# Group, Lattice and Polar Codes for Multi-terminal Communications

by

Aria Ghasemian Sahebi

A dissertation submitted in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
(Electrical Engineering - Systems)
in the University of Michigan
2014

Doctoral Committee:

Associate Professor S. Sandeep Pradhan, Chair
Associate Professor Achilleas Anastasopolous
Professor Robert L. Griess, Jr
Professor David L. Neuhoff

© Aria Ghasemian Sahebi 2014

All Rights Reserved

To my family.

# ACKNOWLEDGEMENTS

It is a pleasure to thank the many people who made this thesis possible.

I would like to express my very great appreciations to my advisor Professor Sandeep Pradhan for his patient guidance, enthusiastic encouragement and constant support. I have been very fortunate to have an advisor who gave me the freedom to explore on my own, and at the same time, the guidance I needed. I am deeply grateful to him for the long discussions that helped me sort out the technical details of my work.

I cannot express enough thanks to my thesis committee members Professor Achilleas Anastasopoulos, Professor Robert Griess and Professor David Neuhoff for their interest in my research and for helping me have the knowledge base needed for my research. I wish to thank Professors Neuhoff and Anastasopoulous for excellent courses in Source Coding theory and Channel Coding theory and I am indebted to Professor Griess for teaching me Abstract Algebra and for his patience in answering my questions.

I would like to express my deep gratitude to Professor Demos Teneketzis for being an excellent teacher and for his support over the years. I would also like to thank Professors Alfred Hero, Raj Rao Nadakuditi, Clayton Scott, Kim Winick, Mingyan Liu, Silvio Savarese, Andrew Yagle, Gregory Wakefield, Amir Mortazawi, Joseph Conlon, Edwin Romeijn and Roman Vershynin for their high standards of teaching and mentorship. I wish to thank Becky Turanski, Karen Liska, Shelly Feldkamp, Ann Pace and Beth Lawson for efficiently and cheerfully helping me deal with administrative

matters.

I have thoroughly enjoyed living in Ann Arbor and that is largely due to the wonderful friends I have had. A big thanks to Hamed, Kaveh , Curtis, Lisa, Dimitris, Molly, Raza, Mahmood, Ali Kakhbod, Ali Nazari, Nima and all of my friends at Michigan. Arun, Farhad, Mohsen, Deepanshu, Raj and David have been great office-mates.

Lastly, I thank my family for their constant encouragement without which this dissertation would not have been possible.

# TABLE OF CONTENTS

**DEDICATION** . . . . . ii

**ACKNOWLEDGEMENTS** . . . . . iii

**LIST OF FIGURES** . . . . . viii

**ABSTRACT** . . . . . x

**CHAPTER**

**I. Introduction** . . . . . 1

**II. Abelian Group Codes for Point-to-Point Communications** . . 7

2.1 Preliminaries . . . . . 8
2.2 The Ensemble of Abelian Group Codes . . . . . 13
2.2.1 A Characterization of Abelian Groups . . . . . 13
2.2.2 The Image Ensemble . . . . . 15
2.3 The Performance of Abelian Group Codes . . . . . 21
2.3.1 Definitions . . . . . 21
2.3.2 Main Results . . . . . 22
2.3.3 Interpretation of the Results . . . . . 24
2.4 Proof for the Source Coding Problem . . . . . 27
2.4.1 The Coding Scheme . . . . . 27
2.4.2 Error Analysis . . . . . 27
2.5 Proof for the Channel Coding Problem . . . . . 30
2.5.1 The Coding Scheme . . . . . 30
2.5.2 Error Analysis . . . . . 31
2.5.3 Simplification of the Result for Symmetric Channels 32
2.6 Examples . . . . . 33
2.6.1 Examples for Source Coding . . . . . 33
2.6.2 Examples for Channel Coding . . . . . 35
2.7 Appendix . . . . . 37

**III. Abelian Group Codes for Multi-terminal Communications** . 47

3.1 Nested Codes for Channels with State Information . . . . . 47
3.1.1 Nested Random/Group Codes for Channel Coding . 47
3.1.2 Nested Group/Random Codes for Channel Coding . 51
3.2 Nested Codes for Sources with Side Information . . . . . 55
3.2.1 Nested Random/Group Codes for Source Coding . . 55
3.2.2 Nested Group/Random Codes for Source Coding . . 60
3.3 Distributed Source Coding . . . . . 64
3.3.1 Preliminaries . . . . . 64
3.3.2 The Main Result . . . . . 67
3.3.3 The Coding Scheme . . . . . 68
3.3.4 Error Analysis . . . . . 71
3.3.5 Examples . . . . . 77
3.3.6 Appendix . . . . . 79
3.4 The 3-User Interference Channel . . . . . 81
3.4.1 Problem Definition and the Coding Scheme . . . . . 81
3.4.2 Error Analysis . . . . . 83

**IV. Non-Abelian Group Codes** . . . . . 90

4.1 Introduction . . . . . 90
4.2 Preliminaries . . . . . 93
4.3 Group Codes over $\mathbb{D}_{2p}$ . . . . . 93
4.4 The Ensemble of Codes . . . . . 98
4.5 Examples: Non-Abelian Group Codes Can Have a Good Performance . . . . . 101
4.5.1 Example 1: Point-to-Point Problem . . . . . 102
4.5.2 Example 2: Computation Over MAC . . . . . 102

**V. Lattice Codes for Multi-terminal Communications** . . . . . 104

5.1 Nested Lattices for Point-to-Point Communications . . . . . 104
5.1.1 Preliminaries . . . . . 105
5.1.2 Nested Lattice Codes for Channel Coding . . . . . 113
5.1.3 Nested Lattice Codes for Source Coding . . . . . 123
5.1.4 Appendix . . . . . 129
5.2 Distributed Source Coding . . . . . 134
5.2.1 The Main Result . . . . . 135
5.2.2 Examples . . . . . 143
5.2.3 Appendix . . . . . 145

**VI. Polar Codes for Point-to-Point Communications** . . . . . 148

6.1 Polar Codes for Arbitrary DMCs . . . . . 148
6.1.1 Preliminaries . . . . . 152
6.1.2 Motivating Examples . . . . . 153
6.1.3 Polar Codes Over Channels with input $\mathbb{Z}_{p^r}$ . . . . . 157
6.1.4 Polar Codes Over Arbitrary Channels . . . . . 173
6.1.5 Relation to Group Codes . . . . . 180
6.1.6 Appendix . . . . . 184
6.2 Polar Codes for Arbitrary DMSs . . . . . 201
6.2.1 Preliminaries . . . . . 201
6.2.2 Polar Codes for Sources with reconstruction alphabet $\mathbb{Z}_{p^r}$ . . . . . 202
6.2.3 Arbitrary Reconstruction Alphabets . . . . . 214
6.3 Nested Polar Codes for Point-to-Point Communications . . . 215
6.3.1 The Lossy Source Coding Problem . . . . . 216
6.3.2 The Channel Coding Problem . . . . . 224

**VII. Polar Codes for Multi-terminal Communications** . . . . . 232

7.1 Introduction . . . . . 232
7.2 Distributed Source Coding: The Berger-Tung Problem . . . . 233
7.3 Distributed Source Coding: Decoding the Sum of Variables . 237
7.4 Multiple Access Channels . . . . . 238
7.5 Computation over MAC . . . . . 240
7.6 The Broadcast Channel . . . . . 241
7.7 Multiple Description Coding . . . . . 242
7.8 Other Problems and Discussion . . . . . 243

**BIBLIOGRAPHY** . . . . . 245

# LIST OF FIGURES

**Figure**


3.1 Comparison of the performance of random codes vs. group codes for a distributed source coding problem. . . . . 79

4.1 A simple channel with input $\mathbb{D}_6$. . . . . 102

4.2 Two user MAC: Computation of $\mathbb{D}_6$ operation. . . . . 102

6.1 Channel 1: The input of the channel has the structure of the group $\mathbb{Z}_4$. 155

6.2 The behavior of $I(W^{b_1 b_2 \cdots b_n})$ for $n = 14$ for Channel 1 when $\epsilon = 0.4$ and $\lambda = 0.2$. . . . . 228

6.3 The asymptotic behavior of $I(W^{b_1 b_2 \cdots b_n})$, $N = 2^n = 2^4, 2^8, 2^{12}, 2^{14}$ for Channel 1 when the data is sorted. . . . . 228

6.4 Channel 2: A channel with a composite input alphabet size. . . . . 229

6.5 Polarization of Channel 2 with parameters $\gamma = 0, \epsilon = 0.4, \lambda = 0.2$. . 230

6.6 Polarization of Channel 2 with parameters $\gamma = 0.4, \epsilon = 0, \lambda = 0.2$. . 230

6.7 Channel 3 . . . . . 230

6.8 Source Coding: Test channel for the inner code. . . . . 231

6.9 Source Coding: Test channel for the outer code. . . . . 231

6.10 Channel Coding: Channel for the inner code. . . . . 231

6.11 Channel Coding: Channel for the outer code. . . . . 231

7.1 Distributed Source Coding: Test channel for the inner code . . . . . 234

7.2 Distributed Source Coding: Test channel for the outer code. . . . . 234
7.3 Korner-Marton Problem, Terminal X: Test channel for the inner code. 238
7.4 Korner-Marton Problem, Terminal X: Test channel for the outer code. 238
7.5 Korner-Marton Problem, Terminal Y: Test channel for the inner code. 238
7.6 Korner-Marton Problem, Terminal Y: Test channel for the outer code. 238
7.7 Multiple-Access Channels: Channel for inner code. . . . . 239
7.8 Multiple-Access Channels: Channel for outer code. . . . . 239
7.9 Computation Over MAC, Termianl X: Channel for inner code. . . . . 240
7.10 Computation Over MAC, Termianl X: Channel for outer code. . . . . 240
7.11 Computation Over MAC, Termianl Y: Channel for inner code. . . . . 241
7.12 Computation Over MAC, Termianl Y: Channel for outer code. . . . . 241
7.13 Broadcast Channels: Test channel for inner code . . . . . 242
7.14 Broadcast Channels: Test channel for outer code . . . . . 242
7.15 Multiple Description Coding, Terminal X: Channel for inner code. . . . . 243
7.16 Multiple Description Coding, Terminal X: Channel for outer code. . . . 243
7.17 Multiple Description Coding, Terminal Y: Channel for inner code. . . . . 243
7.18 Multiple Description Coding, Terminal Y: Channel for outer code. . . . 243
7.19 Three User MAC: Channel for inner code. . . . . 244
7.20 Three User MAC: Channel for outer code. . . . . 244

# ABSTRACT

Group, Lattice and Polar Codes for Multi-terminal Communications

by

Aria Ghasemian Sahebi

Chair: S. Sandeep Pradhan

We study the performance of algebraic codes for multi-terminal communications. This thesis consists of three parts: In the first part, we analyze the performance of group codes for communications systems. We observe that although group codes are not optimal for point-to-point scenarios, they can improve the achievable rate region for several multi-terminal communications settings such as the Distributed Source Coding and Interference Channels. The gains in the rates are particularly significant when the structure of the source/channel is matched to the structure of the underlying group. In the second part, we study the continuous alphabet version of group/linear codes, namely lattice codes. We show that similarly to group codes, lattice codes can improve the achievable rate region for multi-terminal problems. In the third part of the thesis, we present coding schemes based on polar codes to practically achieve the performance limits derived in the two earlier parts. We also present polar coding schemes to achieve the known achievable rate regions for multi-terminal communications problems such as the Distributed Source Coding, the Multiple Description Coding, Broadcast Channels, Interference Channels and Multiple Access Channels.

# CHAPTER I

# Introduction

Approaching information theoretic performance limits of communications using structured codes has been of great interest for the last several decades. The earlier attempts to design computationally efficient encoding and decoding algorithms for point-to-point communication (both channel coding and source coding) resulted in injection of finite field structures to the coding schemes. In the channel coding problem, the channel input alphabets are replaced with algebraic fields and encoders are replaced with matrices. Similarly in source coding problem, the reconstruction alphabets are replaced with a finite fields and decoders are replaced with matrices. Later, these coding approaches were extended to weaker algebraic structures such as rings and groups [1–3, 7, 18, 19, 23, 24, 28, 29, 35, 42, 45][1]. The motivation for this are two fold: a) Finite fields exist only for alphabets with size equal to a prime power, and b) For communication under certain constraints, codes with weaker algebraic structures have better properties. For example, when communicating over an additive white Gaussian noise channel with 8-PSK constellation, codes over $\mathbb{Z}_8$, the cyclic group of size 8, are more desirable over binary linear codes because the structure of the code is matched to the structure of the signal set [2], and hence the former have superior error correcting properties. As another example, construction of polar

[1]Note that this is an incomplete list. There is a vast body of work on group codes. See [19] for a more complete bibliography.

codes over alphabets of size $p^r$, for $r > 1$ and $p$ prime, is simpler with a module structure rather than a vector space structure [54, 58, 66]. Subsequently, as interest in network information theory grew, these codes were used to approach the information-theoretic performance limits of certain special cases of multi-terminal communication problems [26, 57, 75, 78]. These limits were obtained earlier using the random coding ensembles in the information theory literature.

In 1979, Korner and Marton, in a significant departure from tradition, showed that for a binary distributed source coding problem, the asymptotic average performance of binary linear code ensembles can be superior to that of the standard random coding ensembles. Although structured codes were being used in communication mainly for computational complexity reasons, the duo showed that, in contrast, even when computational complexity is not an issue, the use of structured codes leads to superior asymptotic performance limits in multi-terminal communication problems. In the recent past, such gains were shown for a wide class of problems [4, 42, 50, 56, 72]. In [42, 60], an inner bound to the optimal rate-distortion region for the distributed source coding problem is developed in which Abelian group codes were used as building blocks in the coding schemes. Similar coding approaches were applied for the interference channel and the broadcast channel in [52, 53]. The motivation for studying Abelian group codes beyond the non-existence of finite fields over arbitrary alphabets is the following: The algebraic structure of the code imposes certain restrictions on the performance. For certain problems, linear codes were shown to be not optimal [42], and finite Abelian group codes exhibit a superior performance. For example, consider a distributed source coding problem with two statistically correlated but individually uniform quaternary sources $X$ and $Y$ that are related via the relation $X = Y + Z$, where $+$ denotes addition modulo-4 and $Z$ is a hidden quaternary random variable that has a non-uniform distribution and is independent of $Y$. The joint decoder wishes to reconstruct $Z$ losslessly. In this problem, Abelian group codes over the cyclic group

$\mathbb{Z}_4$ perform better than linear codes over the Galois field of size 4. In summary, the main reason for using algebraic structured codes in this context is performance rather than complexity of encoding and decoding. Hence information-theoretic characterizations of asymptotic performance of Abelian group code ensembles for various communication problems and under various decoding constraints became important.

Such performance limits have been characterized in certain special cases. It is well-known that binary linear codes achieve the capacity of binary symmetric channels [25]. More generally, it has also been shown that $q$-ary linear codes can achieve the capacity of symmetric memoryless channels [23] and linear codes can be used to compress a source losslessly down to its entropy [41]. Goblick [3] showed that binary linear codes achieve the rate-distortion function of binary uniform sources with Hamming distortion criterion. Group codes were first studied by Slepian [68] for the Gaussian channel. In [6], the capacity of group codes for certain classes of channels has been computed. Further results on the capacity of group codes were established in [7, 8]. The capacity of group codes over a class of channels exhibiting symmetries with respect to the action of a finite Abelian group has been investigated in [18].

The thesis is organized as follows: Chapter II is devoted to the introduction of finite Abelian group codes and the performance of such codes is studied for point-to-point problems. We study both the channel coding and the source coding problems for arbitrary discrete memoryless sources and channels. Our contribution in this chapter is the source coding result and the generality of the channel coding result. Furthermore, we employ joint encoding and decoding schemes based on joint typicality, resulting in a simplified derivation. The existing results on the performance of Abelian group codes include [18] in which the performance of Abelian group codes over symmetric channels is investigated and [42] in which $\mathbb{Z}_{p^r}$ alphabets are considered. In Chapter III, we study the performance of these codes for some multi-terminal

problems. We derive an achievable rate region for the distributed source coding problem and interference channels as examples of multi-terminal problems in which structured codes prove to be superior to traditional random codes. Further results for other problems can be obtained in the same fashion. In Chapter IV, we consider a class of non-Abelian groups and investigate the coding performance of codes over these groups. The contribution of this chapter is the characterization of the ensemble of all group codes over Dihedral groups and showing that the average performance of this ensemble can be superior to other coding schemes for some examples.

Lattice codes are the analogue of linear/group codes for the the case where the channel inputs or the source reconstructions take values from a continuous alphabet ($\mathbb{R}$ for example). In Chapter V, we discuss the performance of lattice codes for some multi-terminal communications problems namely the Gelfand-Pinsker, the Wyner-Ziv and the distributed source coding problems. For the Gelfand-Pinsker and the Wyner-Ziv problems, we show that nested lattice codes are optimal. For the distributed source coding problem, we derive an achievable rate region which is strictly larger that known achievable regions.

In Chapters VI and VII, we study polar codes. Polar codes were originally introduced as linear codes achieving the symmetric capacity of channels with binary input alphabets. They were later generalized to achieve the symmetric rate-distortion function for sources with binary reconstructions. Traditionally in information and coding theory, random ensembles of codes are considered and the average performance over the ensemble is evaluated. In contrast, polar codes constitute the first class of codes with an explicit construction with a (sub)-optimal performance. We make the observation that polar codes can be extended for arbitrary DMCs and DMSs if they are considered as nested group codes. In other words, we extend polar codes to achieve

the symmetric capacity of arbitrary DMCs and the symmetric rate-distortion function for arbitrary DMSs.

Our next contribution is to show that polar codes are optimal (in the Shannon sense) for both channel coding and source coding problems. We also show that polar codes are optimal for many multi-terminal communication problems in the sense that they achieve the best known achievable rate regions for such problems. This includes the distributed source coding problem, the Korner-Marton problem, the multiple access channel, and computation over MAC. For the broadcast channel, we show that polar codes achieve Marton's inner bound with one additional constraint on auxiliary random variables.

In summary, the thesis consists of results on the performance of structured codes for the following problems:

- Abelian group codes:
  - Point-to-point channel coding
  - Lossy source coding
  - Distributed source coding
  - The interference channel
- Non-Abelian group codes (over $\mathbb{D}_{2^p}$ only):
  - Point-to-point channel coding
  - Computation over multiple-access channels
- Lattice Codes
  - Point-to-point channel coding problem with state information (Gelfand-Pinsker problem).

  - Lossy source coding with state information (Wyner-Ziv problem)
  - Distributed source coding

- Polar codes
  - Point-to-point channel coding (symmetric capacity)
  - Lossy source coding (Symmetric rate-distortion)
  - Point-to-point channel coding (Shannon capacity)
  - Lossy source coding (Shannon rate-distortion)
  - Distributed source coding (Berger-Tung and Korner-Marton problems)
  - Multiple access channels and computation over MAC
  - Broadcast channels
  - Multiple descriptions Coding

# CHAPTER II

# Abelian Group Codes for Point-to-Point Communications

In this chapter, we focus on two problems. First, we consider the lossy source coding problem for arbitrary discrete memoryless sources in which the distortion in measured using a single-letter criterion and the reconstruction alphabet is equipped with the structure of a finite Abelian group $G$. We derive an upper bound on the achievable rate-distortion function using group codes over $G$ of some arbitrarily large block-length $n$. The average performance of the ensemble is shown to be the symmetric rate-distortion function of the source when the underlying group is a field i.e. the Shannon rate-distortion function with the additional constraint that the reconstruction variable is uniformly distributed. For the general case, it turns out that several additional terms appear corresponding to subgroups of the underlying group in the form of a maximization and this can result in a larger rate compared to the symmetric rate for a given distortion level.

In the second part, we consider the channel coding problem for arbitrary discrete memoryless channels. Without a loss of generality, we assume that the channel input alphabet is equipped with the structure of a finite Abelian group $G$. We derive a lower bound on the capacity of such channels achievable using group codes which are subgroups of $G^n$. We show that the achievable rate is equal to the symmetric

capacity of the channel when the underlying group is a field; i.e., it is equal to the Shannon mutual information between the channel input and the channel output when the channel input is uniformly distributed. Similarly to the source coding problem, we show that in the general case, several additional terms appear corresponding to subgroups of the underlying group in the form of a minimization and the achievable rate can be smaller than the symmetric capacity of the channel.

It can be noted that the bounds on the performance limits as mentioned above apply to any arbitrary discrete memoryless case. Moreover, we use joint typicality encoding and decoding [21] for both problems at hand. This will make the analysis more tractable. In this approach we use a synergy of information-theoretic and group-theoretic tools. The traditional approaches have looked at encoding and decoding of structured codes based on either minimum distance or maximum likelihood. We introduce two information quantities that capture the performance limits achievable using Abelian group codes that are analogous to the mutual information which captures the Shannon performance limits when no algebraic structure is enforced on the codes. They are source coding group mutual information and channel coding group mutual information. The converse bounds for both problems will be addressed in a future work.

## 2.1 Preliminaries

### The Source Model

The source is modeled as a discrete-time memoryless random process with each sample taking values from a finite set $\mathscr{X}$ called alphabet according to the distribution $p_X$. The reconstruction alphabet is denoted by $\mathscr{U}$ and the quality of reconstruction is measured by a single-letter distortion functions $d : \mathscr{X} \times \mathscr{U} \to \mathbb{R}^+$. We denote this source by $(\mathscr{X}, \mathscr{U}, p_X, d)$. For two sequences $\boldsymbol{x} = (x_1, \cdots, x_n) \in \mathscr{X}^n$ and $\boldsymbol{u} =$

$(u_1, \cdots, u_n) \in \mathscr{U}^n$, with a slight abuse of notation, we denote the average distortion by

$$d(\boldsymbol{x}, \boldsymbol{u}) = \frac{1}{n} \sum_{i=1}^{n} d(x_i, u_i)$$

**The Channel Model**

We consider discrete memoryless channels used without feedback. We associate two finite sets $\mathscr{X}$ and $\mathscr{Y}$ with the channel as the input and output alphabets. The input-output relation of the channel is characterized by a conditional probability law $W_{Y|X}(y|x)$ for $x \in \mathscr{X}$ and $y \in \mathscr{Y}$. The channel is specified by $(\mathscr{X}, \mathscr{Y}, W_{Y|X})$.

**Review of Groups**

In this section, we review some of the basic concepts of group theory. For a more complete discussion, we refer the reader to [16]. A *group* $(G, +)$ is a set $G$ together with a binary operation $+$ such that

- For all $a, b \in G$, $a + b \in G$.
- For all $a, b, c \in G$, $a + (b + c) = (a + b) + c$.
- There exists $0 \in G$ such that $a + 0 + 0 + a = a \in G$.
- For all $a \in G$, there exists $b \in G$ such that $a + b = b + a = 0$.

If in addition to the above, the following condition is satisfied

- For all $a, b \in G$, $a + b = b + a$.

then the group is called *Abelian*. We focus on finite groups, i.e., groups whose set is finite. When the group operation is clear from the context, we sometimes denote the group $(G, +)$ simply as $G$. Given a group $G$, a subset $H$ of $G$ is called a *subgroup* of $G$ if it is closed under the group operation. In this case, $(H, +)$ is a group in its own

right. This is denoted by $H \leq G$. A *coset* $C$ of a subgroup $H$ is a shift of $H$ by an arbitrary element $a \in G$ (i.e., $C = a + H$ for some $a \in G$). For a subgroup $H$ of $G$, cosets of $H$ is $G$ form a partition of $G$. The number of cosets of $H$ in $G$ is called the *index* of $H$ in $G$ and is denoted by $|G : H|$. The index of $H$ in $G$ is equal to $|G|/|H|$ where $|G|$ and $|H|$ are the cardinalities of $G$ and $H$ respectively. If $|G|$ is a power of a prime $p$, we say $G$ is a $p$-group. For a prime $p$ dividing the cardinality of $G$, a *Sylow-p* subgroup of $G$ is a subgroup of $G$ whose cardinality is a power of $p$ which is not contained in another $p$-subgroup of $G$.

Given two groups $(G, +_G)$ and $(K, +_K)$, a mapping $\phi : G \to K$ is called a homomorphism if for all $a, b \in G$, $\phi(a +_G b) = \phi(a) +_K \phi(b)$. The groups $G$ and $K$ are called to be isomorphic if there exists a bijective homomorphism $\phi$ between $G$ and $K$. In this case, we write $G \cong K$.

All groups referred to in this chapter are Abelian groups.

### Group Codes

Given a group $G$, a group code $\mathbb{C}$ over $G$ with block length $n$ is any subgroup of $G^n$. A shifted group code over $G$, $\mathbb{C} + \boldsymbol{b}$ is a translation of a group code $\mathbb{C}$ by a fixed vector $\boldsymbol{b} \in G^n$. When the underlying group $G$ is a finite field, the group code is a subspace over $G$ and is called a linear code. Group codes generalize the notion of linear codes over fields to sources with reconstruction alphabets (and channels with input alphabets) having composite sizes.

### Achievability for Source Coding and the Rate-Distortion Function

For a group $G$, a group transmission system with parameters $(n, \Theta, \Delta, \tau)$ for compressing a given source $(\mathscr{X}, \mathscr{U} = G, P_X, d)$ consists of a codebook $\mathbb{C}$, an encoding mapping $\mathrm{Enc}(\cdot)$, and a decoding mapping $\mathrm{Dec}$. The codebook $\mathbb{C}$ is a shifted group

code over $G$ whose size is equal to $\Theta$ and the mappings are defined as

$$\text{Enc} : \mathscr{X}^n \to \{1, 2, \ldots, \Theta\},$$

$$\text{Dec} : \{1, 2, \ldots, \Theta\} \to \mathbb{C}$$

such that

$$P\Big[d\Big(X^n, \text{Dec}\big(\text{Enc}(X^n)\big)\Big) > \Delta\Big] \leq \tau$$

where $X^n$ is the random vector of length $n$ generated by the source. In this transmission system, $n$ denotes the block length, $\log \Theta$ denotes the number of "channel uses", $\Delta$ denotes the distortion level, and $\tau$ is a bound on the probability of exceeding the distortion level $\Delta$.

Given a source $(\mathscr{X}, \mathscr{U} = G, P_X, d)$, a pair of non-negative real numbers $(R, D)$ is said to be achievable using group codes if for every $\epsilon > 0$ and for all sufficiently large numbers $n$, there exists a group transmission system with parameters $(n, \Theta, \Delta, \tau)$ for compressing the source such that

$$\frac{1}{n} \log \Theta \leq R + \epsilon, \qquad \Delta \leq D + \epsilon, \qquad \tau \leq \epsilon$$

The optimal group rate-distortion function $R^*(D)$ of the source is given by the infimum of the rates $R$ such that $(R, D)$ is achievable using group codes.

**Achievability for Channel Coding**

For a group $G$, a group transmission system with parameters $(n, \Theta, \tau)$ for reliable communication over a given channel $(\mathscr{X} = G, \mathscr{Y}, W_{Y|X})$ consists of a codebook $\mathbb{C}$, an encoding mapping $\text{Enc}(\cdot)$, and a decoding mapping $\text{Dec}(\cdot)$. The codebook $\mathbb{C}$ is a shifted subgroup of $G^n$ group code over $G$ whose size is equal to $\Theta$ and the mappings are defined as

$$\text{Enc} : \{1, 2, \cdots, \Theta\} \to \mathbb{C}$$

$$\text{Dec} : \mathscr{Y}^n \to \{1, 2, \cdots, \Theta\}$$

such that

$$\sum_{m=1}^{\Theta} \frac{1}{\Theta} \sum_{\boldsymbol{y}:\mathrm{Dec}(\boldsymbol{y})\neq m} W^n(\boldsymbol{y}|\mathrm{Enc}(m)) \leq \tau$$

or equivalently,

$$\sum_{m=1}^{\Theta} \frac{1}{\Theta} \sum_{\boldsymbol{x}\in\mathscr{X}^n} \mathbb{1}_{\{\boldsymbol{x}=\mathrm{Enc}(m)\}} \sum_{\boldsymbol{y}\in\mathscr{Y}^n} W^n(\boldsymbol{y}|\boldsymbol{x}) \mathbb{1}_{\{m\neq\mathrm{Dec}(\boldsymbol{y})\}} \leq \tau$$

Given a channel $(\mathscr{X} = G, \mathscr{Y}, W_{Y|X})$, the rate $R$ is said to be achievable using group codes if for all $\epsilon > 0$ and for all sufficiently large $n$, there exists a group transmission system for reliable communication with parameters $(n, \Theta, \tau)$ such that

$$\frac{1}{n}\log\Theta \geq R - \epsilon, \qquad \tau \leq \epsilon$$

The group capacity of the channel $C$ is defined as the supremum of the set of all achievable rates using group codes.

**Typicality**

Consider two random variables $X$ and $Y$ with joint probability mass function $p_{XY}(x, y)$ for $(x, y) \in \mathscr{X} \times \mathscr{Y}$. Let $n$ be an integer and let $\epsilon$ be a positive real number. The sequence pair $(\boldsymbol{x}, \boldsymbol{y})$ belonging to $\mathscr{X}^n \times \mathscr{Y}^n$ is said to be jointly $\epsilon$-typical with respect to $p_{XY}$ if

$$\forall a \in \mathscr{X},\ \forall b \in \mathscr{Y} : \left|\frac{1}{n} N\left(a, b|\boldsymbol{x}, \boldsymbol{y}\right) - p_{XY}(a, b)\right| \leq \frac{\epsilon}{|\mathscr{X}||\mathscr{Y}|}$$

and none of the pairs $(a, b)$ with $p_{XY}(a, b) = 0$ occurs in $(\boldsymbol{x}, \boldsymbol{y})$. Here, $N(a, b|\boldsymbol{x}, \boldsymbol{y})$ counts the number of occurrences of the pair $(a, b)$ in the sequence pair $(\boldsymbol{x}, \boldsymbol{y})$. We denote the set of all jointly $\epsilon$-typical sequence pairs in $\mathscr{X}^n \times \mathscr{Y}^n$ by $A_\epsilon^n(X, Y)$.
Given a sequence $\boldsymbol{x} \in A_\epsilon^n(X)$, the set of conditionally $\epsilon$-typical sequences $A_\epsilon^n(Y|\boldsymbol{x})$ is defined as

$$A_\epsilon^n(Y|\boldsymbol{x}) = \{\boldsymbol{y} \in \mathscr{Y}^n \,|(\boldsymbol{x}, \boldsymbol{y}) \in A_\epsilon^n(X, Y)\}$$

**Notation**

In our notation, $\mathbb{P}$ is the set of all primes, $\mathbb{Z}^+$ is the set of positive integers, $\mathbb{R}^+$ is the set of non-negative reals, and for a prime $p$ and a positive integer $r$, $\mathbb{Z}_{p^r}$ is the cyclic group of order $p^r$. Since we deal with summations over several groups in this thesis, when not clear from the context, we indicate the underlying group in each summation, e.g., summation over the group $G$ is denoted by $\overbrace{\sum}^{(G)}$. Direct sum of groups is denoted by $\bigoplus$ and direct product of sets is denoted by $\bigotimes$.

## 2.2 The Ensemble of Abelian Group Codes

In this section, we use a standard characterization of Abelian groups and introduce the ensemble of Abelian group codes used in the thesis.

### 2.2.1 A Characterization of Abelian Groups

For an Abelian group $G$, let $\mathscr{P}(G)$ denote the set of all prime divisors of $|G|$ and for a prime $p \in \mathscr{P}(G)$ let $S_p(G)$ be the corresponding Sylow subgroup of $G$. It is known [36, Theorem 3.3.1] that any Abelian group $G$ can be decomposed into a direct sum of its Sylow subgroups in the following manner

$$G = \bigoplus_{p \in \mathscr{P}(G)} S_p(G) \tag{2.1}$$

Furthermore, each Sylow subgroup $S_p(G)$ can be decomposed into $\mathbb{Z}_{p^r}$ groups as follows:

$$S_p(G) \cong \bigoplus_{r \in \mathscr{R}_p(G)} \mathbb{Z}_{p^r}^{M_{p,r}} \tag{2.2}$$

where $\mathscr{R}_p(G) \subseteq \mathbb{Z}^+$ and for $r \in \mathscr{R}_p(G)$, $M_{p,r}$ is a positive integer. Note that $\mathbb{Z}_{p^r}^{M_{p,r}}$ is defined as the direct sum of the ring $\mathbb{Z}_{p^r}$ with itself for $M_{p,r}$ times. Combining

Equations (2.1) and (2.2), we can represent any Abelian group as follows:

$$G \cong \bigoplus_{p \in \mathscr{P}(G)} \bigoplus_{r \in \mathscr{R}_p(G)} \mathbb{Z}_{p^r}^{M_{p,r}} = \bigoplus_{p \in \mathscr{P}(G)} \bigoplus_{r \in \mathscr{R}_p(G)} \bigoplus_{m=1}^{M_{p,r}} \mathbb{Z}_{p^r}^{(m)} \tag{2.3}$$

where $\mathbb{Z}_{p^r}^{(m)}$ is called the $m^{\text{th}}$ $\mathbb{Z}_{p^r}$ ring of $G$ or the $(p, r, m)^{\text{th}}$ ring of $G$. Equivalently, this can be written as follows

$$G \cong \bigoplus_{(p,r,m) \in \mathscr{G}(G)} \mathbb{Z}_{p^r}^{(m)}$$

where $\mathscr{G}(G) \subseteq \mathbb{P} \times \mathbb{Z}^+ \times \mathbb{Z}^+$ is defined as:

$$\mathscr{G}(G) = \{(p, r, m) \in \mathbb{P} \times \mathbb{Z}^+ \times \mathbb{Z}^+ | p \in \mathscr{P}(G), r \in \mathscr{R}_p(G), m \in \{1, 2, \cdots, M_{p,r}\}\}$$

This means that any element $a$ of the Abelian group $G$ can be regarded as a vector whose components are indexed by $(p, r, m) \in \mathscr{G}(G)$ and whose $(p, r, m)^{\text{th}}$ component $a_{p,r,m}$ takes values from the ring $\mathbb{Z}_{p^r}$. With a slight abuse of notation, we represent an element $a$ of $G$ as

$$a = \bigoplus_{(p,r,m) \in \mathscr{G}(G)} a_{p,r,m}$$

Furthermore, for two elements $a, b \in G$, we have

$$a + b = \bigoplus_{(p,r,m) \in \mathscr{G}(G)} a_{p,r,m} +_{p^r} b_{p,r,m}$$

where $+$ denotes the group operation and $+_{p^r}$ denotes addition mod-$p^r$. More generally, let $a, b, \cdots, z$ be any number of elements of $G$. Then we have

$$a + b + \cdots + z = \bigoplus_{(p,r,m) \in \mathscr{G}(G)} (a_{p,r,m} +_{p^r} b_{p,r,m} +_{p^r} \cdots +_{p^r} z_{p,r,m}) \tag{2.4}$$

This can equivalently be written as

$$[a + b + \cdots + z]_{p,r,m} = a_{p,r,m} +_{p^r} b_{p,r,m} +_{p^r} \cdots +_{p^r} z_{p,r,m}$$

where $[\cdot]_{p,r,m}$ denotes the $(p, r, m)^{\text{th}}$ component of it's argument.

Let $\mathbb{I}_{G:p,r,m} \in G$ be a generator for the group which is isomorphic to the $(p,r,m)^{\text{th}}$ ring of $G$. Then we have

$$a = \overbrace{\sum_{(p,r,m)\in\mathscr{G}(G)}}^{(G)} a_{p,r,m}\mathbb{I}_{G:p,r,m} \tag{2.5}$$

where the summations are done with respect to the group operation and the multiplication $a_{p,r,m}\mathbb{I}_{G:p,r,m}$ is by definition the summation (with respect to the group operation) of $\mathbb{I}_{G:p,r,m}$ to itself for $a_{p,r,m}$ times. In other words, $a_{p,r,m}\mathbb{I}_{G:p,r,m}$ is the short hand notation for

$$a_{p,r,m}\mathbb{I}_{G:p,r,m} = \overbrace{\sum_{i\in\{1,\cdots,a_{p,r,m}\}}}^{(G)} \mathbb{I}_{G:p,r,m}$$

where the summation is the group operation.

**Example:** Let $G = \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_9^2$. Then we have $\mathscr{P}(G) = \{2,3\}$, $S_2(G) = \mathbb{Z}_4$ and $S_3(G) = \mathbb{Z}_3 \oplus \mathbb{Z}_9^2$, $\mathscr{R}_2(G) = \{2\}$, $\mathscr{R}_3(G) = \{1,2\}$, $M_{2,2} = 1$, $M_{3,1} = 1$, $M_{3,2} = 2$ and

$$\mathscr{G}(G) = \{(2,2,1),(3,1,1),(3,2,1),(3,2,2)\}$$

Each element $a$ of $G$ can be represented by a quadruple $(a_{2,2,1}, a_{3,1,1}, a_{3,2,1}, a_{3,2,2})$ where $a_{2,2,1} \in \mathbb{Z}_4$, $a_{3,1,1} \in \mathbb{Z}_3$ and $a_{3,2,1}, a_{3,2,2} \in \mathbb{Z}_9$. Finally, we have $\mathbb{I}_{G:2,2,1} = (1,0,0,0)$, $\mathbb{I}_{G:3,1,1} = (0,1,0,0)$, $\mathbb{I}_{G:3,2,1} = (0,0,1,0)$, $\mathbb{I}_{G:3,2,2} = (0,0,0,1)$ so that Equation (2.5) holds.

In the following section, we introduce the ensemble of Abelian group codes which we use in this chapter.

### 2.2.2 The Image Ensemble

Recall that for a positive integer $n$, an Abelian group code of length $n$ over the group $G$ is a subgroup of $G^n$. Our ensemble of codes consists of all Abelian group codes over $G$, i.e., we consider all subgroups of $G^n$. We use the following fact to characterize all subgroups of $G^n$:

**Lemma II.1.** *For an Abelian group $\tilde{G}$, let $\phi : J \to \tilde{G}$ be a homomorphism from some Abelian group $J$ to $\tilde{G}$. Then $\phi(J) \leq \tilde{G}$, i.e., the image of the homomorphism is a subgroup of $\tilde{G}$. Moreover, for any subgroup $\tilde{H}$ of $\tilde{G}$ there exists a corresponding Abelian group $J$ and a homomorphism $\phi : J \to \tilde{G}$ such that $\tilde{H} = \phi(J)$.*

*Proof.* The first part of the lemma is proved in [16, Theorem 12-1]. For the second part, Let $J$ be isomorphic to $\tilde{H}$ and let $\phi$ be the identity mapping (more rigorously, let $\phi$ be the isomorphism between $J$ and $\tilde{H}$). □

In order to use the above lemma to construct an ensemble of subgroups of $G^n$, we need to identify all groups $J$ from which there exist non-trivial homomorphisms to $G^n$. Then the above lemma implies that for each such $J$ and for each homomorphism $\phi : J \to G^n$, the image of the homomorphism is a group code over $G$ of length $n$ and for each group code $\mathbb{C} \leq G^n$, there exists a group $J$ and a homomorphism such that $\mathbb{C}$ is the image of the homomorphism. This ensemble corresponds to the ensemble of linear codes characterized by their generator matrix when the underlying group is a field of prime size. Note that as in the case of standard ensembles of linear codes, the correspondence between this ensemble and the set of Abelian group codes over $G$ of length $n$ may not be one-to-one.

Let $\tilde{G}$ and $J$ be two Abelian groups with decompositions:

$$\tilde{G} = \bigoplus_{(p,r,m)\in\mathscr{G}(\tilde{G})} \mathbb{Z}_{p^r}^{(m)}$$

$$J = \bigoplus_{(q,s,l)\in\mathscr{G}(J)} \mathbb{Z}_{q^s}^{(l)}$$

and let $\phi$ be a homomorphism from $J$ to $\tilde{G}$. For $(q,s,l) \in \mathscr{G}(J)$ and $(p,r,m) \in \mathscr{G}(\tilde{G})$, let

$$g_{(q,s,l)\to(p,r,m)} = [\phi(\mathbb{I}_{J:q,s,l})]_{p,r,m}$$

where $\mathbb{I}_{J:q,s,l} \in J$ is the standard generator for the $(q,s,l)^{\text{th}}$ ring of $J$ and $[\phi(\mathbb{I}_{J:q,s,l})]_{p,r,m}$ is the $(p,r,m)^{\text{th}}$ component of $\phi(\mathbb{I}_{J:q,s,l}) \in \tilde{G}$. For $a = \bigoplus_{(q,s,l)\in\mathscr{G}(J)} a_{q,s,l} \in J$, let $b = \phi(a)$ and write $b = \bigoplus_{(p,r,m)\in\mathscr{G}(\tilde{G})} b_{p,r,m}$. Note that as in Equation (2.5), we can write:

$$\begin{aligned} a &= \overbrace{\sum_{(q,s,l)\in\mathscr{G}(J)}}^{(J)} a_{q,s,l}\mathbb{I}_{J:q,s,l} \\ &= \overbrace{\sum_{(q,s,l)\in\mathscr{G}(J)}}^{(J)} \overbrace{\sum_{i\in\{1,\cdots,a_{q,s,l}\}}}^{(J)} \mathbb{I}_{J:q,s,l} \end{aligned}$$

where the summations are the group summations. We have

$$\begin{aligned} b_{p,r,m} &= [\phi(a)]_{p,r,m} \\ &= \left[\phi\left(\overbrace{\sum_{(q,s,l)\in\mathscr{G}(J)}}^{(J)} \overbrace{\sum_{i\in\{1,\cdots,a_{q,s,l}\}}}^{(J)} \mathbb{I}_{J:q,s,l}\right)\right]_{p,r,m} \\ &\overset{(a)}{=} \left[\overbrace{\sum_{(q,s,l)\in\mathscr{G}(J)}}^{(\tilde{G})} \overbrace{\sum_{i\in\{1,\cdots,a_{q,s,l}\}}}^{(\tilde{G})} \phi\left(\mathbb{I}_{J:q,s,l}\right)\right]_{p,r,m} \\ &\overset{(b)}{=} \overbrace{\sum_{(q,s,l)\in\mathscr{G}(J)}}^{(\mathbb{Z}_{p^r})} \overbrace{\sum_{i\in\{1,\cdots,a_{q,s,l}\}}}^{(\mathbb{Z}_{p^r})} \left[\phi\left(\mathbb{I}_{J:q,s,l}\right)\right]_{p,r,m} \\ &\overset{(c)}{=} \overbrace{\sum_{(q,s,l)\in\mathscr{G}(J)}}^{(\mathbb{Z}_{p^r})} a_{q,s,l}\left[\phi\left(\mathbb{I}_{J:q,s,l}\right)\right]_{p,r,m} \\ &= \overbrace{\sum_{(q,s,l)\in\mathscr{G}(J)}}^{(\mathbb{Z}_{p^r})} a_{q,s,l} g_{(q,s,l)\to(p,r,m)} \end{aligned}$$

Note that $(a)$ follows since $\phi$ is a homomorphism; $(b)$ follows from Equation (2.4); and $(c)$ follows by using $a_{q,s,l}\left[\phi\left(\mathbb{I}_{J:q,s,l}\right)\right]_{p,r,m}$ as the short hand notation for the summation of $\left[\phi\left(\mathbb{I}_{J:q,s,l}\right)\right]_{p,r,m}$ to itself for $a_{q,s,l}$ times.

Note that $g_{(q,s,l)\to(p,r,m)}$ represents the effect of the $(q,s,l)^{\text{th}}$ component of $a$ on the $(p,r,m)^{\text{th}}$ component of $b$ dictated by the homomorphism. This means that the

homomorphism $\phi$ can be represented by

$$\phi(a) = \bigoplus_{(p,r,m)\in\mathscr{G}(\tilde{G})} \overbrace{\sum_{(q,s,l)\in\mathscr{G}(J)}}^{(\mathbb{Z}_{p^r})} a_{q,s,l} g_{(q,s,l)\to(p,r,m)} \tag{2.6}$$

where $a_{q,s,l}g_{(q,s,l)\to(p,r,m)}$ is the short-hand notation for the mod-$p^r$ addition of $g_{(q,s,l)\to(p,r,m)}$ to itself for $a_{q,s,l}$ times. We have the following lemma on $g_{(q,s,l)\to(p,r,m)}$:

**Lemma II.2.** *For a homomorphism described by* (2.6)*, we have*

$$\begin{aligned} g_{(q,s,l)\to(p,r,m)} &= 0 && \text{If } p \neq q \\ g_{(q,s,l)\to(p,r,m)} &\in p^{r-s}\mathbb{Z}_{p^r} && \text{If } p = q, r \geq s \end{aligned}$$

*Moreover, any mapping described by* (2.6) *and satisfying these conditions is a homomorphism.*

*Proof.* The proof is provided in Appendix 2.7.0.1. □

This lemma implies that in order to construct a subgroup of $\tilde{G}$, we only need to consider homomorphisms from an Abelian group $J$ to $\tilde{G}$ such that

$$\mathscr{P}(J) \subseteq \mathscr{P}(\tilde{G})$$

since if for some $(q,s,l) \in \mathscr{G}(J)$, $q \notin \mathscr{P}(\tilde{G})$ then $\phi(a)$ would not depend on $a_{q,s,l}$. For $p \in \mathscr{P}(\tilde{G})$, define

$$r_p = \max \mathscr{R}_p(G) \tag{2.7}$$

We show that we can restrict ourselves to $J$'s such that for all $(q,s,l) \in \mathscr{G}(J)$, $s \leq r_q$. For $(q,s,l) \in \mathscr{G}(J)$, assume $s > r_p$. Then for all $(p,r,m) \in \mathscr{G}(\tilde{G})$, if $p = q$, we have $s > r$. Let $(p,r,m) \in \mathscr{G}(\tilde{G})$ be such that $p = q$. Since $g_{(q,s,l)\to(p,r,m)} \in \mathbb{Z}_{p^r}$ and $r \leq r_q$, we have

$$\begin{aligned} \left(a_{q,s,l}g_{(q,s,l)\to(p,r,m)}\right) \pmod{p^r} &= \left((a_{q,s,l}) \pmod{p^r} g_{(q,s,l)\to(p,r,m)}\right) \pmod{p^r} \\ &= \left((a_{q,s,l}) \pmod{p^{r_q}} g_{(q,s,l)\to(p,r,m)}\right) \pmod{p^r} \end{aligned}$$

This implies that for all $a \in J$ and all $(q,s,l) \in \mathscr{G}(J)$, in the expression for the $(p,r,m)^{\text{th}}$ component of $\phi(a)$ with $p=q$, $a_{q,s,l}$ appears as $(a_{q,s,l}) \pmod{q^{r_q}}$. Therefore, it suffices for $a_{q,s,l}$ to take values from $\mathbb{Z}_{q^{r_q}}$ and this happens if $s \leq r_q$.

To construct Abelian group codes of length $n$ over $G$, let $\tilde{G} = G^n$. we have

$$G^n \cong \bigoplus_{p\in\mathscr{P}(G)} \bigoplus_{r\in\mathscr{R}_p} \mathbb{Z}_{p^r}^{nM_{p,r}} = \bigoplus_{p\in\mathscr{P}(G)} \bigoplus_{r\in\mathscr{R}_p} \bigoplus_{m=1}^{nM_{p,r}} \mathbb{Z}_{p^r}^{(m)} = \bigoplus_{(p,r,m)\in\mathscr{G}(G^n)} \mathbb{Z}_{p^r}^{(m)} \tag{2.8}$$

Define $J$ as

$$J = \bigoplus_{q\in\mathscr{P}(G)} \bigoplus_{s=1}^{r_q} \mathbb{Z}_{q^s}^{k_{q,s}} = \bigoplus_{q\in\mathscr{P}(G)} \bigoplus_{s=1}^{r_q} \bigoplus_{l=1}^{k_{q,s}} \mathbb{Z}_{q^s}^{(l)} = \bigoplus_{(q,s,l)\in\mathscr{G}(J)} \mathbb{Z}_{q^s}^{(l)} \tag{2.9}$$

for some positive integers $k_{q,s}$.

**Example:** Let $G = \mathbb{Z}_8 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_5$. Then we have

$$J = \mathbb{Z}_2^{k_{2,1}} \oplus \mathbb{Z}_4^{k_{2,2}} \oplus \mathbb{Z}_8^{k_{2,3}} \oplus \mathbb{Z}_3^{k_{3,1}} \oplus \mathbb{Z}_9^{k_{3,2}} \oplus \mathbb{Z}_5^{k_{5,1}}$$

Define

$$k = \sum_{q\in\mathscr{P}(G)} \sum_{s=1}^{r_q} k_{q,s}$$

and $w_{q,s} = \frac{k_{q,s}}{k}$ for $q \in \mathscr{P}(G)$ and $s = 1, \cdots, r_q$ so that we can write

$$J = \bigoplus_{q\in\mathscr{P}(G)} \bigoplus_{s=1}^{r_q} \bigoplus_{l=1}^{kw_{q,s}} \mathbb{Z}_{q^s}^{(l)} \tag{2.10}$$

for some constants $w_{q,s}$ adding up to one.

The ensemble of Abelian group encoders consists of all mappings $\phi : J \to G^n$ of the form

$$\phi(a) = \bigoplus_{(p,r,m)\in\mathscr{G}(G^n)} \overbrace{\sum_{(q,s,l)\in\mathscr{G}(J)}}^{(\mathbb{Z}_{p^r})} a_{q,s,l} g_{(q,s,l)\to(p,r,m)} \tag{2.11}$$

for $a \in J$ where $g_{(q,s,l)\to(p,r,m)} = 0$ if $p \neq q$, $g_{(q,s,l)\to(p,r,m)}$ is a uniform random variable over $\mathbb{Z}_{p^r}$ if $p = q, r \leq s$, and $g_{(q,s,l)\to(p,r,m)}$ is a uniform random variable over $p^{r-s}\mathbb{Z}_{p^r}$ if $p = q, r \geq s$. The corresponding shifted group code is defined by

$$\mathbb{C} = \{\phi(a) + B | a \in J\} \tag{2.12}$$

where $B$ is a uniform random variable over $G^n$.

*Remark* II.3. An alternate approach to characterizing Abelian group codes is to consider kernels of homomorphisms (the kernel ensemble). To construct an ensemble of Abelian group codes in this manner, let $\phi$ be a homomorphism from $G^n$ into $J$ such that for $a \in G^n$,

$$\phi(a) = \bigoplus_{(q,s,l)\in\mathscr{G}(J)} \overbrace{\sum_{(p,r,m)\in\mathscr{G}(G^n)}}^{(\mathbb{Z}_{q^s})} a_{p,r,m} g_{(p,r,m)\to(q,s,l)}$$

where $g_{(p,r,m)\to(q,s,l)} = 0$ if $q \neq p$, $g_{(p,r,m)\to(q,s,l)}$ is a uniform random variable over $\mathbb{Z}_{q^s}$ if $q = p, s \leq r$, and $g_{(p,r,m)\to(q,s,l)}$ is a uniform random variable over $p^{s-r}\mathbb{Z}_{q^s}$ if $q = p, s \geq r$. The code is given by $\mathbb{C} = \{a \in G^n | \phi(a) = c\}$ where $c$ is a uniform random variable over $J$.

In this paper, we use the image ensemble for both the channel and the source coding problem; however, similar results can be derived using the kernel ensemble as well.

*Remark* II.4. For an Abelian group $G$, define

$$\mathscr{Q}(G) = \{(p, r) | p \in \mathscr{P}(G), r \in \mathscr{R}_p(G)\} \tag{2.13}$$

Consider the smaller ensemble of codes consisting of homomorphisms from Abelian groups $J$ of the form

$$J = \bigoplus_{(p,r)\in\mathscr{Q}(G)} \mathbb{Z}_{p^r}^{kw_{p,r}} \tag{2.14}$$

for some integer $k$ and some $w_{p,r}$'s adding up to one. The rate of a code in this ensemble is equal to

$$R = \frac{1}{n}\log|J| = \frac{k}{n}\sum_{(p,r)\in\mathscr{Q}(G)} r w_{p,r}\log p \tag{2.15}$$

It can be shown that the average performance of codes over this ensemble is equal to the average performance of the ensemble of all codes considered above. In the rest of this paper, we consider this simpler ensemble to prove the achievability results.

## 2.3 The Performance of Abelian Group Codes

In this section, we provide an upper bound on the rate-distortion function for a given source and a lower bound on the capacity of a given channel using group codes when the underlying group is an arbitrary Abelian group represented by Equation (2.3). We start by defining seven objects and then state two theorems using these objects, and finally provide an interpretation of the results and these objects with two examples.

### 2.3.1 Definitions

For an Abelian group $G$, define

$$\mathscr{Q}(G) = \{(p, r) | p \in \mathscr{P}(G), r \in \mathscr{R}_p(G)\} \tag{2.16}$$

We denote vectors $\hat{\theta}$, $w$ and $\theta$ whose components are indexed by $(p, r) \in \mathscr{Q}(G)$ by $(\hat{\theta}_{p,r})_{(p,r)\in\mathscr{Q}(G)}$, $(w_{p,r})_{(p,r)\in\mathscr{Q}(G)}$ and $(\theta_{p,r})_{(p,r)\in\mathscr{Q}(G)}$ respectively. For $\hat{\theta} = (\hat{\theta}_{p,r})_{(p,r)\in\mathscr{Q}(G)}$, define

$$\boldsymbol{\theta}(\hat{\theta}) = \left( \min_{\substack{(q,s)\in\mathscr{Q}(G) \\ q=p}} |r - s|^+ + \hat{\theta}_{q,s} \right)_{(p,r)\in\mathscr{Q}(G)}$$

Note that $\hat{\theta}$ and $\theta = \boldsymbol{\theta}(\hat{\theta})$ correspond to unique subgroups $H_{\hat{\theta}}$ and $H_\theta$ of $J$ and $G$ respectively where

$$H_{\hat{\theta}} = \bigoplus_{(p,r)\in\mathscr{Q}(G)} p^{\hat{\theta}_{p,r}} \mathbb{Z}_{p^r}^{kw_{p,r}} \leq J$$

$$H_\theta = \bigoplus_{(p,r,m)\in\mathscr{G}(G)} p^{\theta_{p,r}} \mathbb{Z}_{p^r}^{(m)} \leq G$$

To give some intuition about the function $\boldsymbol{\theta}(\cdot)$, we state that for any homomorphism $\phi : J \to G^n$, we have $\phi(H_{\hat{\theta}}) \leq H_\theta$ and for some homomorphism $\phi : J \to G^n$, we have $\phi(H_{\hat{\theta}}) = H_\theta$. Let

$$\Theta = \left\{ \boldsymbol{\theta}(\hat{\theta}) \,\middle|\, (\hat{\theta}_{q,s})_{(q,s)\in\mathscr{Q}(G)} : 0 \leq \hat{\theta}_{q,s} \leq s \right\} \tag{2.17}$$

This set corresponds to a collection of subgroups of $G$ which appear in the rate-distortion function. In other words only certain subgroups of the underlying group rather than all of them become important in the rate-distortion function. This will be clarified in the proof of the theorem. For $\theta \in \Theta$, define

$$\omega_\theta = \frac{\sum_{(p,r)\in\mathscr{Q}(G)} \theta_{p,r} w_{p,r} \log p}{\sum_{(p,r)\in\mathscr{Q}(G)} r w_{p,r} \log p} \tag{2.18}$$

Let $X$ and $U$ be jointly distributed random variables and let $[U]_\theta = U + H_\theta$ be a random variable taking values from the cosets of $H_\theta$ in $G$. We define *the source coding group mutual information* between $U$ and $X$ as

$$I^G_{s.c.}(U;X) = \min_{\substack{w_{p,r},(p,r)\in\mathscr{Q}(G) \\ \sum w_{p,r}=1}} \max_{\substack{\theta\in\Theta \\ \theta\neq\mathbf{0}}} \frac{1}{\omega_\theta} \left( \log \frac{|G|}{|H_\theta|} - H([U]_\theta|X) \right) \tag{2.19}$$

where $\mathbf{0}$ is a vector whose components are indexed by $(p,r) \in \mathscr{Q}(G)$ and whose $(p,r)^{\text{th}}$ component is equal to 0.

Let $X$ and $Y$ be jointly distributed random variables and let $[X]_\theta = X + H_\theta$ be a random variable taking values from the cosets of $H_\theta$ in $G$. We define *the channel coding group mutual information* between $X$ and $Y$ as

$$I^G_{c.c.}(X;Y) = \max_{\substack{w_{p,r},(p,r)\in\mathscr{Q}(G) \\ \sum w_{p,r}=1}} \min_{\substack{\theta\in\Theta \\ \theta\neq\boldsymbol{r}}} \frac{1}{1-\omega_\theta} \Big( \log |H_\theta| - H(X|Y[X]_\theta) \Big) \tag{2.20}$$

where $\boldsymbol{r}$ is a vector whose components are indexed by $(p,r) \in \mathscr{Q}(G)$ and whose $(p,r)^{\text{th}}$ component is equal to $r$.

### 2.3.2 Main Results

The following theorem provides an upper bound on the rate-distortion function achievable using group codes..

**Theorem II.5.** *For a source $(\mathscr{X}, \mathscr{U} = G, p_X, d)$ and a given distortion level $D$, let $p_{XU}$ be a joint distribution over $\mathscr{X} \times \mathscr{U}$ such that its first marginal is equal to the source distribution $p_X$, its second marginal $p_U$ is uniform over $\mathscr{U} = G$ and such that $\mathbb{E}\{d(X,U)\} \leq D$. Then the rate-distortion pair $(R, D)$ is achievable using group codes where $R = I^G_{s.c.}(U;X)$.*

*Proof.* The proof is provided in Section 2.4.2. □

When the underlying group is a $\mathbb{Z}_{p^r}$ ring, this result can be simplified. We state this result in the form of a corollary:

**Corollary II.6.** Let $X$, $U$ be jointly distributed random variables such that $U$ is uniform over $\mathscr{U} = G = \mathbb{Z}_{p^r}$ for some prime $p$ and positive integer $r$. For $\theta = 1, 2, \cdots, r$, let $H_\theta$ be a subgroup of $\mathbb{Z}_{p^r}$ defined by $H_\theta = p^\theta \mathbb{Z}_{p^r}$ and let $[U]_\theta = U + H_\theta$. Then,

$$I^G_{s.c.}(U;X) = \max_{\theta=1}^{r} \frac{r}{\theta} I([U]_\theta; X)$$

*Proof.* Immediate from the theorem. □

The following theorem is the dual channel coding result to Theorem II.5.

**Theorem II.7.** *For a channel $(\mathscr{X} = G, \mathscr{Y}, W_{Y|X})$, the rate $R = I^G_{c.c.}(X;Y)$ is achievable using group codes over $G$.*

*Proof.* The proof is provided in Section 2.5.2. □

When the underlying group is a $\mathbb{Z}_{p^r}$ ring, this result can be simplified. We state this result in the form of a corollary:

**Corollary II.8.** Let $X$, $Y$ be jointly distributed random variables such that $X$ is uniform over $\mathscr{X} = G = \mathbb{Z}_{p^r}$ for some prime $p$ and a positive integer $r$. For $\theta =$

$0, 1, \cdots, r-1$, let $H_\theta$ be a subgroup of $\mathbb{Z}_{p^r}$ defined by $H_\theta = p^\theta \mathbb{Z}_{p^r}$ and let $[X]_\theta = X + H_\theta$. Then,

$$I^G_{c.c.}(X;Y) = \max_{\theta=0}^{r-1} \frac{r}{r-\theta} I(X;Y|[X]_\theta)$$

*Proof.* Immediate from the theorem. □

When dealing with group codes for the purpose of channel coding, an important case is when the channel exhibits some sort of symmetry. The capacity of group codes for channels with some notion of symmetry is found in [18]. The next corollary states that the result of this paper simplifies to the result of [18] when the channel is symmetric in the sense defined in [18].

**Corollary II.9.** When the channel $(\mathscr{X} = G, \mathscr{Y}, W_{Y|X})$ is $G$-symmetric in the sense defined in [18], i.e. if

1. $G$ acts simply transitively on $\mathscr{X}$ (trivially holds for this case)
2. $G$ acts isometrically on $\mathscr{Y}$
3. For all $x, g \in G, y \in \mathscr{Y}$, $W(y|x) = W(g \cdot y|g + x)$

then $I^G_{c.c}(X;Y)$ is equal to the rate provided in [18, Equation (33)].

*Proof.* The proof is provided in Section 2.5.3. □

### 2.3.3 Interpretation of the Results

In this section, we try to give some intuition about the result and the quantities defined above using several examples. At a high level, $w_{p,r}$ denotes the normalized weight given to the $\mathbb{Z}_{p^r}$ component of the input group $J$ in constructing the homomorphism from $J$ to $G^n$, and $\theta$ indexes a subgroup $H_\theta$ of $G$ that comes from a set $\Theta$. $\frac{1}{\omega_\theta} I([U]_\theta; X)$ in source coding and $\frac{1}{(1-\omega_\theta)} I(X;Y|[X]_\theta)$ in channel coding denote the rate constraints imposed by the subgroup $H_\theta$. Due to the algebraic structure

of the code in the ensemble, two random codewords corresponding to two distinct indexes are statistically dependent, unless $G$ is a finite field. For the source coding problem, when the code is chosen randomly, consider the event that all components of their difference belong to a proper subgroup $H_\theta$ of $G$. Then if one of them is a poor representation of a given source sequence, so is the other with a probability that is higher than the case when no algebraic structure on the code is enforced. This means that the code size has to be larger so that with high probability one can find a good representation of the source. For the channel coding problem, when a random codeword corresponding to a given message index is transmitted over the channel, consider the event that all components of the difference between the codeword transmitted and a random codeword corresponding to another message index belong to a proper subgroup $H_\theta$ of $G$. Then the probability that the latter is decoded instead of the former is higher than the case when no algebraic structure on the code is enforced.

**Example:** We start with the simple example where $G = \mathbb{Z}_8$. In this case, we have $\mathscr{P}(G) = \{2\}$ and $\mathscr{Q}(G) = \{(2,3)\}$. For vectors $w$, $\hat{\theta}$ and $\theta$ defined as above, we have $w = w_{2,3} = 1$, $\hat{\theta} = \hat{\theta}_{2,3}$ and $\theta = \theta_{2,3}$. Recall that the ensemble of Abelian group codes used in the random coding argument consists of the set of all homomorphisms from some $J = \mathbb{Z}_8^{kw_{2,3}} = \mathbb{Z}_8^k$. Any $\hat{\theta} = \hat{\theta}_{2,3}$ with $0 \leq \hat{\theta}_{2,3} \leq 3$ corresponds to a subgroup $K_{\hat{\theta}}$ of the input group $J$ given by

$$K_{\hat{\theta}} = 2^{\hat{\theta}_{2,3}}\mathbb{Z}_8^k$$

Similarly, any $\theta = \theta_{2,3}$ with $0 \leq \theta_{2,3} \leq 3$ corresponds to a subgroup $H_\theta$ of the group space $G^n$ given by

$$H_\theta = 2^{\theta_{2,3}}\mathbb{Z}_8^n$$

In this case, it turns out that if

$$\theta = \boldsymbol{\theta}(\hat{\theta}) = \hat{\theta}_{2,3} = \hat{\theta} \tag{2.21}$$

then for any random homomorphism $\phi$ from $J$ into $G^n$, and for any $a \in J$ with $a \in 2^{\hat{\theta}_{2,3}}\mathbb{Z}_8^k \backslash 2^{\hat{\theta}_{2,3}+1}\mathbb{Z}_8^k$, $\phi(a)$ is uniformly distributed over $H_\theta^n$. The set $\Theta$ consists of all vectors $\theta$ for which there exists at least one such $a$. Note that this set corresponds to a collection of subgroups of $G^n$. The quantity $1-\omega_\theta$ is a measure of the number of elements $a$ of $J$ for which $\phi(a)$ is uniform over $H_\theta$. It turns out that for this example, $\Theta = \{0, 1, 2, 3\}$ and $\omega_0 = 0$, $\omega_1 = \frac{1}{3}$, $\omega_2 = \frac{2}{3}$ and $\omega_3 = 1$.

**Example:** Next, we consider the case where $G = \mathbb{Z}_4 \oplus \mathbb{Z}_3$. In this case, we have $\mathscr{P}(G) = \{2, 3\}$ and $\mathscr{Q}(G) = \{(2, 2), (3, 1)\}$. For vectors $w$, $\hat{\theta}$ and $\theta$ defined as before, we have $w = (w_{2,2}, w_{3,1})$, $\hat{\theta} = (\hat{\theta}_{2,2}, \hat{\theta}_{3,1})$ and $\theta = (\theta_{2,2}, \theta_{3,1})$. The ensemble of Abelian group codes consists of the set of all homomorphisms from some $J = \mathbb{Z}_4^{kw_{2,2}} \oplus \mathbb{Z}_3^{kw_{3,1}}$. Any vector $\hat{\theta} = (\hat{\theta}_{2,2}, \hat{\theta}_{3,1})$ with $0 \leq \hat{\theta}_{2,2} \leq 2$ and $0 \leq \hat{\theta}_{3,1} \leq 1$ corresponds to a subgroup $K_{\hat{\theta}}$ of the input group $J$ given by

$$K_{\hat{\theta}} = 2^{\hat{\theta}_{2,2}}\mathbb{Z}_4^{kw_{2,2}} \oplus 3^{\hat{\theta}_{3,1}}\mathbb{Z}_8^{kw_{3,1}}$$

Similarly, any $\theta = (\theta_{2,2}, \theta_{3,1})$ with $0 \leq \theta_{2,2} \leq 2$ and $0 \leq \theta_{3,1} \leq 1$ corresponds to a subgroup $H_\theta$ of the group space $G^n$ given by

$$H_\theta = 2^{\theta_{2,2}}\mathbb{Z}_4^n \oplus 3^{\theta_{3,1}}\mathbb{Z}_3^n$$

It turns out that if

$$\theta_{2,2} = \hat{\theta}_{2,2} \tag{2.22}$$

$$\theta_{3,1} = \hat{\theta}_{3,1} \tag{2.23}$$

then for any random homomorphism $\phi$ from $J$ into $G^n$, and for any $a = (\beta, \gamma) \in J$ with $\beta \in 2^{\hat{\theta}_{2,2}}\mathbb{Z}_4^{kw_{2,2}} \backslash 2^{\hat{\theta}_{2,2}+1}\mathbb{Z}_4^{kw_{2,2}}$ and $\gamma \in 3^{\hat{\theta}_{3,1}}\mathbb{Z}_3^{kw_{3,1}} \backslash 3^{\hat{\theta}_{3,1}+1}\mathbb{Z}_3^{kw_{3,1}}$, $\phi(a)$ is uniformly distributed over $H_\theta^n$. Moreover, for this example we have

$$\Theta = \{(0, 0), (1, 0), (2, 0), (0, 1), (1, 1), (2, 1)\}$$

## 2.4 Proof for the Source Coding Problem

### 2.4.1 The Coding Scheme

Following the analysis of Section 2.2.2, we construct the ensemble of group codes of length $n$ over $G$ as the image of all homomorphisms $\phi$ from some Abelian group $J$ into $G^n$ where $J$ and $G^n$ are as in Equations (2.10) and (2.8) respectively. The random homomorphism $\phi$ is described in Equation (2.11).

To find an achievable rate for a distortion level $D$, we use a random coding argument in which the random encoder is characterized by the random homomorphism $\phi$, a random vector $B$ uniformly distributed over $G^n$ and a joint distribution $p_{XU}$ over $\mathscr{X} \times \mathscr{U}$ such that its first marginal is equal to the source distribution $p_X$, its second marginal $p_U$ is uniform over $\mathscr{U} = G$ and such that $\mathbb{E}\{d(X,U)\} \leq D$. The code is defined as in (2.12) and its rate is given by (2.15).

Given the source output sequence $x \in \mathscr{X}^n$, the random encoder looks for a codeword $u \in \mathbb{C}$ such that $u$ is jointly typical with $x$ with respect to $p_{XU}$. If it finds at least one such $u$, it encodes $x$ to $u$ (if it finds more than one such $u$ it picks one of them at random). Otherwise, it declares error. The decoder outputs $u$ as the source reconstruction.

### 2.4.2 Error Analysis

Let $x = (x_1, \cdots, x_n)$ and $u = (u_1, \cdots, u_n)$ be the source output and the encoder/decoder output respectively. Note that if the encoder declares no error then since $x$ and $u$ are jointly typical, $(d(x_i, u_i))_{i=1,\cdots,n}$ is typical with respect to the distribution of $d(X,U)$. Therefore for large $n$, $\frac{1}{n}d(x,u) = \frac{1}{n}\sum_{i=1}^{n} d(x_i,u_i) \approx \mathbb{E}\{d(X,U)\} \leq D$. It remains to show that the rate can be as small as $I^G_{s.c.}(X;U)$ while keeping the probability of encoding error small.

Given the source output $x \in \mathscr{X}^n$, define

$$\alpha(x) = \sum_{u \in A_\epsilon^n(U|x)} \mathbb{1}_{\{u \in \mathbb{C}\}} = \sum_{u \in A_\epsilon^n(U|x)} \sum_{a \in J} \mathbb{1}_{\{\phi(a)+B=u\}}$$

An encoding error occurs if and only if $\alpha(x) = 0$. We use the following Chebyshev's inequality to show that under certain conditions the probability of error can be made arbitrarily small:

$$P\left(\alpha(x) = 0\right) \leq \frac{\text{var}\{\alpha(x)\}}{\mathbb{E}\{\alpha(x)\}^2}$$

We need the following lemmas to proceed:

**Lemma II.10.** *For $a, \tilde{a} \in J$, $u, \tilde{u} \in G^n$ and for $(q, s, l) \in \mathscr{G}(J)$, let $\hat{\theta}_{q,s,l} \in \{0, 1, \cdots, s\}$ be such that*

$$\tilde{a}_{q,s,l} - a_{q,s,l} \in q^{\hat{\theta}_{q,s,l}} \mathbb{Z}_{q^s} \backslash q^{\hat{\theta}_{q,s,l}+1} \mathbb{Z}_{q^s}$$

*For $(p, r) \in \mathscr{Q}(G)$ define*

$$\boldsymbol{\theta}_{p,r}(a, \tilde{a}) = \min_{\substack{(q,s,l) \in \mathscr{G}(J) \\ q=p}} |r - s|^+ + \hat{\theta}_{q,s,l}$$

*and let $\theta_{p,r} = \boldsymbol{\theta}_{p,r}(a, \tilde{a})$. Define the subgroup $H_\theta$ of $G$ as*

$$H_\theta = \bigoplus_{(p,r,m) \in \mathscr{G}(G)} p^{\theta_{p,r}} \mathbb{Z}_{p^r}^{(m)}$$

*Then,*

$$P\left(\phi(a) + B = u, \phi(\tilde{a}) + B = \tilde{u}\right) = \begin{cases} \frac{1}{|G|^n} \frac{1}{|H_\theta|^n} & \text{If } \tilde{u} - u \in H_\theta^n \\ 0 & \text{Otherwise} \end{cases}$$

*Proof.* The proof is provided in Appendix 2.7.0.2 □

**Lemma II.11.** *For $a \in J$ and $\theta = (\theta_{p,r})_{(p,r) \in \mathscr{Q}(G)}$, let*

$$T_\theta(a) = \{\tilde{a} \in J | \forall (p, r) \in \mathscr{Q}(G), \boldsymbol{\theta}_{p,r}(a, \tilde{a}) = \theta_{p,r}\}$$

*where $\boldsymbol{\theta}_{p,r}(a,\tilde{a})$ is defined as in the previous lemma. Then we have*

$$|T_\theta(a)| \leq \prod_{(p,r)\in\mathscr{Q}(G)} p^{(r-\theta_{p,r})kw_{p,r}} = 2^{nR(1-\omega_\theta)}$$

*In particular, $|T_\theta(a)|$ does not depend on $a$. We denote this by $|T_\theta| = |T_\theta(a)|$.*

*Proof.* The proof is provided in Appendix 2.7.0.3 □

**Lemma II.12.** *For $a \in J$ and $u \in G^n$, we have*

$$P\left(\phi(a) + B = u\right) = \frac{1}{|G|^n}$$

*Proof.* Immediate from Lemma II.10. □

We have

$$\begin{aligned}\mathbb{E}\{\alpha(x)\} &= \sum_{u\in A_\epsilon^n(U|x)} \sum_{a\in J} P\left(\phi(a) + B = u\right) \\ &= \frac{|A_\epsilon^n(U|x)| \cdot |J|}{|G|^n}\end{aligned}$$

and

$$\begin{aligned}\mathbb{E}\{\alpha(x)^2\} &= \mathbb{E}\left\{\sum_{u,\tilde{u}\in A_\epsilon^n(U|x)} \sum_{a,\tilde{a}\in J} \mathbb{1}_{\{\phi(a)+B=u,\phi(\tilde{a})+B=\tilde{u}\}}\right\} \\ &= \sum_{u,\tilde{u}\in A_\epsilon^n(U|x)} \sum_{a,\tilde{a}\in J} P\left(\{\phi(a)+B=u,\phi(\tilde{a})+B=\tilde{u}\}\right) \\ &= \sum_{\theta\in\Theta}\sum_{a\in J}\sum_{u\in A_\epsilon^n(U|x)}\sum_{\tilde{a}\in T_\theta(a)}\sum_{\substack{\tilde{u}\in A_\epsilon^n(U|x)\\ \tilde{u}-u\in H_\theta^n}} \frac{1}{|G|^n}\cdot\frac{1}{|H_\theta|^n}\end{aligned}$$

Note that the term corresponding to $\theta = \mathbf{0}$ is upper bounded by $\mathbb{E}\{\alpha(x)\}^2$. Using Lemma II.14, we have

$$|A_\epsilon^n(U|x) \cap (u + H_\theta^n)| \leq 2^{n[H(U|[U]_\theta X)+O(\epsilon)]}$$

Therefore,

$$\begin{aligned}\mathrm{var}\{\alpha\} &= \mathbb{E}\{\alpha(x)^2\} - \mathbb{E}\{\alpha(x)\}^2 \\ &\leq \sum_{\substack{\theta\in\Theta\\ \theta\neq\mathbf{0}}} |J| \cdot |A_\epsilon^n(U|x)| \cdot |T_\theta| \cdot \frac{2^{n[H(U|[U]_\theta X)+O(\epsilon)]}}{|G|^n \cdot |H_\theta|^n}\end{aligned}$$

Therefore,

$$P\left(\alpha(x)=0\right) \leq \frac{\mathrm{var}\{\alpha(x)\}}{\mathbb{E}\{\alpha(x)\}^2}$$
$$\leq \sum_{\substack{\theta\in\Theta \\ \theta\neq\mathbf{0}}} \frac{2^{nR(1-\omega_\theta)} \cdot 2^{-n[H(U|X)-H(U|[U]_\theta X)-O(\epsilon)]} \cdot |G|^n}{|J| \cdot |H_\theta|^n}$$

Note that $H(U|X) - H(U|[U]_\theta X) = H([U]_\theta|X)$ and $|J| = 2^{nR}$; therefore,

$$P\left(\alpha(x)=0\right) \leq$$
$$\sum_{\substack{\theta\in\Theta \\ \theta\neq\mathbf{0}}} \exp_2\Big\{ -n\Big[H([U]_\theta|X) - \log|G:H_\theta| + \omega_\theta R - O(\epsilon)\Big]\Big\}$$

In order for the probability of error to go to zero as $n$ increases, we require the exponent of all the terms to be negative; or equivalently,

$$R > \frac{1}{\omega_\theta}\Big(\log|G:H_\theta| - H([U]_\theta|X)\Big)$$

with the convention $\frac{1}{0}=\infty$. Therefore, the achievable rate is equal to

$$R = \min_{\substack{w_{p,r},(p,r)\in\mathscr{Q}(G) \\ \sum w_{p,r}=1}} \max_{\substack{\theta\in\Theta \\ \theta\neq\mathbf{0}}} \frac{1}{\omega_\theta}\Big(\log|G:H_\theta| - H([U]_\theta|X)\Big)$$

## 2.5 Proof for the Channel Coding Problem

### 2.5.1 The Coding Scheme

Following the analysis of Section 2.2.2, we construct the ensemble of group codes of length $n$ over $G$ as the image of all homomorphisms $\phi$ from some Abelian group $J$ into $G^n$ where $J$ and $G^n$ are as in Equations (2.10) and (2.8) respectively. The random homomorphism $\phi$ is described in Equation (2.11).

To find an achievable rate, we use a random coding argument in which the random encoder is characterized by the random homomorphism $\phi$ and a random vector $B$ uniformly distributed over $G^n$. Given a message $u \in J$, the encoder maps it to $x = \phi(u) + B$ and $x$ is then fed to the channel. At the receiver, after receiving the

channel output $y \in \mathscr{Y}^n$, the decoder looks for a unique $\tilde{u} \in J$ such that $\phi(\tilde{u}) + B$ is jointly typical with $y$ with respect to the distribution $p_X W_{Y|X}$ where $p_X$ is uniform over $G$. If the decoder does not find such $\tilde{u}$ or if such $\tilde{u}$ is not unique, it declares error.

### 2.5.2 Error Analysis

Let $u$, $x$ and $y$ be the message, the channel input and the channel output respectively. The error event can be characterized by the union of two events: $E(u) = E_1(u) \cup E_2(u)$ where $E_1(u)$ is the event that $\phi(u) + B$ is not jointly typical with $y$ and $E_2(u)$ is the event that there exists a $\tilde{u} \neq u$ such that $\phi(\tilde{u}) + B$ is jointly typical with $y$. We can provide an upper bound on the probability of the error event as $P(E(u)) \leq P(E_1(u)) + P(E_2(u) \cap (E_1(u))^c)$. Using the standard approach, one can show that $P\left(E_1(u)\right) \to 0$ as $n \to \infty$. The probability of the error event $E_2(u) \cap (E_1(u))^c$ averaged over all messages can be written as

$$P_{avg}(E_2(u) \cap (E_1(u))^c) = \sum_{u \in J} \frac{1}{|J|} \sum_{x \in G^n} \mathbb{1}_{\{\phi(u)+B=x\}} \sum_{y \in A_\epsilon^n(Y|x)} W_{Y|X}^n(y|x) \mathbb{1}_{\{\exists \tilde{u} \in J : \tilde{u} \neq u, \phi(\tilde{u})+B \in A_\epsilon^n(X|y)\}}$$

The expected value of this probability over the ensemble is given by $\mathbb{E}\{P_{avg}(E_2(u) \cap (E_1(u))^c)\} = P_{err}$ where

$$P_{err} = \sum_{u \in J} \frac{1}{|J|} \sum_{x \in G^n} \sum_{y \in A_\epsilon^n(Y|x)} W_{Y|X}^n(y|x) P\left(\phi(u) + B = x, \exists \tilde{u} \in J : \tilde{u} \neq u, \phi(\tilde{u}) + B \in A_\epsilon^n(X|y)\right)$$

Using the union bound, we have

$$P_{err} \leq \sum_{u \in J} \frac{1}{|J|} \sum_{x \in G^n} \sum_{y \in A_\epsilon^n(Y|x)} \sum_{\substack{\tilde{u} \in J \\ \tilde{u} \neq u}} \sum_{\tilde{x} \in A_\epsilon^n(X|y)} W_{Y|X}^n(y|x) P\left(\phi(u) + B = x, \phi(\tilde{u}) + B = \tilde{x}\right)$$

Define $\Theta$ as in Equation (2.17) and for $\theta \in \Theta$ and $u \in J$, define $T_\theta(u)$ as in Lemma II.11. It follows that

$$P_{err} \leq \sum_{u \in J} \frac{1}{|J|} \sum_{x \in G^n} \sum_{y \in A_\epsilon^n(Y|x)} \sum_{\substack{\theta \in \Theta \\ \theta \neq \boldsymbol{r}}} \sum_{\tilde{u} \in T_\theta(u)} \sum_{\tilde{x} \in A_\epsilon^n(X|y)} W_{Y|X}^n(y|x) P\left(\phi(u) + B = x, \phi(\tilde{u}) + B = \tilde{x}\right)$$

Using Lemmas II.10, II.14 and II.11, we have

$$\begin{aligned}
P_{err} &\leq \sum_{\substack{\theta\in\Theta\\ \theta\neq \boldsymbol{r}}} \sum_{u\in J} \frac{1}{|J|} \sum_{x\in G^n} \sum_{y\in A_\epsilon^n(Y|x)} \sum_{\tilde{u}\in T_\theta(u)} \sum_{\substack{\tilde{x}\in A_\epsilon^n(X|y)\\ \tilde{x}\in x+H_{\theta^n}}} W_{Y|X}^n(y|x) \frac{1}{|G|^n} \frac{1}{|H_\theta|^n} \\
&\leq \sum_{\substack{\theta\in\Theta\\ \theta\neq \boldsymbol{r}}} \sum_{u\in J} \frac{1}{|J|} \sum_{x\in G^n} \sum_{y\in A_\epsilon^n(Y|x)} \sum_{\tilde{u}\in T_\theta(u)} W_{Y|X}^n(y|x) 2^{n[H(X|Y[X]_\theta)+O(\epsilon)]} \frac{1}{|G|^n} \frac{1}{|H_\theta|^n} \\
&\leq \sum_{\substack{\theta\in\Theta\\ \theta\neq \boldsymbol{r}}} \frac{|T_\theta| \cdot 2^{n[H(X|Y[X]_\theta)+O(\epsilon)]}}{|H_\theta|^n}
\end{aligned}$$

Equivalently, this can be written as

$$P_{err} \leq \sum_{\substack{\theta\in\Theta\\ \theta\neq \boldsymbol{r}}} \exp_2 \Big\{ -n \Big[ -(1-\omega_\theta)R - H(X|Y[X]_\theta) + \log|H_\theta| - O(\epsilon) \Big] \Big\}$$

Therefore, the achievability condition is

$$R = \min_{\substack{\theta\in\Theta\\ \theta\neq \boldsymbol{r}}} \frac{1}{1-\omega_\theta} \Big( \log|H_\theta| - H(X|Y[X]_\theta) \Big)$$

If we maximize over the choice of $w$, we can conclude that the rate $R = I_{c.c}^G(X;Y)$ is achievable.

### 2.5.3 Simplification of the Result for Symmetric Channels

In this section, we provide a proof of corollary II.9. Note that since we take $\mathscr{X} = G$, we can take the action of $G$ on $\mathscr{X}$ to be the group operation. We need to show that for all subgroups $H$ of $G$, $I(X;Y|[X]) = C_H$ where $X = X + H$ and $C_H$ is the mutual information between the channel input and the channel output when the input is uniformly distributed over $H$; in other words, $C_H = I(X;Y|[X] = H)$. This in turn follows by showing that for all $g \in G$

$$I(X;Y|[X] = g + H) = I(X;Y|[X] = H)$$

This can be shown as follows:

$$\begin{aligned} I(X;Y|[X]=g+H) &= \sum_{x\in g+H}\sum_{y\in\mathscr{Y}}\frac{1}{|H|}W(y|x)\log\frac{W(y|x)}{P(y)} \\ &= \sum_{\tilde{x}\in H}\sum_{y\in\mathscr{Y}}\frac{1}{|H|}W(y|\tilde{x}+g)\log\frac{W(y|\tilde{x}+g)}{P(y)} \\ &\overset{(a)}{=} \sum_{\tilde{x}\in H}\sum_{y\in\mathscr{Y}}\frac{1}{|H|}W(g\cdot y|\tilde{x}+g)\log\frac{W(g\cdot y|\tilde{x}+g)}{P(y)} \\ &\overset{(b)}{=} \sum_{\tilde{x}\in H}\sum_{y\in\mathscr{Y}}\frac{1}{|H|}W(y|\tilde{x})\log\frac{W(y|\tilde{x})}{P(y)} \\ &= I(X;Y|[X]=H) \end{aligned}$$

where $(a)$ follows since the action of $g$ on $\mathscr{Y}$ is a bijection of $\mathscr{Y}$ and $(b)$ follows from the symmetric property of the channel. Using this result, it can be shown that the rate provided in [18, Equation (33)] is equal to $I^G_{c.c.}(X;Y)$. The difference in the appearance of the two expressions is due to the fact that in [18, Equation (33)] the minimization is carried out over the subgroups of the input group whereas in the expression for $I^G_{c.c.}(X;Y)$ the minimization is carried out over the resulting subgroups of the output group.

## 2.6 Examples

In this section, we provide a few examples for both the source coding problem as well as the channel coding problem. We show that when the underlying group is a field, the source coding group mutual information and the channel coding group mutual information are both equal to the Shannon mutual information. We also provide several non-field examples for both problems.

### 2.6.1 Examples for Source Coding

In this section, we find the rate-distortion region for a few examples. First, we consider the case where the underlying group is a field i.e. when $G = \mathbb{Z}_p^m$ for some

prime $p$ and positive integer $m$. In this case, we have $\mathscr{P}(G) = \{p\}$, $\mathscr{R}_p(G) = \{1\}$, $M_{p,1} = m$ and $\mathscr{Q}(G) = \{(p, 1)\}$. Since the set $\mathscr{Q}(G)$ is a singleton, the only choice for the weights is $w = w_{p,1} = 1$ and

$$\Theta = \{0, 1\}$$

For $\theta = 1$, we have $w_\theta = 0$ and $[U]_\theta = U$. Therefore,

$$I_{s.c.}^G = I(U; X)$$

This means when the underlying group is a field, the rate is equal to the regular mutual information between $U$ and $X$ when $U$ is a uniform random variable.

Next, we consider the case where the reconstruction alphabet is $\mathbb{Z}_4$. In this case, we have $p = 2$ and $r = 2$. Therefore,

$$\begin{aligned} R &= \max_{\theta=1}^{2} \frac{2}{\theta} I([U]_\theta; X) \\ &= \max(2I([U]_1; X), I(U; X)) \end{aligned}$$

where $U$ is uniform over $\mathbb{Z}_4$, $X$ is the source output and $[U]_1 = U + 2^1\mathbb{Z}_4 = X + \{0, 2\}$ and the joint distribution is such that $\mathbb{E}\{d(U, X)\} \leq D$. Therefore,

$$2I([U]_1; X) = I(U + \{0, 2\}; X) + I(U + \{1, 3\}; X)$$

Hence,

$$R = \max\left(I(U; X), I(U + \{0, 2\}; X) + I(U + \{1, 3\}; X)\right)$$

Next, we consider the case where the reconstruction alphabet is $\mathbb{Z}_8$. For this source, we have $p = 2$ and $r = 3$. Following a similar argument as above we have:

$$R = \max\left(I(U; X), \frac{3}{2} I([U]_2; X), 3I([U]_1; X)\right)$$

where $U$ is uniform over $\mathbb{Z}_8$, $X$ is the source output, $[U]_1 = U + \{0, 2, 4, 6\}$ and $[U]_2 = U + \{0, 4\}$.

Similarly, for channels with input $\mathbb{Z}_9$, we have $p = 3$, $r = 2$ and

$$R = \max\left(I(U;X), 2I([U]_1;X)\right)$$

where $U$ is uniform over $\mathbb{Z}_9$, $X$ is the source output and $[U]_1 = U + \{0,3,6\}$.

Finally, we consider $G = \mathbb{Z}_2 \times \mathbb{Z}_4$. In this case, $\mathscr{P}(G) = \{2\}$, $\mathscr{R}_2(G) = \{1,2\}$, $\mathscr{Q}(G) = \{(2,1),(2,2)\}$, $\mathbf{0} = (0,0)$ and $w = (w_1, w_2)$ such that $w_1 + w_2 = 1$. We have $\Theta = \{(0,0),(0,1),(1,1),(1,2)\}$. For $\theta = (0,1)$ we have $\omega_\theta = \frac{w_1+w_2}{w_1+2w_2} = \frac{1}{1+w_2}$, for $\theta = (1,1)$ we have $\omega_\theta = \frac{w_2}{1+w_2}$, and for $\theta = (1,2)$ we have $\omega_\theta = 0$; therefore,

$$\begin{aligned} R &= \min_{w_1,w_2} \max\left((1+w_2)I([U]_{\theta=(0,1)};X), \frac{1+w_2}{w_2}I([U]_{\theta=(1,1)};X), I([U]_{\theta=(1,2)};X)\right) \\ &= \min_{w_1,w_2} \max\left((1+w_2)I([U]_{\theta=(0,1)};X), \frac{1+w_2}{w_2}I([U]_{\theta=(1,1)};X), I(U;X)\right) \end{aligned}$$

The minimum of $R$ is achieved when

$$(1+w_2)I([U]_{\theta=(0,1)};X) = \frac{1+w_2}{w_2}I([U]_{\theta=(1,1)};X)$$

or equivalently

$$w_2 = \frac{I([U]_{\theta=(1,1)};X)}{I([U]_{\theta=(0,1)};X)}$$

Therefore,

$$R = \max\left(I([U]_{\theta=(1,1)};X) + I([U]_{\theta=(0,1)};X), I(X;Y)\right)$$

### 2.6.2 Examples for Channel Coding

In this section, we find the achievable rate for a few examples: First, we consider the case where the underlying group is a field i.e. when $G = \mathbb{Z}_p^m$ for some prime $p$ and positive integer $m$. As in the source coding case, the only choice for the weights is $w = w_{p,1} = 1$ and $\Theta = \{0,1\}$. For $\theta = 0$, we have $w_\theta = 1$ and $[U]_\theta$ is a trivial random variable. Hence

$$I_{s.c.}^G = I(U;X)$$

This means when the underlying group is a field, the rate is equal to the regular mutual information between $U$ and $X$ when $U$ is a uniform random variable.

Next, we consider the case where the channel input alphabet is $\mathbb{Z}_4$. In this case, we have $p = 2$ and $r = 2$. Therefore,

$$\begin{aligned} R &= \min_{\theta=0}^{1} \frac{2}{2-\theta} I(X;Y|[X]_\theta) \\ &= \min(I(X;Y), 2I(X;Y|[X]_1)) \end{aligned}$$

where the channel input $X$ is uniform over $\mathbb{Z}_4$, $Y$ is the channel output and $[X]_1 = X + 2^1\mathbb{Z}_4 = X + \{0,2\}$. Therefore,

$$2I(X;Y|[X]_1) = I(X;Y|X \in \{0,2\}) + I(X;Y|X \in \{1,3\})$$

Hence,

$$R = \min\left(I(X;Y), I(X;Y|X \in \{0,2\}) + I(X;Y|X \in \{1,3\})\right)$$

Next, we consider a channel of input alphabet $\mathbb{Z}_8$. For this channel we have $p = 2$ and $r = 3$. Following a similar argument as above we have:

$$R = \min\left(I(X;Y), \frac{3}{2} I(X;Y|[X]_1), 3I(X;Y|[X]_2)\right)$$

where the channel input $X$ is uniform over $\mathbb{Z}_8$, $Y$ is the channel output, $[X]_1 = X + \{0,2,4,6\}$ and $[X]_2 = X + \{0,4\}$.

Similarly, for channels with input $\mathbb{Z}_9$, we have $p = 3$, $r = 2$ and

$$R = \min\left(I(X;Y), 2I(X;Y|[X]_1)\right)$$

where the channel input $X$ is uniform over $\mathbb{Z}_9$, $Y$ is the channel output and $[X]_1 = X + \{0,3,6\}$.

Finally, we consider $G = \mathbb{Z}_2 \times \mathbb{Z}_4$. In this case, $\mathscr{P}(G) = \{2\}$, $\mathscr{R}_2(G) = \{1,2\}$, $\mathscr{Q}(G) = \{(2,1),(2,2)\}$, $\boldsymbol{r} = (1,2)$ and $w = (w_1, w_2)$ such that $w_1 + w_2 = 1$. We have

$\Theta = \{(0,0),(0,1),(1,1),(1,2)\}$. For $\theta = (0,0)$ we have $\omega_\theta = 1$, for $\theta = (0,1)$ we have $\omega_\theta = \frac{w_1+w_2}{w_1+2w_2} = \frac{1}{1+w_2}$ and for $\theta = (1,1)$ we have $\omega_\theta = \frac{w_2}{1+w_2}$ therefore,

$$\begin{aligned} R &= \max_{w_1,w_2} \min \left( \frac{1+w_2}{w_2} I(X;Y|[X]_{\theta=(1,1)}), (1+w_2) I(X;Y|[X]_{\theta=(0,1)}), I(X;Y|[X]_{\theta=(0,0)}) \right) \\ &= \max_{w_1,w_2} \min \left( \frac{1+w_2}{w_2} I(X;Y|[X]_{\theta=(1,1)}), (1+w_2) I(X;Y|[X]_{\theta=(0,1)}), I(X;Y) \right) \end{aligned}$$

The maximum of $R$ is achieved when

$$\frac{1+w_2}{w_2} I(X;Y|[X]_{\theta=(1,1)}) = (1+w_2) I(X;Y|[X]_{\theta=(0,1)}$$

or equivalently

$$w_2 = \frac{I(X;Y|[X]_{\theta=(1,1)})}{I(X;Y|[X]_{\theta=(0,1)})}$$

Therefore,

$$R = \min \left( I(X;Y|[X]_{\theta=(1,1)}) + I(X;Y|[X]_{\theta=(0,1)}), I(X;Y) \right)$$

## 2.7 Appendix

#### 2.7.0.1 Proof of Lemma II.2

We first prove that for a homomorphism $\phi$, $g_{(q,s,l)\to(p,r,m)}$ satisfies the above conditions. First assume $p \neq q$. Note that the only nonzero component of $\mathbb{I}_{J:q,s,l}$ takes values from $\mathbb{Z}_{q^s}$ and therefore

$$q^s \mathbb{I}_{J:q,s,l} = \overbrace{\sum_{i=1,\cdots,q^s}}^{(J)} \mathbb{I}_{J:q,s,l} = 0$$

Note that since $\phi$ is a homomorphism, we have $\phi(q^s\mathbb{I}_{J:q,s,l}) = 0$. On the other hand,

$$\begin{aligned}
\phi(q^s\mathbb{I}_{J:q,s,l}) &= \phi(\overbrace{\sum_{i=1,\cdots,q^s}}^{(J)} \mathbb{I}_{J:q,s,l}) \\
&= \overbrace{\sum_{i=1,\cdots,q^s}}^{(\tilde{G})} \phi(\mathbb{I}_{J:q,s,l}) \\
&= \bigoplus_{(p,r,m)\in\mathscr{G}(\tilde{G})} \left[ \overbrace{\sum_{i=1,\cdots,q^s}}^{(\tilde{G})} \phi(\mathbb{I}_{J:q,s,l}) \right]_{p,r,m} \\
&= \bigoplus_{(p,r,m)\in\mathscr{G}(\tilde{G})} \overbrace{\sum_{i=1,\cdots,q^s}}^{(\mathbb{Z}_{p^r})} \left[\phi(\mathbb{I}_{J:q,s,l})\right]_{p,r,m} \\
&= \bigoplus_{(p,r,m)\in\mathscr{G}(\tilde{G})} q^s \left[\phi(\mathbb{I}_{J:q,s,l})\right]_{p,r,m} \\
&= \bigoplus_{(p,r,m)\in\mathscr{G}(\tilde{G})} q^s g_{(q,s,l)\to(p,r,m)}
\end{aligned}$$

Therefore, we have $q^s g_{(q,s,l)\to(p,r,m)} = 0 \pmod{p^r}$ or equivalently $q^s g_{(q,s,l)\to(p,r,m)} = Cp^r$ for some integer $C$. Since $p \neq q$, this implies $p^r | g_{(q,s,l)\to(p,r,m)}$ and since $g_{(q,s,l)\to(p,r,m)}$ takes value from $\mathbb{Z}_{p^r}$, we have $g_{(q,s,l)\to(p,r,m)} = 0$.

Next, assume $p = q$ and $r \geq s$. Note that same as above, we have $\phi(q^s\mathbb{I}_{J:q,s,l}) = 0$ and

$$\phi(q^s\mathbb{I}_{J:q,s,l}) = \bigoplus_{(p,r,m)\in\mathscr{G}(\tilde{G})} q^s g_{(q,s,l)\to(p,r,m)}$$

and therefore, $q^s g_{(q,s,l)\to(p,r,m)} = 0 \pmod{p^r}$. Since $g_{(q,s,l)\to(p,r,m)}$ takes values from $\mathbb{Z}_{p^r}$ and $p = q$, this implies $p^{r-s} | g_{(q,s,l)\to(p,r,m)}$ or equivalently $g_{(q,s,l)\to(p,r,m)} \in p^{r-s}\mathbb{Z}_{p^r}$.

Next we show that any mapping described by (2.6) satisfying the conditions of the lemma is a homomorphism. For two elements $a, b \in J$ and for $(p, r, m) \in \mathscr{G}(\tilde{G})$

we have

$$
\begin{aligned}
[\phi(a+b)]_{p,r,m} &= \left[\phi\left(\bigoplus_{(q,s,l)\in\mathscr{G}(J)} (a_{q,s,l} +_{q^s} b_{q,s,l})\right)\right]_{p,r,m} \\
&= \left[\phi\left(\overbrace{\sum_{(q,s,l)\in\mathscr{G}(J)}}^{(J)} (a_{q,s,l} +_{q^s} b_{q,s,l})\mathbb{I}_{J:q,s,l}\right)\right]_{p,r,m} \\
&= \left[\phi\left(\overbrace{\sum_{(q,s,l)\in\mathscr{G}(J)}}^{(J)} \overbrace{\sum_{i=1,\cdots,a_{q,s,l}+_{q^s}b_{q,s,l}}}^{(J)} \mathbb{I}_{J:q,s,l}\right)\right]_{p,r,m} \\
&= \left[\overbrace{\sum_{(q,s,l)\in\mathscr{G}(J)}}^{(\tilde{G})} \overbrace{\sum_{i=1,\cdots,a_{q,s,l}+_{q^s}b_{q,s,l}}}^{(\tilde{G})} \phi\left(\mathbb{I}_{J:q,s,l}\right)\right]_{p,r,m} \\
&= \overbrace{\sum_{(q,s,l)\in\mathscr{G}(J)}}^{(\mathbb{Z}_{p^r})} \overbrace{\sum_{i=1,\cdots,a_{q,s,l}+_{q^s}b_{q,s,l}}}^{(\mathbb{Z}_{p^r})} \left[\phi\left(\mathbb{I}_{J:q,s,l}\right)\right]_{p,r,m} \\
&= \overbrace{\sum_{(q,s,l)\in\mathscr{G}(J)}}^{(\mathbb{Z}_{p^r})} \overbrace{\sum_{i=1,\cdots,a_{q,s,l}+_{q^s}b_{q,s,l}}}^{(\mathbb{Z}_{p^r})} g_{(q,s,l)\to(p,r,m)}
\end{aligned} \tag{2.24}
$$

On the other hand, we have

$$
\begin{aligned}
[\phi(a)+\phi(b)]_{p,r,m} &= [\phi(a)]_{p,r,m} +_{p^r} [\phi(b)]_{p,r,m} \\
&= \left(\overbrace{\sum_{(q,s,l)\in\mathscr{G}(J)}}^{(\mathbb{Z}_{p^r})} a_{q,s,l} g_{(q,s,l)\to(p,r,m)}\right) +_{p^r} \left(\overbrace{\sum_{(q,s,l)\in\mathscr{G}(J)}}^{(\mathbb{Z}_{p^r})} b_{q,s,l} g_{(q,s,l)\to(p,r,m)}\right) \\
&= \left(\overbrace{\sum_{(q,s,l)\in\mathscr{G}(J)}}^{(\mathbb{Z}_{p^r})} \overbrace{\sum_{i=1,\cdots,a_{q,s,l}}}^{(\mathbb{Z}_{p^r})} g_{(q,s,l)\to(p,r,m)}\right) +_{p^r} \left(\overbrace{\sum_{(q,s,l)\in\mathscr{G}(J)}}^{(\mathbb{Z}_{p^r})} \overbrace{\sum_{i=1,\cdots,b_{q,s,l}}}^{(\mathbb{Z}_{p^r})} g_{(q,s,l)\to(p,r,m)}\right) \\
&= \overbrace{\sum_{(q,s,l)\in\mathscr{G}(J)}}^{(\mathbb{Z}_{p^r})} \overbrace{\sum_{i=1,\cdots,a_{q,s,l}+b_{q,s,l}}}^{(\mathbb{Z}_{p^r})} g_{(q,s,l)\to(p,r,m)}
\end{aligned} \tag{2.25}
$$

where the addition in $a_{q,s,l} + b_{q,s,l}$ is the integer addition.

In order to show that $\phi$ is a homomorphism, it suffices to show that under the conditions of the lemma, Equations (2.24) and (2.25) are equivalent. We show that for a

fixed $(q,s,l) \in \mathscr{G}(J)$, if the conditions of the lemma are satisfied, then

$$\overbrace{\sum_{i=1,\cdots,a_{q,s,l}+b_{q,s,l}}}^{(\mathbb{Z}_{p^r})} g_{(q,s,l)\to(p,r,m)} = \overbrace{\sum_{i=1,\cdots,a_{q,s,l}+_{q^s}b_{q,s,l}}}^{(\mathbb{Z}_{p^r})} g_{(q,s,l)\to(p,r,m)} \tag{2.26}$$

Note that if $p \neq q$, then both summations are zero. Note that we have

$$\overbrace{\sum_{i=1,\cdots,a_{q,s,l}+b_{q,s,l}}}^{(\mathbb{Z}_{p^r})} g_{(q,s,l)\to(p,r,m)} = \overbrace{\sum_{i=1,\cdots,\left(a_{q,s,l}+b_{q,s,l}\right) \pmod{p^r}}}^{(\mathbb{Z}_{p^r})} g_{(q,s,l)\to(p,r,m)}$$

and

$$\overbrace{\sum_{i=1,\cdots,a_{q,s,l}+_{q^s}b_{q,s,l}}}^{(\mathbb{Z}_{p^r})} g_{(q,s,l)\to(p,r,m)} = \overbrace{\sum_{i=1,\cdots,\left(a_{q,s,l}+_{q^s}b_{q,s,l}\right) \pmod{p^r}}}^{(\mathbb{Z}_{p^r})} g_{(q,s,l)\to(p,r,m)}$$

If $p = q$ and $r \leq s$, then we have $(a_{q,s,l} +_{q^s} b_{q,s,l}) \pmod{p^r} = (a_{q,s,l} + b_{q,s,l}) \pmod{p^r}$ and hence it follows that Equation (2.26) is satisfied. If $p = q$ and $r \geq s$, since $g_{(q,s,l)\to(p,r,m)} \in p^{r-s}\mathbb{Z}_{p^r}$ we have

$$\overbrace{\sum_{i=1,\cdots,a_{q,s,l}+b_{q,s,l}}}^{(\mathbb{Z}_{p^r})} g_{(q,s,l)\to(p,r,m)} = \overbrace{\sum_{i=1,\cdots,\left(a_{q,s,l}+b_{q,s,l}\right) \pmod{p^s}}}^{(\mathbb{Z}_{p^r})} g_{(q,s,l)\to(p,r,m)}$$

and hence it follows that Equation (2.26) is satisfied.

#### 2.7.0.2 Proof of Lemma II.10

Note that since $g_{(q,s,l)\to(p,r,m)}$'s and $B$ are uniformly distributed, in order to find the desired joint probability, we need to count the number of choices for $g_{(q,s,l)\to(p,r,m)}$'s and $B$ such that for $(p,r,m) \in \mathscr{G}(G^n)$,

$$\left(\overbrace{\sum_{(q,s,l)\in\mathscr{G}(J)}}^{(\mathbb{Z}_{p^r})} a_{q,s,l} g_{(q,s,l)\to(p,r,m)}\right) +_{p^r} B_{p,r,m} = u_{p,r,m}$$

$$\left(\overbrace{\sum_{(q,s,l)\in\mathscr{G}(J)}}^{(\mathbb{Z}_{p^r})} \tilde{a}_{q,s,l} g_{(q,s,l)\to(p,r,m)}\right) +_{p^r} B_{p,r,m} = \tilde{u}_{p,r,m}$$

and divide this number by the total number of choices which is equal to

$$|G|^n \cdot \prod_{(p,r,m)\in\mathscr{G}(G^n)} \prod_{\substack{(q,s,l)\in\mathscr{G}(J)\\ q=p}} p^{\min(r,s)} = |G|^n \cdot \left[ \prod_{(p,r,m)\in\mathscr{G}(G)} \prod_{\substack{(q,s,l)\in\mathscr{G}(J)\\ q=p}} p^{\min(r,s)} \right]^n$$

where the term $p^{\min(r,s)}$ appears since the number of choices for $g_{(q,s,l)\to(p,r,m)}$ is $p^r$ if $p = q, r \leq s$ and is equal to $p^s$ if $p = q, r \geq s$. Since $B$ can take values arbitrarily from $G^n$, the number of choices for the above set of conditions is equal to the number of choices for $g_{(q,s,l)\to(p,r,m)}$'s such that,

$$\left( \sum_{(q,s,l)\in\mathscr{G}(J)} \overbrace{(\tilde{a}_{q,s,l} - a_{q,s,l})}^{(\mathbb{Z}_{p^r})} g_{(q,s,l)\to(p,r,m)} \right) = \tilde{u}_{p,r,m} - u_{p,r,m}$$

Note that for all $(q,s,l) \in \mathscr{G}(J)$, $(\tilde{a}_{q,s,l} - a_{q,s,l})g_{(q,s,l)\to(p,r,m)} \in p^{\theta_{p,r}}\mathbb{Z}_{p^r}$. Therefore we require $\tilde{u}_{p,r,m} - u_{p,r,m} \in p^{\theta_{p,r}}\mathbb{Z}_{p^r}$ and therefore we require $\tilde{u} - u \in H^n_\theta$ or otherwise the probability would be zero.

For fixed $p \in \mathscr{P}(G)$ and $r \in \mathscr{R}_p(G)$, let $(q^*, s^*, l^*) \in \mathscr{G}(J)$ be such that $q^* = p$ and

$$\theta_{p,r} = |r - s^*|^+ + \hat{\theta}_{q^*,s^*,l^*}$$

For fixed $(p,r,m) \in \mathscr{G}(G^n)$, and for $(q,s,l) \neq (q^*,s^*,l^*)$, choose $g_{(q,s,l)\to(p,r,m)}$ arbitrarily from it's domain. The number of choices for this is equal to

$$\left[ \prod_{(p,r,m)\in\mathscr{G}(G)} \prod_{\substack{(q,s,l)\in\mathscr{G}(J)\\ q=p\\ (q,s,l)\neq(q^*,s^*,l^*)}} p^{\min(r,s)} \right]^n$$

For each $(p,r,m) \in \mathscr{G}(G^n)$, we need to have

$$(\tilde{a}_{q^*,s^*,l^*} - a_{q^*,s^*,l^*}) g_{(q^*,s^*,l^*)\to(p,r,m)}$$
$$= \tilde{u}_{p,r,m} - u_{p,r,m} - \left( \overbrace{\sum}^{(\mathbb{Z}_{p^r})}_{\substack{(q,s,l)\in\mathscr{G}(J)\\(q,s,l)\neq(q^*,s^*,l^*)}} (\tilde{a}_{q,s,l} - a_{q,s,l}) g_{(q,s,l)\to(p,r,m)} \right)$$

Note that the right hand side is included in $p^{\theta_{p,r}}\mathbb{Z}_{p^r}$ and $(\tilde{a}_{q^*,s^*,l^*} - a_{q^*,s^*,l^*})$ is included in $p^{\hat{\theta}_{q^*,s^*,l^*}}\mathbb{Z}_{(q^*)^{(s^*)}}$. We need to count the number of solutions for $g_{(q^*,s^*,l^*)\to(p,r,m)}$ in $p^{|r-s^*|^+}\mathbb{Z}_{p^r}$. Using Lemma II.13, we can show that the number of solutions is equal to $p^{\hat{\theta}_{q^*,s^*,l^*}}$. The total number of solutions for $\phi$ is equal to

$$\left[ \left( \prod_{(p,r,m)\in\mathscr{G}} \prod_{\substack{(q,s,l)\in\mathscr{G}(J)\\q=p\\(q,s,l)\neq(q^*,s^*,l^*)}} p^{\min(r,s)} \right) \cdot p^{\hat{\theta}_{q^*,s^*,l^*}} \right]^n$$

Hence we have

$$P\left(\phi(a)+B=u, \phi(\tilde{a})+B=\tilde{u}\right) = \frac{\left[ \prod_{(p,r,m)\in\mathscr{G}(G)} \left( p^{\hat{\theta}_{q^*,s^*,l^*}} \cdot \prod_{\substack{(q,s,l)\in\mathscr{G}(J)\\q=p\\(q,s,l)\neq(q^*,s^*,l^*)}} p^{\min(r,s)} \right) \right]^n}{\left[ \prod_{(p,r,m)\in\mathscr{G}(G)} \prod_{\substack{(q,s,l)\in\mathscr{G}(J)\\q=p}} p^{\min(r,s)} \right]^n}$$
$$= \left[ \prod_{(p,r,m)\in\mathscr{G}(G)} \prod_{\substack{(q,s,l)\in\mathscr{G}(J)\\q=p\\(q,s,l)=(q^*,s^*,l^*)}} \frac{p^{\hat{\theta}_{q^*,s^*,l^*}}}{p^{\min(r,s)}} \right]^n$$

Note that for $(q,s,l) = (q^*,s^*,l^*)$ we have

$$\min(r,s) = \min(r,s^*) = r - |r-s^*|^+ = r - \left(\theta_{p,r} - \hat{\theta}_{q^*,s^*,l^*}\right)$$

Therefore, the above probability is equal to

$$\left[\prod_{(p,r,m)\in\mathscr{G}}\prod_{\substack{(q,s,l)\in\mathscr{G}(J)\\ q=p\\ (q,s,l)=(q^*,s^*,l^*)}}\frac{p^{\hat{\theta}_{q^*,s^*,l^*}}}{p^{r-\left(\theta_{p,r}-\hat{\theta}_{q^*,s^*,l^*}\right)}}\right]^n = \left[\prod_{(p,r,m)\in\mathscr{G}}\prod_{\substack{(q,s,l)\in\mathscr{G}(J)\\ q=p\\ (q,s,l)=(q^*,s^*,l^*)}}\frac{1}{p^{r-\theta_{p,r}}}\right]^n$$
$$= \left[\prod_{(p,r,m)\in\mathscr{G}}\frac{p^{\theta_{p,r}}}{p^r}\right]^n = \frac{1}{|H_\theta|^n}$$

Since the dither $B$ is uniform, we conclude that

$$P\begin{pmatrix}\phi(u)+B=x\\ \phi(\tilde{u})+B=\tilde{x}\end{pmatrix} = \frac{1}{|G|^n}\frac{1}{|H_\theta|^n}$$

#### 2.7.0.3 Proof of Lemma II.11

Let $\tilde{a}\in T_\theta(a)$ be such that for $(q,s,l)\in\mathscr{G}(J)$,

$$\tilde{a}_{q,s,l} - a_{q,s,l} \in q^{\hat{\theta}_{q,s,l}}\mathbb{Z}_{q^s}\backslash q^{\hat{\theta}_{q,s,l}+1}\mathbb{Z}_{q^s}$$

for some $0\le\hat{\theta}_{q,s,l}\le s$. Since for all $\tilde{a}\in T_\theta(a)$ and all $(p,r)\in\mathscr{Q}(G)$

$$\min_{(p,s,l)\in\mathscr{G}(J)}|r-s|^+ + \hat{\theta}_{q,s,l} = \theta_{p,r}$$

we require $\hat{\theta}_{p,s,l}\ge\theta_{p,s}$ for all $(p,s,l)\in\mathscr{G}(J)$. This means for $(q,s,l)\in\mathscr{G}(J)$, $\tilde{a}_{q,s,l}$ can only take values from

$$a_{q,s,l} + q^{\theta_{q,s}}\mathbb{Z}_{q^s}$$

The cardinality of this set is equal to $q^{s-\theta_{q,s}}$. Therefore,

$$|T_\theta(a)| \le \prod_{(q,s,l)\in\mathscr{G}(J)} q^{s-\theta_{q,s}} = \prod_{(q,s)\in\mathscr{Q}(G)} q^{(s-\theta_{q,s})kw_{q,s}}$$

The last part of the proof is straightforward given the definitions of $\omega_\theta$ and $R$.

#### 2.7.0.4 Useful Lemmas

**Lemma II.13.** *Let $p$ be a prime and $s, r$ a positive integer such that $s \leq r$. For $a \in \mathbb{Z}_{p^s}$ and $b \in \mathbb{Z}_{p^r}$, let $0 \leq \hat{\theta} \leq s$ and $\hat{\theta} \leq \theta \leq r$ be such that*

$$a \in p^{\hat{\theta}}\mathbb{Z}_{p^s} \backslash p^{\hat{\theta}+1}\mathbb{Z}_{p^s}$$

$$b \in p^{\theta}\mathbb{Z}_{p^r}$$

*Write $a = p^{\hat{\theta}}\alpha$ for some invertible element $\alpha \in \mathbb{Z}_{p^r}$ and $b = p^{\theta}\beta$ for some $\beta \in \beta \in \{0, 1, \cdots, p^{r-\theta} - 1\}$. Then, the set of solutions to the equation $ax \pmod{p^r} = b$ is*

$$\left\{p^{\theta-\hat{\theta}}\alpha^{-1}\beta + i\alpha^{-1}p^{r-\hat{\theta}} | i = 0, 1, \cdots, p^{\hat{\theta}} - 1\right\}$$

*Proof.* Note that the representation of $b$ as $b = p^{\theta}\beta$ is not unique and for any $\tilde{\beta}$ of the form $\tilde{\beta} = \beta + ip^{r-\theta}$ for $i = 0, 1, \cdots, p^{\theta} - 1$, $b$ can be written as $p^{\theta}\tilde{\beta}$. Also, the representation of $a$ as $a = p^{\hat{\theta}}\alpha$ is not unique and for any $\tilde{\alpha} = \alpha + ip^{r-\hat{\theta}}$ for $i = 0, 1, \cdots, p^{\hat{\theta}} - 1$, we have $a = p^{\hat{\theta}}\tilde{\alpha}$. The set of solutions to $ax = b$ is identical to the set of solutions to $p^{\hat{\theta}}x = p^{\theta}\alpha^{-1}\beta$. The set of solutions to the latter is

$$\left\{p^{\theta-\hat{\theta}}\alpha^{-1}\beta + i\alpha^{-1}p^{r-\hat{\theta}} | i = 0, 1, \cdots, p^{\hat{\theta}} - 1\right\}$$

It remains to show that this set of solutions is independent of the choice of $\alpha$ and $\beta$. First, we show that the set of solutions is independent of the choice of $\beta$. For $\tilde{\beta} = \beta + jp^{r-\theta}$ for some $j \in \{0, 1, \cdots, p^{\theta_2} - 1\}$, we have

$$\begin{aligned}
&\left\{p^{\theta-\hat{\theta}}\alpha^{-1}\tilde{\beta} + i\alpha^{-1}p^{r-\hat{\theta}} | i = 0, 1, \cdots, p^{\hat{\theta}} - 1\right\} \\
&\qquad = \left\{p^{\theta-\hat{\theta}}\alpha^{-1}\left(\beta + jp^{r-\theta}\right) + i\alpha^{-1}p^{r-\hat{\theta}} | i = 0, 1, \cdots, p^{\hat{\theta}} - 1\right\} \\
&\qquad = \left\{p^{\theta-\hat{\theta}}\alpha^{-1}\beta + (i+j)\,\alpha^{-1}p^{r-\hat{\theta}} | i = 0, 1, \cdots, p^{\hat{\theta}} - 1\right\} \\
&\qquad \overset{(a)}{=} \left\{p^{\theta-\hat{\theta}}\alpha^{-1}\beta + i\alpha^{-1}p^{r-\hat{\theta}} | i = 0, 1, \cdots, p^{\hat{\theta}} - 1\right\}
\end{aligned}$$

where $(a)$ follows since the set $p^{r-\hat{\theta}}\{0, 1, \cdots, p^{\hat{\theta}} - 1\}$ is a subgroup of $\mathbb{Z}_{p^r}$ and $jp^{r-\hat{\theta}}$ lies in this set.

Next, we show that the set of solutions is independent of the choice of $\alpha$. For $\tilde{\alpha} = \alpha + jp^{r-\hat{\theta}}$ for some $j \in \{0, 1, \cdots, p^{\hat{\theta}} - 1\}$, we have

$$\tilde{\alpha}\left(\alpha^{-1} - \alpha^{-1} j p^{r-\hat{\theta}} \tilde{\alpha}^{-1}\right) = 1$$

Therefore, it follows that the unique inverse of $\tilde{\alpha}$ satisfies $\alpha^{-1} - \tilde{\alpha}^{-1} \in \alpha^{-1} p^{r-\hat{\theta}} \mathbb{Z}_{p^r}$. Assume $\tilde{\alpha}^{-1} = \alpha^{-1} + k\alpha^{-1} p^{r-\hat{\theta}}$. We have,

$$\begin{aligned}
&\left\{p^{\theta-\hat{\theta}} \tilde{\alpha}^{-1} \beta + i\tilde{\alpha}^{-1} p^{r-\hat{\theta}} | i = 0, 1, \cdots, p^{\hat{\theta}} - 1\right\} \\
&\quad = \left\{p^{\theta-\hat{\theta}} \left(\alpha^{-1} + k\alpha^{-1} p^{r-\hat{\theta}}\right) \beta + i\left(\alpha^{-1} + k\alpha^{-1} p^{r-\hat{\theta}}\right) p^{r-\hat{\theta}} | i = 0, 1, \cdots, p^{\hat{\theta}} - 1\right\} \\
&\quad = \left\{p^{\theta-\hat{\theta}} \alpha^{-1} \beta + \left(i + ikp^{r-\hat{\theta}} + k\beta p^{\theta-\hat{\theta}}\right) \alpha^{-1} p^{r-\hat{\theta}} | i = 0, 1, \cdots, p^{\hat{\theta}} - 1\right\} \\
&\quad \overset{(a)}{=} \left\{p^{\theta-\hat{\theta}} \alpha^{-1} \beta + i\alpha^{-1} p^{r-\hat{\theta}} | i = 0, 1, \cdots, p^{\hat{\theta}} - 1\right\}
\end{aligned}$$

where same as above, $(a)$ follows since the set $p^{r-\hat{\theta}}\{0, 1, \cdots, p^{\hat{\theta}} - 1\}$ is a subgroup of $\mathbb{Z}_{p^r}$ and $(ikp^{r-\hat{\theta}} + k\beta p^{\theta-\hat{\theta}})p^{r-\hat{\theta}}$ lies in this set. □

**Lemma II.14.** *Let $X$ be a random variable taking values from the group $G$ and for a subgroup $H$ of $G$, define $[X] = X + H$. For $y \in A_\epsilon^n(Y)$ and $x \in A_\epsilon^n(X|y)$, let $z = [x] = x + H^n$. Then we have*

$$(x + H^n) \cap A_\epsilon^n(X|y) = A_\epsilon^n(X|zy)$$

*and*

$$(1 - \epsilon) 2^{n[H(X|Y[X]) - O(\epsilon)]} \leq |(x + H^n) \cap A_\epsilon^n(X|y)| \leq 2^{n[H(X|Y[X]) + O(\epsilon)]}$$

*Proof.* First, we show that $(x + H^n) \cap A_\epsilon^n(X|y)$ is contained in $A_\epsilon^n(X|zy)$. Since $z$ is a function of $x$, we have $(x, z, y) \in A_\epsilon^n(X, [X], Y)$. For $x' \in (x + H^n) \cap A_\epsilon^n(X|y)$, we have $[x'] = x' + H^n = x + H^n = z$ and $(x', z, y) = (x', [x'], y) \in A_\epsilon^n(X, [X], Y)$. Therefore, $x' \in A_\epsilon^n(X|zy)$ and hence,

$$(x + H^n) \cap A_\epsilon^n(X|y) \subseteq A_\epsilon^n(X|zy)$$

Conversely, for $x' \in A_\epsilon^n(X|zy)$, since $(x,z) \in A_\epsilon^n(X,[X])$ where $[X]$ is a function of $X$, we have $[x'] = z$. This implies $x' \in z + H^n = x + H^n$. Clearly, we also have $x' \in A_\epsilon^n(X|y)$. The claim on the size of the set follows since $(z,y) \in A_\epsilon^n([X]Y)$. $\square$

#### 2.7.0.5 How to Compute the Rate

For $(p,r) \in \mathscr{Q}(G)$, define

$$\Theta^{p,r} = \{\theta \in \Theta | \forall (p,r') \in \mathscr{Q}(G) : \frac{\theta_{p,r}}{r} \geq \frac{\theta_{p,r'}}{r'}\}$$

and distribute the break evens so that $\Theta^{p,r}, (p,r) \in \mathscr{Q}(G)$ forms a partition of $\Theta$. Let $(w^*_{p,r})_{(p,r)\in\mathscr{Q}(G)}$ be the optimal weights (need not be unique) and let $\Theta^*$ be set of the maximizing $\theta$'s for the optimal rate. Define $\mathscr{S}(G) = \{(p',r') \in \mathscr{Q}(G) | w^*_{p',r'} \neq 0\}$. Since $\Theta^{p,r}, (p,r) \in \mathscr{Q}(G)$ forms a partition of $\Theta$, we have $\theta^* \in \Theta^{p,r}$ for some $(p,r) \in \mathscr{Q}(G)$. For $(p',r') \in \mathscr{Q}(G)$ such that $(p',r') \neq (p,r)$, if there is no $\theta^* \in \Theta^*$ such that $\theta^* \in \Theta^{p',r'}$, we can decrease $w^*_{p',r'}$ and increase some of the other weights to get a better rate which is a contradiction. Hence, the optimal weight can be found as follows:

Let $\mathscr{S}(G)$ be a subset of $\mathscr{Q}(G)$ and Let $R(\mathscr{S}(G))$ be an empty set. For $(p,r) \in \mathscr{S}(G)$, choose $\theta^{p,r}$ from $\Theta^{p,r}$ and solve the system of equations:

$$\text{For all } (p,r) \in \mathscr{S}(G) \text{ and } \theta = \theta^{p,r}, \frac{1}{\omega_\theta} I([U]_\theta; X) = C$$

$$\sum_{(p,r)\in\mathscr{S}(G)} w_{p,r} = 1$$

where $C$ is an arbitrary constant. Given the solutions $w_{p,r}, (p,r) \in \mathscr{S}(G)$, find $C$ and add it to the set $R(\mathscr{S}(G))$. Do this for all choices of $\theta^{p,r}$'s and take the maximum of the set $R(\mathscr{S}(G))$. We also minimize the rate over the choice of $\mathscr{S}(G)$.

# CHAPTER III

# Abelian Group Codes for Multi-terminal Communications

## 3.1 Nested Codes for Channels with State Information

Consider a point-to-point channel coding problem with channel state information available at the transmitter. Denote the channel by $(\mathscr{X}, \mathscr{S}, \mathscr{Y}, W)$ where $\mathscr{X}$ is the channel input alphabet, $\mathscr{S}$ is the channel state alphabet and $\mathscr{Y}$ is the channel output alphabet and for the channel input $x \in \mathscr{X}$ and the channel state $s \in \mathscr{S}$, $W(y|x,s)$ denotes the conditional probability of observing $y \in \mathscr{Y}$ in the channel output. We assume $\mathscr{X} = G$ for some Abelian group $G$. We study the performance of "nested random/group codes" and "nested group/random codes" for this problem. These ensembles are important because they can be used in many multi-terminal communications such as broadcast channels and interference channels.

### 3.1.1 Nested Random/Group Codes for Channel Coding

A nested code consists of an outer code which is partitioned into smaller inner codes and the set of messages is equal to the set of inner codes. We employ a nested code in which the inner code is a group code and the outer code consists of random shifts of the inner code. Let $\mathbb{C}_{\text{in}} = \{\phi(a)|a \in J\}$ where $\phi$ and $J$ are defined in (2.11)

and (2.14) respectively and let

$$\mathbb{C}_{\text{out}} = \bigcup_{m=1}^{2^{nR}} \Big( \mathbb{C}_{\text{in}} + B_m \Big)$$

where $B_m$'s are iid random variables distributed uniformly over $G^n$. Note that the rates of the inner and outer codes are equal to $R_{\text{in}} = \frac{1}{n} \log |J|$ and $R_{\text{out}} = R_{\text{in}} + R$ where $R$ is the communication rate of our coding scheme.

The encoding and decoding rules are as follows: Given a message $m \in \{1, 2, \cdots, 2^{nR}\}$, and the channel state $\boldsymbol{s} \in \mathscr{S}^n$, define

$$\alpha(m, \boldsymbol{s}) = \sum_{a \in J} \sum_{\boldsymbol{x} \in A_\epsilon^n(X|\boldsymbol{s})} \mathbb{1}_{\{\phi(a) + B_m = \boldsymbol{x}\}}$$

Note that if $\alpha(m, \boldsymbol{s}) > 0$, then there exists at least one $a \in J$ with $\phi(a) + B_m \in A_\epsilon^n(X|\boldsymbol{s})$. In this case, the encoder picks one such $a$ and sends $\boldsymbol{x} = \phi(a) + B_m$ over the channel. The encoder will declare an encoding error if $\alpha(m, \boldsymbol{s}) = 0$. Although it may be unnecessary, it is convenient in the proofs to assume that the encoder declares error if $\alpha(m, \boldsymbol{s}) \leq \frac{|J| \cdot |A_\epsilon^n(X|\boldsymbol{s})|}{2 \cdot |G|^n}$. We denote this error event by $Err_e$. We also assume that $a \in J$ is picked with probability $\frac{\sum_{\boldsymbol{x} \in A_\epsilon^n(X|\boldsymbol{s})} \mathbb{1}_{\{\phi(a) + B_m = \boldsymbol{x}\}}}{\alpha(m, \boldsymbol{s})}$.

At the decoder, after receiving the channel output $\boldsymbol{y} \in \mathscr{Y}^n$, the decoder looks for a unique message $\hat{m} \in \{1, 2, \cdots, 2^{nR}\}$ for which there exists $a \in J$ with $\phi(a) + B_{\hat{m}} \in A_\epsilon(X|\boldsymbol{y})$. If it doesn't find such $\hat{m}$ ($Err_{d1}$) or if it finds multiple such $\hat{m}$'s ($Err_{d2}$), it declares error.

We show that if

$$R \leq \bar{I}(X; Y) - I_{s.c.}^G(X; S)$$

then the probability of all the errors ($Err_e$, $Err_{d1}$ and $Err_{d2}$) approach zero as the block length approaches infinity. Note that by the standard typicality results [20,

Theorem 3.1.2] one can show that with probability approaching one as the block length increases, $\phi(a) + B_m \in A_\epsilon(X|\boldsymbol{y})$. Therefore, the probability of the error event $Err_{d1}$ vanishes as the block length increases. It suffices to show that for any choice of weights $(w_{p,r})_{(p,r)\in\mathscr{Q}(G)}$, the probability of the two error events $Err_e$ and $Err_{d2}$ vanish if

$$R_{\text{in}} > \frac{1}{\omega_\theta}\Big(\log|G:H_\theta| - H([X]_\theta|S)\Big)$$
$$R + R_{\text{in}} < \bar{I}(X;Y)$$

#### 3.1.1.1 The Error Event $Err_e$

Note that given the message $m$ and the channel state $s^n$, the error event $Err_e$ occurs if $\alpha(m,\boldsymbol{s}) \leq \frac{|J|\cdot|A_\epsilon^n(X|\boldsymbol{s})|}{2\cdot|G|^n}$. We bound the probability of error using the following Chebyshev's inequality:

$$P\Big(Err_e|m,\boldsymbol{s}\Big) = P\Big(\alpha(m,\boldsymbol{s}) \leq \frac{|J|\cdot|A_\epsilon^n(X|\boldsymbol{s})|}{2\cdot|G|^n}\Big) \leq \frac{\text{var}\{\alpha(m,\boldsymbol{s})\}}{\mathbb{E}\{\alpha(m,\boldsymbol{s})\}^2}$$

We have

$$\begin{aligned}\mathbb{E}\{\alpha(m,\boldsymbol{s})\} &= \sum_{a\in J}\sum_{\boldsymbol{x}\in A_\epsilon^n(X|\boldsymbol{s})} P\Big(\phi(a)+B_m=\boldsymbol{x}\Big)\\ &= \frac{|J|\cdot|A_\epsilon^n(X|\boldsymbol{s})|}{|G|^n}\end{aligned}$$

and

$$\begin{aligned}\mathbb{E}\{\alpha(m,\boldsymbol{s})^2\} &= \sum_{a,\tilde{a}\in J}\sum_{\boldsymbol{x},\tilde{\boldsymbol{x}}\in A_\epsilon^n(X|\boldsymbol{s})} P\Big(\phi(a)+B_m=\boldsymbol{x},\phi(\tilde{a})+B_m=\tilde{\boldsymbol{x}}\Big)\\ &= \sum_{a\in J}\sum_{\boldsymbol{x}\in A_\epsilon^n(X|\boldsymbol{s})}\sum_{\theta\in\Theta}\sum_{\tilde{a}\in T_\theta(a)}\sum_{\substack{\tilde{\boldsymbol{x}}\in A_\epsilon^n(X|\boldsymbol{s})\\ \tilde{\boldsymbol{x}}\in\boldsymbol{x}+H_\theta^n}}\frac{1}{|G|^n\cdot|H_\theta|^n}\end{aligned}$$

Therefore,

$$\begin{aligned}\mathrm{var}\{\alpha(m,\boldsymbol{s})\} &= \mathbb{E}\{\alpha(m,\boldsymbol{s})^2\} - \mathbb{E}\{\alpha(m,\boldsymbol{s})\}^2 \\ &\leq \sum_{\substack{\theta\in\Theta\\ \theta\neq\mathbf{0}}} \sum_{a\in J} \sum_{\boldsymbol{x}\in A_\epsilon^n(X|\boldsymbol{s})} \sum_{\tilde{a}\in T_\theta(a)} \sum_{\substack{\tilde{\boldsymbol{x}}\in A_\epsilon^n(X|\boldsymbol{s})\\ \tilde{\boldsymbol{x}}\in\boldsymbol{x}+H_\theta^n}} \frac{1}{|G|^n\cdot|H_\theta|^n} \\ &\leq \sum_{\substack{\theta\in\Theta\\ \theta\neq\mathbf{0}}} \frac{|J|\cdot 2^{n[H(X|S)+\delta]}\cdot|T_\theta|\cdot 2^{n[H(X|[X]_\theta S)+\delta]}}{|G|^n\cdot|H_\theta|^n}\end{aligned}$$

Hence,

$$P\Big(Err_e|m,\boldsymbol{s}\Big) \leq \sum_{\substack{\theta\in\Theta\\ \theta\neq\mathbf{0}}} \frac{|G|^n\cdot|T_\theta|\cdot 2^{n[H(X|[X]_\theta S)+\delta]}}{|J|\cdot 2^{n[H(X|S)+\delta]}\cdot|H_\theta|^n}$$

Note that $|J| = 2^{nR_{\text{in}}}$ and $|T_\theta| = 2^{n(1-\omega_\theta)R_{\text{in}}}$ and $H(X|S) - H(X|[X]_\theta S) = H([X]_\theta|S)$. Therefore, for $\theta\in\Theta$ and $\theta\neq\mathbf{0}$, we require

$$R_{\text{in}} > \frac{1}{\omega_\theta}\Big(\log|G:H_\theta| - H([X]_\theta|\Big)$$

#### 3.1.1.2 The Error Event $Err_{d2}$

Let $Err = Err_{d2}\cap Err_e^c\cap Err_{d1}^c$. Then the probability of the error event $Err$ is equal to

$$\begin{aligned}P\Big(Err\Big) &= \frac{1}{2^{nR}}\sum_{m=1}^{2^{nR}}\sum_{s^n\in\mathscr{S}^n} p_S^n(\boldsymbol{s})\sum_{a\in J}\sum_{\boldsymbol{x}\in A_\epsilon^n(X|\boldsymbol{s})} \mathbb{1}_{\{\alpha(m,\boldsymbol{s})>\frac{|J|\cdot|A_\epsilon^n(X|\boldsymbol{s})|}{2\cdot|G|^n}\}}\frac{1}{\alpha(m,\boldsymbol{s})}\mathbb{1}_{\{\phi(a)+B_m=\boldsymbol{x}\}} \\ &\qquad \sum_{\boldsymbol{y}\in\mathscr{Y}^n} W^n(\boldsymbol{y}|\boldsymbol{x},\boldsymbol{s})\sum_{\substack{\tilde{m}=1\\ \tilde{m}\neq m}}^{2^{nR}}\sum_{\tilde{a}\in J}\sum_{\tilde{\boldsymbol{x}}\in A_\epsilon^n(X|\boldsymbol{y})}\mathbb{1}_{\{\phi(\tilde{a})+B_{\tilde{m}}=\tilde{\boldsymbol{x}}\}} \\ &\leq \frac{1}{2^{nR}}\sum_{m=1}^{2^{nR}}\sum_{\boldsymbol{s}\in\mathscr{S}^n} p_S^n(\boldsymbol{s})\sum_{a\in J}\sum_{\boldsymbol{x}\in A_\epsilon^n(X|\boldsymbol{s})}\frac{2\cdot|G|^n}{|J|\cdot|A_\epsilon^n(X|\boldsymbol{s})|}\mathbb{1}_{\{\phi(a)+B_m=\boldsymbol{x}\}} \\ &\qquad \sum_{\boldsymbol{y}\in\mathscr{Y}^n} W^n(\boldsymbol{y}|\boldsymbol{x},\boldsymbol{s})\sum_{\substack{\tilde{m}=1\\ \tilde{m}\neq m}}^{2^{nR}}\sum_{\tilde{a}\in J}\sum_{\tilde{\boldsymbol{x}}\in A_\epsilon^n(X|\boldsymbol{y})}\mathbb{1}_{\{\phi(\tilde{a})+B_{\tilde{m}}=\tilde{\boldsymbol{x}}\}}\end{aligned}$$

Therefore,

$$\begin{aligned}
\mathbb{E}\Big\{P(Err)\Big\} &\leq \frac{1}{2^{nR}} \sum_{m=1}^{2^{nR}} \sum_{\boldsymbol{s}\in\mathscr{S}^n} p_S^n(\boldsymbol{s}) \sum_{a\in J} \sum_{\boldsymbol{x}\in A_\epsilon^n(X|\boldsymbol{s})} \frac{2\cdot|G|^n}{|J|\cdot|A_\epsilon^n(X|\boldsymbol{s})|} \sum_{\boldsymbol{y}\in\mathscr{Y}^n} W^n(\boldsymbol{y}|\boldsymbol{x},\boldsymbol{s}) \\
&\qquad \sum_{\substack{\tilde{m}=1\\ \tilde{m}\neq m}}^{2^{nR}} \sum_{\tilde{a}\in J} \sum_{\tilde{\boldsymbol{x}}\in A_\epsilon^n(X|\boldsymbol{y})} P\Big(\phi(a)+B_m=\boldsymbol{x}, \phi(\tilde{a})+B_{\tilde{m}}=\tilde{\boldsymbol{x}}\Big) \\
&= \frac{1}{2^{nR}} \sum_{m=1}^{2^{nR}} \sum_{\boldsymbol{s}\in\mathscr{S}^n} p_S^n(\boldsymbol{s}) \sum_{a\in J} \sum_{\boldsymbol{x}\in A_\epsilon^n(X|\boldsymbol{s})} \frac{2\cdot|G|^n}{|J|\cdot|A_\epsilon^n(X|\boldsymbol{s})|} \sum_{\boldsymbol{y}\in\mathscr{Y}^n} W^n(\boldsymbol{y}|\boldsymbol{x},\boldsymbol{s}) \\
&\qquad \sum_{\substack{\tilde{m}=1\\ \tilde{m}\neq m}}^{2^{nR}} \sum_{\tilde{a}\in J} \sum_{\tilde{\boldsymbol{x}}\in A_\epsilon^n(X|\boldsymbol{y})} \frac{1}{|G|^{2n}} \\
&\leq \frac{2^{nR}\cdot|J|\cdot 2^{n[H(X|Y)+\delta]}\cdot 2}{|G|^n}
\end{aligned}$$

Therefore, we require to have

$$R + R_{\text{in}} < \log|G| - H(X|Y) = \bar{I}(X;Y)$$

### 3.1.2 Nested Group/Random Codes for Channel Coding

We employ a nested code in which the outer code is a group code and the inner code is obtained by random binning of the outer code. Let $\mathbb{C}_{\text{out}} = \{\phi(a)+B | a\in J\}$ where $\phi$ and $J$ are defined in (2.11) and (2.14) respectively and $B$ is uniformly distributed over $G^n$. Define the random mapping $s : J \to \{1,2,\cdots,2^{nR}\}$ where $R$ is the rate of communication and for $a\in J$, $s(a)$'s are independent and uniformly distributed over $\{1,2,\cdots,2^{nR}\}$. Note the rate of the outer code is $R_{\text{out}} = \frac{1}{n}\log|J|$.

The encoding and decoding rules are as follows: Given a message $m$ from the set $\{1,2,\cdots,2^{nR}\}$, and the channel state $\boldsymbol{s}\in\mathscr{S}^n$, define

$$\alpha(m,\boldsymbol{s}) = \sum_{a\in J} \sum_{\boldsymbol{x}\in A_\epsilon^n(X|\boldsymbol{s})} \mathbb{1}_{\{\phi(a)+B=\boldsymbol{x}, s(a)=m\}}$$

Note that if $\alpha(m,\boldsymbol{s})>0$, then there exists at least one $a\in J$ with $s(a)=m$ and $\phi(a)+B\in A_\epsilon^n(X|\boldsymbol{s})$. In this case, the encoder picks one such $a$ and sends $\boldsymbol{x}=\phi(a)+B$

over the channel. The encoder will declare an encoding error if $\alpha(m, \boldsymbol{s}) = 0$. Although it may be unnecessary, it is convenient in the proofs to assume that the encoder declares error if $\alpha(m, \boldsymbol{s}) \leq \frac{|J| \cdot |A_\epsilon^n(X|\boldsymbol{s})|}{2 \cdot 2^{nR} \cdot |G|^n}$. We denote this error event by $Err_e$. We also assume that $a \in J$ is picked with probability $\frac{\sum_{\boldsymbol{x} \in A_\epsilon^n(X|\boldsymbol{s})} \mathbb{1}_{\{\phi(a)+B=\boldsymbol{x}, s(a)=m\}}}{\alpha(m,\boldsymbol{s})}$.

At the decoder, after receiving the channel output $\boldsymbol{y} \in \mathscr{Y}^n$, the decoder looks for a unique message $\hat{m} \in \{1, 2, \cdots, 2^{nR}\}$ for which there exists $a \in J$ with $s(a) = \hat{m}$ and $\phi(a) + B + \in A_\epsilon(X|\boldsymbol{y})$. If it doesn't find such $\hat{m}$ ($Err_{d1}$) or if it finds multiple such $\hat{m}$'s ($Err_{d2}$), it declares error.

We show that if $I_{s.c.}^G(X;S) \leq I_{c.c}^G(X;Y)$, then for any rate

$$R \leq I_{c.c.}^G(X;Y) - \bar{I}(X;S)$$

the probability of all the errors ($Err_e$, $Err_{d1}$ and $Err_{d2}$) approach zero as the block length approaches infinity. Note that by the standard typicality results [20, Theorem 3.1.2] one can show that with probability approaching one as the block length increases, $\phi(a) + B \in A_\epsilon(X|\boldsymbol{y})$. Therefore, the probability of the error event $Err_{d1}$ vanishes as the block length increases. It suffices to show that for any choice of weights $(w_{p,r})_{(p,r)\in\mathscr{Q}(G)}$, the probability of the two error events $Err_e$ and $Err_{d2}$ vanish if

$$\begin{aligned} R_{\text{out}} - R &> \bar{I}(X;S) \\ R_{\text{out}} &< \frac{1}{\omega_\theta}\Big( \log|H_\theta| - H(X|[X]_\theta Y)\Big) \end{aligned}$$

assuming $I_{s.c.}^G(X;S) \leq I_{c.c}^G(X;Y)$.

#### 3.1.2.1 The Error Event $Err_e$

Note that given the message $m$ and the channel state $\boldsymbol{s}$, the error event $Err_e$ occurs if $\alpha(m, \boldsymbol{s}) \leq \frac{|J| \cdot |A_\epsilon^n(X|\boldsymbol{s})|}{2 \cdot 2^{nR} \cdot |G|^n}$. We bound the probability of error using the following

Chebyshev's inequality:

$$P\Big(Err_e|m,\boldsymbol{s}\Big) = P\Big(\alpha(m,\boldsymbol{s}) \leq \frac{|J|\cdot|A_\epsilon^n(X|\boldsymbol{s})|}{2\cdot 2^{nR}\cdot|G|^n}\Big) \leq \frac{\mathrm{var}\{\alpha(m,\boldsymbol{s})\}}{\mathbb{E}\{\alpha(m,\boldsymbol{s})\}^2}$$

We have

$$\begin{aligned}\mathbb{E}\{\alpha(m,\boldsymbol{s})\} &= \sum_{a\in J}\sum_{\boldsymbol{x}\in A_\epsilon^n(X|\boldsymbol{s})} P\Big(\phi(a)+B=\boldsymbol{x}, s(a)=m\Big)\\ &= \frac{|J|\cdot|A_\epsilon^n(X|\boldsymbol{s})|}{2^{nR}\cdot|G|^n}\end{aligned}$$

and

$$\begin{aligned}\mathbb{E}\{\alpha(m,\boldsymbol{s})^2\} &= \sum_{a,\tilde{a}\in J}\sum_{\boldsymbol{x},\tilde{\boldsymbol{x}}\in A_\epsilon^n(X|\boldsymbol{s})} P\Big(\phi(a)+B=\boldsymbol{x},\phi(\tilde{a})+B=\tilde{\boldsymbol{x}}, s(a)=m, s(\tilde{a})=m\Big)\\ &= \sum_{a\in J}\sum_{\boldsymbol{x}\in A_\epsilon^n(X|\boldsymbol{s})}\frac{1}{2^{nR}\cdot|G|^n}\\ &\quad + \sum_{a\in J}\sum_{\boldsymbol{x}\in A_\epsilon^n(X|\boldsymbol{s})}\sum_{\substack{\theta\in\Theta\\ \theta\neq\boldsymbol{r}}}\sum_{\tilde{a}\in T_\theta(a)}\sum_{\substack{\tilde{\boldsymbol{x}}\in A_\epsilon^n(X|\boldsymbol{s})\\ \tilde{x}\in x+H_\theta^n}}\frac{1}{2^{2nR}\cdot|G|^n\cdot|H_\theta|^n}\end{aligned}$$

Therefore,

$$\begin{aligned}\mathrm{var}\{\alpha(m,\boldsymbol{s})\} &= \mathbb{E}\{\alpha(m,\boldsymbol{s})^2\} - \mathbb{E}\{\alpha(m,\boldsymbol{s})\}^2\\ &= \frac{|J|\cdot|A_\epsilon^n(X|\boldsymbol{s})|}{2^{nR}\cdot|G|^n} + \sum_{\substack{\theta\in\Theta\\ \theta\neq\mathbf{0}\\ \theta\neq\boldsymbol{r}}}\sum_{a\in J}\sum_{\boldsymbol{x}\in A_\epsilon^n(X|\boldsymbol{s})}\sum_{\tilde{a}\in T_\theta(a)}\sum_{\substack{\tilde{\boldsymbol{x}}\in A_\epsilon^n(X|\boldsymbol{s})\\ \tilde{x}\in x+H_\theta^n}}\frac{1}{2^{2nR}\cdot|G|^n\cdot|H_\theta|^n}\\ &\leq \frac{|J|\cdot|A_\epsilon^n(X|\boldsymbol{s})|}{2^{nR}\cdot|G|^n} + \sum_{\substack{\theta\in\Theta\\ \theta\neq\mathbf{0}\\ \theta\neq\boldsymbol{r}}}\frac{|J|\cdot 2^{n[H(X|S)+\delta]}\cdot|T_\theta|\cdot 2^{n[H(X|[X]_\theta S)+\delta]}}{2^{2nR}\cdot|G|^n\cdot|H_\theta|^n}\end{aligned}$$

Hence,

$$P\Big(Err_e|m,\boldsymbol{s}\Big) \leq \frac{2^{nR}\cdot|G|^n}{|J|\cdot 2^{n[H(X|S)+\delta]}} + \sum_{\substack{\theta\in\Theta\\ \theta\neq\mathbf{0}\\ \theta\neq\boldsymbol{r}}}\frac{|G|^n\cdot|T_\theta|\cdot 2^{n[H(X|[X]_\theta S)+\delta]}}{|J|\cdot 2^{n[H(X|S)+\delta]}\cdot|H_\theta|^n}$$

Note that $|J| = 2^{nR_{\mathrm{out}}}$ and $|T_\theta| = 2^{n(1-\omega_\theta)R_{\mathrm{out}}}$ and $H(X|S) - H(X|[X]_\theta S) = H([X]_\theta|S)$.

Therefore, for $\theta\in\Theta$, $\theta\neq\mathbf{0}$, and $\theta\neq\boldsymbol{r}$, we require

$$R_{\mathrm{out}} > \frac{1}{\omega_\theta}\Big(\log|G:H_\theta| - H([X]_\theta|S)\Big)$$

$$R_{\mathrm{out}} - R > \log|G| - H(X|S)$$

These conditions are equivalent to the following conditions:

$$R_{\text{out}} > \frac{1}{\omega_\theta}\Big(\log|G:H_\theta| - H([X]_\theta|S)\Big)$$

$$R_{\text{out}} - R > \log|G| - H(X|S)$$

for $\theta \in \Theta$ and $\theta \neq \boldsymbol{r}$.

#### 3.1.2.2 The Error Event $Err_{d2}$

Let $Err = Err_{d2} \cap Err_e^c \cap Err_{d1}^c$. Then the probability of the error event $Err$ is equal to

$$P\Big(Err\Big) = \frac{1}{2^{nR}} \sum_{m=1}^{2^{nR}} \sum_{s^n \in \mathscr{S}^n} p_S^n(\boldsymbol{s}) \sum_{a \in J} \sum_{\boldsymbol{x} \in A_\epsilon^n(X|\boldsymbol{s})} \mathbb{1}_{\{\alpha(m,\boldsymbol{s}) > \frac{|J|\cdot|A_\epsilon^n(X|\boldsymbol{s})|}{2\cdot 2^{nR}\cdot|G|^n}\}} \frac{1}{\alpha(m,\boldsymbol{s})} \mathbb{1}_{\{\phi(a)+B=\boldsymbol{x}, s(a)=m\}}$$

$$\sum_{\boldsymbol{y} \in \mathscr{Y}^n} W^n(\boldsymbol{y}|\boldsymbol{x},\boldsymbol{s}) \sum_{\substack{\tilde{m}=1 \\ \tilde{m}\neq m}}^{2^{nR}} \sum_{\tilde{a} \in J} \sum_{\tilde{\boldsymbol{x}} \in A_\epsilon^n(X|\boldsymbol{y})} \mathbb{1}_{\{\phi(\tilde{a})+B=\tilde{\boldsymbol{x}}, s(\tilde{a})=\tilde{m}\}}$$

$$\leq \frac{1}{2^{nR}} \sum_{m=1}^{2^{nR}} \sum_{s^n \in \mathscr{S}^n} p_S^n(\boldsymbol{s}) \sum_{a \in J} \sum_{\boldsymbol{x} \in A_\epsilon^n(X|\boldsymbol{s})} \frac{2 \cdot 2^{nR} \cdot |G|^n}{|J| \cdot |A_\epsilon^n(X|s^n)|} \mathbb{1}_{\{\phi(a)+B=\boldsymbol{x}, s(a)=m\}}$$

$$\sum_{\boldsymbol{y} \in \mathscr{Y}^n} W^n(\boldsymbol{y}|\boldsymbol{x},\boldsymbol{s}) \sum_{\substack{\tilde{m}=1 \\ \tilde{m}\neq m}}^{2^{nR}} \sum_{\tilde{a} \in J} \sum_{\tilde{\boldsymbol{x}} \in A_\epsilon^n(X|\boldsymbol{y})} \mathbb{1}_{\{\phi(\tilde{a})+B=\tilde{\boldsymbol{x}}, s(\tilde{a})=\tilde{m}\}}$$

Therefore,

$$\begin{aligned}
\mathbb{E}\Big\{P(Err)\Big\} &\leq \frac{1}{2^{nR}}\sum_{m=1}^{2^{nR}}\sum_{\boldsymbol{s}\in\mathscr{S}^n} p_S^n(\boldsymbol{s})\sum_{a\in J}\sum_{\boldsymbol{x}\in A_\epsilon^n(X|\boldsymbol{s})}\frac{2\cdot 2^{nR}\cdot|G|^n}{|J|\cdot|A_\epsilon^n(X|s^n)|}\sum_{\boldsymbol{y}\in\mathscr{Y}^n} W^n(\boldsymbol{y}|\boldsymbol{x},\boldsymbol{s}) \\
&\quad \sum_{\substack{\tilde{m}=1\\ \tilde{m}\neq m}}^{2^{nR}}\sum_{\tilde{a}\in J}\sum_{\tilde{\boldsymbol{x}}\in A_\epsilon^n(X|\boldsymbol{y})} P\Big(\phi(a)+B=\boldsymbol{x},\phi(\tilde{a})+B=\tilde{\boldsymbol{x}},s(a)=m,s(\tilde{a})=\tilde{m}\Big) \\
&\leq \frac{1}{2^{nR}}\sum_{m=1}^{2^{nR}}\sum_{s^n\in\mathscr{S}^n} p_S^n(\boldsymbol{s})\sum_{a\in J}\sum_{\boldsymbol{x}\in A_\epsilon^n(X|\boldsymbol{s})}\frac{2\cdot 2^{nR}\cdot|G|^n}{|J|\cdot|A_\epsilon^n(X|s^n)|}\sum_{\boldsymbol{y}\in\mathscr{Y}^n} W^n(\boldsymbol{y}|\boldsymbol{x},\boldsymbol{s}) \\
&\quad \sum_{\substack{\tilde{m}=1\\ \tilde{m}\neq m}}^{2^{nR}}\sum_{\theta\in\Theta}\sum_{\tilde{a}\in T_\theta(a)}\sum_{\substack{\tilde{\boldsymbol{x}}\in A_\epsilon^n(X|\boldsymbol{y})\\ \tilde{\boldsymbol{x}}\in\boldsymbol{x}+H_\theta^n}}\frac{1}{|G|^n\cdot|H_\theta|^n\cdot 2^{2nR}} \\
&\leq \sum_{\substack{\theta\in\Theta\\ \theta\neq\boldsymbol{r}}}\frac{|T_\theta|\cdot 2^{n[H(X|[X]_\theta Y)+\delta]}\cdot 2}{|H_\theta|^n}
\end{aligned}$$

Therefore, we require to have

$$R_{out} < I_{c.c.}^G(X;Y)$$

## 3.2 Nested Codes for Sources with Side Information

Consider a point to point source coding problem with side information available at the decoder. Denote the source by $(\mathscr{X},\mathscr{S},\mathscr{U},p_{XS},d)$ where $\mathscr{X}$, $\mathscr{S}$ and $\mathscr{U}$ are the source, side information and reconstruction alphabets correspondingly, $p_{XS}$ is the joint distribution of the source and the side information and $d:\mathscr{X}\times\mathscr{U}\to\mathbb{R}^+$ is the measure of reconstruction. We assume $\mathscr{U}=G$ for some Abelian group $G$. We study the performance of "nested random/group codes" and "nested group/random codes" for this problem. These ensembles can be used in multi-terminal communications problems such as the distributed source coding and the multiple description coding.

### 3.2.1 Nested Random/Group Codes for Source Coding

We employ a nested code in which the inner code is a group code and the outer code consists of random shifts of the inner code. Let $\mathbb{C}_{\text{in}}=\{\phi(a)|a\in J\}$ where $\phi$ and

$J$ are defined in (2.11) and (2.14) respectively and let

$$\mathbb{C}_{\text{out}} = \bigcup_{m=1}^{2^{nR}} \Big( \mathbb{C}_{\text{in}} + B_m \Big)$$

where $B_m$'s are iid random variables distributed uniformly over $G^n$. Note that the rates of the inner and outer codes are equal to $R_{\text{in}} = \frac{1}{n} \log |J|$ and $R_{\text{out}} = R_{\text{in}} + R$ where $R$ is the compression rate of our coding scheme.

The encoding and decoding rules are as follows: Given a source sequence $\boldsymbol{x} \in \mathscr{X}^n$, define

$$\alpha(\boldsymbol{x}) = \sum_{m=1}^{2^{nR}} \sum_{a \in J} \sum_{\boldsymbol{u} \in A_\epsilon^n(U|\boldsymbol{x})} \mathbb{1}_{\{\phi(a)+B_m=\boldsymbol{u}\}}$$

Note that if $\alpha(\boldsymbol{x}) > 0$, then there exists at least one $m \in \{1, \cdots, 2^{nR}\}$ and one $a \in J$ with $\phi(a) + B_m \in A_\epsilon^n(U|\boldsymbol{x})$. In this case, the encoder picks one such pair and sends $m$ to the channel. The encoder will declare an encoding error if $\alpha(\boldsymbol{x}) = 0$. Although it may be unnecessary, it is convenient in the proofs to assume that the encoder declares error if $\alpha(\boldsymbol{x}) \leq \frac{2^{nR} \cdot |J| \cdot |A_\epsilon^n(U|\boldsymbol{x})|}{2 \cdot |G|^n}$. We denote this error event by $Err_e$. We also assume that the pair $(a, m)$ is picked with probability $\frac{\sum_{\boldsymbol{u} \in A_\epsilon^n(U|\boldsymbol{x})} \mathbb{1}_{\{\phi(a)+s_i=\boldsymbol{u}\}}}{\alpha(\boldsymbol{x})}$.

At the decoder, having access to $\boldsymbol{s}$ and $m$, the decoder looks for a unique $\hat{a} \in J$ such that $\phi(\hat{a}|) + B_m \in A_\epsilon^n(U|\boldsymbol{s})$. If it doesn't find such $\hat{a}$ ($Err_{d1}$) or if it finds multiple such $\hat{a}$'s ($Err_{d2}$), it declares error.

We show that if

$$R \leq \bar{I}(U;X) - I_{c.c.}^G(U;S)$$

then the probability of all the errors ($Err_e$, $Err_{d1}$ and $Err_{d2}$) approach zero as the block length approaches infinity. Note that by the standard typicality results [20,

Theorem 3.1.2] one can show that with probability approaching one as the block length increases, $\phi(a) + B_m \in A_\epsilon(U|\boldsymbol{x})$. Therefore, the probability of the error event $Err_{d1}$ vanishes as the block length increases. It suffices to show that for any choice of weights $(w_{p,r})_{(p,r)\in\mathscr{Q}(G)}$, the probability of the two error events $Err_e$ and $Err_{d2}$ vanish if

$$R + R_{\text{in}} > \bar{I}(U;X)$$
$$R_{\text{in}} < I^G_{c.c.}(U;S)$$

We first show that the error events vanish if for any $\theta \in \Theta$, $\theta \neq \mathbf{0}$,

$$R + \omega_\theta R_{\text{in}} > \bar{I}([U]_\theta;X)$$
$$R_{\text{in}} < I^G_{c.c.}(U;S)$$

#### 3.2.1.1 The Error Event $Err_e$

Note that given the source sequence $\boldsymbol{x}$, the error event $Err_e$ occurs if $\alpha(\boldsymbol{x}) \leq \frac{2^{nR}\cdot|J|\cdot|A^n_\epsilon(U|\boldsymbol{x})|}{2\cdot|G|^n}$. We bound the probability of error using the following Chebyshev's inequality:

$$P\Big(Err_e|\boldsymbol{x}\Big) = P\Big(\alpha(\boldsymbol{x}) \leq \frac{2^{nR}\cdot|J|\cdot|A^n_\epsilon(U|\boldsymbol{x})|}{2\cdot|G|^n}\Big) \leq \frac{\text{var}\{\alpha(\boldsymbol{x})\}}{\mathbb{E}\{\alpha(\boldsymbol{x})\}^2}$$

We have

$$\begin{aligned}\mathbb{E}\{\alpha(\boldsymbol{x})\} &= \sum_{m=1}^{2^{nR}}\sum_{a\in J}\sum_{\boldsymbol{u}\in A^n_\epsilon(U|\boldsymbol{x})} P\Big(\phi(a)+B_m=\boldsymbol{u}\Big)\\ &= \frac{2^{nR}\cdot|J|\cdot|A^n_\epsilon(U|\boldsymbol{x})|}{|G|^n}\end{aligned}$$

and

$$\begin{aligned}
\mathbb{E}\{\alpha(\boldsymbol{x})^2\} &= \sum_{m,\tilde{m}=1}^{2^{nR}} \sum_{a,\tilde{a}\in J} \sum_{\boldsymbol{u},\tilde{\boldsymbol{u}}\in A_\epsilon^n(U|\boldsymbol{s})} P\Big(\phi(a)+B_m=\boldsymbol{u}, \phi(\tilde{a})+B_m=\tilde{\boldsymbol{u}}\Big) \\
&= \sum_{m=1}^{2^{nR}} \sum_{a\in J} \sum_{\boldsymbol{u}\in A_\epsilon^n(U|\boldsymbol{x})} \sum_{\theta\in\Theta} \sum_{\tilde{a}\in T_\theta(a)} \sum_{\substack{\tilde{\boldsymbol{u}}\in A_\epsilon^n(U|\boldsymbol{x}) \\ \tilde{\boldsymbol{u}}\in \boldsymbol{u}+H_\theta^n}} \frac{1}{|G|^n\cdot|H_\theta|^n} \\
&\qquad + \sum_{\substack{m,\tilde{m}=1 \\ \tilde{m}\neq m}}^{2^{nR}} \sum_{a,\tilde{a}\in J} \sum_{\boldsymbol{u},\tilde{\boldsymbol{u}}\in A_\epsilon^n(U|\boldsymbol{s})} \frac{1}{|G|^{2n}} \\
&\leq \sum_{\substack{\theta\in\Theta \\ \theta\neq\mathbf{0}}} \frac{2^{nR}\cdot|J|\cdot 2^{n[H(U|X)+\delta]}\cdot|T_\theta|\cdot 2^{n[H(U|[U]_\theta X)+\delta]}}{|G|^n\cdot|H_\theta|^n} + \frac{2^{2nR}\cdot|J|^2\cdot|A_\epsilon^n(U|\boldsymbol{x})|^2}{|G|^{2n}}
\end{aligned}$$

Therefore,

$$\begin{aligned}
\mathrm{var}\{\alpha(\boldsymbol{x})\} &= \mathbb{E}\{\alpha(\boldsymbol{x})^2\} - \mathbb{E}\{\alpha(\boldsymbol{x})\}^2 \\
&\leq \sum_{\substack{\theta\in\Theta \\ \theta\neq\mathbf{0}}} \frac{2^{nR}\cdot|J|\cdot 2^{n[H(U|X)+\delta]}\cdot|T_\theta|\cdot 2^{n[H(U|[U]_\theta X)+\delta]}}{|G|^n\cdot|H_\theta|^n}
\end{aligned}$$

Hence,

$$P\Big(Err_e|\boldsymbol{x}\Big) \leq \sum_{\substack{\theta\in\Theta \\ \theta\neq\mathbf{0}}} \frac{|G|^n\cdot|T_\theta|\cdot 2^{n[H(X|[X]_\theta S)+\delta]}}{2^{nR}\cdot|J|\cdot 2^{n[H(X|S)+\delta]}\cdot|H_\theta|^n}$$

Note that $|J| = 2^{nR_{\text{in}}}$ and $|T_\theta| = 2^{n(1-\omega_\theta)R_{\text{in}}}$ and $H(U|X) - H(U|[U]_\theta X) = H([U]_\theta|X)$. Therefore, for $\theta\in\Theta$ and $\theta\neq\mathbf{0}$, we require

$$R + \omega_\theta R_{\text{in}} > \Big(\log|G:H_\theta| - H([U]_\theta|X)\Big)$$

#### 3.2.1.2 The Error Event $Err_{d2}$

Let $Err = Err_{d2}\cap Err_e^c\cap Err_{d1}^c$. Then the probability of the error event $Err$ is equal to

$$\begin{aligned}
P\Big(Err\Big) \leq \sum_{\boldsymbol{x}\in\mathscr{X}^n} \sum_{\boldsymbol{s}\in\mathscr{S}^n} p_{XS}^n(\boldsymbol{x},\boldsymbol{s}) \sum_{m=1}^{2^{nR}} \sum_{a\in J} \sum_{\boldsymbol{u}\in A_\epsilon^n(U|\boldsymbol{x})} \frac{\mathbb{1}_{\{\phi(a)+B_m=\boldsymbol{u}\}}}{\alpha(\boldsymbol{x})} \\
\sum_{\substack{\tilde{a}\in J \\ \tilde{a}\neq a}} \sum_{\tilde{\boldsymbol{u}}\in A_\epsilon^n(U|\boldsymbol{s})} \mathbb{1}_{\{\phi(\tilde{a})+B_m=\tilde{\boldsymbol{u}}\}}
\end{aligned}$$

Therefore,

$$\begin{aligned}
\mathbb{E}\Big\{P(Err)\Big\} &\leq \sum_{\boldsymbol{x}\in\mathscr{X}^n}\sum_{\boldsymbol{s}\in\mathscr{S}^n} p^n_{XS}(\boldsymbol{x},\boldsymbol{s}) \sum_{m=1}^{2^{nR}} \sum_{a\in J}\sum_{\boldsymbol{u}\in A^n_\epsilon(U|\boldsymbol{x})} \frac{2\cdot|G|^n}{2^{nR}\cdot|J|\cdot|A^n_\epsilon(U|\boldsymbol{x})|} \\
&\qquad \sum_{\substack{\tilde{a}\in J\\ \tilde{a}\neq a}}\sum_{\tilde{\boldsymbol{u}}\in A^n_\epsilon(U|\boldsymbol{s})} P\Big(\phi(a)+B_m=\boldsymbol{u},\phi(\tilde{a})+B_m=\tilde{\boldsymbol{u}}\Big) \\
&\leq \sum_{\boldsymbol{x}\in\mathscr{X}^n}\sum_{\boldsymbol{s}\in\mathscr{S}^n} p^n_{XS}(\boldsymbol{x},\boldsymbol{s}) \sum_{m=1}^{2^{nR}} \sum_{a\in J}\sum_{\boldsymbol{u}\in A^n_\epsilon(U|\boldsymbol{x})} \frac{2\cdot|G|^n}{2^{nR}\cdot|J|\cdot|A^n_\epsilon(U|\boldsymbol{x})|} \\
&\qquad \sum_{\substack{\theta\in\Theta\\ \theta\neq\boldsymbol{r}}}\sum_{\tilde{a}\in T_\theta(a)}\sum_{\substack{\tilde{\boldsymbol{u}}\in A^n_\epsilon(U|\boldsymbol{s})\\ \tilde{\boldsymbol{u}}\in\boldsymbol{u}+H^n_\theta}} \frac{1}{|G|^n\cdot|H_\theta|^n} \\
&\leq \sum_{\substack{\theta\in\Theta\\ \theta\neq\boldsymbol{r}}} \frac{|T_\theta|\cdot 2^{n[H(U|[U]_\theta S)+\delta]}}{|H_\theta|^n}
\end{aligned}$$

Therefore, we require to have $R_{\text{in}} < \frac{1}{1-\omega_\theta}\Big(\log|H_\theta| - H(U|[U]_\theta X)\Big)$ for all $\theta\in\Theta$, $\theta\neq\boldsymbol{r}$. Equivalently,

$$R_{\text{in}} < I^G_{c.c.}(U;S)$$

#### 3.2.1.3 Simplification of the Rate Region

In this section, we show that if $R_{\text{in}} < I^G_{c.c.}(U;S)$ then

$$\max_{\substack{\theta\in\Theta\\ \theta\neq\mathbf{0}}}\Big(\log|G:H_\theta| - H([U]_\theta|X) - \omega_\theta R_{\text{in}}\Big) = \log|G| - H(U|X) - R_{\text{in}}$$

We show this by contradiction. Note that the right-hand-side is equal to the left-hand-side for $\theta=\boldsymbol{r}$. Assume for some $\theta\in\Theta$, $\theta\neq\mathbf{0}$,

$$\log|G:H_\theta| - H(U|[U]_\theta X) - \omega_\theta R_{\text{in}} > \log|G| - H(U|X) - R_{\text{in}}$$

Then we have

$$\begin{aligned}
(1-\omega_\theta)R_{\text{in}} &> \log|G| - H(U|X) - \Big(\log|G:H_\theta| - H(U|[U]_\theta X)\Big) \\
&= \log|H_\theta| - H([U]_\theta|X)
\end{aligned}$$

which is a contradiction by the definition of $I^G_{c.c.}(U;S)$ if we have the Markov chain $U\leftrightarrow X\leftrightarrow S$.

### 3.2.2 Nested Group/Random Codes for Source Coding

We employ a nested code in which the outer code is a group code and the inner code is a random subset of the outer code. Let $\mathbb{C}_{\text{out}} = \{\phi(a) + B | a \in J\}$ where $\phi$ and $J$ are defined in (2.11) and (2.14) respectively and $B$ is uniformly distributed over $G^n$. Define the mapping $s : J \to \{1, 2, \cdots, 2^{nR}\}$ such that for $a \in J$, $s(a)$'s are iid random variables uniformly distributed over $\{1, 2, \cdots, 2^{nR}\}$ where $R$ is the communication rate of the coding scheme. Note that the rates of the inner and outer codes are equal to $R_{\text{out}} = \frac{1}{n} \log |J|$ and $R_{\text{in}} = R_{\text{out}} - R$.

The encoding and decoding rules are as follows: Given a source sequence $\boldsymbol{x} \in \mathscr{X}^n$, define

$$\alpha(\boldsymbol{x}) = \sum_{a \in J} \sum_{\boldsymbol{u} \in A_\epsilon^n(U|\boldsymbol{x})} \mathbb{1}_{\{\phi(a)+B=\boldsymbol{u}\}}$$

Note that if $\alpha(\boldsymbol{x}) > 0$, then there exists at least one $a \in J$ with $\phi(a) + B \in A_\epsilon^n(U|\boldsymbol{x})$. In this case, the encoder picks one such pair and sends $m = s(a)$ to the channel. The encoder will declare an encoding error if $\alpha(\boldsymbol{x}) = 0$. Although it may be unnecessary, it is convenient in the proofs to assume that the encoder declares error if $\alpha(\boldsymbol{x}) \leq \frac{|J| \cdot |A_\epsilon^n(U|\boldsymbol{x})|}{2 \cdot |G|^n}$. We denote this error event by $Err_e$. We also assume that $a \in J$ is picked with probability $\frac{\sum_{\boldsymbol{u} \in A_\epsilon^n(U|\boldsymbol{x})} \mathbb{1}_{\{\phi(a)+B=\boldsymbol{u}\}}}{\alpha(\boldsymbol{x})}$.

At the decoder, having access to $\boldsymbol{s}$ and $m$, the decoder looks for a unique $\hat{a} \in J$ such that $\phi(\hat{a}|) + B \in A_\epsilon^n(U|\boldsymbol{s})$ and $s(\hat{a}) = m$. If it doesn't find such $\hat{a}$ ($Err_{d1}$) or if it finds multiple such $\hat{a}$'s ($Err_{d2}$), it declares error.

We show that if

$$R \leq I_{s.c.}^G(U; X) - \bar{I}(U; S)$$

then the probability of all the errors ($Err_e$, $Err_{d1}$ and $Err_{d2}$) approach zero as the block length approaches infinity. Note that by the standard typicality results [20, Theorem 3.1.2] one can show that with probability approaching one as the block length increases, $\phi(a) + B \in A_\epsilon(U|\boldsymbol{x})$. Therefore, the probability of the error event $Err_{d1}$ vanishes as the block length increases. It suffices to show that for any choice of weights $(w_{p,r})_{(p,r)\in\mathscr{Q}(G)}$, the probability of the two error events $Err_e$ and $Err_{d2}$ vanish if

$$R_{\text{out}} > I^G_{s.c.}(U;X)$$
$$R_{\text{out}} - R < \bar{I}(U;S)$$

#### 3.2.2.1 The Error Event $Err_e$

Note that given the source sequence $\boldsymbol{x}$, the error event $Err_e$ occurs if $\alpha(\boldsymbol{x}) \leq \frac{|J|\cdot|A^n_\epsilon(U|\boldsymbol{x})|}{2\cdot|G|^n}$. We bound the probability of error using the following Chebyshev's inequality:

$$P\Big(Err_e|\boldsymbol{x}\Big) = P\Big(\alpha(\boldsymbol{x}) \leq \frac{|J|\cdot|A^n_\epsilon(U|\boldsymbol{x})|}{2\cdot|G|^n}\Big) \leq \frac{\text{var}\{\alpha(\boldsymbol{x})\}}{\mathbb{E}\{\alpha(\boldsymbol{x})\}^2}$$

We have

$$\begin{aligned}\mathbb{E}\{\alpha(\boldsymbol{x})\} &= \sum_{m=1}^{2^{nR}}\sum_{a\in J}\sum_{\boldsymbol{u}\in A^n_\epsilon(U|\boldsymbol{x})} P\Big(\phi(a)+B=\boldsymbol{u}, s(a)=m\Big)\\ &= \frac{|J|\cdot|A^n_\epsilon(U|\boldsymbol{x})|}{|G|^n}\end{aligned}$$

and

$$\begin{aligned}\mathbb{E}\{\alpha(\boldsymbol{x})^2\} &= \sum_{m,\tilde{m}=1}^{2^{nR}}\sum_{a,\tilde{a}\in J}\sum_{\boldsymbol{u},\tilde{\boldsymbol{u}}\in A^n_\epsilon(U|\boldsymbol{s})} P\Big(\phi(a)+B_m=\boldsymbol{u}, \phi(\tilde{a})+B_m=\tilde{\boldsymbol{u}}, s(a)=m, s(\tilde{a})=\tilde{m}\Big)\\ &= \sum_{m,\tilde{m}=1}^{2^{nR}}\sum_{a\in J}\sum_{\boldsymbol{u}\in A^n_\epsilon(U|\boldsymbol{x})}\sum_{\theta\in\Theta}\sum_{\tilde{a}\in T_\theta(a)}\sum_{\substack{\tilde{\boldsymbol{u}}\in A^n_\epsilon(U|\boldsymbol{x})\\ \tilde{\boldsymbol{u}}\in\boldsymbol{u}+H^n_\theta}}\frac{1}{|G|^n\cdot|H_\theta|^n\cdot 2^{2nR}}\\ &\leq \sum_{\theta\in\Theta}\frac{|J|\cdot 2^{n[H(U|X)+\delta]}\cdot|T_\theta|\cdot 2^{n[H(U|[U]_\theta X)+\delta]}}{|G|^n\cdot|H_\theta|^n}\end{aligned}$$

Therefore,

$$\begin{aligned}\mathrm{var}\{\alpha(\boldsymbol{x})\} &= \mathbb{E}\{\alpha(\boldsymbol{x})^2\} - \mathbb{E}\{\alpha(\boldsymbol{x})\}^2 \\ &\leq \sum_{\substack{\theta\in\Theta \\ \theta\neq\mathbf{0}}} \frac{|J|\cdot 2^{n[H(U|X)+\delta]}\cdot|T_\theta|\cdot 2^{n[H(U|[U]_\theta X)+\delta]}}{|G|^n\cdot|H_\theta|^n}\end{aligned}$$

Hence,

$$P\Big(Err_e|\boldsymbol{x}\Big) \leq \sum_{\substack{\theta\in\Theta \\ \theta\neq\mathbf{0}}} \frac{|G|^n\cdot|T_\theta|\cdot 2^{n[H(X|[X]_\theta S)+\delta]}}{|J|\cdot 2^{n[H(X|S)+\delta]}\cdot|H_\theta|^n}$$

Note that $|J| = 2^{nR_{\text{out}}}$ and $|T_\theta| = 2^{n(1-\omega_\theta)R_{\text{out}}}$ and $H(U|X) - H(U|[U]_\theta X) = H([U]_\theta|X)$. Therefore, for $\theta\in\Theta$ and $\theta\neq\mathbf{0}$, we require

$$\omega_\theta R_{\text{out}} > \Big(\log|G:H_\theta| - H([U]_\theta|X)\Big)$$

Equivalently, we require

$$R_{\text{out}} > I^G_{s.c.}(U;X)$$

#### 3.2.2.2 The Error Event $Err_{d2}$

Let $Err = Err_{d2}\cap Err_e^c\cap Err_{d1}^c$. Then the probability of the error event $Err$ is equal to

$$P\Big(Err\Big) \leq \sum_{\boldsymbol{x}\in\mathscr{X}^n}\sum_{\boldsymbol{s}\in\mathscr{S}^n} p^n_{XS}(\boldsymbol{x},\boldsymbol{s})\sum_{m=1}^{2^{nR}}\sum_{a\in J}\sum_{\boldsymbol{u}\in A^n_\epsilon(U|\boldsymbol{x})}\frac{\mathbb{1}_{\{\phi(a)+B=\boldsymbol{u},s(a)=m\}}}{\alpha(\boldsymbol{x})}$$
$$\sum_{\substack{\tilde{a}\in J\\ \tilde{a}\neq a}}\sum_{\tilde{\boldsymbol{u}}\in A^n_\epsilon(U|\boldsymbol{s})}\mathbb{1}_{\{\phi(\tilde{a})+B_m=\tilde{\boldsymbol{u}},s(\tilde{a})=m\}}$$

Therefore,

$$\begin{aligned}
\mathbb{E}\Big\{P(Err)\Big\} &\leq \sum_{\boldsymbol{x}\in\mathscr{X}^n}\sum_{\boldsymbol{s}\in\mathscr{S}^n} p^n_{XS}(\boldsymbol{x},\boldsymbol{s}) \sum_{m=1}^{2^{nR}}\sum_{a\in J}\sum_{\boldsymbol{u}\in A^n_\epsilon(U|\boldsymbol{x})} \frac{2\cdot|G|^n}{2^{2nR}\cdot|J|\cdot|A^n_\epsilon(U|\boldsymbol{x})|} \\
&\qquad \sum_{\substack{\tilde{a}\in J\\ \tilde{a}\neq a}}\sum_{\tilde{\boldsymbol{u}}\in A^n_\epsilon(U|\boldsymbol{s})} P\Big(\phi(a)+B_m=\boldsymbol{u},\phi(\tilde{a})+B_m=\tilde{\boldsymbol{u}}\Big) \\
&\leq \sum_{\boldsymbol{x}\in\mathscr{X}^n}\sum_{\boldsymbol{s}\in\mathscr{S}^n} p^n_{XS}(\boldsymbol{x},\boldsymbol{s}) \sum_{m=1}^{2^{nR}}\sum_{a\in J}\sum_{\boldsymbol{u}\in A^n_\epsilon(U|\boldsymbol{x})} \frac{2\cdot|G|^n}{2^{2nR}\cdot|J|\cdot|A^n_\epsilon(U|\boldsymbol{x})|} \\
&\qquad \sum_{\substack{\theta\in\Theta\\ \theta\neq\boldsymbol{r}}}\sum_{\tilde{a}\in T_\theta(a)}\sum_{\substack{\tilde{\boldsymbol{u}}\in A^n_\epsilon(U|\boldsymbol{s})\\ \tilde{\boldsymbol{u}}\in\boldsymbol{u}+H_{\theta^n}}} \frac{1}{|G|^n\cdot|H_\theta|^n} \\
&\leq \sum_{\substack{\theta\in\Theta\\ \theta\neq\boldsymbol{r}}} \frac{|T_\theta|\cdot 2^{n[H(U|[U]_\theta S)+\delta]}}{2^{nR}\cdot|H_\theta|^n}
\end{aligned}$$

Therefore, we require to have $(1-\omega_\theta)R_{\text{out}} - R < \Big(\log|H_\theta| - H(U|[U]_\theta S)\Big)$ for all $\theta\in\Theta$, $\theta\neq\boldsymbol{r}$.

#### 3.2.2.3 Simplification of the Rate Region

In this section, we show that if $R_{\text{out}} > I^G_{s.c.}(U;X)$ then

$$\max_{\substack{\theta\in\Theta\\ \theta\neq\boldsymbol{r}}}(1-\omega_\theta)R_{\text{out}} - \Big(\log|H_\theta| - H(U|[U]_\theta S)\Big) = R_{\text{out}} - \Big(\log|G| - H(U|S)\Big)$$

We show this by contradiction. Note that the right-hand-side is equal to the left-hand-side for $\theta=\mathbf{0}$. Assume for some $\theta\in\Theta$, $\theta\neq\boldsymbol{r}$,

$$(1-\omega_\theta)R_{\text{out}} - \Big(\log|H_\theta| - H(U|[U]_\theta S)\Big) > R_{\text{out}} - \Big(\log|G| - H(U|S)\Big)$$

Then we have

$$\begin{aligned}
\omega_\theta R_{\text{out}} &< \log|G| - H(U|S) - \Big(\log|H_\theta| - H(U|[U]_\theta S)\Big) \\
&= \log|G:H_\theta| - H([U]_\theta|S)
\end{aligned}$$

which is a contradiction by the definition of $I^G_{s.c.}(U;S)$ if the Markov chain $U\leftrightarrow X\leftrightarrow S$ holds.

## 3.3 Distributed Source Coding

In this section, we consider a distributed source coding problem with one distortion constraint and provide an information-theoretic inner bound to the optimal rate-distortion region using group codes. This inner bound strictly contains the available bounds based on random codes.

### 3.3.1 Preliminaries

#### 3.3.1.1 The Source Model

Consider two distributed sources generating discrete random variables $X$ and $Y$. Assume $X$ and $Y$ take values from alphabets $\mathscr{X}$ and $\mathscr{Y}$ respectively with joint distribution $p_{XY}(\cdot,\cdot)$. The source sequence $(X^n, Y^n)$ is independent over time and has the product distribution $P((X^n,Y^n) = (\boldsymbol{x},\boldsymbol{y})) = \prod_{i=1}^n p_{XY}(x_i,y_i)$ for $\boldsymbol{x} = (x_1,\cdots,x_n) \in \mathscr{X}^n$ and $\boldsymbol{y} = (y_1,\cdots,y_n) \in \mathscr{Y}^n$. We consider the following distributed source coding problem: The two components, $X$ and $Y$, of the source are observed by two encoders which do not communicate with each other. Each encoder communicates a compressed version of its input through a noiseless channel to a joint decoder. For a discrete set $\mathscr{Z}$, the decoder wishes to reconstruct a function $f : \mathscr{X} \times \mathscr{Y} \to \mathscr{Z}$ of the sources with respect to a general fidelity criterion. Let $\hat{\mathscr{Z}}$ denote the reconstruction alphabet, and the fidelity criterion is characterized by a mapping: $d : \mathscr{X} \times \mathscr{Y} \times \hat{\mathscr{Z}} \to \mathbb{R}^+$. We restrict our attention to additive distortion measures, i.e., the distortion among three $n$-length sequences $\boldsymbol{x} = (x_1,\cdots,x_n) \in \mathscr{X}^n$, $\boldsymbol{y} = (y_1,\cdots,y_n) \in \mathscr{Y}^n$ and $\hat{\boldsymbol{z}} = (\hat{z}_1,\cdots,\hat{z}_n) \in \hat{\mathscr{Z}}^n$ is given by

$$d(\boldsymbol{x},\boldsymbol{y},\hat{\boldsymbol{z}}) \triangleq \frac{1}{n}\sum_{i=1}^{n} d(x_i,y_i,\hat{z}_i).$$

We denote this distributed source by $(\mathscr{X},\mathscr{Y},\hat{\mathscr{Z}},p_{XY},d)$.

#### 3.3.1.2 Achievability and the Rate-Distortion Region

Given a distributed source $(\mathscr{X}, \mathscr{Y}, \mathscr{Z}, p_{XY}, d)$, a transmission system with parameters $(n, \Theta_1, \Theta_2, \Delta)$ is defined by the set of mappings

$$\mathrm{Enc}_1 \colon \mathscr{X}^n \to \{1, 2, \ldots, \Theta_1\}, \qquad \mathrm{Enc}_2 \colon \mathscr{Y}^n \to \{1, 2, \ldots, \Theta_2\} \tag{3.1}$$

$$\mathrm{Dec} \colon \{1, \ldots, \Theta_1\} \times \{1, \ldots, \Theta_2\} \to \hat{\mathscr{Z}}^n \tag{3.2}$$

such that the following constraint is satisfied.

$$\mathbb{E}\Big\{ d\Big( X^n, Y^n, \mathrm{Dec}\left( \mathrm{Enc}_1(X^n), \mathrm{Enc}_2(Y^n) \right) \Big) \Big\} \leq \Delta. \tag{3.3}$$

We say that a tuple $(R_1, R_2, D)$ is achievable if for all $\epsilon > 0$ and for all sufficiently large $n$, there exists a transmission system with parameters $(n, \Theta_1, \Theta_2, \Delta)$ such that

$$\frac{1}{n} \log \Theta_i \leq R_i + \epsilon \quad \text{for } i = 1, 2$$
$$\Delta \leq D + \epsilon.$$

The performance limit is given by the optimal rate-distortion region which is defined as the set of all achievable tuples $(R_1, R_2, D)$.

#### 3.3.1.3 The Berger-Tung Region

An achievable rate region for the problem defined in Section 3.3.1.2 can be obtained based on the Berger-Tung coding scheme [15, 70] as follows: Let $\mathscr{U}$ and $\mathscr{V}$ be two finite sets and let $U$ and $V$ be two auxiliary random variables distributed over $\mathscr{U}$ and $\mathscr{V}$ according to the conditional probabilities $P_{U|X}$ and $P_{V|Y}$ respectively. Define $g \colon \mathscr{U} \times \mathscr{V} \to \hat{\mathscr{Z}}$ as that function of $U$ and $V$ that gives the optimal reconstruction $\hat{Z}$ with respect to the distortion measure $d(\cdot, \cdot, \cdot)$ so that $\mathbb{E}\{d(X, Y, g(U, V))\}$ is minimized.

With these definitions, an achievable rate region for this problem is as follows: For a given distributed source $(\mathscr{X}, \mathscr{Y}, \mathscr{Z}, p_{XY}, d)$ let $D$ be a distortion level for the reconstruction. Let $U$ and $V$ be auxiliary random variables for which there exists a function $g(\cdot,\cdot)$ such that $\mathbb{E}\{d(X,Y,g(U,V))\} \leq D$. Then the rate-distortion tuple $(R_1, R_2, D)$ is achievable if

$$R_1 \geq I(X;U|V)$$
$$R_2 \geq I(Y;V|U)$$
$$R_1 + R_2 \geq I(XY;UV)$$

This assertion follows from the analysis of the Berger-Tung problem [15, 70] in a straightforward way.

#### 3.3.1.4 The Korner-Marton and the Ahlswede-Han Schemes

Consider a distributed source coding problem in which two distributed binary sources $X$ and $Y$ seek to communicate the sum of the two sources $Z = X + Y$ to a centralized decoder losslessly. Korner and Marton [41] propose a coding scheme based on binary linear codes to achieve the rates $R_1 = R_2 = H(Z)$. For certain cases, this rate is not achievable using the Berger-Tung scheme. Ahlswede and Han [9] propose a two layered coding scheme, consisting a Berger-Tung layer and a Korner-Marton layer to achieve the following rate region: Let $P$ and $Q$ be finite auxiliary random variables satisfying the Markov chain $P \leftrightarrow X \leftrightarrow Y \leftrightarrow Q$. Then the rate pair $(R_1, R_2)$ is achievable if

$$R_1 \geq I(X;P|Q) + H(Z|PQ)$$
$$R_2 \geq I(Y;Q|P) + H(Z|PQ)$$
$$R_1 + R_2 \geq I(XY;PQ) + 2H(Z|PQ)$$

### 3.3.2 The Main Result

In this section, we provide an inner bound to the achievable rate-distortion region which strictly contains the Berger-Tung rate region. The following theorem is the main result of this section.

**Theorem III.1.** *For the distributed source $(\mathscr{X}, \mathscr{Y}, \mathscr{Z}, p_{XY}, d)$, let $U$, $V$, $P$ and $Q$ be random variables jointly distributed with $XY$ such that $U$ and $V$ take values from an Abelian group $G$, and $P$ and $Q$ take values from finite sets $\mathscr{P}$ and $\mathscr{Q}$ respectively. Assume the following Markov chains hold*

$$P \leftrightarrow X \leftrightarrow Y \leftrightarrow Q$$

$$U \leftrightarrow (P, X) \leftrightarrow (Y, Q) \leftrightarrow V$$

*and assume there exists a function $g : G \times \mathscr{P} \times \mathscr{Q} \to \hat{\mathscr{Z}}$ such that*

$$\mathbb{E}\Big\{ d(X, Y, g(Z, P, Q)) \Big\} \leq D$$

*for $Z = U + V$ where $+$ is the group operation. We show that with these definitions the rate-distortion triple $(R_1, R_2, D)$ is achievable where*

$$R_1 \geq I(X; P|Q) + \bar{I}(U; XP) - I^G_{c.c.}(Z; PQ)$$

$$R_2 \geq I(Y; Q|P) + \bar{I}(V; YQ) - I^G_{c.c.}(Z; PQ)$$

$$R_1 + R_2 \geq I(XY; PQ) + \bar{I}(UV|XYPQ) - 2I^G_{c.c.}(Z; PQ)$$

Note that the case where $U$ and $V$ are trivial, corresponds to the Berger-Tung scheme and the case where $P$ and $Q$ are trivial, $U = X$, $V = Y$ and the alphabets are binary corresponds to the Korner-Marton scheme. When $P$ and $Q$ are non-trivial, $U = X$, $V = Y$ and the alphabets are binary this scheme corresponds to the Ahlswede-Han scheme.

### 3.3.3 The Coding Scheme

In order to show the achievability, it suffices to show the achievability of the following corner point:

$$R_1 = I(X;P) + \bar{I}(U;XP) - I^G_{c.c.}(Z;PQ)$$
$$R_2 = I(Y;Q|P) + \bar{I}(V;YQ) - I^G_{c.c.}(Z;PQ)$$

To show the achievability, we use a random coding argument as follows: Let $\mathbb{C}_p$ be the code designed for the random variable $P$ defined as follows:

$$\mathbb{C}_p = \left\{\mathbb{C}_p(1), \mathbb{C}_p(2), \cdots, \mathbb{C}_p(2^{nR_p})\right\}$$

where $R_p$ is the rate of this code and for $i = 1, \cdots, 2^{nR_p}$, $\mathbb{C}_p(i)$'s are iid random variables uniformly distributed over $A^n_\epsilon(P)$. For the random variable $Q$, we use a nested code in which the outer code is defined as

$$\mathbb{C}_{qo} = \left\{\mathbb{C}_{qo}(1), \mathbb{C}_p(2), \cdots, \mathbb{C}_p(2^{nR_{qo}})\right\}$$

where $R_{qo}$ is the rate of the outer code and for $i = 1, \cdots, 2^{nR_{qo}}$, $\mathbb{C}_{qo}(i)$'s are iid random variables uniformly distributed over $A^n_\epsilon(Q)$. The outer code is partitioned into inner codes using the mapping

$$m : \mathbb{C}_{qo} \to \{1, 2, \cdots, 2^{nR_q}\}$$

where $R_q$ is the transmission rate for sending $Q$ and for $\boldsymbol{c} \in \mathbb{C}_{qo}$, $m(\boldsymbol{c})$'s are iid random variables uniformly distributed over $\{1, 2, \cdots, 2^{nR_q}\}$. Note that the codes for $P$ and $Q$ are unstructured random codes. In the next layer of coding, we use structured random codes to transmit $U + V$ where the random variables $U$ and $V$ are transmitted using nested codes with a common inner code. Let $\mathbb{C}_g$ be a group code over $G$ defined as follows:

$$\mathbb{C}_g = \{\phi(a) | a \in J\}$$

where the Abelian group $J$ and the homomorphism $\phi$ are defined according to (2.14) and (2.11) respectively. The code $\mathbb{C}_g$ is the common inner code between $U$ and $V$ and its rate is given by (2.15). The outer code for $U$ is defined as

$$\mathbb{C}_{uo} = \bigcup_{i\in\{1,\cdots,2^{nR_u}\}} \boldsymbol{s}_i + \mathbb{C}_g$$

where $R_u$ is the transmission rate for sending $U$ and for $i = 1, \cdots, 2^{nR_u}$, $\boldsymbol{s}_i$'s are iid random variables uniformly distributed over $G^n$. Similarly, the outer code for $V$ is defined as

$$\mathbb{C}_{vo} = \cup_{i\in\{1,\cdots,2^{nR_v}\}} \boldsymbol{t}_i + \mathbb{C}_g$$

where $R_v$ is the transmission rate for sending $V$ and for $i = 1, \cdots, 2^{nR_v}$, $\boldsymbol{t}_i$'s are iid random variables uniformly distributed over $G^n$. In the above code constructions, different random variables are assumed to be independent unless otherwise stated. For convenience, we also define the mappings $s : \mathbb{C}_{uo} \to \{1, \cdots, 2^{nR_u}\}$ and $t : \mathbb{C}_{vo} \to \{1, \cdots, 2^{nR_v}\}$ where for $i \in \{1, \cdots, 2^{nR_u}\}$ and $\boldsymbol{c} \in \boldsymbol{s}_i + \mathbb{C}_g$, $s(\boldsymbol{c}) = \boldsymbol{s}_i$ and the map $t$ is similarly defined.

The encoding and decoding rules are as follows: Given a source pair $(\boldsymbol{x}, \boldsymbol{y}) \in \mathscr{X}^n \times \mathscr{Y}^n$, if $\boldsymbol{x} \notin A_\epsilon^n(X)$, the $X$-encoder declares error ($Err_x$); otherwise it looks for $\boldsymbol{p} \in \mathbb{C}_p$ such that $\boldsymbol{p} \in A_\epsilon^n(P|\boldsymbol{x})$. If it finds such $\boldsymbol{p}$, it is sent to the decoder; otherwise, it declares error ($Err_p$). Similarly, if $\boldsymbol{y} \notin A_\epsilon^n(Y)$, the $Y$-encoder declares error ($Err_y$); otherwise it looks for $\boldsymbol{q} \in \mathbb{C}_{qo}$ such that $\boldsymbol{q} \in A_\epsilon^n(Q|\boldsymbol{y})$. If it finds such $\boldsymbol{q}$, $m(\boldsymbol{q})$ is sent to the decoder; otherwise, it declares error ($Err_q$). This stage of encoding is essentially the Berger-Tung layer of the coding scheme.

In the second stage of encoding, assuming that no error occurred in the first stage, the $X$-encoder looks for $\boldsymbol{u} \in \mathbb{C}_{uo}$ such that $\boldsymbol{u} \in A_\epsilon^n(U|\boldsymbol{x}\boldsymbol{p})$. Given the sequences

$\boldsymbol{x} \in \mathscr{X}^n$ and $\boldsymbol{p} \in \mathscr{P}^n$, define

$$\alpha(\boldsymbol{x}, \boldsymbol{p}) = \sum_{i=1}^{2^{nR_u}} \sum_{a \in J} \sum_{\boldsymbol{u} \in A_\epsilon^n(U|\boldsymbol{x},\boldsymbol{p})} \mathbb{1}_{\{\phi(a)+\boldsymbol{s}_i=\boldsymbol{u}\}}$$

Note that if $\alpha(\boldsymbol{x}, \boldsymbol{p}) > 0$, then there exists at least one $i \in \{1, \cdots, 2^{nR_u}\}$ and one $a \in J$ with $\phi(a) + \boldsymbol{s}_i \in A_\epsilon^n(U|\boldsymbol{x}, \boldsymbol{p})$. In this case, the encoder picks one such pair and sends $i$ to the channel. The encoder will declare an encoding error if $\alpha(\boldsymbol{x}, \boldsymbol{p}) = 0$. Although it may be unnecessary, it is convenient in the proofs to assume that the encoder declares error if $\alpha(\boldsymbol{x}, \boldsymbol{p}) \leq \frac{2^{nR_u} \cdot |J| \cdot |A_\epsilon^n(U|\boldsymbol{x},\boldsymbol{p})|}{2 \cdot |G|^n}$. We denote this error event by $Err_u$. We also assume that the pair $(a, i)$ is picked with probability $\frac{\sum_{\boldsymbol{u} \in A_\epsilon^n(U|\boldsymbol{x},\boldsymbol{p})} \mathbb{1}_{\{\phi(a)+\boldsymbol{s}_i=\boldsymbol{u}\}}}{\alpha(\boldsymbol{x},\boldsymbol{p})}$. Similarly, assuming that no error occurred in the first stage, the $Y$-encoder looks for $\boldsymbol{v} \in \mathbb{C}_{vo}$ such that $\boldsymbol{v} \in A_\epsilon^n(V|\boldsymbol{y}\boldsymbol{q})$. Given the sequences $\boldsymbol{y} \in \mathscr{Y}^n$ and $\boldsymbol{q} \in \mathscr{Q}^n$, define

$$\beta(\boldsymbol{x}, \boldsymbol{p}) = \sum_{j=1}^{2^{nR_v}} \sum_{b \in J} \sum_{\boldsymbol{v} \in A_\epsilon^n(V|\boldsymbol{y},\boldsymbol{q})} \mathbb{1}_{\{\phi(b)+\boldsymbol{t}_j=\boldsymbol{v}\}}$$

Note that if $\beta(\boldsymbol{y}, \boldsymbol{q}) > 0$, then there exists at least one $j \in \{1, \cdots, 2^{nR_v}\}$ and one $b \in J$ with $\phi(b) + \boldsymbol{t}_j \in A_\epsilon^n(V|\boldsymbol{y}, \boldsymbol{q})$. In this case, the encoder picks one such pair and sends $j$ to the channel. The encoder will declare an encoding error if $\beta(\boldsymbol{y}, \boldsymbol{q}) = 0$. Same as above, it is convenient in the proofs to assume that the encoder declares error if $\beta(\boldsymbol{y}, \boldsymbol{q}) \leq \frac{2^{nR_v} \cdot |J| \cdot |A_\epsilon^n(V|\boldsymbol{y},\boldsymbol{q})|}{2 \cdot |G|^n}$. We denote this error event by $Err_v$. We also assume that the pair $(b, j)$ is picked with probability $\frac{\sum_{\boldsymbol{v} \in A_\epsilon^n(V|\boldsymbol{y},\boldsymbol{q})} \mathbb{1}_{\{\phi(b)+\boldsymbol{t}_j=\boldsymbol{v}\}}}{\beta(\boldsymbol{y},\boldsymbol{q})}$.

At the receiver, assuming no encoding errors occurred in either of the terminals, $\boldsymbol{p}$, $m(\boldsymbol{q})$, $s(\boldsymbol{u})$ and $t(\boldsymbol{v})$ are available. The decoder sets $\hat{\boldsymbol{p}} = \boldsymbol{p}$ and looks for $\hat{\boldsymbol{q}} \in \mathbb{C}_{qo}$ such that $\hat{\boldsymbol{q}} \in A_\epsilon^n(Q|\hat{\boldsymbol{p}})$. If it does not find such $\hat{\boldsymbol{q}}$ it declares error ($Err_{\hat{q}}$). In the next stage of decoding, assuming no error occurred in the first stage, the decoder looks for $\hat{\boldsymbol{z}} \in A_\epsilon^n(Z|\hat{\boldsymbol{p}}\hat{\boldsymbol{q}})$ for which there exist $\hat{\boldsymbol{u}} \in \mathbb{C}_{uo}$ and $\hat{\boldsymbol{v}} \in \mathbb{C}_{vo}$ such that $s(\hat{\boldsymbol{u}}) = s(\boldsymbol{u})$, $t(\hat{\boldsymbol{v}}) = t(\boldsymbol{v})$ and $\hat{\boldsymbol{u}} + \hat{\boldsymbol{v}} = \hat{\boldsymbol{z}}$. If it does not find such $\hat{\boldsymbol{z}}$, it declares error ($Err_{\hat{z}}$).

### 3.3.4 Error Analysis

In Section 3.3.3, we defined the error events $Err_x$, $Err_p$, $Err_y$, $Err_q$, $Err_u$, $Err_v$, $Err_{\hat{q}}$ and $Err_{\hat{z}}$. In addition, we define the following error events which may not be necessarily observable at any terminal: The error event $Err_{xy}$ is the event $(\boldsymbol{x}, \boldsymbol{y}) \notin A_\epsilon^n(XY)$; $Err_{q\neq\hat{q}}$ is the event that $\hat{\boldsymbol{q}} \neq \boldsymbol{q}$; and $Err_{\boldsymbol{z}\neq\hat{\boldsymbol{z}}}$ is the event that $\hat{\boldsymbol{z}} \neq \boldsymbol{z}$.

First we show that if none of the error events occur, then $(\boldsymbol{x}, \boldsymbol{y}, \hat{\boldsymbol{p}}, \hat{\boldsymbol{q}}, \hat{\boldsymbol{z}}) \in A_\epsilon^n(XYPQZ)$. This is equivalent to showing $(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{p}, \boldsymbol{q}, \boldsymbol{z}) \in A_\epsilon^n(XYPQZ)$ where $\boldsymbol{z} = \boldsymbol{u} + \boldsymbol{v}$ and in turn, it suffices to show $(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{p}, \boldsymbol{q}, \boldsymbol{u}, \boldsymbol{v}) \in A_\epsilon^n(XYPQUV)$. Note that $(\boldsymbol{x}, \boldsymbol{y}, \hat{\boldsymbol{p}}, \hat{\boldsymbol{q}}, \hat{\boldsymbol{z}}) \in A_\epsilon^n(XYPQZ)$ implies $\boldsymbol{x}$, $\boldsymbol{y}$ and $g(\hat{\boldsymbol{z}}, \hat{\boldsymbol{p}}, \hat{\boldsymbol{q}})$ are jointly typical which in turn implies $d(\boldsymbol{x}, \boldsymbol{y}, g(\hat{\boldsymbol{z}}, \hat{\boldsymbol{p}}, \hat{\boldsymbol{q}})) \approx \mathbb{E}\{d(X, Y, g(Z, P, Q))\} \leq D$. We need the following Markov lemma:

**Lemma III.2.** *Let $X, Y, Z$ be random variables taking values from finite sets $\mathscr{X}, \mathscr{Y}, \mathscr{Z}$ respectively such that the Markov chain $X \leftrightarrow Y \leftrightarrow Z$ holds. For $n = 1, 2, \cdots$, let $(\boldsymbol{x}^{(n)}, \boldsymbol{y}^{(n)}) \in A_\epsilon^n(XY)$ and let $K^{(n)}$ be a random vector taking values from $\mathscr{Z}^n$ with distribution satisfying (for simplicity of notation we call them $\boldsymbol{x}, \boldsymbol{y}, K$ respectively)*

$$P\left(K = \boldsymbol{z}\right) \leq p_{Z|Y}^n(\boldsymbol{z}|\boldsymbol{y})e^{\epsilon_n n}$$

*for some $\epsilon_n \to 0$ as $n \to \infty$. Then, as $n \to \infty$*

$$P\left((\boldsymbol{x}, \boldsymbol{y}, K) \in A_\epsilon^n(XYZ)\right) \to 1$$

*Proof.* Provided in Section 3.3.6.1. □

Note that if the error event $Err_{xy}$ does not happen, $(\boldsymbol{x}, \boldsymbol{y}) \in A_\epsilon^n(XY)$ and therefore, the regular Markov lemma implies that $(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{p}, \boldsymbol{q}) \in A_\epsilon^n(XY)$ since the Markov chain $P \leftrightarrow X \leftrightarrow Y \leftrightarrow Q$ holds. Assuming that $Err_u$ does not occur, let $K \in \mathscr{U}^n$ be

the output of the encoder. We have

$$\begin{aligned} P(K=\boldsymbol{u}|\phi,\boldsymbol{s}_1,\boldsymbol{s}_2,\cdots) &= \sum_{a\in J}\sum_{i=1}^{2^{nR_u}} \frac{\sum_{\tilde{\boldsymbol{u}}\in A_\epsilon^n(U|\boldsymbol{x},\boldsymbol{p})} \mathbb{1}_{\{\phi(a)+\boldsymbol{s}_i=\tilde{\boldsymbol{u}}\}}}{\alpha(\boldsymbol{x},\boldsymbol{p})} \mathbb{1}_{\{\phi(a)+\boldsymbol{s}_i=\boldsymbol{u}\}} \\ &= \sum_{a\in J}\sum_{i=1}^{2^{nR_u}} \frac{1}{\alpha(\boldsymbol{x},\boldsymbol{p})} \mathbb{1}_{\{\phi(a)+\boldsymbol{s}_i=\boldsymbol{u},\boldsymbol{u}\in A_\epsilon^n(U|\boldsymbol{x},\boldsymbol{p})\}} \\ &\leq \sum_{a\in J}\sum_{i=1}^{2^{nR_u}} \frac{2|G|^n}{2^{nR_u}\cdot|J|\cdot|A_\epsilon^n(U|\boldsymbol{x},\boldsymbol{p})|} \mathbb{1}_{\{\phi(a)+\boldsymbol{s}_i=\boldsymbol{u},\boldsymbol{u}\in A_\epsilon^n(U|\boldsymbol{x},\boldsymbol{p})\}} \end{aligned}$$

Therefore,

$$P(K=\boldsymbol{u}) \leq \frac{2}{|A_\epsilon^n(U|\boldsymbol{x},\boldsymbol{p})|} \mathbb{1}_{\{\boldsymbol{u}\in A_\epsilon^n(U|\boldsymbol{x},\boldsymbol{p})\}}$$

Let $U^n$ be distributed according to $p^n_{U|XYPQ}(\cdot|\boldsymbol{x},\boldsymbol{y},\boldsymbol{p},\boldsymbol{q}) = p^n_{U|XP}(\cdot|\boldsymbol{x},\boldsymbol{p})$. It is known that for $\boldsymbol{u}\in A_\epsilon^n(U|\boldsymbol{x},\boldsymbol{p})$, $P\left(U^n=\boldsymbol{u}\right) \geq \frac{e^{\delta_n n}}{|A_\epsilon^n(U|\boldsymbol{x},\boldsymbol{p})|}$ for some $\delta_n$ converging to zero. This implies that there exist a sequence $\epsilon_n$ converging to zero such that

$$P(K=\boldsymbol{u}) \leq P(U^n=\boldsymbol{u})e^{\epsilon_n n} = p^n_{U|XP}(\boldsymbol{u}|\boldsymbol{x},\boldsymbol{p})e^{\epsilon_n n}$$

Consider the Markov chain $U \leftrightarrow (P,X) \leftrightarrow (Y,Q)$ and use Lemma III.2 for $(\boldsymbol{x},\boldsymbol{p}),(\boldsymbol{y},\boldsymbol{q}),K$. It follows that with high probability, $(\boldsymbol{x},\boldsymbol{y},\boldsymbol{p},\boldsymbol{q},\boldsymbol{u}) \in A_\epsilon^n(XYPQU)$. Similarly, using the above argument for $\boldsymbol{v}$ and considering the Markov chain $(U,P,X) \leftrightarrow (Y,Q) \leftrightarrow V$, we can show that with high probability

$$(\boldsymbol{x},\boldsymbol{y},\boldsymbol{p},\boldsymbol{q},\boldsymbol{u},\boldsymbol{v}) \in A_\epsilon^n(XYPQUV) \tag{3.4}$$

Next we show that the expected value of the probability of all of the error events vanish zero as $n$ increases for the following rates:

$$R_p > I(X;P)$$

$$R_{qo} > I(Y;Q)$$

$$R_q > I(Y;Q) - I(P;Q) = I(Y;Q|P)$$

$$R_g < I^G_{c.c}(Z;PQ)$$

$$R_g + R_u > \bar{I}(U;XP) \Rightarrow R_u > \bar{I}(U;XP) - I^G_{c.c}(Z;PQ)$$

$$R_g + R_v > \bar{I}(V;YQ) \Rightarrow R_v > \bar{I}(V;YQ) - I^G_{c.c}(Z;PQ)$$

This will show that the claimed rates are achievable since $R_1 = R_p + R_u$ and $R_2 = R_q + R_v$.

It is straightforward to show that the probabilities of the error events $Err_x$, $Err_y$, $Err_{xy}$ fall exponentially by $n$. It also follows from the standard approaches that the probabilities of the error events $Err_p$, $Err_q$ and $Err_{q\neq\hat{q}}$ vanish as $n$ increases [15,70]. It remains to show the same for $Err_u$, $Err_v$, $Err_{\hat{z}}$, $Err_{\hat{q}}$ and $Err_{z\neq\hat{z}}$

#### 3.3.4.1 The Error Events $Err_u$ and $Err_v$

For the source output $\boldsymbol{x} \in \mathscr{X}^n$, assuming that $Err_p$ did not occur, let $\boldsymbol{p}$ be the output of the first step of encoding. The error event $Err_u$ occurs if $\alpha(\boldsymbol{x},\boldsymbol{p}) \leq \frac{2^{nR_u}\cdot|J|\cdot|A_\epsilon^n(U|\boldsymbol{x},\boldsymbol{p})|}{2\cdot|G|^n}$. We bound the probability of error using the following Chebyshev's inequality:

$$P\Big(Err_u|\boldsymbol{x},\boldsymbol{p}\Big) = P\Big(\alpha(\boldsymbol{x},\boldsymbol{p}) \leq \frac{2^{nR_u}\cdot|J|\cdot|A_\epsilon^n(U|\boldsymbol{x},\boldsymbol{p})|}{2\cdot|G|^n}\Big) \leq \frac{\mathrm{var}\{\alpha(\boldsymbol{x},\boldsymbol{p})\}}{\mathbb{E}\{\alpha(\boldsymbol{x},\boldsymbol{p})\}^2}$$

We have

$$\mathbb{E}\{\alpha(\boldsymbol{x},\boldsymbol{p})\} = \sum_{i=1}^{2^{nR_u}}\sum_{a\in J}\sum_{\boldsymbol{u}\in A_\epsilon^n(U|\boldsymbol{x},\boldsymbol{p})} P\left(\phi(a)+\boldsymbol{s}_i=\boldsymbol{u}\right)$$

Note that $\phi(a)+\boldsymbol{s}_i$ is uniform over $G^n$; therefore,

$$\begin{aligned}\mathbb{E}\{\alpha(\boldsymbol{x},\boldsymbol{p})\} &= \sum_{i=1}^{2^{nR_u}}\sum_{a\in J}\sum_{\boldsymbol{u}\in A_\epsilon^n(U|\boldsymbol{x},\boldsymbol{p})}\frac{1}{|G|^n}\\ &= 2^{nR_u}\cdot|J|\cdot|A_\epsilon^n(U|\boldsymbol{x},\boldsymbol{p})|\cdot\frac{1}{|G|^n}\end{aligned}$$

Furthermore,

$$\begin{aligned}
\mathbb{E}\{\alpha(\boldsymbol{x},\boldsymbol{p})^2\} &= \sum_{i=1}^{2^{nR_u}} \sum_{a\in J} \sum_{\boldsymbol{u}\in A_\epsilon^n(U|\boldsymbol{x},\boldsymbol{p})} \sum_{j=1}^{2^{nR_u}} \sum_{\tilde{a}\in J} \sum_{\tilde{\boldsymbol{u}}\in A_\epsilon^n(U|\boldsymbol{x},\boldsymbol{p})} P\left(\phi(a)+\boldsymbol{s}_i=\boldsymbol{u},\phi(\tilde{a})+\boldsymbol{s}_j=\tilde{\boldsymbol{u}}\right) \\
&= \sum_{i=1}^{2^{nR_u}} \sum_{a\in J} \sum_{\boldsymbol{u}\in A_\epsilon^n(U|\boldsymbol{x},\boldsymbol{p})} \sum_{\tilde{a}\in J} \sum_{\tilde{\boldsymbol{u}}\in A_\epsilon^n(U|\boldsymbol{x},\boldsymbol{p})} P\left(\phi(a)+\boldsymbol{s}_i=\boldsymbol{u},\phi(\tilde{a})+\boldsymbol{s}_i=\tilde{\boldsymbol{u}}\right) \\
&+ \sum_{i=1}^{2^{nR_u}} \sum_{a\in J} \sum_{\boldsymbol{u}\in A_\epsilon^n(U|\boldsymbol{x},\boldsymbol{p})} \sum_{\substack{j=1\\ j\neq i}}^{2^{nR_u}} \sum_{\tilde{a}\in J} \sum_{\tilde{\boldsymbol{u}}\in A_\epsilon^n(U|\boldsymbol{x},\boldsymbol{p})} P\left(\phi(a)+\boldsymbol{s}_i=\boldsymbol{u},\phi(\tilde{a})+\boldsymbol{s}_j=\tilde{\boldsymbol{u}}\right) \\
&= \sum_{i=1}^{2^{nR_u}} \sum_{a\in J} \sum_{\boldsymbol{u}\in A_\epsilon^n(U|\boldsymbol{x},\boldsymbol{p})} \sum_{\tilde{a}\in J} \sum_{\tilde{\boldsymbol{u}}\in A_\epsilon^n(U|\boldsymbol{x},\boldsymbol{p})} \frac{1}{|G|^n} P\left(\phi(\tilde{a}-a)=\tilde{\boldsymbol{u}}-\boldsymbol{u}\right) \\
&+ \sum_{i=1}^{2^{nR_u}} \sum_{a\in J} \sum_{\boldsymbol{u}\in A_\epsilon^n(U|\boldsymbol{x},\boldsymbol{p})} \sum_{\substack{j=1\\ j\neq i}}^{2^{nR_u}} \sum_{\tilde{a}\in J} \sum_{\tilde{\boldsymbol{u}}\in A_\epsilon^n(U|\boldsymbol{x},\boldsymbol{p})} \frac{1}{|G|^{2n}} \\
&\leq \mathbb{E}\{\alpha(\boldsymbol{x},\boldsymbol{p})\}^2 + \sum_{\theta\in\Theta} \sum_{i=1}^{2^{nR_u}} \sum_{a\in J} \sum_{\boldsymbol{u}\in A_\epsilon^n(U|\boldsymbol{x},\boldsymbol{p})} \sum_{\tilde{a}\in T_\theta(a)} \sum_{\substack{\tilde{\boldsymbol{u}}\in A_\epsilon^n(U|\boldsymbol{x},\boldsymbol{p})\\ \tilde{\boldsymbol{u}}-\boldsymbol{u}\in H_\theta^n}} \frac{1}{|G|^n}\frac{1}{|H_\theta|^n}
\end{aligned}$$

Therefore,

$$\begin{aligned}
\mathrm{var}\{\alpha(\boldsymbol{x},\boldsymbol{p})\} &\leq \sum_{\theta\in\Theta} \sum_{i=1}^{2^{nR_u}} \sum_{a\in J} \sum_{\boldsymbol{u}\in A_\epsilon^n(U|\boldsymbol{x},\boldsymbol{p})} \sum_{\tilde{a}\in T_\theta(a)} \sum_{\substack{\tilde{\boldsymbol{u}}\in A_\epsilon^n(U|\boldsymbol{x},\boldsymbol{p})\\ \tilde{\boldsymbol{u}}-\boldsymbol{u}\in H_\theta^n}} \frac{1}{|G|^n}\frac{1}{|H_\theta|^n} \\
&\leq \sum_{\theta\in\Theta} 2^{nR_u}\cdot|J|\cdot|T_\theta|\cdot 2^{n[H(U|XP)+\epsilon]} 2^{n[H(U|XP[U]_\theta)+\epsilon]} \frac{1}{|\mathbf{G}|^n}\frac{1}{|H_\theta|^n}
\end{aligned}$$

Therefore,

$$P\Big(Err_u|\boldsymbol{x},\boldsymbol{p}\Big) \leq \sum_{\theta\in\Theta} \frac{|\mathbf{G}|^n}{|J|\cdot 2^{nR_u} 2^{nH(U|XP)}} \cdot \frac{|T_\theta|\cdot 2^{nH(U|XP[U]_\theta)}}{|H_\theta|^n}$$

Note that by Lemma II.11, $|T_\theta| = 2^{nR(1-\omega_\theta)}$. Therefore, $R_g < I_{c.c.}^G(Z;PQ)$ implies for all $\theta\in\Theta$ such that $\theta\neq\boldsymbol{r}$,

$$\frac{|T_\theta|\cdot 2^{nH(Z|PQ[Z]_\theta)}}{|H_\theta|^n} \to 0$$

as $n$ increases. Note that

$$\begin{aligned} H(U|XP[U]_\theta) &\overset{(a)}{=} H(U|XP) - H([U]_\theta|XP) \\ &\overset{(b)}{=} H(U|XPQV) - H([U]_\theta|XPQV) \\ &= H(U|XPQV[U]_\theta) \\ &= H(UV|XPQV[U]_\theta) \\ &\overset{(c)}{=} H(VZ|XPQV[Z]_\theta) \\ &= H(Z|XPQV[Z]_\theta) \\ &\leq H(Z|PQ[Z]_\theta) \end{aligned}$$

where $(a)$ follows since $[U]_\theta$ is a function of $U$; $(b)$ follows since the Markov chains $U \leftrightarrow (P, X) \leftrightarrow (Q, V)$ and $[U]_\theta \leftrightarrow P \leftrightarrow (Q, V)$ hold; and $(c)$ holds since there are one to one correspondences between $(U, V)$ and $(V, Z)$ and between $([U]_\theta, V)$ and $(V, [Z]_\theta)$. Therefore, for $\theta \neq \boldsymbol{r}$,

$$\frac{|T_\theta| \cdot 2^{nH(U|XP[U]_\theta)}}{|H_\theta|^n} \leq \frac{|T_\theta| \cdot 2^{nH(Z|PQ[Z]_\theta)}}{|H_\theta|^n} \to 0$$

Note that for $\theta = \boldsymbol{r}$, we have

$$\frac{|T_\theta| \cdot 2^{nH(U|XP[U]_\theta)}}{|H_\theta|^n} = 1$$

Therefore, it remains to show that

$$\frac{|\mathbf{G}|^n}{|J| \cdot 2^{nR_u} 2^{nH(U|XP)}} \to 0$$

as $n \to \infty$. Note that $|J| = 2^{nR_g}$; therefore,

$$\frac{|\mathbf{G}|^n}{|J| \cdot 2^{nR_u} 2^{nH(U|XP)}} = \frac{|\mathbf{G}|^n}{2^{n(R_g+R_u)} 2^{nH(U|XP)}} \to 0$$

since $R_g + R_u > \log|\mathbf{G}| - H(U|XP)$. With a similar argument, we can show that the probability of the event $Err_v$ approaches zero as $n$ increases.

#### 3.3.4.2 The Error Events $Err_{\hat{q}}$ and $Err_{\hat{z}}$

Equation (3.4) implies that with hight probability, the choice of $\hat{\boldsymbol{q}} = \boldsymbol{q}$ satisfies the conditions $\hat{\boldsymbol{q}} \in \mathbb{C}_{qo}$ and $\hat{\boldsymbol{q}} \in A_\epsilon^n(Q|\hat{\boldsymbol{p}})$. Therefore, the probability of the error event $Err_{\hat{q}}$ vanishes as $n$ increases. Similarly, $\hat{\boldsymbol{z}} = \boldsymbol{z} = \boldsymbol{u} + \boldsymbol{v}$ satisfies the necessary conditions and it is straightforward to show that the probability of the event $Err_{\hat{z}}$ approaches zero as $n \to \infty$.

#### 3.3.4.3 The Error Event $Err_{z \neq \hat{z}}$

Let $Err$ be the event that the error $Err_{z \neq \hat{z}}$ occurs but none of the other error events occur. Then the probability of the error event $Err$ is equal to

$$
\begin{aligned}
P\Big(Err\Big) \leq & \sum_{(\boldsymbol{x},\boldsymbol{y},\boldsymbol{p},\boldsymbol{q}) \in A_\epsilon^n(XYPQ)} p_{XY}^n(\boldsymbol{x},\boldsymbol{y}) \sum_{k=1}^{2^{nR_p}} \sum_{l=1}^{2^{nR_{qo}}} \mathbb{1}_{\{\mathbb{C}_p(k)=\boldsymbol{p}, \mathbb{C}_{qo}(l)=\boldsymbol{q}\}} \\
& \sum_{i=1}^{2^{nR_u}} \sum_{a \in J} \sum_{\boldsymbol{u} \in A_\epsilon^n(U|\boldsymbol{x},\boldsymbol{p})} \frac{1}{\alpha(\boldsymbol{x},\boldsymbol{p})} \mathbb{1}_{\{\phi(a)+\boldsymbol{s}_i=\boldsymbol{u}\}} \\
& \sum_{j=1}^{2^{nR_v}} \sum_{b \in J} \sum_{\boldsymbol{v} \in A_\epsilon^n(V|\boldsymbol{y},\boldsymbol{q})} \frac{1}{\beta(\boldsymbol{y},\boldsymbol{q})} \mathbb{1}_{\{\phi(b)+\boldsymbol{t}_j=\boldsymbol{v}\}} \sum_{\substack{\tilde{\boldsymbol{z}} \in A_\epsilon^n(Z|\boldsymbol{p},\boldsymbol{q}) \\ \tilde{\boldsymbol{z}} \neq \boldsymbol{z}}} \sum_{\tilde{c} \in J} \mathbb{1}_{\{\phi(\tilde{c})+\boldsymbol{s}_i+\boldsymbol{t}_j=\tilde{\boldsymbol{z}}\}} \\
\leq & \sum_{(\boldsymbol{x},\boldsymbol{y},\boldsymbol{p},\boldsymbol{q}) \in A_\epsilon^n(XYPQ)} p_{XY}^n(\boldsymbol{x},\boldsymbol{y}) \sum_{k=1}^{2^{nR_p}} \sum_{l=1}^{2^{nR_{qo}}} \mathbb{1}_{\{\mathbb{C}_p(k)=\boldsymbol{p}, \mathbb{C}_{qo}(l)=\boldsymbol{q}\}} \\
& \sum_{i=1}^{2^{nR_u}} \sum_{a \in J} \sum_{\boldsymbol{u} \in A_\epsilon^n(U|\boldsymbol{x},\boldsymbol{p})} \frac{2|G|^n}{2^{nR_u} \cdot |J| \cdot |A_\epsilon^n(U|\boldsymbol{x},\boldsymbol{p})|} \mathbb{1}_{\{\phi(a)+\boldsymbol{s}_i=\boldsymbol{u}\}} \\
& \sum_{j=1}^{2^{nR_v}} \sum_{b \in J} \sum_{\boldsymbol{v} \in A_\epsilon^n(V|\boldsymbol{y},\boldsymbol{q})} \frac{2|G|^n}{2^{nR_v} \cdot |J| \cdot |A_\epsilon^n(V|\boldsymbol{y},\boldsymbol{q})|} \mathbb{1}_{\{\phi(b)+\boldsymbol{t}_j=\boldsymbol{v}\}} \sum_{\substack{\tilde{\boldsymbol{z}} \in A_\epsilon^n(Z|\boldsymbol{p},\boldsymbol{q}) \\ \tilde{\boldsymbol{z}} \neq \boldsymbol{z}}} \sum_{\tilde{c} \in J} \mathbb{1}_{\{\phi(\tilde{c})+\boldsymbol{s}_i+\boldsymbol{t}_j=\tilde{\boldsymbol{z}}\}}
\end{aligned}
$$

Therefore,

$$\mathbb{E}\Big\{P(Err)\Big\} \leq \sum_{(\boldsymbol{x},\boldsymbol{y})\in A_\epsilon^n(XY)} p_{XY}^n(\boldsymbol{x},\boldsymbol{y}) \frac{2^{nR_p}\cdot|A_\epsilon(P|\boldsymbol{x})|}{|A_\epsilon(P)|}\cdot\frac{2^{nR_{qo}}\cdot|A_\epsilon(Q|\boldsymbol{y})|}{|A_\epsilon(Q)|}\sum_{i=1}^{2^{nR_u}}\sum_{a\in J}\sum_{\boldsymbol{u}\in A_\epsilon^n(U|\boldsymbol{x},\boldsymbol{p})}$$
$$\frac{2|G|^n}{2^{nR_u}\cdot|J|\cdot|A_\epsilon^n(U|\boldsymbol{x},\boldsymbol{p})|}\sum_{j=1}^{2^{nR_v}}\sum_{c\in J}\sum_{\boldsymbol{v}\in A_\epsilon^n(V|\boldsymbol{y},\boldsymbol{q})}\frac{2|G|^n}{2^{nR_v}\cdot|J|\cdot|A_\epsilon^n(V|\boldsymbol{y},\boldsymbol{q})|}$$
$$\sum_{\substack{\tilde{\boldsymbol{z}}\in A_\epsilon^n(Z|\boldsymbol{p},\boldsymbol{q})\\ \tilde{\boldsymbol{z}}\neq\boldsymbol{z}}}\sum_{\tilde{c}\in J} P\Big(\phi(a)+\boldsymbol{s}_i=\boldsymbol{u},\phi(c)+\boldsymbol{s}_i+\boldsymbol{t}_j=\boldsymbol{u}+\boldsymbol{v},\phi(\tilde{c})+\boldsymbol{s}_i+\boldsymbol{t}_j=\tilde{\boldsymbol{z}}\Big)$$
$$\leq \sum_{(\boldsymbol{x},\boldsymbol{y})\in A_\epsilon^n(XY)} p_{XY}^n(\boldsymbol{x},\boldsymbol{y})2^{n\epsilon}\sum_{i=1}^{2^{nR_u}}\sum_{a\in J}\sum_{\boldsymbol{u}\in A_\epsilon^n(U|\boldsymbol{x},\boldsymbol{p})}\frac{2|G|^n}{2^{nR_u}\cdot|J|\cdot|A_\epsilon^n(U|\boldsymbol{x},\boldsymbol{p})|}$$
$$\sum_{j=1}^{2^{nR_v}}\sum_{c\in J}\sum_{\boldsymbol{v}\in A_\epsilon^n(V|\boldsymbol{y},\boldsymbol{q})}\frac{2|G|^n}{2^{nR_v}\cdot|J|\cdot|A_\epsilon^n(V|\boldsymbol{y},\boldsymbol{q})|}$$
$$\sum_{\substack{\theta\in\Theta\\ \theta\neq\boldsymbol{r}}}\sum_{\substack{\tilde{\boldsymbol{z}}\in A_\epsilon^n(Z|\boldsymbol{p},\boldsymbol{q})\\ \tilde{\boldsymbol{z}}\in\boldsymbol{z}+H_\theta^n}}\sum_{\tilde{c}\in T_\theta(c)}\frac{1}{|G|^{2n}\cdot|H_\theta|^n}$$
$$\leq \sum_{\substack{\theta\in\Theta\\ \theta\neq\boldsymbol{r}}}\frac{4\cdot 2^{n\epsilon}\cdot|T_\theta|\cdot 2^{n[H(Z|[Z]_\theta PQ)+\epsilon]}}{|H_\theta|^n}$$

Therefore, we require to have $R_g < \frac{1}{1-\omega_\theta}\Big(\log|H_\theta| - H(Z|[Z]_\theta PQ)\Big)$ for all $\theta\in\Theta$, $\theta\neq\boldsymbol{r}$. Equivalently,

$$R_g < I_{c.c.}^G(Z;PQ)$$

### 3.3.5 Examples

Consider a two-user distributed source coding problem in which the two sources $X$ and $Y$ take values from $\mathbb{Z}_4$ and a centralized decoder in interested in decoding the sum of the two sources losslessly. Furthermore, assume that $X$ is uniformly distributed over $\mathbb{Z}_4$ and $Y=-X+Z$ where $Z$ is independent from $X$ and is distributed over $\mathbb{Z}_4$ such that $p_Z(0)=1-\tau$ and $p_Z(1)=p_Z(2)=p_Z(3)=\frac{\tau}{3}$ for some $\tau\in(0,1)$. Let $R_1$ and $R_2$ be the rates of the two encoders. Using unstructured codes (Slepian-Wolf

coding), a sum rate of $R = R_1 + R_2 = H(X, Y)$ is achievable. We have

$$R = H(X, Y) = H(X, -X + Z) = H(X) + H(Z) = 2 + h(\tau) + \tau \log 3$$

where $h(\cdot)$ denotes the binary entropy function. Using the scheme proposed by Krithivasan and Pradhan [42], the mod-4 operation can be embedded in Abelian groups $\mathbb{Z}_4$, $\mathbb{Z}_7$, $\mathbb{Z}_2^3$ and $\mathbb{Z}_4^2$. Let the auxiliary random variables $U$ and $V$ be equal to $X$ and $Y$ respectively and let $P$ and $Q$ be trivial random variables. It turns out that the rate pair $(R_1, R_2)$ is achievable where

$$R_1 = R_2 = 2 - \min\Big(2 - H(Z), 2 - 2H([Z])\Big) = \max\Big(H(Z), 2H([Z])\Big)$$

where $[Z] = Z + \{0, 2\}$. Therefore, a sum rate of $R = R_1 + R_2 = 2\max\Big(H(Z), 2H([Z])\Big)$ is achievable using the scheme proposed in [42]. Note that any $a \in \mathbb{Z}_4$ can be uniquely represented by $a = \widehat{a} + \widetilde{a}$ where $\widehat{a} \in \{0, 1\}$ and $\widetilde{a} \in \{0, 2\}$. Now consider the following assignments for the auxiliary random variables: Let $P = \widehat{X}$, $Q = \widehat{Y}$, $U = \widetilde{X}$ and $V = \widetilde{Y}$. It can be verified that $X + Y = g(U + V, P, Q) = \Big(\widehat{X} + \widehat{Y}\Big) \pmod 2 + \widetilde{X} + \widetilde{Y}$. Therefore the new coding theorem implies that the following sum rate is achievable:

$$\begin{aligned} R = R_1 + R_2 &= I(XY; \widehat{X}\widehat{Y}) + H(\widetilde{X} + \widetilde{Y} | \widehat{X}\widehat{Y}) \\ &= H(\widehat{X}\widehat{Y}) + H(\widetilde{X} + \widetilde{Y} | \widehat{X}\widehat{Y}) \\ &= H(\widehat{X}\widehat{Z}) + H(\widetilde{Z} | \widehat{X}\widehat{Z}) \\ &= H(\widehat{X}\widehat{Z}\widetilde{Z}) \\ &= H(\widehat{X}) + H(Z) \end{aligned}$$

Figure 3.3.5 compares the sum rate for the coding schemes for different values of $\tau$. As can be seen in the figure, the scheme based on group codes presented in this section outperforms the other schemes.

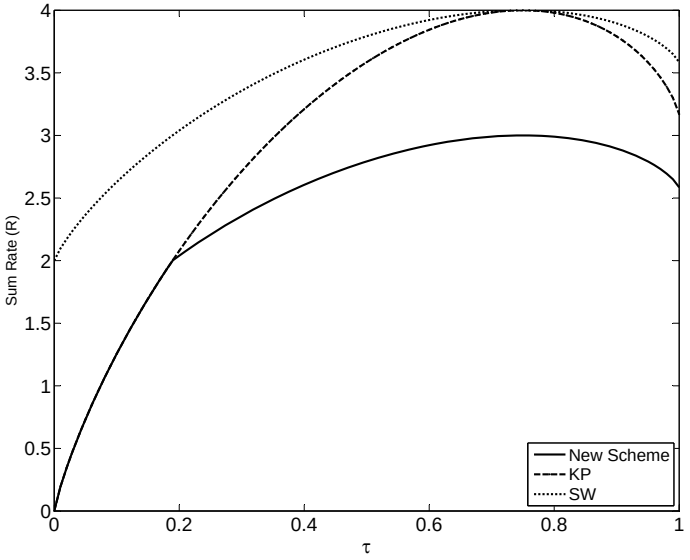


Figure 3.1: Comparison of the performance of random codes vs. group codes for a distributed source coding problem. As can be seen in the picture, group codes outperform random codes as the structure of the code is matched to the desired function of the two sources.

### 3.3.6 Appendix

#### 3.3.6.1 Proof of Lemma III.2

It suffices to show that for all $a \in \mathscr{X}$, $b \in \mathscr{Y}$ and $c \in \mathscr{Z}$,

$$\left| \frac{1}{n} N(a,b,c|\boldsymbol{x},\boldsymbol{y},K) - p_{XYZ}(a,b,c) \right| \to 0$$

with probability one as $n \to \infty$ where $N(a,b,c|x,y,K)$ counts the number of occurrences of the triple $(a,b,c)$ in the vector of triples $(\boldsymbol{x},\boldsymbol{y},K)$. We have

$$\begin{aligned} \left| \frac{1}{n} N(a,b,c|\boldsymbol{x},\boldsymbol{y},K) - p_{XYZ}(a,b,c) \right| \leq & \left| p_{XYZ}(a,b,c) - \frac{1}{n} N(a,b|\boldsymbol{x},\boldsymbol{y}) W^n_{Z|Y}(K|\boldsymbol{y}) \right| \\ & + \left| \frac{1}{n} N(a,b|\boldsymbol{x},\boldsymbol{y}) W^n_{Z|Y}(K|\boldsymbol{y}) - \frac{1}{n} N(a,b,c|\boldsymbol{x},\boldsymbol{y},K) \right| \end{aligned}$$

Note that it follows from standard typicality results that the first term in the equation above vanishes as $n$ increases almost surely. Next, we show that the second term also

vanishes almost surely. We have

$$\frac{1}{n}N(a,b|\boldsymbol{x},\boldsymbol{y})W^n_{Z|Y}(K|\boldsymbol{y})-\frac{1}{n}N(a,b,c|\boldsymbol{x},\boldsymbol{y},K)=\frac{1}{n}\sum_{i=1}^{n}\mathbb{1}_{\{x_i=a,y_i=b\}}\left[p_{Y|Z}(c|y_i)-\mathbb{1}_{\{K_i=c\}}\right]$$
$$\leq \frac{1}{n}\sum_{i=1}^{n}\theta_i$$

where for $i=1,2,\cdots,n$,

$$\theta_i = p_{Y|Z}(c|y_i) - \mathbb{1}_{\{K_i=c\}}$$

Let $Z^n$ be a random vector generated according to $p_{Z|Y}(\cdot|\boldsymbol{y})$ and define

$$\tilde{\theta}_i = p_{Y|Z}(c|y_i) - \mathbb{1}_{\{Z_i=c\}}$$

Note that both $\theta_i$ and $\tilde{\theta}_i$ are binary random variables taking values from the set $\{p_{Z|Y}(c|y_i), p_{Z|Y}(c|y_i)-1\}$ and $|\theta_i|, |\tilde{\theta}_i| \leq 1$. We have $\mathbb{E}\{\tilde{\theta}_i\}=0$ and $\text{var}\{\tilde{\theta}_i\} \leq 1$. It follows from [Proposition 1, Zhiyi Chi's paper] that $\tilde{\theta}_i$ satisfied the large deviations principle with a good rate function $I(\cdot)$ such that

$$P\left(\frac{\tilde{\theta}_1+\cdots+\tilde{\theta}_n}{n}\geq t\right)\leq e^{-nI(t)}$$

where $I(t)$ is positive. For $b\in\{p_{Z|Y}(c|y_i), p_{Z|Y}(c|y_i)-1\}^n$, we have

$$\begin{aligned}
P\left(\theta=\boldsymbol{b}\right) &= \sum_{\substack{\boldsymbol{z}\in\mathcal{Z}^n \\ z_i\neq c \text{ if } b_i=p_{Z|Y}(c|y_i) \\ z_i=c \text{ if } b_i=p_{Z|Y}(c|y_i)-1}} P\left(K=z\right) \\
&\leq \sum_{\substack{z\in\mathcal{Z}^n \\ z_i\neq c \text{ if } b_i=p_{Z|Y}(c|y_i) \\ z_i=c \text{ if } b_i=p_{Z|Y}(c|y_i)-1}} p^n_{Z|Y}(\boldsymbol{z}|\boldsymbol{y})e^{\epsilon_n n} \\
&= e^{\epsilon_n n}P\left(\tilde{\theta}=\boldsymbol{b}\right)
\end{aligned}$$

We have

$$P\left(\frac{\theta_1+\cdots+\theta_n}{n}\geq t\right)=\sum_{\boldsymbol{b}:\left|\frac{b_1+\cdots+b_n}{n}\right|\geq nt} P\left(\theta=\boldsymbol{b}\right)$$
$$\leq e^{\epsilon_n n}\sum_{\boldsymbol{b}:\left|\frac{b_1+\cdots+b_n}{n}\right|\geq nt} P\left(\tilde{\theta}=\boldsymbol{b}\right)$$
$$\leq e^{-n(I(t)-\epsilon_n)}$$

Note that since $e^{-n(I(t)-\epsilon_n)}$ is summable, the Borel-Cantelli lemma implies that for all $t>0$,

$$\limsup_{n\to\infty}|\frac{1}{n}\sum_{i=1}^{n}\theta_i|\leq t$$

Therefore, $|\frac{1}{n}\sum_{i=1}^{n}\theta_i|\to 0$ as $n\to\infty$ almost surely.

## 3.4 The 3-User Interference Channel

### 3.4.1 Problem Definition and the Coding Scheme

Consider a three-user discrete memoryless interference channel with inputs $X_1$, $X_2$ and $X_3$ and outputs $Y_1$, $Y_2$ and $Y_3$. Assume that $X_1$ takes values from a finite set $\mathscr{X}_1$ and $X_2$ and $X_3$ take values from an Abelian group $\mathbf{G}$. The decoder 1 decodes $X_1$ and $Z=X_2+X_3$ jointly where $+$ is the group operation and decoders 2 and 3 decode $X_2$ and $X_3$ respectively.

The encoder 1 uses the random code

$$\mathbb{C}_{r1}=\{\mathbb{C}_{r1}(1),\cdots,\mathbb{C}_{r1}(2^{nR_1})\}$$

where $R_1$ is the rate of the first user and $\mathbb{C}_{r1}(1),\cdots,\mathbb{C}_{r1}(2^{nR_1})$ are iid random variables uniformly distributed over $A_\epsilon^n(X_1)$. The encoder 2 uses a nested code whose outer code is a shifted group code $\mathbb{C}_g+\boldsymbol{b}_2$ over $\mathbf{G}$ where $\boldsymbol{b}_2$ is uniform over $\mathbf{G}^n$ and

$$\mathbb{C}_g=\{\phi(a)|a\in J\}$$

where $\phi$ and $J$ are defined in (2.11) and (2.14) respectively. The code $\mathbb{C}_g$ is the common code between $X_2$ and $X_3$ and its rate is equal to

$$R_g = \frac{k}{n} \sum_{(p,r)\in\mathscr{Q}(G)} r w_{p,r} \log p$$

The outer code is partitioned into inner codes by the mapping

$$s : J \to \{1, 2, \cdots, 2^{nR_2}\}$$

where $R_2$ is the rate of the second encoder and $\{s(a)\}_{a\in J}$ are iid and uniformly distributed over $\{1, 2, \cdots, 2^{nR_2}\}$. Similarly, encoder 3 uses a nested code whose outer code is $\mathbb{C}_g + \boldsymbol{b}_3$ where $\boldsymbol{b}_3$ is uniform over $\mathbf{G}^n$ and whose inner code is determined by a mapping

$$t : J \to \{1, 2, \cdots, 2^{nR_3}\}$$

where $R_3$ is the rate of the third encoder and $\{t(a)\}_{a\in J}$ are iid and uniformly distributed over $\{1, 2, \cdots, 2^{nR_3}\}$. Note that the above random codes and random mappings are independent from each other unless otherwise stated.

The encoding and decoding rules are as follows: Given a message $m_1 \in \{1, \cdots, 2^{nR_1}\}$, the encoder 1 sends $\mathbb{C}_{r1}(m_1)$. Given a message $m_2 \in \{1, \cdots, 2^{nR_2}\}$, the encoder 2 looks for $a \in J$ such that $\phi(a) + \boldsymbol{b}_2 \in A_\epsilon^n(X_2)$ and $s(a) = m_2$. If it finds such $a$, it sends $x_2 = \phi(a) + \boldsymbol{b}_2$ over the channel; otherwise it declares error ($Err_{e2}$). Similarly, given a message $m_3 \in \{1, \cdots, 2^{nR_3}\}$, the encoder 3 looks for $b \in J$ such that $\phi(b) + \boldsymbol{b}_3 \in A_\epsilon^n(X_3)$ and $t(b) = m_3$. If it finds such $b$, it sends $\boldsymbol{x}_3 = \phi(b) + \boldsymbol{b}_3$ over the channel; otherwise it declares error ($Err_{e3}$).

At the receiver side, the decoder 1 after receiving $y_1 \in \mathscr{Y}_1^n$, looks for an index $\hat{m}_1 \in \{1, \cdots, 2^{nR_1}\}$ and $\boldsymbol{z} \in \mathbb{C}_g + \boldsymbol{b}_2 + \boldsymbol{b}_3$ such that $(\mathbb{C}_{r1}(\hat{m}_1), \boldsymbol{z}) \in A_\epsilon^n(X_1, X_2 + X_3|y_1)$. If it does not find such a pair or if it finds more than one such index $\hat{m}$, it declares error ($Err_{d1}$). The receiver 2 after receiving $\boldsymbol{y}_2 \in \mathscr{Y}_2^n$, looks for the index $\hat{m}_2 \in \{1, \cdots, 2^{nR_2}\}$ for which there exists a unique $\hat{a} \in J$ with $\phi(\hat{a}) + \boldsymbol{b}_2 \in A_\epsilon^n(X_2|\boldsymbol{y}_2)$

and $s(\hat{a}) = \hat{m}_2$. If it does not find such $\hat{m}_2$, it declares error ($Err_{d2}$). The decoding rule for the third receiver is similar to that of the second receiver.

In the following, we show that the expected value of the probability of all the error events over the ensemble approach zero as the block length increases if

$$\begin{aligned}
&R_1 < I(X_1; Y_1 Z) \\
&R_1 + R_g < I(X_1; Y_1) + I_{c.c.}(Z; X_1 Y_1) \\
&R_g - R_2 > \log |\mathbf{G}| - H(X_2) \\
&R_g < I^{\mathbf{G}}_{c.c.}(X_2; Y_2) \\
&R_g - R_3 > \log |\mathbf{G}| - H(X_3) \\
&R_g < I^{\mathbf{G}}_{c.c.}(X_3; Y_3)
\end{aligned}$$

and $R_g > I^{\mathbf{G}}_{s.c.}(X_2; X_2)$. In the following analysis, for simplicity we are assume $H(X_2) = H(X_3)$ so that one group code can be used for both terminals.

### 3.4.2 Error Analysis

#### 3.4.2.1 The Error Event $Err_{e2}$:

Given a message $m_2 \in \{1, 2, \cdots, 2^{nR_2}\}$, define

$$\theta_2(m_2) = \sum_{a \in J} \sum_{x_2 \in A^n_\epsilon(X_2)} \mathbb{1}_{\{\phi(a) + \boldsymbol{b}_2 = x_2, s(a) = m_2\}}$$

To simplify the analysis, we use the following modified encoding rule: If $\theta_2(m_2) < \frac{\mathbb{E}\{\theta_2(m_2)\}}{2}$ declare error otherwise pick one such $a$ uniformly and send $x_2 = \phi(a) + \boldsymbol{b}_2$. We use Chebyshev's inequality as follows.

$$P(Err_{e2}|m_2) = P(\theta_2(m_2) < \frac{\mathbb{E}\{\theta_2(m_2)\}}{2}) \leq \frac{\mathrm{var}\{\theta_2(m_2)\}}{\mathbb{E}\left\{\theta_2(m_2)\right\}^2}$$

We have

$$\begin{aligned}\mathbb{E}\left\{\theta_2(m_2)\right\} &= \sum_{a\in J}\sum_{x_2\in A_\epsilon^n(X_2)} P\left(\phi(a)+\boldsymbol{b}_2 = x_2, s(a)=m_2\right)\\ &= \sum_{a\in J}\sum_{x_2\in A_\epsilon^n(X_2)} \frac{1}{|\mathbf{G}|^n}\cdot\frac{1}{2^{nR_2}}\\ &= \frac{|J|\cdot|A_\epsilon^n(X_2)|}{|\mathbf{G}|^n\cdot 2^{nR_2}}\end{aligned}$$

and

$$\begin{aligned}\mathbb{E}\left\{\theta_2(m_2)^2\right\} &= \sum_{a,\tilde{a}\in J}\sum_{x_2,\tilde{\boldsymbol{x}}_2\in A_\epsilon^n(X_2)} P\left(\phi(a)+\boldsymbol{b}_2=x_2, \phi(\tilde{a})+\boldsymbol{b}_2=\tilde{\boldsymbol{x}}_2, s(a)=m_2, s(\tilde{a})=m_2\right)\\ &= \sum_{\theta\in\Theta}\sum_{a\in J}\sum_{\tilde{a}\in T_\theta(a)}\sum_{x_2\in A_\epsilon^n(X_2)}\sum_{\substack{\tilde{\boldsymbol{x}}_2\in A_\epsilon^n(X_2)\\ \tilde{\boldsymbol{x}}_2\in x_2+H_\theta^n}} \frac{1}{|\mathbf{G}|^n}\cdot\frac{1}{|H_\theta|^n}\cdot P\left(s(a)=m_2, s(\tilde{a})=m_2\right)\\ &= \sum_{a\in J}\sum_{\boldsymbol{x}_2\in A_\epsilon^n(X_2)}\frac{1}{|\mathbf{G}|^n}\cdot\frac{1}{2^{nR_2}}\\ &+ \sum_{\substack{\theta\in\Theta\\ \theta\neq\boldsymbol{r}}}\sum_{a\in J}\sum_{\tilde{a}\in T_\theta(a)}\sum_{\boldsymbol{x}_2\in A_\epsilon^n(X_2)}\sum_{\substack{\tilde{\boldsymbol{x}}_2\in A_\epsilon^n(X_2)\\ \tilde{\boldsymbol{x}}_2\in\boldsymbol{x}_2+H_\theta^n}} \frac{1}{|\mathbf{G}|^n}\cdot\frac{1}{|H_\theta|^n}\cdot\frac{1}{2^{2nR_2}}\\ &\leq \frac{|J|\cdot|A_\epsilon^n(X_2)|}{|\mathbf{G}|^n\cdot 2^{nR_2}} + \sum_{\substack{\theta\in\Theta\\ \theta\neq\boldsymbol{r}}}\frac{|J|\cdot|T_\theta|\cdot|A_\epsilon^n(X_2)|\cdot|A_\epsilon^n(X_2)\cap(\boldsymbol{x}_2+H_\theta^n)|}{|\mathbf{G}|^n\cdot|H_\theta|^n\cdot 2^{2nR_2}}\end{aligned}$$

where, $\boldsymbol{r}$ is a vector whose components are indexed by $(p,r)\in\mathscr{Q}(G)$ and whose $(p,r)^{\text{th}}$ component is equal to $r$. Using Lemma II.14, we get

$$\operatorname{var}\left\{\theta_2(m_2)^2\right\} \leq \frac{|J|\cdot|A_\epsilon^n(X_2)|}{|\mathbf{G}|^n\cdot 2^{nR_2}} + \sum_{\substack{\theta\in\Theta\\ \theta\neq\mathbf{0},\theta\neq\boldsymbol{r}}}\frac{|J|\cdot|T_\theta|\cdot 2^{n[H(X_2)+\epsilon]}2^{n[H(X_2|[X_2]_\theta)+\epsilon]}}{|\mathbf{G}|^n\cdot|H_\theta|^n\cdot 2^{2nR_2}}$$

For some $\epsilon > 0$ such that $\epsilon \to 0$ as $n \to \infty$. Here, $\mathbf{0}$ is a vector whose components are indexed by $(p, r) \in \mathscr{Q}(G)$ and whose $(p, r)^{\text{th}}$ component is equal to 0. We have

$$P(Err_{e2}|m_2) \leq \frac{|\mathbf{G}|^n \cdot 2^{nR_2}}{|J| \cdot 2^{n[H(X_2)-\epsilon]}} + \sum_{\substack{\theta \in \Theta \\ \theta \neq \mathbf{0}, \theta \neq \boldsymbol{r}}} \frac{|\mathbf{G}|^n \cdot |T_\theta| \cdot 2^{n[H(X_2|[X_2]_\theta)+\epsilon]}}{|H_\theta|^n \cdot |J| \cdot 2^{n[H(X_2)-\epsilon]}}$$

Note that $|J| = 2^{nR_g}$, $|T_\theta| = 2^{n(1-\omega_\theta)R_g}$ and $\frac{|\mathbf{G}|^n}{|H_\theta|^n} = |\mathbf{G} : H_\theta|^n$. In order for the probability of error to go to zero, we require

$$\begin{aligned} R_g - R_2 &> \log|\mathbf{G}| - H(X_2) \\ R_g &> \max_{\substack{\theta \in \Theta \\ \theta \neq \mathbf{0}, \theta \neq \boldsymbol{r}}} \frac{1}{\omega_\theta}[\log|\mathbf{G} : H_\theta| - H([X_2]_\theta)] \end{aligned}$$

which is equivalent to

$$\begin{aligned} R_g - R_2 &> \log|\mathbf{G}| - H(X_2) \\ R_g &> \max_{\substack{\theta \in \Theta \\ \theta \neq \mathbf{0}}} \frac{1}{\omega_\theta}[\log|\mathbf{G} : H_\theta| - H([X_2]_\theta)] \end{aligned}$$

or

$$\begin{aligned} R_g - R_2 &> \log|\mathbf{G}| - H(X_2) \\ R_g &> I^{\mathbf{G}}_{s.c.}(X_2; X_2) \end{aligned}$$

#### 3.4.2.2 The Error Event $Err_{d2}$:

We have

$$P_{avg}(Err_{d2} \cap Err^c_{e2}) = \frac{1}{2^{nR_2}} \sum_{m_2=1}^{2^{nR_2}} \sum_{\boldsymbol{x}_2 \in A^n_\epsilon(X_2)} \mathbb{1}_{\{\cup_{a \in J}\{\phi(a)+\boldsymbol{b}_2 = \boldsymbol{x}_2, s(a)=m_2\}\}} P(\boldsymbol{x}_2 \text{ is sent})$$

$$\sum_{\boldsymbol{y}_2 \in \mathscr{Y}_2^n} p^n_{Y_2|X_2}(\boldsymbol{y}_2|\boldsymbol{x}_2) \mathbb{1}\left\{\cup_{\substack{\tilde{m}_2=1 \\ \tilde{m}_2 \neq m_2}}^{2^{nR_2}} \cup_{\tilde{\boldsymbol{x}}_2 \in A^n_\epsilon(X_2|\boldsymbol{y}_2)} \cup_{\tilde{a} \in J}\{\phi(\tilde{a}) + \boldsymbol{b}_2 = \tilde{\boldsymbol{x}}_2, s(\tilde{a}) = \tilde{m}_2\}\right\}$$

Therefore,

$$\mathbb{E}\{P(Err_{d2})\} \leq \frac{1}{2^{nR_2}} \sum_{m_2=1}^{2^{nR_2}} \sum_{\boldsymbol{x}_2 \in A_\epsilon^n(X_2)} \frac{2}{\mathbb{E}\{\theta_2(m_2)\}} \sum_{a \in J} \sum_{\boldsymbol{y}_2 \in \mathscr{Y}_2^n} p_{Y_2|X_2}^n(\boldsymbol{y}_2|\boldsymbol{x}_2) \sum_{\substack{\tilde{m}_2=1 \\ \tilde{m}_2 \neq m_2}}^{2^{nR_2}}$$

$$\sum_{\tilde{\boldsymbol{x}}_2 \in A_\epsilon^n(X_2|\boldsymbol{y}_2)} \sum_{\tilde{a} \in J} P\left(\phi(\tilde{a}) + \boldsymbol{b}_2 = \tilde{\boldsymbol{x}}_2, \phi(a) + \boldsymbol{b}_2 = \boldsymbol{x}_2\right) P\left(s(a) = m_2, s(\tilde{a}) = \tilde{m}_2\right)$$

$$= \frac{1}{2^{nR_2}} \sum_{m_2=1}^{2^{nR_2}} \sum_{\substack{\tilde{m}_2=1 \\ \tilde{m}_2 \neq m_2}}^{2^{nR_2}} \sum_{a \in J} \sum_{\substack{\tilde{a} \in J \\ \tilde{a} \neq a}} \sum_{\boldsymbol{x}_2 \in A_\epsilon^n(X_2)} \frac{2}{\mathbb{E}\{\theta_2(m_2)\}} \sum_{\boldsymbol{y}_2 \in \mathscr{Y}_2^n} p_{Y_2|X_2}^n(\boldsymbol{y}_2|\boldsymbol{x}_2)$$

$$\sum_{\tilde{\boldsymbol{x}}_2 \in A_\epsilon^n(X_2|\boldsymbol{y}_2)} P\left(\phi(\tilde{a}) + \boldsymbol{b}_2 = \tilde{\boldsymbol{x}}_2, \phi(a) + \boldsymbol{b}_2 = \boldsymbol{x}_2\right) P\left(s(a) = m_2, s(\tilde{a}) = \tilde{m}_2\right)$$

$$= \frac{1}{2^{nR_2}} \sum_{m_2=1}^{2^{nR_2}} \sum_{\substack{\tilde{m}_2=1 \\ \tilde{m}_2 \neq m_2}}^{2^{nR_2}} \sum_{a \in J} \sum_{\substack{\theta \in \Theta \\ \theta \neq \boldsymbol{r}}} \sum_{\tilde{a} \in T_\theta(a)} \sum_{\boldsymbol{x}_2 \in A_\epsilon^n(X_2)} \frac{2}{\mathbb{E}\{\theta_2(m_2)\}} \sum_{\boldsymbol{y}_2 \in \mathscr{Y}_2^n} p_{Y_2|X_2}^n(\boldsymbol{y}_2|\boldsymbol{x}_2)$$

$$\sum_{\substack{\tilde{\boldsymbol{x}}_2 \in A_\epsilon^n(X_2|\boldsymbol{y}_2) \\ \tilde{\boldsymbol{x}}_2 \in \boldsymbol{x}_2 + H_\theta^n}} \frac{1}{|\mathbf{G}|^n \cdot |H_\theta|^n} \frac{1}{2^{2nR_2}}$$

$$\leq 2 \sum_{\substack{\theta \in \Theta \\ \theta \neq \boldsymbol{r}}} \frac{|T_\theta| \cdot 2^{n[H(X_2|[X_2]_\theta Y_2) + \epsilon]}}{|H_\theta|^n}$$

Therefore, in order for the probability of error to go to zero, we require

$$\frac{2^{nH(X_2|[X_2]_\theta Y_2)} \cdot |T_\theta|}{|H_\theta|^n} = \frac{2^{nH(X_2|[X_2]_\theta Y_2)} \cdot 2^{n(1-\omega_\theta)R_g}}{|H_\theta|^n} \to 0$$

for $\theta \neq \boldsymbol{r}$ or equivalently, we need to have

$$R_g < \frac{1}{1-\omega_\theta} \left[\log |H_\theta| - H(X_2|[X_2]_\theta Y_2)\right]$$

for $\theta \neq \boldsymbol{r}$. Therefore, it is sufficient to have $R_g < I_{c.c.}^{\mathbf{G}}(X_2; Y_2)$.

#### 3.4.2.3 The Error Event $Err_{d1}$:

Let $P_1$ be the probability that both $x_1$ and $\boldsymbol{x}_2 + \boldsymbol{x}_3$ are decoded incorrectly and let $P_2$ be the probability that $x_1$ is decoded incorrectly but $\boldsymbol{x}_2 + \boldsymbol{x}_3$ is decoded correctly. We have

$$P_{avg}(Err_{d1} \cap Err_{e1}^c \cap Err_{e2}^c \cap Err_{e3}^c) \leq P_1 + P_2$$

where

$$P_1 \leq \frac{1}{2^{nR_1}} \sum_{m_1=1}^{2^{nR_1}} \sum_{x_1 \in A_\epsilon^n(X_1)} \mathbb{1}_{\{\mathbb{C}_{r1}(m_1)=x_1\}} \frac{1}{2^{nR_2}} \sum_{m_2=1}^{2^{nR_2}} \frac{1}{2^{nR_3}} \sum_{m_3=1}^{2^{nR_3}} \sum_{\boldsymbol{x}_2 \in A_\epsilon^n(X_2)} \frac{2}{\mathbb{E}\{\theta_2(m_2)\}}$$
$$\sum_{\boldsymbol{x}_3 \in A_\epsilon^n(X_3)} \frac{2}{\mathbb{E}\{\theta_3(m_3)\}} \sum_{y_1 \in \mathscr{Y}_1^n} p_{Y_1|X_1}^n(y_1|x_1, \boldsymbol{x}_2, \boldsymbol{x}_3)$$
$$\sum_{\substack{\tilde{m}_1=1 \\ \tilde{m}_1 \neq m_1}}^{2^{nR_1}} \sum_{a,b \in J} \mathbb{1}_{\{\phi(a)+\boldsymbol{b}_2=\boldsymbol{x}_2, \phi(b)+\boldsymbol{b}_3=\boldsymbol{x}_3, s(a)=m_2, t(b)=m_3\}}$$
$$\sum_{\substack{(\tilde{x_1}, \tilde{z}) \in A_\epsilon^n(X_1, X_2+X_3|y_1) \\ \tilde{z} \neq \boldsymbol{x}_2+\boldsymbol{x}_3}} \mathbb{1}_{\{\tilde{x}_1=\mathbb{C}_{r1}(\tilde{m}_1)\}} \mathbb{1}_{\{\exists \tilde{a}, \tilde{b} \in J : \phi(\tilde{a})+\boldsymbol{b}_2+\phi(\tilde{b})+\boldsymbol{b}_3=\tilde{z}\}}$$

and

$$P_2 \leq \frac{1}{2^{nR_1}} \sum_{m_1=1}^{2^{nR_1}} \sum_{x_1 \in A_\epsilon^n(X_1)} \mathbb{1}_{\{\mathbb{C}_{r1}(m_1)=x_1\}} \frac{1}{2^{nR_2}} \sum_{m_2=1}^{2^{nR_2}} \frac{1}{2^{nR_3}} \sum_{m_3=1}^{2^{nR_3}} \sum_{\boldsymbol{x}_2 \in A_\epsilon^n(X_2)}$$
$$\frac{2}{\mathbb{E}\{\theta_2(m_2)\}} \sum_{\boldsymbol{x}_3 \in A_\epsilon^n(X_3)} \frac{2}{\mathbb{E}\{\theta_3(m_3)\}} \sum_{y_1 \in \mathscr{Y}_1^n} p_{Y_1|X_1}^n(y_1|x_1, \boldsymbol{x}_2, \boldsymbol{x}_3)$$
$$\sum_{\substack{\tilde{m}_1=1 \\ \tilde{m}_1 \neq m_1}}^{2^{nR_1}} \sum_{a,b \in J} \mathbb{1}_{\{\phi(a)+\boldsymbol{b}_2=\boldsymbol{x}_2, \phi(b)+\boldsymbol{b}_3=\boldsymbol{x}_3, s(a)=m_2, t(b)=m_3\}} \sum_{(\tilde{x_1}, \boldsymbol{x}_2+\boldsymbol{x}_3) \in A_\epsilon^n(X_1, X_2+X_3|y_1)} \mathbb{1}_{\{\tilde{x}_1=\mathbb{C}_{r1}(\tilde{m}_1)\}}$$

Note that the event $\{\exists \tilde{a}, \tilde{b} \in J : \phi(\tilde{a}) + \boldsymbol{b}_2 + \phi(\tilde{b}) + \boldsymbol{b}_3 = \tilde{z}\}$ is equal to the event $\{\exists \tilde{c} \in J : \phi(\tilde{c}) + \boldsymbol{b}_2 + \boldsymbol{b}_3 = \tilde{z}\}$. Therefore, using the union bound, we get

$$P_1 \leq \frac{1}{2^{nR_1}} \sum_{m_1=1}^{2^{nR_1}} \sum_{x_1 \in A_\epsilon^n(X_1)} \mathbb{1}_{\{\mathbb{C}_{r1}(m_1)=x_1\}} \frac{1}{2^{nR_2}} \sum_{m_2=1}^{2^{nR_2}} \frac{1}{2^{nR_3}} \sum_{m_3=1}^{2^{nR_3}} \sum_{\boldsymbol{x}_2 \in A_\epsilon^n(X_2)}$$
$$\frac{2}{\mathbb{E}\{\theta_2(m_2)\}} \sum_{\boldsymbol{x}_3 \in A_\epsilon^n(X_3)} \frac{2}{\mathbb{E}\{\theta_3(m_3)\}} \sum_{y_1 \in \mathscr{Y}_1^n} p_{Y_1|X_1}^n(y_1|x_1, \boldsymbol{x}_2, \boldsymbol{x}_3)$$
$$\sum_{\substack{\tilde{m}_1=1 \\ \tilde{m}_1 \neq m_1}}^{2^{nR_1}} \sum_{a,b \in J} \mathbb{1}_{\{\phi(a)+\boldsymbol{b}_2=\boldsymbol{x}_2, \phi(b)+\boldsymbol{b}_3=\boldsymbol{x}_3, s(a)=m_2, t(b)=m_3\}} \sum_{\substack{(\tilde{x_1}, \tilde{z}) \in A_\epsilon^n(X_1, X_2+X_3|y_1) \\ \tilde{z} \neq \boldsymbol{x}_2+\boldsymbol{x}_3}}$$
$$\mathbb{1}_{\{\tilde{x}_1=\mathbb{C}_{r1}(\tilde{m}_1)\}} \sum_{\tilde{c} \neq a+b} \mathbb{1}_{\{\phi(\tilde{c})+\boldsymbol{b}_2+\boldsymbol{b}_3=\tilde{z}\}}$$

Therefore,

$$\begin{aligned}
\mathbb{E}\{P_1\} \leq & \frac{1}{2^{nR_1}} \sum_{m_1=1}^{2^{nR_1}} \sum_{x_1 \in A_\epsilon^n(X_1)} \mathbb{1}_{\{\mathbb{C}_{r1}(m_1)=x_1\}} \frac{1}{2^{nR_2}} \sum_{m_2=1}^{2^{nR_2}} \frac{1}{2^{nR_3}} \sum_{m_3=1}^{2^{nR_3}} \sum_{\substack{\boldsymbol{x}_2 \in A_\epsilon^n(X_2) \\ \boldsymbol{x}_3 \in A_\epsilon^n(X_3)}} \\
& \frac{4}{\mathbb{E}\{\theta_2(m_2)\} \cdot \mathbb{E}\{\theta_3(m_3)\}} \sum_{y_1 \in \mathscr{Y}_1^n} p_{Y_1|X_1}^n(y_1|x_1, \boldsymbol{x}_2, \boldsymbol{x}_3) \\
& \sum_{\substack{\tilde{m}_1=1 \\ \tilde{m}_1 \neq m_1}}^{2^{nR_1}} \sum_{a,b \in J} \sum_{\substack{\theta \in \Theta \\ \theta \neq \boldsymbol{r}}} \sum_{\substack{(\tilde{x_1}, \tilde{z}) \in A_\epsilon^n(X_1, X_2+X_3|y_1) \\ \tilde{z} \neq \boldsymbol{x}_2 + \boldsymbol{x}_3}} \sum_{\tilde{c} \in T_\theta(a+b)} \frac{1}{|\mathbf{G}|^n} \cdot \frac{1}{|A_\epsilon^n(X_1)|} \cdot \\
& P\left(\phi(a+b) + \boldsymbol{b}_2 + \boldsymbol{b}_3 = \boldsymbol{x}_2 + \boldsymbol{x}_3, \phi(\tilde{c}) + \boldsymbol{b}_2 + \boldsymbol{b}_3 = \tilde{z}\right) \\
= & \frac{1}{2^{nR_1}} \sum_{m_1=1}^{2^{nR_1}} \sum_{x_1 \in A_\epsilon^n(X_1)} \mathbb{1}_{\{\mathbb{C}_{r1}(m_1)=x_1\}} \frac{1}{2^{nR_2}} \sum_{m_2=1}^{2^{nR_2}} \frac{1}{2^{nR_3}} \sum_{m_3=1}^{2^{nR_3}} \sum_{\substack{\boldsymbol{x}_2 \in A_\epsilon^n(X_2) \\ \boldsymbol{x}_3 \in A_\epsilon^n(X_3)}} \\
& \frac{4}{\mathbb{E}\{\theta_2(m_2)\} \cdot \mathbb{E}\{\theta_3(m_3)\}} \sum_{y_1 \in \mathscr{Y}_1^n} p_{Y_1|X_1}^n(y_1|x_1, \boldsymbol{x}_2, \boldsymbol{x}_3) \\
& \sum_{\substack{\tilde{m}_1=1 \\ \tilde{m}_1 \neq m_1}}^{2^{nR_1}} \sum_{a,b \in J} \sum_{\substack{\theta \in \Theta \\ \theta \neq \boldsymbol{r}}} \sum_{\substack{(\tilde{x_1}, \tilde{z}) \in A_\epsilon^n(X_1, X_2+X_3|y_1) \\ \tilde{z} \in \boldsymbol{x}_2 + \boldsymbol{x}_3 + H_\theta^n}} \sum_{\tilde{c} \in T_\theta(a+b)} \frac{1}{|\mathbf{G}|^n} \cdot \frac{1}{|A_\epsilon^n(X_1)|} \cdot \frac{1}{|\mathbf{G}|^n \cdot |H_\theta|^n} \\
\leq & \sum_{\substack{\theta \in \Theta \\ \theta \neq \boldsymbol{r}}} \frac{2^{nR_1} \cdot 2^{n[H(X_1|Y_1)+\epsilon]} \cdot 2^{n[H(Z|[Z]_\theta X_1 Y_1)+\epsilon]} \cdot |T_\theta|}{2^{n[H(X_1)-\epsilon]} \cdot |H_\theta^n|}
\end{aligned}$$

Note that $|T_\theta| = 2^{n(1-\omega_\theta)R_g}$. Therefore, in order for the probability of error to go to zero, it suffices to have

$$R_1 + (1-\omega_\theta)R_g < I(X_1;Y_1) + \log|H_\theta| - H(Z|[Z]_\theta X_1 Y_1)$$

for $\theta \neq \boldsymbol{r}$. For optimum weights $\{w_{p,r}\}_{(p,r)\in\mathscr{Q}(G)}$, the condition $R_1 + R_g < I(X_1;Y_1) + I_{c.c.}(Z;X_1Y_1)$ implies

$$\begin{aligned}
R_g < & (I(X_1;Y_1) - R_1) + \min_{\substack{\theta \in \Theta \\ \theta \neq \boldsymbol{r}}} \frac{1}{1-\omega_\theta} \left[\log|H_\theta| - H(Z|[Z]_\theta X_1 Y_1)\right] \\
\overset{(a)}{=} & \min_{\substack{\theta \in \Theta \\ \theta \neq \boldsymbol{r}}} \frac{1}{1-\omega_\theta} \left[I(X_1;Y_1) - R_1\right] + \min_{\substack{\theta \in \Theta \\ \theta \neq \boldsymbol{r}}} \frac{1}{1-\omega_\theta} \left[\log|H_\theta| - H(Z|[Z]_\theta X_1 Y_1)\right] \\
\leq & \min_{\substack{\theta \in \Theta \\ \theta \neq \boldsymbol{r}}} \frac{1}{1-\omega_\theta} \left[I(X_1;Y_1) - R_1 + \log|H_\theta| - H(Z|[Z]_\theta X_1 Y_1)\right]
\end{aligned}$$

which is the desired condition. In the above equations, $(a)$ follows since the maximum of $1-\omega_\theta$ is attained for $\theta=\mathbf{0}$ and is equal to 1.

Similarly, for $P_2$ we have

$$\begin{aligned}\mathbb{E}\{P_2\} \leq & \frac{1}{2^{nR_1}} \sum_{m_1=1}^{2^{nR_1}} \sum_{x_1 \in A_\epsilon^n(X_1)} \mathbb{1}_{\{\mathbb{C}_{r1}(m_1)=x_1\}} \frac{1}{2^{nR_2}} \sum_{m_2=1}^{2^{nR_2}} \frac{1}{2^{nR_3}} \sum_{m_3=1}^{2^{nR_3}} \sum_{\boldsymbol{x}_2 \in A_\epsilon^n(X_2)} \\ & \frac{2}{\mathbb{E}\{\theta_2(m_2)\}} \sum_{\boldsymbol{x}_3 \in A_\epsilon^n(X_3)} \frac{2}{\mathbb{E}\{\theta_3(m_3)\}} \sum_{y_1 \in \mathscr{Y}_1^n} p_{Y_1|X_1}^n(y_1|x_1,\boldsymbol{x}_2,\boldsymbol{x}_3) \\ & \sum_{\substack{\tilde{m}_1=1 \\ \tilde{m}_1 \neq m_1}}^{2^{nR_1}} \sum_{a,b \in J} \frac{1}{|\mathbf{G}|^{2n}} \frac{1}{2^{nR_2} \cdot 2^{nR_2}} \sum_{(\tilde{x_1},\boldsymbol{x}_2+\boldsymbol{x}_3) \in A_\epsilon^n(X_1,X_2+X_3|y_1)} \frac{1}{|A_\epsilon^n(X_1)|} \\ \leq & \frac{2^{nR_1} \cdot 2^{n[H(X_1|Y_1,X_2+X_3)+\epsilon]}}{2^{n[H(X_1)-\epsilon]}}\end{aligned}$$

Therefore, it suffices to have $R_1 < I(X_1; Y_1, X_2+X_3)$.

# CHAPTER IV

# Non-Abelian Group Codes

There are several results in the literature suggesting that non-Abelian group block codes do not exhibit a good coding performance. Although there is no known general method to construct such codes, it is believed that these codes have poor Hamming distance properties and are inferior to Abelian group codes. In this paper, we show that to the contrary of this view, non-Abelian group codes can have a good coding performance and should not be ignored. We show that these codes can be superior to their Abelian counterpart if they are employed with joint typicality decoding. Moreover, we show that in certain multi-terminal communication problems such codes outperform random codes and other known structured codes by achieving points outside the known rate region. To do so, we construct the ensemble of non-Abelian group codes over Dihedral groups which constitute an important class of non-Abelian groups.

## 4.1 Introduction

Algebraic codes are an important class of codes in coding and information theory and the information-theoretic performance limits of such codes have been studied extensively in the literature [7, 18, 23, 35, 42, 57, 61]. It is known that linear codes are optimal for the point-to-point symmetric channel coding problem when the size of

the channel input alphabet is a prime power [23, 25]. These codes are also optimal for the lossless compression of a binary source [41]. Linear codes are a special class of algebraic codes which can only be defined over finite fields, hence over alphabets of size a power of a prime. The natural extensions of linear codes over arbitrary alphabets are called group codes which are classified as Abelian (commutative) and non-Abelian (non-commutative) group codes.

Structured codes are equally important in the multi-terminal communications problems. It is shown in [41] that for a special case of the distributed source coding problem, the average performance of the ensemble of linear codes can be superior to that of random codes. In recent years, this phenomenon has been observed for a wide class of multi-termianl problems [42, 50, 55]. Thus, characterizations of the information-theoretic performance limits of these codes became important. However, the structure of the code restricts the encoder to abide by certain algebraic constraints and hence the performance of such codes is inferior to random codes in some communication settings. For example, linear codes are the most structured class of codes and for some problems in multi-terminal communications, they are not optimal.

Abelian group codes are a generalization of linear codes which are algebraically structured and can be defined for any alphabet. Group codes were first studied by Slepian [68] for the Gaussian channel. In [6], the capacity of group codes for certain classes of channels has been found. Further results on the capacity of group codes were established in [7,8,61]. Abelian group codes can outperform unstructured codes as well as linear codes in certain communications problems [42]. It turns out that for the point-to-point communications, Abelian group codes are inferior to linear and random codes.

The class of Abelian group codes is a small fraction of group codes. Another step towards reducing the constraints of the code while maintaining some algebraic structure would be to consider non-Abelian group codes. However, It has been sug-

gested by several authors that non-Abelian group codes are inferior to Abelian group codes [27] [34] [46]. Moreover, they suggest that asymptotically good group codes over non-Abelian groups may not exist.

In this chapter, we consider the problem of evaluating the performance of non-Abelian group codes. Since there is no known method to construct such codes, we first characterize an ensemble of non-Abelian group block codes over an important class of non-Abelian groups, namely the Dihedral groups. We show that these codes can be characterized by the product two "dependent" linear subcodes each built on one of the two generators of the group. The dependency of the two linear subcodes is dictated by the fact the the two subcodes must commute to ensure the closure of the code under the group operation. This is much like any code over Abelian groups; the difference is that in the Abelian case, the commutativity of the linear subcodes is automatically satisfied and hence the subcodes can be chosen independently.

We use this ensemble for a simple point-to-point channel and observe that typical codes in this ensemble achieve the symmetric capacity of this specific channel. We show that this could not have been possible if we were to restrict ourselves to any Abelian subgroup of the input alphabet. Moreover, we show that this performance is superior to the performance of Abelian group codes built for this channel. We also consider a multi-terminal communications problem in which two users send codewords over a multiple access channel and at the receiver, we wish to reconstruct the product of the two codewords where the product is the group operation. We show that these codes are superior to random codes as well as linear codes in certain cases. We use a combination of algebraic and information-theoretic tools for this task.

## 4.2 Preliminaries

#### 4.2.0.4 Dihedral Groups

A dihedral group of order $2p$ is the group of symmetries of a regular $p$-gon, including reflections and rotations and any combination of these operations. A dihedral group can be represented as a quotient of a free group as follows: $D_{2p} = \langle x, y | x^p = 1, y^2 = 1, xyxy = 1 \rangle$. Dihedral groups are an important class of non-Abelian groups. Note that $N = \langle x | x^p = 1 \rangle = \{1, x, \cdots, x^{p-1}\}$ is a normal subgroup of $\mathbb{D}_{2p}$. The group $\mathbb{D}_6$ is the smallest non-Abelian group. Note that for two elements $g, h$ in $\mathbb{D}_6$, $g \cdot h$ may not be equal to $h \cdot g$.

#### 4.2.0.5 Typicality

We use the notion of strong typicality throughout this chapter (See Section 2.1).

#### 4.2.0.6 Notation

For a set $A$, $|A|$ denotes its size (cardinality) and for $g$ an element of a group $G$, $|g|$ denotes its order. Let $x$ be a generator of the group $G$ whose order is a non-negative integer $p$ and let $u = (u_1, \cdots, u_n)$ be a vector in $\mathbb{Z}_p^n$. Then $x^u$ denote the element $(x^{u_1}, \cdots, x^{u_n})$ of $G^n$.

## 4.3 Group Codes over $\mathbb{D}_{2p}$

Although there has been a lot of work on the properties of group codes in the literature, there is no universal approach to constructing the ensemble of such codes over arbitrary groups. Indeed, even for the smallest non-Abelian group, namely $\mathbb{D}_6$, the ensemble of group codes is not characterized. We do so in this section by constructing an ensemble of group codes over the group $\mathbb{D}_{2p}$. First, we consider the case where $p$ is a prime. The following theorem is the main result of this section:

**Theorem IV.1.** *Direct: Let* $\mathbb{N}$ *be a subgroup of* $\{1, x, \cdots, x^{p-1}\}^n \cong \mathbb{Z}_p^n$ *and let* $\mathbb{M}$ *be a subgroup of* $\bigoplus_{i=1}^n \{1, x^{\alpha_i} y\} \cong \mathbb{Z}_2^n$ *for some* $\alpha_1, \cdots, \alpha_n \in \{0, 1, \cdots, p-1\}$. *If* $\mathbb{N}$ *and* $\mathbb{M}$ *commute i.e. if* $\mathbb{N} \cdot \mathbb{M} = \mathbb{M} \cdot \mathbb{N}$, *then* $\mathbb{C} = \mathbb{N} \cdot \mathbb{M} = \mathbb{M} \cdot \mathbb{N}$ *is a group code over* $\mathbb{D}_{2p}$. *Converse: Let* $\mathbb{C}$ *be any group code over* $\mathbb{D}_{2p}$ *of length* $n$. *Then,* $\mathbb{C}$ *can be decomposed as* $\mathbb{C} = \mathbb{N} \cdot \mathbb{M}$ *where* $\mathbb{N} \leq \{1, x, \cdots, x^{p-1}\}^n \cong \mathbb{Z}_p^n$ *and* $\mathbb{M} \leq \bigoplus_{i=1}^n \{1, x^{\alpha_i} y\} \cong \mathbb{Z}_2^n$ *for some* $\alpha_1, \cdots, \alpha_n \in \{0, 1, \cdots, p-1\}$ *such that* $\mathbb{N} \cdot \mathbb{M} = \mathbb{M} \cdot \mathbb{N}$.

Note that this theorem facilitates the construction of group codes over $\mathbb{D}_{2p}$. Note that the two subcodes $\mathbb{N}$ and $\mathbb{M}$ are linear codes which can be easily constructed by taking the images of homomorphisms i.e. for some positive integer $l$ and matrix $G \in \mathbb{Z}_p^{l \times n}$, $\mathbb{N} = \{x^{uG} | u \in \mathbb{Z}_p^l\}$ and for some positive integer $k$ and matrix $H \in \mathbb{Z}_2^{k \times n}$ and numbers $\alpha_1, \cdots, \alpha_n \in \{0, 1, \cdots, p-1\}$, $\mathbb{M} = \{(x^{\alpha_1} y, \cdots, x^{\alpha_n} y)^{vH} | v \in \mathbb{Z}_2^k\}$ where $(x^{\alpha_1}, \cdots, x^{\alpha_n} y)^{vH}$ is an element of $\mathbb{D}_{2p}^n$ whose $i$th component is $x^{\alpha_i} y$ if the $i$th component of $vH$ is one and is 1 otherwise. Note that some care should be taken when choosing the matrices $G$ and $H$ to ensure that the two subcodes commute.
The proof of the direct part of Theorem IV.1 is standard and will be provided in a more complete version of this work. The converse part of the theorem guarantees that all group codes can be constructed in this manner; i.e. all group codes can be decomposed into two subcodes which commute. The rest of this section is devoted to proving the converse. We do so using the following lemmas.

**Lemma IV.2.** *For all* $g \in \mathbb{D}_{2p}^n$, *we have*

***a)*** $|g| \in \{1, 2, p, 2p\}$. *Specially* $g^{2p} = 1$.

***b)*** $g^2 \in N^n$.

***c)*** $g^p \in \{1, y, xy, \cdots, x^{p-1} y\}^n$.

***d)*** *If* $|g| = 2$ *then* $g \in \{1, y, xy, \cdots, x^{p-1} y\}^n$.

***e)*** *If* $|g| = p$ *then* $g \in N^n$.

*Proof.* The proof is standard and will be provided in a more complete version of this work. □

**Lemma IV.3.** *For $\mathbb{C} \leq \mathbb{D}_{2p}^n$, let $\mathbb{N} = \mathbb{C} \cap N^n$. Then we have $|\mathbb{C}| = 2^r|\mathbb{N}|$ for some non-negative integer $r$.*

*Proof.* Note that $N^n$ is a normal subgroup of $\mathbb{D}_p^n$. Therefore the product $\mathbb{C}N^n$ is also a subgroup of $\mathbb{D}_p^n$ and hence $|\mathbb{C}N^n|$ divides $|\mathbb{D}_p^n| = (2p)^n$. Furthermore, we have

$$|\mathbb{C}N^n| = \frac{|\mathbb{C}| \cdot |N^n|}{|\mathbb{C} \cap N^n|} = \frac{|\mathbb{C}| \cdot p^n}{|\mathbb{N}|}$$

It follows that $\frac{|\mathbb{C}|}{|\mathbb{N}|}$ divides $2^n$ and this implies $|\mathbb{C}| = 2^r|\mathbb{N}|$ for some non-negative integer $r$. □

In the following, we consider the implications of this lemma for a few special cases. These special cases are useful in proving the general case described in Lemmas IV.4 and IV.5.

**Special Case $r = 0$:** In this case, the code $\mathbb{C}$ is contained in the subgroup $N^n$ of $\mathbb{D}_{2p}^n$. This means $\mathbb{C}$ is a linear code.

**Special Case $r = 1$:** In this case, we have $|\mathbb{C}| = 2|\mathbb{N}|$. Since $\mathbb{N} = \mathbb{C} \cap N^n \neq \mathbb{C}$, there exist an element $g_1 \in \mathbb{C}$ such that $g_1 \notin N^n$. Since $\mathbb{N} \subseteq \mathbb{C}$ and $g_1 \in \mathbb{C}$, we must have $\mathbb{N} \cup \mathbb{N}g_1 \subseteq \mathbb{C}$. Note that different cosets of a subgroup are disjoint, therefore $|\mathbb{N} \cup \mathbb{N}g_1| = 2|\mathbb{N}| = |\mathbb{C}|$. Therefore, we must have $\mathbb{C} = \mathbb{N} \cup \mathbb{N}g_1$. By part $(b)$ of Lemma IV.2 we have $g_1^2 \in N^n$. By the closure of the code $\mathbb{C}$ under multiplication, we also have $g_1^2 \in \mathbb{C}$. Therefore, we have $g_1^2 \in \mathbb{N}$ or equivalently $\mathbb{N} = \mathbb{N}g_1^2$. Note that since $g_1 \notin \mathbb{N}$, $\mathbb{N}$ and $g_1\mathbb{N}$ are disjoint. Since $g_1\mathbb{N} \subseteq \mathbb{C}$, we have $\mathbb{N}g_1 = g_1\mathbb{N}$. Note that $g_1^2 \in \mathbb{N}$ implies $\mathbb{N}g_1 = \mathbb{N}g_1^3$. Let $h_1 = g_1^3$. By part $(c)$ of Lemma IV.2 the order of $h_1$ is at most two. Therefore, we have $\mathbb{C} = \mathbb{N} \cup \mathbb{N}h_1$ where $h_1$ takes values from $\{1, y, xy, \cdots, x^{p-1}y\}^n$. Furthermore, $\mathbb{N}g_1 = g_1\mathbb{N}$ implies $\mathbb{N}h_1 = h_1\mathbb{N}$ and $g_1 \notin N^n$ implies $h_1 \neq 1$. Note that always $h_1^2 = 1 \in \mathbb{N}$.

To summarize this case, for $r = 1$, we have $\mathbb{C} = \mathbb{N} \cup \mathbb{N}h_1$ for some $h_1 \in \{1, y, xy, \cdots, x^{p-1}y\}^n$ such that $h_1 \neq 1$ and $\mathbb{N}h_1 = h_1\mathbb{N}$. These conditions imply $\mathbb{N} \cup \mathbb{N}h_1 = \langle \mathbb{N}, h_1 \rangle$.

Now Assume $\mathbb{C} = \langle \mathbb{N}, g_1 \rangle$ where $\mathbb{C} \cap N^n = \mathbb{N}$. Then similarly to the above arguments, we have $g_1^2 \in \mathbb{N}$. Also note that for integers $a, b$, if $a + b$ is even, then $g_1^a \mathbb{N} g_1^b \subseteq N^n$ and $g_1^a \mathbb{N} g_1^b \subseteq \mathbb{C}$. Since $|g_1^a \mathbb{N} g_1^b| = |\mathbb{N}|$, we require $g_1^a \mathbb{N} g_1^b = \mathbb{N}$. Similarly, we can show that if $a+b$ is odd, then $g_1^a \mathbb{N} g_1^b = \mathbb{N}g_1$. This implies any sequence formed by $\mathbb{N}$ and $g_1$ can be reduced in one of the following two forms: $\mathbb{N}$ or $\mathbb{N}g_1$. Hence, the size of $\mathbb{C} = \langle \mathbb{N}, g_1 \rangle$ can be at most $2|\mathbb{N}|$ if we require $\mathbb{N} = \mathbb{C} \cap N^n$.

**Special Case $r = 2$:** Similarly to the above case, for $r = 2$, we can show $\mathbb{C} = \mathbb{N} \cup \mathbb{N}h_1 \cup \mathbb{N}h_2 \cup \mathbb{N}h_1h_2$ for some $h_1, h_2 \in \{1, y, xy, \cdots, x^{p-1}y\}^n$ such that $h_1, h_2 \neq 1, h_1 \neq h_2$, $\mathbb{N}h_j = h_j\mathbb{N}$ for $j = 1, 2$ and $h_1, h_2$ commute. These conditions imply $\mathbb{N} \cup \mathbb{N}h_1 \cup \mathbb{N}h_2 \cup \mathbb{N}h_1h_2 = \langle \mathbb{N}, h_1, h_2 \rangle$.

We address the general case in the following lemma:

**Lemma IV.4.** *For $\mathbb{C} \leq \mathbb{D}_{2p}^n$ let $\mathbb{N} = \mathbb{C} \cap N^n$. Write $\mathbb{C} = \langle \mathbb{N}, g_1, \cdots, g_k \rangle$ for some elements $g_1, \cdots, g_k \in \mathbb{C}$. Then we have*

*(a) For all $j = 1, \cdots, k$, $g_j\mathbb{N} = \mathbb{N}g_j$ and $g_j^2 \in \mathbb{N}$.*

*(b) For all $A \subseteq [1, k]$ and for all permutations $\pi : A \to A$,*

$$\mathbb{N}\left(\prod_{j\in A} g_{\pi(j)}\right) = \mathbb{N}\left(\prod_{j\in A} g_j\right) \tag{4.1}$$

*(c) $\mathbb{C} = \bigcup_{A\subseteq[1,k]} \left[\mathbb{N}\left(\prod_{j\in A} g_j\right)\right]$*

*Proof.* The proofs of parts $(a)$ and $(b)$ are through induction on $k$. We have shown above that these statement are valid for $k = 1, 2$. Assume that they are true for all

$k \leq K-1$ for some positive integer $K > 3$. We show that this implies the statements are true for $k = K$.

**Proof of** $(a)$**:** For $j = 1, \cdots, K$, let $\mathbb{C}' = \langle \mathbb{N}, g_j \rangle$. We have $\mathbb{N} \subseteq \mathbb{C}' \cap N^n \subseteq \mathbb{C} \cap N^n = \mathbb{N}$ . Therefore, $\mathbb{C}' \cap N^n = \mathbb{N}$ and hence we can use the induction hypothesis to conclude $g_j \mathbb{N} = \mathbb{N} g_j$ and $g_j^2 \in \mathbb{N}$.

**Proof of** $(b)$**:** If $|A| \leq K-1$, let $\mathbb{C}' = \langle \mathbb{N}, g_j : j \in A \rangle$. Similarly to the argument above, we can show that $\mathbb{C}' \cap N^n = \mathbb{N}$ and therefore we can use the induction hypothesis to conclude (4.1). Now assume $|A| = K$ or equivalently $A = [1, K]$ and fix a permutation $\pi : A \to A$. If $\pi(K) \neq 1$, use part $(a)$ to write

$$\begin{aligned} g_{\pi(1)} \cdots g_{\pi(K-1)} g_{\pi(K)} \mathbb{N} &= g_{\pi(1)} \cdots g_{\pi(K-1)} \mathbb{N} g_{\pi(K)} \\ &\overset{(i)}{=} g_1 \left( \prod_{j \in [2,K] \setminus \{\pi(K)\}} g_j \right) \mathbb{N} g_{\pi(K)} \\ &= g_1 \left( \prod_{j \in [2,K] \setminus \{\pi(K)\}} g_j \right) g_{\pi(K)} \mathbb{N} \\ &\overset{(ii)}{=} g_1 \left( \prod_{j \in [2,K]} g_j \right) \mathbb{N} = g_1 g_2 \cdots g_K \mathbb{N} \end{aligned}$$

where in $(i)$ and $(ii)$ we use the induction hypothesis for $k = K-1$. If $\pi(K) = 1$, use the induction hypothesis for $k = 2$ to write

$$g_{\pi(1)} \cdots g_{\pi(K-1)} g_{\pi(K)} \mathbb{N} = g_{\pi(1)} \cdots g_{\pi(K)} g_{\pi(K-1)} \mathbb{N}$$

After this step, we can use the same argument as above to show (4.1).

**Proof of** $(c)$**:** For any $w \in \mathbb{C} = \langle \mathbb{N}, g_1, \cdots, g_k \rangle$ we can find a sequence of integers $\alpha_{i1}, \cdots, \alpha_{ik}$ and $\beta_i$ for $i \in \mathbb{Z}$ such that $w \in \mathbb{N} \prod_{i \in \mathbb{Z}} \left( g_1^{\alpha_{i1}} \cdots g_k^{\alpha_{ik}} \mathbb{N}^{\beta} \right)$. Using the result of part $(a)$ and the fact that $\mathbb{N}^2 = \mathbb{N}$, we get $w \in \mathbb{N} \prod_{i \in \mathbb{Z}} (g_1^{\alpha_{i1}} \cdots g_k^{\alpha_{ik}})$. Using the result of part $(b)$ to reorder elements we obtain $w \in \mathbb{N} \left( g_1^{\sum_i \alpha_{i1}} \cdots g_k^{\sum_i \alpha_{ik}} \right)$. Using the result of part $(b)$ and the fact that $g_j^2 \in \mathbb{N}$ for $j = 1, \cdots, k$, we get $w \in \mathbb{N} \left( g_1^{\sum_i \alpha_{i1} \pmod 2} \cdots g_k^{\sum_i \alpha_{ik} \pmod 2} \right)$. This is equivalent to $w \in \mathbb{N} \left( \prod_{j \in A} g_j \right)$ for $A = \{ j = 1, \cdots, k | \sum_i \alpha_{i1} \pmod 2 = 1 \}$. $\square$

**Lemma IV.5.** *For $\mathbb{C} \leq \mathbb{D}_{2p}^n$, we can find elements $h_1, \cdots, h_k \in \{1, y, xy, \cdots, x^{p-1}y\}$ and a subgroup $\mathbb{N} \leq N^n$ such that $\mathbb{C} = \langle \mathbb{N}, h_1, \cdots, h_k \rangle$ and*

*(a) For all $j = 1, \cdots, k$, $h_j\mathbb{N} = \mathbb{N}h_j$.*

*(b) All $h_j$'s commute.*

*Proof.* Let $\mathbb{N} = \mathbb{C} \cap N^n$ and write $\mathbb{C} = \langle \mathbb{N}, g_1, \cdots, g_k \rangle$ for some elements $g_1, \cdots, g_k \in \mathbb{C}$. For $j = 1, \cdots, k$, define $h_j^{(0)} = g_j^3$. Define $h_1 = h_1^{(0)}$ and for $j = 2, \cdots, k$, define $h_j$ sequentially as follows: For $l = 1, \cdots, j-1$, let $h_j^{(l)} = h_j^{(l-1)} h_l h_j^{(l-1)} h_l h_j^{(l-1)}$ and finally let $h_j = h_j^{(j-1)}$. It is straightforward to verify that with these definitions $\mathbb{C} = \langle \mathbb{N}, h_1, \cdots, h_k \rangle$ and $(a)$ and $(b)$ are satisfied. The complete proof will be provided in a more complete version of this work. □

We are ready to prove the converse part of Theorem IV.1. For any $\mathbb{C} \leq \mathbb{D}_{2p}^n$, let $\mathbb{N} = \mathbb{C} \cap N^n$ and let $\mathbb{M} = \langle h_1, \cdots, h_k \rangle$ where $h_1, \cdots, h_k$ are as in Lemma IV.5. Is it straightforward to verify that $\mathbb{N}$ and $\mathbb{M}$ satisfy the conditions of the theorem.

*Remark* IV.6. Although in this section we addressed the case where $p$ is a prime, Theorem IV.1 is valid for arbitrary Dihedral groups $\mathbb{D}_{2q}$ for an arbitrary integer $q \geq 3$. The difference is that in the general case, the subcode $\mathbb{N}$ need not be a linear code but rather it is an Abelian group codes over the cyclic group $\mathbb{Z}_q$. The construction of Abelian group codes has been addressed in [61].

## 4.4 The Ensemble of Codes

In this section, we present an ensemble of codes which consists of all non-Abelian group codes over $\mathbb{D}_{2p}$ for some prime $p$. We make use of Lemma IV.5 to construct an ensemble of codes of length $n$ as follows:

- For $i = 1, \cdots, n$, choose $\alpha_1, \cdots, \alpha_n \in \{0, 1, \cdots, p\}$.
- For some $1 \leq m \leq n$, choose a partition $P = \{P_1, \cdots, P_m\}$ of $[1, n]$ so that for $i = 1, \cdots, m$, $|P_i| = r_i n$ for some $0 < r_i \leq 1$.

- For some $0 \leq k \leq n$, choose subsets $I_1, \cdots, I_k$ of $[1, m]$.
- For $j = 1, \cdots, k$, let $A_j = \cup_{i \in I_j} P_i$.
- For $j = 1, \cdots, k$, let $h_j = (h_{1j}, \cdots, h_{nj}) \in \mathbb{D}_{2p}^n$ where $h_{ij} = 1$ if $i \in A_j$ and $h_{ij} = x^{\alpha_i} y$ if $i \in A_j^c$.
- For some $0 \leq \kappa \leq 1$ and for $i = 1, \cdots, m$, Let $G_i$ be a matrix in $\{0, 1, 2\}^{[1, \kappa r_i n] \times P_m}$.
- A message is indexed by a set $J \subseteq [1, k]$ and by $u_i \in \mathbb{Z}_p^{[1, \kappa r_i n]}$ for $i = 1, \cdots, m$. The encoder maps the message $(J, u_1, \cdots, u_m)$ to

$$\mathrm{Enc}(J, u_1, \cdots, u_m) = x^{u_1 G 1 + \cdots u_m G_m} \prod_{j \in J} h_j$$

The rate of each code in this ensemble is equal to $R = \frac{1}{n}(k + \sum_{i=1}^n \kappa r_i \log p)$.
The rest of this section is devoted to proving that this ensemble contains all group codes. As in the statement of Lemma IV.5, let $\mathbb{C} = \langle \mathbb{N}, h_1, \cdots, h_k \rangle$ and for $j = 1, \cdots, k$, let $h_j = (h_{1j}, \cdots, h_{nj})$.

**Lemma IV.7.** *For $i = 1, \cdots, n$, there exists $\alpha_i$ such that for all $j = 1, \cdots, k$, $h_{ji} \in \{1, x^{\alpha_i} y\}$.*

*Proof.* Fix an $i \in [1, n]$ and assume there exists a $j \in [1, k]$ with $h_{ij} \neq 1$. Since $h_{ij} \in \{1, y, xy, \cdots, x^{p-1} y\}$, we can let $h_{ij} = x^{\alpha_i} y$ for some $\alpha_i$. Since all of $h_j$'s commute, for all $j' = 1, \cdots, k$, we have $h_{ij} h_{ij'} = h_{ij'} h_{ij}$ where $h_{ij'} \in \{1, y, xy, \cdots, x^{p-1} y\}$. This can only happen if $h_{ij'} \in \{1, x^{\alpha_i} y\}$. This proves the claim. □

For $j = 1, \cdots, k$, let $A_j = \{i | h_{ij} = 1\}$.

**Lemma IV.8.** *If $\mathbb{N} h_1 = h_1 \mathbb{N}$, then $\mathbb{N} = \mathbb{N}_{A_1} \oplus \mathbb{N}_{A_1^c}$ such that $Proj_{A_1}(\mathbb{N}_{A_1^c}) = 0$ and $Proj_{A_1^c}(\mathbb{N}_{A_1}) = 0$.*

*Proof.* Let $g = (g_1, \cdots, g_2)$ be a vector in $\mathbb{N}$ and with a slight abuse of notation let's write $g = g_{A_1} \oplus g_{A_1^c}$ and $h_1 = h_{A_1,1} \oplus h_{A_1^c,1}$ (Note that $h_{A_1,1}$ is a vector of all ones by definition and $h_{A_1^c,1}$ is a vector of elements of the form $x^\alpha y$). We have $h_1 g h_1 = g_{A_1} \oplus g_{A_1^c}^{-1} \in \mathbb{C}$. Since $h_1 g h_1 \in N^n$, we must have $h_1 g h_1 = g_{A_1} \oplus g_{A_1^c}^{-1} \in \mathbb{N}$. Therefore, $(g_1 h_1 g h_1)^{\frac{p+1}{2}} = g_{A_1} \oplus 1_{A_1^c} \in \mathbb{N}$. With a similar argument, we can show that $1_{A_1} \oplus g_{A_1^c} \in \mathbb{N}$. To complete the proof, let

$$\mathbb{N}_{A_1} = \{g_{A_1} \oplus 1_{A_1^c} | g \in \mathbb{N}\} = \mathrm{Proj}_{A_1}(\mathbb{N})$$
$$\mathbb{N}_{A_1^c} = \{1_{A_1} \oplus g_{A_1^c} | g \in \mathbb{N}\} = \mathrm{Proj}_{A_1^c}(\mathbb{N})$$

In other words, we have shown that if $\mathbb{N} h_1 = h_1 \mathbb{N}$, then $\mathbb{N} = \mathrm{Proj}_{A_1}(\mathbb{N}) \oplus \mathrm{Proj}_{A_1^c}(\mathbb{N})$.

□

**Lemma IV.9.** *The subcode* $\mathbb{N}$ *can be decomposed as*

$$\bigoplus_{J \subseteq [1,k]} Proj_{\left(\cap_{j \in J} A_j\right) \cap \left(\cap_{j \in J^c} A_j^c\right)}(\mathbb{N})$$

*Proof.* By Lemma IV.8, for all $j = 1, \cdots, k$, we have $\mathbb{N} = \mathrm{Proj}_{A_j}(\mathbb{N}) \oplus \mathrm{Proj}_{A_j^c}(\mathbb{N})$. We have

$$\begin{aligned}
\mathbb{N} &= \mathrm{Proj}_{A_2}\Big(\mathrm{Proj}_{A_1}(\mathbb{N}) \oplus \mathrm{Proj}_{A_1^c}(\mathbb{N})\Big) \oplus \\
&\qquad \mathrm{Proj}_{A_2^c}\Big(\mathrm{Proj}_{A_1}(\mathbb{N}) \oplus \mathrm{Proj}_{A_1^c}(\mathbb{N})\Big) \\
&= \mathrm{Proj}_{A_1 \cap A_2}(\mathbb{N}) \oplus \mathrm{Proj}_{A_1^c \cap A_2}(\mathbb{N}) \oplus \\
&\qquad \mathrm{Proj}_{A_1 \cap A_2^c}(\mathbb{N}) \oplus \mathrm{Proj}_{A_1^c \cap A_2^c}(\mathbb{N})
\end{aligned}$$

This proves the lemma for $k = 2$. The general case can be proved in a similar fashion. □

Define the collection of sets $P$ as

$$P = \Big\{ \Big( \cap_{j \in J} A_j \Big) \cap \Big( \cap_{j \in J^c} A_j^c \Big) \Big| J \subseteq [1, k] \Big\}$$

Then $P$ forms a partition of $[1, n]$ as $P = \{P_1, \cdots, P_m\}$ such that each $A_j$ can be written as union of $P_i$'s. To summarize, we have $\mathbb{N} = \bigoplus_{i=1}^{m} \text{Proj}_{P_i}(\mathbb{N})$. In the construction above, the matrix $G_i$ is used to form the subgroup $\text{Proj}_{P_i}(\mathbb{N})$.

## 4.5 Examples: Non-Abelian Group Codes Can Have a Good Performance

In this section, we consider two simple examples. These examples are chosen so that the construction and analysis of the ensemble of non-Abelian group codes and the computation of the achievable rate becomes simple. In the first example, we show that the achievable rate using non-Abelian group codes can be strictly larger than the rate achievable using Abelian group codes for the point-to-point problem. We also show that this rate is not achievable if we restrict ourselves to any Abelian subgroup of the alphabet. In the second example, we consider a scenario in which two users try to communicate the sum of two symbol streams with a joint decoder through a multiple access channel. We show that for this specific example, the achievable rate using non-Abelian codes can be strictly larger than the rate achievable using random codes. This shows in certain multi-terminal communications problems non-Abelian group codes can be beneficial by achieving points which are not achievable using other type of codes.

In both examples, the parameters of the ensemble of codes is as follows: $\beta_0 = \cdots = \beta_n = 0$, $m = n$, $P_i = \{i\}$, $r_i = \frac{1}{n}$, $l$ is a fixed parameter determined by the rate of the code, $I_1, \cdots, I_l$ are uniformly random, $\kappa = 1$ and $G_i$ is uniformly random. Note that with these parameters, $\mathbb{N} = N^n$ and $\mathbb{M} = \{y^{vH} | v \in \mathbb{Z}_2^k\}$ for some uniformly random $k \times n$ matrix $H$.

### 4.5.1 Example 1: Point-to-Point Problem

Consider the channel depicted in Figure 4.1. The Shannon capacity of this channel

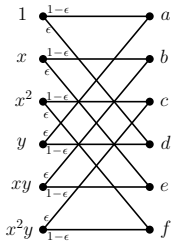


Figure 4.1: A simple channel with input $\mathbb{D}_6$.

is $C = \log 6 - h(\epsilon)$ bits per channel use. It turns out that using the joint typicality decoding, the average code in the ensemble of non-Abelian group codes can achieve the shannon capacity $R = \log 6 - h(\epsilon)$. If we restrict ourselves to Abelian subgroups of $\mathbb{D}_6$ we can achieve (in bits per channel use) 1.585 for $\{1, x, x^2\}$, $1 - h(\epsilon)$ for $\{1, y\}$ and 1.000 for $\{1, xy\}$and $\{1, x^2y\}$. All of these rates are less than the rate achievable using non-Abelian group codes.

### 4.5.2 Example 2: Computation Over MAC

In this section, we use the ensemble of codes constructed in Section 4.4 for a problem of computation over multiple access channels. Consider the two-user MAC depicted in Figure 4.2 where $X$, $Z$ take values from the Dihedral group $\mathbb{D}_6$ and $Y$ takes values from a finite set $\mathscr{Y}$.

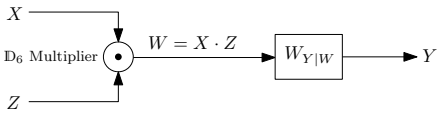


Figure 4.2: Two user MAC: Computation of $\mathbb{D}_6$ operation.

When the inputs of the channel are $x, z \in \mathbb{D}_6$, the channel output is $y \in \mathscr{Y}$ with conditional probability $W_{Y|XZ}(y|x, z)$. Let $n$ be the block length and let $\mathbb{C}_1 \subseteq \mathbb{D}_6^n$ and $\mathbb{C}_2 \subseteq \mathbb{D}_6^n$ be codebooks corresponding to Users 1 and 2 respectively. If User 1

sends a message $\boldsymbol{x} \in \mathbb{C}_1$ and User 2 sends a message $\boldsymbol{z} \in \mathbb{C}_2$, the decoder wishes to reconstruct $\boldsymbol{x} \cdot \boldsymbol{z}$ losslessly where the multiplication is the component-wise group operation.

Note that in this example, the MAC is multiplicative in the sense that the two terminals get multiplied (the group operation) and then the result is passed through a point-to-point channel. The channel $W_{Y|W}$ is taken to be the channel of Example 1. The encoding/decoding strategy is as follows: Let $\mathbb{C}_1 = \{B_1 x^u y^{Hv} | u \in \mathbb{Z}_3^n, v \in \mathbb{Z}_2^k\}$ and $\mathbb{C}_2 = \{y^{Hv} x^u B_2 | u \in \mathbb{Z}_3^n, v \in \mathbb{Z}_2^k\}$ for some $H \in \mathbb{Z}_2^{k \times n}$. The decoder, after receiving the channel output, looks for a unique codeword in $\mathbb{C}_1 \cdot \mathbb{C}_2$ which is jointly typical with the channel output. If it doesn't find such a codeword, it declares error. The average probability of error for the codes in this ensemble is given by

$$P_{err} = \frac{1}{3^{2n} 2^{2k}} \sum_{\boldsymbol{x} \in \mathbb{C}_1} \sum_{\boldsymbol{z} \in \mathbb{C}_2} \sum_{\boldsymbol{y} \in \mathscr{Y}^n} W_{Y|W}^n(\boldsymbol{y}|\boldsymbol{x} \cdot \boldsymbol{z}) \sum_{\substack{\boldsymbol{w} \in \mathbb{C}_1 \cdot \mathbb{C}_2 \\ \boldsymbol{w} \neq \boldsymbol{x} \cdot \boldsymbol{z}}} \mathbb{1}_{\{\boldsymbol{w} \in A_\epsilon^n(W|\boldsymbol{y})\}}$$

This probability of error approaches zero as $n$ increase for $R < \log 6 - h(\epsilon)$ bits per channel use which is equal to the point-to-point capacity of the channel. If we restrict ourselves to the Abelian subgroup $\{1, x, x^2\}$, we can show that the rate $R = 1.585$ is achievable. The achievable rate using random codes is equal to $R = I(XZ;Y)/2 = (\log 6 - h(\epsilon))/2$. We observe that for this example, non-Abelian group codes outperform Abelian group codes and Abelian group codes outperform random codes. This is due to the fact that the structure of the channel is matched to the structure of non-Abelian group codes.

# CHAPTER V

# Lattice Codes for Multi-terminal Communications

## 5.1 Nested Lattices for Point-to-Point Communications

In this section, we show that nested lattice codes achieve the capacity of arbitrary channels with or without non-casual state information at the transmitter. We also show that nested lattice codes are optimal for source coding with or without non-causal side information at the receiver for arbitrary continuous sources.

Lattice codes for continuous sources and channels are the analogue of linear codes for discrete sources and channels and play an important role in information theory and communications. Linear/lattice and nested linear/lattice codes have been used in many communication settings to improve upon the existing random coding bounds [17, 41–44, 50, 55, 69].

In [17] and [43] the existence of lattice codes satisfying Shannon's bound has been shown. These results have been generalized and the close relation between linear and lattice codes has been pointed out in [44]. In [76], several results regarding lattice quantization noise in high resolution has been derived and the problem of constructing lattices with an arbitrary quantization noise distribution has been studied in [30].

Nested lattice codes were introduced in [79] where the concept of structured binning is presented. Nested linear/lattice code are important because in many com-

munication problems, specially multi-terminal settings, such codes can be superior in average performance compared to random codes [42]. It has been shown in [77] that nested lattice codes are optimal for the Wyner-Ziv problem when the source and side information are jointly Gaussian. The dual problem of channel coding with state information has been addressed in [71] and the optimality of lattice codes for Gaussian channels has been shown. In [51] it has been shown that nested linear codes are optimal for discrete channels with state information at the transmitter.

In this section, we focus on two problems: 1) The point to point channel coding with state information at the encoder (the Gelfand-Pinsker problem [31]) and 2) Lossy source coding with side information at the decoder (the Winer-Ziv problem [74] [73]). We consider these two problems in their most general settings i.e. when the source and the channel are arbitrary. We use nested lattice codes with *joint typicality decoding* rather than lattice decoding. We show that in both settings, from an information-theoretic point of view, nested lattice codes are optimal.

### 5.1.1 Preliminaries

#### 5.1.1.1 Channel Model

We consider continuous alphabet memoryless channels with knowledge of channel state information at the transmitter used without feedback. We associate two sets $\mathscr{X}$ and $\mathscr{Y}$ with the channel as the channel input and output alphabets. The set of channel states is denoted by $\mathscr{S}$ and it is assumed that the channel state is distributed over $\mathscr{S}$ according to $P_S$. When the state of the channel $S$ is $s \in \mathscr{S}$, the input-output relation of the channel is characterized by a transition kernel $W_{Y|XS}(y|x,s)$ for $x \in \mathscr{X}$ and $y \in \mathscr{Y}$. We assume that the state of the channel is known at the transmitter non-causally. The channel is specified by $(\mathscr{X}, \mathscr{Y}, \mathscr{S}, P_S, W_{Y|XS}, w)$ where $w : \mathscr{X} \times \mathscr{S} \to \mathbb{R}^+$ is the cost function.

#### 5.1.1.2 Source Model

The source is modeled as a discrete-time random process $X$ with each sample taking values in a fixed set $\mathscr{X}$ called alphabet. Assume $X$ is distributed jointly with a random variable $S$ according to the measure $P_{XS}$ over $\mathscr{X} \times \mathscr{S}$ where $\mathscr{S}$ is an arbitrary set. We assume that the side information $S$ is known to the receiver non-causally. The reconstruction alphabet is denoted by $\mathscr{U}$ and the quality of reconstruction is measured by the average of a single-letter distortion functions $d : \mathscr{X} \times \mathscr{U} \to \mathbb{R}^+$. We denote such sources by $(\mathscr{X}, \mathscr{S}, \mathscr{U}, P_{XS}, d)$.

#### 5.1.1.3 Linear and Coset Codes Over $\mathbb{Z}_p$

For a prime number $p$, a linear code over $\mathbb{Z}_p$ of length $n$ and rate $R = \frac{k}{n} \log p$ is a collection of $p^k$ codewords of length $n$ which is closed under mod-$p$ addition (and hence mod-$p$ multiplication). In other words, linear codes over $\mathbb{Z}_p$ are subspaces of $\mathbb{Z}_p^n$. Any such code can be characterized by its generator matrix $G \in \mathbb{Z}_p^{k \times n}$. This follow from the fact that any subgroup of an Abelian group corresponds to the image of a homomorphism into that group. The linear encoder maps a message tuple $u \in \mathbb{Z}_p^k$ to the codeword $x$ where $x = uG$ and the operations are done mod-$p$. The set of all message tuples for this code is $\mathbb{Z}_p^k$ and the set of all codewords is the range of the matrix $G$. i.e.

$$\mathbb{C} = \left\{ uG | u \in \mathbb{Z}_p^k \right\} \tag{5.1}$$

A coset code over $\mathbb{Z}_p$ is a shift of a linear code by a fixed vector. A coset code of length $n$ and rate $R = \frac{k}{n} \log p$ is characterized by its generator matrix $G \in \mathbb{Z}_p^{k \times n}$ and it's shift vector (dither) $B \in \mathbb{Z}_p^n$. The encoding rule for the corresponding coset code is given by $x = uG + B$, where $u$ is the message tuple and $x$ is the corresponding

codeword. i.e.

$$\mathbb{C} = \left\{uG + B | u \in \mathbb{Z}_p^k\right\} \tag{5.2}$$

In a similar manner, any linear code over $\mathbb{Z}_p$ of length $n$ and rate (at least) $R = \frac{n-k}{n} \log p$ is characterized by its parity check matrix $H \in \mathbb{Z}_p^{k \times n}$. This follows from the fact that any subgroup of an Abelian group corresponds to the kernel of a homomorphism from that group. The set of all codewords of the code is the kernel of the matrix $H$; i.e.

$$\mathbb{C} = \left\{u \in \mathbb{Z}_p^n | Hu = 0\right\} \tag{5.3}$$

where the operations are done mod-$p$. Note that there are at least $p^{n-k}$ codewords in this set. A coset code over $\mathbb{Z}_p$ is a shift of a linear code by a fixed vector. A coset code of length $n$ and rate (at least) $R = \frac{n-k}{n} \log p$ can be characterized by its parity check matrix $H \in \mathbb{Z}_p^{k \times n}$ and it's bias vector $c \in \mathbb{Z}_p^k$ as follows:

$$\mathbb{C} = \left\{u \in \mathbb{Z}_p^n | Hu = c\right\} \tag{5.4}$$

where the operations are done mod-$p$.

#### 5.1.1.4 Lattice Codes and Shifted Lattice Codes

A lattice code of length $n$ is a collection of codewords in $\mathbb{R}^n$ which is closed under real addition. A shifted lattice code is any translation of a lattice code by a real vector. In this paper, we use coset codes to construct (shifted) lattice codes as follows: Given a coset code $\mathbb{C}$ of length $n$ over $\mathbb{Z}_p$ and a *step size* $\gamma$, define

$$\Lambda(\mathbb{C}, \gamma, p) = \gamma(\mathbb{C} - \frac{p-1}{2}\mathbf{1}) \tag{5.5}$$

where $\mathbf{1} = (1, \cdots, 1) \in \mathbb{Z}_p^n$. The corresponding mod-$p$ lattice code $\bar{\Lambda}(\mathbb{C}, \gamma, p)$ is the disjoint union of shifts of $\Lambda$ by vectors in $\gamma p \mathbb{Z}^n$. i.e.

$$\bar{\Lambda}(\mathbb{C}, \gamma, p) = \bigcup_{v \in p\mathbb{Z}^n} (\gamma v + \Lambda)$$

It can be shown that this definition is equivalent to:

$$\bar{\Lambda}(\mathbb{C},\gamma,p)=\left\{\gamma(v-\frac{p-1}{2})\,|v\in\mathbb{Z}^n, v \mod p\in\mathbb{C}\right\}$$

Note that $\Lambda(\mathbb{C},\gamma,p)\subseteq\bar{\Lambda}(\mathbb{C},\gamma,p)$ is a scaled and shifted copy of the linear code $\mathbb{C}$.

#### 5.1.1.5 Nested Linear Codes

A nested linear code consists of two linear codes, with the property than one of the codes (the *inner linear code*) is a subset of the other code (the *outer linear code*). For positive integers $k$ and $l$, let the outer and inner codes $\mathbb{C}_i$ and $\mathbb{C}_o$ be linear codes over $\mathbb{Z}_p$ characterized by their generator matrices $G\in\mathbb{Z}_p^{l\times n}$ and $G'\in\mathbb{Z}_p^{(k+l)\times n}$ and their shift vectors $B\in\mathbb{Z}_p^n$ and $B'\in\mathbb{Z}_p^n$ respectively. Furthermore, assume

$$G'=\begin{bmatrix}G\\ \Delta G\end{bmatrix},\quad B'=B$$

For some $\Delta G\in\mathbb{Z}_p^{k\times n}$. In this case,

$$\mathbb{C}_o=\left\{aG+m\Delta G+B|a\in\mathbb{Z}_p^l, m\in\mathbb{Z}_p^k\right\}, \tag{5.6}$$

$$\mathbb{C}_i=\left\{aG+B|a\in\mathbb{Z}_p^l\right\} \tag{5.7}$$

It is clear that the inner code is contained in the outer code. Furthermore, the inner code induces a partition of the outer code through its shifts. For $m\in\mathbb{Z}_p^k$ define the $m$th *bin* of $\mathbb{C}_i$ in $\mathbb{C}_o$ as

$$\mathbb{B}_m=\left\{aG+m\Delta G+B|a\in\mathbb{Z}_p^l\right\}$$

Similarly, Nested linear codes can be characterized by the parity check representation of linear codes. For positive integers $k$ and $l$, let the outer and inner codes $\mathbb{C}_o$ and $\mathbb{C}_i$ be linear codes over $\mathbb{Z}_p$ characterized by their parity check matrices $H\in\mathbb{Z}_p^{l\times n}$ and

$H' \in \mathbb{Z}_p^{(k+l)\times n}$ and their bias vectors $c \in \mathbb{Z}_p^l$ and $c' \in \mathbb{Z}_p^{k+l}$ respectively. Furthermore assume:

$$H' = \begin{bmatrix} H \\ \Delta H \end{bmatrix}, c' = \begin{bmatrix} c \\ \Delta c \end{bmatrix}$$

For some $\Delta H \in \mathbb{Z}_p^{k\times n}$ and $\Delta c \in \mathbb{Z}_p^k$. In this case,

$$\mathbb{C}_o = \left\{u \in \mathbb{Z}_p^n | Hu = c\right\}, \tag{5.8}$$

$$\mathbb{C}_i = \left\{u \in \mathbb{Z}_p^n | Hu = c, \Delta Hu = \Delta c\right\} \tag{5.9}$$

For $m \in \mathbb{Z}_p^k$ define the $m$th bin of $\mathbb{C}_i$ in $\mathbb{C}_o$ as

$$\mathbb{B}_m = \left\{u \in \mathbb{Z}_p^n | Hu = c, \Delta Hu = m\right\}$$

The outer code is the disjoint union of all the bins and each bin index $m \in \mathbb{Z}_p^k$ is considered as a message. We denote a nested linear code by a pair $(\mathbb{C}_i, \mathbb{C}_o)$.

#### 5.1.1.6 Nested Lattice Codes

Given a nested linear code $(\mathbb{C}_i, \mathbb{C}_o)$ over $\mathbb{Z}_p$ and a step size $\gamma$, define

$$\Lambda_i(\mathbb{C}_i, \gamma, p) = \gamma(\mathbb{C}_i - \frac{p-1}{2}), \tag{5.10}$$

$$\Lambda_o(\mathbb{C}_o, \gamma, p) = \gamma(\mathbb{C}_o - \frac{p-1}{2}) \tag{5.11}$$

Then the corresponding nested lattice code consists of an inner lattice code and an outer lattice code

$$\bar{\Lambda}_i(\mathbb{C}_i, \gamma, p) = \cup_{v\in p\mathbb{Z}^n}(\gamma v + \Lambda_i) \tag{5.12}$$

$$\bar{\Lambda}_o(\mathbb{C}_o, \gamma, p) = \cup_{v\in p\mathbb{Z}^n}(\gamma v + \Lambda_o) \tag{5.13}$$

In this case as well, the inner lattice code induces a partition of the outer lattice code. For $m \in \mathbb{Z}_p^k$, define

$$\mathfrak{B}_m = \gamma(\mathbb{B}_m - \frac{p-1}{2}) \tag{5.14}$$

where $\mathbb{B}_m$ is the $m$th bin of $\mathbb{C}_i$ in $\mathbb{C}_o$. The $m$th bin of the inner lattice code in the outer lattice code is defined by:

$$\bar{\mathfrak{B}}_m = \cup_{v \in p\mathbb{Z}^n} (\gamma v + \mathfrak{B}_m)$$

The set of messages consists of the set of all bins of $\bar{\Lambda}_i$ in $\bar{\Lambda}_o$. We denote a nested lattice code by a pair $(\bar{\Lambda}_i, \bar{\Lambda}_o)$.

#### 5.1.1.7 Achievability for Channel Coding and the Capacity-Cost Function

A transmission system with parameters $(n, M, \Gamma, \tau)$ for reliable communication over a given channel $(\mathscr{X}, \mathscr{Y}, \mathscr{S}, P_S, W_{Y|XS}, w)$ with cost function $w : \mathscr{X} \times \mathscr{S} \to \mathbb{R}^+$ consists of an encoding mapping and a decoding mapping

$$e : \mathscr{S}^n \times \{1, 2, \ldots, M\} \to \mathscr{X}^n$$

$$f : \mathscr{Y}^n \to \{1, 2, \ldots, M\}$$

such that for all $m = 1, 2, \ldots, M$, if $s = (s_1, \cdots, s_n)$ and $x = e(s, m) = (x_1, \cdots, x_n)$, then

$$\frac{1}{n} \sum_{i=1}^{n} w(x_i, s_i) < \Gamma$$

and

$$\mathbb{E}_{P_S} \left\{ \sum_{m=1}^{M} \frac{1}{M} Pr\left(f(Y^n) \neq m | X^n = e(S^n, m)\right) \right\} \leq \tau$$

Given a channel $(\mathscr{X}, \mathscr{Y}, \mathscr{S}, P_S, W_{Y|XS}, w)$, a pair of non negative numbers $(R, W)$ is said to be achievable if for all $\epsilon > 0$ and for all sufficiently large $n$, there exists a transmission system for reliable communication with parameters $(n, M, \Gamma, \tau)$ such that

$$\frac{1}{n} \log M \geq R - \epsilon, \qquad \Gamma \leq W + \epsilon, \qquad \tau \leq \epsilon$$

The optimal capacity cost function $C(W)$ is given by the supremum of $C$ such that $(C, W)$ is achievable.

#### 5.1.1.8 Achievability for Source Coding and the Rate-Distortion Function

A transmission system with parameters $(n, \Theta, \Delta, \tau)$ for compressing a given source $(\mathscr{X}, \mathscr{S}, \mathscr{U}, P_{XS}, d)$ consists of an encoding mapping and a decoding mapping

$$e : \mathscr{X}^n \to \{1, 2, \cdots, \Theta\},$$
$$g : \mathscr{S}^n \times \{1, 2, \cdots, \Theta\} \to \mathscr{U}^n$$

such that the following condition is met:

$$P\left(d(X^n, g(e(X^n))) > \Delta\right) \leq \tau$$

where $X^n$ is the random vector of length $n$ generated by the source. In this transmission system, $n$ denotes the block length, $\log \Theta$ denotes the number of channel uses, $\Delta$ denotes the distortion level and $\tau$ denotes the probability of exceeding the distortion level $\Delta$.

Given a source, a pair of non-negative real numbers $(R, D)$ is said to be achievable if there exists for every $\epsilon > 0$, and for all sufficiently large numbers $n$ a transmission system with parameters $(n, \Theta, \Delta, \tau)$ for compressing the source such that

$$\frac{1}{n} \log \Theta \leq R + \epsilon, \qquad \Delta \leq D + \epsilon, \qquad \tau \leq \epsilon$$

The optimal rate distortion function $R^*(D)$ of the source is given by the infimum of the rates $R$ such that $(R, D)$ is achievable.

#### 5.1.1.9 Typicality

We use the notion of weak* typicality with Prokhorov metric introduced in [47]. Let $M(\mathbb{R}^d)$ be the set of probability measures on $\mathbb{R}^d$. For a subset $A$ of $\mathbb{R}^d$ define its

$\epsilon$-neighborhood by

$$A^\epsilon = \{x \in \mathbb{R}^d | \exists y \in A \text{ such that } \|x - y\| < \epsilon\}$$

where $\|\cdot\|$ denotes the Euclidean norm in $\mathbb{R}^d$. The Prokhorov distance between two probability measures $P_1, P_2 \in M(\mathbb{R}^d)$ is defined as follows:

$$\begin{aligned}\pi_d(P_1, P_2) = &\inf\{\epsilon > 0 | P_1(A) < P_2(A^\epsilon) + \epsilon \text{ and} \\ &P_2(A) < P_1(A^\epsilon) + \epsilon \quad \forall \text{ Borel set } A \text{ in } \mathbb{R}^d\}\end{aligned}$$

Consider two random variables $X$ and $Y$ with joint distribution $P_{XY}(\cdot, \cdot)$ over $\mathscr{X} \times \mathscr{Y} \subseteq \mathbb{R}^2$. Let $n$ be an integer and $\epsilon$ be a positive real number. For the sequence pair $(x, y)$ belonging to $\mathscr{X}^n \times \mathscr{Y}^n$ where $x = (x_1, \cdots, x_n)$ and $y = (y_1, \cdots, y_n)$ define the empirical joint distribution by

$$\bar{P}_{xy}(A, B) = \frac{1}{n} \sum_{i=1}^{n} \mathbb{1}_{\{x_i \in A, y_i \in B\}}$$

for Borel sets $A$ and $B$. Let $\bar{P}_x$ and $\bar{P}_y$ be the corresponding marginal probability measures. It is said that the sequence $x$ is weakly* $\epsilon$-typical with respect to $P_X$ if

$$\pi_1(\bar{P}_x, P_X) < \epsilon$$

We denote the set of all weakly* $\epsilon$-typical sequences of length $n$ by $A_\epsilon^n(X)$. Similarly, $x$ and $y$ are said to be jointly weakly* $\epsilon$-typical with respect to $P_{XY}$ if

$$\pi_2(\bar{P}_{xy}, P_{XY}) < \epsilon$$

We denote the set of all weakly* $\epsilon$-typical sequence pairs of length $n$ by $A_\epsilon^n(XY)$. Given a sequence $x \in A_\epsilon^n$, the set of conditionally $\epsilon$-typical sequences $A_\epsilon^n(Y|x)$ is defined as

$$A_\epsilon^n(Y|x) = \{y \in \mathscr{Y}^n \,|(x, y) \in A_\epsilon^n(X, Y)\}$$

#### 5.1.1.10 Notation

In our notation, $O(\epsilon)$ is any function of $\epsilon$ such that $\lim_{\epsilon\to 0} O(\epsilon) = 0$ and for a set $G$, $|G|$ denotes the cardinality (size) of $G$.

### 5.1.2 Nested Lattice Codes for Channel Coding

We show the achievability of the rate $R = I(U;Y) - I(U;S)$ for the Gelfand-Pinsker channel using nested lattice code for $U$.

**Theorem V.1.** *For the channel $(\mathscr{X}, \mathscr{Y}, \mathscr{S}, P_S, W_{Y|XS}, w)$, let $w : \mathscr{X} \to \mathbb{R}^+$ be a continuous cost function. Let $\mathscr{U}$ be an arbitrary set and let $SUXY$ be distributed over $\mathscr{S} \times \mathscr{U} \times \mathscr{X} \times \mathscr{Y}$ according to $P_S P_{U|S} W_{X|US} W_{Y|SX}$ where the conditional distribution $P_{U|S}$ and the transition kernel $W_{X|US}$ are such that $\mathbb{E}\{w(X)\} \leq W$. Then the pair $(R, W)$ is achievable using nested lattice codes over $U$ where $R = I(U;Y) - I(U;S)$.*

#### 5.1.2.1 Discrete $U$ and Bounded Continuous Cost Function

In this section we prove the theorem for the case when $U = \hat{U}$ takes values from the discrete set $\gamma(\mathbb{Z}_p - \frac{p-1}{2})$ where $p$ is a prime and $\gamma$ is a positive number. We use a random coding argument over the ensemble of mod-$p$ lattice codes to prove the achievability. Let $\mathbb{C}_o$ and $\mathbb{C}_i$ be defined as (5.6) and (5.7) where $G$ is a random matrix in $\mathbb{Z}_p^{l\times n}$, $\Delta G$ is a random matrix in $\mathbb{Z}_p^{k\times n}$ and $B$ is a random vector in $\mathbb{Z}_p^n$. Define $\bar{\Lambda}_i(\mathbb{C}_i, \gamma, p)$ and $\bar{\Lambda}_o(\mathbb{C}_o, \gamma, p)$ accordingly. The ensemble of nested lattice codes consists of all lattices of the form (5.10) and (5.11). The set of messages consists of all bins $\mathfrak{B}_m$ indexed by $m \in \mathbb{Z}_p^k$.

The encoder observes the massage $m \in \mathbb{Z}_p^k$ and the channel state $s \in \mathscr{S}^n$ and looks for a vector $u$ in the $m$th bin $\mathfrak{B}_m$ which is jointly weakly* typical with $s$ and encodes the massage $m$ to $x$ according to $W_{X|SU}$. The encoder declares error if it does not find such a vector.

After receiving $y \in \mathscr{Y}^n$, the decoder decodes it to $m \in \mathbb{Z}_p^k$ if $m$ is the unique tuple such that the $m$th bin $\mathfrak{B}_m$ contains a sequence jointly typical with $y$. Otherwise it declares error.

**Encoding Error**

We begin with some definitions and lemmas. Let

$$S' = [\frac{-\gamma p}{2}, \frac{\gamma p}{2}]^n \cap \gamma \mathbb{Z}^n \tag{5.15}$$

For $a \in \mathbb{Z}_p^k$, $m \in \mathbb{Z}_p^l$, define

$$g(a, m) = \gamma \left( (aG + m\Delta G + B) - \frac{(p-1)}{2} \right)$$

$g(a, m)$ has the following properties:

**Lemma V.2.** *For $a \in \mathbb{Z}_p^l$ and $m \in \mathbb{Z}_p^k$, $g(a, m)$ is uniformly distributed over $S'$. i.e. For $u \in S'$,*

$$P(g(a, m) = u) = \frac{1}{p^n}$$

*Proof.* Note that $B$ is independent of $G$ and $\Delta G$ and therefore $aG + m\Delta G + B$ is a uniform variable over $\mathbb{Z}_p^n$. The lemma follows by noting that

$$S' = \gamma \left( \mathbb{Z}_p^n - \frac{(p-1)}{2} \right)$$

□

**Lemma V.3.** *For $a, \tilde{a} \in \mathbb{Z}_p^l$ and $m \in \mathbb{Z}_p^k$ if $a \neq \tilde{a}$ then $g(a, m)$ and $g(\tilde{a}, m)$ are independent. i.e. For $u \in S'$ and $\tilde{u} \in S'$,*

$$P(g(a, m) = u, g(\tilde{a}, m) = \tilde{u}) = \frac{1}{p^{2n}}$$

*Proof.* It suffices to show that $aG + m\Delta G + B$ and $\tilde{a}G + m\Delta G + B$ are uniform over $\mathbb{Z}_p^n$ and independent. Note that for $u, \tilde{u} \in \mathbb{Z}_p^n$,

$$\begin{aligned} & P\left(aG + m\Delta G + B = u, \tilde{a}G + m\Delta G + B = \tilde{u}\right) \\ & \quad = P\left(aG + m\Delta G + B = u, (\tilde{a} - a)G = \tilde{u} - u\right) \\ & \quad \overset{(a)}{=} P\left(aG + m\Delta G + B = u\right) \times P\left((\tilde{a} - a)G = \tilde{u} - u\right) \\ & \quad \overset{(b)}{=} \frac{1}{p^{2n}} \end{aligned}$$

where $(a)$ follows since the $B$ is uniform over $\mathbb{Z}_p^n$ and independent of $G$ and $(b)$ follows since $B$ and $G$ are uniform and $\tilde{a} - a \neq 0$ □

**Lemma V.4.** *For $a, \tilde{a} \in \mathbb{Z}_p^l$ and $m, \tilde{m} \in \mathbb{Z}_p^k$ if $m \neq \tilde{m}$ then $g(a, m)$ and $g(\tilde{a}, \tilde{m})$ are independent. i.e. For $u \in S'$ and $\tilde{u} \in S'$,*

$$P(g(a, m) = u, g(\tilde{a}, \tilde{m}) = \tilde{u}) = \frac{1}{p^{2n}}$$

*Proof.* The proof is similar to the proof of the previous lemma and is omitted. □

For a message $m \in \mathbb{Z}_p^k$ and state $s \in \mathscr{S}^n$, the encoder declares error if there is no sequence in $\mathfrak{B}_m$ jointly typical with $s$. Define

$$\theta(s) = \sum_{u \in \mathfrak{B}_m} \mathbb{1}_{\{u \in A_\epsilon^n(\hat{U}|s)\}} = \sum_{a \in \mathbb{Z}_p^l} \mathbb{1}_{\{g(a,m) \in A_\epsilon^n(\hat{U}|s)\}}$$

Let $Z$ be a uniform random variable over $\gamma\left(\mathbb{Z}_p - \frac{(p-1)}{2}\right)$ and hence $Z^n$ a uniform random variable over $S'$. Then we have

$$\mathbb{E}\{\theta(s)\} = \sum_{a \in \mathbb{Z}_p^l} P\Big(Z^n \in A_\epsilon^n(\hat{U}|s)\Big)$$

we need the following lemmas from to proceed:

**Lemma V.5.** *Let $P_{XY}$ be a joint distribution on $\mathbb{R}^2$ and $P_X$ and $P_Y$ denote its marginals. Let $Z^n$ be a random sequence drawn according to $P_Z^n$. If $D(P_{XY} \| P_Z P_Y)$ is finite then for each $\delta > 0$, there exist $\epsilon(\delta)$ such that if $\epsilon < \epsilon(\delta)$ and $y \in A_\epsilon^n(P_Y)$ then*

$$\limsup \frac{1}{n} \log P_Z^n((Z^n, y) \in A_\epsilon^n(P_{XY}) \leq -D(P_{XY} \| P_Z P_Y) + \delta$$

*Proof.* This lemma is a generalization of Theorem 21 of [47]. The proof is provided in the Appendix. □

**Lemma V.6.** *Let $P_{XY}$ be a joint distribution on $\mathbb{R}^2$ and $P_X$ and $P_Y$ denote its marginals. Let $Z^n$ be a random sequence drawn according to $P_Z^n$. Then for each $\epsilon, \delta > 0$, there exist $\bar{\epsilon}(\epsilon, \delta)$ such that if $y \in A_{\bar{\epsilon}}^n(P_Y)$ then*

$$\liminf \frac{1}{n} \log P_Z^n((Z^n, y) \in A_\epsilon^n(P_{XY}) \geq -D(P_{XY} \| P_Z P_Y) - \delta$$

*Proof.* This lemma is a generalization of Theorem 22 of [47]. The proof is provided in the Appendix. □

Using these lemmas we get

$$\mathbb{E}\{\theta(s)\} = p^l 2^{-n[D(P_{\hat{U}S} \| P_Z P_S) + O(\epsilon)]}$$

Similarly, let $Z^n = g(a, m)$ and $\tilde{Z}^n = g(\tilde{a}, m)$. Note that $Z^n$ and $\tilde{Z}^n$ are equal if $a = \tilde{a}$ and are independent if $a \neq \tilde{a}$. We have

$$\begin{aligned}
\mathbb{E}\{\theta(s)^2\} &= \sum_{a, \tilde{a} \in \mathbb{Z}_p^l} P\Big(Z^n, \tilde{Z}^n \in A_\epsilon^n(\hat{U}|s)\Big) \\
&= \sum_{a \in \mathbb{Z}_p^l} P\Big(Z^n \in A_\epsilon^n(\hat{U}|s)\Big) \\
&\qquad + \sum_{\substack{a, \tilde{a} \in \mathbb{Z}_p^l \\ a \neq \tilde{a}}} P\Big(Z^n \in A_\epsilon^n(\hat{U}|s)\Big)^2 \\
&= p^l 2^{-n[D(P_{\hat{U}S} \| P_Z P_S) + O(\epsilon)]} \\
&\qquad + p^l (p^l - 1) 2^{-2n[D(P_{\hat{U}S} \| P_Z P_S) + O(\epsilon)]}
\end{aligned}$$

Therefore

$$\begin{aligned}
\mathrm{var}\{\theta(s)\} &= \mathbb{E}\{\theta(s)^2\} - \mathbb{E}\{\theta(s)\}^2 \\
&\leq p^l 2^{-n[D(P_{\hat{U}S} \| P_Z P_S) + O(\epsilon)]}
\end{aligned}$$

Hence,

$$\begin{aligned} P(\theta(s)=0) &\leq P\left(|\theta(s)-\mathbb{E}\{\theta(s)\}| \geq \mathbb{E}\{\theta(s)\}\right) \\ &\overset{(a)}{\leq} \frac{\mathrm{var}\{\theta(s)\}}{\mathbb{E}\{\theta(s)\}^2} \\ &\leq p^l 2^{-n[D(P_{\hat{U}S}\|P_Z P_S]+O(\epsilon)]} \end{aligned}$$

Where $(a)$ follows from Chebyshev's inequality. This bound is valid for all $s \in \mathbb{S}^n$. Therefore if

$$\frac{l}{n}\log p > D(P_{\hat{U}S}\|P_Z P_S) \tag{5.16}$$

then the probability of encoding error goes to zero as the block length increases.

**Decoding Error**

The decoder declares error if there is no bin $\mathfrak{B}_m$ containing a sequence jointly typical with $y$ where $y$ is the received channel output or if there are multiple bins containing sequences jointly typical with $y$. Assume that the message $m$ has been encoded to $x$ according to $W_{X|SU}$ where $u = g(a,m)$ and the channel state is $s$. The channel output $y$ is jointly typical with $u$ with high probability. Given $m, s, a$ and $u$, the probability of decoding error is upper bounded by

$$\begin{aligned} P_{err} &\leq \sum_{\substack{\tilde{m}\in\mathbb{Z}_p^k \\ \tilde{m}\neq m}} \sum_{\tilde{a}\in\mathbb{Z}_p^l} P\left(g(\tilde{a},\tilde{m}) \in A_\epsilon^n(\hat{U}|y) | g(a,m) \in A_\epsilon^n(\hat{U}|y)\right) \\ &\overset{(a)}{=} p^l p^k 2^{-n[D(P_{\hat{U}Y}\|P_Z P_Y)+O(\epsilon)]} \end{aligned}$$

Where in $(a)$ we use Lemmas V.4, V.5 and V.6. Hence the probability of decoding error goes to zero if

$$\frac{k+l}{n}\log p < D(P_{\hat{U}Y}\|P_Z P_Y) \tag{5.17}$$

**The Achievable Rate**

Using (5.16) and (5.17), we conclude that if we choose $\frac{l}{n}\log p$ sufficiently close to $D(P_{\hat{U}S}\|P_ZP_S)$ and $\frac{k+l}{n}\log p$ sufficiently close to $D(P_{\hat{U}S}\|P_ZP_S)$ we can achieve the rate

$$\begin{aligned} R = \frac{k}{n}\log p &\approx D(P_{\hat{U}Y}\|P_ZP_Y) - D(P_{\hat{U}S}\|P_ZP_S) \\ &= I(\hat{U};Y) - I(\hat{U};S) \end{aligned}$$

#### 5.1.2.2 Arbitrary $U$ and Bounded Continuous Cost Function

Let $Q = \{A_1, A_2, \cdots, A_r\}$ be a finite measurable partition of $\mathbb{R}^d$. For random variables $U$ and $Y$ on $\mathbb{R}^d$ with measure $P_{UY}$ define the quantized random variables $U_Q$ and $Y_Q$ on $Q$ with measure

$$P_{U_QY_Q}(A_i, A_j) = P_{UY}(A_i, A_j)$$

The Kullback-Leibler divergence between $U$ and $Y$ is defined as

$$D(U\|Y) = \sup_Q D(U_Q\|Y_Q)$$

where $D(U_Q\|Y_Q)$ is the discrete Kullback-Leibler divergence and the supremum is taken over all finite partitions $Q$ of $\mathbb{R}^d$. Similarly, the mutual information between $U$ and $Y$ is defined as

$$I(U;Y) = \sup_Q I(U_Q;Y_Q)$$

where $I(U_Q;Y_Q)$ is the discrete mutual information between the two random variables and the supremum is taken over all finite partitions $Q$ of $\mathbb{R}^d$.

We have shown in Section 5.1.2.1 that for discrete random variables the region given in Theorem V.1 is achievable. In this part, we make a quantization argument to generalize this result to arbitrary auxiliary random variables. Let $S, U, X, Y$ be distributed according to $P_SP_{U|S}W_{X|US}W_{Y|X}$ where in this case $U$ is an arbitrary random variable. We start with the following theorem:

**Theorem V.7.** *Let $\mathscr{F}_1 \subseteq \mathscr{F}_2 \subseteq \cdots$ be an increasing sequence of $\sigma$-algebras on a measurable set $A$. Let $\mathscr{F}_\infty$ denote the $\sigma$-algebra generated by the union $\cup_{n=1}^{\infty}\mathscr{F}_n$. Let $P$ and $Q$ be probability measures on $A$. Then*

$$D(P|_{\mathscr{F}_n}\|Q|_{\mathscr{F}_n}) \to D(P|_{\mathscr{F}_\infty}\|Q|_{\mathscr{F}_\infty}) \text{ as } n \to \infty$$

*where $P|_{\mathscr{F}}$ denotes the restriction of $P$ on $\mathscr{F}$.*

*Proof.* Provided in [33] and [14] for example. □

For a prime $p > 2$, a real positive number $\gamma$ and for $i = 0 \cdots, p-1$ define

$$a_i = \frac{-\gamma(p-1)}{2} + \gamma i$$

Define the quantization $Q_{\gamma,p}$ as $Q_{\gamma,p} = \{A_0, A_2, \cdots, A_{p-1}\}$ where

$$A_0 = (-\infty, a_0]$$
$$A_i = (a_{i-1}, a_i], \text{ for } i = 1, \cdots, p-2$$
$$A_{p-1} = (a_{p-2}, +\infty)$$

Let the random variable $\hat{U}_{\gamma,p}$ take values from $\{a_0, \cdots, a_{p-1}\}$ according to joint measure

$$P_{S\hat{U}XY}(\hat{U} = a_i, SXY \in B) = P_{SUXY}(U \in A_i, SXY \in B) \tag{5.18}$$

For all Borel sets $B \subseteq \mathbb{R}^3$. For a fixed $\gamma$, let $p \leq q$ be two primes. Then the $\sigma$-algebra induced by $Q_{\gamma,p}$ is included in the $\sigma$-algebra induced by $Q_{\gamma,q}$. Therefore, for a fixed $\gamma$, we can use the above theorem to get

$$I(U|_{\mathscr{F}_{\gamma,p}}; Y|_{\mathscr{F}_{\gamma,p}}) \to I(U|_{\mathscr{F}_{\gamma,\infty}}; Y|_{\mathscr{F}_{\gamma,\infty}}) \text{ as } p \to \infty \tag{5.19}$$

where $U|_{\mathscr{F}_{\gamma,\infty}}$ is a random variable over $Q_{\gamma,\infty} = \{A_i | i \in \mathbb{Z}\}$ where $A_i = \frac{\gamma}{2} + (\gamma i, \gamma(i+1)]$ with measure $P_{U|_{\mathscr{F}_{\gamma,\infty}}}(A_i) = P_U(A_i)$.

Let $\gamma_0 = 1$ and define $\gamma_n = \frac{1}{2^n}$. Note that if $m > n$ then $\mathscr{F}_{\gamma_n,\infty}$ is included in $\mathscr{F}_{\gamma_m,\infty}$.

Also, since dyadic intervals generate the Borel Sigma field ( [49] for example), the restriction of $U$ to the sigma algebra generated by $\cup_{n=1}^{\infty}\mathscr{F}_{\gamma_n,\infty}$ is $U$ itself. We can use Theorem V.7 to get

$$I(U|_{\mathscr{F}_{\gamma_n,\infty}};Y|_{\mathscr{F}_{\gamma_n,\infty}}) \to I(U;Y) \text{ as } n \to \infty \tag{5.20}$$

Combining (5.19) and (5.20) we conclude that for all $\epsilon > 0$, there exist $\Gamma$ and $P$ such that if $\gamma \leq \Gamma$ and $p \geq \Gamma$ then

$$\left|I(U|_{\mathscr{F}_{\gamma,p}};Y|_{\mathscr{F}_{\gamma,p}}) - I(U;Y)\right| < \epsilon$$

Since quantization reduces the mutual information ($X_Q \to X \to Y$), we have

$$I(U|_{\mathscr{F}_{\gamma,p}};Y|_{\mathscr{F}_{\gamma,p}}) \leq I(U|_{\mathscr{F}_{\gamma,p}};Y) \leq I(U;Y)$$

Therefore $\left|I(U|_{\mathscr{F}_{\gamma,p}};Y) - I(U;Y)\right| < \epsilon$. Also note that $I(U|_{\mathscr{F}_{\gamma,p}};Y) = I(\hat{U}_{\gamma,p};Y)$ since we define the joint measure to be the same. Therefore

$$\left|I(\hat{U}_{\gamma,p};Y) - I(U;Y)\right| \leq \epsilon \tag{5.21}$$

With a similar argument, for all $\epsilon > 0$ there exist $\gamma$ and $p$ such that

$$\left|I(\hat{U}_{\gamma,p};S) - I(U;S)\right| \leq \epsilon \tag{5.22}$$

if we take the maximum of the two $p$'s and the minimum of the two $\gamma$'s, we can say for all $\epsilon > 0$ there exist $\gamma$ and $p$ such that both (5.21) and (5.22) happen.
consider the sequence $P_{S\hat{U}_{\gamma_n,p}X}$ as $n, p \to \infty$. In the next lemma we show that under certain conditions this sequence converges in the weak* sense to $P_{SUX}$.

**Lemma V.8.** *Consider the sequence $P_{S\hat{U}_{\gamma_n,p}X}$ where $n \to \infty$ and $p$ is such that $\gamma_n p \to \infty$ as $n \to \infty$ (Take $p$ to be the smallest prime larger than $2^{2n}$ for example.). Then the sequence converges to $P_{SUX}$ in the weak* sense as $n \to \infty$.*

*Proof.* It suffices to show that the three dimensional cumulative distribution function $F_{S\hat{U}_{\gamma_n,p}X}$ converges to $F_{SUX}$ point-wise in all points $(s,u,x) \in \mathbb{R}^3$ where $F$ is continuous. Let $(s,u,x)$ be a point where $F$ is continuous and for an arbitrary $\epsilon > 0$, let $\delta$ be such that

$$|F_{SUX}(s,u-\delta,x) - F_{SUX}(s,u,x)| < \epsilon$$
$$|F_{SUX}(s,u+\delta,x) - F_{SUX}(s,u,x)| < \epsilon$$

Let $p$ be such that $\gamma_n = \frac{1}{2^n} < \delta$ and find $p$ accordingly. Then there exist points $a_i, a_j$ such that $a_i \in [u-\delta, u]$ and $a_j \in [u, u+\delta]$. We have

$$\begin{aligned} F_{SUX}(s,u-\delta,x) &\leq F_{S\hat{U}_{\gamma_n,p}X}(s,a_i,x) \\ &\leq F_{S\hat{U}_{\gamma_n,p}X}(s,u,x) \\ &\leq F_{S\hat{U}_{\gamma_n,p}X}(s,a_j,x) \\ &\leq F_{SUX}(s,u+\delta,x) \end{aligned}$$

Therefore $\left|F_{S\hat{U}_{\gamma_n,p}X}(s,u,x) - F_{SUX}(s,u,x)\right| \leq \epsilon$. This shows the point-wise convergence of $F_{S\hat{U}_{\gamma_n,p}X}$. □

The above lemma implies $\mathbb{E}_{P_{S\hat{U}_{\gamma_n,p}X}}\{w(X,S)\}$ converges to $\mathbb{E}_{P_{SUX}}\{w(X,S)\} \leq W$ since $w$ is assumed to be bounded continuous.

We have shown that for arbitrary $P_{U|S}$ and $W_{X|SU}$, one can find $P_{\hat{U}|S}$ and $W_{X|S\hat{U}}$ induced from (5.18) such that $\hat{U}$ is a discrete variable and

$$I(\hat{U};Y) - I(\hat{U};S) \approx I(U;Y) - I(U;S)$$
$$\mathbb{E}_{P_{S\hat{U}X}}\{w(X,S)\} \approx \mathbb{E}_{P_{SUX}}\{w(X,S)\}$$

Hence, using the result of section 5.1.2.1, we have shown the achievability of the rate region given in Theorem V.1 for arbitrary auxiliary random variables when the cost function is bounded and continuous.

#### 5.1.2.3 Arbitrary $U$ and Continuous Cost Function

For a positive number $l$, define the clipped random variable $\hat{X}$ by $\hat{X} = \text{sign}(X)\min(l, |X|)$ and let $\hat{Y}$ be distributed according to $W_{\hat{Y}|\hat{X}}(\cdot, \hat{x}) = W_{Y|X}(\cdot, \hat{x})$.

**Lemma V.9.** *As $l \to \infty$, $I(U;\hat{Y}) \to I(U;Y)$.*

*Proof.* Note that for Borel sets $B_1, B_2, B_3$ if $B_2 \subseteq (-l, l)$ then

$$P_{U\hat{X}\hat{Y}}(B_1, B_2, B_3) = P_{UXY}(B_1, B_2, B_3)$$

For any $\epsilon > 0$, let $Q = \{A_1, \cdots, A_r\}$ be a quantization such that

$$|I(U_Q; Y_Q) - I(U;Y)| < \epsilon$$

For an arbitrary $\delta > 0$, assume $l$ is large enough such that $P_X((-l, l)) > 1 - \delta$. Then

$$\begin{aligned}
&P_{U_Q Y_Q}(A_i, A_j) = P_{UXY}(A_i, \mathbb{R}, A_j) \\
&= P_{UXY}(A_i, (-l, l), A_j) + P_{UXY}(A_i, (-\infty, -l] \cup [l, \infty), A_j) \\
&\leq P_{UXY}(A_i, (-l, l), A_j) + P_{UXY}(\mathbb{R}, (-\infty, -l] \cup [l, \infty), \mathbb{R}) \\
&= P_{U\hat{X}\hat{Y}}(A_i, (-l, l), A_j) + P_X((-\infty, -l] \cup [l, \infty)) \\
&\leq P_{U\hat{Y}}(A_i, A_j) + \delta \\
&= P_{U_Q \hat{Y}_Q}(A_i, A_j) + \delta
\end{aligned}$$

Also,

$$\begin{aligned}
P_{U_Q Y_Q}(A_i, A_j) &= P_{UXY}(A_i, \mathbb{R}, A_j) \\
&\geq P_{UXY}(A_i, (-l, l), A_j) \\
&= P_{U\hat{X}\hat{Y}}(A_i, (-l, l), A_j) \\
&\geq P_{U\hat{X}\hat{Y}}(A_i, \mathbb{R}, A_j) - \delta \\
&= P_{U\hat{Y}}(A_i, A_j) - \delta \\
&= P_{U_Q \hat{Y}_Q}(A_i, A_j) - \delta
\end{aligned}$$

Since the choice of $\delta$ is arbitrary and since the discrete mutual information is continuous, we conclude that as $\epsilon, \delta \to 0$ (hence $l \to \infty$), $I(U;\hat{Y}) \to I(U;Y)$. $\square$

Since $\hat{X}$ is bounded and $w$ is assumed to be continuous, $w$ is also bounded. This completes the proof.

### 5.1.3 Nested Lattice Codes for Source Coding

In this section, we show the achievability of the rate $R = I(U;X) - I(U;S)$ for the Wyner-Ziv problem using nested lattice codes for $U$.

**Theorem V.10.** *For the source $(\mathscr{X}, \mathscr{S}, \mathscr{U}, P_{XS}, d)$ assume $d : \mathscr{X} \times \mathscr{U} \to \mathbb{R}^+$ is continuous. Let $U$ be a random variable taking values from the set $\mathscr{U}$ jointly distributed with $X$ and $S$ according to $P_{XS}W_{U|X}$ where $W_{U|X}(\cdot|\cdot)$ is a transition kernel. Further assume that there exists a measurable function $f : \mathscr{S} \times \mathscr{U} \to \hat{\mathscr{X}}$ such that $\mathbb{E}\{d(X, f(S,U))\} \leq D$. Then the rate $R^*(D) = I(X;U) - I(S;U)$ is achievable using nested lattice codes.*

#### 5.1.3.1 Discrete $U$ and Bounded Continuous Distortion Function

In this section we prove the theorem for the case when $U$ takes values from the discrete set $\gamma(\mathbb{Z}_p - \frac{p-1}{2})$ where $p$ is a prime and $\gamma$ is a positive number. The generalization to the case where $U$ is arbitrary and the distortion function is continuous is similar to the channel coding problem and is omitted. We use a random coding argument over the ensemble of mod-$p$ lattice codes to prove the achievability. The ensemble of codes used for source coding is based on the parity check matrix representation of linear and lattice codes. Define the inner and outer linear codes as in (5.8) and (5.9) where $H$ is a random matrix in $\mathbb{Z}_p^{l\times n}$, $\Delta H$ is a random matrix in $\mathbb{Z}_p^{k\times n}$, $c$ is a random vector in $\mathbb{Z}_p^l$ and $\Delta c$ is a random vector in $\mathbb{Z}_p^k$. Define $\bar{\Lambda}_i(\mathbb{C}_i, \gamma, p)$ and $\bar{\Lambda}_o(\mathbb{C}_o, \gamma, p)$ accordingly. The set of messages consists of all bins $\mathfrak{B}_m$ indexed by $m \in \mathbb{Z}_p^k$.

For $m \in \mathbb{Z}_p^k$, Let $\mathfrak{B}_m$ be the $m$th bin of $\Lambda_i$ in $\Lambda_o$. The encoder observes the source sequence $x \in \mathscr{X}^n$ and looks for a vector $u$ in the outer code $\Lambda_o$ which is typical with $x$ and encodes the sequence $x$ to the bin of $\Lambda_i$ in $\Lambda_o$ containing $u$. The encoder declares error if it does not find such a vector.

Having observed the index of the bin $m$ and the side information $s$, the decoder looks for a unique sequence $u$ in the $m$th bin which is jointly typical with $s$ and outputs $f(u, s)$. Otherwise it declares error.

**Encoding Error**

Define $S'$ as in (5.15). For $u \in S'$ define

$$g(u) = \frac{1}{\gamma}u + \frac{p-1}{2}$$

$g(u)$ has the following properties:

**Lemma V.11.** *For $u \in S'$,*

$$P(u \in \Lambda_o) = P(Hg(u) = c) = \frac{1}{p^l}$$

*i.e. All points of $S'$ lie on the outer lattice equiprobably.*

*Proof.* Follows from the fact that $c$ is independent of $H$ and is uniformly distributed over $\mathbb{Z}_p^l$. □

**Lemma V.12.** *For $u \in S'$ and $\tilde{u} \in S'$, if $u \neq \tilde{u}$,*

$$P\left(u \in \Lambda_o, \tilde{u} \in \Lambda_o\right) = P\left(Hg(u) = c, Hg(\tilde{u}) = c\right) = \frac{1}{p^{2l}}$$

*i.e. All points of $S'$ lie on the outer lattice independently.*

*Proof.* Note that

$$\begin{aligned} & P\left(Hg(u)=c, Hg(\tilde{u})=c\right) \\ & \quad = P\left(Hg(u)=c, H(g(\tilde{u})-g(u))=0\right) \\ & \quad \overset{(a)}{=} P\left(Hg(u)=c\right) \times P\left(H(g(\tilde{u})-g(u))=0\right) \\ & \quad \overset{(b)}{=} \frac{1}{p^{2l}} \end{aligned}$$

Where $(a)$ follows since $c$ is uniform and independent of $H$ and $(b)$ follows since $H$ and $c$ are uniform and $g(\tilde{u})-g(u)$ is nonzero. □

For a source sequence $x \in \mathscr{X}^n$, the encoder declare error if there is no sequence $u \in \Lambda_o$ jointly typical with $x$. Define

$$\theta(x) = \sum_{u \in \Lambda_o} \mathbb{1}_{\{u \in A_\epsilon^n(\hat{U}|x)\}}$$

Let $Z$ be a uniform random variable over $\gamma(\mathbb{Z}_p - \frac{p-1}{2}))$ and $Z^n$ a uniform random variable over $S'$. We need the following lemmas to proceed:

**Lemma V.13.** *With the above construction $|\Lambda_o| = p^{n-l}$ with high probability. Specifically,*

$$\begin{aligned} P\left(rank(H)=l\right) &= \frac{(p^n-1)(p^n-p)(p^n-p^2)\cdots(p^n-p^{l-1})}{p^{nl}} \\ &\geq 1 - \frac{1}{p^{n-l}} \end{aligned}$$

*and hence the probability that $|\Lambda_o| = p^{n-l}$ is close to one if $n$ is large. Furthermore, for $i = 1, 2, \cdots, l$,*

$$P\left(rank(H)=i\right) \leq \binom{l}{i} \frac{p^{i(l-i)}}{p^{n(l-i)}}$$

*Proof.* The first part of the lemma follows since the total number of choices for $H$ is equal to $p^{nl}$ and the number of choices with independent rows is equal to $(p^n - 1)(p^n - p)(p^n - p^2)\cdots(p^n - p^{l-1})$. Now we show the upper bounds. For a matrix $H$ to

have a rank $i$, there should exist $i$ independent rows and the rest of the rows must be a linear combination of these rows (There are $p^i$ of such linear combinations). Hence the total number of such matrices is upper bounded by

$$\binom{l}{i}(p^n-1)(p^n-p)(p^n-p^2)\cdots(p^n-p^{i-1})(p^i)^{l-i}$$

The lemma follows if we upper bound this quantity by

$$\binom{l}{i}p^{ni}p^{i(l-i)}$$

□

**Lemma V.14.** *With $\theta(x)$ and $Z^n$ defined as above, we have*

$$\mathbb{E}\{\theta(x)\} \leq p^{n-l}P\left(Z^n \in A_\epsilon^n(\hat{U}|s)\right) + \frac{2^l}{p^{n(l-1)}}$$
$$\mathbb{E}\{\theta(x)\} \geq (1-\frac{1}{p^{n-l}})p^{n-l}P\left(Z^n \in A_\epsilon^n(\hat{U}|s)\right)$$

*Proof.* Write the random lattice $\Lambda_o$ as $\{u_1(\Lambda_o), u_2(\Lambda_o), \cdots, u_r(\Lambda_o)\}$ where $r$ is the cardinality of $\Lambda_o$ and $u_1(\Lambda_o), u_2(\Lambda_o), \cdots, u_r(\Lambda_o)$ are picked without replacement from $\Lambda_o$. It follow from Lemma V.11 that given $|\Lambda_o| = r = p^{n-l}$, $u_1(\Lambda_o), u_2(\Lambda_o), \cdots, u_r(\Lambda_o)$ are each uniformly distributed random variables over $S'$. To see this note that for arbitrary $u \in S'$, since $u_1(\Lambda_o), u_2(\Lambda_o), \cdots, u_r(\Lambda_o)$ are picked randomly from $\Lambda_o$,

$$P\left(u = u_1(\Lambda_o)\right) = P\left(u = u_2(\Lambda_o)\right) = \cdots = P\left(u = u_r(\Lambda_o)\right)$$

Therefore

$$\begin{aligned} P(u \in \Lambda_o) &= \sum_{i=1}^{r} P\left(u = u_i(\Lambda_o)\right) \\ &= rP\left(u = u_1(\Lambda_o)\right) = \frac{1}{p^l} \end{aligned}$$

Hence if $r = p^{n-l}$ then $u_1(\Lambda_o)$ is uniform over $S'$. This argument is valid for all $i = 1, \cdots, r$ and hence if $r = p^{n-l}$ then $u_i(\Lambda_o)$ is uniform over $S'$. Note that

$$\mathbb{E}\{\theta(x)\} = \mathbb{E}\{\mathbb{E}\{\theta(x)||\Lambda_o| = r\}\}$$

The conditional expectation on the right hand side of this equation is upper bounded by $p^{n-l}$ and for $r = p^{n-l}$ it is equal to

$$\begin{aligned}
\mathbb{E}\{\theta(x)||\Lambda_o| = p^{n-l}\} &= \mathbb{E}\{\sum_{u\in\Lambda_o} \mathbb{1}_{\{u\in A_\epsilon^n(\hat{U}|x)\}}\} \\
&= \mathbb{E}\{\sum_{i=1}^{p^{n-l}} \mathbb{1}_{\{u_i(\Lambda_o)\in A_\epsilon^n(\hat{U}|x)\}}\} \\
&= \sum_{i=1}^{p^{n-l}} P\left(u_i(\Lambda_o) \in A_\epsilon^n(\hat{U}|x)\right) \\
&\overset{(a)}{=} \sum_{i=1}^{p^{n-l}} P\left(Z^n \in A_\epsilon^n(\hat{U}|x)\right) \\
&= p^{n-l} P\left(Z^n \in A_\epsilon^n(\hat{U}|x)\right)
\end{aligned}$$

Where $(a)$ follows since $u_i(\Lambda_o)$ is uniformly distributed over $S'$ for all $i = 1, \cdots, r$. Next note that

$$\begin{aligned}
\mathbb{E}\{\theta(x)\} &= \sum_{r=0}^{p^n} P\left(|\Lambda_o| = r\right) \mathbb{E}\{\theta(x)||\Lambda_o| = r\} \\
&\leq P\left(|\Lambda_o| = p^{n-l}\right) rP\left(Z^n \in A_\epsilon^n(\hat{U}|x)\right) \\
&\quad + \sum_{i=0}^{l-1} P\left(|\Lambda_o| = p^{n-i}\right) p^{n-i} \\
&\leq p^{n-l} P\left(Z^n \in A_\epsilon^n(\hat{U}|s)\right) + \frac{2^l}{p^{n(l-1)}}
\end{aligned}$$

Similarly,

$$\begin{aligned}
\mathbb{E}\{\theta(x)\} &= \sum_{r=0}^{p^n} P\left(|\Lambda_o| = r\right) \mathbb{E}\{\theta(x)||\Lambda_o| = r\} \\
&\geq P\left(|\Lambda_o| = p^{n-l}\right) rP\left(Z^n \in A_\epsilon^n(\hat{U}|x)\right) \\
&\geq (1 - \frac{1}{p^{n-l}}) p^{n-l} P\left(Z^n \in A_\epsilon^n(\hat{U}|s)\right)
\end{aligned}$$

□

Therefore,

$$\mathbb{E}\{\theta(s)\} = p^{n-l} 2^{-n[D(P_{\hat{U}X}\|P_Z P_X) + O(\epsilon)]}$$

Similarly,

$$\begin{aligned}\theta(x)^2 &= \sum_{u,\tilde{u}\in\Lambda_o} \mathbb{1}_{\{u,\tilde{u}\in A_\epsilon^n(\hat{U}|x)\}} \\ &= \sum_{u\in\Lambda_o} \mathbb{1}_{\{u\in A_\epsilon^n(\hat{U}|x)\}} + \sum_{u\neq\tilde{u}\in\Lambda_o} \mathbb{1}_{\{u,\tilde{u}\in A_\epsilon^n(\hat{U}|x)\}} \\ &\leq \sum_{u\in\Lambda_o} \mathbb{1}_{\{u\in A_\epsilon^n(\hat{U}|x)\}} + \sum_{u,\tilde{u}\in\Lambda_o} \mathbb{1}_{\{u,\tilde{u}\in A_\epsilon^n(\hat{U}|x)\}}\end{aligned}$$

It can be shown that

$$\begin{aligned}\mathbb{E}\{\theta(x)^2\} &= \mathbb{E}\{|\Lambda_o|\}P\Big(Z^n \in A_\epsilon^n(\hat{U}|x)\Big) \\ &\quad + \mathbb{E}\{|\Lambda_o|\}^2 P\Big(Z^n \in A_\epsilon^n(\hat{U}|x)\Big)^2 \\ &\leq p^{n-l}2^{-n[D(P_{\hat{U}X}\|P_ZP_X)+O(\epsilon)]} \\ &\quad + p^{2(n-l)}2^{-2n[D(P_{\hat{U}X}\|P_ZP_X)+O(\epsilon)]}\end{aligned}$$

Hence

$$\mathrm{var}\{\theta(x)\} \leq p^k 2^{-n[D(P_{\hat{U}X}\|P_ZP_X)+O(\epsilon)]}$$

Hence,

$$P(\theta(s)=0) \leq \frac{\mathrm{var}\{\theta(x)\}}{\mathbb{E}\{\theta(x)\}^2} \leq p^{-(n-l)}2^{n[D(P_{\hat{U}X}\|P_ZP_X)+O(\epsilon)]}$$

Therefore if

$$\frac{l}{n}\log p < \log p - D(P_{\hat{U}X}\|P_ZP_X) \tag{5.23}$$

then the probability of encoding error goes to zero as the block length increases.

**Decoding Error**

After observing $m$ and the side information $s$, the decoder declares error if it does not find a sequence in the bin $\mathfrak{B}_m$ jointly typical with $s$ or if there are multiple of

such sequences. We will show that the probability that a sequence $\tilde{u} \neq u$ is in the same bin as $u$ and is jointly typical with $s$ goes to zero as the block length increases if $\frac{k+l}{n} \log p > \log p - D(P_{\hat{U}S} \| P_Z P_S)$. The probability of decoding error is upper bounded by

$$\begin{aligned} P_{err} &\leq \sum_{\tilde{u} \in \prime S^n} P\left(u \in \mathfrak{B}_m, u \in A_\epsilon^n(\hat{U}|s)\right) \\ &= \sum_{\tilde{u} \in \prime S^n} P\left(u \in \mathfrak{B}_m\right) P\left(Z^n \in A_\epsilon^n(\hat{U}|s)\right) \\ &= \frac{p^n}{p^{k+l}} 2^{-n[D(P_{\hat{U}S} \| P_Z P_S) + O(\epsilon)]} \end{aligned}$$

Hence the probability of decoding error goes to zero if

$$\frac{k+l}{n} \log p > \log p - D(P_{\hat{U}S} \| P_Z P_S) \tag{5.24}$$

**The Achievable Rate**

Using (5.24) and (5.24), we conclude that if we choose $\frac{l}{n} \log p$ sufficiently close to $\log p - D(P_{\hat{U}X} \| P_Z P_X)$ and $\frac{k+l}{n} \log p$ sufficiently close to $\log p - D(P_{\hat{U}S} \| P_Z P_S)$ we can achieve the rate

$$\begin{aligned} R &= \frac{k}{n} \log p \\ &\approx D(P_{\hat{U}X} \| P_Z P_X) - D(P_{\hat{U}S} \| P_Z P_S) \\ &= I(X; \hat{U}) - I(S; \hat{U}) \end{aligned}$$

### 5.1.4 Appendix

#### 5.1.4.1 Proof of Lemma V.5

The proof follows along the lines of the proof of Theorem 21 of [47]. Let $Q = \{A_1, A_2, \cdots, A_r\}$ be a finite partition of $\mathbb{R}$. Let $Q_{XYZ}$, $Q_{XY}$, $Q_{XZ}$, $Q_{YZ}$, $Q_X$, $Q_Y$ and $Q_Z$ be measures induced by this partition, corresponding to $P_{XYZ}$, $P_{XY}$, $P_{XZ}$, $P_{YZ}$, $P_X$, $P_Y$ and $P_Z$ respectively. For the random sequence $Z^n = (Z_1, \cdots, Z_n)$ and the

deterministic sequence $y = (y_1, \cdots, y_n)$ let $\bar{Q}_y$ be the deterministic empirical measure of $y$ and define the random empirical measures

$$\bar{Q}_{Zy}(A_i, A_j) = \frac{1}{n} \sum_{i=1}^{n} \mathbb{1}_{\{Z_i \in A_i, y_i \in A_j\}}$$
$$\bar{Q}_{Z}(A_i) = \frac{1}{n} \sum_{i=1}^{n} \mathbb{1}_{\{Z_i \in A_i\}}$$

for $i, j = 1, 2, \cdots, r$. As a property of weakly* typical sequences, for a fixed $\epsilon_1 > 0$, there exists a sufficiently small $\epsilon > 0$ such that for a sequence pair $(x, y) \in A_\epsilon^n(XY)$ and for all $i, j = 1, 2, \cdots, r$,

$$\left|\bar{Q}_{xy}(A_i, A_j) - Q_{XY}(A_i, A_j)\right| \leq \epsilon_1$$

where $\bar{Q}_{xy}$ is the joint empirical measure of $(x, y)$. It follows that the rare event $(Z^n, y) \in A_\epsilon^n(XY)$ is included in the intersection of events

$$\left\{\left|\bar{Q}_{Zy}(A_i, A_j) - Q_{XY}(A_i, A_j)\right| \leq \epsilon_1\right\} \tag{5.25}$$

for $i, j = 1, 2, \cdots, r$. Therefore

$$Q_Z^n\left((Z^n, y) \in A_\epsilon^n(XY)\right) \leq$$
$$Q_Z^n\left(\bigcap_{i,j=1}^{r} \left\{\left|\bar{Q}_{Zy}(A_i, A_j) - Q_{XY}(A_i, A_j)\right| \leq \epsilon_1\right\}\right)$$

Let $\epsilon(\delta)$ be such that for $j = 1, \cdots, r$,

$$\left|\bar{Q}_y(A_j) - Q_Y(A_j)\right| \leq \epsilon_1$$
$$1 - \epsilon_1 < \frac{\bar{Q}_y(A_j)}{Q_Y(A_j)} < 1 + \epsilon_1$$

Note that if $Q_Y(A_j) = 0$ then $Q_{XY}(A_i, A_j) = 0$ and hence

$$\left|\bar{Q}_{Zy}(A_i, A_j) - Q_{XY}(A_i, A_j)\right| = \bar{Q}_{Zy}(A_i, A_j)$$
$$\leq \bar{Q}_y(A_j) \leq \epsilon_1$$

and (5.25) is satisfied. If we choose $\epsilon_1$ smaller than any nonzero $Q_Y(A_j)$ it follows that $\bar{Q}_y(A_j) > 0$ whenever $Q_Y(A_j) > 0$. Now assume that $Q_Y(A_j) > 0$ and hence $\bar{Q}_y(A_j) > 0$. Define

$$Q_{X|Y}(A_i|A_j) = \frac{Q_{XY}(A_i, A_j)}{Q_Y(A_j)}$$
$$\bar{Q}_{Z|y}(A_i|A_j) = \frac{\bar{Q}_{Zy}(A_i, A_j)}{\bar{Q}_y(A_j)}$$

If $Q_Y(A_j) > 0$, the event in (5.25) is included in the event

$$\{\big|\bar{Q}_{Z|y}(A_i|A_j)\bar{Q}_y(A_j) - Q_{X|Y}(A_i|A_j)\bar{Q}_y(A_j) + Q_{X|Y}(A_i|A_j)\bar{Q}_y(A_j) - Q_{X|Y}(A_i|A_j)Q_Y(A_j)\big| \leq \epsilon_1\} \tag{5.26}$$

Note that

$$\begin{aligned}\big|Q_{X|Y}(A_i|A_j)\bar{Q}_y(A_j) - Q_{X|Y}(A_i|A_j)Q_Y(A_j)\big| &= Q_{X|Y}(A_i|A_j)\left|\bar{Q}_y(A_j) - Q_Y(A_j)\right| \\ &\leq \epsilon_1\end{aligned}$$

Therefore (5.26) implies

$$\{\big|\bar{Q}_{Z|y}(A_i|A_j)\bar{Q}_y(A_j) - Q_{X|Y}(A_i|A_j)\big|\,\bar{Q}_y(A_j) \leq 2\epsilon_1\}$$

And this implies

$$\{\big|\bar{Q}_{Z|y}(A_i|A_j)\bar{Q}_y(A_j) - Q_{X|Y}(A_i|A_j)\big| \leq \frac{2\epsilon_1}{\bar{Q}_y(A_j)(1-\epsilon_1)}\}$$

Let

$$\epsilon_2 = \max_{\substack{j=1 \\ Q_Y(A_j)>0}}^{r} \frac{2\epsilon_1}{\bar{Q}_y(A_j)(1-\epsilon_1)}$$

then the event in (5.25) is included in the event

$$\{\big|\bar{Q}_{Z|y}(A_i|A_j)\bar{Q}_y(A_j) - Q_{X|Y}(A_i|A_j)\big| \leq \epsilon_2$$

Therefore

$$Q_Z^n\left((Z^n,y)\in A_\epsilon^n(XY)\right)\leq$$
$$Q_Z^n\left(\bigcap_{\substack{i,j=1\\ Q_Y(A_j)>0}}^{r}\left\{\left|\bar{Q}_{Z|y}(A_i|A_j)-Q_{X|Y}(A_i|A_j)\right|\leq\epsilon_2\right\}\right)$$

Note that since $y$ is a deterministic sequence and $Z_i$'s are iid, the events

$$\left\{\left|\bar{Q}_{Z|y}(A_i|A_j)-Q_{X|Y}(A_i|A_j)\right|\leq\epsilon_2\right\}$$

are independent for different values of $j=1,\cdots,r$. Let $n_j=n\bar{Q}_y(A_j)$. Then,

$$Q_Z^n\left((Z^n,y)\in A_\epsilon^n(XY)\right)\leq$$
$$\prod_{\substack{j=1\\ Q_Y(A_j)>0}}^{r}Q_Z^{n_j}\left(\bigcap_{i=1}^{r}\left\{\left|\bar{Q}_{Z|y}(A_i|A_j)-Q_{X|Y}(A_i|A_j)\right|\leq\epsilon_2\right\}\right)$$

Since for $Q_Y(A_j)>0$, $n_j\to\infty$ as $n\to\infty$, it follows from Sanov's theorem [22] that

$$\limsup_{n\to\infty}\frac{1}{n_j}\log$$
$$Q_Z^{n_j}\left(\bigcap_{i=1}^{r}\left\{\left|\bar{Q}_{Z|y}(A_i|A_j)-Q_{X|Y}(A_i|A_j)\right|\leq\epsilon_2\right\}\right)$$
$$\leq-\left[D(Q_{X|Y}(\cdot|A_j)||Q_Z(\cdot))-\delta_j\right]$$

where $\delta_j\to0$ as $\epsilon_2\to0$. Therefore

$$\limsup_{n\to\infty}\frac{1}{n}\log Q_Z^n\left((Z^n,y)\in A_\epsilon^n(XY)\right)$$
$$\leq\sum_{\substack{j=1\\ Q_Y(A_j)>0}}^{r}\limsup_{n\to\infty}\frac{n_j}{n}D(Q_{X|Y}(\cdot|A_j)||Q_Z(\cdot))$$
$$\leq\sum_{\substack{j=1\\ Q_Y(A_j)>0}}^{r}-(1-\epsilon_1)Q_Y(A_j)\left[D(Q_{X|Y}(\cdot|A_j)||Q_Z(\cdot))-\delta_j\right]$$
$$\leq-(1-\epsilon_1)D(Q_{XY}||Q_ZQ_Y)+\delta'$$

where $\delta'\to0$ as $\epsilon_2\to0$. For finite $D(P_{XY}||P_ZP_Y)$ the statement of the lemma follows by choosing the quantization $Q$ such that $D(Q_{XY}||Q_ZQ_Y)$ is sufficiently close to $D(P_{XY}||P_ZP_Y)$.

#### 5.1.4.2 Proof of Lemma V.6

The proof follows along the lines of the proof of Theorem 22 of [47]. Let $Q = \{A_1, A_2, \cdots, A_r\}$ be a finite partition of $\mathbb{R}$. Let $Q_{XYZ}$, $Q_{XY}$, $Q_{XZ}$, $Q_{YZ}$, $Q_X$, $Q_Y$ and $Q_Z$ be measures induced by this partition, corresponding to $P_{XYZ}$, $P_{XY}$, $P_{XZ}$, $P_{YZ}$, $P_X$, $P_Y$ and $P_Z$ respectively. For the random sequence $Z^n = (Z_1, \cdots, Z_n)$ and the deterministic sequence $y = (y_1, \cdots, y_n)$ let $\bar{Q}_y$ be the deterministic empirical measure of $y$ and define the random empirical measures

$$\bar{Q}_{Zy}(A_i, A_j) = \frac{1}{n}\sum_{i=1}^{n} \mathbb{1}_{\{Z_i \in A_i, y_i \in A_j\}}$$
$$\bar{Q}_{Z}(A_i) = \frac{1}{n}\sum_{i=1}^{n} \mathbb{1}_{\{Z_i \in A_i\}}$$

For arbitrary $\delta > 0$, let $Q$ be such that

$$\pi(Q_{XY}, P_{XY}) < \epsilon$$
$$\pi(Q_{ZY}, P_{ZY}) < \epsilon$$
$$|D(P_{XY}||P_Z P_Y) - D(Q_{XY}||Q_Z Q_Y)| < \epsilon$$

We show that for such a quantization, under certain conditions, the probability of the event

$$\left\{\pi(\bar{Q}_{Zy}, Q_{XY}) < \epsilon\right\}$$

is close to the probability of the event

$$\left\{\pi(\bar{P}_{Zy}, P_{XY}) < 5\epsilon\right\}$$

It follows from Theorem 18 of [47] that for arbitrary $\epsilon, \delta' > 0$, there exists some $\bar{\epsilon} > 0$ such that for all $n$ greater than some $N$ if $y \in A^n_{\bar{\epsilon}}(Y)$, then

$$\lim_{n\to\infty} P\left(\pi(\bar{P}_{Zy}, P_{ZY}) < \epsilon\right) > 1 - \delta$$
$$\lim_{n\to\infty} P\left(\pi(\bar{Q}_{Zy}, Q_{ZY}) < \epsilon\right) > 1 - \delta$$

Consider the event

$$\left\{\pi(\bar{Q}_{Zy}, Q_{XY}) < \epsilon, \pi(\bar{P}_{Zy}, P_{ZY}) < \epsilon, \pi(\bar{Q}_{Zy}, Q_{ZY}) < \epsilon\right\}$$

This event implies

$$\begin{aligned}\pi(\bar{P}_{Zy}, P_{XY}) \leq \pi(\bar{P}_{Zy}, P_{ZY}) + \pi(Q_{ZY}, P_{ZY}) \\ + \pi(\bar{Q}_{Zy}, Q_{ZY}) + \pi(\bar{Q}_{Zy}, Q_{XY}) \\ + \pi(Q_{XY}, P_{XY}) \leq 5\epsilon\end{aligned}$$

Therefore

$$\begin{aligned}&P\left(\pi(\bar{P}_{Zy}, P_{XY}) \leq 5\epsilon\right) \geq \\ &P\left(\pi(\bar{Q}_{Zy}, Q_{XY}) < \epsilon, \pi(\bar{P}_{Zy}, P_{ZY}) < \epsilon, \bar{Q}_{Zy}, Q_{ZY}) < \epsilon\right)\end{aligned}$$

The right hand side can be lower bounded by

$$1 - P\left(\pi(\bar{Q}_{Zy}, Q_{XY}) \geq \epsilon\right) \tag{5.27}$$

$$- P\left(\pi(\bar{P}_{Zy}, P_{ZY}) \geq \epsilon\right) - P\left(\bar{Q}_{Zy}, Q_{ZY}) \geq \epsilon\right) \tag{5.28}$$

$$\geq P\left(\pi(\bar{Q}_{Zy}, Q_{XY}) < \epsilon\right) - \delta - \delta \tag{5.29}$$

Note that for arbitrary $\delta'$ and for sufficiently large $n$,

$$P\left(\pi(\bar{Q}_{Zy}, Q_{XY})\right) \geq 2^{-n[D(Q_{XY}||Q_Z Q_Y)+\delta']}$$

Since $\delta, \delta'$ are arbitrary and $D(Q_{XY}||Q_Z Q_Y) \approx D(P_{XY}||P_Z P_Y)$, it follows that

$$P\left(\pi(\bar{P}_{Zy}, P_{XY}) \leq 5\epsilon\right) \geq 2^{-n[D(P_{XY}||P_Z P_Y)+\delta+\epsilon']} - 2\delta$$

## 5.2 Distributed Source Coding

In this section, we consider a distributed source coding problem in which the sources can take values from continuous alphabets and there is one distortion constraint. We provide an information-theoretic inner bound to the optimal rate-distortion

region using group codes which strictly contains the available bounds based on random codes. The problem definition and the Berger-Tung rate regions are the continuous alphabets versions of those provided in Section 5.2.

### 5.2.1 The Main Result

In this section, we provide an inner bound to the achievable rate-distortion region which strictly contains the Berger-Tung rate region. Without a loss of generality, we assume that all the alphabets $\mathscr{X}, \mathscr{Y}, \hat{\mathscr{Z}}, \mathscr{P}, \mathscr{Q}, \mathscr{U}, \mathscr{V}, \mathscr{Z}$ are included in a Polish space $\mathscr{R}$.

#### 5.2.1.1 Finite Auxiliary Random variables and Bounded Continuous Distortion Function

In this section, we consider the case where the sources are not necessarily discrete but all of the auxiliary random variables are finite (subsets of $\mathscr{R}$). We generalize the definition of the channel coding mutual information as follows:

$$I^G_{c.c.}(X;Y) = \max_{\substack{w_{p,r},(p,r)\in\mathscr{Q}(G)\\ \sum w_{p,r}=1}} \min_{\substack{\theta\in\Theta\\ \theta\neq \boldsymbol{r}}} \frac{1}{1-\omega_\theta} D(p_{X[X]_\theta Y}||p_W p_{[X]_\theta Y}) \tag{5.30}$$

where $W$ is uniformly distributed over $G$. The following theorem is a generalization of Theorem III.1 to the case where the sources are not necessarily finite.

**Theorem V.15.** *For the distributed source $(\mathscr{X}, \mathscr{Y}, \mathscr{Z}, p_{XY}, d)$ assume the distortion function $d$ is bounded and continuous. Let $\hat{U}$, $\hat{V}$, $\hat{P}$ and $\hat{Q}$ be finite random variables jointly distributed with $XY$ according to the channel $p_{\hat{P}\hat{Q}\hat{U}\hat{V}|XY}$ such that $\hat{U}$ and $\hat{V}$ take values from a finite Abelian group $G$, and $\hat{P}$ and $\hat{Q}$ take values from finite sets $\mathscr{P}$ and $\mathscr{Q}$ respectively. Assume the following Markov chains hold*

$$\hat{P} \leftrightarrow X \leftrightarrow Y \leftrightarrow \hat{Q}$$

$$\hat{U} \leftrightarrow (\hat{P}, X) \leftrightarrow (Y, \hat{Q}) \leftrightarrow \hat{V}$$

*and assume there exists a bounded and continuous (with respect to its first argument) function* $g : G \times \mathscr{P} \times \mathscr{Q} \to \hat{\mathscr{Z}}$ *such that*

$$\mathbb{E}\Big\{d(X, Y, g(\hat{Z}, \hat{P}, \hat{Q}))\Big\} \leq D$$

*for* $\hat{Z} = \hat{U} + \hat{V}$ *where* $+$ *is the group operation. We show that with these definitions the rate-distortion triple* $(R_1, R_2, D)$ *is achievable where*

$$R_1 \geq I(X; \hat{P}|\hat{Q}) + D(p_{\hat{U}X\hat{P}}||p_{\hat{W}}p_{X\hat{P}}) - I^G_{c.c.}(\hat{Z}; \hat{P}\hat{Q})$$
$$R_2 \geq I(Y; \hat{Q}|\hat{P}) + D(p_{\hat{V}Y\hat{Q}}||p_{\hat{W}'}p_{Y\hat{Q}}) - I^G_{c.c.}(\hat{Z}; \hat{P}\hat{Q})$$
$$R_1 + R_2 \geq I(XY; \hat{P}\hat{Q}) + D(p_{\hat{U}\hat{V}XY\hat{P}\hat{Q}}||p_{\hat{W}\hat{W}'}p_{XY\hat{P}\hat{Q}}) - 2I^G_{c.c.}(Z; PQ)$$

*where* $\hat{W}$ *and* $\hat{W}'$ *are independent random variables uniformly distributed over* $G$.

The rest of this section is devoted to proving this theorem. In order to prove the theorem, it suffices to show the achievability of the following corner point:

$$R_1 = I(X; \hat{P}) + D(p_{\hat{U}X\hat{P}}||p_{\hat{W}}p_{X\hat{P}}) - I^G_{c.c.}(\hat{Z}; \hat{P}\hat{Q})$$
$$R_2 = I(Y; \hat{Q}|\hat{P}) + D(p_{\hat{V}Y\hat{Q}}||p_{\hat{W}'}p_{Y\hat{Q}}) - I^G_{c.c.}(\hat{Z}; \hat{P}\hat{Q})$$

The proof of this theorem is similar or the proof of Theorem III.1 with the difference that we use the notion of weak* typicality instead of the strong typicality. We need to show the following for the proof to go through:

**Size of the Typical Set:**

**Lemma V.16.** *Let* $X$ *and* $\hat{P}$ *be jointly distributed random variables distributed according to the measure* $p_{X\hat{P}}$ *such that* $X$ *is a random variable over a Polish alphabet* $\mathscr{X}$ *and* $\hat{P}$ *is a finite random variable over* $\mathscr{P}$. *Let* $\boldsymbol{x}$ *be a weakly* typical sequence in* $\mathscr{X}^n$ *then for any* $\epsilon > 0$ *there exists a* $\delta > 0$ *such that*

$$2^{\log|\mathscr{P}| - D(p_{X\hat{P}}||p_X p_{\hat{W}}) - \delta} \leq |A^n_\epsilon(\hat{P}|\boldsymbol{x})| \leq 2^{\log|\mathscr{P}| - D(p_{X\hat{P}}||p_X p_{\hat{W}}) + \delta}$$

*where $\hat{W}$ is a uniform random variable over $\mathscr{P}$ independent of $X$ and $\hat{P}$ and $\delta$ can be made to go to zero as $\epsilon \to 0$.*

*Proof.* Let $\hat{W}^n$ be random variable uniformly distributed over $\mathscr{P}^n$. Then we have

$$|A_\epsilon^n(\hat{P}|\boldsymbol{x})| = |\mathscr{P}|^n p_{\hat{W}}^n(\hat{W}^n \in A_\epsilon^n(\hat{P}|\boldsymbol{x}) \in) = |\mathscr{P}|^n p_{\hat{W}}^n((\boldsymbol{x}, \hat{W}^n) \in A_\epsilon^n(X\hat{P}) \in)$$

The rest of the proof follows from Lemmas V.5 and V.6. A special case is where both $X = \hat{X}$ and $\hat{P}$ are finite which is the standard strong typicality result since $\log|\mathscr{P}| - D(p_{\hat{X}\hat{P}}||p_{\hat{X}}p_{\hat{P}}) = H(\hat{P}|\hat{X})$. □

**Probability of the Typical Set and the Regular Markov Lemma:**

Let $X$ and $Y$ be two random variables over polish alphabets with joint distribution $p_{XY}$. It is shown in [47] that the probability of the typical set $P((X^n, Y^n) \in A_\epsilon^n(XY))$ approaches one as $\epsilon \to 0$ and $n \to \infty$. Let $\boldsymbol{x} \in A_\epsilon^n(X)$ and let $Y^n$ be distributed according to $p_{Y|X}^n(\cdot|\boldsymbol{x})$ then it is shown in [47] that $P((\boldsymbol{x}, Y^n) \in A_\epsilon^n(XY))$ approaches one as $\epsilon \to 0$ and $n \to \infty$ (the regular Markov Lemma).

**Probability of a Typical Sequence:**

Let $X$ and $\hat{P}$ be jointly distributed random variables distributed according to the measure $p_{XP}$ such that $X$ is a random variable over a Polish alphabet $\mathscr{X}$ and $\hat{P}$ is a finite random variable over $\mathscr{P}$. Let $\boldsymbol{x}$ be a weakly* typical sequence in $\mathscr{X}^n$. Then, for any $\hat{\boldsymbol{p}} \in A_\epsilon^n(\hat{P}|\boldsymbol{x})$ and for any such $\epsilon > 0$ there exists a $\delta > 0$ such that

$$\frac{1}{2^{\log|\mathscr{P}| - D(p_{X\hat{P}}||p_X p_{\hat{W}}) + \delta}} \leq p_{\hat{P}|X}^n(\hat{\boldsymbol{p}}|\boldsymbol{x}) \leq \frac{1}{2^{\log|\mathscr{P}| - D(p_{X\hat{P}}||p_X p_{\hat{W}}) - \delta}}$$

where $\hat{W}$ is a uniform random variable over $\mathscr{P}$ independent of $X$ and $\hat{P}$ and $\delta$ can be made to go to zero as $\epsilon \to 0$. To show this, let $Q_1, Q_2, \cdot$ be a sequence of increasing finite quantizations such that the sigma field generated by $\cup_{i=1}^\infty \mathscr{F}_{Q_i}$ is equal to $\mathscr{F}_X$ and let $[X]_{Q_i}$ and $[\boldsymbol{x}]_{Q_i}$ be the corresponding quantized random variables and sequences.

Such a sequence exists by [47, Lemma]. It remains to show that

$$\lim_{i\to\infty} p_{\hat{P}|[X]_{Q_i}}(\hat{\boldsymbol{p}}|[\boldsymbol{x}]_{Q_i}) = p_{\hat{P}|X}(\hat{\boldsymbol{p}}|\boldsymbol{x})$$
$$\lim_{i\to\infty} \frac{1}{2^{\log|\mathscr{P}|-D(p_{[X]_{Q_i}\hat{P}}||p_{[X]_{Q_i}}p_{\hat{W}})}} = \frac{1}{2^{\log|\mathscr{P}|-D(p_{X\hat{P}}||p_X p_{\hat{W}})}}$$

The first equality holds since $p_{\hat{P}|X}$ is a channel (see [47, Definition 2]). The second equality holds since by definition, $D(p_{[X]_{Q_i}\hat{P}}||p_{[X]_{Q_i}}p_{\hat{W}}) \to D(p_{X\hat{P}}||p_X p_{\hat{P}})$ and since $\frac{1}{2^{\log|\mathscr{P}|-x}}$ is a continuous function of $x$.

**The Strong Markov Lemma:**

Lemma III.2 can be extended to the case where $X$ and $Y$ are not necessarily finite:

**Lemma V.17.** *Let $X, Y, Z$ be random variables taking values from Polish alphabets $\mathscr{X}, \mathscr{Y}, \mathscr{Z}$ respectively such that $\mathscr{Z}$ is finite and the Markov chain $X \leftrightarrow Y \leftrightarrow Z$ holds. For $n = 1, 2, \cdots$, let $(\boldsymbol{x}^{(n)}, \boldsymbol{y}^{(n)}) \in A_\epsilon^n(XY)$ and let $K^{(n)}$ be a random vector taking values from $\mathscr{Z}^n$ with distribution satisfying (for simplicity of notation we call them $\boldsymbol{x}, \boldsymbol{y}, K$ respectively)*

$$P\left(K = \boldsymbol{z}\right) \leq p^n_{Z|Y}(\boldsymbol{z}|\boldsymbol{y})e^{\epsilon_n n}$$

*for some $\epsilon_n \to 0$ as $n \to \infty$. Then, as $n \to \infty$*

$$P\left((\boldsymbol{x}, \boldsymbol{y}, K) \in A_\epsilon^n(XYZ)\right) \to 1$$

*Proof.* Provided in Section 5.2.3.1. □

**Law of Large Numbers and the Convergence of the Average Distortion:**

We need to show that for $(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}, \boldsymbol{p}, \boldsymbol{q}) \in A_\epsilon^n(XYZPQ)$,

$$\frac{1}{n}\sum_{i=1}^{n} d(x_i, y_i, z_i, p_i, q_i) \to \mathbb{E}\{d(X, Y, g(Z, P, Q))\}$$

By definition of weak* typicality (and weak convergence of measures), the above happens if the function $d(X, Y, g(Z, P, Q))$ is bounded and continuous. A sufficient condition is to have $d$ bounded and both $d$ and $g$ continuous.

#### 5.2.1.2 Arbitrary Auxiliary Random Variables and Bounded Continuous Distortion Function

If we restrict the result of the previous section to the case where the Abelian groups are finite fields, then the following rates are achievable for finite auxiliary random variables:

$$R_1 = I(X;\hat{P}) + D(p_{\hat{U}X\hat{P}}||p_{\hat{W}}p_{X\hat{P}}) - D(p_{\hat{Z}\hat{P}\hat{Q}}||p_W p_{\hat{P}\hat{Q}})$$
$$R_2 = I(Y;\hat{Q}|\hat{P}) + D(p_{\hat{V}Y\hat{Q}}||p_W p_{Y\hat{Q}}) - D(p_{\hat{Z}\hat{P}\hat{Q}}||p_{\hat{W}}p_{\hat{P}\hat{Q}})$$

Where $\hat{Z} = \hat{U} + \hat{V}$ and $\hat{W}$ is a uniform random variable over the finite field. For random variables $X, P, Q, U, Z$, let the random variables $Z', P', Q'$ be identically distributed to $Z, P, Q$ and be independent of $X, P, Q, U, Z$. Define

$$r(X,P,Q,U,Z) = \sup_{Q_1}\inf_{Q_2}\mathbb{E}\{\log\frac{p_{[U]_{Q_1}|[X]_{Q_1}[P]_{Q_1}}([U]_{Q_1}|[X]_{Q_1}[P]_{Q_1})}{p_{[Z']_{Q_2}|[P']_{Q_2}[Q']_{Q_2}}([Z']_{Q_2}|[P']_{Q_2}[Q']_{Q_2})}\}$$

where the supremum and infimum are taken over the set of all finite partitions of the Polish space and similarly define $r(Y,P,Q,V,Z)$. Then, the above rates are equivalent to

$$R_1 = I(X;\hat{P}) + r(X,\hat{P},\hat{Q},\hat{U},\hat{Z})$$
$$R_2 = I(Y;\hat{Q}|\hat{P}) + r(Y,\hat{P},\hat{Q},\hat{V},\hat{Z})$$

It is straightforward to generalize the above result to the case where $\mathscr{P}$ and $\mathscr{Q}$ are not necessarily discrete to achieve the following corner point:

$$R_1 = I(X;P) + r(X,P,Q,\hat{U},\hat{Z})$$
$$R_2 = I(Y;Q|P) + r(Y,P,Q,\hat{V},\hat{Z})$$

**Definition 5.2.1.** Let $\mathscr{U} = \mathscr{V} = \mathscr{Z} = \mathscr{R}$ be Polish spaces and let $f : \mathscr{U} \times \mathscr{V} \to \mathscr{Z}$ be an arbitrary function. Let $G_1, G_2, G_3, \cdots$ be a sequence of finite fields and with a slight abuse of notation, for $i = 1, 2, \cdots$, define the corresponding quantization

mappings as follows:

$$q_i : \mathscr{R} \to G_i$$
$$q_i^{-1} : G_i \to \mathscr{R}$$

For $i = 1, 2, \cdots$, let $\hat{U}_i = q_i^{-1}(q_i(U))$, $\hat{V}_i = q_i^{-1}(q_i(V))$ and $\hat{Z}_i = q_i^{-1}\Big(q_i(U) +_{G_i} q_i(V)\Big)$. We say that the function $f(\cdot,\cdot)$ is embeddable in the sequence $G_1, G_2, \cdots$ if there exist quantization mappings so that the sequence $(X, Y, P, Q, \hat{U}_i, \hat{V}_i, \hat{Z}_i)$ converges weakly (in distribution) to $(X, Y, P, Q, U, V, Z)$.

**Lemma V.18.** *Let $(X, Y, P, Q, \hat{U}_i, \hat{V}_i, \hat{Z}_i)$ be a sequence of random variables converging in distribution to $(X, Y, P, Q, U, V, Z)$. Then*

$$r(X, P, Q, \hat{U}_i, \hat{Z}_i) \to r(X, P, Q, U, Z)$$
$$r(Y, P, Q, \hat{V}_i, \hat{Z}_i) \to r(Y, P, Q, V, Z)$$

*if the quantities on the right-hand-side exist.*

*Proof.* For any $\epsilon > 0$, let $Q_1$ and $Q_2$ be finite partitions such that

$$\left| r(X, P, Q, U, Z) - \mathbb{E}\{\log \frac{p_{[U]_{Q_1}|[X]_{Q_1}[P]_{Q_1}}([U]_{Q_1}|[X]_{Q_1}[P]_{Q_1})}{p_{[Z']_{Q_2}|[P']_{Q_2}[Q']_{Q_2}}([Z']_{Q_2}|[P']_{Q_2}[Q']_{Q_2})}\} \right| \leq \epsilon$$

Using [47, Lemma 7], we can restrict attention to partitions $Q_1$ and $Q_2$ consisting of continuity sets. It can be verified that $r(\hat{X}, \hat{P}, \hat{Q}, \hat{U}, \hat{Z})$ is a continuous function of the probability masses when all random variables are finite. Let $\delta > 0$ be such that if the total variation distance between a probability mass functions of $(\hat{X}, \hat{P}, \hat{P}', \hat{Q}', \hat{U}, \hat{Z}')$ and $([X]_{Q_1}, [P]_{Q_1}, [P]_{Q_2}[Q]_{Q_2}, [U]_{Q_1}, [Z]_{Q_2})$ is less than $\delta$ then

$$\left| r(\hat{X}, \hat{P}, \hat{Q}, \hat{U}, \hat{Z}) - \mathbb{E}\{\log \frac{p_{[U]_{Q_1}|[X]_{Q_1}[P]_{Q_1}}([U]_{Q_1}|[X]_{Q_1}[P]_{Q_1})}{p_{[Z']_{Q_2}|[P']_{Q_2}[Q']_{Q_2}}([Z']_{Q_2}|[P']_{Q_2}[Q']_{Q_2})}\} \right| \leq \frac{\epsilon}{2}$$

Let $N$ be such that for $i > N$, the total variation distance between the probability mass density of $([\hat{X}_i]_{Q_1}, [\hat{P}_i]_{Q_1}, [\hat{P}_i']_{Q_2}, [\hat{Q}_i']_{Q_2}, [\hat{U}_i]_{Q_1}, [\hat{Z}_i']_{Q_2})$ and the probability mass

density of $([X]_{Q_1}, [P]_{Q_1}, [P']_{Q_1}, [Q']_{Q_2}, [U]_{Q_1}, [Z']_{Q_2})$ is less than $\delta$. Then for $i > N$, we have

$$\left| r(\hat{X}_i, \hat{P}_i, \hat{Q}_i, \hat{U}_i, \hat{Z}_i) - \mathbb{E}\{\log \frac{p_{[U]_{Q_1}|[X]_{Q_1}[P]_{Q_1}}([U]_{Q_1}|[X]_{Q_1}[P]_{Q_1})}{p_{[Z']_{Q_2}|[P']_{Q_2}[Q']_{Q_2}}([Z']_{Q_2}|[P']_{Q_2}[Q']_{Q_2})}\} \right| \leq \frac{\epsilon}{2}$$

Therefore,

$$\left| r(X, P, Q, U, Z) - r(\hat{X}_i, \hat{P}_i, \hat{Q}_i, \hat{U}_i, \hat{Z}_i) \right| \leq \epsilon$$

for all $i > N$. □

**Theorem V.19.** *For the distributed source $(\mathscr{X}, \mathscr{Y}, \hat{\mathscr{Z}}, p_{XY}, d)$ assume $\mathscr{X}$, $\mathscr{Y}$ and $\hat{\mathscr{Z}}$ are polish spaces and assume the distortion function $d : \mathscr{X} \times \mathscr{Y} \times \hat{\mathscr{Z}} \to \mathbb{R}^+$ is bounded and continuous. Let $U$, $V$, $P$ and $Q$ be random variables jointly distributed with $XY$ according to the channel $p_{PQUV|XY}$ such that $U$ and $V$ take values from a polish spaces $\mathscr{U} = \mathscr{V} = \mathscr{R}$, and $P$ and $Q$ take values from sets $\mathscr{P}$ and $\mathscr{Q}$ respectively. Assume the following Markov chains hold*

$$P \leftrightarrow X \leftrightarrow Y \leftrightarrow Q$$
$$U \leftrightarrow (P, X) \leftrightarrow (Y, Q) \leftrightarrow V$$

*Let $Z = f(U, V)$ for some function $f(\cdot, \cdot)$ which is embeddable in a sequence $G_1, G_2, \cdots$ of finite fields. Assume there exists a continuous function $g : \mathscr{R} \times \mathscr{P} \times \mathscr{Q} \to \hat{\mathscr{Z}}$ such that*

$$\mathbb{E}\Big\{ d(X, Y, g(Z, P, Q)) \Big\} \leq D$$

*Then, if $r(X, P, Q, U, Z)$ and $r(Y, P, Q, V, Z)$ exist, the rate-distortion triple $(R_1, R_2, D)$ is achievable where*

$$R_1 = I(X; P) + r(X, P, Q, U, Z)$$
$$R_2 = I(Y; Q|P) + r(Y, P, Q, V, Z)$$

*Proof.* Note that for $i = 1, 2, \cdots$, $\hat{U}_i$ and $\hat{V}_i$ are functions of $U$ and $V$ respectively. Therefore, the following Markov chains hold:

$$P \leftrightarrow X \leftrightarrow Y \leftrightarrow Q$$

$$\hat{U}_i \leftrightarrow (P, X) \leftrightarrow (Y, Q) \leftrightarrow \hat{V}_i$$

The weak convergence of $(X, Y, P, Q, \hat{U}_i, \hat{V}_i, \hat{Z}_i)$ to $(X, Y, P, Q, U, V, Z)$ and the continuity of the functions $g$ and $d$ and the boundedness of $d$ imply that

$$\mathbb{E}\Big\{d(X, Y, g(\hat{Z}_i, P, Q))\Big\} \to \mathbb{E}\Big\{d(X, Y, g(Z, P, Q))\Big\} \leq D$$

Therefore, the rate-distortion tuple $(R_1, R_2, D)$ is achievable where

$$R_1 = I(X; P) + r(X, P, Q, \hat{U}_i, \hat{Z}_i)$$

$$R_2 = I(Y; Q|P) + r(Y, P, Q, \hat{V}_i, \hat{Z}_i)$$

The proofs follows since

$$r(X, P, Q, \hat{U}_i, \hat{Z}_i) \to r(X, P, Q, U, Z)$$

$$r(Y, P, Q, \hat{V}_i, \hat{Z}_i) \to r(Y, P, Q, V, Z)$$

□

#### 5.2.1.3 Arbitrary Auxiliary Random Variables and Bounded Continuous Distortion Function

The result above can be generalized to the case where the distortion function is continuous but not necessarily bounded. The approach is similar to the one proposed in Section 5.1.2.3 and is omitted.

#### 5.2.1.4 Calculation of the Rates for Distributions with Densities

In this section, we calculate the rates $r(X, P, Q, U, Z)$ and $r(Y, P, Q, V, Z)$ for the case where all probability density functions are defined. It is straightforward to show

that in this case,

$$r(X,P,Q,U,Z) = \mathbb{E}\Big\{ \log \frac{f_{U|XP}(U|XP)}{f_{Z'|P'Q'}(Z'|P'Q')} \Big\}$$
$$= h(Z|PQ) - h(U|XP)$$

Similarly, we can show that

$$r(Y,P,Q,V,Z) = h(Z|PQ) - h(V|YQ)$$

so that the rate-distortion tuple $(R_1, R_2, D)$ is achievable where

$$R_1 = I(X;P) + h(Z|PQ) - h(U|XP)$$
$$R_2 = I(Y;Q|P) + h(Z|PQ) - h(V|YQ)$$

### 5.2.2 Examples

In this section, we present two examples of mappings which are embeddable in a sequence of finite fields.

**Real Addition is Embeddable in a Sequence of Fields:**

Let all alphabets be equal to $\mathbb{R}$ and let $f(U,V) = U+V$ where $+$ is the real addition. For $i = 1, 2, \cdots$, let $\gamma_i = \frac{1}{2^i}$ and let $p_i$ be the smallest prime larger than $2^{2i}$ (so that $\gamma_i p_i \to \infty$ as $i \to \infty$). Let the sequence of finite fields be defined by $G_i = \mathbb{F}_{p_i}$ for $i = 1, 2, \cdots$. Define the quantization mappings $q_i : \mathbb{R} \to G_i$ and $q_i^{-1} : G_i \to \mathbb{R}$ as follow:

$$q_i(x) = \begin{cases} 0 & x < -\frac{\gamma_i p_i}{2} + \gamma_i \\ k-1 & x \in \big( -\frac{\gamma_i p_i}{2} + k\gamma_i, -\frac{\gamma_i p_i}{2} + (k+1)\gamma_i \big), k = 2, \cdots, p_i - 1 \\ p_i - 1 & x > -\frac{\gamma_i p_i}{2} + (p_i - 1)\gamma_i = \frac{\gamma_i p_i}{2} - \gamma_i \end{cases}$$

$$q_i^{-1}(k) = \frac{2k + 1 - p_i}{2}\gamma_i \qquad k = 0, \cdots, p_i - 1$$

Note that this is essentially a uniform quantizer. We show that with these quantizers, the real addition is embeddable in the sequence $G_1, G_2, \cdots$. It suffices to show that $(X, Y, P, Q, \hat{U}_i, \hat{V}_i, \hat{Z}_i)$ converges in probability to $(X, Y, P, Q, U, V, Z)$. We need to show that for any $\epsilon, \delta > 0$, there exists $N > 0$ such that for all $i > N$,

$$P(|U - \hat{U}_i| < \delta, |V - \hat{V}_i| < \delta, |Z - \hat{Z}_i| < \delta) \geq 1 - \epsilon$$

Let $L$ be such that $P(U \in (-L, L), V \in (-L, L)) > 1 - \frac{\epsilon}{3}$ and let $N$ be such that for $i = N$, $\gamma_i \leq \frac{\delta}{2}$ and $\gamma_i p_i > 4L$. These conditions guarantee that $|U - \hat{U}_i| < \frac{\delta}{2}$ and $|V - \hat{V}_i| < \frac{\delta}{2}$ with probability larger than $1 - \frac{\epsilon}{3}$. Furthermore, under the condition $\gamma_i p_i > 4L$ and for $|u|, |v| \leq L$ we have $q_i^{-1}(q_i(u) +_{G_i} q_i(v)) = q_i^{-1}(q_i(u)) + q_i^{-1}(q_i(v))$ where the addition on the right-hand-side is the real addition. We have

$$\begin{aligned} P(|Z - \hat{Z}_i| \geq \delta) &\leq P(|Z - \hat{Z}_i| \geq \delta, |U| \leq L, |V| \leq L) + \frac{\epsilon}{3} \\ &= P(|U + V - \hat{U}_i - \hat{V}_i| \geq \delta, |U| \leq L, |V| \leq L) + \frac{\epsilon}{3} \\ &\leq P(|U - \hat{U}_i| + |V - \hat{V}_i| \geq \delta, |U| \leq L, |V| \leq L) + \frac{\epsilon}{3} \\ &= \frac{\epsilon}{3} \end{aligned}$$

**Mod-$2\pi$ Addition is Embeddable in a Sequence of Fields:**

This case is similar to the previous case. The rate-distortion tuple $(R_1, R_2, D)$ is achievable where

$$\begin{aligned} R_1 &= I(X; P) + h(Z|PQ) - h(U|XP) \\ R_2 &= I(Y; Q|P) + h(Z|PQ) - h(V|YQ) \end{aligned}$$

where $Z = U + V \pmod{2\pi}$.

**Other examples:**

Real addition in $\mathbb{R}^n$ and mod-$2\pi$ addition in $\mathbb{R}^n$ can be embedded in the sequence $\mathbb{F}_{p_i}^n$. $\mathbb{R}^+$ with multiplication operation is embeddable in $\mathbb{F}_{p_i}$ with pre-mappings $u \to \log u$

and $v \to \log v$ and the post mapping $\log z \to z$. $(2^{\mathbb{R}}, \cdot)$ is embeddable in $\mathbb{F}_{p_i}$ with log pre-mappings.

### 5.2.3 Appendix

#### 5.2.3.1 Proof of Lemma V.17

Let $f_{XYZ}$ be a generating field defined over $\mathscr{X} \times \mathscr{Y} \times \mathscr{Z}$ according to [47, Cor. 8]. By definition of weak* typicality (see Definition 11 and Theorem 1 of [47]), we need to show that for any set $S$ in $f_{XYZ}$, $\lim_{n\to\infty} \bar{P}_{x,y,K}(S) = P_{XYZ}(S)$ with probability one. Any open set in $f_{XYZ}$ can be represented as a disjoint countable union of sets of the form $A \times B \times C$ where $A \in \mathscr{X}$, $B \in \mathscr{Y}$ and $C \in \mathscr{Z}$. Let $f_X$, $f_Y$ and $f_Z$ be generating fields over $\mathscr{X}$, $\mathscr{Y}$ and $\mathscr{Z}$ respectively defined as in [47, Cor. 8]. It suffices to show that for all $A \in f_X$, $B \in f_Y$ and $C \in f_Z$,

$$\left|\bar{P}_{x,y,K}(A,B,C) - P_{XYZ}(A,B,C)\right| \to 0$$

with probability one as $n \to \infty$. We have

$$\begin{aligned}&\left|\bar{P}_{x,y,K}(A,B,C) - p_{XYZ}(A,B,C)\right| \leq \\ &\left|p_{XYZ}(A,B,C) - \bar{P}_{x,y}W_{Z|Y}(A,B,C)\right| + \left|\bar{P}_{x,y}W_{Z|Y}(A,B,C) - \bar{P}_{x,y,K}(A,B,C)\right|\end{aligned}$$

Note that w-$\lim_{n\to\infty} \bar{P}_{x,y} = p_{XY}$. Therefore, [47, Lemma 16] implies w-$\lim_{n\to\infty} \bar{P}_{x,y,K} = p_{XYZ}$ with probability one. This implies $\lim_{n\to\infty} \bar{P}_{x,y,K}(A,B,C) = p_{XYZ}$ with probability one or equivalently, the first term in the equation above vanishes as $n$ increases almost surely. Next, we show that the second term also vanishes almost surely. We have

$$\begin{aligned}\bar{P}_{x,y}W_{Z|Y}(A,B,C) - \bar{P}_{x,y,K}(A,B,C) &= \frac{1}{n}\sum_{i=1}^{n} \mathbb{1}_{\{x_i\in A, y_i \in B\}}\left[W_{Y|Z}(C|y_i) - \mathbb{1}_{\{K_i \in C\}}\right] \\ &= \frac{1}{n}\sum_{i=1}^{n}\theta_i\end{aligned}$$

where for $i = 1, 2, \cdots, n$,

$$\theta_i = \mathbb{1}_{\{x_i \in A, y_i \in B\}} \left[ W_{Y|Z}(C|y_i) - \mathbb{1}_{\{K_i \in C\}} \right]$$

It suffices to show that

$$|\frac{1}{n} \sum_{i=1}^{n} \tilde{\theta}_i| \to 0$$

almost surely as $n \to \infty$ where

$$\theta_i = W_{Y|Z}(C|y_i) - \mathbb{1}_{\{K_i \in C\}}$$

Let $Z^n$ be a random vector generated according to $W_{Z|Y}(\cdot|y)$ and define

$$\tilde{\theta}_i = W_{Y|Z}(C|y_i) - \mathbb{1}_{\{Z_i \in C\}}$$

Note that both $\theta_i$ and $\tilde{\theta}_i$ are binary random variables taking values from the set $\{W_{Z|Y}(C|y_i), W_{Z|Y}(C|y_i) - 1\}$ and $|\theta_i|, |\tilde{\theta}_i| \leq 1$. We have $\mathbb{E}\{\tilde{\theta}_i\} = 0$ and $\text{var}\{\tilde{\theta}_i\} \leq 1$. It follows from [Proposition 1, Zhiyi Chi's paper] that $\tilde{\theta}_i$ satisfied the large deviations principle with a good rate function $I(\cdot)$ such that

$$P\left( \frac{\tilde{\theta}'_1 + \cdots + \tilde{\theta}'_n}{n} \geq t \right) \leq e^{-nI(t)}$$

where $I(t)$ is positive. For $b \in \{W_{Z|Y}(C|y_i), W_{Z|Y}(C|y_i) - 1\}^n$, we have

$$\begin{aligned} P\left(\tilde{\theta} = b\right) &= \sum_{\substack{z \in \mathcal{Z}^n \\ b_i = W_{Z|Y}(C|y_i) \Rightarrow z_i \notin C \\ b_i = W_{Z|Y}(C|y_i) - 1 \Rightarrow z_i \in C}} P\left(K = z\right) \\ &\leq \sum_{\substack{z \in \mathcal{Z}^n \\ b_i = W_{Z|Y}(C|y_i) \Rightarrow z_i \notin C \\ b_i = W_{Z|Y}(C|y_i) - 1 \Rightarrow z_i \in C}} W^n_{Z|Y}(z|y) e^{\epsilon_n n} \\ &= e^{\epsilon_n n} P\left(\tilde{\theta}' = b\right) \end{aligned}$$

We have

$$P\left(\frac{\tilde{\theta}_1+\cdots+\tilde{\theta}_n}{n}\geq t\right) = \sum_{b:\left|\frac{b_1+\cdots+b_n}{n}\right|\geq nt} P\left(\tilde{\theta}=b\right)$$
$$\leq e^{\epsilon_n n} \sum_{b:\left|\frac{b_1+\cdots+b_n}{n}\right|\geq nt} P\left(\tilde{\theta}'=b\right)$$
$$\leq e^{-n(I(t)-\epsilon_n)}$$

Note that since $e^{-n(I(t)-\epsilon_n)}$ is summable, the Borel-Cantelli lemma implies that for all $t>0$,

$$\limsup_{n\to\infty} |\frac{1}{n}\sum_{i=1}^{n}\tilde{\theta}_i| \leq t$$

Therefore, $|\frac{1}{n}\sum_{i=1}^{n}\tilde{\theta}_i| \to 0$ as $n\to\infty$ almost surely.

# CHAPTER VI

# Polar Codes for Point-to-Point Communications

## 6.1 Polar Codes for Arbitrary DMCs

In this section, we show that polar codes with their original $(u, u+v)$ kernel, achieve the symmetric capacity of discrete memoryless channels with arbitrary input alphabet sizes. It is shown that in general, channel polarization happens in several, rather than only two levels so that the synthesized channels are either useless, perfect or "partially perfect". Any subset of the channel input alphabet which is closed under addition, induces a coset partition of the alphabet through its shifts. For any such partition of the input alphabet, there exists a corresponding partially perfect channel whose outputs uniquely determine the coset to which the channel input belongs. By a slight modification of the encoding and decoding rules, it is shown that perfect transmission of certain information symbols over partially perfect channels is possible. Our result is general regarding both the cardinality and the algebraic structure of the channel input alphabet; i.e we show that for any channel input alphabet size and any Abelian group structure on the alphabet, polar codes are optimal. Due to the modifications we make to the encoding rule of polar codes, the constructed codes fall into a larger class of structured codes called nested group codes.

Polar codes were originally proposed by Arikan in [10] for discrete memoryless

channels with a binary input alphabet. Polar codes over binary input channels are shifted linear (coset) codes capable of achieving the symmetric capacity of channels. These codes are constructed based on the Kronecker power of the $2 \times 2$ matrix $\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$ and are the first known class of capacity achieving codes with an explicit construction.

It is known that non-binary codes outperform binary codes in certain communication settings. Therefore, constructing capacity achieving codes for channels of arbitrary input alphabet sizes is of great interest. In order to construct capacity achieving codes over non-binary channels, there have been attempts to extend polar coding techniques to channels of arbitrary input alphabet sizes. It is shown in [66] that polar codes achieve the symmetric capacity of channels when the size of the input alphabet is a prime. For channels of arbitrary input alphabet sizes, it is shown in [66] that the original construction of polar codes does not necessarily achieve the symmetric capacity of the channel due to the fact that polarization (into two levels) may not occur for arbitrary channels. In the same paper, a randomized construction of polar codes based on permutations is proposed. In this approach, the existence of a polarizing transformation is shown by a random coding argument over the ensemble of permutations of the input alphabet. In another approach in [66], a code construction method is proposed which is based on the decomposition of the composite input channel into sub-channels of prime input alphabet sizes. In this multilevel code construction method, a separate polar code is designed for each sub-channel of prime input alphabet size. In [48], the problem of channel polarization using arbitrary kernels is studied and several sufficient conditions are provided under which a kernel can polarize a non-binary channels. It is shown in [65] that the two-level polarization of arbitrary DMC's can be achieved using a variety of non-linear polarizing transforms.

Another related work is [5], in which the authors have shown that polar codes, with their original $(u, u+v)$ kernel, are sufficient to achieve the uniform sum rate on any binary input MAC and it is stated that the same technique can be used for the point-to-point problem to achieve the symmetric capacity of the channel when the size of the alphabet is a power of 2. In a recent work, it has been shown in [54] that polar codes achieve the symmetric capacity of channels with input alphabet size a power of 2. The difference between the approach proposed in [5] and the result of [54] is that in the former, the channel's input alphabet is assumed to be the group $\mathbb{Z}_2^r$ (with componentwise mod-2 operation) for some integer $r$ and in the latter, the channel's input alphabet is assumed to be the group $\mathbb{Z}_{2^r}$ (with mod-$2^r$ operation) for some integer $r$. Both of these cases can be recovered from the general result we propose in this paper depending on how the channel input alphabet is endowed with an Abelian group structure. The techniques used in [54] to prove the polarization, although not explicitly using the group-theoretical terminology, are similar to the techniques used in [58] and the current paper when they are specialized to channels of size $2^r$ with mod-$2^r$ operation. However in [54], the convergence of Bhattacharyya parameters is shown through a new "martingale convergence" type result which is different from the approach of this paper.

In this section, we show that with a slight modification of the encoding and decoding rules, polar codes, with their original $(u, u+v)$ kernel, are sufficient to achieve the symmetric capacity of all discrete memoryless channels. Our result is general regarding both the cardinality and the algebraic structure of the channel input alphabet; i.e we show that for any channel input alphabet size and any Abelian group structure on the alphabet, polar codes are optimal. This result was first reported in [58]. We use a combination of algebraic and coding techniques and show that in general, channel

polarization occurs in several levels rather than only two: Suppose the channel input alphabet is $\mathbf{G}$ and is endowed with an Abelian group structure. Then for any subset $H$ of the channel input alphabet $\mathbf{G}$ which is closed under addition (i.e any subgroup of $\mathbf{G}$), there may exist a corresponding polarized channel which can perfectly transmit the index of the shift (coset) of $H$ in $\mathbf{G}$ which contains the input. As an example, for a channel of input alphabet $\mathbb{Z}_6$, there are four subgroups of the input alphabet: **i)** $\{0\}$ with cosets $\{0\}$, $\{1\}$, $\{2\}$, $\{3\}$, $\{4\}$ and $\{5\}$, **ii)** $\{0,3\}$ with cosets $\{0,3\}$, $\{1,4\}$ and $\{2,5\}$, **iii)** $\{0,2,4\}$ with cosets $\{0,2,4\}$ and $\{1,3,5\}$ and **iv)** $\mathbb{Z}_6$. For polar codes over $\mathbb{Z}_6$, the asymptotic synthesized channels can exist in four forms: **i)** can determine which one of the cosets $\{0\}$, $\{1\}$, $\{2\}$, $\{3\}$, $\{4\}$ or $\{5\}$ contains the input symbol, (perfect channels with capacity $\log_2 6$ bits per channel use), **ii)** can determine which one of the cosets $\{0,3\}$, $\{1,4\}$ or $\{2,5\}$ contains the input symbol (partially perfect channels with capacity $\log_2 3$ bits per channel use), **iii)** can determine which one of the cosets $\{0,2,4\}$ or $\{1,3,5\}$ contains the input symbol (partially perfect channels with capacity 1 bit per channel use), **iv)** can only determine the input belongs to $\{0,1,2,3,4,5\}$ (useless channel). Cases **i**,**ii**,**iii** and **iv** correspond to coset decompositions of $\mathbb{Z}_6$ based on subgroups $\{0\}$, $\{0,3\}$, $\{0,2,4\}$ and $\{0,1,2,3,4,5\}$ respectively.

Although standard binary polar codes are group (linear) codes, the class of capacity achieving codes constructed and analyzed in this paper are not group codes. If polar codes are used in their standard form, i.e. when only perfect channels are used and partially perfect and useless channels are ignored, it can be shown that they will form group codes. It is known that group codes do not generally achieve the symmetric capacity of discrete memoryless channels [6, 18]. Hence, one could have predicted that standard polar codes cannot achieve the symmetric capacity of arbitrary channels and a modification of the encoding rule is indeed necessary to achieve that goal. Due to the modifications we make to the encoding rule of polar codes, the

constructed codes fall into a larger class of structured codes called nested group codes.

### 6.1.1 Preliminaries

#### 6.1.1.1 Symmetric Capacity and the Bhattacharyya Parameter

For a channel $(\mathscr{X}, \mathscr{Y}, W)$, the symmetric capacity is defined as $I^0(W) = I(X;Y)$ where the channel input $X$ is uniformly distributed over $\mathscr{X}$ and $Y$ is the output of the channel; i.e. for $q = |\mathscr{X}|$,

$$I^0(W) = \sum_{x \in \mathscr{X}} \sum_{y \in \mathscr{Y}} \frac{1}{q} W(y|x) \log \frac{W(y|x)}{\sum_{\tilde{x} \in \mathscr{X}} \frac{1}{q} W(y|\tilde{x})}$$

The Bhattacharyya distance between two distinct input symbols $x$ and $\tilde{x}$ is defined as

$$Z(W_{\{x,\tilde{x}\}}) = \sum_{y \in \mathscr{Y}} \sqrt{W(y|x)W(y|\tilde{x})}$$

and the average Bhattacharyya distance is defined as

$$Z(W) = \sum_{\substack{x,\tilde{x} \in \mathscr{X} \\ x \neq \tilde{x}}} \frac{1}{q(q-1)} Z(W_{\{x,\tilde{x}\}})$$

#### 6.1.1.2 Binary Polar Codes

For any $N = 2^n$, a polar code of length $N$ designed for the channel $(\mathbb{Z}_2, \mathscr{Y}, W)$ is a linear (coset) code characterized by a generator matrix $G_N$ and a set of indices $A \subseteq \{1, \cdots, N\}$ of *almost perfect channels*. The generator matrix for polar codes is defined as $G_N = B_N F^{\otimes n}$ where $B_N$ is a permutation of rows, $F = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$ and $\otimes$ denotes the Kronecker product. The set $A$ is a function of the channel and determines the locations of the *information bits*. The decoding algorithm for polar codes is a specific form of successive cancellation [10].

#### 6.1.1.3 Polar Codes Over Abelian Groups

For any discrete memoryless channel, there always exists an Abelian group of the same size as that of the channel input alphabet. In general, for an Abelian group, there may not exist a multiplication operation. Since polar encoders are characterized by a matrix multiplication, before using these codes for channels of arbitrary input alphabet sizes, a generator matrix for codes over Abelian groups needs to be properly defined. In Appendix 6.1.6.1, a convention is introduced to generate codes over groups using $\{0, 1\}$-valued generator matrices.

#### 6.1.1.4 Notation

We denote by $O(\epsilon)$ any function of $\epsilon$ which is right-continuous around 0 and that $O(\epsilon) \to 0$ as $\epsilon \downarrow 0$.

For positive integers $N$ and $r$, let $\{A_0, A_1, \cdots, A_r\}$ be a partition of the index set $\{1, 2, \cdots, N\}$. Given sets $T_t$ for $t = 0, \cdots, r$, the direct sum $\bigoplus_{t=0}^{r} T_t^{A_t}$ is defined as the set of all tuples $u_1^N = (u_1, \cdots, u_N)$ such that $u_i \in T_t$ whenever $i \in A_t$.

### 6.1.2 Motivating Examples

A key property of the basic polarizing transforms used for binary polar codes is that they have perfect and useless channels as their "fixed points"; in the sense that, if these transforms are applied to a perfect (useless) channel, the resulting channel is also perfect (useless). Moreover, these type of channels are the only fixed points of these transformations. In the following, we try to demonstrate that for non-binary channels, the basic transforms have fixed points which are neither perfect nor useless. Consider a 4-ary channel $(\mathbb{Z}_4, \mathscr{Y}, W)$ and assume the channel is such that $W(y|u) = W(y|u + 2)$ for all $y \in \mathscr{Y}$ and all $u \in \mathbb{Z}_4$; i.e. the channel cannot distinguish between inputs $u$ and $u + 2$. Consider the transformed channels $W^-$ and

$W^+$ originally introduced in [10] (Refer to Equations (6.32) and (6.33) of the current paper). It turns out that

$$W^+(y_1, y_2, u_1|u_2) = W^+(y_1, y_2, u_1|u_2 + 2)$$
$$W^-(y_1, y_2|u_1) = W^-(y_1, y_2|u_1 + 2)$$

for all $y_1, y_2 \in \mathscr{Y}$ and all $u_1, u_2 \in \mathbb{Z}_4$. This observation is closely related to the fact that $\{0, 2\}$ is closed under addition mod-4; i.e. the fact that $\{0, 2\}$ forms a subgroup of $\mathbb{Z}_4$. This means that the transformed channels inherit this characteristic feature of the original channel, in the sense that they cannot distinguish between inputs $u_i$ and $u_i + 2$ ($i = 2$ for $W^+$ and $i = 1$ for $W^-$). This suggests that even in the asymptotic regime, the transformed channels can only distinguish between the sets $\{0, 2\}$ and $\{1, 3\}$, and not within each set. In the following, we give an example for which such cases indeed exist in the asymptotic regime.

Consider the channel depicted in Figure 6.1. For this channel, the symmetric capacity is equal to $C = I(X;Y) = 2-\epsilon-2\lambda$ bits per channel use. Depending on the values of the parameters $\epsilon$ and $\lambda$, this channel can present three extreme cases: 1) If $\lambda = 1$, this channel is useless. 2) If $\epsilon = 1$, this channel cannot distinguish between inputs $u$ and $u + 2$ and has a capacity of 1 bit per channel use. 3) If $\epsilon = \lambda = 0$, this channel is perfect and has a capacity of 2 bits per channel use.

Given a sequence of bits $b_1 b_2 \cdots b_n$, define $W^{b_1 b_2 \cdots b_n}$ as in [10, Section IV], and let $I(W^{b_1 b_2 \cdots b_n})$ be the mutual information between the input and output of $W^{b_1 b_2 \cdots b_n}$ when the input is uniformly distributed. We can find $I(W^{b_1 b_2 \cdots b_n})$ using the following recursion for which the proof can be found in Appendix 6.1.6.2.

Define $\epsilon_0 = \epsilon$ and $\lambda_0 = \lambda$. For $i = 1, \cdots, n$,

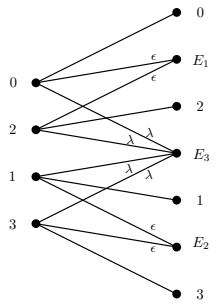


Figure 6.1: Channel 1: The input of the channel has the structure of the group $\mathbb{Z}_4$. The parameters $\epsilon$ and $\lambda$ take values from $[0,1]$ such that $\epsilon + \lambda \leq 1$. $E_1$ and $E_2$ are erasures connected to cosets of the subgroup $\{0,2\}$. The lines connecting the output symbols $0,2,1,3$ to their corresponding inputs, represent a conditional probability of $1-\epsilon-\lambda$. For this channel, the process $I(W^{b_1 b_2 \cdots b_n})$ can be explicitly found for each $n$ and the multilevel polarization can be observed.

- If $b_i = 1$, let

$$\begin{cases} \epsilon_i = \epsilon_{i-1}^2 + 2\epsilon_{i-1}\lambda_{i-1} \\ \lambda_i = \lambda_{i-1}^2 \end{cases} \tag{6.1}$$

- If $b_i = 0$, let

$$\begin{cases} \epsilon_i = 2\epsilon_{i-1} - \left(\epsilon_{i-1}^2 + 2\epsilon_{i-1}\lambda_{i-1}\right) \\ \lambda_i = 2\lambda_{i-1} - \lambda_{i-1}^2 \end{cases} \tag{6.2}$$

Then we have $I(W^{b_1 b_2 \cdots b_n}) = 2 - \epsilon_n - 2\lambda_n$ bits per channel use.

Consider the function $f : [0,1]^2 \to [0,1]^2$, $f(\epsilon, \lambda) = (\epsilon^2 + 2\epsilon\lambda, \lambda^2)$ corresponding to Equation (6.1). The fixed points of this function are given by $(0,1)$, $(1,0)$ and $(0,0)$. Similarly, consider the function $g : [0,1]^2 \to [0,1]^2$, $g(\epsilon, \lambda) = (2\epsilon - (\epsilon^2 + 2\epsilon\lambda), 2\lambda - \lambda^2)$ corresponding to Equation (6.2). It turns out that the fixed points of $g$ are the same as those of $f$. This suggests that in the limit, the transformed channels converge to one of three extreme cases discussed above. Figures 6.2 and 6.3 show that it is indeed the case and depict the three level polarization of the mutual information process $I(W^{b_1 b_2 \cdots b_n})$ to a discrete random variable $I^\infty$ as $n$ grows.

When $N = 2^n$ is large, let $N_0$ be the number of useless channels (corresponding to the width of the first step in Figure 6.3), $N_1$ be the number of partially perfect

channels (corresponding to the width of the second step in Figure 6.3) and $N_2$ be the number of perfect channels (corresponding to the width of the third step in Figure 6.3). Since the mutual information process is a martingale, it follows that

$$C = \mathbb{E}\{I^{\infty}\} \approx \frac{N_0}{N} \times 0 + \frac{N_1}{N} \times 1 + \frac{N_2}{N} \times 2$$

where $C$ is the symmetric capacity of the channel. Consider the following encoding rule: For indices corresponding to useless channels, let the input symbol take values from $\{0\}$ (from the transversal of the subgroup $\mathbb{Z}_4$ of $\mathbb{Z}_4$ i.e. fix the input). For indices corresponding to partially perfect channels, let the input symbol take values from $\{0, 1\}$ (from the transversal of the subgroup $\{0, 2\}$ of $\mathbb{Z}_4$). For indices corresponding to perfect channels, let the input symbol take values from $\mathbb{Z}_4$ (choose information symbols from the transversal of the subgroup $\{0\}$ of $\mathbb{Z}_4$). It turns out that this encoding rule used with an appropriate decoding rule has a vanishingly small probability of error as $N$ becomes large. The rate of this code is equal to

$$R = \frac{1}{N} \left( N_0 \log_2 1 + N_1 \log_2 2 + N_2 \log_2 4 \right)$$

This means $R = C$ is achievable using polar codes.

Next, we consider a channel with a composite input alphabet size. Consider the channel depicted in Figure 6.4. We call this Channel 2. It turns out that given a sequence of bits $b_1 b_2 \cdots b_n$, the transformed channel $W^{b_1 b_2 \cdots b_n}$ is (equivalent to) a channel of the same type as Channel 2 but with possibly different parameters $\epsilon, \lambda$ and $\gamma$. At each step $n$, the corresponding parameters can be found using the following recursion: Define $\epsilon_0 = \epsilon$, $\lambda_0 = \lambda$ and $\gamma_0 = \gamma$. For $i = 1, \cdots, n$,

- If $b_i = 1$, let

$$\begin{cases} \gamma_i = \gamma_{i-1}^2 + 2\gamma_{i-1}\epsilon_{i-1} + 2\gamma_{i-1}\lambda_{i-1} \\ \epsilon_i = \epsilon_{i-1}^2 + 2\gamma_{i-1}\epsilon_{i-1} + 2\epsilon_{i-1}\lambda_{i-1} \\ \lambda_i = \lambda_{i-1}^2 - 2\gamma_{i-1}\epsilon_{i-1} \end{cases} \tag{6.3}$$

- If $b_i = 0$, let

$$\begin{cases} \gamma_i = 2\gamma_{i-1} - \left(\gamma_{i-1}^2 + 2\gamma_{i-1}\epsilon_{i-1} + 2\gamma_{i-1}\lambda_{i-1}\right) \\ \epsilon_i = 2\epsilon_{i-1} - \left(\epsilon_{i-1}^2 + 2\gamma_{i-1}\epsilon_{i-1} + 2\epsilon_{i-1}\lambda_{i-1}\right) \\ \lambda_i = 2\lambda_{i-1} + 2\gamma_{i-1}\epsilon_{i-1} - \left(\lambda_{i-1}^2\right) \end{cases} \tag{6.4}$$

Then we have

$$I(W^{b_1 b_2 \cdots b_n}) = \log_2 6 - \gamma_n \log_2 2 - \epsilon_n \log_2 3 - \lambda_n \log_2 6$$

The proof of the recursion formulas for Channel 2 is similar to that of Channel 1 and is omitted. The fixed points of the functions corresponding to Equations (6.3) and (6.4) are given by $(0,0,0)$, $(1,0,0)$, $(0,1,0)$, $(0,0,1)$, $(-1,0,1)$, $(0,-1,1)$, $(1,1,-1)$, and $(-1,-1,2)$, out of which $(0,0,0)$, $(1,0,0)$, $(0,1,0)$ and $(0,0,1)$ are admissible. Note that $(0,0,0)$ corresponds to a perfect channel with a capacity of $\log_2 6$ bits per channel use, $(1,0,0)$ corresponds to a partially perfect channel which can perfectly send the index of the coset of the subgroup $\{0,3\}$ to which the input belongs and has a capacity of $\log_2 3$ bits per channel use, $(0,1,0)$ corresponds to a partially perfect channel which can perfectly send the index of the coset of the subgroup $\{0,2,4\}$ to which the input belongs and has a capacity of $\log_2 2$ bits per channel use, and $(0,0,1)$ corresponds to a useless channel. This suggests that in the limit, the transformed channels converge to one of these four extreme cases. This can be confirmed using the recursion formulas for this channel as depicted in Figures 6.5 and 6.6. With encoding and decoding rules similar to those of Channel 1, we can show that polar codes achieve the symmetric capacity of this channel.

In the next section, we show that polar codes achieve the symmetric capacity of channels with input alphabet size equal to a power of a prime.

### 6.1.3 Polar Codes Over Channels with input $\mathbb{Z}_{p^r}$

In this section, we consider channels of input alphabet size $q = p^r$ for some prime number $p$ and a positive integer $r$. In this case, the input alphabet of the channel can

be considered as a ring with addition and multiplication modulo $p^r$. We prove the achievability of the symmetric capacity of these channels using polar codes and later in Section 6.1.4 we will generalize this result to channels of arbitrary input alphabet sizes and arbitrary group operations.

#### 6.1.3.1 $\mathbb{Z}_{p^r}$ Rings

Let $\mathbf{G} = \mathbb{Z}_{p^r} = \{0, 1, 2, \cdots, p^r - 1\}$ with addition and multiplication modulo $p^r$ be the input alphabet of the channel, where $p$ is a prime and $r$ is an integer. For $t = 0, 1, \cdots, r$, define the subgroup $H_t$ of $\mathbf{G}$ as the set:

$$H_t = p^t \mathbf{G} = \{0, p^t, 2p^t, \cdots, (p^{r-t} - 1)p^t\}$$

and define $H_{r+1} = \emptyset$. For $t = 0, 1, \cdots, r$, define the subset $K_t$ of $\mathbf{G}$ as $K_t = H_t \backslash H_{t+1}$; i.e. $K_t$ is defined as the set of elements of $\mathbf{G}$ which are a multiple of $p^t$ but are not a multiple of $p^{t+1}$. Note that $K_0$ is the set of all invertible elements (i.e. set of all elements with a multiplicative inverse) of $\mathbf{G}$ and $K_r = \{0\}$. Let $T_t$ be a transversal of $H_t$ in $\mathbf{G}$; i.e. a subset of $\mathbf{G}$ containing one and only one element from each coset of $H_t$ in $\mathbf{G}$. One valid choice for $T_t$ is $\{0, 1, \cdots, p^t - 1\}$. Note that given $H_t$ and $T_t$, each element $g$ of $\mathbf{G}$ can be represented uniquely as a sum $g = \widehat{g} + \widetilde{g}$ where $\widehat{g} \in T_t$ and $\widetilde{g} \in H_t$.

#### 6.1.3.2 Recursive Channel Transformation

It has been shown in [10] that the error probability of polar codes over binary input channels is upper bounded by the sum of Bhattacharyya parameters of certain channels defined by a recursive channel transformation. Hence, the study of these channels is essential to show that polar codes achieve the symmetric capacity of channels. A similar set of synthesized channels appear for polar codes over channels

with arbitrary input alphabet sizes. The channel transformations are given by:

$$W^{-}(y_1, y_2|u_1) = \sum_{u_2' \in \mathbf{G}} \frac{1}{q} W(y_1|u_1 + u_2')W(y_2|u_2') \tag{6.5}$$

$$W^{+}(y_1, y_2, u_1|u_2) = \frac{1}{q} W(y_1|u_1 + u_2)W(y_2|u_2) \tag{6.6}$$

for $y_1, y_2 \in \mathscr{Y}$ and $u_1, u_2 \in \mathbf{G}$. Repeating these operations $n$ times recursively, we obtain $N = 2^n$ channels $W_N^{(1)}, \cdots, W_N^{(N)}$. For $i = 1, \cdots, N$, these channels are given by:

$$W_N^{(i)}(y_1^N, u_1^{i-1}|u_i) = \sum_{u_{i+1}^N \in \mathbf{G}^{N-i}} \frac{1}{q^{N-1}} W^N(y_1^N|u_1^N G_N)$$

where $G_N$ is the generator matrix for polar codes.

For the case of binary input channels, it has been shown in [10] that as $N \to \infty$, these channels polarize in the sense that their Bhattacharyya parameters approaches either zero (perfect channels) or one (useless channels). In the next part, we formally state the following multilevel polarization result: In general, when the input alphabet is a prime power, polarization happens in multiple levels so that as $N \to \infty$, these channels become useless, perfect or "partially perfect".

#### 6.1.3.3 The Multilevel Polarization Result

In this section, we state the multilevel polarization result for the $\mathbb{Z}_{p^r}$ case and we prove it in the subsequent section. First, we define some quantities which are used in the statement and the proof of multilevel polarization. For an integer $n$, let $J_n$ be a uniform random variable over the set $\{1, 2, \cdots, N = 2^n\}$.

**1)** Define the random variable $I^n(W)$ as

$$I^n(W) = I(X; Y) \tag{6.7}$$

where $X$ and $Y$ are the input and the output of $W_N^{(J_n)}$ respectively and $X$ is uniformly distributed. It has been shown in [10] that the process $I^0, I^1, I^2, \cdots$ is a martingale

for the binary case. The same proof is valid for the general case as well. Hence $\mathbb{E}\{I^n\} = I^0$.

**2)** For an integer $n$ and for $d \in \mathbf{G}$, define the random variable $Z_d^n(W) = Z_d(W_N^{(J_n)})$ where for a channel $(\mathbf{G}, \mathscr{Y}, W)$,

$$\begin{aligned} Z_d(W) &= \frac{1}{q} \sum_{x \in \mathbf{G}} \sum_{y \in \mathscr{Y}} \sqrt{W(y|x)W(y|x+d)} \\ &= \frac{1}{q} \sum_{x \in \mathbf{G}} Z(W_{\{x,x+d\}}) \end{aligned} \tag{6.8}$$

Note that similar to the Bhattacharyya parameter, $Z_d(W)$ takes values from $[0, 1]$. In the extreme case when $Z_d(W)$ is zero, for any $x \in \mathbf{G}$, the channel can completely distinguish between $x$ and $x + d$. On the other hand, when $Z_d(W)$ is one, for any $x \in \mathbf{G}$, the two input symbols $x$ and $x + d$ are equilikely given any channel output.

**3)** Let $H$ be an arbitrary subgroup of $\mathbf{G}$. Note that any uniform random variable defined over $\mathbf{G}$ can be decomposed into two uniform and independent random variables $\widehat{X}$ and $\widetilde{X}$ where $\widehat{X}$ takes values from the transversal $T$ of $H$ and $\widetilde{X}$ takes values from $H$. For an integer $n$, define the random variable $I_H^n(W)$ as

$$I_H^n(W) = I(X; Y|\widehat{X}) = I(\widetilde{X}; Y|\widehat{X}) \tag{6.9}$$

where $X$ and $Y$ are the input and the output of $W_N^{(J_n)}$ respectively. These processes along with $Z_d^n(W)$ processes are used to show the convergence of the mutual information process to a discrete random variable.

**4)** For $t = 0, \cdots, r$, define the random variable $Z^t(W_N^{(i)}) = \sum_{d \notin H_t} Z_d(W_N^{(i)})$ and the random process $(Z^t)^{(n)}(W) = Z^t(W_N^{(J_n)})$ where $J_n$ is a uniform random variable over $\{1, 2, \cdots, N = 2^n\}$. We will see later that these processes are related to the probability of error incurred by polar codes.

The following theorem states the multilevel polarization result for the $\mathbb{Z}_{p^r}$ case:

**Theorem VI.1.** *For all $\epsilon > 0$ and $\beta < \frac{1}{2}$, there exists a number $N = N(\epsilon) = 2^{n(\epsilon)}$ and disjoint subsets $A_0^\epsilon, A_1^\epsilon, \cdots, A_r^\epsilon$ of $\{1, \cdots, N\}$ such that for $t = 0, \cdots, r$ and $i \in A_t^\epsilon$, $\left| I(W_N^{(i)}) - t \log_2 p \right| \leq \epsilon$ and $Z^t(W_N^{(i)}) < 2^{-2^{\beta n(\epsilon)}}$. Moreover, as $\epsilon \to 0$, $\frac{|A_t^\epsilon|}{N} \to p_t$ for some probabilities $p_0, \cdots, p_r$ adding up to one.*

#### 6.1.3.4 Proof of Multilevel Polarization

In this section, we prove the multilevel polarization through a series of lemmas. In the first lemma, we show that $I_H^n(W)$ is a super-martingale.

**Lemma VI.2.** *For an arbitrary group $\mathbf{G}$ and for any subgroup $H$ of $\mathbf{G}$, the random process $I_H^n(W)$ defined by Equation (6.9) is a super-martingale.*

*Proof.* Define the channels $W^-$ and $W^+$ as in (6.32) and (6.33). Define the random variables $U_1$, $U_2$, $X_1$, $X_2$, $Y_1$ and $Y_2$ where $U_1$ and $U_2$ are uniformly distributed over $\mathbf{G}$, $X_1 = U_1 + U_2$ where addition is the group operation, $X_2 = U_2$ and $Y_1$ (respectively $Y_2$) is the channel output when the input is $X_1$ (respectively $X_2$). Decompose the random variable $U_1$ into two uniform and independent random variables $\widehat{U}_1$ and $\widetilde{U}_1$ where $\widehat{U}_1$ takes values from the transversal $T$ of $H$ and $\widetilde{U}_1$ takes values from $H$. Similarly define, $\widehat{U}_2, \widehat{X}_1, \widehat{X}_2$ and $\widetilde{U}_2, \widetilde{X}_1, \widetilde{X}_2$. We need to show that

$$I(\widetilde{U}_1; Y_1 Y_2 | \widehat{U}_1) + I(\widetilde{U}_2; Y_1 Y_2 U_1 | \widehat{U}_2) \leq 2 I(\widetilde{X}_1; Y_1 | \widehat{X}_1)$$

Note that $I(\widetilde{X}_1; Y_1 | \widehat{X}_1) = I(X_1; Y_1) - I(\widehat{X}_1; Y_1)$. Since $I^n$ is a martingale, we have

$$I(U_1; Y_1 Y_2) + I(U_2; Y_1 Y_2 U_1) = 2 I(X; Y)$$

Therefore, it suffices to show

$$I(\widehat{U}_1; Y_1 Y_2) + I(\widehat{U}_2; Y_1 Y_2 U_1) \geq 2 I(\widehat{X}_1; Y_1)$$

We have

$$\begin{aligned} I(\widehat{U}_2; Y_1 Y_2 U_1) &= I(\widehat{U}_2; Y_1 Y_2 \widehat{U}_1 \widetilde{U}_1) \\ &= I(\widehat{U}_2; Y_1 Y_2 \widehat{U}_1) + I(\widehat{U}_2; \widetilde{U}_1 | Y_1 Y_2 \widehat{U}_1) \\ &\geq I(\widehat{U}_2; Y_1 Y_2 \widehat{U}_1) \end{aligned}$$

Hence,

$$\begin{aligned} I(\widehat{U}_1; Y_1 Y_2) + I(\widehat{U}_2; Y_1 Y_2 U_1) &\geq I(\widehat{U}_1; Y_1 Y_2) + I(\widehat{U}_2; Y_1 Y_2 \widehat{U}_1) \\ &= I(\widehat{U}_1 \widehat{U}_2; Y_1 Y_2) \\ &\overset{(a)}{=} I(\widehat{X}_1 \widehat{X}_2; Y_1 Y_2) = 2I(\widehat{X}_1; Y_1) \end{aligned}$$

where $(a)$ follows since $\widehat{U}_1$ and $\widehat{U}_2$ are recoverable from $\widehat{X}_1$ and $\widehat{X}_2$ and vice versa as shown in the following: To show the forward direction, let $U_1'$ and $U_2'$ take values from $\mathbf{G}$ and let $X_1' = U_1' + U_2'$ and $X_2' = U_2'$. We need to show that if $X_1'$ is in the same coset of $H$ as $X_1$ (i.e. if $X_1' - X_1 \in H$ or equivalently $\widehat{X}_1' = \widehat{X}_1$) and $X_2'$ is in the same coset of $H$ as $X_2$ (i.e. if $X_2' - X_2 \in H$ or equivalently $\widehat{X}_2' = \widehat{X}_2$), then $U_1'$ is in the same coset of $H$ as $U_1$ (i.e. $U_1' - U_1 \in H$ or equivalently $\widehat{U}_1' = \widehat{U}_1$) and $U_2'$ is in the same coset of $H$ as $U_2$ (i.e. $U_2' - U_2 \in H$ or equivalently $\widehat{U}_2' = \widehat{U}_2$). Note that $X_2' - X_2 \in H$ implies $U_2' - U_2 \in H$ and $X_1' - X_1 \in H$ implies $U_1' + U_2' - U_1 - U_2 \in H$. Since $U_2' - U_2 \in H$ (and hence $U_2 - U_2' \in H$), $U_1' - U_1 \in H + U_2 - U_2'$ implies $U_1' - U_1 \in H$. For the other direction, note that $\widehat{X}_1 = T \cap \left( \widehat{U}_1 + \widehat{U}_2 + H \right)$ and $\widehat{X}_2 = \widehat{U}_2$. $\square$

The next lemma is a restatement of Lemma 2 of [66] with a slight generalization:

**Lemma VI.3.** *Suppose $B_n$, $n \in \mathbb{Z}^+$ is a $\{-,+\}$-valued process with $P(B_n = -) = P(B_n = +) = \frac{1}{2}$. Suppose $I_n$ and $T_n$ are two processes adapted to the process $B_n$ satisfying the following conditions*

1. *$I_n$ takes values in the interval $[0,1]$.*

2. *$I_n$ converges almost surely to a random variable $I_\infty$.*

*3.* $T_n$ *takes values in the interval* $[0,1]$.

*4.* $T_{n+1} = T_n^2$ *when* $B_{n+1} = +$.

*5. For all* $\epsilon > 0$*, there exists* $\delta > 0$ *such that for* $n \in \mathbb{Z}^+$, $T_n \leq \delta$ *implies* $I_n \geq 1-\epsilon$.

*6. For all* $\epsilon > 0$*, there exists* $\delta > 0$ *such that for* $n \in \mathbb{Z}^+$, $T_n \geq 1-\delta$ *implies* $I_n \leq \epsilon$.

*Then* $T_\infty = \lim_{n\to\infty} T_n$ *exists with probability* 1 *and* $I_\infty, T_\infty$ *both take values in* $\{0,1\}$.

*Proof.* The proof follows from Lemma 2 of [66] in a straightforward fashion. □

In the next lemma, we show that for any $d \in \mathbf{G}$, the random process $Z_d^n$ converges to a Bernoulli random variable.

**Lemma VI.4.** *For all* $d \in \mathbf{G}$, $Z_d^n(W)$ *converges almost surely to a* $\{0,1\}$*-valued random variable* $Z_d^\infty(W)$ *as* $n$ *grows. Moreover, if* $\tilde{d} \in \mathbf{G}$ *is such that* $\langle \tilde{d} \rangle = \langle d \rangle$ *then* $Z_{\tilde{d}}^\infty(W) = Z_d^\infty(W)$ *almost surely; i.e. the random processes* $Z_{\tilde{d}}^n(W)$ *and* $Z_d^n(W)$ *converge to the same random variable.*

*Proof.* Let $H = \langle d \rangle$ be the subgroup of $\mathbf{G}$ generated by $d$ and let $M$ be a maximal subgroup of $H$. Let

$$d' = \operatorname*{argmax}_{\substack{a \in H \\ a \notin M}} Z_a(W) \tag{6.10}$$

In Lemma VI.3, let $I^n$ (Here we use the notation $I^n$ instead of $I_n$ for notational convenience) be equal to the process $I_H^n(W) - I_M^n(W)$ where $I_H^n(W)$ and $I_M^n(W)$ are defined by Equation (6.9) and let $T_n$ be equal to the process $Z_{d'}^n(W)$ defined in (6.8). We claim that $I^n$ and $T_n$ satisfy the conditions of Lemma VI.3. The proof is given in the following:

Recall that a uniform random variable $X$ over $\mathbf{G}$ can be decomposed into two uniform and independent random variables $\widetilde{X}$ taking values from $H$ and $\widehat{X}$ taking values from

the transversal of $H$ in $\mathbf{G}$. Similarly, the uniform random variable $\widetilde{X}$ over $H$ can be decomposed into two uniform and independent random variables $\widetilde{\widetilde{X}}$ taking values from $M \leq H$ and $\widehat{\widetilde{X}}$ taking values from the transversal of $M$ in $H$. Using the chain rule, we have:

$$\begin{aligned} I(\widetilde{X}; Y|\widehat{X}) &= I(\widetilde{\widetilde{X}}\widehat{\widetilde{X}}; Y|\widehat{X}) \\ &= I(\widehat{\widetilde{X}}; Y|\widehat{X}) + I(\widetilde{\widetilde{X}}; Y|\widehat{X}\widehat{\widetilde{X}}) \end{aligned}$$

Note that $\widetilde{\widetilde{X}} \in M$ and $(\widehat{X}, \widehat{\widetilde{X}})$ indicate the coset of $M$ in $\mathbf{G}$ to which $X$ belongs. Therefore, the equation above implies that for each $n$, $I_H^n(W) - I_M^n(W) = I(\widehat{\widetilde{X}}; Y|\widehat{X})$ where $X$ and $Y$ are the input and the output of the channel $W_N^{(J_n)}$. Note that $\widehat{\widetilde{X}}$ takes values from cosets of $M$ in $H$ and $\widehat{X}$ takes values from cosets of $H$ in $\mathbf{G}$. Therefore, $I(\widehat{\widetilde{X}}; Y|\widehat{X})$ is the mutual information between the coset of $M$ in $H$ to which $X$ belongs and $Y$ given the coset of $H$ in $\mathbf{G}$ to which $X$ belongs. Since $\widehat{\widetilde{X}}$ can at most take $\frac{|H|}{|M|}$ values, by choosing the base of the log function to be equal to $\frac{|H|}{|M|}$ condition (1) of Lemma VI.3 is satisfied.

We have shown in Lemma VI.2 that both processes $I_H^n(W)$ and $I_M^n(W)$ are supermartingales and hence both converge almost surely. This means that the vector valued random process $(I_H^n(W), I_M^n(W))$ converges almost surely (refer to Proposition 5.25 of [37]). Hence condition (2) is satisfied.

Condition (3) trivially holds and condition (4) is shown in Lemma VI.16 in Appendix 6.1.6.3.

To show (5), assume $Z_{d'}^n(W) \leq \delta$ for some $\delta > 0$ to be determined later. Let $T_H$ be a transversal of $H$ in $\mathbf{G}$ and let $T_M$ be a transversal of $M$ in $H$. Given $X \in t_H + H$ for some $t_H \in T_H$, the joint probability distribution of cosets of $M$ in $t_H + H$ and the

channel output is given by:

$$\begin{aligned}\bar{p}(t_H+t_M+M,y) &\triangleq \sum_{m\in M} P(X=t_H+t_M+m, Y=y|X\in t_H+H)\\ &= \sum_{m\in M}\frac{P(X=t_H+t_M+m,Y=y)}{P(X\in t_H+H)}\\ &= \sum_{m\in M}\frac{P(X=t_H+t_M+m,Y=y)}{|H|/|\mathbf{G}|}\\ &= \frac{|\mathbf{G}|}{|H|}\sum_{m\in M}\frac{1}{|\mathbf{G}|}W(y|t_H+t_M+m)\\ &= \frac{1}{|H|}\sum_{m\in M}W(y|t_H+t_M+m)\end{aligned}$$

where $t_M$ takes values from $T_M$. The corresponding channel is defined as:

$$\begin{aligned}\bar{W}(y|t_H+t_M+M) &= \frac{\frac{1}{|H|}\sum_{m\in M}W(y|t_H+t_M+m)}{P(X\in t_H+t_M+M|X\in t_H+H)}\\ &= \frac{1}{|M|}\sum_{m\in M}W(y|t_H+t_M+m)\end{aligned} \tag{6.11}$$

Note that the input of this channel takes values from the set $\{t_H+t_M+M|t_M\in T_M\}$ uniformly and the size of the input alphabet is $\bar{q}\triangleq\frac{|H|}{|M|}$ which is a prime (since $M$ is maximal in $H$). Furthermore, by definition $I(\bar{W})=I(\widehat{\widehat{X}};Y|\widehat{X}=t_H)$. It is shown in Appendix 6.1.6.4 that $Z_{d'}(W)\le\delta$ implies $Z(\bar{W})\le C\delta$ for a constant $C=\frac{|M|\cdot|H|\cdot|\mathbf{G}|}{|H|-|M|}$. Therefore, part (1) of Lemma VI.14 in Appendix 6.1.6.3 implies

$$I(\bar{W})\ge\log_{\bar{q}}\frac{\bar{q}}{1+C(\bar{q}-1)\delta}=\log_{\bar{q}}\frac{\bar{q}}{1+|H|\cdot|\mathbf{G}|\delta}$$

where the base of the logarithm in the calculation of the mutual information is set to be $\bar{q}$. This result is valid for all $t_H\in T_H$. Therefore

$$\begin{aligned}I_H(W)-I_M(W) &= \sum_{t_H\in T_H}P(\widehat{X}=t_H)I(\widehat{\widehat{X}};Y|\widehat{X}=t_H)\\ &\ge\log_{\bar{q}}\frac{\bar{q}}{1+|H|\cdot|\mathbf{G}|\delta}\end{aligned}$$

Hence, for any $\epsilon>0$, any choice of $0<\delta\le\frac{\bar{q}^{\epsilon}-1}{|H|\cdot|\mathbf{G}|}$ guarantees for $n\in\mathbb{Z}^+$, $Z_{d'}^n(W)\le\delta\Rightarrow I_H(W)-I_M(W)\ge 1-\epsilon$.

To show condition (6), assume that $Z^n_{d'}(W) \geq 1-\delta$. For the channel $\bar{W}$ defined as above, it is shown in Appendix 6.1.6.5 (An alternate proof for the $\mathbb{Z}_{p^r}$ case is provided in Appendix 6.1.6.6) that $Z_{d'}(W) \geq 1-\delta$ implies $Z_{d'+t_H+M}(\bar{W}) \geq 1-\frac{2q\sqrt{2\delta-\delta^2}}{\bar{q}|M|}$. Since the input alphabet of the channel $\bar{W}$ has a prime size and $d' \in H\backslash M$, we can use Lemma VI.15 in Appendix 6.1.6.3 to conclude that $Z(\bar{W}) > 1-\frac{2q\bar{q}^2\sqrt{2\delta-\delta^2}}{|M|}$ and therefore, $1-Z(\bar{W})^2 = (1+Z(\bar{W}))(1-Z(\bar{W})) \leq 2(1-Z(\bar{W})) \leq \frac{4q\bar{q}^2\sqrt{2\delta-\delta^2}}{|M|}$. Now we use part (2) of Lemma VI.14 in Appendix 6.1.6.3 to conclude

$$I(\bar{W}) \leq 2(\bar{q}-1)\log_{\bar{q}} e\sqrt{\frac{4q\bar{q}^2\sqrt{2\delta-\delta^2}}{|M|}} \leq C\sqrt[4]{\delta}$$

for a constant $C = 4\bar{q}(\bar{q}-1)\log_{\bar{q}} e\sqrt{\frac{q\sqrt{2}}{|M|}}$ where as above, the base of the logarithm in the calculation of the mutual information is set to be $\bar{q}$. This implies:

$$\begin{aligned} I_H(W) - I_M(W) &= \sum_{t_H \in T_H} P(\widehat{X} = t_H) I(\widehat{\widetilde{X}}; Y | \widehat{X} = t_H) \\ &\leq C\sqrt[4]{\delta} \end{aligned}$$

Hence, for any $\epsilon > 0$, any choice of $0 < \delta \leq \left(\frac{\epsilon}{C}\right)^4$ guarantees for $n \in \mathbb{Z}^+$, $Z^n_{d'}(W) \geq 1-\delta \Rightarrow I_H(W) - I_M(W) \leq \epsilon$.

So far, we have shown that for any $d \in \mathbf{G}$, for $H = \langle d \rangle$ and $d'$ defined as in (6.10), the random variable $Z^n_{d'}(W)$ converges to a Bernoulli random variable. Note that so far the proof is general and applies to arbitrary groups as well. We will use this part of the proof later in Section 6.1.4. Next, we show that when $\mathbf{G} = \mathbb{Z}_{p^r}$, for any $\tilde{d} \in H\backslash M$ (including $d$ itself), $Z^n_{\tilde{d}}(W)$ converges to a Bernoulli random variable. Moreover, using the fact that they all take values from $\{0,1\}$, we show that for all such $\tilde{d}$'s, they converge to the same random variable. To see this, note that if $Z^n_{d'} \leq \delta$, it follows that $Z^n_{\tilde{d}} \leq \delta$ for all $\tilde{d} \in H\backslash M$ (since by definition, $a = d'$ achieves the maximum of $Z_a(W)$ among all $a \in H\backslash M$) and if $Z^n_{d'} \geq 1-\delta$ it follows from Lemma VI.17 in

Appendix 6.1.6.3 that for all $\tilde{d} \in \langle d' \rangle = H$, $Z^n_{\tilde{d}} \geq 1 - q^3\delta$. Note that when $\mathbf{G} = \mathbb{Z}_{p^r}$, $H \backslash M$ is the set of all elements $\tilde{d}$ such that $\langle \tilde{d} \rangle = \langle d \rangle$. This completes the proof of the lemma. □

The next lemma gives a sufficient condition for two processes $Z^n_d$ and $Z^n_{\tilde{d}}$ to converge to the same random variable. Recall that for $0 \leq t \leq r-1$, $K_t = H_t \backslash H_{t+1}$.

**Lemma VI.5.** *If $d, \tilde{d} \in K_t$ for some $0 \leq t \leq r-1$, then $Z^n_d$ and $Z^n_{\tilde{d}}$ converge to the same Bernoulli random variable.*

*Proof.* Note that $d, \tilde{d} \in K_t$ implies $\langle d \rangle = \langle \tilde{d} \rangle = H_t$. Therefore, Lemma VI.4 implies $Z^n_d$ and $Z^n_{\tilde{d}}$ converge to the same Bernoulli random variable. □

For $t = 0, 1, \cdots, r-1$, pick an arbitrary element $k_t \in K_t$. The lemma above suggests that we only need to study $Z_{k_t}$'s rather than all $Z_d$'s.

**Lemma VI.6.** *For $t \leq s \leq r-1$, if $Z_{k_t} \geq 1 - \delta$ for some $k_t \in K_t$, then $Z_{k_s} \geq 1 - q^3\delta$ for all $k_s \in K_s$.*

*Proof.* Follows from Lemma VI.17 in Appendix 6.1.6.3 and the fact that $k_s \in \langle k_t \rangle$. □

This lemma implies that for the group $\mathbf{G} = \mathbb{Z}_{p^r}$ all possible asymptotic cases are:

- **Case 0:** $Z_{k_0} = 1, Z_{k_1} = 1, Z_{k_2} = 1, \cdots, Z_{k_{r-1}} = 1$
- **Case 1:** $Z_{k_0} = 0, Z_{k_1} = 1, Z_{k_2} = 1, \cdots, Z_{k_{r-1}} = 1$
- **Case 2:** $Z_{k_0} = 0, Z_{k_1} = 0, Z_{k_2} = 1, \cdots, Z_{k_{r-1}} = 1$

  $\vdots$

- **Case r:** $Z_{k_0} = 0, Z_{k_1} = 0, Z_{k_2} = 0, \cdots, Z_{k_{r-1}} = 0,$

where for $t = 0, \cdots, r$, case $t$ happens with some probability $p_t$. This implies $(Z^t)^{(n)}(W)$ converges to a random variable $(Z^t)^{(\infty)}(W)$ almost surely and $P\left((Z^t)^{(\infty)} = 0\right) = \sum_{s=t}^{r} p_s$.

Next, we study the behavior of $I^n$ in each of these asymptotic cases.

**Lemma VI.7.** *For a channel $(\mathbb{Z}_{p^r}, \mathscr{Y}, W)$, let $t$ be an integer taking values from $\{0, 1, \cdots, r\}$. For any $\epsilon > 0$, there exists a $\delta > 0$ such that if $Z_{k_0} \leq \delta, Z_{k_1} \leq \delta, \cdots, Z_{k_{t-1}} \leq \delta, Z_{k_t} \geq 1-\delta, \cdots, Z_{k_{r-1}} \geq 1-\delta$ for all $k_s \in K_s$ $(s = 0, \cdots, r-1)$, then $t \log_2 p - \epsilon \leq I^0(W) \leq t \log_2 p + \epsilon$.*

*Proof.* Note that for all $s = 0, \cdots, r-1$, $M_s \triangleq \langle k_{s+1} \rangle$ is a maximal subgroup of $\langle k_s \rangle$. In the proof of Lemma VI.4, if we let $d = k_0$ and $M_0 = \langle k_1 \rangle$, the choice of $\delta = \frac{p^{\epsilon/\log_2 q}-1}{|H| \cdot |\mathbf{G}|}$ guarantees that $(1 - \epsilon/\log_2 q) \log_2 p \leq I_{\mathbf{G}}(W) - I_{M_0}(W) = I(W) - I_{M_0}(W) \leq \log_2 p$ (in bits). Similarly, it follows that $(1-\epsilon/\log_2 q) \log_2 p \leq I_{M_s}(W) - I_{M_{s+1}}(W) \leq \log_2 p$ for all $0 \leq s \leq t-1$. For $s \geq t$, the choice of $\delta = \left(\frac{\epsilon}{C \log_2 q}\right)^4$ guarantees $I_{M_s} - I_{M_{s+1}} \leq (\epsilon/\log_2 q) \log_2 p = \epsilon/r$ (in bits). Therefore,

$$\begin{aligned} I^0(W) = I_{\mathbf{G}}(W) &= \sum_{s=0}^{r-1} \big(I_{M_s}(W) - I_{M_{s+1}}(W)\big) \\ &= \sum_{s=0}^{t-1} \big(I_{M_s}(W) - I_{M_{s+1}}(W)\big) + \\ &\qquad \sum_{s=t}^{r-1} \big(I_{M_s}(W) - I_{M_{s+1}}(W)\big) \\ &\leq \sum_{s=0}^{t-1} \log_2 p + \sum_{s=t}^{r-1} \epsilon/r \\ &\leq t \log_2 p + \epsilon \end{aligned}$$

and

$$\begin{aligned} I^0(W) = I_{\mathbf{G}}(W) &= \sum_{s=0}^{t-1} \big(I_{M_s}(W) - I_{M_{s+1}}(W)\big) + \\ &\qquad \sum_{s=t}^{r-1} \big(I_{M_s}(W) - I_{M_{s+1}}(W)\big) \\ &\geq \sum_{s=0}^{t-1} (1 - \epsilon/\log_2 q) \log_2 p \\ &\geq t \log_2 p - \epsilon \end{aligned}$$

□

We have shown that the process $I^n$ converges to the following $r+1$ valued discrete random variable: $I^\infty = t \log_2 p$ with probability $p_t$ for $t = 0, \cdots, r$.

We are now ready to prove the theorem: For the channel $(\mathbb{Z}_{p^r}, \mathscr{Y}, W)$, consider the vector random process $\mathbf{V}^n = (Z^n_{k_0}, Z^n_{k_1}, \cdots, Z^n_{k_{r-1}}, I^n)$. We have seen in the previous section that each component of this vector random process converges almost surely. Proposition 5.25 of [37] implies that the vector random process $\mathbf{V}^n$ also converges almost surely to a random vector $\mathbf{V}^\infty$. The random vector $\mathbf{V}^\infty$ is a discrete random variable defined as follows:

$$P\left(\mathbf{V}^\infty = (\overbrace{0, \cdots, 0}^{t \text{ times}}, \overbrace{1, \cdots, 1}^{r-t \text{ times}}, t \log_2 p)\right) = p_t$$

for $t = 0, 1, \cdots, r$ where $p_t$'s are some probabilities. This implies that for all $\delta > 0$, there exists a number $N = N(\delta) = 2^{n(\delta)}$ and disjoint subsets $A^\delta_0, A^\delta_1, \cdots, A^\delta_r$ of $\{1, \cdots, N\}$ such that for $t = 0, \cdots, r$ and $i \in A^\delta_t$, $Z_{k_s}(W^{(i)}_N) \leq \delta$ if $0 \leq s < t$ and $Z_{k_s}(W^{(i)}_N) \geq 1 - \delta$ if $t \leq s < r$. This implies if $i \in A^\delta_t$ then $Z^t(W^{(i)}_N) \leq q\delta$. Moreover, as $\delta \to 0$, $\frac{|A^\delta_t|}{N} \to p_t$ for some probabilities $p_0, \cdots, p_r$ adding up to one.

For $\epsilon > 0$, let $\delta$ be as in Lemma VI.7. Then, for $t = 0, \cdots, r$ and $i \in A^\delta_t$, we have $\left| I(W^{(i)}_N) - t \log_2 p \right| \leq \epsilon$. Similarly, for $\epsilon > 0$ if we let $\delta = \epsilon/q$, we get $Z^t(W^{(i)}_N) \leq \epsilon$. For any $\epsilon > 0$, taking the minimum of the two $\delta$'s guarantees the existence of a number $N = N(\epsilon) = 2^{n(\epsilon)}$ and disjoint subsets $A^\epsilon_0, A^\epsilon_1, \cdots, A^\epsilon_r$ of $\{1, \cdots, N\}$ such that for $t = 0, \cdots, r$ and $i \in A^\epsilon_t$, $\left| I(W^{(i)}_N) - t \log_2 p \right| \leq \epsilon$ and $Z^t(W^{(i)}_N) < \epsilon$. Finally, in Appendix 6.1.6.7, we show that for any $\beta < \frac{1}{2}$ and for $t = 0, \cdots, r$,

$$\begin{aligned} \lim_{n \to \infty} P\left((Z^t)^{(n)} < 2^{-2^{\beta n}}\right) &\geq P\left((Z^t)^{(\infty)} = 0\right) \\ &= \sum_{s=t}^{r} p_s \end{aligned} \tag{6.12}$$

This rate of polarization result concludes the proof of Theorem VI.1.

#### 6.1.3.5 Encoding and Decoding

In the original construction of polar codes, we fix the input symbols corresponding to useless channels and send information symbols over perfect channels. Here, since the channels do not polarize into two levels, the encoding is slightly different and we send "some" information bits over "partially perfect" channels. At the encoder, if $i \in A_t^\epsilon$ for some $t = 0, \cdots, r$, the information symbol is chosen from the transversal $T_t$ uniformly and not from the whole set $\mathbf{G}$. As we will see later, the channel $W_N^{(i)}$ is perfect for symbols chosen from $T_t$ and perfect decoding is possible at the decoder. Let $\mathscr{X}_N^\epsilon = \bigoplus_{t=0}^r T_t^{A_t^\epsilon}$ be the set of all valid input sequences. For the sake of analysis, as in the binary case, the message $u_1^N$ is dithered with a uniformly distributed random vector $b_1^N \in \bigoplus_{t=0}^r H_t^{A_t^\epsilon}$ revealed to both the encoder and the decoder. A message $v_1^N \in \mathscr{X}_N^\epsilon$ is encoded to the vector $x_1^N = (v_1^N + b_1^N)G_N$. Note that $u_1^N = v_1^N + b_1^N$ is uniformly distributed over $\mathbf{G}^N$.

At the decoder, after observing the output vector $y_1^N$, for $t = 0, \cdots, r$ and $i \in A_t^\epsilon$ , use the following decoding rule:

$$\hat{u}_i = f_i(y_1^N, \hat{u}_1^{i-1}) = \underset{g \in b_i + T_t}{\operatorname{argmax}} W_N^{(i)}(y_1^N, \hat{u}_1^{i-1} | g)$$

where the ties are broken arbitrarily. Finally, the message is decoded as $\hat{v}_1^N = \hat{u}_1^N - b_1^N$. The total number of valid input sequences is equal to

$$2^{NR} = \prod_{t=0}^{r} |T_t|^{|A_t|} = \prod_{t=0}^{r} p^{t|A_t|} \approx \prod_{t=0}^{r} p^{tp_t N}$$

Therefore, $R \approx \sum_{t=0}^r p_t t \log_2 p$. On the other hand, since $I^n$ is a martingale, we have $\mathbb{E}\{I^\infty\} = I^0$. Since $\mathbb{E}\{I^\infty\} = \sum_{t=0}^r p_t t \log_2 p$, we observe that the rate $R$ is equal to the symmetric capacity $I^0$. We will see in the next section that this rate is achievable.

#### 6.1.3.6 Error Analysis

In this section, we show that the error probability of polar codes approaches zero as the block length increases when the rate of transmission is equal to the symmetric capacity of the channel.

Let $B_i$ be the event that the first error occurs when the decoder decodes the $i$th symbol:

$$\begin{aligned} B_i = \big\{(u_1^N, y_1^N) \in \mathbf{G}^N \times \mathscr{Y}^N \,\big|\forall j < i, u_j = f_j(y_1^N, u_1^{j-1}), \\ u_i \neq f_i(y_1^N, u_1^{i-1})\big\} \\ \subseteq \big\{(u_1^N, y_1^N) \in \mathbf{G}^N \times \mathscr{Y}^N | u_i \neq f_i(y_1^N, u_1^{i-1})\big\} \end{aligned} \tag{6.13}$$

For $t = 0, \cdots, r$ and $i \in A_t^\epsilon$, define

$$\begin{aligned} E_i = \Big\{(u_1^N, y_1^N) \in \mathbf{G}^N \times \mathscr{Y}^N \,\Big|W_N^{(i)}(y_1^N, u_1^{i-1}|u_i) \leq \\ W_N^{(i)}(y_1^N, u_1^{i-1}|\tilde{u}_i) \text{ for some } \tilde{u}_i \in b_i + T_t, \tilde{u}_i \neq u_i\Big\} \end{aligned} \tag{6.14}$$

**Lemma VI.8.** *For $t = 0, \cdots, r$ and $i \in A_t^\epsilon$, $P(E_i) \leq q^2 Z^t(W_N^{(i)})$.*

*Proof.* For $u_i \in \mathbf{G}$, write $u_i = b_i(u_i) + v_i(u_i)$ where $b_i(u_i) \in H_t$ and $v_i(u_i) \in T_t$. We

have

$$
\begin{aligned}
P(E_i) &= \sum_{u_1^N, y_1^N} \frac{1}{q^N} W_N(y_1^N|u_1^N) \mathbb{1}_{E_i}(u_1^N, y_1^N) \\
&\leq \sum_{u_1^N, y_1^N} \frac{1}{q^N} W_N(y_1^N|u_1^N) \sum_{\substack{\tilde{u}_i \in b_i(u_i)+T_t \\ \tilde{u}_i \neq u_i}} \sqrt{\frac{W_N^{(i)}(y_1^N, u_1^{i-1}|\tilde{u}_i)}{W_N^{(i)}(y_1^N, u_1^{i-1}|u_i)}} \\
&= \sum_{u_1^i, y_1^N} \frac{1}{q} \left( \sum_{u_{i+1}^N} \frac{1}{q^{N-1}} W_N(y_1^N|u_1^N) \right) \\
&\qquad \sum_{\substack{\tilde{u}_i \in b_i(u_i)+T_t \\ \tilde{u}_i \neq u_i}} \sqrt{\frac{W_N^{(i)}(y_1^N, u_1^{i-1}|\tilde{u}_i)}{W_N^{(i)}(y_1^N, u_1^{i-1}|u_i)}} \\
&= \sum_{u_1^i, y_1^N} \frac{1}{q} W_N^{(i)}(y_1^N, u_1^{i-1}|u_i) \sum_{\substack{\tilde{u}_i \in b_i(u_i)+T_t \\ \tilde{u}_i \neq u_i}} \sqrt{\frac{W_N^{(i)}(y_1^N, u_1^{i-1}|\tilde{u}_i)}{W_N^{(i)}(y_1^N, u_1^{i-1}|u_i)}} \\
&= \sum_{\substack{u_i \in \mathbf{G} \\ \tilde{u}_i \in b_i(u_i)+T_t \\ \tilde{u}_i \neq u_i}} \frac{1}{q} \sum_{u_1^{i-1}, y_1^N} \sqrt{W_N^{(i)}(y_1^N, u_1^{i-1}|\tilde{u}_i) W_N^{(i)}(y_1^N, u_1^{i-1}|u_i)} \\
&= \sum_{\substack{u_i \in \mathbf{G} \\ \tilde{u}_i \in b_i(u_i)+T_t \\ \tilde{u}_i \neq u_i}} \frac{1}{q} Z_{\{u_i, \tilde{u}_i\}}(W_N^{(i)})
\end{aligned}
$$

For $u_i \in \mathbf{G}$ and $\tilde{u}_i \in b_i(u_i) + T_t$, if $u_i \neq \tilde{u}_i$, then $u_i, \tilde{u}_i$ are not in the same coset of $H_t$ and hence $u_i - \tilde{u}_i \notin H_t$. Therefore, $u_i - \tilde{u}_i \in \mathbf{G} \backslash H_t$. Note that for $d = u_i - \tilde{u}_i$, $Z_{\{u_i, \tilde{u}_i\}}(W_N^{(i)}) \leq q Z_d(W_N^{(i)})$. Since $d \in \mathbf{G} \backslash H_t$, we have $Z_d(W_N^{(i)}) \leq Z^t(W_N^{(i)})$ and hence,

$$Z_{\{u_i, \tilde{u}_i\}}(W_N^{(i)}) \leq q Z^t(W_N^{(i)})$$

Therefore, $P(E_i) \leq q|T_t| Z^t(W_N^{(i)}) \leq q^2 Z^t(W_N^{(i)})$. □

The probability of block error is given by $P(err) = \sum_{t=0}^{r} \sum_{i \in A_t^\epsilon} P(B_i)$. Since

$B_i \subseteq E_i$, we get

$$P(err) \leq \sum_{t=0}^{r} \sum_{i \in A_t^\epsilon} q^2 Z^t(W_N^{(i)}) \tag{6.15}$$

$$\overset{(a)}{\leq} \sum_{t=0}^{r} |A_t^\epsilon| q^2 2^{-2^{\beta n}} \tag{6.16}$$

$$\leq q^2 N 2^{-2^{\beta n}} \tag{6.17}$$

for any $\beta < \frac{1}{2}$ where $(a)$ follows from Theorem VI.1. Therefore, the probability of error goes to zero as $\epsilon \to 0$ (and hence $n \to \infty$).

### 6.1.4 Polar Codes Over Arbitrary Channels

For any channel input alphabet there always exist an Abelian group of the same size. In this section, we generalize the result of the previous section to channels of arbitrary input alphabet sizes and arbitrary group operations.

#### 6.1.4.1 Abelian Groups

Let the Abelian group $\mathbf{G}$ be the input alphabet of the channel. It is known that any Abelian group can be decomposed into a direct sum of $\mathbb{Z}_{p^r}$ rings [16]. Let $\mathbf{G} = \bigoplus_{l=1}^{L} \mathbf{R}_l$ with $\mathbf{R}_l = \mathbb{Z}_{p_l^{r_l}}$ where $p_l$'s are prime numbers and $r_l$'s are positive integers. For $t = (t_1, t_2, \cdots, t_L)$ with $t_l \in \{0, 1, \cdots, r_l\}$, there exists a corresponding subgroup $H$ of $\mathbf{G}$ defined by $H = \bigoplus_{l=1}^{L} p_l^{t_l} \mathbf{R}_l$. For a subgroup $H$ of $\mathbf{G}$ define $T_H$ to be a transversal of $H$ in $\mathbf{G}$.

#### 6.1.4.2 Recursive Channel Transformation

**The Basic Channel Transforms**

The transformed channels $W^+$ and $W^-$ and the process $I^n(W)$ are defined the same way as the $\mathbb{Z}_{p^r}$ case through Equations (6.32), (6.33) and (6.7).

**Asymptotic Behavior of Synthesized Channels**

For $d \in \mathbf{G}$, define $Z_d^n(W)$ similarly to (6.8) where $q = |\mathbf{G}|$ and for $H \leq \mathbf{G}$, define $I_H^n(W)$ by Equation (6.9). The following lemma is a restatement of Lemma VI.4. Here, we prove it for arbitrary groups.

**Lemma VI.9.** *For all $d \in \mathbf{G}$, $Z_d^n(W)$ converges almost surely to a $\{0,1\}$-valued random variable $Z_d^\infty(W)$ as $n$ grows. Moreover, if $\tilde{d} \in \mathbf{G}$ is such that $\langle \tilde{d} \rangle = \langle d \rangle$ then $Z_{\tilde{d}}^\infty(W) = Z_d^\infty(W)$ almost surely; i.e. the random processes $Z_{\tilde{d}}^n(W)$ and $Z_d^n(W)$ converge to the same random variable.*

*Proof.* Similarly to the proof of Lemma VI.4, let $H = \langle d \rangle$ and let $M$ be any maximal subgroup of $H$. Define

$$d' = \underset{\substack{a \in H \\ a \notin M}}{\operatorname{argmax}} Z_a(W) \tag{6.18}$$

It is relatively straightforward to show that in the general case as well, $Z_{d'}^n(W)$ converges to a $\{0,1\}$-valued random variable $Z_{d'}^\infty(W)$. Indeed this part of the proof of Lemma VI.4 is general enough for arbitrary Abelian groups. Here we show that this implies $Z_d^n(W)$ also converges to a Bernoulli random variable.

Let $|H| = \prod_{i=1}^k q_i^{a_i}$ where $q_i$'s are distinct primes and $a_i$'s are positive integers. Note that $H$ is isomorphic to the cyclic group $\mathbb{Z}_{|H|}$. For $i = 1, \cdots, k$, define the subgroup $M_i = \langle q_i \rangle$ of $\mathbb{Z}_{|H|}$ (and isomorphically of $H$) and let $d_i' = \underset{\substack{a \in H \\ a \notin M_i}}{\operatorname{argmax}} Z_a(W)$. Note that for $i = 1, \cdots, k$, $M_i$ is a maximal subgroup of $\mathbb{Z}_{|H|}$ (and isomorphically of $H$). Therefore, for $i = 1, \cdots, k$, $Z_{d_i'}^n(W)$ converges to a $\{0,1\}$-valued random variable. If for some $i = 1, \cdots, k$, $Z_{d_i'}(W) \leq \delta$ it follows that $Z_d(W) \leq \delta$ (since $d \in H \backslash M_i$) and if for all $i = 1, \cdots, k$, $Z_{d_i'}(W) \geq 1 - \delta$, it follows from Lemma VI.18 in Appendix 6.1.6.3 that $Z_{\tilde{d}}(W) \geq 1 - 2kq^3\delta$ for any $\tilde{d} \in \langle d_1', d_2', \cdots, d_k' \rangle$. Next, we show that $\langle d_1', d_2', \cdots, d_k' \rangle = H$ and this will prove that if for all $i = 1, \cdots, k$, $Z_{d_i'}(W) \geq 1 - \delta$

then $Z_d(W) \geq 1 - 2kq^3\delta$. For $i = 1, \cdots, k$, since $d'_i \notin M_i$ it follows that $d'_i \not\equiv 0 \pmod{q_i}$. Let

$$a = \sum_{i=1}^{k} \left( \prod_{\substack{j=1 \\ j \neq i}}^{k} q_j \right) d'_i$$

Then we have $a \not\equiv 0 \pmod{q_i}$ for all $i = 1, \cdots, k$. This implies $\langle a \rangle = H$ and hence $\langle d'_1, d'_2, \cdots, d'_k \rangle = H$. Therefore, if in the limit $Z_{d'_i}(W) = 0$ for some $i = 1, \cdots, k$ then $Z_d(W) = 0$ and if $Z_{d'_i}(W) = 0$ for all $i = 1, \cdots, k$ then $Z_d(W) = 1$. This proves that $Z_d^n(W)$ converges to a Bernoulli random variable.

If $\tilde{d} \in \mathbf{G}$ is such that $\langle \tilde{d} \rangle = \langle d \rangle$ then it follows that $\tilde{d} \in H$ and $\tilde{d} \notin M_i$ for $i = 1, \cdots, k$. Therefore if in the limit $Z_{d'_i}(W) = 0$ for some $i = 1, \cdots, k$ then $Z_{\tilde{d}}(W) = 0$ and if $Z_{d'_i}(W) = 1$ for all $i = 1, \cdots, k$ then $Z_{\tilde{d}}(W) = 1$. This proves that the random processes $Z_{\tilde{d}}^n(W)$ and $Z_d^n(W)$ converge to the same random variable. □

In the asymptotic regime, let $d_1, d_2, \cdots, d_m$ be all elements of $\mathbf{G}$ such that $Z_{d_i}(W) = 1$ and assume that for all other elements $d \in \mathbf{G}$, $Z_d(W) = 0$ (we can make this assumption since in the limit $Z_d$'s are $\{0, 1\}$-valued). It is shown in Lemma VI.18 in Appendix 6.1.6.3 that if $Z_{d_i}(W) = 1$ for $i = 1, \cdots, m$ then for any $\tilde{d} \in \langle d_1, d_2, \cdots, d_m \rangle$, $Z_{\tilde{d}}(W) = 1$. Therefore, $\langle d_1, d_2, \cdots, d_m \rangle \subseteq \{d_1, d_2, \cdots, d_m\}$ and hence we must have $\{d_1, d_2, \cdots, d_m\} = \langle d_1, d_2, \cdots, d_m \rangle = H$ for some subgroup $H$ of $\mathbf{G}$. This means all possible asymptotic cases can be indexed by subgroups of $\mathbf{G}$. i.e. for any $H \leq \mathbf{G}$, one possible asymptotic case is

- **Case $H$:** $Z_d(W) = \begin{cases} 1 & \text{if } d \in H; \\ 0 & \text{Otherwise.} \end{cases}$

where for $H \leq \mathbf{G}$, case $H$ happens with some probability $p_H$.

Next, We study the behavior of $I^n$ in each of these cases.

**Lemma VI.10.** *For a channel* $(\mathbf{G}, \mathscr{Y}, W)$ *let* $S$ *be a subgroup of* $\mathbf{G}$*. For any* $\epsilon > 0$ *there exists a* $\delta > 0$ *such that if* $Z_d \geq 1 - \delta$ *for* $d \in S$ *and* $Z_d \leq \delta$ *for* $d \notin S$*, then* $\log_2 \frac{|\mathbf{G}|}{|S|} - \epsilon \leq I^0(W) \leq \log_2 \frac{|\mathbf{G}|}{|S|} + \epsilon$*.*

*Proof.* Let $0 = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_{t-1} \subseteq S = M_t \subseteq M_{t+1} \subseteq \cdots \subseteq \mathbf{G} = M_k$ for some positive integer $k \leq \log_2 |\mathbf{G}|$ be any chain of subgroups such that $M_{s-1}$ is maximal in $M_s$ for $s = 1, \cdots, k$.

Fix some $s \in \{1, \cdots, t\}$ and let $H = M_s$ and $M = M_{s-1}$ and let $T_H$ be a transversal of $H$ in $\mathbf{G}$ and let $T_M$ be a transversal of $M$ in $H$. For $d \in H$, we have $Z_d(W) \geq 1 - \delta$. For $t_H \in T_H$ define the channel $\bar{W}(y|t_H + t_M + M_{s-1})$ similar to (6.11). We have shown in Appendix 6.1.6.5 that if for some $d \in H \backslash M$, $Z_d(W) \geq 1 - \delta$ then $Z_{d+t_H+M}(\bar{W}) \geq 1 - \frac{2q\sqrt{2\delta - \delta^2}}{\bar{q}|M|}$. Since the input alphabet of the channel $\bar{W}$ has a prime size (see Lemma VI.19 in Appendix 6.1.6.3), we can use Lemma VI.15 in Appendix 6.1.6.3 to conclude that $Z(\bar{W}) \geq 1 - \frac{2q\bar{q}^2\sqrt{2\delta - \delta^2}}{|M|}$. Now, similarly to the proof of Lemma VI.4, we use part (2) of Lemma VI.14 in Appendix 6.1.6.3 to conclude $I(\bar{W}) \leq C\sqrt[4]{\delta}$ for $C = 4\bar{q}(\bar{q} - 1)\log_2 e\sqrt{\frac{q\sqrt{2}}{|M|}}$. This result is valid for all $t_H \in T_H$. Since $I(\bar{W}) = I(\widehat{\widehat{X}}; Y|\widehat{X} = t_H)$, we conclude that

$$\begin{aligned} I_{M_s}(W) - I_{M_{s-1}}(W) &= I_H(W) - I_M(W) \\ &= \sum_{t_H \in T_H} P(\widehat{X} = t_H) I(\widehat{\widehat{X}}; Y|\widehat{X} = t_H) \\ &< C\sqrt[4]{\delta} \end{aligned}$$

Fix some $s \in \{t + 1, \cdots, k\}$ and let $H = M_s$ and $M = M_{s-1}$ and let $T_H$ be a transversal of $H$ in $\mathbf{G}$ and let $T_M$ be a transversal of $M$ in $H$. For $d \in H \backslash M$, we have $Z_d(W) \leq \delta$. For the channel $\bar{W}$ defined as above, we have shown in Appendix 6.1.6.4 that if for all $d \in H \backslash M$, $Z_d(W) \leq \delta$ then $Z(\bar{W}) \leq \frac{|M| \cdot |H| \cdot |\mathbf{G}|}{|H| - |M|}$. Therefore, part (1) of

Lemma VI.14 in Appendix 6.1.6.3 implies $I(\bar{W}) \geq \log_2 \frac{\bar{q}}{1+\cdot|H|\cdot|\mathbf{G}|\delta}$. We conclude that

$$\begin{aligned} I_{M_s}(W) - I_{M_{s-1}}(W) &= I_H(W) - I_M(W) \\ &= \log_2 \frac{\bar{q}}{1 + \cdot|H| \cdot |\mathbf{G}|\delta} \\ &\geq \log_2 \frac{|M_s|/|M_{s-1}|}{1 + |\mathbf{G}|^2\delta} \end{aligned}$$

Therefore,

$$\begin{aligned} I_{\mathbf{G}}(W) &= \sum_{s=1}^{t} \big(I_{M_s}(W) - I_{M_{s-1}}(W)\big) + \sum_{s=t+1}^{k} \big(I_{M_s}(W) - I_{M_{s-1}}(W)\big) \\ &\geq \sum_{s=t+1}^{k} I_{M_s}(W) - I_{M_{s-1}} \\ &\geq \sum_{s=t+1}^{k} \log_2 \frac{|M_s|/|M_{s-1}|}{1 + |\mathbf{G}|^2\delta} \\ &\geq \log_2 \frac{|\mathbf{G}|}{|S|} - k \log_2(1 + |\mathbf{G}|^2\delta) \end{aligned}$$

The choice of $0 < \delta \leq \frac{2^{\epsilon/k}-1}{|\mathbf{G}|^2}$ will guarantee that $I^0(W) \geq \log_2 \frac{|\mathbf{G}|}{|S|} - \epsilon$. Similarly,

$$\begin{aligned} I_{\mathbf{G}}(W) &= \sum_{s=1}^{t} \big(I_{M_s}(W) - I_{M_{s-1}}(W)\big) + \sum_{s=t+1}^{k} \big(I_{M_s}(W) - I_{M_{s-1}}(W)\big) \\ &\leq \sum_{s=1}^{t} C\sqrt[4]{\delta} + \sum_{s=t+1}^{k} \log_2 \frac{|M_s|}{|M_{s-1}|} \\ &\leq kC\sqrt[4]{\delta} + \log_2 \frac{|\mathbf{G}|}{|S|} \end{aligned}$$

The choice of $0 < \delta \leq \left(\frac{\epsilon}{kC}\right)^4$ will guarantee that $I^0(W) \leq \log_2 \frac{|\mathbf{G}|}{|S|} + \epsilon$. □

We have shown that the process $I^n$ converges to the following discrete random variable: $I^\infty = \log_2 \frac{|\mathbf{G}|}{|H|}$ with probability $p_H$ for $H \leq \mathbf{G}$.

For $H \leq \mathbf{G}$, define the random variable $Z^H(W_N^{(i)}) = \sum_{d \notin H} Z_d(W_N^{(i)})$ and the random process $(Z^H)^{(n)}(W) = Z^H(W_N^{(J_n)})$ where $J_n$ is a uniform random variable over $\{1, 2, \cdots, N = 2^n\}$. Note that $(Z^H)^{(n)}(W)$ converges almost surely to a random variable $(Z^H)^{(\infty)}(W)$ and $P\left((Z^H)^{(\infty)} = 0\right) = \sum_{S \leq H} p_S$.

**Summary of Channel Transformation**

For the channel $(\mathbf{G}, \mathscr{Y}, W)$, the convergence of the processes $I^n$ and $(Z^H)^n$ for $H \leq \mathbf{G}$ implies that for all $\epsilon > 0$, there exists a number $N = N(\epsilon)$ and a partition $\{A_H^\epsilon | H \leq \mathbf{G}\}$ of $\{1, \cdots, N\}$ such that for $H \leq \mathbf{G}$ and $i \in A_H^\epsilon$, $I(W_N^{(i)}) = \log_2 \frac{|\mathbf{G}|}{|H|} + O(\epsilon)$ and $Z^H(W_N^{(i)}) = O(\epsilon)$. Moreover, as $\epsilon \to 0$, $\frac{|A_H^\epsilon|}{N} \to p_H$ for some probabilities $p_H, H \leq \mathbf{G}$.

In Appendix 6.1.6.7, we show that for any $\beta < \frac{1}{2}$ and for $H \leq \mathbf{G}$,

$$\begin{aligned} \lim_{n\to\infty} P\left((Z^H)^{(n)} < 2^{-2^{\beta n}}\right) &\geq P\left((Z^H)^{(\infty)} = 0\right) \\ &= \sum_{S \leq H}^{r} p_S \end{aligned} \tag{6.19}$$

We have proved the following theorem:

**Theorem VI.11.** *For all $\epsilon > 0$, there exists a number $N = N(\epsilon) = 2^{n(\epsilon)}$ and a partition $\{A_H^\epsilon | H \leq \mathbf{G}\}$ of $\{1, \cdots, N\}$ such that for $H \leq \mathbf{G}$ and $i \in A_H^\epsilon$, $I(W_N^{(i)}) = \log_2 \frac{|\mathbf{G}|}{|H|} + O(\epsilon)$ and $Z^H(W_N^{(i)}) < 2^{-2^{\beta n(\epsilon)}}$. Moreover, as $\epsilon \to 0$, $\frac{|A_H^\epsilon|}{N} \to p_H$ for some probabilities $p_H, H \leq \mathbf{G}$.*

#### 6.1.4.3 Encoding and Decoding

At the encoder, if $i \in A_H^\epsilon$ for some $H \leq \mathbf{G}$, the information symbol is chosen from the transversal $T_H$ arbitrarily. Let $\mathscr{X}_N^\epsilon = \bigoplus_{H \leq \mathbf{G}} T_H^{A_H^\epsilon}$ be the set of all valid input sequences. As in the $\mathbb{Z}_{p^r}$ case, the message $u_1^N$ is dithered with a uniformly distributed random vector $b_1^N \in \bigoplus_{H \leq \mathbf{G}} H^{A_H^\epsilon}$ revealed to both the encoder and the decoder. A message $v_1^N \in \mathscr{X}_N^\epsilon$ is encoded to the vector $x_1^N = (v_1^N + b_1^N)G_N$. Note that $u_1^N = v_1^N + b_1^N$ is uniformly distributed over $\mathbf{G}^N$.

At the decoder, after observing the output vector $y_1^N$, for $H \leq \mathbf{G}$ and $i \in A_H^\epsilon$ , use the following decoding rule:

$$\hat{u}_i = f_i(y_1^N, \hat{u}_1^{i-1}) = \underset{g \in b_i + T_H}{\operatorname{argmax}} W_N^{(i)}(y_1^N, \hat{u}_1^{i-1} | g)$$

where the ties are broken arbitrarily. Finally, the message is recovered as $\hat{v}_1^N = \hat{u}_1^N - b_1^N$.

The total number of valid input sequences is equal to

$$2^{NR} = \prod_{H \leq \mathbf{G}} |T_H|^{|A_H|} \approx \prod_{H \leq \mathbf{G}} \left( \frac{|\mathbf{G}|}{|H|} \right)^{|A_H|}$$

Therefore, $R \approx \sum_{H \leq \mathbf{G}} \frac{|A_H|}{N} \log_2 \frac{|\mathbf{G}|}{|H|}$. On the other hand, since $I^n$ is a martingale, we have $\mathbb{E}\{I^\infty\} = I^0$. Since $\mathbb{E}\{I^\infty\} = \sum_{H \leq \mathbf{G}} p_H \log_2 \frac{|\mathbf{G}|}{|H|}$, we observe that the rate $R$ converges to the symmetric capacity $I^0$ as $\epsilon \to 0$. We will see in the next section that this rate is achievable.

It is worth mentioning the complexity of these codes is similiar to the binary case; i.e. the complexity of encoding and the complexity of successive cancelation decoding are both $O(N \log N)$ as functions of code blocklength $N$.

#### 6.1.4.4 Error Analysis

For $H \leq G$ and $i \in A_H^\epsilon$, define the events $B_i$ and $E_i$ according to Equations (6.13) and (6.14). Similar to the $\mathbb{Z}_{p^r}$ case, it is straightforward to show that for $H \leq G$ and $i \in A_H^\epsilon$, $P(E_i) \leq q^2 Z^H(W_N^{(i)})$ where $q = |\mathbf{G}|$. The probability of block error is given by $P(err) = \sum_{H \leq \mathbf{G}} \sum_{i \in A_H^\epsilon} P(B_i)$. Since $B_i \subseteq E_i$, we get

$$\begin{aligned} P(err) &\leq \sum_{H \leq \mathbf{G}} \sum_{i \in A_H^\epsilon} q^2 Z^H(W_N^{(i)}) \\ &\leq \sum_{H \leq \mathbf{G}} |A_H^\epsilon| q^2 2^{-2^{\beta n}} \\ &\leq q^2 N 2^{-2^{\beta n}} \end{aligned}$$

for any $\beta < \frac{1}{2}$. Therefore, the probability of block error goes to zero as $\epsilon \to 0$ ($n \to \infty$).

### 6.1.5 Relation to Group Codes

Recall that for an arbitrary group $\mathbf{G}$, the polar encoder of length $N$ introduced in this paper maps the set $\bigoplus_{H\leq\mathbf{G}} T_H^{A_H}$ to $\mathbf{G}^N$ where for a subgroup $H$ of $\mathbf{G}$, $T_H$ is a transversal of $H$ and $\{A_H|H\leq\mathbf{G}\}$ is some partition of $\{1,\cdots,N\}$. Note that the set of messages $\bigoplus_{H\leq\mathbf{G}} T_H^{A_H}$ is not necessarily closed under addition and hence in general, the set of encoder outputs is not a subgroup of $\mathbf{G}^N$; i.e. polar codes constructed and analyzed in Sections 6.2.2 and 6.1.4 are not group encoders. To the contrary, standard polar codes (i.e. polar codes in which only perfect channels are used) are indeed group codes since their set of messages is of the form $\mathbf{G}^A\oplus\{0\}^{\{1,\cdots,N\}\setminus A}$ for some $A\subseteq\{1,\cdots,N\}$ which is closed under addition.

It is worth mentioning that polar encoders constructed in this paper fall into a larger class of structured codes called *nested group codes*. Nested group codes consist of two group codes: the inner code $\mathbb{C}_i$ and the outer code $\mathbb{C}_o$ such that the inner code is a subgroup of the outer code ($\mathbb{C}_i\leq\mathbb{C}_o$). The set of messages consists of cosets of $\mathbb{C}_i$ in $\mathbb{C}_o$. For the case of polar codes, the inner code is given by

$$\begin{aligned}\mathbb{C}_i&=\left[\bigoplus_{H\leq\mathbf{G}} H^{A_H}\right]G\\&=\left\{mG\,\middle|\,m\in\bigoplus_{H\leq\mathbf{G}} H^{A_H}\right\}\end{aligned}$$

and the outer code is the whole group space: $\mathbb{C}_o=\mathbf{G}^N$. To verify that this is indeed the case, it suffices to show that the set of codewords of polar codes $\left[\bigoplus_{H\leq\mathbf{G}} T_H^{A_H}\right]G$ has only one common element with each coset of $\mathbb{C}_i$. Equivalently, it suffices to show that for $m_1,m_2\in\mathbf{G}^N$, if $m_1G-m_2G\in\mathbb{C}_i$, then either $m_1\notin\bigoplus_{H\leq\mathbf{G}} T_H^{A_H}$ or $m_2\notin\bigoplus_{H\leq\mathbf{G}} T_H^{A_H}$.

**Lemma VI.12.** *For $N=2^n$ where $n$ is a positive integer, the generator matrix corresponding to polar codes $G_N=B_NF^{\otimes n}$ is full rank.*

*Proof.* Since $G_N = B_N F^{\otimes n}$ where $B_N$ is a permutation of rows, it suffices to show that $F^{\otimes n}$ is full rank. Note that the rank of the Kronecker product of two matrices is equal to the product of the ranks of matrices and the rank of $F$ is equal to 2. Hence we have $\text{rank}(G) = \text{rank}(F^{\otimes n}) = 2^n = N$. □

This lemma implies that if $m_1 G - m_2 G \in \mathbb{C}_i$ then $m_1 - m_2 \in \bigoplus_{H \leq \mathbf{G}} H^{A_H}$. This means either $m_1 \notin \bigoplus_{H \leq \mathbf{G}} T_H^{A_H}$ or $m_2 \notin \bigoplus_{H \leq \mathbf{G}} T_H^{A_H}$. This proves that polar codes are indeed nested group codes.

In this section, we consider two examples of channels over $\mathbb{Z}_4$. The first example is Channel 1 introduced in Section 6.1.2. Based on the symmetry of this channel, we show that polar codes achieve the group capacity of this specific channel. The intent of the second example is to show that in general, polar codes do not achieve the group capacity of channels. In order to find the capacity of polar codes as group codes, we use the standard construction of polar codes, i.e. we only use perfect channels and fix partially perfect and useless channels.

#### 6.1.5.1 Example 1

Consider Channel 1 of Figure 6.1. Define $H_0 = \{0, 1, 2, 3\}$, $H_1 = \{0, 2\}$ and $H_2 = \{0\}$ and define $K_0 = \{1, 3\}$, $K_1 = \{2\}$ and $K_2 = \{0\}$. For this channel we have:

$$I^0 \triangleq I(X;Y) = 2 - \epsilon - 2\lambda$$

$$I_2^0 \triangleq I(X_1;Y) = 1 - (\epsilon + \lambda)$$

$$(I_2')^0 \triangleq I(X_1';Y) = 1 - (\epsilon + \lambda) = I_2^0$$

where $X$ is uniform over $\mathbb{Z}_4$, $X_1$ is uniform over $H_1$ and $X_1'$ is uniform over $1 + H_1$. The capacity of group codes over this symmetric channel is equal to [61]:

$$C = \min(I_4^0, I_2^0 + (I_2')^0) = \min(2 - \epsilon - 2\lambda, 2 - 2\epsilon - 2\lambda)$$

$$= 2 - 2\epsilon - 2\lambda$$

All possible cases for this channel are

- **Case 0:** $Z_1^\infty = Z_3^\infty = 1, Z_2^\infty = 1$
- **Case 1:** $Z_1^\infty = Z_3^\infty = 0, Z_2^\infty = 1$
- **Case 2:** $Z_1^\infty = Z_3^\infty = 0, Z_2^\infty = 0$

As we saw in Figures 6.2 and 6.3, this result agrees with the asymptotic behavior of $I^n$ predicted by the recursion formulas (6.1) and (6.2).

Define $I(W^{b_1 b_2 \cdots b_n}) = I(X;Y)$ where $X$, $Y$ are the input and output of $W^{b_1 b_2 \cdots b_n}$ and $X$ is uniform over $\mathbb{Z}_4$. Similarly, define $I_2(W^{b_1 b_2 \cdots b_n}) = I(X_1;Y)$ where $X_1$, $Y$ are the input and output of $W^{b_1 b_2 \cdots b_n}$ and $X_1$ is uniform over $H_1$ and define $I_2'(W^{b_1 b_2 \cdots b_n}) = I(X_1';Y)$ where $X_1'$, $Y$ are the input and output of $W^{b_1 b_2 \cdots b_n}$ and $X_1'$ is uniform over $1 + H_1$. Define the mutual information processes $I_4^n$, $I_2^n$ and $(I_2')^n$ to be equal to $I(W^{b_1 b_2 \cdots b_n})$, $I_2(W^{b_1 b_2 \cdots b_n})$ and $I_2'(W^{b_1 b_2 \cdots b_n})$ where for $i = 1, \cdots, n$, $b_i$'s are iid Bernoulli(0.5) random variables. For this channel, we can show that $I_2(W^{b_1 b_2 \cdots b_n}) = I_2'(W^{b_1 b_2 \cdots b_n}) = 1 - (\epsilon_n + \lambda_n)$ and conclude that $(I_2 + I_2')^n \triangleq I_2^n + (I_2')^n$ is a martingale. Therefore $I_4^n$ and $(I_2 + I_2')^n$ converge almost surely to random variables $I_4^\infty$ and $(I_2 + I_2')^\infty$ respectively. This observation provides us with an ad-hoc way to find the probabilities $p_t$, $t = 0, 1, 2$ of the limit random variable $I_4^\infty$ for this simple channel. We can show the following for the final states:

- **case 0** $\Rightarrow I_4^\infty = 0, (I_2 + I_2')^\infty = 0$
- **case 1** $\Rightarrow I_4^\infty = 1, (I_2 + I_2')^\infty = 0$
- **case 2** $\Rightarrow I_4^\infty = 2, (I_2 + I_2')^\infty = 2$

Therefore, we obtain the following three equations:

$$\mathbb{E}\{I_4^\infty\} = p_0 \cdot 0 + p_1 \cdot 1 + p_2 \cdot 2 = I_4^0 = 2 - \epsilon - 2\lambda$$

$$\mathbb{E}\{(I_2 + I_2')^\infty\} = p_0 \cdot 0 + p_1 \cdot 0 + p_2 \cdot 2 = (I_2 + I_2')^0 = 2 - 2\epsilon - 2\lambda$$

$$p_0 + p_1 + p_2 = 1$$

Solving this system of equations, we obtain:

$$p_2 = 1 - \epsilon - \lambda = C/2$$

$$p_1 = I_4^0 - (I_2 + I_2')^0$$

$$p_0 = 1 - \left(I_4^0 - (I_2 + I_2')^0/2\right)$$

We see that the fraction of perfect channels is equal to the capacity of the channel achievable using group codes and therefore, polar codes achieve the capacity of group codes for this channel.

#### 6.1.5.2 Example 2

The channel is depicted in Figure 6.7. We call this Channel 3. For this channel, when $\lambda = 0.2$ we have:

$$I^0 = I(X;Y) = 0.6390$$

$$(I_2^0 + I_2')^0 = 0.2161$$

The rate $C = \min(I_4^0, (I_2 + I_2')^0) = (I_2 + I_2')^0 = 0.2161$ is achievable using group codes over this channel [61].

For this channel, we have three possible asymptotic cases:

- **Case 0:** $Z_1^\infty = 1, Z_2^\infty = 1 \Rightarrow I_4^\infty = 0, (I_2 + I_2')^\infty = 0$
- **Case 1:** $Z_1^\infty = 0, Z_2^\infty = 1 \Rightarrow I_4^\infty = 1, (I_2 + I_2')^\infty = 0$
- **Case 2:** $Z_1^\infty = 0, Z_2^\infty = 0 \Rightarrow I_4^\infty = 2, (I_2 + I_2')^\infty = 2$

Therefore we obtain the following three equations:

$$\mathbb{E}\{I_4^\infty\} = p_0 \cdot 0 + p_1 \cdot 1 + p_2 \cdot 2$$
$$\mathbb{E}\{(I_2 + I_2')^\infty\} = p_0 \cdot 0 + p_1 \cdot 0 + p_2 \cdot 2$$
$$p_0 + p_1 + p_2 = 1$$

Therefore, the achievable rate using polar codes over this channel is equal to $R = 2p_2 = \mathbb{E}\{(I_2 + I_2')^\infty\}$. We have $\mathbb{E}\{(I_2 + I_2')^1\} = 0.2063$ which is strictly less than $(I_2 + I_2')^0$. The following lemma implies $R = \mathbb{E}\{(I_2 + I_2')^\infty\} \leq \mathbb{E}\{(I_2 + I_2')^1\} < C = (I_2 + I_2')^0$ and completes the proof.

**Lemma VI.13.** *For a channel $(\mathbb{Z}_4, \mathscr{Y}, W)$, the process $(I_2 + I_2')^n, n = 0, 1, 2, \cdots$ is a super-martingale.*

*Proof.* Follow from Lemma VI.2 with $H = \{0, 2\}$. □

### 6.1.6 Appendix

#### 6.1.6.1 Polar Codes Over Abelian Groups

Given a $k \times n$ matrix $G_n$ of 0's and 1's, one can construct a group code as follows: Given any message tuple $u^k \in G^k$, encode it to $u^k \cdot G_n$. Where the elements of $G_n$ determine whether an element of $u^k$ appears as a summand in the encoded word or not. For example consider the generator matrix

$$G_4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix}$$

Then $u^4 \cdot G_4$ is defined as

$$[u_1 u_2 u_3 u_4] \cdot \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix} = \begin{pmatrix} u_1 + u_2 + u_3 + u_4 \\ u_3 + u_4 \\ u_2 + u_4 \\ u_4 \end{pmatrix}$$

Using this convention, we can define a group code based on a given binary matrix without actually defining a multiplication operation for the group.

#### 6.1.6.2 Recursion Formula for Channel 1

**Recursion for $W^+$**

We show that $W^+$ (corresponding to $b_1 = 1$) is equivalent to a channel of the same type as $W$ but with different parameters $\epsilon_1$ and $\lambda_1$ corresponding to $\epsilon$ and $\lambda$ respectively; where,

$$\epsilon_1 = \epsilon^2 + 2\epsilon\lambda$$

$$\lambda_1 = \lambda_1^2$$

We say an output tuple $(y_1, y_2, u_1)$ is connected to an input $u_2 \in \mathbb{Z}_4$ if $W^+(y_1, y_2, u_1|u_2) = \frac{1}{4}W(y_1|u_1 + u_2)W(y_2|u_2)$ is strictly positive.

First, let us assume the output tuple $(y_1, y_2, u_1)$ is connected to all $u_2 \in \mathbb{Z}_4$. Then $W(y_2|u_2)$ must be nonzero for all $u_2$ and hence $y_2 = E_3$. Similarly since $W(y_1|u_1+u_2)$ is nonzero for all $u_2$ (and hence all $u_1 + u_2$) it follows that $y_1 = E_3$. Therefore $W^+(E_3, E_3, u_1|u_2) = \frac{1}{4}\lambda^2$ for all $u_1, u_2 \in \mathbb{Z}_4$ and these are all output tuples connected to all inputs (with positive probability). Since all of these output tuples are equivalent we can combine them to get a single output symbol connected to all four inputs with probability $\lambda^2$.

Next we show that if an output tuple is connected to an input from $\{0, 2\}$ and an input from $\{1, 3\}$, then it is connected to all inputs. Consider the case where the output tuple $(y_1, y_2, u_1)$ is connected to both 0 and 1 i.e. $W^+(y_1, y_2, u_1|0)$ and $W^+(y_1, y_2, u_1|1)$ are both nonzero. Then since $W(y_2|0) \neq 0$ and $W(y_2|1) \neq 0$, it follows that $y_2 = E_3$. Similarly since $W(y_1|u_1) \neq 0$ and $W(y_1|u_1 + 1) \neq 0$, it follows that $y_1 = E_3$. We have already seen that for all $u_1 \in \mathbb{Z}_4$, the output tuple $(E_3, E_3, u_1)$ is connected to all input symbols. The proof is similar for other three cases i.e. when $(y_1, y_2, u_1)$ is connected to 0 and 3, when $(y_1, y_2, u_1)$ is connected to 2 and 1, and when $(y_1, y_2, u_1)$ is connected to 2 and 3.

Next we find all output tuples which are connected to both 0 and 2 but are not connected to 1 or 3. Let $(y_1, y_2, u_1)$ be an output tuple such that $W^+(y_1, y_2, u_1|0) \neq 0$, $W^+(y_1, y_2, u_1|2) \neq 0$, $W^+(y_1, y_2, u_1|1) = 0$ and $W^+(y_1, y_2, u_1|3) = 0$.
First assume $u_1 \in \{0, 2\}$. Since $W(y_2|0) \neq 0$ and $W(y_2|2) \neq 0$, it follows that $y_2 \in \{E_1, E_3\}$ and since $W(y_1|u_1) \neq 0$ and $W(y_1|u_1 + 2) \neq 0$, it follows that $y_1 \in \{E_1, E_3\}$. Note that for $y_1 = E_3$ and $y_2 = E_3$, the output tuple is connected to all inputs and therefore all possible cases are $y_1 = E_1, y_2 = E_1$, $y_1 = E_1, y_2 = E_3$ and $y_1 = E_3, y_2 = E_1$. In all cases it can be shown that $W^+(y_1, y_2, u_1|1) = 0$ and $W^+(y_1, y_2, u_1|3) = 0$. Hence for $u_1 \in \{0, 2\}$, $(E_1, E_1, u_1)$ is connected to 0 and 2 with probabilities $\frac{1}{4}\epsilon^2$ and is not connected to 1 or 3. $(E_1, E_3, u_1)$ is connected to 0 and 2 with probabilities $\frac{1}{4}\epsilon\lambda$ and is not connected to 1 or 3. $(E_3, E_1, u_1)$ is connected to 0 and 2 with probabilities $\frac{1}{4}\epsilon\lambda$ and is not connected to 1 or 3.
Now assume $u_1 \in \{1, 3\}$. Same as above we have $y_2 \in \{E_1, E_3\}$ and since $W(y_1|u_1) \neq 0$ and $W(y_1|u_1 + 2) \neq 0$, it follows that $y_1 \in \{E_2, E_3\}$. In this case, all possible cases are $y_1 = E_2, y_2 = E_1$, $y_1 = E_2, y_2 = E_3$ and $y_1 = E_3, y_2 = E_1$. In all cases it can be shown that $W^+(y_1, y_2, u_1|1) = 0$ and $W^+(y_1, y_2, u_1|3) = 0$. Hence for $u_1 \in \{1, 3\}$, $(E_2, E_1, u_1)$ is connected to 0 and 2 with probabilities $\frac{1}{4}\epsilon^2$ and is not connected to 1 or

3. $(E_2, E_3, u_1)$ is connected to 0 and 2 with probabilities $\frac{1}{4}\epsilon\lambda$ and is not connected to 1 or 3. $(E_3, E_1, u_1)$ is connected to 0 and 2 with probabilities $\frac{1}{4}\epsilon\lambda$ and is not connected to 1 or 3.

Therefore, there are four equivalent outputs connected to 0 and 2 with probabilities $\frac{1}{4}\epsilon^2$ and not connected to 1 or 3 and there are eight equivalent outputs connected to 0 and 2 with probabilities $\frac{1}{4}\epsilon\lambda$ and not connected to 1 or 3. Since all of these outputs are equivalent, we can combine them into one output connected to 0 and 2 with probabilities

$$4\left(\frac{1}{4}\epsilon^2\right) + 8\left(\frac{1}{4}\epsilon\lambda\right) = \epsilon^2 + 2\epsilon\lambda$$

Now we find all output tuples which are connected to both 1 and 3 but are not connected to 0 or 2. Let $(y_1, y_2, u_1)$ be an output tuple such that $W^+(y_1, y_2, u_1|1) \neq 0$, $W^+(y_1, y_2, u_1|3) \neq 0$, $W^+(y_1, y_2, u_1|0) = 0$ and $W^+(y_1, y_2, u_1|2) = 0$.

First assume $u_1 \in \{0, 2\}$. Since $W(y_2|1) \neq 0$ and $W(y_2|3) \neq 0$, it follows that $y_2 \in \{E_2, E_3\}$ and since $W(y_1|u_1 + 1) \neq 0$ and $W(y_1|u_1 + 3) \neq 0$, it follows that $y_1 \in \{E_2, E_3\}$. Note that for $y_1 = E_3$ and $y_3 = E_3$, the output tuple is connected to all inputs and therefore all possible cases are $y_1 = E_2, y_2 = E_2$, $y_1 = E_2, y_2 = E_3$ and $y_1 = E_3, y_2 = E_2$. In all cases it can be shown that $W^+(y_1, y_2, u_1|0) = 0$ and $W^+(y_1, y_2, u_1|2) = 0$. Hence for $u_1 \in \{0, 2\}$, $(E_2, E_2, u_1)$ is connected to 1 and 3 with probabilities $\frac{1}{4}\epsilon^2$ and is not connected to 0 or 2. $(E_2, E_3, u_1)$ is connected to 1 and 3 with probabilities $\frac{1}{4}\epsilon\lambda$ and is not connected to 0 or 2. $(E_3, E_2, u_1)$ is connected to 1 and 3 with probabilities $\frac{1}{4}\epsilon\lambda$ and is not connected to 0 or 2.

Now assume $u_1 \in \{1, 3\}$. Same as above we have $y_2 \in \{E_2, E_3\}$ and since $W(y_1|u_1 + 1) \neq 0$ and $W(y_1|u_1 + 3) \neq 0$, it follows that $y_1 \in \{E_1, E_3\}$. In this case, all possible cases are $y_1 = E_1, y_2 = E_2$, $y_1 = E_1, y_2 = E_3$ and $y_1 = E_3, y_2 = E_2$. In all cases it can be shown that $W^+(y_1, y_2, u_1|0) = 0$ and $W^+(y_1, y_2, u_1|2) = 0$. Hence for $u_1 \in \{1, 3\}$, $(E_1, E_2, u_1)$ is connected to 1 and 3 with probabilities $\frac{1}{4}\epsilon^2$ and is not connected to 0 or 2. $(E_1, E_3, u_1)$ is connected to 1 and 3 with probabilities $\frac{1}{4}\epsilon\lambda$ and is not connected to

0 or 2. $(E_3, E_2, u_1)$ is connected to 1 and 3 with probabilities $\frac{1}{4}\epsilon\lambda$ and is not connected to 0 or 2.

Therefore, there are four equivalent outputs connected to 1 and 3 with probabilities $\frac{1}{4}\epsilon^2$ and not connected to 0 or 2 and there are eight equivalent outputs connected to 1 and 3 with probabilities $\frac{1}{4}\epsilon\lambda$ and not connected to 0 or 2. Same as above, since all of these outputs are equivalent, we can combine them into one output connected to 1 and 3 with probabilities $\epsilon^2 + 2\epsilon\lambda$.

We have shown that there is (equivalently) one channel output (call it $E_3^+$) connected to all inputs $u_2 \in \mathbb{Z}_4$ with conditional probability $\lambda_1 = \lambda^2$ and we have shown that if a channel output is connected to more that one input but is not connected to all inputs, it is either connected to $\{0, 2\}$ and is not connected to $\{1, 3\}$ (call it $E_1^+$) or it is connected to $\{0, 2\}$ and is not connected to $\{1, 3\}$ (call it $E_2^+$). 0 and 2 are connected to $E_1^+$ with probabilities $\epsilon_1 = \epsilon^2 + 2\epsilon\lambda$ and 1 and 3 are connected to $E_2^+$ with probabilities $\epsilon_1 = \epsilon^2 + 2\epsilon\lambda$. Then for each input $u_2 \in \mathbb{Z}_4$ these exist several outputs which are only connected to $u_2$ and not other inputs and whose sum of probabilities add up to $1 - \epsilon_1 - \lambda_1$. This completes the proof for $W^+$.

**Recursion for $W^-$**

We show that $W^-$ (corresponding to $b_1 = 0$) is equivalent to a channel of the same type as $W$ but with different parameters $\epsilon_1$ and $\lambda_1$ corresponding to $\epsilon$ and $\lambda$ respectively; where,

$$\epsilon_1 = 2\epsilon - \left(\epsilon^2 + 2\epsilon\lambda\right)$$

$$\lambda_1 = 2\lambda - \lambda_1^2$$

Note that each channel output is a pair $(y_1, y_2) \in \{0, 1, 2, 3, E_1, E_2, E_3\}^2$. The channel $W^-$ can be shown to be as following:

Output pairs $(0,0)$, $(1,1)$, $(2,2)$, $(3,3)$ are only connected to input 0 each with conditional probability $\frac{1}{4}(1-\epsilon-\lambda)^2$. This is equivalent to one channel output only connected to 0 with probability $(1-\epsilon-\lambda)^2$.

Output pairs $(0,2)$, $(1,3)$, $(2,0)$, $(3,1)$ are only connected to input 2 each with conditional probability $\frac{1}{4}(1-\epsilon-\lambda)^2$. This is equivalent to one channel output only connected to 2 with probability $(1-\epsilon-\lambda)^2$.

Output pairs $(0,3)$, $(1,0)$, $(2,1)$, $(3,2)$ are only connected to input 1 each with conditional probability $\frac{1}{4}(1-\epsilon-\lambda)^2$. This is equivalent to one channel output only connected to 1 with probability $(1-\epsilon-\lambda)^2$.

Output pairs $(0,1)$, $(1,2)$, $(2,3)$, $(3,0)$ are only connected to input 3 each with conditional probability $\frac{1}{4}(1-\epsilon-\lambda)^2$. This is equivalent to one channel output only connected to 3 with probability $(1-\epsilon-\lambda)^2$.

Output pairs $(0,E_1)$, $(1,E_2)$, $(2,E_1)$, $(3,E_2)$, $(E_1,0)$, $(E_1,2)$, $(E_2,1)$, $(E_2,3)$ are only connected to inputs 0 and 2 each with conditional probability $\frac{1}{4}\epsilon(1-\epsilon-\lambda)$. Output pairs $(E_1,E_1)$, $(E_2,E_2)$ are only connected to inputs 0 and 2 each with conditional probability $\frac{1}{2}\epsilon^2$. This is equivalent to one channel output only connected to 0 and 2 with probability

$$\begin{aligned}\epsilon_1 &= 8\times\frac{1}{4}\epsilon(1-\epsilon-\lambda)+2\times\frac{1}{2}\epsilon^2\\ &= 2\epsilon-\left(\epsilon^2+2\epsilon\lambda\right)\end{aligned}$$

Output pairs $(0,E_2)$, $(1,E_1)$, $(2,E_2)$, $(3,E_1)$, $(E_1,1)$, $(E_1,3)$, $(E_2,0)$, $(E_2,2)$ are only connected to inputs 1 and 3 each with conditional probability $\frac{1}{4}\epsilon(1-\epsilon-\lambda)$. Output pairs $(E_1,E_2)$, $(E_2,E_1)$ are only connected to inputs 1 and 3 each with conditional probability $\frac{1}{2}\epsilon^2$. This is equivalent to one channel output only connected to 1 and 3 with probability $2\epsilon-(\epsilon^2+2\epsilon\lambda)$.

Output pairs $(0,E_3)$, $(1,E_3)$, $(2,E_3)$, $(3,E_3)$, $(E_3,0)$, $(E_3,1)$, $(E_3,2)$, $(E_3,3)$ are connected to all inputs each with conditional probability $\frac{1}{4}\lambda(1-\epsilon-\lambda)$. Output pairs

$(E_1, E_3)$, $(E_2, E_3)$, $(E_3, E_1)$, $(E_3, E_2)$ are connected to all inputs each with conditional probability $\frac{1}{2}\epsilon\lambda$. Output pair $(E_3, E_3)$ is connected to all inputs with conditional probability $\lambda^2$. This is equivalent to one channel output only connected to all inputs with probability

$$\begin{aligned}\epsilon_1 &= 8 \times \frac{1}{4}\lambda(1-\epsilon-\lambda) + 4 \times \frac{1}{2}\epsilon\lambda + \lambda^2 \\ &= 2\lambda - \lambda^2\end{aligned}$$

We have listed all 49 channel outputs and the corresponding probabilities. This completes the proof for $W^-$.

#### 6.1.6.3 Some Useful Lemmas

**Lemma VI.14.** *Let $\bar{W}$ be a channel with prime input alphabet size $\bar{q}$. We have the following relations between $I(\bar{W})$ (in bits) and $Z(\bar{W})$:*

1. $I(\bar{W}) \geq \log_2 \frac{\bar{q}}{1+(\bar{q}-1)Z(\bar{W})}$
2. $I(\bar{W}) \leq 2(\bar{q}-1)(\log_2 e)\sqrt{1-Z(W)^2}$

*Proof.* This lemma is a restatement of Proposition 2 of [66]. □

**Lemma VI.15.** *Let $\bar{W}$ be a channel with prime input alphabet size $\bar{q}$ and define $d' = \text{argmax}_{a\neq 0} Z_a(\bar{W})$. If $Z_{d'}(\bar{W}) \geq 1-\delta$ for some $\delta > 0$, then $Z(\bar{W}) \geq 1-\bar{q}(\bar{q}-1)^2\delta$.*

*Proof.* This lemma has been proved in [66] (Lemma 4). □

**Lemma VI.16.** *For any $d \in \mathbf{G}$, we have*

$$Z_d(W^+) = Z_d(W)^2$$

*Proof.* By definition, $Z_d(W^+)$ is equal to

$$\begin{aligned}
&\frac{1}{q}\sum_{\substack{u_1\in\mathbf{G}\\ u_2\in\mathbf{G}\\ y_1,y_2\in\mathscr{Y}}}\sqrt{\frac{1}{q^2}W(y_1|u_1+u_2)W(y_2|u_2)W(y_1|u_1+u_2+d)W(y_2|u_2+d)}\\
&=\frac{1}{q}\sum_{u_2\in\mathbf{G}}\sum_{y_2\in\mathscr{Y}}\sqrt{W(y_2|u_2)W(y_2|u_2+d)}\\
&\qquad\qquad\frac{1}{q}\sum_{u_1\in\mathbf{G}}\sum_{y_1\in\mathscr{Y}}\sqrt{W(y_1|u_1+u_2)W(y_1|u_1+u_2+d)}\\
&=\frac{1}{q}\sum_{u_2\in\mathbf{G}}\sum_{y_2\in\mathscr{Y}}\sqrt{W(y_2|u_2)W(y_2|u_2+d)}\\
&\qquad\qquad\frac{1}{q}\sum_{\tilde{u}_1\in\mathbf{G}}\sum_{y_1\in\mathscr{Y}}\sqrt{W(y_1|\tilde{u}_1)W(y_1|\tilde{u}_1+d)}\\
&=Z_d(W)^2
\end{aligned}$$

□

**Lemma VI.17.** *For $d\in\mathbf{G}$, if $Z_d(W)\geq 1-\delta$ for some $\delta>0$, then for $\tilde{d}\in\langle d\rangle$, $Z_{\tilde{d}}(W)\geq 1-q^3\delta$ where $q=|\mathbf{G}|$.*

*Proof.* First note that

$$\begin{aligned}
Z_d(W)&=\frac{1}{q}\sum_{x\in\mathbf{G}}\sum_{y\in\mathscr{Y}}\sqrt{W(y|x)W(y|x+d)}\\
&=1-\frac{1}{2q}\sum_{x\in\mathbf{G}}\sum_{y\in\mathscr{Y}}\left[\sqrt{W(y|x)}-\sqrt{W(y|x+d)}\right]^2
\end{aligned}$$

Therefore $Z_d(W)\geq 1-\delta$ implies

$$\sum_{y\in\mathscr{Y}}\left[\sqrt{W(y|x)}-\sqrt{W(y|x+d)}\right]^2\leq 2q\delta$$

for all $x \in \mathbf{G}$. Since $\tilde{d} \in \langle d \rangle$, we have $\tilde{d} = id$ for some $i \leq q$. Therefore,

$$\begin{aligned}
1 - Z_{\tilde{d}}(W) &= 1 - \frac{1}{q} \sum_{x \in \mathbf{G}} \sum_{y \in \mathscr{Y}} \sqrt{W(y|x) W(y|x+id)} \\
&= \frac{1}{2q} \sum_{x \in \mathbf{G}} \sum_{y \in \mathscr{Y}} \left[ \sqrt{W(y|x)} - \sqrt{W(y|x+id)} \right]^2 \\
&= \frac{1}{2q} \sum_{x \in \mathbf{G}} \sum_{y \in \mathscr{Y}} \left[ \sum_{j=0}^{i-1} \left( \sqrt{W(y|x+jd)} - \sqrt{W(y|x+(j+1)d)} \right) \right]^2 \\
&\leq \frac{i}{2q} \sum_{x \in \mathbf{G}} \sum_{y \in \mathscr{Y}} \sum_{j=0}^{i-1} \left[ \sqrt{W(y|x+jd)} - \sqrt{W(y|x+(j+1)d)} \right]^2 \\
&= \frac{i}{2q} \sum_{x \in \mathbf{G}} \sum_{j=0}^{i-1} \sum_{y \in \mathscr{Y}} \left[ \sqrt{W(y|x+jd)} - \sqrt{W(y|x+(j+1)d)} \right]^2 \\
&\leq \frac{1}{2} \sum_{x \in \mathbf{G}} \sum_{j=0}^{i-1} 2q\delta \\
&\leq q^3 \delta
\end{aligned}$$

□

**Lemma VI.18.** *For $d_1, \cdots, d_m \in \mathbf{G}$, if $Z_{d_1}(W) \geq 1-\delta, Z_{d_2}(W) \geq 1-\delta, \cdots, Z_{d_m}(W) \geq 1-\delta$, then $Z_{\tilde{d}}(W) \geq 1-2mq^3\delta$ for any $\tilde{d} \in \langle d_1, d_2, \cdots, d_m \rangle$ where $\tilde{d} \in \langle d_1, d_2, \cdots, d_m \rangle$ is the subgroup of $\mathbf{G}$ generated by $d_1, \cdots, d_m$.*

*Proof.* We prove this theorem for $m = 2$. The general case is a straightforward generalization of this case. Similarly to the proof of Lemma VI.17, for all $x \in \mathbf{G}$, we have

$$\sum_{y \in \mathscr{Y}} \left[ \sqrt{W(y|x)} - \sqrt{W(y|x+d_l)} \right]^2 \leq 2q\delta$$

for $l = 1, 2$. Since $\tilde{d} \in \langle d_1, d_2 \rangle$, it can be written as $\tilde{d} = id_1 + jd_2$ for some integers

$i, j \leq q$. Therefore,

$$
\begin{aligned}
1 - Z_{\tilde{d}}(W) &= \frac{1}{q} \sum_{x \in \mathbf{G}} \sum_{y \in \mathscr{Y}} \sqrt{W(y|x) W(y|x + id_1 + jd_2)} \\
&= \frac{1}{2q} \sum_{x \in \mathbf{G}} \sum_{y \in \mathscr{Y}} \left[ \sqrt{W(y|x)} - \sqrt{W(y|x + id_1 + jd_2)} \right]^2 \\
&= \frac{1}{2q} \sum_{\substack{x \in \mathbf{G} \\ y \in \mathscr{Y}}} \left[ \sum_{k=0}^{i-1} \left( \sqrt{W(y|x + kd_1)} - \sqrt{W(y|x + (k+1)d_1)} \right) \right. \\
&\quad \left. + \sum_{k=0}^{j-1} \left( \sqrt{W(y|x + id_1 + kd_2)} - \sqrt{W(y|x + id_1 + (k+1)d_2)} \right) \right]^2 \\
&\leq \frac{i+j}{2q} \sum_{\substack{x \in \mathbf{G} \\ y \in \mathscr{Y}}} \left( \sum_{k=0}^{i-1} \left[ \sqrt{W(y|x + kd_1)} - \sqrt{W(y|x + (k+1)d_1)} \right]^2 \right. \\
&\quad \left. + \sum_{k=0}^{j-1} \left[ \sqrt{W(y|x + id_1 + kd_2)} - \sqrt{W(y|x + id_1 + (k+1)d_2)} \right]^2 \right) \\
&\leq \sum_{x \in \mathbf{G}} \left( \sum_{k=0}^{i-1} 2q\delta + \sum_{k=0}^{j-1} 2q\delta \right) \\
&\leq 4q^3 \delta
\end{aligned}
$$

□

**Lemma VI.19.** *For an Abelian group* $\mathbf{G}$*, let* $M$ *be a maximal subgroup. Then the index of* $M$ *in* $\mathbf{G}$ *is a prime.*

*Proof.* Since $M$ is normal in $\mathbf{G}$, there is a one-to-one correspondence between the subgroups of the quotient group $\mathbf{G}/M$ and the subgroups of $\mathbf{G}$ containing $M$. By maximality of $M$, the latter only contains $\mathbf{G}$ and $M$ (which is not equal to $\mathbf{G}$). Hence, the only subgroups of $\mathbf{G}/M$ are $\{0\}$ and $\mathbf{G}/M$ (which is not equal to $\{0\}$). Hence the order of $\mathbf{G}/M$ must be a prime. □

#### 6.1.6.4 Upper Bound on $Z(\bar{W})$

Assume $Z_{d'}(W) \leq \delta$. This implies

$$\frac{1}{q} \sum_{x \in \mathbf{G}} \sum_{y \in \mathscr{Y}} \sqrt{W(y|x)W(y|x+\tilde{d})} \leq \delta$$

for all $\tilde{d} \in H \backslash M$. Therefore for each $x \in \mathbf{G}$,

$$\sum_{y \in \mathscr{Y}} \sqrt{W(y|x)W(y|x+\tilde{d})} \leq q\delta \tag{6.20}$$

The Bhattacharyya parameter of the channel $\bar{W}$, $Z(\bar{W})$, is given by:

$$\begin{aligned}
&\frac{1}{\bar{q}(\bar{q}-1)} \sum_{\substack{y \in \mathscr{Y} \\ t_M, t'_M \in T_M \\ t_M \neq t'_M}} \sqrt{\bar{W}(y|t_H + t_M + M)\bar{W}(y|t_H + t'_M + M)} \\
&= \frac{1/|M|}{\bar{q}(\bar{q}-1)} \sum_{\substack{y \in \mathscr{Y} \\ t_M, t'_M \in T_M \\ t_M \neq t'_M}} \sqrt{\sum_{m \in M} W(y|t_H + t_M + m) \sum_{m' \in M} W(y|t_H + t'_M + m')} \\
&= \frac{1/|M|}{\bar{q}(\bar{q}-1)} \sum_{\substack{y \in \mathscr{Y} \\ t_M, t'_M \in T_M \\ t_M \neq t'_M}} \sqrt{\sum_{m,m'} W(y|t_H + t_M + m)W(y|t_H + t'_M + m')} \\
&\leq \frac{1/|M|}{\bar{q}(\bar{q}-1)} \sum_{\substack{y \in \mathscr{Y} \\ t_M, t'_M \in T_M \\ t_M \neq t'_M}} \sum_{m,m'} \sqrt{W(y|t_H + t_M + m)W(y|t_H + t'_M + m')}
\end{aligned}$$

Let $x = t_H + t_M + m$ and $x' = t_H + t'_M + m'$. Note that $x - x' = t_M - t'_M + m - m' \in H$ since $t_M, t'_M, m, m' \in H$. Also note that since $t_M \neq t'_M$ and $m - m' \in M$, $x - x' \notin M$. Now we use (6.20) to conclude:

$$\begin{aligned}
Z(\bar{W}) &\leq \frac{1}{\bar{q}(\bar{q}-1)} \frac{1}{|M|} \sum_{\substack{t_M, t'_M \in T_M \\ t_M \neq t'_M}} \sum_{m,m' \in M} q\delta \\
&\leq \frac{1}{\bar{q}(\bar{q}-1)} \frac{1}{|M|} \left(\frac{|H|}{|M|}\right)^2 |M|^2 q\delta = \frac{|M| \cdot |H| \cdot |\mathbf{G}|}{|H| - |M|} \delta
\end{aligned}$$

*Remark* VI.20. For an arbitrary Abelian group $\mathbf{G}$, let $H \leq \mathbf{G}$ be an arbitrary subgroup and let $M$ be any maximal subgroup of $H$. If for all $\tilde{d} \in H \backslash M$, $Z_{\tilde{d}}(W) \leq \delta$ then with a similar argument as above we can show that $Z(\bar{W}) \leq \frac{|M| \cdot |H| \cdot |\mathbf{G}|}{|H| - |M|} \delta$ where $\bar{W}$ is defined by (6.11).

#### 6.1.6.5 Lower Bound on $Z_{d'+t_H+M}(\bar{W})$

Assume $Z_{d'}(W) \geq 1 - \delta$. Define

$$D_{d'}(W) = \frac{1}{2q} \sum_{x \in \mathbf{G}} \sum_{y \in \mathscr{Y}} |W(y|x) - W(y|x + d')|$$

First we show that $Z_{d'}(W) \geq 1 - \delta$ implies $D_{d'}(W) \leq \sqrt{2\delta - \delta^2}$. Define the following quantities:

$$q_{x,y} = \frac{W(y|x) + W(y|x + d')}{2}$$
$$\delta_{x,y} = \frac{1}{2} |W(y|x) - W(y|x + d')|$$

Then we have

$$\begin{aligned} Z_{d'}(W) &= \frac{1}{q} \sum_{x \in \mathbf{G}} \sum_{y \in \mathscr{Y}} \sqrt{(q_{x,y} - \delta_{x,y})(q_{x,y} + \delta_{x,y})} \\ &= \frac{1}{q} \sum_{x \in \mathbf{G}} \sum_{y \in \mathscr{Y}} \sqrt{q_{x,y}^2 - \delta_{x,y}^2} \end{aligned}$$

Also we have

$$D \triangleq \frac{1}{q} \sum_{x \in \mathbf{G}} \sum_{y \in \mathscr{Y}} \delta_{x,y} = D_{d'}(W),$$

and

$$0 \leq \delta_{x,y} \leq q_{x,y}$$

Note that

$$Z_{d'}(W) \leq \max_{\substack{d_{x,y}: \\ \frac{1}{q} \sum_{x \in \mathbf{G}} \sum_{y \in \mathscr{Y}} d_{x,y} = D}} \frac{1}{q} \sum_{x \in \mathbf{G}} \sum_{y \in \mathscr{Y}} \sqrt{q_{x,y}^2 - d_{x,y}^2}$$

The Lagrangian for this optimization problem is given by

$$\mathscr{L} = \frac{1}{q}\sum_{x\in\mathbf{G}}\sum_{y\in\mathscr{Y}}\sqrt{q_{x,y}^2 - d_{x,y}^2} - \lambda\left(\frac{1}{q}\sum_{x\in\mathbf{G}}\sum_{y\in\mathscr{Y}} d_{x,y} - D\right)$$

we have

$$\frac{\partial}{\partial d_{x,y}}\mathscr{L} = -\frac{d_{x,y}}{\sqrt{q_{x,y}^2 - d_{x,y}^2}} - \frac{\lambda}{q}$$

and

$$\frac{\partial^2}{\partial d_{x,y}^2}\mathscr{L} = -\frac{q_{x,y}^2}{(q_{x,y}^2 - d_{x,y}^2)^{\frac{3}{2}}} \leq 0$$

Define $\gamma = -\frac{\lambda}{q}$ to get $d_{x,y} = \sqrt{\frac{\gamma^2}{1+\gamma^2}}q_{x,y}$. We have $\sum_{y\in\mathscr{Y}} q_{x,y} = 1$, therefore,

$$\begin{aligned}
\frac{1}{q}\sum_{x\in\mathbf{G}}\sum_{y\in\mathscr{Y}} d_{x,y} &= \frac{1}{q}\sum_{x\in\mathbf{G}}\sum_{y\in\mathscr{Y}}\sqrt{\frac{\gamma^2}{1+\gamma^2}}q_{x,y} \\
&= \sqrt{\frac{\gamma^2}{1+\gamma^2}}\frac{1}{q}\sum_{x\in\mathbf{G}}\sum_{y\in\mathscr{Y}} q_{x,y} \\
&= \sqrt{\frac{\gamma^2}{1+\gamma^2}}
\end{aligned}$$

Therefore we have $D = \sqrt{\frac{\gamma^2}{1+\gamma^2}}$ and hence $d_{x,y} = Dq_{x,y}$. For this choice of $d_{x,y}$ we have

$$\begin{aligned}
\frac{1}{q}\sum_{x\in\mathbf{G}}\sum_{y\in\mathscr{Y}}\sqrt{q_{x,y}^2 - d_{x,y}^2} &= \frac{\sqrt{1-D^2}}{q}\sum_{x\in\mathbf{G}}\sum_{y\in\mathscr{Y}} q_{x,y} \\
&= \sqrt{1-D^2}
\end{aligned}$$

Therefore, we have shown that $Z_{d'}(W) \leq \sqrt{1 - D_{d'}(W)^2}$. This implies that $D_{d'}(W) \leq \sqrt{2\delta - \delta^2}$.

Next, we show that $D_{d'}(W) \leq \delta$ implies $D_{d'+t_H+M}(\bar{W}) \leq \frac{2q\delta}{\bar{q}|M|}$. By definition,

$D_{d'+t_H+M}(\bar{W})$ is equal to

$$\begin{aligned}
&\frac{1}{\bar{q}} \sum_{\substack{y\in\mathscr{Y}\\ t_M\in T_M}} \left|\bar{W}(y|t_H+t_M+M) - \bar{W}(y|t_H+t_M+d'+M)\right| \\
&= \frac{1}{\bar{q}} \frac{1}{|M|} \sum_{\substack{y\in\mathscr{Y}\\ t_M\in T_M}} \left| \sum_{m\in M} W(y|t_H+t_M+m) - \sum_{m\in M} W(y|t_H+t_M+d'+m) \right| \\
&\leq \frac{1}{\bar{q}} \frac{1}{|M|} \sum_{\substack{y\in\mathscr{Y}\\ t_M\in T_M\\ m\in M}} |W(y|t_H+t_M+m) - W(y|t_H+t_M+d'+m)| \\
&\leq \frac{1}{\bar{q}} \frac{1}{|M|} 2q D_{d'}(W)
\end{aligned}$$

This shows that $D_{d'}(W) \leq \delta$ implies $D_{d'+t_H+M}(\bar{W}) \leq \frac{2q\delta}{\bar{q}|M|}$.

Next, we show that $D_{d'}(W) \leq \delta$ implies $Z_{d'}(W) \geq 1 - \delta$. We need the following lemma:

**Lemma VI.21.** *For constants $0 \leq a \leq b \leq 1$, with $b - a \leq \delta$,*

$$\sqrt{ab} \geq \frac{a+b}{2} - \frac{\delta}{2}$$

*Proof.* Note that

$$\frac{a+b}{2} - \sqrt{ab} \leq \max_{0\leq x-a\leq\delta} \frac{a+x}{2} - \sqrt{ax}$$

We have

$$\frac{\partial}{\partial x}\left[\frac{a+x}{2} - \sqrt{ax}\right] = \frac{1}{2} - \frac{a}{2\sqrt{ax}} \geq 0$$

for all $x \geq a$. Therefore the maximum is attained at $x = a + \delta$. Therefore,

$$\frac{a+b}{2} - \sqrt{ab} \leq \frac{a+(a+\delta)}{2} - \sqrt{a(a+\delta)}$$

The maximum of the right hand side is attained at $a = 0$, hence,

$$\frac{a+b}{2} - \sqrt{ab} \leq \frac{\delta}{2}$$

□

Assume $D_{d'}(W) \leq \delta$. By definition, we have $1 - Z_{d'}(W)$ is equal to

$$\begin{aligned}
&1 - \frac{1}{q} \sum_{x \in \mathbf{G}} \sum_{y \in \mathscr{Y}} \sqrt{W(y|x) W(y|x+d')} \\
&= \frac{1}{q} \sum_{\substack{y \in \mathscr{Y} \\ x \in \mathbf{G}}} \left( \frac{W(y|x) + W(y|x+d')}{2} - \sqrt{W(y|x) W(y|x+d')} \right) \\
&\overset{(a)}{\leq} \frac{1}{q} \sum_{x \in \mathbf{G}} \sum_{y \in \mathscr{Y}} \frac{1}{2} \left| W(y|x) - W(y|x+d') \right| \\
&= D_{d'}(W)
\end{aligned}$$

where $(a)$ follows from Lemma VI.21 with $a = W(y|x)$, $b = W(y|x+d')$ and $\delta = |W(y|x) - W(y|x+d')|$. This shows that $D_{d'}(W) \leq \delta$ implies $Z_{d'}(W) > 1 - \delta$.

We have shown that $Z_{d'}(W) \geq 1 - \delta$ implies $D_{d'}(W) \leq \sqrt{2\delta - \delta^2}$. This implies $D_{d'+t_H+M}(\bar{W}) \leq \frac{2q\sqrt{2\delta-\delta^2}}{\bar{q}|M|}$ and this in turn implies $Z_{d'+t_H+M}(\bar{W}) \geq 1 - \frac{2q\sqrt{2\delta-\delta^2}}{\bar{q}|M|}$.

*Remark* VI.22. For an arbitrary Abelian group $\mathbf{G}$, let $H \leq \mathbf{G}$ be an arbitrary subgroup and let $M$ be any maximal subgroup of $H$. If for some $\tilde{d} \in H \backslash M$, $Z_{\tilde{d}}(W) \geq 1 - \delta$ then with a similar argument as above, we can show that $Z_{\tilde{d}+t_H+M}(\bar{W}) \geq 1 - \frac{2q\sqrt{2\delta-\delta^2}}{\bar{q}|M|}$ where $\bar{W}$ is defined by (6.11).

#### 6.1.6.6 Alternate Proof for a Lower Bound on $Z_{d'+t_H+M}(\bar{W})$

In Appendix 6.1.6.5, we proved that $Z_{d'}(W) \geq 1 - \delta$ implies $Z_{d'+t_H+M}(\bar{W}) \geq 1 - \frac{2q\sqrt{2\delta-\delta^2}}{\bar{q}|M|}$ for the general case. In this part, we give a shorter proof for the $\mathbb{Z}_{p^r}$ case for a slightly different statement: If $Z_{d'}(W) \geq 1 - \delta$ then $Z_{d'+t_H+M}(\bar{W}) \geq 1 - q^2\delta$

Assume $Z_{d'}(W) \geq 1 - \delta$. It follows that for all $x \in \mathbf{G}$,

$$\frac{1}{2} \sum_{y \in \mathscr{Y}} \left[ \sqrt{W(y|x)} - \sqrt{W(y|x+d')} \right]^2 =$$

$$1 - \sum_{y \in \mathscr{Y}} \sqrt{W(y|x) W(y|x+d')} \leq q\delta$$

For any $\tilde{d} \in \langle d' \rangle$ we have $\tilde{d} = id$ for some $i \leq q$. Therefore, for any $x \in \mathbf{G}$, $1 - \sum_{y \in \mathscr{Y}} \sqrt{W(y|x)W(y|x+\tilde{d})}$ is equal to

$$\begin{aligned}
&\frac{1}{2} \sum_{y \in \mathscr{Y}} \left[ \sqrt{W(y|x)} - \sqrt{W(y|x+\tilde{d})} \right]^2 \\
&= \frac{1}{2} \sum_{y \in \mathscr{Y}} \left[ \sum_{j=0}^{i-1} \left( \sqrt{W(y|x+jd')} - \sqrt{W(y|x+(j+1)d')} \right) \right]^2 \\
&\leq \frac{1}{2} \sum_{y \in \mathscr{Y}} \sum_{j=0}^{i-1} \left[ \sqrt{W(y|x+jd')} - \sqrt{W(y|x+(j+1)d')} \right]^2 \\
&\leq \sum_{j=0}^{i-1} q\delta \leq q^2\delta
\end{aligned} \tag{6.21}$$

By definition, $Z_{d'+t_H+M}(\bar{W})$ is equal to

$$\begin{aligned}
&\frac{1}{\bar{q}} \sum_{\substack{y \in \mathscr{Y} \\ t_M \in T_M}} \sqrt{\bar{W}(y|t_H+t_M+M)\bar{W}(y|t_H+t_M+d'+M)} \\
&= \frac{1}{\bar{q}} \sum_{\substack{y \in \mathscr{Y} \\ t_M \in T_M}} \sqrt{\sum_{\substack{m \in M \\ m' \in M}} \frac{1}{|M|^2} W(y|t_H+t_M+m)W(y|t_H+t_M+d'+m')} \\
&\overset{(a)}{\geq} \frac{1}{\bar{q}} \sum_{\substack{y \in \mathscr{Y} \\ t_M \in T_M \\ m,m' \in M}} \frac{1}{|M|^2} \sqrt{W(y|t_H+t_M+m)W(y|t_H+t_M+d'+m')} \\
&\geq \frac{1}{\bar{q}} \sum_{t_M \in T_M} \min_{m,m'} \sum_{y \in \mathscr{Y}} \sqrt{W(y|t_H+t_M+m)W(y|t_H+t_M+d'+m')}
\end{aligned}$$

where $(a)$ follows since $\sqrt{\cdot}$ is a concave function. Let $x = t_H + t_M + m$ and $x' = t_H + t_M + d' + m'$. It follows that $x' - x = d' + (m' - m)$. Since $d', m', m \in H$ we have $x' - x \in H$. Since $\mathbf{G}$ and hence $H$ are $\mathbb{Z}_{p^r}$ rings it follows that $d' \in H \backslash M$ generates $H$; hence $x' - x \in \langle d' \rangle$. We can use (6.21) to get

$$Z_{d'+t_H+M}(\bar{W}) \geq \frac{1}{\bar{q}} \sum_{t_M \in T_M} \min_{m,m' \in M} (1 - q^2\delta) = 1 - q^2\delta$$

#### 6.1.6.7 The Rate of Polarization

Recall that for $t = 0, \cdots, r$, $(Z^t)^{(n)} = \sum_{d \notin H_t} Z_d(W_N^{(J_n)})$ where $J_n$ is uniform over $\{1, 2, \cdots, 2^n\}$. For $t = 0, \cdots, r$, define $(Z_{\max}^t)^{(n)} = \max_{d \notin H_t} Z_d(W_N^{(J_n)})$ where $J_n$ is

same as above. Since for all $d \in \mathbf{G}$, $Z_d(W^+) = Z_d(W)^2$ it follows that $Z^t_{\max}(W^+) \leq Z^t_{\max}(W)^2$. It has been shown in [66, p. 6] that

$$Z_d(W^-) \leq 2Z_d(W) + \sum_{\substack{\Delta \neq 0 \\ \Delta \neq -d}} Z_\Delta(W) Z_{d+\Delta}(W)$$

Note that for any $\Delta \in G$, $d \notin H_t$ implies that either $\Delta \notin H_t$ or $d+\Delta \notin H_t$. Therefore, $d \notin H_t$ implies either $Z_\Delta(W) \leq Z^t_{\max}(W)$ or $Z_{d+\Delta}(W) \leq Z^t_{\max}(W)$ (or both). Since $Z_\Delta(W)$ and $Z_{d+\Delta}(W)$ both take values from $[0,1]$, it follows that

$$Z_\Delta(W) Z_{d+\Delta}(W) \leq Z^t_{\max}(W)$$

Therefore, for any $d \notin H_t$, $Z_d(W^-) \leq 2Z_d(W) + qZ^t_{\max}(W)$. Hence

$$\begin{aligned} Z^t_{\max}(W^-) &= \max_{d \notin H_t} Z_d(W^-) \\ &\leq \max_{d \notin H_t} \left(2Z_d(W) + qZ^t_{\max}(W)\right) \\ &\leq (q+2) Z^t_{\max}(W) \end{aligned}$$

Since for all $d \in \mathbf{G}$, $Z^n_d$ converges to a Bernoulli random variable it follows that $(Z^t_{\max})^{(n)}$ also converges to a $\{0,1\}$-valued random variable $(Z^t_{\max})^{(\infty)}$. Note that $P\left((Z^t_{\max})^{(\infty)} = 0\right) = P\left((Z^t)^\infty = 0\right) = \sum_{s=t}^r p_s$. Therefore, $(Z^t_{\max})^{(n)}$ satisfies the conditions of [13, Theorem 1] and hence

$$\lim_{n\to\infty} P\left((Z^t_{\max})^{(n)} < 2^{-2^{\beta n}}\right) = P\left((Z^t_{\max})^{(\infty)} = 0\right)$$

for any $\beta < \frac{1}{2}$. It clearly follows that $\lim_{n\to\infty} P\left(q(Z^t_{\max})^{(n)} < 2^{-2^{\beta n}}\right) = P\left((Z^t_{\max})^{(\infty)} = 0\right)$. Note that the event $\{(Z^t)^{(n)} < 2^{-2^{\beta n}}\}$ includes the event $\{q(Z^t_{\max})^{(n)} < 2^{-2^{\beta n}}\}$. Therefore,

$$\lim_{n\to\infty} P\left((Z^t)^{(n)} < 2^{-2^{\beta n}}\right) \geq P\left((Z^t)^\infty = 0\right)$$

Similarly, for an arbitrary Abelian group $\mathbf{G}$ and a subgroup $H$ of $\mathbf{G}$, define $(Z^H_{\max})^{(n)} = \max_{d \notin H} Z_d(W_N^{(J_n)})$ where $J_n$ is defined as above. It is straightforward

to show that $(Z^H_{\max})^{(n)}$ satisfies the conditions of [13, Theorem 1]. Therefore, with an argument similar to above, we can show that,

$$\lim_{n\to\infty} P\left((Z^H)^{(n)} < 2^{-2^{\beta n}}\right) \geq P\left((Z^H)^{\infty} = 0\right)$$

for any $\beta < \frac{1}{2}$.

## 6.2 Polar Codes for Arbitrary DMSs

In Section 6.1, we have shown that polar codes can achieve the symmetric capacity of arbitrary discrete memoryless channels regardless of the size of the channel input alphabet. It is shown in [39] that polar codes employed with a successive cancelation encoder can achieve the symmetric rate-distortion function for the lossy source coding problem when the size of the reconstruction alphabet is two. This result is extended to the case where the size of the reconstruction alphabet is a prime in [38]. In this section, we show that polar codes achieve the symmetric rate-distortion bound for the lossy source coding problem when the size of the reconstruction alphabet is finite. We show that similarly to the channel coding problem, polar transformations applied to (test) channels can converge to several asymptotic cases each corresponding to a subgroup $H$ of the reconstruction alphabet $\mathbf{G}$. We employ a modified randomized rounding encoding rule to achieve the symmetric rate-distortion bound.

### 6.2.1 Preliminaries

#### 6.2.1.1 The Rate-Distortion Function

It is known that the optimal rate-distortion function is given by:

$$R(D) = \min_{\substack{p_{U|X} \\ \mathbb{E}_{p_X p_{U|X}}\{d(X,U)\}\leq D}} I(X;U)$$

where $p_{U|X}$ is the conditional probability of $U$ given $X$ and $p_X p_{U|X}$ is the joint distribution of $X$ and $U$.

The *symmetric rate-distortion* function $\bar{R}(D)$ is defined as follows:

$$\bar{R}(D) = \min_{\substack{p_{U|X} \\ \mathbb{E}_{p_X p_{U|X}}\{d(X,U)\} \leq D \\ p_U = \frac{1}{q}}} I(X;U)$$

where $p_U$ is the marginal distribution of $U$ given by $p_U(u) = \sum_{x \in \mathscr{X}} p_X(x) p_{U|X}(u|x)$ and $q$ is the size of the reconstruction alphabet $\mathscr{U}$.

#### 6.2.1.2 Channel Parameters

For a test channel $(\mathscr{U}, \mathscr{X}, W)$ assume $\mathscr{U}$ is equipped with the structure of a group $(\mathbf{G}, +)$. The quantities $I^0(W) = I(U;X)$, $Z(W_{\{u,\tilde{u}\}})$ and $Z(W)$ are defined similarly to Section 6.1.1.1. In addition, we use the following two quantities in the paper extensively:

$$D_d(W) = \frac{1}{2q} \sum_{u \in \mathscr{U}} \sum_{x \in \mathscr{X}} |W(x|u) - W(x|u+d)|$$

$$\tilde{D}_d(W) = \frac{1}{2q} \sum_{u \in \mathscr{U}} \sum_{x \in \mathscr{X}} (W(x|u) - W(x|u+d))^2$$

where $d$ is some element of $\mathbf{G}$ and $+$ is the group operation.

### 6.2.2 Polar Codes for Sources with reconstruction alphabet $\mathbb{Z}_{p^r}$

In this section, we consider sources whose reconstruction alphabet size $q$ is of the form $q = p^r$ for some prime number $p$ and a positive integer $r$. In this case, the reconstruction alphabet can be considered as a ring with addition and multiplication modulo $p^r$. We prove the achievability of the symmetric rate-distortion bound for these sources using polar codes and later in Section 6.2.3 we will generalize this result to sources with arbitrary finite reconstruction alphabets.

#### 6.2.2.1 Recursive Channel Transformation

**The Basic Channel Transforms**

For a test channel $(\mathscr{U} = \mathbf{G}, \mathscr{X}, W)$ where $|\mathbf{G}| = q$, the channel transformations are given by:

$$W^-(x_1, x_2|u_1) = \sum_{u_2' \in \mathbf{G}} \frac{1}{q} W(x_1|u_1 + u_2')W(x_2|u_2') \tag{6.22}$$

$$W^+(x_1, x_2, u_1|u_2) = \frac{1}{q} W(x_1|u_1 + u_2)W(x_2|u_2) \tag{6.23}$$

for $x_1, x_2 \in \mathscr{X}$ and $u_1, u_2 \in \mathbf{G}$. Repeating these operations $n$ times recursively, we obtain $N = 2^n$ channels $W_N^{(1)}, \cdots, W_N^{(N)}$. For $i = 1, \cdots, N$, these channels are given by:

$$W_N^{(i)}(x_1^N, u_1^{i-1}|u_i) = \sum_{u_{i+1}^N \in \mathbf{G}^{N-i}} \frac{1}{q^{N-1}} W^N(x_1^N|u_1^N G_N) \tag{6.24}$$

where $G_N$ is the generator matrix for polar codes.

Let $V_1^N$ be a random vector uniformly distributed over $\mathbf{G}^N$ and assume the random vectors $V_1^N$, $U_1^N$ and $X_1^N$ are distributed over $\mathbf{G}^N \times \mathbf{G}^N \times \mathscr{X}^N$ according to

$$p_{V_1^N U_1^N X_1^N}(v_1^N, u_1^N, x_1^n) = \frac{1}{q^N} \mathbb{1}_{\{u_1^N = v_1^N G_N\}} \prod_{i=1}^N W(x_i|u_i)$$

The conditional probability distribution induced from the above equation is consistent with (6.24). We use this probability distribution extensively throughout the paper.

#### 6.2.2.2 Encoding and Decoding

Let $n$ be a positive integer and let $G_N$ be the generator matrix for polar codes where $N = 2^n$. Let $\{A_t | 0 \leq t \leq r\}$ be a partition of the index set $\{1, 2, \cdots, N\}$. Let $b_1^N$ be an arbitrary element from the set $\bigoplus_{t=0}^r H_t^{A_t}$. Assume that the partition $\{A_t | 0 \leq t \leq r\}$ and the vector $b_1^N$ are known to both the encoder and the decoder. The encoder maps a source sequence $x_1^N$ to a vector $v_1^N \in \mathbf{G}^N$ by the following rule:

For $i = 1, \cdots, N$, if $i \in A_t$, let $v_i$ be a random element $g$ from the set $b_i + T_t$ picked with probability

$$P(v_i = g) = \frac{P_{V_i|V_1^{i-1},X_1^N}(g|v_1^{i-1}, x_1^N)}{P_{V_i|V_1^{i-1},X_1^N}(b_i + T_t|v_1^{i-1}, x_1^N)}$$

This encoding rule is a generalization of the randomized rounding encoding rule used for the binary case in [39].

Given a sequence $v_1^N \in \mathbf{G}^N$, the decoder decodes it to $v_1^N G_N$.

For the sake of analysis we assume that the vector $b_1^N$ is uniformly randomly distributed over the set $\bigoplus_{t=0}^{r} H_t^{A_t}$ (Although it's common information between the encoder and the decoder). The average distortion is given by $\frac{1}{N}\mathbb{E}\{d(X_1^N, U_1^N)\}$ and the rate of the code is given by

$$R = \frac{1}{N}\sum_{t=0}^{r} |A_t| \log |T_t| = \sum_{t=0}^{r} \frac{|A_t|}{N} t \log p$$

#### 6.2.2.3 Test Channel Polarization

The following result has been proved in [59]: For all $\epsilon > 0$, there exists a number $N = N(\epsilon) = 2^{n(\epsilon)}$ and a partition $\{A_0^\epsilon, A_1^\epsilon, \cdots, A_r^\epsilon\}$ of $\{1, \cdots, N\}$ such that for $t = 0, \cdots, r$ and $i \in A_t^\epsilon$, $Z_d(W_N^{(i)}) < O(\epsilon)$ if $d \in H_s$ for $0 \leq s < t$ and $Z_d(W_N^{(i)}) > 1 - O(\epsilon)$ if $d \in H_s$ for $t \leq s < r$. For $t = 0, \cdots, r$ and $i \in A_t^\epsilon$, we have $I(W_N^{(i)}) = t\log(p) + O(\epsilon)$ and $Z^t(W_N^{(i)}) = O(\epsilon)$ where

$$Z^t(W) = \frac{1}{|H_t|}\sum_{d \in H_t} Z_d(W)$$

Moreover, as $\epsilon \to 0$, $\frac{|A_t^\epsilon|}{N} \to p_t$ for some probabilities $p_0, \cdots, p_r$.

In the next section, we show that for any $\beta < \frac{1}{2}$ and for $t = 0, \cdots, r$,

$$\begin{aligned} \lim_{n\to\infty} P\left((Z^t)^{(n)} > 1 - 2^{-2^{\beta n}}\right) &\geq P\left((Z^t)^{(\infty)} = 1\right) \\ &= 1 - \sum_{s=t}^{r} p_s \end{aligned} \tag{6.25}$$

*Remark* VI.23. This observation implies the following stronger result: For all $\epsilon > 0$, there exists a number $N = N(\epsilon) = 2^{n(\epsilon)}$ and a partition $\{A_0^\epsilon, A_1^\epsilon, \cdots, A_r^\epsilon\}$ of $\{1, \cdots, N\}$ such that for $t = 0, \cdots, r$ and $i \in A_t^\epsilon$, $I(W_N^{(i)}) = t\log(p) + O(\epsilon)$ and $Z^t(W_N^{(i)}) > 1 - 2^{-2^{\beta n(\epsilon)}}$. Moreover, as $\epsilon \to 0$, $\frac{|A_t^\epsilon|}{N} \to p_t$ for some probabilities $p_0, \cdots, p_r$.

#### 6.2.2.4 Rate of Polarization

In this section we derive a rate of polarization result for the source coding problem. In this proof, we do not assume $q$ is a power of a prime and hence the rate of polarization result derived in this section is valid for the general case.

It is shown in [13] (with a slight generalization) that if a random process $Z_n$ satisfies the following two properties

$$Z_{n+1} \leq kZ_n \text{ w.p. } \frac{1}{2} \tag{6.26}$$

$$Z_{n+1} \leq Z_n^2 \text{ w.p. } \frac{1}{2} \tag{6.27}$$

for some constant $k$, then for any $\beta < \frac{1}{2}$, $\lim_{n\to\infty} P(Z_n < 2^{-2^{\beta n}}) = P(Z_\infty = 0)$. We prove that the random process $\tilde{D}_d^n$ satisfied these properties. First note that by definition

$$\tilde{D}_d(W^+) = \frac{1}{2q} \sum_{u_2 \in \mathbf{G}} \sum_{\substack{x_1, x_2 \in \mathscr{X} \\ u_1 \in \mathbf{G}}} \left[ \frac{1}{q} W(x_1|u_1 + u_2) W(x_2|u_2) - \frac{1}{q} W(x_1|u_1 + u_2 + d) W(x_2|u_2 + d) \right]^2$$

If we add and subtract the term $\frac{1}{q} W(x_1|u_1 + u_2) W(x_2|u_2 + d)$ to the term inside brackets and use the inequality $(a+b)^2 \leq 2(a^2 + b^2)$ with

$$a = W(x_1|u_1+u_2)W(x_2|u_2) - W(x_1|u_1 + u_2)W(x_2|u_2+d)$$

$$b = W(x_1|u_1 + u_2)W(x_2|u_2 + d) - W(x_1|u_1 + u_2 + d)W(x_2|u_2 + d)$$

we obtain

$$\tilde{D}_d(W^+) \leq \frac{1}{2q} \sum_{u_2 \in \mathbf{G}} \sum_{x_1, x_2 \in \mathscr{X}, u_1 \in \mathbf{G}} \frac{2}{q^2}$$
$$\Big[\big(W(x_1|u_1+u_2)W(x_2|u_2) - W(x_1|u_1+u_2)W(x_2|u_2+d)\big)^2$$
$$+ \big(W(x_1|u_1+u_2)W(x_2|u_2+d)$$
$$- W(x_1|u_1+u_2+d)W(x_2|u_2+d)\big)^2\Big] \tag{6.28}$$

This summation can be expanded into two separate summations. For the first summation, we have

$$\frac{1}{2q} \sum_{u_2 \in \mathbf{G}} \sum_{x_1, x_2 \in \mathscr{X}, u_1 \in \mathbf{G}} \frac{2}{q^2}$$
$$\big(W(x_1|u_1+u_2)W(x_2|u_2) - W(x_1|u_1+u_2)W(x_2|u_2+d)\big)^2$$
$$\leq \frac{2}{q^2}\frac{1}{2q} \sum_{u_2 \in \mathbf{G}} \sum_{x_1, x_2 \in \mathscr{X}, u_1 \in \mathbf{G}}$$
$$W(x_1|u_1+u_2)^2 \left(W(x_2|u_2) - W(x_2|u_2+d)\right)^2$$
$$\leq \frac{2q}{q^2}\frac{1}{2q} \sum_{u_2 \in \mathbf{G}} \sum_{x_2 \in \mathscr{X}} \left(W(x_2|u_2) - W(x_2|u_2+d)\right)^2$$
$$= \frac{2}{q}\tilde{D}_d(W) \tag{6.29}$$

Similarly, for the second summation we can show that

$$\frac{1}{2q} \sum_{u_2 \in \mathbf{G}} \sum_{\substack{x_1, x_2 \in \mathscr{X} \\ u_1 \in \mathbf{G}}} \frac{2}{q^2} \left(W(x_1|u_1+u_2)W(x_2|u_2+d)\right.$$
$$\left. - W(x_1|u_1+u_2+d)W(x_2|u_2+d)\right)^2$$
$$\leq \frac{2}{q}\tilde{D}_d(W) \tag{6.30}$$

Therefore, it follows from (6.28), (6.29) and (6.30) that condition (6.26) is satisfied for $k = \frac{4}{q}$.

Next we show that $\tilde{D}_d(W^-) \leq \left(\tilde{D}_d(W)\right)^2$. Note that

$$\begin{aligned}
\tilde{D}_d(W^-) = & \\
& \frac{1}{2q} \sum_{v_1 \in \mathbf{G}} \sum_{x_1, x_2 \in \mathscr{X}} \left[ \left( \frac{1}{q} \sum_{v_2 \in \mathbf{G}} W(x_1|v_1 + v_2) W(x_2|v_2) \right) \right. \\
& \qquad \left. - \left( \frac{1}{q} \sum_{v_2 \in \mathbf{G}} W(x_1|v_1 + d + v_2) W(x_2|v_2) \right) \right]^2 \\
= & \frac{1}{2q} \sum_{v_1 \in \mathbf{G}} \sum_{x_1, x_2 \in \mathscr{X}} \frac{1}{q^2} \left[ \sum_{v_2 \in \mathbf{G}} W(x_2|v_2) \left( W(x_1|v_1 + v_2) \right. \right. \\
& \qquad \left. \left. - W(x_1|v_1 + d + v_2) \right) \right]^2
\end{aligned}$$

The squared term in the brackets can be expanded as

$$\begin{aligned}
& \frac{1}{q^2} \sum_{v_2, v_2' \in \mathbf{G}} W(x_2|v_2) W(x_2|v_2') \left( W(x_1|v_1 + v_2) - \right. \\
& \left. W(x_1|v_1 + d + v_2) \right) \left( W(x_1|v_1 + v_2') - W(x_1|v_1 + d + v_2') \right)
\end{aligned}$$

Therefore, $\tilde{D}_d(W^-)$ can be written as a summation of four terms $\tilde{D}_d(W^-) = D_1^- + D_2^- + D_3^- + D_4^-$ where

$$\begin{aligned}
D_1^- = & \frac{1}{2q} \sum_{v_1 \in \mathbf{G}} \sum_{x_1, x_2 \in \mathscr{X}} \frac{1}{q^2} \sum_{v_2, v_2' \in \mathbf{G}} W(x_2|v_2) \\
& W(x_2|v_2') W(x_1|v_1 + v_2) W(x_1|v_1 + v_2') \\
D_2^- = & \frac{1}{2q} \sum_{v_1 \in \mathbf{G}} \sum_{x_1, x_2 \in \mathscr{X}} \frac{1}{q^2} \sum_{v_2, v_2' \in \mathbf{G}} W(x_2|v_2) \\
& W(x_2|v_2') W(x_1|v_1 + v_2 + d) W(x_1|v_1 + v_2' + d) \\
D_3^- = & \frac{1}{2q} \sum_{v_1 \in \mathbf{G}} \sum_{x_1, x_2 \in \mathscr{X}} \frac{1}{q^2} \sum_{v_2, v_2' \in \mathbf{G}} W(x_2|v_2) \\
& W(x_2|v_2') W(x_1|v_1 + v_2) W(x_1|v_1 + v_2' + d) \\
D_4^- = & \frac{1}{2q} \sum_{v_1 \in \mathbf{G}} \sum_{x_1, x_2 \in \mathscr{X}} \frac{1}{q^2} \sum_{v_2, v_2' \in \mathbf{G}} W(x_2|v_2) \\
& W(x_2|v_2') W(x_1|v_1 + v_2 + d) W(x_1|v_1 + v_2')
\end{aligned}$$

For $d \in \mathbf{G}$ define

$$S_d(W) = \frac{1}{2q} \sum_{v \in \mathbf{G}} \sum_{x \in \mathscr{X}} W(x|v) W(x|v+d)$$

Note that $S_d(W) = S_{-d}(W)$. We have

$$\begin{aligned}
D_1^- &= \frac{1}{q^2} \sum_{x_2 \in \mathscr{X}} \sum_{v_2, v_2' \in \mathbf{G}} W(x_2|v_2) W(x_2|v_2') \\
&\quad \frac{1}{2q} \sum_{v_1 \in \mathbf{G}} \sum_{x_1 \in \mathscr{X}} W(x_1|v_1+v_2) W(x_1|v_1+v_2') \\
&= \frac{1}{q^2} \sum_{x_2 \in \mathscr{X}} \sum_{v_2, v_2' \in \mathbf{G}} W(x_2|v_2) W(x_2|v_2') S_{v_2 - v_2'}(W) \\
&= \frac{1}{q^2} \sum_{x_2 \in \mathscr{X}} \sum_{v_2 \in \mathbf{G}} \sum_{\substack{a \in \mathbf{G} \\ v_2' = v_2 - a}} W(x_2|v_2) W(x_2|v_2-a) S_a(W) \\
&= \frac{2}{q} \sum_{a \in \mathbf{G}} S_a(W) \frac{1}{2q} \sum_{v_2 \in \mathbf{G}} \sum_{x_2 \in \mathscr{X}} W(x_2|v_2) W(x_2|v_2-a) \\
&= \frac{2}{q} \sum_{a \in \mathbf{G}} S_a(W) S_{-a}(W) \\
&= \frac{2}{q} \sum_{a \in \mathbf{G}} S_a(W)^2
\end{aligned}$$

With similar arguments we can show that

$$\begin{aligned}
D_2^- &= \frac{2}{q} \sum_{a \in \mathbf{G}} S_a(W)^2 \\
D_3^- &= \frac{2}{q} \sum_{a \in \mathbf{G}} S_a(W) S_{a-d}(W) \\
D_4^- &= \frac{2}{q} \sum_{a \in \mathbf{G}} S_a(W) S_{a-d}(W)
\end{aligned}$$

Therefore

$$\begin{aligned}
\tilde{D}_d(W^-) &= \frac{4}{q} \sum_{a \in \mathbf{G}} \left( S_a(W)^2 - S_a(W) S_{a-d}(W) \right) \\
&= \frac{2}{q} \sum_{a \in \mathbf{G}} \left( S_a(W) - S_{a-d}(W) \right)^2
\end{aligned}$$

Note that

$$\begin{aligned}\tilde{D}_d(W) &= \frac{1}{2q}\sum_{v\in\mathbf{G}}\sum_{x\in\mathscr{X}}\left(W(x|v)-W(x|v+d)\right)^2 \\ &= 2S_0(W)-2S_d(W)\end{aligned}$$

Therefore

$$\left(\tilde{D}_d(W)\right)^2 = 4(S_0(W)-S_d(W))^2$$

To show that $\tilde{D}_d(W^-) \leq \left(\tilde{D}_d(W)\right)^2$ it suffices to show that $S_a(W)-S_{a-d}(W) \leq S_0(W)-S_d(W)$. We will make use of the rearrangement inequality:

**Lemma VI.24.** *Let $\pi$ be an arbitrary permutation of the set $\{1,\cdots,n$. If $a_1 \leq \cdots \leq a_n$ and $b_1 \leq \cdots \leq b_n$ then*

$$\sum_{i=1}^{n} a_i b_i \geq \sum_{i=1}^{n} a_i b_{\pi(i)}$$

The rearrangement inequality implies that $S_0(W)-S_d(W) \geq S_a(W)-S_{a-d}(W)$. Therefore it follows that condition (6.27) is also satisfied and hence $\lim_{n\to\infty} P(\tilde{D}_d^n < 2^{-2^{\beta n}}) = P(\tilde{D}_d^\infty = 0)$. It has been shown in Appendix D of [59] that $\tilde{D}_d(W) < \epsilon$ implies $Z_d(W) > 1-\epsilon$. This completes the rate of polarization result.

#### 6.2.2.5 Polar Codes Achieve the Rate-Distortion Bound

The average distortion for the encoding and decoding rules described in Section 6.2.2.2 is given by

$$\begin{aligned} D_{avg} &= \sum_{x_1^N \in \mathscr{X}^N} p_X^N(x_1^N) \sum_{b_1^N \in \bigoplus_{t=0}^r H_t^{A_t}} \sum_{v_1^N \in b_1^N + \bigoplus_{t=0}^r T_t^{A_t}} \\ &\qquad \left( \prod_{t=0}^{r} \prod_{i \in A_t} \frac{P_{V_i|V_1^{i-1},X_1^N}(g|v_1^{i-1}, x_1^N)}{P_{V_i|V_1^{i-1},X_1^N}(b_i + T_t|v_1^{i-1}, x_1^N)} \right) \\ &\qquad\qquad \left( \prod_{t=0}^{r} \frac{1}{|H_t|^{|A_t|}} \right) d(x_1^N, v_1^N G_N) \\ &= \sum_{x_1^N \in \mathscr{X}^N} p_X^N(x_1^N) \sum_{b_1^N \in \bigoplus_{t=0}^r H_t^{A_t}} \sum_{v_1^N \in b_1^N + \bigoplus_{t=0}^r T_t^{A_t}} \\ &\qquad \left( \prod_{t=0}^{r} \prod_{i \in A_t} \frac{P_{V_i|V_1^{i-1},X_1^N}(g|v_1^{i-1}, x_1^N)}{P_{V_i|V_1^{i-1},X_1^N}(b_i + T_t|v_1^{i-1}, x_1^N) \cdot |H_t|} \right) \\ &\qquad\qquad d(x_1^N, v_1^N G_N) \end{aligned}$$

This can be written as

$$D_{avg} = \mathbb{E}_Q\{d(X_1^N, V_1^N G_N)\}$$

where the distribution $Q$ is defined by

$$Q(v_i|v_1^{i-1}, x_1^N) = \frac{P_{V_i|V_1^{i-1},X_1^N}(v_i|v_1^{i-1}, x_1^N)}{P_{V_i|V_1^{i-1},X_1^N}(b_i + T_t|v_1^{i-1}, x_1^N) \cdot |H_t|}$$

and

$$Q(x_1^N) = p_X^N(x_1^N)$$

and hence

$$\begin{aligned} Q(v_1^N, x_1^N) &= \prod_{i=1}^{N} Q(v_i|v_1^{i-1}, x_1^N) \\ &= \prod_{t=0}^{r} \prod_{i \in A_t} \frac{P_{V_i|V_1^{i-1},X_1^N}(v_i|v_1^{i-1}, x_1^N)}{P_{V_i|V_1^{i-1},X_1^N}(b_i + T_t|v_1^{i-1}, x_1^N) \cdot |H_t|} \end{aligned}$$

Recall that

$$P(v_1^N, x_1^N) = \prod_{i=1}^{N} P_{V_i|V_1^{i-1},X_1^N}(v_i|v_1^{i-1}, x_1^N)$$

The total variation distance between the distributions $P$ and $Q$ is given by

$$\begin{aligned}\|P-Q\|_{\text{t.v.}} &= \sum_{v_1^N \in \mathbf{G}^N, x_1^N \in \mathscr{X}^N} \left|Q(v_1^N, x_1^N) - P(v_1^N, x_1^N)\right| \\ &= \sum_{x_1^N \in \mathscr{X}^N} p_X^N(x_1^N) \sum_{v_1^N \in \mathbf{G}^N} \left|Q(v_1^N|x_1^N) - P(v_1^N|x_1^N)\right|\end{aligned}$$

We have

$$\begin{aligned}&\sum_{v_1^N \in \mathbf{G}^N} \left|Q(v_1^N|x_1^N) - P(v_1^N|x_1^N)\right| \\ &= \sum_{v_1^N \in \mathbf{G}^N} \left| \left( \prod_{t=0}^{r} \prod_{i \in A_t} \frac{P(v_i|v_1^{i-1}, x_1^N)}{P(b_i + T_t|v_1^{i-1}, x_1^N) \cdot |H_t|} \right) \right. \\ &\qquad \left. - \left( \prod_{t=0}^{r} \prod_{i \in A_t} P(v_i|v_1^{i-1}, x_1^N) \right) \right| \\ &\overset{(a)}{=} \sum_{v_1^N \in \mathbf{G}^N} \left| \sum_{t=0}^{r} \sum_{i \in A_t} \right. \\ &\quad \left[ \left( \frac{P(v_i|v_1^{i-1}, x_1^N)}{P(b_i + T_t|v_1^{i-1}, x_1^N) \cdot |H_t|} - P(v_i|v_1^{i-1}, x_1^N) \right) \right. \\ &\qquad \cdot \left( \prod_{t=0}^{r} \prod_{\substack{j=1 \\ j \in A_t}}^{i-1} P(v_i|v_1^{i-1}, x_1^N) \right) \\ &\quad \left. \left. \cdot \left( \prod_{t=0}^{r} \prod_{\substack{j=i+1 \\ j \in A_t}}^{N} \frac{P(v_i|v_1^{i-1}, x_1^N)}{P(b_i + T_t|v_1^{i-1}, x_1^N) \cdot |H_t|} \right) \right] \right|\end{aligned}$$

where in $(a)$ we used the telescopic inequality introduced in [39]. It is straightforward to show that

$$\|P - Q\|_{\text{t.v.}} \leq \sum_{t=0}^{r} \sum_{i \in A_t} \mathbb{E}\left\{ \left| \frac{1}{P(b_i + T_t|v_1^{i-1}, x_1^N) \cdot |H_t|} - 1 \right| \right\}$$

It has been shown in Appendix D of [59] that if $Z_d(W) > 1-\epsilon$ then $D_d(W) \leq 2\epsilon - \epsilon^2$. Therefore if $Z_d(W_N^{(i)}) > 1-\epsilon$ for all $d \in H$ we have

$$\begin{aligned} D_d(W_N^{(i)}) = \frac{1}{2q} \sum_{v_i \in \mathbf{G}} \sum_{v_1^{i-1} \in \mathbf{G}^{i-1}, x_1^N \in \mathscr{X}^N} & \\ & \left| W_N^{(i)}(v_1^{i-1}, x_1^N | v_i) - W_N^{(i)}(v_1^{i-1}, x_1^N | v_i + d) \right| \\ & \leq 2\epsilon - \epsilon^2 \end{aligned}$$

Therefore for all $v_i \in \mathbf{G}$

$$\begin{aligned} \sum_{\substack{v_1^{i-1} \in \mathbf{G}^{i-1} \\ x_1^N \in \mathscr{X}^N}} & \left| W_N^{(i)}(v_1^{i-1}, x_1^N | v_i) - W_N^{(i)}(v_1^{i-1}, x_1^N | v_i + d) \right| \\ & \leq 2q(2\epsilon - \epsilon^2) \end{aligned}$$

We have

$$
\begin{aligned}
&\mathbb{E}\left\{\left|\frac{1}{|H_t|}-P(T_t|V_1^{i-1},X_1^N)\right|\right\}\\
&=\sum_{v_1^{i-1}\in\mathbf{G}^{i-1},x_1^N\in\mathscr{X}^N} P(v_1^{i-1},x_1^N)\left|\frac{1}{|H_t|}-P(T_t|v_1^{i-1},x_1^N)\right|\\
&=\sum_{\substack{v_1^{i-1}\in\mathbf{G}^{i-1}\\ x_1^N\in\mathscr{X}^N}}\left|\frac{1}{|H_t|}P(v_1^{i-1},x_1^N)-\sum_{g\in T_t}P(g,v_1^{i-1},x_1^N)\right|\\
&=\sum_{v_1^{i-1}\in\mathbf{G}^{i-1},x_1^N\in\mathscr{X}^N}\left|\sum_{g\in T_t}\left[\frac{1}{|\mathbf{G}|}W(v_1^{i-1},x_1^N|g)\right.\right.\\
&\qquad\left.\left.-\sum_{d\in H}\frac{1}{|H_t|\cdot|\mathbf{G}|}W(v_1^{i-1},x_1^N|g+d)\right]\right|\\
&\le\sum_{v_1^{i-1}\in\mathbf{G}^{i-1},x_1^N\in\mathscr{X}^N}\frac{1}{|\mathbf{G}|}\sum_{g\in T_t}\left|\left[W(v_1^{i-1},x_1^N|g)\right.\right.\\
&\qquad\left.\left.-\sum_{d\in H}\frac{1}{|H_t|}W(v_1^{i-1},x_1^N|g+d)\right]\right|\\
&\le\frac{1}{|\mathbf{G}|}\sum_{g\in T_t}\frac{1}{|H_t|}\sum_{d\in H}\sum_{v_1^{i-1}\in\mathbf{G}^{i-1},x_1^N\in\mathscr{X}^N}\\
&\qquad\left|W(v_1^{i-1},x_1^N|g)-W(v_1^{i-1},x_1^N|g+d)\right|\\
&\le\frac{2q(2\epsilon-\epsilon^2)}{|H_t|}
\end{aligned}
$$

Therefore for if for all $d\in H_t$, $Z_d>1-\epsilon$ then for $\delta=\frac{2q(2\epsilon-\epsilon^2)}{|H_t|}$ we have

$$\mathbb{E}_P\left\{\left|\frac{1}{|H_t|}-P(b_i+T_t|V_1^{i-1},X_1^N)\right|\right\}<\delta$$

A similar argument as in [39] implies that

$$
\begin{aligned}
D_{avg}&=\frac{1}{N}\mathbb{E}_Q\{d(X_1^N,V_1^NG_N)\}\\
&\le\frac{1}{N}\mathbb{E}_P\{d(X_1^N,V_1^NG_N)\}+\frac{1}{N}\sum_{t=0}^{r}|A_t|d_{\max}\delta
\end{aligned}
$$

where $d_{\max}$ is the maximum value of the distortion function. Note that

$$\mathbb{E}_P\{d(X_1^N,V_1^NG_N)\}=ND$$

Therefore,

$$D_{avg} \leq D + \frac{1}{N}\sum_{t=0}^{r} |A_t| d_{\max}\delta$$

Note that from the rate of polarization derived in Section 6.2.2.4 we can choose $\epsilon$ to be $\epsilon = 2^{-2^{\beta n}}$. This implies that as $n \to \infty$, $D + \frac{1}{N}\sum_{t=0}^{r} |A_t| d_{\max}\delta \to D$. Also note that the rate of the code $R = \sum_{t=0}^{r} \frac{|A_t|}{N} t \log p$ converges to $\sum_{t=0}^{r} p_t t \log p$ and this last quantity is equal to the symmetric capacity of the test channel since the mutual information is a martingale. This means the rate $I(X;U)$ is achievable with distortion $D$.

### 6.2.3 Arbitrary Reconstruction Alphabets

For an arbitrary Abelian group $\mathbf{G}$, The following polarization result has been provided in [59]: For all $\epsilon > 0$, there exists a number $N = N(\epsilon) = 2^{n(\epsilon)}$ and a partition $\{A_H^\epsilon | H \leq \mathbf{G}\}$ of $\{1, \cdots, N\}$ such that for $H \leq \mathbf{G}$ and $i \in A_H^\epsilon$, $Z_d(W_N^{(i)}) < O(\epsilon)$ if $d \in H$ and $Z_d(W_N^{(i)}) > 1 - O(\epsilon)$ if $d \notin H$. For $H \leq \mathbf{G}$ and $i \in A_H^\epsilon$, we have $I(W_N^{(i)}) = \log \frac{|\mathbf{G}|}{|H|} + O(\epsilon)$ and $Z^H(W_N^{(i)}) = O(\epsilon)$ where

$$Z^H(W) = \frac{1}{|H|}\sum_{d \in H} Z_d(W)$$

Moreover, as $\epsilon \to 0$, $\frac{|A_H^\epsilon|}{N} \to p_H$ for some probabilities $p_H, H \leq \mathbf{G}$.

As mentioned earlier the rate of polarization result derived in Section 6.2.2.4 is valid for the general case. Therefore it follows that for any $\beta < \frac{1}{2}$ and for $H \leq \mathbf{G}$,

$$\begin{aligned} \lim_{n\to\infty} P\left((Z^H)^{(n)} > 1 - 2^{-2^{\beta n}}\right) &\geq P\left((Z^H)^{(\infty)} = 1\right) \\ &= 1 - \sum_{S \leq H} p_H \end{aligned} \tag{6.31}$$

*Remark* VI.25. This observation implies the following stronger result: For all $\epsilon > 0$, there exists a number $N = N(\epsilon) = 2^{n(\epsilon)}$ and a partition $\{A_H^\epsilon | H \leq \mathbf{G}\}$ of $\{1, \cdots, N\}$

such that for $H \leq \mathbf{G}$ and $i \in A_H^\epsilon$, $I(W_N^{(i)}) = \log \frac{|\mathbf{G}|}{|H|} + O(\epsilon)$ and $Z^H(W_N^{(i)}) > 1 - 2^{-2^{\beta n(\epsilon)}}$. Moreover, as $\epsilon \to 0$, $\frac{|A_H^\epsilon|}{N} \to p_H$ for some probabilities $p_H, H \leq \mathbf{G}$.

The encoding and decoding rules for the general case is as follows: Let $n$ be a positive integer and let $G_N$ be the generator matrix for polar codes where $N = 2^n$. Let $\{A_H | H \leq \mathbf{G}\}$ be a partition of the index set $\{1, 2, \cdots, N\}$. Let $b_1^N$ be an arbitrary element from the set $\bigoplus_{H \leq \mathbf{G}} H^{A_H}$. Assume that the partition $\{A_H | H \leq \mathbf{G}\}$ and the vector $b_1^N$ are known to both the encoder and the decoder. The encoder maps a source sequence $x_1^N$ to a vector $v_1^N \in \mathbf{G}^N$ by the following rule:
For a subgroup $H$ of $\mathbf{G}$, let $T_H$ be a transversal of $H$ in $\mathbf{G}$. For $i = 1, \cdots, N$, if $i \in A_H$, let $v_i$ be a random element $g$ from the set $b_i + T_H$ picked with probability

$$P(v_i = g) = \frac{P_{V_i|V_1^{i-1}, X_1^N}(g | v_1^{i-1}, x_1^N)}{P_{V_i|V_1^{i-1}, X_1^N}(b_i + T_H | v_1^{i-1}, x_1^N)}$$

Given a sequence $v_1^N \in \mathbf{G}^N$, the decoder decodes it to $v_1^N G_N$.
It follows from the analysis of the $\mathbb{Z}_{p^r}$ case in a straightforward fashion that this encoding/decoding scheme achieves the symmetric rate-distortion bound when the group $\mathbf{G}$ is an arbitrary Abelian group.

## 6.3 Nested Polar Codes for Point-to-Point Communications

In this section, we show that nested polar codes achieve the Shannon rate-distortion function for arbitrary (binary or non-binary) discrete memoryless sources and the Shannon capacity of arbitrary discrete memoryless channels.

Polar codes for lossy source coding were investigated in [40] where it is shown that polar codes achieve the symmetric rate-distortion function for sources with binary reconstruction alphabets. For the lossless source coding problem, the source polarization phenomenon is introduced in [11] to compress a source down to its entropy.

It is well known that linear codes can at most achieve the symmetric capacity of discrete memoryless channels and the symmetric rate-distortion function for discrete memoryless sources. This indicates that polar codes are optimal linear codes in terms of the achievable rate. It is also known that nested linear codes achieve the Shannon capacity of arbitrary discrete memoryless channels and the Shannon rate-distortion function for arbitrary discrete memoryless sources. In this paper, we investigate the performance of nested polar codes for the point-to-point channel and source coding problems and show that these codes achieve the Shannon capacity of arbitrary (binary or non-binary) DMCs and the Shannon rate-distortion function for arbitrary DMSs.

The results of this chapter are general regarding the size of the channel and source alphabets. To generalize the results to non-binary cases, we use the approach of [62] in which it is shown that polar codes with their original $(u, u+v)$ kernel, achieve the symmetric capacity of arbitrary discrete memoryless channels where $+$ is the addition operation over any finite Abelian group.

### 6.3.1 The Lossy Source Coding Problem

In this section, we prove the following theorem:

**Theorem VI.26.** *For an arbitrary discrete memoryless source $(\mathscr{X}, \mathscr{U}, p_X, d)$, nested polar codes achieve the Shannon rate-distortion function.*

For the source $(\mathscr{X}, \mathscr{U}, p_X, d)$, let $\mathscr{U} = \mathbf{G}$ where $\mathbf{G}$ is an arbitrary Abelian group and let $q = |\mathbf{G}|$ be the size of the group. For a pair $(R, D) \in \mathbb{R}^2$, let $X$ be distributed according to $p_X$ and let $U$ be a random variable such that $\mathbb{E}\{d(X, U)\} \leq D$. We prove that there exists a pair of polar codes $\mathbb{C}_i \subseteq \mathbb{C}_o$ such that $\mathbb{C}_i$ induces a partition of $\mathbb{C}_o$ through its shifts, $\mathbb{C}_o$ is a good source code for $X$ and each shift of $\mathbb{C}_i$ is a good channel code for the test channel $p_{X|U}$. This will be made clear in the following.

Given the test channel $p_{X|U}$, define the artificial channels $(\mathbf{G}, \mathbf{G}, W_c)$ and $(\mathbf{G}, \mathscr{X} \times \mathbf{G}, W_s)$ such that for $s, z \in \mathbf{G}$ and $x \in \mathscr{X}$, $W_c(z|s) = p_U(z-s)$ and $W_s(x, z|s) = p_{XU}(x, z-s)$. These channels have been depicted in Figures 6.8 and 6.9.

Let $S$ be a random variable uniformly distributed over $\mathbf{G}$ which is independent from $X$ and $U$. It is straightforward to show that in this case, $Z$ is also uniformly distributed over $\mathbf{G}$. The symmetric capacity of the channel $W_c$ is equal to $\bar{I}(W_c) = \log q - H(U$. For the channel $W_s$, it is shown in [63] that the symmetric capacity of the channel $W_s$ is equal to $\bar{I}(W_s) = \log q - H(U|X)$. We employ a nested polar code in which the inner code $\mathbb{C}_i$ is a good channel code for the channel $W_c$ and the outer code $\mathbb{C}_o$ is a good source code for $W_s$. The rate of this code is equal to $R = \bar{I}(W_s) - \bar{I}(W_c)$. Therefore,

$$R = \log q - H(U|X) - (\log q - H(U)) = I(X;U)$$

Note that the channels $W_c$ and $W_s$ are chosen so that the difference of their *symmetric* capacities is equal to the *Shannon* mutual information between $U$ and $X$. This enables us to use channel coding polar codes to achieve the symmetric capacity of $W_c$ (as the inner code) and source coding polar codes to achieve the symmetric capacity of the test channel $W_s$ (as the outer code). The exact proof is postponed to Section 6.3.1.2 where the result is proved for the binary case and Section 6.3.1.3 in which the general proof (for arbitrary Abelian groups) is presented.

The next section is devoted to some general definitions and useful lemmas which are used in the proofs.

#### 6.3.1.1 Definitions and Lemmas

For a channel $(\mathscr{X}, \mathscr{Y}, W)$, the basic channel transformations associated with polar codes are given by:

$$W^{-}(y_1, y_2|u_1) = \sum_{u_2' \in \mathbf{G}} \frac{1}{q} W(y_1|u_1 + u_2')W(y_2|u_2') \tag{6.32}$$

$$W^{+}(y_1, y_2, u_1|u_2) = \frac{1}{q} W(y_1|u_1 + u_2)W(y_2|u_2) \tag{6.33}$$

for $y_1, y_2 \in \mathscr{Y}$ and $u_1, u_2 \in \mathbf{G}$. We apply these transformations to both channels $(\mathbf{G}, \mathbf{G}, W_c)$ and $(\mathbf{G}, \mathscr{X} \times \mathbf{G}, W_s)$. Repeating these operations $n$ times recursively for $W_c$ and $W_s$, we obtain $N = 2^n$ channels $W_{c,N}^{(1)}, \cdots, W_{c,N}^{(N)}$ and $W_{s,N}^{(1)}, \cdots, W_{s,N}^{(N)}$ respectively. For $i = 1, \cdots, N$, these channels are given by:

$$W_{c,N}^{(i)}(z_1^n, v_1^{i-1}|v_i) = \sum_{v_{i+1}^N \in \mathbf{G}^{N-i}} \frac{1}{q^{N-1}} W_c^N(z_1^N|v_1^N G)$$

$$W_{s,N}^{(i)}(x_1^N, z_1^n, v_1^{i-1}|v_i) = \sum_{v_{i+1}^N \in \mathbf{G}^{N-i}} \frac{1}{q^{N-1}} W_s^N(x_1^N, z_1^N|v_1^N G)$$

for $z_1^N, v_1^N \in \mathbf{G}^N$, $x_1^N \in \mathscr{X}^N$ where $G$ is the generator matrix of dimensions $N \times N$ for polar codes. For the case of binary input channels, it has been shown in [10] that as $N \to \infty$, these channels polarize in the sense that their Bhattacharyya parameter gets either close to zero (perfect channels) or close to one (useless channels). For arbitrary channels, it is shown in [62] that polarization happens in multiple levels so that as $N \to \infty$ channels get useless, perfect or "partially perfect".

**Definition VI.27.** The channel $(\mathbf{G}, \mathscr{Y}_1, W_1)$ is degraded with respect to the channel $(\mathbf{G}, \mathscr{Y}_2, W_2)$ if there exists a channel $(\mathscr{Y}_2, \mathscr{Y}_1, W)$ such that for $x \in \mathbf{G}$ and $y_1 \in \mathscr{Y}_1$,

$$W_1(y_1|x) = \sum_{y_2 \in \mathscr{Y}} W_2(y_2|x)W(y_1|y_2)$$

**Lemma VI.28.** *If the channel $(\mathbf{G}, \mathscr{Y}_1, W_1)$ is degraded with respect to the channel $(\mathbf{G}, \mathscr{Y}_2, W_2)$ in the sense of Definition VI.27, then for any $d \in G$, $Z_d(W_1) \geq Z_d(W_2)$.*

*Proof.* Provided in a more complete version of this work [63]. □

A special case of this lemma is when $\mathbf{G} = \mathbb{Z}_2$ and $d = 1$. In this case, the lemma implies, $Z(W_1) \geq Z(W_2)$ if $W_1$ is degraded with respect to $W_2$.

**Lemma VI.29.** *The channel $W_c$ is degraded with respect to the channel $W_s$ in the sense of Definition VI.27.*

*Proof.* In Definition VI.27, let the channel $(\mathscr{X} \times \mathbf{G}, \mathbf{G}, W)$ be such that for $z, z' \in \mathbf{G}$ and $x \in \mathscr{X}$, $W(z|x, z') = \mathbb{1}_{\{z=z'\}}$. □

Let the random vectors $X_1^N, U_1^N$ be distributed according to $P_{XU}^N$ and let $Z_1^N$ be a random variable uniformly distributed over $\mathbf{G}^N$ which is independent of $X_1^N, U_1^N$. Let $S_1^N = Z_1^N - U_1^N$ and $V_1^N = S_1^N G^{-1}$ (Here, $G^{-1}$ is the inverse of the one-two-one mapping $G : \mathbf{G}^N \to \mathbf{G}^N$). In other words, the joint distribution of these random vectors is given by

$$\begin{aligned} &p_{V_1^N S_1^N U_1^N X_1^N Z_1^N}(v_1^N, s_1^N, u_1^N, x_1^N, z_1^N) \\ &\qquad = \frac{1}{q^N} p_{XU}^N(x_1^N, u_1^N) \mathbb{1}_{\{s_1^N = v_1^N G, u_1^n = z_1^N - v_1^N G\}} \end{aligned}$$

#### 6.3.1.2 Source Coding: Proof for the Binary Case

The standard result of channel polarization for the binary input channel $W_c$ implies [10] that for any $\epsilon > 0$ and $0 < \beta < \frac{1}{2}$, there exist a large $N = 2^n$ and a partition $A_0, A_1$ of $[1, N]$ such that for $t = 0, 1$ and $i \in A_t$, $\left|\bar{I}(W_{c,N}^{(i)}) - t\right| < \epsilon$ and such that for $i \in A_1$ $Z(W_{c,N}^{(i)}) < 2^{-N^\beta}$. Moreover, as $\epsilon \to 0$ (and $N \to \infty$), $\frac{|A_t|}{N} \to p_t$ for some $p_0, p_1$ adding up to one with $p_1 = \bar{I}(W_c)$.

Similarly, for the channel $W_s$ we have the following: For any $\epsilon > 0$ and $0 < \beta < \frac{1}{2}$, there exist a large $N = 2^n$ and a partition $B_0, B_1$ of $[1, N]$ such that for $\tau = 0, 1$ and $i \in B_\tau$, $\left|\bar{I}(W_{s,N}^{(i)}) - \tau\right| < \epsilon$ and such that for $i \in B_1$, $Z(W_{s,N}^{(i)}) < 2^{-N^\beta}$. Moreover, as $\epsilon \to 0$ (and $N \to \infty$), $\frac{|B_\tau|}{N} \to q_\tau$ for some $q_0, q_1$ adding up to one with $q_1 = \bar{I}(W_s)$.

**Lemma VI.30.** *For $i = 1, \cdots, N$, $Z(W_{c,N}^{(i)}) \geq Z(W_{s,N}^{(i)})$.*

*Proof.* Provided in a more complete version [63]. □

To introduce the encoding and decoding rules, we need to make the following definitions:

$$A_0 = \left\{ i \in [1, N] \,\middle|\, Z(W_{c,N}^{(i)}) > 2^{-N^\beta} \right\}$$
$$B_0 = \left\{ i \in [1, N] \,\middle|\, Z(W_{s,N}^{(i)}) > 1 - 2^{-N^\beta} \right\}$$

and $A_1 = [1, N] \backslash A_0$ and $B_1 = [1, N] \backslash B_0$. For $t = 0, 1$ and $\tau = 0, 1$, define $A_{t,\tau} = A_t \cap B_\tau$. Note that for large $N$, $2^{-N^\beta} < 1 - 2^{-N^\beta}$ and therefore, Lemma VI.30 implies $A_{1,0} = \emptyset$. Note that the above polarization results imply that as $N$ increases, $\frac{|A_1|}{N} \to \bar{I}(W_c)$ and $\frac{|B_\tau|}{N} \to \bar{I}(W_s)$.

### Encoding and Decoding

Let $z_1^N \in \mathbf{G}^N$ be an outcome of the random variable $Z_1^N$ known to both the encoder and the decoder. Given a source sequence $x_1^N \in \mathscr{X}^N$, the encoding rule is as follows: For $i \in [1, N]$, if $i \in B_0$, then $v_i$ is uniformly distributed over $\mathbf{G}$ and is known to both the encoder and the decoder (and is independent from other random variables). If $i \in B_1$, $v_i = g$ for some $g \in \mathbf{G}$ with probability

$$P(v_i = g) = p_{V_i | X_1^N Z_1^N V_1^{i-1}}(g | x_1^N, z_1^N, v_1^{i-1})$$

Note that $[1, N]$ can be partitioned into $A_{0,0}, A_{0,1}$ and $A_{1,1}$ (since $A_{1,0}$ is empty) and $B_0 = A_{0,0}$, $B_1 = A_{0,1} \cup A_{1,1}$. Therefore, $v\_1^N$ can be decompose as $v_1^N = v_{A_{0,0}} + v_{A_{0,1}} + v_{A_{1,1}}$ in which $v_{A_{0,0}}$ is known to the decoder. The encoder sends $v_{A_{0,1}}$ to the decoder and the decoder uses the channel code to recover $v_{A_{1,1}}$. The decoding rule is as follows: Given $z_1^N$, $v_{A_{0,0}}$ and $v_{A_{0,1}}$, let $\hat{v}_{A_{0,0}} = v_{A_{0,0}}$ and $\hat{v}_{A_{0,1}} = v_{A_{0,1}}$. For

$i \in A_{1,1}$, let

$$\hat{v}_i = \underset{g \in G}{\operatorname{argmax}} \, W_{c,N}^{(i)}(z_1^N, \hat{v}_1^{i-1} | g)$$

Finally, the decoder outputs $z_1^N - \hat{v}_1^N G$.

**Error Analysis**

The analysis is a combination of the-point-to point channel coding and source coding results for polar codes. The average distortion between the encoder input and the decoder output is upper bounded by

$$D_{avg} \leq \sum_{z_1^N \in \mathbf{G}^N} \frac{1}{q^N} \sum_{x_1^N \in \mathscr{X}^N} p_X^N(x_1^N) \sum_{v_1^N \in \mathbf{G}^N} \frac{1}{q^{|B_0|}} \left( \prod_{i \in B_1} p(v_i | x_1^N, z_1^N, v_1^{i-1}) \right) \Big( d_{max} \cdot \mathbb{1}_{\{\hat{v} \neq v\}} + d(x_1^N, z_1^N - v_1^N G) \Big)$$

where we have replaced $p_{V_i|X_1^N Z_1^N V_1^{i-1}}(v_i | x_1^N, z_1^N, v_1^{i-1})$ with $p(v_i | x_1^N, z_1^N, v_1^{i-1})$ for simplicity of notation and $d_{max}$ is the maximum value of the $d(\cdot, \cdot)$ function. Let $q(x_1^N, z_1^N) = p(x_1^N, z_1^N)$ and

$$q(v_i | x_1^N z_1^N v_1^{i-1}) = \begin{cases} \frac{1}{2} & \text{If } i \in B_0 \\ p_{V_i|X_1^N Z_1^N V_1^{i-1}}(v_i | x_1^N z_1^N v_1^{i-1}) & \text{If } i \in B_1 \end{cases}$$

It is shown in [63] that we have $D_{avg} \leq D_1 + D_2 + D_3$ where

$$D_1 = \sum_{\substack{v_1^N, z_1^N \in \mathbf{G}^N \\ x_1^N \in \mathscr{X}^N}} p(v_1^N, x_1^N, z_1^N) d_{max} \cdot \mathbb{1}_{\{\hat{v} \neq v\}} \tag{6.34}$$

$$D_2 = \sum_{\substack{v_1^N, z_1^N \in \mathbf{G}^N \\ x_1^N \in \mathscr{X}^N}} p(v_1^N, x_1^N, z_1^N) d(x_1^N, z_1^N - v_1^N G) \tag{6.35}$$

$$D_3 = \sum_{\substack{v_1^N, z_1^N \in \mathbf{G}^N \\ x_1^N \in \mathscr{X}^N}} \left| q(v_1^N, x_1^N, z_1^N) - p(v_1^N, x_1^N, z_1^N) \right| \Big( d_{max} \cdot \mathbb{1}_{\{\hat{v} \neq v\}} + d(x_1^N, z_1^N - v_1^N G) \Big) \tag{6.36}$$

The proof proceeds as follows: It is straightforward to show that $D_1 \to D$ as $N$ increases. It can also be shown that $D_2 \to 0$ as $N$ increases since the inner code is a good channel code. Finally, it can be shown that $D_3 \to 0$ as $N$ increases since the total variation distance between the $P$ and the $Q$ measures is small (in turn since the outer code is a good source code). For the complete proof, please see [63].

#### 6.3.1.3 Source Coding: Proof for the General Case

The result of channel polarization for arbitrary discrete memoryless channels applied to $W_c$ implies [62] that for any $\epsilon > 0$ and $0 < \beta < \frac{1}{2}$, there exist a large $N = 2^n$ and a partition $\{A_H | H \leq \mathbf{G}\}$ of $[1, N]$ such that for $H \leq \mathbf{G}$ and $i \in A_H$, $\left|\bar{I}(W_{c,N}^{(i)}) - \log \frac{|\mathbf{G}|}{|H|}\right| < \epsilon$ and $Z^H(W_{c,N}^{(i)}) < 2^{-N^\beta}$. Moreover, as $\epsilon \to 0$ (and $N \to \infty$), $\frac{|A_H|}{N} \to p_H$ for some probabilities $p_H, H \leq \mathbf{G}$ adding up to one with $\sum_{H \leq \mathbf{G}} p_H \log \frac{|\mathbf{G}|}{|H|} = \bar{I}(W_c)$.

Similarly, for the channel $W_s$ we have the following: For any $\epsilon > 0$ and $0 < \beta < \frac{1}{2}$, there exist a large $N = 2^n$ and a partition $\{B_H | H \leq \mathbf{G}\}$ of $[1, N]$ such that for $H \leq \mathbf{G}$ and $i \in B_H$, $\left|\bar{I}(W_{s,N}^{(i)}) - \log \frac{|\mathbf{G}|}{|H|}\right| < \epsilon$ and $Z^H(W_{s,N}^{(i)}) < 2^{-N^\beta}$. Moreover, as $\epsilon \to 0$ (and $N \to \infty$), $\frac{|B_H|}{N} \to q_H$ for some probabilities $q_H, H \leq \mathbf{G}$ adding up to one with $\sum_{H \leq \mathbf{G}} q_H \log \frac{|\mathbf{G}|}{|H|} = \bar{I}(W_s)$.

**Lemma VI.31.** *For $i = 1, \cdots, N$ and for $d \in \mathbf{G}$ and $H \leq \mathbf{G}$, $Z_d(W_{c,N}^{(i)}) \geq Z_d(W_{s,N}^{(i)})$ and $Z^H(W_{c,N}^{(i)}) \geq Z^H(W_{s,N}^{(i)})$.*

*Proof.* Provided in a more complete version [63]. □

We define some quantities before we introduce the encoding and decoding rules.

For $H \leq \mathbf{G}$, define

$$A_H = \Big\{ i \in [1,N] \Big| Z^H(W_{c,N}^{(i)}) < 2^{-N^\beta}, \\ \nexists K \leq H \text{such that } Z^K(W_{c,N}^{(i)}) < 2^{-N^\beta} \Big\}$$

$$B_H = \Big\{ i \in [1,N] \Big| Z^H(W_{s,N}^{(i)}) < 1 - 2^{-N^\beta}, \\ \nexists K \leq H \text{ such that } Z^K(W_{s,N}^{(i)}) < 1 - 2^{-N^\beta} \Big\}$$

For $H \leq \mathbf{G}$ and $K \leq \mathbf{G}$, define $A_{H,K} = A_H \cap B_K$. Note that for large $N$, $2^{-N^\beta} < 1 - 2^{-N^\beta}$ and therefore, if for some $i \in [1,N]$, $i \in A_H$, Lemma VI.31 implies $Z^H(W_{s,N}^{(i)}) < 1 - 2^{-N^\beta}$ and hence $i \in \cup_{K \leq H} B_K$. Therefore, for $K \not\leq H$, $A_{H,K} = \emptyset$. Therefore $\{A_{H,K} | K \leq H \leq \mathbf{G}\}$ is a partition of $[1,N]$. Note that the channel polarization results imply that as $N$ increases, $\frac{|A_H|}{N} \to p_H$ and $\frac{|B_H|}{N} \to q_H$.

**Encoding and Decoding**

Let $z_1^N \in \mathbf{G}^N$ be an outcome of the random variable $Z_1^N$ known to both the encoder and the decoder. Given $K \leq H \leq \mathbf{G}$, let $T_H$ be a transversal of $H$ in $\mathbf{G}$ and let $T_{K \leq H}$ be a transversal of $K$ in $H$. Any element $g$ of $\mathbf{G}$ can be represented by $g = [g]_K + [g]_{T_{K \leq H}} + [g]_{T_H}$ for unique $[g]_K \in K$, $[g]_{T_{K \leq H}} \in T_{K \leq H}$ and $[g]_{T_H} \in T_H$. Also note that $T_{K \leq H} + T_H$ is a transversal $T_K$ of $K$ in $\mathbf{G}$ so that $g$ can be uniquely represented by $g = [g]_K + [g]_{T_K}$ for some $[g]_{T_K} \in T_K$ and $[g]_{T_K}$ can be uniquely represented by $[g]_{T_K} = [g]_{T_{K \leq H}} + [g]_{T_H}$.

Given a source sequence $x_1^N \in \mathscr{X}^N$, the encoding rule is as follows: For $i \in [1,N]$, if $i \in A_{H,K}$ for some $K \leq H \leq \mathbf{G}$, $[v_i]_K$ is uniformly distributed over $K$ and is known to both the encoder and the decoder (and is independent from other random variables). The component $[v_i]_{T_K}$ is chosen randomly so that for $g \in [v_i]_K + T_K$,

$$P(v_i = g) = \frac{p_{V_i | X_1^N Z_1^N V_1^{i-1}}(g | x_1^N, z_1^N, v_1^{i-1})}{p_{V_i | X_1^N Z_1^N V_1^{i-1}}([v_i]_K + T_K | x_1^N, z_1^N, v_1^{i-1})}$$

Note that $v_1^N$ can be decomposed as $v_1^N = [v_1^N]_K + [v_1^N]_{T_{K\leq H}} + [v_1^N]_{T_H}$ (with a slight abuse of notation since $K$ and $H$ depend on the index $i$) in which $[v_1^N]_K$ is known to the decoder. The encoder sends $[v_1^N]_{T_{K\leq H}}$ to the decoder and the decoder uses the channel code to recover $[v_1^N]_{T_H}$. The decoding rule is as follows: Given $z_1^N$, $[v_1^N]_K$ and $[v_1^N]_{T_{K\leq H}}$, and for $i \in A_{H,K}$, let

$$\hat{v}_i = \underset{g\in[v_i]_K+[v_i]_{T_{K\leq H}}+T_H}{\operatorname{argmax}} W_{c,N}^{(i)}(z_1^N, \hat{v}_1^{i-1}|g)$$

Finally, the decoder outputs $z_1^N - \hat{v}_1^N G$. Note that the rate of this code is equal to

$$\begin{aligned} R &= \sum_{K\leq H\leq \mathbf{G}} \frac{|A_{H,K}|}{N} \log \frac{|H|}{|K|} \\ &= \sum_{K\leq H\leq \mathbf{G}} \frac{|A_{H,K}|}{N} \log \frac{|\mathbf{G}|}{|K|} - \sum_{K\leq H\leq \mathbf{G}} \frac{|A_{H,K}|}{N} \log \frac{|\mathbf{G}|}{|H|} \\ &\to \bar{I}(W_s) - \bar{I}(W_c) = I(X;U) \end{aligned}$$

**Error Analysis**

The average distortion between the encoder input and the decoder output is upper bounded by

$$\begin{aligned} D_{avg} \leq \sum_{z_1^N\in\mathbf{G}^N} \frac{1}{q^N} \sum_{x_1^N\in\mathscr{X}^N} p_X^N(x_1^N) \sum_{v_1^N\in\mathbf{G}^N} \frac{1}{q^{|B_0|}} \\ \left(\prod_{K\leq\mathbf{G}} \prod_{i\in B_K} \frac{p(g|x_1^N, z_1^N, v_1^{i-1})}{p([v_i]_K + T_K|x_1^N, z_1^N, v_1^{i-1}) \cdot |K|}\right) \\ \left(d_{max} \cdot \mathbb{1}_{\{\hat{v}\neq v\}} + d(x_1^N, z_1^N - v_1^N G)\right) \end{aligned}$$

where $p_{V_i|X_1^N Z_1^N V_1^{i-1}}(\cdot|x_1^N, z_1^N, v_1^{i-1})$ is replaced with $p(\cdot|x_1^N, z_1^N, v_1^{i-1})$ for simplicity of notation. The rest of the proof is essentially similar to the binary case. For the complete proof, please see [63].

### 6.3.2 The Channel Coding Problem

In this section, we prove the following theorem:

**Theorem VI.32.** *For an arbitrary discrete memoryless channel $(\mathscr{X}, \mathscr{Y}, W)$, nested polar codes achieve the Shannon capacity.*

For the channel let $\mathscr{X} = \mathbf{G}$ for some Abelian group $\mathbf{G}$ and let $|\mathbf{G}| = q$. Similarly to the source coding problem, we show that there exists nested polar code $\mathbb{C}_i \subseteq \mathscr{C}_o$ such that $\mathbb{C}_o$ is a good channel code and each shift of $\mathbb{C}_i$ is a good source code. This will be made clear later in the following.

Let $X$ be a random variable with the capacity achieving distribution and let $U$ be uniformly distributed over $\mathbf{G}$. Define the artificial channels $(\mathbf{G}, \mathbf{G}, W_s)$ and $(\mathbf{G}, \mathscr{Y} \times \mathbf{G}, W_c)$ such that for $u, z \in \mathbf{G}$ and $y \in \mathscr{Y}$, $W_s(z|u) = p_X(z-u)$ and $W_c(y, z|u) = p_{XY}(z-u, y)$. These channels have been depicted in Figures 6.10 and 6.11.

Note that for $u, x, z \in G$ and $y \in \mathscr{Y}$, $p_{UXYZ}(u, x, y, z) = p_U(u)p_X(x)W(y|x)\mathbb{1}_{\{z=u+x\}}$. Similarly to the source coding case, one can show that the symmetric capacities of the channels are equal to $\bar{I}(W_s) = \log q - H(X)$ and $\bar{I}(W_c) = \log q - H(X|Y)$. We employ a nested polar code in which the inner code is a good source code for the test channel $W_s$ and the outer code is a good channel code for $W_c$. The rate of this code is equal to $R = \bar{I}(W_c) - \bar{I}(W_x) = I(X;Y)$. We only present our encoding and decoding rules here. The proofs can be found in [63]. To introduce our encoding and decoding rules, we need to make some definitions.

Let $n$ be a positive integer and let $N = 2^n$. Similar to the source coding case, for $i = 1 \cdots N$, define the synthesized channels $W_{c,N}^{(i)}$ and $W_{s,N}^{(i)}$. Let the random vector $U_1^N$ be distributed according to $p_U^N$ (uniform) and let $V_1^N = U_1^N G^{-1}$ where $G$ is the polar coding matrix of dimension $N \times N$. Note that since $G$ is a one-to-one mapping, $V_1^N$ is also uniformly distributed. Let $Y_1^N$ and $Z_1^N$ be the outputs of the channel $W_c$

when the input is $U_1^N$. For $H \leq \mathbf{G}$, define

$$A_H = \Big\{ i \in [1,N] \Big| Z^H(W_{s,N}^{(i)}) < 1 - 2^{-N^\beta}, \\ \nexists K \leq H \text{such that } Z^K(W_{s,N}^{(i)}) < 1 - 2^{-N^\beta} \Big\}$$

$$B_H = \Big\{ i \in [1,N] \Big| Z^H(W_{c,N}^{(i)}) < 2^{-N^\beta}, \\ \nexists K \leq H \text{ such that } Z^K(W_{c,N}^{(i)}) < 2^{-N^\beta} \Big\}$$

For $H \leq \mathbf{G}$ and $K \leq \mathbf{G}$, define $A_{H,K} = A_H \cap B_K$. Note that for $K \leq H \leq \mathbf{G}$, $Z^H(W) \leq Z^K(W)$. Also note that $Z^H(W_{c,N}^{(i)}) \leq Z^H(W_{s,N}^{(i)})$ Therefore, if $K \not\leq H$ then

$$A_{H,K} \subseteq \Big\{ i \in [1,N] \Big| 2^{-N^\beta} < Z^H(W_{c,N}^{(i)}) \leq \\ Z^H(W_{s,N}^{(i)}) < 1 - 2^{-N^\beta} \Big\}$$

Since $Z^H(W_{c,N}^{(i)})$ and $Z^H(W_{s,N}^{(i)})$ both polarize to $0, 1$, as $N$ increases $\frac{A_{H,K}}{N} \to 0$ if $K \not\leq H$. Note that the channel polarization results imply that as $N$ increases, $\frac{|A_H|}{N} \to p_H$ and $\frac{|B_H|}{N} \to q_H$.

The encoding and decoding rules are as follows: Let $z_1^N \in \mathbf{G}^N$ be an outcome of the random variable $Z_1^N$ known to both the encoder and the decoder. Given $K \leq H \leq \mathbf{G}$, let $T_H$ be a transversal of $H$ in $\mathbf{G}$ and let $T_{K \leq H}$ be a transversal of $K$ in $H$. Any element $g$ of $\mathbf{G}$ can be represented by $g = [g]_K + [g]_{T_{K \leq H}} + [g]_{T_H}$ for unique $[g]_K \in K$, $[g]_{T_{K \leq H}} \in T_{K \leq H}$ and $[g]_{T_H} \in T_H$. Also note that $T_{K \leq H} + T_H$ is a transversal $T_K$ of $K$ in $\mathbf{G}$ so that $g$ can be uniquely represented by $g = [g]_K + [g]_{T_K}$ for some $[g]_{T_K} \in T_K$ and $[g]_{T_K}$ can be uniquely represented by $[g]_{T_K} = [g]_{T_{K \leq H}} + [g]_{T_H}$.

Given a source sequence $x_1^N \in \mathscr{X}^N$, the encoding rule is as follows: For $i \in [1,N]$, if $i \in A_{H,K}$ for some $K \leq H \leq \mathbf{G}$, $[v_i]_K$ is uniformly distributed over $K$ and is known to both the encoder and the decoder (and is independent from other random variables). The component $[v_i]_{T_{K \leq H}}$ is the message and is uniformly distributed but is only known to the encoder. The component $[v_i]_{T_K}$ is chosen randomly so that for

$g \in [v_i]_K + [v_i]_{T_{K \leq H}} + T_H$,

$$P(v_i = g) = \frac{p_{V_i|X_1^N Z_1^N V_1^{i-1}}(g|x_1^N, z_1^N, v_1^{i-1})}{p_{V_i|X_1^N Z_1^N V_1^{i-1}}([v_i]_K + [v_i]_{T_{K \leq H}} + T_H|x_1^N, z_1^N, v_1^{i-1})}$$

For $i \in [1, N]$, if $i \in A_{H,K}$ for some $K \not\leq H$, $[v_i]_H$ is uniformly distributed over $H$ and is known to both the encoder and the decoder and the component $[v_i]_{T_H}$ is chosen randomly so that for $g \in [v_i]_H + T_H$,

$$P(v_i = g) = \frac{p_{V_i|X_1^N Z_1^N V_1^{i-1}}(g|x_1^N, z_1^N, v_1^{i-1})}{p_{V_i|X_1^N Z_1^N V_1^{i-1}}([v_i]_H + T_H|x_1^N, z_1^N, v_1^{i-1})}$$

For the moment assume that in this case $v_i$ is known at the receiver. Note that for $i \in [1, N]$, if $i \in A_{H,K}$ for some $K \leq H \leq \mathbf{G}$, $v_i$ can be decomposed as $v_i = [v_i]_K + [v_i]_{T_{K \leq H}} + [v_i]_{T_H}$ in which $[v_i]_K$ is known to the decoder. The decoding rule is as follows: Given $z_1^N$ and for $i \in A_{H,K}$ for some $K \leq H \leq \mathbf{G}$, let

$$\hat{v}_i = \underset{g \in [v_i]_K + [v_i]_{T_{K \leq H}} + T_H}{\operatorname{argmax}} W_{c,N}^{(i)}(z_1^N, \hat{v}_1^{i-1}|g)$$

It is shown in [63] that with this encoding and decoding rules, the probability of error goes to zero. It remains to send the $v_i$ $i \in A_{H,K}$ with $K \not\leq H$ to the decoder which can be done using a regular polar code (which achieves the symmetric capacity of the channel). Note that since the fraction $\frac{|A_{H,K}|}{N}$ vanishes as $N$ increases if $K \not\leq H$, the rate loss due to this transmission can be made arbitrarily small.

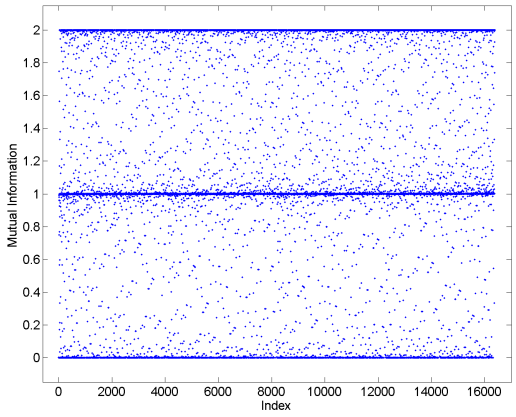


Figure 6.2: The behavior of $I(W^{b_1 b_2 \cdots b_n})$ for $n = 14$ for Channel 1 when $\epsilon = 0.4$ and $\lambda = 0.2$. The three solid lines represent the three discrete values of $I^\infty$ with positive probability.

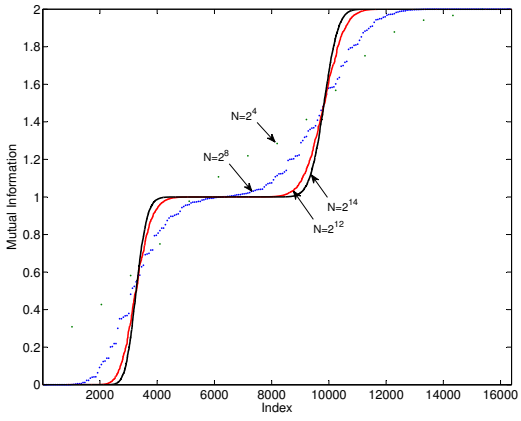


Figure 6.3: The asymptotic behavior of $I(W^{b_1 b_2 \cdots b_n})$, $N = 2^n = 2^4, 2^8, 2^{12}, 2^{14}$ for Channel 1 when the data is sorted. We observe that for this channel, all three extreme cases appear with positive probability. In general, it is possible to have fewer cases in the asymptotic regime.

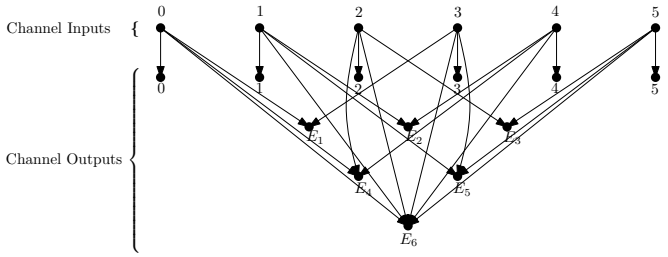


Figure 6.4: Channel 2: A channel with a composite input alphabet size. For this channel, the process $I^n$ can be explicitly found for each $n$ and the multilevel polarization can be observed. $E_1$, $E_2$ and $E_3$ are erasures corresponding to cosets of the subgroup $\{0, 3\}$ and $E_4$ and $E_5$ are erasures corresponding to cosets of the subgroup $\{0, 2, 4\}$. The lines connected to outputs $E_1, E_2$ and $E_3$ correspond to a conditional probability of $\gamma$, the lines connected to outputs $E_4$ and $E_5$ correspond to a conditional probability of $\epsilon$, the lines connected to the output $E_6$ correspond to a conditional probability of $\lambda$, and the lines connected to outputs $0, 1, 2, 3, 4$ and $5$ correspond to a conditional probability of $1-\gamma-\epsilon-\lambda$. The parameters $\gamma, \epsilon, \lambda$ take values from $[0, 1]$ such that $\gamma + \epsilon + \lambda \leq 1$.

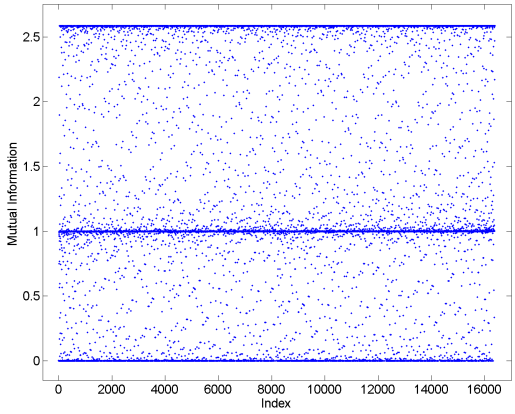


Figure 6.5: Polarization of Channel 2 with parameters $\gamma = 0, \epsilon = 0.4, \lambda = 0.2$. The middle line represents the subgroup $\{0, 2, 4\}$ of $\mathbb{Z}_6$.

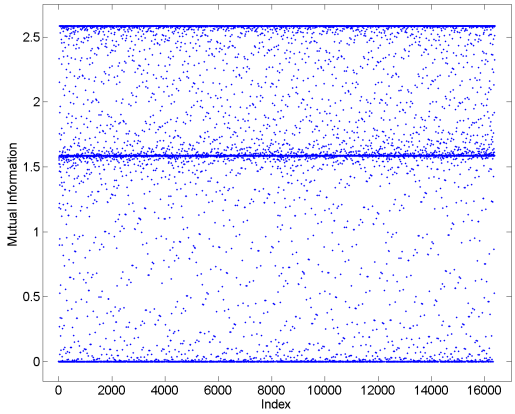


Figure 6.6: Polarization of Channel 2 with parameters $\gamma = 0.4, \epsilon = 0, \lambda = 0.2$. The middle line represents the subgroup $\{0, 3\}$ of $\mathbb{Z}_6$.

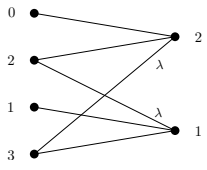


Figure 6.7: Channel 3

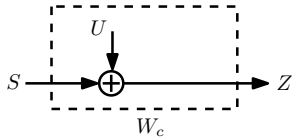


Figure 6.8: Source Coding: Test channel for the inner code (the channel coding component).

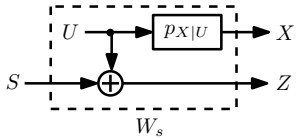


Figure 6.9: Source Coding: Test channel for the outer code (the source coding component).

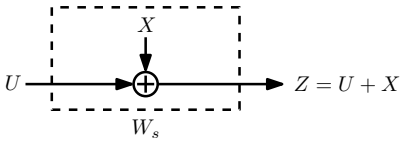


Figure 6.10: Channel Coding: Channel for the inner code.

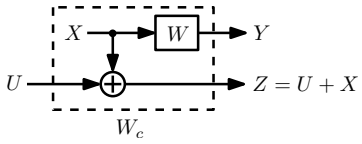


Figure 6.11: Channel Coding: Channel for the outer code.

# CHAPTER VII

# Polar Codes for Multi-terminal Communications

In this section, we show that polar coding schemes achieve the known achievable rate regions for several multi-terminal communications problems including lossy distributed source coding, multiple access channels, broadcast channels and multiple description.

## 7.1 Introduction

Among the existing works on the application of polar codes for multi-terminal cases we note [11, 12] for distributed source coding, [5, 67] for the multiple access channels and [32] for broadcast channels.

In Section 6.1.1.1, we showed that nested polar codes can be used to achieve the Shannon capacity of arbitrary discrete memoryless channels and the Shannon rate-distortion function for discrete memoryless sources [64]. In this chapter, we show that nested polar codes can achieve the best known achievable rate regions for several multi-terminal communication systems. We present several examples in this chapter, including the distributed source coding problem, multiple access channels, computation over MAC, broadcast channels, multiple description coding, to illustrate how these codes can be employed to have an optimal performance for multi-terminal

cases. The results of this chapter are general regarding the size of alphabets using the approach of [62].

## 7.2 Distributed Source Coding: The Berger-Tung Problem

In the distributed source coding problem, two separate sources $X$ and $Y$ communicates with a centralized decoder. Let $\mathscr{X}, \mathscr{Y}$ and $\mathscr{U}, \mathscr{V}$ be the source and the reconstruction alphabets of the two terminals and assume $X$ and $Y$ have the joint distribution $p_{XY}$. Let $d_1 : \mathscr{X} \times \mathscr{U} \to \mathbb{R}^+$ and $d_2 : \mathscr{Y} \times \mathscr{V} \to \mathbb{R}^+$ be the distortion measures for terminals $X$ and $Y$ respectively. We denote this source by $(\mathscr{X}, \mathscr{Y}, \mathscr{U}, \mathscr{V}, p_{XY}, d_1, d_2)$. Let $U$ and $V$ be auxiliary random variables taking values from $\mathscr{U}$ and $\mathscr{V}$ respectively such that $U \leftrightarrow X \leftrightarrow Y \leftrightarrow V$, $\mathbb{E}\{d_1(X,U)\} \leq D_1$ and $\mathbb{E}\{d_2(Y,V)\} \leq D_2$ for some distortion levels $D_1, D_2 \in \mathbb{R}^+$. It is known by the Berger-Tung coding scheme that the tuple $(R_1, R_2, D_1, D_2)$ is achievable if

$$\begin{cases} R_1 \geq I(X;U) - I(U;V) \\ R_2 \geq I(Y;V) - I(U;V) \\ R_1 + R_2 \geq I(X;U) + I(Y;V) - I(U;V) \end{cases}$$

In this section, we prove the following theorem:

**Theorem VII.1.** *For a source $(\mathscr{X}, \mathscr{Y}, \mathscr{U}, \mathscr{V}, p_{XY}, d_1, d_2)$, assume $\mathscr{U}$ and $\mathscr{V}$ are finite. Then the Berger-Tung rate region is achievable using nested polar codes.*

It suffices to show that the following rates are achievable:

$$R_1 = I(X;U) - I(U;V), \quad R_2 = I(Y;V)$$

Let $\mathbf{G}$ be an Abelian group of the size larger than or equal to the size of both $\mathscr{U}$ and $\mathscr{V}$. Note that for the source $Y$, we can use a nested polar codes as introduced in [64] to achieve the rate $I(Y;V)$. Furthermore, we have access to the outcome $v_1^N$ of $V_1^N$ at the decoder with high probability. It remains to show that

the rate $R_1 = I(X;U) - I(U;V)$ is achievable when the sequence $v_1^N \in \mathbf{G}^N$ with $d_2(y_1^N, v_1^N) \leq D_2$ is available at the decoder.

Given the test channel $p_{X|U}$, define the artificial channels $(\mathbf{G}, \mathbf{G}^2, W_c)$ and $(\mathbf{G}, \mathscr{X} \times \mathbf{G}, W_s)$ such that for $s, z \in \mathbf{G}$ and $x \in \mathscr{X}$,

$$W_c(v, z|s) = p_{VU}(v, z - s), \quad W_s(x, z|s) = p_{XU}(x, z - s)$$

These channels have been depicted in Figures 7.1 and 7.2. Let $S$ be a random variable

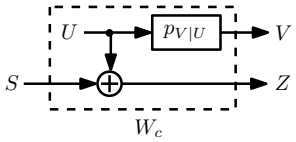


Figure 7.1: Distributed Source Coding: Test channel for the inner code (the channel coding component).

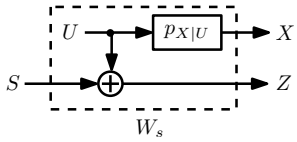


Figure 7.2: Distributed Source Coding: Test channel for the outer code (the source coding component).

uniformly distributed over $\mathbf{G}$ which is independent from $X$ and $U$. It is straightforward to show that in this case, $Z$ is also uniformly distributed over $\mathbf{G}$. Similarly to the point-to-point result [64], we can show that the symmetric capacities of the channels $W_c$ and $W_s$ are given by $\bar{I}(W_c) = \log q - H(U|V)$ and $\bar{I}(W_s) = \log q - H(U|X)$. We employ a nested polar code in which the inner code is a good channel code for the channel $W_c$ and the outer code is a good source code for $W_s$. The rate of this code is equal to $R = \bar{I}(W_s) - \bar{I}(W_c) = I(X;U) - I(U;V)$. The rest of this section is devoted to some general definitions and lemmas which are used in the proofs.

**Lemma VII.2.** *The channel $W_c$ is degraded with respect to the channel $W_s$ in the sense of [63, Definition III.1].*

*Proof.* In the Definition [63, Definition III.1], let the channel $(\mathscr{X} \times \mathbf{G}, \mathbf{G}^2, W)$ be such that for $v, z, z' \in \mathbf{G}$ and $x \in \mathscr{X}$, $W(v, z|x, z') = p_{V|X}(v|x)\mathbb{1}_{\{z=z'\}}$. □

Let $N = 2^n$ for some positive integer $n$ and let $G$ be the corresponding $N \times N$ generator matrix for polar codes. For $i = 1, \cdots, N$, and for $z_1^N, a_1^N \in \mathbf{G}^N$, $v_1^N \in \mathscr{V}^N$

and $x_1^N \in \mathscr{X}^N$, let

$$W_{c,N}^{(i)}(z_1^n, v_1^N, a_1^{i-1}|a_i) = \sum_{a_{i+1}^N \in \mathbf{G}^{N-i}} \frac{1}{q^{N-1}} W_c^N(z_1^N, v_1^N|a_1^N G)$$
$$W_{s,N}^{(i)}(x_1^N, z_1^n, a_1^{i-1}|a_i) = \sum_{a_{i+1}^N \in \mathbf{G}^{N-i}} \frac{1}{q^{N-1}} W_s^N(x_1^N, z_1^N|a_1^N G)$$

Let the random vectors $X_1^N, Y_1^N, U_1^N, V_1^N$ be distributed according to $P_{XYUV}^N$ and let $Z_1^N$ be a random variable uniformly distributed over $\mathbf{G}^N$ which is independent of $X_1^N, Y_1^N, U_1^N, V_1^N$. Let $S_1^N = Z_1^N - U_1^N$ and $A_1^N = S_1^N G^{-1}$ (Here, $G^{-1}$ is the inverse of the mapping $G : \mathbf{G}^N \to \mathbf{G}^N$). In other words, the joint distribution of the random vectors is given by

$$p_{A_1^N S_1^N U_1^N V_1^N X_1^N Z_1^N}(a_1^N, s_1^N, u_1^N, v_1^N, x_1^N, z_1^N)$$
$$= \frac{1}{q^N} p_{XUV}^N(x_1^N, u_1^N, v_1^N) \mathbb{1}_{\{s_1^N = a_1^N G, u_1^n = z_1^N - a_1^N G\}}$$

**8**

Sketch of the proof The following theorems state the standard channel coding and source coding polarization phenomenons for the general case.

**Theorem VII.3.** *For any $\epsilon > 0$ and $0 < \beta < \frac{1}{2}$, there exist a large $N = 2^n$ and a partition $\{A_H | H \leq \mathbf{G}\}$ of $[1, N]$ such that for $H \leq \mathbf{G}$ and $i \in A_H$, $\left|\bar{I}(W_{c,N}^{(i)}) - \log \frac{|\mathbf{G}|}{|H|}\right| < \epsilon$ and $Z^H(W_{c,N}^{(i)}) < 2^{-N^\beta}$. Moreover, as $\epsilon \to 0$ (and $N \to \infty$), $\frac{|A_H|}{N} \to p_H$ for some probabilities $p_H, H \leq \mathbf{G}$ adding up to one with $\sum_{H \leq \mathbf{G}} p_H \log \frac{|\mathbf{G}|}{|H|} = \bar{I}(W_c)$.*

**Theorem VII.4.** *For any $\epsilon > 0$ and $0 < \beta < \frac{1}{2}$, there exist a large $N = 2^n$ and a partition $\{B_H | H \leq \mathbf{G}\}$ of $[1, N]$ such that for $H \leq \mathbf{G}$ and $i \in A_H$, $\left|\bar{I}(W_{s,N}^{(i)}) - \log \frac{|\mathbf{G}|}{|H|}\right| < \epsilon$ and $Z^H(W_{s,N}^{(i)}) < 2^{-N^\beta}$. Moreover, as $\epsilon \to 0$ (and $N \to \infty$), $\frac{|B_H|}{N} \to q_H$ for some probabilities $q_H, H \leq \mathbf{G}$ adding up to one with $\sum_{H \leq \mathbf{G}} q_H \log \frac{|\mathbf{G}|}{|H|} = \bar{I}(W_s)$.*

For $H \leq \mathbf{G}$, define

$$A_H = \Big\{ i \in [1,N] \Big| Z^H(W_{c,N}^{(i)}) < 2^{-N^\beta}, \\ \nexists K \leq H : Z^K(W_{c,N}^{(i)}) < 2^{-N^\beta} \Big\}$$

$$B_H = \Big\{ i \in [1,N] \Big| Z^H(W_{s,N}^{(i)}) < 1 - 2^{-N^\beta}, \\ \nexists K \leq H : Z^K(W_{c,N}^{(i)}) < 1 - 2^{-N^\beta} \Big\}$$

For $H \leq \mathbf{G}$ and $K \leq \mathbf{G}$, define $A_{H,K} = A_H \cap B_K$. Note that for large $N$, $2^{-N^\beta} < 1 - 2^{-N^\beta}$. This implies for $i \in A_H$, we have $Z^H(W_{s,N}^{(i)}) < 1 - 2^{-N^\beta}$ and hence $i \in \cup_{K \leq H} B_K$. Therefore, for $K \not\leq H$, we have $A_{H,K} = \emptyset$. This means $\{A_{H,K} | K \leq H \leq \mathbf{G}\}$ forms a partition of $[1,N]$. Note that as $N$ increases, $\frac{|A_H|}{N} \to p_H$ and $\frac{|B_H|}{N} \to q_H$.

The encoding and decoding rules are as follows: Let $z_1^N \in \mathbf{G}^N$ be an outcome of the random variable $Z_1^N$ known to both the encoder and the decoder. Given $K \leq H \leq \mathbf{G}$, let $T_H$ be a transversal of $H$ in $\mathbf{G}$ and let $T_{K \leq H}$ be a transversal of $K$ in $H$. Any element $g$ of $\mathbf{G}$ can be represented by $g = [g]_K + [g]_{T_{K \leq H}} + [g]_{T_H}$ for unique $[g]_K \in K$, $[g]_{T_{K \leq H}} \in T_{K \leq H}$ and $[g]_{T_H} \in T_H$. Also note that $T_{K \leq H} + T_H$ is a transversal $T_K$ of $K$ in $\mathbf{G}$ so that $g$ can be uniquely represented by $g = [g]_K + [g]_{T_K}$ for some $[g]_{T_K} \in T_K$ and $[g]_{T_K}$ can be uniquely represented by $[g]_{T_K} = [g]_{T_{K \leq H}} + [g]_{T_H}$.

Given a source sequence $x_1^N \in \mathscr{X}^N$, the encoding rule is as follows: For $i \in [1,N]$, if $i \in A_{H,K}$ for some $K \leq H \leq \mathbf{G}$, $[a_i]_K$ is uniformly distributed over $K$ and is known to both the encoder and the decoder (and is independent from other random variables). The component $[a_i]_{T_K}$ is chosen randomly so that for $g \in \mathbf{G}$,

$$P(a_i = g) = \frac{p_{A_i | X_1^N Z_1^N A_1^{i-1}}(g | x_1^N, z_1^N, a_1^{i-1})}{p_{A_i | X_1^N Z_1^N A_1^{i-1}}([a_i]_K + T_K | x_1^N, z_1^N, a_1^{i-1})}$$

Note that $a_1^N$ can be decomposed as $a_1^N = [v_1^N]_K + [a_1^N]_{T_{K \leq H}} + [a_1^N]_{T_H}$ in which $[a_1^N]_K$ is known to the decoder. The encoder sends $[a_1^N]_{T_{K \leq H}}$ to the decoder and the decoder

uses the channel code to recover $[a_1^N]_{T_H}$. The decoding rule is as follows: Given $z_1^N$, $v_1^N$, $[a_1^N]_K$ and $[a_1^N]_{T_{K\leq H}}$, and for $i \in A_{H,K}$, let

$$\hat{a}_i = \underset{g\in[a_i]_K+[a_i]_{T_{K\leq H}}+T_H}{\operatorname{argmax}} W_{c,N}^{(i)}(z_1^N, v_1^N, \hat{a}_1^{i-1}|g)$$

Finally, the decoder outputs $z_1^N - \hat{a}_1^N G$. Note that the rate of this code is equal to

$$\begin{aligned} R &= \sum_{K\leq H\leq \mathbf{G}} \frac{|A_{H,K}|}{N} \log \frac{|H|}{|K|} \\ &= \sum_{K\leq H\leq \mathbf{G}} \frac{|A_{H,K}|}{N} \log \frac{|\mathbf{G}|}{|K|} - \sum_{K\leq H\leq \mathbf{G}} \frac{|A_{H,K}|}{N} \log \frac{|\mathbf{G}|}{|H|} \\ &\to \bar{I}(W_s) - \bar{I}(W_c) = I(X;U) - I(U;V) \end{aligned}$$

## 7.3 Distributed Source Coding: Decoding the Sum of Variables

For a distributed source $(\mathscr{X} \times \mathscr{Y}, p_{X,Y})$ let the random variable $U$ and $V$ take values from a group $\mathbf{G}$. Assume that $U$ and $V$ satisfy the Markov chain $U \leftrightarrow X \leftrightarrow Y \leftrightarrow V$ and assume $\mathbb{E}\{d(X,Y,g(U+V)) \leq D\}$ for some function $g$. For $W = U+V$, we show that the following rates are achievable:

$$R_1 = H(W) - H(U|X), \quad R_2 = H(W) - H(V|Y)$$

The source $X$ employs a nested polar codes whose inner code is a good channel code for the channel $(\mathbf{G}, \mathbf{G}, W_{c,X})$ and whose outer code is a good source code for the test channel $(\mathbf{G}, \mathscr{X} \times \mathbf{G}, W_{s,X})$ where for $s,t,q,z \in G$ and $x \in \mathscr{X}$,

$$W_{c,X}(q|s+t) = p_W(q-s-t), W_{s,X}(x,z|s) = p_{XU}(x,z-s)$$

Similarly, the source $Y$ employs a nested polar code whose inner code is a good channel code for the channel $(\mathbf{G}, \mathbf{G}, W_{c,Y})$ and whose outer code is a good source code for the test channel $(\mathbf{G}, \mathscr{Y} \times \mathbf{G}, W_{s,Y})$ where for $s,t,q,r \in G$ and $y \in \mathscr{Y}$,

$$W_{c,Y}(q|s+t) = p_W(q-s-t), W_{s,Y}(y,r|t) = p_{YV}(y,r-t)$$

These channels are depicted in Figures 7.3, 7.4, 7.5 and 7.6.

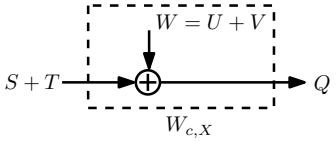


Figure 7.3: Korner-Marton Problem, Terminal X: Test channel for the inner code.

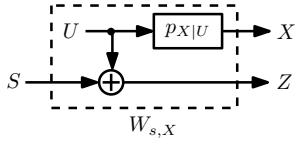


Figure 7.4: Korner-Marton Problem, Terminal X: Test channel for the outer code.

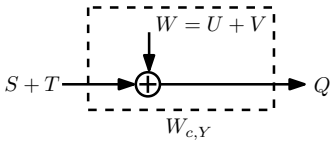


Figure 7.5: Korner-Marton Problem, Terminal Y: Test channel for the inner code.

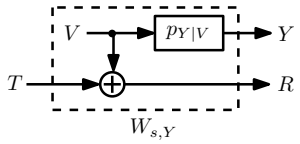


Figure 7.6: Korner-Marton Problem, Terminal Y: Test channel for the outer code.

We need to show that $W_{c,X}$ is degraded with respect to $W_{s,X}$ (and $W_{c,Y}$ is degraded with respect to $W_{s,Y}$). To show this, in the definition of degradedness [63, Definition III.1], we let the channel $(\mathbf{G}, \mathscr{X} \times \mathbf{G}, W)$ be such that that for $q, z \in \mathbf{G}$ and $x \in \mathscr{X}$, $W(q|x, z) = p_{V|X}(q - z|x)$.

## 7.4 Multiple Access Channels

Let the finite sets $\mathscr{X}$ and $\mathscr{Y}$ be the input alphabets of a two-user MAC and let $\mathscr{Z}$ be the output alphabet. In order to show that nested polar codes achieve the capacity of a MAC, it suffices to show that the rates $R_1 = I(X; Z|Y) = H(X) - H(X|YZ)$ and $R_2 = I(Y; Z)$ are achievable. It is known from the point-to-point result [64] that the $Y$ terminal can communicate with the decoder with rate $I(Y; Z)$ so that $y_1^N$ is available at the decoder with high probability. It remains to show that the rate $R_1$ is achievable for the $X$ terminal when $y_1^N$ is available at the decoder. Let $\mathbf{G}$ be an Abelian group with $|\mathbf{G}| = |\mathscr{X}|$. Define the artificial channels $(\mathbf{G}, \mathbf{G}, W_s)$ and

$(\mathbf{G}, \mathscr{Y} \times \mathscr{Z} \times \mathbf{G}, W_c)$ such that for $u, z \in \mathbf{G}$ and $y \in \mathscr{Y}$,

$$W_s(s|u) = p_X(s-u), W_c(y,z,s|u) = p_{XYZ}(s-u,y,z)$$

These channels have been depicted in Figures(7.7) and (7.8).

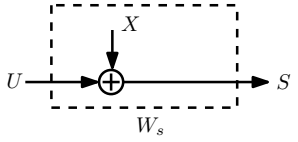


Figure 7.7: Multiple-Access Channels: Channel for inner code.

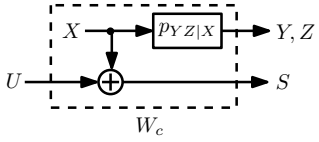


Figure 7.8: Multiple-Access Channels: Channel for outer code.

Similarly to previous cases, one can show that the symmetric capacities of the channels are equal to $\bar{I}(W_s) = \log q - H(X)$ and $\bar{I}(W_c) = \log q - H(X|YZ)$. We employ a nested polar code in which the inner code is a good source code for the test channel $W_s$ and the outer code is a good channel code for $W_c$. The rate of this code is equal to $R = \bar{I}(W_c) - \bar{I}(W_x) = I(X; Z|Y)$. Here, we only give a sketch of the proof. First note that the channel $W_s$ is degraded with respect to $W_c$ so that the the source code is contained in the channel code.

For $s_1^N \in \mathbf{G}^N$, $y_1^N \in \mathscr{Y}^N$ and $z_1^N \in \mathscr{Z}^N$, let

$$W_{s,N}^{(i)}(s_1^N, a_1^{i-1}|a_i) = \sum_{a_{i+1}^N \in \mathbf{G}^{N-i}} \frac{1}{q^{N-1}} W_s^N(s_1^N|a_1^N G)$$

$$W_{c,N}^{(i)}(y_1^N, z_1^n, s_1^N, a_1^{i-1}|a_i) = \sum_{a_{i+1}^N \in \mathbf{G}^{N-i}} \frac{1}{q^{N-1}} W_c^N(y_1^N, z_1^N, s_1^N|a_1^N G)$$

Let the random vectors $X_1^N, Y_1^N, U_1^N, V_1^N$ be distributed according to $P_{XYUV}^N$ and let $S_1^N$ be a random variable uniformly distributed over $\mathbf{G}^N$ which is independent of $X_1^N, Y_1^N, U_1^N, V_1^N$. Let $U_1^N = S_1^N - X_1^N$ and $A_1^N = U_1^N G^{-1}$. The encoding and decoding rules are similar to those of the point-to-point channel coding result; i.e., at the encoder, the distribution $p_{A_i|S_1^N A_1^{i-1}}$ is used for soft encoding and at the decoder, $W_{c,N}^{(i)}(y_1^N, z_1^n, s_1^N, a_1^{i-1}|a_i)$ is used in the successive cancelation decoder to decode $a_1^N$. The final decoder output is equal to $z_1^N - a_1^N G$. Note that since $y_1^N$ is known to the decoder with high probability, it can be used as the channel output for $W_c$.

## 7.5 Computation over MAC

In this section, we consider a simple computation problem over a MAC with input alphabets $\mathscr{X}$, $\mathscr{Y}$ and output alphabet $\mathscr{Z}$. The two input terminals of a MAC, $X$ and $Y$ are trying to communicate with a centralized decoder which is interested in the sum of the inputs $S = X + Y$ where $+$ is summation over a group $\mathbf{G}$. We show that the rate $R = \min(H(X), H(Y)) - H(S|Z)$ is achievable using polar codes. The terminal $X$ employs a nested polar code whose inner code is a good source code for the test channel $(\mathbf{G}, \mathbf{G}, W_{s,X})$ and whose outer code is a good channel code for the channel $(\mathbf{G}, \mathscr{Z} \times \mathbf{G}, W_{c,X})$ where for $u, v, r, z \in \mathbf{G}$ and $z \in \mathscr{Z}$,

$$W_{s,X}(r|u) = p_X(r-u), W_{c,X}(z, q|u+v) = p_{SZ}(q-u-v, z)$$

Similarly, the terminal $Y$ employs a nested polar code whose inner code is a good source code for the test channel $(\mathbf{G}, \mathbf{G}, W_{s,Y})$ and whose outer code is a good channel code for the channel $(\mathbf{G}, \mathscr{Z} \times \mathbf{G}, W_{c,Y})$ where for $u, v, t, z \in \mathbf{G}$ and $z \in \mathscr{Z}$,

$$W_{s,Y}(t|v) = p_Y(t-v), W_{c,Y}(z, q|u+v) = p_{SZ}(q-u-v, z)$$

Note that the two terminals use the same channel code. These channels are depicted in Figures 7.9, 7.10, 7.12 and 7.11.

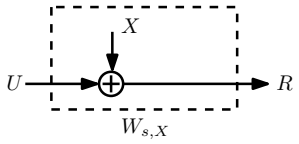


Figure 7.9: Computation Over MAC, Termianl X: Channel for inner code.

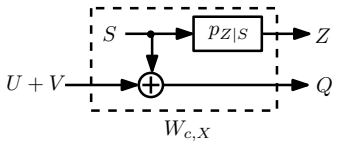


Figure 7.10: Computation Over MAC, Termianl X: Channel for outer code.

Similarly to previous cases, one can show that the symmetric capacities of the channels are equal to $\bar{I}(W_s) = \log q - H(X)$ and $\bar{I}(W_c) = \log q - H(X|YZ)$. We employ a nested polar code in which the inner code is a good source code for both test channels $W_{s,X}$ and $W_{s,Y}$ and the outer code is a good channel code for $W_{c,X} =$

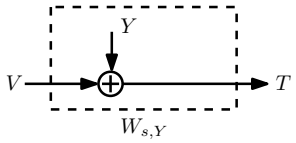


Figure 7.11: Computation Over MAC, Termianl Y: Channel for inner code.

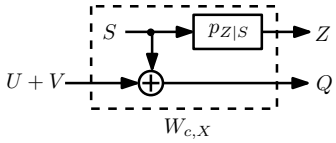


Figure 7.12: Computation Over MAC, Termianl Y: Channel for outer code.

$W_{c,Y}$. The rate of this code is equal to $R = \bar{I}(W_{c,X}) - \max(\bar{I}(W_{s,X}), \bar{I}(W_{s,Y})) = \min(H(X), H(Y)) - H(S|Z)$. It is worth noting that it can be shown that the intersection of the two source codes is contained in the common channel code.

## 7.6 The Broadcast Channel

In this section, we show that polar codes achieve the capacity of a broadcast channel $(\mathscr{X}, \mathscr{Y} \times \mathscr{Z}, W, w)$ when $\mathscr{X} = \mathbf{G}$ for some arbitrary Abelian group $\mathbf{G}$.

Let $X$ be a random variable over $\mathscr{X}$ such that $\mathbb{E}\{w(X)\} \leq D$ and let $Y, Z$ be the corresponding channel outputs. Let $U, V$ be random variable over $\mathbf{G}$ satisfying the Markov chain $UV \leftrightarrow X \leftrightarrow YZ$ such that there exists a function $g : \mathbf{G}^2 \rightarrow \mathscr{X}$ with $g(U, V) = X$. It suffices to show that the following rates are achievable

$$R_1 = I(U;Y) - I(U;V) = H(U|Y) - H(U|V), R_2 = I(V;Z)$$

Note that the $Z$ terminal can use a point-to-point channel code to achieve the desired rate. It remains to show that the rate $R_2$ is achievable when $v_1^N$ is available at the encoder.

Define the artificial channels $(\mathbf{G}, \mathbf{G}^2, W_s)$ and $(\mathbf{G}, \mathscr{Y} \times \mathbf{G}, W_c)$ such that for $s, v, z \in \mathbf{G}$ and $y \in \mathscr{Y}$,

$$W_s(v, z|s) = p_{UV}(z - s, v), W_c(y, z|s) = p_{UY}(z - s, y)$$

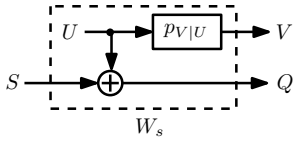


Figure 7.13: Broadcast Channels: Test channel for inner code

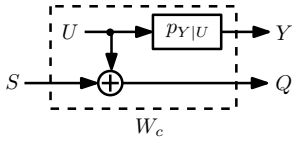


Figure 7.14: Broadcast Channels: Test channel for outer code

These channels have been depicted in Figures(7.13) and (7.14).

Similarly to previous cases, one can show that the symmetric capacities of the channels are equal to $\bar{I}(W_s) = \log q - H(U|V)$ and $\bar{I}(W_c) = \log q - H(U|Y)$. Note that to guarantee that $W_s$ is degraded with respect to $W_c$, we need an additional condition on the auxiliary random variables. It is sufficient to assume that the Markov chain $U \leftrightarrow X \leftrightarrow V$ holds.

We employ a nested polar code in which the inner code is a good source code for the test channel $W_s$ and the outer code is a good channel code for $W_c$. The rate of this code is equal to $R = \bar{I}(W_c) - \bar{I}(W_x) = I(U;Y) - I(U;V)$.

## 7.7 Multiple Description Coding

Consider a multiple description problem in which a source $X$ is to be reconstructed at three terminals $U$, $V$ and $W$. There are two encoders and three decoders. Terminals $U$ and $V$ have access to the output of their corresponding encoders and terminal $W$ has access to the output of both encoders. The goal is to find all achievable tuples $(R_1, R_2, D_1, D_2, D_3)$ where $R_1$ and $R_2$ are the rates of encoders $U$ and $V$ respectively and $D_1$, $D_2$ and $D_3$ are the distortion levels corresponding to decoders $U$, $V$ and $W$ respectively. $D_1$, $D_2$ and $D_3$ are measured as the average of distortion measures $d_1(\cdot,\cdot)$, $d_1(\cdot,\cdot)$ and $d_1(\cdot,\cdot)$ respectively. Let $U$, $V$ and $W$ be random variables such that $\mathbb{E}\{d_1(X,U)\} \leq D_1$, $\mathbb{E}\{d_2(X,V)\} \leq D_2$ and $\mathbb{E}\{d_3(X,W)\} \leq D_3$. We show that

the tuple $(R_1, R_2, D_1, D_2, D_3)$ is achievable if

$$R_1 \geq I(X;U)$$

$$R_2 \geq I(X;V)$$

$$R_1 + R_2 \geq I(X;UVW) + I(U;V)$$

It suffices to show that the rates $R_1 = I(X;UVW) - I(X;V) + I(U;V)$, $R_2 = I(X;V)$ are achievable. The point-to-point source coding result implies that with $R_2 = I(X;V)$ we can have $v_1^N$ at the output of the second decoder with high probability. To achieve the rate $R_1$ when $v_1^N$ is available, first we note that $R_1 = H(U) - H(U|VX) + H(W|UV) - H(W|UVX)$. We use a code with rate $R_{11} = H(U) - H(U|VX)$ for sending $U$ and another code $R_{12} = H(W|UV) - H(W|UVX)$ for sending $W$. The corresponding channels are depicted in Figures 7.15, 7.16, 7.17 and 7.18.

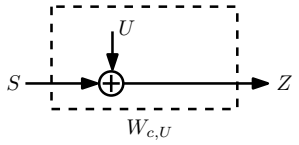


Figure 7.15: Multiple Description Coding, Terminal X: Channel for inner code.

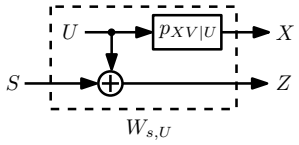


Figure 7.16: Multiple Description Coding, Terminal X: Channel for outer code.

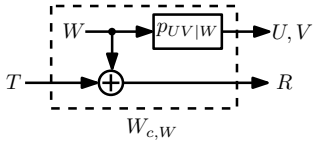


Figure 7.17: Multiple Description Coding, Terminal Y: Channel for inner code.

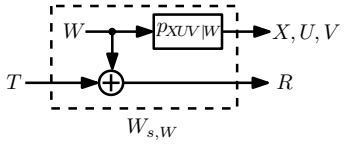


Figure 7.18: Multiple Description Coding, Terminal Y: Channel for outer code.

## 7.8 Other Problems and Discussion

In this paper, we studied the main multi-terminal communication problems in their simplest forms (e.g., no time sharing etc.). The approach of this paper can

be extended to the more general formulations and to other similar problems. The approach presented in this paper can also be extended to multiple user (more than two) cases in a straightforward fashion. We briefly discuss the 3-user MAC as an example. Consider a 3-user MAC with inputs $W$, $X$ and $Y$ and output $Z$. We have seen in Section 7.4 that with rates $R_X = I(X; YZ)$ and $R_Y = I(Y; Z)$, we can have access to $x_1^N$ and $y_1^N$ at the decoder with high probability. The channels $W_{s,W}$ and $W_{c,W}$ depicted in Figures 7.19 and 7.20 can be used to design a nested polar code of rate $R_W = I(W; Z|XY)$ for terminal $W$.

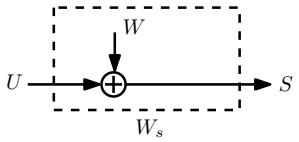


Figure 7.19: Three User MAC: Channel for inner code.

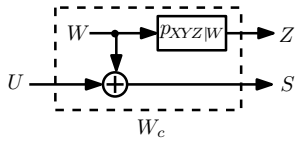


Figure 7.20: Three User MAC: Channel for outer code.

# BIBLIOGRAPHY

# BIBLIOGRAPHY


[1] H. A. Loeliger and T. Mittelholzer, "Convolutional codes over groups", *IEEE Trans. Inform. Theory*,vol. 42, no. 6, pp. 1660–1686, November 1996.

[2] H. A. Loeliger, "Signal sets matched to groups", *IEEE Trans. Inform. Theory*, vol. 37, no. 6, pp. 1675–1682, November 1991.

[3] T. J. Goblick, Jr., "Coding for a discrete information source with a distortion measure", *Ph.D. dissertation*, Dept. Electr. Eng., MIT , Cambridge, MA, 1962.

[4] S. Shridharan, A. Jafarian, S. Vishwanath, and S. A. Jafar, "Lattice Coding for K User Gaussian Interference Channels", *IEEE Transactions on Information Theory*, April 2010.

[5] E. Abbe and E. Telatar. Polar Codes for the m-User MAC. 2010. Online: http://arxiv.org/abs/1002.0777.

[6] R. Ahlswede. Group codes do not achieve Shannons's channel capacity for general discrete channels. *The annals of Mathematical Statistics*, 42(1):224–240, Feb. 1971.

[7] R. Ahlswede and J. Gemma. Bounds on algebraic code capacities for noisy channels I. *Information and Control*, 19(2):124–145, 1971.

[8] R. Ahlswede and J. Gemma. Bounds on algebraic code capacities for noisy channels II. *Information and Control*, 19(2):146–158, 1971.

[9] R. Ahlswede‘ and Te Han. On source coding with side information via a multiple-access channel and related problems in multi-user information theory. *Information Theory, IEEE Transactions on*, 29(3):396–412, May 1983.

[10] E. Arikan. Channel Polarization: A Method for Constructing Capacity-Achieving Codes for Symmetric Binary-Input Memoryless Channels. *IEEE Transactions on Information Theory*, 55(7):3051–3073, 2009.

[11] E. Arikan. Source polarization. In *Information Theory Proceedings (ISIT), 2010 IEEE International Symposium on*, pages 899–903, 2010.

[12] E. Arikan. Polar coding for the slepian-wolf problem based on monotone chain rules. In *Information Theory Proceedings (ISIT), 2012 IEEE International Symposium on*, pages 566–570, 2012.

[13] E. Arikan and E. Telatar. On the rate of channel polarization. *Proceedings of IEEE International Symposium on Information Theory*, 2009. Seoul, Korea.

[14] A. R. Barron. Limits of Information, Markov Chains, and Projection. *Proceedings of IEEE International Symposium on Information Theory*, 2000. Sorrento, Italy.

[15] T. Berger. Multiterminal source coding. *Lectures presented at CISM summer school on the Inform. Theory approach to communications*, July 1977.

[16] N. J. Bloch. *Abstract Algebra With Applications*. Prentice-Hall, Inc, Englewood Cliffs, New Jersey, 1987.

[17] R. De Buda. Some optimal codes have structure. *IEEE Journal on Selected Areas in Communications*, 7:893–899, 1989.

[18] G. Como and F. Fagnani. The capacity of finite abelian group codes over symmetric memoryless channels. *IEEE Transactions on Information Theory*, 55(5):2037–2054, 2009.

[19] J. H. Conway and N. J. A. Sloane. *Sphere Packings, Lattices and Groups*. Springer-Verlag, New York, 1988.

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

[21] I. Csiszar and J. Korner. *Information theory: Coding theorems for Discrete memoryless Systems*. 1981.

[22] A. Dembo and O. Zeitouni. *Large Deviations Techniques And Applications*. Jones and Barlett Publishers International, 1993.

[23] R. L. Dobrushin. Asymptotic optimality of group and systematic codes for some channels. *Theor. Probab. Appl.*, 8:47–59, 1963.

[24] R. L. Dobrusin. Asymptotic bounds of the probability of error for the transmission of messages over a discrete memoryless channel with a symmetric transition probability matrix. *Teor. Veroyatnost. i Primenen*, pages 283–311, 1962.

[25] P. Elias. Coding for noisy channels. *IRE Conv. Record*, part. 4:37–46, 1955.

[26] U. Erez and S. tenBrink. A close-to-capacity dirty paper coding scheme. *IEEE Trans. Inform. Theory*, 51:3417–3432, October 2005.

[27] D. Forney. On the hamming distance properties of group codes.

[28] S. Litsyn G. Cohen, I. Honkala and A. Lobstein. *Covering Codes*. Elsevier-North-Holland, Amsterdam, 1997.

[29] R. Garello and S. Benedetto. Multilevel construction of block and trellis group codes. *IEEE Trans. Inform. Theory*, 41:1257–1264, Sep. 1995.

[30] T. Gariby and U. Erez. On general lattice quantization noise. *Proceedings of IEEE International Symposium on Information Theory*, 2008. Toronto, Canada.

[31] S. I. Gelfand and M. S. Pinsker. Coding for channel with random parameters. *Problems of Control and Information Theory*, 9:19–31, 1980.

[32] N Goela, E Abbe, and M Gastpar. Polar Codes For Broadcast Channels. 2013. Online: http://arxiv.org/abs/1301.6150.

[33] P Harremos and K Khler Holst. Convergence of Markov Chains in Information Divergence. *Journal of Theoretical Probability*, 22(1):186–202, 2011.

[34] J. Interlando, R. Palazzo, and M Elia. Group block codes over nonabelian groups are asymptotically bad. *IEEE Transactions on Information Theory*, 42:1277–1280, 1996.

[35] G. D. Forney Jr and M. Trott. The dynamics of group codes: State spaces, trellis diagrams, and canonical encoders. *IEEE Transactions on Information Theory*, 39(9):1491–1513, 1993.

[36] M. Hall Jr. *The Theory of Groups*. The Macmillan Company, New York, 1959.

[37] A. F. Karr. *Probability*. Springer, 1993.

[38] M. Karzand and E. Telatar. Polar Codes for Q-ary Source Coding. *Proceedings of IEEE International Symposium on Information Theory*, 2010. Austin, TX.

[39] S. Babu Korada and R. Urbanke. Polar Codes are Optimal for Lossy Source Coding. *IEEE Transactions on Information Theory*, 56(4):1751–1768, Apr. 2010.

[40] S.B. Korada and R. Urbanke. Polar codes are optimal for lossy source coding. In *Information Theory Workshop, 2009. ITW 2009. IEEE*, pages 149–153, 2009.

[41] J. Korner and K. Marton. How to encode the modulo-two sum of binary sources. *IEEE Transactions on Information Theory*, IT-25:219–221, Mar. 1979.

[42] D. Krithivasan and S. S. Pradhan. Distributed source coding using abelian group codes. 2011. IEEE Transactions on Information Theory(57)1495-1519.

[43] T. Linder and C. Schlegel. Corrected proof of de buda's theorem. *IEEE Transactions on Information Theory*, 39:1735–1737, 1993.

[44] H. A. Loeliger. Averaging bounds for lattices and linear codes. *IEEE Transactions on Information Theory*, 43:1767–1773, 1997.

[45] F. J. MacWilliams and N. J. A. Sloane. *The theory of error-correcting codes*. Elsevier-North-Holland, 1977.

[46] P. Massey. Many non-abelian groups support only group codes that are conformant to abelian group codes.

[47] P. Mitran. Typical Sequences for Polish Alphabets. 2010. Online: http://arxiv.org/abs/1005.2321.

[48] R. Mori and T. Tanaka. Channel Polarization on q-ary Discrete Memoryless Channels by Arbitrary Kernels. *Proceedings of IEEE International Symposium on Information Theory*, July 2010. Austin, TX.

[49] P. Mrters, O. Schramm Y. Peres, and W. Werner. *Brownian Motion*. Cambridge University Press, 2010.

[50] B. A. Nazer and M. Gastpar. Computation over multiple-access channels. *IEEE Transactions on Information Theory*, 53(10 pages =), Oct. 2007.

[51] A. Padakandla and S. S. Pradhan. Nested linear codes achieve martons inner bound for general broadcast channels. *Proceedings of IEEE International Symposium on Information Theory*, 2011. Saint Petersburg, Russia.

[52] A. Padakandla and S.S. Pradhan. A new coding theorem for three user discrete memoryless broadcast channel. 2012. Online: http://128.84.158.119/abs/1207.3146v2.

[53] A. Padakandla, A.G. Sahebi, and S.S. Pradhan. A new achievable rate region for the 3-user discrete memoryless interference channel. In *Information Theory Proceedings (ISIT), 2012 IEEE International Symposium on*, pages 2256–2260, 2012.

[54] W. Park and A. Barg. Polar codes for $q$-ary channels, $q = 2^r$. 2012. Online: http://arxiv.org/abs/1107.4965.

[55] T. Philosof, A. Kishty, U. Erez, and R. Zamir. "Lattice strategies for the dirty multiple access channel". *Proceedings of IEEE International Symposium on Information Theory*, July 2007. Nice, France.

[56] T. Philosof and R. Zamir. On the loss of single-letter characterization: The dirty multiple access channel. *IEEE Transactions on Information Theory*, 55:2442–2454, June 2009.

[57] S. S. Pradhan and K. Ramchandran. Distributed source coding using syndromes (DISCUS): Design and construction. *IEEE Transactions on Information Theory*, 49(3):626–643, 2003.

[58] A. G. Sahebi and S. S. Pradhan. Multilevel Polarization of Polar Codes Over Arbitrary Discrete Memoryless Channels. *Proc. 49th Allerton Conference on Communication, Control and Computing*, Sept. 2011.

[59] A. G. Sahebi and S. S. Pradhan. Multilevel Polarization of Polar Codes over Arbitrary Discrete Memoryless Channels. July 2011. Online: http://http://arxiv.org/abs/1107.1535.

[60] A. G. Sahebi and S. S. Pradhan. On Distributed Source Coding Using Abelian Group Codes. *Proceedings of Fiftieth Annual Allerton Conference*, Oct. 2011. IL, USA.

[61] A. G. Sahebi and S. S. Pradhan. On the Capacity of Abelian Group Codes Over Discrete Memoryless Channels. *Proceedings of IEEE International Symposium on Information Theory*, July 2011. St. Petersburg, Russia.

[62] A.G. Sahebi and S.S. Pradhan. Multilevel Channel Polarization for Arbitrary Discrete Memoryless Channels. *Information Theory, IEEE Transactions on*, 59(12):7839–7857, 2013.

[63] A.G. Sahebi and S.S. Pradhan. Nested Polar Codes Achieve the Shannon Rate-Distortion Function and the Shannon Capacity. 2014. Online: http://arxiv.org/abs.

[64] A.G. Sahebi and S.S. Pradhan. Nested Polar Codes Achieve the Shannon Rate-Distortion Function and the Shannon Capacity. 2014. Submitted to ISIT 2014.

[65] E. Sasoglu. Polar Coding Theorems for Discrete Systems. Ph.D. Dissertation, EPFL, 2011.

[66] E. Sasoglu, E Telatar, and E Arikan. Polarization for arbitrary discrete memoryless channels. *IEEE Information Theory Worshop*, Dec. 2009. Lausanne, Switzerland.

[67] E. Sasoglu, E. Telatar, and E. Yeh. Polar codes for the two-user binary-input multiple-access channel. In *Information Theory Workshop (ITW), 2010 IEEE*, pages 1–5, 2010.

[68] D. Slepian. Group codes for for the Gaussian channel. *Bell Syst. Tech. Journal*, 1968.

[69] S. Sridharan, A. Jafarian, S. Vishwanath, S. A. Jafar, and S. Shamai. A layered lattice coding scheme for a class of three user gaussian interference channels. 2008. Online: http://arxiv.org/abs/0809.4316.

[70] S. Y. Tung. Multiterminal source coding. *PhD thesis, School of Electrical Engineering, Cornell University*, May 1978.

[71] R. Urbanke and B. Rimoldi. Lattice codes can achieve capacity on the awgn channel. *IEEE Transactions on Information Theory*, 44:273–278, 1998.

[72] K. Vinodh, V. Lalitha, N. Prakash, P.V. Kumar, and S.S. Pradhan. On the achievable rates of sources having a group alphabet in a distributed source coding setting. In *Communication, Control, and Computing (Allerton), 2010 48th Annual Allerton Conference on*, pages 479–486, 2010.

[73] A. Wyner. The rate distortion function for source coding with side information at the decoder-ii. *Information and Control*, 38:60–80, 1978.

[74] A. Wyner and J. Ziv. The rate distortion function for source coding with side information at the decoder. *IEEE Transactions on Information Theory*, 22:1–10, 1976.

[75] A. D. Wyner. Recent results in the Shannon theory. *IEEE Trans. Inform. Theory*, IT-20:2–10, January 1974.

[76] R. Zamir and M. Feder. On lattice quantization noise. *IEEE Transactions on Information Theory*, 42:1152–1159, 1996.

[77] R. Zamir and S. Shamai. Nested linear/lattice codes for wyner-ziv encoding. *ITW*, 1998. Ireland.

[78] R. Zamir, S. Shamai, and U. Erez. Nested linear/lattice codes for structured multiterminal binning. *IEEE Trans. Inform. Theory*, 48:1250–1276, June 2002.

[79] R. Zamir, S. Shamai, and U. Erez. Nested linear/lattice codes for structured multiterminal binning. *IEEE Transactions on Information Theory*, 48(6):1250–1276, 2002.