ABSTRACT

Title of dissertation: DESIGN AND ANALYSIS OF COMMUNICATION SCHEMES VIA POLAR CODING

Talha Cihad Gulcu
Doctor of Philosophy, 2015

Dissertation directed by: Professor Alexander Barg
Department of Electrical and Computer Engineering
and Institute for System Research

Polar codes, introduced by Arıkan in 2009, gave the first solution to the problem of designing explicit coding schemes that attain Shannon capacity of several basic models of communication channels. This discovery made it possible to attain theoretical limits of communication in a number of other problems of data compression and multi-user communication as well as provided new perspectives on extremal configurations of some discrete-time random walks.

This thesis is devoted to the design of communication protocols for several basic information-theoretic problems as well to the problem of efficient construction of polar codes.

In the first part we consider the problem of optimizing the amount of data transmitted between two terminals performing interactive computation of a function. Information-theoretic limits for one model of interactive computation were found in recent literature. We consider the distributed source coding problem that arises in the analysis of this model,

designing a polar coding scheme that serves the basis for the distributed computation. As a result, it becomes possible to attain the smallest possible rate of data exchange between the terminals using an explicit protocol of encoding and data exchange that supports reliable computation of the function by both parties. We also extend our considerations to a multi-terminal variation of this problem.

Secondly, we turn to the problem of communication between two parties over a link observed by an adversary, known as the "wiretap channel." Explicit capacity-achieving schemes for various models of the wiretap channel have received significant attention in recent literature. In this work, we address the general model of the channel, removing the constraints on the channels adopted in the earlier works. We show that secrecy capacity of the wiretap channel under a "strong secrecy constraint" can be achieved using an explicit scheme based on polar codes. We also extend our construction to the case of the broadcast channel with confidential messages due to Csiszár and Körner, achieving the entire capacity region of this communication model.

In the last part of the thesis we consider the problem of efficient construction of polar codes. While Arıkan's scheme is explicit, his original proposal suffers from high construction complexity which grows exponentially with the number of evolution steps. An approximation procedure for binary-input channels was proposed and analyzed in the literature. Here we propose and study a construction algorithm for polar codes with arbitrarily-sized input alphabets. We establish a complexity estimate of the algorithm and derive an estimate of the approximation error that ensues from its use. The approximation error reduces the gap to the recently established lower bound for this type of algorithms. The validity of the proposed algorithm is supported by experimental results.

DESIGN AND ANALYSIS OF COMMUNICATION SCHEMES VIA POLAR CODING

by

Talha Cihad Gulcu

Dissertation submitted to the Faculty of the Graduate School of the
University of Maryland, College Park in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
2015

Advisory Committee:
Professor Alexander Barg, Chair/Advisor
Professor Prakash Narayan
Professor Anthony Ephremides
Professor Behtash Babadi
Professor Leonid Koralov

To my family

Acknowledgments

First I would like to thank my advisor, Professor Alexander Barg for working with me during past four years. His guidance and support made it easier for me to find and solve nice research problems. Completing this work would not be possible without his help. He has always followed the progress I have made closely, and he was always accessible whenever I needed to talk with him.

I would also like to thank Professor Prakash Narayan for drawing my attention to the problems of interactive computation. The research performed in Chapter 2 originated with this suggestion. I also thank Professor Anthony Ephremides, Professor Behtash Babadi and Professor Leonid Koralov for agreeing to serve on my thesis committee.

I owe my deepest thanks to my family. The love and support of my mother, father and brother provided me the motivation to solve the problems I encountered during the time I spent as a PhD student. My colleagues and friends I have met at UMD also deserve special thanks since they have made life easier for me.

I would like to acknowledge financial support of this research provided by NSF project CCF1217245.

Table of Contents

List of Tables vi

List of Figures vii

1 Introduction 1
- 1.1 Polarization . . . 3
- 1.2 Symmetric Channel Coding . . . 5
- 1.3 Source Coding . . . 9
- 1.4 General Channel Coding . . . 10
- 1.5 Motivation and Outline . . . 13
  - 1.5.1 Interactive function computation . . . 13
  - 1.5.2 Coding for the discrete wiretap channel . . . 15
  - 1.5.3 Constructing nonbinary polar codes . . . 17

2 Interactive Function Computation via Polar Coding 20
- 2.1 Introduction . . . 20
- 2.2 Problem Statement . . . 22
  - 2.2.1 Two-terminal network . . . 22
  - 2.2.2 Multiterminal collocated networks . . . 26
- 2.3 The Analysis of Polar Codes for Interactive Function Computation Problem 28
  - 2.3.1 First round of communication . . . 29
  - 2.3.2 Analysis of the first round of communication . . . 32
  - 2.3.3 The remaining rounds of communication . . . 34
  - 2.3.4 Generalization of Lemmas 2.4 and 2.5 to multiple rounds . . . 37
  - 2.3.5 Computing the functions . . . 39
  - 2.3.6 An example of interactive function computation . . . 43
- 2.4 Polar Codes for Collocated Networks . . . 45
  - 2.4.1 Communication protocol . . . 45
  - 2.4.2 The analysis of the protocol . . . 48
- 2.5 Appendix 2.A: Proof of Lemma 2.4 . . . 52
- 2.6 Appendix 2.B: Proof of Lemma 2.5 . . . 59

3 Achieving Secrecy Capacity of the Wiretap Channel and Broadcast Channel with a Confidential Component 66
3.1 Introduction . . . 66
3.2 A Closer Look at Prior Works on Polar Coding for the Wiretap Channel . . . 72
3.3 Polar Coding for the Wiretap Channel . . . 75
3.4 Polar Coding for Broadcast Channel with Confidential Messages . . . 85
3.4.1 The Model . . . 85
3.4.2 Polar Coding for the Csiszár-Körner Region . . . 88
3.4.2.1 The common-message encoding . . . 89
3.4.2.2 The secret-message encoding . . . 91
3.4.2.3 Decoding of the common message and the secret message 95
3.4.2.4 Achievability of the rate region (3.23)-(3.25) . . . 97

4 Construction of Polar Codes for Arbitrary Discrete Channels 102
4.1 Introduction . . . 102
4.2 The Code Construction Scheme . . . 106
4.2.1 The approach . . . 106
4.2.2 The degrading step . . . 116
4.3 Experimental Results . . . 118

5 Concluding Remarks 127

Bibliography 130

List of Tables

4.1 The highest rate R for which the sum error probability of the $NR, N = 2^n$ most reliable subchannels (out of the 2^n channels) is at most 10^{-3}. 126
4.2 The highest rate R for which the sum error probability of the $NR, N = 2^n$ most reliable subchannels is at most 10^{-3} with μ quantization levels and $n = 15$ recursions. 126

List of Figures

1.1 The basic channel transform consisting of a single XOR gate. 4
1.2 The channels W^0 (left) and W^1 (right). 4
1.3 Block diagram of the symmetric channel coding 7

2.1 Interactive distributed source coding with t alternating messages. 23

3.1 Block diagram of the coding scheme in [17]. Good bit channels and bad bit channels are as defined by (1.6). 73
3.2 Block diagram of the coding scheme in [46]. 74
3.3 Partition of N coordinates of the block for transmission over the wiretap channel $\mathcal{W}$; see (3.9). The highlighted part of the top block represents high-entropy coordinates for the distribution P_V. Similarly, in the middle block we highlight the high-entropy coordinates of the distribution $P_{V|Z}$ and in the bottom block the low-entropy coordinates for the distribution $P_{V|Y}$. 77
3.4 Block diagram of the wiretap coding scheme: Forming the blocks $t^N(j), j = 1, \ldots, m$. 78
3.5 Encoding for the common-message case: The structure of the blocks $q^N(j), j = 1, \ldots, m$ 91

4.1 The capacity distribution of the virtual channels for Example 1, Example 2, and Example 3 120
4.2 The capacity distribution of the virtual channels for Example 4, Example 5, and Example 6 122
4.3 The capacity distribution of the virtual channels for Example 7, Example 8, and Example 9 124
4.4 The capacity distribution of the virtual channels for Example 10 and Example 11. 124

Chapter 1: Introduction

One of the basic problems of communication theory is reliable transmission of data over noisy channels. The data stream is partitioned into blocks of K information bits that are encoded into N-blocks sent over the medium such as a wireless or an optical link. The goal of the encoding is to enable the receiving party to recover the contents of the transmitted message with high probability. In his fundamental work [1], Shannon proved that this goal can be achieved if N is large enough and the transmission rate K/N is less than the capacity of the channel. While Shannon's results imply that capacity-approaching communication schemes are possible, he did not suggest efficient ways of constructing them. Much of later research in information theory has been devoted to designing efficient methods of encoding and transmitting the information in a variety of communication settings with the purpose of approaching the theoretical limits of the transmission established in [1] and later extensions of the point-to-point transmission scenario to more complicated communication systems.

Despite important achievements in algebraic coding and iterative coding, finding codes that

- operate at rates close to capacity,
- have low computational complexity,

- have reliability that can be verified analytically

was an open problem until recently. The invention of polar codes [2] made it possible to satisfy these three conditions simultaneously. Indeed, polar codes

- achieve capacity of finite-input memoryless channels [2–4]. In particular, they achieve capacity of several channel classes of practical importance such as the binary-input additive white Gaussian noise channel, the binary symmetric channel, and the binary erasure channel.

- have low complexity. It is shown in [2] that the time and space complexity of both the encoder and decoder is $O(N \log N)$, where N is the number of channel uses.

- have block error probability that declines as $O(2^{-\sqrt{N}})$.

After their introduction by Arıkan in 2008, polar codes were subsequently applied in a variety of problems related to communication and data compression [5–7]. The capacity-achieving feature of polar coding also extends to such applications of polar codes as lossy data compression [7], codes over nonbinary alphabets [8–12], and a number of other problems of information theory [13–20]. Overall, polar codes provide a flexible and versatile paradigm that enabled researchers for the first time to design explicit schemes that attain theoretical limits of a class of problems in communication and signal processing.

1.1 Polarization

Polar codes rely on transformations of random sequences that lead to isolating a small number of extremal configurations in a phenomenon called polarization. To explain it, consider transmission over a binary-input memoryless communication channel W. Let $\mathcal{Y}$ be the output alphabet of W, let $\mathcal{X} = \{0, 1\}$ be its input alphabet, and let $W_{Y|X}$ be the set of transition probabilities expressed as a conditional distribution of receiving $y \in \mathcal{Y}$ at the output given that the transmitted symbol is $x \in \mathcal{X}$. The channel W is called *symmetric* if

- The PMF $(W_{Y|X}(y|1), y \in \mathcal{Y})$ can be obtained from $(W_{Y|X}(y|0), y \in \mathcal{Y})$ through a permutation π.
- π is the inverse of itself.

Let $C(W)$ be the Shannon capacity of the channel W. If W is symmetric then $C(W)$ is attained under the uniform distribution on the input alphabet, i.e., $P_X(0) = P_X(1) = 1/2$. Otherwise, the capacity-achieving distribution P_X is different from the uniform one, so assuming the uniform P_X entails some rate loss. The maximum attainable rate under the uniform prior is called the *symmetric capacity* of W, denoted $I(W)$.

The idea which leads to polarization is to derive two new channels W^0 and W^1 out of two independent copies of W. These two channels are desired to satisfy the following conditions.

- The sum of the (symmetric) capacities of W^1 and W^0 should be equal to twice the capacity of W so that no information is lost.

- The channel W^1 should be "better" than W and the channel W^0 should be "worse" than W in some sense.

These two conditions can be met by applying a simple transformation to the inputs of two independent copies of W shown by Figure 1.1. Upon their application we define W^0 to be the channel with input u_0 and output (y_0, y_1), and W^1 the channel with input u_1 and output (y_0, y_1, u_0). These channels are shown in Figure 1.2.

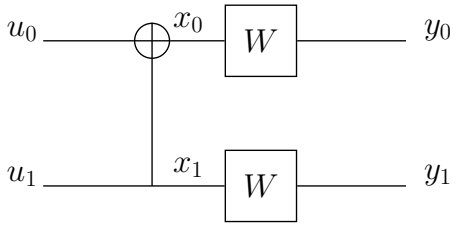


Figure 1.1: The basic channel transform consisting of a single XOR gate.

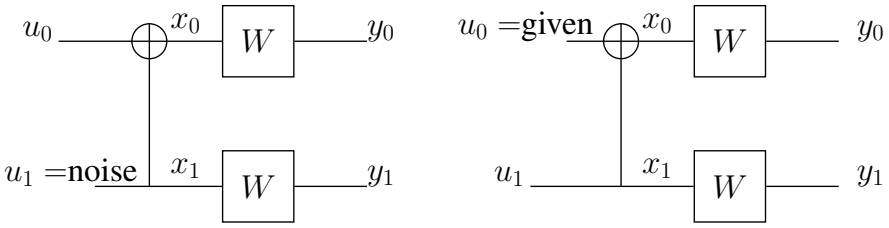


Figure 1.2: The channels W^0 (left) and W^1 (right).

It is easy to see that $I(W^0) + I(W^1) = 2I(W)$. Moreover, if $0 < I(W) < 1$, then it can be shown that $I(W^0) < I(W) < I(W^1)$. So, the transform

$$u_0 = x_0 + x_1, \tag{1.1}$$

$$u_1 = x_1 \tag{1.2}$$

makes it possible to satisfy the two conditions given above. Hence we observe that the symmetric capacity of the channels W^0 and W^1 shifts (is partially polarized) towards

the two extremes, 0 and 1. The basic transform (1.1)-(1.2) can be applied recursively to the channels W^1 and W^0 to create four channels $(W^1)^1, (W^1)^0, (W^0)^1, (W^0)^0$ that are further polarized, and so on. In general, we begin with $N = 2^n$ copies of W and create 2^n new channels $W^{11\ldots1}$, $W^{11\ldots0}$, $\ldots$, $W^{00\ldots0}$. Ultimately there emerges a group of channels whose capacity is close to one (almost noiseless channels) and the opposite group of almost useless channels, i.e., those whose capacity is close to zero. Arıkan [2] proved that the fraction of nearly noiseless channels tends to $I(W)$ and the fraction of fully noisy channels tends to $1 - I(W)$ as n goes to infinity, i.e.,

$$\lim_{n\to\infty} \frac{|\{(b_1,\ldots,b_n) \in \{0,1\}^n : I(W^{b_1\ldots b_n}) \geq 1-\epsilon\}}{2^n} = I(W) \tag{1.3}$$

$$\lim_{n\to\infty} \frac{|\{(b_1,\ldots,b_n) \in \{0,1\}^n : I(W^{b_1\ldots b_n}) \leq \epsilon\}}{2^n} = 1 - I(W) \tag{1.4}$$

for all $\epsilon > 0$. This fact is called polarization.

The polarization phenomenon can be used to solve the channel coding problem described above by sending information through the noiseless channels and not sending any information at all through the useless channels. In the next section, we explain this in a more detailed way.

1.2 Symmetric Channel Coding

We begin with introducing basic notation for polar codes and then continue with the scheme of capacity-achieving communication over discrete binary-input symmetric channels.

Given a binary random variable X and a discrete random variable Y supported on

$\mathcal{Y}$, define the *Bhattacharyya parameter* $Z(X|Y)$ as follows:

$$Z(X|Y) = 2\sum_{y\in\mathcal{Y}} P_Y(y)\sqrt{P_{X|Y}(0|y)P_{X|Y}(1|y)}$$

where $P_{X|Y}$ is the conditional distribution of X given Y. The value $Z(X|Y), 0 \leq Z(X|Y) \leq 1$ measures the amount of randomness in X given Y in the sense that if it is close to zero, then X is almost constant given Y, while if it is close to one, then X is almost uniform on $\{0,1\}$ given Y. The Bhattacharyya parameter $Z(W)$ of a binary-input channel W is defined as

$$Z(W) = \sum_{y\in\mathcal{Y}} \sqrt{W_{Y|X}(y|0)W_{Y|X}(y|1)}.$$

It can be seen that if $P_X(0) = P_X(1) = 1/2$, then $Z(X|Y)$ coincides with $Z(W)$ for the communication channel $W : X \to Y$.

For $N = 2^n$ and $n \in \mathbb{N}$, the polarizing matrix (or the *Arıkan transform matrix*) is defined as $G_N = B_N F^{\otimes n}$, where $F = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, $\otimes$ is the Kronecker product of matrices, and B_N is a "bit reversal" permutation matrix [2].

Given a binary-input symmetric channel W, define the channel W^N with the input alphabet $\{0,1\}^N$ and the output alphabet $\mathcal{Y}^N$ by the conditional distribution

$$W^N(y^N|x^N) = \prod_{i=1}^{N} W_{Y|X}(y_i|x_i).$$

Then, the "combined" channel $\widetilde{W}$ is defined by the conditional

$$\widetilde{W}(y^N|u^N) = W^N(y^N|u^N G_N)$$

In terms of $\widetilde{W}$, the channel seen by the i-th bit U_i, $i = 1,\ldots,N$, (also known as the

bit-channel[1] of the i-th bit) can be expressed as

$$W_i(y^N, u^{i-1}|u_i) = \frac{1}{2^{n-1}} \sum_{\widetilde{u}\in\{0,1\}^{n-i}} \widetilde{W}(y^N|(u_1^{i-1}, u_i, \widetilde{u})) \tag{1.5}$$

where $u^{i-1} = (u_1, u_2, \ldots, u_{i-1})$. From Figure 1.3 we see that W_i is in fact the conditional distribution of (Y^N, U^{i-1}) given U_i, provided that the channel inputs X_i are uniformly distributed for all $i = 1, \ldots, N$. The bit-channels thus defined are partitioned into good

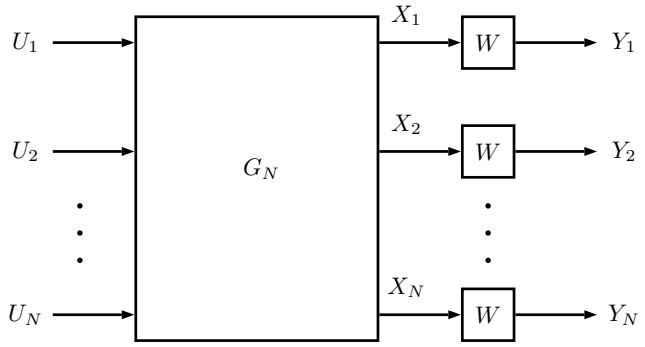


Figure 1.3: Block diagram of the symmetric channel coding

channels $\mathcal{G}_N(W, \beta)$ and bad channels $\mathcal{B}_N(W, \beta)$ based on the value of their Bhattacharyya parameters. More precisely, define

$$\begin{aligned} \mathcal{G}_N(W, \beta) &= \{i \in [N] : Z(W_i) \leq \epsilon\} \\ \mathcal{B}_N(W, \beta) &= \{i \in [N] : Z(W_i) > 1 - \epsilon\} \end{aligned} \tag{1.6}$$

where $[N] \triangleq \{1, 2, \ldots, N\}$. As shown in [2], for any symmetric binary-input channel W and any constant $\beta < 1/2$,

$$\begin{aligned} \lim_{N\to\infty} \frac{|\mathcal{G}_N(W, \beta)|}{N} &= C(W) \\ \lim_{N\to\infty} \frac{|\mathcal{B}_N(W, \beta)|}{N} &= 1 - C(W) \end{aligned} \tag{1.7}$$

[1]Note that for $n = 2$ the channels W_1, W_2 defined below are precisely the channels W^0, W^1 discussed in the previous section.

(cf. (1.3),(1.4)). Based on this equality, information can be transmitted over the good bit-channels while the remaining bits are fixed to some values known in advance to the receiver (following [2] they are called the *frozen bits*).

The transmission scheme can be described as follows: A message of $k = |\mathcal{G}_N(W, \beta)|$ bits is written in the bits $u_i, i \in \mathcal{G}_N(W, \beta)$. The remaining $N - k$ frozen bits are set to the pre-defined values. This determines the sequence u^N which is transformed to $x^N = u^N G_N$, and the vector x^N is sent over the channel. Denote by y^N the sequence received at the output. The decoder finds an estimate of u^N by computing the values $\hat{u}_i, i = 1, \ldots, N$ based on the *successive cancellation* (SC) decoding:

$$\hat{u}_i = \begin{cases} \text{argmax}_{u \in \{0,1\}} W_i(y^N, \hat{u}^{i-1} | u), & \text{if } i \in \mathcal{G}_N(W, \beta), \\ 0, & \text{if } i \in \mathcal{B}_N(W, \beta). \end{cases} \tag{1.8}$$

The results of [2, 21] imply the following upper bound on the error probability $P_e = \Pr(\hat{u}^N \neq u^N)$:

$$P_e \leq \sum_{i \in \mathcal{G}_N(W,\beta)} Z(W_i) \leq N 2^{-N^\beta} \leq 2^{-N^{\beta'}} \tag{1.9}$$

where β is any number in the interval $(0, 0.5)$ and $\beta' = \beta'(N) < \beta$.

This describes the basic construction of polar codes [2] which attains symmetric capacity $I(W)$ of the channel W with a low error rate. For symmetric channels, the values of the frozen bits can be set be chosen arbitrarily; it particular, they can be set to zero [2].

Remark 1.2.1. *There is a subtle point about the limit relations in* (1.7)*. Even though asymptotically the bit channels are either good or bad, it is not true that* $\mathcal{G}_N(W, \beta)^c = \mathcal{B}_N(W, \beta)$ *because there is a subset of indices* $\mathcal{G}_N(W, \beta)^c \backslash \mathcal{B}_N(W, \beta)$ *of cardinality* $o(N)$

that is neither good nor bad. This distinction has no import for the simple situation of transmitting over W, but leads to complications in the multi-user systems considered below; see, e.g., (3.9) *in Sect. 3.3.*

1.3 Source Coding

Let X be a binary memoryless source, let X^N denote N independent copies of X, and let $U^N = X^N G_N$. Define subsets $\mathcal{H}_X = \mathcal{H}_{X,N}$ and $\mathcal{L}_X = \mathcal{L}_{X,N}$ of $[N]$ as follows:

$$\begin{aligned} \mathcal{H}_X &= \{i \in [N] : Z(U_i|U^{i-1}) \geq 1 - \delta_N\} \\ \mathcal{L}_X &= \{i \in [N] : Z(U_i|U^{i-1}) \leq \delta_N\} \end{aligned} \tag{1.10}$$

where $\delta_N \triangleq 2^{-N^\beta}$, $\beta \in (0, 1/2)$. (The choice of this particular value of δ_N is related to the convergence rate of the polarizing process [21].) Note that each bit $U_i, i \in \mathcal{L}_X$ is nearly deterministic given the values U^{i-1}, while the bits in $\mathcal{H}_X$ are nearly uniformly random. As shown in [6], the proportion of indices $i \in [N]$ that are contained in $\mathcal{H}_X$ approaches $H(X)$, and the proportion of bits that are not polarized (i.e., are in $(\mathcal{H}_X \cap \mathcal{L}_X)^c$) behaves as $o(N)$. Therefore, as $N \to \infty$, the source sequence x^N can be recovered with high probability from $NH(X)$ bits in $\mathcal{H}_X$.

Suppose further that there is a random variable Y with a joint distribution P_{XY} with the source (Y is often called the side information about X). Similarly to (1.10) define

$$\begin{aligned} \mathcal{H}_{X|Y} &= \{i \in [N] : Z(U_i|U^{i-1}, Y^N) \geq 1 - \delta_N\} \\ \mathcal{L}_{X|Y} &= \{i \in [N] : Z(U_i|U^{i-1}, Y^N) \leq \delta_N\}. \end{aligned} \tag{1.11}$$

Suppose again that the polarizing transformation is applied to X^N. It can be shown that [6]

$$\begin{aligned}\lim_{N\to\infty}\frac{1}{N}|\mathcal{H}_{X|Y}| &= H(X|Y)\\ \lim_{N\to\infty}\frac{1}{N}|\mathcal{L}_{X|Y}| &= 1-H(X|Y).\end{aligned}$$

In other words, using polarization the source can be compressed to $NH(X|Y)$ bits. This setting is useful, for instance, in distributed lossless compression where the correlation between the observations of two terminals plays the role of side information. Note that $Z(U_i|U^{i-1},Y^N)\leq Z(U_i|U^{i-1})$ and therefore,

$$\begin{aligned}\mathcal{H}_{X|Y}&\subseteq\mathcal{H}_X\\ \mathcal{L}_X&\subseteq\mathcal{L}_{X|Y}.\end{aligned}\tag{1.12}$$

1.4 General Channel Coding

For nonsymmetric channels, Arıkan's scheme attains the rate $I(W)$ which is generally less than the Shannon capacity $C(W)$. To achieve the full channel capacity, [3] proposed an extension of the above construction described below.

Let W be a binary-input discrete memoryless channel $W:\mathcal{X}\to\mathcal{Y}$ and let P_X be the capacity achieving distribution of W. For a given block length N define the sets

$$\begin{aligned}\mathcal{H}_X&=\{i\in[N]:Z(U_i|U^{i-1})\geq 1-\delta_N\}\\ \mathcal{L}_X&=\{i\in[N]:Z(U_i|U^{i-1})\leq\delta_N\}\\ \mathcal{H}_{X|Y}&=\{i\in[N]:Z(U_i|U^{i-1},Y^N)\geq 1-\delta_N\}\\ \mathcal{L}_{X|Y}&=\{i\in[N]:Z(U_i|U^{i-1},Y^N)\leq\delta_N\}\end{aligned}\tag{1.13}$$

where δ_N and U^N,X^N,Y^N have the same meaning as above. It can be shown [21, 22]

that

$$\lim_{N\to\infty}\frac{1}{N}|\mathcal{H}_X| = H(X)$$
$$\lim_{N\to\infty}\frac{1}{N}|\mathcal{H}_{X|Y}| = H(X|Y).$$

We note that the set $\mathcal{L}_{X|Y}$ is the set of good bit-channels defined in (1.6). Unlike the case of uniform P_X, it is not possible to use all of these channels to transmit information over W. This is because if $i \notin \mathcal{H}_X$, then U_i cannot be used to carry information conditioned on previous bits U^{i-1}. Hence [3] argued that the set of information indices should be chosen as $\mathcal{I} \triangleq \mathcal{H}_X \cap \mathcal{L}_{X|Y}$ rather than $\mathcal{L}_{X|Y}$.

Since $\mathcal{H}_{X|Y} \subseteq \mathcal{H}_X$ (1.12) and the number of indices that are neither in $\mathcal{H}_{X|Y}$ nor in $\mathcal{L}_{X|Y}$ is $o(N)$, we have

$$\lim_{N\to\infty}\frac{1}{N}|\mathcal{I}| = \lim_{N\to\infty}\frac{1}{N}(|\mathcal{H}_X| - |\mathcal{H}_{X|Y}|) = C(W),$$

i.e., transmitting the information using the bits $U_i, i \in \mathcal{I}$ attains the capacity of the channel W.

The code construction in [3] makes use of the following partition of the coordinate set $[N]$:

$$\left.\begin{aligned}\mathcal{F}_r &= \mathcal{H}_X \cap \mathcal{L}^c_{X|Y}\\ \mathcal{F}_d &= \mathcal{H}^c_X\\ \mathcal{I} &= \mathcal{H}_X \cap \mathcal{L}_{X|Y}\end{aligned}\right\} \tag{1.14}$$

where the superscript ^{c} refers to the complement of the subset in $[N]$. In terms of this partition, the encoding is done as follows. The information bits are stored in $\{u_i, i \in \mathcal{I}\}$. As for the bits in the subset $\{i \in \mathcal{F}_r \cup \mathcal{F}_d\}$, [3] suggested to sample their values from the distribution $P_{U_i|U^{i-1}}$. These values are shared with the receiver similarly to the "frozen

bits" of the symmetric scheme of [2]. Once u^N is determined, the transmitter finds $x^N = u^N G_N$ and sends it over the channel.

The receiver uses the following successive decoding function: for $i = 1, 2, \ldots, N$ let

$$\hat{u}_i = \begin{cases} \text{argmax}_{u \in \{0,1\}} P_{U_i|U^{i-1},Y^N}(u|\hat{u}^{i-1}, y^N), & i \in \mathcal{I} \\ u_i, & i \in \mathcal{F}_r \cup \mathcal{F}_d. \end{cases} \tag{1.15}$$

Note that this rule represents a MAP-like decoder[2] for the ith subchannel, which for the symmetric case coincides with the maximum likelihood-like decoder rule (1.8).

The probability of decoding error can be bounded above similarly to (1.9):

$$P_e \leq \sum_{i \in \mathcal{I}} Z(U_i|U^{i-1}, Y^N) \leq N 2^{-N^\beta} \leq 2^{-N^{\beta'}} \tag{1.16}$$

where the parameters have the same meaning as before.

Moreover, [3] argues that there exists a set of deterministic maps $\lambda_i : \{0,1\}^{i-1} \to \{0,1\}, i \in \mathcal{F}_r \cup \mathcal{F}_d$ such that (1.16) holds true, stating the decoding rule in the form

$$\hat{u}_i = \begin{cases} \text{argmax}_{u \in \{0,1\}} P_{U_i|U^{i-1},Y^N}(u|\hat{u}^{i-1}, y^N), & i \in \mathcal{I} \\ \lambda_i(\hat{u}^{i-1}), & i \in \mathcal{F}_r \cup \mathcal{F}_d. \end{cases} \tag{1.17}$$

The mappings λ_i are shared between the transmitter and the receiver prior to communication.

Observe that the subset of bits $\mathcal{H}_X$ can be used in a polarization procedure to compress a discrete memoryless source to its entropy rate [21] (recall than linear codes can

[2]We say MAP-like decoder because the rule in (1.15) treats future frozen bits as random variables rather than as known values. As observed in [2], this decoder is simpler to implement, but entails some perfomance loss compared to the true MAP rule.

be used for this purpose [23, Probl. 1.7]). Therefore, because of the inclusion (1.12) we can view the source code as being partitioned into cosets that form capacity-achieving channel codes. This observation will be useful in our studies in later chapters.

1.5 Motivation and Outline

As noted above, the idea of polarization has been used to provide explicit solutions in a variety of problems in information theory. To name a few, polar codes have been used to provide optimal transmission schemes for lossy compression, multiple-access and broadcast channels, and interference networks [5, 22, 24–26]. In our research we contribute to these studies by addressing several outstanding problems for which explicit constructions were missing from the literature.

1.5.1 Interactive function computation

In the first part of this thesis, covered in Chapter 2, we design explicit communication schemes for several problems of interactive function computation. Interactive computation in networks has been recently attracting attention of researchers in information theory and computer science alike. Aspects of interactive computation have been analyzed from various perspectives including establishing the region of achievable rates, complexity and security of computations, as well as a number of other problems [27–31].

A line of work starting with the paper [32] examined the question of computing a function $f(X, Y)$ where X is a discrete memoryless source and Y represents side information provided to the decoder as a random variable correlated with X. The main

question addressed in these works is whether communication for computing the function rather than communicating the source itself can reduce the volume of transmission. While [32] confined itself to the modulo-two sum of X and Y, later works, e.g., [33] extended the problem to arbitrary functions f, finding the region of achievable rates for one or two rounds of communication for computing f.

We focus on the problems considered in [34,35] which generalize the setting of [33] to multiple rounds of communication. The main problem considered in these papers concerns the scenario in which two terminals observe multiple independent realizations of correlated random variables. The objective of the terminals is to establish and conduct communication that enables them to compute a function of their observations. An obvious solution is to transmit the entire sequence of observations from Terminal A to Terminal B and the same in the reverse direction whereupon the computation can be trivially completed. The problem considered in [34, 35] is to reduce the amount of transmitted information using ideas from distributed lossy compression, thereby reducing the problem to a version of distributed source coding. An extension of this problem considered in [35] concerns transmission in a multiterminal network where the computation is performed by a single dedicated node. In both scenarios the cited papers characterized exactly the region of achievable rates of communication for the function computation.

As our main contributions, we design constructive schemes based on polar codes that achieve the optimal rates established earlier by information-theoretic considerations. The communication scheme designed in this chapter supports distributed computation under the rates of data exchange that approach the optimal values. The lossy source coding results in [7, 22] establishes the base of our analysis, but there are numerous new

challenges coming from interactive nature of the problem. In particular, an obvious idea would be to apply several rounds of the lossy compression scheme in succession. In our study we need to go beyond this because neither the coding of [22] nor its analysis generalize immediately to multiple rounds.

A more detailed discussion of the ideas behind our solution as well as of the technical ideas behind the proofs is presented in the introduction to Ch. 2.

The results of this chapter are covered in publications [36, 37].

1.5.2 Coding for the discrete wiretap channel

The wiretap channel model $\mathcal{W}$ was introduced by Wyner in 1975 [38]. In this model, there are two receivers Y, Z and a single transmitter X. The transmitter aims at sending messages to Receiver 1 through a communication channel W_1. The information sent from X to Y is also received by Receiver 2 through another channel W_2. The transmission problem in the system $\mathcal{W}(W_1, W_2)$ calls for designing a coding system that supports communication between X and Y in a way that is both reliable and secure. The reliability requirement is the usual one for communication systems, namely, that the error probability of decoding the information by Y be made arbitrarily low by increasing the block length of the encoding. At the same time, the transmission needs to be made secure in the sense that the information extracted by Receiver 2 about the message of X approaches zero as a function of the block length.

While most general constructive coding schemes for the wiretap channels in the literature rely on polar codes, there were some constructive solutions even before the

publication of [2]. At the same time, these schemes applied only to some special cases of the channels W_1, W_2. For instance the case when W_1 is noiseless and W_2 is a binary erasure channel was addressed in [39, 40] which show that in this case the capacity C_s can be achieved using low-density parity-check codes. The results in [39] are based on the weak security assumption while strong security is considered in [40]. Moreover, [39] extends the construction to the cases when both W_1 and W_2 are erasure channels, and when W_1 is noiseless and W_2 is a binary symmetric channel. As usual with the application of low-density codes, the constructions are based on code ensembles and strictly speaking are not explicit.

After the discovery of the polar codes, they have been used in several special cases of the general wiretap channel problem. In particular, a number of papers [17, 41–43] considered transmission over the channel $\mathcal{W}$ under the assumption that the channel W_2 is *degraded* with respect to W_1 (see the definition in (3.5)). Another limitation of these and some other previous results was their reliance on a particular type of security assumption whereby the information leakage to the eavesdropper is amortized per transmitted bit. This is the so-called *weak security constraint* defined formally in (3.3). At the same time, as shown already in [44, 45], this assumption is insufficient for secure transmission over the channel. Instead it, most of the studies in information-theoretic security and cryptography adopt the so-called *strong security constraint*. In particular, several works [46–49] attempted to construct explicit communication schemes for the considered problem under the stronger assumption widely. However, the schemes designed in these papers either do not cover general wiretap channels, limiting themselves to the symmetric case, or suggest high-complexity procedures that stop short of providing explicit schemes (a more detailed

discussion appears below in Sect. 3.1).

In Chapter 3, we provide a solution to the communication problem over the wiretap channel in full generality, removing the assumptions of degradedness and channel symmetry, and satisfying the strong security requirement[3]. We also show that it is possible to build on this solution by adding a second layer of encoding which enables one to attain the capacity region of the broadcast channel with confidential messages model of Csiszár and Körner [50]. The application of the Markov chain conditions in the encoding procedures, and the strong security analysis are the new ideas that were introduced in this work.

The results of this chapter are covered in publications [51, 52].

1.5.3 Constructing nonbinary polar codes

While the polar coding scheme of Arıkan [2] provided an explicit code design for achieving capacity of binary-input channels, he did not give an efficient algorithm of constructing polar codes. Recalling the definitions of Sect. 1.1, we note that the construction problem reduces to identifying the indices of the good bit-channels to be used for sending the information to the receiver. In other words, one needs to compute all the bit-channels W_i to determine the set of indices $\mathcal{G}_N(W, \beta)$ over which the information bits are transmitted; see (1.6). Rephrasing again, constructing a polar code amounts to identifying the basis vectors of the linear subspace (the rows of the generator matrix) among the 2^n rows

[3] A concurrent study [53], posted after the completion of [51], also contains a solution of the problems considered in this work, including the general wiretap channel. The transmission scheme and the proof methods in [53] are different from our work. Another recent paper, [54], also devoted to the general wiretap channel, focuses on the weak security requirement.

of the transform matrix G_N. This problem remains a difficult unresolved challenge in the whole area of polar coding.

Short of explicitly answering this question, a large number of papers gave numerous approximations and semi-explicit procedures for the choice of the basis [55–59]. A detailed overview of the relevant publications is included in Sect. 4.1. Here we note the papers [56, 57] that suggested and analyzed an approximation algorithm of constructing polar codes for binary-input channels. The main obstacle on the way of explicitly constructing polar codes is the fact, seen from (1.5), that the output alphabet of the bit-channels grows exponentially with the number of evolution steps n. The main idea of [56] is collapsing the outputs of the subchannels to a smaller-sized alphabet while tracking the loss of the approximation.

Extending this idea to nonbinary inputs was addressed in [58], but their solution worked for alphabets of size only slightly greater than 2, rapidly becoming too complex as the size of the channel input q increased. In Chapter 4 of this work we take up this problem, suggesting an approximation algorithm that resolves the construction problem of polar codes for moderately sized nonbinary alphabets. Nonbinary codes are widely used in practice, for instance, in memory and storage systems. This provides added motivation for studying nonbinary polar codes, which the results of this chapter bring closer to applications. The scheme that we propose uses the same general idea of reducing the size of the output alphabet of the subchannels and controlling the rate loss that entails from the approximation. At the same time, we design a new approximation procedure based on the estimate of the capacity loss due to the merging of two output symbols into one symbol of the alphabet. This estimate suggests a constructive reduction scheme which we

implement in a new construction algorithm of polar codes. The algorithm works for both binary and non-binary channels with a complexity $O(N\mu^4)$, where N is the blocklength and μ is the parameter that limits the output alphabet size.

The error estimate the we derive generalizes the estimate of [57] to the case of nonbinary input alphabets (but the proof method is completely new). It is also interesting to note that the error is close to a *lower bound* for this type of construction algorithms, derived very recently in [60].

In our experiments we were able to construct codes for q as large as 16; see the examples in Sect. 4.3. At the same time, it can be argued that there is no need to design approximations for very large alphabets because their applicability in practice is rather questionable.

The results of this chapter are as yet unpublished. They will be included in the preprint [61] which is currently under preparation.

Chapter 2: Interactive Function Computation via Polar Coding

2.1 Introduction

Starting with the results of [34, 35], in this chapter we design explicit communication protocols that achieve the rate regions of the two communication models considered in the cited works. In our schemes, communication is performed by exchanging several messages between the terminals formed by using specially designed polar coding constructions. As remarked earlier, it is possible to design a polar-coding scheme for lossy source coding, including Wyner-Ziv's distributed version of this problem [7, 22]. These results serve a starting point of our research which also proceeds in the context of distributed lossy compression. The new challenges in our constructions arise from the fact that for function computation we need to implement an interactive scheme. To address them, we define a partition of coordinates of the encoded block that ensures the validity of our interactive communication scheme. Inspired by the ideas of [3], we define a partition of coordinates of the encoded block that ensures the validity of our interactive communication scheme (this partition can be viewed as a refinement of (1.14)). This setup, however, comes at a price of more involved analysis, which we proceed to discuss.

Recall that the main challenge in proving that polar codes attain the rate-distortion function consisted in showing that the joint statistic of the source sequence and the polar-

compressed sequence is close to the "ideal" statistic arising from the rate-distortion theorem [22]. Estimates of this kind present the main technical challenges of our research, and form the core of the proofs. Our situation however is more difficult than the setting of distributed compression because we need to show that the mentioned statistic is close to the ideal distribution both for the transmitting and receiving parties. It may seem that the transmitter already has all the information, and there is no reason that it cannot recover the data with high probability or even probability one. This is not the case because the interactive nature of the communication protocol calls for a different encoding procedure of polar codes. To define it, we introduce a partition of the data block into message bits, random bits, and near-deterministic bits. This supports the required functionality, but at the same time biases the joint statistic. For this reason, to prove proximity of the distributions even in the first round, we have to rely on rather involved induction arguments, analyzing separately the observations of the transmitter and the receiver. At a high level, we need to show that both terminals generate the same sequence of random variables with high probability, leading to the reliable computation of their functions. Proofs of the described claims take up a large part of the chapter. These ideas are developed in Sect. 2.3.1, 2.3.2; see in particular Lemmas 2.4 and 2.5.

Once the needed properties of the distributions are established for the first round, we proceed to extend the argument to multiple rounds of communication. Namely, in Sect. 2.3.3, 2.3.4 we show that after several rounds of communication at rates that approach the optimal rate for this problem, the terminals recover the random sequences generated by each other with high probability. This is proved via another induction argument which has to take account of multiple Markov chain conditions that arise naturally

in the course of the exchange.

Our overall goal is to show that the terminals are able to compute the functions of their observations with high probability. We show this in Sect. 2.3.5 by proving that the desired values are computed by the terminals with probability approaching one. To complete the discussion, in Sect. 2.3.6 we give an example of distributed computation where our scheme provides a gain in the amount of transmitted data over sending the realizations of the random variables observed by the terminals.

Finally, in Sect. 2.4 we show that the designed scheme can be extended to a version of distributed computation performed in a network of terminals [35]. It turns out that our scheme for two terminals can be modified to attain optimal rates of communication for this scenario. The main elements of the analysis are similar to the case of two terminals.

In summary, we suggest a version of polar codes that support the primitive of interactive lossy source coding and apply it to some function computation problems. This takes interactive source coding one step closer towards practicality by showing that polar codes, which are known to have near linear coding complexity, can indeed recover the rate regions. We also introduce some new technical tools that could be useful in other interactive communication schemes based on polar codes.

2.2 Problem Statement

2.2.1 Two-terminal network

The two-terminal interactive distributed source coding problem that we consider in this chapter is illustrated in Figure 2.1. Let X and Y be discrete random variables taking

values in finite sets (alphabets) $\mathcal{X}$ and $\mathcal{Y}$ and let p_{XY} be their joint distribution. Suppose that we are given N independent realizations

$$(X,Y)^N = ((X(1),Y(1)),(X(2),Y(2)),\ldots,(X(N),Y(N)))$$

of the pair (X,Y). We assume that Terminal A observes the sequence $X^N \in \mathcal{X}^N$ and Terminal B observes the sequence $Y^N \in \mathcal{Y}^N$.

The aim of Terminal A is to calculate the function $f_A : \mathcal{X} \times \mathcal{Y} \to \mathcal{Z}_A$ for indices $i = 1,\ldots,N$. Similarly, the aim of Terminal B is to calculate the function $f_B : \mathcal{X} \times \mathcal{Y} \to \mathcal{Z}_B$, where $\mathcal{Z}_A, \mathcal{Z}_B$ are some finite alphabets. In other words, Terminals A and B attempt to compute $Z_A^N \triangleq (Z_A(1), Z_A(2),\ldots,Z_A(N))$ and $Z_B^N \triangleq (Z_B(1), Z_B(2),\ldots,Z_B(N))$ respectively, where $Z_A(i) = f_A(X(i),Y(i))$ and $Z_B(i) = f_B(X(i),Y(i))$, for $i = 1,\ldots,N$.

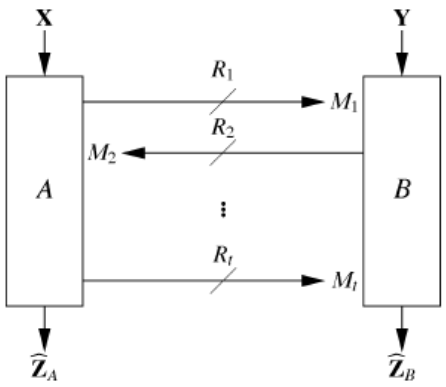


Figure 2.1: Interactive distributed source coding with t alternating messages.

Definition 1. *A two-terminal t-round interactive source code with the parameters $(t, N, |\mathcal{M}_1|,\ldots,|\mathcal{M}_t|)$ is formed by t encoding functions $e_1,\ldots,e_t$ and two block decod-*

ing functions g_A, g_B of blocklength N such that

$$\text{(Enc } j, j = 1, \ldots, t) \quad e_j : \begin{cases} \mathcal{X}^N \times \bigotimes_{i=1}^{j-1} \mathcal{M}_i \to \mathcal{M}_j & \text{if } j \text{ is odd} \\ \mathcal{Y}^N \times \bigotimes_{i=1}^{j-1} \mathcal{M}_i \to \mathcal{M}_j & \text{if } j \text{ is even} \end{cases}$$

$$\text{(Dec A)} \quad g_A : \mathcal{X}^N \times \bigotimes_{j=1}^{t} \mathcal{M}_j \to \mathcal{Z}_A^N$$

$$\text{(Dec B)} \quad g_B : \mathcal{Y}^N \times \bigotimes_{j=1}^{t} \mathcal{M}_j \to \mathcal{Z}_B^N.$$

Without loss of generality we are assuming that communication is initiated by Terminal A. The value of the encoder mapping e_j is called the jth message (of A or B, as appropriate) and denoted by $M_j, j = 1, \ldots, t$, where t is the total number of messages in the protocol. The outputs of the decoders A and B are denoted by $\hat{Z}_A^N$ and $\hat{Z}_B^N$, respectively.

Definition 2. *A rate tuple $\mathbf{R} = (R_1, \ldots, R_t)$ is achievable for t-round interactive function computation if for every $\epsilon > 0$ there exists $N(\epsilon, t)$ such that for all $N > N(\epsilon, t)$, there exists a two-terminal interactive source code with the parameters $(t, N, |\mathcal{M}_1|, \ldots, |\mathcal{M}_t|)$ such that*

$$\frac{1}{N} \log_2 |\mathcal{M}_j| \leq R_j + \epsilon, \ j = 1, \ldots, t$$

$$\Pr(Z_A^N \neq \hat{Z}_A^N) \leq \epsilon, \ \Pr(Z_B^N \neq \hat{Z}_B^N) \leq \epsilon.$$

The set of all achievable rate tuples is denoted by $\mathcal{R}_t^A$.

Theorem 2.1. *[34] A t-tuple of rate values $\mathbf{R}$ is contained in the region of achievable rates $\mathcal{R}_t^A$ if and only if there exist random variables $U^t = (U_1, \ldots, U_t)$ such that for all*

$i = 1, \ldots, t$

$$R_i \geq \begin{cases} I(X; U_i|Y, U^{i-1}), \quad U_i \to (X, U^{i-1}) \to Y, \quad i \textit{ odd} \\ \\ I(Y; U_i|X, U^{i-1}), \quad U_i \to (Y, U^{i-1}) \to X, \quad i \textit{ even} \end{cases} \tag{2.1}$$

$$H(f_A(X, Y)|X, U^t) = 0, \; H(f_B(X, Y)|Y, U^t) = 0$$

where the auxiliary random variables U^t are supported on finite sets $\mathcal{U}_i$ such that

$$|\mathcal{U}_j| \leq \begin{cases} |\mathcal{X}|(\prod_{i=1}^{j-1} |\mathcal{U}_i|) + t - j + 3, \quad j \textit{ odd} \\ \\ |\mathcal{Y}|(\prod_{i=1}^{j-1} |\mathcal{U}_i|) + t - j + 3, \quad j \textit{ even}. \end{cases} \tag{2.2}$$

The conditions of entropy being equal to zero in this theorem simply reflect the fact that f_A (or f_B) is a deterministic function of X, U^t (or Y, U^t), and no additional randomness is involved in its evaluation. Finding the auxiliary random variables $U_1, U_2, \ldots, U_t$ that satisfy the conditions of this theorem for a given pair of functions f_A, f_B is a separate question which is addressed on a case-by-case basis.

Of course, the main question associated with this result, before we even try to construct an explicit scheme that aims at attaining this rate region is whether the communication protocol implied by this theorem results in overall saving in communication compared to a straightforward transmission of X to B and Y to A. The answer is positive at least in some examples [34]. We discuss one of them below in this chapter; see Sect. 2.3.6.

2.2.2 Multiterminal collocated networks

Ma, Ishwar and Gupta [35] also considered a multiterminal extension of the problem described in the previous section. To describe the problem, consider a network with m source terminals and a single sink terminal. Each source terminal j observes a random sequence $(X_j)^N = (X_j(1), \ldots, X_j(N)) \in \mathcal{X}^N, j = 1, \ldots, m$. Unlike the two-terminal case, the sources are assumed to be independent, i.e., for any $i \in [N]$, the random variables $(X_1(i), X_2(i), \ldots, X_m(i))$ satisfy

$$P_{X^m}(x^m) = \prod_{j=1}^{m} P_{X_j}(x_j).$$

Let $f : \mathcal{X}_1 \times \ldots \mathcal{X}_m \to \mathcal{Z}$ be the function that the sink terminal aims to compute. In other words, the purpose of the sink terminal is to compute the sequence $Z^N = (Z(1), \ldots, Z(N))$, where $Z(i) \triangleq f(X_1(i), X_2(i), \ldots, X_m(i))$ is the i^{th} coordinate of the function.

We assume that communication is initiated by Terminal 1. The terminals take turns to broadcast messages in t steps. Every broadcasted message is recovered correctly by every terminal. Based on all the t messages transmitted, the sink node computes Z^N. If $t > m$, the communication is called interactive.

Definition 3. *A t-message distributed source code in a collocated network with parameters $(t, N, |\mathcal{M}_1|, \ldots, |\mathcal{M}_t|)$ is a collection of t encoding functions $e_1, \ldots, e_t$ and a decoding function g, where for every $i \in [t]$, $j = (i-1) \bmod m + 1$*

$$e_i : (\mathcal{X}^j)^N \times \bigotimes_{l=1}^{i-1} \mathcal{M}_l \to \mathcal{M}_i, \qquad g : \bigotimes_{l=1}^{t} \mathcal{M}_l \to \mathcal{Z}^N.$$

The output of the encoder e_i is called the i^{th} message. The output of the decoder is denoted by $\hat{Z}^N$.

Definition 4. *A rate tuple $\mathbf{R} = (R_1, \ldots, R_t)$ is achievable for t-round function computation in a collocated network if for all $\epsilon > 0$ there exists $N(\epsilon, t)$ such that for every $N > N(\epsilon, t)$, there exists a t-message distributed source code with the parameters $(t, N, |\mathcal{M}_1|, \ldots, |\mathcal{M}_t|)$ such that*

$$\frac{1}{N} \log_2 |\mathcal{M}_i| \leq R_i + \epsilon, \quad i = 1, \ldots, t,$$
$$P(Z^N \neq \hat{Z}^N) \leq \epsilon.$$

The set of all achievable rate tuples is denoted by $\mathcal{R}_t$.

Theorem 2.2. *[35] For $i = 1, \ldots, t$ let*

$$D_i = \{R_i : R_i \geq I(X_j; U_i | U^{i-1}) \text{ for all } j = (i-1) \bmod m + 1\}. \tag{2.3}$$

For all $t \in \mathbb{N}$, we have

$$\mathcal{R}_t = \bigcup_{P_{U^t|X^m}} \{\boldsymbol{R} = (R_1, \ldots, R_t) | R_i \in D_i, i \in [t]\} \tag{2.4}$$

where the union is over the distributions $P_{U^t|X^m}$ that satisfy the following conditions:

(i) $H(f(X^m)|U^t) = 0$,

(ii) For every $i \in [t], j = 1 + (i - 1 \bmod m)$,

$$U_i \to (U^{i-1}, X_j) \to (X^{j-1}, X_{j+1}, X_{j+2}, \ldots, X_m)$$

is a Markov chain;

(iii) The cardinalities of the alphabets of the auxiliary random variables U^t are bounded above as in (2.2).

A polar-coded scheme that attains this rate region is presented in Sect. 2.4.

2.3 The Analysis of Polar Codes for Interactive Function Computation Problem

In this section we show that the rate region (2.1) of the two-terminal function computation is achievable via polar coding. The overall idea is to transmit the value of the auxiliary random variables U_i in their respective rounds of communication; see Theorem 2.1. This is done interactively by alternating the roles of the transmitter and the receiver between the terminals. Upon completion of the communication, both terminals have the realizations of the U_is, and their respective values coincide with high probability. The random variables associated with these realizations are denoted by U_i^A and U_i^B below. Once the desired properties of these random variables are established, the actual function computation is accomplished relying on the conditional entropy constraints in (2.1).

In the first part of our presentation (Sections 2.3.1 and 2.3.2), we describe and analyze the first round of communication between the terminals. As already mentioned, we will need to show that the joint distributions of U_1^A and the observations of the terminals given by the random variables X, Y are close to the ideal distribution $P_{(U_1)^{1:N},X^{1:N},Y^{1:N}}$. The reason that this needs to be proved for the transmitter terminal (Terminal A in Round 1) is discussed in the Introduction in general terms. In greater detail, it stems from the fact that, apart from the data bits, we also have a subblock of low-entropy (nearly deterministic) bits encoded into the vector U_1^A. This entails the need for a careful analysis of the empirical probability distribution, which is performed in Lemma 2.4.

Once this is accomplished, we move to the analysis of the data received by Ter-

minal B. We need to show that its version of the realization of U_1 equals U_1^A with high probability. To prove this, we would like to make use of the proximity of the joint statistics to the ideal distribution, but this fact itself requires a proof. Thus, we are faced with proving two concurrent and mutually interdependent estimates. This question is resolved by an induction argument that gets rather technical and relies on delicate estimates of the distance between various distributions and on Markov chain conditions. This argument forms the contents of Lemma 2.5 below.

The next step is to generalize the claim for Round 1 to multiple rounds. This part is relatively easier, but still new to the analysis of polar codes because of accounting for multiple Markov chain conditions. It is contained in Sect. 2.3.4. To conclude the proof, we show in Sect. 2.3.5 that each terminal correctly computes its function value with a probability converging to 1.

Let $U_1, \ldots, U_t$ be random variables that satisfy the Markov chain conditions and conditional entropy conditions of Theorem 2.1. Throughout the section, P_{XYU_1} and P_{XYU^t} refer to the joint distribution of the random variables X, Y, U_1 and $X, Y, U_1, \ldots, U_t$, respectively. We will also assume that all the random variables $U_1, \ldots, U_t$ are binary. Generalizations to the case of a nonbinary alphabet can be easily accomplished using a multitude of methods available in the literature.

2.3.1 First round of communication

We begin with a detailed discussion of the first round of communication, i.e., the round in which A transmits to B a message from its set of 2^{NR_1} messages.

Consider the joint distribution

$$P_{(V_1)^N X^N Y^N (U_1)^N}((v_1)^N, x^N, y^N, (u_1)^N)$$
$$= \mathbb{1}((u_1)^N G_N = (v_1)^N) \prod_{i=1}^{N} P_{XYU_1}(x_i, y_i, (u_1)_i)$$

Various marginal and conditional distributions used below, denoted by P, are assumed to be implied by this expression. The purpose of the first round of communication is to make it possible for both terminals to generate the random vector $(U_1)^N$ so that the joint distribution of $(U_1)^N, X^N, Y^N$ is close to $P_{(U_1)^N X^N Y^N}$.

Consider the following partition:

$$\left.\begin{aligned} \mathcal{F}_r &= \mathcal{L}_{U_1}^c \cap \mathcal{H}_{U_1|X} \\ \mathcal{F}_d &= \mathcal{L}_{U_1} \\ \mathcal{I} &= \mathcal{L}_{U_1}^c \cap \mathcal{H}_{U_1|X}^c. \end{aligned}\right\} \tag{2.5}$$

Remark: For readers familiar with [3] we note that this partition, while inspired by this paper, is different from the one used in it. Our choice is better suited for the analysis of joint statistics of the observations and the auxiliary random variables that arise in the present study.

Round 1: The transmission scheme in the first round of communication pursues the goal of sharing the sequence $(u_1)^N$ between the two terminals. This goal is accomplished using the following procedure. Given x^N, Terminal A computes the sequence $(v_1^A)^N$ in a

successive fashion by sampling from the conditional distribution

$$
\begin{aligned}
&Q_{(V_1^A)_i|(V_1^A)^{i-1}X^N}((v_1^A)_i|(v_1^A)^{i-1},x^N)\\
&=\begin{cases}
1/2, & i\in\mathcal{F}_r\\
P_{(V_1)_i|(V_1)^{i-1}}((v_1^A)_i|(v_1^A)^{i-1}), & i\in\mathcal{F}_d\\
P_{(V_1)_i|(V_1)^{i-1}X^{1:N}}((v_1^A)_i|(v_1^A)^{i-1},x^N), & i\in\mathcal{I}.
\end{cases}
\end{aligned}
\tag{2.6}
$$

Once $(v_1^A)^N$ is found, Terminal A transmits $(v_1^A)_i$ to Terminal B. Note that the bits in the subset $\mathcal{L}_{U_1}^c\cap\mathcal{L}_{U_1|Y}$ can be recovered by B with high probability based on its own observations. For this reason, A transmits only the subvector of $(v_1^A)^N$ whose coordinate indices satisfy

$$
i\in\mathcal{I}'\triangleq\mathcal{I}\backslash(\mathcal{L}_{U_1}^c\cap\mathcal{L}_{U_1|Y}).
\tag{2.7}
$$

After observing y^N and receiving $(v_1^A)_i, i\in\mathcal{I}'$ from Terminal A, Terminal B calculates $(v_1^B)_i, i\in(\mathcal{I}')^c$ in a probabilistic way by sampling from the distribution

$$
\begin{aligned}
&Q_{(V_1^B)_i|(V_1^B)^{i-1}Y^N}((v_1^B)_i|(v_1^B)^{i-1},y^N)\\
&=\begin{cases}
1/2, & i\in\mathcal{F}_r\\
P_{(V_1)_i|(V_1)^{i-1}}((v_1^B)_i|(v_1^B)^{i-1}), & i\in\mathcal{F}_d\\
P_{(V_1)_i|(V_1)^{i-1}Y^N}((v_1^B)_i|(v_1^B)^{i-1},y^N), & i\in\mathcal{I}\backslash\mathcal{I}'.
\end{cases}
\end{aligned}
\tag{2.8}
$$

Since $(v_1^B)_i=(v_1^A)_i$ for all $i\in\mathcal{I}'$, Terminal B can form the sequence $(v_1^B)^N$. It then computes $(u_1^B)^N$ by performing the multiplication $(u_1^B)^N=(v_1^B)^NG_N$. Terminal A also computes its version of the sequence $(u_1^A)^N$ by finding $(u_1^A)^N=(v_1^A)^NG_N$.

2.3.2 Analysis of the first round of communication

First let us show that the rate of the first round of communication approaches the limiting value given in Theorem 2.1.

Lemma 2.3. *The rate of the first round of communication tends to $I(X;U_1|Y)$ as N goes to infinity.*

Proof. Since $\mathcal{L}_{U_1} \subseteq \mathcal{L}_{U_1|Y}$ (1.12), it follows that

$$\begin{aligned}\lim_{N\to\infty} \frac{|\mathcal{L}_{U_1}^c \cap \mathcal{L}_{U_1|Y}|}{N} &= \lim_{N\to\infty} \Big(\frac{|\mathcal{L}_{U_1|Y}|}{N} - \frac{|\mathcal{L}_{U_1}|}{N}\Big) \\ &= (1 - H(U_1|Y)) - (1 - H(U_1)) \\ &= I(U_1;Y).\end{aligned}$$

Moreover, the Markov chain condition $U_1 \to X \to Y$ imposed by Theorem 2.1 implies the inclusion $\mathcal{L}_{U_1|Y} \subseteq \mathcal{L}_{U_1|X}$. (See Lemma 4.7 of [7] for the proof.) Therefore, as the blocklength N goes to infinity, the rate of the first round of communication converges to

$$\begin{aligned}\lim_{N\to\infty} \frac{|\mathcal{I}|}{N} - I(U_1;Y) &= I(U_1;X) - I(U_1;Y) \\ &= (H(U_1) - H(U_1|X)) - (H(U_1) - H(U_1|Y)) \\ &= H(U_1|Y) - H(U_1|X) \\ &= H(U_1|Y) - H(U_1|X,Y) \qquad (2.9) \\ &= I(X;U_1|Y)\end{aligned}$$

as desired, where (2.9) again follows from the Markov condition. □

As already discussed, the main technical obstacle is to show that the joint statistics of the observations and the auxiliary random variables are close to the ideal statistic.

More specifically, we need to prove that the joint distributions of both $(U_1^A)^N, X^N, Y^N$ and $(U_1^B)^N, X^N, Y^N$ are close to $P_{(U_1)^N X^N Y^N}$, and in fact $(U_1^A)^N = (U_1^B)^N$ holds true with probability converging to 1.

Let $Q_{(U_1^A)^N X^N Y^N}((u_1^A)^N, x^N, y^N)$ denote the probability that Terminal A observes the source sequence x^N, Terminal B observes the source sequence y^N, and the procedure described by (2.6) outputs $(u_1^A)^N$.

Lemma 2.4. *For any $\beta_1 < \beta \in (0, 1/2)$, starting with some N we have*

$$\|Q_{(U_1^A)^N X^N Y^N} - P_{(U_1)^N X^N Y^N}\|_1 = O(2^{-N^{\beta_1}}).$$

The proof is given in Section 2.5.

Now we turn to the information processing by Terminal B described above (see (2.8)). Let

$$Q_{(U_1^B)^N X^N Y^N}((u_1^B)^N, x^N, y^N)$$

denote the probability that Terminals A and B observe the source sequences x^N and y^N respectively, and the described procedure outputs $(u_1^B)^N$. Then Terminal B's counterpart of Lemma 2.4 can be stated as follows.

Lemma 2.5. *For any $\beta_2 < \beta \in (0, 1/2)$, starting with some N we have*

$$\|Q_{(U_1^B)^N X^N Y^N} - P_{(U_1)^N X^N Y^N}\|_1 = O(2^{-N^{\beta_2}}) \tag{2.10}$$

$$\Pr\{(U_1^A)^N = (U_1^B)^N\} = 1 - O(2^{-N^{\beta_2}}). \tag{2.11}$$

Remark: The statement that we need below is given by (2.11). However, both claims (2.10) and (2.11) are used in the proof (recall the discussion in the introduction to this section).

The proof is given in Section 2.6.

2.3.3 The remaining rounds of communication

The purpose of this round to make it possible for both terminals to generate the random vector $(U_{i+1})^N$ so that the joint distribution of $\boldsymbol{U}^{i+1}, X^N, Y^N$ is close to the ideal distribution $P_{\boldsymbol{U}^{i+1},X^N,Y^N}$, where $\boldsymbol{U}^{i+1} \triangleq ((u_1)^N, \ldots, (u_{i+1})^N)$.

The communication protocol of the first round easily generalizes to the remaining rounds of communication. Consider for instance round $i+1$, where i is even. This means that information is communicated from A to B, and that sequences $\boldsymbol{u}^i \triangleq ((u_1)^N, \ldots, (u_i)^N)$ are already known to both sides.

Below we use notation P for the joint distribution

$$\begin{aligned} &P_{\boldsymbol{U}^t\boldsymbol{V}^tX^NY^N}(\boldsymbol{u}^t, \boldsymbol{v}^t, x^N, y^N) \\ &= \prod_{j=1}^{N} P_{XYU^t}(x_j, y_j, (u_1)_j, \ldots, (u_t)_j) \prod_{i=0}^{t-1} \mathbb{1}((u_{i+1})^N G_N = (v_{i+1})^N) \end{aligned} \tag{2.12}$$

and distributions derived from it, where $\boldsymbol{V}^t \triangleq ((V_1)^N, \ldots, (V_t)^N)$ and $\boldsymbol{U}^t \triangleq ((U_1)^N, \ldots, (U_t)^N)$. We assume that no errors occurred in earlier rounds, so both terminals observe identical copies of $\boldsymbol{U}^i$.

Round $i+1$ (i even): Terminal A partitions $[N]$ as follows:

$$\left.\begin{aligned} \mathcal{F}_r^{i+1} &= \mathcal{L}_{U_{i+1}}^c \cap \mathcal{H}_{U_{i+1}|(X,U^i)} \\ \mathcal{F}_d^{i+1} &= \mathcal{L}_{U_{i+1}} \\ \mathcal{I}^{i+1} &= \mathcal{L}_{U_{i+1}}^c \cap \mathcal{H}_{U_{i+1}|(X,U^i)}^c. \end{aligned}\right\} \tag{2.13}$$

It then generates a sequence $(v_{i+1}^A)^N$ randomly and successively by sampling from the

distribution

$$Q_{(V_{i+1}^A)_j|(V_{i+1}^A)^{j-1},(X^N,\boldsymbol{U}^i)}((v_{i+1}^A)_j|(v_{i+1}^A)^{j-1},(x^N,\boldsymbol{u}^i))$$
$$= \begin{cases} 1/2, & j \in \mathcal{F}_r^{i+1} \\ P_{(V_{i+1})^j|(V_{i+1})^{j-1}}((v_{i+1}^A)_j|(v_{i+1}^A)^{j-1}), & j \in \mathcal{F}_d^{i+1} \\ P_{(V_{i+1})^j|(V_{i+1})^{j-1},(X^N,\boldsymbol{U}^i)}((v_{i+1}^A)_j|(v_{i+1}^A)^{j-1},(x^N,\boldsymbol{u}^i)), & j \in \mathcal{I}^{i+1}. \end{cases} \tag{2.14}$$

Having found $(v_{i+1}^A)^N$, Terminal A computes the sequence $(u_{i+1}^A)^N = (v_{i+1}^A)^N G_N$.

To communicate information, A sends to B the sequence $(v_{i+1}^A)_j, j \in \mathcal{I}'^{i+1}$, where (2.13)

$$\mathcal{I}'^{i+1} = \mathcal{I}^{i+1} \backslash (\mathcal{L}^c_{U_{i+1}} \cap \mathcal{L}_{U_{i+1}|(Y,U^i)}).$$

Upon receiving the transmission, Terminal B generates $(v_{i+1}^B)_j, j \notin \mathcal{I}'^{i+1}$ by sampling from the distribution

$$Q_{(V_{i+1}^B)_j|(V_{i+1}^B)^{j-1},(Y^N,\boldsymbol{U}^i)}((v_{i+1}^B)_j|(v_{i+1}^B)^{j-1},(y^N,\boldsymbol{u}^i))$$
$$= \begin{cases} 1/2, & j \in \mathcal{F}_r, \\ P_{(V_{i+1})_j|(V^{i+1})^{j-1}}((v_{i+1}^B)_j|(v_{i+1}^B)^{j-1}), & j \in \mathcal{F}_d, \\ P_{(V_{i+1})_j|(V^{i+1})^{j-1},(Y^N,\boldsymbol{U}^i)}((v_{i+1}^B)_j|(v_{i+1}^B)^{j-1},(y^N,\boldsymbol{u}^i)), & j \in \mathcal{I}^{i+1} \backslash \mathcal{I}'^{i+1}. \end{cases} \tag{2.15}$$

The values $(v_{i+1}^B)_j, j \in \mathcal{I}'^{i+1}$ are known perfectly from the communication. Once the sequence $(v_{i+1}^B)^N$ has been formed, Terminal B finds $(u_{i+1}^B)^N = (v_{i+1}^B)^N G_N$.

If i is odd, the transmission proceeds from Terminal B to A. Both the description of the information processing and the analysis below apply after obvious changes of no-

tation.

Let us show that the rate of $(i+1)^{\text{th}}$ round of communication matches the lower bound of R_{i+1} given in (2.1).

Lemma 2.6. *If $i+1$ is odd, the rate of the $(i+1)^{th}$ round converges to $I(X;U_i|Y,U^{i-1})$ as N as goes to infinity. If $i+1$ is even, the rate converges to $I(Y;U_i|X,U^{i-1})$.*

Proof. Since $\mathcal{L}_{U_{i+1}} \subseteq \mathcal{L}_{U_{i+1}|(Y,U^i)}$, we have

$$\begin{aligned}\lim_{N\to\infty} \frac{|\mathcal{L}^c_{U_{i+1}} \cap \mathcal{L}_{U_{i+1}|(Y,U^i)}|}{N} &= \lim_{N\to\infty} \Big(\frac{|\mathcal{L}_{U_{i+1}|(Y,U^i)}|}{N} - \frac{|\mathcal{L}_{U_{i+1}}|}{N}\Big) \\ &= (1 - H(U_{i+1}|Y,U^i)) - (1 - H(U_{i+1})) \\ &= I(U_{i+1};Y,U^i).\end{aligned}$$

At the same time, Theorem 2.1 implies that $U_{i+1} \to (X,U^i) \to Y$, and so also $U_{i+1} \to (X,U^i) \to (Y,U^i)$. Hence, we have $\mathcal{L}_{U_{i+1}|(Y,U^i)} \subseteq \mathcal{L}_{U_{i+1}|(X,U^i)}$. So, as the blocklength goes to infinity, the rate of communication converges to

$$\begin{aligned}\lim_{N\to\infty} \frac{|\mathcal{I}|}{N} - I(U_{i+1};Y,U^i) &= I(U_{i+1};X,U^i) - I(U_{i+1};Y,U^i) \\ &= (H(U_{i+1}) - H(U_{i+1}|X,U^i)) \\ &\quad - (H(U_{i+1}) - H(U_{i+1}|Y,U^i)) \\ &= H(U_{i+1}|Y,U^i) - H(U_{i+1}|X,U^i) \\ &= H(U_{i+1}|Y,U^i) - H(U_{i+1}|X,U^i,Y) \qquad (2.16) \\ &= I(X;U_{i+1}|Y,U^i)\end{aligned}$$

which is consistent with (2.1). Eq. (2.16) is justified by the fact that $U_{i+1} \to (X,U^i) \to Y$ is a Markov chain.

The claim for the case when $i+1$ is even follows similarly. $\square$

2.3.4 Generalization of Lemmas 2.4 and 2.5 to multiple rounds

In this section we show that the joint distributions of both $\boldsymbol{U}_A^t, X^N, Y^N$ and $\boldsymbol{U}_B^t, X^N, Y^N$ are close to $P_{\boldsymbol{U}^t X^N Y^N}$, and that $\boldsymbol{U}_A^t = \boldsymbol{U}_B^t$ holds true with probability close to 1. This is accomplished by extending Lemmas 2.4 and 2.5 to the case of $t > 1$. We again face the same technical difficulties as discussed in the beginning of Sect. 2.3, but fortunately it is possible to leverage the proofs of these lemmas to complete the argument.

Let $Q_{(\boldsymbol{U}^t)^A X^N Y^N}$ and $Q_{(\boldsymbol{U}^t)^B X^N Y^N}$ be the empirical distributions induced by the sequence generation and communication protocols explained in Section 2.3.3. More formally, let

$$\begin{aligned}
&Q_{(\boldsymbol{U}^t)^A (\boldsymbol{V}^t)^A X^N Y^N}((\boldsymbol{u}^t)^A, (\boldsymbol{v}^t)^A, x^N, y^N) \\
&= \prod_{j=1}^{N} P_{X,Y}(x_j, y_j) \prod_{i=0}^{t-1} \mathbb{1}((u_{i+1}^A)^N G_N = (v_{i+1}^A)^N) \\
&\times \prod_{i=0}^{t-1} \prod_{j=1}^{N} Q_{(V_{i+1}^A)_j | (V_{i+1}^A)^{j-1}, (X^N, \boldsymbol{U}^i)}((v_{i+1}^A)_j | (v_{i+1}^A)^{j-1}, (x^N, (\boldsymbol{u}^i)^A))
\end{aligned}$$

and let $Q_{(\boldsymbol{U}^t)^B (\boldsymbol{V}^t)^B X^N Y^N}((\boldsymbol{u}^t)^B, (\boldsymbol{v}^t)^B, x^N, y^N)$ be defined similarly. Here, $(\boldsymbol{V}^t)^A \triangleq ((V_1^A)^N, \ldots, (V_t^A)^N), (\boldsymbol{U}^t)^A \triangleq ((U_1^A)^N, \ldots, (U_t^A)^N)$ and the notation $(\boldsymbol{V}^t)^B$ and $(\boldsymbol{U}^t)^B$ has a similar meaning.

Lemma 2.7. *For any $\beta_3 < \beta \in (0, 1/2)$, starting with some N we have*

$$\boldsymbol{Pr}\left\{(\boldsymbol{V}^t)^A = (\boldsymbol{V}^t)^B\right\} = 1 - O(2^{-N^{\beta_3}}) \tag{2.17}$$

$$\|Q_{(\boldsymbol{U}^t)^A X^N Y^N} - P_{\boldsymbol{U}^t X^N Y^N}\|_1 = O(2^{-N^{\beta_3}}) \tag{2.18}$$

$$\|Q_{(\boldsymbol{U}^t)^B X^N Y^N} - P_{\boldsymbol{U}^t X^N Y^N}\|_1 = O(2^{-N^{\beta_3}}). \tag{2.19}$$

Proof. The proof proceeds by induction on the number of rounds. From the Lemmas 2.4 and 2.5 we know that (2.17)-(2.19) hold true for $t = 1$. Let us assume that they hold for $t = i$ and prove them for $t = i + 1$. If $i + 1$ is odd, then the transmitting party is Terminal A. Then, from the induction hypothesis

$$\|Q_{(\boldsymbol{U}^i)^A X^N Y^N} - P_{\boldsymbol{U}^i X^N Y^N}\|_1 = O(2^{-N^{\beta_3}}) \tag{2.20}$$

one can prove (2.20) for $i + 1$ in the same way as done in the proof of Lemma 2.4 in Section 2.3.1 with the only difference that the Markov chain $U_{i+1} \to (X, U^i) \to Y$ is used instead of $U_1 \to X \to Y$. Further, we use the induction hypothesis

$$\|Q_{(\boldsymbol{U}^i)^B X^N Y^N} - P_{\boldsymbol{U}^i X^N Y^N}\|_1 = O(2^{-N^{\beta_3}}) \tag{2.21}$$

$$(\boldsymbol{V}^i)^A = (\boldsymbol{V}^i)^B = 1 - O(2^{-N^{\beta_3}}) \tag{2.22}$$

and the triangle inequality

$$\begin{aligned}\|Q_{(\boldsymbol{U}^{i+1})^B X^N Y^N} - P_{\boldsymbol{U}^{i+1} X^N Y^N}\|_1 \leq{}& \|Q_{(\boldsymbol{V}^i)^B X^N Y^N} - P_{\boldsymbol{V}^i X^N Y^N}\|_1 \\ &+ \|\widehat{Q}_{(\boldsymbol{V}^{i+1})^B X^N Y^N} - P_{\boldsymbol{V}^{i+1} X^N Y^N}\|_1\end{aligned} \tag{2.23}$$

where

$$\begin{aligned}\widehat{Q}_{(\boldsymbol{V}^{i+1})^B X^N Y^N}(\boldsymbol{v}^{i+1}, x^N, y^N) = {}& Q_{\boldsymbol{V}^B_{i+1}|(\boldsymbol{V}^i)^B X^N Y^N}(\boldsymbol{v}_{i+1}|\boldsymbol{v}^i, x^N, y^N) \\ &\times P_{\boldsymbol{V}^i X^N Y^N}(\boldsymbol{v}^i, x^N, y^N)\end{aligned}$$

similarly to (2.81), to observe that one can prove (2.21), (2.22) for $i + 1$ in the same way as in the proof of Lemma 2.5. This is because together with (2.21), (2.22), the inequality given by (2.23) makes it possible to reduce the analysis of Round $i + 1$ to that of Round 1. Here again we rely on the Markov condition $U_{i+1} \to (X, U^i) \to Y$ instead

of $U_1 \to X \to Y$. The case of $i+1$ even is handled similarly. In that case, we have the Markov chain condition $U_{i+1} \to (Y, U^i) \to X$ instead of $U_{i+1} \to (X, U^i) \to Y$. This completes the induction argument. □

2.3.5 Computing the functions

Let us show that the functions $f_A(x^N, y^N), f_B(x^N, y^N)$ can be computed based on the communication between the terminals described in the previous sections. Using Lemma 2.7, we prove that Terminals A and B compute their respective values of f_A and f_B respectively with probability close to one.

Proposition 2.8. *For Terminal A, there exists a $\tilde{Z}_A^N$ depending on x^N and $\boldsymbol{u}^t$ such that for all $0 < \beta_7 < \beta < 1/2$, we have*

$$\Pr\{\tilde{Z}_A^N = f_A(X^N, Y^N)\} = 1 - O(2^{-N^{\beta_7}}) \tag{2.24}$$

starting from some N. Similarly, for Terminal B, there exists a $\tilde{Z}_B^N$ depending on y^N and $\boldsymbol{u}^t$ such that

$$\Pr\{\tilde{Z}_B^N = f_B(X^N, Y^N)\} = 1 - O(2^{-N^{\beta_7}}) \tag{2.25}$$

starting from some N. Moreover, the computation of $\tilde{Z}_A^N$ and $\tilde{Z}_B^N$ is linear in blocklength.

Proof. The proof relies on the conditional entropy constraints $H(f_A(X,Y)|X,U^t) = 0$ and $H(f_B(X,Y)|Y,U^t) = 0$ in (2.1). First observe that these constraints easily extend to the case of N independent repetitions, i.e., that we have

$$H(f_A(X^N, Y^N)|X^N, \boldsymbol{U}^t) = 0 \tag{2.26}$$

$$H(f_B(X^N, Y^N)|Y^N, \boldsymbol{U}^t) = 0. \tag{2.27}$$

Then, define $\tilde{Z}_A^N$ and $\tilde{Z}_B^N$ as the values which satisfy

$$P_{f_A(X^N,Y^N)|X^N,\boldsymbol{U}^t}(\tilde{Z}_A^N|X^N,(\boldsymbol{U}^t)^A)=1$$

$$P_{f_B(X^N,Y^N)|Y^N,\boldsymbol{U}^t}(\tilde{Z}_B^N|Y^N,(\boldsymbol{U}^t)^B)=1$$

Note that the computation of both $\tilde{Z}_A^N$ and $\tilde{Z}_B^N$ is linear in blocklength. From (2.18)-(2.19) and the conditional entropy constraints (2.26)-(2.27), it follows that $\tilde{Z}_A^N$ and $\tilde{Z}_B^N$ exist with probability $1-O(2^{-N\beta_3})$. The rest of proof is devoted to show (2.24) and (2.25). For that purpose, we first rewrite (2.26) and (2.27) as

$$H(f_A(X^N,Y^N),X^N,\boldsymbol{U}^t)-H(X^N,\boldsymbol{U}^t)=0 \tag{2.28}$$

$$H(f_B(X^N,Y^N),Y^N,\boldsymbol{U}^t)-H(Y^N,\boldsymbol{U}^t)=0. \tag{2.29}$$

Let $H_Q(f_A(X^N,Y^N),X^N,(\boldsymbol{U}^t)^A)$ refer to the entropy defined by the distribution $Q_{(\boldsymbol{U}^t)^A X^N Y^N}$. For a sufficiently large N and for all $0<\beta_4<\beta_3<1/2$ we have

$$\begin{aligned}
&|H_Q(f_A(X^N,Y^N),X^N,(\boldsymbol{U}^t)^A)-H(f_A(X^N,Y^N),X^N,\boldsymbol{U}^t)| \\
&\le -\|Q_{f_A(X^N,Y^N)X^N(\boldsymbol{U}^t)^A}-P_{f_A(X^N,Y^N)X^N\boldsymbol{U}^t}\|_1 \\
&\qquad\times\log_2\frac{\|Q_{f_A(X^N,Y^N)X^N(\boldsymbol{U}^t)^A}-P_{f_A(X^N,Y^N)X^N\boldsymbol{U}^t}\|_1}{|\mathcal{Z}_A|^N\,|\mathcal{X}|^N\,2^{Nt}} &(2.30)\\
&\le -\|Q_{(\boldsymbol{U}^t)^A X^N Y^N}-P_{\boldsymbol{U}^t X^N Y^N}\|_1 \\
&\qquad\times\log_2\frac{\|Q_{(\boldsymbol{U}^t)^A X^N Y^N}-P_{\boldsymbol{U}^t X^N Y^N}\|_1}{|\mathcal{Z}_A|^N\,|\mathcal{X}|^N\,2^{Nt}} &(2.31)\\
&\le N(t+\log_2|\mathcal{X}|+\log_2|\mathcal{Z}_A|)\,\|Q_{(\boldsymbol{U}^t)^A X^N Y^N}-P_{\boldsymbol{U}^t X^N Y^N}\|_1 \\
&\qquad-\|Q_{(\boldsymbol{U}^t)^A X^N Y^N}-P_{\boldsymbol{U}^t X^N Y^N}\|_1\log_2(\|Q_{(\boldsymbol{U}^t)^A X^N Y^N}-P_{\boldsymbol{U}^t X^N Y^N}\|_1) \\
&= O(N2^{-N\beta_3})+O(N^{\beta_3}2^{-N\beta_3}) &(2.32)\\
&= O(2^{-N\beta_4}) &(2.33)
\end{aligned}$$

where (2.30) uses a standard estimate (e.g., [62, Theorem 17.3.3]), (2.31) is implied by the inequality

$$\|Q_{(\boldsymbol{U}^t)^A X^N Y^N} - P_{\boldsymbol{U}^t X^N Y^N}\|_1 \geq \|Q_{f_A(X^N,Y^N)X^N(\boldsymbol{U}^t)^A} - P_{f_A(X^N,Y^N)X^N\boldsymbol{U}^t}\|_1$$

and (2.32) is a consequence of (2.18). In the calculations above, $|\mathcal{Z}_A|$ denotes the cardinality of the range of f_A. Similarly to (2.33), we observe that

$$|H_Q(X^N, (\boldsymbol{U}^t)^A) - H(X^N, \boldsymbol{U}^t)| = O(2^{-N^{\beta_4}}). \tag{2.34}$$

Now estimates (2.33), (2.34) and the equality (2.28) imply that

$$H_Q(f_A(X^N, Y^N)|X^N, (\boldsymbol{U}^t)^A) = O(2^{-N^{\beta_4}}) \tag{2.35}$$

for all $0 < \beta_4 < \beta < 1/2$ and N large enough.

On account of (2.19) and (2.29) this derivation can be repeated for f_B as well, and we obtain

$$H_Q(f_B(X^N, Y^N)|X^N, (\boldsymbol{U}^t)^B) = O(2^{-N^{\beta_4}}). \tag{2.36}$$

Expanding (2.35), we get

$$\sum_{x^N,(\boldsymbol{u}^t)^A} Q_{X^N,(\boldsymbol{U}^t)^A}(x^N, (\boldsymbol{u}^t)^A) \sum_{z_A^N \in \mathcal{Z}_A^N} Q_{f_A(X^N,Y^N)|X^N,(\boldsymbol{U}^t)^A}(z_A^N|x^N, (\boldsymbol{u}^t)^A)$$
$$\times \log_2 \frac{1}{Q_{f_A(X^N,Y^N)|X^N,(\boldsymbol{U}^t)^A}(z_A^N|x^N, (\boldsymbol{u}^t)^A)} = O(2^{-N^{\beta_4}}) \leq 2^{-N^{\beta_5}} \tag{2.37}$$

where $\beta_5 < \beta_4$ can be chosen arbitrarily close to β_4 provided that N is sufficiently large.

Now let us define the set

$$S = \Bigg\{(x^N, (\boldsymbol{u}^t)^A) \ : \ \sum_{z_A^N \in \mathcal{Z}_A^N} Q_{f_A(X^N,Y^N)|X^N,(\boldsymbol{U}^t)^A}(z_A^N|x^N, (\boldsymbol{u}^t)^A)$$
$$\times \log_2 \frac{1}{Q_{f_A(X^N,Y^N)|X^N,(\boldsymbol{U}^t)^A}(z_A^N|x^N, (\boldsymbol{u}^t)^A)} > \sqrt{2^{-N^{\beta_5}}}\Bigg\}.$$

Using (2.37) we obtain

$$\sum_{(x^N,(\boldsymbol{u}^t)^A)\in S} Q_{X^N,(\boldsymbol{U}^t)^A}(x^N,(\boldsymbol{u}^t)^A) \leq \sqrt{2^{-N^{\beta_5}}}$$

and therefore with probability at least $1-2^{-\frac{N^{\beta_5}}{2}}$ Terminal A can find a value $\hat{Z}_A^N$ such that

$$\frac{1-Q_{f_A(X^N,Y^N)|X^N,(\boldsymbol{U}^t)^A}(\hat{Z}_A^N|x^N,(\boldsymbol{u}^t)^A)}{(e-1)\ln 2} \leq 2^{-\frac{N^{\beta_5}}{2}} \tag{2.38}$$

where we have used the inequality $(1-x)/(e-1) \leq -x\ln x, e^{-1} \leq x \leq 1$ which can be proved by differentiation. From (2.38) we obtain

$$Q_{f_A(X^N,Y^N)|X^N,(\boldsymbol{U}^t)^A}(\hat{Z}_A^N|x^N,(\boldsymbol{u}^t)^A) \geq 1-\ln 2\,(e-1)\,2^{-\frac{N^{\beta_5}}{2}}. \tag{2.39}$$

Hence, from (2.39), we conclude that Terminal A can calculate the function $f_A(X^N,Y^N)$ correctly with probability at least

$$(1-2^{-\frac{N^{\beta_5}}{2}})\left[1-\ln 2\,(e-1)\,2^{-\frac{N^{\beta_5}}{2}}\right] = 1-O(2^{-N^{\beta_6}}).$$

Repeating the derivation above starting from (2.36), we prove that Terminal B can find a value $\hat{Z}_B^N$ and thus calculate the function $f_B(X^N,Y^N)$ correctly with probability $1-O(2^{-N^{\beta_6}})$. Lastly, using (2.18)-(2.19) again, we observe that

$$\Pr\{\tilde{Z}_A^N = \hat{Z}_A^N\} = 1-O(2^{-N^{\beta_3}})$$

$$\Pr\{\tilde{Z}_B^N = \hat{Z}_B^N\} = 1-O(2^{-N^{\beta_3}})$$

Hence, we conclude

$$\Pr\{f_A(X^N,Y^N) = \tilde{Z}_A^N\} = 1-O(2^{-N^{\beta_6}})-O(2^{-N^{\beta_3}}) = 1-O(2^{-N^{\beta_7}})$$

$$\Pr\{f_B(X^N,Y^N) = \tilde{Z}_B^N\} = 1-O(2^{-N^{\beta_6}})-O(2^{-N^{\beta_3}}) = 1-O(2^{-N^{\beta_7}})$$

as desired. □

The proof that the rate region (2.1) can be achieved using polar coding is now complete.

In conclusion we note that all the proofs presented in Sections 2.3.1, 2.3.3, and 2.3.4 can be extended to the case when the auxiliary random variables $U_1, U_2, \ldots, U_t$ are not binary using for instance the methods in [9], [10]. Another alternative is viewing U_i as the composition of bits $U_{i,1}, \ldots, U_{i,r}$ and dividing each round of communication into r steps each of which are responsible from the conditional distribution

$$Q(u_{i,k}|u^{i-1}, u_{i,1}, \ldots, u_{i,k-1}, x^N), k = 1, 2, \ldots, r.$$

We confine ourselves to this brief remark, leaving the details to the reader.

2.3.6 An example of interactive function computation

As observed earlier, to complete the description of the communication scheme we need to specify the random variables $U_1, U_2, \ldots, U_t$ that satisfy the Markov chain conditions and conditional entropy equalities in (2.1). The description of these random variables depends on the function being computed and is studied on a case-by-case basis.

Following [34] consider the example in which Terminals A and B observe binary random sequences with $X \sim \text{Ber}(p)$, $Y \sim \text{Ber}(q)$, where X and Y are independent. Suppose that both terminals need to compute the AND function, i.e., $f_A(x, y) = f_B(x, y) = x \wedge y$. We can assume that there exist random variables $(V_x, V_y) \sim \text{Uniform}([0, 1]^2)$ such that $X \triangleq \mathbb{1}_{[1-p,1]}(V_x)$ and $Y \triangleq \mathbb{1}_{[1-q,1]}(V_y)$. Further, let $\Gamma \triangleq \{(\alpha(s), \beta(s)), 0 \leq s \leq 1\}$ be a curve defined parametrically with boundary conditions $\alpha(0) = \beta(0) = 0$, $\alpha(1) = 1 - p$ and $\beta(1) = 1 - q$ and let $0 = s_0 < s_1 < \cdots < s_{t/2-1} < s_{t/2} = 1$ be a partition of

the segment $[0, 1]$. Consider the following t random variables

$$\begin{aligned} U_{2i-1} &\triangleq \mathbb{1}_{[\alpha(s_i),1]\times[\beta(s_{i-1}),1]}(V_x, V_y) \\ U_{2i} &\triangleq \mathbb{1}_{[\alpha(s_i),1]\times[\beta(s_i),1]}(V_x, V_y) \end{aligned} \tag{2.40}$$

where $i = 1, \ldots, t/2$. In [34] it is shown that for all partitions and curves Γ of the form defined above, random variables (2.40) satisfy both the Markov chain and the conditional entropy constraints in (2.1).

Hence, for the AND function, we can construct a polar-coded communication scheme based on (2.40). In each transmission round, we can construct codes following the partition of the index set $[N]$ as in (2.5) and (2.13). For example, according to (2.13) we have to determine the noiseless and noisy bits of the transmission for the channel with binary input U_{i+1} and output (X, U^i). After $n = \log_2 N$ iterations the size of the output alphabets of the virtual channels obtained will be $2^{N(i+1)} = 2^{2^n(i+1)}$. To simplify the computations involved in the code construction one can rely on the alphabet reduction methods proposed in [56].

Moreover, the choice of random variables according to (2.40) minimizes the *sum-rate* $\sum_{j=1}^{t} R_j$ for $t \to \infty$. (See [63] for the proof.) In [34], it is also shown that

$$R_{\text{sum},\infty} = h_2(p) + ph_2(q) + p\log_2(q) + p(1-q)\log_2 e < h_2(p) + ph_2(q) = R^A_{\text{sum},2} \tag{2.41}$$

where h_2 is the binary entropy function, $R_{\text{sum},\infty}$ is the minimum sum-rate as $t \to \infty$, and $R^A_{\text{sum},2}$ is the minimum sum-rate for the case $t = 2$ and it is Terminal A that transmits first. This example shows that for the problem of computing the AND function one can gain by performing several rounds on interactive communication.

2.4 Polar Codes for Collocated Networks

In this section we consider the multi-terminal function computation problem introduced in Sect. 2.2.2. We will show that the polar-coded communication scheme introduced above can be modified to achieve the rate region given in Theorem 2.2.

Let $U_1, \ldots, U_t$ be random variables that satisfy the Markov chain conditions and conditional entropy conditions of Theorem 2.2.

2.4.1 Communication protocol

Before starting to explain the protocol, we define P as

$$\begin{aligned} &P_{\boldsymbol{V}^t,\boldsymbol{U}^t,\boldsymbol{X}^m}(\boldsymbol{v}^t,\boldsymbol{u}^t,\boldsymbol{x}^m) \\ &= \prod_{i=1}^{t} \mathbb{1}((u_i)^N G_N = (v_i)^N) \prod_{k=1}^{N} P_{X^m,U^t}((x_1)_k,\ldots,(x_m)_k,(u_1)_k,\ldots,(u_t)_k) \end{aligned} \tag{2.42}$$

where $\boldsymbol{x}^m \triangleq ((x_1)^N,\ldots,(x_m)^N)$, $\boldsymbol{v}^t \triangleq ((v_1)^N,\ldots,(v_t)^N)$, and $\boldsymbol{u}^t \triangleq ((u_1)^N,\ldots,(u_t)^N)$. Similarly to Section 2.3, the aim of the communication is to let the terminals generate $\boldsymbol{U}^t$ such that the joint distribution of $\boldsymbol{X}^m$ and $\boldsymbol{U}^t$ is close to $P_{\boldsymbol{U}^t,\boldsymbol{X}^m}$.

Suppose that the transmission starts with Terminal 1. We again rely on the partition of $[N]$ of the form

$$\left.\begin{aligned} \mathcal{F}_r &= \mathcal{L}^c_{U_1} \cap \mathcal{H}_{U_1|X_1} \\ \mathcal{F}_d &= \mathcal{L}_{U_1} \\ \mathcal{I} &= \mathcal{L}^c_{U_1} \cap \mathcal{H}^c_{U_1|X_1} \end{aligned}\right\} \tag{2.43}$$

similarly to (2.5). Having observed a realization $(x_1)^N$, the first terminal finds a sequence $(v_1)^N$ by sampling from the distribution

$$Q_{(V_1)_i|(V_1)^{i-1},(X_1)^N}((v_1)_i|(v_1)^{i-1},(x_1)^N) = \begin{cases} 1/2, & i \in \mathcal{F}_r \\ P_{(V_1)_i|(V_1)^{i-1}}((v_1)_i|(v_1)^{i-1}), & i \in \mathcal{F}_d \\ P_{(V_1)_i|(V_1)^{i-1},(X_1)^N}((v_1)_i|(v_1)^{i-1},(x_1)^N), & i \in \mathcal{I}. \end{cases} \tag{2.44}$$

Based on $(v_1)^N$ Terminal 1 finds the sequence $(u_1)^N = (v_1)^N G_N$. and broadcasts the bits $(v_1)_i, i \in \mathcal{I}$. The remaining terminals including the sink terminal calculate their versions of $(v_1)_i, i \notin \mathcal{I}$ from the conditional distribution

$$Q_{(V_1)_i|(V_1)^{i-1}}((v_1)_i|(v_1)^{i-1}) = \begin{cases} 1/2, & i \in \mathcal{F}_r, \\ P_{(V_1)_i|(V_1)^{i-1}}((v_1)_i|(v_1)^{i-1}), & i \in \mathcal{F}_d. \end{cases}$$

Then they find the sequence $(u_1)^N = (v_1)^N G_N$ and record the result[1].

Note that for large N the rate of communication converges to $R_1 = \lim_{N\to\infty} |\mathcal{I}|/N = I(U_1; X_1)$, consistent with (2.3).

In general, the i^{th} message, $i \in [t]$ is generated and sent by Terminal $j, j = 1 + (i - 1 \bmod m)$. At the start of the i^{th} round of communication we assume that all the terminals have the same $i-1$ sequences $\boldsymbol{u}^{i-1}$, each of which was computed as a result of

[1]With small probability the sequences $(u_1)^N$ computed at different terminals will be different; see also Sect. 2.4.2 below. Abusing notation, we do not differentiate them below in this section.

the previous messages. Terminal j first relies on the partition of $[N]$ given by

$$\left.\begin{aligned}\mathcal{F}_r^i &= \mathcal{L}_{U_i}^c \cap \mathcal{H}_{U_i|X_j,U^{i-1}} \\ \mathcal{F}_d^i &= \mathcal{L}_{U_i} \\ \mathcal{I}^i &= \mathcal{L}_{U_i}^c \cap \mathcal{H}_{U_i|X_j,U^{i-1}}^c.\end{aligned}\right\} \tag{2.45}$$

and finds computes $(v_i)^N$ by sampling from the distribution

$$\begin{aligned}&Q_{(V_i)_k|(V_i)^{k-1},(X_j)^N,\boldsymbol{U}^{i-1}}((v_i)_k|(v_i)^{k-1},(x_j)^N,\boldsymbol{u}^{i-1}) \\ &= \begin{cases} 1/2, & k \in \mathcal{F}_r^i \\ P_{(V_i)_k|(V_i)^{k-1}}((v_i)_k|(v_i)^{k-1}), & k \in \mathcal{F}_d^i \\ P_{(V_i)_k|(V_i)^{k-1},(X_j)^N,\boldsymbol{U}^{i-1}}((v_i)_k|(v_i)^{k-1},(x_j)^N,\boldsymbol{u}^{i-1}), & k \in \mathcal{I}^i. \end{cases}\end{aligned} \tag{2.46}$$

Then, as usual, Terminal j computes $(u_i)^N = (v_i)^N G_N$ and broadcasts the sequence $(v_i)_k, k \in \mathcal{I}'^i$, where $\mathcal{I}'^i = \mathcal{I}^i \backslash \mathcal{L}_{U_i}^c \cap \mathcal{L}_{U_i|U^{i-1}}$. Since $\mathcal{L}_{U_i|U^{i-1}} \subseteq \mathcal{L}_{U_i|X_j,U^{i-1}}$ implies the inclusion $\mathcal{L}_{U_i}^c \cap \mathcal{L}_{U_i|U^{i-1}} \subseteq \mathcal{I}^i$, the rate of this broadcast converges to

$$\begin{aligned}\lim_{N\to\infty} \frac{|\mathcal{I}'^i|}{N} &= I(U_i;U^{i-1},X^j) - I(U_i;U^{i-1}) \\ &= H(U_i|U^{i-1}) - H(U_i|U^{i-1},X^j) \\ &= I(X_j;U_i|U^{i-1})\end{aligned}$$

in accordance with (2.3). Based on the sequence $(v_i)_k, k \in \mathcal{I}'^i$, the remaining terminals determine $(v_i)_k, k \notin \mathcal{I}'^i$ by sampling from the distribution

$$Q_{(V_i)_k|(V_i)^{k-1},\boldsymbol{U}^{i-1}}((v_i)_k|(v_i)^{k-1},\boldsymbol{u}^{i-1})$$

$$= \begin{cases} 1/2, & k \in \mathcal{F}_r^i \\ P_{(V_i)_k|(V_i)^{k-1}}((v_i)_k|(v_i)^{k-1}), & k \in \mathcal{F}_d^i \\ P_{(V_i)_k|(V_i)^{k-1},\boldsymbol{U}^{i-1}}((v_i)_k|(v_i)^{k-1},\boldsymbol{u}^{i-1}) & k \in \mathcal{I}^i \backslash \mathcal{I}'^i. \end{cases} \tag{2.47}$$

As a result, the remaining terminals acquire their versions of the sequence $(u_i)^N$.

2.4.2 The analysis of the protocol

To show that the proposed protocol attains the overall goal of function computation we need to show two facts. First, we should prove in each round the sequences $(u_i)^N$ found by the receiving terminals with high probability are the same as the sequence computed by the broadcasting terminal. Second, we need to prove that the sequences $\boldsymbol{u}^t$ we obtain have a joint distribution with the source sequence which is very close to the distribution P given by (2.42), making it possible to satisfy the condition $H(f(X^m)|U^t) = 0$. This entails the same problem as the one we faced in Section 2.3.1: namely, to prove one of these facts directly, we need the other one. As in Lemma 2.5 in Section 2.3.1, we will prove both statements simultaneously by induction. Similarly to Section 2.3.1, we assume that the terminals are provided with random bits whose indices fall in the subsets $\mathcal{F}_r^1, \ldots, \mathcal{F}_r^t$.

Let us introduce some notation. Denote by $(U_l)_j^N$ the random sequence generated by Terminal $j = 1 + (l - 1 \bmod m)$ in Round l and by $(U_l)_r^N$ the sequence computed by Terminal $r \neq j$ after the transmission by Terminal j. Denote by $Q_{\boldsymbol{U}^t,\boldsymbol{X}^m}$ the joint

distribution of the source sequences $\boldsymbol{x}^m = ((x_1)^N, (x_2)^N, \ldots, (x_m)^N)$ and the sequences $\boldsymbol{u}^t = ((u_1)^N, (u_2)^N, \ldots, (u_t)^N)$ generated in the course of the communication. More formally, we define $Q_{\boldsymbol{U}^t,\boldsymbol{X}^m}$ as the marginal distribution of

$$Q_{\boldsymbol{U}^t\boldsymbol{V}^t\boldsymbol{X}^m}(\boldsymbol{u}^t, \boldsymbol{v}^t, \boldsymbol{x}^m) = \prod_{k=1}^{N} P_{X^m}((x_1)_k, \ldots, (x_m)_k) \prod_{i=1}^{t} \mathbb{1}((u_i)^N G_N = (v_i)^N)$$
$$\times \prod_{i=1}^{t}\prod_{k=1}^{N} Q_{(V_i)^k|(V_i)^{k-1},((X_j)^N,\boldsymbol{U}^{i-1})}((v_i)_k|(v_i)^{k-1}, ((x_j)^N, \boldsymbol{u}^{i-1}))$$

where $Q_{(V_i)_k|(V_i)^{k-1},((X_j)^N,\boldsymbol{U}^{i-1})}((v_i)_k|(v_i)^{k-1}, (x_j)^N, \boldsymbol{u}^{i-1})$ is given in (2.46).

Lemma 2.9. *For any $\beta_7 < \beta \in (0, 1/2)$ and for all $l \in [t]$, and for all $r \neq j$, starting from some N, we have*

$$\Pr\{(U_l)_j^N = (U_l)_r^N\} = 1 - O(2^{-N^{\beta_7}}) \tag{2.48}$$

$$\|Q_{\boldsymbol{U}^t\boldsymbol{X}^m} - P_{\boldsymbol{U}^t\boldsymbol{X}^m}\|_1 = O(2^{-N^{\beta_7}}) \tag{2.49}$$

Proof. We begin with the case $t = 1$ in which case (2.49) takes the form

$$\|Q_{(U_1)^N\boldsymbol{X}^m} - P_{(U_1)^N\boldsymbol{X}^m}\|_1 = O(2^{-N^{\beta_7}}). \tag{2.50}$$

Recall that from Lemma 2.4 we have the estimate

$$\|Q_{(U_1)^N(X_1)^N} - P_{(U_1)^N(X_1)^N}\|_1 = O(2^{-N^{\beta_1}}). \tag{2.51}$$

On account of the Markov condition $U_1 \to X_1 \to X_2, \ldots, X_m$ in the statement of Theorem 2.2, we have

$$\mathcal{L}_{U_1}^c \cap \mathcal{H}_{U_1|X_1} = \mathcal{L}_{U_1}^c \cap \mathcal{H}_{U_1|X^m}$$

$$\mathcal{L}_{U_1}^c \cap \mathcal{H}_{U_1|X_1}^c = \mathcal{L}_{U_1}^c \cap \mathcal{H}_{U_1|X^m}^c \tag{2.52}$$

Hence for all $i \in \mathcal{I} = \mathcal{L}_{U_1}^c \cap \mathcal{H}_{U_1|X_1}^c$ we have

$$P_{(V_1)_i|(V_1)^{i-1},(X_1)^N}((v_1)_i|(v_1)^{i-1},(x_1)^N) = P_{(V_1)_i|(V_1)^{i-1},\boldsymbol{X}^m}((v_1)_i|(v_1)^{i-1},\boldsymbol{x}^m) \quad (2.53)$$

From (2.52) and (2.53), we see that (2.44) is fully equivalent to the computation which uses $\boldsymbol{x}^m$ rather than just $(x_1)^N$ in the conditional probability for the case $i \in \mathcal{I}$. Therefore, (2.50) follows from Lemma 2.4, completing the proof of (2.49) for $t = 1$. In regards to (2.48) we note that for $t = 1$ it reduces to a special case of (2.11) in which Y^N is unavailable.

Our next step is to generalize (2.50) to t broadcasts, i.e., to show (2.49). For that purpose, similarly to the triangle inequality method used in Sections 2.3.1 and 2.3.4, we write

$$\begin{aligned}\|\mathbb{Q}_{\boldsymbol{U}^i\boldsymbol{X}^m} - \mathbb{P}_{\boldsymbol{U}^i\boldsymbol{X}^m}\|_1 \leq \|\mathbb{Q}_{\boldsymbol{U}^{i-1}\boldsymbol{X}^m} - \mathbb{P}_{\boldsymbol{U}^{i-1}\boldsymbol{X}^m}\|_1 \\ + \|\widehat{\mathbb{Q}}_{\boldsymbol{U}^i\boldsymbol{X}^m} - \mathbb{P}_{\boldsymbol{U}^i\boldsymbol{X}^m}\|_1 \end{aligned} \quad (2.54)$$

where

$$\begin{aligned}\widehat{Q}_{\boldsymbol{U}^i\boldsymbol{X}^m}(\boldsymbol{u}^i,\boldsymbol{x}^m) = \mathbb{1}((v_i)^{1:N}G_N = (u_i)^{1:N})\, P_{\boldsymbol{U}^{i-1},\boldsymbol{X}^m}(\boldsymbol{u}^{i-1},\boldsymbol{x}^m) \\ \times \prod_{k=1}^{N} Q_{(V_i)_k|(V_i)^{k-1},(X_j)^N,\boldsymbol{U}^{i-1}}((v_i)_k|(v_i)^{k-1},(x_j)^N,\boldsymbol{u}^{i-1}). \end{aligned} \quad (2.55)$$

Now we are ready to use induction. From (2.50) we see that (2.49) is true for $t = 1$. Assume that it is also true for $t = i - 1$. Eq. (2.54) implies that to prove (2.49) holds for $t = i$, it is sufficient to show

$$\|\widehat{\mathbb{Q}}_{\boldsymbol{U}^i\boldsymbol{X}^m} - \mathbb{P}_{\boldsymbol{U}^i\boldsymbol{X}^m}\|_1 = O(2^{-N^{\beta_7}}). \quad (2.56)$$

Since the marginal of $\widehat{Q}$ for $\boldsymbol{u}^{i-1}, \boldsymbol{x}^m$ equals P, to show (2.56) we need to focus on the error introduced by the i^{th} round of sequence generation. Owing to the Markov chain condition $U_i \to (U^{i-1}, X_j) \to (X^{j-1}, X_{j+1}, X_{j+2}, \ldots, X_m)$, for all $k \in \mathcal{I}^i = \mathcal{L}^c_{U_i} \cap \mathcal{H}^c_{U_i|X_j,U^{i-1}} = \mathcal{L}^c_{U_i} \cap \mathcal{H}^c_{U_i|X^m,U^{i-1}}$ we have

$$\begin{aligned} &P_{(V_i)_k|(V_i)^{k-1},(X_j)^N,\boldsymbol{U}^{i-1}}((v_i)_k|(v_i)^{k-1},(x_j)^N,\boldsymbol{u}^{i-1}) \\ &\quad = P_{(V_i)_k|(V_i)^{k-1},\boldsymbol{X}^m,\boldsymbol{U}^{i-1}}((v_i)_k|(v_i)^{k-1},\boldsymbol{x}^m,\boldsymbol{u}^{i-1}) \end{aligned}$$

Therefore (2.56) follows from Lemma 2.4. This completes the induction argument for (2.49).

Finally let us justify the the induction step for (2.48) for $t = i$. For this assume that (2.48) and (2.49) hold for $t = i - 1$ and note that the proof follows the steps in the proof of Lemma 2.5 with no changes. □

In regards to the function computation, we note that the analysis carried out in Section 2.3.5 implies that the sink node computes the function $f(\boldsymbol{X}^m)$ correctly with probability converging to 1 as N goes to infinity. This completes the proof of achievability for the region (2.4) using the described polar coding scheme.

The analysis presented in this section can be easily modified to account for the case of nonbinary auxiliary random variables $U_1, \ldots, U_t$. The remarks made in the end of Section 2.3.5 apply to the present case as well.

2.5 Appendix 2.A: Proof of Lemma 2.4

To simplify the notation, in the proof we write $Q((u_1)^N, x^N, y^N)$, $Q((v_1)^N, x^N)$ instead of

$$Q_{(U_1^A)^N X^N Y^N}((u_1^A)^N, x^N, y^N), Q_{(V_1^A)^N X^N}((v_1^A)^N, x^N)$$

etc. and extend this convention to the distributions derived from P as well as the corresponding conditional and marginal distributions.

First let us rewrite $P((u_1)^N, x^N, y^N)$ as

$$\begin{aligned} P((u_1)^N, x^N, y^N) &= \prod_{i=1}^{N} P_{XYU_1}(x_i, y_i, (u_1)_i) \\ &= \prod_{i=1}^{N} P_{XY}(x_i, y_i) P_{U_1|X}((u_1)_i|x_i) \qquad (2.57) \\ &= P(x^N, y^N) P((u_1)^N|x^N) \qquad (2.58) \end{aligned}$$

where (2.57) is due to $U_1 \to X \to Y$. Now note that according to (2.6) Terminal A has to generate the sequence $(u_1)^N$ based only on x^N because it does not have access to y^N. So, for all $(u_1)^N, x^N, y^N$ it follows that

$$\begin{aligned} Q((u_1)^N, x^N, y^N) &= Q(x^N, y^N) Q((u_1)^N|x^N) \\ &= P(x^N, y^N) Q((u_1)^N|x^N). \qquad (2.59) \end{aligned}$$

Using (2.58) and (2.59) we compute

$$\sum_{(u_1)^N,x^N,y^N} |Q((u_1)^N,x^N,y^N) - P((u_1)^N,x^N,y^N)|$$

$$= \sum_{(u_1)^N,x^N,y^N} P(x^N,y^N)\ \left|Q((u_1)^N|x^N) - P((u_1)^N|x^N)\right|$$

$$= \sum_{(u_1)^N,x^N} P(x^N)\ \left|Q((u_1)^N|x^N) - P((u_1)^N|x^N)\right|$$

$$= \sum_{(u_1)^N,x^N} |Q((u_1)^N,x^N) - P((u_1)^N,x^N)|. \tag{2.60}$$

Denote the right-hand side of (2.60) by $\Delta(P,Q)$. Since Arıkan's transform is a one-to-one map between $(u_1)^N$ and $(v_1)^N$, we have

$$\sum_{(v_1)^N,x^N} |Q((v_1)^N,x^N) - P((v_1)^N,x^N)| = \Delta(P,Q). \tag{2.61}$$

Then from (2.60) and (2.61) we conclude that

$$\sum_{(v_1)^N,x^N} |Q((v_1)^N,x^N) - P((v_1)^N,x^N)| = \|Q_{(U_1^A)^N X^N Y^N} - P_{(U_1)^N X^N Y^N}\|_1$$

Thus, to prove the lemma it suffices to show that

$$\Delta(P,Q) = \sum_{(v_1)^N,x^N} |Q((v_1)^N,x^N) - P((v_1)^N,x^N)| = O(2^{-N^{\beta_1}}).$$

Let us write $\Delta(P,Q)$ as

$$\Delta(P,Q) = \sum_{(v_1)^N,x^N} P(x^N) \left| \prod_{i=1}^{N} Q((v_1)_i|(v_1)^{i-1},x^N) - \prod_{i=1}^{N} P((v_1)_i|(v_1)^{i-1},x^N) \right|. \tag{2.62}$$

Applying the telescoping expansion argument used in Lemma 3.5 of [7], one can bound

above the right-hand side of (2.62) to obtain

$$\Delta(P,Q) \le \sum_{x^N} P(x^N) \sum_{(v_1)^N} \sum_{i=1}^{N} |Q((v_1)_i|(v_1)^{i-1}, x^N) - P((v_1)_i|(v_1)^{i-1}, x^N)| \\ \times \prod_{j=1}^{i-1} P((v_1)_j|(v_1)^{j-1}, x^N) \prod_{j=i+1}^{N} Q((v_1)_j|(v_1)^{j-1}, x^N). \tag{2.63}$$

Substituting (2.6) into (2.63), we obtain

$$\begin{aligned} &\Delta(P,Q) \\ &\le \sum_{i\in\mathcal{F}_r\cup\mathcal{F}_d} \sum_{(v_1)^{i-1},x^N} \sum_{(v_1)_i=0}^{1} |Q((v_1)_i|(v_1)^{i-1}, x^N) - P((v_1)_i|(v_1)^{i-1}, x^N)| \\ &\quad \times P((v_1)^{i-1}, x^N) \\ &= 2\sum_{i\in\mathcal{F}_r} E_P \left|\frac{1}{2} - P((V_1)_i = 0|(V_1)^{i-1}, X^N)\right| \\ &+ 2\sum_{i\in\mathcal{F}_d} E_P|P((V_1)_i = 0|(V_1)^{i-1}) - P((V_1)_i = 0|(V_1)^{i-1}, X^N)| \end{aligned} \tag{2.64}$$

where E_P is a shorthand for the expected value $E_{P_{(V_1)^{i-1},X^N}}$.

Proposition 2.10. *If $i \in \mathcal{F}_r$, then*

$$E_P \left|\frac{1}{2} - P((V_1)_i = 0|(V_1)^{i-1}, X^N)\right| \le 2^{-\frac{N^\beta}{2}-\frac{1}{2}}. \tag{2.65}$$

Proof. The proof of Lemma 3.8 of [7] is directly applicable here. We first observe

$$\begin{aligned} &Z((V_1)_i|(V_1)^{i-1}, X^N) \\ &= 2\sum_{(v_1)^{i-1},x^N} P((v_1)^{i-1}, x^N)\sqrt{P((V_1)_i = 0|(v_1)^{i-1}, x^N)} \\ &\quad \times \sqrt{P((V_1)_i = 1|(v_1)^{i-1}, x^N)} \\ &= 2E_P\Big[\sqrt{P((V_1)_i = 0|(V_1)^{i-1}, X^N)P((V_1)_i = 1|(V_1)^{i-1}, X^N)}\Big]. \end{aligned} \tag{2.66}$$

Making use of the fact that for $i \in \mathcal{F}_r$, Def. (2.5) implies that $Z((V_1)_i|(V_1)^{i-1}, X^N) \geq 1 - 2^{-N^\beta}$, we observe that

$$E_P\left[\frac{1}{2} - \sqrt{P((V_1)_i = 0|(V_1)^{i-1}, X^N)P((V_1)_i = 1|(V_1)^{i-1}, X^N)}\right] \leq 2^{-N^\beta}/2.$$

Hence also

$$E_P\left[\frac{1}{4} - P((V_1)_i = 0|(V_1)^{i-1}, X^N)P((V_1)_i = 1|(V_1)^{i-1}, X^N)\right] \leq 2^{-N^\beta}/2.$$

Note that the two probabilities inside the brackets sum to one, so we obtain

$$E_P\left[\frac{1}{2} - P((V_1)_i = 0|(V_1)^{i-1}, X^N)\right]^2 \leq 2^{-N^\beta}/2.$$

Finally, using convexity, we obtain (2.65), as desired. □

Proposition 2.11. *If $i \in \mathcal{F}_d$, then there exists an absolute constant $c \in \mathbb{R}$ such that*

$$E_P|P((V_1)_i = 0|(V_1)^{i-1}) - P((V_1)_i = 0|(V_1)^{i-1}, X^N)| \leq c\, 2^{-\frac{N^\beta}{2}}.$$

Proof. First note that $i \in \mathcal{F}_d \subseteq \mathcal{L}_{U_1}$ implies $Z((V_1)_i|(V_1)^{i-1}) \leq 2^{-N^\beta}$ which in turn implies

$$Z((V_1)_i|(V_1)^{i-1}, X^N) \leq 2^{-N^\beta}.$$

Hence for any $a \in (0, 1)$

$$\begin{aligned} 2\sqrt{a(1-a)}\,\Pr\{a < P((V_1)_i = 0|(V_1)^{i-1}) < 1 - a\} \\ &\leq 2E_P\sqrt{P((V_1)_i = 0|(V_1)^{i-1})P((V_1)_i = 1|(V_1)^{i-1})} \\ &\leq 2^{-N^\beta} \end{aligned}$$

and

$$2\sqrt{a(1-a)}\Pr\{a < P((V_1)_i = 0|(V_1)^{i-1}, X^N) < 1-a\}$$
$$\leq 2E_P\sqrt{P((V_1)_i = 0|(V_1)^{i-1}, X^N)P((V_1)_i = 1|(V_1)^{i-1}, X^N)}$$
$$\leq 2^{-N^\beta}$$

follows. In particular, for $a = 2^{-N^\beta}$, we obtain

$$P\left(2^{-N^\beta} < P((V_1)_i = 0|(V_1)^{i-1}) < 1 - 2^{-N^\beta}\right) \leq \frac{1}{2}\sqrt{\frac{2^{-N^\beta}}{1-2^{-N^\beta}}} \tag{2.67}$$

$$P\left(2^{-N^\beta} < P((V_1)_i = 0|(V_1)^{i-1}, X^N) < 1 - 2^{-N^\beta}\right) \leq \frac{1}{2}\sqrt{\frac{2^{-N^\beta}}{1-2^{-N^\beta}}}. \tag{2.68}$$

Now, letting $D = [0, 2^{-N^\beta}] \cup [1 - 2^{-N^\beta}, 1]$ we obtain

$$\Pr\left\{P((V_1)_i = 0|(V_1)^{i-1}) \in D \wedge P((V_1)_i = 0|(V_1)^{i-1}, X^N) \in D\right\}$$
$$\geq 1 - \sqrt{\frac{2^{-N^\beta}}{1-2^{-N^\beta}}}. \tag{2.69}$$

Our next step will be to show that both the probabilities

$$\Pr\Big\{P((V_1)_i = 0|(V_1)^{i-1}) \in [1 - 2^{-N^\beta}, 1]$$
$$\wedge\, P((V_1)_i = 0|(V_1)^{i-1}, X^N) \in [0, 2^{-N^\beta}]\Big\} \tag{2.70}$$

$$\Pr\Big\{P((V_1)_i = 0|(V_1)^{i-1}) \in [0, 2^{-N^\beta}]$$
$$\wedge\, P((V_1)_i = 0|(V_1)^{i-1}, X^N) \in [1 - 2^{-N^\beta}, 1]\Big\} \tag{2.71}$$

are small. Let $S(i, N)$ be the set of pairs $((v_1)^{i-1}, x^N)$ accounting for the event in (2.70).

Write

$$\Pr\{(V_1)_i = 0 | (V_1)^{i-1} = (v_1)^{i-1}\} \Pr\{(V_1)_i = 1, (V_1)^{i-1} = (v_1)^{i-1}\}$$
$$= \Pr\{(V_1)_i = 1 | (V_1)^{i-1} = (v_1)^{i-1}\}$$
$$\times \Pr\{(V_1)_i = 0 | (V_1)^{i-1} = (v_1)^{i-1}\} \Pr\{(V_1)^{i-1} = (v_1)^{i-1}\}$$

and observe that if the pair $((v_1)^{i-1}, x^N) \in S(i, N)$ then the first term on the left is ≈ 1 and the first term on the right is ≈ 0. This implies that

$$(1 - 2^{-N^\beta}) \Pr\{(V_1)_i = 1, (V_1)^{i-1} = (v_1)^{i-1}\}$$
$$\leq 2^{-N^\beta} \Pr\{(V_1)_i = 0, (V_1)^{i-1} = (v_1)^{i-1}\}. \tag{2.72}$$

In the same way from (2.70) we obtain

$$2^{-N^\beta} \Pr\{(V_1)_i = 1, (V_1)^{i-1} = (v_1)^{i-1}, X^N = x^N\}$$
$$\geq (1 - 2^{-N^\beta}) \Pr\{(V_1)_i = 0, (V_1)^{i-1} = (v_1)^{i-1}, X^N = x^N\}. \tag{2.73}$$

From (2.72), (2.73) we see that (2.70) can be bounded above as follows:

$$\sum_{((v_1)^{i-1}, x^N) \in S(i,N)} \Pr\{(V_1)^{i-1} = (v_1)^{i-1}, X^N = x^N\}$$
$$= \sum_{((v_1)^{i-1}, x^N) \in S(i,N)} \sum_{(v_1)_i = 0}^{1} \Pr\{(V_1)_i = (v_1)_i, (V_1)^{i-1} = (v_1)^{i-1}, X^N = x^N\}$$
$$\leq \left(1 + \frac{2^{-N^\beta}}{1 - 2^{-N^\beta}}\right) \sum_{((v_1)^{i-1}, x^N) \in S(i,N)} \Pr\{(V_1)_i = 1, (V_1)^{i-1} = (v_1)^{i-1}, X^N = x^N\}$$
$$\leq \frac{1}{1 - 2^{-N^\beta}} \sum_{(v_1)^{i-1} \in S(i,N)} \Pr\{(V_1)_i = 1, (V_1)^{i-1} = (v_1)^{i-1}\}$$
$$\leq \frac{2^{-N^\beta}}{(1 - 2^{-N^\beta})^2} \sum_{(v_1)^{i-1} \in S(i,N)} \Pr\{(V_1)_i = 0, (V_1)^{i-1} = (v_1)^{i-1}\}$$
$$\leq \frac{2^{-N^\beta}}{(1 - 2^{-N^\beta})^2} \Pr\{(V_1)_i = 0\}. \tag{2.74}$$

Similarly, it can be shown that the probability (2.71) is small. Indeed, let $T(i,N)$ be the set of pairs $((v_1)^{i-1}, x^N)$ accounting for the event in (2.71). As in (2.72), (2.73), for each $((v_1)^{i-1}, x^N) \in T(i,N)$ we have

$$\begin{aligned} & 2^{-N^\beta} \Pr\{(V_1)_i = 1, (V_1)^{i-1} = (v_1)^{i-1}\} \\ & \quad \geq (1 - 2^{-N^\beta}) \Pr\{(V_1)_i = 0, (V_1)^{i-1} = (v_1)^{i-1}\} \end{aligned}$$

$$\begin{aligned} & (1 - 2^{-N^\beta}) \Pr\{(V_1)_i = 1, (V_1)^{i-1} = (v_1)^{i-1}, X^N = x^N\} \\ & \quad \leq 2^{-N^\beta} \Pr\{(V_1)_i = 0, (V_1)^{i-1} = (v_1)^{i-1}, X^N = x^N\}. \end{aligned}$$

From these two relations we conclude that (2.71) can be bounded above as

$$\begin{aligned} & \sum_{((v_1)^{i-1}, x^N) \in T(i,N)} \Pr\{(V_1)^{i-1} = (v_1)^{i-1}, X^N = x^N\} \\ & = \sum_{((v_1)^{i-1}, x^N) \in T(i,N)} \sum_{(v_1)_i = 0}^{1} \Pr\{(V_1)_i = (v_1)_i, (V_1)^{i-1} = (v_1)^{i-1}, X^N = x^N\} \\ & \leq \Big(1 + \frac{2^{-N^\beta}}{1 - 2^{-N^\beta}}\Big) \sum_{((v_1)^{i-1}, x^N) \in T(i,N)} \Pr\{(V_1)_i = 0, (V_1)^{i-1} = (v_1)^{i-1}, X^N = x^N\} \\ & \leq \frac{1}{1 - 2^{-N^\beta}} \sum_{(v_1)^{i-1} \in T(i,N)} \Pr\{(V_1)_i = 0, (V_1)^{i-1} = (v_1)^{i-1}\} \\ & \leq \frac{2^{-N^\beta}}{(1 - 2^{-N^\beta})^2} \sum_{(v_1)^{i-1} \in T(i,N)} \Pr\{(V_1)_i = 1, (V_1)^{i-1} = (v_1)^{i-1}\} \\ & \leq \frac{2^{-N^\beta}}{(1 - 2^{-N^\beta})^2} \Pr\{(V_1)_i = 1\}. \end{aligned} \tag{2.75}$$

Substituting (2.74) and (2.75) in (2.69), we observe that

$$\begin{aligned} & \Pr\Big\{ \big|P((V_1)_i = 0 | (V_1)^{i-1}) - P((V_1)_i = 0 | (V_1)^{i-1}, X^N)\big| \leq 2^{-N^\beta} \Big\} \\ & \quad \geq 1 - \sqrt{\frac{2^{-N^\beta}}{1 - 2^{-N^\beta}}} - \frac{2^{-N^\beta}}{(1 - 2^{-N^\beta})^2}. \end{aligned}$$

Let ξ be the random variable in the brackets, and note that $\Pr\{\xi \in [0,1]\} = 1$. Then use the fact that

$$E\xi \le 2^{-N^\beta} \Pr(\xi \le 2^{-N^\beta}) + \Pr(\xi > 2^{-N^\beta}) \le 2^{-N^\beta} + \Pr(\xi > 2^{-N^\beta}).$$

This translates into

$$\begin{aligned} &E_P|P((V_1)_i = 0|(V_1)^{i-1}) - P((V_1)_i = 0|(V_1)^{i-1}, X^N)| \\ &\le \sqrt{\frac{2^{-N^\beta}}{1-2^{-N^\beta}}} + \frac{2^{-N^\beta}}{(1-2^{-N^\beta})^2} + 2^{-N^\beta}. \end{aligned} \tag{2.76}$$

which completes the proof of Proposition 2.11. □

Combining Propositions 2.10 and 2.11 with (2.64), we obtain

$$\|Q_{(U_1^A)^N X^N Y^N} - P_{(U_1)^N X^N Y^N}\|_1 = \Delta(P,Q) = O(N 2^{-\frac{N^\beta}{2}})$$

which proves Lemma 2.4.

2.6 Appendix 2.B: Proof of Lemma 2.5

We prove (2.10) and (2.11) by induction on i, using the following forms of these relations for a given value of i:

$$\|Q_{(U_1^B)^i X^N Y^N} - P_{(U_1)^i X^N Y^N}\|_1 = O(2^{-N^{\beta_2}}) \tag{2.77}$$

$$\Pr\left\{(V_1^A)^i = (V_1^B)^i\right\} = 1 - O(2^{-N^{\beta_2}}). \tag{2.78}$$

To prove the induction base, note that there are four different possibilities for $i = 1$ which may be contained in any of the sets $\mathcal{F}_r$, $\mathcal{F}_d$, $\mathcal{I}\backslash\mathcal{I}'$, and $\mathcal{I}'$; see (2.5), (2.7).

1. If $1 \in \mathcal{F}_r$, then Terminals A and B will make the same decision with probability 1, i.e., $\Pr\left\{(V_1^A)_1 = (V_1^B)_1\right\} = 1$. This is because we assume that the terminals share a common randomness to decide $(v_1^A)_i$ and $(v_1^B)_i$, $i \in \mathcal{F}_r$. To prove (2.77), note that the Markov condition $U_1 \to X \to Y$ implies that $(U_1)^N \to X^N \to Y^N$, which implies that $(V_1)^N \to X^N \to Y^N$ and finally $(V_1)_1 \to X^N \to Y^N$. We use this in the following calculation:

$$
\begin{aligned}
&\|Q_{(V_1^B)_1 X^N Y^N} - P_{(V_1)_1 X^N Y^N}\|_1 \\
&= \sum_{x^N, y^N} \sum_{v_1=0}^{1} |Q_{(V_1^B)_1|X^N Y^N}(v_1|x^N, y^N) - P_{(V_1)_1|X^N Y^N}(v_1|x^N, y^N)| P_{X^N Y^N}(x^N, y^N) \\
&= \sum_{x^N} \sum_{v_1=0}^{1} |1/2 - P_{(V_1)_1|X^N}(v_1|x^N)| P_{X^N}(x^N) \\
&= 2E_P|1/2 - P((V_1)_1 = 0|X^N)|.
\end{aligned}
$$

   Here the last step follows because $(v_1^B)_i$'s are uniformly random for $i \in \mathcal{F}_r$, as given by (2.8). Now using Proposition 2.10, we obtain (2.77) for $i = 1$.

2. Let $1 \in \mathcal{F}_d = \mathcal{L}_{U_1}$. To prove (2.77) we use the same argument as above in item (1), using the Markov condition $(V_1)_1 \to X^N \to Y^N$ together with Proposition 2.11.

   To prove (2.78) note that for $i \in \mathcal{F}_d$ we have $Z((V_1)_i|(V_1)^{i-1}) \leq 2^{-N^\beta}$; see (2.5), (1.13)[2]. Therefore, the random variable $(V_1^A)_i$ is almost deterministic, and the same is true for the random variable $(V_1^B)_i$. This observation is stated formally in (2.67).

   From (2.67), we see that with probability $1 - \frac{1}{2}\sqrt{\frac{2^{-N^\beta}}{1-2^{-N^\beta}}}$, Terminals A and B decide $(V_1^A)_1$ and $(V_1^B)_1$ respectively based on independent copies of a Bernoulli random

[2]If $i = 1$ then $(V)^{i-1}$ is empty, but below we will use this argument for all i.

variable that takes the value 0 with probability p such that either $p \leq 2^{-N^\beta}$ or $p \geq 1 - 2^{-N^\beta}$. Therefore, it follows that for sufficiently large N

$$\Pr\{(V_1^A)_1 = (V_1^B)_1\} \geq \left(1 - \frac{1}{2}\sqrt{\frac{2^{-N^\beta}}{1 - 2^{-N^\beta}}}\right)(1 - 2p(1-p)) = 1 - O(2^{-\frac{N^\beta}{2}})$$

$$= 1 - O(2^{-N^{\beta_2}}).$$

3. Let $1 \in \mathcal{I}\backslash\mathcal{I}' \subseteq \mathcal{L}_{U_1|Y} \subseteq \mathcal{L}_{U_1|X}$. Estimate (2.77) will follow from the following proposition.

Proposition 2.12. *If $i \in \mathcal{I}\backslash\mathcal{I}'$, then for sufficiently large N*

$$E_P|P((V_1)_i = 0|(V_1)^{i-1}, Y^N) - P((V_1)_i = 0|(V_1)^{i-1}, X^N, Y^N)|$$

$$= O(2^{-\frac{N^\beta}{2}}).$$

Proof. On account of (1.11) for $i \in \mathcal{I}\backslash\mathcal{I}' \subseteq \mathcal{L}_{U_1|Y}$ we obtain

$$Z((V_1)_i|(V_1)^{i-1}, Y^N) \leq 2^{-N^\beta},$$

which implies that

$$Z((V_1)_i|(V_1)^{i-1}, X^N, Y^N) \leq 2^{-N^\beta}.$$

The remaining part of the proof follows the steps in the proof of Proposition 2.11. Namely, inequalities (2.74), (2.75) and (2.69) are valid in this case as well, and we again obtain the estimate

$$E_P\big|P((V_1)_i = 0|(V_1)^{i-1}, Y^N) - P((V_1)_i = 0|(V_1)^{i-1}, X^N, Y^N)\big|$$

$$\leq \sqrt{\frac{2^{-N^\beta}}{1 - 2^{-N^\beta}}} + \frac{2^{-N^\beta}}{(1 - 2^{-N^\beta})^2} + 2^{-N^\beta}.$$

This completes the proof of Proposition 2.12. □

Now notice that

$$
\begin{aligned}
&\|Q_{(V_1^B)_1X^NY^N} - P_{(V_1)_1X^NY^N}\|_1 \\
&= \sum_{x^N,y^N}\sum_{a=0}^{1} |Q_{(V_1^B)_1X^NY^N}(a,x^N,y^N) - P_{(V_1)_1X^NY^N}(a,x^N,y^N)| \\
&= \sum_{x^N,y^N}\sum_{a=0}^{1} P_{X^NY^N}(x^N,y^N) \\
&\quad \times |Q_{(V_1^B)_1|X^NY^N}(a|x^N,y^N) - P_{(V_1)_1|X^NY^N}(a|x^N,y^N)| \\
&\overset{(2.8)}{=} \sum_{x^N,y^N}\sum_{a=0}^{1} P_{X^NY^N}(x^N,y^N) \\
&\quad \times |P_{(V_1)_1|Y^N}(a|y^N) - P_{(V_1)_1|X^NY^N}(a|x^N,y^N)| \\
&= \sum_{a=0}^{1} E_{P_{X^NY^N}} \left|P_{(V_1)_1|Y^N}(a|Y^N) - P_{(V_1)_1|X^NY^N}(a|X^N,Y^N)\right| \\
&= 2E_{P_{X^NY^N}} \left|P_{(V_1)_1|Y^N}(0|Y^N) - P_{(V_1)_1|X^NY^N}(0|X^N,Y^N)\right| \\
&= O(2^{-\frac{N^\beta}{2}})
\end{aligned}
$$

where the last estimate follows from Proposition 2.12. This proves (2.77).

Regarding (2.78) note that for $i \in \mathcal{I}\backslash\mathcal{I}'$ we have $Z((V_1)_i|(V_1)^{i-1},Y^N) \le 2^{-N^\beta}$; see (2.5), (1.11). This also implies that

$$Z((V_1)_i|(V_1)^{i-1},X^N) = Z((V_1)_i|(V_1)^{i-1},X^N,Y^N) \le 2^{-N^\beta}.$$

Hence, similarly to (2.67) and (2.68), we have

$$
\begin{aligned}
P\left(2^{-N^\beta} < P((V_1)_i = 0|(V_1)^{i-1},X^N) < 1-2^{-N^\beta}\right) &\le \frac{1}{2}\sqrt{\frac{2^{-N^\beta}}{1-2^{-N^\beta}}} \\
P\left(2^{-N^\beta} < P((V_1)_i = 0|(V_1)^{i-1},Y^N) < 1-2^{-N^\beta}\right) &\le \frac{1}{2}\sqrt{\frac{2^{-N^\beta}}{1-2^{-N^\beta}}}.
\end{aligned}
$$

Repeating the arguments that led us to conclude that the probabilities in (2.70) and (2.71) are small, we obtain

$$\begin{aligned}
&\Pr\Big\{P((V_1)_i = 0|(V_1)^{i-1}, X^N) \in [1 - 2^{-N^\beta}, 1] \\
&\quad \wedge P((V_1)_i = 0|(V_1)^{i-1}, Y^N) \in [0, 2^{-N^\beta}]\Big\} \\
&+ \Pr\Big\{P((V_1)_i = 0|(V_1)^{i-1}, X^N) \in [0, 2^{-N^\beta}] \\
&\quad \wedge P((V_1)_i = 0|(V_1)^{i-1}, Y^N) \in [1 - 2^{-N^\beta}, 1]\Big\} \leq \frac{2^{-N^\beta}}{(1 - 2^{-N^\beta})^2}
\end{aligned}$$

Now let us perform a calculation similar to the one in item (2):

$$\begin{aligned}
\Pr\{(V_1^A)_1 = (V_1^B)_1\} &\geq \left(1 - \sqrt{\frac{2^{-N^\beta}}{1 - 2^{-N^\beta}}} - \frac{2^{-N^\beta}}{(1 - 2^{-N^\beta})^2}\right)(1 - 2^{-N^\beta + 1}) \\
&= 1 - O(2^{-\frac{N^\beta}{2}}) \\
&= 1 - O(2^{-N^{\beta_2}})
\end{aligned}$$

This completes the proof of (2.78).

4. If $1 \in \mathcal{I}'$, then using the Markov condition $U_1 \to X \to Y$, we observe that (2.77) holds trivially. Since the bit $(V_1^A)_1$ is known perfectly at terminal B, the same is true for (2.78).

This establishes the induction base.

Now assume that (2.77) and (2.78) hold for some $i \geq 1$. To prove that (2.77) is also valid for $i + 1$ write

$$
\begin{aligned}
&\|Q_{(V_1^B)^{i+1}X^NY^N} - P_{(V_1)^{i+1}X^NY^N}\|_1 \\
&\quad = \sum_{(v_1)^{i+1},x^N,y^N} |Q_B((v_1)^{i+1},x^N,y^N) - P((v_1)^{i+1},x^N,y^N)| \\
&\quad \leq \sum_{(v_1)^{i+1},x^N,y^N} Q_B((v_1)_{i+1}|(v_1)^i,x^N,y^N) \\
&\qquad \times |Q_B((v_1)^i,x^N,y^N) - P((v_1)^i,x^N,y^N)| \\
&\qquad + \sum_{(v_1)^{i+1},x^N,y^N} P((v_1)^i,x^N,y^N) \\
&\qquad \times |Q_B((v_1)_{i+1}|(v_1)^i,x^N,y^N) - P((v_1)_{i+1}|(v_1)^i,x^N,y^N)| \qquad (2.79) \\
&\quad = \sum_{(v_1)^i,x^N,y^N} |Q_B((v_1)^i,x^N,y^N) - P((v_1)^i,x^N,y^N)| \\
&\qquad + \sum_{(v_1)^{i+1},x^N,y^N} |\widehat{Q}_B((v_1)^{i+1},x^N,y^N) - P((v_1)^{i+1},x^N,y^N)| \\
&\quad = \|Q_{(V_1^B)^iX^NY^N} - P_{(V_1)^iX^NY^N}\|_1 + \|\widehat{Q}_{(V_1^B)^{i+1}X^NY^N} - P_{(V_1)^{i+1}X^NY^N}\|_1 \qquad (2.80)
\end{aligned}
$$

where for simplicity we write $Q_B((v_1)^{i+1},x^N,y^N)$ instead of

$$Q_{(V_1^B)^{i+1}X^NY^N}((v_1^B)^{i+1},x^N,y^N),$$

and where

$$
\begin{aligned}
&\widehat{Q}_{(V_1^B)^{i+1}X^NY^N}((v_1)^{i+1},x^N,y^N) \\
&\quad = Q_{(V_1^B)_{i+1}|(V_1^B)^iX^NY^N}((v_1)_{i+1}|(v_1)^i,x^N,y^N)P_{(V_1)^iX^NY^N}((v_1)^i,x^N,y^N) \qquad (2.81)
\end{aligned}
$$

is the distribution whose marginal for $(v_1)^i,x^N,y^N$ equals $P((v_1)^i,x^N,y^N)$. From the induction hypothesis given by (2.77), the first term in (2.80) is small, and so it is enough to prove that

$$\|\widehat{Q}_{(V_1^B)^{i+1}X^NY^N} - P_{(V_1)^{i+1}X^NY^N}\|_1 = O(2^{-N^{\beta_2}}).$$

This estimate follows from the arguments made for the case $i = 1$ with no changes.

Regarding (2.78) we note that the induction hypothesis implies that the distribution $Q_{(V_1^B)^i X^N Y^N}$ is close to the "true" distribution P by the L_1 distance. Therefore, the arguments given above for each of the cases (1)-(4) for $i = 1$ are applicable to the case of general $i + 1$ given i.

This completes the induction argument and finishes the proof of Lemma 2.5.

Chapter 3: Achieving Secrecy Capacity of the Wiretap Channel and Broadcast Channel with a Confidential Component

3.1 Introduction

We begin with introducing the communication problem for the wiretap channel. Denote the input alphabet of the transmitter by $\mathcal{X}$, and the output alphabets of the channels W_1 and W_2 by $\mathcal{Y}$ and $\mathcal{Z}$, respectively. The messages that the transmitter can convey to Receiver 1 form a finite set denoted below by $\mathcal{M}$. For transmission over the channel the message is encoded using a mapping $f : \mathcal{M} \to \mathcal{X}^N$, where $\mathcal{X}^N$ is an N-fold repetition of the input alphabet. We say that f is a length-N block encoder of the transmitter. Capacity-attaining schemes for the wiretap channel rely on randomized encoding, i.e., a mapping that sends $\mathcal{M}$ to a probability distribution on $\mathcal{X}^N$. In other words, the message $m \in \mathcal{M}$ is encoded as a sequence $x^N \in \mathcal{X}^N$ with probability $f(x^N|m)$, and the encoder is defined as a matrix of conditional probabilities $(f(x^N|m))_{m\in\mathcal{M}}^{x^N\in\mathcal{X}^N}$.

The decoder of Receiver 1 is a mapping $\phi : \mathcal{Y}^N \to \mathcal{M}$. We also denote by $P_{Y|X}$ and $P_{Z|X}$ the conditional distributions induced by the channels W_1 and W_2, respectively, and define the induced distributions $P_{Y^N|X^N}, P_{Z^N|X^N}$, where, for instance, $P_{Y^N|X^N}(y^N|x^N) = \prod_{i=1}^N P_{Y|X}(y_i|x_i)$, where y_i and x_i refer to the i-th symbol of the

vectors y^N and x^N, respectively.

Definition 3.1.1. *We say that the encoder-decoder pair* (f, ϕ) gives rise to (N, ϵ)-transmission *over the wiretap channel* $\mathcal{W}$ *if*

$$\sum_{x^N \in \mathcal{X}^N} f(x^N|m) P_{Y^N|X^N}(\phi(y^N) = m|x^N) \geq 1 - \epsilon \quad \forall m \in \mathcal{M} \tag{3.1}$$

$$I(M; Z^N) \leq \epsilon, \tag{3.2}$$

where M *is the message random variable (RV) and* Z^N *is the RV that corresponds to the observations of Receiver 2.*

In Definition 3.1.1, Eq. (3.1) represents the reliability of communication condition while (3.2) answers the security of transmission requirement. We note that in many works on transmission with a secrecy constraint the security condition was formulated in a more relaxed way, namely as the inequality

$$(1/N) I(M; Z^N) < \epsilon. \tag{3.3}$$

This is particularly true about pre-1990s works in information theory, but also applies to some very recent works on the wiretap channel, e.g., [39, 41, 42]. However, as shown by Maurer in [44,45], this constraint does not fulfill the intuitive security requirements in the system. More specifically, it is possible to construct examples in which inequality (3.3) is satisfied and at the same time Receiver 2 is capable of learning $N^{1-\epsilon}$ out of N bits of the encoding x^N. In view of this, Maurer suggested (3.2) as a better alternative to condition (3.3). As a result, currently (3.3) is called the "weak security constraint" as opposed to the stronger constraint (3.2). In this chapter we design coding schemes that provide strong

secrecy, so below we work only with condition (3.2).

The secrecy capacity of the wiretap channel is defined as follows.

Definition 3.1.2. *The value $R > 0$ is called an achievable rate for the wiretap channel $\mathcal{W}$ if there exists a sequence of message sets $\mathcal{M}_N$ and encoder-decoder pairs (f_N, ϕ_N) giving rise to (N, ϵ_N) transmission with $\epsilon_N \to 0$ and $\frac{1}{N} \log |\mathcal{M}_N| \to R$ as $N \to \infty$. The secrecy capacity C_s is the supremum of achievable rates for the wiretap channel.*

The following theorem provides an expression for C_s.

Theorem 3.1. ([50]; see also [23, p.411]) *The secrecy capacity of the wiretap channel $\mathcal{W}$ equals*

$$C_s = \max[I(V;Y) - I(V;Z)], \tag{3.4}$$

where the maximum is computed over all RVs V, X, Y, Z such that the Markov condition $V \to X \to Y, Z$ holds true, and such that $P_{Y|X} = W_1$, $P_{Z|X} = W_2$.

Another special case of the wiretap channel relates to the combinatorial version of the erasure channel (the so-called wiretap channel of type II [64]) in which Receiver 2 can choose to observe any t symbols out of N transmitted symbols. Constructive capacity-achieving solutions for this case are based on MDS codes [65] or extractors [66].

In [67], it is shown that C_s is achievable with strong security using invertible extractors, if both W_1 and W_2 are binary symmetric channels. Both encoding and decoding algorithms in [67] have polynomial complexity. Moreover, [67] also claims that its proof method can be easily extended to other wiretap channels as long as both W_1 and W_2 are symmetric.

After the introduction of polar codes by Arıkan, achieving C_s via polar coding has been considered by different works, mostly under the degradedness assumption. Recall that a channel $W_2 : \mathcal{X} \to \mathcal{Z}$ is called *degraded* with respect to a channel $W_1 : \mathcal{X} \to \mathcal{Y}$ if there exists a stochastic $|\mathcal{Y}| \times |\mathcal{Z}|$ matrix $P_{Z|Y}(z|y)$ such that for all $x \in \mathcal{X}, z \in \mathcal{Z}$

$$P_{Z|X}(z|x) = \sum_{y \in \mathcal{Y}} P_{Y|X}(y|x) P_{Z|Y}(z|y). \tag{3.5}$$

The wiretap channel $\mathcal{W}$ is called degraded if the channel to the eavesdropper is degraded with respect to the main channel. In this case Theorem 3.1 affords a simpler formulation because there is no need in the auxiliary RV V. Namely, in the degraded case the secrecy capacity equals [23, Probl. 17.8]

$$C_s = C(W_1) - C(W_2) \tag{3.6}$$

(this specialization is true under slightly more general assumptions, but we will not need them below).

Communication over degraded wiretap channels using polar codes was considered in a number of papers, notably, [17, 41–43]. The main result of these works is that secrecy capacity (3.6) can be attained under the weak security constraint. We note that the degraded case is easier to handle with polar codes because of the specific nature of the polar codes construction (more on this below in Sect. 3.2). Another step was made by [46] which suggested a polar coding scheme that attains the rate C_s of a symmetric degraded wiretap channel $\mathcal{W}$ under the strong security requirement (3.2). More details about the results of [46] are given in Sect. 3.2 below.

The problem of attaining secrecy capacity of the general wiretap channel (3.4) under the strong secrecy condition and without the degradedness assumption was further studied

in [47]. A polar coding scheme suggested in this work attains a transmission rate of $\max_{p_X(x)}[H(X|Z) - H(X|Y)]$. Clearly $H(X|Z) - H(X|Y) \leq C_s$ for all X since one can take $V = X$ in the Markov chain $V \to X \to Y, Z$, which appears in Theorem 3.1. It is not immediately clear for which channels the result of [47] actually attains the secrecy capacity of $\mathcal{W}$. At the same time, the coding scheme employed in [47] relies on two nested layers of the polarizing transform. The decoder for the second (outer) layer works with the probability distribution generated by the first decoder, which is not easily computable. Thus, the low complexity decoding claim of the construction made in [47] is not supported by the known decoding procedures for polar codes. For these reasons the construction in [47] does not resolve the question of constructing an explicit capacity-achieving scheme for the nondegraded case of wiretap channels.

In related works [48, 49] the problem of constructing capacity achieving schemes for wiretap channels was addressed for the case of quantum channels. The constructions suggested in these works attain symmetric secrecy capacity of quantum wiretap channels. These constructions require a shared secret key between the transmitter and Receiver 1. This requirement seems to be intrinsic to polar code constructions for this problem including our work. However the constructions in [48, 49] require a positive-rate shared key, which results in a communication scheme that transmits at rates separated from capacity.

In this chapter we aim to solve the general problem of communicating over the wiretap channel, removing the degradedness assumption (3.5). We also do not assume that either of the channels W_1, W_2 is symmetric. The main idea of our work is to exploit the Markov chain conditions intrinsic to secure communication problems using polar

codes. In Section 3.3 we propose a polar coding scheme that attains the secrecy capacity (3.4) under the strong security assumption. Both the encoding and decoding complexity estimates of our construction are $O(N \log N)$, where N is the length of the encoding. In Section 3.4.2 we generalize our construction to cover the case when a part of transmitter's message is public, i.e., is designed to be conveyed both to Receivers 1 and 2. This model, called a broadcast channel with confidential messages, is in fact the principal model in the founding work of Csiszár and Körner [50] on this topic.

Apart from the basic polar coding results [2], our solution of the described problems relies on the previous work on the wiretap channel [46], the polar coding scheme for the broadcast channel of [24], and the construction of polar codes for general memoryless channels in [3]. A new idea introduced in our solution is related to a stochastic encoding scheme that emulates the random coding proof of the capacity theorem in [50], whereby polarization is used for the values of the auxiliary random variable V in Theorem 3.1, followed by a stochastic encoding into a channel codeword. Another insight, which is particularly useful for the broadcast channel result in Sect. 3.4, is related to a partition of the coordinates of the transmitted block that enables simultaneous decoding of different parts of the transmitted message by both receivers, whereby the decoder of polar codes is used by the receivers according to their high- and low-entropy bits. It becomes possible to show that the receivers recover the bits designed to communicate with each of them with high probability, and that the secret part of the message is not accessible to the unintended recipient.

3.2 A Closer Look at Prior Works on Polar Coding for the Wiretap Channel

To explain our proposal we will first discuss some of the schemes available in the literature. We begin with the transmission scheme of [17] (see also [41–43]). As already remarked, these works are concerned with the special case when the channel W_2 is degraded with respect to W_1 and aim to attain the rate value (3.6) with weak secrecy. Let X^N be a random uniform vector over $\{0,1\}^N$. Similarly to $\mathcal{H}_{X|Y}$ and $\mathcal{L}_{X|Y}$ given by (1.13), define the following subsets of indices:

$$\mathcal{H}_{X|Z} = \{i \in [N] : Z(U_i|U^{i-1}, Z^N) \geq 1 - \delta_N\}$$

$$\mathcal{L}_{X|Z} = \{i \in [N] : Z(U_i|U^{i-1}, Z^N) \leq \delta_N\}$$

where $U^N = X^N G_N$, and Z^N is the output that Receiver 2 observes when the transmitter sends X^N. Partition the set $[N]$ as follows:

$$\begin{aligned} \mathcal{R} &= \mathcal{L}_{X|Z} \\ \mathcal{I} &= \mathcal{L}_{X|Y} \backslash \mathcal{L}_{X|Z} \\ \mathcal{B} &= \mathcal{L}^c_{X|Y}. \end{aligned} \tag{3.7}$$

Note that the degradedness assumption (3.5) implies the inclusion $\mathcal{L}_{X|Z} \subseteq \mathcal{L}_{X|Y}$. The coding scheme for the wiretap channel relies on the partition (3.7) and is summarized in Figure 3.1. The information is stored in the bits $u_i, i \in \mathcal{I}$. The bits in the coordinates in $\mathcal{R}$ are chosen randomly while the bits in $\mathcal{B}$ form a subset of the frozen bits.

Attainability of the rate (3.6) using this coding scheme is proved in the cited papers. An essential remark here is that the bits $u_i, i \in \mathcal{R}$ are randomly selected because fixing

their values contradicts even the weak security constraint, let alone the stronger one.

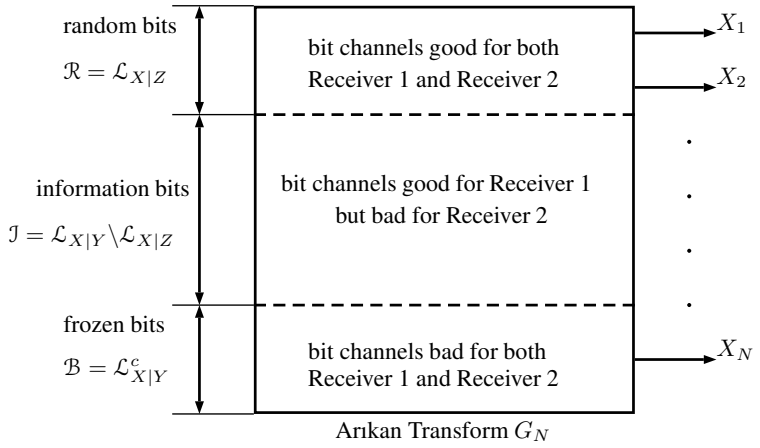


Figure 3.1: Block diagram of the coding scheme in [17]. Good bit channels and bad bit channels are as defined by (1.6).

We note that generally $\mathcal{H}^c_{X|Z} \not\subset \mathcal{L}_{X|Y}$, and even though the number of coordinates in $\mathcal{L}^c_{X|Y} \cap \mathcal{H}^c_{X|Z}$ behaves as $o(N)$, this constitutes an obstacle to achieving strong security. To bypass it, [46] uses a different partition of the coordinates, namely

$$\begin{aligned} \widetilde{\mathcal{I}} &= \mathcal{L}_{X|Y} \cap \mathcal{H}_{X|Z} \\ \widetilde{\mathcal{B}} &= \mathcal{L}^c_{X|Y} \cap \mathcal{H}_{X|Z} \\ \widetilde{\mathcal{R}}_1 &= \mathcal{L}_{X|Y} \cap \mathcal{H}^c_{X|Z} \\ \widetilde{\mathcal{R}}_2 &= \mathcal{L}^c_{X|Y} \cap \mathcal{H}^c_{X|Z}. \end{aligned} \tag{3.8}$$

Apart from transmitting the information, the coding scheme aims to convey the bits in $\widetilde{\mathcal{R}}_2$ to Receiver 1 using the good indices of Receiver 1, at the same time preserving the security requirement. This is accomplished using the "chaining" construction proposed in [46][1] and shown in Fig. 3.2. As the figure suggests, the bits in $\widetilde{\mathcal{R}}_2(j)$ contained in block j are transmitted over the channel as a part of the message of block $j-1$, for

[1]The term "chaining" was introduced later in [24].

all $j = 2, \ldots, m$. This enables Receiver 1 to recover these bits reliably as a part of the successive decoding procedure for block j, which is performed similarly to (1.17). At the same time, because of the inclusion $\widetilde{\mathcal{I}} \subset \mathcal{H}_{X|Z}$, Receiver 2 does not have the resources for their reliable decoding, which provides the desired security.

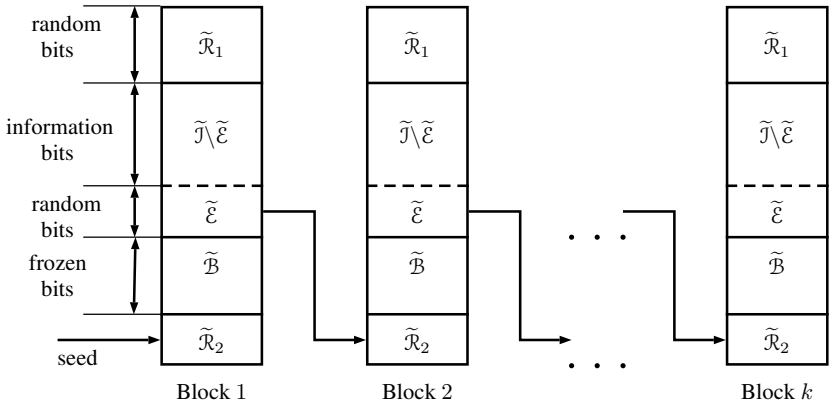


Figure 3.2: Block diagram of the coding scheme in [46].

The analysis of the transmission is performed based on m blocks of N bits as opposed to a single block. The seed for the transmission is provided by choosing $|\widetilde{\mathcal{R}}_2| = o(N)$ random bits which are shared with Receiver 1 (more on this below). In each of the blocks 1 to m, the bits indexed by the set $\widetilde{\mathcal{I}}\backslash\widetilde{\mathcal{E}}$ are used to send the message. Here $\widetilde{\mathcal{E}}$ is an arbitrary subset of the set $\widetilde{\mathcal{I}}$ of size $\widetilde{\mathcal{R}}_2$ whose role is explained below.

The bits in $\widetilde{\mathcal{R}}_1$ are selected randomly, and the bits $u_i, i \in \widetilde{\mathcal{B}}$ are frozen, i.e., assigned arbitrarily and shared in advance with Receiver 1 (they may be also known to Receiver 2 without compromising secrecy).

The assignment of bits in the set $\widetilde{\mathcal{R}}_2$ in block j depends on the block index. In block 1 these bits are set equal to the message bits of the seed block. In block $j = 2, \ldots, m$ the bits indexed by the set $\widetilde{\mathcal{R}}_2$ are set to be equal to the bits in the set $\widetilde{\mathcal{E}}$ in block $j - 1$, representing the chaining procedure.

Having formed the sequence $u^N(j)$ in block $j = 1, \ldots, m$, the encoder passes it through the polarizing transform and transmits the sequence $x^N = u^N G_N$ over the channel. The only remaining problem is to convey to Receiver 1 the bits of $\widetilde{\mathcal{R}}_2$ of the first block. This is done by performing the seed transmission of a block which encodes the $|\widetilde{\mathcal{R}}_2|$ bits using some error correcting code of length N. As claimed in [46], it is possible to choose such a code to fulfill the reliability and security requirements because its rate can be made arbitrarily close to zero. The fact that the seed code needs to encode only a small number $o(N)$ of message bits follows from the degradedness assumption, which is therefore essential in this construction.

As shown in [46], this scheme satisfies both constraints (3.1) and (3.2) under the assumption that the channel to the eavesdropper is degraded with respect to the channel W_1. The rate of communication between the transmitter and Receiver 1 can be made arbitrarily close to the value $I(W_1) - I(W_2)$ since the assumption that W_2 is degraded with respect to W_1 ensures that $|\widetilde{\mathcal{R}}_2| = o(N)$, i.e., there is no asymptotic loss in rate by removing the bits $\{u_i, i \in \widetilde{\mathcal{E}}\}$ from the message in order to support the strong security condition.

3.3 Polar Coding for the Wiretap Channel

In this section, we show that secrecy capacity for the wiretap channel given by Theorem 3.1 is achievable using polar codes. For this purpose, we consider the RVs V, X, Y, Z as described by Theorem 3.1, i.e., we assume some fixed distributions P_V, $P_{X|V}$ and the conditional distributions $P_{Y|X} = W_1$, $P_{Z|X} = W_2$ that satisfy the Markov condi-

tion $V \to X \to Y, Z$ and maximize the expression in (3.4). Define the RV $T^N = V^N G_N$, where V^N denotes N independent realizations of V. The transformation $V^N \to T^N$ induces conditional distributions $P_{T_i|T^{i-1}}$ derived from the corresponding distributions of the RVs V_i. Define the sets $\mathcal{H}_V$, $\mathcal{L}_V$, $\mathcal{H}_{V|Y}$, $\mathcal{L}_{V|Y}$ as follows:

$$\begin{aligned}
\mathcal{H}_V &= \{i \in [N] : Z(T_i|T^{i-1}) \geq 1 - \delta_N\} \\
\mathcal{L}_V &= \{i \in [N] : Z(T_i|T^{i-1}) \leq \delta_N\} \\
\mathcal{H}_{V|Y} &= \{i \in [N] : Z(T_i|T^{i-1}, Y^N) \geq 1 - \delta_N\} \\
\mathcal{L}_{V|Y} &= \{i \in [N] : Z(T_i|T^{i-1}, Y^N) \leq \delta_N\}
\end{aligned}$$

and define the sets $\mathcal{H}_{V|Z}$, $\mathcal{L}_{V|Z}$ analogously. The cardinalities of these sets satisfy [6, 21, 22] $\frac{1}{N}|\mathcal{H}_V| \to H(V)$, $\frac{1}{N}|\mathcal{L}_{V|Y}| \to 1 - H(V|Y)$, $\frac{1}{N}|\mathcal{H}_{V|Z}| \to H(V|Z)$ as $N \to \infty$.

Define a partition of $[N]$ into the following sets which will be used to describe the coding scheme[2]

$$\begin{aligned}
\mathcal{I} &= \mathcal{H}_V \cap \mathcal{L}_{V|Y} \cap \mathcal{H}_{V|Z} \\
\mathcal{B} &= \mathcal{H}_V \cap \mathcal{L}^c_{V|Y} \cap \mathcal{H}_{V|Z} \\
\mathcal{R}_1 &= \mathcal{H}_V \cap \mathcal{L}_{V|Y} \cap \mathcal{H}^c_{V|Z} \\
\mathcal{R}_2 &= \mathcal{H}_V \cap \mathcal{L}^c_{V|Y} \cap \mathcal{H}^c_{V|Z} \\
\mathcal{D} &= \mathcal{H}^c_V.
\end{aligned} \tag{3.9}$$

The partition of $[N]$ that thus arises is illustrated in Figure 3. It will be seen that the subsets $\mathcal{I}$, $\mathcal{R}_1$, $\mathcal{R}_2$, $\mathcal{B}$ in our coding scheme play the role similar to that of the analogously denoted subsets in (3.8). Importantly, the cardinality of $\mathcal{R}_2$ is not $o(N)$ any more, which requires

[2]We use the notation $\mathcal{I}, \mathcal{B}$ in this section in the sense different from Sect. 3.2. Since both uses are localized to their respective sections, this should not cause confusion.

adjustments in the transmission scheme. Moreover, there is an extra randomness needed to determine the sequence to be transmitted, as will be seen in the encoding algorithm below.

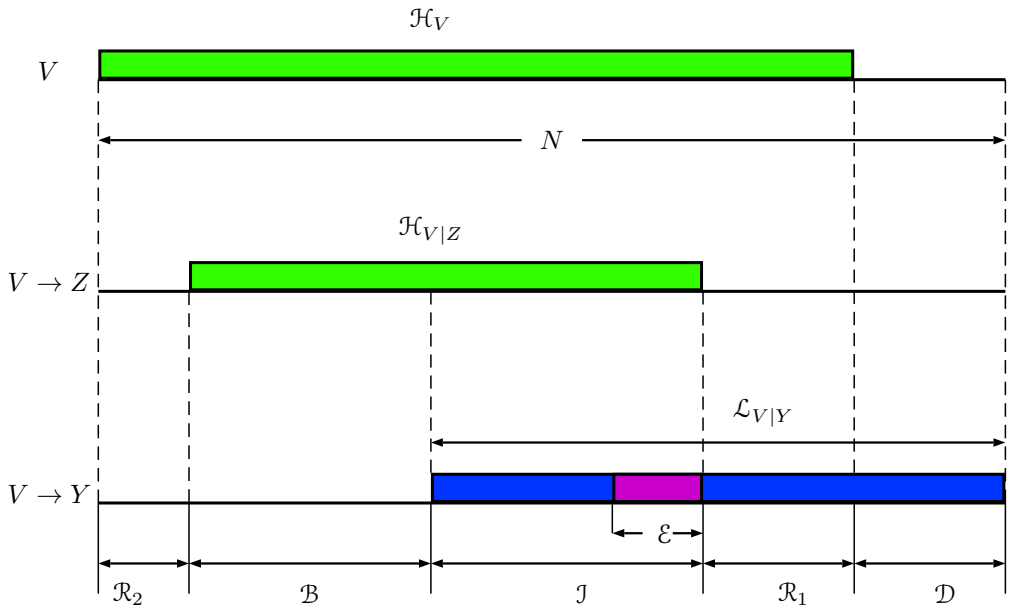


Figure 3.3: Partition of N coordinates of the block for transmission over the wiretap channel $\mathcal{W}$; see (3.9). The highlighted part of the top block represents high-entropy coordinates for the distribution P_V. Similarly, in the middle block we highlight the high-entropy coordinates of the distribution $P_{V|Z}$ and in the bottom block the low-entropy coordinates for the distribution $P_{V|Y}$.

Encoding: We build on the chaining idea of [46], connecting multiple blocks in a cluster whose performance in transmission will attain the desired goals. The cluster consists of a seed block and a number, m, of other blocks. The seed block consists of $|\mathcal{R}_2|$ random bits. Even though the cardinality of the set $\mathcal{R}_2$ constitutes a nonvanishing proportion of $[N]$, the rate of the seed $|\mathcal{R}_2|/mN$ can be made arbitrarily small by choosing m sufficiently large. (For example, one can set $m = N^\alpha$ for some $\alpha > 0$, and let $N \to \infty$.)

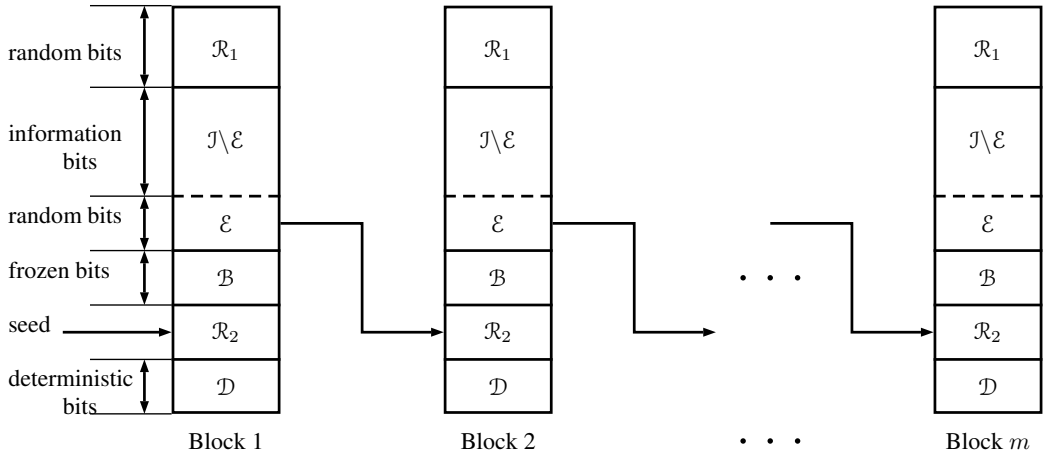


Figure 3.4: Block diagram of the wiretap coding scheme: Forming the blocks $t^N(j), j = 1, \ldots, m$.

Let us describe the encoding and decoding procedures. The transmission is accomplished using m blocks of length N each and the seed block. Every block $t^N = t^N(j), j = 1, \ldots, m$ contains a group of almost deterministic bits, denoted by $\mathcal{D}$ in Figure 3.4. The values of these bits are assigned according to a family of deterministic rules $\{\lambda_i, i \in \mathcal{D}\}$ described in (1.15). The bits $t_i, i \in \mathcal{B}$ in each of the m blocks are determined similarly, based on $\{\lambda_i, i \in \mathcal{B}\}$. These bits are assigned the same values for each block, and are shared with Receiver 1. Note that the rate $(|\mathcal{B}| + |\mathcal{D}|)/mN$ can be made arbitrarily small similarly to $|\mathcal{R}_2|/mN$.

The remaining subsets of coordinates are filled as follows. For block 1, the bits in the set $\mathcal{R}_2$ are assigned the value of the bits of the seed block, while for blocks $j = 2, \ldots, m$ these bits are set to be equal to the bits in $\mathcal{E}(j-1)$ of block $j-1$. Here, $\mathcal{E}$ is a subset of $\mathcal{I}$ having the same size as $\mathcal{R}_2$. The messages are stored in the bits indexed by $\mathcal{I}\backslash\mathcal{E}$. The randomly chosen bits in $\mathcal{E}$ are written in the coordinates that are good for Receiver 1 and contained in the bad (high-entropy) set of Receiver 2. These bits are transmitted to

Receiver 1 in block j and used for the decoding of the message contained in block $j+1$, for all $j = 1, 2, \ldots, m-1$. Finally, the bits in $\mathcal{R}_1$ are assigned randomly and uniformly for each of the m blocks. The diagram of the chaining construction for encoding is given in Figure 3.4.

Once the blocks $t^N(j), j = 1, 2, \ldots, m$ are formed, we find m sequences $v^N(j) = t^N(j)G_N$ by using the polarizing transform. Finally, given v^N, the codeword to be sent over the wiretap channel will be chosen as x^N with probability $P_{X^N|V^N}(x^N|v^N) = \prod_{i=1}^{N} P_{X|V}(x_i|v_i)$, where $P_{X|V}$ is the conditional distribution induced by the joint distribution of the RVs V and X. This logic is suggested by the proof of the capacity theorem, Theorem 3.1, which first considers "transmitting" the RV V^N to the receivers, and then choosing X^N so as to satisfy the Markov chain condition in the statement.

Decoding: Denote by $\mathcal{E}(0)$ the message sequence encoded in the seed block, and by $\mathcal{E}(j), j = 1, \ldots, m$ the corresponding sequences in the other blocks (see Fig. 3.4). Let $y^N(1), \ldots, y^N(m)$ be the sequences that Receiver 1 observes on the output of the channel W_1. The decoding rule is as follows:

$$\hat{t}_i = \begin{cases} \lambda_i(\hat{t}^{i-1}), & \text{if } i \in \mathcal{B} \cup \mathcal{D} \\ \text{argmax}_{t\in\{0,1\}} P_{T_i|T^{i-1}Y^N}(t|\hat{t}^{i-1}, y^N), & \text{if } i \in \mathcal{I} \cup \mathcal{R}_1 \\ \mathcal{E}_i(j-1), & \text{if } i \in \mathcal{R}_2 \end{cases} \tag{3.10}$$

where $P_{T_i|T^{i-1}}$ and $P_{T_i|T^{i-1},Y^N}$ are the conditional distributions induced by the joint distribution of the RVs V^N and Y^N (this rule is applied to each of the blocks $j = 1, \ldots, m$, and j is mostly omitted from the notation).

Let us show that the described scheme attains the secrecy capacity of $\mathcal{W}$. Namely,

the following is true.

Theorem 3.2. *For any $\gamma > 0$, $\epsilon > 0$ and $N \to \infty$ it is possible to choose m so that the transmission scheme described above attains the transmission rate R that is within γ of the secrecy capacity of $\mathcal{W}$* (3.4) *and the information leaked to Receiver 2 satisfies the strong secrecy condition* (3.2)*.*

Proof. Throughout the proof we assume that the RVs V, X, Y, Z are as given in Theorem 3.1 and denote by P_{VXYZ} their joint distribution. The distribution $P_{V^N X^N Y^N Z^N} = \prod_{i=1}^{N} P_{VXYZ}(v_i, x_i, y_i, z_i)$ refers to N independent repetitions of the RVs.

The rate of the proposed coding scheme is

$$\frac{m(|\mathcal{I}| - |\mathcal{E}|)}{mN} = \frac{(|\mathcal{H}_V \cap \mathcal{L}_{V|Y}| - |\mathcal{H}_V \cap \mathcal{H}^c_{V|Z}|)}{N},$$

which approaches $I(V;Y) - I(V;Z)$ as $N \to \infty$. According to Theorem 3.1, this is the target rate that we want to achieve for given V and X satisfying $V \to X \to Y, Z$ and $P_{Y|X} = W_1$, $P_{Z|X} = W_2$.

Now let us prove the reliability and security conditions. Let us introduce the following RVs: Let $M^m = (M_1, M_2, \ldots, M_m)$ correspond to the sequence of message bits $\{t_i, i \in \mathcal{I} \backslash \mathcal{E}\}$ transmitted in blocks $1, \ldots, m$, and let $Z^m = (Z^N(1), \ldots, Z^N(m))$ be a sequence of observations of Receiver 2 as a result of the transmission of the m blocks. Further, let E_j correspond to the bits contained in the subset $\mathcal{E}(j), j = 1, \ldots, m$.

Reliability: The claim of low error probability for Receiver 1 follows from the results of [3]. Since our communication scheme is more complicated compared to [3], we give some additional details.

Since we know the distribution P_{V^N}, we can compute the distributions $P_{T_i|T^{i-1}}, i = 1, \ldots, N$. Now assume that the assignments of the bits indexed by $\mathcal{B}$ and $\mathcal{D}$ are done randomly by sampling from the distribution $P_{T_i|T^{i-1}}$, for each of the blocks $1, \ldots, m$. Let $Q_{V^N X^N Y^N Z^N}$ be the joint distribution of the corresponding sequences arising from this assignment. Denote by $\|\cdot\|$ the l_1 distance between the distributions. From the proof of Lemma 1 in [3] it follows that

$$\|P_{V^N X^N Y^N Z^N} - Q_{V^N X^N Y^N Z^N}\| \leq N 2^{-N^\beta} \tag{3.11}$$

holds for all the m blocks of transmission. Moreover, since the message bits are entirely contained in the set of good bits for channel W_1, the probability of error is bounded by

$$\|P_{V^N X^N Y^N} - Q_{V^N X^N Y^N}\| + \sum_{i \in \mathcal{I}} Z(T_i|T^{i-1}, Y^N) \leq 2N 2^{-N^\beta}$$

for each individual block (see [3], Eqns (59)-60)). Therefore, there exists a family of deterministic rules $\{\lambda_i, i \in \mathcal{B} \cup \mathcal{D}\}$ such that the overall error probability for the successive decoding procedure (3.10) is at most $2mN2^{-N^\beta}, \beta \in (0, 1/2)$. We conclude that the probability that Receiver 1 decodes the information bits correctly approaches 1 as N tends to infinity.

Security: We will show that condition (3.2) is fulfilled for the sequence of m blocks of transmission. For that purpose, we will first prove the following lemma.

Lemma 3.3. *Let $\mathcal{A} \subset \mathcal{I}$ be a subset of coordinates, and let let $T[\mathcal{A}] = \{t_i, i \in \mathcal{A}\}$ and $T[\mathcal{I}\backslash\mathcal{A}] = \{t_i, i \in \mathcal{I}\backslash\mathcal{A}\}$. Then*

$$I(T[\mathcal{I}\backslash\mathcal{A}]; T[\mathcal{A}], Z^N) = O(N^3 2^{-N^\beta}). \tag{3.12}$$

Proof. By definition in (3.9) we have the inclusion $\mathcal{I} \subseteq \mathcal{H}_{V|Z}$. Let us label the indices in $\mathcal{I}$ as $a_1, a_2, \ldots, a_{|\mathcal{I}|}$, and assume that $a_1 < a_2 < \cdots < a_{|\mathcal{I}|}$. Using the inequality $Z(X|Y)^2 \leq H(X|Y)$ [6], we obtain the estimate

$$H_P(T_{a_i}|T^{a_i-1}, Z^N) \triangleq H_P(T_{a_i}|T_1, \ldots, T_{a_i-1}, Z^N) \geq 1 - 2\delta_N = 1 - 2^{-N^\beta+1} \quad (3.13)$$

for all $i = 1, 2, \ldots, |\mathcal{I}|$, where H_P refers to the entropy under the distribution $P_{V^N X^N Z^N}$. Our aim is to find an estimate on the mutual information in (3.12) under the distribution Q. To find an upper bound for the entropy $H(T_{a_i}|T^{a_i-1}\, Z^N)$ (computed under Q), we use a standard estimate (e.g., [62, Theorem 17.3.3]), and write

$$|H(T_{a_i}|T^{a_i-1}, Z^N) - H_P(T_{a_i}|T^{a_i-1}, Z^N)| \leq -\|P_{V^N X^N Z^N} - Q_{V^N X^N Z^N}\| \times \log \frac{\|P_{V^N X^N Z^N} - Q_{V^N X^N Z^N}\|}{|\mathcal{Z}|^N 2^N}$$

where $|\mathcal{Z}|$ refers to the alphabet size for a single observation of the eavesdropper. Then, we get from (3.11) that

$$H(T_{a_i}|T^{a_i-1}, Z^N) \geq 1 - O(N^2 2^{-N^\beta}) - O(N^{(\beta+1)} 2^{-N^\beta}) = 1 - O(N^2 2^{-N^\beta}). \quad (3.14)$$

Observe that (3.14) implies

$$H(T_{a_i}|T_{a_1}, T_{a_2}, \ldots, T_{a_{i-1}}, Z^N) \geq H(T_{a_i}|T^{a_i-1}, Z^N) \geq 1 - O(N^2 2^{-N^\beta}) \quad (3.15)$$

for all $i \in \mathcal{I}$.

Then we obtain

$$
\begin{aligned}
H(T[\mathcal{I}\backslash\mathcal{A}]\,|T[\mathcal{A}], Z^N) &= H(T[\mathcal{I}]\,|Z^N) - H(T[\mathcal{A}]\,|Z^N) \\
&\geq H(T[\mathcal{I}]|Z^N) - |\mathcal{A}| \\
&= \sum_{i=1}^{|\mathcal{I}|} H(T_{a_i}|T_{a_1}, T_{a_2}, \ldots, T_{a_{i-1}}, Z^N) - |\mathcal{A}| \\
&\geq |\mathcal{I}|(1 - O(N^2 2^{-N^\beta})) - |\mathcal{A}| \qquad (3.16) \\
&\geq |\mathcal{I}\backslash\mathcal{A}| - O(N^3 2^{-N^\beta})
\end{aligned}
$$

where (3.16) is due to (3.15). This completes the proof of (3.12). □

Lemma 3.4. *Let* $M^j \triangleq (M_1, M_2, \ldots, M_j)$ *and* $Z^j \triangleq (Z_1, Z_2, \ldots, Z_j)$. *For all* $j = 1, \ldots, m$, *we have*

$$I(E_j; M^j, Z^j) = O(jN^3 2^{-N^\beta}).$$

Proof. The proof is by induction on j. The base case $j = 1$ follows from Lemma 3.3. Now assume that the claim of the lemma is true for $j = k - 1$ and write

$$I(E_k; M^k, Z^k) = I(E_k; M_k, Z_k) + I(E_k; M^{k-1}, Z^{k-1}|M_k, Z_k).$$

Using the chaining structure shown in Figure 3.4 we argue that the only part of the transmission that connects block $k-1$ to block k is given by E_{k-1}. This implies that, conditional on (M_k, Z_k), we have a Markov chain $M^{k-1}Z^{k-1} \to E_{k-1} \to E_k$, so

$$I(E_k; M^{k-1}, Z^{k-1}|M_k, Z_k) \leq I(E_{k-1}; M^{k-1}, Z^{k-1}|M_k, Z_k) \leq I(E_{k-1}; M^{k-1}, Z^{k-1}),$$

Therefore,

$$\begin{aligned} I(E_k; M^k, Z^k) &\leq I(E_k; M_k, Z_k) + I(E_{k-1}; M^{k-1}, Z^{k-1}) \\ &= O(N^3 2^{-N^\beta}) + O((k-1)N^3 2^{-N^\beta}) \qquad (3.17) \\ &= O(kN^3 2^{-N^\beta}). \end{aligned}$$

Here (3.17) is due to Lemma 3.3 and the induction hypothesis. This completes the proof.

□

Now we are ready to complete the proof of the strong security condition. For this purpose, consider the following sequence of inequalities:

$$\begin{aligned} I(M^m; Z^m) &\leq I(M^m; Z^m, E_m) \\ &= I(M^{m-1}; Z^m, E_m) + I(M_m; Z^m, E_m | M^{m-1}) \\ &\leq I(M^{m-1}; Z^{m-1}, E_{m-1}) + I(M_m; Z^m, E_m | M^{m-1}) \qquad (3.18) \\ &\leq I(M^{m-1}; Z^{m-1}, E_{m-1}) + I(M_m; Z^m E_m, M^{m-1}) \\ &= I(M^{m-1}; Z^{m-1}, E_{m-1}) + I(M_m; E_m, Z_m) \\ &\quad + I(M_m; M^{m-1}, Z^{m-1} | E_m, Z_m) \end{aligned}$$

$$\begin{aligned} I(M^m; Z^m) &\leq I(M^{m-1}; Z^{m-1}, E_{m-1}) + I(M_m; E_m, Z_m) \\ &\quad + I(E_{m-1}; M^{m-1}, Z^{m-1}) \qquad (3.19) \\ &= I(M^{m-1}; Z^{m-1}, E_{m-1}) + O(N^3 2^{-N^\beta}) + O((m-1)N^3 2^{-N^\beta}) \qquad (3.20) \\ &= I(M^{m-1}; Z^{m-1} E_{m-1}) + O(mN^3 2^{-N^\beta}), \qquad (3.21) \end{aligned}$$

where (3.18) and (3.19) are implied by the chaining structure in Figure 3.4, and (3.20) is

due to Lemmas 3.3 and 3.4. From (3.21), we have

$$I(M^m; Z^m, E_m) \leq I(M^{m-1}; Z^{m-1}, E_{m-1}) + O(mN^3 2^{-N^\beta})$$

which implies

$$I(M^m; Z^m) \leq I(M^m; Z^m E_m) = O(m^2 N^3 2^{-N^\beta}).$$

Thus, we observe that $\lim_{N\to\infty} I(M^m;\ Z^m) = 0$ as required.

We conclude that a secrecy rate of $I(V;Y) - I(V;Z)$ is achievable for any V such that $V \to X \to Y, Z$ holds. Therefore, the secrecy capacity C_s given by (3.4) is also achievable. □

3.4 Polar Coding for Broadcast Channel with Confidential Messages

In this section we observe that ideas of the previous section together with some earlier works enable us to extend our code construction to a more general communication model introduced in [50].

3.4.1 The Model

Consider a pair of discrete memoryless channels with one transmitter X and two receivers Y, Z. As before, let $W_1 : X \to Y$ and $W_2 : X \to Z$ denote the channels and let $\mathcal{X}$ and $\mathcal{Y}, \mathcal{Z}$ denote the input alphabet and the output alphabets. We assume that the system transmits three types of messages:

(i), a message $s_1 \in \mathcal{S}_1$ from X to Y for which there are no secrecy requirements;

(ii), a message $s_2 \in \mathcal{S}_2$ from X to Y which is secret from Z;

(iii), a message $t \in \mathcal{T}$ from X to Y and Z, called the "common message".

Following [50], we call this communication scheme a *broadcast channel with confidential messages* (BCC).

As before, a block encoder for the BCC is a mapping $f : \mathcal{S}_1 \times \mathcal{S}_2 \times \mathcal{T} \to \mathcal{X}^N$. A stochastic version of the encoder is a probability matrix $f(x^N|s_1, s_2, t)$ with columns indexed by $x^N \in \mathcal{X}^N$ and rows indexed by the triples (s_1, s_2, t). Given such a triple, the stochastic encoder samples from the conditional probability distribution on $\mathcal{X}^N$. In accordance with the problem statement, there are two decoders: The decoder of Receiver 1 is defined by a mapping $\phi : \mathcal{Y}^N \to \mathcal{S}_1 \times \mathcal{S}_2 \times \mathcal{T}$ and the decoder of Receiver 2 is a mapping $\psi : \mathcal{Z}^N \to \mathcal{T}$.

Denote the rate of the common message t by R_0, and denote the rates of the secret and non-secret messages to Y by R_s and R_1, respectively. The analogs of Definitions 3.1.1, 3.1.2 in this case look as follows.

Definition 3.4.1. *The encoder-decoder mappings (f, ϕ, ψ) give rise to* (N, ϵ)- transmission *over the BCC if for every $s_1 \in \mathcal{S}_1$, $s_2 \in \mathcal{S}_2$, $t \in \mathcal{T}$, decoder ϕ outputs the transmitted triple (s_1, s_2, t) and decoder ψ outputs the message t with probability greater than $1 - \epsilon$, i.e.,*

$$\sum_{x^N \in \mathcal{X}^N} f(x^N|s_1, s_2, t) P_{Y^N|X^N}(\phi(y^N) = (s_1, s_2, t)|x^N) \geq 1 - \epsilon$$

$$\sum_{x^N \in \mathcal{X}^N} f(x^N|s_1, s_2, t) P_{Z^N|X^N}(\psi(z^N) = t|x^N) \geq 1 - \epsilon.$$

Definition 3.4.2. *(R_1, R_s, R_0) is an achievable rate triple for the BCC if there exists a sequence of message sets $\mathcal{S}_{1,N}$, $\mathcal{S}_{2,N}$, $\mathcal{T}_N$ and encoder-decoder triples (f_N, ϕ_N, ψ_N) giving*

rise to (N, ϵ_N) *transmission with* $\epsilon_N \to 0$*, such that*

$$\begin{aligned} \lim_{N\to\infty} \frac{1}{N} \log |\mathcal{S}_{1,N}| &= R_1 \\ \lim_{N\to\infty} \frac{1}{N} \log |\mathcal{S}_{2,N}| &= R_s \\ \lim_{N\to\infty} \frac{1}{N} \log |\mathcal{T}_N| &= R_0 \\ \lim_{N\to\infty} I(S_{2,N}; Z^N) &= 0. \end{aligned} \tag{3.22}$$

where $S_{2,N}$ *is the random variable that corresponds to the secret message.*

Note that our definition takes into account the formulation in [23] and is slightly different from the one in [50] (where we write (R_1, R_s, R_0), [50] has $(R_1 + R_s, R_s, R_0)$).

The following theorem gives the achievable rate region for the triple (R_1, R_s, R_0).

Theorem 3.5. *[50], [23, p. 414] The capacity region of the BCC consists of those triples of nonnegative numbers* (R_1, R_s, R_0) *that satisfy, for some RVs* $U \to V \to X \to Y, Z$ *with* $P_{Y|X} = W_1$ *and* $P_{Z|X} = W_2$*, the inequalities*

$$R_0 \leq \min[I(U;Y), I(U;Z)] \tag{3.23}$$

$$R_s \leq I(V;Y|U) - I(V;Z|U) \tag{3.24}$$

$$R_0 + R_1 + R_s \leq I(V;Y|U) + \min[I(U;Y), I(U;Z)]. \tag{3.25}$$

Moreover, it may be assumed that $V = (U, V')$ *and the range sizes of* U *and* V' *are at most* $|X| + 3$ *and* $|X| + 1$.

One can define the secrecy capacity C_s in terms of the capacity region of the BCC, and then recover Theorem 3.1 as a particular case of Theorem 3.5.

3.4.2 Polar Coding for the Csiszár-Körner Region

In this section, we aim to show that the capacity region of the BCC can be achieved using polar codes. In the first two steps we design a scheme that achieves the rate pairs (R_0, R_s) in (3.23)-(3.24), and in the last step we show that for any such pair (R_0, R_s) any rate value

$$R_1 \leq I(V;Y|U) + \min[I(U;Y), I(U;Z)] - R_0 - R_s \tag{3.26}$$

is also achievable. Finally, the security condition in (3.22) will be shown in Proposition 3.6 below.

The overall encoding scheme is stochastic and assumes some fixed joint distribution of the RVs U, V, X, Y, Z such that the constraints of Theorem 3.5 are satisfied. Since the results below are valid for any such distribution, this will enable us to claim achievability of the rate region in this theorem. The encoder is formed of two stages performed in succession. At the outcome of the first stage, which deals with the common message s_2, the encoder computes a sequence of m blocks of N bits denoted below by $q^N(j), j = 1, \ldots, m$. These blocks are used in the second stage to construct the data encoding that is going to be sent to both receivers. Namely, it will be seen that the transformed blocks $u^N = q^N G_N$ can at the same time encode the common message to both receivers and also encode side information for Receiver 1 to ensure reliable transmission of the confidential message. The actual sequences to be transmitted are computed in the second stage based on the sequences $u^N(j)$. This is done by first constructing sequences $t^N(j)$ using the ideas developed in Sect. 3.3 and by using a stochastic mapping of these sequences on the codewords $x^N(j)$. Upon transmitting, these codewords are received by Receiver 1 as

$y^N(j)$ and by Receiver 2 as $z^N(j)$. We will argue that the receivers can independently perform decoding procedures that recover the three desired types of messages reliably (and when appropriate, also securely).

3.4.2.1 The common-message encoding

The proof of the fact that any R_0 satisfying (3.23) is achievable follows from the polar coding scheme for the superposition region given in [24]. Given the RVs $U \to V \to X \to Y, Z$ with $P_{Y|X} = W_1$ and $P_{Z|X} = W_2$, let U^N, V^N, X^N, Y^N, Z^N be N independent repetitions of the RVs U, V, X, Y, Z. Set

$$Q^N = U^N G_N, \tag{3.27}$$

where G_N is Arıkan's transform. As before, lowercase letters denote realizations of these RVs.

Define the sets $\mathcal{H}_U$, $\mathcal{L}_{U|Y}$, $\mathcal{L}_{U|Z}$ as follows:

$$\mathcal{H}_U = \{i \in [N] : Z(Q_i|Q^{i-1}) \geq 1 - \delta_N\}$$

$$\mathcal{L}_{U|Y} = \{i \in [N] : Z(Q_i|Q^{i-1}, Y^N) \leq \delta_N\}$$

$$\mathcal{L}_{U|Z} = \{i \in [N] : Z(Q_i|Q^{i-1}, Z^N) \leq \delta_N\}.$$

The cardinalities of these sets, normalized by N, approach respectively $H(U)$, $1 - H(U|Y), 1 - H(U|Z)$ as $N \to \infty$.

Now observe that for Receiver 1 to recover q^N correctly, the indices of the information bits should be a subset of $\mathcal{I}_u^{(1)} = \mathcal{H}_U \cap \mathcal{L}_{U|Y}$. Similarly, for Receiver 2 to recover the sequence q^N correctly, the information bits should be placed only in those positions

of q^N that are indexed by the set $\mathcal{I}_u^{(2)} = \mathcal{H}_U \cap \mathcal{L}_{U|Z}$. Therefore, choosing the indices of information bits as $\mathcal{I}_u = \mathcal{I}_u^{(1)} \cap \mathcal{I}_u^{(2)}$ ensures that the message embedded into q^N will be decoded correctly by both receivers. In this case, the rate of the common message is $R_0 = |\mathcal{I}_u^{(1)} \cap \mathcal{I}_u^{(2)}|/N$. Given that

$$\lim_{N\to\infty} \frac{1}{N}|\mathcal{I}_u^{(1)}| = I(U;Y)$$
$$\lim_{N\to\infty} \frac{1}{N}|\mathcal{I}_u^{(2)}| = I(U;Z)$$

we conclude the common message rate R_0 attains the value $\min[I(U;Y); I(U;Z)]$ only if either $\mathcal{I}_u^{(2)} \subseteq \mathcal{I}_u^{(1)}$ or $\mathcal{I}_u^{(1)} \subseteq \mathcal{I}_u^{(2)}$ holds starting from some N. However, generally this does not have to be the case. To overcome this problem, [24] proposed the following coding scheme. Define the sets

$$\mathcal{D}^{(1)} = \mathcal{I}_u^{(1)} \backslash \mathcal{I}_u^{(2)}$$
$$\mathcal{D}^{(2)} = \mathcal{I}_u^{(2)} \backslash \mathcal{I}_u^{(1)}.$$

Without loss of generality, assume that $I(U;Y) \leq I(U;Z)$, which implies that $|\mathcal{D}^{(2)}| \geq |\mathcal{D}^{(1)}|$ starting with some N. To describe the encoding procedure, consider m blocks of N coordinates each. In block 1, we use the positions indexed by $\mathcal{D}^{(1)}$ to store message bits and assign the bits indexed by $\mathcal{D}^{(2)}$ to some fixed values that are available to Receiver 1. In Block $j, j = 2, \ldots, m-1$, we again use the positions indexed by $\mathcal{D}^{(1)}$ to store message bits and copy the part of Block $j-1$ indexed by the coordinates in $\mathcal{D}^{(1)}$ into the positions indexed by a subset of coordinates $\mathcal{E}^{(2)} \subset \mathcal{D}^{(2)}$ in block j (thus $|\mathcal{E}^{(2)}| = |\mathcal{D}^{(1)}|$). Fill the remaining $|\mathcal{D}^{(2)} \backslash \mathcal{E}^{(2)}|$ bits in each block $j \in \{2, \ldots, m-1\}$ with random and independent bits and communicate them to Receiver 1. These bits can be the

same for each block as long as they are independent and uniform within the same block, so this part of the scheme has negligible impact on the overall rate. In the final block m, we assign the bits indexed by $\mathcal{D}^{(1)}$ to some fixed values that are available to Receiver 2 and copy the bits in $\mathcal{D}^{(1)}(m-1)$ to the positions in $\mathcal{E}^{(2)}(m)$. The remaining $|\mathcal{D}^{(2)} \backslash \mathcal{E}^{(2)}|$ coordinates in block m are filled with random bit values. The bits in $\mathcal{H}_U \cap (\mathcal{I}_u^{(1)} \cup \mathcal{I}_u^{(2)})^c$ and $\mathcal{H}_U^c$ are chosen based on deterministic rules λ_i similarly to Sect. 3.3. These bits are the same for each block and are shared with both receivers. The block diagram of the described coding scheme is shown by Figure 3.5.

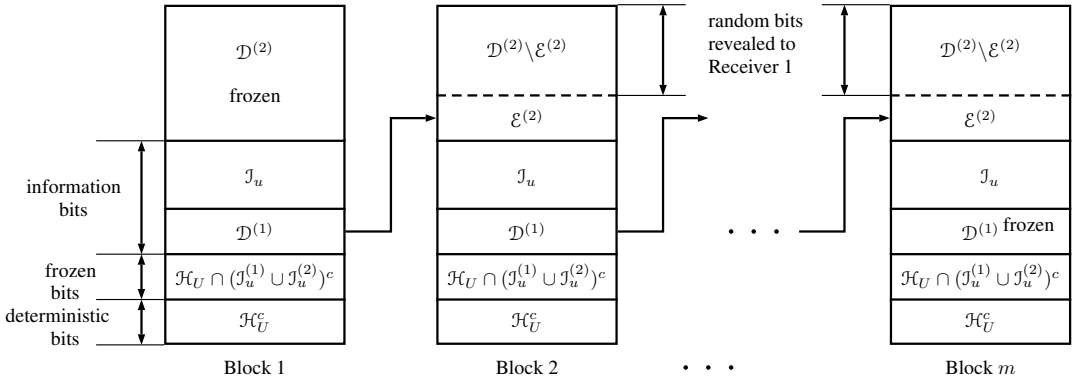


Figure 3.5: Encoding for the common-message case: The structure of the blocks $q^N(j), j = 1, \ldots, m$

The encoding stage described passes the sequences $u^N(j), j = 1, \ldots, m$ to the second stage which is responsible for actual communication. Upon observing the channel outputs, both receivers perform decoding, which will be described below in Sect. 3.4.2.3.

3.4.2.2 The secret-message encoding

In this section we describe the construction of sequences x^N that are sent by transmitter X. The construction relies on the sequences $u^N(j)$ constructed by X in the first

stage. These sequences can be thought of as side information that enables Receiver 1 to reconstruct the secret message.

The transmission scheme we propose to achieve the rate R_s that satisfies (3.24), is very similar to the scheme described for the wiretap channel problem in Section 3.3. Our solution consists of choosing the indices of information bits and random bits appropriately and using a chaining scheme quite similar to the one shown in Figure 3.4.

Let U^N, V^N, X^N, Y^N, Z^N be as defined in Section 3.4.2.1, and let $T^N = V^N G_N$. Viewing U as side information about V, we define the sets

$$\mathcal{H}_{V|U} = \{i \in [N] : Z(T_i|T^{i-1}, U^N) \geq 1 - \delta_N\}$$

$$\mathcal{L}_{V|U,Y} = \{i \in [N] : Z(T_i|T^{i-1}, U^N, Y^N) \leq \delta_N\}$$

$$\mathcal{H}_{V|U,Z} = \{i \in [N] : Z(T_i|T^{i-1}, U^N, Z^N) \geq 1 - \delta_N\}$$

whose cardinalities, normalized by N, approach respectively the values $H(V|U), 1 - H(V|U,Y), H(V|U,Z)$ as $N \to \infty$.

The intuition behind the construction presented below can be described as follows. First, note that the coordinates of T^N indexed by

$$\mathcal{J}^{(1)} = \mathcal{H}_{V|U} \cap \mathcal{L}_{V|U,Y} \tag{3.28}$$

can be decoded by Receiver 1, and so they can be used to send more data in addition to the common message. Of these bits, the part indexed by $(\mathcal{H}_{V|U} \cap \mathcal{L}_{V|U,Y}) \backslash (\mathcal{H}_{V|U} \cap \mathcal{H}^c_{V|U,Z})$ can be used to transmit the confidential message. Then, given that $\frac{1}{N}|\mathcal{H}_{V|U} \cap \mathcal{L}_{V|U,Y}| \to I(V;Y|U)$ and $\frac{1}{N}|\mathcal{H}_{V|U} \cap \mathcal{H}^c_{V|U,Z}| \to I(V;Z|U)$, we obtain

$$\lim_{N\to\infty} \frac{1}{N}|(\mathcal{H}_{V|U} \cap \mathcal{L}_{V|U,Y}) \backslash (\mathcal{H}_{V|U} \cap \mathcal{H}^c_{V|U,Z})| \geq I(V;Y|U) - I(V;Z|U).$$

This implies that the proposed scheme transmits the secret message at rates arbitrarily close to the rate given by (3.24) (provided that it also satisfies the strong security condition).

Building on this observation, we proceed to describe the coding scheme, adding some details that make the secrecy part work. Define the sets[3]

$$\begin{aligned}
\mathcal{I} &= \mathcal{H}_{V|U} \cap \mathcal{L}_{V|U,Y} \cap \mathcal{H}_{V|U,Z} \\
\mathcal{B} &= \mathcal{H}_{V|U} \cap \mathcal{L}^c_{V|U,Y} \cap \mathcal{H}_{V|U,Z} \\
\mathcal{R}_1 &= \mathcal{H}_{V|U} \cap \mathcal{L}_{V|U,Y} \cap \mathcal{H}^c_{V|U,Z} \\
\mathcal{R}_2 &= \mathcal{H}_{V|U} \cap \mathcal{L}^c_{V|U,Y} \cap \mathcal{H}^c_{V|U,Z} \\
\mathcal{D} &= \mathcal{H}^c_{V|U}.
\end{aligned} \tag{3.29}$$

Note that the sets $\mathcal{I}, \mathcal{R}_1, \mathcal{R}_2, \mathcal{B}, \mathcal{D}$ partition $[N]$. This partition is basically the same as in (3.9) (see also Figures 3 and 3.3) except for the fact that the high- and low-entropy subsets rely on entropy quantities that are additionally conditioned on U.

The transmission scheme that we propose is formed of multiple blocks joined in clusters of m blocks. Similarly to the wiretap coding scheme, there is a seed block shared between the transmitter and Receiver 1. The seed block consists of $|\mathcal{R}_2|$ random bits. Even if the set $\mathcal{R}_2$ constitutes a nonvanishing proportion of $[N]$, the rate of the seed $|\mathcal{R}_2|/mN$ can be made arbitrarily small by choosing m sufficiently large. (For example, one can set

[3]We again use the same notation as in (3.9); since the earlier notation is used only in Section 3.3, this should not cause confusion.

$m = N^{\alpha}$ for some $\alpha > 0$, and let N tend to infinity.)

The encoding procedure is as follows. Our aim is to construct m blocks $t^N(j)$ which will be used to form the transmitted sequences $x^N(j), j = 1, \ldots, m$. Apart from the seed block, all the other blocks t^N contain a group of almost deterministic bits, denoted by $\mathcal{D}$ in (3.29). For block $j, j = 1, \ldots, m$, the values of these bits are assigned according to a deterministic rule λ_i (similarly to the earlier appearance of this mapping, see, e.g., Sect. 3.3), namely

$$t_i = \lambda_i(t^{i-1}, u^N(j))$$

for all $i \in \mathcal{D}$. The set of frozen bits $\mathcal{B}$ in each of the m blocks is chosen similarly based on a family of deterministic rules $\{\lambda_i, i \in \mathcal{B}\}$. These bits are going to be the same for the each block and shared with Receiver 1. Note that the rate $(|\mathcal{B}| + |\mathcal{D}|)/mN$ can be made arbitrarily small similarly to $|\mathcal{R}_2|/mN$.

The remaining subsets of coordinates in are filled as follows. For block 1, the bits in the set $\mathcal{R}_2$ are assigned the values of the bits of the seed block, while for block j, $j = 2, \ldots, m$ these bits are set to be equal to the bits in $\mathcal{E}$ of block $j - 1$. Here, $\mathcal{E}$ is a subset of $\mathcal{I}$ having the same size as $\mathcal{R}_2$. The messages are stored in the bits indexed by $\mathcal{I} \backslash \mathcal{E}$ which are good for Receiver 1 and contained in the bad (high-entropy) set of Receiver 2. The indices in the subset $\mathcal{E}$ are still good for Receiver 1 but bad for Receiver 2. Nevertheless, they are filled with random bits that are used for decoding by Receiver 1 in the same way as was done in Sect. 3.3. Finally, the bits in $\mathcal{R}_1$ are assigned randomly and uniformly for each of the m blocks. We once again refer to Fig. 3.3 which illustrates the described processing. Once the blocks $t^N(j), j = 1, \ldots, m$ are formed, we compute

m sequences $v^N(j) = t^N(j)G_N$ by using the polarizing transform.

Finally, the codewords to be sent by the transmitter are computed as follows. The codeword $x^N(j), j = 1, \ldots, m$ is sampled from $\mathcal{X}^N$ according to the distribution $P_{X^N|V^N}(x^N|v^N) = \prod_{i=1}^N P_{X|V}(x_i|v_i)$, where $P_{X|V}$ is the conditional distribution induced by the joint distribution of the RVs V and X.

3.4.2.3 Decoding of the common message and the secret message

Assume that the transmitted sequence x^N is received as y^N by Receiver 1 and as z^N by Receiver 2. Importantly, by our construction these sequences follow the conditional distributions $P_{Y|X}$ and $P_{Z|X}$ given by the channels W_1 and W_2. We describe the decoding procedures by Receivers 1 and 2. Initially they perform similar operations aimed at recovering the common message. Once this is accomplished, Receiver 1 performs additional decoding to recover the secret message.

We begin with the common-message part. In accordance with (3.27), Receivers 1 and 2 decode the blocks $q^N(j), j = 1, \ldots, m$ relying on a iterative procedure. As the construction suggests, Receiver 1 decodes in the forward direction, starting with block 1 and ending with block m, and Receiver 2 decodes backwards, starting with block m and ending with block 1. Let

$$D(j) = \{q_i, i \in \mathcal{D}^{(1)}(j)\}, j = 1, \ldots, m-1$$

$$C(j) = \{q_i, i \in \mathcal{E}^{(2)}(j)\}, j = 2, \ldots, m$$

denote the subblocks $\mathcal{D}, \mathcal{E}$ of the corresponding blocks (see Fig. 3.5).

The processing by Receiver 1 is as follows. For block 1, it computes

$$\hat{q}_i = \begin{cases} q_i, & \text{if } i \in \mathcal{D}^{(2)} \\ \text{argmax}_{q\in\{0,1\}} P_{Q_i|Q^{i-1}Y^N}(q|\hat{q}^{i-1}, y^N), & \text{if } i \in \mathcal{I}_u \cup \mathcal{D}^{(1)} \\ \lambda_i(\hat{q}^{i-1}), & \text{otherwise.} \end{cases} \tag{3.30}$$

For the remaining blocks $j = 2, \ldots, m$ Receiver 1 computes the vector $(\hat{q}_i(j), i = 1, \ldots, N)$ as follows:

$$\hat{q}_i(j) = \begin{cases} D_i(j-1), & \text{if } i \in \mathcal{E}^{(2)} \\ q_i(j), & \text{if } i \in \mathcal{D}^{(2)} \backslash \mathcal{E}^{(2)} \\ \text{argmax}_{q\in\{0,1\}} P_{Q_i|Q^{i-1}Y^N}(q|\hat{q}^{i-1}(j), y^N(j)), & \text{if } i \in \mathcal{I}_u \cup \mathcal{D}^{(1)} \\ \lambda_i(\hat{q}^{i-1}(j)), & \text{otherwise.} \end{cases} \tag{3.31}$$

The processing by Receiver 2 is quite similar except that it starts with block m and advances "backwards" for $j = m-1, m-2, \ldots, 1$. For block m the rule is as follows:

$$\hat{q}_i = \begin{cases} q_i, & \text{if } i \in \mathcal{D}^{(1)} \\ \text{argmax}_{q\in\{0,1\}} P_{Q_i|Q^{i-1}Z^N}(q|\hat{q}^{i-1}, z^N), & \text{if } i \in \mathcal{I}_u \cup \mathcal{D}^{(2)} \\ \lambda_i(\hat{q}^{i-1}), & \text{otherwise.} \end{cases} \tag{3.32}$$

For blocks $j = m-1, m-2, \ldots, 1$, Receiver 2 computes its estimates of the vector $q^N(j)$ as follows:

$$\hat{q}_i(j) = \begin{cases} C_i(j+1), & \text{if } i \in \mathcal{D}^{(1)} \\ \text{argmax}_{q\in\{0,1\}} P_{Q_i|Q^{i-1}Z^N}(q|\hat{q}^{i-1}(j), z^N(j)), & \text{if } i \in \mathcal{I}_u \cup \mathcal{D}^{(2)} \\ \lambda_i(\hat{q}^{i-1}(j)), & \text{otherwise.} \end{cases} \tag{3.33}$$

(in (3.30)-(3.33) the notation is somewhat abbreviated to keep the formulas compact, e.g., no reference is made to the index of the receiver, and the block index j is sometimes omitted).

The processing described above in (3.30)-(3.31) yields the sequences $\hat{u}^N(j) = q^N(j)G_N, j = 1, \ldots, m$ which are used by Receiver 1 to recover the secret messages. Denote by $\mathcal{E}(0)$ the message sequence encoded in the seed block, and let $\mathcal{E}(j), j = 1, \ldots, m$ be the subblock of block j indexed by the set $\mathcal{E}$. For $j = 1, \ldots, m$, the decoding rule is as follows:

$$\hat{t}_i(j) = \begin{cases} \lambda_i(\hat{t}^{i-1}(j), \hat{u}^N(j)), & \text{if } i \in \mathcal{D} \cup \mathcal{B} \\ \text{argmax}_{t\in\{0,1\}} P_{T_i|T^{i-1}U^N Y^N}(t|\hat{t}^{i-1}(j), \hat{u}^N(j), y^N(j)), & \text{if } i \in \mathcal{I} \cup \mathcal{R}_1 \\ \mathcal{E}_i(j-1), & \text{if } i \in \mathcal{R}_2, \end{cases} \tag{3.34}$$

where $P_{T_i|T^{i-1}U^N Y^N}$ is the conditional distribution induced by the joint distribution of the RVs U^N, V^N and Y^N (the notation is again abbreviated similarly to (3.10)).

3.4.2.4 Achievability of the rate region (3.23)-(3.25)

The rate of the common message achieved by the construction in Sect. 3.4.2.1 is equal to

$$R_0 = \frac{1}{mN}\left[m|\mathcal{I}_u| + (m-1)|\mathcal{D}^{(1)}|\right].$$

As N increases, we obtain

$$\frac{m-1}{m} I(U;Y) \leq R_0 \leq I(U;Y).$$

For sufficiently large m this quantity is arbitrarily close to the common-message rate value given in (3.23). Note that we have assumed that $I(U;Z) \geq I(U;Y)$; to handle the opposite case is suffices to interchange the roles of the pieces $\mathcal{D}^{(1)}$ and $\mathcal{D}^{(2)}$ in the common-message encoding and decoding procedures.

As shown in [24], both receivers can decode the common message correctly with probability of error at most $mN2^{-N^{\beta}}, \beta \in (0, 1/2)$. This follows because in this stage, Receivers 1 and 2 aim only at decoding the bits corresponding to the index sets $\mathcal{D}^{(1)} \cup \mathcal{I}_u = \mathcal{H}_U \cap \mathcal{L}_{U|Y}$ and $\mathcal{D}^{(2)} \cup \mathcal{I}_u = \mathcal{H}_U \cap \mathcal{L}_{U|Z}$, respectively. That these bits can be recovered in a sucessive decoding procedure follows from the basic results on polar codes [2, 21] and [3].

For the secret-message part of the communication the properties of the scheme are characterized by the following proposition.

Proposition 3.6. *For any $\gamma > 0$, $\epsilon > 0$ and $N \to \infty$ it is possible to choose m so that the transmission scheme described above attains a secrecy rate R_s such that $R_s \geq I(V;Y|U) - I(V;Z|U) - \gamma$ and the information leaked to Receiver 2 satisfies the strong secrecy condition in Definition 3.4.2.*

Proof. Assume that X, V, Y, Z are as given by Theorem 3.5. The rate of proposed coding scheme is

$$\frac{m(|\mathcal{I}| - |\mathcal{E}|)}{mN} = \frac{(|\mathcal{H}_{V|U} \cap \mathcal{L}_{V|U,Y}| - |\mathcal{H}_{V|U} \cap \mathcal{H}^{c}_{V|U,Z}|)}{N}$$

which converges to $I(V;Y|U) - I(V;Z|U)$ as N goes to infinity. Recalling Theorem 3.5, we note that this is the target value of the rate R_s for given U, V and X satisfying $U \to V \to X \to Y, Z$ and $P_{Y|X} = W_1$, $P_{Z|X} = W_2$.

Introduce the following RVs: Let $M^m = (M_1, M_2, \ldots, M_m)$ be a sequence of message bits $\{t_i, i \in \mathcal{I}\backslash\mathcal{E}\}$ sent in blocks $1, \ldots, m$, and let $Z^m = (Z^N(1), \ldots, Z^N(m))$ be the RVs that represent the random observations of Receiver 2 upon transmitting m blocks $X^N(j)$. Further, let E_j correspond to the bits contained in the subset $\mathcal{E}(j)$ for all $j = 1, \ldots, m$.

Reliability: The proof of reliable decoding by Receiver 1 follows from the results of [3] and is very similar to Section 3.3. Let $P_{U^N V^N X^N Y^N Z^N}(u^N, v^N, x^N, y^N, z^N) \triangleq \prod_{i=1}^N P_{U,V,X,Y,Z}(u_i, v_i, x_i, y_i, z_i)$, where P_{UVXYZ} is the joint distribution of the RVs U, V, X, Y, Z appearing in Theorem 3.5. Let $\tilde{P}_{U^N,V^N,X^N,Y^N,Z^N}$ be the empirical distribution induced by the transmission scheme if the deterministic rules λ_i in both stages of the encoding are replaced by random assignments such that, for $a = 0, 1$,

$$\Pr(q_i = a) = P_{Q_i|Q^{i-1}}(a|q^{i-1})$$

$$\Pr(t_i = a) = P_{T_i|T^{i-1}}(a|t^{i-1})$$

holds for the first and second stages, respectively. Here Q^N is the RV defined in (3.27). Then, from the proof of Lemma 1 in [3], it follows that

$$\|P_{U^N} - \tilde{P}_{U^N}\| \leq N2^{-N^\beta}$$

$$\|P_{V^N|U^N}(.|u^N) - \tilde{P}_{V^N|U^N}(.|u^N)\| \leq N2^{-N^\beta},$$

the second estimate for every u^N. Hence, we conclude that

$$\|P_{U^N V^N} - \tilde{P}_{U^N V^N}\| \leq 2N2^{-N^\beta}$$

$$\|P_{U^N V^N X^N Y^N Z^N} - \tilde{P}_{U^N V^N X^N Y^N Z^N}\| \leq 2N2^{-N^\beta}$$

holds for all the m blocks of transmission. Moreover, since the message bits are entirely contained in the set of $\mathcal{L}_{V|U,Y}$, the successive decoding procedure (3.34) has the probability of error bounded by

$$|P_{U^N V^N X^N Y^N} - \tilde{P}_{U^N V^N X^N Y^N}\| + \sum_{i \in \mathcal{I}} Z(T_i | T^{i-1}, U^N, Y^N) \leq 3N2^{-N^\beta}$$

for each individual block. Thus, we observe that there exists a family of deterministic rules λ_i for each stage such that the overall error probability is at most $3mN2^{-N^\beta}, \beta \in (0, 1/2)$. We conclude that the probability that Receiver 1 decodes the information bits correctly approaches 1 as N goes to infinity.

Security: We will show that condition (3.2) is fulfilled for the sequence of m blocks of transmission. Note that Receiver 2 observes not only a realization of Z^m, but also estimates the RVs $U^m = (U^N(1), \ldots, U^N(m))$ through procedure (3.32)-(3.33). For this reason the strong security condition to be proved takes the form

$$\lim_{N \to \infty} I(M^m; U^m, Z^m) = 0. \tag{3.35}$$

The proof of (3.35) is very similar to the proof of strong secrecy in Section 3.3. The counterparts of Lemmas 3.3 and 3.4 for the BCC are provided below. The proofs are the same as the ones in Section 3.3 and will be omitted.

Lemma 3.7. *Let* $T[\mathcal{A}] = \{t_i, i \in \mathcal{A}\}$ *and* $T[\mathcal{I} \backslash \mathcal{A}] = \{t_i, i \in \mathcal{I} \backslash \mathcal{A}\}$, *where* $\mathcal{A}$ *is any subset of* $\mathcal{I}$. *Then*

$$I(T[\mathcal{I} \backslash \mathcal{A}]; T[\mathcal{A}], U^N, Z^N) = O(N^3 2^{-N^\beta}) \tag{3.36}$$

Lemma 3.8. *Let* $M^j \triangleq (M_1, M_2, \ldots, M_j)$, $Z^j \triangleq (Z_1, Z_2, \ldots, Z_j)$, *and* $U^j \triangleq (U_1, U_2, \ldots, U_j)$. *Then, for all* $j = 1, \ldots, m$, *we have*

$$I(E_j; M^j, U^j, Z^j) = O(jN^3 2^{-N^\beta}) \tag{3.37}$$

The rest of the proof also follows similarly to the proof in Section 3.3. Repeating the inequalities which led to (3.21), we get

$$\begin{aligned} I(M^m;\, U^m, Z^m) &\leq I(M^m;\, U^m, Z^m, E_m) \\ &\leq I(M^{m-1}; U^{m-1}, Z^{m-1}, E_{m-1}) + O(mN^3 2^{-N^\beta}) \end{aligned}$$

which implies

$$I(M^m;\, U^m, Z^m) \leq I(M^m;\, U^m, Z^m, E_m) = O(m^2 N^3 2^{-N^\beta}).$$

This completes the proof of (3.35). □

Finally, let us show that the "additional-message" rate R_1 as given by (3.25) is also achievable. We have seen that any rate pair (R_0, R_s) satisfying (3.23)-(3.24) is achievable in the system. Moreover, observe that Receiver 1 decodes correctly messages at the rate of $\min[I(U;Y), I(U;Z)]$ according to (3.30)-(3.31), and additionally decodes messages at the rate of $I(V;Y|U)$ owing to the part of the encoding $\{t_i, i \in \mathcal{J}^{(1)}\}$ given by (3.28). Since these two groups of information bits can be decoded simultaneously by Receiver 1, we conclude that it is possible to communicate to Receiver 1 an additional message at rate R_1.

Chapter 4: Construction of Polar Codes for Arbitrary Discrete Channels

4.1 Introduction

As already mentioned in Ch. 1, the construction complexity of polar codes is high because of the exponentially growing cardinality of the output alphabet of the bit-channels. This drawback of Arıkan's original proposal [2] has ushered in a large number of papers that aim to propose an efficient method of constructing the polar codes. Early on, an important observation was made in [55] which remarked that the construction procedure of polar codes for binary-input channels relies on essentially the same density evolution procedure that plays a key role in the analysis of low-density parity-check codes. It was soon realized that the proposal of [55] requires increasing precision of the computations, but this paper paved way for later research on the construction problem. An important step was taken in [56] which suggested to approximate each bit-channel after each evolution step by its degraded or upgraded version whose output alphabet size is constrained by a specified threshold μ that serves as a parameter of the procedure. As a result, [56] put forward an approximation procedure that results in a code not too far removed from the ideal choice of the bit-channels of [2]. This code construction scheme has a complexity of $O(N\mu^2 \log \mu)$, where $N = 2^n$ is the code length. For the channel degradation method described in [56], an error analysis and approximation guarantees are provided in [57].

Another approximation scheme for the construction of binary codes was considered in [69]. It is based on degrading each bit-channel after each evolution step, performed by merging several output symbols into one symbol based on quantizing the curve $p_{X|Y}(0|y)$ vs $h(p_{X|Y}(0|y))$, where $p_{X|Y}$ is the conditional distribution of the "reverse channel" that corresponds to the bit-channel in question. Symbols of the output alphabet that share the same range of quantization are merged into a single symbol of the approximating channel. Another algorithm based on bit-channel upgrading was described in [70], in which the authors argue that it is possible to obtain a channel which is arbitrarily close to the bit-channel of interest in terms of the capacity. However, no error or complexity analysis is provided in this work.

Moving to more general input alphabets, let us mention a code construction algorithm based on degrading the subchannels in each evolution step designed in [58]. This algorithm involves a merging procedure of output symbols similarly to [69]. However, as noted by the authors, their construction scheme is practical only for small values of input alphabet size q, its efficiency constrained by the complexity of order $O(\mu^q)$. Paper [59] proposed to perform the upgrading instead of degrading of the subchannels, but did not manage to reduce the implementation complexity. In [71], the authors consider another channel upgrading method for nonbinary-input channels, but stop short of providing an explicit construction scheme or error analysis.

Papers [72–74] addressed the construction problem of polar codes for AWGN channels. These works are based on Gaussian approximation of the intermediate likelihood ratios and do not analyze the error guarantees or rate loss of the obtained codes. A comparative study of various polar code constructions for AWGN channel is presented in [75].

Some other heuristic constructions for binary-input channels similar to the cited results for the Gaussian channel appear in [76–78]. Construction methods for some special examples of channels are given in [79, 80].

In this chapter we present a construction method of polar codes for arbitrary input alphabets. Our algorithm can be viewed as a generalization of the channel degradation method in [56] to nonbinary input channels. Our results differ from the previous works in the sense that we address channels with input alphabet of arbitrary cardinality and provide explicit error and complexity analysis. In particular, the complexity estimate of our procedure grows as $O(N\mu^4)$ as opposed to $O(N\mu^q)$ in earlier works. Although approach and the proof methods here are rather different from the approach in [57], the estimate of the approximation error that we derive generalizes the error bound given by [57] for the binary case. Another interesting connection with the literature concerns a very recent result of [60] which derives a lower bound on the alphabet size μ that is necessary to restrict the capacity loss by at most a given value ϵ. This bound is valid for any approximation procedure that is based only on the degrading of the subchannels in each evolution step. The construction scheme presented here relies on the value μ that is not too far from this theoretical limit (see Proposition 4.3 for more details).

Concluding the introductory part of this chapter, let us mention that the code construction technique presented below can be applied to any polarizing transform based on combining pairs of subchannels. There has been a great deal of research on properties of polarizing operations in general. In particular, it was shown in [81] that (1.9) holds true whenever the input alphabet size q of the channel W is a prime number, meaning that

Arıkan's transform $F = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ is polarizing for prime alphabets. For the case when q is a power of a prime, it was proved in [11] that there exist binary linear transforms different from F that support the estimate in (1.9) for some exponent β that depends on F. For example, [11] shows that the transform

$$G_\gamma = \begin{pmatrix} 1 & 0 \\ \gamma & 1 \end{pmatrix} \tag{4.1}$$

is polarizing whenever γ is a primitive element of the field $\mathbb{F}_q$. Paper [9] considered the use of Arıkan's transform for the channels with input alphabet of size $q = 2^r$, showing that the symmetric capacities of the subchannels converge to one of $r + 1$ integer values in the set $\{0, 1, \ldots, r\}$.

Even more generally, necessary and sufficient conditions for a binary operation $f : \mathcal{X}^2 \to \mathcal{X}^2$ given by

$$\begin{aligned} u_1 &= f(x_1, x_2), \\ u_2 &= x_2. \end{aligned} \tag{4.2}$$

to be a polarizing mapping were identified in [82, 83]. A simple set of *sufficient* conditions for the same was given in [84], which also gave a concrete example of a polarizing mapping for an alphabet of arbitrary size q. According to [84], in (4.2) one can take f in the form $f(x_1, x_2) = x_1 + \pi(x_2)$, where $\pi : \mathcal{X} \to \mathcal{X}$ is the following permutation:

$$\pi(x) = \begin{cases} \lfloor q/2 \rfloor, & \text{if} \quad x = 0, \\ x - 1, & \text{if} \quad 1 \leq x \leq \lfloor q/2 \rfloor, \\ x, & \text{otherwise.} \end{cases} \tag{4.3}$$

We include experimental results for code construction using the transforms (4.1) and (4.3) in Sect. 4.3.

Finally recall that it is possible to attain polarization based on transforms that combine $l > 2$ subchannels. In particular, polarization results for transformation kernels of size $l \times l$ with $l > 2$ for binary-input channels were studied in [20]. Apart from that, [11] derived estimates of the error probability of polar codes for nonbinary channels based on transforms defined by generator matrices of Reed-Solomon codes. However, below we will restrict our attention to binary combining operations of the form discussed above.

The rest of the chapter is organized as follows. In Section 4.2 we present our construction algorithm and its theoretical analysis. Our proposal is supported by extensive experimentation reported in Section 4.3.

4.2 The Code Construction Scheme

4.2.1 The approach

In the algorithm that we define, the subchannels are constructed recursively, and after each evolution step the resultant channel is replaced by its degraded version which has an output alphabet size less than a given threshold μ. The procedure is described in more detail in the figure that follows.

As discussed above, the operation Q^{b_j} appearing in Algorithm 1 does not have to be Arıkan's transform defined in Chapter 1. In Sect. 4.3 we give examples based on other transforms [11], [84] as discussed above.

Note that although the high-level description of our algorithm is the same as Al-

Algorithm 1 Degrading of subchannels

input: DMC W, Bound on the output size μ, Code length $N = 2^n$, Channel index i with binary representation $i = \langle b_1, b_2, \dots b_n \rangle_2$.

output: A DMC obtained from the subchannel W_i.

1: $Q \leftarrow$ `degrading_merge`(W, μ)
2: **for** $j = 1, 2, \dots, n$ **do**
3: $\quad Q \leftarrow Q^{b_j}$
4: $\quad Q \leftarrow$ `degrading_merge`(Q, μ)
5: **end for**
6: **return** Q

gorithm A in [56], the details are very different. The next step is to define the function `degrading_merge` in such a way that it can be applied for general discrete channels. Ideally, the degrading-merge operation on line 1 of the algorithm should optimize the degraded channel by attaining the smallest rate loss over all Q' :

$$\inf_{\substack{Q' : Q' \prec W \\ |\text{out}(Q')| \leq \mu}} I(W) - I(Q') \tag{4.4}$$

Equation (4.4) defines a convex maximization problem, which is difficult to solve with reasonable complexity. To reduce the computational load, [56] proposed the following approximation to (4.4): replace $y, y' \in \mathcal{Y}$ by a single symbol if the pair y, y' gives the minimum loss of capacity among all pairs of output symbols, and repeat this as many times as needed until the number of the remaining output symbols is equal to or less than μ (see Algorithm C in [56]). In [57, 69] this procedure was called *greedy mass merging*. In the binary case this procedure can be implemented with complexity $O(N\mu^2 \log \mu)$ because one can check only those pairs of symbols (y_1, y_2) which are closest to each other in terms of likelihood ratios (see Theorem 8 in [56]). This simplification does not generalize to the channels with nonbinary inputs, meaning that we need to sort all pairs of symbols. Since the total number of pairs is $O(\mu^4)$ after each evolution step, the overall

complexity of the greedy mass merging algorithm for nonbinary input alphabets becomes $O(N\mu^4 \log \mu)$.

The `degrading_merge` function we consider follows the paradigm of mapping a pair of output symbols to a single symbol at each step as well, but it is different from greedy mass merging function described above. The algorithm based on it (implemented in our experiments below) has a total running time of order $O(N\mu^4)$.

For a given channel W, let P_Y and $P_{X|Y}$ be the distributions induced by the joint distribution

$$P_{X,Y}(x, y) = \frac{1}{|\mathcal{X}|} W(y|x).$$

Recall that $I(W)$ is the symmetric capacity of the channel. The following lemma suggests a way of locating a pair of symbols to be merged.

Lemma 4.1. *Let $W : \mathcal{X} \to \mathcal{Y}$ be a discrete memoryless channel and let $y_1, y_2 \in \mathcal{Y}$ be two output symbols. Let $\tilde{W} : \mathcal{X} \to \mathcal{Y}\backslash\{y_1, y_2\} \cup \{y_{merge}\}$ be the channel obtained from by W by merging y_1 and y_2 which has the transition probabilities*

$$\tilde{W}(y|x) = \begin{cases} W(y|x), & \text{if} \quad y \in \mathcal{Y}\backslash\{y_1, y_2\} \\ W(y_1|x) + W(y_2|x), & \text{if} \quad y = y_{merge} \end{cases}.$$

Then

$$0 \leq I(W) - I(\tilde{W}) \leq \frac{P_Y(y_1) + P_Y(y_2)}{\ln 2} \, ||P_{X|Y}(.|y_1) - P_{X|Y}(.|y_2)||_1. \tag{4.5}$$

Proof. Since $\tilde{W}$ is degraded with respect to W, we clearly have that $I(W) \geq I(\tilde{W})$. To prove the upper bound for $I(W) - I(\tilde{W})$ in (4.5) let X be the random variable uniformly

distributed on $\mathcal{X}$, and let Y be the random output of W. Then, we have

$$I(W) - I(\tilde{W}) = \Big(H(X) - \sum_{y\in\mathcal{Y}} H(X|Y=y)P_Y(y)\Big)$$

$$-\Big(H(X) - H(X|Y\in\{y_1,y_2\})(P_Y(y_1)+P_Y(y_2)) - \sum_{y\in\mathcal{Y}\setminus\{y_1,y_2\}} H(X|Y=y)P_Y(y)\Big)$$

$$= H(X|Y\in\{y_1,y_2\})(P_Y(y_1)+P_Y(y_2))$$

$$- H(X|Y=y_1)P_Y(y_1) - H(X|Y=y_2)P_Y(y_2). \quad (4.6)$$

Next we have

$$\begin{aligned}
\Pr(X=x|Y\in\{y_1,y_2\}) &= \frac{\frac{1}{|\mathcal{X}|}(W(y_1|x)+W(y_2|x))}{P_Y(y_1)+P_Y(y_2)} \\
&= \frac{\frac{1}{|\mathcal{X}|}W(y_1|x)}{P_Y(y_1)+P_Y(y_2)} + \frac{\frac{1}{|\mathcal{X}|}W(y_2|x)}{P_Y(y_1)+P_Y(y_2)} \\
&= \frac{P_Y(y_1)}{P_Y(y_1)+P_Y(y_2)}P_{X|Y}(x|y_1) + \frac{P_Y(y_2)}{P_Y(y_1)+P_Y(y_2)}P_{X|Y}(x|y_2) \\
&= \alpha_{12}P_{X|Y}(x|y_1) + (1-\alpha_{12})P_{X|Y}(x|y_2)
\end{aligned}$$

where $\alpha_{12} \triangleq \frac{P_Y(y_1)}{P_Y(y_1)+P_Y(y_2)}$. Hence, it follows from (4.6) that

$$\begin{aligned}
&I(W) - I(\tilde{W}) \\
&= (P_Y(y_1)+P_Y(y_2)) \sum_{x\in\mathcal{X}} \big[\alpha_{12}P_{X|Y}(x|y_1) + (1-\alpha_{12})P_{X|Y}(x|y_2)\big] \\
&\times \log_2 \frac{1}{\alpha_{12}P_{X|Y}(x|y_1) + (1-\alpha_{12})P_{X|Y}(x|y_2)} \\
&- P_Y(y_1)\sum_{x\in\mathcal{X}} P_{X|Y}(x|y_1)\log_2\frac{1}{P_{X|Y}(x|y_1)} - P_Y(y_2)\sum_{x\in\mathcal{X}} P_{X|Y}(x|y_2)\log_2\frac{1}{P_{X|Y}(x|y_2)}.
\end{aligned}$$

Rearranging the terms, we obtain

$$I(W) - I(\tilde{W}) = P_Y(y_1) \sum_{x \in \mathcal{X}} P_{X|Y}(x|y_1) \log_2 \frac{P_{X|Y}(x|y_1)}{\alpha_{12} P_{X|Y}(x|y_1) + (1-\alpha_{12}) P_{X|Y}(x|y_2)}$$
$$+ P_Y(y_2) \sum_{x \in \mathcal{X}} P_{X|Y}(x|y_2) \log_2 \frac{P_{X|Y}(x|y_2)}{\alpha_{12} P_{X|Y}(x|y_1) + (1-\alpha_{12}) P_{X|Y}(x|y_2)}.$$

Next use the inequality $\ln x \leq x - 1$ to write

$$\begin{aligned} & I(W) - I(\tilde{W}) \\ & \leq P_Y(y_1) \sum_{x \in \mathcal{X}} \frac{P_{X|Y}(x|y_1)}{\ln 2} \left(\frac{P_{X|Y}(x|y_1)}{\alpha_{12} P_{X|Y}(x|y_1) + (1-\alpha_{12}) P_{X|Y}(x|y_2)} - 1 \right) \\ & \quad + P_Y(y_2) \sum_{x \in \mathcal{X}} \frac{P_{X|Y}(x|y_2)}{\ln 2} \left(\frac{P_{X|Y}(x|y_2)}{\alpha_{12} P_{X|Y}(x|y_1) + (1-\alpha_{12}) P_{X|Y}(x|y_2)} - 1 \right) \end{aligned}$$

which simplifies to

$$\begin{aligned} & I(W) - I(\tilde{W}) \\ & \leq \frac{P_Y(y_1)}{\ln 2} \sum_{x \in \mathcal{X}} P_{X|Y}(x|y_1) \frac{(1-\alpha_{12})(P_{X|Y}(x|y_1) - P_{X|Y}(x|y_2))}{\alpha_{12} P_{X|Y}(x|y_1) + (1-\alpha_{12}) P_{X|Y}(x|y_2)} \\ & \quad + \frac{P_Y(y_2)}{\ln 2} \sum_{x \in \mathcal{X}} P_{X|Y}(x|y_2) \frac{\alpha_{12}(P_{X|Y}(x|y_2) - P_{X|Y}(x|y_1))}{\alpha_{12} P_{X|Y}(x|y_1) + (1-\alpha_{12}) P_{X|Y}(x|y_2)}. \end{aligned} \tag{4.7}$$

Bound the first term in (4.7) using the inequality

$$\left| \frac{(1-\alpha_{12})(P_{X|Y}(x|y_1) - P_{X|Y}(x|y_2))}{\alpha_{12} P_{X|Y}(x|y_1) + (1-\alpha_{12}) P_{X|Y}(x|y_2)} \right| \leq \frac{(1-\alpha_{12}) |P_{X|Y}(x|y_1) - P_{X|Y}(x|y_2)|}{\alpha_{12} P_{X|Y}(x|y_1)}$$

and do the same for the second term. We obtain the estimate

$$\begin{aligned} I(W) - I(\tilde{W}) & \leq \frac{P_Y(y_1)}{\ln 2} \frac{1-\alpha_{12}}{\alpha_{12}} \sum_{x \in \mathcal{X}} |P_{X|Y}(x|y_1) - P_{X|Y}(x|y_2)| \\ & \quad + \frac{P_Y(y_2)}{\ln 2} \frac{\alpha_{12}}{1-\alpha_{12}} \sum_{x \in \mathcal{X}} |P_{X|Y}(x|y_1) - P_{X|Y}(x|y_2)| \\ & = \frac{P_Y(y_1) + P_Y(y_2)}{\ln 2} ||P_{X|Y}(.|y_1) - P_{X|Y}(.|y_2)||_1. \end{aligned}$$

This completes the proof of (4.5). □

The bound in (4.5) brings in metric properties of the probability vectors. Leveraging them, we can use simple volume arguments to bound the rate loss due to approximation.

Lemma 4.2. *Let the input and output alphabet sizes of W be q and M, respectively. Then, there exists a pair of output symbols (y_1, y_2) such that*

$$P_Y(y_1) = O\left(\frac{1}{M}\right), \quad P_Y(y_2) = O\left(\frac{1}{M}\right),$$
$$||P_{X|Y}(.|y_1) - P_{X|Y}(.|y_2)||_1 = O\left(\left(\frac{1}{M}\right)^{\frac{1}{q-1}}\right)$$

which implies the estimate

$$0 \leq I(W) - I(\tilde{W}) = O\Big(\Big(\frac{1}{M}\Big)^{1+\frac{1}{q-1}}\Big) \tag{4.8}$$

Proof. Consider the subset of output symbols $A_M(\mathcal{Y}) = \{y : P_Y(y) \leq 2/M\}$. Noticing that $|(A_M(\mathcal{Y}))^c| \leq M/2$, we conclude that

$$|(A_M(\mathcal{Y}))| \geq \frac{M}{2}. \tag{4.9}$$

Keeping in mind the bound (4.5), let us estimate the maximum value of the quantity

$$\min_{y_1, y_2 \in A_M(\mathcal{Y}))} \|P_{X|Y}(\cdot|y_1) - P_{X|Y}(\cdot|y_2)\|_1. \tag{4.10}$$

For each $y \in \mathcal{Y}$, the vector $P_{X|Y}(.|y)$ is an element of the probability simplex

$$S_q = \left\{(s_1, \ldots, s_q) \in \mathbb{R}^q \middle| s_i \geq 0, \sum_{i=1}^{q} s_i = 1\right\}.$$

Let $R > 0$ be a number less than the quantity in (4.10). Clearly, for any $y_1, y_2 \in A_M(\mathcal{Y}))$ the q-dimensional ℓ_1-balls of radius $R/2$ centered at $P_{X|Y}(\cdot|y_i), i = 1, 2$ are disjoint, and

therefore, so are their intersections with S_q. Let $\mathrm{vol}(S_q)$ be the $(q-1)$-dimensional volume of S_q. It is easily seen that $\mathrm{vol}(S_q) = \sqrt{q}/(q-1)!$, but in this proof we will stay with crude bounds (a more precise calculation is performed in the remark below). Clearly for any $y \in \mathcal{Y}$

$$\mathrm{vol}\left\{B_{R/2}(P_{X|Y}(\cdot|y_i)) \cap S_q\right\} = O\Big(\frac{R}{2}\Big)^{q-1}$$

On account of (4.9) we obtain that

$$\frac{M}{2}\, O\Big(\Big(\frac{R}{2}\Big)^{q-1}\Big) \leq \mathrm{vol}(S_q) \tag{4.11}$$

whence

$$R = O\Big(\Big(\frac{1}{M}\Big)^{1/(q-1)}\Big)$$

for all R less than (4.10). Hence, we see that there exist two output symbols $y_1, y_2 \in A_M(\mathcal{Y})$ such that the conditions

$$\|P_{X|Y}(\cdot|y_1) - P_{X|Y}(\cdot|y_2)\|_1 = O\Big(\Big(\frac{1}{M}\Big)^{\frac{1}{q-1}}\Big) \tag{4.12}$$

hold simultaneously. So if these symbols are merged in the algorithm discussed, the rate loss is bounded above as

$$I(W) - I(\tilde{W}) = O\bigg(\Big(\frac{1}{M}\Big)^{1+\frac{1}{q-1}}\bigg)$$

□

This lemma leads to an important conclusion for the code construction: to degrade the subchannels we should merge the symbols y_1, y_2 with small $P_Y(y_i)$ and such that the reverse channel conditional PMFs $P_{X|Y}(\cdot|y_i), i = 1, 2$ are ℓ_1-close. Performing this step several times in succession, we obtain the operation called `degrading_merge` in the

description of Algorithm 1. The properties of this operation are stated in in the following proposition.

Proposition 4.3. *Let W be a DMC with input of size q.*

(a) There exists a function `degrading_merge`(W, μ) *such that its output channel Q satisfies*

$$0 \leq I(W) - I(Q) \leq O\Big(\Big(\frac{1}{\mu}\Big)^{\frac{1}{q-1}}\Big). \tag{4.13}$$

(b) For a given block length, let $W_N^{(i)}$ be the i-th subchannel after n evolution steps of the polarization recursion. Let $Q_N^{(i)}$ denote the its approximation returned by Algorithm 1. Then

$$0 \leq \frac{1}{N} \sum_{0 \leq i \leq N} (I(W_N^{(i)}) - I(Q_N^{(i)})) \leq n\, O\Big(\Big(\frac{1}{\mu}\Big)^{\frac{1}{q-1}}\Big). \tag{4.14}$$

Proof. Let M be the cardinality of the output alphabet of W. Performing $M - \mu$ merging steps of the output symbols in succession, we obtain a channel with an output alphabet of size μ. If the pairs of symbols to be merged are chosen based on Lemma 4.2, then (4.12) implies that

$$\begin{aligned} 0 \leq I(W) - I(Q) &\leq C(q) \sum_{i=\mu+1}^{M} \Big(\frac{1}{i}\Big)^{1+\frac{1}{q-1}} \\ &\leq C(q) \int_{\mu}^{M} (x-1)^{-(1+\frac{1}{q-1})} dx = O\Big(\Big(\frac{1}{\mu}\Big)^{\frac{1}{q-1}}\Big) \end{aligned}$$

where $C(q)$ is a constant which depends on the input alphabet size q but not on the number n of recursion steps. This proves (4.13), and (4.14) follows immediately. □

Remark 4.2.1. *This result provides a generalization to the nonbinary case of a result in [57] which analyzed the a merging (degrading) algorithm of [56]. For the case of*

binary-input channels, Lemma 1 of [57] gave an estimate $O(1/\mu)$ of the approximation error. Substituting $q = 2$ in (4.13)*, we observe that this result is a generalization of [57] to channels with arbitrary finite-size input.*

Remark 4.2.2. *Upper bounds similar to* (4.13) *are derived in [58, Lemma 6] and [59, Lemma 8]. The output symbol merging policy in [58] makes it possible to have $I(W) - I(\tilde{W}) = O\big((1/\mu)^{1/q}\big)$. On the other hand, the channel upgrading technique introduced in [59] gives the same bound as* (4.13)*. Recall that the code construction schemes considered in those two works have complexity $O(\mu^q)$. It is interesting to observe that merging a pair of output symbols to a single symbol successively as we do here is as good as the algorithms based on binning of output symbols which requires a higher complexity.*

Remark 4.2.3. *A very recent result of [60] states that any construction procedure of polar codes construction based on degrading after each polarization step, that guarantees the rate loss bounded as $I(W) - I(Q) \leq \epsilon$, necessarily has the output alphabet of size $\mu = \Omega((1/\epsilon)^{\frac{q-1}{2}})$. Proposition 4.3 implies that the alphabet size of the algorithm that we propose scales as the square of this bound, meaning that the proposed procedure procedure is not too far from being optimal, namely for any channel, our degradation scheme satisfies $\mu \leq (1/\epsilon)^{q-1}$, and there exists a channel for which $\mu \geq (1/\sqrt{\epsilon})^{q-1}$ holds true even for the optimal degradation scheme.*

A MORE EXPLICIT CALCULATION RELATED TO (4.11): Some of the implicit constants in the calculation that leads to (4.12) in the proof of Lemma 4.2 can be removed using the

following (heuristic) geometric argument. Let

$$\mathcal{S}_q = \left\{ x \in \mathbb{R}^q, \sum_{i=1}^{q} s_i \le 1, s_i \ge 0, i = 1, \ldots, q \right\}$$

be the regular q-dimensional simplex whose "outer" face is S_q. Consider the intersection of the q-dimensional balls with $\mathcal{S}_q$ rather than S_q. The volume of this intersection is the smallest when the center of the ball is located at a vertex of $\mathcal{S}_q$. Let $V_q^p(R)$ be the volume of the ℓ_p-ball of radius R in q dimensions. Computing a crude estimate for the number of simplices that share a common vertex, note that they all fit in the ℓ_2 sphere of radius $\sqrt{2}$, so their number is at most $V_q^2(\sqrt{2}) / \operatorname{vol}(\mathcal{S}_q)$. Assuming that the volume of the ℓ_1-ball around the vertex is shared equally between these simplices, we estimate the volume of the intersection to be[1]

$$V_q^1(R/2) \frac{\operatorname{vol}(\mathcal{S}_q)}{V_q^2(\sqrt{2})} = \frac{(\Gamma(2)R)^q}{\Gamma(q+1)} \frac{\Gamma\left(\frac{q}{2}+1\right)}{\left(2\sqrt{2}\,\Gamma(3/2)\right)^q} \operatorname{vol}(\mathcal{S}_q).$$

Using a packing argument similar to (4.11), we obtain

$$\frac{R^q}{q!} \frac{\Gamma\left(\frac{q}{2}+1\right)}{\left(2\sqrt{2}\,\Gamma(3/2)\right)^q} \le \frac{2}{M}$$

which gives

$$R \le C \Big(\frac{1}{M}\Big)^{1/q}$$

where $C = 2\sqrt{2}\,\Gamma\left(\frac{3}{2}\right)\left(\frac{2q!}{\Gamma(\frac{q}{2}+1)}\right)^{1/q} \le \sqrt{2\pi}q$. This calculation results in a bound slightly weaker than the one in (4.13), but contains no implicit constants.

[1]The expressions for the volume of the ball in different norms are taken from the Wikipedia article "Volume of an n ball".

4.2.2 The degrading step

In the previous section we established the principles of the code construction. The idea was to approximate each subchannel by another channel having output alphabet size μ after each evolution step. We have also proposed a method to carry out such an approximation in Lemma 4.2 and Proposition 4.3. In this section we present a specific procedure that can be used to construct a polar code of a given length adopted to a channel W. This is the procedure we implemented in our experiments in Sect. 4.3. We note that the procedure described below is not the only way to utilize our results: we could in principle implement the greedy mass merging (i.e., merging pairs of symbols based on their symmetric capacities) rather than on the distance between the probability distributions.

Let us define more explicitly the `degrading_merge` function described in Proposition 4.3. We attempt to find a pair of output symbols y_1 and y_2 such that

$$P_Y(y_1) \leq \frac{C_1}{M}, \quad P_Y(y_2) \leq \frac{C_1}{M}$$
$$||P_{X|Y}(.|y_1) - P_{X|Y}(.|y_2)||_1 \leq C_2 \left(\frac{1}{M}\right)^{1/(q-1)},$$

where C_1, C_2 are some constants. Once such a pair of symbols is found, we merge them into one symbol of the output of the new degraded channel, and update the P_Y and $P_{X|Y}$ matrices accordingly. This step is iterated as many times as needed until the cardinality of the output alphabet falls below μ. The described procedure is summarized in Algorithm 2 below. The notation in the algorithm is mostly self-explanatory; let us just note that `Calc_PY`(Q) refers to computing the marginal PMF of the channel output and `Calc_X|Y`(Q) is the same for the conditional PMF of the reverse channel.

Algorithm 2 The `degrading_merge` function

input: DMC $W : \mathcal{X} \to \mathcal{Y}, |\mathcal{X}| = q, |\mathcal{Y}| = M$; constants C_1 and C_2; desired output size μ
output: Degraded channel $Q : \mathcal{X} \to \mathcal{Y}'$, where $|\mathcal{Y}'| \leq \mu$.

```
Q ← W
py ← Calc_PY(Q)
x_given_y ← Calc_X|Y(Q)
ℓ ← M
for k = 1, 2, ..., M do
    if py[k] ≤ C_1/μ then
        for j = k + 1, k + 2, ..., M do
            if py[j] ≤ C_1/ℓ and ||x_given_y[j] − x_given_y[k]||_1 ≤ C_2(1/μ)^{1/(q−1)} then
                Q ← merge_two_symbols(Q, j, k)
                py ← update_py(py, j, k)
                x_given_y ← update_x_given_y(x_given_y, j, k)
                ℓ ← ℓ − 1
                break
            end if
        end for
    end if
    if ℓ ≤ μ then
        break
    end if
end for
return Q
```

Proposition 4.4. (COMPLEXITY ESTIMATE) *The running time of the proposed implementation of the code construction algorithm is at most* $O(N\mu^6)$.

Proof. Lemma 4.2 guarantees that there exists a constant C_2 for which running $M - \mu$ rounds of the degrading-merge function produces a degraded channel with an output alphabet of size μ. Since each iteration has complexity $O(M^2)$, the whole degrading operation can be performed in $O(M^3)$ steps. Moreover, Algorithm 1 implies that the maximum value that M can take during the polar code construction procedure is $q\mu^2$. Hence, we see that `degrading_merge` takes $O(\mu^6)$ time in Algorithm 1, meaning that the total running time for the computation of a single subchannel W_i is $O(n\mu^6)$. Getting

to the block length $N = 2^n$ involves computing $2^1 + 2^2 + \cdots + 2^n = 2N - 2$ subchannels in the nodes of the splitting-combining tree, and so the overall running time of our polar code construction is $O(N\mu^6)$, as claimed. □

In our experiments we run `degrading_merge` a constant number of times which is independent of μ. Hence, what we have in practice is that `degrading_merge` takes $O(\mu^4)$ time, resulting in an overall complexity of $O(N\mu^4)$ as opposed to $O(N\mu^6)$.

4.3 Experimental Results

We have tested the code construction algorithm of the previous section for a number of communication channels. As an outcome of the algorithm, we always obtain the indices of the subchannels that provide the indices of the bits that should be used for transmitting the data (in the case of linear codes, they also give the indices of the basis vectors of the code). In our examples we plot the sorted capacities of the subchannels from 1 to N, providing an immediate view of the polarization attained. Since we are approximating the outcome, we should expect some rate loss compared to the channel capacity. We compute the gap to capacity (denoted by $\Delta(I(W))$) and provide it for each of the examples. In the limit of $n \to \infty$ we should observe a rectangular-shaped transition from channels with capacity 0 to positive capacity. This ideal distribution is plotted in the figures with the dashed line.

In the examples we use some of many available polarization transforms mentioned above in Sect. 4.1. This confirms that the algorithm does not discriminate between the transforms (in fact, it does not even know which transform is used). We also tried con-

structing codes for some of the channels introduced in [9] for which Arıkan's transform is known to yield more than two levels of polarization. The resulting codes clearly show the expected multilevel-polarized constructions.

In our examples, we do not provide results associated with the probability of error (except for Example 12.) This is because codes of rather large length (such as $N = 2^{20}$) are needed to present meaningful results for error probability, which would require significant running time in most of our examples.

Example 1. Let W be the q-ary symmetric channel (qSC) with $q = 5$ and $\epsilon = 0.05$. More precisely, $W(y|x)$ is defined as

$$W(y|x) = \begin{cases} 0.8, & \textit{if} \quad y = x \\ 0.05, & \textit{if} \quad y \neq x. \end{cases}$$

In this example we have chosen $C_1 = 10$ and $C_2 = 2$ in Algorithm 2. The resultant capacities of the virtual channels for $n = 8$ and $\mu = 200$ are shown by Figure 4.1(a). We have $I(W) = 1.2$, $\Delta(I(W)) = 0.075$.

Example 2. Let $W : \{0, 1, 2, 3, 4\} \to \{0, 1, 2, 3, 4\}$ be defined by the transition matrix

$$W(y|x) = \begin{bmatrix} 0.5 & 0.5 & 0 & 0 & 0 \\ 0 & 0.5 & 0.5 & 0 & 0 \\ 0 & 0 & 0.5 & 0.5 & 0 \\ 0 & 0 & 0 & 0.5 & 0.5 \\ 0.5 & 0 & 0 & 0 & 0.5 \end{bmatrix}.$$

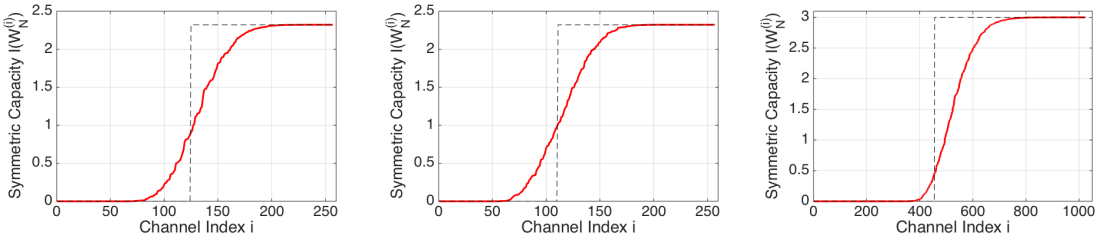
In other words, W is a channel such that whenever a symbol is transmitted, with probability $1/2$ the same symbol is observed at the output, and with probability $1/2$ the next symbol is observed at the output. For this channel, the result is plotted in Figure 4.1(b). We have $I(W) = 1.322$, $\Delta(I(W)) = 0.047$.

Both Example 1 and Example 2 correspond to the case when the virtual channels polarize to two levels. This is consistent with the polarization theorem proved in [81] which states that this is always the case for input alphabets of prime size.

Example 3. Let W be the qSC with $q = 8$ and $\epsilon = 0.03$, viz.,

$$W(y|x) = \begin{cases} 0.79, & \textit{if} \quad y = x \\ \\ 0.03, & \textit{if} \quad y \neq x \end{cases}$$

The results obtained for this channel are given by Figure 4.1(c). We have $I(W) = 1.669$ and $\Delta(I(W)) = 0.224$. Interestingly, even though the general result [9] suggests that the channels may polarize to 4 levels, the actual polar codes have only two types of the subchannels, of capacity zero and of the full 3-bit capacity.



(a) Example 1 (b) Example 2 (c) Example 3

Figure 4.1: The capacity distribution of the virtual channels.
(a) qSC with $q = 5, \epsilon = 0.05$. The parameters of the algorithm are taken to be $n = 8, \mu = 200, C_1 = 10, C_2 = 2$.
(b) Noisy typewriter channel with $q = 5$ and crossover probability $1/2$. The parameters are the same as in Part (a).
(c) qSC with $q = 8, \epsilon = 0.03$. The parameters are $n = 10, \mu = 200, C_1 = 10, C_2 = 2$.

Example 4. Let W be the qSC with $q = 16$ and $\epsilon = 0.01$. In other words, we have

$$W(y|x) = \begin{cases} 0.85, & \textit{if} \quad y = x \\ \\ 0.01 & \textit{if} \quad y \neq x \end{cases}$$

In this example, we use the polarizing mapping (4.3) rather than the regular Arıkan's transform. The result we get is shown in Figure 4.2(a). We have $I(W) = 2.804$ and $\Delta(I(W)) = 0.352$.

Example 5. In this example we take the same channel as in Example 4, but use the polarizing transform G_γ of [11], performed over the field $\mathbb{F}_{16}$. The polarized channels computed after $n = 8$ steps are shown in Figure 4.2(b). We have $I(W) = 2.804$ and $\Delta(I(W)) = 0.417$.

As seen from Figures 4.2(a) and 4.2(b), the virtual channels polarize to two levels, which is consistent with the polarization theorems of [84] and [11], respectively.

Example 6. Let $W : \mathcal{X} \to \mathcal{Y}$ be an "ordered erasure channel" (OEC, [9]) with 4 inputs, 7 outputs and transition probabilities $\epsilon_0 = 0.5$, $\epsilon_1 = 0.4$, $\epsilon_2 = 0.1$. More precisely, assume that $\mathcal{X} = \{00, 01, 10, 11\}$ and $\mathcal{Y} = \{00, 01, 10, 11, ?0, ?1, ??\}$, and define the transition probabilities as follows:

$$W(x_1x_2|x_1x_2) = 0.5$$

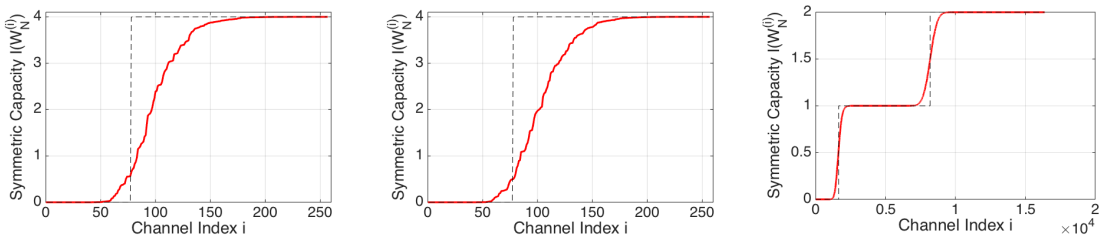
$$W(?x_2|x_1x_2) = 0.4$$

$$W(??|x_1x_2) = 0.1$$

for all $x_1, x_2 \in \{0, 1\}$.

The resultant capacities for $n = 14$ and $\mu = 16$ are shown by Figure 4.2(c). We have $I(W) = 1.4$ and no loss in the average capacity was observed in this example.

For channels of this type, the capacity distribution of the virtual channels for $n \to \infty$ approaches the PMF $F(i) = \epsilon_{r-i}, i = 1, 2, 3$, where $r = \log_2 q = 3$ [9]. As seen from Figure 4.2(c), the obtained results are consistent with this property.



(a) Example 4 (b) Example 5 (c) Example 6

Figure 4.2: The capacity distribution of the virtual channels.

(a) Polarization of the qSC with $q = 16, \epsilon = 0.01$ under the transform (4.3). The parameters of the algorithm are $n = 8, \mu = 300, C_1 = 1.5, C_2 = 1.5$.

(b) The channel and the parameters of the algorithm are the same as previous case. The polarizing transform we use is given in (4.1).

(c) OEC with $\epsilon_0 = 0.5$, $\epsilon_1 = 0.4$, $\epsilon_2 = 0.1$. The parameters are $n = 14, \mu = 16, C_1 = 1.5, C_2 = 2$.

Example 7. Let $W : \mathcal{X} \to \mathcal{Y}$ be an OEC with 8 inputs, 15 outputs and transition probabilities $\epsilon_0 = 0.3$, $\epsilon_1 = 0.2$, $\epsilon_2 = 0.3$, $\epsilon_3 = 0.2$, i.e.,

$$W(x_1x_2x_3|x_1x_2x_3) = 0.3$$

$$W(?x_2x_3|x_1x_2x_3) = 0.2$$

$$W(??x_3|x_1x_2x_3) = 0.3$$

$$W(???|x_1x_2x_3) = 0.2$$

In this example we choose $C_1 = 1.5, C_2 = 2$, $n = 12$, and $\mu = 200$ in Algorithm 2. The obtained results are plotted in Figure 4.3(a). We have $I(W) = 1.6$ and observe that the obtained code shows no capacity loss due to approximation.

To compare our algorithm with the existing results, we tried to implement the polar code construction scheme proposed in [58]. Because of the binning algorithm that this scheme involves, the output alphabet size limit μ has to be of the form $\mu = k^q$ for some

even integer k. In this example, we have $q = 8$, and thus the smallest two values that μ can take are 256 and 65536. For $\mu = 256$, the average capacity loss of 20% is observed even for $n = 2$ (since in each step we perform approximations, the loss can only increase with n). Choosing $\mu = 65536$, we run into implementation problems such as the memory allocation error after a few steps of the recursion.

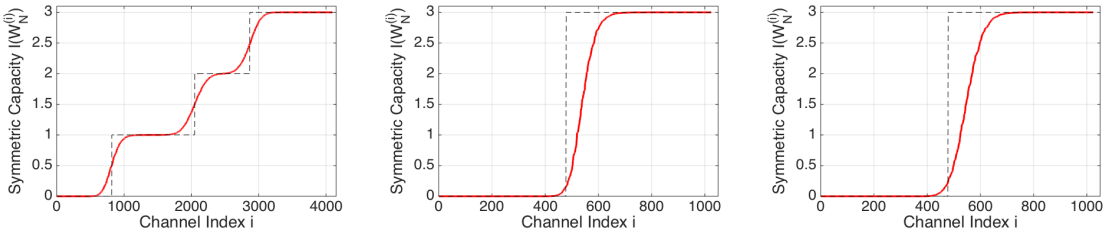
Example 8. Let W be the same channel as in Example 7 used together with the polarizing mapping of [84] rather than the Arıkan's transform. The obtained results are shown in Fig. 4.3(b). We have $I(W) = 1.6$ and $\Delta(I(W)) = 0.185$. As predicted by [84], the transform used in this example polarizes the channels to the two extremes, removing the intermediate levels present in Fig. 4.3(a).

Example 9. Let W be the same channel as in Example 7 once again, but this time used together with the finite field transform G_γ over $\mathbb{F}_8$ suggested in [11]. The output we have obtained is shown in Figure 4.3(c), from which we clearly see how G_γ polarizes the virtual channels to two levels. We have $I(W) = 1.6$ and $\Delta(I(W)) = 0.206$.

Example 10. Let $W : \mathcal{X} \to \mathcal{Y}$ be the q-ary erasure channel (qEC) with $q = 8$ and $\epsilon = 0.5$. In this case, we have $\mathcal{X} = \{0, 1, \ldots, 7\}$, $\mathcal{Y} = \mathcal{X} \cup \{?\}$, and $W(y|x)$ has the form

$$W(y|x) = \begin{cases} 0.5, & \textit{if} \quad y = x \\ \\ 0.5, & \textit{if} \quad y =? \end{cases}$$

This channel has the capacity curve given in Figure 4.4(a). This channel is a specialization of an OEC with the transition probabilities $\epsilon_0 = 0.5, \epsilon_1 = 0, \epsilon_2 = 0, \epsilon_3 = 0.5$. As expected, the virtual channels polarize to two levels under Arıkan's transform.



(a) Example 7 (b) Example 8 (c) Example 9

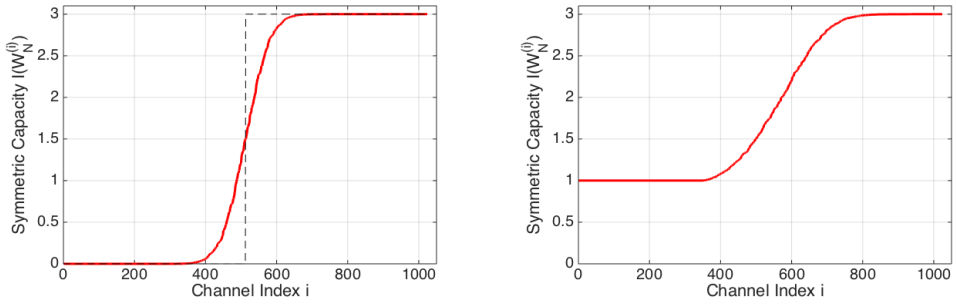
Figure 4.3: The capacity distribution of the virtual channels for the OEC with $\epsilon_0 = 0.3$, $\epsilon_1 = 0.2$, $\epsilon_2 = 0.3$, $\epsilon_3 = 0.2$. The parameters of the algorithm are $\mu = 200, C_1 = 1.5, C_2 = 2$.

(a) Arıkan's transform, $n = 12$.

(b) Şaşoğlu's transform (4.3), $n = 10$,

(c) Mori-Tanaka's transform (4.1), $n = 10$.

We have $I(W) = 1.5$ and we do not observe any loss in the average capacity for this example.



(a) Example 10 (b) Example 11

Figure 4.4: The capacity distribution of the virtual channels.

(a) qEC with $q = 8, \epsilon = 0.5$. The parameters of the algorithm are taken to be $n = 10, \mu = 200, C_1 = 1.5, C_2 = 2$.

(b) OSC with $\epsilon_0 = 0.8, \epsilon_1 = 0.1, \epsilon_2 = 0.1, \epsilon_3 = 0$. The parameters are $n = 10, \mu = 200, C_1 = 1.5, C_2 = 0.8$.

Example 11. Let W be an "ordered symmetric channel" (OSC) of [9] with the input alphabet of size 8, and the parameters $\epsilon_0 = 0.8$, $\epsilon_1 = 0.1$, $\epsilon_2 = 0.1$, and $\epsilon_3 = 0$. More

precisely, W is defined as

$$W(x_1x_2x_3|y_1y_2y_3) = \begin{cases} 0.8, & \textit{if} \quad x_1 = y_1, x_2 = y_2, x_3 = y_3 \\ 0.1, & \textit{if} \quad x_1 \neq y_1, x_2 = y_2, x_3 = y_3 \\ 0.05, & \textit{if} \quad x_2 \neq y_2, x_3 = y_3 \\ 0, & \textit{if} \quad x_3 \neq y_3. \end{cases}$$

For this channel, the capacity distribution curve that we obtain is given by Figure 4.4(b). We have $I(W) = 1.978$ and $\Delta(I(W)) = 0.093$. We see that the virtual channels polarize to two levels, one level being one bit of capacity, and the other level being three bits of capacity. We do not have zero bit of capacity as one of the levels in this example.

Example 12. The last example that we consider is the *binary* symmetric channel BSC(p) with crossover probability $p = 0.11$. The capacity of this channel is $I(W) \approx 0.5$. For this channel, we compare our algorithm with the bin-and-merge algorithm in [69] and the channel degradation algorithm in [56] (called the "greedy mass merging algorithm" in [57, 69], as explained above.) For $C_1 = 10$ and $C_2 = 3$, the results are provided in Table 4.1 and Table 4.2.

It is to be expected there is a gain in merging output symbol pairs optimally at each step compared to the `degrading_merge` function we have defined. Note that this gain decreases as the number of iterations n or the number of quantization levels μ increases. We also observe from Tables 4.1 and 4.2 that our algorithm is slightly inferior to the bin-and-merge algorithm for binary-input channels.

n	5	8	11	14	17	20
Greedy mass merging, degrade [56]	0.1250	0.2109	0.2969	0.3620	0.4085	0.4403
Bin and merge, degrade [69]	0.1250	0.1836	0.2422	0.3063	0.3626	0.4051
Our algorithm	0.0625	0.1446	0.2188	0.2853	0.3385	0.3830

Table 4.1: The highest rate R for which the sum error probability of the $NR, N = 2^n$ most reliable subchannels (out of the 2^n channels) is at most 10^{-3}.

μ	4	8	16	32	64
Greedy mass merging, degrade [56]	0.3667	0.3774	0.3795	0.3799	0.3800
Bin and merge, degrade [69]	0.3019	0.3134	0.3264	0.3343	0.3422
Our algorithm	0.2573	0.2775	0.3046	0.3191	0.3369

Table 4.2: The highest rate R for which the sum error probability of the $NR, N = 2^n$ most reliable subchannels is at most 10^{-3} with μ quantization levels and $n = 15$ recursions.

Chapter 5: Concluding Remarks

This thesis is devoted to the design and analysis of constructive schemes for some problems in information theory relying on polar codes and polarization.

In the first two chapters we analyze several problems related to multi-user or interactive communication for which capacity regions have been found in the literature, but no explicit schemes that attain these regions were available prior to our research. In Chapter 2 we study some problems of interactive computation by two or several communicating terminals. The aim of the communication is to reduce the amount of data transmitted between the terminals based on ideas from distributed data compression. The design of explicit schemes calls for careful analysis of the joint statistics of the messages exchanged between the terminals to ensure the proximity of the realizations of random variables to their desired distributions. We hope that the technical arguments developed in the course of this analysis can find uses in other interactive communication problems. One promising direction of development is related to the multitude of scenarios for interactive computation and communication in networks that are actively studied in the current literature; see, e.g., [27, 28, 31].

A somewhat similar technical setting (albeit in the context of communication over noisy channels rather than distributed compression) underlies the analysis of the scheme

for transmission over the wiretap channel designed in Chapter 3. Similarly to Ch. 2 we also have to incorporate auxiliary random variables that characterize the capacity region in the encoding scheme and the analysis of the encoding scheme and its validity. While communication designs for a number of particular cases of the wiretap channel were known in the literature prior to our work, we have covered the general case that does not assume any symmetry conditions or the degradedness of the wiretapper's channel compared to the main channel in the system. The approach chosen in this chapter enables us to extent our coding scheme to the more general case when the transmitter aims to communicate with both receiving parties in the system, at the same time keeping one part of the message secret from one of the receivers. Interestingly, polar codes can be also used to address this (more general) problem.

In the final Chapter 4 we take up the problem of constructing polar codes for non-binary alphabets. Constructing polar codes has been a difficult open question since the introduction of the binary polar codes in [2]. Ideally, one would like to obtain an explicit description of the polar codes for a given block length, but this seems to be beyond reach at this point. As an alternative, one could attempt to construct the code by approximating each step of the recursion process. For binary codes, this has been done in [56], but extending this to the nonbinary case was an open problem despite several attempts in the literature. We take this question one step closer to the solution be designing an algorithm that approximates the construction for moderately-sized input alphabets such as $q = 8$ or $q = 16$. Apart from presenting a theoretical advance, this algorithm provides a useful tool in the analysis of properties of various polarizing transforms applied to nonbinary codes over alphabets of different structure. The proposed construction algorithm brings

nonbinary codes closer to practical applications, which is another promising direction to be explored in the future.

Further theoretical problems related to this construction include constructing codes for asymmetric channels as well as for the problems involving interactive communication, distributed data compression and secure communication. Another interesting problem is to construct nonbinary LDPC codes by using an appropriate degradation algorithm in each step of density evolution.

Bibliography

[1] C.E. Shannon, *A mathematical theory of communication*, Bell System Tech. J., 27(1948), 379–423, 623–656.

[2] E. Arıkan, *Channel polarization: a method for constructing capacity-achieving codes for symmetric binary-input memoryless channels*, IEEE Trans. Inform. Theory **55** (2009), no. 7, 3051–3073.

[3] J. Honda and H. Yamamoto, *Polar coding without alphabet extension for asymmetric models*, IEEE Trans. Inform. Theory **59** (2013), no. 12, 7829–7838.

[4] M. Mondelli, R. Urbanke and S. H. Hassani, *How to Achieve the Capacity of Asymmetric Channels*, Proc. 52th Annual Allerton Conf. on Comm., Control and Computing, 2014, pp. 789–796.

[5] E. Abbe and E. Telatar, *Polar codes for the m-user multiple access channel.* IEEE Trans. Inform. Theory **58** (2012), no. 8, 5437–5448.

[6] E. Arıkan, *Source polarization*, Proc. IEEE Int. Sympos. Inform. Theory, Austin, TX, 2010, pp. 899–903.

[7] S. B. Korada, *Polar codes for channel and source coding*, Ph.D. thesis, EPFL, 2009.

[8] R Mori and T. Tanaka, *Channel polarization on q-ary discrete memoryless channels by arbitrary kernels*, Proc. IEEE Int. Sympos. Inform. Theory, Austin, TX, 2010, pp. 894–898.

[9] W. Park and A. Barg, *Polar codes for q-ary channels, $q = 2^r$*, IEEE Trans. Inform. Theory **59** (2013), no. 2, 955–969.

[10] E. Şaşoğlu, E. Telatar, and E. Arıkan, *Polarization for arbitrary discrete memoryless channels*, arXiv:0908.0302, 2009.

[11] R. Mori and T. Tanaka, *Source and channel polarization over finite fields and Reed-Solomon matrices*, IEEE Trans. Inform. Theory, **60** (2014), no. 5, 2720–2736.

[12] A. G. Sahebi and S. S. Pradhan, *Multilevel channel polarization for arbitrary discrete memoryless channels*, IEEE Trans. Inform. Theory, **59** (2013), no. 12, 7839–7857.

[13] M. R. Bloch, L. Luzzi and J. Kliewer, *Strong coordination with polar codes*, Proc. 50th Annual Allerton Conf. on Comm., Control and Computing, 2012, pp. 565–571.

[14] E. Hof, I. Sason, and S. Shamai, *Polar coding for reliable communications over parallel channels*, Proc. IEEE Inform. Theory Workshop, Dublin, Ireland, 2010, pp. 1–5.

[15] E. Abbe and A. Barron, *Polar coding schemes for the AWGN channel*, Proc. IEEE Int. Sympos. Inform. Theory, St. Petersburg, Russia, 2011, pp. 194–198.

[16] A. G. Sahebi and S. S. Pradhan, *Polar codes for some multi-terminal communications problems*, Proc. IEEE Int. Sympos. Inform. Theory, Honolulu, HI 2014, pp. 316–320.

[17] H. Mahdavifar and A. Vardy, *Achieving the secrecy capacity of wiretap channels using polar codes*, IEEE Trans. Inform. Theory, **57** (2011), no. 10, 6428–6443.

[18] N. Goela, E. Abbe, M. Gastpar, *Polar codes for broadcast channels.* Proc. IEEE Int. Sympos. Inform. Theory, Istanbul, Turkey, 2013, pp. 1127–1131.

[19] E. Şaşoğlu, E. Telatar, E. M. Yeh. *Polar codes for the two-user multiple-access channel*, IEEE Trans. Inform. Theory **59** (2013), no. 10, 6583–6592.

[20] S.B. Korada, E. Şaşoğlu, R. Urbanke, *Polar codes: Characterization of exponent, bounds, and constructions*, IEEE Trans. Inform. Theory, **56** (2010), no. 12, 6253–6264.

[21] E. Arıkan and E. Telatar, *On the rate of channel polarization*, Proc. IEEE Int. Sympos. Inform. Theory , Seoul, Korea, 2009, pp. 1493–1495.

[22] S. B. Korada and R. Urbanke, *Polar codes are optimal for lossy source coding*, IEEE Trans. Inform. Theory, **56** (2010), no. 4, 1751–1768.

[23] I. Csiszár and J. Körner, *Information theory: Coding theorems for discrete memoryless systems*. Cambridge University Press, 2011.

[24] M. Mondelli, H. Hassani, I. Sason, and R. Urbanke, *Achieving Marton's Region for Broadcast Channels Using Polar Codes*, IEEE Trans. Inform. Theory **61** (2015), no. 2, 783–800.

[25] M. Ye and A. Barg, *Polar codes for distributed hierarchical source coding*, Advances in Math. of Comm., **9** (2015), no. 1, 87–103.

[26] L. Wang and E. Sasoglu, *Polar coding for interference networks*, Proc. IEEE Int. Sympos. Inform. Theory , Honolulu, HI, 2014, pp. 311–315.

[27] B. Nazar and M. Gastpar, *Computation over multiple-access channels*, IEEE Trans. Inform. Theory **53** (2007), no. 10, 3498–3516.

[28] O. Ayaso, D. Shah, and M. Daleh, *Information theoretic bounds for distributed computation over networks of point-to-point channels*, IEEE Trans. Inform. Theory **56** (2010), no. 12, 6020–6039.

[29] H. Chen, R. Cramer, S. Goldwasser, R. de Haan, and V. Vaikuntanathan, *Secure computation from random error correcting codes*, Eurocrypt 2007, Lecture Notes in Computer Science, vol. 4515, Spinger, 2007, pp. 291–310.

[30] H. Tyagi, P. Narayan, and P. Gupta, *When is the function securely computable?*, IEEE Trans. Inform. Theory **57** (2011), no. 10, 6337–6350.

[31] M. Braverman and A. Rao, *Towards coding for maximum errors in interactive communication*, Proc. 43rd Annual ACM Symposium on Theory of Computing (STOC '11), ACM, 2011, pp. 159–166.

[32] J. Körner and K. Marton, *How to encode the modulo-two sum of binary sources*, IEEE Trans. Inform. Theory **25** (1979), no. 2, 219–221.

[33] A. Orlitsky and J. R. Roche, *Coding for computing*, IEEE Trans. Inform. Theory **47** (2001), no. 3, 903–917.

[34] N. Ma and P. Ishwar, *Some results on distributed source coding for interactive function computation*, IEEE Trans. Inform. Theory **57** (2011), no. 9, 6180–6195.

[35] N. Ma, P. Ishwar and P. Gupta, *Interactive source coding for function computation in collocated networks*, IEEE Trans. Inform. Theory **59** (2012), no. 7, 4289–4305.

[36] T.C. Gülcü and A. Barg, *Interactive function computation via polar coding*, arXiv: 1405.0894, 2014.

[37] T.C. Gülcü and A. Barg, *Interactive function computation via polar coding*, Proc. 52nd Annual Allerton Conf. on Comm., Control and Computing, 2014, pp. 820–827.

[38] A. D. Wyner, *The wire-tap channel*, Bell Syst. Tech. J., vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[39] A. Thangaraj, S. Dihidar, A.R. Calderbank, S.W. McLaughlin, and J. Merolla, *Applications of LDPC codes to the wiretap channel*, IEEE Trans. Inform. Theory, **53** (2007), no. 8, 2933–2945.

[40] A. Suresh, A. Subramanian, A. Thangaraj, M. Bloch, and S.W. McLaughlin. *Strong security for erasure wiretap channels*, in Proc. IEEE Inform. Theory Workshop, Dublin, Ireland, 2010, pp. 1–5.

[41] E. Hof and S. Shamai, *Secrecy-achieving polar-coding*, Proc. IEEE Information Theory Workshop, Dublin, Ireland, Sept. 2010, pp. 1–5, Preprint arXiv:1005.2759, 2010.

[42] O. O. Köylüoğlu and H. El Gamal, *Polar coding for secure transmission and key agreement*, Proc. IEEE Int. Sympos. on Personal Indoor and Mobile Radio Communications (PIMRC), pp. 2698–2703, 2010.

[43] M. Andersson, V. Rathi, R. Thobaben, J. Kliewer, M. Skoglund, *Nested polar codes for wiretap and relay channels*, IEEE Communication Letters, no. 14, pp.752–754, 2010.

[44] U. M. Maurer, *The strong secret key rate of discrete random triples*, in Communication and Cryptography–Two Sides of One Tapestry, R. Blahut et al., Eds., Boston, MA, 1994, pp. 271–285.

[45] U. M. Maurer and S. Wolf, *Information-theoretic key agreement: From weak to strong secrecy for free*, in Lecture Notes in Computer Science, Berlin, Germany: Springer, 2000, vol. 1807, pp. 351–368.

[46] E. Şaşoğlu and A. Vardy. *A new polar coding scheme for strong security on wiretap channels.* Proc. IEEE Int. Sympos. Inform. Theory, Istanbul, Turkey, 2013, pp. 1117–1121.

[47] D. Sutter, J. M. Renes, R. Renner, *Efficient one-way secret-key agreement and private channel coding via polarization*, arXiv: 1304.3658v1, 2013.

[48] J. M. Renes and M. M. Wilde, *Polar codes for private and quantum communication over arbitrary channels*, IEEE Trans. Inform. Theory, **60** (2014). no. 6, 3090–3103.

[49] M. M. Wilde and J. M. Renes, *Polar codes for private classical communication*, Proc. IEEE Int. Sympos. Inform. Theory Appl., 2012, pp. 745–749.

[50] I. Csiszár and J. Körner, *Broadcast channels with confidential messages*, IEEE Trans. Inform. Theory, **24** (1978), no. 3, 339–348.

[51] T.C. Gülcü and A. Barg, *Achieving secrecy capacity of the wiretap channel and broadcast channel with a confidential component*, arXiv: 1410.3422, 2014.

[52] T.C Gülcü and A. Barg, *Achieving secrecy capacity of the wiretap channel and broadcast channel with a confidential component*, Proc. IEEE Inform. Theory Workshop, Jerusalem, Israel, 2015, pp. 1–5.

[53] R. A. Chou and M. R. Bloch, *Polar coding for the broadcast channel with confidential messages and constrained randomization*, Proc. IEEE Inform. Theory Workshop, Jerusalem, Israel, 2015. Preprint: arXiv:1411.0281, 2014.

[54] Y.-P. Wei and S. Ulukus, *Polar coding for the general wiretap channel*, Proc. IEEE Inform. Theory Workshop, Jerusalem, Israel, 2015. Preprint: arXiv:1410.3812, 2014.

[55] R. Mori and T. Tanaka, *Performance and construction of polar codes on symmetric binary-input memoryless channels*, Proc. IEEE Int. Sympos. Inform. Theory, Seoul, Korea, 2009, pp. 1496–1500.

[56] I. Tal and A. Vardy, *How to construct polar codes*, IEEE Trans. Inform. Theory **59** (2013), no. 10, 6562–6582.

[57] R. Pedarsani, S.H Hassani, I. Tal, E. Telatar, *On the construction of polar codes*, Proc. IEEE Int. Sympos. Inform. Theory, St. Peterburg, Russia, 2011, pp. 1–15.

[58] I. Tal, A. Sharov, A. Vardy, *Constructing polar codes for non-binary alphabets and MACs*, Proc. IEEE Int. Sympos. Inform. Theory, Boston, MA, 2012, pp. 2132–2136.

[59] U. Pereg and I. Tal, *Channel upgradation for non-binary input alphabets and MACs*, Proc. IEEE Int. Sympos. Inform. Theory, Honolulu, HI, 2014, pp. 411–415, arXiv: 1308.5793v3.

[60] I. Tal, *On the construction of polar codes for channels with moderate input alphabet sizes*, arXiv:1506.08370, 2015.

[61] T.C. Gülcü and A. Barg, *Polar code construction for arbitrary discrete memoryless channels*, preprint.

[62] T. Cover and J. A. Thomas, *Elements of information theory*, 2nd ed., J. Wiley & Sons, 2006.

[63] N. Ma and P. Ishwar, *The infinite-message limit of two-terminal interactive source coding*, IEEE Trans. Inform. Theory **59** (2013), no. 7, 4071–4094.

[64] L. H. Ozarow and A. D. Wyner, *Wire-Tap Channel II*, Bell Lab. Tech. Journal, **63** (1984), no. 10, 2135–2157.

[65] V. K. Wei, *Generalized Hamming weights of linear codes*, IEEE Trans. Inform. Theory, **37** (1991), no. 5, 1412–1418.

[66] M. Cheraghchi, F. Didier, and A. Shokrollahi, *Invertible extractors and wiretap protocols*, IEEE Trans. Inform. Theory, **58** (2012), no. 2, 1254–1274.

[67] M. Bellare, S. Tessaro, A. Vardy, *Semantic security for the wiretap channel* in Advances in Cryptology CRYPTO 2012, Lecture Notes in Computer Science, Vol. **7417**, pp. 294–311.

[68] R. Mori, *Properties and construction of polar codes*, Master's thesis, Kyoto University, arXiv:1002.3521, 2010.

[69] E. Şaşoğlu, *Polarization and Polar Codes*, Foundations and Trends in Communications and Information Theory 8, no. 4, 2012, 259–381.

[70] A. Ghayoori, and T.A. Gulliver, *Constructing polar codes using iterative bit-channel upgrading*, arXiv:1302.5153, 2013.

[71] A. Ghayoori, and T.A. Gulliver, *Upgraded approximation of non-binary alphabets for polar code construction*, arXiv:1304.1790, 2013.

[72] P. Trifonov, *Efficient design and decoding of polar codes*, IEEE Trans. on Comm., **60** (2012), no. 11, 3221–3227.

[73] H. Li and J. Yuan, *A practical construction method for polar codes in AWGN channels*, in TENCON Spring Conference, Sydney, Australia, 2013, pp. 223–226.

[74] D. Wu, Y. Li, Y. Sun, *Construction and block error rate analysis of polar codes over AWGN channel based on Gaussian approximation*, IEEE Comm. Letters, **18** (2014), no. 7, 1099–1102.

[75] H. Vangala, E. Viterbo and Y. Hong, *A comparative study of polar code constructions for the AWGN channel*, arXiv:1501.02473, 2015.

[76] D. Kern, S. Vorkoper, V. Kuhn, *A new code construction for polar codes using min-sum density*, 8th Int. Sympos. Turbo Codes and Iterative Information Processing, Bremen, Germany, 2014, pp. 228–232.

[77] G. Bonik, S. Goreinov, N. Zamarashkin, *Construction and analysis of polar and concatenated polar codes: practical approach*, arXiv:1207.4343, 2012.

[78] S. Zhao, P. Shi and B. Wang, *Designs of Bhattacharyya parameter in the construction of polar codes*, 7th Int. Conference Wireless Comm., Networking and Mobile Computing, Wuhan, China, 2011, pp. 1–4.

[79] A. Bravo-Santos, *Polar codes for the Rayleigh fading channel*, IEEE Comm. Letters, **17**(2013), no. 12, 2352–2355.

[80] K. Chen, K. Niu, J.R. Lin, *Practical polar code construction over parallel channels*, IET Comm., **7** (2013), no. 7, 620–627.

[81] E. Şaşoğlu, E. Telatar, E. Arıkan, *Polarization for arbitrary discrete memoryless channels*, Proc. IEEE Inform. Theory Workshop, Taormina, Italy, 2009, pp. 144–148.

[82] R. Nasser, *Ergodic theory meets polarization. I: An ergodic theory for binary operations*, arXiv:1406.2943, 2014.

[83] R. Nasser, *Ergodic theory meets polarization. II: A foundation of polarization theory*, arXiv: 1406.2949, 2014.

[84] E. Şaşoğlu, *Polar codes for discrete alphabets*, Proc. IEEE Int. Sympos. Inform. Theory, Boston, MA, 2012, pp. 2137–2141.