ON THE CAPACITY REGION FOR
DETERMINISTIC TWO-WAY CHANNELS AND
WRITE-UNIDIRECTIONAL MEMORIES

W.M.C.J. VAN OVERVELD
On the Capacity Region for Deterministic Two-Way Channels and Write-Unidirectional Memories

PROEFSCHRIFT

ter verkrijging van de graad van doctor aan de Technische Universiteit Eindhoven, op gezag van de Rector Magnificus, prof. ir. M. Tels, voor een commissie aangewezen door het College van Dekanen in het openbaar te verdedigen op vrijdag 25 januari 1991 om 16.00 uur

door

Wilhelmina Maria Cornelia Johanna van Overveld

geboren te Dongen
Dit proefschrift is goedgekeurd door
de promotoren
prof. dr. ir. J. P. M. Schalkwijk
en
prof. dr. J. H. van Lint

Cover image: 'Teeken', by M. C. Escher (1948)
Summary

In this thesis, two subjects in information theory are treated, to wit Two-Way Channels (TWCs) and Write Unidirectional Memories (WUMs).

A TWC is a model of communication in two directions: two users want to send information to each other at the same time. The channel they use produces a (discrete) output for each user depending on both inputs. The channel is memoryless, but each user may use previous inputs and outputs when selecting the next input symbol. We investigate how efficiently this channel can be used, i.e., we study its capacity region.

In the thesis, several isolated old results are collected in one theory. We use the so-called 'graphical representation', which relates communication over the channel to the partitioning of the unit square. This was known already for one example of a TWC, the Binary Multiplying Channel (BMC), but it turns out that this method can be used for a large class of channels. With this approach it is possible to derive good lower bounds for the capacity region.

A WUM models the use of a rewritable optical disk. Binary information is recorded on such a disk and per writing cycle, symbols can be changed in just in one direction: either zeroes can be changed into ones (over the entire disk; we call this a 1-cycle), or ones can change into zeroes (a 0-cycle). We assume that 0- and 1-cycles alternate. Again we are interested in the capacity: we want to record as much information as possible on a given disk.

We distinguish four cases, depending on whether the writer and/or the reader knows the state of the disk before writing. For each of these situations we derive the capacity. For some of these cases, the capacity was known already; in this thesis, we generalize the results to a more general type of WUM, namely the WUM over an alphabet containing \( q \) symbols. We then have \( q \) different cyclically executed writing cycles. For this situation we derive the capacity region as well, for three out of the four cases. For the fourth case (neither writer nor reader knows the old state) we give an inner bound which is believed to equal capacity.

Finally we study connections between TWCs and WUMs. Since the capacity region for the binary WUM in two cases is equal to a fundamental outer bound for the capacity of the BMC, we look for a generalization of this phenomenon over arbitrary alphabets. This gives rise to a generalization of TWCs with \( q \) users, for which we derive some properties.
Preface

This thesis could not have been written without the support of many people. Among others, I would especially like to thank the following persons:

- my advisor prof. dr. J. P. M. Schalkwijk, for introducing me to information theory in general and Two-Way Channels in particular. The many discussions we had about the Binary Multiplying Channel were very valuable for me.
- Frans Willems, for suggesting the subject of Write Unidirectional Memories to me and for giving me every possible assistance with my research in this area.
- professors J. H. van Lint, J. L. Massey and E. C. van der Meulen, for their careful proof-reading of the manuscript. Their remarks have greatly contributed to the final version of this thesis.
- my colleagues in the Information and Communication Theory group at the Eindhoven University of Technology, for providing a perfect atmosphere for the realization of this thesis.
- my family — especially my father — and friends, for showing constant interest in what I was doing during the past five years.
## Contents

Summary
Preface
Contents

**Chapter 1: Introduction**
1.1. General introduction
1.2. Outline of the thesis

**Chapter 2: Representation of Two-Way Channels**
2.1. Two-Way Channel model
2.2. Historical perspective: previous results
2.3. Graphical representation of deterministic channels
   2.3.1. The inner bound resolution
   2.3.2. The inner bound resolution for the derived channel
2.4. Simplification of graphical representations
2.5. Partition patterns

**Chapter 3: Strategy Trees for Two-Way Channels**
3.1. The rate of a tree
3.2. Fixed length trees
   3.2.1. Fixed length trees and the capacity region
   3.2.2. Fixed length trees ending in rootlike rectangles
   3.2.3. From fixed length trees to codes and vice versa
3.3. Variable length trees
   3.3.1. Variable length trees and the capacity region
   3.3.2. Variable length trees ending in rootlike rectangles
   3.3.3. From variable length trees to fixed length codes
   3.3.4. From variable length trees to variable length codes and vice versa
3.4. Bootstrap trees
   3.4.1. Definition and statement of result
   3.4.2. Proof of the achievability of bootstrap rates
3.5. Relations between strategy trees
Contents

3.6. Examples of strategy trees
  3.6.1. Strategy trees for the Binary Multiplying Channel 98
  3.6.2. Miscellaneous results 110

Chapter 4: The Write Unidirectional Memory

4.1. Binary WUM codes
  4.1.1. Introduction 114
  4.1.2. Definitions 116
  4.1.3. Previous results 121

4.2. WUM codes over arbitrary alphabets
  4.2.1. The model 125
  4.2.2. Statement of results 127
  4.2.3. Proof of achievability for case 1 and 2 128
  4.2.4. Converse for case 1 and 2 133
  4.2.5. Proof for case 3 136
  4.2.6. Proof for case 4: achievability 147

4.3. Bounding the average rate 151

Appendix A 163
Appendix B 167
Appendix C 172

Chapter 5: Some Connections between Write Unidirectional Memories and Two-Way Channels

5.1. Introduction: the binary WUM and the BMC 174
5.2. The q-ary WUM and generalizations of the BMC 180
  5.2.1. The q-ary 'two-way channel' 180
  5.2.2. The q-ary BMC 188
  5.2.3. A q-ary ring channel resembling the WUM 192

List of Symbols 200
Subject Index 203
References 205
Samenvatting 209
Curriculum Vitae 210

— iv —
Chapter 1: Introduction

1.1. General introduction

This thesis deals with two unsolved problems in the field of information theory. In this field, different kinds of communication situations are studied and answers are given to questions like

- 'How fast (and yet reliably) can data be transmitted over a given channel and how should that be done?'
- 'How efficiently can two persons transmit messages to each other over one channel at the same time?'
- 'How much information can be stored in a defective computer memory?'

In 1948, C.E. Shannon [SHA48] gave an answer to the first question, using a mathematical model of the channel under consideration. For several restricted cases he showed how to compute the capacity of a channel, which is a formal description of 'how efficiently' the channel can be used. This publication initiated the research in the theory of channel coding.

The second question was considered by the same author in 1961 [SHA61]. It proved to be essentially more difficult than the first one, because of the interaction between the users. Problems in which two or more users try to transmit and/or receive messages simultaneously are treated in so-called multi-user information theory. For an overview of the type of problems considered there, we refer the reader to [MEU77] or [ELG80]. In the case of two users transmitting to
each other, the channel is called a two-way channel, abbreviated as TWC. The first part of this thesis is devoted to some special classes of TWCs.

The topic launched in the third question is in fact again a subject of study in channel coding theory, but now for a specific type of channel. In the case of the first question, we usually think of the channel as a medium for communication in space (from the location of the transmitter to the location of the receiver); in the same way a memory cell can be used for communication in time, from the storage time to some later instant of data retrieval. In the second part of this thesis we study a channel similar to this, called a 'Write Unidirectional Memory' (WUM).

Finally we study an interesting connection between the two topics (TWCs and WUMs). It appears that a fundamental bound on the capacity region of the binary multiplying channel (BMC, one of the least complex TWCs) is exactly the same as the capacity region of the WUM. This similarity suggests a generalization of the BMC in the same way as the WUM can be generalized. This 'generalized BMC' is investigated in the last part of this thesis.

Although we try to keep this thesis as self-contained as possible, it cannot be avoided that some basic knowledge about mathematics and information theory is assumed. The reader who is not familiar with concepts like entropy, mutual information and channel capacity is referred to one of the many textbooks ([GAL68], [ASH65]) that present an appropriate introduction to this field. All notations (except the standard ones in mathematics, like \( \mathbb{R}, \{0,1\}, Pr\{X = 0\}, \) et cetera) will be explained where they are first introduced. Furthermore, a list of symbols can be found in the back of this thesis.
1.2. Outline of the thesis

This thesis is organized as follows. Apart from this introductory chapter, in which we explain the kinds of problems that are studied and mention the main results, there are four more chapters. Chapters 2 and 3 are devoted to TWCs, Chapter 4 is about WUMs; in the final chapter these two subjects are linked together.

In Chapter 2, we start with the definition of the TWC model (Section 2.1) and we mention some previous results (Section 2.2). Apart from Shannon's theorems on TWCs in general, we mainly concentrate on the BMC. The results for the BMC obtained by Schalkwijk and some of his students were found by looking at the channel in a graphical way, in which the construction of codes for the BMC could be seen as the partitioning of a square. In Sections 2.3 through 2.5 we generalize this idea to arbitrary deterministic TWCs. We give a formal definition of the 'graphical representation', we explain how it should be interpreted and we show how it can be used to classify channels.

In Chapter 3, the graphical representation is used to find inner bounds for the capacity region of TWCs. Schalkwijk used the partitioning of the square to bound the capacity region of the BMC, by changing a partitioning corresponding to a code into a Markov chain. Furthermore he reasoned that one of the states (the 'bad' state) of the Markov chain could be left out of consideration. The rate found in this way is the best bound known for the capacity region, although it was never rigidly proved that this rate is indeed achievable.

The techniques used by Schalkwijk are generalized to arbitrary TWCs in Chapter 3 of this thesis. In Sections 3.1 through 3.4, we define different types of
trees in which partitionings of the square can be represented: fixed length and variable length trees, ending either in rectangles or in arbitrarily shaped vertices, and so-called 'bootstrap' trees. For each of these trees, the rate of the tree is defined and we prove that this rate is achievable for the TWC. Since this result includes both Schalkwijk's original Markov chain and the Markov chain without the 'bad' state, this proves that Schalkwijk's scheme indeed yields an inner bound for the BMC capacity. In Section 3.6, we give examples of different TWCs and we show how inner bounds for the capacity can be found using the trees.

Furthermore we prove (Section 3.5) that the achievable rate regions for the different types of trees are all equal and that they are equal to the capacity region. This shows, for instance, that variable length trees do not yield higher rates than fixed length trees, even though the class of fixed length trees is just a small subclass of the class of variable length trees.

Chapter 4 is split into three sections. In Section 4.1, we introduce the binary WUM as studied by Willems/Vinck, Borden, Simonyi and others. We mention previous results concerning the capacity region for the binary WUM in four cases (depending on whether the encoder and/or decoder is informed about the state of the WUM). In Section 4.2, we generalize the concept of the WUM to arbitrarily large alphabets. We define the so-called 'q-ary WUM' and generalize the definitions from Section 4.1. The rest of this section is devoted to the capacity region in the four cases for the q-ary WUM. For three out of four cases, we are able to determine the capacity region; for the fourth case, we derive an inner bound region which we conjecture to be the actual capacity region.

In Section 4.3, finally, we look at the maximum achievable rate sum in each of the four cases for the q-ary WUM. Using the results from Section 4.2, we derive expressions for this rate sum. We prove that the maximum achievable rate
sum for case 4 is equal to the maximum rate sum in the inner bound region found in Section 4.2, which seems to affirm our conjecture.

Chapter 5 deals with possible connections between TWCs and WUMs. In Section 5.1, we point out a similarity between the binary WUM and the BMC: the so-called 'Shannon outer bound' for the BMC equals the WUM capacity for cases 1, 2 and 3. This leads us to investigations how this may be generalized to the situation with arbitrary alphabets. In other words, we are looking for a generalization of the BMC having a 'generalized Shannon outer bound' equal to the $q$-ary WUM capacity region for any of the four cases.

In Section 5.2, we define a generalization of the TWC called a $q$-ary ring channel. We generalize Shannon's TWC theorems to this channel, which gives us a 'generalized Shannon outer bound'. In Section 5.3, some examples of $q$-ary ring channels are examined to see whether their outer bound equals the WUM capacity region. The last one of these examples seems to have this property, although we do not have a proof. The other two channels studied do not have the desired property for $q > 2$. Nevertheless these ring channels provide promising material for further research.
Chapter 2: Representation of Two-Way Channels

2.1. Two-way channel model

Two-way channels were introduced by Shannon in 1961 [SHA61]. He presented a model of a communication situation in which two users want to send information to each other simultaneously over the same physical channel. In Figure (2.1.1), the model for a two-way channel (TWC) called $\mathcal{K}$ is shown.

Two users (or terminals) are called 0 and 1. The (time-discrete) channel $\mathcal{K}$ consists of two input alphabets $\mathcal{X}_0$ and $\mathcal{X}_1$ (for user 0 and 1, respectively), two output alphabets $\mathcal{Y}_0$ and $\mathcal{Y}_1$ and a so-called transition matrix $p^*(y_0, y_1 | x_0, x_1)$, with

$$p^*(y_0, y_1 | x_0, x_1) \in [0, 1] \text{ for } x_0 \in \mathcal{X}_0, x_1 \in \mathcal{X}_1, y_0 \in \mathcal{Y}_0, y_1 \in \mathcal{Y}_1,$$

and

$$\sum_{(y_0, y_1) \in \mathcal{Y}_0 \times \mathcal{Y}_1} p^*(y_0, y_1 | x_0, x_1) = 1 \text{ for } x_0 \in \mathcal{X}_0, x_1 \in \mathcal{X}_1.$$
The channel is used as follows. At each time instant (e.g. each second; this plays no role in the rest of the paper), both users select symbols \( I_0 \) and \( I_1 \) from their respective input alphabets \( \mathcal{X}_0 \) and \( \mathcal{X}_1 \) and use these as inputs for channel \( \mathcal{K} \). Depending on the input pair, the channel produces two output symbols \( Y_0 \) and \( Y_1 \); symbol \( Y_0 \in \mathcal{Y}_0 \) can be observed by user 0 and user 1 observes \( Y_1 \in \mathcal{Y}_1 \). The pair \( (Y_0, Y_1) \) is statistically related to input pair \( (I_0, I_1) \) in a way described by \( P^* \):

\[
P_r\{ (Y_0, Y_1) = (y_0, y_1) | (I_0, I_1) = (x_0, x_1) \} = P^*(y_0, y_1 | x_0, x_1).
\]

(Here and in the rest of this thesis, upper case letters are used for random variables and the corresponding lower case letters denote actual outcomes of the stochastic process that is considered.)

Channel \( \mathcal{K} \) is assumed to be \textit{discrete}, which expresses the fact that both the input and the output alphabets have finite cardinalities. If some alphabet, say \( \mathcal{A} \), has \( q \) elements, then without loss of generality we will take \( \mathcal{A} = \{0, 1, \ldots, q-1\} \).

It follows from the channel model that the channel is \textit{memoryless}. This means that the probability distribution of the output pair \( (Y_0, Y_1) \) at instant \( t \) is determined completely by the input pair at that instant. However, the output pair does depend on all previous input pairs since we allow feedback: each user may choose the next input symbol depending on all previous input and output symbols observed by him. Hence we have the following situation. Let \( x_0^n = (X_0, X_1, \ldots, X_0, X_1, \ldots, X_0_n) \) and \( x_1^n = (X_1_0, X_1_1, \ldots, X_1_n, X_1_1, \ldots, X_1_n) \) be input sequences of length \( N \) and let \( y_0^n \) and \( y_1^n \) be the corresponding output sequences. Then, with \( P(x_0^n, x_1^n, y_0^n, y_1^n) \) := \( P_r\{ (Y_0^n, Y_1^n) = (y_0^n, y_1^n) \} = (x_0^n, x_1^n) \), \( y_0^n, y_1^n \) we have

\[
P(x_0^n, x_1^n, y_0^n, y_1^n) = \\
\prod_{n=0}^{N-1} P(x_0^n, n | y_0^n, y_0^n) \cdot P(x_1^n, n | y_1^n, y_1^n) \cdot P^*(y_0^n, n, y_1^n, n | x_0^n, n, x_1^n, n).
\]
This notation should be interpreted in such a way that for \( n = 0 \), \( \mathbb{Z}^n \) and 
\((x_0, x_1, \ldots, x_{n-1})\) denote the empty sequence.

An interesting example of a discrete memoryless TWC is the so-called binary multiplying channel, or BMC, first studied by Blackwell and described in [SHA61).

(2.1.2) Example. The binary multiplying channel:

\[
x_0 = x_1 = y_0 = y_1 = \{0, 1\} \quad \text{and} \quad p^*(y_0, y_1 | x_0, x_1) = \begin{cases} 1 & \text{if } y_0 = y_1 = x_0x_1 \\ 0 & \text{otherwise.} \end{cases}
\]

The channel in Example (2.1.2) is a deterministic TWC and it is also a T-channel. Both of these concepts are defined below.

(2.1.3) Definition. A TWC with parameters \((X_0, X_1, Y_0, Y_1, P^*)\) is called deterministic if the output pair is completely determined by the input pair; in other words, all entries in the transition matrix \(P^*\) are either 0 or 1. In this case we can define a function \(f_K: X_0 \times X_1 \rightarrow Y_0 \times Y_1\), where \(f_K(x_0, x_1)\) is the output pair generated by channel \(K\) if the input pair is \((x_0, x_1)\). \(\square\)

For the BMC example, we have \(f_{BMC}(x_0, x_1) = (x_0x_1, x_0x_1)\).

(2.1.4) Definition. A TWC with parameters \((X_0, X_1, Y_0, Y_1, P^*)\) is called a T-channel if the transition matrix is such that for all input pairs \((I_0, I_1)\), the output pair has \(Y_0 = Y_1\). Such a channel is also known as a single-output TWC; its output is called \(Y\) (instead of \(Y_0\) or \(Y_1\)). \(\square\)
Consider an arbitrary (discrete, memoryless, but not necessarily deterministic) two-way channel $\mathcal{X}$. The channel can be used for communication in the following way (see Figure (2.1.5)).

![Diagram](image)

(2.1.5) Figure. Communication situation for a TWC.

Let $\mathcal{M}_0 \in \mathbb{N}$, $\mathcal{M}_1 \in \mathbb{N}$, $N \in \mathbb{N}$ and let $\mathcal{M}_i := \{0, 1, \ldots, N-1\}$ for $i \in \{0, 1\}$. The sources generate messages $V_0$ and $V_1$, respectively, with $V_0 \in \mathcal{M}_0$ and $V_1 \in \mathcal{M}_1$. The sets $\mathcal{M}_0$ and $\mathcal{M}_1$ are called the message sets. $V_0$ and $V_1$ are independent and uniformly distributed: for all $w_0 \in \mathcal{M}_0$, $w_1 \in \mathcal{M}_1$,

$$Pr\{V_0 = w_0, V_1 = w_1\} = Pr\{V_0 = w_0\} \cdot Pr\{V_1 = w_1\},$$

$$Pr\{V_0 = w_0\} = 1/N_0, \ Pr\{V_1 = w_1\} = 1/N_1.$$

A message is transmitted to the other terminal by selecting appropriate input symbols for the channel in $N$ consecutive instances of time. The selection is made by the encoders. Let $i \in \{0, 1\}$, $j \in \{0, 1\}$, $i \neq j$. At instant $n$, $n \in \{0, 1, \ldots, N-1\}$, user $i$ can select his input symbol $I_{i,n}$ depending on the message $V_i$ he is transmitting, but $I_{i,n}$ may also depend on the sequence of $n$ $V_i$—symbols that user $i$ has observed up to this moment. After all $N$ symbol pairs have been sent over the channel, the decoder of user $i$ estimates user $j$'s message $V_j$ as $\hat{V}_j$ by looking at the output sequence $I_i^N$ and knowing the fact that his own transmitted message is $V_i$. 
Chapter 2

Formally this process can be described by a code, see Definition (2.1.6).

The reader familiar with the classical one-way channel (cf. [GAL68], [SHA48]) will recognize definitions (2.1.6) through (2.1.10), since they are straightforward generalizations of some one-way channel coding concepts.

(2.1.6) Definition. An \((W_0, W_1, N)\) code consists of \(2N\) encoding functions \(f_{i,0}, f_{i,1}, \ldots, f_{i,N-1}\) (\(i=0,1\)) and two decoding functions \(g_0\) and \(g_1\). For \(n \in \{0,1,\ldots,N-1\}\), the function

\[
f_{i,n} : M_i \times Y_i^n \rightarrow X_i
\]

maps the message \(V_i\) and the received \(Y_i\)-sequence \(Y_i^n = (Y_{i,0}, Y_{i,1}, \ldots, Y_{i,n-1})\) into the next channel input symbol \(X_{i,n}\) for user \(i:\)

\[
X_{i,n} = f_{i,n}(V_i, Y_i^n).
\]

The decoding function

\[
g_i : M_i \times Y_i^n \rightarrow M_j
\]

describes the way in which \(V_j\) is estimated by user \(i\) (\(i \neq j\)):

\[
\tilde{V}_j = g_i(V_i, Y_i^n).
\]

The parameter \(N\) is called the block length (or codeword length) of the code.

For a fixed code, we can study the probability that either one of the messages will be decoded incorrectly if this code is used. Hence we define the following.

(2.1.7) Definition. The (average) error probabilities \(p_{e,0}\) and \(p_{e,1}\) of a code are defined by

\[
p_{e,i} := \sum_{w_i \in M_i} pr\{V_i = w_i \text{ and } \tilde{V}_i \neq w_i\}, \quad i \in \{0,1\}.
\]
We will look at the rate pair (sometimes called the rate point) of a code, which can be interpreted as the average amount of information (in bits) that is sent over the channel – from terminal 0 to terminal 1 and vice versa – per channel use.

(2.1.8) Definition. For an \((H_0, H_1, N)\) code, the rate pair \((R_0, R_1)\) is defined by
\[
R_i := \frac{\log(H_i)}{N}, \quad i \in \{0, 1\}.
\]
Here, like everywhere else in this thesis, the logarithm is to the base 2.

The next two definitions are important for finding out how efficiently the two-way channel can be used for reliable communication, in terms of high rates and yet small error probability.

(2.1.9) Definition. A rate pair \((R_0, R_1)\) is called achievable if for all \(\varepsilon > 0\) and all sufficiently large \(N\), an \((H_0, H_1, N)\) code exists having error probabilities \(P_{e,0}\) and \(P_{e,1}\), such that
\[
\frac{\log(H_i)}{N} > R_i - \varepsilon \quad \text{and} \quad P_{e,i} < \varepsilon \quad \text{for} \quad i \in \{0, 1\}.
\]

The expression 'achievable rate' suggests that a code having this rate exists, which is not necessarily true. 'Approachable' might be a more appropriate word, but the term 'achievable' is more commonly used in the literature.

(2.1.10) Definition. The capacity region of a two-way channel is the set of all achievable rate pairs. If the TWC is called \(\mathcal{X}\), then its capacity region will be denoted by \(C_{\mathcal{X}}\); if no confusion is possible, it will just be denoted by \(C\).

It should be noted that a capacity region is a closed convex set (cf. [SHA61]).
Chapter 2

2.2. Historical perspective: previous results

The first results on capacity regions for TWCs were obtained by Shannon [SHA61]. For a discrete memoryless TWC with parameter set \((X_0, X_1, Y_0, Y_1, P^*)\), he derived an upper and lower bound for the capacity region. Before we can state this result, we need to introduce some notation.

(2.2.1) Notation. Consider a TWC as described above and let \(P(x_0, x_1)\) be some probability distribution on \(X_0\) and \(X_1\). Then \(I(X_0; Y_1 | I_1)\) denotes the conditional mutual information [GAL68] between \(X_0\) and \(Y_1\) conditional on \(I_1\):

\[
I(X_0; Y_1 | I_1) = \sum_{x_0, x_1, y_1} P(x_0, x_1, y_1) \cdot \log \left( \frac{P(x_0, x_1, y_1 | Y_1) P(y_1)}{P(x_1, y_1 | x_0, x_1)} \right).
\]

Here the distributions \(P(x_0, x_1, y_1), P(x_1, y_1)\) and \(P(x_1)\) are found using the given distribution \(P(x_0, x_1)\) and the channel transition matrix \(P^*\). Thus:

\[
P(x_0, x_1, y_1) = P(x_0, x_1) \cdot \sum_{y_0 \in Y_0} P^*(y_0, y_1 | x_0, x_1).
\]

Similarly, we denote entropy and conditional entropy as \(H(X_0)\) and \(H(Y_1 | I_0)\).

Hence we have e.g.

\[
I(X_0; Y_1 | I_1) = H(Y_1 | I_1) - H(Y_1 | I_0, I_1),
\]

\[
H(Y_1 | I_1) = H(Y_1, I_1) - H(I_1).
\]

(2.2.2) Definition. The Shannon inner bound region \(G_i\) is defined as

\[
\text{co} \cup \{ (K_0, K_1) \in \mathbb{R}^2 \mid 0 \leq K_0 \leq I(X_0; Y_1 | I_1), 0 \leq K_1 \leq I(X_1; Y_0 | I_0) \},
\]

where \(\text{co}\) denotes taking the the convex hull and the union is taken over all product distributions \(P(x_0, x_1) = P(x_0)P(x_1)\).
(2.2.3) Definition. The Shannon outer bound region $G_o$ is defined as
\[
\bigcup \{(x_0, x_1) \in \mathbb{R}^2 \mid 0 \leq x_0 \leq I(X_0; Y_1), 0 \leq x_1 \leq I(X_1; Y_0 | I_0)\},
\]
where the union is taken over all simultaneous distributions $P(x, x')$. No 'co' is necessary here, because $G_o$ is already convex, as shown in [SHA61].

(2.2.4) Theorem (Shannon '61). For a TWC with parameters $(x, y, p, p^*)$ and capacity region $C$, we have
\[
G_i \subset C \subset G_o.
\]

Shannon also proved that the capacity region for a TWC can be expressed in terms of the inner bound regions for its 'derived channels'. The definition of a derived channel is given below. Theorem (2.2.6) states Shannon's result.

(2.2.5) Definition. Let $\mathcal{K}$ be a TWC and let $N \in \mathbb{N}$. The $N^{th}$ derived channel of $\mathcal{K}$, denoted as $\mathcal{K}(N)$, is defined such that each use of $\mathcal{K}(N)$ corresponds to $N$ successive uses of $\mathcal{K}$. To be more precise, input letters $x_0^N, x_1^N$ for $\mathcal{K}(N)$ are strategies of length $N$ for $\mathcal{K}$, where the next input $x_i$ (for $\mathcal{K}$) may depend on previous input and output symbols $x_{-i}$, $y_{-i}$ within the same block of length $N$; output letters $y_0^N, y_1^N$ for $\mathcal{K}(N)$ are blocks of outputs for $\mathcal{K}$: $y_0^N = y_0^N$ and $y_1^N = y_1^N$.

(2.2.6) Theorem (Shannon '61). Let $\mathcal{K}$ be a TWC with capacity region $C$. Let, for $N \in \mathbb{N}$, $G_i(N)$ denote the Shannon inner bound for the derived channel $\mathcal{K}(N)$. Then
\[
\forall N \in \mathbb{N} \left[ G_i(N) / N \subset C \right] \quad \text{and} \quad C = \lim_{N \to \infty} G_i(N) / N,
\]
where $G_i(N) / N := \{(g_0/N, g_1/N) \mid (g_0, g_1) \in G_i(N)\}$. 

---

19
Chapter 2

The limit occurring in Theorem (2.2.6) involves a sequence of regions converging to another region. Although the meaning of this limiting process may be clear intuitively, we still give a formal definition of this notion because it will be needed in Chapter 3, where we will prove theorems similar to (2.2.6).

(2.2.7) Definition. The distance between \( p \in \mathbb{R}^2 \) and \( A \subset \mathbb{R}^2 \), \( d(p, A) \), is defined as

\[
d(p, A) = \inf \{ d(p, \alpha) \mid \alpha \in A \}
\]

where \( d(p, \alpha) \) is the Euclidean distance between the points \( p \) and \( \alpha \).

(2.2.8) Definition. Let \( \{ A_N \}_{N \in \mathbb{N}} \) be a sequence of regions in \( \mathbb{R}^2 \). Then \( A_\infty \) is the limiting region of \( \{ A_N \} \), denoted as

\[
\lim_{N \to \infty} A_N = A_\infty,
\]

if (i) and (ii) hold.

\[
(i) \quad \forall \alpha \in A_\infty \forall \epsilon > 0 \exists N_0 \in \mathbb{N} \forall N > N_0 \{ d(\alpha, A_N) < \epsilon \}
\]

\[
(ii) \quad \forall \alpha \notin A_\infty \exists \epsilon > 0 \exists N_0 \in \mathbb{N} \forall N > N_0 \{ d(\alpha, A_N) > \epsilon \}.
\]

Theorem (2.2.6) theoretically solves the problem of finding the capacity region for a TWC. However, since it involves taking a limit, the actual boundaries of this region are still not computable for most TWCs. Obviously, if \( G_i = G_o \) for some TWC, then its capacity region is determined by Theorem (2.2.4). This equality holds for some TWCs (e.g., TWCs with a 'symmetrical structure', cf. [SHA61]), but Shannon showed that there are also TWCs for which \( G_i \neq G_o \). The least complex example of such a channel is Example (2.1.2), the BMC. By evaluating (2.2.2) and (2.2.3) for this channel, it follows that (cf. [SHA61])

(2.2.9) \( G_i = \{ (a \cdot h(\beta), \beta \cdot h(a)) \mid 0 \leq a \leq 1, 0 \leq \beta \leq 1 \} \) and

(2.2.10) \( G_o = \{ (\beta \cdot h(\frac{1-a}{\beta}), a \cdot h(\frac{1-\beta}{a})) \mid 0 \leq a \leq 1, 0 \leq \beta \leq 1, a + \beta \geq 1 \} \).
Here $h(\cdot)$ denotes the binary entropy function:

$$h(z) = -z \cdot \log(z) - (1-z) \cdot \log(1-z) \quad \text{for} \quad 0 < z < 1, \quad h(0) = h(1) = 0.$$  

Figure (2.2.11) shows the situation for the BMC. The regions $G_i$ and $G_o$ are bounded by the respective convex curves and the axis segments.

(2.2.11) Figure. Shannon bounds for the BMC.

One can check that $G_o$ is strictly larger than $G_i$ by looking at the equal rate point $(R_0 = R_1)$ on the border of both regions: For $G_i$ we find $R_0 = R_1 = 0.61695$ and for $G_o$ we have $R_0 = R_1 = 0.69424$.

At the time of Shannon's paper, in 1961, it was not yet known whether the inner bound for the BMC was strictly interior to the capacity region; the best BMC code known at that time (in the symmetrical case) had $R_0 = R_1 = 0.57143$. This code was developed by Hagelbarger [SHA61]. However, this is not a code in the sense of Definition (2.1.6), since it has codewords of different lengths (for a description of the Hagelbarger code, see Section 3.3.4 of this thesis).

The problem 'can the capacity region exceed the Shannon inner bound?' was open not only for the BMC; in fact, it was unknown whether this could happen for any TWC at all. This is a fundamental problem: if the capacity is equal to the inner bound, then it is impossible to take advantage of possible
statistical dependency that can be created between the two users by means of previous inputs and outputs. Indeed, the proof of the Shannon inner bound [SHA61] is based on the existence of codes achieving any rate in $\mathcal{G}_i$ that do not 'use' previous output symbols (in terms of Definition (2.1.6): the function value $f_{i,n}(v_i, y_i^n)$ varies with $v_i$ only.)

An attempt to solve the aforementioned problem was first made by Jelinek [JEL64]. He devised a coding scheme for an arbitrary TWC, by decomposing the TWC into two one-way channels. Unfortunately the rate of this coding scheme was still within the Shannon inner bound region. Jelinek (incorrectly) conjectured that, at least for the BMC, it would not be possible to achieve rates outside $\mathcal{G}_i$.

Not until 1979 it was shown that a capacity region can exceed the Shannon inner bound. Dueck [DUE79] constructed an example of a TWC (not the BMC) for which $C \notin \mathcal{G}_i$. In 1982, Schalkwijk [SCH82] showed that the same is true for the BMC by developing a scheme with rate $(k_0, k_1)$, $k_0 = k_1 = 0.61914$. Like Hagelbarger's code, this was not a code in the sense of Definition (2.1.6), but Tolhuizen [TOL85] proved that Schalkwijk's scheme can be used to construct a code having the same rate. Schalkwijk improved his scheme in 1983 using a technique called 'bootstrapping' [SCH83a] and obtained an achievable symmetrical rate pair with $k_0 = k_1 = 0.63056$. Because of the bootstrapping, it was not obvious that this new rate could also be achieved with 'strict-sense' codes. Nevertheless this is true, as shown in [OVE88] and in Section 3.4 of this thesis. In 1986, Schalkwijk [SCH86] conjectured this rate point to be optimum, but recently, using a more intricate bootstrap scheme [SCH90], he found a slightly higher rate: 0.630555299 instead of 0.630555256. For the BMC, this gives a total improvement upon the Shannon inner bound from 0.61695 to 0.63056.

The Shannon inner bound could be exceeded not only for specific channels: Han [HAN84] developed a coding scheme for the arbitrary TWC, yielding an
achievable rate region which strictly includes Shannon's inner bound for a large class of channels. Unfortunately this result cannot be compared to Schalkwijk's rate point, since computing Han's achievable rate region for the BMC involves quite complex numerical calculations. In the same paper [HAN84], Han proved that the capacity region is equal to the Shannon inner bound for the Gaussian TWC (which is a TWC having $X_0 = X_1 = Y_0 = Y_1 = \mathbb{R}$ and $Y_0 = aI_0 + bI_1 + N_0$, $Y_1 = cI_0 + dI_1 + N_1$ where the noise terms $N_0$ and $N_1$ are Gaussian).

As for the Shannon outer bound: it took even longer before this was improved. Again, let us consider the symmetrical rate pair $(I_0, I_1)$ with $I_0 = I_1$ for the BMC. In 1986, Zhang, Berger and Schalkwijk [ZHA86] lowered the bound from 0.69424 to 0.64891. Around the same time, the tightest upper bound known up to now was found by Hekstra and Willems [HEK89]: $I_0 = I_1 = 0.64628$. The true capacity region of the BMC is still unknown.

For arbitrary TWCs, the Shannon outer bound can be improved upon by the technique described in [ZHA86]; the outer bound for the BMC is just an example of the general Zhang–Berger–Schalkwijk (ZBS) bound. However, it is very hard to evaluate the ZBS bound in general, because it involves optimization over probability distributions of auxiliary random variables that may take values in large alphabets. The bound in [HEK89], which is known as the dependence balance bound, is also applicable to more channels than just the BMC: it holds for any T–channel. In general it is stronger than the ZBS bound, but unfortunately it has the same disadvantage: the optimization over arbitrary random variables hampers numerical computation of the bound.

Recently, some problems related to Shannon's classical two–way situation have been studied. Salehi [SAL88] looked at the situation in which the two sources are correlated, but the channel is 'restricted'. The restriction on the channel is
the fact that the users are not allowed to look at previous outputs before they decide on their next input symbols. In this situation we have a different kind of dependency between the users, originating from the message pair rather than from the fact that the new input pair depends on old output pairs. Salehi derived an achievable rate region for this case, which is typically somewhere in between $G_i$ and $G_0$ (depending on the kind of correlation); as in Theorem (2.2.6), he was able to express the capacity region as his inner bound region for the $N$th derived channel, for $N \to \infty$.

Tiersma [TIE89] studied an extension of the TWC for three users. In this situation, each of the three users is sending messages to the other two via the three-way channel which produces an output triple $(Y_0, Y_1, Y_2)$ depending on the input triple $(I_0, I_1, I_2)$. Tiersma derived bounds on the capacity region that generalize the Shannon inner and outer bound for the TWC. As an example, he looked at the BMC with $Y_0 = Y_1 = Y_2 = I_0 \cdot I_1 \cdot I_2$. For both the inner and outer bound region, he computed the rate point with highest sum rate, $I_0 + I_1 + I_2$. He also developed a coding scheme reminiscent of the one in [SCH82], which achieved a sum rate slightly below his inner bound value.

Finally we should mention the work of numerous students in the Information Theory Group of the Electrical Engineering Department of the Eindhoven University of Technology. Between 1982 and 1988, many of them have worked on problems related to Schalkwijk’s coding scheme for the BMC. Some of them tried to improve the scheme or to construct different types of strategies for the BMC ([HAZ85], [LEU84], [OVE85], [SME83], [TOL85]); others concentrated on more complicated channels (e.g. with ternary input and output alphabets), tried to characterize them and to find good strategies for them ([ENG87], [GAA85], [HAM87], [HEI87], [JAC86], [LOR88]). Since part of their work is used in this thesis, we will describe their results in the sections where they are used.
2.3. Graphical representation of deterministic channels

2.3.1. The inner bound resolution

In this section we will introduce the graphical representation of a deterministic TWC. This is a way to depict the probability distribution of input and output symbols in a unit square. This approach was first used by Schalkwijk [SCH82] (and could also be applied to multiple access channels, as shown by Zhang, Berger and Massey [ZHA87]). It appears to be a useful way to represent distributions for deterministic TWCs. Therefore we will restrict ourselves to deterministic TWCs in the rest of this thesis.

From now on, $\mathcal{K}$ will be a discrete memoryless deterministic TWC with alphabets $\mathcal{X}_0$, $\mathcal{X}_1$, $\mathcal{Y}_0$ and $\mathcal{Y}_1$. Let the relation between inputs and outputs be given by $(Y_0, Y_1) = f_{K}(I_0, I_1)$. To avoid trivialities, we will assume that the capacity region $\mathcal{C}$ is not confined to one of the coordinate axes in the $(I_0, I_1)$ plane; this implies that both users can reliably transmit a positive amount of information to each other, however low the rate of the code may be (e.g. by time sharing; we will come back to this in Section 3.3.2). For this case, we have $H(Y_1|I_0, I_1) = H(Y_0|I_0, I_1) = 0$, since $Y_0$ and $Y_1$ can be determined from $I_0$ and $I_1$. Now the Shannon inner bound defined in (2.2.2) can be rewritten as follows.

\[(2.3.1.1) \ G_i = \{ (I_0, I_1) | 0 \leq I_0 \leq H(Y_1|I_1), 0 \leq I_1 \leq H(Y_0|I_0) , (Y_0, Y_1) = f_K(I_0, I_1) , P(x_0, x_1) = P(x_0)P(x_1) \} .\]

Consider a distribution $P(x_0, x_1) = P(x_0)P(x_1)$. For user $i \ (i \in \{0, 1\})$, we represent $P(x_i)$ by a unit interval which is partitioned into $|X_i|$ subintervals, one for each possible input symbol, such that the size of each subinterval corresponds to the probability that that input symbol is chosen. As an example, take
\( \mathcal{X}_0 = \{0,1,2\} \) with \( P(0) = 0.2, \ P(1) = 0.5, \ P(2) = 0.3 \). The corresponding partitioning of the unit interval for user 0 is depicted in Figure (2.3.1.2).

\[
\begin{array}{c|c|c}
I_0 = 0 & I_0 = 1 & I_0 = 2 \\
0.2 & 0.5 & 0.3 \\
\end{array}
\]

(2.3.1.2) Figure. Partitioning of a unit interval for user 0.

Since the users are independent, the simultaneous distribution \( P(x_0, x_1) \) can be represented in a square being the Cartesian product of the unit intervals for both users. The square is partitioned into subrectangles corresponding to pairs \((x_0, x_1)\).

Let channel \( K \) be used once with the given input distribution. Since \( K \) is deterministic, we can assign to each of the subrectangles the channel output pair \((y_0, y_1) = f_K(x_0, x_1)\). The following example will make this clear.

(2.3.1.3) Example. The ternary TWC \( K \) for which \( \mathcal{X}_0 = \mathcal{X}_1 = \mathcal{Y}_0 = \mathcal{Y}_1 = \{0,1,2\} \) with \( f_K \) following from the output matrices below.

\[
\begin{array}{c|c|c|c}
& I_1 & \\
& 0 & 1 & 2 \\
\hline
I_0 & 0 & 1 & 0 \\
& 1 & 2 & 0 \\
& 2 & 1 & 2 \\
\end{array}
\quad
\begin{array}{c|c|c|c}
& I_1 & \\
& 0 & 1 & 2 \\
\hline
I_0 & 0 & 0 & 1 \\
& 1 & 0 & 0 \\
& 2 & 0 & 2 \\
\end{array}
\]

Assume that the users independently choose their input distribution, which means that the simultaneous input distribution is a product distribution: \( P(x_0, x_1) = P(x_0) \cdot P(x_1) \). If this distribution is used on \( K \), then the unit square is
Representation of TWCs

partitioned as shown in Figure (2.3.1.4). In a subrectangle corresponding to 
\((z_0, z_1)\), the corresponding output \((y_0, y_1)\) is written.

\[
\begin{array}{ccc}
I_1=0 & I_1=1 & I_1=2 \\
I_0=0 & 10 & 01 & 00 \\
I_0=1 & 20 & 00 & 20 \\
I_0=2 & 10 & 22 & 21 \\
\end{array}
\]

(2.3.1.4) Figure. Partitioning of the unit square for channel \(\mathcal{K}\).

Figure (2.3.1.4) summarizes the operation of channel \(\mathcal{K}\): the input and output alphabets and the relation between inputs and outputs can be obtained from it. For this reason we refer to pictures like (2.3.1.4) as a graphical representation of the TWC. Since we have a product distribution for the inputs, the area of the \((x_0, x_1, y_0, y_1)\) rectangle in Figure (2.3.1.4) equals

\[P(x_0, x_1, y_0, y_1) = P(x_0) \cdot P(x_1) \cdot \phi((y_0, y_1) = f_{\mathcal{K}}(x_0, x_1)).\]

In this notation, \(\phi(\lambda) := 1\) if assertion \(\lambda\) is true and otherwise \(\phi(\lambda) := 0\). Therefore the distribution \(P(x_0, x_1, y_0, y_1)\) can be derived from the areas of all subrectangles in the figure and, consequently, \(\mathbb{H}(Y_1|I_1)\) and \(\mathbb{H}(Y_0|I_0)\) can be computed from the figure. By varying the lengths of the subintervals for the two users (i.e., varying \(P(z_0)\) and \(P(z_1)\)), we find all points in region \(\mathcal{G}_i\), see (2.3.1.1). This already shows that the graphical representation of a channel is an important tool for the computation of achievable rates. In the rest of this chapter and in Chapter 3, the importance of pictures like these will become more transparent.
Chapter 2

We say that Figure (2.3.1.4) depicts an inner bound resolution. 'Inner bound' because of the independence between the inputs; 'resolution' because if the channel is used with the given input distribution, then an amount of uncertainty is resolved, namely \( I(I_0; Y_1 | I_1) = H(Y_1 | I_1) \) and \( I(I_1; Y_0 | I_0) = H(Y_0 | I_0) \) in the two directions (before transmission, the uncertainty about the other user's input was \( H(I_0 | I_1) \) and \( H(I_1 | I_0) \), respectively; afterwards these amounts are lowered to \( H(I_0 | I_1, Y_1) \) and \( H(I_1 | I_0, Y_0) \), respectively. Each difference equals an average mutual information).

It should be noted that the correspondence between probabilities and areas is possible only because we started with independent \( I_0 \) and \( I_1 \). An arbitrary distribution \( P(z_0, x_1) \) cannot be drawn by partitioning the unit square into rectangles; therefore, in general, the Shannon outer bound cannot be computed using such a picture. Nevertheless, the kind of dependency that we will encounter in strategies (the dependency arising from previous input and output pairs) can be represented in a square. How this can be done is explained in the next section.

2.3.2. The inner bound resolution for the derived channel

Again we consider Example (2.3.1.3). In Section 2.3.1, we represented the simultaneous distribution of inputs and outputs in a unit square, for a single transmission over the channel with independent users. The distribution of the input \( I_i \), \( P(x_i) \), could be chosen freely by user \( i \). In Figure (2.3.1.4), the distribution choice of user 0 is visible as the positions of the horizontal lines cutting the square; user 1's choice corresponds to the vertical lines in the picture. We call these lines, or more accurately, the positions of these lines, the thresholds for user 0 and 1. We have called this the graphical representation of an inner bound resolution.

Now we consider an inner bound resolution for \( \mathcal{K}(2) \) and its graphical
representation. As an illustration, suppose that user 0 sent $I_{00}=2$. The number of strategies of length 2 for user 0 that start with $I_{00}=2$ equals 9: indeed, user 0 can either receive $r_{00}=1$ or $r_{00}=2$; in either case he can send $I_{01}=0$, 1 or 2, depending on $r_{00}$. The probability distribution for these 9 strategies, $P(z_0^2)$, is drawn as the horizontal thresholds in Figure (2.3.2.1) that partition the lower part of the unit square into 9 rows.

If we draw all horizontal and vertical thresholds according to $P(z_0^2)$ and $P(z_1^2)$ in the unit square, then we have the graphical representation for the inner bound resolution for $\mathcal{C}(2)$. In other words, the strategy distribution $P(z_0^2) \cdot P(z_1^2)$ corresponds to a partitioning of the square into subrectangles.

In this way we can represent an inner bound resolution for the derived channel $\mathcal{C}(N)$ for all $N$ and for any channel $\mathcal{K}$. Consider the graphical representation of a transmission over $\mathcal{C}(N)$ for some channel $\mathcal{K}$. Then each point on user 0's unit interval (i.e., each horizontal line in the square) corresponds to a choice of
input letter \( \bar{I}_0^N \) for the TWC \( \mathcal{K}(N) \) and every vertical line corresponds to a choice of \( \bar{I}_1^N \). The relation between the points on the two unit intervals and the input strategies \( \bar{I}_0^N \) and \( \bar{I}_1^N \) is described more formally in Definition (2.3.2.2).

(2.3.2.2) Definition. Let \( N \in \mathbb{N} \) and let \( \bar{X}_i^N \) be the input alphabet of user \( i \) for the TWC \( \mathcal{K}(N) \). Two mappings \( \sigma_0 \) and \( \sigma_1 \):

\[
\sigma_i : [0,1) \rightarrow \bar{X}_i^N \quad (i = 0, 1),
\]

are strategy functions if the set-valued inverse \( I_i \) of \( \sigma_i \), defined by

\[
I_i(\bar{x}_i^N) := \{ \theta_i \in [0,1) \mid \sigma_i(\theta_i) = \bar{x}_i^N \},
\]

is a subinterval of \([0,1)\) for all \( \bar{x}_i^N \in \bar{X}_i^N \). We call \( I_i(\bar{x}_i^N) \) a basic interval for user \( i \). A region \( I_0(\bar{z}_0^N) \times I_1(\bar{z}_1^N) \) is called a basic rectangle.

Now it is not difficult to see that a pair of strategy functions uniquely defines a product distribution on the pair \((\bar{I}_0^N, \bar{I}_1^N)\): we have

\[
Pr\{ \bar{I}_0^N = z_0^N \} = Pr\{ \sigma_0(\theta_0) = \bar{z}_0^N \} = Pr\{ \theta_0 \in I_0(\bar{z}_0^N) \} = \text{length } (I_0(\bar{z}_0^N))
\]

if \( \theta_0 \) is distributed uniformly over the interval \([0,1)\). In the same way the area of the basic rectangle \( I_0(\bar{z}_0^N) \times I_1(\bar{z}_1^N) \) equals \( Pr\{ \bar{I}_0^N = \bar{z}_0^N \text{ and } \bar{I}_1^N = \bar{z}_1^N \} \). Therefore the strategy functions describe a strategy distribution and hence an inner bound resolution for \( \mathcal{K}(N) \). Conversely, if a strategy distribution \( P(\bar{z}_0^N, \bar{z}_1^N) = P(\bar{z}_0^N)P(\bar{z}_1^N) \) is given, then this corresponds to an inner bound resolution for \( \mathcal{K}(N) \); its graphical representation provides a way to find the corresponding strategy functions.

We can rewrite the expression for \( g_i((N)/N \) in Theorem (2.2.6) using the strategy functions. The distribution \( P(\bar{z}_0^N, \bar{z}_1^N) = P(\bar{z}_0^N)P(\bar{z}_1^N) \) needed in Theorem (2.2.6) is derived from the uniform distribution of \((\theta_0, \theta_1)\) on the unit square, via the relation \( P(\theta_0, \theta_1) = P(\theta_0)P(\theta_1) \) and using the strategy functions \( \sigma_0 \) and \( \sigma_1 \):

\[
Pr\{ (\bar{x}_0^N, \bar{x}_1^N) = (\bar{z}_0^N, \bar{z}_1^N) \} = Pr\{ \theta_0 \in I_0(\bar{z}_0^N) \} \cdot Pr\{ \theta_1 \in I_1(\bar{z}_1^N) \}.
\]
Let us now define \( H(\tilde{y}_1^N | \theta_1) \). Note that \( \theta_1 \) ranges over \([0, 1)\), so we cannot use the definition for discrete variables. For given \( \sigma_0 \) and \( \sigma_1 \), let \( I_k, k = 1, 2, \ldots, I \), enumerate all possible basic intervals \( I_1(\tilde{z}_1^N) \). Then we define

\[
H(\tilde{y}_1^N | \theta_1) := - \sum_{k=1}^I Pr(\theta \in I_k) \sum_{\tilde{y}_1^N} Pr(\tilde{y}_1^N | \theta \in I_k) \log Pr(\tilde{y}_1^N | \theta \in I_k).
\]

With this definition, we find

\[
H(\tilde{y}_1^N | \tilde{y}_1^N) = H(\tilde{y}_1^N | \theta_1),
\]

which yields the following theorem.

(2.3.2.3) Theorem. We have

\[
G_1(\tilde{y}_1^N) = \text{co} \cup \{ (R_0/N, R_1/N) | R_0 \leq H(\tilde{y}_1^N | \theta_1), R_1 \leq H(\tilde{y}_1^N | \theta_0),
\]

\[
(\tilde{y}_1^N, \tilde{y}_1^N) = f_{\theta}(\tilde{y}_1^N, \tilde{y}_1^N), \tilde{y}_1^N = \sigma_0(\theta_0), \tilde{y}_1^N = \sigma_1(\theta_1),
\]

where the union is taken over all strategy functions \( \sigma_0, \sigma_1 \).

Henceforth, we will call the pair \((H(\tilde{y}_1^N | \theta_1)/N, \sigma(\tilde{y}_1^N | \theta_0)/N)\) occurring in Theorem (2.3.2.3) the rate pair of the strategy distribution corresponding to \( \sigma_0, \sigma_1 \). In Chapter 3, we will use (2.3.2.3) for the computation of points in \( G_1(\tilde{y}_1^N) \) and other regions that can be found using similar graphical representations.

2.4. Simplification of graphical representations

Pictures like Figure (2.3.1.4) tend to become illegible if we draw all thresholds for a \( K(N) \) resolution in a unit square, even for small values of \( N \). The aim of
this section is to simplify the figures. In Section 2.3.2, we considered strategies as input letters for $\kappa^{(N)}$ without looking at the separate transmissions for $\kappa$. Here we will take a slightly different viewpoint: we will look at the $N$ transmissions step-by-step. This will enable us to draw the thresholds for $P(\tilde{x}^N_i)$ in $N$ separate unit squares: one for each transmission. Later on in this section we will simplify this even further by splitting the square into separate regions.

As we have seen in Figure (2.3.2.1), the $\kappa^{(2)}$ resolution for Example (2.3.1.3) is already too complicated to draw in one square. Therefore we will take the BMC (Example (2.1.2)) as our example in this section. Figure (2.4.1) shows a $\kappa^{(2)}$ resolution for the BMC. Each row corresponds to one strategy $z^2_0$ and each column corresponds to one strategy $z^2_1$. As an example, the third row from the bottom corresponds to the strategy where user 0 first sends $I_{00} = 1$; if $r_0 = 1$, then he sends $I_{01} = 1$ and if $r_0 = 0$ then he sends $I_{01} = 0$. The numbers in the rectangles represent the two outputs $r_0, r_1$ (remember that the BMC is a T-channel, so $r_0$ and $r_1$ denote the first and second output for both users).

![Figure (2.4.1)](image)

(2.4.1) Figure. Graphical representation of $\kappa^{(2)}$ resolution for the BMC.

Figure (2.4.2) shows how the above figure can be decomposed into two separate squares, one for the first transmission and one for the second transmission. Each
number in a rectangle in the top figure represents the output $Y_0$ corresponding to the strategy pair; the numbers in the bottom figure are the second outputs, $Y_1$.

\[
\begin{array}{ccccccc}
0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 1 & 1 & 0 \\
0 & 0 & 1 & 1 & 1 & 1 & 0 \\
0 & 0 & 1 & 1 & 1 & 1 & 0 \\
0 & 0 & 1 & 1 & 1 & 1 & 0 \\
\end{array}
\]

\[
\downarrow
\]

\[
\begin{array}{ccccccc}
0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 1 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 1 & 0 & 1 & 0 \\
\end{array}
\]

(2.4.2) Figure. The $\mathcal{K}^{(2)}$ resolution of Figure (2.4.1) with separate pictures for each transmission.

A further simplification can be obtained as follows. If the two users each choose a strategy (hence a pair $(\theta_0, \theta_1)$, corresponding to a row and a column) and send the first input according to this strategy, then user $i$ can determine in which part of the square the pair $(\theta_0, \theta_1)$ lies, using $\theta_i$ and $Y_0$. The common knowledge of both users enables them to determine a part of the square of which they both know that $(\theta_0, \theta_1)$ lies in it. In this way, by looking at all strategy
pairs, we can partition the square into such regions. These regions will be called 
'connected'. The definition of this is given below.

(2.4.3) Definition. Consider a graphical representation of a $K^{(N)}$ transmission, 
with the output sequences $(Y_0^N, Y_1^N)$ written in each subrectangle. Let $0 \leq n \leq N$. 
We call two rectangles in one row 0--connected at level $n$ if the same $Y_0^n$ (i.e., the 
first $n$ symbols of $Y_0^N$) is written in both rectangles; two rectangles in one column 
are 1--connected at level $n$ if they have the same $Y_1^n$. Two rectangles are connected 
at level $n$ if they are either 0-- or 1--connected at level $n$. The transitive closure of 
this relation leads to the definition of connected regions at level $n$. 

This definition implies that two rectangles in a row are 0--connected at 
level $n$ if and only if user 0 cannot determine in which of the two rectangles the 
pair $(\theta_0, \theta_1)$ lies after the first $n$ transmissions. To fully appreciate the definition 
of 0-- and 1--connectedness, it is best to illustrate it using a non--T--channel; we 
take Figure (2.3.1.4). The top row of this figure contains three rectangles. The left 
one is not 0--connected at level 1 to any other, but the other two are 0--connected 
at level 1 because they both have $Y_0^1 = 0$. There are three connected regions at 
level 1: the rectangle in the middle, the two right--hand rectangles in the bottom 
row and the remaining part of the square. For the BMC in Figure (2.4.2), we find 
two connected regions at level 1: the rectangle in the lower right--hand corner 
corresponding to $Y_0^1 = 1$ and the L--shaped region where $Y_0^1 = 0$.

With this definition, we now introduce the concept of 'strategy tree'. A 
strategy tree is a representation of a $K^{(N)}$ resolution in a tree with depth $N$, where 
the $(n+1)^{th}$ transmission over $K$ is found at level $n$ $(0 \leq n \leq N-1)$ in the tree. For 
the first transmission, we draw the thresholds corresponding to the distribution 
$P(\bar{z}_0^N) \cdot P(\bar{z}_1^N)$ and we write the first output pairs $(Y_{00}^1, Y_{10}^1)$ (or just $Y_0^1$, for a T--
channel) in all rectangles. The square representing this transmission is the root of the strategy tree. Let the first transmission be such that the square is split into $q$ connected regions at level 1: $A_1, A_2, \ldots, A_q$ with $\cup (A_i) = [0,1)^2$. The second transmission will then be drawn in $q$ separate pictures, one for each $A_i$, and these appear in the tree at level 1 as successors of the root. Each vertex $A_i$ is cut into subrectangles, in which the second output pair $(r_{01}, r_{11})$ (or just $r_1$) is written. Each $A_i$ is decomposed into connected regions at level 2 and we proceed with the third transmission. Subdividing the square further with decomposition into connected regions at all levels thus results in a tree where each vertex represents a partitioning of the part of the square corresponding to its predecessor. As an example, the tree corresponding to Figures (2.4.1) and (2.4.2) is drawn below.

\begin{verbatim}
0 0 0 0 0 0
0 0 0 0 0 0
0 0 1 1 1 1
0 0 1 1 1 1
0 0 1 1 1 1
0 0 1 1 1 1
\end{verbatim}

(2.4.4) Figure. Strategy tree for a $k^{(2)}$ resolution for the BMC.
A $k^{(N)}$ strategy tree has $N$ levels of vertices, where the root has level 0 and the leaves have level $N-1$. Let the two users apply strategies corresponding to a pair $(\theta_0, \theta_1)$ and let $n < N$. By definition of connectedness we see that, after the first $n$ transmissions, the transmitted input sequence $I^n_i$ and output sequence $J^n_i$ received up to that moment enable user $i$ to determine the vertex at level $n$ corresponding to the connected region at level $n$ in which $(\theta_0, \theta_1)$ lies. Thus, in the $(n+1)^{th}$ transmission, the users have to look at the partitioning of this vertex only instead of the whole unit square. This observation will be important in Chapter 3, where we are going to compute the rate of a strategy distribution using its strategy tree. As a consequence of these computations, we will also be able to present further simplifications of strategy trees in Chapter 3.

### 2.5. Partition patterns

In this section we present another way to represent the fact that two rectangles are 0-connected or 1-connected at level 1, if the input alphabets of the channel have at most three elements. From this representation, called the partition pattern of the channel, we obtain an equivalence relation on ternary TWCs. This enables us to count how many 'essentially different' ternary channels there are; by generalization of this argument, we find the number of nonequivalent TWCs over arbitrary alphabets.

Consider a deterministic ternary TWC with $X_0 = X_1 = Y_0 = Y_1 = \{0, 1, 2\}$; for a moment, we will take Example (2.3.1.3). In Figure (2.5.1), the inner bound resolution for this channel is shown, with all input probabilities equal to $1/3$. The unit square is divided into nine subsquares, some of which are 0- or 1-connected at level 1. If two squares in a row are 0-connected, we draw a dashed vertical line.
between them (viewed cyclically: if the first and last one are connected, we draw dashed lines to the left and right ends of the row). Between two 1-connected squares, we draw a dashed horizontal line. The configuration of solid and dashed lines in the figure (i.e., the graphical representation of the inner bound resolution without output symbols) is called the partition pattern of the TWC.

\begin{figure}[h]
\centering
\begin{array}{|c|c|}
\hline
10 & 01 & 00 \\
\hline
20 & 00 & 20 \\
\hline
10 & 22 & 21 \\
\hline
\end{array}
\caption{Partition pattern of $K$.}
\end{figure}

Since we are interested in codes, achievable rates and capacity regions for TWCs, it is clear that the actual input and output symbols of a particular channel are not important: there will be many ternary channels that have the same capacity region as Example (2.3.1.3). For instance, if we permute the output alphabets of one or more users, this will not influence the mutual information corresponding to a $k(n)$ resolution: only the conditional entropy of an output symbol is used, not the output symbol itself. It is also possible to change any code for the original channel to a code having the same rate for the channel with permuted alphabets. Because of this, we have the following theorem, first stated in [JAC86].

\begin{theorem}
All ternary deterministic channels having the same partition pattern have the same capacity region.
\end{theorem}
The importance of this theorem follows if we determine the number of TWCs with all alphabets equal to \( \{0, 1, 2\} \). This number is equal to \( 9^9 \): for every one of the nine input combinations \( (x_0, x_1) \), we can define the outcome \( (y_0, y_1) \) in nine ways. Hence there are more than \( 3 \cdot 10^8 \) ternary TWCs. If we count all TWCs that have the partition pattern of Figure (2.5.1), we find \( (6^6)/2 = 23,328 \) channels with this pattern. Therefore Theorem (2.5.2) gives a significant reduction of the number of channels to be inspected.

However, if we permute the input alphabets and/or permute the user numbers 0 and 1, the characteristics of a channel do not change either (swapping users reflects every rate pair — and hence the capacity region — in the \( I_0 = I_1 \) axis, but we will consider a capacity region and its reflection the same). Therefore we define the following equivalence relation.

\[
(2.5.3) \text{Definition. Two ternary TWCs } \mathcal{K}_1 \text{ and } \mathcal{K}_2 \text{ are equivalent } (\mathcal{K}_1 \equiv \mathcal{K}_2) \text{ if the partition pattern of } \mathcal{K}_1 \text{ can be transformed into the partition pattern of } \mathcal{K}_2 \text{ by permutation of rows, columns and/or user numbers.} \]

The following theorem is now immediate.

\[
(2.5.4) \text{Theorem. TWCs that are equivalent under relation } \equiv \text{ have the same (or reflected) capacity regions.} \]

Using Pólya theory, Jacobs [JAC86] found that the number of equivalence classes of \( \equiv \) equals 322. This was a considerable improvement over an earlier result by Gaal [GAA85], who had defined an equivalence relation with 152,176 classes.

The partition pattern approach has the disadvantage that it requires
alphabet size at most three: with four rectangles in a row, 0–connected but non-adjacent rectangles cannot be drawn using dashed and solid lines. Van der Ham [HAM87] generalized the theory developed by Jacobs and was able to compute the number of equivalence classes of TWCs for arbitrary alphabets. Unfortunately he found that the number of classes increases rapidly with the alphabet size: for alphabet size four he found 2,336,169 different classes! For this reason, channels over larger alphabets have not been studied in great detail yet.

Jacobs found that partition patterns could be used to derive bounds on capacity regions. To this aim she introduced 'dominating part patterns', further investigated by Engels [ENG87]. Since very little is known about this, we shall use partition patterns in this thesis as representations of ternary channels only.
Chapter 3: Strategy Trees for Two-Way Channels

3.1. The rate of a tree

In this chapter we look again at the inner bound resolution for the derived channel $\mathcal{X}^N$, studied in Section 2.3.2. In Theorem (2.3.2.3), we found that the mutual information appearing in the Shannon inner bound expression could be written as $(H(T^N_1|\theta_1)/N, H(T^N_0|\theta_0)/N)$ for given strategy functions $\sigma_0$, $\sigma_1$. We will introduce the notation $I(\sigma_0, \sigma_1)$ for this:

\[(3.1.1) \ I(\sigma_0, \sigma_1):= (H(T^N_1|\theta_1)/N, H(T^N_0|\theta_0)/N).\]

The rate pair $I(\sigma_0, \sigma_1)$ can be computed from the graphical representation of the derived channel by using the areas of subrectangles in the square, in exactly the same way as was shown in Section 2.3.1 for $N = 1$. Here we look at the square as a whole, i.e., the simplifications introduced in Section 2.4 are not reflected in the computations.

However, we also study some related notions in this chapter: more general types of partitionings of the unit square that can be derived from trees. For these partitionings we wish to define rate pairs too, because then we have the analogue of Theorem (2.2.6) stating that these rates are achievable and they cover the whole capacity region if the partitionings are sufficiently complex.

The rate of such a tree, say $I(\mathcal{T})$ if the tree is called $\mathcal{T}$, will be defined as the weighted average of the mutual information in each vertex of the tree. See Definition (3.1.3) below. Theorem (3.1.4) states the fact that for the $\mathcal{X}^N$ inner
bound resolution as described in Section 2.3.2, it makes no difference whether we compute the rate using (3.1.1), or using Definition (3.1.3).

First of all we will define the rate of a vertex in a tree. To this aim we consider a $K^{(N)}$ resolution with strategy functions $\sigma_0$ and $\sigma_1$. If $A$ is a vertex in the corresponding strategy tree at level $n$, then we define

$$H(Y_1^n | \theta_1^n, \theta_0, \theta_1 \in A) := - \sum_{y_{1n}, \theta_1^n, y_1^n} Pr\{Y_{1n} = y_{1n}, \theta_1 = \theta_1^n, Y_1^n = y_1^n | (\theta_0, \theta_1) \in A\} \cdot \log Pr\{Y_{1n} = y_{1n}, \theta_1 = \theta_1^n, Y_1^n = y_1^n, (\theta_0, \theta_1) \in A\},$$

and $H(Y_0^n | \theta_0, \theta_1^n, (\theta_0, \theta_1) \in A)$ is defined analogously.

(3.1.2) Definition. Let $N \in \mathbb{N}$. Consider an inner bound resolution for the derived channel $K^{(N)}$ with strategy functions $\sigma_0$ and $\sigma_1$ and strategy tree $T$. Let $A$ be a part of the unit square that occurs as a vertex at level $n$ in $T$. The rate of $A$, $\tau(A) = (r_0(A), r_1(A))$, is defined by

$$\tau(A) := (H(Y_{1n} | \theta_1^n, (\theta_0, \theta_1) \in A), H(Y_{0n} | \theta_0, (\theta_0, \theta_1) \in A))$$

where $(\theta_0, \theta_1)$ is uniformly distributed over the unit square and $(Y_0^{n+1}, Y_1^{n+1})$ depends on $(\theta_0, \theta_1)$ via the functions $\sigma_0$, $\sigma_1$ and $f_K$.

The weight of $A$, $w(A)$, is defined as the area of region $A$, so

$$w(A) := Pr\{ (\theta_0, \theta_1) \in A \}. \quad \Box$$

The rate of $A$ can be understood as the amount of information that is transmitted with the inputs $(Y_{0n}, Y_{1n})$ if we only look at region $A$. Hence we consider the case where after the first $n$ transmissions, the outputs $y_0^n$ and $y_1^n$ are such that both users know that connected region $A$ is the only part of the square in which $(\theta_0, \theta_1)$ can be.
Chapter 3

(3.1.3) Definition. Consider a strategy tree for $X^{(N)}$ as in Definition (3.1.2). Call this tree $T$ and call its vertices $A_{n,i}$, where $n \in \{0,1,\ldots,N-1\}$ ranges over the levels and $i \in \{0,1,\ldots,m_n-1\}$ ranges over all nodes at level $n$. Here $m_n$ is the number of nodes at level $n$. The rate of the tree $T$, $R(T)$, is defined by

$$R(T) = \left( R_0(T), R_1(T) \right) := \frac{\sum_n \sum_i w(A_{n,i}) \cdot r(A_{n,i})}{\sum_n \sum_i w(A_{n,i})}.$$  

Now we show that the rate of a $X^{(N)}$ resolution can be computed by (3.1.3).

(3.1.4) Theorem. Consider a $X^{(N)}$ strategy distribution with strategy functions $\sigma_0$ and $\sigma_1$ and strategy tree $T$. The following equality holds.

$$R(\sigma_0, \sigma_1) = R(T).$$

Proof: As before, let the vertices of $T$ be labeled as $A_{n,i}$, where $n$ denotes the level of the vertex and $i \in \{0,1,\ldots,m_n-1\}$ ranges over all vertices in level $n$. Then

$$H(Y_1^{N} | \theta_1) = H((Y_{10}, Y_{11}, \ldots, Y_{1,N-1}) | \theta_1)$$

$$= \sum_{n = 0, \ldots, N-1} H(Y_{1n} | \theta_1, Y_{1n}^{m_n}) \quad \text{by the chain rule}$$

$$= \sum_{n = 0, \ldots, N-1} H(Y_{1n} | \theta_1, Y_{1n}^{m_n}, A_n),$$

if $A_n$ is a random variable with values in $\{A_{n,i} \mid 0 \leq i < m_n\}$ and $A_n$ assumes the value of the vertex uniquely determined by $\theta_1$ and $Y_{1n}^{m_n}$ (which is the same as the vertex determined by $\theta_0$ and $Y_{0n}$). Hence $A_n$ is a deterministic function of $\theta_1$ and $Y_{1n}^{m_n}$, which explains the last equality in the above derivation. We find

$$H(Y_{1n} | \theta_1, Y_{1n}^{m_n}, A_n) = \sum_i \Pr\{ (\theta_0, \theta_1) \in A_n,i \} \cdot H(Y_{1n} | \theta_1, Y_{1n}^{m_n}, (\theta_0, \theta_1) \in A_n,i)$$

$$= \sum_i w(A_{n,i}) \cdot r_0(A_{n,i})$$

- 36 -
and hence
\[
\mathcal{H}(\hat{T}_1^n|\theta_1) = \sum_{n=0}^{N-1} \sum_{i=0}^{m_n-1} w(A_n,i) \cdot r_0(A_n,i).
\]
By definition of the strategy tree \(T\), the connected regions occurring in a fixed level of \(T\) partition the unit square. Therefore
\[
\sum_{n=0}^{N-1} \sum_{i=0}^{m_n-1} w(A_n,i) = \sum_{n=0}^{N-1} 1 = N.
\]
Finally we have
\[
\mathcal{H}(\hat{T}_1^n|\theta_1)/N = \frac{\sum \sum w(A_n,i) \cdot r_0(A_n,i)}{\sum \sum w(A_n,i)},
\]
which is the first component of the tree rate according to Definition (3.1.3). Clearly the second component is computed analogously. \(\square\)

Definition (3.1.3) can be reduced to (3.1.5) in the case of a T-channel.

(3.1.5) \(\mathcal{I}(A) = (\mathcal{H}(Y_n|\theta_1, (\theta_0, \theta_1) \in A), \mathcal{H}(Y_n|\theta_0, (\theta_0, \theta_1) \in A)).\)

This holds because for a T-channel, all subrectangles within one connected region \(A\) at level \(n\) correspond to the same output sequence, say \(y^n(A)\). This follows from Definition (2.4.3). Therefore \((\theta_0, \theta_1) \in A\) implies \(Y_0^n = Y_1^n = y^n(A)\), so \(Y^n\) is not needed in the condition. Formula (3.1.5) is convenient for computing the rate of a T-channel strategy tree.

As an example, consider the strategy tree in Figure (2.4.4). Let us assume that all rows and columns are equally wide, so that each subrectangle in the square has area \((1/6) \cdot (1/6)\). The rate of the root, \(\mathcal{I}(A_0,0)\), is given by
\[
r_0(A_0,0) = \sum_{\bar{z}_1} Pr(\theta_1 \in I_1(\bar{z}_1^2)) \cdot \mathcal{H}(Y_0|\theta_1 \in I_1(\bar{z}_1^2)).
\]
and similarly \( r_1(A_0, 0) = (2/3) \cdot h(2/3) \). For the left-hand leaf, \( A_1, 0 \), we have

\[
\begin{align*}
\sum_{z_1^2} P\{ \theta_1 \in I_1(z_1^2) \} \cdot H(Y_0 \mid \theta_1 \in I_1(z_1^2), (\theta_0, \theta_1) \in A_1, 0 \\
= \frac{1}{20/36} \left\{ (6/36) \cdot 0 + (6/36) \cdot h(1/2) + 2 \cdot (2/36) \cdot 0 + 2 \cdot (2/36) \cdot h(1/2) \right\} \\
= 1/2
\end{align*}
\]

and \( r_1(A_1, 0) = 1/2 \). Finally, for the right-hand leaf \( A_1, 1 \), we find

\[
\begin{align*}
\sum_{z_1^2} P\{ \theta_1 \in I_1(z_1^2) \} \cdot H(Y_0 \mid \theta_1 \in I_1(z_1^2), (\theta_0, \theta_1) \in A_1, 0 \\
= \frac{1}{16/36} \left\{ 2 \cdot (4/36) \cdot 0 + 2 \cdot (4/36) \cdot h(1/2) \right\} = 1/2.
\end{align*}
\]

From this example we see that the rate of a vertex at level \( n \) only depends on the areas of subrectangles corresponding to a certain output \( Y_n \) within one column or within one row. This means that if we permute certain rows and/or columns within a vertex, this does not change the lengths or widths of subrectangles and hence \( H(Y_n \mid \theta_1, (\theta_0, \theta_1) \in A) \) and \( H(Y_n \mid \theta_0, (\theta_0, \theta_1) \in A) \) are not changed by permutation (even if not all rows and columns are equally wide!). It also means that, when computing the \( r_0 \)-component of a rate, two 1-connected rectangles do not have to distinguish: we only need the total area of both rectangles and not the two separate areas. Therefore we can draw two neighboring 1-connected rectangles as one big rectangle by deleting the part of the horizontal threshold that separates them. Of course we can also delete vertical thresholds between 0-connected rectangles (therefore, in the case of a T-channel, the term 'connected regions' has a very practical meaning: if there are no borders between two rectangles, then they are connected).

In other words, if we permute rows and columns in the vertices of Figure (2.4.4) and delete borders between connected rectangles such that Figure (3.1.6)
results, the rate of each vertex in Figure (3.1.6) is still the same as each rate in Figure (2.4.4). The 'permuted' thresholds in Figure (3.1.6) have a useful interpretation. The horizontal thresholds occurring in a vertex $A$ at level $n$ represent the probability distribution of $I_{0n}$ conditional to the previous inputs and outputs of user 0. Similarly the vertical thresholds depict the distribution of $I_{1n}$ given $I_1^n$ and $I_1^n$. This will be explained further below Figure (3.1.7).

![Strategy tree diagram]

(3.1.6) Figure. Simplified strategy tree for a $k^{(2)}$ resolution for the BMC.

It should be noted that the above observations arising from computations for the BMC only hold for T-channels. For a channel like Example (2.3.1.3), we are not allowed to permute complete columns in a vertex, since we are interested in $H(Y_{1n},\theta_1,\Lambda_{n,i})$ instead of $H(Y_{1n},\theta_1,\Lambda_{n,i})$. Hence
we may only permute parts of columns corresponding to the same $I_1^0$, i.e., the parts of columns lying in 1-connected rectangles. Similarly we may permute rows only within 0-connected rectangles. As an example, the part of the square corresponding to $I_{00}=2$ as depicted in Figure (2.3.2.1) may be transformed to Figure (3.1.7) (assuming that the total lengths and widths of the rectangles are the same in both figures). The reader should convince himself that this does not influence the rate. It goes without saying that a picture like Figure (3.1.7) is considerably more comprehensible than Figure (2.3.2.1).

\[
\begin{array}{ccc}
I_{10} = 0 & I_{10} = 1 & I_{10} = 2 \\
I_{01} = 0 & I_{01} = 0 & I_{01} = 0 \\
I_{01} = 1 & I_{01} = 1 & I_{01} = 1 \\
I_{01} = 2 & I_{01} = 2 & I_{01} = 2 \\
I_{00} = 1 & I_{00} = 2 & I_{00} = 2
\end{array}
\]

(3.1.7) Figure. Simplification of Figure (2.3.2.1).

In Figure (3.1.7), the permuted thresholds in each of the connected rectangles again represent distributions $P(x_{01}|x_{00},y_{00})$. If we normalize the thresholds to the unit interval (i.e., consider user 0's interval corresponding to $I_{00}=2$ as having size 1), the thresholds for the left-hand rectangle represent $P(x_{01}|I_{00}=2,Y_{00}=1)$ and the thresholds for the right-hand pair of rectangles depict $P(x_{01}|I_{00}=2,Y_{00}=2)$. Note that there is just one probability distribution for the two 0-connected rectangles on the right, since both of these rectangles correspond to $I_{00}=2$ and $Y_{00}=2$. In the figure, this is reflected in the fact that the horizontal lines run over the entire area of these two rectangles.
This simplification makes it possible to draw strategy trees also for non-T-channels, if $N$ is not too large. Figure (3.1.8) illustrates this: it shows the complete strategy tree for a $\kappa^{(2)}$ resolution over the channel of Example (2.3.1.3). The detail shown in Figure (3.1.7) appears in two separate vertices of the tree: the left-hand rectangle occurs in the bottom part of the leaf on the left and the two 0-connected rectangles form the leaf on the right.

(3.1.8) Figure. Strategy tree for the channel of Example (2.3.1.3).

In the remaining part of this chapter, we will draw all strategy trees using the simplifications described in Section 2.4 and in this section.
Chapter 3

3.2. Fixed length trees

3.2.1. Fixed length trees and the capacity region

Here we will introduce a new notation for the inner bound resolution of the derived channel $\mathcal{K}^{(N)}$: we will call it an $F(N)$ tree. In this way the analogy between fixed and variable length trees (that will be studied in Section 3.3) will be stressed, since the '$F'$ in this notation is an abbreviation for 'fixed length' and the trees in Section 3.3 will be denoted as '$V(N)$ trees' where the '$V$' means 'variable length'.

For an arbitrary tree, we define the distance between two vertices on a path from the root to a leaf as usual; we define the depth of a tree as the maximum distance between any vertex and the root. Hence a strategy tree for a $\mathcal{K}^{(N)}$ resolution has depth $N-1$.

(3.2.1.1) Definition. Let $N \in \mathbb{N}$. An $F(N)$ tree for $\mathcal{K}$ is a strategy tree for an inner bound resolution for $\mathcal{K}^{(N)}$. Furthermore we define

$$\mathcal{T}(N) := \{ T(T) \mid T \text{ is an } F(N) \text{ tree for channel } \mathcal{K} \},$$

$$\mathcal{T} := \bigcup_{N \in \mathbb{N}} \mathcal{T}(N).$$

By (3.1.1) and Theorem (3.1.4), we can now state Theorem (2.2.6) as

$$\forall N \in \mathbb{N} \left[ \co \mathcal{T}(N) \subset C \right] \text{ and } \lim_{N \to \infty} \co \mathcal{T}(N) = C.$$

In Theorem (3.2.1.2) this is formulated differently, namely in such a form that it can be generalized for variable length (and other) trees. For an arbitrary region $\mathcal{A}$, let $\overline{\mathcal{A}}$ denote the closure of $\mathcal{A}$. We can state the following.
(3.2.1.2) Theorem. We have

\[ \forall N \in \mathbb{N} \left[ \co \mathcal{F}(N) \subseteq C \right] \quad \text{and} \quad \lim_{N \to \infty} \mathcal{F}(N) = \bar{F} = C. \]

Proof: see Section 3.5.

The reason why we postpone the proof to Section 3.5 is the following. The proof of Theorem (3.2.1.2) is similar to the proofs of the generalized theorems in the following sections; we can use this theorem and a part of its proof to prove some of the other theorems. It seems more natural to give all of the proofs together in one section because then the relation between them is more evident.

3.2.2. Fixed length trees ending in rootlike rectangles

In this section we will study a special type of fixed length tree, namely one in which all connected regions that are not partitioned any further (that is, the resulting regions of the splitting in the leaves) must be so-called rootlike rectangles, defined below.

(3.2.2.1) Definition. Consider a strategy tree of depth \( N - 1 \). For \( 0 \leq n \leq N \), a rootlike rectangle at level \( n \) is a connected region \( A \) at level \( n \) that occurs in the tree as a result of the partitioning of the square after \( n \) transmissions such that the following holds for \( A \).

(i) The region \( A \) is a rectangle; that is, a uniform distribution of \((\theta_0, \theta_1)\) over \( A \) implies independence between \( \theta_0 \) and \( \theta_1 \).

(ii) For \( i \in \{0,1\} \): only one output sequence \( y_i^n \) for user \( i \) corresponds to region \( A \). Hence if \((\theta_0, \theta_1) \in A, y_0^n \) and \( y_1^n \) do not depend on the positions (or basic intervals) of \( \theta_0 \) and \( \theta_1 \) within \( A \).
Let us take a more detailed look at rootlike rectangles. Since we are considering 'full' trees only (i.e., trees in which every part of the square is partitioned at every level), all rootlike rectangles at level \( n \) for \( n < N \) are vertices at level \( n \), and all rootlike rectangles at level \( N \) are regions remaining after splitting in the leaves. Note that for a T-channel, condition (iii) is void. This follows from the discussion in Section 2.4. In that case, any rectangular connected region is a rootlike rectangle. Also note that if vertex \( \mathcal{A} \) is a rootlike rectangle at level \( n \), then \( \mathcal{L}(\mathcal{A}) = (\mathcal{H}(Y_{1n} | \theta_1, (\theta_0, \theta_1) \in \mathcal{A}), \mathcal{H}(Y_{0n} | \theta_0, (\theta_0, \theta_1) \in \mathcal{A})) \), because previous outputs add no knowledge about \( Y_{1n} \) and \( Y_{0n} \) if the users know that \( (\theta_0, \theta_1) \in \mathcal{A} \).

Now consider an \( F(N) \) tree. The root of the tree is a rootlike rectangle at level 0, since it is a square and no previous outputs exist. If we compute the rate of this vertex, \( (\mathcal{H}(Y_{10} | \theta_1), \mathcal{H}(Y_{00} | \theta_0)) \), then we use the uniform distribution of \( (\theta_0, \theta_1) \) over the square. Therefore \( \theta_0 \) and \( \theta_1 \) are independent and the first input symbols of both users (that follow from the strategy functions) are independently chosen. In the next transmissions, regions that may have arbitrary shapes are subdivided in the tree. The subsequent inputs of the two users will be dependent since they have knowledge about previous inputs and outputs. Only if region \( \mathcal{A} \) is again a rootlike rectangle, at level \( n \), say, then (i) and (iii) imply independence between the new inputs \( I_{0n} \) and \( I_{1n} \) even though the two users share knowledge about previous outputs. Hence in that case the rate is \( (\mathcal{H}(Y_{1n} | \theta_1, (\theta_0, \theta_1) \in \mathcal{A}), \mathcal{H}(Y_{0n} | \theta_0, (\theta_0, \theta_1) \in \mathcal{A})) \) with independent \( \theta_0 \) and \( \theta_1 \), as if it were the root of the tree. This explains the name 'rootlike rectangle'.

If a rootlike rectangle \( \mathcal{A} \) at level \( N \) occurs in the \( F(N) \) tree, we can use \( \mathcal{A} \) as the root of a new tree. If the new tree has \( k \) levels, then its root occurs at level \( N \) of the old tree, which changes into an \( F(N+k) \) tree in this way. If we use the \( F(N) \) tree itself for the new tree \( (k = N) \) and repeat the procedure \( t \) times, then \( t \) copies of the \( F(N) \) tree form an \( F(tN) \) tree.
What if the regions remaining after the partitioning in the leaves of the $F(N)$ tree are not rootlike rectangles? Let $A$ be such a region consisting of several basic rectangles, corresponding to input pairs $(z_{0}^{N}, z_{1}^{N})$ of the $F(N)$ tree. Let $I \in \mathbb{N}$. Now $A$ may be subdivided using an $F(I)$ tree with strategy distribution $P(z_{0}^{I}, z_{1}^{I}) = P(z_{0}^{I}) \cdot P(z_{1}^{I})$, if the users 'forget' about the dependency in $A$. This new strategy distribution can be represented in $A$ by choosing the same set of horizontal thresholds, corresponding to $P(z_{0}^{I})$, for every basic interval $I_{0}(z_{0}^{N})$ (i.e., every row) in $A$, and the same set of vertical thresholds ($P(z_{1}^{I})$) in every column of $A$. In this way the $F(I)$ tree is 'appended' below the original tree.

It is easy to see that the rates of the new vertices in the $F(N+I)$ tree are equal to those in the $F(I)$ tree itself. If we take the same $F(N)$ tree $t$ times we obtain an $F(tN)$ tree again. Moreover, the $F(tN)$ tree has the same rate as the $F(N)$ tree, since the weighted average of the rates in the vertices does not change. In fact, the technique described here is exactly the same as used by Shannon [SHA61] to prove that $G/N$ is included in $G/(tN)$ for all $t$.

Now that we know the interpretation and the use of rootlike rectangles, we define the following (compare Definition (3.2.1.1)). The 'c' in the notation can be seen as the root of a tree (the unit square), which denotes the fact that we restrict ourselves to rootlike rectangles.

(3.2.2.2) Definition. Let $N \in \mathbb{N}$. An $F^{c}(N)$ tree is an $F(N)$ tree such that every connected region in the tree that is not subdivided any further (i.e., every region remaining after the splitting in the leaves) is a rootlike rectangle. Define

$F^{c}(N) := \{ \mathcal{A}(T) \mid T \text{ is an } F^{c}(N) \text{ tree} \}$,

$F^{c} := \bigcup_{N \in \mathbb{N}} F^{c}(N)$. 

- 45 -
Chapter 3

The theorem below states the analog of Theorem (3.2.1.2): $\mathcal{F}^D(N)$ converges to the capacity region. As before, we postpone the proof to Section 3.5.

(3.2.2.3) Theorem. We have

$$\forall N \in \mathbb{N} \left[ \text{co} \mathcal{F}^D(N) \subset C \right] \quad \text{and} \quad \lim_{N \to \infty} \mathcal{F}^D(N) = \mathcal{F}^D = C.$$  

Proof: see Section 3.5.

As can be seen from Figures (3.1.6) and (3.1.8), most $F(N)$ trees are not $F^D(N)$ trees: usually one or more non-rectangular regions will remain in the leaves. If such non-rectangular regions are not allowed, then this poses restrictions on the transmission in the leaves. Therefore it is likely that the rates in the leaves are lower than in the case of an arbitrary $F(N)$ tree. Because of this restriction, $F^D(N)$ trees are not very useful. However, if we look at the same restriction for variable length trees (to be studied in Section 3.3.2), it turns out to be quite useful there. In the following section we will consider an even stronger restriction for an $F(N)$ tree, having even lower rate; still it is an interesting kind of tree since we can easily derive codes from it.

3.2.3. From fixed length trees to codes and vice versa

This section is devoted to a special kind of $F(N)$ tree, namely one corresponding to a code (in the sense of Definition (2.1.6)). First of all, we will show that any code gives rise to an $F(N)$ tree. Let $\mathcal{M}_0 \in \mathbb{N}$, $\mathcal{M}_1 \in \mathbb{N}$, $N \in \mathbb{N}$ and consider an $(\mathcal{M}_0, \mathcal{M}_1, N)$ code for a deterministic TWC $\mathcal{K}$ defined by function $f_\mathcal{K}$. The message sets are $\mathcal{M}_0$ and $\mathcal{M}_1$ and the encoding functions are called $f_{i,n}$ ($i \in \{0,1\}$, $n \in \{0,1,\ldots,N-1\}$). Using the code, we will construct an $F(N)$ tree that partitions the unit square. We partition user 0's unit interval into $\mathcal{M}_0$...
Strategy Trees for TWCs

intervals of length $1/M_0$. These intervals are labeled $0, 1, \ldots, M_0-1$ such that each interval corresponds to a message $w_0 \in M_0$. In the same way user 1’s unit interval is divided into $M_1$ intervals, indexed with the messages in $M_1$. Hence each of the $M_0 M_1$ rectangles in the square corresponds to a message pair $(w_0, w_1)$.

The strategy functions $\sigma_0$ and $\sigma_1$ will follow from the code. User 0’s sub-interval corresponding to message $w_0$ will be a basic interval $I_0(\tilde{x}_0)$ where the strategy $\tilde{z}_0$ will follow from the encoding functions $f_{0,n}$ for message $w_0$. Similarly each subinterval of user 1 will be linked — via $w_1$ and the encoding functions $f_{1,n}$ — to a strategy $\tilde{z}_1$. The independence between the messages of the two users yields a product distribution on $(\tilde{z}_0, \tilde{z}_1)$. Let $\tilde{z}_0$ be the strategy corresponding to $w_0$. The first symbol $x_{00}$ in the strategy $\tilde{z}_0$ is $f_{00}(w_0)$. In the same way the first letter $x_{10}$ of user 1’s strategy $\tilde{z}_1$ is determined via $f_{10}$. Hence the output pair $(y_{00}, y_{10})$ for the rectangle corresponding to $(w_0, w_1)$ is

$$(y_{00}, y_{10}) = f_1(f_{00}(w_0), f_{10}(w_1)).$$

This explains the partitioning in the root of the tree. The second layer of the tree is partitioned using functions $f_{01}$ and $f_{11}$: if a row corresponds to $w_0$ and user 0’s first output is $y_{00}$; then the input $x_{01}$ for this part of the square is $f_{01}(w_0, y_{00})$.

We can construct a complete $F(N)$ tree like this. Note that the horizontal thresholds in the tree are restricted to coordinates $(i/M_0)$ ($i \in \{0, 1, \ldots, M_0\}$) and the vertical thresholds are multiples of $1/M_1$. We say that the thresholds are on an $(M_0+1) \times (M_1+1)$ grid. Figure (3.2.3.1) shows an $F(3)$ tree for the BMC that corresponds to a $(3,3,3)$ code. We explain the mapping from rows and columns to strategies in this figure by an example. The top row of user 0 corresponds to the following strategy: first send $x_{00} = 0$, such that $y_{00} = 0$ with certainty (root). Then send $x_{01} = 1$ (left-hand vertex at level 1). If $y_{01} = 1$, then send $x_{02} = 1$ (left-hand leaf below this vertex); otherwise send $x_{02} = 0$ (right-hand leaf). This
example also shows how a tree with thresholds on a grid can be interpreted as a code.

\[
\begin{array}{c}
000 \\
011 \\
011
\end{array}
\]

\[
\begin{array}{c}
110 \\
10
\end{array}
\]

\[
\begin{array}{c}
10 \\
0
\end{array}
\]

\[
\begin{array}{c}
00 \\
00
\end{array}
\]

\[
\begin{array}{c}
10 \\
0
\end{array}
\]

\[
\begin{array}{c}
0
\end{array}
\]

\[
\begin{array}{c}
0
\end{array}
\]

\[
\begin{array}{c}
10 \\
0
\end{array}
\]

\[
\begin{array}{c}
0
\end{array}
\]

\[
\begin{array}{c}
10 \\
0
\end{array}
\]

\[
\begin{array}{c}
0
\end{array}
\]

(3.2.3.1) **Figure.** \( F(3) \) tree for the BMC representing a code.

It should be remarked that the code represented in Figure (3.2.3.1) has error probability \( P_{e,0} = P_{e,1} = 0 \), for the appropriate decoding functions: every basic rectangle corresponding to a message pair is a connected region at level 3, and both users can uniquely determine this connected region by looking at their own message and the output sequence of length 3. We also see that the \( F(3) \) tree is in fact an \( F^D(3) \) tree, since all connected regions at level 3 are squares.

This is true for all codes: any \( (\mathcal{M}_0, \mathcal{M}_1, N) \) code can be represented in an \( F(N) \) tree and any zero-error code gives rise to an \( F^D(N) \) tree. Conversely, if we have an \( F(N) \) tree such that all thresholds are confined to an \( (\mathcal{M}_0 + 1) \times (\mathcal{M}_1 + 1) \) grid, then the encoding functions for an \( (\mathcal{M}_0, \mathcal{M}_1, N) \) code can be derived from this tree. Moreover, if every basic rectangle of size \( (1/\mathcal{M}_0) \times (1/\mathcal{M}_1) \) forms a connected region at level \( N \) in the tree, then this yields an error-free decoder for the code: each user can determine the connected region at level \( N \), and hence the message pair, using his own message and the output sequence. A tree in which such an error-free code can be represented will be called an \( F^0(N) \) tree, where the '0'
stands for error probability 0. We also define $\mathcal{F}^0(N)$ and $\mathcal{F}^\prime$, as in Definitions (3.2.1.1) and (3.2.2.2). A theorem like (3.2.1.2) and (3.2.2.3) cannot be given for $\mathcal{F}^0(N)$ and $\mathcal{F}^\prime$, but in Section 3.5 we present a slightly different theorem about these regions.

(3.2.3.2) Definition. Let $N \in \mathbb{N}$. An $\mathcal{F}^0(N)$ tree is an $\mathcal{F}^\prime(N)$ tree on a grid such that all basic rectangles have the same measurements and every basic rectangle is a separate connected region at level $N$. Furthermore

$$
\mathcal{F}^0(N) := \{ \mathcal{A}(T) \mid T \text{ is an } \mathcal{F}^0(N) \text{ tree } \},
$$

$$
\mathcal{F}^\prime := \bigcup_{N \in \mathbb{N}} \mathcal{F}^0(N).
$$

We will show that the rate of a code (Definition (2.1.8)) that is constructed from a tree can be computed via the rate of the tree (Definition (3.1.3)). This is similar to Theorem (3.1.4), where we showed that the rate of a $k(N)$ strategy distribution is equal to the tree rate.

(3.2.3.3) Theorem. Consider an $\mathcal{F}^0(N)$ tree $T$ representing an $(N_0, N_1, N)$ code. The rate of the code is equal to $\mathcal{A}(T)$. 

Proof: By definition, the code rate is $(\log(N_0)/N, \log(N_1)/N)$. From Theorem (3.1.4) we know that we can compute the tree rate $\mathcal{A}(T)$ either per vertex, or in the unit square as a whole. Here we use the latter method:

$$
\mathcal{A}(\tilde{T}_1^N|\theta_1) = \sum_{i = 0, \ldots, N_1 - 1} \Pr\{ \theta_1 \in \left[ \frac{i}{N_1}, \frac{i+1}{N_1} \right] \} \cdot \mathcal{A}(\tilde{T}_1|\theta_1 \in \left[ \frac{i}{N_1}, \frac{i+1}{N_1} \right]).
$$

Since the error probability is 0, user 1 is able to determine the basic rectangle by
Chapter 3

the output sequence $I_1^N$ and by his own message (hence by the column in the square). Hence the $I_0$ output sequences $I_1^N$ occurring within one column must be distinct. Since user 0's messages are equally likely, the same holds for the $I_1^N$ sequences within a column. Therefore the entropy of the output sequence in every column is equal to $\log(I_0)$. We find

$$R_0(T) = H(I_1^N | \theta_1) / N = \sum_{i=0, \ldots, I_1-1} \frac{1}{I_1} \cdot \log(I_0) / N = \log(I_0) / N,$$

which is the $I_0$ component of the code rate. Because a similar relation holds for the $I_1$ component, this proves the equality of the tree rate and the code rate. □

It is interesting to compare this result to Theorem (2.2.6). Shannon has shown that the rate of every $F(N)$ tree is achievable, hence that codes exist having (almost) the same rate as the tree and having arbitrarily small error probability. In this section we have shown the achievability of the rate of a special type of $F(N)$ tree, namely an $F^0(N)$ tree. Not only have we proved, in Theorem (2.2.3.3), the existence of a code with this rate; we have also shown how a such a code can be constructed from the tree. This code even has error probability equal to 0, instead of just tending to 0 with increasing block length. For more examples of zero-error codes and with higher rate, we refer to Section 3.6.

3.3. Variable length trees

3.3.1. Variable length trees and the capacity region

Here we will study one of the generalizations of $F(N)$ trees. If we compute the rate of an $F(N)$ tree, then it may happen that some of the vertices have very
Strategy Trees for TWCs

low \(^1\) rates, lower than the (weighted) average rate of the whole tree. Clearly it is in our interest to construct trees with high rates, since these give good lower bounds on the capacity region of the TWC. Therefore it may be advantageous to delete a subtree having a low rate from the \(F(K)\) tree, thereby increasing the rate of the tree in total. This is why we introduce the following concept.

(3.3.1.1) Definition. Let \(N \in \mathbb{N}\). A variable length tree of maximum length \(N\), abbreviated as a \(V(N)\) tree, is a tree that can be obtained from an \(F(K)\) tree by deleting zero or more vertices and the complete subtrees having these vertices as roots in such a way that the \(V(N)\) tree still has depth \(N-1\).

A variable length tree can be seen as a 'pruned' \(F(K)\) tree. Note that each \(F(K)\) tree is also a \(V(K)\) tree. The definitions for fixed length trees that have been introduced in the previous sections generalize to variable length trees in a natural way. Hence the rate of a \(V(N)\) tree again equals the weighted average of the rates in all vertices.

Rootlike rectangles may also be found in a \(V(N)\) tree; however, as opposed to \(F(K)\) trees, a \(V(N)\) tree may contain a rootlike rectangle at level \(n\), \(n < N\), that is not a vertex. For an example of this, we refer to Figure (3.3.1.2), where the rectangle corresponding to \(Y_0 = 1\) in the root of the \(V(2)\) tree is a rootlike rectangle at level 1 but not a vertex.

\(^1\) We must remark here that the words 'low' and 'high' should not be interpreted too literally, since we are talking about 2-dimensional vectors. A 'high' rate can be seen as having a small Euclidean distance to the border of the actual capacity region, and a 'low' rate is far from the border of \(C\). It may be helpful to think of the sum rate, \(L_0 + L_1\), as a measure for 'high' or 'low' rates.
Figure (3.3.1.2) illustrates the difference between fixed and variable length trees: it shows an $F(2)$ tree and a $V(2)$ tree for the BMC. All thresholds are in the middle of the intervals, i.e., the next input symbol is 1 with probability 0.5 in vertices $A_{0,0}$ and $A_{1,1}$. We compute the rates of the trees by (3.1.3).

\[
\begin{align*}
\omega(A_{0,0}) &= 1, & r(A_{0,0}) &= (1/2, 1/2), \\
\omega(A_{0,1}) &= 3/4, & r(A_{0,1}) &= (2/3, 2/3), \\
\omega(A_{1,1}) &= 1/4, & r(A_{1,1}) &= (1/2, 1/2). \\
K(F(2) \text{ tree}) &= (9/16, 9/16), & K(V(2) \text{ tree}) &= (4/7, 4/7).
\end{align*}
\]

Since $9/16 = 0.56250$ and $4/7 \approx 0.57143$, it follows from this example that a $V(\mathcal{N})$ tree can indeed yield a better rate than an $F(\mathcal{N})$ tree. In Section 3.2.1 we found that the set of all rates of $F(\mathcal{N})$ trees tends to the capacity region of the channel. Now we compare this to the set of all rates of $V(\mathcal{N})$ trees.
(3.3.1.3) Definition. For \( N \in \mathbb{N} \), we define
\[
\mathcal{V}(N) := \{ \mathcal{L}(T) \mid T \text{ is a } \mathcal{V}(N) \text{ tree} \},
\]
\[
\mathcal{V} := \bigcup_{N \in \mathbb{N}} \mathcal{V}(N).
\]

The following theorem is a generalization of (3.2.1.2).

(3.3.1.4) Theorem. We have
\[
\forall N \in \mathbb{N} \left[ \text{co } \mathcal{V}(N) \subseteq \mathcal{C} \right] \text{ and } \lim_{N \to \infty} \mathcal{V}(N) = \mathcal{C}.
\]

Proof: see Section 3.5.

Theorem (3.3.1.4) is useful for finding inner bounds on \( C \) that are better than \( \mathcal{F}(N) \), since the class of \( \mathcal{V}(N) \) trees strictly includes the class of \( \mathcal{F}(N) \) trees and therefore \( \mathcal{V}(N) \) generally strictly includes \( \mathcal{F}(N) \). This follows from the examples in Section 3.6, which show that, for comparatively small \( N \), the optimum \( \mathcal{V}(N) \) rate can exceed the optimum \( \mathcal{F}(N) \) rate. On the other hand, finding an outer bound on \( C \) via outer bounds on \( \mathcal{V}(N) \) for \( N \to \infty \) is much harder. It is unknown how this should be done for \( \mathcal{F}(N) \); yet if this were possible, it would be even more difficult for \( \mathcal{V}(N) \) trees, since these have more 'degrees of freedom' than \( \mathcal{F}(N) \) trees.

3.3.2. Variable length trees ending in rootlike rectangles

In this section we consider the same restriction on trees as in Section 3.2.2, but now for \( \mathcal{V}(N) \) trees. Hence we require again that rootlike rectangles remain as connected regions after the unit square has been subdivided in a \( \mathcal{V}(N) \) tree. Note, however, that these connected regions do not have to occur in the leaves only, as remarked below Definition (3.3.1.1). An example of such a tree is the \( \mathcal{V}(2) \) tree in Figure (3.3.1.2). The following is an obvious generalization of Definition (3.2.2.2).
Chapter 3

(3.3.2.1) Definition. For \( N \in \mathbb{N} \), a \( \mathcal{V}^{\Omega}(N) \) tree is a \( \mathcal{V}(N) \) tree such that all connected regions not subdivided any further in the tree are rootlike rectangles. Furthermore

\[
\mathcal{V}^{\Omega}(N) := \{ \mathcal{A}(T) \mid T \text{ is a } \mathcal{V}^{\Omega}(N) \text{ tree} \},
\]

\[
\mathcal{V}^{\Omega} := \bigcup_{N \in \mathbb{N}} \mathcal{V}^{\Omega}(N). \]

As we will prove in Section 3.5, the regions \( \mathcal{V}^{\Omega}(N) \) also converge to the capacity region. This is stated in the following theorem.

(3.3.2.2) Theorem. We have

\[
\forall N \in \mathbb{N} \left[ \text{co } \mathcal{V}^{\Omega}(N) \subseteq C \right] \quad \text{and} \quad \lim_{N \to \infty} \mathcal{V}^{\Omega}(N) = \mathcal{V}^{\Omega} = C.
\]

Proof: see Section 3.5.

It is easy to show that every \( \mathcal{V}(N) \) tree can be changed into a \( \mathcal{V}^{\Omega}(N') \) tree for some \( N' \geq N \) by adding some extra vertices to the tree. As is explained in the following lemma, the tree can be extended in such a way that the extra vertices have a property that will be needed in Section 3.4.

(3.3.2.3) Lemma. Consider a \( \mathcal{V}(N) \) tree for some \( N \in \mathbb{N} \). This tree can be extended to a \( \mathcal{V}^{\Omega}(N') \) tree for some integer \( N' \geq N \) by adding vertices in which all remaining connected regions are subdivided into rootlike rectangles. This can be done in such a way that in each added vertex at level \( n \), user 1 can determine \( I_{0n} \) from \( (R_{1n}, R_{1n}', \theta_{1}) \) and vice versa; hence the rate of such a vertex \( A \) is

\[
\left( H(I_{0n} | \theta_{1}, R_{1n}', (\theta_{0}, \theta_{1}) \in A), H(I_{1n} | \theta_{0}, R_{0n}', (\theta_{0}, \theta_{1}) \in A). \right)
\]

Proof: Let \( A \) be a connected region in the \( \mathcal{V}(N) \) tree that is not partitioned and is not a rootlike rectangle (e.g., the L-shape in vertex \( A_{1,0} \) of Figure (3.3.1.2)). \( A \) consists of some basic rectangles \( I_{0}(\tilde{x}_{0}^{N}) \times I_{1}(\tilde{x}_{1}^{N}) \) for various \( \tilde{x}_{0}^{N} \) and \( \tilde{x}_{1}^{N} \). Assume

\[ -54 - \]
there are at least two basic intervals for user 0 that contribute to \( A \) (note that if \( A \) contains just one basic interval for each user, then \( A \) is a rootlike rectangle). Partition the union of all basic intervals for user 0 that correspond to \( A \) into two nonempty sets, say \( I_{0a} \subset [0,1) \) and \( I_{0b} \subset [0,1) \). Since user 0 can transmit information to user 1 at positive rate (by the assumption in Section 2.3.1), two different input letters for user 0, say \( z_0(a) \) and \( z_0(b) \), and an input \( z_1 \) for user 1 exist such that the input pairs \( (z_0(a), z_1) \) and \( (z_0(b), z_1) \) result in distinct outputs \( y_1 \), say \( y_1(a) \) and \( y_1(b) \) (otherwise user 1 can never distinguish between user 0's inputs). The next transmission in vertex \( A \) is the following: user 0 sends \( z_0(a) \) for \( \theta_0 \in I_{0a} \) and \( z_0(b) \) for \( \theta_0 \in I_{0b} \), user 1 sends \( z_1 \) always. After this transmission, user 1 sees different outputs for the two regions. Now user 0's basic intervals can again be partitioned into two parts for both \( I_{0a} \) and \( I_{0b} \). We repeat this procedure, transmitting the same two input pairs every time, until user 1 sees a different output sequence for each basic interval of user 0. Then the basic rectangles in \( A \) are not 1-connected anymore (Definition (2.4.3)).

After this, we do a similar thing to partition user 1's interval into basic intervals, which is possible since the rate of transmission from user 1 to user 0 is positive too. After a number of transmissions, the basic rectangles in \( A \) are not 0-connected anymore. Hence, after all of these transmissions each basic rectangle is a separate connected region. Clearly there is just one \( Y_0 \) — and one \( Y_1 \) — sequence that corresponds to such a rectangle; in other words, \( A \) has been partitioned into rootlike rectangles. Since we can do this for every region \( A \), a \( \mathcal{P}(N') \) tree can be constructed. It is obvious that all 'new' vertices in this tree have the property mentioned in the lemma.

The technique used in the proof of Lemma (3.3.2.3) will be called slicing. The transmission of symbols to tell the difference between user 0's intervals (i.e.,
Chapter 3

the rows in the region) is called row slicing; the partitioning of columns is called column slicing. We will refer to these notions in the sequel.

3.3.3. From variable length trees to fixed length codes

In this section, we present a generalization of Tolhuizen's result [TOL85]. This will show how a code can be constructed from a \( r^D(N) \) tree such that the rate of the code approximates the rate of the tree. Let \( T \) be a \( r^D(N) \) tree. As in Section (3.2.2), the rootlike rectangles that are not subdivided in \( T \) can serve as roots of new trees. In this way we can build a \( r^D(tN) \) tree out of \( t \) copies of \( T \) (note that the new tree is indeed a \( r^D(tN) \) tree: the connected regions that remain after partitioning are rootlike rectangles again. The same holds for fixed length trees, where \( t f^D(N) \) trees form an \( f^D(tN) \) tree). Using this, Tolhuizen [TOL85] proved that a \( r^D(N) \) tree for the BMC can be used to construct codes having arbitrarily small error probability, such that the code rate approximates the tree rate. Here we generalize this to arbitrary deterministic TWCs. Moreover, we sharpen Tolhuizen's error probability bound because we need this in Section 3.4.

(3.3.3.1) Theorem. Let \( N \in \mathbb{N} \) and let \( T \) be a \( r^D(N) \) tree. Then

\[ \forall \varepsilon > 0 \exists c > 0, \ 0 < \lambda < 1 \exists T_0 \in \mathbb{N} \forall t \geq T_0 \text{ a code } C_t \text{ exists with rate } I(C_t) \text{ and error probabilities } P_{e_i} \text{ satisfying } I_t(C_t) \geq I_t(T) - \varepsilon, P_{e_i} \leq c \cdot \lambda^t \text{ (} i = 0, 1 \text{).} \]

Proof: For \( t \in \mathbb{N} \), consider the \( r^D(tN) \) tree that is constructed by copying the original \( r^D(N) \) tree in every rootlike rectangle remaining in the \( r^D(N) \) tree and repeating this \( t \) times. Let \( S_t \) be the set of all rootlike rectangles \([a, b) \times [c, d)\) that remain unpartitioned in the \( r^D(tN) \) tree. Then \( S_t \) forms a partitioning of the square. Let \( \varepsilon > 0 \) and \( \delta > 0 \). Define the set of typical rectangles \( r \) as follows:

\[ T(t, \delta) := \{ r \in S_t \mid n_t(r) - tN \leq t\delta, b_t(r) - t\delta \leq t\delta, h_t(r) - t\delta \leq t\delta \}. \]
Here
\[ n_t(r) := n \text{ if } r \text{ is a rootlike rectangle at level } n \text{ in the tree}, \]
\[ b_t(r) := -\log(\text{breadth}(r)), \]
\[ h_t(r) := -\log(\text{height}(r)), \]
and \( \bar{N}, \bar{B} \text{ and } \bar{H} \) are the means of \( n_1(r'), b_1(r') \text{ and } h_1(r') \), respectively, averaged over \( r' \in S_1 \). Notice that in [TOL85], the typical rectangles are defined with \(|\ldots| \leq t^{3/4}\) instead of \( t\delta \). With our definition, we can use the exponential convergence in the weak law of large numbers as it is stated in [ASH65, Lemma 3.6.3, Theorem 3.6.4 and remark in Section 3.8]:

'For \( t \) independently identically distributed random variables \( X_1, X_2, \ldots, X_t \),
\[ \Pr\{ \sum_{i=1}^t X_i - t \bar{X}_1 \geq t\delta \} \leq c \cdot \lambda^t \] for some \( c > 0 \) and some \( 0 < \lambda < 1 \) independent of \( t \).'

Therefore the total area of all \( r \in T(t, \delta) \) tends to 1 exponentially as \( t \to \infty \), since
\[ \Pr\{ |n_t(r) - t\bar{N}| > t\delta \text{ or } |b_t(r) - t\bar{B}| > t\delta \text{ or } |h_t(r) - t\bar{H}| > t\delta \}
\[ \leq \Pr\{ |n_t(r) - t\bar{N}| > t\delta \} + \Pr\{ |b_t(r) - t\bar{B}| > t\delta \} + \Pr\{ |h_t(r) - t\bar{H}| > t\delta \}. \]

For \( t \in \mathbb{N} \), we now construct a code \( C_t \). Let \( M_{0t} := \lfloor 2^t(\bar{N}+2\delta) \rfloor, M_{1t} := \lfloor 2^t(\bar{B}+2\delta) \rfloor \). Let user 0 have \( M_{0t} \) messages and let user 1 have \( M_{1t} \) messages. We regard the message pairs as equally spaced points in a lattice in the unit square. The probability that a lattice point lies in one of the typical rectangles is equal to
\[ \sum_{r \in T(t, \delta)} \frac{\#\text{lattice points in } r}{M_{0t} \cdot M_{1t}} \]
\[ \geq \sum_{r \in T(t, \delta)} \frac{(\text{height}(r) \cdot M_{0t}^{-1})(\text{breadth}(r) \cdot M_{1t}^{-1})}{M_{0t} \cdot M_{1t}}. \]

- 57 -
\[ \sum_{r \in T(t, \delta)} \text{area}(r) \cdot \left\{ 1 - \frac{1}{\text{height}(r) \cdot \mu_{0t}} - \frac{1}{\text{breadth}(r) \cdot \mu_{1t}} \right\} \geq \sum_{r \in T(t, \delta)} \text{area}(r) \cdot \left\{ 1 - 2^{-t\delta+1} - 2^{-t\delta+1} \right\} \]

for large enough \( t \). Since the total area of all \( r \in T(t, \delta) \) is at least \( 1 - (c') \cdot (\lambda')^t \) for some \( c' \) and \( \lambda' \), the probability that a message point does not lie in a typical rectangle is bounded by \( c \cdot \lambda^t \) for some \( c > 0 \) and \( 0 < \lambda < 1 \) independent of \( t \).

The code \( \mathcal{C}_t \) is defined as follows. Each message point corresponds to a row and column in the square and hence, via the \( V(tN) \) tree, to a pair of strategies for the two users. Each user applies the strategy corresponding to his message, but he transmits at most \( a_t \) symbols, where \( a_t := \lfloor t(N+\delta) \rfloor \). After the \( n \)th transmission \( (n = 1, 2, \ldots, a_t) \) each user determines the connected region at level \( n \) in which the message point must lie. If the path from the root to the leaf in which the message point lies contains less than \( a_t \) vertices, then the users continue with sending dummy letters.

The message point lies in exactly one of the rootlike rectangles \( r \in \mathcal{S}_t \). If this rectangle \( r \) is typical, then after the \( a_t \) transmissions the users know that the point lies in \( r \), since \( n_t(r) \leq a_t \). Now \( r \) contains at most \( 2^{-t(\overline{N}-\delta)} \mu_{0t} \leq 2^{3t\delta} \) horizontal lattice lines since \( h_t(r) \geq t(\overline{N}-\delta) \). Therefore user 0 can specify his message in \( 3t\delta + 1 \) transmissions by row slicing (cf. Lemma (3.3.2.3)) and so can user 1 by column slicing. Hence it takes \( \ell_t \) transmissions to determine the message pair, with \( \ell_t := a_t + 2[3t\delta] + 2 \). If less transmissions are needed, dummy letters are added until both users have sent \( \ell_t \) input letters. If \( r \) is not typical, dummy letters are sent until we have \( \ell_t \) inputs.

The code \( \mathcal{C}_t \) has block length \( \ell_t \) and its error probability tends to zero.
exponentially as $t \to \infty$. Its rate is

$$\left( \frac{\log(M_{0,t})}{\ell_t}, \frac{\log(M_{1,t})}{\ell_t} \right) \to \left( \frac{\overline{H} + 2\delta}{\overline{N} + 7\delta}, \frac{\overline{B} + 2\delta}{\overline{N} + 7\delta} \right) \text{ if } t \to \infty.$$ 

This rate tends to $(\overline{B}/\overline{N}, \overline{B}/\overline{N})$ if we let $\delta \downarrow 0$. The only thing left to show is

$$\overline{B}/\overline{N} = I_0(T) \quad \text{and} \quad \overline{B}/\overline{N} = I_1(T).$$

We show this for the $I_0$ part only, since the $I_1$ part is proved analogously. We have

$$\overline{B} = \sum_{r \in S_1} \text{area}(r) \cdot (-\log(\text{height}(r)))$$

$$= \sum_{r = r_0 \times r_1} Pr\{\theta_0 \in r_0\} \cdot Pr\{\theta_1 \in r_1\} \cdot (-\log(Pr\{\theta_0 \in r_0 | \theta_1 \in r_1\})), $$

where $r = r_0 \times r_1$ denotes the projection of the rectangle in the two directions: $r_0$ is user 0's subinterval of $[0,1)$ corresponding to $r$ and $r_1$ is user 1's subinterval corresponding to $r$. We will write $\tilde{y}_1(r)$ for the $y_1$ sequence of length $n_1(r)$ corresponding to $r (= r_0 \times r_1)$ in the tree $T$. Now $\overline{B}$ can be written as

$$\sum_{r_1} Pr\{\theta_1 \in r_1\} \cdot$$

$$\sum_{r_0} Pr\{\tilde{y}_1 = \tilde{y}_1(r) | \theta_1 \in r_1\} \cdot (-\log(Pr\{\tilde{y}_1 = \tilde{y}_1(r) | \theta_1 \in r_1\}))$$

$$= \sum_{r_1} Pr\{\theta_1 \in r_1\} \cdot H(\tilde{y}_1 | \theta_1)$$

$$= \sum_n H(Y_{1n} | \theta_1, I_1^T).$$

It should be noted that not all $Y_{1n}$ exist, in general, because of the variable length of the tree $T$. We solve this problem by adding a suitable number of $*$'s to the end of a $Y_0$- and $Y_1$ sequence such that all sequences obtain length $\overline{N}$. The $*$'s
do not change the entropy (they give contribution 0), since the pair \((\theta_1, I^n_1)\) (and also \((\theta_0, I^n_0)\)) determines whether the *'s must be added. Let \(i\) range over all vertices \(A_{n,i}\) at level \(n\) in the tree. As in the proof of Theorem (3.1.4), user 1 can determine the vertex \(A_{n,i}\) given \(\theta_1\) and \(I^n_1\). Hence \(H(\hat{Y}_1|\theta_1)\) may be expressed as

\[
\sum_n \sum_i \Pr\{(\theta_0, \theta_1) \in A_{n,i}\} \cdot H(Y_{1n}|\theta_1, I^n_1, (\theta_0, \theta_1) \in A_{n,i}) = \sum_n \sum_i w(A_{n,i}) \cdot r_0(A_{n,i}).
\]

Furthermore we have

\[
\bar{R} = \sum_r \frac{\Phi}{\text{area}(r)}
\]

\[
= \sum_r \left( \sum_n \sum_i \phi(A_{n,i} \text{ contains } r) \right) \cdot \frac{\text{area}(r)}
\]

\[
= \sum_n \sum_i \sum_r \phi(A_{n,i} \text{ contains } r) \cdot \text{area}(r)
\]

\[
= \sum_n \sum_i w(A_{n,i}).
\]

Hence \(\bar{R}/\bar{N} = K_0(\mathcal{R})\).

\[\Box\]

3.3.4. From variable length trees to variable length codes and vice versa

In Section 3.2.3, we constructed a zero–error code from an \(\mathcal{P}(N)\) tree. In Section 3.3.3, we constructed a (fixed length) code with vanishing error probability from an \(\mathcal{V}(N)\) tree. Here we will construct a 'variable length code' (which is not a code in the sense of Definition (2.1.6)!) with error probability 0, if the thresholds in a \(\mathcal{V}(N)\) tree are on an \((M_0+1) \times (M_1+1)\) grid and the unit square is partitioned into \(M_0 \cdot M_1\) basic rectangles. As in Theorem (3.2.3.3), we will show that the tree rate is equal to the code rate for these codes, if the code rate is defined appropriately.

Consider a \(\mathcal{V}(N)\) tree (in fact, a \(\mathcal{V}(N)\) tree) with thresholds on a grid such that the \(M_0 \cdot M_1\) basic rectangles remain as connected regions after the partitioning.
An example for the BMC is shown below (compare this to Figure (3.2.3.1)).

(3.3.4.1) Figure. \( Y(3) \) tree for the BMC representing a code.

We can use this tree to construct a code in the following way. Let user \( i \) have \( M_i \) possible messages, \( i \in \{0,1\} \). Each of the \( M_0 \) basic intervals for user 0 (each row) corresponds to a message of user 0 and each column corresponds to a message of user 1. Suppose the users want to transmit message pair \( (w_0, w_1) \) to each other. The first input symbol that they have to use in the code can be found from the root of the tree: if the row corresponding to message \( w_0 \) has \( I_{00} = x \) in the tree, then the first symbol of user 0's codeword will be \( f_{00}(w_0) = x \). In the same way user 1 can determine his first input, \( f_{10}(w_1) \).

After this transmission they both know in which of the connected regions at level 1 of the tree the pair \( (w_0, w_1) \) lies. If this connected region, say \( A \), consists of just one basic rectangle, then both users can now determine the other user's message. Hence they can stop, or proceed with a new message pair. If \( A \) contains more than one basic rectangle in some row or column, the users choose a second input symbol. They look at the vertex representing \( A \) to find out which input \( I_{01} = f_{01}(w_0, r_{00}) \) must be sent for row \( w_0 \) and which \( I_{11} = f_{11}(w_1, r_{10}) \).
Chapter 3

is needed in column $w_1$.

In this way the users go on until the connected region has shrunk to one basic rectangle. As soon as they have reached this, they stop (notice that both users determine to stop at the same time!). At this point, both users know the message pair corresponding to the basic rectangle, which can only be the transmitted pair $(w_0, w_1)$. Therefore the transmission of messages is error free.

We call this system a **variable length code** (with error probability equal to zero; we will not consider variable length codes with positive error probability). Obviously it is possible to define encoding and decoding functions (although not in the sense of Definition (2.1.6)) for it. We shall not do this here; a more formal definition of variable length codes can be found in [TIE89].

As we know, a fixed length code (cf. (2.1.6)) has three parameters: $n_0, n_1$ and $N$. The parameters $n_0$ and $n_1$ apply to a variable length code too, but a block length cannot be defined for such a code. Instead, we have $n_0, n_1$ possibly different codeword lengths: one for each message pair. Therefore we define the following.

(3.3.4.2) **Definition.** Consider a variable length code constructed from a $I^2(N)$ tree with grid size $(n_0+1) \times (n_1+1)$. For each message pair $(w_0, w_1)$, we define $N(w_0, w_1)$ as the length $n$ of the output sequence $L_0$ (or $L_1$, as they are equally long) if the transmitted pair is $(w_0, w_1)$. Define the **average codeword length** $\bar{N}$ by

$$\bar{N} := \frac{\sum (w_0, w_1) N(w_0, w_1)}{n_0 \cdot n_1}.$$
(3.3.4.3) Definition. For a variable length code with parameters $n_0$, $n_1$ and $N(w_0,w_1)$ ($0 \leq w_0 \leq n_0-1$, $0 \leq w_1 \leq n_1-1$) we define the rate pair of the code, $\mathcal{R}$, as
\[ R_i := \log(n_i), \quad i \in \{0,1\}. \]

The following theorem generalizes Theorem (3.2.3.3), where we proved that the rate of a fixed length code is equal to the rate of the corresponding tree.

(3.3.4.4) Theorem. Consider a variable length code with error probability $0$ that is constructed from a $\mathcal{F}^2(N)$ tree $T$. Then the rate of this code, as defined in Definition (3.3.4.3), is equal to the rate of the $\mathcal{F}^2(N)$ tree, $R(T)$.

Proof. In the proof of Theorem (3.3.3.1), we showed that the rate of the $\mathcal{F}^2(N)$ tree equals $(\bar{H}/\overline{N}, \bar{B}/\overline{N})$ with $\bar{H} := -\log(\text{height}(r))$ averaged over all rootlike rectangles $r$ remaining after partitioning, $\bar{B} := -\log(\text{breadth}(r))$ averaged over $r$, and $\overline{N} :=$ the average block length as defined in (3.3.4.2). Since all basic rectangles have equal size, $\text{height}(r) = 1/n_0$ for all basic rectangles $r$, so $\bar{H} = \log(n_0)$. Similarly $\bar{B} = \log(n_1)$, proving the theorem after division by $\overline{N}$.

In Section (3.2.3), we defined an $\mathcal{F}^0(N)$ tree as the kind of tree in which a fixed length code with error probability $0$ could be represented. In Definition (3.3.4.5) below we define something similar for variable length codes. For fixed length trees, we could not prove that $\mathcal{F}^0(N)$ converges to the capacity region. For variable length trees, however, we can show that the regions $\mathcal{V}^0(N)$ tend to $C$.

(3.3.4.5) Definition. Let $N \in \mathbb{N}$. A $\mathcal{F}^0(N)$ tree (or strategy) is a $\mathcal{F}^2(N)$ tree (or strategy) on a grid in which a 0–error variable length code is represented such that the largest codeword length occurring in the code is $N$. Also
Chapter 3

\[ V^0(N) := \{ T \mid T \text{ is a } V^0(N) \text{ tree} \}, \]
\[ V^0 := \bigcup_{N \in \mathbb{N}} V^0(N). \]

(3.3.4.6) Theorem. We have

\[ \forall N \in \mathbb{N} \left[ \text{co } V^0(N) \subseteq C \right] \text{ and } \lim_{N \to \infty} V^0(N) = \mathbb{R}. \]

Proof: see Section 3.5.

Because of Theorem (3.3.4.6) it is interesting to try to develop variable length codes. Not only do these provide an easy way to use the channel for actual communication — and even error free — but we also know that variable length codes achieve capacity: if the average block length is large enough, variable length codes exist with rates that are close to the maximum possible rate for the TWC.

Variable length codes have already been mentioned in [SHA61]: the Hagelbarger code is the least complex variable length code for the BMC. It is in fact the code described by the \( \mathcal{V}^0(2) \) tree in Figure (3.3.1.2). Each user has two messages and the average block length is 7/4. More complex examples of variable length codes for the BMC are shown in Section 3.6.

3.4. Bootstrap trees

3.4.1. Definition and statement of result

In Section 3.3 we have considered a possible improvement over fixed length trees. We managed to achieve higher rates, in general, by deleting some of the low-rate vertices in an \( F(N) \) tree. (We stress the fact that this improvement only holds for finite \( N \), since we showed that the limiting region for \( N \to \infty \) is the same

\[ -64 - \]
Strategy Trees for TWCs

for both fixed — and variable length trees.) However, with $V(N)$ trees we are limited in the choice of the vertices to be deleted from the $F(N)$ tree: if we want to delete a low-rate vertex somewhere halfway the tree, we have to delete the complete subtree below it (which might contain vertices with high rates) as well!

In this section we provide a way to get around this problem. Using a technique introduced by Schalkwijk [SCH83a] for the BMC, it is sometimes possible to delete single vertices from a tree without deleting the subtree. We will prove that the average rate of the remaining set of vertices (which is not a tree in the strict sense anymore) is an achievable rate for the TWC again. Schalkwijk called this technique 'bootstrapping', since it is based on the idea of 'pulling oneself up by one's own bootstraps': a given tree with rate $A(0)$ is used to develop a coding scheme having a higher rate, $A(1)$, which in turn is used to construct a code with even higher rate, $A(2)$, et cetera, until we reach the rate of the tree without the deleted vertex. 2

Clearly we cannot delete an arbitrary vertex from a tree and still keep an achievable rate. Definition (3.4.1.1) states necessary requirements for a vertex such that it has the above property.

(3.4.1.1) Definition. Consider a $V(N)$ tree $T$ for some $N \in \mathbb{N}$. The set of possible bootstrap vertices (PBV) for $T$ is the set of vertices in the tree for which (3.4.1.2), the so-called PBV property, holds. Here $A$ denotes a vertex at level $n$.

(3.4.1.2) $r(A) = (R(I_{0n}^{1}, I_{1}^{1}, (\theta_{0}, \theta_{1}) \in A), R(I_{1n}^{1}, (\theta_{0}, (\theta_{0}, \theta_{1}) \in A).$ □

2 The term 'bootstrapping' is not uncommon in science: the Oxford English Dictionary [BUR72] quotes several technical papers (the earliest one from 1946), in which this word is used with a similar meaning.
Chapter 3

Note that the slicing vertices occurring in Lemma (3.3.2.3) have the PBV property. The PBV property means that the transmission in a vertex $A$ satisfying (3.4.1.2) is such that the a priori uncertainty about output $Y_{i,n}$ for user $i$, knowing that we are in vertex $A$, is equal to the uncertainty about the other user's input. Suppose that we use a code based on the tree, as in Theorem (3.3.3.1). In Section 3.4.2 we will show that the information transmitted in vertex $A$ does not have to be transmitted by sending the inputs as described by $A$; the users can directly transmit the information about their inputs using another code. If this 'other' code has a rate higher than $r(A)$, then the rate of the complete coding scheme will be higher than the rate of the tree.

The new code can be used to repeat the procedure. Now the information about the inputs in vertex $A$ can be transmitted using the new code, which again increases the total rate. This is where idea of 'bootstrapping' is used. If we repeat the procedure infinitely many times, it will turn out that the rate of $A$, $r(A)$, does not occur in the formula for the code rate anymore: $A$ has become 'invisible'. Note that this can be done only for vertices with the PBV property; all other vertices necessarily remain 'visible' in the rate formula. This explains the following definition.

(3.4.1.3) Definition. Consider a $V(K)$ tree $T$ and its PBV set. A type assignment for $T$ is defined as follows. To each vertex in $T$, we assign a type, 'visible' or 'invisible'. For the root and for (other) vertices not in the PBV set, the type must be 'visible'. For vertices in the PBV set (except for the root) we may choose the type at will. The visible distance between visible vertices is defined analogously to the ordinary distance (cf. Section 3.2.1), but now we only count visible vertices on the path between the vertices. The visible depth of $T$ is defined analogously.

- 66 -
(3.4.1.4) Definition. Let \( N \in \mathbb{N} \). A \( B(N) \) tree (bootstrap tree) is defined as a \( Y(N_0) \) tree for some \( N_0 \geq N \), with a type assignment such that the visible depth is \( N-1 \).

An example of this is given in Figure (3.4.1.5).

(3.4.1.5) Figure. \( F(5) \), \( V(5) \) and \( B(4) \) tree.

At the left, an \( F(5) \) tree is shown in schematic form. In the middle, the tree has been pruned to a \( V(5) \) tree. The three vertices in this tree labeled 'PBV' form the PBV set. The \( B(4) \) tree on the right is constructed from the \( V(5) \) tree by considering two of the PBV vertices invisible ('inv', the open circles).

The next definition describes how the rate of a \( B(N) \) tree should be computed. As said before, invisible vertices do not contribute to the rate.

(3.4.1.6) Definition. Let \( T \) be a \( B(N) \) tree constructed from a \( Y(N_0) \) tree with vertex set \( V \). Partition \( V \) into \( V_{vis} \) and \( V_{inv} \) the sets of visible and invisible vertices, respectively. The rate of the \( B(N) \) tree, denoted as \( \lambda_{vis}(T) \), is defined as

\[
\lambda_{vis}(T) := \frac{\sum_{A \in V_{vis}} w(A) \cdot \tau(A)}{\sum_{A \in V_{vis}} w(A)}.
\]
The definition and theorem below are generalizations of the ones in Section 3.3. They state that the rate of a bootstrap tree as defined above is indeed achievable and tends to capacity if the visible depth is large enough.

(3.4.1.7) Definition. We define, for $N \in \mathbb{N}$:

$B(N) := \{ L_{\text{vis}}(T) | T \text{ is a } B(N) \text{ tree } \}$

$B := \bigcup_{N \in \mathbb{N}} B(N)$. □

(3.4.1.8) Theorem. We have

$\forall N \in \mathbb{N} \ [ \text{co} B(N) \subset C ]$ and $\lim_{N \to \infty} B(N) = \bar{B} = C$. □

Proof: Part of this proof follows the proofs for fixed or variable length strategies, especially where the limit is concerned. For this part we refer to Section 3.5. The fact that every point in $B(N)$ is achievable, however, is proved in an entirely different way. Since this proof is quite involved, we devote Section 3.4.2 to it. □

Theorem (3.4.1.8) offers a way to find significantly better inner bounds on the capacity region of certain TWCs. The most famous example of this technique is Schalkwijk's bootstrapping strategy for the BMC. In Section 3.6, this strategy is shown, along with some more bootstrap trees for other TWCs.

3.4.2. Proof of the achievability of bootstrap rates

Here we will prove the achievability of every rate point corresponding to a bootstrap tree as defined in the previous section; hence we will show $B(N) \subset C$ for all $N \in \mathbb{N}$. For the case of the BMC with Schalkwijk's bootstrap tree [SCH83a], the achievability was proved by the author in [OVE88a]. This proof was based on a term paper by Hazewindus [HAZ85], which contained the basic idea for the proof.
(although the paper itself was very concise and unfortunately incorrect). Here we basically use the same argument as in [OVE88a], but in a slightly more general form since we are discussing arbitrary deterministic TWCs now.

Consider a $V(N_0)$ tree with a type assignment and the corresponding $B(N)$ tree, $N \leq N_0$. We use Lemma (3.3.2.3) to change the $V(N_0)$ tree into a $V^D(N'_0)$ tree for some $N'_0 \geq N_0$. The slicing vertices that had to be added in this procedure are given type 'invisible'; as shown in the lemma, these vertices satisfy (3.4.1.2).

Because of this, the bootstrap tree corresponding to the $V^D(N'_0)$ tree has the same set of visible vertices (and hence, the same rate) as the $B(N)$ tree following from the $V(N_0)$ tree. Let the $V^D(N'_0)$ tree be called $T$. Its rate is $R(T) = (K_0(T), K_1(T))$.

We assume that both components of $R(T)$ are positive. The case where one of the two components is zero is trivial and follows by continuity. We will show that $R(T)$ is the first of a sequence of achievable rates, $R(n)$ for $n = 0, 1, 2, \ldots$ with $R(0) = R(T)$. The limit of this sequence will be the rate of the $B(N)$ tree, $\mathcal{R}_{\text{vis}}(T)$:

$$\lim_{n \to \infty} R(n) = R_{\text{vis}}(T) = (K_{\text{vis},0}(T), K_{\text{vis},1}(T))$$

as computed by Definition (3.4.1.6). We also assume $K_{\text{vis},i}(T) > 0$ for $i = 0, 1$.

In this section we prove that for each $n$, a sequence of block codes exists such that the rate approximates $R(n)$ and both error probabilities decrease exponentially as the block length increases. As in [OVE88a], the main ingredients of the proof are Theorem (3.3.3.1) and the correlated source coding result by Slepian and Wolf [SLE73]. The Slepian–Wolf result is stated in Lemma (3.4.2.1) below, in the form in which we are going to use it.

(3.4.2.1) Lemma. For each vertex $A_n, i$ at some level $n$ in the tree $T$, we have the following. Let $\varepsilon > 0$. Real numbers $c > 0$ and $0 < \lambda < 1$ exist such that, for large enough $K \in \mathbb{N}$, an encoder–decoder pair exists for which the following holds.
Chapter 3

I symbols $I_{0n}$ that correspond to I independent transmissions in vertex $\mathcal{A}_{n,i}$ can be encoded by user 0 into

$$\left( H(I_{0n} | \theta_1, I_{1n}, (\theta_0, \theta_1) \in \mathcal{A}_{n,i}^I + \varepsilon_{\mathcal{Z}}) \cdot I \right)$$

binary symbols such that, if user 1 decodes these using $\theta_1$ and $I_{1n}^n$, the probability of a decoding error is at most $c \cdot I$. Similarly user 1 can encode $I I_{1n}$-symbols in

$$\left( H(I_{1n} | \theta_0, I_{1n}, (\theta_0, \theta_1) \in \mathcal{A}_{n,i} + \varepsilon_{\mathcal{Z}}) \cdot I \right)$$

binary symbols with a decoding error probability for user 0 of at most $c \cdot I$.

Proof: This follows from the theorem in [SLE73]. In fact we do not consider the classical case of two correlated information streams that have to be encoded by separate encoders; we only look at the case where one information stream, consisting of i.i.d. symbols $I_{0n}$, is encoded and where the decoder has side information, namely the i.i.d. sequences $I_{1n}$ and $\theta_1$. This is indeed a special case of the aforementioned theorem; however, we must make two remarks about this.

Firstly, in the proof in [SLE73] it is needed that the decoder's side information, say $\mathcal{U}$, is described with symbols in a finite alphabet $\mathcal{U}$. Here we do not have this: $\theta_1$ is a real number. However, in Section 2.3.2 we defined $H(I_{1n}^n | \theta_1)$ in terms of the basic intervals $I_k$ of user 1. Therefore the index $k$ of the interval $I_k$ containing $\theta_1$ bears all information: the position of $\theta_1$ within $I_k$ adds no further knowledge about $I_{0n}$ or $I_{1n}$. So, if $I(\theta_1)$ is the index of the basic interval in which $\theta_1$ lies, we could have stated the lemma with $H(I_{0n} | I(\theta_1), I_{1n}^n, (\theta_0, \theta_1) \in \mathcal{A}_{n,i})$ instead of with $H(I_{0n} | \theta_1, I_{1n}^n, (\theta_0, \theta_1) \in \mathcal{A}_{n,i})$: these represent the same entropy.

Secondly it should be noted that the theorem in [SLE73] is stated with a bound on the error probability that does not depend on the block length $I$. However, Koševlev [KOŠ77] proved that the theorem also holds with an exponential error bound (also see [CSI81], problem 3.1.5).

For the $I^D(N_0^I)$ tree $T$, we define the set of visible and invisible vertices as
Strategy Trees for TWCs

$\mathcal{V}_{\text{vis}}$ and $\mathcal{V}_{\text{inv}}$, respectively. Let the total weight of all vertices in these sets be $\mathcal{V}_{\text{vis}}$ and $\mathcal{V}_{\text{inv}}$, respectively. If we define $\bar{V}, \bar{H}$ and $\bar{B}$ for the $V^J(N)^0_0$ tree $T$ as in Theorem (3.3.3.1), we find $\bar{V} = \mathcal{V}_{\text{vis}} + \mathcal{V}_{\text{inv}}$. We abbreviate $E_{\text{vis}}(T)$ as $E_{\text{vis}}$; similarly we define $E_{\text{inv}}$ as the average rate of the invisible vertices. Thus

\begin{equation}
E_{\text{vis}} = (E_{\text{vis},0}, E_{\text{vis},1}) = \frac{\sum_{A \in \mathcal{V}_{\text{vis}}} w(A) \cdot r(A)}{\mathcal{V}_{\text{vis}}},
\end{equation}

\begin{equation}
E_{\text{inv}} = (E_{\text{inv},0}, E_{\text{inv},1}) = \frac{\sum_{A \in \mathcal{V}_{\text{inv}}} w(A) \cdot r(A)}{\mathcal{V}_{\text{inv}}},
\end{equation}

\begin{equation}
E(T) = (E_0(T), E_1(T)) = \frac{(E_{\text{inv}} E_{\text{inv}} + E_{\text{vis}} E_{\text{vis}})}{(E_{\text{inv}} + E_{\text{vis}})} = (\bar{V}/\bar{H}, \bar{B}/\bar{H}).
\end{equation}

Now we construct a Markov chain from the tree $T$ (cf. [SCH82], [SCH83a]). Each state in the chain will correspond to a vertex in the tree. Call the vertices $A_{n,i}$ and let the states of the Markov chain have the same names. The transition probability of going from a state $A_{n,i}$ to $A_{m,j}$ is given by the following three rules.

(i) If $m = n+1$ and $A_{m,j}$ is a successor of $A_{n,i}$ in the tree, then

\[
Pr\{\text{next state} = A_{m,j} \mid \text{previous state} = A_{n,i}\} := \frac{w(A_{m,j})}{w(A_{n,i})}.
\]

(ii) If $A_{m,j}$ is the root ($m = 0$) and in the partitioning of $A_{n,i}$ at least one rootlike rectangle remains that is not partitioned further in $T$, then

\[
Pr\{\text{next state} = A_{m,j} \mid \text{previous state} = A_{n,i}\} := \frac{w(r)}{w(A_{n,i})},
\]

where $w(r)$ is the weight of all rootlike rectangles remaining in $A_{n,i}$;

(iii) In any other case:

\[
Pr\{\text{next state} = A_{m,j} \mid \text{previous state} = A_{n,i}\} := 0.
\]

As a consequence of the above rules, transitions are possible only from a vertex $A_{n,i}$ to a direct successor $A_{n+1,j}$ or from a vertex $A_{n,i}$ to the root $A_{0,0}$; the
latter transition is possible only in the case that a rootlike rectangle remains in $A_{n,\tau}$. Figure (3.4.2.3) illustrates this. It shows the $\mathcal{P}(3)$ tree for Schalkwijk's bootstrap strategy, plus the Markov chain that is derived from it. In this figure, $a$ is the area of the subrectangle in $A_{0,0}$ and $b$ is the area of the two rectangles in $A_{1,0}$ that correspond to $Y = 0$. The transition probabilities are written next to the arrows in the Markov chain.

(3.4.2.3) Figure. $\mathcal{P}(3)$ tree and the corresponding Markov chain.

An infinite walk through the Markov chain corresponding to a tree $T$ can be seen as a partitioning of the square derived from infinitely many copies of $T$. Compare this to the proof of Theorem (3.3.3.1), where we took $t$ copies of a $\mathcal{P}(N)$ tree. Whenever we reach a rootlike rectangle that is not partitioned in the original tree $T$, we return to the root of $T$ and partition this rectangle according to the tree.

It is not difficult to see that the Markov chain is irreducible (cf. [FEL70, Ch. XV, Section 4]), since every state can be reached from every other state: to
wit, the root can be reached from every state because each partitioning necessarily ends in rootlike rectangles, and from the root we can reach all other states because of the tree structure. We also assume that the chain is aperiodic. This is not a severe restriction, since we can always change a periodic chain into an aperiodic one without changing the corresponding bootstrap tree. Indeed, if the chain is periodic, then we add a vertex below one of the leaves of the \( V(H_0^j) \) tree in which we use slicing to separate the remaining rootlike rectangle into two halves. In one of these halves, we return directly to the root and to the other half we append another slicing vertex before returning to the root. Now the chain is aperiodic and still irreducible. The slicing vertices are given type 'invisible' (which is possible, see before), so \( \xi_{\text{vis}}(T) \) is not affected by this.

For a state \( A \), define \( q_A \) by

\[
q_A = \frac{w(A)}{\sum_{A_i \in \mathcal{A}} w(A_i)} = \frac{w(A)}{\bar{N}}.
\]

It is left to the reader to check that the \( q_A \)'s satisfy

\[
\forall m, j \ [ q_{A_{m,j}} = \sum_{A_n, i} Pr\{ \text{next state} = A_{m,j} | \text{previous state} = A_{n,i} \} \cdot q_{A_{n,i}} ].
\]

Hence by [FEL70, Ch. XV, Section 7], the \( q_A \)'s form the stationary distribution of the Markov chain. So, if \( A(d) \) is the random variable denoting the state that is reached after \( d \) transitions in the chain, starting from the root, then

\[
\forall A \in \mathcal{A} \ [ \lim_{d \to \infty} Pr\{ A(d) = A \} = q_A ].
\]

Let \( q_{\text{vis}} \) be the probability of being in a visible vertex and define \( q_{\text{inv}} \) likewise:

\[
q_{\text{inv}} = \frac{q_{\text{vis}}}{\bar{N}}, \quad q_{\text{vis}} = 1 - q_{\text{inv}} = \frac{\bar{N} - q_{\text{inv}}}{\bar{N}}.
\]

Assume \( q_{\text{inv}} > 0 \); otherwise \( \xi_{\text{vis}}(T) \) equals \( \xi(T) \), which is achievable by Theo-
rem (3.3.1.4). There are three possibilities, given by (3.4.2.5.a through c).

(3.4.2.5.a) \( L_1(T) \cdot L_{\text{inv},0} > L_0(T) \cdot L_{\text{inv},1} \)

(3.4.2.5.b) \( L_1(T) \cdot L_{\text{inv},0} < L_0(T) \cdot L_{\text{inv},1} \)

(3.4.2.5.c) \( L_1(T) \cdot L_{\text{inv},0} = L_0(T) \cdot L_{\text{inv},1} \)

In the rest of this proof we assume that (3.4.2.5.a) holds. Case (3.4.2.5.b) can be treated by interchanging 0's and 1's everywhere. The third case asks for some minor changes. We will explicitly point out the differences with (3.4.2.5.a).

Now we define the sequence of rates \( \xi(n) \). Two extra variables are needed:
a term \( \xi^*(n) \) to ensure that the direction of \( \xi(n) \) tends to the direction of \( \xi_{\text{vis}} \)(this can be compared to the dissecting state \( d \) in [SCH83b]), and a factor \( \eta(n) \) which affects the Euclidean norm of \( \xi(n) \) such that \( \|\xi(n)\| \to \|\xi_{\text{vis}}\| \) for \( n \to \infty \).

(3.4.2.6) Definition. We define \( \xi^*_1(n), \eta(n) \) and \( \xi(n) = (\xi_0(n), \xi_1(n)) \) recursively:

a) \( \xi^*_1(0) := 0, \quad \eta_0 := 1, \quad \xi(0) := \xi(T) \) and for \( n > 0 \):

b) \( \xi^*_1(n) := \frac{L_1(n-1)}{L_0(n-1)} \cdot L_{\text{inv},0} - L_{\text{inv},1} \)

c) \( \eta(n) := \xi_{\text{inv},0}/\xi_0(n-1) \)

d0) \( \xi_0(n) := \left(V_{\text{inv}}^0 L_{\text{inv},0} + V_{\text{vis}}^0 L_{\text{vis},0}\right)/(V_{\text{inv}}^\eta(n) + V_{\text{vis}}) \)

d1) \( \xi_1(n) := \left(V_{\text{inv}}^1 L_{\text{inv},1} + \xi^*_1(n) + V_{\text{vis}} L_{\text{vis},1}\right)/(V_{\text{inv}}^\eta(n) + V_{\text{vis}}) \).

A first observation about the term \( \xi^*_1(n) \) is made below.

(3.4.2.7) Lemma. \( \forall n > 0 \quad [\xi^*_1(n) > 0] \).

(Note: if (3.4.2.5.b) holds, then \( \xi^*_1(n) > 0 \); if c holds, then \( \xi^*_1(n) = 0 \))

Proof: By induction: \( \xi^*_1(1) > 0 \) by (3.4.2.5.a). If \( \xi^*_1(n) > 0 \), then by (3.4.2.6.d):

\[ -74 - \]
\[
\frac{\mathcal{L}_1(n)}{\mathcal{L}_0(n)} = \frac{\mathcal{L}_1(0) + q_{\text{inv}} \mathcal{L}_1^*(n)}{\mathcal{L}_0(0)} > \frac{\mathcal{L}_1(0)}{\mathcal{L}_0(0)}.
\]

So, by (3.4.2.6.b), \( \mathcal{L}_1^*(n+1) > \mathcal{L}_1^*(1) > 0 \) for all \( n > 0. \)

Furthermore we derive the following relations that will be needed in the sequel.

By (3.4.2.2), (3.4.2.6) and the definitions of \( q_{\text{inv}} \) and \( q_{\text{vis}} \) we obtain

\[
(3.4.2.8) \quad \mathcal{L}_0(n+1) = \frac{\bar{H}}{\bar{H}(q_{\text{vis}} + q_{\text{inv}})} , \quad \mathcal{L}_1(n+1) = \frac{\bar{H} + \bar{H} q_{\text{inv}} \mathcal{L}_1^*(n+1)}{\bar{H}(q_{\text{vis}} + q_{\text{inv}}^* \mathcal{L}_1^* n+1)}.
\]

Also, c) and d) of (3.4.2.6) yield

\[
(3.4.2.9) \quad \mathcal{L}_0(n) = \frac{\mathcal{L}_0(0)}{q_{\text{vis}} + q_{\text{inv}}^* \mathcal{L}_1^* n+1} \quad \text{and} \quad \frac{\mathcal{L}_0(n)}{\mathcal{L}_0(n-1)} = \frac{\mathcal{L}_1^* \mathcal{L}_0^* + q_{\text{vis}} \mathcal{L}_0^*}{\mathcal{L}_1^* \mathcal{L}_0^* + q_{\text{vis}} \mathcal{L}_0^*}.
\]

Let \( n \in \mathbb{N} \). We will construct a sequence of codes \( \mathcal{C}_k(n) \) such that rate \( \mathcal{L}(n) \) is achievable with \( \mathcal{C}_k(n) \) if \( k \to \omega \). In the following, the expression ' \( \{a, b\} \) bit is transmitted ' is an abbreviation for: 'simultaneously, an amount of information of \( a \) bit is transmitted in the \( 0 \to 1 \) direction and \( b \) bit is transmitted in the \( 1 \to 0 \) direction '. Consider assertion \( \mathcal{A}_n \), stating that \( \mathcal{L}(n) \) is achievable.

\( \mathcal{A}_n : = \forall \varepsilon_n > 0 \exists c_n > 0 \exists \lambda_n < 1 , 0 < \alpha_n \leq 1 \exists k_n \forall k \geq k_n \ [ \text{a block code} \]

\( \mathcal{C}_k(n) \) for \( k \) exists allowing at least \( \lfloor (\mathcal{L}_0(n)-\varepsilon_n)k \rfloor ; \lfloor (\mathcal{L}_1(n)-\varepsilon_n)k \rfloor \) bit to be transmitted in \( k \) transmissions, with both error probabilities at most \( c_n \cdot (\lambda_n)^{\varepsilon_n} , \varepsilon_n := (k)^{\alpha_n} \).

(3.4.2.10) Theorem. \( \mathcal{A}_n \) holds for all \( n \geq 0. \)

Proof: We use induction on \( n \). For \( n = 0 \), the assertion follows from Theorem (3.3.3.1), where the sequence of codes \( \mathcal{C}_k(0) \) is constructed with \( a_0 = 1 , e_0 = k. \)
Chapter 3

Assume that $\mathcal{A}_n$ holds for some $n$ and let $\varepsilon_{n+1} > 0$. Let $\delta$, $\varepsilon$, and $\varepsilon_n$ be positive numbers, to be specified later and depending on $\varepsilon_{n+1}$ only. Let $k > 0$. For the given $\delta$, we choose a number $D \in \mathbb{N}$ such that (3.4.2.11) holds. Here $\mathcal{A}(d)$ denotes the state in the chain reached after $d$ transitions. Note that $D$ exists since $q_A$ is the stationary probability of $A$ (cf. (3.4.2.4)) and the convergence is uniform.

(3.4.2.11) $\forall d \geq D \forall A \in \mathcal{A}_{\text{inv}} \left| \Pr\{\mathcal{A}(d) = A\} - q_A \right| \leq \delta/2$.

Let

(3.4.2.12) $\epsilon_m := \left\{ \varepsilon (1 + \delta \mathcal{A}_{\text{inv}}) + \delta \sum_{A \in \mathcal{A}_{\text{inv}}} (r_0(A) + r_1(A)) \right\}/\rho_{\text{inv}}$,

then $\epsilon_m \to 0$ if $\varepsilon \to 0$ and $\delta \to 0$. For $t \in \mathbb{N}$, let $a_t$ and $\ell_t$ be as in Theorem (3.3.3.1) (where $\epsilon$ plays the role of the $\epsilon$ in Theorem (3.3.3.1)) and define $b_t$ by

(3.4.2.13) $b_t := \left\lfloor t - t(\ell_{\text{inv}} - \delta \mathcal{A}_{\text{inv}}) + t(\rho_{\text{inv}} + \delta) \cdot \frac{\rho_{\text{inv},0^+} \cdot \varepsilon_m + 1}{\rho_0(n) - \varepsilon_n} \right\rfloor$.

Let $t$ be the largest integer for which (3.4.2.14) holds.

(3.4.2.14) $k \geq (a_t - D) \cdot b_t + t(\ell_t - a_t + D)$.

Assume that $a_t > D$, which means that $t$ must be large enough and hence $k$ must be large enough (depending on $\varepsilon_{n+1}$). Define $R_i^{(n+1)}$ by the following equality.

(3.4.2.15) $R_i^{\text{inv},1} + \frac{\epsilon_m + R_i^{(n+1)}}{R_i(n) - \varepsilon_n} = \frac{R_i^{\text{inv},0} + \epsilon_m}{R_0(n) - \varepsilon_n}$.

Since $R_i^{(n+1)} \to R_i^{\text{inv},1}$ if $\epsilon_m$ and $\epsilon_n$ tend to zero, it is possible to choose $\epsilon$, $\epsilon_n$, and $\delta$ such that $R_i^{(n+1)} \geq 0$ by Lemma (3.4.2.7). (Note: if (3.4.2.5.c) holds, it may happen that $R_i^{(n+1)} < 0$, depending on the sign of $R_i(n) - R_0(n)$. In this case we use $R_i^{(n+1)} \to R_i^{\text{inv},1}$ instead of $R_i^{(n+1)}$. Then $R_i^{(n+1)} \geq 0$ and the rest of the proof should be read with 0's and 1's interchanged.) Hence, by

}\]
(3.4.2.8), it is possible to choose \( \varepsilon_n, \varepsilon_n', \delta \) such that (3.4.2.16) holds.

\[
(3.4.2.16)
\]

\[
\frac{\bar{H} + 2\delta}{(\bar{H} + \delta)\{1 - (\varphi_{\text{inv}} - \delta|\mathcal{N}_{\text{inv}}|) + (\varphi_{\text{inv}} + \delta)\left[\frac{p_{\text{inv},0} + \varepsilon_{\mathcal{M}}}{P_0(n) - \varepsilon_n}\right]\} + 6\delta}
\geq P_0(n + 1) - \frac{\varepsilon_{n+1}}{2},
\]

\[
\frac{\bar{H} + 2\delta + (\bar{H} + \delta)\varphi_{\text{inv}} - \delta L_1(n + 1)}{(\bar{H} + \delta)\{1 - (\varphi_{\text{inv}} - \delta|\mathcal{N}_{\text{inv}}|) + (\varphi_{\text{inv}} + \delta)\left[\frac{p_{\text{inv},0} + \varepsilon_{\mathcal{M}}}{P_0(n) - \varepsilon_n}\right]\} + 6\delta}
\geq P_1(n + 1) - \frac{\varepsilon_{n+1}}{2}.
\]

Hence we can choose a large enough \( t \) such that (3.4.2.17) holds.

\[
(3.4.2.17)
\]

\[
\frac{t[ t(\bar{H} + 2\delta)]}{(a_{t+1} - D)\cdot b_{t+1} + (t+1)(\ell_{t+1} - a_{t+1} + D)}
\geq P_0(n + 1) - \varepsilon_{n+1},
\]

\[
\frac{t[ t(\bar{H} + 2\delta)]}{(a_{t+1} - D)\cdot b_{t+1} + (t+1)(\ell_{t+1} - a_{t+1} + D)}
\geq P_1(n + 1) - \varepsilon_{n+1}.
\]

Now we construct the block code \( \mathcal{C}_k(n+1) \). The block length of this code will be \( k \). Only \( (a_{t-} - D)\cdot b_t + t(\ell_{t} - a_{t} + D) \) transmissions are used for the sending of information; any remaining transmissions (cf. (3.4.2.14)) consist of dummy symbols. We show that \( \{ (P_0(n+1) - \varepsilon_{n+1})k, (P_1(n+1) - \varepsilon_{n+1})k \} \) bit can be transmitted with \( \mathcal{C}_k(n+1) \). In fact,

\[
(3.4.2.18) \{ t[ t(\bar{H} + 2\delta)], t[ t(\bar{H} + 2\delta)] + (a_{t-} - D)\varphi_{\text{inv}} - \delta L_1(n + 1) \}
\]

bit will be transmitted with it. This is at least as much as was required, since

\[
t[ t(\bar{H} + 2\delta)] \geq \lceil (P_0(n+1) - \varepsilon_{n+1})((a_{t+1} - D)\cdot b_{t+1} + (t+1)(\ell_{t+1} - a_{t+1} + D)) \rceil
\]

- 77 -
\[ \geq \lceil (k_0(n+1) - \varepsilon_{n+1})k \rceil. \]

The first inequality follows from (3.4.2.17) and the second one from the definition of \( t \). The inequality for the \( 1 \to 0 \) direction can be found in the same way.

The amount of information that will be transmitted is split up as

\[ (3.4.2.19) \{ \ell t(\bar{\beta} + 2\delta), \ell t(\bar{\beta} + 2\delta) \} \text{ and } \{ 0, (a_1 - \theta) t(\ell \text{inv} - \delta) k_1(n+1) \} \]

bit. With \( \mathcal{M}_0 = [2^t(\bar{\beta} + 2\delta)] \) and \( \mathcal{M}_1 = [2^t(\bar{\beta} + 2\delta)] \) as in Theorem (3.3.3.1), the first part can be considered as the information of \( t \) independent message pairs \((w_0, w_1)\) with \( w_i \in \{0, 1, \ldots, \mathcal{M}_i, t-1\} \) for \( i \in \{0, 1\} \). These \( t \) pairs are denoted by \((w_0, w_1)_0, (w_0, w_1)_1, \ldots, (w_0, w_1)_{t-1}\). Each of the pairs \((w_0, w_1)_j\) can be transmitted with the block code \( \mathcal{E}_t \) that can be constructed from the tree \( T \) using Theorem (3.3.3.1). Hereto \( \ell t \) symbols per pair are needed, and the error probability per pair is at most \( c_T(\lambda_T)^t \) for some \( c_T > 0, 0 < \lambda_T < 1 \).

All pairs are encoded simultaneously in the following way. Also, see Figure (3.4.2.27). First consider user 0. Let pair \((w_0, w_1)_j\) correspond to \((x_0, x_1, \ldots, x_{t-1}) \in \ell t, \) the input sequence that would be sent by user 0 using the code \( \mathcal{E}_t \). User 0 transmits \( \mathcal{P}_0, \mathcal{P}_1, \ldots, \mathcal{P}_{\ell t-1} \) where \( \mathcal{P}_i \) contains the information about \((x_{i0}, x_{i1}, \ldots, x_{it-1}) \) for \( 0 \leq i < \ell t \). We call \( \mathcal{P}_i \) the \( i^{th} \) packet. We distinguish between the cases \( i \leq D, D < i \leq a_t \) and \( i > a_t \).

If \( i \leq D \) or \( i > a_t \), we set \( \mathcal{P}_i := (x_{i0}, x_{i1}, \ldots, x_{it-1}) \), so \( \mathcal{P}_i \) contains \( t \) symbols. No further coding takes place. For \( D < i \leq a_t \) we proceed as follows. The symbols \( x_{i0}, x_{i1}, \ldots, x_{it-1} \) correspond to independent transmissions in the tree \( T \). More specifically, \( x_{i,j} \) corresponds to a transmission in a vertex at level \( i \) in the \( j^{th} \) replica of the \( T \) consisting of \( t \) copies of \( T \). This is illustrated in Figure (3.4.2.20), where the vertices for the \( x_{i,j} \) are shown as open circles.
(3.4.2.20) Figure. The $i^{\text{th}}$ transmission for $t$ independent message pairs.

For each transmitted symbol, user 0 can determine the vertex in $T$ it corresponds to. For $A \in K_{\text{inv}}$, let $W(A) :=$ the number of symbols among these $t$ that are transmitted in vertex $A$, and let $W := \sum_{A \in K_{\text{inv}}} W(A)$. The packet $P_i$ will contain $b_t$ symbols (cf. (3.4.2.13)). We distinguish two cases. If some $A \in K_{\text{inv}}$ exists for which $|W(A) - q_{\lambda t}| > \delta t$, then the $b_t$ symbols of $P_i$ are randomly chosen. Otherwise user 0 first transmits the $t-W$ symbols corresponding to visible vertices. The remaining $W$ symbols are compressed by user 0 such that, for all $A \in K_{\text{inv}}$, the $W(A)$ symbols transmitted in vertex $A$ are represented by $\lfloor (r_0(A) + \varepsilon_x) \cdot W(A) \rfloor$ binary digits. This is possible by Lemma (3.4.2.1) and since $A \in K_{\text{inv}}$, so (3.4.1.2) holds. The error probability for the compression is at most

\begin{equation}
\sum_{A \in K_{\text{inv}}} c_{A}(\lambda_A)^{W(A)} \leq c_S(\lambda_S)^t
\end{equation}

for some $c_A, \lambda_A, c_S$ and $\lambda_S$. How these binary digits are transmitted will be explained later; their number is (using (3.4.2.2) in the second inequality)

\begin{equation}
\sum_{A \in K_{\text{inv}}} \lfloor (r_0(A) + \varepsilon_x) \cdot W(A) \rfloor
\end{equation}
\[ \sum_{A \in \mathcal{U}_{\text{inv}}} ((r_0(A) + \varepsilon_z) \cdot (q_A^t + \delta) t + 1) \]

\[ \leq t \cdot q_{\text{inv}}^t \cdot (r_0(A) + \varepsilon_m) + \varepsilon_{\text{inv}}^t + |\mathcal{U}_{\text{inv}}| \]

\[ \leq t \cdot q_{\text{inv}}^t (r_0(A) + \varepsilon_m) + |\mathcal{U}_{\text{inv}}| \]

with \( \varepsilon_m \) defined in (3.4.2.12). User 0 adds some dummy binary digits until he has enough symbols. This is possible if \( t \) is large enough, depending on \( \varepsilon_m \) and \( \delta \).

Similarly, user 1 sends symbols of \( I_1 \). For packet \( P_i \) with \( 0 < i \leq a_i \), he sends symbols. If \( D < i \leq a_i \), he sends symbols. If \( |\mathcal{U}(A) - q_A^t| > \delta t \) for some \( A \in \mathcal{U}_{\text{inv}} \), the symbols are random; otherwise he sends the \( t - \mathcal{U} \) symbols corresponding to visible vertices and compresses the remaining \( \mathcal{U} I_1 - \)symbols to

\[ \sum_{A \in \mathcal{U}_{\text{inv}}} \left( (r_1(A) + \varepsilon_z) \cdot |\mathcal{U}(A)| \right) \]

binary digits. He adds dummy symbols until their number is enough.

Now recall that some extra information must be sent from user 1 to 0. For each packet \( P_i \) with \( D < i \leq a_i \), user 1 has exactly \( \left. t(q_{\text{inv}}(t - \delta) R_1^{t+1}(n+1)) \right. \) bit of extra information to be transmitted (cf. (3.4.2.19)). In the \( i \)-th packet, this is done as follows. If for some \( A \in \mathcal{U}_{\text{inv}} \), \( |\mathcal{U}(A) - q_A^t| > \delta t \), no extra information is sent. Otherwise, user 1 takes the \( \left( (q_{\text{inv}}(t - \delta) R_1^{t+1}(n+1)) \right. \) bit together with the \( \left( (R_{\text{inv},1}^t + \varepsilon_m) q_{\text{inv}}(t + \delta) t \right. \) that he still has to transmit by (3.4.2.25). If necessary, he adds some information to this until he has enough symbols.

\[ \left( (R_{\text{inv},1}^t + \varepsilon_m + R_1^{t+1}(n+1)) \right. \cdot (q_{\text{inv}} + \delta) t \]

\[ \left. \right. \]
bit. Notice that the latter number is larger than the sum of the two former if $t$ is large enough. At the same time, user 0 still has to transmit the amount of information given by (3.4.2.22). Hence

\[(3.4.2.25)\]

\[\{ [(R_{\text{inv},0} + \varepsilon_m) \cdot (Q_{\text{inv}} + \delta) t], [(R_{\text{inv},1} + \varepsilon_m + R'_1(n+1)) \cdot (Q_{\text{inv}} + \delta) t] \} \]

bit must be transmitted in this situation. Now we describe how this is done. Let

\[(3.4.2.26)\]

\[k' := \frac{[(R_{\text{inv},0} + \varepsilon_m) \cdot (Q_{\text{inv}} + \delta) t]}{R_0(n) - \varepsilon_n} = \frac{[(R_{\text{inv},1} + \varepsilon_m + R'_1(n+1)) \cdot (Q_{\text{inv}} + \delta) t]}{R_1(n) - \varepsilon_n}.\]

The equality holds because of (3.4.2.15). By assumption $\lambda_n$, a code $C_{(k')(n)}$ with block length $k'$ exists, such that $\{ [(R_0(n) - \varepsilon_n) k'], [(R_1(n) - \varepsilon_n) k'] \}$ bit can be transmitted with it, with error probability $\leq c_n(\lambda_n)^{\varepsilon_n}, \varepsilon_n = (k')^\alpha n$. We assume that $k'$ is large enough ($k' \geq \varepsilon_n$) to make this possible. This yields a bound on $t$ and hence on $k$. By (3.4.2.25) and (3.4.2.26), the users can transmit the $\{ [(R_{\text{inv},0} + \varepsilon_m) \cdot (Q_{\text{inv}} + \delta) t], [(R_{\text{inv},1} + \varepsilon_m + R'_1(n+1)) \cdot (Q_{\text{inv}} + \delta) t] \}$ bit of (3.4.2.25) with this code.

At this point in the proof the 'bootstrapping' idea is used: in the new code $C_{k(n+1)}$, some of the information is transmitted using an old code $C_{(k')(n)}$. The new code itself can again be used to create another code. This gives rise to an infinite sequence of codes with increasing rates, as will be seen later (at least if $R_{\text{vis}}$ is higher than $R(T)$).

In this way all invisible-vertex transmissions, plus the extra information $R'_1(n+1)$ for the $i^{th}$ packet are encoded in $k'$ symbols. Therefore all information contained in the packet $P_i$ is encoded in at most
Chapter 3

\[ \max \{b_t, t - M + \left[ \frac{(l_{\text{inv}, 0} + \varepsilon_m)(q_{\text{inv}} + \delta)t}{l_0(n) - \varepsilon_n} \right] \} \]

symbols. Using \(|M(\mathcal{A}) - q_{\mathcal{A}}| - \delta t\) for \(\mathcal{A} \in \mathcal{V}_{\text{inv}}\) and \(M = \sum_{\mathcal{A} \in \mathcal{V}_{\text{inv}}} M(\mathcal{A})\), we find

\[
t - M + \frac{(l_{\text{inv}, 0} + \varepsilon_m)(q_{\text{inv}} + \delta)t}{l_0(n) - \varepsilon_n} + 1
\]

\[
\leq t - (q_{\text{inv}} - |\mathcal{V}_{\text{inv}}|)t + \frac{(l_{\text{inv}, 0} + \varepsilon_m)(q_{\text{inv}} + \delta)t}{l_0(n) - \varepsilon_n} + 1 \leq b_t.
\]

Hence each packet \(\mathcal{P}_i\), \(0 < i \leq a_t\), can be lengthened until it contains \(b_t\) symbols.

| \(\mathcal{P}_0\) | \(x_{0,0}, x_{0,1}, \ldots, x_{0,t-1}\) | \(t\) symb. |
| \(\vdots\) | \(\vdots\) | \(\vdots\) |
| \(\mathcal{P}_{a_t}\) | \(x_{a_t,0}, x_{a_t,1}, \ldots, x_{a_t,t-1}\) | \(b_t\) symb. |
| \(\vdots\) | \(\vdots\) | \(\vdots\) |
| \(\mathcal{P}_{\ell_{\mathcal{C}}-1}\) | \(x_{\ell_{\mathcal{C}}-1,0}, x_{\ell_{\mathcal{C}}-1,1}, \ldots, x_{\ell_{\mathcal{C}}-1,t-1}\) | \(t\) symb |

(3.4.2.27) Figure. Simultaneous transmission of information in packets.

Summarizing, the situation is as in Figure (3.4.2.27): the users transmit \(a_{\mathcal{C}}\) packets containing \(b_t\) symbols each and \((\ell_{\mathcal{C}} - a_{\mathcal{C}})\) packets containing \(t\)
symbols each. The total number of transmissions is \((a_t \cdot D) \cdot b + i(\ell_t \cdot a_t + D)\), which is what we had to show.

Decoding is done in the natural way: the decoding functions of \(C(k')^{(n)}\) and \(C_t\) together with the decoding function for the Slepian–Wolf compression scheme enable the two users to find an estimate for each other's message.

Finally we show that the error probabilities \(P_{e,0}\) and \(P_{e,1}\) (cf. (2.1.7)) are bounded by \(c_n+1(\lambda_{n+1})^{e_{n+1}}\) for some \(c_n+1 > 0, \ 0 < \lambda_{n+1} < 1, \ a_n+1 > 0, \ e_n+1 = k^2n+1\) and large enough \(k\). Errors can occur in one of the following ways.

1. An \(i, \ D < i \leq a_t\), and an invisible vertex \(A\) exist such that in the \(i\)th packet \(|W(A) - q_A^t| > \delta t\), and hence the Slepian–Wolf compression is not applied.

2. An \(i, \ D < i \leq a_t\), exists such that an error occurs in the Slepian–Wolf compression scheme for the \(i\)th packet.

3. An \(i, \ D < i \leq a_t\), exists such that the \{ \([R_{inv,0} + \varepsilon_m] \cdot (q_{inv} + \delta) t], \ [R_{inv,1} + \varepsilon_m + R_{t}^{(n+1)}] \cdot (q_{inv} + \delta) t] \} \) bit of the \(i\)th packet are not transmitted correctly with the code \(C(k')^{(n)}\).

4. A message pair \((w_0, w_1)\), \(j \in \{0, 1, \ldots, t-1\}\), exists for which code \(C_t\) is in error (though the symbols in all packets may be transmitted correctly).

The probabilities of these events are called \(P_1, P_2, P_3 \) and \(P_4\). We find

\[
P_1 \leq (a_t \cdot D) \cdot \sum_{A \in V_{inv}} Pr\{|W(A) - q_A^t| > \delta t\}
\leq (a_t \cdot D) \cdot c_L(\lambda_L)^t \ {\text{by (3.4.2.11) and the weak law of large numbers}}
\leq c(1)(\lambda(1))^t
\]

if \(t\) is large enough, for some \(c_L > 0, \ 0 < \lambda_L < 1, \ c(1) > 0, \) and \(0 < \lambda(1) < 1.\)
Chapter 3

\[ P_2 \leq (a_t - \theta) \cdot c(\lambda_S) t \{ \text{by (3.4.2.21)} \} \]

\[ \leq c(2)(\lambda(2)) t \]

for some \( c_S, \lambda_S, c(2), \lambda(2) \) and \( t \) large enough. Note that this is the place where we use the exponential error bound in the Slepian-Wolf lemma, (3.4.2.1).

\[ P_3 \leq (a_t - \theta) \cdot c_n(\lambda_n) e_n \text{ with } e_n = (k')^t(a_n), \]

for some \( c_n \) and \( \lambda_n \). This follows from assumption \( \lambda_n \). Hence, for large \( t \)

\[ P_3 \leq c(3)(\lambda(3)) e_n \]

\[ \leq c(3)(\lambda(3)) e_n' \text{ with } e_n' := t(a_n) \]

since \( k' = \mathcal{C} \cdot t \) for some constant \( \mathcal{C} > 0 \), by (3.4.2.26).

\[ P_4 \leq t \cdot c_4(\lambda_P) t \{ \text{by Theorem (3.3.3.1)} \} \]

\[ \leq c(4)(\lambda(4)) t \]

for some \( c(4), \lambda(4) \) and \( t \) large.

Now let

\[ c' := c(1) + c(2) + c(3) + c(4) > 0 \]

\[ \lambda' := \max \{ \lambda(1), \lambda(2), \lambda(3), \lambda(4) \} \ (0 < \lambda' < 1), \]

Then the total error probability \( P_{e,0} + P_{e,1} \) satisfies

\[ P_{e,0} + P_{e,1} \leq (c')(\lambda')(e_n') \text{ with } e_n' := t(a_n) \leq t. \]

By definition of \( t \) (see (3.4.2.14)), we have \( t^2 \geq \mathcal{P} \cdot k \), where \( \mathcal{P} \) depends on \( e_{n+1} \) but not on \( k \). Consequently

\[ e_n' = t(a_n) = t^2(a_n/2) \geq \mathcal{P} \cdot k(a_n/2) \]

for some \( \mathcal{P} \). With \( a_{n+1} := a_n/2 \) and \( e_{n+1} := k(a_{n+1}) \) we find
\[ P_{e_0} + P_{e_1} \leq (c')^{(\lambda')^F} e_{n+1} = c_{n+1} (\lambda_{n+1})^e_{n+1} \]

for some \( c_{n+1} > 0 \) and \( 0 < \lambda_{n+1} < 1 \) depending on \( e_{n+1} \). This concludes the proof of Theorem (3.4.2.10).

Now that we know that every rate \( \bar{r}(n) \) is achievable, we still have to prove that the sequence \( \{\bar{r}(n)\}_{n \in \mathbb{N}} \) converges and that its limit is \( \bar{r}_{vis} \), the visible rate of the bootstrap tree.

(3.4.2.28) Lemma. The sequence \( \{\bar{r}(n)\}_{n \in \mathbb{N}} \) defined in (3.4.2.6) converges. \( \square \)

Proof: With \( \eta_1 \) as defined in (3.4.2.6.c), first let us assume \( \eta_1 \geq 1 \). It follows by induction that the sequence \( \eta_n \) is nondecreasing and \( r_0(n) \) is nonincreasing in \( n \). Indeed, if \( \eta_n \geq \eta_{n-1} \), then by the first equality of (3.4.2.9), \( r_0(n) \leq r_0(n-1) \) and hence, using (3.4.2.6.c), \( \eta_{n+1} \geq \eta_n \). By the second equality of (3.4.2.9) this implies

\[
1 \geq \frac{r_0(n)}{r_0(n-1)} = \frac{r_{inv,0} + r_{vis,0}}{r_{inv,0} + r_{vis,0} (n-1)}
\]

Hence

\( r_{vis,0} < r_0(n-1) \)

for all \( n \). Therefore the sequence \( r_0(n) \) is bounded from below by \( r_{vis,0} \) and hence it has a limit that we call \( r_0 \).

In the case where \( \eta_1 < 1 \), we find analogously that \( \eta_n \) is nonincreasing and \( r_0(n) \) is nondecreasing. Now \( r_0(n) \) is bounded from above by \( r_{vis,0} \) and again the sequence converges to a limit \( r_0 \). We define

\[
\mu_n := \frac{r_{inv,0}}{r_{inv,0} + r_{vis}}.
\]

Since \( \eta_n r_1(n-1) = r_{inv,1} + r_{vis}^*(n) \) by b and c of (3.4.2.6), we obtain

\[ \mu_n = \frac{r_{inv,0}}{r_{inv,0} + r_{vis}} = r_0 \]
In other words, $R_1(n)$ can be written as a convex combination of $R_1(n-1)$ and $R_{vis,1}$. This reflects the proof of Theorem (3.4.2.10): in the code with rate $R(n)$, the information of the visible vertices is transmitted with rate $R_{vis}$ and the information of the invisible vertices is transmitted with a code of rate $R(n-1)$.

If $R_1(0) \leq R_{vis,1}$, then $R_1(n)$ will be a nondecreasing sequence bounded from above by $R_{vis,1}$; if $R_1(0) \geq R_{vis,1}$, then the sequence is nonincreasing with lower bound $R_{vis,1}$. In either case $R_1(n)$ converges to a limit, say $R_1$. This concludes the proof of the lemma.

Now we investigate the limit $(R_0, R_1)$. If we substitute

\[ R_0(n-1) = R_0(n) = R_0, \quad R_1(n-1) = R_1(n) = R_1 \]

in (3.4.2.6), then we find

\[
R_0 = \frac{V_{inv} R_{inv,0} + V_{vis} R_{vis,0}}{V_{inv} R_{inv,0} + V_{vis}}
\]

\[
R_1 = \frac{V_{inv} R_{inv,0} R_0 + V_{vis} R_{vis,1}}{V_{inv} R_{inv,0} R_0 + V_{vis}}.
\]

By multiplying both sides of these equalities by $V_{inv} R_{inv,0} R_0 + V_{vis}$, we find

\[ R_0 = R_{vis,0}, \quad R_1 = R_{vis,1}. \]

This completes the proof of the achievability of the bootstrap rate $R_{vis}(T)$. 

---

86
3.5. Relations between strategy trees

Here we present the proofs of the theorems in the previous sections. For reference purposes, we once more list the theorems themselves.

(3.2.1.2) Theorem. \( \forall N \in \mathbb{N} \left[ \text{co } \mathcal{F}(N) \subset C \right] \), \( \lim_{N \to \infty} \mathcal{F}(N) = \bar{\mathcal{F}} = C. \)

(3.2.2.3) Theorem. \( \forall N \in \mathbb{N} \left[ \text{co } \mathcal{F}^D(N) \subset C \right] \), \( \lim_{N \to \infty} \mathcal{F}^D(N) = \bar{\mathcal{F}}^D = C. \)

(3.3.1.4) Theorem. \( \forall N \in \mathbb{N} \left[ \text{co } \mathcal{V}(N) \subset C \right] \), \( \lim_{N \to \infty} \mathcal{V}(N) = \bar{\mathcal{V}} = C. \)

(3.3.2.2) Theorem. \( \forall N \in \mathbb{N} \left[ \text{co } \mathcal{V}^D(N) \subset C \right] \), \( \lim_{N \to \infty} \mathcal{V}^D(N) = \bar{\mathcal{V}}^D = C. \)

(3.3.4.6) Theorem. \( \forall N \in \mathbb{N} \left[ \text{co } \mathcal{V}^0(N) \subset C \right] \), \( \lim_{N \to \infty} \mathcal{V}^0(N) = \bar{\mathcal{V}}^0 = C. \)

(3.4.1.8) Theorem. \( \forall N \in \mathbb{N} \left[ \text{co } \mathcal{B}(N) \subset C \right] \), \( \lim_{N \to \infty} \mathcal{B}(N) = \bar{\mathcal{B}} = C. \)

In the proofs we will use several inclusions between the regions defined, like \( \mathcal{F}(N) \subset \mathcal{V}(N) \) and \( \mathcal{F}(N) \subset \mathcal{F}(2N) \). Figure (3.5.1) shows some of the relations that will be used. In this figure, arrows denote inclusions: an arrow pointing from region \( A \) to \( B \) means \( A \subset B \).

\[
\begin{array}{cccccccc}
\text{C} \\
\uparrow \\
\text{B}(N) \\
\uparrow \\
\mathcal{V}(N) \\
\mathcal{V}^D(N) \quad \mathcal{F}(N) \quad \mathcal{V}^0(N) \quad \mathcal{F}^D(N) \quad \mathcal{F}^0(N) \\
\end{array}
\]

(3.5.1) Figure. Relations between the strategy trees.
The inclusions pictured in Figure (3.5.1) are easy to prove. In Section (3.4.2) we have shown that $B(N) \subseteq C$ for all $N$. Since every $V(N)$ tree can be regarded as a $B(N)$ tree (just assign type 'visible' to all vertices), we have $V(N) \subseteq B(N)$. In the same way it follows that $V^D(N) \subseteq V(N)$, $F(N) \subseteq V(N)$, etc: if we go one step 'down' in the figure, we add restrictions to the trees considered, so the set of rates is a subset of the one directly above it.

It is a well-known fact that, if a set of rates $\lambda$ is achievable for the TWC, then also the region $\text{co} \lambda$ is achievable. In fact, this follows from time sharing and was already used by Shannon [SHA61] in the definition of the inner bound, (2.2.2). Together with the above inclusions, this proves $\forall N \in \mathbb{N} \left[ \text{co} \ T(N) \subseteq C \right]$ and similar statements for all other types of trees mentioned in the list of theorems. The second part of each theorem will be proved using the following lemma.

(3.5.2) Lemma. Suppose the following holds for a sequence of regions $\lambda_N \subseteq \mathbb{R}^2$ and for all $\mathbf{a} \in \mathbb{R}^2$ (here $d(\mathbf{a}, \lambda_N)$ is defined as in (2.2.7)):

$$\exists_{N_0} \left[ \mathbf{a} \in \lambda_{N_0} \right] \implies \forall \epsilon > 0 \exists_{N_1} \forall N > N_1 \left[ d(\mathbf{a}, \lambda_N) < \epsilon \right].$$

Then $\{\lambda_N\}_{N \in \mathbb{N}}$ converges to a limit $\lambda$, with

$$\lambda := \bigcup_{N \in \mathbb{N}} \lambda_N.$$  \hfill \Box

Proof: First we prove that (i) of Definition (2.2.8) holds. Let $\mathbf{a} \in \lambda$ and $\epsilon > 0$. By definition of closure, an $N_0 \in \mathbb{N}$ and $\mathbf{a}_0 \in \lambda_{N_0}$ exist such that $d(\mathbf{a}, \mathbf{a}_0) < \epsilon/2$. By the assumption in the lemma, we have

$$\exists_{N_1} \forall N > N_1 \left[ d(\mathbf{a}_0, \lambda_N) < \epsilon/2 \right].$$

Hence, for such an $N_1$ and $N > N_1$, we have

$$d(\mathbf{a}, \lambda_N) = \inf \{ d(\mathbf{a}, \mathbf{a}_N) | \mathbf{a}_N \in \lambda_N \}$$

$$\leq \inf \{ d(\mathbf{a}, \mathbf{a}_0) + d(\mathbf{a}_0, \mathbf{a}_N) | \mathbf{a}_N \in \lambda_N \}$$

$$< \epsilon/2 + \epsilon/2 = \epsilon.$$
which proves (i). Now let $a \notin \lambda$, so $a$ is in the complement of $\lambda$. Since this set is open, $a$ is an interior point of the complement. Hence an $\varepsilon > 0$ exists for which

$$\forall y \in \lambda \ [d(a, y) > \varepsilon], \text{ or}$$

$$\forall N \in \mathbb{N} \ [d(a, A_N) > \varepsilon].$$

This proves that (ii) of Definition (2.2.8) holds.

Using this lemma, we will now prove

$$\lim_{N \to \infty} \mathcal{F}(N) = \tilde{\mathcal{F}}$$

and the corresponding statements for the other regions. First we show that the condition in Lemma (3.5.2) holds for the sequences $\mathcal{F}(N)$. Let $N_0 \in \mathbb{N}$, $\epsilon > 0$ and $f \in \mathcal{F}(N_0)$. In Section 3.2.2 we showed $f \in \mathcal{F}(tN_0)$ for all $t \in \mathbb{N}$. Now we prove

$$(3.5.3) \forall N \in \mathbb{N} \forall f_N \in \mathcal{F}(N) \ d(f_N, \mathcal{F}(N+K)) = O(1/N), \ N \to \infty.$$  

Consider an $F(N)$ tree with rate $f_N$. Its vertices are labeled $\lambda_i$, $i = 0, 1, 2, \ldots$. We append $K$ 'layers' of vertices to the leaves in the tree in which no uncertainty is resolved (e.g. both users send a single input symbol for the whole region). This results in an $F(N+K)$ tree with rate $f_{N+K}$.

$$f_{N+K} = \sum_i w(\lambda_i) \xi(\lambda_i) \frac{N}{N + K} = f_N \left(1 - \frac{K}{N + K}\right).$$

Therefore

$$d(f_N, f_{N+K}) = \|f_{N+K} - f_N\| = \|f_N - \frac{K}{N+K}\| = \|f_N\| \cdot 0(1/N), \ N \to \infty,$$

which proves (3.5.3) because $f_N$ is bounded. It follows that for $N = tN_0 + K$ with $t \geq 1$ and $0 \leq K < N_0$:

$$d(f, \mathcal{F}(N)) = d(f, \mathcal{F}(tN_0 + K)) = O(1/t), \ t \to \infty.$$
Chapter 3

Therefore, if $N$ is large enough,

$$d(\mathcal{L}, \mathcal{T}(N)) < \varepsilon.$$  

Now we can apply Lemma (3.5.2), yielding

$$\lim_{N \to \infty} \mathcal{T}(N) = \mathcal{\tilde{T}}.$$  

We will apply the same reasoning to prove

$$\lim_{N \to \infty} \mathcal{T}_0(N) = \mathcal{\tilde{T}}_0.$$  

Let $N_0 \in \mathbb{N}$, $\varepsilon > 0$ and $f \in \mathcal{T}_0(N_0)$. As argued in Section 3.2.2 and 3.3.3, we have $f \in \mathcal{T}_0(tN_0)$ for all $t \in \mathbb{N}$. By appending $K$ layers of dummy vertices to an $\mathcal{T}_0(tN_0)$ tree we obtain an $\mathcal{T}_0(tN_0+K)$ tree with the same rate as computed above. Therefore again

$$d(f, \mathcal{T}_0(tN_0+K)) = 0(1/t), \quad t \to \infty.$$  

Hence $d(f, \mathcal{T}_0(N)) < \varepsilon$ if $N$ is sufficiently large. Lemma (3.5.2) yields

$$\lim_{N \to \infty} \mathcal{T}_0(N) = \mathcal{\tilde{T}}_0.$$  

For the regions $\mathcal{V}(N)$ appearing in Theorem (3.3.1.4) we have to change the argument a little, but we can still apply Lemma (3.5.2). Let $N_0 \in \mathbb{N}$, $\varepsilon > 0$ and $\mathcal{V}(N_0)$. Then $\mathcal{V}(tN_0)$ for all $t \in \mathbb{N}$, as before. We will prove

$$\forall f \in \mathbb{N} \forall \mathcal{V}_{N_0} \in \mathcal{V}(N) \quad d(\mathcal{V}_{N_0}, \mathcal{V}(N+K)) = 0(1/K), \quad N \to \infty.$$  

Let $I \in \mathbb{N}$. Consider a $\mathcal{V}(N)$ tree with rate $\mathcal{V}_{N}$ and vertices $A_0, A_1, \ldots$. Let $A_z$ be a leaf at level $N-1$ of the tree. We change the tree into a $\mathcal{V}(N+I)$ tree by adding a path of $I$ dummy vertices (with rate $0$) below vertex $A_z$. Call the new vertices $A_0', A_1', \ldots, A_{I-1}'$, then $w(A_j') = w(A_j)$ for all $j$ and $w(A_0') \leq w(A_z)$. Since $A_0'$ has $N$ predecessors in the tree, the weight of the $\mathcal{V}(N)$ tree satisfies
Strategy Trees for TWCs

\[ \sum_{i} w(A_i) \geq \sum_{i} w(A_i) = N \cdot w(A_0). \]

\[ A_i : \text{predecessor of } A_0 \]

\[ A_i : \text{predecessor of } A_0 \]

Hence the rate of the \( V(N+1) \) tree equals \( v_{N+1} \).

\[ \frac{\sum_{i} w(A_i) \cdot v(A_i)}{\sum_{i} w(A_i) + K \cdot w(A_0)} = \frac{\sum_{i} w(A_i) \cdot v(A_i)}{\sum_{i} w(A_i) + K \cdot w(A_0)} \]

\[ = v_N \cdot \left( 1 - \frac{K \cdot w(A_0)}{\sum_{i} w(A_i) + K \cdot w(A_0)} \right). \]

Hence

\[ d(v_N, v_{N+1}) = \| v_N - v_{N+1} \| \]

\[ = \| v_N \cdot \frac{K \cdot w(A_0)}{\sum_{i} w(A_i) + K \cdot w(A_0)} \| = \| v_N \| \cdot \frac{K \cdot w(A_0)}{\sum_{i} w(A_i) + K \cdot w(A_0)}. \]

Since

\[ \sum_{i} w(A_i) + K \cdot w(A_0) \geq (N+1) \cdot w(A_0), \]

we find

\[ d(v_N, v_{N+1}) \leq \| v_N \| \cdot \frac{K}{N+1} = 0(1/N), N \to \infty. \]

This proves (3.5.4). With \( N = tN_0 + k, t \geq 1 \) and \( 0 \leq k < N_0 \), we find

\[ d(v, V(N)) = d(v, V(tN_0 + k)) = 0(1/t), t \to \infty. \]

Therefore \( d(v, V(N)) < \epsilon \) if \( N \) is large enough. By Lemma (3.5.2), this proves

\[ \lim_{N \to \infty} V(N) = \bar{V}. \]

The above proof for \( V(N) \) trees can be applied to \( V^2(N) \) and \( V^0(N) \) trees as well, in the same way as the proof for \( F(N) \) and \( F^1(N) \) trees is similar. However, the reader should be aware of the implication of 'taking \( t \) copies of a \( V^0(N) \) tree'.
(necessary to show $y \in \mathcal{V}^0(N) \Rightarrow y \in \mathcal{V}^0(tN)$). If the $\mathcal{V}^0(N)$ tree has thresholds on an $(N_0 + 1) \times (N_1 + 1)$ grid, then the $\mathcal{V}^0(tN)$ tree has thresholds on an $(N_0^t + 1) \times (N_1^t + 1)$ grid and it represents a variable length code with error probability zero for $(N_0^t, N_1^t)$ messages. Since the rate of the tree (and the rate of the code) is not affected by this, the rest of the proof can be continued as before. We find

$$\lim_{N \to \infty} \mathcal{V}^0(N) = \bar{v}^0 \quad \text{and} \quad \lim_{N \to \infty} \mathcal{V}^0(N) = \bar{v}^0.$$

Finally we show that Lemma (3.5.2) can be applied to the regions $B(N)$. Let $\varepsilon > 0$, $N_0 \in \mathbb{N}$, $h \in B(N_0)$. Consider a $B(N_0)$ tree with visible rate $h$ and let $T$ be the corresponding $T(N_0)$ tree with type assignment, for some $N_0^t$. If we take $t$ copies of the tree $T$ in the usual way, and we define the types of the new vertices according to the types in $T$, then it is easy to check that this yields a $B(tN_0)$ tree with rate $h$. Therefore $h \in B(tN_0)$. Next, we show

$$\forall N \in \mathbb{N} \forall \varepsilon > 0 \exists N_0 \in \mathbb{N} \left( B(N_0) \Rightarrow \forall \varepsilon > 0 \exists N_1 \in \mathbb{N} \left( B(N_1) \Rightarrow d(h, B(N)) = 0(1/N), \quad N \to \infty \right) \right).$$

Let $N \in \mathbb{N}$, $N \in \mathbb{N}$. Let $h_N$ be the visible rate of a $B(N)$ tree constructed from a $T(N)$ tree with type assignment. Let $A_x$ be a visible vertex at visible distance $N-1$ (i.e., the maximum possible visible distance) from the root of the tree. We remove any invisible vertices below $A_x$, which does not change the visible rate. Consider one of the connected regions remaining after the resolution in $A_x$. We partition this region into rootlike rectangles by slicing (cf. Lemma (3.3.2.3)), in such a way that at least one rectangle remains, say $\mathcal{Z}$, having area at most $1/(MN)$. The slicing vertices appear in the tree below $A_x$ and they are given type 'invisible' (by Lemma (3.3.2.3), these vertices have the PBV property). Finally we add a path of $N$ visible vertices (thus creating a $B(N)$ tree) in which a dummy resolution in $\mathcal{Z}$ is done. Call these vertices $A_0^l, A_1^l, \ldots, A_{l-1}^l$, then
\( r(A_j^*) = 0 \) and \( w(A_j^*) \leq 1/(MN) \) for all \( j \). Let \( b_{N+K} \) be the rate of this tree. Now

\[
\begin{align*}
    b_{N+K} &= \frac{\sum_{A_i \in \mathcal{K}_{vis}} w(A_i) r(A_i)}{\sum_{A_i \in \mathcal{K}_{vis}} w(A_i) + \sum_{j} w(A_j^*)} = b_N \cdot \left(1 - \frac{\sum_{j} w(A_j^*)}{\sum_{A_i \in \mathcal{K}_{vis}} w(A_i) + \sum_{j} w(A_j^*)}\right).
\end{align*}
\]

Since

\[
\sum_{j} w(A_j^*) \leq 1/N \quad \text{and} \quad \sum_{A_i \in \mathcal{K}_{vis}} w(A_i) \geq 1,
\]

we find

\[
||b_{N+K} - b_N|| = ||b_N|| \cdot (1 + O(\frac{1}{N})), \quad N \to \infty
\]

which proves (3.5.5). For all \( \epsilon > 0 \) and sufficiently large \( N \), we can now prove — as before — that \( d(b, B(N)) < \epsilon \). By Lemma (3.5.2) we can conclude

\[
\lim_{N \to \infty} B(N) = B.
\]

The last part of the six theorems that we have to prove is

\[
\hat{\mathcal{F}} = \hat{\mathcal{F}}^0 = \hat{\mathcal{V}} = \hat{\mathcal{V}}^0 = \hat{\mathcal{V}} = B = C.
\]

First we prove that \( \hat{\mathcal{F}}, \hat{\mathcal{V}} \) and \( B \) are equal to \( C \). From Figure (3.5.1) it follows that \( \mathcal{F}(N) \subset \mathcal{V}(N) \subset B(N) \subset C \) for all \( N \). Hence, for \( N \to \infty \), we also find \( \hat{\mathcal{F}} \subset \hat{\mathcal{V}} \subset B \subset C \).

Furthermore we have the following lemma.

\textbf{(3.5.6) Lemma.} For all \( N \), we have \( co \mathcal{F}(N) \subset \hat{\mathcal{F}} \). \(\square\)

\textbf{Proof:} Let \( N \in \mathbb{N} \) let \( T_0 \) and \( T_1 \) be \( F(N) \) trees and let \( \lambda \in (0,1) \). For \( t \in \mathbb{N} \), we will construct an \( F(tN+1) \) tree \( T \) such that \( \mathcal{F}(T) = \lambda \mathcal{F}(T_0) + (1-\lambda) \mathcal{F}(T_1) \) for \( t \to \infty \). See Figure (3.5.7). This will prove the fact that \( \lambda \mathcal{F}(T_0) + (1-\lambda) \mathcal{F}(T_1) \in \hat{\mathcal{F}} \).

In the root of the tree \( T \) we perform row slicing. By choosing appropriate input symbols (say \( x_0(a) \) and \( x_0(b) \) for user 0 and \( x_1 \) for user 1) we can partition the unit square into two rootlike rectangles, one with area \( \lambda \) and the other with
area $1-\lambda$. To the rectangle with area $\lambda$ we append $t$ copies of the tree $r_0$ in the usual way. We partition the other region according to $t$ copies of $r_1$.

\[
\begin{array}{c}
\begin{array}{c}
\Rightarrow \quad t \text{ times} \\
\downarrow \\
\text{tree } r_0 \quad \lambda \\
\end{array} \\
\begin{array}{c}
\Rightarrow \quad t \text{ times} \\
\downarrow \\
\text{tree } r_1 \quad 1-\lambda \\
\end{array} \\
\end{array}
\]

(3.5.7) Figure. Combining two $F(N)$ trees into an $F(tN+1)$ tree.

It is easy to see that $T$ is an $F(tN+1)$ tree with rate

\[
\mathbb{A}(T) = \{ 1 \cdot (A,0) + \lambda tN \cdot \mathbb{A}(r_0) + (1-\lambda) tN \cdot \mathbb{A}(r_1) \}/\{tN+1\},
\]

which tends to $\lambda \mathbb{A}(r_0) + (1-\lambda) \mathbb{A}(r_1)$ if $t \to \infty$. Thus $\lambda \mathbb{A}(r_0) + (1-\lambda) \mathbb{A}(r_1) \in \mathcal{F}$ and the lemma is proved.

By Theorem (2.2.6), we know that

\[
\lim_{N \to \infty} \mathfrak{R}(N) = C.
\]

With Lemma (3.5.6) this yields $C \subset \mathcal{F}$. We have already proved $\mathcal{F} \subset C$, so $\mathcal{F} = C$.

Since we know $\mathcal{F} \subset \mathcal{Y} \subset \mathcal{B} \subset C$, it immediately follows that $\mathcal{Y} = \mathcal{B} = C$. 

\[94\]
To prove that $\mathcal{V}^0 = \mathcal{C}$, we need to think about the definition of a capacity region. Consider a rate point $\mathbf{R}$ lying in $\mathcal{C}$. Then, by Definition (2.1.9) and (2.1.10), a sequence of fixed length codes, say $\{\mathcal{C}(n)\}_{n \in \mathcal{W}}$, can be constructed such that the rate of code $\mathcal{C}(n)$ tends to $\mathbf{R}$, the block length tends to infinity and the error probabilities $P_{e,0}$ and $P_{e,1}$ tend to 0 with increasing $n$. Let code $\mathcal{C}(n)$ have parameters $\{M_0(n), M_1(n), N(n)\}$. Hence

$$
\lim_{n \to \infty} \left( \frac{\log(M_0(n))}{N(n)}, \frac{\log(M_1(n))}{N(n)} \right) = \mathbf{R} = (\mathbf{R}_0, \mathbf{R}_1).
$$

As we have seen in Section 3.2.3, the code $\mathcal{C}(n)$ can be represented in an $F(N(n))$ tree with thresholds on an $(M_0(n) + 1) \times (M_1(n) + 1)$ grid. Let $P_{e,0}$ and $P_{e,1}$ be $\varepsilon(n)$ for this code. We will change the $F(N(n))$ tree into a $F^0(N')$ tree for some $N' > N(n)$, to be defined later. Suppose that the two users use the code $\mathcal{C}(n)$. They partition the unit square according to the tree, in $N(n)$ steps, after which they try to determine the basic rectangle in which the message pair $(w_0, w_1)$ lies. In $\varepsilon(n) \cdot M_0(n) \cdot M_1(n)$ cases, on the average, they will not be able to do so. In that case, two or more basic rectangles will be connected; indeed, if there is just one basic rectangle remaining after transmission, then this is the correct one and it is known by both users.

If user 1 does not yet know the message of user 0, then both users are aware of this, and row slicing can be performed to tell user 1 the message $w_0$. At worst, this may take $\lfloor \log(M_0(n)) \rfloor$ transmissions. The row slicing vertices will appear below some of the leaves of the $F(N(n))$ tree. In the same way column slicing helps user 0 to determine the message $w_1$ sent by user 1. We need a path of at most $\lfloor \log(M_1(n)) \rfloor$ column slicing vertices in the tree for this. For every basic rectangle that could not be determined in $N(n)$ transmissions, we add dummy vertices until we have $N'$ of them, where
$N' := N(n) + \lceil \log(N_0(n)) \rceil + \lceil \log(N_1(n)) \rceil$.

Clearly we have constructed a $F^0(N')$ tree, since the unit square is partitioned into basic rectangles. The rate of this tree is, by Theorem (3.3.4.4),

$$\frac{\log(N_0(n))}{N}, \frac{\log(N_1(n))}{N}$$

where $N$ is the average codeword length. This rate lies in $\gamma^0$. With probability $1-e(n)$, the $N(n)$ transmissions in the $F(N(n))$ tree are sufficient to determine the message pair; with probability $e(n)$, $N'$ transmissions are used. Hence

$$N = (1-e(n)) \cdot N(n) + e(n) \cdot (N(n) + \lceil \log(N_0(n)) \rceil + \lceil \log(N_1(n)) \rceil)$$

Because of this we have

$$\lim_{n \to \infty} \frac{N}{N(n)} = \lim_{n \to \infty} \left\{ \frac{N(n)}{N(n)} + e(n) \cdot \left( \frac{\lceil \log(N_0(n)) \rceil}{N(n)} + \frac{\lceil \log(N_1(n)) \rceil}{N(n)} \right) \right\}$$

$$= 1 + \lim_{n \to \infty} e(n) \cdot (L_0 + L_1) = 1$$

by (3.5.8). Consequently

$$\lim_{n \to \infty} \left( \frac{\log(N_0(n))}{N}, \frac{\log(N_1(n))}{N} \right) = \lim_{n \to \infty} \left( \frac{\log(N_0(n))}{N(n)}, \frac{\log(N_1(n))}{N(n)} \right).$$

Since the rate on the right equals $\lambda$, this proves that every rate in $C$ can be approximated with rate points in $\gamma^0$. Therefore $C \subseteq \bar{\gamma}^0$. Together with the inclusions pictured in Figure (3.5.1), we find

$C = \bar{\gamma}^0$ and $C = \bar{\gamma}^0$.

Finally we show that $\tilde{F}^0 \subseteq \bar{\gamma}^0$. This yields, with Figure (3.5.1), $\tilde{F}^0 = \bar{\gamma}^0 = C$ and therefore the six theorems will be proved. This is done by changing a $F^0(N)$
tree into an $F^\mathcal{O}(N')$ tree that has almost the same rate as the $F^\mathcal{O}(N)$ tree, if $N'$ is sufficiently large. A similar technique was applied in [OVE87] to show $\bar{F} \supset \bar{V}$.

Let $N \in \mathbb{N}$ and let $T$ be a $F^\mathcal{O}(N)$ tree. Let $t \in \mathbb{N}$ and change the tree into a $F^\mathcal{O}(tN)$ tree by adding as many copies of the original tree as possible, without exceeding the maximum depth $tN-1$. This means that the $F^\mathcal{O}(N)$ strategy tree is repeated in every rootlike rectangle that remains in the tree, unless it appears at a level with number at least $(t-1)N+1$; in that case there is no room for one more copy below this vertex. The $F^\mathcal{O}(tN)$ tree has the same rate as the original tree, $\mathcal{I}(T)$. Now we complete the tree by adding dummy vertices with rate $0$, until we have an $F^\mathcal{O}(tN)$ tree. Call this tree $T_t$. Its rate, $\mathcal{I}(T_t)$, satisfies

$$\mathcal{I}(T_t) = \mathcal{I}(T) \cdot (1 - w_d/(tN)),$$

if $w_d$ is the total weight of all dummy vertices. By the construction method we have $w_d \leq N$, or $w_d/(tN) = O(1/t)$, $t \to \infty$. Hence we can approximate the rate $\mathcal{I}(T)$ in $F^\mathcal{O}$ arbitrarily closely with rates in $\bar{F}^\mathcal{O}$, if $t$ is large enough. Thus $\mathcal{V}^\mathcal{O} \subset \bar{F}^\mathcal{O}$.

We have now proved that the sequences $\mathcal{F}(N)$, $\mathcal{V}^\mathcal{O}(N)$, $\mathcal{V}(N)$, $\mathcal{V}^\mathcal{O}(N)$ and $\mathcal{B}(N)$ tend to the capacity region for large $N$. However, there is one more type of strategy tree that we have defined in Section 3.2, for which we could not prove the analogue of these theorems. This is the $F^\mathcal{O}(K)$ tree, defined in Definition (3.2.3.2). We have seen that every $F^\mathcal{O}(N)$ tree describes a fixed length code with error probability 0, and that every code with error probability 0 can be pictured in an $F^\mathcal{O}(N)$ tree. Therefore, if we define the zero-error capacity region as done in Definition (3.5.9), Theorem (3.5.10) is immediate.

(3.5.9) Definition. A rate $(\mathcal{I}_0, \mathcal{I}_1)$ is called zero-error achievable for a TWC $K$ if for all $\varepsilon > 0$ and large enough $N$, an $(\mathcal{I}_0, \mathcal{I}_1, N)$ code exists with error probability
Chapter 3

\[ P_{e,0} = P_{e,1} = 0 \quad \text{and} \quad \frac{\log(N)}{N} > I_0 - \epsilon, \quad \frac{\log(N)}{N} > I_1 - \epsilon. \]

The zero-error capacity region for \( K \), denoted by \( C^0_K \) (or just \( C^0 \)), is defined as the set of all zero-error achievable rates for \( K \).

\[ (3.5.10) \text{Theorem.} \quad \forall N \in \mathbb{N} \left[ \text{co} \mathcal{T}^0(N) \subset C^0 \right], \quad \lim_{N \to \infty} \mathcal{T}^0(N) = \mathcal{F}^0 = C^0. \]

It should be noted that, just like with ordinary one-way channels, the zero-error capacity region is not necessarily equal to the capacity region as defined in Definition (2.1.10). Unfortunately, very little is known about the zero-error capacity for TWCs. In the case of the BMC, we only have some lower bounds following from constructions (see Section 3.6), but we do not even know whether the Shannon inner bound is zero-error achievable for this channel.

3.6 Examples of strategy trees

3.6.1. Strategy trees for the Binary Multiplying Channel

In this section we take the BMC as our two-way channel \( K \) and we present rate pairs in the regions \( \mathcal{T}(N), \mathcal{T}^0(N), \mathcal{F}^0(N), \mathcal{V}(N), \mathcal{V}(N), \) etcetera, for some small values of \( N \). We are interested in the maximum achievable average rate for the two users, \( (I_0 + I_1)/2 \). Therefore we define

\[ f(N) := \sup \{ (I_0 + I_1)/2 \mid (I_0, I_1) \in \mathcal{T}(N) \}. \]

Similarly we can consider \( f^0(N), f^0(N), \) etcetera, as the supremum of all average rates in the regions \( \mathcal{T}^0(N), \mathcal{F}^0(N), \mathcal{V}(N), \ldots \).
Although $\mathcal{F}(1)$ is a convex region for the BMC (which has been proved by the author), it is not certain that the maximum average rate for some region is always achieved for a rate point with $I_0 = I_1$. We return to this later. This makes it very difficult to find good lower bounds on the average rate.

Even if we restrict our attention to symmetrical rates $(l, l)$, this does not make the search much easier. Since the BMC is a symmetrical channel (it is a $T$–channel with $f_K(x_0, x_1) = f_K(x_1, x_0)$ for all inputs), the obvious thing to do if we want to find a symmetrical rate is to construct a symmetrical tree. This is a tree that can be derived from some $F(N)$ tree for which the strategy functions $\sigma_0$ and $\sigma_1$ are equal. However, strangely enough, it cannot be proved that for each symmetrical rate in some region (say $A(N)$), a symmetrical $A(N)$ tree exists having this rate. Still, no counterexample has been found yet, and all results for symmetrical rates in this section have been obtained using symmetrical trees.

The tables below list the best lower bounds known for the average rates in the various regions. In some cases these correspond to symmetrical rates (and symmetrical trees). These cases are denoted with '(%s)' in the tables.

<table>
<thead>
<tr>
<th>$N$</th>
<th>$f^0(N)$</th>
<th>lower bound</th>
<th>$#(N)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>0.50000</td>
<td>(s)</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>0.52832</td>
<td>(s)</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>0.50000</td>
<td>(s)</td>
<td>4</td>
</tr>
<tr>
<td>5</td>
<td>0.51699</td>
<td>(s)</td>
<td>6</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>16</td>
<td>0.58402</td>
<td>(s)</td>
<td>650</td>
</tr>
</tbody>
</table>

(3.6.1.1) Table. Lower bounds on $f^0(N)$.

The results in Table (3.6.1.1) are taken from [OVE85]. In this table, $\#(N)$ denotes the number of messages (for both users) of the zero–error code that
corresponds to the $\mathcal{F}(V)$ tree. Hence the listed lower bound for $\mathcal{F}(V)$ equals $\log(V(N))/N$. It should be noted that the result for $N = 3$ stems from the code shown in Figure (3.2.3.1). The bounds for $N = 6, 7, \ldots, 15$ have been omitted since they are all lower than the bound for $N = 16$; they can be found in [OVE85]. The value 0.58402 for $N = 16$ is the highest rate known to be achievable with any $\mathcal{F}(V)$ tree. Therefore this is the sharpest lower bound for the zero-error capacity region of the BMC in the symmetrical case.

<table>
<thead>
<tr>
<th>$N$</th>
<th>$\mathcal{F}(V)$ lower bound</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>0.57549</td>
</tr>
<tr>
<td>3</td>
<td>0.59402</td>
</tr>
</tbody>
</table>

(3.6.1.2) Table. Lower bounds on $\mathcal{F}(V)$.

Although, for $N \in \{2, 3\}$, the values of the bounds for $\mathcal{F}(V)$ are considerably higher than the bounds for $\mathcal{F}(V)$, we do not list values for larger $N$. This is partly because we have already argued in Section 3.2.2 that $\mathcal{F}(V)$ trees do not provide interesting bounds on the capacity region, but it is also true that these bounds are hard to compute for larger values of $N$. Computing the maximum rate of an $\mathcal{F}(V)$ tree for fixed $N$ is a finite search problem since the thresholds are confined to a grid, but for $\mathcal{F}(V)$ trees the thresholds can assume values in $[0, 1]$ which makes it more complex to find the optimum rate.

The two trees that achieve the rates in Table (3.6.1.2) are given in Figures (3.6.1.3) and (3.6.1.4). In Figure (3.6.1.3), $t_1$ and $u_1$ denote the first thresholds for the two users: $t_1 = \Pr\{X_{00} = 1\}$, $u_1 = \Pr\{X_{10} = 1\}$. (An arrow to the left indicates the region where $Y = 0$, and an arrow to the right points to the region with $Y = 1$. This holds in all pictures of trees for the BMC in this section.)
The average rate of 0.57549 corresponds to a choice of $t_1 = u_4 = 0.60300$. The reader should notice that the highest possible rate for any symmetrical $F'(2)$ tree is less than 0.57549, since for a symmetrical tree we necessarily have rate 0 in the square region on the right.
Chapter 3

The best $F^2(3)$ tree is shown in Figure (3.6.1.4). In this figure, $F^2(2)$ denotes subdivision of the rectangle according to the $F^2(2)$ tree of Figure (3.6.1.3). The parameters $t_1$ and $u_1$ have the same meaning as before, and $t_2$ and $u_2$ are the thresholds for the left-hand vertex at level 1:

$$t_2 = \Pr\{I_{01}=1|I_{00}=1, I_{0}=0\}, \quad u_2 = \Pr\{I_{11}=1|I_{10}=1, I_{0}=0\}.$$  

This is in accordance with the notation used in [SME83]; a similar notation will be used in the figures to come. For the tree with rate 0.59402 we find:

$$t_1 = u_1 = 0.66752, \quad t_2 = u_2 = 0.33332.$$  

<table>
<thead>
<tr>
<th>$N$</th>
<th>$f(N)$ lower bound</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0.61695 (s)</td>
</tr>
<tr>
<td>2</td>
<td>0.61695 (s)</td>
</tr>
<tr>
<td>3</td>
<td>0.61964 (s)</td>
</tr>
<tr>
<td>4</td>
<td>0.62138</td>
</tr>
<tr>
<td>5</td>
<td>0.62333</td>
</tr>
<tr>
<td>6</td>
<td>0.62405</td>
</tr>
<tr>
<td>7</td>
<td>0.62966</td>
</tr>
</tbody>
</table>

(3.6.1.5) Table. Lower bounds on $f(N)$.

Most entries in Table (3.6.1.5) were found by Smeets (cf. [SME83]). They were found via a computer program that optimizes a function (the average rate) over many parameters (the thresholds in the tree). The bounds on $f(1)$ and $f(2)$ are equal to the symmetrical rate point of the Shannon inner bound. The tree corresponding to the bound for $f(3)$ is also symmetrical, but for $N = 4$, Smeets found an asymmetrical tree achieving a higher rate (0.62136) than any computed symmetrical tree. Close inspection of this tree showed that it could not be the global optimum over all $F(4)$ trees since its division of the rectangle remaining at level 1 of the tree was already suboptimal. Therefore we replaced this part of the tree with the optimum $F(3)$ tree (with rate 0.61964, as found by Smeets). After re-optimization this gave the improvement to 0.62138 listed in the table. The
thresholds for this optimum hardly differ from the ones found by Smeets and thus they are not listed here; they may be found in [SME83].

We are not convinced that this new point is the global optimum, because the tree is still asymmetrical. Since the function to be optimized has 54 parameters and has a large number of local optima, it is extremely hard to find its global optimum. This of course holds a fortiori for the $P(N)$ trees with $N = 5, 6$ and 7. For $N = 5$, we replaced the $P(4)$ tree (with rate 0.62136) in the subsquare by the new one with rate 0.62138, but this did not improve the $P(5)$ tree significantly (to wit, its rate increased from 0.623326 to 0.623334). For this reason the values in the table for $N \geq 5$ are equal to those found by Smeets.

<table>
<thead>
<tr>
<th>$N$</th>
<th>$v^0(N)$ lower bound</th>
<th>$M(N)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>0.57143 (s)</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>0.59436 (s)</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>0.59259 (s)</td>
<td>4</td>
</tr>
<tr>
<td>5</td>
<td>0.59273 (s)</td>
<td>6</td>
</tr>
<tr>
<td>6</td>
<td>0.60188 (s)</td>
<td>8</td>
</tr>
<tr>
<td>7</td>
<td>0.60989 (s)</td>
<td>16</td>
</tr>
<tr>
<td>8</td>
<td>0.61079 (s)</td>
<td>17</td>
</tr>
<tr>
<td>9</td>
<td>0.61111 (s)</td>
<td>39</td>
</tr>
<tr>
<td>10</td>
<td>0.61154 (s)</td>
<td>57</td>
</tr>
</tbody>
</table>

(3.6.1.6) Table. Lower bounds on $v^0(N)$.

All rates listed in Table (3.6.1.6) were found by Van der Leur [LEU84] in an attempt to construct variable length codes having rates outside $G_4$. Although she did not succeed in this, it is still remarkable that for just 17 messages a zero-error code could be found having rate larger than 0.61. In the table, $M(N)$ is the number of messages of the symmetrical variable length code with maximum block length $N$. For $N = 2$, the entry in the table corresponds to the Hagelbarger code (cf. Section 3.3.4) and for $N = 3$, the optimum code is the one in Figure (3.3.4.1).
Chapter 3

<table>
<thead>
<tr>
<th>( N )</th>
<th>( v^\Delta(N) ) lower bound</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>0.59305 (s)</td>
</tr>
<tr>
<td>3</td>
<td>0.61914 (s)</td>
</tr>
<tr>
<td>4</td>
<td>0.60401 (s)</td>
</tr>
</tbody>
</table>

(3.6.1.7) Table. Lower bounds on \( v^\Delta(N) \).

As with \( f^\Delta(N) \) trees, it is not easy to find good lower bounds for \( v^\Delta(N) \) if \( N \) becomes large. This is mainly because at every vertex of a \( f^\Delta(N) \) tree we are in a kind of dilemma: either we subdivide the vertex directly into rectangles (which usually gives a high rate for that vertex, as in the \( L \)-shape subdivision in Figure (3.3.1.2)) and stop there, or we cut the region into more intricate shapes, postponing the high rate resolutions to levels further from the root.

Because of this we do not list any bounds on \( v^\Delta(N) \) for \( N > 4 \). For \( N = 2 \), our bound is the rate of the tree in Figure (3.6.1.8) with \( t_1 = u_1 = 0.62587 \). This tree may be seen as a Hagelbarger code for two non-equiprobable messages per user.

(3.6.1.8) Figure. \( f^\Delta(2) \) tree for the BMC.

For \( N = 3 \), the bound in Table (3.6.1.7) is the rate of Schalkwijk's \( f^\Delta(3) \)
tree described in [SCH82]. This tree is equal to the tree of Figure (3.6.1.4) (or Figure (3.6.1.15)), without the partitioning of rootlike rectangles (i.e., without the $r^{\Omega}(2)$ tree on the right and the slicing vertices at level 2). The optimum values of the thresholds for the $r^{\Omega}(3)$ tree are (notation as in Figure (3.6.1.4)):

$$t_1 = u_1 = 0.67571 \quad \text{(called } \hat{a} \text{ in [SCH82]),}$$

$$t_2 = u_2 = 0.29770 \quad (= \frac{\hat{a} + \hat{\gamma} - 1}{\hat{a}} \text{ in [SCH82]).}$$

(3.6.1.9) Figure. $r^{\Omega}(4)$ tree for the BMC

The best $r^{\Omega}(4)$ tree that we could find is shown in Figure (3.6.1.9). The subrectangle remaining at level 1 is partitioned according to Schalkwijk's optimum $r^{\Omega}(3)$ tree, and the L-shaped region at level 1 is partitioned as in Figure (3.6.1.8). The optimum values of the parameters are $t_1 = u_1 = 0.60401$.

<table>
<thead>
<tr>
<th>$N$</th>
<th>$v(N)$ lower bound</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>0.61695 (s)</td>
</tr>
<tr>
<td>3</td>
<td>0.62116 (s)</td>
</tr>
<tr>
<td>4</td>
<td>0.62254</td>
</tr>
<tr>
<td>5</td>
<td>0.62448</td>
</tr>
<tr>
<td>6</td>
<td>0.62453</td>
</tr>
<tr>
<td>7</td>
<td>0.62557</td>
</tr>
</tbody>
</table>

(3.6.1.10) Table. Lower bounds on $v(N)$. 

- 105 -
As can be seen from Table (3.6.1.10), the best \( V(2) \) tree does not yield a rate beyond the Shannon inner bound. The optimum \( V(3) \) tree is depicted in Figure (3.6.1.11), with \( t_i = u_i \) for \( i = 1, 2, 3 \), and \( t_1 = 0.67414, \ t_2 = 0.95439, \ t_3 = 0.34667. \)

(3.6.1.11) Figure. \( V(3) \) tree for the BMC.

To find an optimum (or at least a 'good') \( V(4) \) tree, we took the asymmetrical \( F(4) \) tree as found by Smeets, achieving rate 0.62136, and deleted from it the \( F(3) \) tree for the subsquare at level 1. We obtained a tree with rate 0.62233. For the tree with this structure we tried to find the optimum threshold values by computer, but it turned out that the thresholds in Smeets' \( F(4) \) tree are locally optimum also for the \( V(4) \) tree. However, a slight increase in rate did occur by deleting the vertex at level 3 that corresponds to output sequence \( I = (0, 1, 0) \). Once more we optimized the corresponding rate function over the thresholds and
Strategy Trees for TWCs

found rate 0.62254. The threshold values are listed in Table (3.6.1.12) below and the tree itself is shown in Figure (3.6.1.13).

<table>
<thead>
<tr>
<th>i</th>
<th>ti</th>
<th>ui</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0.68476</td>
<td>0.68897</td>
</tr>
<tr>
<td>2</td>
<td>0.74067</td>
<td>0.76191</td>
</tr>
<tr>
<td>3</td>
<td>0.61594</td>
<td>0.60101</td>
</tr>
<tr>
<td>4</td>
<td>0.94928</td>
<td>0.94585</td>
</tr>
<tr>
<td>5</td>
<td>0.35479</td>
<td>0.35354</td>
</tr>
<tr>
<td>6</td>
<td>1.00000</td>
<td>1.00000</td>
</tr>
<tr>
<td>7</td>
<td>0.00000</td>
<td>0.00000</td>
</tr>
<tr>
<td>8</td>
<td>0.91071</td>
<td>0.85421</td>
</tr>
<tr>
<td>9</td>
<td>0.59413</td>
<td>0.62187</td>
</tr>
<tr>
<td>10</td>
<td>0.58915</td>
<td>0.61627</td>
</tr>
<tr>
<td>11</td>
<td>0.62670</td>
<td>0.56490</td>
</tr>
<tr>
<td>12</td>
<td>1.00000</td>
<td>0.63621</td>
</tr>
<tr>
<td>13</td>
<td>0.32648</td>
<td>1.00000</td>
</tr>
<tr>
<td>14</td>
<td>0.35842</td>
<td>1.00000</td>
</tr>
<tr>
<td>15</td>
<td>1.00000</td>
<td>0.00000</td>
</tr>
<tr>
<td>16</td>
<td>0.93740</td>
<td>0.92554</td>
</tr>
<tr>
<td>17</td>
<td>1.00000</td>
<td>1.00000</td>
</tr>
<tr>
<td>18</td>
<td>1.00000</td>
<td>1.00000</td>
</tr>
<tr>
<td>19</td>
<td>0.00000</td>
<td>0.00000</td>
</tr>
<tr>
<td>20</td>
<td>1.00000</td>
<td>1.00000</td>
</tr>
<tr>
<td>21</td>
<td>0.00000</td>
<td>0.00000</td>
</tr>
<tr>
<td>22</td>
<td>0.00000</td>
<td>0.00000</td>
</tr>
<tr>
<td>23</td>
<td>1.00000</td>
<td>1.00000</td>
</tr>
</tbody>
</table>

(3.6.1.12) Table. Threshold values for the tree in Figure (3.6.1.13).

For $N \geq 5$, we can do the same to change the 'optimum' $F(N)$ tree into a good $V(N)$ tree. Because of the numerous possibilities to delete subtrees from such a tree and because of the many thresholds, however, it turns out to be practically impossible to find an optimum $V(N)$ tree in this way. Therefore we just took Smeets' $F(N)$ tree and deleted the $F(N-1)$ tree in the lower right-hand subsquare. Table (3.6.1.10) shows the rates of the $V(N)$ trees thus constructed for $N \geq 5$. 

-- 107 --
(3.6.1.13) Figure. \( f(4) \) tree for the BMC.
<table>
<thead>
<tr>
<th>$N$</th>
<th>$b(N)$ lower bound</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>0.63056 (s)</td>
</tr>
<tr>
<td>3</td>
<td>0.63056 (s)</td>
</tr>
</tbody>
</table>

(3.6.1.14) Table. Lower bounds on $b(N)$.

For $N = 2$, the best bootstrap tree that could be found is Schalkwijk's tree [SCH83a], shown in Figure (3.6.1.15). Both the vertices at level 1 and 2 have the PBV property, but only the middle vertex (at level 1) has type 'invisible'. The threshold values are: $t_1 = u_1 = 0.69070$, $t_2 = u_2 = 0.32059$.

(3.6.1.15) Figure. $b(2)$ tree for the BMC.

For $N = 3$, nothing better could be found than the tree of Figure (3.6.1.15) with the same tree appended to it in the subsquare remaining after the first transmission. Clearly this yields the same rate as the $b(2)$ tree, namely 0.63056. Although Schalkwijk [SCH90] recently found a $b(4)$ tree having a rate exceeding the optimum $b(2)$ rate in the eighth decimal, it still remains an open problem whether or not a tree exists having a rate larger than 0.63056.
Chapter 3

3.6.2. Miscellaneous results

Here we mention some results for TWCs other than the BMC. Trees have been constructed for ternary channels by Van der Heijden [HEI87] and Lormans [LOR88]. All results in this section can be found in these two references. From the 322 classes of ternary TWCs found by Jacobs [JAC86], eleven channels have been studied (not including the BMC, which can also be seen as as ternary TWC). For five of these channels, trees could be constructed that achieved rates outside the Shannon inner bound. Figure (3.6.2.1) lists the partition patterns of these TWCs.

(3.6.2.1) Figure. Partition patterns of the investigated channels.

In Table (3.6.2.2) and (3.6.2.3) we list some achievable rates for each of the five channels. The channels are referred to by the names shown in Figure (3.6.2.1). As before, we only look at the average rate, $(R_0 + R_1)/2$. We define $f(N)$, $v(N)$, et cetera, as in the previous section. In the tables below we give the sharpest lower bounds known for these rate points. Hence e.g. in the column labeled '$f(1)$' we list the highest average rate of all $F(1)$ trees that have been
considered. The meaning of column 'b(a)' is explained in the text below the tables. We also list the Shannon outer bound \( G_0 \), denoting the maximum average rate of any point in \( G_0 \). An '(s)' indicates that the tree is symmetrical (This applies to \( S_{3,3} \), \( S_{5,5}(d) \) and \( S_{10,10}(b) \) only, since they are the only channels equivalent to symmetrical channels.).

<table>
<thead>
<tr>
<th>channel</th>
<th>( f(1) )</th>
<th>( f(2) )</th>
<th>( f(3) )</th>
<th>( G_0 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( S_{3,3} )</td>
<td>0.83483 (s)</td>
<td>0.87576 (s)</td>
<td>0.87523</td>
<td>1.00000</td>
</tr>
<tr>
<td>( S_{5,5}(d) )</td>
<td>0.68207 (s)</td>
<td>0.73176 (s)</td>
<td>0.72430 (s)</td>
<td>0.84956</td>
</tr>
<tr>
<td>( S_{10,10}(b) )</td>
<td>0.91830 (s)</td>
<td>0.93865 (s)</td>
<td>0.93606</td>
<td>1.00000</td>
</tr>
<tr>
<td>( S_{3,7} )</td>
<td>1.02818</td>
<td>1.02818</td>
<td>1.02818</td>
<td>1.09477</td>
</tr>
<tr>
<td>( S_{4,6}(a) )</td>
<td>1.04936</td>
<td>1.04936</td>
<td>1.04936</td>
<td>1.09477</td>
</tr>
</tbody>
</table>

(3.6.2.2) Table. Fixed length tree rates for five channels.

<table>
<thead>
<tr>
<th>channel</th>
<th>( v(2) )</th>
<th>( b(2) )</th>
<th>( b(a) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( S_{3,3} )</td>
<td>0.88495 (s)</td>
<td>0.88547 (s)</td>
<td>0.73881</td>
</tr>
<tr>
<td>( S_{5,5}(d) )</td>
<td></td>
<td></td>
<td>0.94719 (s)</td>
</tr>
<tr>
<td>( S_{10,10}(b) )</td>
<td>1.03323</td>
<td></td>
<td></td>
</tr>
<tr>
<td>( S_{3,7} )</td>
<td>1.05411</td>
<td></td>
<td></td>
</tr>
<tr>
<td>( S_{4,6}(a) )</td>
<td>1.05411</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(3.6.2.3) Table. Variable length and bootstrap tree rates for five channels.

The reason why Table (3.6.2.3) contains only some isolated rates whereas Table (3.6.2.2) is 'full' is the following. Clearly the rate of an \( F(N) \) tree can be calculated by computer, and optimization is done by varying the threshold values. It is far less obvious how good \( V(N) \) or \( B(N) \) trees should be found, since there are many possibilities to prune an \( F(N) \) tree, as mentioned already for the BMC. The
Chapter 3

trees achieving the rates of Table (3.6.2.3) could only be found by looking at the best $F(2)$ or $F(3)$ tree for the given TWC and adjusting this tree a little.

The column name 'b(m)' should be interpreted as follows. Trees achieving rates in this column have been constructed as Markov chains, in the same way as a $B(N)$ tree can be viewed as a Markov chain. For a $B(N)$ tree we have seen that every vertex corresponds to a state in the chain, where the only possible transitions are: either one step down in the tree, or directly back to the root.

\[(3.6.2.4) \text{ Figure. A Markov chain for } S_{10,10}(b).\]

The Markov chains considered here behave differently: here it is possible to return to a vertex higher in the tree that is not equal to the root. For an example of this, see Figure (3.6.2.4), which shows one of the trees from [LOR88] in a schematic form. Such a tree cannot be described by a finite bootstrap tree as
defined in Section 3.4.1. The only way to show that the rate of this Markov chain is achievable is by looking at a $B(N)$ tree for all $N \in \mathbb{N}$, where the $B(N)$ tree shows all sequences of $N$ transitions in the Markov chain starting from the root. The rate of this tree (which is achievable by Theorem (3.4.1.8)) tends to the rate of the Markov chain if $N \to \infty$. For this reason we refer to the Markov chain tree as a $B(\infty)$ tree.

With the trees given in this section we end the chapter on two-way channels. It should be understood that the trees presented here are nothing more than examples; by no means do we claim that the rates given in the tables are optimum. Also, many of the results from Section 3.6 are not new.

The new results are the theorems listed in the beginning of Section 3.5. These show that every TWC tree or code that has been constructed in the past years (i.e., the trees described in this section, among others) belongs to one of the types defined throughout this chapter. The theorems link all of these trees together and show that they can indeed be used to find arbitrarily good lower bounds on the capacity region.
Chapter 4: The Write Unidirectional Memory

4.1. Binary WUM codes

4.1.1. Introduction

Chapter 4 is devoted to a model of a communication situation that is called a 'Write Unidirectional Memory' or WUM, as it is abbreviated. In this section we describe the historical background of this model, which can also be found in [WIL89].

The concept of the WUM is relatively new. It dates back from December 1985, when a question was raised by researchers at Philips Research Laboratories, concerning a magneto-optical recording system. (The reader interested in more technical details of this system is referred to [THO87].) In such a system, binary symbols are stored on an optical disc in the following way. Depending on the symbol ('0' or '1') that has to be written on a specific spot of the disk, a magnetic field with the appropriate orientation is generated via an electromagnet. When heating up the spot on the disc by a laser beam, the material of the disc in this spot is magnetized in the direction of the magnetic field.

The direction of magnetization can be retrieved later when a laser beam is pointed at the spot: the polarization of the reflected light can be used to determine the direction of magnetization in this spot.

Because of inductivity, the polarity of the current through the coil of the electromagnet cannot be reversed too often in a short period of time. Hence fast
switching between writing '0's and '1's is not possible. For this reason it was proposed to keep the direction of the magnetization constant as long as possible (i.e., for the time it takes to record the whole disc) but to write symbols only in specific positions, to be chosen by the writer. In this way we only need to switch the laser on and off in different spots of the disc, but the current does not need to be reversed.

Assume that the disc initially contains only '0's. We set the direction of the current in such a way that '1's can be written. Then information is written on the disc by changing some of the '0's into '1's and by leaving the remaining positions unchanged. For obvious reasons we will call this a '1-cycle'. After writing, the information can be retrieved by a person who receives the disc, if he knows that the disc contained only '0's before writing.

The next time that we want to store information on the disc, we reverse the polarity of the current, such that we can only write '0's. A 0-cycle is performed, in which some of the '1's that were on the disc are changed into '0's. It should be noted that the spots containing '0' after the 1-cycle cannot be changed in the 0-cycle. The receiver of the disc must be able to determine what was written during this cycle, even if he does not know the previous state of the disc. Clearly this is a nontrivial task and some way of coding is needed to ensure transmission with a small (or even zero) probability of error.

The above implies that not every spot of the disc can be used to store a

---

3 This describes the situation of 1985. In the mean time (1989) this problem does not exist anymore: solutions have been found that allow fast switching between '0's and '1's. Among other things, different media have been proposed in which the information is stored by amorphous/crystalline phase changes, that can be created by heat only. Here inductivity does not play a role since this system does not use an electromagnet.
complete bit of information. In other words, the rate of a code (formally defined in Section 4.1.2) will be less than 1 bit/spot. The obvious question was: how high can the rate of a code really be?

Before this question can be answered, we must make more specific assumptions about the situation we are interested in. For instance, we can study the case where the encoder looks at the previous state of the disc before he chooses the spots in which to write a new symbol, but we can also consider the case where he is not allowed to look at the old state of the disc. Similarly we must distinguish between the cases in which the decoder is either informed or uninformed about the old state of the disc. Furthermore we can restrict ourselves to the case where the code has to be the same for every cycle, or to the case where we allow just two codes: one for every 0–cycle and one for every 1–cycle. For each of these cases, models have been developed that are described in the next section.

4.1.2. Definitions

The definitions in this section reflect some information-theoretical aspects of the optical recording system. We present the definitions in such a setting that they can easily be transferred to more general situations, like the one with arbitrarily large alphabets as described in Section 4.2.

(4.1.2.1) Definition. Let $N \in \mathbb{N}$. A (binary) Write Unidirectional Memory or WUM of block length $N$ is a sequence of $N$ cells that can assume values in $\{0,1\}$. The state of the WUM at a time $k \in \mathbb{N}$ is denoted by $s_k$ or $(s_k(0),s_k(1),\ldots,s_k(N-1))$, where $s_k(n)$ is the value of the $n$th cell of the WUM at this time.

(4.1.2.2) Definition. Let $N \in \mathbb{N}$ and $c \in \{0,1\}$. A $c$–filter (cf. [SIM89]) is a vector in $\{c,0\}^N$. Here $c$ is called the type of the filter and $0$ is called a hole. A $c$–filter $\mathbf{g}$
The Write Unidirectional Memory

operates on a state \( s_k \) by changing it into a state \( s_{k+1} \) (denoted as \( s_{k+1} = z \circ s_k \)) according to the following rules.

\[
\begin{align*}
  s_{k+1}(n) &= s_k(n) \text{ if } x(n) = 1 \\
  s_{k+1}(n) &= c \text{ if } x(n) = c, \text{ for all } n \in \{0,1,\ldots,N-1\}.
\end{align*}
\]

We will also use the notation \( s_{k+1}(n) = x(n) \circ s_k(n) \) for the operation of a filter on a single cell of the WUM.

Now we describe the way in which a WUM can be used for communication. We must distinguish between four different cases, depending on whether or not the encoder or decoder knows the state of the WUM before writing, since this knowledge will influence the efficiency with which the WUM can be used. Hence we have four cases, which will be named in the same way as in [SIM89].

**Definition.** We define the following four cases for WUM communication. Here the 'old state' stands for the state of the WUM before writing takes place.

- **Case 1:** both encoder and decoder know the old state of the WUM
- **Case 2:** only the encoder knows the old state of the WUM
- **Case 3:** only the decoder knows the old state of the WUM
- **Case 4:** neither encoder nor decoder knows the old state of the WUM.

Figure (4.1.2.4) depicts the communication situation for all four cases. The dashed lines represent the side information about the old state of the WUM, which is present in some of the cases only. Let \( k \in \mathbb{N} \) and suppose that the WUM has been used \( k-1 \) times (or cycles), starting from state \( s_1 = (0,0,\ldots,0) \), such that the state before the \( k \)th use is \( s_k \). The source generates a message \( \mathcal{V}_k \) from a set \( \mathcal{U}_k := \{0,1,\ldots,U_k-1\} \) for some \( U_k \in \mathbb{N} \). It is assumed that all messages in the set are equally likely.
Chapter 4

[Diagram of communication situation for a WUM]

(4.1.2.4) Figure. Communication situation for a WUM.

The encoder chooses a filter \( f_k \) that will operate on the state \( S_k \) to form a new state, \( S_{k+1} \). This filter can be described by two components: its type, say \( c_k \) (which can be seen as the direction of the current through the electromagnet, in terms of the optical disc) and the set of positions \( n \) where \( I_k(n) = c_k \) (which can be seen as the spots that have to be heated by the laser beam for writing). We denote this set as \( X_k \). In general, the choice of both \( c_k \) and \( X_k \) may depend on \( k \), \( V_k \) and (in cases 1 and 2) on \( S_k \). Because of this, the encoder's choice can be written as either \( (c_k, X_k) = f_k(V_k, S_k) \) or \( (c_k, X_k) = f_k(V_k) \), depending on the case. Here \( f_k \) is a so-called encoding function with either

(4.1.2.5.a) \( f_k: \mathcal{U}_k \times \{0,1\}^N \rightarrow \{0,1\} \times \mathcal{P}(\{0,1, \ldots, N-1\}) \) or

(4.1.2.5.b) \( f_k: \mathcal{U}_k \rightarrow \{0,1\} \times \mathcal{P}(\{0,1, \ldots, N-1\}) \),

where \( \mathcal{P}(\{0,1, \ldots, N-1\}) \) denotes the power set of \( \{0,1, \ldots, N-1\} \).

The decoder takes \( \hat{V}_k := g_k(S_{k+1}, S_k) \) (in cases 1 and 3) or \( \hat{V}_k := g_k(S_{k+1}) \) (in cases 2 and 4) as an estimate for message \( V_k \). If \( \hat{V}_k = '?' \), then a good estimate for the message cannot be found. We call \( g_k \) a decoding function with either

(4.1.2.6.a) \( g_k: \{0,1\}^N \times \{0,1\}^N \rightarrow \mathcal{U}_k \cup {?} \) or

(4.1.2.6.b) \( g_k: \{0,1\}^N \rightarrow \mathcal{U}_k \cup {?} \).

In the most commonly studied situation (cf. [WIL86], [BOR88], [KUZ88], [SIM89]), \( c_k \) does not depend on \( V_k \) and \( S_k \) but only on \( k \). This is indeed a sensible choice, because it allows concatenation to create codes for arbitrarily
large block length. In that case, \( c_k \equiv k \mod 2 \) is taken. From now on we will assume that this relation between \( c_k \) and \( k \) holds. Then we can also define the encoding function \( f_k \) in (4.1.2.5) as

\[
(4.1.2.7.a) \quad f_k : \mathbb{N}_k \times \{0,1\}^N \rightarrow \{c_k, 0\}^N
\]

\[
(4.1.2.7.b) \quad f_k : \mathbb{N}_k \rightarrow \{c_k, 0\}^N,
\]

such that the image of the function is the \( c_k \)-filter \( I_k \) with \( c_k := 0 \) if \( k \) is even and \( c_k := 1 \) if \( k \) is odd. In the sequel we will use (4.1.2.7) rather than (4.1.2.5).

The above model describes one of the most general situations. If the WUM is used an infinite number of times, we theoretically need infinitely many numbers \( N_1, N_2, \ldots \) for the number of messages that can be written per cycle, together with an infinite sequence of encoding and decoding functions: \( f_1, g_1, f_2, g_2, \) et cetera. For practical reasons, however, we will assume that a code has only a finite number of \( N_k \)'s, \( f_k \)'s and \( g_k \)'s. In most papers on WUMs, the number of messages is assumed to be fixed: \( N_k = N \) for all \( k \). Some exceptions to this rule are [OVE88b], [OVE88c] and a concluding remark in [COH88].

If the number of messages is fixed, then it is clear (cf. [SIM89]) that only finitely many different encoding and decoding functions exist, since the number of states of the WUM is finite. This is the motive for the assumption in [WIL89] that a period \( T \) exists, such that \( f_k = f_k \mod T \) and \( g_k = g_k \mod T \). Two extensively studied cases are \( T = 2 \) and \( T = 1 \). If \( T = 2 \), the code is called alternating and if \( T = 1 \), the code is called symmetric. (Note that in the symmetric case, \( f_0 \) and \( f_1 \) cannot really be the same since the ranges of the two functions differ. A more correct way to express the symmetry is that the description of \( f_1 \) can be obtained from the description of \( f_0 \) by reversing the roles of '0' and '1'.)
Chapter 4

We will look at the alternating case, but with two numbers of messages, $N_0$ and $N_1$. It turns out that this type of WUM code is suitable for generalization to larger alphabets. Therefore we arrive at the following set of definitions.

(4.1.2.8) Definition. Let $N \in \mathbb{N}$, $N_c \in \mathbb{N}$ and $\mathcal{N}_c := \{0, 1, \ldots, N_c - 1\}$ for $c \in \{0, 1\}$. A Case 1-WUM code with parameters $(N, N_0, N_1)$ consists of encoding functions $f_c$ and decoding functions $g_c, c \in \{0, 1\}$:

$$f_c: \mathcal{N}_c \times \{0, 1\}^N \rightarrow \{c, \square\}^N,$$
$$g_c: \{0, 1\}^N \rightarrow \{0, 1\}^N \rightarrow \mathcal{N}_c \cup \{?\}.$$

(4.1.2.9) Definition. Let $N \in \mathbb{N}$, $N_c \in \mathbb{N}$ for $c \in \{0, 1\}$. A Case 2-WUM code with parameters $(N, N_0, N_1)$ consists of encoding functions $f_c$ and decoding functions $g_c, c \in \{0, 1\}$:

$$f_c: \mathcal{N}_c \times \{0, 1\}^N \rightarrow \{c, \square\}^N,$$
$$g_c: \{0, 1\}^N \rightarrow \mathcal{N}_c \cup \{?\}.$$

(4.1.2.10) Definition. Let $N \in \mathbb{N}$, $N_c \in \mathbb{N}$ for $c \in \{0, 1\}$. A Case 3-WUM code with parameters $(N, N_0, N_1)$ consists of encoding functions $f_c$ and decoding functions $g_c, c \in \{0, 1\}$:

$$f_c: \mathcal{N}_c \rightarrow \{c, \square\}^N,$$
$$g_c: \{0, 1\}^N \times \{0, 1\}^N \rightarrow \mathcal{N}_c \cup \{?\}.$$

(4.1.2.11) Definition. Let $N \in \mathbb{N}$, $N_c \in \mathbb{N}$ for $c \in \{0, 1\}$. A Case 4-WUM code with parameters $(N, N_0, N_1)$ consists of encoding functions $f_c$ and decoding functions $g_c, c \in \{0, 1\}$:

$$f_c: \mathcal{N}_c \rightarrow \{c, \square\}^N,$$
$$g_c: \{0, 1\}^N \rightarrow \mathcal{N}_c \cup \{?\}.$$

— 120 —
(4.1.2.12) Definition. Consider a WUM code $C$ for any of the four cases defined above. The (average) error probability of $C$, $P_{err}(C)$, is defined by

$$P_{err}(C) := \lim_{K \to \infty} \frac{1}{K} \sum_{k=1}^{K} \Pr\{\hat{V}_k \neq V_k | \text{code } C\}.$$ 

(4.1.2.13) Definition. Consider a WUM code for any of the four cases, with parameters $(N, N_0, N_1)$. The rate pair, $R = (R_0, R_1)$, of the code is defined by

$$R_c := \frac{\log(N_c)}{N}, \ c \in \{0, 1\}.$$ 

(4.1.2.14) Definition. Let $i \in \{1, 2, 3, 4\}$. A pair $(R_0, R_1)$ is achievable for case $i$ if, for all $\varepsilon > 0$ and all large enough $N$, a case $i$–WUM code $C$ with block length $N$ and rate $(R_0, R_1)$ exists such that $R_0 > R_0 - \varepsilon$, $R_1 > R_1 - \varepsilon$ and $P_{err}(C) < \varepsilon$. 

(4.1.2.15) Definition. Let $i \in \{1, 2, 3, 4\}$. The capacity region for case $i$, denoted by $C_i$, is defined as the set of pairs in $\mathbb{R}^2$ that are achievable for case $i$. 

In Section 4.1.3, we summarize some of the results obtained for WUM codes as defined above.

4.1.3. Previous results

Since 1985, many constructions for WUM codes have been found achieving 'high' rates (see the footnote in Section 3.3.1), for all of the models described in Section 4.1.2. The codes were constructed using combinatorial theory. An informationtheoretical approach (i.e., random coding arguments and the concept of typicality) yielded inner bounds to the capacity regions. Conversely, upper bounds to the capacity could be derived using standard informationtheoretical
Chapter 4

techniques. In most cases it could be shown that the bounds yield the actual capacity region.

The first code construction was proposed by the Philips researchers themselves and can be found in e.g. [BOR88]. This code, say $\mathcal{C}$, is a case 4 WUM code with parameters $(N, M_0, M_1) = (1,1,2)$ and rate $(0,1)$. It is defined by

$$
\begin{align*}
&f_0(0) := 0, & g_0(0) := 0, & g_0(1) := 1, \\
&f_1(0) := n, & f_1(1) := 1 & g_1(0) := 0, & g_1(1) := 1.
\end{align*}
$$

It is easy to check that this code has $P_{\text{err}}(\mathcal{C}) = 0$. Indeed, every 0-cycle is used to 'clean' the WUM, such that after a 0-cycle the state is always (0). In the 1-cycles, 1 bit of information can be stored in the WUM by either changing the state to (1) or leaving it unchanged.

Obviously we can form a code with parameters $(N,1,2^N)$ by concatenating $N$ copies of $\mathcal{C}$. This WUM code is a zero-error code, which means that the decoder can always retrieve the message sent, no matter what the message or the previous state is. This proves that $(0,1)$ is an achievable rate for case 4. Since this code can also be used if the encoder or the decoder knows the state of the WUM before writing, we have $(0,1) \in C_i$ for all $i \in \{1,2,3,4\}$.

As in Section (3.6.1), we define the 'average rate' of a code, $R_{\text{av}}$, by

$$
R_{\text{av}} := (R_0 + R_1)/2.
$$

We also define, for $i \in \{1,2,3,4\}$,

$$
(4.1.3.1) \quad C_i := \max \{R_{\text{av}} \mid (R_0,R_1) \in C_i\}
$$

as the maximum average rate achievable by a WUM code for each of the cases.

The above construction shows $C_i \geq 0.5$ for all $i$. However, the achievable rate can be much higher, as is shown in Table (4.1.3.2). This table summarizes
what is known about $C_i$ for all $i$. The column labeled 'constr' gives the highest average rate of any WUM code that has been constructed. It should be noted that the constructed codes are zero-error codes in every case. Further explanation about the codes and the bounds is given below the table.

<table>
<thead>
<tr>
<th>$i$</th>
<th>$C_i$</th>
<th>constr</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0.69424</td>
<td>0.69424</td>
</tr>
<tr>
<td>2</td>
<td>0.69424</td>
<td>0.56371</td>
</tr>
<tr>
<td>3</td>
<td>0.69424</td>
<td>0.52832</td>
</tr>
<tr>
<td>4</td>
<td>0.54589</td>
<td>0.50000</td>
</tr>
</tbody>
</table>

(4.1.3.2) Table. Highest achievable rates for binary case $i$-WUM codes.

The code construction for case 1 is the following (cf. [BOR88]). Let $a < 0.5$ and assume that the state of the WUM before a 0-cycle contains $a \cdot N$ 0's. Both encoder and decoder know the positions of these 0's, which are 'useless' to them since they cannot be changed. Hence they only consider the $(1-a) \cdot N$ positions of the 1's in which information can be stored. Since the encoder knows the effect of each 0-filter on the state, he can make sure that the writing is done in such a way that after the 0-cycle, the state contains $a \cdot N$ 1's. The number of different words that can be written in this way equals $\left\lfloor \frac{(1-a) \cdot N}{a \cdot N} \right\rfloor$.

Clearly the same number of words can be written in each 1-cycle, by leaving $a \cdot N$ of the $(1-a) \cdot N$ 0's unchanged and changing the rest into 1's. By letting $N \to \infty$, it follows that

$$((1-a) h(\frac{a}{1-a}), (1-a) h(\frac{a}{1-a})) \in C_1.$$ 

Thus, by optimization over $a$, we find that $R_{av} = 0.69424$ is achievable for case 1.

The fact that average rates higher than 0.69424 are not achievable was proved by Borden [BOR88] and Simonyi [SIM89], but for zero-error codes only.
Cohen [COH88] gave a proof for the ε-error case. We do not give the proofs here, since generalizations of them are presented in the next sections.

For case 2, it was proved in [BOR88] that rate 0.69424 is achievable with 0-error codes. A random coding argument is needed for this, which is generalized in Section 4.2.3 to codes over larger alphabets. It is clear that higher rates are not achievable, since these are not even achievable in case 1, where the decoder knows the previous state as well. Many code constructions have been presented for this case (which is known as the 'classical' situation because of its origin, the optical recording system). First, Willems and Vinck [WIL86] improved upon the trivial rate 0.5 code with a code achieving rate \( \frac{\log(6)}{5} \approx 0.51699 \). Their result was generalized by Simonyi [SIM89], who found a code with rate \( \frac{\log(58)}{11} \approx 0.53254 \). After this, many ad hoc constructions have been found by several people. At the moment, the highest average rate known is 0.56371 [KOS90].

As in case 2, it is obvious that average rates higher than 0.69424 cannot be achieved in case 3. In [COH88] it was conjectured that the rate could not exceed \( \frac{\log(3)}{3} \approx 0.52832 \). In the same paper, a construction is given of a 0-error code achieving this average rate. In Section 4.2.5 of this thesis we prove that average rate 0.69424 is case 3-achievable, as a corollary of a more general theorem.

For case 4, no constructions have been found that improve upon the trivial code with rate \((0,1)\). Many authors have noticed that a WUM in case 4 resembles a Z-channel under special circumstances (cf. [COH88], [WIL89]). Computing the capacity of this Z-channel gives rate 0.54589. A rigorous proof that this rate is indeed achievable, however, has not yet been published, as far as known by the author. In Section 4.2.6, we will present the proof of the achievability in a more general situation. For symmetrical codes, the converse is proved in [WIL89]. The more general case of alternating codes is treated in Section 4.3.
4.2 WUM codes over arbitrary alphabets

4.2.1. The model

At the 1988 IEEE Information Theory Symposium, the author gave a talk entitled 'Generalized WUM codes' [OVE88c]. The generalization referred to was the one to different numbers of messages in the two cycles. However, this title inspired Kuznetsov [KUZ88b] to contrive a different kind of generalization, namely to an arbitrary alphabet. Instead of writing binary symbols, 0 and 1, we can use an alphabet of size $q$, say $\{0, 1, \ldots, q-1\}$.

In this situation, the state of a WUM with block length $N$ can be any vector in $\{0, 1, \ldots, q-1\}^N$. Again, writing is done in cycles, but now we have $q$ different types of cycles. As before, in a $c$-cycle ($0 \leq c < q$), only $c$'s can be written. Therefore we define the following. Let $q \in \mathbb{N}$, $q \geq 2$ and $\mathcal{A} := \{0, 1, \ldots, q-1\}$ throughout this chapter.

(4.2.1.1) Definition. Let $N \in \mathbb{N}$. A ($q$-ary) WUM with block length $N$ consists of $N$ cells assuming values in $\mathcal{A}$. The state $s_k$ of the WUM before the $k$th use is a vector in $\mathcal{A}^N$, where $s_k(n)$ is the value of the $n$th cell ($0 \leq n < N$). A state $s_k$ is changed into a state $s_{k+1}$ by a $c$-filter ($c \in \mathcal{A}$) as described in Definition (4.1.2.2).

For a binary WUM, we usually omit the word 'binary'. We do the same in the $q$-ary case, since we will always use a fixed $q$, so no confusion is possible. Similarly, the $q$-ary WUM codes defined later will just be called WUM codes.

Again we consider four cases of communication with a WUM. In the $k$th transmission (starting with state $s_1 := (0, 0, \ldots, 0)$), the encoder who wants to send message $v_k$ chooses a $c_k$-filter for some $c_k \in \mathcal{A}$, depending on $v_k$ and possibly on the state $s_k$. The decoder who observes $s_{k+1}$ and possibly $s_k$ makes an
estimate $\hat{V}_k$ for the message sent. For reasons explained before, we will restrict ourselves to the case where the type $c_k$ of the filter chosen by the encoder depends on $k$ only.

The most straightforward generalization of the situation considered in the previous section seems to be $c_k \equiv k \mod q$. This is indeed the choice we will make, but we stress that other choices are conceivable. For instance, we could start with a 0-cycle, then have a 1-cycle, 2-cycle, up to a $(q-1)$-cycle and then go 'down' with a $(q-2)$-cycle followed by a $(q-3)$-cycle, et cetera, and finally a 0-cycle. After this we could go 'up' again. It appears that this and other choices do not allow the computation of capacity regions, whereas for the choice $c_k \equiv k \mod q$, we are able to give quite elegant generalizations of both the results and the proofs mentioned in Section 4.1.3.

For the same reason as above, we restrict ourselves to codes for $q$ different numbers of messages with $q$ different encoding and decoding functions; one for each type of cycle. This gives the most natural and most promising generalization of Definitions (4.1.2.8) through (4.1.2.15). Hence we have the following definition, which is a compressed version of (4.1.2.8) through (4.1.2.11) for alphabet $\mathcal{A}$.

(4.2.1.2) Definition. Let $N \in \mathbb{N}$ and $M_c \in \mathbb{N}$ for $c \in \mathcal{A}$. Define $\mathcal{M}_c := \{0, 1, \ldots, M_c - 1\}$.

For $i \in \{1, 2, 3, 4\}$, a case $i$-WUM code with parameters $(N, \mathcal{M}_0, \mathcal{M}_1, \ldots, \mathcal{M}_{q-1})$ consists of $q$ encoding functions $f_c$ and $q$ decoding functions $g_c$ ($c \in \mathcal{A}$). Here

- $f_c : \mathcal{M}_c \times \mathcal{A}^N \rightarrow \{c, \square\}^N$ for $i = 1$ and $i = 2$, and
- $f_c : \mathcal{M}_c \rightarrow \{c, \square\}$ for $i = 3$ and $i = 4$;
- $g_c : \mathcal{A}^N \times \mathcal{A}^N \rightarrow \mathcal{M}_c \cup \{?\}$ for $i = 1$ and $i = 3$, and
- $g_c : \mathcal{A}^N \rightarrow \mathcal{M}_c \cup \{?\}$ for $i = 2$ and $i = 4$.

The error probability for $q$-ary WUM codes is defined as in Definition
(4.1.2.12) We can also define the rate, achievability and capacity region in this case, where the only difference with Definitions (4.1.2.13), (4.1.2.14) and (4.1.2.15) is the fact that a rate tuple now has \( q \) components instead of 2. This is summarized in the following definition.

(4.2.1.3) Definition. Let \( i \in \{1,2,3,4\} \). A tuple \( (k_0, k_1, \ldots, k_{q-1}) \in \mathbb{R}^q \) is called achievable for case \( i \) if, for all \( \epsilon > 0 \) and large enough \( N \), a case \( i \)-WUM code \( C \) with parameters \( (N, k_0, k_1, \ldots, k_{q-1}) \) exists for which \( P_{\text{err}}(C) < \epsilon \) and \( \bar{R}_C > R - \epsilon \) for all \( c \in \mathcal{A} \), with \( \bar{R}_C := \log(k_c)/N \). \( \bar{R} \) is called the rate of this code. The capacity region for case \( i \), \( C_i \), is the set of case \( i \)-achievable \( q \)-tuples. \( \square \)

4.2.2. Statement of results

Here we state the main results of this chapter: we have found the capacity region for cases 1, 2 and 3. For case 4, a region of achievable rate tuples is given which we conjecture to be the capacity region. In the rest of this chapter, superscripts and subscripts like in \( a_i^{c+1} \) (see Definition (4.2.2.1) below) should be considered mod \( q \). This does not include subscripts (usually called \( k \)) that denote the number of the cycle, as in \( S_{k+1} \).

(4.2.2.1) Definition. We define

\[
\mathcal{Z}_1 := \{ (k_0, k_1, \ldots, k_{q-1}) \in [0,1]^q \mid \forall c \in \mathcal{A} \quad k_c = \sum_{i \in \mathcal{A} \setminus \{c\}} a_i^c \cdot \left( \frac{a_i^{c+1}}{a_i^c} \right),
\]

for some \( a_i^c \geq 0 \) such that \( \sum_{i \in \mathcal{A}} a_i^c = 1 \) for all \( c \) and \( a_i^c \geq a_i^{c+1} \) for all \( i \neq c \). In this formula, \( 0 \cdot h(0/0) \) should be understood as 0. \( \square \)

(4.2.2.2) Theorem. We have \( C_1 = C_2 = co \mathcal{Z}_1 \) (\( 'co' \) denotes the convex hull). \( \square \)
Chapter 4

(4.2.2.3) Definition. We define
\[
\mathcal{K}_3 := \{ (k_0, k_1, \ldots, k_{q-1}) \in [0,1]^q \mid \forall c \in \mathcal{A} \ p_c = h(p_c) \{1 - \frac{p_c \cdot h(p)}{(1-p_c)(1-P)}\},
\]
for some \( p_c \in [0,1] \) and \( P := \prod_{c \in \mathcal{A}} (1-p_c) \}. \]

(4.2.2.4) Theorem. We have \( C_3 = c \mathcal{K}_3 \).

(4.2.2.5) Definition. We define
\[
\mathcal{K}_4 := \{ (k_0, k_1, \ldots, k_{q-1}) \in [0,1]^q \mid \forall c \in \mathcal{A} \ p_c = \frac{p_{c_0} \cdot h(p)}{1-p},
\]
for some \( p_c \in [0,1] \) and \( P := \prod_{c \in \mathcal{A}} (1-p_c) \}. \]

(4.2.2.6) Theorem. We have \( C_4 \supset c \mathcal{K}_4 \).

(4.2.2.7) Conjecture. \( C_4 = c \mathcal{K}_4 \).

The proofs of Theorems (4.2.2.2), (4.2.2.4) and (4.2.2.6) are given in the next sections.

4.2.3. Proof of achievability for case 1 and 2

In this section we prove the 'positive half' of Theorem (4.2.2.2), namely \( c \mathcal{K}_1 \subset C_1 \) and \( c \mathcal{K}_1 \subset C_2 \). First we show that all \( q \)-tuples in \( \mathcal{K}_1 \) are achievable for case 2; by Definition (4.1.2.3), this proves that these tuples are also achievable for case 1. Our proof is a generalization of Borden's random coding proof [BOR88] for the achievability of rate 0.69424 for binary case 2-WUM codes.

Let \( \epsilon > 0 \); let, for \( i \in \mathcal{A} \) and \( c \in \mathcal{A} \), \( a^c_i \in (0,1) \) be such that the \( a^c_i \) satisfy the requirements mentioned in Definition (4.2.2.1). The case \( a^c_i = 0 \) or \( a^c_i = 1 \)
follows by continuity. Let \( N \in \mathbb{N} \). For simplicity, we will consider all numbers \( a_i^c \cdot N \) to be integers, which does not matter if \( N \) is large enough. For \( c \in \mathcal{A} \), let

\[
R_c := \sum_{i \in \mathcal{A} \setminus \{c\}} a_i^c \cdot h\left[ \frac{a_i^{c+1}}{a_i^c} \right], \quad M_c := \left[ 2^{N \cdot (R_c - \varepsilon)} \right] \text{ and } \mathcal{M}_c := \{0, 1, \ldots, M_c - 1\}.
\]

Clearly \( R \in \mathcal{A}_1 \). For \( c \in \mathcal{A} \), consider the set \( \mathcal{T}_c \subset \mathcal{A}^N \) defined as

\[
\mathcal{T}_c := \{ g \in \mathcal{A}^N \mid \forall i \in \mathcal{A} \cdot N(i \cdot g) = a_i^{c+1} \cdot N \}
\]

where \( N(i \cdot g) \) denotes the number of \( i \)'s in \( g \). The cardinality of this set is a multinomial coefficient:

\[
|\mathcal{T}_c| = \frac{N!}{\prod_{i} (a_i^{c+1} \cdot N)!}
\]

We define the vector \( g^* \) as \( (a_0^0 \cdot N)^1 \cdot 1 \cdot (a_1^0 \cdot N)^2 \cdot 2 \cdot (a_2^0 \cdot N)^3 \cdot 3 \cdot \ldots \cdot (a_{q-1}^0 \cdot N)^{q-1} \cdot (q-1) \); that is, a sequence of \( a_0^0 \cdot N \) 0's followed by \( a_1^1 \cdot N \) 1's, et cetera. We have \( g^* \in \mathcal{T}_{q-1} \).

Furthermore we introduce the following concept.

(4.2.3.1) Definition. Let \( g \in \mathcal{A}^N \) and \( c \in \mathcal{A} \). The \textit{c-pattern of} \( g \) is defined as the set of positions where \( g \) has \( 'c' \), so

\[
(c\text{-pattern of} \ g) = \{ n \in \{0, 1, \ldots, N-1\} \mid s(n) = c \}.
\]

We partition the set \( \mathcal{T}_c \) into equivalence classes in such a way that a class contains all words that have the same \textit{c-pattern}. Now we want to assign a label from \( \mathcal{M}_c \) to every word in \( \mathcal{T}_c \) in such a way that words with the same \textit{c-pattern} obtain the same label. We do this by randomly assigning labels from \( \mathcal{M}_c \) to each equivalence class; all labels of classes are chosen independently and the labels are equiprobable. Now each word in \( \mathcal{T}_c \) gets the label of the equivalence class it belongs to. In this way, the words in all \( q \) sets \( \mathcal{T}_c \ (c \in \mathcal{A}) \) are labeled.
Chapter 4

Given the labeling, we define the following case 2—WUM code \( C \) with parameters \( (N, N_0, N_1, \ldots, N_{q-1}) \). Let \( c \in A \) and \( i \in A_c \). Encoding function \( f_c \) maps message \( w_k = i \) and state \( s_k \) into a \( c \)-filter \( s_k^c \in \{c, \emptyset\}^N \) such that the new state \( s_{k+1} = (s_k^c \circ s_k^c) \) is a word in \( T_c \) having label \( i \). If such a \( c \)-filter does not exist, we take the \( c \)-filter having \( c \)'s in the positions of the \( c \)-pattern of \( s^* \). The decoding function \( g_c \) maps the state \( s_{k+1} \) to its label in \( T_c \) if \( s_{k+1} \in T_c \); if \( s_{k+1} \notin T_c \), then \( g_c(s_{k+1}) := \text{'?'}. \)

After the first \( q-1 \) uses of this WUM code, the state \( s_q \) of the WUM is an element of \( T_{q-1} \). This is seen as follows. The initial state is \( s_1 = 0^N \). If \( q = 2 \), \( s_1 \) can be changed into every word in \( T_1 \) in the first cycle (a 1—cycle). For \( q > 2 \), it is impossible to change \( s_1 \) into a word in \( T_1 \) in the first transmission, since words in \( T_1 \) contain all \( q \) symbols at least once, for large enough \( N \). Hence \( s_2 \) consists of 0's and 1's only and the 1-pattern of \( s_2 \) equals the 1-pattern of \( s^* \). In the next cycle it is again impossible to change the state into a word in \( T_2 \), if \( q > 3 \), so both the 1-pattern and the 2-pattern of \( s_3 \) and \( s^* \) are equal. Continuing in this way, we find

\[
s_{q-1} = (a_0^0 \cdot N)_{(q-1)} (a_1^0 \cdot N)_{(q-2)} (a_2^0 \cdot N)_{(q-3)} \cdots (a_{q-2}^0 \cdot N)_{(q-3)} (a_{q-1}^0 \cdot N)_{(q-2)}
\]

In the \( (q-1) \)th transmission, this can be changed to a word in \( T_{q-1} \) (possibly \( s^* \)).

Now we look at all uses of the WUM beyond the first \( q-1 \). We will show that at least one of the WUM codes corresponding to the random labeling has the property that \( w_k = \hat{w}_k \) for all \( k \geq q \). A code having this property will be called \textit{eventually error—free}. Although the word 'eventually' suggests that errors may occur in any finite set of initial transmissions, we will only consider the case where errors are confined to the first \( q \) transmissions.

An eventually error—free code \( C \) has \( P_{\text{err}}(C) = 0 \), since
We will compute the probability that the random labeling does not correspond to an eventually error-free WUM code $\mathcal{C}$. Suppose $\mathcal{C}$ is not eventually error-free and consider a sequence of transmissions in which the decoder makes an error for some $k \geq q$. Let $k \geq q$ be smallest index such that $w_k \neq \hat{w}_k$ and let $c \in \mathcal{A}$ satisfy $k \equiv c \mod q$. Since $k$ is the first time (after the initial $q-1$ transmissions) that an error occurs, we have $s_k \in T_{c-1}$. This follows from the code definition. Now $w_k \neq \hat{w}_k$ implies that the encoder could not find a $c$-filter changing $s_k$ into a word in $T_c$ having the right label. Hence the labeling is such that for some $s \in T_{c-1}$ and some $i \in \mathcal{M}$, no word $s' \in T_c$ with label $i$ can be found such that $s$ can be updated to $s'$ in a $c$-cycle.

For fixed $c$ and $s \in T_{c-1}$, the number of words $s'$ in $T_c$ to which $s$ can be updated by a $c$-filter equals $A_c$, where

$$A_c := \prod_{i \neq c} \left[ \frac{a_i^c}{a_i^{c+1}} \right] N \cdot N_c$$

Since all of these words $s'$ have different $c$-patterns, their labels were chosen independently during the code construction. Hence the probability that none of the words $s'$ has label $i$ equals $p_c$, where

$$p_c := \left[ \frac{N_{c-1}}{N_c} \right] A_c$$

which is independent of $s$ and $i$. By the union bound, the total probability that
the randomly constructed code is not eventually error-free can be bounded by

\[ Pr\{ C \text{ is not eventually error-free} \} \]

\[ \leq \sum_{c \in A} \sum_{\Delta \in \mathcal{C}_{c-1}} \frac{\sum_{i \in \mathcal{C}_c} P_c}{\sum_{i \in \mathcal{C}_c} A_c} \]

\[ = \sum_{c \in A} \mathcal{T}_{c-1} \cdot \mathcal{M}_c \cdot \left( \frac{\mathcal{M}_c - 1}{\mathcal{M}_c} \right)^{A_c} \]

As in [BOR88], we have

\[ |\mathcal{T}_{c-1} \cdot \mathcal{M}_c \cdot \left( \frac{\mathcal{M}_c - 1}{\mathcal{M}_c} \right)^{A_c} = |\mathcal{T}_{c-1} \cdot \mathcal{M}_c \cdot \left( \frac{\mathcal{M}_c - 1}{\mathcal{M}_c} \right)^{A_c} | \log(1 - 1/\mathcal{M}_c) \]

This is true because \( \ln(1 - z) \leq -z \) for \( z \geq 0 \), so \( \log(1 - z) \leq -z/\ln(2) \). We have

\[ |\mathcal{T}_{c-1} \cdot \mathcal{M}_c \cdot \left( \frac{\mathcal{M}_c - 1}{\mathcal{M}_c} \right)^{A_c} | \log(1 - 1/\mathcal{M}_c) \]

\[ = \frac{N!}{\Pi(a_i \cdot N)} \cdot \left[ 2^{\mathcal{N}(\mathcal{M}_c - \epsilon)} \cdot \left( \frac{A_c}{\ln(2) \cdot \mathcal{M}_c} \right) \right]. \]

Applying Stirling's formula, we find that this is

\[ \frac{N \cdot \log(N) - \sum_i (a_i \cdot N) \log(a_i \cdot N) + N(\ln(N) - \mathcal{A}_c/(\ln(2) \cdot [2^{\mathcal{N}(\mathcal{M}_c - \epsilon)}])) + 0(\log(N))}{N} \rightarrow \infty. \]

Because

\[ A_c = 2^{(N \cdot \mathcal{M}_c - o(N))}, \quad N \rightarrow \infty, \]

the expression can be simplified to

\[ 2^{\left( \frac{-2N\epsilon - o(N)}{\ln(2)} + 0(N \cdot \log(N)) \right)}, \quad N \rightarrow \infty. \]

Therefore \( Pr\{ C \text{ is not eventually error-free} \} \) can be bounded as

\[ Pr\{ C \text{ is not eventually error-free} \} \]

- 132 -
Consequently, with probability tending to 1, the random construction yields an eventually error-free case 2-WUM code if $N \to \infty$. This code has $P_{\text{err}}(C) = 0$ and rate approximating $R$ if the block length is large enough. This proves the case 2- (and case 1-) achievability of all points in $Z_1$.

By concatenating (or time sharing) codes with different rate points in $Z_1$, we find that $co Z_1$ is included in the capacity regions $C_1$ and $C_2$.

**4.2.4. Converse for case 1 and 2**

Now we show that for a case 1-WUM code with error probability tending to zero, the rate tuple approximates a point in $co Z_1$. Together with the proof in Section 4.2.3, this proves Theorem (4.2.2.2). Our proof generalizes Willems’ proof [WIL89] for the binary equal rate case.

Let $\varepsilon > 0$, $N \in \mathbb{N}$. Consider a case 1-WUM code $C$ with block length $N$, $P_{\text{err}}(C) < \varepsilon$ and rate $(R_0, R_1, \ldots, R_{q-1}) = (\log(N_0)/N, \ldots, \log(N_{q-1})/N)$. Consider a long sequence of transmissions. Let $c \in \mathcal{A}$ and $k = c \mod q$. Then

$$
\log(N_c) = H(\hat{V}_k) = \{\text{since } \hat{V}_k \text{ and } \hat{S}_k \text{ are independent}\}
= H(\hat{V}_k | \hat{S}_k)
= I(\hat{V}_k; \hat{V}_k | \hat{S}_k) + H(\hat{V}_k | \hat{V}_k, \hat{S}_k).
$$

So

$$
(4.2.4.1) \quad \log(N_c) = I(\hat{V}_k; \hat{V}_k | \hat{S}_k) + H(\hat{V}_k | \hat{V}_k, \hat{S}_k).
$$

For the first term on the right-hand side of (4.2.4.1), we have

$$
I(\hat{V}_k; \hat{V}_k | \hat{S}_k) \leq H(\hat{V}_k | \hat{S}_k)
\leq H(\hat{V}_k | \hat{S}_{k+1}, \hat{S}_k)
= H(\hat{S}_{k+1} | \hat{S}_k) \quad \{\text{since } \hat{V}_k = g_c(\hat{S}_{k+1}, \hat{S}_k)\}
$$
Chapter 4

\[ N - 1 \leq \sum_{n=0}^{N-1} H(S_{k+1}(n) | S_k) \leq H(S_{k+1}(n) | S_k(n)). \]

For all \( n, k \) and \( i \), we define

\[ I_k(n) := H(S_{k+1}(n) | S_k(n)) \quad \text{and} \quad \beta_k^i(n) := Pr\{S_k(n) = i\}. \]

Then, since \( S_{k+1}(n) = I_k(n) \circ S_k(n) \),

\[ Pr\{S_{k+1}(n) = j, S_k(n) = i\} = \begin{cases} 
\beta_{k+1}^i(n) & \text{if } i \neq c, i = j, \\
\beta_k^i(n) & \text{if } i = j = c, \\
\beta_k^i(n) - \beta_{k+1}^i(n) & \text{if } i \neq c, j = c, \\
0 & \text{otherwise.} 
\end{cases} \]

Therefore

\[ I_k(n) = H(S_{k+1}(n) | S_k(n)) = \sum_{i \neq k} \beta_k^i(n) \cdot h\left( \frac{\beta_{k+1}^i(n)}{\beta_k^i(n)} \right). \]

The numbers \( \beta_k^i(n) \) can be computed for large \( k \) if we know the asymptotic distribution of \( S_k \). We can describe this distribution by a Markov chain with \( q \cdot q^N \) states, labeled \((c, s)\) for \( c \in A \) and \( 0 \leq s \leq q^N - 1 \). For fixed \( c \), the states \((c, s)\) correspond to all possible values of \( S_k \) (i.e., all elements of \( A^N \)) if \( k = c \mod q \). The transition probabilities are given by the distribution of \( I_k \) conditional to \( S_k \): the probability of going from a state \((c, s)\) to a state \((c+1, s')\) is equal to the probability that a \( c \)-filter \( I_k = f_c(\psi_k, S_k) \) was chosen transforming \( S_k \), the WUM state corresponding to \((c, s)\), into \( S_{k+1} \) (corresponding to \((c+1, s')\)). Clearly this Markov chain models the statistical behavior of \( S_k \) because of the periodicity of
the cycles in the WUM code.

It follows from the definition of the code that the chain is irreducible (every state can be reached from every other state) if we consider only those states that can be reached at all. Hence by [FEL70, Ch. XV, Section 9] a unique stationary distribution over the states exists, which can be computed from the transition probabilities given by the code. If we consider the \( n \)th cell of the state \( S_k \) only, the following definition is valid.

\[
\alpha_{i}^{c}(n) := \lim_{t \to \infty} P \{ S_{i}^{t q + c}(n) = i \} = \lim_{t \to \infty} \beta_{i}^{t q + c}(n), \text{ for } c \in A, i \in A.
\]

The numbers \( \alpha_{i}^{c}(n) \) for fixed \( n \) satisfy the requirements mentioned in Definition (4.2.2.1). This is true because for any finite \( k \) (by the definition of \( \beta_{c}^{k}(n) \) and because of the way a \( c \)-filter operates)

\[
\sum_{i} \beta_{i}^{k}(n) = 1 \text{ and } \beta_{i}^{k}(n) \leq \beta_{i}^{k+1}(n) \text{ if } i \neq k.
\]

Hence we find the same relations for the limits \( \alpha_{i}^{c}(n) \). Now, if \( k \) is sufficiently large and \( k \equiv c \mod q \), (4.2.4.2) yields

\[
I_{c}(n) \leq \sum_{i \neq c} \alpha_{i}^{c}(n) \cdot h\left( \frac{\alpha_{i}^{c+1}(n)}{\alpha_{i}^{c}(n)} \right) + \varepsilon.
\]

Since this upper bound only depends on \( c \) and not on \( k \), we can define

\begin{equation}
(4.2.4.3) \quad I_{c}(n) := \sum_{i \neq c} \alpha_{i}^{c}(n) \cdot h\left( \frac{\alpha_{i}^{c+1}(n)}{\alpha_{i}^{c}(n)} \right)
\end{equation}

which yields

\begin{equation}
(4.2.4.4) \quad I(\tilde{V}_{k}; V_{k} \mid S_{k}) \leq \sum_{n=0}^{N-1} I_{c}(n) + N \cdot \varepsilon.
\end{equation}

Now consider the second term on the right-hand side of (4.2.4.1). By Definition (4.1.2.12), for all \( k \in \mathbb{N} \), a \( k > k \) with \( k \equiv c \mod q \) exists such that
Chapter 4

\[ \Pr\{ \tilde{V}_k \neq \hat{V}_k | \text{code } C \} < q \varepsilon. \]

For such a \( k \), we have by Fano's theorem (cf. [GAL68, Theorem 4.3.1]):

\[ H(V_k | \tilde{V}_k, S_k) \leq H(V_k | \hat{V}_k) \leq h(q \varepsilon) + q \varepsilon \log(N_c) =: \varphi(\varepsilon) \]

with \( \varphi(\varepsilon)/N \to 0 \) if \( \varepsilon \to 0 \), for constant \( N_c \). Hence, combining this with (4.2.4.1) and (4.2.4.4) we find: for all \( c \in \Lambda \) a \( k \in \mathbb{N} \) exists with \( k \equiv c \mod q \) such that

\[ R_c = \log(N_c)/N \leq \sum_{n=0}^{N-1} R_c(n)/N + \varepsilon + \varphi(\varepsilon)/N \]

for arbitrary \( \delta > 0 \), if \( \varepsilon \) is small enough.

For the rate of the code, \( \underline{R} = (R_0, R_1, \ldots, R_{q-1}) \), this yields:

\[ \underline{R} \leq \sum_{n=0}^{N-1} \underline{R}(n)/N + (\delta, \delta, \ldots, \delta), \]

where '≤' denotes that the inequality '≤' holds componentwise, and \( \underline{R}(n) = (R_0(n), R_1(n), \ldots, R_{q-1}(n)) \) is an element of \( \mathcal{R}_1 \), by (4.2.4.3). Therefore

\[ \sum_{n=0}^{N-1} \underline{R}(n)/N \in \text{co } \mathcal{R}_1. \]

Hence \( \underline{R} \) approximates \( \text{co } \mathcal{R}_1 \) arbitrarily closely if \( \varepsilon \downarrow 0 \). This concludes the converse part of the proof of Theorem (4.2.2.2).

4.2.5. Proof for case 3

The proof of Theorem (4.2.2.4) is split into an achievability part and a converse part, like the proof of Theorem (4.2.2.2). We start with the proof of the case 3—achievability of all rates in \( \text{co } \mathcal{R}_3 \). This proof is based on an unpublished result by Willems for case 4—achievability in the symmetrical case for \( q = 2 \), in which block Markov encoding (described in [COV81]) is used. We present a simplified version of this.
Let \( 0 < \epsilon < 1 \). For \( c \in A \), we fix numbers \( p_c \in (0,1) \). Define

\[
(4.2.5.1) \quad P := \prod_{c \in A} (1-p_c) \quad \text{and} \quad R_c := h(p_c) \{(1 - \frac{p_c \cdot p}{(1-p_c)(1-P)}) \}.
\]

Let \( N \in \mathbb{N} \) be large. As before, we assume that \( p_c \cdot N \) is an integer for all \( c \). We will consider an ensemble of possible case 3-WUM codes having a rate tuple, \( \tilde{R} \), that is approximately equal to the desired rate tuple: \( \tilde{R}_c \approx R_c \) for all \( c \). We show that the average error probability over this ensemble tends to 0 with increasing block length. This will imply the existence of a 'good' code achieving rate \( \tilde{R} \).

In order to be able to compute the probability of error, we construct each code in the ensemble in such a way that the distribution of the states (in a Markov chain, as in Section 4.2.4) is more or less 'uniform'. We will explain later what we mean by this. To this aim, all codewords in the ensemble will be partitioned into blocks of length \( N \) that have a fixed number of \( c \)'s and \( \bar{c} \)'s. The writing will be such that at each time instant, every \( N \)-block of this form is equally likely to be written.

For large enough \( N \) and \( c \in A \), let \( N_0(c) \) and \( N_1(c) \) be integers such that

\[
(4.2.5.2) \quad N_0(c), N_1(c) = \left\lfloor \frac{N}{p_c \cdot N} \right\rfloor,
\]

\[
\frac{N}{2} \left[ h(p_c) \cdot \frac{p_c \cdot p}{(1-p_c)(1-P)} + \epsilon/4 \right] \leq N_0(c) \leq 2 \left[ h(p_c) \cdot \frac{p_c \cdot p}{(1-p_c)(1-P)} + \epsilon \right],
\]

\[
\frac{N(R_c - \epsilon/2)}{2} \leq N_1(c) \leq N(R_c - \epsilon/3).
\]

It can be seen as follows that this is possible. Firstly,
Chapter 4

\[ \begin{aligned} 
\left[ \frac{N}{p_c N} \right] &= 2^{N(h(p_c) + o(1))} (N \to \infty), \text{ and } h(p_c) = h(p_c) \cdot \frac{p_c \cdot P}{(1-p_c) (1-P)} + R_c. 
\end{aligned} \]

Furthermore, \( \left[ \frac{N}{p_c N} \right] \) has a divisor between \( d \) and \( N \cdot d \) for all \( d \in \{1, 2, \ldots, \left[ \frac{N}{p_c N} \right] \} \) (consider an ordered list of all divisors of \( \left[ \frac{N}{p_c N} \right] \); two consecutive divisors in the list differ by a factor of at most \( N \), since the expansion of \( \left[ \frac{N}{p_c N} \right] \) consists of divisors that are less than or equal to \( N \)). Hence \( \mathcal{W}_1(c) \) has a divisor that differs at most by a factor \( N \) from \( \left[ 2^N (2^{c} - \varepsilon/2) \right] \). For large \( N \), this number lies in the interval specified by the above inequalities. The quotient \( \left[ \frac{N}{p_c N} \right] / \mathcal{W}_1(c) =: \mathcal{W}_0(c) \) satisfies the other inequalities if \( N \) is large enough.

For fixed \( c \), let \( \mathcal{S}^c \) denote the set of all \( c \)-filters of length \( N \) that contain \( p_c N \) times \( 'c' \) and \( (1-p_c) N \) times \( '\circ' \). Since \( |\mathcal{S}^c| = \left[ \frac{N}{p_c N} \right] \), the set \( \mathcal{S}^c \) can be partitioned into \( \mathcal{W}_1(c) \) subsets each containing \( \mathcal{W}_1(c) \) words. We call these subsets \( \mathcal{C}^c \), \( 0 \leq i \leq \mathcal{W}_0(c) - 1 \). The words in \( \mathcal{C}^c \) are ordered:

\[ \mathcal{C}^c = \{ E(c, i, 0), E(c, i, 1), \ldots, E(c, i, \mathcal{W}_1(c) - 1) \}. \]

Every case 3–WUM code in our ensemble will correspond to some choice of the ordered partitionings of \( \mathcal{S}^0, \mathcal{S}^1, \ldots, \mathcal{S}^{q-1} \). Consider a fixed choice of partitionings, that can be denoted as \( \{ \mathcal{C}^c \}, c \in A, 0 \leq i \leq \mathcal{W}_0(c) - 1 \). The WUM code, say \( \mathcal{C} \), that corresponds to this choice is the following.

Let \( T := [\log(N)] \). The code \( \mathcal{C} \) will have parameters \( (\bar{N}, \bar{N}_0, \ldots, \bar{N}_{q-1}) \) with

\[ \bar{N} := T \cdot N + \sum_{i \in A} [\log(W^c_0(i))], \]

\[ \bar{N}_c := W_0^c \cdot (W_1^c)^T \text{ for all } c. \]

The rate of the code, \( \bar{R} = (\bar{R}_0, \bar{R}_1, \ldots, \bar{R}_{q-1}) \), has
The Write Unidirectional Memory

\[ \tilde{R}_c = \frac{\log(N^0(c)) + T \cdot \log(N^1(c))}{\sum_{i \in \mathcal{A}} \left[ \log(N^0(i)) \right] + TN} \geq \frac{0(N) + [\log(N)] \cdot N(R_c - \varepsilon/2)}{0(N) + [\log(N)] \cdot N} \]

Hence, if \( N \) is large enough:

\[ \tilde{R}_c \geq R_c - \varepsilon. \]

Let \( c \in \mathcal{A} \) and \( k \equiv c \mod q \). The encoding function \( f_c \) is described as follows.

Suppose the encoder wants to send message \( w_k \in \{0,1,\ldots,\tilde{R}_c-1\} \). This message is written as

\[ w_k = w_{k,0} + w_{k,1}N^0(c) + w_{k,2}N^1(c) + \ldots + w_{k,T}N^1(c)T^{-1} \]

with \( 0 \leq w_{k,0} < N^0(c) \) and \( 0 \leq w_{k,t} < N^1(c) \) for \( t = 1,2,\ldots,T \). The number \( w_{k,0} \) is encoded using a trivial time sharing code: the information is written in \( \lfloor \log(N^0(c)) \rfloor \) prescribed positions where \( s_k \) had \( 'c-1' \) (hence the decoder can uniquely determine the positions in which \( c \)'s are written), and the remaining \( \sum_{i \neq c} \lfloor \log(N^0(i)) \rfloor \) positions of the first block of the codeword are filled with \( c \)'s.

Now the set \( \mathcal{C}(c)_{w_{k,0}} \) is used to encode the numbers \( w_{k,t} \) for \( t \geq 1 \): \( w_{k,t} \) will be encoded by a block of length \( N \), namely \( \mathcal{E}(c,w_{k,0},w_{k,t}) \in \mathcal{C}(c)_{w_{k,0}} \). We have \( T \) of these blocks. Let the state \( s_k \) be partitioned according to these blocks:

\[ s_k = (s_{k,0},s_{k,1},\ldots,s_{k,T}), \]

where \( s_{k,0} \) has length \( \sum_{i \in \mathcal{A}} \lfloor \log(N^0(i)) \rfloor \) and \( s_{k,t} \) for \( t \geq 1 \) has length \( N \).

The decoding functions \( g_c \) are the same for all codes in the ensemble. Let \( \delta > 0; \delta \) will be specified later, and it will only depend on \( p_0,p_1,\ldots,p_{q-1} \) and \( \varepsilon \).

For the decoder, \( s_{k+1,0} \) and \( s_{k,0} \) uniquely determine the index \( w_{k,0} \) of the set \( \mathcal{C}(c)_{w_{k,0}} \) with which the remaining (and largest) part of the message was encoded.

Each block \( s_{k+1,t} \) for \( t \geq 1 \) is decoded as follows. The decoder takes \( \hat{w}_{k,t} = \) the
unique $w \in \{0, 1, \ldots, \binom{q}{c} - 1\}$ such that the triple $(z(c, w_k, c, 0, w), s_k, t, s_{k+1}, t)$ is jointly $\delta$-typical (see Definition (4.2.5.4) below). If such a $w$ does not exist, then he decodes $\tilde{w}_k := g_c(s_k, s_{k+1}) := \tilde{w}_k$. If not $\tilde{w}_k = \tilde{w}_k$, then $\tilde{w}_k$ is computed via the $\tilde{w}_k, t$ in a way similar to (4.2.5.3).

(4.2.5.4) Definition. Let $\delta > 0$. A state $s = s_k, t$, for $k \equiv c \mod q$, is $\delta$-typical (or just typical, if no confusion about $\delta$ is possible) if

$$\forall i \in \mathcal{A} \left[ |N(i, s) - N \cdot a_i^c| \leq N\delta \right],$$

where the $a_i^c$ satisfy (4.2.5.5):

$$\begin{cases}
    \sum_{i \in \mathcal{A}} a_i^c = 1, \\
    a_i^{c+1} = a_i^c(1 - p_c) \quad \text{for } i \neq c, \\
    a_c^{c+1} = a_c^c + p_c(1 - a_c^c).
\end{cases}$$

(The complete solution of (4.2.5.5) is given in Appendix A of this chapter; for now, it is only important to know that the $a_i^c$ can be expressed in the $p_c$ in a unique way.)

For a word $z \in S^c$ and states $s_k, t$ and $s_{k+1}, t$, we say that $(z, s_k, t, s_{k+1}, t)$ is jointly ($\delta$-)typical (or just j.t.) if both $s_k, t$ and $s_{k+1}, t$ are $\delta$-typical and $s_{k+1}, t = z \circ s_k, t$ holds.

Now that we have defined the code ensemble, we will prove that the average error probability over the ensemble tends to zero if the block length $\bar{N}$ tends to infinity. In this proof we use that a state $s_k$ is $\delta$-typical with probability tending to 1, which will be proved in Appendix A. Let $\bar{p}_{\text{err}}$ be the error probability over the ensemble of codes:
The Write Unidirectional Memory

\[ P_{\text{err}} = \sum_{A \in C} Pr\{C = A\} \cdot P_{\text{err}}(A). \]

Here \( C \) is the ensemble of codes and \( C \) is a random variable denoting the choice of code, where \( Pr\{C = A\} = 1/|C| \) for all codes \( A \) in the ensemble \( C \). We write \( C = \{\mathcal{C}_1(c)\} \), which denotes the partitioning of the sets \( \mathcal{S}^c \) corresponding to \( C \). By Definition (4.1.2.12) and changing the order of summation, we obtain

\[ \lim_{K \to \infty} \frac{1}{K} \sum_{k = 1}^{K} \sum_{A \in C} Pr\{\hat{V}_k \neq V_k \text{ and } C = A\}. \]

Let \( k \equiv c \mod q \). Since the first block, \( S_{k+1,0} \), can always be decoded correctly, we find

\[ \sum_{A \in C} Pr\{\hat{V}_k \neq V_k \text{ and } C = A\} \]

\[ \leq \sum_{A \in C} \sum_{t = 1}^{T} Pr\{\hat{V}_k, t \neq V_k, t \text{ and } C = A\} \]

\[ = T \sum_{A^* \in C^*} Pr\{\hat{V}_k, 1 \neq V_k, 1 \text{ and } \mathcal{C}_0(c) = A^*\}. \]

In (\#), we have assumed (without loss of generality) that \( w_{k,0} = 0 \). The set \( C^* \)
contains all ordered sets \( \mathcal{C}_0(c) = \{\mathfrak{z}(c,0,0), \mathfrak{z}(c,0,1), \ldots, \mathfrak{z}(c,0,M_1(c)-1)\} \)
where the \( \mathfrak{z}(c,0,i) \) are distinct elements of \( \mathcal{S}^c \). Now we may also assume
\( w_{k,1} = 0 \). Let \( C^* \setminus \{z\} \) denote the set of all possible \( \mathcal{C}_0(c) \) that have \( \mathfrak{z}(c,0,0) = z \), and let \( C^\prime \) denote \( \mathcal{C}_0(c) \setminus \{\mathfrak{z}(c,0,0)\} \). Then

\[ \sum_{A^* \in C^*} Pr\{\hat{V}_k, 1 \neq V_k, 1 \text{ and } \mathcal{C}_0(c) = A^*\} \]

\[ = \sum_{z \in \mathcal{S}^c, A^* \in C^* \setminus \{z\}, z, z'} Pr\{C = A^*, z(c,0,0) = z, S_{k,1} = z, S_{k+1,1} = z', \hat{V}_k, 1 \neq 0\}. \]
Let $z$, $z'$ and $s$ be such that $s' = z \circ s$. By Definition (4.2.5.4), if $s$ and $s'$ are typical, then also $(z, s, s')$ is j.t. Therefore $v_{k, 1} \neq 0$ can only occur either if $s$ or $s'$ is not typical, or if a different codeword $y \in C'$ exists for which $(y, z, s')$ is jointly typical. Hence we can bound the above sum as

\begin{equation}
\sum_{s: \text{not typical}} \Pr\{S_{k, 1} = s\} + \sum_{s': \text{not typical}} \Pr\{S_{k+1, 1} = s'\} + \sum_{z \in S^c, A' \in C^* \setminus \{z\}, z} \Pr\{C' = A', z(c, 0, 0) = z, S_{k, 1} = s, S_{k+1, 1} = s'\} \cdot \phi(3_{y \in A}, [(y, z, s') \text{ j.t.}]).
\end{equation}

We write (4.2.5.7) as $P_0 + P_1 + P_2$. In Appendix A it is shown that

\begin{align*}
\Pr\{S_{k, 1} \text{ not typical}\} &= \frac{1}{\delta^3} O(1/N) \quad \text{and} \\
\Pr\{S_{k+1, 1} \text{ not typical}\} &= \frac{1}{\delta^3} O(1/N), \quad N \to \infty
\end{align*}

if $k$ is large enough, say $k \geq \llbracket N \rrbracket$ for some $\llbracket N \rrbracket$ dependent of $p_0, p_1, \ldots, p_{q-1}, \delta$ and $N$. Since $T = \lceil \log(N) \rceil$, we have for large enough $N$:

\begin{equation}
T \cdot P_0 = T \cdot \sum_{s: \text{not typical}} \Pr\{S_{k, 1} = s\} \leq \varepsilon/3
\end{equation}

and similarly $T \cdot P_1 \leq \varepsilon/3$. We can bound $P_2$ by

\begin{equation}
P_2 \leq \sum_{z \in S^c, s \text{ and } s' \text{ typical}} \Pr\{z(c, 0, 0) = z, S_{k, 1} = s, S_{k+1, 1} = s'\} \cdot \sum_{A' \in C^* \setminus \{z\}} \Pr\{C' = A'\} \cdot \sum_{y \in S^c} \phi(3_{y \in A}, [(y, z, s') \text{ j.t.}]).
\end{equation}

Consider fixed typical $s$ and $s'$. Every $y$ that is j.t. with $(s, s')$ is contained in
ordered sets \( A' \) (apart from \( z \) and \( y \) there are \( N(c)-2 \) other words in \( \mathcal{C}_0(c) \) that can be chosen from \( \mathcal{S}^c \)). The total number of ordered sets \( A' \) is

\[
\left[ \frac{N(c) N(c)-1}{N(c)-2} \right] \cdot (N(c)-1)!.
\]

Therefore, for any \( z, z' \) and \( \mathcal{A}' \),

\[
\sum_{A' \in \mathcal{C}^n \setminus \{z\}} P_{r}(C' = A') \cdot \sum_{y \in \mathcal{S}^c} \phi(y \in A' \text{ and } (y, z, z') \text{ j.t.})
\]

\[
\leq \frac{1}{N(c)} \cdot \sum_{y \in \mathcal{S}^c} \phi((y, z, z') \text{ j.t.}).
\]

Substituting this in (4.2.5.8) yields

\[
(4.2.5.9) \quad P_2 \leq \frac{1}{N(c)} \sum_{y, z^*} \phi(y \in A' \text{ and } (y, z, z') \text{ j.t.}).
\]

For every \( (z, z') \) j.t. with some \( y \), there are (for some constant \( c_1 \))

\[
\left[ N(c; z) \right] \leq 2^{N\left[ a_c \cdot h\left( \frac{p_c - a_c^{c+1} + a_c^c}{a_c^c} \right) + c_1 \delta \right]} + O(\log(n))
\]

words \( y \) j.t. with this pair: in the \( N(c; z') - N(c; z) \) positions where \( s'(n) = c \) and \( s(n) \neq c \), \( y(n) \) must be \( c \) and the remaining \( (p_c^N - N(c; z') + N(c; z)) \) positions of the \( c \)'s in \( y \) can be chosen among the \( c \)-positions in \( z \). Hence for all
Chapter 4

typical $g$ and $g'$, we have

$$\sum_{y \in D^c} \phi((y, g, g')) j . t . \leq 2 N \left[ a^c_c \cdot h \left( \frac{p^c_c - a^c_c + a^c_c}{a^c_c} \right) + c_1 \delta \right] + O(\log(N)),$$

or

$$P_2 \leq \frac{1}{N(0)} \cdot 2 N \left[ a^c_c \cdot h \left( \frac{p^c_c - a^c_c + a^c_c}{a^c_c} \right) + c_1 \delta \right] + O(\log(N)).$$

With (4.2.5.2), this is less than

$$N \left[ a^c_c \cdot h \left( \frac{p^c_c - a^c_c + a^c_c}{a^c_c} \right) - h(p_c) \cdot \frac{p^c_c \cdot p}{(1-p_c)(1-P)} + c_1 \delta - \epsilon/4 \right] + O(\log(N)).$$

From Appendix A, we find $a^c_c = p_c/(1-P)$ and $a^c_c = \frac{p^c_c \cdot p}{(1-p_c)(1-P)}$. This yields

$$a^c_c \cdot h \left( \frac{p^c_c - a^c_c + a^c_c}{a^c_c} \right) = h(p_c) \cdot \frac{p^c_c \cdot p}{(1-p_c)(1-P)}.$$

Hence with $\delta \leq \epsilon/(8c_1)$ and $\delta \leq 1/2$ we have

$$P_2 \leq 2^{-N \epsilon/8} + O(\log(N)) < \epsilon/3T$$

if $N$ is large enough.

Now we combine the inequalities for $P_0$, $P_1$ and $P_2$ with (4.2.5.6): for sufficiently large block length $N$,

$$\bar{p}_{err} = \lim_{K \to \infty} \sum_{k = \mathbb{N}, K' \to K} \frac{1}{K' - K + 1} \cdot T(P_0 + P_1 + P_2)$$

$$\leq T(\epsilon/(3T) + \epsilon/(3T) + \epsilon/(3T)) = \epsilon.$$

Finally we can conclude that at least one case 3-WUM code $C$ in the ensemble
exists for which $P_{\text{err}}(C) < \varepsilon$ and for which the rate tuple $(\hat{r}_0, \hat{r}_1, \ldots, \hat{r}_{q-1})$ satisfies $\hat{r}_c > 1 - \varepsilon$. This proves the achievability of the rate point $\underline{r} \in \mathcal{Z}_3$. By time sharing it is obvious that every convex combination of points in $\mathcal{Z}_3$ is also achievable for case 3. This completes the proof of the statement $C_3 \supset \text{co} \mathcal{Z}_3$.

Now we prove the converse, namely that points outside $\text{co} \mathcal{Z}_3$ are not achievable. Let $C$ be a case 3–WUM code with parameters $(N, n_0, n_1, \ldots, n_{q-1})$ and error probability $P_{\text{err}}(C) < \varepsilon$. Let $c \in A$ and $k \equiv c \mod q$. We have, exactly as in case 1 and 2 (compare the derivation of (4.2.4.1) and following inequalities):

$$\log(n_c) = I(\hat{V}_k; V_k | S_k) + H(V_k | \hat{V}_k, S_k),$$

with

$$I(\hat{V}_k; V_k | S_k) \leq \sum_{n=0}^{N-1} H(S_{k+1}(n) | S_k(n)).$$

As in Section 4.2.4, let

$$R_k(n) := H(S_{k+1}(n) | S_k(n)).$$

Then

$$R_k(n) = \sum_{i \neq c} Pr[S_k(n) = i] \cdot H(S_{k+1}(n) | S_k(n) = i)$$

$$= \sum_{i \neq c} Pr[S_k(n) = i] \cdot H(I_k(n) | S_k(n) = i)$$

$$= Pr[S_k(n) \neq c] \cdot H(I_k(n)).$$

For a fixed coordinate $n$, we define $p_c(n) := Pr[I_k(n) = c]$. Note that the numbers $p_c(n)$ only depend on $k \mod q (= c)$ because of the code definition. As before, the distribution of the states is described by a Markov chain. Although this Markov chain is different from the one described in Appendix A (where every codeword of fixed composition has the same probability of being written, which is clearly not true for any code), we do find the same stationary distribution if we look at one cell only, since for a fixed cell we have equal probability of writing a
'c' in both models. Hence, as proved in Appendix A, we find for $k \to \infty$:

$$
Pr\{S_{k}(n) = i\} \to a_{i}^{c}(n),
$$

where the $a_{i}^{c}(n)$ form the solution of (4.2.5.5), if (4.2.5.5) is read with $a_{i}^{c}(n)$ instead of $a_{i}$ and $p_{c}(n)$ instead of $p_{c}$. The solution is given in (A.3). However, the notation in Appendix A is slightly different: $p_{i}$ should be read as $p_{i}(n)$, $a_{i}$ as $a_{i}^{c}(n)$, $p_{i}^{i}$ as $1-p_{i}(n)$ and $P$ as $P(n) := \Pi_{i}(1-p_{i}(n))$.

For large enough $k$, we find

$$
\mathcal{R}_{k}(n) \leq (1-a_{c}^{c}(n)) \cdot h(p_{c}(n)) + \varepsilon/2
$$

$$
= (1 - \frac{p_{c}(n)P(n)}{(1-P(n))(1-p_{c}(n))}) \cdot h(p_{c}(n)) + \varepsilon/2.
$$

If we define, for all $c$,

$$
\mathcal{R}_{c}(n) := (1 - \frac{p_{c}(n)P(n)}{(1-P(n))(1-p_{c}(n))}) \cdot h(p_{c}(n)),
$$

then it follows that

$$
I(\hat{Y}_{k}; \hat{V}_{k}|S_{k}) \leq \sum_{n=0}^{N-1} \mathcal{R}_{c}(n) + N\varepsilon/2.
$$

As in case 1, the Fano inequality yields: for all $c$, a $k$ with $k \equiv c \mod q$ exists such that

$$
\mathcal{H}(\hat{V}_{k}|\hat{V}_{k}, S_{k}) \leq \varphi(\varepsilon).
$$

This shows

$$
\mathcal{R}_{c} \leq \sum_{n=0}^{N-1} \mathcal{R}_{c}(n)/N + \delta
$$

for arbitrarily small $\delta$, if $\varepsilon$ is small enough. As in Section 4.2.4, let

$$
\mathcal{R}(n) := (\mathcal{R}_{0}(n), \mathcal{R}_{1}(n), \ldots, \mathcal{R}_{q-1}(n)).
$$

By Definition (4.2.2.3), $\mathcal{R}(n) \in \mathcal{X}_{3}$. Now the code rate, $\mathcal{R}$, can be bounded as
\[ \sum_{n=0}^{N-1} k \leq \frac{k}{N} + (\delta, \delta, \ldots, \delta) \in \mathcal{Z}_3 \]

if \( \varepsilon \downarrow 0 \). This concludes the converse part of the proof of Theorem (4.2.2.4).

4.2.6. Proof for case 4: achievability

We will prove the case 4–achievability for points in \( \mathcal{Z}_4 \) in almost exactly the same way as we proved the achievability for case 3, in Section 4.2.5. Therefore we will skip some of the details and only point out the differences between the two cases.

Let \( 0 < \varepsilon < 1 \). For \( c \in \mathcal{A} \), let \( p_c \in (0,1) \). We define

\[
(4.2.6.1) \quad P := \prod_{c \in \mathcal{A}} (1-p_c) \quad \text{and} \quad P_c := h(p_c) - \frac{p_c}{1-P} \cdot h(P).
\]

Let \( N \in \mathbb{N} \) be large and assume that \( p_c \cdot N \) is an integer for all \( c \). Let \( N_0(c) \) and \( N_1(c) \) be such that (compare (4.2.5.2))

\[
(4.2.6.2) \quad N_0(c) \cdot N_1(c) = \left[ \frac{N}{p_c \cdot N} \right],
\]

\[
2^N \left[ h(P) \cdot p_c / (1-P) + \varepsilon / 4 \right] \leq N_0(c) \leq 2^N \left[ h(P) \cdot p_c / (1-P) + \varepsilon \right],
\]

\[
2^N \left( e - \varepsilon / 2 \right) \leq N_1(c) \leq 2^N \left( e - \varepsilon / 3 \right).
\]

As in case 3, such numbers can be found. We will construct an ensemble of case 4–codes by looking at partitionings of \( \mathcal{A}^0, \mathcal{A}^1, \ldots, \mathcal{A}^{q-1} \), where \( \mathcal{A}^c \) denotes the set of all words in \( \{c, \bar{c}\}^N \) that contain \( p_c \cdot N \) times \('c'\) and \((1-p_c) \cdot N \) times \('\bar{c}'\). Every \( \mathcal{A}^c \) can be partitioned into\( N_0(c) \) subsets containing \( N_1(c) \) words each. We call these subsets \( c_i(c) \), \( 0 \leq i \leq N_0(c)-1 \), and we write

\[
c_i(c) = \{z(c,i,0), z(c,i,1), \ldots, z(c,i,N_1(c)-1)\}.
\]
Consider a fixed choice of partitionings, denoted as \( \{ e_t^{(c)} \}, c \in \mathcal{A}, 0 \leq i \leq N_0^{(c)} - 1 \).

The case 4–WUM code, say \( \mathcal{C} \), that corresponds to this choice is the following.

Let \( T = \lceil \log(N) \rceil \). The code \( \mathcal{C} \) has parameters \((N, \tilde{N}_0, \ldots, \tilde{N}_{q-1})\) that are equal to the parameters for the case 3–WUM codes in Section 4.2.5. With these parameters, we have for the rate tuple \( \tilde{k} \):

\[ \tilde{k}_c \geq \tilde{k}_c - \varepsilon, \quad \text{for all } c \in \mathcal{A} \]

if \( N \) is large enough.

The encoding function \( f_c \) for \( c \in \mathcal{A} \) is the same as for the case 3–codes (in both cases the encoder cannot use the previous state, \( z_{k+1} \), so we can take the same functions in case 3 and 4). The decoder, however, is not allowed to use the old state \( z_{k+1} \) in his estimate for \( \hat{\omega}_k \). Let \( \delta > 0 \). If the decoder receives \( z_{k+1} \), where

\[ z_{k+1} = (z_{k+1,0}, z_{k+1,1}, \ldots, z_{k+1,T}) \]

then \( z_{k+1,0} \) determines the index \( w_{k,0} \) of the set \( e_{w_{k,0}}^{(c)} \) that was used to encode the rest of the message. A block \( z_{k+1,t} \) for \( t \geq 1 \) is decoded by taking

\[ \hat{\omega}_k, t := \text{the unique } \omega \in \{0, 1, \ldots, N_1^{(c)} - 1\} \text{ such that } (\omega, w_{k,0}, z_{k+1,0}, z_{k+1,1}, \ldots, z_{k+1,T}) \text{ is jointly } \delta \text{–typical (see Definition (4.2.6.3)). If such a } \omega \text{ does not exist, then } \hat{\omega}_k := ?? \text{.} \]

(4.2.6.3) Definition. Let \( \delta > 0 \). For a word \( z \in S^C \) and a state \( z = z_{k+1, t} \), we say that \( z \) and \( z \) are jointly \( \delta \text{–typical (j.t.)} \) if \( z \) is \( \delta \text{–typical (see Definition (4.2.5.4))} \) and \( s(n) = c \) for all positions \( n \) for which \( z(n) = c \).

As in Section 4.2.5, we will now bound the average error probability over the code ensemble,

\[ P_{\text{err}} = \sum_{A \in \mathcal{C}} P_r(\mathcal{C} = A) \cdot P_{\text{err}}(A). \]

The first part of the derivation in Section 4.2.5 is valid also in this case. Therefore
\[
\sum_{\mathcal{C}} \Pr\{\hat{V}_k \neq V_k \text{ and } \mathcal{C} = A\}
\leq T \cdot \sum_{A^* \in \mathcal{C}^*} \Pr\{\hat{V}_{k,1} \neq V_{k,1} \text{ and } \mathcal{C}_0^*(c) = A^*\}
= T \cdot \sum_{\exists \in \mathcal{C}^*, A^* \in \mathcal{C}^* \setminus \{\exists\}, \mathfrak{a}, \mathfrak{a}'} \Pr\{\mathcal{C} = A', \mathfrak{z}(c,0,0) = \mathfrak{z}, \mathfrak{s}_{k,1} = \mathfrak{a}, \mathfrak{s}_{k+1,1} = \mathfrak{a}', \hat{V}_{k,1} \neq 0\}.
\]

Now \(\hat{V}_{k,1} \neq 0\) can only occur either if \(\mathfrak{a}'\) (\(= \mathfrak{s}_{k+1,1}\)) is not typical, or if a different filter \(\mathfrak{y} \in \mathcal{C}'\) exists for which \(\mathfrak{y}\) and \(\mathfrak{a}'\) are jointly typical. Since \(\mathfrak{z}\) is the \(c\)-filter operating on \(\mathfrak{a}\) to form \(\mathfrak{a}'\), it follows with Definition (4.2.6.3) that \((\mathfrak{z}, \mathfrak{a}')\) is j.t. if \(\mathfrak{a}'\) is typical. Hence we can bound the above sum as (compare (4.2.5.7)):

\[
T \cdot \sum_{\mathfrak{a}': \text{not typical}} \Pr\{\mathfrak{s}_{k+1,1} = \mathfrak{a}'\} + \\
+ T \cdot \sum_{\exists \in \mathcal{C}^*, A^* \in \mathcal{C}^* \setminus \{\exists\}, \mathfrak{a}': \text{typical}, \mathfrak{a}} \Pr\{\mathcal{C} = A', \mathfrak{z}(c,0,0) = \mathfrak{z}, \mathfrak{s}_{k,1} = \mathfrak{a}, \mathfrak{s}_{k+1,1} = \mathfrak{a}', \hat{V}_{k,1} \neq 0\} \cdot \phi(\exists y \in \mathcal{A}^*, [(y, \mathfrak{a}') \text{ j.t.}]).
\]

We write this as \(T \cdot P_1 + T \cdot P_2\). As in the previous case, we have (see Appendix A)

\[
\Pr\{\mathfrak{s}_{k+1,1} \text{ not typical}\} \leq \frac{1}{\delta^3} \theta(1/N), \quad N \to \infty
\]

if \(k \geq K_N\) for some \(K_N\) dependent of \(p_0, p_1, \ldots, p_{q-1}, \delta\) and \(N\). Since \(T = \lceil \log(N) \rceil\), we have for sufficiently large \(N\):

\[
T \cdot P_1 = T \cdot \sum_{\mathfrak{a}': \text{not typical}} \Pr\{\mathfrak{s}_{k+1,1} = \mathfrak{a}'\} \leq \varepsilon/2.
\]

Also, \(P_2\) can be bounded by
(4.2.6.4) \( P_2 \leq \sum_{\mathcal{S} \in \mathcal{S}^c, \mathcal{S}, \mathcal{S}' \text{ typical}} \Pr\{\mathcal{S}(c,0,0) = \mathcal{S}, \mathcal{S}_k, \mathcal{S}_{k+1} = \mathcal{S}'\} \cdot \\
\cdot \sum_{\mathcal{S}' \in \mathcal{C}' \setminus \{\mathcal{S}\}} \Pr\{\mathcal{C}' = \mathcal{A}'\} \cdot \sum_{\mathcal{S} \in \mathcal{S}^c} \phi(\mathcal{S} \in \mathcal{A}' \text{ and } (\mathcal{S}, \mathcal{S}') \text{ j.t.}).
\]

Consider a typical \( \mathcal{S}' \). As before, every \( \mathcal{S} \) that is j.t. with \( \mathcal{S}' \) is contained in ordered sets \( \mathcal{A}' \). The total number of ordered sets \( \mathcal{A}' \) is
\[
\binom{N(c)N_1(c) - 2}{N_1(c) - 2} \cdot (N_1(c) - 1)!
\]

As in case 3, this yields for any \( \mathcal{S} \) and \( \mathcal{S}' \):
\[
\sum_{\mathcal{A}' \in \mathcal{C}' \setminus \{\mathcal{S}\}} \Pr\{\mathcal{C}' = \mathcal{A}'\} \cdot \sum_{\mathcal{S} \in \mathcal{S}^c} \phi(\mathcal{S} \in \mathcal{A}' \text{ and } (\mathcal{S}, \mathcal{S}') \text{ j.t.})
\leq \frac{1}{N_0(c)} \cdot \sum_{\mathcal{S} \in \mathcal{S}^c} \phi((\mathcal{S}, \mathcal{S}') \text{ j.t.}).
\]

Substituting this in (4.2.6.4), we find
(4.2.6.5) \( P_2 \leq \frac{1}{N_0(c)} \cdot \sum_{\mathcal{S}' \text{ typical}} \Pr\{\mathcal{S}_{k+1,1} = \mathcal{S}'\} \cdot \sum_{\mathcal{S} \in \mathcal{S}^c} \phi((\mathcal{S}, \mathcal{S}') \text{ j.t.}).
\]

For every typical \( \mathcal{S}' \), there are (for some constant \( c_1 \))
\[
\left[ N(c;\mathcal{S}') \right] \leq 2^{-N \left[ a_c c+1 \cdot h(p_c/a_c c+1) + c_1 \delta \right] + O(\log(N))}
\]
c-filters \( \mathcal{S} \) that are j.t. with it, since \( \mathcal{S} \) must have its \( p_c N \) c's in the positions where \( \mathcal{S}' \) has c's. Hence
The Write Unidirectional Memory

\[ P_2 \leq \frac{1}{N(c)} \cdot 2^{N \left[ a_c^{c+1} \cdot h(p_c/a_c^{c+1}) + c_1 \delta \right] + O(\log(N))}. \]

With (4.2.6.2), this is less than

\[ 2^{- Ne/8 + O(\log(N))} < e/2T \]

if \( N \) is large enough.

Now the inequalities for \( P_1 \) and \( P_2 \) yield with (4.2.5.6): for large enough \( N \),

\[ P_{\text{err}} = \lim_{K \to \infty} \sum_{k = I_N, K} \frac{1}{I - I_{K+1}} \cdot T(P_1 + P_2) \leq T(\epsilon/(2T) + \epsilon/(2T)) = \epsilon. \]

We conclude the proof of Theorem (4.2.2.6) in the same way as in case 3: at least one case 4--code exists in the ensemble such that the rate \( \tilde{r} \) satisfies \( \tilde{r}_c > r_c - \epsilon \) and \( P_{\text{err}}(\tilde{r}) < \epsilon. \) By time sharing this proves the achievability of all points in \( co \mathcal{Z}_4. \)

4.3 Bounding the average rate

In this section we will study the largest possible value of the average rate of a WUM code. This will be defined analogously to the definition for the binary case (compare (4.1.3.1)).
Chapter 4

(4.3.1) Definition. Let \( i \in \{1,2,3,4\} \). The average rate \( R_{av} \) of a case \( i \)-WUM code with rate \((R_0, R_1, \ldots, R_{q-1})\) is defined by
\[
R_{av} := \frac{\sum_{c \in C} R_c}{q}.
\]
The average capacity for case \( i \), \( C_{i,av} \), is defined by
\[
C_{i,av} := \max \{ R_{av} \mid (R_0, R_1, \ldots, R_{q-1}) \in C_i \}.
\]

First we will prove the following quite obvious theorem.

(4.3.2) Theorem. \( C_{i,av} \geq (q-1)/q \) for all \( i \).

Proof: We will construct a case 4-WUM code with rate \((0,1,1,\ldots,1)\) and error probability 0. This code has average rate \((q-1)/q\), which shows the achievability of this average rate for case 4. Clearly rate \((0,1,1,\ldots,1)\) is achievable for the other cases as well, which proves the theorem.

The code will have parameters \((N,1,2^N,2^N,\ldots,2^N)\). In the 0-cycle, the only 0-filter that can be written is \( f_0(0) := (0,0,\ldots,0) \). In other words, we 'clean' the WUM in such a way that we can use it in the following transmissions. In the 1-cycle, the \( 2^N \) different 1-filters that can be written correspond to every possible word in the set \( \{1,0\}^N \). The decoder will be able to see the difference between them, since before writing the state of the WUM contained 0's only.

After writing, there will be only 0's and 1's in the state. Hence if we allow every word from the set \( \{2,0\}^N \) to be written in the subsequent 2-cycle, then the decoder will again be able to determine which of these words was written by looking at the positions of the 2's. In this way we can go on until the \((q-1)\)-cycle, but then we have to clean the WUM again in the 0-cycle.
If we want to know the exact value of \( C_{i, av} \), then, for \( i = 1, 2 \) or 3, we can just use Theorems (4.2.2.2) and (4.2.2.4) and compute \( C_{i, av} \) from the regions \( \mathcal{Z}_1 \) and \( \mathcal{Z}_3 \). For case 1 and 2, this means that we have to maximize a function of \( q^2 \) parameters under some restrictions. Since this involves long and uninteresting computations, the details are given in Appendix B. The result is stated below, in Theorem (4.3.5). First we introduce a polynomial that is needed in the theorem.

\textbf{(4.3.3) Definition.} Define the polynomial \( f : \mathbb{C} \to \mathbb{C} \) by
\[
f(z) := z^q(z - 2) + 1.
\]
Let \( \zeta_0, \zeta_1, \ldots, \zeta_q \) denote the zeros of the polynomial \( f \) and let \( \zeta_0 \) be the largest real zero (it follows from the lemma below that at least one real zero exists). □

\textbf{(4.3.4) Lemma.} With \( \zeta \) as defined above, the following three propositions hold.
\begin{itemize}
\item[(i)] All \( \zeta \) are distinct,
\item[(ii)] \( \zeta_0 > 1.5 \),
\item[(iii)] for all \( i > 0 \): \( |\zeta_i| < \zeta_0 \).
\end{itemize}

\textbf{Proof:} (i) For a multiple zero \( \zeta \) we would have
\[
f(\zeta) = 0 \quad \text{and} \quad \frac{df(z)}{dz}\bigg|_{z=\zeta} = 0,
\]
so
\[
\zeta^q(\zeta - 2) + 1 = 0 \quad \text{and} \quad (q+1)\zeta^q - 2q\cdot\zeta^{q-1} = 0.
\]
The second equation yields \( \zeta = 0 \) (which is not a zero of \( f \)) or \( \zeta = \frac{2q}{q+1} \). The latter possibility gives, after substitution in the first equation,
\[
2\cdot(2q)^q = (q+1)^{q+1}
\]
which is impossible because the left-hand side is 0 (mod \( q \)) and the right-hand side is 1 (mod \( q \)). Therefore no multiple zeroes exist.
We have \( f(z) > 0 \) for all \( z \in \mathbb{R} \) with \( z \geq 2 \); we also have
\[
f(1.5) = - (1.5)^{q/2} + 1 \leq - (1.5)^2/2 + 1 = - 1/8 < 0.
\]
Since \( f \) is continuous, this implies that the largest real zero lies in \((1.5, 2)\).

We use Rouché's theorem (cf. [SAF76]) to prove \( |\zeta_i| \leq 1 \) for all \( i > 0 \). Since \( \zeta_0 > 1.5 \), this will prove the theorem. Define \( g(z) := -2z^q \) for \( z \in \mathbb{C} \).

Then, for \( \epsilon > 0 \) and \( |z| = 1 + \epsilon \):
\[
|g(z)| = 2(1+\epsilon)^q = 2 + 2q\epsilon + O(\epsilon^2) \quad \text{and}
\]
\[
|f(z)-g(z)| = |z^{q+1} + 1| \leq (1+\epsilon)^{q+1} + 1 = 2 + (q+1)\epsilon + O(\epsilon^2).
\]
Hence, if \( \epsilon \) is small enough: \( |f(z) - g(z)| \leq |g(z)| \) on the circle with radius \( 1 + \epsilon \).

Now, if we let \( \epsilon \downarrow 0 \), Rouché's theorem implies that \( f \) and \( g \) have equally many zeros (counting multiplicities) inside or on the circle of unity. Obviously, \( g \) has \( q \) zeros for which \( |z| \leq 1 \); hence the same holds for \( f \). Since \( f \) has \( q+1 \) zeros in total and \( |\zeta_0| > 1 \), we find \( |\zeta_i| \leq 1 \) if \( i > 0 \).

\((4.3.5)\) Theorem. The average capacities \( c_{1,av} \) and \( c_{2,av} \) of the WUM equal
\[
c_{1,av} = c_{2,av} = \log(\zeta_0).
\]

Proof: As mentioned before, the proof can be given by maximizing the function
\[
\kappa(a_0^0, a_0^1, \ldots, a_{q-1}^{q-1}),
\]
where
\[
\kappa(a_0^0, a_0^1, \ldots, a_{q-1}^{q-1}) := \sum_{c} \sum_{i \neq c} a_i^c \cdot \frac{a_i^{c+1}}{a_i^c},
\]
under the constraints \( \sum_i a_i^c = 1 \) for all \( c \) and \( a_i^c \geq a_i^{c+1} \) for all \( i \neq c \). This is done in Appendix B. Here we will present a different proof of the theorem.

First we prove that average rate \( \log(\zeta_0) \) is achievable with case 2–codes, if the block length tends to infinity. After that we show that \( \log(\zeta_0) \) is an upper bound for the rate of any eventually error–free case 2–code (defined in Section 4.2.3). Since we already know that \( \epsilon \)–error case 1–codes cannot achieve higher
rates than eventually error–free case 2–codes (which follows from Section 4.2.3 and 4.2.4), this shows that \( \log(\zeta_0) \) is the maximum achievable average rate for both case 1 and case 2.

Let \( N \in \mathbb{N} \). Let \( a := (a_0, a_1, \ldots, a_{q-1}) \in \mathbb{R}^q \) such that \( a_c \cdot N \in \mathbb{N} \) for all \( c \in \mathcal{A} \), \( 0 \leq a_0 \leq a_1 \leq \ldots \leq a_{q-1} \) and \( \sum_c a_c = 1 \). Consider the following restriction on the use of the WUM. In a \( c \)--cycle, the writing must be such that only words from a set \( \mathcal{T}_c \) can be the new state \( s_{k+1} \), where \( \mathcal{T}_c \subset \mathcal{A}^N \) is the set of words that contain \( a_{i-c-1} \cdot N \) i's for all \( i \in \mathcal{A} \). Hence writing in a \( c \)--cycle means that a word \( s_k \in \mathcal{T}_{c-1} \) is changed into a word \( s_{k+1} \in \mathcal{T}_c \). It can be readily checked that this is possible only by changing \( (a_{i-c} - a_{i-c-1}) \cdot N \) of the i's into c's (the \( a_i \)'s are nondecreasing) for all \( i \neq c \). Note that the encoder can take care of this: by choosing an appropriate case 2–code, he can make sure that the restriction is met.

We now adapt the notation of [KU83, KU88a] and consider the WUM with sets \( \mathcal{T}_0, \ldots, \mathcal{T}_{q-1} \) as a channel with generalized defects. The words in \( \mathcal{T}_{c-1} \) that can be on the disk before writing in a \( c \)--cycle are the states of the channel, such that each state \( s \) allows some set \( \mathcal{Y}_s \subset \mathcal{T}_c \subset \mathcal{A}^N \) to be written. Kuznetsov [KU83] showed that the capacity \( C(a) \) of this channel with generalized defects is

\[
C(a) = \lim_{N \to \infty} \min_{s} \frac{\log |\mathcal{Y}_s|}{N}.
\]

To compute the numbers \( |\mathcal{Y}_s| \), we must count the number of ways in which some fixed word \( g \) (representing the state of the channel) in set \( \mathcal{T}_{c-1} \) can be updated to a word in \( \mathcal{T}_c \). Call this number \( N_{g,c} \). Then

\[
N_{g,c} = \prod_{i \in \mathcal{A} \setminus \{c\}} \left[ \frac{a_{i-c} \cdot N}{a_{i-c-1} \cdot N} \right] = \prod_{i=0}^{q-2} \left[ \frac{a_{i+1} \cdot N}{a_i \cdot N} \right],
\]

which is dependent on neither \( g \) nor \( c \). Therefore we find that all sets \( \mathcal{Y}_s \) contain the same number of elements,
Chapter 4

$$|\mathcal{Y}_q| = q^{-2} \prod_{i=0}^{N-2} \left[ \frac{a_{i+1}^N}{a_i^N} \right].$$

Consequently,

$$C(\mathcal{g}) = \lim_{N \to \infty} \frac{\log \left( \prod_{i=0}^{N-2} \left[ \frac{a_{i+1}^N}{a_i^N} \right] \right)}{N} = \sum_{i=0}^{q-2} a_{i+1} h(\frac{a_i}{a_{i+1}}).$$

Therefore, for all vectors $\mathcal{g}$ satisfying the conditions mentioned in the beginning of the proof, rate $C(\mathcal{g})$ is case 2–achievable if the block length is large enough. Maximizing over $\mathcal{g}$ in a straightforward manner, we find

$$\max \{ C(\mathcal{g}) \mid 0 \leq a_0 \leq \ldots \leq a_{q-1}, \sum a_i = 1 \} = \log(\zeta_0).$$

(This maximization occurs in a concealed form in the proof given in Appendix B. Notice, though, that the maximization in the appendix involves $q^2$ parameters, whereas here we have only $q$.) Hence the average rate in $q$ consecutive cycles can achieve the value $\log(\zeta_0)$, which concludes the first half of the proof.

Now we prove the converse. This part generalizes Simonyi’s proof [SIM89] of the converse for the binary case 2–WUM with $H_0 = H_1$. Let $C$ be an eventually error–free case 2–code with parameters $H$ and $H_c$ for $c \in \mathcal{A}$. We consider $q \cdot t$ consecutive writing cycles, and we look at the ‘fate’ of one cell during these cycles. For $q = 3$, all possible fates of length at most 3 are shown in Table (4.3.6). As mentioned before, each cell contains ‘0’ before the first writing.

Let $\mathcal{N}_{t,i}$ denote the number of fates (sequences) of length $t$ for which the last ($t^{th}$) content of the cell equals $i$ and let $S_t$ be the total number of fates of length $t$. So

$$S_t = \sum_{i \in \mathcal{A}} \mathcal{N}_{t,i}.$$

We find the following recurrences for the $\mathcal{N}_{t,i}$:

---

-156-
The Write Unidirectional Memory

<table>
<thead>
<tr>
<th>cyclenumber</th>
<th>type of cycle</th>
<th>possible fates of cell</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>00</td>
</tr>
<tr>
<td></td>
<td></td>
<td>02</td>
</tr>
<tr>
<td></td>
<td></td>
<td>11</td>
</tr>
<tr>
<td></td>
<td></td>
<td>12</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>000</td>
</tr>
<tr>
<td></td>
<td></td>
<td>022</td>
</tr>
<tr>
<td></td>
<td></td>
<td>020</td>
</tr>
<tr>
<td></td>
<td></td>
<td>111</td>
</tr>
<tr>
<td></td>
<td></td>
<td>110</td>
</tr>
<tr>
<td></td>
<td></td>
<td>122</td>
</tr>
<tr>
<td></td>
<td></td>
<td>120</td>
</tr>
</tbody>
</table>

(4.3.6) Table. Example of 'fate' of a cell.

\[ N_{t+1,i} = N_{t,i} \quad \text{if } t+1 \not\equiv i \mod q \quad (\text{the last cycle is not an } i\text{-cycle}), \]

\[ N_{t+1,i} = S_t \quad \text{if } t+1 \equiv i \mod q. \]

Summation and repeated application of the first identity leads to

\[ S_{t+1} = 2^i S_t - S_{t-q} \quad \text{with } S_0 = 1, \ S_1 = 2, \ S_t = 0 \quad \text{for } t < 0. \]

It should be noted that for \( q = 2 \), this is equivalent to the Fibonacci relation.

By [LOV79, pp. 158–160] and (i) of Lemma (4.3.4), we have the following formula for \( S_t \). With \( \zeta_0, \zeta_1, \ldots, \zeta_q \) as in Definition (4.3.3), we find

\[
S_t = \sum_{i=0}^{q} \zeta_i \Pi_{j \neq i} (\zeta_i - \zeta_j)
\]

\[
= \zeta_0^t + (\text{other terms } \zeta_{i_1} \zeta_{i_2} \cdots \zeta_{i_t} \text{ with } (i_1, \ldots, i_t) \in \{0, \ldots, q\}^t). \]

Because of Lemma (4.3.4), (i), it can be seen that the following limit exists:

\[
\lim_{t \to \infty} \frac{\log(S_t)}{t} = \log(\zeta_0). \]

- 157 -
We know that each cell can have $S_q t$ different fates of length $t$; for the sequence of $q \cdot t$ consecutive writings of words of length $N$, the number of possibilities is $(S_q t)^N$. Since code $C$ is eventually error-free, decoding errors may occur in the first $q-1$ transmissions only. Hence the decoder must be able to determine which sequence of $(q \cdot t-q)$ messages out of the $(S_0 t)^{t-1} \cdot (S_1 t)^{t-1} \cdots (S_{q-1} t)^{t-1}$ possible sequences was transmitted during the $(q \cdot t-q)$ most recent cycles. Therefore we must have

$$(S_q t)^N \geq (S_0 t)^{t-1} \cdot (S_1 t)^{t-1} \cdots (S_{q-1} t)^{t-1},$$

or

$$\frac{\sum_c \log(S_c t)}{N} \leq \frac{\log(S_q t)}{t-1}.$$

This is true for all $t \in \mathbb{N}$, so we have

$$R_{av} \leq \lim_{t \to \infty} \frac{\log(S_q t)}{qt^{t-1}} = \log(\zeta_0),$$

proving the converse part of the theorem. \( \square \)

Now that we have found an expression for the average capacity in cases 1 and 2, we can compute $C_{1,av}$ for several values of $q$. For $q \leq 10$, these numbers can be found in Table (4.3.8). This table also lists values of $C_{3,av}$, which have been found by maximizing the function $I(p_0, p_1, \ldots, p_{q-1})$, where

$$I(p_0, p_1, \ldots, p_{q-1}) := \sum_c h(p_c) \{1 - \frac{p_c^P}{(1-p_c)(1-P)}\}, \ P := \Pi(1-p_c).$$

Unfortunately, no analytical expression could be obtained for the maximum of this function, even though we have just $q$ parameters (instead of $q^2$ as in case 1) and no restrictions here. Therefore the maximization was done numerically. For all values of $q \leq 10$, it turns out that the point $p$ where $I(p)$ assumes its maxi-
mum (as found by computer) satisfies $p_0 = p_1 = \ldots = p_{q-1}$ and hence also all $k_c$ are equal for the maximum average rate. This was to be expected, since we also saw this in cases 1 and 2: if the average rate is maximum, the rate is symmetrical. This leads us to the conjecture that the same will be true in case 4.

Since the true capacity region for case 4 is unknown, we need a different approach to find $c_{4,av}$. Theorem (4.3.7) is a justification for Conjecture (4.2.2.7).

(4.3.7) Theorem. We have

$$c_{4,av} = \max \{ (\Sigma E_c)/q | (k_0, k_1, \ldots, k_{q-1}) \in \mathcal{Z}_4 \}. \quad \Box$$

Proof: It follows from Theorem (4.2.2.6) that

$$c_{4,av} \geq \max \{ (\Sigma E_c)/q | (k_0, k_1, \ldots, k_{q-1}) \in \mathcal{Z}_4 \}.$$

Therefore it remains to prove that for every case 4–achievable rate, the average rate is in the set $\{ (\Sigma E_c)/q | (k_0, k_1, \ldots, k_{q-1}) \in \mathcal{Z}_4 \}$. The main part of this proof is a generalization of the case 4–converse for binary symmetrical codes given in [WIL89] (also found by Wyner and Ozarow, [WYN88]).

Let $\epsilon > 0$ and let $C$ be a case 4–code with parameters $N$ and $\mathcal{M}_c$ for $c \in \mathcal{A}$. Assume $P_{err}(C) \leq \epsilon$. Let $c \in \mathcal{A}$, $k \equiv c \mod q$. We have

$$H(W_k) = H(W_k | S_{k+1}) + I(S_{k+1}; W_k)$$

$$\leq H(W_k, \hat{V}_k | S_{k+1}) + I(S_{k+1}; W_k)$$

$$= H(W_k | \hat{V}_k, S_{k+1}) + H(\hat{V}_k | S_{k+1} W_k) + I(S_{k+1}; W_k)$$

$$= H(W_k | \hat{V}_k, S_{k+1}) + I(S_{k+1}; W_k) \quad \{\text{since } \hat{V}_k \text{ is determined by } S_{k+1}\}$$

$$\leq \varphi(Pr{\hat{V}_k \neq V_k}) + I(S_{k+1}; W_k)$$

where the last step is Fano's inequality (see Sections 4.2.4 and 4.2.5). Hence, for large $k$:
Chapter 4

\[ K \cdot R_{av} = K \cdot \sum c \log(N_c)/(Nq) = qK \sum_{k=1}^{qK} N_k/(Nq) \]

\[ \leq \sum_{k=1}^{qK} I(S_{k+1}^n;V_k)/Nq + \sum_{k=1}^{qK} \varphi(Pr\{\tilde{V}_k=\tilde{V}_k\})/(Nq) \]

\[ = \sum_{n=0}^{N-1} I(S_{k+1}^n;V_k|S_{k+1}^n)/Nq + \sum_{k=1}^{qK} \varphi(Pr\{\tilde{V}_k=\tilde{V}_k\})/(Nq) \]

\[ \leq \max_{n} \sum_{k=1}^{qK} I(S_{k+1}^n;V_k|S_{k+1}^n)/q + \sum_{k=1}^{qK} \varphi(Pr\{\tilde{V}_k=\tilde{V}_k\})/(Nq). \]

Let \( n' \) be the value of \( n \) for which the maximum is assumed in the above sum; so

\[ K \cdot R_{av} \leq \sum_{k=1}^{qK} I(S_{k+1}^n;V_k|S_{k+1}^n)/q + \sum_{k=1}^{qK} \varphi(Pr\{\tilde{V}_k=\tilde{V}_k\})/(Nq). \]

Now

\[ I(S_{k+1}^n;V_k|S_{k+1}^n) = H(S_{k+1}^n|S_{k+1}^n) - H(S_{k+1}^n|V_k,S_{k+1}^n) \]

\[ \leq H(S_{k+1}^n|S_{k+1}^n) - H(S_{k+1}^n|V_k,S_{k+1}^n,S_{k}^n,X_k(n')) \]

\[ = H(S_{k+1}^n|S_{k+1}^n) - Pr\{I_k(n')=\emptyset\} \cdot H(S_{k+1}^n|V_k,S_{k+1}^n,S_{k}^n,X_k(n')=\emptyset) \]

\[ = H(S_{k+1}^n|S_{k+1}^n) - Pr\{I_k(n')=\emptyset\} \cdot H(S_{k+1}^n|S_{k}^n). \]

The last equality follows from the fact that \( S_{k+1}^n = R_{k+1}^c \cdot S_{k}^n \) and from the definition of a case 4--WUM code. Substituting this and dividing by \( K \) yields

\[ K \cdot R_{av} \leq \sum_{k} \{H(S_{k+1}^n|S_{k}^n) - Pr\{I_k(n')=\emptyset\} \cdot H(S_{k+1}^n|S_{k}^n)\}/(Kq) + \]

\[ + \sum_{k} \varphi(Pr\{\tilde{V}_k=\tilde{V}_k\})/(Kq) \]

\[ \leq \sum_{k} \{((1-Pr\{I_k(n')=\emptyset\}) \cdot H(S_{k+1}^n|S_{k}^n)))/(Kq) + O(1/K) \]

\[ + \varphi(\sum_{k} Pr\{\tilde{V}_k=\tilde{V}_k\})/(Kq))/N \]

by convexity of \( \varphi(\cdot) \). This can be bounded from above by

\[ \sum_{k} \{((1-Pr\{I_k(n')=\emptyset\}) \cdot H(S_{k+1}^n)))/(Kq) + O(1/K) + \varphi(\sum_{k} Pr\{\tilde{V}_k=\tilde{V}_k\})/(Kq))/N \]

\[ -160 - \]
The Write Unidirectional Memory

\[
= \sum_k \{H(S_{k+1}(n')) - Pr\{I_k(n')=0\} \cdot H(S_k(n'))\}/(kq) + O(1/k) + \\
+ \varphi(\sum_k Pr\{\hat{V}_{k}\neq V_{k}\}/(kq))/N
\]

\[
= \sum_k \{H(S_{k+1}(n')) - H(S_{k+1}(n')|I_k(n'))\}/(kq) + O(1/k) + \\
+ \varphi(\sum_k Pr\{\hat{V}_{k}\neq V_{k}\}/(kq))/N
\]

\[
= \sum_k \{H(I_k(n')) - H(I_k(n')|S_{k+1}(n'))\}/(kq) + O(1/k) + \\
+ \varphi(\sum_k Pr\{\hat{V}_{k}\neq V_{k}\}/(kq))/N.
\]

Let \(p_c := Pr\{I_k(n')=c\}\) for \(k \equiv c \mod q\); by definition of the code, this number only depends on \(c\) and \(n'\). Define \(\beta_i^k := Pr\{S_k(n') = i\}\) for all \(i\) and \(k\). As argued in the converse proof for case 3 (Section 4.2.5), the distribution of \(S_k(n')\) is described by a Markov chain. It should be noticed that we have exactly the same model here. Hence the number \(\beta_i^k\) tends to \(a_i^c\) if \(k \equiv c \mod q\), where the \(a_i^c\) satisfy (A.3). Hence, for large enough \(k\) with \(k \equiv c \mod q\):

\[
H(I_k(n')) - H(I_k(n')|S_{k+1}(n')) \\
\leq h(p_c) - a_{c+1}^c \cdot h(p_c/a_{c+1}^c) + \varepsilon \\
= h(p_c) - h(P) \cdot p_c/(1-P) + \varepsilon.
\]

Consequently

\[
R_{av} \leq \sum_{c\in A} \{h(p_c) - \frac{p_c}{1-P} \cdot h(P) + \varepsilon\}/q + 0(1/k) + \varphi(\sum_k Pr\{\hat{V}_{k}\neq V_{k}\}/(kq))/N.
\]

This holds for all large \(K\), so we may take the limit for \(K \to \infty\). Since \(P_{err}(C) \leq \varepsilon\),

\[
R_{av} \leq \sum_{c\in A} \{h(p_c) - \frac{p_c}{1-P} \cdot h(P) + \varepsilon\}/q + \varphi(\varepsilon)/N.
\]

Letting \(\varepsilon \downarrow 0\) gives the desired result.

\(\square\)
Theorem (4.3.7) enables us to find $c_{4, av}$ by maximizing the rate sum over $\mathbb{Z}_4$. Again this was done by computer. As predicted, the maximum is assumed for a vector $(p_0, p_1, \ldots, p_{q-1})$ with $p_0 = p_1 = \cdots = p_{q-1}$. For $q > 2$ this follows from the computer results, but for $q = 2$, it is proved in Appendix C that

$$c_{4, av} = \max \{ h(p) - h(p^2)/(1+p) \mid 0 \leq p \leq 1 \} = 0.54589 \ldots$$

It follows that $c_{4, av}$ equals the upper bound on the capacity for case 4 period-1 codes found in [WIL89]. In other words, Willems' converse for period-1 codes also holds for the larger class of period-2 codes.

Table (4.3.8) lists $c_{i, av}$ for $i \in \{1, 3, 4\}$ and $q \leq 10$. Since $c_{2, av} = c_{1, av}$, this gives the average capacity for all cases. The table also lists the values of $(q-1)/q$, which can be achieved with the code described in the proof of Theorem (4.3.2).

<table>
<thead>
<tr>
<th>$q$</th>
<th>$c_{1, av}$</th>
<th>$c_{3, av}$</th>
<th>$c_{4, av}$</th>
<th>$(q-1)/q$</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>0.69424</td>
<td>0.69424</td>
<td>0.54589</td>
<td>0.50000</td>
</tr>
<tr>
<td>3</td>
<td>0.87915</td>
<td>0.87305</td>
<td>0.76072</td>
<td>0.66667</td>
</tr>
<tr>
<td>4</td>
<td>0.94678</td>
<td>0.94089</td>
<td>0.86572</td>
<td>0.75000</td>
</tr>
<tr>
<td>5</td>
<td>0.97523</td>
<td>0.97101</td>
<td>0.92239</td>
<td>0.80000</td>
</tr>
<tr>
<td>6</td>
<td>0.98811</td>
<td>0.98545</td>
<td>0.95462</td>
<td>0.83333</td>
</tr>
<tr>
<td>7</td>
<td>0.99419</td>
<td>0.99268</td>
<td>0.97345</td>
<td>0.85714</td>
</tr>
<tr>
<td>8</td>
<td>0.99713</td>
<td>0.99626</td>
<td>0.98456</td>
<td>0.87500</td>
</tr>
<tr>
<td>9</td>
<td>0.99858</td>
<td>0.99811</td>
<td>0.99112</td>
<td>0.88889</td>
</tr>
<tr>
<td>10</td>
<td>0.99929</td>
<td>0.99904</td>
<td>0.99496</td>
<td>0.90000</td>
</tr>
</tbody>
</table>

(4.3.8) Table. Values of $c_{i, av}$ for $i \in \{1, 3, 4\}$ and $q \leq 10$.

This concludes the chapter on WUMs over arbitrary alphabets. We have found the capacity region for three out of four cases, with a strong conjecture about the fourth one inspired by the known average capacity for this case. It remains an interesting open problem to find a proof for the converse in case 4.

Another problem is of course the construction of good codes for any of the
four cases. Some constructions have been found by the author, but these are basically time sharing codes that give only slight improvements over the trivial code with average rate \((q-1)/q\).

Appendix A

In this appendix we study the distribution of the WUM state \(S_{k+1} \in \mathcal{A}^N\) (notation as in Section 4.2.5 and 4.2.6) for fixed \(N\) and large values of \(k\), under the assumption that at each instant \(k\) with \(k \equiv c \mod q\), every \(c\)-filter \(\mathcal{E}\) having \(p_c^N\) \(c\)'s and \((1-p_c)^N\) \(\mathcal{O}\)'s has the same probability of being written by the encoder. It should be noted that this is indeed the case with every code in the ensemble considered in the random coding proofs in both Section 4.2.5 and 4.2.6.

Let us abbreviate \(S_{k+1} S_k\) by \(S_k\) and let \(I_k\) be the \(c\)-filter that transforms state \(S_k\) into \(S_{k+1}\). We consider a Markov chain similar to the one defined in Section 4.2.4. Its states are called \((c,s)\), \(c \in \mathcal{A}\), \(0 \leq s \leq q^N-1\). The states \((c,s)\) correspond to all possibilities for \(S_k\) if \(k \equiv c \mod q\). The transition probabilities follow from the distribution of \(I_k\): the probability of going from state \((c,s) = S_k\) to state \((c+1,s') = S_{k+1}\) equals the probability that a \(c\)-filter \(I_k\) is chosen for which \(S_{k+1} = I_k \circ S_k\). We will show that the stationary probability distribution of this chain is such that \(S_k\) is typical (Definition (4.2.5.4)) with large probability.

First consider a single cell of the WUM, \(S_k(n)\). Let \(I_i^k := Pr\{S_k(n) = i\}\) and \(k \equiv c \mod q\). Define \(p_i^\circ := 1-p_c\). By the definition of the code ensemble, we have for every code:

\[
\text{(A.1) } Pr\{X(n) = c\} = p_c \quad \text{and} \quad Pr\{X(n) = \mathcal{O}\} = p_\mathcal{O}^\circ
\]
The way in which the WUM is used implies

\[
\beta_{i}^{k+1} = p_{i}^{c} \cdot \beta_{i}^{k} \quad \text{if } i \neq c,
\]

\[
\beta_{c}^{k+1} = \beta_{c}^{k} + p_{c}(1 - \beta_{c}^{k}) = p_{c} + p_{c}^{c} \cdot \beta_{c}^{k}.
\]

Consider the Markov chain that can be derived from the original Markov chain by looking at the \(n\)th cell only; it has states \((c, i)\) where \(i\) is the value of \(S_{k}(n)\). This Markov chain has the following stationary distribution. Let \(a_{i}^{c} (i \in \mathcal{A}, c \in \mathcal{A})\) satisfy

\[
\begin{cases}
\sum_{i \in \mathcal{A}} a_{i}^{c} = 1, \\
a_{i}^{c+1} = p_{i}^{c} \cdot a_{i}^{c} \quad \text{for } i \neq c, \\
a_{c}^{c} = p_{c} + p_{c}^{c} \cdot a_{c}^{c}.
\end{cases}
\]

(\text{A.2})

Then the stationary probability of state \((c, i)\) equals \(a_{i}^{c}/q\). In other words, for fixed \(c, k \equiv c \mod q\) and \(k \to \infty\), we have \(\beta_{i}^{k} \to a_{i}^{c}\).

The solution of (\text{A.2}) (which is equivalent to (4.2.5.5)) is the following. For \(i, j \in \mathcal{A}\) and a \(q\)-tuple \((a_{0}, a_{1}, \ldots, a_{q-1})\), we define the 'cyclic product' \(\tilde{\Pi}\) by

\[
\tilde{\Pi}(a_{i}; a_{j}) := \begin{cases}
a_{i} \cdot a_{i+1} \cdots a_{j} & \text{if } i \leq j \text{ and not } (i, j) = (0, q-1) \\
1 & \text{if } i \equiv j+1 \mod q \\
a_{i} \cdot a_{i+1} \cdots a_{q-1} \cdot a_{0} \cdots a_{j} & \text{if } i \geq j+2.
\end{cases}
\]

Then it can be checked that

(\text{A.3}) \quad a_{i}^{c} = p_{i}^{c} \cdot \tilde{\Pi}(p_{i}^{c} + p_{i}^{c-1})/(1 - p) \quad \text{with } \quad p := \prod_{c \in \mathcal{A}} (p_{c}^{c}).

Next, we look at two distinct cells, \(S_{k}(n_{0})\) and \(S_{k}(n_{1})\). For \(k \equiv c \mod q\) we define
The Write Unidirectional Memory

\[
p_{cc} := \Pr\{X_k(n_0) = X_k(n_1) = c\},
\]
\[
p_{c0} := \Pr\{X_k(n_0) = c, X_k(n_1) = 0\} \text{ and } p_{c0} \text{ analogously},
\]
\[
p_{c} := \Pr\{X_k(n_0) = X_k(n_1) = 0\}.
\]

From the definition of the code, we find

\[
\begin{align*}
p_{cc} &= \frac{(p_c^N)(p_c^{N-1})}{N(N-1)}, \\
p_{c0} &= \frac{(p_c^N)(p_c^{cN})}{N(N-1)}, \\
p_{c} &= \frac{(p_c^N)(p_c^{cN-1})}{N(N-1)}.
\end{align*}
\]  

We can determine the stationary probability distribution of the pair \((S_k(n_0), S_k(n_1))\) from a set of equations similar to (A.2). For \(k = \text{mod } q\) and \(k \to \infty\), we find:

\[
\Pr\{S_k(n_0) = i, S_k(n_1) = j\} \sim a_{ij}^c,
\]

where \(a_{ij}^c\) satisfies

\[
\begin{align*}
\sum_{ij} a_{ij}^c &= 1, \\
a_{ij}^{c+1} &= p_{\square}^i \cdot a_{ij}^c \quad \text{if } i \neq c, j \neq c, \\
a_{ic}^{c+1} &= a_{ic}^{c+1} = a_{ic}^c \cdot p_{\square}^i + a_{ic}^c \cdot p_{\square}^c \quad \text{if } i \neq c, \\
a_{cc}^{c+1} &= p_{cc}^{c+1} + 2a_{cc}^c \cdot p_{\square}^c + a_{cc}^c \cdot p_{\square}^c.
\end{align*}
\]  

The solution of (A.5) turns out to be

\[
\begin{align*}
a_{ii}^c &= \frac{p_{ii}^c \cdot a_{ii}^c \cdot p_{\square}^c \cdot f\{(p_{\square}^{i+1}, p_{\square}^{c-1})\}}{1 - p_{\square}^c}, \\
a_{ij}^c &= \frac{1}{1 - p_{\square}^c} \cdot \{a_{i}^c \cdot p_{\square}^i \cdot f\{(p_{\square}^{i+1}, p_{\square}^{c-1}) + a_{i}^c \cdot p_{\square}^i \cdot f\{(p_{\square}^{i+1}, p_{\square}^{c-1})\} \text{ if } i \neq j,
\end{align*}
\]
Chapter 4

where \( p_{\Box} := \prod_{c \in A} (p_{\Box}^c) \).

Solution (A.6) holds for any simultaneous distribution of \((I_k(n_0), I_k(n_1))\) that can be expressed in \( p_{cc}, p_{\Box c}, p_c \). Indeed, we only need some obvious relations like \( p_{cc} + p_{\Box c} = p_c^2 \), \( p_{cc} + p_{\Box c} = p_c^2 \) and \( p_{cc} + 2p_{\Box c} + p_{\Box} = 1 \), but (A.4) is not used. Taking \( p_{cc} := (p_c)^2 \), \( p_{\Box c} := p_c \cdot p_{\Box} \) and \( p_{\Box} := (p_{\Box})^2 \) gives a valid distribution, corresponding to independent \( I_k(n_0) \) and \( I_k(n_1) \), each with probability \( p_c \) of writing \( c \). In this case, the cells of \( S_k \) are also independent, so \( a_{i,j}^c = (a_i^c)(a_j^c) \) for all \( c, i \) and \( j \) (which can be checked from (A.6) and (A.3)).

Again we look at (A.4). It is easy to see that

\[
\begin{align*}
p_{cc} &= (p_c)^2(1 + o(1/N)), \\
p_{\Box c} &= p_c \cdot (p_{\Box})^2(1 + o(1/N)), \\
p_{\Box} &= (p_{\Box})^2(1 + o(1/N)).
\end{align*}
\]

Now we can apply some standard asymptotics in (A.6), like

\[
\begin{align*}
p_{\Box} &= \prod_{c} (p_{\Box}^c) = \{\prod_{c} (p_{\Box}^c)\}^2 \cdot (1 + o(1/N)),
\end{align*}
\]

to find \( a_{i,j}^c = (a_i^c)(a_j^c)(1 + o(1/N)) \).

Let \( \delta_0 := \delta^4/N \) with \( \delta \) as defined in Sections 4.2.5 and 4.2.6. We can find a \( k_N \) (depending on \( p_0, \ldots, p_{q-1}, N \) and \( \delta \)) such that for \( k \geq k_N \) and \( k \equiv c \mod q \):

\[
\begin{align*}
\forall_i \quad |P_{r_(S_k(n)=i)} - a_i^c| < \delta_0, \\
\forall_{i,j} \quad |P_{r_\{S_k(n_0)=i, S_k(n_1)=j\}} - a_{i,j}^c| < \delta_0.
\end{align*}
\]

Then, with \( \mu_{k_i} := E(\phi(S_k(n)=i)) \):

\[
\begin{align*}
|\mu_{k_i} - a_i^c| &< \delta_0, \\
\text{var}(\phi(S_k(n)=i)) &\leq a_i^c(1-a_i^c) + 2\delta_0, \\
\text{cov}(\phi(S_k(n_0)=i), \phi(S_k(n_1)=i)) &= a_i^c - a_i^c \cdot a_i^c + 2\delta_0 = o(1/N) + 2\delta_0.
\end{align*}
\]
Therefore

\[
\Pr \{ S_k \not\text{ typical} \} \leq \sum_i \Pr \{ |N(i; S_k) - \mu_k i N| > (\delta - \delta_0) N \} \leq \sum_i \frac{\var N(i; S_k)}{(\delta - \delta_0)^2 N^2}.
\]

The last inequality is Čebyshev's inequality. We can write this as

\[
\frac{1}{(\delta - \delta_0)^2 N^2} \sum_i \var \{ \sum_n \phi(S_k(n) = i) \} = \frac{1}{(\delta - \delta_0)^2 N^2} \sum_i \var \{ \phi(S_k(n) = i) \} + \frac{2}{(\delta - \delta_0)^2 N^2} \sum_i \sum_{n_0 < n_1} \cov(\phi(S_k(n_0) = i), \phi(S_k(n_1) = i)) \leq \frac{N}{(\delta - \delta_0)^2 N^2} \sum_i (\sigma^2_i (1 - \sigma^2_i) + 2\delta_0) + \frac{N^2}{(\delta - \delta_0)^2 N^2} g \cdot (0(1/N) + 2\delta_0)
\]

\[
= \frac{1}{(\delta - \delta_0)^2} 0(1/N) + \frac{4q\delta_0}{(\delta - \delta_0)^2}.
\]

Since \( \delta \leq 1/2 \) and \( \delta_0 = \delta^4/N \), we find

\[
\frac{1}{(\delta - \delta_0)^2} < \frac{1}{3\delta^2} \quad \text{and} \quad \frac{4q\delta_0}{(\delta - \delta_0)^2} < \frac{1}{3\delta^2} 0(1/N).
\]

Therefore, for \( k > K_N \), \( \Pr \{ S_k \not\text{ typical} \} \) can be bounded by \( \frac{1}{\delta^3} 0(1/N) \), \( N \to \infty \).

**Appendix B**

We consider the function \( \mathcal{K} : [0,1]^2 \to \mathbb{R} \),

(B.1) \( \mathcal{K}(q) := \sum_{c \in A} \sum_i a^c_i \cdot \frac{a^c_{i+1}}{a^c_i} \cdot h(i) \)

with \( a := (a_0^0, a_0^1, \ldots, q_{q-1}) \). We also define the region \( G \),
In this appendix we will prove that
\[ \max \{ k(a) \mid a \in G \} = q \cdot \log(\zeta_0), \]
with \( \zeta_0 \) as in Definition (4.3.3). First we note that, using the definition of \( h(\cdot) \),
\[
k(a) = \sum_{c} \sum_{i \neq c} \left\{ -a_i^{c+1} \log(a_i^{c+1}) + a_i^{c+1} \log(a_i^{c}) - (a_i^{c} - a_i^{c+1}) \log(a_i^{c}) + (a_i^{c} - a_i^{c+1}) \log(a_i^{c}) \right\}.
\]
By changing the order of summation, we obtain
\[
k(a) = \sum_{i} \left\{ a_i^{i+1} \log(a_i^{i+1}) - a_i^{i} \log(a_i^{i}) \right\} - \sum_{c \neq i} \sum_{c} \left( a_i^{c} - a_i^{c+1} \right) \log(a_i^{c}) \log(a_i^{c+1})\].
\]
We define the vector \( \underline{\zeta} := (\gamma_0, \gamma_0^1, \ldots, \gamma_0^{q-1}) \) by
\[
\gamma_i^{c} := \begin{cases} 
    a_i^{c} - a_i^{c+1} & \text{if } c \neq i \\
    a_i^{c} & \text{if } c = i.
\end{cases}
\]
This implies
\[
a_i^{c} = \hat{\delta}(\gamma_i^{c}, \gamma_i^{\hat{i}}),
\]
where \( \hat{\delta}(\cdot) \) is the 'cyclic sum' defined in a way similar to the 'cyclic product' in Appendix A:
\[
\hat{\delta}(\gamma_i^{c}, \gamma_i^{\hat{i}}) := \begin{cases} 
    \gamma_i^{c} + \gamma_i^{c+1} + \ldots + \gamma_i^{\hat{i}} & \text{if } c \leq i \\
    \gamma_i^{c} + \gamma_i^{c+1} + \ldots + \gamma_i^{q-1} + \gamma_i^{0} + \ldots + \gamma_i^{\hat{i}} & \text{if } c > i.
\end{cases}
\]
Now (B.4) yields: \( k(a) = k^*(\underline{\zeta}), \) with
\[
k^*(\underline{\zeta}) = \sum_{i} \sum_{c} \gamma_i^{c} \cdot \log(\gamma_i^{c}) - \sum_{i} \sum_{c} \gamma_i^{c} \log(\gamma_i^{c}).
\]
The set of restrictions \( G \) in (B.2) translates to \( G^* \),
(B.6) \( g^* = \{ z \in [0,1]^2 \mid \forall c \in A \sum_{i \in A} \hat{E}(\gamma_i^c,\gamma_i^z) = 1 \} \).

Now we have to find the maximum of \( \mathbb{E}^* \) over the region \( G^* \). Since \( G^* \) is a compact region, \( \mathbb{E}^* \) has a global maximum on \( G^* \). It is easy to see that points on the border (some \( \gamma_i^c = 0 \) or \( \gamma_i^c = 1 \)) do not correspond to a global maximum: if \( \gamma_i^c = 0 \), the partial derivative \( \frac{\partial \mathbb{E}^*}{\partial \gamma_i^c} \) tends to \(+ \infty\) for \( \gamma_i^c \downarrow 0 \), so the function value increases if we increase \( \gamma_i^c \) a little at the expense of some \( \gamma_i^d > 0 \). If \( \gamma_i^c = 1 \), it can be checked that \( \mathbb{E}^*(z) < q-1 \), whereas the global maximum is larger than this (cf. Table (4.3.8)). For the interior points we use the Lagrange multiplier method. Let, for all \( c \),

\[ g_c(z) := \sum_{i \in A} \hat{E}(\gamma_i^c,\gamma_i^z) - 1. \]

Then we can write the restrictions in the form \( g_c(z) = 0 \). Therefore parameters \( \lambda_0, \lambda_1, \ldots, \lambda_{q-1} \) in \( \mathbb{R} \) exist such that

\[ \begin{cases} 
  g_c(z) = 0 & \text{for all } c \\
  \frac{\partial (\mathbb{E}^* - \sum_c \lambda_c g_c)}{\partial \gamma_j^d} = 0 & \text{for all } j \text{ and } d.
\end{cases} \]

(B.7)

Computing partial derivatives, we find

\[ \frac{\partial g_c}{\partial \gamma_j^d} = \begin{cases} 
  1 & \text{if } c \leq d \leq j \text{ or } d \leq j < c \text{ or } j < c \leq d \\
  0 & \text{otherwise},
\end{cases} \]

so (B.7) implies

(B.8) \( \log(\sum_c \gamma_j^c) - \log(\gamma_j^d) = \hat{E}(\lambda_{j+1},\lambda_d) \)

for all \( j \text{ and } d \). Multiplying by \( \gamma_j^d \) and summing over \( j \text{ and } d \) yields, with (B.5),
Chapter 4

\[ f^*(z) = \sum_{d} \sum_{j} \lambda_c \cdot \gamma_d^j = \sum_{d} \sum_{j} \lambda_c \cdot (\sum_{\gamma^c_j, \gamma^d_j}) \]

By (B.7), we have \( g_c(2) = 0 \), so

(B.9) \( f^*(z) = \sum_{c} \lambda_c \).

From (B.8) we find for all \( j \) and \( d \)

\[ \gamma_d^j = (\sum_c \gamma^c_j) \cdot 2^{-\hat{\delta}(\lambda_{j+1}, \lambda_d)} \]

Summing over \( d \) yields

\[ \sum_d \gamma_d^j = (\sum_c \gamma^c_j) \cdot \sum_d 2^{-\hat{\delta}(\lambda_{j+1}, \lambda_d)} \]

or

(B.10) \( \sum_d 2^{-\hat{\delta}(\lambda_{j+1}, \lambda_d)} = 1 \) for all \( j \).

Hence we find

\[ 1 = \sum_d 2^{-\hat{\delta}(\lambda_{j}, \lambda_d)} = \sum_{d \neq j} 2^{-\hat{\delta}(\lambda_{j+1}, \lambda_d)} + 2^{-\lambda_j} \]

\[ = 2^{-\lambda_j} \cdot \{ \sum_{d \neq j} 2^{-\hat{\delta}(\lambda_{j+1}, \lambda_d)} + 1 \} = 2^{-\lambda_j} \left( \sum_d 2^{-\hat{\delta}(\lambda_{j+1}, \lambda_d)} - \hat{\delta}(\lambda_{j+1}, \lambda_d) \right) + 1 \].

By (B.10), this equals

\[ 2^{-\lambda_j} \cdot \{ 2 - (\sum_i \lambda_i) \} \].

Therefore

(B.11) \( 2^{-\lambda_j} \cdot \{ 2 - (\sum_i \lambda_i) \} = 1 \) for all \( j \).

Clearly (B.11) can hold only if all \( \lambda_j \) are equal. We define \( \lambda \) as the common value of all \( \lambda_j \): \( \lambda_0 = \lambda_1 = \ldots = \lambda \). Substituting this in (B.10) yields
where \((d-j)\) should be considered modulo \(q\), with values in \(\{1, 2, \ldots, q\}\). Hence
\[
\sum_{d} 2^{-(d-j)\lambda} = 1 \text{ for all } j,
\]
where \((d-j)\) should be considered modulo \(q\), with values in \(\{1, 2, \ldots, q\}\). Hence
\[
\sum_{i=1}^{q} 2^{-\epsilon_{i}\lambda} = 1.
\]
Setting \(x := 2^\lambda\), we get
\[
x^{-1} + x^{-2} + \ldots + x^{-q} = 1 \text{ or } x^q - x^{q-1} - x^{q-2} - \ldots - 1 = 0.
\]
In other words,
\[
f(x) = 0 \quad x - 1
\]
with \(f(\cdot)\) as defined in (4.3.3). The real roots of this equation are the ones among \(\zeta_0, \zeta_1, \ldots, \zeta_q\) that are unequal to 1, so the solutions for \(\lambda\) are the real ones \((\neq 0)\) among \(\log(\zeta_0), \log(\zeta_1), \ldots, \log(\zeta_q)\); notice that \(\log(\zeta_0)\) is among them by (ii) of Lemma (4.3.4).

By (B.9), we have for every solution for \(\lambda\):
\[
I^*(x) = q \cdot \lambda.
\]
Each of these corresponds to a stationary point of the function \(I^*\). Obviously, the global maximum is found for the largest one among them, \(\lambda = \log(\zeta_0)\). This proves that
\[
\max \{ I^*(x) \mid x \in G^* \} = q \cdot \log(\zeta_0)
\]
which is equivalent to (B.3).
Appendix C
Here we prove that the average case 4 capacity, $c_{av}^4$, equals

$$\max \{ h(p) - h(p^2)/(1+p) \mid 0 \leq p \leq 1 \}. $$

From Theorem (4.3.7) and Definition (4.2.2.5), we see that

$$c_{av}^4 = \max \{ (h(p_0) + h(p_1) - \frac{p_0+p_1}{1-(1-p_0)(1-p_1)} \cdot h((1-p_0)(1-p_1))/2 \mid$$

$$0 \leq p_0 \leq 1, 0 \leq p_1 \leq 1 \}. $$

Letting $a := 1-p_0, \beta := 1-p_1$ and $f(a,\beta) := h(a) + h(\beta) - \frac{2\cdot a - \beta}{1-a\beta} \cdot h(a\beta)$, we find

$$c_{av}^4 = \max \{ f(a,\beta)/2 \mid 0 \leq a \leq 1, 0 \leq \beta \leq 1 \}. $$

If we can show that

$$\max \{ f(a,\beta) \mid 0 \leq a \leq 1, 0 \leq \beta \leq 1 \} = \max \{ f(a,a) \mid 0 \leq a \leq 1 \},$$

then the proof is finished. First of all, the maximum of $f(a,\beta)$ is at least $f(0.2887,0.2887) \approx 1.09177$. If $a = 0, a = 1, \beta = 0$ or $\beta = 1$, then $f(a,\beta) \leq 1$, so the maximum is not attained on the border of the region $[0,1]^2$. Hence the maximum corresponds to a point $(a,\beta)$ for which

$$\frac{\partial f}{\partial a} = 0 \text{ and } \frac{\partial f}{\partial \beta} = 0.$$

Straightforward calculus shows

$$\frac{\partial f}{\partial a} = \log(\frac{(1-a)\beta}{1-a\beta}) - (\frac{1-\beta}{1-a\beta})^2 \log(a\beta)$$

and $\frac{\partial f}{\partial \beta}$ is equal to $\frac{\partial f}{\partial a}$ with $a$ and $\beta$ interchanged. With $z := \frac{1-a}{1-a\beta}$ and $y := \frac{1-\beta}{1-a\beta}$, (C.1) yields

$$\frac{\log(1-y)}{y} = \frac{\log(1-z)}{z} = h'(x) + h'(y).$$

Let $g_1(x) := \frac{\log(1-x)}{x^2}$ and $g_2(x) := g_1(x) - h'(x)$. Then, with (C.2):

$$-172-$$
Analysis of the functions $g_1$ and $g_2$ yields the following lemmas.

(C.5) Lemma. A number $x_0 \in (0.71, 0.72)$ exists such that $g_1$ is monotonically increasing on $[0.5, x_0)$ and monotonically decreasing on $(x_0, 1)$. 

(C.6) Lemma. Function $g_2$ is monotonically increasing on $(0, 1)$ and $g_2(x) < 0$ for all $x \in (0, 1)$.

Because of (C.4) and Lemma (C.6), we have $h'(x) < 0$, so $x > 0.5$. Now assume $x < x_0$ (defined in Lemma (C.5)). Then, by (C.4) and Lemma (C.6):

$$h'(y) = g_2(x) \leq g_2(x_0) < g_2(0.72) < -2.18.$$ 

Since $h'(y)$ is decreasing in $y$, this implies $y > 0.819$. With Lemma (C.5) we have

$$g_1(y) < g_1(0.819) < -3.676.$$ 

This implies $x < 0.6$, since otherwise $g_1(x) > g_1(0.6) > -3.673$, violating (C.3).

Again, we use (C.4) and Lemma (C.6):

$$h'(y) = g_2(x) < g_2(0.6) < -3.08.$$ 

Therefore $y > 0.894$. But now find a contradiction with (C.3):

$$g_1(y) < g_1(0.894) < -4.05 < g_1(0.5) < g_1(z).$$ 

We conclude that $x \geq x_0$. Similarly we must have $y \geq x_0$. Now the equality $g_1(x) = g_1(y)$ together with the fact that $g_1$ is monotonic on $(x_0, 1)$ shows that $x = y$. It is easy to check from the definitions of $x$ and $y$ that this implies $a = \beta$. This concludes the proof.
Chapter 5: Some Connections between Write Unidirectional Memories and Two-Way Channels

5.1. Introduction: the binary WUM and the BMC

In this final chapter, we investigate some possible links between the TWCs studied in Chapters 2 and 3 and the WUM studied in Chapter 4. This search for connections was initiated by some remarkable similarities in the results for the binary WUM and the Binary Multiplying Channel defined in Example (2.1.2). The most striking resemblance is the following. We recall that the Shannon outer bound $G_o$ for the BMC equals (see (2.2.10))

$$
G_o = \{ (\beta \cdot h(\frac{1-a}{\beta}), a \cdot h(\frac{1-\beta}{a})) | 0 \leq a \leq 1, 0 \leq \beta \leq 1, a + \beta \geq 1 \}.
$$

From Theorem (4.2.2.2) it follows that the capacity region $C_{1,2}$ for cases 1 and 2 of the binary WUM equals

$$
C_{1,2} = \{ (a_0^1 \cdot h(a_1^1/a_1^0), a_0^0 \cdot h(a_0^0/a_0^1) | a_0^0 + a_1^0 = 1, a_1^1 + a_0^1 = 1, a_0^1 \geq a_0^0, a_1^1 \geq a_1^0 \}.
$$

(No 'co' is necessary, since it turns out that the region is convex.) If we take $a_0^1 = a$ and $a_0^0 = \beta$, we find that region $C_{1,2}$ equals $G_o$. Furthermore Theorem (4.2.2.4) yields the following expression for the case 3 capacity region $C_3$:

$$
C_3 = \{ (h(p_0) \cdot \{1 - \frac{p_0(1-p_1)}{1-(1-p_0)(1-p_1)}\}, h(p_1) \cdot \{1 - \frac{p_1(1-p_0)}{1-(1-p_0)(1-p_1)}\}) | 0 \leq p_0 \leq 1, 0 \leq p_1 \leq 1 \}
$$
Summarizing, we see that the Shannon outer bound for the BMC equals the capacity region for the binary WUM in cases 1, 2 and 3. By looking more closely at the expressions for the outer bound and capacity region, respectively, we can show why this equality is not purely 'coincidental'.

As derived in Chapter 2, the BMC outer bound region consists of pairs \( h(Y_1), h(Y_0) \) for any distribution \( P(x_0, x_1) \). It is a well-known fact ([SCH83a]) that the points on the border of this region have \( P(0,0) = 0 \). In other words, if we use the graphical representation, the optimum resolution takes place in an L-shape \( A \) as in Figure (5.1.1). Here \( p_0 := Pr\{I_0 = 1 \mid I_1 = 1, \text{ vertex } A \} \) and \( p_1 := Pr\{I_1 = 1 \mid I_0 = 1, \text{ vertex } A \} \).

![Figure 5.1.1](image)

(5.1.1) Figure. Outer bound resolution for the BMC.

The total weight of vertex \( A \) is \( 1 - (1 - p_0)(1 - p_1) \). Therefore we find, with \( a_0 := Pr\{I_0 = 1 \mid A \} \) and \( a_1 := Pr\{I_1 = 1 \mid A \} \):

\[
\{ \left( \frac{p_1 \cdot h(p_0)}{1 - (1 - p_0)(1 - p_1)} , \frac{p_0 \cdot h(p_1)}{1 - (1 - p_0)(1 - p_1)} \right) | 0 \leq p_0 \leq 1, 0 \leq p_1 \leq 1 \}.
\]
Chapter 5

\[ 1 - p_0 = Pr\{I_0 = 0 \mid I_1 = 1, A\} = \frac{Pr\{I_0 = 0 \mid A\}}{Pr\{I_1 = 1 \mid A\}} = \frac{1 - a_0}{a_1} \]

and \[ 1 - p_1 = (1 - a_1)/a_0. \] Therefore

\[ (5.1.2) \]
\[ H(Y \mid I_1) = a_1 \cdot h(p_0) \]
\[ H(Y \mid I_0) = a_0 \cdot h(p_1) \]

with \[ a_1 = \frac{p_1}{1 - (1 - p_0)(1 - p_1)}, \]
\[ a_0 = \frac{p_0}{1 - (1 - p_0)(1 - p_1)}. \]

Now we look at the binary WUM. A typical rate point in the capacity region looks like \((H(S_1 \mid S_0), H(S_2 \mid S_1))\), which follows from the proof in Section (4.2.4). The notation is the same as in Chapter 4: \(S_k\) denotes a state and \(I_k\) denotes a filter. If we define \(p_0 := Pr(I_0 = 0)\), \(p_1 := Pr(I_1 = 1)\), \(a_0 := Pr(S_1 = 0)\) and \(a_1 := Pr(S_0 = 1)\), then we find

\[ H(S_1 \mid S_0) = a_1 \cdot h(p_0), \]
\[ H(S_2 \mid S_1) = a_0 \cdot h(p_1). \]

It remains to show that the \(a_k\) can be expressed in the \(p_k\) as in (5.1.2). To stress the similarity, we draw the distributions and relations between \(S_k\) and \(S_{k+1}\) in a figure like (5.1.1).

\[ (5.1.3) \text{ Figure. Two cycles for the binary WUM.} \]
In the figure on the left, $I_0$ is written in the L-shape; on the right $I_1$ is written. Note that the lower right-hand corner in the figure is missing because a transition $S_0 = 0 \rightarrow S_1 = 1$ is not possible in a 0-cycle. From Figure (5.1.3), we see that $a_0$ can be found from the figure on the left: $Pr\{S_1 = 0\} = a_1 \cdot Pr\{I_0 = 0\} + (1 - a_1)$, so $a_0 = a_1 p_0 + 1 - a_1$. Because of the periodicity of the binary WUM, $S_2$ must have the same distribution as $S_0$. Hence $a_1 = a_0 \cdot Pr\{I_1 = 1\} + 1 - a_0 = a_0 p_1 + 1 - a_0$.

From these two equations, we find

$$a_1 = \frac{p_1}{1 - (1 - p_0)(1 - p_1)}, \quad a_0 = \frac{p_0}{1 - (1 - p_0)(1 - p_1)}.$$

This proves that the expression for a rate point in the capacity region of the WUM is equal to expression (5.1.2) for a rate point in $G_0$.

If we compare the computations for the BMC and the WUM, it can also be made plausible why this rate point is achievable for the WUM, whereas it is only an outer bound for the rate of the BMC.

In the BMC situation, user $i$ cannot obtain information about the other user's input if he sends $I_i = 0$. Indeed, this causes an 'erasure' for his output $Y_i$.

If both users send the 'erasure causing' symbol 0 simultaneously, neither user receives any information. Hence it is not surprising that the input pair $(0, 0)$ should be avoided in optimum transmission. Clearly we cannot always avoid this pair in a strategy: if the two users are independent (which they are, initially), then the pair $(0, 0)$ will occur with positive probability. Because of this, achievability of the rate in $G_0$ cannot be guaranteed.

For the WUM, something similar holds. If $S_0 = 0$, no information can be stored in the 0-cycle: an 'erasure' occurs in the output pair $(S_0, S_1)$. Similarly, if $S_1 = 1$, we have an erasure in the output $(S_2, S_1)$ of the 1-cycle. Note, however, that the erasures cannot occur in two consecutive cycles: if we have an erasure
Chapter 5

after the 0-cycle, then $S_1 = 0$, so a positive amount of information $I(I_2)$ can be stored in the subsequent 1-cycle. Hence the 'double erasure' occurring for the BMC if $(0,0)$ is sent never occurs for the WUM, so the rate can be achieved here.

Another interesting similarity between the BMC and the WUM should be mentioned here. This involves coding for the binary case 3 WUM and for the BMC without feedback. (We will explain later what we mean by 'without feedback'.)

The best code known for the WUM in case 3, having error probability 0, achieves rate 0.52832 as mentioned in Section 4.1.3. Its parameters satisfy $M_0 = M_1 = N = 3$. The encoding functions for this code are the following (cf. [COH88]).

$$f_0(0) := (0 0 0), \quad f_0(1) := (0 0 0), \quad f_0(2) := (0 0 0),$$
$$f_1(0) := (1 1 0), \quad f_1(1) := (1 1 0), \quad f_1(2) := (1 1 0).$$

The reader may check that the pair $(S_k, S_{k+1})$ always determines the filter $I_k$ used. This code is symmetric (see Section 4.1.2); therefore we can translate the encoding functions $f_0$ and $f_1$ to one function $f$, by replacing 0 by 1 and 1 by 0 in the range of $f_0$ and replacing 0 by 1 and 1 by 0 in the range of $f_1$. Now '1' means 'write a symbol in this position' and '0' means 'leave this position unchanged'. We find

$$f: \{0,1,2\} \rightarrow \{0,1\}^3,$$
$$f(0) := (1 1 0), \quad f(1) := (1 0 1), \quad f(2) := (0 1 1).$$

Now we will show that the same code can be used for the BMC without feedback. 'No feedback' means that the two users are not allowed to look at previous output symbols $Y_0, Y_1, \ldots, Y_{n-1}$ before transmitting input symbol $I_i, n$ ($i \in \{0,1\}$, $n \in \mathbb{N}$). Therefore a code for the BMC without feedback has just two
Some Connections

encoding functions, $f_0$ and $f_1$ (as opposed to the $2^N$ functions that are needed if feedback is allowed, see Definition (2.1.6)):

$$f_i : \{0,1,2,\ldots,M_i-1\} \rightarrow \{0,1\}^N,$$

where $M_i$ is the number of messages for user $i$ and $N$ is the codeword length. The decoding functions are the same as in the case with feedback. It follows from [SHA61] that the capacity region of the BMC without feedback coincides with the Shannon inner bound region $\mathcal{G}_i$. In fact, this holds for any TWC. (Also, compare [SAL88].) However, all codes that have been found up to now obtain rates not even close to the border of $\mathcal{G}_i$.

The best code constructed up to this moment was found by Benschop [BEN90]. It has error probability 0, codeword length 3 and each user has three messages. Its encoding functions $f_0$ and $f_1$ are equal, say $f = f_0 = f_1$, where $f$ is given by (5.1.4). It can be seen from Table (5.1.5) that both users are able to determine the other user's message by looking at their own message and the output sequence, $Y$.

<table>
<thead>
<tr>
<th></th>
<th>$I_0$</th>
<th>$I_1$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$Y$</td>
<td>110</td>
<td>101</td>
</tr>
<tr>
<td></td>
<td>110</td>
<td>100</td>
</tr>
<tr>
<td>101</td>
<td>100</td>
<td>101</td>
</tr>
<tr>
<td>011</td>
<td>010</td>
<td>001</td>
</tr>
</tbody>
</table>

(5.1.5) Table. Codewords and output for the BMC without feedback.

Hence we have the surprising fact that the code given by (5.1.4) seems to
be optimum both for the zero-error WUM in case 3 and for the zero-error BMC without feedback! Unfortunately, no other (nontrivial) codes for the case 3-WUM or for the BMC without feedback could be found, so it is not clear whether this implies any connection between codes for the two channels in general. This might be an interesting topic for future research. In the rest of this chapter, however, we will go further into the first similarity noticed: that of the BMC outer bound being equal to the WUM capacity region.

5.2. The $q$-ary WUM and generalizations of the BMC

5.2.1. The $q$-ary ‘two-way channel’

Now that we have noticed a connection between the binary WUM and the BMC, we can try to transfer this connection to WUMs over higher alphabets, as studied in Section 4.2, and a possible generalization of the BMC. We have seen that the rate $H(S_c | S_{c-1})$, obtained in the $(c-1)$-cycle of the binary WUM, can be linked to the optimum information rate over the BMC from user $c+1$ to user $c$, $H(Y | I_c)$. (Note that $c+1$ should be considered modulo 2) 4. If we want to generalize this to an alphabet $\mathcal{A} = \{0, 1, \ldots, q-1\}$, then we must find a link between the rate in the $(c-1)$-cycle of the $q$-ary WUM and the rate from user $c+1$ (modulo $q$) to user $c$ over some yet to define 'generalized BMC'.

---

4 It may seem more logical to call this the information rate from user $c-1$ to user $c$. This does not make any difference in the binary case, but after generalization to a larger alphabet, it will turn out that this alternative does not represent the connection with the WUM as clearly as the other one. Since the only difference between the two possibilities is the direction of the information flow, this does not affect the theory in any way.
The above implies that such a generalized BMC, say $\mathcal{K}$, necessarily has $q$ users and that, for all $c \in A$, user $c$ wants to know the message transmitted by user $c+1$ and at the same time he wants to transmit a message to user $c-1$. For this reason, we will call such a channel a \((q\text{-}ary)\) ring channel.

Let user $c$'s input alphabet be $\mathcal{X}_c$, let his output alphabet be $\mathcal{Y}_c$. If user $c$'s input is $I_c$ and he receives output $Y_c$, then $I_c$ and $Y_c$ should tell him something about $I_{c+1}$. Hence we will assume that $Y_c$ depends on $I_c$ and $I_{c+1}$ only, in a deterministic way. Therefore, generalizing Definition (2.1.3), we assume the existence of $q$ channel functions, $f_{\mathcal{K},0}, f_{\mathcal{K},1}, \ldots, f_{\mathcal{K},q-1}$, with

$$f_{\mathcal{K},c} : \mathcal{X}_{c+1} \times \mathcal{X}_c \to \mathcal{Y}_c$$

and $f_{\mathcal{K},c}(I_{c+1}, I_c)$ is the output $Y_c$ for user $c$ if the input pair for user $c+1$ and $c$ is $(I_{c+1}, I_c)$. Now we can depict the ring channel $\mathcal{K}$ as in Figure (5.2.1.1).

\begin{center}
\begin{tikzpicture}
  \node (I-1) at (0,0) {$I_{c-1}$};
  \node (I-0) at (1,0) {$I_0$};
  \node (I+1) at (2,0) {$I_1$};
  \node (I+2) at (3,0) {$I_2$};
  \node (Y-1) at (0,-1) {$Y_{c-1}$};
  \node (Y-0) at (1,-1) {$Y_0$};
  \node (Y+1) at (2,-1) {$Y_1$};

  \draw[->] (I-1) -- (f-K-q-1) node [midway, above] {$f_{\mathcal{K},q-1}$};
  \draw[->] (f-K-q-1) -- (I-0) node [midway, above] {$f_{\mathcal{K},0}$};
  \draw[->] (I-0) -- (Y-0) node [midway, above] {$f_{\mathcal{K},1}$};
  \draw[->] (Y-0) -- (I+1) node [midway, above] {$f_{\mathcal{K},1}$};
  \draw[->] (I+1) -- (I+2) node [midway, above] {$f_{\mathcal{K},0}$};

  \draw[->] (Y-1) -- (f-K-q-1) node [midway, below] {$f_{\mathcal{K},q-1}$};
  \draw[->] (f-K-q-1) -- (I-0) node [midway, below] {$f_{\mathcal{K},0}$};
  \draw[->] (I-0) -- (Y-0) node [midway, below] {$f_{\mathcal{K},1}$};
  \draw[->] (Y-0) -- (I+1) node [midway, below] {$f_{\mathcal{K},1}$};
  \draw[->] (I+1) -- (I+2) node [midway, below] {$f_{\mathcal{K},0}$};

\end{tikzpicture}
\end{center}

(5.2.1.1) Figure. A ring channel $\mathcal{K}$ for $q$ users.

Note that we do not consider a specific channel with fixed functions $f_{\mathcal{K},c}$. This is because we do not know the best choice for these functions yet; the BMC can be generalized in many ways, as will be shown in the next sections. We could even consider a larger class of $q$-user channels, e.g. by allowing the output for each user to depend on all $q$ input symbols. However, this generalization does not seem to have the spirit of the $q$-ary WUM: the rate of a cycle in the $q$-ary WUM depends on two consecutive states and therefore it is more natural to look at a
channel where only 'consecutive' (neighboring) users interact with each other.

Another reason for not specifying the channel yet is the fact that we have to derive an equivalent to the BMC outer bound for the ring channel, because we intend to show a link between the q-ary WUM capacity and the outer bound for the 'generalized BMC'. Since Shannon [SHA61] proved his inner and outer bound for TWCs in general, we will do the same and generalize Theorem (2.2.4) to q-ary ring channels in general. First we generalize the definitions of a code, error probability, achievability and capacity (cf. Section 2.1) to ring channels.

(5.2.1.2) Definition. Consider a q-ary ring channel $\mathcal{X}$ as described above. A code for $\mathcal{X}$ with parameters $(N, N_0, N_1, \ldots, N_{q-1})$ consists of $q \cdot N$ encoding functions $f_c, n$ ($c \in \mathcal{A}$, $n \in \{0,1, \ldots, N-1\}$) and $q$ decoding functions $g_c$, $c \in \mathcal{A}$. Function $f_c, n$,

$$f_c, n : \{0,1, \ldots, N\} \times Y_c^n \rightarrow X_c,$$

maps message $V_c$ and received sequence $Y^n_c$ for user $c$ into his next channel input $I_{c, n}$. The decoding function $g_c$,

$$g_c : \{0,1, \ldots, N\} \times Y_c^n \rightarrow \{0,1, \ldots, N_{c+1}-1\},$$

defines how user $(c+1)$'s message is estimated by user $c$: $V_{c+1} = g_c(V_c, Y^n_c)$. 

(5.2.1.3) Definition. For a code with parameters $N$ and $N_c$, $c \in \mathcal{A}$, the rate tuple $R = (R_0, R_1, \ldots, R_{q-1})$ is defined by

$$R_c := \log(N_c)/N, \ c \in \mathcal{A}.$$ 

(5.2.1.4) Definition. A rate tuple $R$ is achievable if for all $\varepsilon > 0$, a code with parameters $N$ and $N_c$ ($c \in \mathcal{A}$) exists, having error probabilities $P_{e,c}$ defined as

$$Pr\{V_c \neq V_c\}$$

for all $c$, such that

$$\log(N_c)/N > R_c - \varepsilon$$

and $P_{e,c} < \varepsilon$ for all $c \in \mathcal{A}$. 

- 182 -
Some Connections

Now we can state the equivalent of Shannon's theorem for ring channels.

(5.2.1.5) Theorem. Let, for a given ring channel,

\[ G_i := \{ x \in \mathbb{R}^q | \forall c, 0 \leq R \leq I(x_i; Y_{i-1} | x_{i-1}) \} \]

for any input distribution

\[ P(x_0, x_1, \ldots, x_q) = \prod_c P(x_c) \]

and

\[ G_o := \{ x \in \mathbb{R}^q | \forall c, 0 \leq R \leq I(x_i; Y_{i-1} | x_{i-1}) \} \] for any \( P(x_0, x_1, \ldots, x_q) \). Then all points in \( G_i \) are achievable and points outside \( G_o \) are not achievable. \( \Box \)

Proof: We start with the proof of the fact that all points in \( G_i \) are achievable. Let \( \varepsilon > 0 \) and consider a product distribution over \( (X_0, X_1, \ldots, X_{q-1}) \), i.e.,

\[ P_{X_0, X_1, \ldots, X_{q-1}}(x_0, x_1, \ldots, x_{q-1}) = P_{X_0}(x_0) \cdot P_{X_1}(x_1) \cdots P_{X_{q-1}}(x_{q-1}). \]

Define \( R_c := I(X_c; Y_{c-1} | X_{c-1}) \) for all \( c \). If we can prove that \( (R_0, R_1, \ldots, R_{q-1}) \) is an achievable rate, then, by time sharing, all points in \( G_i \) are achievable. Let \( N \in \mathbb{N} \) and define \( N_c := \lceil 2^{N(R_c - \varepsilon)} \rceil \) for all \( c \). We will consider an ensemble of codes, randomly constructed, each with parameters \( (N, N_0, N_1, \ldots, N_{q-1}) \). If we can show that at least one of these codes has \( P_{e, c} < \varepsilon \) for all \( c \), then this proves the achievability. In this proof we are going to use a well-known lemma on typicality, which can be found in any textbook on information theory. For the sake of completeness, we state this lemma (quoted from [ELG80]) below.

(5.2.1.6) Lemma. Consider a set of discrete random variables, \( z^{(1)}, z^{(2)}, \ldots, z^{(k)} \) with a probability distribution \( P(z^{(1)}, z^{(2)}, \ldots, z^{(k)}) \). Consider sequences of length \( N \) of these random variables, with distribution

\[ P_{z^{(1)}_N, z^{(2)}_N, \ldots, z^{(k)}_N} = \prod_{n=0}^{N-1} P(z^{(1)}_n, z^{(2)}_n, \ldots, z^{(k)}_n). \]

For \( \delta > 0 \), define the \( \delta \)-typical set \( A_\delta(z^{(1)}, z^{(2)}, \ldots, z^{(k)}) \) by...
Chapter 5

\[ A_\delta(z^{(1)}, z^{(2)}, \ldots, z^{(k)}) := \{ (z^{(1)}, z^{(2)}, \ldots, z^{(k)}) \mid H(S) \leq |\log P(z)/N - H(S)| < \delta \} \]

and let \( A_\delta(S) \) denote the restriction of this set to the coordinates in \( S \). Then, if \( S_1 \) and \( S_2 \) are subsets of \{\( z^{(1)}, z^{(2)}, \ldots, z^{(k)} \)\}, the following holds.

(i) \( P(A_\delta(S_1)) \geq 1 - \delta \)
(ii) \( ||A_\delta(S_1)|| = 2^N \cdot H(S_1) + o(N), \ N \to \infty \)
(iii) If \( z \in A_\delta(S_1): P(z) = 2^{-N(H(S_1) - \delta)} + o(N), \ N \to \infty \)
(iv) If \( (z_1, z_2) \in A_\delta(S_1, S_2): P(z_1 | z_2) = 2^{-N(H(S_1 | S_2) - 2\delta)} + o(N), \ N \to \infty \).

Now we define the code ensemble. Let \( \delta < \min\{\varepsilon/(2q), \varepsilon/8\} \). For \( c \in A \) and \( w_c \in \{0, 1, \ldots, n_c - 1\} \), we randomly choose words \( x_c, w_c \in X_c^N \) according to

\[ Pr\{x_c, w_c = z\} = \prod_{n=0}^{N-1} P_{x_c^n}(z_n) \]

We write this as \( P_{x_c^n}(z) \). Every code in the ensemble will correspond to a choice of these words, \( \{x_c, w_c\} \). For a fixed choice \( \{x_c, w_c\} \), the encoding function \( f_{c,n} \) maps message \( w_c \) and output sequence \( y_c^n \) to the input letter \( z_c, w_c, n \) (that is, the \( n \)th letter in \( x_c, w_c \)). Decoding function \( g_c \) maps message \( w_c \) and output \( y_c^n (= y_c^N) \) to the unique index \( \hat{w}_{c+1} \) for which \( (z_{c+1}, \hat{w}_{c+1}, z_c, w_c, y_c) \in A_\delta(I_{c+1}, I_c, y_c) \) (see the definition in Lemma (5.2.1.6)). We abbreviate \( A_\delta(I_{c+1}, I_c, y_c) \) by \( A_\delta \). If no such \( \hat{w}_{c+1} \) exists, or if more than one \( \hat{w}_{c+1} \) exists, then an error is declared.

Now that we have defined how the random code ensemble is constructed, we proceed with bounding the error probability averaged over all codes. We have

\[ \sum_{\text{code } \{x_c, w_c\}} \sum_{c \in A} Pr\{\text{code } = \{x_c, w_c\}\} \cdot Pr\{\hat{w}_c \neq w_c \mid \text{code } \{x_c, w_c\}\} \]
\begin{align*}
\sum_{c \in A} \sum_{z \in X_c} \sum_{z' \in X_{c-1}} P_{\tilde{\mathcal{X}}_c}^c (\tilde{z}) \cdot P_{\tilde{\mathcal{X}}_{c-1}}^c (\tilde{z}') \cdot \left\{ \phi((\tilde{z}, \tilde{z}', y) \notin A_\delta) + \phi(\exists \tilde{w}_c \neq 0 \left[ (\tilde{z}_c, \tilde{w}_c, \tilde{z}', y) \in A_\delta \right]) \right\} \\
\leq \sum_{c} \delta + \sum_{c} (M_c - 1) \sum_{\tilde{z}, \tilde{z}' \in X_c} \sum_{z' \in X_{c-1}} P_{\tilde{\mathcal{X}}_c}^c (\tilde{z}) \cdot P_{\tilde{\mathcal{X}}_{c-1}}^c (\tilde{z}') \cdot \left\{ \phi((\tilde{z}, \tilde{z}', y) \notin A_\delta) \right\}.
\end{align*}

The inequality in the first term follows from (i) of Lemma (5.2.1.6) and the inequality in the second term follows from the union bound. Because \( \delta < \epsilon/(2q) \), we can bound the above by

\begin{align*}
\frac{\epsilon}{2} + \sum_{c} M_c \sum_{\tilde{z}, \tilde{z}' \in X_c} P_{\tilde{\mathcal{X}}_c}^c (\tilde{z}) \cdot P_{\tilde{\mathcal{X}}_{c-1}}^c (\tilde{z}') \cdot P_y (\tilde{z}') \\
= \frac{\epsilon}{2} + \sum_{c} M_c \sum_{\tilde{z}, \tilde{z}', y : (\tilde{z}, \tilde{z}', y) \in A_\delta} P_{\tilde{\mathcal{X}}_c}^c (\tilde{z}) \cdot P_{\tilde{\mathcal{X}}_{c-1}}^c (\tilde{z}') \cdot P_y (y | \tilde{z}') \\
\leq \epsilon/2 + \sum_{c} M_c \| A_\delta \| \cdot 2^{-N(H(X_c) + H(X_{c-1}) + H(Y_{c-1} | X_{c-1}) - 4\delta) + o(N)} \\
\leq \epsilon/2 + \sum_{c} M_c \| A_\delta \| \cdot 2^{-N(H(X_c) + H(X_{c-1}) + H(Y_{c-1} | X_{c-1}) - 4\delta) + o(N)}
\end{align*}

Here (1) follows from (iii) and (iv) of Lemma (5.2.1.6) and (2) follows from the definition of \( M_c \) and by (ii) of Lemma (5.2.1.6). Since \( X_c \) and \( X_{c-1} \) are independent in the distribution \( P_{X_0, X_1, \ldots, X_{q-1}} \), and \( X_c \) and \( X_{c-1} \) determine \( Y_{c-1} \), we have

\begin{align*}
I(X_c; Y_{c-1} | X_{c-1}) + H(X_c, X_{c-1}, Y_{c-1}) - H(X_c) - H(X_{c-1}) - H(Y_{c-1} | X_{c-1}) \\
= H(Y_{c-1} | X_{c-1}) + H(X_c, X_{c-1}) - H(X_c) - H(X_{c-1}) - H(Y_{c-1} | X_{c-1}) = 0.
\end{align*}
Therefore $\sum_c P_{e,c}$ averaged over all codes can be bounded by
\[
\frac{\varepsilon}{2} + \sum_c 2^N(-\varepsilon + 4\delta) + o(N), \ N \to \infty
\]
\[
\leq \frac{\varepsilon}{2} + \sum_c 2^{-N\varepsilon/2} + o(N), \ N \to \infty
\]
\[
< \varepsilon \text{ if } N \text{ is sufficiently large.}
\]

It follows that at least one code for the ring channel exists, having the desired rate, such that $\sum_c P_{e,c} < \varepsilon$. This concludes the proof of the achievability of all rates in $G_i$.

Now we prove the converse. Consider an $(N,N_0,N_1,\ldots,N_{q-1})$ code with $P_{e,c} < \varepsilon$ for all $c$. Firstly, for fixed $c$, we have Fano's inequality (see Section 4.2.4) stating that a function $\varphi(\cdot)$ exists such that $\varphi(\varepsilon)/N \to 0$ if $\varepsilon \to 0$ and
\[
H(V_c | \hat{V}_c) < \varphi(\varepsilon).
\]
Secondly, for all $c$:
\[
\log(N_c) = H(V_c) = H(V_c | V_{c-1})
\]
since $V_c$ and $V_{c-1}$ are independent. Furthermore
\[
(5.2.1.7) \ H(V_c | V_{c-1}) = H(V_c | V_{c-1}) - H(V_c | V_{c-1}, Y_c^{N}) + H(V_c | V_{c-1}, Y_c^{N}).
\]
The third term on the right-hand side of (5.2.1.7) satisfies
\[
H(V_c | V_{c-1}, Y_c^{N}) \leq H(V_c | \hat{V}_c, V_{c-1}, Y_c^{N})
\]
\[
= H(\hat{V}_c | V_{c-1}, Y_c^{N}) + H(V_c | \hat{V}_c, V_{c-1}, Y_c^{N})
\]
\[
\leq 0 + H(V_c | \hat{V}_c)
\]
since $\hat{V}_c = g_{c-1}(V_{c-1}, Y_c^{N})$. Because of Fano's inequality, this yields
\[
H(V_c | V_{c-1}, Y_c^{N}) \leq \varphi(\varepsilon).
\]
The first two terms on the right-hand side of (5.2.1.7) amount to
Some Connections

\[ H(V_c | V_{c-1}) - H(V_c | V_{c-1}, Y_c^n) = I(V_c; Y_c^n | V_{c-1}) \]

\[ \leq H(Y_{c-1}^n | V_{c-1}) \]

\[ = \sum_n H(Y_{c-1,n} | V_{c-1}, Y_{c-1}^n) \quad \text{by the chain rule} \]

\[ \leq \sum_n H(Y_{c-1,n} | V_{c-1}, Y_{c-1}^n, X_{c-1,n}^n) \]

\[ = \sum_n H(Y_{c-1,n} | V_{c-1}, Y_{c-1}^n, X_{c-1,n}^n) \]

because \( X_{c-1,n} = f_{c-1}(V_{c-1}, Y_{c-1}^n) \). We can bound this as

\[ \sum_n H(Y_{c-1,n} | V_{c-1}, Y_{c-1}^n, X_{c-1,n}^n) \]

\[ \leq \sum_n H(Y_{c-1,n} | X_{c-1,n}) \]

\[ = \sum K_c(n), \]

if we define \( K_c(n) \) as \( H(Y_{c-1,n} | X_{c-1,n}) \) \( (= I(Y_{c-1,n}; X_{c,n} | X_{c-1,n}) \). It should be noted that \( K(n) \in G_o \), where

\[ K(n) = (K_0(n), K_1(n), \ldots, K_{q-1}(n)) \]

We have shown

\[ \log(M_c) \leq \sum_n K_c(n) + \varphi(\varepsilon) \]

and therefore, the rate of the code is bounded (componentwise) as

\[ \left( \frac{\log(M_0)}{N}, \frac{\log(M_1)}{N}, \ldots, \frac{\log(M_{q-1})}{N} \right) \leq \sum_n K(n) \Rightarrow + (\varphi(\varepsilon), \varphi(\varepsilon), \ldots, \varphi(\varepsilon)) / N. \]

Now \( \sum_n K(n) / N \in G_o \), since \( G_o \) is convex, and \( (\varphi(\varepsilon), \varphi(\varepsilon), \ldots, \varphi(\varepsilon)) / N \Rightarrow 0 \) as \( \varepsilon \to 0 \).

Hence an achievable rate cannot be an interior point of the complement of \( G_o \). \( \square \)

In the following sections, we look at a few examples of ring channels. We apply Theorem (5.2.1.5) to determine the outer bound region for each channel and we investigate whether this region is equal to the \( q \)-ary WUM capacity region.
5.2.2. The $q$–ary BMC

Perhaps the most obvious generalization of the binary multiplying channel is the 'q–ary BMC', defined as follows.

(5.2.2.1) Definition. Let $q \in \mathbb{N}$, $\mathcal{A} := \{0,1,\ldots,q-1\}$. The $q$–ary BMC is a $q$–ary ring channel $\mathcal{K}$ as described in Section 5.2.1, with

$$X_c = \{0,1\}, Y_c = \{0,1\} \text{ and } f_{X_c, Y_c}(x_{c+1}, x_c) = I_{c+1} \cdot I_c \text{ for all } c \in \mathcal{A}. \quad \Box$$

Let $G_i$ and $G_o$ be the inner and outer bound for this channel, respectively, as defined in Theorem (5.2.1.5). We find the following relations.

(5.2.2.2) $G_i = \inf \{ \ell \in \mathbb{R}^q \mid 0 \leq \ell_c \leq a_{c-1} h(a_c) \text{ for } a_c \in [0,1], \ c \in \mathcal{A} \}.$

(5.2.2.3) $G_o = \inf \{ \ell \in \mathbb{R}^q \mid 0 \leq \ell_c \leq Pr\{I_{c-1} = 1\} \cdot h(Pr\{I_c = 1\mid I_{c-1} = 1\}) \}$ for any distribution $P(x_0, x_1, \ldots, x_{q-1})$.

This follows from the fact that $H(Y_{c-1} \mid I_{c-1}) = Pr\{I_{c-1} = 1\} \cdot h(Pr\{I_c = 1\mid I_{c-1} = 1\})$ for the $q$–ary BMC. For the inner bound, this can be further simplified to $Pr\{I_{c-1} = 1\} \cdot h(Pr\{I_c = 1\})$ since $I_c$ and $I_{c-1}$ are independent in this case. Define

$G_i := \max \{ \sum_c g_c / q \mid (g_0, g_1, \ldots, g_{q-1}) \in G_i \}$ and

$G_o := \max \{ \sum_c g_c / q \mid (g_0, g_1, \ldots, g_{q-1}) \in G_o \}.$

For $q = 2$, we know that $G_i = 0.61695$ and $G_o = 0.69424$ (see Section 2.2). If $G_o$ equals the WUM capacity for case 1, 2 or 3, then we must have $G_o = 0.87915$ or $G_o = 0.87305$ for $q = 3$, according to Table (4.3.8). However, we find the following.

(5.2.2.4) Theorem. For $q = 3$, the $q$–ary BMC has $G_o = 0.69424$. \Box

Proof: see below Lemma (5.2.2.6).
This shows that the $q$-ary BMC does not have the property we were looking for, namely that its outer bound coincides with the capacity region of the $q$-ary WUM. Nevertheless it is interesting to see that the outer bound for this channel does not increase with increasing $q$, at least for $q = 2$ and $q = 3$. In fact, the author even proved that $\mathcal{C}_o = (3/4) \cdot h(2/3) = 0.68872$ for $q = 4$, so the bound really seems to decrease in $q$. We do not give the proof of the statement for $q = 4$, since it is similar to (but much longer than) the proof for $q = 3$.

For the inner bound, it is easy to see that $\mathcal{C}_i \geq 0.61695$ for all $q$ by taking $a_c = 0.70350$ for all $c$ in (5.2.2.2). Computer search showed that $\mathcal{C}_i$ is equal to $0.61695$ for $q \in \{3, 4\}$. For larger $q$, there are too many parameters involved to be certain that the computer program found the global maximum over the region $\mathcal{C}_i$. The above observations lead us to the following conjecture.

**(5.2.2.5) Conjecture.** For all $q \geq 2$, the $q$-ary BMC has

$$\mathcal{C}_i = 0.61695 \quad \text{and} \quad \mathcal{C}_o \leq 0.69424.$$  

Now we give the proof of Theorem (5.2.2.4). We will use some properties of the entropy function in this proof that will also be applicable in Section 5.2.3. Therefore we will state these properties in a lemma.

**(5.2.2.6) Lemma.** Define the function $\rho$ by

$$\rho : [0, 1] \times [0, 1] \rightarrow [0, 1],$$

$$\rho(x, y) := (x+y) \cdot h\left(\frac{x}{x+y}\right) \text{ if } x+y > 0 \quad \text{and} \quad \rho(0, 0) := 0.$$  

The following holds for $\rho$.

(i) $\rho(x, y)$ is nondecreasing both in $x$ and in $y$.

(ii) For all $x_1$, $x_2$, $y_1$ and $y_2$ in $[0, 1]$:

$$\rho\left(\frac{x_1+x_2}{2}, \frac{y_1+y_2}{2}\right) \geq \rho(x_1, y_1)/2 + \rho(x_2, y_2)/2.$$  

- 189 -
Proof: (i) Since \( \rho(x,y) = -x \cdot \log(x) - y \cdot \log(y) + (x+y) \cdot \log(x+y) \), we have
\[
\frac{\partial \rho(x,y)}{\partial x} = \log\left(\frac{x+y}{x}\right) \geq 0 \text{ for } x > 0.
\]
Therefore \( \rho(x,y) \) is nondecreasing in \( x \). Because \( \rho(x,y) = \rho(y,x) \), it immediately follows that \( \rho(x,y) \) is nondecreasing in \( y \) as well.

(ii) For given \( x_1, x_2, y_1 \) and \( y_2 \) (not all 0), let \( \theta := \frac{x_1+y_1}{x_1+x_2+y_1+y_2} \). Then \( \theta \in [0,1] \). Since it is well-known that \( h(\cdot) \) is a convex-\( \alpha \) function, we find
\[
h(\theta \cdot \frac{x_1}{x_1+y_1} + (1-\theta) \cdot \frac{x_2}{x_2+y_2}) \geq \theta \cdot h\left(\frac{x_1}{x_1+y_1}\right) + (1-\theta) \cdot h\left(\frac{x_2}{x_2+y_2}\right).
\]
Multiplying both sides of this inequality by \( \frac{x_1+x_2+y_1+y_2}{2} \) yields
\[
\rho\left(\frac{x_1+x_2}{2}, \frac{y_1+y_2}{2}\right) \geq \rho(x_1,y_1)/2 + \rho(x_2,y_2)/2.
\]
\[\square\]

Proof of Theorem (5.2.2.4): Consider a probability distribution \( P \) over \( I_0, I_1, I_2 \). Let \( P(1*) := P(100) + P(101) + P(110) + P(111) \), so \( P(1*) = P(I_0 = 1) \) for the given distribution. Similarly we define \( P(11*) \) and other probabilities. Next, we define \( R(P) := (R_0(P) + R_1(P) + R_2(P))/3 \), with
\[
R_0(P) := P(1*1) h\left(\frac{P(1*1)}{P(1**)}\right),
R_1(P) := P(1**1) h\left(\frac{P(1**1)}{P(1***)}\right),
R_2(P) := P(1***) h\left(\frac{P(1***)}{P(1***)}\right).
\]
It follows from the definition of \( G_0 \) that \( G_0 = \max \{ R(P) \mid \text{distribution } P \} \). If \( P \) is a distribution for which this maximum is achieved, then it can be seen that distribution \( P^* \), defined by
\[
P^*(x_0, x_1, x_2) := P(x_0, x_1, x_2)
\]
also achieves the maximum (since \( R_0(P^*) = R_1(P^*) \), et cetera). Applying Lemma (5.2.2.6), (ii) with \( x_1 := P(1*1) \), \( y_1 := P(0*1) \), \( x_2 := P^*(1*1) \) and \( y_2 := P^*(0*1) \),
we find
\[ I_0 \left( \frac{(P + P^*)}{2} \right) \geq I_0(P)/2 + I_0(P^*)/2. \]
Since similar relations hold for \( I_1(\cdot) \) and \( I_2(\cdot) \), we obtain
\[ I \left( \frac{(P + P^*)}{2} \right) \geq I(P)/2 + I(P^*)/2 = I(P). \]
Therefore, distribution \( (P + P^*)/2 \) also achieves the maximum. This argument shows that we may assume for the optimum distribution \( P \):
\[ P(z_0, z_1, z_2) = P(z_2, z_0, z_1) \quad \text{for all } (z_0, z_1, z_2) \in \{0,1\}^3. \]
Hence we have reduced the number of parameters \( P(z_0, z_1, z_2) \) from 8 to 4: we have \( P(000), P(001) \) (which is equal to \( P(010) \) and \( P(100) \)), \( P(011) \) (equal to \( P(101) \) and \( P(110) \)) and \( P(111) \). These parameters must satisfy
\[ P(000) + 3P(001) + 3P(011) + P(111) = 1. \]
Now \( I(P) \) can be written as
\[ I(P) = (P(001) + 2P(011) + P(111)) \cdot h(\frac{P(011) + P(111)}{P(001) + 2P(011) + P(111)}). \]
Clearly \( I(P) \) is maximum when \( P(000) = 0 \). If \( P(001) > 0 \) for the optimum distribution, then we can define the following distribution \( P^* \):
\[ P^*(z_0, z_1, z_2) := P(z_2, z_0, z_1) \quad \text{for } (z_0, z_1, z_2) \notin \{(001), (011)\}; \]
\[ P^*(001) := 0, \quad P^*(011) := P(011) + P(001). \]
Obviously \( P^* \) satisfies \( P^*(000) + 3P^*(001) + 3P^*(011) + P^*(111) = 1, \) and
\[ I(P^*) = (2P(001) + 2P(011) + P(111)) \cdot h(\frac{P(001) + P(011) + P(111)}{2P(001) + 2P(011) + P(111)}). \]
If we write \( z := P(011) + P(111) \) and \( y := P(001) + P(011) \), then the above yields (with \( \rho \) as defined in Lemma (5.2.2.6)):
\[ I(P) = \rho(z, y) \quad \text{and} \quad I(P^*) = \rho(z + P(001), y). \]
Because of (i) of Lemma (5.2.2.6), we find \( I(P^*) \geq I(P) \). Therefore we may
assume \( P(001) = 0 \) in the optimum distribution \( P \). The function \( \mathcal{R}(P) \) reduces to

\[
\mathcal{R}(P) = (2P(011) + P(111)) \cdot h\left(\frac{P(011) + P(111)}{2P(011) + P(111)}\right)
\]

\[
= (1 - P(011)) \cdot h\left(\frac{P(011)}{1 - P(011)}\right).
\]

Here we used \( 3P(011) + P(111) = 1 \) and \( h(p) = h(1 - p) \). Now it is easy to verify (as in the binary case) that the maximum of \( \mathcal{R}(P) \) is taken for \( P(011) = 0.27639 \), \( P(111) = 0.17082 \) and that the maximum value is 0.69424.

\[\square\]

5.2.3. A \( q \)-ary ring channel resembling the WUM

In the previous section we have seen that the \( q \)-ary BMC is not the generalization of the BMC that we hoped to find. In fact, if we compare expression (4.2.2.1) and expression (5.2.2.3), we could have expected that the outer bound \( \mathcal{G}_o \) of the \( q \)-ary BMC does not equal the capacity region of the WUM in case 1 and 2. Since each component of a rate tuple in capacity region \( C_1 \) is the sum of \( q - 1 \) terms and each component of a point in \( \mathcal{G}_o \) consists of just one term, it is not surprising that the regions are equal for \( q = 2 \) but not for larger values of \( q \).

Let us try to find a ring channel \( K \) for which the outer bound expression

\[ I(I_{c-1}; Y_{c-1} | I_c) \]

(as found in Theorem (5.2.1.5)) can be written as the sum of \( q - 1 \) terms, like

\[ I_c = \sum_{i \in \mathcal{A} \setminus \{c\}} \alpha_i c \cdot h\left(\frac{a_i^{c+1}}{a_i^c}\right). \]

For every deterministic ring channel, we have

\[ I(I_{c}; Y_{c-1} | I_{c-1}) = H(Y_{c-1} | I_{c-1}) \]

\[ = \sum_{i \in \mathcal{X}_{c-1}} P_{r} \{ I_{c-1} = i \} \cdot H(Y_{c-1} | I_{c-1} = i). \]

Since the WUM rate point has \( R_c = H(S_{c+1} | S_c) \) (see the discussion in the introduction to Section 5.2.1), we know that \( I_{c-1} \) should play the role of \( S_c \), the
Some Connections

state of the WUM before the c-cycle, and \( Y_{c-1} \) should correspond to \( S_{c+1} \), the state after the c-cycle. Therefore it seems promising to take \( X_c = A \) for all c.

Comparing the expression for \( H(Y_{c-1}|I_{c-1}) \) to (5.2.3.1), we see that the term \( H(Y_{c-1}|I_{c-1} = i) \) with \( i = c \) should not contribute to the entropy and that all other terms for \( i \neq c \) should be of the form

\[
Pr\{I_{c-1} = i\} \cdot h \left( \frac{Pr\{Y_{c-1} = j \text{ and } I_{c-1} = i\}}{Pr\{I_{c-1} = i\}} \right),
\]

where \( Y_{c-1} \) can assume two values (conditional to \( I_{c-1} \)).

These considerations lead us to two possible suggestions for the channel functions \( f_{K,c} \). We will call the corresponding ring channels \( K(1) \) and \( K(2) \), respectively.

\( \text{(5.2.3.2) Definition.} \) For \( q \in \mathbb{N} \) and \( A := \{0,1,\ldots,q-1\} \), we define the \( q \)-ary ring channel \( K(1) \) with alphabets \( X_c \) and \( Y_c \) and channel functions \( f_{K(1),c} \) by

\[
X_c := A, \quad Y_c := \{0,1\},
\]

\[
f_{K(1),c}(I_{c+1},I_c) := \phi(I_c \neq c+1 \text{ and } I_{c+1} = c+1). \]

\( \text{(5.2.3.3) Definition.} \) For \( q \in \mathbb{N} \) and \( A := \{0,1,\ldots,q-1\} \), we define the \( q \)-ary ring channel \( K(2) \) with alphabets \( X_c \) and \( Y_c \) and channel functions \( f_{K(2),c} \) by

\[
X_c := A, \quad Y_c := \{0,1\},
\]

\[
f_{K(2),c}(I_{c+1},I_c) := \phi(I_c \neq c+1 \text{ and } I_{c+1} = I_c). \]

It should be noted that, for \( q = 2 \), these two channels have the same partition pattern as the BMC (cf. Section 2.5) and therefore their inner and outer bounds coincide with the Shannon bounds for the BMC.
Chapter 5

For each of these channels, we now derive the expression $H(Y_{c-1} | I_{c-1})$ occurring in the outer bound. Let $H(1)$ and $H(2)$ be the expressions for channels $X(1)$ and $X(2)$, respectively. We find

\[
H(1) = \sum_{i \neq c} Pr\{I_{c-1} = i\} \cdot h(Pr\{Y_{c-1} = 1 | I_{c-1} = i\}) \\
H(2) = \sum_{i \neq c} Pr\{I_{c-1} = i\} \cdot h(Pr\{Y_{c-1} = 1 | I_{c-1} = i\})
\]

It is quite easy to show that the outer bound region of channel $X(1)$ cannot be equal to the WUM capacity region for values of $q$ larger than 2. This follows from the theorem below.

(5.2.3.4) Theorem. If we define $G_i$ and $G_o$ as the 'maximum average rates' over the inner and outer bound regions $G_i$ and $G_o$ for the channel $X(1)$, similar to the definitions in Section 5.2.2, then we have $G_i = G_o = 1$ for all $q > 2$.

Proof: It follows from the expression for $H(1)$ that $G_o \leq 1$, since this implies $R_c \leq Pr\{I_{c-1} \neq c\} \leq 1$. For a rate point in the inner bound, we have

\[
R_c = \sum_{i \neq c} Pr\{I_{c-1} = i\} \cdot h(Pr\{I_c = c\}).
\]

If we take $Pr\{I_c = c\} = 1/2$ and $Pr\{I_c = c+2 \text{ (mod } q)\} = 1/2$, then it is easy to see that $R_c = 1$ for all $c$. Hence rate $(1,1,\ldots,1)$ is achievable for $q > 2$.

This theorem shows that channel $X(1)$ is a generalization of the BMC which has a quite surprising behavior. For $q = 2$, its capacity region is unknown, but for all values larger than 2, the channel is completely trivial: its capacity

- 194 -
region is equal to the unit hypercube in $q$ dimensions. Furthermore, the rate $(1,1,\ldots,1)$ can be achieved using an error–free code with $N = 2$ and $M_c = 2$ for all $c$. The latter follows from the proof of Theorem (5.2.3.4): if user $c$ transmits $c$ or $c+2$, depending on the message, then user $c-1$ can always tell the difference.

We now concentrate on channel $K(2)$ to see whether the outer bound for this channel is equal to the cases 1 and 2 — capacity region for the WUM. We define $C_i$ and $C_0$ as above, but this time for $K(2)$. Computer optimization yielded the results listed in Table (5.2.3.5). For comparison, this table also lists the maximum average rate $C_{1, av}$ for the case 1–WUM, as defined in (4.3.1). These values are the same as in Table (4.3.8).

<table>
<thead>
<tr>
<th>$q$</th>
<th>$C_i$</th>
<th>$C_0$</th>
<th>$C_{1, av}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>0.61695</td>
<td>0.69424</td>
<td>0.69424</td>
</tr>
<tr>
<td>3</td>
<td>0.73731</td>
<td>0.87915</td>
<td>0.87915</td>
</tr>
<tr>
<td>4</td>
<td>0.80298</td>
<td>0.94678</td>
<td>0.94678</td>
</tr>
</tbody>
</table>

(5.2.3.5) Table. Values of $C_i$, $C_0$ and $C_{1, av}$ for $q = 2$, 3 and 4.

Table (5.2.3.5) suggests that the outer bound $C_0$ for $K(2)$ is equal to the WUM capacity region $C_1$, at least for the maximum average rate point and for $q \leq 4$. As in Section 5.2.2, computer search could not be performed (i.e., the results were unreliable) for larger values of $q$ because of the large number of parameters. Indeed, for $q = 4$, the probability distribution $P(z_0, z_1, z_2, z_3)$ already consists of $4^4 = 256$ parameters! Computer search was possible only because this number of variables could be reduced to 57, by applying some techniques that are described below. For $q \geq 5$, not even this reduction made computations feasible.
Chapter 5

Now we will show how the number of parameters in the probability distribution can be reduced when searching for an optimum rate point. Let $q \geq 2$ and define $P(i \cdots i) := Pr\{X_0 = i\}$, et cetera, analogous to the definition in the proof of Theorem (5.2.2.4). Now the rate point in $G_o$ corresponding to this distribution, say $\mathbf{R}(P) = (\mathbb{E}_0(P), \mathbb{E}_1(P), \ldots, \mathbb{E}_{q-1}(P))$, can be written as

\begin{equation}
R_c(P) = \sum_{i \neq c} P(*)_{i \cdots i} h(i_{\cdots i}) \frac{P(*)_{i \cdots i}^{(P)}}{P(*)_{i \cdots i}}
\end{equation}

where the $i$ in $P(*)_{i \cdots i}$ is in coordinate position $c-1$ and the two $i$'s in $P(*)_{i \cdots i}$ are in positions $c-1$ and $c$.

First of all, if we want to find the maximum average rate $G_o$, we can apply exactly the same reasoning as used in the proof of Theorem (5.2.2.4) to show that the optimum $P(\cdot)$ satisfies

$P(x_0, x_1, x_2, \ldots, x_{q-1}) = P(x_{q-1}+1, x_0+1, x_1+1, \ldots, x_{q-2}+1)$

for all $(x_0, x_1, x_2, \ldots, x_{q-1}) \in \Lambda^q$. For $q = 4$, this reduced the number of parameters from 256 to 70. Further reduction to 57 parameters is possible by Theorem (5.2.3.7) below, stating that, for an optimum rate point $\mathbf{R}(P)$ in $G_o$, we may assume

$P(* \cdots c, c+1, \cdots) = 0$ if the $c+1$ is in coordinate position $c$.

(5.2.3.7) Theorem. Let $P$ be a distribution such that $\mathbf{R}(P) \in G_o$. Then there is a distribution $P^*$ such that $\mathbf{R}(P^*) \succeq \mathbf{R}(P)$ (componentwise inequality) and

$P^*(*)_{c+1, \cdots} = 0$

if the $c+1$ is in coordinate position $c$. \qed

Proof: Let $P$ be a distribution with $P(1 \cdots 0) > 0$. We will define a distribution $P^*$ for which $\mathbf{R}(P^*) \succeq \mathbf{R}(P)$ with strict inequality and $P^*(1 \cdots 0) = 0$. Let, for all $(x_0, x_1, \ldots, x_{q-1}) \in \Lambda^q$,
Some Connections

\[ P^*(x_0, x_1, \ldots, x_{q-1}) := P(x_0, x_1, \ldots, x_{q-1}) \text{ if } (x_0, x_{q-1}) \notin \{(1,0), (0,0)\}, \]

\[ P^*(1, x_1, \ldots, x_{q-2}, 0) := 0, \]

\[ P^*(0, x_1, \ldots, x_{q-2}, 0) := P(0, x_1, \ldots, x_{q-2}, 0) + P(1, x_1, \ldots, x_{q-2}, 0). \]

Clearly, \( P^* \) is a probability distribution. It satisfies

\[ P^*(*\ldots*i\ldots*) = P(*\ldots*i\ldots*) \text{ if the } i \text{ is not in position } 0 \]

and

\[ P^*(*\ldots*i\ldots*) = P(*\ldots*i\ldots*) \]

if the pair of \( i \)'s are not in positions \((0,1)\) or \((q-1,0)\). By (5.2.3.6), this yields

\[ \mathbb{E}_c(P^*) = \mathbb{E}_c(P) \text{ for } c \notin \{0,1\}. \]

For \( c = 0 \), we find

\[ \mathbb{E}_0(P^*) = \sum_{i \neq 0} P^*(\ldots i\ldots) h\left(\frac{P^*(i\ldots i)}{P^*(\ldots i\ldots)}\right). \]

It is easy to check that

\[ P^*(\ldots i\ldots) = P(\ldots i\ldots) \text{ and } P^*(i\ldots i) = P(i\ldots i) \]

for \( i \neq 0 \). Therefore \( \mathbb{E}_0(P^*) = \mathbb{E}_0(P) \). Finally,

\[ \mathbb{E}_1(P^*) = \sum_{i \neq 1} P^*(i\ldots i) h\left(\frac{P^*(i\ldots i)}{P^*(\ldots i\ldots)}\right). \]

We have

\[ P^*(i\ldots i) = P(i\ldots i) \text{ and } P^*(i\ldots i) = P(i\ldots i) \text{ for } i \neq 0, i \neq 1, \]

\[ P^*(0\ldots 0) = P(0\ldots 0) + P(1\ldots 0), \]

\[ P^*(00\ldots 0) = P(00\ldots 0) + P(10\ldots 0). \]

It follows that

\[ \mathbb{E}_1(P^*) = \sum_{i \neq 1} P^*(i\ldots i) h\left(\frac{P^*(i\ldots i)}{P^*(\ldots i\ldots)}\right) = \sum_{i \neq 0,1} P(i\ldots i) h\left(\frac{P(i\ldots i)}{P(i\ldots i)}\right) + \]

\[ + (P(0\ldots 0) + P(1\ldots 0)) h\left(\frac{P(00\ldots 0) + P(10\ldots 0)}{P(00\ldots 0) + P(10\ldots 0)}\right). \]
Define
\[ x := P(00\cdots), \quad \Delta x := P(10\cdots 0), \]
\[ y := P(0\cdots)-P(00\cdots), \quad \Delta y := P(1\cdots 0)-P(10\cdots 0). \]

Then, by Lemma (5.2.2.6):
\[ (P(0\cdots)+P(1\cdots 0))h(P(00\cdots)+P(10\cdots 0)) = \rho(x+\Delta x, y+\Delta y) \]
\[ > \rho(x, y) = P(0\cdots)h(P(00\cdots)). \]

Therefore
\[ R_1(P^*) \geq \sum_{i \neq 1} P(i\cdots)h(P(ii\cdots)) = R_1(P). \]

This proves that $R(P^*) \geq R(P)$ with strict inequality. If $P^*$ is such that $P^*(\cdots c, c+1, \cdots) > 0$ for some $c \neq 0$, then the above argument can be repeated to change $P^*$ to a new distribution $P^{**}$ having $P^{**}(\cdots c, c+1, \cdots) = 0$ and $R(P^{**}) \geq R(P^*)$, et cetera. This proves the theorem. $\square$

Theorem (5.2.3.7) is one more indication that $G_\emptyset$ and $C_1$ may be equal for all $q$, because of the following. Let $\bar{P} \in G_\emptyset$ correspond to a distribution for which

(5.2.3.8) $P(\cdots ij\cdots) = 0$ if $j \neq c, i \neq j$ and the $j$ is in position $c$.

Hence, for this distribution, $I_c = j$ implies $I_{c-1} = j$ if $j \neq c$. Now define
\[ a^c_i := Pr\{I_{c-1} = i\} \quad \text{for } i \in A, \quad c \in A. \]

Then, because of property (5.2.3.8), we have for $i \neq c$:
\[ Pr\{I_{c-1} = i \text{ and } I_c = i\} = Pr\{I_c = i\} = a^c_i + 1. \]

Consequently,
\[ R_c = \sum_{i \in A \setminus \{c\}} a^c_i \cdot h(a^{c+1}_i/a^c_i), \]

- 198 -
\[ \sum_{i \in \mathcal{A}} a_i^c = 1 \text{ for all } c \text{ and } a_i^c \geq a_i^{c+1} \text{ for } i \neq c. \]

This shows that \( \mathcal{K} \in \mathcal{C}_1 \), by Definition (4.2.2.1). Therefore, if (5.2.3.8) would hold for all points in \( \mathcal{G}_o \), we would have \( \mathcal{G}_o \subset \mathcal{C}_1 \). Now Theorem (5.2.3.7) states that, at least for \( i = c \) and \( j = c+1 \), (5.2.3.8) holds for all 'good' rate points in \( \mathcal{G}_o \).

Summarizing, we have found that the optimum points in \( \mathcal{G}_o \) have some of the properties of rate points in \( \mathcal{C}_1 \). Because of this, we conjecture that the outer bound region of \( \mathcal{K}(2) \) and the case 1-capacity region of the WUM are indeed equal and hence, that \( \mathcal{K}(2) \) is the \( q \)-ary ring channel we were looking for. We have not found a proof for this statement yet, but computer search appears to confirm the conjecture.

Our search for a generalization of the BMC with the aforementioned property has lead us to some new examples of multi-user channels. Our study of \( q \)-ary ring channels, as defined in this chapter, may be a step towards a more general theory of Shannon-like '\( q \)-way channels'.
List of Symbols

The following notational conventions are used in this thesis.

Sets are denoted with script capitals: \( \mathcal{A}, \mathcal{C}, \mathcal{G}, \mathcal{F}, \mathcal{Z}, \mathcal{V} \). A bar over such a symbol denotes the closure of the set: \( \bar{\mathcal{F}}, \bar{\mathcal{V}} \).

Constants are denoted with italic capitals: \( \Im, \mathbb{N}, \mathbb{N}, \mathbb{R} \), and indices are denoted with italic minuscules: \( c, i, j, k, n \).

Random variables and their realizations are denoted with italic capitals and the corresponding lower case letters, respectively: \( \xi, \omega, I, x, y, S, s \).

A vector of length \( N \) is denoted as \( \mathbf{z}^N \) or \( (x_0, x_1, \ldots, x_{N-1}) \) or \( (x(0), x(1), \ldots, x(N-1)) \).

If \( N = 0 \), this notation represents the empty sequence.

\( \mathbb{N}, \mathbb{R} \) and \( \mathbb{C} \) denote the sets of natural, real and complex numbers, respectively.

Here \( \mathbb{N} := \{1, 2, \ldots\} \).

Let \( X \) and \( Y \) be random variables over finite sets \( \mathcal{X} \) and \( \mathcal{Y} \) with distribution \( P_{XX} \) and marginals \( P_X \) and \( P_Y \). We denote the entropy of \( X \) as \( H(X) \):

\[
H(X) := \sum_{z \in \mathcal{X}} -P_X(z) \cdot \log(P_X(z)).
\]

The average mutual information between \( X \) and \( Y \) is denoted as \( I(X; Y) \), with

\[
I(X; Y) := \sum_{(x, y) \in \mathcal{X} \times \mathcal{Y}} P_{XY}(x, y) \cdot \log \left( \frac{P_{XY}(x, y)}{P_X(x) P_Y(y)} \right).
\]

In these expressions, the base of the logarithm is 2.

The following is a list of the most important symbols used in this thesis. The page number refers to the page where the symbol is introduced. Symbols not occurring in this list are defined in the text at the point where they are used.
symbol | page | symbol | page
---|---|---|---
\(d\) | 45, 116 | \(\phi_i(c)\) | 138, 147
\(c\) | 117 | \(\phi_k(n)\) | 75
\(z\) | 136 | \(C_i\) | 121, 127
\(a\) | 167 | \(C, C_K\) | 11
\(a_i^c\) | 127, 140, 164 | \(d(\cdot,\cdot)\) | 14
\(a_i^c\) | 165 | \(\theta\) | 76
\(a_i^c(n)\) | 135, 146 | \(f(z)\) | 153, 178
\(\beta_i^c(n)\) | 134 | \(f_N, f_{\Omega}(N), \ldots\) | 98
\(x, \gamma_i^c\) | 168 | \(f_c(\cdot)\) | 118, 120, 126
\(\zeta_0\) | 153 | \(f_{i,n}(\cdot)\) | 10, 182
\(\eta_n\) | 74 | \(f_K(\cdot,\cdot)\) | 181
\(\theta_i^c, \Theta_i\) | 24 | \(P(H)\) | 42
\(\lambda_c\) | 169 | \(P^\Omega(N)\) | 45
\(\Pi(\cdot,\cdot)\) | 164 | \(P^0(N)\) | 49
\(\rho(\cdot,\cdot)\) | 189 | \(\mathcal{F}, \mathcal{F}(N)\) | 42
\(\sigma_i(\cdot)\) | 24 | \(\mathcal{F}^0, \mathcal{F}^0(N)\) | 45
\(\Sigma\) | 168 | \(\mathcal{F}^0, \mathcal{F}^0(N)\) | 49
\(\phi(\cdot)\) | 21 | \(g_c(\cdot)\) | 118, 120, 126, 169
\(\varphi(\cdot)\) | 136 | \(g_{i}(\cdot,\cdot)\) | 10, 182
\(a_t\) | 58 | \(g_{i, o}\) | 188
\(A_0(\cdot)\) | 183 | \(g_{i}^{(N)}\) | 13
\(A\) | 7, 29, 35, 125 | \(g_{i}^{((N))}\) | 13, 188
\(A_{n,i}\) | 36 | \(h(\cdot)\) | 15
\(b(\alpha)\) | 111 | \(H(\cdot), H(\cdot | \cdot)\) | 12
\(b(N)\) | 98 | \(\bar{H}\) | 57
\(b_l\) | 76 | \(I(\cdot; \cdot | \cdot)\) | 12
\(B\) | 57 | \(I(\cdot)\) | 24
\(B(N)\) | 67 | \(\mathcal{K}\) | 6, 181
\(B, B(N)\) | 68 | \(\mathcal{K}(N)\) | 13
\(c_0\) | 12 | \(\mathcal{L}_l\) | 58
\(C_i\) | 122 | \(\mathcal{M}_0(c), \mathcal{M}_1(c)\) | 137, 147
\(C_i, a_{\text{av}}\) | 152 | \(\mathcal{M}(A)\) | 79
symbol | page | symbol | page
---|---|---|---
$M_c$, $\bar{M}_c$ | 9, 117, 120, 126, 182 | $S_c$ | 138
$N$ | 9, 10, 116 | $t_1$, $t_2$ | 100
$\bar{N}$ | 57, 62 | $T_c$ | 129, 155
$\mathcal{N}(\cdots)$ | 129 | $u_1$, $u_2$ | 100
$\mathcal{N}_{\text{inv}}$, $\mathcal{N}_{\text{vis}}$ | 71 | $v(n)$, $v^D(n)$ | 98
$p_c^c$, $p_c$, $p_{cd}$ | 128, 161, 163 | $V(n)$ | 51
$p_{cc}$ | 163 | $V^D(n)$ | 54
$P$ | 128, 164 | $V^0(n)$ | 63
$P^*(\cdot | \cdot)$ | 6 | $V$, $V(n)$ | 53
$P_{\text{err}}(\mathcal{C})$ | 121, 127 | $V^0$, $V^D(n)$ | 54
$P(\cdot)$ | 12 | $w(A)$ | 35
$P(i^{**})$ | 190, 196 | $V_{\text{inv}}$, $V_{\text{vis}}$ | 71
$p_i$ | 78 | $V_k$, $\tilde{V}_k$ | 9, 118, 125, 182
$q$ | 125 | $x_c$, $I_c$ | 6, 181
$q_A$ | 73 | $x(c,i,j)$ | 138, 147
$q_{\text{inv}}$, $q_{\text{vis}}$ | 73 | $x_{c', \mathcal{A}}$ | 7
$r(A)$ | 35 | $x_{i,n'}$, $I_{i,n}$ | 7, 10
$\mathcal{R}$, $\mathcal{R}_c$ | 11, 121, 127, 182 | $x_{k'}$, $I_k'$ | 118, 125
$\mathcal{R}(\sigma_0, \sigma_1)$ | 34 | $\tilde{x}_i$, $\tilde{I}_i$ | 13
$\mathcal{R}_i(n)$ | 74 | $X_c$ | 6, 181
$\mathcal{R}_i(n)$ | 76 | $Y_c$, $Y_{c'}$ | 6, 181
$\mathcal{R}_{\text{av}}$ | 122, 152 | $Y_{c'}$, $Y_{c'}$ | 7, 182
$\mathcal{R}_{\text{inv}}$, $\mathcal{R}_{\text{vis}}$ | 71 | $y_{i,n'}$, $Y_{i,n}$ | 7
$\mathcal{R}_{\text{vis}}(\mathcal{T})$ | 67 | $\mathcal{U}_N(A)$ | 37
$\mathcal{R}(n)$, $\mathcal{R}_c(n)$ | 74, 135, 146 | $\mathcal{Y}_i$, $\mathcal{Y}_i^N$ | 13
$\mathcal{R}(P)$, $\mathcal{R}_c(P)$ | 190, 196 | $\mathcal{Y}_c$ | 6, 181
$\mathcal{R}(\mathcal{T})$ | 36
$\mathcal{Z}_1$, $\mathcal{Z}_3$, $\mathcal{Z}_4$ | 127, 128
$\mathcal{S}_k$, $\mathcal{S}_k(n)$ | 116, 125 | $\mathcal{S}_k^N$, $\mathcal{S}_k^N(n)$ | 117, 125

- 202 -
Subject Index

Achievable, 11, 68, 121, 127, 182
alphabet, 7, 33, 70, 125
input, 6, 181
output, 6, 181
alternating, 119
area, 21

Basic interval, 24, 25, 70
basic rectangle, 24, 48
Benschop, 179
Berger, 17, 19
binary multiplying channel, 8, 174
block length, 10, 125
BMC, 8, 14, 98-109
generalized, 180
q-ary, 188-191
bootstrapping, 16, 64-66, 81
Borden, 123, 128
breadth, 57

Capacity, 1
average, 152, 172
region, 2, 11, 31, 95, 121, 127
zero-error, 97-98
Čebyshev’s inequality, 167
cell, 116, 125
channel, 1
function, 8, 181, 193
restricted, 18
T-, 8, 17, 37
ternary, 18, 30, 110
closure, 42
code, 10, 46, 182
fixed length, 60, 95
variable length, 62
zero-error, 48, 60, 99
codeword, 142
length, 10, 62, 96
Cohen, 124
compression, 70, 79-80
connected regions, 28, 38
construction, 75, 103, 123
converse, 124, 133, 145, 159, 186
convex, 11, 12, 86, 145, 187
copies of tree, 44, 56, 72, 91
correlated source coding, 69
cycle, 115, 125

Decoder, 9, 117-118
decoding function, 10, 118, 126, 182
dependence balance bound, 17
depth, 42
derived channel, 13, 22
deterministic, 8
distance, 14, 42
Dueck, 16

Encoder, 9, 117-118
encoding function, 10, 118, 126, 182
Engels, 33
entropy, 12, 50
equivalence, 32, 129
erasure, 177-178
error probability, 10, 83, 121, 140, 182
eventually error-free, 130
exponential convergence, 57

Fano, 136, 146, 159, 186
fate of a cell, 156-158
feedback, 7, 178-179
filter, 116, 125

Gaal, 32
generalized defects, 155
graphical representation, 3, 19, 21
grid, 47, 60, 92

Hagelbarger code, 64, 103
Han, 16
Hazewindus, 68
height, 57
Hekstra, 17
hole, 116

Information theory, 1
inner bound, 12, 19
input, 7, 24, 181
interval, 19
invisible vertex, 66

Jacobs, 32, 110
Jelinek, 16
jointly typical (j.t.), 140, 148

Kuznetsov, 125, 155

Labeling, 129-131
Lagrange multiplier method, 169
limiting region, 14, 88
Lormans, 110
L-shape, 54, 104, 177

— 203 —
Markov chain, 71, 112, 134, 145, 163
Massey, 19
memoryless, 7
message, 9, 117
pair, 57, 78
set, 9
mutual information, 12, 22

Optical disc, 114
optimization, 100, 103, 123, 162
outer bound, 13, 174, 195
output, 7, 181
Ozarow, 159
Packet, 78
partition pattern, 30-33, 110, 193
partitioning, 22, 29, 55
pattern, 129
PBV, 65
periodicity, 73, 119, 134
Pólya theory, 32
possible bootstrap vertex, 65
product distribution, 12, 20, 183
pruning, 51
Random coding, 128, 183
rate, 4
average, 98, 110, 122, 151
of code, 11, 49, 63, 121, 182
of strategy distribution, 25
of tree, 34, 36, 49, 51
of vertex, 35
resolution, 22
ring channel, 5, 181-199
rootlike rectangle, 43-46, 53-54
Rouché, 154
Salehi, 17
Schalkwijk, 3, 16, 65, 105, 109
Shannon, 1, 6, 12, 45, 88, 182
Simonyi, 123, 124, 156
Slepian, 69
slicing, 55, 66, 69, 92
Smeets, 102, 106
source, 9, 117
state
of channel, 155
of Markov chain, 71-73, 134
of WUM, 116-117, 125
stationary distribution, 73, 135, 163
strategy, 13
distribution, 45
function, 24, 35, 47
tree, 28, 35, 87
subrectangle, 21
successor, 29
symmetrical
WUM code, 119
rate, 15, 99
strategy tree, 99, 101
Threshold, 22, 39-40, 100
Tiersma, 18
time sharing, 19, 88, 133, 139
Tolhuizen, 16, 56
transition
matrix, 6, 8
probability, 71, 163
tree, 4, 29, 42
bootstrap, 67
fixed length, 42
variable length, 42, 51
TWC, 2
two-way channel, 2, 6, 180
type assignment, 66, 92
type of filter, 116, 126
typical, 140, 183
jointly, 140, 148
rectangle, 56
state, 140, 148, 163
Uniform distribution, 24, 35, 44
unit square, 19
user, 6, 18
Van der Ham, 33
Van der Heijden, 110
Van der Leur, 103
vertex, 29
Vinck, 124
visible
depth, 66
distance, 66
rate, 67, 92
vertex, 66
Weight, 35, 71
Willems, 17, 124, 133, 136
Wolf, 69
write-unidirectional memory, 2
WUM, 2, 120, 174
binary, 114, 116
q-ary, 125-126
Wyner, 159
ZBS bound, 17
Z-channel, 124
Zhang, 17, 19
References


References


References


References


Samenvatting

Dit proefschrift behandelt twee onderwerpen uit de informatietheorie, te weten tweewegkanalen (TWC's) en schrijf-eeenrichtings-geheugens (WUM's).

Een TWC modelleert communicatie in twee richtingen: twee gebruikers willen elkaar gelijktijdig informatie sturen. Het kanaal dat zij gebruiken produceert voor elke gebruiker een (discrete) output die afhangt van beide inputs. Het kanaal is geheugenloos, maar elke gebruiker mag zijn volgende input afhankelijk van vroegere inputs en outputs. We onderzoeken hoe efficiënt dit kanaal gebruikt kan worden, d.w.z. we zoeken het capaciteitsgebied.

In het proefschrift brengen we enige 'loose' resultaten uit het verleden samen onder één theorie. We gebruiken de zogenaamde 'grafische representatie', die tweeweg-communicatie herleidt tot partitionering van het eenheidsvierkant. Dit was reeds bekend voor een voorbeeld van een TWC, het binaire 'and' kanaal (BMC), maar deze methode blijkt bruikbaar voor een grote klasse van kanalen. Hiermee is het mogelijk goede ondergrenzen aan capaciteitsgebieden af te leiden.

Een WUM is een model van een herschrijfbare optische plaat. Op zo'n plaat staat binaire informatie en in een schrijfcyclus kunnen symbolen slechts in één richting veranderd worden: ofwel nullen kunnen in enen veranderen (over de hele plaat; we noemen dit een 1–cyclus), of enen kunnen in nullen veranderen (een 0–cyclus). We nemen aan dat 0– en 1–cycli elkaar afwisselen. Ook hier vragen we naar de capaciteit: we willen zo veel mogelijk informatie opslaan op een plaat.

We onderscheiden vier gevallen, afhankelijk van de vraag of de schrijver en/of de lezer de toestand van de plaat kent vóór het schrijven. Voor elk van deze vier gevallen bepalen we de capaciteit. Voor een aantal van deze gevallen was de capaciteit al bekend; in dit proefschrift generaliseren we deze resultaten naar een algemener type WUM, namelijk de WUM over een alfabet met q symbolen. We hebben nu q verschillende (cyclisch doorlopen) schrijfacyclen. Ook hiervoor bepalen we het capaciteitsgebied, in drie van de vier gevallen. Voor geval 4 (schrijver noch lezer kent de oude toestand) geven we een binnengrens waarvan we vermoeden dat hij gelijk is aan de capaciteit.

Tenslotte leggen we een verband tussen TWC's en WUM's. Omdat het capaciteitsgebied voor twee gevallen van de binaire WUM gelijk is aan een fundamentele buitengrens aan de capaciteit van het BMC, zoeken we een generalisatie van dit fenomeen over een willekeurig alfabet. Dit geeft aanleiding tot gegeneraliseerde TWC's voor q gebruikers, waarvoor we enige eigenschappen afleiden.
Curriculum Vitæ

Ineke van Overveld was born on June 25, 1962 in Dongen, The Netherlands. After graduating from the John F. Kennedy Atheneum in Dongen, in 1980, she studied mathematics at the Eindhoven University of Technology. She received her M.Sc. degree (cum laude) in February 1986.

During the period March 1986 - September 1990 she has been with the Electrical Engineering Department of the Eindhoven University of Technology as a research assistant. In October 1990 she joined the Institute for Perception Research in Eindhoven, where she is currently working on processing and perception of images.
Stellingen

bij het proefschrift

"On the Capacity Region for Deterministic Two-Way Channels and Write-Unidirectional Memories"

W. M. C. J. van Overveld

Een $d$-dimensionale product code met geschikte afmetingen, $n_1, n_2, \ldots, n_d$, waarbij de codesymbolen cyclisch gerangschikt zijn, kan niet alleen bursts ter lengte $n_1$ corrigeren, zoals aangetoond door Bahl en Chien, maar is tevens in staat bursts ter lengte $n_1 \cdot n_2 \cdot \cdots \cdot n_s$ te corrigeren voor $s \leq d - 2$. Bovendien kan er een eenvoudig decodeeralgoritme gegeven worden voor het geval dat $d = 3$.


Bij vaste–lengte strategieën voor een tweewegkanaal neemt zowel het aantal parameters in de inputverdeling als het aantal locale maxima van de ratefunctie exponentieel toe in de bloklengte. Om deze reden zijn numerieke optimaliseringsmethoden in de praktijk niet bruikbaar bij het zoeken naar een globaal maximum.

Dit proefschrift, § 3.6.

Voor WUM codes met alfabetgrootte $q$ voor geval 2 zoals gedefinieerd in dit proefschrift, maar waarbij de volgorde van decycli door de encoder bestlist mag worden (zoals voor $q = 2$ is beschreven door Borden), is de maximale rate voor kleine bloklengte aanzienlijk groter dan bij het cyclisch doorlopen van de schrijf–cycli. Als $R(N)$ de maximale rate is bij bloklengte $N$, dan geldt:

$R(1) \geq \log(q)/N$, $R(2) \geq \log(2q - 1)/N$, $R(3) \geq \log(4q - 3)/N$, $R(4) \geq \log(6q - 5)/N$.

Voor $q = 2$ treedt hierin gelijkheid op.


Dit proefschrift, hoofdstuk 4.

Beschouw de volgende generalisatie van Tiersma’s vermoeden:

"Voor $k \in \mathbb{N}$ bevat elke 0/1 matrix met $4k$ enen een submatrix met $2k$ enen".

Als de matrix minstens $2k$ niet–lege rijen bevat, dan is deze bewering waar en is de submatrix te vormen door een aantal rijen uit de matrix te schrappen.

In zijn algemeenheid echter is de vraag of het schrappen van rijen kan leiden tot de gewenste submatrix een NP–volledig probleem.


V

Laat $N \in \mathbb{N}$, $M \in \mathbb{N}$ en $a \in [0, 1/2]$ met $M \leq \left\lfloor \frac{(1-a)N}{a} \right\rfloor$. De constructie van bepaalde binaire symmetrische WUM codes voor geval 2 (cf. Simonyi) met rate $\log(M)/N$ is equivalent met de constructie van een "goede $M$-kleuring" (cf. Berge) van de hypergraaf $(X, E)$ met

$$X := \{ x_i \in \{0, 1\}^N \mid \text{wt}(x_i) = aN \}, \quad E := \{ e_i \mid i = 1, 2, \ldots, \left\lfloor \frac{N}{a} \right\rfloor \},$$

en $e_i := \{ x_j \in X \mid (x_i, x_j) = aN \}$ waarbij $\overline{x_i}$ het complement van $x_i$ is.


VI

Het door verscheidene auteurs opgemerkte verband tussen de afname in (informa-tietheoretische) entropie van een systeem en de hiermee gepaard gaande energiedissipatie (d.w.z. de toename in thermodynamische entropie) is te beschouwen als een omzetting van "verwarring" in "verwarming".


VII

Het alfabet dat "Cyrillisch" genoemd wordt, draagt deze naam niet terecht omdat het een duidelijk andere oorsprong heeft dan het door Cyrillus ontworpen schrift.


VIII

Het aantal malen dat een vrouwelijke promovendus aan een technische universiteit bij vergissing voor vakgroepssecretaresse aangezien wordt is wellicht te verminderen door meer mannen als secretaresse in dienst te nemen.