ABSTRACT

Title of dissertation: APPLICATIONS OF ORDERED WEIGHTS IN INFORMATION TRANSMISSION

Woomyoung Park
Doctor of Philosophy, 2012

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

This dissertation is devoted to a study of a class of linear codes related to a particular metric space that generalizes the Hamming space in that the metric function is defined by a partial order on the set of coordinates of the vector.

We begin with developing combinatorial and linear-algebraic aspects of linear ordered codes. In particular, we define multivariate rank enumerators for linear codes and show that they form a natural set of invariants in the study of the duality of linear codes. The rank enumerators are further shown to be connected to the shape distributions of linear codes, and enable us to give a simple proof of a MacWilliams-like theorem for the ordered case. We also pursue the connection between linear codes and matroids in the ordered case and show that the rank enumerator can be thought of as an instance of the classical matroid invariant called the Tutte polynomial. Finally, we consider the distributions of support weights of ordered codes and their expression via the rank enumerator. Altogether, these results generalize a group of well-known results for codes in the Hamming space to the ordered case.

Extending the research in the first part, we define simple probabilistic channel models that are in a certain sense matched to the ordered distance, and prove several results related to performance of linear codes on such channels. In particular, we define ordered wire-tap channels and establish several results related to the use of linear codes for reliable and secure transmission in such channel models.

In the third part of this dissertation we study polar coding schemes for channels with nonbinary input alphabets. We construct a family of linear codes that achieve the capacity of a nonbinary symmetric discrete memoryless channel with input alphabet of size $q = 2^r, r = 2, 3, \ldots$. A new feature of the coding scheme that arises in the nonbinary case is related to the emergence of several extremal configurations for the polarized data symbols. We establish monotonicity properties of the configurations and use them to show that total transmission rate approaches the symmetric capacity of the channel. We develop these results to include the case of "controlled polarization" under which the data symbols polarize to any predefined set of extremal configurations. We also outline an application of this construction to data encoding in video sequences of the MPEG-2 and H.264/MPEG-4 standards.

APPLICATIONS OF ORDERED WEIGHTS IN INFORMATION TRANSMISSION

by

Woomyoung Park

Dissertation submitted to the Faculty of the Graduate School of the
University of Maryland, College Park in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
2012

Advisory Committee:
Professor Alexander Barg, Chair/Advisor
Professor Leonid Koralov
Professor Prakash Narayan
Professor Adrian Papamarcou
Professor Sennur Ulukus

Dedication

To my loving wife, Eunyoung and my son, Isan

Acknowledgments

First and foremost I would like to thank my advisor, Professor Alexander Barg for giving me the opportunity to work with him. It has been a great pleasure to know him and to be his doctoral student. His guidance and support were essential to my research and this work would not have been possible without him. He has always made himself available when I need his help. Over the years, I have received a lot of advice and help from him on a wide variety of subjects, both academic and non-academic.

I thank my dissertation committee members Professor Alexander Barg, Leonid Koralov, Prakash Narayan, Adrian Papamarcou, and Sennur Ulukus. Especially, I am thankful to Professor Narayan and Papamarcou who served as members for both my proposal exam and thesis defense. They have pointed out the importance of having a broader perspective and gave me useful advice on technical presentations. I am grateful to Professor Koralov for his assistance in a convergence proof in Chapter 4. I also thank Professor Ulukus for useful feedback during the thesis defense.

The love and support received from my family is another essential part for my accomplishments including finishing this dissertation. I have received a lot from my family. My parents are always supportive what I am doing and give constant love and affection over the years. Since I was young, my sister has been taken care of me all the time. When I want to talk, she always opens her ears to listen whatever I am saying. Sometimes, I miss my late mother especially when I look after my little boy. She sacrificed a lot for her children. Thanks to her upbringing, I was able to concentrate on whatever I wanted to do during my early years.

I would like to give special thanks to my wife, Eunyoung. As we have studied in Maryland, we are always together at home and in the school sharing all the good and bad moments in our lives. She has accomplished difficult tasks over the years as a mother and as a graduate student. She has given me the happiest moment in my life including the birth of our baby, Isan. Since his birth he has been a joy of our lives. I am also grateful to Ilwoo and her children, Hyungjun and Yoojin for taking care of Isan.

Living in a foreign country often involves loneliness. However, I can overcome this difficulty by making good friendships with many friends including Dongwoon, Hojin, Doohyun, and their families. We have been together to share the joys and sorrows, have many lively conversations. I would like to thank Punarbasu who were here at the early stage of my research providing advice and many ideas toward the first part of my work. I also thank Sohil for his help of finding applications of the last part of the project. I am happy to have a chance to know many good colleagues over the years.

I would like to thank Tracy Chung, Melanie Prange, Maria Hoo, and other ECE staffs for their administrative support and assistance. I am also thankful to Vivian Lu who makes many complicated financial problems easy.

Finally, I thank the NSF for their grants, CCF0916919 and CCF0830699.

Table of Contents

List of Figures

Chapter 1
Introduction

1.1 Linear Codes

Applications of error correcting codes include a range of communication problems such as noise reduction in long-haul optical and wireless communication, increasing write density in flash memory devices, bandwidth savings in the transport layer of networks, and many more. Coding methods employed in many practical applications map data to code sequences using linear transformations. Linear codes have an advantage of short description, simple encoding procedures, and in many cases can be equipped with simple error correction (decoding) algorithms. Families of linear codes are also often amenable to easier theoretical analysis, and therefore have become ubiquitous in engineering applications. Moreover, the same set of properties of linear codes has made them useful in many problems of theoretical computer science and discrete mathematics.

In simple models of information exchange, linear codes have been shown to attain the theoretical limit set forth by Shannon's "mathematical theory of communication" [62]. Linear codes are known to support transmission at data rates arbitrarily close to channel capacity in symmetric discrete memoryless channels (DMCs) [23, 3], to enable the optimal compression rate for discrete memoryless sources [19], as well as to support optimal distributed data compression [64], transmission over simple models of "wiretap channels" [67], generation of secret bits from correlated random observations [71, 73], and a range of other applied and theoretical problems.

Many decoding procedures of linear codes for basic transmission models such as the binary symmetric channel (BSC) are based on finding or approximating the member of the codebook that minimizes the Hamming distance to the sequence received from the channel. The introduction of the Hamming metric has lead to numerous studies of linear codes and their structural properties, sometimes motivated by communication problems, while sometimes extending beyond the context of applications. These studies gave rise to algebraic and combinatorial theory of error correcting codes that includes numerous sophisticated constructions of codes as well as deep structural results. At the same time, even though early results in information theory guarantee the existence of linear capacity-achieving codes, until very recently effective versions of Shannon theorem remained elusive. The first such result was obtained in 2009 with the discovery of the family of polar codes [3].

This dissertation is devoted to a study of a class of linear codes related to a particular metric space that generalizes the Hamming space in that the metric function is defined by a partial order on the set of coordinates of the vector. This metric, called the ordered distance or the Niederreiter-Rosenbloom-Tsfasman (NRT) distance, initially arose in several independent works devoted to numerical analysis, communication, and algebraic coding theory [47, 57]. In the first part of the thesis, we address several structural questions of the theory of linear codes motivated by

this metric, calling them linear ordered codes. In the second part, we define simple probabilistic channel models that are in a certain sense matched to the ordered distance, and prove several results related to performance of linear codes on such channels. These results extend the body of classical results on linear codes to the ordered case. This extension, which covers linear-algebraic properties of codes and their relations to the theory of ordered matroids, is the subject of the first two chapters in the main text.

In the third part of this dissertation we study polar codes that are related to the ordered metric. This study leads to a construction of a family of polar codes that support reliable transmission at rates up to capacity on a nonbinary symmetric channel with input of cardinality $q = 2^r, r = 2, 3, \ldots$. The polarization procedure in this case shows an interesting feature compared to the basic construction of [3]: the data symbols polarize to many (rather than 2) levels, at the same time, permitting an easy and compact description of such "extremal configurations."

1.2 A Theory of Linear Ordered Codes

1.2.1 Linear Codes and Their Invariants

The main aspects of classical theory of linear codes over finite fields (for the Hamming metric) involve studying their structural properties derived from the distribution of Hamming weights, a range of related algebraic facts, as well as their performance on communication channels and their applications in capacity-achieving results for various data transmission and processing models.

We develop elements of this theory for codes in the ordered Hamming space. To define it, let $\mathbb{F}_q$ be the finite field of q elements and let $\mathbb{F}_q^N$ be the vector space of dimension N over it. Suppose that the set of $N = nr$ coordinates is partitioned into n disjoint subsets. Define the weight of a vector $\boldsymbol{x} \in \mathbb{F}_q^N$ as

$$\|\boldsymbol{x}\| = \sum_{i=1}^{n} \max\{j, 1 \le j \le r : x_{i,j+1} = x_{i,j+2} = \cdots = x_{i,r} = 0\}.$$

(it is easy to prove that this is a well-defined norm). We call $\|\boldsymbol{x}\|$ the ordered weight of $\boldsymbol{x}$ and call the corresponding distance the *ordered distance*. This term is related to a partial order on the set $[N] = \{1, 2, \ldots, N\}$ and will be made clear below in Chapter 2, where we put this definition in the framework of poset weights on the space of q-ary vectors. The set $\mathbb{F}_q^N$ together with the ordered distance is called the ordered Hamming space.

The ordered weight was first defined by Niederreiter [46, 47]. These works prompter Brualdi et al. [15] to define norms associated with general partial orders on $[N]$. However, most applications of poset metrics are associated with the ordered Hamming space $\mathbb{F}_q^{nr}$. Codes in $\mathbb{F}_q^{nr}$ are used to construct uniformly distributed sets of points in the unit cube for the purpose of numerical integration [46]. Rosenbloom and Tsfasman [57] defined the ordered metric by considering one generalization of Reed-Solomon (RS) codes. The ordered norm was also used by Massey and Serconek [43] in their study of linear complexity of sequences. Nielsen [48] considered the ordered distance for the analysis of a list decoding algorithm for the RS-like codes of [57]. Currently the ordered Hamming space and more general metrics on partial orders form the subject of a large body of literature (e.g., [42, 24, 35, 11, 32, 7, 8, 49]).

In this thesis we have pursued a linear-algebraic approach to the enumeration of vectors in linear ordered codes. It turns out that an algebraically meaningful invariant is obtained if the codewords are grouped not by the value of their weights, but by certain numerical characteristics that we call shapes. Taking the perspective of shape enumerators, we examine the MacWilliams

relations as well as related results such as the Greene theorem (a relation known classically to connect linear codes and matroids). A related set of combinatorial invariants of codes, introduced by Wei [67] generated much interest in the study of subcode weights and supports of linear codes. In [67], Wei showed that generalized Hamming weights (or support weights) characterize the code's performance for a certain model of a wiretap channel ("Wiretap channel of type II" [50]). Later, Greene's results were extended to support weight distributions [6, 12, 13]. We study support shape distributions in their relation to the Tutte polynomial of matroids. The cornerstone of this relation is formed by the so-called *Tutte polynomial* of matroids and closely connected functions such as the rank-nullity function (the Whitney rank function). We define a multivariable version of the Tutte polynomial for poset matroids and establish its links with the shape enumerators of codes.

1.2.2 Information Transmission with Linear Ordered Codes

Until recently, most of the works on ordered codes have focused on combinatorial aspects of the ordered Hamming metric. There are a few notable exceptions, the most important being the works by Rosenbloom and Tsfasman [57] and Tavildar and Viswanath [66] (see also [28]). The first of these papers discussed a setting under which information is transmitted over a set of parallel channels subject to fading for which the ordered metric is a figure of merit. The second one independently introduced a closely related model which describes the noise process in an actual wireless fading system. To describe the model, suppose that the sender encodes a message $\boldsymbol{u}$ into a codeword vector $\boldsymbol{x} \in \mathbb{F}_q^{nr}$ of length $N = nr$ and transmits it through r parallel channels to the receiver. Denoting by $\boldsymbol{y}$ the received N-dimensional sequence, we proceed from observing that the distance $\|\boldsymbol{y} - \boldsymbol{x}\|$ is computed blockwise by the r-blocks in the vectors. The distance within a block is dominated by rightmost coordinate in which $\boldsymbol{y}$ and $\boldsymbol{x}$ are different.

Motivated by this description, we define a class of DMCs in which each r-block is sent over r parallel synchronized links that are subordinated in the sense that if the ith link is exposed to high noise in a given time slot, then so are the links $1, \ldots, i-1$ within the same slot. Thus if $(y_1, \ldots, y_r)$ and $(x_1, \ldots, x_r)$ denote one r-block of the received and transmitted data, respectively, and the noise in the channels is confined to erasures, then the typical situation is described by the relations $y_1 = \cdots = y_i =?$ (the erasure symbol) and $y_j = x_j, j = i+1, \ldots, r$.

This channel model prompted us to examine the question of more general channels that can be associated with the ordered distance introduced above. In the classical setting of symmetric channels, the Hamming distance serves as a sufficient statistic for optimal decoding of received patterns in the sense that the closest code sequence is also the most probable one. For the ordered distance and the newly defined channels, this link is not as straightforward because of the complicated combinatorial structure of the metric; nevertheless, we show that the channel models we introduce still support one direction of the above correspondence. We also establish a number of other basic results for ordered linear codes and examine the problem of transmission over the "ordered wiretap channel." We establish capacity results for this case as well as the connection between such channels and support (ordered) weight distributions.

1.3 Polarization of Nonbinary Channels

Polarization is a new concept in information theory discovered in the context of capacity-achieving families of codes for symmetric memoryless channels and later generalized to source coding, multi-user channels and other problems. Polarization phenomenon was first introduced by Arıkan [3] who constructed binary codes that achieve capacity of symmetric memoryless channels (and

"symmetric capacity" of general binary-input channels). The main idea of [3] is to combine the bits of the source sequence using repeated application of the "polarization kernel" $H_2 = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$. The resulting linear code of length $N = 2^n$ has the generator matrix which forms a submatrix of $G_N = H_2^{\otimes n}$. The choice of the rows of G_N is governed by the polarization of virtual channels for individual bits that arise in the process of channel evolution. More specifically, the data bits are written in the coordinates that correspond to near-perfect channels while the other bits are fixed to some values known to both the transmitter and the decoder. It was shown later that polarization on binary channels can be achieved using a variety of other kernels: in particular, any $m \times m$ matrix whose columns cannot be arranged to form an upper triangular matrix, achieves the desired polarization [37].

A connection between our studies of the ordered distance and polar codes arises when one attempts to extend the construction of polar codes to q-ary channels with alphabets other than binary. We focus on the case of $q = 2^r$ (arguably the most important one for applications) and restrict our attention to the polarization kernel H_2. A number of interesting properties of polar codes arise when encoding with the matrix G_N follows the operations in the ring $\mathbb{Z}_q$ rather than the field $\mathbb{F}_q$.

Earlier studies of nonbinary polar codes were undertaken in a number of works starting with the papers by Şaşoğlu et al. [59] and Mori and Tanaka [45]. For prime q, [59] showed that by using H_2, the virtual channels for individual q-ary symbols after sufficiently many steps become either fully noisy or perfect, and the proportion of perfect channels approaches the symmetric capacity of the channel. At the same time, [59] remarked that the transmission scheme that uses the kernel H_2 with modulo-q addition for composite q does not necessarily lead to polarization of the channels to the two extremes. Rather, they showed that there exists a sequence of permutations of the input alphabet such that when they are combined with H_2, the virtual channels for the transmitted symbols become either nearly perfect or nearly useless. The authors of [59] suggested several alternatives to the kernel H_2 that rely on randomized permutations or, in the case of $q = 2^r$, on multilevel schemes that implement polar coding for each of the bits of the symbol independently, combining them in the decoding procedure. Very recently a class of transformations that achieve two-level polarization for arbitrary q was found in [60].

Another related work is the paper by Abbe and Telatar [1]. In it, the authors observed multilevel polarization in a somewhat different context. The main result of their paper provides a characterization of extremal points of the region of attainable rates when polar codes are used for each of the r users of a multiple-access channel. Namely, as shown in [1] (see also [2]), these points form a subset in the set of vertices of a matroid on the set of r users. [1] also remarks that these results translate directly to transmission over a q-ary DMC, showing that the rate polarizes to many levels. To explain the difference between [1] and our work, we note that transmission over the multiple-access channel in [1] is set up in such a way that, once applied to the DMC, it corresponds to encoding each bit of the q-ary symbol by its own polar code (we again assume that $q = 2^r$). In other words, the polarization kernel employed is a linear operator $G = I_r \otimes H_2$. Thus, the group acting on $\mathcal{X}$ is $\mathbb{F}_{2^r}^+ = \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2$ rather than the cyclic additive group of order q considered in this thesis. This results in a large number of extremal configurations, which complicates the actual construction of the codes.

1.4 Contributions and the Structure of the Dissertation

The dissertation is organized as follows. Chapter 2 is devoted to a study of basic properties of linear ordered codes over finite fields. We begin with describing an algebraic perspective of the

invariants of linear codes in the classical case, including the connection of the weight distribution of the code and the rank polynomial of the underlying matroid. Developing this link, we define the Tutte polynomial of a linear ordered code and establish an analog of the Greene's theorem [29] for it. An interesting feature of this result is that, unlike its many other versions, we need to consider a multivariate Tutte polynomial. As a by-product we obtain a new proof of the MacWilliams theorem for ordered linear codes [42, 24]. We further extend these considerations to *higher poset weights* introduced in [8] in analogy to Wei's work [67] (independently they were also defined in [49]). In particular, we relate the distribution of higher weights of an ordered code to the multivariate Tutte polynomial. Using these considerations, we find the higher weight distribution of ordered Maximum Distance Separable (MDS) codes. Finally, we remark that ordered MDS codes represent uniform poset matroids, which is an extension of the corresponding result in the Hamming space. This work is published in [52].

In Chapter 3, we develop the relation of the ordered Hamming space to the context of information transmission. Using the models in [57, 66] as a starting point, we define the *ordered symmetric channel* and the *ordered erasure channel* which are counterparts of the q-ary symmetric channel and the q-ary erasure channel, respectively. These channels can be also viewed as vector channels or as dependent parallel channels. We compute the capacity of the newly defined channels and show that this quantity is achieved by linear ordered codes. As an application of these results, we present the parallel wiretap channels which extend the wiretap channel of type I [72] and type II [50] and show that linear ordered codes attain secrecy capacity of these channels (these results were previously published in [53]).

In Chapter 4, we study polarization for channels with input alphabet of size $q = 2^r, r = 2, 3, \ldots$. Suppose that the channel is given by a stochastic matrix $W(y|x)$ where $x \in \mathcal{X}, y \in \mathcal{Y}, \mathcal{X} = \{0, 1, \ldots, q-1\}$, and $\mathcal{Y}$ is a finite alphabet. Assuming that the steps of the polarization process are performed using the kernel H_2 with addition modulo-q, we establish results about the polarization of channels for individual symbols. A symbol from the alphabet $\mathcal{X}$ is transmitted in each channel use. For the purpose of analysis we represent the symbols as r-blocks of bits and write $x = (x_1, x_2, \ldots, x_r), x \in \mathcal{X}$. It turns out that virtual channels for the transmitted symbols converge to one of $r + 1$ *extremal configurations* in which j out of r bits are transmitted nearly perfectly while the remaining $r - j$ bits carry almost no information, $j = 0, 1, \ldots, r$. Moreover, the good bits are always aligned to the right of the transmitted r-block, and no other situations arise in the limit. Thus, the extremal configurations that arise as a result of polarization are easily characterized: they form an upper-triangular matrix as described in Section 4.4 (see also Figs. 4.2 and 4.3). This characterization also constitutes the main difference of our results from the multilevel schemes in [59, 1]; namely, our construction gives rise to a much smaller number and easier description of the emerging extremal configurations. These results form the subject of the papers [54, 55, 56].

Another result in this part is related to the question of "controlled polarization." As noted above, very recently Şaşoğlu [60] found kernels that result in polarization to two extremal configurations (fully noisy or noiseless symbols) for general q-ary alphabets. At the same time, the polarization scheme for q-ary symbols ($q = 2^r$) based on the Arıkan kernel results in $r + 1$ extremal configurations of bits in polarized channels. A natural theoretical extension of this result, supported by applications in video coding, calls for designing polarizing transforms that yield in a predefined subset of extremal configurations. Answering this challenge, we design polarization maps that result in polarization to any specified number of levels in the range $2 \leq k \leq r$, at the

same time obtaining a new proof of the result in [60].

Publications: The results of this dissertation are published in a number of papers that appeared in 2010-2012, see [52]-[56].

Chapter 2

Linear Ordered Codes

In this chapter we develop combinatorial and linear-algebraic aspects of the theory of linear ordered codes. In Section 2.1 we recall the setting of the theory of linear codes in the classical case with an outlook to the case of the ordered metric, which is covered in the subsequent sections.

2.1 Introduction: Linear Codes in the Hamming Space

2.1.1 Hamming Weight

Let $\mathbb{F}_q$ be the finite field of order q and let $\mathcal{X}^n = \mathbb{F}_q^n$ be the n-dimensional vector space over $\mathbb{F}_q$. A linear $[n, k]$ code $\mathcal{C}$ is a linear k dimensional subspace of $\mathcal{X}^n$. In the context of information transmission, a linear code is a linear map $\mathcal{C} : \mathbb{F}_q^k \to \mathbb{F}_q^n$ which "encodes" k data symbols into n channel symbols. Below we do not differ between these two definitions, using both as convenient.

Linear codes afford a concise description in terms of their bases and support easily implementable decoding algorithm based on this description. Moreover, many particular families of linear codes are based on algebraic constructions (e.g., BCH and RS codes), or are constructed in terms of bipartite graphs. In both cases, the additional structure gives rise to relatively simple decoding procedures, making the above two families the method of choice for various communication systems such as coding for flash memories and hard drives, coding for wireless links, mobile applications, fixed wireless systems, and many others.

One of the main tools in structural analysis of linear codes as well as in the analysis of their performance in communication systems is related to the "distribution of weights" in the code. To motivate it, let $d_H(\cdot, \cdot)$ denote the Hamming distance on $\mathcal{X}^n$ (the number of distinct coordinates). A transformation $g : \mathcal{X}^n \to \mathcal{X}^n$ such that $d(g\boldsymbol{x}, g\boldsymbol{y}) = d(\boldsymbol{x}, \boldsymbol{y})$ for all $\boldsymbol{x}, \boldsymbol{y} \in \mathcal{X}^n$ is called an isometry. Isometries of the Hamming space form a group $G = \mathfrak{S}_q \wr \mathfrak{S}_n$ which consists of permutations of coordinates followed by permutations of symbols in each coordinate. G acts transitively on $\mathcal{X}^n$ in the sense that for any $\boldsymbol{x}, \boldsymbol{y}$ there is an isometry such that $g\boldsymbol{x} = \boldsymbol{y}$. The linear part of the group is formed by the subgroup $GL(\mathcal{X}^n) = (\mathbb{F}_q^*)^n \rtimes \mathfrak{S}_n$ (permutations of coordinates and multiplications by a nonzero element of the field).

Now let $\mathcal{C}$ be a linear code and let $S_\delta(\boldsymbol{x}) := \{\boldsymbol{y} \in \mathcal{C} : d_H(\boldsymbol{x}, \boldsymbol{y}) = \delta\}$ be the set of neighbors of $\boldsymbol{x}$ in $\mathcal{C}$ that are distance δ away from it. Since the code is linear, and since the Hamming distance is translation invariant, $|S_\delta(\boldsymbol{x})| = |S_\delta(0)|$, which is shown by shifting $\boldsymbol{x}$ to the all-zero vector. Hence the distribution of distances in the code is completely characterized by the distribution of neighbors of zero. At the same time, we observe that $GL(\mathcal{X}^n)$ acts linearly and transitively on the sphere $S_\delta(0)$. Therefore, the Hamming weight emerges not only as a natural metric on $\mathcal{X}^n$ but also as a natural invariant in the study of linear codes and of the space $\mathcal{X}^n$ in

general. This point of view will be useful when we develop a similar invariant in the ordered case in the next section. As will be seen, it is not as immediate as the Hamming weight, and would be difficult to isolate without considering the action of the isometry group.

2.1.2 Weight Enumerators

2.1.2.1 ***MacWilliams Theorem.*** Given a linear code $\mathcal{C} \in \mathcal{X}^n$, we define the *weight enumerator* as a homogeneous polynomial

$$A_{\mathcal{C}}(z_0, z_1) = \sum_{\boldsymbol{x} \in \mathcal{C}} z_0^{n-\mathrm{wt}_H(\boldsymbol{x})} z_1^{\mathrm{wt}_H(\boldsymbol{x})},$$

where $\mathrm{wt}_H(\cdot)$ denotes the Hamming weight. This polynomial depends on one variable $u = z_1/z_0$, which corresponds to the fact that the action of G on $\mathcal{X}^n$ is distance-transitive. Letting $A_w := |\{\boldsymbol{x} \in \mathcal{C} : \mathrm{wt}_H(\boldsymbol{x}) = w\}|$, we can write

$$A_{\mathcal{C}}(z_0, z_1) = \sum_{w=0}^{n} A_w z_0^{n-w} z_1^w.$$

A useful point of view is provided by considering duality of linear codes. Let $\chi_{\boldsymbol{a}}(\boldsymbol{x}) = e^{2\pi i(\boldsymbol{a},\boldsymbol{x})/q}$, $\boldsymbol{a} \neq 0$ be a character of the additive group $\mathbb{Z}_q$. The dual code $\mathcal{C}^\perp := \{\chi : \chi(\boldsymbol{x}) = 1 \text{ for all } \boldsymbol{x} \in \mathcal{C}\}$ is defined by a subset of the character group. Identifying the dual groups, we can write $\mathcal{C}^\perp = \{\boldsymbol{y} \in \mathcal{X}^n : (\boldsymbol{x}, \boldsymbol{y}) = 0 \text{ for all } \boldsymbol{x} \in \mathcal{C}\}$. A finite version of the Poisson summation formula yields the *MacWilliams equation:*

$$A_{\mathcal{C}^\perp}(z_0, z_1) = A_{\mathcal{C}}(u_0, u_1), \tag{2.1}$$

where $u_0 = z_0 + (q-1)z_1$ and $u_1 = z_0 - z_1$. This equation can be proved using harmonic analysis on $\mathcal{X}^n$ (as in the above approach) or using a linear-algebraic point of view as detailed below (both approaches were suggested in the original paper by MacWilliams [40]).

Observe that a vector $\boldsymbol{x} \in \mathcal{C} \setminus \{0\}$ gives rise to a one-dimensional subspace $\{\alpha\boldsymbol{x}, \alpha \in \mathbb{F}_q^*\}$. Let $\mathrm{supp}(\boldsymbol{x}) := \{i \in [n] : x_i \neq 0\}$ be the support of the vector. Given a subcode A of the code $\mathcal{C}$, define its support as

$$\mathrm{supp}(A) = \cup_{\boldsymbol{x} \in A} \mathrm{supp}(\boldsymbol{x}).$$

We can think of the distribution of Hamming weights in $\mathcal{C}$ as of the distribution of support weights of one-dimensional linear subspaces of $\mathcal{C}$. Extending this notion, let us introduce the mth *support weight enumerator* of $\mathcal{C}$ as

$$A_{\mathcal{C}}^j(z_0, z_1) = \sum_{D \subset \mathcal{C} : \dim D = m} z_0^{n - |\mathrm{supp}(A)|} z_1^{|\mathrm{supp}(A)|},$$

where the sum ranges over all m-dimensional linear subcodes of $\mathcal{C}$ and $m = 1, 2, \ldots, k$. Support weight distributions were defined by Wei [67] in the context of communication over a combinatorial wire-tap channel. MacWilliams identities for support weight enumerators were proved by Kløve [36] using the linear-algebraic approach. At the same time, support weights do not seem to afford an interpretation in the context of harmonic analysis.

2.1.2.2 ***Matroids and linear codes*** A matroid $\mathcal{M}$ is a finite set E together with a nonempty set $\mathcal{B}$ of its subsets, called bases, that satisfy the following property [68]:

(*Base exchange property*) If A and B are distinct members of $\mathcal{B}$ and $a \in A \setminus B$, then there exists an element $b \in B \setminus A$ such that $(A \setminus \{a\}) \cup \{b\} \in \mathcal{B}$.

It can be shown that all bases are of the same cardinality, and no base is a subset of another base. The common cardinality of the bases is called the rank of $\mathcal{M}$. Any subset $I \subset B, B \in \mathcal{B}$ is called an *independent set* of $\mathcal{M}$. The *rank function* of the matroid $\mathcal{M}$ is defined as $\rho : 2^E \to \mathbb{N} \cup \{0\}$ where $\rho(A), A \subset E$ equals the cardinality of a largest-size independent subset contained in A.

A matroid is called *linear* if it can be realized in a k-dimensional vector space $\mathbb{F}_q^k$. To represent the linear matroid $\mathcal{M}$, we choose a basis of the space and a set $\mathbf{G}$ of n vectors that form a k-dimensional subspace. Letting $E = \{1, 2, \ldots, n\}$, we take E with the ground set of $\mathcal{M}$. Suppose that the n vectors are numbered by the elements of E. Then we say that the matroid $\mathcal{M}$ is represented over $\mathbb{F}_q$ if the bases of $\mathcal{M}$ correspond to all the k-tuples of linearly independent vectors out of $\mathbf{G}$.

A connection between matroids and linear codes was developed by Greene in [29]. Namely, suppose that a matroid $\mathcal{M}$ is represented by a linear $[n, k]$ code $\mathcal{C}$. Let E be an n-set of k vectors such that the $k \times n$ matrix formed of them forms a basis of the code $\mathcal{C}$. Define the *rank enumerator* of $\mathcal{M}$ as follows:

$$R_{\mathcal{M}}(x, y) = \sum_{u=0}^{n} \sum_{v=0}^{k} R_u^v x^u y^v, \tag{2.2}$$

where

$$R_u^v = \{F \subset E : |F| = u, \mathrm{rk}(F) = v\}.$$

The rank enumerator is related to the *Tutte polynomial* $\mathcal{T}_{\mathcal{M}}$ through a change of variables [68, 65]:

$$\mathcal{T}_{\mathcal{M}}(z_0, z_1) = (z_0 - 1)^k R_{\mathcal{M}}(x, y),$$

where $x = z_1 - 1, y = ((z_0 - 1)(z_1 - 1))^{-1}$.

Both polynomials contain the same information about the matroid and in this sense are equivalent.

The Greene theorem [29]. Let $R_{\mathcal{M}\perp}(x, y)$ be the rank enumerator of $\mathcal{M}^\perp$. The Greene theorem states that

$$z_1^{-n} q^{-k} A_{\mathcal{C}}(z_0, z_1) = R_{\mathcal{M}}(x, y)$$

where $x = (z_0 - z_1)/z_1, y = 1/q$.

The linear-algebraic content of the MacWilliams equation is related to the concept of the dual matroid. The *dual matroid* $\mathcal{M}^\perp$ of the matroid $\mathcal{M}$ is defined on the same ground set E as $\mathcal{M}$ by the condition that the bases of $\mathcal{M}^\perp$ are given by the complements of the bases of $\mathcal{M}$. A simple linear-algebraic argument shows that

$$R_{\mathcal{M}^\perp}(x, y) = x^n y^{n-k} R_{\mathcal{M}}\Big(\frac{1}{xy}, y\Big).$$

Combining these two equations, we can recover the MacWilliams relation (2.1).

This theorem was generalized to support weight distributions in [6]. Namely, let

$$D_C^j(z_0, z_1) = \sum_{w=0}^{n} \Big(\sum_{m=0}^{j} A_w^j \prod_{s=0}^{m-1} (q^j - q^s) \Big) z_0^{n-i} z_1^i,$$

where A_w^j is the number of j-dimensional subcodes of C with support of size w. For all $j \geq 1$, we have

$$z_1^{-n} q^{-k} D_C^j(z_0, z_1) = R_{\mathcal{M}}(x, y),$$

where $x = (z_0 - z_1)/z_1, y = 1/q^j$. Later this theorem was generalized in several other related ways; see Britz [12, 13]. Recently, Jurrius and Pellikaan [33] wrote an extensive survey on support weight enumerators of linear codes and the Tutte polynomial of matroids. Duursma [25] studied the rank polynomial for a matroid and two-variable zeta functions for codes and established a relation between them which also includes Greene's theorem.

2.2 Ordered Hamming Metric

In the remainder of this chapter we develop an extension of the properties of classical linear codes discussed in the previous sections to the setting of the ordered Hamming space.

We begin with the definition of general metrics on partially ordered sets (poset metrics) [15]. Denote by E a finite set of N elements that will correspond to the coordinate set of a linear code. Let P be a partial order $\prec$ defined on E. We call the resulting structure a poset and denote it by $\mathcal{P} = (E, P)$. An *order ideal* is a subset $I \subset E$ such that if $i \in I$ and $j \prec i$ then $j \in I$. The set of all ideals of P will be denoted by $\mathcal{I}(P)$. For a subset $A \subset E$ let $\langle A \rangle = \bigcap_{I \supset A} I$ be the smallest-size ideal of P that contains A. Following [15], define the *poset weight* of a vector $\boldsymbol{x} \in \mathbb{F}_q^N$ as the cardinality of the smallest ideal that contains all the nonzero coordinates of $\boldsymbol{x}$:

$$\mathrm{wt}_P(\boldsymbol{x}) = |\langle \mathrm{supp}(\boldsymbol{x}) \rangle|.$$

It is easy to see that the poset weight satisfies the triangle inequality. The distance d_P derived from wt_P is called the *poset metric* on $\mathbb{F}_q^N$.

The Hamming metric corresponds to P being a single antichain (all the coordinates are incomparable). Below we are mostly interested in the Niederreiter-Rosenbloom-Tsfasman (NRT) metric which is obtained if $N = nr$ and P is taken to be a disjoint union of n chains of length r:

$$E = U_1 \cup \cdots \cup U_n \tag{2.3}$$

$$|U_i| = r, i = 1, \ldots, n;\ U_i \cap U_j = \emptyset \text{ if } i \neq j; \tag{2.4}$$

$$u_{i,j} \prec u_{i',j'} \text{ iff } i = i' \text{ and } j < j'.$$

Below we call the corresponding distance the *ordered metric*, and call $\mathbb{F}_q^{nr}$ the ordered Hamming space. Our main object of study in this chapter is codes and coding for the ordered Hamming space.

Let E be the set of code's coordinates, and let P be the NRT partial order on E given as in (2.3). Call a subset $X \subset E$ *left-adjusted* (l.a.) if it is an ideal in P. Thus, the ordered weight of a vector equals the size of the smallest l.a. subset that contains its support.

The *dual poset* $P^\perp$ on the set E is identical to P except the fact that the order is inverted: $x \prec y$ in $P^\perp$ if and only if $y \prec x$ in P. This definition is standard in combinatorics, but in our context it is additionally motivated by the duality of linear codes and the associated duality of association schemes related to the metric spaces. The dual space of $\mathcal{P}$ is written as $\mathcal{P}^\perp = (E, P^\perp)$.

We consider linear codes in the space $\mathbb{F}_q^N$. As before, the code $\mathcal{C}^\perp$ which is dual to a linear code $\mathcal{C} \subset \mathbb{F}_q^N$ is defined using the character group of $\mathbb{Z}_q$. We can write

$$\mathcal{C}^\perp = \{\boldsymbol{y} \in \mathbb{F}_q^N : (\boldsymbol{x}, \boldsymbol{y}) = 0 \text{ for all } \boldsymbol{x} \in C\}.$$

Importantly, the distances in the dual code are measured with respect to the dual poset $P^\perp$. This makes the theory of linear codes consistent in a number of examples including the ordered Hamming space. The general situation was examined in [9], where some relations between dual codes

and dual posets were characterized in terms of association schemes. Without going into these details, we refer the reader to Delsarte's work [20] which was the first to define duality of linear codes in an algebraic way. A detailed description of this theory is given in [14]. It was further specialized for the ordered Hamming space in [42] and [7].

Now let us determine the invariants of linear codes in the ordered Hamming space that are likely to have properties analogous to the properties of the Hamming weight and related quantities considered above. For this, we use the insight developed in Sect. 2.1.1. It will become apparent that the ordered weight is not a good choice because the linear group of isometries of the ordered Hamming space is not transitive on spheres of a given (ordered) radius around zero.

Groups of linear automorphisms of poset metric spaces were computed in [51]. They are formed of poset automorphisms combined with linear transformations of the space that preserve the P-support of vectors. For the ordered Hamming space, the group of linear isometries $GL_P = T(q,r) \wr \mathfrak{S}_n$, where $T(q,r)$ is the group of upper triangular matrices over $\mathbb{F}_q$ with nonzero main diagonal and $\mathfrak{S}_n$ is the permutation group on n elements. Clearly, $\mathfrak{S}_n$ is the automorphism group of the NRT poset P while $T(q,r)$ preserves the ideals (the P-supports). A linear isometry acts by permuting the chains and multiplying the subvectors on each r-chain by triangular matrices.

To define the appropriate invariant, we need to describe the "sphere" S_e around zero on which GL_P acts transitively, i.e. each vector $\boldsymbol{x} \in S_e$ is moved to any other vector $\boldsymbol{y} \in S_e$ by an appropriate element of the group. For

$$\boldsymbol{x} = (x_{11}, \ldots, x_{1r}; x_{21}, \ldots, x_{2r}; \ldots; x_{n1}, \ldots, x_{nr})$$

define the *shape* of $\boldsymbol{x}$ with respect to P as an r-vector $e = (e_1, e_2, \cdots, e_r)$, where

$$e_i = |\{U_j : \max(l : x_{jl} \neq 0) = i,\ 1 \leq i \leq n\}|.$$

(see (2.3)). We denote the set of vectors of a given shape e by S_e and observe that the action of GL_P is transitive on S_e. At the same time, it is easy to see that the action of GL_P is not transitive on vectors of the same weight (it suffices to take two vectors of equal weights, but different shapes). We conclude that the theory of linear codes should be developed for shapes and their enumerators.

The above definition extends in an obvious way to the shape of an ideal $I \in \mathcal{I}(P)$. We use the same notation $\mathrm{shape}(I)$ to refer to the shape of I. Thus, $\mathrm{shape}(\boldsymbol{x}) = \mathrm{shape}(\langle \mathrm{supp}(\boldsymbol{x}) \rangle)$.

In conclusion, we have a few remarks on notation. For a shape vector $e = (e_0, e_1, \cdots, e_r)$ we denote by $\bar{e}$ the shape obtained by setting $\bar{e}_i = e_{r-i}$, $i = 0, \cdots, r$. For brevity we write $|e| = \sum_{i=1}^{n} e_i$ and denote $e_0 = n - |e|$. We also use the notation $|e|' = \sum_i i e_i$. It is easy to check that $\mathrm{wt}_P(\boldsymbol{x}) = |e|'$ where e is the shape of a vector $\boldsymbol{x}$. We also use the notation $f \leq e$, where f and e are shape vectors, as a shorthand for the following set of conditions:

$$f_{r-l+1} + \cdots + f_r \leq e_{r-l+1} + \cdots + e_r, \quad l = 1, \ldots, r. \tag{2.5}$$

2.3 Linear Codes and Shape Enumerators

Let $\mathbb{F}_q^{nr}$ be the ordered Hamming space. An (nr, M, d) ordered code $\mathcal{C} \subseteq \mathbb{F}_q^{nr}$ is a subset of M vectors in $\mathbb{F}_q^{nr}$ whose ordered distance between any two distinct vectors in $\mathcal{C}$ is at least d. A linear $[nr, k, d]$ ordered code $\mathcal{C}$ is a linear k-dimensional subspace of the ordered Hamming space. We begin with an example of a family of linear ordered codes.

Example 2.1 *(Ordered RS codes [57]) Let $\mathcal{F}_k = \{f \in \mathbb{F}_q[x], \deg f \leq k-1\}$ be the set of all polynomials of degree less than k over $\mathbb{F}_q$. Let $P = \{p_1, \ldots, p_n\} \subset \mathbb{F}_q$ be a set of points in $\mathbb{F}_q$.*

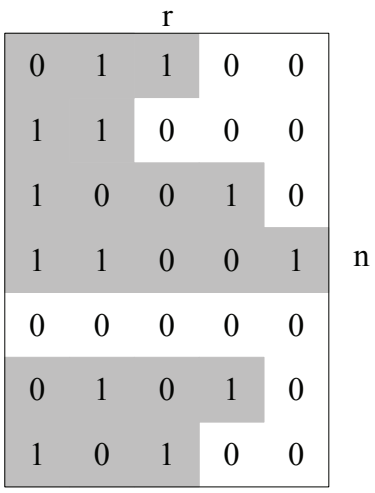

Figure 2.1: A vector in the NRT metric space $\mathbb{F}_q^{nr}, n = 7, r = 5$. The shaded area represents the smallest ideal which contains the support of this vector. The support of this vector is $(0, 1, 2, 2, 1)$.

The usual RS codes are defined through evaluations of the polynomials from $\mathcal{F}$ at the points in the set P. The ordered version of RS codes is obtained if together with the values of the polynomial f we evaluate the values of its first $r-1$ derivatives at each point of P.

Let $f = \sum_{s\geq 0} f_s x^s, f \in \mathcal{F}$ and let $f^{[j]}(x) = \sum_{s\geq j} f_s \binom{s}{j} x^{s-j}$ denote its jth order hyper-derivative. Let us define the evaluation map eval(f) that maps f to a vector $\mathbf{c} \in \mathbb{F}_q^{nr}$ as

$$f \mapsto \boldsymbol{c} = (c_{1,1}, \ldots, c_{1,r}, \ldots, c_{n,1}, \ldots, c_{n,r})$$

where $c_{i,j} = f^{[r-j]}(p_i)$. An $[nr, k]$ ordered RS code is defined as

$$\mathcal{C} = \{eval(f), f \in \mathcal{F}_k\}.$$

It is not difficult to check that the minimum ordered weight of the above code is $nr - k + 1$ which meets the (ordered) Singleton bound. Therefore, the ordered RS codes belong to the class of MDS codes in the ordered metric. Properties and decoding of ordered RS codes are studied in [57], [48].

In accordance with the discussion earlier in this chapter, we define the dual code $\mathcal{C}^\perp$ of a linear code $\mathcal{C}$ as the set of vectors $\{\boldsymbol{x} \in \mathbb{F}_q^{nr} : \forall_{c\in\mathcal{C}} \sum_{i,j} x_{ij} c_{ij} = 0\}$. The distances in the code $\mathcal{C}^\perp$ follow the structure of ideals of the poset $P^\perp$. The metric spaces $\mathcal{P} = (E, P)$ and $\mathcal{P}^\perp = (E, P^\perp)$ are isomorphic linear spaces, and the isomorphism preserves the distance. The weight function in $\mathcal{P}^\perp$ is defined as follows:

$$\mathrm{wt}_{P^\perp}(\boldsymbol{x}) = \sum_{i=1}^{n} \min\{j : x_{i1} = x_{i2} = \cdots = x_{i,j-1} = 0\}, \quad \boldsymbol{x} \in \mathbb{F}_q^{nr}.$$

Let $\mathcal{C}$ be a linear ordered code. Following the previous section, we will be interested in the the *shape enumerator* of $\mathcal{C}$, defined as follows:

$$\begin{aligned} A(z_0, z_1, \cdots, z_r) &= \sum_{\boldsymbol{x} \in \mathcal{C}} z^{\mathrm{shape}(\boldsymbol{x})} \\ &= \sum_{e} \mathcal{A}_e {z_0}^{e_0} {z_1}^{e_1} \cdots {z_r}^{e_r}, \end{aligned}$$

Here on the first line, $z = (z_0, z_1, \ldots, z_r)$ is a vector variable which agrees with the detailed expression on the next line, and $\mathcal{A}_e = |\{\boldsymbol{x} \in \mathcal{C} : \mathrm{shape}(\boldsymbol{x}) = e\}|$ is the number of vectors of shape e in $\mathcal{C}$. The sum on e extends to all partitions of a number n' into a sum of r parts, for all $n' \leq n$.

Let us introduce some notation related to linear codes. Let S be an ideal in P. Let $\mathcal{C}_S := \mathrm{proj}_S \mathcal{C}$ and $\mathcal{C}^S := \{\boldsymbol{c} \in \mathcal{C} : c_e = 0 \text{ for all } e \in S^c\}$ The subcode $\mathcal{C}^S$ is called the *shortening* of $\mathcal{C}$ and the subcode $\mathcal{C}_S$ the *puncturing* of $\mathcal{C}$. While these operations are defined for any subset of E, in the context of our study we restrict them to ideals. By $\mathbf{G}$ and $\mathbf{H}$ we denote a generator and a parity-check matrix of a linear code $\mathcal{C}$. For $S \subset E$ we denote by $\mathbf{G}(S)$ a submatrix of $\mathbf{G}$ formed of the columns indexed by the elements of S.

The following lemma is obvious.

Lemma 2.1 *Let a code $\mathcal{C}$ be a linear ordered code. Then the followings are true:*
1) $\mathcal{C}_S \cong \mathcal{C}/\mathcal{C}^{S^c}$; $\dim \mathcal{C}_S = k - \dim C^{S^c}$,
2) $\dim \mathcal{C}^S = |S| - \mathrm{rank}(\mathbf{H}(S))$,
3) $\dim \mathcal{C}_S = \mathrm{rank}(\mathbf{G}(S))$.

2.3.1 Multivariate Tutte Polynomial

The Tutte polynomial was originally defined for graphs as an invariant that encodes information about the number of various subgraphs such as cycles etc. Crapo [17] generalized the definition of the Tutte polynomial for matroids. For linear codes, the Tutte polynomial contains information about the support weight distribution as well as other numerical invariants of codes. In this section we extend this concept to the case of ordered linear codes.

We begin with a general definition of the Tutte polynomial recently introduced by Sokal in [65]. Let $\mathcal{M}$ be a matroid with ground set $E = \{1, \ldots, N\}$ and the rank function $\rho : 2^E \to \mathbb{Z}^+ \cup \{0\}$. Let $\boldsymbol{v} = (v_1, \ldots, v_N)$. The *multivariate Tutte polynomial* of $\mathcal{M}$ in variables $\boldsymbol{v}, q^{-1}$ is given by

$$Z_{\mathcal{M}}(q, \boldsymbol{v}) = \sum_{S \subseteq E} q^{-\rho(S)} \prod_{s \in S} v_s. \tag{2.6}$$

By $Z_{\mathcal{M}^\perp}$ we denote the Tutte polynomial of the dual matroid (it is obtained upon replacing ρ in the above definition with the dual rank function $\rho^\perp$). By [65],

$$Z_{\mathcal{M}^\perp}(q, \boldsymbol{v}) = q^{\rho(E)} \Big(\prod_{s \in E} \frac{v_s}{q} \Big) Z\Big(\frac{q}{\boldsymbol{v}}\Big) \tag{2.7}$$

where

$$Z\Big(\frac{q}{\boldsymbol{v}}\Big) = \sum_{S \subseteq E} q^{-\rho(S)} \prod_{s \in S} \Big(\frac{q}{v_s}\Big).$$

In the situation of interest for us, the matroid $\mathcal{M}$ is represented by a linear code $\mathcal{C}$. In this case $\rho(S) = \mathrm{rk}(\mathbf{G}(S)), \rho^\perp(S) = \mathrm{rk}(\mathbf{H}(S))$. Below when we have in mind a pair of codes $\mathcal{C}, \mathcal{C}^\perp$, we write Z and $Z^\perp$ instead of $Z_{\mathcal{C}}$ and $Z_{\mathcal{C}^\perp}$, respectively.

These definitions are different from usual definitions of the bivariate rank polynomial of a code (matroid) (2.2), but reduce to them upon putting $x = v_1 = \cdots = v_N$ and $y = 1/q$. Sokal remarks that in several instances the "multivariate extension of a single variable result is not only vastly more powerful but also much easier to prove" [65]. Our study lends further support to this observation: the multivariate Tutte polynomial is well-suited to the case of poset structures on the coordinate set.

2.3.2 The Ordered Case

Let $\mathcal{C} \subset \mathbb{F}_q^{nr}$ be a linear code with the rank function $\rho(S) = \mathrm{rk}(\mathbf{G}(S))$ and let P be the NRT order on E. Our definition of the Tutte polynomial of $\mathcal{C}$ relies on the following two ideas. First, we restrict the summation in (2.6) from all subsets of E to the ideals in (E, P). This idea ties well with the notion of poset matroids below in this chapter. Next, prompted by the shape distribution of codes, we collapse some of the variables in $\boldsymbol{v}$.

Definition 2.1 *Let $\boldsymbol{z} = (z_1, z_2, \ldots, z_r)$ be a vector variable. Define the multivariate Tutte polynomial of $\mathcal{C}$ by*

$$Z(q, \boldsymbol{z}) = \sum_{e} \sum_{\substack{S \in \mathcal{I}(P) \\ \mathrm{shape}(S) = e}} q^{-\rho S} \prod_{i=1}^{r} z_i^{e_i}.$$

The relation of $Z(q, \boldsymbol{z})$ to (2.6) is as follows. For a given ideal S we put $v_s = 1$ if s is not a maximal element in S and put $v_s = z_i$ if s is a maximal element in S and has index i in its chain. Our purpose in this section is to relate Z to the shape enumerator of the code $\mathcal{C}$.

Expanding the ideas of (2.7), we are able to obtain a duality relation for the multivariate Tutte polynomials of a pair of dual ordered codes.

Proposition 2.1 *Let $\mathcal{C}$ be an ordered code, $\mathcal{C}^\perp$ be its dual code, and $Z(q, \boldsymbol{z})$ and $Z^\perp(q, \boldsymbol{z})$ be their Tutte polynomials. Then*

$$Z^\perp(q, z_1, z_2, \ldots, z_r) = q^{\rho E - nr} z_r^n Z\Big(q, \frac{q z_{r-1}}{z_r}, \frac{q^2 z_{r-2}}{z_r}, \ldots, \frac{q^{r-1} z_1}{z_r}, \frac{q^r}{z_r}\Big). \tag{2.8}$$

Proof: From Lemma 2.1, we can obtain the term-by-term duality relation. Let $\bar{A} \in \mathcal{I}(P^\perp), A^c = E \setminus \bar{A} \in \mathcal{I}(P)$, where the bar above the set reflects the fact that this set is considered with respect to the dual poset $P^\perp$. Then

$$\rho^\perp \bar{A} = \rho A^c + |\bar{A}| - \rho E. \tag{2.9}$$

Since this relation can be applied to each term independently, it suffices to prove the claim for one (arbitrary) pair of subsets $(\bar{A}, A^c)$. Let $\mathrm{shape}(\bar{A}) = \bar{e} = (\bar{e}_1, \ldots, \bar{e}_r)$. Then $\mathrm{shape}(A^c) = e = (e_1, e_2, \ldots, e_r)$, where

$$\bar{e}_i = e_{r-i}, \;\; 1 \le i \le r-1; \; \bar{e}_r = n - |e|$$

and $|e|' + |\bar{e}|' = nr$. We have

$$\begin{aligned} q^{-\rho^\perp \bar{A}} \prod_{i=1}^{r} z_i^{\bar{e}_i} &= q^{-\rho A^c - |\bar{A}| + \rho E} \Big(\prod_{i=1}^{r-1} z_i^{e_{r-i}} \Big) z_r^{n-|e|} \\ &= q^{\rho E - nr - \rho A^c + |A^c|} z_r^{n-e_r} \prod_{i=1}^{r-1} \Big(\frac{z_{r-i}}{z_r} \Big)^{e_i} \\ &= q^{\rho E - nr} z_r^n q^{-\rho A^c} \Big(\frac{q^r}{z_r} \Big)^{e_r} \prod_{i=1}^{r-1} \Big(\frac{q^i z_{r-i}}{z_r} \Big)^{e_i}. \end{aligned} \tag{2.10}$$

The claim of the proposition is obtained upon summing on all $\bar{A}$ on the left and all A^c on the right-hand side. ■

Lemma 2.2

$$A(z_0, z_1, \dots, z_r) = \sum_{e, f : f \le e} \mathcal{A}_f N(f, e) (z_0 - z_1)^{e_0} (z_1 - z_2)^{e_1} \dots (z_{r-1} - z_r)^{e_{r-1}} {z_r}^{e_r},$$

where $N(f, e)$, $f \le e$ is the number of pairs $(\boldsymbol{x}, S)$ with $\mathrm{shape}(S) = e$ for a given $\boldsymbol{x}$ with $\mathrm{shape}(\boldsymbol{x}) = f$.

Proof: First, let us consider $N(f, e)$.

$$\begin{aligned} &N(f,e) \\ &= \binom{n}{e} \binom{e_r}{f_r} \binom{e_r + e_{r-1} - f_r}{f_{r-1}} \cdots \binom{e_r + \cdots + e_0 - (f_r + \cdots + f_1)}{f_0} \binom{n}{f}^{-1} \\ &= \binom{e_r + e_{r-1} - f_r}{e_r - f_r} \binom{e_r + e_{r-1} + e_{r-2} - (f_r + f_{r-1})}{e_r + e_{r-1} - (f_r + f_{r-1})} \\ &\quad \times \cdots \times \binom{e_r + \cdots + e_0 - (f_r + \cdots + f_1)}{e_r + \cdots + e_1 - (f_r + \cdots + f_1)} \end{aligned}$$

where $\binom{n}{e} = \binom{n}{e_1\ e_2\ \dots\ e_r}$ is the number of ways to choose r subsets of size $e_1, \dots, e_r$ out of an n-set. We have $\binom{n}{e}$ different sets with shape e. Once the set is given, the number of different vectors with shape f is $\binom{e_r}{f_r} \binom{e_r + e_{r-1} - f_r}{f_{r-1}} \dots \binom{e_r + \cdots + e_0 - (f_r + \cdots + f_1)}{f_0}$. Finally, since we want to count the number of pairs $(\boldsymbol{x}, S)$ for a given $\boldsymbol{x}$, we divide this quantity by $\binom{n}{f}$.

Now, setting $g_i = e_i + \cdots + e_r$ and repeatedly applying the binomial theorem, we obtain the following sequence of equalities:

$$\begin{aligned}
&\sum_e \sum_{f \le e} \mathcal{A}_f N(f,e)(z_0 - z_1)^{e_0}(z_1 - z_2)^{e_1} \dots (z_{r-1} - z_r)^{e_{r-1}} {z_r}^{e_r}. \\
&= \sum_f \mathcal{A}_f \sum_{e_r \ge f_r}^{n} \sum_{e_{r-1} \ge f_r + f_{r-1} - e_r} \cdots \sum_{e_1 \ge f_r + \cdots + f_1 - (e_r + \cdots + e_2)} \binom{e_r + \cdots + e_0 - (f_r + \cdots + f_1)}{e_r + \cdots + e_1 - (f_r + \cdots + f_1)} \\
&\qquad \times \cdots \times \binom{e_r + e_{r-1} - f_r}{e_r - f_r} (z_0 - z_1)^{e_0} \dots (z_{r-1} - z_r)^{e_{r-1}} {z_r}^{e_r} \\
&= \sum_f \mathcal{A}_f \sum_{g_1 = f_1 + \cdots + f_r}^{n} \binom{n - (f_r + \cdots + f_1)}{g_1 - (f_r + \cdots + f_1)} (z_0 - z_1)^{n - g_1} \\
&\qquad \sum_{g_2 = f_2 + \cdots + f_r}^{g_1} \cdots \sum_{g_r = f_r}^{g_{r-1}} \binom{g_{r-1} - f_r}{g_r - f_r} (z_{r-1} - z_r)^{g_{r-1} - g_r} {z_r}^{g_r - f_r} {z_r}^{f_r} \\
&= \sum_f \mathcal{A}_f \sum_{g_1 = f_1 + \cdots + f_r}^{n} \binom{n - (f_r + \cdots + f_1)}{g_1 - (f_r + \cdots + f_1)} (z_0 - z_1)^{n - g_1} \\
&\qquad \sum_{g_2 = f_2 + \cdots + f_r}^{g_1} \cdots \sum_{g_{r-1} = f_{r-1} + f_r}^{g_{r-2}} \binom{g_{r-2} - (f_r + f_{r-1})}{g_{r-1} - (f_r + f_{r-1})} \\
&\qquad\qquad \times (z_{r-2} - z_{r-1})^{g_{r-2} - g_{r-1}} {z_{r-1}}^{g_{r-1} - (f_r + f_{r-1})} {z_{r-1}}^{f_{r-1}} \cdot {z_r}^{f_r} \\
&= \cdots = \sum_f \mathcal{A}_f {z_0}^{f_0} \dots {z_{r-1}}^{f_{r-1}} {z_r}^{f_r} \\
&= A(z_0, z_1, \dots, z_r)
\end{aligned}$$

and therefore the lemma is proved. ∎

Let $\mathcal{B}_e = \sum_{f \le e} \mathcal{A}_f N(f,e)$. Note that this number $\mathcal{B}_e$ generalizes results for binomial moments of linear codes to the ordered case. For linear codes in the Hamming space, binomial moments were implicitly used in [40], while in [5] they became the central object of study in both linear and nonlinear settings.

Remark: The polynomial Z can be written in a different form that is analogous to the Whitney rank function of usual matroids. For an ordered linear code with generator matrix $\mathbf{G}$ let us introduce the *shape-rank distribution* as the set of coefficients

$$R_e^v \triangleq |\{S \in \mathcal{I}(P) : \mathrm{shape}(S) = e, \mathrm{rk}(\mathbf{G}(S)) = v\}|.$$

Then

$$Z(y^{-1}, \boldsymbol{z}) = \sum_e \sum_{v=0}^{k} R_e^v {z_1}^{e_1} {z_2}^{e_2} \dots {z_r}^{e_r} y^v.$$

Using Lemma 2.2, it is possible to relate the shape polynomial to the multivariate Tutte polynomial.

Theorem 2.1 *(Greene's theorem for ordered codes)*

$$A(z_0, z_1, \dots, z_r) = q^k {z_r}^n Z\Big(q, \frac{z_{r-1} - z_r}{z_r}, \frac{z_{r-2} - z_{r-1}}{z_r}, \dots, \frac{z_0 - z_1}{z_r}\Big). \tag{2.11}$$

Proof: Consider the set

$$\{(\boldsymbol{x}, A) : A \in \mathcal{I}(P), \text{shape}(A) = e, \boldsymbol{x} \in \mathcal{C}^A, \text{shape}(\boldsymbol{x}) \leq e\}$$

where A is an ideal. We have the following chain of equalities

$$\begin{aligned}
\sum_{f \leq e} \mathcal{A}_f N(f, e) &= \sum_{\text{shape}(A)=e} |\mathcal{C}^A| \\
&= \sum_{\text{shape}(A)=e} q^{|A| - \text{rank}(\mathbf{H}(A))} \\
&= \sum_{\text{shape}(A^c)=\bar{e}} q^{k - \text{rank}(\mathbf{G}(A^c))} \\
&= q^k \sum_{\text{shape}(A^c)=\bar{e}} q^{-\text{rank}(\mathbf{G}(A^c))} \\
&= q^k \sum_{u=0}^{k} q^{-u} R_{\bar{e}}^u.
\end{aligned}$$

The second and the third equalities follow from Lemma 2.1 and equation (2.9), respectively. The last equality can be obtained from the definition of the rank coefficient R_e^v. Next, we invoke Lemma 2.2 to conclude the proof as follows:

$$\begin{aligned}
A(z_0, z_1, \ldots, z_r) &= \sum_e \sum_{f \leq e} \mathcal{A}_f N(f, e)(z_0 - z_1)^{e_0} \ldots (z_{r-1} - z_r)^{e_{r-1}} {z_r}^{e_r} \\
&= \sum_e \sum_{u=0}^{k} q^{k-u} R_{\bar{e}}^u (z_0 - z_1)^{e_0} \ldots (z_{r-1} - z_r)^{e_{r-1}} {z_r}^{e_r} \\
&= \sum_{\bar{e}} \sum_{u=0}^{k} q^{k-u} R_{\bar{e}}^u (z_0 - z_1)^{\bar{e}_r} \ldots (z_{r-1} - z_r)^{\bar{e}_1} {z_r}^{\bar{e}_0} \\
&= \sum_{\bar{e}} \sum_{u=0}^{k} q^{k-u} R_{\bar{e}}^u \left(\frac{z_{r-1} - z_r}{z_r}\right)^{\bar{e}_1} \ldots \left(\frac{z_0 - z_1}{z_r}\right)^{\bar{e}_r} {z_r}^n \\
&= q^k {z_r}^n \sum_{\bar{e}} \sum_{u=0}^{k} R_{\bar{e}}^u \left(\frac{z_{r-1} - z_r}{z_r}\right)^{\bar{e}_1} \ldots \left(\frac{z_0 - z_1}{z_r}\right)^{\bar{e}_r} \left(\frac{1}{q}\right)^u \\
&= q^k {z_r}^n Z\left(q, \frac{z_{r-1} - z_r}{z_r}, \ldots, \frac{z_0 - z_1}{z_r}\right).
\end{aligned}$$

■

This theorem enables one to obtain a simple proof of the MacWilliams theorem for linear ordered codes previously proved in [42] (see also [11, 7]).

Theorem 2.2 *Let $\mathcal{C} \subset P$ and $\mathcal{C}^\perp \subset P^\perp$ be dual linear codes. Then*

$$A^\perp(u_0, u_1, \ldots, u_r) = \frac{1}{|\mathcal{C}|} A(z_0, z_1, \ldots, z_r)$$

where

$$z_0 = u_0 + (q-1)\sum_{i=1}^{r} q^{i-1}u_i,$$
$$z_{r-j+1} = u_0 + (q-1)\sum_{i=1}^{j-1} q^{i-1}u_k - q^{j-1}u_j, \qquad 1 \le j \le r.$$

Proof : From Theorem 2.1 and Proposition 2.1, we obtain the following series of equalities:

$$\begin{aligned}
&A^{\perp}(u_0, u_1, \ldots, u_r) \\
&= q^{nr-k} u_r^n Z^{\perp}\Big(q; \frac{u_{r-1}-u_r}{u_r}, \ldots, \frac{u_{r-j}-u_{r-j+1}}{u_r}, \ldots, \frac{u_0-u_1}{u_r}\Big) \\
&= (u_0-u_1)^n Z\Big(q; \frac{u_1-u_2}{u_0-u_1}q, \ldots, \frac{u_j-u_{j+1}}{u_0-u_1}q^j, \ldots, \frac{u_{r-1}-u_r}{u_0-u_1}q^{r-1}, \frac{u_r}{u_0-u_1}q^r\Big) \\
&= \frac{1}{|\mathcal{C}|}A(z_0, z_1, \ldots, z_r).
\end{aligned}$$

Comparing this relation with (2.11), we find the following relations for the variables $z_1, \ldots, z_r$:

$$\begin{aligned}
z_r &= u_0 - u_1 \\
z_{r-j} &= z_{r-j+1} + (u_j - u_{j+1})q^j, \quad j = 1, 2, \ldots, r-1; \\
z_0 &= z_1 + u_r q^r.
\end{aligned}$$

Solving for the z-variables results in the claimed expression. ■

This proof is a counterpart of the linear-algebraic proof of the MacWilliams identities for the usual Hamming space given in [40]. Previous proofs in [11] emphasized the character-theoretic approach.

The Tutte polynomial for a code in the Hamming metric is usually defined for a different set of variables [68] in order to express the duality relation in a simpler form. We can do the same for an ordered code. Let

$$T(x, \boldsymbol{y}) \triangleq \sum_{e} \sum_{\substack{S \in \mathcal{I}(P) \\ \mathrm{shape}(S)=e}} (x-1)^{\rho E - \rho S}(y_1-1)^{e_1} \ldots (y_{r-1}-1)^{e_{r-1}}(y_r-1)^{|S|-\rho S}.$$

To move between Z and T we perform the following change of variables:

$$q = (x-1)(y_r-1), \tag{2.12}$$
$$z_i = (y_i-1)(y_r-1)^i, \ \ 1 \le i \le r-1, \tag{2.13}$$
$$z_r = (y_r-1)^r. \tag{2.14}$$

Then one can check that

$$T(x, \boldsymbol{y}) = (x-1)^{\rho E} Z(q, \boldsymbol{z}).$$

The duality relation (2.8) becomes

Lemma 2.3

$$T^{\perp}(x, y_1, \ldots, y_r) = T(y_r, y_{r-1}, \ldots, y_1, x).$$

Proof: Again it suffices to prove the relations for any one term of the polynomials. Write $\tilde{x} = x - 1, \tilde{y}_i = y_i - 1$. Let us multiply both sides of (2.10) by $\tilde{x}^{\rho^\perp E}$ and perform the change of variables (2.12)-(2.14). We obtain

$$\begin{aligned}
&\tilde{x}^{\rho^\perp E - \rho^\perp \bar{A}} \tilde{y}_r^{|\bar{A}| - \rho^\perp \bar{A}} \prod_{i=1}^{r-1} \tilde{y}_i^{\bar{e}_i} \\
&= \tilde{x}^{\rho^\perp E + \rho E - nr + |A^c| - \rho A^c} \Big(\prod_{i=1}^{r-1} \tilde{y}_{r-i}^{e^i} \Big) \tilde{y}_r^{(\rho E - nr - \rho A^c + |A^c|) + r(n - e_r) - \sum_{i=1}^{r-1} i e_i} \\
&= \tilde{x}^{|A|^c - \rho A^c} \tilde{y}_r^{\rho E - \rho A^c} \prod_{i=1}^{r-1} \tilde{y}_{r-i}^{e^i}.
\end{aligned}$$

Now sum on all $\bar{A} \in \mathcal{I}(P^\perp)$ and observe that on the right the sum goes over all $A^c \in \mathcal{I}(P)$. This proves the theorem. ■

This lemma offers an interesting extension of the classical result for the two-variable Tutte polynomial of usual matroids. In that case we have

$$T_{\mathcal{M}}(z_0, z_1) = T_{\mathcal{M}^\perp}(z_1, z_0).$$

This relation follows from the above considerations by taking $r = 1$. At the same time, its extension to the ordered case is not entirely predictable.

2.4 Support Weight Distributions

There are numerous ways to generalize the weight distribution of codes [12, 13], with the most inclusive definition suggested recently in [34]. Of these generalizations we isolate the so-called generalized Hamming weights (or support weights) for linear codes. For the Hamming space they were defined by Wei in [67]. The reason for us to study support weight distributions is that they extend the linear-algebraic approach adopted in this chapter. Wei's result has attracted much attention and was generalized in several ways. For example, Kløve [36] and Simonis [61] generalized the MacWilliams identity for support weights. Barg [6] and Britz [12] sought the connection between support weight distributions of linear codes and the Tutte polynomial of matroids by generalizing Greene's work [29]. Higher weight distributions for the poset case were recently introduced in [8]. In this section we relate higher poset weight distributions to the multivariate Tutte polynomial of the ordered code.

We remark that paper [67] introduced generalized Hamming weights with no link to the invariants of linear codes: rather, it was motivated by an application of linear codes in a particular combinatorial model of the "wire-tap channel" (the so-called wire-tap channel of type II). Following this lead, we will extend this application to the ordered case. It will require us to define suitable models of communications channels, which is the subject of the next chapter.

Let $\mathcal{C} \subset \mathbb{F}_q^{nr}$ be a linear ordered code, and let

$$A^j(I) = |\{D : D \subseteq \mathcal{C}, \dim(D) = j, \langle \mathrm{supp}(D) \rangle = I\}|$$

where $\mathrm{supp}(D) = \cup_{\boldsymbol{x} \in D} \mathrm{supp}(\boldsymbol{x})$ and $I \in \mathcal{I}(P)$ is an ideal.

Define

$$A_e^j = \sum_{I : \mathrm{shape}(I) = e} A^j(I).$$

The collection of A_e^j for all possible shapes e is called the *jth support shape distribution* of $\mathcal{C}$.

Let us introduce the following notation:

$$[m]_u = \prod_{i=0}^{u-1}(q^m - q^i),\ [m]_0 := 1; \quad \begin{bmatrix} t \\ u \end{bmatrix} = \frac{[t]_u}{[u]_u}$$

$$D^m(I) = \sum_{u=0}^{m} [m]_u A^u(I),\ \ m \geq 0$$

$$D_e^m = \sum_{I:\mathrm{shape}(I)=e} D^m(I)$$

$$D^m(z_0, z_1, \ldots, z_r) = \sum_e D_e^m z_0^{e_0} \ldots z_r^{e_r},\ \ m \geq 0.$$

These definitions as well as the next result extend the case of the Hamming space [6].

Theorem 2.3

$$D^m(z_0, z_1, \ldots, z_r) = q^{mk} {z_r}^n Z\left(q^m, \frac{z_{r-1} - z_r}{z_r}, \frac{z_{r-2} - z_{r-1}}{z_r}, \ldots, \frac{z_0 - z_1}{z_r}\right).$$

Proof: Repeating the argument in the proof of lemma 2.2, we obtain the equalities

$$\begin{aligned} &D^m(z_0, z_1, \ldots, z_r) \\ &= \sum_e D_e^m z_0^{e_0} \ldots z_r^{e_r} \\ &= \sum_e \sum_{f \leq e} D_f^m N(f, e)(z_0 - z_1)^{e_0}(z_1 - z_2)^{e_1} \ldots (z_{r-1} - z_r)^{e_{r-1}} {z_r}^{e_r}. \end{aligned}$$

Extending the ideas in [61], let us introduce the quantities

$$N_e^m = |\{X : X \subseteq E, X \text{ an ideal }, \mathrm{shape}(X) = e, \dim \mathcal{C}^X = m\}|$$

and $A^j = \{D : D \subseteq \mathcal{C}, \dim D = j\}$ which is the set of j-dimensional subcodes of $\mathcal{C}$. Consider the set

$$\{(D, X) : D \in A^j, X \text{ a left-adjusted } e\text{-subset of } S, \langle \mathrm{supp}\, D \rangle \subseteq X\}$$

Counting the cardinality of this set in two ways, we obtain the equality

$$\sum_{f \leq e} A_f^j N(f, e) = \sum_{m=j}^{k} \begin{bmatrix} m \\ j \end{bmatrix} N_e^m.$$

This enables us to obtain the following relation between the quantities D_f^m and R_e^v:

$$\begin{aligned}\sum_{f\leq e} D_f^m N(f,e) &= \sum_{f\leq e}\sum_{u=0}^{m}[m]_u A_f^u N(f,e) = \sum_{u=0}^{m}[m]_u \sum_{f\leq e} N(f,e)A_f^u \\ &= \sum_{u=0}^{m}[m]_u \sum_{t=u}^{k}\begin{bmatrix} t \\ u \end{bmatrix} R_{\bar{e}}^{k-t} = \sum_{u=0}^{m}\sum_{t=0}^{k}[m]_u \begin{bmatrix} t \\ u \end{bmatrix} R_{\bar{e}}^{k-t} \\ &= \sum_{u=0}^{m}\sum_{j=0}^{k}[m]_u \begin{bmatrix} k-j \\ u \end{bmatrix} R_{\bar{e}}^{j} = \sum_{j=0}^{k}\sum_{u=0}^{m}[m]_u \begin{bmatrix} k-j \\ u \end{bmatrix} R_{\bar{e}}^{j} \\ &= \sum_{j=0}^{k} q^{m(k-j)} R_{\bar{e}}^{j}.\end{aligned}$$

Comparing the definitions of N_e^m and R_e^v, we obtain $N_e^m = R_{\bar{e}}^{k-m}$. Therefore,

$$\begin{aligned}D^m(z_0, z_1, \ldots, z_r) &= \sum_{e}\sum_{j=0}^{k} q^{m(k-j)} R_{\bar{e}}^{j} (z_0 - z_1)^{e_0} \ldots (z_{r-1} - z_r)^{e_{r-1}} {z_r}^{e_r} \\ &= \sum_{\bar{e}}\sum_{j=0}^{k} q^{m(k-j)} R_{\bar{e}}^{j} (\frac{z_0 - z_1}{z_r})^{\bar{e_r}} \ldots (\frac{z_{r-1} - z_r}{z_r})^{\bar{e_1}} {z_r}^{n} \\ &= q^{mk} {z_r}^{n} Z(q^m, \frac{z_{r-1} - z_r}{z_r}, \ldots, \frac{z_0 - z_1}{z_r})\end{aligned}$$

which completes the proof. ■

The MacWilliams relations for the support weight enumerators of $\mathcal{C}$ in the ordered Hamming space take the following form.

Theorem 2.4 *Let $\mathcal{C} \subset P$ and $\mathcal{C}^\perp \subset P^\perp$ be dual linear codes. Then*

$$(D^m)^\perp(u_0, u_1, \ldots, u_r) = \frac{1}{|\mathcal{C}|^m} D^m(z_0, z_1, \ldots, z_r)$$

where

$$\begin{aligned} z_0 &= u_0 + (q^m - 1)\sum_{i=1}^{r} q^{(i-1)m} u_i, \\ z_{r-j+1} &= u_0 + (q^m - 1)\sum_{i=1}^{j-1} q^{(i-1)m} u_k - q^{(j-1)m} u_j, \qquad 1 \leq j \leq r. \end{aligned}$$

The proof of this theorem is a simple extension of the proof of Theorem 2.2 which will be omitted.

To conclude this section, we present an application of the above concepts to a particular family of linear ordered codes. In Example 2.1 we considered a family of ordered RS codes. In the classical case, the RS codes meet the Singleton bound that relates the length, dimension, and distance of a linear code, and therefore are called MDS codes. The same applies in the ordered case (see [57]): an ordered $[N = nr, k, d]$ linear code is called MDS if $d = N - k + 1$. Below we compute the support weight distributions of ordered MDS codes.

Let us start with the following straightforward lemma.

Lemma 2.4 *Let $F_l = \{U : U$ a subspace of $\mathbb{F}_q^k$ of dimension $l\}$. Let B be a j-dimensional subcode of a linear code $\mathcal{C}$ of dimension k. For $j = 0, \ldots, k$, $B \mapsto U_B$ is a bijection between the set of j-dimensional subspaces of $\mathcal{C}$ and the set F_{k-j} where $U_B \in F_{k-j}$.*

First we prove a result that extends a lemma due to Helleseth et al. [31] to the ordered case on support weight distributions of codes in the Hamming metric space.

Proposition 2.2 *Let $\mathcal{C} \subset P$ be an $[nr, k]$ linear ordered code. Let i_0 be the largest integer such that any i_0 right-adjusted column vectors from the generator matrix of $\mathcal{C}$ are linearly independent. If $k - j < i_0$, then*

$$A_e^j = \binom{n}{e} \sum_{h=0}^{k-j-nr+i} (-1)^h \binom{i}{h} \begin{bmatrix} k-nr+i-h \\ j \end{bmatrix}$$

where e is a shape vector with $i = |e|'$.

Proof: Let S be a set of column vectors of a generator matrix of $\mathcal{C}$, $S_1 \subseteq S$ be a right-adjusted subset with $|S_1| = i$, and $i \leq j < i_0$. And let us define $K_j(S_1)$ and $M_j(S_1)$ as follows:

$$\begin{aligned} K_j(S_1) =& |\{U : U \subset \mathbb{F}_{q^k}, U \text{ is a vector space}, \dim U = j, U \cap S = S_1\}|. \\ M_j(S_1) =& |\{U : U \subset \mathbb{F}_{q^k}, U \text{ is a vector space}, \dim U = j, U \supset S_1\}|. \end{aligned}$$

We have

$$\sum_{S_1 \subset S_2 \subset S} K_j(S_2) = M_j(S_1). \tag{2.15}$$

Here the set S_2 does not have to be right-adjusted.

The quantity $M_j(S_1)$ is the number of j-dimensional subspaces of $\mathbb{F}_{q^k}$ containing the i-dimensional subspace which is spanned by the set S_1. Therefore,

$$M_j(S_1) = \begin{bmatrix} k-i \\ j-i \end{bmatrix}$$

For $j < i_0$ the quantity $K_j(S_1)$ depends only on i for the following reason. First, when $j - i = 0$, we have $K_j(S_1) = 1$. Arguing by induction, assume that $K_j(S_1)$ does not depend on S_1 for $j - i < t$. If $j - i = t$, Equation (2.15) becomes

$$K_j(S_1) + \sum_{S_1 \subsetneq S_2 \subset S} K_j(S_2) = \begin{bmatrix} k-i \\ j-i \end{bmatrix}.$$

Since the size of S_2 is greater than i by the induction hypotheses, all the terms of the summation do not depend on S_2 and thus $K_j(S_1)$ does not depend on S_1. Let us put $K_j(S_1) = K_{i,j}$. By a result in [31]

$$K_{i,j} = \sum_{h=0}^{j-i} (-1)^h \binom{nr-i}{h} \begin{bmatrix} k-i-h \\ k-j \end{bmatrix}.$$

By the definitions of $K_{i,j}$ and A_e^j and Lemma 2.4, we have that

$$\begin{aligned} A_e^j &= \binom{n}{e} A_I^j \\ &= \binom{n}{e} K_{nr-i,k-j} \\ &= \binom{n}{e} \sum_{h=0}^{k-j-nr+i} (-1)^h \binom{i}{h} \begin{bmatrix} k-nr+i-h \\ j \end{bmatrix}, \end{aligned}$$

which completes the proof. ■

Finally, consider the case of ordered MDS codes. If $\mathcal{C}$ is MDS, then the largest number i_0 introduced in the proof of Proposition 2.2 equals k. Therefore, Proposition 2.2 gives the complete jth support shape distribution of $\mathcal{C}$ for $0 < j < k$. The cases $j = 0, j = k$ are trivial since the only subcodes in these cases are the zero-dimensional space and the entire code, respectively.

Appendix: Linear Ordered MDS codes and Poset Matroids

In conclusion, let us discuss one possibility of defining matroids on posets. While there is a number of ways to generalize matroids from sets to posets [70], the idea that we find useful is to replace subsets in the usual definition by ideals. This idea underlies the following definition due to M. Barnabei et al. [10]

Let P be a poset. A filter in P is a complement of an ideal in the same poset. We write $A \subset P$ to refer to a subset of E considered with the order inherited from P. The *poset matroid* $\mathcal{M}$ on P is a family $\mathfrak{B}$ of filters in P, called bases, satisfying the following axioms:

1. $\mathfrak{B} \neq \emptyset$.
2. For every $B_1, B_2 \in \mathfrak{B}; B_1 \not\subset B_2$.
3. For every $B_1, B_2 \in \mathfrak{B}$ and for every pair of filters X, Y of E such that $X \subseteq B_1, B_2 \subseteq Y, X \subseteq Y$, there exists $B \in \mathfrak{B}$ such that $X \subseteq B \subseteq Y$.

As proved in [10], all the bases of $\mathcal{M}$ have the same size.

Similarly to usual matroids, it is possible to define a poset matroid via its independent sets. The family $\mathfrak{F}$ of all independent sets of a poset matroid $\mathcal{M}$ on the partially ordered set P satisfies the following properties:

1. $\mathfrak{F} \neq \emptyset$.
2. If X, Y are filters in P such that $Y \in \mathfrak{F}$ and $X \subseteq Y$, then $X \in \mathfrak{F}$.
3. For every $X, Y \in \mathfrak{F}$ with $|X| < |Y|$, there exists $y \in \mathrm{Max}(Y - X)$ such that $X \cup y \in \mathfrak{F}$

where $\mathrm{Max}(A) = \{x \in A, x \text{ is maximal in } A\}$.

A poset matroid $\mathcal{M}$ is called *k-uniform* if every filter of size k is a base. To describe the relation between MDS codes and poset matroids, let us begin with the following straightforward proposition.

Proposition 2.3 *Let $\mathcal{P} = (E, P)$ be a poset metric space. A linear $[N, k]$ poset code $\mathcal{C}$ is MDS if and only if any submatrix $\mathbf{H}(I)$ has full rank, where $\mathbf{H}$ is the parity-check matrix of $\mathcal{C}$ and $I \in \mathcal{I}(P)$ is an ideal. If $\mathcal{C}$ is MDS in P, then the dual code $\mathcal{C}^\perp$ of $\mathcal{C}$ is MDS in $P^\perp$.*

Observe that a linear ordered MDS code of dimension k represents a k-uniform poset matroid on its set of coordinates. Indeed, let $\mathbf{G}$ be a generator matrix of $\mathcal{C}$. Since $\mathcal{C}^\perp$ is MDS with respect to the dual order $P^\perp$, every submatrix $\mathbf{G}(I), I \in \mathcal{I}(P^\perp)$ has full rank (i.e., has rank $\min(|I|, k)$). This means that every filter $F \in P$ of size k forms an independent subset with respect to the rank function $\rho(\mathbf{G}(\cdot))$, and that k is the maximum size of an independent subset. By the definition of the poset matroid above, the set of all filters (ideals $I \in \mathcal{I}(P^\perp), |I| = k$) forms the set of bases of a matroid $\mathcal{M}$ which is also uniform. Thus, the ordered RS codes of Example 2.1 represent uniform ordered matroids.

At the same time, the link between general linear poset codes and the poset matroids defined above is not as straightforward. Namely, let $\mathcal{C}$ and $\mathcal{C}^\perp$ be a pair of linear poset codes with respect to a poset $\mathcal{P} = (E, P)$. Suppose that the distance of the code $\mathcal{C}^\perp$ is d. Then every submatrix $G(I), I \in \mathcal{I}(P^\perp), |I| \leq d - 1$ has full rank, so every such subset will be independent. At the same time, some submatrices that correspond to larger-size ideals will also have full rank, so it is not possible to claim that the code represents a poset matroid based only on the cardinality of ideals.

Chapter 3
Ordered Discrete Memoryless Channels

In the previous chapter we studied combinatorial properties of codes in metric spaces with distance defined by a partial order on the coordinates. Poset metrics are motivated in part by transmission over parallel channels in which the noise levels are coordinated in the sense that if in a given time slot, a link is exposed to high noise, then all the lower-numbered links also experience high levels of noise. In this chapter we define and study simple probabilistic models of DMCs that model this definition in information-theoretic terms. Specifically, we introduce "ordered DMCs" which provide a probabilistic counterpart to the combinatorial constructions of the previous chapter. These models will also yield simple examples for the construction of nonbinary polar codes in the next chapter.

3.1 Introduction

Let $W : \mathcal{X} \to \mathcal{Y}$ be a DMC with input alphabet $\mathcal{X}$ and the output alphabet $\mathcal{Y}$, i.e., a stochastic map that associates a probability distribution on $\mathcal{Y}$ to every element of $\mathcal{X}$. We assume that both $\mathcal{X}$ and $\mathcal{Y}$ are finite sets and write $W(y|x) = P(Y = y|X = x)$, where X and Y are the random input and output symbols of the channel. Let $\boldsymbol{x} = x_1^n = (x_1, \ldots, x_n) \in \mathcal{X}^n$ be an input vector of length n and $\boldsymbol{y} = y_1^n = (y_1, \ldots, y_n) \in \mathcal{Y}^n$ be an output vector. The channel is described by memoryless if

$$W^n(y_1^n|x_1^n) = \prod_{i=1}^{n} W(y_i|x_i).$$

For a DMC W, the *capacity* $\mathscr{C}$ is given by

$$\mathscr{C} = \max_{P_X(x)} I(X;Y).$$

where $I(X;Y)$ is mutual information between X and Y and the maximum is taken over all possible one-dimensional distributions on $\mathcal{X}$.

The Hamming metric on strings over a q-ary alphabet is motivated in part by the model of the q-ary symmetric channel. Define the q-ary symmetric channel $W : \mathcal{X} \to \mathcal{Y}$, $\mathcal{X} = \mathcal{Y} = \{0, 1, \ldots, q-1\}$ by

$$W(y|x) = \begin{cases} 1-p, & \text{if } x = y \\ \frac{p}{q-1}, & \text{if } x \neq y \end{cases}$$

The capacity of this channel is $1 - h_q(p)$ where $h_q(p) = -(1-p)\log_q(1-p) - p\log_q \frac{p}{q-1}$ is the "q-ary entropy function."

Another popular related model is the q-ary erasure channel $W : \mathcal{X} \to \mathcal{Y}$, $\mathcal{X} = \{0, 1, \ldots, q-1\}$, $\mathcal{Y} = \{0, 1, \ldots, q-1\} \cup \{?\}$ where ? is the erasure symbol, and the transitions are given by

$$W(y|x) = \begin{cases} 1-\varepsilon, & \text{if } x = y \\ \varepsilon, & \text{if } y = ? \\ 0, & \text{otherwise.} \end{cases}$$

In this case capacity $\mathscr{C}(W) = 1 - \varepsilon$.

In both cases, capacity can be attained by performing *maximum likelihood decoding* of the received sequence $\boldsymbol{y}$, under which the decoding result is given by the input sequence $\boldsymbol{x} \in \{0,1\}^n$ that maximizes the probability $W^n(\boldsymbol{y}|\boldsymbol{x}')$ over all the possible code sequences $\boldsymbol{x}'$. Equivalently, we need to find a codeword $\boldsymbol{x}$ that is the closest to $\boldsymbol{y}$ by the Hamming distance. This covers both the channel models defined above, where for the case of the erasure channel we simply look for the codeword that equals $\boldsymbol{y}$ on all the nonerased positions. The goal of this chapter is to define and study similar channel models for the case of the NRT (ordered) metric. We define the ordered symmetric channel (OSC) and the ordered erasure channel (OEC) and study properties of linear codes when used for communication over them.

3.2 Ordered Symmetric Channel

Suppose that one use of the channel corresponds to transmission of a vector $x \in \mathbb{F}_q^r$ over r parallel links. Let $\varepsilon = (\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_r)$, where $0 \le \varepsilon_i \le 1$ for all i and $\sum_{i=0}^r \varepsilon_i = 1$. Let $W_r : \mathbb{F}_q^r \to \mathbb{F}_q^r$ be a memoryless vector channel defined by

$$W_r(y|x) = \frac{\varepsilon_i}{q^{i-1}(q-1)}, \quad \text{where } d_P(x,y) = i, 1 \le i \le r,$$

and $W_r(y|x) = \varepsilon_0$ if $y = x$. Every row of the matrix of transition probabilities $W_r(y|x)$ contains one instance of ε_0 and $q^{i-1}(q-1)$ entries of the form $\frac{\varepsilon_i}{q^{i-1}(q-1)}$ for all $i = 1, \ldots, r$, and the same is true for every column. Therefore, the channel W_r is symmetric in the sense of [27]. We call $W_r = W_r(\varepsilon)$ the q-ary OSC. This is also a channel with additive noise, so we can think of the noise in terms of error vectors. If in a given error vector, the jth symbol in a particular chain is nonzero, the values of the symbols with indices $1, \ldots, j-1$ in the same chain are of no importance, thereby justifying the term *ordered*. The channel can be also thought of as a set of dependent parallel symmetric channels because the conditional probability of error in symbol $x_j, 1 \le j \le r-1$ depends on the values of errors in higher-numbered symbols within the same block of r symbols.

Below we assume that

$$\varepsilon_0 > \frac{\varepsilon_1}{q-1} > \cdots > \frac{\varepsilon_r}{q^{r-1}(q-1)}. \tag{3.1}$$

This assumption accounts for the fact that correct transmission has higher probability than an error, and that the transition probability $W_r(y|x)$ is monotone decreasing with the distance $d_P(x,y)$.

To underscore the analogy with the scalar q-ary symmetric channel, we let $a, b \in \mathbb{F}_q$ with $a \ne b$ and compute the probabilities

$$\sum_{\substack{y \in \mathbb{F}_q^r \\ d_P(x,y)=j, y_j=b}} W_r(y|x) = \Pr[y_j = b, y_{j+1} = x_{j+1}, \ldots, y_r = x_r | x_j = a] = \frac{\varepsilon_j}{q-1},$$

$$(j = 1, 2, \ldots, r).$$

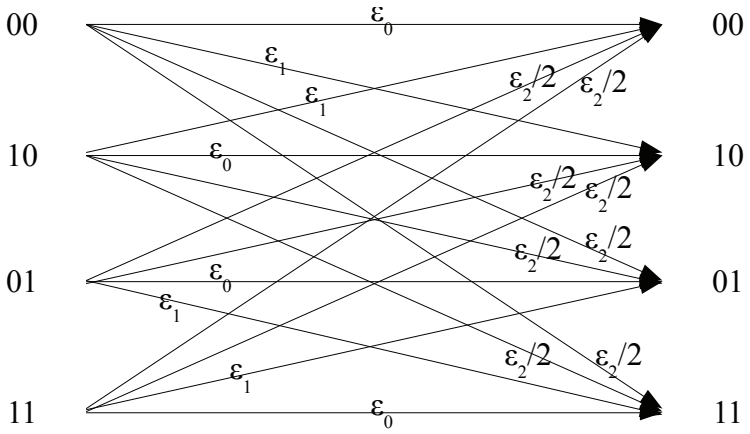

Figure 3.1: Ordered symmetric channel with $q = 2$ and $r = 2$.

The shape distribution of a linear code (but not the weight distribution) characterizes the performance of the code on the channel considered. To illustrate this point, let us assume that $\mathrm{shape}(y) = e$ and compute the transition probability from 0 to y :

$$\begin{aligned} W_r(y|0) &= \varepsilon_0^{e_0} \left(\frac{\varepsilon_1}{q-1}\right)^{e_1} \cdots \left(\frac{\varepsilon_r}{q^{r-1}(q-1)}\right)^{e_r} \\ &= \varepsilon^e \left(\frac{q-1}{q}\right)^{-|e|} q^{-|e|'} \\ &= \frac{\varepsilon_0^{e_0}}{q^{\mathrm{wt}_P(y)}} \prod_{i=1}^{r} \left(\frac{q\varepsilon_i}{q-1}\right)^{e_i}. \end{aligned}$$

The above equation shows that the shape of the error vector determines the transition probability (note that the ordered weight is insufficient for that purpose). The shape distribution can also be used to compare the transition probabilities of two vectors in some cases as we can see in the following lemma.

Lemma 3.1 *Let W_r be an OSC with crossover shape ε that satisfies conditions* (3.1)*. Let $y, z \in \mathbb{F}_q^r$ where $\mathrm{shape}(y) = e$ and $\mathrm{shape}(z) = f$ with $f \leq e$ (cf.* (2.5)*). Then, $W_r(y|0) \leq W_r(z|0)$ with equality if (but not only if) $f = e$.*

Proof: The probability of transitioning from 0 to y is

$$
\begin{aligned}
&W_r(y|0)\\
&= \varepsilon_0^{e_0}\left(\frac{\varepsilon_1}{q-1}\right)^{e_1}\cdots\left(\frac{\varepsilon_r}{q^{r-1}(q-1)}\right)^{e_r}\\
&= \varepsilon_0^{e_0}\left(\frac{\varepsilon_1}{q-1}\right)^{e_1}\cdots\left(\frac{\varepsilon_{r-1}}{q^{r-2}(q-1)}\right)^{e_{r-1}}\left(\frac{\varepsilon_r}{q^{r-1}(q-1)}\right)^{e_r-f_r}\left(\frac{\varepsilon_r}{q^{r-1}(q-1)}\right)^{f_r}\\
&\le \varepsilon_0^{e_0}\left(\frac{\varepsilon_1}{q-1}\right)^{e_1}\cdots\left(\frac{\varepsilon_{r-1}}{q^{r-2}(q-1)}\right)^{e_{r-1}+e_r-f_r}\left(\frac{\varepsilon_r}{q^{r-1}(q-1)}\right)^{f_r}\\
&= \varepsilon_0^{e_0}\left(\frac{\varepsilon_1}{q-1}\right)^{e_1}\cdots\left(\frac{\varepsilon_{r-1}}{q^{r-2}(q-1)}\right)^{e_{r-1}+e_r-f_{r-1}-f_r}\left(\frac{\varepsilon_{r-1}}{q^{r-2}(q-1)}\right)^{f_{r-1}}\left(\frac{\varepsilon_r}{q^{r-1}(q-1)}\right)^{f_r}\\
&\le \cdots \le \varepsilon_0^{f_0}\left(\frac{\varepsilon_1}{q-1}\right)^{f_1}\cdots\left(\frac{\varepsilon_r}{q^{r-1}(q-1)}\right)^{f_r}\\
&= W_r(z|0)
\end{aligned}
$$

where the inequalities follow from condition (3.1) and the assumption $f \le e$. All the equalities hold when $\left(\sum_{i=j}^r e_i\right) - \left(\sum_{i=j}^r f_i\right) = 0$ for all $j = 1, \ldots, r$ and thus if $f = e$, then $W(y|0) = W(z|0)$. This completes the proof. ■

Proposition 3.1 *The capacity of $W_r(\varepsilon)$ equals*

$$\mathscr{C}(W_r(\varepsilon)) = r(1 - h_{q,r}(\varepsilon)), \tag{3.2}$$

where

$$h_{q,r}(\varepsilon) \triangleq \frac{1}{r}\Big(H_q(\varepsilon) + \sum_{i=1}^r \varepsilon_i \log_q(q^{i-1}(q-1))\Big)$$

and $H_q(\varepsilon) = -\sum_{i=0}^r \varepsilon_i \log_q \varepsilon_i$.

Proof: This is shown by a straightforward calculation:

$$\mathscr{C}(W_r(\varepsilon)) = \max_{P_X} I(X;Y) = \max_{P_X}(H(Y) - H(Y|X)),$$

where P_X is a distribution on $\mathbb{F}_q^r$. Since the channel is symmetric, the maximum is attained on uniform P_X, so X is uniformly distributed on $\mathbb{F}_q^r$, and therefore, Y is also uniform. Thus, $H(Y)$ above equals r. Furthermore,

$$
\begin{aligned}
H(Y|X) &= \sum_{x,y} P_{XY}(x,y) \log_q \frac{1}{P_{Y|X}(y|x)}\\
&= -\varepsilon_0 \log_q \varepsilon_0 - \sum_{i=1}^r \varepsilon_i \log_q \frac{\varepsilon_i}{q^{i-1}(q-1)}\\
&= H_q(\varepsilon) + \sum_{i=1}^r \varepsilon_i \log_q(q^{i-1}(q-1)).
\end{aligned}
$$

This gives (3.2). ■

Note that for $r = 1$, $h_{q,r}(\varepsilon)$ becomes $-\varepsilon_1 \log_q \frac{\varepsilon_1}{q-1} - (1-\varepsilon_1)\log_q(1-\varepsilon_1)$, and we recover the capacity formula of the usual q-ary symmetric channel.

Random linear ordered codes. Consider a partition of $\mathbb{F}_q^{nr} \times \mathbb{F}_q^{nr}$ into disjoint subsets R_e such that (x, y) belong to one subset if and only if $\mathrm{shape}(x - y) = e$. To each subset R_e we associate a complete regular graph $\mathcal{R}_e$ on $|R_e|$ vertices. The degree of the graph $\mathcal{R}_e$ equals the number of neighbors of a given point x that satisfy $\mathrm{shape}(x - y) = e$. This number does not depend on x and equals

$$v_e = \binom{n}{e} \Big(\frac{q-1}{q}\Big)^{\sum_{i=1}^r e_i} q^{\sum_{i=1}^r i e_i}$$

where $\binom{n}{e}$ is the number of ways to choose r subsets of size $e_1, \dots, e_r$ out of an n-set (see also [8] which developed the graph approach to the ordered Hamming space). Using the Stirling approximation, we compute

$$v_e \cong q^{n(H_q(\varepsilon) + \sum_{i=1}^r \varepsilon_i \log_q(q^{i-1}(q-1)))} = q^{nr h_{q,r}(\varepsilon)},$$

where $H_q(\varepsilon)$ is the entropy of the vector $(\varepsilon_0, \varepsilon_1, \dots, \varepsilon_r)$. We observe that $h_{q,r}(\varepsilon)$ gauges the exponential growth of the number of vectors of shape $e = (\varepsilon_1 n, \dots, \varepsilon_r n)$ in the space $\mathbb{F}_q^{nr}$. As in the classical case, this estimate is exponentially tight.

Lemma 3.2 *Consider the ensemble of linear codes defined by random uniform $(nr(1-R) \times nr)$ parity-check matrices. Let $\mathcal{A}_e$ be the number of vectors with shape $e \neq 0$ in a linear code $\mathcal{C}$ from the ensemble. We have*

$$\begin{aligned} E\mathcal{A}_e &= v_e \cdot q^{k-nr} \cong q^{-nr(1-R-h_{q,r}(\varepsilon))} \\ \mathrm{Var}(\mathcal{A}_e) &\le (q-1) v_e \cdot q^{k-nr}. \end{aligned}$$

The function $h_{q,r}(\varepsilon)$ has a maximum value of 1 when ε has the following form:

$$\varepsilon_0 = q^{-r}, \;\; \varepsilon_i = q^{i-r-1}(q-1), \;\; 1 \le i \le r. \tag{3.3}$$

This set of crossover probabilities ("the crossover shape") accounts for fully random noise and corresponds to $\mathscr{C}(W_r) = 0$. Vectors generated according to the distribution in (3.3) are uniformly distributed in the space $\mathbb{F}_q^{nr}$. The typical set for this distribution is formed of the vectors with shape $n\varepsilon$, where ε is given as in (3.3), and nearby shapes (in terms of the probability).

We also have the following proposition.

Proposition 3.2 *The capacity of the OSC W_r is attained by linear ordered codes.*

This follows from the fact that random linear codes attain capacity of symmetric channels with additive noise; viz. Problem 6.13 in [19]. To show this, linear codes are chosen with uniform probability from the space $\mathbb{F}_q^{nr}$. The uniform choice can be accomplished, for instance, by selecting uniformly random parity-check matrices (the parity-check, or the Elias ensemble) or uniform random generator matrices (the generator-matrix ensemble). The resulting linear codes are formed of uniformly random vectors (except for the zero vector). Almost all vectors in such codes, apart from an exponentially small proportion of them, have relative shape of the form (3.3).

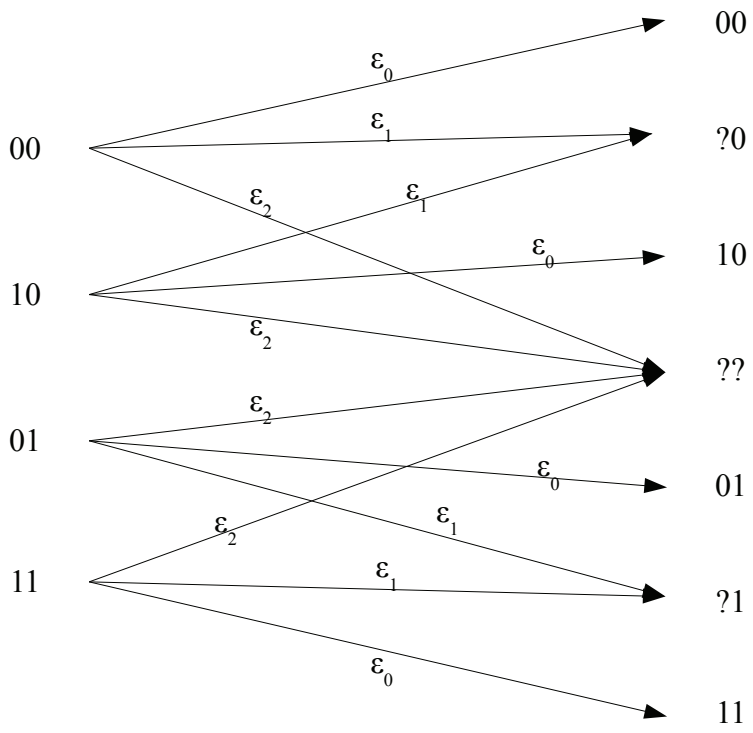

Figure 3.2: Ordered erasure channel with $q = 2$ and $r = 2$.

3.3 Ordered Erasure Channel

Let us consider the channel in which a fraction of the transmitted coordinates in a block can be lost to erasures. Suppose that the transmitter sends a vector $x \in \mathbb{F}_q^r$ over r parallel links. Let $\varepsilon = (\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_r)$, where $0 \leq \varepsilon_i \leq 1$ for all i and $\sum_i \varepsilon_i = 1$. We assume that coordinates are erased according to the NRT partial order: if the ith coordinate is erased, then also all the coordinates $j \prec i$ in the same chain are erased. For example, if $r = 5$ and the third coordinate is the rightmost erased coordinate when an all-zero vector is transmitted, the received vector is $(?, ?, ?, 0, 0)$, where $?$ denotes the erasure symbol. This channel model is consistent with the communication system considered in [66].

Definition 3.1 *The q-ary OEC is a vector memoryless channel, $W_r : \mathbb{F}_q^r \to (\mathbb{F}_q \cup \{?\})^r$ where*

$$W_r(y|x) = \begin{cases} \varepsilon_0, & y = x, \\ \varepsilon_i, & y_1 = \cdots = y_i = ?, y_{i+1} = x_{i+1}, \cdots, y_r = x_r,\ 1 \leq i \leq r, \end{cases} \tag{3.4}$$

and $W_r(y|x) = 0$ if y does not contain any erased coordinates and $y \neq x$.

Similarly to the OSC, this channel can also be thought of as a set of dependent parallel channels. It is symmetric in the sense of [27, p.94].

The capacity of this channel is attained for the uniform inputs, so calculating it is a simple exercise. Call the $(r+1)$-tuple ε the *erasure shape*. We calculate the capacity of the OEC $W_r(\varepsilon)$

as follows:

$$\mathscr{C} = \max_{P_X} I(X;Y) = \max_{P_X}(H(Y) - H(Y|X)) = \max_{P_X} H(Y) - H_q(\varepsilon).$$

By letting $\Pr[x = \boldsymbol{v}] = p_v$ for all $\boldsymbol{v} \in \mathbb{F}_q^r$ where $\boldsymbol{v} = (v_1, v_2, \ldots, v_r)$ and $v = q^{r-1}v_r + q^{r-2}v_{r-1} + \cdots + q^0 v_1$, we have

$$\begin{aligned}
H(Y) = &- \sum_{i=0}^{q^r-1} \varepsilon_0 p_i \log_q \varepsilon_0 p_i - \sum_{i=0}^{q^{r-1}-1} \left(\varepsilon_1 \sum_{j=0}^{q-1} p_{i\cdot q+j}\right) \log_q \left(\varepsilon_1 \sum_{j=0}^{q-1} p_{i\cdot q+j}\right) - \cdots \\
&- \sum_{i=0}^{q-1} \left(\varepsilon_{r-1} \sum_{j=0}^{q^{r-1}-1} p_{i\cdot q^{r-1}+j}\right) \log_q \left(\varepsilon_{r-1} \sum_{j=0}^{q^{r-1}-1} p_{i\cdot q^{r-1}+j}\right) - \varepsilon_r \log_q \varepsilon_r \\
= &-\varepsilon_0 \sum_{i=0}^{q^r-1} p_i \log_q p_i - \varepsilon_1 \sum_{i=0}^{q^{r-1}-1} \left(\sum_{j=0}^{q-1} p_{i\cdot q+j}\right) \log_q \left(\sum_{j=0}^{q-1} p_{i\cdot q+j}\right) - \cdots \\
&- \varepsilon_{r-1} \sum_{i=0}^{q-1} \left(\sum_{j=0}^{q^{r-1}-1} p_{i\cdot q^{r-1}+j}\right) \log_q \left(\sum_{j=0}^{q^{r-1}-1} p_{i\cdot q^{r-1}+j}\right) + H_q(\varepsilon).
\end{aligned}$$

If X is uniformly distributed on $\mathbb{F}_q^r$, every term in $H(Y)$ which is dependent on P_X has a maximum value. Thus, the maximum of $H(Y)$ is attained on uniform P_X. As a result,

$$\begin{aligned}
\mathscr{C} = \max_{P_X} H(Y) - H_q(\varepsilon) &= -\varepsilon_0 \log_q \frac{1}{q^r} - \varepsilon_1 \log_q \frac{1}{q^{r-1}} - \cdots - \varepsilon_{r-1} \log_q \frac{1}{q^1} \\
&= (r\varepsilon_0 + (r-1)\varepsilon_1 + \cdots + \varepsilon_{r-1}) = r - |\varepsilon|'.
\end{aligned}$$

Similarly to the case of the OSC, the capacity of the OEC is attained by linear ordered codes.

3.4 Parallel Wiretap Channels

We consider the wiretap channel model of Wyner [72] in which Alice sends a message M to a legitimate receiver, Bob through a channel called the main channel, while an eavesdropper, Eve, tries to obtain information about this message through another channel called the wiretap channel. The goal of this section is to design a coding scheme under which Alice is able to communicate messages to Bob both reliably and securely.

This model was studied in probabilistic and combinatorial formulations which are termed wiretap channel of type I and type II in accordance with references [72, 50].

3.4.1 Wiretap Channel of Type I

The system model is presented in Fig. 3.3. We restrict our considerations to the case when the eavesdropper's channel is a stochastic degradation of the main communication channel. This setting enables us to obtain closed-form results as opposed to a more general formulation of [18].

Suppose that Alice's messages $S_i, i \geq 1$ are i.i.d. random variables. A vector of k message symbols S^k is encoded into a vector X^N (we use capital letters to indicate that the vectors are random variables on their respective spaces). Let W_1 be the main channel from Alice to Bob and

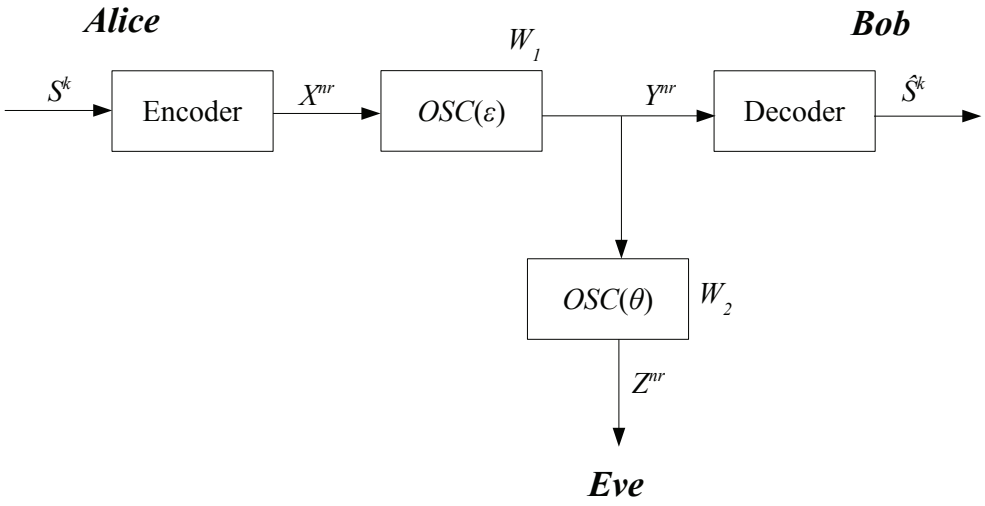

Figure 3.3: Block diagram of parallel wiretap channels over the ordered DMCs

let W_2 be the wiretap channel to Eve. Denote by Y^N and Z^N the random vectors representing the output of W_1 and W_2, respectively.

Reliability is described in terms of Bob's probability of decoding error and is achieved when

$$\lim_{k\to\infty} P_e = 0$$

where

$$P_e = \frac{1}{k}\sum_{i=1}^{k} Pr\{S_i \neq \hat{S}_i\}.$$

The security condition is measured in terms of the normalized mutual information between the message and Eve's observation. Define the equivocation as the conditional entropy $H(S^k|Z^N)$. There are two ways to quantify security: the weak security condition asserts that secrecy is attained when

$$\lim_{k\to\infty} \frac{1}{k} H(S^k|Z^N) = H(S).$$

According to the strong security condition [44], perfect secrecy corresponds to the limiting relation

$$\lim_{k\to\infty} H(S^k|Z^N) = H(S^k).$$

We use these concepts in the formulation of our main results in this section.

Wyner [71] studied two special cases of the wiretap channel of the kind defined above. The first case assumes that the main channel is noiseless and the wiretap channel is a binary symmetric channel. The second one studies the situation when the main channel is any binary DMC, while the wiretap channel is degraded with respect to the main channel. He proved the achievable rate-equivocation region and provided the coding scheme for the first scenario based on the random linear codes that achieves the secrecy capacity of the wiretap channel.

In this section, we extend his result to the ordered case and show that linear ordered codes can be used to achieve reliable communication over parallel channels in the following situation.

Suppose that the communication channel between Alice and Bob as well as Eve's channel are ordered DMCs, and the wiretap channel to Eve is a degraded version of the main channel. This can happen, for instance, when Eve's cost of eavesdropping increases as she attempts to access channels with higher indices in the set of r parallel channels.

We will use the same notation as above with $N = nr$. Suppose that the channel from Alice to Bob is an OSC $W_1 = W_r(\varepsilon)$ with crossover shape $\varepsilon = (\varepsilon_1, \ldots, \varepsilon_r)$, and the wiretap channel $W_2 = W_r(\theta)$ (the channel to Eve) is an OSC with crossover shape θ. We will also examine the case when the OSCs are replaced with OECs, whereby ε and θ will denote the vectors of erasure probabilities. We compute the capacity of the wiretap channels and show that it is attained by ordered linear codes. The following theorem constitutes the main result of this section.

Theorem 3.1 *Suppose that both the main and the eavesdropper channels are OSCs, namely, $W_1 = W_r(\varepsilon)$ and $W_2 = W_r(\theta)$ (see Figure 3.3). Let γ be given by (3.5) and (3.6). Then the secrecy capacity of the wiretap channel equals*

$$C_s = r(h_{q,r}(\gamma) - h_{q,r}(\varepsilon))$$

Similarly, suppose that the channels $W_1 = W_r(\varepsilon)$ and $W_2 = W_r(\theta)$ are OECs. Then the secrecy capacity of the wiretap channel equals

$$C_s = |\gamma|' - |\varepsilon|'$$

where $\gamma = (\gamma_0, \ldots, \gamma_r)$ with γ_i's are equal to (3.7) and (3.8). The capacity in both cases can be achieved by linear ordered codes.

The proof of this result relies on domination conditions among the crossover shapes, motivating their introduction earlier in the thesis. To begin, we show that a cascade of two ordered channels is an ordered channel. This is an elementary but tedious calculation that is relegated to the appendix to this chapter.

Lemma 3.3 *Let the channel W^* be a cascade of the channels W_1 and W_2. If the channel W_1 is an OSC with crossover shape ε and W_2 is an OSC with θ, the channel W^* becomes an OSC with crossover shape γ where*

$$\gamma_0 = \varepsilon_0\theta_0 + \sum_{i=1}^{r} \frac{\varepsilon_i\theta_i}{q^{i-1}(q-1)}, \tag{3.5}$$

$$\gamma_j = \theta_j \sum_{i=0}^{j-1} \varepsilon_i + \varepsilon_j \sum_{i=0}^{j-1} \theta_i + \theta_j\varepsilon_j \frac{q-2}{q-1} + \sum_{i=j+1}^{r} \frac{\theta_i\varepsilon_i}{q^{i-j}}, \qquad (j = 1, \ldots, r). \tag{3.6}$$

Similarly, if the channel W_1 is an OEC with erasure shape ε and W_2 is an OEC with θ. Then W^* becomes an OEC with erasure shape γ, where

$$\gamma_0 = \varepsilon_0\theta_0, \tag{3.7}$$

$$\gamma_j = \theta_j \sum_{i=0}^{j-1} \varepsilon_i + \varepsilon_j \sum_{i=0}^{j-1} \theta_i + \varepsilon_j\theta_j, \quad j = 1, \ldots, r. \tag{3.8}$$

The next lemma establishes the domination conditions.

Lemma 3.4 *The vectors ε and γ are related by $\varepsilon \leq \gamma$ (2.5).*

The proof of this lemma is given in the appendix.

Lemma 3.5 *Let W_1 and W_2 be the OSCs with crossover shape ε and γ, respectively. If $\varepsilon \leq \gamma$, then $\mathscr{C}(W_1) \geq \mathscr{C}(W_2)$ with equality if $\varepsilon = \gamma$.*

Proof: Let $T(x_1, x_2, \ldots, x_r) = -x_0 \ln x_0 - \sum_{i=1}^{r} x_i \ln \frac{x_i}{q^{i-1}(q-1)}$ where $x_0 = 1 - x_1 - \cdots - x_r$. From the capacity formula (3.2), we can prove the lemma by showing that $T(\varepsilon) \leq T(\gamma)$ for $\varepsilon \leq \gamma$. Let $\boldsymbol{v} = (v_1, \ldots, v_r)$ be a unit vector in the direction given by $\gamma - \varepsilon$. Then $(\gamma_1, \ldots, \gamma_r) = (\varepsilon_1 + \alpha v_1, \ldots, \varepsilon_r + \alpha v_r)$ for some $\alpha \geq 0$. Since $\varepsilon \leq \gamma$, we have $v_{r-l+1} + \cdots + v_r \geq 0$ for $l = 1, \ldots, r$. We find the rate of change of T from ε in the direction of $\boldsymbol{v}$ as

$$\nabla T \cdot \alpha \boldsymbol{v} = \alpha \sum_{j=1}^{r} \ln \frac{\varepsilon_0}{\varepsilon_j / q^{j-1}(q-1)} v_j.$$

Using the conditions on v_l for $l = 1, \ldots, r$ above and (3.1), we get

$$\begin{aligned} \alpha(\ln \frac{\varepsilon_0}{\varepsilon_1/(q-1)} v_1 + \cdots + \ln \frac{\varepsilon_0}{\varepsilon_r/q^{r-1}(q-1)} v_r) & \\ \geq \alpha(\ln \frac{\varepsilon_1/(q-1)}{\varepsilon_2/q(q-1)} v_2 + \cdots + \ln \frac{\varepsilon_1/(q-1)}{\varepsilon_r/q^{r-1}(q-1)} v_r) & \\ \geq \cdots \geq \alpha \ln \frac{\varepsilon_{r-1}/q^{r-2}(q-1)}{\varepsilon_r/q^{r-1}(q-1)} v_r. & \end{aligned}$$

Since $\alpha \geq 0$, $\frac{\varepsilon_{r-1}}{q^{r-2}(q-1)} > \frac{\varepsilon_r}{q^{r-1}(q-1)}$, and $v_r \geq 0$, the last term is greater than or equal to 0. Thus, $T(\varepsilon) \leq T(\gamma)$ as long as $\varepsilon \leq \gamma$. Therefore, $T(\cdot)$ is an increasing function along any path from ε to γ and $\mathscr{C}(W_r(\varepsilon)) \geq \mathscr{C}(W_r(\gamma))$, as required where equality holds when $\alpha = 0$ or $\varepsilon = \gamma$. ■

Proof of Theorem 3.1: The general results of [72] with respect to the wiretap channel of Fig. 3.3 imply that the secrecy capacity of the system is given by

$$C_s = \max_{P_X} [I(X;Y) - I(X;Z)].$$

Since a channel from Alice to Eve is degraded with respect to a channel from Alice to Bob, the main channel is *less noisy* than the wiretap channel. It was shown in [22] that if the main channel is less noisy than the wiretap channel and $I(X;Y)$ and $I(X;Z)$ are individually maximized by the same input distribution P_X, the secrecy capacity equals the difference between the capacity of the main channel and the capacity of the wiretap channel. The wiretap channel W^* is the cascade of the channels W_1 and W_2. Then by Lemma 3.3 W^* is an OSC with crossover shape $\gamma = (\gamma_0, \ldots, \gamma_r)$, where the γ_i's are given by (3.5)-(3.6). If W_2 is noiseless, i.e., $\theta_0 = 1$ and $\theta_i = 0$ for $i = 1, \ldots, r$, then W^* becomes the same channel as W_1. Otherwise from Lemma 3.4 and Lemma 3.5, the capacity of W^* is less than W_1. Therefore, the secrecy capacity of parallel wiretap channels over the OSC is

$$C_s = \mathscr{C}(W_1) - \mathscr{C}(W^*) = r(h_{q,r}(\gamma) - h_{q,r}(\varepsilon))$$

Now let us show that the secrecy capacity C_s can be achieved by linear ordered codes. Wyner [72] introduced the basic idea of coding scheme using random linear codes when the main channel is noiseless and the wiretap channel is a binary symmetric channel. In [16], the authors showed that the secrecy capacity can be achieved by using random linear codes when both the

main channel and the wiretap channel are binary symmetric channels. The proof that there exist secrecy capacity achieving linear ordered codes is an extension of the above works.

To encode a message, we choose q-ary matrices $\mathbf{H}$, $\mathbf{H}_1$, and $\mathbf{H}_2$ in the following way. Independently and randomly choose an $nr \times k_1$ matrix $\mathbf{H}_1$ and an $nr \times k$ matrix $\mathbf{H}$, where $0 < k < k_1$. Let

$$\mathbf{H}_2 = \begin{pmatrix} \mathbf{H}_1 \\ \mathbf{H} \end{pmatrix}.$$

Choosing $k_2 = k_1 - k$, we observe that $\mathbf{H}_2$ is a matrix with $nr - k_2$ rows and nr columns. Note that with probability arbitrarily close to 1, all the rows of $\mathbf{H}_2$ are linearly independent. For arbitrary small $\delta > 0$, let

$$k_1 = nr\lfloor(1 - h_{q,r}(\varepsilon) - 2\delta)\rfloor$$
$$k_2 = nr\lfloor(1 - h_{q,r}(\theta) - 2\delta)\rfloor.$$

Then we obtain

$$\begin{aligned} \frac{k}{nr} &= \frac{nr\lfloor(1 - h_{q,r}(\varepsilon) - 2\delta)\rfloor - nr\lfloor(1 - h_{q,r}(\theta) - 2\delta)\rfloor}{nr} \\ &\geq \frac{nr(1 - h_{q,r}(\varepsilon) - 2\delta) - 1 - nr(1 - h_{q,r}(\theta) - 2\delta)}{nr} \\ &= h_{q,r}(\theta) - h_{q,r}(\varepsilon) - \frac{1}{nr} \end{aligned}$$

and thus for any given $\alpha > 0$ there exists an integer $n_0 > 1/r\alpha$ such that $R \geq h_{q,r}(\theta) - h_{q,r}(\varepsilon) - \alpha$.

To encode a message $\boldsymbol{s}$, an output sequence $\boldsymbol{x}$ is chosen randomly and uniformly among the sequences that satisfy the following equation:

$$\boldsymbol{x}\mathbf{H}_2^T = (\boldsymbol{x}\mathbf{H}_1^T | \boldsymbol{x}\mathbf{H}^T) = (0|\boldsymbol{s}) \tag{3.9}$$

Since $\mathbf{H}_2$ and $\mathbf{H}_1$ have full rank, this equation is satisfied by 2^{k_2} vectors which form disjoint subsets for every choice of $\boldsymbol{s}$. We observe that the linear code $\mathcal{C}_1$ defined by the parity-check matrix $\mathbf{H}_1$ is partitioned into 2^k cosets of code $\mathcal{C}_2$ which is defined by $\mathbf{H}_2$. Thus, Eve can locate the transmission only up to the coset index, and her uncertainty about the message is $\log 2^k$. Informally speaking, this means that Alice is able to transmit securely the message of size close to $\log 2^k$.

To formalize this conclusion and at the same time to argue about the reliability of transmission to Bob, assume that both the legitimate receiver and the wiretapper use the typical sets decoder. The typical sets for Bob and Eve are as follows:

$$T_{\mathbf{E}}^N(\delta) = \{\boldsymbol{e} : q^{-nr(h_{q,r}(\varepsilon)+\delta)} \leq \Pr[\mathbf{E} = \boldsymbol{e}] \leq q^{-nr(h_{q,r}(\varepsilon)-\delta)}\},$$
$$T_{\mathbf{E}_w}^N(\delta) = \{\boldsymbol{e}_w : q^{-nr(h_{q,r}(\theta)+\delta)} \leq \Pr[\mathbf{E}_w = \boldsymbol{e}_w] \leq q^{-nr(h_{q,r}(\theta)-\delta)}\},$$

where $\boldsymbol{e}$ is the error sequence for Bob and $\boldsymbol{e}_w$ is the error sequence for Eve and $\mathbf{E}$ and $\mathbf{E}_w$ are random variables on their respective spaces. Then, from [16], it can be shown that $P_e \to 0$ and the equivocation $\frac{1}{k}H(S^k|Z^N) \to 1$ as $k \to \infty$ with fixed r. Therefore, the above code achieves the reliability and weak security condition. It was shown in [44] that we can obtain a coding scheme which achieves the strong security condition from any coding scheme which satisfies the weak security condition through privacy amplification. Notice that this coding scheme enables us to achieve the top-left corner in the rate region in Fig. 3.4, i.e. the point $R_e = R_1 = C_s$.

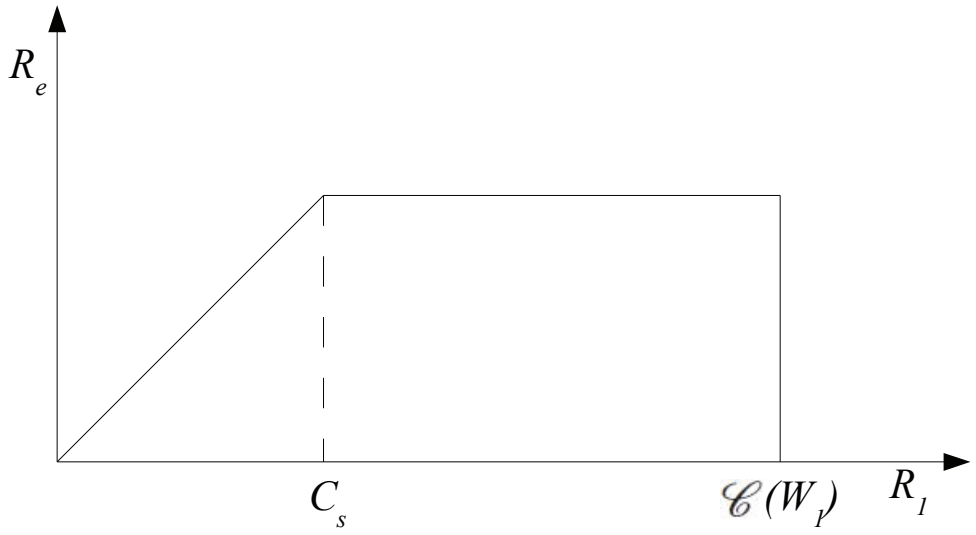

Figure 3.4: The rate region of parallel wiretap channels over OSCs

Let us switch to the case of OECs and assume that Eve's channel is degraded with respect to the main channel. Similarly to the argument of parallel wiretap channels over the OSC, the secrecy capacity of the parallel wiretap channels over the OEC is the difference between the capacity of the main channel and the capacity of the wiretap channel. Let $W_1 = W_r(\varepsilon)$ be the main channel which is the OEC with erasure shape ε and let $W_2 = W_r(\theta)$ be the channel from Alice to Eve, also an OEC with erasure shape θ. The wiretap channel W^* is a cascade channel of W_1 and W_2, which becomes an OEC with erasure shape γ given in (3.7)-(3.8) in Lemma 3.3.

From Lemma 3.4 we have $\varepsilon \leq \gamma$ as given in (2.5) and thus capacity of two channels W_1 and W^* are related by $\mathscr{C}(W_1) \geq \mathscr{C}(W^*)$ with the equality when $\varepsilon = \gamma$. Therefore, the secrecy capacity of parallel wiretap channels is

$$C_s = \mathscr{C}(W_1) - \mathscr{C}(W^*) = |\gamma|' - |\varepsilon|'$$

and this capacity can be attained by linear ordered codes. ■

Furthermore, the following theorem can be readily obtained by extending the results in [72] and [18]. Let R_1 be an achievable transmission rate from Alice to Bob. Define Eve's equivocation rate as

$$R_{eq} = \frac{1}{n} H(S^k | Z^{nr}).$$

Theorem 3.2 *The region $\mathfrak{R}$ which is the set of achievable rate pairs (R_1, R_{eq}) for parallel wiretap channels defined above is given by*

$$\begin{aligned} &0 \leq R_{eq} \leq R_1 \\ &R_{eq} \leq C_s \\ &R_1 \leq \mathscr{C}(W_1). \end{aligned}$$

The rate region of parallel wiretap channels formed of q-ary ordered symmetric (erasure) channels is given in Fig. 3.4.

3.4.2 Wiretap Channel of Type II

A combinatorial counterpart of the wiretap channel in the previous section was considered in [50]. In this model, Alice encodes k data symbols into a codeword of length N and transmits the coded sequence over a noiseless channel to Bob. An eavesdropper, Eve, is able to observe any $s < N$ symbols of her choosing noiselessly. Let $R = \frac{k}{N}$ be the rate of the encoder, let $\alpha = \frac{s}{N}$ be the fraction of the encoded bits that the eavesdropper is able to observe, and let $\Delta = \frac{1}{k}\min_{A\subseteq\{1,\ldots,N\}:|A|=s} H(S^k|Z^N)$ be the normalized equivocation. Here Z_i is equal to X_i if $i \in A$ and is an erasure if $i \notin A$. As shown in [50], the triple $(R, \alpha, \Delta) \in [0,1]^3$ is achievable if and only if

$$\Delta \leq \begin{cases} 1, & 0 \leq \alpha \leq 1-R \\ \frac{1-\alpha}{R}, & 1-R \leq \alpha \leq 1. \end{cases}$$

They also proved that if the triple (R, α, Δ) is achievable, then there exists a coding scheme using group codes that achieves the capacity of the wiretap channel.

Later, Wei [67] considered the implementation of this transmission with linear codes, thereby finding a connection between generalized Hamming weights and the wiretap channel of type II. Consider the coding scheme suggested in [50] using an $[N, N-k]$ linear code $\mathcal{C}$. Let $\mathbf{H}$ be a parity-check matrix of a linear code $\mathcal{C}$. There are 2^k cosets. To encode a message, Alice chooses a coset based on the k bits of information and transmits a codeword $\boldsymbol{x}$ which is randomly selected from this coset. Bob receives the transmitted vector with no errors. Eve also has full knowledge of the code $\mathcal{C}$ but does not know the location of the vector from the coset.

Let Δ_s be the equivocation of Eve upon observing s symbols of the transmitted codeword. The quantity Δ_s is given by the following lemma.

Lemma 3.6 *[50] Let $\mathcal{C}$ be an $[N, N-k]$ linear code and $\mathbf{H} = (h_1, h_2, \ldots, h_N)$ be a parity-check matrix of this code, where h_i is the ith column of $\mathbf{H}$. Assume that $\boldsymbol{s}$ is a message and $\boldsymbol{x}$ is a codeword and consider the encoding scheme described above. Then the equivocation Δ_s, $s = 0, 1, \ldots, N$ becomes*

$$\Delta_s = \min_{|A|=N-s} \mathrm{rk}(\mathbf{H}(A))$$

where $\mathbf{H}(A)$ is the submatrix of $\mathbf{H}$ formed by the columns with indices in A.

The outline of the proof is as follows. The quantity $H(S^k|Z^N)$ is

$$H(S^k|Z^N) = H(X^N, S^k|Z^N) - H(X^N|S^k, Z^N) = N - s - H(X^N|S^k, Z^N)$$

and thus let us compute $H(X^N|S^k, Z^N)$. Assume that Eve taps s coordinates of $\boldsymbol{x}$ and denote the set of indices of the remaining coordinates by A. Given S^k and Z^N, the remaining unknown symbols of X^N are the solutions for x_i, $i \in A$ of

$$\sum_{i\in A} h_i x_i = \boldsymbol{s}' + \sum_{i\in A^c}^{N} h_i x_i$$

where $\boldsymbol{s}' = \mathbf{H}\boldsymbol{x}^T$. This quantity is known because we know the coset leader of the transmitted codeword. Since all the solutions of this equation are equally likely, $H(X^N|S^k, Z^N) = N - s - \mathrm{rk}(\mathbf{H}(A))$. Thus $\Delta_s = \min_{|A|=N-s} \mathrm{rk}(\mathbf{H}(A))$

Recall the support weight distributions defined earlier in Sect. 2.1. Consider m-dimensional subcodes of the code $\mathcal{C}$. The support of a subcode A is the set of coordinates in which at least one

of the vectors in A is nonzero. Define the m-th higher weight of the code $\mathcal{C}$ as the size of the smallest support of its m-dimensional subcode, $m \geq 1$. By Corollary A in [67], we have

$$d_{n-s-\Delta_s}(\mathcal{C}^\perp) \leq n - s < d_{n-s-\Delta_s+1}(\mathcal{C}^\perp).$$

For a given s we obtain the normalized equivocation $\Delta = \frac{1}{k}\Delta_s$. This means that the change of the equivocation Δ is determined by the higher Hamming weights of the dual code $\mathcal{C}^\perp$, and thus the distributions of support weights completely characterize the performance of a linear code $\mathcal{C}$ on the wiretap channel of type II.

Consider the ordered version of this transmission: suppose that the eavesdropper observes s symbols that form an ideal $I \in \mathcal{I}(P)$, where P is the NRT poset. Consider a linear $[nr, nr-k, d]$ code $\mathcal{C}$ and suppose that Alice sends a random vector from some coset in $\mathbb{F}_q^{nr}/\mathcal{C}$. The equivocation of Eve upon observing the symbols in I equals

$$\Delta_I = \min_{I^c \in \mathcal{I}(P^\perp),\, |I^c| = nr-s} \mathrm{rk}(\mathbf{H}(I^c)),$$

where $\mathbf{H}$ is the parity-check matrix of $\mathcal{C}$. Since I^c is an ideal in $P^\perp$, the guaranteed gain of Eve is controlled by higher ordered weights of the dual code $\mathcal{C}^\perp$. This provides a cryptographic motivation for the study of higher poset weights, previously considered in [8] as a combinatorial problem.

Appendix

Proof of Lemma 3.3: Let us compute the conditional probability $W^*(z|x) = \sum_y W_1(y|x)W_2(z|y)$ when W_1 and W_2 are OSCs first. If $z = x$ this quantity is

$$\begin{aligned}
&W^*(z|x)\\
&= \sum_y W_1(y|x)W_2(z|y)\\
&= \sum_{y:\ y=x} W_1(y|x)W_2(z|y) + \sum_{y:\ d_r(x,y)=1} W_1(y|x)W_2(z|y) + \dots\\
&\quad + \sum_{y:\ d_r(x,y)=r} W_1(y|x)W_2(z|y)\\
&= \varepsilon_0\theta_0 + (q-1)\frac{\varepsilon_1}{q-1}\frac{\theta_1}{q-1} + \dots + q^{r-1}(q-1)\frac{\varepsilon_r}{q^{r-1}(q-1)}\frac{\theta_r}{q^{r-1}(q-1)}\\
&= \varepsilon_0\theta_0 + \sum_{i=1}^{r} \frac{\varepsilon_r\theta_r}{q^{i-1}(q-1)}.
\end{aligned}$$

When $d_r(x,z) = j$, $j = 1, \dots, r$ and $d_r(x,y) = k \neq j$ the ordered distance between y and z is j if $k < j$ and k if $k > j$. In addition if $d_r(x,y) = j$, the ordered distance $d_r(y,z) \in \{0, 1, \dots, j\}$.

Thus the conditional probability $W^*(z|x)$ becomes

$$
\begin{aligned}
&W^*(z|x)\\
&= \sum_y W_1(y|x)W_2(z|y)\\
&= \sum_{y:\ y=x} W_1(y|x)W_2(z|y) + \sum_{i=1}^{j-1} \sum_{y:\ d_r(x,y)=i} W_1(y|x)W_2(z|y)\\
&\quad + \sum_{i=j+1}^{r} \sum_{y:\ d_r(x,y)=i} W_1(y|x)W_2(z|y) + \sum_{i=0}^{j} \sum_{\substack{y:\ d_r(x,y)=j,\\ d_r(y,z)=i}} W_1(y|x)W_2(z|y)\\
&= \varepsilon_0 \frac{\theta_j}{q^{j-1}(q-1)} + \sum_{i=1}^{j-1} q^{i-1}(q-1) \frac{\varepsilon_i}{q^{i-1}(q-1)} \frac{\theta_j}{q^{j-1}(q-1)}\\
&\quad + \sum_{i=j+1}^{r} q^{i-1}(q-1) \frac{\varepsilon_i}{q^{i-1}(q-1)} \frac{\theta_i}{q^{i-1}(q-1)} + \frac{\varepsilon_j}{q^{j-1}(q-1)}\theta_0\\
&\quad + \sum_{i=0}^{j-1} q^{i-1}(q-1) \frac{\varepsilon_j}{q^{j-1}(q-1)} \frac{\theta_i}{q^{i-1}(q-1)} + q^{j-1}(q-2) \frac{\varepsilon_j}{q^{j-1}(q-1)} \frac{\theta_j}{q^{j-1}(q-1)}\\
&= \frac{1}{q^{j-1}(q-1)} (\theta_j \sum_{i=0}^{j-1} \varepsilon_i + \varepsilon_j \sum_{i=0}^{j-1} \theta_i) + \frac{q-2}{q-1} \frac{\varepsilon_j \theta_j}{q^{j-1}(q-1)} + \sum_{i=j+1}^{r} \frac{\varepsilon_i \theta_i}{q^{i-1}(q-1)}.
\end{aligned}
$$

By setting γ to be (3.5) and (3.6) we obtain $W^*(z|x) = \frac{\gamma_j}{q^{j-1}(q-1)}$ if $d_r(x,z) = j$, $j = 1, \ldots, r$ and $W^*(z|x) = \gamma_0$ if $x = z$.

It remains to prove that γ also satisfies condition (3.1). First let us consider the difference $\gamma_0 - \frac{\gamma_1}{q-1}$:

$$
\begin{aligned}
\gamma_0 - \frac{\gamma_1}{q-1} &= \varepsilon_0\theta_0 - \frac{1}{q-1}(\varepsilon_0\theta_1 + \varepsilon_1\theta_0 + \varepsilon_1\theta_1) + \frac{\varepsilon_1\theta_1}{q-1} + \frac{\varepsilon_1\theta_1}{(q-1)^2}\\
&= \varepsilon_0\theta_0 - \frac{\varepsilon_1\theta_0}{q-1} - \frac{\varepsilon_0\theta_1}{q-1} + \frac{\varepsilon_1\theta_1}{(q-1)^2}\\
&= \theta_0(\varepsilon_0 - \frac{\varepsilon_1}{q-1}) - \frac{\theta_1}{q-1}(\varepsilon_0 - \frac{\varepsilon_1}{q-1})\\
&= (\varepsilon_0 - \frac{\varepsilon_1}{q-1})(\theta_0 - \frac{\theta_1}{q-1}) > 0.
\end{aligned}
$$

Further for $j = 1, \ldots, r-1$, the quantity $\frac{\gamma_j}{q^{j-1}(q-1)} - \frac{\gamma_{j+1}}{q^j(q-1)}$ is

$$
\begin{aligned}
&\frac{\gamma_j}{q^{j-1}(q-1)} - \frac{\gamma_{j+1}}{q^j(q-1)} \\
&= \frac{1}{q^j(q-1)}\big(q\varepsilon_j(\theta_0 + \cdots + \theta_{j-1}) + q\theta_j(\varepsilon_0 + \cdots + \varepsilon_{j-1}) + q\varepsilon_j\theta_j - \varepsilon_{j+1}(\theta_0 + \cdots + \theta_j) \\
&\quad - \theta_{j+1}(\varepsilon_0 + \cdots + \varepsilon_j)\big) - \frac{\varepsilon_j\theta_j}{q^{j-1}(q-1)^2} + \frac{\varepsilon_{j+1}\theta_{j+1}}{q^j(q-1)^2} \\
&= \frac{1}{q^j(q-1)}((q\varepsilon_j - \varepsilon_{j+1})(\theta_0 + \cdots + \theta_{j-1}) + (q\theta_j - \theta_{j+1})(\varepsilon_0 + \cdots + \varepsilon_{j-1}) \\
&\quad + q\varepsilon_j\theta_j - \varepsilon_{j+1}\theta_j - \varepsilon_j\theta_{j+1}) - \frac{1}{q^j(q-1)^2}(q\varepsilon_j\theta_j - \varepsilon_{j+1}\theta_{j+1}) \\
&= \frac{1}{q^j(q-1)^2}((q-1)(q\varepsilon_j - \varepsilon_{j+1})(\theta_0 + \cdots + \theta_{j-1}) + (q-1)(q\theta_j - \theta_{j+1})(\varepsilon_0 + \cdots + \varepsilon_{j-1}) \\
&\quad + (q-1)\theta_j(q\varepsilon_j - \varepsilon_{j+1}) - \varepsilon_j(q\theta_j - \theta_{j+1}) - \theta_{j+1}(q\varepsilon_j - \varepsilon_{j+1})) \\
&= \frac{1}{q^j(q-1)^2}((q\varepsilon_j - \varepsilon_{j+1})((q-1)(\theta_0 + \cdots + \theta_j) - \theta_{j+1}) \\
&\quad + (q\theta_j - \theta_{j+1})((q-1)(\varepsilon_0 + \cdots + \varepsilon_{j-1}) - \varepsilon_j)) \\
&> 0
\end{aligned}
$$

where the last inequality follows from (3.1) for ε and θ. Namely,

$$
\begin{aligned}
&(q-1)(\varepsilon_0 + \cdots + \varepsilon_{j-1}) \\
&> \varepsilon_1 + (q-1)(\varepsilon_1 + \cdots + \varepsilon_{j-1}) \\
&= q\varepsilon_1 + (q-1)(\varepsilon_2 + \cdots + \varepsilon_{j-1}) > \varepsilon_2 + (q-1)(\varepsilon_2 + \cdots + \varepsilon_{j-1}) \\
&\cdots > \varepsilon_j.
\end{aligned}
$$

Next suppose that both channels W_1 and W_2 are OECs. Since some parts of the input vector of the channel W_2 may contain erasures, we extend the definition of the channel W_2 and assume that the erasure of the output of W_2 is the union of the erasures introduced by W_1 and W_2. Let x be the input to the channel W_1, y be the output of W_1 which is the input to W_2, and z be the output of W_2. For example, let y contain one erasure. Then the conditional probability $P(z|y)$ is 0 if z does not have erasure, $\theta_0 + \theta_1$ if $z = y$ and θ_j, $j = 2, \ldots, r$ if $z_1 = \cdots = z_j = ?$ and $z_i = y_i$, $i = j+1, \ldots, r$.

From the above argument and the definition of the OEC, we obtain Equations (3.7) and (3.8) in the following way. The conditional probability $W^*(z|x)$ becomes $\varepsilon_0\theta_0$ when $z = x$. Assuming that $d_r(x, z) = j$, $j = 1, \ldots, r$ and the first j entries of z are erasures, we have

$$
\begin{aligned}
W^*(z|x) &= \sum_y W_1(y|x)W_2(z|y) \\
&= \sum_{i=0}^{j} \sum_{\substack{y:\ d_r(x,y)=i, \\ y_1^i = ?^i}} W_1(y|x)W_2(z|y) \\
&= (\varepsilon_0 + \cdots + \varepsilon_{r-1})\theta_r + (\theta_0 + \cdots + \theta_{r-1} + \theta_r)\varepsilon_r
\end{aligned}
$$

where $y_1^i = (y_1, \ldots, y_i)$ and ? is the erasure symbol. This gives (3.8). ■

Proof of Lemma 3.4: Let us consider the OSC case first. Since ε is crossover shape for an

OSC, it must satisfy (3.1). The following is a direct consequence of this condition for any $j \geq 1$.

$$\begin{aligned}\varepsilon_0 + \varepsilon_1 + \cdots + \varepsilon_j &> \frac{q}{q-1}\varepsilon_1 + \varepsilon_2 + \cdots + \varepsilon_j \\ &> \cdots > \frac{q}{q-1}\varepsilon_j.\end{aligned}$$

From (3.5) and (3.6) and the above constraint, we obtain

$$\begin{aligned}\gamma_r &= \varepsilon_r\theta_0 + \cdots + \varepsilon_r\theta_{r-1} + (\varepsilon_0 + \cdots + \varepsilon_r - \frac{\varepsilon_r}{q-1})\theta_r \\ &\geq \varepsilon_r(\theta_0 + \cdots + \theta_{r-1}) + \varepsilon_r\theta_r = \varepsilon_r,\end{aligned}$$

where equality holds when $\theta_r = 0$. For any $1 \leq j \leq r-1$

$$\begin{aligned}&\gamma_j + \cdots + \gamma_r \\ &= (\varepsilon_j + \cdots + \varepsilon_r)(\theta_0 + \cdots + \theta_{j-1}) + \sum_{i=j}^{r}(\varepsilon_0 + \cdots + \varepsilon_r - \frac{\varepsilon_i}{q-1} + \sum_{l=1}^{i-j}\frac{\varepsilon_i}{q^l})\theta_i \\ &= (\varepsilon_j + \cdots + \varepsilon_r)(\theta_0 + \cdots + \theta_{j-1}) + \sum_{i=j}^{r}(\varepsilon_0 + \cdots + \varepsilon_r - \frac{\varepsilon_i}{q^{i-j}(q-1)})\theta_i \\ &\geq (\varepsilon_j + \cdots + \varepsilon_r)(\theta_0 + \cdots + \theta_{j-1}) + \sum_{i=j}^{r}(\varepsilon_j + \cdots + \varepsilon_r + \frac{q}{q-1}\varepsilon_{j-1} - \frac{\varepsilon_i}{q^{i-j}(q-1)})\theta_i \\ &= (\varepsilon_j + \cdots + \varepsilon_r)(\theta_0 + \cdots + \theta_r) + \frac{q}{q-1}\varepsilon_{j-1}(\theta_j + \cdots + \theta_r) - \left(\frac{\varepsilon_j\theta_j}{q-1} + \cdots + \frac{\varepsilon_r\theta_r}{q^{r-j}(q-1)}\right) \\ &= \varepsilon_j + \cdots + \varepsilon_r + \frac{\theta_j}{q-1}(q\varepsilon_{j-1} - \varepsilon_j) + \cdots + \frac{\theta_r}{q^{r-j}(q-1)}(q^{r-j+1}\varepsilon_{j-1} - \varepsilon_r) \\ &\geq \varepsilon_j + \cdots + \varepsilon_r\end{aligned}$$

and thus we have $\varepsilon \leq \gamma$ with equality when $\theta_i = 0$ for all $i = 1, \ldots, r$ which means that the channel W_2 is noiseless.

When both channels W_1 and W_2 are OECs, the quantity γ_j, $j = 1, \ldots, r$ given by (3.8), equals

$$\begin{aligned}\gamma_j &= \theta_j\sum_{i=0}^{j-1}\varepsilon_i + \varepsilon_j\sum_{i=0}^{j-1}\theta_i + \varepsilon_j\theta_j \\ &= \Big(\sum_{i=0}^{j}\varepsilon_i\Big)\Big(\sum_{i=0}^{j}\theta_i\Big) - \Big(\sum_{i=0}^{j-1}\varepsilon_i\Big)\Big(\sum_{i=0}^{j-1}\theta_i\Big).\end{aligned}$$

Thus for any $j = 1, \ldots, r$, the summation

$$\begin{aligned}
\gamma_j + \cdots + \gamma_r &= \Big(\sum_{i=0}^{r} \varepsilon_i\Big)\Big(\sum_{i=0}^{r} \theta_i\Big) - \Big(\sum_{i=0}^{j-1} \varepsilon_i\Big)\Big(\sum_{i=0}^{j-1} \theta_i\Big) \\
&= 1 - \Big(\sum_{i=0}^{j-1} \varepsilon_i\Big)\Big(\sum_{i=0}^{j-1} \theta_i\Big) \\
&\geq 1 - \Big(\sum_{i=0}^{j-1} \varepsilon_i\Big) \\
&= \sum_{i=j}^{r} \varepsilon_i
\end{aligned}$$

where equality holds when $\sum_{i=0}^{j-1} \theta_i = 1$. Therefore $\varepsilon = \gamma$ if $\theta_0 = 1$ and $\theta_i = 0$, $i = 1, \ldots, r$ which means that the channel W_2 is noiseless. ■

Chapter 4

Polar Codes for q-ary Channels, $q = 2^r$

In this chapter we study a family of codes called polar codes which achieve the (symmetric) capacity of DMCs with low encoding and decoding complexity. These codes were suggested by Arıkan [3] for binary-input channels. In this chapter we extend Arıkan's results to the case of DMCs with q-ary input, $q = 2^r$.

4.1 Introduction: Binary Polar Codes

In this section we give a brief introduction to the construction of binary polar codes in [3]. Let W be a binary-input DMC $W : \mathcal{X} \to \mathcal{Y}$, where $\mathcal{X} = \{0, 1\}$ and $\mathcal{Y}$ is any discrete set. Let P_X be a probability distribution on $\mathcal{X}$, where X is the random value of the channel input. The capacity of W is given by $\max_{P_X} I(X;Y)$, where Y is the random variable on $\mathcal{Y}$ whose distribution is induced by P_X and W. Let $\tilde{P}_X$ be the uniform distribution given by $\tilde{P}_X(0) = \tilde{P}_X(1) = 1/2$. This choice is the maximizing distribution in the capacity expression if the channel is symmetric, which includes many practically important cases such as a binary symmetric channel. Using $\tilde{P}_X$ in the above expression, we obtain the *symmetric capacity* of the channel W:

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

Define the Bhattacharyya parameter of the channel by

$$Z(W) \triangleq \sum_{y} \sqrt{W(y|0)W(y|1)}.$$

Binary polar codes form a family of linear codes whose encoding map is explained through the following argument. Let u_1, u_2 be two bits of data to be transmitted over W. Suppose that they are transmitted over the channel using the bits $x_1 = u_1 \oplus u_2$ and $x_2 = u_2$ where $\oplus$ is a modulo-2 summation. We write this transformation as

$$(x_1, x_2) = (u_1, u_2)H_2$$

where the matrix $H_2 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ is called the polarization kernel (see Fig. 4.1). We obtain a channel derived from two uses of the channel W and given by

$$W_2(y_1, y_2|u_1, u_2) = W(y_1|u_1 \oplus u_2)W(y_2|u_2).$$

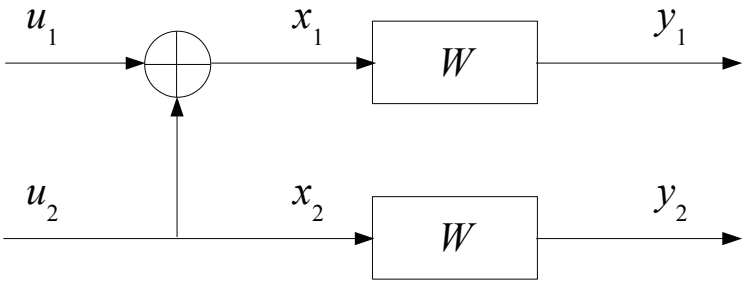

Figure 4.1: The first level of the recursion step using a kernel H_2.

The capacity of this channel is $I(W_2) = 2I(W)$.

Let $U_i, Y_i, i = 1, 2$ be random variables that correspond to the input and the output. Since U_1 and U_2 are independent, we have

$$I(U_1; Y_1, Y_2) \leq I(W) \leq I(U_2; Y_1, Y_2, U_1).$$

This defines "virtual channels" for the bits $u_i, i = 1, 2$ given by

$$W^-(y_1, y_2|u_1) = \sum_{u_2 \in \mathcal{X}} \frac{1}{2} W(y_1|u_1 \oplus u_2) W(y_2|u_2) \tag{4.1}$$

$$W^+(y_1, y_2, u_1|u_2) = \frac{1}{2} W(y_1|u_1 \oplus u_2) W(y_2|u_2). \tag{4.2}$$

We observe that capacity of the channel W^+ is greater than $I(W)$ and therefore, capacity of W^- is smaller than $I(W)$.

Iterating this transformation, one can amplify the separation of capacity values which eventually "polarize" to almost 0 and almost 1. After n iteration steps we obtain $N = 2^n$ channels $W_N^{(i)}, j = 1, \ldots, N$ where

$$W_N^{(i)}(y_1^N, u_1^{i-1}|u_i) = \frac{1}{2^{N-1}} \sum_{u_{i+1}^N \in \mathcal{X}^{N-i}} W^N(y_1^N|u_1^N G_N).$$

It is shown in [3] that as n increases, the channels $W_N^{(i)}$ become either almost perfect or almost completely noisy (polarize). In formal terms, for any $\varepsilon > 0$

$$\lim_{n \to \infty} \frac{|\{b \in \{+,-\}^n : I(W^b) \in (\varepsilon, 1-\varepsilon)\}|}{2^n} = 0. \tag{4.3}$$

To justify this equality, let us recall the setting of [3] for the evolution of the channel parameters. This setting will be used in our study of nonbinary alphabets below in this chapter. On the set $\Omega = \{+,-\}^*$ of semi-infinite binary sequences define a σ-algebra $\mathcal{F}$ generated by the cylinder sets $S(b_1, \ldots, b_n) = \{\omega \in \Omega : \omega_1 = b_1, \ldots, \omega_n = b_n\}$ for all sequences $(b_1, \ldots, b_n) \in \{+,-\}^n$ and for all $n \geq 0$. Consider the probability space $(\Omega, \mathcal{F}, P)$, where $P(S(b_1, \ldots, b_n)) = 2^{-n}, n \geq 0$. Define a filtration $\mathcal{F}_0 \subset \mathcal{F}_1 \subset \cdots \subset \mathcal{F}$ where $\mathcal{F}_0 = \{\emptyset, \Omega\}$ and $\mathcal{F}_n, n \geq 1$ is generated by the cylinder sets $S(b_1, \ldots, b_n), b_i \in \{+,-\}$. This filtration is used for defining the tree process associated with the transformation (4.1) -(4.2) and for proving results about the convergence of its parameters.

Let $B_i, i = 1, 2, \cdots$ be i.i.d. $\{+, -\}$-valued random variables with $\Pr(B_1 = +) = \Pr(B_1 = -) = 1/2$. We obtain a random process on an infinite binary tree whose value after n steps is given by the random vector $B = (B_1, B_2, \ldots, B_n)$. This process gives rise to a random process of channel evolution, where in step n we obtain a random channel $W^B = W^{B_1,B_2,\ldots,B_n}$. Thus, $P(W^B = W_N^{(i)}) = 2^{-n}$ for all $i = 1, \ldots, N$. We will denote the random channel at time n by $W_n = W^B$. The symmetric capacity of the random channel at time n becomes a random variable that we denote by $I_n = I(W^B)$. We can analogously define a random variable $Z_n = Z(W^B)$. These random variables are adapted to the above filtration (meaning that I_n and Z_n are measurable with respect to $\mathcal{F}_n$ for every $n \geq 1$).

To prove (4.3), [3] uses the following sequence of arguments. First, the sequence of random variables $\{I_n, \mathcal{F}_n, n \geq 0\}$ forms a martingale. Secondly, the sequence of random variables $\{Z_n, \mathcal{F}_n, n \geq 0\}$ forms a supermartingale. This is proved using the relations

$$Z(W^+) = \big(Z(W)\big)^2,$$
$$Z(W^-) \leq 2Z(W) - \big(Z(W)\big)^2.$$

Third, Z_n converges a.s. to a $(0, 1)$-valued random variable. Finally, the quantities $I(W)$ and $Z(W)$ are related by the following lemma.

Lemma 4.1 *[3] For any binary-input DMC W*

$$I(W) \geq \log \frac{2}{1 + Z(W)},$$
$$I(W) \geq 1 - Z(W),$$
$$I(W) \leq \sqrt{1 - Z(W)^2}.$$

This proves the desired polarization for any binary-input DMC.

Paper [3] goes on to discuss the encoding and decoding procedures for polar codes as well as to establish initial results on the error probability of decoding using a simple recursive procedure termed successive cancellation decoding. The results on the error probability were later significantly advanced in [4, 30].

Polar codes represent a significant step in information theory, providing the first effective version of Shannon's capacity theorem. The discovery of polar codes generated a significant amount of follow-up works some of them are mentioned in the next section.

In this chapter we extend the results of [3] to the q-ary case, $q = 2^r$. We find that the virtual channels polarize to $r + 1$ levels, supporting capacity-attaining transmission over symmetric q-ary channels.

4.2 Prior Work on Nonbinary Polar Codes

A study of nonbinary polar codes was first undertaken by Şaşoğlu et al. [59]. In this paper, the authors proved polarization of any q-ary DMC using the basic kernel H_2 in the case when q is a prime number. Moreover, if q is not prime, they proved the existence of a series of permutations on the input alphabets such that coupled with a kernel H_2, the channels are polarized into two extremes. However, they stopped short of identifying an explicit transformation for the code construction. Mori and Tanaka [45] studied the q-ary polar codes using arbitrary kernels, although their work also did not contain explicit results.

Another study of nonbinary polar codes was performed by Abbe and Telatar [1]. The main goal of their work is a study of the polar coding scheme for multiple access channels. In this

scheme, the transmitters encode their messages independently using iterations of the mapping H_2. In the situation when independent users are merged into a single nonbinary input, [1] implies polarization of the channels to a potentially large number of extremal configurations. The main difference between [1] and the work in this chapter is that we use H_2 together with addition modulo q rather than the finite field addition in [1]. This enables us to reduce the number of extremal configurations and to establish a number of other desirable properties of the construction. We note that independently a related study was performed in the work by Sahebi and Pradhan [58] who also observed the multilevel polarization phenomenon for q-ary channels. The motivation of the approach of [58] relates to a detailed study of linear and group codes on q-ary channels, and is different from our approach.

Very recently, Şaşoğlu studied a class of transformations which polarize all i.i.d. processes over arbitrary alphabets into two-levels. Leveraging his work, in the last part of the chapter we adjust the polarization map to gain better control over the emerging extremal configurations.

4.3 Definitions

We consider the combining of the q-ary data under the action of the operator H_2, where $q = 2^r, r \geq 2$. Let $W : \mathcal{X} \to \mathcal{Y}$, $|\mathcal{X}| = q$ be a DMC. The *symmetric capacity* of the channel W equals

$$I(W) \triangleq \sum_{x\in\mathcal{X}} \sum_{y\in\mathcal{Y}} \frac{1}{q} W(y|x) \log \frac{W(y|x)}{\sum_{x'\in\mathcal{X}} \frac{1}{q} W(y|x')}$$

where the base of the logarithm is 2. Define the combined channel W_2 and the channels W^- and W^+ by

$$W_2(y_1, y_2|u_1, u_2) = W(y_1|u_1 + u_2)W(y_2|u_2)$$

$$W^-(y_1, y_2|u_1) = \sum_{u_2\in\mathcal{X}} \frac{1}{q} W_2(y_1, y_2|u_1, u_2) \tag{4.4}$$

$$W^+(y_1, y_2, u_1|u_2) = \frac{1}{q} W_2(y_1, y_2|u_1, u_2), \tag{4.5}$$

where $u_1, u_2 \in \mathcal{X}, y_1, y_2 \in \mathcal{Y}$ and $+$ is a modulo-q sum. This transformation can be applied recursively to the channels W^-, W^+ resulting in four channels of the form $W^{b_1 b_2}, b_1, b_2 \in \{+, -\}$.

As shown in [3], after n steps of the transformation (4.4)-(4.5) the channels $W_N^{(i)} : \mathcal{X} \to \mathcal{Y}^N \times \mathcal{X}^{i-1}, 1 \leq i \leq N$ are given by

$$W_N^{(i)}(y_1^N, u_1^{i-1}|u_i) = \frac{1}{q^{N-1}} \sum_{u_{i+1}^N \in \mathcal{X}^{N-i}} W^N(y_1^N|u_1^N G_N), \tag{4.6}$$

where $G_N = H_2^{\otimes n}$ and W^N denotes the "Nth degree extension" of W, i.e., $W^N(y_1^N|x_1^N) = \prod_i W(y_i|x_i)$. Here we use the shorthand notation for sequences of symbols: for instance, $y_1^N \triangleq (y_1, y_2, \ldots, y_N)$, etc.

For any pair of input symbols $x, x' \in \mathcal{X}$, the Bhattacharyya distance between them is defined as

$$Z(W_{\{x,x'\}}) = \sum_{y\in\mathcal{Y}} \sqrt{W(y|x)W(y|x')}$$

where $W_{\{x,x'\}}$ is the channel obtained by restricting the input alphabet of W to the subset $\{x, x'\} \subset \mathcal{X}$.

Define the quantity $Z_v(W)$ for $v \in \mathcal{X} \setminus \{0\}$:

$$Z_v(W) = \frac{1}{2^r} \sum_{x \in \mathcal{X}} Z(W_{\{x,x+v\}}).$$

Introduce the ith average Bhattacharyya distance of the channel W by

$$Z_i(W) = \frac{1}{2^{i-1}} \sum_{v \in \mathcal{X}_i} Z_v(W) \tag{4.7}$$

where $i = 1, 2, \cdots, r$ and $\mathcal{X}_i = \{v \in \mathcal{X} : \text{wt}_r(v) = i\}$. Then

$$\begin{aligned} Z(W) &\triangleq \frac{1}{2^r(2^r-1)} \sum_{x \neq x'} Z(W_{\{x,x'\}}) \\ &= \frac{1}{2^r - 1} \sum_{i=1}^{r} 2^{i-1} Z_i(W) \end{aligned} \tag{4.8}$$

We define random variables $Z_{\{x,x'\},n} = Z(W^B_{\{x,x'\}})$, $Z_{v,n} = Z_v(W^B)$, $Z_{i,n} = Z_i(W^B)$ and other similar random variables analogously to the random variables, I_n and Z_n defined in Section 4.1.

4.4 Channel Polarization

In this section, we state a sequence of results that shows that q-ary polar codes based on the kernel H_2 can be used to transmit reliably over the channel W for all rates $R < I(W)$. We rely on the notation and definitions for the evolution of channels given in the end of Sect. 4.1.

Theorem 4.1 *(a) Let $n \to \infty$. The random variable I_n converges a.s. to a random variable I_∞ with $E(I_\infty) = I(W)$.*

(b) For all $i = 1, 2, \ldots, r$

$$\lim_{n \to \infty} Z_{i,n} = Z_{i,\infty} \quad a.s.,$$

where the variables $Z_{i,\infty}$ take values in $\{0, 1\}$. With probability one the vector $(Z_{i,\infty}, i = 1, \ldots, r)$ takes one of the following values:

$$\begin{array}{ccc} (Z_{1,\infty} = 0, Z_{2,\infty} = 0, \ldots, Z_{r-1,\infty} = 0, Z_{r,\infty} = 0) \\ (Z_{1,\infty} = 1, Z_{2,\infty} = 0, \ldots, Z_{r-1,\infty} = 0, Z_{r,\infty} = 0) \\ (Z_{1,\infty} = 1, Z_{2,\infty} = 1, \ldots, Z_{r-1,\infty} = 0, Z_{r,\infty} = 0) \\ \vdots \qquad\qquad \vdots \qquad\qquad \vdots \\ (Z_{1,\infty} = 1, Z_{2,\infty} = 1, \ldots, Z_{r-1,\infty} = 1, Z_{r,\infty} = 0) \\ (Z_{1,\infty} = 1, Z_{2,\infty} = 1, \ldots, Z_{r-1,\infty} = 1, Z_{r,\infty} = 1). \end{array} \tag{4.9}$$

Let us restate part (b) of this theorem for finite n.

Proposition 4.1 *Let $0 < \varepsilon < 1/2, \delta > 0$ be fixed. For $k = 0, 1, \ldots, r$ define disjoint events*

$$B_{k,n}(\varepsilon) = \Big\{\omega : (Z_{1,n}, Z_{2,n}, \ldots, Z_{r,n}) \in \mathcal{R}_k\Big\}$$

where $\mathcal{R}_k = \mathcal{R}_k(\varepsilon) \triangleq \Big(\prod_{i=1}^{k} D_1\Big) \times \Big(\prod_{i=k+1}^{r} D_0\Big)$ and $D_0 = [0, \varepsilon)$, $D_1 = (1-\varepsilon, 1]$. Then there exists $n_0 = n_0(\varepsilon, \delta)$ such that $P(\cup_{k=0}^{r} B_{k,n}(\varepsilon)) \geq 1 - \delta$ for all $n \geq n_0$.

The proofs of these statements are given in a later part of this section.

We need the following lemma.

Lemma 4.2 *For a DMC $W : \mathcal{X} \to \mathcal{Y}$ with q-ary input $\mathcal{X}$, $I(W)$ and $Z(W)$ are related by*

$$I(W) \geq \log \frac{2^r}{1 + \sum_{i=1}^{r} 2^{i-1} Z_i(W)} \tag{4.10}$$

$$I(W) \leq \sum_{i=1}^{r} \sqrt{1 - Z_i(W)^2}. \tag{4.11}$$

For $r = 1$ these inequalities are proved in [3]. For $r > 1$ Eq. (4.10) is a restatement of [59, Prop. 3] using (4.8). This inequality represents the classical fact that the (symmetric) capacity of a channel is greater than or equal to its (symmetric) *cutoff rate*. We refer to [3] and [59] for details. The fact that (4.11) holds for all $r > 1$ is new, and is proved in the Section 4.11.2.

Inequalities (4.10) and (4.11) imply that if $(Z_1, \ldots, Z_r) \in \mathcal{R}_k(\varepsilon)$ then $|I(W) - (r-k)| \leq \gamma$ where $\gamma \geq \max(k\sqrt{\varepsilon}, (2^{r-k} - 1)\varepsilon \log e)$.

The following proposition is an immediate corollary of the above results.

Proposition 4.2 *(a) The random variable I_∞ is supported on the set $\{0, 1, \ldots, r\}$.*

(b) For every $0 \leq k \leq r$ and every $\delta > 0$ there exists $\varepsilon > 0$ such that

$$\lim_{n \to \infty} P(\{|I_n - (r-k)| \leq \delta\} \triangle B_{k,n}(\varepsilon)) = 0.$$

where $\triangle$ means the symmetric difference of sets.

(c) $E(|\{i : Z_{i,\infty} = 0\}|) = I(W)$.

Proof: The first statement is obvious from (4.10) and (4.11). To prove the second statement we note that, with the appropriate choice of ε

$$\{|I_n - (r-k)| \leq \delta\} \supset B_{k,n}(\varepsilon)$$

for all $n \geq 0$. At the same time, $P(\{|I_n - (r-k)| \leq \delta\} \cap B_{k',n}(\varepsilon)) = 0$ for all $k' \neq k$, and the probability of the disjoint union $P(\cup B_{k,n}(\varepsilon)) \to 1$ for any $\varepsilon > 0$. Together this implies (b). Finally, we have that $E(I_\infty) = I(W)$. Then use (a) and (b) to claim that $E(|\{i : Z_{i,\infty} = 0\}|) = \sum_{k=0}^{r} k P(I_\infty = k) = I(W)$. ∎

We can say a bit more about the nature of convergence established in this proposition. Let us fix $k \in \{0, 1, \ldots, r\}$ and define the channel for the $r - k$ rightmost bits of the transmitted symbol as follows:

$$W^{[r-k]}(y|u) = \frac{1}{2^k} \sum_{x \in \mathcal{X} : x_{k+1}^r = u} W(y|x), \qquad u \in \{0,1\}^{r-k}$$

where $x = (x_1, x_2, \ldots, x_r)$.

Lemma 4.3 *Let $V : \mathcal{X} \to \tilde{\mathcal{Y}}$ be a DMC and let $\delta > 0$. Suppose that $(Z_1(V), Z_2(V), \ldots, Z_r(V)) \in \mathcal{R}_k(\varepsilon)$, for some $0 \le k \le r$. If ε is sufficiently small, then $I(V^{[r-k]}) \ge r - k - \delta$. In particular, it suffices to take $\varepsilon \le 2^{-3r}$.*

Proof: We may assume that $1 \le k \le r-1$. Let $u \in \{0,1\}^{r-k}, x = (x_1, \ldots, x_k, u) \in \mathcal{X}, x' = (x'_1, \ldots, x'_k, u) \in \mathcal{X}$. Let $v \in \{0,1\}^{r-k}$, not all-zero, and consider

$$\begin{aligned} Z(V^{[r-k]}_{\{u,u+v\}}) &= \sum_y \sqrt{V^{[r-k]}(y|u)V^{[r-k]}(y|u+v)} \\ &= \frac{1}{2^k} \sum_y \sqrt{\sum_x \sum_{x'} V(y|x)V(y|x'+v')} \\ &\le \frac{1}{2^k} \sum_y \sum_x \sum_{x'} \sqrt{V(y|x)V(y|x'+v')} \\ &= \frac{1}{2^k} \sum_{x,x'} Z(V_{\{x,x'+v'\}}), \end{aligned}$$

where $v' = 0^k v_1 v_2 \ldots v_{r-k}$. Next observe that $d_r(x, x'+v') \ge k+1$, and that

$$Z_i(V) = \frac{1}{2^{r+i-1}} \sum_{w \in \mathcal{X}_i} \sum_{x \in \mathcal{X}} Z(V_{x,x+w}) < \varepsilon$$

for $i = k+1, \ldots, r$. This implies that $Z(V_{x,x'+v'}) < 2^{r+i-1}\varepsilon \le 2^{2r-1}\varepsilon$ for any x, x', v' of the chosen form. Now from the above we obtain that $Z(V^{[r-k]}_{\{u,u+v\}}) < 2^{2r+k-1}\varepsilon$. Since $Z_i(V^{[r-k]})$ is the average of the $Z(V^{[r-k]}_{\{u,u+v\}})$ over all v with $\mathrm{wt}_r(v) = i$, $Z_i(V^{[r-k]}) < 2^{2r+k-1}\varepsilon$ for all $i = 1, \ldots, r-k$. Now substitute this estimate into (4.10). We note that if $\varepsilon < (2^{k+\delta}-1)/2^{3r+k-1}$ (which is true if $\varepsilon < 2^{-3r}$ for any $\delta > 0$) then $I(V^{[r-k]})$ satisfies the claimed inequality. ∎

It turns out that the channels for individual bits converge to either perfect or fully noisy channels. If the channel for bit j is perfect then the channels for all bits $i, r \ge i > j$ are perfect. If the channel for bit i is noisy then the channels for all bits $j, 1 \le j < i$ are noisy. The total number of near-perfect bits approaches $I(W)$. This is made formal in the next proposition.

Proposition 4.3 *Let $\Omega_k = \{\omega : (Z_{1,\infty}, Z_{2,\infty}, \ldots, Z_{r,\infty}) = 1^k 0^{r-k}\}, k = 0, 1, \ldots, r$. For every $\omega \in \Omega_k$*

$$\lim_{n \to \infty} |I_n - I(W_n^{[r-k]})| = 0.$$

Proof: For every $\omega \in \Omega_k$ we have that $I_n(\omega) \to r-k$. Combining this with the previous lemma and Proposition 4.2(b), we conclude that for such ω also $I(W_n^{[r-k]}) \to r-k$. ∎

The concluding claim of this section describes the channel polarization and establishes that the total number of bits sent over almost noiseless channels approaches $NI(W)$.

Theorem 4.2 *For any DMC $W : \mathcal{X} \to \mathcal{Y}$ the channels $W_N^{(i)}$ polarize to one of the $r+1$ extremal configurations. Namely, let $V_i = W_N^{(i)}$ and*

$$\pi_{k,N} \triangleq \frac{|\{i \in [N] : |I(V_i) - k| < \delta \wedge |I(V_i^{[k]}) - k| < \delta\}|}{N},$$

where $\delta > 0$, *then* $\lim_{N\to\infty} \pi_{k,N} = P(I_\infty = k)$ *for all* $k = 0, 1, \ldots, r$. *Consequently as* $N \to \infty$,

$$\sum_{k=1}^{r} k\pi_{k,N} \to I(W).$$

This theorem follows directly from Theorem 4.1 and Propositions 4.2 and 4.3. Some examples of convergence to the extremal configurations described by this theorem are given later.

4.5 Transmission with Polar Codes

Let us describe a scheme of transmitting over the channel W with polar codes. Take $\varepsilon > 0$ and choose a sufficiently large n. Assume that the length of the code is $N = 2^n$. Proposition 4.1 implies that set $[N]$, apart from a small subset, is partitioned into $r + 1$ subsets $\mathcal{A}_{k,n}$ such that for $j \in \mathcal{A}_{k,n}$ the vector $(Z_1(W_N^{(j)}), Z_2(W_N^{(j)}), \ldots, Z_r(W_N^{(j)})) \in \mathcal{R}_k(\varepsilon)$. Each $j \in \mathcal{A}_{k,n}$ refers to an r-bit symbol in which $r - k$ rightmost bits correspond to small values of $Z_i(W_N^{(j)})$. To transmit data over the channel, we write the data bits in these coordinates and encode them using the linear transformation G_N.

More specifically, let us order the coordinates $j \in [N]$ by the increase of the quantity $\sum_{i=1}^{r} 2^{i-1} Z_i(W_N^{(j)})$ and use these numbers to locate the subsets $\mathcal{A}_{k,n}$. We transmit data by encoding messages $u_1^N = (u_1, \ldots, u_N)$ in which if $j \in \mathcal{A}_{k,n}, k = 0, \ldots, r-1$ then the symbol u_j is taken from the subset of symbols of $\mathcal{X}$ with the first k symbols fixed and known to both the encoder and the decoder ([3] calls them frozen bits). In particular, the subset $\mathcal{A}_{r,n}$ is not used to transmit data. A polar codeword is computed as $x_1^N = u_1^N G_N$ and sent over the channel.

Decoding is performed using the "successive cancellation" procedure of [3] with the obvious constraints on the symbol values. Namely, for $j = 1, \ldots, N$ put

$$\hat{u}_j = \begin{cases} u_j, & j \in \mathcal{A}_{r,n} \\ \arg\max_x W_N^{(j)}(y_1^N, \hat{u}_1^{j-1}|x), & j \in \cup_{k\le r-1}\mathcal{A}_{k,n} \end{cases}$$

where if $j \in \mathcal{A}_{k,n}, k = 0, 1, \ldots, r-1$, then the maximum is computed over the symbols $x \in \mathcal{X}$ with the fixed (known) values of the first k bits.

The error probability of this decoding is estimated in Sect. 4.7.

4.6 Proof of Channel Polarization

Part (a) of Theorem 4.1 follows straightforwardly from [3, 59]. Namely, as shown in [3, Prop. 4], $I(W^+) + I(W^-) = 2I(W)$. We note that the proof in [3] uses only the fact that u_1, u_2 are recoverable from x_1, x_2 which is true in our case. Hence the sequence $I_n, n \ge 1$ forms a bounded martingale. By Doob's theorem [38, p.196], it converges a.s. in $L^1(\Omega, \mathcal{F}, P)$ to a random variable I_∞ with $E(I_\infty) = I(W)$.

To prove part (b) we show that each of the $Z_{i,n}$'s converges a.s. to a $(0, 1)$ Bernoulli random variable $Z_{i,\infty}$. This convergence occurs in a concerted way in that the limit r.v.'s satisfy the property that $Z_{i,\infty} = 1$ implies $Z_{j,\infty} = 1$ if $j < i$. This is shown by observing that for any fixed $i = 1, \ldots, r$ and for all $v \in \mathcal{X}_i$, the $Z_{v,n}(W)$ converge to identical copies of a Bernoulli random variable.

4.6.1 Convergence of $Z_{v,n}, v \in \mathcal{X}$

In this section, we shall prove that the Bhattacharyya parameters $Z_{v,n}$ converge almost surely to Bernoulli random variables. The proof forms the main technical result of this chapter and is accomplished in several steps.

Lemma 4.4 *Let*

$$Z_{\max}^{(i)}(W) \triangleq \max_{v \in \mathcal{X}_i} Z_v(W), \quad i = 1, \ldots, r.$$

Then for the channel W^+ we have

$$Z_{\max}^{(r-j)}(W^+) = Z_{\max}^{(r-j)}(W)^2, \quad j = 0, \ldots, r-1. \tag{4.12}$$

For the channel W^- we have

$$Z_{\max}^{(r)}(W) \le Z_{\max}^{(r)}(W^-) \le q Z_{\max}^{(r)}(W) \tag{4.13}$$

and generally

$$Z_{\max}^{(r-j)}(W) \le Z_{\max}^{(r-j)}(W^-) \le \sum_{s=0}^{j-1} \frac{q}{2^{s+1}} Z_{\max}^{(r-s)}(W) + \frac{q}{2^j} Z_{\max}^{(r-j)}(W), \tag{4.14}$$
$$j = 1, \ldots, r-1.$$

Proof: In [59] it is shown that for all $v \in \mathcal{X} \backslash \{0\}$

$$Z_v(W^+) = Z_v(W)^2 \tag{4.15}$$

$$Z_v(W^-) \le 2Z_v(W) + \sum_{u \in \mathcal{X} \backslash \{0, -v\}} Z_u(W) Z_{v+u}(W). \tag{4.16}$$

The first of these two equations implies (4.12). To prove (4.13) take $v \in \mathcal{X}_r$. Then in the sum on the right-hand side of (4.16) we have that either $u \in \mathcal{X}_r$ or $u + v \in \mathcal{X}_r$, and

$$Z_v(W^-) \le 2Z_v(W) + (q-2) Z_{\max}^{(r)}(W),$$

implying the right-hand side inequality in (4.13).

Now take $v \in \mathcal{X}_{r-j}, j \ge 1$. The sum on u in (4.16) contains $q/2$ terms with $u \in \mathcal{X}_r$, $q/4$ terms with $u \in \mathcal{X}_{r-1}$, and so on, before reaching $\mathcal{X}_{r-j}$. Using (4.16), we obtain

$$\begin{aligned} Z_{\max}^{(r-j)}(W^-) \le 2Z_v(W) &+ \sum_{u \in \cup_{s=0}^{j-1} \mathcal{X}_{r-s}} Z_u(W) Z_{v+u}(W) \\ &+ \sum_{u \in \mathcal{X}_{r-j} \backslash \{-v\}} Z_u(W) Z_{v+u}(W) \\ &+ \sum_{u \in \cup_{s=j+1}^{r-1} \mathcal{X}_{r-s}} Z_u(W) Z_{v+u}(W) \end{aligned}$$

Now observe that $|\mathcal{X}_{r-s}| = q/2^{s+1}$. We obtain

$$Z_{\max}^{(r-j)}(W^-) \le 2Z_{\max}^{(r-j)}(W) + \sum_{s=0}^{j-1} \frac{q}{2^{s+1}} Z_{\max}^{(r-s)}(W) + 2\Big(\frac{q}{2^{j+1}} Z_{\max}^{(r-j)}(W) - 1\Big).$$

This implies the right-hand side inequality in (4.14).

For the lower bounds in (4.13)-(4.14), suppose that the largest values of $Z_v(W^-)$ and of $Z_v(W)$ for $v \in \mathcal{X}_i$ and some $i, 1 \le i \le r$ are attained for v_1 and v_2, respectively. Suppose that $v_1 = v_2$. Note that $Z(W^-_{\{x,x'\}}) \ge Z(W_{\{x,x'\}})$, which follows from the concavity of $Z(W)$ in W [3, 59]. Therefore also $Z_v(W^-) \ge Z_v(W)$ for all $v \ne 0$. At the same time, if $v_1 \ne v_2$, then

$$Z^{(i)}_{\max}(W^-) = Z_{v_1}(W^-) \ge Z_{v_2}(W^-) \ge Z_{v_2}(W) = Z^{(i)}_{\max}(W).$$

■

In particular, take $j = 0$. Relations (4.12), (4.13) imply that

$$Z^{(r)}_{\max,n+1} = (Z^{(r)}_{\max,n})^2 \text{ if } B_{n+1} = + \tag{4.17}$$

$$Z^{(r)}_{\max,n+1} \le qZ^{(r)}_{\max,n} \text{ if } B_{n+1} = -. \tag{4.18}$$

Iterated random maps of this kind were studied in [21] which contains general results on their convergence and stationary distributions. We need more detailed information about this process, and established in the following lemma.

Lemma 4.5 *Let $U_n, n \ge 0$ be a sequence of random variables adapted to a filtration $\mathcal{F}_n$ with the following properties:*
(i) $U_n \in [0, 1]$
(ii) $P(U_{n+1} = U_n^2|\mathcal{F}_n) \ge 1/2$
(iii) $U_{n+1} \le qU_n$ for some number $q \in \mathbb{Z}_+$.
Then there are events Ω_0, Ω_1 such that $P(\Omega_0 \cup \Omega_1) = 1$ and $U_n(\omega) \to a$ for $\omega \in \Omega_a, a = 0, 1$.

Proof: (a) First let us rescale the process U_n so that in the neighborhood of zero it has a drift to zero. Let $\beta \in (0, 1)$ be such that

$$q^\beta - 1 < 1/4.$$

Let $X_n = U_n^\beta$. Take $\tau(\omega)$ to be the first time when $X_n(\omega) \ge 1/2$. Let $Y_n = X_{\min(n,\tau)}$. On the event $Y_n \ge 1/2$ we have $Y_n = Y_{n+1}$ or

$$E(Y_{n+1} - Y_n|\mathcal{F}_n) = 0$$

while on the event $Y_n < 1/2$ we have

$$\begin{aligned} E(Y_{n+1} - Y_n|\mathcal{F}_n) &\le \frac{1}{2}(Y_n^2 - Y_n) + \frac{1}{2}(q^\beta Y_n - Y_n) \\ &\le -\frac{1}{8}Y_n \le 0. \end{aligned}$$

This implies that the sequence $Y_n, n \ge 0$ forms a supermartingale which is bounded between 0 and 1. By the convergence theorem, $Y_n \to Y_\infty$ a.s. and in $L^1(\Omega, \mathcal{F}, P)$, where Y_∞ is a random variable supported on $[0, 1]$. This implies that $EY_0 \ge EY_n \downarrow EY_\infty$. Further, if $X_0 \in [0, 1/4]$ then (since $EY_0 = EX_0$)

$$P(Y_\infty \ge 1/2) \le 2EY_0 \le 1/2. \tag{4.19}$$

(b) Now we shall prove that $P(Y_\infty \in (\delta, \frac{1}{2} - \delta)) = 0$ for any $\delta > 0$. From (ii) it follows that $P(X_{n+1} = X_n^2|\mathcal{F}_n) \ge 1/2$, which implies that

$$P(Y_{n+1} = Y_n^2|\mathcal{F}_n) \ge 1/2 \quad \text{on } Y_n < 1/2 \tag{4.20}$$

for all $n \geq 0$. Suppose that Y_∞ takes values in $(\delta, 1/2 - \delta)$ with probability $\alpha > 0$. Let $A_n = \{\omega : Y_n \in (\delta, 1/2 - \delta)\}$. Since $Y_n \to Y_\infty$ a.s., the Egorov theorem implies that there is a subset of probability arbitrarily close to $P(A_n)$ on which this convergence is uniform, and thus $P(A_n) \geq \alpha/2$ for all sufficiently large n. Therefore

$$\begin{aligned} P(|Y_{n+1} - Y_n| \geq \delta^2/2) &\geq P(Y_{n+1} = Y_n^2, Y_n \in (\delta, 1/2 - \delta)) \\ &\geq \frac{\alpha}{4}, \end{aligned}$$

the last step by (4.20). This however contradicts the almost sure convergence of Y_n.

(c) This implies that $P(Y_\infty < 1/2) = P(Y_n \to 0) = P(U_n \to 0)$. From (4.19)

$$P(U_n \to 0) \geq \frac{1}{2} \quad \text{provided that } U_0 \leq \left(\frac{1}{4}\right)^{\frac{1}{\beta}}. \tag{4.21}$$

Moreover, if $U_0 \leq (1/2)^{1/\beta}$ then either $Y_n \to 0$ or $Y_n \geq 1/2$ for some n. This translates to

$$P((U_n \to 0) \text{ or } (U_n \geq (1/2)^{1/\beta} \text{ for some } n)) = 1 \tag{4.22}$$

provided that $U_0 \leq (1/2)^{1/\beta}$.

(d) Let $\delta > 0$ be such that $q(\frac{1}{2})^{\frac{1}{\beta}} < 1 - \delta$ (depending on q this may require taking a sufficiently small β). Let $L := [0, (\frac{1}{4})^{\frac{1}{\beta}}]$ and $R := [1 - \delta, 1]$. Observe that the process U_n cannot move from L to R without visiting $C := ((\frac{1}{2})^{\frac{1}{\beta}}, 1 - \delta)$. Let σ_1 be the first time when $U_n \in C$, let η_1 be the first time after σ_1 when $U_n \in L \cup R$, let σ_2 be the first time after η_1 when $U_n \in C$, etc., $\sigma_1 < \eta_1 < \sigma_2 < \eta_2 < \dots$. We shall prove that every sample path of the process eventually stays outside C, i.e., that for almost all ω there exists $k = k(\omega) < \infty$ such that $\sigma_k(\omega) = \infty$.

Assume the contrary, i.e., $\lim_{k\to\infty} P(\sigma_k < \infty) = \alpha > 0$ (since $P(\sigma_{k+1} < \infty) < P(\sigma_k < \infty)$, this limit exists.) We have

$$\begin{aligned} P(\exists k : \sigma_k = \infty) &\geq \sum_{j=1}^{\infty} P(\sigma_j \neq \infty,\, U_{\eta_j} \in L,\, \sigma_{j+1} = \infty) \\ &\geq \alpha \sum_{j=1}^{\infty} P(U_{\eta_j} \in L,\, \sigma_{j+1} = \infty | \sigma_j \neq \infty). \end{aligned} \tag{4.23}$$

Consider the process $U'_n = U_{\sigma_k + n}$ on the event $\sigma_k < \infty$ (with the measure renormalized by $P(\sigma_k < \infty)$). This process has the same properties (i)-(iii) as U_n. Let $J = \lceil \log_2(\frac{1}{\beta} \log_{1-\delta} 1/4) \rceil$, then $x^{2^J} \in L$ for any $x \in C$. Therefore, $P(U'_J \in L) \geq 2^{-J}$ by property (ii). Now consider the process U'_{J+n} on the event $U'_J \in L$. This process has properties (i)-(iii), so we can use (4.21) to conclude that for

$$P(U_{\eta_k} \in L; \sigma_{k+1} = \infty | \sigma_k \neq \infty) \geq 2^{-(J+1)}$$

uniformly in k. But then the sum in (4.23) is equal to infinity, a contradiction.

(e) The proof is completed by showing that the probability of U_n staying in $R^c = [0, 1] \backslash R$ without converging to zero is zero. We know that almost all trajectories stay outside C, so suppose that the process starts in $(0, (1/2)^{1/\beta})$. Then the probability that it enters L in a finite number of steps is uniformly bounded from below (this is shown similarly to (4.23)), so the probability that it does not go to L is zero. Next assume that the process starts in L, then by (4.22) it either goes to zero or enters C with probability one. Together with part (d) this implies that the process that starts in L converges to zero or one with probability one. ∎

Lemma 4.6 *Let $V : \mathcal{X} \to \tilde{\mathcal{Y}}$ be a channel. Let $v, v' \in \mathcal{X}\backslash\{0\}$ be such that $wt_r(v) \geq wt_r(v')$. For any $\delta' > 0$ there exists $\delta > 0$ such that $Z_{v'}(V) \geq 1 - \delta'$ whenever $Z_v(V) \geq 1 - \delta$. In particular, we can take $\delta = \delta' q^{-3}$.*

Proof: If $\mathrm{wt}_r(v) = 1$ then $v = 10\ldots0$, so the statement is trivial. Let $Z_v(V) \geq 1 - \delta$, where $\mathrm{wt}_r(v) = i \geq 2$. Then for every pair $x, x' = x + v$ we have $Z(V_{\{x,x'\}}) \geq 1 - \varepsilon$, where $\varepsilon = q\delta$. Consider the unit-length vectors $z = (\sqrt{V(y|x)}, y \in \tilde{\mathcal{Y}}), z' = (\sqrt{V(y|x')}, y \in \tilde{\mathcal{Y}})$, and let $\theta(z, z')$ be the angle between them. We have $\cos(\theta(z, z')) = Z(V_{\{x,x'\}}) \geq 1 - \varepsilon$, and so $\|z - z'\|^2 = 2 - 2\cos(\theta(z, z')) \leq 2\varepsilon$.

Now take a pair of symbols $x_1, x_2 = x_1 + v'$ where $v' \in \mathcal{X}_s, s \leq i$. Since $\mathrm{wt}_r(v) \geq \mathrm{wt}_r(v')$, there exists a number $t \in \mathcal{X}_{r-i+s}$ such that $v' = tv$, where the multiplication is modulo q. Define $z_1 = (\sqrt{V(y|x_1)}, y \in \tilde{\mathcal{Y}})$ and $z_2 = (\sqrt{V(y|x_2)}, y \in \tilde{\mathcal{Y}})$. Let $w_j = (\sqrt{V(y|x_1 + jv)}, y \in \tilde{\mathcal{Y}}), j = 1, \ldots, t-1$. From the triangle inequality

$$\begin{aligned}\|z_1 - z_2\| &\leq \|z_1 - w_1\| + \|w_1 - w_2\| + \cdots + \|w_{t-1} - z_2\| \\ &\leq t\sqrt{2\varepsilon} \\ &\leq q\sqrt{2\varepsilon}.\end{aligned}$$

We obtain

$$\begin{aligned}Z(V_{\{x_1,x_2\}}) &= \cos(\theta(z_1, z_2)) = 1 - 1/2\|z_1 - z_2\|^2 \\ &\geq 1 - q^2\varepsilon \\ &= 1 - q^3\delta.\end{aligned}$$

Thus we obtain

$$Z_{v'}(V) = \frac{1}{q}\sum_x Z(V_{\{x,x+v'\}}) \geq 1 - q^3\delta.$$

■

Remark : We can prove the previous lemma in a different way by relating the Bhattacharyya distance to the ℓ_1-distance between $V(y|x_1)$ and $V(y|x_2)$ [54]. Then the estimate $\delta = \delta' q^{-3}$ can be improved to $\delta = \delta'(2q)^{-2}$.

Lemma 4.7 *For all $j = 1, \ldots, r$*

$$Z^{(j)}_{\max,n} \xrightarrow{a.s.} Z^{(j)}_{\max,\infty}.$$

where $Z^{(j)}_{\max,\infty}$ is a Bernoulli random variable supported on $\{0, 1\}$.

Proof: For a given channel V denote

$$Z^{[s,r]}_{\max}(V) = \max(Z^{(s)}_{\max}(V), Z^{(s+1)}_{\max}(V), \ldots, Z^{(r)}_{\max}(V)).$$

Eq. (4.15) gives us that

$$Z^{[r-j,r]}_{\max}(W^+) = (Z^{[r-j,r]}_{\max}(W))^2$$

and (4.14) implies that

$$Z^{[r-j,r]}_{\max}(W^-) \leq qZ^{[r-j,r]}_{\max}(W).$$

Hence by Lemma 4.5 the random variables $Z^{[r-j,r]}_{\max,\infty}$ are well-defined and are Bernoulli 0-1 valued a.s. for all $j = 0, 1, \ldots, r-1$.

We need to prove the same for $Z^{(r-j)}_{\max,\infty}$. The proof is by induction on j. We just established the needed claim for $Z^{(r)}_{\max,n}$. For ease of understanding let us show that this implies the convergence of $Z^{(r-1)}_{\max,n}$. Indeed, $Z^{[r-1,r]}_{\max,\infty}$ is a Bernoulli 0-1 valued random variable. But so is $Z^{(r)}_{\max,\infty}$, so the possibilities are

$$(Z^{[r-1,r]}_{\max,\infty}, Z^{(r)}_{\max,\infty}) = (1,1) \text{ or } (1,0) \text{ or } (0,0)$$

with probability one (note that $(0,1)$ is ruled out by the definition of $Z^{[r-1,r]}_{\max}$). If $Z^{(r)}_{\max,\infty} = 1$ then $Z^{(r-1)}_{\max,\infty} = 1$ by Lemma 4.6 (this statement holds trajectory-wise). If on the other hand, the case that is realized is $(1,0)$ then $Z^{(r-1)}_{\max,\infty} = 1$ by the definition of $Z^{[r-1,r]}_{\max}$. Finally in the case $(0,0)$ we clearly have that $Z^{(r-1)}_{\max,\infty} = 0$, both holding trajectory-wise.

The general induction step is almost exactly the same. Assume that we have proved the required convergence for $Z^{(r-i)}_{\max}, i = 0, 1, \ldots, j-1$. Assume that $Z^{[r-j,r]}_{\max,\infty} = 0$, then $Z^{(r-j)}_{\max} = 0$. If on the other hand, $Z^{[r-j,r]}_{\max,\infty} = 1$ then either one of $Z^{(r-i)}_{\max,\infty}, i < j$ equals one, and then $Z^{(r-j)}_{\max,\infty} = 1$ by Lemma 4.6, or $Z^{(r-i)}_{\max,\infty} = 0$ for all $i < j$, and then $Z^{(r-j)}_{\max,\infty} = 1$ by definition of $Z^{[r-j,r]}_{\max,\infty}$. ■

Now we are in a position to complete the proof of convergence.

Lemma 4.8 *$Z_{v,n} \to Z_{v,\infty}$ a.s., where $Z_{v,\infty}$ is a $(0,1)$-valued random variable whose distribution depends only on the ordered weight $\mathrm{wt}_r(v)$.*

Proof: Let $\Omega^{(i)}_a = \{\omega : Z^{(i)}_{\max,n} \to a\}$, where $a = 0, 1$ and $i = 1, \ldots, r$, where some of the events may be empty. For every $\omega \in \Omega^{(i)}_1, i = 1, \ldots, r$ we have that for any $\delta > 0$, starting with some n_0, the quantity $Z^{(i)}_{\max,n} \geq 1 - \delta$. Thus, for $n \geq n_0$ there exists $v \in \mathcal{X}_i$, possibly depending on n, such that $Z_{v,n}(\omega) \geq 1 - \delta$. Then Lemma 4.6 implies that $Z_{v',n}(\omega) \geq 1 - q^3\delta$ for all $v' \in \mathcal{X}_i$, so $Z_{v,n}(\omega) \to 1$. At the same time, if $\omega \in \Omega^{(i)}_0$ then $Z_{v,n}(\omega) \to 0$ for all $v \in \mathcal{X}_i$. ■

4.6.2 Proof of Part (b) of Theorem 4.1

Lemma 4.9 *For any $i = 1, \ldots, r$, the random variable $Z_{i,n}$ converges a.s. to a $(0,1)$-valued random variable $Z_{i,\infty}$. Moreover, $Z_{i,\infty} = 1$ implies that $Z_{i-1,\infty} = 1$.*

Proof: The first part follows because all the $Z_v, v \in \mathcal{X}_i$ converge to identical copies of the same random variable. Formally, Lemma 4.8 asserts that $Z_{v,n} \to a$ for every $v \in \mathcal{X}_i$ and every $\omega \in \Omega^{(i)}_a, a = 0, 1$. Hence taking the limit $n \to \infty$ in (4.7) we see that $Z_{i,n} \to a$ on $\Omega^{(i)}_a$ where $P(\Omega^{(i)}_0 \cup \Omega^{(i)}_1) = 1$.

Let us prove the second part. Suppose that $Z_{i,n} \geq 1 - \varepsilon$, then using (4.7) we see that $Z_{v',n} \geq 1 - 2^{i-1}\varepsilon$ for all $v' \in \mathcal{X}_i$. Lemma 4.6 implies that $Z_{v,n} \geq 1 - 2^{3r+i-1}\varepsilon$ for any $v \in \mathcal{X}$, $\mathrm{wt}_r(v) = i-1$, and therefore $Z_{i-1,n} \geq 1 - 2^{3r+i-1}\varepsilon$. Thus $Z_{i,n}(\omega) \to 1$ implies $Z_{i-1,n}(\omega) \to 1$ for all $\omega \in \Omega^{(i)}_1$ and all i. Taking the limit, we obtain the second claim of the lemma. ■

We obtain that $Z_{i,\infty}$ is a $(0,1)$ random variable a.s. and for all i, and if $Z_{i,\infty} = 1$ then $Z_{j,\infty} = 1$ for all $1 \leq j < i$. Consider the events $\Psi^{(i)}_a = \{\omega : Z_{i,\infty} = a\}, a = 0, 1; i = 1, \ldots, r$. We have

$$\Psi^{(1)}_1 \supset \Psi^{(2)}_1 \supset \cdots \supset \Psi^{(r)}_1$$
$$\Psi^{(1)}_0 \subset \Psi^{(2)}_0 \subset \cdots \subset \Psi^{(r)}_0.$$

We need to prove that with probability one, the vector $(Z_{i,\infty}, i = 1, \ldots, r)$ takes one of the values (4.9). With probability one, $Z_{r,\infty} = 1$ or 0. If it is equal to 1 then necessarily $Z_{r-1,\infty} = \cdots = Z_{1,\infty} = 1$. Otherwise, $Z_{r,\infty} = 0$. In this case it is possible that $Z_{r-1,\infty} = 1$ (in which case $Z_{r-2,\infty} = \cdots = Z_{1,\infty} = 1$) or $Z_{r-1,\infty} = 0$. Of course $P(\Psi_0^{(r-1)} \cup \Psi_1^{(r-1)}) = 1$, so in particular

$$P(\Psi_0^{(r)} \backslash (\Psi_0^{(r-1)} \cup (\Psi_1^{(r-1)} \backslash \Psi_1^{(r)}))) = 0.$$

If $Z_{r-1,\infty} = 0$ then the possibilities are $Z_{r-2,\infty} = 1$ or 0, up to another event of probability 0, and so on. Thus, the union of the disjoint events given by (4.9) holds with probability one. Theorem 4.1 is proved. ■

4.6.3 The Case of Finite Code Length

The proof is analogous to the argument in the previous paragraph. The random variable $Z_{r,n} \to Z_{r,\infty}$ a.s. . By the Egorov theorem, for any $\gamma > 0$ there are disjoint subsets $\widetilde{\Psi}_0^{(r)} \subset \Psi_0^{(r)}, \widetilde{\Psi}_1^{(r)} \subset \Psi_1^{(r)}$ with $P(\widetilde{\Psi}_0^{(r)} \cup \widetilde{\Psi}_1^{(r)}) \geq 1 - \gamma$ on which this convergence is uniform. Take $n_1^{(r)}$ such that $Z_{r,n} > 1 - \varepsilon/2^{4r-1}$ for every $\omega \in \widetilde{\Psi}_1^{(r)}$ and $n \geq n_1^{(r)}$. By Lemma 4.6 and (4.7) for every such ω we have $Z_{i,n} \geq 1 - \varepsilon$ for all $i = 1, \ldots, r-1$; $n \geq n_1^{(r)}$. This gives rise to the event $B_{r,n}$. Otherwise, let $n_0^{(r)}$ be such that $\sup_\omega Z_{r,n} < \varepsilon$ for $\omega \in \widetilde{\Psi}_0^{(r)}$ and $n \geq n_0^{(r)}$. Consider the events $\widetilde{\Psi}_0^{(r-1)} \subset \Psi_0^{(r-1)}, \widetilde{\Psi}_1^{(r-1)} \subset \Psi_1^{(r-1)}$ with $P(\widetilde{\Psi}_0^{(r-1)} \cup \widetilde{\Psi}_1^{(r-1)}) \geq 1 - \gamma$ on which $Z_{r-1,n} \to Z_{r-1,\infty}$ uniformly. Choose $n_1^{(r-1)}$ such that $Z_{r-1,n} > 1 - \varepsilon/2^{4r-2}$ for all $n \geq n_1^{(r-1)}$ and all $\omega \in \widetilde{\Psi}_1^{(r-1)}$. For every such ω we have $Z_{i,n} \geq 1 - \varepsilon$ for all $i = 1, \ldots, r-2$; $n \geq n_1^{(r-1)}$. Next,

$$P(\widetilde{\Psi}_0^{(r)} \backslash (\widetilde{\Psi}_0^{(r-1)} \cup (\widetilde{\Psi}_1^{(r-1)} \backslash \widetilde{\Psi}_1^{(r)}))) \leq 2\gamma.$$

We continue in this manner until we construct all the $r + 1$ events $B_{k,n}$. For this, n should be taken sufficiently large, $n \geq \max_k \max(n_0^{(k)}, n_1^{(k)})$. By taking $\gamma = \delta/r$ we can ensure that $P(\cup_k B_{k,n}) \geq 1 - \delta$. This concludes the proof. ■

Remark : For binary-input channels, the transmitted bits in the limit are transmitted either perfectly or carry no information about the message. Şaşoğlu et al. [59] observed that q-ary codes constructed using Arıkan's kernel H_2 share this property for transmitted symbols only if q is prime. Otherwise, Şaşoğlu et al. [59] note that the symbols can polarize to states that carry partial information about the transmission. In particular, they give an example of a quaternary-input channel $W : \{0, 1, 2, 3\} \to \{0, 1\}$ with $W(0|0) = W(0|2) = W(1|1) = W(1|3) = 1$. This channel has capacity 1 bit. Computing the channels W^+ and W^- we find that they are equivalent to the original channel W. The conclusion reached in [59] is that there are nonbinary channels that do not polarize under the action of H_2.

We observe that the above channel corresponds to the extremal configuration 10 in (4.9) (the other two configurations arise with probability 0), and therefore has to be, and is, a stable point of the channel combining operation. It is possible to reach capacity by transmitting the least significant bit of every symbol.

The paper [59] went on to show that for every $n \geq 1$ there exists a permutation $\pi_n : \mathcal{X} \to \mathcal{X}$ such that the kernels $H_2(n) : (u, v) \to (u + v, \pi_n(v))$ lead to channels that polarize to perfect or fully noisy. While the result of [59] holds for any q, in the case of $q = 2^r$ this means that configurations $00 \ldots 0$ and $11 \ldots 1$ arise with probability $I(W)$ and $1 - I(W)$ respectively, while all the other configurations have probability zero.

4.7 Rate of Polarization and Error Probability of Decoding

The following theorem, due to Arıkan and Telatar [4], is useful in quantifying the rate of convergence of the channels W_n to one of the extremal configurations (4.9).

Theorem 4.3 *[4] Suppose that a random process $U_n, n \geq 0$ satisfies the conditions (i)-(iii) of Lemma 4.5 and that (iv), U_n converges a.s. to a $\{0,1\}$-valued random variable U_∞ with $P(U_\infty = 0) = p$. Then for any $\alpha \in (0, 1/2)$*

$$\lim_{n\to\infty} P(U_n < 2^{-N^\alpha}) = p. \tag{4.24}$$

If condition (iii) is replaced with (iii′) $U_n \leq U_{n+1}$ and $U_0 > 0$, then for any $\alpha > 1/2$,

$$\lim_{n\to\infty} P(U_n < 2^{-N^\alpha}) = 0.$$

Note that, as a consequence of Lemma 4.5, assumption (iv) in this theorem is superfluous in that it follows from (i)-(iii).

Processes $Z^{(r)}_{\max,n}$ and $Z^{[r-j,r]}_{\max,n}, j = 0, \ldots, r-1$ satisfy conditions (i)-(iii) of Lemma 4.5. Hence the above theorem gives the rate of convergence of each of them to zero. We argue that the convergence rate of $Z^{(r-j)}_{\max,n}, j \geq 1$ to zero is also governed by Theorem 4.3. Indeed, let $\Omega^{[r-j,r]}_a = \{\omega : Z^{[r-j,r]}_{\max,n} \to a\}, \Omega^{(r-j)}_a = \{\omega : Z^{(r-j)}_{\max,n} \to a\}, a = 0, 1$. Then

$$\Omega^{(r-j)}_0 \supseteq \Omega^{[r-j,r]}_0 \text{ and } \Omega^{(r-j)}_1 = \Omega^{[r-j,r]}_1 \tag{4.25}$$

the last equality because by Lemma 4.6, $Z^{[r-j,r]}_{\max,n} \to 1$ implies $Z^{(r-j)}_{\max,n} \to 1$ on every trajectory. As a consequence of (4.25) we have that $P(\Omega^{(r-j)}_0 \backslash \Omega^{[r-j,r]}_0) = 0$. Hence $P(Z^{(r-j)}_{\max,\infty} = 0) = P(Z^{[r-j,r]}_{\max,\infty} = 0)$. Denote this common value by p_j. The random variable $Z^{[r-j,r]}_{\max,n}$ satisfies a condition of the form (4.24) with $p = p_j$. We obtain that for any $\alpha \in (0, 1/2)$

$$\lim_{n\to\infty} P(Z^{(r-j)}_{\max,n} < 2^{-N^\alpha}) = \lim_{n\to\infty} P(Z^{[r-j,r]}_{\max,n} < 2^{-N^\alpha}) = p_j.$$

Of course if $Z^{(r-j)}_{\max,n}$ is small then so is every $Z_{v,n}$ for $v \in \mathcal{X}_{r-j}$. We conclude as follows.

Proposition 4.4 *For any $\alpha \in (0, 1/2)$ and any $v \in \mathcal{X}_j, j = 1, 2, \ldots, r$*

$$\lim_{n\to\infty} P(Z_{v,n} < 2^{-N^\alpha}) = p_j.$$

This result enables us to estimate the probability of decoding error under successive cancellation decoding. To do this, we extend the argument of [3] to nonbinary alphabets.

The following statement follows directly from the previously established results, notably Proposition 4.2.

Theorem 4.4 *Let $0 < \alpha < 1/2$. For any DMC $W : \mathcal{X} \to \mathcal{Y}$ with $I(W) > 0$ and any $R < I(W)$ there exists a sequence of r-tuples of disjoint subsets $\mathcal{A}_{0,N}, \ldots, \mathcal{A}_{r-1,N}$ of $[N]$ such that $\sum_k |\mathcal{A}_{k,N}|(r-k) \geq NR$ and $Z_v(W^{(i)}_N) < 2^{-N^\alpha}$ for all $i \in \mathcal{A}_{k,N}$, all $v \in \bigcup_{l=k+1}^r \mathcal{X}_l$, and all $k = 0, 1, \ldots, r-1$.*

Let

$$\mathcal{E} \triangleq \{(u_1^N, y_1^N) \in \mathcal{X}^N \times \mathcal{Y}^N : \hat{u}_1^N \neq u_1^N\}$$
$$\mathcal{B}_i \triangleq \{(u_1^N, y_1^N) \in \mathcal{X}^N \times \mathcal{Y}^N : \hat{u}_1^{i-1} = u_1^{i-1}, \hat{u}_i \neq u_i\}.$$

Then the block error probability of decoding is defined as

$$P_e = P(\mathcal{E}) = P\Big(\bigcup_{i \in \mathcal{A}_{0,N} \cup \cdots \cup \mathcal{A}_{r-1,N}} \mathcal{B}_i \Big).$$

The next theorem is the main result of this section.

Theorem 4.5 *Let $0 < \alpha < 1/2$ and let $0 < R < I(W)$, where $W : \mathcal{X} \to \mathcal{Y}$ is a DMC. The error probability of block error under successive cancellation decoding at block length $N = 2^n$ and rate R satisfies*

$$P_e(N, R) = O(2^{-N^\alpha}).$$

As a consequence, for every n, there exists an assignment of values of frozen bits such that the error probability $P_e = O(2^{-N^\alpha})$.

Proof: Let

$$\begin{aligned} \mathcal{E}_{i,v} \triangleq \{(u_1^N, y_1^N) \in \mathcal{X}^N \times \mathcal{Y}^N : \\ W_N^{(i)}(y_1^N, u_1^{i-1} | u_i) \le W_N^{(i)}(y_1^N, u_1^{i-1} | u_i + v)\}. \end{aligned}$$

For a fixed value of $a_1^k = (a_1, a_2, \ldots, a_k) \in \{0,1\}^k$ let us define $\mathcal{X}(a_1^k) = \{x \in \mathcal{X} : x_1^k = a_1^k\}$. Notice that the decoder finds $\hat{u}_i$, $i \in \mathcal{A}_{k,N}$ by taking the maximum over the symbols $x \in \mathcal{X}(a_1^k)$. Then we obtain

$$\mathcal{B}_i \subseteq \bigcup_{v \in \mathcal{X}(a_1^k)} \mathcal{E}_{i,v}.$$

Using (4.6), we obtain

$$\begin{aligned} P(\mathcal{B}_i) &\le \sum_{v \in \mathcal{X}(a_1^k)} P(\mathcal{E}_{i,v}) \\ &= \sum_{v \in \mathcal{X}(a_1^k)} \sum_{u_1^N, y_1^N} \frac{1}{q^N} W_N(y_1^N | u_1^N) 1_{\mathcal{E}_{i,v}}(u_1^N, y_1^N) \\ &\le \sum_{v \in \mathcal{X}(a_1^k)} \sum_{u_1^N, y_1^N} \frac{1}{q^N} W_N(y_1^N | u_1^N) \sqrt{\frac{W_N^{(i)}(y_1^N, u_1^{i-1} | u_i + v)}{W_N^{(i)}(y_1^N, u_1^{i-1} | u_i)}} \\ &= \sum_{v \in \mathcal{X}(a_1^k)} \sum_{u_i} \frac{1}{q} Z(W^{(i)}_{N,\{u_i, u_i+v\}}) \\ &= \sum_{v \in \mathcal{X}(a_1^k)} Z_v(W_N^{(i)}). \end{aligned}$$

Thus the decoding error is bounded by

$$P(\mathcal{E}) \le \sum_{i \in \mathcal{A}_{0,N} \cup \cdots \cup \mathcal{A}_{r-1,N}} \sum_{v \in \mathcal{X}(a_1^k)} Z_v(W_N^{(i)}).$$

By Theorem 4.4, for any $R < I(W)$ there exists a sequence of r-tuples of disjoint subsets $\mathcal{A}_{0,N}, \ldots, \mathcal{A}_{r-1,N}$ with $\sum_k |\mathcal{A}_{k,N}|(r-k) \ge NR$ such that

$$\sum_{i \in \mathcal{A}_{0,N} \cup \cdots \cup \mathcal{A}_{r-1,N}} \sum_{v \in \mathcal{X}(a_1^k)} Z_v(W_N^{(i)}) \le qN2^{-N^\alpha}$$

and thus we obtain that $P(\mathcal{E}) = O(2^{-N^\alpha})$. ∎

4.8 Symmetric Channels

So far we have proved that polar codes achieve the symmetric capacity of any DMC. The proof is based on the fact that the input sequence u_1^N is uniformly distributed over $\{0, 1, \ldots, q-1\}^N$. However, when encoding codewords, we fix the values of the frozen bits and therefore the vector u_1^N is no longer uniformly distributed. In this section, we prove that if the channel is symmetric, the probability of decoding error does not depend on the values of the frozen bits. We give a brief introduction to the binary case.

Let $W : \mathcal{X} \to \mathcal{Y}$ be a symmetric binary DMC where $\mathcal{X} = \{0, 1\}$. Then by Proposition 12 and 13 in [3], the channels $W^N(y_1^N|x_1^N)$, $W_N(y_1^N|u_1^N)$, and $W_N^{(i)}(y_1^N, u_1^{i-1}|u_i)$, $i = 1, \ldots, N$ are symmetric. This proves the symmetry property of error events $\mathcal{E}_i = \{(u_1^N, y_1^N) \in \mathcal{X}^N \times \mathcal{Y}^N : W_N^{(i)}(y_1^N, u_1^{i-1}|u_i) \leq W_N^{(i)}(y_1^N, u_1^{i-1}|u_i \oplus 1)\}$ and thus the events $\mathcal{E}_i$ are independent of the input u_1^N.

Similarly to the above argument, it is possible to show that the choice of values of frozen bits does not matter if the q-ary channel W is symmetric.

Theorem 4.6 *In addition to the assumptions of Theorem 4.5, assume that W is symmetric. Then for any assignment of values of the frozen bits, the error probability of decoding satisfies $P_e(N, R) = O(2^{-N^\alpha})$.*

Let $W : \mathcal{X} \to \mathcal{Y}, |\mathcal{X}| = q = 2^r$ be a symmetric DMC. By definition of the symmetric channel, there exists a permutation $\rho_{x,x'}$ on $\mathcal{Y}$ such that $W(y|x) = W(\rho_{x,x'}(y)|x')$ for all $x, x' \in \mathcal{X}, x \neq x'$ and $y \in \mathcal{Y}$. For brevity, let us denote $\prod_{i=1}^N \rho_{x_i,x_i'}(y_i)$ by $\rho_{x_1^N,{x'}_1^N}(y_1^N)$, where $x_i, x_i' \in \mathcal{X}$ for all i.

The proof of the following statement follows [3, Prop. 12,13].

Proposition 4.5 *Let W be a symmetric DMC. Let $x_1^N, b_1^N \in \mathcal{X}^N$ and $y_1^N \in \mathcal{Y}^N$. The channel W^N is also symmetric in the sense that*

$$W^N(y_1^N|x_1^N) = W^N(\rho_{x_1^N, x_1^N + b_1^N}(y_1^N)|x_1^N + b_1^N)$$

where $+$ is symbol-wise modulo-q addition.

Let $u_1^N, a_1^N \in \mathcal{X}^N$ and let $x_1^N = u_1^N G_N$, and $b_1^N = a_1^N G_N$. The channels W_N and $W_N^{(i)}$ for all $1 \leq i \leq N$ are symmetric in the sense that

$$\begin{aligned} W_N(y_1^N|u_1^N) &= W_N(\rho_{x_1^N, x_1^N + b_1^N}(y_1^N)|u_1^N + a_1^N), \\ W_N^{(i)}(y_1^N, u_1^{i-1}|u_i) &= W_N^{(i)}(\rho_{x_1^N, x_1^N + b_1^N}(y_1^N), u_1^{i-1} + a_1^{i-1}|u_i + a_i) \end{aligned}$$

Proof: The first claim of this proposition is obvious. From this claim, we have $W_N(y_1^N|u_1^N) = W^N(y_1^N|x_1^N) = W^N(\rho_{x_1^N, x_1^N + b_1^N}(y_1^N)|x_1^N + b_1^N) = W_N(\rho_{x_1^N, x_1^N + b_1^N}(y_1^N)|u_1^N + a_1^N)$. To prove the last statement, let us consider

$$\begin{aligned} W_N^{(i)}(y_1^N, u_1^{i-1}|u_i) &= \frac{1}{q^{N-1}} \sum_{u_{i+1}^N} W_N(y_1^N|u_1^N) \\ &= \frac{1}{q^{N-1}} \sum_{u_{i+1}^N} W_N(\rho_{x_1^N, x_1^N + b_1^N}(y_1^N)|u_1^N + a_1^N) \\ &= W_N^{(i)}(\rho_{x_1^N, x_1^N + b_1^N}(y_1^N), u_1^{i-1} + a_1^{i-1}|u_i + a_i) \end{aligned}$$

where the last equality holds because the sum over u_{i+1}^N is equivalent to the sum over $u_{i+1}^N + a_{i+1}^N$ for any fixed a_1^N. ■

Using this proposition, we now prove Theorem 4.6. First of all, from the symmetry of a channel $W_N^{(i)}$, error event, $\mathcal{E}_{i,v}$ defined in the proof of Theorem 4.5 has the following property: for any $1 \leq i \leq N$, $v \in \mathcal{X}$, and all $u_1^N, a_1^N \in \mathcal{X}^N$, $y_1^N \in \mathcal{Y}^N$, a pair of vectors of symbols, $(u_1^N, y_1^N) \in \mathcal{E}_{i,v}$ if and only if $(u_1^N + a_1^N, \rho_{x_1^N,(x_1^N+b_1^N)}(y_1^N)) \in \mathcal{E}_{i,v}$ where $x_1^N = u_1^N G_N$ and $b_1^N = a_1^N G_N$. Then,

$$\begin{aligned} P(\mathcal{E}_{i,v}|\{U_1^N = u_1^N\}) &= \sum_{y_1^N} W_N(y_1^N|u_1^N) 1_{\mathcal{E}_{i,v}}(u_1^N, y_1^N) \\ &= \sum_{y_1^N} W_N(\rho_{x_1^N,0_1^N}(y_1^N)|0_1^N) 1_{\mathcal{E}_{i,v}}(0, \rho_{x_1^N,0_1^N}(y_1^N)) \\ &= P(\mathcal{E}_{i,v}|\{U_1^N = 0_1^N\}) \end{aligned}$$

where the second equality follows from Proposition 4.5 and the symmetry property of error events and the last equality is due to the fact that sum over y_1^N is equivalent with the sum over $\rho_{x_1^N,0_1^N}(y_1^N)$ for any fixed $x_1^N \in \mathcal{X}^N$. This proves that error events $\mathcal{E}_{i,v}$ are independent of the vector of input symbols.

Now, for any symmetric DMC W and a code with every possible frozen bit assignment, we have

$$P_e = \sum_u \frac{1}{q^K} P(\mathcal{E}|\{U_1^N = u_1^N\}) \leq \sum_{i \in \mathcal{A}_{0,N} \cup \cdots \cup \mathcal{A}_{r-1,N}} \sum_{v \in \mathcal{X}(a_1^k)} Z_v(W_N^{(i)})$$

which is independent of the values of the frozen parts. Following the proof of Theorem 4.5 we can prove the Theorem 4.6.

4.9 Polarization of Ordered Channels

To compute a few examples, we confine ourselves to the case of erasure-like channels. Similarly to the binary case [3], in this case there are exact relationships between the quantities $Z_i(W)$ and $Z_i(W^{\pm})$ for all i, which makes the recursive calculations easy. Consider the OEC introduced in Chapter 3.

Define the channels for individual bits of the transmission:

$$V^{(i)}(v|u) \triangleq \frac{2}{q} \sum_{x \in \mathcal{X}: x_i = u} \sum_{y \in \mathcal{Y}: y_i = v} W(y|x).$$

The following properties of the channel are verified by direct calculations: for all $i = 1, 2, \ldots, r$,

$$\begin{aligned} &V^{(i)}(1|1) = V^{(i)}(0|0) = \varepsilon_0 + \varepsilon_1 + \cdots + \varepsilon_{i-1} \\ &V^{(i)}(?|0) = V^{(i)}(?|1) = \varepsilon_i + \cdots + \varepsilon_r \\ &Z_i(W) = Z(V^{(i)}) = \varepsilon_i + \cdots + \varepsilon_r \\ &Z_i(W^+) = Z((V^{(i)})^+) = Z_i(W)^2 \\ &Z_i(W^-) = Z((V^{(i)})^-) = 2Z(V^{(i)}) - Z(V^{(i)})^2 \\ &I(W) = \sum_{i=1}^r I(V^{(i)}) = r - \sum_{i=1}^r Z_i(W). \end{aligned}$$

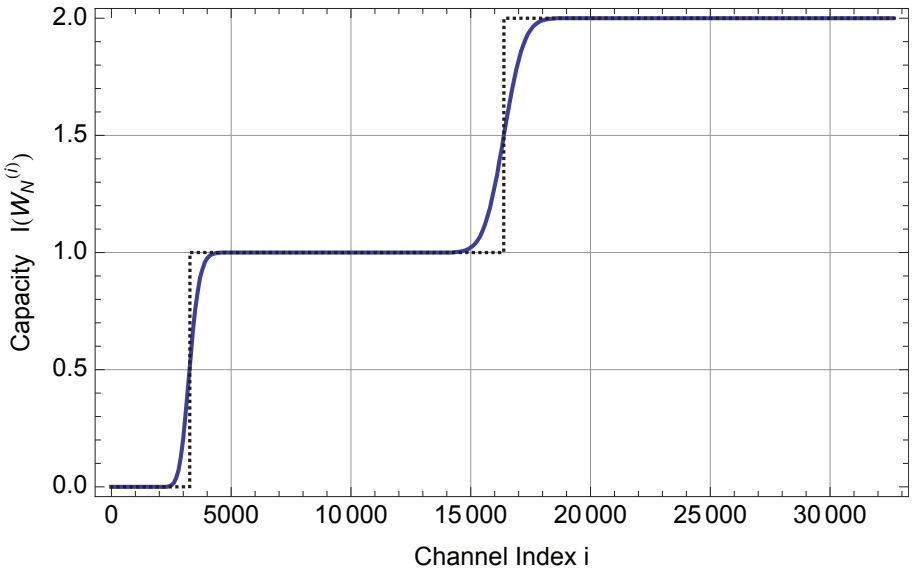

Figure 4.2: 3-level polarization on the OEC $W : \mathcal{X} \to \mathcal{Y}, \mathcal{X} = \{00, 01, 10, 11\}$ with transition probabilities $\varepsilon_0 := W(x_1x_2|x_1x_2) = 0.5, \varepsilon_1 := W(?x_2|x_1x_2) = 0.4, \varepsilon_2 := W(??|x_1, x_2) = 0.1$, for all $x_1, x_2 \in \{0, 1\}$. The channels are sorted by the increase of the capacity $I(W_N^{(i)})$, $N = 2^{15}$.

The capacity of the channel W is attained by sending r independent streams of data encoded for the binary erasure channels $V^{(i)}$ Therefore, sending r independent polar codewords over the r bit channels, one can approach the capacity of the channel.

Despite the fact that this example is trivial, it already shows the domination pattern observed in Theorem 4.1. Namely, it is easy to prove directly that $Z_{j,\infty} \geq Z_{i,\infty}$ for all $i > j$. Indeed, both the functions $x \mapsto x^2$ and $x \mapsto 2x - x^2$ are monotone increasing on $(0, 1)$. Since $Z_j(W) \geq Z_i(W)$, the relation $Z_{j,n} \geq Z_{i,n}$ is preserved on every trajectory of the random walk. This implies the claim of Lemma 4.9. For that, it suffices to observe that the erasure in higher-numbered bits implies that all the lower-numbered bits are erased with probability 1. We include two examples. In Fig. 4.2, $r = 2$, and $\varepsilon_0 = 0.5, \varepsilon_1 = 0.4, \varepsilon_2 = 0.1$. In Fig. 4.3, $r = 9$ and $\varepsilon_i = 0.1, i = 0, 1, \ldots, 9$. Note that the proportion of the channels with capacity $i = 0, 1, \ldots, r$ bits converges to ε_{r-i}.

We note that the "conventional" q-ary erasure channel $W(y|x) = \varepsilon\delta_{?,y} + (1 - \varepsilon)\delta_{x,y}$ is a particular case of the above example given by $\varepsilon_1 = \cdots = \varepsilon_{r-1} = 0$. In this case the channels polarize to just two levels corresponding to capacity 0 and r. It is possible to define other erasure-like channels for the q-ary input alphabet, but computing explicit examples (essentially, constructing polar codes) becomes more difficult.

Another example is given by the OSC. The OSC models transmission over r parallel links such that, if in a given time slot a bit is received incorrectly, the bits with indices lower than that are equiprobable. This system was proposed in [66] as an abstraction of transmission in wireless fading environment. The capacity of the channel equals

$$I(W) = r + \varepsilon_0 \log_2 \varepsilon_0 + \sum_{i=1}^{r} \varepsilon_i \log_2 \frac{\varepsilon_i}{2^{i-1}}.$$

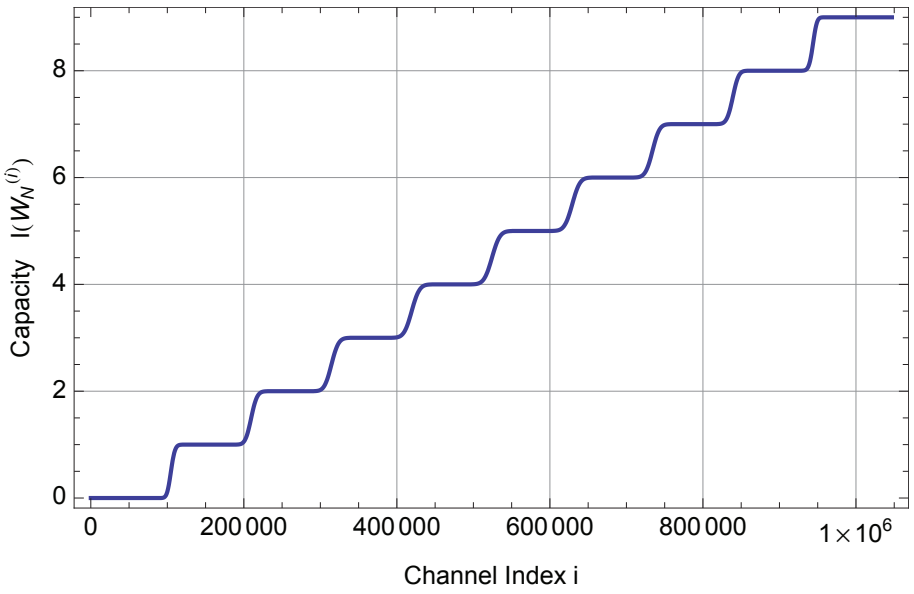

Figure 4.3: 10-level polarization for the OEC $W : \{0,1\}^9 \to \mathcal{Y}$ with transition probabilities $\varepsilon_i = 0.1, i = 0, 1, \ldots, 9$. The code length is $N = 2^{20}$.

By Theorem 4.1 q-ary polar codes, $q = 2^r$ can be used to transmit at rates close to capacity on this channel; moreover, the domination pattern that emerges, exactly matches the fading nature of the bundle of r parallel channels, achieving the capacity of the system discussed above.

4.10 Two-level Polarization

Recently, Şaşoğlu [60] found polarization kernels that achieve full (i.e., two-level) polarization for nonbinary DMCs with arbitrary-size input alphabets. His proof relies on establishing entropy polarization, i.e., tracking the behavior of conditional entropies of the transmitted symbols and proving polarization based on their convergence. [60] designed a set of kernels that force the entropies to approach 0 and 1, thereby polarizing the data symbols into fully noisy and almost noiseless. In this section, we give another proof of Şaşoğlu's result, establishing two-level polarization for $q = 2^r$ relying on Bhattacharyya distances rather than on entropies. The new proof is a by-product of our construction in the next section where we design transformations that polarize the symbols to an arbitrary predefined subset of levels. Therefore, the new method seems more flexible than the earlier proof in that it enables us to generalize both our construction in the previous section and the two-level result of [60]. Moreover, the known construction methods of polar codes rely on Bhattacharyya distances, so we anticipate that the new considerations will be useful in constructing coding schemes that straddle the line between the two extremes in terms of the number of different types of polarized data symbols.

Suppose that $g : \mathcal{X}^2 \to \mathcal{X}$ is a map that combines two data symbols into one channel symbol. In the previous sections, we have used a mapping $x_1 = g(u_1, u_2)$ given by $u_1 + u_2$ with modulo-q addition. Generally, let the combined channel W_2 and the channels W^- and W^+ be

defined as follows:

$$W_2(y_1, y_2|u_1, u_2) = W(y_1|g(u_1, u_2))W(y_2|u_2)$$
$$W^-(y_1, y_2|u_1) = \sum_{u_2 \in \mathcal{X}} \frac{1}{q} W_2(y_1, y_2|u_1, u_2)$$
$$W^+(y_1, y_2, u_1|u_2) = \frac{1}{q} W_2(y_1, y_2|u_1, u_2),$$

where $u_1, u_2 \in \mathcal{X}, y_1, y_2 \in \mathcal{Y}$.

Define g by the relation

$$g(u_1, u_2) = u_1 + \pi(u_2) \mod q \tag{4.26}$$

where π is a permutation from $\mathcal{X}$ to $\mathcal{X}$ with the following property: there is at least one number $x \in \mathcal{X}$ satisfying

$$\mathrm{wt}_r(\pi(x) - \pi(x + q/2)) = r. \tag{4.27}$$

As an example, one can take

$$\pi(u_2) = \begin{cases} q/2, & \text{if } u_2 = 0 \\ 1 - u, & \text{if } 1 \le u_2 \le q/2 \\ -u, & \text{if } u_2 > q/2 \end{cases} \tag{4.28}$$

where the operations are performed modulo q.

The map used in [60] is an inverse of the map g. Generally, [60] observed that the following set of conditions suffices to prove the entropy polarization.

Definition 4.1 *[60] A map $f : \mathcal{X}^2 \to \mathcal{X}$ is called polarizing if the following 3 conditions hold:*
(a) for all $x_2 \in \mathcal{X}$, the map $x_1 \mapsto f(x_1, x_2)$ is invertible,
(b) for all $x_1 \in \mathcal{X}$, the map $x_2 \mapsto f(x_1, x_2)$ is invertible, and
(c) for all $2 \le K \le q - 1$ and any choice of distinct $a_0, \ldots, a_{K-1} \in \mathcal{X}$, the matrix

$$B_{ij} = f(a_i, a_j), \qquad i, j = 0, \ldots, K - 1$$

has at least $K + 1$ distinct entries.

We will prove that the channel combining operation (4.26) supports convergence of the Bhattacharyya parameters. First, let us establish relations for them that extend inequalities (4.12) and (4.13).

Proposition 4.6 *For $v \in \mathcal{X}$, the quantities $Z_v(W^-)$ and $Z_v(W^+)$ are related to $Z_v(W)$ by*

$$Z_v(W^-) \ge Z_v(W), \tag{4.29}$$
$$Z_v(W^-) \le Z_v(W) + \frac{1}{q} \sum_x \frac{1}{q} \sum_{\substack{u_1, u_2 \\ g(x,u_1) = g(x+v,u_2)}} Z(W_{\{u_1,u_2\}})$$
$$+ \frac{1}{q} \sum_x \frac{1}{q} \sum_{\substack{u_1, u_2 \\ u_1 \ne u_2 \\ g(x,u_1) \ne g(x+v,u_2)}} Z(W_{\{g(x,u_1),g(x+v,u_2)\}}) Z(W_{\{u_1,u_2\}}), \tag{4.30}$$
$$Z_v(W^+) = \frac{1}{q} \sum_x Z_{s(x,x+v)}(W) Z(W_{\{x,x+v\}}) \tag{4.31}$$

where $s(x_1, x_2) = \pi(x_1) - \pi(x_2) \mod q$ and $x_1, x_2 \in \mathcal{X}$.

Proof: First let us prove the upper bound for $Z_v(W^-)$. From the definitions of $Z_v(\cdot)$ and W^- we have

$$\begin{aligned}
Z_v(W^-) &= \frac{1}{q}\sum_x Z(W^-_{\{x,x+v\}}) \\
&= \frac{1}{q}\sum_x \sum_{y_1,y_2} \sqrt{W^-(y_1,y_2|x)W^-(y_1,y_2|x+v)} \\
&= \frac{1}{q}\sum_x \frac{1}{q}\sum_{y_1,y_2} \sqrt{\sum_{u_1,u_2} W(y_1|g(x,u_1))W(y_2|u_1)W(y_1|g(x+v,u_2))W(y_2|u_2)} \\
&\le \frac{1}{q}\sum_x \frac{1}{q}\sum_{u_1,u_2}\sum_{y_1,y_2} \sqrt{W(y_1|g(x,u_1))W(y_2|u_1)W(y_1|g(x+v,u_2))W(y_2|u_2)} \\
&= \frac{1}{q}\sum_x \frac{1}{q}\sum_u Z(W_{\{g(x,u),g(x+v,u)\}}) + \frac{1}{q}\sum_x \frac{1}{q} \sum_{\substack{u_1,u_2 \\ g(x,u_1)=g(x+v,u_2)}} Z(W_{\{u_1,u_2\}}) \\
&\quad + \frac{1}{q}\sum_x \frac{1}{q} \sum_{\substack{u_1,u_2 \\ u_1\neq u_2 \\ g(x,u_1)\neq g(x+v,u_2)}} Z(W_{\{g(x,u_1),g(x+v,u_2)\}})Z(W_{\{u_1,u_2\}}).
\end{aligned}$$

Note that $g(x+v,u)-g(x,u) = x+v+\pi(u)-x-\pi(u) = v$ for any $x \in \mathcal{X}$. Since $x \mapsto g(x,u)$ is a permutation for a fixed u, $\frac{1}{q}\sum_x Z(W_{\{g(x,u),g(x+v,u)\}}) = Z_v(W)$ for any $u \in \mathcal{X}$. Thus the first term becomes $Z_v(W)$, which gives the estimate in (4.30). The lower bound on $Z_v(W^-)$ is shown as follows:

$$\begin{aligned}
Z_v(W^-) &= \frac{1}{q}\sum_x \frac{1}{q}\sum_{y_1,y_2} \sqrt{\sum_{u_1,u_2} W(y_1|g(x,u_1))W(y_2|u_1)W(y_1|g(x+v,u_2))W(y_2|u_2)} \\
&\ge \frac{1}{q}\sum_x \frac{1}{q}\sum_u \sum_{y_1,y_2} \sqrt{W(y_1|g(x,u))W(y_2|u)W(y_1|g(x+v,u))W(y_2|u)} \\
&= \frac{1}{q}\sum_x \frac{1}{q}\sum_u \sum_{y_1} \sqrt{W(y_1|g(x,u))W(y_1|g(x+v,u))} \\
&= \frac{1}{q}\sum_x \frac{1}{q}\sum_u Z(W_{\{g(x,u),g(x+v,u)\}}) \\
&= Z_v(W).
\end{aligned}$$

To prove (4.31), let us consider the Bhattacharyya distance of W^+ between $x, x' \in \mathcal{X}$, $x \neq x'$.

$$\begin{aligned}
Z(W^+_{\{x,x'\}}) &= \sum_{y_1,y_2,u_1} \sqrt{W^+(y_1,y_2,u_1|x)W^+(y_1,y_2,u_1|x')} \\
&= \frac{1}{q}\sum_{y_1,y_2,u_1} \sqrt{W(y_1|g(u_1,x)))W(y_2|x)W(y_1|g(u_1,x'))W(y_2|x')} \\
&= \frac{1}{q}\sum_{u_1} Z(W_{\{g(u_1,x),g(u_1,x')\}})Z(W_{\{x,x'\}}) \\
&= Z_{s'}(W)Z(W_{\{x,x'\}})
\end{aligned}$$

where $s' = g(u_1, x) - g(u_1, x') = u_1 + \pi(x) - u_1 - \pi(x') = \pi(x) - \pi(x') = s(x, x') \mod q$ which is the same for all $u_1 \in \mathcal{X}$. The last equality holds because the set $\{g(u_1, x) : u_1 \in \mathcal{X}\} = \mathcal{X}$ for any $x \in \mathcal{X}$. From the definition of $Z_v(W)$ we now obtain (4.31). ■

Our next goal is to prove that the map g given by (4.26) and (4.27) supports two-level polarization for channels with input alphabet of size q. We rely on Bhattacharyya distances. In the next lemma we prove convergence of the quantities $Z_{v,n}$ relying on Proposition 4.6.

Lemma 4.10 *For $v \in \mathcal{X} \setminus \{0\}$, $Z_{v,n}$ converges a.s. to a $(0,1)$-valued Bernoulli random variable Z_∞ that does not depend on v.*

Proof: We begin with proving convergence of $Z^{[1,r]}_{\max,n}$ defined in Section 4.6. Let $v_1 = \operatorname{argmax}_{v \in \mathcal{X}} Z_{v,n}$ and $v_2 = \operatorname{argmax}_{v \in \mathcal{X}} Z_{v,n+1}$. Consider the case of moving along the $+$ path from level n to level $n+1$ in the tree. In this case we have

$$\begin{aligned} Z^{[1,r]}_{\max,n+1} = Z_{v_2,n+1} &= \frac{1}{q} \sum_x Z_{s(x,x+v_2),n} Z(W_{\{x,x+v_2\},n}) \\ &\le Z_{v_1,n} \frac{1}{q} \sum_x Z(W_{\{x,x+v_2\},n}) \\ &= Z_{v_1,n} Z_{v_2,n} \\ &\le \big(Z^{[1,r]}_{\max,n}\big)^2. \end{aligned}$$

Here the first inequality follows because, by definition of v_1, the quantity $Z_{s(x,x+v_2),n}$ for all $x \in \mathcal{X}$ can be bounded above by $Z_{v_1,n}$. Suppose that $v_1 = v_2$. Then the last inequality holds with equality. At the same time, if $v_1 \neq v_2$, then $Z_{v_2,n} \le Z_{v_1,n} = Z^{[1,r]}_{\max,n}$.

Now consider the case of moving along the $-$ path. For any $v \in \mathcal{X} \setminus \{0\}$, the quantity $Z_{v,n} = \frac{1}{q} \sum_x Z(W_{\{x,x+v\},n}) \le Z^{[1,r]}_{\max,n}$ and $Z(W_{\{x,x'\},n}) \le q Z^{[1,r]}_{\max,n}$ for all $x, x' \in \mathcal{X}$, $x \neq x'$. Therefore the second term in the upper bound on $Z^{[1,r]}_{\max,n+1}$ in (4.30) is bounded above by $q Z^{[1,r]}_{\max,n}$, and the third term is bounded above by $(q^2 - 2q) Z^{[1,r]}_{\max,n}$. Now invoke Lemma 4.5, in which condition (ii) is replaced with $P(U_{n+1} \le U_n^2 | \mathcal{F}_n) \ge 1/2$. This change does not affect the proof, so we conclude that $Z^{[1,r]}_{\max,n}$ converges a.s. to a Bernoulli random variable $Z^{[1,r]}_{\max,\infty}$.

Having established that $Z^{[1,r]}_{\max,n}$ converges to 0 or to 1, let us consider both cases. If it is the former, then $Z_{v,n}$ converges to 0 for all v by the definition. If $Z^{[1,r]}_{\max,n}$ converges to 1, at least one of $Z_{v,n}$ converges to 1, and from the monotone behavior of the Z_v's (Lemma 4.6), $Z_{v,n}$ with $\mathrm{wt}_r(v) = 1$ must converge to 1. Since there exists at least one $x \in \mathcal{X}$ that satisfies the condition (4.27), without loss of generality we can assume that $\mathrm{wt}_r(s(0, q/2)) = r$. The quantity $Z_{1,n+1}$ with $b_{n+1} = +$ is

$$\begin{aligned} Z_{1,n+1} &= \frac{2}{q}\big(Z(W_{\{0,q/2\},n+1}) + Z(W_{\{1,q/2+1\},n+1}) + \cdots + Z(W_{\{q/2-1,q-1\},n+1})\big) \\ &= \frac{2}{q}\big(Z_{s(0,q/2),n} Z(W_{\{0,q/2\},n}) + Z_{s(1,q/2+1),n} Z(W_{\{1,q/2+1\},n}) + \dots \\ &\quad + Z_{s(q/2-1,q-1),n} Z(W_{\{q/2-1,q-1\},n})\big) \\ &\le \frac{2}{q}\big(Z_{s(0,q/2),n} + \frac{q}{2} - 1\big) \\ &= \frac{2}{q}\big(Z_{s(0,q/2),n} - 1\big) + 1 \end{aligned}$$

where the inequality follows from the fact that $Z(W_{\{x,x+q/2\},n}) \leq 1$ and $Z_{s(i,q/2+i),n} \leq 1$, $i = 1, \ldots, q/2-1$. Let $\Omega_a^{(1)} = \{\omega : Z_{1,n} \to a\}, a = 0, 1$. Since the above inequality holds trajectory-wise and $\frac{2}{q}\big(Z_{s(0,q/2),n} - 1\big) + 1 \leq 1$, the sequence of random variables $\frac{2}{q}\big(Z_{s(0,q/2),n} - 1\big) + 1$ converges to 1 and thus $Z_{s(0,q/2),n} \to 1$ on the event $\Omega_1^{(1)}$. Finally, notice that $\mathrm{wt}_r(s(0, q/2)) = r$, and so from Lemma 4.6 we conclude that $Z_{v,n}$ converges to 1 on $\Omega_1^{(1)}$ for all v. This completes the proof. ■

From the relation between $I(W)$ and $Z_i(W)$ described in Lemma 4.2, we see that if $Z_i(W) = 0$ for $i = 1, \ldots, r$, then $I(W) = r$, and if $Z_i(W) = 1$ for all i, then $I(W) = 0$. This implies that with probability one the virtual channels for transmitted symbols converge to either perfect channels or purely noisy channels.

4.11 Controlling Polarization: Any Number of Levels

4.11.1 Multilevel Polar Codes and Coding of Video Sequences

In this section we advance the designs of the previous section by constructing polar codes that support polarization to any subset of the set of $r + 1$ levels chosen in advance.

We begin with a brief discussion of possible applications of multilevel coding schemes. Let us consider an information transmission system that requires several types of data symbols, each of which carries a prescribed number of "noiseless" bits over the channel. To be concrete, consider the video sequence structure of MPEG-2 [39]. The overall structure of the encoding is as follows. The video stream consists of 6 layers that are: video sequence, group of pictures (GOP), picture, slice, macroblock, and block layers. From fine to coarse, these layers have the following functions. A block is an array of 8×8 pixels of the actual video signal. 16×16 blocks become a macroblock. A series of macroblocks are grouped into a slice, and multiple slices form one frame which contains all the information about one picture. There are three types of frames: an intra frame (I-frame), a predictive frame (P-frame), and a bidirectionally predictive frame (B-frame). A GOP is a group of successive pictures in the video sequence that can be decoded independently. A GOP starts with an I-frame followed by many P-frames and B-frames. Finally, the video sequence is formed of a sequence header followed by one or more GOPs and terminated by an end code.

Let us take a closer look at the information in the picture layer. An I-frame contains the reference picture and does not require additional information to reconstruct the image. Because of this, the data in the I-frames have to be encoded for high reliability and thus their compression ratio is low. At the same time, a P-frame carries data only for macroblocks that are changed from one reference picture to the next one. The picture is decoded based on the prior I-frame or the P-frame. As a slight variation, a B-frame encodes the difference between the frame that precedes the current one as well as the frame that succeeds it. To reconstruct the image for P-frames or B-frames, we start with the full image of the neighboring frame and obtain a new image by applying the new motion information. Although this information may be decoded with errors, we can still obtain good quality of the picture as long as the distortion level of the recovered image is low or if the user does not notice the distortion caused by errors. Therefore, usually data in P-frames and B-frames require less reliability than those in the I-frames and so this portion of the data can be compressed at a higher rate.

For simplicity assume that the channel between the transmitter and the receiver is symmetric. Suppose that the actual encoding of the data is performed using the polar coding scheme. It is possible to use the original binary polar codes of [3]. For that, we first break each information unit (for instance a pixel that generally consists of several bits) into bits, then encode and transmit,

and finally merge the recovered bits after decoding. This introduces additional overhead on both the encoder and the decoder sides. To avoid this, we can use q-ary polar codes with $q = 2^r$. We can choose between the two-level (fully polarizing) design of [60] and the $r + 1$-level scheme of the previous section. However, neither choice enables us to overcome the overhead. Indeed, suppose that we are relying on the two-level scheme and use r_I bits to represent an information unit in the I-frame. Since the data in the P-frames and the B-frames are subjected to a higher compression ratio, number of bits to represent each information unit in the P-frames, call it r_P, or in the B-frames, call it r_B, is smaller than r_I. Therefore, if we use q-ary polar codes based on the 2-level polarization with $q = 2^{r_I}$, we need to rearrange the data from P-frames and B-frames before encoding and after decoding. Thus, the two-level scheme does not offer enough variability for seamless operation of the encoder and decoder circuits. At the same time, the $r + 1$-level scheme has too much variation because many levels go unclaimed in the design of the coding scheme. An optimal solution is somewhere in the middle, for instance, a polarizing scheme with just 4 levels for the symbols that carry the payload, one level for each of the r_P and r_B bits, and a level for r_I bits as well as a level for 0 bits.

Currently the most widely used format for video data is the H.264/MPEG-4 video coding standard [69]. In this standard, one achieves higher compression rate while keeping or improving the quality of pictures by allowing up to 16 reference frames. The overall structure of the data in this standard is complicated. However, the information in different types of frames requires different levels of reliability, and thus the polar coding scheme studied in this section could also be useful. Moreover, this scheme can also be efficient if the source messages are described with different amounts of distortion so that each message is encoded into binary vectors of different lengths.

4.11.2 The Construction

In Section 4.10, following [60], we proved that the polarizing mapping g given by (4.26) and (4.27) gives us the two-level polarization for q-ary DMCs. In this section, we find mappings $(u_1, u_2) \mapsto (x_1, x_2)$ that polarize a DMC with the q-ary input to q-ary channels with capacity k bits, where $k \in T$ and T is a subset of $\{0, 1, \ldots, r\}$ of cardinality $3 \leq |T| \leq r$ that includes 0 and r.

Let k be the running index of the channels in (4.9) and suppose that capacity of channel k is k (this corresponds to row $r - k + 1$ in the array (4.9)). In the previous section, using the map (4.26), we have removed all the levels from $k = 1$ to $k = r - 1$. The technical tool for accomplishing this is to force the random variables $Z_{i,n}, i = 1, 2, \ldots, r$ to converge to identical copies of a Bernoulli random variable; see also the proof of Lemma 4.10. Generalizing this idea let us find a mapping that leaves all the extremal configurations except those in rows $r-j$ to $r-i$,, $i \leq j$. In this case, the set of extremal configurations becomes

$$\{1^k 0^{r-k}, k = 0, 1, \ldots, i-1, j+1, \ldots, r\}.$$

To obtain this set, we will make the random variables $Z_{i,n}, Z_{i+1,n}, \ldots, Z_{j+1,n}$ converge to the same $(0, 1)$-valued random variable, thereby collapsing the corresponding levels. For a number n, denote the set $\{0, 1, \ldots, n-1\}$ by $[n]$. Let $q_1 = 2^{j-i+2}$. In order to remove $j - i + 1$ consecutive levels, we define a permutation π by first defining $\pi_{q_1} : [q_1] \mapsto [q_1]$ so that it satisfies condition

(4.27). The resulting permutation π is given by

$$\pi(u) = \begin{cases} 2^{r-j-1} \cdot \pi_{q_1}(\frac{u}{2^{r-j-1}}), & \text{if } 2^{r-j-1} | u, u < 2^{r-i+1} \\ \pi(u - u'') + u'', & \text{if } 2^{r-j-1} \not| u, u < 2^{r-i+1} \\ \pi(u') + (u - u'), & \text{otherwise} \end{cases} \tag{4.32}$$

where $u' = u \mod 2^{r-i+1}$ and $u'' = u \mod 2^{r-j-1}$, and addition is modulo q.

The intuition behind this definition is as follows. Consider the set $B_l = \{g(u_1, u_2) : u_1, u_2 \in \mathcal{X}_0^l\}$, where $\mathcal{X}_0^l = \mathcal{X}_0 \cup \cdots \cup \mathcal{X}_l$, $l \geq 1$ and $\mathcal{X}_0 = \{0\}$. If the mapping g is defined using addition modulo q, then the size of the set B_l is 2^l, $l = 1, \ldots, r$, which is equal to the size of the set $\mathcal{X}_0^l$. At the same time, if we use the mapping g given by (4.26) and (4.27), then $|B_l|$ is strictly greater than 2^l when $1 \leq l \leq r-1$. Based on this, we assume that the lth level is present among the extreme configurations if the size of the set B_l is equal to $|\mathcal{X}_0^l|$. Therefore, in order to remove levels i to j from the set of extremal configurations, we design g so that $|B_l| = |\mathcal{X}_0^l|$ if $l = 1, \ldots, i-1, j+1, \ldots, r$, while $|B_l| > |\mathcal{X}_0^l|$ for $l = i, \ldots, j$. To achieve this goal, we use the permutation $\pi_{q_1}(u)$ if $i \leq \text{wt}_r(u) \leq j+1$ and use modulo-q addition otherwise. The value $j+1$ is included for the following reason. For 2-level polarization, we make the random variables $Z_{k,n}$, $k = 1, 2, \ldots, r$ converge to the same $(0,1)$-valued random variable by using the permutation $\pi(u)$ when $1 \leq \text{wt}_r(u) \leq r$ to define a mapping g. Likewise, since the random variables $Z_{k,n}$, $k = i, \ldots, j+1$ must converge to the same Bernoulli random variable, we need a permutation $\pi(u)$ of size 2^{j-i+2} for vectors with ordered weight from i to $j+1$.

The permutation π has the following property.

Proposition 4.7 *Suppose that π is given by (4.32). Then for $u_1, u_2 \in \mathcal{X}$, the ordered weight $wt_r(\pi(u_1) - \pi(u_2)) = t$ if and only if $wt_r(u_1 - u_2) = t$, $t = 1, 2, \ldots, i-1, j+2, \ldots, r$.*

Proof: Let us consider the case when $j+2 \leq t \leq r$ and let $q' = 2^{r-i+1}$, $q'' = 2^{r-j-1}$, $u_1' = u_1 \mod q'$, $u_2' = u_2 \mod q'$, $u_1'' = u_1 \mod q''$, and $u_2'' = x_2 \mod q''$. The difference

$$\begin{aligned} \pi(u_1) - \pi(u_2) &= \pi(u_1') + (u_1 - u_1') - \pi(u_2') - (u_2 - u_2') = \pi(u_1') - \pi(u_2') + l'q' \\ &= q''\pi_{q_1}(\frac{u_1' - u_1''}{q''}) + u_1'' - q''\pi_{q_1}(\frac{u_2' - u_2''}{q''}) - u_2'' + l'q' \\ &= u_1'' - u_2'' + l''q'' + l'q' \end{aligned}$$

for some $l' \in [2^{i-1}]$ and $l'' \in [2^{j+1}]$, where $q_1 = 2^{j-i+2}$. Thus $\pi(u_1) - \pi(u_2) = u_1'' - u_2'' = u_1 - u_2 \mod q''$, where $u_1'' \neq u_2''$. Therefore $\pi(u_1) - \pi(u_2) = u_1'' - u_2'' + k_1 q''$ and $u_1 - u_2 = u_1'' - u_2'' + k_2 q''$ for some $k_1, k_2 \in [2^{j+1}]$. This means that $\text{wt}_r(\pi(u_1) - \pi(u_2)) = \text{wt}_r(u_1 - u_2)$.

Suppose next that $t \leq i-1$. The ordered weight of difference $v = u_1 - u_2$ is less than i and $v' = 0 \mod q'$. This means that $u_1' = u_2'$ and the difference

$$\pi(u_1) - \pi(u_2) = \pi(u_1') + (u_1 - u_1') - \pi(u_2') - (u_2 - u_2') = u_1 - u_2$$

modulo q. This completes the proof. ■

In the next theorem, we prove convergence of $Z_{v,n}$, which is the main technical result of this section.

Theorem 4.7 *Let the mapping $g : \mathcal{X}^2 \to \mathcal{X}$ be given by (4.32). For all $i = 1, 2, \ldots, r$*

$$\lim_{n \to \infty} Z_{i,n} = Z_{i,\infty} \ \ a.s.,$$

where $Z_{i,\infty} \in \{0,1\}$. Moreover, with probability 1, the vector $(Z_{1,\infty}, Z_{2,\infty}, \ldots, Z_{r,\infty})$ is one of the vectors of the form $\{1^i 0^{r-i} : i = 0, 1, \ldots, i-1, j+1, \ldots, r\}$.

Proof: Let us consider the upper bound of $Z_v(W^-)$ first. Let $v \in \mathcal{X}_t$, $t = 1, 2, \ldots, r$. When $g(x, u_1) = g(x + v, u_2)$, $g(x, u_1) - g(x + v, u_2) = -v + \pi(u_1) - \pi(u_2) = 0$ and $\mathrm{wt}_r(\pi(u_1) - \pi(u_2)) = t$. By Proposition 4.7, $\mathrm{wt}_r(u_1 - u_2) = t$ if $t = 1, \ldots, i-1), j+2, \ldots, r$. Therefore, the second term on the r.h.s. of (4.30) in the case $\mathrm{wt}_r(v) = 1, \ldots, i-1, j+2, \ldots, r$ is bounded above by $qZ^{(t)}_{\max}(W)$ or $qZ^{[t,r]}_{\max}(W)$. If $i \le t \le j+1$, the ordered weight of the vector $u_1 - u_2$ is also between i and $j+1$ so the second term in this case is upper bounded by $qZ^{[i,j+1]}_{\max}(W)$ or $qZ^{[i,r]}_{\max}(W)$.

Consider the case $g(x, u_1) \neq g(x + v, u_2)$. If $\mathrm{wt}_r(u_1 - u_2) = s \ge t$, then

$$\begin{aligned} Z(W_{\{u_1,u_2\}})Z(W_{\{g(x,u_1),g(x+v,u_2)\}}) &\le qZ^{(s)}_{\max}(W) \\ &\le qZ^{[t,r]}_{\max}(W). \end{aligned}$$

On the other hand, if $\mathrm{wt}_r(u_1 - u_2) = s < t$, then term inside the last summation in (4.30) can also be bounded above by $qZ^{[t,r]}_{\max}(W)$ if $t \le i-1$ or $t \ge j+2$ and $qZ^{[i,r]}_{\max}(W)$ if $i \le t \le j+1$. Indeed, consider the difference $g(x, u_1) - g(x + v, u_2) = -v + \pi(u_1) - \pi(u_2)$. If $t \le i-1$ or $t \ge j+2$, then $\mathrm{wt}_r(\pi(u_1) - \pi(u_2)) = s < t$, so $\mathrm{wt}_r(g(x, u_1) - g(x + v, u_2)) = t$. This means that the term

$$\begin{aligned} Z(W_{\{u_1,u_2\}})Z(W_{\{g(x,u_1),g(x+v,u_2)\}}) &\le Z(W_{\{g(x,u_1),g(x+v,u_2)\}}) \\ &\le qZ^{(t)}_{\max}(W) \\ &\le qZ^{[t,r]}_{\max}(W). \end{aligned}$$

At the same time, if $i \le t \le j+1$, then the ordered weight of the vector $z = \pi(u_1) - \pi(u_2)$ satisfies $\mathrm{wt}_r(z) = s$ if $s < i$ or $i \le \mathrm{wt}_r(z) \le j+1$ if $s \ge i$. This implies that $i \le \mathrm{wt}_r(g(x, u_1) - g(x + v, u_2)) \le j+1$. Therefore,

$$\begin{aligned} Z(W_{\{u_1,u_2\}})Z(W_{\{g(x,u_1),g(x+v,u_2)\}}) &\le Z(W_{\{g(x,u_1),g(x+v,u_2)\}}) \\ &\le qZ^{[i,j+1]}_{\max}(W) \\ &\le qZ^{[i,r]}_{\max}(W). \end{aligned}$$

Summarizing, the upper bound on $Z_v(W^-)$ is

$$Z_v(W^-) \le Z_v(W) + qZ^{[t,r]}_{\max}(W) + q(q-2)Z^{[t,r]}_{\max}(W)$$

if $t = 1, \ldots, i-1, j+2, \ldots, r$ and

$$Z_v(W^-) \le Z_v(W) + qZ^{[i,r]}_{\max}(W) + q(q-2)Z^{[i,r]}_{\max}(W)$$

if $t = i, \ldots, j+1$. If $\mathrm{wt}_r(v) = t$,

$$Z_v(W) \le Z^{(t)}_{\max}(W) \le Z^{[t,r]}_{\max}(W) \le Z^{[s,r]}_{\max}(W)$$

for any $s \le t$. Therefore, the term $Z_v(W)$ in the first inequality can be replaced with $Z^{[t,r]}_{\max}(W)$ and the term in the second inequality with $Z^{[i,r]}_{\max}(W)$.

From Proposition 4.7, if $\mathrm{wt}_r(v) = t$, where $t = 1, \ldots, i-1, j+2, \ldots, r$, then $\mathrm{wt}_r(s(x, x+v)) = \mathrm{wt}_r(\pi(x) - \pi(x+v)) = t$ and $Z_{s(x,x+v)} \le Z^{(t)}_{\max}(W)$. Therefore we obtain

$$\begin{aligned} Z_v(W^+) &= \frac{1}{q}\sum_x Z_{s(x,x+v)}(W)Z(W_{\{x,x+v\}}) \\ &\le Z^{(t)}_{\max}(W)Z_v(W) \\ &\le \left(Z^{(t)}_{\max}(W)\right)^2 \le \left(Z^{[t,r]}_{\max}(W)\right)^2. \end{aligned}$$

In addition, if $t = i, \ldots, j+1$, the ordered weight of $s(x, x+v)$ is one of the values in the set $\{i, i+1, \ldots, j+1\}$. Thus,

$$\begin{aligned} Z_v(W^+) &= \frac{1}{q} \sum_x Z_{s(x,x+v)} Z(W_{\{x,x+v\}}) \\ &\leq Z_{\max}^{[i,j+1]}(W) Z_v(W) \\ &\leq \left(Z_{\max}^{[i,j+1]}(W)\right)^2 \leq \left(Z_{\max}^{[i,r]}(W)\right)^2. \end{aligned}$$

This means that the random variable $Z_{\max,n}^{[t,r]}$ converges a.s. to a $(0,1)$-valued random variable $Z_{\max,\infty}^{[t,r]}$ for $t = 1, 2, \ldots, i-1, i, j+2, \ldots, r$.

Now we will prove that the random variables $Z_{\max,n}^{(t)}$, $t = 1, \ldots, r$ converge a.s. to $Z_{\max,\infty}^{(t)}$ which is $(0,1)$-valued random variables. By following the induction argument in the proof of Lemma 4.7 we can show that $Z_{\max,\infty}^{(t)}$ takes values 0 or 1 with probability 1 and so does $Z_{v,\infty}$, $v \in \mathcal{X}_t$, $t = j+2, \ldots, r$. Assume that we have proved the needed convergence for $Z_{\max,n}^{(t)}$, $t = j+2, \ldots, r$ and let us prove the convergence for $Z_{\max,n}^{(s)}$, $s = i, \ldots, j+1$. Suppose that $Z_{\max,\infty}^{[i,r]} = 0$, then $Z_{\max,\infty}^{(s)} = 0$, $s = i, \ldots, r$. On the other hand if $Z_{\max,\infty}^{[i,r]} = 1$, by Lemma 4.6 $Z_{\max,\infty}^{(i)} = 1$ and $Z_{v,\infty} = 1$ for all $v \in \mathcal{X}_i$. Observe that π_{q_1} is the same permutation as in (4.26) with q replaced with q_1. Therefore, Lemma 4.10 implies that the variables $Z_{v,n}$,$\mathrm{wt}_r(v) = i, \ldots, j+1$ converge to the same Bernoulli random variable. We conclude that $Z_{i,\infty} = \cdots = Z_{j+1,\infty}$, while configurations from the $(r-j)$th to the $(r-i)$th level occur with probability zero. By applying the same induction argument, we can also obtain the needed convergence for $t = i-1, \ldots, 1$. ■

Let us give an example of the above mapping.

Example 4.1 *Let $q = 2^3$. In the original construction of Sect. 4.4, the channels polarize to 4 levels, corresponding to* 0,1,2, *and* 3 *bits in the data symbols. Suppose we would like to remove the extremal configuration that corresponds to channels with capacity 1. Use the mapping $g(u_1, u_2) = u_1 + \pi(u_2)$ where π is given by (4.32), where we take $q = 8$, $i = j = 2$, and π_4 a permutation given by (4.28) with $q = 4$. Then the matrix G, $G_{i,j} = g(i,j)$, $i, j \in \mathcal{X}$ becomes*

$$G = \begin{pmatrix} 2 & 0 & 3 & 1 & 6 & 4 & 7 & 5 \\ 3 & 1 & 4 & 2 & 7 & 5 & 0 & 6 \\ 4 & 2 & 5 & 3 & 0 & 6 & 1 & 7 \\ 5 & 3 & 6 & 4 & 1 & 7 & 2 & 0 \\ 6 & 4 & 7 & 5 & 2 & 0 & 3 & 1 \\ 7 & 5 & 0 & 6 & 3 & 1 & 4 & 2 \\ 0 & 6 & 1 & 7 & 4 & 2 & 5 & 3 \\ 1 & 7 & 2 & 0 & 5 & 3 & 6 & 4 \end{pmatrix}.$$

The relations between $Z_v(W^{\pm})$ and $Z_v(W)$ for all 3-dimensional binary vectors $v \in \mathcal{X}$ are as

follows.

$$
\begin{aligned}
Z_{100}(W^+) &= \frac{1}{4}\big(Z(W^+_{\{0,4\}}) + Z(W^+_{\{1,5\}}) + Z(W^+_{\{2,6\}}) + Z(W^+_{\{3,7\}})\big) = (Z_{100}(W))^2,\\
Z_{010}(W^+) &= \frac{1}{8}\big(Z(W^+_{\{0,2\}}) + Z(W^+_{\{1,3\}}) + Z(W^+_{\{2,4\}}) + Z(W^+_{\{3,5\}})\\
&\qquad + Z(W^+_{\{4,6\}}) + Z(W^+_{\{5,7\}}) + Z(W^+_{\{6,0\}}) + Z(W^+_{\{7,1\}})\big)\\
&= \frac{1}{8}\big(Z_{001}(W)(Z(W_{\{0,2\}}) + Z(W_{\{1,3\}}) + Z(W_{\{4,6\}}) + Z(W_{\{5,7\}})\\
&\qquad + Z_{011}(W)(Z(W_{\{2,4\}}) + Z(W_{\{3,5\}}) + Z(W_{\{6,0\}}) + Z(W_{\{7,1\}}))\big),\\
Z_{001}(W^+) &= \frac{1}{8}\big(Z_{010}(W)(Z(W_{\{0,1\}}) + Z(W_{\{2,3\}}) + Z(W_{\{4,5\}}) + Z(W_{\{6,7\}})\\
&\qquad + Z_{011}(W)(Z(W_{\{1,2\}}) + Z(W_{\{3,4\}}) + Z(W_{\{5,6\}}) + Z(W_{\{7,0\}}))\big),\\
Z_{011}(W^+) &= \frac{1}{8}\big(Z_{010}(W)(Z(W_{\{1,4\}}) + Z(W_{\{3,6\}}) + Z(W_{\{5,0\}}) + Z(W_{\{7,2\}})\\
&\qquad + Z_{001}(W)(Z(W_{\{0,3\}}) + Z(W_{\{2,5\}}) + Z(W_{\{4,7\}}) + Z(W_{\{6,1\}}))\big)
\end{aligned}
$$

and

$$
\begin{aligned}
Z_v(W^-) \le Z_v(W) &+ \frac{1}{q}\sum_x \frac{1}{q} \sum_{\substack{u_1,u_2\\ g(x,u_1)=g(x+v,u_2)}} Z(W_{\{u_1,u_2\}})\\
&+ \frac{1}{q}\sum_x \frac{1}{q} \sum_{\substack{u_1,u_2\\ u_1\neq u_2\\ g(x,u_1)\neq g(x+v,u_2)}} Z(W_{\{g(x,u),g(x+v,u)\}})Z(W_{\{u_1,u_2\}}).
\end{aligned}
$$

From the above inequalities and Theorem 4.7, $Z_{i,n}$ converges to $Z_{i,\infty}$, $i = 1, 2, 3$ where the vector $(Z_{1,\infty}, Z_{2,\infty}, Z_{3,\infty})$ takes one of the following values: $(0, 0, 0)$, $(1, 0, 0)$, and $(1, 1, 1)$. This gives the desired polarization.

The relations between $Z(W)$ and $Z(W^{\pm})$ simplify in the case of the OEC. Let W be an OEC with erasure shape $\varepsilon = (\varepsilon_0, \varepsilon_1, \varepsilon_2, \varepsilon_3)$. Then the quantities $Z_v(W^{\pm})$ and $Z_v(W)$ are related by

$$
\begin{aligned}
Z_1(W^+) &= \big(Z_1(W)\big)^2,\\
Z_2(W^+) &= Z_2(W)Z_3(W),\\
Z_3(W^+) &= \frac{1}{2}\big(Z_2(W)Z_3(W) + (Z_3(W))^2\big)
\end{aligned}
$$

and

$$
\begin{aligned}
Z_1(W^-) &= 2Z_1(W) - \big(Z_1(W)\big)^2,\\
Z_2(W^-) &= Z_2(W) + Z_3(W) - Z_2(W)Z_3(W),\\
Z_3(W^-) &= \frac{1}{2}\big((Z_2(W))^2 + Z_2(W) + 3Z_3(W) - 3Z_2(W)Z_3(W)\big).
\end{aligned}
$$

Note that the newly obtained channels are not OECs so in the next step of the transformation, some of equalities will be replaced with inequalities.

Generalizing the above idea, we can find a mapping which removes some of the intermediate extremal configurations that do not necessarily located on adjacent levels. For instance,

suppose that we would like to remove levels from $(r-j_2)$ to $(r-i_2)$ and from $(r-j_1)$ to $(r-i_1)$, $1 \le i_1 \le j_1$, $i_2 \le j_2 \le r-1$, and $j_1+1 < i_2$. In this case, random variables $(Z_{i_1,n}, \ldots, Z_{j_1+1,n})$ converge to the same random variable, and so do random variables $(Z_{i_2,n}, \ldots, Z_{j_2+1,n})$. Thus, we need a permutation π_{q_1} with $q_1 = 2^{j_1-i_1+2}$ for removing $(j_1 - i_1 + 1)$ consecutive levels starting with the $(r-j_1)$th one, and a permutation π_{q_2} with $q_2 = 2^{j_2-i_2+2}$ that removes levels from $(r-j_2)$ to $(r-i_2)$. The permutation π is given by:

$$\pi(u_1) = \begin{cases} q_1^{(j)} \cdot \pi_{q_1}\big(\frac{u_1-u_1^{(j)}}{q_1^{(j)}}\big) + \pi^{(2)}(u_1 - u_1^{(j)}), & \text{if } u < q_1^{(i)} \\ \pi(u_1^{(i)}) + (u_1 - u_1^{(i)}), & \text{if } q_1^{(i)} \le u_1 \le q_1^{(j)} \end{cases}$$

where $q_1 = 2^{j_1-i_1+2}$, $q_1^{(i)} = 2^{r-i_1+1}$, $q_1^{(j)} = 2^{r-j_1-1}$, $u_1^{(j)} = u_1 \mod q_1^{(j)}$, and $u_1^{(i)} = u_1 \mod q_1^{(i)}$. Further, $\pi^{(2)}$ is a permutation from $[q_1^{(j)}]$ to $[q_1^{(j)}]$ with

$$\pi^{(2)}(u_2) = \begin{cases} q_2^{(j)} \cdot \pi_{q_2}\big(\frac{u_2-u_2^{(j)}}{q_2^{(j)}}\big) + (u_2 - u_2^{(j)}), & \text{if } u_2 < q_2^{(i)} \\ \pi(u_2^{(i)}) + (u_2 - u_2^{(i)}), & \text{if } q_2^{(i)} \le u_2 < q_2^{(j)} \end{cases}$$

where $q_2 = 2^{j_2-i_2+2}$, $q_2^{(i)} = 2^{r-i_2+1}$, $q_2^{(j)} = 2^{r-j_2-1}$, $u_2^{(j)} = u_2 \mod q_2^{(j)}$, and $u_2^{(i)} = u_2 \mod q_2^{(i)}$. Finally, π_{q_1} and π_{q_2} are permutations that satisfy condition (4.27) with q replaced with q_1 and q_2, respectively.

Let us consider the following example.

Example 4.2 *Let $q = 16$ and suppose that we would like to remove the 1st and the 3rd levels from the set of 5 extremal configurations. Construct the following mapping: $g(u_1, u_2) = u_1 + \pi(u_2)$. where π is given above with $q = 16$, $i_1 = j_1 = 1$, and $i_2 = j_2 = 3$. The first row of the Cayley table G is* $[10\ 8\ 11\ 9\ 2\ 0\ 3\ 1\ 14\ 12\ 15\ 13\ 6\ 4\ 7\ 5]$.

To analyze this example, consider the cases of following the + and the - paths. For the + case, the quantity $Z_{v,n+1}$ with $v \in \mathcal{X}_1 \cup \mathcal{X}_2$ is a sum of the multiples of $Z_{\{x,x'\},n}$ and of $Z_{v',n}$ where $v' \in \mathcal{X}_1 \cup \mathcal{X}_2$ and $d_r(x,x') \le 2$. The same is true for $Z_{v,n+1}$ with $v \in \mathcal{X}_3 \cup \mathcal{X}_4$ with $v' \in \mathcal{X}_3 \cup \mathcal{X}_4$ and $d_r(x,x') \ge 3$. In addition, by Proposition 4.7, $wt_r(u_1 - u_2) \ge 3$ if and only if $wt_r(\pi(u_1) - \pi(u_2)) \ge 3$. This implies that, in the - case, each term of $Z_{v,n+1}, v \in \mathcal{X}_3 \cup \mathcal{X}_4$ can be bounded above by $qZ_{v',n}, wt_r(v') \ge 3$. In summary, we obtain

$$Z^{[3,4]}_{\max,n+1} \le \big(Z^{[3,4]}_{\max,n}\big)^2$$

with probability $1/2$ and

$$Z^{[3,4]}_{\max,n+1} \le (q^2 - q + 1) Z^{[3,4]}_{\max,n}$$

with probability $1/2$. This proves the almost sure convergence of $Z^{[3,4]}_{\max,n}$ to a Bernoulli $(0,1)$-valued random variable $Z^{[3,4]}_{\max,\infty}$. As before, we only need to check the case of $Z^{[3,4]}_{\max,\infty} = 1$, which means $Z^{(3)}_{\max,\infty} = 1$. Since the equation for Z^{+}_{0010} contains the quantity $Z_{s,n}$ with $wt_r(s) = 4$, $Z^{(4)}_{\max,\infty}$ is also 1 and thus all the random variables $Z_{v,n}$ with $v \in \mathcal{X}_3 \cup \mathcal{X}_4$ converge a.s. to the same random variable. Repeating the above argument, $Z^{[1,4]}_{\max,n}$ also converges a.s. to a $(0,1)$-valued random variable.

Thus what we have so far is the following: $(Z^{[1,4]}_{\max,\infty}, Z^{[3,4]}_{\max,\infty}) = (0,0), (1,0), (1,1)$. The first and the third cases are clear. If the second case happens, by the definition of $Z^{[1,4]}_{\max,\infty}$,

$Z^{[1,2]}_{\max,\infty} = 1$ *which implies that* $Z^{(1)}_{\max,\infty} = 1$ *and from the equation for* Z^{+}_{1000} *both* $Z^{(1)}_{\max,\infty}$ *and* $Z^{(2)}_{\max,\infty}$ *become* 1. *Therefore* $Z_{i,n}$ *converges a.s. to* $Z_{i,\infty}$, $i = 1,2,3,4$ *where the vector* $(Z_{1,\infty}, Z_{2,\infty}, Z_{3,\infty}, Z_{4,\infty})$ *takes one of the following vectors:* $(0,0,0,0)$, $(1,1,0,0)$, *and* $(1,1,1,1)$ *and the first and the third levels are removed.*

We conclude by formulating the main result of this section.

Theorem 4.8 *Let* $q = 2^r$ *and let* m *be an integer. Fix a set of indices* $\{i_1, j_1, \ldots, i_m, j_m\} \subset \{0,1,\ldots,r\}$, *where* $i_1 \geq 1$, $i_s \leq j_s < i_{s+1} - 1$, $s = 1,\ldots,m$ *and* $i_{m+1} = r+1$. *Define the mapping* g *by*

$$g : (u_1, u_2) \mapsto u_1 + \pi^{(1)}(u_2) \mod q$$

where the permutation $\pi^{(1)}$ *is defined in the following.*

(a) Let $q_s = 2^{j_s - i_s + 2}$, $q_s^{(i)} = 2^{r - i_s + 1}$, $q_s^{(j)} = 2^{r - j_s - 1}$, $u_s^{(i)} = u_s \mod q_s^{(i)}$, *and* $u_s^{(j)} = u_s \mod q_s^{(j)}$.

(b) Define the permutations $\pi_{q_s} : [q_s] \to [q_s]$, $s = 1,\ldots,m$ *so that they satisfy condition (4.27).*

(c) Define the permutations $\pi^{(s)} : [q_{s-1}^{(j)}] \to [q_{s-1}^{(j)}], q_0^{(j)} = q, s = 1,\ldots,m$ *by the following equalities. If* $s = m$ *then*

$$\pi^{(m)}(u_m) = \begin{cases} q_m^{(j)} \cdot \pi_{q_m}(\frac{u_m - u_m^{(j)}}{q_m^{(j)}}) + (u_m - u_m^{(j)}), & \text{if } u_m < q_m^{(i)} \\ \pi(u_m^{(i)}) + (u_m - u_m^{(i)}), & \text{if } q_m^{(i)} \leq u_m < q_m^{(j)} \end{cases}$$

If $s = 1,\ldots,m-1$, *then*

$$\pi^{(s)}(u_s) = \begin{cases} q_s^{(j)} \cdot \pi_{q_s}(\frac{u_s - u_s^{(j)}}{q_s^{(j)}}) + \pi^{(s+1)}(u_s - u_s^{(j)}), & \text{if } u_s < q_s^{(i)} \\ \pi(u_s^{(i)}) + (u_s - u_s^{(i)}), & \text{if } q_s^{(i)} \leq u_s < q_s^{(j)} \end{cases}.$$

Then the mapping g *removes* m *disjoint sets of consecutive extremal configurations. More specifically, the random variables* $Z_{i,n}, i = 1,\ldots,r$ *converge a.s. to* $(0,1)$*-valued random variables,* $Z_{i,\infty}$. *Furthermore, with probability* 1 *the vector* $(Z_{i,\infty}, i = 1,\ldots,r)$ *takes one of the values in the set* $\left\{(1^k 0^{r-k}) : k \in \{0,1,\ldots,r\} \setminus \left(\bigcup_{s=1}^{m}\{i_s,\ldots,j_s\}\right)\right\}$.

The basic idea of the proof of this theorem is presented in Example 4.2. The only difference between the above permutation g and the permutation used in Theorem 4.7 is in using $\pi^{(s)}, s = 2,\ldots,m$ instead of modulo-q addition. Therefore, the proof of convergence of $Z_{i,n}$ is a simple extension of the proof of Theorem 4.7 and is omitted here.

Appendix: Proof of Lemma 4.2

We shall break the expression for $I(W)$ into a sum of symmetric capacities of B-DMCs.

Let $z = (z_1,\ldots,z_k)$ be a k-tuple of symbols from $\mathcal{X}$. Define the probability distribution $P(y|z) = \frac{1}{k}\sum_{i=1}^{k} W(y|z_i)$. Define a B-DMC $W^{(k)}_{\{z^{(1)},z^{(2)}\}} : \mathcal{X}^k \to \mathcal{Y}$ with inputs $z^{(i)} \in \mathcal{X}^k$, where the transition $z^{(i)} \to y$ is given by $P(y|z^{(i)})$, $i = 1,2$.

Lemma 4.11 *The Bhattacharyya parameter of the channel* $W^{(k)}_{\{z^{(1)},z^{(2)}\}}$, *where* $z^{(1)} = (x_1,\ldots,x_k)$, $z^{(2)} = (x_{k+1},\ldots,x_{2k})$, *can be lower bounded by*

$$Z(W^{(k)}_{\{z^{(1)},z^{(2)}\}}) \geq \frac{1}{k}\sum_{j=1}^{k} Z(W_{\{x_j, x_{f(j)}\}}) \tag{4.33}$$

for any f which is a one-to-one mapping from the set $\{1, 2, \ldots, k\}$ to $\{k+1, \ldots, 2k\}$.

Proof: For brevity denote $w_{i,y} = W(y|x_i)$. We have

$$Z(W^{(k)}_{\{z^{(1)}, z^{(2)}\}}) = \frac{1}{k} \sum_y \sqrt{\Big(\sum_{i=1}^{k} w_{i,y}\Big)\Big(\sum_{i'=k+1}^{2k} w_{i',y}\Big)},$$

while the right hand side of (4.33) is

$$\frac{1}{k}\sum_{i=1}^{k} Z(W_{\{x_i, x_{f(i)}\}}) = \frac{1}{k}\sum_y \sum_{i=1}^{k} \sqrt{w_{i,y} w_{f(i),y}}.$$

The Cauchy-Schwartz inequality gives us

$$\Big(\sum_{i=1}^{k} w_{i,y}\Big)\Big(\sum_{i'=k+1}^{2k} w_{i',y}\Big) \geq \Big(\sum_{i=1}^{k} \sqrt{w_{i,y} w_{f(i),y}}\Big)^2$$

hence the lemma. ∎

Let us introduce some notation. Given $z = (z_1, \ldots, z_k) \in \mathcal{X}^k$, let $z \oplus x = (z_1 \oplus x, \ldots, z_k \oplus x)$ where $x \in \mathcal{X}$ and $\oplus$ is a bit-wise modulo-2 summation. In the next lemma we consider B-DMCs

$$W^{(k)}_{\{z_m^{(1)}, z_m^{(2)}\}} : \mathcal{X}^k \to \mathcal{Y}, \quad k = 2^{m-1}, m = 1, \ldots, r$$

with inputs of special form. Namely, for a given m we let

$$z_m^{(1)} = (x_1 \oplus \sum_{i=2}^{m} a_i x_i \mid (a_2, \ldots, a_m) \in \{0,1\}^{m-1});$$

for instance, $z_1^{(1)} = x_1$; $z_2^{(1)} = (x_1, x_1 \oplus x_2)$; $z_3^{(1)} = (x_1, x_1 \oplus x_2, x_1 \oplus x_3, x_1 \oplus x_2 \oplus x_3)$, etc. Finally, $z_m^{(2)} = z_m^{(1)} \oplus x_{m+1}$.

For $m = 0, 1, \ldots, r-1$ introduce the set $\mathcal{A}_{m+1} \subset \mathcal{X}^{m+1}$ as follows:

$$\mathcal{A}_{m+1} = \Big\{(x_1, \ldots, x_{m+1}) \in \mathcal{X}^{m+1} \Big| x_1 \in \mathcal{X};$$
$$(x_2, \ldots, x_{m+1}) \text{ are linearly independent as vectors over } \mathbb{F}_2\Big\}.$$

Then the cardinality of the above set is

$$|\mathcal{A}_{m+1}| = 2^r \prod_{j=0}^{m-1} (2^r - 2^j).$$

The concepts and notation introduced above are needed to establish a decomposition of the quantity $I(W)$ into a sum of capacities of B-DMCs. This is done in the following technical lemma.

Lemma 4.12

$$I(W) = \sum_{m=1}^{r} \frac{1}{|\mathcal{A}_{m+1}|} \sum_{(x_1, \ldots, x_{m+1}) \in \mathcal{A}_{m+1}} I(W^{(k)}_{\{z_m^{(1)}, z_m^{(2)}\}}) \tag{4.34}$$

where the number k, the vectors $z_m^{(1)}, z_m^{(2)}$, and the set $\mathcal{A}_{m+1}$ are defined before the lemma.

Proof: First we express the capacity of W as the sum of symmetric capacities of B-DMCs.

$$\begin{aligned}
I(W) &= \frac{1}{2^r}\sum_x\sum_y W(y|x)\log\frac{W(y|x)}{P(y)} \\
&= \frac{1}{2^r}\sum_y\frac{1}{2(2^r-1)}\sum_{x_1}\sum_{x_2:x_2\neq 0}\Big(W(y|x_1)\log\frac{W(y|x_1)}{P(y)} \\
&\qquad + W(y|x_1\oplus x_2)\log\frac{W(y|x_1\oplus x_2)}{P(y)}\Big) \\
&= \frac{1}{2^r(2^r-1)} \\
&\cdot\sum_y\sum_{\substack{x_1,x_2\\ x_2\neq 0}}\Big(\frac{1}{2}W(y|x_1)\log\frac{W(y|x_1)}{\frac{1}{2}(W(y|x_1)+W(y|x_1\oplus x_2))} \\
&\quad + \frac{1}{2}W(y|x_1\oplus x_2)\log\frac{W(y|x_1\oplus x_2)}{\frac{1}{2}(W(y|x_1)+W(y|x_1\oplus x_2))} \\
&\quad + \frac{1}{2}(W(y|x_1)+W(y|x_1\oplus x_2))\log\frac{\frac{1}{2}(W(y|x_1)+W(y|x_1\oplus x_2))}{P(y)}\Big) \\
&= \frac{1}{2^r(2^r-1)}\Big\{\sum_{\substack{x_1,x_2\\ x_2\neq 0}} I(W_{\{x_1,x_1\oplus x_2\}}) + T_2\Big\}
\end{aligned}$$

where

$$T_2 = \sum_y\sum_{\substack{x_1,x_2\\ x_2\neq 0}}\frac{1}{2}(W(y|x_1)+W(y|x_1\oplus x_2))\log\frac{\frac{1}{2}(W(y|x_1)+W(y|x_1\oplus x_2))}{P(y)}\Big\}.$$

We will apply the same technique repeatedly. In the next step we add another sum, this time on x_3 which has to satisfy the conditions $x_3\neq 0, x_3\neq x_2$. Writing x_1^3 for x_1,x_2,x_3, we have

$$\begin{aligned}
T_2 &= \sum_y\frac{1}{2(2^r-2)}\sum_{x_1^3\in\mathcal{A}_3}\Big(\frac{1}{2}(W(y|x_1)+W(y|x_1\oplus x_2))\log\frac{\frac{1}{2}(W(y|x_1)+W(y|x_1\oplus x_2))}{P(y)} \\
&\quad + \frac{1}{2}(W(y|x_1\oplus x_3)+W(y|x_1\oplus x_2\oplus x_3)) \\
&\qquad \cdot\log\frac{\frac{1}{2}(W(y|x_1\oplus x_3)+W(y|x_1\oplus x_2\oplus x_3))}{P(y)}\Big) \\
&= \frac{1}{2^r-2}\sum_y\sum_{x_1^3\in\mathcal{A}_3}\Big(\frac{1}{2}\cdot\frac{1}{2}(W(y|x_1)+W(y|x_1\oplus x_2))\log\frac{\frac{1}{2}(W(y|x_1)+W(y|x_1\oplus x_2))}{B} \\
&\quad + \frac{1}{2}\cdot\frac{1}{2}(W(y|x_1\oplus x_3)+W(y|x_1\oplus x_2\oplus x_3)) \\
&\qquad \cdot\log\frac{\frac{1}{2}(W(y|x_1\oplus x_3)+W(y|x_1\oplus x_2\oplus x_3))}{B}\Big) + B\log\frac{B}{P(y)}
\end{aligned}$$

where $B = \frac{1}{4}(W(y|x_1)+W(y|x_1\oplus x_2)+W(y|x_1\oplus x_3)+W(y|x_1\oplus x_2\oplus x_3))$.

By now it is clear what we want to accomplish. Let us again take the sum on y inside. Recalling the definition of the channel $W^{(k)}$ before Lemma 4.11, we obtain

$$T_2 = \frac{1}{2^r - 2}\left\{ \sum_{x_1^3 \in \mathcal{A}_3} I(W^{(2)}_{\{z_2^{(1)}, z_2^{(2)}\}}) + T_3 \right\};$$

here $I(W^{(2)}_{\{z_2^{(1)}, z_2^{(2)}\}})$ is the symmetric capacity of the B-DMC $W^{(2)}_{\{z_2^{(1)}, z_2^{(2)}\}}$ with $z_2^{(1)} = \{x_1, x_1 \oplus x_2\}$ and $z_2^{(2)} = \{x_1 \oplus x_3, x_1 \oplus x_2 \oplus x_3\}$, and T_3 is the term remaining in the expression for T_2 upon isolating this capacity:

$$T_3 = \sum_y \sum_{x_1^3 \in \mathcal{A}_3} B \log \frac{B}{P(y)}.$$

Now repeat the above trick for T_3, namely, average over all the linear combinations that this time include the vector x_4 and isolate the symmetric capacity of the channel $W^{(4)}$ that arises. Proceeding in this manner, we obtain

$$\begin{aligned} I(W) &= \frac{1}{2^r(2^r-1)} \sum_{\substack{x_1, x_2 \\ x_2 \neq 0}} I(W_{\{x_1, x_1 \oplus x_2\}}) + \frac{1}{2^r(2^r-1)(2^r-2)} \sum_{x_1^3 \in \mathcal{A}_3} I(W^{(2)}_{\{z_2^{(1)}, z_2^{(2)}\}}) \\ &\quad + \frac{1}{2^r(2^r-1)(2^r-2)} \sum_y \sum_{x_1^3 \in \mathcal{A}_3} B \log \frac{B}{P(y)} \\ &= \dots \\ &= \sum_{m=1}^{r} \frac{1}{|\mathcal{A}_{m+1}|} I(W^{(k)}_{\{z_m^{(1)}, z_m^{(2)}\}}) \end{aligned}$$

where the notation $z_m^{(1)}, z_m^{(2)}, \mathcal{A}_{m+1}$ is introduced before the statement of lemma. ■

We continue with the proof of inequality (4.11). For this, we will need to bound above the right-hand side of (4.34). This is accomplished by grouping the terms of the sum according to the weights of symbols in $\mathcal{A}_{m+1}$ for all $m = 1, \dots, r$. First we handle the case $m = 1$ which is easy.

Fact 4.1 *The term with* $m = 1$ *in* (4.34) *equals*

$$\frac{1}{2^r - 1} \sum_{d=1}^{r} 2^{d-1} \sqrt{1 - Z_d^2}.$$

Proof: We have

$$\begin{aligned} I(W) &= \frac{1}{2^r(2^r-1)} \sum_{\substack{x_1, x_2 \\ x_2 \neq 0}} I(W_{\{x_1, x_1 \oplus x_2\}}) \\ &\leq \frac{1}{2^r(2^r-1)} \sum_{\substack{x_1, x_2 \\ x_2 \neq 0}} \sqrt{1 - Z(W_{\{x_1, x_1 \oplus x_2\}})^2} \\ &= \frac{1}{2^r(2^r-1)} \sum_{\substack{x_1, x_2 \\ x_2 \neq 0}} \sqrt{1 - Z(W_{\{x_1, x_1 + x_2\}})^2} \\ &= \frac{1}{2^r(2^r-1)} \sum_{d=1}^{r} \sum_{\substack{x_1, x_2 \\ \mathrm{wt}_r(x_2) = d}} \sqrt{1 - Z(W_{\{x_1, x_1 + x_2\}})^2} \end{aligned}$$

In the first step we used the relation between the symmetric capacity and the Bhattacharyya parameter of B-DMCs [3], and in the second replaced bitwise addition with modulo-q addition. This is possible because as x_1, x_2 range over $\mathcal{X}$ with $x_2 \neq 0$, the pair $\{x_1, x_1 \oplus x_2\}$ takes all the possible $q(q-1)$ values, and the same is true for the pair $\{x_1, x_1 + x_2\}$. Now use convexity to continue as follows:

$$I(W) \leq \frac{1}{2^r(2^r-1)} \sum_{d=1}^{r} 2^{r+d-1} \sqrt{1 - \left(\frac{1}{2^{r+d-1}} \sum_{\substack{x_1, x_2 \\ \mathrm{wt}_r(x_2)=d}} Z(W_{\{x_1, x_1+x_2\}}) \right)^2}$$

Together with (4.7) this completes the proof. ■

The main reason for isolating the above case is to highlight the change from $\oplus$ to $+$. We will use the same trick in the general case which we discuss next. It turns out that (4.34) can be decomposed in a similar way for all $m, 1 \leq m \leq r$. Again we would like to group the terms according to the weights of the symbols in $\mathcal{A}_{m+1}$. There is more than one way to do this, and not every such grouping gives the needed result. We will identify a way of arranging the sum (4.34) that yields the following representation:

Lemma 4.13

$$\begin{aligned} I(W) &= \sum_{m=1}^{r} \frac{1}{|\mathcal{A}_{m+1}|} \sum_{(x_1,\ldots,x_{m+1}) \in \mathcal{A}_{m+1}} I(W^{(k)}_{\{z_m^{(1)}, z_m^{(2)}\}}) \\ &\leq \sum_{m=1}^{r} \frac{2^r}{|\mathcal{A}_{m+1}|} \sum_{d=1}^{r} \lambda_{d,m} \sqrt{1 - Z_d^2}, \end{aligned} \tag{4.35}$$

where $\lambda_{d,m} = \Lambda_{d,m} - \Lambda_{d-1,m}$ *with*

$$\Lambda_{0,m} = 0$$

and

$$\begin{aligned} \Lambda_{d,m} = (2^d - 1) \prod_{i=1}^{m-1} (2^r - 2^i) + (2^r - 2^d) \sum_{t=1}^{d} \frac{(-1)^{t-1}}{2^{\binom{t}{2}}} \\ \cdot \Big(\prod_{i=0}^{t-1} (2^d - 2^i)(2^{m-1} - 2^i) \Big) \Big(\prod_{j=t+1}^{m-1} (2^r - 2^j) \Big) \end{aligned}$$

for all $d, m = 1, \ldots, r$, $t = 1, \ldots, d$.

Additionally, we have

Fact 4.2 *Let* r *be fixed. Then for all* $d = 1, \ldots, m$

$$\sum_{m=1}^{r} \Lambda_{d,m} \prod_{j=1}^{m} (2^r - 2^{j-1})^{-1} = d$$

Hence $\sum_{m=1}^{r} \lambda_{d,m} \prod_{j=1}^{m} (2^r - 2^{j-1})^{-1} = 1$.

Example: E.g., for $r = 3$ we obtain (letting $\zeta_i = \sqrt{1 - Z_i^2}$):

$$\begin{aligned} I(W) &= \frac{1}{8 \cdot 7} \sum_{\mathcal{A}_2} I(W_{\{x_1, x_1 \oplus x_2\}}) + \frac{1}{8 \cdot 7 \cdot 6} \sum_{\mathcal{A}_3} I(W^{(2)}_{\{z_2^{(1)}, z_2^{(2)}\}}) \\ &\quad + \frac{1}{8 \cdot 7 \cdot 6 \cdot 4} \sum_{\mathcal{A}_4} I(W^{(3)}_{\{z_3^{(1)}, z_3^{(2)}\}}) \\ &\leq \frac{1}{7}(\zeta_1 + 2\zeta_2 + 4\zeta_3) + \frac{1}{7 \cdot 6}(12\zeta_1 + 18\zeta_2 + 12\zeta_3) \\ &\quad + \frac{1}{7 \cdot 6 \cdot 4}(96\zeta_1 + 48\zeta_2 + 24\zeta_3) \\ &= \zeta_1 + \zeta_2 + \zeta_3. \end{aligned}$$

Proof of Lemma 4.13 (outline): The proof of Lemma 4.13 amounts to counting of the number of terms of a given weight d. We proceed as follows. We would like to use Lemma 4.11 so that for given $z_m^{(1)}, z_m^{(2)}$, every term on the right-hand side of (4.33) satisfies $d_r(x_j, x_{f(j)}) = d$ for some fixed value d. Choose a map $f : \{1, \ldots, k\} \to \{k+1, \ldots, 2k\}$ such that the symbol

$$a_s(z_m^{(1)}, z_m^{(2)}) = (z_m^{(1)})_s \oplus (z_m^{(2)})_{f(s)},\ s = 1, \ldots, 2^{m-1}$$

is the same for all s. Such maps exist because of the way we defined $z_m^{(i)}, i = 1, 2$. For instance, one possible choice is $f(i) = k + i, i = 1, \ldots, k$; then $a_s = z_{m+1}$ for all s. Moreover, we will assume that f is chosen such that the weight $\mathrm{wt}_r(a_s(z_m^{(1)}, z_m^{(2)}))$ is the smallest among all the possible matchings between $\{1, \ldots, k\}$ and $\{k+1, \ldots, 2k\}$ (this choice depends on the values $x_1, x_2, \ldots, x_{m+1}$ used to construct $z_m^{(1)}, z_m^{(2)}$). In the following, when the values $x_1, x_2, \ldots, x_{m+1}$ are implied, we will write simply a instead of $a_s(z_m^{(1)}, z_m^{(2)})$.

By construction, given $x_1, x_2, \ldots, x_{m+1}$, we observe that the symbol $(z_m^{(1)})_s \oplus (z_m^{(2)})_{f(s)}$ is one of the symbols $x_{m+1} \oplus \sum_{i=2}^m \alpha_i x_i$, where $\alpha_i \in \{0, 1\}$ for all i. Note that x_{m+1} is always present because it is a part of every entry of $z_m^{(2)}$, and that x_1 appears in each entry of both $z_m^{(1)}$ and $z_m^{(2)}$ and is therefore absent from their sum.

Let $1 \leq d \leq r$. Let us find the number of possible assignments of $x_1, x_2, \ldots, x_{m+1} \in \mathcal{A}_{m+1}$ so that $\mathrm{wt}_r(a) \leq d$. We consider two cases. First, suppose that $\mathrm{wt}_r(x_{m+1}) \leq d$. Then for any assignment of $x_2, \ldots, x_m$ that together with x_{m+1} are linearly independent (as vectors over $\mathbb{F}_2$), there exists at least one symbol of the form $x_{m+1} \oplus \sum_{i=2}^m \alpha_i x_i$ of weight $\leq d$, and thus $\mathrm{wt}_r(a)$ is also $\leq d$. The total number of possibilities, including x_1, becomes $2^r(2^d - 1)\prod_{i=1}^{m-1}(2^r - 2^i)$.

Now let $x_{m+1} \in \mathcal{X}$ be such that $\mathrm{wt}_r(x_{m+1}) > d$, and note that there are $2^r - 2^d$ such choices. To count the number of assignments of $x_1, x_2, \ldots, x_{m+1}$ let us first fix x_{m+1}. The counting is done by first finding the number of assignments such that the weight of a is $\leq d$ for all d, and then finding the needed number by subtracting the results for d and $d - 1$.

As before, there are 2^r possibilities for x_1. Next, let $y_1, \ldots, y_s \in \mathcal{X}$ be distinct symbols. We are interested in the number of choices for $x_2, \ldots, x_m$ such that s of the 2^{m-1} symbols of the form $\sum_{j=2}^m \alpha_j^{(i)} x_j$ satisfy the condition

$$x_{m+1} \oplus \sum_{j=2}^m \alpha_j^{(i)} x_j = y_i,$$

where $\alpha_j^{(i)} \in \{0, 1\}, j = 2, \ldots, m$ and $\mathrm{wt}(y_i) \leq d$ for all $i = 1, \ldots, s$. Of these constraints, a certain number $t, 1 \leq t \leq d$ are linearly independent over $\mathbb{F}_2$. Fixing $y_i, i = 1, \ldots, s$ and $(\alpha_j^{(i)}), j =$

$2, \ldots, m$ gives the values of some t symbols among $x_2, \ldots, x_m$, and there are $\prod_{j=t+1}^{m-1}(2^r - 2^j)$ choices of the remaining $m - 1 - t$ symbols. Moreover, there are $\prod_{i=0}^{t-1}(2^{m-1} - 2^i)$ choices of the coefficients $\alpha_j^{(i)}$ and $\prod_{i=0}^{t-1}(2^d - 2^i)$ choices for the symbols y_i. Accounting for these possibilities, and performing an inclusion-exclusion argument, we find that the number of assignments of $x_2, \ldots, x_m$ equals

$$\sum_{t=1}^{d} \frac{(-1)^{t-1}}{2^{\binom{t}{2}}} \Big(\prod_{i=0}^{t-1} (2^d - 2^i)(2^{m-1} - 2^i) \Big) \Big(\prod_{j=t+1}^{m-1} (2^r - 2^j) \Big).$$

Together with the case $\mathrm{wt}_r(x_{m+1}) \leq d$ above we obtain the number of choices of linearly independent symbols $x_1, x_2, \ldots, x_{m+1}$ such that the weight of a is $\leq d$, which is given by $2^r \Lambda_{d,m}$. Finally, the number of choices with weight $\mathrm{wt}_r(a) = d$ is

$$2^r \lambda_{d,m} = 2^r (\Lambda_{d,m} - \Lambda_{d-1,m}).$$

This concludes the proof. ■

The proof of the inequality (4.11) can now be completed by interchanging the order of summation in (4.35) and taking account of Fact A2.

Remark: It is possible to remove the restriction of linear independence from the definition of $\mathcal{A}_{m+1}$; however then the counting problem tackled in Lemma 4.13 is shifted to Lemma 4.12, so there is no gain in doing so.

Chapter 5
Summary and Open Problems

This thesis is devoted to problems in information theory motivated by a communication system modeled as transmission over dependent parallel channels. We examine combinatorial and linear-algebraic aspects of coding schemes as well as several information-theoretic aspects of transmission. Many of our considerations are unified by the concept of ordered metrics on the set of q-ary strings. Ordered metric spaces form a starting point in our study of linear codes in the first part of the thesis and lead to simple models of ordered discrete memoryless channels. The ordered weight also plays an important role in results on polar codes in the last part of the thesis.

Combinatorial and linear-algebraic aspects of linear ordered codes are considered in Chapter 2. The contributions of this chapter are related to the idea of multivariate polynomial invariants of linear codes. In particular, we introduce the multivariate rank enumerator of the code and observe its close relation to the multivariate Tutte polynomial of matroids considered in earlier works. As a by-product of these considerations, we obtain a linear-algebraic proof of the MacWilliams theorem for ordered codes, which previously was proved using harmonic analysis. We also extend the concept of the rank enumerator to the distribution of support weights of a linear code and link them to a model of the wiretap channel that we extend to the ordered context.

In the classical case of codes in the Hamming space, there is a straightforward connection between linear codes and vector matroids on the set of code coordinates. Attempting to extend this connection to the ordered metric space, we are able to associate poset matroids with maximum distance separable codes (ordered MDS codes). At the same time, we were not able to establish a universal connection between poset matroids and ordered codes because linear dependence between code's coordinates does not follow the partial ordering. Establishing a firmer connection between ordered codes and some form of poset matroids remains an interesting challenge for future research.

The consideration of communication channels in the first part of the thesis is furthered in Chapter 3 where we introduce simple models of parallel channels that are related to the ordered metric. We show that the behavior of the transition probability is monotone if the error vectors are comparable with respect to the partial order that defines the metric. Capacity of these channels is attained by linear ordered codes. We also extend the definitions to the case of ordered wiretap channels, compute capacity in simple examples, and describe a connection between them and linear ordered codes. In particular, we show that generalized poset weights of linear codes arise naturally in the combinatorial model of the wiretap channel.

The last part of the thesis is devoted to polar codes. The polar coding scheme is a major recent advance in information theory related to explicit methods of achieving Shannon capacity of symmetric memoryless channels [4]. The starting point of the research reported in Chapter 4 is an attempt to construct polar codes for ordered channels. This leads us to a study of polar coding for

general nonbinary memoryless channels with inputs of size $q = 2^r, r \geq 2$. We find that a variant of the basic polar coding scheme supports transmission at rates close to capacity of symmetric q-ary channels, although unlike the binary case, the data symbols are not necessarily perfectly decoded or completely random, as is the case for binary channels. Instead, symbols are grouped into subsets that carry almost noiselessly $1, 2, \ldots, r$ bits of the symbol. An interesting monotonicity relation between the symbols enables us to obtain a concise description of the extremal configurations that is fully described through the Bhattacharyya parameters of the channel. Extending the work in [4], we also estimate the error probability of decoding of q-ary polar codes under a simple recursive decoding procedure.

A second line of work in Chapter 4 is related to our attempt to gain better control over the arising extremal configurations in q-ary channels. We describe code constructions in which the data symbols polarize into any k levels of our choosing, including two-level polarization recently established in [60]. Our approach, which also gives a new proof of the result in [60], is based on the evolution of the Bhattacharyya parameters. As an application of these results, we describe the use of polar codes for encoding of picture data of different types in the MPEG-2 and H.264/MPEG-4 video standards.

Bibliography

[1] E. Abbe and E. Telatar, "Polar codes for the m-user multiple access channel," *IEEE Trans. Inform. Theory*, vol. 58, no. 8, pp. 5437-5448, 2012.

[2] E. Abbe, "Mutual information, matroids and extremal dependencies," arXiv:1012.4755.

[3] E. Arıkan, "Channel polarization: a method for constructing capacity-achieving codes for symmetric binary-input memoryless channels," *IEEE Trans. Inform. Theory*, vol. 55, no. 7, pp. 3051–3073, 2009.

[4] E. Arıkan and E. Telatar, "On the rate of channel polarization," in *Proc. 2009 IEEE International Symposium on Information Theory, Seoul, Korea, June 28-July 3, 2009*, pp. 1493–1495.

[5] A. Ashikhmin and A. Barg, "Binomial moments of the distance distribution: Bounds and applications", *IEEE Trans. Inform. Theory*, vol. 45, no. 2, pp. 438-452, 1999.

[6] A. Barg, "The matroid of supports of a linear code", *Applicable Algebra Eng. Commun. Comput.*, vol. 8, pp. 165-172, 1997.

[7] A. Barg and P. Purkayastha, "Bounds on ordered codes and orthogonal arrays", *Moscow Math. J.*, vol. 9, no. 2, pp. 211-243, 2009.

[8] A. Barg and P. Purkayastha, "Near-MDS poset codes and distributions", *Error-Correcting Codes, Cryptography and Finite Geometries (A. Bruen and D. Wehlau, eds.), Providence,RI: AMS*, pp. 135–147, 2010.

[9] A. Barg and M. Firer,"Translation association schemes and the shape enumerator of codes," *Proc. 2012 IEEE Interntational Sympos. on Information Theory (ISIT2012), Boston, MA, July 1-5, 2012*, pp.

[10] M. Barnabei, G. Nicoletti, and L. Pezzoli, "Matroids on partially ordered sets", *Adv. Appl. Math.*, vol. 21, pp. 78-112, 1998.

[11] J. Bierbrauer, "A direct approach to linear programming bounds for codes and tms-nets", *Des. Codes Cryptogr.*, vol. 42, pp. 127-143, 2007.

[12] T. Britz, "MacWilliams identities and matroid polynomials", *Electron. J. Combin.*, vol. 9(1), no. R19, 2002.

[13] T. Britz, "Code enumerators and Tutte polynomials", *IEEE Trans. Inform. Theory*, vol. 56, no. 9, pp. 4350-4358, 2010.

[14] A. E. Brouwer, A. M. Cohen, and A. Neumaier, *Distance-regular graphs*, Springer-Verlag, Berlin e. a., 1989.

[15] R. A. Brualdi, J. S. Graves, and K. M. Lawrence, "Codes with a poset metric", *Discrete Math.*, vol. 147, no. 1-3, pp. 57-72, 1995.

[16] Y. Chen and A. J. Han Vinck, "Secrecy coding for the binary symmetric wiretap channel", *Security and Communication Networks*, vol. 4, no. 8, pp. 966-978, 2011.

[17] H. H. Crapo, "The Tutte polynomial", *Aequationes Math.*, vol. 3, pp. 211-229, 1969.

[18] I. Csiszár and J. Körner, "Broadcast channels with confidential messages", *IEEE Trans. Inform. Theory*, vol. 24, no. 3, pp. 339-348, 1978.

[19] I. Csiszár and J. Körner, *Information theory: Coding theorems for discrete memoryless systems*, Cambridge University Press, 2nd ed., Cambridge, 2011.

[20] P. Delsarte, "An algebraic approach to the association schemes of coding theory", *Philips Res. Rep. Suppl.*, no. 10, pp. 1-97, 1973.

[21] P. Diaconis and D. Freedman, "Iterated random functions," *SIAM Review*, vol. 41, no. 1, pp. 45–76, 1999.

[22] M. van Dijk, "On a special class of broadcast channels with confidential messages", *IEEE Trans. Inform. Theory*, vol. 43, no. 2, pp. 712-714, 1997.

[23] R. L. Dobrushin, "Asymptotic bounds on error probability for transmission over DMC with symmetric transition probabilities," *Theory Probab. Appl.*, vol. 7, pp. 283-311, 1962.

[24] S. T. Dougherty and M. M. Skriganov, "MacWilliams duality and the Rosenbloom-Tsfasman metric", *Mosc. Math. J.*, vol. 2, no. 1, pp. 81-97, 2002.

[25] I. Duursma, "Combinatorics of the two-variable zeta function", *Finite Fields and Appl. Lecture Notes Comput. Sci.*, vol. 2948, pp. 109-136, 2004.

[26] P. Elias, "Coding for noisy channels", *IRE Convention Record, Part IV*, pp. 37-46, 1955.

[27] R. G. Gallager, *Information theory and reliable communication*, John Wiley & Sons, New York, 1968

[28] A. Ganesan and P. O. Vontobel, "On the existence of universally decodable matrices", *IEEE Trans. Inform. Theory*, vol. 53, no. 7, pp. 2572-2575, 2007.

[29] C. Greene, "Weight enumeration and the geometry of linear codes", *Stud. Appl. Math.*, vol. 55, pp. 119-128, 1976.

[30] S. Hassini, R. Mori, T. Tanaka, and R. Urbanke, "Rate-Dependent Analysis of the Asymptotic Behavior of Channel Polarization," arXiv:1110.0194.

[31] T. Helleseth, T. Kløve, J. Mykkeltveit, "The weight distribution of irreducible cyclic codes with block lengths $n_1((q^l-1)/N)$", *Discrete Mathematics*, vol. 18, pp. 179-211, 1977.

[32] J. Y. Hyun and H. K. Kim, "Maximum distance separable poset codes", *Des. Codes Cryptogr.*, vol. 28, no. 3, pp. 247-261, 2008.

[33] R. P. M. J. Jurrius and R. Pellikaan, "Extended and generalized weight enumerators", in *Proc. Int. Workshop on Coding and Crypto. WCC2009*, Bergen, Norway, pp. 76-91, 2009.

[34] N. Kaplan, "MacWilliams identities for m-tuple weight enumerators," arXiv:1205.1277.

[35] H. K. Kim and D. Y. Oh, "A classification of posets admitting the MacWilliams identity", *IEEE Trans. Inform. Theory*, vol. 51, no. 4, pp. 1424-1431, 2005.

[36] T. Kløve, "Support weight distribution of linear codes", *Discrete Math.*, vol. 106/107, pp. 311-316, 1992.

[37] S. B. Korada, E. Şaşoğlu, and R. Urbanke, "Polar codes: Characterization of exponent, bounds, and constructions," *IEEE Trans. Inform. Theory*, vol. 56, no. 12, pp. 6253–6264, 2010.

[38] L. B. Koralov and Y. G. Sinai, *Theory of Probability and Random Processes*, Berlin: Springer-Verlag, 2nd ed., 2007.

[39] D. Le Gall, "MPEG: A video compression standard for multimedia applications," *Commun. ACM,* vol. 34, no. 4, pp. 47-58, 1991.

[40] F. J. MacWilliams, "A theorem on the distribution of weights in a systematic code", *Bell Syst. Tech. J.*, vol. 42, pp. 79-94, 1963.

[41] F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes,* North-Holland, Amsterdam, 1991.

[42] W. J. Martin and D. R. Stinson, "Association scheme for ordered orthogonal arrays and (T,M,S)-nets", *Canad. J. Math.*, vol. 51, no. 2, pp. 326-346, 1999.

[43] J. L. Massey and S. Serconek, "Linear complexity of periodic sequence: a general theory", *Advances in cryptology-CRYPTO'96 (Santa Barbara, CA), Lecture Notes in Comput. Sci.*, vol. 1109, pp. 358-371, Springer, Berlin, 1996.

[44] U. M. Maurer and S. Wolf, "Information-theoretic key agreement: From weak to strong secrecy for free", *Lecture Notes in Comput. Sci.*, vol. 1807, pp. 351-368, Springer, Berlin, 2000.

[45] R. Mori and T. Tanaka, "Channel polarization on q-ary discrete memoryless channels by arbitrary kernels", in *Proc. 2010 IEEE International Symposium on Information Theory, Austin, TX, June 13-18, 2010*, pp. 894-898.

[46] H. Niederreiter, "Low-discrepancy point sets", *Monatsh. Math.*, vol. 102, no. 2, pp. 155-167, 1986.

[47] H. Niederreiter, "A combinatorial problem for vector spaces over finite fields", *Discrete Math.*, vol. 96, no. 3, pp. 221-228, 1991.

[48] R. R. Nielsen, "A class of Sudan-decodable codes", *IEEE Trans. Inform. Theory*, vol. 46, no. 4, pp. 1564-1572, 2000.

[49] A. de Oliveira Moura and M. Firer, "Duality for poset codes", *IEEE Trans. Inform. Theory*, vol. 56, no. 7, pp. 3180-3186, 2010.

[50] L. H. Ozarow and A. D. Wyner, "Wire-tap channel II", *AT&T Bell Labs Techn. J.*, vol. 63, no. 10, pp. 2135-2157, 1984.

[51] L. Panek, M. Firer, H. K. Kim and J. Y. Hyun, "Groups of linear isometries on poset structures", *Discrete Mathematics*, vol. 308, pp. 4116–4123, 2008.

[52] W. Park and A. Barg, "Linear ordered codes, shape enumerators, and parallel channels", in *Proc. 48th Annual Allerton Conference on Communication, Control, and Computing, Monticello, IL, USA, Sep.29-Oct.1, 2010*, pp. 361-367.

[53] W. Park and A. Barg, "The ordered Hamming metric and ordered symmetric channels," in *Proc. 2011 IEEE International Symposium on Information Theory, St.Petersburg, Russia, Aug. 1-5, 2011*, pp. 2194–2198.

[54] W. Park and A. Barg, "Multilevel polarization for nonbinary codes and parallel channels," in *Proc. 49th Annual Allerton Conference on Communication, Control, and Computing, Monticello, IL, USA, Sep. 28–30, 2011*, pp. 228–234.

[55] W. Park and A. Barg, "Polar codes for q-ary channels, $q = 2^r$," in *Proc. 2012 IEEE International Symposium on Information Theory, Boston, MA, July 1-5, 2012*, pp. 2142–2146.

[56] W. Park and A. Barg, "Polar codes for q-ary channels, $q = 2^r$," *IEEE Trans. Inform. Theory*, DOI: 10.1109/TIT.2012.2219035, 2012.

[57] M. Y. Rosenbloom and M. A. Tsfasman, "Codes for the m-metric", *Probl. Inform. Trans.*, vol. 33, no. 1, pp. 45-52, 1997.

[58] A. G. Sahebi and S. S. Pradhan, "Multilevel polarization of polar codes over arbitrary discrete memoryless channels," arXiv:1107.1535.

[59] E. Şaşoğlu, E. Telatar, and E. Arıkan, "Polarization for arbitrary discrete memoryless channels," arXiv:0908.0302.

[60] E. Şaşoğlu, "Polar codes for discrete alphabets," in *Proc. 2012 IEEE International Symposium on Information Theory, Boston, MA, July 1-5, 2012*, pp. 2147–2151.

[61] J. Simonis, "The effective length of subcodes", *Appl. Algebra Engr. Comm. Comput.*, vol. 5, pp. 371-377, 1994.

[62] C. E. Shannon, "A mathematical theory of communication," *Bell Syst. Tech. J.,* vol. 27, pp. 379–423, 623–656, July and October 1948.

[63] C. E. Shannon, "Probability of error for optimal codes in a Gaussian channel", *Bell Syst. Tech. J.*, vol. 38, no. 3, pp. 611–656, 1959.

[64] D. Slepian and J. K. Wolf, "Noiseless coding of correlated information sources," *IEEE Trans. Inform. Theory,* vol. 19, pp. 471-480, 1973.

[65] A. D. Sokal, "The multivariate Tutte polynomial (alias Potts model) for graphs and matroids", *Surveys in Combinatorics (Cambridge University Press)*, pp. 173-226, 2005.

[66] S. Tavildar and P. Viswanath, "Approximately universal codes over slow-fading channels", *IEEE Trans. Inform. Theory*, vol. 52, no. 7, pp. 3233-3258, 2006.

[67] V. Wei, "Generalized Hamming weights for linear codes", *IEEE Trans. Inform. Theory*, vol. 37, no. 5, pp. 1412-1418, 1991.

[68] D. J. A. Welsh, *Matroid Theory*, Academic Press, London, 1976.

[69] T. Wiegand, G. J. Sullivan, G. Bjøntegaard, and A. Luthra, "Overview of the H.264/AVC video coding standard," *IEEE Trans. Inform. Theory,* vol. 13, no. 7, pp. 560-576, 2003.

[70] M. Wild, "Weakly submodular rank functions, supermatroids, and the flat lattice of a distributive supermatroid", *Discrete Math.*, vol. 308, pp. 999–1017, 2008.

[71] A. D. Wyner, "Recent results in the Shannon theory", *IEEE Trans. Inform. Theory,* vol. 20, no. 1, pp. 2-10, 1974.

[72] A. D. Wyner, "The wire-tap channel", *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355-1387, 1975.

[73] C. Ye and P. Narayan, "Secret key and private key constructions for simple multiterminal source models," *IEEE Trans. Inform. Theory*, vol. 58, no. 2, pp. 639-651, 2012.