CHANNEL POLARIZATION WITH HIGHER-ORDER MEMORY

by

Hüseyin Afşer

M.S., Electrical and Electronics Engineering, Boğaziçi University, 2008

B.S., Electrical and Electronics Engineering, Boğaziçi University, 2006

Submitted to the Institute for Graduate Studies in
Science and Engineering in partial fulfillment of
the requirements for the degree of
Doctor of Philosophy

Graduate Program in Electrical and Electronics Engineering

Boğaziçi University

2015

ACKNOWLEDGEMENTS

I am very grateful to be advised by Prof. Hakan Deliç. His guidance and mentoring not only helped to finish my Ph.D study but also provided me knowledge, methodology and direction for my post Ph.D life. I consider myself lucky for working close with him, observing and sharing his perspective for academia, teaching and even common life events. This dissertation would not have been completed without his support and guidance.

I am also grateful to my friends at WCL. Without their friendship and joy I could not have found enough motivation to finish my dissertation.

I want to thank to Kıvanç Mıhçak for introducing me to information theory without him this dissertation would have been on something totally different.

Finally, I am grateful to Aselsan Elektronik A.Ş. for it's scholarship during my Ph.D education. This dissertation is also partially funded by Boğaziçi Research Fund (BAB) under the project 11A02D10.

ABSTRACT

CHANNEL POLARIZATION WITH HIGHER-ORDER MEMORY

Channel coding is one of the most fundamental problems regarding the nature of communication. Polar codes, developed by Arıkan, were the first demonstration of practical channel codes that provably achieve theoretical limits in a wide range of communication scenarios. Based on simple channel transformations which are called channel combining and splitting, Arıkan developed the idea of channel polarization which resulted in polar codes. In this dissertation we focus on the unique properties of polar codes and channel polarization. First, we investigate the channel-specific construction of polar codes, a point which discriminates polar codes from Reed-Muller (RM) codes. We obtain results showing the inherent effect of the underlying channel on the construction of polar codes and provide a bridge between polar and RM codes. Our results easily extend to obtaining a characterization for the rate of polarization as well. Next, we consider practical uses of polar codes for fading channels. We design a bit-interleaved polar-coded modulation scheme (BIPCM) by deriving a low complexity code-construction method and designing a lower complexity successive cancellation list decoder (SCLD). We compare the resultant BIPCM system with the existing solutions and show that it provides significant performance advantages. Finally, we generalize the channel polarization idea by changing channel combining and splitting operations. By introducing a memory order in the channel combining process we obtain a class of codes, including the original ones, that are parametrized by the memory order. We show that the new family of polar codes achieve the theoretical limits as well and they can also be used with lower complexity by increasing the memory order. We thereby complement Arıkan's conjecture that channel polarization is in fact a general phenomenon.

ÖZET

YÜKSEL DERECELİ KANAL KUTUPSALLAŞTIRMA

Kanal kodlama, doğası gereği haberleşmenin en temel problemlerinden biridir. Arıkan'ın geliştirdiği kutupsal kodlar, birçok haberleşme senaryosunda Shannon'ın belirlediği teorik limitlere ulaştığı matematiksel olarak gösterilmiş ilk kanal kodlarıdır. Arıkan, kanal kutuplaşma yöntemini kanal birleştirme ve kanal ayırma adında iki basit dönüşüm kullanarak geliştirmiş ve bu da kutupsal kodların bulunmasıyla sonuçlanmıştır. Kutupsal kodların başarısının bir kısmı da bu basitliğinden ve kanal kodlamanın neden işe yaradığını açıklayan yapısından kaynaklanmaktadır. Bu tezde kutupsal kodlara has özellikler üzerinde odaklandık. İlk olarak, kutupsal kodları Reed-Muller (RM) kodlardan ayıran özelliği olan haberleşme kanalına bağlı tasarlanmasını inceledik. Haberleşme sisteminin gerçeklendiği kanalın kutupsal kodların tasarımını nasıl değiştirdiğini gösteren sonuçlar elde ettik; böylelikle, kutupsal kodlar ve RM kodları arasında bir köprü sağladık. Elde ettiğimiz sonuçlar, kanal kutuplaşma hızını belirlemek için de kullanılabilir. Buna ek olarak, kutupsal kodların, sönümlü kanallarda pratik kullanımını inceledik. Düşük karmaşıklı bir kod oluşturma yöntemi geliştirerek ve yine düşük karmaşıklı bir listeli ardışık çözümleme yöntemi kullanarak bit-serpiştirmeli kutupsal-kodlamalı kipleme sistemi tasarladık. Bu sistemin varolan diğer çözümlerle performans kıyaslamasını yaptık ve önerilen sistemin önemli performans kazancı sağladığını gösterdik. Son olarak, kutupsal kodların temel yapıtaşı olan kanal birleştirme ve kanal ayırma yöntemlerini değiştirerek kutupsal kodları genelleştirdik. Kanal birleştirme işlemi içerisine bir hafıza derecesi ekleyerek, asıl kodların da içinde olduğu bir kod ailesi elde ettik. Bu kod ailesinin de teorik limitlere eriştiğini ve hafıza derecesini arttırarak daha düşük karmaşıklıkla kullanılabileceğini gösterdik. Böylelikle, Arıkan'ın, kanal kutupsallaşmasının aslında daha genel bir olgu olduğu varsayımını desteklemiş olduk.

TABLE OF CONTENTS

ACKNOWLEDGEMENTS iii
ABSTRACT iv
ÖZET v
LIST OF FIGURES ix
LIST OF TABLES xi
LIST OF SYMBOLS xii
LIST OF ACRONYMS/ABBREVIATIONS xiii
1. INTRODUCTION 1
1.1. The Problem of Reliable Communication 1
1.2. The History of Channel Coding 2
1.3. Polar Codes 4
1.4. Contribution of This Dissertation 4
1.5. Organization of This Dissertation 5
1.6. Preliminaries 6
2. POLAR CODES 10
2.1. Channel Combining 10
2.2. Channel Splitting 12
2.3. Code Construction 13
2.4. Decoding 14
2.5. Probabilistic Model 15
2.5.1. Polarization 17
2.5.2. Rate of Polarization 18
2.6. Complexity 19
3. ON THE CHANNEL-SPECIFIC CONSTRUCTION OF POLAR CODES . 21
3.1. Probabilistic Model 22
3.2. Effect of Hamming Weights on the Construction of Polar Codes 23
3.3. Effect of Hamming Weights on the Exponent of Polar Codes 27
3.4. Discussion 28
4. BIT-INTERLEAVED POLAR-CODED MODULATION 29

4.1. Introduction . . . 29
4.2. Channel Model . . . 30
4.3. Polar-Coded Modulation . . . 32
4.3.1. Code Construction . . . 33
4.3.2. Successive Cancellation List Decoding . . . 34
4.4. Simulation Results . . . 36
4.5. Discussion . . . 38
5. POLAR CODES WITH HIGHER ORDER MEMORY . . . 40
5.1. Motivation . . . 40
5.2. Recursive Channel Transformations . . . 42
5.2.1. Channel Combining . . . 42
5.2.2. Channel Ordering . . . 43
5.2.3. Channel Splitting . . . 48
5.2.4. Effects of Channel Combining and Splitting on the Symmetric Capacity . . . 50
5.3. Decoding . . . 51
5.4. Code-Length . . . 52
5.5. Code Construction . . . 53
5.6. Channel Polarization . . . 54
5.6.1. Probabilistic Model for Channel Evolution . . . 54
5.6.2. Polarization . . . 56
5.6.3. A Typicality Result . . . 59
5.6.4. Rate of Polarization . . . 62
5.7. Complexity and Sparsity . . . 67
5.7.1. Encoding and Decoding Complexity . . . 67
5.7.2. Sparsity . . . 68
5.8. Discussion . . . 69
6. CONCLUSION . . . 70
REFERENCES . . . 72
APPENDIX A: PROOFS . . . 76
A.1. Proof of Lemma 3.1 . . . 76

A.2. Proof of Proposition 5.2 77
A.3. Proof of Proposition 5.3 77
A.4. Proof of Proposition 5.5 78
A.5. Proof of Lemma 5.1 79
A.6. Proof of Lemma 5.2 80
A.7. Proof of Lemma 5.3 81
A.8. Proof of Lemma 5.4 83
A.9. Proof of Proposition 5.7 85
A.10.Proof of Lemma 5.5 85

LIST OF FIGURES

Figure 1.1. The basic communication problem where symbols $x \in \mathcal{X}$ are transmitted from a source but they received as $y \in \mathcal{Y}$ due to the uncertainties in the channel, W. 1

Figure 1.2. Channel coding problem. 2

Figure 2.1. Channel combining operation at level n. 11

Figure 2.2. Probabilistic model for the evolution of $W_n^{(i)}$ channels. 16

Figure 4.1. BIPCM system model. 32

Figure 4.2. Tree formation for SCLD. 35

Figure 4.3. Bit error rate performance of BIPCM with different mappings. . 36

Figure 4.4. Achievable rates of different mappings for 16-QAM. 37

Figure 4.5. Performance of RA and LDPC based BIPCM. Curves are taken from [28]. 38

Figure 5.1. Recursive construction of the vector channel W_n from W_{n-1} and $\hat{W}_{n-m}$. 44

Figure 5.2. State labeling procedure $\varphi_n : \mathcal{S}_{n-1} \to \mathcal{S}_n$. State vectors $\mathbf{s}_n^{(i)} \in \mathcal{S}_n$, are obtained by appending a new state $\{+, -, \bigstar\}$, to the vectors $\mathbf{s}_{n-1}^{(j)} \in \mathcal{S}_{n-1}$. 45

Figure 5.3. Possible state transitions observed between s_k and s_{k+1}, $k = 1, 2, \ldots, n$. 47

Figure 5.4. Transition probabilities of $W_n^{(i)}$ channels after combining and splitting W_{n-1} and $\bar{W}_{n-m}$. 49

Figure 5.5. Illustration of the evolution of $\{S_n\}$ as a tree for the case $m = 2$, where each branch is a state vector $\mathbf{s}_n \in \mathcal{S}_n$. 55

Figure 5.6. Achievable exponent, $\beta < p^+$, as scaled with m. 65

Figure 5.7. Upper bounds on P_e of $\{\mathcal{C}_n^{(m)}\}$ where transmission takes place over a BEC with capacity 0.5. Code-lengths are 1024 and 987 for $m = 2$ and $m = 1$, respectively. 66

Figure 5.8. Scaling of encoding and decoding complexities as m increases where N is chosen to be the code-length closest to $1 \times 10^4, 1 \times 10^6$. . . . 68

LIST OF TABLES

Table 4.1. Performance of BICM with different codes. 39

LIST OF SYMBOLS

$\{B_n\}$	Bernoulli process $\Pr(B_n = +) = \Pr(B_n = -) = 1/2$
$\mathbf{G}_n$	$N \times N$ encoding matrix
$\{I_n\}$	Symmetric capacity process, $I_n = I(K_n)$
$I_n^{(i)}$	Symmetric capacity of $W_n^{(i)}$
$I(W)$	Symmetric capacity of W
$J(W)$	Symmetric cut-off rate of W
$\{K_n\}$	Random Channel process, $K_n = B_1, B_2, \ldots, B_n$
$L_n^{(i)}$	Likelihood ratio for the input of $W_n^{(i)}$
n	Recursion level $n = 1, 2, \ldots$
N	Code-length at recursion level n
m	Memory order $m = 1, 2, \ldots$
$u_n^{(i)}$	Binary-input of $W_n^{(i)}$
W	Binary-input discrete-output channel $W : \mathcal{X} \to \mathcal{Y}$
$W(y\|x)$	Transition probabilities of channel W
W_n	Vector channel at recursion level n, $W_n : \mathcal{X}^N \to \mathcal{Y}^N$
$W_n^{(i)}$	Binary-input channel in W_n, $i \in \{1, 2, \ldots, N\}$
x	Binary input symbol $x \in \mathcal{X}$
y	Discrete output symbol $y \in \mathcal{Y}$
$Z(W)$	Bhattacharyya parameter of W
$Z_n^{(i)}$	Bhattacharyya parameter of $W_n^{(i)}$
$\{Z_n\}$	Bhattacharyya process, $Z_n = Z(K_n)$

LIST OF ACRONYMS/ABBREVIATIONS

BDMC	Binary-input discrete-output memoryless channel
BEC	Binary erasure channel
BIPCM	Bit-interleaved polar-coded modulation
CM	Coded-modulation
CRC	Cyclic-redundancy check
GL	Gray labeling
LDPC	Low-density parity check (codes)
ML	Maximum Likelihood (decoding)
RM	Reed-Muller (codes)
RS	Reed-Solomon (codes)
QAM	Quadrature amplitude modulation
RA	Repeat-accumulate (codes)
SCD	Successive cancellation decoding
SCLD	Successive cancellation list decoding
SNR	Signal to noise ratio
SP	Mapping by set partitioning

1. INTRODUCTION

1.1. The Problem of Reliable Communication

The communication problem can be described as finding efficient methods to send information from a source to a destination (sink) through a physical medium (channel). However, any physical medium, by nature, has some sort of uncertainty in itself and this undermines the act of communication. In order to provide reliable communication between the source and the sink, one needs to combat this uncertainty. Let us consider a simple scenario where a source transmits symbols, $x \in \mathcal{X}$, through a channel, W, but, due to the uncertainties in the channel, the transmitted symbols are received at the sink as, $y \in \mathcal{Y}$. In order to understand the communication problem, even in this basic setting, we need to quantify a rate $R \in [0, 1]$ which is the fraction of symbols $x \in \mathcal{X}$ that can be understood from the received ones, $y \in \mathcal{Y}$.

Figure 1.1. The basic communication problem where symbols $x \in \mathcal{X}$ are transmitted from a source but they received as $y \in \mathcal{Y}$ due to the uncertainties in the channel, W.

The area of modern communication starts with the seminal work of Shannon [1] where he formulates the problem of reliable communication in this basic setting and shows that for any channel, W, there exists a capacity, $I(W)$, such that for rates $R < I(W)$ reliable communication between the source and the sink is possible and for $R > I(W)$ one can not communicate reliably. This result implies that if the source needs to convey information through symbols, $x \in \mathcal{X}$, then it needs to send a group of them, $\mathbf{x}_N = (x_1, x_2, \ldots, x_N)$, and looking through the received symbols, the sink can recover RN, $R < I(W)$, of them correctly. Moreover, the sink and the source need to agree a on a protocol beforehand such that first, the sink creates an information vector $\mathbf{u}_k$, $k/N = R$; next, by adding redundancy to $\mathbf{u}_k$ the source generates and transmits $\mathbf{x}_N$ and from the received symbols, $\mathbf{y}_N$, the sink can recover $\mathbf{u}_k$ reliably. Channel coding deals with the problem of finding such protocols.

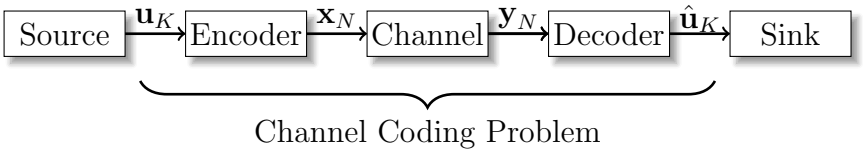

Figure 1.2. Channel coding problem.

The channel coding problem is illustrated in the above figure where the source uses an encoder to add redundancy to an information vector, $\mathbf{u}_k$, to generate a vector of encoded symbols, $\mathbf{x}_N$. After transmission through the channel the sink uses a decoder on the received symbols, $\mathbf{y}_N$, to obtain the estimate, $\hat{\mathbf{u}}_K$, of $\mathbf{u}_K$.

1.2. The History of Channel Coding

Channel coding problem arises with Shannon [1] in 1948 where he introduces and formulates the channel capacity and shows the existence of channel coding schemes that achieve this capacity. After the introduction of the channel coding problem the initial research was algebraic in nature where the main focus was to find encoders such that the minimum distance between the information vectors, $\mathbf{u}_k$, when they are encoded as $\mathbf{x}_N$ is maximized. On the receiver side a decoder with hard decisions was usually the preferred method. In decoding with hard decision, the decoder first maps the received symbols, $y \in \mathcal{Y}$, to the most likely transmitted ones, $x \in \mathcal{X}$, and obtains an estimate, $\hat{\mathbf{x}}_N$, on $\mathbf{x}_N$. Next, it employs maximum likelihood (ML) decoding by trying every $\mathbf{u}_k$ to find the most likely one that will result in $\hat{\mathbf{x}}_N$ hoping that the minimum distance between different $\hat{\mathbf{x}}_N$ will help recovery. Many different coding schemes such as Hamming [2], Golay, [3], Reed-Muller (RM) [4] and Reed-Solomon (RS) [5] are the results of this approach. The performance of this codes are not optimal as they can only be used with small code-lengths, N, because the decoder needs to employ ML decoding whose complexity increases exponentially in N.

Decoding with soft decisions was the next milestone for the channel coding problem. While employing soft decisions the decoder does not initially maps the received symbols, $y \in \mathcal{Y}$, to the most likely transmitted ones, $x \in \mathcal{X}$, but it uses ML decoding to estimate a group of symbols whose size is determined with a constraint length.

Viterbi [6] and BCJR [7] algorithms are the most famous of such decoding schemes that are shown to provide good performance with convolution codes, a class of codes whose encoding operation is performed by convolving the information vector, $\mathbf{u}_k$, with a fixed vector to obtain $\mathbf{x}_N$. Unfortunately, the complexity of such decoding schemes also increase exponentially in the constraint length.

Another class of decoding algorithms that are known as sequential decoding had a similar problem. When used with convolution codes these decoding algorithms are shown to have a bounded decoding complexity if the transmission rate, R, is below a critical rate and have exponential complexity above it. This critical rate is mathematically formulated and known, in the literature, as the "cut-off rate" [8]. Fano [9] and Wozencraft [8] are the well known pioneers of these class of decoding algorithms that draw attention due to having bounded complexity although not being able to provide near capacity operation.

Next major breakthrough in the history of channel coding comes with the introduction of Turbo codes [10] by Berrou, Glavieux and Thitimajshime in 1993. Turbo codes was the first example of channel codes that operate near capacity with complexity linear in the code-length. The demonstration of turbo codes broke the paradigm that operation above cut-off rate was difficult and provided hope and direction for future research on the channel coding problem.

In 2001, with the re-discovery of Gallager's low-density parity check (LDPC) codes, it was possible to approach the capacity of Gaussian channels within 0.0045db [11] with linear complexity. As it turns out, Gallager introduced LDPC codes in 1962 [12] and provided a low complexity decoding algorithm but could not demonstrate its operation due to lack of computational resources. LDPC codes provided the first example of channel codes operating at the channel capacity with linear complexity. But, it was the introduction of polar codes by Arıkan [13] in 2008 that provided the first example of a channel code that provably achieves the capacity of a wide range of communication channels with linear complexity in the code-length.

1.3. Polar Codes

In 2006 Arıkan proposed a channel transformation method based on channel combining and splitting [14]. This transformation took two uses of an arbitrary binary-input discrete output channel (BDMC), W, as an argument and output two synthesized channels, W' and W'', such that the sum cut-off rate of W' and W'' was larger than that of two W channels combined. This attempt was motivated by solving the cut-off phenomena that exists in the sequential decoding because these decoding algorithms have unbounded complexity above the cut-off rate. Later on, in 2008, Arıkan generalized the channel combining and splitting idea via recursive operations and this resulted in the channel polarization [13]. With channel polarization, it was possible to obtain code-sequences, $\{\mathcal{C}_n : n \geq 1\}$, called polar codes, having code-length $N = 2^n$ and complexity $O(N \log N)$. Arıkan showed that $\{\mathcal{C}_n : n \geq 1\}$ achieves the capacity of arbitrary BDMCs. With polar codes, 60 years after the introduction of the channel coding problem we finally had a rigorous solution along with a practical code that will allow reliable communication.

Interestingly, polar codes have the same encoding structure of a class of RM codes which are known and used for over 50 years [15]. Different from RM codes, polar codes have a channel-specific construction and can achieve the capacity of arbitrary BDMCs with a sub-optimal decoders such as successive cancellation decoder (SCD). These unique properties resulted in the popularity of polar codes.

1.4. Contribution of This Dissertation

Most of this dissertation focuses on the theoretical aspects of polar codes and channel polarization but, for the sake of completeness, we consider some practical uses of polar codes as well. Our contributions in the area of polar coding can be classified in three categorizes

(i) We investigate the channel-specific construction of polar codes and obtain asymptotic results which explain the inherent effect of the underlying channel on the

construction of polar codes. Our results bring lights on the constructional similarities and differences between polar and RM codes and they easily extend to provide a characterization for the asymptotic polarization performance of polar codes. These results are presented in Chapter 3.

(ii) We consider practical uses of polar codes for fading channels. By providing an easy construction method, we design a high performance and low complexity bit-interleaved polar-coding (BIPCM) scheme. We compare the performance of the proposed scheme with the existing ones and show that BIPCM provides significant performance advantages. This is explained in Chapter 4.

(iii) We generalize the channel polarization idea by introducing higher order memory in the channel combining and splitting operations. The newly introduced memory parameter allows us to control the speed of polarization as well as the speed of code-length. Channel polarization with higher order memory results in a new family of polar codes $\{\mathcal{C}_n^{(m)} : n \geq 1, m \geq 1\}$ with code-length $O(\phi^n)$, $\phi \in (1, 2]$, and memory parameter m. We prove that $\{\mathcal{C}_n^{(m)}\}$ achieves the capacity of arbitrary BDMCs for any fixed m and we obtain bounds on its asymptotic polarization performance as scaled with m. When $m = 1$, $\{\mathcal{C}_n^{(m)}\}$ coincides with the polar codes presented by Arıkan and as m increases the encoding and decoding complexities of $\{\mathcal{C}_n^{(m)}\}$ decrease. $\{\mathcal{C}_n^{(m)}\}$ is the first example of a new family of polar codes that require lower complexity compared to the original codes presented by Arıkan. Our results are presented in Chapter 5.

1.5. Organization of This Dissertation

In Chapter 2 we overview polar codes and channel polarization. Chapters 3, 4 and 5 are devoted to explaining our contributions in the area of polar coding, as summarized in the previous section. In Chapter 6 we conclude the dissertation and provide some future research directions. .

1.6. Preliminaries

Let $W(y|x)$, $x \in \mathcal{X} = \{0,1\}$, $y \in \mathcal{Y}$, denote the transition probabilities of W, where $\mathcal{X}$ is the binary-input alphabet and $\mathcal{Y}$ is an arbitrary discrete output alphabet. Throughout this dissertation we assume that x is uniformly distributed in $\mathcal{X}$, and use base-2 logarithm. The symmetric capacity, $I(W)$, of W is

$$I(W) \triangleq \sum_{y\in\mathcal{Y}} \sum_{x\in\mathcal{X}} \frac{1}{2} W(y|x) \log \frac{W(y|x)}{\frac{1}{2}W(y|0) + \frac{1}{2}W(y|1)}. \tag{1.1}$$

The Bhattacharyya parameter, $Z(W)$, of W provides an upper bound on the probability of error for maximum likelihood (ML) decoding over W and is defined as

$$Z(W) \triangleq \sum_{y\in\mathcal{Y}} \sqrt{W(y|0)W(y|1)}. \tag{1.2}$$

The symmetric cut-off rate, $J(W)$, of W is [13]

$$J(W) \triangleq \log \frac{2}{1+Z(W)}. \tag{1.3}$$

As Arıkan shows in [13, Prop. 1] $Z(W) = 1$ implies $I(W) = 0$ and $Z(W) = 0$ implies $I(W) = 1$. By using this fact and from (1.3) we see that if $J(W) = 0$ then $I(W) = 0$ holds and $J(W) = 1$ indicates $I(W) = 1$.

Let W' and W'' be two B-DMCs with inputs $x_1, x_2 \in \mathcal{X}$ and outputs $y_1 \in \mathcal{Y}_1$ and $y_2 \in \mathcal{Y}_2$, respectively. Channel polarization is based on a single-step channel transformation where one first combines the inputs of W' and W'' to obtain a vector channel

$$W(y_1, y_2|x_1, x_2) = W'(y_1|x_1 \oplus x_2)W''(y_2|x_2), \tag{1.4}$$

where $\oplus$ is the XOR operation. Next, by choosing a channel ordering, one splits the vector channel to obtain two new binary-input channels, $W^- : \mathcal{X} \to \mathcal{Y}_1 \times \mathcal{Y}_2$ and

$W^+ : \mathcal{X} \to \mathcal{X} \times \mathcal{Y}_1 \times \mathcal{Y}_2$, with transition probabilities

$$W^-(y_1, y_2|x_1) = \sum_{x_2} \frac{1}{2} W'(y_1|x_1 \oplus x_2) W''(y_2|x_2), \tag{1.5}$$

$$W^+(y_1, y_2, x_1|x_2) = \frac{1}{2} W'(y_1|x_1 \oplus x_2) W''(y_2|x_2), \tag{1.6}$$

We use the following short-hand notations for the transforms in (1.5) and (1.6), respectively.

$$W^- = W' \boxminus W'', \tag{1.7}$$

$$W^+ = W' \boxplus W''. \tag{1.8}$$

The polarization transforms preserve the symmetric capacity as

$$I(W^-) + I(W^+) = I(W') + I(W''), \tag{1.9}$$

and they help polarization by creating disparities in $I(W^+)$ and $I(W^-)$ such that

$$I(W^+) \geq \max\{I(W'), I(W'')\}, \tag{1.10}$$

$$I(W^-) \leq \min\{I(W'), I(W'')\}, \tag{1.11}$$

where the above inequalities are strict as long as $I(W') \in (0, 1)$ and $I(W'') \in (0, 1)$. This polarization effect quantitatively observed in the Bhattacharyya parameters as they take the form

$$Z(W^+) = Z(W')Z(W''), \tag{1.12}$$

$$Z(W^-) \leq Z(W') + Z(W'') - Z(W')Z(W''), \tag{1.13}$$

where the equality in (1.13) is achieved if $Z(W') \in \{0, 1\}$ or $Z(W'') \in \{0, 1\}$, or if W' and W'' are binary erasure channels (BECs).

Equations (1.9)-(1.13) are proved in [13] when W' is identical to W''. Their generalizations for the case W' and W'' are different channels are straightforward and omitted. The proposition below will be crucial in the sequel.

Proposition 1.1.

$$J(W^-) + J(W^+) \geq J(W') + J(W''),$$

where equality is achieved only if $J(W') \in \{0, 1\}$ *or* $J(W'') \in \{0, 1\}$.

Proof. We have $J(W^-) = \frac{2}{1+Z(W^-)}$ and $J(W^+) = \frac{2}{1+Z(W^+)}$. By using (1.13) and (1.12) we obtain

$$\begin{aligned} J(W^+) + J(W^-) &\geq \log \frac{2}{1 + Z(W')Z(W'')} + \\ &\log \frac{2}{1 + Z(W') + Z(W'') - Z(W')Z(W'')} \\ &= \log \frac{2}{1+Z(W')+Z(W'') + w(W', W'')Z(W')Z(W'')} \end{aligned} \tag{1.14}$$

where $w(W', W'') = Z(W') + Z(W'') - Z(W')Z(W'') \leq 1$ indicating

$$\begin{aligned} J(W^+) + J(W^-) &\geq \log \frac{2}{1 + Z(W')} + \log \frac{2}{1 + Z(W'')} \\ &= J(W') + J(W''). \end{aligned} \tag{1.15}$$

In order to have $J(W^+) + J(W^-) = J(W') + J(W'')$, the equalities in (1.14) and (1.15) must be achieved. From (1.13) we know that the equality in (1.14) is achieved only if $Z(W') \in \{0, 1\}$ or $Z(W'') \in \{0, 1\}$ or if W' and W'' are BECs. When $(Z(W'), Z(W'')) \in (0, 1)^2$ we have $w(W', W'') < 1$ and the inequality in (1.15) is always strict, whether or not W' and W'' being BECs. Consider the case $Z(W') = 1$ or $Z(W'') = 1$, then we have $w(W', W'') = 1$ and the equalities in (1.14) and (1.15) are achieved. When $Z(W') = 0$ we have $J(W') = 1$, $w(W', W'') = 0$ and $J(W^+) + J(W^-) = J(W') + J(W'')$, and the case $J(W') = 1$ follows from the symmetry in (1.14) and (1.15). Hence the equalities in (1.14) and (1.15) are both achieved

only if $Z(W') \in \{0,1\}$ or $Z(W'') \in \{0,1\}$, or alternatively only if $J(W') \in \{0,1\}$ or $J(W'') \in \{0,1\}$. □

The above proposition indicates that one can obtain a coding gain by applying channel combining and splitting operation as long as the symmetric cut-off rate of W' and W'' are in $(0,1)$, where the coding gain manifests itself as an increase in the sum cut-off rate of channels W^- and W^- compared to W' and W^+. We use the parameters $J(W)$ and $I(W)$ together to show that $\{\mathcal{C}_n^{(m)}\}$ achieves $I(W)$ of an arbitrary W, whereas the parameter $Z(W)$ will be used to characterize polarization performance of $\{\mathcal{C}_n^{(m)}\}$.

Notation: We use uppercase letter A, B for random variables and lower cases a, b for their realizations taking values from sets $\mathcal{A}$, $\mathcal{B}$, where the sets have sizes $|\mathcal{A}|$ and $|\mathcal{B}|$ respectively. $\Pr(a)$ denotes the probability of the event $A = a$. We write $\mathbf{a}_n = (a_1, a_2, \ldots, a_n)$ to denote a vector and $(\mathbf{a}_n, \mathbf{b}_n)$ to denote the concatenation of $\mathbf{a}_n$ and $\mathbf{b}_n$. We use standard Landau notation $o(n), O(N)$ to denote the limiting values of functions.

2. POLAR CODES

In this chapter we overview the construction, encoding and decoding of Arıkan's polar codes. We investigate the probabilistic model used for explaining the channel polarization phenomena and by using this model we characterize the asymptotic polarization performance of polar codes. The results in this chapter are mostly based on the works of Arıkan in [13].

2.1. Channel Combining

Consider a BDMC, $W(y|x)$, with binary-input $x \in \mathcal{X} = \{0, 1\}$ and arbitrary discrete output $y \in \mathcal{Y}$. Let $W(y_i|x_i)$ denote the ith use of the channel W. Channel combining phase consists of generating a vector channel $W_n : \mathcal{X}^N \to \mathcal{Y}^N$, $N = 2^n$, $n = 1, 2, \ldots$. Clearly, there are N different binary-input channels in the vector channel W_n to transmit information. In order to refer to these, let us define

$$W_n^{(i)} \stackrel{\Delta}{=} i\text{th binary-input channel in } W_n,$$

and

$$u_n^{(i)} \stackrel{\Delta}{=} \text{Binary-input of } W_n^{(i)}.$$

The vector channel W_n is obtained by combining the inputs of W_{n-1} and $\bar{W}_{n-1}$ where $\bar{W}_{n-1}$ denotes an independent realization of W_{n-1} and channel combining recursion starts with $W_0 = W$. The input combining is performed as

$$\begin{aligned} u_n^{(i)} &= u_{n-1}^{(i)} \oplus \bar{u}_{n-1}^{(i)}, \\ u_n^{(i+N/2)} &= \bar{u}_{n-1}^{(i)}, \end{aligned} \qquad i = 1, 2, \ldots, N/2,$$

where we use the notation $\bar{u}_{n-1}^{(i)}$ to denote the binary-input of $\bar{W}_{n-1}$. This combining process is demonstrated in Fig. 2.1. Let $\mathbf{u}_N = (u_1, u_2, \ldots, u_N)$ denote the information

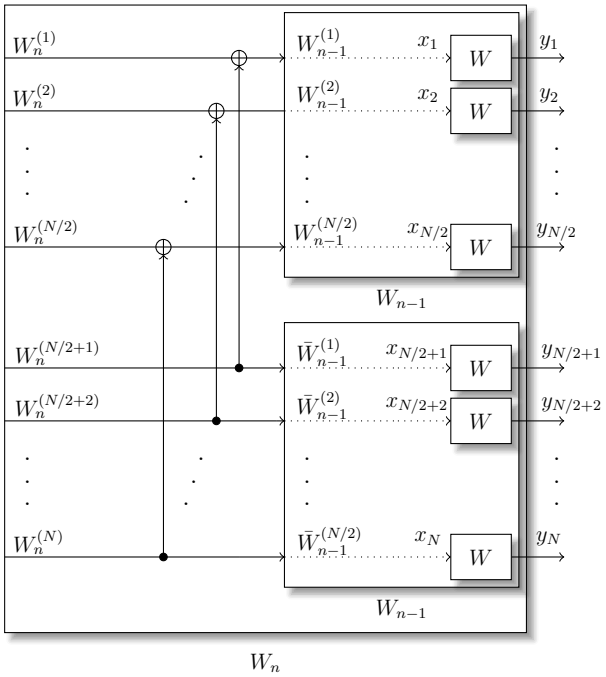

Figure 2.1. Channel combining operation at level n.

vector so that $u_1, u_2, \ldots, u_N$ are transmitted through the inputs of $W_n^{(1)}, W_n^{(2)}, \ldots, W_n^{(N)}$, respectively. We can formulate the encoding operation which maps the information vector, $\mathbf{u}_N$, to encoded bits, $\mathbf{x}_N$, as

$$\mathbf{x}_N = \mathbf{u}_N \mathbf{G}_n, \tag{2.1}$$

where $\mathbf{G}_n$ is an $N \times N$, $N = 2^n$, encoding matrix and encoding operation is performed in GF(2). Inspecting Fig. 2.1 we see that $\mathbf{G}_n$, in particular, is of the form

$$\mathbf{G}_n = \begin{bmatrix} \mathbf{G}_{n-1} & 0 \\ \mathbf{G}_{n-1} & \mathbf{G}_{n-1} \end{bmatrix} = \mathbf{F} \otimes \mathbf{G}_{n-1},$$

where $\mathbf{F} = \mathbf{G}_1 = \left[\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right]$ and $\otimes$ denotes the Kronecker product. We can alternatively respresent $\mathbf{G}_n$ as $\mathbf{G}_n = \underbrace{\mathbf{F} \otimes \mathbf{F} \otimes \ldots \mathbf{F}}_{n \text{ times}} = \mathbf{F}^{\otimes n}$.

2.2. Channel Splitting

Channel splitting is the operation of separating $W_n : \mathcal{X}^N \to \mathcal{Y}^N$, $N = 2^n$, and obtaining N synthesized binary-input channels. In order to split W_n we need to define a splitting order $\pi_n : \{1, 2, \ldots, N\} \to \{1, 2, \ldots, N\}$ which we explain in the following definition.

Definition 2.1. *Bit-reversed Order: Let* $\pi_n : \{1, 2, \ldots, N\} \to \{1, 2, \ldots, N\}$ *and let* $\mathbb{B}(i) = (b_1, b_2, \ldots, b_n)_2 + 1$, $i = 1, 2, \ldots, N$, *denote the* n*-bit binary expansion of* i *where* b_n *is taken as the most significant bit. The mapping* π_n *is obtained in terms of increasing* $\mathbb{B}(i)$ *values such that if* $\mathbb{B}(i) > \mathbb{B}(j)$ *then* $\pi_n(i) > \pi_n(j)$.

The mapping π_n is the so-called bit-reversed order presented by Arıkan [13]. The binary-input channels $W_n^{(i)}$ in W_n are split in increasing π_n values so that each $W_n^{(i)}$ is of the form $W_n^{(i)} : \mathcal{X} \to \mathcal{Y}^N \times \mathcal{X}^{\pi_n(i)-1}$. The transition probabilities of $W_n^{(i)}$ channels are explained with the following proposition.

Proposition 2.1. *For* $n \geq 1$ *the transition probabilities associated with* $W_n^{(i)}$ *can be recursively calculated as*

$$\begin{aligned} W_n^{(i)} &= W_{n-1}^{(i)} \boxminus \bar{W}_{n-1}^{(i)}, \\ W_n^{(i+N/2)} &= W_{n-1}^{(i)} \boxplus \bar{W}_{n-1}^{(i)}, \end{aligned} \qquad i = 1, 2, \ldots, N/2, \tag{2.2}$$

where $W_0 = W$ *is the underlying channel.*

Proof. For $n \geq 1$, let $\mathbb{B}(i) = (b_1, b_2, \ldots, b_{n-1})_2$, $i = 1, 2, \ldots, N/2$. We have $\mathbb{B}(i) = (b_1, b_2, \ldots, b_{n-1}, 0)_2$ and $\mathbb{B}(i + N/2) = (b_1, b_2, \ldots, b_{n-1}, 1)_2$. Therefore, $W_n^{(i)}$ precedes $W_n^{(i+N/2)}$ in terms of the bit-reversed order π_n. Since $u_n^{(i)} = u_{n-1}^{(i)} \oplus \bar{u}_{n-1}^{(i)}$ and $u_n^{(i+N/2)} = \bar{u}_{n-1}^{(i)}$ holds by the channel combining procedure, induction through stages $1, 2, \ldots, n$ indicates that $W_n^{(i)} = W_{n-1}^{(i)} \boxminus \bar{W}_{n-1}^{(i)}$ and $W_n^{(i+N/2)} = W_{n-1}^{(i)} \boxplus \bar{W}_{n-1}^{(i)}$ hold. □

2.3. Code Construction

In order to use polar codes one has to fix a code parameter vector $(W, N, K, \mathcal{A})$, where W is the underlying B-DMC, N is the code-length, K is the dimensionality of the code, and $\mathcal{A} \subseteq \{1, 2, \ldots, N\}$ is the set of information carrying symbols. We have $|\mathcal{A}| = K$ and $K/N = R$, where $R \in [0, 1]$ is the rate of the code.

Let $Z_n^{(i)}$ denote the Bhattacharyya parameter of $W_n^{(i)}$ channel. Code construction problem is choosing the set $\mathcal{A}$ such that

$$\text{minimize} \sum_{i \in \mathcal{A}} Z_n^{(i)}, \quad \text{subject to} \quad \frac{|A|}{N} = R \tag{2.3}$$

This problem can be analytically solved only when W is a BEC since for this case the $W_n^{(i)}$ channels are also BECs [13] and the Bhattacharyya terms, $Z_n^{(i)}$, can be calculated in closed form. In this case, in the light of (1.12)-(1.13) and Proposition 2.1, $Z_n^{(i)}$ terms can be recursively calculated as

$$\begin{aligned} Z_n^{(i)} &= 2Z_{n-1}^{(j)} - (Z_{n-1}^{(j)})^2, \\ Z_n^{(i+N/2)} &= (Z_{n-1}^{(i)})^2, \end{aligned} \qquad i = 1, 2, \ldots, N/2. \tag{2.4}$$

No other recursive calculation are known for channels other than BEC. This brings a code construction problem for polar codes because calculating a suitable reliability metric for channel $W_n^{(i)} : \mathcal{X} \to \mathcal{Y}^N \times \mathcal{X}^{\pi_n(i)-1}$ has complexity exponential in the code-length. This results from the fact that the output alphabet size of $W_n^{(i)}$ i.e. $|\mathcal{Y}^N \times \mathcal{X}^{\pi_n(i)-1}|$ increases exponentially in the code-length N. This problem is well-studied in the literature, where one approximates a suitable reliability measure for $W_n^{(i)}$ channels and uses this measure to choose the set $\mathcal{A}$. We refer the reader to [16] for an overview.

After choosing the set $\mathcal{A}$ one only uses $W_n^{(i)}$ channels with $i \in \mathcal{A}$ while the remaining channel are not used for transmission and their inputs are kept frozen and

known to the decoder. Let $\mathbf{u}_A = (u_i : i \in \mathcal{A})$ and $\mathbf{u}_{A^c} = (u_i : i \in \mathcal{A}^c)$ denote the vector of information and frozen bits, respectively. The encoding operation, in particular, is of the form

$$\begin{aligned} \mathbf{x}_N &= \mathbf{u}_N \mathbf{G}_n, \\ &= \mathbf{u}_{\mathcal{A}} \mathbf{G}_n(A) \oplus \mathbf{u}_{\mathcal{A}^c} \mathbf{G}_n(\mathcal{A}^c), \end{aligned}$$

where $G_n(A)$ is the matrix obtained by choosing the rows of $\mathbf{G}_n$ with indices in $\mathcal{A}$. The above encoding structure is the same as a class of RM codes, known for 50 years. The distinction being for RM codes the set $\mathcal{A}$ is selected as

$$\text{maximize} \sum_{i \in \mathcal{A}} H_n^{(i)}, \quad s.t. \quad \frac{|A|}{N} = R \tag{2.5}$$

where $H_n^{(i)}$ denotes the Hamming weight of the ith row of $\mathbf{G}_n$. The distinction between polar and RM codes lies in the selection of the set $\mathcal{A}$ in the sense that RM codes are constructed independently of the underlying channel whereas polar codes are channel-specific codes. This results from the fact that $Z_n^{(i)}$ terms depend on the underlying channel. However, one expects $H_n^{(i)}$ to have some effect on $Z_n^{(i)}$ as well because, from coding perspective, choosing large $H_n^{(i)}$ results in a larger minimum distance on codewords. We bring some light on this discussion in Chapter 3 by showing that the Hamming weights, $H_n^{(i)}$, also have some effect on $Z_n^{(i)}$ because, as it turns out, asymptotically some $Z_n^{(i)}$ depend more on the corresponding $H_n^{(i)}$ and the fraction of those $Z_n^{(i)}$ increases in $I(W)$.

2.4. Decoding

The default decoding algorithm for polar codes, as Arıkan suggests in [13], is the successive cancellation decoding (SCD). SCD directly follows from the channel splitting procedure and the recursive formulation of the transition probabilities of $W_n^{(i)}$ channels,

as given by Proposition 2.1. In order to explain SCD let us define

$$W_n^{(i)}(x) \triangleq \text{ The posterior probability of transmitting } x \in \mathcal{X} \text{ from the input of } W_n^{(i)}.$$

Likelihood ratio (LR), $L_n^{(i)}$, for the input of the channel, $W_n^{(i)}$, is defined as

$$L_n^{(i)} \triangleq \frac{W_n^{(i)}(0)}{W_n^{(i)}(1)}.$$

Representing the transition probabilities of $W_n^{(i)}$ recursively via $\boxminus$ and $\boxplus$ transforms, as in Proposition 2.1, allows us to recursively calculate LR relations as well. This results from the fact that the effect of $\boxminus$ and $\boxplus$ on LR relations can be formulated in closed form [13, Eqs. 74-75]. By using this fact we obtain

$$\begin{aligned} L_n^{(i)} &= \frac{L_n^{(i)}\bar{L}_{n-1}^{(i)} + 1}{L_{n-1}^{(i)} + \bar{L}_{n-1}^{(i)}}, \\ L_n^{(i+N/2)} &= L_{n-1}^{(i)}.(\bar{L}_{n-1}^{(i)})^{1-2\hat{u}_n^{(i)}}, \end{aligned} \qquad i = 1, 2, \ldots, N/2, \tag{2.6}$$

where $\bar{L}_{n-1}^{(i)}$ is the LR of $\bar{W}_n^{(i)}$ channel and $\hat{u}_n^{(i)}$ denotes the estimate of $u_n^{(i)}$. SCD algorithm for polar codes is based on calculating $L_n^{(i)}$ values recursively with the above relations, in the order $\pi_n(i) = 1, 2, \ldots, N$, and deciding on the estimates $\hat{u}_n^{(i)}$ by using

$$\hat{u}_n^{(i)} = \begin{cases} 0 & \text{if} \quad L_n^{(i)} \geq 1, \\ 1 & \text{otherwise}, \end{cases} \tag{2.7}$$

where only the decisions on $u_n^{(i)}$, $i \in \mathcal{A}$, are made since the remaining $u_n^{(i)}$ are fixed at the encoder side and known at the decoder.

2.5. Probabilistic Model

Recursive formulation of the transition probabilities of $W_n^{(i)}$ also allows one to obtain a probabilistic model for their evolution. In order to explain this let us define

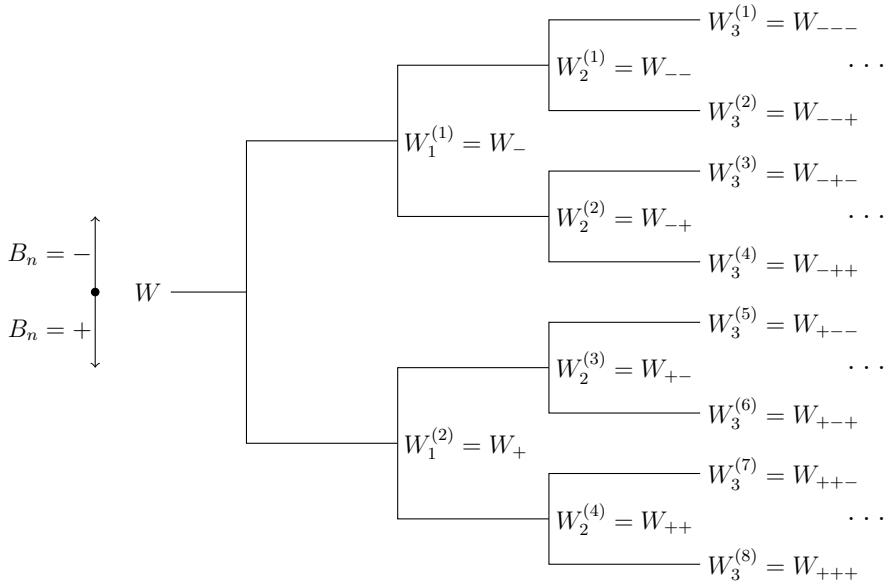

Figure 2.2. Probabilistic model for the evolution of $W_n^{(i)}$ channels.

a random channel process $\{K_n : n \geq 1\}$ where $K_n = W_{B_1,B_2,\ldots,B_n}$, $B_i \in \{+,-\}$, $i = 1, 2, \ldots, n$, and $\Pr(B_i = +) = \Pr(B_i = -) = 1/2$. As Arıkan shows in [13], we can view $\{K_n\}$ as a tree process where its realizations correspond to $W_n^{(i)}$ channels where each different realization occurs with probability $1/2^n = 1/N$. This is illustrated in Fig. 2.5 By using Proposition 2.1 and the definition of the bit-reversed order in Definition 2.1 the process $\{K_n\}$ can be formulated as

$$K_n = \begin{cases} K_{n-1} \boxminus K_{n-1}, & \text{if} \quad B_n = -, \\ K_{n-1} \boxplus K_{n-1}, & \text{if} \quad B_n = +, \end{cases} \tag{2.8}$$

where $K_0 = W$ is the underlying channel. Next, define the process $\{Z_n : n \geq 1\}$ where $Z_n = Z(K_n)$ is the Bhattacharyya parameter of K_n. By using the above recursive formulation and (1.12)-(1.13) we can formulate Z_n as

$$Z_n \begin{cases} \leq 2Z_{n-1} - Z_{n-1}^2, & \text{if} \quad B_n = -, \\ = Z_{n-1}^2, & \text{if} \quad B_n = +, \end{cases} \tag{2.9}$$

where $Z_0 = Z(W)$.

2.5.1. Polarization

We define the process $\{I_n : n \geq 1\}$, where $I_n = I(K_n)$ is the symmetric capacity of K_n. From the fact that $\boxplus$ and $\boxminus$ transforms preserves the symmetric capacity and from the random channel model in (2.8) we obtain

$$E[I_n] = \frac{1}{2}(I_{n-1} + I_{n-1}) = I_{n-1}. \tag{2.10}$$

Therefore, the process $\{I_n\}$ is martingale. Continuing the above recursion we notice that $E[I_n] = I_0 = I(W)$. Since I_n is bounded in $[0, 1]$ the Martingale convergence theorem states that it must converge to a random variable I_∞ with probability 1. A similar treatment applies to the process $\{Z_n\}$ since from (2.9) we have

$$E[Z_n] \leq \frac{1}{2}(2Z_{n-1} - Z_{n-1}^2 + Z_{n-1}^2) = Z_{n-1}, \tag{2.11}$$

indicating $\{Z_n\}$ is also a martingale and it must converge to a random variable Z_∞ with probability 1. Next, we see that

$$E[Z_n - Z_{n-1}] \geq \frac{1}{2}E[Z_{n-1}^2 - Z_{n-1}] = E[Z_{n-1}(1 - Z_{n-1})] \tag{2.12}$$

Since convergence in probability implies convergence in expectation we must have $E[Z_n - Z_{n-1}] \to 0$ as $n \to \infty$. By using this fact in the above relation we obtain $E[Z_\infty(1 - Z_\infty] = 0$ which, in turn, means $Z_\infty \in \{0, 1\}$. This result also indicates $I_\infty \in \{0, 1\}$ ([13, Prop. 1]) and having $E[I_n] = I(W)$ results in $\Pr(I_\infty = 1) = I(W)$ and $\Pr(I_\infty = 0) = 1 - I(W)$. Therefore, $I(W)$ fraction of the realizations of the process I_n converges to 1.

The above result have the following implications for the $W_n^{(i)}$ channels. It ensures that, as n gets large, for $I(W)$ fractions of $W_n^{(i)}$ the corresponding symmetric capacities will be arbitrarily close to 1. This result brings a different meaning to the channel capacity in the sense that for polar codes $I(W)$ is the fraction of synthesized binary-

input channels $W_n^{(i)}$, by using which, one can transmit binary information reliably.

2.5.2. Rate of Polarization

In the previous section we showed that, as n gets large, $W_n^{(i)}$ channels polarize in the sense their symmetric capacities get close to 1 or 0. A crucial point is analyzing the rate of this polarization as it will bring light on the performance of polar codes. In Arıkan and Telater [17] characterizes the rate of polarization by providing probabilistic bounds on the process $\{Z_n\}$ as given below

Theorem 2.1. *When n is large, for $\beta < \frac{1}{2}$*

$$\Pr(Z_n \leq 2^{-N^\beta}) \geq I(W), \tag{2.13}$$

conversely, for $\beta > \frac{1}{2}$,

$$\Pr(Z_n \geq 2^{-N^\beta}) = 1. \tag{2.14}$$

The above theorem has the following implications on polar codes. Notice that each realization of the process $\{Z_n\}$ occurs with probability $1/N$ and it corresponds to the Bhattacharyya parameters, $Z_n^{(i)}$, of $W_n^{(i)}$ channels. Therefore, for $I(W)$ fractions of $W_n^{(i)}$ the corresponding Bhattacharyya parameters will be bounded as $Z_n^{(i)} \leq 2^{-N^\beta}$, for $\beta < 1/2$. Since Bhattacharyya parameter is an upper bound on the probability error, $P_{e,n}^{(i)}$, of channel $W_n^{(i)}$, we also have $P_{e,n}^{(i)} \leq 2^{-N^\beta}$. Let P_e denote the block-decoding error probability of polar codes with code-length $N = 2^n$. We have

$$P_e \leq \sum_{i=1}^{N} P_{e,n}^{(i)} \leq \sum_{i=1}^{N} 2^{-N^\beta} = N2^{-N^\beta} = O(2^{-N^\beta}) \tag{2.15}$$

for $\beta < 1/2$. This is an achievable result on the error probability of polar codes. Next,

by using the converse part of the above theorem we see that

$$P_e \geq \max\{Z_n^{(i)}\} \geq 2^{-N^\beta} \tag{2.16}$$

holds for $\beta \geq 1/2$. The term β is called the exponent of polar codes as it shows how fast the block-decoding error probability scales exponentially in the code-length.

2.6. Complexity

Let us consider a single core processor where we are interested in the time complexity of the encoding operation. Let χ_n^E denote the encoding complexity at channel combining and splitting level n. Investigating Fig. 2.1 and by taking the complexity of $\oplus$ operation as 1 unit we can formulate χ_n^E as

$$\begin{aligned}\chi_n^E &= 2\chi_{n-1}^E + N/2 \\ &= \underbrace{N/2 + \ldots + N/2}_{n \text{ times}} \\ &= O(N \log N),\end{aligned}$$

where we have used $\chi_1^E = 1$ and $\chi_0^E = 0$.

Next, we let χ_n^D to denote the decoding complexity where we consider SCD as the decoding method and LR relations in (2.6) are used for calculating the transition probabilities of $W_n^{(i)}$. Investigating (2.6) we see that the problem of calculating N LRs of level n can be accomplished if the LRs of level $n-1$ are ready. If we take the combining operation of two LRs coming from previous stage as 1 unit, we can formulate

χ_n^D as

$$\begin{aligned}\chi_n^D &= 2\chi_{n-1}^D + N \\ &= \underbrace{N + \ldots + N}_{n+1 \text{ times}} \\ &= O(N \log N),\end{aligned}$$

where we used $\chi_0^D = 1$.

The above results indicate that the encoding and decoding operation of polar codes have complexities $O(N \log N)$ which is linear in the code-length.

3. ON THE CHANNEL-SPECIFIC CONSTRUCTION OF POLAR CODES

Recall from Section 2.3 that polar codes and RM codes have the same encoding structure as

$$\begin{aligned}\mathbf{x}_N &= \mathbf{u}_N \mathbf{G}_n, \\ &= \mathbf{u}_{\mathcal{A}} \mathbf{G}_n(A) \oplus \mathbf{u}_{\mathcal{A}^c} \mathbf{G}_n(\mathcal{A}^c),\end{aligned}$$

where the main distinction was the selection of the set $\mathcal{A}$. For polar codes one choses the set $\mathcal{A}$ by minimizing $\sum_{i\in\mathcal{A}} Z_n^{(i)}$ whereas, for RM codes one maximizes $\sum_{i\in\mathcal{A}} H_n^{(i)}$. This fact results in polar codes to be channel-specific because the Bhattacharyya parameters, $Z_n^{(i)}$, depend on the underlying channel, W. However, the Hamming weights, $H_n^{(i)}$, of $\mathbf{G}_n$, are independent of the channel.

In this chapter we consider a relationship between the Hamming weights, $H_n^{(i)}$, and the Bhattacharyya parameters, $Z_n^{(i)}$. We obtain upper and lower bounds on $Z_n^{(i)}$ by using $H_n^{(i)}$ and the symmetric capacity, $I(W)$, of the underlying channel W. These bounds, which are asymptotically tight in $H_n^{(i)}$, demonstrate the effect of W and $H_n^{(i)}$ on $Z_n^{(i)}$, and provide insight on the channel-specific construction of polar codes, complementing [15]. Our analysis, thereby, shows that both the underlying channel and the Hamming weights have effect on the construction of polar codes. This observation provides a bridge between polar and RM codes. The bounds derived in this chapter can be extended to obtain the exponent, β, of polar codes alternative to the analysis of Arıkan and Telatar in [17] where the inherent effect of Hamming weights on the exponent, β, of polar codes becomes evident as well.

3.1. Probabilistic Model

Recall from Section 2.5 that we have defined a random channel process $\{K_n : n \geq 1\}$ where $K_n = W_{B_1,B_2,\ldots,B_n}$, $\Pr(B_i = +) = \Pr(B_i = -) = 1/2$, and the realizations of K_n are viewed as the binary-input channel $W_n^{(i)}$. We have also defined a Bhattacharyya process $\{Z_n : n \geq 1\}$ for the corresponding channel process $\{K_n : n \geq 1\}$ by letting $Z_n = Z(K_n)$ where the realization of Z_n are the Bhattacharyya parameter, $Z_n^{(i)}$, of $W_n^{(i)}$ channels. Now, we extend this probabilistic model by defining a Hamming process $\{H_n\}$, $H_n \in \{1, 2, 2^2, \ldots, 2^n\}$, such that the realization of H_n will correspond to the Hamming weights, $H_n^{(i)}$, of the rows of $\mathbf{G}_n$. This process is of the form [18]

$$H_n = \begin{cases} 2H_{n-1}, & \text{if } B_n = 1, \\ H_{n-1}, & \text{if } B_n = 0, \end{cases} \tag{3.1}$$

where $H_0 = 1$. Our aim is to investigate the processes $\{Z_n\}$ and $\{H_n\}$ jointly, where process $\{Z_n\}$, as explained in Section 2.5, is of the form

$$Z_n \begin{cases} \leq 2Z_{n-1} - Z_{n-1}^2, & \text{if} \quad B_n = -, \\ = Z_{n-1}^2, & \text{if} \quad B_n = +, \end{cases} \tag{3.2}$$

Examining $\{Z_n\}$ and $\{H_n\}$ as given by (3.2) and (3.1), respectively, we observe that the recursive natures of $\{Z_n\}$ and $\{H_n\}$ have some similarities. When $B_n = 1$ the value of Z_n is the square of Z_{n-1} and the value of H_n doubles with respect to H_{n-1} implying that $Z_n < Z_{n-1}$ holds if $H_n > H_{n-1}$. On the other hand, when $B_n = 0$, Z_n increases compared to Z_{n-1} but the value of H_n does not change over H_{n-1}. Let us fix $\sum_{i=1}^n B_i$ and $H_n = 2^{\sum_{i=1}^n B_i}$. Then the largest realization for Z_n occurs if all of the 1s in $\{B_n\}$ come after the 0s. Similarly, the smallest realization of $\{Z_n\}$ occurs if all of the 1s in $\{B_n\}$ come before the 0s. Therefore, both the position and the number of 1s in $\{B_n\}$ have an effect on Z_n. This observation was also made in [18], where authors propose a coding scheme $\{\mathcal{C}^\alpha : \alpha \in [0, 1]\}$ which smoothly interpolates between

polar and RM codes. The interpolation between polar codes and RM codes is based on the fact that, as $\alpha \to 0$, Z_n depends more on $\sum_{i=1}^{n} B_i$, and thus H_n, rather than the position of 1s in $\{B_n\}$.

3.2. Effect of Hamming Weights on the Construction of Polar Codes

We consider a polar code used for transmission over a BDMC, W, whose symmetric capacity and Bhattacharyya parameter are $I(W) \in (0,1)$ and $Z(W) \in (0,1)$, respectively. The receiver employs SCD for a polar code with length $N = 2^n$, which we assume to be fixed. We seek a relationship between the Hamming weights, $H_n^{(i)}$, of the rows of the generator matrix $\mathbf{G}_N$ and the Bhattacharyya parameters, $Z_n^{(i)}$, of the synthesized binary-input channels, $W_n^{(i)}$. We define $w(i)$, $w(i) \in \{0, 1, \ldots, n\}$, as

$$w(i) = \sum_{j=1}^{n} b_j, \quad \mathbb{B}(i) = (b_1, b_2, \ldots, b_n)_2 + 1.$$

Investigating the recursive formulation of $\mathbf{G}_n$

$$\mathbf{G}_n = \mathbf{G}_{n-1} \otimes F = \begin{bmatrix} \mathbf{G}_{n-1} & \mathbf{0}_{n-1} \\ \mathbf{G}_{n-1} & \mathbf{G}_{n-1} \end{bmatrix},$$

we notice that $H_n^{(i)} = 2^{w(i)}$ holds [19]. We fix $w(i) = w$, $w \in \{0, 1, \ldots, n\}$, and define a type class $\mathcal{H}_n^w$ as

$$\mathcal{H}_n^w = \{H_n^{(i)} : H_n^{(i)} = 2^w, i = 1, 2, \ldots, N\}.$$

The cardinality of $\mathcal{H}_n^w$ is $|\mathcal{H}_n^w| = \binom{n}{w}$. With the following theorem we provide bounds on $Z_n^{(i)}$ by using $H_n^{(i)} \in \mathcal{H}_n^w$ and $I(W)$.

Theorem 3.1. *For any $\epsilon \in (0,1)$, there exists a fixed $N = 2^n$ so that, for some $f_H = O\left(\frac{1}{\log H_n^{(i)}}\right)$ as $H_n^{(i)} \to N$, and for $I(W) - \epsilon$ fraction of $H_n^{(i)} \in \mathcal{H}_n^w$, we have*

$$Z_n^{(i)} \leq 2^{-(H_n^{(i)})^{(1-\epsilon-f_H)}}. \tag{3.3}$$

Conversely, for all $H_n^{(i)} \in \mathcal{H}_n^w$ *and independent of the underlying channel* W*,*

$$Z_n^{(i)} \geq 2^{-\left(H_n^{(i)}\right)^{(1+f_H)}}. \tag{3.4}$$

Proof. In order to prove (3.3) we consider another process $\{\hat{Z}_n\}$ so that for $i = 1, 2, \ldots, m$, $m < n$, we have $\hat{Z}_i = Z_i$ and for $i > m$, $\hat{Z}_i$ obeys

$$\hat{Z}_i = \begin{cases} \hat{Z}_{i-1}^2, & \text{if } B_n = 1, \\ 2\hat{Z}_{i-1} - \hat{Z}_{i-1}^2, & \text{if } B_n = 0. \end{cases} \tag{3.5}$$

Comparing (2.9) and (3.5) one observes that the process $\{Z_n\}$ is stochastically dominated by $\{\hat{Z}_n\}$ in the sense that for some $g_n \in (0,1)$ we have $\Pr(Z_n \leq g_n) \geq \Pr(\hat{Z}_n \leq g_n)$. Letting $\zeta \in (0,1)$ and $\gamma \in (0,1)$, we define

$$D_{n_0}(\zeta) \triangleq \{\hat{Z}_m \leq \zeta\},$$
$$G_{n_0}^n(\gamma) \triangleq \left\{ \frac{\sum_{n_0+1}^n B_i}{n-m} \geq \gamma \right\},$$

and observe that $D_{n_0}(\zeta)$ and $G_{n_0}^n(\gamma)$ are independent events. The next lemma, which simplifies the bootstrapping technique of [17], is proved in the Appendix A.

Lemma 3.1. *For some* $\epsilon, \gamma \in (0,1)$*,*

$$\hat{Z}_n \leq 2^{-2^{(\gamma-\epsilon)(n-n_0)}}, \quad D_{n_0}(\zeta) \cap G_{n_0}^n(\gamma).$$

Let $A = \sum_{i=1}^n B_i$ so that $H_n = 2^A$. The event $G_{n_0}^n(\gamma)$ is always valid if we take $\gamma = \frac{A-n_0}{n-n_0}$. Using this fact in Lemma 1, we obtain

$$\hat{Z}_n \leq 2^{-2^{A\left(1-\frac{n_0+n\epsilon}{A}\right)}}, \quad D_{n_0}(\zeta) \cap \{H_n = 2^A\}. \tag{3.6}$$

The convergence of Z_n to $Z_\infty = 0$ with probability $\Pr(Z_\infty = 0) = I(W)$ implies that

there exists a fixed n_0, $n_0 < n$, so that

$$\Pr\left(D_{n_0}(\zeta)\right) \geq I(W) - \epsilon.$$

In (3.6) observe that for any fixed N, $N = 2^n$, we have $\frac{n_0+n\epsilon}{A} = O\left(\frac{1}{\log_2 H_n}\right) + \epsilon$ as $A \to n$. Combining the above results gives

$$\Pr\left(\hat{Z}_n \leq 2^{-H_n^{\left(1-\epsilon-O(\frac{1}{\log_2 H_n})\right)}}\right) \geq I(W) - \epsilon,$$

which completes the proof of (3.3).

For the proof of (3.4) we consider another process $\{\tilde{Z}_n\}$ which is of the form

$$\tilde{Z}_n = \begin{cases} \tilde{Z}_{n-1}^2, & \text{if } B_n = 1, \\ \tilde{Z}_{n-1}, & \text{if } B_n = 0, \end{cases} \tag{3.7}$$

where $\tilde{Z}_0 = Z_0$. By using the recursion in (3.7), we obtain

$$\begin{aligned} \log_2 \tilde{Z}_n &= -2^A \log_2(1/Z_0), \\ &= -2^{A\left(1+\frac{\log_2 \log_2(1/Z_0)}{A}\right)}. \end{aligned}$$

Since $Z_0 \in (0,1)$ is a constant, we have $\frac{\log_2 \log_2(1/Z_0)}{A} = O\left(\frac{1}{\log_2 H_n}\right)$ as $A \to n$, and thus,

$$\Pr\left(\tilde{Z}_n \geq 2^{-H_n^{\left(1+O\left(\frac{1}{\log_2 H_n}\right)\right)}}\right) \geq 1.$$

The proof follows by comparing (2.9) and (3.7), and observing that $\{\tilde{Z}_n\}$ is stochastically dominated by $\{Z_n\}$ in the sense that for some $g_n \in (0,1)$, we have $\Pr(Z_n \geq g_n) \geq \Pr(\tilde{Z}_n \geq g_n)$. □

Let us interpret Theorem 3.1. Observe that the upper bound on $Z_N^{(i)}$ is only

valid for $I(W)-\epsilon$ fraction of $H_N^{(i)} \in \mathcal{H}_N^w$, whereas the lower bound on $Z_N^{(i)}$ holds for all $H_N^{(i)} \in \mathcal{H}_N^w$ and is independent of the underlying channel, W. The gap between the upper and lower bounds in (3.3) and (3.4) decreases with increasing $H_N^{(i)}$ so that bounds become asymptotically tight in $H_n^{(i)}$. The upper and lower bounds together indicate that, within each type class $\mathcal{H}_n^w$, the corresponding $Z_n^{(i)}$ values concentrate around $2^{-H_n^{(i)}}$ in the sense that for $\lfloor (I(W)-\epsilon)\binom{n}{w} \rfloor$ elements of $\mathcal{H}_n^w$, one observes

$$2^{-(H_n^{(i)})^{(1+f_H)}} \leq Z_n^{(i)} \leq 2^{-(H_n^{(i)})^{(1-\epsilon-f_H)}}.$$

For the remaining $1-I(W)+\epsilon$ fraction of $\mathcal{H}_N^w$ one can only infer that

$$2^{-(H_n^{(i)})^{(1+f_H)}} \leq Z_n^{(i)} \leq 1.$$

Therefore, we can consider $I(W)$ as a correlation parameter between $H_n^{(i)} \in \mathcal{H}_n^w$ and $Z_n^{(i)}$ where increasing its value will make $Z_n^{(i)}$ depend more on $H_n^{(i)} \in \mathcal{H}_n^w$ rather than the underlying channel. The above analysis complements [15] by showing the inherent play between $H_n^{(i)}$ and W on $Z_n^{(i)}$, where the effect of W is manifested by the $I(W)$ term.

Now we investigate the $Z_n^{(i)}$ terms when the corresponding $H_n^{(i)}$ values are large so that the bounds in Theorem 1 are tight. We consider two such type classes, $\mathcal{H}_n^{w_1}$ and $\mathcal{H}_n^{w_2}$, where $1<w_1<w_2<n$. The cardinalities of $\mathcal{H}_n^{w_1}$ and $\mathcal{H}_n^{w_2}$ are $\binom{n}{w_1}$ and $\binom{n}{w_2}$, respectively. Let i and j correspond to the indices of the members of two type classes such that $H_n^{(i)} \in \mathcal{H}_n^{w_1}$ and $H_n^{(j)} \in \mathcal{H}_n^{w_2}$, with corresponding Bhattacharyya parameters $Z_n^{(i)}$ and $Z_n^{(j)}$, respectively. Under these assumptions there exist $\left\lfloor (I(W)-\epsilon) \times \binom{n}{w_1} \right\rfloor$ distinct i and $\left\lfloor (I(W)-\epsilon) \times \binom{n}{w_2} \right\rfloor$ distinct j such that $Z_n^{(i)} < Z_n^{(j)}$ holds. Consequently, if we increase $I(W)$, more $Z_n^{(i)}$ values will depend on the corresponding $H_n^{(i)}$ in the sense that a larger $H_n^{(i)}$ will correspond to a smaller $Z_n^{(i)}$. As $I(W) \to 1$, $Z_n^{(i)}$ terms depend entirely on $H_n^{(i)}$ for which the bounds in Theorem 1 are tight.

The above implications of Theorem 1 also complement [18, Prop. 1], where the

authors prove that a polar code designed for a BEC with erasure probability ε tends to an RM code as $\varepsilon \to 0$. In our set-up, a BEC having $\varepsilon \to 0$ corresponds to $I(W) \to 1$, and our analysis shows that, in this case, $Z_N^{(i)}$ terms depend entirely on $H_N^{(i)}$, so long as the latter are large enough.

3.3. Effect of Hamming Weights on the Exponent of Polar Codes

In this section we obtain bounds on the exponent, β, of polar codes with a simple application of Theorem 3.1. Our analysis is based on the following lemma, whose proof easily follows from the Method of Types [20] and is omitted.

Lemma 3.2. *For any $\epsilon \in (0,1)$ there exists a sufficiently large N, $N = 2^n$, so that for $1-\epsilon$ fraction of i we have*

$$H_N^{(i)} \in \mathcal{H}_N^w, \quad \left\lfloor \frac{n}{2} - \epsilon \leq w \leq \frac{n}{2} + \epsilon \right\rfloor.$$

The above Lemma states that among $\mathcal{H}_N^w$, $w \in \{1, 2, \ldots, n\}$, one typically observes the ones with $\left\lfloor \frac{n}{2} - \epsilon \leq w \leq \frac{n}{2} + \epsilon \right\rfloor$. Recall that Theorem 3.1 is a general result because it relates $Z_N^{(i)}$ to all $H_N^{(i)} \in \mathcal{H}_N^w$. But the above lemma indicates that as N gets large, one typically observes $N^{1/2-\epsilon} \leq H_N^{(i)} \leq N^{1/2+\epsilon}$, except for a vanishing fraction of i. This fact, when used together with Theorem 1, implies that for $I(W) - \epsilon$ fraction of i,

$$Z_N^{(i)} \leq 2^{-N^{\frac{1}{2}-\epsilon}}. \tag{3.8}$$

Conversely, for $1-\epsilon$ fraction of i,

$$Z_N^{(i)} \geq 2^{-N^{\frac{1}{2}+\epsilon}}. \tag{3.9}$$

Equation (3.8) implies that the block error probability, P_e, of polar codes obeys $P_e \leq \sum_{i=1}^{N} Z_N^{(i)} = O(2^{-N^\beta})$ for $\beta < 1/2$, and from (3.9), one sees that $P_e \geq \max_i Z_N^{(i)} = 2^{-N^\beta}$

holds for $\beta > 1/2$. We have thereby unified (2.15) and (2.16) by using Theorem 1, providing an easier alternative to [17] where the inherent effect of the Hamming weights on the exponent, β, of polar codes becomes visible.

3.4. Discussion

We have obtained bounds on the Bhattacharyya parameters, $Z_n^{(i)}$, of the synthetic binary-input channels, $W_n^{(i)}$, by using the Hamming weights, $H_n^{(i)}$, of the rows of the generator matrix, $\mathbf{G}_n$, and the symmetric capacity, $I(W)$, of the underlying channel, W. These bounds provide insight on the channel-specific construction of polar codes and complement the results in [15]. We have shown that the Bhattacharyya parameters $Z_n^{(i)}$ depend more on $H_n^{(i)}$ than the underlying channel, W, with increasing $I(W)$, which complements the results in [18]. The analysis presented in this paper simplifies the bootstrapping technique of Arıkand and Telatar in [17] and extends it to providing a characterization for the exponent, β, of polar codes, where the inherent effect of $H_n^{(i)}$ on β becomes visible. Future work should investigate the effect of the Hamming weights on the Bhattacharyya parameters and the exponent of polar codes obtained from $\ell \times \ell$, $\ell \geq 2$, arbitrary polarization kernel, $\mathbf{K}$, where the generator matrix takes the form, $\mathbf{G}_n = \mathbf{K}^{\otimes n}$, $N = \ell^n$, and it is possible to have exponents exceeding $1/2$ by using larger kernels [21].

4. BIT-INTERLEAVED POLAR-CODED MODULATION

In this chapter, we develop a bit-interleaved polar-coded modulation (BIPCM) architecture for communication over fading channels. In particular, we present a low-complexity code construction approach that is based on the adaptation of Arıkan's heuristic method in [15] to BICM. We also propose a numerically robust and lower-complexity version of the successive cancellation list decoder (SCLD) of [22], employing cyclic-redundancy check (CRC). The above-mentioned methods are employed in the design of a BIPCM system using 16-ary quadrature-amplitude modulation (16-QAM) with gray labeling (GL) and mapping by set partitioning (SP), and its performance is compared to existing high-performance BICM systems for moderate block lengths. Simulation results illustrate that BIPCM provides significant performance benefits over BICM with other codes.

4.1. Introduction

In [23], Zehavi proposed a method to increase the code diversity over fading channels. His observation was to replace the symbol-wise interleaver in Ungerboeck's trellis-coded modulation system [24] with a bit-wise interleaver and to perform independent binary encoding and decoding in channels, obtained by applying a binary decomposition to the underlying non-binary input channel. The resulting bit-interleaved coded modulation (BICM) system provides excellent performance gains at high signal-to-noise ratio (SNR) with low implementation complexity despite being suboptimal due to independence assumptions of the so-called bit channels. A comprehensive study of BICM can be found in [25].

The construction of BICM is investigated in conjunction with convolutional codes in [26], low-density parity check codes (LDPC) in [27] and repeat accumulate codes (RA) in [28]. Because coding and modulation are viewed as a single entity, performance optimization of BICM usually depends on the underlying coding and modulation schemes. In addition, iterative methods are proposed for BICM in [26] to compensate

for the performance degradation due to the independence assumption.

4.2. Channel Model

We consider a fading additive white Gaussian noise (AWGN) channel with discrete input signal $x \in \mathcal{X}$, with cardinality $|\mathcal{X}| = 2^q$, and continuous output $y \in \mathcal{Y}$. The input symbols are assumed to be uniformly distributed over the alphabet $\mathcal{X}$. For flat fading, a single use of the channel can be described as

$$y = hx + n$$

where h is the complex channel fading coefficient with $\mathbf{E}[|h|^2] = 1$ and n is circularly symmetric additive white Gaussian noise (AWGN) with zero mean and variance σ^2. Such a channel can be represented by the channel transition probability density function $W(y|x,h)$, and its capacity with perfect channel state information (CSI) at the receiver is given by

$$I_{\text{CSI}}(W) = \mathbf{E}_{x,y,h}\left[\log_2 \frac{W(y|x,h)}{\sum_x W(y|x,h)2^{-q}}\right].$$

When the fading channel is memoryless, N successive uses of the channel is described as

$$W(\mathbf{y}_N|\mathbf{h}_N,\mathbf{x}_N) = \prod_{i=1}^{N} W(y_i|h_i,x_i). \tag{4.1}$$

If the fading information is not available at the receiver, the channel can not be considered memoryless [25]. However, with ideal interleaving, an average channel transition probability can be calculated as

$$W(y|x) = \mathbf{E}_h\left[W(y|x,h)\right],$$

and the channel capacity without CSI then becomes

$$I_{\text{no\_CSI}}(W) = \mathbf{E}_{x,y}\left[\log_2 \frac{W(y|x)}{\sum_x W(y|x)2^{-q}}\right]. \tag{4.2}$$

In classical BICM, the input symbol x is represented by a binary labeling $\mu\colon \{0,1\}^q \to \mathcal{X}$. Then each labeling position $\ell^{(j)}(x), j \in \{1,2,\ldots,q\}$, is used to transmit binary information independently. Gray labeling is usually preferred for non-iterative BICM, since it ensures a large Euclidean distance between constellation points [25]. However, depending on the constellation, it may not always be possible to implement Gray labeling. Set partitioning is opted for in iterative BICM, because it provides good Euclidean distance with ideal feedback [28]. Labeling effectively transforms the 2^q-ary input channel into q binary channels. This transformation allows binary encoding and decoding implementation which can be implemented easier than coding on non-binary alphabet. As Zehavi notes in [23], code diversity also increases when binary coding is applied. These properties account for the popularity of BICM.

Since x is assumed to be uniform in $\mathcal{X}$, the induced probabilities at each labeling position $\ell^{(j)}(x)$ are identical so that $\ell^{(j)}(x) = B(1/2)$, where $B(1/2)$ is a Bernoulli random variable with parameter $1/2$. The conditional probability of y given $\ell^{(j)}(x)$ can be written as

$$W(y|\ell^{(j)}(x), h) = \sum_{x \neq \ell^{(j)}(x)} W(y|x,h)2^{-(q-1)}.$$

The resulting bit channel can be viewed as a binary channel with input $\ell^{(j)}(x) \in \{0,1\}$ and output y. We will use the short hand notation

$$W^{(j)} \triangleq W(y|\ell^{(j)}(x), h),$$

to refer to the bit channel seen by $\ell^{(j)}(x)$.

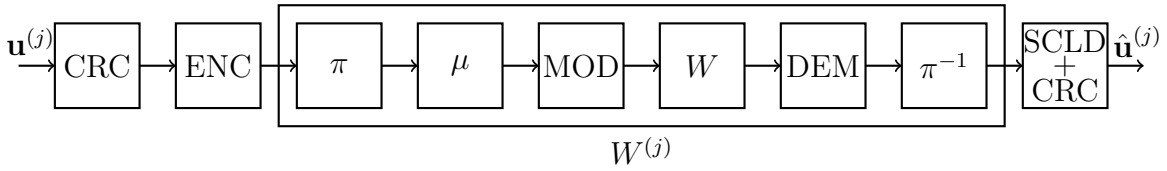

Figure 4.1. BIPCM system model.

4.3. Polar-Coded Modulation

Let $\mathbf{u}^{(j)} = [u_1^{(j)}, u_2^{(j)}, \ldots, u_N^{(j)}]$, $j \in \{1, 2, \ldots, q\}$, denote the information vector with length N transmitted on channel $W^{(j)}$. The BIPCM system acting on $\mathbf{u}^{(j)}$ is demonstrated in Fig. 1. We append a CRC prior to encoding. After encoding, the bit stream is interleaved with a randomly constructed inter-leaver denoted by π. Then a symbol mapper μ is used to select the modulated symbol based on $\ell^{(j)}(x), j \in \{1, 2, \ldots, q\}$. After modulation and transmission through the channel, the demodulator calculates the channel transition probabilities for each $\ell^{(j)}(x)$ and passes them to the corresponding decoder following de-interleaving by the block π^{-1}. Next, SCLD is used to obtain a list of L most probable codewords. Finally, CRC is applied to select the most probable CRC-valid codeword and obtain the estimated vector, $\hat{\mathbf{u}}^{(j)}$. CRC and encoding operations prior to interleaving and the decoding operation after de-interleaving are generic for all vectors $\mathbf{u}^{(j)}$. Therefore, in BIPCM one designs q polar codes with SCLD for transmission through $W^{(j)}$, $j \in \{1, 2, \ldots, q\}$, channels.

In BIPCM, depending on the rate $R^{(j)}$ on channel $W^{(j)}$, only a subset of $\mathbf{u}^{(j)}$ is used to send information while the remaining indices are kept frozen and their true values are revealed to the decoder before transmission. Let $A^{(j)} \subset \{1, 2, \ldots, N\}$ denote the set of information indices and $\mathbf{u}_{A^{(i)}}^{(j)}$ and $\mathbf{u}_{A^{c,(j)}}^{(j)}$ denote the set of information and frozen bits, respectively. Encoding is performed via

$$\mathbf{x}^{(j)} = \mathbf{u}_{A^{(j)}}^{(j)} G_n(A^{(j)}) \oplus \mathbf{u}_{A^{c,(j)}}^{(j)} G_n(A^{c,(j)}),$$

where $G_N(A)$ is formed by selecting the rows of G_N with indices in A and $\oplus$ denotes the modulo-2 sum. A polar code is completely characterized by the parameter vector

$(N, K^{(j)}, A^{(j)}, \mathbf{u}_{A^c}^{(j)})$ where $K^{(j)} = |A^{(j)}|$ is the code dimension and $R^{(j)} = K^{(j)}/N$ is the code rate on $B^{(j)}$. The total transmission rate is

$$\sum_{j=1}^{q} R^{(j)} = R_{\text{BICM}}.$$

Before transmission one has to fix the set $A^{(j)}$ which is the code construction problem.

4.3.1. Code Construction

Let us use $W_n^{(i,j)}$, $i \in \{1, 2, \ldots, N\}$, $N = 2^n$, $j \in \{1, 2, \ldots, q\}$ to denote the ith synthesized binary-input channel obtained from $N = 2^n$ use of channel $W^{(j)}$. Let $Z_n^{(i,j)}$ denote the Bhattacharyya parameter of this channel. The code construction problem for the considered coding scheme can be formalized as

$$\begin{aligned} \text{Minimize} \quad & \sum_{j=1}^{q} \sum_{i \in A^{(i)}} Z_n^{(i,j)}, \\ \text{subject to} \quad & \sum_{i} R^{(i)} = R_{\text{BIPCM}}. \end{aligned}$$

Although the construction problem is well-defined, as we have explained in Section 2.3, no explicit construction formulas are available to exactly calculate $Z_n^{(i,j)}$ terms except for BECs. To solve this problem we resort to Arıkan's heuristic code construction method [15], which can be implemented with complexity $O(N)$. This heuristic method is performed as follows. Given an arbitrary channel, W, with capacity $I(W)$, assume that the Bhattacharyya parameter of this channel to be $1 - I(W)$. After this assumption use the recursive formulas (2.4) to calculate the Bhattacharyya parameters of binary-input input channels synthesized from N uses of W assuming the underlying channel to be BEC. Our numerical analysis indicates that Arıkan's code construction method performs almost the same as [29] and [16] for binary symmetric channels, albeit with less complexity. Our solution is as follows. We first calculate the capacity of each $W^{(j)}$, $I(W^{(j)})$ by using (4.2). Then, we use (2.4) by assuming $Z_0 = 1 - I(W^{(j)})$ and

underlying channel, $W^{(j)}$, to be BEC.

$$\begin{aligned} Z_n^{(i,j)} &= 2Z_{n-1}^{(j,j)} - (Z_{n-1}^{(j,j)})^2, \\ Z_n^{(i+N/2,j)} &= (Z_{n-1}^{(i,j)})^2, \end{aligned} \qquad i = 1, 2, \ldots, N/2.$$

Our approach can be viewed as a simple generalization of Arıkan's code construction method to parallel independent channels with a joint rate constraint. As we show in Section IV, even with this simple construction method, BIPCM offers performance advantages compared to some existing codes, for moderate code-lengths.

4.3.2. Successive Cancellation List Decoding

In [22], the authors propose a list decoding version of SCD, called successive cancellation list decoding (SCLD), to reach the ML decoding performance of polar codes. In SCLD, hard decisions on the inputs of $W_n^{(i)}$ are avoided and $W_n^{(i)}(0)$ and $W_n^{(i)}(1)$ are both considered by creating a decision tree, where $W_n^{(i)}(x)$, $x \in \mathcal{X} = \{0, 1\}$, denotes the posterior probability of transmitting the symbol x from the input of $W_n^{(i)}$. Because the number of paths in the tree increases exponentially, only the best L of them are preserved while the rest of them are pruned. Thus L denotes the list size. SCLD can be implemented with complexity $O(LN \log N)$, increasing the original SCD complexity only linearly with the list size. In the original implementation of SCLD the path probabilities are calculated by using $W_n^{(i)}(0)$ and $W_n^{(i)}(1)$. As n increases those probabilities become arbitrarily small and create numerical underflow. Since there are N such probabilities at each level of decoding, one needs to normalize $N \log N$ probabilities for a stable algorithm. Hence the complexity of normalization unit is $O(N \log N)$.

One is limited by precision and has to put enough resources for a stable hardware implementation to avoid numerical underflow. We present an alternative solution to overcome this problem. We use the LLR (log likelihood ration) relationships as given below, instead of the LR relations in (2.6), to calculate the posterior probabilities of

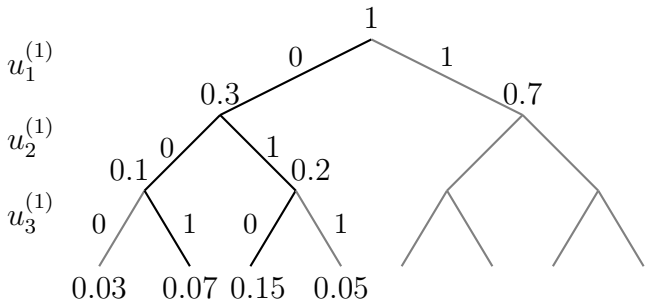

Figure 4.2. Tree formation for SCLD.

bit channels.

$$L_n^{(i)} = 2\tanh^{-1}\Big(\tanh(\frac{L_{n-1}^{(i)}}{2}).\tanh(\frac{\bar{L}_{n-1}^{(i)}}{2})\Big), \quad i = 1, 2, \ldots, N/2 \qquad (4.3)$$
$$L_N^{(i+N/2)} = L_{n-1}^{(i)} + (-1)^{2\tilde{u}_n^{(i)}}\bar{L}_{n-1}^{(i)},$$

Then, we create and expand the decision tree by using $W_n^{(i)}(0)/W_n^{(i)}(1)$. An example with $L = 2$ is shown in Fig. 2, where the decoding of the first three bits $u_1^{(1)}, u_2^{(1)}, u_3^{(1)}$ of $\mathbf{u}^{(1)}$ is shown. The bit $u_1^{(1)}$ shows a frozen bit with value of 0; thus, without expanding the tree, $u_1^{(1)} = 0$ path is selected. Bits $u_2^{(1)}$ and $u_3^{(1)}$ are information bits, and hence the decision on $u_2^{(1)}$ is split into two paths. The four resultant paths at level 3 are pruned to two paths by selecting the most probable ones. After expanding the tree for all $u_i^{(1)}$, at the decoder output L candidate codewords are obtained. The most likely one is chosen as the decoded codeword. Observe that at most L paths are preserved at every level of the tree. Because there are $n = \log N$ levels on the decision tree, one only needs to normalize $L \log N$ probabilities. With our approach, although the complexity of SCLD is still $O(LN \log N)$, the complexity of normalization unit is $O(L \log N)$, which is an improvement over $O(N \log N)$.

As suggested in [22], CRC can be employed to further improve the performance of polar codes. When employing CRC, ℓ_{CRC} more bits are transmitted, where ℓ_{CRC} denotes the lengh of the CRC. In order to preserve R_{BICM}, the size $K^{(j)}$ of each set $A^{(j)}$ is incremented by ℓ_{CRC} so that the effective code rate stays the same. The final decision on L candidate codewords is made in accordance with their probabilities and

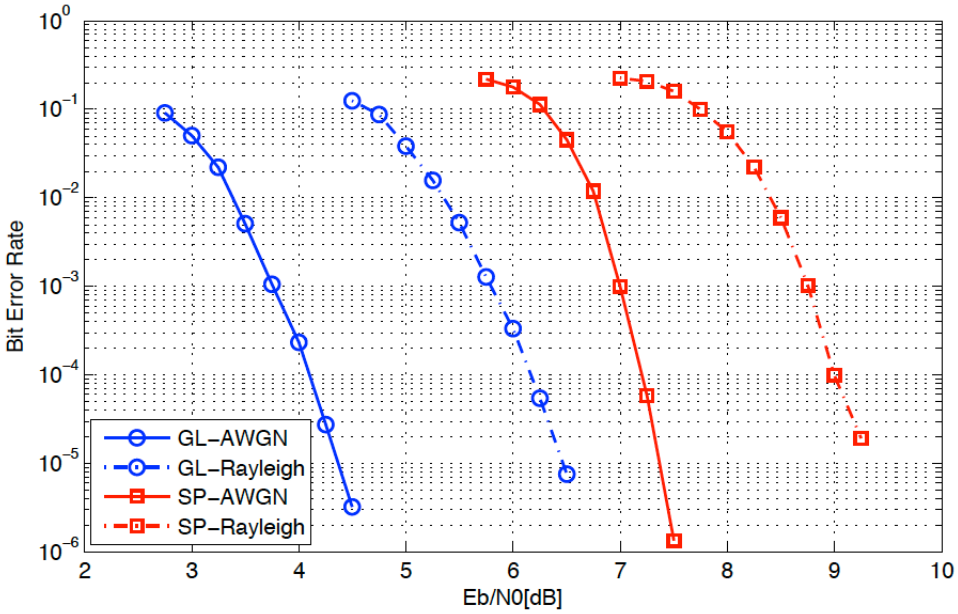

Figure 4.3. Bit error rate performance of BIPCM with different mappings.

CRCs. Since some of the unused bit channels still have some capacity left, CRC takes advantages of the residual capacity of those bit channels, providing improved performance beyond ML decoding. The residual capacity in unpolarized channels is discussed in [30]. We note that there are other methods to increase the performance of polar codes, e.g., applying an outer code (as an example see [31]). However, those methods increase the decoding complexity significantly. Indeed, SCLD with CRC offers a nice complexity versus performance trade-off.

4.4. Simulation Results

In this section, we present the bit-error rate (BER) simulation results for comparing the performance of the proposed scheme with those of some well-known high-performance BICM approaches. BIPCM system is simulated with 16-QAM alphabets. Code-length is set to 2048 for each $W^{(j)}$ channel and the total rate of BICM is set to $R_{\text{BIPCM}} = 0.5$ (2 bits/channel use for 16-QAM). Prior to encoding, a CRC with length 16 (CCITT CRC-16) with generator polynomial $g(x) = x^{16} + x^{12} + x^5 + 1$ is appended to each information stream. SCLD is used with $L = 32$. Performances of GL and SP are investigated for AWGN and Rayleigh channels.

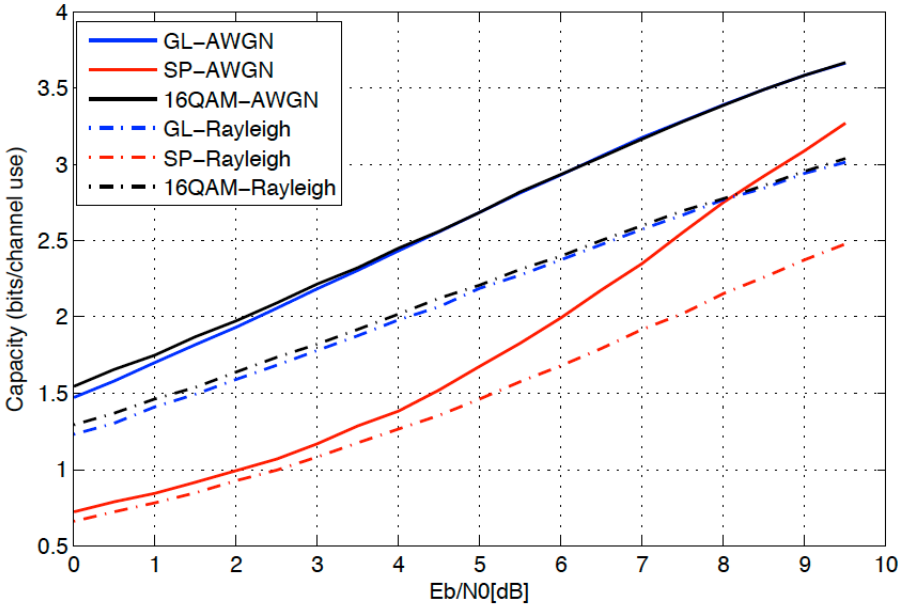

Figure 4.4. Achievable rates of different mappings for 16-QAM.

Bit error rates of the two labeling methods are shown in Fig. 4.3. The plot indicates that GL provides better performance than SP. This is expected because the capacity of SP with non-iterative BICM is strictly less than that of 16-QAM. This is demonstrated in Fig. 4.4, where the capacities of SP, GL and 16-QAM are plotted for AWGN and Rayleigh channels. As seen in the figure, the GL capacity is very close to 16-QAM capacity. At 1×10^{-4} BER levels, BIPCM with GL performs 2.1 dB away from the AWGN capacity and for Rayleigh channels the gap is around 2.2 dB for the block-length 2048 bits.

The performance of BIPCM is compared with the results for systematic RA code-based and LDPC-based BICM presented in [28]. These codes have block length $N = 2000$, rate $R = 0.5$ and use GL as mapping and are randomly constructed with constant column and row weight 3. For decoding belief propagation algorithm with maximum iteration number 100 is adopted.

Investigating Fig. 4.5 we observe that the performance of RA-based BICM is slightly better than LDPC-based BICM. However, RA-based BICM shows an error floor just above $1x10^{-5}$ and LDPC-based BICM seems to be free of error floor for the

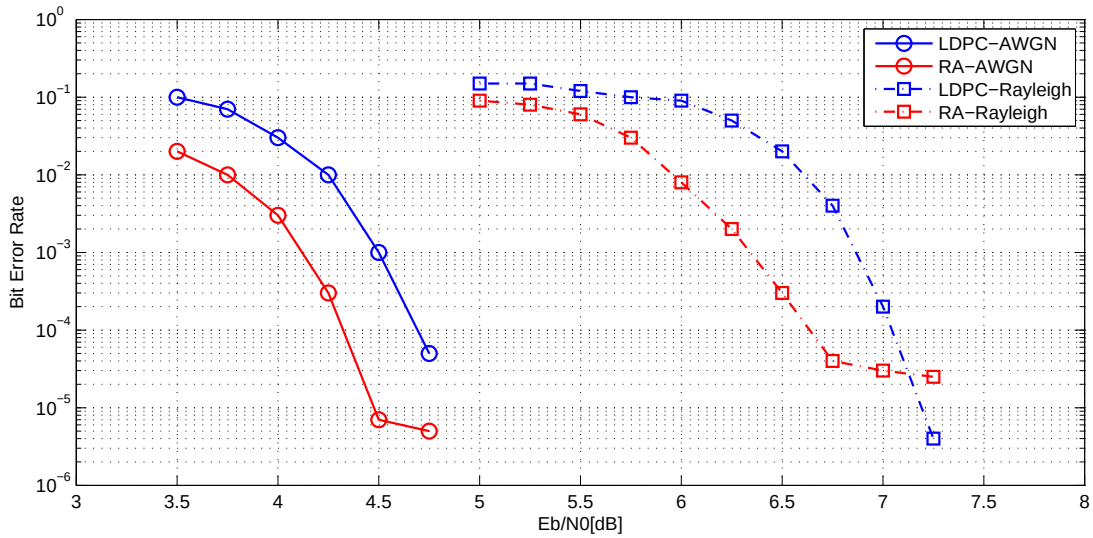

Figure 4.5. Performance of RA and LDPC based BIPCM. Curves are taken from [28].

considered bit-error probability range.

Table I gives a performance comparison between BIPCM and the results presented in [28], where E_b/N_0 values needed to reach a BER $= 1 \times 10^{-4}$ are given for different codes. Table I clearly shows the performance advantage of BIPCM for the proposed set-up. In AWGN channel, the performance improvement of BIPCM is 0.2 dB and 0.6 dB compared to RA- and LDPC-based BICM, respectively. In Rayleigh channel, BIPCM outperforms RA- and LDPC-based BICM by 0.4 dB and 0.8 dB, respectively.

4.5. Discussion

A polar coding scheme for BICM is proposed. A low complexity code construction method which is based on a generalization of Arıkan's heuristic method in [15] is adopted. To get the best performance from polar codes, SCLD with CRC is employed. A lower complexity and robust implementation of SCLD is explained. Performance of BIPCM is compared to some existing codes such as LDPC, and it is shown that polar codes provide significant performance benefits in conjunction with BICM for moderate block lengths.

We note that no mathematical formulations exist on how to choose the CRC or

Table 4.1. Performance of BICM with different codes.

	E_b/N_0 [dB] at BER $= 1 \times 10^{-4}$		
	Polar	RA	LDPC
AWGN	4.1	4.3	4.7
Rayleigh	6.2	6.6	7.0

its size in SCLD. Obtaining them or having design guidelines for CRC choice is an important open problem.

5. POLAR CODES WITH HIGHER ORDER MEMORY

In this chapter, we explain the design of a set of code sequences $\{\mathcal{C}_n^{(m)} : n \geq 1, m \geq 1\}$, with memory order m and code-length $N = O(\phi^n)$, where $\phi \in (1, 2]$ is the largest real root of the polynomial equation $F(m, \rho) = \rho^m - \rho^{m-1} - 1$ and ϕ is decreasing in m. $\{\mathcal{C}_n^{(m)}\}$ is based on the channel polarization idea, where $\{\mathcal{C}_n^{(1)}\}$ coincides with the polar codes presented by Arıkan. We show that $\{\mathcal{C}_n^{(m)}\}$ also achieves the symmetric capacity, $I(W)$, of an arbitrary BDMC, W, for any fixed m and therefore we complement Arıkan's conjecture that channel polarization is in fact a general phenomenon. We show that $\{\mathcal{C}_n^{(m)}\}$ offers complexity benefits compared to the original codes as its encoding and decoding complexities decrease with growing m. We obtain an achievable bound on the probability of block-decoding error, P_e, of $\{\mathcal{C}_n^{(m)}\}$ and showed that $P_e = O(2^{-N^\beta})$ is achievable for $\beta < \frac{\phi-1}{1+m(\phi-1)}$.

5.1. Motivation

Recalling Arıkan's polar codes in Chapter 2, consider the vector channel, $W_n : \mathcal{X}^N \to \mathcal{Y}^N$, $N = 2^n$, $n \geq 1$, obtained at channel combining level n. The vector channel, W_n, is obtained from W_{n-1} in a recursive manner where one first injects an independent realization of W_{n-1}, denoted as $\bar{W}_{n-1}$, and then combines the input of W_{n-1} and $\bar{W}_{n-1}$ to obtain W_n, where the recursion starts with $W_0 = W$. The injection of $\bar{W}_{n-1}$, in a way, creates $N/2$ diversity paths for the $N/2$ inputs of W_{n-1}, and this allows polarization which one sees in the synthesized binary-input channels obtained by splitting W_n. Consequently, at each combining level the code-length doubles with respect to the previous step scaling as $N = 2^n$.

With higher order memory in channel polarization, let us write $N = N(n, m)$ to denote the code-length at channel combining level n and memory parameter m, $m \geq 1$, which we assume to be fixed. The vector channel, W_n, is obtained by combining the inputs of W_{n-1} with $\bar{W}_{n-m}$, where one chooses $W_0 = W_{-1} = \ldots = W_{1-m} = W$ to initiate the recursion. The number of binary-inputs in W_{n-1} and $\bar{W}_{n-m}$ are $N(n-1)$

and $N(n-m)$, respectively. In turn, with the controlled memory parameter, m, and at channel combining level n, one only injects $N(n-m)$ new diversity paths with $\bar{W}_{n-m}$, for the $N(n-1)$ inputs of W_{n-1}, to obtain W_n. Because $N(n-m)$ gets smaller compared to $N(n-1)$ as m increases, it is possible to slow the speed at which one inject new channels to provide polarization. At first glance, it seems that increasing m will decrease the polarization effect obtained after each combining and splitting stage, however it will also allow the code-length to increase less rapidly in n. In order to see this consider the code-length obeying the recursion

$$N = N(n-1) + N(n-m), \quad n \geq 1, m \geq 1, \tag{5.1}$$

with initial conditions

$$N(0) = N(-1) = \ldots = N(1-m) = 1, \quad m \geq 1. \tag{5.2}$$

As will be explained in the sequel, the code-length takes the form

$$N = O(\phi^n), \quad n \geq 1 \tag{5.3}$$

where $\phi \in (1, 2]$ is the largest real root of the m-th order polynomial equation

$$F(m, \rho) = \rho^m - \rho^{m-1} - 1, \tag{5.4}$$

and ϕ decreases with increasing m. Therefore, if we increase m, it will take more channel combining and splitting stages to reach a pre-defined code-length, where the ratio of injected diversity paths to existing paths in each combining stage will also decrease. The aim of this chapter is to understand the effects of this trade-off on the polarization performance one can obtain at a fixed code-length N, as well as on the complexities of encoding and decoding.

In [21] Korada *et al.* generalize the channel polarization idea where $\ell \geq 2$ inde-

pendent uses of W_{n-1} are arbitrarily combined to obtain W_n and code-length scales as $N = \ell^n$. Although the channel combining mechanism is generalized to combining arbitrary numbers of W_{n-1} to obtain W_n, this setup has also first order memory in the channel combining. The authors express the combining mechanism by an $\ell \times \ell$ polarization kernel $\mathbf{K}$. With an arbitrary $\mathbf{K}$, the encoding matrix takes the form $\mathbf{G}_n = \mathbf{K}^{\otimes n}$. The asymptotic polarization performance is characterized by the distance properties of the rows of $\mathbf{K}$. Our work differs from [21] in the sense that by introducing higher order memory we modify the channel combining process. Moreover the encoding matrix of polar codes with memory $m > 1$ can not be obtained by applying Kronecker power to an arbitrary polarization kernel. As a result, one needs new mathematical tools to investigate β.

5.2. Recursive Channel Transformations

5.2.1. Channel Combining

Consider an arbitrary B-DMC, W, where its N independent uses take the form $W(\mathbf{y}_N|\mathbf{x}_N) = \prod_{i=1}^{N} W(y_i|x_i)$, $\mathbf{x}_N \in \mathcal{X}^N$, $\mathbf{y}_N \in \mathcal{Y}^N$. Let $\mathbf{u}_N \in \mathcal{X}^N$ be the binary information vector that needs to be transmitted over N uses of W. Channel combining phase creates a vector channel $W_n : \mathcal{X}^N \to \mathcal{Y}^N$ of the form

$$W_n(\mathbf{y}_N|\mathbf{u}_N) = \prod_{i=1}^{N} W(y_i|x_i),$$

where $\mathbf{x}_N = \mathbf{u}_N\mathbf{G}_N$. $\mathbf{G}_N$ is an $N \times N$ encoding matrix where encoding takes place in GF(2).

Let $\mathbb{N}_n = \{1, 2, \ldots, N\}$, $N = O(\phi^n)$, denote the set of the indices at the channel combining level n. There are N binary-input channels in W_n to transmit information. We index those channels as $W_n^{(i)}$, $i \in \mathbb{N}_n$, and demonstrate the channel combining operations in Fig 5.1. Inspecting this figure observe that we index the topmost binary-input channel of W_n as $W_n^{(1)}$ and index i of $W_n^{(i)}$ increases as one move downwards.

The vector channel W_n is obtained by combining W_{n-1} with $\bar{W}_{n-m}$. To accomplish this combining we apply XOR operations on the binary-inputs of W_n and transmit the resultant bits through the inputs of W_{n-1} and $\bar{W}_{n-m}$. By continuing the same recursion within W_{n-1} and $\bar{W}_{n-m}$, the encoded bits are transmitted through independent uses of W channels because we start the combining recursion by choosing $W_0 = W_{-1} = \ldots = W_{1-m} = W$. If we use the binary-input channels $W_n^{(1)}, W_n^{(2)}, \ldots, W_n^{(N)}$ to transmit the symbols $u_1, u_2, \ldots, u_N$, respectively, the encoding matrix $\mathbf{G}_n$ can be expressed as

$$\mathbf{G}_n = \left[\begin{array}{c|c} \mathbf{G}_{n-1} & \begin{matrix}\mathbf{G}_{n-m}\\ \mathbf{0}_2\end{matrix} \\ \hline \mathbf{0}_1 & \mathbf{G}_{n-m} \end{array}\right], \quad n \geq 1 \tag{5.5}$$

where $\mathbf{G}_0 = \mathbf{G}_{-1} = \ldots = \mathbf{G}_{1-m} = [1]$, and $\mathbf{0}_1$ and $\mathbf{0}_2$ are $N(n-m) \times N(n-1)$ and $(N(n-1) - N(n-m)) \times N(n-m)$ all zero matrices, respectively. Observe that when $m = 1$, $\mathbf{0}_2$ matrix vanishes and $\mathbf{G}_n$ can be represented as $\mathbf{G}_n = (\mathbf{F}^{\intercal})^{\otimes n}$, where $\mathbf{F} = \left[\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right]$ is the Kernel used by Arıkan in [13]. However, when $m > 1$, $\mathbf{G}_n$ can not be represented via Kronecker power.

5.2.2. Channel Ordering

After performing channel combining operation we have to define an order to split the vector $W_n : \mathcal{X}^N \to \mathcal{Y}^N$ and obtain N binary-input channels. This ordering is carried out with the help of a permutation $\pi_n : \mathbb{N}_n \to \mathbb{N}_n$. The $W_n^{(i)}$ channels in W_n are split in increasing $\pi_n(i)$ values (from 1 to N) so that each $W_n^{(i)}$ channel is of the form $W_n^{(i)} : \mathcal{X} \to \mathcal{Y}^N \times \mathcal{X}^{\pi(i)-1}$. In order to explain this operation we associate a unique state vector $\mathbf{s}_n^{(i)}$ with each $W_n^{(i)}$ channel, which has the form

$$\mathbf{s}_n^{(i)} = (s_1^{(i)}, s_2^{(i)}, \ldots, s_n^{(i)}),$$

where

$$\mathbf{s}_k^{(i)} \in \{+, -, \bigstar\}, \quad k = 1, 2, \ldots, n$$

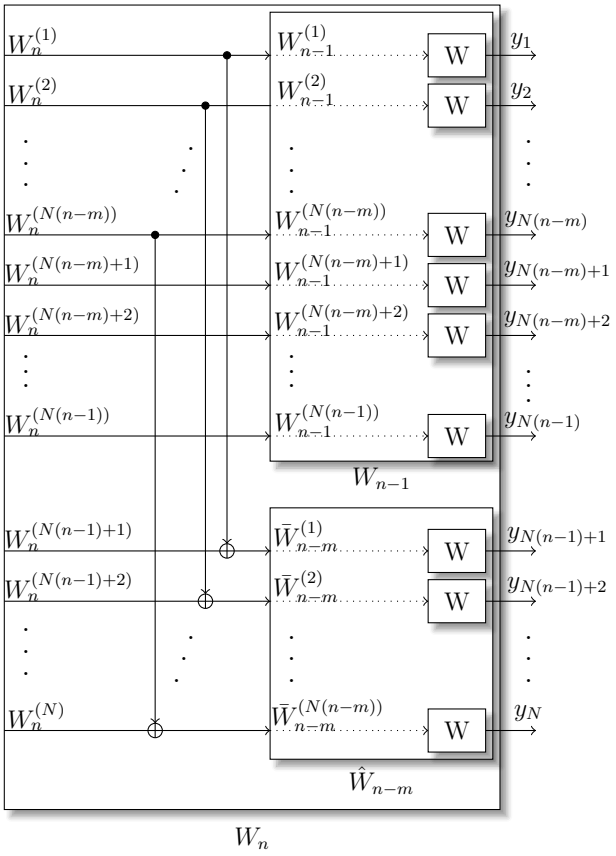

Figure 5.1. Recursive construction of the vector channel W_n from W_{n-1} and $\hat{W}_{n-m}$.

$s_k^{(i)}$ terms will be referred as a "state" and we use $+, -, \bigstar$ symbols to track down the channel transformations that $W_n^{(i)}$ channels undergo as $n = 1, 2, \ldots$. States $+$, $-$ will correspond to the polarization transforms $\boxplus$ and $\boxminus$, as defined in (1.5) and (1.6), respectively; whereas state $\bigstar$ will correspond to a non-polarizing transform. We let

$$\mathcal{S}_n = \{\mathbf{s}_n^{(i)} : i \in \mathbb{N}_n\} \tag{5.6}$$

to be the set of all possible state vectors at level n. Since each $\mathbf{s}_n^{(i)} \in \mathcal{S}_n$ is unique (as we will show shortly) we have $|\mathcal{S}_n| = N$ and $\mathcal{S}_n \subset \{+, -, \bigstar\}^n$. The vectors, $\mathbf{s}_n^{(i)} \in \mathcal{S}_n$, are assigned recursively from $\mathbf{s}_{n-1}^{(j)} \in \mathcal{S}_{n-1}$, with a state assigning procedure $\varphi_n : \mathcal{S}_{n-1} \to \mathcal{S}_n$. The operation of φ_n is explained in the following definition.

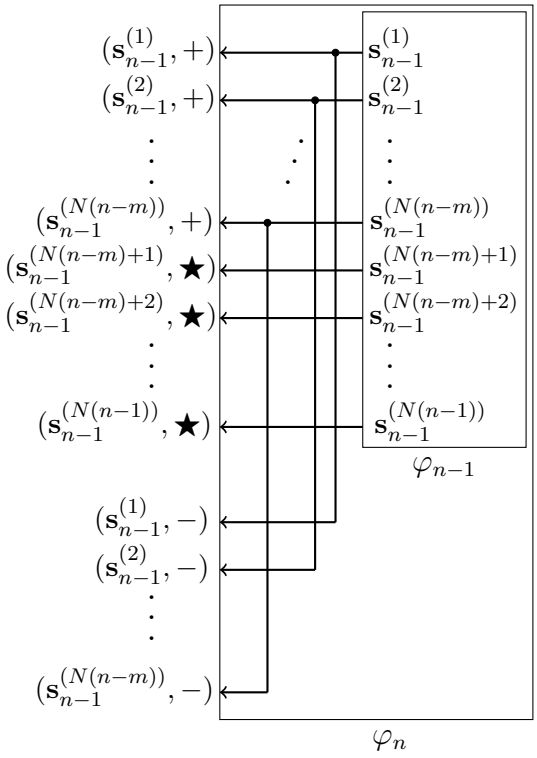

Figure 5.2. State labeling procedure $\varphi_n : \mathcal{S}_{n-1} \to \mathcal{S}_n$. State vectors $\mathbf{s}_n^{(i)} \in \mathcal{S}_n$, are obtained by appending a new state $\{+, -, \bigstar\}$, to the vectors $\mathbf{s}_{n-1}^{(j)} \in \mathcal{S}_{n-1}$.

Definition 5.1. ***(State Vector Assigning Procedure)*** *Let $\boldsymbol{s}_{n-1}^{(j)} \in \mathcal{S}_{n-1}$ be the state vector of $W_{n-1}^{(j)}$. The state vectors $\boldsymbol{s}_n^{(i)} \in \mathcal{S}_n$, associated with $W_n^{(i)}$ take the form*

$$\begin{aligned} \boldsymbol{s}_n^{(j)} &= (\boldsymbol{s}_{n-1}^{(j)}, +), \\ \boldsymbol{s}_n^{(j+N(n-1))} &= (\boldsymbol{s}_{n-1}^{(j)}, -), \end{aligned} \qquad j \in \mathbb{N}_{n-m}, \tag{5.7}$$

$$\boldsymbol{s}_n^{(j)} = (\boldsymbol{s}_{n-1}^{(j)}, \bigstar), \qquad j \in \mathbb{N}_{n-1} \setminus \mathbb{N}_{n-m}. \tag{5.8}$$

Investigating the above definition, as also demonstrated in Fig. 5.2, we observe that φ_n appends a new state, $\{+, -, \bigstar\}$, to $\mathbf{s}_{n-1}^{(j)} \in \mathcal{S}_{n-1}$ in order to construct $\mathbf{s}_n^{(i)} \in \mathcal{S}_n$. For $j \in \mathbb{N}_{n-m}$, φ_n appends $+$ and $-$ to $\mathbf{s}_{n-1}^{(j)}$ to obtain $\mathbf{s}_n^{(j)}$ and $\mathbf{s}_n^{(j+N_{n-1})}$, respectively. For $j \in \mathbb{N}_{n-1} \setminus \mathbb{N}_{n-m}$, φ_n appends $\bigstar$ to $\mathbf{s}_{n-1}^{(j)}$ in order to construct $\mathbf{s}_n^{(j)}$. Because of the inherent memory in the combining procedure, it is difficult to obtain closed form expressions for $\mathbf{s}_n^{(i)}$, for any i and m. Nevertheless, with the above definition one can

recursively obtain $\mathbf{s}_n^{(i)}$, by applying $\varphi_1, \varphi_2, \ldots, \varphi_n$. With the following proposition, we give the formal structure of the possible state vector, $\mathbf{s}_n^{(i)}$, and thus the set $\mathcal{S}_n$.

Proposition 5.1. *Let $\boldsymbol{s}_n$, $\boldsymbol{s}_n \in \mathcal{S}_n$, be a valid state vector one can obtain after applying $\varphi_1, \varphi_2, \ldots, \varphi_n$. Only the transitions between s_k and s_{k+1}, $k = 1, 2, \ldots, n$, that are shown in the state transition diagram of Fig. 5.3 are possible, where the imposed initial condition is $s_1 \in \{+, -\}$.*

Proof. Proof follows as a direct consequence of the channel combining and state vector assigning procedure, φ_n, and it can be verified by induction through stages $\varphi_1, \varphi_2, \ldots, \varphi_n$. □

Proposition 5.2. *The state vector $\boldsymbol{s}_n^{(i)} \in \mathcal{S}_n$, $i \in \mathbb{N}_n$, assigned to each $W_n^{(i)} \in \mathcal{W}_n$ is unique.*

Proof. See Appendix. □

The above proposition will be crucial for the ongoing analysis as it states that each $W_n^{(i)}$ is uniquely addressable by $\mathbf{s}_n^{(i)}$. We will use this fact to obtain the ordering π_n. Before accomplishing this, we obtain binary vectors $\mathbf{b}_n^{(i)} = (b_1^{(i)}, b_2^{(i)}, \ldots, b_n^{(i)})$, $b_k^{(i)} \in \mathcal{X}$, $k = 1, 2, \ldots, n$, from $\mathbf{s}_n^{(i)}$, which will allows us to sort and provide an order. The mapping between $\mathbf{s}_n^{(i)}$ and $\mathbf{b}_n^{(i)}$ is obtained as

$$b_k^{(i)} = \begin{cases} 0 & \text{if} \quad s_k^{(i)} \in \{-, \bigstar\}, \\ 1 & \text{if} \quad s_k^{(i)} = +, \end{cases} \qquad k = 1, 2, \ldots, n. \tag{5.9}$$

We notice that although both $s_k^{(i)} = -$ and $s_k^{(i)} = \bigstar$ are mapped as $b_k^{(i)} = 0$, the $\mathbf{b}_n^{(i)}$ vectors will also be unique for each i because every state $-$ in $\mathbf{s}_n^{(i)}$ is followed by $m-1$ occurrences of state $\bigstar$, and the distinction between different $\mathbf{s}_n^{(i)}$ is hidden in the location of $+$ states in $\mathbf{s}_n^{(i)}$. The following definition uses this uniqueness property to obtain the ordering, π_n. It is an adaptation of the bit-reversed order of Arıkan in [13] to the proposed coding scheme.

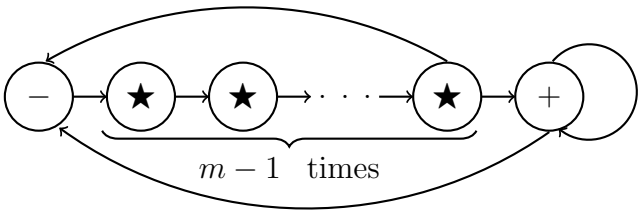

Figure 5.3. Possible state transitions observed between s_k and s_{k+1}, $k = 1, 2, \ldots, n$.

Definition 5.2. ***(Bit-Reversed Order)*** *Let $(\boldsymbol{b}_n^{(i)})_2$ denote value of $\boldsymbol{b}_n^{(i)}$ in Mod-2 as $(b_1^{(i)}, b_2^{(i)}, \ldots, b_n^{(i)})_2$ where $b_1^{(i)}$ is the most significant bit. The uniqueness of $\boldsymbol{b}_n^{(i)}$ for each i ensures the existence of a permutation $\pi_n : \mathbb{N}_n \to \mathbb{N}_n$, so that for some $i, j \in \mathbb{N}_n$, we have $\pi_n(i) < \pi_n(j)$ if $(\boldsymbol{b}_n^{(i)})_2 < (\boldsymbol{b}_n^{(j)})_2$.*

Therefore the bit-reversed order π_n is obtained in terms of increasing $(\mathbf{b}_n^{(i)})_2$ values. Notice that the binary input channels $\bar{W}_{n-m}^{(j)}$, $j \in \mathbb{N}_{n-m}$, of Fig. 5.1 have no effect in the recursive state assigning procedure, φ_n, and thus in the bit-reversed order. Their sole purpose is to provide auxiliary channels for the combining process. In fact, the $N(n-m)$ inputs of $\bar{W}_{n-m}$ can be combined with the $N(n-1)$ inputs of $\bar{W}_{n-1}$ in $\frac{N(n-1)!}{N(n-m)!}$ different ways. However, we deliberately align the inputs of W_{n-1} and $\hat{W}_{n-m}$ so that the first $N(n-m)$ inputs of W_{n-1} are combined, respectively, with the the first $N(n-m)$ inputs of $\bar{W}_{n-m}$ as shown in Fig. 5.1. This alignment in the combining process will be crucial in the next section when we investigate the evolution of binary-input channels in a probabilistic setting, because the channel pairs, $W_{n-1}^{(j)}$ and $\bar{W}_{n-m}^{(j)}$, share the same state history as explained in the following proposition.

Proposition 5.3. *Let $\boldsymbol{s}_{n-1}^{(j)} = (s_1, s_2, \ldots, s_{n-1}) \in \mathcal{S}_{n-1}$ be the state vector of $W_{n-1}^{(j)}$. Channel $\hat{W}_{(n-m)}^{(j)}$ shares the same state history with $W_{(n-1)}^{(j)}$, through combining stages $1, 2, \ldots, n-m$, in the sense that its state vector is $\boldsymbol{s}_{n-m}^{(j)} = (s_1, s_2, \ldots, s_{n-m}) \in \mathcal{S}_{n-m}$.*

Proof. See Appendix. □

5.2.3. Channel Splitting

We assume a genie-aided decoding mechanism where the $W_n^{(i)}$ channels are decoded successively in increasing $\pi_n(i)$ values, from 1 to N, and the genie provides the true values of already decoded bits. The decoder has no knowledge of the future bits that it will decode. With these assumptions $W_n^{(i)}$ is the effective bit-channel that this genie-aided decoder faces while trying to decode its next bit. Let us define $u_n^{(i)} \in \mathcal{X}$ as

$$u_n^{(i)} = \text{binary input of the channel } W_n^{(i)},$$

and for $i, j \in \mathbb{N}_n$ let

$$\begin{aligned} \mathbf{u}_{n,b}^{(i)} &\triangleq (u_n^{(j)} : \pi_n(j) < \pi_n(i)), \\ \mathbf{u}_{n,a}^{(i)} &\triangleq (u_n^{(j)} : \pi_n(j) > \pi_n(i)). \end{aligned} \tag{5.10}$$

$\mathbf{u}_{n,b}^{(i)}$ and $\mathbf{u}_{n,a}^{(i)}$ are the information vectors that are decoded, by the genie-aided decoder, before and after $u_n^{(i)}$, respectively. The length of $\mathbf{u}_{n,b}^{(i)}$ is $\pi_n(i) - 1$ and the length of $\mathbf{u}_{n,a}^{(i)}$ is $N - \pi_n(i)$ so that $\mathbf{u}_{n,b}^{(i)} \in \mathcal{X}^{\pi_n(i)-1}$ and $\mathbf{u}_{n,a}^{(i)} \in \mathcal{X}^{N_n - \pi_n(i)}$. The following definition formalizes the transition probabilities of the $W_n^{(i)}$ channels.

$$W_n^{(i)} \triangleq \sum_{\mathbf{u}_{n,a}^{(i)}} \Pr\left(\mathbf{y}_N, \mathbf{u}_{n,a}^{(i)}, \mathbf{u}_{n,b}^{(i)} | u_n^{(i)}\right). \tag{5.11}$$

The above definition indicates that $W_n^{(i)}$ is the posterior probability of an arbitrary B-DMC obtained at channel combining and splitting level n. The genie-aided decoder has no knowledge of $\mathbf{u}_{n,a}^{(i)}$, therefore it averages the joint probability of all outputs and all inputs over $\mathbf{u}_{n,a}^{(i)}$ and takes $\mathbf{y}_N$ and $\mathbf{u}_{n,b}^{(i)}$ as the effective output (observation) of the combined channels. Hence each $W_n^{(i)}$ has input $u_n^{(i)} \in \mathcal{X}$ and output $(\mathbf{y}_N, \mathbf{u}_{n,b}^{(i)}) \in \mathcal{Y}^N \times \mathcal{X}^{\pi_n(i)-1}$.

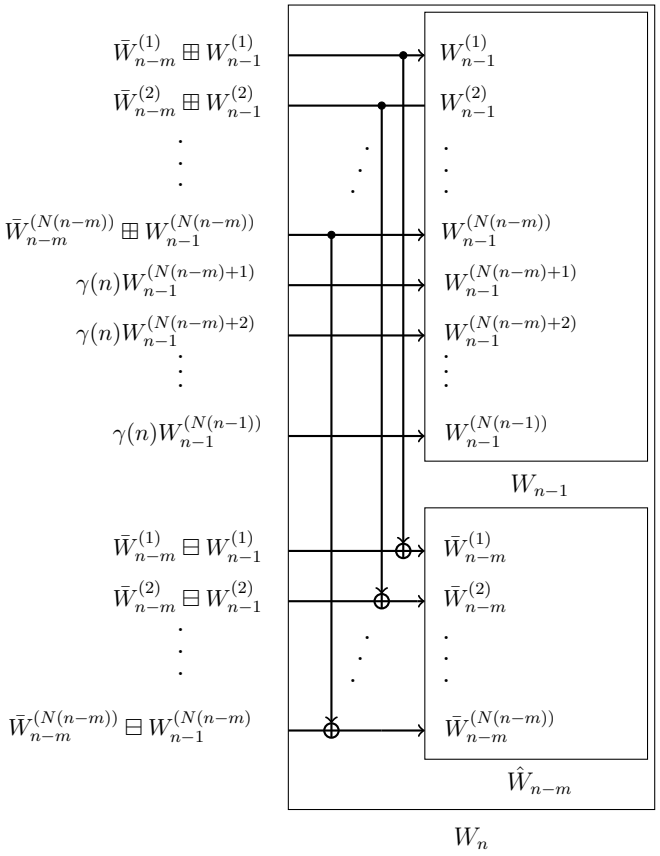

Figure 5.4. Transition probabilities of $W_n^{(i)}$ channels after combining and splitting W_{n-1} and $\bar{W}_{n-m}$.

Proposition 5.4. *The transition probabilities of $W_n^{(i)}$ channels take the following forms*

$$\left.\begin{aligned} W_n^{(j)} &= \bar{W}_{n-m}^{(j)} \boxplus W_{n-1}^{(j)}, \\ W_n^{(j+N_{n-1})} &= \bar{W}_{n-m}^{(j)} \boxminus W_{n-1}^{(j)}, \end{aligned}\right\} \quad j \in \mathbb{N}_{n-m}, \tag{5.12}$$

$$W_n^{(j)} = \gamma(n) W_{n-1}^{(j)}, \qquad j \in \mathbb{N}_{n-1} \setminus \mathbb{N}_{n-m}, \tag{5.13}$$

where $\gamma(n) = \Pr(y_{N(n-1)+1}, y_{N(n-1)+2}, \ldots, y_N)$ and $W_0 = W_{-1} = \ldots = W_{1-m} = W$.

In order to provide a proof for the above proposition and explain the underlying idea behind the bit-reversed order we make the following analysis. Investigating Fig. 5.4, we see that the overall effect of XOR operations, after channel splitting, is to provide diversity paths for the $N(n-m)$ inputs of W_{n-1} in the sense that for $j \in \mathbb{N}_{n-m}$ we have $W_n^{(j)} = \bar{W}_{n-m}^{(j)} \boxplus W_{n-1}^{(j)}$. Therefore the input of $W_n^{(j)}$ is transmitted through

both $\bar{W}_{n-m}^{(j)}$ and $\bar{W}_{n-m}^{(j)}$. Notice that in order to provide this diversity, the inputs of $W_n^{(j+N_{n-1})}$ must be decoded, by the genie-aided decoder, before the inputs of $W_n^{(j)}$ indicating $\pi_n(j) > \pi_n(j + N(n-1))$ must hold. Thanks to the bit-reversed order, as explained in Definition. 5.2, this requirement can be easily accomplished. To see this consider the state vectors $\mathbf{s}_{n-1}^{(j)}$ of $W_{n-1}^{(j)}$ to which one appends + and − in order to construct $\mathbf{s}_n^{(j)}$ and $\mathbf{s}_n^{(j+N(n-1))}$, respectively. After this operation, the mapping between $\mathbf{s}_n^{(i)}$ and $\mathbf{b}_n^{(i)}$, as given by (5.9), indicates that $\mathbf{b}_n^{(j)} = (\mathbf{b}_{n-1}^{(j)}, 1)$ and $\mathbf{b}_n^{(j+N(n-1))} = (\mathbf{b}_{n-1}^{(j)}, 0)$ holds. Therefore

$$(\mathbf{b}_n^{(j)})_2 > (\mathbf{b}_n^{(j+N(n-1))})_2, \quad n = 1, 2, \ldots$$

and by Definition 5.2, $\pi_n(j) > \pi_n(j+N(n-1))$ holds for all $n \geq 1$. On the other hand, in order to decode $W_n^{(j+N_{n-1})}$ correctly, the inputs of $W_{n-1}^{(j)}$ and $\bar{W}_{n-m}^{(j)}$ must be decoded correctly indicating we must have $W_n^{(j+N(n-1))} = \hat{W}_{n-m}^{(j)} \boxminus W_{n-1}^{(j)}$. The above analysis, by induction through combining and splitting stages $1, 2, \ldots, n$ proves (5.12). In order to prove (5.13), we inspect that for $j \in \mathbb{N}_{n-1} \setminus \mathbb{N}_{n-m}$ the channel $W_n^{(j)}$ is as good as $W_{n-1}^{(j)}$ in the sense that the genie-aided decoder can always decode $W_{n-1}^{(j)}$ instead of $W_n^{(j)}$. Inspecting Fig. 5.4 we notice that the binary-input of $W_n^{(j)}$ is not transmitted through the inputs of $\bar{W}_{n-m}$. Therefore, the combining of $\bar{W}_{n-m}$ with W_{n-1} does not provide any new information regarding the input of $W_n^{(j)}$. This, in turn, indicates that $W_n^{(j)}$ is the same as $W_{n-1}^{(j)}$ except for a scaling factor $\gamma(n)$, as in (5.13).

5.2.4. Effects of Channel Combining and Splitting on the Symmetric Capacity

Let us define $I_n^{(i)} = I(W_n^{(i)})$ and analyze the implications of Proposition 5.4. Equation (5.12) states that the channel pairs, $\bar{W}_{n-m}^{(j)}$ and $W_{n-1}^{(j)}$, $j \in \mathbb{N}_{n-m}$, undergo a polarization transform, $\boxminus$ and $\boxplus$, from which two new channels, $W_n^{(j)}$ and $W_n^{(j+N_{n-1})}$, emerge. In the light of (1.10) we have

$$I_n^{(j)} \geq \max\{I_{n-1}^{(j)}, I_{n-m}^{(j)}\}, \quad j \in \mathbb{N}_{n-m}. \tag{5.14}$$

Therefore, the injection of $\bar{W}_{n-m}^{(j)}$ allows $W_n^{(j)}$ to be superior channel compared to $\bar{W}_{n-m}^{(j)}$ and $W_{n-1}^{(j)}$. This comes with the expense that now $W_n^{(j+N(n-1)}$ is an inferior channel compared to $\bar{W}_{n-m}^{(j)}$ and $W_{n-1}^{(j)}$ because, from (1.11), one has

$$I_n^{(j+N(n-1))} \leq \min\{I_{n-1}^{(j)}, I_{n-m}^{(j)}\}, \quad j \in \mathbb{N}_{n-m}. \tag{5.15}$$

Although $I_n^{(j)}$ and $I_n^{(j+N(n-1))}$ move away from $I_{n-1}^{(j)}$ and $I_{n-m}^{(j)}$, the transformations preserve the symmetric capacity because, as indicated by (1.9), we have

$$I_n^{(j)} + I_n^{(j+Nn-1)} = I_{n-1}^{(j)} + I_{n-m}^{(j)}, \quad j \in \mathbb{N}_{n-m}. \tag{5.16}$$

The remaining channels $W_n^{(j)}$, $j \in \mathbb{N}_{n-1} \backslash \mathbb{N}_{n-m}$, in Equation (5.13), do not see any polarization transforms as their transition probabilities are scaled by $\Pr(y_{N(n-1)+1}, \ldots, y_N)$ with respect to $W_{n-1}^{(j)}$. This scaling, in turn, results in

$$I_n^{(j)} = I_{n-1}^{(j)}, \quad j \in \mathbb{N}_{n-1} \setminus \mathbb{N}_{n-m}. \tag{5.17}$$

All in all, the combining and splitting of W_{n-1} and W_{n-m} preserves the sum symmetric capacity as

$$\sum_{i \in \mathbb{N}_n} I_n^{(i)} = \sum_{j \in \mathbb{N}_{n-1}} I_{n-1}^{(j)} + \sum_{k \in \mathbb{N}_{n-m}} I_{n-m}^{(k)}, \tag{5.18}$$

5.3. Decoding

We will take successive cancellation decoding (SCD) of [13] as the default decoding method for $\{\mathcal{C}_n^{(m)}\}$. The genie-aided decoder that we have explained in the previous section and the definition of $W_n^{(i)}$ as given by (5.11) already provide us a guideline for SCD. The only difference is, during the calculation of (5.11), SCD uses its own estimates for the vector $\mathbf{u}_{n,b}^{(i)}$.

Likelihood ratios (LRs) should be preferred in SCD so that one can eliminate the $P(y_{N_{n-1}+1}, y_{N_{n-1}+1}, \ldots, y_{N_n})$ term in (5.13). The LR for the channel $W_n^{(i)}$ is defined as

$$L_n^{(i)} \triangleq \frac{\sum_{\mathbf{u}_{n,a}^{(i)}} \Pr\left(\mathbf{y}_N, \mathbf{u}_{n,a}^{(i)}, \hat{\mathbf{u}}_{n,b}^{(i)} | 0\right)}{\sum_{\mathbf{u}_{n,a}^{(i)}} \Pr\left(\mathbf{y}_N, \mathbf{u}_{n,a}^{(i)}, \hat{\mathbf{u}}_{n,b}^{(i)} | 1\right)}.$$

By using the LR relations given in [13] for $\boxplus$ and $\boxminus$ transformations and from Proposition 5.4 we obtain

$$\begin{aligned} L_n^{(j)} &= L_{n-1}^{(j)} (\bar{L}_{n-m}^{(j)})^{1-2\hat{u}_n^{(j+N_{n-1})}}, \\ L_n^{(j+N_{n-1})} &= \frac{L_{n-1}^{(j)} \bar{L}_{n-m}^{(j)} + 1}{L_{n-1}^{(j)} + \bar{L}_{n-m}^{(j)}}, \qquad j \in \mathbb{N}_{n-m}, \end{aligned} \tag{5.19}$$

$$L_n^{(j)} = L_{n-1}^{(j)}, \qquad j \in \mathbb{N}_{n-1} \setminus \mathbb{N}_{n-1}. \tag{5.20}$$

Therefore, while decoding $W_n^{(i)}$ one only needs to calculate $2N(n-m)$ LRs as given by (5.19) while the remaining $N - N(n-m)$ LRs for (5.20) are the same as the previous level. This fact can be exploited to avoid unnecessary decoding complexity in hardware implementation.

5.4. Code-Length

Recall that the code-length $N = N(n, m)$ obeys the recursion in (5.1) with initial conditions of (5.2). It is easy to show that N can be calculated as

$$N = \sum_{i=1}^{m} c_i (\rho_i)^n, \tag{5.21}$$

where each ρ_i, $i = 1, 2, \ldots, m$, is a root of the mth order polynomial equation

$$F(m, \rho) = \rho^m - \rho^{m-1} - 1, \tag{5.22}$$

and constants, c_i, are calculated by using the initial conditions in (5.2) together with (5.21).

Proposition 5.5. *For $m \geq 1$, let $\phi \in (1, 2]$ be a real root of $F(m, \rho)$.*

(i) ϕ is unique, i.e., there is only one real root in $\in (1, 2]$.

(ii) If $\rho_i \neq \phi$ we have $\sqrt{\rho_i \rho_i^*}/\phi < 1$ indicating ϕ is the the largest magnitude root of $F(m, \rho)$.

(iii) ϕ is decreasing in increasing m.

Proof. See Appendix. □

Part *ii* of the above proposition indicates that, as n gets large, the summation in (5.21) will be dominated by ϕ^n term therefore the code-length will scale as $N = \kappa\phi^n = O(\phi^n)$ where $\kappa > 0$ is the constant scaler of ϕ^n in (5.21). Part *iii* of Proposition 5.5 implies that as m increases the code-length increases less rapidly in n which we have mentioned in the beginning of the paper.

5.5. Code Construction

The following proposition is a generalization of [13, Prop. 5] and it's proof is omitted.

Proposition 5.6. *If W is a BEC then $W_n^{(i)}$ channels, obeying the transition probabilities as given by Proposition 5.4, are also BECs.*

In order to use $\{\mathcal{C}_n^{(m)}\}$ one has to fix a code parameter vector $(W, N, K, \mathcal{A})$, where W is the underlying B-DMC, N is the code-length, K is the dimensionality of the code, and $\mathcal{A} \subseteq \mathbb{N}_n$ is the set of information carrying symbols. We have $|\mathcal{A}| = K$ and $K/N = R$, where $R \in [0, 1]$ is the rate of the code.

Let $P_{e,n}^{(i)}$, $i \in \mathbb{N}_n$, denote the bit-error probability of $W_n^{(i)}$ with SCD. Code construction problem is choosing the set $\mathcal{A}$ so that $\sum_{i \in \mathcal{A}} P_{e,n}^{(i)}$ is minimum. This problem can be analytically solved only when W is a BEC [13] since for this case the $W_n^{(i)}$ channels are also BECs (Proposition 5.6) and the Bhattacharyya parameters, $Z_n^{(i)}$, obey

$P_{e,n}^{(i)} = Z_n^{(i)}$. In this case, in the light of (1.12)-(1.13) and Proposition 5.4, $Z_n^{(i)}$ terms can be recursively calculated as

$$\begin{aligned} Z_n^{(j)} &= Z_{n-1}^{(j)} Z_{n-m}^{(j)}, \\ Z_n^{(j+N_{n-1})} &= Z_{n-1}^{(j)} + Z_{n-m}^{(j)} - Z_{n-1}^{(j)} + Z_{n-m}^{(j)}, \qquad j \in \mathbb{N}_{n-m}, \\ Z_n^{(j)} &= Z_{n-1}^{(j)} \qquad\qquad\qquad j \in \mathbb{N}_{n-1} \setminus \mathbb{N}_{n-1}. \end{aligned}$$

5.6. Channel Polarization

Channel polarization should be investigated by observing the evolution of the set $\{W_n^{(i)} : i \in \mathbb{N}_n\}$ as n increases. To track this evolution we use the state vectors $\mathbf{s}_n^{(i)} \in \mathcal{S}_n$ assigned to $W_n^{(i)}$ because each $W_n^{(i)}$ is uniquely addressable by its $\mathbf{s}_n^{(i)}$.

5.6.1. Probabilistic Model for Channel Evolution

We define a random process $\{S_n\}$ and a random vector $\mathbf{S}_n = (S_1, S_2, \ldots, S_n)$ obtained from the process $\{S_n\}$ where the state vectors, $\mathbf{s}_n = (s_1, s_2, \ldots, s_n)$, $\mathbf{s}_n \in \mathcal{S}_n$ are the realizations of $\mathbf{S}_n$. The process $\{S_n\}$ can be regarded as a tree process where $\mathbf{s}_n$ form the branches of the tree where we illustrate it in Fig 5.5 for the case $m = 2$. Since $|\mathcal{S}_n| = N = N(n)$, there are $N(n)$ different branches at tree level n. The process $\{S_n\}$ starts with the initial conditions $S_1 \in \{+, -\}$. At tree level n, $N(n)$ new branches emerge from $N(n-1)$ branches of level $n-1$. We assume that each branch is observed with identical probability

$$\Pr(\mathbf{S}_n = \mathbf{s}_n) = \frac{1}{N(n)}. \tag{5.23}$$

This, in turn, implies that each valid state transition of Fig. 5.3, between s_{n-1} and s_n, has probability $N(n-1)/N(n)$. Investigating this figure, consider the case $m = 1$, which coincides with Arıkan's setup in [13], where there are two possible states as $S_n \in \{+, -\}$ and $|\mathcal{S}_n| = N(n) = 2^n$. Since transitions between S_{n-1} and S_n are

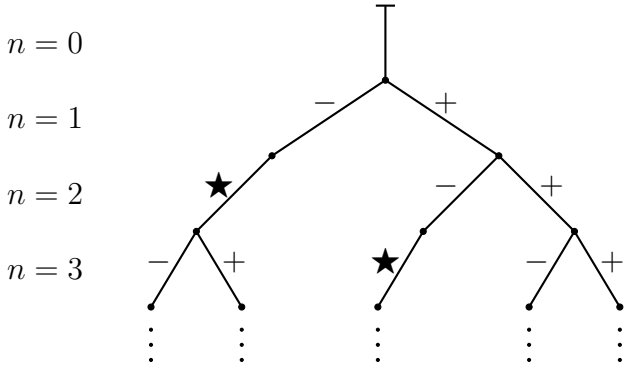

Figure 5.5. Illustration of the evolution of $\{S_n\}$ as a tree for the case $m = 2$, where each branch is a state vector $\mathbf{s}_n \in \mathcal{S}_n$.

valid if $S_n \in \{+, -\}$ and $S_{n-1} \in \{+, -\}$, each possible transition has probability $N(n-1)/N(n) = 1/2$. Consequently, the process $\{S_n\}$ is composed of independent realizations of Bernoulli(1/2) random variables as $\Pr(S_n = +) = \Pr(S_n = -) = 1/2$. On the other hand, when $m > 1$, there exists a memory in the state transition model as depicted in Fig. 5.3. Therefore, the process $\{S_n\}$ can be modeled as a Markov process with order $m - 1$ in the sense that

$$\mathbb{P}(S_n|\mathbf{S}_{n-1}) = \mathbb{P}(S_n|S_{n-1}, S_{n-2}, \ldots, S_{n-(m-1)}).$$

Throughout the paper we find it easier to work with the random vector $\mathbf{S}_n$ keeping in mind the Markovian property of the process $\{S_n\}$.

We define a random channel process $\{K_n\}$, driven by $\{S_n\}$, as $K_n = W_{S_1,S_2,\ldots,S_n}$. The realizations of K_n are $k_n = W_{s_1,s_2,\ldots,s_n}$ and they correspond to the binary-input channels, $W_n^{(i)}$, with state vectors $\mathbf{s}_n = (s_1, s_2, \ldots, s_n) \in \mathcal{S}_n$.

In order to obtain a characterization for the process $\{K_n\}$ we fix $(s_1, s_2, \ldots, s_{n-1})$ to be the state vector associated with $W_{n-1}^{(j)}$, $j \in \mathbb{N}_{n-m}$ and let $k_{n-1} = W_{n-1}^{(j)}$. In the light of Proposition 5.3, we know that the state vector of $\bar{W}_{n-m}^{(j)}$ is $(s_1, s_2, \ldots, s_{n-m})$ indicating $k_{n-m} = \hat{W}_{n-m}^{(j)}$. Investigating the operation of $\varphi_n : \mathcal{S}_{n-1} \to \mathcal{S}_n$ in Fig. 5.2, we observe that the state vectors of $W_n^{(j)}$ and $W_n^{(j+N_{n-1})}$ are $(s_1, s_2, \ldots, s_{n-1}, +)$ and $(s_1, s_2, \ldots, s_{n-1}, -)$, respectively. From Proposition 5.4 we notice that $W_n^{(j)} = \bar{W}_{n-m}^{(j)} \boxplus$

$W_{n-1}^{(j)}$ and $W_n^{(j+N(n-1))} = \bar{W}_{n-m}^{(j)} \boxminus W_{n-1}^{(j)}$ holds. These observations, in turn, indicate $k_n = k_{n-1} \boxplus k_{n-m}$ holds when $s_n = +$, and $k_n = k_{n-1} \boxminus k_{n-m}$ holds when $s_n = -$. Next, we fix $(s_1, s_2, \ldots, s_{n-1})$ to be the state vector associated with $W_{n-1}^{(j)}$, $j \in \mathbb{N}_{n-1} \setminus \mathbb{N}_{n-m}$ and hence $k_{n-1} = W_{n-1}^{(j)}$. From the operation of $\varphi_n : \mathcal{S}_{n-1} \to \mathcal{S}_n$ we know that the state vector of $W_n^{(j)}$ is $(s_1, s_, \ldots, s_{n-1}, \bigstar)$ and Proposition 5.4 tells us $W_n^{(j)} = \gamma(n) W_{n-1}^{(j)}$. Combining these facts tells us $k_n = \gamma(n) k_{n-1}$ holds if $s_n = \bigstar$. The above analysis relates k_n to k_{n-1} and k_{n-m} for all $s_n \in \{+, -, \bigstar\}$, which we formally present with the below recursion.

$$K_n = \begin{cases} K_{n-m} \boxplus K_{n-1} & \text{if} \quad S_n = +, \\ K_{n-m} \boxminus K_{n-1} & \text{if} \quad S_n = -, \\ \gamma(n) K_{n-1} & \text{otherwise,} \end{cases} \tag{5.24}$$

where $K_n = W$ for $n < 1$.

5.6.2. Polarization

We define the processes $\{I_n : n \geq 1\}$ and $\{J_n : n \geq 1\}$ where $I_n = I(K_n) \in [0, 1]$ and $J_n = J(K_n) \in [0, 1]$. In [13] Arıkan shows that I_n converges to a random variable I_∞ as $\Pr(I_\infty = 1) = I(W)$ and $\Pr(I_\infty = 0) = 1 - I(W)$. This result indicates that the synthesized binary-input channels, $W_n^{(i)}$, either become error-free or useless. We will show that the same holds for polar codes with higher order memory as well. This result is presented with the following theorem.

Theorem 5.1. *For any fixed $m \geq 1$ and for some $\delta \in (0, 1)$ as n tends to infinity, the probability of $I_n \in (1 - \delta, 1]$ goes to $I(W)$ and the probability of having $I_n \in [0, \delta)$ goes to $1 - I(W)$.*

Proof. We investigate the polarization of $\{J_n\}$ towards 0 and 1 as it will imply the polarization of $\{I_n\}$ as well. We write $E[J_n] = \frac{1}{N} \sum_{\mathbf{s}_n \in \mathcal{S}_n} J_n$ to denote the expected value of J_n and $\{E[J_n] : n \geq 1\}$ to denote the deterministic sequences obtained from $E[J_n]$. The following lemma will be crucial for the proof.

Lemma 5.1.

$$E[J_n] \geq \mu E[J_{n-1}] + (1-\mu)\, E[J_{n-m}], \tag{5.25}$$

where $\mu = N(n-1)/N(n)$ *and the above equality is achieved only if* $J_{n-1} \in \{0,1\}$ *or* $J_{n-m} \in \{0,1\}$ *holds for all* $S_n \in \{+,-\}$

Proof. See Appendix. □

We apply a decimation operation on the sequence $\{E[J_n]\}$ and obtain a subsequence $\{E[\hat{J}_k] : k = 1, 2, \ldots, \lfloor n/m \rfloor\}$, where the decimation operation is performed as

$$E[\hat{J}_k] = \min_{i \in \{0,1,\ldots,m-1\}} \{E[J_{km-i}]\}\,. \tag{5.26}$$

The elements of $\{E[\hat{J}_k]\}$ are obtained by choosing the minimum of m consecutive and non-overlapping elements of $\{E[J_n]\}$.

Lemma 5.2. *The sequence* $\{E[\hat{J}_k]\}$ *is monotonically increasing in the sense that*

$$E[\hat{J}_k] \geq E[\hat{J}_{k-1}].$$

Proof. See Appendix. □

We know that $E[\hat{J}_k]$ is bounded in $[0,1]$ and since $\{E[\hat{J}_k]\}$ is monotonically increasing, from the monotone convergence theorem [32, p. 21.] we conclude that there exists a unique limit for $\{E[\hat{J}_k]\}$ in the sense that

$$\lim_{k \to \infty} E[\hat{J}_k] = \sup\{E[\hat{J}_k]\}. \tag{5.27}$$

Next, we let $n = km - i$ in Lemma 5.1 to obtain

$$E[J_{km-i}] \geq \mu E[J_{km-(i+1)}] + (1-\mu)E[J_{(k-1)m-i}]. \tag{5.28}$$

We fix i such that $E[J_{km-i}] = E[\hat{J}_k]$ is satisfied. For any choice of i observe that $E[J_{(k-1)m-i)}] \geq E[\hat{J}_{k-1}]$ and $E[J_{km-(i+1)}] \geq \min\{E[\hat{J}_k], E[\hat{J}_{k-1}]\} \geq E[\hat{J}_{k-1}]$ hold. Using these results in (5.28) gives

$$E[\hat{J}_k] \geq \mu E[\hat{J}_{k-1}] + (1-\mu)E[\hat{J}_{k-1}] \geq E[\hat{J}_{k-1}] \tag{5.29}$$

Therefore, the monotonic increase in $E[\hat{J}_k]$ will continue until the inequality in Lemma 5.1 is achieved with equality. This fact, together with the convergence of $E[\hat{J}_k]$, indicates that conditioned on the event $\{S_n : S_n \in \{+,-\}\}$ either $\lim_{n\to\infty} J_{n-1} \in \{0,1\}$ or $\lim_{n\to\infty} J_{n-m} \in \{0,1\}$ holds, indicating

$$\lim_{n\to\infty} J_n \in \{0,1\}, \quad S_n \in \{+,-\}. \tag{5.30}$$

Investigating the operation of $\varphi_n : \mathcal{S}_{n-1} \to \mathcal{S}_n$ in Figure 5.2 we see that

$$\Pr\left(S_n \in \{+,-\}\right) = \frac{2N(n-m)}{N(n)} \geq 0, \tag{5.31}$$

which implies that the event $\{S_n : S_{n-1} \in \{+,-\}\}$ occurs infinitely many times as $n \to \infty$ and $\sum_{n\to\infty} \Pr\left(S_{n-1} \in \{+,-\}\right)$ diverges. Consequently, and by using the first Borel Contelli lemma [33, p. 36] we conclude that

$$\lim_{n\to\infty} \Pr(J_n \in \{0,1\}) = 1.$$

One to one correspondence between J_n and I_n implies

$$\lim_{n\to\infty} \Pr(I_n \in \{0,1\}) = 1,$$

and having $E[I_n] = I(W)$ results in

$$\lim_{n\to\infty} \Pr(I_n = 1) = I(W),$$

and

$$\lim_{n\to\infty} \Pr(I_n = 0) = 1 - I(W).$$

which completes the proof. □

5.6.3. A Typicality Result

In this section we use the Method of Types to investigate the state vectors, $\mathbf{s}_n$, obtained from the realizations of the process $\{S_n\}$. We let $s \in \{+, -, \bigstar\}$ and write $P_{\mathbf{s}_n}^{(s)}$, $P_{\mathbf{s}_n}^{(s)} \in [0, 1]$, to denote the type (frequency) of s in $\mathbf{s}_n$ as

$$P_{\mathbf{s}_n}^{(s)} = \#(\mathbf{s}_n|s)/n,$$

where $\#(\mathbf{s}_n|s)$ denotes the number times the symbol s occurs in $\mathbf{s}_n$. Investigating the state transition diagram of Fig. 5.3 we inspect that, as n gets large, $P_{\mathbf{s}_n}^{(\bigstar)} = (m-1)P_{\mathbf{s}_n}^{(-)}$ holds because each $-$ state in $\mathbf{s}_n$ is followed by $m-1$ occurrences of state $\bigstar$. As the remaining states in $\mathbf{s}_n$ will be $+$, we must have $P_{\mathbf{s}_n}^{(+)} = 1 - mP_{\mathbf{s}_n}^{(-)}$ indicating $P_{\mathbf{s}_n}^{(+)} \in [0, 1]$, $P_{\mathbf{s}_n}^{(-)} \in [0, \frac{1}{m}]$, and $P_{\mathbf{s}_n}^{(\bigstar)} \in [0, \frac{m-1}{m}]$. As it tuns out, depending on $P_{\mathbf{s}^n}^{(s)}$, not all realizations of $\{S_n\}$ are observed with the same probability. This is explained with the following theorem.

Theorem 5.2. *As n gets large, except for a vanishing fraction of $\boldsymbol{s}_n \in \mathcal{S}_n$, and for some $\epsilon \in (0, 1)$ we have*

$$|P_{\boldsymbol{s}^n}^{(-)} - p^-| \leq \epsilon,$$
$$|P_{\boldsymbol{s}^n}^{(+)} - p^+| \leq \epsilon,$$
$$|P_{\boldsymbol{s}^n}^{(\bigstar)} - p^\bigstar| \leq \epsilon,$$

where $p^- = \frac{\phi-1}{1+m(\phi-1)}$, $p^\bigstar = (m-1)p^-$ *and* $p^+ = 1 - mp^-$.

Therefore we can consider p^+, p^- and $p^\bigstar$ as the frequencies of states $+$, $-$, and $\bigstar$, in $\mathbf{s}_n$, respectively, that one typically observes as n gets large.

Proof. The proof is based on the Method of Types [20]. We let $q \in [0, 1/m]$ and define

$$\mathcal{T}_n^{(q)} = \{\mathbf{s}^n : P_{\mathbf{s}^n}^{(-)} = q\}. \tag{5.32}$$

$\mathcal{T}_n^{(q)}$ is a type class and it consists of $\mathbf{s}_n$ having $nq \in [0, n/m]$ occurrences of state $-$. For all $m \geq 1$, there are at most $n+1$ different such type classes. However, the number of all possible $\mathbf{s}_n$, $|\mathcal{S}_n|$, increases exponentially in n as $|\mathcal{S}_n| = N = O(\phi^n)$. The Method of Types ensures the existence of a type class with exponentially many elements. Our aim is to find this type class. Recalling that each $\mathbf{s}_n$ is observed with probability $1/N$, the probability of observing a given $\mathbf{s}_n$ in $\mathcal{T}_n^{(q)}$ is

$$\Pr\left(\mathbf{s}_n \in \mathcal{T}_q^n\right) = \frac{|\mathcal{T}_q^n|}{N}.$$

Lemma 5.3.

$$|\mathcal{T}_q^n| < 2^{n(G(m,q)+o(1))}. \tag{5.33}$$

where

$$G(m,q) = (1-(m-1)q))H\left(\frac{q}{1-(m-1)q}\right),$$

and H *is the binary entropy function.*

Proof. See Appendix. □

Investigating $G(m,q)$ we observe that it is a concave function of $q \in [0, 1/m]$. We

establish a similarity between $\frac{\partial G(m,q)}{\partial q}$ and $F(m,\rho)$ in (5.22). The following lemma is a direct consequence of this result.

Lemma 5.4. *The function $G(m,q)$ attains its maximum when $q = p^-$ and its maximum value is*

$$G(m,p^-) = \log\phi.$$

Proof. See Appendix. □

Consequently, for every $\mathcal{T}_n^{(q)}$ with $|q-p^-| > 0$ there exists a $D(q,p^-) > 0$ such that

$$\begin{aligned} D(q,p^-) &\triangleq G(m,p^-) - G(m,q), \\ &= \log\phi - G(m,q). \end{aligned}$$

Using the above fact in (5.33) results in

$$|\mathcal{T}_n^{(q)}| \leq \phi^n 2^{n\left(-D(q,p^-)+o(1)\right)}.$$

From the above result and the fact that $N = O(\phi^n)$ we obtain

$$\Pr(\mathbf{s}_n \in \mathcal{T}_n^{(q)}) \leq 2^{-n\left(D(q,p^-)+o(1)\right)}, \tag{5.34}$$

The above result shows that depending on $D(q,p^-)$, and in turn q, the probabilities of some type classes decay exponentially in n. The following proposition results from this fact.

Proposition 5.7. *As n tends to infinity $D(q,p^-)$ converges to 0 with probability 1.*

Proof. See Appendix. □

The above proposition implies the convergence of q to p^- as well, because $D(q, p^-)$ is 0 only if $q = p^-$. Therefore among all $T_n^{(q)}$, one observes the ones with $|q - p^-| \leq \epsilon$ with probability 1.

□

5.6.4. Rate of Polarization

We define the Bhattacharyya process $\{Z_n\}$ where $Z_n = Z(K_n)$ is the Bhattacharyya parameter of the random channel K_n. By using the channel evolution model in (5.24), this process can be expressed as

$$Z_n \begin{cases} = Z_{n-1}Z_{n-m} & \text{if } S_n = +, \\ \leq Z_{n-1} + Z_{n-m} - Z_{n-1}Z_{n-m} & \text{if } S_n = -, \\ = Z_{n-1} & \text{otherwise,} \end{cases} \tag{5.35}$$

where $Z_n = Z(W)$ for $n < 1$.

Theorem 5.3. *For any $\epsilon \in (0, 1)$ there exists an n such that for $\beta < p^+$ we have*

$$\Pr\left(Z_n \leq 2^{-\phi^{n\beta}}\right) \geq I(W) - \epsilon. \tag{5.36}$$

Proof. We consider another process $\{\hat{Z}_n\}$, driven by $\{S_n\}$, so that for $i = 1, 2, \ldots, n_0$, $n_0 < n$, we have $\hat{Z}_i = Z_i$ and for $i > n_0$, $\hat{Z}_i$ obeys

$$\hat{Z}_i = \begin{cases} \hat{Z}_{i-1}\hat{Z}_{i-m} & \text{if } S_n = +, \\ \hat{Z}_{i-1} + \hat{Z}_{i-m} - \hat{Z}_{i-1}\hat{Z}_{i-m} & \text{if } S_n = -, \\ \hat{Z}_{i-1} & \text{otherwise.} \end{cases} \tag{5.37}$$

Comparing (5.35) and (5.37) we observe that Z_n is stochastically dominated by $\hat{Z}_n$ in the sense that for some $f_n \in (0, 1)$, $\Pr(Z_n \leq f_n) \geq \Pr(\hat{Z}_n \leq f_n)$. For the proof it will

suffice to show that $\Pr(\hat{Z}_n \leq f_n) \geq I(W) - \epsilon$ holds for $f_n = 2^{-\phi^{n\beta}}$ and $\beta < p_+$.

With Lemma 3.1 we derived an upper bound on $\hat{Z}_n$, for the case $m = 1$, by using the frequency of state + in the realizations of $\{S_{n_0+1}, S_{n_0+2}, \ldots, S_n\}$ and the fact that Z_{n_0} gets arbitrarily close to 0, with probability $I(W)$, when n_0 is large enough. Following lemma is a generalization of this approach for arbitrary $m \geq 1$.

Lemma 5.5. *For some $\zeta \in (0,1)$ and $\gamma \in (0,1)$ define the events*

$$C_{n_0}(\zeta) = \{Z_{n_0} \leq \zeta\},$$
$$D^n_{n_0}(\gamma) = \{\#\big((S_{n_0+1}, \ldots, S_n)| + \big) \geq \gamma(n - n_0)\}.$$

We have

$$\hat{Z}_n \leq 2^{-\phi^{(\gamma-\epsilon)(n-n_0)}}, \quad C_{n_0}(\zeta) \cap D^n_{n_0}(\gamma).$$

Proof. See Appendix. □

From the convergence of Z_n to Z_∞ with probability $\Pr(Z_\infty = 0) = I(W)$ we know that for any $\epsilon \in (0,1)$ there exist a fixed n_0 such that

$$\Pr(C_{n_0}(\zeta)) \geq I(W) - \epsilon.$$

Next, from Theorem 5.2, we infer that when $m \ll n - n_0$

$$\Pr(D^n_{n_0}(\gamma)) \geq 1 - \epsilon, \quad \gamma \geq p^+ - \epsilon \tag{5.38}$$

holds. This results from the fact that the probability of observing + in $\{S_{n_0+1}, \ldots, S_{n_0}\}$ approaches to p^+ when $n - n_0$ is much larger than the memory, m, of the process $\{S_n\}$.

Choosing $n_0 = n\epsilon$ and using the above results in lemma 5.5 gives

$$\begin{aligned}\Pr\left(\hat{Z}_n \leq 2^{-\phi^{n(p^+-2\epsilon)(1-\epsilon)}}\right) &\geq (1-\epsilon)(I(W)-\epsilon) \\ &\geq I(W)-\epsilon\end{aligned}$$

Since $\epsilon \in (0,1)$ can be chosen arbtirarily close to 0, the above result indicates that

$$\Pr\left(\hat{Z}_n \leq 2^{-\phi^{n\beta}}\right) \geq I(W)-\epsilon$$

holds for $\beta < p^+$. □

Let us analyze the implications of Theorem 5.3 on the block-decoding error probability, P_e, of $\{\mathcal{C}_n^{(m)}\}$. It states that for $I(W)-\epsilon$ fraction of $W_n^{(i)}$ the corresponding Bhattacharyya parameters will be bounded as $Z_n^{(i)} \leq 2^{-\phi^{n\beta}}$ for $\beta < p^+$. We have $P_e \leq \sum_{i=1}^{N} Z_n^{(i)} \leq N2^{-\phi^{n\beta}} = O(2^{-\phi^{n\beta}})$. Since the code-length of $\{\mathcal{C}_n^{(m)}\}$ scales as $N = O(\phi^n)$ we also see that $P_e = O(2^{-N^\beta})$ holds for $\beta < p^+$.

The term p^+ is plotted in Fig. 5.6 as a m increases from 1 to 50. Investigating this figure we see that p^+ equals to 0.5 when $m = 1$ which coincides with the bound for the exponent of polar codes presented by Arıkan and Telatar in [17]. As m increases from 1 to 50, p^+ and thus the achievable exponent decreases. The decrease is more steep for small values of m and it becomes more monotone as m increases.

In order to fully characterize the asymptotic performance of $\{\mathcal{C}_n^{(m)}\}$ one needs to provide a converse bound on β which may be a difficult task. We believe that for the case $m > 1$, the achievable β for $\{\mathcal{C}_n^{(m)}\}$ may show a dependency on the rate, $R \in [0,1]$, chosen for the code; a phenomenon that does not exist when $m = 1$ (see [34]). In order explain our conjecture, consider the process $\{\hat{Z}_n\}$ in (5.37) which we use to obtain an achievable bound on β as $\beta < p^+$. Our proof is based on the observation that once the realizations of $\hat{Z}_{n_0}$ are sufficiently close to 0, which happens with probability $I(W)$, the scaling of Z_n is mostly determined by the number

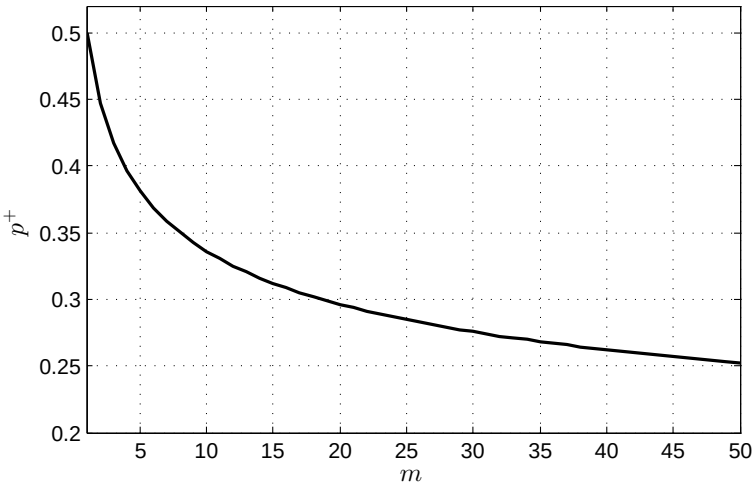

Figure 5.6. Achievable exponent, $\beta < p^+$, as scaled with m.

of occurrences of state + in $\{S_{n_0+1}, S_{n_0+2}, \ldots, S_n\}$. From Theorem 5.2 we know that one typically observes $(n-n_0)p^+$ occurrences of + in $\{S_{n_0+1}, S_{n_0+2}, \ldots, S_n\}$, therefore the value of $\log Z_n$ decreases $(n-n_0)p^+$ times with the same speed as the code-length, $\log \hat{Z}_n = \log \hat{Z}_{n-1} + \log \hat{Z}_{n-m}$, scaling as $\log Z_n = -\phi^{(n-n_0)p^+} = -\phi^{n(1-\epsilon)p^+}$. This result in the achievable exponent $\beta < p^+$. However, when $m > 1$ the value of $\log \hat{Z}_n$ may also decrease with a faster rate compared to that of the code-length. To see this, consider the case $(S_{n-1}, S_{n-2}, \ldots, S_{n-(m-1)}) = (\bigstar, \bigstar, \ldots, \bigstar)\}$ and $S_n = +$, where we have $\hat{Z}_{n-1} = \hat{Z}_{n-2} = \ldots = \hat{Z}_{n-(m-1)}$ and $\log \hat{Z}_n = \log \hat{Z}_{n-1} + \log \hat{Z}_{n-m} = \log \hat{Z}^2_{n-1}$. Therefore, there may be times where $\log Z_n$ decreases with a faster rate as $\log \hat{Z}_n = \log Z^2_{n-1}$ instead of $\log \hat{Z}_n = \log \hat{Z}_{n-1} + \log \hat{Z}_{n-m}$ and this may result in a higher achievable β. In order to quantify this we need to know not only the number of times state + occurs in $\{S_n\}$, but also the number of times a state + in $\{S_n\}$ is preceded by $\bigstar$ states. Therefore, we need to refine Theorem 5.2 in terms of the number of transitions between states +, − and $\bigstar$, as well. This might be a difficult nevertheless an important problem whose solution will provide a full characterization on the asymptotic polarization performance of $\{\mathcal{C}_n^{(m)}\}$ and we leave it as a future work.

We want to emphasize that the exponent, β, only provides an asymptotic characterization for the polarization performance. Therefore, it is not a good indicator

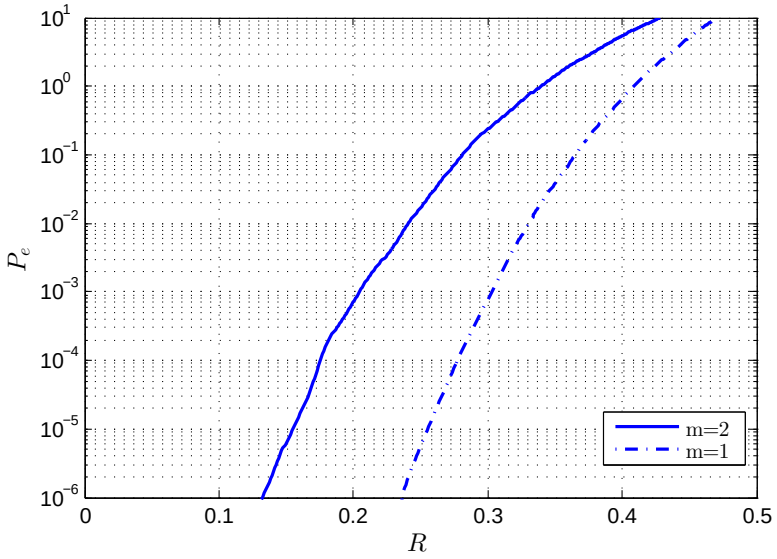

Figure 5.7. Upper bounds on P_e of $\{\mathcal{C}_n^{(m)}\}$ where transmission takes place over a BEC with capacity 0.5. Code-lengths are 1024 and 987 for $m = 2$ and $m = 1$, respectively.

of performance for practical code-lengths. This result from the fact that the exponent measures the polarization performance assuming one is operation very close to channel capacity, which requires arbitrarily large code-length. However, for practical code-lengths one operates strictly below capacity. In order to demonstrate the error correction capabilities of $\{\mathcal{C}_n^{(m)}\}$ we considered a BEC with Bhattacharyya parameter $\varepsilon = 0.5$ and symmetric capacity 0.5. We have plotted the upper bounds on block-decoding error probability, P_e, in Fig. 5.7, by calculating the Bhattacharyya parameters, $Z_n^{(i)}$, and using the fact $P_e \leq \sum_{i\in\mathcal{A}} Z_n^{(i)}$, $|\mathcal{A}|/N = R$. The figure shows that a lower P_e can be achieved when $m = 1$ compared to the case $m = 2$. Therefore, for the considered case original polar codes performs slightly better than the polar codes with memory order 2. However, as we explain in the following section, one can obtain a benefit in terms of complexity by taking $m = 2$ because the encoding and decoding complexities of $\{\mathcal{C}_n^{(m)}\}$ are decreasing in m. Notice that Fig. 5.7 is just a demonstration of the performance of $\{\mathcal{C}_n^{(m)}\}$ on BEC for the case $m = 1$ and $m = 2$. In order to provide a full performance evaluation, we need to consider different channels and values for m, which we leave as a future work.

5.7. Complexity and Sparsity

5.7.1. Encoding and Decoding Complexity

We consider a single core processor with random access memory and investigate the time complexity of encoding and decoding of $\{\mathbb{C}_n^{(m)}\}$. Let χ_n^E denote the complexity for encoding the information vector $\mathbf{u}_N$ to encoded bits $\mathbf{x}_N$. We take complexity of each XOR operation as 1 unit. By inspection of Fig 5.1, we have

$$\chi_n^E = \chi_{n-1}^E + \chi_{n-m}^E + N_{n-m} \quad n, m \geq 1, \tag{5.39}$$

where $\chi_1^E = 1$ and $\chi_0^E = \chi_{-1}^E = \ldots = \chi_{1-m}^E = 0$.

Similarly, let χ_n^D denote the complexity for decoding the inputs of $W_n^{(i)}$ channels, where SCD is the decoding method. We take the complexity of computing the LR. relations in (5.19) as 1 unit. We observe that one does not make any operations to calculate the LR in (5.20). By inspection of Fig 5.1, we have

$$\chi_n^D = \chi_{n-1}^D + \chi_{n-m}^D + 2N_{n-m} \quad n, m \geq 1, \tag{5.40}$$

where $\chi_0^D = \chi_{-1}^D = \ldots = \chi_{1-m}^D = 0$.

The recursions in (5.39) and (5.40) are cumbersome to deal with. To observe the scaling behavior of χ_n^E and χ_n^D in m, we define

$$\eta^E \triangleq \frac{\chi_n^E}{N \log N}, \quad \eta^D \triangleq \frac{\chi_n^D}{N \log N}, \tag{5.41}$$

and demonstrate the scaling of η^E and η^D in Fig .5.8, where we have numerically calculated χ_n^E and χ_n^D as in (5.39) and (5.40) by choosing $N = O(\phi^n)$ to be the code-length closest to 10^4 and 10^6. From Fig. 5.8 we observe that, there exist a decrease in η_n^E and η_n^D as m increases, where the decrease is more steep for small values of m and it becomes more monotone as m increases. This decrease in complexity, although

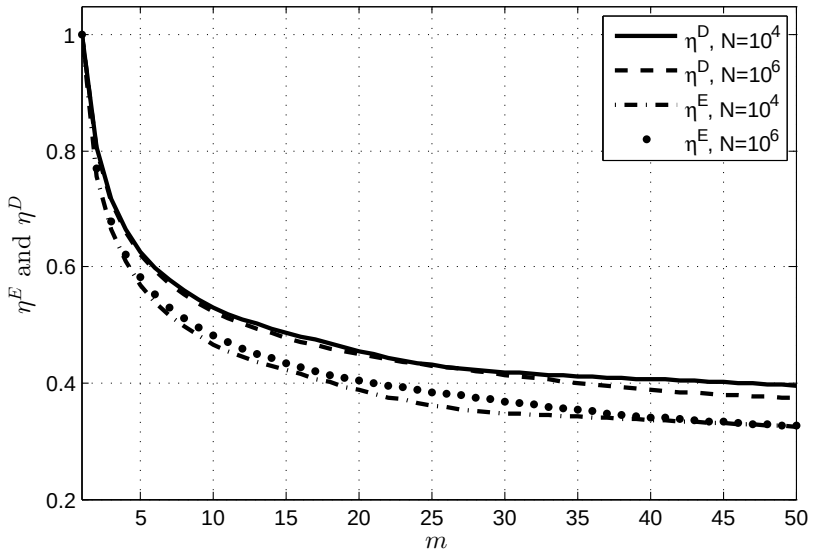

Figure 5.8. Scaling of encoding and decoding complexities as m increases where N is chosen to be the code-length closest to $1 \times 10^4, 1 \times 10^6$.

not being orders of magnitude, is promising in showing the existence of polar codes requiring lower complexity. For example, from Fig. 5.8 we observe that η_n^D is around $1/2$ when $m = 12$. This indicates that the decoding complexity of $\{\mathcal{C}_n^{(12)}\}$ is reduced by half compared to $\{\mathcal{C}_n^{(1)}\}$ which is the polar code presented by Arıkan in [13].

5.7.2. Sparsity

As we have explained at the beginning of the chapter, there exist a sparsity in the channel combining process in the sense that at each combining level, the vector channel W_n is obtained by combining W_{n-1} and $\bar{W}_{n-m}$ which are obtained from $N(n-1)$ and $N(n-m)$ uses of underlying B-DMC, W, respectively. From Proposition 5.4 we observe that the overall effect of channel combining and splitting is that, at each level n, there exist $N(n-m)$ bit-channel pairs that participate in $\boxplus$ and $\boxminus$ transforms. As m increases $N(n-m)$ decreases with respect to $N(n-1)$ implying the fraction of bit-channels participating in $\boxplus$ and $\boxminus$ transforms also decreases. On the other hand, as m increases, the code-length increases less rapidly in n because $N = O(\phi^n)$ and ϕ is decreasing in m, thus one can fit more channel combining and splitting levels within fixed code-length. A natural question is to understand the overall effect of increasing

m on the total number of $\boxplus$ and $\boxminus$ transforms that one can obtain when the number of uses of W channels is fixed. The importance of χ_n^D in (5.40) comes to play at this point because it gives us the total number of $\boxplus$ and $\boxminus$ transformation that are recursively applied to independent uses of W channels to obtain the bit-channels in W_n. Consequently, one can view η_D as a *packing ratio* in the sense that one can pack $\eta_n^D N \log N$ recursive applications of $\boxplus$ and $\boxminus$ transformation to N independent uses of W. Inspecting the scaling of η_D in Fig. 5.8 we observe that this packing ratio is 1 when $m = 1$ and it decreases with increasing m, and this decrease manifests itself as a reduction in the decoding complexity of $\{\mathcal{C}_n^{(m)}\}$.

5.8. Discussion

We have introduced a method to design a class of code sequences $\{\mathcal{C}_n^{(m)}; n \geq 1, m \geq 1\}$ to achieve the symmetric capacity of a B-DCM, W, where m is a an arbitrary and fixed memory parameter in the channel combining phase. With the newly introduced memory parameter m, we have generalized the channel combining phase in Arıkan's polar codes so that the vector channel W_n is obtained by combining W_{n-1} and $\bar{W}_{n-m}$, where taking $m = 1$ results with Arıkan's setup. By defining a splitting order which is based on a generalization of Arıkan's bit-reversed order we have split the the vector channel W_n to obtain a set of synthesized binary-input channels $\{W_n^{(i)}; i \in \mathbb{N}_n\}$. We showed that $W_n^{(i)}$ channels polarize with arbitrary m as well, thus complementing Arıkan's conjecture that channel polarization is in fact a general phenomenon. We have obtained an achievable bound on the asymptotic polarization of performance of $\{\mathcal{C}_n^{(m)}\}$ as scaled with m and showed that the encoding and decoding complexities of $\{\mathcal{C}_n^{(m)}\}$ decrease with increasing m. Future work will include a rate dependent analysis and a converse result on the asymptotic polarization performance of $\{\mathcal{C}_n^{(m)}\}$.

6. CONCLUSION

In this dissertation we considered theoretical and practical aspects of polar coding. In Chapters 3,4, and 5 we have explained our contributions in the fields of polar coding. Before concluding the dissertation we want to summarize our main results and mention some open problems that we could not cover.

In Chapter 3, we have obtained bounds on the Bhattacharyya parameters, $Z_n^{(i)}$, by using the Hamming weights, $H_n^{(i)}$, of the rows of the encoding matrix, $\mathbf{G}_n$, and the symmetric capacity, $I(W)$, of the underling channel W. We show that as $I(W)$ increases more $Z_n^{(i)}$ terms concentrate around $2^{-H_n^{(i)}}$ provided that $H_n^{(i)}$ are large enough. This fact indicates that the channel manifests its effect via the symmetric capacity, $I(W)$, and as $I(W)$ increases the effect of the channel decreases in the sense that $Z_n^{(i)}$ depend more on $H_n^{(i)}$ rather than the underlying channel, W. Our analysis, in this chapter was for Arıkan's polar codes where the encoding matrix was of the form $\mathbf{G}_n = \mathbf{F}^{\otimes n}$, $\mathbf{F} = \left[\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right]$. By using our results, it would be interesting to generalize our analysis for polar codes obtained from arbitrary $\ell \times \ell$, $\ell \geq 2$ kernels, $\mathbf{K}$, where the encoding matrix takes the form, $\mathbf{G}_n = \mathbf{K}^{\otimes n}$.

In Chapter 4, we have designed a BIPCM system where SCLD with CRC used as the decoding method. In order to design the code for fading channels, we derived a low complexity code-construction method which is based on generalization of Arıkan's heuristic code-construction method to parallel channels having a joint rate constraint. We have also presented a lower complexity and robust implementation of SCLD algorithm. We have compared the performance of resultant BIPCM system to RA and LDPC based counterparts and showed that it provides significant performance advantages. Although the proposed system outperforms the existing methods it would be nice to obtain results on choosing the appropriate CRC when SCLD is used for decoding. Formulating the effect of CRC together with the construction of polar codes may allow further performance gains and optimization guidelines for the proposed BIPCM system.

In Chapter 5, we have generalized the polar coding idea by introducing a memory parameter in the combining process. This resulted in a new family of polar codes, $\{\mathcal{C}_n^{(m)} : n \geq 1, m \geq 1\}$, with memory parameter m, where the case $m = 1$ is the the original polar codes. The new family of codes allows one to apply channel polarization in a controlled fashion by choosing the memory order $m = 1$. We have provided an information theoretic analysis for $\{\mathcal{C}_n^{(m)}\}$ and showed that it achieves the symmetric capacity of arbitrary BDMCs for any choice of m. We have also obtained an achievable bound on the exponent, β, of $\{\mathcal{C}_n^{(m)}\}$ as scaled with m. The new code family offers some complexity benefits because the its encoding and decoding complexities decrease with increasing m. $\{\mathcal{C}_n^{(m)}\}$ is the first demonstration for the existence of polar codes that achieve capacity and require lower complexity compared to the original codes proposed by Arıkan. Although we have provided an achievable region for the exponent, β, of the proposed codes family, our results indicate that the achievable β decreases with increasing m. In order to fully characterize the performance of $\{\mathcal{C}_n^{(m)}\}$ a converse result on β is needed. As we have explained in Section 5.6.4, we believe that for $m > 1$, $\{\mathcal{C}_n^{(m)}\}$ may achieve larger values for β depending on the rate, R, chosen for $\{\mathcal{C}_n^{(m)}\}$. For us, the solution of this conjecture is an important future goal.

REFERENCES

1. Shannon, C. E., "A Mathematical Theory of Communication", *Bell Systems Technical Journal*, Vol. 27, No. 379-473, pp. 623–656, 1948.

2. Hamming, R. W., "Error Detecting and Error Correcting Codes", *Bell Systems Technical Journal*, Vol. 29, pp. 147–160, 1950.

3. Golay, M. J. E., "Notes on Digital Coding", *Proc. IRE*, Vol. 37, p. 657, 1949.

4. Reed, I. S., "A Class of Multiple-Error-Correcting Codes and the Decoding Scheme", *IRE Transactions on Information Theory*, Vol. IT-4, pp. 38–49, 1954.

5. Reed, I. S. and G. Solomon, "Polynomial Codes Over Certain Finite Fields", *SIAM Journals on Computing*, Vol. 8, pp. 300–304, 1960.

6. Viterbi, A. J., "Error Bounds of Convolutional Codes and an Asymptotically Optimum decoding algorithm", *IEEE Transactions on Information Theory*, Vol. 13, No. 2, pp. 260–269, 1967.

7. Bahl, L., J. Cocke, F. Jelinek and J. Raviv, "Optimal Decoding of Linear Codes for Minimizing Sybol Error Rate", *IEEE Transactions on Information Theory*, Vol. 20, No. 2, pp. 284–287, 1974.

8. Wozencraft, J. M. and B. Reiffen, *Sequential Decoding*, MIT and Wiley, 1961.

9. Fano, R. M., "A Heuristic Discussion of Probabilistic Decoding", *IEEE Transactions on Information Theory*, Vol. 9, No. 2, pp. 64–74, 1963.

10. Berrou, C., A. Glavieux and P. Thitimajshima, "Near Shannon Limit Error-Correcting Coding and Decoding: Turbo-codes", *IEEE International Conference on Communications*, Vol. 2, pp. 1064–1070, 1993.

11. Richardson, T. and U. R., "The Capacity of Low-Density Parity Check Codes Under Message-Passing Decoding", *IEEE Transactions on Information Theory*, Vol. 47, No. 2, pp. 599–618, 2001.

12. Gallager, R. G., "Low-Density Parity-Check Codes", *IRE Transactions on Information Theory*, Vol. IT-8, pp. 21–28, 1962.

13. Arıkan, E., "Channel Polarization: A Method for Constructing Capacity-Achieving Codes for Symmetric Binary-Input Memoryless Channels", *IEEE Transactions on Information Theory*, Vol. 55, No. 7, pp. 3051–3073, 2009.

14. Arıkan, E., "Channel Combining and Splitting for Cutoff Rate Improvement", *IEEE Transactions on Information Theory*, Vol. 52, No. 2, pp. 628–639, 2006.

15. Arıkan, E., "A Performance Comparison of Polar Codes and Reed-Muller Codes", *IEEE Communucation Letters*, Vol. 12, No. 6, pp. 447–449, 2008.

16. Tal, I. and A. Vardy, "How to Construct Polar Codes", *IEEE Transactions on Information Theory*, Vol. 59, No. 10, pp. 6562–6582, 2013.

17. Arıkan, E. and I. Telatar, "On the Rate of Channel Polarization", *Proceedings IEEE Symposium on Information Theory*, pp. 1493–1495, 2009.

18. Mondelli, M., S. Hassani and R. Urbanke, "From polar to Reed-Muller Codes: A Technique to Improve the Finite-Length Performance", *IEEE Transactions on Information Theory*, Vol. 62, No. 9, pp. 3084–3091, 2014.

19. Korada, S. B., *Polar Codes for Channel and Source Coding*, Ph.D. Thesis, EPFL, 2009.

20. Cover, T. and J. Thomas, *Elements of Information Theory*, Wiley, 2005.

21. Korada, S., E. Şaşoğlu and R. Urbanke, "Polar Codes: Characterization of Exponent, Bounds, and Constructions", *IEEE Transactions on Information Theory*,

Vol. 56, No. 12, pp. 6253–6264, 2010.

22. Tal, I. and A. Vardy, "List Decoding of polar codes", *Proceedings IEEE Symposium on Information Theory*, pp. 1–5, 2011.

23. Zehavi, E., "8-PSK Trellis Codes on Rayleigh Channel", *Proceeding IEEE Military Communication Conference*, pp. 536–540 vol.2, 1989.

24. Ungerboeck, G., "Channel Coding with Multilevel/Phase Signals", *IEEE Transactions on Information Theory*, Vol. 28, No. 1, pp. 55–67, 1982.

25. Caire, G., G. Taricco and E. Biglieri, "Bit-Interleaved Coded Modulation", *IEEE Transactions on Information Theory*, Vol. 44, No. 3, pp. 927–946, 1998.

26. Chindapol, A. and J. Ritcey, "Design, Analysis, and Performance Evaluation for BICM-ID with Square QAM Constellations in Rayleigh Fading Channels", *IEEE Journal on Selected Areas in Communication*, Vol. 19, No. 5, pp. 944–957, 2001.

27. Hou, J., P. Siegel, L. Milstein and H. Pfister, "Capacity-Approaching Bandwidth-Efficient Coded Modulation Schemes Based on Low-Density Parity-Check Codes", *IEEE Transactions on Information Theory*, Vol. 49, No. 9, pp. 2141–2155, 2003.

28. Han, W. K., S. Le Goff and B. Sharif, "Systematic Repeat Accumulate Codes for Bit-Interleaved Coded Modulation with Iterative Demapping over AWGN and Rayleigh Fading Channels", *Proceeding Internation Symposuium on Wireless Pervasive Computing*, pp. 152–155, 2008.

29. Tanaka, T. and R. Mori, "Refined Rate of Channel Polarization", *Proceedings IEEE Symposium on Information Theory*, pp. 889–893, 2010.

30. Hassani, S., K. Alishahi and R. Urbanke, "On the Scaling of Polar Codes: II. The Behavior of Un-polarized Channels", *Proc. IEEE Int. Symp. Inform. Theory (ISIT)*, pp. 879–883, 2010.

31. Bakshi, M., S. Jaggi and M. Effros, "Concatenated Polar Codes", *Proceedings IEEE Symposium on Information Theory*, pp. 918–922, 2010.

32. Bartle, R. G., *The Elements of Real Analysis*, John Wiley & Sons, 1995.

33. Billingsley, P., *Probability and Measure*, John Wiley & Sons, 1927.

34. Hassani, S. and R. Urbanke, "On the Scaling of Polar Codes: I. The Behavior of Polarized Channels", *Proceedings IEEE Symposium on Information Theory*, pp. 874–878, 2010.

APPENDIX A: PROOFS

A.1. Proof of Lemma 3.1

Conditioned on the event $G_m^n(\gamma)$ there exists at least $(n-m)\gamma$ occurrences of 1 in $\{B_{m+1}B_{m+2}\ldots B_n\}$. In light of (3.5), we have $\hat{Z}_n \leq \hat{Z}_{n-1}$ when $B_n = 1$ and $\hat{Z}_n \geq \hat{Z}_{n-1}$ when $B_n = 0$. Moreover, $\hat{Z}_n$ is increasing in $\hat{Z}_{n-1}$ regardless of B_n. Consequently, if we fix $\hat{Z}_m$, the largest value of $\hat{Z}_n$ will occur if $\{B_{m+1}B_{m+2}\ldots B_n\}$ has the following realization

$$\{\overbrace{00\ldots0}^{(n-m)(1-\gamma)\text{ times}}\underbrace{11\ldots1}_{(n-m)\gamma\text{ times}}\}.$$

During consecutive runs of 1, the value of $\log_2 \hat{Z}_i$, doubles with respect to $\log_2 \hat{Z}_{i-1}$, which happens $(n-m)\gamma$ times. We thus have

$$\log_2 \hat{Z}_n = 2^{\gamma(n-m)} \log_2 \hat{Z}_k, \tag{A.1}$$

where $k = m+(n-m)(1-\gamma)$. During consecutive runs of 0, $\hat{Z}_i$ obeys $1-\hat{Z}_i = (1-\hat{Z}_{i-1}^2)$. This recursion occurs $(n-m)(1-\gamma)$ times resulting in

$$\begin{aligned} 1-\hat{Z}_k &= (1-Z_m)^{2(n-m)(1-\gamma)}, \\ \hat{Z}_k &= 1-(1-Z_m)^{2(n-m)(1-\gamma)}. \end{aligned}$$

We next employ the inequality $\log x \leq x-1$, $x \in [0,1]$, by letting $x = \hat{Z}_k$ to obtain

$$\log_2 \hat{Z}_k \leq -(1-Z_m)^{2(n-m)(1-\gamma)}. \tag{A.2}$$

Using (A.2) in (A.1) gives

$$\begin{aligned}\log_2 \hat{Z}_n &\leq -2^{\gamma(n-m)}(1-Z_m)^{2(n-m)(1-\gamma)},\\ &\leq -2^{(\gamma-\epsilon)(n-m)}\left((1-Z_m)^2 2^{\epsilon}\right)^{n-m}.\end{aligned}$$

Choose $\zeta \in (0,1)$ so that $\zeta \leq 1-2^{\frac{-\epsilon}{2}}$ holds. Conditioned on $D_m(\zeta)$, we have $(1-Z_m)^2 2^{\epsilon} \geq 1$, resulting in

$$\log_2 \hat{Z}_n \leq -2^{(\gamma-\epsilon)(n-m)}, \quad D_m(\zeta) \cap G_m^n(\gamma),$$

which proves the lemma.

A.2. Proof of Proposition 5.2

From the operation of φ_n in Defn. 5.1 we obtain $\mathcal{S}_1 = \{+,-\}$ such that $\mathbf{s}_1^{(1)} = (+)$ and $\mathbf{s}_1^{(2)} = (-)$, indicating $\mathbf{s}_1^{(1)}$ and $\mathbf{s}_1^{(2)}$ are unique. Proof is by induction, assume that $s_{n-1}^{(j)} \in \mathcal{S}_{n-1}$ are unique. Let $j \in \mathbb{N}_{n-m}$ and consider $\mathbf{s}_{n-1}^{(j)}$ to whom by appending $+$ and $-$ one obtains $\mathbf{s}_n^{(j)}$ and $\mathbf{s}_n^{(j+N(n-1))}$, respectively, indicating $\mathbf{s}_n^{(j+N(n-1))}$ and $\mathbf{s}_n^{(j)}$ are different from each other. Next, let $j \in \mathbb{N}_{n-1} \setminus \mathbb{N}_{n-m}$ then $\mathbf{s}_n^{(j)}$ are obtained by appending $\bigstar$ to $\mathbf{s}_{n-1}^{(j)}$ which, by assumption, are unique. Combining the result we see that for all $j \in \mathbb{N}_n$ the vectors $s_n^{(j)} \in \mathcal{S}_n$ are different from each other.

A.3. Proof of Proposition 5.3

Investigating Fig 5.2 consider the operation of φ_{n-1} where $s_{n-2}^{(k)} = (s_1, s_2, \ldots, s_{n-2})$, $k \in \mathbb{N}_{n-2}$, holds at level $n-1$. Next, consider the operation of φ_{n-2} where one has $s_{n-3}^{(k)} = (s_1, s_2, \ldots, s_{n-3})$ for $k \in \mathbb{N}_{n-3}$. In turn and by induction through $\varphi_{n-2}, \varphi_{n-3}, \ldots, \varphi_{n-(m-1)}$ we conclude that $s_{n-m}^{(j)} = (s_1, s_2, \ldots, s_{n-m})$, $j \in \mathbb{N}_{n-m}$.

A.4. Proof of Proposition 5.5

i) For $m > 1$ we have $F(m,1) = -1 < 0$ and $F(m,2) = 2^{m-1} - 1 \geq 0$ so that there exists at least one real root in (1,2]. Proof is by contradiction, let $\rho_1, \rho_2 \in (1,2]$ be two real roots of $F(m,\rho)$ then from (5.22) we have

$$\rho_1^{m-1}(\rho_1 - 1) = 1, \tag{A.3}$$

$$\rho_2^{m-1}(\rho_2 - 1) = 1. \tag{A.4}$$

Let $\rho_1 < \rho_2$, then $\rho_2^{m-1} > \rho_1^{m-1}$ and $\rho_2 - 1 > \rho_1 - 1 > 0$ implying $\rho_2^{m-1}(\rho_2 - 1) > 1$ if $\rho_1^{m-1}(\rho_1 - 1) = 1$ which contradicts (A.4), carrying a similar analysis for $\rho_1 < \rho_2$ also contradicts (A.4), which indicates $\rho_1 = \rho_2 = \phi$.

ii) Assume that ρ is a complex root of $F(m,\rho)$, with $\sqrt{\rho\rho^*} = \sigma > 1$ where $*$ denotes the conjugate operation. Since the coefficients of $F(m,\rho)$ are real, its complex roots must be in conjugate pairs. From (5.22)

$$\rho^{m-1}(\rho - 1) = 1,$$
$$\rho^{*m-1}(\rho^* - 1) = 1.$$

Multiplying the above equations we obtain

$$\sigma^{2(m-1)}(\sigma^2 - 2Re(\rho) + 1) = 1,$$
$$\sigma^{2(m-1)}(\sigma^2 - 2\sigma\alpha + 1) = 1, \tag{A.5}$$

where $0 \leq \alpha < 1$. In turn for any ρ, σ must be a root of

$$g(\sigma,\alpha) = \sigma^{2(m-1)}(\sigma^2 - 2\sigma\alpha + 1) - 1, \tag{A.6}$$

Observe that when σ is fixed $g(\sigma,\alpha)$ is decreasing in α. We also have

$$\frac{\partial g(\sigma,\alpha)}{\partial \sigma} = 2(m-1)\sigma^{2(m-1)-1}(\sigma^2 - 2\sigma\alpha + 1) + \sigma^{2(m-1)}(2\sigma - 2\alpha)$$

From (A.5) observe that $(\sigma^2 - 2\sigma\alpha + 1) > 0$, and since $(2\sigma - 2\alpha) > 0$ for $\sigma > 1$ we have $\frac{\partial g(\sigma,\alpha)}{\partial \sigma} > 0$. This indicates that $g(\sigma,\alpha)$ is increasing with σ. But ϕ is a root of $g(\sigma,\alpha)$ with $\alpha = 1$ and thus $g(\phi,1) = 0$. Since $g(\sigma,\alpha)$ is decreasing in α we have $g(\phi,\alpha) \geq 0$ and $g(\sigma,\alpha) = 0$ is only achieved if $\sigma < \phi$ because $g(\sigma,\alpha)$ is increasing with σ.

iii) Observe that for some $\rho \in (1,2]$ we have $\frac{\partial F(m,\rho)}{\partial \rho} > 0$ so that $F(m,\rho)$ is increasing in ρ and when ρ is fixed $F(m,\rho)$ is also increasing in m. Assume that $\rho_1, \rho_2 \in (1,2]$ are real roots of $F(m_1,\rho)$ and $F(m_2,\rho)$, respectively, where $m_1, m_2 \geq 1$. Then $f(m_1,\rho_1) < f(m_2,\rho_1)$ holds if $m_2 > m_1$ and $f(m_1,\rho_1) = f(m_2,\rho_2) = 0$ is satisfied only if $\rho_1 < \rho_2$.

A.5. Proof of Lemma 5.1

Let $J_n^{(i)} = J(W_n^{(i)})$ denote symmetric cut-off rate of $W_n^{(i)}$. From Proposition 5.4 we know that for $j \in \mathbb{N}_{n-m}$ we have $W_n^{(j)} = W_{n-1}^{(j)} \boxplus W_{n-m}^{(j)}$ and $W_n^{(j+N(n-1))} = W_{n-1}^{(j)} \boxminus W_{n-m}^{(j)}$. Proposition 1.1 indicates that these transforms increase the sum cut-off rate as $J_n^{(j)} + J_n^{(j+N(n-1))} \geq J_{n-1}^{(j)} + J_{n-1}^{(j)}$ where the equality is achieved only if $J_{n-1}^{(j)} \in \{0,1\}$ or $J_{n-m}^{(j)} \in \{0,1\}$ holds. For $j \in \mathbb{N}_{n-1} \setminus \mathbb{N}_{n-m}$, from Proposition 5.4, we have $J_n^{(j)} = \gamma(n) J_{n-1}^{(j)}$ which implies $J_n^{(j)} = J_{n-1}^{(j)}$. Combining the above results gives

$$\sum_{i \in \mathbb{N}_n} J_n^{(i)} \geq \sum_{j \in \mathbb{N}_{n-1}} J_n^{(j)} + \sum_{k \in \mathbb{N}_{n-m}} J_n^{(k)},$$

where the equality is achieved only of if $J_{n-1}^{(j)} \in \{0,1\}$ or $J_{n-m}^{(j)} \in \{0,1\}$ holds for all $j \in \mathbb{N}_{n-m}$. In the probabilistic domain of Section5.6 the above result is equivalent to

$$\sum_{\mathbf{s}_n \in \mathcal{S}_n} J_n \geq \sum_{\mathbf{s}_{n-1} \in \mathcal{S}_{n-1}} J_{n-1} + \sum_{\mathbf{s}_{n-m} \in \mathcal{S}_{n-m}} J_{n-m},$$

where the equality is achieved only of if $J_{n-1} \in \{0,1\}$ or $J_{n-m} \in \{0,1\}$ holds for all $S_n \in \{+,-\}$. Dividing both sides of the above inequality by $1/N(n)$ and using $E[J_n] = \frac{1}{N(n)} \sum_{\mathbf{s}_n \in \mathcal{S}_n} J_n$ we obtain

$$E[J_n] \geq \frac{N(n-1)}{N(n)} E[J_{n-1}] + \frac{N(n-m)}{N(n)} E[J_{n-m}].$$

Noticing $\frac{N(n-1)}{N(n)} = \mu(n)$ and $\frac{N(n-m)}{N(n)} = 1 - \mu(n)$ completes the proof.

A.6. Proof of Lemma 5.2

From (5.25) we have

$$\begin{aligned} E[J_n] &\geq \mu E[J_{n-1}] + (1-\mu)\, E[J_{n-m}], \\ &\geq \min\{E[J_{n-1}], E[J_{n-m}]\}, \end{aligned} \tag{A.7}$$

Let us define the set

$$\mathcal{E}_k^{(m)} \triangleq \{E_{km}, E_{km-1}, \ldots, E_{km-(m-1)}\}.$$

By definition in (5.26) we have we have $E[\hat{J}_k] = \min \mathcal{E}_k^{(m)}$. Proof is by induction. We use (A.7) to upper bound the elements of $\mathcal{E}_k^{(m)}$ with respect to $\min \mathcal{E}_{k-1}^{(m)} = E[\hat{J}_{k-1}]$. Let $n = km - (m-1)$ and use (A.7) to obtain

$$\begin{aligned} E_{km-(m-1)} &\geq \min\{E_{(k-1)m}, E_{(k-1)m-(m-1)}\}, \\ &\geq \min \mathcal{E}_{k-1}^{(m)} \end{aligned}$$

For $i = 2, 3, \ldots, m-1$ assume

$$E_{km-(m-i)} \geq \min \mathcal{E}_{k-1}^{(m)}$$

holds. Next, let $n = km - (m - (i+1))$ in (A.7) to write

$$E_{km-(m-(i+1))} \geq \min\{E_{km-(m-i)}, E_{(k-1)m-(m-(i+1))}\}.$$

By assumption $E_{km-(m-i)} \geq \min \mathcal{E}_{k-1}^{(m)}$ and by definition $E_{(k-1)m-(m-(i+1))} \geq \min \mathcal{E}_{k-1}^{(m)}$ holds, indicating

$$E_{km-(m-(i+1))} \geq \min \mathcal{E}_{k-1}^{(m)}.$$

Combining the above results tells us for $i = 1, 2, \ldots, m$ we have $E_{km-(m-i)} \geq \min \mathcal{E}_{k-1}^{(m)} = E[\hat{J}_{k-1}]$ which indicates $E[\hat{J}_k] \geq E[\hat{J}_{k-1}]$.

A.7. Proof of Lemma 5.3

In order to bound $|\mathcal{T}_n^{(q)}|$ we decompose $\mathcal{T}_n^{(q)}$ it into two different sets

$$\mathcal{T}_n^{(a,q)} \triangleq \left\{\mathbf{s}^n : P_{\mathbf{s}^n}^{(-)} = q, s_n = +\right\},$$
$$\mathcal{T}_n^{(b,q)} \triangleq \left\{\mathbf{s}^n : P_{\mathbf{s}^n}^{(-)} = q, s_n \neq +\right\}$$

and we have $T_n^{(q)} = \mathcal{T}_n^{(a,q)} \cup \mathcal{T}_n^{(b,q)}$. Recall that each state $-$ in $\mathbf{s}_n$ is followed by $m-1$ occurrences of state $\bigstar$. In turn, $\mathcal{T}_n^{(a,q)}$ consists of $\mathbf{s}_n$ having $k = nq$, $0 \leq k \leq n/m$, occurrences of the vector $\mathbf{a} = (-, \underbrace{\bigstar, \bigstar, \ldots, \bigstar}_{m-1 \text{ times}})$ and $n - km$ occurrences of state $+$. By combinatorial analysis we have

$$|\mathcal{T}_n^{(a,q)}| = \binom{n-(m-1)k}{k}.$$

$\mathcal{T}_n^{(b,q)}$ consists of $k-1$ occurrences of the vector $\mathbf{a}$, an occurrence of $\mathbf{b} = (-, \underbrace{0, 0, \ldots, 0}_{p \text{ times}})$, $1 \leq p < m-1$, and $n - mk - (p+1)$ occurrences of state $+$. The vector $\mathbf{b}$ can only occur in the last $p+1$ entries in $\mathbf{s}_n$ and it will be completed to a vector $\mathbf{a}$ if we had prolonged the channel combining operation $m - 1 - p \leq m$ more levels. Therefore

$$|\mathcal{T}_n^{(b,q)}| \leq \binom{n+m-(m-1)k}{k}.$$

For some $c \in \mathbb{Z}$ and $d \in \mathbb{Z}$ with $c < d$ we have $\binom{d}{c} = \frac{d}{d-c}\binom{d-1}{c} \leq d\binom{d-1}{c}$, using this fact we obtain

$$\begin{aligned}
\binom{n+m-(m-1)k}{k} &\leq (n+m)\binom{n+(m-1)-(m-1)k}{k}, \\
&< (n+m)^2\binom{n+(m-2)-(m-1)k}{k} \\
&\vdots \\
&< (n+m)^m\binom{n-(m-1)k}{k}
\end{aligned}$$

Then we have

$$\begin{aligned}
|\mathcal{T}_n^{(q)}| &= |\mathcal{T}_n^{(a,q)}| + |\mathcal{T}_n^{(b,q)}|, \\
&< (1 + (n+m)^m)\binom{n-(m-1)k}{k}, \\
&< (1 + (n+m))^m\binom{n-(m-1)k}{k}, \\
&= 2^{nB(m,n)}\binom{n-(m-1)k}{k}, \qquad \text{(A.8)}
\end{aligned}$$

where $B(m,n) = \frac{m\log(1+n+m)}{n} = o(1)$. Next, we use the upper bound $\binom{n}{k} \leq 2^{nH(k/n)}$ in [20] to upper bound $\binom{n-(m-1)k}{k}$ as

$$\begin{aligned}
\binom{n-(m-1)k}{k} &\leq 2^{n(1-(m-1)(k/n))H(\frac{(k/n)}{1-(m-1)(k/n)}}, \\
&= 2^{nG(m,q)}. \qquad \text{(A.9)}
\end{aligned}$$

Combining (A.8) and (A.9)we obtain the desired bound as $|T_n^{(q)}| < 2^{n(G(m,q)+B(m,n))} = 2^{n(G(m,q)+o(1))}$.

A.8. Proof of Lemma 5.4

We have

$$G(m,q) = (1-(m-1)q)H\left(\frac{(q)}{1-(m-1)q}\right).$$

We know that, for $q \in [0, 1/m]$, $H(\frac{q}{1-(m-1)q})$ is concave in q and $(1-(m-1)q)$ is linear in q indicating $G(m,q)$ is concave in q. Let $q*$ denote the maximizer of $G(m,q)$. The maximum of $H(\frac{q}{1-(m-1)q})$ occurs when $\frac{q}{1-(m-1)q} = \frac{1}{2}$ or equivalently when $q = \frac{1}{m+1}$ and since $(1-(m-1)q)$ is decreasing in q, we have $q* \in [0, \frac{1}{m+1}]$. We next evaluate $\frac{\partial G(m,q)}{\partial q}$

$$\begin{aligned}\frac{\partial G(m,q)}{\partial q} &= (m-1)\log(1-(m-1)q) \\ &\quad + \log q - m\log(1-mq).\end{aligned}$$

setting $\frac{\partial G(m,q)}{\partial q}|_{q=q*} = 0$ gives

$$(m-1)\log(1-(m-1)q^*) + \log q^* = m\log(1-mq^*). \tag{A.10}$$

Re-arranging the above equation we obtain

$$\begin{aligned}m\log\frac{(1-(m-1)q^*)}{1-mq^*} + \log\frac{q^*}{1-mq^*} \\ = \log\frac{(1-(m-1)q^*)}{1-mq^*}.\end{aligned} \tag{A.11}$$

Let us use the following substitutions

$$\eta = \frac{1-(m-1)q^*}{1-mq^*}, \quad \eta - 1 = \frac{q^*}{1-mq^*}.$$

For $q* \in [0, \frac{1}{m+1}]$ we have $\eta \in [1, 2]$. Using the above substitutions in (A.11) we obtain

$$m \log \eta + \log(\eta - 1) = \log \eta,$$

or alternatively

$$\eta^m(\eta - 1) = \eta.$$

Dividing both sides of the above relation by η and re-arranging the terms we obtain

$$\eta^m - \eta^{m-1} - 1 = 0. \tag{A.12}$$

But the above polynomial is same as 5.22. Consequently from part i of Proposition. 5.5 we conclude that $\eta = \phi$ which indicates that $\frac{1-(m-1)q^*}{1-mq^*} = \phi$ and hence $q^* = \frac{1}{1+m(\phi-1)} = p^-$. Next we evaluate the maximum of $G(m, q)$ attained at $q = q^*$.

$$\begin{aligned} G(m, q^*) = -q^* \log \frac{q^*}{1-(m-1)q^*} + \\ (mq^* - 1) \log \frac{1-mq^*}{1-(m-1)q^*} \end{aligned} \tag{A.13}$$

Re-arranging (A.10) we observe that

$$\log \frac{q^*}{1-(m-1)q^*} = m \log \frac{1-mq^*}{1-(m-1)q^*}$$

Using the above relation in (A.13) gives

$$G(m, q^*) = \log \frac{1-(m-1)q^*}{1-mq^*} = \log \phi.$$

A.9. Proof of Proposition 5.7

We define a typical set $\mathcal{T}_n^{(q,\epsilon)}$ as

$$\mathcal{T}_n^{(q,\epsilon)} = \{\mathbf{s}_n : P_{s^n}^{(-)} = q, D(q,p^-) \leq \epsilon\}.$$

The probability that $\mathcal{T}_n^{(q)}$ is not typical is

$$\begin{aligned}
1 - \Pr(\mathcal{T}_n^{(q,\epsilon)}) &= \sum_{\Pr(D(q,p^-)>\epsilon)} \Pr(\mathcal{T}_n^{(q)}), \\
&\overset{a}{\leq} \sum_{\Pr(D(q,p^-)>\epsilon)} 2^{-n(D(q,s_-)+B'(m,n))}, \\
&\leq \sum_{\Pr(D(q,p^-)>\epsilon)} 2^{-n(\epsilon+B'(m,n))}, \\
&\overset{b}{\leq} (n+1)2^{-n(\epsilon-B'(m,n))}, \\
&= 2^{-n(\epsilon-B''(m,n))}, \qquad \text{(A.14)}
\end{aligned}$$

where $B''(m,n) = \frac{m\log(1+n+m)-\log\kappa+\log(n+1)}{n}$. In the above derivation (a) follows from (5.34) and (b) follows from the fact that there exist at most $n+1$ different type classes having $\Pr(D(q,s_-) > \epsilon)$. The above result indicates that $\sum_{n\to\infty} \Pr(D(q,s_-) \geq \epsilon)$ converges, thus the expected number of the occurrences of the event $D(q,s_-) > \epsilon$ for all n is finite. By using the first Borel Cantelli Lemma [33, p. 59] we conclude that $D(q,s_-)$ converges to 0 with probability 1.

A.10. Proof of Lemma 5.5

Conditioned on the event $D_{n_0}^n(\gamma) = \#\big((s_{n_0+1},\ldots,s_n)| + \big) \geq \gamma(n-n_0)$ there exists at least $\gamma(n-n_0)$ occurrences of state + in $\{S_{n_0+1}, S_{n_0+2}, \ldots, S_n\}$. Investigating (5.37), we have $\hat{Z}_n \leq \hat{Z}_{n-1}$ when $S_n = +$ and $Z_n \geq Z_{n-1}$ when $S_n \neq +$. Moreover, Z_n is increasing in Z_{n-1} when S_n is fixed. Consequently, if we fix $\hat{Z}_m$, the largest value of

$\hat{Z}_n$ will occur if $\{S_{n_0+1}, S_{n_0+2}, \dots S_n\}$ has the following realization

$$\{\overbrace{\mathbf{a}, \mathbf{a}, \dots, \mathbf{a}}^{(1-\gamma)(n-n_0)/m \text{ times}}, \underbrace{+, +, \dots, +}_{\gamma(n-n_0) \text{ times}}\}.$$

where $\mathbf{a} = (-, \underbrace{\bigstar, \bigstar, \dots, \bigstar}_{m-1 \text{ times}})$. In order to upper bound $\hat{Z}_n$ we assume that the above realization has occured for $\{S_{n_0+1}, S_{n_0+2}, \dots S_n\}$. During consecutive runs of $+$, the value of $\log \hat{Z}_n$ increases with the same recursion as the code-length in (5.1) as $\log \hat{Z}_n = \log \hat{Z}_{n-1} + \log \hat{Z}_{n-m}$. This recursion happens $\gamma(n-m)$ times and since the code-legth obeying the same recursion scales as $\phi^{\gamma(n-m)}$, $\phi \in (1, 2]$, we have

$$\log \hat{Z}_n = \phi^{\gamma(n-n_0)} \log \hat{Z}_k, \tag{A.15}$$

where $k = n_0 + (1-\gamma)(n-m)$. During consecutive runs of $\mathbf{a}$ the value of $\hat{Z}_i$ does not change with respect to $\hat{Z}_{i-1}$ when $S_i = \bigstar$ and it increases as $\hat{Z}_i = \hat{Z}_{i-1} + \hat{Z}_{i-m} - \hat{Z}_{n-1}\hat{Z}_{i-m}$ when $S_i = -$. By construction of $\{S_{n_0+1}, S_{n_0+2}, \dots S_n\}$ each state $-$ is preceed by $m-1$ occurances of $\bigstar$ therefore if $S_i = -$ we have $(S_{i-1}, S_{i-2}, \dots, S_{i-(m-1)}) = (\bigstar, \bigstar, \dots, \bigstar)$ indicating $\hat{Z}_{i-1} = \hat{Z}_{i-2} = \dots = \hat{Z}_{i-(m-1)}$. Therefore during each occurance of state $-$ in $\mathbf{a}$ we see the recursion $\hat{Z}_{i-1} + \hat{Z}_{i-m} - \hat{Z}_{i-1}\hat{Z}_{i-m} = 2\hat{Z}_{i-1} - \hat{Z}_i^{(i)}$ or equvalently $1 - \hat{Z}_i = (1 - \hat{Z}_i^{(i)})^2$. This recursion occurs $(1-\gamma)(n-n_0)$ times resulting in $1 - \hat{Z}_k = (1 - \hat{Z}_{n_0})^{2(1-\gamma)(n-n_0)}$ and $\hat{Z}_k = 1 - (1 - \hat{Z}_{n_0})^{2(1-\gamma)(n-n_0)}$. Next, employ the inequality $\log x \leq x - 1$, $x \in [0, 1]$, by letting $x = \hat{Z}_k$ to obtain

$$\log \hat{Z}_k \leq -(1 - \hat{Z}_{n_0})^{2(1-\gamma)(n-n_0)}. \tag{A.16}$$

Using (A.16) in (A.15) gives

$$\begin{aligned}
\log \hat{Z}_n &= -\phi^{\gamma(n-n_0)}(1 - Z_{n_0})^{2(1-\gamma)(n-n_0)}, \\
&\leq -\phi^{\gamma(n-n_0)}(1 - Z_{n_0})^{2(n-n_0)} \\
&= -\phi^{(\gamma-\epsilon)(n-n_0)} \left((1 - Z_{n_0})^2 \phi^{\epsilon}\right)^{(n-n_0)}.
\end{aligned}$$

Choose $\zeta \in (0,1)$ so that $\zeta \leq 1 - \phi^{\frac{-\epsilon}{2}}$ holds. Conditioned on $C_{n_0}(\zeta) = \{Z_{n_0} \leq \zeta\}$ we have $(1 - Z_{n_0})^2 \phi^{\epsilon} \geq 1$, resulting in

$$\log_2 \hat{Z}_n \leq -\phi^{(\gamma-\epsilon)(n-m)}, \quad C_{n_0}(\zeta) \cap D^n_{n_0}(\gamma),$$

which proves the lemma.