Capacity Computation and Coding for Input-Constrained Channels

A Thesis

Submitted for the Degree of

Doctor of Philosophy

in the **Faculty of Engineering**

by

V. Arvind Rameshwar

under the Guidance of

Navin Kashyap

Electrical Communication Engineering
Indian Institute of Science
Bangalore – 560 012, INDIA

July 2023

Acknowledgments

A dissertation such as this is the work of several individuals. Foremost, in my case, are my parents, whose unconditional love and support have nurtured me into the person I am, today. My passion for the sciences and the arts, shared equally, is entirely due to the environment at home. Immediately after, in the list of people who have helped bring out this thesis, and with whom I am truly grateful to have worked, is my thesis adviser, Prof. Navin Kashyap. I have learnt enormously under him, beginning with my short stint as an undergraduate research intern, and later as a PhD student. Indeed, all the work covered here and in papers outside the scope of this thesis, have resulted from discussions with him on ideas that seemed ill-formed at the outset, but were soon moulded into interesting research directions, by his expert hands. I am certain that any career that I will pursue will be driven by the ideals, mathematical and otherwise, that he has impressed on me during the course of my PhD. I must also thank him for his continued help with my technical writing; if you, the reader, appreciates the writing in this thesis, a large part of the credit is due to Prof. Kashyap.

It has also been a wonderful experience having in-depth discussions on my research with Prof. Henry Pfister. His insightful comments and constant encouragement have resulted in works of which I am truly proud.

I thank Professors Vijay Kumar, Manjunath Krishnapur, Rajesh Sundaresan, Himanshu Tyagi, and Parimal Parag, at IISc, for their comments on my work and recommendations for further exploration. My thanks are also due to Professors Andrew Thangaraj, Adrish Banerjee, Sibi Raj Pillai, Krishna Jagannathan, and Srikrishna Bhashyam, of the IITs, for their questions and suggestions, which spurred my research

in several interesting directions. I also wish to thank Prof. Lalitha Vadlamani, of IIIT Hyderabad, and Prof. Prajakta Nimbhorkar, of CMI, for initiating me into research in the theoretical sciences, as an undergraduate student, and for the time spent on helping me with my research problems then.

My research in my PhD has also been helped on its way by illuminative discussions with Aashish Tolambiya and Nikhil Verma, both Master's students under Prof. Navin Kashyap, with whom I teamed up for research projects as part of Qualcomm Innovation Fellowships 2020 and 2022, respectively.

I am grateful to my many labmates: Shivkumar, Vinay, Praneeth, Tania, Adway, Anaswara, Puspabeethi, Supriya, and Athin, who livened up the lab, and of whose company I have several fond memories. I also thank Ms. Veena for her help with administrative tasks and for her smooth handling of all the financial paperwork related to my PhD. My thanks must also reach my several friends at IISc and at BITS Pilani, with whom I shared some of my most happy times.

It is also important that I highlight the efforts of my teachers at the Padma Seshadri Bala Bhavan school, in Chennai, towards the holistic development of the skills of their young students, and towards offering them platforms to realize their potential.

Finally, my thanks go to those masters of their craft who created everything that I have watched, read, and listened to, in these 27 years of my life. My view of the world is shaped by them.

The research work in this thesis was generously supported by a Prime Minister's Research Fellowship, from the Ministry of Education, Government of India, and by Qualcomm Innovation Fellowships India 2020 and 2022.

Abstract

The setting of the transmission of information over noisy, binary-input, memoryless channels is today well-understood, owing to the work of several information theorists, beginning with Claude Shannon. It is known that it is impossible to transmit information reliably over such channels at rates larger than the fundamental limit that is the capacity of the channel. Moreover, progress made in the last three decades has led to the construction of explicit, practically-implementable coding schemes that achieve rates arbitrarily close to the capacities of such channels. Now, suppose that the inputs of the memoryless channel are required to obey an additional constraint, which stems from physical limitations of the medium over which transmission or storage occurs. What then can be said about the fundamental limits of information transmission over such input-constrained channels, with and without decoder feedback? Is it possible to design good constrained coding schemes of high rate over these channels? If the channel introduces errors adversarially, instead of randomly, how much information can then be sent through, reliably? This dissertation explores answers to such questions.

We first derive computable lower bounds on the capacities of runlength limited (RLL) input-constrained memoryless channels, such as the binary symmetric and binary erasure channels (BSC and BEC, respectively), by considering random Markov input distributions that respect the constraint. These bounds unify well-known approaches in the literature, and extend them to the so-called input-driven finite-state channels (FSCs). For the special case of the BEC with a no-consecutive-ones input constraint, we discuss an iterative stochastic approximation algorithm that numerically

computes achievable rates that are very close to known upper bounds on the capacity of the channel. We also derive improved analytical lower bounds, for this specific channel.

Next, we consider the special case of the (d, ∞)-runlength limited (RLL) constraint, which mandates that any pair of successive 1s be separated by at least d 0s. We design explicit coding schemes, derived from Reed-Muller (RM) codes, for transmission over binary-input memoryless symmetric (BMS) channels, whose inputs respect the constraint. In particular, we provide constructions using constrained subcodes of RM codes, analytically compute their rates, and derive converse upper bounds on the rates of the largest constrained subcodes of RM codes. We also provide a Fourier-theoretic perspective on the problem of counting arbitrarily-constrained codewords in general linear codes, which can help estimate the rates achievable by using linear codes over input-constrained BMS channels. We illustrate the utility of our method using the somewhat surprising observation that for different constraints of interest, the Fourier transforms of the indicator functions of the constraints are efficiently computable.

We then shift our attention to the setting of the (d, ∞)-RLL input-constrained BEC in the presence of noiseless feedback from the decoder. We demonstrate a simple, labelling-based, zero-error feedback coding scheme, which we prove to be feedback capacity-achieving, and, as a by-product, obtain an explicit characterization of the feedback capacity. The feedback capacity thus computed is an upper bound on the non-feedback capacity of such a channel. Numerical comparisons made with upper bounds on the non-feedback capacity then reveal that that feedback increases the capacity of such a channel, at least for select values of d.

Finally, we consider the setting of an input-constrained adversarial channel, where there is an upper bound on the number of bit-flip errors that the channel can introduce, and we seek to design codes that can be recovered with zero error. We present numerical upper bounds on the sizes of the largest such codes, via a version of Delsarte's linear program. We observe that for different constraints of interest, our upper bounds beat the "generalized sphere packing bounds" that are the state-of-the-art.

Publications Based on this Thesis

Submissions to Journals

(J1) V. A. Rameshwar and N. Kashyap, "Estimating the sizes of binary error-correcting constrained codes," to appear in the IEEE Journal on Selected Areas in Information Theory, Jan. 2023.

(J2) V. A. Rameshwar and N. Kashyap, "Coding schemes based on Reed-Muller codes for (d, ∞)-RLL input-constrained channels," submitted to the IEEE Transactions on Information Theory, Oct. 2022.

Conference Papers (Accepted/Submitted)

(C1) V. A. Rameshwar and N. Kashyap, "A version of Delsarte's linear program for constrained systems," 2023 IEEE International Symposium on Information Theory (ISIT), Taipei, Taiwan. **Recipient of a Jack Keil Wolf ISIT Student Paper Award**.

(C2) V. A. Rameshwar and N. Kashyap, "Counting constrained codewords in binary linear codes via Fourier expansions," 2023 IEEE International Symposium on Information Theory (ISIT), Taipei, Taiwan.

(C3) V. A. Rameshwar and N. Kashyap, "Linear runlength-limited subcodes of Reed-Muller codes and coding schemes for input-constrained BMS channels," 2022 IEEE Information Theory Workshop (ITW), Mumbai, Nov. 6–9, 2022.

(C4) V. A. Rameshwar and N. Kashyap, "A feedback capacity-achieving coding scheme

for the (d, ∞)-RLL input-constrained binary erasure channel," 2022 IEEE International Conference on Signal Processing and Communications (SPCOM), Jul. 11–15, 2022. **Recipient of a Best Student Paper Award**.

(C5) V. A. Rameshwar and N. Kashyap, "On the performance of Reed-Muller codes over (d, ∞)-RLL input-constrained BMS channels," 2022 IEEE International Symposium on Information Theory (ISIT), Espoo, Finland, Jun. 26–Jul. 1, 2022.

(C6) V. A. Rameshwar and N. Kashyap, "Numerically computable lower bounds on the capacity of the $(1, \infty)$-RLL input-constrained binary erasure channel," 2021 National Conference on Communications (NCC), Kanpur, Jul. 27–30, 2021. **Recipient of a Best Paper Award**.

(C7) V. A. Rameshwar and N. Kashyap, "Bounds on the feedback capacity of the (d, ∞)-RLL input-constrained binary erasure channel," 2021 IEEE International Symposium on Information Theory (ISIT), Melbourne, Victoria, Australia, Jul. 12–20, 2021.

(C8) V. A. Rameshwar and N. Kashyap, "Computable lower bounds for capacities of input-driven finite-state channels," 2020 IEEE International Symposium on Information Theory (ISIT), Los Angeles, California, USA, Jun. 21–26, 2020.

Preface

All the work discussed in this thesis was done in collaboration with Prof. Navin Kashyap of the Department of ECE, IISc, Bengaluru.

Chapter 4 covers material from (C6) and (C8), on bounds on the capacities of certain input-constrained memoryless channels. Chapters 5 and 6, on coding schemes over (d, ∞)-RLL input-constrained BMS channels using Reed-Muller codes, discusses the results in (J2), which, in turn, contains the material in (C3) and (C5), in addition to more theorems and proofs. Chapters 7 and 9, which are on estimates of the sizes of error-correcting constrained codes, are based on the work in (C1) and (C2), respectively, which are contained in (J1). The material in Chapter 8, on the feedback capacity of the (d, ∞)-RLL input-constrained BEC, is from (C4), which subsumes the results in (C7).

Contents

List of Tables

List of Figures

Keywords

Input-constrained channels, finite-state channels, capacity computation, coding schemes

Notation

Sets

$\mathbb{R}$	The set of real numbers
$\mathbb{N}$	The set of natural numbers $1, 2, \ldots$
$[n]$	The set $\{1, 2, \ldots, n\}$, for $n \in \mathbb{N}$
$[a : b]$	The set $\{a, a+1, \ldots, b\}$, for $a, b \in \mathbb{N}$, with $a \leq b$
$\mathbb{F}_2$	Finite field of 2 elements $\{0, 1\}$
$\mathbb{F}_2[x_1, \ldots, x_m]$	Ring of polynomials over $\mathbb{F}_2$ in m variables
$\mathcal{S}$	State space of channel with memory
$\mathcal{X}$	Channel input alphabet
$\mathcal{Y}$	Channel output alphabet

Sequences

$a_n = O(b_n)$	$\exists c > 0$ such that $a_n < c \cdot b_n$ for all sufficiently large n
$a_n = o(b_n)$	$a_n / b_n \to 0$ as $n \to \infty$

Vectors and matrices

$\mathbf{x}, \mathbf{y}, \mathbf{u}, \mathbf{v}$	Vectors
x^N	Vector $\mathbf{x} = (x_1, \ldots, x_N)$ of length N
x_i^j	The vector $(x_i, \ldots, x_j)$, for $i \leq j$, given a vector $\mathbf{x}$
$\mathbf{x} \cdot \mathbf{y}$	Dot product $\sum_{i=1}^{n} x_i y_i$ of vectors $\mathbf{x}$ and $\mathbf{y}$
0^N and 1^N	The length-N vectors $(0, \ldots, 0)$ and $(1, \ldots, 1)$, respectively
$\mathbf{xy}$ or $(\mathbf{x} \mid \mathbf{y})$	Concatenation of vectors $\mathbf{x}$ and $\mathbf{y}$
$\mathrm{supp}(\mathbf{x})$	Support of $\mathbf{x}$, or the set of indices corresponding to nonzero entries of $\mathbf{x}$
$w(\mathbf{x})$	Hamming weight, or number of ones, in $\mathbf{x}$
$w_{\mathbf{z}}(\mathbf{x})$	Number of ones in $\mathbf{x}$ in the coordinates in $\mathrm{supp}(\mathbf{x})$
$\mathbf{e}_i^{(n)}$ or $\mathbf{e}_i$	Standard basis vector of length n, with a 1 at coordinate i, and 0s elsewhere
$\mathbf{B}_m(i)$ or $\mathbf{B}(i)$	Length-m binary representation of i, for $0 \leq i \leq 2^m - 1$
$M, G, \ldots$	Matrices
$M(i)$	The i^{th} row of matrix M
$M[j]$	The j^{th} column of matrix M

Random Variables and Events

$U, V, X, Y, Z, \ldots$	Random variables
X^n or $\mathbf{X}$	Random vectors
$P(x)$ and $P(y\|x)$	The probabilities $P_X(x)$ and $P_{Y\|X}(y\|x)$, respectively, given random variables X and Y
$\mathbb{E}[Z]$	Expectation of the random variable Z
$H(X)$ or $H(P_X)$	Entropy of the random variable X with distribution P_X
$H(X\|Y)$	Conditional entropy of X given Y
$I_P(X;Y)$ or $I(X;Y)$	Mutual information between X and Y when $X \sim P$
$X \sim \mathcal{N}(\mu, \sigma^2)$	X is a Gaussian random variable with mean μ and variance σ^2

Functions, Expressions, and Operations

$\mathbb{1}_A$	Indicator function given set A, which equals 1 at a vector $\mathbf{x}$ if $\mathbf{x} \in A$ and equals 0, otherwise
ln and $\log_2$	Logarithms to the base e and 2, respectively
$h_b(p)$	Binary entropy function that equals $-p \log_2 p - (1-p) \log_2 (1-p)$, for $p \in [0,1]$
$\exp_2(z)$	The value 2^z, for $z \in \mathbb{R}$
$\lfloor r \rfloor$ and $\lceil r \rceil$	The floor and ceiling functions, respectively
$\binom{m}{\leq r}$	The summation $\sum_{i=0}^{r} \binom{m}{i}$
$p \equiv r \pmod{n}$ or $r = \mathrm{mod}(p, n)$	If it holds that $p = qn + r$, for some integer q, for integers p, r, and n, with $n > 0$ and $1 \leq r \leq n$
$\overline{\alpha}$	Equals $1 - \alpha$, for $\alpha \in \mathbb{R}$

Chapter 1

A Layman's Introduction

Down to the dark, to the utter dark, where the blind white sea-snakes are.
There is no sound, no echo of sound, in the deserts of the deep,
Or the great grey level plains of ooze where the shell-burred cables creep.

Rudyard Kipling, The Deep-Sea Cables, 1896.

On 16 August 1858, James Buchanan, the 15th president of the United States, conveyed his fervent hope, to Queen Victoria of the United Kingdom, that the "instrument destined by Divine Providence" would prove to be a bond of "perpetual peace and friendship" between the two nations, and help "diffuse religion, civilization, liberty and law throughout the world". Interestingly, this message was transmitted through the very instrument spoken of, which was billed in a popular lithograph as "The Eighth Wonder of the World". The instrument was the great transatlantic telegraph cable [1]—a monstrosity of two and a half thousand tons of copper and iron over two thousand miles of ocean—connecting Europe to North America. Very soon, it was discovered that sustained, reliable communication through the cable was next to impossible, since the noise in the telegraph lines corrupted almost all of the message that was intended to be sent. Three weeks later, the cable lay destroyed at the bottom of the ocean, owing to efforts by Wildman Whitehouse, an amateur electrical experimenter, to boost signal quality, by blasting shocks of 2000 volts through the cable.

Through the ages, humans have tried a variety of techniques to get information across as large a landscape, as quickly, and at the same time, as reliably, as possible. Very early attempts at this included beacon fires in China and signal drums in parts of Africa, which for obvious reasons, could transmit only very select messages, any deviation from which could easily be misinterpreted. Yet another system was the "Pony Express", an American mail-service of the mid-1800s, stretching from Missouri to California, which involved a relay of horse riders, and which was still in use at around the time of the transatlantic cable. Then came the electrical telegraph, the failed deep-sea cable, Graham Bell's telephone and telephone lines. All through these times, Whitehouse's naïve methods were in play, and there was little understanding of the fundamental tradeoff between the rate, or the amount of information that can be transmitted in a given time, and the reliability of communication. This was changed in 1948, with Claude Shannon's seminal work on information theory and the fundamental limits of reliable communication, which provided a precise limiting constant for any channel (or medium of communication), called its capacity, rates beyond which would lead to unreliable information transfer, and below which it was possible to communicate extremely reliably, so long as the number of times the channel was used, escaped to infinity. The decades thereafter saw a tremendous amount of work being done in the construction of explicit coding schemes, or communication strategies, whose rates of reliable information transfer came very close to the capacity of several channels. Such codes form the backbone of cellular, satellite, and deep-space communications today.

The digital age after Shannon's work also saw rapid strides being made in storage technology, with ever-increasing demands for reliable storage of high-definition images and videos. Shannon's theory applies to storage media too, and there is hence an intrinsic tradeoff between the amount of data that can be stored on a given device, and the reliability of storage. Furthermore, the storage of data on magnetic media such as magnetic tapes, disk drives, and flash drives could lead to some data sequences being more prone to error than others. The technique of *constrained coding* was thus applied

to help alleviate such errors by only allowing the storage of (relatively error-free) sequences that obey a hard constraint. As explained in later chapters, constrained coding now has applications in wireless communication too, especially in energy-harvesting scenarios, where the receiver's battery is charged using energy from the transmitted signal.

In this thesis, we are broadly interested in the fundamental limits of constrained coding in the presence of noise. We shall also work towards explicitly designing coding schemes whose rates are comparable with estimates of the capacities of such input-constrained channels. For much of the thesis, we shall consider the setting where the noise is memoryless, in that the noise that affects a particular symbol in a transmitted word is independent of that which affects the other symbols. In the last part of the thesis, we shall also take a look at adversarial noise models, where there is a bound on the amount of noise that can corrupt a given word. The next chapter discusses these noise models in greater detail, and also puts down some questions about the transmission (or storage) of information in such settings. These questions will be refined and made more precise in later chapters, wherein we shall also attempt to address them in a rigorous manner.

Chapter 2

A Technical Introduction

In this chapter, we provide a summary of our technical contributions and lay out the organization of this thesis.

2.1 Summary of Our Contributions

Our work is chiefly concerned with the explicit determination of bounds on the capacities of, and the design of good coding schemes for, discrete memoryless channels (DMCs) with input constraints.

At first, we focus on deriving information-theoretic lower bounds on the capacities of input-constrained DMCs, via achievable rates of special *random* coding schemes. To this end, we derive lower bounds on the capacities of input-driven finite-state channels (FSCs), a broad class of channels that includes most input-constrained DMCs. Our approach is to restrict the distribution of inputs to be Markov, and employ simple information-theoretic inequalities to come up with a single-letter lower bound. We show that this bound unifies known lower bounds in the literature, and extends them to input-driven FSCs. We also explicitly evaluate our lower bound for runlength limited (RLL) input-constrained binary symmetric and binary erasure channels (BSC and BEC, respectively). We then consider the special case of the binary erasure channel (BEC) with a no-consecutive-ones input constraint. Once again, we restrict our input

distribution to be Markov, and present a numerical stochastic approximation-based algorithm for numerically computing a lower bound on the capacity. We observe that our numerical results are close to known upper bounds on the capacity of the channel, and also align with numerical sampling-based bounds in the literature. We also derive an analytical single-parameter optimization problem as a lower bound on the capacity, and demonstrate that this new bound is better than the single-letter lower bound derived earlier, specialized to this channel.

Next, our objective is to use our knowledge of estimates of the capacities, to design *explicit* coding schemes, using subcodes of Reed-Muller (RM) codes, over binary-input memoryless symmetric (BMS) channels (a class of DMCs) with a specific RLL input constraint. This constraint that we work with is the (d, ∞)-RLL constraint, which mandates that any pair of successive 1s be separated by at least d 0s. We first demonstrate a simple construction, using linear constrained subcodes of RM codes, and analytically compute its rate. For the special case when $d = 1$, we prove the existence of coding schemes using potentially non-linear subcodes that achieves larger rates than those achieved by our previous scheme. Finally, we present a new two-stage (or concatenated) constrained coding scheme, again using RM codes, which outperforms the coding schemes constructed earlier, in terms of rate.

Building on our work on designing coding schemes using RM subcodes, we then explore upper bounds on the rates of constrained subcodes of RM codes, where the constraint is once again the (d, ∞)-RLL constraint. We first show that our previous construction of a linear coding scheme is essentially rate-optimal, by deriving an upper bound on the rates of linear (d, ∞)-RLL subcodes of RM codes of rate R. We further derive upper bounds on the rates of $(1, \infty)$-RLL subcodes, not necessarily linear, of a certain canonical sequence of RM codes of rate R, using estimates of the weight distribution of RM codes. We then shift our attention to settings where the coordinates of the RM code are not ordered according to the standard ordering, and derive rate upper bounds for linear (d, ∞)-RLL subcodes in these cases as well.

Next, with the aim of generalizing our approach of using subcodes of RM codes

over input-constrained BMS channels to arbitrary constraints, we consider the problem of counting (arbitrarily-)constrained codewords in general linear codes. Using a simple identity from the Fourier analysis of Boolean functions, we transform our counting problem into a question about the structure of the dual code. We illustrate the utility of our method in providing explicit values or numerical algorithms for our counting problem, from the somewhat surprising observation that for different constraints of interest, the Fourier transform of the indicator function of the constraint is efficiently computable.

Since we would have by then acquired some knowledge about good lower bounds (via explicit constructions or existential arguments) on the capacities of input-constrained DMCs, we then turn to the problem of deriving upper bounds on the capacities. As part of our first approach, we derive upper bounds on the capacity of the BEC with the (d, ∞)-RLL input constraint, via the feedback capacity of the channel. We demonstrate a simple, labelling-based, zero-error feedback coding scheme, which we prove to be feedback capacity-achieving, and, as a by-product, obtain an explicit characterization of the feedback capacity. Moreover, we show numerically that there is a gap between the feedback capacities and dual capacity-based upper bounds on the non-feedback capacities of the (d, ∞)-RLL input constrained BEC, at least for $d = 1, 2$.

In our second approach, which is also the final contribution of this thesis, we take up the study of codes over input-constrained adversarial bit-flip or erasure channels, and consider the setting where we would like to recover the input codeword with zero error. By standard arguments in coding theory, the problem of designing error-resilient codes over such a channel is equivalent to the design of constrained codes with a large minimum Hamming distance. We present numerical upper bounds on the sizes of constrained codes with a prescribed minimum distance, by extending Delsarte's linear program (LP) to the setting of constrained codes. We also describe an equivalent LP, with fewer variables and LP constraints, obtained by symmetrizing our LP. We observe that for different constraints of interest, our upper bounds beat the generalized sphere packing upper bounds, which are the state-of-the-art.

2.2 Organization of This Thesis

We begin the thesis with a detailed description of the channel models we shall work with, in Chapter 3; we recommend that the reader reads this chapter first before moving on to the others. Chapters 4–9 in this thesis contain our main technical contributions. Each such chapter (with the exception of Chapter 6, which draws on material in Chapter 5) can be read independent of the other chapters. In order to make each such chapter self-sufficient, we have also provided a detailed introduction to the problem(s) considered in the chapter, at its beginning, and an outline of interesting questions for future work, at its end. Also, whenever appropriate, individual chapters have their own literature surveys. Moreover, in order to avoid repetition in the technical material in this thesis, we have collected oft-used notation and presented them as tables in the section on notation at the start of this thesis (pp. xiv–xvi). The thesis is concluded in Chapter 10, where some interesting open questions are discussed.

Chapter 4 contains material on information-theoretic lower bounds on capacities. Chapters 5 and Chapter 6 (to be read together), respectively, describe explicit constrained code constructions using RM codes and upper bounds on the rates of constrained subcodes of RM codes. Chapter 7 discusses work on a Fourier-analytic perspective on counting constrained codewords in binary linear codes. The material on the feedback capacity of the (d, ∞)-RLL input-constrained BEC is contained in Chapter 8. Finally, Chapter 9 contains material on good upper bounds on the sizes of error-resilient constrained codes, via a version of Delsarte's linear program.

Chapter 3

Channel Models

In this chapter, we define the input-constrained channel models that are the objects of concern in this thesis. Later chapters define generalizations of these channels, but our chief results pertain to the channels defined here.

A large part of this thesis focuses on input-constrained discrete memoryless channels. A discrete memoryless channel (DMC) is defined by a triple $(\mathcal{X}, W, \mathcal{Y})$, where $\mathcal{X}$ and $\mathcal{Y}$ are the channel input and output alphabets, respectively, and at any time $t \geq 1$, the channel produces (stochastically) an output $Y_t \in \mathcal{Y}$ from a (random) input $X_t \in \mathcal{X}$ according to the channel law

$$P_{Y_t|X_t}(y_t \mid x_t) = W(y_t \mid x_t).$$

We assume that the input alphabet $\mathcal{X}$ is finite (and is often the binary alphabet $\{0, 1\}$), and we allow the output alphabet $\mathcal{Y}$ to be potentially uncountably infinite (in this thesis, however, we shall primarily be concerned with situations where $|\mathcal{Y}| < \infty$). We let $W(\cdot|x)$ be a density function with respect to the counting measure, if $\mathcal{Y}$ is discrete, and with respect to the Lebesgue measure, if $\mathcal{Y} = \mathbb{R}$ and the output distribution is continuous. The "memoryless" nature of the channel stems from the fact that if the channel is used n times, with Y^n denoting the output sequence for an input sequence

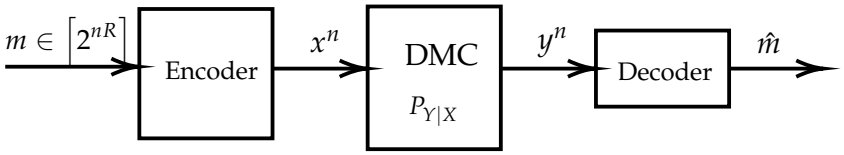


Figure 3.1: The channel model of a DMC without feedback

X^n, we have that in the absence of feedback,

$$P_{Y^n|X^n}(y^n \mid x^n) = \prod_{t=1}^{n} W(y_i \mid x_i). \tag{3.1}$$

Often, we shall refer to a DMC by just its transition probability function W. The joint distribution of inputs and outputs until time n can hence be written as

$$P_{X^n,Y^n}(x^n, y^n) = \prod_{t=1}^{n} P(x_t \mid x^{t-1}, y^{t-1}) \cdot W(y_t \mid x_t). \tag{3.2}$$

The channel model with a DMC that we consider, hence, takes a message m, which belongs to a set $\mathcal{M} = \{1, \ldots, 2^{nR}\}$ of 2^{nR} messages, for some $R \in [0, 1]$. The message is then mapped by an encoder to the input sequence x^n, of blocklength n, and is passed through the DMC W, which in turn produces the output sequence y^n, according to (3.1). The output sequence is handed over to a suitable decoder, which produces an estimate, $\hat{m}$, of the message m. Figure 3.1 shows the channel model. Note that in this case, since the encoder does not have access to the outputs received by the decoder at any time t, the conditioning on y^{t-1} within the product in (3.2) can be removed.

In this thesis, we consider DMCs whose inputs obey some additional (hard) constraints. We refer the reader to [2] for an extensive treatment of constrained systems and coding in the presence of constraints. Suppose that the constraint is represented by a set $\mathcal{A}_n \subseteq \mathcal{X}^n$ of constrained sequences, for every blocklength $n \geq 1$. Then, an input-constrained DMC without feedback is described by the setup defined above, with the added restriction that the inputs $x^n \in \mathcal{A}_n$, for all blocklengths n. The channel model with a constrained encoder is shown in Figure 3.2.

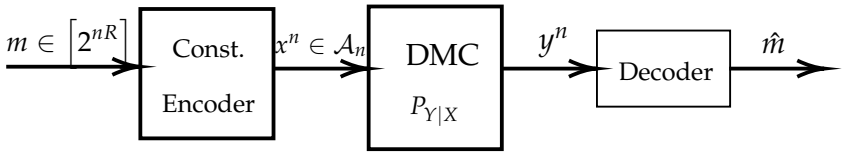


Figure 3.2: The channel model of an input-constrained DMC without feedback

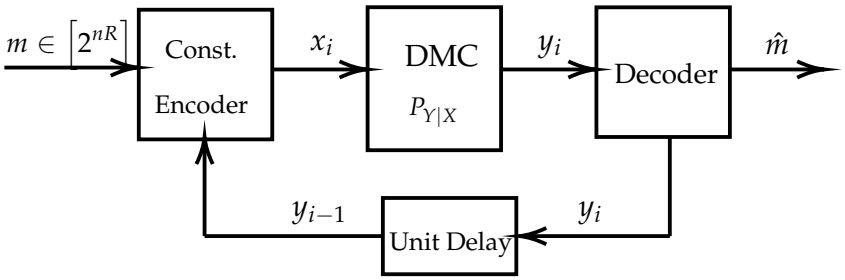


Figure 3.3: The channel model of an input-constrained DMC without feedback

Next, we consider the setting where the encoder has access to additional information from the decoder, in the form of feedback through a noiseless link. Again, in this thesis, our interest is in situations where the encoder produces only sequences that lie in some set $\mathcal{A}_n \subseteq \mathcal{X}^n$ of constrained sequences, for all $n \geq 1$. In the channel model with feedback, the constrained encoder at time i has, in addition to the message, access to noiseless feedback in the form of the outputs, y^{i-1}, from the decoder. It then produces a binary input symbol $x_i \in \mathcal{X}$, as a function of the message, m, and the outputs, y^{i-1}, in such a manner that the input sequence x^n is constrained. The inputs x^n are passed to a DMC, and decoded to an estimate $\hat{m}$, as before. The communication setting of an input-constrained memoryless channel with causal, noiseless feedback is shown in Figure 3.3.

Finally, we also consider "adversarial" (or worst-case noise) channel models, without feedback, wherein there is an upper bound on the number of symbols of the constrained input sequence (as a function of its blocklength) that the channel can corrupt. Here, we assume that the number of corrupted symbols, $e = e(n)$ is such that $\frac{e}{n} \leq p$, for some $p \in (0, 1)$. Note the contrast with the setting of the DMC wherein the errors are introduced stochastically, and for a given blocklength n, there is positive probability that all symbols in x^n are corrupted. Our interest is in the setting where the

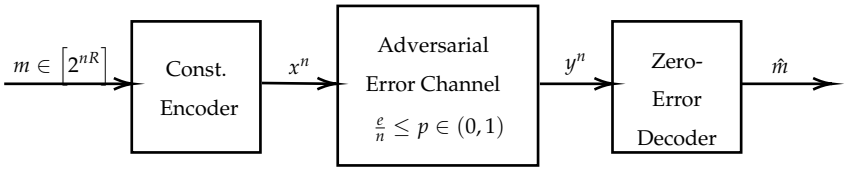


Figure 3.4: The channel model of an input-constrained adversarial channel

message that is sent, is recovered by the decoder, with zero error. Figure 3.4 shows this adversarial channel model.

Several questions, of interest to theorists and practitioners alike, can be framed with these models in place:

1. What are the fundamental limits of communication over input-constrained DMCs, with and without feedback? In particular, what can we say about the largest rate of reliable information transfer over such channels?

2. Are there explicit coding schemes achieving good rates over input-constrained DMCs, with and without feedback, which also guarantee reliable recovery of the message transmitted?

3. Can we come up with a recipe for determining the "goodness" of well-known codes for transmission over input-constrained DMCs without feedback?

4. Can we characterize the resilience of arbitrary constrained coding schemes to adversarial noise?

This dissertation is an attempt to contribute to the body of knowledge on error-correcting constrained coding, via progress made on these questions.

Chapter 4

Bounds on the Capacities of Input-Constrained Channels

"Begin at the beginning," the King said, very gravely, "and go on till you come to the end: then stop."

Lewis Caroll, Alice's Adventures in Wonderland, 1865

4.1 Introduction

In this chapter, we try to understand the fundamental limits of communication over input-constrained DMCs; in particular we shall derive estimates of the capacities of such channels. We shall, however, begin by defining a much broader class of channel models—the so-called "channels with memory" or finite-state channels (FSCs)—of which a large number of input-constrained DMCs are a part. FSCs are common mathematical models for noisy magneto-optical recording media (see, for example, [2] or [3]) and intersymbol interference and fading in wireless communications (see [4] and [5] for channel models in wireless communications). We briefly survey some well-known facts about the capacities of such channels. We then define the subclass of "input-driven" channels—the object of interest in this chapter—which includes many input-constrained DMCs. We derive some simple lower bounds on the capacities

of input-driven channels, using specific input distributions. These bounds are well-known to information theorists, and we attempt to present them in a unified manner. Next, we improve on the lower bounds for a very special case, which is that of the input-constrained binary erasure channel, whose binary inputs are required to have no consecutive ones. We present an iterative two-timescale stochastic approximation algorithm that numerically computes a lower bound, and we also provide an analytical improvement over the simple bound derived earlier.

4.2 Channel Model and Literature Survey

In this section, we define channels with memory or finite-state channels (FSCs), and review some well-known results pertaining to their capacities. For every time instant $t \geq 1$, an FSC takes as input $x_t \in \mathcal{X}$, and outputs $y_t \in \mathcal{Y}$, with the channel memory encapsulated in a "state" of the channel at time t, called s_t, which takes values in a state alphabet $\mathcal{S}$. We assume that the input and state alphabets $\mathcal{X}, \mathcal{S}$ are finite, and we allow the output alphabet $\mathcal{Y}$ to be potentially uncountably infinite. We fix an initial state $s_0 \in \mathcal{S}$, which is made known to both the encoder and the decoder, and define at each time $t \geq 1$, the (causal) FSC channel law:

$$P(s_t, y_t | x^t, s^{t-1}, y^{t-1}) = P(s_t, y_t | x_t, s_{t-1}).$$

We assume further that s_0 is known to both the encoder and the decoder. The joint distribution of inputs, outputs, and states of the FSC until time n, given the initial state s_0, hence can be written as

$$\begin{aligned} P(x^n, y^n, s^n \mid s_0) &= \prod_{t=1}^{n} P(x_t, y_t, s_t \mid x^{t-1}, y^{t-1}, s^{t-1}, s_0) \\ &= \prod_{t=1}^{n} P(x_t \mid x^{t-1}, y^{t-1}, s_0^{t-1}) \cdot P(y_t, s_t \mid x_t, s_{t-1}). \end{aligned}$$

Furthermore, for an FSC *without feedback*, since the encoder does not have access to the outputs received by the decoder at any time t, we have

$$P(x^n, y^n, s^n \mid s_0) = \prod_{t=1}^{n} P(x_t \mid x^{t-1}, s_0^{t-1}) \cdot P(y_t, s_t \mid x_t, s_{t-1}).$$

The channel model of an FSC without feedback is similar to what is shown in Figure 3.1 in Chapter 3, with the DMC replaced by an FSC. Observe that if the state space $\mathcal{S}$ were a singleton, we have that the channel is a DMC, in that the channel law obeys $P(y^n \mid x^n) = \prod_{t=1}^{n} P(y_t \mid x_t)$, with the state at all times being equal to s_0. We then define the subclass of input-driven FSCs, below:

Definition 1. *An input-driven FSC is a channel such that there exists a time-invariant function, $f : \mathcal{S} \times \mathcal{X} \to \mathcal{S}$, with $s_t = f(s_{t-1}, x_t)$, for all time instants $t \geq 1$.*

Again, the channel model for an input-driven FSC can be derived from Figure 3.1 by replacing the DMC with an input-driven FSC. Some well-known examples of input-driven FSCs are given below:

Example 1 (ISI channel)**.** *An intersymbol interference (or ISI) channel is such that for some positive integer $M > 0$, for all time instants $t \geq 1$,*

$$Y_t = \sum_{k=0}^{M} h_k \cdot X_{t-k} + Z_t,$$

where $(h_0, \ldots, h_M)$ are channel tap coefficients that are fixed (non-random) and known to the encoder and decoder, and the noise process $(Z_t)_{t\geq 1}$ is typically independent of the input process $(X_t)_{t\geq 1}$, with $Z_t \in \mathcal{Z}$, for all $t \geq 1$. Here, we assume that $(X_{-M+1}, \ldots, X_0)$ are fixed to be some $(x^\star_{-M+1}, \ldots, x^\star_0) \in \mathcal{X}^M$.

The state of the channel at time t can be taken to be $s_t = (x_t, x_{t-1}, \ldots, x_{t-M+1})$.

The next example shows that several input-constrained DMCs of Chapter 3 can be viewed as input-driven channels. We again refer the reader to [2] for definitions related to constrained systems.

Example 2 (DMCs with input constraints of finite memory)**.** *Consider a constrained system S with finite memory (equivalently, a finite-type constrained system), and let $G = G(S)$ denote a deterministic presentation of the constraint, with vertex set $\mathcal{V}$ (note that $|\mathcal{V}| < \infty$), edge set $\mathcal{E}$ and labelling function $\mathcal{L} : \mathcal{E} \to \mathcal{X}$.*

An input-constrained DMC W (see Chapter 3), with input constraint S and channel state alphabet $\mathcal{V}$ obeys

$$P(y_t, s_t \mid x_t, s_{t-1}) = \phi(s_t; (x_t, s_{t-1})) \cdot W(y_t \mid x_t),$$

where the probability on the left is undefined if there exists no outgoing edge labelled by x_t from s_{t-1}, and if otherwise, we define $\phi(s_t; (x_t, s_{t-1}))$ to be 1 if the edge $s_{t-1} \xrightarrow{x_t} s_t$ is in $\mathcal{E}$, and equals 0, otherwise. Since the state s_t is a deterministic time-invariant function of (s_{t-1}, x_t), this class of channels is a subclass of input-driven channels.

We now provide the definition of a class of constraints that we shall frequently work with: the class of (d, k)-runlength limited (RLL) constraints. We recall that for a given binary sequence $\mathbf{x}$, a run of 0s (resp. a run of 1s) is a contiguous subsequence $(x_i, x_{i+1}, \ldots, x_j)$, with $i \leq j$, all of whose symbols are 0 (resp. 1).

Definition 2. *A binary sequence $\mathbf{x} = (x_1, x_2, \ldots) \in \{0, 1\}^*$ is said to obey the (d, k)-RLL constraint, (for $0 \leq d < k \leq \infty$) if each run of 0s in $\mathbf{x}$ has length at most k, and any pair of successive 1s is separated by at least d 0s.*

It is easily verified that (d, k)-RLL input-constrained DMCs are input-driven. Indeed, this fact can be seen to be true, by taking the channel state space $\mathcal{S}$ to be $\{0, 1, 2, \ldots, d\}$ if $k = \infty$, and $\{0, 1, 2, \ldots, k\}$ if $k < \infty$. The state transitions are shown in the edge-labelled directed graphs in Figures 4.1 and 4.2: an edge $s \xrightarrow{x} s'$ represents the transition $s' = f(s, x)$.

We now turn to questions regarding the capacities of FSCs in general, and input-driven FSCs in particular. Loosely speaking, the capacity of a channel (with or without memory) is the largest rate of information transmission over the channel, such that the probability of incorrect decoding (using a suitably defined decoder) at the receiver,

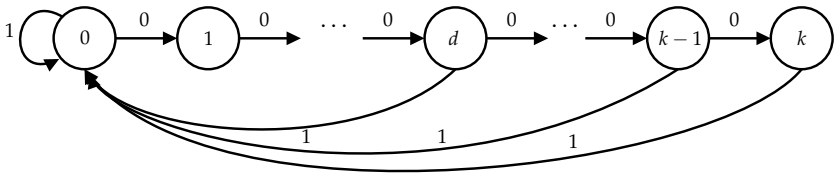


Figure 4.1: State transition graph for the (d, k)-RLL constraint, for $k < \infty$

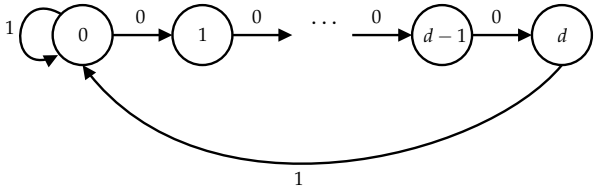


Figure 4.2: State transition graph for the (d, ∞)-RLL constraint

vanishes as the number of channel uses goes to infinity. We refer the reader to Chapters 4 and 5 of [6] and Chapter 7 in [7] for formal definitions of the capacities of channels (DMCs and FSCs) and other information-theoretic preliminaries. For FSCs as defined above, with the initial state s_0 fixed and known to both the encoder and decoder, the expression for the capacity is well-known to be the limit of the maximum mutual information rate over the channel:

Theorem 4.2.1 ([6], Ch. 4.6)**.** *The capacity of an FSC with a fixed, known, initial state s_0 is given by*

$$C = \lim_{n\to\infty} \max_{\{P(x^n|s_0)\}} \frac{1}{n} I_P(X^n; Y^n|s_0).$$

Remark 4.2.2. *The limit above exists by superadditivity (or subadditivity) arguments (see Theorem 4.6.1 in [6]). While the assumption that s_0 known to both the encoder and decoder can be removed through a suitable notion of channel indecomposability [6, (4.6.26)], we retain the assumption as it is realistic in the context of input-constrained DMCs, which is the main application of interest to us.*

For the special case of input-constrained memoryless channels, the maximization above is performed over all distributions supported on input sequences that respect the constraint.

For the special case that the FSC is in fact an unconstrained DMC, the following theorem holds:

Theorem 4.2.3 (Part II of [8], Theorem 7.7.1 in [7])**.** *The capacity of a DMC is*

$$C_{DMC} = \max_{\{P(x)\}} I_P(X;Y).$$

In what follows, we suppress the subscript 'P' in the mutual information expressions above. Observe that Shannon's formula for the capacity of an unconstrained DMC is given by an elegant, single-letter expression, but the capacity of FSCs, with the exception of special cases, is characterized only by a hard-to-compute multi-letter expression. Moreover, there exist well-known alternating maximization procedures [9, 10] for evaluating the capacities of DMCs, in contrast to the case of FSCs, where optimization procedures for evaluating the maximum mutual information rates apply to only select structured input distributions [11].

Since our objective in this chapter is to attempt to provide good approximations to the capacity in Theorem 4.2.1, for select classes of channels, it is useful to understand if the maximization domain in the expression for the capacity can be simplified, for at least select classes of channels. From Lemma 1 in [12], we note that at least for input-constrained DMCs, where the input constraint is of finite memory and is irreducible, besides (see [2]), the maximization can be carried out over the smaller class of stationary probability distributions over inputs. In fact, a more general result in this vein can be found in the work [13] by Feinstein, where it was shown that for general "finite-memory" channels with discrete inputs, of which the ISI channels and finite-memory input-constrained DMCs form a part, the capacity C is achieved by stationary, ergodic input processes. This is a useful observation to keep in mind when we attempt to derive lower bounds on the capacity, by restricting the class of input distributions. We mention that even when the inputs are restricted to be stationary and Markovian, the computation of the mutual information rate reduces to the computation of the entropy rate of a Hidden Markov process, which is a well-known hard problem.

In the context of deriving bounds on the capacity expression in 4.2.1, we mention

that there exists extensive previous literature that attempts to address the question of capacity computation. Existing work on lower bounding the capacity of FSCs includes the simulation-based approaches in [14–17]. In these approaches, the key insight is that the mutual information term in 4.2.1 is the expected value of a quantity, which, for select input distributions, can be estimated efficiently by Monte-Carlo evaluation. The technique makes use of the recursive algorithm for computing posterior probabilities in [18], to efficiently compute the posterior probabilities of channel states given long observed output sequences. Numerical methods of estimating lower bounds on the capacity also include the generalized Blahut-Arimoto algorithm developed in [11], and the stochastic approximation algorithm proposed in [19] (see also [20]). Analytical lower bounds were first derived by Zehavi and Wolf [21] for binary symmetric channels with a (d, k)-runlength-limited (RLL) constraint — see Definition 2 — at the input. Later works gave capacity lower bounds for input-constrained binary symmetric and binary erasure channels in the asymptotic (very low or very high noise) regimes [20], [22], [23].

4.3 Simple Lower Bounds

In this section, we derive simple lower bounds on the capacity expression in Theorem 4.2.1. Our lower bounds, like many of the bounds previously mentioned, are based on restricting the class of input distributions P to first-order Markov distributions supported on the channel state space. We then apply the lower bounding technique to the class of input-constrained binary symmetric channels (BSCs) and binary erasure channels (BECs). We consider the (d, k)-RLL input-constrained BSC and BEC, and provide explicit lower bounds for each of these channels. The motivation for using Markov input distributions to calculate lower bounds for such channels stems from the work in [24], which demonstrated that for general indecomposable FSCs, of which the (d, k)-RLL input-constrained DMCs form a part, the capacity can be approached arbitrarily closely using Markov input distributions of increasing order. Our techniques recover

the lower bounds given in [21] (see also Lemma 2 of [12]), for the (d,k)-RLL input-constrained BSC, for $k < \infty$. For the $(1,\infty)$-RLL input-constrained BSC and BEC, the analytical lower bounds thus found compare favourably with asymptotic lower bounds given in [20], [22] (we mention that our lower bounds for the input-constrained BEC have been stated in more generality, for all finite-type input constrained BECs, in Theorem 2.2 of [20]).

Our lower bound is presented below:

Theorem 4.3.1. *The capacity of an input-driven FSC with fixed, known, initial state is bounded below as:*

$$C \geq \sup_{\{Q(x|s)\}\in\mathcal{P}} I_Q(X;Y|S)$$

where $\mathcal{P}$ is the set of distributions $\{Q(x \mid s) : x \in \mathcal{X}, s \in \mathcal{S}\}$ such that the Markov chain on $\mathcal{S}$ induced by Q has an aperiodic, closed, communicating class containing s_0.

Proof. We have that for a fixed s_0 known to both the encoder and decoder, and for a fixed distribution $P(x^n \mid s_0)$,

$$\begin{aligned} I_P(X^n;Y^n \mid s_0) &= \sum_{t=1}^{n} I(X_t;Y^n \mid X^{t-1}, s_0) \\ &\geq \sum_{t=1}^{n} I(X_t;Y_t \mid X^{t-1}, s_0). \end{aligned} \tag{4.1}$$

Hence, via Theorem 4.2.1, we have

$$\begin{aligned} C &= \lim_{n\to\infty} \max_{\{P(x_t|x^{t-1},s_0)\}_{t=1}^n} \frac{1}{n} I(X^n;Y^n \mid s_0) \\ &\geq \lim_{n\to\infty} \max_{\{P(x_t|x^{t-1},s_0)\}_{t=1}^n} \frac{1}{n} \sum_{t=1}^{n} I(X_t;Y_t \mid X^{t-1}, s_0) \\ &= \sup_{\{P(x_t|x^{t-1})\}_{t\geq 1}} \liminf_{n\to\infty} \frac{1}{n} \sum_{t=1}^{n} I(X_t;Y_t \mid X^{t-1}), \end{aligned}$$

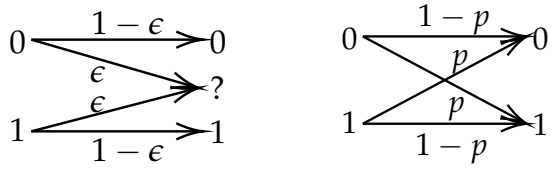
the last equality above following by the arguments in Lemma 4 of [25], the conditioning

on s_0 being suppressed in the notation. Finally, we can replace the supremum over $\{P(x_t|x^{t-1})\}_{t\geq 1}$ by a supremum over input distributions of the form $\{Q(x_t|s_{t-1})\}_{t\geq 1}$, where $Q \in \mathcal{P}$ (see the statement of the theorem), at the expense of another inequality. Hence,

$$\begin{aligned} C &\geq \sup_{\{Q(x_t|s_{t-1})\}_{t\geq 1}} \liminf_{n\to\infty} \frac{1}{n} \sum_{t=1}^{n} I(X_t; Y_t \mid X^{t-1}) \\ &= \sup_{\{Q(x_t|s_{t-1})\}_{t\geq 1}} \liminf_{n\to\infty} \frac{1}{n} \sum_{t=1}^{n} I(X_t; Y_t \mid S_{t-1}) \\ &= \sup_{\{Q(x|s)\in\mathcal{P}\}} I_Q(X; Y|S), \end{aligned}$$

where the first equality above follows since given s_0, X^{t-1} determines S_{t-1} (as the channel is input-driven) and since X_t (and hence Y_t) depends on X^{t-1} only through S_{t-1}, by the choice of input distributions being maximized over. □

We then apply Theorem 4.3.1 to runlength-limited input-constrained DMCs; in particular, input-constrained binary symmetric channels (BSCs) and binary erasure channels (BECs), shown in Figures 4.3b and 4.3a, respectively.



(a) (b)

Figure 4.3: (a) The binary erasure channel (BEC(ϵ)) with erasure probability ϵ and output alphabet $\mathcal{Y} = \{0, ?, 1\}$. (b) The binary symmetric channel (BSC(p)) with crossover probability p and output alphabet $\mathcal{Y} = \{0, 1\}$.

We obtain the following lower bounds:

- The capacity of the (d, ∞)-RLL input-constrained BSC(p) satisfies

$$C \geq \max_{a\in[0,1]} \frac{h_b(ap + \bar{a}\bar{p}) - h_b(p)}{ad + 1}.$$

This result holds for all $p \in [0,1]$, and, for $d = 1$, numerical evaluations indicate that our bound is close to the asymptotic bounds of [22] (as $p \to 0$), and of [23] (as $p \to 0.5$).

- The capacity of the (d,k)-RLL input-constrained BSC(p) obeys

$$C \geq \max_{a_d,\ldots,a_{k-1}} \frac{\sum_{i=d}^{k-1} \left(h_b(a_i p + \bar{a}_i \bar{p}) - h_b(p)\right) \prod_{j=d}^{i-1} (1-a_j)}{d+1+\sum_{i=d}^{k-1} \prod_{j=d}^{i} (1-a_j)},$$

where $a_d, \ldots, a_{k-1} \in [0,1]$. These lower bounds hold for arbitrary $0 \leq d < k < \infty$. We mention also that our lower bounds in this setting, which were also derived in [12], were shown therein to be better than the lower bounds obtained via an application of the so-called "Mrs. Gerber's lemma" [26] to lower bound the entropy rate of the output sequences from a BSC, when an arbitrary stationary source is used as the input to the channel. An extension of "Mrs. Gerber's lemma" to arbitrary binary-input symmetric channels was carried out in [27].

- For $0 \leq d < k \leq \infty$, the capacity of the (d,k)-RLL input-constrained BEC(ϵ) satisfies $C \geq \kappa_{d,k} \cdot \bar{\epsilon}$, where $\kappa_{d,k}$ is the noiseless capacity of the (d,k)-RLL constraint. In particular, when $d = 0$, the bound becomes tight as $k \to \infty$.

Remark 4.3.2. *For the input-constrained channels described above, it can easily be checked that in the zero noise regime (when $p = 0$ in the BSC and $\epsilon = 0$ in the BEC), the lower bound equals the noiseless capacity (see [2]) of the constraint. Indeed, by substituting $X = Y$ in our lower bound expression, we obtain that at zero noise, $C \geq \sup_{\{Q(x|s) \in \mathcal{P}\}} H(X \mid S) = \kappa$, where κ is the noiseless capacity of the constraint (see [2]), and the equality holds by Theorem 3.23 in [2].*

For $d = 1$, Figure 4.4 shows plots of our lower bound, alongside the lower bound of Ordentlich [23]. Upper bounds on the capacity in the form of the feedback capacity of the $(1,\infty)$-RLL input-constrained BSC(p) [89], and the dual capacity upper bound of

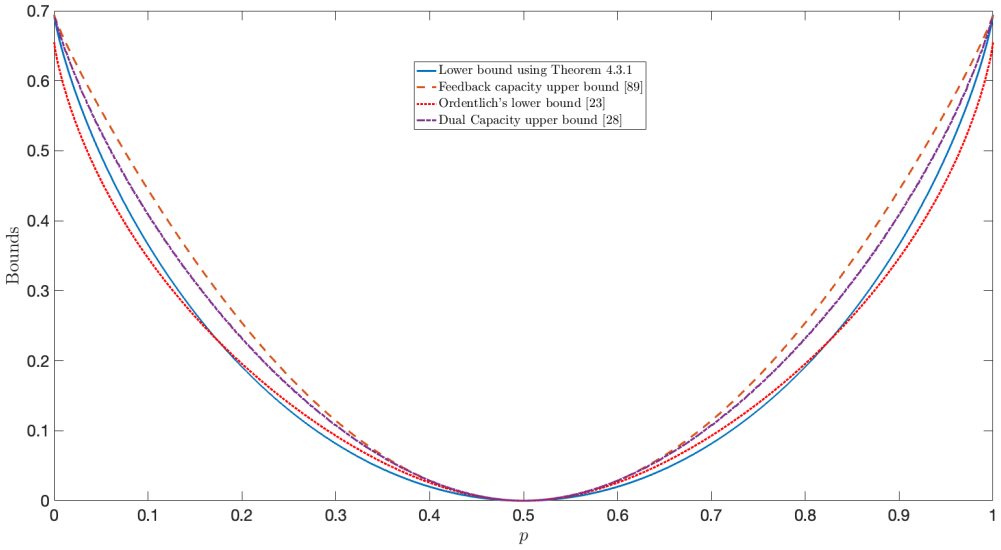


Figure 4.4: Comparison of our lower bound for the $(1,\infty)$-RLL input-constrained BSC(p) with bounds in [23], [89] and [28].

Thangaraj [28] are also shown. Numerical evaluations indicate that our lower bound is close to the asymptotic bounds in [22] as $p \to 0$, and in [23] as $p \to 0.5$. Plots of the lower bound for $d = 1, 2, 3$, are given in Figure 4.5, with the unconstrained ($d = 0$) capacity also indicated.

Figure 4.6 shows plots of the lower bound for the $(0,k)$-RLL input-constrained BSC(p), for $k = 1, 2, 3$, alongside the capacity of the unconstrained ($k \to \infty$) BSC(p). We reiterate here that our lower bound is exactly equal to that presented in Lemma 5 of [21] and Lemma 2 in [12] (assuming first-order Markov input distributions).

For the input-constrained BEC, for $d = 1$, a comparison between the lower bound and the "memory-1" dual capacity upper bound of Thangaraj [28] are shown in Figure 4.7, along with a plot of the feedback capacity [88]. Our lower bound recovers the expression in Theorem 2.2 of [20].

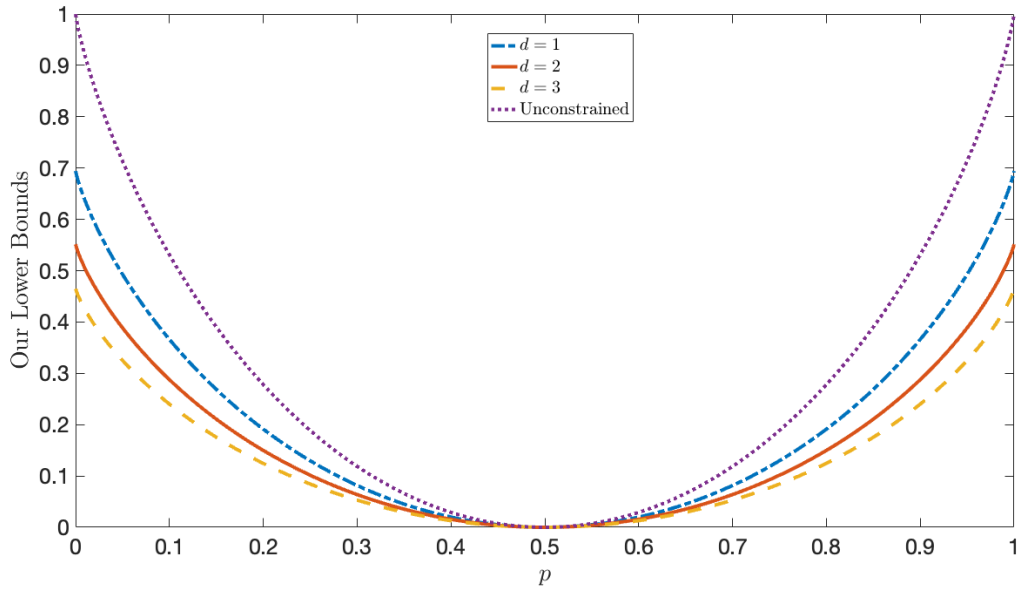


Figure 4.5: Our lower bounds for the (d, ∞)-RLL input-constrained BSC(p), when $d = 1, 2, 3$.

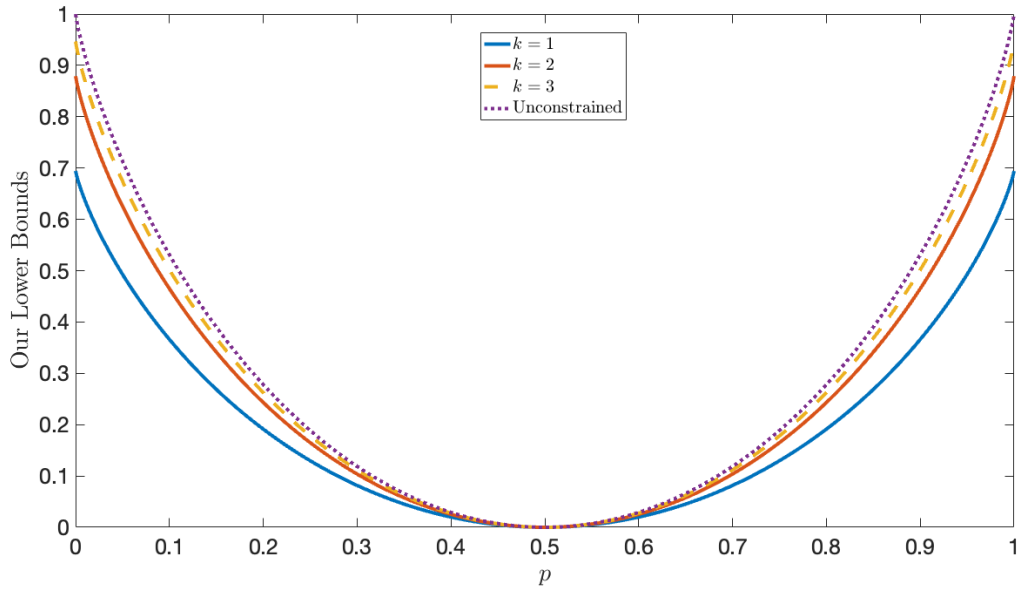


Figure 4.6: Our lower bounds for the $(0, k)$-RLL input-constrained BSC(p), when $k = 1, 2, 3$.

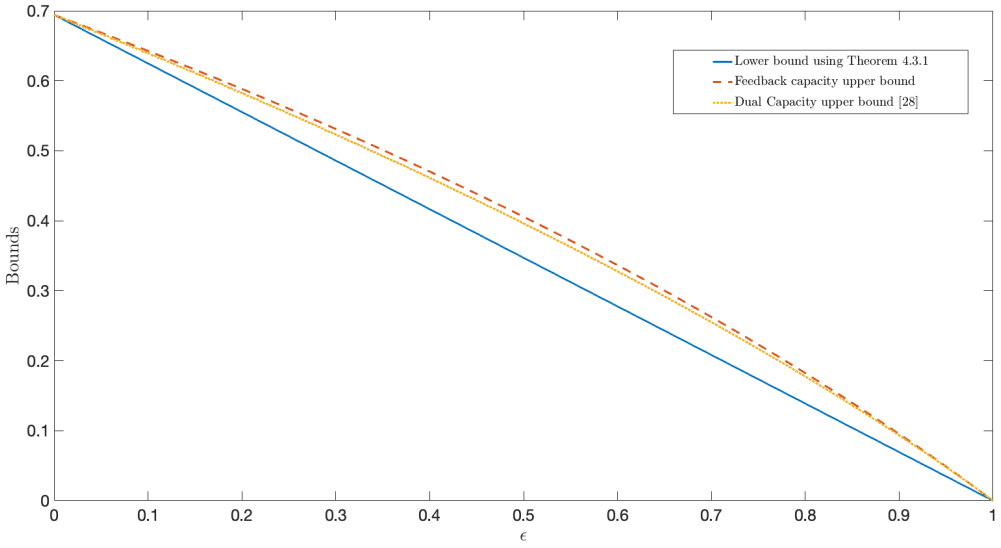


Figure 4.7: Comparison of the DP lower bound for the $(1,\infty)$-RLL input-constrained BEC(ϵ) with bounds in [88] and [28].

4.4 Improvements for the $(1,\infty)$-RLL Input-Constrained BEC

In this section, we attempt to improve on the simple lower bounds of the previous section, for the special case of the $(1,\infty)$-RLL input-constrained BEC(ϵ), where ϵ is the erasure probability of the channel. Here, too, we consider inputs that are drawn from a first-order Markov process. We first provide a numerical algorithm for computing the so-called first-order capacity of this channel, which is the maximum mutual information rate between the first-order Markov inputs and the outputs. Recall that this first-order capacity is a lower bound on the capacity of the channel[1]. Our approach is different from (and somewhat simpler than) the methods in [19], in that it relies on

[1]Note that the capacity of the $(0,1)$-RLL input-constrained BEC, $C_{(0,1)}(\epsilon)$, is equal to the capacity of the $(1,\infty)$-RLL input-constrained BEC, $C_{(1,\infty)}(\epsilon)$, for all $\epsilon \in [0,1]$, as there exists a bijective mapping (that flips 0s to 1s and vice versa) between sequences that respect the $(1,\infty)$-RLL constraint and those that obey the $(0,1)$-RLL constraint. Our algorithm, hence, also computes a lower bound on $C_{(0,1)}(\epsilon)$.

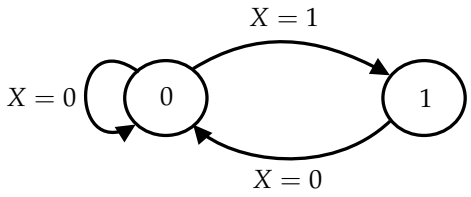


Figure 4.8: A state transition graph for the $(1, \infty)$-RLL input constraint. The nodes of the graph represent the previous input and the labels on the edges represent the current inputs.

the identification of two accompanying random processes that lead to a novel parameterization of the entropy rate of the output Hidden Markov process. We also observe that the lower bound expression that we work with is the same as the series expansion type bound in Corollary 5 of [20]. Further, evaluations of our numerical algorithm indicate that the lower bound is close in value to the dual capacity-based upper bound expression in [28]. We also provide a simple, analytical lower bound, which is given by a single-parameter optimization problem. This analytical bound is better than the linear lower bound from Theorem 4.3.1 (or that in Theorem 2 of [20]), for $\epsilon \gtrapprox 0.77$.

4.4.1 Preliminaries

The channel model that we are working with is shown in Figure 3.2, with the DMC replaced by a BEC. The constraint on the input sequences, which is the $(1, \infty)$-RLL constraint, is a special case of the (d, k)-RLL constraint discussed in the previous section. A state transition graph representing the constraint is shown in Figure 4.8. It is easy to see that this constraint is equivalent to a "no-consecutive-ones" constraint.

By assigning a probability distribution $P(x|x^-), x \in \{0, 1\}$, to each node $x^- \in \{0, 1\}$ of the presentation in Figure 4.8, we can define joint distributions on input sequences $(X_1, X_2, X_3, \ldots)$ that respect the $(1, \infty)$-RLL constraint. We set $P(x = 0|1) = 1$ and we have the flexibility of assigning $P(x = 1|0)$ to be some $a \in [0, 1]$. We set $P(x^n) = \prod_{i=1}^{n} P(x_i \mid x_{i-1})$. It can be verified that this induces a first-order Markov chain $(X_i)_{i \geq 1}$ on $\mathcal{X}$, and we set $P(x_i \mid x_{i-1}) =: Q(x_{i-1}, x_i)$. With a slight abuse of notation, we denote

by Q the matrix $[Q(x^-, x)]$, $x^-, x \in \{0,1\}$. The matrix Q is then given by

$$Q = \begin{bmatrix} 1-a & a \\ 1 & 0 \end{bmatrix},$$

For our purposes, we will assume that $P(x = 1|0) = a \in (0,1)$, so that the resulting Markov chain $(X_i)_{i\geq 1}$ is ergodic with (unique) stationary distribution π, with $\pi(0) = \frac{1}{1+a}$ and $\pi(1) = \frac{a}{1+a}$. We let $X_0 \sim \pi$, as the choice of the distribution of the initial state X_0 does not affect the capacity of the channel (see [6, Chapter 4]).

Recall that our objective is to obtain a lower bound on the capacity expression in Theorem 4.2.1. Following [20], we define the first-order capacity of the $(1,\infty)$-RLL input-constrained DMC as

$$C_f = \sup_{\{P(x|x^-)\}} \lim_{N\to\infty} \frac{1}{N} I(X^N; Y^N), \tag{4.2}$$

where the maximum is taken over all choices of the probability distributions $P(x|x^-)$, defined for each $x^- \in \{0,1\}$. As explained above, the only flexibility we have is in choosing an $a \in (0,1)$ to be assigned to $P(x = 1|x^- = 0)$. Note that the definition of C_f allows us to work with larger lower bounds than that in Theorem 4.3.1.

From the following set of inequalities, it is easy to see that the first-order capacity, C_f, is a lower bound on the capacity, C. Let $C_N := \max_{P_{X^N}} \frac{1}{N} I(X^N; Y^N)$.

$$\begin{aligned}
C &= \lim_{N\to\infty} C_N \\
&= \sup_N \left(C_N - \frac{\log|\mathcal{X}|}{N} \right) \\
&= \sup_{\{P(x_i|x^{i-1})\}_{i\geq 1}} \sup_N \left(\frac{1}{N} I(X^N; Y^N) - \frac{1}{N} \right) \\
&\geq \sup_{\{P(x_i|x^{i-1})\}_{i\geq 1}} \liminf_{N\to\infty} \frac{1}{N} I(X^N; Y^N) \\
&\geq \sup_{\{P(x|x^-)\}} \lim_{N\to\infty} \frac{1}{N} I(X^N; Y^N) = C_f,
\end{aligned}$$

where the second equality follows from the super-additivity of the sequence $\{NC_N + \log|\mathcal{X}|\}_{N\geq 1}$ (see Theorem 4.6.1 in [6]).

Recall that our focus is on the binary erasure channel, or the BEC, shown in Figure 4.3a. Let $\epsilon \in [0,1]$ be the erasure probability of the channel. Further, for a given sequence of outputs, $(Y_i)_{i\geq 1}$, we define the associated random processes $(\tilde{X}_i)_{i\geq 1}$ and $(L_i)_{i\geq 1}$, where for any $j \geq 1$, $\tilde{X}_j \in \{0,1\}$ represents the last unerased input that the decoder, with knowledge of Y^{j-1}, can identify exactly, and $L_j \in [j]$ is the location, counting backwards from j, of this last unerased input, i.e., $X_{j-L_j} = \tilde{X}_j$. If all the outputs Y^{j-1} are erasures, we set $L_j = j$. In what follows, we use $\tilde{x}_i$ and ℓ_i to denote specific instances of $\tilde{X}_i$ and L_i, for a fixed output sequence, y^{i-1}.

4.4.2 Our Results

In this subsection, we provide an expression for the first-order capacity, $C_f(\epsilon)$, of the $(1,\infty)$-RLL input-constrained BEC, which is obtained using the $(\tilde{X}_i)_{i\geq 1}$ and $(L_i)_{i\geq 1}$ processes defined in the previous subsection. We then discuss a numerical algorithm for computing $C_f(\epsilon)$, which is a lower bound on the capacity. We also provide a simple analytical lower bound on $C_f(\epsilon)$.

The proposition below follows from the definitions of the associated random processes, in the previous subsection.

Proposition 4.4.1. *The random process $(L_i, \tilde{X}_i, Y_i)_{i\geq 1}$ forms a Markov chain.*

Before we prove the proposition, it will be useful to state and prove a simple lemma about the $(1,\infty)$-RLL input-constrained BEC.

Lemma 4.4.2. *For $2 \leq i \leq N$ and for a fixed output sequence y^{i-1} of a BEC with $(1,\infty)$-RLL constrained inputs, we have that the conditional probability $P(x_i|y^{i-1}) = P(x_i|\tilde{x}_i, \ell_i)$.*

Proof. For $2 \leq i \leq N$, let $I(i) \subseteq [i-1]$ denote the set of indices corresponding to

unerased symbols in y^{i-1}. Then,

$$\begin{aligned} P(x_i \mid y^{i-1}) &= P\left(x_i \mid (y_j)_{j\in I(i)}\right) \\ &= P\left(x_i \mid (y_j)_{j\in I(i)}, \tilde{x}_i, \ell_i\right) \\ &= P\left(x_i \mid (x_j)_{j\in I(i)}, \tilde{x}_i, \ell_i\right) = P(x_i|\tilde{x}_i, \ell_i), \end{aligned}$$

where the last equality follows from the Markov property of the sequence $(X_i)_{i\geq 1}$. □

We now prove Proposition 4.4.1.

Proof of Proposition 4.4.1. For notational convenience, we denote the history of the process under consideration as $\Gamma_{i-1} := (\ell^{i-1}, \tilde{x}^{i-1}, y^{i-1})$. Now,

$$\begin{aligned} &P(L_i = \ell_i, \tilde{X}_i = \tilde{x}_i, Y_i = y_i|\Gamma_{i-2}, \ell_{i-1}, \tilde{x}_{i-1}, y_{i-1}) \\ &\overset{(a)}{=} P(L_i = \ell_i)P(\tilde{x}_i|\tilde{x}_{i-1}, \ell_i, \ell_{i-1})P(y_i|\Gamma_{i-1}, \ell_i, \tilde{x}_i) \\ &\overset{(b)}{=} P(L_i = \ell_i)P(\tilde{x}_i|\tilde{x}_{i-1}, \ell_i, \ell_{i-1}) \left(\sum_{x_i} P(y_i|x_i)P(x_i|\tilde{x}_i, \ell_i)\right) \\ &= P(\ell_i, \tilde{x}_i, y_i|\ell_{i-1}, \tilde{x}_{i-1}, y_{i-1}), \end{aligned}$$

where equality (a) follows from the definitions of the random processes $(L_i)_{i\geq 1}$ and $(\tilde{X}_i)_{i\geq 1}$ and the fact that the erasures are independently introduced by the channel at each time step, and equality (b) follows from an application of Lemma 4.4.2. □

We now provide an alternative expression for $C_f(\epsilon)$.

Theorem 4.4.3. *The first-order capacity, $C_f(\epsilon)$, of the $(1,\infty)$-RLL input-constrained BEC is given by*

$$C_f(\epsilon) = \bar{\epsilon} \cdot \max_{a\in(0,1)} \lim_{N\to\infty} \frac{1}{N} \sum_{i=2}^{N} \mathbb{E}\left[h_b\left(aQ^{(L_i-1)}(\tilde{X}_i, 0)\right)\right], \tag{4.3}$$

where the parameter, a, is equal to the transition probability $P(X = 1|X^- = 0)$ of the stationary input Markov process.

Proof. For the $(1,\infty)$-RLL input-constrained BEC, for any $i \geq 2$, the conditional entropy, $H(Y_i|Y^{i-1})$ can be written as

$$\begin{aligned} H(Y_i|Y^{i-1}) &= \mathbb{E}[H(Y_i|y^{i-1})] \\ &= \mathbb{E}\left[H\left(\sum_{x_i} P(y_i|x_i)P(x_i|y^{i-1})\right)\right] \\ &= \bar{\epsilon}\cdot\mathbb{E}[h_b(P(X_i=1|\tilde{X}_i,L_i))] + h_b(\epsilon) \\ &= \bar{\epsilon}\cdot\mathbb{E}_{L_i,\tilde{X}_i}\left[h_b\left(aQ^{(L_i-1)}(\tilde{X}_i,0)\right)\right] + h_b(\epsilon) \end{aligned} \tag{4.4}$$

where the penultimate inequality makes use of Lemma 4.4.2 and the identity that $H(a\bar{c},\bar{a}\bar{c},c) = h_b(c) + \bar{c}h_b(a)$, for all $a,c \in [0,1]$. The last inequality follows from the fact that

$$\begin{aligned} P(X_i=1|\tilde{x}_i,\ell_i) &= \sum_{x_{i-1}} P(X_i=1|x_{i-1})Q^{(\ell_i-1)}(\tilde{x}_i,x_{i-1}) \\ &= aQ^{(\ell_i-1)}(\tilde{x}_i,0). \end{aligned}$$

Now, we have that

$$\begin{aligned} C_f(\epsilon) &= \sup_{\{P(x|x^-)\}} \lim_{N\to\infty} \frac{1}{N}H(Y^N) - h_b(\epsilon) \\ &= \max_{a\in(0,1)} \lim_{N\to\infty} \frac{1}{N}\sum_{i=1}^{N} H(Y_i|Y^{i-1}) - h_b(\epsilon) \\ &= \bar{\epsilon}\cdot\max_{a\in(0,1)} \lim_{N\to\infty} \frac{1}{N}\sum_{i=2}^{N} \mathbb{E}\left[h_b\left(aQ^{(L_i-1)}(\tilde{X}_i,0)\right)\right], \end{aligned}$$

where the last equation follows from equation (4.4). □

Theorem 4.4.3 gives rise to a numerical algorithm for computing the first-order capacity of the $(1,\infty)$-RLL input-constrained BEC, which we now present. For a fixed $j \geq 2$, we define the function

$$g(L_j,\tilde{X}_j;a) := h_b(aQ^{(L_j-1)}(\tilde{X}_j,0)).$$

Algorithm 1 Two-Timescale FDSA Scheme

procedure TT-FDSA
  Pick $a_0 \in (0,1)$, and a large positive integer N.
  Pick $\{\alpha_n\}, \{\beta_n\}$ s.t. $\sum \alpha_n = \sum \beta_n = \infty$, with $\sum \alpha_n^2 + \sum \beta_n^2 < \infty$, $\alpha_n = o(\beta_n)$, $\alpha_0 = \beta_0 = 1$.
  Set $n_0 = 0$ and $n_{m+1} = \min\{j > n_m : \sum_{i=n_m+1}^{j} \alpha_i \geq \beta_m\}$, $m \geq 0$.
  Fix a small $\delta \in (0,1)$. Set $i = j = m = 0$.
  while $i < N$ **do**
    while $n_m + 1 \leq j \leq n_{m+1}$ **do**
      Sample $X^{(1)}(j), Y^{(1)}(j)$ using $a_i - \delta$.
      Sample $X^{(2)}(j), Y^{(2)}(j)$ using $a_i + \delta$.
      Compute $L_j^{(1)}, \tilde{X}_j^{(1)}$ using the $Y^{(1)}$ process.
      Compute $L_j^{(2)}, \tilde{X}_j^{(2)}$ using the $Y^{(2)}$ process.
      Set $\theta(j) := \frac{g(L_j^{(2)}, \tilde{X}_j^{(2)}; a_i+\delta) - g(L_j^{(1)}, \tilde{X}_j^{(1)}; a_i-\delta)}{2\delta}$.
      Update $j \leftarrow j + 1$.
    Set $a_{i+1} = a_i + \sum_{j=n_m+1}^{n_{m+1}} \alpha_j \theta(j)$.
    if $a_{i+1} \notin (0,1)$ **then**
      Set a_{i+1} to a random point in $(0,1)$.
    Update $m = m + 1$ and $i = i + 1$.
  Output a_N.

Note that the function g corresponds to samples of each summand in the objective function in (4.3). One approach towards computing the maximum in equation (4.3) is by an iterative algorithm that updates the parameter a along the direction of the gradient (or an estimate thereof) of the objective function. Our algorithm (shown as Algorithm 1) uses a two-timescale finite difference stochastic approximation (TT-FDSA) scheme (see, for example, [30], [31]), and employs an estimator of the gradient based on finite differences between samples. The output of the algorithm is an estimate of the optimal value of the parameter a, which completely determines an estimate of the

optimal input distribution. Figure 4.9 shows plots of numerical values of our lower bound on the capacity for the $(1,\infty)$-RLL input-constrained BEC, with plots of the linear lower bound from Theorem 4.3.1 and the dual capacity-based upper bound in [28]. We observe that our lower bound is numerically close in value to the upper bound in [28] and is at least as large as the linear lower bound, thereby providing an improvement over our previous analytical lower bound for this channel. Figure 4.10 shows comparisons of the estimates of the optimal values of the parameter a obtained using our scheme and those obtained using the sampling-based approach in [14]. We note that our estimates are close in value to those obtained using the approach in [14].

While a straightforward evaluation of Theorem 4.4.3 yields the series expansion type lower bound in Corollary 5 of Li and Han [20], the next theorem provides a simple, analytical, single-letter optimization problem as a lower bound on this series expansion type bound.

We first define the function $R(\cdot)$, which takes as argument the parameter $a \in (0,1)$.

$$R(a) = h_b\left(\frac{1}{1+a}\right) + \left(\frac{\bar{\epsilon}}{(1-a\epsilon)(1+a)}\right)\left(h_b\left(\frac{1-a}{1+a}\right) - 2h_b\left(\frac{1}{1+a}\right)\right). \tag{4.5}$$

Theorem 4.4.4. *The first-order capacity $C_f(\epsilon)$ of the $(1,\infty)$-RLL input-constrained BEC obeys*

$$C_f(\epsilon) \geq \bar{\epsilon} \cdot \max_{a\in(0,1)} R(a),$$

where the function $R(a)$ is given in (4.5).

Proof. First, since the inputs are drawn from a stationary Markov process, it follows that

$$P(X_i = 1|\tilde{x}_i, \ell_i = i) = \pi(X_i = 1). \tag{4.6}$$

Further, for $i \geq 2$, we have that

$$P(L_i = k) = \begin{cases} \bar{\epsilon}\epsilon^{k-1}, \ k \in [i-1], \\ \epsilon^{i-1}, \ k = i. \end{cases} \tag{4.7}$$

Note that the ℓ-step transition probability matrix, $Q^{(\ell)}$, can be expressed as

$$Q^{(\ell)} = \begin{bmatrix} \frac{1+(-1)^{\ell}a^{\ell+1}}{1+a} & \frac{a+(-a)^{\ell+1}}{1+a} \\ \frac{1+(-1)^{\ell-1}a^{\ell}}{1+a} & \frac{a+(-a)^{\ell}}{1+a} \end{bmatrix},$$

Also, we note that for any $j \geq 1$, $P(\tilde{X}_j = 1) = \pi(1)$, since the input process is stationary and independent of the erasures introduced by the channel according to equation (4.7).

We now compute a lower bound on $C_f(\epsilon)$ by working with the expression given in Theorem 4.4.3. For $i \geq 2$, we have

$$\begin{aligned}
&\mathbb{E}_{L_i,\tilde{X}_i}\left[h_b\left(aQ^{(L_i-1)}(\tilde{X}_i,0)\right)\right] \\
&= \bar{\epsilon}\cdot\sum_{j=1}^{i-1}\epsilon^{j-1}\left[\pi(0)h_b(Q^{(j-1)}(0,0)) + \pi(1)h_b(Q^{(j-1)}(1,0))\right] + \epsilon^{i-1}h_b(\pi(X=0)) \\
&\overset{(a)}{\geq} \bar{\epsilon}\cdot\sum_{j=1}^{i-1}\epsilon^{j-1}\left[\left(1-\tfrac{2a^{j-1}}{1+a}\right)h_b\left(\tfrac{1}{1+a}\right) + \left(\tfrac{a^{j-1}}{1+a}\right)h_b\left(\tfrac{1-a}{1+a}\right)\right] + \epsilon^{i-1}h_b\left(\tfrac{1}{1+a}\right) \\
&= \bar{\epsilon}\cdot\left\{h_b\left(\tfrac{1}{1+a}\right)\left[\left(\tfrac{1-\epsilon^{i-1}}{1-\epsilon}\right) - \left(\tfrac{2}{1+a}\right)\left(\tfrac{1-(a\epsilon)^{i-1}}{1-a\epsilon}\right)\right] + \left(\tfrac{1}{1+a}\right)\left(\tfrac{1-(a\epsilon)^{i-1}}{1-a\epsilon}\right)h_b\left(\tfrac{1-a}{1+a}\right)\right\} + \\
&\qquad\qquad \epsilon^{i-1}h_b\left(\tfrac{1}{1+a}\right).
\end{aligned}$$

where, in the first equality, we have made use of equations (4.6) and (4.7), and the inequality (a) follows from equations (19) and (20) of [23]. Hence,

$$\begin{aligned}
C_f(\epsilon) &= \bar{\epsilon}\cdot\max_{a}\lim_{N\to\infty}\frac{1}{N}\sum_{i=2}^{N}\mathbb{E}_{L_i,\tilde{X}_i}\left[h_b\left(aQ^{(L_i-1)}(\tilde{X}_i,0)\right)\right] \\
&\geq \bar{\epsilon}\cdot\max_{a\in(0,1)}R(a),
\end{aligned}$$

where $R(a)$ is as defined in (4.5). □

Figure 4.11 shows comparisons of the maximum of the lower bounds on the capacity in Theorem 4.4.4 and in Theorem 4.3.1, with the linear lower bound of Theorem 4.3.1, the dual capacity upper bound in [28], and the feedback capacity upper bound in [88]. Clearly, the linear lower bound is better than our bound for $\epsilon \gtrapprox 0.389$, but for

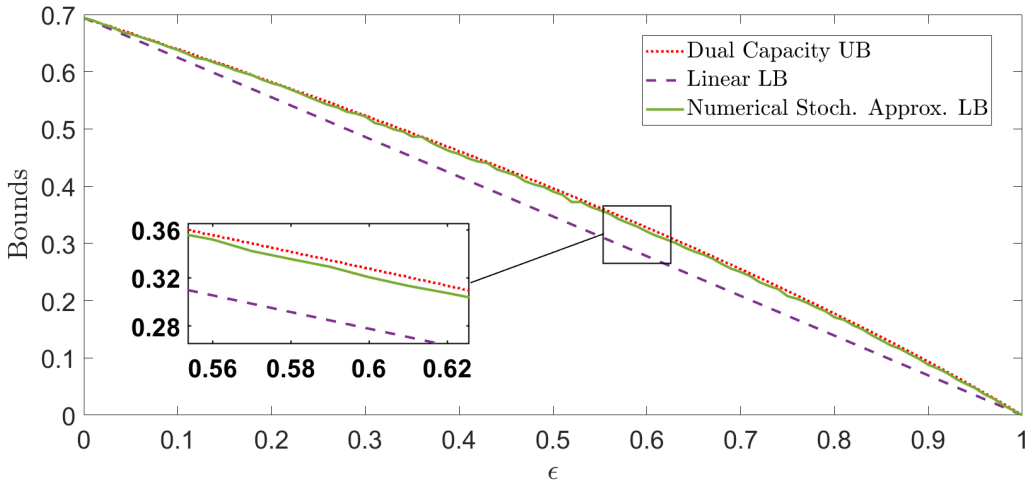


Figure 4.9: Plots comparing our numerical lower bound with the linear lower bound in [19] and [29] and the dual capacity-based upper bound in [28].

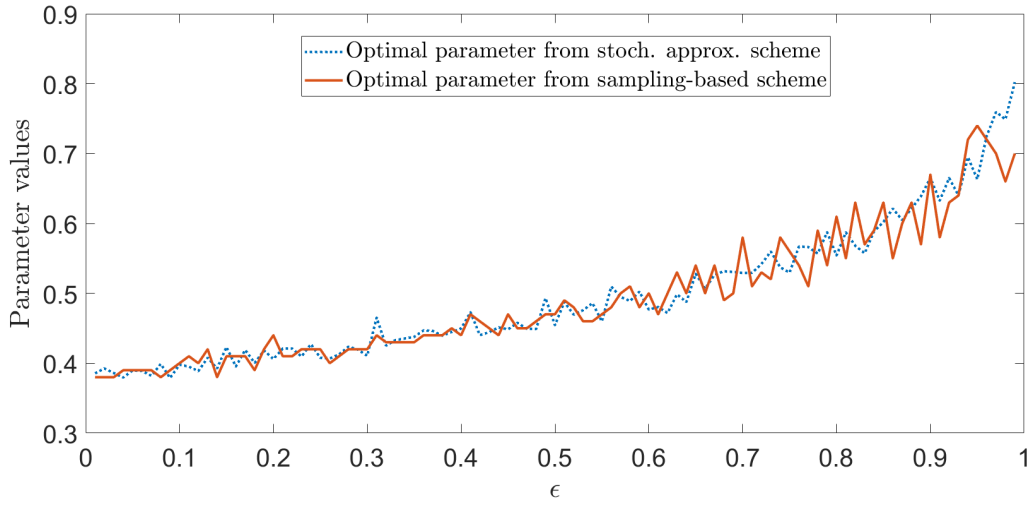


Figure 4.10: Plot shows comparisons of the estimates of the optimal values of the parameter $a = P(X = 1|X^- = 0)$ for the $(1, \infty)$-RLL input-constrained BEC with those obtained from the sampling-based approach in [14]. We observe that our estimates of the parameter a are less noisy than the estimates from the sampling-based method.

smaller values of ϵ, the lower bound in Theorem 4.4.4 is larger.

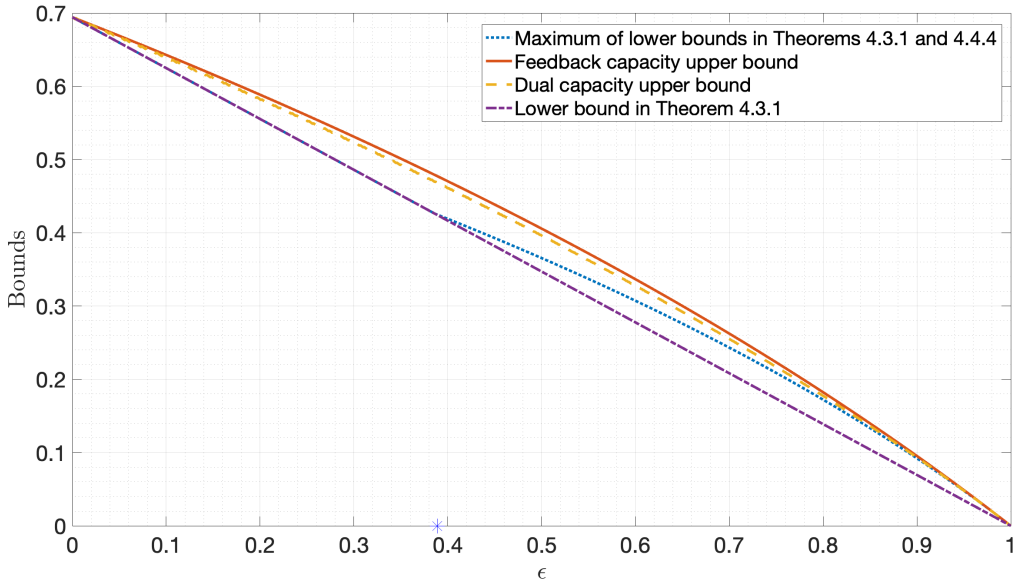


Figure 4.11: Plots comparing the the maximum of the lower bounds on the capacity in Theorem 4.4.4 and in Theorem 4.3.1, with the linear lower bound of Theorem 4.3.1, the dual capacity upper bound in [28], and the feedback capacity upper bound in [88]. Note that the analytical bound in Theorem 4.4.4 beats the simple linear lower bound for $\epsilon \gtrapprox 0.389$; a $*$ marker has been provided on the ϵ-axis to identify this cross-over point.

4.5 Conclusions and Directions for Future Work

In this chapter, we provided lower bounds on the capacities of so-called "input-driven" channels with finitely-many states, which include many input-constrained DMCs. Our approach, like other approaches in the literature, was to restrict the input distributions to be first-order Markov. We first obtained simple single-letter lower bounds, which provided a unified treatment of bounds for different input-constrained channels from the literature, and extended them to the class of input-driven FSCs. Next, for the special case of the binary erasure channel (BEC) with a "no-consecutive-ones" input constraint, we derived a series expansion-type lower bound on the capacity, which recovers the lower bound in [20], by making use of two novel stochastic processes. We

then provided a numerical stochastic approximation-based algorithm for the computation of the lower bound and demonstrated that the lower bound is close in value to the dual capacity-based upper bound in [28]. We also presented a simple analytical lower bound that is better than the simple single-letter lower bound that we originally derived for this channel, for large values of the erasure probability.

An important open question in the context of the capacities of input-constrained BSCs is Wolf's conjecture [32], which goes as follows:

Conjecture 4.5.1. *For the (d,k)-RLL input-constrained BSC(p), with capacity C, we have that*

$$C \geq \kappa_{d,k} \cdot (1 - h_b(p)),$$

where $\kappa_{d,k}$ is the noiseless capacity of the (d,k)-RLL constraint.

Note that a counterpart of this result for the input-constrained BEC(ϵ) was proved in Theorem 2.2 of [20] and in Theorem 4.3.1 of this chapter. Future work could hence look at resolving this conjecture using the tools herein or otherwise. Another direction for research is to extend the numerical algorithm presented here to more general input-constrained BECs.

Chapter 5

Constrained Coding Schemes Using RM Codes: Achievable Rates

We deliberate not about ends, but about means. For a doctor does not deliberate whether he shall heal, nor an orator whether he shall persuade [...] they consider how it will be achieved and by what means this will be achieved, until they come to the first cause [...] and what is last in the order of analysis seems to be the first in the order of becoming.

Aristotle, Nicomachean Ethics, Book III, 3, 1112b

5.1 Introduction

In the previous chapter, we discussed information-theoretic lower bounds on the capacities of input-constrained DMCs. This chapter focuses on designing *explicit* constrained coding schemes over a large class of DMCs with runlength-limited (RLL) constraints, and deriving lower bounds on their achievable rates. In particular, the codes we construct are derived from the Reed-Muller (RM) family of codes.

Our focus is on the (d, ∞)-runlength limited (RLL) input constraint, defined in Definition 2, which is a special case of the class of (d, k)-RLL input constraints. The (d, ∞)-RLL constraint finds application in magnetic recording systems, as a constraint on the

data sequence (where the bit 1 corresponds to a voltage peak of high amplitude and the bit 0 corresponds to no peak), which ensures that successive 1s are spaced far enough apart, so that there is little inter-symbol interference between the voltage responses corresponding to the magnetic transitions. Reference [33] contains many examples of (d,k)-RLL codes used in practice in magnetic storage and recording. More recently, (d,k)-RLL input constrained sequences have also been investigated for joint energy and information transfer performance [34].

We are interested in the transmission of (d,∞)-RLL constrained codes over input-constrained, noisy binary-input memoryless symmetric (BMS) channels, without feedback, which form a subclass of input-constrained DMCs, without feedback (see Figure 3.2). Examples of BMS channels include the familiar binary erasure channel (BEC) and binary symmetric channel (BSC), shown in Figures 4.3a and 4.3b.

We recall that for the setting of *unconstrained* DMCs without feedback, explicit codes achieving the capacities, or whose rates are very close to the capacities, have been derived in works such as [35–39]. However, to the best of our knowledge, there are no explicit coding schemes with provable rate and probability of error guarantees, for input-constrained DMCs without feedback.

In this chapter, we make progress on the construction of explicit codes over (d,∞)-RLL input-constrained BMS channels. Our motivation for constructing (d,∞)-RLL constrained codes using RM codes, are the very recent results of Reeves and Pfister [40] and Abbe and Sandon [41] that Reed-Muller (RM) codes achieve, under bitwise maximum a-posteriori probability (bit-MAP) and blockwise maximum a-posteriori probability (block-MAP) decoding, respectively, any rate $R \in [0, C)$, over unconstrained BMS channels, where C is the capacity of the BMS channel. We note that for the specific setting of the BEC, Kudekar et al. in [36] were the first to show that Reed-Muller (RM) codes are capacity-achieving. As a consequence of these results, the constrained coding schemes we construct have bit- and block-error probabilities going to 0 (using the bit-MAP and block-MAP decoders for the RM code, respectively), as the block-length goes to infinity, if the codes are used over (d,∞)-RLL input-constrained BMS

channels.

We invite the reader to also refer to Chapter 6 for upper bounds on rates achievable using (d, ∞)-RLL constrained RM subcodes.

5.2 Some Approaches From Prior Art

There is extensive literature on constrained code constructions that can correct a fixed number of errors, under a combinatorial error model[1] (see Chapter 9 in [2] and the references therein). Another related line of work that aims to limit error propagation during the decoding of constrained codes can be found in [42–45]. More recently, the work [46] proposed the insertion of parity bits for error correction, into those positions of binary constrained codewords that are unconstrained, i.e., whose bits can be flipped, with the resultant codeword still respecting the constraint. However, such works do not analyze the resilience of constrained codes to stochastic channel noise—the standard noise model in information theory, which is taken up in this chapter (and which was discussed in Chapter 3).

To the best of our knowledge, the paper [47], on rates achievable by (d, k)-RLL subcodes of cosets of a linear block code, was the first to consider the problem of coding schemes over RLL input-constrained DMCs. Specifically, Corollary 1 of [47] shows via an averaging argument that there must exist, in the limit as the blocklength goes to infinity, cosets of codes of rate equalling the capacity of the unconstrained BMS channel, whose (d, k)-RLL constrained (with $0 \leq d < k \leq \infty$) subcodes have rate at least $\kappa_{d,k} + C - 1$, where $\kappa_{d,k}$ is the noiseless capacity of the (d, k)-RLL constraint. Recall, from Chapter 3 of [2], that if $S_{(d,k)}^{(n)} \subseteq \{0, 1\}^n$ represented the collection of (d, k)-RLL constrained binary sequences of length n, then

$$\kappa_{d,k} = \lim_{n \to \infty} \frac{\log_2 |S_{(d,k)}^{(n)}|}{n},$$

[1] We shall derive upper bounds on the sizes of the largest constrained codes correcting a fixed number of errors, in Chapter 9.

where the limit exists by subadditivity arguments (see also Definition 5 in this chapter). The proof of the averaging argument goes as follows: pick any code of rate $C \in (0,1)$, and observe that at blocklength n, the *average* number of constrained codewords in a coset of the code (including the code itself) is at least $\frac{2^{n\left(\kappa_{d,k}-\delta_n\right)}}{2^{n(1-C)}}$, for some $\delta_n > 0$ with $\delta_n \xrightarrow{n\to\infty} 0$. Hence, as $n \to \infty$, the coset containing the *largest* number of (d,k)-RLL constrained sequences, has rate at least $\kappa_{d,k} + C - 1$. However, the work in [47] does not identify *explicit* codes over RLL input-constrained channels.

In the context of designing coding schemes over (input-constrained) BMS channels, it would be remiss to not comment on the rates achieved by polar codes—another family of explicit codes that is capacity-achieving over a broad class of channels (see, for example, [35,48,49], and references therein). Following the work of Li and Tan in [50], it holds that the capacity without feedback of the class of input-constrained DMCs can be approached arbitrarily closely using stationary, ergodic Markov input distributions of finite order (see also [24], which shows that Markov processes of increasing order can come arbitrarily close to the capacity, but does not comment on the properties of these processes). Moreover, from the results in [49], it follows that polar codes can achieve the mutual information rate of any stationary, ergodic finite-state Markov input process, over any DMC. In particular, this shows that polar codes achieve the capacity of (d,∞)-RLL input-constrained DMCs, which includes the class of (d,∞)-RLL input-constrained BMS channels. However, this observation is not very helpful for the following reasons:

- We do not possess knowledge of an optimal sequence of Markov input distributions.
- The polar code construction described above is not explicit, since the choice of bit-channels to send information bits over is not explicitly known for an arbitrary BMS channel.
- It is hard to compute the rate achieved by such a coding scheme, since such a computation reduces to the calculation of the mutual information rate of a hidden

Markov process.

We mention here that for the ISI channels defined in Chapter 4, there exist works [17, 51] that construct codes, using low-density parity-check (LDPC) codes, which under a decoding procedure called multistage decoding, approach the mutual information rate of the ISI channel using independent, uniformly distributed inputs.

5.3 Summary of Our Contributions

We propose explicit coding schemes using RM codes, with computable rate lower bounds, over input-constrained BMS channels. In the first part of the chapter, we fix the ordering of the coordinates of the RM codes we consider to be the standard lexicographic ordering, and consider the problem of identifying (d, ∞)-RLL constrained subcodes of RM codes of rate R, of good rate. Suppose that C is the capacity of the unconstrained BMS channel. Our first approach to designing (d, ∞)-RLL constrained codes is simply to identify *linear* (d, ∞)-RLL subcodes of RM codes of rate R, and compute their rates. The rates we compute are in fact achievable (using the bit-MAP or block-MAP decoders of the parent RM code) over (d, ∞)-RLL input-constrained BMS channels, so long as $R < C$. Next, we present a lower bound on rates of *non-linear* $(1, \infty)$-RLL subcodes of RM codes of R, and derive achievable rates using such codes, too.

Finally, as an improvement over the rates achievable using (d, ∞)-RLL subcodes, we propose a new explicit two-stage (or concatenated) coding scheme using RM codes, and compute explicit rate lower bounds for this scheme, over the input-constrained binary erasure channel (BEC). For example, when $d = 1$, we observe that the rates achieved using this two-stage scheme are better than those achieved by any scheme that uses linear $(1, \infty)$-RLL subcodes of RM codes (under almost all coordinate orderings), when $C \gtrapprox 0.7613$, and better than the rate achieved by our non-linear subcodes for all $C \lessapprox 0.55$ and $C \gtrapprox 0.79$. Moreover, as the capacity of the channel approaches 1, i.e., as the channel noise approaches 0, the rate achieved by our two-stage coding

scheme can be made arbitrarily close to κ_d, which is the largest rate achievable, at zero noise, given the constraint.

5.4 Notation and Preliminaries

5.4.1 Notation

Recall the notation $\mathbf{e}_i^{(n)}$ that denotes the standard basis vector of length n, with a 1 at position i, and 0s elsewhere, for $i \in [n]$. When $n = 2^m$, for some m, we interchangeably index the coordinates of vectors $\mathbf{v} \in \{0,1\}^n$ by integers $i \in [0 : n-1]$ and by m-tuples $\mathbf{b} = (b_1, \ldots, b_m) \in \{0,1\}^m$. We then use the notation $\mathbf{e}_{\mathbf{b}}^{(n)}$ to denote the standard basis vector of length n, with a 1 at position $\mathbf{b}$, and 0s elsewhere. The superscript '(n)' will be dropped when clear from context. For any $n \in \mathbb{N}$, we denote by $S_{(d,\infty)}^{(n)}$, the set of all n-length binary words that respect the (d,∞)-RLL constraint, and we set $S_{(d,\infty)} = \bigcup_{n\geq 1} S_{(d,\infty)}^{(n)}$.

Given a set A, we define the notation $\mathbb{1}\{x \in A\}$ to be equal to $\mathbb{1}_A(x)$. All through, the empty summation is defined to be 0, and the empty product is defined to be 1.

5.4.2 Information Theoretic Preliminaries

Block Codes and Constrained Codes

We recall the following definitions of block codes over $\mathbb{F}_2$ and their rates (see, for example, Chapter 1 of [57]).

Definition 3. *An (n, M) block code $\mathcal{C}$ over $\mathbb{F}_2$ is a nonempty subset of $\mathbb{F}_2^n$, with $|\mathcal{C}| = M$. The rate of the block code $\mathcal{C}$ is given by*

$$\mathit{rate}(\mathcal{C}) := \frac{\log_2 M}{n}.$$

Moreover, given a sequence of codes $\{\mathcal{C}^{(n)}\}_{n\geq 1}$, if it holds that $\text{rate}(\mathcal{C}^{(n)}) \xrightarrow{n\to\infty} R$, for some $R \in [0,1]$, then we say that $\{\mathcal{C}^{(n)}\}_{n\geq 1}$ is of rate R.

Definition 4. *An $[n,k]$ linear code $\mathcal{C}$ over $\mathbb{F}_2$ is an $(n,2^k)$ block code that is a subspace of $\mathbb{F}_2^n$.*

Consider now the set $S^{(n)}_{(d,\infty)}$ of length-n binary words that satisfy the (d,∞)-RLL constraint. We reiterate the following definition, which appeared in the previous section (see, for example, Chapter 3 of [2]):

Definition 5. *The noiseless capacity κ_d of the (d,∞)-RLL constraint is defined as*

$$\kappa_d := \lim_{n\to\infty} \frac{\log_2 \left|S^{(n)}_{(d,\infty)}\right|}{n} = \inf_n \frac{\log_2 \left|S^{(n)}_{(d,\infty)}\right|}{n},$$

where the last equality follows from the subadditivity of the sequence $\left(\log_2 \left|S^{(n)}_{(d,\infty)}\right|\right)_{n\geq 1}$.

Linear Codes Over BMS Channels

A binary-input memoryless channel is a DMC W (see Chapter 3) with input alphabet $\mathcal{X} = \{0,1\}$. A binary-input memoryless symmetric (BMS) channel is symmetric, besides, in that $P(y|1) = P(-y|0)$, for all $y \in \mathcal{Y}$. Every such channel can be expressed as a multiplicative noise channel, in the following sense: if at any i the input random symbol is $X_i \in \{0,1\}$, then the corresponding output symbol $Y_i \in \mathcal{Y}$ is given by

$$Y_i = (-1)^{X_i} \cdot Z_i,$$

where the noise random variables Z^n are independent and identically distributed, and the noise process $(Z_i)_{i\geq 1}$ is independent of the input process $(X_i)_{i\geq 1}$. Common examples of such channels include the binary erasure channel (BEC(ϵ)), with $P(Z_i = 1) = 1-\epsilon$ and $P(Z_i = 0) = \epsilon$, the binary symmetric channel (BSC(p)), with $P(Z_i = 1) = 1-p$ and $P(Z_i = -1) = p$, and the binary additive white Gaussian noise (BI-AWGN) channel, where $Z_i \sim \mathcal{N}(1,\sigma^2)$. Note that we make minor changes to the output alphabets in Figures 4.3a and 4.3b, in order to make them comply with the definition of BMS channels, here.

In this chapter, we are interested in designing codes over input-constrained BMS channels. We refer the reader to [40] for definitions of the bitwise maximum a-posteriori

probability (bit-MAP) decoder and bit-error probability $P_b^{(n)}$ (under bit-MAP decoding), indexed by the blocklength n of the code. We also refer the reader to standard texts on information theory such as [6], [7] for definitions of blockwise maximum a-posteriori probability (block-MAP) decoding and block-error probability $P_B^{(n)}$.

Specifically, we shall be using constrained subcodes of linear codes $\left\{\mathcal{C}^{(n)}\right\}_{n\geq 1}$ over BMS channels. At the decoder end, we shall employ the bit-MAP or block-MAP decoders of the parent linear codes $\left\{\mathcal{C}^{(n)}\right\}_{n\geq 1}$ (note that the decoders we use are *not* tailored to the subcodes we use at the encoder end). Since $\mathcal{C}^{(n)}$ is linear, the average bit-error probability $P_b^{(n)}$ (resp. the average block-error probability $P_B^{(n)}$), using the bit-MAP decoder (resp. block-MAP decoder) of $\mathcal{C}^{(n)}$ is the same as the average bit-error probability (resp. the average block-error probability) when a subcode of $\mathcal{C}^{(n)}$ is used (see [40] for a discussion).

We say that a rate R is achieved by $\left\{\mathcal{C}^{(n)}\right\}_{n\geq 1}$ over a BMS channel, under bit-MAP decoding (resp. under block-MAP decoding), if rate $\left(\mathcal{C}^{(n)}\right) \xrightarrow{n\to\infty} R$, with $P_b^{(n)} \xrightarrow{n\to\infty} 0$ (resp. $P_B^{(n)} \xrightarrow{n\to\infty} 0$). Hence, any sequence of subcodes of $\left\{\mathcal{C}^{(n)}\right\}_{n\geq 1}$ are also such that their bit-error and block-error probabilities go to zero, as the blocklength goes to infinity, when the bit-MAP and block-MAP decoders of the parent linear codes are used.

5.4.3 Reed-Muller Codes: Definitions and BMS Channel Performance

We recall the definition of the binary Reed-Muller (RM) family of codes (see Chapter 13 of [58], or the survey [52], or the monograph [59] for more details). Codewords of binary RM codes consist of the evaluation vectors of multivariate polynomials over the binary field $\mathbb{F}_2$. Consider the polynomial ring $\mathbb{F}_2[x_1, x_2, \ldots, x_m]$ in m variables. Note that in the specification of a polynomial $f \in \mathbb{F}_2[x_1, x_2, \ldots, x_m]$, only monomials of the form $\prod_{j\in S: S\subseteq[m]} x_j$ need to be considered, since $x^2 = x$ over the field $\mathbb{F}_2$, for an indeterminate x. For a polynomial $f \in \mathbb{F}_2[x_1, x_2, \ldots, x_m]$ and a binary vector $\mathbf{z} = (z_1, \ldots, z_m) \in \mathbb{F}_2^m$, let $\mathrm{Eval}_{\mathbf{z}}(f) := f(z_1, \ldots, z_m)$. We let the evaluation points be ordered according to the standard lexicographic order on strings in $\mathbb{F}_2^m$, i.e., if

$\mathbf{z} = (z_1, \ldots, z_m)$ and $\mathbf{z}' = (z'_1, \ldots, z'_m)$ are two distinct evaluation points, then, $\mathbf{z}$ occurs before $\mathbf{z}'$ in our ordering if and only if for some $i \geq 1$, it holds that $z_j = z'_j$ for all $j < i$, and $z_i < z'_i$. Now, let $\mathrm{Eval}(f) := (\mathrm{Eval}_{\mathbf{z}}(f) : \mathbf{z} \in \mathbb{F}_2^m)$ be the evaluation vector of f, where the coordinates $\mathbf{z}$ are ordered according to the standard lexicographic order.

Definition 6 (see [58], Chap. 13)**.** *For $0 \leq r \leq m$, the r^{th}-order binary Reed-Muller code $RM(m, r)$ is defined as the set of binary vectors:*

$$RM(m, r) := \{Eval(f) : f \in \mathbb{F}_2[x_1, x_2, \ldots, x_m],\ deg(f) \leq r\},$$

where $deg(f)$ is the degree of the largest monomial in f, and the degree of a monomial $\prod_{j \in S : S \subseteq [m]} x_j$ is simply $|S|$.

It is a known fact that the evaluation vectors of all the distinct monomials in the variables $x_1, \ldots, x_m$ are linearly independent over $\mathbb{F}_2$. It then follows that $\mathrm{RM}(m, r)$ has dimension $\binom{m}{\leq r}$. Furthermore, $\mathrm{RM}(m, r)$ has minimum Hamming distance $d_{\min}(\mathrm{RM}(m, r)) = 2^{m-r}$. The weight of a codeword $\mathbf{c} = \mathrm{Eval}(f)$ is the number of 1s in its evaluation vector, i.e,

$$\mathrm{wt}\left(\mathrm{Eval}(f)\right) := \left|\{\mathbf{z} \in \mathbb{F}_2^m : f(\mathbf{z}) = 1\}\right|.$$

The number of codewords in $\mathrm{RM}(m, r)$ of weight w, for $w \in [2^{m-r} : 2^m]$, is given by the weight distribution function at w:

$$A_{m,r}(w) := \left|\{\mathbf{c} \in \mathrm{RM}(m, r) : \mathrm{wt}\left(\mathbf{c}\right) = w\}\right|.$$

The subscripts m and r in $A_{m,r}$ will be suppressed when clear from context.

We also set $G_{\mathrm{Lex}}(m, r)$ to be the generator matrix of $\mathrm{RM}(m, r)$ consisting of rows that are the evaluations, in the lexicographic order, of monomials of degree less than or equal to r. The columns of $G_{\mathrm{Lex}}(m, r)$ will be indexed by m-tuples $\mathbf{b} = (b_1, \ldots, b_m)$ in the lexicographic order.

In this work, we shall use (d, ∞)-RLL constrained subcodes of RM codes, over BMS channels. We now recall the main results of Reeves and Pfister in [40] and Abbe and

Sandon in [41], which provides context to our using RM codes over input-constrained BMS channels. For a given $R \in (0,1)$, consider any sequence of Reed-Muller codes $\{\hat{\mathcal{C}}_m = \mathrm{RM}(m, r_m)\}_{m\geq 1}$, under the lexicographic ordering of coordinates, such that $\mathrm{rate}(\hat{\mathcal{C}}_m) \xrightarrow{m\to\infty} R$. We let C be the capacity of the unconstrained BMS channel under consideration. The following theorems then hold true:

Theorem 5.4.1 (see Theorem 1 of [40] and Theorem 1 of [41])**.** *Any rate $R \in [0, C)$ is achieved by the sequence of codes $\{\hat{\mathcal{C}}_m\}_{m\geq 1}$, under bit-MAP and block-MAP decoding.*

As an example, for $R \in (0,1)$, consider the specific sequence of Reed-Muller codes $\{\mathcal{C}_m = \mathrm{RM}(m, r_m)\}_{m\geq 1}$ with

$$r_m = \max\left\{\left\lfloor \frac{m}{2} + \frac{\sqrt{m}}{2} Q^{-1}(1-R)\right\rfloor, 0\right\}, \tag{5.1}$$

where $Q(\cdot)$ is the complementary cumulative distribution function (c.c.d.f.) of the standard normal distribution, i.e.,

$$Q(t) = \frac{1}{\sqrt{2\pi}} \int_t^\infty e^{-\tau^2/2} d\tau,\ t \in \mathbb{R}.$$

From Remark 24 in [36], it follows that $\mathrm{rate}(\mathcal{C}_m) \xrightarrow{m\to\infty} R$. Theorem 5.4.1 then states that the sequence of codes $\{\mathcal{C}_m\}_{m\geq 1}$ achieves a rate R over any unconstrained BMS channel, so long as $R < C$.

Remark 5.4.2. *We note that by Theorem 5.4.1, for the unconstrained BEC (resp. unconstrained BSC) with erasure probability $\epsilon \in (0,1)$ (resp. crossover probability $p \in (0, 0.5) \cup (0.5, 1)$), the sequence of codes $\{\mathcal{C}_m\}_{m\geq 1}$ with $R = 1 - \epsilon - \delta$ (resp. with $R = 1 - h_b(p) - \delta$) achieves a rate of $1 - \epsilon - \delta$ (resp. a rate of $1 - h_b(p) - \delta$), for all $\delta > 0$ suitably small.*

The following important property of RM codes, which is sometimes called the Plotkin decomposition (see [58, Chap. 13] and [52]), will be of use several times in this chapter: any Boolean polynomial $f \in \mathbb{F}_2[x_1, \ldots, x_m]$, such that $\mathrm{Eval}(f) \in \mathrm{RM}(m, r)$ (or

equivalently, with $\deg(f) \leq r$), can be expressed as:

$$f(x_1, \ldots, x_m) = g(x_1, \ldots, x_{m-1}) + x_m \cdot h(x_1, \ldots, x_{m-1}), \tag{5.2}$$

where g, h are such that $\text{Eval}(g) \in \text{RM}(m-1, r)$ and $\text{Eval}(h) \in \text{RM}(m-1, r-1)$, and the '$+$' operation is over $\mathbb{F}_2$. Note that the polynomials g and h above are uniquely determined, given the polynomial f. Given the sequence of RM codes $\{\mathcal{C}_m = \text{RM}(m, r_m)\}_{m \geq 1}$, where r_m is as in (5.1), we use the notations $\mathcal{C}_{m,+} := \text{RM}(m-1, r_m)$ and $\mathcal{C}_{m,-} := \text{RM}(m-1, r_m - 1)$, with $\text{rate}(\mathcal{C}_{m,+}) := R_{m,+}$ and $\text{rate}(\mathcal{C}_{m,-}) := R_{m,-}$.

In our (d, ∞)-RLL constrained code constructions in this chapter, we shall use constrained subcodes of a sequence $\left\{\hat{\mathcal{C}}_m = \text{RM}(m, v_m)\right\}_{m \geq 1}$ of rate R, and explicitly compute the rates of the coding schemes. From the discussion in Section 5.4.2 above, we arrive at the fact that using the bit-MAP or block-MAP decoders of $\hat{\mathcal{C}}_m$, the rates of the constrained subcodes of $\hat{\mathcal{C}}_m$, computed in this chapter, are in fact achievable over (d, ∞)-RLL input-constrained BMS channels, so long as $R < C$.

5.5 Our Results

In this section, we briefly state our main theorems, and provide comparisons with the literature. We assume that the BMS channel that we are working with, has an unconstrained capacity of $C \in (0, 1)$.

5.5.1 Rates of Subcodes Under the Lexicographic Coordinate Ordering

We first fix the coordinate ordering of the RM codes to be the standard lexicographic ordering. Our first approach to designing (d, ∞)-RLL constrained codes using RM codes is constructing a sequence of *linear* subcodes of $\{\mathcal{C}_m = \text{RM}(m, r_m)\}_{m \geq 1}$, with r_m as in (5.1), which respect the (d, ∞)-RLL input-constraint, and analyzing the rate of the chosen subcodes. We obtain the following result:

Theorem 5.5.1. *For any $R \in (0,1)$, there exists a sequence of linear (d,∞)-RLL codes $\left\{\mathcal{C}_m^{(d)}\right\}_{m\geq 1}$, where $\mathcal{C}_m^{(d)} \subset \mathcal{C}_m$, of rate $\frac{R}{2^{\lceil \log_2(d+1)\rceil}}$.*

Remark 5.5.2. *We mention here that a sequence of constrained codes of rate $R/(d+1)$ can be constructed by simply taking any sequence of codes of rate R and inserting d 0s between consecutive symbols of codewords in each code. Moreover, using arguments similar to those made previously, if the sequence of codes of rate R achieved vanishing error probabilities over a BMS channel, we have that the sequence of constrained codes of rate $R/(d+1)$ constructed as mentioned will also achieve vanishing error probabilities in the limit as the blocklength goes to infinity, using a suitable decoder. The result in Theorem 5.5.1 is interesting in that a rate that is essentially equal to $R/(d+1)$ can be achieved without increasing the blocklengths of the parent (RM) codes, by using just a sequence of their subcodes.*

The proof of Theorem 5.5.1 (which is Theorem III.2 in [60]), which contains an explicit identification of the subcodes $\left\{\mathcal{C}_m^{(d)}\right\}_{m\geq 1}$, is provided in Section 5.6. From the discussion in Section 5.4.3, we see that by Theorem 5.5.1, using linear constrained subcodes of RM codes over the (d,∞)-RLL input-constrained BEC, a rate of $\frac{1}{d+1}(1-\epsilon)$ is achievable when $d = 2^t - 1$, for some $t \in \mathbb{N}$, and a rate of $\frac{1}{2(d+1)}(1-\epsilon)$ is achievable, otherwise. We note, however, that using random coding arguments, or using the techniques in [21] or [29], a rate of $\kappa_d(1-\epsilon)$ is achievable over the (d,∞)-RLL input-constrained BEC, where κ_d is the noiseless capacity of the input constraint (for example, $\kappa_1 \approx 0.6942$ and $\kappa_2 \approx 0.5515$). For the (d,∞)-RLL input-constrained BSC, similarly, a rate of $\frac{1}{d+1}(1-h_b(p))$ is achievable when $d = 2^t - 1$, for some $t \in \mathbb{N}$, and a rate of $\frac{1}{2(d+1)}(1-h_b(p))$ is achievable, otherwise. Such a result is in the spirit of, but is weaker than, the conjecture by Wolf [32] that a rate of $\kappa_d(1-h_b(p))$ is achievable over the (d,∞)-RLL input-constrained BSC.

For the specific case when $d = 1$, we now state an existence result that provides another lower bound on rates of (potentially non-linear) $(1,\infty)$-RLL constrained subcodes of RM codes of rate R.

Theorem 5.5.3. *For any $R \in (0,1)$ and for any sequence of codes $\left\{\hat{\mathcal{C}}_m = RM(m, r_m)\right\}_{m\geq 1}$ of rate R, following the lexicographic coordinate ordering, there exists a sequence of $(1,\infty)$-RLL*

subcodes of rate at least $\max\left(0, R - \frac{3}{8}\right)$.

The proof of Theorem 5.5.3 is provided in Section 5.6. Again, we note from the discussion in Section 5.4.3, that Theorem 5.5.3 implies that rates of at least $\max\left(0, C - \frac{3}{8}\right)$ are achievable over the (d, ∞)-RLL input-constrained BMS channel. Further, we observe that the lower bound in the theorem above beats the achievable rate of $\frac{R}{2}$ in Theorem 5.5.1, when $R > 0.75$.

5.5.2 Rates Using Other Coding Strategies

We then design (d, ∞)-RLL constrained codes, whose rates improve on those in Theorems 5.5.1 and 5.5.3, by using a two-stage (or concatenated) encoding procedure that employs systematic RM codes of rate R.

Theorem 5.5.4. *For any $R \in (0, 1)$, there exists a sequence of (d, ∞)-RLL constrained concatenated codes $\{\mathcal{C}_m^{conc}\}_{m \geq 1}$, constructed using systematic RM codes of rate R, such that*

$$\liminf_{m \to \infty} rate(\mathcal{C}_m^{conc}) \geq \frac{\kappa_d \cdot R^2 \cdot 2^{-\lceil \log_2(d+1) \rceil}}{R^2 \cdot 2^{-\lceil \log_2(d+1) \rceil} + 1 - R + 2^{-\tau}},$$

where τ is an arbitrarily large, but fixed, positive integer. Further, the rate lower bound above is achievable, under block-MAP decoding, over a (d, ∞)-RLL input-constrained BMS channel, when $R < C$, where C is the capacity of the unconstrained BMS channel.

It can be checked that the rates achieved using Theorem 5.5.4 are better than those achieved using Theorem 5.5.1, and in fact, better than those achieved using any sequence of linear (d, ∞)-RLL subcodes of RM codes (see Chapter 6), for high rates R. Moreover, the rates achieved using Theorem 5.5.4 are larger than those obtained Theorem 5.5.3, for $d = 1$ and for low noise regimes of the BMS channel. For example, when $d = 1$, the rates achieved using the codes in Theorem 5.5.4 are better than those achieved using linear subcodes, for $R \gtrapprox 0.7613$, and are better than those achieved using the subcodes of Theorem 5.5.3, for $R \lessapprox 0.55$ and $R \gtrapprox 0.79$. Figures 5.1 and 5.2 show comparisons between the lower bounds (achievable rates), under block-MAP decoding, in Theorems 5.5.1, 5.5.3, and 5.5.4, with the coset-averaging bound of [47], for

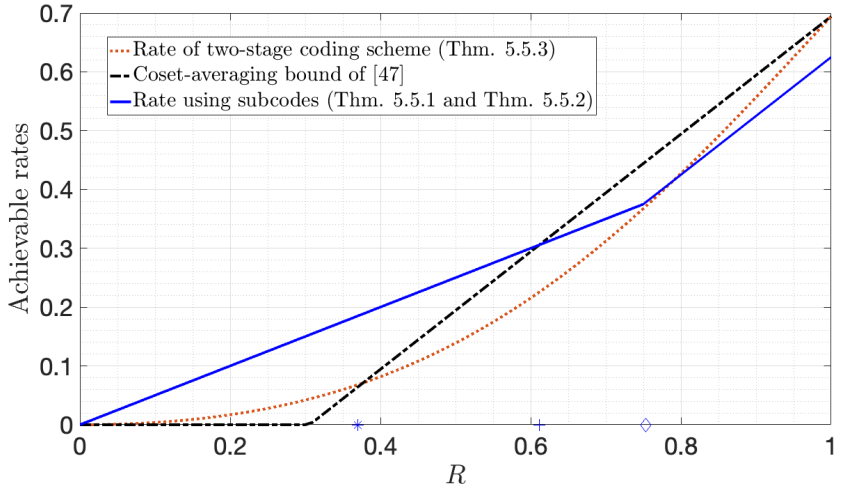


Figure 5.1: Plot comparing, for $d = 1$, the rate lower bounds of $\max\left(\frac{R}{2}, R - \frac{3}{8}\right)$ achieved using subcodes, from Theorems 5.5.1 and 5.5.3, with the rate lower bound achieved using Theorem 5.5.4, with $\tau = 50$, and the coset-averaging lower bound of $\max(0, \kappa_1 + R - 1)$, of [47]. The $*$ and $+$ markers indicate the values of R beyond which the rate of the coset-averaging bound is larger than that of our two-stage coding scheme and the coding scheme using linear subcodes, respectively; the $\Diamond$ marker shows the value of R beyond which the rate of our two-stage coding scheme is larger than the rates achieved using our linear or non-linear subcodes. Here, the noiseless capacity, $\kappa_1 \approx 0.694$.

$d = 1$ and $d = 2$, respectively. While [47] provides existence results on rates achieved using cosets of RM codes, with the rates calculated therein being better than those in Theorem 5.5.4 in the low noise regimes of the BMS channel, our construction is more explicit. The code construction leading to Theorem 5.5.4, and the proof of achievability of the rate lower bound, is taken up in Section 5.7.

We end this section with a remark. Note that the all-ones codeword $\mathbf{1}$ belongs to the RM code. Since any codeword $\mathbf{c}$ that respects the $(0,1)$-RLL constraint can be written as $\mathbf{c} = \mathbf{1} + \hat{\mathbf{c}}$, where $\hat{\mathbf{c}}$ respects the $(1,\infty)$-RLL constraint, the lower bounds of the theorems above hold for the rate of $(0,1)$-RLL subcodes as well. Moreover, since for any $k > 1$, a $(0,1)$-RLL subcode of an RM code is a subset of a $(0,k)$-RLL subcode, the

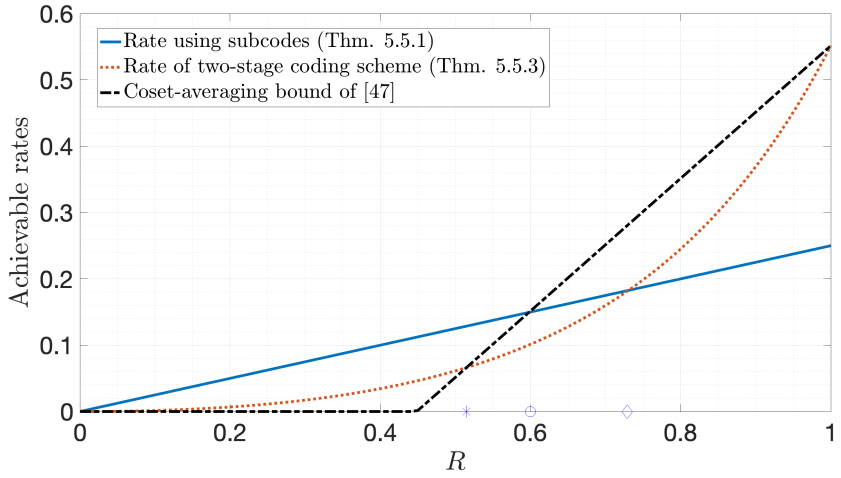


Figure 5.2: Plot comparing, for $d = 2$, the rate lower bound of $R/4$ achieved using subcodes, from Theorem 5.5.1, the rate lower bound achieved using Theorem 5.5.4, with $\tau = 50$, and the coset-averaging lower bound of $\max(0, \kappa_2 + R - 1)$, of [47]. The $*$ and $\circ$ markers indicate the values of R beyond which the rate of the coset-averaging bound is larger than that of our two-stage coding scheme and the coding scheme using linear subcodes, respectively; the $\Diamond$ marker shows the value of R beyond which the rate of our two-stage coding scheme is larger than the rates achieved using our linear subcodes. Here, the noiseless capacity, $\kappa_2 \approx 0.552$.

lower bounds hold over $(0, k)$-RLL input-constrained BMS channels as well.

5.6 Achievable Rates Using Subcodes

As mentioned in Section 5.5, we work with the Reed-Muller (RM) family of codes, $\{\mathcal{C}_m = \mathrm{RM}(m, r_m)\}_{m \geq 1}$, under the lexicographic coordinate ordering, with

$$r_m = \max\left\{\left\lfloor \frac{m}{2} + \frac{\sqrt{m}}{2} Q^{-1}(1-R) \right\rfloor, 0\right\},$$

and rate $R \in (0, 1)$. We then select subcodes of these codes that respect the (d, ∞)-RLL constraint, and compute their rate. We first consider the case when $d = 1$. For this situation, we provide a complete characterization of $(1, \infty)$-RLL constrained subcodes

of RM codes, which will help us identify $(1,\infty)$-RLL constrained subcodes of $\{\mathcal{C}_m\}_{m\geq 1}$. This characterization will also be of use in our derivation of upper bounds on the rates of general (potentially non-linear) $(1,\infty)$-RLL subcodes of RM codes, in Section 6.3.2.

We now set up some definitions and notation for our characterization: we define a "run" of coordinates belonging to a set $\mathcal{A}\subseteq\{0,1\}^m$, to be a contiguous collection of coordinates, $(i, i+1, \ldots, i+\ell-1)$, for some integers $\ell \geq 1$ and $i \in [0 : 2^m - \ell]$, such that $\mathbf{B}(j) \in \mathcal{A}$, for all $i \leq j \leq i+\ell-1$, and $\mathbf{B}(i-1), \mathbf{B}(i+\ell) \notin \mathcal{A}$. To cover the corner cases of $i = 0$ and $i = 2^m - \ell$, we set $\mathbf{B}(i-1)$ and $\mathbf{B}(i+\ell)$, respectively, to be the dummy symbol $\times$, which does not belong to $\mathcal{A}$. The length of such a run is ℓ; note that we allow ℓ to be 1. For example, a run of 1s in a vector $\mathbf{v} \in \{0,1\}^m$ is a collection of contiguous coordinates, $(i, \ldots, i+\ell-1)$, such that $v(i+k) = 1$, for $0 \leq k \leq \ell-1$. Finally, given the code $\mathrm{RM}(m,r)$, for g as in equation (5.2), we let $\Gamma(g)$ denote the set of all coordinates $\mathbf{b}$, excluding the coordinate $(1,1,\ldots,1)$, such that $\mathbf{b}$ is the last coordinate in a run of 0s in $\mathrm{Eval}(g)$, i.e.,

$$\Gamma(g) := \{\boldsymbol{b} = (b_1, \ldots, b_{m-1}) : \ \boldsymbol{b} \text{ is the end of a run of 0s in } \mathrm{Eval}(g), \boldsymbol{b} \neq (1,1,\ldots,1)\}.$$

We now present our characterization of $(1,\infty)$-RLL subcodes of the code $\mathrm{RM}(m,r)$:

Proposition 5.6.1. *For any $\mathrm{Eval}(f) \in RM(m,r)$, we have that $\mathrm{Eval}(f) \in S_{(1,\infty)}$ if and only if the following two conditions (C1) and (C2) are simultaneously satisfied:*

$$\text{(C1): } supp(Eval(g)) \subseteq supp(Eval(h))$$
$$\text{(C2): } h(\boldsymbol{b}) = 0, \text{ if } \boldsymbol{b} \in \Gamma(g),$$

where g, h are as in (5.2).

Proof. First, we shall prove that if $\mathrm{Eval}(f) \in S_{(1,\infty)}$, then (C1) and (C2) hold.

To show that (C1) must hold, let us assume the contrary. Suppose that there exists some evaluation point $\mathbf{b} = (b_1, \ldots, b_{m-1}) \in \mathbb{F}_2^{m-1}$ such that $g(\mathbf{b}) = 1$ and $h(\mathbf{b}) = 0$. Then it follows that at evaluation points $\mathbf{b}_1, \mathbf{b}_2 \in \mathbb{F}_2^m$ such that $\mathbf{b}_1 = \mathbf{b}0$ and $\mathbf{b}_2 = \mathbf{b}1$,

we have $f(\mathbf{b}_1) = f(\mathbf{b}_2) = 1$. Since by construction the points $\mathbf{b}_1$ and $\mathbf{b}_2$ are consecutive in the lexicographic ordering, the codeword $\text{Eval}(f) \notin S_{(1,\infty)}$.

Similarly, to show that (C2) must hold, we assume the contrary. Suppose that there exists some evaluation point $\mathbf{b} = \mathbf{B}_{m-1}(i) \in \mathbb{F}_2^{m-1}$, for some $i \in [0 : 2^{m-1} - 2]$, such that $\mathbf{b} \in \Gamma(g)$ and $h(\mathbf{b}) = 1$. We let $\mathbf{b}' = (b'_1, \ldots, b'_{m-1})$ be such that $\mathbf{b}' = \mathbf{B}_{m-1}(i + 1)$. We note that in the code $\text{RM}(m, r)$, the coordinates $\mathbf{b}_1 = \mathbf{b}1$ and $\mathbf{b}_2 = \mathbf{b}'0$ occur successively. Again, by simply evaluating (5.2) at the coordinates $\mathbf{b}_1$ and $\mathbf{b}_2$, we obtain that $f(\mathbf{b}_1) = f(\mathbf{b}_2) = 1$, implying that the codeword $\text{Eval}(f) \notin S_{(1,\infty)}$.

Next, we shall prove the converse, i.e., that if (C1) and (C2) hold, then $\text{Eval}(f) \in S_{(1,\infty)}$. Pick any pair of consecutive coordinates $\mathbf{z}_1 = \mathbf{B}_m(i)$ and $\mathbf{z}_2 = \mathbf{B}_m(i + 1)$, in the lexicographic ordering, for some $i \in [0 : 2^m - 2]$. Note that it suffices to prove that if (C1) and (C2) hold, then it cannot be that $f(\mathbf{z}_1) = f(\mathbf{z}_2) = 1$. Now, consider the following two cases, for $\mathbf{b}, \mathbf{b}' \in \{0, 1\}^{m-1}$:

1. $\mathbf{z}_1 = \mathbf{b}0$ **and** $\mathbf{z}_2 = \mathbf{b}1$: In this case, if $f(\mathbf{z}_1) = f(\mathbf{b}0) = 1$, then, from the Plotkin decomposition in (5.2), we see that $g(\mathbf{b}) = 1$. From (C1), it hence holds that $h(\mathbf{b}) = 1$. Thus, $f(\mathbf{z}_2) = f(\mathbf{b}1) = g(\mathbf{b}) + h(\mathbf{b}) = 0$.

2. $\mathbf{z}_1 = \mathbf{b}1$ **and** $\mathbf{z}_2 = \mathbf{b}'0$: Suppose that $f(\mathbf{z}_1) = f(\mathbf{b}1) = 1$. This then implies that $\mathbf{b} \notin \Gamma(g)$, since otherwise, $f(\mathbf{z}_1) = g(\mathbf{b}) + h(\mathbf{b}) = 0$, by (C2). Further, it cannot be that $g(\mathbf{b}) = 1$, as then, using (C1), we see that $f(\mathbf{z}_1) = g(\mathbf{b}) + h(\mathbf{b}) = 0$. Hence, it must be that $g(\mathbf{b}) = 0$ and $g(\mathbf{b}') = 0$, in which case, it immediately follows that $f(\mathbf{z}_2) = g(\mathbf{b}') = 0$.

□

5.6.1 Construction of Linear (d, ∞)-RLL Constrained Subcodes

Given the characterization in Proposition 5.6.1, our first construction of a *linear* $(1, \infty)$-RLL subcode of $\mathcal{C}_m$ is simply to pick those codewords $\text{Eval}(f) \in \mathcal{C}_m$ such that $g \equiv 0$, where g is as in equation (5.2). It is straightforward to verify that both (C1) and (C2) in Proposition 5.6.1 are trivially satisfied.

In other words, we define the $(1,\infty)$-RLL constrained subcode $\mathcal{C}_m^{(1)}$ of $\mathcal{C}_m$ to be

$$\mathcal{C}_m^{(1)} := \Big\{ \text{Eval}(f) : f = x_m \cdot h(x_1, \ldots, x_{m-1}), \text{ where } \deg(h) \leq r_m - 1 \Big\}. \tag{5.3}$$

Towards computing the rates of subcodes we work with in this paper, we state and prove the following lemma:

Lemma 5.6.2. *For r_m as defined in* (5.1) *and any sequence of positive integers $(t_m)_{m\geq 1}$ such that $t_m = o(\sqrt{m})$, we have*

$$\lim_{m\to\infty} \frac{1}{2^{m-t_m}} \binom{m-t_m}{\leq r_m} \;=\; R.$$

In particular, for any fixed integer $t > 0$, $\lim_{m\to\infty} \frac{1}{2^m}\binom{m-t}{\leq r_m} = 2^{-t}R$.

Proof. Let S_m denote a $\text{Bin}(m, \frac{1}{2})$ random variable, and note that $\frac{1}{2^{m-t_m}}\binom{m-t_m}{\leq r_m}$ equals $\Pr[S_{m-t_m} \leq r_m]$. Further, note that by our choice of r_m, for any integer $t > 0$, we have for all m large enough,

$$\begin{aligned} |r_m - r_{m-t}| &\leq \left| \frac{m}{2} + \frac{\sqrt{m}}{2} Q^{-1}(1-R) \;-\; \left(\frac{m-t}{2} + \frac{\sqrt{m-t}}{2} Q^{-1}(1-R) \right) + 1 \right| \\ &\leq \frac{t}{2} + \frac{\sqrt{t}}{2} |Q^{-1}(1-R)| + 1. \end{aligned} \tag{5.4}$$

Hence, we have $r_{m-t_m} - \nu_m \leq r_m \leq r_{m-t_m} + \nu_m$, with $\nu_m := \frac{t_m}{2} + \frac{\sqrt{t_m}}{2}|Q^{-1}(1-R)| + 1$. Consequently, $\Pr[S_{m-t_m} \leq r_{m-t_m} - \nu_m] \leq \Pr[S_{m-t_m} \leq r_m] \leq \Pr[S_{m-t_m} \leq r_{m-t_m} + \nu_m]$. Setting $\overline{S}_{m-t_m} := \frac{S_{m-t_m} - \frac{1}{2}(m-t_m)}{\frac{1}{2}\sqrt{m-t_m}}$, we have

$$\begin{aligned} &\Pr[\overline{S}_{m-t_m} \leq Q^{-1}(1-R) - \frac{\nu_m}{\frac{1}{2}\sqrt{m-t_m}}] \\ &\quad\leq\; \Pr[S_{m-t_m} \leq r_m] \\ &\quad\leq\; \Pr[\overline{S}_{m-t_m} \leq Q^{-1}(1-R) + \frac{\nu_m}{\frac{1}{2}\sqrt{m-t_m}}]. \end{aligned} \tag{5.5}$$

Now, by the central limit theorem (or, in this special case, by the de Moivre-Laplace theorem), $\overline{S}_{m-t_m}$ converges in distribution to a standard normal random variable, Z.

Therefore, via (5.5) and the fact that t_m and ν_m are both $o(\sqrt{m})$, we obtain that

$$\lim_{m\to\infty} \Pr[S_{m-t_m} \leq r_m] \;=\; \Pr[Z \leq Q^{-1}(1-R)] \;=\; R,$$

which proves the lemma. □

From Lemma 5.6.2, we calculate the rate of the $(1,\infty)$-RLL constrained subcode $\mathcal{C}_m^{(1)}$ in (5.3) as:

$$\begin{aligned} \text{rate}\left(\mathcal{C}_m^{(1)}\right) \;&=\; \frac{\log_2\left(\left|\mathcal{C}_m^{(1)}\right|\right)}{2^m} \\ &=\; \frac{\binom{m-1}{\leq r_m-1}}{2^m} \;=\; \frac{\binom{m-1}{\leq r_m-1}}{\binom{m-1}{\leq r_m}} \frac{\binom{m-1}{\leq r_m}}{2^m} \;\xrightarrow{m\to\infty}\; \frac{R}{2}. \end{aligned} \tag{5.6}$$

We now extend our simple construction of linear $(1,\infty)$-RLL subcodes in (5.3) and the rate computation in (5.6) to general d, thereby proving Theorem 5.5.1. But before we do so, we state a simple observation, presented below as a lemma. We recall the definition of the support of a vector $\mathbf{c} \in \mathbb{F}_2^n$: $\text{supp}(\mathbf{c}) = \{i : c_i = 1\}$.

Lemma 5.6.3. *Given $d \geq 1$, if $\hat{\mathbf{c}}$ is such that $\hat{\mathbf{c}} \in S_{(d,\infty)}$, and $supp(\mathbf{c}) \subseteq supp(\hat{\mathbf{c}})$, then $\mathbf{c} \in S_{(d,\infty)}$.*

We are now in a position to prove Theorem 5.5.1.

Proof of Theorem 5.5.1. For a fixed $d \geq 1$, let $z := \lceil \log_2(d+1) \rceil$. Consider the subcode $\mathcal{C}_m^{(d)}$ of the code $\mathcal{C}_m$, defined as:

$$\mathcal{C}_m^{(d)} := \left\{ \text{Eval}(f) : f = \left(\prod_{i=m-z+1}^{m} x_i \right) \cdot h(x_1, \ldots, x_{m-z}), \text{where } \deg(h) \leq r_m - z \right\}.$$

It is easy to verify that the polynomial $q(x_{m-z+1}, \ldots, x_m) := \prod_{i=m-z+1}^{m} x_i$ is such that its corresponding evaluation vector, $\text{Eval}(q)$, obeys $\text{Eval}(q) \in S_{(d,\infty)}^{(2^m)}$. This is because $q(\mathbf{y}) = 1$ if and only if $(y_{m-z+1}, \ldots, y_m) = (1, \ldots, 1)$, and in the lexicographic ordering, such evaluation points $\mathbf{y}$ are spaced apart by $2^z - 1$ coordinates, where $2^z - 1 \geq d$.

Now, for any polynomial f such that $\text{Eval}(f) \in \mathcal{C}_m^{(d)}$, it is true that $\text{supp}(\text{Eval}(f)) \subseteq \text{supp}(\text{Eval}(q))$. Hence, $\text{Eval}(f) \in S_{(d,\infty)}^{(2^m)}$ via Lemma 5.6.3.

Finally, the rate of the subcode $\mathcal{C}_m^{(d)}$ can be calculated as follows:

$$\begin{aligned}\text{rate}\left(\mathcal{C}_m^{(d)}\right) &= \frac{\log_2\left(\left|\mathcal{C}_m^{(d)}\right|\right)}{2^m} \\ &= \frac{\binom{m-z}{\leq r_m - z}}{2^m} = \frac{\binom{m-z}{\leq r_m - z}}{\binom{m-z}{\leq r_m}} \frac{\binom{m-z}{\leq r_m}}{2^m} \xrightarrow{m\to\infty} 2^{-z}R.\end{aligned}$$

To obtain the limit as $m \to \infty$, we have used Lemma 5.6.2 and the fact that the ratio $\frac{\binom{m-z}{\leq r_m - z}}{\binom{m-z}{\leq r_m}}$ converges to 1 as $m \to \infty$. Towards proving this fact, note that

$$\begin{aligned}\binom{m-z}{\leq r_m - z} &= \binom{m-z}{\leq r_m} - \sum_{i=r_m-z+1}^{r_m} \binom{m-z}{i} \\ &\geq \binom{m-z}{\leq r_m} - z \cdot \binom{m-z}{\lfloor \frac{m-z}{2} \rfloor},\end{aligned}$$

and hence, we have that

$$1 - \frac{z \cdot \binom{m-z}{\lfloor \frac{m-z}{2} \rfloor}}{\binom{m-z}{\leq r_m}} \leq \frac{\binom{m-z}{\leq r_m - z}}{\binom{m-z}{\leq r_m}} \leq 1.$$

Now, consider the expression $\frac{z\cdot\binom{m-z}{\lfloor \frac{m-z}{2} \rfloor}}{\binom{m-z}{\leq r_m}}$. We have that $\lim_{m\to\infty} \frac{z\cdot\binom{m-z}{\lfloor \frac{m-z}{2} \rfloor}}{2^m} = 0$ (in fact, $\frac{z\cdot\binom{m-z}{\lfloor \frac{m-z}{2} \rfloor}}{2^m} = O\left(\frac{1}{\sqrt{m-z}}\right)$) and that $\lim_{m\to\infty} \frac{\binom{m-z}{\leq r_m}}{2^m} = 2^{-z}R$ (from Lemma 5.6.2). Hence, it follows that $1 - \frac{z\cdot\binom{m-z}{\lfloor \frac{m-z}{2} \rfloor}}{\binom{m-z}{\leq r_m}}$ converges to 1, as $m \to \infty$, implying that the ratio $\frac{\binom{m-z}{\leq r_m - z}}{\binom{m-z}{\leq r_m}}$ also converges to 1 as $m \to \infty$. □

5.6.2 Existence of Larger (Potentially) Non-Linear $(1,\infty)$-RLL Constrained Subcodes

We now proceed to proving Theorem 5.5.3, which establishes the existence of $(1,\infty)$-RLL subcodes of rates better than those in Theorem 5.5.1. Before we do so, we state

and prove a useful lemma on the expected number of runs of 1s in a codeword of a linear code with dual distance at least 3. Let $\mathcal{C}^\perp$ denote the dual code of a given length-n linear code $\mathcal{C}$, and for a binary vector $\mathbf{v} \in \{0,1\}^n$, let $\tau_0(\mathbf{v})$ and $\tau_1(\mathbf{v})$ be the number of runs of 0s and 1s, respectively, in $\mathbf{v}$, with $\tau(\mathbf{v}) := \tau_0(\mathbf{v}) + \tau_1(\mathbf{v})$. Further, given a set A, we define the indicator function $\mathbb{1}\{x \in A\}$ to be 1 when $x \in A$, and 0, otherwise.

Lemma 5.6.4. *Let $\mathcal{C}$ be an $[N, K]$ linear code with $d_{min}(\mathcal{C}^\perp) \geq 3$. Then, by drawing codewords $\mathbf{c} \in \mathcal{C}$ uniformly at random, we have that*

$$\mathbb{E}_{\mathbf{c} \sim Unif(\mathcal{C})}[\tau(\mathbf{c})] = \frac{N+1}{2}.$$

Further,

$$\mathbb{E}_{\mathbf{c} \sim Unif(\mathcal{C})}[\tau_0(\mathbf{c})] = \mathbb{E}_{\mathbf{c} \sim Unif(\mathcal{C})}[\tau_1(\mathbf{c})] = \frac{N+1}{4}.$$

Proof. To prove the first part, we note that for any $\mathbf{c} \in \mathcal{C}$, whose coordinates are indexed by $0, 1, 2, \ldots, N-1$,

$$\tau(\mathbf{c}) = 1 + \#\{0 \leq i \leq N-2 : (c_i, c_{i+1}) = (0,1) \text{ or } (c_i, c_{i+1}) = (1,0)\}. \tag{5.7}$$

Further, since $\mathcal{C}^\perp$ has distance at least 3, it implies that in any two coordinates $i \neq j$ of $\mathcal{C}$, all binary 2-tuples occur, and each with frequency $\frac{1}{4}$ (see e.g. [58, Chapter 5, Theorem 8] for a proof). In particular, from (5.7), we have that

$$\begin{aligned}
\mathbb{E}_{\mathbf{c} \sim \mathrm{Unif}(\mathcal{C})}[\tau(\mathbf{c})] &= 1 + \sum_{i=0}^{N-2} \mathbb{E}[\mathbb{1}\{(c_i, c_{i+1}) = (0,1)\} + \mathbb{1}\{(c_i, c_{i+1}) = (1,0)\}] \\
&= 1 + \sum_{i=0}^{N-2} \Big(\Pr[(c_i, c_{i+1}) = (0,1)] + \Pr[(c_i, c_{i+1}) = (1,0)] \Big) \\
&= 1 + \sum_{i=0}^{N-2} \frac{1}{2} = \frac{N+1}{2}.
\end{aligned}$$

To prove the second part, we note that since $\mathbb{E}[\tau(\mathbf{c})] = \mathbb{E}[\tau_0(\mathbf{c})] + \mathbb{E}[\tau_1(\mathbf{c})]$, it suffices to show that $\mathbb{E}[\tau_0(\mathbf{c})] = \mathbb{E}[\tau_1(\mathbf{c})]$, when $\mathbf{c}$ is drawn uniformly at random from $\mathcal{C}$. To

this end, observe that given any codeword $\mathbf{c} \in \mathcal{C}$, we have that

$$\tau_1(\mathbf{c}) - \tau_0(\mathbf{c}) = \begin{cases} 1, \text{ if } c_0 = c_{N-1} = 1, \\ -1, \text{ if } c_0 = c_{N-1} = 0, \\ 0, \text{ otherwise.} \end{cases}$$

Hence, when $\mathbf{c}$ is drawn uniformly at random from $\mathcal{C}$,

$$\begin{aligned} \mathbb{E}[\tau_1(\mathbf{c})] - \mathbb{E}[\tau_0(\mathbf{c})] &= \mathbb{E}[\mathbb{1}\{(c_0, c_{N-1}) = (1,1)\}] - \mathbb{E}[\mathbb{1}\{(c_0, c_{N-1}) = (0,0)\}] \\ &= \frac{1}{4} - \frac{1}{4} = 0, \end{aligned}$$

thereby proving that $\mathbb{E}[\tau_0(\mathbf{c})] = \mathbb{E}[\tau_1(\mathbf{c})]$. □

The following standard coding-theoretic fact will also prove useful (see [58] or [64] for discussions on shortening codes):

Lemma 5.6.5. *Consider an $[N, K]$ linear code $\mathcal{C}$, and let $T \subseteq [0 : N-1]$ be a collection of its coordinates. If $\mathcal{C}\big|_T$ denotes the restriction of $\mathcal{C}$ to the coordinates in T, and $\mathcal{C}_T$ denotes the code obtained by shortening $\mathcal{C}$ at the coordinates in T, then*

$$dim(\mathcal{C}_T) = K - dim(\mathcal{C}\big|_T).$$

In particular, we have that

$$dim(\mathcal{C}_T) \geq K - |T|.$$

Now, we move on to the proof of Theorem 5.5.3.

Proof of Theorem 5.5.3. Fix any sequence of codes $\left\{\hat{\mathcal{C}}_m = \text{RM}(m, r_m)\right\}_{m \geq 1}$ of rate $R \in (0,1)$. Let $\mathcal{H}_m^{(1)}$ be the largest $(1,\infty)$-RLL subcode of $\hat{\mathcal{C}}_m$. Let $\hat{\mathcal{C}}_{m,+} := \text{RM}(m-1, r_m)$

and $\hat{\mathcal{C}}_{m,-} := \mathrm{RM}(m-1, r_m - 1)$. The following set of equalities then holds:

$$\begin{aligned}
\left|\mathcal{H}_m^{(1)}\right| &= \sum_{f:\ \deg(f)\le r_m} \mathbb{1}\{\mathrm{Eval}(f) \in S_{(1,\infty)}\} \\
&\overset{(a)}{=} \sum_{g:\ \deg(g)\le r_m} \sum_{h:\ \deg(h)\le r_m - 1} \mathbb{1}\{(g,h) \text{ satisfy (C1) and (C2)}\} \\
&= \left|\hat{\mathcal{C}}_{m,+}\right| \cdot \mathbb{E}_{\mathrm{Eval}(g)\sim \mathrm{Unif}(\hat{\mathcal{C}}_{m,+})} \left[\sum_{h:\ \deg(h)\le r_m - 1} \mathbb{1}\{(g,h) \text{ satisfy (C1) and (C2)}\} \right] \\
&= \left|\hat{\mathcal{C}}_{m,+}\right| \cdot \mathbb{E}_{\mathrm{Eval}(g)\sim \mathrm{Unif}(\hat{\mathcal{C}}_{m,+})} \left[\#\{h : (g,h) \text{ satisfy (C1) and (C2)}\} \right], \qquad (5.8)
\end{aligned}$$

where (a) holds from Proposition 5.6.1. The following fact will be of use to us: if $\hat{R}_{m,+} := \mathrm{rate}\left(\hat{\mathcal{C}}_{m,+}\right)$ and $\hat{R}_{m,-} := \mathrm{rate}\left(\hat{\mathcal{C}}_{m,-}\right)$, then

$$\hat{R}_{m,+} + \hat{R}_{m,-} = \frac{\binom{m-1}{\le r_m} + \binom{m-1}{\le r_m - 1}}{2^{m-1}} \xrightarrow{m\to\infty} 2R.$$

Now, from the definitions of (C1) and (C2) in Proposition 5.6.1, we have that for a fixed $\mathrm{Eval}(g) \in \hat{\mathcal{C}}_{m,+}$,

$$\begin{aligned}
&\#\{h : (g,h) \text{ satisfy (C1) and (C2)}\} \\
&\quad = \#\{h : h(\mathbf{b}) = 1\ \forall\ \mathbf{b} \in \mathrm{supp}(\mathrm{Eval}(g)), \text{ and } h(\mathbf{b}') = 0\ \forall\ \mathbf{b}' \in \Gamma(g)\}.
\end{aligned}$$

The right-hand side of the above equality is precisely the number of codewords in the code obtained by shortening $\hat{\mathcal{C}}_{m,-}$ at the coordinates in $S := \mathrm{supp}(\mathrm{Eval}(g)) \cup \Gamma(g)$. Note that

$$|S| = |\mathrm{supp}(\mathrm{Eval}(g))| + |\Gamma(g)| \le \mathrm{wt}(\mathrm{Eval}(g)) + \tau_0(\mathrm{Eval}(g)).$$

Hence, from the second part of Lemma 5.6.5, we have that

$$\#\{h : (g,h) \text{ satisfy (C1) and (C2)}\} \ge \exp_2\left(2^{m-1} \cdot \hat{R}_{m,-} - (\mathrm{wt}(\mathrm{Eval}(g)) + \tau_0(\mathrm{Eval}(g)))\right) \qquad (5.9)$$

Plugging (5.9) back in equation (9.1), we get that for m large enough,

$$\begin{aligned}
&\left|\mathcal{H}_m^{(1)}\right| \\
&\geq \left|\hat{\mathcal{C}}_{m,+}\right| \cdot \mathbb{E}_{\mathrm{Eval}(g)\sim\mathrm{Unif}(\hat{\mathcal{C}}_{m,+})}\left[\exp_2\left(2^{m-1}\cdot\left(\hat{R}_{m,-}-\frac{\mathrm{wt}(\mathrm{Eval}(g))}{2^{m-1}}-\frac{\tau_0(\mathrm{Eval}(g))}{2^{m-1}}\right)\right)\right] \qquad (5.10)\\
&\overset{(b)}{\geq} \left|\hat{\mathcal{C}}_{m,+}\right| \cdot \exp_2\left(2^{m-1}\cdot\left(\hat{R}_{m,-}-\frac{\mathbb{E}[\mathrm{wt}(\mathrm{Eval}(g))]}{2^{m-1}}-\frac{\mathbb{E}[\tau_0(\mathrm{Eval}(g))]}{2^{m-1}}\right)\right)\\
&\overset{(c)}{=} \left|\hat{\mathcal{C}}_{m,+}\right| \cdot \exp_2\left(2^{m-1}\cdot\left(\hat{R}_{m,-}-\frac{1}{2}-\frac{1}{4}-\delta_m\right)\right)\\
&\overset{(d)}{=} \exp_2\left(2^{m}\cdot\left(\frac{\hat{R}_{m,+}+\hat{R}_{m,-}}{2}-\frac{3}{8}-\frac{\delta_m}{2}\right)\right),
\end{aligned}$$

where $\delta_m := \frac{1}{4\cdot 2^{m-1}} \xrightarrow{m\to\infty} 0$. Here, (b) holds by an application of Jensen's inequality and the linearity of expectation. To see why (c) holds, we note that the RM code $\hat{\mathcal{C}}_{m,+}$ has no coordinate that is identically 0. Thus, in a randomly chosen codeword $\mathrm{Eval}(g) \sim \mathrm{Unif}(\hat{\mathcal{C}}_{m,+})$, every coordinate is equally likely to be 0 or 1, and hence,

$$\mathbb{E}[\mathrm{wt}(\mathrm{Eval}(g))] = \sum_{\mathbf{z}\in\{0,1\}^{m-1}} \Pr[g(\mathbf{z})=1] = 2^{m-2}.$$

Moreover, by Lemma 5.6.4, we have that

$$\mathbb{E}[\tau_0(\mathrm{Eval}(g))] = \frac{2^{m-1}+1}{4}.$$

Finally, (d) holds from the fact that $\left|\hat{\mathcal{C}}_{m,+}\right| = \exp_2\left(2^{m-1}\cdot\hat{R}_{m,+}\right)$.

Hence, the largest rate of $(1,\infty)$-RLL constrained subcodes of $\left\{\hat{\mathcal{C}}_m\right\}_{m\geq 1}$ obeys

$$\begin{aligned}
\mathsf{R}^{(1)}(\hat{\mathcal{C}}) &= \limsup_{m\to\infty} \max_{\mathcal{H}_m^{(1)}\subseteq\hat{\mathcal{C}}_m} \frac{\log_2\left|\mathcal{H}_m^{(1)}\right|}{2^m}\\
&\geq \limsup_{m\to\infty} \frac{2^m\cdot\left(\frac{\hat{R}_{m,+}+\hat{R}_{m,-}}{2}-\frac{3}{8}-\frac{\delta_m}{2}\right)}{2^m}\\
&= R-\frac{3}{8}.
\end{aligned}$$

Thus, there exists a sequence of $(1,\infty)$-RLL constrained subcodes of any sequence of RM codes $\{\hat{\mathcal{C}}_m\}_{m\geq 1}$ of rate R, such that the subcodes are of rate of at least $\max\left(0, R-\frac{3}{8}\right)$. □

Although Theorem 5.5.3 proves the existence of non-linear $(1,\infty)$-RLL subcodes of rate larger than (for high rates R) that of the linear subcodes of Theorem 5.5.1, it is of interest to check if further improvements on the rates of $(1,\infty)$-RLL constrained subcodes are possible, by performing numerical computations. For a fixed $R \in (0,1)$, we work with the sequence of RM codes $\left\{\hat{\mathcal{C}}_m = \mathrm{RM}(m, v_m)\right\}_{m\geq 1}$, where

$$v_m := \min\left\{u : \sum_{i=0}^{u}\binom{m}{i} \geq \lfloor 2^m \cdot R \rfloor\right\}.$$

It can be checked that $\mathrm{rate}\left(\hat{\mathcal{C}}_m\right) \xrightarrow{m\to\infty} R$. We then have from inequality (5.10) that

$$\mathsf{R}^{(1)}(\hat{\mathcal{C}}) \geq \max\left\{0, \limsup_{m\to\infty}\left(\frac{\hat{R}_{m,+}+\hat{R}_{m,-}}{2} + \frac{\log_2\left(\mathbb{E}\left[\exp_2\left(-\mathrm{wt}(\mathrm{Eval}(g)) - \tau_0(\mathrm{Eval}(g))\right)\right]\right)}{2^m}\right)\right\}, \tag{5.11}$$

where the expectation is taken over codewords $\mathrm{Eval}(g) \sim \mathrm{Unif}(\hat{\mathcal{C}}_{m,+})$. Inequality (5.11) suggests that one can estimate a lower bound on $\mathsf{R}^{(1)}(\hat{\mathcal{C}})$, by picking a large m and replacing the expectation by a sample average over codewords $\mathrm{Eval}(g)$ chosen uniformly at random from $\hat{\mathcal{C}}_{m,+}$. We can then obtain a new (numerical) lower bound, which does not make use of a further lower bounding argument via Jensen's inequality. We performed this Monte-Carlo sampling and estimation procedure, with $m = 11$, and for varying values of R, by averaging over 10^4 uniformly random samples of codewords, $\mathrm{Eval}(g)$. Figure 5.3 shows a plot comparing the lower bound in (5.11), with the lower bound that is approximately $\hat{R}_m - \frac{3}{8}$, from Theorem 5.5.3, where $\hat{R}_m := \mathrm{rate}\left(\hat{\mathcal{C}}_m\right)$. We observe that there is a noticeable improvement in the numerical rate lower bound, as compared to the bound in Theorem 5.5.3, for some values of $\hat{R}_m$.

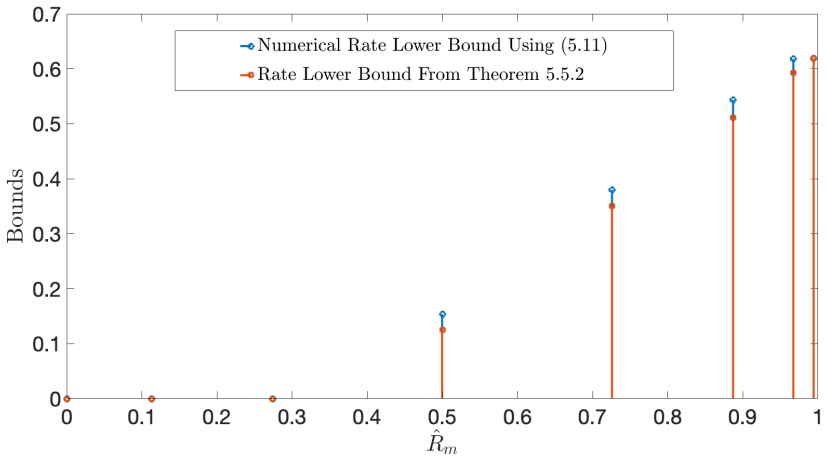


Figure 5.3: Plot comparing, for $d = 1$, the rate lower bound of approximately $\hat{R}_m - \frac{3}{8}$, from Theorem 5.5.3, with the numerical lower bound obtained by Monte-Carlo simulation, using (5.11).

5.7 A Two-Stage Constrained Coding Scheme

The results summarized in the previous sections provide lower bounds on rates of (d, ∞)-RLL constrained subcodes of RM codes of rate R. In particular, Theorem 5.5.1 identifies linear subcodes of RM codes of rate $2^{-\lceil \log_2(d+1) \rceil} \cdot R$, and for the special case when $d = 1$, Theorem 5.5.3 improves upon this lower bound, for a range of R values, by proving the existence of (non-linear) subcodes of rate at least $\max\left(0, R - \frac{3}{8}\right)$. Furthermore, using the bit-MAP or block-MAP decoders corresponding to the parent RM codes, we observe that these rates are achievable over (d, ∞)-RLL input-constrained BMS channels, so long as $R < C$, where C is the capacity of the unconstrained BMS channel. In this section, we provide another explicit construction of (d, ∞)-RLL constrained codes via a concatenated (or two-stage) coding scheme, the outer code of which is a systematic RM code of rate R, and the inner code of which employs the (d, ∞)-RLL constrained subcodes identified in Theorem 5.5.1. The strategy behind our coding scheme is very similar to the "reversed concatenation" scheme that is used to limit error propagation while decoding constrained codes over noisy channels (see

[42–45] and Section 8.5 in [2]). However, to keep the exposition self-contained, we describe the scheme from first principles here. We then derive a rate lower bound for this scheme (see Theorem 5.5.4), and prove that this lower bound is achievable, under *block-MAP* decoding over (d, ∞)-RLL input-constrained BMS channels, if $R < C$. Hence, the lower bound given in Theorem 5.5.4 is achievable, when $R \in (0, 1)$ is replaced by C. Note that here we use the fact that RM codes achieve any rate $R < C$, under block-MAP decoding (see [41]).

We now describe our two-stage coding scheme. Fix a rate $R \in (0, 1)$ and any sequence $\left\{\hat{\mathcal{C}}_m = \mathrm{RM}(m, r_m)\right\}_{m \geq 1}$ of RM codes of rate R. We interchangeably index the coordinates of any codeword in $\hat{\mathcal{C}}_m$ by m-tuples in the lexicographic order, and by integers in $[0 : 2^m - 1]$. We make use of the following fact that is formally proved as Lemma 6.3.3 in the next chapter: the set $\mathcal{I}_{m,r_m} := \{\mathbf{b} = (b_1, \ldots, b_m) \in \mathbb{F}_2^m : \mathrm{wt}(\mathbf{b}) \leq r_m\}$ is an information set of $\hat{\mathcal{C}}_m$. Recall that an information set of a linear code $\mathcal{C}$ is a set of $\dim(\mathcal{C})$ coordinates where all binary $\dim(\mathcal{C})$-tuples occur. For the remainder of this section, we let m be a large positive integer.

We first set up some notation. Let $K_m = \dim\left(\hat{\mathcal{C}}_m\right) = \binom{m}{\leq r_m}$ and $N_m := 2^m$ and note that $N_m - K_m = (1 + \beta_m) N_m (1 - R)$, where β_m is a correction term that vanishes as $m \to \infty$. For the outer code, or the first stage, of our coding scheme, we shall work with an RM code in systematic form, in which the first K_m positions form the information set $\mathcal{I}_{m,r_m}$. Consider any permutation $\pi_m : [0 : N_m - 1] \to [0 : N_m - 1]$ with the property that $\pi_m([0 : K_m - 1]) = \mathcal{I}_{m,r_m}$, where, for a permutation σ, and a set $\mathcal{A} \subseteq [0 : N_m - 1]$, we define the notation $\sigma(\mathcal{A}) := \{\sigma(i) : i \in \mathcal{A}\}$. We then define the equivalent systematic RM code $\mathcal{C}_m^{\pi}$ as

$$\mathcal{C}_m^{\pi} = \left\{(c_{\pi_m(0)}, c_{\pi_m(1)}, \ldots, c_{\pi_m(N_m - 1)}) : (c_0, c_1, \ldots, c_{N_m - 1}) \in \hat{\mathcal{C}}_m\right\}.$$

We let G_m^{π} be a *systematic* generator matrix for $\mathcal{C}_m^{\pi}$. We then recall the definition of the subcode $\mathcal{C}_n^{(d)}$ of the code $\mathcal{C}_n$ (see (5.1) and the proof of Theorem 5.5.1). We let a generator matrix of the linear code $\mathcal{C}_n^{(d)}$ be denoted by $G_n^{(d)}$.

Algorithm 2 Construction of (d, ∞)-RLL constrained code $\mathcal{C}_m^{\text{conc}}$

1: **procedure** CODING-SCHEME(G_m^{π}, $G_{n^\star}^{(d)}$)
2: Pick a (d, ∞)-RLL constrained K_m-tuple $\mathbf{w}$
3: Obtain $\mathbf{c} \in \mathcal{C}_m^{\pi}$ as $\mathbf{c} = \mathbf{w} \cdot G_m^{\pi}$.
4: Set $\mathbf{x}_1 := \mathbf{w}$.
5: Divide $c_{K_m}^{N_m-1}$ into L equal-length blocks, $\mathbf{c}_1, \ldots, \mathbf{c}_L$.
6: **for** $i = 1 : L$ **do**
7: Set $\mathbf{x}_{2,i} = \mathbf{c}_i \cdot G_{n^\star}^{(d)}$.
8: Set $\mathbf{x}_2 = \mathbf{x}_{2,1} \ldots \mathbf{x}_{2,L}$.
9: Transmit $\mathbf{x} = \mathbf{x}_1 \mathbf{x}_2$.

Encoding

Our encoding algorithm is shown as Algorithm 2, where the values of the parameters L and $n^\star$ will be specified later. As mentioned earlier, our (d, ∞)-RLL constrained coding scheme comprises two stages: an outer encoding stage (**E1**) and an inner encoding stage (**E2**) as given below.

(**E1**) Pick a (d, ∞)-RLL constrained K_m-tuple, $\mathbf{w}$. Encode $\mathbf{w}$ into a codeword $\mathbf{c} \in \mathcal{C}_m^{\pi}$, using the systematic generator matrix G_m^{π}: $\mathbf{c} = \mathbf{w} \cdot G_m^{\pi}$. Note that $c_0^{K_m-1} = \mathbf{w}$ is (d, ∞)-RLL constrained. This is shown in Steps 2 and 3 in Algorithm 2. Note that choosing an RLL constrained word in Step (**E1**) above can be accomplished using well-known constrained encoders (see, for example, [67] and Chapters 4 and 5 of [2]), of rates arbitrarily close to the noiseless capacity κ_d of the (d, ∞)-RLL constraint.

(**E2**) Encode the last $N_m - K_m$ bits, $c_{K_m}^{N_m-1}$, of $\mathbf{c}$, using (d, ∞)-RLL constrained codewords of RM codes of rate R, as shown in Steps 5–7 in Algorithm 2. In what follows, we elaborate on the choices of L and $n^\star$ in this part of the algorithm.

The main idea is to encode $c_{K_m}^{N_m-1}$ using the family of linear (d, ∞)-RLL subcodes $\left\{\mathcal{C}_n^{(d)}\right\}_{n \geq 1}$ of rate-R RM codes, given by Theorem 5.5.1. Recall that these subcodes

achieve rate $2^{-\lceil \log_2(d+1) \rceil} \cdot R$ as $n \to \infty$. So, encoding the $N_m - K_m$ bits in $c_{K_m}^{N_m-1}$ using a code $\mathcal{C}_n^{(d)}$ will result in an encoded blocklength of roughly $\left(\frac{N_m-K_m}{R}\right) 2^{\lceil \log_2(d+1) \rceil}$ bits. However, the codes $\mathcal{C}_n^{(d)}$ have blocklength equal to 2^n, so the $\left(\frac{N_m-K_m}{R}\right) 2^{\lceil \log_2(d+1) \rceil}$ encoded bits must be formed by concatenating an integer number of codewords of blocklength 2^n. In other words, $\left(\frac{N_m-K_m}{R}\right) 2^{\lceil \log_2(d+1) \rceil}$ must be an integer multiple of a power of 2. Writing $N_m - K_m \approx N_m(1-R)$ and recalling that $N_m = 2^m$, we observe that $\left(\frac{N_m-K_m}{R}\right) 2^{\lceil \log_2(d+1) \rceil}$ is (approximately) expressible as $\left(\frac{1-R}{R}\right) 2^{m+\lceil \log_2(d+1) \rceil}$. For this to be an integer multiple of a power of 2, $\frac{1-R}{R}$ should be well-approximated by a dyadic rational of the form $\frac{L}{2^\tau}$. Then, choosing $n^\star = m - \tau + \lceil \log_2(d+1) \rceil$, we obtain that $\left(\frac{1-R}{R}\right) 2^{m+\lceil \log_2(d+1) \rceil}$ is (approximately) equal to $L \cdot 2^{n^\star}$. Thus, it should be possible to encode the $N_m - K_m$ bits $c_{K_m}^{N_m-1}$ by first chopping it up into L equal-length blocks, and encoding each block using the code $\mathcal{C}_{n^\star}^{(d)}$. We formalize this argument below.

Pick an arbitrarily small $\epsilon > 0$, and choose large positive integers m_0 and τ, and a positive integer L, such that

$$\frac{(1-R)(1+\beta_m)}{R(1-\epsilon)} \subseteq \left[\frac{L-1}{2^\tau}, \frac{L}{2^\tau}\right], \text{ for all } m \geq m_0. \tag{5.12}$$

Note that L and τ, though large, are constants. We then set $n^\star := m - \tau + \lceil \log_2(d+1) \rceil$. Now, partition the $N_m - K_m$ bits, $c_{K_m}^{N_m-1}$, into L blocks $\mathbf{c}_1, \ldots, \mathbf{c}_L$, each $\mathbf{c}_i$ having $\frac{N_m-K_m}{L}$ bits[2]. As indicated by Step 7 of Algorithm 2, to encode each $\mathbf{c}_i$, $i = 1, \ldots, L$, we use a code $\mathcal{C}_{n^\star}^{(d)}$ from the family of linear (d, ∞)-RLL RM subcodes $\left\{\mathcal{C}_n^{(d)}\right\}_{n \geq 1}$ of rate $2^{-\lceil \log_2(d+1) \rceil} \cdot R$ given by Theorem 5.5.1. We choose $n^\star$ large enough (by taking m large enough) that the rate of the subcode $\mathcal{C}_{n^\star}^{(d)}$ is at least $2^{-\lceil \log_2(d+1) \rceil} \cdot R(1-\epsilon)$. With this, the dimension of the code $\mathcal{C}_{n^\star}^{(d)}$ is

$$\dim\left(\mathcal{C}_{n^\star}^{(d)}\right) \geq 2^{n^\star - \lceil \log_2(d+1) \rceil} \cdot R(1-\epsilon) = 2^{m-\tau} \cdot R(1-\epsilon). \tag{5.13}$$

[2]For ease of description, we assume that m is such that L divides $N_m - K_m$. The general case can be handled by appending at most $L-1$ 0s at the end of the $N_m - K_m$ bits, so that the overall length is divisible by L, thereby giving rise to the same lower bound in Theorem 5.5.4.

From (5.12), we find that $2^{-\tau} \cdot R(1-\epsilon) \geq \frac{1}{L}(1-R)(1+\beta_m)$, so that carrying on from (5.13), we have

$$\dim\left(\mathcal{C}_{n^\star}^{(d)}\right) \geq \frac{1}{L} N_m (1-R)(1+\beta_m) = \frac{N_m - K_m}{L}.$$

This means that each block $\mathbf{c}_i$ can indeed be encoded into a unique codeword of $\mathcal{C}_{n^\star}^{(d)}$, as encapsulated in Step 7 of Algorithm 2.[3] Thus, each $\mathbf{c}_i$ is encoded into a codeword of $\mathcal{C}_{n^\star}^{(d)}$, having blocklength $N_{\text{part}} := 2^{n^\star}$. Hence, the total encoded blocklength for all the blocks $\mathbf{c}_1, \ldots, \mathbf{c}_L$ is $N_{\text{part}} \cdot L$, and the total number of channel uses for transmission (see Step 9 of Algorithm 2) is $N_{\text{tot}} := K_m + N_{\text{part}} \cdot L$.

Moreover, we note from the construction of $\mathcal{C}_n^{(d)}$ in the proof of Theorem 5.5.1 in Section 5.6 that the first d symbols in $\mathbf{x}_{2,i}$ are 0s, for all $i \in [L]$. Hence, the (d, ∞)-RLL input constraint is also satisfied at the boundaries of the concatenations in Steps 8 and 9 of Algorithm 1.

Decoding

Since we intend transmitting the (d, ∞)-RLL constrained code $\mathcal{C}_m^{\text{conc}}$ over a noisy BMS channel, we now specify the decoding strategy. Let $y_0^{N_{\text{tot}}-1}$ be the vector of symbols received by the decoder. Decoding is, as encoding was, a two-stage procedure. In the first stage, the block-MAP decoder of the code $\mathcal{C}_{n^\star} \supseteq \mathcal{C}_{n^\star}^{(d)}$, is used for each of the L parts $\mathbf{c}_1, \ldots, \mathbf{c}_L$, to obtain the estimate $\hat{c}_{K_m}^{N_m-1} := (\hat{c}_{K_m}, \ldots, \hat{c}_{N_m-1})$ of the last $N_m - K_m$ bits $c_{K_m}^{N_m-1}$. In the second stage, the block-MAP decoder of the systematic RM code $\mathcal{C}_m^{\pi}(R)$ takes as input the vector $y_0^{K_m-1}\hat{c}_{K_m}^{N_m-1}$, and produces as (the final) estimate, $\hat{c}_0^{K_m-1} := (\hat{c}_0 \ldots, \hat{c}_{K_m-1})$, of the information bits $c_0^{K_m-1} = \mathbf{w}$. The decoding strategy is summarized below.

(**D1**) Decode each of the L parts $\mathbf{c}_1, \ldots, \mathbf{c}_L$, using the block-MAP decoder of $\mathcal{C}_{n^\star}$, to obtain the estimate $\hat{c}_{K_m}^{N_m-1}$.

[3] It may be necessary to pad $\mathbf{c}_i$ with some extra 0s to make its blocklength match the dimension of $\mathcal{C}_{n^\star}^{(d)}$.

(**D2**) Using the vector $y_0^{K_m-1}\hat{c}_{K_m}^{N_m-1}$ as input to the block-MAP decoder of $\mathcal{C}_m^{\pi}$, obtain the estimate $\hat{c}_0^{K_m-1}$ of the information bits $\mathbf{w}$.

A rate lower bound of the coding scheme in Algorithm 2 and a lower bound on the probability of correct decoding is provided in the proof of Theorem 5.5.4 below.

Proof of Theorem 5.5.4. Consider the code $\mathcal{C}_m^{\text{conc}}$, given in Algorithm 1, for large values of m, and the decoding procedure given in (**D1**)–(**D2**). By picking m large enough (and hence K_m large enough), we note that for Step 2 of Algorithm 1, there exist constrained coding schemes (see [67] and Chapters 4 and 5 of [2]) of rate $\kappa_d - \alpha_m$, for $\alpha_m > 0$, with $\alpha_m \xrightarrow{m\to\infty} 0$. Hence, we see that for large m, the number of possible K_m-tuples $\mathbf{w}$ that can be picked, equals $2^{K_m(\kappa_d-\alpha_m)}$. Since the codeword $\mathbf{c}$ and the words $\mathbf{x}_1$ and $\mathbf{x}_2$ are determined by $\mathbf{w}$, we have that for large m, the rate of the code $\mathcal{C}_m^{\text{cos}}$ obeys

$$\text{rate}(\mathcal{C}_m^{\text{conc}}) \geq \frac{\log_2\left(2^{K_m(\kappa_d-\alpha_m)}\right)}{K_m + N_{\text{part}}\cdot L},$$

where the denominator, $K_m + N_{\text{part}} \cdot L$, is the total number of channel uses. The following statements then hold true:

$$\begin{aligned}
\text{rate}(\mathcal{C}_m^{\text{conc}}) &\geq \frac{\log_2\left(2^{K_m(\kappa_d-\alpha_m)}\right)}{K_m + N_{\text{part}}\cdot L} \\
&\overset{(a)}{=} \frac{\frac{(\kappa_d-\alpha_m)\cdot K_m}{N_m}}{\frac{K_m}{N_m} + L\cdot 2^{-\tau+\lceil\log_2(d+1)\rceil}} \\
&\overset{(b)}{\geq} \frac{\frac{(\kappa_d-\alpha_m)\cdot K_m}{N_m}}{\frac{K_m}{N_m} + 2^{\lceil\log_2(d+1)\rceil}\cdot\left(\frac{(1-R)(1+\beta_m)}{R(1-\epsilon)} + 2^{-\tau}\right)},
\end{aligned}$$

where (a) follows from the definition of N_{part} and (b) holds due to equation (5.12), with $L\cdot 2^{-\tau} \leq \left(\frac{(1-R)(1+\beta_m)}{R(1-\epsilon)} + 2^{-\tau}\right)$. Hence, by taking $\liminf_{m\to\infty}$ on both sides of the

inequality (b) above, we get

$$\begin{aligned}\liminf_{m\to\infty} \text{rate}(\mathcal{C}_m^{\cos}) &\geq \frac{\kappa_d \cdot R}{R + 2^{\lceil \log_2(d+1)\rceil} \cdot \left(\frac{1-R}{R(1-\epsilon)}\right) + 2^{\lceil \log_2(d+1)\rceil - \tau}} \\ &= \frac{(1-\epsilon)\cdot \kappa_d \cdot R^2 \cdot 2^{-\lceil \log_2(d+1)\rceil}}{(1-\epsilon)R^2 \cdot 2^{-\lceil \log_2(d+1)\rceil} + 1 - R + R \cdot 2^{-\tau}(1-\epsilon)} \\ &\geq \frac{(1-\epsilon)\cdot \kappa_d \cdot R^2 \cdot 2^{-\lceil \log_2(d+1)\rceil}}{(1-\epsilon)R^2 \cdot 2^{-\lceil \log_2(d+1)\rceil} + 1 - R + 2^{-\tau}(1-\epsilon)}\end{aligned}$$

where the first inequality holds since $\frac{K_m}{N_m} \xrightarrow{m\to\infty} R$ and $\alpha_m, \beta_m \xrightarrow{m\to\infty} 0$, and the last inequality holds since $R \in (0,1)$. Finally, taking $\epsilon \downarrow 0$, we obtain the rate lower bound in the statement of the Lemma.

We now prove that the rate lower bound derived above, is achievable over a (d,∞)-RLL input-constrained BMS channel, using the decoding procedure given in (**D1**)–(**D2**), as long as $R < C$, where C is the capacity of the unconstrained channel. To this end, note that Step (**D1**) decodes the L parts, $\mathbf{c}_1, \ldots, \mathbf{c}_L$, each with probability of error at most $\eta_m > 0$, with $\eta_m \xrightarrow{m\to\infty} 0$, if $R < C$. Hence, the block probability of error $\Pr\left[\hat{c}_{K_m}^{N_m-1} \neq c_{K_m}^{N_m-1}\right]$ of the decoding stage (**D1**), is at most $L \cdot \eta_m$. Moreover, given the event $\left\{\hat{c}_{K_m}^{N_m-1} = c_{K_m}^{N_m-1}\right\}$, Step (**D2**) determines the information bits $\mathbf{w}$, with conditional block probability of error $\Pr\left[\hat{c}_0^{K_m-1} \neq \mathbf{w} \middle|\, \hat{c}_{K_m}^{N_m-1} = c_{K_m}^{N_m-1}\right] \leq \delta_m$, with $\delta_m > 0$ such that $\delta_m \xrightarrow{m\to\infty} 0$, if $R < C$. Hence, the overall probability of correct estimation of the information bits $\mathbf{w}$ can be bounded as

$$\begin{aligned}\Pr\left[\hat{c}_0^{K_m-1} = \mathbf{w}\right] &\geq \Pr\left[\hat{c}_{K_m}^{N_m-1} = c_{K_m}^{N_m-1}\right] \cdot \Pr\left[\hat{c}_0^{K_m-1} = \mathbf{w} \mid \hat{c}_{K_m}^{N_m-1} = c_{K_m}^{N_m-1}\right] \\ &\geq (1 - L\cdot\eta_m)\cdot(1-\delta_m).\end{aligned}$$

As L is a constant, the lower bound on the probability of correct estimation converges to 1, as $m \to \infty$. □

In Section 5.5, we compared the achievable rate of $\frac{C}{2}$, for $d = 1$, obtained using linear subcodes of RM codes in Theorem 5.5.1 (using the block-MAP decoder of the larger

RM codes), with rates achievable by the two-stage coding scheme above. An equivalent way of stating our observations there is that the two-stage coding scheme achieves a higher rate for erasure probabilities $\epsilon \lessapprox 0.2387$, when used over the $(1, \infty)$-RLL input-constrained BEC, and for crossover probabilities p that are in the approximate interval $(0, 0.0392) \cup (0.9608, 1)$, when used over the $(1, \infty)$-RLL input-constrained BSC.

5.8 Conclusions and Directions for Future Work

In this chapter, we proposed explicit, deterministic coding schemes, without feedback, for binary memoryless symmetric (BMS) channels with (d, ∞)-runlength limited (RLL) constrained inputs. Achievable rates were calculated by identifying specific constrained linear subcodes and proving the existence of constrained, potentially non-linear subcodes, of a sequence of RM codes of rate R. Furthermore, a new explicit two-stage (or concatenated) coding scheme was proposed, whose rates are better than our coding schemes using subcodes, for large R.

There is much scope for future work in this line of investigation. Firstly, using the techniques presented here, it is of interest to check if there exist explicit constructions, using RM codes or any other capacity-achieving (over unconstrained channels) codes of rate R, whose rates beat the coset-averaging lower bound, for all values of $R \in (0, 1)$. We mention that for rates R close to capacity, the coset-averaging lower bound is in general poorer than the linear lower bound derived in Chapter 4, for the input-constrained BEC, and the lower bound conjectured by Wolf (see the Conclusions section in Chapter 4), for the input-constrained BSC.

Next, given the potential of RM codes to achieve good rates over runlength-limited input-constrained BMS channels, as this chapter illustrates, one could try to design explicit coding schemes using RM codes for other channels with memory such as ISI channels (see Chapter 4) and Gilbert-Elliott channels [68], which find application in wireless communications.

Chapter 6

Constrained Coding Schemes Using RM Codes: Upper Bounds[1]

"Remember that you and I made this journey together to a place where there was nowhere left to go."

Jhumpa Lahiri, The Namesake, 2003

6.1 Introduction

In the previous chapter, we discussed lower bounds on the achievable rates of coding schemes designed using Reed-Muller (RM) codes, over input-constrained binary-input memoryless symmetric (BMS) channels. The input constraint of interest, which is the (d, ∞)-RLL constraint, admits only those binary sequences that have at least d 0s between successive 1s (see Definition 2). We first showed an explicit construction of a simple constrained coding scheme using *linear* (d, ∞)-RLL subcodes of RM codes of rate $R \in (0, 1)$. The rate of this coding scheme was shown to be at least $R \cdot 2^{-\lceil \log_2(d+1) \rceil}$.

[1]This chapter depends on and draws from the material in Chapter 5. We hence recommend that the reader reads Chapters 5 and 6 in the order of their presentation.

For the special case when $d = 1$, we then showed the existence of (potentially non-linear) subcodes of rate at least $\max\left(R - \frac{3}{8}, 0\right)$, which beats the rate of the simple linear coding scheme for high values of R. Next, we demonstrated a two-stage (concatenated) constrained coding scheme using RM codes of rate R, whose rate is larger than the rates achievable using just constrained subcodes of RM codes. Finally, we argued that all the rates calculated above are achievable (with error probabilities going to zero as the blocklength goes to infinity) over (d, ∞)-RLL input-constrained BMS channels.

Our objective in this chapter is to derive upper bounds on the rates of (d, ∞)-RLL constrained subcodes of RM codes of rate $R \in (0, 1)$. First, we fix the coordinate ordering to be the standard lexicographic ordering. With this assumption, we then impose the additional restriction that the subcodes be linear. Under this restriction, we show that the linear (d, ∞)-RLL subcodes we constructed in Chapter 5 are essentially rate-optimal. Next, we consider general (not necessarily linear) constrained subcodes of RM codes, and derive an upper bound on the rate of the largest $(1, \infty)$-RLL subcodes of a certain canonical sequence of RM codes of rate R, which we had also used in our lower bounds. Our novel method of analysis involves using an alternative characterization of $(1, \infty)$-RLL codewords of RM codes, and employs properties of the weight distribution of RM codes—a topic that has received revived attention over the last decade (see, for example, the survey [52] and the papers [53–56, 62]). Unfortunately, this method does not readily extend to the (d, ∞)-RLL case, upper bounds for which remain an open problem. We shall then attempt to reconcile our learnings about achievable rates using random codes (in the form of Markov input distributions), from Chapter 4, and the achievable rates using RM codes that we derive, in this chapter.

Next, since permutations of coordinates have the potential to convert a binary word that does not respect the (d, ∞)-RLL constraint to one that does, we ask the question if under alternative coordinate orderings, we can obtain *linear* (d, ∞)-RLL subcodes of RM codes of rate R, of rate larger than the upper bound that we had derived for the case when the coordinates follow the lexicographic ordering. We show that for RM codes of large enough blocklength, under almost all coordinate permutations, linear

(d,∞)-RLL subcodes must respect a rate upper bound that is at most an additive factor of δ larger than our upper bound under the lexicographic ordering, where $\delta > 0$ can be arbitrarily small. We mention that in the context of rates achievable over BMS channels, if we were to replace R in the rates calculated with C (the capacity of the unconstrained BMS channel), then the upper bounds we have computed give rise to upper bounds on rates achievable over (d,∞)-RLL input-constrained BMS channels, if the sub-optimal bit-MAP or block-MAP decoders of the larger RM codes were used for decoding. Moreover, by arguments identical to those made in the end of Section 5.5, we note that our upper bounds also hold for the $(0,1)$-RLL constraint.

We invite the reader to refer to Section 5.4 for the necessary notation and preliminaries on RM codes and BMS channels.

6.2 Our Results

In this section, we briefly state our main theorems, and provide comparisons with the literature. We assume that the BMS channel that we are working with has an unconstrained capacity of $C \in (0,1)$.

6.2.1 Upper Bounds on Rates Under the Lexicographic Coordinate Ordering

We first state a theorem that provides upper bounds on the largest rate of *linear* (d,∞)-RLL subcodes of RM codes, where the coordinates are ordered according to the lexicographic ordering. Fix any sequence of codes $\left\{\hat{\mathcal{C}}_m = \mathrm{RM}(m, r_m)\right\}_{m\geq 1}$ of rate $R \in (0,1)$ and let $\overline{\mathsf{R}}^{(d)}(\hat{\mathcal{C}})$ be the largest rate of linear (d,∞)-RLL subcodes of $\left\{\hat{\mathcal{C}}_m\right\}_{m\geq 1}$. Formally,

$$\overline{\mathsf{R}}^{(d)}(\hat{\mathcal{C}}) := \limsup_{m\to\infty} \max_{\overline{\mathcal{H}}^{(d)} \subseteq \hat{\mathcal{C}}_m} \frac{\log_2 \left|\overline{\mathcal{H}}^{(d)}\right|}{2^m}, \tag{6.1}$$

where the maximization is over linear (d,∞)-RLL subcodes $\overline{\mathcal{H}}^{(d)}$ of $\hat{\mathcal{C}}_m$. Then,

Theorem 6.2.1. *For any $R \in (0,1)$ and for any sequence of codes $\left\{\hat{\mathcal{C}}_m = RM(m, r_m)\right\}_{m\geq 1}$ of rate R, following the lexicographic coordinate ordering,*

$$\overline{\mathsf{R}}^{(d)}(\hat{\mathcal{C}}) \leq \frac{R}{d+1}.$$

Thus, Theorem 6.2.1 shows that the sequence of simple linear subcodes $\left\{\mathcal{C}_m^{(d)}\right\}_{m\geq 1}$, identified in Theorem 5.5.1, is rate-optimal whenever $d+1$ is a power of 2, in that it achieves the rate upper bound of $\frac{R}{d+1}$. Moreover, it follows from Theorem 6.2.1, that the subcodes identified in Theorem 5.5.3 must be *non-linear* when $R > 0.75$. Theorem 6.2.1 is proved in Section 6.3.1. Also, from the discussion in Section 5.4.3 and from Theorem 6.2.1, we see that the largest rate achievable over a (d,∞)-RLL input-constrained BMS channel, using linear (d,∞)-RLL subcodes of RM codes, when the sub-optimal bit-MAP or block-MAP decoders of the larger RM codes are used, is bounded above by $\frac{C}{d+1}$.

We remark here that the problem of identifying linear codes that are subsets of the set of (d,∞)-RLL sequences of a fixed length, has been studied in [61]. The results therein show that the largest linear code within $S_{(d,\infty)}^{(n)}$ has rate no larger than $\frac{1}{d+1}$, as $n \to \infty$. However, such a result offers no insight into rates achievable over BMS channels.

Concluding the discussion on rates achievable using subcodes of RM codes, following the lexicographic coordinate ordering, we state a theorem that provides an upper bound on the largest rate of $(1,\infty)$-RLL subcodes of the sequence $\{\mathcal{C}_m = \mathrm{RM}(m, r_m)\}_{m\geq 1}$, where r_m is as in (5.1). We formally define this largest rate to be

$$\mathsf{R}^{(1)}(\mathcal{C}) := \limsup_{m\to\infty} \max_{\mathcal{H}^{(1)}\subseteq\mathcal{C}_m} \frac{\log_2\left|\mathcal{H}^{(1)}\right|}{2^m},$$

where the maximization is over $(1,\infty)$-RLL subcodes $\mathcal{H}^{(1)}$ of $\mathcal{C}_m$. Then,

Theorem 6.2.2. *For the sequence of codes* $\{\mathcal{C}_m = RM(m, r_m)\}_{m\geq 1}$*, with* r_m *as in* (5.1)*,*

$$\mathsf{R}^{(1)}(\mathcal{C}) \leq \min\left(\frac{7R}{8}, \kappa_1\right),$$

where $\kappa_1 = \log_2\left(\frac{1+\sqrt{5}}{2}\right) \approx 0.6942$ *is the noiseless capacity of the* $(1,\infty)$*-RLL constraint.*

The proof of the theorem is taken up in Section 6.3.2. We note that the upper bound in the theorem above is an improvement over the upper bound in [60], due to the use of better upper bounds on the weight distribution, from [56], as compared to those in [62]. Figure 6.1 shows a comparison between the upper bound in Theorem 6.2.2, and the lower bounds of Theorems 5.5.1 and 5.5.3, for the case when $d = 1$. From the discussion in Section 5.4.3, we see that Theorem 6.2.2 shows that the rate achievable over $(1,\infty)$-RLL input-constrained BMS channels, using constrained subcodes of $\{\mathcal{C}_m\}_{m\geq 1}$, when the sub-optimal bit-MAP or block-MAP decoders of the larger RM codes are used, is bounded above by $\min\left(\frac{7C}{8}, \kappa_1\right)$, where C is the capacity of the unconstrained BMS channel. Figure 6.2 shows comparisons, for the specific case of the $(1,\infty)$-RLL input-constrained BEC, of the upper bound of $\min\left(\frac{7}{8}\cdot(1-\epsilon), \kappa_1\right)$, obtained by sub-optimal decoding, in Theorem 6.2.2, with the achievable rate of $\kappa_1 \cdot (1-\epsilon)$ (from [63] and [29]), and the numerically computed achievable rates using the Monte-Carlo method in [14] (or the stochastic approximation scheme in Chapter 4). For large values of the erasure probability ϵ, we observe that the upper bound of $\min\left(\frac{7}{8}\cdot(1-\epsilon), \kappa_1\right)$ lies below the achievable rates of [14], thereby indicating that it is not possible to achieve the capacity of the $(1,\infty)$-RLL input-constrained BEC, using $(1,\infty)$-RLL subcodes of $\{\mathcal{C}_m\}_{m\geq 1}$, when the bit-MAP or block-MAP decoders of $\{\mathcal{C}_m\}_{m\geq 1}$ are used for decoding. We conjecture that this numerically verified fact is indeed true.

6.2.2 Rates of Subcodes Under Alternative Coordinate Orderings

Next, we consider situations where the coordinates of the RM codes follow orderings different from the standard lexicographic ordering. First, we study upper bounds on the rates of *linear* (d,∞)-RLL subcodes of RM codes, whose coordinates are ordered

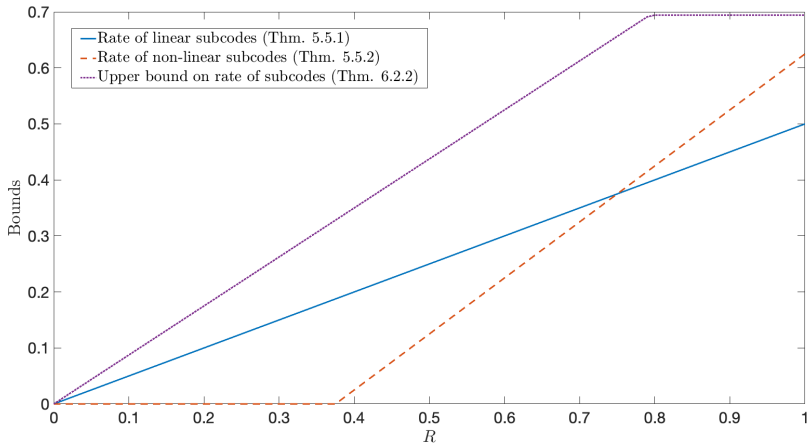


Figure 6.1: A comparison between the upper bound of Theorem 6.2.2 and achievable rates of $R/2$ and $\max\left(0, R - \frac{3}{8}\right)$, from Theorems 5.5.1 and 5.5.2, respectively, when $d = 1$.

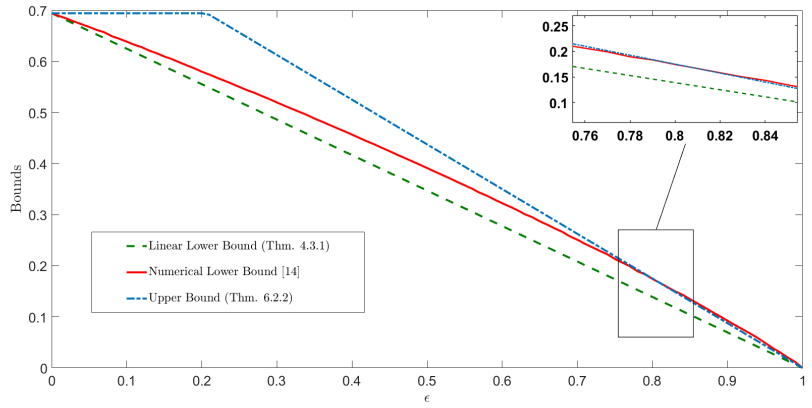


Figure 6.2: A comparison between the upper bound of Theorem 6.2.2 and the achievable rates of [63] and [14] (or equivalently, Algorithm 1 in Chapter 4). For large ϵ, the upper bound of Theorem 6.2.2, under sub-optimal decoding, lies below the numerically-computed achievable rates in [14].

according to a Gray ordering (see Section 6.3.3 for a description of a Gray ordering). For a fixed $R \in (0,1)$, let $\left\{\mathcal{C}_m^{\mathrm{G}}\right\}_{m\geq 1}$ be any sequence of RM codes following a Gray coordinate ordering, such that $\mathrm{rate}\left(\mathcal{C}_m^{\mathrm{G}}\right) \xrightarrow{m\to\infty} R$. Let $\overline{\mathrm{R}}^{(d)}(\mathcal{C}^{\mathrm{G}})$ denote the largest rate

of *linear* (d,∞)-RLL subcodes of $\left\{\mathcal{C}_m^{\mathrm{G}}\right\}_{m\geq 1}$. Formally,

$$\overline{\mathsf{R}}^{(d)}(\mathcal{C}^{\mathrm{G}}) := \limsup_{m\to\infty} \max_{\overline{\mathcal{H}}_{\mathrm{G}}^{(d)} \subseteq \mathcal{C}_m^{\mathrm{G}}} \frac{\log_2 \left|\overline{\mathcal{H}}_{\mathrm{G}}^{(d)}\right|}{2^m}, \tag{6.2}$$

where the maximization is over linear (d,∞)-RLL subcodes $\overline{\mathcal{H}}_{\mathrm{G}}^{(d)}$ of $\mathcal{C}_m^{\mathrm{G}}(R)$. We obtain the following result:

Theorem 6.2.3. *For any $R \in (0,1)$ and for any sequence of RM codes $\left\{\mathcal{C}_m^{G}\right\}_{m\geq 1}$ of rate R, following a Gray coordinate ordering,*

$$\overline{\mathsf{R}}^{(d)}(\mathcal{C}^{G}) \leq \frac{R}{d+1}.$$

The proof of Theorem 6.2.3 is provided in Section 6.3.3. Again, Theorem 6.2.3 provides an upper bound on the rates achieved over a (d,∞)-RLL input-constrained BMS channel, using linear subcodes of Gray-ordered RM codes of rate R, when the sub-optimal bit-MAP or block-MAP decoders of $\left\{\mathcal{C}_m^{\mathrm{G}}\right\}_{m\geq 1}$ are used, for decoding.

Now, we consider arbitrary orderings of coordinates, defined by the sequence of permutations $(\pi_m)_{m\geq 1}$, with $\pi_m : [0 : 2^m - 1] \to [0 : 2^m - 1]$. As with the Gray coordinate ordering, we define the sequence of π-ordered RM codes $\{\mathcal{C}_m^{\pi}\}_{m\geq 1}$, with

$$\mathcal{C}_m^{\pi} := \left\{(c_{\pi_m(0)}, c_{\pi_m(1)}, \ldots, c_{\pi_m(2^m-1)}) : (c_0, c_1, \ldots, c_{2^m-1}) \in \hat{\mathcal{C}}_m\right\},$$

where $\left\{\hat{\mathcal{C}}_m = \mathrm{RM}(m, r_m)\right\}_{m\geq 1}$ is any sequence of RM codes of rate R. We also define $\overline{\mathcal{H}}_{\pi}^{(d)}$ be the largest *linear* (d,∞)-RLL subcode of $\mathcal{C}_m^{\pi}$. The theorem below is then shown to hold:

Theorem 6.2.4. *For any $R \in (0,1)$, for large m and for all but a vanishing fraction of coordinate permutations, $\pi_m : [0 : 2^m - 1] \to [0 : 2^m - 1]$, the following rate upper bound holds:*

$$\frac{\log_2 \left|\overline{\mathcal{H}}_{\pi}^{(d)}\right|}{2^m} \leq \frac{R}{d+1} + \epsilon_m,$$

where $\epsilon_m \xrightarrow{m\to\infty} 0$.

Section 6.3.3 contains the proof of Theorem 6.2.4.

6.3 Upper Bounds on Rates of Constrained Subcodes

In this section, we derive upper bounds on the rates of (d,∞)-RLL constrained subcodes of RM codes of rate $R \in (0,1)$. In the first subsection, we restrict our subcodes to be linear, while in the second subsection, we fix d to be 1 and relax the assumption of linearity of the subcodes. Additionally, in the first two subsections, we assume that the RM codes follow a lexicographic coordinate ordering. We consider RM codes under other coordinate orderings in the last subsection, and derive upper bounds on the rates of linear (d,∞)-RLL constrained subcodes.

6.3.1 Linear Subcodes

We fix a sequence of codes $\left\{\hat{\mathcal{C}}_m = \mathrm{RM}(m, r_m)\right\}_{m\geq 1}$ of rate R, whose coordinates follow a lexicographic ordering. We first state and prove a fairly general proposition on the rates of linear (d,∞)-RLL subcodes of linear codes. Recall that for an $[N,K]$ linear code $\mathcal{C}$ over $\mathbb{F}_2$, of blocklength N and dimension K, an information set is a collection of K coordinates in which all possible K-tuples over $\mathbb{F}_2$ can appear. Equivalently, if G is any generator matrix for $\mathcal{C}$, an information set is a set of K column indices such that G restricted to those columns is a full-rank matrix. As usual, we index the coordinates of the code from 0 to $N-1$.

Proposition 6.3.1. *Let $\mathcal{C}$ be an $[N,K]$ binary linear code. If $\mathcal{I}$ is an information set of $\mathcal{C}$ that contains t disjoint $(d+1)$-tuples of consecutive coordinates $(i_1, i_1+1, \ldots, i_1+d), (i_2, i_2+1, \ldots, i_2+d), ..., (i_t, i_t+1, \ldots, i_t+d)$, with $i_1 \geq 0$, $i_j > i_{j-1}+d$, for all $j \in [2:t]$, and $i_t \leq N-1-d$, then the dimension of any linear (d,∞)-RLL subcode of $\mathcal{C}$ is at most $K-dt$.*

Proof. Suppose that the information set $\mathcal{I}$ contains exactly t disjoint $(d+1)$-tuples of

consecutive coordinates as in the statement of the proposition. By definition, all possible K-tuples appear in the coordinates in $\mathcal{I}$. Now, consider any linear (d,∞)-RLL subcode $\overline{\mathcal{C}}$ of $\mathcal{C}$, and any $(d+1)$-tuple of consecutive coordinates $\{i_j, i_j+1, \ldots, i_j+d\} \in \mathcal{I}$, for $j \in [t]$. Since the (d,∞)-RLL constraint requires that successive 1s be separated by at least d 0s, the only possible tuples of $d+1$ consecutive symbols in any codeword of the linear subcode are $(0,0,\ldots,0)$ and at most one of $\mathbf{e}_i^{(d+1)}$, $i \in [d+1]$. This is because, if $\mathbf{e}_i^{(d+1)}$ and $\mathbf{e}_j^{(d+1)}$ both occur in a collection of $d+1$ consecutive positions, then, by linearity of the subcode $\overline{\mathcal{C}}$, we have $\mathbf{e}_i^{(d+1)} + \mathbf{e}_j^{(d+1)}$ (where the addition is over vectors in $\mathbb{F}_2^{d+1}$) must occur in some codeword of the subcode, thereby making the codeword not (d,∞)-RLL compliant. Hence, for every $(d+1)$-tuple of consecutive coordinates in $\mathcal{I}$, only a 2^{-d} fraction of the 2^{d+1} possible tuples are allowed. Thus, overall, the number of possible K-tuples that can appear in the information set $\mathcal{I}$ in the codewords of the linear subcode is at most $\frac{2^K}{2^{dt}}$. Hence, the number of codewords in the linear subcode is at most 2^{K-dt}.

□

In order to obtain an upper bound, as in Theorem 6.2.1, on the rate of linear (d,∞)-RLL subcodes of the sequence of codes $\{\hat{\mathcal{C}}_m\}_{m\geq 1}$, we shall first identify an information set of $\hat{\mathcal{C}}_m = \mathrm{RM}(m, r_m)$. We then compute the number of disjoint $(d+1)$-tuples of consecutive coordinates in the information set, and apply Proposition 6.3.1 to get an upper bound on the dimension of the linear constrained subcodes.

Given the integers m and r, consider the binary linear code $\tilde{\mathcal{C}}(m,r)$ (which is a subspace of $\mathbb{F}_2^{2^m}$), spanned by the codewords in the set

$$\mathcal{B}_{m,r} := \left\{ \mathrm{Eval}\left(\prod_{i\in S} x_i \right) : S \subseteq [m] \text{ with } |S| \geq r+1 \right\}. \tag{6.3}$$

From the discussion in Section 5.4.3, we observe that the vectors in $\mathcal{B}_{m,r}$ are linearly independent, and, hence, $\mathcal{B}_{m,r}$ forms a basis for $\tilde{\mathcal{C}}(m,r)$, with $\dim\big(\tilde{\mathcal{C}}(m,r)\big) = \binom{m}{\geq r+1}$. Moreover, the codewords in $\tilde{\mathcal{C}}(m,r)$ are linearly independent from codewords in $\mathrm{RM}(m,r)$, since the evaluation vectors of all the distinct monomials in the variables

$x_1, \ldots, x_m$ are linearly independent over $\mathbb{F}_2$.

The following lemma identifies an alternative basis for $\tilde{\mathcal{C}}(m,r)$, which will prove useful in our analysis, later on.

Lemma 6.3.2. *Consider the code $\tilde{\mathcal{C}}(m,r) = span\,(\mathcal{B}_{m,r})$, where $\mathcal{B}_{m,r}$ is as in* (6.3)*. We then have that $\tilde{\mathcal{C}}(m,r) = span\,(\{\mathbf{e_b} : wt(\mathbf{b}) \geq r+1\})$.*

Proof. Note that any standard basis vector $\mathbf{e_b}$, with $\mathrm{wt}(\mathbf{b}) \geq r+1$, can be written as $\mathrm{Eval}(f)$, where

$$f(x_1, \ldots, x_m) = \prod_{i \in \mathrm{supp}(\mathbf{b})} x_i \cdot \prod_{i \notin \mathrm{supp}(\mathbf{b})} (1 + x_j).$$

From the fact that $\mathrm{wt}(\mathbf{b}) \geq r+1$, we have that the degree of any monomial in f is at least $r+1$, and hence, $\mathrm{Eval}(f) = \mathbf{e_b} \in \mathrm{span}(\mathcal{B}_{m,r}) = \tilde{\mathcal{C}}(m,r)$. The result follows by noting that $\{\mathbf{e_b} : \mathrm{wt}(\mathbf{b}) \geq r+1\}$ is a collection of linearly independent vectors of size $\binom{m}{\geq r+1}$, which, in turn, equals $\dim\big(\tilde{\mathcal{C}}(m,r)\big)$. □

We now introduce some further notation: given a $p \times q$ matrix M, we use the notation $M[\mathcal{U}, \mathcal{V}]$ to denote the submatrix of M consisting of the rows in the set $\mathcal{U} \subseteq [p]$ and the columns in the set $\mathcal{V} \subseteq [q]$. We recall the definition of the generator matrix $G_{\mathrm{Lex}}(m,r)$, of $\mathrm{RM}(m,r)$, and the indexing of columns of the matrix, from Section 5.4.3. Finally, towards identifying an information set of $\mathrm{RM}(m,r)$, we define the set of coordinates

$$\mathcal{I}_{m,r} := \{\mathbf{b} = (b_1, \ldots, b_m) \in \mathbb{F}_2^m : \mathrm{wt}(\mathbf{b}) \leq r\}. \tag{6.4}$$

Lemma 6.3.3. *The set of coordinates $\mathcal{I}_{m,r}$ is an information set of $RM(m,r)$.*

Proof. In order to prove that $\mathcal{I}_{m,r}$ is an information set of $\mathrm{RM}(m,r)$, it is sufficient to show that $G_{\mathrm{Lex}}(m,r)$ restricted to the columns in $\mathcal{I}_{m,r}$ is full rank.

Now, consider the generator matrix $\tilde{G}(m,r)$, of $\tilde{\mathcal{C}}(m,r)$, consisting of rows that are vectors in $\mathcal{B}_{m,r}$. We build the $2^m \times 2^m$ matrix

$$\mathsf{H} := \left[\begin{array}{c} \tilde{G}(m,r) \\ \hline \\ G_{\mathrm{Lex}}(m,r) \end{array}\right],$$

with H being full rank. Note that, from Lemma 6.3.2, any standard basis vector $\mathbf{e_b}$, with $\mathbf{b} \in \mathcal{I}^c_{m,r}$, belongs to rowspace$(\tilde{G}(m,r))$. By Gaussian elimination, it is then possible to replace the first $\binom{m}{\geq r+1}$ rows of H, corresponding to the submatrix $\tilde{G}(m,r)$, with the standard basis vectors $\mathbf{e_b}$, with $\mathbf{b} \in \mathcal{I}^c_{m,r}$. Clearly, from the fact that H is full rank, this then means that $\mathsf{H}\left[\left[\binom{m}{\geq r+1}+1 : 2^m\right], \mathcal{I}_{m,r}\right]$ is full rank, or equivalently, $G_{\text{Lex}}(m,r)$ restricted to columns in $\mathcal{I}_{m,r}$ is full rank. □

We thus have that an information set of $\hat{\mathcal{C}}_m$ is $\mathcal{I}_{m,r_m}$. Note that in order to get an upper bound on the rate of linear (d,∞)-RLL subcodes of $\hat{\mathcal{C}}_m$, we need only calculate the number of disjoint $(d+1)$-tuples of consecutive coordinates in $\mathcal{I}_{m,r_m}$.

To this end, for any $0 \leq r \leq m-1$, we define

$$\Gamma_{m,r} := \{s \in [0 : 2^m - 2] : \mathbf{B}(s) \in \mathcal{I}_{m,r}, \text{ but } \mathbf{B}(s+1) \notin \mathcal{I}_{m,r}\}, \tag{6.5}$$

to be the set of right end-point coordinates of runs that belong to $\mathcal{I}_{m,r}$. We refer the reader to Section 5.6 for the definition of a run of coordinates belonging to a specific set. The number of such runs is $|\Gamma_{m,r}|$. Observe that since $r \leq m-1$, we have $2^m - 1 \notin \mathcal{I}_{m,r}$. In the case where $r = m$, we have that $\mathcal{I}_{m,r} = [0 : 2^m - 1]$, and we define $\Gamma_{m,r}$ to be $\{2^m - 1\}$. However, this special case need not be considered, for our purposes.

Lemma 6.3.4. *For $0 \leq r \leq m-1$, the equality $|\Gamma_{m,r}| = \binom{m-1}{r}$ holds.*

Proof. Let $r \in [0 : m-1]$. Note that every right end-point of a run, $s \in \Gamma_{m,r}$, with $s \in [0 : 2^m - 2]$, is such that $\text{wt}(\mathbf{B}(s)) \leq r$, but $\text{wt}(\mathbf{B}(s+1)) \geq r+1$. We now claim that an integer $s \in \Gamma_{m,r}$ iff $\mathbf{B}(s) = (b_1, \ldots, b_{m-1}, 0)$, for $b_1, \ldots, b_{m-1} \in \{0,1\}$, with $\text{wt}((b_1, \ldots, b_{m-1}, 0)) = r$.

To see this, note that if $\mathbf{B}(s) = (b_1, \ldots, b_{m-1}, 0)$, then $\mathbf{B}(s+1) = (b_1, \ldots, b_{m-1}, 1)$. Hence, if $\text{wt}((b_1, \ldots, b_{m-1})) = r$, then $s \in \Gamma_{m,r}$. Conversely, if $s \in \Gamma_{m,r}$, then $\mathbf{B}(s)$ cannot end in a 1. Indeed, if this were the case, then we would have $\mathbf{B}(s)$ being of the form $(b_1, \ldots, b_\ell, 0, 1, \ldots, 1)$, with $b_1, \ldots, b_\ell \in \{0,1\}$, so that $\mathbf{B}(s+1)$ would be $(b_1, \ldots, b_\ell, 1, 0, \ldots, 0)$, the weight of which does not exceed that of $\mathbf{B}(s)$. So, $\mathbf{B}(s)$ must

be of the form $(b_1, \ldots, b_{m-1}, 0)$, and so, $\mathbf{B}(s+1) = (b_1, \ldots, b_{m-1}, 1)$. From $\mathrm{wt}(\mathbf{B}(s)) \leq r$ and $\mathrm{wt}(\mathbf{B}(s+1)) \geq r+1$, we obtain that $\mathrm{wt}(b_1 \ldots b_{m-1}) = r$.

This then implies that the number of runs, which is equal to the number of right end-points of runs, exactly equals $\binom{m-1}{r}$. □

With the ingredients in place, we are now in a position to prove Theorem 6.2.1.

Proof of Theorem 6.2.1. Fix a sequence of codes $\left\{\hat{\mathcal{C}}_m = \mathrm{RM}(m, r_m)\right\}_{m \geq 1}$ of rate $R \in (0,1)$, with $r_m \leq m-1$, for all m. We use the notation $K_m := \binom{m}{\leq r_m}$ to denote the dimension of $\hat{\mathcal{C}}_m$.

Now, for a given m, consider the information set $\mathcal{I}_{m,r_m}$ (see (6.4)). We know from Lemma 6.3.4 that the number of runs, $|\Gamma_{m,r_m}|$, of coordinates that lie in $\mathcal{I}_{m,r_m}$, is exactly $\binom{m-1}{r_m}$. Now, note that the i^{th} run $(s_i, \ldots, s_i + \ell_i - 1)$, of length ℓ_i, with $s_i \in \Gamma_{m,r_m}$ and $i \in [|\Gamma_{m,r_m}|]$, contributes $\left\lfloor \frac{\ell_i}{d+1} \right\rfloor$ disjoint $(d+1)$-tuples of consecutive coordinates in $\mathcal{I}_{m,r}$. It then holds that the overall number of disjoint $(d+1)$-tuples of consecutive coordinates in $\mathcal{I}_{m,r}$ is t_m, where

$$\begin{aligned} t_m &= \sum_{i=1}^{|\Gamma_{m,r_m}|} \left\lfloor \frac{\ell_i}{d+1} \right\rfloor \\ &\geq \sum_{i=1}^{|\Gamma_{m,r_m}|} \left(\frac{\ell_i}{d+1} - 1 \right) \\ &= \frac{K_m}{d+1} - |\Gamma_{m,r_m}| = \frac{K_m}{d+1} - \binom{m-1}{r_m}, \end{aligned}$$

where the last equality follows from Lemma 6.3.4.

Using Proposition 6.3.1, it follows that the dimension of any linear (d,∞)-RLL subcode $\overline{\mathcal{H}}^{(d)} \subseteq \hat{\mathcal{C}}_m$ is at most $K_m - dt_m$. Then,

$$\begin{aligned}
\overline{\mathsf{R}}^{(d)}(\hat{\mathcal{C}}) &= \limsup_{m\to\infty} \max_{\overline{\mathcal{H}}^{(d)} \subseteq \hat{\mathcal{C}}_m} \frac{\log_2 \left|\overline{\mathcal{H}}^{(d)}\right|}{2^m} \\
&\leq \limsup_{m\to\infty} \frac{K_m - dt_m}{2^m} \\
&\leq \limsup_{m\to\infty} \frac{K_m - \frac{dK_m}{d+1} + d\cdot\binom{m-1}{r_m}}{2^m} \\
&\leq \lim_{m\to\infty} \frac{\frac{K_m}{d+1} + d\cdot\binom{m-1}{\lfloor\frac{m-1}{2}\rfloor}}{2^m} \\
&= \frac{R}{d+1},
\end{aligned}$$

where the last equality holds from the fact that $\binom{m-1}{\lfloor\frac{m-1}{2}\rfloor}$ is $O\left(\frac{2^m}{\sqrt{m-1}}\right)$, and $\lim_{m\to\infty} \frac{K_m}{2^m} = R$. □

6.3.2 General Subcodes

In this section, we provide upper bounds on the rates of $(1,\infty)$-RLL subcodes of $\{\mathcal{C}_m = \mathrm{RM}(m, r_m)\}_{m\geq 1}$, where

$$r_m = \max\left\{\left\lfloor \frac{m}{2} + \frac{\sqrt{m}}{2} Q^{-1}(1-R)\right\rfloor, 0\right\}.$$

Recall that $\{\mathcal{C}_m = \mathrm{RM}(m, r_m)\}_{m\geq 1}$ is a sequence of RM codes of rate R. We fix the coordinate ordering to be the standard lexicographic ordering.

Recall also, from Lemma 5.6.1, that any $(1,\infty)$-RLL subcode of $\mathcal{C}_m$ must be such that both conditions (C1) and (C2) are simultaneously satisfied. Therefore, to obtain an upper bound on the number of codewords $\mathrm{Eval}(f) \in \mathcal{C}_m$ that respect the $(1,\infty)$-RLL constraint, it is sufficient to obtain an upper bound on the number of $\mathrm{Eval}(f) \in \mathcal{C}_m$ that satisfy (C1) alone. In other words, we wish to obtain an upper bound on the number of pairs of polynomials (g,h) (see the Plotkin decomposition in (5.2)), with $\mathrm{Eval}(g) \in \mathcal{C}_{m,+}$ and $\mathrm{Eval}(h) \in \mathcal{C}_{m,-}$, such that $\mathrm{supp}(\mathrm{Eval}(g)) \subseteq \mathrm{supp}(\mathrm{Eval}(h))$.

The following two lemmas from the literature will be useful in the proof of Theorem 6.2.2.

Lemma 6.3.5 ([53], Lemma 36)**.** *Let $\mathcal{V} \subseteq \mathbb{F}_2^m$ be such that $|\mathcal{V}| \geq 2^{m-u}$, for some $u \in \mathbb{N}$. Then,*

$$rank(G_{m,r}[\mathcal{V}]) > \binom{m-u}{\leq r},$$

where $G_{m,r}$ is a generator matrix of $RM(m,r)$, and $G_{m,r}[\mathcal{V}]$ denotes the set of columns of $G_{m,r}$, indexed by $\mathcal{V}$.

The lemma below follows from Theorem 1 in [56], by noting that the Reed-Muller code is transitive:

Lemma 6.3.6. *Let the weight distribution of $RM(m,r)$ be $(A_{m,r}(w) : 0 \leq w \leq 2^m)$. Then,*

$$A_{m,r}(w) \leq exp_2\left(\binom{m}{\leq r} \cdot h_b\left(\frac{w}{2^m}\right)\right),$$

where $h_b(\cdot)$ is the binary entropy function.

We now provide the proof of Theorem 6.2.2.

Proof of Theorem 6.2.2. Fix the sequence $\{\mathcal{C}_m = \mathrm{RM}(m, r_m)\}_{m\geq 1}$ of RM codes, with $r_m = \max\left\{\left\lfloor \frac{m}{2} + \frac{\sqrt{m}}{2}Q^{-1}(1-R)\right\rfloor, 0\right\}$, as in the statement of the theorem. Now, for any codeword $\mathrm{Eval}(g) \in \mathcal{C}_{m,+}$ of weight w, we shall first calculate the number, $N_w(g)$, of codewords $\mathrm{Eval}(h) \in \mathcal{C}_{m,+}$ such that $\mathrm{supp}(\mathrm{Eval}(g)) \subseteq \mathrm{supp}(\mathrm{Eval}(h))$.

Suppose that for any weight w, the integer $u = u(w)$ is the smallest integer such that $\mathrm{wt}(\mathrm{Eval}(g)) = w \geq 2^{m-1-u}$. Note that for any polynomial g as above of weight w, the number of codewords in the code produced by shortening $\mathcal{C}_{m,+}$ at the indices in $\mathrm{supp}(\mathrm{Eval}(g))$, equals $N_w(g)$. Now, since $\dim(\mathcal{C}_{m,+}) = \binom{m-1}{\leq r_m}$, and from the fact that $w \geq 2^{m-1-u}$, we obtain by an application of Lemmas 5.6.5 and 6.3.5, that

$$\begin{aligned} N_w(g) &\leq \exp_2\left(\binom{m-1}{\leq r_m} - \binom{m-1-u}{\leq r_m}\right) \\ &=: M_{u(w)}. \end{aligned} \tag{6.6}$$

Let $\mathcal{H}_m^{(1)}$ denote the largest $(1,\infty)$-RLL subcode of $\mathcal{C}_m$, and let $\mathsf{R}_m^{(1)}(\mathcal{C})$ denote its rate. Then,

$$\begin{aligned}
\left|\mathcal{H}_m^{(1)}\right| &\leq \sum_{g:\mathrm{Eval}(g)\in\mathcal{C}_{m,+}} N_w(g) \\
&\overset{(a)}{\leq} \sum_{w=2^{m-1-r_m}}^{2^{m-1}} A_{m-1,r_m}(w) M_{u(w)} \\
&\overset{(b)}{\leq} \left\{ \sum_{w=2^{m-1-r_m}}^{2^{m-2}} A(w) M_{u(w)} \right\} + \frac{1}{2}\cdot \exp_2\left(\binom{m-1}{\leq r_m}\right)\cdot \exp_2\left(\binom{m-1}{\leq r_m} - \binom{m-2}{\leq r_m}\right) \\
&\overset{(c)}{\leq} \left\{ \sum_{w=2^{m-1-r_m}}^{2^{m-2}} A(w) M_{u(w)} \right\} + \frac{1}{2}\cdot \exp_2\left(\binom{m-1}{\leq r_m} + \binom{m-2}{\leq r_m}\right) \\
&\overset{(d)}{\leq} \left\{ \sum_{i=1}^{r_m-1} A\left(\left[2^{m-2-i} : 2^{m-1-i}\right]\right)\cdot \exp_2\left(\binom{m-1}{\leq r_m} - \binom{m-2-i}{\leq r_m}\right) \right\} + \\
&\qquad\qquad \frac{1}{2}\cdot \exp_2\left(\binom{m-1}{\leq r_m} + \binom{m-2}{\leq r_m}\right), \quad (6.7)
\end{aligned}$$

where, for ease of reading, we write $A(w) := A_{m-1,r_m}(w)$, in inequalities (b)–(d). Further, $A([a:b])$ is shorthand for $\sum_{w=a}^{b} A(w)$. Here,

(a) follows from (6.6), and

(b) holds due to the following fact: since the all-ones codeword $\mathbf{1}$ is present in $\mathcal{C}_{m,+} = \mathrm{RM}(m-1, r_m)$, it implies that $A(w) = A(2^{m-1} - w)$, i.e., that the weight distribution of $\mathcal{C}_{m,+}$ is symmetric about the weight $w = 2^{m-2}$. Therefore,

$$A\left(\left[2^{m-2}+1 : 2^{m-1}\right]\right) \leq \frac{1}{2}\cdot \exp_2\binom{m-1}{\leq r_m}. \quad (6.8)$$

Next,

(c) follows from the fact that for positive integers n, k with $n > k$:

$$\binom{n-1}{k} + \binom{n-1}{k-1} = \binom{n}{k}.$$

Picking $n = m-1$, we obtain that for $k \leq m-2$,

$$\binom{m-1}{k} - \binom{m-2}{k} = \binom{m-2}{k-1},$$

and hence that

$$\binom{m-1}{\leq r_m} - \binom{m-2}{\leq r_m} < \binom{m-2}{\leq r_m}, \text{ and}$$

(d) holds again by (6.6).

It is clear that a simplification of (6.7) depends crucially on good upper bounds on the weight distribution function. Recall the notation $R_{m,+} := \frac{\binom{m-1}{\leq r_m}}{2^{m-1}}$. We now use the result in Lemma 6.3.6, to get that for $1 \leq i \leq r_m - 1$,

$$\begin{aligned} A_{m-1,r_m}\left(\left[2^{m-2-i} : 2^{m-1-i}\right]\right) &\leq \sum_{w=2^{m-2-i}}^{2^{m-1-i}} \exp_2\left(2^{m-1} \cdot R_{m,+} \cdot h_b\left(\frac{w}{2^{m-1}}\right)\right) \\ &\overset{(e)}{\leq} \sum_{w=2^{m-2-i}}^{2^{m-1-i}} \exp_2\left(2^{m-1} \cdot R_{m,+} \cdot h_b(2^{-i})\right) \\ &= \exp_2\left(2^{m-1} \cdot R_{m,+} \cdot h_b(2^{-i}) + o(2^m)\right) := B_i(m), \quad (6.9) \end{aligned}$$

where inequality (e) above follows from the fact that the binary entropy function, $h_b(p)$, is increasing for arguments $p \in \left[0, \frac{1}{2}\right)$. Therefore, putting (6.9) back in (6.7), we get that

$$\begin{aligned} 2^m \mathsf{R}_m^{(1)}(\mathcal{C}) &= \log_2 \left|\mathcal{H}_m^{(1)}\right| \\ &\leq \binom{m-1}{\leq r_m} + \log_2 \left\{ \frac{1}{2} \cdot \exp_2 \binom{m-2}{\leq r_m} + \sum_{i=1}^{r_m - 1} B_i(m) \cdot \exp_2\left(-\binom{m-2-i}{\leq r_m}\right) \right\} \\ &= \binom{m-1}{\leq r_m} + \log_2\left(\alpha(m) + \beta(m)\right), \quad (6.10) \end{aligned}$$

where we define

$$\alpha(m) := \frac{1}{2} \cdot \exp_2 \binom{m-2}{\leq r_m}, \text{ and}$$
$$\beta(m) := \sum_{i=1}^{r_m - 1} B_i(m) \cdot \exp_2 \left(- \binom{m-2-i}{\leq r_m} \right). \tag{6.11}$$

In Lemma that appears after the end of this proof, we show that for all $\delta \in (0,1)$ sufficiently small and for m sufficiently large, we have

$$\begin{aligned} \beta(m) \ &\leq \ \exp_2 \left(2^{m-1} R \cdot \left(\frac{3}{4} + \delta \right) + o(2^m) \right) \\ &=: \ \theta(m). \end{aligned} \tag{6.12}$$

Now, using Lemma 5.6.2, we have

$$\lim_{m \to \infty} \frac{1}{2^m} \binom{m-2}{\leq r_m} = \frac{R}{4}.$$

Hence, for small $\delta \in (0,1)$, and for m large enough,

$$\binom{m-2}{\leq r_m} \leq (1+\delta) \cdot 2^{m-2} \cdot R.$$

Therefore, we get that

$$\alpha(m) \ \leq \ \exp_2 \left((1+\delta) \cdot 2^{m-2} \cdot R \right) \ =: \ \eta(m). \tag{6.13}$$

Now, substituting (6.12) and (6.13) in (6.10), we get that

$$2^m \mathsf{R}_m^{(1)}(\mathcal{C}) \leq \binom{m-1}{\leq r_m} + \log_2 \left(\eta(m) + \theta(m) \right). \tag{6.14}$$

Putting everything together, we see that

$$\begin{aligned}
\mathsf{R}^{(1)}(\mathcal{C}) &= \limsup_{m\to\infty} \mathsf{R}_m^{(1)}(\mathcal{C}) \\
&\leq \lim_{m\to\infty} \frac{1}{2^m}\left[\binom{m-1}{\leq r_m} + \log_2\left(\eta(m)+\theta(m)\right)\right] \\
&\overset{(p)}{\leq} \lim_{m\to\infty} \frac{1}{2^m}\left[\binom{m-1}{\leq r_m} + \log_2\left(2\cdot\theta(m)\right)\right] \\
&\overset{(q)}{=} \frac{R}{2} + \lim_{m\to\infty} \frac{1}{2^m}\cdot\log_2\theta(m) \\
&= \frac{R}{2} + \frac{3R}{8} + \frac{\delta R}{2} \\
&= \frac{7R}{8} + \frac{\delta R}{2}. \qquad (6.15)
\end{aligned}$$

Note that inequality (p) follows from the fact for any $R \in (0,1)$, $\eta(m) \leq \theta(m)$ holds for all sufficiently small $\delta > 0$. Further, equation (q) is valid because $\lim_{m\to\infty} \frac{1}{2^m}\binom{m-1}{\leq r_m} = \frac{R}{2}$, by Lemma 5.6.2. Since (6.15) holds for all $\delta > 0$ sufficiently small, we can let $\delta \to 0$, thereby obtaining that

$$\mathsf{R}^{(1)}(\mathcal{C}) \leq \frac{7R}{8}.$$

Moreover, since for any $m \geq 1$, we have that $\mathcal{H}_m^{(1)} \subseteq S_{(1,\infty)}^{(2^m)}$, with $\lim_{m\to\infty} \frac{\log_2\left|S_{(1,\infty)}^{(2^m)}\right|}{2^m} = \kappa_1$, the inequality $\mathsf{R}^{(1)}(\mathcal{C}) \leq \kappa_1$ holds. □

We now prove inequality (6.12), which is required to complete the proof of Theorem 6.2.2. Recall that we define

$$\begin{aligned}
\alpha(m) &:= \frac{1}{2}\cdot\exp_2\binom{m-2}{\leq r_m}, \text{ and} \\
\beta(m) &:= \sum_{i=1}^{r_m-1} B_i(m)\cdot\exp_2\left(-\binom{m-2-i}{\leq r_m}\right),
\end{aligned}$$

for all $m \geq 1$, where $r_m = \max\left\{\left\lfloor \frac{m}{2} + \frac{\sqrt{m}}{2}Q^{-1}(1-R)\right\rfloor, 0\right\}$.

Lemma 6.3.7. *We have that for m sufficiently large,*

$$\beta(m) \;\leq\; exp_2\left(2^{m-1}R\cdot\left(\frac{3}{4}+\delta\right)+o(2^m)\right).$$

Proof. We start with the expression

$$\beta(m) = 2^{o(2^m)}\cdot\sum_{i=1}^{r_m-1}\exp_2\left(2^{m-1}\cdot R_{m,+}\cdot h_b(2^{-i})-\binom{m-2-i}{\leq r_m}\right) \tag{6.16}$$

We will split the sum $\sum_{i=1}^{r_m-1}$ into two parts: $\sum_{i=1}^{t_m}$ and $\sum_{i=t_m+1}^{r_m-1}$, where $t_m := \lfloor m^{1/3}\rfloor$. For $i\in[t_m+1 : r_m-1]$, we have

$$2^{m-1}\cdot R_{m,+}\cdot h_b(2^{-i})-\binom{m-2-i}{\leq r_m} \;\leq\; 2^{m-1}\cdot R_{m,+}\cdot h_b(2^{-i}) \;=\; o(2^m),$$

since $h_b(2^{-i}) \leq h_b(2^{-t_m-1})$, and $h_b(2^{-t_m-1}) \xrightarrow{m\to\infty} 0$, by the continuity of entropy. Thus, the contribution of each term of the sum $\sum_{i=t_m+1}^{r_m-1}$ is $2^{o(2^m)}$, and since there are at most $r_m = O(m)$ terms in the sum, the total contribution from the sum is $2^{o(2^m)}$.

Turning our attention to $i\in[t_m]$, we note first that for m large enough, we have $R_{m,+}\leq R(1+\epsilon)$, for $\epsilon\in(0,1)$ suitably small. Also, we write

$$\begin{aligned}2^{m-1}\cdot R_{m,+}\cdot h_b(2^{-i})-\binom{m-2-i}{\leq r_m}&\\ \leq\; 2^{m-1}\cdot\left[R(1+\epsilon)\cdot h_b(2^{-i})-2^{-(i+1)}\cdot\frac{1}{2^{m-2-i}}\binom{m-2-i}{\leq r_m}\right].&\end{aligned} \tag{6.17}$$

By Lemma 5.6.2, we obtain that $\frac{1}{2^{m-2-i}}\binom{m-2-i}{\leq r_m}$ converges to R for all $i\in[t_m]$. In fact, with a bit more effort, we can show that this convergence is uniform in i. Indeed, since $i\leq t_m$, by virtue of (5.4), we have $|r_m - r_{m-2-i}| \leq \frac{t_m+2}{2}+\frac{\sqrt{t_m+2}}{2}|Q^{-1}(1-R)|+1 =: \nu_m$. Using the notation in the proof of Lemma 5.6.2, we have $\frac{1}{2^{m-2-i}}\binom{m-2-i}{\leq r_m} = \Pr[S_{m-2-i}\leq$

$r_m]$. Thus, analogous to (5.5), we have for all sufficiently large m,

$$\Pr[\overline{S}_{m-2-i} \leq Q^{-1}(1-R) - \frac{\nu_m}{\frac{1}{2}\sqrt{m-2-t_m}}] \leq \Pr[S_{m-2-i} \leq r_m] \leq \Pr[\overline{S}_{m-2-i} \leq Q^{-1}(1-R) + \frac{\nu_m}{\frac{1}{2}\sqrt{m-2-t_m}}].$$

Now, we apply the Berry-Esseen theorem (see e.g., [69, Theorem 3.4.17]) which, in this case, asserts that $\left|\Pr[\overline{S}_m \leq x] - \Pr[Z \leq x]\right| \leq 3/\sqrt{m}$, for all $x \in \mathbb{R}$ and positive integers m, where $Z \sim N(0,1)$. Thus, $\left|\Pr[\overline{S}_{m-2-i} \leq x] - \Pr[Z \leq x]\right| \leq \frac{3}{\sqrt{m-2-i}} \leq \frac{3}{\sqrt{m-2-t_m}}$ holds for all $x \in \mathbb{R}$ and $i \in [t_m]$. This yields

$$\begin{aligned}\Pr[Z \leq Q^{-1}(1-R) - \frac{\nu_m}{\frac{1}{2}\sqrt{m-2-t_m}}] - \frac{3}{\sqrt{m-2-t_m}} &\leq \Pr[S_{m-2-i} \leq r_m] \\ &\leq \Pr[Z \leq Q^{-1}(1-R) + \frac{\nu_m}{\frac{1}{2}\sqrt{m-2-t_m}}] + \frac{3}{\sqrt{m-2-t_m}}.\end{aligned}$$

Since t_m and ν_m are both $o(\sqrt{m})$, we deduce that, as $m \to \infty$, $\Pr[S_{m-2-i} \leq r_m] = \frac{1}{2^{m-2-i}}\binom{m-2-i}{\leq r_m}$ converges to R uniformly in $i \in [t_m]$.

Hence, for small $\epsilon \in (0,1)$ and m large enough, we have that for all $i \in [t_m]$ that

$$\frac{1}{2^{m-2-i}}\binom{m-2-i}{\leq r_m} \geq (1-\epsilon)R,$$

so that, carrying on from (6.17), we have that

$$R(1+\epsilon)\cdot h_b(2^{-i}) - 2^{-(i+1)}\cdot\frac{1}{2^{m-2-i}}\binom{m-2-i}{\leq r_m} \leq R\left[(1+\epsilon)\cdot h_b(2^{-i}) - 2^{-(i+1)}\cdot(1-\epsilon)\right]. \tag{6.18}$$

Now, we claim that for any $i \in \mathbb{N}$, the expression within square brackets above can be

bounded above as:

$$(1+\epsilon)\cdot h_b(2^{-i}) - 2^{-(i+1)}\cdot(1-\epsilon) \leq \frac{3}{4} + 2\epsilon, \tag{6.19}$$

Modulo the proof of this claim, we proceed to put all inequalities together. Recall that we split the sum $\sum_{i=1}^{r_m-1}$ in (6.16) into two parts: $\sum_{i=1}^{t_m}$ and $\sum_{i=t_m+1}^{r_m-1}$, where $t_m := \lfloor m^{1/3} \rfloor$. Given an arbitrarily small $\delta > 0$, setting $\epsilon = \delta/2$, we obtain via (6.17)–(6.19) that, for all sufficiently large m, the contribution from the sum $\sum_{i=1}^{t_m}$ is at most

$$m^{1/3}\cdot \exp_2\left(2^{m-1}R\cdot\left(\frac{3}{4}+\delta\right)\right).$$

We noted earlier that the contribution from the sum $\sum_{i=t_m+1}^{r_m-1}$ is $\exp_2(o(2^m))$. Therefore, the overall sum $\sum_{i=1}^{r_m-1}$ in (6.16) can be bounded above, for all sufficiently large m, by

$$2m^{1/3}\cdot \exp_2\left(2^{m-1}R\cdot\left(\frac{3}{4}+\delta\right)\right),$$

Consequently,

$$\beta(m) \;\leq\; \exp_2\left(2^{m-1}R\cdot\left(\frac{3}{4}+\delta\right) + o(2^m)\right) \;=:\; \theta(m).$$

To finish the proof of this lemma, we prove inequality (6.19).

Firstly, we note that the expression on the left of (6.19) obeys, for $i \geq 1$,

$$\begin{aligned}(1+\epsilon)\cdot h_b(2^{-i}) - 2^{-(i+1)}\cdot(1-\epsilon) &= h_b(2^{-i}) - 2^{-(i+1)} + \epsilon\left(h_b(2^{-i}) + 2^{-(i+1)}\right)\\ &\leq h_b(2^{-i}) - 2^{-(i+1)} + 2\epsilon. \end{aligned}\tag{6.20}$$

Now, consider the function $f(x) = h_b(2^{-x}) - 2^{-(x+1)}$, where $x \in [0,\infty)$. By taking the derivative with respect to x on both sides, we get

$$f'(x) = (2^{-x}\ln 2)\cdot\left[\frac{1}{2} - \log_2\left(\frac{1-2^{-x}}{2^{-x}}\right)\right].$$

The term within square brackets above is positive when $x \in \left(0, \log_2(1+\sqrt{2})\right)$, and is negative for $x \in \left(\log_2(1+\sqrt{2}), \infty\right)$. Importantly, this implies that f is decreasing in the interval $[2, \infty)$. Furthermore, we note that $f(1) = h_b(\frac{1}{2}) - \frac{1}{4} = \frac{3}{4}$, and $f(2) = h_b(\frac{1}{4}) - \frac{1}{8} \approx 0.68 < f(1)$. Hence, f is decreasing over integers $i \in \mathbb{N}$.

With this, we obtain that the right side of the inequality in (6.20) is at most $\frac{3}{4} + 2\epsilon$. □

6.3.3 Alternative Coordinate Orderings

Throughout the previous subsections, we have assumed that the coordinates of the RM codes are ordered according to the standard lexicographic ordering. In this subsection, we shall address the question of whether alternative coordinate orderings allow for larger rates of *linear* (d, ∞)-RLL constrained subcodes of RM codes of rate R, as compared to the upper bound of $\frac{R}{d+1}$ derived for RM codes under the lexicographic coordinate ordering, in Theorem 6.2.1.

First, we consider a Gray ordering of coordinates of the code $\mathrm{RM}(m, r)$. In such an ordering, consecutive coordinates $\mathbf{b} = (b_1, \ldots, b_m)$ and $\mathbf{b}' = (b'_1, \ldots, b'_m)$ are such that for some bit index $i \in [m]$, $b_i \neq b'_i$, but $b_j = b'_j$, for all $j \neq i$. In words, consecutive coordinates in a Gray ordering, when represented as m-tuples, differ in exactly one bit index. Note that there are multiple orderings that satisfy this property. Indeed, Gray orderings correspond to Hamiltonian paths (see, for example, [65], Chap. 10) on the m-dimensional unit hypercube.

In what follows, we work with a fixed sequence of Gray orderings defined as follows: let $(\pi_{\mathrm{G},m})_{m \geq 1}$ be a sequence of permutations, with $\pi_{\mathrm{G},m} : [0 : 2^m - 1] \to [0 : 2^m - 1]$, for any $m \geq 1$, having the property that $\mathbf{B}(\pi_{\mathrm{G},m}(j))$ differs from $\mathbf{B}(\pi_{\mathrm{G},m}(j-1))$ in exactly one bit index, for any $j \in [1 : 2^m - 1]$.

Now, as before, fix a sequence of codes $\left\{\hat{\mathcal{C}}_m = \mathrm{RM}(m, r_m)\right\}_{m \geq 1}$ of rate $R \in (0, 1)$. Note that for large enough m, we have that $r_m \leq m - 1$. We again use the notation

$K_m := \binom{m}{\leq r_m}$ to denote the dimension of $\hat{\mathcal{C}}_m$. We then define the sequence of Gray-ordered RM codes $\left\{\mathcal{C}_m^{\mathrm{G}}\right\}_{m\geq 1}$, via

$$\mathcal{C}_m^{\mathrm{G}} := \left\{(c_{\pi_{\mathrm{G},m}(0)}, c_{\pi_{\mathrm{G},m}(1)}, \ldots, c_{\pi_{\mathrm{G},m}(2^m-1)}) : (c_0, c_1, \ldots, c_{2^m-1}) \in \hat{\mathcal{C}}_m\right\}.$$

Clearly, the sequence of codes $\left\{\mathcal{C}_m^{\mathrm{G}}\right\}_{m\geq 1}$ is also of rate $R \in (0,1)$. In order to obtain an upper bound on the rate of the largest linear (d,∞)-RLL subcode of the code $\mathcal{C}_m^{\mathrm{G}}$, as in Theorem 6.2.1, we shall again work with the information set $\mathcal{I}_{m,r_m}$ (see (6.4) for the definition of the set $\mathcal{I}_{m,r}$ of coordinates of $\mathrm{RM}(m,r)$).

Analogous to (6.5), we define the set

$$\Gamma_m^{\mathrm{G}} := \{s \in [0 : 2^m - 1] : \ \mathbf{B}(\pi_{\mathrm{G},m}(s)) \in \mathcal{I}_{m,r_m}, \text{ but } \mathbf{B}(\pi_{\mathrm{G},m}(s+1)) \notin \mathcal{I}_{m,r_m}\}. \quad (6.21)$$

to be the collection of right end-points of runs of coordinates in the information set $\mathcal{I}_{m,r_m}$, where the coordinates are now ordered according to the fixed Gray ordering. We use the convention that when $s = 2^m - 1$, $\mathbf{B}(\pi_{\mathrm{G},m}(s+1))$ is defined to be a dummy symbol '$\times$' that does not belong to $\mathcal{I}_{m,r_m}$. The number of such runs is $\left|\Gamma_m^{\mathrm{G}}\right|$. Note now that unlike in (6.5), it is possible that $2^m - 1 \in \Gamma_m^{\mathrm{G}}$, since, depending on the specific Gray coordinate ordering chosen, it is possible that $\mathbf{B}(\pi_{\mathrm{G},m}(2^m-1)) \in \mathcal{I}_{m,r_m}$.

We now state and prove a lemma analogous to Lemma 6.3.4:

Lemma 6.3.8. *Under a fixed Gray ordering defined by π_m^G, the inequality $\left|\Gamma_{m,r_m}^{\mathrm{G}}\right| \leq \binom{m}{r_m+1} + 1$ holds, for $0 \leq r_m \leq m-1$.*

Proof. For any $s \in [0 : 2^m - 2]$ that belongs to Γ_m^{G}, we have $\mathrm{wt}(\mathbf{B}(\pi_{\mathrm{G},m}(s))) \leq r_m$, but $\mathrm{wt}(\mathbf{B}(\pi_{\mathrm{G},m}(s+1))) \geq r_m + 1$. In fact, since consecutive coordinates differ in exactly one bit index in the Gray ordering, it must be the case that $\mathrm{wt}(\mathbf{B}(\pi_{\mathrm{G},m}(s+1))) = r_m + 1$. Thus, the number of integers $s \in [0 : 2^m - 2]$ belonging to Γ_m^{G} is bounded above by $\binom{m}{r_m+1}$, which is the number of coordinates whose binary representation has weight exactly $r_m + 1$. In order to account for the possibility that $2^m - 1 \in \Gamma_m^{\mathrm{G}}$, we state the overall upper bound on the number of runs as $\binom{m}{r_m+1} + 1$. □

With Lemma 6.3.8 established, we now prove Theorem 6.2.3. Our proof strategy is similar to that for Theorem 6.2.1: for a given code $\mathcal{C}_m^{\mathrm{G}}$, we first calculate a lower bound on the number of $(d+1)$-tuples of consecutive coordinates, ordered according to the fixed Gray ordering, in the information set $\mathcal{I}_{m,r_m}$. Via Proposition 6.3.1, this gives us an upper bound on the rate of any linear (d,∞)-RLL subcode of $\mathcal{C}_m^{\mathrm{G}}$. We then let the blocklength go to infinity, to obtain our desired result.

Proof of Theorem 6.2.3. Similar to the proof of Theorem 6.2.1, the calculation of the overall number, t_m^{G}, of disjoint $(d+1)$-tuples of consecutive coordinates in $\mathcal{I}_{m,r_m}$, for large enough m, results in

$$t_m^{\mathrm{G}} \geq \frac{K_m}{d+1} - \binom{m}{r_m+1} - 1.$$

Note that here too, as in the proof of Theorem 6.2.1, we use the notation K_m to denote the dimension of $\mathcal{C}_m^{\mathrm{G}}$. Again, using Proposition 6.3.1, it follows that the dimension of any linear (d,∞)-RLL subcode $\overline{\mathcal{H}}_{\mathrm{G}}^{(d)} \subseteq \mathcal{C}_m^{\mathrm{G}}$ is at most $K_m - dt_m^{\mathrm{G}}$. Now, recalling the definition of $\overline{\mathsf{R}}^{(d)}(\mathcal{C}^{\mathrm{G}})$, from equation (6.2), we see that

$$\begin{aligned}
\overline{\mathsf{R}}^{(d)}(\mathcal{C}^{\mathrm{G}}) &\leq \limsup_{m\to\infty} \frac{K_m - dt_m^{\mathrm{G}}}{2^m} \\
&\leq \limsup_{m\to\infty} \frac{K_m - \frac{dK_m}{d+1} + d\cdot\binom{m}{r_m+1} + d}{2^m} \\
&\leq \lim_{m\to\infty} \frac{\frac{K_m}{d+1} + d\cdot\binom{m}{\lfloor \frac{m}{2} \rfloor} + d}{2^m} \\
&= \frac{R}{d+1},
\end{aligned}$$

where the last equality holds for reasons similar to those in the proof of Theorem 6.2.1. □

Next, we shift our attention to π-ordered RM codes $\{\mathcal{C}_m^{\pi}\}_{m\geq 1}$, defined by the sequence of arbitrary permutations $(\pi_m)_{m\geq 1}$, with $\pi_m : [0 : 2^m - 1] \to [0 : 2^m - 1]$ (see the discussion preceding Theorem 6.2.4 in Section 8.4). Note that the code $\mathcal{C}_m^{\pi}$ has the

same dimension K_m. as the code $\hat{\mathcal{C}}_m = \mathrm{RM}(m, r_m)$. Also recall the definition of $\overline{\mathcal{H}}_{\pi}^{(d)}$ being the largest *linear* (d, ∞)-RLL subcode of $\mathcal{C}_m^{\pi}$.

We shall now prove Theorem 6.2.4. The proof goes as follows: we first show that for large m, for almost all coordinate permutations π_m, the first block of $K_m(1+\alpha_m)$ coordinates in the π-ordered code $\mathcal{C}_m^{\pi}$ contains an information set $\mathcal{J}_{m,r_m}$, where $\alpha_m \to 0$ as $m \to \infty$. This then allows us to arrive at a lower bound on the number of disjoint $(d+1)$-tuples of consecutive coordinates in this information set $\mathcal{J}_{m,r_m}$. Again, using Proposition 6.3.1, we arrive at the desired upper bound on the rate of any (d, ∞)-RLL constrained linear subcode of $\mathcal{C}_m^{\pi}$, for almost all permutations π_m.

Proof of Theorem 6.2.4. We wish to prove that for "most" orderings, and for large m, the rate of $\overline{\mathcal{H}}_{\pi}^{(d)}$ is bounded above by $\frac{R}{d+1} + \epsilon_m$, where $\epsilon_m \xrightarrow{m\to\infty} 0$.

To this end, we first make the observation that the sequence of Reed-Muller codes $\left\{\hat{\mathcal{C}}_m = \mathrm{RM}(m, r_m)\right\}_{m\geq 1}$ achieves a rate R over the BEC, under block-MAP decoding too (see [36] and [66]). Hence, for large enough m, the (linear) RM code $\hat{\mathcal{C}}_m$ can correct erasures that are caused by a $\mathrm{BEC}(1-R-\gamma_m)$, with $\gamma_m > 0$, and $\gamma_m \xrightarrow{m\to\infty} 0$. This then means that for large m, $\hat{\mathcal{C}}_m$ can correct $2^m(1-R-\gamma_m) - c\cdot\sqrt{2^m(1-R-\gamma_m)}$ erasures, with high probability (see Lemma 15 of [53]), for $c > 0$ suitably small. Finally, from Corollary 18 of [53], it then holds that for large enough m, any collection of $2^m R(1+\beta_m)$ columns of $G_{\mathrm{Lex}}(m, r_m)$, chosen uniformly at random, must have full row rank, $K_m := \binom{m}{\leq r_m}$, with probability $1-\delta_m$, with $\beta_m, \delta_m > 0$ and $\beta_m, \delta_m \xrightarrow{m\to\infty} 0$.

In other words, the discussion above implies that for large enough m, a collection of $K_m(1+\alpha_m)$ coordinates, chosen uniformly at random, contains an information set, with probability $1-\delta_m$, where, again, $\alpha_m > 0$, with $\alpha_m \xrightarrow{m\to\infty} 0$. An equivalent view of the above statement is that for large enough m, for a $1-\delta_m$ fraction of the possible permutations $\pi_m : [0 : 2^m - 1] \to [0 : 2^m - 1]$, the first block of $K_m(1+\alpha_m)$ coordinates of the code $\mathcal{C}_m^{\pi}$, contains an information set, $\mathcal{J}_{m,r_m}$, with $\dim(\mathcal{C}_m^{\pi}) = K_m$. Now, within these "good" permutations, since $|\mathcal{J}_{m,r_m}| = K_m$, it follows that the number of runs, $|\Gamma_m^{\pi}|$, of consecutive coordinates that belong to $\mathcal{J}_{m,r_m}$, obeys $|\Gamma_m^{\pi}| \leq K_m\alpha_m + 1$, with Γ_m^{π} defined similar to equation (6.21). This is because the number of runs, $|\Gamma_m^{\pi}|$, equals the

number of coordinates s, such that $s \in \mathcal{J}_{m,r_m}$, but $s+1 \notin \mathcal{J}_{m,r_m}$. Hence, accounting for the possibility that the last coordinate in the $K_m(1+\alpha_m)$-block belongs to $\mathcal{J}_{m,r_m}$, we get that the number of such coordinates s is at most $K_m(1+\alpha_m)+1-K_m$, which equals $K_m\alpha_m+1$.

Hence, the overall number, t_m^π, of disjoint $(d+1)$-tuples of consecutive coordinates in $\mathcal{J}_{m,r}$, satisfies (see the proof of Theorem 6.2.1)

$$t_m^\pi \geq \frac{K_m}{d+1} - K_m\alpha_m - 1,$$

for a $1-\delta_m$ fraction of permutations π_m. Again, applying Proposition 6.3.1, we have that for a $1-\delta_m$ fraction of permutations, with $\delta_m \xrightarrow{m\to\infty} 0$, the rate of the largest (d,∞)-RLL subcode obeys, for m large,

$$\begin{aligned}\frac{\log_2\left|\overline{\mathcal{H}}_\pi^{(d)}\right|}{2^m} &\leq \frac{K_m - dt_m^\pi}{2^m} \\ &\leq \frac{K_m - \frac{dK_m}{d+1} + dK_m\alpha_m + d}{2^m} \\ &= \frac{R}{d+1} + \epsilon_m,\end{aligned}$$

where $\epsilon_m \xrightarrow{m\to\infty} 0$, with the last equality following from the fact that $\lim_{m\to\infty}\frac{K_m}{2^m} = R$. The theorem thus follows. □

6.4 Conclusions and Directions for Future Work

In this chapter, we derived upper bounds on the rates of (d,∞)-RLL constrained subcodes of Reed-Muller (RM) codes. We first fixed the coordinate ordering to be the lexicographic ordering and derived upper bounds on the rates of the largest *linear* (d,∞)-RLL subcodes of RM codes of rate R, thereby showing that the linear constrained subcodes explicitly constructed in Chapter 5 are essentially rate-optimal. Furthermore, a novel upper bound on the rate of general $(1,\infty)$-RLL subcodes was derived using

properties of the weight distribution of RM codes. We next considered other coordinate orderings and showed that for most orderings, almost the same upper bound on the rates of linear subcodes that was derived for the lexicographic ordering still holds, so long as the blocklength of the RM code is large enough.

There is certainly scope for future work along the lines explored in this chapter. Firstly, following the close relationship between the sizes of $(1, \infty)$-RLL subcodes and the weight distributions of RM codes established in this work, a more sophisticated analysis of *achievable rates* can be performed with the availability of better *lower bounds* on the weight distributions of RM codes. Likewise, sharper upper bounds on the weight distributions of RM codes will also lead to better upper bounds on the rate of any $(1, \infty)$-RLL subcodes of a certain canonical sequence of RM codes. It would also be of interest to derive good upper bounds on the rates of general (d, ∞)-RLL subcodes of RM codes, via weight distributions or otherwise.

Chapter 7

Counting Constrained Codewords in Binary Linear Codes

"When someone seeks," said Siddhartha, "then it easily happens that his eyes see only the thing that he seeks, and he is able to find nothing [...] Seeking means: having a goal. But finding means: being free, being open, having no goal."

Hermann Hesse, Siddhartha: An Indian Novel, 1922

7.1 Introduction

In the previous chapter, we considered the construction of explicit constrained codes, using subcodes of RM codes, over input-constrained binary-input DMCs. The key idea there was that if the unconstrained channel were symmetric, there exist *linear* codes such as RM codes, polar codes, and LDPC codes that achieve either the capacity or rates very close to the capacity of the channel (see [35,38,40]). In particular, this means that constrained subcodes of such linear codes also enjoy vanishing error probabilities over such binary-input memoryless symmetric (BMS) channels, in the limit as the blocklength goes to infinity.

Motivated by such considerations, in this chapter, we shall concern ourselves with the computation of the sizes of (arbitrarily) constrained subcodes of general linear

codes. Our approach makes use of a simple identity from the Fourier analysis of Boolean functions, namely, Plancherel's Theorem, which transforms our counting problem to one in the space of the dual code. An immediate advantage of this approach is that the dimension of the vector space over which we count, which is the minimum of the dimensions of the linear code and its dual, is always bounded above by half the blocklength of the code. Our study reveals the somewhat surprising fact that for many constraints, the Fourier transform of the indicator function of the constraint is computable, either analytically, or via efficient recursive procedures—an observation that can be of independent theoretical interest. We show, using specific examples of constraints, that our approach can yield not just the values of the sizes of constrained subcodes of specific linear codes, but also interesting insights into the construction of linear codes with a prescribed number of constrained codewords.

7.2 Some Approaches from Prior Art

It is possible, using random linear coding schemes, to show the existence of linear codes of rate $R \in (0, 1)$, the rates of whose constrained subcodes is at least $R + \kappa - 1$, in the limit as the blocklength goes to infinity, where κ is the noiseless capacity of the constraint (see Chapter 3 of [2]). Exactly the same existential lower bound was derived for the rates of constrained subcodes of cosets of linear codes of rate R in [47] (see also the early work of [96]). To the best of our knowledge, there do not exist works besides these that investigate the rates of generic constrained subcodes (or subcodes of cosets) of linear codes.

There however exists a lot of literature on the problem of determining the sizes of constant-weight subcodes of linear codes via the weight distribution of the code (see the book [58] for results on the weight distributions of several well-known linear codes), and on constant-composition subcodes of linear codes (see [97] and the references therein).

A closely-related line of investigation is on the largest rates of constrained linear

codes, and derivations of such rates in the context of specific runlength limited (RLL) constraints can be found in [61].

7.3 Preliminaries

7.3.1 Notation

For a given length n, we use the notation $W_i := \{\mathbf{x} \in \{0,1\}^n : w(\mathbf{x}) = i\}$.

7.3.2 Block Codes and Constrained Sequences

We recall, from Section 4.4.2 of Chapter 5, the definitions of block codes and linear codes over $\mathbb{F}_2$. Like in Chapter 5, our interest is in constraints over binary sequences [2], which are represented by sets $\mathcal{A} \subseteq \{0,1\}^n$ of binary words. We call the sequences in $\mathcal{A}$ as *constrained* sequences, and refer to a block code $\mathcal{C}$, all of whose codewords lie in $\mathcal{A}$, as a "constrained code". Note that we make no further assumption about the constrained system (such as it being finite-type, almost-finite-type, irreducible, etc.). Given such a collection of sets of constrained sequences $\{\mathcal{A}_n\}_{n\geq 1}$ for each blocklength $n \geq 1$, where $\mathcal{A}_n \subseteq \{0,1\}^n$, for all n, the noiseless capacity (see Chapter 3 of [2]) of the constraint is defined as

$$C_0 := \limsup_{n\to\infty} \frac{\log_2 |\mathcal{A}_n|}{n}.$$

Special cases, κ_d and $\kappa_{d,k}$, of the noiseless capacity, were considered in the previous chapters.

7.3.3 Fourier Expansions of Functions

Consider functions $f : \{0,1\}^n \to \mathbb{R}$, mapping $\mathbf{x} = (x_1, \ldots, x_n) \in \{0,1\}^n$ to $f(\mathbf{x}) \in \mathbb{R}$. If the range of f is $\{0,1\}$, then f is called a Boolean function. Now, given any function $f : \{0,1\}^n \to \mathbb{R}$ and a vector $\mathbf{s} = (s_1, \ldots, s_n) \in \{0,1\}^n$, we define the Fourier coefficient

of f at $\mathbf{s}$ as

$$\widehat{f}(\mathbf{s}) := \frac{1}{2^n} \sum_{\mathbf{x} \in \{0,1\}^n} f(\mathbf{x}) \cdot (-1)^{\mathbf{x} \cdot \mathbf{s}}.$$

The function $\widehat{f}$ is known as the Fourier transform (sometimes called the Hadamard transform) of f. Moreover, the functions $(\chi_{\mathbf{s}} : \mathbf{s} \in \{0,1\}^n)$, where $\chi_{\mathbf{s}}(\mathbf{x}) := (-1)^{\mathbf{x} \cdot \mathbf{s}}$, form a basis for the vector space V of functions $f : \{0,1\}^n \to \mathbb{R}$. If we define an inner product $\langle \cdot, \cdot \rangle$ over the vector space V, as follows:

$$\langle f, g \rangle := \frac{1}{2^n} \sum_{\mathbf{x} \in \{0,1\}^n} f(\mathbf{x}) g(\mathbf{x}),$$

for functions $f, g \in V$, we also have that the basis functions $(\chi_{\mathbf{s}} : \mathbf{s} \in \{0,1\}^n)$ are orthonormal, in that

$$\langle \chi_{\mathbf{s}}, \chi_{\mathbf{s}'} \rangle = \begin{cases} 1, \text{ if } \mathbf{s} = \mathbf{s}', \\ 0, \text{ otherwise.} \end{cases}$$

For more details on the Fourier analysis over $\mathbb{F}_2^n$, we refer the reader to [70]. In this chapter, we shall make use of Plancherel's Theorem from Fourier analysis, which is recalled below, without proof (see [70, Chapter 1, p. 26]).

Theorem 7.3.1 (Plancherel's Theorem)**.** *For any $f, g \in \{0,1\}^n \to \mathbb{R}$, we have that*

$$\langle f, g \rangle = \sum_{\mathbf{s} \in \{0,1\}^n} \widehat{f}(\mathbf{s}) \widehat{g}(\mathbf{s}).$$

7.4 Main Theorem

Consider an $[n, k]$ linear code $\mathcal{C}$. Suppose that we are interested in computing the number of codewords $\mathbf{c} \in \mathcal{C}$, each of which satisfies a certain property, which we call a constraint. Let $\mathcal{A} \subseteq \{0,1\}^n$ denote the set of length-n words that respect the constraint. We let $N(\mathcal{C}; \mathcal{A})$ denote the number of such constrained codewords in $\mathcal{C}$. We

can then write

$$N(\mathcal{C};\mathcal{A}) = \sum_{\mathbf{c}\in\mathcal{C}} \mathbb{1}_{\mathcal{A}}(\mathbf{c}). \tag{7.1}$$

Observe that the summation in (7.1) is over a set of size 2^k, which could be quite large, especially when $k > n/2$. Our interest is in obtaining insight into the summation above, by employing a simple trick from the Fourier expansions of Boolean functions. For a linear code $\mathcal{C}$, we denote its dual code by $\mathcal{C}^{\perp}$.

Theorem 7.4.1. *Given a linear code $\mathcal{C}$ of blocklength n and a set $\mathcal{A} \subseteq \{0,1\}^n$, we have that*

$$N(\mathcal{C};\mathcal{A}) = |\mathcal{C}| \cdot \sum_{\mathbf{s}\in\mathcal{C}^{\perp}} \widehat{\mathbb{1}_{\mathcal{A}}}(\mathbf{s}).$$

Proof. The proof is a straightforward application of Plancherel's Theorem. Observe that

$$N(\mathcal{C};\mathcal{A}) = \sum_{\mathbf{x}\in\{0,1\}^n} \mathbb{1}_{\mathcal{A}}(\mathbf{x}) \cdot \mathbb{1}_{\mathcal{C}}(\mathbf{x}) = 2^n \cdot \sum_{\mathbf{s}\in\{0,1\}^n} \widehat{\mathbb{1}_{\mathcal{A}}}(\mathbf{s}) \cdot \widehat{\mathbb{1}_{\mathcal{C}}}(\mathbf{s}). \tag{7.2}$$

Now, via arguments similar to Lemma 2 in Chapter 5, p. 127, of [58], we have that

$$\widehat{\mathbb{1}_{\mathcal{C}}}(\mathbf{s}) = \begin{cases} \frac{|\mathcal{C}|}{2^n}, \text{ if } \mathbf{s} \in \mathcal{C}^{\perp}, \\ 0, \text{ otherwise.} \end{cases} \tag{7.3}$$

Plugging (7.3) back in (7.2), we obtain the statement of the theorem. □

Theorem 7.4.1 provides an alternative approach to addressing our problem of counting constrained codewords in linear codes. In particular, note that if $\mathcal{C}$ had large dimension, i.e., if $k > n/2$, then, it is computationally less intensive to calculate the number of constrained codewords using Theorem 7.4.1, provided we knew the Fourier coefficients $\widehat{\mathbb{1}_{\mathcal{A}}}(\mathbf{s})$, since $\dim\left(\mathcal{C}^{\perp}\right) = n - k < n/2$, in this case. Additionally, if the structure of the Fourier coefficients is simple to handle, we could also use Theorem 7.4.1 to construct linear codes that have a large (or small) number of constrained codewords, or to

obtain estimates of the number of constrained codewords in a fixed linear code.

Below, we discuss the connection between Theorem 7.4.1 and the well-known MacWilliams' identities for linear codes [71]. This material is well-known, and we provide it for completeness.

Consider the simple constraint that admits only sequences having a fixed weight $i \in [0 : n]$, where n is the blocklength of the code. Note that in this case, the set of constrained sequences is $\mathcal{A} = W_i$. By applying Theorem 7.4.1 to this constraint, for a given linear code $\mathcal{C}$, we obtain the well-known MacWilliams' identities [71] for linear codes. We use the notation $a_i(\mathcal{C})$ for the number of codewords of weight $i \in [0 : n]$ in $\mathcal{C}$, which equals $N(\mathcal{C}; W_i)$, following the notation of Theorem 7.4.1.

Theorem 7.4.2 (MacWilliams' identities)**.** *The equality*

$$a_i(\mathcal{C}) = \frac{1}{\left|\mathcal{C}^{\perp}\right|} \sum_{j=0}^{n} K_i^{(n)}(j) \cdot a_j(\mathcal{C}^{\perp}).$$

holds. Here, $K_i^{(n)}(j) = \sum_{t=0}^{i} (-1)^t \binom{j}{t} \binom{n-j}{i-t}$ *is the* i^{th}*-Krawtchouk polynomial, for the length* n*.*

Proof. The proof simply uses the fact that $\widehat{\mathbb{1}_{W_i}}(\mathbf{s}) = \frac{K_i^{(n)}(w(\mathbf{s}))}{2^n}$. By simplifying the summation in Theorem 7.4.1, and by using the fact that $|\mathcal{C}| \cdot \left|\mathcal{C}^{\perp}\right| = 2^n$, we obtain the required result. □

In the rest of this chapter, we shall look at specific examples of constraints and apply the above theorem. In particular, we shall consider the $[2^m - 1, 2^m - 1 - m]$ binary Hamming code, for $m \geq 1$ and the binary Reed-Muller codes. Since the constraints we work with are sensitive to the ordering of coordinates of the code, in the sense that a permutation of the coordinates can transform a codeword that does not satisfy the constraint into one that does, we shall first fix a canonical ordering of coordinates for the codes that we analyze. For the binary Hamming code, we assume that a parity-check matrix H_{Ham} is such that $H_{\text{Ham}}[i] = \mathbf{B}_m(i)$, for $1 \leq i \leq 2^m - 1$.

Recall, from Chapter 5, that the Reed-Muller (RM) family of codes is known to achieve the capacities of BMS channels under bit-MAP decoding [40] (see also [36]).

Thus, RM codes are linear codes that offer the maximum resilience to symmetric, stochastic noise, for a given rate. We refer the reader to 5.4.3 for more details on this family of codes. In this chapter, we use the convention that the coordinates of RM(m, r) are written as binary m-tuples that are ordered according to the standard lexicographic ordering, i.e., the i^{th} coordinate from the start is the m-tuple $\mathbf{B}_m(i-1)$, for $1 \leq i \leq 2^m$.

7.5 Applications: Explicitly Computable Fourier Coefficients

In this section, we shall work with select constraints for which the Fourier coefficients of the indicator function that a word satisfies the constraint, are explicitly (or, analytically) computable.

7.5.1 2-Charge Constraint

We first consider a special kind of a spectral null constraint [72], [73]. This constraint that we shall work with is the so-called 2-charge constraint (see Section 1.5.4 in [2]), whose sequences have a spectral null at zero frequency. The 2-charge constraint admits only sequences $\mathbf{y} \in \{-1, +1\}^n$, whose running sum $\sum_{i=1}^{r} y_i$, for any $1 \leq r \leq n$, obeys $0 \leq \sum_{i=1}^{r} y_i \leq 2$. To any sequence $\mathbf{x} \in \{0,1\}^n$, we associate (in a one-one manner) the sequence $\mathbf{y} = ((-1)^{x_1}, \ldots, (-1)^{x_n}) \in \{-1, +1\}^n$. We let S_2 denote the set of sequences $\mathbf{x} \in \{0,1\}^n$ such that $\mathbf{y} = ((-1)^{x_1}, \ldots, (-1)^{x_n})$ is 2-charge constrained. Thus, the set of constrained sequences of interest to us is $\mathcal{A} = S_2$. Figure 7.1 shows a state transition graph for sequences in the set S_2, in that the binary sequences that lie in S_2 can be read off the labels of edges in the graph:

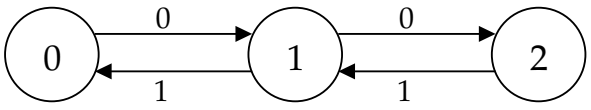


Figure 7.1: State transition graph for sequences in the set S_2.

We assume that the initial state is $v_0 = 0$. Since labels of paths in the state transition graph (beginning at state 0) correspond to binary sequences $\mathbf{x} \in S_2$, we denote by x_i the label of the i^{th} edge in the path. Observe that $x_1 = 0$, by our choice of initial state. Further, for a given path in the graph, we let v_i denote the i^{th} state, which is the terminal state of the i^{th} edge.

Further, we claim that $|S_2| = 2^{\lfloor \frac{n}{2} \rfloor}$. To see this, observe that for any $\mathbf{x} \in S_2$, the state v_{2i-1}, for any $1 \leq i \leq n$, equals 1. Owing to this fact, the label of the j^{th} edge, x_j, in any path in the graph G in Figure 9.1, can be either 0 or 1, when $j = 2i$, and is fixed to be exactly one of 0 or 1, when $j = 2i + 1$, based on the label of the $(j-1)^{\text{th}}$ edge, for $1 \leq j \leq n$. In particular, it holds that $x_{2i} + x_{2i+1} = 1$, for all $1 \leq i \leq \left\lfloor \frac{n-1}{2} \right\rfloor$, with x_1 fixed to be 0.

We now state a lemma that completely determines the Fourier transform of $\mathbb{1}_{S_2}$. We define the set of vectors $\mathcal{B} = \left\{ \mathbf{b}_0, \mathbf{b}_1, \ldots, \mathbf{b}_{\lceil \frac{n}{2} \rceil - 1} \right\}$, where $\mathbf{b}_0 = 10^{n-1}$ and for $1 \leq i \leq \lceil \frac{n}{2} \rceil - 1$, the vector $\mathbf{b}_i$ is such that $b_{i,j} = 1$, for $j \in \{2i, 2i+1\}$, and $b_{i,j} = 0$, otherwise. For example, when $n = 5$, we have that $\mathcal{B} = \{10000, 01100, 00011\}$. Let $V_{\mathcal{B}} = \text{span}(\mathcal{B})$. In what follows, we assume that $n \geq 3$.

Lemma 7.5.1. *For $n \geq 3$ and for $\mathbf{a} = \left(a_0, a_1, \ldots, a_{\lceil \frac{n}{2} \rceil - 1} \right) \in \{0,1\}^{\lceil \frac{n}{2} \rceil}$, consider $\mathbf{s} = \sum_{i=0}^{\lceil \frac{n}{2} \rceil - 1} a_i \cdot \mathbf{b}_i$ (where the summation is over $\mathbb{F}_2^n$). It holds that*

$$\widehat{\mathbb{1}_{S_2}}(\mathbf{s}) = 2^{\lfloor \frac{n}{2} \rfloor - n} \cdot (-1)^{w(\mathbf{a}) - a_0}.$$

Further, for $\mathbf{s} \notin V_{\mathcal{B}}$, we have that $\widehat{\mathbb{1}_{S_2}}(\mathbf{s}) = 0$.

Proof. First, we note that for any $\mathbf{s} \in \{0,1\}^n$,

$$\begin{aligned} \widehat{\mathbb{1}_{S_2}}(\mathbf{s}) &= \frac{1}{2^n} \sum_{\mathbf{x} \in \{0,1\}^n} \mathbb{1}_{S_2}(\mathbf{x}) \cdot (-1)^{\mathbf{x} \cdot \mathbf{s}} \\ &= 2^{-n} \cdot \left(\#\{\mathbf{x} \in S_2 : \ w_{\mathbf{s}}(\mathbf{x}) \text{ is even}\} - \#\{\mathbf{x} \in S_2 : \ w_{\mathbf{s}}(\mathbf{x}) \text{ is odd}\} \right). \end{aligned} \tag{7.4}$$

Now, for $\mathbf{s} = \mathbf{b}_0$, note that since all words $\mathbf{x} \in S_2$ have $x_1 = 0$, we obtain that $\widehat{\mathbb{1}_{S_2}}(\mathbf{b}_0) =$

$2^{-n} \cdot |S_2| = 2^{\lfloor \frac{n}{2} \rfloor - n}$.

Further, recall that since $v_{2i-1} = 1$, for any $1 \leq i \leq n$, we have that $x_{2i} + x_{2i+1} = 1$ (over $\mathbb{F}_2$). Hence, we see that for $\mathbf{s} = \mathbf{b}_j$, for $1 \leq j \leq \lceil \frac{n}{2} \rceil - 1$, it is true that $\#\{\mathbf{x} \in S_2 : w_{\mathbf{s}}(\mathbf{x}) \text{ is odd}\} = |S_2| = 2^{\lfloor \frac{n}{2} \rfloor}$ and $\#\{\mathbf{x} \in S_2 : w_{\mathbf{s}}(\mathbf{x}) \text{ is even}\} = 0$. Substituting in (7.4), we get that $\widehat{\mathbb{1}_{S_2}}(\mathbf{b}_j) = -2^{\lfloor \frac{n}{2} \rfloor - n}$ for all $1 \leq j \leq \lceil \frac{n}{2} \rceil - 1$. Furthermore, we claim that $\widehat{\mathbb{1}_{S_2}}(0^n) = 2^{\lfloor \frac{n}{2} \rfloor - n}$. To see this, note that

$$\widehat{\mathbb{1}_{S_2}}(0^n) = \frac{1}{2^n} \sum_{\mathbf{x} \in S_2} 1 = \frac{|S_2|}{2^n} = 2^{\lfloor \frac{n}{2} \rfloor - n}.$$

Now, suppose that for some $\mathbf{s}_1, \mathbf{s}_2 \in V_{\mathcal{B}}$, we have $\widehat{\mathbb{1}_{S_2}}(\mathbf{s}_1) = (-1)^{i_1} \cdot 2^{\lfloor \frac{n}{2} \rfloor - n}$ and $\widehat{\mathbb{1}_{S_2}}(\mathbf{s}_2) = (-1)^{i_2} \cdot 2^{\lfloor \frac{n}{2} \rfloor - n}$, for some $i_1, i_2 \in \{0, 1\}$, with $w_{\mathbf{s}_1}(\mathbf{x})$ being even for all $\mathbf{x} \in S_2$, if $i_1 = 0$, and odd otherwise (similar arguments hold for $w_{\mathbf{s}_2}(\mathbf{x})$). Hence, it can be checked that if $i_1 = i_2$, it holds that $w_{\mathbf{s}_1 + \mathbf{s}_2}(\mathbf{x})$ is even, and hence, $\widehat{\mathbb{1}_{S_2}}(\mathbf{s}_1 + \mathbf{s}_2) = 2^{\lfloor \frac{n}{2} \rfloor - n} = (-1)^{i_1 + i_2} \cdot 2^{\lfloor \frac{n}{2} \rfloor - n}$, and similarly if $i_1 \neq i_2$ as well. By applying this fact iteratively, and using the expressions for the Fourier coefficients $\widehat{\mathbb{1}_{S_2}}(\mathbf{b}_j)$, for $0 \leq j \leq \lceil \frac{n}{2} \rceil - 1$, we obtain the first part of the lemma.

To show that $\widehat{\mathbb{1}_{S_2}}(\mathbf{s}) = 0$ for $\mathbf{s} \notin V_{\mathcal{B}}$, we use Plancherel's Theorem again. Note that

$$\begin{aligned}
\frac{|S_2|}{2^n} &= \frac{1}{2^n} \sum_{\mathbf{x} \in \{0,1\}^n} \mathbb{1}_{S_2}(\mathbf{x}) \\
&\overset{(a)}{=} \frac{1}{2^n} \sum_{\mathbf{x} \in \{0,1\}^n} \mathbb{1}_{S_2}^2(\mathbf{x}) \\
&\overset{(b)}{=} \sum_{\mathbf{s} \in \{0,1\}^n} \left(\widehat{\mathbb{1}_{S_2}}(\mathbf{s}) \right)^2 = \sum_{\mathbf{s} \in V_{\mathcal{B}}} \left(\widehat{\mathbb{1}_{S_2}}(\mathbf{s}) \right)^2 + \sum_{\mathbf{s} \notin V_{\mathcal{B}}} \left(\widehat{\mathbb{1}_{S_2}}(\mathbf{s}) \right)^2, \qquad (7.5)
\end{aligned}$$

where (a) holds since $\mathbb{1}_{S_2}$ is a Boolean function, and (b) holds by Plancherel's Theorem. However, from the first part of the lemma, we get that

$$\begin{aligned}
\sum_{\mathbf{s} \in V_{\mathcal{B}}} \left(\widehat{\mathbb{1}_{S_2}}(\mathbf{s}) \right)^2 &= |V_{\mathcal{B}}| \cdot 2^{2 \cdot \left(\lfloor \frac{n}{2} \rfloor - n \right)} \\
&\overset{(c)}{=} 2^{\lceil \frac{n}{2} \rceil} \cdot 2^{2 \cdot \left(\lfloor \frac{n}{2} \rfloor - n \right)} = 2^{-\lceil \frac{n}{2} \rceil} = \frac{|S_2|}{2^n},
\end{aligned}$$

where equality (c) follows from the fact that $|V_{\mathcal{B}}| = 2^{\lceil \frac{n}{2} \rceil}$, since $V_{\mathcal{B}} = \text{span}(\mathcal{B})$ and the vectors in $\mathcal{B}$ are linearly independent. Hence, plugging back in (7.5), we obtain that $\sum_{\mathbf{s} \notin V_{\mathcal{B}}} \left(\widehat{\mathbb{1}_{S_2}}(\mathbf{s}) \right)^2 = 0$, implying that $\widehat{\mathbb{1}_{S_2}}(\mathbf{s}) = 0$, for all $\mathbf{s} \notin V_{\mathcal{B}}$. □

Lemma 7.5.1 informs the construction of linear codes $\mathcal{C}$ that have a large number of codewords $\mathbf{c} \in S_2$. In particular, note that from Theorem 7.4.1, we have that

$$\begin{aligned} N(\mathcal{C}; S_2) &= |\mathcal{C}| \cdot \sum_{\mathbf{s} \in \mathcal{C}^\perp} \widehat{\mathbb{1}_{S_2}}(\mathbf{s}) \\ &= |\mathcal{C}| \cdot \sum_{\mathbf{s} \in \mathcal{C}^\perp \cap V_{\mathcal{B}}} \widehat{\mathbb{1}_{S_2}}(\mathbf{s}), \end{aligned} \tag{7.6}$$

where, for $\mathbf{s} \in \mathcal{C}^\perp \cap V_{\mathcal{B}}$, with $\mathbf{s} = \sum_{i=0}^{\lceil \frac{n}{2} \rceil - 1} a_i \cdot \mathbf{b}_i$, for some $\mathbf{a} = \left(a_0, a_1, \ldots, a_{\lceil \frac{n}{2} \rceil - 1} \right) \in \{0,1\}^{\lceil \frac{n}{2} \rceil}$, we have that $\widehat{\mathbb{1}_{S_2}}(\mathbf{s}) = 2^{\lfloor \frac{n}{2} \rfloor - n} \cdot \left((-1)^{\sum_{j=1}^{\lceil \frac{n}{2} \rceil - 1} a_j} \right)$. Now, suppose that $n \geq 3$ and $\mathcal{C}$ is such that $\mathcal{C}^\perp$ *does not* satisfy the criterion (**C**) below:

(**C**) For all $\mathbf{s} \in \mathcal{C}^\perp \cap V_{\mathcal{B}}$, it holds that $\widehat{\mathbb{1}_{S_2}}(\mathbf{s}) \geq 0$.

If (**C**) does not hold, then, it implies that for some $\mathbf{s}^\star \in \mathcal{C}^\perp \cap V_{\mathcal{B}}$, it holds that $\widehat{\mathbb{1}_{S_2}}(\mathbf{s}^\star) < 0$. Hence, following the reasoning in the proof of Lemma 7.5.1, since $\mathcal{C}^\perp \cap V_{\mathcal{B}}$ is a vector space, we have that via the map $\mathbf{s} \mapsto \mathbf{s} + \mathbf{s}^\star$, the number of elements $\mathbf{s} \in \mathcal{C}^\perp \cap V_{\mathcal{B}}$ such that $\widehat{\mathbb{1}_{S_2}}(\mathbf{s}) < 0$ equals the number of elements $\mathbf{s} \in \mathcal{C}^\perp \cap V_{\mathcal{B}}$ such that $\widehat{\mathbb{1}_{S_2}}(\mathbf{s}) > 0$. Furthermore, since $\left| \widehat{\mathbb{1}_{S_2}}(\mathbf{s}) \right| = 2^{\lfloor \frac{n}{2} \rfloor - n}$, for all $\mathbf{s} \in \mathcal{C}^\perp \cap V_{\mathcal{B}}$, we get from (7.6) that $N(\mathcal{C}; S_2) = 0$, in this case.

Hence, in order to construct linear codes $\mathcal{C}$ such that $N(\mathcal{C}, S_2) > 0$, we require that criterion (**C**) is indeed satisfied by the dual code $\mathcal{C}^\perp$ of $\mathcal{C}$, with $\widehat{\mathbb{1}_{S_2}}(\mathbf{s}^\star) > 0$, for some $\mathbf{s}^\star \in \mathcal{C}^\perp$. With this instruction in mind, we can construct linear codes $\mathcal{C}$ such that its dual code $\mathcal{C}^\perp$ contains t linearly independent vectors $(\mathbf{s}_1, \ldots, \mathbf{s}_t)$ with $\widehat{\mathbb{1}_{S_2}}(\mathbf{s}_i) > 0$, for all $1 \leq i \leq t$, and no vectors $\mathbf{s} \in V_{\mathcal{B}}$ with $\widehat{\mathbb{1}_{S_2}}(\mathbf{s}) < 0$. In such a case, we obtain that $N(\mathcal{C}; S_2) = |\mathcal{C}| \cdot 2^{t + \lfloor \frac{n}{2} \rfloor - n}$. From the structure of $V_{\mathcal{B}}$, we see that the largest number of vectors $\mathbf{s} \in \{0,1\}^n$ such that $\widehat{\mathbb{1}_{S_2}}(\mathbf{s}) > 0$, equals $\frac{|V_{\mathcal{B}}|}{2} = 2^{\lceil \frac{n}{2} \rceil - 1}$. Hence, the largest

number of linearly independent vectors t as above, is $\lceil \frac{n}{2} \rceil - 1$. The discussion above is summarized below as a lemma.

Lemma 7.5.2. *For any linear code $\mathcal{C}$ of blocklength $n \geq 3$, the following are true:*

1. *If criterion (**C**) is not satisfied, then, $N(\mathcal{C}, S_2) = 0$.*
2. *If criterion (**C**) is satisfied and there exist $t_n \in \left[1 : \lceil \frac{n}{2} \rceil - 1\right]$ linearly independent vectors $(\mathbf{s}_1, \ldots, \mathbf{s}_{t_n})$ in $\mathcal{C}^\perp$ with $\widehat{\mathbb{1}_{S_2}}(\mathbf{s}_i) > 0$, for all $1 \leq i \leq t_n$, then, $N(\mathcal{C}; S_2) = |\mathcal{C}| \cdot 2^{t_n + \lfloor \frac{n}{2} \rfloor - n}$.*

We thus understand that given a linear code whose dual code satisfies item 2 of Lemma 7.5.2, the rate of the largest constrained subcode, $\mathcal{C}_2$, of $\mathcal{C}$, all of whose codewords are in S_2, obeys

$$\text{rate}\,(\mathcal{C}_2) = \frac{\log_2 N(\mathcal{C}; S_2)}{n} = \frac{\log_2 (|\mathcal{C}|)}{n} + \frac{t_n + \lfloor \frac{n}{2} \rfloor - n}{n}.$$

In particular, given a sequence of linear codes $\left\{\mathcal{C}^{(n)}\right\}_{n \geq 1}$ satisfying item 2 of Lemma 7.5.2, if it holds that $\text{rate}(\mathcal{C}^{(n)}) \xrightarrow{n \to \infty} R \in (0, 1)$, then, the rate of their largest constrained subcodes $\left\{\mathcal{C}_2^{(n)}\right\}_{n \geq 1}$, all of whose codewords are in S_2, obeys

$$\liminf_{n \to \infty} \text{rate}\left(\mathcal{C}_2^{(n)}\right) = R - \frac{1}{2} + \liminf_{n \to \infty} \frac{t_n}{n}. \tag{7.7}$$

By arguments similar to those in [47], we obtain that for the constraint identified by the set S_2, there exist cosets of the linear codes $\left\{\mathcal{C}^{(n)}\right\}_{n \geq 1}$ with $\text{rate}(\mathcal{C}^{(n)}) \xrightarrow{n \to \infty} R$, the rate of the constrained subcodes of which (in the limit as the blocklength goes to infinity) is at least $R - \frac{1}{2}$. From (7.7), since $t_n \in \left[1 : \lceil \frac{n}{2} \rceil - 1\right]$, we see that we can construct a sequence of linear codes whose 2-charge constrained subcodes are of rate larger than or equal to the coset-averaging lower bound in [47]. In other words, it is possible to achieve the coset-averaging rate lower bound for the 2-charge constraint (and potentially more) by using the linear code itself, instead of one of its cosets.

Specifically, suppose that we choose $t_n = \lceil \frac{n}{2} \rceil - p_n$, for some positive integer p_n such that $\lim_{n \to \infty} \frac{p_n}{n} = 0$, thereby making $\dim(\mathcal{C}_n^\perp) \geq \frac{\lceil \frac{n}{2} \rceil - p_n}{n}$, where $\mathcal{C}_n^\perp$ is the dual

code of $\mathcal{C}_n$. Note that this implies that $1 - R = \lim_{n\to\infty} \text{rate}\left(\mathcal{C}^{\perp}\right) \geq \frac{1}{2}$, and hence that $R \in (0, \frac{1}{2}]$. In this case, by plugging into (7.7), we obtain that the rate of the largest constrained subcodes $\left\{\mathcal{C}_2^{(n)}\right\}_{n\geq 1}$ of $\left\{\mathcal{C}^{(n)}\right\}_{n\geq 1}$ is

$$\lim_{n\to\infty} \text{rate}\left(\mathcal{C}_2^{(n)}\right) = R - \frac{1}{2} + \lim_{n\to\infty} \frac{t_n}{n} = R.$$

In other words, in the case where $t_n = \left\lceil \frac{n}{2} \right\rceil - p_n$, for $p_n > 0$ as above, the asymptotic rate of the codewords that lie in S_2 equals the asymptotic rate $R \in (0, \frac{1}{2}]$ of the code itself.

Next, we shall make use of Theorem 7.4.1 to compute the number of codewords of specific linear codes $\mathcal{C}$, which lie in S_2. First, we shall apply our results to the $[2^m - 1, 2^m - 1 - m]$ binary Hamming code, for $m \geq 3$. We shall use the coordinate ordering discussed in Section 7.4.

Corollary 7.5.3. *For $m \geq 3$ and for $\mathcal{C}$ being the $[2^m - 1, 2^m - 1 - m]$ Hamming code, we have that $N(\mathcal{C}; S_2) = 2^{\left\lfloor \frac{2^m-1}{2} \right\rfloor - 1}$.*

Proof. The dual code $\mathcal{C}^{\perp}$ of the $[2^m - 1, 2^m - 1 - m]$ Hamming code is the $[2^m - 1, m]$ simplex code, all of whose non-zero codewords (i.e., codewords that are not equal to 0^{2^m-1}) are of weight 2^{m-1}. Further, a generator matrix of the simplex code under consideration is H_{Ham}. Now, let the columns of H_{Ham} be indexed by m-tuples $(x_1, \ldots, x_m) \in \{0,1\}^m \setminus \{0^m\}$, ordered in the standard lexicographic order, i.e., the i^{th} column of G is indexed as $\mathbf{B}_m(i)$, for $1 \leq i \leq 2^m - 1$. It is well-known (see, for example, Section 1.10 of [64]) that the j^{th} row $H_{\text{Ham}}(j)$ is the evaluation vector, over the m-tuples indexing the columns, of the monomial x_j, for $1 \leq j \leq m$. We write this row as $\text{Eval}^{\setminus \mathbf{0}}(x_j)$.

Consider the first $m - 1$ rows of H_{Ham}, which are the evaluation vectors $\text{Eval}^{\setminus \mathbf{0}}(x_j)$, for $1 \leq j \leq m - 1$. It can be checked that the Hamming weight, 2^{m-1}, of any of these rows is a multiple of 4, when $m \geq 3$. Moreover, in any of these rows, if the entry corresponding to the evaluation point $(x_1, \ldots, x_{m-1}, 0)$ equals 1, then so does the entry corresponding to the evaluation point $(x_1, \ldots, x_{m-1}, 1)$. The above two facts imply that

each of the first $m-1$ rows of H_{Ham} can be written as a linear combination of an *even* number of vectors $\mathbf{b}_\ell \in \mathcal{B}$, for $\ell \in [1 : \left\lceil \frac{2^m-1}{2} \right\rceil - 1]$. Hence, from Lemma 7.5.1, it holds that the Fourier coefficient $\widehat{\mathbb{1}_{S_2}}\left(\text{Eval}^{\setminus \mathbf{0}}(x_j)\right) = 2^{\left\lfloor \frac{2^m-1}{2} \right\rfloor - (2^m-1)}$, for all $1 \leq j \leq m-1$. Furthermore, observe that the above arguments also hold for any linear combination of the first $m-1$ rows of H_{Ham}, i.e., it holds that $\widehat{\mathbb{1}_{S_2}}\left(\text{Eval}^{\setminus \mathbf{0}}(\mathbf{s})\right) = 2^{\left\lfloor \frac{2^m-1}{2} \right\rfloor - (2^m-1)}$, where $\mathbf{s} = \sum_{j=2}^{m} c_j \cdot \text{Eval}^{\setminus \mathbf{0}}(x_j)$, for $c_j \in \{0,1\}$, $j \in [2:m]$.

It can also be seen that since $\text{Eval}^{\setminus \mathbf{0}}(x_m) \notin V_{\mathcal{B}}$, we have that $\widehat{\mathbb{1}_{S_2}}\left(\text{Eval}^{\setminus \mathbf{0}}(x_m)\right) = 0$, and similarly, that $\widehat{\mathbb{1}_{S_2}}\left(\text{Eval}^{\setminus \mathbf{0}}(\mathbf{s})\right) = 0$, where $\mathbf{s} = \text{Eval}(x_1) + \sum_{j=1}^{m-1} c_j \cdot \text{Eval}(x_j)$, for $c_j \in \{0,1\}$, $j \in [m-1]$. Putting everything together, we observe that for half of the codewords $\mathbf{s} \in \mathcal{C}^\perp$, the Fourier coefficient $\widehat{\mathbb{1}_{S_2}}(\mathbf{s})$ equals $2^{\left\lfloor \frac{2^m-1}{2} \right\rfloor - (2^m-1)}$, and for another half of the codewords, the Fourier coefficient $\widehat{\mathbb{1}_{S_2}}(\mathbf{s})$ equals zero. Applying (7.6), we get that

$$\begin{aligned} N(\mathcal{C}; S_2) &= |\mathcal{C}| \cdot \sum_{\mathbf{s} \in \mathcal{C}^\perp} \widehat{\mathbb{1}_{S_2}}(\mathbf{s}) \\ &= 2^{2^m - 1 - m} \cdot 2^{m-1} \cdot 2^{\left\lfloor \frac{2^m-1}{2} \right\rfloor - (2^m-1)} = 2^{\left\lfloor \frac{2^m-1}{2} \right\rfloor - 1}, \end{aligned}$$

where the second inequality holds since $|\mathcal{C}| = 2^{2^m-1-m}$ and $\left|\mathcal{C}^\perp\right| = 2^m$, and half the codewords $\mathbf{s} \in \mathcal{C}^\perp$ have nonzero Fourier coefficient $\widehat{\mathbb{1}_{S_2}}(\mathbf{s})$. □

Note that in Corollary 7.5.3, the number of constrained codewords in the linear codes is half the total number of constrained codewords, $2^{\left\lfloor \frac{n}{2} \right\rfloor}$, of the same blocklength n as the codes under consideration. However, in the limit as the blocklength goes to infinity, the rates of the subcodes of the single parity-check and Hamming codes that lie in S_2, equal the noiseless capacity C_0 of the constraint (see Section 5.2.2), which in turn equals $\frac{1}{2}$.

We then move on to counting constrained codewords in the Reed-Muller (RM) family of codes. Using the structure of Fourier coefficients given in Lemma 7.5.1 and using the fact that the dual code of $\text{RM}(m,r)$ is the code $\text{RM}(m, m-r-1)$, for $r \leq m-1$, we numerically calculate the number of constrained codewords $N(\text{RM}(m,r); S_2)$, for

(m,r)	$(4,2)$	$(4,3)$	$(5,3)$	$(6,4)$	$(7,5)$	$(8,6)$
$N(\mathrm{RM}(m,r);S_2)$	16	128	2048	6.711×10^7	1.441×10^{17}	1.329×10^{36}

Table 7.1: Table of values of $N(\mathrm{RM}(m,r);S_2)$, for select parameters m and r

certain (large) values of m and r. Our results are documented in Table 7.1. Note that the computational technique in Theorem 7.4.1 proves particularly useful when the rate of $\mathrm{RM}(m,r)$ is larger than $\frac{1}{2}$, or equivalently, when $r > \left\lceil \frac{m}{2} \right\rceil$. The algorithm we have used for generating the entries in Table 7.1, as an illustration of the application of Theorem 7.4.1, simply plugs in the Fourier coefficients from Lemma 7.5.1. The time complexity of this algorithm is thus $O(n \cdot |\mathcal{C}^{\perp}|)$ for $\mathcal{C} = \mathrm{RM}(m,r)$.

More generally though, observe that the constraint that a word $\mathbf{x} \in \{0,1\}^n$ lies in S_2 can be represented by the set of linear equations (over $\mathbb{F}_2$) given by $x_1 = 0$ and $x_{2i} + x_{2i+1} = 1$, for all $1 \leq i \leq \left\lfloor \frac{n-1}{2} \right\rfloor$. Furthermore, any linear code $\mathcal{C}$ of dimension k and parity-check matrix H is such that its codewords $\mathbf{c}$ are solutions to $H \cdot \mathbf{c}^T = 0^{n-k}$. The 2-charge constrained codewords in $\mathcal{C}$ can thus be represented as solutions to a system of linear equations over $\mathbb{F}_2$, and the number of such solutions can be determined by Gaussian elimination, in time that is polynomial in the blocklength n.

7.5.2 Constant Subblock-Composition Constraint

We here consider a different constraint, the constant subblock-composition CSC_z^p constraint, which requires that each one of the p "subblocks" of a binary sequence have a constant number, z, of 1s. In particular, for any sequence $\mathbf{x} \in \{0,1\}^n$, we first partition the n coordinates into p subblocks, with the ℓ^{th} subblock being the vector of symbols $\mathbf{x}_\ell := \left(x_i \in \{0,1\} : \frac{(\ell-1)n}{p} + 1 \leq i \leq \frac{\ell n}{p} \right)$, for $1 \leq \ell \leq p$. We implicitly assume that p divides n. Note that hence $\mathbf{x} = \mathbf{x}_1 \mathbf{x}_2 \ldots \mathbf{x}_p$. A binary sequence $\mathbf{x}$ respects the CSC_z^p constraint if $w(\mathbf{x}_\ell) = z$, for all $1 \leq \ell \leq p$. We let C_z^p denote the set of all CSC_z^p-constrained

sequences of length n. CSC_z^p-constrained sequences were introduced in [74] for simultaneous information and energy transfer to an energy harvesting receiver, while ensuring that the receiver battery does not drain out during periods of low signal energy (see [75] and [76] for applications).

The lemma below provides the Fourier coefficients of $\mathbb{1}_{C_z^p}$.

Lemma 7.5.4. *For $\mathbf{s} \in \{0,1\}^n$ with $\mathbf{s} = \mathbf{s}_1\mathbf{s}_2 \ldots \mathbf{s}_p$, we have that*

$$2^n \cdot \widehat{\mathbb{1}_{C_z^p}}(\mathbf{s}) = \prod_{\ell=1}^{p} K_z^{(n/p)}(w(\mathbf{s}_\ell)),$$

where $K_i^{(n/p)}(j) = \sum_{t=0}^{i}(-1)^t\binom{j}{t}\binom{n/p-j}{i-t}$ is the i^{th}-Krawtchouk polynomial, for the length n/p.

Proof. We have that

$$\begin{aligned}
2^n \cdot \widehat{\mathbb{1}_{C_z^p}}(\mathbf{s}) &= \sum_{\mathbf{x}\in\{0,1\}^n:\ \mathbf{x}\in C_z^p} (-1)^{\mathbf{x}\cdot\mathbf{s}} \\
&= \sum_{\mathbf{x}_1\in\{0,1\}^{n/p}:\ w(\mathbf{x}_1)=z} \cdots \sum_{\mathbf{x}_p\in\{0,1\}^{n/p}:\ w(\mathbf{x}_p)=z} (-1)^{\mathbf{x}_1\cdot\mathbf{s}_1}\ldots(-1)^{\mathbf{x}_p\cdot\mathbf{s}_p} \\
&= \prod_{\ell=1}^{p}\left(\sum_{\mathbf{x}_\ell\in\{0,1\}^{n/p}:\ w(\mathbf{x}_\ell)=z} (-1)^{\mathbf{x}_\ell\cdot\mathbf{s}_\ell}\right).
\end{aligned}$$

Now, for any $\ell \in [p]$, the summation above only on the weight $w(\mathbf{s}_\ell)$, i.e., for any permutation of coordinates $\pi : \{0,1\}^{n/p} \to \{0,1\}^{n/p}$, it holds that

$$\begin{aligned}
\sum_{\mathbf{x}\in\{0,1\}^{n/p}:\ w(\mathbf{x})=z} (-1)^{\mathbf{x}\cdot(\pi\cdot\mathbf{s}_\ell)} &= \sum_{\mathbf{x}\in\{0,1\}^{n}:\ w(\mathbf{x})=z} (-1)^{(\pi\cdot\mathbf{x})\cdot(\pi\cdot\mathbf{s}_\ell)} \\
&= \sum_{\mathbf{x}\in\{0,1\}^{n}:\ w(\mathbf{x})=z} (-1)^{\mathbf{x}\cdot\mathbf{s}_\ell}.
\end{aligned}$$

Hence, for any $\ell \in [p]$ and for $\mathbf{s}_\ell$ such that $w(\mathbf{s}_\ell) = j$, it suffices that we calculate the summation above at $\mathbf{s}_\ell = \mathbf{s}^\star = (s_1^\star, \ldots, s_{n/p}^\star)$, with $s_1^\star = \ldots = s_j^\star = 1$ and $s_{j+1}^\star = \ldots = s_{n/p}^\star = 0$. By a direct computation, it can be checked that the summation above equals

$K_z^{(n/p)}(w(\mathbf{s}_\ell))$. □

In what follows, we shall concern ourselves with the application of Lemma 7.5.4 and Theorem 7.4.1 to calculating the number of subblock constrained codewords in Reed-Muller (RM) codes $\mathrm{RM}(m,r)$, for selected values of the number of subblocks p.

First, we recall an important property of RM codes, which is sometimes called the Plotkin decomposition (see [58, Chap. 13] or the survey [52]): any length-2^m codeword $\mathbf{c} \in \mathrm{RM}(m,r)$ can be written as the concatenation $\mathbf{c} = (\mathbf{u} \mid \mathbf{u}+\mathbf{v})$, where $\mathbf{u} \in \mathrm{RM}(m-1,r)$ and $\mathbf{v} \in \mathrm{RM}(m-1,r-1)$ and the '$+$' operation in $\mathbf{u}+\mathbf{v}$ is over $\mathbb{F}_2^{2^{m-1}}$. Observe that since $\mathrm{RM}(m,t)$, for $1 \leq t \leq m$, consists of evaluation vectors of Boolean polynomials of degree at most t, it holds that $\mathrm{RM}(m-1,r-1) \subset \mathrm{RM}(m-1,r)$. In what follows, we ensure that $r \geq 1$ and m is large.

Assume, for simplicity, that $p = 2$. We then have that for $0 \leq z \leq 2^{m-1}$,

$$\begin{aligned} N\left(\mathrm{RM}(m,r); C_z^2\right) &= \sum_{\mathbf{c}\in\mathrm{RM}(m,r)} \mathbb{1}_{C_z^2}(\mathbf{x}) \\ &= \sum_{\substack{\mathbf{u}\in\mathrm{RM}(m-1,r),\\ \mathbf{v}\in\mathrm{RM}(m-1,r-1)}} \mathbb{1}_{W_z}(\mathbf{u}) \cdot \mathbb{1}_{W_z}(\mathbf{u}+\mathbf{v}), \end{aligned} \tag{7.8}$$

where the second equality uses the Plotkin decomposition and the fact that the set W_z consists of sequences of Hamming weight exactly z. Further, let $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_M$ be an enumeration of coset representatives of distinct cosets of $\mathrm{RM}(m-1,r-1)$ in $\mathrm{RM}(m-1,r)$, where $M = \frac{|\mathrm{RM}(m-1,r)|}{|\mathrm{RM}(m-1,r-1)|} = 2^{\binom{m-1}{\leq r}-\binom{m-1}{\leq r-1}} = 2^{\binom{m-1}{r}}$. In other words, $\mathbf{u}_i$ is a representative of the coset $\mathbf{u}_i + \mathrm{RM}(m-1,r-1)$, with $\mathbf{u}_i \in \mathrm{RM}(m-1,r)$, for $1 \leq i \leq M$, where the cosets $\mathbf{u}_j + \mathrm{RM}(m-1,r-1)$, for different values of j, are disjoint. Let $A_{\mathbf{u}}(y)$ be the weight enumerator of the coset $\mathbf{u} + \mathrm{RM}(m-1,r-1)$, at the weight

$0 \leq y \leq 2^{m-1}$, for $\mathbf{u} \in \mathrm{RM}(m-1, r)$. Then, from (7.8), we see that

$$\begin{aligned} N\left(\mathrm{RM}(m,r); C_z^2\right) &= \sum_{\substack{\mathbf{u}\in\mathrm{RM}(m-1,r),\\ \mathbf{v}\in\mathrm{RM}(m-1,r-1)}} \mathbb{1}_{W_z}(\mathbf{u}) \cdot \mathbb{1}_{W_z}(\mathbf{u}+\mathbf{v}) \\ &= \sum_{\mathbf{u}\in\mathrm{RM}(m-1,r)} \mathbb{1}_{W_z}(\mathbf{u}) \cdot \sum_{\mathbf{v}\in\mathrm{RM}(m-1,r-1)} \mathbb{1}_{W_z}(\mathbf{u}+\mathbf{v}) \\ &= \sum_{\mathbf{u}\in\mathrm{RM}(m-1,r)} \mathbb{1}_{W_z}(\mathbf{u}) \cdot A_{\mathbf{u}}(z) \\ &\overset{(a)}{=} \sum_{i=1}^{M} \sum_{\mathbf{u}\in\mathbf{u}_i+\mathrm{RM}(m-1,r-1)} \mathbb{1}_{W_z}(\mathbf{u}) \cdot A_{\mathbf{u}_i}(z) = \sum_{i=1}^{M} \left(A_{\mathbf{u}_i}(z)\right)^2, \end{aligned} \tag{7.9}$$

where equality (a) uses the fact that any $\mathbf{u} \in \mathrm{RM}(m-1, r)$ belongs to some coset $\mathbf{u}_i + \mathrm{RM}(m-1, r-1)$.

While equality (7.9) provides a neat method to count the number of constrained codewords $N\left(\mathrm{RM}(m,r); C_z^2\right)$, provided the coset weight enumerators $A_{\mathbf{u}_i}(z)$, $1 \leq i \leq M$, are known, observe that in the summation in (7.9), we need to perform $M - 1 = 2^{\binom{m-1}{r}} - 1$ additions. If r is large, the number of such additions can be fairly high. We show next that with the help of Theorem III.1 and Lemma IV.3, it is possible to reduce the number of computations, when r is large. Before we do so, we recall the fact that for $r \leq m-1$, the dual code of $\mathrm{RM}(m, r)$ is the code $\mathrm{RM}(m, m-r-1)$. We let $\overline{A}_{\mathbf{u}}(y)$ be the weight enumerator of the coset $\mathbf{u} + \mathrm{RM}(m-1, m-r-2)$, at the weight $0 \leq y \leq 2^{m-1}$, for $\mathbf{u} \in \mathrm{RM}(m-1, m-r-1)$. Further, we let $\overline{\mathbf{u}}_1, \overline{\mathbf{u}}_2, \ldots, \overline{\mathbf{u}}_{\overline{M}}$ be an enumeration of coset representatives of distinct cosets of $\mathrm{RM}(m-1, m-r-2)$ in $\mathrm{RM}(m-1, m-r-1)$, where $\overline{M} = \frac{|\mathrm{RM}(m-1,m-r-1)|}{|\mathrm{RM}(m-1,m-r-2)|} = 2^{\binom{m-1}{m-r-1}}$.

Now, applying Theorem III.1, we see that

$$\begin{aligned}
N\left(\mathrm{RM}(m,r);C_z^2\right) &= \sum_{\mathbf{s}_1\mathbf{s}_2\in\mathrm{RM}(m,m-r-1)} K_z^{(n/2)}(w(\mathbf{s}_1))\cdot K_z^{(n/2)}(w(\mathbf{s}_2)) \\
&= \sum_{\substack{\mathbf{u}\in\mathrm{RM}(m-1,m-r-1),\\ \mathbf{v}\in\mathrm{RM}(m-1,m-r-2)}} K_z^{(n/2)}(w(\mathbf{u}))\cdot K_z^{(n/2)}(w(\mathbf{u}+\mathbf{v})) \\
&= \sum_{\mathbf{u}\in\mathrm{RM}(m-1,m-r-1)} K_z^{(n/2)}(w(\mathbf{u}))\cdot \sum_{\mathbf{v}\in\mathrm{RM}(m-1,m-r-2)} K_z^{(n/2)}(w(\mathbf{u}+\mathbf{v})) \\
&= \sum_{\mathbf{u}\in\mathrm{RM}(m-1,m-r-1)} K_z^{(n/2)}(w(\mathbf{u}))\cdot \sum_{j=0}^{2^{m-1}} \overline{A}_{\mathbf{u}}(j)\cdot K_z^{(n/2)}(j) \\
&= \sum_{i=1}^{\overline{M}} \left(\sum_{j=0}^{2^{m-1}} \overline{A}_{\overline{\mathbf{u}}_i}(j)\cdot K_z^{(n/2)}(j)\right)^2 . \qquad (7.10)
\end{aligned}$$

Now, observe that using equality (7.10), the number of computations required, in the form of summations, assuming that the coset weight enumerators $\overline{A}_{\overline{\mathbf{u}}_i}(\cdot)$ are known, for all $1 \leq i \leq \overline{M}$, is $2^{m-1+\overline{M}} - 1 = 2^{m-1+\binom{m-1}{m-r-1}} - 1$. Clearly, since for large r (and large m), we have that $m-1+\binom{m-1}{m-r-1} < \binom{m-1}{r}$, we note the relative ease of calculating $N\left(\mathrm{RM}(m,r);C_z^2\right)$ via (7.10), with the aid of Theorem III.1, as compared to using (7.9). We remark here that the analysis of the number of codewords in $\mathrm{RM}(m,r)$ that lie in C_z^p can be extended to values of p that are powers of 2, by iteratively applying the Plotkin decomposition. Finally, we note that in order to compute the coset weight enumerators required in (7.9) and (7.10), one can use the recursive algorithm provided in [77], which applies to RM codes, in addition to polar codes.

7.6 Applications: Numerically Computable Fourier Coefficients

In this section, we shall work with runlength-limited constraints on binary sequences. We provide recurrence relations for the Fourier coefficients, which allow them to be efficiently computable, numerically.

7.6.1 (d,∞)-Runlength Limited Constraint

In this subsection, we concern ourselves with the (d,∞)-runlength limited (RLL) constraint, considered in Chapters 4 and 5. Recall that this constraint mandates that there be at least d 0s between every pair of successive 1s in the binary input sequence, where $d \geq 1$. We let $S_{(d,\infty)}$ denote the set of (d,∞)-RLL constrained binary words of length n.

Now, for $n \geq 1$, and for $\mathbf{s} \in \{0,1\}^n$, let $\widehat{\mathbb{1}_{S_{(d,\infty)}}}^{(n)}(\mathbf{s})$ denote the Fourier coefficient at $\mathbf{s}$, when the blocklength is n. We then have that:

Lemma 7.6.1. *For $n \geq d+2$ and for $\mathbf{s} = (s_1, \ldots, s_n) \in \{0,1\}^n$, it holds that*

$$\widehat{\mathbb{1}_{S_{(d,\infty)}}}^{(n)}(\mathbf{s}) = 2^{-1} \cdot \widehat{\mathbb{1}_{S_{(d,\infty)}}}^{(n-1)}\left(s_2^n\right) + (-1)^{s_1} \cdot 2^{-(d+1)} \cdot \widehat{\mathbb{1}_{S_{(d,\infty)}}}^{(n-d-1)}\left(s_{d+2}^n\right).$$

Proof. We first write

$$\begin{aligned}\widehat{\mathbb{1}_{S_{(d,\infty)}}}^{(n)}(\mathbf{s}) &= \frac{1}{2^n} \cdot \sum_{\mathbf{x} \in S_{(d,\infty)}} (-1)^{\mathbf{x}\cdot\mathbf{s}} \\ &= 2^{-n} \cdot \big(\#\{x^n \in S_{(d,\infty)} :\ w_{\mathbf{s}}(x^n) \text{ is even}\} - \#\{x^n \in S_{(d,\infty)} :\ w_{\mathbf{s}}(x^n) \text{ is odd}\}\big).\end{aligned} \tag{7.11}$$

We now prove the recurrence relation when $s_1 = 0$. Observe that in this case,

$$\begin{aligned}&\#\{x^n \in S_{(d,\infty)} :\ w_{\mathbf{s}}(x^n) \text{ is even}\} \\ &= \#\{x^n \in S_{(d,\infty)} :\ w_{\mathbf{s}}(x^n) \text{ is even and } x_1 = 0\} + \#\{x^n \in S_{(d,\infty)} :\ w_{\mathbf{s}}(x^n) \text{ is even and } x_1 = 1\} \\ &\overset{(a)}{=} \#\{x_2^n \in S_{(d,\infty)} :\ w_{s_2^n}(x_2^n) \text{ is even}\} + \#\{x^n \in S_{(d,\infty)} :\ w_{\mathbf{s}}(x^n) \text{ is even and } x_1^{(d+1)} = 10^d\} \\ &= \#\{x_2^n \in S_{(d,\infty)} :\ w_{s_2^n}(x_2^n) \text{ is even}\} + \#\{x_{d+2}^n \in S_{(d,\infty)} :\ w_{s_{d+2}^n}(x_{d+2}^n) \text{ is even}\},\end{aligned} \tag{7.12}$$

where (a) holds because $s_1 = 0$ and from the fact that the (d,∞)-RLL constraint requires that $x_2^{d+1} = 0^d$, if $x_1 = 1$. Similarly, we obtain that

$$\begin{aligned}\#\{x^n \in S_{(d,\infty)} :\ w_{\mathbf{s}}(x^n) \text{ is odd}\} =& \#\{x_2^n \in S_{(d,\infty)} :\ w_{s_2^n}(x_2^n) \text{ is odd}\} + \\ & \#\{x_{d+2}^n \in S_{(d,\infty)} :\ w_{s_{d+2}^n}(x_{d+2}^n) \text{ is odd}\}.\end{aligned} \tag{7.13}$$

Now, observe that

$$\widehat{\mathbb{1}_{S_{(d,\infty)}}}^{(n-1)}(s_2^n) = 2^{-(n-1)} \cdot \Big(\#\{x_2^n \in S_{(d,\infty)} : \ w_{s_2^n}(x_2^n) \text{ is even}\} - \#\{x_2^n \in S_{(d,\infty)} : \ w_{s_2^n}(x_2^n) \text{ is odd}\}\Big) \tag{7.14}$$

and that

$$\begin{aligned}&\widehat{\mathbb{1}_{S_{(d,\infty)}}}^{(n-d-1)}(s_{d+2}^n) \\ &= 2^{-(n-d-1)} \cdot \Big(\#\{x_{d+2}^n \in S_{(d,\infty)} : \ w_{s_{d+2}^n}(x_{d+2}^n) \text{ is even}\} - \\ &\qquad \#\{x_{d+2}^n \in S_{(d,\infty)} : \ w_{s_{d+2}^n}(x_{d+2}^n) \text{ is odd}\}\Big).\end{aligned} \tag{7.15}$$

Substituting (7.12) and (7.13) in (7.11) and using (7.14) and (7.15), we get the recurrence relation when $s_1 = 0$. The case when $s_1 = 1$ is proved similarly. □

We shall now explain how Lemma 7.6.1 helps compute the Fourier coefficients for a given (large) n, efficiently. First, we note that a direct computation of all the Fourier coefficients of $\mathbb{1}_{S_{(d,\infty)}}$ at blocklength n, can be accomplished by the fast Walsh-Hadamard transform (FWHT) algorithm (see Exercise 1.12(b) in [70]), in time $n \cdot 2^n$. Now, let us assume that we pre-compute and store the Fourier coefficients $\left(\widehat{\mathbb{1}_{S_{(d,\infty)}}}^{(m)}(\mathbf{s}) : \ \mathbf{s} \in \{0,1\}^m\right)$, for $1 \leq m \leq d+1$. These Fourier coefficients help initialize the recurrences in Lemma 7.6.1. Now, given a fixed (large) n, the Fourier coefficients at which blocklength we intend computing, we shall calculate, using the recurrence relations above, the Fourier coefficients at all blocklengths $d+2 \leq m \leq n$, iteratively, beginning at length $d+2$, and increasing m. Assuming that the additions and multiplications in Lemma 7.6.1 take unit time, it can be seen that the time complexity of computing the Fourier coefficient at length n grows as $\sum_{d+2}^{n} 2^i < 2^{n+1}$. This is much less than the time that is $2^{n+\log_2 n}$, taken by the FWHT algorithm.

However, there still remains the issue of storage cost: at a blocklength m, one needs to store all 2^m Fourier coefficients in order to facilitate computation of the Fourier coefficients at blocklengths $n > m$. Hence, assuming that the storage of a single Fourier

$\mathcal{C}$	RM$(4,2)$	RM$(4,3)$	Ham$_3$	Ham$_4$
$N(\mathcal{C}; S_{(1,\infty)})$	83	1292	4	101

Table 7.2: Table of values of $N(\mathcal{C}; S_{(1,\infty)}))$, for select codes $\mathcal{C}$

coefficient takes up one unit of space, we see that we require at least 2^n units of memory in order to store the Fourier coefficients at blocklength n.

We now use the Fourier coefficients that are numerically computed using Lemma 7.6.1, to calculate, in Table 7.2, the number of $(1,\infty)$-RLL constrained codewords in select codes, by applying Theorem 7.4.1. We denote the binary Hamming code of blocklength $2^t - 1$ as Ham$_t$.

7.7 Conclusions and Directions for Future Work

In this chapter, motivated by the approach in Chapter 5 of designing coding schemes using subcodes of linear codes, for use over input-constrained DMCs, we provided a Fourier-analytic perspective on the question of calculating the number of (arbitrarily) constrained codewords in a general linear code. Our approach helped transform our counting problem into a question about the dual code, via an application of Plancherel's Theorem. An important ingredient of our method was the Fourier transform of the indicator function of the constraint, which we showed to be computable (analytically or numerically), for a number of constraints. Using this Fourier transform, we provided values (either analytical or numerical) for the number of constrained codewords for well-known linear codes.

We believe that the Fourier transform of the indicator function of the constraint is in itself an interesting object for future study, and it is of interest to explore its computability for general families of constraints. In particular, we ask the question if recurrence relations such as that in Lemma 7.6.1 can be derived more generally for a class of constraints. Preliminary experiments seem to suggest patterns for such recurrence relations, which derive their structure from the characteristic equations of certain

matrices with entries in $\{-1, 0, +1\}$. We believe that this observation merits further exploration. We are also interested in the applications of such Fourier transforms in other problems such as obtaining bounds on the sizes of the largest constrained codes with a prescribed minimum distance. Another interesting line of study would be to build on the techniques in our work and study the asymptotics of the rates of constrained subcodes of linear codes of a given rate $R \in (0, 1)$.

Chapter 8

Coding Schemes for Runlength-Limited BECs With Feedback

> "Jeeves," I said. "A rummy communication has arrived. From Mr. Glossop. ... Message runs as follows:
> When you come tomorrow, bring my football boots. Also, if humanly possible, Irish water-spaniel. Urgent. Regards. Tuppy.
> "What do you make of that, Jeeves?"
> "As I interpret the document, sir, Mr. Glossop wishes you, when you come tomorrow, to bring his football boots. Also, if humanly possible, an Irish water-spaniel. He hints that the matter is urgent, and sends his regards."
>
> P. G. Wodehouse, Very Good, Jeeves!, 1930

8.1 Introduction

The chapters until now have focused on deriving lower bounds on the capacities of input-constrained DMCs via either information-theoretic inequalities or by explicit constructions of coding schemes over such channels. This chapter in part presents an approach to derive upper bounds on the capacities of a specific class of input-constrained DMCs, by explicitly solving for the capacity of a related channel model. In

particular, we work with the setting of the input-constrained DMC with causal, noiseless feedback, and explicitly derive the feedback capacity of the channel. We refer the reader to Chapter 3 for a brief description of the channel model. Recall that for the *unconstrained* DMC, it is known that feedback does not increase its capacity [78]. However, this statement does not hold in general for channels with memory[1]. The specific input-constrained DMC that we shall work with is the (d, ∞)-RLL input-constrained binary erasure channel (BEC), for which we shall derive a feedback capacity-achieving coding scheme. However, we shall first present some results on the feedback capacities of a broad class of channels with memory.

8.2 Literature Survey and Our Work

The feedback capacities of channels with memory were first considered by Massey in [80], wherein, for causal channels, the supremum of the "directed mutual information rate" was proved to be an upper bound on the feedback capacity. Much later, Tatikonda, in his Ph.D. thesis [81], derived the feedback capacity of a class of memoryless channels, whose inputs are produced by a finite-state machine. For this class of channels, the problem of feedback capacity computation was cast in [82] as an average-reward stochastic control problem (see [83]), which was shown to be solvable by dynamic programming (DP) methods. The results of these works were unified and generalized in [84], which extended the proofs of Gallager in [6], to the setting of finite-state channels (FSCs) with causal feedback, where the feedback information provided to the

[1]For the special class of finite-alphabet channels with additive random noise (where the capacity-achieving output distribution is the uniform distribution), it was shown in [79] that feedback does not increase the capacity. Note that here the noise random process can be *arbitrary* (the noise process is not even required to be stationary); the result holds so long as the noise process is independent of the input process. For example, this shows that for the Gilbert-Elliott channel [68], feedback does not increase capacity. For channels with non-trivial hard input constraints, the capacity-achieving output distribution is in general *not* the uniform distribution.

encoder is a time-invariant, deterministic function of the outputs received by the decoder. For formal definitions of the feedback capacity and related information-theoretic quantities, we refer the reader to [84].

We first state some results from the literature on the (causal, noiseless) feedback capacities of general finite-state channels (refer Section 4.2 for the definition of FSCs), the channel model for which is obtained from Figure 3.3, by replacing the DMC with a generic FSC, and by replacing the constrained encoder with an unconstrained encoder. We assume, in addition, that the initial state $s_0 \in \mathcal{S}$ is fixed and is known to both the encoder and the decoder. Then, the feedback capacity of such an FSC is (see, for example, [84])

$$C^{\text{fb}} = \lim_{n\to\infty} \frac{1}{n} \max_{P(x^n||y^{n-1})} I(X^n \to Y^n),$$

where, the notation

$$P(x^n||y^{n-1}) := \prod_{t=1}^{n} P(x_t \mid x^{t-1}, y^{t-1})$$

is the "causal conditional distribution" of the inputs given the outputs, and the notation

$$I(X^n \to Y^n) := \sum_{t=1}^{n} I(X^t; Y_t \mid Y^{t-1})$$

stands for the "directed information" between the inputs and the outputs. Note that in the definitions above, the conditioning on the known initial state s_0 is implicitly present, although it is suppressed in the notation.

At around the same time, the authors of [85] considered the class of the so-called "unifilar" channels, which are FSCs in which the state s_t at any time $t \geq 1$ is a time-invariant, deterministic function of the previous state, and the current input and output, i.e., $s_t = f(s_{t-1}, x_t, y_t)$, for some function f (see Chapter 4 and contrast this with the definition of an input-driven FSC therein). If the channel is connected[2], besides, it was shown that the feedback capacity of the unifilar channel (with fixed, known initial

[2]An FSC is connected if for any state $s \in \mathcal{S}$, there exists an integer $T(s) \geq 1$ and an input distribution $\{Q(x_t \mid s_{t-1})\}_{t\geq 1}$ (which may depend on s), such that $\sum_{t=1}^{T(s)} \Pr[S_t = s \mid s_0] > 0$, for all $s_0 \in \mathcal{S}$.

state s_0) can be expressed as:

$$C_{\mathrm{u}}^{\mathrm{fb}} = \sup_{\{P(x_t|s_{t-1},\, y^{t-1})\}_{t\geq 1}} \liminf_{n\to\infty} \frac{1}{n} \sum_{t=1}^{n} I(X_t, S_{t-1}; Y_t \mid Y^{t-1}).$$

Furthermore, the problem of computing the feedback capacity of this class of channels was cast as a dynamic programming (DP) problem, thereby subsuming the work in [81]. The work in [85] then applied this technique for explicitly computing the feedback capacity of the so-called trapdoor channel, and the insights from the DP approach were used to construct an explicit, zero-error, feedback capacity-achieving coding scheme. Explicit solutions of the feedback capacity DP problem for several other unifilar finite-state channels such as the Ising channel [86], the chemical channel [87], the $(1,\infty)$-RLL input-constrained BEC [88] and BIBO [89] (binary-input binary-output) channels, and the $(0,k)$-RLL input-constrained BEC [90], were provided in later works. The work [91] then provided (potentially tight) single-letter upper and lower bounds on the feedback capacities of connected, unifilar channels, which were extended in [92] to derive encoder structures, which yield coding schemes based on the posterior-matching principle [89, 93].

In what follows, we study the problem of the computation of the feedback capacity of, and the design of good coding schemes for, the BEC (with erasure probability ϵ; recalled in Figure 8.1) with the (d,∞)-RLL input-constraint.

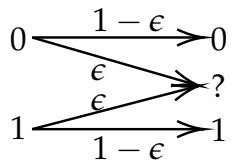


Figure 8.1: The binary erasure channel with erasure probability ϵ, with input alphabet $\mathcal{X} = \{0, 1\}$ and output alphabet $\mathcal{Y} = \{0, ?, 1\}$.

Recall that the (d,∞)-RLL input constraint, which mandates that there are at least d 0s between every pair of successive 1s in the input sequence. Figure 8.2 recalls a state transition graph that represents the constraint. Recall also that the (d,∞)-RLL

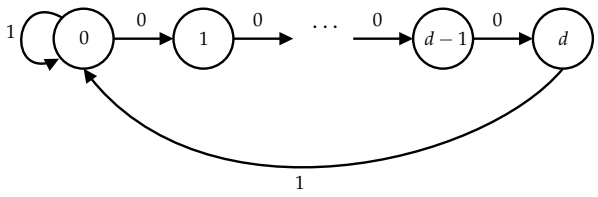


Figure 8.2: State transition graph for the (d, ∞)-RLL constraint

constraint is a special case of the (d, k)-RLL constraint, which admits only binary sequences with at least d and at most k 0s between successive 1s.

In the exposition here, we provide a simple, labelling-based, zero-error feedback coding scheme for the (d, ∞)-RLL input-constrained BEC, similar to the those presented in [88] and [90], for other input-constrained BECs. We then prove that our feedback coding scheme is in fact feedback capacity-achieving. Our method uses the single-letter bounding techniques in [91] to obtain an upper bound on feedback capacity, which we show to be equal to the rate of our proposed coding scheme. As a result, we are able to explicitly characterize the feedback capacity of the (d, ∞)-RLL input-constrained BEC, which is given by a $(d+1)$-parameter optimization problem:

$$C^{\text{fb}}_{(d,\infty)}(\epsilon) = \max_{\substack{\delta_0,\ldots,\delta_d \geq 0 \\ \sum_{i=0}^{d} \delta_i \leq 1}} \frac{\bar{\epsilon}\left(\sum_{i=0}^{d} \epsilon^i h_b(\delta_i)\right)}{\sum_{i=0}^{d} \epsilon^i + d\bar{\epsilon}\left(\sum_{i=0}^{d} \epsilon^i \delta_i\right)}.$$

Our formula generalizes the coding scheme in [88], where the feedback capacity of the $(1, \infty)$-RLL input-constrained BEC was derived using dynamic programming techniques. Our work also supplements the results in [90], which provided the feedback capacity of the $(0, k)$-RLL input-constrained BEC. However, interestingly, unlike the previous two results, the feedback capacity of the (d, ∞)-RLL input-constrained BEC, for general d, does not equal the capacity when the encoder possesses non-causal knowledge of erasures (this observation was also made in [90]). We also compare the feedback capacity that we compute with known upper bounds on the non-feedback capacity, and arrive at the conclusion that at least for select values of d, feedback increases

the capacity of the channel.

8.3 Preliminaries

8.3.1 Problem Definition

In this subsection, we provide more details about the system model of a (d, ∞)-RLL input-constrained DMC with feedback (the system model of a generic input-constrained DMC with feedback was first discussed in Chapter 3). Recall that in this setting, the constrained encoder at time i has, in addition to the message, access to noiseless feedback in the form of the outputs, y^{i-1}, from the decoder. It then produces a binary input symbol $x_i \in \{0, 1\}$, as a function of the specific instance of the message, m, and the outputs, y^{i-1}, in such a manner that the (d, ∞)-RLL constraint (see Figure 8.2) is respected. We set the channel state alphabet, $\mathcal{S}$, to be $\{0, 1, \ldots, d\}$. In what follows, we define some information-theoretic quantities related to this channel model.

Definition 7. *An* $(n, 2^{nR}, (d, \infty))$ feedback *code for an input-constrained channel is defined by the encoding functions:*

$$f_i : \{1, \ldots, 2^{nR}\} \times \mathcal{Y}^{i-1} \to \mathcal{X}, \quad i \in [n],$$

which satisfy $f_i(m, y^{i-1}) = 0$*, if* $f_{(i-j)^+}(m, y^{(i-j-1)^+}) = 1$ *(where* x^+ *is equal to* $\max\{x, 0\}$*), for some* $j \in [d]$*, and a decoding function* $\Gamma : \mathcal{Y}^n \to \{1, \ldots, 2^{nR}\}$*.*

The average probability of error for a code is defined as $P_e^{(n)} = P(M \neq \Psi(Y^n))$*. A rate* R *is said to be* (d, ∞)*-feedback achievable if there exists a sequence of* $(n, 2^{nR}, (d, \infty))$ *feedback codes, such that* $\lim_{n\to\infty} P_e^{(n)} = 0$*. The feedback capacity* $C_{(d,\infty)}^{fb}$ *is defined to be the supremum over all* (d, ∞)*-achievable rates, and is a function of the channel parameters.*

Note that our focus will be on the DMC that is the binary erasure channel, or the BEC, with erasure probability $\epsilon \in [0, 1]$.

8.3.2 Q-graphs and (S, Q)-graphs

We now recall the definitions of the Q-graph and the (S, Q)-graph introduced in [91].

Definition 8. *A Q-graph is a finite irreducible labelled directed graph on a vertex set $\mathcal{Q}$, with the property that each $q \in \mathcal{Q}$ has at most $|\mathcal{Y}|$ outgoing edges, each labelled by a unique $y \in \mathcal{Y}$.*

Thus, there exists a function $\Phi : \mathcal{Q} \times \mathcal{Y} \to \mathcal{Q}$, such that $\Phi(q, y) = q'$ if, and only if, there is an edge $q \xrightarrow{y} q'$ in the $\mathcal{Q}$-graph. Figure 8.3 depicts a sample $\mathcal{Q}$-graph.

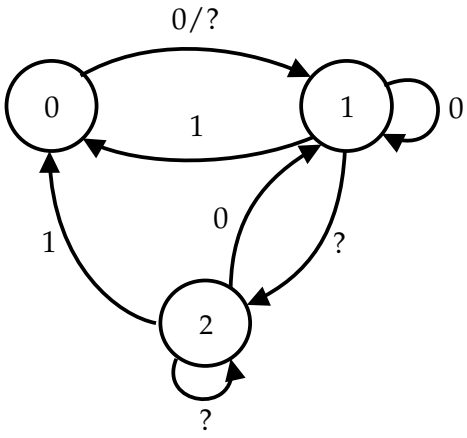


Figure 8.3: A sample $\mathcal{Q}$-graph. The edge labels represent outputs. The edge labelled by $0/?$ should be viewed as two edges, one labelled by 0 and another by ?, merged into one.

Suppose that we are given an input-constrained DMC W specified by $\{W(y|x)\}$. Let the states of the presentation of the input constraint obey $s_t = f(s_{t-1}, x_t)$. Further, suppose we are given a $\mathcal{Q}$-graph with vertex set $\mathcal{Q}$. We then define an (S, Q)-graph for this input-constrained DMC as follows:

Definition 9. *The (S, Q)-graph is defined to be a directed graph on the vertex set $\mathcal{S} \times \mathcal{Q}$, with edges $(s, q) \xrightarrow{(x,y)} (s', q')$ if, and only if, $W(y|x) > 0$, $s' = f(s, x)$, and $q' = \Phi(q, y)$.*

Given an input distribution $\{P(x|s, q)\}$ defined for each (s, q) in the $(\mathcal{S}, \mathcal{Q})$-graph, we have a Markov chain on $\mathcal{S} \times \mathcal{Q}$, where the transition probability associated with any edge (x, y) emanating from $(s, q) \in \mathcal{S} \times \mathcal{Q}$ is $W(y|x)P(x|s, q)$. Let $\mathcal{G}(\{P(x|s, q)\})$

be the subgraph remaining after discarding edges of zero probability. We then define

$$\Omega \triangleq \big\{\{P(x|s,q)\} : \mathcal{G}(\{P(x|s,q)\}) \text{ has a single closed communicating class}\big\}.$$

An input distribution $\{P(x|s,q)\} \in \Omega$ is said to be *aperiodic*, if the corresponding graph, $\mathcal{G}(\{P(x|s,q)\})$, is aperiodic. For such distributions, the Markov chain on $\mathcal{S} \times \mathcal{Q}$ has a unique stationary distribution $\pi(s,q)$.

8.3.3 Bounds on Feedback Capacity

We shall make use of the following single-letter upper bound on feedback capacity (specialized to input-constrained DMCs) [91]. The theorem assumes that the state transition graph corresponding to the input constraint is irreducible, and that the encoder and the decoder know the initial channel state, s_0.

Theorem 8.3.1 ([91], Theorem 2)**.** *The feedback capacity, C_{DMC}^{fb}, of an input-constrained DMC, when the state transition graph of the input-constraint is irreducible, is upper bounded as*

$$C_{DMC}^{fb} \leq \sup_{P(x|s,q)\in\Omega} I(X;Y|Q),$$

for all irreducible Q-graphs with q_0 such that (s_0, q_0) lies in an aperiodic closed communicating class.

8.4 Main Results

8.4.1 Capacity With Feedback

The following theorem states our main result concerning the capacity of the (d,∞)-RLL input-constrained BEC with feedback. For $\vec{\delta} = (\delta_0, \ldots, \delta_d)$, with $\delta_i \in [0,1]$, $\forall i$, we

define the function $R(\vec{\delta})$, where $\vec{\delta} \in [0,1]^{d+1}$, to be

$$R(\vec{\delta}) := \frac{\bar{\epsilon}\left(\sum_{i=0}^{d} \epsilon^i h_b(\delta_i)\right)}{\sum_{i=0}^{d} \epsilon^i + d\bar{\epsilon}\left(\sum_{i=0}^{d} \epsilon^i \delta_i\right)}. \tag{8.1}$$

We let Δ_{d+1} denote the following $(d+1)$-dimensional simplex: $\Delta_{d+1} := \{\vec{\delta} \in [0,1]^{d+1} : \sum_{i=0}^{d} \delta_i \leq 1\}$.

Theorem 8.4.1. *For $\epsilon \in [0,1]$, the feedback capacity of the (d,∞)-RLL input-constrained BEC is given by*

$$C_{(d,\infty)}^{fb}(\epsilon) = \max_{\vec{\delta} \in \Delta_{d+1}} R(\vec{\delta}), \tag{8.2}$$

and is achievable by a zero-error feedback coding scheme.

Remark 8.4.2. *At $\epsilon = 0$, the capacities with and without feedback are identical, and are given by $C_{(d,\infty)}(0) = \max_{\delta \in [0,1]} \frac{h_b(\delta)}{d\delta+1}$, the noiseless capacity of the (d,∞)-RLL input constraint.*

Remark 8.4.3. *Since from operational considerations, the zero-error feedback capacity, $C_{(d,\infty)}^{ze}$, is less than or equal to the feedback capacity, $C_{(d,\infty)}^{fb}$, Theorem 8.4.1 also shows that the two feedback capacities are indeed equal, i.e., $C_{(d,\infty)}^{ze} = C_{(d,\infty)}^{fb}$.*

Theorem 8.4.1 follows from the construction of a feedback coding scheme in Section 8.5, whose rate equals an upper bound on the feedback capacity computed using the single-letter bounding technique in [91]. The proof is presented in Section 8.5.

The expression for the feedback capacity provided in Theorem 8.4.1 admits the following simplification:

Proposition 8.4.4. *The vector $\vec{\delta}^\star := (\delta_0^*, \ldots, \delta_d^*)$ that attains the maximum in* (8.2) *is such that either $\vec{\delta}^\star$ is in the interior of Δ_{d+1}, or that $\sum_{i=0}^{d} \delta_i = 1$. Further, in the first case, we have that for any $\epsilon \in [0,1]$:*

$$C_{(d,\infty)}^{fb}(\epsilon) = \max_{\delta \in [0, \frac{1}{d+1}]} \frac{h_b(\delta)}{d\delta + \frac{1}{1-\epsilon}}.$$

Proof. Proposition 8.4.4 simplifies the maximizing values $\vec{\delta}^* := (\delta_0^*, \ldots, \delta_d^*)$ in the two cases when the maximum is attained at an interior point of Δ_{d+1} and when it is attained on the boundary.

First, we characterize the stationary points of $R(\vec{\delta})$. We define

$$N(\vec{\delta}) := \bar{\epsilon}\left(\sum_{i=0}^{d} \epsilon^i h_b(\delta_i)\right), \text{ and}$$
$$D(\vec{\delta}) := \sum_{i=0}^{d} \epsilon^i + d\bar{\epsilon}\left(\sum_{i=0}^{d} \epsilon^i \delta_i\right),$$

to be the numerator and the denominator of $R(\vec{\delta})$, respectively. Note that for any $i \in [0 : d]$,

$$\left.\frac{\partial R(\vec{\delta})}{\partial \delta_i}\right|_{\vec{\delta}=\tilde{\vec{\delta}}} = 0 \implies \bar{\epsilon}\epsilon^i \log_2\left(\frac{1-\tilde{\delta}_i}{\tilde{\delta}_i}\right) \cdot D(\tilde{\vec{\delta}}) = d\bar{\epsilon}\epsilon^i \cdot N(\tilde{\vec{\delta}})$$
$$\implies \frac{N(\tilde{\vec{\delta}})}{D(\tilde{\vec{\delta}})} = \frac{1}{d}\log_2\left(\frac{1-\tilde{\delta}_i}{\tilde{\delta}_i}\right). \tag{8.3}$$

Therefore, from (8.3), we get that

$$\left.\frac{\partial R(\vec{\delta})}{\partial \delta_i}\right|_{\vec{\delta}=\tilde{\vec{\delta}}} = 0, \forall i \implies \tilde{\delta}_0 = \ldots = \tilde{\delta}_d.$$

Thus, when the maximum in (8.2) is attained at an interior point, we have that $\delta_0^* = \ldots = \delta_d^* = \delta^*$, thereby showing that in the first case, the feedback capacity

$$C_{(d,\infty)}^{\text{fb}}(\epsilon) = \max_{\delta \in [0, \frac{1}{d+1}]} \frac{h_b(\delta)}{d\delta + \frac{1}{1-\epsilon}}.$$

If the maximum is attained at a boundary point of Δ_{d+1}, we wish to show that it holds that $\sum_{i=0}^{d} \delta_i^* = 1$. To this end, we first the define the following non-linear optimization

problem with affine constraints:

$$\begin{aligned}
&\textbf{maximize } R(\delta_0, \ldots, \delta_d) \\
&\textbf{subj. to } g_0(\vec{\delta}) := -\delta_0 \leq 0, \ldots, g_d(\vec{\delta}) := -\delta_d \leq 0, \\
&\qquad \tilde{g}_0(\vec{\delta}) := \delta_0 - 1 \leq 0, \ldots, \tilde{g}_d(\vec{\delta}) := \delta_d - 1 \leq 0, \\
&\qquad\qquad \hat{g}(\vec{\delta}) := \delta_0 + \ldots + \delta_d - 1 \leq 0.
\end{aligned} \tag{8.4}$$

Note that the objective function in (8.4) and the constraint functions are all continuously differentiable in $[0,1]^{d+1}$ and the constraints are affine functions. Therefore, it holds from the necessity of the Karush-Kuhn-Tucker (KKT) conditions being satisfied, that there exist constants $\{\mu_i\}_{i=0}^{d}$, $\{\tilde{\mu}_i\}_{i=0}^{d}$, and $\hat{\mu}$, with $\mu_i, \tilde{\mu}_i \geq 0$, $\forall i$, and $\hat{\mu} \geq 0$, such that:

$$\nabla R(\vec{\delta})\Big|_{\vec{\delta}=\vec{\delta}^*} = \left(\sum_{i=0}^{d} \mu_i \nabla g_i(\vec{\delta}) + \sum_{i=0}^{d} \tilde{\mu}_i \nabla \tilde{g}_i(\vec{\delta}) + \hat{\mu} \nabla \hat{g}(\vec{\delta}) \right) \Bigg|_{\vec{\delta}=\vec{\delta}^*}. \tag{8.5}$$

Suppose that the maximum is attained at a boundary point with $\delta_j^* = 0$, for some $j \in [0:d]$. Following reasoning similar to that in Lemma 13 in Appendix A of [90], we note that since $\delta_j^* = 0$, we do not need to worry about the constraint that $\tilde{g}_j(\vec{\delta}) \leq 0$. Equation (8.5) then gives us:

$$\frac{\partial R(\vec{\delta})}{\partial \delta_j}\bigg|_{\delta_j=0} = -\mu_j + \hat{\mu}.$$

However, we note that

$$\frac{\partial R(\vec{\delta})}{\partial \delta_j} = \frac{\bar{\epsilon}\epsilon^j \log_2\left(\frac{1-\delta_j}{\delta_j}\right) \cdot D(\vec{\delta}) - d\bar{\epsilon}\epsilon^j \cdot N(\vec{\delta})}{\left(D(\vec{\delta})\right)^2},$$

which tends to $+\infty$ as $\delta_j \to 0^+$. Therefore, it must be that $\hat{\mu} = +\infty$.

Now, again, since the KKT conditions are necessary conditions for optimality in our

maximization problem, from the complementary slackness condition, we see that:

$$\hat{\mu}\hat{g}(\vec{\delta}^*) + \sum_{i=0}^{d} \mu_i g_i(\vec{\delta}^*) + \sum_{i=0}^{d} \tilde{\mu}_i \tilde{g}_i(\vec{\delta}^*) = 0. \tag{8.6}$$

Since $\hat{\mu} = +\infty$ when the maximum is attained at a boundary point, it follows from equation (8.6) that $\hat{g}(\vec{\delta}^*) = 0$, or, that $\sum_{i=0}^{d} \delta_i^* = 1$ when $\delta_j^* = 0$ for some j. □

Figure 8.4 shows plots of the feedback capacity for $d = 1, 2, 3$. Several comments are now in order. The feedback capacity is equal to the noiseless capacity at $\epsilon = 0$, and monotonically decreases to 0 at $\epsilon = 1$. As in [90], numerical evaluations indicate that the feedback capacity is a concave function of the channel parameter, ϵ. At $d = 0$, which corresponds to the case of the BEC with no constraints, $R(0.5)$ equals $1 - \epsilon$, which, in turn, equals the (feedback) capacity of the BEC with no input constraints. For $d = 1$, it is easy to see that our feedback capacity expression recovers the formula for feedback capacity derived in [88]. Indeed, for any ϵ, we have that:

$$C_{(1,\infty)}^{\text{fb}}(\epsilon) \geq \max_{\delta \in [0, \frac{1}{2}]} R(\delta, \delta) = \max_{\delta \in [0, \frac{1}{2}]} \frac{h_b(\delta)}{\delta + \frac{1}{1-\epsilon}} = C_{(1,\infty)}^{\text{nc}}(\epsilon),$$

where in the last equality, $C_{(1,\infty)}^{\text{nc}}(\epsilon)$ is the capacity with non-causal knowledge of erasures (or non-causal capacity), the expression for which was derived in [88]. However, once again, from operational considerations, the feedback capacity is less than or equal to the non-causal capacity, thereby showing that $C_{(1,\infty)}^{\text{fb}} = C_{(1,\infty)}^{\text{nc}}(\epsilon)$, which agrees with the main result of [88].

Similar reasoning leads us to the following corollary of Theorem 8.4.1 (stated as Corollary III.1 in [94]), for the case when $d = 2$:

Corollary 8.4.5. *For $d = 2$ and $\epsilon \in [0, 1 - \frac{1}{2\log_2(3/2)}]$, it holds that the feedback and non-causal capacities are equal, i.e.,*

$$C_{(2,\infty)}^{fb}(\epsilon) = C_{(2,\infty)}^{nc}(\epsilon) = \max_{\delta \in [0, \frac{1}{3}]} \frac{h_b(\delta)}{2\delta + \frac{1}{1-\epsilon}}.$$

Proof. We note, as before, that it suffices to show that for $\epsilon \in [0, 1 - \frac{1}{2\log_2(3/2)}]$, it holds that $C^{\text{fb}}_{(2,\infty)}(\epsilon) \geq C^{\text{nc}}_{(2,\infty)}(\epsilon)$.

From [90], we know that the non-causal capacity of the (d, ∞)-RLL input-constrained BEC is given by:

$$C^{\text{nc}}_{(d,\infty)}(\epsilon) = \max_{\delta \in [0, \frac{1}{2}]} V(\delta),$$

where $V(\delta) = \frac{h_b(\delta)}{d\delta + \frac{1}{1-\epsilon}}$. We note that the derivative, $V'(\cdot)$, is given by

$$V'(\delta) = \frac{(\kappa + d)\log(1-\delta) - \kappa \log \delta}{(\kappa + d\delta)^2},$$

where we write $\frac{1}{1-\epsilon}$ as κ. It can be checked that $V'(\delta)$ is strictly decreasing in δ. Now, when $d = 2$, it is true that $V'\left(\frac{1}{3}\right) \leq 0$ if, and only if, $\kappa \leq \frac{2\log(1+1/2)}{\log 2}$, or, equivalently, if, and only if, $\epsilon \leq 1 - \frac{1}{2\log(\frac{3}{2})}$. Since $V'(0^+) > 0$, we have that for $\epsilon \leq 1 - \frac{1}{2\log(\frac{3}{2})}$, the unique maximum of $V(\cdot)$, over $[0, 1]$, occurs in the interval $[0, \frac{1}{3}]$. Hence, for $\epsilon \in [0, 1 - \frac{1}{2\log_2(3/2)}]$, we have that

$$C^{\text{nc}}_{(d,\infty)}(\epsilon) = \max_{\delta \in [0, \frac{1}{3}]} V(\delta).$$

Furthermore, from Theorem 8.4.1, we get that

$$C^{\text{fb}}_{(2,\infty)}(\epsilon) \geq \max_{\delta \in [0, \frac{1}{3}]} R(\delta, \delta, \delta) = \max_{\delta \in [0, \frac{1}{3}]} V(\delta) = C^{\text{nc}}_{(2,\infty)}(\epsilon).$$

□

We note from the observations in [90] that this equality of feedback and non-causal capacities is not true for general d.

Figures 8.5a and 8.5b show comparisons of the feedback capacities for $d = 1$ and $d = 2$, respectively, with dual capacity-based upper bounds on the capacities without feedback, derived in [28]. Clearly, the capacity without feedback is less than the feedback capacity, for this class of channels.

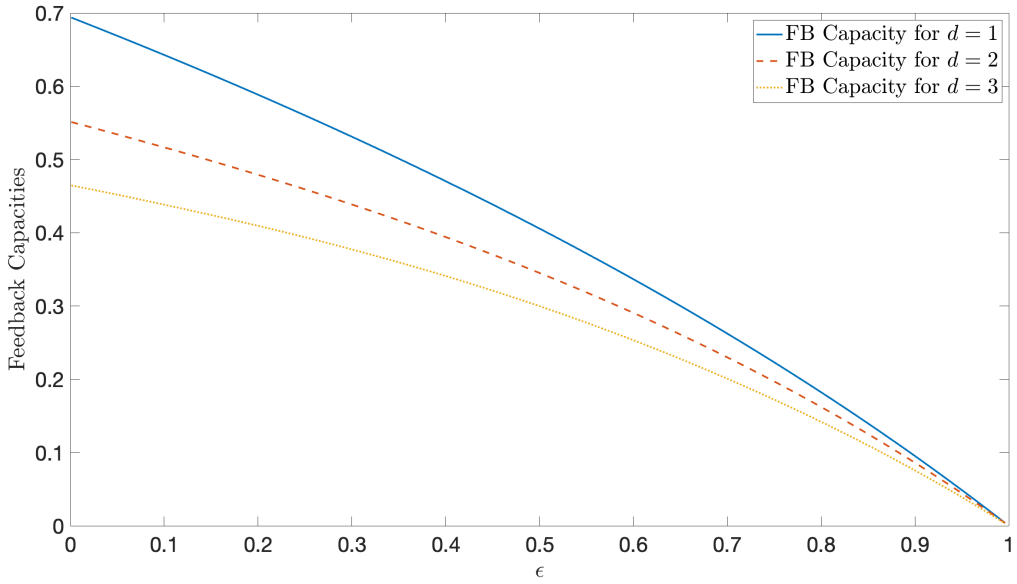


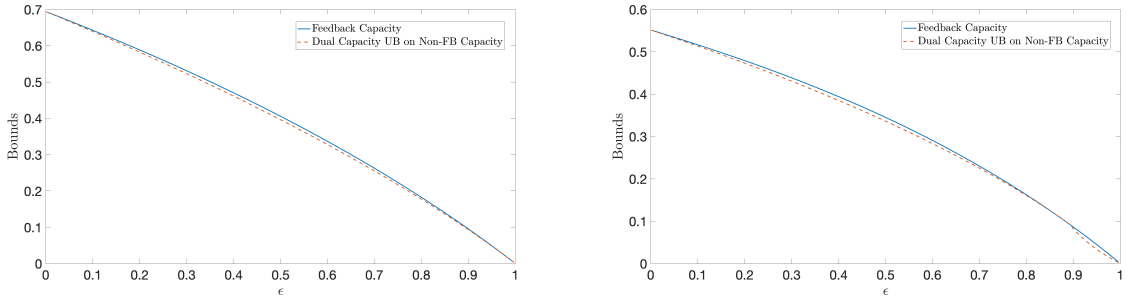
Figure 8.4: Plots of the feedback capacities for $d = 1, 2, 3$.

8.5 Optimal Feedback Coding Scheme

This section presents a simple feedback coding scheme that achieves the lower bound in Theorem 8.4.1. Our labelling-based coding scheme is similar to the coding schemes in [88] and [90]. The main feature of the scheme is a dynamically-changing set of possible messages that is known to both the encoder and the decoder at all times. The objective of the encoder is to communicate a sequence of bits that will enable the decoder to narrow down the set of possible messages to a single message.

Each message $m \in [2^{nR}]$ is mapped uniformly to a point in the unit interval, i.e., the message m is mapped to the point $\frac{m-1}{2^{nR}}$. At each time instant i, the unit interval is partitioned into sub-intervals that are labelled by either a '0' or a '1'. The input x_i to the channel is determined using the label of the sub-interval containing the message.

The coding scheme proceeds as follows: we first fix positive $\delta_0, \delta_1, \ldots, \delta_d$ such that $\sum_i \delta_i \leq 1$. To determine the input bits to be sent, we use a set of $d+2$ labellings, $\mathcal{L}_0, \ldots, \mathcal{L}_d, \hat{\mathcal{L}}$, with the interval $[\sum_{j<i} \delta_j, \sum_{j \leq i} \delta_j)$, in $\mathcal{L}_i$, labelled by a '1'. Further, labelling $\hat{\mathcal{L}}$ is such that the entire interval $[0, 1)$ is labelled by a '0'. Figure 8.6 shows an illustration of the set of labellings.



(a) (b)

Figure 8.5: Plots (a) and (b) show comparisons of the feedback capacities of the $(1,\infty)$- and $(2,\infty)$-RLL input-constrained BEC with dual capacity-based upper bounds on the capacity without feedback, from [28].

The labelling to be used at any time instant is a function of the channel outputs upto that time instant and can be recursively computed using the previous labelling and previous $d+1$ channel outputs. Thus, both the encoder and the decoder can compute the labelling used at all times. Let L_i denote the labelling used at time i. We fix $L_0 := \mathcal{L}_0$. Then, $L_{i+1} = G(L_i, Y_{i-d}^i)$, where the function G is defined as follows:

$$G(L_i, Y_{i-d}^i) = \begin{cases} \hat{\mathcal{L}}, & \text{if one of } Y_{i-d+1}^i \text{ is a 1,} \\ \mathcal{L}_0, & \text{if } Y_{i-d} = 1, \\ \mathcal{L}_0, & \text{if } Y_i = 0, \text{ and none of } Y_{i-d+1}^i \text{ is a 1,} \\ \mathcal{L}_{j+1 \bmod (d+1)}, & \text{if } L_i = \mathcal{L}_j,\ Y_i = ?, \text{ and none of } Y_{i-d+1}^i \text{ is a 1.} \end{cases}$$

The transitions between the labellings can be represented by the finite state machine (FSM) shown in Figure 8.7. The labellings in conjunction with the message are used to determine the bit X_{i+1} to be transmitted. Formally, $X_{i+1} = \Gamma(m, L_{i+1})$, where the function Γ is defined as:

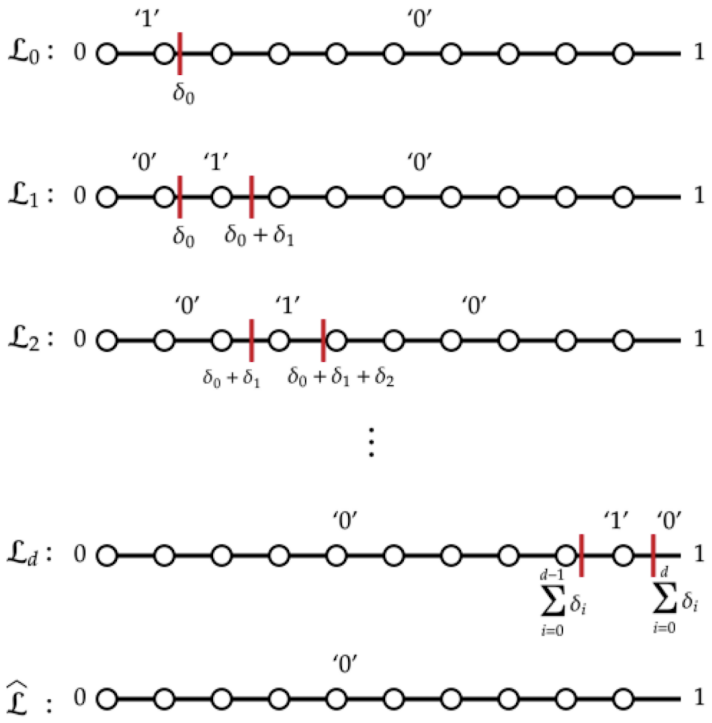


Figure 8.6: The set of labellings, $\mathcal{L}_0, \ldots, \mathcal{L}_d$, used in the coding scheme.

$$\Gamma(m, L_{i+1}) = \begin{cases} 0, \text{ if } L_{i+1} = \mathcal{L}_j, \text{ for some } j, \text{ and } \frac{m-1}{2^{nR}} \notin [\sum_{z<j}\delta_z, \sum_{z\leq j}\delta_z), \\ 0, \text{ if } L_{i+1} = \hat{\mathcal{L}}, \\ 1, \text{ if } L_{i+1} = \mathcal{L}_j, \text{ for some } j, \text{ and } \frac{m-1}{2^{nR}} \in [\sum_{z<j}\delta_z, \sum_{z\leq j}\delta_z). \end{cases}$$

The chronological order of a single use of the channel at time i, for a fixed message m, thus is $L_i \to X_i \to Y_i$, with $L_{i+1} = G(L_i, Y_{i-d}^i)$.

For a given output sequence y^i, we denote by $\mathcal{M}_i$ the set of *possible messages* after time i, i.e., $\mathcal{M}_i := \{m \in [2^{nR}] : P(m|y^i) > 0\}$, with $\mathcal{M}_0 := [2^{nR}]$. Note that both the encoder and the decoder can compute the conditional distribution $P(m|y^i)$ using Bayes' rule. We use the notation $\mathcal{M}_i^{(0)}$ and $\mathcal{M}_i^{(1)}$ to denote the set of messages labelled by a '0' and by a '1', respectively, in $\mathcal{M}_i$.

A transmission at time i is said to be *successful* if $|\mathcal{M}_i| < |\mathcal{M}_{i-1}|$. Specifically, a

Algorithm 3 Coding Scheme

procedure CODE(m)
  Set $\mathcal{M}_0 = [2^{nR}]$ and $Y_{-d}^0 = (0, \ldots, 0)$.
  Set Label = $\mathcal{L}_0$.
  Set time index $i = 1$.
  while $|\mathcal{M}_{i-1}| > 1$ **do**
    Transmit $X_i = \Gamma(m, \text{Label})$. ▷ Encoder
    if none of Y_{i-d-1}^{i-1} is a 1 **then**
      if $Y_i = 0$ **then**
        Set $\mathcal{M}_i = \mathcal{M}_{i-1}^{(0)}$.
      else if $Y_i = 1$ **then**
        Set $\mathcal{M}_i = \mathcal{M}_{i-1}^{(1)}$.
      else
        Set $\mathcal{M}_i = \mathcal{M}_{i-1}$.
    else
      Set $\mathcal{M}_i = \mathcal{M}_{i-1}$.
    Label $\leftarrow G(\text{Label}, Y_{i-d}^i)$.
    Update $i = i + 1$.
  Output $\hat{m}$, where $\mathcal{M}_{i-1} = \{\hat{m}\}$. ▷ Decoder

successful transmission can occur in one of two scenarios: the first is $y_i = 1$, and the second is where $y_i = 0$ and none of y_{i-d}^{i-1} is a 1. After a successful transmission, the set of possible messages is calculated and expanded uniformly to the unit interval. It is easy to see that in the first kind of successful transmission, the new set of possible messages, $\mathcal{M}_i$, is equal to $\mathcal{M}_{i-1}^{(1)}$, and in the second kind, $\mathcal{M}_i$ equals $\mathcal{M}_{i-1}^{(0)}$. Figure 8.8 shows an illustration of the second of the two kinds of successful transmissions. Figure 8.9 depicts the situation when a sequence of erasures is received. In this case, the new set of possible messages, $\mathcal{M}_i$, is equal to $\mathcal{M}_{i-1}$. This transmission procedure continues repeatedly until the set of possible messages contains one message. Additionally, we

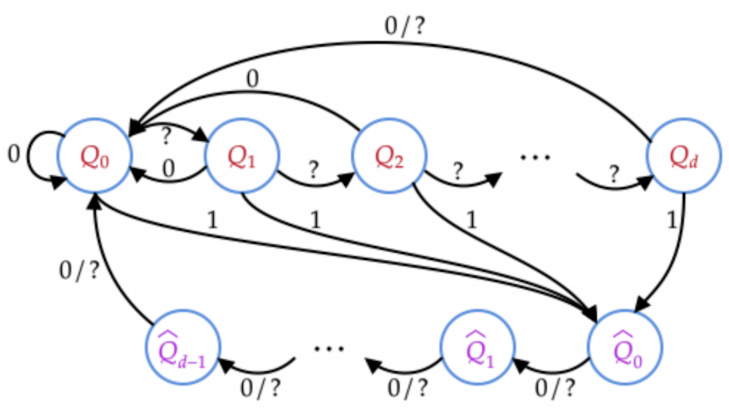


Figure 8.7: Figure shows the finite-state machine (FSM) that represents transitions between the labellings, with the edges labelled by outputs. When the encoder is in state Q_i, for $i \in \{0, 1, \ldots, d\}$, the labelling used is $\mathcal{L}_i$, and when the encoder is in state $\hat{Q}_i$, for $i \in \{0, 1, \ldots, d-1\}$, the labelling used is $\hat{\mathcal{L}}$. The edges labelled by $0/?$ should be viewed as two edges merged into one.

note that the coding scheme is zero-error, since at the end of the algorithm, the decoder can uniquely decode the transmitted message. The encoding and decoding procedures are described in Algorithm 3.

The construction of the labellings ensures that the (d, ∞)-RLL input constraint is obeyed. This can be seen from the fact that if ever $Y_i = 1$ for some i, then the next d inputs are all set to be 0s. Further, the staggered manner in which the sub-intervals are labelled by a 1 in the labellings $\mathcal{L}_0, \ldots, \mathcal{L}_d$ ensures that the input constraint is satisfied when a sequence of erasures is received, too.

The analysis of the rate of the feedback coding scheme is similar to the proofs of Lemma 3 and Lemma 4 in [90]. In order to make the exposition self-contained, we repeat parts of the proofs here. For a time index $i \in [n]$, we define J_i to be the number of information bits gained in a single channel use, which is the logarithm of the change in the size of possible messages at the end of the channel use, i.e.,

$$\mathsf{J}_i := \log_2 |\mathcal{M}_{i-1}| - \log_2 |\mathcal{M}_i|. \tag{8.7}$$

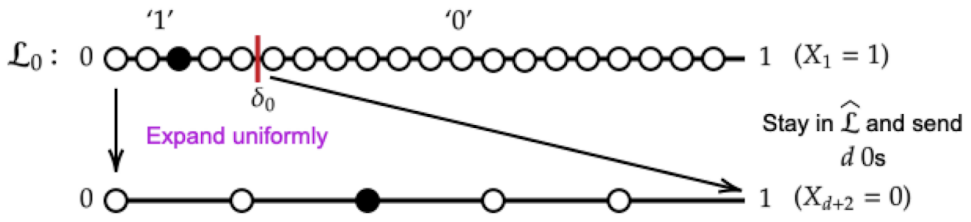


Figure 8.8: Figure shows an illustration of a successful transmission of the second kind, when $X_1 = Y_1 = 1$, and when the encoder then transmits d additional zeros. Note that the size of the set of possible messages reduces.

and L_i to denote the random variable corresponding to the labelling used, with $\mathsf{L}_i \in \mathcal{L} := \{\hat{\mathcal{L}}, \mathcal{L}_0, \ldots, \mathcal{L}_d\}$. The following lemma then holds true:

Lemma 8.5.1. *For any time $i \in [n]$, and for all $\ell \in \mathcal{L}$, we have that $\mathbb{E}[\mathsf{J}_i|\mathsf{L}_i = \ell] = \bar{\epsilon} h_b(\delta_\ell)$, where*

$$\delta_\ell = \begin{cases} 0, \text{ if } \ell = \hat{\mathcal{L}}, \\ \delta_j, \text{ if } \ell = \mathcal{L}_j. \end{cases}$$

Proof. We let the random variable θ denote the indicator that the current output is unerased, i.e.,

$$\theta_i = \mathbb{1}\{Y_i \neq \text{'?'}\}.$$

Then,

$$\begin{aligned} \mathbb{E}[\mathsf{J}_i|\mathsf{L}_i = \ell] &= \epsilon \mathbb{E}[\mathsf{J}_i|\mathsf{L}_i = \ell, \theta_i = 0] + \bar{\epsilon}\mathbb{E}[\mathsf{J}_i|\mathsf{L}_i = \ell, \theta_i = 1] \\ &= \bar{\epsilon}\mathbb{E}[\mathsf{J}_i|\mathsf{L}_i = \ell, \theta_i = 1], \end{aligned} \tag{8.8}$$

where the second equality holds since if an erasure is received, the set of possible messages remains the same.

We now note that in any of the labellings $\mathcal{L}_j$, it holds that the length of the subinterval labelled by a '1' equals δ_j, and equals 0 in $\hat{\mathcal{L}}$. Hence, if labelling $\ell \in \mathcal{L}$ is employed, the bit transmitted is distributed according to $\text{Ber}(\delta_\ell)$ (see the remark immediately after this proof), where δ_ℓ is as defined in the statement of the theorem.

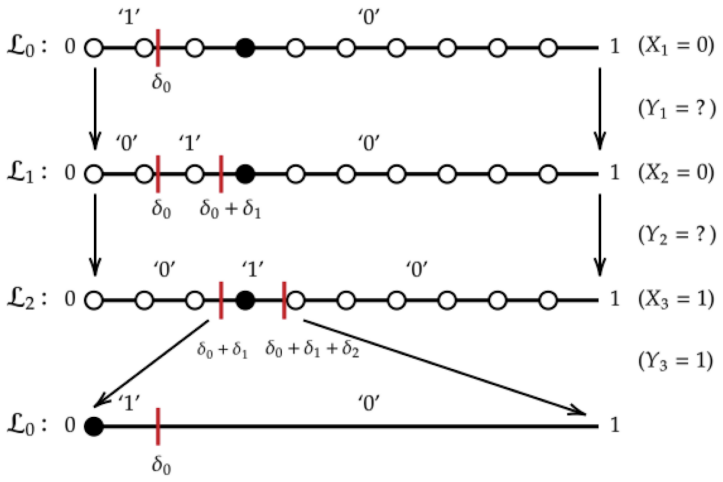


Figure 8.9: The figure shows the setting when two consecutive erasures are received ($Y_1 = Y_2 = ?$), followed by the successful reception of $X_3 = 1$. So long as erasures are received, the set of possible messages is retained as such, while the labellings cycle through $\mathcal{L}_0$ to $\mathcal{L}_d$. Upon the successful reception of X_3, and after the transmission of d 0s, the labelling is changed to $\mathcal{L}_0$. However, since the set of possible messages is now a singleton, the transmission ends with the decoder declaring the correct identity of the message.

Assume that the current size of the set of possible messages, $\mathcal{M}$, equals k, with the current labelling used being ℓ. If the current bit transmitted is received successfully, then, the new set of possible messages has size $k\delta_\ell$, if the current input bit is a '1', and is equal to $k\bar{\delta}_\ell$, otherwise. Hence, the expected number of bits required to describe the new set of possible messages is $\bar{\delta}_\ell k \log_2(\bar{\delta}_\ell k) + \delta_\ell k \log_2(\delta_\ell k) = \log_2(k) - h_b(\delta_\ell)$. Thus, given that $\mathsf{L} = \ell$, following a successful transmission, the decoder gains $h_b(\delta_\ell)$ bits of information. Substituting into (8.8), we get that

$$\mathbb{E}[\mathsf{J}|\mathsf{L} = \ell] = \bar{\epsilon} h_b(\delta_\ell).$$

□

Remark 8.5.2. *We note as in [90] that since the messages are discrete points in* $[0,1)$*, the transmitted bit is actually distributed according to* $Ber(\delta_\ell - e_i)$*, where* e_i *is a correction factor*

that is bounded as $0 \leq e_i \leq \frac{1}{|\mathcal{M}_{i-1}|}$. *We use Algorithm 3 for encoding, until a time t such that* $|\mathcal{M}_t| \leq 2^{\lambda}$, *for an absolute constant,* $\lambda > 0$. *A clean-up coding phase can then be employed, after the labelling-based scheme, similar to [88, Appendix C], using which the remaining at most* λ *bits are then transmitted. The rate of the overall two-stage coding scheme can then be made arbitrarily close to the rate calculated using the analysis in this paper.*

The following lemma computes the rate of the proposed coding scheme:

Lemma 8.5.3. *For any* $\epsilon \in [0, 1]$, *the proposed coding scheme achieves a rate*

$$R = \max_{\vec{\delta} \in \Delta_{d+1}} R(\vec{\delta}),$$

where $R(\vec{\delta})$ *is as defined in equation* (8.1).

Proof. Fix $0 \leq \delta_0, \delta_1, \ldots, \delta_d \leq 1$, with $\sum_{i=0}^{d} \delta_i \leq 1$. The constraint is chosen so as to ensure that the lengths of the intervals used in the labellings in Figure 8.6 are all non-negative.

Consider the Markov chain induced by the transitions shown in Figure 8.7, with the transition probabilities $P(Y = ?|q) = \epsilon$, for all $q \in \{Q_0, Q_1, \ldots, Q_d, \hat{Q}_0, \hat{Q}_1, \ldots, \hat{Q}_{d-1}\}$, and

$$P(Y = 1|q) = \begin{cases} \bar{\epsilon}\delta_i, \text{ if } q = Q_i, \text{ for some } i, \\ 0, \text{ otherwise.} \end{cases}$$

Let $\pi(\ell)$ denote the stationary probability of using labelling ℓ, which can be calculated using the stationary probabilities of states of the Markov chain on the FSM. Clearly, for $i \in \{0, 1, \ldots, d\}$, $\pi(\mathcal{L}_i)$ equals $\pi(Q_i)$, and $\pi(\hat{\mathcal{L}})$ equals $\sum_{j=0}^{d-1} \pi(\hat{Q}_j)$. The rate of the

coding scheme can be computed to be:

$$\begin{aligned}
R &= \lim_{n\to\infty} \frac{\log_2 |\mathcal{M}_0|}{n} \\
&\overset{(a)}{=} \lim_{n\to\infty} \frac{1}{n} \sum_{k=1}^{n} \mathbb{E}[\mathsf{J}_k] \\
&= \lim_{n\to\infty} \frac{1}{n} \sum_{k=1}^{n} \sum_{\ell\in\mathcal{L}} P(\mathsf{L}_k = \ell)\mathbb{E}[\mathsf{J}_k|\mathsf{L}_k = \ell] \\
&\overset{(b)}{=} \sum_{\ell\in\mathcal{L}} \bar{\epsilon} h_b(\delta_\ell) \lim_{n\to\infty} \frac{1}{n} \sum_{k=1}^{n} P(\mathsf{L}_k = \ell) \\
&\overset{(c)}{=} \sum_{\ell\in\mathcal{L}} \bar{\epsilon} h_b(\delta_\ell)\pi(\ell) \\
&= \sum_{i=0}^{d} \bar{\epsilon} h_b(\delta_i)\pi(\mathcal{L}_i) \overset{(d)}{=} R(\vec{\delta}),
\end{aligned}$$

where

(a) holds from equation (8.7),

(b) follows from Lemma 8.5.1 and by exchanging the order of the summations,

(c) follows from the definition of stationary probability and from the fact that the random process $(\mathsf{L}_n : n \in \mathbb{N})$ is a positive recurrent, irreducible, aperiodic Markov chain (this follows from the irreducibility and aperiodicity of the graph in Figure 8.7), and

(d) holds by an explicit calculation of the stationary probabilities of the Markov process $(\mathsf{L}_n : n \in \mathbb{N})$, which are given by:

$$\pi(\ell) = \begin{cases} \frac{\epsilon^i}{\sum_{j=0}^{d} \epsilon^j + d\bar{\epsilon}\left(\sum_{j=0}^{d} \epsilon^j \delta_j\right)}, & \ell = \mathcal{L}_i, \\ \frac{d\bar{\epsilon}\left(\sum_{j=0}^{d} \epsilon^j \delta_j\right)}{\sum_{j=0}^{d} \epsilon^j + d\bar{\epsilon}\left(\sum_{j=0}^{d} \epsilon^j \delta_j\right)}, & \ell = \hat{\mathcal{L}}. \end{cases}$$

Therefore, maximizing over all allowed parameters $\delta_0, \ldots, \delta_d$, it follows that our coding scheme achieves a rate $R = \max_{\vec{\delta}\in\Delta_{d+1}} R(\vec{\delta})$. □

We now provide an upper bound on the feedback capacity of the (d,∞)-RLL input-constrained BEC, using Theorem 8.3.1.

Lemma 8.5.4. *For any $\epsilon \in [0,1]$, the feedback capacity of the (d,∞)-RLL input-constrained BEC is bounded as:*

$$C^{fb}_{(d,\infty)}(\epsilon) \leq \max_{\vec{\delta}\in\Delta_{d+1}} R(\vec{\delta}).$$

Proof. We simply apply Theorem 8.3.1 to the Q-graph that is the FSM in Figure 8.7. The transition probabilities $P(Y=y|q)$ are the same as those in the proof of Lemma 8.5.3, for $y \in \{0,?,1\}$ and $q \in \{Q_0, Q_1, \ldots, Q_d, \hat{Q}_0, \hat{Q}_1, \ldots, \hat{Q}_{d-1}\}$. Note that the definition of the transition probabilities implies that

$$P(X=1|q) = \begin{cases} \delta_i, \text{ if } q = Q_i, \text{ for some } i, \\ 0, \text{ otherwise.} \end{cases}$$

We then have that

$$\begin{aligned} I(X;Y|Q) &\overset{(a)}{=} H(Y|Q) - H(Y|X) \\ &= H(Y|Q) - h_b(\epsilon) \\ &\overset{(b)}{=} \bar{\epsilon}H(X|Q) + h_b(\epsilon) - h_b(\epsilon) \\ &= \sum_{\ell\in\mathcal{L}} \bar{\epsilon}h_b(\delta_\ell)\pi(\ell) = \sum_{i=0}^{d} \bar{\epsilon}h_b(\delta_i)\pi(\mathcal{L}_i) = R(\vec{\delta}), \end{aligned}$$

where

(a) holds due to the memorylessness of the BEC, and

(b) follows from the simple identity that $H(a\bar{c},\bar{a}\bar{c},c) = h_b(c) + \bar{c}h_b(a)$, for all $a,c \in [0,1]$.

Hence, all that remains to be shown for the proof to be complete is that

$$\sup_{\{P(x|s,q)\}} R(\vec{\delta}) = \max_{\sum_{i=0}^{d}\delta_i \leq 1} R(\vec{\delta}).$$

This is true since for any valid input distribution $\{P(x|s,q)\}$ on the (S,Q)-graph corresponding to the Q-graph in Figure 8.7, we have

$$\sum_{i=0}^{d} \delta_i = \sum_{i=0}^{d} P(X=1|Q_i) = \sum_{i=0}^{d} \frac{P(X=1,Q_i)}{\pi(\mathcal{L}_i)}$$
$$= \sum_{i=0}^{d} \frac{P(X=1,Q_i)}{\epsilon^i \pi(\mathcal{L}_0)} = \frac{1}{\pi(\mathcal{L}_d)} \sum_{i=0}^{d} \epsilon^{d-i} P(X=1,Q_i).$$

Now,

$$\begin{aligned}
\sum_{i=0}^{d} \delta_i &= \frac{1}{\pi(\mathcal{L}_d)} \sum_{i=0}^{d} \epsilon^{d-i} P(X=1,Q_i) \\
&= \frac{1}{\pi(\mathcal{L}_d)} \sum_{i=0}^{d} \epsilon^{d-i} P(X=1,S=d,Q_i) \\
&\leq \frac{1}{\pi(\mathcal{L}_d)} \left(\sum_{i=0}^{d-1} \epsilon^{d-i} P(X=1,S=d,Q_i) + P(S=d,Q_d) \right) \\
&= \frac{1}{\pi(\mathcal{L}_d)} \left(\sum_{i=0}^{d-1} P(S=i,Q_d) + P(S=d,Q_d) \right) = 1,
\end{aligned}$$

where the penultimate equality holds from the structure of the (S,Q)-graph. □

Remark 8.5.5. *We note that for the case when $d = 2$, the authors in [90] provide the optimal Q-graph of Figure 8.7 for evaluating an upper bound on the feedback capacity. We have shown here that their upper bound is tight.*

Lemmas 8.5.3 and 8.5.4, taken together, prove Theorem 8.4.1. We thus obtain an exact characterization of the feedback capacity, in addition to providing an explicit coding scheme.

8.6 Conclusions and Directions for Future Work

In this chapter, we proposed explicit, deterministic coding schemes for the binary erasure channel (BEC) with a (d,∞)-runlength limited (RLL) input constraint with feedback. In particular, a zero-error, labelling-based feedback capacity-achieving coding

scheme was demonstrated, thereby allowing for the exact computation of the feedback capacity of the class of channels under consideration—a problem that was left open. This allowed us to obtain upper bounds, via the feedback capacity, on the non-feedback capacity of such input-constrained channels. It was also shown that for this class of channels, for at least selected values of d, feedback indeed increases the capacity.

An important open question in the setting with causal, noiseless feedback is whether the feedback capacity of general input-constrained DMCs is achievable using input distributions of finite output memory. This question can also be asked of other unifilar FSCs. For the $(0, k)$- and (d, ∞)-RLL BECs, we know (from our work and from [90]) that there exists an optimal input distribution that depends only on finitely-many past outputs. However, there does exist a unifilar FSC, the so-called chemical channel, for which it was observed [87] that for a range of channel parameters, under the (numerically calculated) optimal input distribution, in the steady-state, there are infinitely-many states of the dynamic programming problem associated with feedback capacity computation. This indicates (see [85] for more on the DP formulation) that the optimal input distribution in this case depends on infinitely-many past outputs. It is of interest, hence, to characterize the classes of input constraints for which optimal input distributions of finite memory exist. As a first step, one could try to extend the coding schemes in the literature (including the one presented in this paper) to the BEC with a (d, k)-RLL input constraint, for $d \neq 0$ and $k \neq \infty$.

Another interesting question is the study of the delayed feedback capacities of input-constrained DMCs. The work in [81] provided a DP formulation of the problem of delayed feedback capacity computation, and also discussed some numerical results. Clearly, since the delayed feedback capacity $C^{\mathrm{fb},\Delta}$, where the output feedback is delayed by $\Delta > 1$ time steps, is an upper bound on the non-feedback capacity, such an approach can lead us to non-trivial upper bounds on the non-feedback capacity C. A recent work [95], for example, has explicitly derived the delayed feedback capacity of the trapdoor channel when the delay $\Delta = 2$. Moreover, [81] contains the assertion

that the feedback capacities $C^{\mathrm{fb},\Delta}$ converge to C in the limit as the delay Δ tends to infinity—a fact for which a rigorous proof was not provided. While one can artificially construct FSCs such that $C^{\mathrm{fb},\Delta} > C$, for any $\Delta > 1$, it is of broad interest to characterize the classes of channels for which such a convergence holds (we attempted a proof of this for the $(1,\infty)$-RLL input-constrained BEC, without much success).

Chapter 9

A Version of Delsarte's Linear Program for Constrained Systems

There is, one knows not what sweet mystery about this sea, whose gently awful stirrings seem to speak of some hidden soul beneath...

Herman Melville, Moby Dick; or, The Whale, 1851

9.1 Introduction

Chapters 4–8 were concerned with the computation of the capacities of and the design of coding schemes for stochastic noise channels (see Chapter 3), with input constraints. In this final chapter of the thesis, we focus on the channel model of the input-constrained adversarial channel, introduced in Chapter 3. In particular, our interest is in adversarial symmetric bit-flip error or erasure channels, where there is an upper bound on the number of errors or erasures that can be introduced. Recall that our objective is to recover the transmitted constrained codeword with zero error.

Recall also the well-known coding-theoretic fact (see, for example, [57]) that the minimum Hamming distance (or simply, minimum distance) of a (constrained) code determines the number of such adversarial errors or erasures that it can, with certainty, tolerate, with zero decoding error. In particular, a (constrained) code $\mathcal{C}$ can correct *all*

patterns of e erasures if and only if $e \leq d(\mathcal{C}) - 1$, where $d(\mathcal{C})$ is the minimum distance of $\mathcal{C}$. Likewise, a (constrained) code $\mathcal{C}$ can correct *all* patterns of e bit-flip errors if and only if $e \leq \left\lfloor \frac{d(\mathcal{C})-1}{2} \right\rfloor$. Hence, in this chapter, we seek to obtain good bounds on the sizes of constrained codes with a prescribed minimum distance.

9.2 Brief Literature Survey and Our Approach

There is extensive literature on the construction of and bounds for constrained codes with a certain minimum distance, and we refer the reader to Chapter 9 of [2] for references. In particular, [96] provided a simple lower bound on the sizes of runlength-limited (RLL) constrained codes with a given minimum Hamming distance, by a coset-averaging argument for linear codes. These bounds were then improved upon by Kolesnik and Krachkovsky [98] and Marcus and Roth [99], via the solutions to certain constrained optimization problems. Less was known in the case of upper bounds on constrained codes with a given minimum distance, until the works of Cullina and Kiyavash [100] (see also [101]) and Fazeli, Vardy, and Yaakobi [102], which provided a generalization of the well-known sphere packing bound for codes, to the setting of constrained codes[1]. The approach in [100] and [102] was based on finding the size of the largest matching, or equivalently, the size of the smallest transversal, in a suitably defined hypergraph.

In this chapter, we provide a different approach to deriving good upper bounds on the sizes of constrained codes with a given minimum Hamming distance, by modifying Delsarte's well-known linear program (LP) [103] to the setting of constrained systems. While on a first pass, we propose an LP whose number of variables is exponential in the blocklength of the code, we show that for certain constraints, it is

[1]While these papers were focused on obtaining bounds on the sizes of codes for combinatorial error models, their techniques can be easily applied to determining upper bounds on the sizes of constrained codes with a given minimum distance as well.

possible to "symmetrize" this LP to derive an equivalent LP with much smaller numbers of variables and constraints, which are sometimes only polynomial functions of the blocklength. We use our LPs to numerically calculate upper bounds on the sizes of the largest constrained codes with a prescribed minimum distance, for different constraints, and show that the values we obtain by our approach beat those obtained via the generalized sphere packing bounds.

9.3 Preliminaries

We refer the reader to Sections 5.4 and 7.3 for details on block codes and constrained codes. For this chapter, we also recall the following definition:

Definition 10. *The minimum distance $d(\mathcal{C})$ of a block code $\mathcal{C}$ is the minimum Hamming distance between any two distinct codewords of $\mathcal{C}$, i.e.,*

$$d(\mathcal{C}) = \min_{\mathbf{c}_1, \mathbf{c}_2 \in \mathcal{C}:\ \mathbf{c}_1 \neq \mathbf{c}_2} d(\mathbf{c}_1, \mathbf{c}_2).$$

An (n, M) block code with minimum distance d is called an (n, M, d) block code.

As in Chapter 7, we shall be concerned with constrained binary words that lie in a certain set $\mathcal{A} \subseteq \{0,1\}^n$. Here, too, we make no further assumption about the constrained system (such as it being finite-type, almost-finite-type, irreducible, etc.). For a given blocklength n, we use the notation $A(n, d; \mathcal{A})$ to denote the size of the largest constrained code, of minimum distance at least d, such that all of its codewords lie in $\mathcal{A}$. More formally,

$$A(n, d; \mathcal{A}) := \max_{\mathcal{C} \subseteq \mathcal{A}:\ d(\mathcal{C}) \geq d} |\mathcal{C}|.$$

For the case where $\mathcal{A} = \{0,1\}^n$, we write $A(n, d; \mathcal{A})$ as simply $A(n, d)$.

We also refer the reader to Section 7.3.3 for background on the Fourier transforms of real-valued functions on the Boolean hypercube. For this chapter, we will also require

the operation of convolution of two functions $f, g : \{0,1\}^n \to \mathbb{R}$, defined as

$$f \star g(\mathbf{x}) = \frac{1}{2^n} \sum_{\mathbf{z} \in \{0,1\}^n} f(\mathbf{z}) \cdot g(\mathbf{x} + \mathbf{z}),$$

where the '$+$' operation in $\mathbf{x} + \mathbf{z}$ above is over vectors in $\mathbb{F}_2^n$. It is well-known (see [70]) that the Fourier transform $\widehat{f \star g}(\mathbf{s}) = \widehat{f}(\mathbf{s}) \cdot \widehat{g}(\mathbf{s})$, for any $\mathbf{s} \in \{0,1\}^n$.

9.4 Our Linear Program for Constrained Systems

In this section, we consider the problem of upper bounding the sizes of constrained codes with a prescribed minimum distance. In particular, we present a linear program (LP) to upper bound $A(n, d; \mathcal{A})$, for any $\mathcal{A} \subseteq \{0,1\}^n$. This LP is based on Delsarte's linear programming approach [103] to bounding from above the value of $A(n, d)$, for $n \geq 1$ and $1 \leq d \leq n$. We first recall Delsarte's LP[2], which we call $\mathsf{Del}(n, d)$. Given an LP L, we denote by $\mathrm{OPT}(\mathsf{L})$ its optimal value, and for any feasible solution f of L, we denote the value of the objective function of L evaluated at f as $\mathrm{val}_{\mathsf{L}}(f)$. The subscript will be omitted when the LP being referred to is clear from the context. We remark here that the LPs in this paper can return non-integral optimal values, and that integer upper bounds on the sizes of codes can be obtained by suitable rounding of real numbers. The LP $\mathsf{Del}(n, d)$ is given below:

[2]The version of Delsarte's LP that is most often used in papers in coding theory, such as in [104], is obtained after symmetrizing $\mathsf{Del}(n, d)$. In particular, the common version of Delsarte's LP is $\mathsf{Del}_{/S_n}(n, d)$ (see the remark following Theorem 9.5.3), where S_n is the symmetry group on n elements.

Del(n, d)

$$\underset{f\colon \{0,1\}^n \to \mathbb{R}}{\text{maximize}} \quad \sum_{\mathbf{x}\in\{0,1\}^n} f(\mathbf{x}) \tag{Obj}$$

subject to:

$$f(\mathbf{x}) \geq 0, \ \forall\, \mathbf{x} \in \{0,1\}^n, \tag{C1}$$

$$\widehat{f}(\mathbf{s}) \geq 0, \ \forall\, \mathbf{s} \in \{0,1\}^n, \tag{C2}$$

$$f(\mathbf{x}) = 0, \text{ if } 1 \leq w(\mathbf{x}) \leq d-1, \tag{C3}$$

$$f(0^n) = 1. \tag{C4}$$

We then have the following well-known result (see, for example, Section 3 in [108]). We provide a complete proof, since the arguments within lead us to the construction of our LP for constrained systems.

Theorem 9.4.1. *The inequality $A(n,d) \leq \mathrm{OPT}(Del(n,d))$ holds.*

Proof. For any block code $\mathcal{C}$ of blocklength n and minimum distance at least d, let $\mathbb{1}_{\mathcal{C}}$ denote its indicator function. Let us define $f_{\mathcal{C}} := \frac{2^n}{|\mathcal{C}|}\mathbb{1}_{\mathcal{C}} \star \mathbb{1}_{\mathcal{C}}$. We claim that $f_{\mathcal{C}}$ is a feasible solution for Del(n,d), with $\mathrm{val}(f_{\mathcal{C}}) = |\mathcal{C}|$. Indeed, observe that (C1) is trivially satisfied, by the definition of the convolution operator. Further, since $\widehat{f_{\mathcal{C}}} = \frac{2^n}{|\mathcal{C}|} \cdot \widehat{\mathbb{1}_{\mathcal{C}}}^2$, (C2) is satisfied as well. Next, note that (C3) also holds since $\mathcal{C}$ is such that $d(\mathcal{C}) \geq d$, then $\mathbb{1}_{\mathcal{C}}(\mathbf{x}+\mathbf{z}) = 0$, for all $\mathbf{z} \in \mathcal{C}$ and any $\mathbf{x}$ such that $1 \leq w(\mathbf{x}) \leq d-1$. Finally,

$$\begin{aligned} f_{\mathcal{C}}(0^n) &= \frac{1}{|\mathcal{C}|} \sum_{\mathbf{z}\in\{0,1\}^n} \mathbb{1}_{\mathcal{C}}(\mathbf{z}) \cdot \mathbb{1}_{\mathcal{C}}(\mathbf{z}) \\ &= \frac{1}{|\mathcal{C}|} \sum_{\mathbf{z}\in\{0,1\}^n} \mathbb{1}_{\mathcal{C}}(\mathbf{z}) = 1, \end{aligned}$$

thereby satisfying (C4) also. Now, the objective value $\mathrm{val}(f_{\mathcal{C}})$ is given by

$$\begin{aligned}\sum_{\mathbf{x}\in\{0,1\}^n} f_{\mathcal{C}}(\mathbf{x}) &= \frac{1}{|\mathcal{C}|}\sum_{\mathbf{x}\in\{0,1\}^n}\sum_{\mathbf{z}\in\{0,1\}^n} \mathbb{1}_{\mathcal{C}}(\mathbf{z})\cdot\mathbb{1}_{\mathcal{C}}(\mathbf{x}+\mathbf{z}) \\ &= \frac{1}{|\mathcal{C}|}\sum_{\mathbf{z}\in\{0,1\}^n}\mathbb{1}_{\mathcal{C}}(\mathbf{z})\sum_{\mathbf{x}\in\{0,1\}^n}\mathbb{1}_{\mathcal{C}}(\mathbf{x}+\mathbf{z}) = |\mathcal{C}|. \end{aligned} \tag{9.1}$$

Hence, it follows that the optimal value of the LP, $\mathrm{OPT}(\mathsf{Del}(n,d)) \geq |\mathcal{C}|$, and since this holds for all block codes $\mathcal{C}$ of blocklength n and minimum distance at least d, we obtain the statement of the theorem. □

We refer the reader to [103–108] and the references therein for a more detailed treatment of linear programming-based upper bounds on the sizes of block codes and linear codes, and for the derivation of analytical upper bounds via the dual LP or using modern Fourier-theoretic or expander graph-based arguments.

Our LP, which we call $\mathsf{Del}(n,d;\mathcal{A})$, is but a small modification of $\mathsf{Del}(n,d)$, to take into account the fact that all codewords of the code of minimum distance at least d, whose size we are attempting to bound, must also lie in the set $\mathcal{A} \subseteq \mathbb{F}_2^n$. The LP $\mathsf{Del}(n,d;\mathcal{A})$ is:

$\mathsf{Del}(n, d; \mathcal{A})$

$$\underset{f\colon \{0,1\}^n \to \mathbb{R}}{\text{maximize}} \quad \sum_{\mathbf{x} \in \{0,1\}^n} f(\mathbf{x}) \tag{Obj'}$$

subject to:

$$f(\mathbf{x}) \geq 0, \ \forall\, \mathbf{x} \in \{0,1\}^n, \tag{D1}$$

$$\widehat{f}(\mathbf{s}) \geq 0, \ \forall\, \mathbf{s} \in \{0,1\}^n, \tag{D2}$$

$$f(\mathbf{x}) = 0, \text{ if } 1 \leq w(\mathbf{x}) \leq d-1, \tag{D3}$$

$$f(0^n) \leq \mathrm{OPT}(\mathsf{Del}(n, d)), \tag{D4}$$

$$f(\mathbf{x}) \leq 2^n \cdot (\mathbb{1}_{\mathcal{A}} \star \mathbb{1}_{\mathcal{A}})(\mathbf{x}), \ \forall\, \mathbf{x} \in \{0,1\}^n. \tag{D5}$$

Like in the case with $\mathsf{Del}(n, d)$, we have an upper bound on $A(n, d; \mathcal{A})$ via the optimal value of $\mathsf{Del}(n, d; \mathcal{A})$.

Theorem 9.4.2. *For any $\mathcal{A} \subseteq \{0,1\}^n$, we have $A(n, d; \mathcal{A}) \leq \mathrm{OPT}(\mathsf{Del}(n, d; \mathcal{A}))^{1/2}$.*

Proof. The proof is very similar to that of Theorem 9.4.1. Let $\mathcal{C}_{\mathcal{A}}$ be any length-n constrained code, with $d(\mathcal{C}_{\mathcal{A}}) \geq d$, such that all codewords in $\mathcal{C}_{\mathcal{A}}$ lie in $\mathcal{A}$. Observe that we can write $\mathcal{C}_{\mathcal{A}}$ as $\mathcal{C} \cap \mathcal{A}$, for some block (not necessarily constrained) code $\mathcal{C}$, with $d(\mathcal{C}) \geq d$. Thus, an upper bound on $\max\limits_{\mathcal{C}\colon d(\mathcal{C}) \geq d} |\mathcal{C} \cap \mathcal{A}|$ serves as an upper bound on (and in fact, equals) $A(n, d; \mathcal{A})$.

Let $\mathbb{1}_{\mathcal{C}}$ be the indicator function of a block code $\mathcal{C}$ as above, and let $\mathbb{1}_{\mathcal{A}}$ be the indicator function of the constraint. We define $f_{\mathcal{C},\mathcal{A}} := 2^n \cdot (\mathbb{1}_{\mathcal{C}} \mathbb{1}_{\mathcal{A}} \star \mathbb{1}_{\mathcal{C}} \mathbb{1}_{\mathcal{A}})$, and claim that $f_{\mathcal{C},\mathcal{A}}$ is a feasible solution for $\mathsf{Del}(n, d; \mathcal{A})$, with the objective function (Obj') evaluating to $|\mathcal{C} \cap \mathcal{A}|^2$. To see this, note that the LP constraints (D1)–(D3) are satisfied for the same reasons as why $f_{\mathcal{C}}$ satisfied (C1)–(C3) in $\mathsf{Del}(n, d)$ (see the proof of Theorem 9.4.1). Furthermore,

$$f_{\mathcal{C},\mathcal{A}}(0^n) = |\mathcal{C} \cap \mathcal{A}| \leq |\mathcal{C}| \leq \mathrm{OPT}(\mathsf{Del}(n, d)),$$

since $\mathcal{C}$ is a block code of distance at least d. Hence, (D4) is satisfied by $f_{\mathcal{C},\mathcal{A}}$. Finally, observe that for any $\mathbf{x} \in \{0,1\}^n$,

$$\begin{aligned} f_{\mathcal{C},\mathcal{A}}(\mathbf{x}) &= \sum_{\mathbf{z}\in\{0,1\}^n} \mathbb{1}_{\mathcal{C}}(\mathbf{z})\mathbb{1}_{\mathcal{A}}(\mathbf{z}) \cdot \mathbb{1}_{\mathcal{C}}(\mathbf{x}+\mathbf{z})\mathbb{1}_{\mathcal{A}}(\mathbf{x}+\mathbf{z}) \\ &\leq \sum_{\mathbf{z}\in\{0,1\}^n} \mathbb{1}_{\mathcal{A}}(\mathbf{z}) \cdot \mathbb{1}_{\mathcal{A}}(\mathbf{x}+\mathbf{z}) = 2^n \cdot (\mathbb{1}_{\mathcal{A}} \star \mathbb{1}_{\mathcal{A}})(\mathbf{x}), \end{aligned}$$

showing that (D5) also holds. Now, note that $\mathrm{val}(f_{\mathcal{C},\mathcal{A}}) = \sum_{\mathbf{x}\in\{0,1\}^n} f_{\mathcal{C},\mathcal{A}}(\mathbf{x}) = |\mathcal{C} \cap \mathcal{A}|^2$, by calculations as in (9.1). Hence, we have that $\mathrm{OPT}(\mathsf{Del}(n,d;\mathcal{A})) \geq |\mathcal{C} \cap \mathcal{A}|^2$, for any $\mathcal{C}$ with minimum distance at least d. The statement of the theorem then follows. □

In Section 9.6, we obtain numerical upper bounds on the sizes of constrained codes with a given minimum Hamming distance, for a number of constraints, via an application Theorem 9.4.2 (and Theorem 9.5.3). We now discuss a couple of observations about $\mathsf{Del}(n,d;\mathcal{A})$, stated as propositions.

Proposition 9.4.3. *For any $\mathcal{A} \subseteq \{0,1\}^n$, the inequality $(\mathrm{OPT}(\mathsf{Del}(n,d;\mathcal{A})))^{1/2} \leq |\mathcal{A}|$ holds.*

Proof. Note that by (D5), for any feasible solution f of $\mathsf{Del}(n,d;\mathcal{A})$, the objective value

$$\begin{aligned} \sum_{\mathbf{x}\in\{0,1\}^n} f(\mathbf{x}) &\leq \sum_{\mathbf{x}\in\{0,1\}^n} \sum_{\mathbf{z}\in\{0,1\}^n} \mathbb{1}_{\mathcal{A}}(\mathbf{z}) \cdot \mathbb{1}_{\mathcal{A}}(\mathbf{x}+\mathbf{z}) \\ &= \sum_{\mathbf{z}\in\{0,1\}^n} \mathbb{1}_{\mathcal{A}}(\mathbf{z}) \sum_{\mathbf{x}\in\{0,1\}^n} \mathbb{1}_{\mathcal{A}}(\mathbf{x}+\mathbf{z}) = |\mathcal{A}|^2. \end{aligned}$$

The statement of the proposition then follows. □

Proposition 9.4.4. *For any $\mathcal{A} \subseteq \{0,1\}^n$, we have $(\mathrm{OPT}(\mathsf{Del}(n,d;\mathcal{A})))^{1/2} \leq \mathrm{OPT}(\mathsf{Del}(n,d))$.*

Proof. Given the LP $\mathsf{Del}(n,d;\mathcal{A})$, defined by the objective function (Obj′) and the constraints (D1)–(D5), we define the new LP $\overline{\mathsf{Del}}(n,d)$ with the same objective function (Obj′) and using the constraints (D1)–(D4) alone (excluding constraint (D5)). Thus,

$\overline{\mathsf{Del}}(n,d)$ is given by:

$$\underset{f\colon \{0,1\}^n \to \mathbb{R}}{\text{maximize}} \quad \sum_{\mathbf{x}\in\{0,1\}^n} f(\mathbf{x}) \tag{Obj'}$$

subject to:

$$f(\mathbf{x}) \geq 0, \ \forall\, \mathbf{x} \in \{0,1\}^n, \tag{D1}$$

$$\widehat{f}(\mathbf{s}) \geq 0, \ \forall\, \mathbf{s} \in \{0,1\}^n, \tag{D2}$$

$$f(\mathbf{x}) = 0, \text{ if } 1 \leq w(\mathbf{x}) \leq d-1, \tag{D3}$$

$$f(0^n) \leq \mathrm{OPT}(\mathsf{Del}(n,d)), \tag{D4}$$

It is therefore clear that for any $\mathcal{A} \subseteq \{0,1\}^n$, the inequality $\mathrm{OPT}(\mathsf{Del}(n,d;\mathcal{A})) \leq \mathrm{OPT}(\overline{\mathsf{Del}}(n,d))$ holds. We now claim that $\mathrm{OPT}(\overline{\mathsf{Del}}(n,d)) = (\mathrm{OPT}(\mathsf{Del}(n,d)))^2$.

First, we shall show that the inequality in constraint (D4) in $\overline{\mathsf{Del}}(n,d)$ can be replaced with an equality. To see this, suppose that f were an optimal solution to $\overline{\mathsf{Del}}(n,d)$, with $f(0^n) < \mathrm{OPT}(\mathsf{Del}(n,d))$. Let $c > 0$ be such that $c \leq \mathrm{val}(\mathsf{Del}(n,d)) - f(0^n)$. We then construct the function $\overline{f} : \{0,1\}^n \to \mathbb{R}$ such that $\overline{f}(0^n) = f(0^n) + c$, and $\overline{f}(\mathbf{x}) = f(\mathbf{x})$, for $\mathbf{x} \neq 0^n$. It can then easily be verified that $\overline{f}$ satisfies constraints (D1), (D3) and (D4). Furthermore, $\overline{f}$ satisfies (D2) also, since by linearity of the Fourier transform, for any $\mathbf{s} \in \{0,1\}^n$,

$$\begin{aligned}\widehat{(\overline{f})}(\mathbf{s}) &= \widehat{f}(\mathbf{s}) + c \cdot \widehat{\mathbb{1}_{\{0^n\}}}(\mathbf{s}) \\ &= \widehat{f}(\mathbf{s}) + \frac{c}{2^n} \geq 0.\end{aligned}$$

Hence, $\overline{f}$ is a feasible solution to $\overline{\mathsf{Del}}(n,d)$, with $\mathrm{val}(\overline{f}) = \sum_{\mathbf{x}\in\{0,1\}^n} f(\mathbf{x}) + c > \mathrm{val}(f)$, which contradicts the optimality of f. Hence, any optimal solution to $\overline{\mathsf{Del}}(n,d)$ must be such that (D4) is satisfied with an equality, and we can thus replace the inequality in (D4) with an equality.

Now, in order to prove that $(\mathrm{OPT}(\overline{\mathsf{Del}}(n,d)))^{1/2} = \mathrm{OPT}(\mathsf{Del}(n,d))$, it suffices to observe that any feasible solution f of $\mathsf{Del}(n,d)$ yields a feasible solution $\mathrm{OPT}(\mathsf{Del}(n,d)) \cdot$

f, to $\overline{\mathsf{Del}}(n,d)$ (with the inequality in (D4) changed to an equality). Likewise, any feasible solution f of $\overline{\mathsf{Del}}(n,d)$ yields a feasible solution $\frac{f}{\mathrm{OPT}(\overline{\mathsf{Del}}(n,d))}$, to $\mathsf{Del}(n,d)$. Owing to this bijection, we obtain that $\mathrm{OPT}(\overline{\mathsf{Del}}(n,d)) = \mathrm{OPT}(\mathsf{Del}(n,d))^2$.

Using the fact that $\mathrm{OPT}(\mathsf{Del}(n,d;\mathcal{A})) \leq \mathrm{OPT}(\overline{\mathsf{Del}}(n,d))$, we obtain the statement of the proposition. □

From Propositions 9.4.3 and 9.4.4, we obtain that the size of the largest constrained code with minimum distance at least d obeys $A(n,d;\mathcal{A}) \leq \min\{\mathrm{OPT}(\mathsf{Del}(n,d)), |\mathcal{A}|\}$, for all constraints represented by $\mathcal{A} \subseteq \{0,1\}^n$.

9.5 Symmetrizing $\mathsf{Del}(n,d;\mathcal{A})$

The linear program $\mathsf{Del}(n,d;\mathcal{A})$ discussed in Section 9.4, for a fixed $\mathcal{A} \subseteq \mathbb{F}_2^n$, suffers from the drawback that the variables, which are precisely the values $(f(\mathbf{x}) : \mathbf{x} \in \{0,1\}^n)$, are 2^n in number, i.e., exponentially large in the blocklength. The number of LP constraints, similarly, are exponentially large in n. It would therefore be of interest to check if the size of the linear program $\mathsf{Del}(n,d;\mathcal{A})$, which is the sum of the number of variables and the number of LP constraints, can be reduced, using symmetries present in the formulation.

Our exposition in this section on symmetrizing $\mathsf{Del}(n,d;\mathcal{A})$, follows that in [108] (see also [109] for a more general study of symmetrization procedures and [102] for an application to the generalized sphere packing bounds). Let S_n denote the symmetric group on n elements, which is the set of all permutations $\sigma : [n] \to [n]$. Note that given a length-n vector $\mathbf{x} = (x_1, \ldots, x_n) \in \{0,1\}^n$, a permutation $\sigma \in S_n$ acts on $\mathbf{x}$ as follows: $\sigma \cdot \mathbf{x} = (x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)})$. The permutation σ also acts on functions $f : \{0,1\}^n \to \mathbb{R}$ via the mapping $(\sigma \circ f)(\mathbf{x}) = f(\sigma \cdot \mathbf{x})$, for $\mathbf{x} \in \{0,1\}^n$. Now, given any set $\mathcal{A} \subseteq \mathbb{F}_2^n$, we define the "symmetry group" of the constraint represented by $\mathcal{A}$ to be the set of all permutations $\pi \in S_n$ that leave the indicator function $\mathbb{1}_{\mathcal{A}}$ invariant. In other words, the symmetry group $G_{\mathcal{A}}$ of the constraint represented by $\mathcal{A}$ is the set of all permutations $\pi \in S_n$ such that $\mathbb{1}_{\mathcal{A}} = \pi \circ \mathbb{1}_{\mathcal{A}}$.

Given a group $G \subseteq S_n$ of permutations, which acts on the vectors $\mathbf{x} \in \{0,1\}^n$, we say that $\mathsf{Del}(n,d;\mathcal{A})$ is G-invariant, if for all $\sigma \in G$, we have that if $f : \{0,1\}^n \to \mathbb{R}$ is a feasible solution to $\mathsf{Del}(n,d;\mathcal{A})$, then so is $\sigma \circ f$, with $\mathrm{val}(f) = \mathrm{val}(\sigma \circ f)$. The following proposition then holds:

Proposition 9.5.1. $\mathsf{Del}(n,d;\mathcal{A})$ *is* $G_{\mathcal{A}}$*-invariant.*

Before we prove the above proposition, we shall state and prove a simple lemma.

Lemma 9.5.2. *For any function* $f : \{0,1\}^n \to \mathbb{R}$ *and for any permutation* $\sigma \in S_n$*,*

$$\widehat{\sigma \circ f}(\mathbf{s}) = (\sigma \circ \widehat{f})(\mathbf{s}), \quad \textit{for all } \mathbf{s} \in \{0,1\}^n.$$

Proof. Observe that

$$\begin{aligned}
\widehat{\sigma \circ f}(\mathbf{s}) &= \sum_{\mathbf{x} \in \{0,1\}^n} f(\sigma \cdot \mathbf{x}) \cdot (-1)^{\mathbf{x} \cdot \mathbf{s}} \\
&= \sum_{\mathbf{x} \in \{0,1\}^n} f(\sigma \cdot \mathbf{x}) \cdot (-1)^{(\sigma \cdot \mathbf{x}) \cdot (\sigma \cdot \mathbf{s})} \\
&= \sum_{\mathbf{x} \in \{0,1\}^n} f(\mathbf{x}) \cdot (-1)^{\mathbf{x} \cdot (\sigma \cdot \mathbf{s})} = (\sigma \circ \widehat{f})(\mathbf{s}).
\end{aligned}$$

□

We shall now prove Proposition 9.5.1.

Proof of Proposition 9.5.1. Let $\pi \in G_{\mathcal{A}}$ be a permutation in the symmetry group of $\mathcal{A}$ and let f be some feasible solution to $\mathsf{Del}(n,d;\mathcal{A})$. We first show that $\pi \circ f$ is also a feasible solution to $\mathsf{Del}(n,d;\mathcal{A})$.

(D1) It is clear that if $f(\mathbf{x}) \geq 0$, then $f(\pi \cdot \mathbf{x}) \geq 0$, for all $\mathbf{x} \in \{0,1\}^n$.

(D2) The fact that if $\widehat{f}(\mathbf{s}) \geq 0$, then $\widehat{\pi \circ f}(\mathbf{s}) \geq 0$, for all $\mathbf{s} \geq 0$, follows directly from Lemma 9.5.2.

(D3) Since any permutation in $G_{\mathcal{A}}$ also lies in S_n and hence preserves the weights of vectors in $\{0,1\}^n$, we have $(\pi \circ f)(\mathbf{x}) = 0$, for all $\mathbf{x} \in \{0,1\}^n$ such that $1 \leq w(\mathbf{x}) \leq d-1$.

(D4) This constraint is also satisfied by $\pi \circ f$, since $\pi(0^n) = 0^n$, for all $\pi \in G_{\mathcal{A}}$.

(D5) Observe that for any $\pi \in G_{\mathcal{A}}$,

$$\begin{aligned} 2^n \cdot (\mathbb{1}_{\mathcal{A}} \star \mathbb{1}_{\mathcal{A}})(\pi \cdot \mathbf{x}) &= \sum_{\mathbf{z} \in \{0,1\}^n} \mathbb{1}_{\mathcal{A}}(\mathbf{z}) \cdot \mathbb{1}_{\mathcal{A}}(\pi \cdot \mathbf{x} + \mathbf{z}) \\ &= \sum_{\mathbf{z} \in \{0,1\}^n} \mathbb{1}_{\mathcal{A}}(\pi \cdot \mathbf{z}) \cdot \mathbb{1}_{\mathcal{A}}(\pi \cdot \mathbf{x} + \pi \cdot \mathbf{z}) \\ &= \sum_{\mathbf{z} \in \{0,1\}^n} \mathbb{1}_{\mathcal{A}}(\pi \cdot \mathbf{z}) \cdot \mathbb{1}_{\mathcal{A}}(\pi \cdot (\mathbf{x} + \mathbf{z})) \\ &= \sum_{\mathbf{z} \in \{0,1\}^n} \mathbb{1}_{\mathcal{A}}(\mathbf{z}) \cdot \mathbb{1}_{\mathcal{A}}(\mathbf{x} + \mathbf{z}) = 2^n \cdot (\mathbb{1}_{\mathcal{A}} \star \mathbb{1}_{\mathcal{A}})(\mathbf{x}). \end{aligned}$$

Hence, since for all $\mathbf{x} \in \{0,1\}^n$, we have that

$$\begin{aligned} \pi \circ f(\mathbf{x}) &\leq 2^n \cdot (\mathbb{1}_{\mathcal{A}} \star \mathbb{1}_{\mathcal{A}})(\pi \cdot \mathbf{x}) \\ &= 2^n \cdot (\mathbb{1}_{\mathcal{A}} \star \mathbb{1}_{\mathcal{A}})(\mathbf{x}), \end{aligned}$$

where the equality holds since $\pi \in G_{\mathcal{A}}$, it follows that (D5) is also satisfied by $\pi \circ f$.

Finally, we show that the values of the feasible solutions f and $\pi \circ f$ are identical:

(Obj′) It is clear that $\sum_{\mathbf{x}} f(\mathbf{x}) = \sum_{\mathbf{x}} f(\pi \cdot \mathbf{x})$, and hence that $\mathrm{val}(f) = \mathrm{val}(\pi \circ f)$.

□

From the preceding discussion, we see that given a feasible solution f to $\mathsf{Del}(n, d; \mathcal{A})$, we can construct the function $\overline{f} := \frac{1}{|G_{\mathcal{A}}|} \sum_{\pi \in G_{\mathcal{A}}} \pi \circ f$, such that $\overline{f}$ is also a feasible solution to the LP (by linearity), with $\mathrm{val}(\overline{f}) = \mathrm{val}(f)$. Observe, in addition, that $\overline{f}$ is such that $\pi \circ \overline{f} = \overline{f}$, for all $\pi \in G_{\mathcal{A}}$. Now, given a group H of permutations of n elements, we

define the equivalence relation '$\sim_H$' as follows: for vectors $\mathbf{x}, \mathbf{y} \in \{0,1\}^n$, we say that $\mathbf{x} \sim_H \mathbf{y}$, if $\mathbf{y} = \sigma \cdot \mathbf{x}$, for some $\sigma \in H$. Further, we define the set $\{0,1\}^n/H$ to be the collection of equivalence classes under $\sim_H$, or orbits, given the group H. From the above discussion, it follows that in order to arrive at an optimal solution to $\mathsf{Del}(n,d;\mathcal{A})$, one can restrict oneself to searching among feasible solutions f that are constant on each orbit O in $\{0,1\}^n/G_{\mathcal{A}}$. Such functions f can be expressed as

$$f(\mathbf{x}) = \sum_{O \in \{0,1\}^n/G_{\mathcal{A}}} a_O \cdot \mathbb{1}_O(\mathbf{x}), \tag{9.2}$$

where $a_O \in \mathbb{R}$, for all $O \in \{0,1\}^n/G_{\mathcal{A}}$. Before we work on symmetrizing the constraints of $\mathsf{Del}(n,d;\mathcal{A})$, we introduce some notation. For an orbit $O \in \{0,1\}^n/G_{\mathcal{A}}$, we denote by $|O|$ the number of elements in the orbit and by $\mathbf{x}_O$ (or $\mathbf{s}_O$) a representative element of the orbit. Further, for a given element $\mathbf{x} \in \{0,1\}^n$, we define $O(\mathbf{x})$ to be the orbit in which $\mathbf{x}$ lies. We shall now formulate (D1)–(D5) and the objective function (Obj′) in $\mathsf{Del}(n,d;\mathcal{A})$, based on (9.2).

(D1′) The fact that $f(\mathbf{x}) \geq 0$ for all $\mathbf{x}$ implies that $a_O \geq 0$, for all $O \in \{0,1\}^n/G_{\mathcal{A}}$.

(D2′) By the linearity of the Fourier transform operation, we obtain that

$$\widehat{f}(\mathbf{s}) = \sum_{O \in \{0,1\}^n/G_{\mathcal{A}}} a_O \cdot \widehat{\mathbb{1}_O}(\mathbf{s}) \geq 0,$$

for all $\mathbf{s} \in \{0,1\}^n$.

In fact, note that since $G_{\mathcal{A}} \subseteq S_n$, it can be argued using Lemma 9.5.2 that the above inequality only needs to hold for orbit representatives $\mathbf{s}_O \in \{0,1\}^n$, of $O \in \{0,1\}^n/G_{\mathcal{A}}$. Indeed, we have that for any $\pi \in G_{\mathcal{A}}$, and for functions f as in (9.2),

$$\widehat{f}(\pi \cdot \mathbf{s}) = \widehat{\pi \circ f}(\mathbf{s}) = \widehat{f}(\mathbf{s}),$$

where the first equality holds by Lemma 9.5.2 and the second holds since $\pi \circ f =$

f.

(D3′) The constraint (D3) implies that $a_O = 0$, for all O such that $1 \leq w(\mathbf{x}_O) \leq d-1$, where $\mathbf{x}_O \in \{0,1\}^n$ is a representative element of the orbit $O \in \{0,1\}^n/G_{\mathcal{A}}$.

(D4′) The constraint (D4) becomes: $a_{O(0^n)} = a_{0^n} \leq \mathrm{OPT}(\mathsf{Del}(n,d))$, where $O(0^n) = \{0^n\}$ is the orbit that contains the all-zeros word 0^n.

(D5′) Similarly, the constraint (D5) reduces to: $a_O \leq 2^n \cdot (\mathbb{1}_{\mathcal{A}} \star \mathbb{1}_{\mathcal{A}})(\mathbf{x}_O)$, where, again, $\mathbf{x}_O$ is some representative element of the orbit $O \in \{0,1\}^n/G_{\mathcal{A}}$.

(Obj″) From (9.2), we see that the new objective function simply becomes

$$\underset{a_O \in \mathbb{R}}{\text{maximize}} \sum_{O \in \{0,1\}^n/G_{\mathcal{A}}} |O| \cdot a_O.$$

We call the symmetrized version of $\mathsf{Del}(n,d;\mathcal{A})$ as $\mathsf{Del}_{/G_{\mathcal{A}}}(n,d;\mathcal{A})$, which is given below.

$\mathsf{Del}_{/G_{\mathcal{A}}}(n,d;\mathcal{A})$

$$\underset{\{a_O \in \mathbb{R}:\ O \in \{0,1\}^n/G_{\mathcal{A}}\}}{\text{maximize}} \quad \sum_O |O| \cdot a_O \tag{Obj″}$$

subject to:

$$a_O \geq 0, \forall\, O \in \{0,1\}^n/G_{\mathcal{A}}, \tag{D1′}$$

$$\sum_{O \in \{0,1\}^n/G_{\mathcal{A}}} a_O \cdot \widehat{\mathbb{1}_O}(\mathbf{s}_{\tilde{O}}) \geq 0,\ \forall \text{ orbit rep. } \mathbf{s}_{\tilde{O}} \in \{0,1\}^n, \tag{D2′}$$

$$a_O = 0, \text{ if } 1 \leq w(\mathbf{x}_O) \leq d-1, \tag{D3′}$$

$$a_{0^n} \leq \mathrm{OPT}(\mathsf{Del}(n,d)), \tag{D4′}$$

$$a_O \leq 2^n \cdot (\mathbb{1}_{\mathcal{A}} \star \mathbb{1}_{\mathcal{A}})(\mathbf{x}_O),\ \forall\, O \in \{0,1\}^n/G_{\mathcal{A}}. \tag{D5′}$$

The preceding discussion can then be summarized as a theorem.

Theorem 9.5.3. *The LPs* $\mathsf{Del}(n,d;\mathcal{A})$ *and* $\mathsf{Del}_{/G_{\mathcal{A}}}(n,d;\mathcal{A})$ *are equivalent in that*

$$\mathrm{OPT}(\mathsf{Del}(n,d;\mathcal{A})) = \mathrm{OPT}(\mathsf{Del}_{/G_{\mathcal{A}}}(n,d;\mathcal{A})).$$

Remark 9.5.4. *All the above arguments remain valid if we use a subgroup H of the symmetry group $G_{\mathcal{A}}$ as well. For the special case when $\mathcal{A} = \{0,1\}^n$, we have $G_{\mathcal{A}} = S_n$, and we then recover the more common version of Delsarte's LP that is $M_{LP}(n,d)$ in [104]. It is this version that we use for evaluating the right-hand side of constraints (D4) and (D4$'$), in our numerical examples.*

Observe that in the symmetrized LP $\mathsf{Del}_{/G_{\mathcal{A}}}(n,d;\mathcal{A})$, the number of variables is the number $N_{\mathcal{A}}$ of orbits $O \in \{0,1\}^n/G_{\mathcal{A}}$ and the number of constraints is at most $4N_{\mathcal{A}}+1$. Hence, if the constraint is such that the number of orbits $N_{\mathcal{A}}$ induced by its symmetry group is small (as a function of the blocklength n), then the size of the symmetrized LP is small. In the section that follows, we shall explicitly write down $\mathsf{Del}_{/G_{\mathcal{A}}}(n,d;\mathcal{A})$, for select constraints (or sets $\mathcal{A}$), and provide numerical results obtained by running $\mathsf{Del}_{/G_{\mathcal{A}}}(n,d;\mathcal{A})$ on those constraints.

9.6 Numerical Trials

9.6.1 2-Charge Constraint

We shall first work with the so-called 2-charge constraint (see Section 1.5.4 in [2] and Section 7.5.1 for more on the constraint). Recall that the 2-charge constraint admits only sequences $\mathbf{y} \in \{-1,+1\}^n$, whose running sum $\sum_{i=1}^{r} y_i$, for any $1 \le r \le n$, obeys $0 \le \sum_{i=1}^{r} y_i \le 2$.

To any sequence $\mathbf{x} \in \{0,1\}^n$, we associate (in a one-one manner) the sequence $\mathbf{y} = ((-1)^{x_1},\ldots,(-1)^{x_n}) \in \{-1,+1\}^n$. We let S_2 denote the set of sequences $\mathbf{x} \in \{0,1\}^n$ such that $\mathbf{y} = ((-1)^{x_1},\ldots,(-1)^{x_n})$ is 2-charge constrained. Thus, the set of constrained sequences of interest to us is $\mathcal{A} = S_2$, with Figure 9.1 being a state transition graph for sequences in the set S_2.

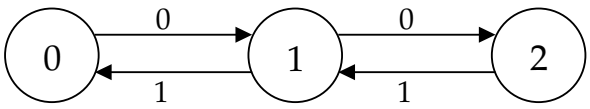


Figure 9.1: State transition graph for sequences in the set S_2.

In what follows, we fix the blocklength n to be odd. Slight modifications of the construction of the symmetry group G_{S_2} and the identification of the orbits, below, yield a symmetrized LP $\mathsf{Del}_{/G_{S_2}}(n, d; S_2)$, when n is even.

Now, consider the following permutations, where n is odd:

1. For even indices $i \in [n]$, define $\pi_i^{\text{adj}} : [n] \to [n]$, such that $\pi_i^{\text{adj}}(i) = i+1$, $\pi_i^{\text{adj}}(i+1) = i$, and $\pi_i^{\text{adj}}(j) = j$, for $j \notin \{i, i+1\}$.

   In words, $\pi_{i,j}^{\text{adj}}$ swaps adjacent positions i and $i+1$, for even $i \in [n]$, and leaves other positions unchanged.

2. For even indices $i, j \in [n]$, define $\pi_{i,j}^{\text{swap}} : [n] \to [n]$, such that $\pi_{i,j}^{\text{swap}}(i) = j$, $\pi_{i,j}^{\text{swap}}(i+1) = j+1$, and $\pi_{i,j}{}^{\text{swap}}(j) = i$, $\pi_{i,j}^{\text{swap}}(j+1) = i+1$, with $\pi_{i,j}^{\text{swap}}(k) = k$, for $k \notin \{i, i+1, j, j+1\}$.

   In words, $\pi_{i,j}^{\text{swap}}$ swaps i and j, and $i+1$ and $j+1$, for i, j being even, and leaves other positions unchanged.

The discussion above on the sequences in S_2 implies that the symmetry group G_{S_2} of the constraint is generated (via compositions) by $\{\pi_i^{\text{adj}} : i \text{ even}\} \cup \{\pi_{i,j}^{\text{adj}} : i, j \text{ even}\}$. Further, consider tuples $\boldsymbol{\alpha} \in \{0,1\} \times \left[0 : \lfloor \frac{n}{2} \rfloor\right] \times \left[0 : \lfloor \frac{n}{2} \rfloor\right]$ of the form $\boldsymbol{\alpha} = (b, t_{00}, t_{11})$, with $t_{00} + t_{11} \leq \lfloor \frac{n}{2} \rfloor$. For a sequence $\mathbf{x} \in \{0,1\}^n$, we identify $b \in \{0,1\}$ with x_1, the integer t_{00} with $|\{i : \ i \text{ even and } (x_i, x_{i+1}) = (0,0)\}|$, and the integer t_{11} with $|\{i : \ i \text{ even and } (x_i, x_{i+1}) = (1,1)\}|$. Note that then $|\{i : \ i \text{ even and } (x_i, x_{i+1}) = (0,1) \text{ or } (1,0)\}| = \lfloor \frac{n}{2} \rfloor - t_{00} - t_{11}$. We thus have that the orbits of the symmetry group of the constraint $\{0,1\}^n / G_{S_2}$ are in one-one correspondence with tuples of the form $\boldsymbol{\alpha} = (b, t_{00}, t_{11})$. Observe that the number of orbits is hence bounded above by $2 \cdot \lfloor \frac{n}{2} \rfloor^2$, and therefore the number of variables and the number of constraints in the LP $\mathsf{Del}_{/G_{S_2}}(n, d; S_2)$, are bounded above by a polynomial function of the blocklength

d	$\mathsf{Del}_{/G_{S_2}}(n,d;S_2)$	$\mathsf{GenSph}(n,d;S_2)$	$\mathsf{Del}(n,d)$
2	64	64	4096
3	45.255	64	512
4	45.255	64	292.571
5	22.627	64	64
6	17.889	64	40
7	5.657	32	8
8	4.619	32	5.333
9	2.828	16	3.333
10	2.619	16	2.857

Table 9.1: Table of optimal values of the symmetrized $\mathsf{Del}_{/G_{S_2}}(n,d;S_2)$ LP, the generalized sphere packing bound LP $\mathsf{GenSph}(n,d;S_2)$ in [102] and [100], and the $\mathsf{Del}(n,d)$ LP, for $n = 13$ and varying values of d.

n, unlike the number of variables in $\mathsf{Del}(n,d;S_2)$, which equals 2^n. Table 9.1 shows numerical evaluations of $\mathsf{Del}_{/G_{S_2}}(n,d;S_2)$, when $n = 13$, for varying values of d. The table also includes comparisons with upper bounds via the generalized sphere packing bound of [100] and [102] and with $\mathsf{Del}(n,d)$. We observe that once again our LP provides tighter upper bounds than those obtained by the sphere packing approach.

9.6.2 Constant Subblock Composition Constraint

In this section, we study the derivation of upper bounds for the so-called constant subblock-composition constraint CSC_z^p (see Section 7.5.2), which requires that each one of the p "subblocks" of a binary sequence have a constant number, z, of 1s. We let C_z^p denote the set of all CSC_z^p-constrained sequences of length n. The structure of the symmetry group $G_{C_z^p}$ was derived in [110] (see the group H in Section III of [110]), but to make the exposition self-contained, we present the symmetry group here too. Explicit closed-form expressions for the generalized sphere packing bounds for this

constraint were also derived in [110].

We now provide a more explicit form of $\mathsf{Del}_{/G_{\mathcal{A}}}(n,d;\mathcal{A})$, when $\mathcal{A}=C_z^p$, for a fixed blocklength n and parameters p and z. From the description of the constraint, it can be checked that the symmetry group $G_{C_z^p}$ is generated (via compositions) by the following permutations:

1. For $1\leq \ell\leq p$, and $\frac{(\ell-1)n}{p}+1\leq j\leq \frac{\ell n}{p}$, define $\pi_\ell^{\mathrm{perm},j}:[n]\to[n]$ such that $\pi_\ell^{\mathrm{perm},j}$ swaps the indices $\frac{(\ell-1)n}{p}+1$ and j, and leaves the other indices in $[n]$ unchanged.

   Note that for a fixed block indexed by $1\leq\ell\leq p$, the collection of permutations $\{\pi_\ell^{\mathrm{perm},j}:\ \frac{(\ell-1)n}{p}+1\leq j\leq\frac{\ell n}{p}\}$ generates a group isomorphic to the symmetric group $S_{n/p}$, which contains all permutations of the indices $\frac{(\ell-1)n}{p}+1\leq i\leq\frac{\ell n}{p}$.

2. For $1\leq\ell,\ell'\leq p$, define $\pi_{\ell,\ell'}^{\mathrm{exch}}:[n]\to[n]$ such that $\pi_{\ell,\ell'}^{\mathrm{exch}}$ swaps the element $\frac{(\ell-1)n}{p}+j$ with $\frac{(\ell'-1)n}{p}+j$, for all $1\leq j\leq\frac{n}{p}$, and leaves the other indices in $[n]$ unchanged.

   In other words, $\pi_{\ell,\ell'}^{\mathrm{exch}}$ exchanges entire blocks indexed by ℓ and ℓ'.

Note that for a fixed block indexed by $1\leq\ell\leq p$, the collection of permutations $\left\{\pi_\ell^{\mathrm{perm},j}:\frac{(\ell-1)n}{p}+1\leq j\leq\frac{\ell n}{p}\right\}$ generates a group isomorphic to the symmetric group $S_{n/p}$, which contains all permutations of the indices $\frac{(\ell-1)n}{p}+1\leq i\leq\frac{\ell n}{p}$. Also, the collection of permutations $\{\pi_{\ell,\ell'}^{\mathrm{exch}}:1\leq\ell,\ell'\leq p\}$ generates a group isomorphic to the symmetric group S_p.

From the description of the symmetry group $G_{C_z^p}$ above, we arrive at the fact that the orbits of the symmetry group are in one-one correspondence with *unordered* p-tuples $\boldsymbol{\alpha}\in\left[0:\frac{n}{p}\right]^p$. Indeed, a given sequence $\mathbf{x}\in\{0,1\}^n$ lies in the orbit $\boldsymbol{\alpha}(\mathbf{x})=(\alpha_1(\mathbf{x}),\ldots,\alpha_p(\mathbf{x}))$, where $\mathrm{wt}(\mathbf{x}_\ell)=\alpha_{\sigma(\ell)}$, for $1\leq\ell\leq p$ and some permutation $\sigma\in S_p$. Note hence that the number of orbits, and therefore the sum of the number of variables and the number of constraints in $\mathsf{Del}_{/G_{C_z^p}}(n,d;C_z^p)$ is bounded above by $c\cdot\left(\frac{n}{p}\right)^p$, for some constant $c>0$, which is only a polynomial function of the blocklength. Further, for a given orbit $\boldsymbol{\alpha}$, we let $\mathbf{x}_{\boldsymbol{\alpha}}$ be a representative element of the orbit. In particular, we

define $\mathbf{x}_{\boldsymbol{\alpha}}$ to be the concatenation $\mathbf{x}_{\boldsymbol{\alpha},1}\mathbf{x}_{\boldsymbol{\alpha},2}\dots\mathbf{x}_{\boldsymbol{\alpha},p}$, with

$$\mathbf{x}_{\boldsymbol{\alpha},\ell} = (\underbrace{1,1,\dots,1}_{\alpha_1 \text{ such}},0,0,\dots,0) \tag{9.3}$$

being of length n/p, for $1 \leq \ell \leq p$. We thus obtain the following lemma:

Lemma 9.6.1. *For given orbits $\boldsymbol{\alpha}, \tilde{\boldsymbol{\alpha}}$, with $\mathbf{s}_{\tilde{\boldsymbol{\alpha}}}$ being an orbit representative of $\tilde{\boldsymbol{\alpha}}$, we have*

$$2^n \cdot \widehat{\mathbb{1}_{\boldsymbol{\alpha}}}(\mathbf{s}_{\tilde{\boldsymbol{\alpha}}}) = \prod_{\ell=1}^{p} K_{\alpha_\ell}^{(n/p)}(\tilde{\alpha}_\ell),$$

where for a given length m, $K_i^{(m)}$ is the i^{th} Krawtchouk polynomial, with

$$K_i^{(m)}(j) = \sum_{t=0}^{i} (-1)^t \binom{j}{t}\binom{m-j}{i-t}.$$

Proof. We have that

$$\begin{aligned} 2^n \cdot \widehat{\mathbb{1}_{\boldsymbol{\alpha}}}(\mathbf{s}_{\tilde{\boldsymbol{\alpha}}}) &= \sum_{\mathbf{x}\in\{0,1\}^n:\ \boldsymbol{\alpha}(\mathbf{x})=\boldsymbol{\alpha}} (-1)^{\mathbf{x}\cdot\mathbf{s}_{\tilde{\boldsymbol{\alpha}}}} \\ &= \prod_{\ell=1}^{p} \left(\sum_{\mathbf{x}_\ell\in\{0,1\}^{n/p}:\ w(\mathbf{x})=\alpha_\ell} (-1)^{\mathbf{x}\cdot\mathbf{s}_{\tilde{\boldsymbol{\alpha}},\ell}} \right). \end{aligned}$$

By direct calculations, it holds that for any $\ell \in [p]$, the sum in the expression above equals $K_{\alpha_\ell}^{(n/p)}(\tilde{\alpha}_\ell)$, when $\mathbf{s}_{\tilde{\boldsymbol{\alpha}},\ell}$ follows the convention in (9.3). □

Tables 9.2 and 9.3 show numerical evaluations of $\mathsf{Del}_{/G_{C_z^p}}(n,d;C_z^p)$, when $n = 14$ and $n = 15$, respectively, for fixed parameters p and z, and for varying values of d, and comparisons with upper bounds via the generalized sphere packing bound of [100] and [102]. Here too our LP provides tighter upper bounds than the generalized sphere packing bounds.

d	$\mathsf{Del}_{/G_{C_5^2}}(n,d;C_5^2)$	$\mathsf{GenSph}(n,d;C_5^2)$
2	441	441
3	197.9899	441
4	197.9899	441
5	49.574	147
6	35.0542	147
7	11.3137	73.5

Table 9.2: Table of optimal values of the $\mathsf{Del}_{/G_{C_5^2}}(n,d;C_5^2)$ LP, and the generalized sphere packing bound LP $\mathsf{GenSph}(n,d;C_5^2)$, for $(n,p,z)=(14,2,5)$, and varying values of d.

d	$\mathsf{Del}_{/G_{C_2^3}}(n,d;C_2^3)$	$\mathsf{GenSph}(n,d;C_2^3)$
2	1000	1000
3	826.236	1000
4	826.236	1000
5	157.767	333.333
6	110.851	333.333
7	22.627	166.667

Table 9.3: Table of optimal values of the $\mathsf{Del}_{/G_{C_2^3}}(n,d;C_2^3)$ LP, and the generalized sphere packing bound LP $\mathsf{GenSph}(n,d;C_2^3)$, for $(n,p,z)=(15,3,2)$, and varying values of d.

9.6.3 Tail-Biting Constraints

In this section, we briefly discuss the specialization of the $\mathsf{Del}_{/G_{\mathcal{A}}}(n,d;\mathcal{A})$ LP to the case of tail-biting constraints represented by a special set $\mathcal{A}$ of constrained sequences. In particular, $\mathcal{A}$ has the property that if a sequence $\mathbf{x}\in\mathcal{A}$, then $\pi^{\mathrm{cyc},i}\cdot\mathbf{x}$ also lies in $\mathcal{A}$, where for $1\leq i\leq n$, $\pi^{\mathrm{cyc},i}$ shifts each bit in $\mathbf{x}$ by i bits to the left, wrapping around cyclically, if needed. More formally, $x_{\pi^{\mathrm{cyc},i}(j)}=x_{\mathrm{mod}(j+i,n)+1}$, for $1\leq j\leq n$. Clearly, we have that the symmetry group of the constraint $G_{\mathcal{A}}$ contains the cyclic group C_n, and it is hence possible to symmetrize $\mathsf{Del}(n,d;\mathcal{A})$ using C_n. The orbits

$\boldsymbol{\alpha}$ thus are in one-one correspondence with (fixed) 2-ary necklaces of length n, with turnovers prohibited (see pg. 18 in [111] and sequence A000031 of [112]). It is known that the number of such necklaces, and hence the number of orbits, $N_{\text{cyc}}(n)$, is such that $\lim_{n\to\infty} \frac{N_{\text{cyc}}(n)}{2^n/n} = 1$ (see [113]); in other words, the sum of the number of variables and constraints in $\mathsf{Del}_{/G_{\mathcal{A}}}(n, d; \mathcal{A})$, is bounded above by $c \cdot \frac{2^n}{n}$, for some constant $c > 0$, and large enough n. Thus, we obtain a slight reduction in the size of the LP as compared to $\mathsf{Del}(n, d; \mathcal{A})$, which had 2^n variables.

We then apply this symmetrization procedure to the tail-biting $(1, \infty)$-RLL constraint, which admits only binary sequences $\mathbf{x} \in \{0, 1\}^n$ with no consecutive ones and which are such that $(x_1, x_n) \neq (1, 1)$. We let $S^{\text{tail}}_{(1,\infty)}$ denote the collection of such sequences. Similar to the approach in the previous two subsections, we can set up a symmetrized LP $\mathsf{Del}_{/G_{S^{\text{tail}}_{(1,\infty)}}}(n, d; S^{\text{tail}}_{(1,\infty)})$, using the orbits of the cyclic group C_n. Table 9.4 shows numerical evaluations of $\mathsf{Del}_{/G_{S^{\text{tail}}_{(1,\infty)}}}(n, d; S^{\text{tail}}_{(1,\infty)})$, when $n = 13$, for varying values of d, and comparisons with the generalized sphere packing bound. Again, our LP provides tighter upper bounds than the generalized sphere packing bounds. Observe also that for certain values of minimum distance d, the optimal value of our LP coincides with the optimal value of $\mathsf{Del}(n, d)$.

9.7 Conclusions and Directions for Future Work

In this chapter, we considered the input-constrained adversarial bit-flip error and erasure channels, and sought to obtain bounds on the sizes of the largest constrained codes that allow for zero-error decoding over such channels. We observed that our problem is equivalent to determining bounds on the sizes of constrained codes with a prescribed minimum Hamming distance. Our approach was to provide an extension of Delsarte's linear program (LP) for the setting of constrained systems, the square root of whose optimal value is an upper bound on the size of the largest constrained code of length n and minimum distance at least d. For select constraints, we showed that it is possible to reduce the number of variables and LP constraints, via a symmetrization

d	$\mathsf{Del}_{/G_{S^{\mathrm{tail}}_{(1,\infty)}}}(n, d; S^{\mathrm{tail}}_{(1,\infty)})$	$\mathsf{GenSph}(n, d; S^{\mathrm{tail}}_{(1,\infty)})$	$\mathsf{Del}(n, d)$
2	480.676	521	4096
3	350.055	448.5	512
4	229.569	448.5	292.571
5	64	316.727	64
6	40	316.727	40
7	8	169	8
8	5.333	169	5.333
9	3.333	73.667	3.333

Table 9.4: Table of optimal values of the $\mathsf{Del}_{/G_{S^{\mathrm{tail}}_{(1,\infty)}}}(n, d; S^{\mathrm{tail}}_{(1,\infty)})$ LP, the generalized sphere packing bound LP $\mathsf{GenSph}(n, d; S^{\mathrm{tail}}_{(1,\infty)})$ in [102] and [100], and $\mathsf{Del}(n, d)$, for $n = 13$, and varying values of d.

procedure that made use of the symmetry group of the constraint. We then applied our LP to different constraints, and observed that our numerical upper bounds are better than the generalized sphere packing bounds of Fazeli, Vardy, and Yaakobi (2015).

An interesting direction for future work would be to derive a good dual LP formulation for the LP presented here and use this dual LP to arrive at asymptotic (in the limit as the blocklength goes to infinity) upper bounds on the rate-distance tradeoff for constrained codes, similar to those that were derived in [104] for unconstrained systems. This will help us understand if the Gilbert-Varshamov lower bounds of Marcus and Roth (1992) are tight for any constrained system.

Chapter 10

Conclusions and Future Work

In this thesis, we worked on the explicit computation of bounds on the capacities of, and the design of coding schemes for, channels with input constraints. In particular, we derived information-theoretic bounds (lower bounds via Shannon inequalities and upper bounds via the feedback capacity) on the capacities of input-constrained discrete memoryless channels (DMCs), and constructed coding schemes, using constrained subcodes of Reed-Muller (RM) codes, whose rates were comparable with the lower bounds. We also provided Fourier-analytic insight into the problem of counting arbitrarily-constrained codewords in general binary linear codes, in keeping with our approach of using constrained subcodes of good linear codes over input-constrained memoryless channels. Finally, we studied upper bounds on the sizes of constrained codes with a given minimum Hamming distance (or equivalently, upper bounds on the sizes of error-resilient constrained codes over an adversarial bit-flip error/erasure channel), via a version of Delsarte's linear program (LP) for constrained systems.

As is the case with any dissertation, we are left with more questions than answers. The sections on future work at the end of Chapters 4–9 identified many engaging still-open research problems. We mention here three problems that we believe are challenging and promising directions to work on:

1. **Resolving Wolf's Conjecture**: As mentioned in Chapter 4, Wolf's conjecture on the capacities of runlength limited input-constrained BSCs is still left wanting a

rigorous proof:

Conjecture 10.0.1 (see [32]). *For the (d,k)-RLL input-constrained BSC(p), with capacity C, the inequality*

$$C \geq \kappa_{d,k} \cdot (1 - h_b(p)),$$

holds, where $\kappa_{d,k}$ is the noiseless capacity of the (d,k)-RLL constraint.

2. **Designing explicit codes over other FSCs**: While this thesis has focused primarily on coding schemes over input-constrained DMCs, it is of broad interest to design explicit codes over other channels with memory such as the Gilbert-Elliot channel (GEC). Is it possible achieve good rates over the GEC using well-known capacity-achieving (over DMCs) codes such as Reed-Muller and polar codes?

3. **Deriving asymptotic rate-distance tradeoff for constrained codes**: In Chapter 9, we derived a new LP for upper bounding the sizes of constrained codes with a given minimum Hamming distance, via a version of Delsarte's LP. Can one derive good asymptotic bounds on the rate-distance tradeoff for constrained codes, using our LP, à la the seminal work of McEliece, Rodemich, Rumsey, and Welch [104]?

References

[1] B. Burns, "History of the Atlantic cable & undersea communications". [Online]. Available: https://atlantic-cable.com

[2] B. H. Marcus, R. M. Roth, and P. H. Siegel, "An introduction to coding for constrained systems," Lecture notes. [Online]. Available: https://ronny.cswp.cs.technion.ac.il/wp-content/uploads/sites/54/2016/05/chapters1-9.pdf

[3] K. A. S. Immink, P. H. Siegel, and J. K. Wolf, "Codes for digital recorders," *IEEE Transactions on Information Theory*, vol. 44, no. 6, pp. 2260–2299, Oct. 1998.

[4] P. Sadeghi, R. A. Kennedy, P. B. Rapajic, and R. Shams, "Finite-state Markov modeling of fading channels — a survey of principles and applications," *IEEE Signal Processing Magazine*, vol. 25, no. 5, pp. 57–80, Sep. 2008.

[5] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. Cambridge University Press, 2005.

[6] R. G. Gallager, *Information Theory and Reliable Communication*. Wiley, 1968.

[7] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed. Wiley-India, 2010.

[8] C. E. Shannon, "A mathematical theory of communication," *The Bell System Technical Journal*, vol. 27, no. 3, pp. 379-423, July 1948, doi: 10.1002/j.1538-7305.1948.tb01338.x.

[9] R. Blahut, "Computation of channel capacity and rate-distortion functions," *IEEE Transactions on Information Theory*, vol. 18, no. 4, pp. 460–473, 1972.

[10] S. Arimoto, "An algorithm for computing the capacity of arbitrary discrete memoryless channels," *IEEE Transactions on Information Theory*, vol. 18, no. 1, pp. 14–20, 1972.

[11] P. O. Vontobel, A. Kavcic, D. M. Arnold, and H.-A. Loeliger, "A generalization of the Blahut-Arimoto algorithm to finite-state channels," *IEEE Transactions on Information Theory*, vol. 54, no. 5, pp. 1887–1918, May 2008.

[12] S. Shamai and Y. Kofman, "On the capacity of binary and Gaussian channels with run-length-limited inputs," *IEEE Transactions on Communications*, vol. 38, no. 5, pp. 584–594, 1990.

[13] A. Feinstein, "On the coding theorem and its converse for finite-memory channels," *Information and Control*, vol. 2, no. 1, pp. 25–44, 1959. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S001999585990066X

[14] D. Arnold, H.-A. Loeliger, P. Vontobel, A. Kavcic, and W. Zeng, "Simulation-based computation of information rates for channels with memory," *IEEE Transactions on Information Theory*, vol. 52, no. 8, pp. 3498–3508, 2006.

[15] D. Arnold and H.-A. Loeliger, "On the information rate of binary-input channels with memory," in *ICC 2001. IEEE International Conference on Communications. Conference Record (Cat. No.01CH37240)*, vol. 9, 2001, pp. 2692–2695.

[16] V. Sharma and S. K. Singh, "Entropy and channel capacity in the regenerative setup with applications to Markov channels," in *2001 IEEE International Symposium on Information Theory Proceedings*, 2001, p. 283.

[17] H. Pfister, J. Soriaga, and P. Siegel, "On the achievable information rates of finite state ISI channels," in *GLOBECOM'01. IEEE Global Telecommunications Conference (Cat. No.01CH37270)*, vol. 5, 2001, pp. 2992–2996.

[18] L. Bahl, J. Cocke, F. Jelinek, and J. Raviv, "Optimal decoding of linear codes for minimizing symbol error rate (corresp.)," *IEEE Transactions on Information Theory*, vol. 20, no. 2, pp. 284–287, 1974.

[19] G. Han, "A randomized algorithm for the capacity of finite-state channels," *IEEE Transactions on Information Theory*, vol. 61, no. 7, pp. 3651–3669, July 2015.

[20] Y. Li and G. Han, "Asymptotics of input-constrained erasure channel capacity," *IEEE Transactions on Information Theory*, vol. 64, no. 1, pp. 148–162, Jan. 2018.

[21] E. Zehavi and J. K. Wolf, "On runlength codes," *IEEE Transactions on Information Theory*, vol. 34, no. 1, pp. 45–54, Jan. 1988.

[22] G. Han and B. Marcus, "Asymptotics of input-constrained binary symmetric channel capacity," *The Annals of Applied Probability*, vol. 19, no. 3, pp. 1063–1091, 2009. [Online]. Available: https://doi.org/10.1214/08-AAP570

[23] O. Ordentlich, "Novel lower bounds on the entropy rate of binary hidden Markov processes," in *Proc. 2016 IEEE International Symposium on Information Theory (ISIT 2016)*, Barcelona, Spain, 10–15 July 2016, pp. 690–694.

[24] J. Chen and P. H. Siegel, "Markov processes asymptotically achieve the capacity of finite-state intersymbol interference channels," *IEEE Transactions on Information Theory*, vol. 54, no. 3, pp. 1295–1303, 2008.

[25] H. Permuter, P. Cuff, B. Van Roy, and T. Weissman, "Capacity of the trapdoor channel with feedback," *IEEE Transactions on Information Theory*, vol. 54, no. 7, pp. 3150–3165, July 2008.

[26] A. Wyner and J. Ziv, "A theorem on the entropy of certain binary sequences and applications–I," *IEEE Transactions on Information Theory*, vol. 19, no. 6, pp. 769–772, 1973.

[27] N. Chayat and S. Shamai, "Extension of an entropy property for binary input memoryless symmetric channels," *IEEE Transactions on Information Theory*, vol. 35, no. 5, pp. 1077–1079, 1989.

[28] A. Thangaraj, "Dual capacity upper bounds for noisy runlength constrained channels," *IEEE Transactions on Information Theory*, vol. 63, no. 11, pp. 7052–7065, Nov. 2017.

[29] V. A. Rameshwar and N. Kashyap, "Computable lower bounds for capacities of input-driven finite-state channels," in *Proc. 2020 IEEE International Symposium on Information Theory (ISIT 2020)*, virtual conference, 21–26 June 2020, pp. 2002–2007.

[30] V. S. Borkar, "Stochastic approximation with two time scales," *Systems & Control Letters*, vol. 29, no. 5, pp. 291–294, 1997. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167691197900153

[31] S. Bhatnagar, M. C. Fu, S. I. Marcus, and S. Bhatnagar, "Two-timescale algorithms for simulation optimization of hidden Markov models," *IIE Transactions*, vol. 33, no. 3, pp. 245–258, Mar 2001. [Online]. Available: https://doi.org/10.1023/A:1007611801240

[32] J. K. Wolf, "Invited talk on the magnetic recording channel," 26$^{\text{th}}$ Annual Allerton Conference, Sep. 1988.

[33] K. A. S. Immink, "Runlength-limited sequences," *Proceedings of the IEEE*, vol. 78, no. 11, pp. 1745–1759, 1990.

[34] A. M. Fouladgar, O. Simeone, and E. Erkip, "Constrained codes for joint energy and information transfer," *IEEE Transactions on Communications*, vol. 62, no. 6, pp. 2121–2131, 2014.

[35] E. Arikan, "Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels," *IEEE Transactions on Information Theory*, vol. 55, no. 7, pp. 3051–3073, 2009.

[36] S. Kudekar, S. Kumar, M. Mondelli, H. D. Pfister, E. Sasoglu, and R. L. Urbanke, "Reed-Muller codes achieve capacity on erasure channels," *IEEE Transactions on Information Theory*, vol. 63, no. 7, pp. 4298–4316, 2017.

[37] M. G. Luby, M. Mitzenmacher, M. A. Shokrollahi, and D. A. Spielman, "Efficient erasure correcting codes," *IEEE Transactions on Information Theory*, vol. 47, no. 2, pp. 569–584, 2001.

[38] T. J. Richardson, M. A. Shokrollahi, and R. L. Urbanke, "Design of capacity-approaching irregular low-density parity-check codes," *IEEE Transactions on Information Theory*, vol. 47, no. 2, pp. 619–637, 2001.

[39] S. Kudekar, T. Richardson, and R. L. Urbanke, "Spatially coupled ensembles universally achieve capacity under belief propagation," *IEEE Transactions on Information Theory*, vol. 59, no. 12, pp. 7761–7813, 2013.

[40] G. Reeves and H. D. Pfister, "Reed-Muller codes achieve capacity on BMS channels," arXiv:2110.14631, Oct. 2021.

[41] E. Abbe and C. Sandon, "A proof that Reed-Muller codes achieve Shannon capacity on symmetric channels," *arXiv e-prints*, p. arXiv:2304.02509, Apr. 2023.

[42] W. G. Bliss, "Circuitry for performing error correction calculations on baseband encoded data to eliminate error propagation," *IBM Technical Disclosure Bulletin*, vol. 23, pp. 4633–4634, 1981. [Online]. Available: https://cir.nii.ac.jp/crid/1570009751553045248

[43] M. Mansuripur, "Enumerative modulation coding with arbitrary constraints and postmodulation error correction coding for data storage systems," in *Optical Data Storage '91*, J. J. Burke, T. A. Shull, and N. Imamura, Eds. Society of Photo-Optical Instrumentation Engineers (SPIE) Conference Series, 1991, vol. 1499, pp. 72–86.

[44] K. Immink, "A practical method for approaching the channel capacity of constrained channels," *IEEE Transactions on Information Theory*, vol. 43, no. 5, pp. 1389–1399, 1997.

[45] J. Fan and A. Calderbank, "A modified concatenated coding scheme, with applications to magnetic data storage," *IEEE Transactions on Information Theory*, vol. 44, no. 4, pp. 1565–1574, 1998.

[46] J. Campello de Souza, B. Marcus, R. New, and B. Wilson, "Constrained systems with unconstrained positions," *IEEE Transactions on Information Theory*, vol. 48, no. 4, pp. 866–879, 2002.

[47] A. Patapoutian and P. Kumar, "The (d, k) subcode of a linear block code," *IEEE Transactions on Information Theory*, vol. 38, no. 4, pp. 1375–1382, 1992.

[48] I. Tal, H. D. Pfister, A. Fazeli, and A. Vardy, "Polar codes for the deletion channel: weak and strong polarization," *IEEE Transactions on Information Theory*, vol. 68, no. 4, pp. 2239–2265, 2022.

[49] E. Sasoglu and I. Tal, "Polar coding for processes with memory," *IEEE Transactions on Information Theory*, vol. 65, no. 4, pp. 1994–2003, 2019.

[50] Y. Li and V. Y. F. Tan, "On the capacity of channels with deletions and states," *IEEE Transactions on Information Theory*, vol. 67, no. 5, pp. 2663–2679, 2021.

[51] J. B. Soriaga, H. D. Pfister, and P. H. Siegel, "Determining and approaching achievable rates of binary intersymbol interference channels using multistage decoding," *IEEE Transactions on Information Theory*, vol. 53, no. 4, pp. 1416–1429, 2007.

[52] E. Abbe, A. Shpilka, and M. Ye, "Reed-Muller codes: Theory and algorithms," *IEEE Transactions on Information Theory*, vol. 67, no. 6, pp. 3251–3277, 2021.

[53] E. Abbe, A. Shpilka, and A. Wigderson, "Reed-Muller codes for random erasures and errors," *IEEE Transactions on Information Theory*, vol. 61, no. 10, pp. 5229–5252, 2015.

[54] T. Kaufman, S. Lovett, and E. Porat, "Weight distribution and list-decoding size of Reed-Muller codes," *IEEE Transactions on Information Theory*, vol. 58, no. 5, pp. 2689–2696, 2012.

[55] O. Sberlo and A. Shpilka, "On the performance of Reed-Muller codes with respect to random errors and erasures," in *Proc. 31st Annual ACM-SIAM Symposium on Discrete Algorithms (SODA'20)*, Salt Lake City, Utah, USA, 2020, pp. 1357–1376.

[56] A. Rao and O. Sprumont, "On list decoding transitive codes from random errors," 2022. [Online]. Available: https://homes.cs.washington.edu/~anuprao/pubs/rmlist.pdf

[57] R. Roth, *Introduction to Coding Theory*. Cambridge University Press, 2006.

[58] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, 2nd ed. North-Holland, 1978.

[59] E. Abbe, O. Sberlo, A. Shpilka, and M. Ye, "Reed-Muller codes," *Foundations and Trends® in Communications and Information Theory*, vol. 20, no. 1–2, pp. 1–156, 2023. [Online]. Available: http://dx.doi.org/10.1561/0100000123

[60] V. A. Rameshwar and N. Kashyap, "On the performance of Reed-Muller codes over (d, ∞)-RLL input-constrained BMS channels," in *Proc. 2022 IEEE International Symposium on Information Theory (ISIT 2022)*, June 26 – July 1, 2022.

[61] G. Lechner, I. Land, and A. Grant, "Linear and non-linear run length limited codes," *IEEE Communications Letters*, vol. 19, no. 7, pp. 1085–1088, Jul. 2015.

[62] A. Samorodnitsky, "An upper bound on ℓ_q norms of noisy functions," *IEEE Transactions on Information Theory*, vol. 66, no. 2, pp. 742–748, 2020.

[63] Y. Li and G. Han, "Asymptotics of input-constrained erasure channel capacity," *IEEE Transactions on Information Theory*, vol. 64, no. 1, pp. 148–162, Jan. 2018.

[64] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*. Cambridge University Press, 2003.

[65] R. Diestel, *Graph Theory*, 5th ed. Springer, 2017.

[66] S. Kudekar, S. Kumar, M. Mondelli, H. D. Pfister, and R. Urbanke, "Comparing the bit-MAP and block-MAP decoding thresholds of Reed-Muller codes on BMS channels," in *Proc. 2016 IEEE International Symposium on Information Theory (ISIT 2016)*, Barcelona, Spain, 10–15 July 2016, pp. 1755–1759.

[67] R. Adler, D. Coppersmith, and M. Hassner, "Algorithms for sliding block codes – an application of symbolic dynamics to information theory," *IEEE Transactions on Information Theory*, vol. 29, no. 1, pp. 5–22, 1983.

[68] M. Mushkin and I. Bar-David, "Capacity and coding for the Gilbert-Elliott channels," *IEEE Transactions on Information Theory*, vol. 35, no. 6, pp. 1277–1290, 1989.

[69] R. Durrett, *Probability: Theory and Examples*, 5th ed. Cambridge University Press, 2019.

[70] R. O'Donnell, *Analysis of Boolean Functions*. Cambridge University Press, 2014.

[71] J. MacWilliams, "A theorem on the distribution of weights in a systematic code," *The Bell System Technical Journal*, vol. 42, no. 1, pp. 79–94, 1963.

[72] B. Marcus and P. Siegel, "On codes with spectral nulls at rational submultiples of the symbol frequency," *IEEE Transactions on Information Theory*, vol. 33, no. 4, pp. 557–568, 1987.

[73] G. Pierobon, "Codes for zero spectral density at zero frequency (corresp.)," *IEEE Transactions on Information Theory*, vol. 30, no. 2, pp. 435–439, 1984.

[74] A. Tandon, M. Motani, and L. R. Varshney, "Subblock-constrained codes for real-time simultaneous energy and information transfer," *IEEE Transactions on Information Theory*, vol. 62, no. 7, pp. 4212–4227, 2016.

[75] S. Zhao, "A serial concatenation-based coding scheme for dimmable visible light communication systems," *IEEE Communications Letters*, vol. 20, no. 10, pp. 1951–1954, 2016.

[76] Y. M. Chee, H. M. Kiah, and P. Purkayastha, "Matrix codes and multitone frequency shift keying for power line communications," in *2013 IEEE International Symposium on Information Theory*, 2013, pp. 2870–2874.

[77] H. Yao, A. Fazeli, and A. Vardy, "A deterministic algorithm for computing the weight distribution of polar codes," in *2021 IEEE International Symposium on Information Theory (ISIT)*, 2021, pp. 1218–1223.

[78] C. Shannon, "The zero error capacity of a noisy channel," *IRE Trans. Inf. Theory*, vol. 2, no. 3, pp. 8–19, 1956.

[79] F. Alajaji, "Feedback does not increase the capacity of discrete channels with additive noise," *IEEE Transactions on Information Theory*, vol. 41, no. 2, pp. 546–549, 1995.

[80] J. L. Massey, "Causality, feedback and directed information," in *Proc. 1990 International Symposium on Information Theory and its Applications*, 1990, pp. 27–30.

[81] S. C. Tatikonda, "Control under communication constraints," Ph.D. dissertation, MIT, Cambridge, MA, 2000.

[82] S. Yang, A. Kavcic, and S. Tatikonda, "Feedback capacity of finite-state machine channels," *IEEE Transactions on Information Theory*, vol. 51, no. 3, pp. 799–810, 2005.

[83] A. Arapostathis, V. S. Borkar, E. Fernandez-Gaucherand, M. K. Ghosh, and S. Marcus, "Discrete time controlled Markov processes with average cost criterion — a survey," *SIAM Journal on Control and Optimization*, vol. 31, no. 2, pp. 282–344, 1993.

[84] H. H. Permuter, T. Weissman, and A. J. Goldsmith, "Finite state channels with time-invariant deterministic feedback," *IEEE Transactions on Information Theory*, vol. 55, no. 2, pp. 644–662, 2009.

[85] H. Permuter, P. Cuff, B. Van Roy, and T. Weissman, "Capacity of the trapdoor channel with feedback," *IEEE Transactions on Information Theory*, vol. 54, no. 7, pp. 3150–3165, 2008.

[86] O. Elishco and H. Permuter, "Capacity and coding for the Ising channel with feedback," *IEEE Transactions on Information Theory*, vol. 60, no. 9, pp. 5138–5149, 2014.

[87] J. Wu and A. Anastasopoulos, "On the capacity of the chemical channel with feedback," in *2016 IEEE International Symposium on Information Theory (ISIT)*, 2016, pp. 295–299.

[88] O. Sabag, H. H. Permuter, and N. Kashyap, "The feedback capacity of the binary erasure channel with a no-consecutive-ones input constraint," *IEEE Transactions on Information Theory*, vol. 62, no. 1, pp. 8–22, Jan. 2016.

[89] O. Sabag, H. H. Permuter, and N. Kashyap, "Feedback capacity and coding for the BIBO channel with a no-repeated-ones input constraint," *IEEE Transactions on Information Theory*, vol. 64, no. 7, pp. 4940–4961, 2018.

[90] O. Peled, O. Sabag, and H. H. Permuter, "Feedback capacity and coding for the $(0,k)$-RLL input-constrained BEC," *IEEE Transactions on Information Theory*, vol. 65, no. 7, pp. 4097–4114, 2019. [Online]. Available: https://doi.org/10.1109/TIT.2019.2903252

[91] O. Sabag, H. H. Permuter, and H. D. Pfister, "A single-letter upper bound on the feedback capacity of unifilar finite-state channels," *IEEE Transactions on Information Theory*, vol. 63, no. 3, pp. 1392–1409, March 2017.

[92] O. Sabag, B. Huleihel, and H. H. Permuter, "Graph-based encoders and their performance for finite-state channels with feedback," *IEEE Transactions on Communications*, vol. 68, no. 4, pp. 2106–2117, 2020.

[93] O. Shayevitz and M. Feder, "Optimal feedback communication via posterior matching," *IEEE Transactions on Information Theory*, vol. 57, no. 3, pp. 1186–1222, 2011.

[94] V. A. Rameshwar and N. Kashyap, "Bounds on the feedback capacity of the (d,∞)-RLL input-constrained binary erasure channel," *2021 IEEE International Symposium on Information Theory (ISIT)*. [Online]. Available: https://arxiv.org/abs/2101.08638.

[95] B. Huleihel, O. Sabag, and H. H. Permuter, "Capacity of the trapdoor channel with delayed feedback," in *2022 IEEE International Symposium on Information Theory (ISIT)*, 2022, pp. 492–497.

[96] H. Ferreira, "Lower bounds on the minimum Hamming distance achievable with runlength constrained or DC free block codes and the synthesis of a (16,8) Dmin= 4 DC free block code," *IEEE Transactions on Magnetics*, vol. 20, no. 5, pp. 881–883, 1984.

[97] J. Luo and T. Helleseth, "Constant composition codes as subcodes of cyclic codes," *IEEE Transactions on Information Theory*, vol. 57, no. 11, pp. 7482-7488, Nov. 2011, doi: 10.1109/TIT.2011.2161631.

[98] V. Kolesnik and V. Krachkovsky, "Generating functions and lower bounds on rates for limited error-correcting codes," *IEEE Transactions on Information Theory*, vol. 37, no. 3, pp. 778–788, 1991.

[99] B. Marcus and R. Roth, "Improved Gilbert-Varshamov bound for constrained systems," *IEEE Transactions on Information Theory*, vol. 38, no. 4, pp. 1213–1221, 1992.

[100] D. Cullina and N. Kiyavash, "Generalized sphere-packing bounds on the size of codes for combinatorial channels," *IEEE Transactions on Information Theory*, vol. 62, no. 8, pp. 4454–4465, 2016.

[101] A. A. Kulkarni and N. Kiyavash, "Nonasymptotic upper bounds for deletion correcting codes," *IEEE Transactions on Information Theory*, vol. 59, no. 8, pp. 5115–5130, 2013.

[102] A. Fazeli, A. Vardy, and E. Yaakobi, "Generalized sphere packing bound," *IEEE Transactions on Information Theory*, vol. 61, no. 5, pp. 2313–2334, 2015.

[103] P. Delsarte, "An algebraic approach to the association schemes of coding theory," vol. 10, Philips Research Reports, Supplements, 1973.

[104] R. McEliece, E. Rodemich, H. Rumsey, and L. Welch, "New upper bounds on the rate of a code via the Delsarte-MacWilliams inequalities," *IEEE Transactions on Information Theory*, vol. 23, no. 2, pp. 157–166, 1977.

[105] J. Friedman and J.-P. Tillich, "Generalized Alon–Boppana theorems and error-correcting codes," *SIAM Journal on Discrete Mathematics*, vol. 19, no. 3, pp. 700–718, 2005. [Online]. Available: https://doi.org/10.1137/S0895480102408353

[106] M. Navon and A. Samorodnitsky, "Linear programming bounds for codes via a covering argument," *Discrete & Computational Geometry*, vol. 41, no. 2, pp. 199–207, Mar 2009. [Online]. Available: https://doi.org/10.1007/s00454-008-9128-0

[107] L. N. Coregliano, F. G. Jeronimo, and C. Jones, "A complete linear programming hierarchy for linear codes," in *Information Technology Convergence and Services*, 2022.

[108] E. Loyfer and N. Linial, "New LP-based upper bounds in the rate-vs.-distance problem for linear codes," *arXiv e-prints*, p. arXiv:2206.09211, Jun. 2022.

[109] F. Margot, "Exploiting orbits in symmetric ILP," *Mathematical Programming*, vol. 98, no. 1, pp. 3–21, Sep 2003. [Online]. Available: https://doi.org/10.1007/s10107-003-0394-6

[110] H. M. Kiah, A. Tandon, and M. Motani, "Generalized sphere-packing bound for subblock-constrained codes," *IEEE Transactions on Information Theory*, vol. 67, no. 1, pp. 187–199, 2021.

[111] P. Flajolet and R. Sedgewick, *Analytic Combinatorics*, 1st ed. USA: Cambridge University Press, 2009.

[112] OEIS Foundation Inc. (2022). The On-Line Encyclopedia of Integer Sequences. [Online]. Available: http://oeis.org

[113] Answer by user Clement C. to "Asymptotic growth of a convolution (counting n-bead 2-colour necklaces)". [Online]. Available: https://math.stackexchange.com/questions/1979352/asymptotic-growth-of-a-convolution-counting-n-bead-2-colour-necklaces