|Y)+\delta\right\} \\
&\geq \underline{\xi}_H(X|Y,\lambda,n)e^{-nr_{X|Y}(\delta)} \\
&\geq \left(1+\eta_0\sqrt{\frac{\ln n}{n}}\right)\frac{n^{-\alpha}}{2\sqrt{\pi\alpha\ln n}}\left(1-\frac{1}{2\alpha\ln n}\right) \\
&\geq \left(1+\frac{1}{\sigma_H(X|Y)}\sqrt{\frac{-2\ln\epsilon_n}{n}}\right)\epsilon_n
\end{aligned} \tag{3.25}$$

satisfied, where $\lambda = r'_{X|Y}(\delta)$ and

$$\frac{1}{\sigma_H(X|Y,\lambda)}\sqrt{\frac{-2\ln\epsilon_n}{n}} = \Theta\left(\sqrt{\frac{\ln n}{n}}\right) \leq \eta_0\sqrt{\frac{\ln n}{n}} \tag{3.26}$$

for some constant η_0. Towards this, by part (a) of Result 1.1

$$r_{X|Y}(\delta) = \frac{1}{2\sigma_H^2(X|Y)}\delta^2 + O(\delta^3) \tag{3.27}$$

and the fact that

$$\underline{\xi}_H(X|Y,\lambda,n) = \Theta\left(\frac{1}{\sqrt{n}\lambda}\right) \tag{3.28}$$

when $\delta = o(1)$ and $\delta = \Omega(1/\sqrt{n})$,

$$\begin{aligned} e^{-nr_{X|Y}(\delta)} &= e^{-nr_{X|Y}\left(\sigma_H(X|Y)\sqrt{\frac{2\alpha\ln n}{n}}-\frac{\eta\ln n}{n}\right)} \\ &= e^{-n\left[\frac{1}{2\sigma_H^2(X|Y)}\left(\sigma_H(X|Y)\sqrt{\frac{2\alpha\ln n}{n}}-\frac{\eta\ln n}{n}\right)^2+O\left(\sqrt{\frac{\ln^3 n}{n^3}}\right)\right]} \\ &= e^{-\alpha\ln n+\frac{\eta}{\sigma_H(X|Y)}\sqrt{\frac{2\alpha\ln^3 n}{n}}-O\left(\sqrt{\frac{\ln^3 n}{n}}\right)} \\ &\geq e^{-\alpha\ln n+\left(\frac{\sqrt{2\alpha}\eta}{\sigma_H(X|Y)}-\eta_1\right)\sqrt{\frac{\ln^3 n}{n}}} \end{aligned} \tag{3.29}$$

for some constant η_1, and

$$\begin{aligned} &\underline{\xi}_H(X|Y,\lambda,n) \\ &= e^{\frac{n\lambda^2\sigma_H^2(X|Y,\lambda)}{2}}Q\left(\rho_*+\sqrt{n}\lambda\sigma_H(X|Y,\lambda)\right) \\ &\geq e^{\frac{n\lambda^2\sigma_H^2(X|Y,\lambda)}{2}}\frac{e^{-\frac{\left(\rho_*+\sqrt{n}\lambda\sigma_H(X|Y,\lambda)\right)^2}{2}}}{\sqrt{2\pi}(\rho_*+\sqrt{n}\lambda\sigma_H(X|Y,\lambda))}\left[1-\frac{1}{(\rho_*+\sqrt{n}\lambda\sigma_H(X|Y,\lambda))^2}\right] \\ &= \frac{e^{-\frac{\rho_*^2+2\rho_*\sqrt{n}\lambda\sigma_H(X|Y,\lambda)}{2}}}{\sqrt{2\pi}(\rho_*+\sqrt{n}\lambda\sigma_H(X|Y,\lambda))}\left[1-\frac{1}{(\rho_*+\sqrt{n}\lambda\sigma_H(X|Y,\lambda))^2}\right] \\ &\geq \frac{1}{2\sqrt{\pi\alpha\ln n}}\left(1-\frac{1}{2\alpha\ln n}\right)\left(1-\Theta\left(\sqrt{\frac{\ln n}{n}}\right)\right) \\ &\geq \frac{1}{2\sqrt{\pi\alpha\ln n}}\left(1-\frac{1}{2\alpha\ln n}\right)\left(1-\eta_2\sqrt{\frac{\ln n}{n}}\right) \end{aligned} \tag{3.30}$$

for another constant η_2, where $\rho_* = Q^{-1}\left(\frac{1}{2}-\frac{2C_{BE}M_H(X|Y,\lambda)}{\sqrt{n}\sigma_H^3(X|Y,\lambda)}\right) = \Theta\left(\frac{1}{\sqrt{n}}\right)$, and we utilize the fact that

$$\begin{aligned} \lambda &= r'_{X|Y}(\delta) \\ &= \frac{\delta}{\sigma_H^2(X|Y)}+O(\delta^2) \end{aligned} \tag{3.31}$$

$$\sigma_H(X|Y,\lambda) = \sigma_H(X|Y)\pm O(\lambda). \tag{3.32}$$

Then (3.25) is satisfied by choosing a constant η such that

$$\begin{aligned} & e^{\left(\frac{\sqrt{2\alpha}\eta}{\sigma_H(X|Y)}-\eta_1\right)\sqrt{\frac{\ln^3 n}{n}}}\left(1-\eta_2\sqrt{\frac{\ln n}{n}}\right) \\ \geq & \left[1+\left(\frac{\sqrt{2\alpha}\eta}{\sigma_H(X|Y)}-\eta_1\right)\sqrt{\frac{\ln^3 n}{n}}\right]\left(1-\eta_2\sqrt{\frac{\ln n}{n}}\right) \\ \geq & 1+\eta_0\sqrt{\frac{\ln n}{n}} \end{aligned} \tag{3.33}$$

for some constants η_0, η_1 and η_2.

4) According to (3.19), we should select δ such that

$$\Pr\left\{-\frac{1}{n}\ln p(X^n|Y^n) > H(X|Y)+\delta\right\} \geq \left(1+\frac{1}{\sigma_H(X|Y)}\sqrt{\frac{-2\ln\epsilon}{n}}\right)\epsilon. \tag{3.34}$$

Then by part (c) of Result 1.1,

$$\delta = \frac{\sigma_H(X|Y)}{\sqrt{n}}Q^{-1}\left(\epsilon+\frac{1}{\sqrt{n}}\left(\frac{\sqrt{-2\ln\epsilon}}{\sigma_H(X|Y)}\epsilon+\frac{M_H(X|Y)}{\sigma_H^3(X|Y)}\right)\right) \tag{3.35}$$

will guarantee (3.34). Consequently, (3.15) is proved by substituting (3.35) and $\epsilon_n = \epsilon$ into (3.22) and applying the trivial bound $P(B_{n,\delta}) \leq 1$, and (3.16) follows the fact that

$$Q^{-1}\left(\epsilon+\frac{1}{\sqrt{n}}\left(\frac{\sqrt{-2\ln\epsilon}}{\sigma_H(X|Y)}\epsilon+\frac{C_{BE}M_H(X|Y)}{\sigma_H^3(X|Y)}\right)\right) = Q^{-1}(\epsilon)-O\left(\frac{1}{\sqrt{n}}\right). \tag{3.36}$$

□

Remark 3.1. *It is clear that the above converse proof technique depends heavily on the concept of the outer mirror image of jar corresponding to codewords. To facilitate its future reference, it is beneficial to loosely call such a converse proof technique the outer mirror image of jar.*

Remark 3.2. *In general, the evaluation of $P(B_{n,\delta})$ may not be feasible, in which case the trivial bound $P(B_{n,\delta}) \leq 1$ can be applied without affecting the second order performance in the non-exponential error probability regime, as shown above. However, there are cases where $P(B_{n,\delta})$ can be tightly bounded (e.g. BEC, shown in section 4.3).*

Remark 3.3. *For the bound (3.15), when ϵ is small with respect to $\frac{1}{\sqrt{n}}$, $\frac{C_{BE}M_H(X|Y)}{\sqrt{n}\sigma_H^3(X|Y)}$ (the estimation error that comes from Berry-Esseen central limit theorem) will be dominant; in this case, (3.15) is loose.*

Remark 3.4. *The choice $\beta_n = \frac{1}{\sigma_H(X|Y)}\sqrt{\frac{-2\ln\epsilon_n}{n}}$ in the proof of Theorem 3.1 is not arbitrary. Actually, it is optimal when δ is small in the sense of minimizing the upper bound (3.9) in which δ depends on β_n through (3.10). To derive the expression for β_n, the following approximations can be adopted when δ is small:*

$$\frac{d\delta}{d\beta_n} \approx -\frac{2\beta_n\sigma_H^2(X|Y)}{n\delta} \tag{3.37}$$

$$\delta^2 \approx \frac{-2\sigma_H^2(X|Y)\ln\epsilon_n}{n} \tag{3.38}$$

where (3.37) and (3.38) can be developed from parts (a) and (b) of Result 1.1.

3.2 Non-Asymptotic Converse: DIMC

We now extend Theorems 3.1 to the case of DIMC $P = \{p(y|x), x \in \mathcal{X}, y \in \mathcal{Y}\}$, where $\mathcal{X}$ is discrete, but $\mathcal{Y}$ is arbitrary (discrete or continuous).

Recall definitions in Section 1.4.2. In addition, for any $t \in \mathcal{P}_n$ and any $x^n \in \mathcal{T}_t^n$, define

$$B_t(x^n, \delta) \triangleq \left\{ y^n : -\infty < \frac{1}{n}\ln\frac{p(y^n|x^n)}{q_t(y^n)} \le I(t;P) - \delta \right\} \tag{3.39}$$

and consequently

$$\begin{aligned} P_{x^n}(B_t(x^n,\delta)) &= \Pr\left\{ \frac{1}{n}\ln\frac{p(Y^n|X^n)}{q_t(Y^n)} \le I(t;P) - \delta \,\middle|\, X^n = x^n \right\} \\ &= P_{t,\delta} \end{aligned} \tag{3.40}$$

where $P_{t,\delta}$ only depends on type t and δ. Since for any $y^n \in \mathcal{Y}^n$, the following set

$$\left\{ x^n \in \mathcal{T}_t^n : \frac{1}{n}\ln\frac{p(y^n|x^n)}{q_t(y^n)} \ge I(t;P) - \delta \right\} \tag{3.41}$$

is referred to as a DIMC jar for y^n based on type t in Chapter 2, we shall call $B_t(x^n,\delta)$ the *outer mirror image of jar* corresponding to x^n. Further define

$$B_{t,n,\delta} \triangleq \cup_{x^n \in \mathcal{X}_t^n} B_t(x^n, \delta) \tag{3.42}$$

$$P(B_{t,n,\delta}) \stackrel{\Delta}{=} \int_{y^n \in B_{t,n,\delta}} q_t(y^n) dy^n. \tag{3.43}$$

For any channel code $\mathcal{C}_n$ of block length n with average word error probability $P_e(\mathcal{C}_n) = \epsilon_n$, assume that the message M is uniformly distributed in $\{1, 2, \ldots, e^{n\mathcal{R}(\mathcal{C}_n)}\}$. Let $x^n(m)$ be the codeword corresponding to the message m, and $\epsilon_{m,n}$ the conditional error probability given message m. Then

$$\epsilon_n = \mathbb{E}[\epsilon_{M,n}]. \tag{3.44}$$

Let $\beta_n = \sqrt{\frac{-2 \ln \epsilon_n}{n}}$ and

$$\mathcal{M} \stackrel{\Delta}{=} \{m : \epsilon_{m,n} \leq \epsilon_n(1 + \beta_n)\}. \tag{3.45}$$

Consider a type $t \in \mathcal{P}_n$ such that

$$|\{m \in \mathcal{M} : t(x^n(m)) = t\}| \geq \frac{|\mathcal{M}|}{(n+1)^{|\mathcal{X}|}}. \tag{3.46}$$

Since $|\mathcal{P}_n| \leq (n+1)^{|\mathcal{X}|}$, it follows from the pigeonhole principle that such a type $t \in \mathcal{P}_n$ exists. In other words, if we classify codewords in $\{x^n(m) : m \in \mathcal{M}\}$ according to their types, then there is at least one type $t \in \mathcal{P}_n$ such that the number of codewords in $\{x^n(m) : m \in \mathcal{M}\}$ with that type is not less than the average.

We are now ready to state our converse theorem for DIMC.

Theorem 3.2. *Given a DIMC, for any channel code $\mathcal{C}_n$ of block length n with average word error probability $P_e(\mathcal{C}_n) = \epsilon_n$,*

$$\begin{aligned} \mathcal{R}(\mathcal{C}_n) \quad \leq \quad & I(t; P) - \delta - \frac{\ln \epsilon_n - \ln P(B_{t,n,\delta})}{n} + |\mathcal{X}| \frac{\ln(n+1)}{n} \\ & - \frac{\ln \frac{-2 \ln \epsilon_n}{n} - \ln \left(1 + \sqrt{\frac{-2 \ln \epsilon_n}{n}}\right)}{n} \end{aligned} \tag{3.47}$$

for any $t \in \mathcal{P}_n$ satisfying (3.46), where δ is the largest number satisfying

$$\left(1 + 2\sqrt{\frac{-2 \ln \epsilon_n}{n}}\right) \epsilon_n \leq P_{t,\delta}. \tag{3.48}$$

Moreover, if a type $t \in \mathcal{P}_n$ satisfying (3.46) also satisfies (1.47) and (1.56), then the following hold:

1)

$$\begin{aligned}\mathcal{R}(\mathcal{C}_n) &\leq I(t;P) - \delta - \frac{\ln \epsilon_n - \ln P(B_{t,n,\delta})}{n} + |\mathcal{X}|\frac{\ln(n+1)}{n} \\ &\quad - \frac{\ln \frac{-2\ln \epsilon_n}{n} - \ln\left(1+\sqrt{\frac{-2\ln \epsilon_n}{n}}\right)}{n}\end{aligned} \tag{3.49}$$

where δ is the solution to

$$\left(1+2\sqrt{\frac{-2\ln \epsilon_n}{n}}\right)\epsilon_n = \underline{\xi}_{D,-}(t;P,\lambda,n)e^{-nr_-(t,\delta)} \tag{3.50}$$

with $\delta_-(t,\lambda)=\delta$.

2) When $\epsilon_n = \frac{e^{-n^\alpha}}{2\sqrt{\pi n^\alpha}}\left(1-\frac{1}{2n^\alpha}\right)$ for $\alpha \in (0,1)$,

$$\mathcal{R}(\mathcal{C}_n) \leq I(t;P) - \sqrt{2}\sigma_D(t;P)n^{-\frac{1-\alpha}{2}} + O(n^{-(1-\alpha)}). \tag{3.51}$$

3) When $\epsilon_n = \frac{n^{-\alpha}}{2\sqrt{\pi\alpha\ln n}}\left(1-\frac{1}{2\alpha\ln n}\right)$ for $\alpha > 0$,

$$\mathcal{R}(\mathcal{C}_n) \leq I(t;P) - \sigma_D(t;P)\sqrt{\frac{2\alpha\ln n}{n}} + O\left(\frac{\ln n}{n}\right). \tag{3.52}$$

4) When $\epsilon_n = \epsilon$ satisfying $\epsilon + \frac{1}{\sqrt{n}}\left(2\epsilon\sqrt{-2\ln\epsilon} + \frac{C_{BE}M_D(t;P)}{\sigma_D^3(t;P)}\right) < 1$,

$$\begin{aligned}\mathcal{R}(\mathcal{C}_n) &\leq I(t;P) - \frac{\sigma_D(t;P)}{\sqrt{n}}Q^{-1}\left(\epsilon + \frac{1}{\sqrt{n}}\left(2\epsilon\sqrt{-2\ln\epsilon} + \frac{C_{BE}M_D(t;P)}{\sigma_D^3(t;P)}\right)\right) \\ &\quad + (|\mathcal{X}|+1)\frac{\ln n}{n} - \frac{\ln\epsilon}{n} \qquad (3.53) \\ &= I(t;P) - \frac{\sigma_D(t;P)}{\sqrt{n}}Q^{-1}(\epsilon) + (|\mathcal{X}|+1)\frac{\ln n}{n} + O(n^{-1}). \qquad (3.54)\end{aligned}$$

Proof. We again apply the outer mirror image of jar converse-proof technique. By Markov inequality,

$$\Pr\{M \in \mathcal{M}\} \geq \frac{\beta_n}{1+\beta_n} \text{ and } |\mathcal{M}| \geq e^{n\mathcal{R}(\mathcal{C}_n)+\ln\frac{\beta_n}{1+\beta_n}}. \tag{3.55}$$

For any $t \in \mathcal{P}_n$ satisfying (3.46), let

$$\mathcal{M}_t \stackrel{\Delta}{=} \{m : \epsilon_{m,n} \leq \epsilon_n(1+\beta_n), t(x^n(m)) = t\}. \tag{3.56}$$

Then

$$|\mathcal{M}_t| \geq \frac{|\mathcal{M}|}{(n+1)^{|\mathcal{X}|}} \geq e^{n\mathcal{R}(\mathcal{C}_n)+\ln\frac{\beta_n}{1+\beta_n}-|\mathcal{X}|\ln(n+1)}. \tag{3.57}$$

Denote the decision region for message $m \in \mathcal{M}_t$ as D_m. Now for any $m \in \mathcal{M}_t$,

$$\begin{aligned} P_{x^n(m)}(B_t(x^n(m),\delta) \cap D_m) &= P_{x^n(m)}(B_t(x^n(m),\delta)) - P_{x^n(m)}(B_t(x^n(m),\delta) \cap D_m^c) \\ &\geq P_{x^n(m)}(B_t(x^n(m),\delta)) - \epsilon_{m,n} \\ &\geq P_{x^n(m)}(B_t(x^n(m),\delta)) - \epsilon_n(1+\beta_n). \end{aligned} \tag{3.58}$$

At this point, we select δ such that for any $x^n \in \mathcal{X}_t^n$,

$$P_{x^n}(B_t(x^n,\delta)) = P_{t,\delta} \geq \epsilon_n(1+2\beta_n). \tag{3.59}$$

Substituting (3.59) into (3.58), we have

$$P_{x^n(m)}(B_t(x^n(m),\delta) \cap D_m) \geq \beta_n\epsilon_n. \tag{3.60}$$

By the fact that D_m are disjoint for different m and

$$\cup_{m\in\mathcal{M}_t}(D_m \cap B_t(x^n(m),\delta)) \subseteq B_{t,n,\delta}, \tag{3.61}$$

we have

$$\begin{aligned} P(B_{t,n,\delta}) &= \int_{B_{t,n,\delta}} q_t(y^n)dy^n \\ &\geq \sum_{m\in\mathcal{M}_t} \int_{B(x^n(m),\delta)\cap D_m} q_t(y^n)dy^n \\ &\geq \sum_{m\in\mathcal{M}_t} \int_{B(x^n(m),\delta)\cap D_m} p(y^n|x^n(m))e^{-n(I(t;P)-\delta)}dy^n \\ &= \sum_{m\in\mathcal{M}_t} e^{-n(I(t;P)-\delta)} \int_{B(x^n(m),\delta)\cap D_m} p(y^n|x^n(m))dy^n \\ &= \sum_{m\in\mathcal{M}_t} e^{-n(I(t;P)-\delta)} P_{x^n(m)}(B(x^n(m),\delta)\cap D_m) \\ &\geq \sum_{m\in\mathcal{M}_t} e^{-n(I(t;P)-\delta)}\beta_n\epsilon_n = |\mathcal{M}_t|e^{-n(I(t;P)-\delta)}\beta_n\epsilon_n \end{aligned} \tag{3.62}$$

which implies that

$$|\mathcal{M}_t| \leq e^{n(I(t;P)-\delta)-\ln\beta_n-\ln\epsilon_n+\ln P(B_{t,n,\delta})}. \tag{3.63}$$

Then combining (3.57) and (3.63) yields

$$\mathcal{R}(\mathcal{C}_n) \leq I(t;P) - \delta - \frac{\ln\epsilon_n - \ln P(B_{t,n,\delta})}{n} - \frac{\ln\frac{\beta_n}{1+\beta_n}}{n} - \frac{\ln\beta_n}{n} + |\mathcal{X}|\frac{\ln(n+1)}{n}. \tag{3.64}$$

Since $\beta_n = \sqrt{\frac{-2\ln\epsilon_n}{n}}$ by definition, (3.47) and (3.48) directly come from (3.64) and (3.59).

1) According to part (b) of Result 1.2, i.e.

$$\Pr\left\{\frac{1}{n}\ln\frac{p(Y^n|X^n)}{q_t(Y^n)} \leq I(t;P) - \delta \middle| X^n = x^n\right\} \geq \underline{\xi}_{D,-}(t;P,\lambda,n)e^{-nr_-(t,\delta)} \tag{3.65}$$

it can be seen that selecting δ to be the solution to (3.50) will suffice (3.59). Consequently, (3.49) is proved.

2) The proof is essentially the same as that for part 2) of Theorem 3.1, where we can show that

$$P_{t,\delta} \geq \left(1 + 2\sqrt{\frac{-2\ln\epsilon_n}{n}}\right)\epsilon_n \tag{3.66}$$

when $\epsilon_n = \frac{e^{-n^\alpha}}{2\sqrt{\pi n^\alpha}}\left(1 - \frac{1}{2n^\alpha}\right)$ and $\delta = \sqrt{2}\sigma_D(t;P)n^{-\frac{1-\alpha}{2}} - \eta n^{-(1-\alpha)}$ for some constant η.

3) Apply the trivial bound $P(B_{t,n,\delta}) \leq 1$. Then similar to the proof for part 3) of Theorem 3.1, one can verify that by making $\delta = \sigma_{D,-}(t;P)\sqrt{\frac{2\alpha\ln n}{n}} - \eta\frac{\ln n}{n}$ for some properly chosen constant η,

$$\begin{aligned} P_{t,\delta} &\geq \underline{\xi}_{D,-}\left(t;P,\frac{\partial r_-(t,\delta)}{\partial\delta},n\right)e^{-nr_-(t,\delta)} \\ &\geq \left(1 + 2\sqrt{\frac{-2\ln\epsilon_n}{n}}\right)\epsilon \end{aligned} \tag{3.67}$$

for $\epsilon_n = \frac{n^{-\alpha}}{2\sqrt{\pi\alpha\ln n}}\left(1 - \frac{1}{2\alpha\ln n}\right)$.

4) According to (3.59), we should select δ such that

$$P_{t,\delta} \geq \left(1 + 2\sqrt{\frac{-2\ln\epsilon}{n}}\right)\epsilon. \tag{3.68}$$

Now by the part (c) of Result 1.2,

$$\delta = \frac{\sigma_D(t;P)}{\sqrt{n}} Q^{-1}\left(\epsilon + \frac{1}{\sqrt{n}}\left(2\epsilon\sqrt{-2\ln\epsilon} + \frac{C_{BE} M_D(t;P)}{\sigma_D^3(t;P)}\right)\right) \tag{3.69}$$

will guarantee (3.68). Consequently, (3.53) is proved by substituting (3.69) and $\epsilon_n = \epsilon$ into (3.64) and applying the trivial bound $P(B_{t,n,\delta}) \leq 1$, and (3.54) is yielded by the property of Q^{-1} function shown in the proof of Theorem 3.1.

□

Remark 3.5. *Remarks similar to Remarks 3.2 and 3.3 can be drawn here too for Theorem 3.2.*

Remark 3.6. *When channel codes are forced to consist of codewords with the same type t, converse bounds (3.47) and (3.48) can be improved. In particular, following the same approach used in the proof of Theorem 3.1, the term $|\mathcal{X}|\frac{\ln(n+1)}{n} + \frac{\ln\frac{-2\ln\epsilon_n}{n} - \ln\left(1+\sqrt{\frac{-2\ln\epsilon_n}{n}}\right)}{n}$ in (3.47) reduces to $\frac{\ln\beta_n}{n}$, while the requirement of δ in (3.48) is relaxed to*

$$(1+\beta_n)\,\epsilon_n \leq P_{t,\delta}, \tag{3.70}$$

where β_n can be further optimized.

For maximal error probability, we have the following corollary, the proof of which follows the same approach as that in the proof of Theorem 3.2.

Corollary 3.1. *Given a DIMC, for any channel code $\mathcal{C}_n$ of block length n with maximum error probability $P_m(\mathcal{C}_n) = \epsilon_n$,*

$$\mathcal{R}(\mathcal{C}_n) \leq I(t;P) - \delta - \frac{\ln\epsilon_n - \ln P(B_{t,n,\delta})}{n} + |\mathcal{X}|\frac{\ln(n+1)}{n} - \frac{\ln\sqrt{\frac{-2\ln\epsilon_n}{n}}}{n} \tag{3.71}$$

for any $t \in \mathcal{P}_n$ such that there are at least $(n+1)^{-|\mathcal{X}|}$ portion of codewords in $\mathcal{C}_n$ with type t, where δ is the largest number satisfying

$$\left(1 + \sqrt{\frac{-2\ln\epsilon_n}{n}}\right)\epsilon_n \leq P_{t,\delta}. \tag{3.72}$$

Moreover, if $t \in \mathcal{P}_n$ satisfies (1.47) and (1.56), then the following hold:

1)

$$\mathcal{R}(\mathcal{C}_n) \leq I(t;P) - \delta - \frac{\ln \epsilon_n - \ln P(B_{t,n,\delta})}{n} + |\mathcal{X}|\frac{\ln(n+1)}{n} - \frac{\ln \sqrt{\frac{-2\ln \epsilon_n}{n}}}{n} \tag{3.73}$$

where δ is the solution to

$$\left(1 + \sqrt{\frac{-2\ln \epsilon_n}{n}}\right)\epsilon_n = \underline{\xi}_{D,-}(t;P,\lambda,n)e^{-nr_-(t,\delta)} \tag{3.74}$$

with $\delta_-(t,\lambda) = \delta$.

2) When $\epsilon_n = \epsilon$ satisfying $\epsilon + \frac{1}{\sqrt{n}}\left(\epsilon\sqrt{-2\ln\epsilon} + \frac{C_{BE}M_D(t;P)}{\sigma_D^3(t;P)}\right) < 1$,

$$\begin{aligned}
\mathcal{R}(\mathcal{C}_n) &\leq I(t;P) - \frac{\sigma_D(t;P)}{\sqrt{n}}Q^{-1}\left(\epsilon + \frac{1}{\sqrt{n}}\left(\epsilon\sqrt{-2\ln\epsilon} + \frac{C_{BE}M_D(t;P)}{\sigma_D^3(t;P)}\right)\right) \\
&\quad + (|\mathcal{X}| + 0.5)\frac{\ln n}{n} - \frac{\ln \epsilon}{n} \qquad (3.75) \\
&= I(t;P) - \frac{\sigma_D(t;P)}{\sqrt{n}}Q^{-1}(\epsilon) + (|\mathcal{X}| + 0.5)\frac{\ln(n+1)}{n} + O(n^{-1}). \qquad (3.76)
\end{aligned}$$

3.3 Comparison with Existing Non-Asymptotic Converse Bounds

In this subsection, we would like to compare our converse with non-asymptotic converse bounds in the literature. Specifically, we focus on the best non-asymptotic converse bound so far, "meta-converse" proved in [15, Theorem 27]. Recall the definitions of $\beta_\alpha(q_1, q_2)$ and $\beta_\alpha(x^n, q_{Y^n})$ in Section 2.4, and meta-converse is stated below as Result 3.1.

Result 3.1. *Given any channel $\{p_{Y^n|X^n}(y^n|x^n) : x^n \in \mathcal{X}^n, y^n \in \mathcal{Y}^n\}$ and any channel code of block length n and codewords from a set $\mathcal{F} \subseteq \mathcal{X}^n$, let M and ϵ be the number of codewords and error probability of this channel code. Then*

$$M \leq \sup_{p_{X^n}} \inf_{q_{Y^n}} \frac{1}{\beta_{1-\epsilon}(p_{X^n}p_{Y^n|X^n}, p_{X^n}q_{Y^n})} \tag{3.77}$$

where the supremum and the infimum are taken over all distributions p_{X^n} on $\mathcal{F}$ and all distributions q_{Y^n} on $\mathcal{Y}^n$ respectively.

Result 3.1 is very general (applicable to any arbitrary input arbitrary output channel and channel codes with any input contraint), tight (involving three fold optimization in the n-dimensional space) and neat (in terms of quantities related to hypothesis testing). However, the evaluation of Result 3.1 is not feasible without any simplification. Towards this, the following result was proved [15, Theorem 28].

Result 3.2. *Adopt the assumption in Result 3.1. Furthermore, fix a q_{Y^n} and suppose that for any $x^n \in \mathcal{F}$, $\beta_{1-\epsilon}(x^n, q_{Y^n})$ is a constant, denoted by $\beta_{1-\epsilon}(q_{Y^n})$. Then*

$$M \leq \frac{1}{\beta_{1-\epsilon}(q_{Y^n})}. \tag{3.78}$$

Compared to Result 3.1, the difficulty of evaluation is mitigated in Result 3.2 when $\mathcal{F}$ and q_{Y^n} satisfy certain conditions. Nevertheless, the evaluation of $\beta_{1-\epsilon}(q_{Y^n})$ is still challenging as the calculation of optimal randomized testing $p_{Z|Y^n}$ in the definition of $\beta_\alpha(x^n, q_{Y^n})$ is difficult in general. Fortunately, it was shown in [15, Equation (106)] that

$$\begin{aligned} \beta_{1-\epsilon}(x^n, q_{Y^n}) &\geq \sup_{\gamma>0} \frac{1}{\gamma}\left(1-\epsilon-\Pr\left\{\frac{p_{Y^n|X^n}(Y^n|x^n)}{q_{Y^n}(Y^n)} \geq \gamma\right\}\right) \\ &= \sup_{\Gamma} e^{-n\Gamma}\left(\Pr\left\{\frac{1}{n}\ln\frac{p_{Y^n|X^n}(Y^n|x^n)}{q_{Y^n}(Y^n)} < \Gamma\right\} - \epsilon\right) \end{aligned} \tag{3.79}$$

where Y^n is the channel response to x^n. Then for any channel code $\mathcal{C}_n$ with $P_e(\mathcal{C}_n) \leq \epsilon$ and codewords from $\mathcal{F}$ satisfying that $\beta_{1-\epsilon}(p_{Y^n|X^n=x^n}, q_{Y^n})$ remains a constant for $x^n \in \mathcal{F}$, combining (3.78) and (3.79) yields

$$\mathcal{R}(\mathcal{C}_n) = \frac{1}{n}\ln M \leq \Gamma - \frac{\ln\left(\Pr\left\{\frac{1}{n}\ln\frac{p_{Y^n|X^n}(Y^n|x^n)}{q_{Y^n}(Y^n)} < \Gamma\right\} - \epsilon\right)}{n} \tag{3.80}$$

for any $x^n \in \mathcal{F}$ and any Γ satisfying

$$\Pr\left\{\frac{1}{n}\ln\frac{p_{Y^n|X^n}(Y^n|x^n)}{q_{Y^n}(Y^n)} < \Gamma\right\} > \epsilon. \tag{3.81}$$

Now for BIMSC, to make (3.80) and (3.81) applicable to any channel code, we can select $q_{Y^n}(y^n) = \prod_{i=1}^n \left[\frac{1}{2}p(y_i|0) + \frac{1}{2}p(y_i|1)\right]$ for any $y^n \in \mathcal{Y}^n$. It is then not hard to verify that $\beta_{1-\epsilon}(x^n, q_{Y^n})$ remains a constant for $x^n \in \mathcal{X}^n$, i.e. $\mathcal{F} = \mathcal{X}^n$. Under this circumstance, (3.80) and (3.81) are almost the same as (3.9) and (3.10) in Theorem 3.1 except that the term $\frac{\ln P(B_{n,\delta})}{n}$ is missing in (3.80). As $P(B_{n,\delta}) \leq 1$, it is shown that (3.80) and (3.81) under

this selection of $q_{Y^n}(y^n)$ are looser than Theorem 3.1 in general. In particular, shown in Section 4.3.2, $P(B_{n,\delta})$ can be bounded far away from 1 for BEC.

Similarly for DIMC, to make (3.80) and (3.81) applicable to any channel code with its codewords sharing the same type t, we can select $q_{Y^n}(y^n) = \prod_{i=1}^n q_t(y_i)$ for any $y^n \in \mathcal{Y}^n$. Then $\beta_{1-\epsilon}(x^n, q_{Y^n})$ remains a constant for $x^n \in \mathcal{T}_t^n$. Compared to Theorem 3.2 (improved according to Remark 3.6), it can be shown that Theorem 3.2 is tighter than (3.80) and (3.81) by the term $\frac{P(B_{t,n,\delta})}{n}$. For Z channel, $P(B_{t,n,\delta})$ is shown to be bounded far away from 1 in Section 4.3.3.

3.4 Summary

In this chapter, towards showing the sharpness of achievabilities established via jar decoding, we have developed a new converse proof technique dubbed the outer mirror image of jar and used it to establish new non-asymptotic converses for any discrete input memoryless channel with discrete or continuous output. Putting the achievabilities in Chapter 2 and the converses in this chapter together, it is evident that they agree on certain terms. For instance, part 2) of Theorem 2.2 for BIMC states that under the error probability $\epsilon = \frac{n^{-\alpha}}{2\sqrt{\pi\alpha \ln n}}(1 + o(1))$ requirement, the first two terms of achievable rate with respect to n are C_{BIMC} and $-\sigma_H(X|Y)\sqrt{\frac{2\alpha \ln n}{n}}$. On the other hand, from part 3) of Theorem 3.1, it can be seen that the optimal channel coding rate under any decoding rule for BIMSC (BIMC with certain symmetric properties) is bounded by $C_{\text{BIMC}} - \sigma_H(X|Y)\sqrt{\frac{2\alpha \ln n}{n}}$ plus some higher order terms with respect to n whenever the probability is $\frac{n^{-\alpha}}{2\sqrt{\pi\alpha \ln n}}\left(1 - \frac{1}{2\alpha \ln n}\right)$. The above discussion implies that jar decoding can achieve the optimal first and second order performance when the error probability is not too small. To make this discussion systematic and general, we consider second order analysis in non-asymptotic regime in the next chapter, where a taylor expansion of the optimal achievable channel coding rate is proposed. And combining achievabilities and converses via jar decoding, we determine the optimal first and second order channel coding performance in terms of this taylor expansion, and further show that jar decoding is indeed optimal up to the second order performance. In addition, some applications of this taylor expansion are also included in the next chapter.

Chapter 4

Taylor Expansion of Optimal Channel Coding Rate

Given a channel, let $R_n(\epsilon)$ denote the optimal achievable channel coding rate with the block length n subject to the error probability ϵ. Traditional asymptotic second order analysis of $R_n(\epsilon)$ [15, 18, 19, 29–31] is to investigate the first and second order of $R_n(\epsilon_n)$ with respect to n, where the error probability ϵ_n is considered to be either a constant or a function of n. In the non-asymptotic regime, however, treating the error probability as a constant or a function with respect to block length n is not convenient. For example, suppose that $n = 1000$ and the error probability ϵ is equal to 10^{-6}. How would one interpret the relationship between ϵ and n in this case? Does it make sense to interpret ϵ as a constant with respect to n? Or is it better to interpret ϵ as a polynomial function of n, namely, $\epsilon = n^{-2}$? In general, when both the error probability ϵ and block length n are finite, what really matters is their relative magnitude to each other, which should be characterized quantitatively.

In this chapter, we introduce a quantity $\delta_{t,n}(\epsilon)$ to measure the relative magnitude of the error probability ϵ and block length n with respect to a given channel and an input distribution t. By combining the achievability and converses via jar decoding and the outer mirror image of jar respectively, we show that when $\epsilon < 1/2$, the best channel coding rate $R_n(\epsilon)$ given n and ϵ has a "Taylor-type expansion" with respect to $\delta_{t,n}(\epsilon)$ in a neighbourhood of $\delta_{t,n}(\epsilon) = 0$, where the first two terms of the expansion are $\max_t[I(t;P) - \delta_{t,n}(\epsilon)]$, which is equal to $I(t^*,P) - \delta_{t^*,n}(\epsilon)$ for some optimal distribution t^*, and the third order term of the expansion is $O(\delta^2_{t^*,n}(\epsilon))$ whenever $\delta_{t^*,n}(\epsilon) = \Omega(\sqrt{\ln n/n})$. Since the leading two terms in the achievability of jar decoding coincide with the first two terms of

this Taylor-type expansion of $R_n(\epsilon)$, jar decoding is indeed optimal up to the second order coding performance in the non-asymptotical regime.

Furthermore, based on the Taylor-type expansion of $R_n(\epsilon)$ and our new non-asymptotic converses, we also derive two approximation formulas (dubbed "SO" and "NEP") for $R_n(\epsilon)$ in the non-asymptotic regime. The SO approximation formula consists only of the first two terms in the Taylor-type expansion of $R_n(\epsilon)$. On the other hand, in addition to the first two terms in the Taylor-type expansion of $R_n(\epsilon)$, the NEP approximation formula includes some higher order terms from our non-asymptotic converses as well. These formulas are further evaluated and compared against some of the best bounds known so far, as well as the normal approximation of $R_n(\epsilon)$ in [15]. It turns out that while the normal approximation is all over the map, i.e. sometime below achievability and sometime above converse, the SO approximation is much more reliable as it is always below converses; in the meantime, the NEP approximation is the best among the three and always provides an accurate estimation for $R_n(\epsilon)$. An important implication arising from the Taylor-type expansion of $R_n(\epsilon)$ is that in the practical non-asymptotic regime, the optimal marginal codeword symbol distribution is not necessarily a capacity achieving distribution.

4.1 Taylor-type Expansion: BIMSC

4.1.1 Taylor-type Expansion

In this subsection, we combine the non-asymptotic achievability given in (2.16) to (2.19) with the non-asymptotic converses given in (3.9) to (3.12) to derive a Taylor-type expansion of $R_n(\epsilon)$ in the non-asymptotic regime where both n and ϵ are finite. As mentioned early, when both n and ϵ are finite, what really matters is the relative magnitude of ϵ and n. As such, we begin with introducing a quantity $\delta_n(\epsilon)$ to measure the relative magnitude of ϵ and n with respect to the given BIMSC.

A close look at the non-asymptotic achievability given in (2.16) to (2.19) and the non-asymptotic converses given in (3.9) to (3.12) reveals that

$$\Pr\left\{-\frac{1}{n}\ln p(X^n|Y^n) > H(X|Y)+\delta\right\}$$

is crucial in both cases. According to part (b) of Result 1.1 in Section 1.4.1,

$$\begin{aligned}\Pr\left\{-\frac{1}{n}\ln p(X^n|Y^n) > H(X|Y)+\delta\right\} &\approx e^{\frac{n\lambda^2\sigma_H^2(X|Y,\lambda)}{2}} Q\left(\sqrt{n}\lambda\sigma_H(X|Y,\lambda)\right) e^{-nr_{X|Y}(\delta)} \\ &\triangleq g_{X|Y,n}(\delta) \end{aligned} \tag{4.1}$$

where $\lambda = r'_{X|Y}(\delta)$. Consequently, we would like to define $\delta_n(\epsilon)$ as the solution to

$$g_{X|Y,n}(\delta) = \epsilon \tag{4.2}$$

given n and $\epsilon \leq 1/2$, where the uniqueness of the solution in certain range is shown in Lemma 4.1.

Lemma 4.1. *There exists $\delta^+ > 0$ such that for any $n > 0$, $g_{X|Y,n}(\delta)$ is a strictly decreasing function of δ over $\delta \in [0, \delta^+]$.*

Proof. Since $\lambda = r'_{X|Y}(\delta)$, it follows that $g_{X|Y,n}(\delta) = g_{X|Y,n}(\delta(\lambda))$ is a function of λ through $\delta = \delta(\lambda)$. (For details about the properties of $\delta(\lambda)$ and $r_{X|Y}(\delta)$, please see Appendix A.) Moreover, by the fact that $\delta(0) = 0$ and $\delta(\lambda)$ is a strictly increasing function of λ, the proof of this lemma is yielded by analyzing the derivative of $g_{X|Y,n}(\delta(\lambda))$ with respect to λ around $\lambda = 0$. Towards this,

$$\begin{aligned}&\frac{dg_{X|Y,n}(\delta(\lambda))}{d\lambda} \\ &= \frac{d}{d\lambda}\left(e^{\frac{n\lambda^2\sigma_H^2(X|Y,\lambda)}{2}} Q\left(\sqrt{n}\lambda\sigma_H(X|Y,\lambda)\right)\right) e^{-nr_{X|Y}(\delta(\lambda))} \\ &\quad - e^{\frac{n\lambda^2\sigma_H^2(X|Y,\lambda)}{2}} Q\left(\sqrt{n}\lambda\sigma_H(X|Y,\lambda)\right) e^{-nr_{X|Y}(\delta(\lambda))} \frac{d}{d\lambda}\left(nr_{X|Y}(\delta(\lambda))\right) \\ &= e^{-nr_{X|Y}(\delta(\lambda))}\left\{\left[xe^{\frac{x^2}{2}}Q(x) - \frac{1}{\sqrt{2\pi}}\right]\frac{dx}{d\lambda} - e^{\frac{x^2}{2}}Q(x)n\left.\frac{dr_{X|Y}(\delta)}{d\delta}\right|_{\delta=\delta(\lambda)}\frac{d\delta(\lambda)}{d\lambda}\right\} \end{aligned} \tag{4.3}$$

where $x = \sqrt{n}\lambda\sigma_H(X|Y,\lambda)$. On one hand,

$$\begin{aligned}\frac{dx}{d\lambda} &= \sqrt{n}\left(\sigma_H(X|Y,\lambda) + \lambda\frac{d\sigma_H(X|Y,\lambda)}{d\lambda}\right) \\ &= \sqrt{n}\left(\sigma_H(X|Y,\lambda) + \frac{\lambda}{2\sigma_H(X|Y,\lambda)}\frac{d\sigma_H^2(X|Y,\lambda)}{d\lambda}\right). \end{aligned} \tag{4.4}$$

On the other hand,

$$\left.\frac{dr_{X|Y}(\delta)}{d\delta}\right|_{\delta=\delta(\lambda)} = \lambda \tag{4.5}$$

$$\frac{d\delta(\lambda)}{d\lambda} = \sigma_H^2(X|Y,\lambda) \tag{4.6}$$

which further implies

$$\begin{aligned} e^{\frac{x^2}{2}}Q(x)n\left.\frac{dr_{X|Y}(\delta)}{d\delta}\right|_{\delta=\delta(\lambda)}\frac{d\delta(\lambda)}{d\lambda} &= e^{\frac{x^2}{2}}Q(x)n\lambda\sigma_H^2(X|Y,\lambda) \\ &= \sqrt{n}\sigma_H(X|Y,\lambda)xe^{\frac{x^2}{2}}Q(x). \end{aligned} \tag{4.7}$$

Substituting (4.4) and (4.7) into (4.3), we have

$$\begin{aligned} &\frac{dg_{X|Y,n}(\delta(\lambda))}{d\lambda} \\ &= e^{-nr_{X|Y}(\delta(\lambda))}\left\{\left[xe^{\frac{x^2}{2}}Q(x)-\frac{1}{\sqrt{2\pi}}\right]\left(\frac{\sqrt{n}\lambda\frac{d\sigma_H^2(X|Y,\lambda)}{d\lambda}}{2\sigma_H(X|Y,\lambda)}\right)-\frac{\sqrt{n}\sigma_H(X|Y,\lambda)}{\sqrt{2\pi}}\right\} \\ &= e^{-nr_{X|Y}(\delta(\lambda))}\frac{\sqrt{n}\sigma_H(X|Y,\lambda)}{\sqrt{2\pi}}\left\{\left[\sqrt{2\pi}xe^{\frac{x^2}{2}}Q(x)-1\right]\left(\frac{\lambda\frac{d\sigma_H^2(X|Y,\lambda)}{d\lambda}}{2\sigma_H^2(X|Y,\lambda)}\right)-1\right\}. \end{aligned} \tag{4.8}$$

Note that

$$\begin{aligned} \sqrt{2\pi}xe^{\frac{x^2}{2}}Q(x) &< \sqrt{2\pi}xe^{\frac{x^2}{2}}\frac{1}{\sqrt{2\pi}x}e^{-\frac{x^2}{2}} \\ &= 1. \end{aligned} \tag{4.9}$$

If $\frac{d\sigma_H^2(X|Y,\lambda)}{d\lambda} \geq 0$, then

$$\left[\sqrt{2\pi}xe^{\frac{x^2}{2}}Q(x)-1\right]\left(\frac{\lambda\frac{d\sigma_H^2(X|Y,\lambda)}{d\lambda}}{2\sigma_H^2(X|Y,\lambda)}\right) \leq 0, \tag{4.10}$$

which further implies that $\frac{dg_{X|Y,n}(\delta(\lambda))}{d\lambda} < 0$. In the meantime, if $\frac{d\sigma_H^2(X|Y,\lambda)}{d\lambda} < 0$,

$$\begin{aligned}
&\left[\sqrt{2\pi}xe^{\frac{x^2}{2}}Q(x)-1\right]\left(\frac{\lambda\frac{d\sigma_H^2(X|Y,\lambda)}{d\lambda}}{2\sigma_H^2(X|Y,\lambda)}\right)-1\\
<&\left[\sqrt{2\pi}xe^{\frac{x^2}{2}}\frac{x}{\sqrt{2\pi}(1+x^2)}e^{-\frac{x^2}{2}}-1\right]\left(\frac{\lambda\frac{d\sigma_H^2(X|Y,\lambda)}{d\lambda}}{2\sigma_H^2(X|Y,\lambda)}\right)-1\\
=&-\frac{1}{1+x^2}\left(\frac{\lambda\frac{d\sigma_H^2(X|Y,\lambda)}{d\lambda}}{2\sigma_H^2(X|Y,\lambda)}\right)-1\\
=&-\frac{\lambda\frac{d\sigma_H^2(X|Y,\lambda)}{d\lambda}}{2\sigma_H^2(X|Y,\lambda)\left(1+n\lambda^2\sigma_H^2(X|Y,\lambda)\right)}-1. \qquad (4.11)
\end{aligned}$$

To continue, let us evaluate $\frac{d\sigma_H^2(X|Y,\lambda)}{d\lambda}$. From the definition of $\sigma_H^2(X|Y,\lambda)$, it is not hard to verify that

$$\frac{d\sigma_H^2(X|Y,\lambda)}{d\lambda}=\sum_{x\in\mathcal{X}}\int p(x,y)\frac{\partial f_\lambda(x,y)}{\partial\lambda}\ln^2 p(x|y)dy-2\sigma_H^2(X|Y,\lambda)\left(H(X)+\delta(\lambda)\right) \qquad (4.12)$$

where

$$\frac{\partial f_\lambda(x,y)}{\partial\lambda}=[-\ln p(x|y)-(H(X|Y)+\delta(\lambda))]f_\lambda(x,y). \qquad (4.13)$$

Plugging (4.13) into (4.12) yields

$$\begin{aligned}
&\frac{d\sigma_H^2(X|Y,\lambda)}{d\lambda}\\
=&\ \mathbb{E}\left(-\ln^3 p(X_\lambda|Y_\lambda)\right)-3\sigma_H^2(X|Y,\lambda)(H(X|Y)+\delta)-(H(X|Y)+\delta)^3\\
=&\ \hat{M}_H(X|Y,\lambda). \qquad (4.14)
\end{aligned}$$

Combining (4.8), (4.10), (4.11), and (4.14) together, we have

$$\begin{aligned}
&\frac{dg_{X|Y,n}(\delta(\lambda))}{d\lambda}\\
\le&\ e^{-nr_{X|Y}(\delta(\lambda))}\frac{\sqrt{n}\sigma_H(X|Y,\lambda)}{\sqrt{2\pi}}\left(\left|-\frac{\lambda\hat{M}_H(X|Y,\lambda)}{2\sigma_H^2(X|Y,\lambda)\left(1+n\lambda^2\sigma_H^2(X|Y,\lambda)\right)}\right|-1\right) \qquad (4.15)\\
\le&\ e^{-nr_{X|Y}(\delta(\lambda))}\frac{\sqrt{n}\sigma_H(X|Y,\lambda)}{\sqrt{2\pi}}\left(\left|-\frac{\lambda\hat{M}_H(X|Y,\lambda)}{2\sigma_H^2(X|Y,\lambda)}\right|-1\right). \qquad (4.16)
\end{aligned}$$

In view of the continuity of $\sigma_H^2(X|Y,\lambda)$ and $\hat{M}_H(X|Y,\lambda)$ as functions of λ, it is easy to see that there is a $\lambda^+ > 0$ such that for any $\lambda \in [0, \lambda^+]$,

$$\left| -\frac{\lambda \hat{M}_H(X|Y,\lambda)}{2\sigma_H^2(X|Y,\lambda)} \right| - 1 < 0$$

and hence

$$\frac{dg_{X|Y,n}(\delta(\lambda))}{d\lambda} < 0$$

for any $n \geq 0$. This completes the proof of Lemma 4.1 with $\delta^+ = \delta(\lambda^+)$. □

Remark 4.1. *From (4.15), it is clear that when n is large,*

$$\left| -\frac{\lambda \hat{M}_H(X|Y,\lambda)}{2\sigma_H^2(X|Y,\lambda)\left(1 + n\lambda^2\sigma_H^2(X|Y,\lambda)\right)} \right| - 1 < 0$$

and hence

$$\frac{dg_{X|Y,n}(\delta(\lambda))}{d\lambda} < 0$$

even for $\lambda \geq \lambda^+$. Nonetheless, as can be seen later, we are concerned only with the case where $\delta_n(\epsilon)$ is around 0. Consequently, the exact value of δ^+ is not important to us.

Remark 4.2. *In view of Lemma 4.1 and the definition of $\delta_n(\epsilon)$ in (4.1) and (4.2), it follows that $\delta_n(\frac{1}{2}) = 0$ for any n and any BIMSC. However, when $\epsilon < 1/2$, $\delta_n(\epsilon)$ depends not only on n and ϵ, but also on the BIMSC itself through the function $r_{X|Y}(\delta)$. Given n and $\epsilon < 1/2$, the value of $\delta_n(\epsilon)$ fluctuates a lot from one BIMSC to another through the behaviour of $r_{X|Y}(\delta)$ around $\delta = 0$, which depends on both the second and third order derivatives of $r_{X|Y}(\delta)$.*

With respect to $\delta_n(\epsilon)$, $R_n(\epsilon)$ has a nice Taylor-type expansion, as shown in Theorem 4.1.

Theorem 4.1. *Given a BIMSC, for any n and ϵ satisfying $g_{X|Y,n}(\delta^+/2) \leq \epsilon < 1$,*

$$|R_n(\epsilon) - (C_{\text{BIMSC}} - \delta_n(\epsilon))| \leq o\left(\delta_n(\epsilon)\right) \tag{4.17}$$

where

$$o\left(\delta_n(\epsilon)\right) \;=\; r_{X|Y}(\delta_n(\epsilon)) + \frac{\frac{1}{2}\ln n + d_1}{n} \tag{4.18}$$

if $\epsilon \leq \frac{1}{3}$, *and*

$$\left| R_n(\epsilon) - \left(C_{\text{BIMSC}} - \frac{\sigma_H(X|Y)}{\sqrt{n}} Q^{-1}(\epsilon) \right) \right| \leq \frac{\frac{1}{2}\ln n + d_2}{n} \tag{4.19}$$

otherwise, where d_1 *and* d_2 *are channel parameters independent of both* n *and* ϵ.

Proof. When $\epsilon > \frac{1}{3}$, (4.19) can be easily proved by combining (2.22), (2.23) and (3.15). Therefore, it suffices for us to show (4.17) and (4.18) for $\epsilon \leq \frac{1}{3}$. By (2.18), (2.19) and definition of $\bar{\xi}_H(X|Y,\lambda,n)$, for any BIMSC there exists a channel code $\mathcal{C}_n$ such that

$$\begin{aligned} P_e(\mathcal{C}_n) &\leq \left(\bar{\xi}_H(X|Y,\lambda,n) + \frac{2(1-C_{BE})M_H(X|Y,\lambda)}{\sqrt{n}\sigma_H^3(X|Y,\lambda)} \right) e^{-nr_{X|Y}(\delta)} \\ &\leq g_{X|Y,n}(\delta) + \frac{2M_H(X|Y,\lambda)}{\sqrt{n}\sigma_H^3(X|Y,\lambda)} e^{-nr_{X|Y}(\delta)} \end{aligned} \tag{4.20}$$

and

$$\mathcal{R}(\mathcal{C}_n) \geq C_{\text{BIMSC}} - \delta + \frac{\ln\left[\frac{2(1-C_{BE})M_H(X|Y,\lambda)}{\sqrt{n}\sigma_H^3(X|Y,\lambda)} e^{-nr_{X|Y}(\delta)}\right]}{n} \tag{4.21}$$

which implies that for any δ such that

$$g_{X|Y,n}(\delta) + \frac{2M_H(X|Y,\lambda)}{\sqrt{n}\sigma_H^3(X|Y,\lambda)} e^{-nr_{X|Y}(\delta)} \leq \epsilon \tag{4.22}$$

the following inequality holds

$$R_n(\epsilon) \geq C_{\text{BIMSC}} - \delta + \frac{\ln\left[\frac{2(1-C_{BE})M_H(X|Y,\lambda)}{\sqrt{n}\sigma_H^3(X|Y,\lambda)} e^{-nr_{X|Y}(\delta)}\right]}{n} \tag{4.23}$$

where $\lambda = r'_{X|Y}(\delta)$. Now let $\bar{\delta} = \delta_n(\epsilon) + \frac{\eta}{n}$ for some constant $\eta > 0$, which will be specified later, and $\bar{\lambda} = r'_{X|Y}(\bar{\delta})$. By convexity of $r_{X|Y}(\delta)$,

$$r_{X|Y}(\bar{\delta}) \geq r_{X|Y}(\delta_n(\epsilon)) + \lambda_n(\epsilon)\frac{\eta}{n} \tag{4.24}$$

where $\lambda_n(\epsilon) = r'_{X|Y}(\delta_n(\epsilon))$. Then

$$
\begin{aligned}
& g_{X|Y,n}(\bar{\delta}) + \frac{2M_H(X|Y,\bar{\lambda})}{\sqrt{n}\sigma_H^3(X|Y,\bar{\lambda})} e^{-nr_{X|Y}(\bar{\delta})} \\
\overset{1)}{\leq} & \left(e^{\frac{n\bar{\lambda}^2\sigma_H^2(X|Y,\bar{\lambda})}{2}} Q\left(\sqrt{n}\bar{\lambda}\sigma_H(X|Y,\bar{\lambda})\right) + \frac{2M_H(X|Y,\bar{\lambda})}{\sqrt{n}\sigma_H^3(X|Y,\bar{\lambda})} \right) e^{-n\left(r_{X|Y}(\delta_n(\epsilon))+\lambda_n(\epsilon)\frac{\eta}{n}\right)} \\
= & \left(1 + \frac{\frac{2M_H(X|Y,\bar{\lambda})}{\sqrt{n}\sigma_H^3(X|Y,\bar{\lambda})}}{e^{\frac{n\bar{\lambda}^2\sigma_H^2(X|Y,\bar{\lambda})}{2}} Q\left(\sqrt{n}\bar{\lambda}\sigma_H(X|Y,\bar{\lambda})\right)} \right) e^{\frac{n\bar{\lambda}^2\sigma_H^2(X|Y,\bar{\lambda})}{2}} Q\left(\sqrt{n}\bar{\lambda}\sigma_H(X|Y,\bar{\lambda})\right)) \\
& \times e^{-nr_{X|Y}(\delta_n(\epsilon))-\eta\lambda_n(\epsilon)} \\
\overset{2)}{\leq} & \left(1 + \frac{2M_H(X|Y,\bar{\lambda})\sqrt{2\pi}\bar{\lambda}\left(1+\frac{1}{n\bar{\lambda}^2\sigma_H^2(X|Y,\bar{\lambda})}\right)}{\sigma_H^2(X|Y,\bar{\lambda})} \right) \\
& \times e^{\frac{n\lambda_n^2(\epsilon)\sigma_H^2(X|Y,\lambda_n(\epsilon))}{2}} Q\left(\sqrt{n}\lambda_n(\epsilon)\sigma_H(X|Y,\lambda_n(\epsilon))\right) e^{-nr_{X|Y}(\delta_n(\epsilon))-\eta\lambda_n(\epsilon)} \\
= & g_{X|Y,n}\left(\delta_n(\epsilon)\right) e^{-\eta\lambda_n(\epsilon)} \left(1 + \frac{2\sqrt{2\pi}M_H(X|Y,\bar{\lambda})\left(1+\frac{1}{n\bar{\lambda}^2\sigma_H^2(X|Y,\bar{\lambda})}\right)}{\sigma_H^2(X|Y,\bar{\lambda})}\bar{\lambda} \right) \\
\overset{3)}{=} & \epsilon e^{-\eta\lambda_n(\epsilon)} \left(1 + \frac{2\sqrt{2\pi}M_H(X|Y,\bar{\lambda})\left(1+\frac{1}{n\bar{\lambda}^2\sigma_H^2(X|Y,\bar{\lambda})}\right)}{\sigma_H^2(X|Y,\bar{\lambda})} \left(\lambda_n(\epsilon) + \frac{1}{\sigma_H^2(X|Y,\tilde{\lambda})}\frac{\eta}{n}\right) \right) \\
\overset{4)}{\leq} & \epsilon \frac{1 + \frac{2\sqrt{2\pi}M_H(X|Y,\bar{\lambda})\left(1+\frac{1}{n\bar{\lambda}^2\sigma_H^2(X|Y,\bar{\lambda})}\right)}{\sigma_H^2(X|Y,\bar{\lambda})} \left(\lambda_n(\epsilon) + \frac{1}{\sigma_H^2(X|Y,\bar{\lambda})}\frac{\eta}{n}\right)}{1 + \eta\lambda_n(\epsilon) + \frac{1}{2}\eta^2\lambda_n^2(\epsilon)} .
\end{aligned}
\tag{4.25}
$$

In the derivation of (4.25), the inequality 1) is due to (4.24); the inequality 2) follows from the fact that $e^{\frac{x^2}{2}}Q(x)$ is a strictly decreasing function of x, $\lambda\sigma_H(X|Y,\lambda)$ is strictly

increasing with respect to λ as shown below

$$\begin{aligned}\frac{d\lambda\sigma_H(X|Y,\lambda)}{d\lambda} &= \sigma_H(X|Y,\lambda)+\lambda\frac{d\sigma_H(X|Y,\lambda)}{d\lambda}\\ &= \sigma_H(X|Y,\lambda)\left(1+\lambda\frac{\frac{d\sigma_H^2(X|Y,\lambda)}{d\lambda}}{2\sigma_H^2(X|Y,\lambda)}\right)\\ &= \sigma_H(X|Y,\lambda)\left(1+\lambda\frac{\hat{M}_H(X|Y,\lambda)}{2\sigma_H^2(X|Y,\lambda)}\right)\\ &> 0 \end{aligned} \tag{4.26}$$

for $\lambda\in[0,\lambda^+]$, and

$$e^{\frac{x^2}{2}}Q(x)\geq\frac{x}{\sqrt{2\pi}(1+x^2)}; \tag{4.27}$$

the equality 3) is attributable to

$$\bar{\lambda}=\lambda_n(\epsilon)+\left.\frac{d\lambda}{d\delta}\right|_{\lambda=\tilde{\lambda}}\frac{\eta}{n}=\lambda_n(\epsilon)+\frac{1}{\sigma_H^2(X|Y,\tilde{\lambda})}\frac{\eta}{n} \tag{4.28}$$

for some $\tilde{\lambda}\in[\lambda_n(\epsilon),\bar{\lambda}]$; and finally, the inequality 4) follows from the inequality

$$e^x>1+x+\frac{x^2}{2}$$

for any $x>0$. In order to satisfy (4.22), let us now choose η such that

$$\eta\lambda_n(\epsilon)\geq\frac{2\sqrt{2\pi}M_H(X|Y,\bar{\lambda})\left(1+\frac{1}{n\bar{\lambda}^2\sigma_H^2(X|Y,\bar{\lambda})}\right)}{\sigma_H^2(X|Y,\bar{\lambda})}\lambda_n(\epsilon) \tag{4.29}$$

and

$$\frac{1}{2}\eta^2\lambda_n^2(\epsilon)\geq\frac{2\sqrt{2\pi}M_H(X|Y,\bar{\lambda})\left(1+\frac{1}{n\bar{\lambda}^2\sigma_H^2(X|Y,\bar{\lambda})}\right)}{\sigma_H^2(X|Y,\bar{\lambda})}\frac{1}{\sigma_H^2(X|Y,\tilde{\lambda})}\frac{\eta}{n}, \tag{4.30}$$

i.e.

$$\eta=\frac{2\sqrt{2\pi}M_H(X|Y,\bar{\lambda})\left(1+\frac{1}{n\bar{\lambda}^2\sigma_H^2(X|Y,\bar{\lambda})}\right)}{\sigma_H^2(X|Y,\bar{\lambda})}\max\left\{1,\frac{2}{n\lambda_n^2(\epsilon)\sigma_H^2(X|Y,\tilde{\lambda})}\right\}. \tag{4.31}$$

To see η is bounded, note that $\frac{M_H(X|Y,\lambda)}{\sigma_H^2(X|Y,\lambda)}$ is always bounded for $\lambda \in [0, \lambda^+]$. On the other hand, for $\epsilon \leq \frac{1}{3}$, $\sqrt{n}\lambda_n(\epsilon)\sigma_H(X|Y, \lambda_n(\epsilon)) > c$ for some constant c, as

$$\sqrt{n}\lambda_n(\epsilon)\sigma_H(X|Y, \lambda_n(\epsilon)) \to 0 \Rightarrow \epsilon = g_{X|Y,n}(\delta_n(\epsilon)) \to \frac{1}{2},$$

and the same argument can be applied to $\sqrt{n}\lambda_n(\epsilon)\sigma_H^2(X|Y, \tilde{\lambda})$. Therefore,

$$\eta \;\leq\; 2\sqrt{2\pi} \max_{\lambda\in[0,\lambda^+]} \left[\frac{M_H(X|Y,\lambda)}{\sigma_H^2(X|Y,\lambda)}\right] \left(1 + c^{-2}\right) \max\left\{1, 2c^{-2}\right\}. \tag{4.32}$$

Then combining (4.22), (4.23), (4.24), (4.25), (4.29) and (4.30) yields

$$\begin{aligned}
R_n(\epsilon) \;&\geq\; C_{\text{BIMSC}} - \bar{\delta} + \frac{\ln\left[\frac{2(1-C_{BE})M_H(X|Y,\bar{\lambda})}{\sqrt{n}\sigma_H^3(X|Y,\bar{\lambda})} e^{-nr_{X|Y}(\bar{\delta})}\right]}{n} \\
&=\; C_{\text{BIMSC}} - \bar{\delta} - r_{X|Y}(\bar{\delta}) + \frac{\ln\left[\frac{2(1-C_{BE})M_H(X|Y,\bar{\lambda})}{\sigma_H^3(X|Y,\bar{\lambda})}\right] - \frac{1}{2}\ln n}{n} \\
&\overset{1)}{\geq}\; C_{\text{BIMSC}} - \delta_n(\epsilon) - r_{X|Y}(\delta_n(\epsilon)) - \bar{\lambda}\frac{\eta}{n} + \frac{\ln\left[\frac{2(1-C_{BE})M_H(X|Y,\bar{\lambda})}{\sigma_H^3(X|Y,\bar{\lambda})}\right] - \eta - \frac{1}{2}\ln n}{n} \\
&\geq\; C_{\text{BIMSC}} - \delta_n(\epsilon) - r_{X|Y}(\delta_n(\epsilon)) \\
&\quad + \frac{-\lambda^+\eta + \ln\left[2(1-C_{BE})\min_\lambda\left(\frac{2M_H(X|Y,\lambda)}{\sigma_H^3(X|Y,\lambda)}\right)\right] - \eta - \frac{1}{2}\ln n}{n} \\
&=\; C_{\text{BIMSC}} - \delta_n(\epsilon) - r_{X|Y}(\delta_n(\epsilon)) - \frac{\frac{1}{2}\ln n + \bar{d}_1}{n},
\end{aligned} \tag{4.33}$$

where $\bar{d}_1$ is independent of both n and ϵ. In the derivation of (4.33), the inequality 1) follows from the convexity of $r_{X|Y}(\delta)$ and the fact that

$$r_{X|Y}(\bar{\delta}) \leq r_{X|Y}(\delta_n(\epsilon)) + \bar{\lambda}\frac{\eta}{n}.$$

We now proceed to establish an upper bound on $R_n(\epsilon)$. Towards this end, recall (3.9) and (3.10) where we choose $\beta_n = \lambda = r'_{X|Y}(\delta)$. Then for any δ such that

$$(1+\lambda)\,\epsilon \leq \underline{\xi}_H(X|Y, \lambda, n)e^{-nr_{X|Y}(\delta)} \tag{4.34}$$

we have

$$\begin{aligned}
R_n(\epsilon) \;&\leq\; C_{\text{BIMSC}} - \delta - \frac{\ln\epsilon - \ln P(B_{n,\delta}) + \ln\lambda}{n} \\
&\leq\; C_{\text{BIMSC}} - \delta + \frac{-\ln\epsilon - \ln\lambda}{n}
\end{aligned} \tag{4.35}$$

where the trivial bound $P(B_{n,\delta}) \leq 1$ is applied. Now let $\underline{\delta} = \delta_n(\epsilon) - \frac{\eta'}{n}$ for some constant $\eta' > 0$, which will be specified later, and $\underline{\lambda} = r'_{X|Y}(\underline{\delta})$. Then

$$\begin{aligned}
&\underline{\xi}_H(X|Y,\underline{\lambda},n)e^{-nr_{X|Y}(\underline{\delta})} \\
&\overset{1)}{\geq} e^{\frac{n\underline{\lambda}^2\sigma_H^2(X|Y,\underline{\lambda})}{2}} Q\left(\rho_* + \sqrt{n}\underline{\lambda}\sigma_H(X|Y,\underline{\lambda})\right) e^{-nr_{X|Y}(\delta_n(\epsilon))+\underline{\lambda}\eta'} \\
&= e^{\frac{n\underline{\lambda}^2\sigma_H^2(X|Y,\underline{\lambda})}{2}} Q\left(\sqrt{n}\underline{\lambda}\sigma_H(X|Y,\underline{\lambda})\right) \frac{Q\left(\rho_* + \sqrt{n}\underline{\lambda}\sigma_H(X|Y,\underline{\lambda})\right)}{Q\left(\sqrt{n}\underline{\lambda}\sigma_H(X|Y,\underline{\lambda})\right)} e^{-nr_{X|Y}(\delta_n(\epsilon))+\underline{\lambda}\eta'} \\
&\overset{2)}{\geq} g_{X|Y,n}(\delta_n(\epsilon)) \frac{Q\left(\rho_* + \sqrt{n}\underline{\lambda}\sigma_H(X|Y,\underline{\lambda})\right)}{Q\left(\sqrt{n}\underline{\lambda}\sigma_H(X|Y,\underline{\lambda})\right)} e^{\underline{\lambda}\eta'} \\
&\overset{3)}{\geq} (1+\underline{\lambda})\epsilon \frac{Q\left(\rho_* + \sqrt{n}\underline{\lambda}\sigma_H(X|Y,\underline{\lambda})\right)}{Q\left(\sqrt{n}\underline{\lambda}\sigma_H(X|Y,\underline{\lambda})\right)} e^{\underline{\lambda}(\eta'-1)}.
\end{aligned} \tag{4.36}$$

In the derivation of (4.36), the inequality 1) is due to the convexity of $r_{X|Y}(\delta)$ and the fact that

$$r_{X|Y}(\underline{\delta}) \leq r_{X|Y}(\delta_n(\epsilon)) - \underline{\lambda}\frac{\eta'}{n};$$

the inequality 2) follows again from the fact that $e^{\frac{x^2}{2}}Q(x)$ is a strictly decreasing function of x and $\lambda\sigma_H(X|Y,\lambda)$ is increasing with respect to λ; and finally the inequality 3) is attributable to the inequality $e^x \geq 1 + x$ for any $x \geq 0$.

In order for (4.34) to be satisfied, we now choose η' such that

$$\begin{aligned}
\eta' &= 1 + \frac{1}{\underline{\lambda}} \ln \frac{Q\left(\sqrt{n}\underline{\lambda}\sigma_H(X|Y,\underline{\lambda})\right)}{Q\left(\rho_* + \sqrt{n}\underline{\lambda}\sigma_H(X|Y,\underline{\lambda})\right)} \\
&= 1 + \frac{1}{\underline{\lambda}} \ln \left[1 + \rho_* \frac{\frac{1}{\sqrt{2\pi}} e^{-\frac{(\tilde{\rho}+\sqrt{n}\underline{\lambda}\sigma_H(X|Y,\underline{\lambda}))^2}{2}}}{Q\left(\rho_* + \sqrt{n}\underline{\lambda}\sigma_H(X|Y,\underline{\lambda})\right)}\right]
\end{aligned} \tag{4.37}$$

where $0 \leq \tilde{\rho} \leq \rho_*$. One can verify that

$$\begin{aligned}
\eta' &\leq 1 + \frac{\rho_*}{\underline{\lambda}} \frac{\frac{1}{\sqrt{2\pi}} e^{-\frac{(\tilde{\rho}+\sqrt{n}\underline{\lambda}\sigma_H(X|Y,\underline{\lambda}))^2}{2}}}{Q\left(\rho_* + \sqrt{n}\underline{\lambda}\sigma_H(X|Y,\underline{\lambda})\right)} \\
&\leq 1 + \frac{\rho_*}{\underline{\lambda}} \frac{1 + (\rho_* + \sqrt{n}\underline{\lambda}\sigma_H(X|Y,\underline{\lambda}))^2}{\rho_* + \sqrt{n}\underline{\lambda}\sigma_H(X|Y,\underline{\lambda})} e^{\sqrt{n}\underline{\lambda}\sigma_H(X|Y,\underline{\lambda})(\rho_*-\tilde{\rho})+\frac{\rho_*^2-\tilde{\rho}^2}{2}}
\end{aligned} \tag{4.38}$$

where the last inequality is due to (4.27). From the definition of ρ_*, it is not hard to see that $\rho_* = \frac{\eta''}{\sqrt{n}}$ for some constant η'' depending only on channel parameters. Meanwhile, we

have $\sqrt{n}\underline{\lambda}\sigma_H(X|Y,\underline{\lambda}) > c$ as discussed above. Then

$$\begin{aligned}\eta' &\leq 1+\frac{\eta''}{\sqrt{n}\underline{\lambda}}\left(c^{-1}+\frac{\eta''}{\sqrt{n}}+\sqrt{n}\underline{\lambda}\sigma_H(X|Y,\underline{\lambda})\right)e^{\eta''\lambda^+\max_{\lambda\in[0,\lambda^+]}\sigma_H(X|Y,\lambda)+\frac{(\eta'')^2}{2n}}\\ &\leq 1+\left(c^{-2}+c^{-1}\eta''+1\right)\eta''\left[\max_{\lambda\in[0,\lambda^+]}\sigma_H(X|Y,\lambda)\right]e^{\eta''\lambda^+\max_{\lambda\in[0,\lambda^+]}\sigma_H(X|Y,\lambda)+(\eta'')^2}\end{aligned} \tag{4.39}$$

which is independent of both n and ϵ. Now combining (4.36) and (4.37), we have

$$\underline{\xi}_H(X|Y,\underline{\lambda},n)e^{-nr_{X|Y}(\underline{\delta})} \geq (1+\underline{\lambda})\epsilon \tag{4.40}$$

and consequently,

$$\begin{aligned}R_n(\epsilon) &\leq C_{\text{BIMSC}}-\underline{\delta}+\frac{-\ln\epsilon-\ln\underline{\lambda}}{n}\\ &\overset{1)}{\leq} C_{\text{BIMSC}}-\delta_n(\epsilon)+r_{X|Y}(\delta_n(\epsilon))\\ &\quad+\frac{\ln\left[\sqrt{2\pi}\sqrt{n}\lambda_n(\epsilon)\sigma_H(X|Y,\lambda_n(\epsilon))\left(1+\frac{1}{n\lambda_n^2(\epsilon)\sigma_H^2(X|Y,\lambda_n(\epsilon))}\right)\right]}{n}\\ &\quad+\frac{-\ln\underline{\lambda}+\eta'}{n}\\ &= C_{\text{BIMSC}}-\delta_n(\epsilon)+r_{X|Y}(\delta_n(\epsilon))+\frac{\ln\left(1+\frac{1}{n\lambda_n^2(\epsilon)\sigma_H^2(X|Y,\lambda_n(\epsilon))}\right)}{n}\\ &\quad+\frac{\ln\sqrt{n}+\ln\sqrt{2\pi}\sigma_H(X|Y,\lambda_n(\epsilon))+\ln\frac{\lambda_n(\epsilon)}{\underline{\lambda}}+\eta'}{n}\\ &\overset{2)}{\leq} C_{\text{BIMSC}}-\delta_n(\epsilon)+r_{X|Y}(\delta_n(\epsilon))+\frac{\frac{1}{2}\ln n+\underline{d}_1}{n}\end{aligned} \tag{4.41}$$

where $\underline{d}_1$ is another constant depending only on the channel. In the derivation of (4.41), the inequality 1) is due to (4.27) and the definition of $\delta_n(\epsilon)$ in (4.2); and the inequality 2) follows from the fact that

$$\frac{\lambda_n(\epsilon)}{\underline{\lambda}} = 1+\frac{1}{\sigma_H^2(X|Y,\hat{\lambda})}\frac{\eta'}{n\underline{\lambda}}$$

for some $\hat{\lambda}\in[\underline{\lambda},\lambda_n(\epsilon)]$ and

$$\sqrt{n}\underline{\lambda}\sigma_H(X|Y,\underline{\lambda}) > c.$$

Then the theorem is proved by combining (4.33) and (4.41) and making $d_1 = \max\{\bar{d}_1,\underline{d}_1\}$. □

Remark 4.3. *The condition $\epsilon \leq \frac{1}{3}$ for (4.17) and (4.18) can be relaxed as we only require that $\sqrt{n}\delta_n(\epsilon)$ or equivalently $\sqrt{n}\lambda$ be lower bounded by a constant, which is true when $\epsilon \leq d$ for any constant $d < \frac{1}{2}$. In addition, when $\epsilon \leq g_{X|Y,n}(\delta^+/2)$, ϵ is an exponential function of n, in which case the maximum achievable rate is below the channel capacity by a positive constant even when n goes to ∞. As such, from a practical point of view, the case $\epsilon \leq g_{X|Y,n}(\delta^+/2)$ is not interesting, especially when one can approach the channel capacity very closely as shown in the achievability given in (2.16) and (2.17).*

Remark 4.4. *In the definition of $R_n(\epsilon)$, the average error probability is used. If the maximal error probability is used instead, Theorem 4.1 remains valid (by replacing $\frac{\ln n}{2n}$ with $\frac{\ln n}{n}$ in (4.18) and (4.19)), in which case the standard technique of removing bad codewords from the code in the achievability given in (2.16) to (2.19) can be used to establish similar achievability with maximal error probability.*

Remark 4.5. *In view of Theorem 4.1, it is now clear that jar decoding is indeed optimal up to the second order coding performance in the non-asymptotical regime. Since the achievability given in (2.16) to (2.19) was established for linear block codes, it follows from Theorem 4.1 that linear block coding is also optimal up to the second order coding performance in the non-asymptotical regime for any BIMSC. In addition, in the Taylor-type expansion of $R_n(\epsilon)$, the third order term is $O(\delta_n^2(\epsilon))$ or $O\left(\ln n/n\right)$ whichever is larger since it follows from part (a) of Result 1.1 that $r_{X|Y}(\delta_n(\epsilon)) = O(\delta_n^2(\epsilon))$.*

4.1.2 Comparison with Asymptotic Analysis

It is instructive to compare Theorem 4.1 with the second order asymptotic performance analysis as n goes to ∞.

Asymptotic analysis with constant $0 < \epsilon < 1$ and $n \to \infty$: Fix $0 < \epsilon < 1$. It was shown in [15, 18, 19] that for a BIMSC with a discrete output alphabet

$$R_n(\epsilon) = C_{\text{BIMSC}} - \frac{\sigma_H(X|Y)}{\sqrt{n}} Q^{-1}(\epsilon) + O\left(\frac{\ln n}{n}\right) \tag{4.42}$$

for sufficiently large n. The expression $C_{\text{BIMSC}} - \frac{\sigma_H(X|Y)}{\sqrt{n}} Q^{-1}(\epsilon)$ was referred to as the normal approximation for $R_n(\epsilon)$. Clearly, when $\epsilon > 1/3$, (4.42) is essentially the same as (4.19). Let us now look at the case $\epsilon \leq 1/3$. In this case, by using the Taylor expansion of

$r_{X|Y}(\delta)$ around $\delta = 0$

$$\begin{aligned} r_{X|Y}(\delta) &= \frac{1}{2\sigma_H^2(X|Y)}\delta^2 + \frac{-\frac{d\sigma_H^2(X|Y,\lambda)}{d\lambda}\Big|_{\lambda=0}}{6\sigma_H^6(X|Y)}\delta^3 + O(\delta^4) \\ &= \frac{1}{2\sigma_H^2(X|Y)}\delta^2 + \frac{-\hat{M}_H(X|Y)}{6\sigma_H^6(X|Y)}\delta^3 + O(\delta^4) \end{aligned} \tag{4.43}$$

it can be verified that

$$\delta_n(\epsilon) = \frac{\sigma_H(X|Y)}{\sqrt{n}}Q^{-1}(\epsilon) + O\left(\frac{1}{n}\right). \tag{4.44}$$

Thus the Taylor-type expansion of $R_n(\epsilon)$ in Theorem 4.1 implies the second order asymptotic analysis with constant $0 < \epsilon < 1$ and $n \to \infty$ shown in (4.42).

Asymptotic analysis with $n \to \infty$ and non-exponentially decaying ϵ: Suppose now ϵ is a function of n and goes to 0 as $n \to \infty$, but at a non-exponential speed. In this case, as $n \to \infty$, $\delta_n(\epsilon)$ goes to 0 at the speed of $\Theta\left(\sqrt{\frac{-\ln\epsilon}{n}}\right)$, and $\sqrt{n}\lambda_n(\epsilon)$ goes to ∞. By ignoring the third and higher order terms in the Taylor expansion of $r_{X|Y}(\delta)$, one has the following approximations:

$$g_{X|Y,n}(\delta_n(\epsilon)) \approx \frac{1}{\sqrt{2\pi}\sqrt{n}\lambda_n(\epsilon)\sigma_H(X|Y,\lambda_n(\epsilon))}e^{-n\frac{\delta_n^2(\epsilon)}{2\sigma_H^2(X|Y)}} \tag{4.45}$$

and

$$Q(x) \approx \frac{1}{\sqrt{2\pi}x}e^{-\frac{x^2}{2}} \text{ for large } x.$$

By these approximations, it is not hard to verify that in this case

$$\lim_{n\to\infty} \frac{\delta_n(\epsilon)}{\frac{\sigma_H(X|Y)}{\sqrt{n}}Q^{-1}(\epsilon)} = 1.$$

Therefore, from Theorem 4.1, it follows that when ϵ goes to 0 at a non-exponential speed as $n \to \infty$, $\frac{\sigma_H(X|Y)}{\sqrt{n}}Q^{-1}(\epsilon)$ is still the second order term of $R_n(\epsilon)$ in the asymptotic analysis with $n \to \infty$. Indeed, this can also be verified by looking at the specific case given by (2.20), (2.21), and (3.14) when ϵ goes to 0 at a polynomial speed as $n \to \infty$. This result is consistent with that of moderate deviation analysis in [29–31].

Divergence of $\delta_n(\epsilon)$ from $\frac{\sigma_H(X|Y)}{\sqrt{n}}Q^{-1}(\epsilon)$: The agreement between $\delta_n(\epsilon)$ and $\frac{\sigma_H(X|Y)}{\sqrt{n}}Q^{-1}(\epsilon)$ terminates when the third order term

$$\frac{-\hat{M}_H(X|Y)}{6\sigma_H^6(X|Y)}\delta^3$$

in the Taylor expansion of $r_{X|Y}(\delta)$ shown in (4.43) can not be ignored. This happens when δ is not small, which is typical in practice for finite block length n, or

$$\zeta_{X|Y} \triangleq \frac{-\hat{M}_H(X|Y)}{6\sigma_H^6(X|Y)} \tag{4.46}$$

is large. In this case, $\frac{\sigma_H(X|Y)}{\sqrt{n}}Q^{-1}(\epsilon)$ will be smaller than $\delta_n(\epsilon)$ by a relatively large margin if $\zeta_{X|Y} < 0$, and larger than $\delta_n(\epsilon)$ by a relatively large margin if $\zeta_{X|Y} > 0$. As such, the normal approximation would fail to provide a reasonable estimate for $R_n(\epsilon)$. This will be further confirmed by numerical results shown in Section 4.3 for well known channels such as the BEC, BSC, and BIAGC for finite n.

4.2 Taylor-type Expansion: DIMC

4.2.1 Taylor-Type Expansion

Fix a DIMC $P = \{p(y|x), x \in \mathcal{X}, y \in \mathcal{Y}\}$ with its capacity $C_{\text{DIMC}} > 0$. In this subsection, we extend Theorem 4.1 to establish a Taylor-type expansion of $R_n(\epsilon)$ in the case of DIMC.

By combining (2.43) to (2.45) with (3.47) to (3.50), it is expected that $R_n(\epsilon)$ would be expanded as

$$R_n(\epsilon) = I(t;P) - \delta + o(\delta) \tag{4.47}$$

for some $t \in \mathcal{P}$, where δ is defined according to (2.44), (3.48), or (3.50). In the rest of this subsection, we shall demonstrate with mathematic rigor that this is indeed the case. To simplify our argument, we impose the following conditions* on the channel:

(C1) For any $t \in \mathcal{P}$, $M_D(t;P) < \infty$.

(C2) $\sigma_D^2(t;P) = 0$ implies $I(t;P) = 0$.

(C3) For any $t \in \mathcal{P}$, $\lambda_-^*(t;P) = +\infty$.

(C4) There exists $\lambda^* > 0$ such that $\delta_-(t,\lambda)$, $\sigma_{D,-}^2(t;P,\lambda)$, $M_{D,-}(t;P,\lambda)$, $\hat{M}_{D,-}(t;P,\lambda)$, and $r_-(t,\delta_-(t,\lambda))$ are continuous functions of t and λ over $(t,\lambda) \in \mathcal{P} \times [0,\lambda^*]$.

*Some of these conditions, for example, Condition C3, can be relaxed. Here we choose not to do so in order not to make our subsequent argument unnecessary complicated.

(C5) There exists $s^* > 0$ such that $r_-^{-1}(t,s)$ is a continuous function of t and s over $(t,s) \in \mathcal{P} \times [0, s^*]$, where $r_-^{-1}(t,\cdot)$ is an inverse function of $r_-(t,\cdot)$.

Since $r_-(t,\delta)$ is a continuous and strictly increasing function of δ before it reaches $+\infty$—which may or may not happen—it can be easily verified that for any $s \geq 0$

$$\begin{aligned} r_-^{-1}(t,s) &= \max\{\delta : r_-(t,\delta) \leq s\} \\ &= \inf\{\delta : r_-(t,\delta) > s\}. \end{aligned} \tag{4.48}$$

In view of the definitions and properties of $\delta_-(t,\lambda)$, $\sigma^2_{D,-}(t;P,\lambda)$, $M_{D,-}(t;P,\lambda)$, $\hat{M}_{D,-}(t;P,\lambda)$, and $r_-(t,\delta)$ in Appendix A, Conditions (C1) to (C5) are generally met by most channels, particularly by channels with discrete output alphabets, and discrete input additive white Gaussian channels.

To characterize δ in (4.47) analytically, we need a counterpart of Lemma 4.1. To this end, define for any $0 < c < C_{\text{DIMC}}$

$$\mathcal{P}(c) \stackrel{\Delta}{=} \{t \in \mathcal{P} : I(t;P) \geq c\} \tag{4.49}$$

$$\mathcal{P}_n(c) \stackrel{\Delta}{=} \{t \in \mathcal{P}_n : I(t;P) \geq c\} \tag{4.50}$$

and for any type $t \in \mathcal{P}$ satisfying $\sigma^2_D(t;P) > 0$

$$g_{t;P,n}(\delta) \stackrel{\Delta}{=} e^{\frac{n\lambda^2\sigma^2_{D,-}(t;P,\lambda)}{2}} Q(\sqrt{n}\lambda\sigma_{D,-}(t;P,\lambda)) e^{-nr_-(t,\delta)} \tag{4.51}$$

where $\lambda = \frac{\partial r_-(t,\delta)}{\partial \delta}$. Note that $\mathcal{P}(c)$ is a closed set, and it follows from Condition (C2) that $\sigma^2_D(t;P) > 0$ for any $t \in \mathcal{P}(c)$. Interpret $g_{t;P,n}(\delta)$ as a function of λ through $\delta = \delta_-(t,\lambda)$. Then we have the following lemma.

Lemma 4.2. *There exists $\lambda^+ > 0$ such that for any $n > 0$ and $t \in \mathcal{P}(c)$, $g_{t;P,n}(\delta_-(t,\lambda))$ is a strictly decreasing function of λ over $\lambda \in [0, \lambda^+]$.*

Proof. The proof is in parallel with that of Lemma 4.1. As such, we point out only places where differences occur. In the place of (4.14), we now have

$$\frac{d\sigma^2_{D,-}(t;P,\lambda)}{d\lambda} = -\hat{M}_{D,-}(t;P,\lambda)\,. \tag{4.52}$$

In parallel with (4.15) and (4.16), we now have for any $t \in \mathcal{P}(c)$

$$\begin{aligned}
&\frac{dg_{t;P,n}(\delta_-(t,\lambda))}{d\lambda} \\
&\leq e^{-nr_-(t,\delta_-(t,\lambda))}\frac{\sqrt{n}\sigma_{D,-}(t;P,\lambda)}{\sqrt{2\pi}}\left(\left|-\frac{\lambda\frac{d\sigma^2_{D,-}(t;P,\lambda)}{d\lambda}}{2\sigma^2_{D,-}(t;P,\lambda)\left(1+n\lambda^2\sigma^2_{D,-}(t;P,\lambda)\right)}\right|-1\right) \\
&= e^{-nr_-(t,\delta_-(t,\lambda))}\frac{\sqrt{n}\sigma_{D,-}(t;P,\lambda)}{\sqrt{2\pi}}\left(\left|\frac{\lambda\hat{M}_{D,-}(t;P,\lambda)}{2\sigma^2_{D,-}(t;P,\lambda)\left(1+n\lambda^2\sigma^2_{D,-}(t;P,\lambda)\right)}\right|-1\right) \quad (4.53) \\
&\leq e^{-nr_-(t,\delta_-(t,\lambda))}\frac{\sqrt{n}\sigma_{D,-}(t;P,\lambda)}{\sqrt{2\pi}}\left(\left|\frac{\lambda\hat{M}_{D,-}(t;P,\lambda)}{2\sigma^2_{D,-}(t;P,\lambda)}\right|-1\right). \quad (4.54)
\end{aligned}$$

Since $\mathcal{P}(c)$ is closed, it then follows from Condition (C4) that there is a $\lambda^+ > 0$ such that for any $\lambda \in [0, \lambda^+]$ and any $t \in \mathcal{P}(c)$

$$\left|\frac{\lambda\hat{M}_{D,-}(t;P,\lambda)}{2\sigma^2_{D,-}(t;P,\lambda)}\right| - 1 < 0$$

and hence

$$\frac{dg_{t;P,n}(\delta_-(t,\lambda))}{d\lambda} < 0$$

for any $n > 0$. This completes the proof of Lemma 4.2. □

Remark 4.6. *In view of (4.53), it is clear that when n is large, $g_{t;P,n}(\delta_-(t,\lambda))$ is a strictly decreasing function of λ over an interval even larger than $[0, \lambda^+]$ for each and every $t \in \mathcal{P}(c)$.*

Now let

$$\epsilon_n^+ \stackrel{\Delta}{=} \max\{g_{t;P,n}(\delta_-(t,\lambda^+/2)) : t \in \mathcal{P}(c)\}$$

which, in view of Condition (C4) and the fact that $\mathcal{P}(c)$ is closed, is well defined and also an exponential function of n. For any $\epsilon_n^+ \leq \epsilon \leq 1/2$ and $t \in \mathcal{P}(c)$, let $\delta_{t,n}(\epsilon)$ be the unique solution to

$$g_{t;P,n}(\delta) = \epsilon\,. \quad (4.55)$$

Further define

$$s(c) \stackrel{\Delta}{=} \max\left\{s : 0 < s \leq s^*, r_-^{-1}(t,s) \leq \frac{C_{\text{DIMC}} - c}{2} \;\; \forall t \in \mathcal{P}\right\} \quad (4.56)$$

and let $\epsilon_n(c)$ be the unique solution ϵ to

$$\frac{-\ln\epsilon\left(1+2\sqrt{\frac{-2\ln\epsilon}{n}}\right)}{n} = s(c). \tag{4.57}$$

It is easy to see that in view of Condition (C5), $s(c) > 0$ is well defined and once again $\epsilon_n(c)$ is also an exponential function of n. Let $\epsilon_n^u < 1$ be the unique solution ϵ to

$$\epsilon\left(1+2\sqrt{\frac{-2\ln\epsilon}{n}}\right) = 1. \tag{4.58}$$

Note that

$$\max\{I(t;P) : t \in \mathcal{P}_n\} = C_{\text{DIMC}} - O\left(\frac{1}{n^2}\right).$$

Let $N(c)$ be the smallest integer $N > 0$ such that

$$\max\{I(t;P) : t \in \mathcal{P}_n\} \geq C_{\text{DIMC}} - \frac{C_{\text{DIMC}} - c}{2} \tag{4.59}$$

for all $n \geq N$. Then we have the following Taylor-type expansion of $R_n(\epsilon)$.

Theorem 4.2. *For any $n \geq N(c)$ and any $\max\{\epsilon_n^+, \epsilon_n(c)\} \leq \epsilon < \epsilon_n^u$, let*

$$t^* \stackrel{\Delta}{=} \arg\max_{t\in\mathcal{P}_n(c)} \left[I(t;P) - \delta_{t,n}(\epsilon)\right] \tag{4.60}$$

$$t^\# \stackrel{\Delta}{=} \arg\max_{t\in\mathcal{P}_n(c)} \left[I(t;P) - \frac{\sigma_D(t;P)}{\sqrt{n}}Q^{-1}(\epsilon)\right]. \tag{4.61}$$

Then

$$|R_n(\epsilon) - (I(t^*;P) - \delta_{t^*,n}(\epsilon))| \leq o\left(\delta_{t^*,n}(\epsilon)\right) \tag{4.62}$$

where

$$o\left(\delta_{t^*,n}(\epsilon)\right) = r_-(t^*, \delta_{t^*,n}(\epsilon)) + \frac{(|\mathcal{X}| + 1.5)\ln(n+1) + d_1}{n} \tag{4.63}$$

if $\epsilon \leq \frac{1}{3}$, and

$$\left|R_n(\epsilon) - \left(I(t^\#;P) - \frac{\sigma_D(t^\#;P)}{\sqrt{n}}Q^{-1}(\epsilon)\right)\right| \leq \frac{(|\mathcal{X}|+1)\ln(n+1) + d_2}{n} \tag{4.64}$$

otherwise, where d_1 and d_2 are constants depending on the channel, but independent of n and ϵ.

Proof. For any $t \in \mathcal{P}_n$ and $0 < \epsilon < 1$, let

$$\delta_{t,n}^P(\epsilon) = \sup\left\{\delta > 0 : P_{t,\delta} \geq \left(1 + 2\sqrt{\frac{-2\ln\epsilon}{n}}\right)\epsilon\right\}.$$

By Theorem 3.2 and the trivial bound $P(B_{t,n,\delta}) \leq 1$, it is not hard to verify that

$$R_n(\epsilon) \leq \max_{t\in\mathcal{P}_n}[I(t;P) - \delta_{t,n}^P] - \frac{\ln\epsilon + \ln\frac{-2\ln\epsilon}{n}}{n} + \frac{\ln\left(1+\sqrt{\frac{-2\ln\epsilon}{n}}\right) + |\mathcal{X}|\ln(n+1)}{n}. \quad (4.65)$$

Let us now examine

$$\max_{t\in\mathcal{P}_n}[I(t;P) - \delta_{t,n}^P].$$

In view of the Chernoff bound (see Result 1.2 in Section 1.4.2),

$$P_{t,\delta} \leq e^{-nr_-(t,\delta)}$$

for any $t \in \mathcal{P}_n$ and $\delta > 0$, which, together with (4.48), implies

$$\begin{aligned}
\delta_{t,n}^P &\leq r_-^{-1}\left(t, \frac{-\ln\left(1+2\sqrt{\frac{-2\ln\epsilon}{n}}\right)\epsilon}{n}\right) && (4.66)\\
&\leq r_-^{-1}(t, s(c)) && (4.67)\\
&\leq \frac{C_{\mathrm{DIMC}} - c}{2} && (4.68)
\end{aligned}$$

whenever $\max\{\epsilon_n^+, \epsilon_n(c)\} \leq \epsilon < \epsilon_n^u$. In the above derivation, (4.66) is due to (4.48); and (4.67) and (4.68) follow from (4.56), (4.57), and (4.58). Therefore,

$$\begin{aligned}
\max_{t\in\mathcal{P}_n}[I(t;P) - \delta_{t,n}^P] &\geq \max_{t\in\mathcal{P}_n} I(t;P) - \frac{C_{\mathrm{DIMC}} - c}{2}\\
&\geq c && (4.69)
\end{aligned}$$

where the last inequality is due to (4.59). In view of (4.69), it is not hard to see that for any $t \in \mathcal{P}_n$ achieving $\max_{t\in\mathcal{P}_n}[I(t;P) - \delta_{t,n}^P]$,

$$I(t;P) \geq c + \delta_{t,n}^P \geq c$$

and hence

$$\max_{t\in\mathcal{P}_n}[I(t;P) - \delta_{t,n}^P] = \max_{t\in\mathcal{P}_n(c)}[I(t;P) - \delta_{t,n}^P]$$

which, together with (4.65), implies

$$R_n(\epsilon) \leq \max_{t\in\mathcal{P}_n(c)} [I(t;P) - \delta^P_{t,n}] - \frac{\ln\epsilon + \ln\frac{-2\ln\epsilon}{n}}{n} + \frac{\ln\left(1+\sqrt{\frac{-2\ln\epsilon}{n}}\right) + |\mathcal{X}|\ln(n+1)}{n}. \quad (4.70)$$

When $\epsilon > \frac{1}{3}$, it follows from part (c) of Result 1.2 that for any $t \in \mathcal{P}_n(c)$,

$$\begin{aligned}\delta^P_{t,n} &\geq \frac{\sigma_D(t;P)}{\sqrt{n}}Q^{-1}\left(\epsilon + \frac{1}{\sqrt{n}}\left(2\epsilon\sqrt{-2\ln\epsilon} + \frac{C_{BE}M_D(t;P)}{\sigma^3_D(t;P)}\right)\right)\\ &\geq \frac{\sigma_D(t;P)}{\sqrt{n}}Q^{-1}(\epsilon) - \sqrt{2\pi}e^{\frac{[Q^{-1}(\epsilon)]^2}{2}}\frac{\sigma_D(t;P)}{n}\left(2\epsilon\sqrt{-2\ln\epsilon} + \frac{C_{BE}M_D(t;P)}{\sigma^3_D(t;P)}\right).\end{aligned} \quad (4.71)$$

Since $\mathcal{P}(c)$ is closed, it follows Condition (C4) that $\sigma_D(t;P)$ and $\frac{M_D(t;P)}{\sigma^3_D(t;P)}$ are bounded over $\mathcal{P}(c)$. Plugging (4.71) into (4.70) yields

$$R_n(\epsilon) \leq \max_{t\in\mathcal{P}_n(c)}\left[I(t;P) - \frac{\sigma_D(t;P)}{\sqrt{n}}Q^{-1}(\epsilon)\right] + \frac{(|\mathcal{X}|+1)\ln(n+1)+d}{n}$$

for some constant d, which, together with the achievability in (2.49) and (2.48), implies (4.64).

Now let us focus on the case when $\epsilon \leq \frac{1}{3}$. For any $t \in \mathcal{P}(c)$, let $\underline{\delta}_{t,n}(\epsilon)$ be the unique solution to

$$\left(1 + 2\sqrt{\frac{-2\ln\epsilon}{n}}\right)\epsilon = \xi_{D,-}(t;P,\lambda,n)e^{-nr_-(t,\delta)} \quad (4.72)$$

where $\lambda = \frac{\partial r_-(t,\delta)}{\partial\delta}$. By following the argument in the proof of Theorem 4.1, it is not hard to verify that for any $t \in \mathcal{P}_n(c)$

$$\delta^P_{t,n}(\epsilon) \geq \underline{\delta}_{t,n}(\epsilon) \geq \delta_{t,n}(\epsilon) - \frac{d}{n} \quad (4.73)$$

for some constant d independent of n, ϵ, and t. Plugging (4.73) into (4.70) then yields

$$R_n(\epsilon) \leq I(t^*;P) - \delta_{t^*,n}(\epsilon) - \frac{\ln\epsilon + \ln\frac{-2\ln\epsilon}{n}}{n} + \frac{\sqrt{\frac{-2\ln\epsilon}{n}} + |\mathcal{X}|\ln(n+1) + d}{n}. \quad (4.74)$$

In the meantime,

$$\begin{aligned}\epsilon &= g_{t^*;P,n}(\delta_{t^*,n}) \\ &\geq \frac{1}{\sqrt{2\pi}\left(\sqrt{n}\lambda_{t^*,n}\sigma_{D,-}(t^*;P,\lambda_{t^*,n}) + \frac{1}{\sqrt{n}\lambda_{t^*,n}\sigma_{D,-}(t^*;P,\lambda_{t^*,n})}\right)} e^{-nr_-(t^*,\delta_{t^*,n}(\epsilon))} \qquad (4.75)\end{aligned}$$

where $\lambda_{t^*,n} = \frac{\partial r_-(t^*,\delta)}{\partial \delta}\Big|_{\delta=\delta_{t^*,n}(\epsilon)}$. Consequently,

$$\begin{aligned}\frac{-\ln\epsilon}{n} &\leq r_-(t^*,\delta_{t^*,n}(\epsilon)) + \frac{\ln\left[\sqrt{2\pi}\left(\sqrt{n}\lambda_{t^*,n}\sigma_{D,-}(t^*;P,\lambda_{t^*,n}) + \frac{1}{\sqrt{n}\lambda_{t^*,n}\sigma_{D,-}(t^*;P,\lambda_{t^*,n})}\right)\right]}{n} \\ &\leq r_-(t^*,\delta_{t^*,n}(\epsilon)) + \frac{\ln n}{2n} + \frac{\eta_1}{n} \qquad (4.76)\end{aligned}$$

where η_1 is a constant independent of n, ϵ, and t^*. Now substituting (4.76) and $\epsilon \leq \frac{1}{3}$ into (4.74) yields

$$\begin{aligned}R_n(\epsilon) &\leq I(t^*;P) - \delta_{t^*,n}(\epsilon) + r_-(t^*,\delta_{t^*,n}(\epsilon)) \\ &\quad + \frac{-\ln\frac{2\ln 3}{n} + \eta_1 + \sqrt{r_-(t^*,\delta_{t^*,n}(\epsilon)) + \frac{1}{2e} + \frac{\eta_1}{n}} + \frac{1}{2}\ln n + |\mathcal{X}|\ln(n+1) + d}{n} \\ &\leq I(t^*;P) - \delta_{t^*,n}(\epsilon) + r_-(t^*,\delta_{t^*,n}(\epsilon)) + \frac{\underline{d}_1 + \left(|\mathcal{X}| + \frac{3}{2}\right)\ln(n+1)}{n} \qquad (4.77)\end{aligned}$$

for some constant $\underline{d}_1$ independent of n, ϵ, and t^*, where the last inequality is due to the fact that in view of Condition (4), $r_-(t^*,\delta_{t^*,n}(\epsilon))$ is bounded over $t \in \mathcal{P}(c)$ and $\epsilon \geq \max\{\epsilon_n^+, \epsilon_n(c)\}$.

To complete the proof, let us go back to the achievability given in (2.44) and (2.45). Now choose t to be t^*, and follow the argument in the proof of Theorem 4.1. Then it is not hard to show that

$$R_n(\epsilon) \geq I(t^*;P) - \delta_{t^*,n}(\epsilon) - r_-(t^*,\delta_n(\epsilon)) - \frac{(|\mathcal{X}|+1)\ln(n+1) + \bar{d}_1}{n} \qquad (4.78)$$

where $\bar{d}_1$ is a constant independent of n, ϵ, and t^*. Combining (4.78) with (4.77) completes the proof of Theorem 4.2. □

Remarks similar to those immediately after Theorem 4.1 also apply here. In particular, Theorem 4.2 and the achievability of jar decoding given in (2.43) to (2.49) once again imply that jar decoding is indeed optimal up to the second order coding performance in the non-asymptotical regime for any DIMC. In addition, the following remarks are helpful to the computation of the Taylor-type expansion of $R_n(\epsilon)$ as expressed in (4.60) to (4.64).

Remark 4.7. *When $I(t;P)$, $\delta_-(t,\lambda)$, $\sigma^2_{D,-}(t;P,\lambda)$, $M_{D,-}(t;P,\lambda)$, and $r_-(t,\delta_-(t,\lambda))$ are all continuously differentiable with respect to t over $t \in \mathcal{P}(c)$ and $\lambda \in [0,\lambda^*]$, which is true for most channels including particularly channels with discrete output alphabets, and discrete input additive white Gaussian channels, $\mathcal{P}_n(c)$ in the definitions of t^* and $t^\#$ can be replaced by $\mathcal{P}(c)$. Thus, in this case,*

$$t^* \stackrel{\Delta}{=} \arg\max_{t\in\mathcal{P}(c)} [I(t;P) - \delta_{t,n}(\epsilon)] \tag{4.79}$$

$$t^\# \stackrel{\Delta}{=} \arg\max_{t\in\mathcal{P}(c)} \left[I(t;P) - \frac{\sigma_D(t;P)}{\sqrt{n}} Q^{-1}(\epsilon)\right]. \tag{4.80}$$

Hereafter, we shall assume that the channel satisfies this continuously differentiable condition, and use (4.79) and (4.60), or (4.80) and (4.61) interchangeably.

Remark 4.8. *It is worth pointing out the impact of c on the maximization problems given in (4.79), (4.60), (4.80), and (4.61). In view of the definitions of $s(c)$ and $\epsilon_n(c)$ in (4.56) and (4.57), it is not hard to see that when ϵ is relatively large with respect to n (in the sense that $\frac{-\ln\epsilon}{n}$ is small), one can select c to be close to C_{DIMC}. In this case, it suffices to search a small range $\mathcal{P}(c)$ for optimal t^*. On the other hand, when ϵ is relatively small with respect to n, e.g., a exponential function of n, c should be selected to be far below C_{DIMC} and hence one has to search a large range $\mathcal{P}(c)$ for optimal t^*.*

Remark 4.9. *When the Taylor-type expansion of $R_n(\epsilon)$ in Theorem 4.2 is applied to the case of BIMSC, it yields essentially the same result as in Theorem 4.1, with explanation as follows. For any BIMSC, $t(0)$ fully characterizes the type t. Then by symmetry, $\frac{\partial\delta_{t,n}(\epsilon)}{\partial t(0)} = 0$ at $t(0) = 0.5$ for any n and ϵ. Note that $\delta_{t,n}(\epsilon) = \delta_n(\epsilon)$ when $t(0) = 0.5$, the capacity achieving input distribution. Therefore,*

$$\begin{aligned}\max_{t\in\mathcal{P}(c)}[I(t;P) - \delta_{t,n}(\epsilon)] &= \max_{t\in\mathcal{P}(C_{\text{BIMSC}}-O(\delta_n(\epsilon)))}[I(t;P) - \delta_{t,n}(\epsilon)] \\ &= C_{\text{BIMSC}} - \delta_n(\epsilon) + O\left(\delta_n^2(\epsilon)\right).\end{aligned} \tag{4.81}$$

Consequently, by observing that the high order term $o(\delta_n(\epsilon))$ in Theorem 4.1 is also in the order of $\delta_n^2(\epsilon)$, the Taylor-type expansion of $R_n(\epsilon)$ for BIMSC in Theorem 4.2 is shown to be the same as that in Theorem 4.1.

4.2.2 Comparison with Asymptotic Analysis and Implication

It is instructive to compare Theorem 4.2 with the second order asymptotic performance analysis as n goes to ∞.

Asymptotic analysis with constant $0 < \epsilon < 1$ *and* $n \to \infty$: Fix $0 < \epsilon < 1$. It was shown in [15, 18, 19] that for a DIMC with a discrete output alphabet and $C_{\text{DIMC}} > 0$,

$$R_n(\epsilon) = C_{\text{DIMC}} - \frac{\sigma_D(P)}{\sqrt{n}} Q^{-1}(\epsilon) + O\left(\frac{\ln n}{n}\right) \tag{4.82}$$

for sufficiently large n, where

$$\sigma_D(P) = \begin{cases} \min\{\sigma_D(t;P) : t \in \mathcal{P} \& I(t;P) = C_{\text{DIMC}}\} & \text{if } \epsilon < \frac{1}{2} \\ \max\{\sigma_D(t;P) : t \in \mathcal{P} \& I(t;P) = C_{\text{DIMC}}\} & \text{if } \epsilon > \frac{1}{2}. \end{cases}$$

Once again, the expression $C_{\text{DIMC}} - \frac{\sigma_D(P)}{\sqrt{n}} Q^{-1}(\epsilon)$ was referred to as the normal approximation for $R_n(\epsilon)$ in [15]. It is not hard to verify that for sufficiently large n,

$$\begin{aligned} C_{\text{DIMC}} - \frac{\sigma_D(P)}{\sqrt{n}} Q^{-1}(\epsilon) &\leq \max_{t \in \mathcal{P}(c)} \left[I(t;P) - \frac{\sigma_D(t;P)}{\sqrt{n}} Q^{-1}(\epsilon) \right] \\ &= \max_{t : \exists p_X, |t - p_X| = O\left(\frac{1}{n^{1/2}}\right)} \left[I(t;P) - \frac{\sigma_D(t;P)}{\sqrt{n}} Q^{-1}(\epsilon) \right] \\ &= C_{\text{DIMC}} - \frac{\sigma_D(P)}{\sqrt{n}} Q^{-1}(\epsilon) + O\left(\frac{1}{n}\right) \end{aligned} \tag{4.83}$$

where the first equality is due to the fact that for any p_X satisfying $I(p_X;P) = C_{\text{DIMC}}$ and t satisfying $|t - p_X| = \omega(1/n^{1/2})$,

$$I(t;P) - \frac{\sigma_D(t;P)}{\sqrt{n}} Q^{-1}(\epsilon) \leq C_{\text{DIMC}} - \frac{\sigma_D(p_X;P)}{\sqrt{n}} Q^{-1}(\epsilon)$$

as

$$\frac{Q^{-1}(\epsilon)}{\sqrt{n}} |\sigma_D(t;P) - \sigma_D(p_X;P)| = O\left(\frac{|t - p_X|}{\sqrt{n}}\right) = o(|t - p_X|^2) = o(C_{\text{DIMC}} - I(t;P)).$$

Therefore, when $\epsilon > 1/3$, (4.82) and (4.64) are essentially the same for sufficiently large n.

Let us now look at the case $\epsilon \leq 1/3$. Again, $0 < \epsilon \leq 1/3$ is fixed. In parallel with (4.43) and (4.44), we have for each $t \in \mathcal{P}(c)$

$$r_-(t,\delta) = \frac{1}{2\sigma_D^2(t;p)} \delta^2 + \frac{-\hat{M}_D(t;P)}{6\sigma_D^6(t;P)} \delta^3 + O(\delta^4) \tag{4.84}$$

and

$$\delta_{t,n}(\epsilon) = \frac{\sigma_D(t;P)}{\sqrt{n}} Q^{-1}(\epsilon) + O\left(\frac{1}{n}\right). \tag{4.85}$$

Combining (4.85) with (4.83) yields

$$\begin{aligned} C_{\text{DIMC}} - \frac{\sigma_D(P)}{\sqrt{n}}Q^{-1}(\epsilon) + O(1/n) &\leq \max_{t\in\mathcal{P}(c)} [I(t;P) - \delta_{t;n}(\epsilon)] \\ &\leq C_{\text{DIMC}} - \frac{\sigma_D(P)}{\sqrt{n}}Q^{-1}(\epsilon) + O\left(\frac{1}{n}\right). \end{aligned} \tag{4.86}$$

Thus the Taylor-type expansion of $R_n(\epsilon)$ in Theorem 4.2 implies the second order asymptotic analysis with constant $0 < \epsilon < 1$ and $n \to \infty$ shown in (4.82).

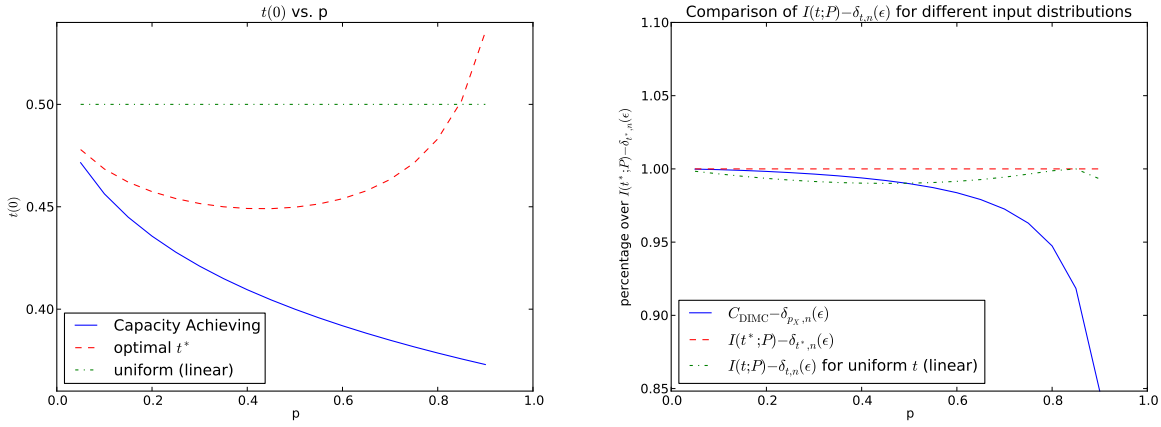
Asymptotic analysis with $n \to \infty$ and non-exponentially decaying ϵ: Suppose now ϵ is a function of n and goes to 0 as $n \to \infty$, but at a non-exponential speed. Using arguments similar to those made above and in Subsection 4.1.2, one can show that the Taylor-type expansion of $R_n(\epsilon)$ in Theorem 4.2 implies that in this case, C_{DIMC} and $-\frac{\sigma_D(P)}{\sqrt{n}}Q^{-1}(\epsilon)$ are still respectively the first order and second order terms of of $R_n(\epsilon)$ in the asymptotic analysis with $n \to \infty$. Once again, this result is consistent with that of moderate deviation analysis in [29–31].

Divergence from the normal approximation: In the non-asymptotic regime where n is finite and ϵ is generally relatively small with respect to n, the first two terms

$$\max_{t\in\mathcal{P}(c)} [I(t;P) - \delta_{t,n}(\epsilon)]$$

in the Taylor-type expansion of $R_n(\epsilon)$ in Theorem 4.2 differ from the normal approximation in a strong way. In particular, the optimal distribution t^* defined in (4.79) is not necessarily a capacity achieving distribution. In this case, the normal approximation would fail to provide a reasonable estimate for $R_n(\epsilon)$.

Example: Consider the Z channel shown in Figure 2.6. In this example, we show that the optimal distribution t^* defined in (4.79) is not a capacity achieving distribution. In the numerical calculation shown in Figure 4.1, the transition probability p (i.e. $\Pr\{Y = 1|X = 0\}$) ranges from 0.05 to 0.95 with block length $n = 1000$ and error probability $\epsilon = 10^{-6}$. As can be seen from Figure 4.1(a), $t^*(0)$ is always different from the capacity achieving $t(0)$. Moreover, Figure 4.1(b) shows the percentage of $I(t;P) - \delta_{t,n}(\epsilon)$ over $I(t^*;P) - \delta_{t^*,n}(\epsilon)$ when t is capacity achieving, t^*, and uniform respectively. It is clear that $C_{\text{DIMC}} - \delta_{p_X,n}(\epsilon)$ is apart from $I(t^*;P) - \delta_{t^*,n}(\epsilon)$ further and further when p gets larger and larger, where p_X is the capacity achieving distribution, indicating that under the practical block length and error probability requirement, Shannon random coding based on the capacity achieving distribution is not optimal. It is also interesting to note that for uniform t, $I(t;P) - \delta_{t,n}(\epsilon)$ is quite close to $I(t^*;P) - \delta_{t^*,n}(\epsilon)$ within the whole range, implying that linear block coding



(a) $t(0)$ vs. p

(b) $\frac{I(t;P)-\delta_{t,n}(\epsilon)}{I(t^*;P)-\delta_{t^*,n}(\epsilon)}$ for different t

Figure 4.1: Illustration for the Z channel with $n = 1000$ and $\epsilon = 10^{-6}$: (a) comparison of t^* with the capacity achieving distribution; and (b) comparison of $I(t;P) - \delta_{t,n}(\epsilon)$ among different distributions t.

is quit suitable for the Z channel even under the practical block length and error probability requirement.

Implication on code design: An important implication arising from the Taylor-type expansion of $R_n(\epsilon)$ in Theorem 4.2 in the non-asymptotic regime is that for values of n and ϵ with practical interest, the optimal marginal codeword symbol distribution is not necessarily a capacity achieving distribution. This is illustrated above for the Z channel. Indeed, other than for symmetric channels like BIMSC, it would expect that the optimal distribution t^* defined in (4.79) is in general not a capacity achieving distribution for values of n and ϵ for which $\delta_{t^*,n}(\epsilon)$ is not relatively small. As such, to design efficient channel codes under the practical block length and error probability requirement, one approach is to solve the maximization problem in (4.79), get t^*, and then design codes so that the marginal codeword symbol distribution is approximately t^*.

4.3 Approximation and Evaluation

Based on our converse theorems and Taylor-type expansion of $R_n(\epsilon)$, in this section, we first derive two approximation formulas for $R_n(\epsilon)$. We then compare them numerically

with the normal approximation and some tight (achievable and converse) non-asymptotic bounds, for the BSC, BEC, BIAGC, and Z Channel. In all Figures 4.3 to 4.10, rates are expressed in bits.

4.3.1 Approximation Formulas

In view of the Taylor-type expansion of $R_n(\epsilon)$ in Theorem 4.2, one reasonable approximation formula is to use the first two terms in Taylor-type expansion of $R_n(\epsilon)$ as an estimate for $R_n(\epsilon)$. We refer to this formula as the second order (SO) formula:

$$\begin{aligned} R_n^{\mathrm{SO}}(\epsilon) &= \max_{t\in\mathcal{P}(c)} [I(t;P) - \delta_{t,n}(\epsilon)] \\ &= I(t^*;P) - \delta_{t^*;P}(\epsilon) \end{aligned} \tag{4.1}$$

where c is selected according to Remark 4.8.

To derive the other approximation formula for $R_n(\epsilon)$, let us put Theorem 3.2 and Theorem 4.2 together. It would make sense for an optimal code of block length n to draw all its codewords from the same type t with $|t - t^*| = O(1/n)$. In this case, it is not hard to see that the term $|\mathcal{X}|\frac{\ln(n+1)}{n}$ in the bounds of Theorems 3.2 and 4.2 (i.e. (3.47), (3.49), (4.63), and (4.64)) can be dropped. By ignoring the higher order term $\frac{\ln\frac{-2\ln\epsilon_n}{n} - \ln\left(1+\sqrt{\frac{-2\ln\epsilon_n}{n}}\right)}{n}$ in (3.47) and (3.49), we get the following approximation formula (dubbed "NEP") :

$$R_n^{\mathrm{NEP}}(\epsilon) = I(t^*;P) - \delta_{t^*;P}(\epsilon) - \frac{\ln\epsilon}{n} + \frac{1}{n}\ln P(B_{t^*,n,\delta_{t^*;P}(\epsilon)}) \tag{4.2}$$

Rewrite the normal approximation as

$$R_n^{\mathrm{Normal}}(\epsilon) = C_{\mathrm{DIMC}} - \frac{\sigma_D(P)}{\sqrt{n}}Q^{-1}(\epsilon). \tag{4.3}$$

4.3.2 BIMSC

In the case of BIMSC, it follows from Theorem 4.1 and Remark 4.9 that $R_n^{\mathrm{SO}}(\epsilon)$, $R_n^{\mathrm{NEP}}(\epsilon)$, and $R_n^{\mathrm{Normal}}(\epsilon)$ become respectively

$$R_n^{\mathrm{SO}}(\epsilon) = C_{\mathrm{BIMSC}} - \delta_n(\epsilon)$$

$$R_n^{\mathrm{NEP}}(\epsilon) = C_{\mathrm{BIMSC}} - \delta_n(\epsilon) - \frac{\ln \epsilon}{n} + \frac{1}{n} \ln P(B_{n,\delta_n(\epsilon)}) \tag{4.4}$$

and

$$R_n^{\mathrm{Normal}}(\epsilon) = C_{\mathrm{BIMSC}} - \frac{\sigma_H(X|Y)}{\sqrt{n}} Q^{-1}(\epsilon). \tag{4.5}$$

From Theorem 4.1 and its comparison with asymptotic analysis, we can expect that when $\delta_n(\epsilon)$ is extremely small, $R_n^{\mathrm{SO}}(\epsilon)$ and $R_n^{\mathrm{Normal}}(\epsilon)$ are close, and both can provide a good approximation for $R_n(\epsilon)$. However, as $\delta_n(\epsilon)$ increases, the relative position of $R_n^{\mathrm{SO}}(\epsilon)$ and $R_n^{\mathrm{Normal}}(\epsilon)$ depends on

$$\zeta_{X|Y} = -\frac{\hat{M}_H(X|Y)}{6\sigma_H^6(X|Y)}.$$

Specifically, given a channel with large magnitude of $\zeta_{X|Y}$, $R_n^{\mathrm{Normal}}(\epsilon)$ is not reliable, as it can be much below achievable bounds or above converse bounds. On the other hand, as shown later on, $R_n^{\mathrm{SO}}(\epsilon)$ is much more reliable. Moreover, $R_n^{\mathrm{NEP}}(\epsilon)$, which has some terms beyond second order on top of $R_n^{\mathrm{SO}}(\epsilon)$, always provides a good approximation for $R_n(\epsilon)$ even if $\delta_n(\epsilon)$ is relatively large.

BSC

For this channel, the trivial bound $P(B_{n,\delta_n(\epsilon)}) \leq 1$ is applied in the evaluation of $R_n^{\mathrm{NEP}}(\epsilon)$. Before jumping into the comparison of those approximations, let us first get some insight by investigating $\zeta_{X|Y}$. It can be easily verified that for BSC with cross-over probability p,

$$\zeta_{X|Y} = -\frac{1}{6 \ln^5 \frac{1-p}{p}} \frac{1-2p}{p^3(1-p)^3}. \tag{4.6}$$

As can be seen, $\zeta_{X|Y}$ is always negative for any $p \in (0,1)$ and $\zeta_{X|Y} \to -\infty$ as $p \to 0$. Therefore, in the case of a very small p, $R_n^{\mathrm{Normal}}(\epsilon)$ will be larger than $R_n^{\mathrm{SO}}(\epsilon)$ by a relatively large margin, and even larger than the converse bound.

Now in order to compare those approximations, we invoke Theorem 33 (dubbed "RCU") and Theorem 35 (dubbed "Converse") in [15], which serve as an achievable bound and a converse bound, respectively. In addition, another converse bound is provided by the exact calculation of (3.9) and (3.10) in Theorem 3.1 (dubbed "Exact") with optimized value of β_n. Moreover, by Theorem 52 in [15], $\frac{\ln n}{2n}$ is the third order in the asymptotic analysis of $R_n(\epsilon)$ as $n \to \infty$ for BSC, and therefore, another approximation is yielded by adding $\frac{\ln n}{2n}$ to the normal approximation (dubbed "Normal_ln"). Then these four approximation formulas (NEP, Normal_ln, Normal, SO), two converse bounds (Converse, Exact), and one

achievable bound (RCU) are compared against each other with block length n ranging from 200 to 2000; their respective performance is shown in Figures 4.3 and 4.4.

In Figure 4.3, the target channel is the BSC with cross-over probability 0.11, where $\zeta_{X|Y}$ is relatively small. In Figure 4.3(a), bounds are compared with fixed average error probability $P_e = 10^{-3}$, while $\delta_n(\epsilon)$ changes with respect to block length n, shown in Figure 4.3(b). In the meantime, Figure 4.3(c) shows comparison of these bounds when $\delta_n(\epsilon)$ is fixed to be 0.06, while $P_e = g_{X|Y,n}(0.06)$ is shown in Figure 4.3(d). As can be seen, when $\delta_n(\epsilon)$ gets smaller, the SO and Normal curves tend to coincide with each other. Moreover, since the SO and Normal approximation formulas are quite close in this case, both the NEP and Normal_ln provide quite accurate approximations for $R_n(\epsilon)$ with the NEP slightly better.

Figure 4.4 shows the same curves as those in Figure 4.3, but for the BSC with cross-over probability 0.001. In this case, the magnitude of $\zeta_{X|Y}$ is large, and therefore, the SO and Normal curves are well apart. In fact, the Normal curve is even above those two converse bounds, and so does the Normal_ln curve, thus confirming our analysis based on $\zeta_{X|Y}$ made at the beginning of this discussion for BSC. On the other hand, the SO curve stays at the same relative position to achievable and converse bounds, and the NEP still provides an accurate approximation for $R_n(\epsilon)$.

BEC

This special channel serves as another interesting example to illustrate the difference between the SO and Normal approximations. On one hand, it can be easily verified that

$$P(B_{n,\delta}) = \Pr\left\{-\frac{1}{n}\ln p(X^n|Y^n) > H(X|Y) + \delta\right\} \approx g_{X|Y,n}(\delta) \tag{4.7}$$

and therefore, $-\frac{\ln\epsilon}{n}$ and $\frac{1}{n}\ln P(B_{n,\delta_n(\epsilon)})$ are cancelled out in $R_n^{\text{NEP}}(\epsilon)$, which is then identical to $R_n^{\text{SO}}(\epsilon)$. On the other hand,

$$\zeta_{X|Y} = -\frac{(1-2p)}{6p^2(1-p)^2\ln^3 2}\begin{cases} <0 & \text{if } p<0.5 \\ =0 & \text{if } p=0.5 \\ >0 & \text{if } p>0.5 \end{cases}. \tag{4.8}$$

Therefore, the Normal curve can be all over the map, i.e. it can be above some converse when $p < 0.5$, and below an achievable bound when $p > 0.5$. When $p = 0.5$, the Normal curve happens to be close to the SO curve, hereby explaining why it provides an accurate approximation for $R_n(\epsilon)$ in this particular case, as shown in [15].

To provide benchmarks for the comparison of approximation formulas, Theorem 37 and 38 in [15] are used here, dubbed "DT" and "Converse" respectively. The exact calculation of (3.9) and (3.10) in Theorem 3.1 (dubbed "Exact") with optimized value of β_n again serves as an additional converse bound. Then those bounds are drawn in Figures 4.5 and 4.6 in the same way as those in figure 4.3, where erasure probabilities are selected to be 0.05 and 0.9, respectively. Once again, numeric results confirm our analysis and discussion above.

BIAGC

Here we assume that codewords are modulated to $\{+1, -1\}$ before going through an AWGN channel, and apply the trivial bound $P(B_{n,\delta_n(\epsilon)}) \leq 1$ in the NEP formula. Similarly to BSC and BEC, we would like to get some insight by investigating $\zeta_{X|Y}$. Since in this case, $\zeta_{X|Y}$ does not seem to have a simple close form expression which can be easily computed, numerical calculation of $\zeta_{X|Y}$ is shown in Figure 4.2, where SNR ranges from 8dB to 10.5dB. As can be seen, BIAGC is similar to BSC, i.e. $\zeta_{X|Y}$ is always negative and its magnitude increases with SNR. Therefore, $R_n^{\text{Normal}}(\epsilon)$ is close to $R_n^{\text{SO}}(\epsilon)$ when SNR is low, but can be above some converse bounds when SNR is high. This is confirmed in Figures 4.7 and 4.8, where exact evaluation of (3.11) and (3.12) in Theorem 3.1 (dubbed "Exact") serves as a converse bound.

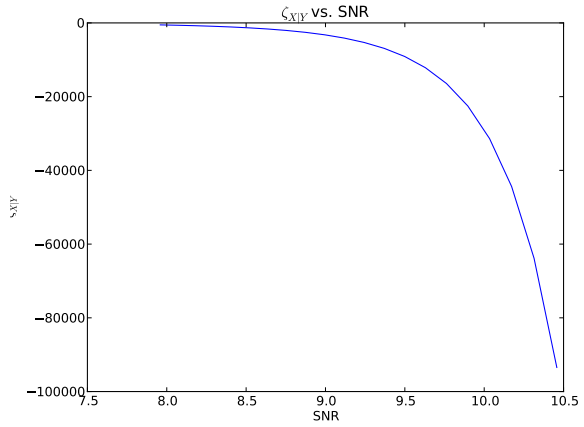


Figure 4.2: $\zeta_{X|Y}$ of BIAGC

4.3.3 DIMC: Z Channel

To show an example of DIMC which is not a BIMSC, we consider again the Z channel shown in Figure 2.6. The capacity of Z channel is well known and given by

$$C_Z = \ln\left(1 + (1-p)p^{\frac{p}{1-p}}\right) \tag{4.9}$$

with the capacity-achieving distribution

$$p_X(x) = \begin{cases} \frac{1}{1-p+p^{-\frac{p}{1-p}}} & \text{for } x = 0 \\ \\ \frac{p^{-\frac{p}{1-p}}-p}{1-p+p^{-\frac{p}{1-p}}} & \text{for } x = 1 \end{cases} \tag{4.10}$$

and the corresponding output distribution

$$p_Y(y) = \begin{cases} \frac{1-p}{1-p+p^{-\frac{p}{1-p}}} & \text{for } y = 0 \\ \\ \frac{p^{-\frac{p}{1-p}}}{1-p+p^{-\frac{p}{1-p}}} & \text{for } y = 1\ . \end{cases} \tag{4.11}$$

To calculate $R_n^{\text{NEP}}(\epsilon)$, $P(B_{t,n,\delta})$ needs to be further investigated, where an interesting observation is that given x^n with type t, $\frac{1}{n}\ln\frac{p(y^n|x^n)}{q_t(y^n)} > -\infty$ if and only if $y_i = 1$ when $x_i = 1$, and the value of $\frac{1}{n}\ln\frac{p(y^n|x^n)}{q_t(y^n)}$ only depends on the number of y_i being 1 for $i \in \{j : x_j = 0\}$. One can then verify that

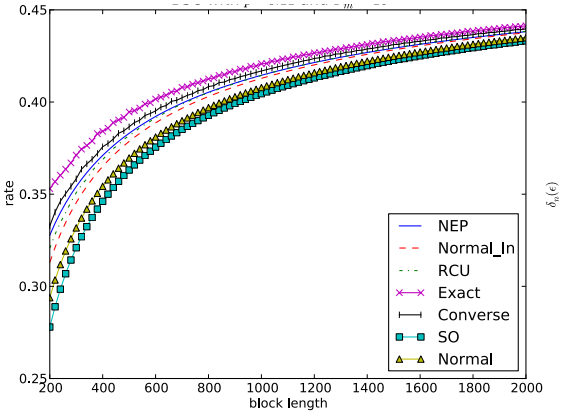
$$B_{t,n,\delta} = \left\{ y^n : \frac{1}{n}|\{i : y_i = 0\}| \le q_t(0) - \frac{\delta}{\ln\frac{1-t(0)+pt(0)}{pt(0)}} \right\}. \tag{4.12}$$

When $q_t(0) \neq 0.5$,

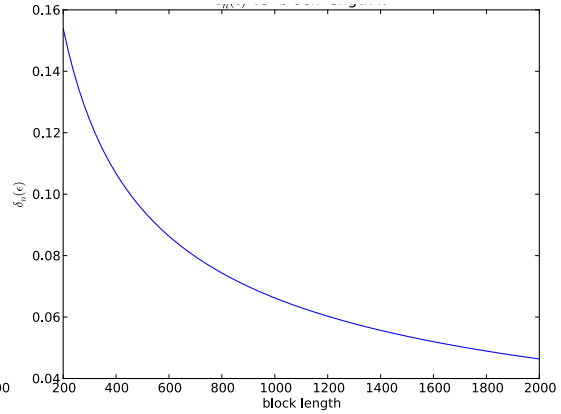
$$P(B_{t,n,\delta}) = \begin{cases} \Pr\left\{ -\frac{1}{n}\ln q_t(Y_t^n) \le H(Y_t) - \frac{\delta}{\ln\frac{1-t(0)+pt(0)}{pt(0)}}\ln\frac{1-q_t(0)}{q_t(0)} \right\} & \text{if } q_t(0) < 0.5 \\ \Pr\left\{ -\frac{1}{n}\ln q_t(Y_t^n) \ge H(Y_t) - \frac{\delta}{\ln\frac{1-t(0)+pt(0)}{pt(0)}}\ln\frac{1-q_t(0)}{q_t(0)} \right\} & \text{if } q_t(0) > 0.5 \end{cases} \tag{4.13}$$

where Y_t is a random variable with distribution q_t. Consequently, we can apply the left NEP [28], chernoff bound, right NEP [28] with respect to entropy to upper bound $P(B_{t,n,\delta})$ when $q_t(0) <, =, > 0.5$, respectively.

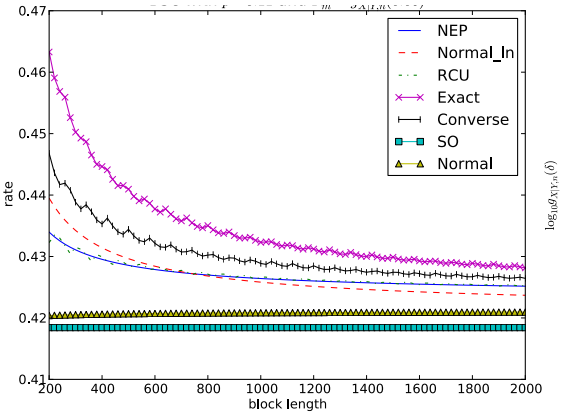
To provide benchmarks for the comparison of approximation formulas, exact evaluation of modified (3.47) (with $|\mathcal{X}|\frac{\ln(n+1)}{n}$ dropped and $t = t^*$) and (3.48) according to Remark 3.6 is provided, which, dubbed "Exact", serves as a converse bound, and the improved jar decoding achievability in (2.97) provides an achievable bound, dubbed "Jar". Figures 4.9 and 4.10 again show that the Normal curve is all over the map while the NEP curve always lies in between the Jar achievable curve and the Exact converse curve. It is also worth pointing out that if the capacity achieving distribution $t = p_X$ instead of t^* was chosen in the calculation of the Exact and Jar bounds, then both of them would be lower, confirming our early discussion that in the practical, non-asymptotic regime, the optimal marginal codeword symbol distribution is not necessarily a capacity achieving distribution.



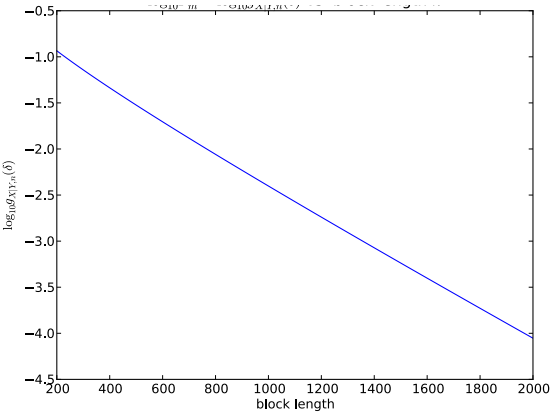
(a) Bounds with $P_e = 10^{-3}$



(b) $\delta_n(\epsilon)$ with $P_e = 10^{-3}$

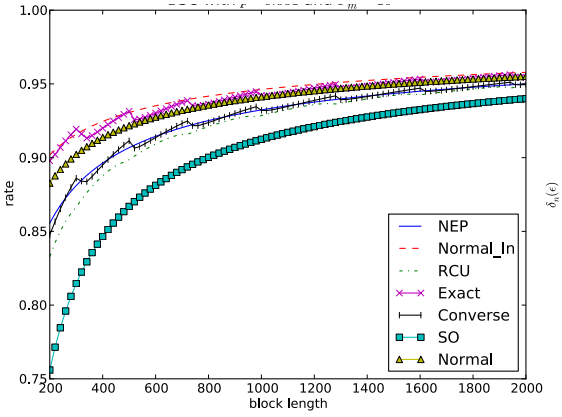


(c) Bounds with $P_e = g_{X|Y,n}(\delta)$ and $\delta = 0.06$

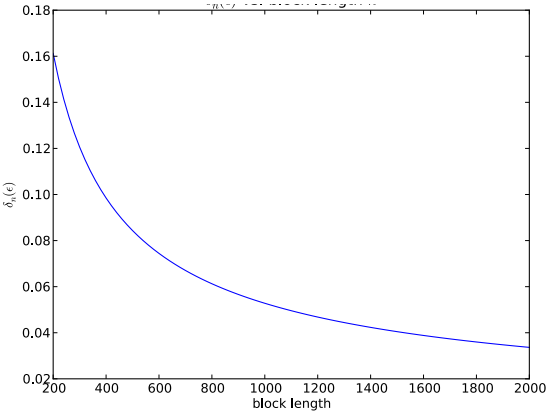


(d) $\log_{10} P_e$ with $P_e = g_{X|Y,n}(\delta)$ and $\delta = 0.06$

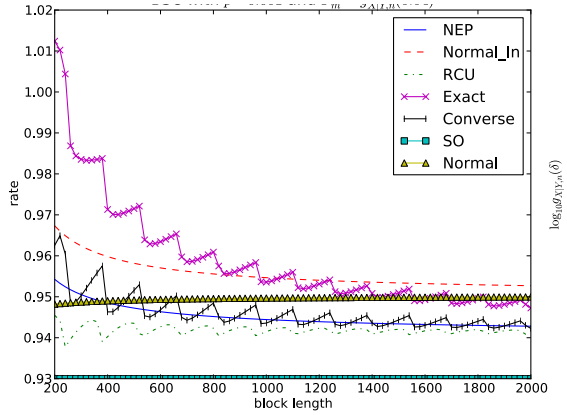
Figure 4.3: Comparison of different bounds for BSC with $p = 0.11$.



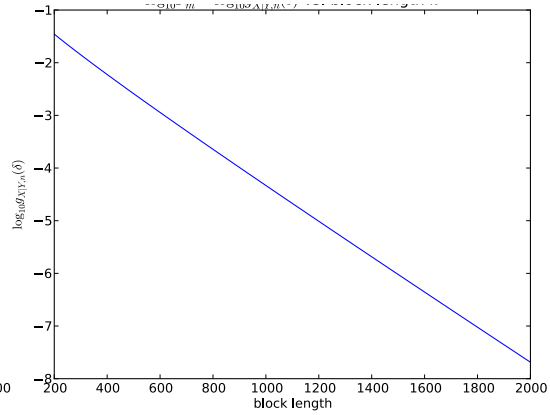
(a) Bounds with $P_e = 10^{-6}$



(b) $\delta_n(\epsilon)$ with $P_e = 10^{-6}$

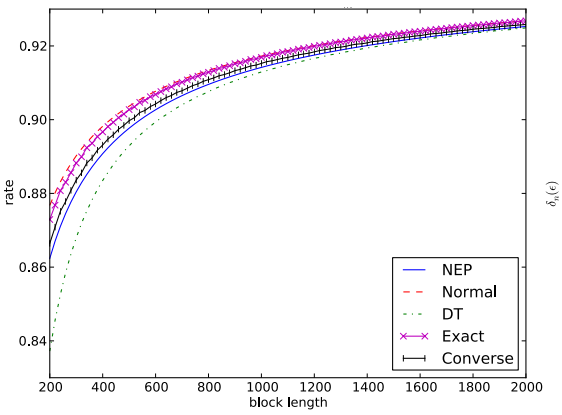


(c) Bounds with $P_e = g_{X|Y,n}(\delta)$ and $\delta = 0.04$

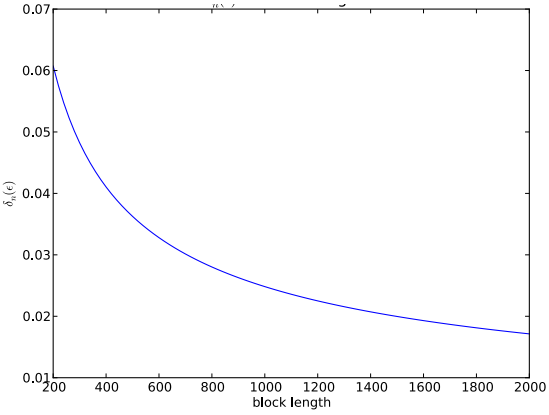


(d) $\log_{10} P_e$ with $P_e = g_{X|Y,n}(\delta)$ and $\delta = 0.04$

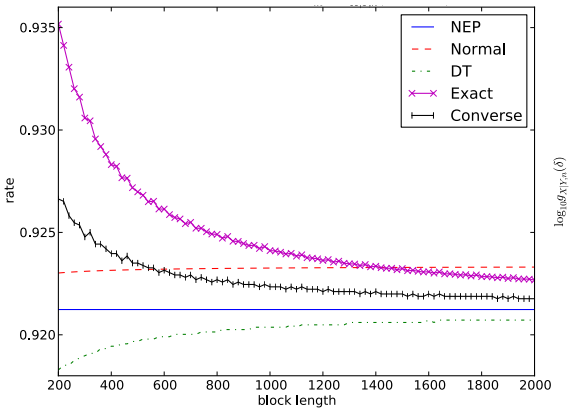
Figure 4.4: Comparison of different bounds for BSC with $p = 0.001$.



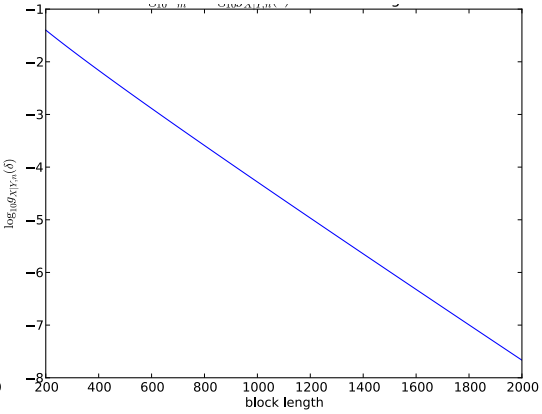
(a) Bounds with $P_e = 10^{-6}$



(b) $\delta_n(\epsilon)$ with $P_e = 10^{-6}$

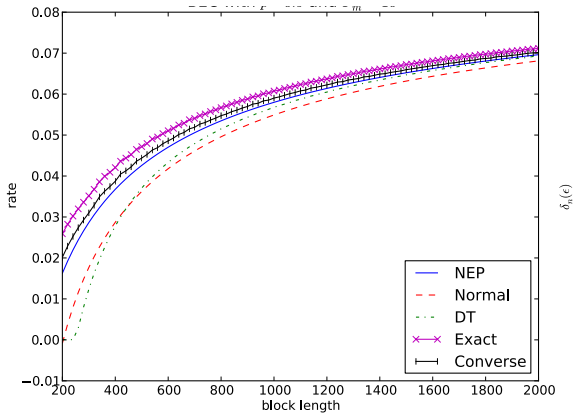


(c) Bounds with $P_e = g_{X|Y,n}(\delta)$ and $\delta = 0.0199$

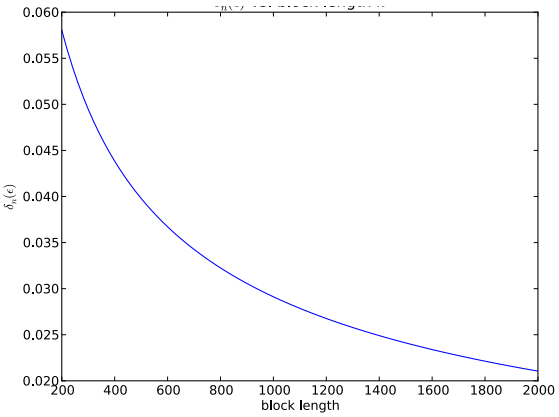


(d) $\log_{10} P_e$ with $P_e = g_{X|Y,n}(\delta)$ and $\delta = 0.0199$

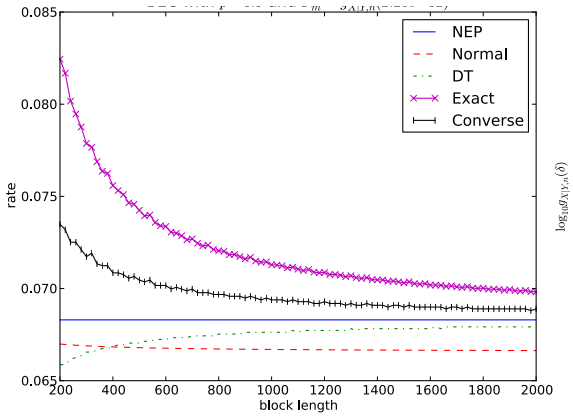
Figure 4.5: Comparison of different bounds for BEC with $p = 0.05$.



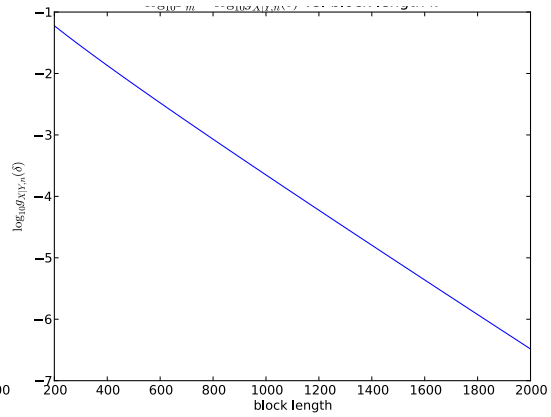
(a) Bounds with $P_e = 10^{-6}$



(b) $\delta_n(\epsilon)$ with $P_e = 10^{-6}$

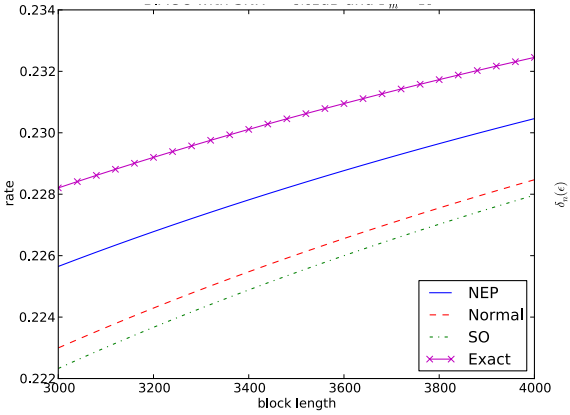


(c) Bounds with $P_e = g_{X|Y,n}(\delta)$ and $\delta = 0.022$

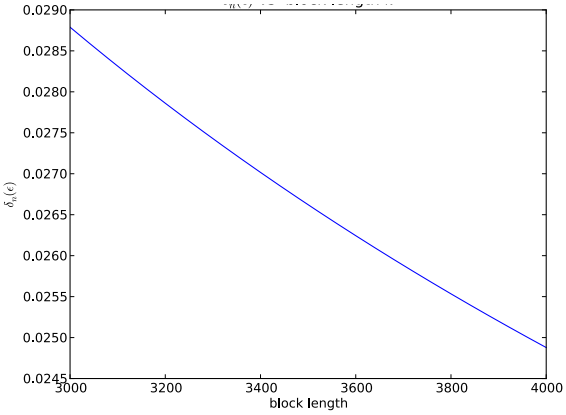


(d) $\log_{10} P_e$ with $P_e = g_{X|Y,n}(\delta)$ and $\delta = 0.022$

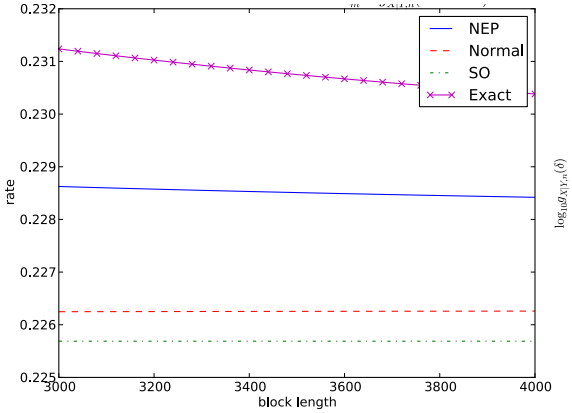
Figure 4.6: Comparison of different bounds for BEC with $p = 0.9$.

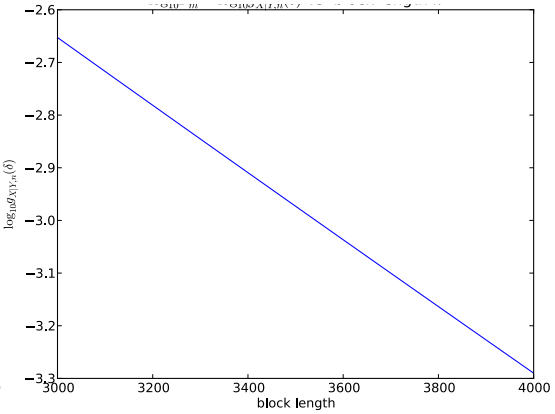


(a) Bounds with $P_e = 10^{-3}$



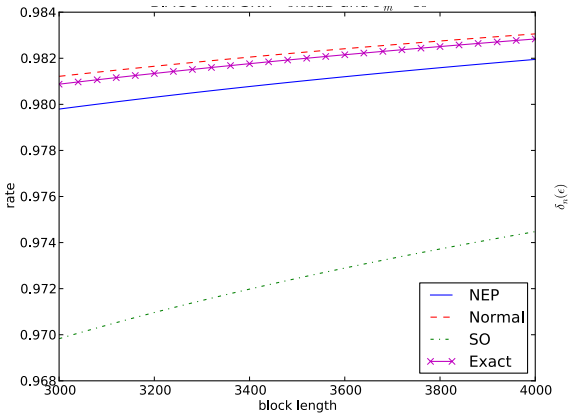
(b) $\delta_n(\epsilon)$ with $P_e = 10^{-3}$



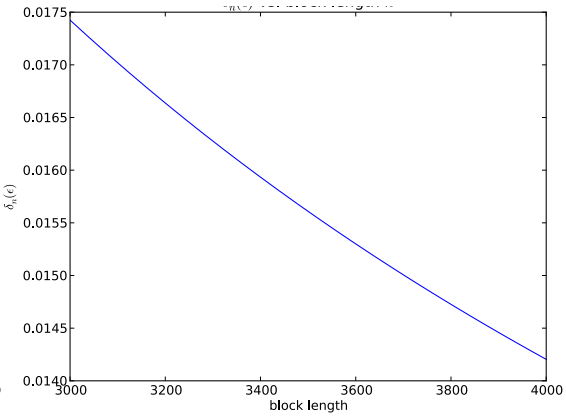


(c) Bounds with $P_e = g_{X|Y,n}(\delta)$ and $\delta = 0.0265$(d) $\log_{10} P_e$ with $P_e = g_{X|Y,n}(\delta)$ and $\delta = 0.0265$

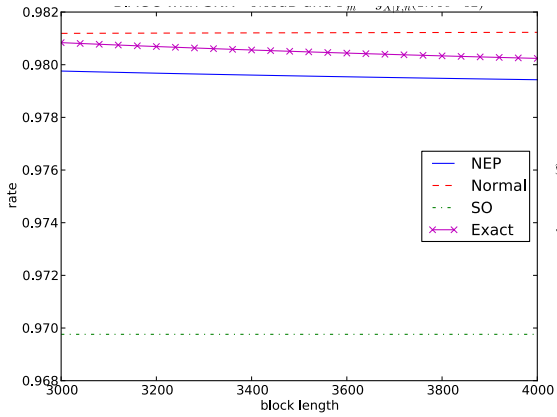
Figure 4.7: Comparison of different bounds for BIAGC with SNR $= -3.52$ dB.



(a) Bounds with $P_e = 10^{-9}$



(b) $\delta_n(\epsilon)$ with $P_e = 10^{-9}$



(c) Bounds with $P_e = g_{X|Y,n}(\delta)$ and $\delta = 0.0175$(d) $\log_{10} P_e$ with $P_e = g_{X|Y,n}(\delta)$ and $\delta = 0.0175$

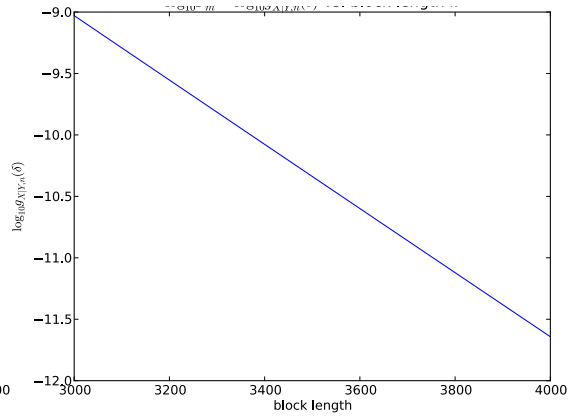
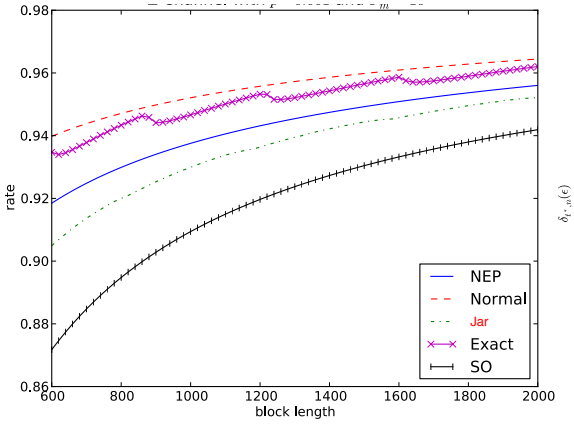
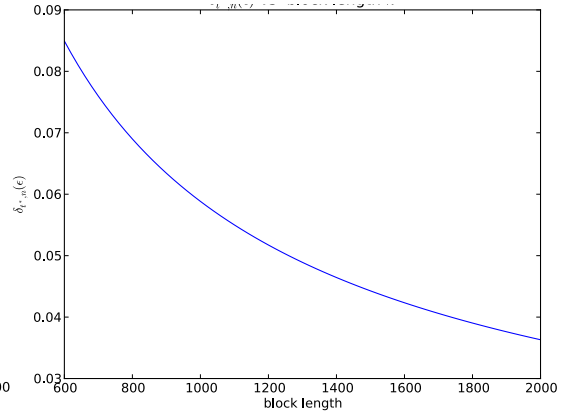


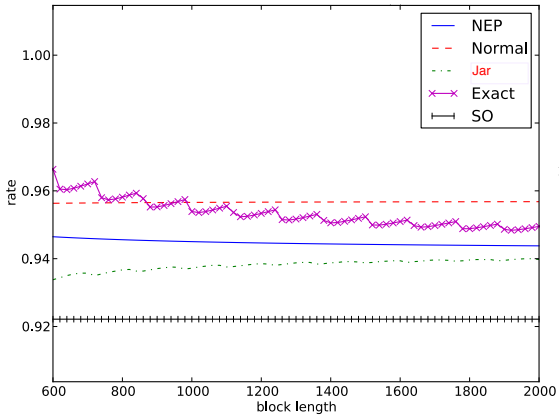
Figure 4.8: Comparison of different bounds for BIAGC with SNR = 9.63 dB.



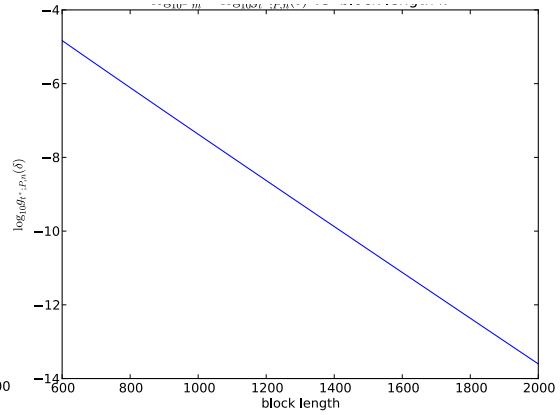
(a) Bounds with $P_e = 10^{-9}$



(b) $\delta_{t^*,n}(\epsilon)$ with $P_e = 10^{-9}$

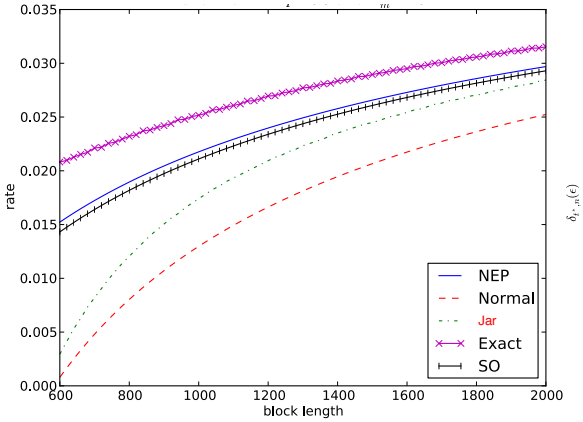


(c) Bounds with $P_e = g_{t^*;P,n}(\delta)$ and $\delta = 0.05$

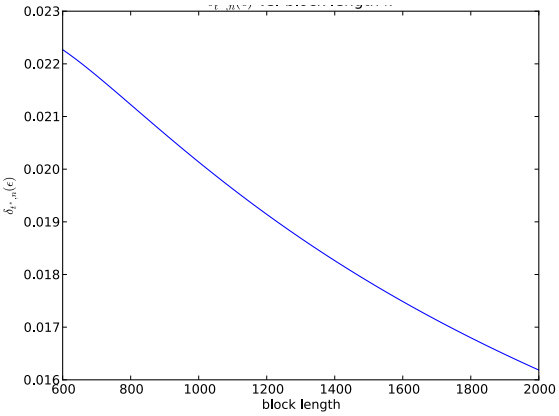


(d) $\log_{10} P_e$ with $P_e = g_{t^*;P,n}(\delta)$ and $\delta = 0.05$

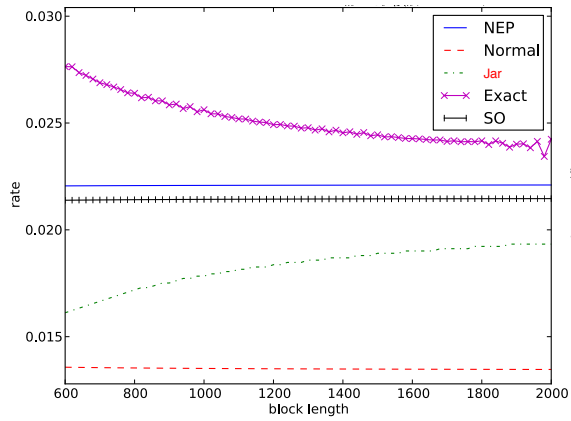
Figure 4.9: Comparison of different bounds for Z Channel with $p = 0.001$.



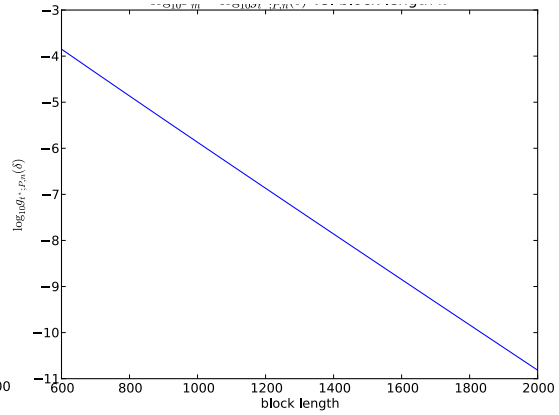
(a) Bounds with $P_e = 10^{-6}$



(b) $\delta_{t^*,n}(\epsilon)$ with $P_e = 10^{-6}$



(c) Bounds with $P_e = g_{t^*;P,n}(\delta)$ and $\delta = 0.02$



(d) $\log_{10} P_e$ with $P_e = g_{t^*;P,n}(\delta)$ and $\delta = 0.02$

Figure 4.10: Comparison of different bounds for Z Channel with $p = 0.9$.

4.4 Application of Taylor Expansion on Adaptive Modulation and Coding

As shown in Section 4.3, Taylor expansion of $R_n(\epsilon)$ provides a very good approximation of $R_n(\epsilon)$. This section is then devoted to illustrating one application of the Taylor expansion to practical systems due to this property. Towards this, we consider a coding technique called adaptive modulation and coding (AMC) . Particularly, we propose to use the Taylor expansion to guide the selection of constellations and coding rates in AMC, and the simulation on a practical communication system adopting the AMC technique, Long Term Evoluation (LTE), confirms that the guidance provided by the Taylor expansion can improve the system performance.

4.4.1 Motivation and Problem Formulation

AMC [32] is widely adopted in wireless communication systems, where the physical channel condition can fluctuate from time to time. In such systems, multiple constellations are available, channel codes can operate at different coding rates, and the transmitter has the flexibility to select a constellation and a channel coding rate to match the channel condition or simply single-to-noise ratio (snr) when the channel model is AWGN. Consequently, an important issue to be addressed in those systems is how to determine which constellation and channel coding rate should be used given the channel snr.

Specifically, consider the AMC system depicted in Figure 4.11. We assume that i^k and c^m are binary vectors, x^n has unit power, i.e.

$$\frac{1}{n}\sum_{i=1}^{n}|x_i|^2 = 1, \tag{4.14}$$

the system has a constant power E, the channel gain h fluctuates, but does not change during the period of transmitting x^n (block fading), and z^n is an independent and identically distributed (i.i.d) Gaussian noise (real or complex) vector with variance $\sigma^2/2$ per dimension. The channel snr is then calculated as

$$\gamma = \frac{h^2 E}{\sigma^2} \tag{4.15}$$

when both x^n and z^n are complex, and as

$$\gamma = \frac{2h^2 E}{\sigma^2} \tag{4.16}$$

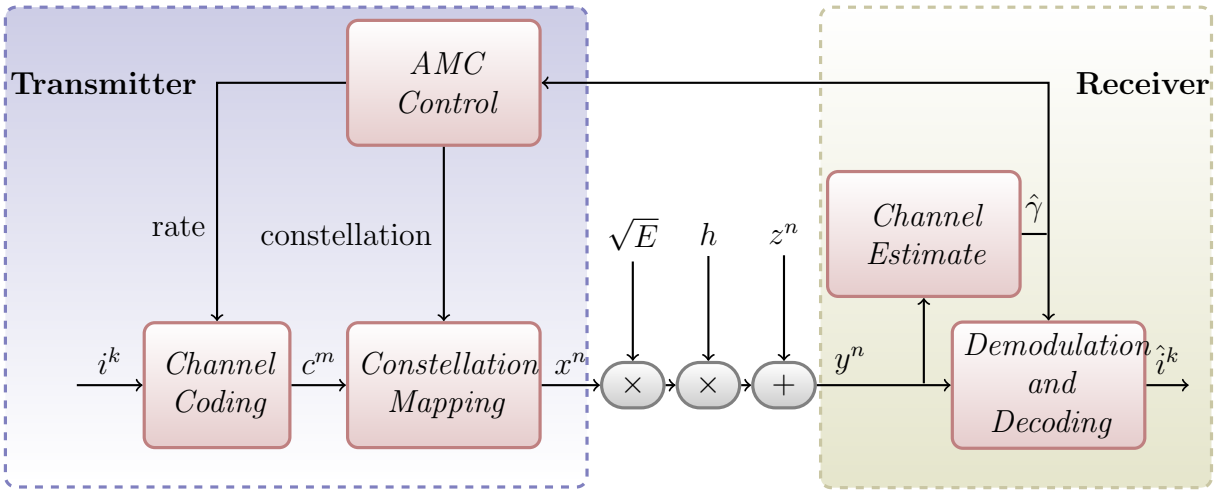


Figure 4.11: Adaptive Modulation and Coding System

when both x^n and z^n are real. Furthermore, the channel estimate is assumed to be perfect, i.e. $\hat{\gamma} = \gamma$. To avoid possible confusion, let $r = \frac{k}{m} \ln 2$ denote the channel coding rate (also called Effective Coding Rate (ECR)) and $R = \frac{k}{n} \ln 2$ denote the spectral efficiency (also called Modulation Order Product Coding Rate (MPR)). It is easy to see that

$$R = r \log_2 M \tag{4.17}$$

where M is the size of the constellation. And the job of AMC control is to select the constellation and r based on γ to maximize R under certain requirement of error probability $\epsilon = \Pr\{\hat{i}^k \neq i^k\}$, or simply the throughput

$$th = (1 - \epsilon)R. \tag{4.18}$$

In this section, we mainly focus on how to design the selecting rules used by AMC control on constellations and ECRs based on the channel snr to maximize the throughput of AMC system, given available constellations and channel codes.

For any practical system, such selecting rules can be determined through simulation [33]. However, due to the continuous snr and enormous combinations of constellations and ECRs available in practical systems, this design approach is very tedious. Moreover, the selecting rule designed in this way is sensitive to the actual implementation of the system and simulation setup. Therefore, some theoretical guidance is needed. Some light on this issue

may be shed by analysis based on channel capacity. However, as channel capacity analysis always assumes that the block length of modulation and coding scheme approaches infinite and the block error probability approaches 0, it fails to consider various factors of practical systems, such as the finite block length and the trade-off between the spectral efficiency and the block error probability to achieve the optimal throughput. This motivates us to use the taylor expansion of the optimal channel coding rate to design constellations and rate selection in AMC systems.

4.4.2 Taylor Expansion of Optimal Spectral Efficiency of Modulation and Coding over AWGN Channel

Consider any discrete input continuous output channel $P = \{p(y|x), x \in \mathcal{X}, y \in \mathcal{Y}\}$ with channel input alphabet $\mathcal{X}$ and channel output alphabet $\mathcal{Y}$. (In the setting of AMC, $\mathcal{X}$ would be the selected constellation.) A channel code with alphabet $\mathcal{X}$ is said to have a type t if all of its codewords share the same type t. Now let $R_{t,n}(\epsilon)$ denote the best coding rate that can be achieved by any channel code of finite block length n, block error probability ϵ and type t. Then it has been shown that[†]

$$R_{t,n}(\epsilon) \approx I(t;P) - \delta_{t;P,n}(\epsilon), \tag{4.19}$$

The interpretations of $I(t;P)$ and $\delta_{t;P,n}(\epsilon)$ are provided as follows:

- $I(t;P)$ is the mutual information between a random variable on $\mathcal{X}$ with the distribution t and its corresponding channel output, and is the best coding rate that can be possibly approached by any channel code of type t when $n \to +\infty$ and $\epsilon \to 0$; and
- $\delta_{t;P,n}(\epsilon)$ is the rate penalty resulting from using finite block length n while maintaining the block error probability ϵ.

Now we would like to apply (4.19) to the modulation and coding scheme in Figure 4.11. As mentioned before, in this case, $\mathcal{X}$ is the constellation in use. Let t be the type shared by all the possible constellation mapping output x^n. According to (4.14), t and $\mathcal{X}$ satisfy

$$\sum_{x \in \mathcal{X}} t(x)|x|^2 = 1. \tag{4.20}$$

[†] $\delta_{t;P,n}(\epsilon)$ was previously defined as $\delta_{t,n}(\epsilon)$. Here we insert the subscript P in $\delta_{t,n}(\epsilon)$ to emphasize the dependency of $\delta_{t;P,n}(\epsilon)$ on P.

Then the channel can be modelled as

$$Y = h\sqrt{E}X + Z \tag{4.21}$$

where X is a random variable on $\mathcal{X}$ with the distribution t and Z is the Gaussian noise with variance $\sigma^2/2$ per dimension. It is not hard to verify that the transition probability $p(y|x)$ is determined by snr γ. As such, let $P_{\mathcal{X},\gamma}$ denote the channel with input alphabet $\mathcal{X}$, output alphabet $\mathbb{C}$ (which is the complex plane when $\mathcal{X}$ is two dimensional as in the case of QPSK, 16QAM and 64QAM), and the transition probability determined by (4.21) with snr γ. By applying (4.19), the best spectral efficiency that can be achieved by any modulation and coding scheme of block length n, block error probability ϵ, type t and constellation $\mathcal{X}$ (satisfying (4.20)) over AWGN channel with snr γ, denoted by $R_{\mathcal{X},t,n}(\gamma,\epsilon)$, is approximated by

$$R_{\mathcal{X},t,n}(\gamma,\epsilon) \approx I\left(t; P_{\mathcal{X},\gamma}\right) - \delta_{t;P_{\mathcal{X},\gamma},n}(\epsilon) \tag{4.22}$$

and the best achievable throughput $th_{\mathcal{X},t,n}(\gamma)$ is then approximated by

$$th_{\mathcal{X},t,n}(\gamma) \approx \max_{\epsilon}(1-\epsilon)R_{\mathcal{X},t,n}(\epsilon,\gamma). \tag{4.23}$$

Also denote the optimal ϵ and the corresponding $R_{\mathcal{X},t,n}(\epsilon,\gamma)$ achieving the maximal throughput in (4.23) by $\epsilon^{th}_{\mathcal{X},t,n}(\gamma)$ and $R^{th}_{\mathcal{X},t,n}(\gamma)$ respectively.

4.4.3 Constellation and Rate Selection based on Taylor Expansion

Based on taylor expansion, particularly (4.23) in the previous subsection, we now discuss how to design selecting rules on constellations and ECRs in an AMC system.

Suppose that $\mathcal{X}_1, \mathcal{X}_2, \ldots, \mathcal{X}_m$ are the available constellations, and for each $\mathcal{X}_i$, the type of output sequences of constellation mapping is fixed to be t_i. (In a practical AMC system, t_i is often the uniform distribution over $\mathcal{X}_i$.) Whenever there is no ambiguity, the subscript i in t_i will be dropped in our subsequent discussion. Based on (4.23), a selecting rule can be designed in theory as follows:

S1 For any snr γ, calculate $th_{\mathcal{X}_i,t,n}(\gamma)$ for $1 \le i \le m$ and determine

$$i^* = \arg\max_{1\le i\le m} th_{\mathcal{X}_i,t,n}(\gamma). \tag{4.24}$$

S2 Select $\mathcal{X}_{i^*}$ as the desired constellation, and calculate the desired ECR according to

$$r = \frac{R^{th}_{\mathcal{X}_{i^*},t,n}(\gamma)}{\log_2 |\mathcal{X}_{i^*}|}. \tag{4.25}$$

When applied to a practical AMC system, however, the above selecting rule has to be modified slightly. Since $th_{\mathcal{X}_i,t,n}(\gamma)$ is the maximal achievable throughput with the constellation $\mathcal{X}_i$, where optimal encoding and optimal demodulation/decoding are assumed, a practical system normally needs to sacrifice a certain amount of snr in order to achieve the throughput $th_{\mathcal{X}_i,t,n}(\gamma)$ with the constellation $\mathcal{X}_i$. In other words, at the snr γ, the throughput that a practical system can achieve with the constellation $\mathcal{X}_i$ is likely $th_{\mathcal{X}_i,t,n}(\gamma - \Delta\gamma_i)$, where $\Delta\gamma_i$ is the corresponding snr penalty. In general, larger the constellation $\mathcal{X}_i$ is, more difficult it is to achieve $th_{\mathcal{X}_i,t,n}(\gamma)$, and hence larger the snr penalty $\Delta\gamma_i$. The exact value of $\Delta\gamma_i$ of course depends on the implementation of channel encoding, demodulation, and decoding in the practical AMC system, and can be easily determined by simulation. Replacing $th_{\mathcal{X}_i,t,n}(\gamma)$ by $th_{\mathcal{X}_i,t,n}(\gamma - \Delta\gamma_i)$ in (4.24) and (4.25), we then get the following modified selecting rule:

S1 Determine, for each constellation $\mathcal{X}_i$, the the snr penalty $\Delta\gamma_i$.

S2 Calculate $th_{\mathcal{X}_i,t,n}(\gamma - \Delta\gamma_i)$ for $1 \le i \le m$ and determine

$$i^* = \arg\max_{1\le i\le m} th_{\mathcal{X}_i,t,n}(\gamma - \Delta\gamma_i). \tag{4.26}$$

S3 Select $\mathcal{X}_{i^*}$ as the desired constellation, and calculate the desired ECR according to

$$r = \frac{R^{th}_{\mathcal{X}_{i^*},t,n}(\gamma - \Delta\gamma_i)}{\log_2 |\mathcal{X}_{i^*}|}. \tag{4.27}$$

4.4.4 Application to the LTE System

Towards confirming that the selecting rule designed in Section 4.4.3 works in practice, let us consider the LTE system. More specifically, we consider Physical Downlink Shared CHannel (PDSCH) with Single-Input and Single-Output (SISO) mode [34], in which the AMC system [35] [36] can be represented by the diagram in Figure 4.12. As can be seen in Figure 4.12, the channel coding output is scrambled by a pseudo-random sequence before constellation mapping, and therefore the scrambled channel codeword will have the uniform

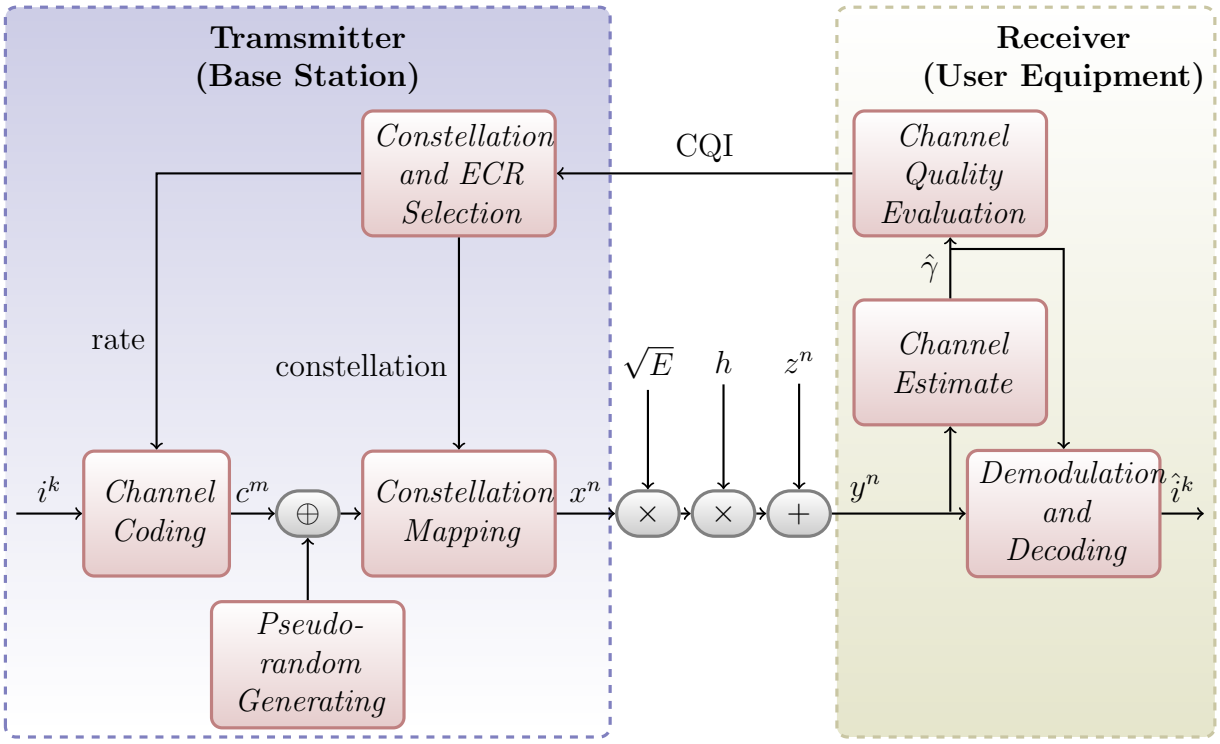


Figure 4.12: Adaptive Modulation and Coding in the LTE system

type, as well as the output sequence of constellation mapping, which implies that uniform t should be used in the taylor expansion. Another major change compared to Figure 4.11 is that AMC control is broken into two parts, i.e. Constellation and ECR Selection and Channel Quality Evaluation, at the transmitter and receiver side respectively. In this diagram, the receiver generates Channel Quality Index (CQI) based on the channel snr and sends it to the transmitter, while the transmitter selects constellations and ECRs according to CQI and Table 4.1, where the available constellations are QPSK, 16QAM and 64QAM, denoted by $\mathcal{X}_1$, $\mathcal{X}_2$ and $\mathcal{X}_3$ respectively, and the channel code is a turbo code whose rate can be adjusted by rate matching. Particularly, the receiver is required to generate the highest CQI index that results in the block error probability $\leq 10^{-1}$. This change is due to the fact that there may be different implementation of receivers (User Equipment), and the transmitter (Base Station) should be able to work with any implementation of receivers. As the different implementation of receivers will influence the selection of constellations and ECRs in the AMC system, more control on the selection is assigned to the receiver

CQI Index	Modulation	ECR	MPR
1	QPSK	78/1024	0.1523
2	QPSK	120/1024	0.2344
3	QPSK	193/1024	0.3770
4	QPSK	308/1024	0.6016
5	QPSK	449/1024	0.8770
6	QPSK	602/1024	1.1758
7	16QAM	378/1024	1.4766
8	16QAM	490/1024	1.9141
9	16QAM	616/1024	2.4063
10	64QAM	466/1024	2.7305
11	64QAM	567/1024	3.3223
12	64QAM	666/1024	3.9023
13	64QAM	772/1024	4.5234
14	64QAM	873/1024	5.1152
15	64QAM	948/1024	5.5547

Table 4.1: CQI Table

Parameter	Assumption
Channel Type	PDSCH
Transmission Mode	1
Channel Model	AWGN
Bandwidth	1.4MHz
Number of User Equipments (UE)	1
Number of receive antennas at UE	1
Cyclic Prefix (CP)	Normal
Channel Estimation	Perfect

Table 4.2: Specification of System Parameters

side. The selecting rule proposed in the previous section also works in this modified AMC system, where different receiver implementation will result in different set of snr shifting $\{\Delta\gamma_i\}_{i=1}^{3}$. In this section, we focus on the implementation of LTE system in [37].

Specifications of system parameters are listed in Table 4.2 for easy references, which apply to all simulations throughout this subsection. Moreover, by inspection on frequency-time resources of the LTE system (for single antenna port), it is not hard to verify that

under the specification in Table 4.2 the block length (of modulation symbols) for data transmission in each subframe is 960.[‡]

Now to apply the modified selecting rule in Section 4.4.3 to LTE system, we would like to determine $\{\Delta\gamma_i\}_{i=1}^3$ under this implementation of the system. Therefore, shown in Figure 4.13, $\{th_{\mathcal{X}_i,t,n}(\gamma)\}_{i=1}^3$ is compared with the throughput of the LTE system using the modulation constellations and ECRs in Table 4.1. The simulation on the LTE system takes 5000 subframes, where snr ranges from -10dB to 22.5dB. From Figure 4.13, $\Delta\gamma_1$, $\Delta\gamma_2$ and $\Delta\gamma_3$ are estimated to be 1.3dB, 1.9dB and 2.4dB respectively. Strictly speaking, $\{\Delta\gamma_i\}_{i=1}^3$ also depends on snr γ. However, this dependency is not significant, and therefore ignored here for simplicity of the selecting rule.

Then $\{th_{\mathcal{X}_i,t,n}(\gamma-\Delta\gamma_i)\}_{i=1}^3$ and the throughput of LTE system using the modulation constellations and ECRs in Table 4.1 are plotted in Figure 4.14, and careful inspection of this figure suggests that the throughput of LTE system can be improved by using some new combination of constellations and ECRs, which are not included in Table 4.1.

In particular, let us focus on the snr region $[4,5]$dB, where Figure 4.15 is yielded by zooming in Figure 4.14. At snr 4.6dB, simulation shows that CQI 06 is the highest CQI index such that the resulting block error probability $\leq 10^{-1}$, as the block error probability of CQI 07 is 0.1224. Therefore, according to the CQI reporting policy, CQI 06 should be selected even though the throughput of CQI 07 is higher. On the other hand, $th_{\mathcal{X}_1,t,n}(\gamma-\Delta\gamma_1)$ and $th_{\mathcal{X}_2,t,n}(\gamma-\Delta\gamma_2)$ reveal that the throughput can be improved by using QPSK and a proper ECR. Now applying the modified selecting rule in Section 4.4.3 for $\gamma=4.6$dB yields QPSK and ECR $\frac{720}{1024}$, where rounding ensures ECR$\times$1024 to be an integer. And simulation of LTE system with QPSK and ECR $\frac{720}{1024}$ shown in Figure 4.16 confirms that this new combination of constellation and ECR provides 20% and 8% gain on the throughput of LTE system at snr 4.6dB over CQI 06 and 07 respectively. It is also worth mentioning here that the block error probability of this new combination at snr 4.6dB is 0.0018, which satisfies the requirement of 0.1 in the LTE system.

Similarly, snr region $[11,13]$dB is considered in Figure 4.17, which shows that at snr 12dB CQI 10 should be selected according to the CQI reporting policy. On the other hand, applying the modified selecting rule at snr 12dB yields 16QAM and ECR $\frac{789}{1024}$, and simulation of LTE system with this combination in Figure 4.18 shows that the throughput is improved by 13% at snr 12dB.

[‡]Resource elements (RE) used by reference signals are excluded when calculating the block length. However, for simplicity of the discussion, we do not take into account the synchronization which only happens every 5 subframes.

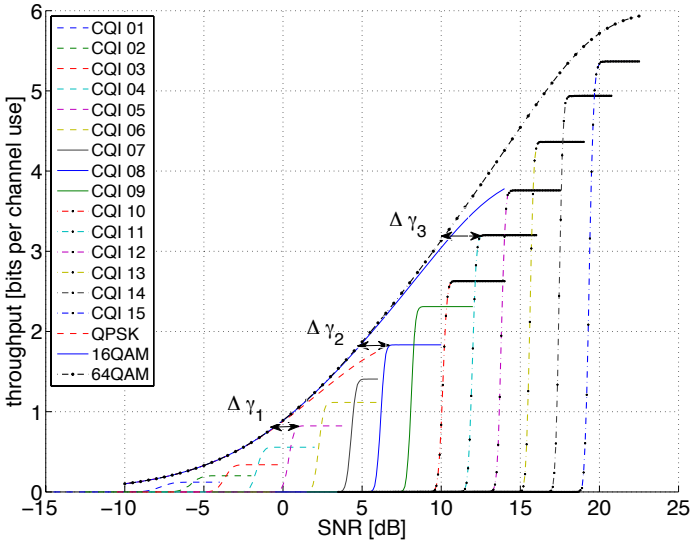


Figure 4.13: $\{th_{\mathcal{X}_i,t,n}(\gamma)\}_{i=1}^{3}$ vs. the Throughput of LTE System

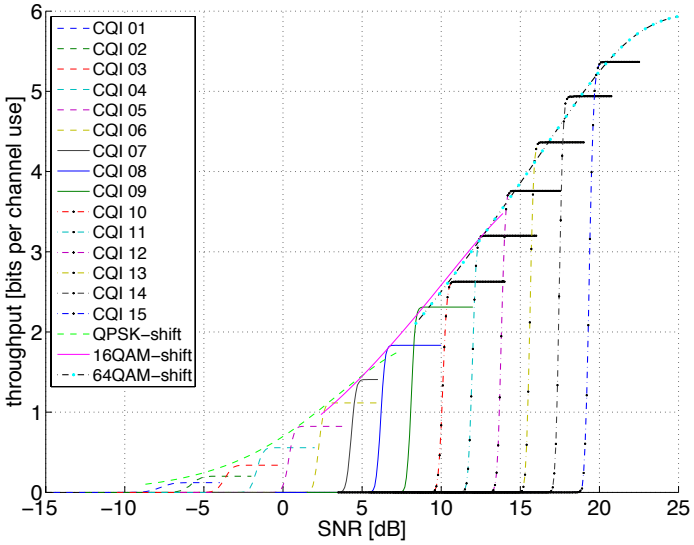


Figure 4.14: $\{th_{\mathcal{X}_i,t,n}(\gamma - \Delta\gamma_i)\}_{i=1}^{3}$ vs. the Throughput of LTE System

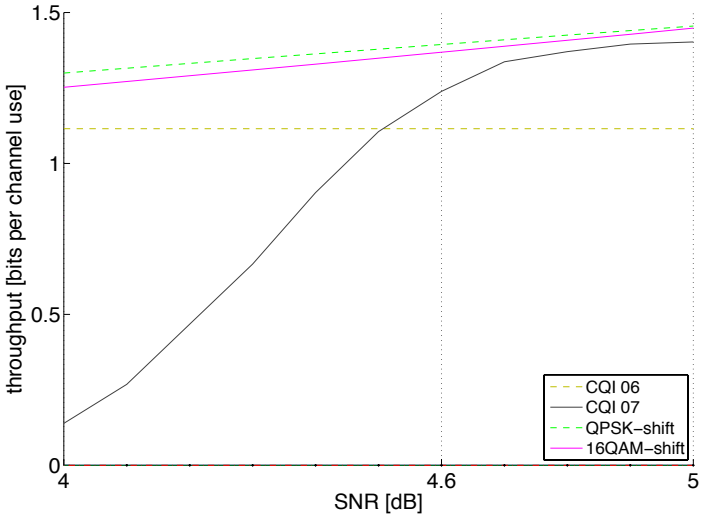


Figure 4.15: SNR Region 4-5dB

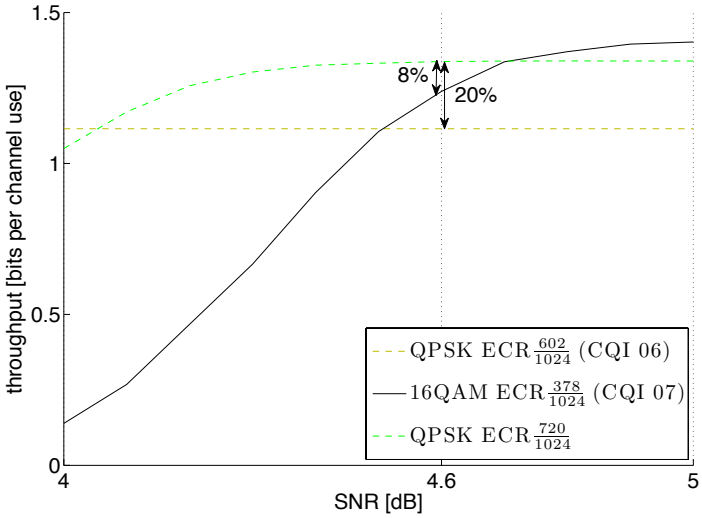


Figure 4.16: Throughput Improvement over CQI 7

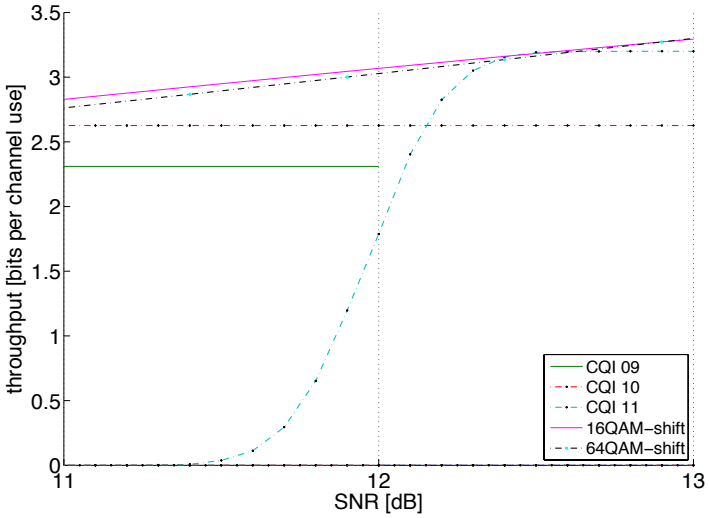


Figure 4.17: SNR Region 11-13dB

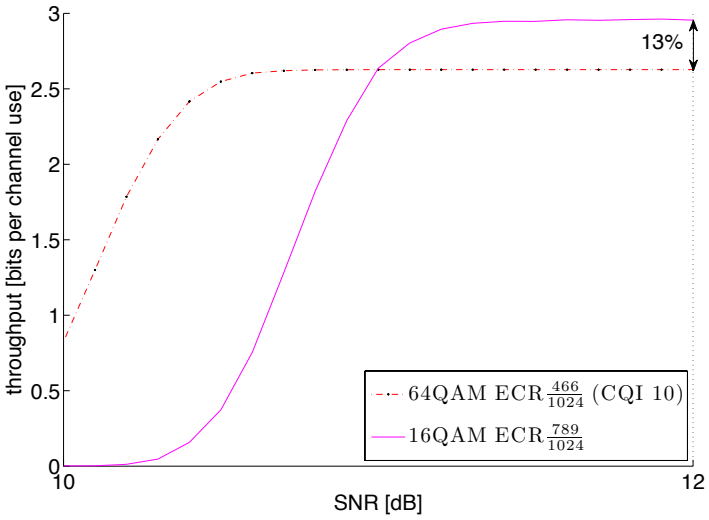


Figure 4.18: Throughput Improvement over CQI 10

4.5 Summary

Combining non-asymptotic converses in Chapter 3 with the non-asymptotic achievability proved in Chapter 2 via jar decoding and with the NEP technique developed in Appendix A, we have characterized the best coding rate $R_n(\epsilon)$ achievable with finite block length n and error probability ϵ through introducing a quantity $\delta_{t,n}(\epsilon)$ to measure the relative magnitude of the error probability ϵ and block length n with respect to a given channel P and an input distribution t. We have showed that in the non-asymptotic regime where both n and ϵ are finite, $R_n(\epsilon)$ has a Taylor-type expansion with respect to $\delta_{t,n}(\epsilon)$, where the first two terms of the expansion are $\max_t[I(t;P) - \delta_{t,n}(\epsilon)]$, which is equal to $I(t^*,P) - \delta_{t^*,n}(\epsilon)$ for some optimal distribution t^*, and the third order term of the expansion is $O(\delta^2_{t^*,n}(\epsilon))$ or $O\left(\ln n/n\right)$ whichever is larger. As a consequence of those results in this chapter, we show that jar decoding achieves the first and second order term in the taylor expansion of the best coding rate.

Moreover, based on the new non-asymptotic converses and the Taylor-type expansion of $R_n(\epsilon)$, we have also derived two approximation formulas (dubbed "SO" and "NEP") for $R_n(\epsilon)$. These formulas have been further evaluated and compared against some of the best bounds known so far, as well as the normal approximation revisited recently in the literature. It turns out that while the normal approximation is all over the map, i.e. sometime below achievability and sometime above converse, the SO approximation is much more reliable and stays at the same relative position to achievable and converse bounds; in the meantime, the NEP approximation is the best among the three and always provides an accurate estimation for $R_n(\epsilon)$.

It is expected that in the non-asymptotic regime where both n and ϵ are finite, the taylor expansion of $R_n(\epsilon)$ and the NEP approximation formula would play a role similar to that of channel capacity [38] in the asymptotic regime as $n \to \infty$. As an example of applications of the taylor expansion, we consider adaptive modulation and coding on AWGN channel, and propose a new selection rule of constellation and coding rate based on the taylor expansion. This new selection rule, when applied to LTE system, suggests some new combination of constellation and coding rate, which can further improve the throughput of the system.

Another possible application of the taylor expansion is to consider the optimal distribution t^*. For values of n and ϵ with practical interest for which $\delta_{t^*,n}(\epsilon)$ is not relatively small, the optimal distribution t^* achieving $\max_t[I(t;P) - \delta_{t,n}(\epsilon)]$ is in general not a capacity achieving distribution except for symmetric channels such as BIMSC. As a result, an important implication arising from the Taylor-type expansion of $R_n(\epsilon)$ is that in the

practical non-asymptotic regime, the optimal marginal codeword symbol distribution is not necessarily a capacity achieving distribution. Therefore, it will be interesting to examine all practical channel codes proposed so far against the Taylor-type expansion of $R_n(\epsilon)$ and the NEP approximation formula and to see how far their performance is away from that predicted by the Taylor-type expansion of $R_n(\epsilon)$ and the NEP approximation formula. If the performance gap is significant, one way to design a better channel code with practical block length and error probability requirement is to solve the maximization problem $\max_t[I(t;P)-\delta_{t,n}(\epsilon)]$, get t^*, and then design a code so that its marginal codeword symbol distribution is approximately t^*.

To sum up Chapters 2, 3 and 4, we have demonstrated that the NEP, jar decoding, and the outer mirror image of jar together form a set of essential techniques needed for non-asymptotic information theory. And we believe that they can also be extended and applied to help develop non-asymptotic multi-user information theory as well.

Chapter 5

LDPC Coding Theorems

In this chapter, the performance of LDPC codes under jar decoding for BSC and BIMC is analyzed, and certain interesting results are reported (including capacity-approaching LDPC codes and optimality of check node concentration degree distribution). Moreover, simulation results on LDPC codes under BP decoding is also included at the end of this chapter, showing the connection between BP decoding and jar decoding, i.e. BP decoding can be regarded as one of many ways to pick up a codeword from a jar.

5.1 Terminology, LDPC Ensemble and Key Lemma

To facilitate the following discussion, let us first introduce some terminology of LDPC codes. The tanner graph [39] of a linear code is a bipartite graph consisting of two sets of nodes $\{v_i\}_{i=1}^n$ and $\{c_j\}_{j=1}^m$, namely, variable and check nodes, where for any i and j such that $1 \leq i \leq n$ and $1 \leq j \leq m$, v_i and c_j, representing the i-th column and j-th row of $\mathbf{H}_{m\times n}$ respectively, are connected if and only if the element h_{ji} of $\mathbf{H}_{m\times n}$ located at i-th column and j-th row is equal to 1. Recall that the degree of a node in a graph is the number of edges connected to it. Now let $\{l_i : 1 \leq i \leq L\}$ ($\{r_j : 1 \leq j \leq R\}$, respectively) be the set of degrees of all variable nodes (check nodes, respectively) in the tanner graph of $\mathbf{H}_{m\times n}$. Furthermore, let Λ_i (P_j, respectively) denote the number of variable nodes (check nodes, respectively) with degree l_i (r_j, respectively) in the tanner graph of $\mathbf{H}_{m\times n}$. Then we call $(\{\Lambda_i\}, \{l_i\})$ $((\{P_j\}, \{r_j\})$, respectively) the variable (check, respectively) degree distribution from a node perspective of $\mathbf{H}_{m\times n}$ (and its tanner graph) [5]. Define polynomials $\Lambda(z)$ and

$P(z)$ as

$$\Lambda(z) = \sum_{i=1}^{L} \Lambda_i z^{l_i}$$

and

$$P(z) = \sum_{j=1}^{R} P_j z^{r_j}.$$

The tanner graph is said to be sparse and accordingly its corresponding code is said to be a low-density parity-check code if $\Lambda'(1)$ is in the order of $O(n)$, where $\Lambda'(1) = \sum_{i=1}^{L} \Lambda_i l_i$ is the total number of edges in the tanner graph. Normalizing $\{\Lambda_i\}$ and $\{P_j\}$ by the total numbers of variable nodes and check nodes respectively, we get normalized variable and check degree distributions $L(z)$ and $R(z)$:

$$L(z) = \sum_{i=1}^{L} L_i z^{l_i} = \frac{\Lambda(z)}{\Lambda(1)}$$

and

$$R(z) = \sum_{j=1}^{R} R_j z^{r_j} = \frac{P(z)}{P(1)}$$

where L_i and R_j represent the percentages of variable and check nodes with degrees l_i and r_j respectively.

Given m, n, and (normalized) variable and check degree distributions $L(z)$ and $R(z)$ satisfying $nL'(1) = mR'(1)$, let

$$\bar{l} \triangleq L'(1), \bar{r} \triangleq R'(1), \frac{\bar{l}}{\bar{r}} = \frac{m}{n}, \tag{5.1}$$

and $\mathcal{H}_{m,n,L(z),R(z)}$ denote the collection of all $m \times n$ parity check matrices with normalized variable and check degree distributions $L(z)$ and $R(z)$. Without loss of generality, we only consider those matrices such that the degrees of rows and columns do not decrease with their indices. (In other words, $i > j$ implies the degree of the i-th row (or column) is not less than that of the j-th row (or column).) Then an LDPC code of designed rate $(1 - m/n) \ln 2$ (in nats) is said to be randomly generated from the ensemble $\mathcal{C}_{m,n,L(z),R(z)}$ with degree distributions $L(z)$ and $R(z)$ if its parity check matrix $\mathbf{H}_{m\times n}$ is uniformly picked from $\mathcal{H}_{m,n,L(z),R(z)}$. Denote the designed rate $(1 - m/n) \ln 2$ as $\mathcal{R}(\mathcal{C}_{m,n,L(z),R(z)})$. The encoding procedure of $\mathcal{C}_{m,n,L(z),R(z)}$ is assumed to be systematic so that the original information bits are visible in each codeword.

To establish our LDPC coding theorems, the following probability

$$\Pr\{\mathbf{H}_{m\times n}x^n = 0^m\}$$

is investigated first, which depends on the support set of x^n, i.e., the positions of non-zero elements in x^n. Let $\varkappa(x^n)$ represent the support set of x^n, and we write $\varkappa(x^n)$ simply as $\varkappa$ whenever x^n is generic or can be determined from context. Let $\mathbf{H}^{\varkappa}_{m\times|\varkappa|}$ be the matrix consisting of those columns of $\mathbf{H}_{m\times n}$ with indices in $\varkappa$. The degree polynomial of $\varkappa$, denoted by $L^{\varkappa}(z)$, is defined by

$$L^{\varkappa}(z) \triangleq \sum_{i=1}^{L} L_i^{\varkappa} z^{l_i}$$

where $L_i^{\varkappa} n$ is the number of columns with degree l_i within $\mathbf{H}^{\varkappa}_{m\times|\varkappa|}$. And define

$$\bar{l}^{\varkappa} \triangleq \sum_{i=1}^{L} L_i^{\varkappa} l_i.$$

Then the following lemma is provided first and proved in Appendix B.2.

Lemma 5.1. *Let $L(z)$ and $R(z)$ be normalized variable and check node degree distributions from a node perspective with minimum variable node degree $l_1 \geq 1$. Let $g(\tau,k) \triangleq (1+\tau)^k + (1-\tau)^k$ for any τ and k. Suppose $\mathbf{H}_{m\times n}$ $(m \leq n)$ is uniformly picked from ensemble $\mathcal{H}_{m,n,L(z),R(z)}$. Then for any $x^n \neq 0$ with its support set $\varkappa$,*

$$\Pr\{\mathbf{H}_{m\times n}x^n = 0^m\} \leq \exp\left\{nP\left(\bar{l},R(z),\bar{l}^{\varkappa}\right) + \frac{\ln(n\hat{l}^{\varkappa})}{2}\sum_{i=1}^{R} r_i + \frac{1}{2}\ln n\bar{l}^{\varkappa}\left(1-\frac{\bar{l}^{\varkappa}}{\bar{l}}\right) + O(1)\right\}$$

where

$$\hat{l}^{\varkappa} = \frac{\min\left\{\bar{l}^{\varkappa}, \bar{l}-\bar{l}^{\varkappa}\right\}}{2} + \frac{1}{n}$$

and for any $\bar{l}$, $\xi \in (0,\bar{l}]$ and $R(z)$, $P\left(\bar{l},R(z),\xi\right)$ is defined as

$$P\left(\bar{l},R(z),\xi\right) \triangleq -\bar{l}H\left(\xi/\bar{l}\right) - \xi\ln\tau + \frac{\bar{l}}{\bar{r}}\sum_{i=1}^{R} R_i \ln\frac{g(\tau,r_i)}{2} \tag{5.2}$$

in which τ is the solution to

$$\frac{\bar{l}}{\bar{r}}\sum_{i=1}^{R} R_i r_i \frac{g(\tau,r_i-1)}{g(\tau,r_i)} = \bar{l}-\xi \tag{5.3}$$

for $\xi \in \left[0, \bar{l} - \frac{\bar{l}}{\bar{r}} \sum_{j=1}^{R} R_j \pi(r_j)\right]$, *and*

$$P\left(\bar{l}, R(z), \xi\right) \stackrel{\Delta}{=} -\infty \tag{5.4}$$

for $\xi \in \left(\bar{l} - \frac{\bar{l}}{\bar{r}} \sum_{j=1}^{R} R_j \pi(r_j), \bar{l}\right]$ *with the convention that* $e^{-\infty} = 0$, *and where for any integer* r

$$\pi(r) = \begin{cases} 0 & \text{if } r \text{ is even} \\ 1 & \text{otherwise.} \end{cases}$$

Remark 5.1. *When* $\xi = \bar{l} - \frac{\bar{l}}{\bar{r}} \sum_{j=1}^{R} R_j \pi(r_j)$, *the solution* τ *to (5.3) is* $\tau = +\infty$. *In this case, the expression in (5.2) should be understood as its limit as* $\tau \to +\infty$, *i.e.,*

$$\begin{aligned} & P\left(\bar{l}, R(z), \xi\right) \\ & \stackrel{\Delta}{=} -\bar{l} H\left(\xi/\bar{l}\right) + \lim_{\tau \to +\infty} \left[-\xi \ln \tau + \frac{\bar{l}}{\bar{r}} \sum_{i=1}^{R} R_i \ln \frac{g(\tau, r_i)}{2} \right] \\ & = -\bar{l} H\left(\xi/\bar{l}\right) + \frac{\bar{l}}{\bar{r}} \sum_{i=1}^{R} R_j \pi(r_i) \ln r_i \end{aligned} \tag{5.5}$$

when $\xi = \bar{l} - \frac{\bar{l}}{\bar{r}} \sum_{j=1}^{R} R_j \pi(r_j)$.

A number of Lemmas about the properties of $P(\bar{l}, R(z), \xi)$ are provided in Appendix B.2.1. In particular, applying Lemmas B.8 and B.9 yields

$$\begin{aligned} & \Pr\left\{\mathbf{H}_{m \times n} z^n = 0^m\right\} \\ & \leq \exp\left\{ n \left(P\left(\bar{l}, R(z), l_1 \epsilon\right) + \left(\frac{1}{2n} \ln \frac{n\bar{l}}{2}\right) \sum_{i=1}^{R} r_i + \frac{1}{2n} \ln \frac{n\bar{l}}{4} + O\left(\frac{1}{n}\right) \right) \right\} \\ & = e^{-n\Gamma^{(\epsilon)}_{m,n,L(z),R(z)} - 2\ln n + O(1)} \end{aligned} \tag{5.6}$$

whenever

$$\epsilon \leq \frac{1}{n} wt(z^n) \leq 1 - \epsilon$$

where

$$\Gamma^{(\epsilon)}_{m,n,L(z),R(z)} \stackrel{\Delta}{=} -P\left(\bar{l}, R(z), l_1 \epsilon\right) - \left(\frac{1}{2n} \ln \frac{n\bar{l}}{2}\right) \sum_{i=1}^{R} r_i - \frac{1}{2n} \ln \frac{n\bar{l}}{4} - \frac{2 \ln n}{n} . \tag{5.7}$$

5.2 LDPC Coding Theorem for BSC

We first establish our LDPC coding result for BSC. By assuming the encoding procedure to be systematic, the original information bits are visible in the transmitted codeword X^n, and we can measure the bit error probability by

$$P_b\left(\mathcal{C}_{m,n,L(z),R(z)}\right) = \mathbb{E}\left[\frac{1}{n} wt(\hat{X}^n - X^n)\right] \tag{5.8}$$

where the expectation is with respect to to the transmitted random codeword, the BSC, and the random LDPC code $\mathcal{C}_{m,n,L(z),R(z)}$ itself. Selecting $\delta = \sqrt{\frac{\ln n}{n}}$ in the Hamming jar (1.7), i.e

$$J(y^n) = \left\{ x^n : \frac{1}{n} wt(y^n - x^n) \leq p + \sqrt{\frac{\ln n}{n}} \right\},$$

we then have the following theorem.

Theorem 5.1. *For any variable and check node degree distributions $L(z)$ and $R(z)$, and for any block length n,*

$$P_b\left(\mathcal{C}_{m,n,L(z),R(z)}\right) \leq \epsilon + O\left(n^{-2}\right) \tag{5.9}$$

whenever

$$\epsilon + 2\left(p + \sqrt{\frac{\ln n}{n}}\right) < 1 \tag{5.10}$$

and

$$\mathcal{R}(\mathcal{C}_{m,n,L(z),R(z)}) \leq C_{\text{BSC}} - \left(\frac{m}{n}\ln 2 - \Gamma^{(\epsilon)}_{m,n,R(z),L(z)}\right) - \left(\ln\frac{1-p}{p}\right)\sqrt{\frac{\ln n}{n}}. \tag{5.11}$$

Proof. Let $B(x^n, \epsilon)$ be a subset of $\mathcal{X}^n$, defined as

$$B(x^n, \epsilon) \triangleq \left\{ z^n : \frac{1}{n} wt(z^n - x^n) > \epsilon \right\}$$

for any $x^n \in \mathcal{X}^n$ and $0 \leq \epsilon < 1$. Let X^n be the transmitted codeword, and Y^n the output of the BSC in response to X^n, i.e.,

$$Y^n = X^n + W^n$$

where W^n is the noise vector. Then

$$\begin{aligned}
&P_b(\mathcal{C}_{m,n,L(z),R(z)}) \\
&= \mathbb{E}\left[\frac{1}{n}wt(\hat{X}^n - X^n)\right] \\
&\leq \epsilon + \Pr\left\{\hat{X}^n \in B(X^n,\epsilon)\right\} \\
&\leq \epsilon + \Pr\left\{X^n \notin J(Y^n)\right\} \\
&\quad + \Pr\{\exists x^n \in J(Y^n) \cap B(X^n,\epsilon), X^n \in J(Y^n), \mathbf{H}_{m\times n}x^n = 0^m\}. \qquad (5.12)
\end{aligned}$$

To continue, on one hand, we have

$$\begin{aligned}
\Pr\left\{X^n \notin J(Y^n)\right\} &\leq \Pr\left\{\frac{1}{n}wt(W^n) > p + \sqrt{\frac{\ln n}{n}}\right\} \\
&\overset{1)}{\leq} n^{-2} \qquad (5.13)
\end{aligned}$$

where 1) is due to Hoeffding's inequality. On the other hand, we have

$$\begin{aligned}
&\Pr\{\exists x^n \in J(Y^n) \cap B(X^n,\epsilon), X^n \in J(Y^n), \mathbf{H}_{m\times n}x^n = 0^m\} \\
&= \Pr\left\{\exists x^n \in J(X^n+W^n) \cap B(X^n,\epsilon), X^n \in J(X^n+W^n), \mathbf{H}_{m\times n}(x^n - X^n) = 0^m\right\} \\
&= \Pr\left\{\exists x^n, x^n - X^n \in J(W^n) \cap B(0^n,\epsilon), 0^n \in J(W^n), \mathbf{H}_{m\times n}(x^n - X^n) = 0^m\right\} \\
&= \Pr\{\exists z^n \in J(W^n) \cap B(0^n,\epsilon), 0^n \in J(W^n), \mathbf{H}_{m\times n}z^n = 0^m\} \\
&= \sum_{w^n \in J(0^n)} \Pr\left\{W^n = w^n\right\} \Pr\{\exists z^n \in J(w^n) \cap B(0^n,\epsilon), \mathbf{H}_{m\times n}z^n = 0^m\} \\
&\overset{2)}{\leq} \sum_{w^n \in J(0^n)} \Pr\left\{W^n = w^n\right\} |J(w^n)| e^{-n\Gamma^{(\epsilon)}_{m,n,L(z),R(z)} - 2\ln n + O(1)} \\
&\leq e^{nH\left(p+\sqrt{\frac{\ln n}{n}}\right)} e^{-n\Gamma^{(\epsilon)}_{m,n,L(z),R(z)} - 2\ln n + O(1)} \\
&\leq e^{n\left[H(p) + \left(\ln\frac{1-p}{p}\right)\sqrt{\frac{\ln n}{n}}\right]} e^{-n\Gamma^{(\epsilon)}_{m,n,L(z),R(z)} - 2\ln n + O(1)} \\
&= O\left(n^{-2}\right) \qquad (5.14)
\end{aligned}$$

where the inequality 2) is due to (5.6), $z^n \in B(0^n,\epsilon)$, and the fact that

$$\begin{aligned}
w^n \in J(0^n)\ \&\ z^n \in J(w^n) \Rightarrow \frac{1}{n}wt(z^n) &\leq \frac{1}{n}wt(w^n) + \frac{1}{n}wt(z^n - w^n) \\
&< 2\left(p + \sqrt{\frac{\ln n}{n}}\right) < 1 - \epsilon
\end{aligned}$$

whenever (5.10) holds. Then (5.9) is proved by combining (5.12), (5.13) and (5.14). This completes the proof of Theorem 5.1. □

A tighter bound can be obtained in the form of (2.70), i.e.

$$\begin{aligned} P_b(\mathcal{C}_{m,n,L(z),R(z)}) \quad \leq \quad & \sum_{n(p+\delta)+1 \leq t \leq n} \binom{n}{t} p^t (1-p)^{n-t} \\ & + \sum_{w^n \in J(0^n)} p^{wt(w)} (1-p)^{n-wt(w)} \sum_{z^n \in J(w^n)} \frac{wt(z^n)}{n} P(z^n) \end{aligned} \tag{5.15}$$

where

$$P(z^n) \stackrel{\Delta}{=} \exp\left\{ nP\left(\bar{l}, R(z), \bar{l}^{\varkappa(z^n)}\right) + \frac{\ln(n\hat{l}^{\varkappa(z^n)})}{2} \sum_{i=1}^{R} r_i + \frac{1}{2} \ln n\bar{l}^{\varkappa(z^n)} \left(1 - \frac{\bar{l}^{\varkappa(z^n)}}{\bar{l}}\right) + O(1) \right\}. \tag{5.16}$$

The evaluation of this bound is subject to further research.

5.3 LDPC Coding Theorem for BIMC

Now let us extend Theorem 5.1 to an arbitrary BIMC $\{p(y|x) : x \in \mathcal{X}, y \in \mathcal{Y}\}$ with $\mathcal{X} = \{0, 1\}$. Towards this, we modify $\mathcal{C}_{m,n,L(z),R(z)}$ in the following way: $\mathbf{H}_{m\times n}$ and S^m are uniformly picked from $\mathcal{H}_{m,n,L(z),R(z)}$ and $\mathcal{X}^m$ respectively, and the codebook consists of

$$\{x^n \in \mathcal{X}^n : \mathbf{H}_{m\times n} x^n = S^m\}.$$

In other words, we randomly choose a coset code of $\mathbf{H}_{m\times n}$ for use over the BIMC. Let X^n be the transmitted random codeword, and Y^n the output of the BIMC in response to X^n. Then it is easily verified that X^n takes values over $\mathcal{X}^n$ uniformly, and $\mathbf{H}_{m\times n}$ is independent of X^n and Y^n. Thus for any $x^n \neq z^n \in \mathcal{X}^n$,

$$\Pr\{z^n \in \mathcal{C}_{m,n,L(z),R(z)} | X^n = x^n\} = \Pr\{\mathbf{H}_{m\times n}(x^n - z^n) = 0^n\} \tag{5.17}$$

and

$$\Pr\{X^n = x^n\} = 2^{-n}\,. \tag{5.18}$$

To present our LDPC coding theorem for BIMC, recall the definition $\sigma_H(X|Y)$ for the uniformly distributed random input X and the corresponding channel output Y, specify

$J(Y^n)$ as the BIMC jar with $\delta = \sigma_H(X|Y)\sqrt{\frac{4\ln n}{n}}$, i.e.

$$J(Y^n) = \left\{ z^n : -\frac{1}{n}\sum_{i=1}^{n} \ln p(z_i|Y_i) \le H(X|Y) + \sigma_H(X|Y)\sqrt{\frac{4\ln n}{n}} \right\}$$

and further define $\gamma_n(X|Y)$ as

$$\sup_{\lambda \ge 0} \left\{ -\lambda \left(H(X|Y) + \sigma_H(X|Y)\sqrt{\frac{4\ln n}{n}} \right) - \frac{1}{2}\ln \mathbb{E}\left[p^{\lambda}(X|Y)\right] - \frac{1}{2}\ln \mathbb{E}\left[p^{\lambda}(-X|Y)\right] \right\}$$

where $-x$ is the complement of x, i.e., the module-2 addition of x and 1. Then we have the following theorem.

Theorem 5.2. *For any variable and check node degree distributions $L(z)$ and $R(z)$, any block length n, and any $\epsilon \in (0, 0.5)$,*

$$P_b(\mathcal{C}_{m,n,L(z),R(z)}) \le \epsilon + O(n^{-2}) \tag{5.19}$$

whenever

$$H(\epsilon) \le \gamma_n(X|Y) - \frac{2\ln n}{n} \tag{5.20}$$

and

$$\mathcal{R}(\mathcal{C}_{m,n,L(z),R(z)}) \le C_{\text{BIMC}} - \left(\frac{m}{n}\ln 2 - \Gamma^{(\epsilon)}_{m,n,L(z),R(z)} \right) - \sigma_H(X|Y)\sqrt{\frac{4\ln n}{n}}\,. \tag{5.21}$$

Proof. Let $B(x^n, \epsilon)$ follow the same definition as that in the proof of Theorem 5.1, and $-x^n$ be the binary vector resulted from applying bit-wise not operation on x^n. Then from the proof of Theorem 5.1,

$$\begin{aligned} & P_b(\mathcal{C}_{m,n,L(z),R(z)}) \\ &\le \epsilon + \Pr\{X^n \notin J(Y^n)\} + \Pr\{\exists z^n \in J(Y^n) \cap B(X^n,\epsilon), z^n \in \mathcal{C}_{m,n,L(z),R(z)}\} \\ &= \epsilon + \Pr\{X^n \notin J(Y^n)\} + \Pr\{\exists z^n \in J(Y^n) \cap B(X^n,\epsilon), \mathbf{H}_{m\times n}(z^n - X^n) = 0^m\} \end{aligned} \tag{5.22}$$

Combining (5.18), the argument in the proof of Theorem 2.2, and Result 1.1, we have

$$\begin{aligned} \Pr\{X^n \notin J(Y^n)\} &= \Pr\left\{ -\frac{1}{n}\sum_{i=1}^{n} \ln p(X_i|Y_i) > H(X|Y) + \sigma_H(X|Y)\sqrt{\frac{4\ln n}{n}} \right\} \\ &= O\left(n^{-2}\right)\,. \end{aligned} \tag{5.23}$$

On the other hand,

$$\begin{aligned}
&\Pr\{\exists z^n \in J(Y^n) \cap B(X^n,\epsilon), \mathbf{H}_{m\times n}(z^n - X^n) = 0^m\} \\
&\quad \le \Pr\{\exists z^n \in J(Y^n) \cap B(X^n,\epsilon) \cap B(-X^n,\epsilon), \mathbf{H}_{m\times n}(z^n - X^n) = 0^m\} \\
&\qquad + \Pr\{\exists z^n \in J(Y^n) \cap \left(\mathcal{X}^n / B(-X^n,\epsilon)\right), \mathbf{H}_{m\times n}(z^n - X^n) = 0^m\} \,. \qquad (5.24)
\end{aligned}$$

Now

$$z^n \in J(y^n) \cap B(x^n,\epsilon) \cap B(-x^n,\epsilon) \Rightarrow \epsilon \le \frac{1}{n} wt(z^n - x^n) \le 1 - \epsilon$$

which implies that

$$\Pr\{\mathbf{H}_{m\times n}(z^n - x^n) = 0^n\} \le e^{-n\Gamma^{(\epsilon)}_{m,n,L(z),R(z)} - 2\ln n + O(1)} \qquad (5.25)$$

according to (5.6). Therefore,

$$\begin{aligned}
&\Pr\{\exists z^n \in J(Y^n) \cap B(X^n,\epsilon) \cap B(-X^n,\epsilon), \mathbf{H}_{m\times n}(z^n - X^n) = 0^m\} \\
&= \sum_{x^n \in \mathcal{X}^n} \int p(x^n, y^n) \\
&\quad \Pr\{\exists z^n \in J(y^n) \cap B(x^n,\epsilon) \cap B(-x^n,\epsilon), \mathbf{H}_{m\times n}(z^n - x^n) = 0^m | \, X^n = x^n, Y^n = y^n\} dy \\
&\overset{2)}{\le} \sum_{x^n \in \mathcal{X}^n} \int p(x^n, y^n) |J(y^n)| e^{-n\Gamma^{(\epsilon)}_{m,n,L(z),R(z)} - 2\ln n + O(1)} dy \\
&\overset{3)}{\le} \sum_{x^n \in \mathcal{X}^n} \int p(x^n, y^n) e^{n\left(H(X|Y) + \sigma_H(X|Y)\sqrt{\frac{4\ln n}{n}}\right)} e^{-n\Gamma^{(\epsilon)}_{m,n,L(z),R(z)} - 2\ln n + O(1)} dy \\
&\le \sum_{x^n \in \mathcal{X}^n} \int p(x^n, y^n) O\left(n^{-2}\right) dy = O\left(n^{-2}\right) \qquad (5.26)
\end{aligned}$$

whenever (5.21) holds, where the inequality 2) follows from the union bound, (5.25) and the fact that $\mathbf{H}_{m\times n}$ is independent of X^n and Y^n, and the inequality 3) is due to (1.10). At the same time,

$$\begin{aligned}
&\Pr\{\exists z^n \in J(Y^n) \cap \left(\mathcal{X}^n / B(-X^n,\epsilon)\right), \mathbf{H}_{m\times n}(z^n - X^n) = 0^m\} \\
&\quad \le \Pr\{\exists z^n \in J(Y^n) \cap \left(\mathcal{X}^n / B(-X^n,\epsilon)\right)\} \\
&\quad \le \sum_{z^n \in \mathcal{X}^n / B(-0^n,\epsilon)} \Pr\{z^n + X^n \in J(Y^n)\} \\
&\quad \overset{4)}{\le} \sum_{z^n \in \mathcal{X}^n / B(-0^n,\epsilon)} e^{-n\gamma_n(X|Y)} \\
&\quad \le e^{nH(\epsilon) - n\gamma_n(X|Y)} \\
&\quad \le n^{-2} \qquad (5.27)
\end{aligned}$$

whenever (5.20) holds, where 4) can be derived as below:

$$\begin{aligned}
&\Pr\{z^n + X^n \in J(Y^n)\} \\
&= \Pr\left\{-\frac{1}{n}\sum_{i=1}^{n} \ln p(z_i + X_i|Y_i) \le H(X|Y) + \sigma_H(X|Y)\sqrt{\frac{4\ln n}{n}}\right\} \\
&\overset{5)}{\le} \inf_{\lambda\ge 0}\left\{e^{n\lambda\left(H(X|Y)+\sigma_H(X|Y)\sqrt{\frac{4\ln n}{n}}\right)}\mathbb{E}\left[e^{\lambda\sum_{i=1}^{n}\ln p(z_i+X_i|Y_i)}\right]\right\} \\
&= \inf_{\lambda\ge 0}\left\{e^{n\lambda\left(H(X|Y)+\sigma_H(X|Y)\sqrt{\frac{4\ln n}{n}}\right)}\left[\mathbb{E}\left[p^\lambda(X|Y)\right]\right]^{n-wt(z^n)}\left[\mathbb{E}\left[p^\lambda(-X|Y)\right]\right]^{wt(z^n)}\right\} \\
&\overset{6)}{\le} \inf_{\lambda\ge 0}\left\{e^{n\lambda\left(H(X|Y)+\sigma_H(X|Y)\sqrt{\frac{4\ln n}{n}}\right)}\left[\mathbb{E}\left[p^\lambda(X|Y)\right]\right]^{0.5n}\left[\mathbb{E}\left[p^\lambda(-X|Y)\right]\right]^{0.5n}\right\} \\
&= e^{-n\gamma_n(X|Y)}
\end{aligned}$$

where 5) is the standard Chernoff's Bound, and 6) holds since $\frac{1}{n}wt(z^n) \ge 1-\epsilon > 0.5$ and we can verify

$$\mathbb{E}\left[p^\lambda(X|Y)\right] \ge \mathbb{E}\left[p^\lambda(-X|Y)\right]$$

in the following way,

$$\begin{aligned}
&\mathbb{E}\left[p^\lambda(X|Y)\right] - \mathbb{E}\left[p^\lambda(-X|Y)\right] \\
&= \mathbb{E}_Y\left[\mathbb{E}_X\left[p^\lambda(X|Y) - p^\lambda(-X|Y)\right]\right] \\
&= \mathbb{E}_Y\left[p(0|Y)\left(p^\lambda(0|Y) - p^\lambda(1|Y)\right) + p(1|Y)\left(p^\lambda(1|Y) - p^\lambda(0|Y)\right)\right] \\
&= \mathbb{E}_Y\left[\left(p(0|Y) - p(1|Y)\right)\left(p^\lambda(0|Y) - p^\lambda(1|Y)\right)\right] \\
&\ge 0
\end{aligned}$$

as $\lambda \ge 0$. Then this theorem is proved by plugging (5.23)-(5.27) into (5.22). □

Remark 5.2. *To show the existence of ϵ satisfying (5.20), we need verify that $\gamma_n(X|Y) > 0$ which is indeed true, by observing that*

$$g_n(\lambda) = -\lambda\left(H(X|Y) + \sigma_H(X|Y)\sqrt{\frac{4\ln n}{n}}\right) - \frac{1}{2}\ln\mathbb{E}\left[p^\lambda(X|Y)\right] - \frac{1}{2}\ln\mathbb{E}\left[p^\lambda(-X|Y)\right]$$

is a concave function of λ, $g_n(0) = 0$, and

$$\begin{aligned}
\left.\frac{dg_n(\lambda)}{d\lambda}\right|_{\lambda=0} &= \frac{1}{2}\mathbb{E}\left[\ln\frac{p(X|Y)}{p(-X|Y)}\right] - \sigma_H(X|Y)\sqrt{\frac{4\ln n}{n}} \\
&= \frac{1}{2}\mathbb{E}\left[\ln\frac{p(Y|X)}{p(Y|-X)}\right] - \sigma_H(X|Y)\sqrt{\frac{4\ln n}{n}} > 0
\end{aligned}$$

whenever $C_{\mathrm{BIMC}} > 0$ *and* n *is large.*

Remark 5.3. *Similar to Remark 2.4, it can be shown that Theorem 5.2 holds for general binary input memoryless channel by replacing* C_{BIMC} *with the mutual information between a uniform random variable and its channel response. Moreover, similar achievability to Theorem 5.2 can be derived along the same proof approach when* $\mathcal{X}$ *is a finite field in general.*

Similarly, for the BEC with erasure probability p, a tighter upper bound can be obtained as follows:

$$\begin{aligned} P_b(\mathcal{C}_{m,n,L(z),R(z)}) \quad \leq \quad & \sum_{n\left(p+\frac{\delta}{\ln 2}\right)+1 \leq t \leq n} \binom{n}{t} p^t (1-p)^{n-t} \\ & + \sum_{w^n \in \{0,\varepsilon\}^n : \varepsilon(w^n) \leq n(p+\frac{\delta}{\ln 2})} p^{\varepsilon(w^n)} (1-p)^{n-\varepsilon(w^n)} \sum_{z^n \in V(w^n)} \frac{wt(z^n)}{n} P(z^n) \end{aligned} \tag{5.28}$$

where

$$\begin{aligned} \varepsilon(w^n) \quad & \triangleq \quad |\{i : w_i = \varepsilon\}| \\ V(w^n) \quad & \triangleq \quad \{v^n \in \mathcal{X}^n : v_i = 0 \text{ if } w_i = 0\}. \end{aligned}$$

and $P(z)$ is defined in (5.16).

5.4 Analysis On Degree Distribution

From Theorems 5.1 and 5.2, it can be clearly seen that there is a constant gap between the rate of LDPC and channel capacity, i.e.

$$\frac{m}{n} \ln 2 - \Gamma^{(\epsilon)}_{m,n,R(z),L(z)}$$

or

$$\frac{\bar{l}}{\bar{r}} \ln 2 + P(\bar{l}, R(z), l_1 \epsilon) + O\left(\frac{\ln n\bar{l}}{n}\right). \tag{5.29}$$

Several interesting results arise from the study of this gap with respect to the degree distributions $L(z)$ and $R(z)$. First of all, let us consider the optimal $R(z)$ which can minimize (5.29) given $L(z)$.

Theorem 5.3. *Given the variable node degree distribution $L(z)$ and the rate of code $\mathcal{R} = 1 - \frac{m}{n}$, the optimal $R(z)$ is the check node concentrated distribution, i.e.*

$$R(z) = (1 + \lfloor \bar{r} \rfloor - \bar{r})\, z^{\lfloor \bar{r} \rfloor} + (\bar{r} - \lfloor \bar{r} \rfloor) z^{\lceil \bar{r} \rceil} \tag{5.30}$$

where

$$\bar{r} = \frac{n}{m}\bar{l} = \frac{\bar{l}}{1 - \mathcal{R}}.$$

Proof. Since minimizing (5.29) is equivalent to minimizing $P(\bar{l}, R(z), l_1\epsilon)$ with respect to $R(z)$, the theorem is the direct result of Lemma B.11 in Appendix B.2.1. □

The next result shows that LDPC codes can achieve asymptotically the channel capacity of any BIMC with diminishing bit error probability when large degrees are used.

Theorem 5.4. *Given any variable and check node degree distributions $L(z)$ and $R(z)$,*

$$P_b(\mathcal{C}_{m,n,L(z^k),R(z^k)}) \leq \frac{1}{2\sqrt{k}} + O(n^{-2}) \tag{5.31}$$

whenever

$$H\left(\frac{1}{2\sqrt{k}}\right) \leq \gamma_n(X|Y) - \frac{2\ln n}{n} \tag{5.32}$$

and

$$\mathcal{R}(\mathcal{C}_{m,n,L(z^k),R(z^k)}) \leq C_{\text{BIMC}} - O\left(e^{-\frac{l_1 r_1}{l}\sqrt{k} + \frac{1}{2}\ln k} + \frac{\ln nk}{n} + \sqrt{\frac{\ln n}{n}}\right). \tag{5.33}$$

Proof. Let $\epsilon = \frac{1}{2\sqrt{k}}$. By Lemma B.10 in Appendix B.2.1,

$$\begin{aligned}
&\frac{\bar{l}}{\bar{r}}\ln 2 + P\left(\bar{l}, R(z^k), \frac{l_1\sqrt{k}}{2}\right) \\
&\quad\leq \frac{\bar{l}}{\bar{r}}\ln 2 + \left\{-\frac{\bar{l}}{\bar{r}}\ln 2 + l_1\sqrt{k}\exp\left[-l_1\sqrt{k}\frac{(r_1 - k^{-1})}{\bar{l}}\right] + \frac{\bar{l}}{\bar{r}}\exp\left(-\frac{l_1 r_1\sqrt{k}}{\bar{l}}\right)\right\} \\
&\quad= O\left(e^{-\frac{l_1 r_1}{l}\sqrt{k} + \frac{1}{2}\ln k}\right)
\end{aligned}$$

which, together with (5.29) and Theorem 5.2, implies (5.33). This completes the proof of Theorem 5.4. □

Remark 5.4. *In Theorem 5.4, k is not related to n, and can remain a constant as n approaches infinity. Therefore, the parity check matrix of the code can be always sparse, although large k is needed to allow the rate of the code to approach channel capacity.*

5.5 Simulation Results

In this section, we demonstrate, by simulation, that for LDPC codes, BP decoding can be regarded as one of many ways to pick up a codeword from a jar when it succeeds in outputting a codeword.

In our simulation, we first selected a LDPC code with block length $n = 8000$, coding rate $1 - \frac{m}{n} = 0.5$ (in bits), variable node degree distribution

$$\begin{aligned} L(z) &= 0.457875z^2 + 0.32375z^3 + 0.0215z^4 \\ &\quad + 0.05925z^6 + 0.038875z^7 + 0.024875z^8 \\ &\quad + 0.00875z^9 + 0.01775z^{19} + 0.047375z^{20} \end{aligned}$$

and check node concentration degree distribution $R(z)$, and then randomly chose its coset code

$$\{x^n : \mathbf{H}_{m\times n}x^n = S^m\}$$

for use over our testing channel. Let X^n denote the transmitted codeword and Y^n denote the channel output. As mentioned earlier, X^n takes values uniformly over $\mathcal{X}^n$. Thus, in our simulation, X^n was first generated uniformly from $\mathcal{X}^n$, and then fixed and passed into the channel multiple times (each time noise is generated independently).

At the decoder, the standard BP decoding algorithm was used, which is described in Algorithm 1, where $\{c_i\}_{i=1}^m$ and $\{v_j\}_{j=1}^n$ represent check and variable nodes in the tanner graph of $\mathbf{H}_{m\times n}$ respectively, $\mathcal{N}(a)$ is the set of nodes connected to node a in the graph. Simply speaking, messages ($m_{c_i\to v}$ and $m_{v_j\to c}$) are passed and modified in certain manner (according to steps 5 to 14) between check and variable nodes in the tanner graph, and eventually the decoding output is the hard decision (steps 15 to 17) on each variable node with channel statistics $\ln\frac{\Pr\{X_i=0|Y_i\}}{\Pr\{X_i=1|Y_i\}}$ and messages passed to it. The algorithm kept running until it either found a codeword $\hat{x}^n$ i.e. $\mathbf{H}_{m\times n}\hat{x}^n = S^m$ or the upper bound on the number iteration (N) was reached (in our simulation $N = 100$).

The first testing channel we selected is the BSC with crossover probability 0.09 and capacity 0.564 (in bits). BP decoding was run for 1000 blocks. In our simulation, we observed that BP decoding always failed whenever

$$\frac{1}{n}wt(Y^n - X^n) > 0.098 = p + 0.008$$

and sometimes succeeded and sometimes failed when

$$\frac{1}{n}wt(Y^n - X^n) < 0.098 = p + 0.008\ .$$

Algorithm 1 Standard BP Decoding Algorithm

Let $\hat{x}^n$ be a sequence such that $\hat{x}_i = \begin{cases} 0 & \text{if } \ln \frac{\Pr\{X_i=0|Y_i\}}{\Pr\{X_i=1|Y_i\}} \geq 0 \\ 1 & \text{otherwise} \end{cases}$.

Initialize $iter = 1$ and

- $m_{c_i \to v}$ to be 0 for $v \in \mathcal{N}(c_i)$ and $1 \leq i \leq m$;
- and $m_{v_j \to c}$ to be 0 for $c \in \mathcal{N}(v_j)$ and $1 \leq j \leq n$.

while $\mathbf{H}_{m \times n} \hat{x}^n \neq s^m$ and $iter < N$ **do**
  $iter = iter + 1$.
  for $j = 1$ to n **do**
    for all $c \in \mathcal{N}(v_j)$ **do**
      $m_{v_j \to c} = \ln \frac{\Pr\{X_i=0|Y_i\}}{\Pr\{X_i=1|Y_i\}} + \sum_{c' \in N(v_j)/\{c\}} m_{c' \to v_j}$.
    end for
  end for
  for $i = 1$ to m **do**
    for all $v \in \mathcal{N}(c_i)$ **do**
      $m_{c_i \to v} = 2 \tanh^{-1} \left[(1 - 2s_i) \prod_{v' \in N(c_i)/\{v\}} \tanh \left(\frac{m_{v' \to c_i}}{2} \right) \right]$.
    end for
  end for
  for $j = 1$ to n **do**
    $\hat{x}_j = \begin{cases} 0 & \text{if } \ln \frac{\Pr\{X_i=0|Y_i\}}{\Pr\{X_i=1|Y_i\}} + \sum_{c \in N(v)} m_{c \to v_j} \geq 0 \\ 1 & \text{otherwise} \end{cases}$
  end for
end while
Output $\hat{x}^n$ as the estimation of X^n.

The second testing channel we selected is the BIAGC with variance of noise $\sigma = 0.875$ and channel capacity 0.575 (in bits). The codeword was modulated to $\{-1, +1\}$. In our simulation, we observed that BP decoding always failed whenever

$$-\frac{1}{n}\ln\frac{p(X^n|Y^n)}{p(Y^n)} > 0.322 = H(X|Y) + 0.028$$

and sometimes succeeded and sometimes failed when

$$-\frac{1}{n}\ln\frac{p(X^n|Y^n)}{p(Y^n)} < 0.322\ .$$

Both simulations confirm that BP decoding can be regarded as one of many ways to pick up a codeword from a jar when it succeeds in outputting a codeword. Of course, if one wants to include BP decoding as a part of jar decoding for LDPC codes, it is clear that one has to deal with the situation in which BP decoding fails to output any codeword. This problem, together with the design of effective jar decoding algorithms and codes, is left open for future research.

5.6 Summary

In this chapter, coding theorems on LDPC ensemble are considered. As can be seen, the proof of LDPC coding theorem via jar decoding is much simpler, in which the (bit) error probability is again broken into two part, i.e. the probability that the true codeword is outside the jar and that there exists other codewords inside the jar. However, in contrast to the pure random linear code (Gallager's and Elias') ensembles, for which the first probability is the major contributor to the error probability, for LDPC codes the second probability is actually dominant. In this case, jar decoding has allowed us to analyze the tradeoff between the capacity gap and bit error probability of LDPC codes for any n. And we have shown that LDPC codes can achieve, with diminishing bit error probability, the capacity of any BIMC as their average node degrees increase. In addition, an interesting connection between BP decoding and jar decoding is demonstrated through simulation, and it is shown that BP decoding can be viewed as one of many ways to pick up a codeword in the jar.

Chapter 6

Interactive Encoding and Decoding Theorems based on LDPC Codes with Syndrome Accumulation

In Chapters 2, 3, 4 and 5, jar decoding is shown to be a fundamental tool to prove non-asymptotic channel coding theorems, where the transmission is one way, the number of symbols per transmission (block length) is fixed, and the jar size is pre-determined by the decoder. In this chapter, it is demonstrated that jar decoding is a powerful tool to prove coding theorems in the scenario of two-way communication, where both the number of transmitted symbols and the jar size are dynamic and determined on the fly. Towards this, a coding scenario, called interactive encoding and decoding, is considered.

6.1 Motivation, Problem Formulation and Literature Review

The concept of interactive encoding and decoding (IED) was formalized in [40, 41]. When applied to (near) lossless one way learning (i.e. lossless source coding) with decoder only side information, IED can be easily explained via Figure 6.1, where X denotes a finite alphabet source to be learned at the decoder, Y denotes another finite alphabet source that is correlated with X and only available to the decoder as side information, and R denotes the average number of nats per symbol exchanged between the encoder and the decoder measuring the rate performance of the IED scheme used. As evident from Figure 6.1,

IED distinguishes itself from non-interactive Slepian-Wolf coding (SWC) in the fact that two-way communication is allowed in IED.

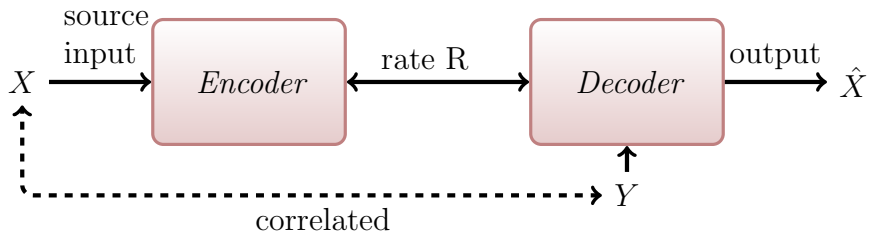


Figure 6.1: Interactive encoding and decoding for one way learning with side information at the decoder

By allowing interactions between the encoder and the decoder, IED has several advantages over SWC [40,41]. For example, in comparison with SWC, it was shown [40,41] that IED not only delivers better first-order performance (i.e. asymptotic compression rate) for general stationary, non-ergodic source-side information pairs, but also achieves better second-order performance (i.e. trade-off between the speeds of convergence of compression rate to optimum and convergence of error probability to zero) for memoryless pairs with known statistics. Furthermore, although given the compression rate SWC schemes [42–44] can be constructed which work for vast classes of source-side information pairs with conditional entropy rate less than this rate, truly universal SWC does not exist as the conditional entropy rate is part of the statistics of source and side information. On the other hand, it was shown [41] that coupled with any classical universal lossless code $\mathcal{C}_n$ (with block length n and with the side information available to both the encoder and decoder) such as the one in [8], one can build an IED scheme which is asymptotically optimal with respect to the class of all stationary, ergodic sources-side information pairs. Indeed, the corresponding IED scheme achieves essentially the same rate performance as that of $\mathcal{C}_n$ for each and every individual sequence pair (x^n, y^n), even though the side information is not available to the encoder in the case of IED, while the word decoding error probability can be made arbitrarily small.

The above advantages make IED much more appealing than SWC to applications where the one-way learning model depicted in Figure 6.1 fits. However, the IED schemes constructed in [40, 41] do not have an intrinsic structure that is amenable to implement in practice. A big challenge is then how to design universal IED schemes with both low encoding and decoding complexity. To address this challenge partially, linear IED schemes, which use linear codes for encoding, were later considered in [45]. The encoder of a linear IED scheme can be conveniently described by a parity-check matrix. Based on different

random matrix ensembles, two universal linear IED schemes were proposed therein. The first universal linear IED scheme proposed in [45] (also called LIED) makes use of Gallager-type of matrix ensembles, where each matrix element is generated independently, selects randomly a matrix from such an ensemble, and then divides the selected matrix into several sub-matrices, each of which is used to generate new syndromes in each round of interaction. In the second universal linear IED scheme proposed in [45] (also called SA-IED), Gallager-type ensembles are extended into vector-type ensembles, where each column of matrices is generated independently, and a matrix is generated in such way that each of its sub-matrices is randomly picked from such a vector-type ensemble; in each round of interaction, new syndromes are then generated by applying syndrome accumulation (described in [45]) once to each and every of those sub-matrices. Define the density of a linear IED scheme as the percentage of non-zero entries in its parity-check matrix. It was then shown [45] that there is no performance loss by restricting IED to linear IED and even to linear IED with density $\Omega(\frac{\ln n}{n})$, where n is the block length. Thus the encoding complexity of universal IED can be kept as low as $O(n \ln n)$.

Although linear IED considered in [45] tackles its encoding complexity very well, its decoding complexity is largely untouched due to the adoption of maximum likelihood (ML) decoding, which results in exponential decoding complexity with respect to block length n. An attempt to apply belief propagation (BP) decoding algorithm on linear codes generated by Gallager-type or vector-type ensemble in [45] fails miserably, due to the property of those ensembles. Details of discussion of Gallager-type or vector-type ensemble and the reason why BP decoding fails for those ensembles can be found in Remark 6.1 in section 6.2.3, while the brief version is provided here. Specifically, in either of Gallager-type or vector-type ensemble, several sub-matrices are generated independently and then concatenated as one matrix used by decoder. Moreover, within each sub-matrix columns are generated independently. The independence mentioned above mitigates the difficulty of theoretical analysis of the performances of IED schemes to some extent, but makes degree distribution of the matrix used for decoding totally uncontrolled. On the other hand, it is well known that the convergence of BP decoding depends largely on those (especially variable node) degree distribution [5, 46]. Therefore, one of the main purposes of this chapter is to address the issue of decoding complexity by building IED schemes from linear codes with low decoding complexity. This leads us to consider LDPC codes, due to their linear complexity decoding based on BP decoding and successful application to fix-rate Slepian-Wolf coding [47–50].

An LDPC code is a linear code with a sparse parity check matrix, each of whose rows and columns has only a finite number of non-zero elements with respect to its block length. Important parameters of an LDPC code include the ratio between the numbers of rows

and columns (called Slepian-Wolf rate (syndrome encoding)), and the portions of rows and columns with certain number of non-zero elements (called the check and variable degree distributions of the LDPC code). Given a block length n and a Slepian-Wolf rate, one way to generate an LDPC code with the given Slepian-Wolf rate, is to randomly select a matrix as its parity check matrix from an ensemble in which all matrices share the same Slepian-Wolf rate, and check and variable degree distributions.

Since rows and columns of parity check matrix of an LDPC code are not generated independently, the approach of dividing the whole matrix into several sub-matrices adopted in [45] can not deliver good results from both theoretical and practical perspectives. To overcome this problem, we shall modify syndrome accumulation (SA) used in [45] to adapt the encoding rates of the LDPC code for IED. The resulting scheme is called an interactive encoding and decoding scheme based on a binary LDPC code with syndrome accumulation (SA-LDPC-IED); its performance is then analyzed theoretically and evaluated practically based on jar decoding and BP decoding, respectively. It is shown that coupled with any classical lossless code $\mathcal{C}_n$ (with side information available to both the encoder and decoder), one can always construct an SA-LDPC-IED scheme such that

- the word decoding error probability approaches 0 sub-exponentially with n; and
- the total rate (including both the forward and backward rates) of the resulting SA-LDPC-IED scheme is upper bounded by a functional of that of $\mathcal{C}_n$, which in turn approaches the compression rate of $\mathcal{C}_n$ for each and every individual sequence pair (x^n, y^n) and the conditional entropy rate $H(X|Y)$ for any stationary, ergodic source and side information (X, Y) as the average variable node degree $\bar{l}$ of the underlying LDPC code increases without bound.

When applied to the class of binary source and side information (X, Y) correlated through a BSC with cross-over probability unknown to either the encoder or decoder, the resulting SA-LDPC-IED scheme can be further simplified, yielding even improved rate performance versus the bit error probability when $\bar{l}$ is not large. It is worth mentioning here that due to dramatic difference between LDPC ensemble and Gallager-type or vector-type ensemble in [45], theoretical results above are by no means implied by those in [45], and as can be seen later on, the proof technique used here is quite different, which is also believed to be valuable for theoretical analysis of rateless or universal codes (in channel or Slepian-Wolf coding) with LDPC property.

Comparison between our work and research done in area of SWC need to be addressed here. First of all, the connection and difference between IED and variable-rate SWC with

feedback ([51], and references in [41,45]) have been extensively discussed in [41,45], where the main difference has two folds. One is that the assumption on source statistics is general and completely unknown to either the encoder or the decoder in IED while either IID is assumed, or the statistics is known at the decoder in those work. The other is that in IED the total exchange rate (forward and backward rate) is concerned while by feedback usually only forward rate (from encoder to decoder) is considered. Also, it should be pointed out that in the literature (see for example [52–54], and references therein), there have been several attempts towards building rateless (or rate-adaptive) SWC schemes using LDPC codes. Specifically, the technique of SA was used to construct the so-called LDPCA codes in [54]. Our SA-LDPC-IED schemes differ from the rateless SWC schemes in the following aspects:

- We are concerned with the total rate defined as the number of bits exchanged between the encoder and the decoder per symbol, while only the forward rate (from the encoder to the decoder) is considered in rateless SWC schemes.
- We assume that the joint statistics of source and side information are unknown to both the encoder and decoder, while the joint statistics are available for decoding in rateless SWC schemes.
- We provide theoretical analysis for our SA-LDPC-IED schemes, while the performance of those rateless SWC schemes has been evaluated mainly through simulation.

6.2 Interactive Encoding and Decoding Scheme based on LDPC Codes with Syndrome Accumulation

6.2.1 LDPC Ensemble with Check-Concentrated Degree Distribution

Recall the definitions of LDPC ensembles in Section 5.1. Given m, n, and (normalized) variable and check degree distributions $L(z)$ and $R(z)$ satisfying $nL'(1) = mR'(1)$, let $\mathcal{H}_{m,n,L(z),R(z)}$ denote the collection of all $m \times n$ parity check matrices with normalized variable and check degree distributions $L(z)$ and $R(z)$. Without loss of generality, we only consider those matrices such that the degrees of rows and columns do not decrease with their indices. (In other words, $i > j$ implies the degree of the i-th row (or column) is not less than that of the j-th row (or column).) Here we focus on a special case, i.e. $m = n$,

and simply denote $\mathcal{H}_{m,n,L(z),R(z)}$ by $\mathcal{H}_{n,L(z),R(z)}$. Moreover, as shown in Chapter 5, check-concentrated degree distributions achieve the best performance under jar decoding, where given a variable node degree distribution, the check node degree distribution is made as concentrated as possible. Therefore, we further narrow down our discussion on this type of degree distributions. In this case of $\mathcal{H}_{n,L(z),R(z)}$, given $L(z)$, $R(z)$ is determined as follows:

$$R(z) = R_1 z^{r_1} + R_2 z^{r_2}$$

where

$$\begin{aligned} r_1 &= \lfloor \bar{l} \rfloor \\ r_2 &= \lceil \bar{l} \rceil \\ R_1 &= 1 + \lfloor \bar{l} \rfloor - \bar{l} \\ R_2 &= \bar{l} - \lfloor \bar{l} \rfloor \end{aligned}$$

and

$$\bar{l} = L'(1) = \sum_{i=1}^{L} L_i l_i \ .$$

$\mathcal{H}_{n,L(z),R(z)}$ with $R(z)$ determined by $L(z)$ as above is simply referred as to $\mathcal{H}_{n,L(z)}$.

6.2.2 Syndrome Accumulation

The concept of syndrome accumulation has been introduced in [45]. To clarify our following discussion, we revise this concept here.

Suppose a syndrome vector $s^n = \mathbf{H}_{n\times n} x^n$ is given, where s^n consists of n syndromes $s_1 s_2 \ldots s_n$, and $\mathbf{H}_{n\times n}$ is an $n \times n$ matrix. To facilitate the discussion below, we assume that n is a power of 2, i.e. 2^T for some positive integer T. Let $\mathcal{N} = \{1, 2, \ldots, n\}$ and $\mathcal{P} = \{\Lambda_1, \Lambda_2, \ldots, \Lambda_{|\mathcal{P}|}\}$ where $\mathcal{P}$ forms a partition on $\mathcal{N}$ with each Λ_i as a subset of $\mathcal{N}$ and $|\mathcal{P}|$ as the number of elements in $\mathcal{P}$. Λ_i is also called a cell in $\mathcal{P}$, and we use $|\Lambda_i|$ to represent the cardinality of Λ_i, i.e. the number of indices in Λ_i. Now given s^n and $\mathcal{P}$, we can form a new syndrome vector $\tilde{s}^{|\mathcal{P}|}$, which is called an accumulated syndrome vector, in

the following way:

$$\begin{aligned}\tilde{s}^{|\mathcal{P}|} &= \begin{pmatrix} \tilde{s}_1 \\ \tilde{s}_2 \\ \vdots \\ \tilde{s}_{|\mathcal{P}|} \end{pmatrix} \\ \tilde{s}_i &= \sum_{j \in \Lambda_i} s_j \text{ for } 1 \leq i \leq |\mathcal{P}|\end{aligned}$$

The derivation below shows that $\tilde{s}^{|\mathcal{P}|}$ is indeed a syndrome vector:

$$\begin{aligned}\tilde{s}^{|\mathcal{P}|} &= \begin{pmatrix} \tilde{s}_1 \\ \tilde{s}_2 \\ \vdots \\ \tilde{s}_{|\mathcal{P}|} \end{pmatrix} \\ &= \begin{pmatrix} \sum_{j \in \Lambda_1} s_j \\ \sum_{j \in \Lambda_2} s_j \\ \vdots \\ \sum_{j \in \Lambda_{|\mathcal{P}|}} s_j \end{pmatrix} \\ &= \begin{pmatrix} \sum_{j \in \Lambda_1} \sum_{k=1}^{n} h_{jk} x_k \\ \sum_{j \in \Lambda_2} \sum_{k=1}^{n} h_{jk} x_k \\ \vdots \\ \sum_{j \in \Lambda_{|\mathcal{P}|}} \sum_{k=1}^{n} h_{jk} x_k \end{pmatrix} \\ &= \begin{pmatrix} \sum_{k=1}^{n} \sum_{j \in \Lambda_1} h_{jk} x_k \\ \sum_{k=1}^{n} \sum_{j \in \Lambda_2} h_{jk} x_k \\ \vdots \\ \sum_{k=1}^{n} \sum_{j \in \Lambda_{|\mathcal{P}|}} h_{jk} x_k \end{pmatrix} \\ &= \left(\sum_{j \in \Lambda_i} h_{jk} \right)_{1 \leq i \leq |\mathcal{P}|, 1 \leq k \leq n|} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \\ &\triangleq \mathbf{H}_{\mathcal{P}} x^n\end{aligned}$$

where h_{jk} is the element in the j-th row and k-th column of $\mathbf{H}_{n \times n}$, and x_k is the k-th

element in x^n. Also, $\mathbf{H}_{\mathcal{P}}$ defined above is the parity check matrix corresponding to the partition $\mathcal{P}$.

To proceed, we introduce a sequence of partitions $\mathcal{P}_1\mathcal{P}_2\cdots\mathcal{P}_n$. (Later on, it can be seen that this sequence effectively represents the procedure of encoding of SA-LDPC-IED schemes.) The sequence $\mathcal{P}_1\mathcal{P}_2\cdots\mathcal{P}_n$ is generated in a recursive manner, depicted below:

- $\mathcal{P}_1 = \{\mathcal{N}\}$.
- Suppose $\mathcal{P}_i = \{\Lambda_{i,1}, \Lambda_{i,2}, \ldots, \Lambda_{i,i}\}$ has been generated. Let $j_i = 2(i - 2^{\lfloor \log_2 i \rfloor}) + 1$. Split Λ_{i,j_i} equally into two parts, Λ_{i,j_i+} and Λ_{i,j_i-}, where Λ_{i,j_i+} (Λ_{i,j_i-}) consists of the first (second) half of elements in Λ_{i,j_i}, ordered by their values.
- $\mathcal{P}_{i+1} = \{\Lambda_{i+1,1}, \Lambda_{i+1,2}, \ldots, \Lambda_{i+1,i+1}\}$ is generated as below:
  - $\Lambda_{i+1,k} = \Lambda_{i,k}$ for $1 \le k < j_i$.
  - $\Lambda_{i+1,j_i} = \Lambda_{i,j_i+}$.
  - $\Lambda_{i+1,j_i+1} = \Lambda_{i,j_i-}$.
  - $\Lambda_{i+1,k} = \Lambda_{i,k-1}$ for $j_i + 1 < k \le i + 1$.

Note that since we assume $n = 2^T$ for some integer T, $|\Lambda_{i,k}|$ is also a power of 2 for $1 \le i \le n, 1 \le k \le i$. Moreover, for $1 < i < n$, $|\Lambda_{i,k_1}| = 2|\Lambda_{i,k_2}| = 2^{T-\lfloor \log_2 i \rfloor}$ always holds for $j_i \le k_1 \le i$ and $1 \le k_2 \le j_i - 1$. Therefore, the splitting of Λ_{i,j_i} can always be applied. In fact,

$$\Lambda_{i,k} = \left\{(k-1)2^{T-\lceil \log_2 i \rceil} + 1, \ldots, k2^{T-\lceil \log_2 i \rceil}\right\}$$

for $1 \le k < j_i$, and

$$\begin{aligned}\Lambda_{i,k} = \big\{&(j_i-1)2^{T-\lceil \log_2 i \rceil} + (k-j_i)2^{T-\lfloor \log_2 i \rfloor} + 1,\\ &\ldots, (j_i-1)2^{T-\lceil \log_2 i \rceil} + (k-j_i+1)2^{T-\lfloor \log_2 i \rfloor}\big\}\end{aligned}$$

for $j_i \le k \le i$.

Now given $s^n = \mathbf{H}_{n\times n}x^n$ and $\mathcal{P}_1\mathcal{P}_2\cdots\mathcal{P}_n$, we can generate a sequence of accumulated syndrome vectors $\tilde{s}_1^1\tilde{s}_2^2\ldots\tilde{s}_n^n$, where the upper scripts represent the dimension and lower scripts indicate which partitions the syndromes are associated with. The upper scripts, which always equal to the lower scripts, are dropped for simplicity. Now for any $\tilde{s}_i$, we use

$\tilde{s}_{i,j}$ to represent its j-th element. In fact, this procedure can be done recursively as above, where

$$\tilde{s}_1 = \tilde{s}_{1,1} = \sum_{j \in \mathcal{N}} s_j$$

and $\tilde{s}_{i+1}$ is generated by replacing $\tilde{s}_{i,j_i}$ with $\tilde{s}_{i+1,j_i}$ and $\tilde{s}_{i+1,j_i+1}$. Moreover, since $\{\Lambda_{i+1,j_i}, \Lambda_{i+1,j_i+1}\}$ is a partition on Λ_{i,j_i}, we have

$$\tilde{s}_{i,j_i} = \tilde{s}_{i+1,j_i} + \tilde{s}_{i+1,j_i+1}$$

and therefore, if $\tilde{s}_i$ is known, only one of $\tilde{s}_{i+1,j_i}$ and $\tilde{s}_{i+1,j_i+1}$ is needed to calculate $\tilde{s}_{i+1}$. We call $\tilde{s}_{i+1,j_i}$ as the augmenting syndrome from $\tilde{s}_i$ to $\tilde{s}_{i+1}$, denoted by a_{i+1}. We also adopt the convention that $a_1 = \tilde{s}_{1,1}$ for convenience. In addition, according to the discussion above, $\tilde{s}_i = \mathbf{H}_{\mathcal{P}_i} x^n$, where $\mathbf{H}_{\mathcal{P}_i}$ can be determined by $\mathbf{H}_{n\times n}$ and $\mathcal{P}_i$. For clarification, we refer to $\mathbf{H}_{\mathcal{P}_i}$ as $\mathbf{H}^{(i)}_{i\times n}$, where the lower script indicates its dimension.

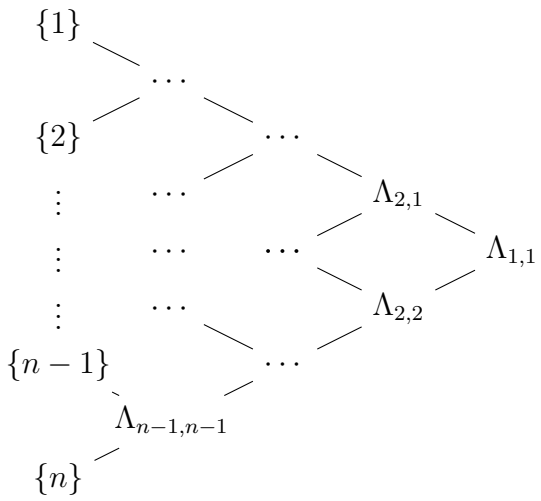


Figure 6.2: Binary Tree Structure of Syndrome Accumulation

By Remark 7 in [45], a binary tree can be associated with $\mathcal{P}_1\mathcal{P}_2\cdots\mathcal{P}_n$ or $\tilde{s}_1\tilde{s}_2\cdots\tilde{s}_n$, shown in figure 6.2, where each node represents a subset of $\mathcal{N}$. Let v and $\Lambda(v)$ be a node and its associated set. $\{\Lambda(v_l), \Lambda(v_r)\}$ forms a partition of $\Lambda(v)$ when v_l and v_r are the left and right child nodes of v. Moreover, let $v(\Lambda)$ be the node associated with the set Λ, and d_v be the depth of a node v. Then $|\Lambda| = 2^{T-d_{v(\Lambda)}}$.

6.2.3 Interactive Encoding and Decoding Schemes

In light of LDPC codes, we consider only binary sources. That is, the source alphabet $\mathcal{X}$ is binary. However, the side information alphabet $\mathcal{Y}$ could be arbitrary. For any $x^n \in \mathcal{X}^n$, let $\bar{x}^n$ be the complement sequence of x^n, i.e., the sequence having hamming distance n from x^n. Let $\mathbf{H}_{n\times n}$ be the parity check matrix of a LDPC code randomly generated from the ensemble $\mathcal{H}_{n,L(z)}$ for some $L(z)$. Let $\mathbf{H}'_{\eta_n n\times n}$ and $\mathbf{H}''_{\left(n\frac{H(\epsilon)}{\ln 2}+\Delta\right)\times n}$ be matrices from Gallager parity check ensemble (the set of matrices with each element generated independently and uniformly from $\mathcal{X}$), where $0 < \eta_n < 1$, $0 < \epsilon < 0.5$, and $n\frac{H(\epsilon)}{\ln 2}$ is assumed to be an integer. Furthermore, let $\mathcal{P}_1\mathcal{P}_2\cdots\mathcal{P}_n$ be the partition sequence described in the previous subsection. Based on the concepts introduced above, we are now ready to describe our SA-LDPC-IED scheme $\mathcal{I}_n$, which is presented in detail in Algorithm 2 below, where x^n is the source sequence to be encoded, $y^n \in \mathcal{Y}^n$ is the side information sequence available only to the decoder, and Δ is an integer to be specified later such that $\frac{n}{\Delta}$ is also an integer. Moreover, given side information y^n, the jar $J_b(y^n)$ at b-th round interaction is defined as

$$J_b(y^n) = \begin{cases} \{z^n \in \mathcal{X}^n : \gamma_n(z^n, y^n) \le \Gamma_b\} & 1 \le b \le \frac{n}{\Delta} \\ \mathcal{X}^n & b > \frac{n}{\Delta} \end{cases} \tag{6.1}$$

where the specification of Γ_b, η_n and the function $\gamma_n : \mathcal{X}^n \times \mathcal{Y}^n \to (0, +\infty)$ depends on $L(z)$, and will be discussed in the next section. Note that when $b > \frac{n}{\Delta}$, $J_b(y^n)$ consists of all possible source sequence of length n, which guarantees the existence of $\hat{x}^n$ at steps 18 and 19 in the algorithm.

As in [40, 41, 45], given any $(x^n, y^n) \in \mathcal{X}^n \times \mathcal{Y}^n$, the performance of $\mathcal{I}_n$ is measured by the number of nats per symbol from the encoder to the decoder $r_f(x^n, y^n|\mathcal{I}_n)$, the number of bits per symbol from the decoder to the encoder $r_b(x^n, y^n|\mathcal{I}_n)$, and the conditional error probability $P(\mathcal{I}_n|x^n, y^n)$ of $\mathcal{I}_n$ given x^n and y^n. Let $j(x^n, y^n)$ be the number of interactions at the time the decoder sends bit 1 to the encoder. It follows from the description of Algorithm 2 that*

$$r_f(x^n, y^n|\mathcal{I}_n) = \begin{cases} \frac{j(x^n,y^n)\Delta}{n}\ln 2 + H(\epsilon) + \frac{\Delta}{n}\ln 2 & \text{if } j(x^n, y^n) \le n/\Delta \\ (1+\eta_n)\ln 2 + H(\epsilon) + \frac{\Delta}{n}\ln 2 & \text{otherwise} \end{cases} \tag{6.2}$$

and

$$r_b(x^n, y^n|\mathcal{I}_n) = \frac{j(x^n, y^n)}{n}\ln 2. \tag{6.3}$$

*By the convention of this thesis, information rates are in nats.

Algorithm 2 SA-LDPC-IED scheme $\mathcal{I}_n$

Based on $\mathcal{P}_1\mathcal{P}_2\cdots\mathcal{P}_n$ and $s^n = \mathbf{H}_{n\times n}x^n$, the encoder generates accumulated syndromes $\tilde{s}_1\tilde{s}_2\cdots\tilde{s}_n$ and augmenting syndromes $a_1a_2\cdots a_n$.

Based on $\mathcal{P}_1\mathcal{P}_2\cdots\mathcal{P}_n$ and $\mathbf{H}_{n\times n}$, the decoder calculates matrices $\mathbf{H}^{(\Delta)}_{\Delta\times n}\mathbf{H}^{(2\Delta)}_{2\Delta\times n}\cdots\mathbf{H}^{(n)}_{n\times n}$.

$b \leftarrow 0$.

while The encoder does not receive bit 1 from the decoder **do**

  $b \leftarrow b+1$.

  if $b \leq \frac{n}{\Delta}$ **then**

    The encoder sends augmenting syndromes $a_{(b-1)\Delta+1}\cdots a_{b\Delta}$ to the decoder by Δ bits.

  else

    The encoder sends syndromes $s'_{\eta_n n} = \mathbf{H'}_{\eta_n n\times n}x^n$ to the decoder by $\eta_n n$ bits.

  end if

  Upon receiving syndromes sent from the encoder, the decoder searches through $J_b(y^n)$ for a sequence $\hat{x}^n$ satisfying $\mathbf{H}^{(b\Delta)}_{b\Delta\times n}\hat{x}^n = \tilde{s}_{b\Delta}$ if $b \leq \frac{n}{\Delta}$ and

$$\begin{bmatrix} \mathbf{H}^{(n)}_{n\times n} \\ \mathbf{H'}_{\eta_n n\times n} \end{bmatrix}\hat{x}^n = \begin{bmatrix} \tilde{s}_n \\ s'_{\eta_n n} \end{bmatrix}$$

  otherwise.

  if Such an $\hat{x}^n$ is found **then**

    The decoder sends bit 1 to the encoder.

  else

    The decoder sends bit 0 to the encoder.

  end if

end while

Upon receiving bit 1 from the decoder, the encoder sends $s''_{n\frac{H(\epsilon)}{\ln 2}+\Delta} = \mathbf{H''}_{\left(n\frac{H(\epsilon)}{\ln 2}+\Delta\right)\times n}x^n$ to the decoder.

Upon receiving $s''_{n\frac{H(\epsilon)}{\ln 2}+\Delta}$, the decoder searches through the set

$$D = \left\{ z^n : \frac{1}{n}wt(z^n - \hat{x}^n) \leq \epsilon \text{ or } \frac{1}{n}wt(z^n - \hat{x}^n) \geq 1-\epsilon \right\}.$$

for a sequence $\tilde{x}^n$ satisfying $\mathbf{H''}_{\left(n\frac{H(\epsilon)}{\ln 2}+\Delta\right)\times n}\tilde{x}^n = s''_{n\frac{H(\epsilon)}{\ln 2}+\Delta}$. If such an $\tilde{x}^n$ is found, the decoder outputs $\tilde{x}^n$ as the estimate of x^n. Otherwise, decoding failure is declared.

Moreover, let $(X,Y)=\{(X_i,Y_i)\}_{i=1}^{\infty}$ be a stationary source pair. We further define

$$r_f(\mathcal{I}_n) \triangleq \mathbb{E}\left[r_f(X^n,Y^n|\mathcal{I}_n)\right]$$

$$r_b(\mathcal{I}_n) \triangleq \mathbb{E}\left[r_b(X^n,Y^n|\mathcal{I}_n)\right]$$

and

$$P_e(\mathcal{I}_n) \triangleq \Pr\{\tilde{X}^n \neq X^n\}.$$

Remark 6.1. *As can be seen, SA-LDPC-IED distinguishes itself from LIED and SA-IED proposed in [45] by the ensembles of parity check matrices. Specifically, SA-LDPC-IED, LIED, and SA-IED schemes all assume that $\tilde{s}_{b\Delta}=\mathbf{H}_{b\Delta\times n}^{(b\Delta)}x^n$ is available to the decoder at b-th interaction, but the ways of generating $\mathbf{H}_{b\Delta\times n}^{(b\Delta)}$ are totally different. In an SA-LDPC-IED scheme, given the variable and check node degree distribution of $\mathbf{H}_{n\times n}$, the variable node degree distribution of $\mathbf{H}_{b\Delta\times n}^{(b\Delta)}$ will be roughly the same as that of $\mathbf{H}_{n\times n}$, considering the fact that the matrix $\mathbf{H}_{n\times n}$ is sparse. On the other hand, for an LIED scheme (using Gallager-type ensembles),*

$$\mathbf{H}_{b\Delta\times n}^{(b\Delta)}=\begin{bmatrix}\mathbf{H}_{\Delta\times n}(1)\\ \mathbf{H}_{\Delta\times n}(2)\\ \vdots\\ \mathbf{H}_{\Delta\times n}(b)\end{bmatrix}$$

where each $\mathbf{H}_{\Delta\times n}(i)$ is generated in the way that elements equal to 1 with probability p_n^* and to 0 with probability $1-p_n^*$. As can be seen, variable node degrees of each $\mathbf{H}_{\Delta\times n}(i)$ are purely random, as well as that of $\mathbf{H}_{b\Delta\times n}^{(b\Delta)}$. Now for an SA-IED scheme (using vector-type ensembles),

$$\mathbf{H}_{b\Delta\times n}^{(b\Delta)}=\begin{bmatrix}\mathbf{H}_{b\times n}^{(b)}(1)\\ \mathbf{H}_{b\times n}^{(b)}(2)\\ \vdots\\ \mathbf{H}_{b\times n}^{(b)}(\Delta)\end{bmatrix}$$

where each $\mathbf{H}_{b\times n}^{(b)}(i)$ is resulted by applying the syndrome accumulation described above to $\mathbf{H}_{\left(\frac{n}{\Delta}+1\right)\times n}(i)$, each column of which is generated independently and equals to a vector of degree one with probability p_n^* or to a zero vector with probability $1-\left(\frac{n}{\Delta}+1\right)p_n^*$. (Note that there are $\frac{n}{\Delta}+1$ different vectors of degree one and dimension $\frac{n}{\Delta}+1$.) In this case, although the variable node degrees of $\mathbf{H}_{b\times n}^{(b)}(i)$ are either 0 and 1, the variable node degrees of $\mathbf{H}_{b\Delta\times n}^{(b\Delta)}$ are still purely random, as each $\mathbf{H}_{b\times n}^{(b)}(i)$ is generated independently. The independence

in Gallager-type and vector-type ensembles mitigates the difficulty of the proof of coding theorems to some extent. However, as the variable node degrees of decoding matrices are purely random, BP decoding does not behave well for those schemes, which is the motivation to propose and investigate SA-LDPC-IED schemes.

6.3 Performance of SA-LDPC-IED: General Case

This section is devoted to the theoretical performance analysis of our proposed SA-LDPC-IED scheme $\mathcal{I}_n$ for both individual sequences x^n and y^n and stationary, ergodic sources. Throughout this section, we assume that $\Delta \sim \sqrt{n}$.

6.3.1 Specification of $\gamma_n(\cdot,\cdot)$, η_n, and $\{\Gamma_b\}$, and Probability Bounds

In order for our proposed SA-LDPC-IED scheme $\mathcal{I}_n$ to be truly universal, i.e., to achieve good performance for each and every individual source and side information pair (x^n, y^n), we associate $\gamma_n(\cdot,\cdot)$ with a classical universal lossless code $\mathcal{C}_n$ (with block length n and the side information available to both the encoder and decoder), where $\mathcal{C}_n$ is a mapping from $\mathcal{X}^n \times \mathcal{Y}^n$ to $\{0,1\}^*$ satisfying that for any $y^n \in \mathcal{Y}^n$, the set $\{\mathcal{C}_n(x^n, y^n) : x^n \in \mathcal{X}^n\}$ is a prefix set. Specifically, we define

$$\gamma_n(x^n, y^n) = h_n(x^n|y^n)$$

where $nh_n(x^n|y^n)$ is the number of nats resulting from applying $\mathcal{C}_n$ to encode x^n from $\mathcal{X}$ given the side information sequence y^n from $\mathcal{Y}$ available to both the encoder and decoder. Consequently, each $J_b(y^n)$ defined in (6.1) for $1 \le b \le \frac{n}{\Delta}$ is a jar from classical prefix code shown in Example 5 in Section 1.2.

Following the approach adopted in [41,45], it is essential to calculate the following probabilities $\Pr\left\{\mathbf{H}'_{\eta_n n\times n}x^n = 0^{\eta_n n}\right\}$, $\Pr\left\{\mathbf{H}''_{\left(n\frac{H(\epsilon)}{\ln 2}+\Delta\right)\times n}x^n = 0^{n\frac{H(\epsilon)}{\ln 2}+\Delta}\right\}$ and $\Pr\left\{\mathbf{H}^{(b\Delta)}_{b\Delta\times n}x^n = 0^{b\Delta}\right\}$ for $1 \le b \le \frac{n}{\Delta}$, given $x^n \neq 0^n$. In addition, in our case, the specification of η_n, and $\{\Gamma_b\}$ is also related to the probability $\Pr\left\{\mathbf{H}^{(b\Delta)}_{b\Delta\times n}x^n = 0^{b\Delta}\right\}$. Since $\mathbf{H}'_{\eta_n n\times n}$ and $\mathbf{H}''_{\left(n\frac{H(\epsilon)}{\ln 2}+\Delta\right)\times n}$ are obtained from Gallager parity check ensemble, it can be easily shown that

$$\begin{aligned}
\Pr\left\{\mathbf{H}'_{\eta_n n\times n}x^n = 0^{\eta_n n}\right\} &= 2^{-\eta_n n} = e^{-\eta_n n \ln 2} \\
\Pr\left\{\mathbf{H}''_{\left(n\frac{H(\epsilon)}{\ln 2}+\Delta\right)\times n}x^n = 0^{n\frac{H(\epsilon)}{\ln 2}+\Delta}\right\} &= 2^{-n\frac{H(\epsilon)}{\ln 2}-\Delta} = e^{-nH(\epsilon)-\Delta\ln 2}
\end{aligned}$$

for any $x^n \neq 0^n$. However, calculating $\Pr\left\{\mathbf{H}^{(b\Delta)}_{b\Delta\times n}x^n = 0^{b\Delta}\right\}$ is much harder.

It can be seen that

$$\Pr\left\{\mathbf{H}^{(b\Delta)}_{b\Delta\times n}x^n = 0^{b\Delta}\right\}$$

depends on the support set of x^n, i.e., the positions of non-zero elements in x^n. Let $\varkappa(x^n)$ represent the support set of x^n, and we write $\varkappa(x^n)$ simply as $\varkappa$ whenever x^n is generic or can be determined from context. Let $\mathbf{H}^{\varkappa}_{n\times|\varkappa|}$ be the matrix consisting of those columns of $\mathbf{H}_{n\times n}$ with indices in $\varkappa$. The degree polynomial of $\varkappa$, denoted by $L^{\varkappa}(z)$, is defined by

$$L^{\varkappa}(z) \triangleq \sum_{i=1}^{L} L_i^{\varkappa} z^{l_i}$$

where $L_i^{\varkappa} n$ is the number of columns with degree l_i within $\mathbf{H}^{\varkappa}_{n\times|\varkappa|}$. And define

$$\bar{l}^{\varkappa} \triangleq \sum_{i=1}^{L} L_i^{\varkappa} l_i.$$

Now let

$$\begin{aligned}
t^{(1)}_{b\Delta} &= \min\left\{2b\Delta - 2^{\lceil\log_2 b\Delta\rceil}, R_1 2^{\lceil\log_2 b\Delta\rceil}\right\},\\
t^{(2)}_{b\Delta} &= \max\left\{R_1 2^{\lceil\log_2 b\Delta\rceil-1} - \left(b\Delta - 2^{\lceil\log_2 b\Delta\rceil-1}\right), 0\right\},\\
t^{(3)}_{b\Delta} &= \max\left\{R_2 2^{\lceil\log_2 b\Delta\rceil} - 2\left(2^{\lceil\log_2 b\Delta\rceil} - b\Delta\right), 0\right\},\\
t^{(4)}_{b\Delta} &= \min\left\{2^{\lceil\log_2 b\Delta\rceil} - b\Delta, R_2 2^{\lceil\log_2 b\Delta\rceil-1}\right\}.
\end{aligned}$$

To understand the meaning of $\left\{t^{(i)}_{b\Delta}\right\}_{i=1}^{4}$, let us focus on $\mathcal{P}_{b\Delta} = \{\Lambda_{b\Delta,i}\}_{i=1}^{b\Delta}$. By the binary tree representation in the previous section,

$$\begin{aligned}
t^{(1)}_{b\Delta} &= \#\text{ of } \Lambda_{b\Delta,i} \text{ s.t. } \Lambda_{b\Delta,i} \subseteq \{1\cdots R_1 n\} \text{ and } d_{v(\Lambda_{b\Delta,i})} = 2^{\lceil\log_2 b\Delta\rceil}\\
t^{(2)}_{b\Delta} &= \#\text{ of } \Lambda_{b\Delta,i} \text{ s.t. } \Lambda_{b\Delta,i} \subseteq \{1\cdots R_1 n\} \text{ and } d_{v(\Lambda_{b\Delta,i})} = 2^{\lceil\log_2 b\Delta\rceil-1}\\
t^{(3)}_{b\Delta} &= \#\text{ of } \Lambda_{b\Delta,i} \text{ s.t. } \Lambda_{b\Delta,i} \subseteq \{R_1 n+1\cdots n\} \text{ and } d_{v(\Lambda_{b\Delta,i})} = 2^{\lceil\log_2 b\Delta\rceil}\\
t^{(4)}_{b\Delta} &= \#\text{ of } \Lambda_{b\Delta,i} \text{ s.t. } \Lambda_{b\Delta,i} \subseteq \{R_1 n+1\cdots n\} \text{ and } d_{v(\Lambda_{b\Delta,i})} = 2^{\lceil\log_2 b\Delta\rceil-1}
\end{aligned}$$

Since the block length n is assumed to be a power of 2, it follows that

$$\begin{aligned}
\frac{t_{b\Delta}^{(1)}}{n} &= \min\left\{\frac{2b\Delta}{n} - 2^{\lceil \log_2 \frac{b\Delta}{n}\rceil}, R_1 2^{\lceil \log_2 \frac{b\Delta}{n}\rceil}\right\} \\
\frac{t_{b\Delta}^{(2)}}{n} &= \max\left\{R_1 2^{\lceil \log_2 \frac{b\Delta}{n}\rceil - 1} - \left(\frac{b\Delta}{n} - 2^{\lceil \log_2 \frac{b\Delta}{n}\rceil - 1}\right), 0\right\} \\
\frac{t_{b\Delta}^{(3)}}{n} &= \max\left\{R_2 2^{\lceil \log_2 \frac{b\Delta}{n}\rceil} - 2\left(2^{\lceil \log_2 \frac{b\Delta}{n}\rceil} - \frac{b\Delta}{n}\right), 0\right\} \\
\frac{t_{b\Delta}^{(4)}}{n} &= \min\left\{2^{\lceil \log_2 \frac{b\Delta}{n}\rceil} - \frac{b\Delta}{n}, R_2 2^{\lceil \log_2 \frac{b\Delta}{n}\rceil - 1}\right\}
\end{aligned}$$

and hence $\frac{t_{b\Delta}^{(i)}}{n}$, $i = 1, 2, 3, 4$, all depend only on $b\Delta/n$.

We have the following result, which is proved in Appendix B.1.

Lemma 6.1. *Let $L(z)$ be a normalized variable node degree distribution from a node perspective with minimum degree $l_1 \geq 2$. Let $c_{b\Delta} = 2^{-\lceil \log_2 \frac{b\Delta}{n}\rceil}$ and $g(\tau, k) \stackrel{\Delta}{=} (1+\tau)^k + (1-\tau)^k$ for any τ and k. Suppose $\mathbf{H}_{n\times n}$ is uniformly picked from ensemble $\mathcal{H}_{n,L(z)}$. Then for any $x^n \neq 0$ with its support set $\varkappa$,*

$$\Pr\left\{\mathbf{H}_{b\Delta\times n}^{(b\Delta)} x^n = 0^{b\Delta}\right\} \leq \exp\left\{nP\left(\frac{b\Delta}{n}, \bar{l}, \bar{l}^{\varkappa}\right) + \frac{3n\lceil \bar{l}\rceil}{b\Delta}\ln(n\hat{l}^{\varkappa}) + \frac{1}{2}\ln n\bar{l}^{\varkappa}(1 - \frac{\bar{l}^{\varkappa}}{\bar{l}}) + O(1)\right\}$$

where

$$\hat{l}^{\varkappa} = \max\left\{\frac{1}{n}, \min\{\bar{l}^{\varkappa}, \bar{l} - \bar{l}^{\varkappa}\}\right\}$$

and for any $\frac{b\Delta}{n}, \bar{l}$ and $\xi \in (0, \bar{l}]$, $P\left(\frac{b\Delta}{n}, \bar{l}, \xi\right)$ is defined as

$$\begin{aligned}
&P\left(\frac{b\Delta}{n}, \bar{l}, \xi\right) \\
&\stackrel{\Delta}{=} -\bar{l}H\left(\xi/\bar{l}\right) - \xi\ln\tau \\
&+ \frac{t_{b\Delta}^{(1)}}{n}\ln\frac{g(\tau, r_1 c_{b\Delta})}{2} \\
&+ \frac{t_{b\Delta}^{(2)}}{n}\ln\frac{g(\tau, 2r_1 c_{b\Delta})}{2} \\
&+ \frac{t_{b\Delta}^{(3)}}{n}\ln\frac{g(\tau, r_2 c_{b\Delta})}{2} \\
&+ \frac{t_{b\Delta}^{(4)}}{n}\ln\frac{g(\tau, 2r_2 c_{b\Delta})}{2}
\end{aligned} \tag{6.4}$$

in which τ is the solution to

$$\begin{aligned}
&r_1 c_{b\Delta} \frac{t_{b\Delta}^{(1)}}{n} \frac{g(\tau, r_1 c_{b\Delta} - 1)}{g(\tau, r_1 c_{b\Delta})} \\
&+2r_1 c_{b\Delta} \frac{t_{b\Delta}^{(2)}}{n} \frac{g(\tau, 2r_1 c_{b\Delta} - 1)}{g(\tau, 2r_1 c_{b\Delta})} \\
&+r_2 c_{b\Delta} \frac{t_{b\Delta}^{(3)}}{n} \frac{g(\tau, r_2 c_{b\Delta} - 1)}{g(\tau, r_2 c_{b\Delta})} \\
&+2r_2 c_{b\Delta} \frac{t_{b\Delta}^{(4)}}{n} \frac{g(\tau, 2r_2 c_{b\Delta} - 1)}{g(\tau, 2r_1 c_{b\Delta})} \\
&= \bar{l} - \xi. \qquad (6.5)
\end{aligned}$$

for $\xi \in \left[0, \bar{l} - \frac{t_{b\Delta}^{(1)}}{n}\pi\left(c_{b\Delta} r_1\right) - \frac{t_{b\Delta}^{(3)}}{n}\pi\left(c_{b\Delta} r_2\right)\right]$, *and*

$$P\left(\frac{b\Delta}{n}, \bar{l}, \xi\right) \triangleq -\infty \qquad (6.6)$$

for $\xi \in \left(\bar{l} - \frac{t_{b\Delta}^{(1)}}{n}\pi\left(c_{b\Delta} r_1\right) - \frac{t_{b\Delta}^{(3)}}{n}\pi\left(c_{b\Delta} r_2\right), \bar{l}\right]$ *with the convention that* $e^{-\infty} = 0$.

Remark 6.2. *When* $\xi = \bar{l} - \frac{t_{b\Delta}^{(1)}}{n}\pi\left(c_{b\Delta} r_1\right) - \frac{t_{b\Delta}^{(3)}}{n}\pi\left(c_{b\Delta} r_2\right)$, *the solution* τ *to (6.5) is* $\tau = +\infty$. *In this case, the expression in (6.4) should be understood as its limit as* $\tau \to +\infty$, *i.e.,*

$$\begin{aligned}
&P\left(\frac{b\Delta}{n}, \bar{l}, \xi\right) \\
&\triangleq -\bar{l} H\left(\xi/\bar{l}\right) + \lim_{\tau \to +\infty} \left[-\xi \ln \tau + \frac{t_{b\Delta}^{(1)}}{n} \ln \frac{g(\tau, r_1 c_{b\Delta})}{2} + \frac{t_{b\Delta}^{(2)}}{n} \ln \frac{g(\tau, 2r_1 c_{b\Delta})}{2} \right. \\
&\quad \left. + \frac{t_{b\Delta}^{(3)}}{n} \ln \frac{g(\tau, r_2 c_{b\Delta})}{2} + \frac{t_{b\Delta}^{(4)}}{n} \ln \frac{g(\tau, 2r_2 c_{b\Delta})}{2} \right] \\
&= -\bar{l} H\left(\xi/\bar{l}\right) + \frac{t_{b\Delta}^{(1)}}{n}\pi(c_{b\Delta} r_1) \ln[c_{b\Delta} r_1] + \frac{t_{b\Delta}^{(3)}}{n}\pi(c_{b\Delta} r_2) \ln[c_{b\Delta} r_2] \qquad (6.7)
\end{aligned}$$

when $\xi = \bar{l} - \frac{t_{b\Delta}^{(1)}}{n}\pi\left(c_{b\Delta} r_1\right) - \frac{t_{b\Delta}^{(3)}}{n}\pi\left(c_{b\Delta} r_2\right)$.

Remark 6.3. *Replace* $\frac{b\Delta}{n}$ *by any real number* $R \in (0,1]$ *in* $\frac{t_{b\Delta}^{(i)}}{n}$, $i = 1,2,3,$ *and* 4, $c_{b\Delta}$, *and* $P\left(\frac{b\Delta}{n}, \bar{l}, \xi\right)$. *It is not hard to verify that* $\frac{t_{b\Delta}^{(i)}}{n}$, $i = 1,2,3,$ *and* 4, $c_{b\Delta}$, *and* $P\left(R, \bar{l}, \xi\right)$ *as a respective function of* $R \in (0,1]$ *are all well defined. One can further verify that as a function of* $R \in (0,1]$, *the following identities hold:*

$$\sum_{i=1}^{4} \frac{t_{b\Delta}^{(i)}}{n} = R \tag{6.8}$$

and

$$r_1 c_{b\Delta} \frac{t_{b\Delta}^{(1)}}{n} + 2r_1 c_{b\Delta} \frac{t_{b\Delta}^{(2)}}{n} + r_2 c_{b\Delta} \frac{t_{b\Delta}^{(3)}}{n} + 2r_2 c_{b\Delta} \frac{t_{b\Delta}^{(4)}}{n} = \bar{l}\,. \tag{6.9}$$

As illustrated in Figure 6.3, the function $P\left(R, \bar{l}, \xi\right)$ has several interesting properties including

PR1 given $(R, \bar{l})$, $P\left(R, \bar{l}, \xi\right)$ is a strictly decreasing function of ξ over $\xi \in (0, \bar{l}/2]$;

PR2 given $0 < \xi \leq \bar{l}/2$, $P\left(R, \bar{l}, \xi\right)$ as a function of R is continuous and strictly decreasing over $R \in (0,1]$, and furthermore

$$P\left(0, \bar{l}, \xi\right) \stackrel{\Delta}{=} \lim_{R \to 0} P\left(R, \bar{l}, \xi\right) = 0$$

PR3 and $P\left(R, \bar{l}, \xi\right)$ is close to $-R \ln 2$ when $\xi \leq \bar{l}/2$ is not too far away from $\bar{l}/2$.

These and other properties of $P\left(R, \bar{l}, \xi\right)$ are needed in the performance analysis of our proposed SA-LDPC-IED Scheme $\mathcal{I}_n$. Their exact statements and respective proofs will be relegated to Appendix B.1.2.

Based on the function $P\left(\frac{b\Delta}{n}, \bar{l}, \xi\right)$, we are now ready to specify η_n and $\{\Gamma_b\}$ for any $1 \leq b \leq \frac{n}{\Delta}$ in our proposed SA-LDPC-IED Scheme $\mathcal{I}_n$, which are defined respectively as

$$\eta_n = 1 + \frac{1}{\ln 2}\left[P\left(1, \bar{l}, l_1\epsilon\right) + \frac{3\lceil \bar{l} \rceil}{n} \ln \frac{n\bar{l}}{2} + \frac{1}{2n} \ln \frac{n\bar{l}}{4}\right] + \frac{\Delta}{n}$$

and

$$\Gamma_b = -P\left(\frac{b\Delta}{n}, \bar{l}, l_1\epsilon\right) - \frac{3\lceil \bar{l} \rceil}{\Delta} \ln \frac{n\bar{l}}{2} - \frac{1}{2n} \ln \frac{n\bar{l}}{4} - \frac{\Delta}{n} \ln 2$$

where $\epsilon > 0$ is the same as in the description of the SA-LDPC-IED Scheme $\mathcal{I}_n$.

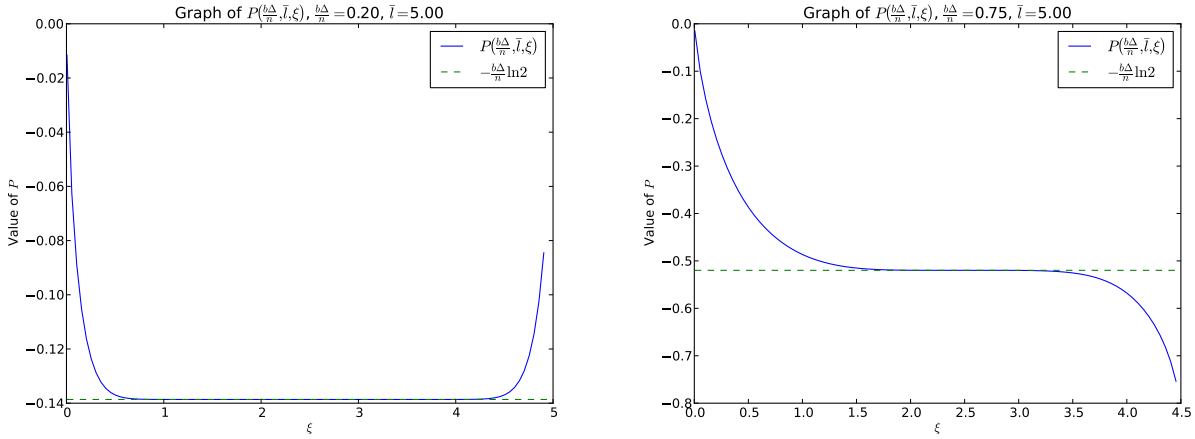


Figure 6.3: Graphical Illustration of $P\left(\frac{b\Delta}{n},\bar{l},\xi\right)$

6.3.2 Performance for Individual Sequences

We now analyze the performance of the SA-LDPC-IED scheme $\mathcal{I}_n$ in terms of the performance of the classical universal code $\mathcal{C}_n$ for any individual sequences x^n and y^n. We have the following theorem.

Theorem 6.1. *Let $L(z)$ represent a normalized variable node degree distribution from a node perspective with minimum degree $l_1 \geq 2$. Then for any $(x^n, y^n) \in \mathcal{X}^n \times \mathcal{Y}^n$,*

$$r_f(x^n, y^n|\mathcal{I}_n) \leq R^{(\Delta)}_{L(z)}\left(\epsilon, h_n(x^n|y^n)\right)\ln 2 + H(\epsilon) + \frac{2\Delta}{n}\ln 2 \tag{6.10}$$

$$r_b(x^n, y^n|\mathcal{I}_n) = O\left(\frac{1}{\sqrt{n}}\right) \tag{6.11}$$

and

$$P_e(\mathcal{I}_n|x^n, y^n) \leq 2^{-\Delta+\log_2\left(\frac{n}{\Delta}+1\right)+O(1)} \tag{6.12}$$

where $P_e(\mathcal{I}_n|x^n, y^n)$ denotes the conditional error probability of $\mathcal{I}_n$ given x^n and y^n, and $R^{(\Delta)}_{L(z)}\left(\epsilon, h_n(x^n|y^n)\right)$ is the positive solution R to

$$-P\left(R, \bar{l}, l_1\epsilon\right) = h_n(x^n|y^n) + \frac{3\lceil\bar{l}\rceil}{\Delta}\ln\frac{n\bar{l}}{2} + \frac{1}{2n}\ln\frac{n\bar{l}}{4} + \frac{\Delta}{n}\ln 2 \tag{6.13}$$

if $h_n(x^n|y^n) \le \Gamma_{\frac{n}{\Delta}}$, *and*

$$R_{L(z)}^{(\Delta)}\left(\epsilon, h_n(x^n|y^n)\right) = 2 + \frac{1}{\ln 2}\left[P\left(1, \bar{l}, l_1\epsilon\right) + \frac{3\lceil \bar{l} \rceil}{n}\ln\frac{n\bar{l}}{2} + \frac{1}{2n}\ln\frac{n\bar{l}}{4}\right] \tag{6.14}$$

otherwise.

Proof. Given x^n and y^n, let $j = j(x^n, y^n)$ be the number of interactions at the time the decoder sends bit 1 to the encoder. From (6.2) and (6.3), it follows that

$$r_f(x^n, y^n|\mathcal{I}_n) = \begin{cases} \frac{j\Delta}{n}\ln 2 + H(\epsilon) + \frac{\Delta}{n}\ln 2 & \text{if } j \le \Delta/n \\ (1+\eta_n)\ln 2 + H(\epsilon) + \frac{\Delta}{n}\ln 2 & \text{otherwise} \end{cases} \tag{6.15}$$

and

$$r_b(x^n, y^n|\mathcal{I}_n) = \frac{j}{n}\ln 2. \tag{6.16}$$

Since $\Delta \sim \sqrt{n}$ and $j \le \frac{n}{\Delta} + 1$ according to Algorithm 2, (6.11) follows immediately.

In view of the description of Algorithm 2, it is not hard to see that at the $(j-1)$th interaction, one always has

$$\Gamma_{j-1} < h_n(x^n|y^n)\ . \tag{6.17}$$

We now distinguish between two cases: (1) $h_n(x^n|y^n) \le \Gamma_{\frac{n}{\Delta}}$, and (2) $h_n(x^n|y^n) > \Gamma_{\frac{n}{\Delta}}$. In case (1), it follows from (6.17) that

$$j \le \frac{n}{\Delta} \tag{6.18}$$

and

$$-P\left(\frac{(j-1)\Delta}{n}, \bar{l}, l_1\epsilon\right) - \frac{3\lceil \bar{l} \rceil}{\Delta}\ln\frac{n\bar{l}}{2} - \frac{1}{2n}\ln\frac{n\bar{l}}{4} - \frac{\Delta}{n}\ln 2 < h_n(x^n|y^n)$$

or equivalently

$$\begin{aligned} -P\left(\frac{(j-1)\Delta}{n}, \bar{l}, l_1\epsilon\right) &< h_n(x^n|y^n) + \frac{3\lceil \bar{l} \rceil}{\Delta}\ln\frac{n\bar{l}}{2} + \frac{1}{2n}\ln\frac{n\bar{l}}{4} + \frac{\Delta}{n}\ln 2 \\ &= -P\left(R_{L(z)}^{(\Delta)}\left(\epsilon, h_n(x^n|y^n)\right), \bar{l}, l_1\epsilon\right)\ . \end{aligned}$$

By Lemma B.5, $P\left(R, \bar{l}, l_1\epsilon\right)$ is strictly decreasing with respect to R. Therefore,

$$\frac{(j-1)\Delta}{n}\ln 2 < R_{L(z)}^{(\Delta)}\left(\epsilon, h_n(x^n|y^n)\right)\ . \tag{6.19}$$

Combining (6.15), (6.18), and (6.19) together yields

$$r_f(x^n, y^n|\mathcal{I}_n) \leq R^{(\Delta)}_{L(z)}\left(\epsilon, h_n(x^n|y^n)\right) \ln 2 + H(\epsilon) + \frac{2\Delta}{n} \ln 2 \, .$$

This completes the proof of (6.10) in case (1).

In case (2), j could be strictly greater than $\frac{n}{\Delta}$. Regardless of the value of j, in case (2), one always has

$$\begin{aligned} r_f(x^n, y^n|\mathcal{I}_n) &\leq (1+\eta_n) \ln 2 + H(\epsilon) + \frac{\Delta}{n} \ln 2 \\ &= R^{(\Delta)}_{L(z)}\left(\epsilon, h_n(x^n|y^n)\right) \ln 2 + H(\epsilon) + \frac{2\Delta}{n} \ln 2 \, . \end{aligned}$$

This completes the proof of (6.10) in case (2).

Towards bounding the error probability, for any $x^n \in \mathcal{X}^n$ and $0 < \epsilon < 0.5$, define

$$B(\epsilon, x^n) = \left\{ z^n \in \mathcal{X}^n : \frac{1}{n} wt(z^n - x^n) < \epsilon \text{ or } \frac{1}{n} wt(z^n - x^n) > 1 - \epsilon \right\} .$$

To proceed,

$$\begin{aligned} P_e\left\{\mathcal{I}_n|x^n, y^n\right\} &= \Pr\left\{\tilde{x}^n \neq x^n\right\} \\ &= \Pr\left\{\hat{x}^n \in B(\epsilon, x^n)\right\} \Pr\left\{\tilde{x}^n \neq x^n \,|\hat{x}^n \in B(\epsilon, x^n)\right\} \\ &\quad + \Pr\left\{\hat{x}^n \notin B(\epsilon, x^n)\right\} \Pr\left\{\tilde{x}^n \neq x^n \,|\hat{x}^n \notin B(\epsilon, x^n)\right\} \\ &\leq \Pr\left\{\tilde{x}^n \neq x^n \,|\hat{x}^n \in B(\epsilon, x^n)\right\} + \Pr\left\{\hat{x}^n \notin B(\epsilon, x^n)\right\} . \end{aligned}$$

We first consider $\Pr\left\{\hat{x}^n \notin B(\epsilon, x^n)\right\}$. By the union bound,

$$\begin{aligned} &\Pr\left\{\hat{x}^n \notin B(\epsilon, x^n)\right\} \\ &\quad \leq \Pr\left\{\exists z^n \notin B(\epsilon, x^n) : \mathbf{H}^{(b\Delta)}_{b\Delta\times n} z^n = \mathbf{H}^{(b\Delta)}_{b\Delta\times n} x^n, z^n \in J_b(y^n) \text{ for some } b,\, 1 \leq b \leq \frac{n}{\Delta}\right\} \\ &\qquad + \Pr\left\{\exists z^n \notin B(\epsilon, x^n) : \mathbf{H}_{n\times n} z^n = \mathbf{H}_{n\times n} x^n, \mathbf{H}'_{\eta_n n\times n} z^n = \mathbf{H}'_{\eta_n n\times n} x^n\right\} \\ &\quad \leq \sum_{b=1}^{\frac{n}{\Delta}} \Pr\left\{\exists z^n \notin B(\epsilon, x^n) : \mathbf{H}^{(b\Delta)}_{b\Delta\times n} z^n = \mathbf{H}^{(b\Delta)}_{b\Delta\times n} x^n, z^n \in J_b(y^n)\right\} \\ &\qquad + \Pr\left\{\exists z^n \notin B(\epsilon, x^n) : \mathbf{H}_{n\times n} z^n = \mathbf{H}_{n\times n} x^n, \mathbf{H}'_{\eta_n n\times n} z^n = \mathbf{H}'_{\eta_n n\times n} x^n\right\} . \end{aligned}$$

Now by Lemma 6.1, for $1 \le b \le \frac{n}{\Delta}$,

$$\begin{aligned}
&\Pr\left\{\mathbf{H}^{(b\Delta)}_{b\Delta\times n} z^n = \mathbf{H}^{(b\Delta)}_{b\Delta\times n} x^n\right\} \\
&= \Pr\left\{\mathbf{H}^{(b\Delta)}_{b\Delta\times n}(z^n - x^n) = 0^{b\Delta}\right\} \\
&\le \exp\left\{nP\left(\frac{b\Delta}{n}, \bar{l}, \xi\right) + \frac{3n\lceil\bar{l}\rceil}{b\Delta}\ln(n\hat{\xi}) + \frac{1}{2}\ln n\xi\left(1 - \frac{\xi}{\bar{l}}\right) + O(1)\right\} \\
&\le \exp\left\{n\left[P\left(\frac{b\Delta}{n}, \bar{l}, \xi\right) + \frac{3\lceil\bar{l}\rceil}{\Delta}\ln\frac{n\bar{l}}{2} + \frac{1}{2n}\ln\frac{n\bar{l}}{4}\right] + O(1)\right\}
\end{aligned}$$

while

$$\begin{aligned}
&\Pr\left\{\mathbf{H}_{n\times n} z^n = \mathbf{H}_{n\times n} x^n\right\} \\
&= \Pr\left\{\mathbf{H}_{n\times n}(z^n - x^n) = 0^n\right\} \\
&\le \exp\left\{nP\left(1, \bar{l}, \xi\right) + 3\lceil\bar{l}\rceil\ln(n\hat{\xi}) + \frac{1}{2}\ln n\xi\left(1 - \frac{\xi}{\bar{l}}\right) + O(1)\right\} \\
&\le \exp\left\{n\left[P\left(1, \bar{l}, \xi\right) + \frac{3\lceil\bar{l}\rceil}{n}\ln\frac{n\bar{l}}{2} + \frac{1}{2n}\ln\frac{n\bar{l}}{4}\right] + O(1)\right\},
\end{aligned}$$

where $\xi = \bar{l}^{\varkappa(z^n - x^n)}$ and $\hat{\xi} = \max\left\{\frac{1}{n}, \min\left\{\xi, \bar{l} - \xi\right\}\right\}$. Simple calculation reveals that $l_1\epsilon \le \xi \le \bar{l} - l_1\epsilon$ for $z^n \notin B(\epsilon, x^n)$, which, together with Lemmas B.2 and B.3, further implies that

$$\begin{aligned}
&\Pr\left\{\mathbf{H}^{(b\Delta)}_{b\Delta\times n} z^n = \mathbf{H}^{(b\Delta)}_{b\Delta\times n} x^n\right\} \\
&\le \exp\left\{n\left[P\left(\frac{b\Delta}{n}, \bar{l}, l_1\epsilon\right) + \frac{3\lceil\bar{l}\rceil}{\Delta}\ln\frac{n\bar{l}}{2} + \frac{1}{2n}\ln\frac{n\bar{l}}{4}\right] + O(1)\right\} = e^{-n\Gamma_b - \Delta\ln 2 + O(1)}
\end{aligned}$$

and

$$\begin{aligned}
&\Pr\left\{\mathbf{H}_{n\times n} z^n = \mathbf{H}_{n\times n} x^n\right\} \\
&\le \exp\left\{n\left[P\left(1, \bar{l}, l_1\epsilon\right) + \frac{3\lceil\bar{l}\rceil}{n}\ln\frac{n\bar{l}}{2} + \frac{1}{2n}\ln\frac{n\bar{l}}{4}\right] + O(1)\right\} = e^{-n(1-\eta_n)\ln 2 - \Delta\ln 2 + O(1)}.
\end{aligned}$$

Now by the union bound again, for $1 \le b \le \frac{n}{\Delta}$,

$$\begin{aligned}
&\Pr\left\{\exists z^n \notin B(\epsilon, x^n) : \mathbf{H}^{(b\Delta)}_{b\Delta\times n} z^n = \mathbf{H}^{(b\Delta)}_{b\Delta\times n} x^n, z^n \in J_b(y^n)\right\} \\
&\le |J_b(y^n)/B(\epsilon, x^n)|\, e^{-n\Gamma_b - \Delta\ln 2 + O(1)} \\
&\le |J_b(y^n)| e^{-n\Gamma_b - \Delta\ln 2 + O(1)}.
\end{aligned}$$

By the upper bound on the size of jar from classical prefix codes in (1.13), we have

$$\Pr\left\{\exists z^n \notin B(\epsilon, x^n) : \mathbf{H}^{(b\Delta)}_{b\Delta\times n} z^n = \mathbf{H}^{(b\Delta)}_{b\Delta\times n} x^n, z^n \in J_b(y^n)\right\} \leq 2^{-\Delta+O(1)}.$$

At the same time,

$$\begin{aligned}
&\Pr\left\{\exists z^n \notin B(\epsilon, x^n) : \mathbf{H}_{n\times n} z^n = \mathbf{H}_{n\times n} x^n, \mathbf{H}'_{\eta_n n\times n} z^n = \mathbf{H}'_{\eta_n n\times n} x^n\right\} \\
\leq & \sum_{z^n\notin B(\epsilon,x^n)} \Pr\left\{\mathbf{H}_{n\times n}(z^n - x^n) = 0^n\right\} \Pr\left\{\mathbf{H}'_{\eta_n n\times n}(z^n - x^n) = 0^{\eta_n n}\right\} \\
\leq & \sum_{z^n\notin B(\epsilon,x^n)} e^{-n(1-\eta_n)\ln 2 - \Delta\ln 2 + O(1)} e^{-\eta_n n \ln 2} \\
\leq & \ 2^{-\Delta+O(1)}.
\end{aligned}$$

To sum up, we have shown that

$$\Pr\left\{\hat{x}^n \notin B(\epsilon, x^n)\right\} \leq 2^{-\Delta+\log_2\left(\frac{n}{\Delta}+1\right)+O(1)}.$$

Before moving to the next target $\Pr\left\{\tilde{x}^n \neq x^n \,|\hat{x}^n \in B(\epsilon, x^n)\right\}$, it is not hard to verify the following bound on $|B(\epsilon, x^n)|$:

$$\begin{aligned}
|B(\epsilon, x^n)| &= 2\sum_{d=0}^{\lfloor n\epsilon\rfloor} \binom{n}{d} \\
&\leq 2e^{nH(\frac{\lfloor n\epsilon\rfloor}{n})} \leq e^{nH(\epsilon)+\ln 2}.
\end{aligned}$$

Now suppose $\hat{x}^n \in B(\epsilon, x^n)$, then $x^n \in B(\epsilon, \hat{x}^n)$, which, according to Algorithm 2, implies that

$$\begin{aligned}
&\Pr\left\{\tilde{x}^n \neq x^n \,|\hat{x}^n \in B(\epsilon, x^n)\right\} \\
= & \ \Pr\left\{\exists z^n \in B(\epsilon, \hat{x}^n)/\{x^n\} : \mathbf{H}''_{\left(n\frac{H(\epsilon)}{\ln 2}+\Delta\right)\times n} z^n = \mathbf{H}''_{\left(n\frac{H(\epsilon)}{\ln 2}+\Delta\right)\times n} x^n\right\} \\
\leq & \ |B(\epsilon, \hat{x}^n)| e^{-nH(\epsilon)+\Delta\ln 2} \\
\leq & \ 2^{-\Delta+O(1)}.
\end{aligned}$$

In summary,

$$\begin{aligned}
P_e\left\{\mathcal{I}_n | x^n, y^n\right\} &\leq \Pr\left\{\tilde{x}^n \neq x^n \,|\hat{x}^n \in B(\epsilon, x^n)\right\} + \Pr\left\{\hat{x}^n \notin B(\epsilon, x^n)\right\} \\
&\leq 2^{-\Delta+O(1)} + 2^{-\Delta+\log_2\left(\frac{n}{\Delta}+1\right)+O(1)} \\
&\leq 2^{-\Delta+\log_2\left(\frac{n}{\Delta}+1\right)+O(1)}.
\end{aligned}$$

The theorem is proved. □

Remark 6.4. *As can be seen, the achievable bounds of coding performance for SA-LDPC-IED schemes in Theorem 6.1 depend only on l_1 and $\bar{l}$, rather than the entire $L(z)$. This property of the results is due to both the bounding technique and the fact that jar decoding is assumed. However, when BP decoding is used as a practical implementation of the decoding algorithm in section 6.5, coding performance will be determined by the entire degree distribution $L(z)$. Optimization of degree distribution for BP decoding is left for future research.*

Remark 6.5. *Readers may be interested in comparing the result above and those of Theorems 1, 3 and 5 in [45] for linear IED schemes with Gallager-type and vector-type ensembles, where the word error probability was considered. However, no fair comparison can be made here. As can be seen, the average degree of ensembles used in Theorem 1, 3 and 5 of [45] is at least on the order of $\ln n$, while the average degree of ensembles used here is finite with respect to block length n.*

In order to analyze the asymptotical performance of the SA-LDPC-IED scheme $\mathcal{I}_n$ first as $n \to \infty$ and then as the average degree $\bar{l}$ of $L(z)$ goes to ∞, we define for any $h \in [0, \ln 2]$

$$R_{L(z)}(\epsilon, h) \triangleq \lim_{n\to\infty} R^{(\Delta)}_{L(z)}(\epsilon, h)$$

and

$$r_{L(z)}(\epsilon, h) \triangleq R_{L(z)}(\epsilon, h) \ln 2 + H(\epsilon) - h.$$

Clearly, $r_{L(z)}(\epsilon, h)$ represents the redundancy of $\mathcal{I}_n$, i.e., the gap between the asymptotical total rate of $\mathcal{I}_n$ and the desired rate h. We have the following two results.

Proposition 6.1. *Let $L(z)$ be a normalized degree distribution with $l_1 \geq 2$ and ϵ be a real number where $\frac{\bar{l}}{l_1 \lfloor \bar{l} \rfloor} \leq \epsilon < 0.5$. Then for any $h \geq 0$,*

$$\begin{aligned} r_{L(z)}(\epsilon, h) \;\leq\; & H(\epsilon) + \left(1 + \mathrm{I}\left(h \geq -P(1, \bar{l}, l_1\epsilon)\right)\right) \\ & \times \left\{ 2l_1\epsilon \exp\left[-\frac{2l_1\epsilon}{\bar{l}} \left(\lfloor \bar{l} \rfloor - 1 \right) \right] + \exp\left(-\frac{2l_1\epsilon}{\bar{l}} \lfloor \bar{l} \rfloor \right) \right\} \end{aligned}$$

where $\mathrm{I}(\cdot)$ is the indicator function such that

$$\mathrm{I}\left(h \geq -P(1, \bar{l}, l_1\epsilon)\right) = \begin{cases} 1 & \text{if } h \geq -P(1, \bar{l}, l_1\epsilon) \\ 0 & \text{otherwise} \end{cases}$$

Proof. In view of Lemma B.5, it follows from the definition of $R_{L(z)}(\epsilon, h)$ that $R_{L(z)}(\epsilon, h)$ is the solution to

$$-P\left(R, \bar{l}, l_1\epsilon\right) = h$$

if $h < -P\left(1, \bar{l}, l_1\epsilon\right)$, and

$$R_{L(z)}(\epsilon, h) = 2 + \frac{1}{\ln 2} P\left(1, \bar{l}, l_1\epsilon\right)$$

otherwise. On the other hand, in view of the fact that $l_1\epsilon \geq \frac{\bar{l}}{\lfloor \bar{l} \rfloor}$ and of Lemma B.4, for $R \in (0, 1]$,

$$\begin{aligned} P\left(R, \bar{l}, l_1\epsilon\right) &\leq -R\ln 2 + 2l_1\epsilon \exp\left[-\frac{2l_1\epsilon}{\bar{l}}\left(c_R r_1 - 1\right)\right] + R\exp\left(-\frac{2l_1\epsilon}{\bar{l}} r_1 c_R\right) \\ &\leq -R\ln 2 + 2l_1\epsilon \exp\left[-\frac{2l_1\epsilon}{\bar{l}}\left(\lfloor \bar{l} \rfloor - 1\right)\right] + \exp\left(-\frac{2l_1\epsilon}{\bar{l}} \lfloor \bar{l} \rfloor\right) \end{aligned}$$

where $c_R \stackrel{\Delta}{=} 2^{-\lceil \log_2 R \rceil} \geq 1$. Now if $h \geq -P\left(1, \bar{l}, l_1\epsilon\right)$, then

$$\begin{aligned} r_{L(z)}(\epsilon, h) &= R_{L(z)}(\epsilon, h)\ln 2 + H(\epsilon) - h \\ &\leq 2\ln 2 + 2P\left(1, \bar{l}, l_1\epsilon\right) + H(\epsilon) \\ &\leq 4l_1\epsilon \exp\left[-\frac{2l_1\epsilon}{\bar{l}}\left(\lfloor \bar{l} \rfloor - 1\right)\right] + 2\exp\left(-\frac{2l_1\epsilon}{\bar{l}} \lfloor \bar{l} \rfloor\right) + H(\epsilon). \end{aligned} \tag{6.20}$$

If $h < -P\left(1, \bar{l}, l_1\epsilon\right)$, then

$$\begin{aligned} h &= -P\left(R_{L(z)}(\epsilon, h), \bar{l}, l_1\epsilon\right) \\ &\geq R_{L(z)}(\epsilon, h)\ln 2 - 2l_1\epsilon \exp\left[-\frac{2l_1\epsilon}{\bar{l}}\left(\lfloor \bar{l} \rfloor - 1\right)\right] - \exp\left(-\frac{2l_1\epsilon}{\bar{l}} \lfloor \bar{l} \rfloor\right) \end{aligned}$$

which implies that

$$R_{L(z)}(\epsilon, h) \leq \frac{h}{\ln 2} + \frac{2l_1\epsilon}{\ln 2} \exp\left[-\frac{2l_1\epsilon}{\bar{l}}\left(\lfloor \bar{l} \rfloor - 1\right)\right] + \frac{1}{\ln 2} \exp\left(-\frac{2l_1\epsilon}{\bar{l}} \lfloor \bar{l} \rfloor\right).$$

Therefore,

$$\begin{aligned} r_{L(z)}(\epsilon, h) &= R_{L(z)}(\epsilon, h)\ln 2 + H(\epsilon) - h \\ &\leq 2l_1\epsilon \exp\left[-\frac{2l_1\epsilon}{\bar{l}}\left(\lfloor \bar{l} \rfloor - 1\right)\right] + \exp\left(-\frac{2l_1\epsilon}{\bar{l}} \lfloor \bar{l} \rfloor\right) + H(\epsilon). \end{aligned} \tag{6.21}$$

Combining (6.20) with (6.21) completes the proof of Proposition 6.1. □

Proposition 6.2. *Let $L(z)$ be a normalized degree distribution with $l_1 \geq 2$. Then*

$$r_{L(z^k)}\left(\frac{\ln k}{2k}, h\right) = O\left(\frac{\ln^2 k}{k}\right)$$

for any $k \geq e^{\frac{2}{l_1}}$ and $h \geq 0$.

Proof. Note that $k \geq e^{\frac{2}{l_1}}$, which implies that

$$kl_1 \frac{\ln k}{k} = l_1 \ln k \geq 2 \geq \frac{k\bar{l}}{\lfloor k\bar{l} \rfloor},$$

and therefore, we can apply Proposition 6.1 on $r_{L(z^k)}\left(\frac{\ln k}{k}, h\right)$, resulting in

$$\begin{aligned} & r_{L(z^k)}\left(\frac{\ln k}{k}, h\right) \\ \leq \;& 4l_1 \ln k \exp\left[-\frac{2l_1\left(\lfloor k\bar{l} \rfloor - 1\right)}{k\bar{l}} \ln k\right] + 2\exp\left(-\frac{2l_1 \lfloor k\bar{l} \rfloor}{k\bar{l}} \ln k\right) + H\left(\frac{\ln k}{k}\right) \end{aligned}$$

It is easily verified that

$$H\left(\frac{\ln k}{k}\right) = O\left(\frac{\ln^2 k}{k}\right).$$

On the other hand,

$$\frac{2l_1 \lfloor k\bar{l} \rfloor}{k\bar{l}} \geq \frac{2l_1\left(\lfloor k\bar{l} \rfloor - 1\right)}{k\bar{l}} \geq \frac{4\left(\lfloor k\bar{l} \rfloor - 1\right)}{k\bar{l}} \geq 1.$$

Therefore,

$$r_{L(z^k)}\left(\frac{\ln k}{k}, h\right) = O\left(\frac{\ln k}{k}\right) + O\left(\frac{1}{k}\right) + O\left(\frac{\ln^2 k}{k}\right) = O\left(\frac{\ln^2 k}{k}\right).$$

□

6.3.3 Performance for Stationary, Ergodic Sources

In this subsection, we analyze the performance of the SA-LDPC-IED scheme $\mathcal{I}_n$ for any stationary, ergodic source-side information pair $(X, Y) = \{(X_i, Y_i)\}_{i=1}^{\infty}$ with alphabet $\mathcal{X} \times$

$\mathcal{Y}$. To this end, we select $\{\mathcal{C}_n\}_{n=1}^{\infty}$ to be a sequence of universal (classical) prefix codes with side information available to both the encoder and decoder such that

$$\lim_{n\to\infty} h_n(X^n|Y^n) = H(X|Y) \quad \text{with probability one} \tag{6.22}$$

for any stationary, ergodic source-side information pair (X, Y). (Note that from the literature of classical universal lossless source coding (see, for example, [8–12], and the references therein), such a sequence exists.) To bring out the dependence of $\mathcal{I}_n$ on $L(z)$ and ϵ, we shall write $\mathcal{I}_n$ as $\mathcal{I}_n(L(z), \epsilon)$. Then we have the following result.

Theorem 6.2. *Let $L(z)$ be a normalized variable node degree distribution. Then for any stationary, ergodic source side information pair (X, Y),*

$$\lim_{k\to\infty}\lim_{n\to\infty} r_f\left(X^n, Y^n \middle| \mathcal{I}_n\left(L(z^k), \frac{\ln k}{2k}\right)\right) = H(X|Y) \quad \textit{with probability one} \tag{6.23}$$

$$r_b\left(X^n, Y^n \middle| \mathcal{I}_n\left(L(z^k), \frac{\ln k}{2k}\right)\right) = O\left(\frac{1}{\sqrt{n}}\right) \tag{6.24}$$

and

$$P_e\left(\mathcal{I}_n\left(L(z^k), \frac{\ln k}{2k}\right)\right) \le 2^{-\Delta+\log_2\left(\frac{n}{\Delta}+1\right)+O(1)} \tag{6.25}$$

whenever $k \ge 9$.

Proof. In view of Theorem 6.1, (6.24) and (6.25) follow immediately. Thus it suffices to prove (6.23). From Theorem 6.1 again, we have

$$r_f\left(X^n, Y^n|\mathcal{I}_n\left(L(z^k), \frac{\ln k}{2k}\right)\right) \le R^{(\Delta)}_{L(z^k)}\left(\frac{\ln k}{2k}, h_n(x^n|y^n)\right)\ln 2 + H\left(\frac{\ln k}{2k}\right) + \frac{2\Delta}{n}\ln 2\,. \tag{6.26}$$

Let $\delta > 0$ be a small number to be specified later. In view of the definition of $R^{(\Delta)}_{L(z)}(\epsilon, h_n(x^n|y^n))$ and Lemma B.5, it is not hard to verify that $R^{(\Delta)}_{L(z)}(\epsilon, h_n(x^n|y^n))$ is non-decreasing as $h_n(x^n|y^n)$ increases. This, coupled with (6.26) and (6.22), implies that with probability one

$$r_f\left(X^n, Y^n|\mathcal{I}_n\left(L(z^k), \frac{\ln k}{2k}\right)\right) \le R^{(\Delta)}_{L(z^k)}\left(\frac{\ln k}{2k}, H(X|Y)+\delta\right)\ln 2 + H\left(\frac{\ln k}{2k}\right) + \frac{2\Delta}{n}\ln 2 \tag{6.27}$$

for sufficiently large n. Applying Propositions 6.1 and 6.2 to (6.27), we have

$$\begin{aligned}\limsup_{n\to\infty} r_f\left(X^n, Y^n | \mathcal{I}_n\left(L(z^k), \frac{\ln k}{2k}\right)\right) &\leq H(X|Y) + \delta + r_{L(z^k)}\left(\frac{\ln k}{2k}, H(X|Y)+\delta\right) \\ &= H(X|Y) + \delta + O\left(\frac{\ln^2 k}{k}\right) \qquad (6.28)\end{aligned}$$

with probability one. Letting $\delta \to 0$ and then $k \to \infty$ in (6.28) yields

$$\limsup_{k\to\infty} \limsup_{n\to\infty} r_f\left(X^n, Y^n \middle| \mathcal{I}_n\left(L(z^k), \frac{\ln k}{2k}\right)\right) \leq H(X|Y)$$

with probability one. This, coupled with the converse [41, Theorem 3], implies (6.23). This competes the proof of Theorem 6.2. □

Remark 6.6. *It is easy to verify that for any stationary ergodic source-side information pair (X, Y), $H(X|Y)$ is the optimal compression rate for IED schemes, which has been proved in [41]. This is expected as even if the side information is fully available to the encoder, the best compression rate is still $H(X|Y)$.*

Remark 6.7. *As can be seen from Theorem 6.2, to approach the optimum $H(X|Y)$, $L(z^k)$ for large k has to be used for the degree distribution of LDPC ensembles. In fact, by utilizing some converse theorems on the average degree of capacity-achieving LDPC ensembles in channel coding, e.g. Theorem 3.94 in Section 3.16 of [5], it can be shown that the average degree of LDPC ensembles has to approach infinity in order to allow SA-LDPC-IED schemes to achieve the optimal compression rate $H(X|Y)$. However, it is worthing pointing out that the result of Theorem 6.2 is doubly asymptotic, in the sense the compression rate take its limit with respect to block length n first, and then with respect to k which controls the average degree of LDPC ensembles. Therefore, k (and consequently, the average degree of LDPC ensembles) is always assumed to be finite with respect to n, implying the low density of ensembles. Readers are directed to [45] for the case when the average degree of ensembles grows with respect to n.*

6.4 Performance of SA-LDPC-IED: Binary Case and Bit Error Probability

Theorems 6.1 and 6.2 show the performance of our proposed SA-LDPC-IED scheme $\mathcal{I}_n$ in terms of the forward and backward rates versus the word error probability for both individual sequences x^n and y^n and stationary, ergodic sources. In this section, we consider instead

the forward and backward rates versus the bit error probability by focusing on independent and identically distributed (i.i.d) source-side information pairs $(X, Y) = \{(X_i, Y_i)\}_{i=1}^{\infty}$, where the source X and side-information Y are correlated through a BSC with cross-over probability $p_0 \in (0, 0.5)$, which is unknown to either the decoder or encoder. Limiting ourselves to this smaller class of source-side information pairs allows us to illustrate the SA-LDPC-IED scheme $\mathcal{I}_n$ by using a specific and simple function $\gamma(\cdot, \cdot)$, which in turn leads to further simplification of the SA-LDPC-IED scheme $\mathcal{I}_n$ itself and paves the way for BP decoding to be used as a decoding method in IED in the next section.

Note that in this binary case

$$H(X|Y) = H(p_0) \, .$$

Now specify $\gamma(\cdot, \cdot)$ as

$$\gamma(x^n, y^n) = \begin{cases} \frac{\ln n + \ln 2}{n} + H\left(\frac{1}{n} wt(x^n - y^n)\right) & \text{if } \frac{1}{n} wt(x^n - y^n) \leq 0.5 \\ \frac{1}{n} \ln 2 + \ln 2 & \text{otherwise.} \end{cases} \tag{6.29}$$

It is easy to see that $\gamma(x^n, y^n)$ is actually the normalized code length function of the classical prefix code $\mathcal{C}_n$ with side information available to both the encoder and decoder as described in Algorithm 3. With the assumption on the correlation between the source X and side information Y and with this specific function $\gamma(\cdot, \cdot)$, we can further get rid of the last round of transmission from the encoder to the decoder in $\mathcal{I}_n$, yielding a simplified version $\tilde{\mathcal{I}}_n$ as described in Algorithm 4, where the specification of η_n and $\{\Gamma_b\}$ is the same as that in Algorithm 2.

Algorithm 3 A classical prefix code $\mathcal{C}_n$ with side information available to both the encoder and decoder

1: The encoder calculates $w = wt(x^n - y^n)$.
2: **if** $w \leq 0.5n$ **then**
3: The encoder sends bit 0 followed by a codeword of fixed-length $\log_2 n$ specifying w and then by a codeword of length $n\frac{H\left(\frac{w}{n}\right)}{\ln 2}$ specifying the index of $x^n - y^n$ in the set $\{z^n : wt(z^n) = w\}$ sorted by the lexicographical order.
4: **else**
5: The encoder sends bit 1 followed by x^n itself.
6: **end if**

Now let us analyze the performance of the SA-LDPC-IED scheme $\tilde{\mathcal{I}}_n$ in terms of the forward and backward rates versus the bit error probability P_b, where

$$P_b \triangleq \frac{1}{n} \mathbb{E}\left[wt(\hat{X}^n - X^n)\right] .$$

Algorithm 4 SA-LDPC-IED scheme $\tilde{\mathcal{I}}_n$ for i.i.d source-side information pairs

Based on $\mathcal{P}_1\mathcal{P}_2\cdots\mathcal{P}_n$ and $s^n = \mathbf{H}_{n\times n}x^n$, the encoder generates accumulated syndromes $\tilde{s}_1\tilde{s}_2\cdots\tilde{s}_n$ and augmenting syndromes $a_1a_2\cdots a_n$.

Based on $\mathcal{P}_1\mathcal{P}_2\cdots\mathcal{P}_n$ and $\mathbf{H}_{n\times n}$, the decoder calculates matrices $\mathbf{H}^{(\Delta)}_{\Delta\times n}\mathbf{H}^{(2\Delta)}_{2\Delta\times n}\cdots\mathbf{H}^{(n)}_{n\times n}$.

$b \leftarrow 0$.

while The encoder does not receive bit 1 from the decoder **do**

  $b \leftarrow b+1$.

  if $b \leq \frac{n}{\Delta}$ **then**

    The encoder sends augmenting syndromes $a_{(b-1)\Delta+1}\cdots a_{b\Delta}$ to the decoder by Δ bits.

  else

    The encoder sends syndromes $s'_{\eta_n n} = \mathbf{H'}_{\eta_n n\times n}x^n$ to the decoder by $\eta_n n$ bits.

  end if

  Upon receiving syndromes sent from the encoder, the decoder searches through $J_b(y^n)$ for a sequence $\hat{x}^n$ satisfying $\mathbf{H}^{(b\Delta)}_{b\Delta\times n}\hat{x}^n = \tilde{s}_{b\Delta}$ if $b \leq \frac{n}{\Delta}$ and

$$\begin{bmatrix} \mathbf{H}^{(n)}_{n\times n} \\ \mathbf{H'}_{\eta_n n\times n} \end{bmatrix}\hat{x}^n = \begin{bmatrix} \tilde{s}_n \\ s'_{\eta_n n} \end{bmatrix}$$

  otherwise.

  if Such an $\hat{x}^n$ is found **then**

    The decoder sends bit 1 to the encoder, and outputs $\hat{x}^n$ as the estimate of x^n.

  else

    The decoder sends bit 0 to the encoder and leaves the estimate of x^n undecided.

  end if

end while

Then we have the following theorem.

Theorem 6.3. *Let $L(z)$ be a normalized variable node degree distribution from a node perspective with minimum degree $l_1 \geq 2$ and average degree $\bar{l}$ being an odd integer. Select $\epsilon > 0$ such that $\epsilon \leq 0.5 - H^{-1}(0.75 \ln 2)$. Then for any i.i.d source-side information pair (X, Y) correlated through a BSC with cross-over probability $p_0 \in (0, 0.5)$ and for sufficiently large n,*

$$\begin{aligned} r_f(\tilde{\mathcal{I}}_n) \quad \leq \quad & R^{(\Delta)}_{L(z)}\left(\epsilon, H(p_0) + \frac{\ln n + \ln 2}{n} + \ln\left(\frac{1-p_0}{p_0}\right)\sqrt{\frac{\ln n}{n}}\right)\ln 2 \\ & + \left[n^{-2} R^{(\Delta)}_{L(z)}(\epsilon, \ln 2) + \frac{\Delta}{n}\right]\ln 2 \end{aligned} \tag{6.30}$$

$$r_b(\tilde{\mathcal{I}}_n) = O\left(\frac{1}{\sqrt{n}}\right) \tag{6.31}$$

and

$$P_b(\tilde{\mathcal{I}}_n) \leq \epsilon + e^{-2n(0.5-p_0)^2} + 2^{-\Delta + \log_2\left(\frac{n}{\Delta}+1\right)+O(1)}\ . \tag{6.32}$$

Proof. In view of Theorem 6.1, it suffices to prove (6.30) and (6.32). Note that from the proof of Theorem 6.1 and the description of Algorithm 4, it can be seen that for any sequence of source-side information pairs (X^n, Y^n),

$$\begin{aligned} r_f\left(X^n, Y^n | \tilde{\mathcal{I}}_n\right) \leq & \frac{\Delta}{n}\ln 2 \\ & + \ln 2 \begin{cases} R^{(\Delta)}_{L(z)}\left(\epsilon, H\left(\frac{1}{n}wt(X^n - Y^n) + \frac{\ln n + \ln 2}{n}\right)\right) & \text{if } wt(X^n - Y^n) \leq 0.5n \\ R^{(\Delta)}_{L(z)}\left(\epsilon, \ln 2\right) & \text{otherwise.} \end{cases} \end{aligned}$$

For convenience, let $E_{p_0}(X, Y)$ denote the event $\frac{1}{n}wt\left(X^n - Y^n\right) \leq p_0 + \sqrt{\frac{\ln n}{n}}$ and $E^c_{p_0}(X, Y)$ be the complement event of $E_{p_0}(X, Y)$. Therefore,

$$\begin{aligned} r_f(\tilde{\mathcal{I}}_n) \quad \leq \quad & \frac{\Delta}{n}\ln 2 + \Pr\left\{E_{p_0}(X, Y)\right\} \\ & \times \mathbb{E}\left[R^{(\Delta)}_{L(z)}\left(\epsilon, H\left(\frac{1}{n}wt(X^n - Y^n)\right) + \frac{\ln n + \ln 2}{n}\right)\middle| E_{p_0}(X, Y)\right]\ln 2 \\ & + \Pr\left\{E^c_{p_0}(X, Y)\right\} R^{(\Delta)}_{L(z)}(\epsilon, \ln 2)\ln 2 \end{aligned}$$

where we assume that

$$p_0 < 0.5 - \sqrt{\frac{\ln n}{n}}$$

which always holds for sufficiently large n as $p_0 < 0.5$. On one hand, given

$$\frac{1}{n} wt\left(X^n - Y^n\right) \leq p_0 + \sqrt{\frac{\ln n}{n}} < 0.5$$

we have

$$\begin{aligned} H\left(\frac{1}{n} wt(X^n - Y^n)\right) &\leq H\left(p_0 + \sqrt{\frac{\ln n}{n}}\right) \\ &\leq H(p_0) + \ln\left(\frac{1-p_0}{p_0}\right)\sqrt{\frac{\ln n}{n}} \end{aligned}$$

which further implies that

$$\begin{aligned} &\mathbb{E}\left[R^{(\Delta)}_{L(z)}\left(\epsilon, H\left(\frac{1}{n} wt(X^n - Y^n)\right) + \frac{\ln n + \ln 2}{n}\right)\middle| E_{p_0}(X,Y)\right] \\ &\leq R^{(\Delta)}_{L(z)}\left(\epsilon, H\left(p_0\right) + \frac{\ln n + \ln 2}{n} + \ln\left(\frac{1-p_0}{p_0}\right)\sqrt{\frac{\ln n}{n}}\right) . \end{aligned}$$

On the other hand, by Hoeffding's inequality,

$$\Pr\{E_{p_0}(X,Y)\} = \Pr\left\{\frac{1}{n} wt\left(X^n - Y^n\right) > p_0 + \sqrt{\frac{\ln n}{n}}\right\} \leq n^{-2}$$

from which (6.30) is proved.

Towards showing (6.32), we have

$$\begin{aligned}
P_b(\tilde{\mathcal{I}}_n) &= \mathbb{E}\left[\frac{1}{n}wt(\hat{X}^n - X^n)\right] \\
&= \mathbb{E}\left[\mathbb{E}\left[\frac{1}{n}wt(\hat{X}^n - X^n)\middle| X^n, Y^n\right]\right] \\
&= \sum_{(x^n,y^n):\frac{1}{n}wt(x^n-y^n)\leq 0.5} \Pr\{X^n = x^n, Y^n = y^n\}\,\mathbb{E}\left[\frac{1}{n}wt(\hat{X}^n - x^n)\middle| x^n, y^n\right] \\
&\quad + \sum_{(x^n,y^n):\frac{1}{n}wt(x^n-y^n)>0.5} \Pr\{X^n = x^n, Y^n = y^n\}\,\mathbb{E}\left[\frac{1}{n}wt(\hat{X}^n - x^n)\middle| x^n, y^n\right] \\
&\leq \sum_{(x^n,y^n):\frac{1}{n}wt(x^n-y^n)\leq 0.5} \Pr\{X^n = x^n, Y^n = y^n\}\,\mathbb{E}\left[\frac{1}{n}wt(\hat{X}^n - x^n)\middle| x^n, y^n\right] \\
&\quad + \Pr\left\{\frac{1}{n}wt(X^n - Y^n) > 0.5\right\}. \qquad (6.33)
\end{aligned}$$

By Hoeffding's inequality,

$$\Pr\left\{\frac{1}{n}wt(X^n - Y^n) > 0.5\right\} \leq e^{-2n(0.5-p_0)^2}. \qquad (6.34)$$

On the other hand,

$$\begin{aligned}
&\mathbb{E}\left[\frac{1}{n}wt(\hat{X}^n - x^n)\middle| x^n, y^n\right] \\
= \;& \Pr\left\{\frac{1}{n}wt(\hat{X}^n - x^n) \leq \epsilon\middle| x^n, y^n\right\}\mathbb{E}\left[\frac{1}{n}wt(\hat{X}^n - x^n)\middle| \frac{1}{n}wt(\hat{X}^n - x^n) \leq \epsilon, x^n, y^n\right] \\
&+ \Pr\left\{\frac{1}{n}wt(\hat{X}^n - x^n) > \epsilon\middle| x^n, y^n\right\}\mathbb{E}\left[\frac{1}{n}wt(\hat{X}^n - x^n)\middle| \frac{1}{n}wt(\hat{X}^n - x^n) > \epsilon, x^n, y^n\right] \\
\leq \;& \epsilon + \Pr\left\{\frac{1}{n}wt(\hat{X}^n - x^n) > \epsilon\middle| x^n, y^n\right\}. \qquad (6.35)
\end{aligned}$$

Now we would like to bound

$$\Pr\left\{\frac{1}{n}wt(\hat{X}^n - x^n) > \epsilon\middle| x^n, y^n\right\}$$

when $\frac{1}{n}wt(x^n - y^n) \le 0.5$. By the argument in the proof of Theorem 6.1,

$$\begin{aligned}
&\Pr\left\{\frac{1}{n}wt(\hat{X}^n - x^n) > \epsilon \middle| x^n, y^n\right\} \\
&\le \Pr\left\{\exists \hat{x}^n \exists b, \frac{1}{n}wt(\hat{x}^n - x^n) > \epsilon, \mathbf{H}^{(b\Delta)}_{b\Delta\times n}(\hat{x}^n - x^n) = 0^{b\Delta}, \hat{x}^n \in J_b(y^n)\right\} \\
&\quad + \Pr\left\{\exists \hat{x}^n, \frac{1}{n}wt(\hat{x}^n - x^n) > \epsilon, \mathbf{H}_{n\times n}(\hat{x}^n - x^n) = 0^n, \mathbf{H}'_{\eta_n n\times n}(\hat{x}^n - x^n) = 0^{\eta_n n}\right\} \\
&\le \sum_{b=1}^{\lfloor \frac{0.75n}{\Delta}\rfloor} \Pr\left\{\exists \hat{x}^n, \frac{1}{n}wt(\hat{x}^n - x^n) > \epsilon, \mathbf{H}^{(b\Delta)}_{b\Delta\times n}(\hat{x}^n - x^n) = 0^{b\Delta}, \hat{x}^n \in J_b(y^n)\right\} \\
&\quad + \sum_{b=\lfloor \frac{0.75n}{\Delta}\rfloor+1}^{\frac{n}{\Delta}} \Pr\left\{\exists \hat{x}^n, \frac{1}{n}wt(\hat{x}^n - x^n) > \epsilon, \mathbf{H}^{(b\Delta)}_{b\Delta\times n}(\hat{x}^n - x^n) = 0^{b\Delta}, \hat{x}^n \in J_b(y^n)\right\} \\
&\quad + \Pr\left\{\exists \hat{x}^n, \frac{1}{n}wt(\hat{x}^n - x^n) > \epsilon, \mathbf{H}_{n\times n}(\hat{x}^n - x^n) = 0^n, \mathbf{H}'_{\eta_n n\times n}(\hat{x}^n - x^n) = 0^{\eta_n n}\right\}.
\end{aligned} \tag{6.36}$$

For $1 \le b \le \lfloor \frac{0.75n}{\Delta}\rfloor$, $\frac{b\Delta}{n} \le 0.75$ and therefore,

$$\gamma(\hat{x}^n, y^n) \le \Gamma_b \le \frac{b\Delta}{n}\ln 2 \le 0.75 \ln 2$$

which, together with (6.29), further implies that

$$\frac{1}{n}wt(\hat{x}^n - y^n) < H^{-1}(0.75\ln 2)$$

and

$$\begin{aligned}
\frac{1}{n}wt(\hat{x}^n - x^n) &\le \frac{1}{n}wt(x^n - y^n) + \frac{1}{n}wt(\hat{x}^n - y^n) \\
&< 0.5 + H^{-1}(0.75\ln 2) \\
&\le 1 - \epsilon
\end{aligned}$$

since $\epsilon \le 0.5 - H^{-1}(0.75\ln 2)$. Consequently, we have for any $1 \le b \le \lfloor \frac{0.75n}{\Delta}\rfloor$

$$\begin{aligned}
&\Pr\left\{\exists \hat{x}^n, \frac{1}{n}wt(\hat{x}^n - x^n) > \epsilon, \mathbf{H}^{(b\Delta)}_{b\Delta\times n}(\hat{x}^n - x^n) = 0^{b\Delta}, \hat{x}^n \in J_b(y^n)\right\} \\
&= \Pr\left\{\exists \hat{x}^n, \epsilon < \frac{1}{n}wt(\hat{x}^n - x^n) < 1 - \epsilon, \mathbf{H}^{(b\Delta)}_{b\Delta\times n}(\hat{x}^n - x^n) = 0^{b\Delta}, \hat{x}^n \in J_b(y^n)\right\} \\
&\le 2^{-\Delta + O(1)}
\end{aligned} \tag{6.37}$$

where the inequality above has been proved in the proof of Theorem 6.1. For $b \geq \lfloor \frac{0.75n}{\Delta} \rfloor + 1$, by Lemmas B.2 and B.6, $P\left(\frac{b\Delta}{n}, \bar{l}, \xi\right)$ is a strictly decreasing function of ξ in the range $\left(0, \bar{l} - \frac{t_{b\Delta}^{(1)}}{n}\right]$. In view of this, it can be shown by the same technique as in proof of Theorem 6.1 that for any $b \geq \lfloor \frac{0.75n}{\Delta} \rfloor + 1$

$$\Pr\left\{\exists \hat{x}^n, \frac{1}{n} wt(\hat{x}^n - x^n) > \epsilon, \mathbf{H}_{b\Delta \times n}^{(b\Delta)}(\hat{x}^n - x^n) = 0^{b\Delta}, \hat{x}^n \in J_b(y^n)\right\} \leq 2^{-\Delta + O(1)} \tag{6.38}$$

and

$$\Pr\left\{\exists \hat{x}^n, \frac{1}{n} wt(\hat{x}^n - x^n) > \epsilon, \mathbf{H}_{n \times n}(\hat{x}^n - x^n) = 0^n, \mathbf{H}'_{\eta_n n \times n}(\hat{x}^n - x^n) = 0^{\eta_n n}\right\} \leq 2^{-\Delta + O(1)}. \tag{6.39}$$

Plugging (6.37), (6.38), and (6.39) into (6.36) yields

$$\Pr\left\{\frac{1}{n} wt(\hat{X}^n - x^n) > \epsilon \middle| x^n, y^n\right\} \leq 2^{-\Delta + \log_2\left(\frac{n}{\Delta} + 1\right) + O(1)} \tag{6.40}$$

for any (x^n, y^n) with $\frac{1}{n} wt(x^n - y^n) \leq 0.5$. This, combined with (6.35), (6.34), and (6.33), implies

$$P_b(\tilde{\mathcal{I}}_n) \leq \epsilon + 2^{-\Delta + \log_2\left(\frac{n}{\Delta} + 1\right) + O(1)} + e^{-2n(0.5 - p_0)^2}$$

which completes the proof of (6.32) and hence of Theorem 6.3. □

Remark 6.8. *From the proof of Theorem 6.3, it can be seen that the error event is broken down to two cases, i.e.*

- $\exists \hat{X}^n : wt(\hat{X}^n - X^n) \leq \epsilon n$ *such that parity check and threshold on cost function* γ *are satisfied;*
- $\exists \hat{X}^n : wt(\hat{X}^n - X^n) > \epsilon n$ *such that parity check and threshold on cost function* γ *are satisfied.*

Then the probability of the second type of error is tightly bounded by

$$e^{-2n(0.5 - p_0)^2} + 2^{-\Delta + \log_2\left(\frac{n}{\Delta} + 1\right) + O(1)}.$$

However, the probability of the first type of error is trivially bounded by 1*. Therefore, further refinement of Theorem 6.3 is possible. Specifically, to improve the result of Theorem 6.3,*

minimum hamming distance analysis of the code with parity check matrix $\mathbf{H}_{b\Delta\times n}^{(b\Delta)}$ *can be applied at the b-th round of interaction for* $1 \leq b \leq \frac{n}{\Delta}$. *Let* $d_{\min}^{(b)}$ *denote the minimum hamming distance at the b-th interaction. As long as we choose* $\epsilon n \leq d_{\min}^{(b)}$, *the first type of error will not happen at the b-th interaction. Consequently, a relatively large value of* ϵ *can be used to calculate the achievable compression rate in* (6.30) *while the error probability can be still tightly bounded, especially for some large* $d_{\min}^{(b)}$ *when b is large. However,* $d_{\min}^{(b)}$ *does not have a simple analytic form in general, and applying minimum distance analysis would result in a much more complicated expression which would not allow the following discussion of redundancy, i.e. the gap between the achievable rate and* $H(X|Y)$. *Moreover, as shown below, this refined analysis will not affect the coding performance too much for ensembles of large average degrees.*

Remark 6.9. *It would be interesting to compare the performance of SA-LDPC-IED schemes given in Theorem 6.3 and those of LIED schemes with Gallager-type ensembles and SA-IED schemes with vector-type ensembles in Theorems 4 and 6 in [45] respectively, where the symbol error probability is considered. To make a fair comparison, however, some details on these three kinds of IED schemes need to be addressed. In particular, as shown in Remark 6.1, given a source* x^n *and a side-information* y^n, *decoders in all three kinds of schemes either directly receive or calculate* $\tilde{s}_{b\Delta} = \mathbf{H}_{b\Delta\times n}^{(b\Delta)} x^n$, *and try to estimate* x^n *based on* $\tilde{s}_{b\Delta}$ *and* y^n. *The main difference is how* $\mathbf{H}_{b\Delta\times n}^{(b\Delta)}$ *is generated. Further inspection on ensembles reveal that: 1) for an SA-IED scheme using a vector-type ensemble, the number of ones in* $\mathbf{H}_{b\Delta\times n}^{(b\Delta)}$ *does not change with respect to b, whose expectation equals to* $\Delta n \left(\frac{n}{\Delta}+1\right) p_n^* = (n+\Delta) n p_n^*$, *where* p_n^* *is a parameter in the vector-type ensemble to control its density; 2) for an SA-LDPC-IED scheme,* $\mathbf{H}_{b\Delta\times n}^{(b\Delta)}$ *for any* $1 \leq b \leq \frac{n}{\Delta}$ *will have roughly the same number of ones as* $\mathbf{H}_{n\times n}$, *i.e.* $n\bar{l}$; *3) for an LIED scheme using a Gallager-type ensemble,* $\mathbf{H}_{b\Delta\times n}^{(b\Delta)}$ *will have* $nb\Delta p_n^*$ *expected number of ones, which changes with respect to b and is bounded by* $n^2 p_n^*$ *for* $1 \leq b \leq \frac{n}{\Delta}$, *where* p_n^* *is a parameter in the Gallager-type ensemble to control its density. For the sake of a fair comparison, we can set* $\bar{l} = np_n^*$ *when comparing SA-LDPC-IED schemes with LIED schemes, and* $\bar{l} = (n+\Delta)p_n^*$ *when comparing SA-LDPC-IED schemes with SA-IED schemes. (The comparison between LIED schemes and SA-IED schemes is included in [45].) Let r be the redundancy, i.e. the gap between the achievable rate of (LIED, SA-IED and SA-LDPC-IED) schemes and the conditional entropy rate. By the lower bounds on* p_n^* *in Theorem 4 and 6 in [45], it is not hard to see for LIED and SA-IED schemes,*

$$r = O\left(\frac{1}{\epsilon\bar{l}}\right) + o_n(1)$$

where ϵ is the symbol error probability, and $o_n(1) \to 0$ as $n \to +\infty$. In the meantime, by Proposition 6.1, it can be shown that for SA-LDPC-IED schemes

$$r = O(l_1 \epsilon e^{-2l_1\epsilon}) + o_n(1).$$

From the calculation, it can be seen that given any ϵ, $r \to 0$ as $n \to +\infty$, $\bar{l} \to +\infty$ and $l_1 \to +\infty$ for LIED, SA-IED and SA-LDPC-IED schemes respectively. Moreover, r of SA-LDPC-IED schemes approaches 0 faster than those of LIED and SA-IED schemes assuming that l_1 and $\bar{l}$ approach infinity in the same speed.

By defining

$$\tilde{r}_{L(z)}(\epsilon, p_0) \stackrel{\Delta}{=} R_{L(z)}\left(\epsilon, H(p_0)\right) \ln 2 - H(p_0)$$

we have the following proposition, the proof of which is omitted due to its similarity to that of Proposition 6.2.

Proposition 6.3. *Let $L(z)$ be a normalized degree distribution with $l_1 \geq 2$ and $k \geq 2$. For $p_0 \in (0, 0.5)$,*

$$\tilde{r}_{L(z^k)}\left(\frac{1}{2\sqrt{k}}, p_0\right) = O\left(e^{-\sqrt{k}+\frac{1}{2}\ln k}\right).$$

We conclude this section by providing the following theorem, which analyzes the performance of the modified SA-LDPC-IED scheme $\tilde{\mathcal{I}}_n$ when $L(z^k)$ is used. Once again, to bring out the dependence of $\tilde{\mathcal{I}}_n$ on $(L(z), \epsilon)$, we write $\tilde{\mathcal{I}}_n$ as $\tilde{\mathcal{I}}_n(L(z), \epsilon)$.

Theorem 6.4. *Let $L(z)$ be a normalized variable node degree distribution with minimum degree $l_1 \geq 2$. For any i.i.d source-side information pair (X, Y) correlated through a binary symmetric channel with cross-over probability $p_0 \in (0, 0.5)$,*

$$\lim_{k\to\infty}\lim_{n\to\infty} r_f\left(\tilde{\mathcal{I}}_n\left(L(z^k), \frac{1}{2\sqrt{k}}\right)\right) = H(p_0) \tag{6.41}$$

$$r_b\left(\tilde{\mathcal{I}}_n\left(L(z^k), \frac{1}{2\sqrt{k}}\right)\right) = O\left(\frac{1}{\sqrt{n}}\right) \tag{6.42}$$

and

$$P_b\left(\tilde{\mathcal{I}}_n\left(L(z^k), \frac{1}{2\sqrt{k}}\right)\right) \leq \frac{1}{2\sqrt{k}} + e^{-2n\left(0.5-\frac{1}{4\sqrt{k}}-\frac{1}{2\sqrt{n}}-p_0\right)^2} + 2^{-\Delta+\log_2\left(\frac{n}{\Delta}+1\right)+O(1)} \tag{6.43}$$

whenever $k > \left(\frac{1}{2(1-2p_0-n^{-0.5})}\right)^2$.

Proof. Note that (6.30) applies to any value of $\bar{l}$, since its proof does not rely on the condition that $\bar{l}$ be an odd integer. Then by using Proposition 6.3 and following the same approach as that in the proof of Theorem 6.2, (6.41) is proved, while (6.42) is obvious.

What remains is to prove (6.43). To this end, let $\epsilon = \frac{1}{2\sqrt{k}}$. Then $p_0 < \frac{1-\epsilon-n^{-0.5}}{2}$ as $k > \left(\frac{1}{2(1-2p_0-n^{-0.5})}\right)^2$. By the same argument as in the proof of Theorem 6.3 ,

$$\begin{aligned} P_b(\tilde{\mathcal{I}}_n) &= \mathbb{E}\left[\frac{1}{n}wt(\hat{X}^n - X^n)\right] \\ &\leq \sum_{(x^n,y^n):\frac{1}{n}wt(x^n-y^n)\leq\frac{1-\epsilon-n^{-0.5}}{2}} \Pr\{X^n = x^n, Y^n = y^n\}\,\mathbb{E}\left[\frac{1}{n}wt(\hat{X}^n - x^n)\middle| x^n, y^n\right] \\ &\quad + \Pr\left\{\frac{1}{n}wt(X^n - Y^n) > \frac{1-\epsilon-n^{-0.5}}{2}\right\} \end{aligned}$$

and

$$\mathbb{E}\left[\frac{1}{n}wt(\hat{X}^n - x^n)\middle| x^n, y^n\right] \leq \epsilon + \Pr\left\{\frac{1}{n}wt(\hat{X}^n - x^n) > \epsilon\middle| x^n, y^n\right\}$$

given $\frac{1}{n}wt(x^n - y^n) \leq \frac{1-\epsilon-n^{-0.5}}{2}$. At the same time, by the decoding procedure of Algorithm 4,

$$\begin{aligned} \gamma(\hat{X}^n, y^n) &\leq \Gamma_{j^*} \\ &= \Gamma_{j^*-1} + (\Gamma_{j^*} - \Gamma_{j^*-1}) \\ &\leq \gamma(X^n, y^n) + \frac{\Delta}{n}\ln 2 \end{aligned}$$

where j^* is the round of interaction at which the decoder terminates, and the result of Lemma B.5 is utilized to bound $\Gamma_{j^*} - \Gamma_{j^*-1}$ by $\frac{\Delta}{n}\ln 2$, and therefore

$$\frac{1}{n}wt(\hat{X}^n - y^n) \leq \frac{1}{n}wt(x^n - y^n) + \frac{\Delta}{n} = \frac{1}{n}wt(x^n - y^n) + n^{-0.5}$$

which further implies that

$$\frac{1}{n}wt(\hat{X}^n - x^n) \leq \frac{1}{n}wt(\hat{X}^n - y^n) + \frac{1}{n}wt(x^n - y^n) \leq 1 - \epsilon.$$

Consequently, for any (x^n, y^n) with $\frac{1}{n}wt(x^n - y^n) \leq \frac{1-\epsilon}{2}$,

$$\begin{aligned} \Pr\left\{\frac{1}{n}wt(\hat{X}^n - x^n) > \epsilon\middle| x^n, y^n\right\} &= \Pr\left\{\epsilon < \frac{1}{n}wt(\hat{X}^n - x^n) \leq 1 - \epsilon\middle| x^n, y^n\right\} \\ &\leq 2^{-\Delta+\log_2\left(\frac{n}{\Delta}+1\right)+O(1)} \end{aligned}$$

where the last inequality has been proved in the proof Theorem 6.1. The inequality (6.43) now follows from the fact that

$$\Pr\left\{\frac{1}{n}wt(X^n - Y^n) > \frac{1-\epsilon-n^{-0.5}}{2}\right\} \leq e^{-2n\left(\frac{1-\epsilon-n^{-0.5}}{2}-p_0\right)^2} = e^{-2n\left(0.5-\frac{1}{4\sqrt{k}}-\frac{1}{2\sqrt{n}}-p_0\right)^2}.$$

This completes the proof of Theorem 6.4. □

6.5 Implementation and Simulation Results

To verify our theoretical analysis in the last two sections, we have implemented our proposed SA-LDPC-IED schemes with some modification, namely by adopting the BP decoding in the place of the minimum coding length. In this section, we report their performance for binary source-side information pairs (X, Y), where X and Y are correlated through a binary channel with probability transition matrix (from Y to X) given by

$$\begin{pmatrix} 1-p_1 & p_2 \\ p_1 & 1-p_2 \end{pmatrix}$$

and where $p_1, p_2 \in (0, 0.5]$ are assumed unknown to either the encoder or decoder. Our strategy towards design of practical SA-LDPC-IED schemes is to start with the special case $p_1 = p_2$, i.e. source and side information are correlated through a binary symmetric channel. In this case, the assumption on source-side information pair is the same as that in section 6.4, and therefore, we can modify Algorithm 4 into a practical version, coupled with BP decoding. Later on, this practical algorithm will be generalized to deal with the case $p_1 \neq p_2$. Consequently, we adopt the same notations of γ_n, $\{\Gamma_b\}$ and η_n as in section 6.4. However, replacing jar decoding in Algorithm 4 with standard BP decoding does not work well, since the standard BP decoding algorithm applies only to fix-rate LDPC codes with known statistics of source-side information pairs. Therefore we first have to modify the BP decoding algorithm so that it fits into our variable-rate and unknown statistics situation as well while maintaining its low complexity.

6.5.1 Modified BP Decoding Algorithm and Practical Implementation of SA-LDPC-IED Schemes

The BP decoding algorithm can be considered as a sum-product algorithm [55] on a Tanner graph, which represents the parity check matrix of the LDPC code, with variable nodes

corresponding to bits of the source, and check nodes corresponding to syndromes. Generally speaking, it tries to marginalize the distribution of each bit of the source based on local calculations. Specifically, it iteratively calculates messages from variable nodes to their connected check nodes, and vice versa, i.e.

$$m_{v_i \to c_j} = \log \frac{\Pr\{X_i = 0|Y_i\}}{\Pr\{X_i = 1|Y_i\}} + \sum_{c_k \neq c_j : c_k \text{ is connected to } v_i} m_{c_k \to v_i} \tag{6.44}$$

$$m_{c_j \to v_i} = 2 \tanh^{-1}(1 - 2s_j) \prod_{v_k \neq v_i : v_k \text{ is connected to } c_j} \tanh\left(\frac{m_{v_k \to c_j}}{2}\right) \tag{6.45}$$

where $m_{v_i \to c_j}$ and $m_{c_j \to v_i}$ are messages passed from the variable node v_i to the check node c_j and vice versa, respectively, and s_j is the syndrome corresponding to c_j. After certain iterations, assuming the calculation converges to a stationary point, the marginal distribution of each variable node is calculated based on the messages sent from its connected check nodes, and the decision on each bit is made according to the distribution in the following way

$$\hat{x}_i = \begin{cases} 0 & \text{if } \frac{\Pr\{X_i=0|Y_i\}}{\Pr\{X_i=1|Y_i\}} + \sum_{c_k : c_k \text{ is connected to } v_i} m_{c_k \to v_i} \geq 0 \\ 1 & \text{otherwise.} \end{cases} \tag{6.46}$$

To initialize the iterative procedure, for each variable node X_i, the marginal distribution is assumed to be $(\Pr\{X_i = 0|Y_i\}, \Pr\{X_i = 1|Y_i\})$. Therefore, the standard BP decoding algorithm needs the statistics of source and side information as inputs.

However, in our case, the statistics of source-side information are unavailable, i.e., p_1 and p_2 are unknown. To deal with this problem, let us first consider the case $p_1 = p_2 = p_0$, i.e. X and Y are correlated through a BSC. Now let

$$p_b = H^{-1}\left(\max\left\{0, \Gamma_b - \frac{\ln n + \ln 2}{n}\right\}\right) \tag{6.47}$$

where p_b can be interpreted as the maximum cross-over probability of the BSC correlating X and Y, such that the error probability of the SA-LDPC-IED scheme $\tilde{\mathcal{I}}_n$ can be maintained asymptotically zero at the b-th interaction. Therefore, we will use p_b as the input to the BP decoding at the b-th interaction. Moreover, at each interaction, decoding failure is detected and the decoder will send bit 0 to the encoder for more syndromes if one of the following two situations occurs:

- the number of bits with significant log-likelihood (larger than certain value) is less than a threshold within first several iterations of BP decoding;
- or the number of syndrome constraints satisfied by the codeword calculated using (6.46) at the end of each iteration does not increase for several iterations.

On the other hand, successful decoding is identified when the modified BP decoding algorithm converges to a codeword satisfying all syndrome constraints without encountering those two situations listed above. Unlike ordinary BP decoding algorithm, no maximum number of iterations is specified here. However, due to detection of decoding success and failure, it is easy to see that modified BP decoding algorithm will terminate within finite iterations. Coupled with modified BP decoding algorithm, this implementation of SA-LDPC-IED scheme is summarized in Algorithm 5. Compared to Algorithm 2 and 4, it can be seen that the search through the jar $J_b(y^n)$ in step 11 is implemented by modified BP decoding algorithm. In addition, to further reduce the compression rate and the number of round of interactions, we enlarge the jar $J_b(y^n)$ such that the output of modified BP decoding algorithm is inside the jar whenever successful decoding is identified. Simulation shows that under this decoding rule, the bit error probability is still very small. Moreover, since this decoding rule is more aggressive than jar decoding used in section 6.4, for some (X, Y) the rate achieved by the SA-LDPC-IED scheme implemented in this way can be smaller than that given in Theorem 6.3.

To further consider a general memoryless source-side information pair, i.e. $p_1 \neq p_2$, at the b-th interaction, we can quantize the interval $(0, 0.5)$ into several quantized values. For each quantized value q_1, calculate its corresponding q_2 according to

$$\Pr\{Y = 0\}H(q_1) + \Pr\{Y = 1\}H(q_2) = H(p_b) \tag{6.48}$$

and finally apply the modified BP decoding algorithm for each such quantized pair (q_1, q_2). Successful decoding is claimed whenever there is one such quantized (q_1, q_2) that makes the BP decoding algorithm converge to a source sequence satisfying syndrome constraints. When there is a tie, i.e. more than one pair (q_1, q_2) that make the BP decoding algorithm succeed with different outputs, we will choose the one with the smaller value of q_1. Here we assume that the distribution of side information Y is known to the decoder. Otherwise, the empirical distribution can be calculated, since the decoder has the full access to side information. The implementation is summarized in Algorithm 6.

Remark 6.10. *Simulation shows that the complexity of the decoding algorithm above for general memoryless source-side information pairs is not high as it seems. First of all, successful decoding is not very sensitive to the values of quantized q_1 and q_2, and therefore*

Algorithm 5 SA-LDPC-IED scheme with Modified BP Decoding for i.i.d source-side information pairs correlated through binary symmetric channel

Based on $\mathcal{P}_1\mathcal{P}_2\cdots\mathcal{P}_n$ and $s^n = \mathbf{H}_{n\times n}x^n$, the encoder generates accumulated syndromes $\tilde{s}_1\tilde{s}_2\cdots\tilde{s}_n$ and augmenting syndromes $a_1a_2\cdots a_n$.
Based on $\mathcal{P}_1\mathcal{P}_2\cdots\mathcal{P}_n$ and $\mathbf{H}_{n\times n}$, the decoder calculates matrices $\mathbf{H}^{(\Delta)}_{\Delta\times n}\mathbf{H}^{(2\Delta)}_{2\Delta\times n}\cdots\mathbf{H}^{(n)}_{n\times n}$.

$b \leftarrow 0$.
while The encoder does not receive bit 1 from the decoder **do**
  $b \leftarrow b+1$.
  if $b \leq \frac{n}{\Delta}$ **then**
    The encoder sends augmenting syndromes $a_{(b-1)\Delta+1}\cdots a_{b\Delta}$ to the decoder by Δ bits.
  else
    The encoder sends syndromes $s'_{\eta_n n} = \mathbf{H}'_{\eta_n n\times n}x^n$ to the decoder by $\eta_n n$ bits.
  end if
  Upon receiving syndromes sent from the encoder, the decoder searches $\hat{x}^n$ by running modified BP decoding algorithm described above with estimated crossover probability p_b in equation (6.47).
  if successful decoding is identified **then**
    The decoder sends bit 1 to the encoder, and outputs $\hat{x}^n$ as the estimate of x^n.
  else
    The decoder sends bit 0 to the encoder and leaves the estimate of x^n undecided.
  end if
end while

Algorithm 6 SA-LDPC-IED scheme with Modified BP Decoding for i.i.d source-side information pairs correlated through binary memoryless channel

Based on $\mathcal{P}_1\mathcal{P}_2\cdots\mathcal{P}_n$ and $s^n = \mathbf{H}_{n\times n}x^n$, the encoder generates accumulated syndromes $\tilde{s}_1\tilde{s}_2\cdots\tilde{s}_n$ and augmenting syndromes $a_1a_2\cdots a_n$.
Based on $\mathcal{P}_1\mathcal{P}_2\cdots\mathcal{P}_n$ and $\mathbf{H}_{n\times n}$, the decoder calculates matrices $\mathbf{H}^{(\Delta)}_{\Delta\times n}\mathbf{H}^{(2\Delta)}_{2\Delta\times n}\cdots\mathbf{H}^{(n)}_{n\times n}$.

$b \leftarrow 0$.
while The encoder does not receive bit 1 from the decoder **do**
  $b \leftarrow b+1$.
  if $b \leq \frac{n}{\Delta}$ **then**
    The encoder sends augmenting syndromes $a_{(b-1)\Delta+1}\cdots a_{b\Delta}$ to the decoder by Δ bits.
  else
    The encoder sends syndromes $s'_{\eta_n n} = \mathbf{H'}_{\eta_n n\times n}x^n$ to the decoder by $\eta_n n$ bits.
  end if
  Upon receiving syndromes sent from the encoder,
  for each quantized value of q_1 **do**
    the decoder searches $\hat{x}^n$ by running modified BP decoding algorithm described above with estimated crossover probability q_1 and q_2 in equation (6.48).
    if successful decoding is identified **then**
      break.
    end if
  end for
  if successful decoding is ever identified **then**
    The decoder sends bit 1 to the encoder, and outputs $\hat{x}^n$ as the estimate of x^n.
  else
    The decoder sends bit 0 to the encoder and leaves the estimate of x^n undecided.
  end if
end while

we can use coarse quantization without much loss of coding performance. Moreover, as the decoding failure can be detected at early stages as discussed above, the number of iterations is very low (usually within 5 iterations) when q_1 and q_2 are far from the actual statistics.

Remark 6.11. *There is a rich literature [43, 56–58] on the design of BP decoding algorithms for SWC schemes with unknown statistics. However, it is not possible to directly apply those techniques to our IED schemes. As pointed out earlier, one of the fundamental differences between SWC and IED is that SWC is fixed rate while IED is variable rate. Moreover, the decoding algorithm proposed here distinguishes itself with those techniques (especially in [58]) by combining the process of estimating statistics of source-side information and actual decoding together. Last but not least, we tackle the problem where source and side information are correlated through a general memoryless channel without assumption of symmetry, while BSC is commonly assumed for the statistics of source and side information in the literatures.*

6.5.2 Simulation Results

We first consider the case where the source and side information are correlated through a binary symmetric channel with unknown cross-over probability, and the side information is uniformly distributed. (In Figures 6.4 to 6.6, rates and conditional entropies are in unit of bits.)

Figure 6.4 shows the performance of our implemented scheme (referred to as the simulation rate) along with the conditional entropy rate and the performance upper bound established in Theorem 6.3, where the blue solid line represents the simulation rate with bit error probabilities below or around 2×10^{-5}, and the green dashed line represents the upper bound established in Theorem 6.3 with $\epsilon = 0.1$. The block length is 8000, $\Delta = \lfloor\sqrt{n}\rfloor = 89$, and the variable degree distribution (from an edge perspective) used is shown below:

$$\begin{aligned}\lambda(x) \quad = \quad & 0.178704x + 0.176202x^2 + 0.102845x^5 \\ & + 0.114789x^6 + 0.0122023x^{12} + 0.0479225x^{13} \\ & + 0.115911x^{14} + 0.251424x^{39}\end{aligned}$$

which is designed for rate 0.5 (in bits), and obtained from [59]. It can be seen that our implemented SA-LDPC-IED scheme can indeed adapt to the entropy rate $\mathrm{H}(X|Y)$ well in a large rate region. The choice of $\Delta = \lfloor\sqrt{n}\rfloor$ is due to that $\Delta = O(\sqrt{n})$ is shown to be optimal from Theorems 6.1 and 6.3. Certainly, it is possible to further optimize Δ, e.g. to be $c\sqrt{n}$ for some tuned constant c; however, simulation shows that benefit of

further optimization on Δ is marginal as the feedback rate is already small and increment of forward rate for each interaction is refined enough to probe the actual compression rate needed for successful decoding.

To interpret the upper bound $R_{L(z)}(\epsilon, H(p_0))$ also shown in Figure 6.4 better, an explanation on ϵ is needed here. The reason that $\epsilon >>$ bit error probability in the simulation is due to Remark 6.8. To rephrase here, let $d_{\min}^{(b)}$ denote the minimum hamming distance of the code generated by $\mathbf{H}_{b\Delta\times n}^{(b\Delta)}$. From the proof of Theorem 6.3, it follows that with high probability, $\frac{1}{n}wt(\hat{X}^n - X^n) \leq \epsilon$. On the other hand, $\frac{1}{n}wt(\hat{X}^n - X^n) \leq \epsilon$ implies that $\hat{X}^n = X^n$ if $d_{\min}^{(b)} > \epsilon n$ when the coding procedure terminates at the b-th interaction. Moreover, since the implemented decoding algorithm only checks syndrome constraints to determine the decoding success, instead of using thresholds given in Theorem 6.3, the bound on rate can be improved if the choice of ϵ for the b-th interaction depends on $d_{\min}^{(b)}$, especially for the high rate case as $d_{\min}^{(b)}$ increases with b. However, since $d_{\min}^{(b)}$ can not be expressed in a simple way and does not affect redundancy analysis when degree distributions with large degrees are used, the corresponding result is not included here. In the meantime, by using the same degree distribution $L(z)$ in Figure 6.4, Figure 6.5 shows how fast $R_{L(z^k)}\left(\frac{1}{2\sqrt{k}}, H(p_0)\right)$ converges to $H(p_0)$, where the gap is always less than 0.02 when $k = 5$, which confirms Proposition 6.1 and 6.2. Note that the reason that the bound $R_{L(z)}(\epsilon, H(p_0))$ improves dramatically for $k = 2$ compared to $k = 1$ in Figure 6.4 lies in that the choice of ϵ. In particular, $\epsilon = \frac{1}{2\sqrt{2}}$ for $k = 2$ in Figure 6.5, while $\epsilon = 0.1$ in Figure 6.4.

As can be seen from Proposition 6.1, given a degree distribution $L(z)$, using $L(z^k)$ for large k is just one of many ways to approach optimum. The essential message conveyed here is that by increasing degrees in degree distribution of SA-LDPC-IED scheme, better performance can be yielded. To confirm this through simulation, another SA-LDPC-IED scheme is constructed by using variable degree distribution (from an edge perspective)

$$\begin{aligned}\tilde{\lambda}(x) &= 0.238563x + 0.210469x^2 + 0.0349301x^3 + 0.120072x^4 \\ &\quad + 0.0159369x^6 + 0.00480289x^{13} + 0.376122x^{14}\end{aligned}$$

with average variable node degree $\bar{l} = 4$. Then its performance is compared with that of SA-LDPC-IED scheme constructed above using $\lambda(x)$ with $\bar{l} = 5$, where statistics of source-side information pair and other simulation parameters (e.g. n and Δ) are kept the same as that used for simulation in Figure 6.4. As shown in Figure 6.6, SA-LDPC-IED scheme with $\bar{l} = 5$ indeed outperforms that with $\bar{l} = 4$.

We next consider source and side-information pairs correlated through binary asymmetric channels. Table 6.1 lists our simulation results, where the side information Y is still

$\Pr\{X=1\|Y=0\}$	$\Pr\{X=0\|Y=1\}$	Rate
0.05	0.1959	0.541
0.1	0.1206	0.544
0.15	0.0766	0.543
0.2	0.0481	0.540

Table 6.1: Performance of SA-LDPC-IED: Asymmetrical Channel

assumed to be uniformly distributed, and the transition probabilities are selected such that $H(X|Y) = 0.5 \ln 2$ for all cases. In our simulation, we did not see any error in 1000 blocks, each block being 8000 bits. As can be seen, our implemented SA-LDPC-IED scheme also works very well in this situation too.

To make a comparison with SWC, a SWC scheme using the same LDPC code (LDPC-SWC) was also implemented for the source and side information correlated through a binary symmetrical channel. The respective results are shown in Table 6.2, where bit error

$\frac{H(X\|Y)}{\ln 2}$	$R_{\text{SA-LDPC-IED}}$	R_{SW}
0.426	0.473	0.5

Table 6.2: SA-LDPC-IED vs. LDPC-SWC

probabilities are maintained below 10^{-5} for both SA-LDPC-IED and LDPC-SWC schemes. Note that R_{SW} is deliberately chosen to be 0.5 (in bits), since the degree distribution of the LDPC code used here is designed for rate 0.5 (in bits). Moreover, in the simulation of the LDPC-SWC scheme, we assumed that the cross-over probability p_0 is known to the decoder, while in our implemented SA-LDPC-IED scheme, p_0 is unknown. Clearly, simulation results show that SA-LDPC-IED outperforms LDPC-SWC.

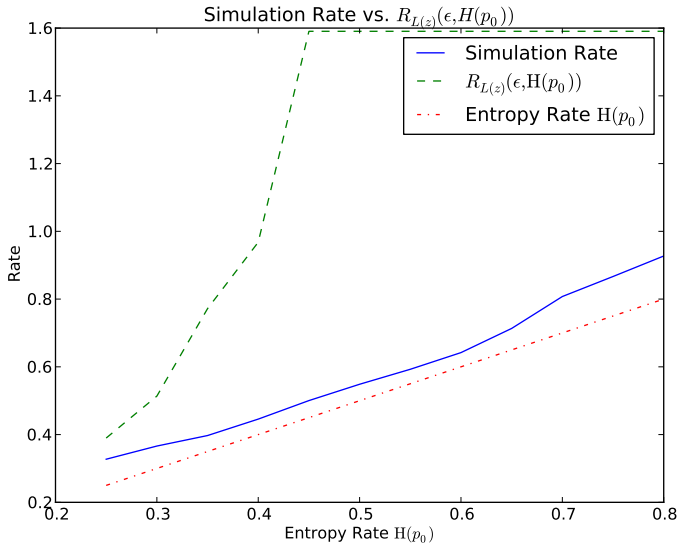


Figure 6.4: Performance of SA-LDPC-IED: Symmetrical Channel

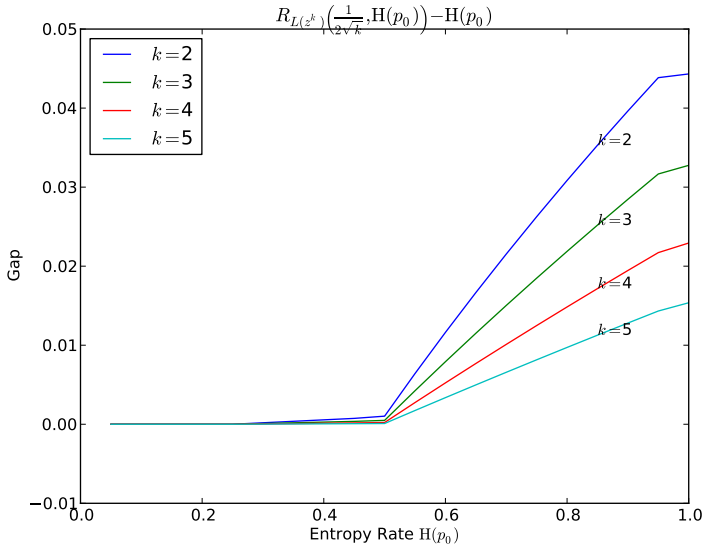


Figure 6.5: Redundancy bound with different k

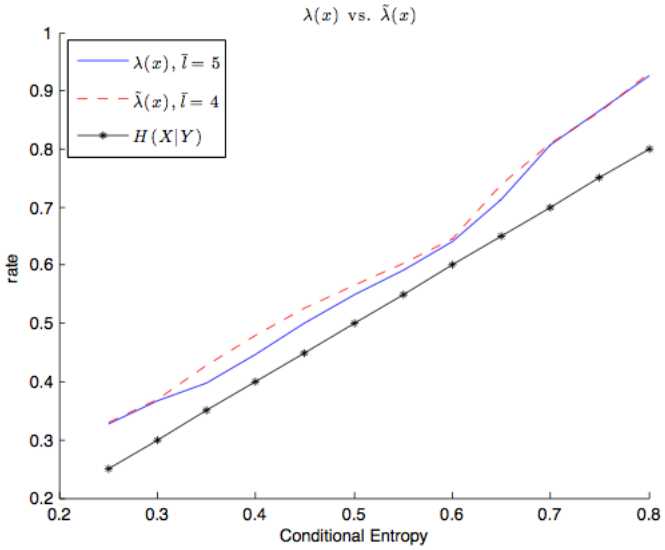


Figure 6.6: $\lambda(x)$ vs. $\tilde{\lambda}(x)$

6.6 Summary

In this chapter, under jar decoding with a dynamic jar, interactive encoding and decoding based on LDPC codes with syndrome accumulation (SA-LDPC-IED) has been proposed and investigated. Given any classical universal lossless code $\mathcal{C}_n$ (with block length n and side information available to both the encoder and decoder) and an LDPC code, we have demonstrated, with the help of syndrome accumulation, how to convert $\mathcal{C}_n$ into a universal SA-LDPC-IED scheme. With its word error probability approaching 0 sub-exponentially with n, the resulting SA-LDPC-IED scheme has been shown to achieve roughly the same rate performance as does $\mathcal{C}_n$ for each and every individual sequence pair (x^n, y^n) and the conditional entropy rate $H(X|Y)$ for any stationary, ergodic source and side information (X, Y) as the average variable node degree $\bar{l}$ of the underlying LDPC code increases without bound. When applied to the class of binary source and side information (X, Y) correlated through a BSC with cross-over probability unknown to either the encoder or decoder, the SA-LDPC-IED scheme has been further simplified, resulting in even improved rate performance versus the bit error probability when $\bar{l}$ is not large. Coupled with linear time BP decoding, the SA-LDPC-IED scheme has been implemented for binary source-side information pairs, which confirms the theoretic analysis, and further shows that the

SA-LDPC-IED scheme consistently outperforms the Slepian-Wolf coding scheme based on the same underlying LDPC code. This work demonstrates that jar decoding is also a powerful analytical tool to prove coding theorems in interactive information theory, and its natural connection to BP decoding allows easy transform from theoretical results to practical coding schemes.

Chapter 7

Conclusion and Future Work

7.1 Conclusion

In this thesis, a new decoding rule called jar decoding is proposed. Unlike MAP, ML, and MD decoding, which are all codebook centric, jar decoding is channel output sequence centric. Given a channel, code, and channel output sequence y^n, jar decoding first forms a jar of suitable size consisting of sequences from the channel input alphabet considered to be closely related to y^n, and then takes any codeword from the jar as the estimate of the transmitted codeword. For most channels, the jar can be formed a priori without the knowledge of the code; when both the input and output alphabets of the channel are finite, the jar can be even formed a priori without knowing either the code or the channel itself. To illustrate jar decoding, we have defined the Hamming jar for the binary symmetric channel (BSC), the BIAGC jar for the binary input additive Gaussian channel, the BIMC jar for any binary input memoryless channels with uniform capacity achieving distribution (BIMC), the DIMC jar for any discrete input arbitrary output channel (DIMC), the empirical conditional entropy jar for discrete memoryless channels with finite channel output alphabet and unknown statistics, and the jar derived from classical prefix codes for discrete ergodic (not necessarily memoryless) channels. We have also discussed the connections of jar decoding with old decoding rules including MAP, ML, MD, typical sequence,threshold and BP decoding.

Based on jar decoding and jars mentioned above, various coding theorems are yielded. In particular, non-asymptotic channel coding theorems are proved via jar decoding, based on random linear code ensembles for BIMC and Shannon random code ensemble with a fixed codeword type for DIMC. Compared to existing results in the literature, those

achievabilities are shown to be new, tight and easy to compute. Moreover, by treating word error probability ϵ as a constant or a sub-exponentially decreasing function of block length n, the achievabilities under jar decoding yield an achievable asymptotic trade-off between ϵ and channel coding rate R up to the second order with respect to n, which is then shown to be tight by non-asymptotic converse channel coding theorems via a proof technique called the outer mirror image of jar. Then towards investigating the second order optimality of jar decoding in the non-asymptotic regime, Taylor-type expansion of optimal channel coding rate with finite block length is discovered by combining the achievabilities via jar decoding and converse theorems via the outer mirror image of jar, and jar decoding is shown to be able to achieve optimal first and second orders in this Taylor-type expansion. In addition, two approximations of optimal channel coding rate are derived from Taylor-type expansion and are shown to be reliable and accurate by numerical evaluation. And the impact of Taylor-type expansion on practical communication system design is further demonstrated by its application to adaptive modulation and coding in LTE system. Beside the near optimality, the flexibility of jar decoding is demonstrated by establishing LDPC coding theorem regarding to bit error probability for general binary input memoryless channels. And interactive encoding and decoding theorems based on LDPC codes with syndrome accumulation under jar decoding with a dynamic jar serves as an example to illustrate the applicability of jar decoding to interactive information and coding theory.

As evidenced by the evolution of digital communication and information theory over the past 60 years, different decoding rules bring in different perspectives not only on decoding itself, but also on how to design codes particularly suitable for the respective decoding rule. With the simplicity brought by jar decoding into channel coding and interactive encoding and decoding analysis, we would expect that similar change would happen. In the jar decoding analysis of random codes, it is not necessary for codewords to be pairwise independent, which implies that one can impose more structures on codes themselves to lower the decoding complexity in jar decoding. With jar decoding, we believe that there is ample room to design effective codes and jar decoding algorithms.

7.2 Future Work

Coding theorems via jar decoding derived in this thesis illustrate various directions to improve the code design in practical communication systems.

1) Jar decoding, the outer image of jar, and non-asymptotic equipartition properties form a set of essential tools to prove non-asymptotic coding theorems in non-asymptotic information theory where point-to-point communication is considered.

Due to their similarity with typical sequence decoding and asymptotic equipartition properties, it is highly believed that those proof techniques developed in this paper can be extended to prove tight non-asymptotic coding theorems in multi-user information theory.

2) Nowadays channel codes (e.g. LDPC and turbo code) in practical systems operate at the rate near the capacity. From non-asymptotic achievability via jar decoding, it can be seen that at this rate region, the dominating error event is that the true codeword is not inside the jar, which suggests that error detection can be achieved by examining whether the decoder output is inside the jar centered by the channel output. As the probability of another codeword existing in the jar is only the minor contributor to the decoding error probability, this error detection enjoys low undetected probability and no extra rate penalty compared to other methods like using cyclic redundancy check codes. The implementation of this error detection method on practical systems such as LTE system is one of future work, which could deliver fruitful results.

3) From the discussion of Taylor-type expansion in Chapter 4, we know that channel code design for DIMC may not follow the capacity-achieving distribution when the block length is finite. Instead, the channel code should be designed according to t^* in Taylor-type expansion. As linear codes are widely used in practice due to its low encoding and decoding complexity, directly applying t^* in this way to linear code design may be difficult, considering the limitation that codewords must form a linear space. However, applying this idea to modulation and coding on AWGN channel, one can change the mapping from the channel codeword to the constellation to shape the empirical distribution of the sequence of modulation symbols according to t^*. In this direction, a mapping with memory should be designed to replace the memoryless mapping (e.g. Gray mapping) widely used in practice. Certainly, when this new mapping is used, decoding algorithm needs to be modified accordingly.

4) As one extension of LDPC coding theorem in Chapter 5, we have some preliminary results on systematic LDPC code under jar decoding. Specifically, we show that a linear code of parity check matrix $\left[\begin{array}{cc}\mathbf{H} & \mathbf{I}\end{array}\right]$ with $\mathbf{H}$ randomly picked from an LDPC ensemble can approach the capacity of any BIMC with diminishing bit error probability when the degrees of the ensemble are large. Directly applying traditional BP decoding to systematic LDPC codes, however, does not work very well, which is explained as follows. Let us fix the channel coding rate near the capacity. On one hand, when the degrees of the ensemble are small, BP decoding can always find a codeword, but the bit error probability decreases too slowly with respect to the block length. On the other hand, when the degrees of the ensemble are large, BP decoding

has the difficulty to find any codeword at all. Then future work in this direction is to design new decoding algorithms for systematic LDPC codes.

5) Practical interactive encoding and decoding scheme design under jar decoding is also quite exciting. As discussed in Chapter 6, the key advantage of interactive encoding and decoding over Slepian-Wolf coding is the universality, which is the essential property required in practical distributed compression systems. Interactive encoding and decoding based on LDPC codes with syndrome accumulation proposed in Chapter 6, coupled with modified BP decoding, can deal with the source and side information correlated through a memoryless channel. In practice, however, the statistics of source and side information is much more complicated, and memoryless channel model will result in great compression inefficiency. Therefore, another future work is to design a truly universal and low-complexity interactive encoding and decoding scheme, and we have already obtained some preliminary results in [60].

APPENDICES

Appendix A

Non-Asymptotic Equipartition Property

Consider an independent and identically distributed (IID) source $X = \{X_i\}_{i=1}^{\infty}$ with source alphabet $\mathcal{X}$ and finite entropy $H(X)$, where $H(X)$ is the Shannon entropy of X_i if $\mathcal{X}$ is discrete, and the differential entropy of X_i if $\mathcal{X}$ is the real line and each X_i is a continuous random variable. Let $p(x)$ be the probability mass function (pmf) or probability density function (pdf) (as the case may be) of X_i. The asymptotic equipartition property (AEP) for X is the assertion that

$$-\frac{1}{n}\ln p(X_1X_2\cdots X_n) \to H(X) \tag{A.1}$$

either in probability or with probability one as n goes to ∞. It implies that for sufficiently large n, with high probability, the outcomes of $X_1X_2\cdots X_n$ are approximately equiprobable with their respective probability ranging from $e^{-n(H(X)+\epsilon)}$ to $e^{-n(H(X)-\epsilon)}$, where $\epsilon > 0$ is a small fixed number.

The AEP is fundamental to information theory. It is not only instrumental to lossless source coding theorems, but also behind almost all asymptotic coding (including source, channel, and multi-user coding) theorems through the concepts of typical sets and typical sequences [4].

However, in the non-asymptotic regime where one wants to establish non-asymptotic coding results for finite block length n, the AEP in its current form can not be applied in general. In Appendix A, we aim to establish the non-asymptotic counterpart of the AEP, which is broadly referred to as the non-asymptotic equipartition property (NEP), so

that the NEP can be applied to finite block length n. Specifically, with respect to $H(X)$, we first characterize, for any finite block length n, how close $-\frac{1}{n}\ln p(X_1X_2\cdots X_n)$ is to $H(X)$ by determining the information spectrum of $X_1X_2\cdots X_n$, i.e., the distribution of $-\frac{1}{n}\ln p(X_1X_2\cdots X_n)$; such a property is referred to as the NEP with respect to $H(X)$. For any IID source pair $(X,Y) = \{(X_i,Y_i)\}_{i=1}^{\infty}$ with finite conditional entropy $H(X|Y)$ and mutual information $I(X;Y)$, where $H(X|Y)$ is the Shannon conditional entropy of X_i given Y_i if X is discrete, and the conditional differential entropy of X_i given Y_i if X is continuous, we then examine, for any finite block length n, how close $-\frac{1}{n}\ln p(X^n|Y^n)$ ($-\frac{1}{n}\ln\frac{p(Y^n|X^n)}{p(Y^n)}$, respectively) is to $H(X|Y)$ ($I(X;Y)$, respectively) by determining the distribution of $-\frac{1}{n}\ln p(X^n|Y^n)$ ($-\frac{1}{n}\ln\frac{p(Y^n|X^n)}{p(Y^n)}$, respectively), where $p(x^n|y^n)$ ($p(y^n|x^n)$, respectively) is the conditional pmf or pdf (as the case may be) of $x^n = x_1x_2\cdots x_n$ ($y^n = y_1y_2\cdots y_n$, respectively) given y^n (x^n, respectively); these properties are referred to as the NEP with respect to $H(X|Y)$ and $I(X;Y)$, respectively.

In the same way as the AEP plays an important role in establishing the asymptotic coding (including source, channel, and multi-user coding) results in information theory, our established NEP is also instrumental to the development of non-asymptotic source and channel coding results.

A.1 NEP With Respect to Entropy

Define

$$\lambda^*(X) \triangleq \sup\left\{\lambda \geq 0 : \int p^{-\lambda+1}(x)dx < \infty\right\}. \tag{A.2}$$

Suppose that

$$\lambda^*(X) > 0\,. \tag{A.3}$$

Let

$$\sigma_H^2(X) \triangleq \int p(x)[-\ln p(x)]^2 dx - H^2(X) \tag{A.4}$$

which will be referred to as the information variance of X. It is not hard to see that under the assumption (A.3),

$$\int \frac{p^{-\lambda+1}(x)}{\left[\int p^{-\lambda+1}(y)dy\right]} \left|-\ln p(x)\right|^k dx < \infty \tag{A.5}$$

and

$$\int p^{-\lambda+1}(x)dx < \infty$$

for any $\lambda \in (0, \lambda^*(X))$ and any positive integer k. Further assume that

$$\sigma_H^2(X) > 0 \text{ and } \int p(x)|\ln p(x)|^3 dx < \infty \,. \tag{A.6}$$

Then we have the following result, which will be referred to as the weak right NEP with respect to $H(X)$.

Theorem A.1 (Weak Right NEP)**.** *For any $\delta \geq 0$, let*

$$r_X(\delta) \stackrel{\Delta}{=} \sup_{\lambda \geq 0} \left[\lambda(H(X) + \delta) - \ln \int p^{-\lambda+1}(x) dx \right] \,.$$

Then the following hold:

(a) *For any positive integer n,*

$$\Pr\left\{ -\frac{1}{n} \ln p(X^n) > H(X) + \delta \right\} \leq e^{-n r_X(\delta)} \tag{A.7}$$

where $X^n = X_1 X_2 \cdots X_n$.

(b) *Under the assumptions (A.3) and (A.6), there exists a $\delta^* > 0$ such that for any $\delta \in (0, \delta^*]$ and any positive integer n,*

$$r_X(\delta) = \frac{1}{2\sigma_H^2(X)} \delta^2 + O(\delta^3) \tag{A.8}$$

and hence

$$\Pr\left\{ -\frac{1}{n} \ln p(X^n) > H(X) + \delta \right\} \leq e^{-n\left(\frac{\delta^2}{2\sigma_H^2(X)} + O(\delta^3)\right)} \,. \tag{A.9}$$

Proof of Theorem A.1. The inequality (A.7) follows from the Chernoff bound. To see this is indeed the case, note that

$$\begin{aligned}
\Pr\left\{ -\frac{1}{n} \ln p(X_1 X_2 \cdots X_n) > H(X) + \delta \right\} &= \Pr\left\{ -\ln p(X_1 X_2 \cdots X_n) > n(H(X) + \delta) \right\} \\
&\leq \inf_{\lambda \geq 0} \frac{\mathbf{E}[e^{-\lambda \ln p(X_1 X_2 \cdots X_n)}]}{e^{n\lambda(H(X)+\delta)}} \\
&= \inf_{\lambda \geq 0} e^{-n\left[\lambda(H(X)+\delta) - \ln \mathbf{E}[p^{-\lambda}(X_1)]\right]} \\
&= \inf_{\lambda \geq 0} e^{-n\left[\lambda(H(X)+\delta) - \ln \int p^{-\lambda+1}(x) dx\right]} \\
&= e^{-n r_X(\delta)} \,.
\end{aligned} \tag{A.10}$$

To show (A.8) and (A.9), we first analyze the property of $r_X(\delta)$ as a function of δ over the region $\delta \geq 0$. It is easy to see that $r_X(\delta)$ is convex and non-decreasing. For any $\lambda \in [0, \lambda^*(X))$, define

$$\delta(\lambda) \triangleq \int \frac{p^{-\lambda+1}(x)}{\left[\int p^{-\lambda+1}(y)dy\right]} \left[-\ln p(x)\right] dx - H(X) \tag{A.11}$$

which, in view of (A.5), is well defined. Using a similar argument as in [61, Properties 1 to 3], it is not hard to show that under the assumption (A.3), $\delta(\lambda)$ as a function of λ is continuously differentiable up to any order over $\lambda \in (0, \lambda^*(X))$. Taking the first order derivative of $\delta(\lambda)$ yields

$$\begin{aligned} \delta'(\lambda) &= \int \frac{p^{-\lambda+1}(x)}{\left[\int p^{-\lambda+1}(y)dy\right]} \left[-\ln p(x)\right]^2 dx - \left[\int \frac{p^{-\lambda+1}(x)}{\left[\int p^{-\lambda+1}(y)dy\right]} \left[-\ln p(x)\right] dx\right]^2 \\ &> 0 \end{aligned} \tag{A.12}$$

where the last inequality is due to (A.6). It is also easy to see that $\delta(0) = 0$ and $\delta'(0) = \sigma_H^2(X)$. Therefore, $\delta(\lambda)$ is strictly increasing over $\lambda \in [0, \lambda^*(X))$. On the other hand, it is not hard to verify that under the assumption (A.3), the function $\lambda(H(X) + \delta) - \ln \int p^{-\lambda+1}(x)dx$ as a function of λ is continuously differentiable over $\lambda \in [0, \lambda^*(X))$ with its derivative equal to

$$\delta - \delta(\lambda) \; . \tag{A.13}$$

To continue, we distinguish between two cases: (1) $\lambda^*(X) = \infty$, and (2) $\lambda^*(X) < \infty$. In case (1), since $\delta(\lambda)$ is strictly increasing over $\lambda \in [0, \infty)$, it follows that for any $\delta = \delta(\lambda)$ for some $\lambda \in [0, \lambda^*(X))$, the supremum in the definition of $r_X(\delta)$ is actually achieved at that particular λ, i.e.,

$$r_X(\delta(\lambda)) = \lambda(H(X) + \delta(\lambda)) - \ln \int p^{-\lambda+1}(x)dx \; . \tag{A.14}$$

In case (2), we have that for any $\delta = \delta(\lambda)$ for some $\lambda \in [0, \lambda^*(X))$,

$$\beta(H(X) + \delta(\lambda)) - \ln \int p^{-\beta+1}(x)dx < \lambda(H(X) + \delta(\lambda)) - \ln \int p^{-\lambda+1}(x)dx \tag{A.15}$$

for any $\beta \in [0, \lambda^*(X))$ with $\beta \neq \lambda$. In view of the definition of $\lambda^*(X)$, (A.15) remains valid for any $\beta > \lambda^*(X)$ since then the left side of (A.15) is $-\infty$. What remains to check is when $\beta = \lambda^*(X)$. If

$$\int p^{-\lambda^*(X)+1}(x)dx = \infty$$

it is easy to see that (A.15) holds as well when $\beta = \lambda^*(X)$. Suppose now

$$\int p^{-\lambda^*(X)+1}(x)dx < \infty \ .$$

In this case, it follows from the dominated convergence theorem that

$$\lim_{\beta\uparrow\lambda^*(X)} \int p^{-\beta+1}(x)dx = \int p^{-\lambda^*(X)+1}(x)dx$$

and hence by letting β go to $\lambda^*(X)$ from the left, we see that (A.15) holds as well when $\beta = \lambda^*(X)$. Putting all cases together, we always have that for any $\delta = \delta(\lambda)$ for some $\lambda \in [0, \lambda^*(X))$,

$$r_X(\delta(\lambda)) = \lambda(H(X) + \delta(\lambda)) - \ln \int p^{-\lambda+1}(x)dx \ . \tag{A.16}$$

Let

$$\Delta^*(X) \stackrel{\Delta}{=} \lim_{\lambda\uparrow\lambda^*(X)} \delta(\lambda) \ .$$

Since both $\delta(\lambda)$ and $\ln \int p^{-\lambda+1}(x)dx$ are continuously differentiable with respect to $\lambda \in (0, \lambda^*(X))$ up to any order, it follows from (A.16) that $r_X(\delta)$ is also continuously differentiable with respect to $\delta \in (0, \Delta^*(X))$ up to any order. (At $\delta = 0$, $r_X(\delta)$ is continuously differentiable up to at least the third order inclusive.) Taking the first and second order derivatives of $r_X(\delta)$ with respect to δ, we have

$$\begin{aligned}
r'_X(\delta) &= \frac{dr_X(\delta)}{d\delta} \\
&= \frac{dr_X(\delta(\lambda))}{d\lambda}\frac{d\lambda}{d\delta} \\
&= \frac{dr_X(\delta(\lambda))}{d\lambda}\frac{1}{\delta'(\lambda)} \\
&= \frac{1}{\delta'(\lambda)}\left[H(X) + \delta(\lambda) + \lambda\delta'(\lambda) - \int \frac{p^{-\lambda+1}(x)}{\left[\int p^{-\lambda+1}(y)dy\right]}\left[-\ln p(x)\right]dx\right] \\
&= \lambda
\end{aligned} \tag{A.17}$$

and

$$\begin{aligned}
r''_X(\delta) &= \frac{d\lambda}{d\delta} \\
&= \frac{1}{\delta'(\lambda)}
\end{aligned} \tag{A.18}$$

where $\delta = \delta(\lambda)$. Therefore, $r_X(\delta)$ is convex, strictly increasing, and continuously differentiable up to at least the third order (inclusive) over $\delta \in [0, \Delta^*(X))$. Note that from (A.17) and (A.18), we have $r'_X(0) = 0$ and $r''_X(0) = 1/\sigma_H^2(X)$. Expanding $r_X(\delta)$ at $\delta = 0$ by the Taylor expansion, we then have that there exists a $\delta^* > 0$ such that

$$r_X(\delta) = \frac{1}{2\sigma_H^2(X)}\delta^2 + O(\delta^3) \tag{A.19}$$

for $\delta \in (0, \delta^*]$. The inequality (A.9) now follows immediately from (A.7) and (A.19). This completes the proof of Theorem A.1. □

Having analyzed the function $r_X(\delta)$, we are now ready for a stronger version of the right NEP. For any $\lambda \in [0, \lambda^*(X))$, define

$$f_\lambda(x) \stackrel{\Delta}{=} \frac{p^{-\lambda}(x)}{\int p^{-\lambda+1}(y)dy} \tag{A.20}$$

$$\sigma_H^2(X, \lambda) \stackrel{\Delta}{=} \int f_\lambda(x)p(x) \left|-\ln p(x) - (H(X) + \delta(\lambda))\right|^2 dx \tag{A.21}$$

$$M_H(X, \lambda) \stackrel{\Delta}{=} \int f_\lambda(x)p(x) \left|-\ln p(x) - (H(X) + \delta(\lambda))\right|^3 dx \tag{A.22}$$

and

$$f_\lambda(x^n) \stackrel{\Delta}{=} \prod_{i=1}^{n} f_\lambda(x_i) \tag{A.23}$$

where $\delta(\lambda)$ is defined in (A.11). Write $M_H(X, 0)$ as $M_H(X)$. It is easy to see that $\sigma_H^2(X, 0) = \sigma_H^2(X)$, $\sigma_H^2(X, \lambda) = \delta'(\lambda)$, and

$$M_H(X) = \int p(x) \left|-\ln p(x) - H(X))\right|^3 dx \ . \tag{A.24}$$

Then we have the following stronger result.

Theorem A.2 (Strong Right NEP)**.** *Under the assumptions (A.3) and (A.6), the following hold:*

(a) *For any $\delta \in (0, \Delta^*(X))$ and any positive integer n*

$$\bar{\xi}_H(X, \lambda, n)e^{-nr_X(\delta)} \geq \Pr\left\{-\frac{1}{n}\ln p(X^n) > H(X) + \delta\right\} \geq \underline{\xi}_H(X, \lambda, n)e^{-nr_X(\delta)} \tag{A.25}$$

where $\lambda = r'_X(\delta) > 0$,

$$\bar{\xi}_H(X,\lambda,n) = \frac{2CM_H(X,\lambda)}{\sqrt{n}\sigma_H^3(X,\lambda)} + e^{\frac{n\lambda^2\sigma_H^2(X,\lambda)}{2}}\left[Q(\sqrt{n}\lambda\sigma_H(X,\lambda)) - Q(\rho^* + \sqrt{n}\lambda\sigma_H(X,\lambda))\right] \tag{A.26}$$

$$\underline{\xi}_H(X,\lambda,n) = e^{\frac{n\lambda^2\sigma_H^2(X,\lambda)}{2}} Q(\rho_* + \sqrt{n}\lambda\sigma_H(X,\lambda)) \tag{A.27}$$

with $Q(\rho^*) = \frac{CM_H(X,\lambda)}{\sqrt{n}\sigma_H^3(X,\lambda)}$ *and* $Q(\rho_*) = \frac{1}{2} - \frac{2CM_H(X,\lambda)}{\sqrt{n}\sigma_H^3(X,\lambda)}$, $Q(t) = \frac{1}{\sqrt{2\pi}}\int_t^\infty e^{-u^2/2}du$ *and* $C < 1$ *is the universal constant in the central limit theorem of Berry and Esseen.*

(b) *For any* $\delta \le c\sqrt{\frac{\ln n}{n}}$, *where* $c < \sigma_H(X)$ *is a constant,*

$$\begin{aligned} Q\left(\frac{\delta\sqrt{n}}{\sigma_H(X)}\right) - \frac{CM_H(X)}{\sqrt{n}\sigma_H^3(X)} &\le \Pr\left\{-\frac{1}{n}\ln p(X^n) > H(X) + \delta\right\} \\ &\le Q\left(\frac{\delta\sqrt{n}}{\sigma_H(X)}\right) + \frac{CM_H(X)}{\sqrt{n}\sigma_H^3(X)}. \end{aligned} \tag{A.28}$$

Proof of Theorem A.2. From (A.16), it follows that with $\lambda = r'_X(\delta)$

$$r_X(\delta) = \lambda(H(X) + \delta) - \ln \int p^{-\lambda+1}(x)dx\ . \tag{A.29}$$

Then it is not hard to verify that

$$
\begin{aligned}
&\Pr\left\{-\frac{1}{n}\ln p(X^n) > H(X)+\delta\right\} \\
&= \int\limits_{-\frac{1}{n}\ln p(x^n)>H(X)+\delta} p(x^n)dx^n \\
&= \int\limits_{-\frac{1}{n}\ln p(x^n)>H(X)+\delta} f_\lambda^{-1}(x^n) f_\lambda(x^n) p(x^n)dx^n \\
&= \int\limits_{-\frac{1}{n}\ln p(x^n)>H(X)+\delta} e^{-n\left[-\frac{1}{n}\lambda\ln p(x^n)-\ln\int p^{-\lambda+1}(y)dy\right]} f_\lambda(x^n) p(x^n)dx^n \\
&= \int\limits_{-\frac{1}{n}\ln p(x^n)>H(X)+\delta} e^{-n\left[-\frac{1}{n}\lambda\ln p(x^n)-\lambda(H(X)+\delta)+r_X(\delta)\right]} f_\lambda(x^n) p(x^n)dx^n \\
&= e^{-nr_X(\delta)} \int\limits_{-\frac{1}{n}\ln p(x^n)>H(X)+\delta} e^{-n\lambda\left[-\frac{1}{n}\ln p(x^n)-(H(X)+\delta)\right]} f_\lambda(x^n) p(x^n)dx^n \\
&= e^{-nr_X(\delta)} \int\limits_{-\frac{1}{n}\ln p(x^n)>H(X)+\delta} e^{-\sqrt{n}\lambda\sigma_H(X,\lambda)\frac{-\ln p(x^n)-n(H(X)+\delta)}{\sqrt{n}\sigma_H(X,\lambda)}} f_\lambda(x^n) p(x^n)dx^n \\
&= e^{-nr_X(\delta)} \int\limits_{\rho>0} \int\limits_{\frac{-\ln p(x^n)-n(H(X)+\delta)}{\sqrt{n}\sigma_H(X,\lambda)}=\rho} e^{-\sqrt{n}\lambda\sigma_H(X,\lambda)\rho} f_\lambda(x^n) p(x^n)dx^n d\rho \\
&= e^{-nr_X(\delta)} \int\limits_0^{+\infty} e^{-\sqrt{n}\lambda\sigma_H(X,\lambda)\rho} d(1-\bar{F}_n(\rho)) \\
&= e^{-nr_X(\delta)} \left[\bar{F}_n(0) - \int\limits_0^{+\infty} \sqrt{n}\lambda\sigma_H(X,\lambda) e^{-\sqrt{n}\lambda\sigma_H(X,\lambda)\rho}\bar{F}_n(\rho)d\rho\right] \qquad \text{(A.30)}
\end{aligned}
$$

where the last equality is due to integration by parts,

$$
\begin{aligned}
\bar{F}_n(\rho) &\triangleq \Pr\left\{\frac{-\ln p(Z^n)-n(H(X)+\delta)}{\sqrt{n}\sigma_H(X,\lambda)} > \rho\right\} \\
&= \Pr\left\{\sum_{i=1}^n \frac{-\ln p(Z_i)-(H(X)+\delta)}{\sqrt{n}\sigma_H(X,\lambda)} > \rho\right\}
\end{aligned}
$$

and $\{Z_i\}_{i=1}^n$ are IID random variables with pmf or pdf (as the case may be) $f_\lambda(x)p(x)$. Let

$$\xi_n \stackrel{\Delta}{=} \bar{F}_n(0) - \int_0^{+\infty} \sqrt{n}\lambda\sigma_H(X,\lambda)e^{-\sqrt{n}\lambda\sigma_H(X,\lambda)\rho}\bar{F}_n(\rho)d\rho \tag{A.31}$$

$$= \int_0^{+\infty} \sqrt{n}\lambda\sigma_H(X,\lambda)e^{-\sqrt{n}\lambda\sigma_H(X,\lambda)\rho}[\bar{F}_n(0) - \bar{F}_n(\rho)]d\rho \tag{A.32}$$

At this point, we invoke the following central limit theorem of Berry and Esseen [62, Theorem 1.2].

Lemma A.1. *Let $V_1, V_2, \cdots$ be independent real random variables with zero means and finite third moments, and set*

$$\sigma_n^2 = \sum_{i=1}^n \mathbb{E}V_i^2.$$

Then there exists a universal constant $C < 1$ such that for any $n \geq 1$,

$$\sup_{-\infty<t<+\infty} \left| \Pr\left\{ \sum_{i=1}^n V_i > \sigma_n t \right\} - Q(t) \right| \leq C\sigma_n^{-3} \sum_{i=1}^n \mathbb{E}|V_i|^3.$$

Towards evaluating ξ_n, we can bound $\bar{F}_n(\rho)$ in terms of $Q(\rho)$, by applying Lemma A.1 to $\{-\ln p(Z_i) - (H(X) + \delta)\}_{i=1}^n$. Then for $\rho > 0$, we have

$$\bar{F}_n(0) \leq Q(0) + \frac{CM_H(X,\lambda)}{\sqrt{n}\sigma_H^3(X,\lambda)}$$

$$= \frac{1}{2} + \frac{CM_H(X,\lambda)}{\sqrt{n}\sigma_H^3(X,\lambda)} \tag{A.33}$$

$$\bar{F}_n(\rho) \geq \left[Q(\rho) - \frac{CM_H(X,\lambda)}{\sqrt{n}\sigma_H^3(X,\lambda)} \right]^+ \tag{A.34}$$

and

$$\bar{F}_n(0) - \bar{F}_n(\rho) \geq \left[Q(0) - \frac{CM_H(X,\lambda)}{\sqrt{n}\sigma_H^3(X,\lambda)} - \left(Q(\rho) + \frac{CM_H(X,\lambda)}{\sqrt{n}\sigma_H^3(X,\lambda)} \right) \right]^+$$

$$= \left[\frac{1}{2} - Q(\rho) - \frac{2CM_H(X,\lambda)}{\sqrt{n}\sigma_H^3(X,\lambda)} \right]^+ \tag{A.35}$$

where $[x]^+ = \max\{x, 0\}$. Now plugging (A.33) and (A.34) into (A.31) yields

$$\begin{aligned}
\xi_n &\leq \frac{1}{2} + \frac{CM_H(X,\lambda)}{\sqrt{n}\sigma_H^3(X,\lambda)} - \int_0^{+\infty} \sqrt{n}\lambda\sigma_H(X,\lambda) e^{-\sqrt{n}\lambda\sigma_H(X,\lambda)\rho} \left[Q(\rho) - \frac{CM_H(X,\lambda)}{\sqrt{n}\sigma_H^3(X,\lambda)} \right]^+ d\rho \\
&= \frac{1}{2} + \frac{CM_H(X,\lambda)}{\sqrt{n}\sigma_H^3(X,\lambda)} - \int_0^{\rho^*} \sqrt{n}\lambda\sigma_H(X,\lambda) e^{-\sqrt{n}\lambda\sigma_H(X,\lambda)\rho} \left[Q(\rho) - \frac{CM_H(X,\lambda)}{\sqrt{n}\sigma_H^3(X,\lambda)} \right] d\rho \\
&= \frac{1}{2} + \frac{CM_H(X,\lambda)}{\sqrt{n}\sigma_H^3(X,\lambda)} - \int_0^{\rho^*} \left[Q(\rho) - \frac{CM_H(X,\lambda)}{\sqrt{n}\sigma_H^3(X,\lambda)} \right] d\left(-e^{-\sqrt{n}\lambda\sigma_H(X,\lambda)\rho} \right) \\
&= \frac{2CM_H(X,\lambda)}{\sqrt{n}\sigma_H^3(X,\lambda)} + \int_0^{\rho^*} \frac{1}{\sqrt{2\pi}} e^{-\frac{\rho^2}{2}} e^{-\sqrt{n}\lambda\sigma_H(X,\lambda)\rho} d\rho \\
&= \frac{2CM_H(X,\lambda)}{\sqrt{n}\sigma_H^3(X,\lambda)} + \int_0^{\rho^*} \frac{1}{\sqrt{2\pi}} e^{-\frac{(\rho+\sqrt{n}\lambda\sigma_H(X,\lambda))^2}{2} + \frac{n\lambda^2\sigma_H^2(X,\lambda)}{2}} d\rho \\
&= \frac{2CM_H(X,\lambda)}{\sqrt{n}\sigma_H^3(X,\lambda)} + e^{\frac{n\lambda^2\sigma_H^2(X,\lambda)}{2}} \left[Q(\sqrt{n}\lambda\sigma_H(X,\lambda)) - Q(\rho^* + \sqrt{n}\lambda\sigma_H(X,\lambda)) \right] \\
&= \bar{\xi}_H(X,\lambda,n) \qquad \text{(A.36)}
\end{aligned}$$

where $Q(\rho^*) = \frac{CM_H(X,\lambda)}{\sqrt{n}\sigma_H^3(X,\lambda)}$, and meanwhile plugging (A.35) into (A.32) yields

$$\begin{aligned}
\xi_n &\geq \int_0^{+\infty} \sqrt{n}\lambda\sigma_H(X,\lambda)e^{-\sqrt{n}\lambda\sigma_H(X,\lambda)\rho}\left[\frac{1}{2} - Q(\rho) - \frac{2CM_H(X,\lambda)}{\sqrt{n}\sigma_H^3(X,\lambda)}\right]^+ d\rho \\
&= \int_{\rho_*}^{+\infty} \sqrt{n}\lambda\sigma_H(X,\lambda)e^{-\sqrt{n}\lambda\sigma_H(X,\lambda)\rho}\left[\frac{1}{2} - Q(\rho) - \frac{2CM_H(X,\lambda)}{\sqrt{n}\sigma_H^3(X,\lambda)}\right] d\rho \\
&= \int_{\rho_*}^{+\infty} \left[\frac{1}{2} - Q(\rho) - \frac{2CM_H(X,\lambda)}{\sqrt{n}\sigma_H^3(X,\lambda)}\right] d\left(-e^{-\sqrt{n}\lambda\sigma_H(X,\lambda)\rho}\right) \\
&= \int_{\rho_*}^{+\infty} \frac{1}{\sqrt{2\pi}} e^{-\frac{\rho^2}{2}} e^{-\sqrt{n}\lambda\sigma_H(X,\lambda)\rho} d\rho \\
&= e^{\frac{n\lambda^2\sigma_H^2(X,\lambda)}{2}} Q(\rho_* + \sqrt{n}\lambda\sigma_H(X,\lambda)) \\
&= \underline{\xi}_H(X,\lambda,n) \qquad \text{(A.37)}
\end{aligned}$$

where $Q(\rho_*) = \frac{1}{2} - \frac{2CM_H(X,\lambda)}{\sqrt{n}\sigma_H^3(X,\lambda)}$. Combining (A.30) with (A.36) and (A.37) completes the proof of part (a) of Theorem A.2.

Applying Lemma A.1 to the IID sequence $\{-\ln p(X_i) - H(X)\}_{i=1}^n$, we get (A.28). This completes the proof of Theorem A.2. □

Remark A.1. *Note that $\lambda = r'_X(\delta) = \Theta(\delta)$. When $\lambda = \Omega(1)$ with respect to n, it can be easily verified that $\bar{\xi}_H(X,\lambda,n)$ and $\underline{\xi}_H(X,\lambda,n)$ are both on the order of $\frac{1}{\sqrt{n}}$, by applying well-known inequality*

$$\frac{1}{t+t^{-1}}\frac{1}{\sqrt{2\pi}}e^{-\frac{t^2}{2}} \leq Q(t) \leq \frac{1}{t}\frac{1}{\sqrt{2\pi}}e^{-\frac{t^2}{2}}.$$

Meanwhile, on one hand, it is easy to see that

$$\bar{\xi}_H(X,\lambda,n) \leq e^{\frac{n\lambda^2\sigma_H^2(X,\lambda)}{2}} Q(\sqrt{n}\lambda\sigma_H(X,\lambda)) + \frac{2CM_H(X,\lambda)}{\sqrt{n}\sigma_H^3(X,\lambda)}.$$

On the other hand,

$$\begin{aligned}
\underline{\xi}_H(X,\lambda,n) &= e^{\frac{n\lambda^2\sigma_H^2(X,\lambda)}{2}}Q(\sqrt{n}\lambda\sigma_H(X,\lambda)) - e^{\frac{n\lambda^2\sigma_H^2(X,\lambda)}{2}}\int\limits_{\sqrt{n}\lambda\sigma_H(X,\lambda)}^{\rho_*+\sqrt{n}\lambda\sigma_H(X,\lambda)}\frac{1}{\sqrt{2\pi}}e^{-\frac{\rho^2}{2}}d\rho \\
&= e^{\frac{n\lambda^2\sigma_H^2(X,\lambda)}{2}}Q(\sqrt{n}\lambda\sigma_H(X,\lambda)) - e^{\frac{n\lambda^2\sigma_H^2(X,\lambda)}{2}}\int\limits_{0}^{\rho_*}\frac{1}{\sqrt{2\pi}}e^{-\frac{(\rho+\sqrt{n}\lambda\sigma_H(X,\lambda))^2}{2}}d\rho \\
&= e^{\frac{n\lambda^2\sigma_H^2(X,\lambda)}{2}}Q(\sqrt{n}\lambda\sigma_H(X,\lambda)) - \int\limits_{0}^{\rho_*}\frac{1}{\sqrt{2\pi}}e^{-\frac{\rho^2+2\rho\sqrt{n}\lambda\sigma_H(X,\lambda)}{2}}d\rho \\
&\geq e^{\frac{n\lambda^2\sigma_H^2(X,\lambda)}{2}}Q(\sqrt{n}\lambda\sigma_H(X,\lambda)) - \int\limits_{0}^{\rho_*}\frac{1}{\sqrt{2\pi}}e^{-\frac{\rho^2}{2}}d\rho \\
&= e^{\frac{n\lambda^2\sigma_H^2(X,\lambda)}{2}}Q(\sqrt{n}\lambda\sigma_H(X,\lambda)) - \frac{2CM_H(X,\lambda)}{\sqrt{n}\sigma_H^3(X,\lambda)}.
\end{aligned}$$

To further shed light on $\bar{\xi}_H(X,\lambda,n)$ *and* $\underline{\xi}_H(X,\lambda,n)$*, we observe that*

$$\frac{1}{\sqrt{2\pi}\sqrt{n}\lambda\sigma_H(X,\lambda)+\frac{1}{\sqrt{2\pi}\sqrt{n}\lambda\sigma_H(X,\lambda)}} \leq e^{\frac{n\lambda^2\sigma_H^2(X,\lambda)}{2}}Q(\sqrt{n}\lambda\sigma_H(X,\lambda)) \leq \frac{1}{\sqrt{2\pi}\sqrt{n}\lambda\sigma_H(X,\lambda)}.$$

And therefore, whenever $\lambda = o(1)$ *and* $\lambda = \omega(n^{-1})$*,*

$$e^{\frac{n\lambda^2\sigma_H^2(X,\lambda)}{2}}Q(\sqrt{n}\lambda\sigma_H(X,\lambda)) = \Theta\left(\frac{1}{\sqrt{n}\lambda}\right) = \omega\left(\frac{1}{\sqrt{n}}\right)$$

which further implies

$$\begin{aligned}
\bar{\xi}_H(X,\lambda,n) &= e^{\frac{n\lambda^2\sigma_H^2(X,\lambda)}{2}}Q(\sqrt{n}\lambda\sigma_H(X,\lambda))\,(1+o(1)) \\
\underline{\xi}_H(X,\lambda,n) &= e^{\frac{n\lambda^2\sigma_H^2(X,\lambda)}{2}}Q(\sqrt{n}\lambda\sigma_H(X,\lambda))\,(1-o(1)).
\end{aligned}$$

Remark A.2. *Another interesting observation from the proof of Theorem A.2, especially (A.30), is the recursive relation between*

$$\begin{aligned}
\Pr\left\{-\frac{1}{n}\ln p(X^n) > H(X)+\delta\right\} &= \Pr\left\{\frac{-\ln p(X^n)-nH(X)}{\sqrt{n}\sigma_H(X)} > \frac{\delta}{\sqrt{n}\sigma_H(X)}\right\} \\
&\triangleq \bar{F}_{X,n}\left(\frac{\delta}{\sqrt{n}\sigma_H(X)}\right)
\end{aligned}$$

and

$$\bar{F}_{Z,n}(\rho) \stackrel{\Delta}{=} \bar{F}_n(\rho) = \Pr\left\{ \frac{-\ln p(Z^n) - n(H(X)+\delta)}{\sqrt{n}\sigma_H(X,\lambda)} > \rho \right\}.$$

As shown in the proof, a proper bound on $\bar{F}_{Z,n}(\rho)$ (using Berry-Esseen Central Limit Theorem) results in a bound (A.25) on $\bar{F}_{X,n}\left(\frac{\delta}{\sqrt{n}\sigma_H(X)}\right)$. To continue, we can apply this bound (A.25) on $\bar{F}_{Z,n}(\rho)$ to get another bound on $\bar{F}_{X,n}\left(\frac{\delta}{\sqrt{n}\sigma_H(X)}\right)$. Numerically, we can keep tightening the bound on $\bar{F}_{X,n}\left(\frac{\delta}{\sqrt{n}\sigma_H(X)}\right)$ in this recursive manner until no significant improvement can be made.

The probability that $-\frac{1}{n}\ln p(X^n)$ is away from $H(X)$ to the left can be bounded similarly. Define

$$\lambda_-^*(X) \stackrel{\Delta}{=} \sup\left\{ \lambda \geq 0 : \int p^{\lambda+1}(x)dx < \infty \right\}. \tag{A.38}$$

Suppose that

$$\lambda_-^*(X) > 0\,. \tag{A.39}$$

Define for any $\delta \geq 0$

$$r_{X,-}(\delta) \stackrel{\Delta}{=} \sup_{\lambda \geq 0}\left[\lambda(\delta - H(X)) - \ln \int p^{\lambda+1}(x)dx\right]$$

and for any $\lambda \in [0, \lambda_-^*(X))$

$$\delta_-(\lambda) \stackrel{\Delta}{=} \int \frac{p^{\lambda+1}(x)}{\left[\int p^{\lambda+1}(y)dy\right]} \left[\ln p(x)\right] dx + H(X)\,.$$

Then under the assumption (A.6), $\delta_-(\lambda)$ is strictly increasing over $\lambda \in [0, \lambda_-^*(X))$ with $\delta_-(0) = 0$. Let

$$\Delta_-^*(X) = \lim_{\lambda \uparrow \lambda_-^*(X)} \delta_-(\lambda)\,.$$

Following the proof of Theorem A.1, we have that $r_{X,-}(\delta)$ is strictly increasing, convex, and continuously differentiable up to at least the third order inclusive over $\delta \in [0, \Delta_-^*(X))$, and furthermore

$$r_{X,-}(\delta) = \lambda(\delta - H(X)) - \ln \int p^{\lambda+1}(x)dx$$

with $\lambda = r'_{X,-}(\delta)$ satisfying

$$\delta_-(\lambda) = \delta\,.$$

Define

$$\sigma^2_{H,-}(X,\lambda) \triangleq \int \frac{p^{\lambda+1}(x)}{\left[\int p^{\lambda+1}(y)dy\right]} \left|-\ln p(x) - (H(X) - \delta_-(\lambda))\right|^2 dx$$

and

$$M_{H,-}(X,\lambda) \triangleq \int \frac{p^{\lambda+1}(x)}{\left[\int p^{\lambda+1}(y)dy\right]} \left|-\ln p(x) - (H(X) - \delta_-(\lambda))\right|^3 dx \ .$$

In parallel with Theorems A.1 and A.2, we have the following result, which is referred to as the left NEP with respect to $H(X)$ and can be proved similarly.

Theorem A.3 (Left NEP)**.** *For any positive integer n,*

$$\Pr\left\{-\frac{1}{n}\ln p(X^n) \le H(X) - \delta\right\} \le e^{-nr_{X,-}(\delta)} \ . \tag{A.40}$$

Furthermore, under the assumptions (A.39) and (A.6), the following also hold:

(a) *There exists a $\delta^* > 0$ such that for any $\delta \in (0, \delta^*]$ and any positive integer n,*

$$r_{X,-}(\delta) = \frac{1}{2\sigma^2_H(X)}\delta^2 + O(\delta^3) \tag{A.41}$$

and hence

$$\Pr\left\{-\frac{1}{n}\ln p(X^n) \le H(X) - \delta\right\} \le e^{-n(\frac{\delta^2}{2\sigma^2_H(X)} + O(\delta^3))} \ . \tag{A.42}$$

(b) *For any $\delta \in (0, \Delta^*_-(X))$ and any positive integer n*

$$\bar{\xi}_{H,-}(X,\lambda,n)e^{-nr_{X,-}(\delta)} \ge \Pr\left\{-\frac{1}{n}\ln p(X^n) \le H(X) - \delta\right\} \ge \underline{\xi}_{H,-}(X,\lambda,n)e^{-nr_{X,-}(\delta)} \tag{A.43}$$

where $\lambda = r'_{X,-}(\delta) > 0$, and

$$\begin{aligned}\bar{\xi}_{H,-}(X,\lambda,n) &= \frac{2CM_{H,-}(X,\lambda)}{\sqrt{n}\sigma^3_{H,-}(X,\lambda)} \\ &\quad + e^{\frac{n\lambda^2\sigma^2_{H,-}(X,\lambda)}{2}}\left[Q(\sqrt{n}\lambda\sigma_{H,-}(X,\lambda)) - Q(\rho^* + \sqrt{n}\lambda\sigma_{H,-}(X,\lambda))\right] \qquad \text{(A.44)}\\ \underline{\xi}_{H,-}(X,\lambda,n) &= e^{\frac{n\lambda^2\sigma^2_{H,-}(X,\lambda)}{2}} Q(\rho_* + \sqrt{n}\lambda\sigma_{H,-}(X,\lambda)) \qquad \text{(A.45)}\end{aligned}$$

with $Q(\rho^*) = \frac{CM_{H,-}(X,\lambda)}{\sqrt{n}\sigma^3_{H,-}(X,\lambda)}$ and $Q(\rho_*) = \frac{1}{2} - \frac{2CM_{H,-}(X,\lambda)}{\sqrt{n}\sigma^3_{H,-}(X,\lambda)}$.

(c) *For any* $\delta \leq c\sqrt{\frac{\ln n}{n}}$, *where* $c < \sigma_H(X)$ *is a constant,*

$$\begin{aligned} Q\left(\frac{\delta\sqrt{n}}{\sigma_H(X)}\right) - \frac{CM_H(X)}{\sqrt{n}\sigma_H^3(X)} &\leq \Pr\left\{-\frac{1}{n}\ln p(X^n) \leq H(X) - \delta\right\} \\ &\leq Q\left(\frac{\delta\sqrt{n}}{\sigma_H(X)}\right) + \frac{CM_H(X)}{\sqrt{n}\sigma_H^3(X)}\,. \end{aligned} \tag{A.46}$$

Remarks similar to those (Remark A.1 and A.2) following Theorem A.2 can be drawn here concerning Theorem A.3.

A.2 NEP With Respect to Conditional Entropy

Consider now an IID source pair $(X, Y) = \{(X_i, Y_i)\}_{i=1}^{\infty}$ with finite conditional entropy $H(X|Y)$, where $H(X|Y)$ is the Shannon conditional entropy of X_i given Y_i if X is discrete, and the conditional differential entropy of X_i given Y_i if X is continuous. Let $p(x|y)$ be the conditional pmf or conditional pdf (as the case may be) of X_i given Y_i, and $p(y)$ the pmf or pdf (as the case may be) of Y_i. By replacing $-\frac{1}{n}\ln p(X^n)$ with $-\frac{1}{n}\ln p(X^n|Y^n)$, all results and arguments in Section A.1 can be carried over to this conditional case, yielding the NEP with respect to $H(X|Y)$.

Specifically, define

$$\lambda^*(X|Y) \triangleq \sup\left\{\lambda \geq 0 : \int p(y)\left[\int p^{-\lambda+1}(x|y)dx\right]dy < \infty\right\}. \tag{A.47}$$

Suppose that

$$\lambda^*(X|Y) > 0\,. \tag{A.48}$$

Let

$$\sigma_H^2(X|Y) \triangleq \int\int p(y)p(x|y)[-\ln p(x|y)]^2 dxdy - H^2(X|Y) \tag{A.49}$$

which will be referred to as the conditional information variance of X given Y. It is not hard to see that under the assumption (A.48),

$$\int\int \frac{p(y)p^{-\lambda+1}(x|y)}{\left[\int\int p(v)p^{-\lambda+1}(u|v)dudv\right]}\,|-\ln p(x|y)|^k\,dxdy < \infty \tag{A.50}$$

and

$$\int\int p(y)p^{-\lambda+1}(x|y)dxdy < \infty$$

for any $\lambda \in (0, \lambda^*(X|Y))$ and any positive integer k. Further assume that

$$\sigma_H^2(X|Y) > 0 \text{ and } \int\int p(y)p(x|y)|\ln p(x|y)|^3 dxdy < \infty \,. \tag{A.51}$$

Define for any $\delta \geq 0$

$$r_{X|Y}(\delta) \stackrel{\Delta}{=} \sup_{\lambda \geq 0} \left[\lambda(H(X|Y) + \delta) - \ln \int\int p(y)p^{-\lambda+1}(x|y)dxdy\right] \tag{A.52}$$

and for any $\lambda \in [0, \lambda^*(X|Y))$

$$\delta(\lambda) \stackrel{\Delta}{=} \int\int \frac{p(y)p^{-\lambda+1}(x|y)}{\left[\int\int p(v)p^{-\lambda+1}(u|v)dudv\right]} \left[-\ln p(x|y)\right] dxdy - H(X|Y) \,. \tag{A.53}$$

(Throughout this section, $\delta(\lambda)$ should be understood with its above definition.) Then under the assumptions (A.48) and (A.51), $\delta(\lambda)$ is strictly increasing over $\lambda \in [0, \lambda^*(X|Y))$ with $\delta(0) = 0$. Let

$$\Delta^*(X|Y) \stackrel{\Delta}{=} \lim_{\lambda \uparrow \lambda^*(X|Y)} \delta(\lambda) \,.$$

By an argument similar to that in the proof of Theorem A.1, it can be shown that $r_{X|Y}(\delta)$ is strictly increasing, convex and continuously differentiable up to at least the third order inclusive over $\delta \in [0, \Delta^*(X|Y))$, and furthermore $r_{X|Y}(\delta)$ has the following parametric expression

$$r_{X|Y}(\delta(\lambda)) = \lambda(H(X|Y) + \delta(\lambda)) - \ln \int\int p(y)p^{-\lambda+1}(x|y)dxdy \tag{A.54}$$

with $\delta(\lambda)$ defined in (A.53) and $\lambda = r'_{X|Y}(\delta)$. For any $\lambda \in [0, \lambda^*(X|Y))$, define

$$f_\lambda(x, y) \stackrel{\Delta}{=} \frac{p^{-\lambda}(x|y)}{\int\int p(v)p^{-\lambda+1}(u|v)dudv} \tag{A.55}$$

$$\sigma_H^2(X|Y, \lambda) \stackrel{\Delta}{=} \int\int f_\lambda(x, y)p(y)p(x|y) \left|-\ln p(x|y) - (H(X|Y) + \delta(\lambda))\right|^2 dxdy \tag{A.56}$$

$$M_H(X|Y, \lambda) \stackrel{\Delta}{=} \int\int f_\lambda(x, y)p(y)p(x|y) \left|-\ln p(x|y) - (H(X|Y) + \delta(\lambda))\right|^3 dxdy \tag{A.57}$$

where $\delta(\lambda)$ is defined in (A.53). Write $M_H(X|Y, 0)$ as $M_H(X|Y)$. It is easy to see that $\sigma_H^2(X|Y, 0) = \sigma_H^2(X|Y)$, $\sigma_H^2(X|Y, \lambda) = \delta'(\lambda)$, and

$$M_H(X|Y) = \int\int p(y)p(x|y) \left|-\ln p(x|y) - H(X|Y))\right|^3 dxdy \,. \tag{A.58}$$

In parallel with Theorems A.1 and A.2, we have the following result, which is referred to as the right NEP with respect to $H(X|Y)$ and can be proved similarly.

Theorem A.4 (Right NEP With Respect to $H(X|Y)$)**.** *For any positive integer n,*

$$\Pr\left\{-\frac{1}{n}\ln p(X^n|Y^n) > H(X|Y)+\delta\right\} \le e^{-nr_{X|Y}(\delta)} \tag{A.59}$$

where $X^n = X_1X_2\cdots X_n$ and $Y^n = Y_1Y_2\cdots Y_n$. Moreover, under the assumptions (A.48) and (A.51), the following also hold:

(a) *There exists a $\delta^* > 0$ such that for any $\delta \in (0,\delta^*]$ and any positive integer n,*

$$r_{X|Y}(\delta) = \frac{1}{2\sigma_H^2(X|Y)}\delta^2 + O(\delta^3) \tag{A.60}$$

and hence

$$\Pr\left\{-\frac{1}{n}\ln p(X^n|Y^n) > H(X|Y)+\delta\right\} \le e^{-n(\frac{\delta^2}{2\sigma_H^2(X|Y)}+O(\delta^3))}. \tag{A.61}$$

(b) *For any $\delta \in (0,\Delta^*(X|Y))$ and any positive integer n*

$$\begin{aligned}\underline{\xi}_H(X|Y,\lambda,n)e^{-nr_{X|Y}(\delta)} &\le \Pr\left\{-\frac{1}{n}\ln p(Y^n|X^n) > H(X|Y)+\delta\right\}\\ &\le \bar{\xi}_H(X|Y,\lambda,n)e^{-nr_{X|Y}(\delta)}\end{aligned} \tag{A.62}$$

where $\lambda = r'_{X|Y}(\delta) > 0$, and

$$\begin{aligned}\bar{\xi}_H(X|Y,\lambda,n) &= \frac{2CM_H(X|Y,\lambda)}{\sqrt{n}\sigma_H^3(X|Y,\lambda)}\\ &\quad + e^{\frac{n\lambda^2\sigma_H^2(X|Y,\lambda)}{2}}\left[Q(\sqrt{n}\lambda\sigma_H(X|Y,\lambda)) - Q(\rho^*+\sqrt{n}\lambda\sigma_H(X|Y,\lambda))\right]\end{aligned} \tag{A.63}$$

$$\underline{\xi}_H(X|Y,\lambda,n) = e^{\frac{n\lambda^2\sigma_H^2(X|Y,\lambda)}{2}}Q(\rho_*+\sqrt{n}\lambda\sigma_H(X|Y,\lambda)) \tag{A.64}$$

with $Q(\rho^*) = \frac{CM_H(X|Y,\lambda)}{\sqrt{n}\sigma_H^3(X|Y,\lambda)}$ and $Q(\rho_*) = \frac{1}{2} - \frac{2CM_H(X|Y,\lambda)}{\sqrt{n}\sigma_H^3(X|Y,\lambda)}$.

(c) *For any $\delta \le c\sqrt{\frac{\ln n}{n}}$, where $c < \sigma_H(X|Y)$ is a constant,*

$$\begin{aligned}Q\left(\frac{\delta\sqrt{n}}{\sigma_H(X|Y)}\right) - \frac{CM_H(X|Y)}{\sqrt{n}\sigma_H^3(X|Y)} &\le \Pr\left\{-\frac{1}{n}\ln p(X^n|Y^n) > H(X|Y)+\delta\right\}\\ &\le Q\left(\frac{\delta\sqrt{n}}{\sigma_H(X|Y)}\right) + \frac{CM_H(X|Y)}{\sqrt{n}\sigma_H^3(X|Y)}.\end{aligned} \tag{A.65}$$

The probability that $-\frac{1}{n}\ln p(X^n|Y^n)$ is away from $H(X|Y)$ to the left can be bounded similarly. For completeness, we state the result without proof again. Define

$$\lambda_-^*(X|Y) \stackrel{\Delta}{=} \sup\left\{\lambda \geq 0 : \int\int p(y)p^{\lambda+1}(x|y)dxdy < \infty\right\} . \tag{A.66}$$

Suppose that

$$\lambda_-^*(X|Y) > 0 . \tag{A.67}$$

Define for any $\delta \geq 0$

$$r_{X|Y,-}(\delta) \stackrel{\Delta}{=} \sup_{\lambda\geq 0}\left[\lambda(\delta - H(X|Y)) - \ln\int\int p(y)p^{\lambda+1}(x|y)dxdy\right]$$

and for any $\lambda \in [0, \lambda_-^*(X|Y))$

$$\delta_-(\lambda) \stackrel{\Delta}{=} \int\int \frac{p(y)p^{\lambda+1}(x|y)}{\left[\int\int p(v)p^{\lambda+1}(u|v)dudv\right]}\left[\ln p(x|y)\right]dxdy + H(X|Y) .$$

(Throughout this section, $\delta_-(\lambda)$ should be understood with its above definition.) Then under the assumption (A.51), $\delta_-(\lambda)$ is strictly increasing over $\lambda \in [0, \lambda_-^*(X|Y))$ with $\delta_-(0) = 0$. Let

$$\Delta_-^*(X|Y) = \lim_{\lambda\uparrow\lambda_-^*(X|Y)} \delta_-(\lambda) .$$

By using an argument similar to that in the proof of Theorem A.1, it can be shown that $r_{X|Y,-}(\delta)$ is strictly increasing, convex, and continuously differentiable up to at least the third order inclusive over $\delta \in [0, \Delta_-^*(X|Y))$, and furthermore $r_{X|Y,-}(\delta)$ has the following parametric expression

$$r_{X|Y,-}(\delta_-(\lambda)) = \lambda(\delta_-(\lambda) - H(X|Y)) - \ln\int\int p(y)p^{\lambda+1}(x|y)dxdy$$

with $\lambda = r'_{X|Y,-}(\delta)$ satisfying

$$\delta_-(\lambda) = \delta .$$

Define

$$\sigma_{H,-}^2(X|Y,\lambda) \stackrel{\Delta}{=} \int\int \frac{p(y)p^{\lambda+1}(x|y)}{\left[\int\int p(v)p^{\lambda+1}(u|v)dudv\right]}\left|-\ln p(x|y) - (H(X|Y) - \delta_-(\lambda))\right|^2 dxdy$$

and

$$M_{H,-}(X|Y,\lambda) \stackrel{\Delta}{=} \int\int \frac{p(y)p^{\lambda+1}(x|y)}{\left[\int\int p(v)p^{\lambda+1}(u|v)dudv\right]}\left|-\ln p(x|y) - (H(X|Y) - \delta_-(\lambda))\right|^3 dxdy .$$

In parallel with Theorem A.3, we have the following result, which is referred to as the left NEP with respect to $H(X|Y)$ and can be proved similarly.

Theorem A.5 (Left NEP With Respect to $H(X|Y)$)**.** *For any positive integer n,*

$$\Pr\left\{-\frac{1}{n}\ln p(X^n|Y^n) \le H(X|Y) - \delta\right\} \le e^{-nr_{X|Y,-}(\delta)} . \tag{A.68}$$

Furthermore, under the assumptions (A.67) and (A.51), the following also hold:

(a) *There exists a $\delta^* > 0$ such that for any $\delta \in (0, \delta^*]$ and any positive integer n,*

$$r_{X|Y,-}(\delta) = \frac{1}{2\sigma_H^2(X|Y)}\delta^2 + O(\delta^3) \tag{A.69}$$

and hence

$$\Pr\left\{-\frac{1}{n}\ln p(X^n|Y^n) \le H(X|Y) - \delta\right\} \le e^{-n(\frac{\delta^2}{2\sigma_H^2(X|Y)}+O(\delta^3))} . \tag{A.70}$$

(b) *For any $\delta \in (0, \Delta_-^*(X|Y))$ and any positive integer n*

$$\begin{aligned}\underline{\xi}_{H,-}(X|Y,\lambda,n)e^{-nr_{X|Y,-}(\delta)} &\le \Pr\left\{-\frac{1}{n}\ln p(Y^n|X^n) \le H(X|Y) - \delta\right\} \\ &\le \bar{\xi}_{H,-}(X|Y,\lambda,n)e^{-nr_{X|Y,-}(\delta)}\end{aligned} \tag{A.71}$$

where $\lambda = r'_{X|Y,-}(\delta) > 0$, and

$$\begin{aligned}\bar{\xi}_{H,-}(X|Y,\lambda,n) &= \frac{2CM_{H,-}(X|Y,\lambda)}{\sqrt{n}\sigma_{H,-}^3(X|Y,\lambda)} \\ &\quad + e^{\frac{n\lambda^2\sigma_{H,-}^2(X|Y,\lambda)}{2}}\left[Q(\sqrt{n}\lambda\sigma_{H,-}(X|Y,\lambda)) - Q(\rho^* + \sqrt{n}\lambda\sigma_{H,-}(X|Y,\lambda))\right]\end{aligned} \tag{A.72}$$

$$\underline{\xi}_{H,-}(X|Y,\lambda,n) = e^{\frac{n\lambda^2\sigma_{H,-}^2(X|Y,\lambda)}{2}}Q(\rho_* + \sqrt{n}\lambda\sigma_{H,-}(X|Y,\lambda)) \tag{A.73}$$

with $Q(\rho^*) = \frac{CM_{H,-}(X|Y,\lambda)}{\sqrt{n}\sigma_{H,-}^3(X|Y,\lambda)}$ and $Q(\rho_*) = \frac{1}{2} - \frac{2CM_{H,-}(X|Y,\lambda)}{\sqrt{n}\sigma_{H,-}^3(X|Y,\lambda)}$.

(c) *For any $\delta \le c\sqrt{\frac{\ln n}{n}}$, where $c < \sigma_H(X|Y)$ is a constant,*

$$\begin{aligned}Q\left(\frac{\delta\sqrt{n}}{\sigma_H(X|Y)}\right) - \frac{CM_H(X|Y)}{\sqrt{n}\sigma_H^3(X|Y)} &\le \Pr\left\{-\frac{1}{n}\ln p(X^n|Y^n) \le H(X|Y) - \delta\right\} \\ &\le Q\left(\frac{\delta\sqrt{n}}{\sigma_H(X|Y)}\right) + \frac{CM_H(X|Y)}{\sqrt{n}\sigma_H^3(X|Y)} .\end{aligned} \tag{A.74}$$

Remarks similar to those (Remark A.1 and A.2) following Theorem A.2 can be drawn here concerning Theorem A.4 and A.5.

We conclude this section by illustrating $r_{X|Y}(\delta)$ and $\sigma_H^2(X|Y)$ when X and Y are the uniform input and the corresponding output of the binary symmetric channel (BSC) and the binary input Gaussian channel.

Example 1 (BSC): Combining (A.53) and (A.54), it is not hard to verify that

$$\begin{aligned} r_{X|Y}(\delta(\lambda)) &= \int\int p(x,y) f_\lambda(x,y) \ln f_\lambda(x,y) dxdy \\ &= \int\int p(x,y) f_\lambda(x,y) \ln \frac{p(x|y) f_\lambda(x,y)}{p(x|y)} dxdy \\ &\triangleq D(p(x|y) f_\lambda(x,y) || p(x|y)) \end{aligned} \tag{A.75}$$

For BSC, simple calculation reveals that

$$p(x|y) = \begin{cases} 1-p & \text{if } x = y \\ p & \text{otherwise} \end{cases} \tag{A.76}$$

and

$$p(x|y) f_\lambda(x,y) = \begin{cases} \frac{(1-p)^{-\lambda+1}}{p^{-\lambda+1}+(1-p)^{-\lambda+1}} & \text{if } x = y \\ \frac{p^{-\lambda+1}}{p^{-\lambda+1}+(1-p)^{-\lambda+1}} & \text{otherwise} \end{cases} \tag{A.77}$$

By defining

$$D(q||p) \triangleq (1-q) \ln \frac{1-q}{1-p} + q \ln \frac{q}{p}$$

and (A.75), we have

$$\begin{aligned} r_{X|Y}(\delta(\lambda)) &= D\left(\frac{p^{-\lambda+1}}{p^{-\lambda+1}+(1-p)^{-\lambda+1}} \middle\| p \right) \\ &= D\left(p + \frac{p(1-p)(p^{-\lambda}-(1-p)^{-\lambda})}{p^{-\lambda+1}+(1-p)^{-\lambda+1}} \middle\| p \right). \end{aligned} \tag{A.78}$$

On the other hand, by substituting (A.76) and (A.77) into (A.53),

$$\delta(\lambda) = \frac{p(1-p)(p^{-\lambda}-(1-p)^{-\lambda})}{p^{-\lambda+1}+(1-p)^{-\lambda+1}} \ln \frac{1-p}{p} \tag{A.79}$$

and eventually, we have

$$r_{X|Y}(\delta) = D\left(p + \frac{\delta}{\ln \frac{1-p}{p}} \middle\| p \right) \tag{A.80}$$

and plugging (A.76) into (A.56) with $\lambda = 0$ yields

$$\begin{aligned}\sigma_H^2(X|Y) &= (1-p)\ln^2(1-p) + p\ln^2 p - [-p\ln p - (1-p)\ln(1-p)]^2 \\ &= p(1-p)\ln^2\frac{1-p}{p} \end{aligned} \tag{A.81}$$

Moreover, as $\mathcal{X}$ and $\mathcal{Y}$ are both finite alphabets, it is easy to show that $\lambda^*(X|Y) = \infty$, where $\lambda^*(X|Y)$ is defined in (A.47). Then

$$\Delta^*(X|Y) = \lim_{\lambda\uparrow+\infty}\delta(\lambda) = (1-p)\ln\frac{1-p}{p} \tag{A.82}$$

and

$$r_{\max} \stackrel{\Delta}{=} \lim_{\delta\uparrow\Delta^*(X|Y)} r_{X|Y}(\delta) = -\ln p \tag{A.83}$$

Based on Theorem A.4, $\Delta^*(X|Y)$ and $r_{\max}$ can be interpreted in the following way. As

$$\max_{x^n,y^n} -\frac{1}{n}\ln p(x^n|y^n) = -\ln p,$$

then

$$\begin{aligned}\lim_{\delta\to\Delta^*(X|Y)} \Pr\left\{-\frac{1}{n}\ln p(X^n|Y^n) > H(X|Y)+\delta\right\} &= \Pr\left\{-\frac{1}{n}\ln p(X^n|Y^n) = -\ln p\right\} \\ &= p^n = e^{n\ln p} = e^{-nr_{\max}}.\end{aligned}$$

In addition, for $\delta \geq \Delta^*(X|Y)$,

$$\Pr\left\{-\frac{1}{n}\ln p(X^n|Y^n) > H(X|Y)+\delta\right\} = 0.$$

By adopting the convention that $0\ln 0 = 0$ and $e^{-\infty} = 0$,

$$r_{X|Y}(\delta) = \begin{cases} D\left(p + \frac{\delta}{\ln\frac{1-p}{p}} \middle\| p\right) & \text{if } \delta \in [0, \Delta^*(X|Y)) \\ +\infty & \text{if } \delta \geq \Delta^*(X|Y) \end{cases}. \tag{A.84}$$

A sample plot of $r_{X|Y}(\delta)$ is provided in Figure A.1 when $p = 0.10$.

Example 2 (Binary Input Gaussian Channel): Without loss of generality, we assume that the input of channel is modulated to $\{+1, -1\}$, and therefore

$$p(y|x) = \frac{1}{\sqrt{2\pi}\sigma}e^{-\frac{|y-x|^2}{2\sigma^2}} \tag{A.85}$$

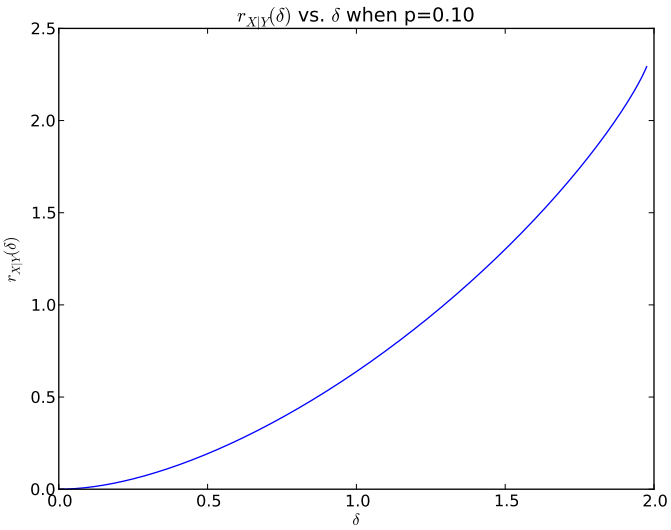


Figure A.1: $r_{X|Y}(\delta)$ for BSC

for $x = \{+1, -1\}$, where σ^2 is the variance of the noise. Calculation of $r_{X|Y}(\delta)$ and $\sigma_H^2(X|Y)$ is much more involved than that for BSC. Tedious evaluation is omitted here with results presented as follows. Let U be a standard Gaussian random variable, i.e.

$$p(u) = \frac{1}{\sqrt{2\pi}} e^{-\frac{|u|^2}{2}}$$

and define

$$g(x) \stackrel{\Delta}{=} 1 + e^{-2x}.$$

Then

$$\delta(\lambda) = \frac{\mathbb{E}\left[g^\lambda\left(\frac{\sigma U+1}{\sigma^2}\right)\ln g\left(\frac{\sigma U+1}{\sigma^2}\right)\right]}{\mathbb{E}\left[g^\lambda\left(\frac{\sigma U+1}{\sigma^2}\right)\right]} - \mathbb{E}\left[\ln g\left(\frac{\sigma U+1}{\sigma^2}\right)\right] \tag{A.86}$$

$$r_{X|Y}(\delta(\lambda)) = \lambda\frac{\mathbb{E}\left[g^\lambda\left(\frac{\sigma U+1}{\sigma^2}\right)\ln g\left(\frac{\sigma U+1}{\sigma^2}\right)\right]}{\mathbb{E}\left[g^\lambda\left(\frac{\sigma U+1}{\sigma^2}\right)\right]} - \ln\left\{\mathbb{E}\left[g^\lambda\left(\frac{\sigma U+1}{\sigma^2}\right)\right]\right\} \tag{A.87}$$

and

$$\sigma_H^2(X|Y) = \mathbb{E}\left[\ln^2 g\left(\frac{\sigma U+1}{\sigma^2}\right)\right] - \left\{\mathbb{E}\left[-\ln g\left(\frac{\sigma U+1}{\sigma^2}\right)\right]\right\}^2 \tag{A.88}$$

To get better understanding of those quantities, let us first determine $\lambda^*(X|Y)$ and $\Delta^*(X|Y)$. In fact, we can show that $\lambda^*(X|Y) = \infty$ by verifying that

$$\int p(y) \left[\sum_{x \in \mathcal{X}} p^{-\lambda+1}(x|y) \right] dy < \infty$$

for any finite $\lambda \geq 0$. Towards this, observe that

$$\int p(y) \left[\sum_{x \in \mathcal{X}} p^{-\lambda+1}(x|y) \right] dy$$

is an increasing function with respect to λ since $p(x|y) \leq 1$ for any x and y. Therefore,

$$\begin{aligned} \int p(y) \left[\sum_{x \in \mathcal{X}} p^{-\lambda+1}(x|y) \right] dy &= \mathbb{E}\left[g^{\lambda}\left(\frac{\sigma U + 1}{\sigma^2} \right) \right] \\ &\leq \mathbb{E}\left[g^{\lceil \lambda \rceil}\left(\frac{\sigma U + 1}{\sigma^2} \right) \right] < \infty \end{aligned}$$

as

$$\mathbb{E}[e^{sU}] = e^{\frac{s^2}{2}} < \infty$$

for any finite s. Now let us show the claim $\Delta^*(X|Y) = \infty$. According to (A.86),

$$\begin{aligned} \delta(\lambda) &= \frac{\mathbb{E}\left[g^{\lambda}\left(\frac{\sigma U+1}{\sigma^2}\right) \ln g\left(\frac{\sigma U+1}{\sigma^2}\right) \right]}{\mathbb{E}\left[g^{\lambda}\left(\frac{\sigma U+1}{\sigma^2}\right) \right]} - \mathbb{E}\left[\ln g\left(\frac{\sigma U + 1}{\sigma^2} \right) \right] \\ &= \frac{d}{d\lambda} \ln \mathbb{E}\left[g^{\lambda}\left(\frac{\sigma U + 1}{\sigma^2} \right) \right] - H(X|Y) \end{aligned}$$

As $H(X|Y)$ is a constant and always less than $\ln 2$, the claim $\Delta^*(X|Y) = \infty$ is equivalent to show

$$\frac{d}{d\lambda} \ln \mathbb{E}\left[g^{\lambda}\left(\frac{\sigma U + 1}{\sigma^2} \right) \right]$$

is unbounded when $\lambda \to \infty$. By the fact that $\delta(\lambda)$ is an increasing function of λ, which also implies that so is

$$\frac{d}{d\lambda} \ln \mathbb{E}\left[g^{\lambda}\left(\frac{\sigma U + 1}{\sigma^2} \right) \right],$$

we only have to verify that

$$\frac{\ln \mathbb{E}\left[g^{k+1}\left(\frac{\sigma U+1}{\sigma^2}\right) \right] - \ln \mathbb{E}\left[g^{k}\left(\frac{\sigma U+1}{\sigma^2}\right) \right]}{k+1-k} = \ln \frac{\mathbb{E}\left[g^{k+1}\left(\frac{\sigma U+1}{\sigma^2}\right) \right]}{\mathbb{E}\left[g^{k}\left(\frac{\sigma U+1}{\sigma^2}\right) \right]}$$

or simply

$$\frac{\mathbb{E}\left[g^{k+1}\left(\frac{\sigma U+1}{\sigma^2}\right)\right]}{\mathbb{E}\left[g^{k}\left(\frac{\sigma U+1}{\sigma^2}\right)\right]}$$

is unbounded when $k \to \infty$, which is indeed the case as

$$\begin{aligned}
\frac{\mathbb{E}\left[g^{k+1}\left(\frac{\sigma U+1}{\sigma^2}\right)\right]}{\mathbb{E}\left[g^{k}\left(\frac{\sigma U+1}{\sigma^2}\right)\right]} &= \frac{\sum_{i=0}^{k+1}\binom{k+1}{i}e^{\frac{2i^2-2i}{\sigma^2}}}{\sum_{i=0}^{k}\binom{k}{i}e^{\frac{2i^2-2i}{\sigma^2}}} \\
&= \frac{\Theta\left(e^{\frac{2(k+1)^2-2(k+1)}{\sigma^2}}\right)}{\Theta\left(e^{\frac{2k^2-2k}{\sigma^2}}\right)} \\
&= \Theta\left(e^{\frac{4k}{\sigma^2}}\right) \to \infty
\end{aligned}$$

as $k \to \infty$. And consequently, it is not hard to see that

$$r_{X|Y}(\delta) \to \infty$$

as $\delta \to \infty$. The interpretation based on Theorem A.4 is as follows:

$$-\frac{1}{n}\ln p(x^n|y^n) - H(X|Y)$$

can approach ∞ for proper choice of x^n and y^n, but

$$\lim_{\delta\to\infty}\Pr\left\{-\frac{1}{n}\ln p(X^n|Y^n) > H(X|Y)+\delta\right\} = e^{-\infty} = 0.$$

Figure A.2 shows a sample plot of $r_{X|Y}(\delta)$ for BIGC with $\sigma = 1.0$.

A.3 NEP With Respect to Mutual Information and Relative Entropy

Consider now an IID source pair $(X,Y) = \{(X_i,Y_i)\}_{i=1}^{\infty}$ with finite mutual information $I(X;Y) > 0$. Let $p(y|x)$ be the conditional pmf or pdf (as the case may be) of Y_i given X_i. In this section, we extend the NEP to $I(X;Y)$ and relative entropy.

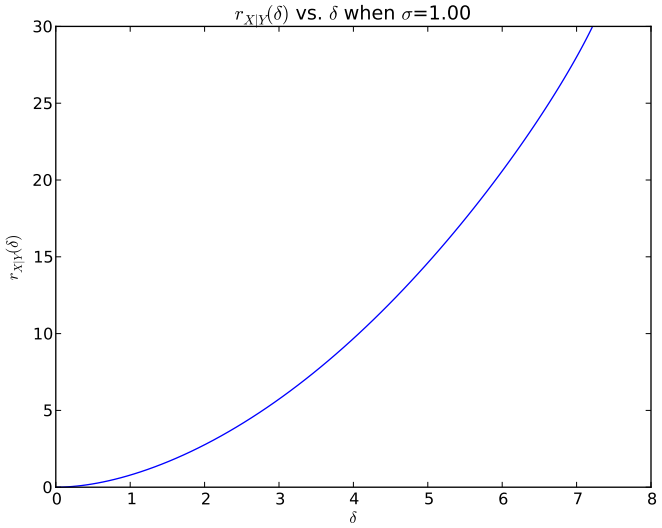


Figure A.2: $r_{X|Y}(\delta)$ for BIGC

A.3.1 NEP With Respect to $I(X;Y)$

We begin with the left NEP with respect to $I(X;Y)$. Define

$$\lambda_{-}^{*}(X;Y) \stackrel{\Delta}{=} \sup\left\{\lambda \geq 0 : \int\int p(x,y)\left[\frac{p(y|x)}{p(y)}\right]^{-\lambda} dxdy < \infty\right\} . \tag{A.89}$$

Suppose that

$$\lambda_{-}^{*}(X;Y) > 0 . \tag{A.90}$$

Let

$$\sigma_I^2(X;Y) \stackrel{\Delta}{=} \int\int p(x,y)\left[\ln\frac{p(y|x)}{p(y)}\right]^2 dxdy - I^2(X;Y) \tag{A.91}$$

which will be referred to as the mutual information variance of X and Y. It is not hard to see that under the assumption (A.90),

$$\int\int \frac{p(x,y)\left[\frac{p(y|x)}{p(y)}\right]^{-\lambda}}{\left[\int\int p(u,v)\left[\frac{p(v|u)}{p(v)}\right]^{-\lambda} dudv\right]}\left|-\ln\frac{p(y|x)}{p(y)}\right|^k dxdy < \infty \tag{A.92}$$

and

$$\int\int p(x,y)\left[\frac{p(y|x)}{p(y)}\right]^{-\lambda} dxdy < \infty$$

for any $\lambda \in (0, \lambda_-^*(X;Y))$ and any positive integer k. Further assume that

$$\sigma_I^2(X;Y) > 0 \text{ and } \int\int p(x,y)\left|\ln\frac{p(y|x)}{p(y)}\right|^3 dxdx < \infty. \tag{A.93}$$

Define for any $\delta \geq 0$

$$r_{X;Y,-}(\delta) \stackrel{\Delta}{=} \sup_{\lambda\geq 0}\left[\lambda(\delta - I(X;Y)) - \ln\int\int p(x,y)\left[\frac{p(y|x)}{p(y)}\right]^{-\lambda} dxdy\right] \tag{A.94}$$

and for any $\lambda \in [0, \lambda_-^*(X;Y))$

$$f_{-\lambda}(x,y) \stackrel{\Delta}{=} \frac{\left[\frac{p(y|x)}{p(y)}\right]^{-\lambda}}{\int\int p(u,v)\left[\frac{p(v|u)}{p(v)}\right]^{-\lambda} dudv} \tag{A.95}$$

$$\delta_-(\lambda) \stackrel{\Delta}{=} \int\int p(x,y) f_{-\lambda}(x,y)\left[-\ln\frac{p(y|x)}{p(y)}\right] dxdy + I(X;Y)\ . \tag{A.96}$$

(Throughout this section, $\delta_-(\lambda)$ should be understood with its above definition.) Then under the assumptions (A.90) and (A.93), $\delta_-(\lambda)$ is strictly increasing over $\lambda \in [0, \lambda_-^*(X;Y))$ with $\delta_-(0) = 0$. Let

$$\Delta_-^*(X;Y) \stackrel{\Delta}{=} \lim_{\lambda\uparrow\lambda_-^*(X;Y)} \delta_-(\lambda)\ .$$

By an argument similar to that in the proof of Theorem A.1, it can be shown that $r_{X;Y,-}(\delta)$ is strictly increasing, convex and continuously differentiable up to at least the third order inclusive over $\delta \in [0, \Delta_-^*(X;Y))$, and furthermore $r_{X;Y,-}(\delta)$ has the following parametric expression

$$r_{X;Y,-}(\delta_-(\lambda)) = \lambda(\delta_-(\lambda) - I(X;Y)) - \ln\int\int p(x,y)\left[\frac{p(y|x)}{p(y)}\right]^{-\lambda} dxdy \tag{A.97}$$

with $\lambda = r'_{X;Y,-}(\delta)$ satisfying

$$\delta_-(\lambda) = \delta\ .$$

Further define for any $\lambda \in [0, \lambda^*_-(X;Y))$

$$\sigma^2_{I,-}(X;Y,\lambda) \triangleq \int\int f_{-\lambda}(x,y)p(x,y)\left|\ln\frac{p(y|x)}{p(y)} - (I(X;Y)-\delta_-(\lambda))\right|^2 dxdy \tag{A.98}$$

$$M_{I,-}(X;Y,\lambda) \triangleq \int\int f_{-\lambda}(x,y)p(x,y)\left|\ln\frac{p(y|x)}{p(y)} - (I(X;Y)-\delta_-(\lambda))\right|^3 dxdy\,. \tag{A.99}$$

Write $M_{I,-}(X;Y,0)$ simply as $M_I(X;Y)$. It is easy to see that $\sigma^2_{I,-}(X;Y,0) = \sigma^2_I(X;Y)$, $\sigma^2_{I,-}(X;Y,\lambda) = \delta'_-(\lambda)$, and

$$M_I(X;Y) = \int\int p(x,y)\left|\ln\frac{p(y|x)}{p(y)} - I(X;Y))\right|^3 dxdy\,. \tag{A.100}$$

In parallel with Theorems A.3 and A.5, we have the following result, which is referred to as the left NEP with respect to $I(X;Y)$ and can be proved similarly.

Theorem A.6 (Left NEP With Respect to $I(X;Y)$)**.** *For any positive integer n,*

$$\Pr\left\{\frac{1}{n}\ln\frac{p(Y^n|X^n)}{p(Y^n)} \le I(X;Y)-\delta\right\} \le e^{-nr_{X;Y,-}(\delta)}\,. \tag{A.101}$$

Furthermore, under the assumptions (A.90) and (A.93), the following also hold:

(a) *There exists a $\delta^* > 0$ such that for any $\delta \in (0,\delta^*]$ and any positive integer n,*

$$r_{X;Y,-}(\delta) = \frac{1}{2\sigma^2_I(X;Y)}\delta^2 + O(\delta^3) \tag{A.102}$$

and hence

$$\Pr\left\{\frac{1}{n}\ln\frac{p(Y^n|X^n)}{p(Y^n)} \le I(X;Y)-\delta\right\} \le e^{-n(\frac{\delta^2}{2\sigma^2_I(X;Y)}+O(\delta^3))}\,. \tag{A.103}$$

(b) *For any $\delta \in (0, \Delta^*_-(X;Y))$ and any positive integer n*

$$\begin{aligned}\underline{\xi}_{I,-}(X;Y,\lambda,n)e^{-nr_{X;Y,-}(\delta)} &\le \Pr\left\{\frac{1}{n}\ln\frac{p(Y^n|X^n)}{p(Y^n)} \le I(X;Y)-\delta\right\}\\ &\le \bar{\xi}_{I,-}(X;Y,\lambda,n)e^{-nr_{X;Y,-}(\delta)}\end{aligned} \tag{A.104}$$

where $\lambda = r'_{X;Y,-}(\delta) > 0$, *and*

$$\bar{\xi}_{I,-}(X;Y,\lambda,n) = \frac{2CM_{I,-}(X;Y,\lambda)}{\sqrt{n}\sigma^3_{I,-}(X;Y,\lambda)} + e^{\frac{n\lambda^2\sigma^2_{I,-}(X;Y,\lambda)}{2}}\left[Q(\sqrt{n}\lambda\sigma_{I,-}(X;Y,\lambda)) - Q(\rho^* + \sqrt{n}\lambda\sigma_{I,-}(X;Y,\lambda))\right] \quad \text{(A.105)}$$

$$\underline{\xi}_{I,-}(X;Y,\lambda,n) = e^{\frac{n\lambda^2\sigma^2_{I,-}(X;Y,\lambda)}{2}}Q(\rho_* + \sqrt{n}\lambda\sigma_{I,-}(X;Y,\lambda)) \quad \text{(A.106)}$$

with $Q(\rho^*) = \frac{CM_{I,-}(X;Y,\lambda)}{\sqrt{n}\sigma^3_{I,-}(X;Y,\lambda)}$ *and* $Q(\rho_*) = \frac{1}{2} - \frac{2CM_{I,-}(X;Y,\lambda)}{\sqrt{n}\sigma^3_{I,-}(X;Y,\lambda)}$.

(c) *For any* $\delta \leq c\sqrt{\frac{\ln n}{n}}$, *where* $c < \sigma_I(X;Y)$ *is a constant,*

$$\begin{aligned} Q\left(\frac{\delta\sqrt{n}}{\sigma_I(X;Y)}\right) - \frac{CM_I(X;Y)}{\sqrt{n}\sigma^3_I(X;Y)} &\leq \Pr\left\{\frac{1}{n}\ln\frac{p(Y^n|X^n)}{p(Y^n)} \leq I(X;Y) - \delta\right\} \\ &\leq Q\left(\frac{\delta\sqrt{n}}{\sigma_I(X;Y)}\right) + \frac{CM_I(X;Y)}{\sqrt{n}\sigma^3_I(X;Y)}. \end{aligned} \quad \text{(A.107)}$$

The probability that $\frac{1}{n}\ln\frac{p(Y^n|X^n)}{p(Y^n)}$ is away from $I(X;Y)$ to the right can be bounded in a similar manner. For completeness, we state these bounds again without proof. Define

$$\lambda^*(X;Y) \stackrel{\Delta}{=} \sup\left\{\lambda \geq 0 : \int\int p(x,y)\left[\frac{p(y|x)}{p(y)}\right]^\lambda dxdy < \infty\right\}. \quad \text{(A.108)}$$

Suppose that

$$\lambda^*(X;Y) > 0\,. \quad \text{(A.109)}$$

Define for any $\delta \geq 0$

$$r_{X;Y}(\delta) \stackrel{\Delta}{=} \sup_{\lambda\geq 0}\left[\lambda(I(X;Y)+\delta) - \ln\int\int p(x,y)\left[\frac{p(y|x)}{p(y)}\right]^\lambda dxdy\right] \quad \text{(A.110)}$$

and for any $\lambda \in [0, \lambda^*(X;Y))$

$$f_\lambda(x,y) \stackrel{\Delta}{=} \frac{\left[\frac{p(y|x)}{p(y)}\right]^\lambda}{\int\int p(u,v)\left[\frac{p(v|u)}{p(v)}\right]^\lambda dudv} \quad \text{(A.111)}$$

$$\delta(\lambda) \triangleq \int\int p(x,y) f_\lambda(x,y) \left[\ln \frac{p(y|x)}{p(y)}\right] dxdy - I(X;Y) \ . \tag{A.112}$$

(Throughout this section, $\delta(\lambda)$ should be understood with its above definition.) Then under the assumptions (A.109) and (A.93), $\delta(\lambda)$ is strictly increasing over $\lambda \in [0, \lambda^*(X;Y))$ with $\delta(0) = 0$. Let

$$\Delta^*(X;Y) \triangleq \lim_{\lambda \uparrow \lambda^*(X;Y)} \delta(\lambda) \ .$$

By an argument similar to that in the proof of Theorem A.1, it can be shown that $r_{X;Y}(\delta)$ is strictly increasing, convex and continuously differentiable up to at least the third order over $\delta \in [0, \Delta^*(X;Y))$, and furthermore $r_{X;Y}(\delta)$ has the following parametric expression

$$r_{X;Y}(\delta(\lambda)) = \lambda(I(X;Y) + \delta(\lambda)) - \ln \int\int p(x,y) \left[\frac{p(y|x)}{p(y)}\right]^\lambda dxdy \tag{A.113}$$

with $\lambda = r'_{X;Y}(\delta)$ satisfying

$$\delta(\lambda) = \delta \ .$$

Further define for any $\lambda \in [0, \lambda^*(X;Y))$

$$\sigma_I^2(X;Y,\lambda) \triangleq \int\int f_\lambda(x,y) p(x,y) \left| \ln \frac{p(y|x)}{p(y)} - (I(X;Y) + \delta(\lambda)) \right|^2 dxdy \tag{A.114}$$

$$M_I(X;Y,\lambda) \triangleq \int\int f_\lambda(x,y) p(x,y) \left| \ln \frac{p(y|x)}{p(y)} - (I(X;Y) + \delta(\lambda)) \right|^3 dxdy \ . \tag{A.115}$$

It is easy to see that $\sigma_I^2(X;Y,0) = \sigma_I^2(X;Y)$ and $\sigma_I^2(X;Y,\lambda) = \delta'(\lambda)$.

In parallel with Theorems A.1, A.2, and A.4, we have the following result, which is referred to as the right NEP with respect to $I(X;Y)$ and can be proved similarly.

Theorem A.7 (Right NEP With Respect to $I(X;Y)$)**.** *For any positive integer n,*

$$\Pr\left\{\frac{1}{n} \ln \frac{p(Y^n|X^n)}{p(Y^n)} > I(X;Y) + \delta\right\} \le e^{-n r_{X;Y}(\delta)} \ . \tag{A.116}$$

Furthermore, under the assumptions (A.109) and (A.93), the following also hold:

(a) *There exists a $\delta^* > 0$ such that for any $\delta \in (0, \delta^*]$ and any positive integer n,*

$$r_{X;Y}(\delta) = \frac{1}{2\sigma_I^2(X;Y)} \delta^2 + O(\delta^3) \tag{A.117}$$

and hence

$$\Pr\left\{\frac{1}{n}\ln\frac{p(Y^n|X^n)}{p(Y^n)} > I(X;Y)+\delta\right\} \le e^{-n\left(\frac{\delta^2}{2\sigma_I^2(X;Y)}+O(\delta^3)\right)}. \tag{A.118}$$

(b) *For any $\delta \in (0, \Delta^*(X;Y))$ and any positive integer n*

$$\begin{aligned}\underline{\xi}_I(X;Y,\lambda,n)e^{-nr_{X;Y}(\delta)} &\le \Pr\left\{\frac{1}{n}\ln\frac{p(Y^n|X^n)}{p(Y^n)} > I(X;Y)+\delta\right\} \\ &\le \bar{\xi}_I(X;Y,\lambda,n)e^{-nr_{X;Y}(\delta)} \end{aligned}\tag{A.119}$$

where $\lambda = r'_{X;Y}(\delta) > 0$, and

$$\begin{aligned}\bar{\xi}_I(X;Y,\lambda,n) &= \frac{2CM_I(X;Y,\lambda)}{\sqrt{n}\sigma_I^3(X;Y,\lambda)} \\ &\quad + e^{\frac{n\lambda^2\sigma_I^2(X;Y,\lambda)}{2}}\left[Q(\sqrt{n}\lambda\sigma_I(X;Y,\lambda)) - Q(\rho^*+\sqrt{n}\lambda\sigma_I(X;Y,\lambda))\right] \end{aligned}\tag{A.120}$$

$$\underline{\xi}_I(X;Y,\lambda,n) = e^{\frac{n\lambda^2\sigma_I^2(X;Y,\lambda)}{2}}Q(\rho_*+\sqrt{n}\lambda\sigma_I(X;Y,\lambda)) \tag{A.121}$$

with $Q(\rho^*) = \frac{CM_I(X;Y,\lambda)}{\sqrt{n}\sigma_I^3(X;Y,\lambda)}$ and $Q(\rho_*) = \frac{1}{2} - \frac{2CM_I(X;Y,\lambda)}{\sqrt{n}\sigma_I^3(X;Y,\lambda)}$.

(c) *For any $\delta \le c\sqrt{\frac{\ln n}{n}}$, where $c < \sigma_I(X;Y)$ is a constant,*

$$\begin{aligned}Q\left(\frac{\delta\sqrt{n}}{\sigma_I(X;Y)}\right) - \frac{CM_I(X;Y)}{\sqrt{n}\sigma_I^3(X;Y)} &\le \Pr\left\{\frac{1}{n}\ln\frac{p(Y^n|X^n)}{p(Y^n)} > I(X;Y)+\delta\right\} \\ &\le Q\left(\frac{\delta\sqrt{n}}{\sigma_I(X;Y)}\right) + \frac{CM_I(X;Y)}{\sqrt{n}\sigma_I^3(X;Y)}. \end{aligned}\tag{A.122}$$

Remarks similar to those (Remark A.1 and A.2) following Theorem A.2 can be drawn here concerning Theorems A.6 and A.7.

A.3.2 NEP With Respect to Relative Entropy

The IID source pair $(X,Y) = \{(X_i,Y_i)\}_{i=1}^{\infty}$ considered so far is arbitrary. Let us now focus on the case in which the source X is discrete, but Y could be either discrete or continuous.

Let $\mathcal{P}$ denote the set of all probability distributions over the source alphabet $\mathcal{X}$. For any $t \in \mathcal{P}$, let

$$q_t(y) \stackrel{\Delta}{=} \sum_{x \in \mathcal{X}} t(x) p(y|x) \tag{A.123}$$

$$q_t(y^n) \stackrel{\Delta}{=} \prod_{i=1}^{n} q_t(y_i) \tag{A.124}$$

$$D(t, x) \stackrel{\Delta}{=} \int p(y|x) \ln \frac{p(y|x)}{q_t(y)} dy \tag{A.125}$$

and

$$I(t; P) \stackrel{\Delta}{=} \sum_{x \in \mathcal{X}} t(x) \int p(y|x) \ln \frac{p(y|x)}{q_t(y)} dy \tag{A.126}$$

where $y^n = y_1 y_2 \cdots y_n$, and $P = \{p(y|x)\}$ represents a channel with $p(y|x)$ as its transitional pmf or pdf (as the case may be). Clearly, $D(t, x)$ is the divergence or relative entropy between $p(y|x)$ and $q_t(y)$; and $I(t; P)$ is the mutual information between the input and output of the channel P when the input is distributed according to t. To be specific, we denote the pmf of each X_i by p_X. Without loss of generality, we assume that $p_X(x) > 0$ for any $x \in \mathcal{X}$. Since

$$\int \int p(x, y) \left[\frac{p(y|x)}{p(y)} \right]^{-\lambda} dx dy = \sum_{a \in \mathcal{X}} p_X(a) \int p(y|a) \left[\frac{\sum_{b \in \mathcal{X}} p_X(b) p(y|b)}{p(y|a)} \right]^{\lambda} dy$$

it is not hard to see that for any $\lambda > 0$,

$$\int \int p(x, y) \left[\frac{p(y|x)}{p(y)} \right]^{-\lambda} dx dy < \infty$$

if and only if

$$\int p(y|a) \left[\frac{\sum_{b \in \mathcal{X}} p(y|b)}{p(y|a)} \right]^{\lambda} dy < \infty$$

for any $a \in \mathcal{X}$. Therefore, $\lambda_-^*(X; Y)$ defined in (A.89) is also equal to

$$\sup \left\{ \lambda \geq 0 : \int p(y|a) \left[\frac{p(y|a)}{q_t(y)} \right]^{-\lambda} dy < \infty, a \in \mathcal{X} \right\}$$

for any $t \in \mathcal{P}$ with $t(a) > 0$ for any $a \in \mathcal{X}$ (such $t \in \mathcal{P}$ will be said to have full support).

Define for any $t \in \mathcal{P}$ with full support and any $\delta \geq 0$

$$r_-(t,\delta) \stackrel{\Delta}{=} \sup_{\lambda \geq 0} \left[\lambda(\delta - I(t;P)) - \sum_{x \in \mathcal{X}} t(x) \ln \int p(y|x) \left[\frac{p(y|x)}{q_t(y)} \right]^{-\lambda} dy \right] \tag{A.127}$$

and for any $\lambda \in [0, \lambda_-^*(X;Y))$ and any $t \in \mathcal{P}$ with full support

$$f_{-\lambda}(y|x) \stackrel{\Delta}{=} \frac{\left[\frac{p(y|x)}{q_t(y)} \right]^{-\lambda}}{\int p(v|x) \left[\frac{p(v|x)}{q_t(v)} \right]^{-\lambda} dv} \tag{A.128}$$

$$D(t,x,\lambda) \stackrel{\Delta}{=} \int p(y|x) f_{-\lambda}(y|x) \left[\ln \frac{p(y|x)}{q_t(y)} \right] dy \tag{A.129}$$

$$\delta_-(t,\lambda) \stackrel{\Delta}{=} \sum_{x \in \mathcal{X}} t(x) \int p(y|x) f_{-\lambda}(y|x) \left[-\ln \frac{p(y|x)}{q_t(y)} \right] dy + I(t;P) \, . \tag{A.130}$$

It is not hard to verify that

$$\delta_-(t,0) = 0$$

and

$$\begin{aligned} \frac{\partial \delta_-(t,\lambda)}{\partial \lambda} &= \sum_{x \in \mathcal{X}} t(x) \left[\int p(y|x) f_{-\lambda}(y|x) \left[-\ln \frac{p(y|x)}{q_t(y)} \right]^2 dy \right. \\ &\quad \left. - \left(\int p(y|x) f_{-\lambda}(y|x) \left[-\ln \frac{p(y|x)}{q_t(y)} \right] dy \right)^2 \right] \\ &= \sum_{x \in \mathcal{X}} t(x) \left[\int p(y|x) f_{-\lambda}(y|x) \left[\ln \frac{p(y|x)}{q_t(y)} \right]^2 dy - D^2(t,x,\lambda) \right] \\ &> 0 \end{aligned}$$

where the last inequality is due to (A.93). Therefore, $\delta_-(t,\lambda)$ as a function of λ is strictly increasing over $\lambda \in [0, \lambda_-^*(X;Y))$. Let

$$\Delta_-^*(t) \stackrel{\Delta}{=} \lim_{\lambda \uparrow \lambda_-^*(X;Y)} \delta_-(t,\lambda) \, .$$

By an argument similar to that in the proof of Theorem A.1, it can be shown that $r_-(t,\delta)$ is strictly increasing, convex and continuously differentiable up to at least the third order inclusive over $\delta \in [0, \Delta_-^*(t))$, and furthermore $r_-(t,\delta)$ has the following parametric

expression

$$r_-(t,\delta_-(t,\lambda)) = \lambda(\delta_-(t,\lambda) - I(t;P)) - \sum_{x\in\mathcal{X}} t(x)\ln\int p(y|x)\left[\frac{p(y|x)}{q_t(y)}\right]^{-\lambda} dy \qquad \text{(A.131)}$$

with

$$\lambda = \frac{\partial r_-(t,\delta)}{\partial\delta}$$

satisfying

$$\delta_-(t,\lambda) = \delta\ .$$

Further define for any $\lambda \in [0, \lambda^*_-(X;Y))$

$$\sigma^2_{D,-}(t;P,\lambda) \triangleq \sum_{x\in\mathcal{X}} t(x)\left[\int p(y|x) f_{-\lambda}(y|x)\left|\ln\frac{p(y|x)}{q_t(y)} - D(t,x,\lambda)\right|^2 dy\right] \qquad \text{(A.132)}$$

and

$$M_{D,-}(t;P,\lambda) \triangleq \sum_{x\in\mathcal{X}} t(x)\left[\int p(y|x) f_{-\lambda}(y|x)\left|\ln\frac{p(y|x)}{q_t(y)} - D(t,x,\lambda)\right|^3 dy\right]\ . \qquad \text{(A.133)}$$

Write $\sigma^2_{D,-}(t;P,0)$ simply as $\sigma^2_D(t;P)$, $M_{D,-}(t;P,0)$ as $M_D(t;P)$, $\sigma^2_D(p_X;P)$ as $\sigma^2_D(X;Y)$, and $M_D(p_X;P)$ as $M_D(X;Y)$. It is not hard to see that

$$\sigma^2_D(t;P) = \sum_{x\in\mathcal{X}} t(x)\left[\int p(y|x)\left|\ln\frac{p(y|x)}{q_t(y)}\right|^2 dy - \left(\int p(y|x)\ln\frac{p(y|x)}{q_t(y)}dy\right)^2\right]$$

$$\sigma^2_D(X;Y) = \sum_{x\in\mathcal{X}} p(x)\left[\int p(y|x)\left|\ln\frac{p(y|x)}{p(y)}\right|^2 dy - \left(\int p(y|x)\ln\frac{p(y|x)}{p(y)}dy\right)^2\right]$$

$$M_D(t;P) \triangleq \sum_{x\in\mathcal{X}} t(x)\left[\int p(y|x)\left|\ln\frac{p(y|x)}{q_t(y)} - \left(\int p(v|x)\ln\frac{p(v|x)}{q_t(v)}dv\right)\right|^3 dy\right]$$

$$M_D(X;Y) \triangleq \sum_{x\in\mathcal{X}} p(x)\left[\int p(y|x)\left|\ln\frac{p(y|x)}{p(y)} - \left(\int p(v|x)\ln\frac{p(v|x)}{p(v)}dv\right)\right|^3 dy\right]$$

and

$$\sigma^2_{D,-}(t;P,\lambda) = \frac{\partial\delta_-(t,\lambda)}{\partial\lambda}\ .$$

For obvious reasons, we will refer to $\sigma_D^2(t;P)$ ($\sigma_D^2(X;Y)$, respectively) as the conditional divergence (or relative entropy) variance of P given t (Y given X, respectively).

In parallel with Theorems A.3, A.5, and A.6, we have the following result, which is referred to as the left NEP with respect to relative entropy.

Theorem A.8 (Left NEP With Respect to Relative Entropy)**.** *For any sequence $x^n = x_1 \cdots x_n$ from $\mathcal{X}$, let $t \in \mathcal{P}$ be the type of x^n, i.e., $nt(a)$, $a \in \mathcal{X}$, is the number of times the symbol a appears in x^n. Assume that t has full support. Then*

$$\Pr\left\{\frac{1}{n}\ln\frac{p(Y^n|X^n)}{q_t(Y^n)} \le I(t;P) - \delta \middle| X^n = x^n\right\} \le e^{-nr_-(t,\delta)}\,. \tag{A.134}$$

Furthermore, under the assumptions (A.90) and (A.93), the following also hold:

(a) *There exists a $\delta^* > 0$ such that for any $\delta \in (0, \delta^*]$*

$$r_-(t,\delta) = \frac{1}{2\sigma_D^2(t;P)}\delta^2 + O(\delta^3) \tag{A.135}$$

and hence

$$\Pr\left\{\frac{1}{n}\ln\frac{p(Y^n|X^n)}{q_t(Y^n)} \le I(t;P) - \delta \middle| X^n = x^n\right\} \le e^{-n(\frac{\delta^2}{2\sigma_D^2(t;P)}+O(\delta^3))}\,. \tag{A.136}$$

(b) *For any $\delta \in (0, \Delta_-^*(X;Y))$*

$$\begin{aligned}\underline{\xi}_{D,-}(t;P,\lambda,n)e^{-nr_-(t,\delta)} &\le \Pr\left\{\frac{1}{n}\ln\frac{p(Y^n|X^n)}{q_t(Y^n)} \le I(t;P) - \delta \middle| X^n = x^n\right\} \\ &\le \bar{\xi}_{D,-}(t;P,\lambda,n)e^{-nr_-(t,\delta)}\end{aligned} \tag{A.137}$$

where $\lambda = \frac{\partial r_-(t,\delta)}{\partial \delta} > 0$, and

$$\begin{aligned}\bar{\xi}_{D,-}(t;P,\lambda,n) &= \frac{2CM_{D,-}(t;P,\lambda)}{\sqrt{n}\sigma_{D,-}^3(t;P,\lambda)} \\ &\quad + e^{\frac{n\lambda^2\sigma_{D,-}^2(t;P,\lambda)}{2}}\left[Q(\sqrt{n}\lambda\sigma_{D,-}(t;P,\lambda)) - Q(\rho^* + \sqrt{n}\lambda\sigma_{D,-}(t;P,\lambda))\right]\end{aligned} \tag{A.138}$$

$$\underline{\xi}_{D,-}(t;P,\lambda,n) = e^{\frac{n\lambda^2\sigma_{D,-}^2(t;P,\lambda)}{2}}Q(\rho_* + \sqrt{n}\lambda\sigma_{D,-}(t;P,\lambda)) \tag{A.139}$$

with $Q(\rho^*) = \frac{CM_{D,-}(t;P,\lambda)}{\sqrt{n}\sigma_{D,-}^3(t;P,\lambda)}$ and $Q(\rho_*) = \frac{1}{2} - \frac{2CM_{D,-}(t;P,\lambda)}{\sqrt{n}\sigma_{D,-}^3(t;P,\lambda)}$.

(c) *For any* $\delta \le c\sqrt{\frac{\ln n}{n}}$, *where* $c < \sigma_D(t;P)$ *is a constant,*

$$\begin{aligned} Q\left(\frac{\delta\sqrt{n}}{\sigma_D(t;P)}\right) - \frac{CM_D(t;P)}{\sqrt{n}\sigma_D^3(t;P)} &\le \Pr\left\{\frac{1}{n}\ln\frac{p(Y^n|X^n)}{q_t(Y^n)} \le I(t;P) - \delta \,\middle|\, X^n = x^n\right\} \\ &\le Q\left(\frac{\delta\sqrt{n}}{\sigma_D(t;P)}\right) + \frac{CM_D(t;P)}{\sqrt{n}\sigma_D^3(t;P)}. \end{aligned} \tag{A.140}$$

Proof of Theorem A.8. The inequality (A.134) comes from the Chernoff bound. To see this is indeed the case, note that

$$\begin{aligned} &\Pr\left\{\frac{1}{n}\ln\frac{p(Y^n|X^n)}{q_t(Y^n)} \le I(t;P) - \delta \,\middle|\, X^n = x^n\right\} \\ &\le \inf_{\lambda\ge 0} \frac{\mathbb{E}\left[\left(\frac{p(Y^n|X^n)}{q_t(Y^n)}\right)^{-\lambda} \,\middle|\, X^n = x^n\right]}{e^{n\lambda(\delta - I(t;P))}} \\ &= \inf_{\lambda\ge 0} \frac{\prod_{a\in\mathcal{X}}\left[\int p(y|a)\left(\frac{p(y|a)}{q_t(y)}\right)^{-\lambda} dy\right]^{nt(a)}}{e^{n\lambda(\delta - I(t;P))}} \\ &= \inf_{\lambda\ge 0} \exp\left\{-n\left[\lambda(\delta - I(t;P)) - \sum_{a\in\mathcal{X}} t(a)\ln\int p(y|a)\left(\frac{p(y|a)}{q_t(y)}\right)^{-\lambda} dy\right]\right\} \\ &= e^{-nr_-(t,\delta)} \end{aligned} \tag{A.141}$$

which completes the proof of (A.134).

The equation (A.135) follows from the Taylor expansion of $r_-(t,\delta)$ at $\delta = 0$ and the fact that

$$\frac{\partial^2 r_-(t,\delta)}{\partial\delta^2} = \frac{1}{\sigma_D^2(t;P)}\,.$$

What remains is to prove (A.137) and (A.140). To this end, let

$$f_{-\lambda}(y^n|x^n) = \prod_{i=1}^n f_{-\lambda}(y_i|x_i).$$

With $\lambda = \frac{\partial r_-(t,\delta)}{\partial\delta}$, it follows from (A.131) that

$$r_-(t,\delta) = \lambda(\delta - I(t;P)) - \sum_{x\in\mathcal{X}} t(x)\ln\int p(y|x)\left[\frac{p(y|x)}{q_t(y)}\right]^{-\lambda} dy\,.$$

Then we have

$$
\begin{aligned}
&\Pr\left\{ \frac{1}{n}\ln\frac{p(Y^n|X^n)}{q_t(Y^n)} \le I(t;P)-\delta \middle| X^n = x^n \right\} \\
&= \int\limits_{\frac{1}{n}\ln\frac{p(y^n|x^n)}{q_t(y^n)} \le I(t;P)-\delta} p(y^n|x^n)dy^n \\
&= \int\limits_{\frac{1}{n}\ln\frac{p(y^n|x^n)}{q_t(y^n)} \le I(t;P)-\delta} f_{-\lambda}^{-1}(y^n|x^n) f_{-\lambda}(y^n|x^n) p(y^n|x^n)dy^n \\
&= \int\limits_{\frac{1}{n}\ln\frac{p(y^n|x^n)}{q_t(y^n)} \le I(t;P)-\delta} e^{\lambda\ln\frac{p(y^n|x^n)}{q_t(y^n)} + n\sum_{a\in\mathcal{X}} t(a)\ln\int p(v|a)\left(\frac{p(v|a)}{q_t(v)}\right)^{-\lambda}dv} f_{-\lambda}(y^n|x^n) p(y^n|x^n)dy^n \\
&= \int\limits_{\frac{1}{n}\ln\frac{p(y^n|x^n)}{q_t(y^n)} \le I(t;P)-\delta} e^{\lambda\ln\frac{p(y^n|x^n)}{q_t(y^n)} + n\lambda(\delta-I(t;P)) - nr_-(t,\delta)} f_{-\lambda}(y^n|x^n) p(y^n|x^n)dy^n \\
&= e^{-nr_-(t,\delta)} \int\limits_{\ln\frac{p(y^n|x^n)}{q_t(y^n)} - n(I(t;P)-\delta) \le 0} e^{\lambda\left[\ln\frac{p(y^n|x^n)}{q_t(y^n)} - n(I(t;P)-\delta)\right]} f_{-\lambda}(y^n|x^n) p(y^n|x^n)dy^n \\
&= e^{-nr_-(t,\delta)} \int\limits_{\rho\le 0} \int\limits_{\frac{\ln\frac{p(y^n|x^n)}{q_t(y^n)} - n(I(t;P)-\delta)}{\sqrt{n}\sigma_{D,-}(t;P,\lambda)} = \rho} e^{\lambda\sqrt{n}\sigma_{D,-}(t;P,\lambda)\rho} f_{-\lambda}(y^n|x^n) p(y^n|x^n)dy^n \\
&= e^{-nr_-(t,\delta)} \int_{-\infty}^{0} e^{\lambda\sqrt{n}\sigma_{D,-}(t;P,\lambda)\rho} dF_{x^n}(\rho) \\
&= e^{-nr_-(t,\delta)} \left[F_{x^n}(0) - \int_{-\infty}^{0} \lambda\sqrt{n}\sigma_{D,-}(t;P,\lambda) e^{\lambda\sqrt{n}\sigma_{D,-}(t;P,\lambda)\rho} F_{x^n}(\rho)d\rho \right] . \qquad \text{(A.142)}
\end{aligned}
$$

where

$$
F_{x^n}(\rho) = \Pr\left\{ \frac{\ln\frac{p(Z^n|x^n)}{q_t(Z^n)} - n(I(t;P)-\delta)}{\sqrt{n}\sigma_{D,-}(t;P,\lambda)} \le \rho \right\}
$$

and Z_i takes values over the alphabet of Y according to the pmf or pdf (as the case may

be) $f_{-\lambda}(z|x_i)p(z|x_i)$. It is easy to verify that

$$\mathbb{E}\left[\ln\frac{p(Z_i|x_i)}{q_t(Z_i)}\right] = D(t, x_i, \lambda)$$

and

$$\begin{aligned}\sum_{i=1}^{n}\mathbb{E}\left[\ln\frac{p(Z_i|x_i)}{q_t(Z_i)}\right] &= \sum_{i=1}^{n} D(t, x_i, \lambda)\\ &= n\sum_{x\in\mathcal{X}} t(x)D(t, x, \lambda)\\ &= n(I(t;P) - \delta)\end{aligned}$$

which further implies that

$$F_{x^n}(\rho) = \Pr\left\{\frac{\sum_{i=1}^{n}\left[\ln\frac{p(Z_i|x_i)}{q_t(Z_i)} - D(t, x_i, \lambda)\right]}{\sqrt{n}\sigma_{D,-}(t;P,\lambda)} \le \rho\right\}.$$

Applying Lemma A.1 to the independent sequence

$$\left\{\ln\frac{p(Z_i|x_i)}{q_t(Z_i)} - D(t, x_i, \lambda)\right\}_{i=1}^{n},$$

the argument similar to that in the proof of Theorem A.2 can then be used to establish (A.137).

Finally, consider another sequence of independent random variables $W_1, W_2, \cdots, W_n$, where W_i takes values over the alphabet of Y according to the pmf or pdf (as the case may be) $p(w|x_i)$. Applying Lemma A.1 directly to

$$\left\{\ln\frac{p(W_i|x_i)}{q_t(W_i)} - D(t, x_i)\right\}_{i=1}^{n}$$

we then get (A.140). This completes the proof of Theorem A.8. □

The conditional probability that given $X^n = x^n$, $\frac{1}{n}\ln\frac{p(Y^n|X^n)}{q_t(Y^n)}$ is away from $I(t;P)$ to the right can be bounded similarly. For completeness, we state these bounds below without proof. Define for any $t \in \mathcal{P}$ with full support and any $\delta \ge 0$

$$r(t,\delta) \stackrel{\Delta}{=} \sup_{\lambda\ge 0}\left[\lambda(I(t;P)+\delta) - \sum_{x\in\mathcal{X}} t(x)\ln\int p(y|x)\left[\frac{p(y|x)}{q_t(y)}\right]^{\lambda} dy\right] \tag{A.143}$$

and for any $\lambda \in [0, \lambda^*(X;Y))$ and any $t \in \mathcal{P}$ with full support

$$f_\lambda(y|x) \triangleq \frac{\left[\frac{p(y|x)}{q_t(y)}\right]^\lambda}{\int p(v|x)\left[\frac{p(v|x)}{q_t(v)}\right]^\lambda dv} \tag{A.144}$$

$$D_+(t,x,\lambda) \triangleq \int p(y|x) f_\lambda(y|x) \left[\ln \frac{p(y|x)}{q_t(y)}\right] dy \tag{A.145}$$

$$\delta(t,\lambda) \triangleq \sum_{x\in\mathcal{X}} t(x) \int p(y|x) f_\lambda(y|x) \left[\ln \frac{p(y|x)}{q_t(y)}\right] dy - I(t;P) \ . \tag{A.146}$$

Then under the condition (A.93), $\delta(t,\lambda)$ as a function of λ is strictly increasing over $\lambda \in [0, \lambda^*(X;Y))$ with $\delta(t,0) = 0$. Let

$$\Delta^*(t) \triangleq \lim_{\lambda \uparrow \lambda^*(X;Y)} \delta(t,\lambda) \ .$$

By an argument similar to that in the proof of Theorem A.1, it can be shown that $r(t,\delta)$ is strictly increasing, convex and continuously differentiable up to at least the third order over $\delta \in [0, \Delta^*(t))$, and furthermore $r(t,\delta)$ has the following parametric expression

$$r(t,\delta(t,\lambda)) = \lambda(I(t;P) + \delta(t,\lambda)) - \sum_{x\in\mathcal{X}} t(x) \ln \int p(y|x) \left[\frac{p(y|x)}{q_t(y)}\right]^\lambda dy \tag{A.147}$$

with

$$\lambda = \frac{\partial r(t,\delta)}{\partial \delta}$$

satisfying

$$\delta(t,\lambda) = \delta \ .$$

Further define for any $\lambda \in [0, \lambda^*(X;Y))$

$$\sigma_D^2(t;P,\lambda) \triangleq \sum_{x\in\mathcal{X}} t(x) \left[\int p(y|x) f_\lambda(y|x) \left|\ln \frac{p(y|x)}{q_t(y)} - D_+(t,x,\lambda)\right|^2 dy\right] \tag{A.148}$$

and

$$M_D(t;P,\lambda) \triangleq \sum_{x\in\mathcal{X}} t(x) \left[\int p(y|x) f_\lambda(y|x) \left|\ln \frac{p(y|x)}{q_t(y)} - D_+(t,x,\lambda)\right|^3 dy\right] \ . \tag{A.149}$$

Then the following result can be proved similarly, which is referred to as the right NEP with respect to relative entropy.

Theorem A.9 (Right NEP With Respect to Relative Entropy)**.** *For any sequence $x^n = x_1 \cdots x_n$ from $\mathcal{X}$, let $t \in \mathcal{P}$ be the type of x^n, i.e., $nt(a)$, $a \in \mathcal{X}$, is the number of times the symbol a appears in x^n. Assume that t has full support. Then*

$$\Pr\left\{\frac{1}{n}\ln\frac{p(Y^n|X^n)}{q_t(Y^n)} > I(t;P)+\delta \middle| X^n = x^n\right\} \le e^{-nr(t,\delta)}\,. \tag{A.150}$$

Furthermore, under the assumptions (A.109) and (A.93), the following also hold:

(a) *There exists a $\delta^* > 0$ such that for any $\delta \in (0, \delta^*]$*

$$r(t,\delta) = \frac{1}{2\sigma_D^2(t;P)}\delta^2 + O(\delta^3) \tag{A.151}$$

and hence

$$\Pr\left\{\frac{1}{n}\ln\frac{p(Y^n|X^n)}{q_t(Y^n)} > I(t;P)+\delta \middle| X^n = x^n\right\} \le e^{-n(\frac{\delta^2}{2\sigma_D^2(t;P)}+O(\delta^3))}\,. \tag{A.152}$$

(b) *For any $\delta \in (0, \Delta^*(X;Y))$*

$$\begin{aligned}\underline{\xi}_D(t;P,\lambda,n)e^{-nr(t,\delta)} &\le \Pr\left\{\frac{1}{n}\ln\frac{p(Y^n|X^n)}{q_t(Y^n)} > I(t;P)+\delta \middle| X^n = x^n\right\}\\ &\le \bar{\xi}_D(t;P,\lambda,n)e^{-nr(t,\delta)}\end{aligned} \tag{A.153}$$

where $\lambda = \frac{\partial r(t,\delta)}{\partial \delta} > 0$, and

$$\begin{aligned}\bar{\xi}_D(t;P,\lambda,n) &= \frac{2CM_D(t;P,\lambda)}{\sqrt{n}\sigma_D^3(t;P,\lambda)}\\ &\quad + e^{\frac{n\lambda^2\sigma_D^2(t;P,\lambda)}{2}}\left[Q(\sqrt{n}\lambda\sigma_D(t;P,\lambda)) - Q(\rho^* + \sqrt{n}\lambda\sigma_D(t;P,\lambda))\right]\end{aligned} \tag{A.154}$$

$$\underline{\xi}_D(t;P,\lambda,n) = e^{\frac{n\lambda^2\sigma_D^2(t;P,\lambda)}{2}}Q(\rho_* + \sqrt{n}\lambda\sigma_D(t;P,\lambda)) \tag{A.155}$$

with $Q(\rho^*) = \frac{CM_D(t;P,\lambda)}{\sqrt{n}\sigma_D^3(t;P,\lambda)}$ and $Q(\rho_*) = \frac{1}{2} - \frac{2CM_D(t;P,\lambda)}{\sqrt{n}\sigma_D^3(t;P,\lambda)}$.

(c) *For any $\delta \le c\sqrt{\frac{\ln n}{n}}$, where $c < \sigma_D(t;P)$ is a constant,*

$$\begin{aligned}Q\left(\frac{\delta\sqrt{n}}{\sigma_D(t;P)}\right) - \frac{CM_D(t;P)}{\sqrt{n}\sigma_D^3(t;P)} &\le \Pr\left\{\frac{1}{n}\ln\frac{p(Y^n|X^n)}{q_t(Y^n)} > I(t;P)+\delta \middle| X^n = x^n\right\}\\ &\le Q\left(\frac{\delta\sqrt{n}}{\sigma_D(t;P)}\right) + \frac{CM_D(t;P)}{\sqrt{n}\sigma_D^3(t;P)}\,.\end{aligned} \tag{A.156}$$

Remarks similar to those (Remark A.1 and A.2) following Theorem A.2 can be drawn here concerning Theorems A.8 and A.9.

A.4 NEP Application to Fixed Rate Source Coding

Assume that the source alphabet $\mathcal{X}$ is finite. In this section, we make use of the NEP with respect to $H(X)$ to establish a non-asymptotic fixed rate source coding theorem, which reveals, for any finite block length n, a complete picture about the tradeoff between the minimum rate of fixed rate coding of $X_1 \cdots X_n$ and error probability when the error probability is a constant, or goes to 0 with block length n at a sub-polynomial $n^{-\alpha}$, $0 < \alpha < 1$, polynomial $n^{-\alpha}$, $\alpha \geq 1$, or sub-exponential $e^{-n^{\alpha}}$, $0 < \alpha < 1$, speed. We begin with the definition of fixed rate source code.

Definition A.1. *Given a source from alphabet $\mathcal{X}$, a fixed rate source code with coding length n is defined as a mapping $i : S_n \to \{1, 2, \ldots, |S_n|\}$, where S_n is a subset of $\mathcal{X}^n$. The performance of the code is measured by the rate $R_n = \frac{1}{n} \ln |S_n|$ (in nats) and error probability $\Pr\{X^n \notin S_n\}$.*

As can be seen from the definition, the design of a fixed rate source code is equivalent to picking a subset of $\mathcal{X}^n$. Given the source statistics $p(x)$, one can easily show that the optimal way to pick S_n is to order x^n in the non-increasing order of $p(x^n)$, and include those x^n with rank less than or equal to $|S_n|$. Then we have the following non-asymptotic fixed rate source coding theorem.

Theorem A.10. *Let $R_n(\epsilon_n)$ denote the minimum rate (in nats) of fixed rate coding of $X_1 X_2 \cdots X_n$ subject to the error probability not larger than ϵ_n. Under the assumptions (A.3) and (A.6), for any n and $\epsilon_n > 0$,*

$$\bar{\delta} \geq R_n(\epsilon_n) - H(X) \geq \underline{\delta} - r_X(\underline{\delta}) + \frac{-d + \ln\left[\frac{1}{2} - Q\left(\frac{d}{\sqrt{n}\sigma_H(X,\lambda)}\right) - \frac{2CM_H(X,\lambda)}{\sqrt{n}\sigma_H^3(X,\lambda)}\right]}{n} \tag{A.157}$$

for any constant d satisfying $\frac{1}{2} - Q\left(\frac{d}{\sqrt{n}\sigma_H(X,\lambda)}\right) - \frac{2CM_H(X,\lambda)}{\sqrt{n}\sigma_H^3(X,\lambda)} > 0$, where $\bar{\delta}$ is the solution to the equation

$$\epsilon_n = \bar{\xi}_H(X, r'_X(\delta), n) e^{-n r_X(\delta)} \tag{A.158}$$

$\underline{\delta}$ is the solution to the equation

$$\left(1 + e^{-n}\right) \epsilon_n = \underline{\xi}_H(X, r'_X(\delta), n) e^{-n r_X(\delta)} \tag{A.159}$$

and $\lambda = r'_X(\underline{\delta})$. In particular, the following hold, depending on whether ϵ_n is a constant, or how fast ϵ_n goes to 0.

(a) When ϵ_n decreases exponentially with respect to n,

$$\begin{aligned} r_X^{(inv)}\left(-\frac{\ln\epsilon_n}{n}-\frac{\ln n}{2n}\right)+O(n^{-1}) &\geq R_n(\epsilon_n)-H(X) \\ &\geq r_X^{(inv)}\left(-\frac{\ln\epsilon_n}{n}-\frac{\ln n}{2n}\right)+\frac{\ln\epsilon_n}{n}-O(n^{-1}) \end{aligned} \tag{A.160}$$

where $r_X^{(inv)}(\cdot)$ is the inverse function of $r_X(\cdot)$.

(b) When $\epsilon_n = n^{-\frac{\alpha}{2}}e^{-n^\alpha}$ for $\alpha\in(0,1)$,

$$\begin{aligned} \sqrt{2}\sigma_H(X)n^{-\frac{1-\alpha}{2}}+O\left(n^{-\frac{1+\alpha}{2}}\right) &\geq R_n(\epsilon_n)-H(X) \\ &\geq \sqrt{2}\sigma_H(X)n^{-\frac{1-\alpha}{2}}-O\left(n^{-\frac{1+\alpha}{2}}\right) \end{aligned} \tag{A.161}$$

for $\alpha\in\left(0,\frac{1}{3}\right)$, and

$$\begin{aligned} \sqrt{2}\sigma_H(X)n^{-\frac{1-\alpha}{2}}+O\left(n^{-(1-\alpha)}\right) &\geq R_n(\epsilon_n)-H(X) \\ &\geq \sqrt{2}\sigma_H(X)n^{-\frac{1-\alpha}{2}}-O\left(n^{-(1-\alpha)}\right) \end{aligned} \tag{A.162}$$

for $\alpha\in\left[\frac{1}{3},1\right)$.

(c) When $\epsilon_n=\frac{n^{-\alpha}}{\sqrt{\ln n}}$ for $\alpha>0$,

$$\begin{aligned} \sigma_H(X)\sqrt{\frac{2\alpha\ln n}{n}}+O\left(\sqrt{\frac{1}{n\ln n}}\right) &\geq R_n(\epsilon_n)-H(X) \\ &\geq \sigma_H(X)\sqrt{\frac{2\alpha\ln n}{n}}-O\left(\sqrt{\frac{1}{n\ln n}}\right) \end{aligned} \tag{A.163}$$

(d) When $\epsilon_n=\epsilon$ remains a constant,

$$\begin{aligned} \frac{\sigma_H}{\sqrt{n}}Q^{-1}\left(\epsilon-\frac{CM_H(X)}{\sqrt{n}\sigma_H^3(X)}\right) &= \frac{\sigma_H}{\sqrt{n}}Q^{-1}(\epsilon)+O\left(\frac{1}{n}\right) \\ &\geq R_n(\epsilon_n)-H(X) \\ &\geq \frac{\sigma_H}{\sqrt{n}}Q^{-1}(\epsilon)-O\left(\frac{\ln n}{n}\right). \end{aligned} \tag{A.164}$$

where $Q^{-1}(\cdot)$ is the inverse function of $Q(\cdot)$.

Proof of Theorem A.10. Define

$$S_n(\delta) \stackrel{\Delta}{=} \left\{ x^n : -\frac{1}{n} \ln p(x^n) \leq H(X) + \delta \right\}$$

and

$$\epsilon_n(\delta) = \Pr\left\{ X^n \notin S_n(\delta) \right\}.$$

Clearly $\epsilon_n(\delta)$ is a non-increasing function of δ. Now let $\bar{\delta}$ and $\underline{\delta}$ satisfy that

$$\epsilon_n(\bar{\delta}) \leq \epsilon_n < \epsilon_n(\underline{\delta}). \tag{A.165}$$

According to the discussion on optimal fixed-rate source codes,

$$\frac{1}{n} \ln S_n(\underline{\delta}) < R_n(\epsilon_n) \leq \frac{1}{n} \ln S_n(\bar{\delta}). \tag{A.166}$$

Observe that

$$\begin{aligned} |S_n(\bar{\delta})| e^{-n(H(X)+\bar{\delta})} &\leq \sum_{x^n \in S_n(\bar{\delta})} p(x^n) \\ &\leq \sum_{x^n \in \mathcal{X}^n} p(x^n) \\ &\leq 1 \end{aligned}$$

which implies that

$$R_n(\epsilon_n) \leq \frac{1}{n} \ln |S_n(\bar{\delta})| \leq H(X) + \bar{\delta}. \tag{A.167}$$

Towards the lower bound on $R_n(\epsilon_n)$, further define

$$S_n(\underline{\delta}, d) \stackrel{\Delta}{=} \left\{ x^n : H(X) + \underline{\delta} - \frac{d}{n} \leq -\frac{1}{n} \ln p(x^n) \leq H(X) + \underline{\delta} \right\}$$

for some constant $d > 0$. Then we have

$$\begin{aligned}
|S_n(\underline{\delta}, d)|e^{-n\left(H(X)+\underline{\delta}-\frac{d}{n}\right)} &\geq \sum_{x^n \in S_n(\underline{\delta},d)} p(x^n) \\
&= \sum_{x^n \in S_n(\underline{\delta},d)} f_\lambda^{-1}(x) f_\lambda(x^n) p(x^n) \\
&= \sum_{x^n \in S_n(\underline{\delta},d)} e^{-n\left[-\frac{1}{n}\lambda \ln p(x^n) - \ln \sum_{u\in\mathcal{X}} p^{-\lambda+1}(u)\right]} f_\lambda(x^n) p(x^n) \\
&\geq e^{-nr_X(\underline{\delta})} \sum_{x^n \in S_n(\underline{\delta},d)} f_\lambda(x^n) p(x^n) \\
&= e^{-nr_X(\underline{\delta})} \Pr\{Z^n \in S_n(\underline{\delta}, d)\} \\
&= e^{-nr_X(\underline{\delta})} \Pr\left\{-\frac{d}{n} \leq \frac{1}{n}\sum_{i=1}^{n} -\ln p(Z_i) - (H(X)+\underline{\delta}) \leq 0\right\} \\
&\geq e^{-nr_X(\underline{\delta})} \left[\frac{1}{2} - Q\left(\frac{d}{\sqrt{n}\sigma_H(X,\lambda)}\right) - \frac{2CM_H(X,\lambda)}{\sqrt{n}\sigma_H^3(X,\lambda)}\right]
\end{aligned}$$

where $\lambda = r'_X(\underline{\delta})$, $\{Z_i\}_{i=1}^n$ are IID random variables with common pmf $f_\lambda(z)p(z)$, and the last inequality is due to the direct application of Lemma A.1 (Berry-Esseen Central Limit Theorem) to $\{-\ln p(Z_i) - (H(X)+\underline{\delta})\}_{i=1}^n$. And therefore

$$\begin{aligned}
R_n(\epsilon_n) &> \frac{1}{n}\ln|S_n(\underline{\delta})| \\
&\geq \frac{1}{n}\ln|S_n(\underline{\delta}, d)| \\
&\geq H(X) + \underline{\delta} - \frac{d}{n} - r_X(\underline{\delta}) \\
&\quad + \frac{1}{n}\ln\left[\frac{1}{2} - Q\left(\frac{d}{\sqrt{n}\sigma_H(X,\lambda)}\right) - \frac{2CM_H(X,\lambda)}{\sqrt{n}\sigma_H^3(X,\lambda)}\right].
\end{aligned} \tag{A.168}$$

Note that $\frac{1}{2} - Q\left(\frac{d}{\sqrt{n}\sigma_H(X,\lambda)}\right) - \frac{2CM_H(X,\lambda)}{\sqrt{n}\sigma_H^3(X,\lambda)} = \Theta\left(\frac{1}{\sqrt{n}}\right)$ for constant $d > 0$. Then (A.157) is proved by showing $\bar{\delta}$ and $\underline{\delta}$ calculated according to (A.158) and (A.159) indeed satisfy (A.165), where we invoke Theorem A.2, i.e.

$$\begin{aligned}
\epsilon_n(\bar{\delta}) &= \Pr\left\{X^n \notin S_n(\bar{\delta})\right\} \\
&\leq \bar{\xi}_H(X, r'_X(\bar{\delta}), n) e^{-nr_X(\bar{\delta})} \\
&= \epsilon_n
\end{aligned}$$

while

$$\begin{aligned}\epsilon_n(\underline{\delta}) &= \Pr\{X^n \notin S_n(\underline{\delta})\} \\ &\geq \underline{\xi}_H(X, r'_X(\underline{\delta}), n)e^{-nr_X(\underline{\delta})} \\ &> \epsilon_n.\end{aligned}$$

Let us now look at special cases.

(a) When ϵ_n decreases exponentially with respect to n, i.e. $\frac{1}{n}\ln\epsilon_n \to c$ as $n \to +\infty$ for some constant $c < 0$, we have

$$\frac{\ln\epsilon_n}{n} = \frac{\ln\bar{\xi}_H(X, r'_X(\bar{\delta}), n)}{n} - r_X(\bar{\delta}). \tag{A.169}$$

Note that

$$\bar{\xi}_H(X, \lambda, n) \geq \frac{2CM_H(X,\lambda)}{\sqrt{n}\sigma_H^3(X,\lambda)} = \Omega\left(\frac{1}{\sqrt{n}}\right).$$

Taking $n \to +\infty$ in (A.169), it can be seen that $r_X(\bar{\delta}) \to -c$. And therefore, $\bar{\xi}_H(X, r'_X(\bar{\delta}), n) = \Theta\left(\frac{1}{\sqrt{n}}\right)$, which further implies that

$$\begin{aligned}\bar{\delta} &= r_X^{(inv)}\left(-\frac{\ln\epsilon_n}{n} + \frac{\ln\bar{\xi}_H(X, r'_X(\bar{\delta}), n)}{n}\right) \\ &= r_X^{(inv)}\left(-\frac{\ln\epsilon_n}{n} - \frac{\ln n}{2n} + O(n^{-1})\right) \\ &= r_X^{(inv)}\left(-\frac{\ln\epsilon_n}{n} - \frac{\ln n}{2n}\right) + O(n^{-1}).\end{aligned} \tag{A.170}$$

On the other hand,

$$\frac{\ln\epsilon_n}{n} + \frac{\ln(1+e^{-n})}{n} = \frac{\ln\underline{\xi}_H(X, r'_X(\underline{\delta}), n)}{n} - r_X(\underline{\delta}). \tag{A.171}$$

and by the same argument, $r_X(\underline{\delta}) \to -c$ as $n \to +\infty$. Consequently, $\underline{\xi}_H(X, r'_X(\underline{\delta}), n) = \Theta\left(\frac{1}{\sqrt{n}}\right)$, which further implies

$$\frac{\ln\epsilon_n}{n} = -r_X(\underline{\delta}) - \frac{\ln n}{2n} + O(n^{-1}) \tag{A.172}$$

and

$$\underline{\delta} = r_X^{(inv)}\left(-\frac{\ln \epsilon_n}{n} - \frac{\ln n}{2n}\right) - O(n^{-1}). \tag{A.173}$$

Combining (A.157) with (A.170), (A.172) and (A.173) yields,

$$\begin{aligned} r_X^{(inv)}\left(-\frac{\ln \epsilon_n}{n} - \frac{\ln n}{2n}\right) + O(n^{-1}) &\geq R_n(\epsilon_n) - H(X) \\ &\geq \underline{\delta} - r_X(\underline{\delta}) - \frac{\ln n}{2n} - O(n^{-1}) \\ &= r_X^{(inv)}\left(-\frac{\ln \epsilon_n}{n} - \frac{\ln n}{2n}\right) + \frac{\ln \epsilon_n}{n} - O(n^{-1}) \end{aligned} \tag{A.174}$$

This completes the proof of (A.160).

(b) First of all, let us consider the case when $\alpha \in \left(0, \frac{1}{3}\right)$. Towards proving (A.161), let us show that $\bar{\delta} = \sqrt{2}\sigma_H(X)n^{-\frac{1-\alpha}{2}} + \eta n^{-\frac{1+\alpha}{2}}$ for some properly chosen constant η will guarantee

$$\epsilon_n(\bar{\delta}) \leq n^{-\frac{\alpha}{2}} e^{-n^{\alpha}}. \tag{A.175}$$

By Theorem A.2 and Remark A.1,

$$\epsilon_n\left(\bar{\delta}\right) \leq \bar{\xi}_H\left(X, r'_X\left(\bar{\delta}\right), n\right) e^{-nr_X\left(\bar{\delta}\right)}$$

while

$$\begin{aligned} &\bar{\xi}_H\left(X, r'_X\left(\bar{\delta}\right), n\right) \\ &= \bar{\xi}_H\left(X, r'_X\left(\sqrt{2}\sigma_H(X)n^{-\frac{1-\alpha}{2}} + \eta n^{-\frac{1+\alpha}{2}}\right), n\right) \\ &= \Theta\left(\frac{1}{\sqrt{n}r'_X\left(\sqrt{2}\sigma_H(X)n^{-\frac{1-\alpha}{2}} + \eta n^{-\frac{1+\alpha}{2}}\right)}\right) \\ &= \Theta\left(n^{-\frac{\alpha}{2}}\right) \leq \eta_1 n^{-\frac{\alpha}{2}} \end{aligned}$$

for some constant $\eta_1 > 0$, and

$$\begin{aligned}
& e^{-nr_X(\bar{\delta})} \\
&= \exp\left\{-nr_X\left(\sqrt{2}\sigma_H(X)n^{-\frac{1-\alpha}{2}} + \eta n^{-\frac{1+\alpha}{2}}\right)\right\} \\
&= \exp\left\{-n\left[\frac{1}{2\sigma_H^2(X)}\left(\sqrt{2}\sigma_H(X)n^{-\frac{1-\alpha}{2}} + \eta n^{-\frac{1+\alpha}{2}}\right)^2 + O\left(n^{-\frac{3(1-\alpha)}{2}}\right)\right]\right\} \\
&= \exp\left\{-n^{\alpha} - \frac{\sqrt{2}\eta}{\sigma_H(X)} - O\left(n^{-\alpha} + n^{-\frac{1-3\alpha}{2}}\right)\right\} \\
&= \exp\left\{-n^{\alpha} - \frac{\sqrt{2}\eta}{\sigma_H(X)} - o(1)\right\}
\end{aligned}$$

since $\alpha \in \left(0, \frac{1}{3}\right)$. Now it is trivial to see that we can select a constant η such that

$$\eta_1 e^{-\frac{\sqrt{2}\eta}{\sigma_H(X)} - o(1)} \leq 1$$

which will make (A.175) satisfied, and consequently

$$\begin{aligned}
\bar{\delta} &= \sqrt{2}\sigma_H(X)n^{-\frac{1-\alpha}{2}} + \eta n^{-\frac{1+\alpha}{2}} \\
&= \sqrt{2}\sigma_H(X)n^{-\frac{1-\alpha}{2}} + O\left(n^{-\frac{1+\alpha}{2}}\right) \\
&\geq R_n(\epsilon_n) - H(X).
\end{aligned}$$

In the similar manner, we can show that by making $\underline{\delta} = \sqrt{2}\sigma_H(X)n^{-\frac{1-\alpha}{2}} - \eta' n^{-\frac{1+\alpha}{2}}$ for another constant $\eta' > 0$,

$$\epsilon_n(\underline{\delta}) > \epsilon_n.$$

Consequently,

$$\begin{aligned}
R_n(\epsilon_n) - H(X) &\geq \underline{\delta} - r_X(\underline{\delta}) - \frac{\ln n}{2n} - O(n^{-1}) \\
&= \sqrt{2}\sigma_H(X)n^{-\frac{1-\alpha}{2}} - \eta' n^{-\frac{1+\alpha}{2}} - O\left(n^{-(1-\alpha)}\right) \\
&= \sqrt{2}\sigma_H(X)n^{-\frac{1-\alpha}{2}} - O\left(n^{-\frac{1+\alpha}{2}}\right)
\end{aligned}$$

for $\alpha \in \left(0, \frac{1}{3}\right)$. The proof of (A.162) for the case $\alpha \in \left[\frac{1}{3}, 1\right)$ is essentially the same, and therefore omitted.

(c) Following the same spirit of the proof for part (b), one can verify that constants η and η' can be chosen respectively such that

$$\left[\epsilon_n\left(\bar{\delta}\right)\Big|_{\bar{\delta}=\sigma_H\sqrt{\frac{2\alpha\ln n}{n}}+\eta\sqrt{\frac{1}{n\ln n}}}\right] \leq \frac{n^{-\alpha}}{\sqrt{\ln n}}$$

and

$$\left[\epsilon_n\left(\underline{\delta}\right)\Big|_{\underline{\delta}=\sigma_H\sqrt{\frac{2\alpha\ln n}{n}}-\eta'\sqrt{\frac{1}{n\ln n}}}\right] > \frac{n^{-\alpha}}{\sqrt{\ln n}}$$

which, together with (A.157), proves (A.163).

(d) It can be readily seen that by Theorem A.2 (b), $\bar{\delta} = \frac{\sigma_H(X)}{\sqrt{n}}Q^{-1}\left(\epsilon - \frac{CM_H(X)}{\sqrt{n}\sigma_H^3(X)}\right)$ is the right choice to guarantee

$$\epsilon_n(\bar{\delta}) \leq \epsilon$$

while $\underline{\delta} = \frac{\sigma_H(X}{\sqrt{n}}Q^{-1}\left(\epsilon + \frac{2CM_H(X)}{\sqrt{n}\sigma_H^3(X)}\right)$ will make

$$\epsilon_n(\underline{\delta}) > \epsilon$$

satisfied. (A.164) then follows immediately from (A.157) and the choices of $\bar{\delta}$ and $\underline{\delta}$.

This completes the proof of Theorem A.10. □

Remark A.3. *To show Theorem A.10 provides a non-trivial bound, we claim that*

$$\delta > r_X(\delta)$$

for $0 < \delta < \ln|\mathcal{X}| - H(X)$. *Indeed, recall the definition of* $\delta(\lambda)$ *and*

$$0 \leq r_X(\delta(1)) = H(X) + \delta(1) - \ln|\mathcal{X}|$$

which implies that $\delta(1) \geq \ln|\mathcal{X}| - H(X)$ *or* $r_X'(\delta) < 1$ *for* $0 < \delta < \ln|\mathcal{X}| - H(X)$. *The claim then follows immediately from the fact that* $r_X(0) = 0$.

Remark A.4. *In Part (d) of Theorem A.10, we can see that if* $\epsilon_n = \epsilon > 0.5$ *is selected, then* $R_n(\epsilon_n)$ *could be strictly less than* $H(X)$ *for finite block length* n*! This means that if the error probability is allowed to be slightly larger than* 0.5*, the rate of source code can be even less than the entropy rate. For an IID binary source with* $p = \Pr\{X_1 = 1\} = 0.12$*, Figure A.3 shows the tradeoff between the error probability and block length when the code rate is* 0.21% *below the entropy rate, where in Figure A.3, both the entropy rate and code rate are expressed in terms of bits. As can be seen from Figure A.3, at the block length* 1000*, the error probability is around* 0.65*, and the code rate is* 0.21% *below the entropy rate. Similar phenomenon can be seen for channel coding shown in [63].*

Remark A.5. *Related to Part (d) of Theorem A.10 is the second order source coding analysis in [19] with a fixed error probability* $0 < \epsilon < 1$*. Both results are concerned with the scenario where the rate is around the entropy rate in the order of* $\frac{1}{\sqrt{n}}$ *and the error probability is a constant. However, the work in [19] is asymptotic. On the other hand, Theorem A.10 ((A.157) and Part (d)) is non-asymptotic and valid for any block length* n*. It reveals a complete picture about the tradeoff between the rate and error probability when the error probability is constant, or approaches* 0 *with block length* n *at an exponential (Part (a)), a sub-exponential (Part (b)), a polynomial (Part (c) with* $\alpha \geq 1$*), or a sub-polynomial (Part (c) with* $0 < \alpha < 1$*) speed.*

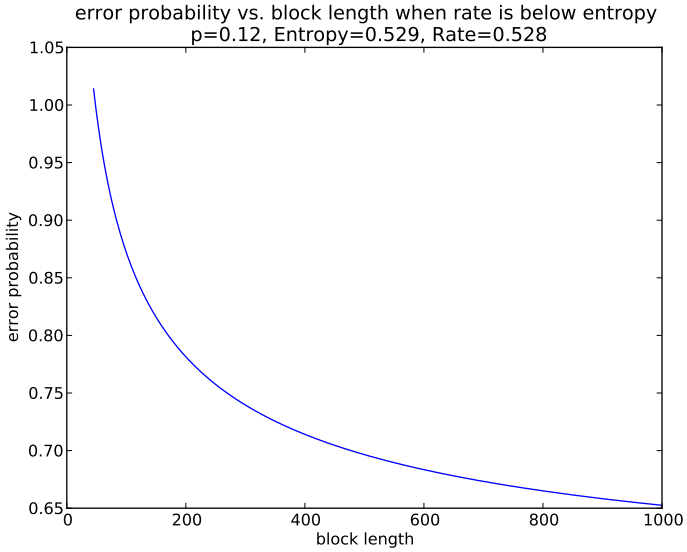


Figure A.3: Tradeoff between the error probability and block length when the rate is below the entropy rate with $p = 0.12$

Appendix B

Lemmas Related to LDPC Ensembles

B.1 LDPC ensemble with Syndrome Accumulation and Check Node Concentrated Degree Distributions

B.1.1 Proof of Lemma 6.1

We consider only the case in which $\bar{l}$ is not an integer. The case where $\bar{l}$ is an integer is a bit easier and can be dealt with in a similar manner.

Although there is thorough analysis of the probability $\Pr\{\mathbf{H}_{m\times n}x^n = 0^m\}$ for $\mathbf{H}_{m\times n}$ from $\mathcal{H}_{m,n,L(z),R(z)}$ in [64–67], the result therein in general is not applicable to $\mathbf{H}^{(b\Delta)}_{b\Delta\times n}$, the matrix obtained from syndrome accumulation on $\mathbf{H}_{n\times n}$. Towards analyzing $\Pr\left\{\mathbf{H}^{(b\Delta)}_{b\Delta\times n}x^n = 0^{b\Delta}\right\}$, we focus on $\{\mathcal{P}_{b\Delta}\}_{b=1}^{\frac{n}{\Delta}}$ defined in section 6.2.2. Given $\mathcal{P}_{b\Delta} = \{\Lambda_{b\Delta,i}\}_{i=1}^{b\Delta}$, one can classify $\Lambda_{b\Delta,i}$ into three categories:

- $\Lambda_{b\Delta,i} \subseteq \{1, 2, \ldots, R_1 n\}$,
- $\Lambda_{b\Delta,i} \subseteq \{R_1 n + 1, R_1 n + 2, \ldots, n\}$, or
- $\Lambda_{b\Delta,i} \nsubseteq \{1, 2, \ldots, R_1 n\}$, and $\Lambda_{b\Delta,i} \nsubseteq \{R_1 n + 1, R_1 n + 2, \ldots, n\}$.

To avoid complicating the analysis unnecessarily, we assume that there does not exist $\Lambda_{b\Delta,i}$ falling into the third category. Further effort reveals that this assumption holds if and only

if $2^{T-\lfloor \log_2 \Delta \rfloor} | R_1 n$, or in other words,

$$R_1 = \frac{C}{2^{\lfloor \log_2 \Delta \rfloor}}$$

for some positive integer C, where the parameter Δ is a function of block length n. In fact, we only consider the case where $\Delta \sim \sqrt{n}$, which implies $2^{\lfloor \log_2 \Delta \rfloor} \sim \sqrt{n}$, and therefore the assumption above always holds for sufficiently large n if $\bar{l}$ is a fractional number with a power of 2 as its denominator. Consequently, each $\Lambda_{b\Delta,i}$ can be further categorized into one of four cases:

- $\Lambda_{b\Delta,i} \subseteq \{1, 2, \ldots, R_1 n\}$, and $|\Lambda_{b\Delta,i}| = 2^{T-\lceil \log_2 b\Delta \rceil}$;
- $\Lambda_{b\Delta,i} \subseteq \{1, 2, \ldots, R_1 n\}$, and $|\Lambda_{b\Delta,i}| = 2^{T-\lceil \log_2 b\Delta \rceil+1}$;
- $\Lambda_{b\Delta,i} \subseteq \{R_1 n + 1, R_1 n + 2, \ldots, n\}$, and $|\Lambda_{b\Delta,i}| = 2^{T-\lceil \log_2 b\Delta \rceil}$; or
- $\Lambda_{b\Delta,i} \subseteq \{R_1 n + 1, R_1 n + 2, \ldots, n\}$, and $|\Lambda_{b\Delta,i}| = 2^{T-\lceil \log_2 b\Delta \rceil+1}$.

Now we use $\left\{t_{b\Delta}^{(i)}\right\}_{i=1}^{4}$ to represent the number of $\Lambda_{b\Delta,i}$'s falling into each category, which are given by the following formulas:

$$\begin{aligned}
t_{b\Delta}^{(1)} &= \min\left\{2b\Delta - 2^{\lceil \log_2 b\Delta \rceil}, R_1 2^{\lceil \log_2 b\Delta \rceil}\right\}, \\
t_{b\Delta}^{(2)} &= \max\left\{R_1 2^{\lceil \log_2 b\Delta \rceil - 1} - \left(b\Delta - 2^{\lceil \log_2 b\Delta \rceil - 1}\right), 0\right\}, \\
t_{b\Delta}^{(3)} &= \max\left\{R_2 2^{\lceil \log_2 b\Delta \rceil} - 2\left(2^{\lceil \log_2 b\Delta \rceil} - b\Delta\right), 0\right\}, \\
t_{b\Delta}^{(4)} &= \min\left\{2^{\lceil \log_2 b\Delta \rceil} - b\Delta, R_2 2^{\lceil \log_2 b\Delta \rceil - 1}\right\}.
\end{aligned}$$

Note that we assume that block length $n = 2^T$ for some integer T. It then follows that

$$\begin{aligned}
\frac{t_{b\Delta}^{(1)}}{n} &= \min\left\{\frac{2b\Delta}{n} - 2^{\lceil \log_2 \frac{b\Delta}{n} \rceil}, R_1 2^{\lceil \log_2 \frac{b\Delta}{n} \rceil}\right\} \\
\frac{t_{b\Delta}^{(2)}}{n} &= \max\left\{R_1 2^{\lceil \log_2 \frac{b\Delta}{n} \rceil - 1} - \left(\frac{b\Delta}{n} - 2^{\lceil \log_2 \frac{b\Delta}{n} \rceil - 1}\right), 0\right\} \\
\frac{t_{b\Delta}^{(3)}}{n} &= \max\left\{R_2 2^{\lceil \log_2 \frac{b\Delta}{n} \rceil} - 2\left(2^{\lceil \log_2 \frac{b\Delta}{n} \rceil} - \frac{b\Delta}{n}\right), 0\right\} \\
\frac{t_{b\Delta}^{(4)}}{n} &= \min\left\{2^{\lceil \log_2 \frac{b\Delta}{n} \rceil} - \frac{b\Delta}{n}, R_2 2^{\lceil \log_2 \frac{b\Delta}{n} \rceil - 1}\right\}
\end{aligned}$$

Recall that

$$c_{b\Delta} = 2^{T-\lceil \log_2 b\Delta \rceil} = 2^{-\left\lceil \log_2 \frac{b\Delta}{n} \right\rceil}.$$

Therefore $c_{b\Delta}$ also depends only on $\frac{b\Delta}{n}$.

Now define $\mathcal{H}_{n,L(z),\varkappa,b\Delta}$ as a subset of $\mathcal{H}_{n,L(z)}$ such that

$$\mathbf{H}_{n\times n} \in \mathcal{H}_{n,L(z),\varkappa,b\Delta}$$

if and only if

$$\mathbf{H}_{n\times n} \in \mathcal{H}_{n,L(z)} \text{ and } \mathbf{H}^{(b\Delta)}_{b\Delta\times n} x^n = 0^{b\Delta}$$

where $\varkappa$ is the support set of x^n. It is easy to see that given x^n (and therefore $\varkappa$), these subsets $\mathcal{H}_{n,L(z),\varkappa,b\Delta}$ are nested with each other

$$\mathcal{H}_{n,L(z),\varkappa,s\Delta} \subseteq \mathcal{H}_{n,L(z),\varkappa,b\Delta}$$

if $s \geq b$. Furthermore, let $\aleph_{n,L(z),\varkappa,b\Delta} = |\mathcal{H}_{n,L(z),\varkappa,b\Delta}|$. Then we have

$$\Pr\left\{\mathbf{H}^{(b\Delta)}_{b\Delta\times n} x^n = 0^{b\Delta}\right\} = \frac{\aleph_{n,L(z),\varkappa,b\Delta}}{|\mathcal{H}_{n,L(z)}|} \tag{B.1}$$

where $\mathbf{H}_{n\times n}$ is uniformly picked from $\mathcal{H}_{n,L(z)}$. Therefore the main issue is to derive asymptotic formulas for $|\mathcal{H}_{n,L(z)}|$ and $\aleph_{n,L(z),\varkappa,b\Delta}$. At this point, we invoke the following result from Mineev and Pavlov [68] (see also [69] for a stronger version).

Theorem B.1 (Mineev-Pavlov)**.** *Suppose $\mathcal{H}_{\vec{r},\vec{l}}$ is the ensemble of $m \times n$ 0-1 matrices with i-th row sum r_i and j-th column sum l_j satisfying $\max\{r_i, l_j : 1 \leq i \leq m \text{ and } 1 \leq j \leq n\} \leq \log^{1/4-\epsilon} m$, where ϵ is an arbitrarily small positive constant. Then*

$$\begin{aligned} |\mathcal{H}_{\vec{r},\vec{l}}| &= \frac{(\sum_{i=1}^m r_i)!}{(\prod_{i=1}^m r_i!)\,(\prod_{i=1}^n l_i!)} \\ &\quad \times \left[\exp\left\{-\frac{2}{(2\sum_{i=1}^m r_i)^2}\left(\sum_{i=1}^m r_i(r_i-1)\sum_{j=1}^n l_j(l_j-1)\right)\right\} + o(m^{-0.5+\delta})\right] \end{aligned} \tag{B.2}$$

where $0 < \delta < 0.5$ is an arbitrarily small constant.

First of all, applying Theorem B.1 to $|\mathcal{H}_{n,L(z)}|$, we have

$$|\mathcal{H}_{n,L(z)}| = \frac{(\bar{l}n)!}{(r_1!)^{R_1 n}(r_2!)^{R_2 n}\prod_{i=1}^L (l_i!)^{L_i n}}(C_{L(z)} + o(n^{-0.5+\delta}))$$

where

$$C_{L(z)} = \exp\left\{ -\frac{(R_1 r_1(r_1-1) + R_2 r_2(r_2-1)) \sum_{i=1}^{L} L_i l_i(l_i-1)}{2\bar{l}^2} \right\}$$

Towards calculating $\aleph_{n,L(z),\varkappa,b\Delta}$, note that each $\mathbf{H}_{n\times n}$ consists of two sub-matrices $\mathbf{H}^{\varkappa}_{n\times|\varkappa|}$ and $\mathbf{H}^{\varkappa^c}_{n\times(n-|\varkappa|)}$, where $\varkappa^c$ is the complement of $\varkappa$. Suppose $\{r_i^{\varkappa}\}_{i=1}^{n}$ is the row-sum profile of $\mathbf{H}^{\varkappa}_{n\times|\varkappa|}$. Then the row-sum profile $\{r_i^{\varkappa^c}\}_{i=1}^{n}$ of $\mathbf{H}^{\varkappa^c}_{n\times(n-|\varkappa|)}$ is given by

$$\begin{aligned} r_i^{\varkappa^c} &= r_1 - r_i^{\varkappa} \text{ for } 1 \le i \le R_1 n \\ r_i^{\varkappa^c} &= r_2 - r_i^{\varkappa} \text{ for } R_1 n + 1 \le i \le n \end{aligned}$$

For each $\mathbf{H}_{n\times n} \in \mathcal{H}_{n,L(z)}$, its $\mathbf{H}^{\varkappa}_{n\times|\varkappa|}$ and $\mathbf{H}^{\varkappa^c}_{n\times(n-|\varkappa|)}$ should have $L^{\varkappa}(z)$ and $L^{\varkappa^c}(z)$ as their column-sum profiles. Therefore

$$0 \le r_i^{\varkappa} \le r_1 \text{ for } 1 \le i \le R_1 n \tag{B.3}$$

$$0 \le r_i^{\varkappa} \le r_2 \text{ for } R_1 n + 1 \le i \le n \tag{B.4}$$

$$\sum_{i=1}^{n} r_i^{\varkappa} = \bar{l}^{\varkappa} n \tag{B.5}$$

Note that

$$\begin{aligned}
\mathbf{H}_{b\Delta\times n}^{(b\Delta)}x^n &= \begin{pmatrix} \sum_{i\in\Lambda_1} h_{i,1} & \sum_{i\in\Lambda_1} h_{i,2} & \cdots & \sum_{i\in\Lambda_1} h_{i,n} \\ \vdots & \vdots & \ddots & \vdots \\ \sum_{i\in\Lambda_{b\Delta}} h_{i,1} & \sum_{i\in\Lambda_{b\Delta}} h_{i,2} & \cdots & \sum_{i\in\Lambda_{b\Delta}} h_{i,n} \end{pmatrix} x^n \\
&= \underbrace{\begin{pmatrix} \sum_{i\in\Lambda_1} h_{i,j_1} & \sum_{i\in\Lambda_1} h_{i,j_2} & \cdots & \sum_{i\in\Lambda_1} h_{i,j_{|\varkappa|}} \\ \vdots & \vdots & \ddots & \vdots \\ \sum_{i\in\Lambda_{b\Delta}} h_{i,j_1} & \sum_{i\in\Lambda_{b\Delta}} h_{i,j_2} & \cdots & \sum_{i\in\Lambda_{b\Delta}} h_{i,j_{|\varkappa|}} \end{pmatrix}}_{\varkappa} \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix} \\
&= \begin{pmatrix} \sum_{j\in\varkappa}\sum_{i\in\Lambda_1} h_{ij} \\ \vdots \\ \sum_{j\in\varkappa}\sum_{i\in\Lambda_{b\Delta}} h_{ij} \end{pmatrix} \\
&= \begin{pmatrix} \sum_{i\in\Lambda_1}\sum_{j\in\varkappa} h_{ij} \\ \vdots \\ \sum_{i\in\Lambda_{b\Delta}}\sum_{j\in\varkappa} h_{ij} \end{pmatrix} \\
&= \begin{pmatrix} \sum_{i\in\Lambda_1} r_i^{\varkappa} \\ \vdots \\ \sum_{i\in\Lambda_{b\Delta}} r_i^{\varkappa} \end{pmatrix}
\end{aligned}$$

Then $\mathbf{H}_{n\times n} \in \mathcal{H}_{n,L(z),\varkappa,b\Delta}$ if and only if

$$2 \left| \sum_{u=1}^{c_{b\Delta}} r^{\varkappa}_{c_{b\Delta}j+u} \quad \text{for } 0 \le j \le t_{b\Delta}^{(1)} - 1 \right. \tag{B.6}$$

$$2 \left| \sum_{u=1}^{2c_{b\Delta}} r^{\varkappa}_{t_{b\Delta}^{(1)}c_{b\Delta}+2c_{b\Delta}j+u} \quad \text{for } 0 \le j \le t_{b\Delta}^{(2)} - 1 \right. \tag{B.7}$$

$$2 \left| \sum_{u=1}^{c_{b\Delta}} r^{\varkappa}_{t_{b\Delta}^{(1)}c_{b\Delta}+2t_{b\Delta}^{(2)}c_{b\Delta}+c_{b\Delta}j+u} \quad \text{for } 0 \le j \le t_{b\Delta}^{(3)} - 1 \right. \tag{B.8}$$

$$2 \left| \sum_{u=1}^{2c_{b\Delta}} r^{\varkappa}_{t_{b\Delta}^{(1)}c_{b\Delta}+2t_{b\Delta}^{(2)}c_{b\Delta}+t_{b\Delta}^{(3)}c_{b\Delta}+2c_{b\Delta}j+u} \quad \text{for } 0 \le j \le t_{b\Delta}^{(4)} - 1 \right. \tag{B.9}$$

Let $\mathcal{R}_{b\Delta,\bar{l}^{\varkappa}}$ denote the set of all row-sum profiles $\{r_i^{\varkappa}\}_{i=1}^n$ which satisfy the constraints (B.3) to (B.9). Furthermore, let $\aleph^{\varkappa}_{\{r_i^{\varkappa}\}_{i=1}^n}$ and $\aleph^{\varkappa^c}_{\{r_i^{\varkappa^c}\}_{i=1}^n}$ denote the number of $\mathbf{H}^{\varkappa}_{n\times|\varkappa|}$'s and

$\mathbf{H}^{\varkappa^c}_{n\times(n-|\varkappa|)}$'s with the given row profile $\{r_i^{\varkappa}\}^n$ and $\{r_i^{\varkappa^c}\}^n$, respectively. Then it is easy to see that

$$\aleph_{n,L(z),\varkappa,b\Delta} = \sum_{\{r_i\}_{i=1}^n \in \mathcal{R}_{b\Delta,\bar{l}^{\varkappa}}} \aleph^{\varkappa}_{\{r_i^{\varkappa}\}_{i=1}^n} \aleph^{\varkappa^c}_{\{r_i^{\varkappa^c}\}_{i=1}^n} \tag{B.10}$$

Applying Theorem B.1 to $\aleph^{\varkappa}_{\{r_i^{\varkappa}\}_{i=1}^n}$ and $\aleph^{\varkappa^c}_{\{r_i^{\varkappa^c}\}_{i=1}^n}$, we have

$$\begin{aligned}\aleph^{\varkappa}_{\{r_i^{\varkappa}\}_{i=1}^n} &= \frac{(\sum_{i=1}^n r_i^{\varkappa})!}{(\prod_{i=1}^n r_i^{\varkappa}!)\prod_{i=1}^L (l_i!)^{L_i^{\varkappa} n}}(C_{r^{\varkappa}} + o(n^{-0.5+\delta})) \\ &= \frac{(\bar{l}^{\varkappa} n)!}{(\prod_{i=1}^n r_i^{\varkappa}!)\prod_{i=1}^L (l_i!)^{L_i^{\varkappa} n}}(C_{r^{\varkappa}} + o(n^{-0.5+\delta})) \end{aligned} \tag{B.11}$$

where

$$\exp\left\{-\frac{r_2(l_L-1)}{2}\right\} \le \exp\left\{-\frac{r_2\sum_{i=1}^L L_i^{\varkappa} l_i(l_i-1)}{2\bar{l}^{\varkappa}}\right\} \le C_{r^{\varkappa}} \le 1\,.$$

Similarly,

$$\aleph^{\varkappa^c}_{\{r_i^{\varkappa^c}\}_{i=1}^n} = \frac{\big((\bar{l}-\bar{l}^{\varkappa})n\big)!}{\Big(\prod_{i=1}^{R_1 n}(r_1 - r_i^{\varkappa})!\prod_{i=R_1 n+1}^n (r_2 - r_i^{\varkappa})!\Big)\prod_{i=1}^L (l_i!)^{(L_i - L_i^{\varkappa})n}}(C_{r^{\varkappa^c}} + o(n^{-0.5+\delta})) \tag{B.12}$$

where

$$\exp\left\{-\frac{r_2(l_L-1)}{2}\right\} \le \exp\left\{-\frac{r_2\sum_{i=1}^L (L_i - L_i^{\varkappa}) l_i(l_i-1)}{2(\bar{l}-\bar{l}^{\varkappa})}\right\} \le C_{r^{\varkappa^c}} \le 1\,.$$

Combining (B.1) with (B.10) to (B.12) yields

$$\begin{aligned}\Pr\left\{\mathbf{H}^{(b\Delta)}_{b\Delta\times n} x^n = 0^{b\Delta}\right\} &= \frac{\aleph_{n,L(z),\varkappa,b\Delta}}{|\mathcal{H}_{n,L(z)}|} \\ &\le \frac{2}{C_{L(z)}} \frac{\sum_{\{r_i^{\varkappa}\}_{i=1}^n \in \mathcal{R}_{b\Delta,\varkappa}} \frac{C_{r^{\varkappa}} C_{r^{\varkappa^c}} \big(n\bar{l}^{\varkappa}\big)!\big(n(\bar{l}-\bar{l}^{\varkappa})\big)!}{\prod_{i=1}^L (l_i!)^{L_i n}\prod_{i=1}^{R_1 n} r_i^{\varkappa}!(r_1 - r_i^{\varkappa})!\prod_{i=R_1 n+1}^n r_i^{\varkappa}!(r_2 - r_i^{\varkappa})!}}{\frac{(n\bar{l})!}{(r_1!)^{R_1 n}(r_2!)^{R_2 n}\prod_{i=1}^L (l_i!)^{L_i n}}} \\ &\le \frac{2}{C_{L(z)}} \binom{n\bar{l}}{n\bar{l}^{\varkappa}}^{-1} \sum_{\{r_i^{\varkappa}\}_{i=1}^n \in \mathcal{R}_{b\Delta,\varkappa}} \prod_{i=1}^{R_1 n}\binom{r_1}{r_i^{\varkappa}} \prod_{i=R_1 n+1}^{n}\binom{r_2}{r_i^{\varkappa}} \end{aligned} \tag{B.13}$$

where

$$\frac{\left(C_{r^{\varkappa}}+o(n^{-0.5+\delta})\right)\left(C_{r^{\varkappa^c}}+o(n^{-0.5+\delta})\right)}{C_{L(z)}+o(n^{-0.5+\delta})} \leq \frac{2C_{r^{\varkappa}}C_{r^{\varkappa^c}}}{C_{L(z)}}$$

for sufficiently large n as $\delta > 0$ can be arbitrarily small. To further evaluate $\Pr\{\mathbf{H}^{(b\Delta)}_{b\Delta\times n}x^n = 0^{b\Delta}\}$, we define the type $\left(m^{(1)}, m^{(2)}, m^{(3)}, m^{(4)}\right)$ of $\{r_i^{\varkappa}\}_{i=1}^n$ as follows:

$$\begin{aligned}
m_s^{(1)} &\stackrel{\Delta}{=} \sum_{j=0}^{t_{b\Delta}^{(1)}-1} \delta\left(\sum_{u=1}^{c_{b\Delta}} r^{\varkappa}_{c_{b\Delta}j+u} - s\right) \text{ for } 0 \leq s \leq c_{b\Delta}r_1 \\
m_s^{(2)} &\stackrel{\Delta}{=} \sum_{j=0}^{t_{b\Delta}^{(2)}-1} \delta\left(\sum_{u=1}^{2c_{b\Delta}} r^{\varkappa}_{c_{b\Delta}t_{b\Delta}^{(1)}+2c_{b\Delta}j+u} - s\right) \text{ for } 0 \leq s \leq 2c_{b\Delta}r_1 \\
m_s^{(3)} &\stackrel{\Delta}{=} \sum_{j=0}^{t_{b\Delta}^{(3)}-1} \delta\left(\sum_{u=1}^{c_{b\Delta}} r^{\varkappa}_{t_{b\Delta}^{(1)}+2t_{b\Delta}^{(2)}c_{b\Delta}+c_{b\Delta}j+u} - s\right) \text{ for } 0 \leq s \leq c_{b\Delta}r_2 \\
m_s^{(4)} &\stackrel{\Delta}{=} \sum_{j=0}^{t_{b\Delta}^{(4)}-1} \delta\left(\sum_{u=1}^{2c_{b\Delta}} r^{\varkappa}_{t_{b\Delta}^{(1)}c_{b\Delta}+2t_{b\Delta}^{(2)}c_{b\Delta}+t_{b\Delta}^{(3)}c_{b\Delta}+2c_{b\Delta}j+u} - s\right) \text{ for } 0 \leq s \leq 2c_{b\Delta}r_2
\end{aligned}$$

where

$$\delta(x) \stackrel{\Delta}{=} \begin{cases} 1 & \text{if } x = 0 \\ 0 & \text{otherwise.} \end{cases}$$

Now we can see that $\{r_i^{\varkappa}\}_{i=1}^n$ belongs to $\mathcal{R}_{b\Delta,\varkappa}$ if and only if its type $\left(m^{(1)}, m^{(2)}, m^{(3)}, m^{(4)}\right)$ satisfies

$$\sum_{j=0}^{\lfloor \frac{c_{b\Delta}r_1}{2} \rfloor} m_{2j}^{(1)} = t_{b\Delta}^{(1)} \tag{B.14}$$

$$\sum_{j=0}^{c_{b\Delta}r_1} m_{2j}^{(2)} = t_{b\Delta}^{(2)} \tag{B.15}$$

$$\sum_{j=0}^{\lfloor \frac{c_{b\Delta}r_2}{2} \rfloor} m_{2j}^{(3)} = t_{b\Delta}^{(3)} \tag{B.16}$$

$$\sum_{j=0}^{c_{b\Delta}r_2} m_{2j}^{(4)} = t_{b\Delta}^{(4)} \tag{B.17}$$

and

$$\sum_{j=0}^{\lfloor \frac{c_{b\Delta} r_1}{2} \rfloor} 2j \cdot m_{2j}^{(1)} + \sum_{j=0}^{c_{b\Delta} r_1} 2j \cdot m_{2j}^{(2)} + \sum_{j=0}^{\lfloor \frac{c_{b\Delta} r_2}{2} \rfloor} 2j \cdot m_{2j}^{(3)} + \sum_{j=0}^{c_{b\Delta} r_2} 2j \cdot m_{2j}^{(4)} = \bar{l}^{\varkappa} n \tag{B.18}$$

Denote the set of types $\left\{m^{(1)}, m^{(2)}, m^{(3)}, m^{(4)}\right\}$ satisfying the above constraints (B.14) to (B.18) by $\mathcal{M}_{b\Delta,\varkappa}$. If $\mathcal{M}_{b\Delta,\varkappa} \neq \emptyset$, then the constraints (B.14) to (B.18) implies

$$\begin{aligned}
&0 \leq \\
&\sum_{j=0}^{\lfloor \frac{c_{b\Delta} r_1}{2} \rfloor} (c_{b\Delta} r_1 - \pi(c_{b\Delta} r_1) - 2j) m_{2j}^{(1)} + \sum_{j=0}^{c_{b\Delta} r_1} (2c_{b\Delta} r_1 - 2j) m_{2j}^{(2)} \\
&+ \sum_{j=0}^{\lfloor \frac{c_{b\Delta} r_2}{2} \rfloor} (c_{b\Delta} r_2 - \pi(c_{b\Delta} r_2) - 2j) m_{2j}^{(3)} + \sum_{j=0}^{c_{b\Delta} r_2} (2c_{b\Delta} r_2 - 2j) m_{2j}^{(4)} \\
&= t_{b\Delta}^{(1)} (c_{b\Delta} r_1 - \pi(c_{b\Delta} r_1)) + 2t_{b\Delta}^{(2)} c_{b\Delta} r_1 + t_{b\Delta}^{(3)} (c_{b\Delta} r_2 - \pi(c_{b\Delta} r_2)) + 2t_{b\Delta}^{(4)} c_{b\Delta} r_2 - \bar{l}^{\varkappa} n \\
&= n\bar{l} - t_{b\Delta}^{(1)} \pi(c_{b\Delta} r_1) - t_{b\Delta}^{(3)} \pi(c_{b\Delta} r_2) - \bar{l}^{\varkappa} n
\end{aligned} \tag{B.19}$$

and therefore

$$\bar{l}^{\varkappa} \leq \bar{l} - \frac{t_{b\Delta}^{(1)}}{n} \pi(c_{b\Delta} r_1) - \frac{t_{b\Delta}^{(3)}}{n} \pi(c_{b\Delta} r_2).$$

On the other hand, $\mathcal{M}_{t,\theta} = \emptyset$ implies $\Pr\left\{\mathbf{H}_{b\Delta \times n}^{(b\Delta)} x^n = 0^{b\Delta}\right\} = 0$, and hence the lemma is proved when

$$\bar{l}^{\varkappa} > \bar{l} - \frac{t_{b\Delta}^{(1)}}{n} \pi(c_{b\Delta} r_1) - \frac{t_{b\Delta}^{(3)}}{n} \pi(c_{b\Delta} r_2).$$

Now suppose

$$\bar{l}^{\varkappa} < \bar{l} - \frac{t_{b\Delta}^{(1)}}{n} \pi(c_{b\Delta} r_1) - \frac{t_{b\Delta}^{(3)}}{n} \pi(c_{b\Delta} r_2).$$

For convenience, define

$$\begin{aligned}
k^{(1)} &= \frac{c_{b\Delta} r_1 - \pi(c_{b\Delta} r_1)}{2} \\
k^{(2)} &= c_{b\Delta} r_1 \\
k^{(3)} &= \frac{c_{b\Delta} r_2 - \pi(c_{b\Delta} r_2)}{2} \\
k^{(4)} &= c_{b\Delta} r_2
\end{aligned}$$

To proceed, we can group $\{r_i^{\varkappa}\}_{i=1}^n$ with the same type together, and therefore have

$$\sum_{\{r_i^{\varkappa}\}_{i=1}^n \in \mathcal{R}_{b\Delta,\varkappa}} \prod_{i=1}^{R_1 n} \left(\begin{array}{c} r_1 \\ r_i^{\varkappa} \end{array} \right) \prod_{i=R_1 n+1}^{n} \left(\begin{array}{c} r_2 \\ r_i^{\varkappa} \end{array} \right) =$$

$$\sum_{\left\{m^{(1)},m^{(2)},m^{(3)},m^{(4)}\right\} \in \mathcal{M}_{b\Delta,\varkappa}} \prod_{i=1}^{4} \left(\begin{array}{c} t_{b\Delta}^{(i)} \\ m_0^{(i)}, m_2^{(i)}, \ldots, m_{2k^{(i)}}^{(i)} \end{array} \right)$$

$$\prod_{j=0}^{k^{(1)}} \left(\sum_{\{r_u^{\varkappa}\}_{u=1}^{c_{b\Delta}} : \sum_{u=1}^{c_{b\Delta}} r_u = 2j} \prod_{u=1}^{c_{b\Delta}} \left(\begin{array}{c} r_1 \\ r_u^{\varkappa} \end{array} \right) \right)^{m_{2j}^{(1)}}$$

$$\prod_{j=0}^{k^{(2)}} \left(\sum_{\{r_u^{\varkappa}\}_{u=1}^{2c_{b\Delta}} : \sum_{u=1}^{2c_{b\Delta}} r_u^{\varkappa} = 2j} \prod_{u=1}^{2c_{b\Delta}} \left(\begin{array}{c} r_1 \\ r_u^{\varkappa} \end{array} \right) \right)^{m_{2j}^{(2)}}$$

$$\prod_{j=0}^{k^{(3)}} \left(\sum_{\{r_u^{\varkappa}\}_{u=1}^{c_{b\Delta}} : \sum_{u=1}^{c_{b\Delta}} r_u^{\varkappa} = 2j} \prod_{u=1}^{c_{b\Delta}} \left(\begin{array}{c} r_2 \\ r_u^{\varkappa} \end{array} \right) \right)^{m_{2j}^{(3)}}$$

$$\prod_{j=0}^{k^{(4)}} \left(\sum_{\{r_u^{\varkappa}\}_{u=1}^{2c_{b\Delta}} : \sum_{u=1}^{c_{b\Delta}} r_u^{\varkappa} = 2j} \prod_{u=1}^{2c_{b\Delta}} \left(\begin{array}{c} r_2 \\ r_u^{\varkappa} \end{array} \right) \right)^{m_{2j}^{(4)}} .$$

Now define for any $j \geq 0$

$$\begin{aligned}
\xi_j^{(1)} &\triangleq \sum_{\{r_u^{\varkappa}\}_{u=1}^{c_{b\Delta}} : \sum_{u=1}^{c_{b\Delta}} r_u^{\varkappa} = j} \prod_{u=1}^{c_{b\Delta}} \left(\begin{array}{c} r_1 \\ r_u^{\varkappa} \end{array} \right) \\
\xi_j^{(2)} &\triangleq \sum_{\{r_u^{\varkappa}\}_{u=1}^{2c_{b\Delta}} : \sum_{u=1}^{2c_{b\Delta}} r_u^{\varkappa} = j} \prod_{u=1}^{2c_{b\Delta}} \left(\begin{array}{c} r_1 \\ r_u^{\varkappa} \end{array} \right) \\
\xi_j^{(3)} &\triangleq \sum_{\{r_u^{\varkappa}\}_{u=1}^{c_{b\Delta}} : \sum_{u=1}^{c_{b\Delta}} r_u^{\varkappa} = j} \prod_{u=1}^{c_{b\Delta}} \left(\begin{array}{c} r_2 \\ r_u^{\varkappa} \end{array} \right) \\
\xi_j^{(4)} &\triangleq \sum_{\{r_u^{\varkappa}\}_{u=1}^{2c_{b\Delta}} : \sum_{u=1}^{2c_{b\Delta}} r_u^{\varkappa} = j} \prod_{u=1}^{2c_{b\Delta}} \left(\begin{array}{c} r_2 \\ r_u^{\varkappa} \end{array} \right) .
\end{aligned}$$

Furthermore, we define

$$M_{\left\{m^{(i)}\right\}_{i=1}^{4}} \triangleq \prod_{i=1}^{4}\left[\left(\begin{array}{c} t_{b\Delta}^{(i)} \\ m_0^{(i)}, m_2^{(i)}, \ldots, m_{2k^{(i)}}^{(i)} \end{array}\right)\prod_{j=0}^{k^{(i)}}\left(\xi_{2j}^{(i)}\right)^{m_{2j}^{(i)}}\right].$$

Therefore

$$\sum_{\left\{r_i^{\varkappa}\right\}_{i=1}^{n}\in\mathcal{R}_{b\Delta,\varkappa}}\prod_{i=1}^{R_1 n}\left(\begin{array}{c} r_1 \\ r_i^{\varkappa} \end{array}\right)\prod_{i=R_1 n+1}^{n}\left(\begin{array}{c} r_2 \\ r_i^{\varkappa} \end{array}\right) = \sum_{\left\{m^{(i)}\right\}_{i=1}^{4}\in\mathcal{M}_{b\Delta,\varkappa}} M_{\left\{m^{(i)}\right\}_{i=1}^{4}}.$$

In view of (B.14) to (B.18), we can get a trivial bound on $|\mathcal{M}_{b\Delta,\kappa}|$ as follows:

$$\begin{aligned}|\mathcal{M}_{b\Delta,\varkappa}| &\leq \left(\frac{n\bar{l}^{\varkappa}}{2}+1\right)^{k^{(1)}}\left(\frac{n\bar{l}^{\varkappa}}{2}+1\right)^{k^{(2)}}\left(\frac{n\bar{l}^{\varkappa}}{2}+1\right)^{k^{(3)}}\left(\frac{n\bar{l}^{\varkappa}}{2}+1\right)^{k^{(4)}} \\ &\leq \left(n\bar{l}^{\varkappa}\right)^{k^{(1)}+k^{(2)}+k^{(3)}+k^{(4)}} \leq \left(n\bar{l}^{\varkappa}\right)^{3\lceil\bar{l}\rceil c_{b\Delta}}.\end{aligned}$$

In a similar manner, in view of (B.14) to (B.17) and (B.19, we have

$$|\mathcal{M}_{b\Delta,\varkappa}| \leq \left(n(\bar{l}-\bar{l}^{\varkappa})\right)^{3\lceil\bar{l}\rceil c_{b\Delta}}.$$

Define

$$\hat{l}^{\varkappa} = \max\left\{\frac{1}{n}, \min\{\bar{l}^{\varkappa}, \bar{l}-\bar{l}^{\varkappa}\}\right\}.$$

Then we have

$$\begin{aligned}&\sum_{\left\{m^{(i)}\right\}_{i=1}^{4}\in\mathcal{M}_{b\Delta,\varkappa}} M_{\left\{m^{(i)}\right\}_{i=1}^{4}} \\ &\leq \left(n\hat{l}^{\varkappa}\right)^{3\lceil\bar{l}\rceil c_{b\Delta}} \max_{\left\{m^{(i)}\right\}_{i=1}^{4}\in\mathcal{M}_{b\Delta,\varkappa}} M_{\left\{m^{(i)}\right\}_{i=1}^{4}} \\ &\leq \exp\left\{\frac{3n\lceil\bar{l}\rceil}{b\Delta}\ln(n\hat{l}^{\varkappa})\right\} \max_{\left\{m^{(i)}\right\}_{i=1}^{4}\in\mathcal{M}_{b\Delta,\varkappa}} M_{\left\{m^{(i)}\right\}_{i=1}^{4}}\end{aligned}$$

where the last inequality is due to the fact that $c_{b\Delta} \leq \frac{n}{b\Delta}$. This, coupled with (B.13), implies

$$\begin{aligned}&\Pr\left\{\mathbf{H}_{b\Delta\times n}^{(b\Delta)}x^n = 0^{b\Delta}\right\} \\ &\leq \exp\left\{\frac{3n\lceil\bar{l}\rceil}{b\Delta}\ln(n\hat{l}^{\varkappa})+O(1)\right\}\left(\begin{array}{c} n\bar{l} \\ n\bar{l}^{\varkappa} \end{array}\right)^{-1} \max_{\left\{m^{(i)}\right\}_{i=1}^{4}\in\mathcal{M}_{b\Delta,\varkappa}} M_{\left\{m^{(i)}\right\}_{i=1}^{4}}. \qquad \text{(B.20)}\end{aligned}$$

To continue, we now upper bound

$$\max_{\left\{m^{(i)}\right\}_{i=1}^{4}\in\mathcal{M}_{b\Delta,\varkappa}} M_{\left\{m^{(i)}\right\}_{i=1}^{4}}$$

under the conditions (B.14) to (B.18). By the type bound [42, Lemma 2.3],

$$\begin{aligned}
\max \ln M_{\left\{m^{(i)}\right\}_{i=1}^{4}} &= \max \ln \prod_{i=1}^{4}\left(\frac{t_{b\Delta}^{(i)}!}{\prod_{j=0}^{k^{(i)}} m_{2j}^{(i)}!}\prod_{j=0}^{k^{(i)}}\left(\xi_{2j}^{(i)}\right)^{m_{2j}^{(i)}}\right) \\
&\leq \max\left\{\sum_{i=1}^{4} t_{b\Delta}^{(i)}\ln t_{b\Delta}^{(i)} - \sum_{i=1}^{4}\sum_{j=0}^{k^{(i)}}\left(m_{2j}^{(i)}\ln m_{2j}^{(i)}\right) + \sum_{i=1}^{4}\sum_{j=0}^{k^{(i)}} m_{2j}^{(i)}\ln\xi_{2j}^{(i)}\right\} \\
&\leq \max G\left(\left\{m^{(i)}\right\}_{i=1}^{4}\right) \qquad \text{(B.21)}
\end{aligned}$$

where

$$G\left(\left\{m^{(i)}\right\}_{i=1}^{4}\right) \triangleq \sum_{i=1}^{4} t_{b\Delta}^{(i)}\ln t_{b\Delta}^{(i)} - \sum_{i=1}^{4}\sum_{j=0}^{k^{(i)}}\left(m_{2j}^{(i)}\ln m_{2j}^{(i)}\right) + \sum_{i=1}^{4}\sum_{j=0}^{k^{(i)}} m_{2j}^{(i)}\ln\xi_{2j}^{(i)} \qquad \text{(B.22)}$$

in which $m_{2j}^{(i)}$ can take any non-negative real number with constraints (B.14) to (B.18). Since the function

$$f(x) = -x\ln x + cx$$

is concave in the region $x > 0$, it follows that $G\left(\left\{m^{(i)}\right\}_{i=1}^{4}\right)$ is a concave function, and hence the maximum can be calculated by using K.K.T condition, which is shown as follows.

Define the function $F\left(\left\{m^{(i)}\right\}_{i=1}^{4}, \{\alpha_i\}_{i=1}^{4}, \beta\right)$ as

$$F\left(\left\{m^{(i)}\right\}_{i=1}^{4}, \{\alpha_i\}_{i=1}^{4}, \beta\right) = G\left(\left\{m^{(i)}\right\}_{i=1}^{4}\right) + \sum_{i=1}^{4}\alpha_i\sum_{j=0}^{k^{(i)}} m_{2j}^{(i)} + \beta\sum_{i=1}^{4}\sum_{j=0}^{k^{(i)}} 2j m_{2j}^{(i)}$$

Now by taking the derivative of $F\left(\left\{m^{(i)}\right\}_{i=1}^{4}, \{\alpha_i\}_{i=1}^{4}, \beta\right)$ with respect to $m^{(i)}$, we have

$$\frac{\partial F}{\partial m_{2j}^{(i)}} = -\ln m_{2j}^{(i)} - 1 + \ln\xi_{2j}^{(i)} + \alpha_i + 2j\beta.$$

According to K.K.T condition, let this derivative be zero, and we have

$$m_{2j}^{(i)} = e^{\alpha_i - 1 + 2j\beta} \xi_{2j}^{(i)}.$$

Since

$$\sum_{j=0}^{k^{(i)}} m_{2j}^{(i)} = t_{b\Delta}^{(i)}$$

it follows that

$$e^{\alpha_i - 1} \sum_{j=0}^{k^{(i)}} \xi_{2j}^{(i)} \left(e^{\beta}\right)^{2j} = t_{b\Delta}^{(i)}.$$

For convenience, define

$$g^{(i)}(\tau) \stackrel{\Delta}{=} \sum_{j=0}^{k^{(i)}} \xi_{2j}^{(i)} \tau^{2j}.$$

Then

$$e^{\alpha_i - 1} = \frac{t_{b\Delta}^{(i)}}{g^{(i)}(e^{\beta})}$$

which implies

$$m_{2j}^{(i)} = \frac{t_{b\Delta}^{(i)}}{g^{(i)}(e^{\beta})} e^{2j\beta} \xi_{2j}^{(i)}. \tag{B.23}$$

Now by taking into account the condition

$$\sum_{i=1}^{4} \sum_{j=0}^{k^{(i)}} 2j m_{2j}^{(i)} = \bar{l}^{\varkappa} n$$

we have

$$\sum_{i=1}^{4} \frac{t_{b\Delta}^{(i)}}{g^{(i)}(e^{\beta})} \sum_{j=0}^{k^{(i)}} 2j e^{2j\beta} \xi_{2j}^{(i)} = \bar{l}^{\varkappa} n.$$

It is easy to see that

$$\sum_{j=0}^{k^{(i)}} 2j \tau^{2j} \xi_{2j}^{(i)} = \tau g'^{(i)}(\tau) \tag{B.24}$$

where

$$g'^{(i)}(\tau) = \frac{dg^{(i)}(\tau)}{d\tau}.$$

Therefore e^β is the solution to

$$\sum_{i=1}^{4} t_{b\Delta}^{(i)} \frac{e^\beta g'^{(i)}(e^\beta)}{g^{(i)}(e^\beta)} = \bar{l}^{\varkappa} n. \tag{B.25}$$

Putting (B.22) to (B.25) together yields

$$\begin{aligned}
\max G\left(\left\{m^{(i)}\right\}_{i=1}^{4}\right) &= \sum_{i=1}^{4}\left[t_{b\Delta}^{(i)} \ln t_{b\Delta}^{(i)} - \sum_{j=0}^{k^{(i)}} \frac{t_{b\Delta}^{(i)}}{g^{(i)}(e^\beta)} e^{2j\beta} \xi_{2j}^{(i)} \ln \frac{t_{b\Delta}^{(i)}}{g^{(i)}(e^\beta)} e^{2j\beta}\right] \\
&= \sum_{i=1}^{4}\left[t_{b\Delta}^{(i)} \ln g^{(i)}(e^\beta) - \beta t_{b\Delta}^{(i)} \frac{e^\beta g'^{(i)}(e^\beta)}{g^{(i)}(e^\beta)}\right] \\
&= \sum_{i=1}^{4} t_{b\Delta}^{(i)} \ln g^{(i)}(e^\beta) - \bar{l}^{\varkappa} n\beta.
\end{aligned}$$

Substituting e^β by τ, we have

$$\max G\left(\left\{m^{(i)}\right\}_{i=1}^{4}\right) = \sum_{i=1}^{4} t_{b\Delta}^{(i)} \ln g^{(i)}(\tau) - \bar{l}^{\varkappa} n \ln \tau \tag{B.26}$$

where τ is the solution to

$$\sum_{i=1}^{4} t_{b\Delta}^{(i)} \frac{\tau g'^{(i)}(\tau)}{g^{(i)}(\tau)} = \bar{l}^{\varkappa} n. \tag{B.27}$$

Notice that

$$\begin{aligned}
(1+\tau)^{c_{b\Delta} r_1} &= ((1+\tau)^{r_1})^{c_{b\Delta}} \\
&= \prod_{u=1}^{c_{b\Delta}} \left(\sum_{r_u^{\varkappa}=0}^{r_1} \binom{r_1}{r_u^{\varkappa}} \tau^{r_u^{\varkappa}}\right) \\
&= \sum_{j=0}^{c_{b\Delta} r_1} \xi_j^{(1)} \tau^j.
\end{aligned}$$

Meanwhile

$$(1-\tau)^{c_{b\Delta} r_1} = \sum_{j=0}^{c_{b\Delta} r_1} \xi_j^{(1)} (-1)^j \tau^j.$$

Therefore

$$\begin{aligned} g^{(1)}(\tau) &= \sum_{j=0}^{k^{(1)}} \xi_{2j}^{(1)}(\tau)^{2j} \\ &= \frac{(1+\tau)^{c_{b\Delta}r_1} + (1-\tau)^{c_{b\Delta}r_1}}{2} \\ &= \frac{g(\tau, c_{b\Delta}r_1)}{2} \end{aligned}$$

where $g(\tau, k)$ is defined in the lemma. Similarly, we can show that

$$\begin{aligned} g^{(2)}(\tau) &= \frac{g(\tau, 2c_{b\Delta}r_1)}{2} \\ g^{(3)}(\tau) &= \frac{g(\tau, c_{b\Delta}r_2)}{2} \\ g^{(4)}(\tau) &= \frac{g(\tau, 2c_{b\Delta}r_2)}{2}. \end{aligned}$$

It is not hard to verify that

$$\begin{aligned} & t_{b\Delta}^{(1)} \frac{\tau g'(\tau, c_{b\Delta}r_1)}{g(\tau, c_{b\Delta}r_1)} + t_{b\Delta}^{(2)} \frac{\tau g'(\tau, 2c_{b\Delta}r_1)}{g(\tau, 2c_{b\Delta}r_1)} + t_{b\Delta}^{(3)} \frac{\tau g'(\tau, c_{b\Delta}r_2)}{g(\tau, c_{b\Delta}r_2)} + t_{b\Delta}^{(4)} \frac{\tau g'(\tau, 2c_{b\Delta}r_2)}{g(\tau, 2c_{b\Delta}r_2)} \\ &= n\bar{l} - t_{b\Delta}^{(1)} c_{b\Delta}r_1 \frac{g(\tau, c_{b\Delta}r_1 - 1)}{g(\tau, c_{b\Delta}r_1)} - 2t_{b\Delta}^{(2)} c_{b\Delta}r_1 \frac{g(\tau, 2c_{b\Delta}r_1 - 1)}{g(\tau, 2c_{b\Delta}r_1)} \\ & - t_{b\Delta}^{(3)} c_{b\Delta}r_2 \frac{g(\tau, c_{b\Delta}r_2 - 1)}{g(\tau, c_{b\Delta}r_2)} - 2t_{b\Delta}^{(4)} c_{b\Delta}r_2 \frac{g(\tau, 2c_{b\Delta}r_2 - 1)}{g(\tau, 2c_{b\Delta}r_2)} \end{aligned}$$

which, together with (B.26) and (B.27), implies

$$\begin{aligned} \max G\left(\left\{m^{(i)}\right\}_{i=1}^{4}\right) &= -n\bar{l}^{\varkappa} \ln \tau \\ &\quad + t_{b\Delta}^{(1)} \ln \frac{g(\tau, r_1 c_{b\Delta})}{2} \\ &\quad + t_{b\Delta}^{(2)} \ln \frac{g(\tau, 2r_1 c_{b\Delta})}{2} \\ &\quad + t_{b\Delta}^{(3)} \ln \frac{g(\tau, r_2 c_{b\Delta})}{2} \\ &\quad + t_{b\Delta}^{(4)} \ln \frac{g(\tau, 2r_2 c_{b\Delta})}{2} \end{aligned} \tag{B.28}$$

where τ is the solution to

$$\begin{aligned}
&r_1 c_{b\Delta} \frac{t_{b\Delta}^{(1)}}{n} \frac{g(\tau, r_1 c_{b\Delta} - 1)}{g(\tau, r_1 c_{b\Delta})} \\
&+2r_1 c_{b\Delta} \frac{t_{b\Delta}^{(2)}}{n} \frac{g(\tau, 2r_1 c_{b\Delta} - 1)}{g(\tau, 2r_1 c_{b\Delta})} \\
&+r_2 c_{b\Delta} \frac{t_{b\Delta}^{(3)}}{n} \frac{g(\tau, r_2 c_{b\Delta} - 1)}{g(\tau, r_2 c_{b\Delta})} \\
&+2r_2 c_{b\Delta} \frac{t_{b\Delta}^{(4)}}{n} \frac{g(\tau, 2r_2 c_{b\Delta} - 1)}{g(\tau, 2r_1 c_{b\Delta})} \\
&= \bar{l} - \bar{l}^{\varkappa} \, . \qquad \text{(B.29)}
\end{aligned}$$

Putting (B.20), (B.21), (B.28), and (B.29) together, we then have

$$\begin{aligned}
&\Pr\left\{\mathbf{H}_{b\Delta\times n}^{(b\Delta)} x^n = 0^{b\Delta}\right\} \\
&\leq \exp\left\{\frac{3n\lceil\bar{l}\rceil}{b\Delta}\ln(n\hat{l}^{\varkappa}) + O(1)\right\}\binom{n\bar{l}}{n\bar{l}^{\varkappa}}^{-1} \max_{\{m^{(i)}\}_{i=1}^4 \in \mathcal{M}_{b\Delta,\varkappa}} M_{\{m^{(i)}\}_{i=1}^4} \\
&\leq \exp\left\{\max G\left(\{m^{(i)}\}_{i=1}^4\right) + \frac{3n\lceil\bar{l}\rceil}{b\Delta}\ln(n\hat{l}^{\varkappa}) + O(1)\right\}\binom{n\bar{l}}{n\bar{l}^{\varkappa}}^{-1} \\
&\leq \exp\left\{-n\bar{l}H\left(\frac{\bar{l}^{\varkappa}}{\bar{l}}\right) + \frac{\ln n\bar{l}^{\varkappa}\left(1-\frac{\bar{l}^{\varkappa}}{\bar{l}}\right)}{2} + \max G\left(\{m^{(i)}\}_{i=1}^4\right) + \frac{3n\lceil\bar{l}\rceil}{b\Delta}\ln(n\hat{l}^{\varkappa}) + O(1)\right\} \\
&= \exp\left\{nP\left(\frac{b\Delta}{n}, \bar{l}, \bar{l}^{\varkappa}\right) + \frac{3n\lceil\bar{l}\rceil}{b\Delta}\ln(n\hat{l}^{\varkappa}) + \frac{1}{2}\ln n\bar{l}^{\varkappa}\left(1-\frac{\bar{l}^{\varkappa}}{\bar{l}}\right) + O(1)\right\}
\end{aligned}$$

where the last inequality above is due to the fact that

$$\ln\binom{n\bar{l}}{n\bar{l}^{\varkappa}}^{-1} \leq -n\bar{l}H(\bar{l}^{\varkappa}/\bar{l}) + \frac{1}{2}\ln n\bar{l}^{\varkappa}\left(1-\frac{\bar{l}^{\varkappa}}{\bar{l}}\right) + O(1)$$

which can be derived from Sterling formula. This competes the proof of Lemma 6.1 when $\bar{l}^{\varkappa} < \bar{l} - \frac{t_{b\Delta}^{(1)}}{n}\pi(c_{b\Delta}r_1) - \frac{t_{b\Delta}^{(3)}}{n}\pi(c_{b\Delta}r_2)$.

Finally, let us look at the case when $\bar{l}^{\varkappa} = \bar{l} - \frac{t_{b\Delta}^{(1)}}{n}\pi(c_{b\Delta}r_1) - \frac{t_{b\Delta}^{(3)}}{n}\pi(c_{b\Delta}r_2)$. In this case, it follows from (B.19) that $\mathcal{M}_{t,\theta}$ contains only one type, i.e., the type given by

$$m_j^{(i)} = \begin{cases} t_{b\Delta}^{(i)} & \text{if } j = 2k^{(i)} \\ 0 & \text{otherwise} \end{cases} \qquad \text{(B.30)}$$

for $i = 1, 2, 3$, and 4. Combining this with (B.21), one can verify that in this case

$$\max \ln M_{\left\{m^{(i)}\right\}_{i=1}^{4}} = t_{b\Delta}^{(1)} \pi(c_{b\Delta} r_1) \ln[c_{b\Delta} r_1] + t_{b\Delta}^{(3)} \pi(c_{b\Delta} r_3) \ln[c_{b\Delta} r_3] \,. \tag{B.31}$$

Plugging (B.31) into (B.20) then leads to the desired result. This completes the proof of Lemma 6.1.

B.1.2 Properties of $P\left(R, \bar{l}, \xi\right)$

This Appendix is devoted to several lemmas related to the function $P\left(R, \bar{l}, \xi\right)$, which are needed in our performance analysis. To keep our notation consistent as in Lemma 6.1, only $R = \frac{b\Delta}{n}$ appears explicitly in the statements of these lemmas. However, in view of Remark 6.3, (6.8), and (6.9), by replacing $\frac{b\Delta}{n}$ by any real number $R \in (0, 1]$, all lemmas in this appendix (Lemmas B.1 to B.5) remain valid. Their respective proofs are the same whether or not $R \in (0, 1]$ is in the form of $R = \frac{b\Delta}{n}$.

In view of (6.5), we define

$$\begin{aligned} \tilde{l}\left(\frac{b\Delta}{n}, \bar{l}, \tau\right) \quad \triangleq \quad & \bar{l} - \frac{t_{b\Delta}^{(1)} c_{b\Delta} r_1}{n} \frac{g(\tau, c_{b\Delta} r_1 - 1)}{g(\tau, c_{b\Delta} r_1)} - \frac{2 t_{b\Delta}^{(2)} c_{b\Delta} r_1}{n} \frac{g(\tau, 2 c_{b\Delta} r_1 - 1)}{g(\tau, 2 c_{b\Delta} r_1)} \\ & - \frac{t_{b\Delta}^{(3)} c_{b\Delta} r_2}{n} \frac{g(\tau, c_{b\Delta} r_2 - 1)}{g(\tau, c_{b\Delta} r_2)} - \frac{2 t_{b\Delta}^{(4)} c_{b\Delta} r_2}{n} \frac{g(\tau, 2 c_{b\Delta} r_2 - 1)}{g(\tau, 2 c_{b\Delta} r_2)} \end{aligned}$$

Lemma B.1. *Given $\frac{b\Delta}{n}$ and $\bar{l}$, the following properties hold:*

P1 *As a function of τ, $\tilde{l}\left(\frac{b\Delta}{n}, \bar{l}, \tau\right)$ is strictly increasing over the interval $[0, +\infty)$.*

P2 *For any $\bar{l}^{\varkappa} \in [0, \bar{l} - \frac{t_{b\Delta}^{(1)}}{n} \pi\left(c_{b\Delta} r_1\right) - \frac{t_{b\Delta}^{(3)}}{n} \pi\left(c_{b\Delta} r_2\right))$, there is a unique solution of τ to $\tilde{l}\left(\frac{b\Delta}{n}, \bar{l}, \tau\right) = \bar{l}^{\varkappa}$.*

*Proof of **Lemma B.1***: In view of the definition of $\tilde{l}\left(\frac{b\Delta}{n}, \bar{l}, \tau\right)$, for Property P1, it is sufficient to prove that $\frac{g(\tau, k-1)}{g(\tau, k)}$ as function of τ is strictly decreasing over $\tau \in [0, \infty)$ for any positive value $k > 1$. To this end, take the first derivative of $\frac{g(\tau, k-1)}{g(\tau, k)}$ with respect to τ, yielding

$$\frac{-(1+\tau)^{2k-2} + (k-1)(1+\tau)^{k-2}(1-\tau)^{k} - (k-1)(1-\tau)^{k-2}(1+\tau)^{k} + (1-\tau)^{2k-2}}{g^2(\tau, k)} \tag{B.32}$$

Denote the enumerator of (B.32) by $f(\tau)$. It is easy to see that $f(0) = 0$. Since the denominator of (B.32) is always positive, it suffices to show that $f(\tau) < 0$ for any $\tau > 0$.

To continue, one can verify that

$$\begin{aligned}
f(\tau) &= -(1+\tau)^{2k-2} + (1-\tau)^{2k-2} + (k-1)(1-\tau^2)^{k-2}[(1-\tau)^2 - (1+\tau)^2] \\
&= -(1+\tau)^{2k-2} + (1-\tau)^{2k-2} - 4\tau(k-1)(1-\tau^2)^{k-2} \\
&= -2\sum_{i=0}^{k-2} \binom{2k-2}{2i+1} \tau^{2i+1} - 4\tau(k-1)(1-\tau^2)^{k-2} \\
&= -2\tau \left[\sum_{i=0}^{k-2} \binom{2k-2}{2i+1} \tau^{2i} + 2(k-1) \sum_{i=0}^{k-2} \binom{k-2}{i} (-1)^i \tau^{2i} \right] \\
&= -2\tau \left[\sum_{0 \le i \le k-2:\ \text{even}} \left(\binom{2k-2}{2i+1} + 2(k-1)\binom{k-2}{i} \right) \tau^{2i} \right. \\
&\quad \left. + \sum_{0 \le i \le k-2:\ \text{odd}} \left(\binom{2k-2}{2i+1} - 2(k-1)\binom{k-2}{i} \right) \tau^{2i} \right] \\
&\le -2\tau \sum_{0 \le i \le k-2:\ \text{even}} \left(\binom{2k-2}{2i+1} + 2(k-1)\binom{k-2}{i} \right) \tau^{2i} \\
&< 0
\end{aligned} \tag{B.33}$$

for any $\tau > 0$. In (B.33), the first inequality is due to the fact that for any odd $i < k-2$

$$\begin{aligned}
\binom{2k-2}{2i+1} &= \binom{2k-3}{2i+1} + \binom{2k-3}{2i} \\
&\ge \binom{k-2}{i}\binom{k-1}{i+1} + \binom{k-2}{i}\binom{k-1}{i} \\
&\ge 2(k-1)\binom{k-2}{i}
\end{aligned}$$

and for $i = k-2$ when k is odd,

$$\binom{2k-2}{2i+1} - 2(k-1)\binom{k-2}{i} = 0.$$

From (B.33), Property P1 follows.

Since $c_{b\Delta}r_2 \geq c_{b\Delta}r_1 > 1$, it is easy to see that

$$\begin{aligned}\tilde{l}\left(\frac{b\Delta}{n}, \bar{l}, 0\right) &= \bar{l} - \frac{t_{b\Delta}^{(1)} c_{b\Delta} r_1}{n} - \frac{2t_{b\Delta}^{(2)} c_{b\Delta} r_1}{n} - \frac{t_{b\Delta}^{(3)} c_{b\Delta} r_2}{n} - \frac{2t_{b\Delta}^{(4)} c_{b\Delta} r_2}{n} \\ &= \bar{l} - R_1 r_1 - r_2 R_2 \\ &= 0. \end{aligned} \tag{B.34}$$

On the other hand, one can verify that for any $k \geq 1$,

$$\lim_{\tau \to +\infty} \frac{g(\tau, k-1)}{g(\tau, k)} = \frac{\pi(k)}{k}$$

which implies that

$$\lim_{\tau \to +\infty} \tilde{l}\left(\frac{b\Delta}{n}, \bar{l}, \tau\right) = \bar{l} - \frac{t_{b\Delta}^{(1)}}{n}\pi\left(c_{b\Delta}r_1\right) - \frac{t_{b\Delta}^{(3)}}{n}\pi\left(c_{b\Delta}r_2\right). \tag{B.35}$$

Property P2 now follows from (B.34), (B.35), and Property P1. This completes the proof of Lemma B.1.

Lemma B.2. *For fixed $\frac{b\Delta}{n}$ and $\bar{l}$, $P\left(\frac{b\Delta}{n}, \bar{l}, \xi\right)$ as a function of ξ is strictly decreasing over $\xi \in (0, \bar{l}/2)$.*

*Proof of **Lemma B.2***: To show that $P\left(\frac{b\Delta}{n}, \bar{l}, \xi\right)$ is strictly decreasing over $\xi \in (0, \bar{l}/2)$, take its first derivative, yielding

$$\begin{aligned}\frac{\partial P}{\partial \xi} &= -\ln\frac{1-\xi/\bar{l}}{\xi/\bar{l}} - \ln\tau - \frac{\xi}{\tau}\frac{\partial \tau}{\partial \xi} \\ &\quad + r_1 c_{b\Delta}\frac{t_{b\Delta}^{(1)}}{n}\frac{(1+\tau)^{r_1 c_{b\Delta}-1} - (1-\tau)^{r_1 c_{b\Delta}-1}}{g(\tau, r_1 c_{b\Delta})}\frac{\partial \tau}{\partial \xi} \\ &\quad + 2r_1 c_{b\Delta}\frac{t_{b\Delta}^{(2)}}{n}\frac{(1+\tau)^{2r_1 c_{b\Delta}-1} - (1-\tau)^{2r_1 c_{b\Delta}-1}}{g(\tau, 2r_1 c_{b\Delta})}\frac{\partial \tau}{\partial \xi} \\ &\quad + r_2 c_{b\Delta}\frac{t_{b\Delta}^{(3)}}{n}\frac{(1+\tau)^{r_2 c_{b\Delta}-1} - (1-\tau)^{r_2 c_{b\Delta}-1}}{g(\tau, r_2 c_{b\Delta})}\frac{\partial \tau}{\partial \xi} \\ &\quad + 2r_2 c_{b\Delta}\frac{t_{b\Delta}^{(4)}}{n}\frac{(1+\tau)^{2r_2 c_{b\Delta}-1} - (1-\tau)^{2r_2 c_{b\Delta}-1}}{g(\tau, 2r_2 c_{b\Delta})}\frac{\partial \tau}{\partial \xi}. \end{aligned} \tag{B.36}$$

Note that

$$\begin{aligned} g(\tau,k) &= (1+\tau)^k + (1-\tau)^k \\ &= (1+\tau)^{k-1}(1+\tau) + (1-\tau)^{k-1}(1-\tau) \\ &= \tau\left[(1+\tau)^{k-1} - (1-\tau)^{k-1}\right] + g(\tau,k-1) \end{aligned}$$

and hence

$$(1+\tau)^{k-1} - (1-\tau)^{k-1} = \frac{g(\tau,k) - g(\tau,k-1)}{\tau}$$

Plugging the above equality into (B.36) yields

$$\begin{aligned} \frac{\partial P}{\partial \xi} &= -\ln\frac{1-\xi/\bar{l}}{\xi/\bar{l}} - \ln\tau - \frac{\xi}{\tau}\frac{\partial\tau}{\partial\xi} \\ &\quad + \frac{r_1 c_{b\Delta}}{\tau}\frac{t_{b\Delta}^{(1)}}{n}\left[1 - \frac{g(\tau, r_1 c_{b\Delta} - 1)}{g(\tau, r_1 c_{b\Delta})}\right]\frac{\partial\tau}{\partial\xi} \\ &\quad + \frac{2r_1 c_{b\Delta}}{\tau}\frac{t_{b\Delta}^{(2)}}{n}\left[1 - \frac{g(\tau, 2r_1 c_{b\Delta} - 1)}{g(\tau, 2r_1 c_{b\Delta})}\right]\frac{\partial\tau}{\partial\xi} \\ &\quad + \frac{r_2 c_{b\Delta}}{\tau}\frac{t_{b\Delta}^{(3)}}{n}\left[1 - \frac{g(\tau, r_2 c_{b\Delta} - 1)}{g(\tau, r_2 c_{b\Delta})}\right]\frac{\partial\tau}{\partial\xi} \\ &\quad + \frac{2r_2 c_{b\Delta}}{\tau}\frac{t_{b\Delta}^{(4)}}{n}\left[1 - \frac{g(\tau, 2r_2 c_{b\Delta} - 1)}{g(\tau, 2r_2 c_{b\Delta})}\right]\frac{\partial\tau}{\partial\xi} \\ &= -\ln\frac{1-\xi/\bar{l}}{\xi/\bar{l}} - \ln\tau \end{aligned} \tag{B.37}$$

where the second step comes from the fact that τ is the solution to (6.5) and from the identity (6.9). Note that $\tau = 1$ is the solution to (6.5) when $\xi = \frac{\bar{l}}{2}$, and therefore by Lemma B.1, $0 < \tau < 1$ whenever $\xi \in (0, \bar{l}/2)$. Furthermore, it can be verified that for any $\tau \in (0,1)$

$$\frac{g(\tau,k-1)}{g(\tau,k)} = \frac{(1+\tau)^{k-1} + (1-\tau)^{k-1}}{(1+\tau)^k + (1-\tau)^k} > \frac{1}{1+\tau}$$

which, coupled with (6.5), implies

$$\frac{\bar{l}}{1+\tau} < \bar{l} - \xi$$

or

$$\tau > \frac{\xi/\bar{l}}{1-\xi/\bar{l}}$$

for $\xi \in (0, \bar{l}/2)$. Plugging the above inequality into (B.37), we have

$$\frac{\partial P}{\partial \xi} < 0$$

for $\xi \in (0, \bar{l}/2)$. This completes the proof of Lemma B.2.

Lemma B.3. *For fixed* $\frac{b\Delta}{n}$ *and* $\bar{l}$, $P\left(\frac{b\Delta}{n}, \bar{l}, \xi\right) \geq P\left(\frac{b\Delta}{n}, \bar{l}, \bar{l} - \xi\right)$ *for* $0 < \xi \leq \bar{l}/2$.

Proof of ***Lemma B.3***: First, we consider the case where

$$\frac{t^{(1)}}{n}\pi(c_{b\Delta} r_1) + \frac{t^{(3)}}{n}\pi(c_{b\Delta} r_2) < \xi \leq \frac{\bar{l}}{2}$$

Define

$$\begin{aligned} P\left(\frac{b\Delta}{n}, \bar{l}, \xi, \tau\right) &= -\bar{l}H(\xi/\bar{l}) - \xi \ln \tau \\ &\quad + \frac{t^{(1)}_{b\Delta}}{n} \ln \frac{g(\tau, r_1 c_{b\Delta})}{2} + \frac{t^{(2)}_{b\Delta}}{n} \ln \frac{g(\tau, 2r_1 c_{b\Delta})}{2} \\ &\quad + \frac{t^{(3)}_{b\Delta}}{n} \ln \frac{g(\tau, r_2 c_{b\Delta})}{2} + \frac{t^{(4)}_{b\Delta}}{n} \ln \frac{g(\tau, 2r_2 c_{b\Delta})}{2} \end{aligned}$$

and τ_ξ as the solution to

$$\xi = \tilde{l}\left(\frac{b\Delta}{n}, \bar{l}, \tau\right)$$

Then it is easy to observe that

$$P\left(\frac{b\Delta}{n}, \bar{l}, \xi\right) = P\left(\frac{b\Delta}{n}, \bar{l}, \xi, \tau_\xi\right)$$

Note that when $\xi \leq \bar{l}/2$, $\tau_\xi \leq 1$. For $\tau \leq 1$,

$$g(\tau^{-1}, k) = \frac{(1+\tau)^k + (\tau - 1)^k}{\tau^k} \leq \frac{g(\tau, k)}{\tau^k}$$

and

$$\begin{aligned}
P\left(\frac{b\Delta}{n}, \bar{l}, \bar{l}-\xi, \tau^{-1}\right) &= -\bar{l}H((\bar{l}-\xi)/\bar{l}) - (\bar{l}-\xi)\ln\tau^{-1} \\
&\quad + \frac{t_{b\Delta}^{(1)}}{n}\ln\frac{g(\tau^{-1}, r_1 c_{b\Delta})}{2} + \frac{t_{b\Delta}^{(2)}}{n}\ln\frac{g(\tau^{-1}, 2r_1 c_{b\Delta})}{2} \\
&\quad + \frac{t_{b\Delta}^{(3)}}{n}\ln\frac{g(\tau^{-1}, r_2 c_{b\Delta})}{2} + \frac{t_{b\Delta}^{(4)}}{n}\ln\frac{g(\tau^{-1}, 2r_2 c_{b\Delta})}{2} \\
&\leq -\bar{l}H(\xi/\bar{l}) + (\bar{l}-\xi)\ln\tau \\
&\quad + \frac{t_{b\Delta}^{(1)}}{n}\ln\frac{g(\tau, r_1 c_{b\Delta})}{2\tau^{r_1 c_{b\Delta}}} + \frac{t_{b\Delta}^{(2)}}{n}\ln\frac{g(\tau, 2r_1 c_{b\Delta})}{2\tau^{2r_1 c_{b\Delta}}} \\
&\quad + \frac{t_{b\Delta}^{(3)}}{n}\ln\frac{g(\tau, r_2 c_{b\Delta})}{2\tau^{r_2 c_{b\Delta}}} + \frac{t_{b\Delta}^{(4)}}{n}\ln\frac{g(\tau, 2r_2 c_{b\Delta})}{2\tau^{2r_2 c_{b\Delta}}} \\
&= -\bar{l}H(\xi/\bar{l}) - \xi\ln\tau \\
&\quad + \frac{t_{b\Delta}^{(1)}}{n}\ln\frac{g(\tau, r_1 c_{b\Delta})}{2} + \frac{t_{b\Delta}^{(2)}}{n}\ln\frac{g(\tau, 2r_1 c_{b\Delta})}{2} \\
&\quad + \frac{t_{b\Delta}^{(3)}}{n}\ln\frac{g(\tau, r_2 c_{b\Delta})}{2} + \frac{t_{b\Delta}^{(4)}}{n}\ln\frac{g(\tau, 2r_2 c_{b\Delta})}{2} \\
&= P\left(\frac{b\Delta}{n}, \bar{l}, \xi, \tau\right)
\end{aligned}$$

where the third step is due to (6.9). Therefore,

$$P\left(\frac{b\Delta}{n}, \bar{l}, \xi, \tau_\xi\right) \geq P\left(\frac{b\Delta}{n}, \bar{l}, \bar{l}-\xi, \tau_\xi^{-1}\right)$$

Now it can be verified that

$$\frac{\partial P\left(\frac{b\Delta}{n}, \bar{l}, \xi, \tau\right)}{\partial\tau} = \frac{-\xi + \tilde{l}\left(\frac{b\Delta}{n}, \bar{l}, \tau\right)}{\tau}$$

and since $\tilde{l}\left(\frac{b\Delta}{n}, \bar{l}, \tau\right)$ is an increasing function of τ, it is easy to see that $\frac{\partial P\left(\frac{b\Delta}{n}, \bar{l}, \xi, \tau\right)}{\partial\tau} < 0$ for $\tau < \tau_\xi$ and $\frac{\partial P\left(\frac{b\Delta}{n}, \bar{l}, \xi, \tau\right)}{\partial\tau} > 0$ for $\tau > \tau_\xi$. Therefore, τ_ξ is the value that minimizes the function $P\left(\frac{b\Delta}{n}, \bar{l}, \xi, \tau\right)$ given ξ. In the other words,

$$P\left(\frac{b\Delta}{n}, \bar{l}, \xi, \tau_\xi\right) \leq P\left(\frac{b\Delta}{n}, \bar{l}, \xi, \tau\right)$$

for any $\tau > 0$. In total, we have

$$\begin{aligned} P\left(\frac{b\Delta}{n}, \bar{l}, \xi\right) &= P\left(\frac{b\Delta}{n}, \bar{l}, \xi, \tau_\xi\right) \\ &\geq P\left(\frac{b\Delta}{n}, \bar{l}, \bar{l} - \xi, \tau_\xi^{-1}\right) \\ &\geq P\left(\frac{b\Delta}{n}, \bar{l}, \bar{l} - \xi, \tau_{\bar{l}-\xi}\right) \\ &= P\left(\frac{b\Delta}{n}, \bar{l}, \bar{l} - \xi\right) \end{aligned}$$

Now if

$$\xi < \frac{t^{(1)}}{n}\pi(c_{b\Delta} r_1) + \frac{t^{(3)}}{n}\pi(c_{b\Delta} r_2),$$

then $P\left(\frac{b\Delta}{n}, \bar{l}, \bar{l} - \xi\right) = -\infty$, and $P\left(\frac{b\Delta}{n}, \bar{l}, \xi\right) \geq P\left(\frac{b\Delta}{n}, \bar{l}, \bar{l} - \xi\right)$ is obvious. For

$$\xi = \frac{t^{(1)}}{n}\pi(c_{b\Delta} r_1) + \frac{t^{(3)}}{n}\pi(c_{b\Delta} r_2),$$

it can be shown that

$$\frac{\partial P\left(\frac{b\Delta}{n}, \bar{l}, \bar{l} - \xi, \tau\right)}{\partial \tau} < 0$$

for $\tau > 0$. Then

$$\begin{aligned} P\left(\frac{b\Delta}{n}, \bar{l}, \xi\right) &= P\left(\frac{b\Delta}{n}, \bar{l}, \xi, \tau_\xi\right) \\ &\geq P\left(\frac{b\Delta}{n}, \bar{l}, \bar{l} - \xi, \tau_\xi^{-1}\right) \\ &\geq \lim_{\tau \to \infty} P\left(\frac{b\Delta}{n}, \bar{l}, \bar{l} - \xi, \tau\right) \\ &= P\left(\frac{b\Delta}{n}, \bar{l}, \bar{l} - \xi\right) \end{aligned}$$

where the last equality is due to (6.7). This completes the proof of Lemma B.3.

Lemma B.4. *For* $\frac{\bar{l}}{\lfloor \bar{l} \rfloor} \leq \xi \leq \frac{\bar{l}}{2}$,

$$P\left(\frac{b\Delta}{n}, \bar{l}, \xi\right) \leq -\frac{b\Delta}{n}\ln 2 + 2\xi \exp\left[-\frac{2\xi}{\bar{l}}\left(c_{b\Delta} r_1 - 1\right)\right] + \frac{b\Delta}{n}\exp\left(-\frac{2\xi}{\bar{l}} r_1 c_{b\Delta}\right)$$

Proof of ***Lemma B.4***: Let τ_ξ be the solution to the equation

$$\tilde{l}\left(\frac{b\Delta}{n}, \bar{l}, \tau\right) = \xi.$$

From the proof of Lemma B.3, we know that

$$\frac{\xi/\bar{l}}{1-\xi/\bar{l}} \leq \tau_\xi \leq 1 \text{ or } \frac{\xi}{\bar{l}} \leq \frac{\tau_\xi}{1+\tau_\xi} \leq \frac{1}{2}$$

whenever $\xi \leq \frac{\bar{l}}{2}$. Furthermore, it can be verified that

$$f(x) = \frac{1+(1-x)^{k-1}}{1+(1-x)^k}$$

is strictly decreasing for $\frac{2}{k} \leq x \leq 1$, where k is an integer no less than 2. To see this is the case, we have

$$\begin{aligned} f'(x) &= \frac{-\left[1+(1-x)^k\right](k-1)(1-x)^{k-2} + \left[1+(1-x)^{k-1}\right]k(1-x)^{k-1}}{\left[1+(1-x)^k\right]^2} \\ &= \frac{(1-x)^{k-2}}{\left[1+(1-x)^k\right]^2}\left[1-kx+(1-x)^k\right] < 0 \end{aligned}$$

for $\frac{2}{k} \leq x \leq 1$. Now assume that

$$\frac{r_1}{\bar{l}}\xi = \frac{\lfloor \bar{l} \rfloor}{\bar{l}}\xi \geq 1.$$

Then

$$\frac{\tau_\xi}{1+\tau_\xi} r_1 c_{b\Delta} \geq \frac{\xi}{\bar{l}} r_1 c_{b\Delta} \geq 1.$$

Therefore,

$$\begin{aligned}
\frac{g\left(\tau_\xi, c_{b\Delta} r_1 - 1\right)}{g\left(\tau_\xi, c_{b\Delta} r_1\right)} &= \frac{1}{1+\tau_\xi} \frac{1 + \left(1 - \frac{2\tau_\xi}{1+\tau_\xi}\right)^{c_{b\Delta} r_1 - 1}}{1 + \left(1 - \frac{2\tau_\xi}{1+\tau_\xi}\right)^{c_{b\Delta} r_1}} \\
&\leq \frac{1}{1+\tau_\xi} \frac{1 + \left(1 - \frac{2\xi}{\bar{l}}\right)^{c_{b\Delta} r_1 - 1}}{1 + \left(1 - \frac{2\xi}{\bar{l}}\right)^{c_{b\Delta} r_1}} \\
&= \frac{1}{1+\tau_\xi} \left[1 + \frac{\left(1 - \frac{2\xi}{\bar{l}}\right)^{c_{b\Delta} r_1 - 1} - \left(1 - \frac{2\xi}{\bar{l}}\right)^{c_{b\Delta} r_1}}{1 + \left(1 - \frac{2\xi}{\bar{l}}\right)^{c_{b\Delta} r_1}}\right] \\
&= \frac{1}{1+\tau_\xi} \left[1 + \frac{\frac{2\xi}{\bar{l}} \left(1 - \frac{2\xi}{\bar{l}}\right)^{c_{b\Delta} r_1 - 1}}{1 + \left(1 - \frac{2\xi}{\bar{l}}\right)^{c_{b\Delta} r_1}}\right] \\
&\leq \frac{1}{1+\tau_\xi} \left[1 + \frac{2\xi}{\bar{l}} \left(1 - \frac{2\xi}{\bar{l}}\right)^{c_{b\Delta} r_1 - 1}\right].
\end{aligned}$$

Similarly,

$$\begin{aligned}
\frac{g\left(\tau_\xi, 2c_{b\Delta} r_1 - 1\right)}{g\left(\tau_\xi, 2c_{b\Delta} r_1\right)} &\leq \frac{1}{1+\tau_\xi} \left[1 + \frac{2\xi}{\bar{l}} \left(1 - \frac{2\xi}{\bar{l}}\right)^{2c_{b\Delta} r_1 - 1}\right] \\
&\leq \frac{1}{1+\tau_\xi} \left[1 + \frac{2\xi}{\bar{l}} \left(1 - \frac{2\xi}{\bar{l}}\right)^{c_{b\Delta} r_1 - 1}\right] \\
\frac{g\left(\tau_\xi, c_{b\Delta} r_2 - 1\right)}{g\left(\tau_\xi, c_{b\Delta} r_2\right)} &\leq \frac{1}{1+\tau_\xi} \left[1 + \frac{2\xi}{\bar{l}} \left(1 - \frac{2\xi}{\bar{l}}\right)^{c_{b\Delta} r_2 - 1}\right] \\
&\leq \frac{1}{1+\tau_\xi} \left[1 + \frac{2\xi}{\bar{l}} \left(1 - \frac{2\xi}{\bar{l}}\right)^{c_{b\Delta} r_1 - 1}\right] \\
\frac{g\left(\tau_\xi, 2c_{b\Delta} r_2 - 1\right)}{g\left(\tau_\xi, 2c_{b\Delta} r_2\right)} &\leq \frac{1}{1+\tau_\xi} \left[1 + \frac{2\xi}{\bar{l}} \left(1 - \frac{2\xi}{\bar{l}}\right)^{2c_{b\Delta} r_2 - 1}\right] \\
&\leq \frac{1}{1+\tau_\xi} \left[1 + \frac{2\xi}{\bar{l}} \left(1 - \frac{2\xi}{\bar{l}}\right)^{c_{b\Delta} r_1 - 1}\right].
\end{aligned}$$

Thus,

$$\begin{aligned}
\xi &= \tilde{l}\left(\frac{b\Delta}{n}, \bar{l}, \tau_\xi\right) \\
&= \bar{l} - \frac{t^{(1)}_{b\Delta} c_{b\Delta} r_1}{n} \frac{g(\tau, c_{b\Delta} r_1 - 1)}{g(\tau, c_{b\Delta} r_1)} - \frac{2t^{(2)}_{b\Delta} c_{b\Delta} r_1}{n} \frac{g(\tau, 2c_{b\Delta} r_1 - 1)}{g(\tau, 2c_{b\Delta} r_1)} \\
&\quad - \frac{t^{(3)}_{b\Delta} c_{b\Delta} r_2}{n} \frac{g(\tau, c_{b\Delta} r_2 - 1)}{g(\tau, c_{b\Delta} r_2)} - \frac{2t^{(4)}_{b\Delta} c_{b\Delta} r_2}{n} \frac{g(\tau, 2c_{b\Delta} r_2 - 1)}{g(\tau, 2c_{b\Delta} r_2)} \\
&\geq \bar{l} - \frac{\bar{l}}{1+\tau_\xi}\left[1 + \frac{2\xi}{\bar{l}}\left(1 - \frac{2\xi}{\bar{l}}\right)^{c_{b\Delta} r_1 - 1}\right]
\end{aligned}$$

where in the last step, the identity (6.9) was applied. This implies that

$$1 + \tau_\xi \leq \frac{\bar{l}}{\bar{l} - \xi}\left[1 + \frac{2\xi}{\bar{l}}\left(1 - \frac{2\xi}{\bar{l}}\right)^{c_{b\Delta} r_1 - 1}\right] .$$

On the other hand,

$$\begin{aligned}
g\left(\tau_\xi, r_1 c_{b\Delta}\right) &= (1+\tau_\xi)^{r_1 c_{b\Delta}} + (1-\tau_\xi)^{r_1 c_{b\Delta}} \\
&= (1+\tau_\xi)^{r_1 c_{b\Delta}}\left[1 + \left(1 - \frac{2\tau_\xi}{1+\tau_\xi}\right)^{r_1 c_{b\Delta}}\right] \\
&\leq (1+\tau_\xi)^{r_1 c_{b\Delta}}\left[1 + \left(1 - \frac{2\xi}{\bar{l}}\right)^{r_1 c_{b\Delta}}\right] .
\end{aligned}$$

Again,

$$\begin{aligned}
g\left(\tau_\xi, 2r_1 c_{b\Delta}\right) &\leq (1+\tau_\xi)^{2r_1 c_{b\Delta}}\left[1 + \left(1 - \frac{2\xi}{\bar{l}}\right)^{2r_1 c_{b\Delta}}\right] \\
&\leq (1+\tau_\xi)^{2r_1 c_{b\Delta}}\left[1 + \left(1 - \frac{2\xi}{\bar{l}}\right)^{r_1 c_{b\Delta}}\right] \\
g\left(\tau_\xi, r_2 c_{b\Delta}\right) &\leq (1+\tau_\xi)^{r_2 c_{b\Delta}}\left[1 + \left(1 - \frac{2\xi}{\bar{l}}\right)^{r_2 c_{b\Delta}}\right] \\
&\leq (1+\tau_\xi)^{r_2 c_{b\Delta}}\left[1 + \left(1 - \frac{2\xi}{\bar{l}}\right)^{r_1 c_{b\Delta}}\right] \\
g\left(\tau_\xi, 2r_2 c_{b\Delta}\right) &\leq (1+\tau_\xi)^{2r_2 c_{b\Delta}}\left[1 + \left(1 - \frac{2\xi}{\bar{l}}\right)^{2r_2 c_{b\Delta}}\right] \\
&\leq (1+\tau_\xi)^{2r_2 c_{b\Delta}}\left[1 + \left(1 - \frac{2\xi}{\bar{l}}\right)^{r_1 c_{b\Delta}}\right]
\end{aligned}$$

By combining the above inequalities with the identities (6.8) and (6.9), we have

$$\begin{aligned}
P\left(\frac{b\Delta}{n},\bar{l},\xi\right) &= -\bar{l}H\left(\xi/\bar{l}\right)-\xi\ln\tau_\xi \\
&\quad+\frac{t_{b\Delta}^{(1)}}{n}\ln\frac{g\left(\tau_\xi,r_1c_{b\Delta}\right)}{2}+\frac{t_{b\Delta}^{(2)}}{n}\ln\frac{g\left(\tau_\xi,2r_1c_{b\Delta}\right)}{2} \\
&\quad+\frac{t_{b\Delta}^{(3)}}{n}\ln\frac{g\left(\tau_\xi,r_2c_{b\Delta}\right)}{2}+\frac{t_{b\Delta}^{(4)}}{n}\ln\frac{g\left(\tau_\xi,2r_2c_{b\Delta}\right)}{2} \\
&\leq -\bar{l}H\left(\xi/\bar{l}\right)-\xi\ln\tau_\xi+\bar{l}\ln\left(1+\tau_\xi\right) \\
&\quad-\frac{b\Delta}{n}\ln 2+\frac{b\Delta}{n}\ln\left[1+\left(1-\frac{2\xi}{\bar{l}}\right)^{r_1c_{b\Delta}}\right] \\
&\leq -\bar{l}H\left(\xi/\bar{l}\right)-\xi\ln\frac{\xi}{\bar{l}-\xi}+\bar{l}\ln\left(1+\tau_\xi\right) \\
&\quad-\frac{b\Delta}{n}\ln 2+\frac{b\Delta}{n}\ln\left[1+\left(1-\frac{2\xi}{\bar{l}}\right)^{r_1c_{b\Delta}}\right] \\
&\leq -\bar{l}H\left(\xi/\bar{l}\right)-\xi\ln\frac{\xi}{\bar{l}-\xi}+\bar{l}\ln\frac{\bar{l}}{\bar{l}-\xi}+\bar{l}\ln\left[1+\frac{2\xi}{\bar{l}}\left(1-\frac{2\xi}{\bar{l}}\right)^{c_{b\Delta}r_1-1}\right] \\
&\quad-\frac{b\Delta}{n}\ln 2+\frac{b\Delta}{n}\ln\left[1+\left(1-\frac{2\xi}{\bar{l}}\right)^{r_1c_{b\Delta}}\right] \\
&\leq -\frac{b\Delta}{n}\ln 2+2\xi\left(1-\frac{2\xi}{\bar{l}}\right)^{c_{b\Delta}r_1-1}+\frac{b\Delta}{n}\left(1-\frac{2\xi}{\bar{l}}\right)^{r_1c_{b\Delta}} \\
&\leq -\frac{b\Delta}{n}\ln 2+2\xi\exp\left[-\frac{2\xi}{\bar{l}}\left(c_{b\Delta}r_1-1\right)\right]+\frac{b\Delta}{n}\exp\left(-\frac{2\xi}{\bar{l}}r_1c_{b\Delta}\right).
\end{aligned}$$

This completes the proof of Lemma B.4.

Lemma B.5. *Given $0<\xi\leq\frac{\bar{l}}{2}$, the following properties hold:*

1) for $1\leq b\leq\frac{n}{\Delta}-1$,

$$-\frac{\Delta}{n}\ln 2\leq P\left(\frac{(b+1)\Delta}{n},\bar{l},\xi\right)-P\left(\frac{b\Delta}{n},\bar{l},\xi\right)\leq-\frac{\Delta}{n}Q_{\xi,\frac{(b+1)\Delta}{n}}$$

where

$$Q_{\xi,\frac{(b+1)\Delta}{n}}=\ln 2-\ln\left(1+\frac{2\left(1-\frac{2\xi}{\bar{l}}\right)^{r_1c_{(b+1)\Delta}}}{1+\left(1-\frac{2\xi}{\bar{l}}\right)^{2r_1c_{(b+1)\Delta}}}\right)$$

2) for $0 < R_1 \le R_2 \le 1$,

$$-(R_2 - R_1)\ln 2 \le P\left(R_2, \bar{l}, \xi\right) - P\left(R_1, \bar{l}, \xi\right) \le -(R_2 - R_1)Q_{\xi,R_2}$$

where

$$Q_{\xi,R_2} = \ln 2 - \ln\left(1 + \frac{2\left(1 - \frac{2\xi}{\bar{l}}\right)^{r_1 c_{R_2}}}{1 + \left(1 - \frac{2\xi}{\bar{l}}\right)^{2r_1 c_{R_2}}}\right)$$

with $c_{R_2} = 2^{-\lceil \log_2 R_2 \rceil}$, *which shows that* $P(R, \bar{l}, \xi)$ *strictly decreasing with respect to* $R \in (0, 1]$, *and Lipschitz-Continuous with constant* $\ln 2$*; and*

3) $\lim_{R\to 0} P(R, \bar{l}, \xi) = 0$.

Proof of ***Lemma B.5***: Let $P\left(\frac{b\Delta}{n}, \bar{l}, \xi, \tau\right)$ be the function defined in the proof of Lemma B.3. Furthermore, let τ_b and τ_{b+1} be the solution to (6.5) for b and $b+1$, respectively. From the proof of Lemma B.3, it follows that given $(\frac{b\Delta}{n}, \bar{l}, \xi)$, the function $P\left(\frac{b\Delta}{n}, \bar{l}, \xi, \tau\right)$ achieves its minimum at $\tau = \tau_b$, and hence

$$\begin{aligned} P\left(\frac{(b+1)\Delta}{n}, \bar{l}, \xi\right) &= P\left(\frac{(b+1)\Delta}{n}, \bar{l}, \xi, \tau_{b+1}\right) \\ &\le P\left(\frac{(b+1)\Delta}{n}, \bar{l}, \xi, \tau_b\right) \end{aligned}$$

Therefore,

$$P\left(\frac{(b+1)\Delta}{n}, \bar{l}, \xi\right) - P\left(\frac{b\Delta}{n}, \bar{l}, \xi\right) \le P\left(\frac{(b+1)\Delta}{n}, \bar{l}, \xi, \tau_b\right) - P\left(\frac{b\Delta}{n}, \bar{l}, \xi, \tau_b\right).$$

Now we have

$$c_{b\Delta} = 2^{-\lceil \log_2 \frac{b\Delta}{n} \rceil} \ge 2^{-\lceil \log_2 \frac{(b+1)\Delta}{n} \rceil} = c_{(b+1)\Delta} = 2^{-\lceil \log_2 \frac{b\Delta}{n} + \log_2 \frac{b+1}{b} \rceil} \ge 2^{-\lceil \log_2 \frac{b\Delta}{n} + 1 \rceil} = \frac{c_{b\Delta}}{2}.$$

To continue, we distinguish between two cases: (1) $c_{b\Delta} = c_{(b+1)\Delta}$, and (2) $c_{b\Delta} = 2c_{(b+1)\Delta}$. In case (1), i.e., when $\lceil \log_2 \frac{b\Delta}{n} \rceil = \lceil \log_2 \frac{(b+1)\Delta}{n} \rceil$, we have

$$\begin{aligned} & P\left(\frac{(b+1)\Delta}{n}, \bar{l}, \xi, \tau_b\right) - P\left(\frac{b\Delta}{n}, \bar{l}, \xi, \tau_b\right) \\ &= \frac{t^{(1)}_{(b+1)\Delta} - t^{(1)}_{(b+1)\Delta}}{n} \ln \frac{g\left(\tau_b, r_1 c_{(b+1)\Delta}\right)}{2} + \frac{t^{(2)}_{(b+1)\Delta} - t^{(2)}_{b\Delta}}{n} \ln \frac{g\left(\tau_b, 2r_1 c_{(b+1)\Delta}\right)}{2} \\ &\quad + \frac{t^{(3)}_{(b+1)\Delta} - t^{(3)}_{b\Delta}}{n} \ln \frac{g\left(\tau_b, r_2 c_{(b+1)\Delta}\right)}{2} + \frac{t^{(4)}_{(b+1)\Delta} - t^{(4)}_{b\Delta}}{n} \ln \frac{g\left(\tau_b, 2r_2 c_{(b+1)\Delta}\right)}{2}. \end{aligned}$$

Meanwhile,

$$\begin{aligned}
\frac{t^{(1)}_{(b+1)\Delta}}{n} &= \min\left\{\frac{2(b+1)\Delta}{n} - 2^{\lceil \log_2 \frac{(b+1)\Delta}{n}\rceil}, R_1 2^{\lceil \log_2 \frac{(b+1)\Delta}{n}\rceil}\right\} \\
&= \min\left\{\frac{2(b+1)\Delta}{n} - 2^{\lceil \log_2 \frac{b\Delta}{n}\rceil}, R_1 2^{\lceil \log_2 \frac{b\Delta}{n}\rceil}\right\} \\
&\geq \min\left\{\frac{2b\Delta}{n} - 2^{\lceil \log_2 \frac{b\Delta}{n}\rceil}, R_1 2^{\lceil \log_2 \frac{b\Delta}{n}\rceil}\right\} \\
&= \frac{t^{(1)}_{b\Delta}}{n}.
\end{aligned}$$

Furthermore, it can be verified that

$$\frac{t^{(1)}_{(b+1)\Delta} + 2t^{(2)}_{(b+1)\Delta}}{n} = R_1 2^{\lceil \log_2 \frac{(b+1)\Delta}{n}\rceil} = R_1 2^{\lceil \log_2 \frac{b\Delta}{n}\rceil} = \frac{t^{(1)}_{b\Delta} + 2t^{(2)}_{b\Delta}}{n}.$$

Therefore,

$$\frac{2\left(t^{(2)}_{b\Delta} - t^{(2)}_{(b+1)\Delta}\right)}{n} = \frac{t^{(1)}_{(b+1)\Delta} - t^{(1)}_{b\Delta}}{n} \geq 0.$$

Similarly, we have

$$\frac{2\left(t^{(4)}_{b\Delta} - t^{(4)}_{(b+1)\Delta}\right)}{n} = \frac{\left(t^{(3)}_{(b+1)\Delta} - t^{(3)}_{b\Delta}\right)}{n} \geq 0.$$

Consequently,

$$\begin{aligned}
&P\left(\frac{(b+1)\Delta}{n}, \bar{l}, \xi, \tau_b\right) - P\left(\frac{b\Delta}{n}, \bar{l}, \xi, \tau_b\right) \\
&= \frac{\left(t^{(2)}_{b\Delta} - t^{(2)}_{(b+1)\Delta}\right)}{n}\left(-\ln 2 + \ln \frac{g^2\left(\tau_b, r_1 c_{(b+1)\Delta}\right)}{g\left(\tau_b, 2r_1 c_{(b+1)\Delta}\right)}\right) \\
&\quad + \frac{\left(t^{(4)}_{b\Delta} - t^{(4)}_{(b+1)\Delta}\right)}{n}\left(-\ln 2 + \ln \frac{g^2\left(\tau_b, r_2 c_{(b+1)\Delta}\right)}{g\left(\tau_b, 2r_2 c_{(b+1)\Delta}\right)}\right).
\end{aligned}$$

At the same time,

$$\begin{aligned}\frac{g^2\left(\tau_b, r_1 c_{(b+1)\Delta}\right)}{g\left(\tau_b, 2r_1 c_{(b+1)\Delta}\right)} &= \frac{\left[(1+\tau_b)^{r_1 c_{(b+1)\Delta}} + (1-\tau_b)^{r_1 c_{(b+1)\Delta}}\right]^2}{(1+\tau_b)^{2r_1 c_{(b+1)\Delta}} + (1-\tau_b)^{2r_1 c_{(b+1)\Delta}}} \\ &= 1 + \frac{2(1+\tau_b)^{r_1 c_{(b+1)\Delta}}(1-\tau_b)^{r_1 c_{(b+1)\Delta}}}{(1+\tau_b)^{2r_1 c_{(b+1)\Delta}} + (1-\tau_b)^{2r_1 c_{(b+1)\Delta}}} \\ &= 1 + \frac{2\left(1-\frac{2\tau_b}{1+\tau_b}\right)^{r_1 c_{(b+1)\Delta}}}{1+\left(1-\frac{2\tau_b}{1+\tau_b}\right)^{2r_1 c_{(b+1)\Delta}}}.\end{aligned}$$

From the proof of Lemma B.4,

$$0 \le 1 - \frac{2\tau_b}{1+\tau_b} \le 1 - \frac{2\xi}{\bar{l}} < 1.$$

On the other hand, it is easily verified that

$$f(x) = \frac{2x}{1+x^2}$$

is an increasing function for $x \in [0,1)$. Therefore,

$$\frac{g^2\left(\tau_b, r_1 c_{(b+1)\Delta}\right)}{g\left(\tau_b, 2r_1 c_{(b+1)\Delta}\right)} \le 1 + \frac{2\left(1-\frac{2\xi}{\bar{l}}\right)^{r_1 c_{(b+1)\Delta}}}{1+\left(1-\frac{2\xi}{\bar{l}}\right)^{2r_1 c_{(b+1)\Delta}}}.$$

Similarly,

$$\begin{aligned}\frac{g^2\left(\tau_b, r_2 c_{(b+1)\Delta}\right)}{g\left(\tau_b, 2r_2 c_{(b+1)\Delta}\right)} &\le 1 + \frac{2\left(1-\frac{2\xi}{\bar{l}}\right)^{r_2 c_{(b+1)\Delta}}}{1+\left(1-\frac{2\xi}{\bar{l}}\right)^{2r_2 c_{(b+1)\Delta}}} \\ &\le 1 + \frac{2\left(1-\frac{2\xi}{\bar{l}}\right)^{r_1 c_{(b+1)\Delta}}}{1+\left(1-\frac{2\xi}{\bar{l}}\right)^{2r_1 c_{(b+1)\Delta}}}.\end{aligned}$$

And finally,

$$
\begin{aligned}
& P\left(\frac{(b+1)\Delta}{n}, \bar{l}, \xi, \tau_b\right) - P\left(\frac{b\Delta}{n}, \bar{l}, \xi, \tau_b\right) \\
\leq\ & -\frac{\left(t^{(2)}_{b\Delta} - t^{(2)}_{(b+1)\Delta}\right) + \left(t^{(4)}_{b\Delta} - t^{(4)}_{(b+1)\Delta}\right)}{n} Q_{\xi, \frac{(b+1)\Delta}{n}} \\
=\ & -\frac{\left(t^{(1)}_{(b+1)\Delta} - t^{(1)}_{b\Delta}\right) - \left(t^{(2)}_{b\Delta} - t^{(2)}_{(b+1)\Delta}\right) + \left(t^{(3)}_{(b+1)\Delta} - t^{(3)}_{b\Delta}\right) - \left(t^{(4)}_{b\Delta} - t^{(4)}_{(b+1)\Delta}\right)}{n} Q_{\xi, \frac{(b+1)\Delta}{n}} \\
=\ & -\frac{\left(t^{(1)}_{(b+1)\Delta} + t^{(2)}_{(b+1)\Delta} + t^{(3)}_{(b+1)\Delta} + t^{(4)}_{(b+1)\Delta}\right) - \left(t^{(1)}_{b\Delta} + t^{(2)}_{b\Delta} + t^{(3)}_{b\Delta} + t^{(4)}_{b\Delta}\right)}{n} Q_{\xi, \frac{(b+1)\Delta}{n}} \\
=\ & -\frac{\Delta}{n} Q_{\xi, \frac{(b+1)\Delta}{n}}.
\end{aligned}
$$

Using a similar argument, we can show that

$$
\begin{aligned}
& P\left(\frac{(b+1)\Delta}{n}, \bar{l}, \xi\right) - P\left(\frac{b\Delta}{n}, \bar{l}, \xi\right) \\
\geq\ & P\left(\frac{(b+1)\Delta}{n}, \bar{l}, \xi, \tau_{b+1}\right) - P\left(\frac{b\Delta}{n}, \bar{l}, \xi, \tau_{b+1}\right) \\
=\ & \frac{\left(t^{(2)}_{b\Delta} - t^{(2)}_{(b+1)\Delta}\right)}{n} \left(-\ln 2 + \ln \frac{g^2\left(\tau_{b+1}, r_1 c_{(b+1)\Delta}\right)}{g\left(\tau_{b+1}, 2r_1 c_{(b+1)\Delta}\right)}\right) \\
& + \frac{\left(t^{(4)}_{b\Delta} - t^{(4)}_{(b+1)\Delta}\right)}{n} \left(-\ln 2 + \ln \frac{g^2\left(\tau_{b+1}, r_2 c_{(b+1)\Delta}\right)}{g\left(\tau_{b+1}, 2r_2 c_{(b+1)\Delta}\right)}\right) \\
\geq\ & -\frac{\left(t^{(2)}_{b\Delta} - t^{(2)}_{(b+1)\Delta}\right) + \left(t^{(4)}_{b\Delta} - t^{(4)}_{(b+1)\Delta}\right)}{n} \ln 2 \\
=\ & -\frac{\Delta}{n} \ln 2.
\end{aligned}
$$

This completes the proof of Property S1 in case (1).

In case (2), i.e. when $\lceil \log_2 \frac{b\Delta}{n} \rceil = \lceil \log_2 \frac{(b+1)\Delta}{n} \rceil - 1$, we have

$$\begin{aligned}
& P\left(\frac{(b+1)\Delta}{n}, \bar{l}, \xi, \tau_b\right) - P\left(\frac{b\Delta}{n}, \bar{l}, \xi, \tau_b\right) \\
= \quad & \frac{t^{(1)}_{(b+1)\Delta}}{n} \ln \frac{g\left(\tau_b, r_1 c_{(b+1)\Delta}\right)}{2} + \frac{t^{(2)}_{(b+1)\Delta} - t^{(1)}_{b\Delta}}{n} \ln \frac{g\left(\tau_b, 2r_1 c_{(b+1)\Delta}\right)}{2} \\
& - \frac{t^{(2)}_{b\Delta}}{n} \ln \frac{g\left(\tau_b, 4r_1 c_{(b+1)\Delta}\right)}{2} \\
& + \frac{t^{(3)}_{(b+1)\Delta}}{n} \ln \frac{g\left(\tau_b, r_2 c_{(b+1)\Delta}\right)}{2} + \frac{t^{(4)}_{(b+1)\Delta} - t^{(3)}_{b\Delta}}{n} \ln \frac{g\left(\tau_b, 2r_2 c_{(b+1)\Delta}\right)}{2} \\
& - \frac{t^{(4)}_{b\Delta}}{n} \ln \frac{g\left(\tau_b, 4r_2 c_{(b+1)\Delta}\right)}{2}.
\end{aligned}$$

On the other hand,

$$\frac{t^{(1)}_{(b+1)\Delta} + 2t^{(2)}_{(b+1)\Delta}}{n} = R_1 2^{\lceil \log_2 \frac{(b+1)\Delta}{n} \rceil} = R_1 2^{\lceil \log_2 \frac{b\Delta}{n} \rceil + 1} = \frac{2t^{(1)}_{b\Delta} + 4t^{(2)}_{b\Delta}}{n}$$

which implies that

$$\frac{t^{(2)}_{(b+1)\Delta} - t^{(1)}_{b\Delta}}{n} = \frac{2t^{(2)}_{b\Delta} - t^{(1)}_{(b+1)\Delta}/2}{n}.$$

Similarly,

$$\frac{t^{(4)}_{(b+1)\Delta} - t^{(3)}_{b\Delta}}{n} = \frac{2t^{(4)}_{b\Delta} - t^{(3)}_{(b+1)\Delta}/2}{n}$$

and therefore,

$$\begin{aligned}
& P\left(\frac{(b+1)\Delta}{n}, \bar{l}, \xi, \tau_b\right) - P\left(\frac{b\Delta}{n}, \bar{l}, \xi, \tau_b\right) \\
= \quad & \frac{t^{(1)}_{(b+1)\Delta}/2}{n} \left[-\ln 2 + \ln \frac{g^2\left(\tau_b, r_1 c_{(b+1)\Delta}\right)}{g\left(\tau_b, 2r_1 c_{(b+1)\Delta}\right)}\right] + \frac{t^{(2)}_{b\Delta}}{n} \left[-\ln 2 + \ln \frac{g^2\left(\tau_b, 2r_1 c_{(b+1)\Delta}\right)}{g\left(\tau_b, 4r_1 c_{(b+1)\Delta}\right)}\right] \\
& + \frac{t^{(3)}_{(b+1)\Delta}/2}{n} \left[-\ln 2 + \ln \frac{g^2\left(\tau_b, r_2 c_{(b+1)\Delta}\right)}{g\left(\tau_b, 2r_2 c_{(b+1)\Delta}\right)}\right] + \frac{t^{(4)}_{b\Delta}}{n} \left[-\ln 2 + \ln \frac{g^2\left(\tau_b, 2r_2 c_{(b+1)\Delta}\right)}{g\left(\tau_b, 4r_2 c_{(b+1)\Delta}\right)}\right] \\
\leq \quad & -\frac{t^{(1)}_{(b+1)\Delta}/2 + t^{(2)}_{b\Delta} + t^{(3)}_{(b+1)\Delta}/2 + t^{(4)}_{b\Delta}}{n} Q_{\xi, \frac{(b+1)\Delta}{n}} \\
= \quad & -\frac{\Delta}{n} Q_{\xi, \frac{(b+1)\Delta}{n}}
\end{aligned}$$

where the last step is due to the fact that

$$\begin{aligned}
&\frac{t^{(1)}_{(b+1)\Delta}/2 + t^{(2)}_{b\Delta} + t^{(3)}_{(b+1)\Delta}/2 + t^{(4)}_{b\Delta}}{n} \\
&= \frac{t^{(1)}_{(b+1)\Delta} - \left(t^{(1)}_{b\Delta} - t^{(2)}_{(b+1)\Delta}\right) - t^{(2)}_{b\Delta} + t^{(3)}_{(b+1)\Delta} - \left(t^{(3)}_{b\Delta} - t^{(4)}_{(b+1)\Delta}\right) - t^{(4)}_{b\Delta}}{n} \\
&= \frac{\left(t^{(1)}_{(b+1)\Delta} + t^{(2)}_{(b+1)\Delta} + t^{(3)}_{(b+1)\Delta} + t^{(4)}_{(b+1)\Delta}\right) - \left(t^{(1)}_{b\Delta} + t^{(2)}_{b\Delta} + t^{(3)}_{b\Delta} + t^{(4)}_{b\Delta}\right)}{n} \\
&= \frac{\Delta}{n}.
\end{aligned}$$

In a similar manner, we have

$$\begin{aligned}
&P\left(\frac{(b+1)\Delta}{n}, \bar{l}, \xi\right) - P\left(\frac{b\Delta}{n}, \bar{l}, \xi\right) \\
&\geq P\left(\frac{(b+1)\Delta}{n}, \bar{l}, \xi, \tau_{b+1}\right) - P\left(\frac{b\Delta}{n}, \bar{l}, \xi, \tau_{b+1}\right) \\
&= \frac{t^{(1)}_{(b+1)\Delta}/2}{n}\left[-\ln 2 + \ln\frac{g^2\left(\tau_{b+1}, r_1 c_{(b+1)\Delta}\right)}{g\left(\tau_{b+1}, 2r_1 c_{(b+1)\Delta}\right)}\right] + \frac{t^{(2)}_{b\Delta}}{n}\left[-\ln 2 + \ln\frac{g^2\left(\tau_{b+1}, 2r_1 c_{(b+1)\Delta}\right)}{g\left(\tau_{b+1}, 4r_1 c_{(b+1)\Delta}\right)}\right] \\
&\quad + \frac{t^{(3)}_{(b+1)\Delta}/2}{n}\left[-\ln 2 + \ln\frac{g^2\left(\tau_{b+1}, r_2 c_{(b+1)\Delta}\right)}{g\left(\tau_{b+1}, 2r_2 c_{(b+1)\Delta}\right)}\right] + \frac{t^{(4)}_{b\Delta}}{n}\left[-\ln 2 + \ln\frac{g^2\left(\tau_{b+1}, 2r_2 c_{(b+1)\Delta}\right)}{g\left(\tau_{b+1}, 4r_2 c_{(b+1)\Delta}\right)}\right] \\
&\geq -\frac{t^{(1)}_{(b+1)\Delta}/2 + t^{(2)}_{b\Delta} + t^{(3)}_{(b+1)\Delta}/2 + t^{(4)}_{b\Delta}}{n}\ln 2 \\
&= -\frac{\Delta}{n}\ln 2\,.
\end{aligned}$$

The completes the proof of Property S1 in case (2).

Property S2 can be proved in a similar manner.

Now let us move to the proof of Property S3. By Lemma B.3, for $\xi \in (0, \bar{l}/2]$,

$$P(R, \bar{l}, \xi) \geq P(R, \bar{l}, \bar{l}/2) = -R\ln 2$$

which implies that

$$\lim_{R\to 0} P(R, \bar{l}, \xi) \geq 0\,.$$

At the same time, let τ_R be the solution to the equation (6.5) with $\frac{b\Delta}{n} = R$, we have

$$\begin{aligned} P(R,\bar{l},\xi) &= P(R,\bar{l},\xi,\tau_R) \\ &\leq P\left(R,\bar{l},\xi,\frac{\xi}{\bar{l}-\xi}\right) \\ &\leq -\bar{l}H(\xi/\bar{l}) - \xi\ln\left(\frac{\xi}{\bar{l}-\xi}\right) + \bar{l}\ln\left(1+\frac{\xi}{\bar{l}-\xi}\right) \\ &= 0 \end{aligned}$$

where the third step follows the fact that $\frac{\xi}{\bar{l}-\xi} \leq 1$ and $\left(1-\frac{\xi}{\bar{l}-\xi}\right)^k \leq \left(1+\frac{\xi}{\bar{l}-\xi}\right)^k$ for any positive integer k. And therefore,

$$\lim_{R\to 0} P(R,\bar{l},\xi) \leq 0$$

which further yields

$$\lim_{R\to 0} P(R,\bar{l},\xi) = 0\ .$$

This completes the proof of Lemma B.5.

Lemma B.6. *Suppose that $\bar{l}$ is an odd integer. Then for any given $\frac{b\Delta}{n} \geq 0.75$, $P\left(\frac{b\Delta}{n},\bar{l},\xi\right)$ is a strictly decreasing function of ξ in the range $\left(\frac{\bar{l}}{2},\bar{l}-\frac{t^{(1)}_{b\Delta}}{n}\right]$.*

*Proof of **Lemma B.6***: Since $\bar{l}$ is an odd integer, we have $R_1 = 1$, $R_2 = 0$, and hence $t^{(3)}_{b\Delta} = t^{(4)}_{b\Delta} = 0$. Furthermore, whenever $\frac{b\Delta}{n} \geq 0.75 > 0.5$, one has $c_{b\Delta} = 1$, which, coupled with $R_1 = 1$, implies

$$\frac{t^{(1)}_{b\Delta}}{n} = \min\left\{\frac{2b\Delta}{n} - 1, 1\right\} = \frac{2b\Delta}{n} - 1$$

and

$$\frac{t^{(2)}_{b\Delta}}{n} = \frac{b\Delta}{n} - \frac{t^{(1)}_{b\Delta}}{n} = 1 - \frac{b\Delta}{n}.$$

In view of (B.37), it suffices to show that

$$\tau > \frac{\xi/\bar{l}}{1-\xi/\bar{l}}$$

or equivalently,

$$\frac{1}{1+\tau} < 1 - \xi/\bar{l}$$

for $\xi \in \left(\frac{\bar{l}}{2}, \bar{l} - \frac{t^{(1)}_{b\Delta}}{n}\right]$, where τ is the solution to the equation (6.5). By Lemma B.1 and the fact that $\tau = 1$ when $\xi = \frac{\bar{l}}{2}$, we have $\tau > 1$ for $\xi \in \left(\frac{\bar{l}}{2}, \bar{l} - \frac{t^{(1)}_{b\Delta}}{n}\right]$. Moreover, according to the discussion above, equation (6.5) can be further simplified as

$$\left(\frac{2b\Delta}{n} - 1\right) \frac{g(\tau, \bar{l}-1)}{g(\tau, \bar{l})} + \left(2 - \frac{2b\Delta}{n}\right) \frac{g(\tau, 2\bar{l}-1)}{g(\tau, 2\bar{l})} = 1 - \xi/\bar{l}$$

or

$$\frac{1}{1+\tau}\left[\left(\frac{2b\Delta}{n} - 1\right) \frac{1 + \left(\frac{\tau-1}{\tau+1}\right)^{\bar{l}-1}}{1 - \left(\frac{\tau-1}{\tau+1}\right)^{\bar{l}}} + \left(2 - \frac{2b\Delta}{n}\right) \frac{1 - \left(\frac{\tau-1}{\tau+1}\right)^{2\bar{l}-1}}{1 + \left(\frac{\tau-1}{\tau+1}\right)^{2\bar{l}}}\right] = 1 - \xi/\bar{l}\,.$$

Let $z = \frac{\tau-1}{\tau+1}$, and the lemma is proved by showing that

$$\left(\frac{2b\Delta}{n} - 1\right) \frac{1 + z^{\bar{l}-1}}{1 - z^{\bar{l}}} + \left(2 - \frac{2b\Delta}{n}\right) \frac{1 - z^{2\bar{l}-1}}{1 + z^{2\bar{l}}} > 1$$

for $z \in (0, 1)$. Towards this, note that

$$\frac{1 + z^{\bar{l}-1}}{1 - z^{\bar{l}}} > 1 > \frac{1 - z^{2\bar{l}-1}}{1 + z^{2\bar{l}}}$$

and

$$\begin{aligned}
&\left(\frac{2b\Delta}{n} - 1\right) \frac{1 + z^{\bar{l}-1}}{1 - z^{\bar{l}}} + \left(2 - \frac{2b\Delta}{n}\right) \frac{1 - z^{2\bar{l}-1}}{1 + z^{2\bar{l}}} \\
&= \frac{1}{2}\left(\frac{1 + z^{\bar{l}-1}}{1 - z^{\bar{l}}} + \frac{1 - z^{2\bar{l}-1}}{1 + z^{2\bar{l}}}\right) + \left(\frac{2b\Delta}{n} - \frac{3}{2}\right)\left(\frac{1 + z^{\bar{l}-1}}{1 - z^{\bar{l}}} - \frac{1 - z^{2\bar{l}-1}}{1 + z^{2\bar{l}}}\right) \\
&\geq \frac{1}{2}\left(\frac{1 + z^{\bar{l}-1}}{1 - z^{\bar{l}}} + \frac{1 - z^{2\bar{l}-1}}{1 + z^{2\bar{l}}}\right)
\end{aligned}$$

when $\frac{b\Delta}{n} \geq 0.75$. Furthermore,

$$\begin{aligned}
\frac{1 + z^{\bar{l}-1}}{1 - z^{\bar{l}}} + \frac{1 - z^{2\bar{l}-1}}{1 + z^{2\bar{l}}} &\geq 2\sqrt{\frac{1 + z^{\bar{l}-1}}{1 - z^{\bar{l}}} \frac{1 - z^{2\bar{l}-1}}{1 + z^{2\bar{l}}}} \\
&= 2\sqrt{\frac{1 + z^{\bar{l}-1}}{1 + z^{2\bar{l}}}}\sqrt{\frac{1 - z^{2\bar{l}-1}}{1 - z^{\bar{l}}}} > 2
\end{aligned}$$

since $0 < z < 1$. This completes the proof of Lemma B.6.

B.2 LDCP Ensemble with General Degree Distribution

The proof of Lemma 5.1 follows the same approach as that of 6.1, and therefore omitted here. Below we focus on the properties of $P\left(\bar{l}, \xi, R(z)\right)$.

B.2.1 Properties of $P\left(\bar{l}, \xi, R(z)\right)$

In view of (6.5), we define

$$\tilde{l}\left(\bar{l}, R(z), \tau\right) \quad \triangleq \quad \bar{l} - \frac{\bar{l}}{\bar{r}} \sum_{i=1}^{R} R_i r_i \frac{g(\tau, r_i - 1)}{g(\tau, r_i)}$$

Lemma B.7. *Given $\bar{l}$ and $R(z)$, the following properties hold:*

P1 *As a function of τ, $\tilde{l}\left(\bar{l}, R(z), \tau\right)$ is strictly increasing over the interval $[0, +\infty)$.*

P2 *For any $\bar{l}^{\varkappa} \in [0, \bar{l} - \frac{\bar{l}}{\bar{r}} \sum_{j=1}^{R} R_j \pi(r_j))$, there is a unique solution of τ to $\tilde{l}\left(\frac{b\Delta}{n}, \bar{l}, \tau\right) = \bar{l}^{\varkappa}$.*

Lemma B.8. *For fixed $\bar{l}$ and $R(z)$, $P\left(\bar{l}, R(z), \xi\right)$ as a function of ξ is strictly decreasing over $\xi \in (0, \bar{l}/2)$.*

Lemma B.9. *For fixed $\bar{l}$ and $R(z)$, $P\left(\bar{l}, R(z), \xi\right) \geq P\left(\bar{l}, R(z), \bar{l} - \xi\right)$ for $0 < \xi \leq \bar{l}/2$.*

Lemma B.10. *For $\frac{\bar{l}}{\lfloor \bar{l} \rfloor} \leq \xi \leq \frac{\bar{l}}{2}$,*

$$P\left(\bar{l}, R(z), \xi\right) \leq -\frac{\bar{l}}{\bar{r}} \ln 2 + 2\xi \exp\left[-\frac{2\xi}{\bar{l}}\left(r_1 - 1\right)\right] + \frac{\bar{l}}{\bar{r}} \exp\left(-\frac{2\xi}{\bar{l}} r_1\right)$$

The proof of Lemma B.7 to B.10 follows the same approach used in Section B.1.2, and therefore is omitted here.

Lemma B.11. *For any $R(z)$ and $\xi \in \left(0, \frac{\bar{l}}{2}\right)$,*

$$P\left(\bar{l}, R(z), \xi\right) \geq P\left(\bar{l}, \tilde{R}(z), \xi\right) \tag{B.38}$$

where

$$\tilde{R}(z) = \left(1 + \lfloor \bar{r} \rfloor - \bar{r}\right) z^{\lfloor \bar{r} \rfloor} + \left(\bar{r} - \lfloor \bar{r} \rfloor\right) z^{\lceil \bar{r} \rceil}$$

and $\bar{r} = R'(1) = \tilde{R}'(1)$.

*Proof of **Lemma B.11***: Towards proving (B.38), observe that

$$P\left(\bar{l}, R(z), \xi\right) = -\bar{l} H(\xi/\bar{l}) + \min_{\tau > 0} \left[-\xi \ln \tau + \frac{\bar{l}}{\bar{r}} \sum_{i=1}^{R} R_i \ln \frac{g(\tau, r_i)}{2} \right].$$

Now first of all, let us show the following claim ($\star$):

$$(\star)\ \ln g(\tau, k) \text{ is a convex function of } k \text{ for } \tau \in (0,1).$$

To prove this claim,

$$\begin{aligned}
\frac{\partial^2 \ln g(\tau,k)}{\partial k^2} &= \frac{\partial}{\partial k}\left[\frac{\partial \ln g(\tau,k)}{\partial k}\right] \\
&= \frac{\partial}{\partial k}\left[\frac{(1+\tau)^k \ln(1+\tau) + (1-\tau)^k \ln(1-\tau)}{(1+\tau)^k + (1-\tau)^k}\right] \\
&= \frac{\partial}{\partial k}\left[\ln(1+\tau) + \frac{(1-\tau)^k}{(1+\tau)^k + (1-\tau)^k} \ln \frac{1-\tau}{1+\tau}\right] \\
&= \frac{\partial}{\partial k}\left[\left(1 - \frac{1}{1 + \left(\frac{1-\tau}{1+\tau}\right)^k}\right)\right] \ln \frac{1-\tau}{1+\tau} \\
&= \frac{\left(\frac{1-\tau}{1+\tau}\right)^k}{\left[1 + \left(\frac{1-\tau}{1+\tau}\right)^k\right]^2} \ln^2 \frac{1-\tau}{1+\tau} > 0
\end{aligned}$$

whenever $\tau \in (0,1)$. Following the same argument in the proof of Lemma 3 in [70], it can be shown that $\tau_\xi \in (0,1)$ if $\xi \in \left(0, \frac{\bar{l}}{2}\right)$ where τ_ξ is the solution to (6.5). Now if $\bar{r}$ is an

integer, then

$$\begin{aligned}
P(\bar{l}, R(z), \xi) &= -\bar{l}H(\xi/\bar{l}) - \xi \ln \tau_\xi + \frac{\bar{l}}{\bar{r}} \sum_{i=1}^{R} R_i \ln \frac{g(\tau_\xi, r_i)}{2} \\
&\geq -\bar{l}H(\xi/\bar{l}) - \xi \ln \tau_\xi + \frac{\bar{l}}{\bar{r}} \ln \frac{g(\tau_\xi, \sum_{i=1}^{R} R_i r_i)}{2} \\
&= -\bar{l}H(\xi/\bar{l}) - \xi \ln \tau_\xi + \frac{\bar{l}}{\bar{r}} \ln \frac{g(\tau_\xi, \bar{r})}{2} \\
&\geq -\bar{l}H(\xi/\bar{l}) + \min_{\tau>0} \left[-\xi \ln \tau + \frac{\bar{l}}{\bar{r}} \ln \frac{g(\tau, \bar{r})}{2} \right] \\
&= P(\bar{l}, \tilde{R}(z), \xi)
\end{aligned}$$

and the lemma is proved. Now suppose $\bar{r}$ is not an integer. Let

$$\begin{aligned}
\tilde{r}_1 &= \lfloor \bar{r} \rfloor \\
\tilde{r}_2 &= \lceil \bar{r} \rceil \\
\tilde{R}_1 &= 1 + \lfloor \bar{r} \rfloor - \bar{r} \\
\tilde{R}_2 &= \bar{r} - \lfloor \bar{r} \rfloor
\end{aligned}$$

and therefore

$$\tilde{R}(z) = \tilde{R}_1 z^{\tilde{r}_1} + \tilde{R}_2 z^{\tilde{r}_2}.$$

To proceed, another claim ($\star\star$) is proved:

($\star\star$) *For any* $R(z)$ *with* $\bar{r} = R'(1)$, $\exists \{a_i\}_{i=1}^{R}, \{b_i\}_{i=1}^{R} \geq 0$ *such that*

$$a_i + b_i = R_i \text{ for } 1 \leq i \leq R \tag{B.39}$$

$$\sum_{i=1}^{R} a_i = \tilde{R}_1 \tag{B.40}$$

$$\sum_{i=1}^{R} b_i = \tilde{R}_2 \tag{B.41}$$

$$\sum_{i=1}^{R} a_i r_i = \tilde{R}_1 \tilde{r}_1 \tag{B.42}$$

$$\sum_{i=1}^{R} b_i r_i = \tilde{R}_2 \tilde{r}_2 \tag{B.43}$$

It is easily shown that

$$\begin{aligned} &(\text{B.39}) \text{ and } (\text{B.41}) \quad \Rightarrow \quad (\text{B.40}) \\ &(\text{B.39}) \text{ and } (\text{B.42}) \quad \Rightarrow \quad (\text{B.43}) \end{aligned}$$

since

$$\tilde{R}_1 + \tilde{R}_2 = 1 = \sum_{i=1}^{R} R_i$$

$$\tilde{R}_1\tilde{r}_1 + \tilde{R}_2\tilde{r}_2 = \bar{r} = \sum_{i=1}^{R} R_i r_i.$$

Therefore, to verify this claim, we only need to prove that $\exists \{a_i\}_{i=1}^R, \{b_i\}_{i=1}^R \geq 0$ satisfying (B.39), (B.41) and (B.42). Now let

$$\begin{aligned} s &= \begin{bmatrix} a_1 & b_1 & a_2 & b_2 & \cdots & a_R & b_R \end{bmatrix}^T \\ b &= \begin{bmatrix} R_1 & \cdots & R_R & \tilde{R}_2 & \tilde{R}_1\tilde{r}_1 \end{bmatrix}^T \\ A &= \begin{bmatrix} 1 & 1 & & & & & \\ & & 1 & 1 & & & \\ & & & & \ddots & & \\ & & & & & 1 & 1 \\ & 1 & & 1 & \cdots & & 1 \\ r_1 & & r_2 & & \cdots & r_R & \end{bmatrix}_{(R+2)\times 2R} \end{aligned}$$

The claim is equivalent to

$$\exists s \geq 0, As = b$$

which, by Farka's Lemma, is further equivalent to show that

$$A^T x \leq 0 \Rightarrow b^T x \leq 0.$$

In the other word, suppose

$$\begin{matrix} x_i + r_i x_{R+2} \leq 0 \\ x_i + x_{R+1} \leq 0 \end{matrix} \quad \text{for } 1 \leq i \leq R, \tag{B.44}$$

we want to show that

$$\sum_{i=1}^{R} R_i x_i + \tilde{R}_2 x_{R+1} + \tilde{R}_1\tilde{r}_1 x_{R+2} \leq 0.$$

The following proof is divided into two cases: (i) $\sum_{i=1}^R R_i x_i \leq 0$, and (ii) $\sum_{i=1}^R R_i x_i > 0$.

- $\sum_{i=1}^{R} R_i x_i \leq 0$.
  In this case, by (B.44), we have

$$\begin{aligned} \sum_{i=1}^{R} R_i x_i + \bar{r} x_{R+2} &\leq 0 \\ \sum_{i=1}^{R} R_i x_i + x_{R+1} &\leq 0 \end{aligned}$$

  which further implies that

$$\left(\tilde{R}_2 + \frac{\tilde{r}_1}{\bar{r}} \tilde{R}_1 \right) \sum_{i=1}^{R} R_i x_i + \tilde{R}_2 x_{R+1} + \tilde{R}_1 \tilde{r}_1 x_{R+2} \leq 0.$$

  Note that

$$\tilde{R}_2 + \frac{\tilde{r}_1}{\bar{r}} \tilde{R}_1 \leq \tilde{R}_2 + \tilde{R}_1 = 1$$

  and therefore,

$$\left(\tilde{R}_2 + \frac{\tilde{r}_1}{\bar{r}} \tilde{R}_1 \right) \sum_{i=1}^{R} R_i x_i \geq \sum_{i=1}^{R} R_i x_i$$

  since $\sum_{i=1}^{R} R_i x_i \leq 0$, which yields the proof.

- $\sum_{i=1}^{R} R_i x_i > 0$.
  Under this circumstance, at least one of x_i for $1 \leq i \leq R$ is positive, and therefore by (B.44), $x_{R+1}, x_{R+2} < 0$. Let j^* be the index such that

$$j^* = \begin{cases} 0 & \text{if } -x_{R+1} \leq -r_1 x_{R+2} \\ \arg\max_{1 \leq j \leq R} \{ j : -x_{R+1} > -r_j x_{R+2} \} & \text{otherwise} \end{cases}$$

  Then (B.44) becomes

$$x_i \leq \begin{cases} -r_i x_{R+2} & \text{if } 1 \leq i \leq j^* \\ -x_{R+1} & \text{if } j^* + 1 \leq i \leq R \end{cases}$$

  and

$$\sum_{i=1}^{R} R_i x_i + \tilde{R}_2 x_{R+1} + \tilde{R}_1 \tilde{r}_1 x_{R+2} \leq \left(\tilde{R}_2 - \sum_{i=j^*+1}^{R} R_i \right) x_{R+1} + \left(\tilde{R}_1 \tilde{r}_1 - \sum_{i=1}^{j^*} R_i r_i \right) x_{R+2}.$$

On one hand,

$$\begin{aligned}
&\left(\tilde{R}_2 - \sum_{i=j^*+1}^{R} R_i\right) x_{R+1} + \left(\tilde{R}_1\tilde{r}_1 - \sum_{i=1}^{j^*} R_i r_i\right) x_{R+2} \\
&= -\tilde{R}_1 x_{R+1} + \tilde{R}_1\tilde{r}_1 x_{R+2} + \sum_{i=1}^{j^*} R_i \left(x_{R+1} - r_i x_{R+2}\right) \\
&\leq \tilde{R}_1(-x_{R+1} + \tilde{r}_1 x_{R+2})
\end{aligned}$$

On the other hand,

$$\begin{aligned}
&\left(\tilde{R}_2 - \sum_{i=j^*+1}^{R} R_i\right) x_{R+1} + \left(\tilde{R}_1\tilde{r}_1 - \sum_{i=1}^{j^*} R_i r_i\right) x_{R+2} \\
&= \tilde{R}_2 x_{R+1} - \tilde{R}_2\tilde{r}_2 x_{R+2} + \sum_{i=j^*+1}^{R} R_i(-x_{R+1} + r_i x_{R+2}) \\
&\leq \tilde{R}_2(x_{R+1} - \tilde{r}_2 x_{R+2})
\end{aligned}$$

Therefore, the proof is done if $-x_{R+1} \leq -\tilde{r}_1 x_{R+2}$ or $-x_{R+1} \geq -\tilde{r}_2 x_{R+2}$. Now suppose $-\tilde{r}_1 x_{R+2} < -x_{R+1} < -\tilde{r}_2 x_{R+2}$. Note that $r_j \leq \tilde{r}_1$ if $j \leq j^*$, and $r_j \geq \tilde{r}_2$ otherwise, since $\tilde{r}_1$ and $\tilde{r}_2$ only differ by 1. Now if

$$\tilde{R}_2 - \sum_{i=j^*+1}^{R} R_i \geq 0, \text{ and } \tilde{R}_1\tilde{r}_1 - \sum_{i=1}^{j^*} R_i r_i \geq 0,$$

immediately we have

$$\left(\tilde{R}_2 - \sum_{i=j^*+1}^{R} R_i\right) x_{R+1} + \left(\tilde{R}_1\tilde{r}_1 - \sum_{i=1}^{j^*} R_i r_i\right) x_{R+2} \leq 0$$

since $x_{R+1}, x_{R+2} \leq 0$. Now assume at least one of them is negative. If

$$\tilde{R}_2 - \sum_{i=j^*+1}^{R} R_i < 0,$$

by the fact that $x_{R+1} > \tilde{r}_2 x_{R+2}$,

$$\begin{aligned}
&\left(\tilde{R}_2 - \sum_{i=j^*+1}^{R} R_i\right) x_{R+1} + \left(\tilde{R}_1\tilde{r}_1 - \sum_{i=1}^{j^*} R_i r_i\right) x_{R+2} \\
\leq\ &\left(\tilde{R}_2 - \sum_{i=j^*+1}^{R} R_i\right) \tilde{r}_2 x_{R+2} + \left(\tilde{R}_1\tilde{r}_1 - \sum_{i=1}^{j^*} R_i r_i\right) x_{R+2} \\
=\ &\left(\sum_{i=j^*+1}^{R} R_i(r_i - \tilde{r}_2)\right) x_{R+2} \leq 0.
\end{aligned}$$

Meanwhile, if

$$\tilde{R}_1\tilde{r}_1 - \sum_{i=1}^{j^*} R_i r_i < 0,$$

by the fact that $x_{R+2} > \frac{x_{R+1}}{\tilde{r}_1}$,

$$\begin{aligned}
&\left(\tilde{R}_2 - \sum_{i=j^*+1}^{R} R_i\right) x_{R+1} + \left(\tilde{R}_1\tilde{r}_1 - \sum_{i=1}^{j^*} R_i r_i\right) x_{R+2} \\
\leq\ &\left(\tilde{R}_2 - \sum_{i=j^*+1}^{R} R_i\right) x_{R+1} + \left(\tilde{R}_1\tilde{r}_1 - \sum_{i=1}^{j^*} R_i r_i\right) \frac{x_{R+1}}{\tilde{r}_1} \\
=\ &\left(\sum_{i=1}^{j^*} R_i \left(1 - \frac{r_i}{\tilde{r}_1}\right)\right) x_{R+1} \leq 0.
\end{aligned}$$

The proof of claim ($\star\star$) is complete. Now given $R(z)$, let $\{a_i\}_{i=1}^R, \{b_i\}_{i=1}^R \geq 0$ satisfy (B.39)

to (B.43). Then

$$\begin{aligned}
P(\bar{l}, R(z), \xi) &= -\bar{l}H(\xi/\bar{l}) - \xi \ln \tau_\xi + \frac{\bar{l}}{\bar{r}} \sum_{i=1}^{R} R_i \ln \frac{g(\tau_\xi, r_i)}{2} \\
&= -\bar{l}H(\xi/\bar{l}) - \xi \ln \tau_\xi + \frac{\bar{l}}{\bar{r}} \sum_{i=1}^{R} (a_i + b_i) \ln \frac{g(\tau_\xi, r_i)}{2} \\
&= -\bar{l}H(\xi/\bar{l}) - \xi \ln \tau_\xi \\
&\quad + \frac{\bar{l}}{\bar{r}} \left[\left(\sum_{i=1}^{R} a_i \right) \sum_{i=1}^{R} \frac{a_i}{\sum_{i=1}^{R} a_i} \ln \frac{g(\tau_\xi, r_i)}{2} + \left(\sum_{i=1}^{R} b_i \right) \sum_{i=1}^{R} \frac{a_i}{\sum_{i=1}^{R} b_i} \ln \frac{g(\tau_\xi, r_i)}{2} \right] \\
&\geq -\bar{l}H(\xi/\bar{l}) - \xi \ln \tau_\xi \\
&\quad + \frac{\bar{l}}{\bar{r}} \left[\left(\sum_{i=1}^{R} a_i \right) \ln \frac{g\left(\tau_\xi, \frac{\sum_{i=1}^{R} a_i r_i}{\sum_{i=1}^{R} a_i}\right)}{2} \left(\sum_{i=1}^{R} b_i \right) \ln \frac{g\left(\tau_\xi, \frac{\sum_{i=1}^{R} b_i r_i}{\sum_{i=1}^{R} b_i}\right)}{2} \right] \\
&= -\bar{l}H(\xi/\bar{l}) - \xi \ln \tau_\xi + \frac{\bar{l}}{\bar{r}} \left[\tilde{R}_1 \ln \frac{g(\tau_\xi, \tilde{r}_1)}{2} + \tilde{R}_2 \ln \frac{g(\tau_\xi, \tilde{r}_2)}{2} \right] \\
&\geq -\bar{l}H(\xi/\bar{l}) + \min_{\tau > 0} \left\{ -\xi \ln \tau + \frac{\bar{l}}{\bar{r}} \left[\tilde{R}_1 \ln \frac{g(\tau_\xi, \tilde{r}_1)}{2} + \tilde{R}_2 \ln \frac{g(\tau_\xi, \tilde{r}_2)}{2} \right] \right\} \\
&= P(\bar{l}, \tilde{R}(z), \xi).
\end{aligned}$$

The lemma is proved.

References

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

[2] J. M. Wozencraft and I. M. Jacobs. *Principles of Communication Engineering*. Waveland Press, Prospect Heights, IL, 1990.

[3] M. K. Simon, S. M. Hinedi, and W. C. Lindsey. *Digital Communication Techniques: Signal Design and Detection*. Prentice-Hall, Englewood Cliffs, NJ, 1995.

[4] T.-M. Cover and J.-A. Thomas. *Elements of Information Theory (second edition)*. Wiley, Hoboken, NJ, 2006.

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

[6] E.-H. Yang and J. C. Kieffer. Simple universal lossy data compression schemes derived from the lempel-ziv algorithm. *IEEE Trans. Inf. Theory*, IT-42:239–245, Jan. 1996.

[7] T. Berger and J. D. Gibson. Lossy source coding. *IEEE Trans. Inf. Theory*, IT-44:2693–2723, Oct. 1998.

[8] E.-H. Yang, A. Kaltchenko, and J. C. Kieffer. Universal lossless data compression with side information by using a conditional mpm grammar transform. *IEEE Trans. Inform. Theory*, 47:2130–2150, 2001.

[9] J. Ziv and A. Lempel. A universal algorithm for sequential data compression. *IEEE Trans. Inf. Theory*, IT-23(No. 3):337–343, May 1977.

[10] J. Ziv and A. Lempel. Compression of lndiwdual sequences via variable-rate coding. *IEEE Trans. Inf. Theory*, IT-24(5):530–536, Sep. 1978.

[11] J.-C. Kieffer and E.-H. Yang. Grammar based codes: A new class of universal lossless source codes. *IEEE Trans. Inf. Theory*, IT-46(3):737–754, May 2000.

[12] E.-H. Yang and J.-C. Kieffer. Effcient universal lossless compression algorithms based on a greedy sequential grammar transform-part one: Without context models. *IEEE Trans. Inf. Theory*, IT-46(3):755–777, May 2000.

[13] J.-C. Kieffer and E.-H. Yang. Grammar-based lossless universal refinement source coding. *IEEE Trans. Inf. Theory*, IT-50(7):1415–1424, July 2004.

[14] A. Feinstein. A new basic theorem of information theory. *Information Theory, IRE Professional Group on*, 4(4):2 –22, September 1954.

[15] Y. Polyanskiy, H. V. Poor, and S. Verdu. Channel coding rate in the finite blocklength regime. *Information Theory, IEEE Transactions on*, 56(5):2307–2359, may 2010.

[16] V. Korolev and I. Shevtsova. An improvement of the berryesseen inequality with applications to poisson and mixed poisson random sums. *Scandinavian Actuarial Journal*, pages 1–25, 2010.

[17] I. Shevtsova. An improvement of convergence rate estimates in the lyapunov theorem. *Doklady Mathematics*, 82:862–864, 2010. 10.1134/S1064562410060062.

[18] V. Strassen. Asymptoticsche abschätzugen in shannon's informationstheorie. In *Proc. 3rd Conf. Inf. Theory*, pages 689–723, Prague, Czech Republic, 1962.

[19] M. Hayashi. Information spectrum approach to second-order coding rate in channel coding. *Information Theory, IEEE Transactions on*, 55(11):4947–4966, nov. 2009.

[20] Igal Sason and Shlomo Shamai. Performance analysis of linear codes under maximum-likelihood decoding: A tutorial. *Foundations and Trends in Communications and Information Theory*, 3(1/2), 2006.

[21] Y. Polyanskiy. *Channel coding: non-asymptotic fundamental limits.* PhD thesis, Princeton, 2010.

[22] Robert G. Gallager. *Information Theory and Reliable Communication.* John Wiley & Sons, Inc., 1968.

[23] G. Poltyrev. Bounds on the decoding error probability of binary linear codes via their spectra. *Information Theory, IEEE Transactions on*, 40(4):1284 –1292, jul 1994.

[24] S. Yousefi and A.K. Khandani. A new upper bound on the ml decoding error probability of linear binary block codes in awgn interference. *Information Theory, IEEE Transactions on*, 50(12):3026 – 3036, dec. 2004.

[25] A. Mehrabian and S. Yousefi. Improved tangential sphere bound on the ml decoding error probability of linear binary block codes in awgn and block fading channels. *Communications, IEE Proceedings-*, 153(6):885 –893, dec. 2006.

[26] N. Shulman and M. Feder. Random coding techniques for nonrandom codes. *Information Theory, IEEE Transactions on*, 45(6):2101 –2104, sep 1999.

[27] R. Fano. *Transmission of Information: A Statistical Theory of Communications*. The MIT Press, Cambridge, MA, 1961.

[28] E.-H. Yang and J. Meng. Non-asymptotic equipartition properties for independent and identically distributed sources.

[29] Y. Altug and A.B. Wagner. Moderate deviation analysis of channel coding: Discrete memoryless case. In *Proceedings of ISIT'2010*, pages 265 –269, 2010.

[30] Y. Altug and A.B. Wagner. Moderate deviations in channel coding.

[31] Y. Polyanskiy and S. Verdu. Channel dispersion and moderate deviations limits for memoryless channels. In *Proceedings of Allerton'2010*, pages 1334–1339, 2010.

[32] A. J. Goldsmith and S-G. Chua. Adaptive coded modulation for fading channels. *IEEE Trans. Commun.*, 46(5):595–602, May 1998.

[33] M. G. Kim, S. H. Ha, and Y. S. Kim. A selection method of modulation and coding scheme in cdma2000 1xev-dv. In *Proceedings of 59th IEEE Vehicular Technology Conference*, volume 2, pages 999–1003, May 2004.

[34] Evolved universal terrestrial radio access (e-utra); lte physical layer; general description. 3GGP Technical Specification 36.201. www.3gpp.org.

[35] Evolved universal terrestrial radio access (e-utra); physical channels and modulation. 3GGP Technical Specification 36.211. www.3gpp.org.

[36] Evolved universal terrestrial radio access (e-utra); multiplexing and channel coding. 3GGP Technical Specification 36.212. www.3gpp.org.

[37] C. Mehlführer, M. Wrulich, J. C. Ikuno, D. Bosanska, and M. Rupp. Simulating the long term evolution physical layer. In *Proc. of the 17th European Signal Processing Conference (EUSIPCO 2009)*, Glasgow, Scotland, August 2009.

[38] C. E. Shannon. A mathematical theory of communication. *The Bell System Technical Journal*, 27:379–423, 623–656, July, October 1948.

[39] R. M. Tanner. A recursive approach to low complexity codes. *IEEE Trans. Inform. Theory*, 27:533–547, 1981.

[40] E.-H. Yang and D.-K. He. On interactive encoding and decoding for lossless source coding with decoder only side information. In *Proc. of ISIT'08*, pages 419–423, July 2008.

[41] E.-H. Yang and D.-K. He. Interactive encoding and decoding for one way learning: Near lossless recovery with side information at the decoder. *IEEE Trans. Inf. Theory*, 56(4):1808–1824, 2010.

[42] I. Csiszar and J. Korner. *Information Theory: Coding Theorems for Discrete Memoryless Systems*. Academic Press, INC, 1981.

[43] S. Cheng, S. Wang, and L. Cui. Adaptive slepian-wolf decoding using particle filtering based belief propagation. In *Proceedings of Allerton'2009*, pages 607–612, 2009.

[44] J. Gracia-Frias and Y. Zhao. Near-shannon/slepian-wolf performance for unknown correlated sources over awgn channels. *IEEE Trans. on Comm.*, 53(4):555–559, April 2005.

[45] J. Meng, E.-H. Yang, and D.-K. He. Linear interactive encoding and decoding for lossless source coding with decoder only side information. *IEEE Trans. Inf. Theory*, 57(8):5281–5297, Aug. 2011.

[46] C. Daskalakis, A. G. Dimakis, R. M. Karp, and M. J. Wainwright. Probabilistic analysis of linear programming decoding. *IEEE Trans. Inf. Theory*, 54(8):pp. 3565–3578, August 2008.

[47] M. Sartipi and F. Fekri. Distributed source coding in wireless sensor networks using ldpc coding: The entire slepian-wolf rate region. In *Proc. Wireless Communications and Networking Conference*, 2005.

[48] D. Schonberg, K. Ramchandran, and S. S. Pradhan. Distributed code constructions for the entire slepian-wolf rate region for arbitarily correlated sources. In *Proc. IEEE Data Compression Conference*, 2004.

[49] D. Schonberg, K. Ramchandran, and S. S. Pradhan. Ldpc codes can approach the slepian-wolf bound for general binary sources. In *Proc. of fortieth Annual Allerton Conference*, Urbana-Champaign, IL, Oct. 2002.

[50] A. D. Liveris, Z. Xiong, and C. N. Georghiades. Compression of binary sources with side information at the decoder using ldpc codes. *IEEE Comm. Letters*, 6:440–442, Oct. 2002.

[51] S. Sarvotham, D. Baron, and R. G. Baraniuk. Variable-rate universal slepian-wolf coding with feedback. In *Proceedings of the Thirty-Ninth Asilomar Conference on Signals, Systems and Computers*, pages 8–12, 2005.

[52] J. Jiang, D. He, and A. Jagmohan. Rateless slepian-wolf coding based on rate adaptive low-density-parity-check codes. In *Proc. of ISIT'07*, pages 1316 –1320, 2007.

[53] Andrew W. Eckford and Wei Yu. Rateless slepian-wolf codes. In *Proc. of Asilomar Conf. on Signals, Syst., Comput'05*, 2005.

[54] D. Varodayan, A. Aaron, and Bernd Girod. Rate-adaptive distributed source coding using low-denstiy-parity-check codes. In *Thirty-Ninth Asilomar Conference on Signals, Systems and Computers*, pages 1203–1207, Oct. 2005.

[55] F. R. Kschischang, B. J. Frey, and H. A. Leoliger. Factor graphs and the sum-product algorithm. *IEEE Trans. Inf. Theory*, IT-47:498–519, Feb. 2001.

[56] J. Garcia-Frias and Y. Zhao. Compression of correlated binary sources using turbo codes. *IEEE Comm. Lett.*, 5(10):417–419, Oct. 2001.

[57] A. Zia, J. Reilly, and S. Shirani. Distributed parameter estimation with side information: A factor graph approach. In *Proceeding of ISIT'2007*, pages 2556–2560, 2007.

[58] Y. Fang. Crossover probability estimation using mean-intrinsic-llr of ldpc syndrome. *IEEE Comm. Lett.*, 13(9):679–681, 2009.

[59] A. Amraouli. Lthc: Ldpcopt. Online available at the website: http://lthcwww.epfl.ch/research/ldpcopt.

[60] Jin Meng, En-Hui Yang, and Zhen Zhang. Tree interactive encoding and decoding: Conditionally ϕ-mixing sources. In *Information Theory Proceedings (ISIT), 2011 IEEE International Symposium on*, pages 1871 –1875, 31 2011-aug. 5 2011.

[61] E.-H. Yang and Z. Zhang. On the redundancy of lossy source coding with abstract alphabets. *IEEE Trans. Inform. Theory*, 44:1092–1110, 1999.

[62] P. Hall. *Rates of Convergence in the Central Limit Theorem*. Pitman Books Limited, Boston, 1982.

[63] E.-H. Yang and J. Meng. Basic concepts and non-asymptotic capacity achieving coding theorems for channels with discrete inputs. submitted to *IEEE Trans. on Inform. Theory*, 2011.

[64] S. Litsyn and V. Shevelev. On ensembles of low-density parity-check codes: Asymptotic distance distributions. *IEEE Trans. Inf. Theory*, 48(4):887–908, April 2002.

[65] S. Litsyn and V. Shevelev. Distance distributions in ensembles of irregular low-density parity-check codes. *IEEE Trans. Inf. Theory*, 49(12):3140–3159, Dec. 2003.

[66] C. Di, T. J. Richardson, and R. L. Urbanke. Weight distribution of low-density parity-check codes. *IEEE Trans. Inf. Theory*, 52(11):4839–4855, Nov. 2006.

[67] G. Miller and D. Burshtein. Asymptotical enumeration method for analyzing ldpc codes. *IEEE Trans. Inf. Theory*, 50(6):1115–1131, June 2004.

[68] M. P. Mineev and A. I. Pavlov. On the number of (0,1)-matrices with prescribed sums of rows and columns. *Doc. Akad. Nauk SSSR*, 230:1276–1282, 1976.

[69] B. McKay. Asymptotics for 0-1 matrices with prescribed line sums. *Enumeration and Design*, pages 225–238, 1984.

[70] J. Meng and E.-H. Yang. Interactive encoding and decoding based on binary ldpc codes with syndrome accumulation. submitted to *IEEE Trans. on Inform. Theory*, 2011.