ASYMPTOTIC ANALYSIS OF TURBO-LIKE CODES.

Average spectra and minimum distances

ASYMPTOTIC ANALYSIS OF TURBO-LIKE CODES.
Average spectra and minimum distances

Chiara Ravazzi

Submitted for the degree of Doctor of Philosophy
POLITO - Politecnico di Torino

Abstract

The topic of this dissertation falls within channel coding theory, and consists in the analysis of a particular class of turbo-like codes, defined by a multiple concatenation of an arbitrary outer encoder with m truncated convolutional encoders through uniform random permutations.

Fixed the number of inner encoders, structural properties of these coding schemes are studied when the truncation length goes to infinity.

As a first step in this study, we focus on truncated convolutional encoders, which are the constituent elements of turbo concatenations. We present a detailed analysis of the related weight distribution functions and of their exponential growth rate. In particular, the weight distribution functions are expressed as coefficients of the generating function of error events associated with a minimal realization of the encoder. Although these expressions can be computed for relatively small truncation lengths, they become prohibitively complex to compute as truncation lengths and weights increase. Fortunately, a very accurate approximation can be derived using the Multidimensional Saddle Point method. This approximation is substantially easier to evaluate and is used to obtain an expression for the asymptotic spectral function and to prove continuity and concavity. Finally, this approach is able to guarantee that the sequence of exponential growth rate converges uniformly to the asymptotic limit and to estimate the speed of this convergence.

Building upon these results, we show that for multiple concatenated coding schemes the average distance spectra can be obtained through the analysis of a dynamical system (dependent on the inner encoder) with initial condition equal to the asymptotic spectra of the outer encoder. Moreover, they are equal to 0 below a threshold distance δ_m and positive beyond it. Then, minimum distances are shown to scale linearly in the code-length with probability one, and the asymptotic normalized minimum distance to be exactly provided by δ_m. Under a very mild condition on the outer encoder asymptotic spectral functions form a uniformly convergent sequence of functions. Their limit is the maximum between 0 and the average spectral shape of the random linear coding ensemble. As a consequence, the threshold sequence δ_m converges to the Gilbert-Varshamov distance, the best lower bound on the largest minimum distance achievable by a code.

Finally, we consider another family of binary codes that can be seen both as particular systematic serial turbo codes and as structured Low-Density Parity-Check codes. Using similar techniques, we analyze minimum distances and prove coding theorems, already obtained for multiple serially concatenated codes, even in this new setting. Summarizing theoretical results, we describe some guidelines to design asymptotically good coding schemes.

Keywords: Asymptotic spectral functions, convolutional encoders, Gilbert–Varshamov distance, multiple serially concatenated codes, turbo like-codes, uniform random permutations.

Acknowledgements

During my Ph.D I have benefited from the help of many people.

Most hearty thanks go to Prof. Fabio Fagnani, who proved to be a great supervisor. Most of this work is due to his outstanding advice and support. Moreover, it is difficult to imagine how these three years would have been without his enthusiasm, patience and personal friendliness.

I also wish to thank Prof. Rudiger Urbanke, who came to Torino to teach a very interesting class, and who taught me Hayman-like techniques, and Prof. H. Pfister for sharing material and ideas. I would like express my sincere gratitude to Prof. Igal Sason for his valuable suggestions and his help in the draft of my first article.

Prof. Devavrat Shah has provided many inputs to my research and a very enjoyed experience visiting Massachussets Institute of Technology. The semester I spent there has been an exciting opportunity to attend classes and seminars from world-renown professors, and to be a member of a big and active research group. Related thanks are due mainly to Prof. Fabio Fagnani and Riccardo Zecchina for making this stay possible.

I am grateful to Professors Valentina Casarino, Fabio Fagnani and Anita Tabacco for the teaching assistant opportunities they have given me.

A special thanks goes to Giacomo, who made me have fun during my stay in Boston and has shared with me conferences and seminars. I would like also thank Federica Garin for his help in the analysis of structured LDPC codes and the entire research group Domenica Borra, Paolo Frasca and Sophie Fosson for interesting discussions and nice lunches toghether. A big hug to Francesco Longo and Valentina Martina for their support and encouragement.

I really would like to express my gratitude to my parents, Renata and Piercarlo, to Stefania, Andrea and Marta, who make me feel so happy with their love.

Finally, the most inspiring suggestions and fundamental support – even during the frustrating weeks of my Ph.D. devoted to write this thesis – have come from Marco, whom I deeply thank.

Major financial support has been provided by Istituto Nazionale di Alta Matematica Francesco Severi (GNAMPA), IEEE, Fondazione Banca di Intra.

Contents

List of Figures

Notational convention

Symbol	Definition
$\omega \in \Omega$	ω is an element of Ω
$\omega \notin \Omega$	ω does not belong to the set Ω
$\Omega \subseteq \Theta$	Ω is included in Θ
$\Theta \setminus \Omega$	Set of elements in Θ but not in Ω
$\lvert\Omega\rvert$	Cardinality of the set Ω
$\mathbb{1}_\Omega$	Indicator function
$\mathbb{Z}_2$	Galois field with two elements
$\mathbb{N}$	Set of natural numbers
$\mathbb{N}_0$	Set of natural numbers with zero
$\mathbb{Z}$	Set of integer numbers
$\mathbb{Q}$	Set of rational numbers
$\mathbb{R}$	Set of real numbers
$\mathbb{R}_+$	Set of non-negative numbers
$\mathbb{R}^+$	Set of positive numbers
$[N]$	Sequence of integers from 1 to $N \in \mathbb{N}$
$\lfloor x \rfloor$	Integer part of real number x
$\lceil x \rceil$	smallest integer greater than real number x
$\lvert x\rvert$	Absolute value of x
$a \vee b$	Maximum between real values a and b
$a \wedge b$	Minimum between real values a and b
$\mathrm{lcm}(a, b)$	Least common multiple of real values a and b
$\mathbb{C}$	Set of complex number
z^*	Conjugate of complex number z
j	Unit imaginary part $\sqrt{-1}$

Symbol	Definition
$\mathbb{R}^n$	Vector space of real-valued n-dimensional vectors
$\|\|\boldsymbol{x}\|\|_2$	Euclidean norm of vector $\boldsymbol{x}$
$\|\|\boldsymbol{x}\|\|_1$	L^1 norm of vector $\boldsymbol{x}$
$\mathrm{supp}(\boldsymbol{x})$	Support of vector $\boldsymbol{x}$
$\overset{\circ}{\Omega}$	Interior of set $\Omega \subseteq \mathbb{R}^n$
$\overline{\Omega}$	Closure of set $\Omega \subseteq \mathbb{R}^n$
$\mathrm{co}(\Omega)$	Convex hull of set $\Omega \subseteq \mathbb{R}^n$
$\mathbf{A}^T$	Transpose of matrix $\mathbf{A}$
$\mathbf{A}^{-1}$	Inverse of matrix $\mathbf{A}$
$\|\mathbf{A}\|$	Determinant of matrix $\mathbf{A}$
$\langle \boldsymbol{x}, \boldsymbol{y} \rangle$	Scalar product of complex vectors $\boldsymbol{x}$ and $\boldsymbol{y}$
$\boldsymbol{x} \cdot \boldsymbol{y}$	Pointwise product of real vectors $\boldsymbol{x}$ and $\boldsymbol{y}$
$\boldsymbol{x}^{\boldsymbol{k}}$	$\prod_{i \in \mathrm{supp}(\boldsymbol{x})} x_i^{k_i}$
$\mathrm{coeff}\{F(\boldsymbol{x}), \boldsymbol{x}^{\boldsymbol{k}}\}$	Coefficient of $\boldsymbol{x}^{\boldsymbol{k}}$ in power series $F(\boldsymbol{x})$
$F_{\boldsymbol{k}}$	Coefficient of $\boldsymbol{x}^{\boldsymbol{k}}$ in power series $F(\boldsymbol{x})$
$\mathrm{Im}(\psi)$	Image of the map ψ
$\mathbb{R}[x]$	Set of polynomials with coefficient in $\mathbb{R}$
$\mathrm{ldeg}(P(x))$	least degree of polynomial $P(x)$
$\deg(P(x))$	Degree of polynomial $P(x)$

Introduction 1

Brief—This chapter gives an introductory view of the motivations that lead to begin this thesis project. A brief introduction about the main subject that this thesis deals with, namely channel coding theory, and a brief state of the art about the relevant topics are included too. This chapter should help the reader to understand what are the phenomena, the mathematical tools addressed and the main contributions in this thesis.

1.1 Outline of the chapter

The purpose of the present chapter is to give an overview of the dissertation. This is also an opportunity to loosely define some fundamental notions and some vocabulary.

Section 1.2 introduces the concepts of channel coding, the most popular coding schemes, and some ways to compare them. Section 1.3 deals with serial turbo-coding schemes: it broadly reviews problems and solutions known in the literature (more detailed literature reviews per topic can be found in the main body of the dissertation) and summarizes the main contributions in this document. Section 1.4 illustrates the organization of next chapters. A list of publications presenting the results of this work concludes the chapter (see Section 1.5).

1.2 Coding theory

1.2.1 State of the art

Aim of communication engineering is to design systems for efficient and reliable transmission of data over a noisy channel. A channel is a physical medium linking a source and a receiver which are separated in space or perhaps in time.

Typically, because of noise, the received message is a distorted version of the corresponding source message. The receiver needs to estimate the transmitted message starting from the observations of the channel output, by using some decoding strategies. Channel coding theory is the study of how to add redundancy to a source message so it can be decoded correctly, even when the communication channel is noisy.

Figure 1.1 depicts a generic coding–decoding scheme. The source emits a message of length k, called *information word* or *information sequence*. We assume from now on that each possible message k-tuple is as likely to be selected for broadcast as any other.

The encoder maps information words into binary messages of length n (with $n > k$) deterministically. These blocks are the *codewords* or *code sequences*. From the assumption of uniform prior on the source message we clearly have that each codeword from the code (the set of all possible codewords) is as likely to be transmitted as any other.

The message is sent on a memoryless channel, which corrupts the sequence with random noise. The channel has no memory, in the sense that an error in one symbol does not affect the reliability of its neighboring symbols.

Finally, the decoder receives from the channel an n-tuple of symbols and estimates the transmitted message. The goodness of a coding–decoding scheme is measured by the probability that the decoded sequence is different from the transmitted message.

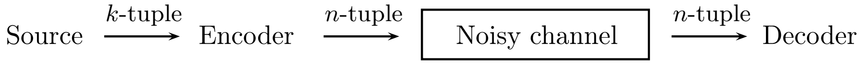


Figure 1.1: Mathematical model for communication. First, the encoder adds some redundancy to the source message. The resulting codeword is sent over the channel. Finally, the decoder estimates the original message.

It is clear that error probability can be made arbitrarily small by adding more and more redundancy, and letting the ratio of the lengths of information words and corresponding codewords (called rate $R = k/n$) go to zero. However, to be efficient, the transfer of information must not require a prohibitive amount of time and effort. A more efficient and reliable approach to the problem is contained in the Shannon's pioneering works [1–3]. Shannon points out that the error probability can be made arbitrarily small by adding bounded redundancy (without sacrificing data rates), at the price of increasing the code complexity.

The novelty of his work consists in the use of the probabilistic method for proving coding theorems [4]. In fact, the analysis concerns an ensemble of codes, namely sets of codes equipped with a probability measure, instead of considering single coding schemes. Through this probabilistic approach, it is showed that, whenever the design rate is below a threshold (capacity of the channel) and under the assumption of maximum likelihood decoding (MLD, which prescribes to choose the most likely codeword), the average error probability vanishes in the limit of large codewords lengths with exponential decaying error rate. Unfortunately, Shannon's theorem does not give any practical technique to construct a good code. The averaging technique, used in the proof, suggests to choose 2^k codewords of length n randomly. However random constructed codes have unfeasible complexity in the decoding process, which requires exponential time in the codewords length. After Shannon, coding theory attempts to realize the promise of these bounds by models which are constructed mainly through algebraic techniques.

In order to define codes with an efficient encoding and decoding complexity, we have to add more structure to the codespace. Block linear codes and convolutional codes are examples of codes based on a simple algebraic structure.

Block linear codes are defined as the image of a generator matrix or as the kernel of a parity check matrix (called also syndrome matrix). The reader is referred to [5] for further details.

Convolutional codes and trellis codes are encoders with memory [6–8]. Convolutional encoders can be seen as finite-state machines with linear update of the state and of the output. The code sequence that emerges from the encoder depends upon previous message symbols as well as the present ones. Moreover, the code string emerges continuously rather than segmented into unrelated blocks.

However, performance of these structured codes are far away from the theoretical limits, which remained practically unreachable for a long time.

A major breakthrough in the discipline comes with the introduction of turbo codes, introduced in 1993 in [9, 10], and Low-Density Parity-Check (LDPC) codes, introduced in 1963 by Gallager [11] and deeply studied after re-discovering [12] in 1995. In particular, the amazing success comes from a good balance in the coding scheme between enough randomness —in order to get good performances (close to that of randomly constructed codes)— and enough structure —to be exploited by a suitable low-complexity decoding algorithm, known as belief propagation (BP) [13, 14].

Classical turbo codes are obtained by concatenating two simple convolutional encoders in a parallel way, linked by an interleaver: the information bits to the first encoder are scrambled by the interleaver before entering the second one; then codewords are obtained by juxtaposing the output bits of both encoders. This construction can be generalized to any number of constituent codes. The iterative algorithm, which decodes each code separately and exchange information from one decoder to the other, reaches good performance, close to the theoretical limits, with complexity comparable to that of the constituent codes [15, 16].

Since the introduction of the classical turbo codes, many variations of the basic scheme have been proposed in the literature. Serially concatenated codes through interleaver are introduced in [17]. Moreover, the use of these coding schemes in combination with an ad-hoc iterative decoding makes them interesting from an applicative point of view. Interconnections of more than two encoders through more than one interleaver both in a serial structure or in a mixed serial and parallel way, known as turbo-like schemes, have been considered in [18–20].

LDPC codes are error-correcting codes defined in terms of a sparse matrix (the parity-check matrix), i.e. binary matrix containing a small amount of non-zero entries. Typically, by very few non-zero entries we mean that, as the codeword length increases, the number of non-zero entries grows linearly with it. LDPC matrix can be represented by a sparse bipartite graph, i.e., a graph with very few edges.

Although LDPC codes achieve good performance under ML-decoding, it can be shown that in the worst-case, ML decoding of an LDPC code is NP-hard, so ML decoding of LDPC codes is likely to be quite complex. By exploiting the graphical representation of LDPC codes, a low complexity suboptimal message-passing algorithm for decoding is proposed in [11]. At each round of the algorithm messages are passed from vertices in the factor graph to their neighbors. These messages are updated iteratively using local update rules (by local, we mean that the updated message leaving a vertex depends only on the messages coming into that vertex at the previous iteration). The reader is referred to [21] for a more detailed exposition of message-passing algorithms.

Despite their linear decoding complexity, the encoding process of LDPC codes requires in general the multiplication of the input vector times the generating matrix, which is not sparse. There is no known linear time algorithm for encoding a general LDPC code (LDPC codes are linear codes, so these codes must be encodable in polynomial time). On the contrary, for turbo-like codes, the constituent encoders are usually convolutional encoders, whose encoding complexity is linear in the length.

To improve the encoding complexity, one can consider codes that share many properties with LDPC codes, but which also have additional structure (called structured LDPC). Some successful constructions are Repeat-Accumulate codes and their generalization, the Irregular Repeat-Accumulate (IRA) codes introduced in [22, 23]. This class of codes can be interpreted as serial turbo scheme, obtained by coupling an outer low-density generator matrix (LDGM) code with an inner convolutional encoder. As it happens for turbo codes, the encoding process requires linear time. At the same time, the graphical structure of these codes looks similar to that of LDPC codes, so practical decoding algorithms can be used.

There are different ways to compare coding schemes and different criteria can be used to optimize their performance. On the one side, analysis can focus on intrinsic properties of the codes, and on the other side on properties of decoding strategies. In this dissertation we focus on the first approach, by using the minimum distance as fundamental design parameter. Most of the results of this thesis concern the minimum distance analysis of turbo-code ensembles.

1.2.2 Design criteria: minimum distance analysis

Much of classical coding theory is aimed at the construction of codes with large minimum distance. Minimum distance is defined as the smallest distance between distinct codewords, measured by Hamming distance (i.e. number of positions in which two sequences differ). The minimum distance of a code gives a measure of how good it is at detecting and correcting errors, since a code with minimum distance d can detect up to $d-1$ errors or correct up to $\lfloor (d-1)/2 \rfloor$ errors in any codeword. Moreover, minimum distance dominates the ML error probability at high signal-to-noise ratio (SNR). The fundamental idea to construct good codes is to separate as much as possible its codewords: codewords which are far apart (in the Hamming distance sense) among each other will have small probability of being mutually equivocated, when transmitted over a noisy channel. In general, different codes can be compared in terms of their tradeoff between rate and minimum distance, and design criteria can be optimized. In the case of binary linear encoders the minimum distance coincides with minimum Hamming weight of their non-null codewords (i.e. the number of non-zero elements in the sequence). From now on we will consider to encode the information with a linear encoder.

When assuming a maximum likelihood decoding, the performance is also influenced by code sequences with higher weight. Another interesting study of the intrinsic properties of codes concerns the weight distribution. The weight enumerators of a binary linear code specify the number of words with a given input and output Hamming weight. They are the main ingredient of all expressions estimating error probabilities and characterize the correction capability of the code. The estimation of weight distributions of codes is a crucial issue in coding theory and there exists an extensive literature on bounds on weight distributions and on their use. We refer the reader to [24, 25]. A particular relevant part is to estimate the spectral function of weight enumerators, namely their exponential growth rate when the code length goes to infinity. Spectral functions provide important asymptotic information on the codes, including their minimum distances.

In order to construct codes achieving Shannon limit, it is mandatory to ensure that their minimum distance does not remain bounded as codewords length grows. Moreover, if we want to design codes with exponential decaying error probability rate, minimum distance has to grow at least linearly in codewords length. A sequence of codes of increasing length is called *an asymptotically good code* if the message length and the minimum distance of the codes grows linearly with the codewords length. Codes for which minimum distances do not grow linearly with the code length are called *asymptotically bad*.

Despite decades of research the best trade-off between rate and distance is unknown for binary codes. For fixed rate, a lower bound on the achievable minimum Hamming distance of binary codes is given by Gilbert and Varshamov bound [26] and then improved in [27, 28]. The proof of this bound is based on a greedy algorithm (with exponential complexity in the code length) to construct such a code.

It is well-known that a random linear code almost matches the GV-bound with high probability, so such linear codes exist in abundance [29, 30]. Then, we could in principle pick a random linear code and then check its minimum distance. However, the random coding ensemble is only of theoretical interest. Finding a deterministic polynomial time construction of a code that meets the GV bound remains an open question.

While a random constructed codes have little structure, there are more structured ensemble of linear codes, which meet the GV-bound asymptotically. Example are binary linear concatenated codes with Reed-Solomon outer codes [31] and random double circulant codes, introduced by Kasami in [32].

A huge literature focuses on the study of the minimum distance distribution of turbo-like codes, LDPC codes with their variants. In general, the minimum distance analysis of these codes is not a trivial issue. However, it has been realized that the probabilistic method is useful to prove coding theorems. In order to prove the existence of a coding scheme with certain properties, a probability space is constructed (code ensemble) and then it is shown that a randomly chosen code from this space satisfies the desired properties with high probability.

For turbo like codes minimum distance distribution is studied by considering a uniform probability distribution over the set of all permutations (uniform interleavers). Results along these lines are in [33–38]. In particular for classical turbo codes minimum distances can grow at most logarithmically with the code length, while for classical serial concatenated codes (just two convolutional encoders interconnected with an interleaver) better scaling laws of minimum distances can be achieved (close to linear).

The probabilistic method is used also in the analysis of LDPC codes, as done for turbo-like coding schemes. The classical family of LDPC, considered by Gallager, has a parity-check matrix chosen uniformly at random among all matrices with fixed number of ones per each row and column. Irregular families have been then introduced in [39]. For LDPC codes, the study of the minimum distance has been considered in [39–43]. In particular, the growth rate of the minimum distance, i.e., whether this growth rate is linear in the code length or merely sublinear, depends exlusively on a quantity which is related to the distribution of ones in the parity-check matrix.

1.3 Multiple serial turbo-coding ensembles

The topic of this thesis falls within classical channel coding theory, and consists in the analysis of a particular class of turbo-like codes, defined by a multiple concatenation of an arbitrary outer encoder with m truncated convolutional encoders (block encoders obtained by considering the inputs and the output supported in N trellis steps) through uniform random permutations. This thesis mainly consists in the development of mathematical tools to study asymptotic properties of average weight distribution and repartition function of the minimum normalized distance.

1.3.1 Previous literature

In the theoretical analysis of the minimum distance distribution of multiple serially concatenated codes we can distinguish two main lines: on the one side, we take the truncation length N fixed and we let m go to infinity; on the other side, we study the minimum distance as a function of code length for a finite number of interconnections in the serial structure.

Using the first approach, H. Pfister and P. Siegel [44] undertake a first analysis of average output weight enumerating function. In particular, they show that these functions converge to that one of the random linear coding ensemble. In Chapter 4 we will prove that this study implies that there exists a sequence of asymptotically good codes in the ensemble with minimum distance close to the GV-bound but it does not guarantee that this happens for all codes in the ensemble. This difficulty is mathematically due to the fact that the two limits for $m \to \infty$ and $n \to \infty$ can not be interchanged automatically.

In this dissertation, we will focus on the second approach.

The case with $m = 1$, which encompasses the serial turbo scheme (just two convolutional codes interconnected by an interleaver [17]), is analyzed in [36]. There, it is proved that such codes are asymptotically bad: typical minimum distance grows only sub-linearly in the codewords length, close to linear by picking an outer code with large free distance.

The case with $m \geq 2$ includes Repeat multiple-Accumulate codes (RA^m) and [20, 45, 46] and Hamming double-Accumulate codes (HA^2) [47]. In [37, 46] it is proved that Repeat/Convolutional double-accumulate codes are asymptotically good and a lower bound on the minimum distance is derived. Our work is largely motivated by these results, which raise the following open questions:

- Can one improve the minimum distance bound on the Repeat/Convolutional double-accumulate codes?

- Can one obtain better minimum distance by replacing the accumulators with generic convolutional encoders? And by considering more concatenation in the serial structure?

Numerical evaluation of the minimum distance shows that these codes are asymptotically good and that the minimum distance is close to GV-distance, even with a small number of inner encoders [44, 46]. However, there is not yet a complete and fully satisfactory theoretic understanding of these phoenomena.

Studying such general setting is not a trivial issue. A basic request to analyze these codes is to determine weight distributions of constituent convolutional encoders. Indeed, the average weight enumerators and the corresponding spectral functions can be expressed in terms of weight distributions of constituent components (see [18]). For example, in the case of repeat multiple-accumulate codes, an explicit analytic formula for the asymptotic spectral functions is known and can be expressed in a recursive way [48].

In general cases, the theoretical justification of the extension of the iterative formula of spectral function [49] requires some finer work, since the limit step needs uniformity in the convergence to the spectral function of the constituent codes. This fact, to the best of our knowledge, has never been proved before.

The weight distributions of convolutional encoders have been studied by a large number of authors [36, 46, 48–51]. Although analytic formulæ of weight spectrum can be derived in some cases by using combinatorial techniques — i.e. for rate-1 convolutional encoders with transfer function $(1 + D)^{-1}$ and $(1+D+D^2)^{-1}$ [48]— there is not a general method that is able to derive explicit expressions. McEliece has shown how the weight distribution can be derived, theoretically, from the adjacency matrix of the state diagram associated with a minimal realization of the encoder [50]. This approach is able to determine the weight spectrum exactly for relatively small lengths, but the computation becomes prohibitively expensive as the truncation lengths increase. Bender et al. have shown in [52] that central and local limit theorems can be derived for the growth of the components of the power of a matrix. This approach would allow in principle to apply Hayman approximation (see [53] for a survey) to the problem of the weight distribution of convolutional codes. However the hypotheses needed to use these techniques are very restrictive and they are not guaranteed in general cases. An overview of these methods can be found in [46] and in [21].

Also for the asymptotic exponential growth rate one can not hope in general to give explicit analytic expressions. Nevertheless, there exists an efficient numerical procedure to determine this growth rate to any desired degree of accuracy [49]. However, this method is not able to provide more refined information on the speed of convergence of the sequence of the exact exponents to the asymptotic growth rate and to guarantee the continuity of limit function.

1.3.2 What is new in this thesis with respect to the literature

In this dissertation, we undertake a rigorous analysis of average spectral functions and minimum distance distribution of turbo-like codes and structured LDPC.

As a first step in this study, we focus on truncated convolutional encoders, which are the constituent elements of turbo concatenations. We present a detailed analysis of weight distribution function and its exponential growth rate.

Our contribution is mainly theoretical. We improve upon previous results in the following ways. We express weight enumerators of convolutional codes as coefficients of formal power series with nonnegative coefficients. Although these expressions can be computed for relatively small truncation lengths, they become prohibitively complex to compute as truncation lengths and weights increase. By applying an extension of Multidimensional Saddle Point (MSP) method (also known under the name of Hayman-like techniques) [52], we prove that weight enumerators admit an accurate approximation (not only their exponent), which allows more efficient numerical evaluations. We show in some examples that our approximation is very accurate, even for quite short truncation lengths, and that it improves estimates known in literature. This approximation is then used to obtain a formula for the asymptotic spectral function. We show that the expression derived for the asymptotic spectral function can be recast into the formulation given in [49]. However, this new representation points out that the function is continuous, concave and differentiable with respect to both variables in its convex and closed domain. These properties were conjectured in [46], but never proved. The expressions obtained for weight distributions can in general only evaluated numerically (except for some specific cases). However, the numerical procedure to compute these functions can be conveniently improved by using any standard algorithm for unconstrained minimization of a convex function (e.g. gradient descent). Finally, we study the speed of convergence of exact exponents of weight enumerators to the asymptotic limit and we prove uniformity of this convergence. This result provides an estimate of the speed of the vanishing truncation effect when the truncation length goes to infinity.

Building upon these results, we study average spectral functions of multiple serially concatenated codes. Our contribution consists in showing analytically that if $m \geq 2$ then the distance spectra are equal to 0 below a threshold distance δ_m and are positive above it. Since the spectral shapes are not negative but only equal to 0 before δ_m, this is not sufficient to conclude that their relative minimum distances also reach δ_m. However, by using techniques proposed by Jin and Mc-Eliece [19], we conclude that indeed for such ensembles, minimum distances scale linearly in the codewords length and the typical linear growth rate, for a specific m, is exactly given by δ_m. Finally, under a very mild condition on the outer encoder we prove that asymptotic spectral functions form a sequence of functions uniformly convergent in m. Their limit is the maximum between 0 and the average spectral shape of the random linear coding ensemble. As a consequence, the threshold sequence δ_m converges to the Gilbert-Varshamov (GV) distance when m goes to infinity.

Finally, we focus on a family of codes that generalize Repeat-Convolute codes, and can be seen both as particular systematic serial turbo codes and as structured LDPC codes. Using techniques, similar to those previously exploited to study serial coding schemes, we analyze minimum distances and prove in this new setting coding theorems, already obtained for serially concatenated codes. In particular, we prove that the minimum distance cannot grow linearly deterministically. Inspired by the the tail estimations of [36], we identify parameters allowing the typical minimum distance to grow sub-linearly in the codewords length with high probability.

This dissertation extends and completes the analysis in [37, 44, 46, 54, 55], and gives a deeper insight into the problem of the distance spectra of multiple serially concatenated codes. It also corrects some wrong statements made in [56–58] and partially revised in [59] for the case of multiple serially concatenated codes and in [42] for structured LDPC.

1.4 Summary and outline of the thesis

1.4.1 Chapter 2

Before presenting the core of the work, this chapter defines recurrent notation and collects some specific tools that are important ingredients in the sequel. This includes a brief review of Shannon classical coding theory for memoryless channel; block linear codes, code ensembles and the Gilbert-Varshamov bound are presented, as well as enumerating functions.

1.4.2 Chapter 3

In Chapter 3, we focus on convolutional codes, which are the constituent elements of turbo concatenations. After recalling some properties which will be instrumental for our derivations, we present a detailed analysis of weight distribution function and its exponential growth rate for truncated convolutional encoders. In particular, exact formulæ are derived in terms of generating functions of error events associated with a minimal realization of the encoder. Although explicit analytic expressions can be computed for relatively small truncation lengths, the explicit expressions become prohibitively complex to compute as truncation lengths and weights increase. Fortunately, a very accurate asymptotic expansion can be derived using the Multidimensional Saddle Point method (MSP-metohd). This approximation is substantially easier to evaluate and is used to obtain an expression for the asymptotic spectral function and to prove continuity and differentiability in its domain (convex and closed). Finally, this approach is able to guarantee that the sequence of exponential growth rate converges uniformly to the asymptotic limit and to estimate the speed of this convergence.

This material has been presented in [60].

1.4.3 Chapter 4

In Chapter 4, we introduce the generic multiple serial turbo-coding ensemble and we study average spectra and minimum distances, using the mathematical tools devised in Chapter 3. Our contribution consists in analytically showing that for $m \geq 2$ the average distance spectra are equal to 0 below a threshold distance δ_m and are positive above it. We show that minimum distances grow linearly in the truncation length with probability one, and that lower bounds on the asymptotic normalized minimum distance are exactly given by δ_m. Finally, we prove under a very mild condition on the outer encoder that asymptotic spectral functions form a uniformly convergent sequence of functions. Their limit is the maximum between 0 and the average spectral shape of the random linear coding ensemble. As a consequence, the threshold sequence δ_m converges to the Gilbert-Varshamov (GV) distance.

Preliminary versions of this material are in [54, 55, 61].

1.4.4 Chapter 5

Chapter 5 deals with the family of irregular repeat-convolute (IRC) codes. They can be seen both as particular systematic serial turbo codes and as structured LDPC codes. We derive the average weight distribution function and its asymptotic growth rate for these code ensembles. Inspired both by the the tail estimations of [36] and by the bounding techniques of [37], we prove typical minimum distance of such coding schemes scales only sub-linearly in the code length with probability approaching one.

1.4.5 Chapter 6

The overall conclusion first summarizes the main contributions, extracting results from different chapters; it gives some general messages suggested by this work; then it concludes with several open questions and more general directions for related future research.

1.4.6 Appendix A

This chapter is devoted to the description of multidimensional saddle-point (MSP) techniques to estimate order of magnitude of coefficients in large powers of multivariate power series with non-negative coefficients.

The first step is to recast the problem as the computation of a Cauchy integral and to apply the residue theorem. In order to estimate complex integrals of an analytic function, a path crossing a saddle-point is chosen and the integrand is estimated locally near this saddle-point. If the generating function satisfies some “nice” properties, which go under the name of *localization* or *concentration*, the contribution near the saddle-point captures the essential part of the integral. Some examples of admissible functions are multivariate polynomial (see Lemma D.14 in [21]) and univariate series (see Section VIII.8.1 in [62]).

We prove that these techniques can be extended to a more general class of function of generating functions, which includes the cases treated in [52, Thm. 2] and [21, Lemma D.14]. Moreover, our modification allows to estimate the order of magnitude of a (convergent) sequence of coefficients in large powers of multivariate functions.

1.5 Publications

The results of the present work are based on the following papers.

- F. Fagnani, C. Ravazzi, "Spectra and minimum distances of Repeat Multiple Accumulate codes", in *Proc. of Information Theory and Applications Workshop*, pp. 77-86, La Jolla, CA, San Diego, Jan. 2008.
- C. Ravazzi, F. Fagnani, "Spectra and minimum distances of Repeat Multiple-Accumulate codes", *IEEE Transactions on Information Theory*, Vol. 55(11), pp. 4905-4924, Nov. 2009.
- C. Ravazzi, F. Fagnani, "Hayman-like techniques for computing input-output weight distribution of convolutional encoders", in *Proc. of IEEE International Symposium on Information Theory*, pp. 1110-114, Austin, Texas, June 2010.
- C. Ravazzi, F. Fagnani, "Minimum distance properties of multiple-serially concatenated codes", in *Proc. International symposium on turbo codes & iterative information processing*, pp. 88-92, Brest, France, Sep. 2010
- C. Ravazzi, F. Fagnani, "On the growth rate of input-output weight enumerators of convolutional encoders", submitted, 2010
- C. Ravazzi, F. Fagnani, "Multiple serial coding ensemble: average spectra and minimum distances", in preparation, 2010

All publications are available online at: calvino.polito.it/∼ravazzi/research

Preliminaries 2

Brief—In this chapter, we summarize some basic results used later in this thesis. The material here presented is known. Nevertheless, this is an opportunity to define in formal way some vocabulary and fundamental notation.

2.1 Outline of the chapter

In Section 2.2, we introduce general notation and definition. Section 2.3 quickly reviews some basic notions from coding theory and information theory, such as Shannon theorem for memoryless channel. Next, in Section 2.4, block linear codes, minimum distance, the enumerating functions are defined and the Gilbert-Varshamov bound is presented. Finally, in Section 2.5, minimum distance distributions are analyzed for typical codes from a random linear code ensemble.

2.2 General notation and definitions

Notation $x \in \Omega$ (respectively $x \notin \Omega$) means that element x belongs to (respectively does not belong to) the set Ω. Given two sets Ω and Θ, the inclusion of Ω in Θ is denoted with $\Omega \subseteq \Theta$, and their union and intersection are denoted with $\Omega \cup \Theta$ and $\Omega \cap \Theta$ respectively. The union –resp. intersection– of sets $\Omega_1, \dots, \Omega_N$ is summarized by $\bigcup_{k\in[N]} \Omega_k$ –resp. by $\bigcap_{k\in[N]} \Omega_k$. The difference between sets Ω and Θ is denoted $\Omega \setminus \Theta = \{x : x \in \Omega \text{ and } x \notin \Theta\}$. Given a set Ω we denote by $|\Omega|$ its cardinality. For any subset $\Omega \subseteq \Theta$, $\Omega^{\mathrm{c}} = \Theta \setminus \Omega$ will denote the complementary of Ω in Θ. The indicator function of Ω is denoted with $\mathbb{1}_\Omega : \Theta \to \{0, 1\}$ and defined by $\mathbb{1}_\Omega(\theta)$ if $\theta \in \Omega$ and $\mathbb{1}_\Omega(\theta) = 0$ otherwise.

Let $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ be the usual number sets and $\mathbb{Z}_2 = \{0, 1\}$ be the Galois field with two elements. With $\mathbb{R}_+ = [0, +\infty)$ and $\mathbb{R}^+ = (0, +\infty)$ we will indicate the sets, respectively, of nonnegative and positive reals. We will also use $\mathbb{N}_0 = \{0\} \cup \mathbb{N}$. The sequence of integers from 1 to $N \in \mathbb{N}$ is summarized by notation $[N]$. For $x \in \mathbb{R}$, notation $\lfloor x \rfloor$ denotes the integer part of x, that is the largest integer $m \in \mathbb{Z}$ suh that $m \leq x$. For $x \in \mathbb{R}$, $\lceil x \rceil$ is the smallest integer $m \in \mathbb{Z}$ suh that $m \geq x$. The absolute value of $x \in \mathbb{R}$ is $|x|$. If z is in $\mathbb{C}$, z^* is its conjugate. The unit imaginary part is denoted by $\mathrm{j} = \sqrt{-1}$. A complex number $x \in \mathbb{C}$ is represented using its norm and argument, $x = ||x|| \mathrm{e}^{\mathrm{j} \arg(x)}$.

The functions log and exp are to be considered with respect to a fixed, arbitrarily chosen positive base, unless explicit mention to the contrary. Conventionally, we set $\exp(-\infty) = 0, \exp(+\infty) = +\infty, \inf(\emptyset) = +\infty$ and $\sup(\emptyset) = -\infty$. We will use $a \vee b$ and $a \wedge b$ to denote the maximum and minimum, resepectively, between real values a and b.

This thesis makes frequent use of the Landau symbols. The notation "$f(N) = O(g(N))$ when $N \to \infty$" means that there exist positive constants c and N_0, such that $f(N) \leq cg(N)$ for all $N > N_0$. The expression "$f(N) = o(g(N))$ when $N \to \infty$" means that $\lim_{N\to\infty} |f(N)/g(N)| = 0$. Finally, we use the expression "$f(N) \sim g(N)$ when $N \to \infty$" for $\limsup_{N\to\infty} |f(N)/g(N)| = 1$.

Boldface letters are used for vectors and matrices. The vector of $\mathbb{R}^n$ whose elements are all equal to 1 is denoted $\mathbf{1}_n$. Given a set $\Omega \subseteq \mathbb{R}^n$ we denote by $\overset{\circ}{\Omega}$, $\overline{\Omega}$ and $\mathrm{co}(\Omega)$ respectively, the interior, the closure and the convex hull of Ω. The identity matrix in $\mathbb{R}^{n\times n}$ is denoted with $\mathbf{I}_n$. The transpose of $\mathbf{A}$ and its inverse are denoted $\mathbf{A}^T$ and $\mathbf{A}^{-1}$, respectively. We use symbols $|\mathbf{A}|$ for the determinant of $\mathbf{A} \in \mathbb{R}^{n\times n}$. Given a vector $\boldsymbol{x} \in \mathbb{Z}_2^n$ with $n \in \mathbb{N}$, we denote by $\mathrm{supp}(\boldsymbol{x})$ the set of indices where $\boldsymbol{x}$ is nonzero. For a vector $\boldsymbol{x} \in \mathbb{R}^n$, $||\boldsymbol{x}||_2 = \sqrt{\sum_{i=1}^n x_i^2}$ denotes its Euclidean norm and $||\boldsymbol{x}||_1 = \sum_i |x_i|$.

Given $\boldsymbol{f}$ and $\boldsymbol{g}$ in the vector space of $\mathbb{C}^n$, we indicate by $\langle \boldsymbol{f}, \boldsymbol{g} \rangle = \sum_k f_k g_k^*$ their scalar product and with $\boldsymbol{f} \cdot \boldsymbol{g}$ their pointwise product. For $\boldsymbol{f} \in \mathbb{R}^n$ and $\boldsymbol{g} \in \mathbb{C}^n$ we define $\boldsymbol{f}^{\boldsymbol{g}}$ in $\mathbb{C}$ as $\boldsymbol{f}^{\boldsymbol{g}} := \prod_{i\in\mathrm{supp}(\boldsymbol{f})} f_i^{g_i}$.

Let $\boldsymbol{x} = (x_1, \ldots, x_n)$ and $F(\boldsymbol{x})$ be a formal multivariate series. We denote by $\boldsymbol{k} = (k_1, \ldots, k_n)$ and $\mathrm{coeff}\{F(\boldsymbol{x}), \boldsymbol{x}^{\boldsymbol{k}}\}$ or by $F_{\boldsymbol{k}}$ the coefficient of $\boldsymbol{x}^{\boldsymbol{k}} = \prod_{i=1}^n x_i^{k_i}$ in $F(\boldsymbol{x})$, i.e.,

$$F(\boldsymbol{x}) = \sum_{\boldsymbol{k}} \mathrm{coeff}\left\{F(\boldsymbol{x}), \boldsymbol{x}^{\boldsymbol{k}}\right\} \boldsymbol{x}^{\boldsymbol{k}} = \sum_{\boldsymbol{k}} F_{\boldsymbol{k}} \boldsymbol{x}^{\boldsymbol{k}}.$$

If $P(x)$ is a polynomial, we denote with ldeg and deg the largest and smallest index for which the coefficient is nonzero, respectively

$$\mathrm{ldeg}[P(x)] = \min\{k | \mathrm{coeff}\{P(x), x^k\} \neq 0\}$$
$$\deg[P(x)] = \max\{k | \mathrm{coeff}\{P(x), x^k\} \neq 0\}.$$

Let $(\Omega, \mathcal{B}, \nu)$ be a σ-finite measure space [63]. The absolutely integrable functions $f : \Omega \to \mathbb{R}$ are probability densities, if $f(\omega) \geq 0$ ν-almost everywhere, and $\int_{\Omega} f(\omega)\mathrm{d}\nu(\omega) = 1$. We will consider the following cases:

- If Ω is finite, then $\mathcal{B} = 2^{\Omega}$, ν is the counting measure and $f(\omega)$ are simply probability vectors such that $\int_{\Omega} f(\omega)\mathrm{d}\nu(\omega) = \sum_{\omega\in\Omega} f(\omega) = 1$
- If $\mathbb{R} = \mathbb{R}^d$, then $\mathcal{B}$ is the Borel σ-algebra, ν is the Lebesgue measure, and f are usual probability densities over $\mathbb{R}^d$.

2.3 Shannon theory for symmetric memoryless channels

A memoryless channel (MC) is described by the triple $(\mathcal{X}, \mathcal{Y}, Q)$ where

- $\mathcal{X}$ is a finite input alphabet;
- $\mathcal{Y}$ is an output set consisting of a σ-finite measure space $\mathcal{Y} = (Y, \mathcal{B}, \nu)$;
- $Q(\cdot|x)$ is a family of transition probability densities on $\mathcal{Y}$ for all $x \in \mathcal{X}$.

In most applications, either $\mathcal{Y}$ is finite, ν is the counting measure and $Q(\cdot|x)$ are simply probability vectors, or $\mathbb{R} = \mathbb{R}^d$ and ν is the Lebesgue measure. Intuitively, $Q(\cdot|x)$ expresses the probability of observing the output symbol y given that we send the symbol $x \in \mathcal{X}$.

If the channel is used repetitively to transmit a sequence of bits, we model a multiple use of the same channel as a new channel having input set $\mathcal{X}^n$ and output set $\mathcal{Y}^n = (Y^n, \mathcal{B}^n, \nu_n)$ where $\mathcal{B}^n$ is the product σ-algebra and ν_n is the product measure. Specifically, if a string $\boldsymbol{x} \in \mathbb{Z}_2^n$ is fed into the channel, then the channel output is a random variable Y^n distributed according to

$$Q_n(Y^n = \boldsymbol{y}|\boldsymbol{x}) = \prod_{i=1}^{n} Q(y_i|x_i).$$

This means that the probability distribution of the output depends only on the input at that time and is conditionally independent of previous channel inputs or outputs. For simplicity we will consider binary memoryless channel, i.e. with $\mathcal{X} = \mathbb{Z}_2$. A binary memoryless channel is said to be output symmetric if $Q(y|0)$ and $Q(y|1)$ differ for an involutive permutation on $\mathcal{Y}$, namely, there exists τ permutation on $\mathcal{Y}$ such that $\tau \circ \tau$ is the identity and $Q(y|1) = Q(\tau(y)|0),\ Q(y|0) = Q(\tau(y)|1)$.

The most common examples of memoryless symmetric channels are the following.

Example 2.1 (The Binary Symmetric Channel (BSC)). *We have $\mathcal{X} = \mathcal{Y} = \mathbb{Z}_2$ with $Q(1|0) = Q(0|1) = \epsilon$. In this channel every transmitted bit is received wrong with probability ϵ. We can assume $\epsilon < 1/2$ without loss of generality.*

Example 2.2 (The Binary Erasure Channel (BEC)). *In this case we have* $\mathcal{X} = \mathbb{Z}_2$ $\mathcal{Y} = 0, 1, ?$ *with* $Q(1|0) = Q(0|1) = 0$, $Q(?|0) = Q(?|1) = \epsilon$. *In this channel, as it happens in the BSC, a bit is wrongly received with probability* ϵ. *However, differently from the BSC, the receiver knows if an error occurs.*

Example 2.3 (The Additive White Gaussian Noise channel with binary input (BIAWGN)). . *We have* $\mathcal{X} = \mathbb{Z}_2$, $\mathcal{Y} = \mathbb{R}$. *It is a continuous channel whose transition densities can be obtained in the following way: we associate to the input signal* 0 *and* 1 *the real numbers* $-L$ *and* L *respectively (where* $L > 0$*) and we assume that the output is obtained by summing to the signal* $\pm L$ *a r.v. of type* $\mathsf{N}(0, \sigma^2)$.

The reader is referred to [64] for further details.

A block encoder for a binary input memoryless channel (BIMSC) $(\mathbb{Z}_2, \mathcal{Y}, Q)$ is an injective map $\phi : \mathbb{Z}_2^k \to \mathbb{Z}_2^n$. We define the corresponding code to be the image of the encoder $\mathcal{C}_\phi := \phi(\mathbb{Z}_2^k) \subseteq \mathbb{Z}_2^n$. The parameters k and n are said to be, respectively, the information and code length, and $R = k/n$ is the transmission rate, a measure of the amount of redundancy we are introducing. A decoder is any mapping $\psi : \mathcal{Y}^n \to \mathbb{Z}_2^n$. We will refer to the coding scheme as the pair (ϕ, ψ). Once a coding scheme has been fixed, its word error probability can be defined as follows. Consider the information word U, a r.v. uniformly distributed on $\mathbb{Z}_2^k$, and let $X = \phi(U)$. Let moreover Y be the r.v. on $\mathcal{Y}^n$ whose probabilistic description is given by the conditional density $Q_n(\boldsymbol{y}|\boldsymbol{x})$. The error probability is the probability of the event $\{[\phi^{-1} \circ \psi](Y) \neq U\}$ or, equivalently, $\{\psi(Y) \neq X\}$ and will be denoted by $\mathrm{p_e}(\phi, \psi)$

$$\mathrm{p_e}(\phi, \psi) = \frac{1}{2^k} \sum_{\boldsymbol{x} \in \mathcal{C}_\phi} \mathrm{p_e}(\phi, \psi|\boldsymbol{x}) \tag{2.1}$$

where

$$\mathrm{p_e}(\phi, \psi|\boldsymbol{x}) = \int_{\mathcal{Y}^n} \mathbb{1}_{\psi^{-1}(\mathcal{C}_\phi \setminus \{\boldsymbol{x}\})}(\boldsymbol{y}) \mathrm{d}\nu_n(\boldsymbol{y}) \tag{2.2}$$

is the error probability conditioned to the transmission of the codeword $\boldsymbol{x}$.

It is well known that, given the encoder ϕ, the decoding scheme minimizing the error probability is the maximum likelihood (ML) decoding

$$\psi_{\mathrm{ML}}(\boldsymbol{y}) = \operatorname*{argmax}_{\boldsymbol{u} \in \mathbb{Z}_2^k} Q_n(\boldsymbol{y}|\phi(\boldsymbol{u})).$$

From now on we will always assume that ML decoding is used and will use the simpler notation $\mathrm{p_e}(\phi)$. Notice that $\mathrm{p_e}(\phi)$ depends on the encoder only through its image, the code $\mathcal{C}_\phi = \phi(\mathbb{Z}_2^k)$. We sometime will use the notation $\mathrm{p_e}(\mathcal{C}_\phi)$ instead of $\mathrm{p_e}(\phi)$.

Theorem 2.1. *Consider a BIMSC. Then there exists a constant* C *such that:*

- *for any $R < C$ there exists a sequence of encoders $\phi_n : \mathbb{Z}_2^{k_n} \to \mathbb{Z}_2^n$ with rate $R_n = k_n/n$ and*

$$\liminf_{n\to\infty} R_n = R \qquad \lim_{n\to\infty} \mathrm{p_e}(\phi_n) = 0;$$

- *for any $R > C$ there exists $\eta > 0$ such that for all encoder ϕ with rate R* $\mathrm{p_e}(\phi_n) > \eta$.

First assertion in Shannon's theorem tells us that we can communicate reliably at high rates, as long as below the threshold C. Moreover, the error probability can be made arbitrarily small without sacrificing data rates, at the price of increasing the code length n. The several proofs in literature [40, 64, 65] consist in considering, for given R and $n \in \mathbb{N}$, a r.v. Φ uniformly distributed over all possible maps from $\mathbb{Z}_2^{\lfloor Rn \rfloor} \to \mathbb{Z}_2^n$ and studying the average error probability $\overline{\mathrm{p}}_\mathrm{e} := \mathbb{E}_\Phi[\mathrm{p_e}(\Phi)]$.

The second point instead says that transmitting at rates near capacity is the best use of the channel: error probabilities can not be made as small as we want if we try to transmit at a rate greater than C. For these reasons, C is called the *capacity* of the channel.

Shannon's theorem does not give any practical technique to construct good codes. We could in principle generate a random code accordingly to the uniform distribution. However, random constructed codes have unfeasible complexity when using ML decoding, which requires exponential time in the codewords length n. Indeed, if we choose the 2^k codewords of a code of length n randomly, we will need to keep in memory something like 2^{kn} bits to perform encoding and decoding. Moreover, ML decoding will require to find a maximum of a set of 2^k real numbers. For k growing linearly with n both the memorization and the ML decoding become therefore too computationally complex.

2.4 Linear block encoders and GV-bound

The fundamental idea to construct good codes is to separate as much as possible its codewords: codewords which are far apart among each other will have small probability of being mutually equivocated, when transmitted over a noisy channel. The Hamming distance and minimum distance of a code will play a fundamental role in this thesis.

Definition 2.1 (Hamming distance). *Let $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{Z}_2^n$, we define $d_\mathrm{H} : \mathbb{Z}_2^n \times \mathbb{Z}_2^n \to \mathbb{N}$ as $d_\mathrm{H}(\boldsymbol{x}, \boldsymbol{y}) = |\mathrm{supp}(\boldsymbol{x} - \boldsymbol{y})|$.*

Definition 2.2 (Hamming spheres). *Hamming spheres are defined $B_\mathrm{H}(\boldsymbol{x}, r) = \{y \in \mathbb{Z}_2^n | d_\mathrm{H}(\boldsymbol{x}, \boldsymbol{y}) \le r\}$.*

Definition 2.3 (Minimum distance). *Consider the encoder $\phi : \mathbb{Z}_2^k \to \mathbb{Z}_2^n$ and the corresponding code $\mathcal{C} = \mathrm{Im}(\phi)$. The minimum distance $d_{\min}(\mathcal{C})$ is defined as $d_{\min}(\mathcal{C}) = \min\{d_\mathrm{H}(\boldsymbol{x}, \boldsymbol{y}) : \ \boldsymbol{x}, \boldsymbol{y} \in \mathcal{C}\}$.*

In this dissertation we will consider exclusively linear block encoders, namely $\mathbb{Z}_2$-linear maps $\phi : \mathbb{Z}_2^k \to \mathbb{Z}_2^n$. In this case there exists a matrix $\mathbf{G} \in \mathbb{Z}_2^{k\times n}$, called *generator matrix*, such that $\phi(\boldsymbol{u}) = \boldsymbol{u}\mathbf{G}$, $\forall \boldsymbol{u} \in \mathbb{Z}_2^k$. The code $\mathcal{C}_\phi = \mathrm{Im}(\phi)$ is then a $\mathbb{Z}_2$-linear subspace of $\mathbb{Z}_2^n$.

Block linear encoders allow some simplifications compared to generic block encoders.

Definition 2.4. *Given $\boldsymbol{x} \in \mathbb{Z}_2^n$, the* Hamming weight $\mathrm{w_H}(\boldsymbol{x})$ *is the number of non-zero elements in $\boldsymbol{x}$:*

$$\mathrm{w_H}(\boldsymbol{x}) = |\{i = 1, \dots, n : \ x_i \neq 0\}| = \mathrm{d_H}(\boldsymbol{x}, \mathbf{0}).$$

In the linear case we have

$$d_{\min}(\phi) = \min_{\boldsymbol{x}\in\mathcal{C}_\phi} \mathrm{d_H}(\boldsymbol{x}, \boldsymbol{y}) = \min_{\boldsymbol{x}\in\mathcal{C}_\phi} \mathrm{d_H}(\boldsymbol{x}+\boldsymbol{y}, \boldsymbol{y}+\boldsymbol{y}) = \min_{\boldsymbol{x}'\in\mathcal{C}_\phi} \mathrm{d_H}(\boldsymbol{x}', \mathbf{0}) = \min_{\boldsymbol{x}'\in\mathcal{C}_\phi} \mathrm{w_H}(\boldsymbol{x}).$$

Moreover, block linear codes have the uniform error property: the error probability does not depend on the transmitted codeword

$$\mathrm{p_e}(\phi) = \mathrm{p_e}(\phi|\boldsymbol{x}).$$

With this simplification the *Union-Bhattacharyya bound* provides the following estimate for error probability [40]

$$\mathrm{p_e}(\phi) \leq \sum_{d=d_{\min}(\phi)}^{n} A_d(\phi)\gamma^d, \tag{2.3}$$

or equivalently

$$\mathrm{p_e}(\phi) \leq \sum_{d=d_{\min}(\phi)}^{n} \sum_{w=1}^{k} A_{w,d}(\phi)\gamma^d.$$

where $A_d(\phi)$ and $A_{w,d}(\phi)$ are the weight enumerators of the encoder ϕ defined as follows

$$A_d(\phi) = |\{\boldsymbol{u} \in \mathbb{Z}_2^k : \ \mathrm{w_H}(\phi(\boldsymbol{u})) = d\}| \tag{2.4}$$

$$A_{w,d}(\phi) = |\{\boldsymbol{u} \in \mathbb{Z}_2^k : \ \mathrm{w_H}(\boldsymbol{u}) = w, \ \mathrm{w_H}(\phi(\boldsymbol{u})) = d\}| \tag{2.5}$$

The expression in (2.3) shows that weight enumerators are the main ingredient to estimate error probabilities. Moreover, if the Bhattacharyya parameter is small then the first term in the summation is generally the dominant one:

$$\sum_{d=d_{\min}(\phi)}^{n} A_d(\phi)\gamma^d \sim A_{d_{\min}(\phi)}(\phi)\gamma^{d_{\min}(\phi)} \qquad \gamma \to 0.$$

A lower bound on the error probability can be obtained in terms exclusively of minimum distance. Define the folowing equivocation sets

$$\Lambda_0 = \{y \in \mathcal{Y} \ : \ Q(y|0) \geq Q(y|1)\} \qquad \Lambda_1 = \{y \in \mathcal{Y} \ : \ Q(y|1) \geq Q(y|0)\},$$

and let p be the equivocation probability

$$p = \int_{\Lambda_1} Q(y|0)\mathrm{d}\nu = \int_{\Lambda_0} Q(y|1)\mathrm{d}\nu. \tag{2.6}$$

Let $\boldsymbol{y} \in \mathcal{C}_\phi$ such that $\mathrm{w_H}(\boldsymbol{y}) = d_{\text{min}}(\mathcal{C}_\phi)$. Assume the sequence $\mathbf{0} \in \mathcal{C}_\phi$ is transmitted over the channel and equivocation happens in all the positions in $\text{supp}(\boldsymbol{y})$. In that case for sure $\mathcal{D}(\boldsymbol{y}) \neq \mathbf{0}$. This event happens with probability $p^{d_{\text{min}}(\mathcal{C}_\phi)}$ and we clearly have

$$\mathrm{p_e}(\phi) \geq p^{d_{\text{min}}(\mathcal{C}_\phi)}. \tag{2.7}$$

The estimate in (2.7), as a consequence, suggests that error probability can not converge to 0 unless $d_{\text{min}}(\phi) \to \infty$ when $n \to \infty$. In other words, in order to construct codes achieving Shannon limit, necessarily we need to make sure that their minimum distance does not remain bounded when n grows. Moreover, if we want to achieve exponential convergence, $d_{\text{min}}(\mathcal{C}_\phi)$ has to grow linearly in n. This motivates the following definition

Definition 2.5. *A sequence of encoders ϕ_n with rate $R_n = k_n/n$ with minimum distance $d_n = d_{\text{min}}(\phi_n)$ is* asymptotically good *if*

$$\liminf_{n\to\infty} R_n = R > 0 \qquad \liminf_{n\to\infty} \frac{d_n}{n} = \delta_{\text{min}} > 0.$$

We call *relative minimum distance* of the sequence ϕ_n the value $\delta_{\text{min}} = \delta_{\text{min}}(R)$.

2.4.1 The Gilbert-Varshamov bound

The GV-bound is a lower bound on the largest minimum distance achievable by codes with rate dimension k and length n. The GV bound has attracted a huge amount of attention from researchers. In particular the asymptotic tightness of the GV bound is one of the most important unproved conjectures in coding theory. A well known fact is that the Gilbert-Varshamov bound is asymptotically achieved with probability one by the binary linear coding ensemble [29], while this is not the case for the random coding ensemble.

For every n and k fixed, define

$$d_{\text{GV}} = \max\left\{ d \leq n/2 \,\middle|\, 2^k \sum_{h=1}^{d-1} \leq 2^n \right\}$$

Theorem 2.2. *For every R there exists a sequence of codes $\mathcal{C}_n \subseteq \mathbb{Z}_2^n$ of dimension k such that $d_{\text{min}}(\mathcal{C}_n) \geq d_{\text{GV}}$.*

The proof is obtained by a "greedy algorithm" construction [26]: it provides a code meeting the bound above.

1. Inizialization: $\mathcal{C}_n = \boldsymbol{x}_1$ with $\boldsymbol{x}_1 \in \mathbb{Z}_2^n$
2. Step $i \geq 2$: Set $S = \bigcup_{j=1}^{i-1} B_{d-1}(\boldsymbol{x}_j)$. If $S = \mathbb{Z}_2^n$, halt. Otherwise choose a vector $\boldsymbol{x}_i$ in $\mathbb{Z}_2^n \setminus S_i$; set $\mathcal{C}_n = \mathcal{C}_n \cup \{\boldsymbol{x}_i\}$; iterate.

Proposition 2.1. *For every pair (R, δ) with $\delta < 1/2$ satisfying the following condition*

$$H(\delta) \leq (1 - R)\ln 2 \tag{2.8}$$

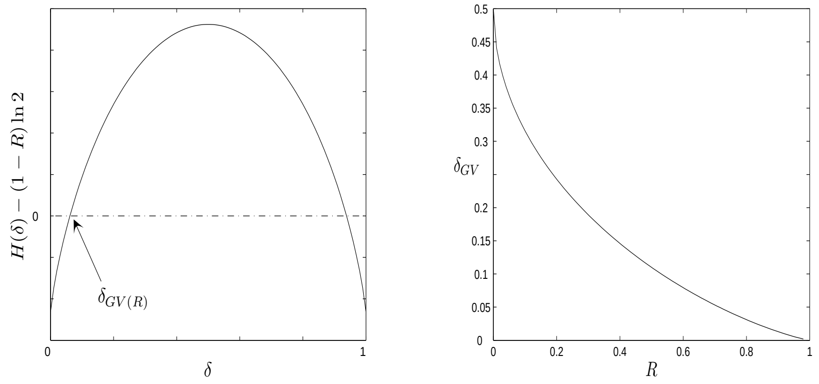
there exists a sequence of codes $\mathcal{C}_n$ with rate $R_n = k_n/n$ and minimum distance d_n such that

$$\liminf_{n\to\infty} R_n = R \qquad \liminf_{n\to\infty} \frac{d_n}{n} = \delta.$$

Definition 2.6. *We call* normalized Gilbert-Varshamov distance *the greatest value δ satisfying the inequality* (2.8)

$$\delta_{GV}(R) = \max\{\delta \leq 1/2 : H(\delta) \leq (1-R)\ln 2\} = (H|_{[0,1/2]})^{-1}[(1-R)\ln 2]. \tag{2.9}$$

The normalized GV-distance δ_{GV} is defined as the smallest root of equation $H(\delta) = (1 - R)\ln 2$ con $0 \leq R \leq 1$ (see Figure 2.1(a)): $\delta_{GV}(0) = 1/2$ and $\delta_{GV}(R)$ is monotonically decreasing in $R \in [0, 1]$ (see Figure 2.1(b)).



(a) $\delta_{GV}(R) = (H|_{[0,1/2]})^{-1}((1-R)\ln 2)$.

(b) Normalized GV-distance δ_{GV} as a function of R.

Figure 2.1: Normalized GV-distance

Proposition 2.1 is the asymptotic version of the GV bound. Given a rate $R \in (0, 1)$, it states that there exist codes of length n and minimum distance at least $n\delta_{\mathrm{GV}}(R)$. This fact leads to the following definition.

Definition 2.7. *The sequence $\mathcal{C}_n \sim (n, k_n, d_n)$* attains the GV-bound *if*

$$\liminf_{n\to\infty} R_n = R \qquad \liminf_{i\to\infty} \frac{d_n}{n} = \delta_{GV}(R).$$

2.5 The probabilistic method

To put the rest of the dissertation into perspective and introduce notation, let us recall how the probabilistic method derives the Gilbert Varshamov bound for linear codes.

In order to prove the existence of a coding scheme with certain properties, a probability space is constructed (code ensemble) and then it is shown that a randomly chosen code from this space satisfies the desired properties with high probability.

Let $\mathscr{E}$ be a set of $\mathbb{Z}_2$-linear encoders with rate R and length N. We can introduce a probabilistic structure on $\mathscr{E}$ by considering a random encoder chosen uniformly from this set. We then define the *average output* and *average input-output weight enumerators* of $\mathscr{E}$, respectively, as follows

$$\overline{A}_d\left(\mathscr{E}\right) \doteq \frac{1}{|\mathscr{E}|}\sum_{\mathcal{E}\in\mathscr{E}} A_d(\mathcal{E})$$

$$\overline{A}_{w,d}\left(\mathscr{E}\right) \doteq \frac{1}{|\mathscr{E}|}\sum_{\mathcal{E}\in\mathscr{E}} A_{w,d}(\mathcal{E}).$$

Consider now a sequence $\overline{\mathscr{E}} = \{\mathscr{E}_N\}_{N\in\mathbb{N}}$, where each $\mathscr{E}_N$ is an ensemble of encoders of length N. For each ensemble $\mathscr{E}_N$, $\overline{A}_d(\mathscr{E}_N)$ and $\overline{A}_{w,d}(\mathscr{E}_N)$ are well defined.

We define the *N-th spectral function* of $\overline{\mathscr{E}}$ as

$$r_N(\delta;\overline{\mathscr{E}}) \doteq \frac{1}{N}\ln \overline{A}_{\lfloor \delta N\rfloor}(\mathscr{E}_N), \quad \text{for } \delta\in[0,1]$$

and the *asymptotic spectral function* of $\overline{\mathscr{E}}$ as

$$\widehat{r}(\delta;\overline{\mathscr{E}}) \doteq \limsup_{N\to\infty} r_N(\delta;\overline{\mathscr{E}}), \quad \text{for } \delta\in[0,1]. \tag{2.10}$$

Whenever $\overline{\mathscr{E}}$ is clear from the context, spectral function will simply be denoted by $r_N(\delta)$ and $\widehat{r}(\delta)$, respectively.

Example 2.4 (Random linear encoder ensemble)**.** *For fixed $N\in\mathbb{N}$ and rate R, let $\mathscr{L}_N$ be the ensemble generated by the set of all generator $\lfloor RN\rfloor \times N$-binary matrices. This is equivalent to the ensemble formed by choosing each entry of a random generator matrix i.i.d. according to a Bernoulli with parameter* $1/2$.

The average output weight enumerators for the linear encoder ensemble can be computed to be (see [29, 30])

$$\overline{A}_d\left(\mathscr{L}_N\right) = \begin{cases} 1+\frac{2^{\lfloor RN\rfloor}-1}{2^N} & d=0\\ \binom{N}{d}\frac{2^{\lfloor RN\rfloor}-1}{2^N} & 1\le d\le N. \end{cases} \tag{2.11}$$

Since the average number of weight-zero codewords is larger than one, there will always be some encoders in this ensemble which are not invertible.

Let now $\overline{\mathscr{L}} = \{\mathscr{L}_N\}_{N\in\mathbb{N}}$. It can be verified that the asymptotic spectral function has the following expression

$$\widehat{r}(\delta;\overline{\mathscr{L}}) = H(\delta) - (1-R)\ln 2 \tag{2.12}$$

where $H(\delta) = -\delta\ln\delta - (1-\delta)\ln(1-\delta)$ is the binary entropy function on the natural base.

Notice that $\widehat{r}(\delta_{GV}(R);\overline{\mathscr{L}}) = 0$ and that the spectral function is negative for $\delta < \delta_{GV}(R)$.

One of the uses of the average weight enumerators and the corresponding spectral functions is to obtain probabilistic information on the minimum distance of the encoders of the ensemble. Indeed the union bound leads to the following estimation

Lemma 2.1 (Lemma 1 in [44])**.**

$$\mathbb{P}\left(d_{\min}(\mathscr{E}) < d\right) \le \sum_{h=1}^{d-1} \overline{A}_h(\mathscr{E})\,, \tag{2.13}$$

where $d_{\min}(\mathscr{E})$ denotes the minimum distance as a random variable on the ensemble.

Proof. Let ϕ be an encoder chosen uniformly from the ensemble $\mathscr{E}$ and $\{A_h(\phi)\}_{h=1}^n$ be weight enumerators defined in (2.4). We thus have

$$\begin{aligned}\mathbb{P}(d_{\min}(\mathscr{E}) < d) = \mathbb{P}\left((A_0(\phi) > 1) \cup \bigcup_{h=1}^{d-1}(A_h(\phi) > 0)\right) = \\ = \mathbb{P}\left((A_0(\phi) - 1 \ge 1) \cup \bigcup_{h=1}^{d-1}(A_h(\phi) \ge 1)\right).\end{aligned}$$

By *union bound* estimation we get

$$\begin{aligned}\mathbb{P}(d_{\min}(\mathscr{E}) < d) \le \mathbb{P}(A_0(\phi) - 1 \ge 1) + \sum_{h=1}^{d-1}\mathbb{P}(A_h(\phi) \ge 1) \le \\ \le \overline{A}_0(\mathscr{E}) - 1 + \sum_{h=1}^{d-1}\overline{A}_h(\mathscr{E}),\end{aligned}$$

where the last step is obtained by using Markov inequality.

□

We have the following simple result:

Proposition 2.2. *Consider a sequence of encoder ensembles* $\overline{\mathscr{E}} = \{\mathscr{E}_N\}_{N\in\mathbb{N}}$. *If there exists* δ_0 *such that*

$$\sup_{\sigma\leq\delta} \widehat{r}(\sigma; \overline{\mathscr{E}}) < 0, \ \forall\delta < \delta_0$$

then, for any $\epsilon > 0$,

$$\mathbb{P}\left(d_{\min}(\mathscr{E}_N) < (\delta_0 - \epsilon)N\right) \overset{N\to\infty}{\longrightarrow} 0. \tag{2.14}$$

Proof. This is a straightforward application of inequality (2.13) considering that $\overline{A}_h(\mathscr{E}_N) = \exp\{N r_N(h/N; \overline{\mathscr{E}})\}$. □

Example 2.5 (Random linear encoder ensemble)**.** *The use of Proposition 2.2 makes surprisingly easy the estimation of the minimum distance growth rate of a typical binary linear encoder, chosen uniformly from the set* $\mathscr{L}_N$.

Notice that the asymptotic spectral function given in (2.12) *is negative for* $\delta < \delta_{GV}(R)$, *crosses zero at* $\delta = \delta_{GV}(R)$ *then is positive for* $\delta \in (\delta_{GV}(R), 1 - \delta_{GV}(R))$. *By Proposition 2.2, it follows that for any* $\epsilon > 0$,

$$\mathbb{P}\left(d_{\min}(\mathscr{L}_N) < (\delta_{GV}(R) - \epsilon)N\right) \overset{N\to\infty}{\longrightarrow} 0. \tag{2.15}$$

Weight distribution of convolutional encoders 3

Brief—In this chapter, the input–output weight distribution functions of truncated convolutional encoders are studied. In particular, they can be expressed in terms of multivariate power series with non-negative coefficients. Although explicit analytic expressions can be computed for relatively small truncation lengths, the explicit expressions become prohibitively complex to compute as truncation lengths and weights increase. Fortunately, a very accurate asymptotic expansion can be derived using the Multidimensional Saddle Point method (MSP-metohd). This approximation is substantially easier to evaluate and is used to obtain an expression for the asymptotic spectral function and to prove continuity and concavity. This approximation is substantially easier to evaluate and is used to obtain an expression for the asymptotic spectral function and to prove continuity and concavity. Finally, this approach is able to guarantee that the sequence of exponential growth rate converges uniformly to the asymptotic limit and to estimate the speed of this convergence.

3.1 Introduction and outline of the chapter

Convolutional encoders can be seen as finite-state machines with linear update of the state and of the output. The code sequence that emerges from the encoder depends upon previous message symbols as well as the present ones. A finite state map can be pictorially described by a trellis and the sequence of the states transitions (and corresponding input-output stream) can be seen as a path through a trellis.

Although the natural setting considers encoders that map semi-infinite sequence into semi-infinite stream, in main applications convolutional encoders are used with a fixed block-length. Every block is obtained by letting the state machine to evolve a finite number of steps, or, equivalently, by truncating the trellis at a fixed depth, called *truncation length*.

The weight distribution of convolutional encoders has been extensively studied in the literature. Here, we address the issue to estimate growth rate of the weight distribution as a function of truncation length and to investigate some additional properties about the asymptotic spectral function.

As a first step, we express the input–output weight enumerators of truncated convolutional encoders as coefficients of generating functions of error events (paths in the trellis starting and ending in the zero state and taking non-zero state values in between). Although explicit analytic expressions can be computed for relatively small truncation lengths, the explicit expressions become computationally complex as truncation lengths and weights increase.

The extraction of coefficients in a fixed enumerating function constitutes a crucial issue in enumerative combinatorics [62]. A technique to approximate the growth rate of coefficients of some generating function has been developed in [66, 67] and applied in [21, 42, 43] in the context of coding theory. We will prove that a similar approach can be extended also to approximate coefficients of generating functions of error events. This approximation is substantially easier to evaluate and is used to obtain an expression for the asymptotic spectral function. It can be proved that this expression can be recast into the formulation given in [49]. Our new representation put in emphasis that the spectral function is continuous and concave. Second, this approach is able to guarantee that the sequence of exponential growth rate converges uniformly to the asymptotic limit and to estimate the speed of this convergence. All these properties are useful to derive results regarding ML properties of concatenated coding schemes (see [19]) and to prove results in next chapter. Finally, although the asymptotic expression can in general only be evaluated numerically, the numerical procedure can be conveniently implemented using any standard algorithm for unconstrained minimization of a convex function (e.g., gradient descent).

The material is organized as follows. We introduce preliminary facts on convolutional encoders (Section 3.2). In particular, we discuss the controller canonical form, minimal realizations of a convolutional encoder, and we define the concept of error events. In Section 3.3 we state our main results. In particular we provide exact formulæ and accurate approximations of weight enumerators and of their exponential growth rate as a function of the truncation length. Some examples and numerical results are shown in Section 3.4. Technical proofs are collected in Section 3.5. Section 3.6 contains some concluding remarks. Some more technical proofs about asymptotic estimates of powers of series with nonnegative coefficients can be found in Appendix A.

3.2 Fundamental facts on convolutional encoders

In this section we recall some basic system-theoretic properties about convolutional encoders. Further details can be found in [24, 25, 29].

3.2.1 Convolutional encoders and weight enumerators

Let $V((D))$ be the $\mathbb{Z}_2$-vector space of formal Laurent series with coefficient in the $\mathbb{Z}_2$-vector space V. Elements in $V((D))$ are represented as $\sum_{-\infty}^{+\infty} \boldsymbol{v}_t D^t$ with $\boldsymbol{v}_t = 0$ for t sufficiently small. Inside $V((D))$ we consider the subspace of causal Laurent series with coefficients in V, denoted by $V[[D]]$, and the subspace of rational functions $V(D)$.

Definition 3.1. *Given $\boldsymbol{v} \in V((D))$, we define the support of $\boldsymbol{v}$ as* $\mathrm{supp}(\boldsymbol{v}) := \{t \in \mathbb{Z} | \boldsymbol{v}_t \neq \boldsymbol{0}\}$ *and the Hamming weight as* $\mathrm{w_H}(\boldsymbol{v}) := \sum_t \mathrm{w_H}(\boldsymbol{v}_t)$.

Given $\boldsymbol{v}^1, \boldsymbol{v}^2 \in V((D))$ and $\widetilde{t} \in \mathbb{Z}$ we define the concatenation of $\boldsymbol{v}^1 \vee_{\widetilde{t}} \boldsymbol{v}^2$ at $\widetilde{t}$ as the Laurent series

$$(\boldsymbol{v}^1 \vee_{\widetilde{t}} \boldsymbol{v}^2)_t = \begin{cases} \boldsymbol{v}^1_t & \text{if } t < \widetilde{t} \\ \boldsymbol{v}^2_t & \text{if } t \geq \widetilde{t} \end{cases}$$

We will also consider multiple concatenations of Laurent series $\boldsymbol{v}_1 \vee_{t_1} \boldsymbol{v}_2 \vee_{t_2} \boldsymbol{v}_2 \ldots \vee_{t_{m-1}} \boldsymbol{v}_m$ at concatenation times $t_1 < t_2 < \ldots < t_{m-1}$. If $\boldsymbol{v} \in V((D))$ and $I \in \mathbb{Z}$, we define the restriction of $\boldsymbol{v}$ to I as the element $\boldsymbol{v}|_I \in V^I$ such that $(\boldsymbol{v}|_I)_t = \boldsymbol{v}_t$ for every $t \in I$.

As a convolutional encoder we mean a homomorphic map $\psi : \mathbb{Z}_2^k((D)) \to \mathbb{Z}_2^n((D))$ which acts as a multiplicative operator $\psi(\boldsymbol{u}(D)) = \boldsymbol{u}(D)\boldsymbol{\Psi}(D)$, where $\boldsymbol{\Psi} \in \mathbb{Z}_2^{k\times n}(D) \cap \mathbb{Z}_2^{k\times n}[[D]]$. We define the corresponding code to be the image of the encoder $\mathcal{C}_\psi = \psi\left(\mathbb{Z}_2^k((D))\right)$ and $\boldsymbol{x}(D) \in \mathcal{C}_\psi$ is a codeword.

As convolutional encoders are rational, there exist a finite state space $Z = \mathbb{Z}_2^\mu$ and matrices $\mathbf{F} \in \mathbb{Z}_2^{\mu\times\mu}$, $\mathbf{G} \in \mathbb{Z}_2^{\mu\times k}$, $\mathbf{H} \in \mathbb{Z}_2^{n\times\mu}$ and $\mathbf{L} \in \mathbb{Z}_2^{n\times k}$ such that $\boldsymbol{x}(D) = \boldsymbol{u}(D)\boldsymbol{\Psi}(D)$ if and only if there exists a state sequence $\boldsymbol{z}(D) \in Z((D))$ satisfying

$$\begin{cases} \boldsymbol{z}_{t+1} &= \mathbf{F}\boldsymbol{z}_t + \mathbf{G}\boldsymbol{u}_t \\ \boldsymbol{x}_t &= \mathbf{H}\boldsymbol{z}_t + \mathbf{L}\boldsymbol{u}_t \end{cases} \tag{3.1}$$

Let us now consider the realization $(\mathbf{F}, \mathbf{G}, \mathbf{H}, \mathbf{L})$ of convolutional encoder $\boldsymbol{\Psi}$. By fixing $\boldsymbol{z}_0 = \boldsymbol{0}$ —which is the usual assumption that the shift register is empty at the beginning of the encoding process— the sequence $\boldsymbol{z}(D)$ is uniquely determined by the input sequence $\boldsymbol{u}(D)$ through the dynamical equations in (3.1); we will say that such $\boldsymbol{z}(D)$ is the state sequence associated with $\boldsymbol{u}(D)$. The interpretation of this representation is discussed in detail in [29].

A finite state map can be pictorially described by a trellis, by drawing, at each time step t, vertices corresponding to the elements of $\mathbb{Z}_2^\mu$, and edge from vertex $\boldsymbol{z}_t$ to vertex $\boldsymbol{z}_{t+1}$, with input tag $\boldsymbol{u}_t$ and output label $\boldsymbol{x}_t$. Formally we have the following definition.

Definition 3.2. *We define the trellis or state diagram of* $(\mathbf{F},\mathbf{G},\mathbf{H},\mathbf{L})$ *as the labeled directed graph given by the vertex set* $\mathbb{Z}_2^\mu$ *and the set of edges*

$$\begin{aligned}\{\boldsymbol{z}_t \overset{(\boldsymbol{u}_t,\boldsymbol{x}_t)}{\longrightarrow} \boldsymbol{z}_{t+1} | \boldsymbol{z}_t, \boldsymbol{z}_{t+1} \in \mathbb{Z}_2^\mu, \boldsymbol{u}_t \in \mathbb{Z}_2^k, \boldsymbol{x}_t \in \mathbb{Z}_2^n :& \\ \boldsymbol{z}_{t+1} = \mathbf{F}\boldsymbol{z}_t + \mathbf{G}\boldsymbol{u}_t, \boldsymbol{x}_t = \mathbf{H}\boldsymbol{z}_t + \mathbf{L}\boldsymbol{u}_t\}&\end{aligned}$$

Notice that the trellis is not an invariant of the code. It depends on the choice of the generator matrix as well as on the realization.

Definition 3.3. *A path in the trellis of length* l *is a sequence of edges of the form*

$$\boldsymbol{z}_{t_0} \overset{(\boldsymbol{u}_{t_0},\boldsymbol{x}_{t_0})}{\longrightarrow} \boldsymbol{z}_{t_1} \overset{(\boldsymbol{u}_{t_1},\boldsymbol{x}_{t_1})}{\longrightarrow} \boldsymbol{z}_{t_2} \overset{(\boldsymbol{u}_{t_1},\boldsymbol{x}_{t_1})}{\longrightarrow} \dots \overset{(\boldsymbol{u}_{t_{l-1}},\boldsymbol{x}_{t_{l-1}})}{\longrightarrow} \boldsymbol{z}_{t_l}$$

It is well-known [29] that each encoder admits a minimal realization (i.e., with observability and controllability properties and with smallest state dimension μ). From now on we will always assume that we are using the minimal trellis.

Now we define some properties of particular convolutional encoders, which will be fundamental in our setting.

Definition 3.4. *Given* $\psi \in \mathbb{Z}_2^{k\times n}(D)$ *we say that* ψ *is* non catastrophic *if every output with compact support comes from an input with compact support.*

Notice that systematic encoders are surely non-catastrophic. We have for non-catastrophic encoders the following characterization: there exists $\zeta > 0$ such that, for all input sequence $\boldsymbol{u}$ it holds $\mathrm{w_H}(\boldsymbol{u}) \leq \zeta \mathrm{w_H}(\psi(\boldsymbol{u}))$.

Given $\psi \in \mathbb{Z}_2^{k\times n}(D)$ we say that ψ is *recursive* if no output with compact support comes from an input with Hamming weight one. Formally, we have the following definition.

Definition 3.5. *The convolutional encoder* $\psi \in \mathbb{Z}_2^{k\times n}(D)$ *is recursive if, for all* $\boldsymbol{u} \in \mathbb{Z}_2^k((D))$*, it holds the following implication*

$$|\mathrm{w_H}(\boldsymbol{u})| = 1 \Longrightarrow \mathrm{w_H}(\phi(\boldsymbol{u})) = +\infty.$$

3.2.2 Truncated convolutional encoders

Given a convolutional encoder $\psi \in \mathbb{Z}_2^{k\times n}(D)$ and fixed $N \in \mathbb{N}$, consider the block encoder $\psi_N : \mathbb{Z}_2^{kN} \to \mathbb{Z}_2^{nN}$ obtained by restricting the inputs of the convolutional encoder ψ to those inputs supported inside the window $[0, N-1]$ and taking the projection of the output on the coordinates also in $[0, N-1]$, namely

$$\psi_N\left(\boldsymbol{u}, \boldsymbol{u}_1, \dots, \boldsymbol{u}_{N-1}\right) = \left(\boldsymbol{x}_0, \boldsymbol{x}_1, \dots, \boldsymbol{x}_{N-1}\right)$$

if

$$\psi(\boldsymbol{u}_0 + \boldsymbol{u}_1 D + \dots + \boldsymbol{u}_{N-1} D^{N-1}) = \boldsymbol{x}_0 + \boldsymbol{x}_1 D + \dots + \boldsymbol{x}_{N-1} D^{N-1} + o(D^{N-1})$$

We say that ψ_N is the truncated convolutional encoder with truncation length N.

For any block encoder ψ_N, obtained by truncating a convolutional encoder $\psi \in \mathbb{Z}_2^{k\times n}(D) \cap \mathbb{Z}_2^{k\times n}[[D]]$, we define the *input–output weight enumerator* as

$$A_{w,d}(\psi_N) := |\{\boldsymbol{u} \in (\mathbb{Z}_2^k)^N : \mathrm{w_H}(\boldsymbol{u}) = w, \mathrm{w_H}(\psi_N(\boldsymbol{u})) = d\}|.$$

We are interested in the linear term of their exponential growth rate. For a given convolutional encoder and $(u,\delta) \in [0,1]^2$, we define the *input–output weight distribution function*

$$G_N(u,\delta;\psi) := \begin{cases} \frac{\ln A_{\lfloor ukN \rfloor, \lfloor \delta n N \rfloor}(\psi_N)}{nN} & \text{if } A_{\lfloor ukN \rfloor, \lfloor \delta n N \rfloor}(\psi_N) > 0, \\ -\infty & \text{if } A_{\lfloor ukN \rfloor, \lfloor \delta n N \rfloor}(\psi_N) = 0 \end{cases}$$

and the asymptotic growth rate as

$$G(u,\delta;\psi) := \lim_{N\to\infty} G_N(u,\delta;\psi).$$

We will also use the *output weight enumerators* $A_d(\psi_N) = \sum_w A_{w,d}(\psi_N)$ and the *output weight distribution function* $G(\delta) = \max_{u\in[0,1]} G(u,\delta)$.

3.2.3 Error events and their generating functions

The concatenation of Laurent series defined in the previous section leads to the following definitions. Some of these definitions can also be found in [50].

Definition 3.6 (Error event)**.** *The sequence $\boldsymbol{u} \in \mathbb{Z}_2^k((D))$ is an error event for ψ if there exists t_b and $t_e \in \mathbb{Z}$ such that $t_b < t_e$ and* $\mathrm{supp}(\boldsymbol{u}) \subseteq [t_b, t_e]$, $\mathrm{supp}(\boldsymbol{z}) = [t_b + 1, t_e]$ *where $\boldsymbol{z}(D) \in Z((D))$ is the state sequence associated to the input sequence $\boldsymbol{u}$. Notice that this implies that necessarily $\boldsymbol{u}_{t_b} \neq \boldsymbol{0}$ and* $\mathrm{supp}(\psi(\boldsymbol{u})) \subseteq [t_e, t_b]$*. We call $[t_b, t_e]$ the active window and we denote by $l(\boldsymbol{u}) = t_e - t_b + 1$ the length of the (input) error event.*

Error events can be depicted as path in the trellis starting and ending in the zero state and taking non-zero state values in between. Every non-zero codeword of a convolutional code (known also as molecular codewords) can be thought as composition of several concatenated error events.

In the classical analysis, essential design parameter of a convolutional encoder is its *free distance.*

Definition 3.7. *Given a convolutional encoder $\psi \in \mathbb{Z}_2^{k\times n}$, we define the free distance of ψ to be*

$$d_f(\psi) := \min\{\mathrm{w_H}(\psi(\boldsymbol{u})) | \boldsymbol{u} \neq \boldsymbol{0}\}.$$

If we consider truncated convolutional encoder, it might happen that the state sequence is not in the 0 state at time N. Thus we have to distinguish two types of error events for the family of truncated convolutional encoder: the regular and the truncated error events.

Definition 3.8 (Regular error events)**.** *An input vector $\boldsymbol{u} \in (\mathbb{Z}_2^k)^N$ is a regular error event of length $l \leq N$ for ψ_N if $\boldsymbol{u}(D) \in \mathbb{Z}_2^k((D))$ is an error event of length l for ψ.*

Definition 3.9 (Truncated error events)**.** *An input vector $\boldsymbol{u} \in \mathbb{Z}_2^{kN}$ is a truncated error event of length $l \leq N$ for ψ_N if there exists $T \in [0, N]$ such that the correspondent state sequence is such that $\boldsymbol{z}_t = 0\ \forall t \leq T$ and $\boldsymbol{z}_t \neq 0\ \forall T \leq t \leq N$ with $l = N - T$.*

These definitions lead to classify codewords as regular and truncated. We denote with $R_{w,d}(\psi_N)$ and $T_{w,d}(\psi_N)$ the number of input sequences having input weight w, output weight d, and consisting exclusively of regular error events, or containing a truncated error event, respectively. We thus have $A_{w,d}(\psi_N) = R_{w,d}(\psi_N) + T_{w,d}(\psi_N)$.

Let ψ_N be the block encoder obtained by truncating after N trellis steps a convolutional encoder $\psi \in \mathbb{Z}_2^{k\times n}(D) \cap \mathbb{Z}_2^{k\times n}[[D]]$. Let μ be the dimension of the state space. Consider a triple (w, d, l), we denote by $E_{w,d,l}$ the number of distinct error events of input weight w, output weight d and length l. Define the following formal power series

$$E(x, y, z) = \sum_{w,d,l} E_{w,d,l} x^w y^d z^l$$

The function $E(x, y, z)$ is called the *detour generating function* [21].

To display this function, we collect the information regarding the effect of the state transitions at each step, except for the zero state, in the matrix form. This matrix, also known as *transition matrix*, appears in different forms in [21, 49, 50, 68]. Fix an ordering of the states. The transition matrix $\mathbf{M} \in (\mathbb{N}_0[x, y, z])^{2^\mu-1\times 2^\mu-1}$ is defined as follows. If there is one step transition from state $\boldsymbol{z}$ to state $\boldsymbol{v}$ with input $\boldsymbol{u}$ and output $\boldsymbol{x}$ we set the $M_{\boldsymbol{v},\boldsymbol{z}}$ entry with a label $x^{\mathrm{w_H}(\boldsymbol{u})} y^{\mathrm{w_H}(\boldsymbol{x})} z$ where $\mathrm{w_H}(\boldsymbol{u})$ is the weight of input sequence that takes the machine from state $\boldsymbol{z}$ to state $\boldsymbol{v}$, $\mathrm{w_H}(\boldsymbol{x})$ is the corresponding output weight and z takes into account the step in the trellis. Otherwise, we set $M_{\boldsymbol{v},\boldsymbol{z}} = 0$ if there is no one step transition from state $\boldsymbol{z}$ to state $\boldsymbol{v}$. Formally, we have

$$M_{\boldsymbol{v},\boldsymbol{z}} = \begin{cases} x^{\mathrm{w_H}(\boldsymbol{u})} y^{\mathrm{w_H}(\boldsymbol{x})} z & \text{if } \boldsymbol{z} \xrightarrow{(\boldsymbol{u},\boldsymbol{x})} \boldsymbol{v} \\ 0 & \text{otherwise} \end{cases}$$

Notice that, once we have fixed an ordering of the states, we will always choose the same ordering for the row index and for the column index. The transfer matrix depends exclusively on the minimal realization of the encoder. In this sense, the transition matrix is well defined up to similarity transformation via a permutation matrix [69].

In similar way, let $\boldsymbol{a}, \boldsymbol{b} \in (\mathbb{N}_0[x, y, z])^{2^\mu-1}$ be the vectors which encode the effect of the transitions from state $\mathbf{0}$ to state $\boldsymbol{z}$ and from state $\boldsymbol{v}$ to state $\mathbf{0}$, respectively:

$$\boldsymbol{a}_{\boldsymbol{z}} = \begin{cases} x^{\mathrm{w_H}(\boldsymbol{u})} y^{\mathrm{w_H}(\boldsymbol{x})} z & \text{if } \boldsymbol{0} \xrightarrow{(\boldsymbol{u},\boldsymbol{x})} \boldsymbol{z} \\ 0 & \text{otherwise} \end{cases}$$

$$\boldsymbol{b}_{\boldsymbol{v}} = \begin{cases} x^{\mathrm{w_H}(\boldsymbol{u})} y^{\mathrm{w_H}(\boldsymbol{x})} z & \text{if } \boldsymbol{v} \xrightarrow{(\boldsymbol{u},\boldsymbol{x})} \boldsymbol{0} \\ 0 & \text{otherwise} \end{cases} .$$

With this formalism the formal power series $E(x, y, z)$ can be represented as follows

$$E(x, y, z) = \sum_j \boldsymbol{b}(x, y, z)^T \mathbf{M}(x, y, z)^j \boldsymbol{a}(x, y, z). \tag{3.2}$$

We define the truncated detour generating function as follows

$$\widetilde{E}(x, y, z) := \sum_{w,d,l} \widetilde{E}_{w,d,l} x^w y^d z^l,$$

where $\widetilde{E}_{w,d,l}$ is the number of paths that start but do not end in the zero state and have no zero transition through the trellis with input weight w, output weight d and length l. With previous formalism we have

$$\widetilde{E}(x, y, z) = \sum_i \left[\sum_j \mathbf{M}^j(x, y, z) \boldsymbol{a}(x, y, z) \right]_i . \tag{3.3}$$

Other algorithms for computing the generating function of error events while avoiding the big transition matrix are Viterbi's method, see [68], or Mason's gain formula as described in [70]. Further methods can be found in [71].

3.3 Main results

In this section we describe how to compute the weight distribution of a convolutional code in terms of the trellis representation and its corresponding exponential growth rate. The resulting expressions are either new, or otherwise require more laborious methods to obtain. We discuss in detail our contribution.

In the following, we present a new representation for the weight enumerators of convolutional encoders. A main tool is the use of generating function of both kinds of error event (regular and truncated). We will use the subsequent expressions to evaluate the growth rate of the weight distribution as a function of truncation length N.

Consider the following formal power series

$$F(x, y, z) := \frac{E(x, y, z)}{(1 - z)} \tag{3.4}$$

$$L(x, y, z) := \frac{1}{1 - z} + \frac{\widetilde{E}(x, y, z)}{E(x, y, z)}. \tag{3.5}$$

At the moment we do not require any concept of convergence and we interpret x, y, z as formal indeterminates.

Theorem 3.1 (Weight enumerators)**.** *The weight distribution of a truncated convolutional encoder ψ_N is given by*

$$A_{w,d}(\psi_N) = \sum_{t=1}^{N} \text{coeff}\left\{L(x,y,z)F(x,y,z)^t, x^w y^d z^N\right\}. \tag{3.6}$$

While the computation of the expression in (3.6) is easy for reasonably sized parameters, it quickly becomes unpractical when the truncation length N is growing. Notice that formula in (3.6) involves powers of series with nonnegative coefficients. A technique for approximate evaluation of the growth rate of coefficients of a multivariate polynomial has been developed in [66, 67] and applied in [21, 42, 43] to evaluate weight and stopping set distribution of LDPC. We will prove that a similar approach can be extended also to approximate coefficients of generating functions in (3.6). With this technique we obtain the asymptotic exponential growth rate of (3.6), which can indeed be estimated much more easily.

Define the following set

$$\mathcal{W} := \{(u,\delta) \in [0,1]^2 | \exists N_0 \in \mathbb{N} : R_{\lfloor ukN_0 \rfloor, \lfloor \delta n N_0 \rfloor}(\psi_{N_0}) > 0\}. \tag{3.7}$$

Proposition 3.1. *$\mathcal{W}$ is convex and closed.*

Theorem 3.2 (Asymptotic growth rate)**.** *For a given convolutional encoder ψ, when $N \to \infty$ the functions $G_N(u,\delta;\psi)$ converge uniformly for all $(u,\delta) \in \mathcal{W}$ to*

$$G(u,\delta;\psi) = \begin{cases} \dfrac{\max\limits_{\alpha\in[0,1]} \min\limits_{(x,y,z)\in\Sigma^+} \{\alpha \ln F(x,y,z) - uk\ln x - \delta n \ln y - \ln z\}}{n} & \text{if } (u,\delta) \in \mathcal{W} \\ -\infty & \text{otherwise} \end{cases} \tag{3.8}$$

where $\mathcal{W}$ is defined in (3.7), $\Sigma \subseteq \mathbb{R}^3$ is the region of absolute convergence of the power series $F(x,y,z)$, and $\Sigma^+ = \Sigma \cap (\mathbb{R}^+)^3$.

The espression in (3.8) points out the following property, conjectured in [46] but never proved before.

Corollary 3.1. *$G(u,\delta;\psi)$ is continuous and concave with respect to u and δ in $\mathcal{W}$.*

An algorithm to efficiently compute the asymptotic growth rate of the weight distribution for a convolutional encoder was already given by Sason et al. in [49]. We improve their results in the following ways. First, the continuity and concavity of function $G(u,\delta,\psi)$ is guaranteed with our representation

(3.1). Second, we can ensure the uniform convergence in both variables u and δ of functions $G_N(u, \delta; \psi)$ to the asymptotic limit $G(u, \delta; \psi)$. Although the expression in (3.8) can in general only be evaluated numerically, the minimization required can be conveniently implemented by minimizing

$$f(\xi_1, \xi_2, \xi_3) = \widehat{F}_\alpha(\mathrm{e}^{\xi_1}, \mathrm{e}^{\xi_2}, \mathrm{e}^{\xi_3}),$$

where

$$\widehat{F}_\alpha(x, y, z) = \ln\left[\frac{F(x, y, z)^\alpha}{x^{uk} y^{\delta n} z}\right].$$

using any standard algorithm for unconstrained minimization of a convex function (e.g., gradient descent).

Finally, we present an approximation for the weight distribution of finite truncation-length (not only the exponent) and, consequently, we can estimate the measure of the convergence of the sequence of exponential $G_N(u, \delta; \psi)$ to the asymptotic limit.

Theorem 3.3 (Finite length approximation)**.** *Suppose the set*

$$\mathscr{F} = \{(k_1, k_2, k_3) \in \mathbb{Z}^3 | \mathrm{coeff}\{F(x, y, z), x^{k_1} y^{k_2} z^{k_3}\} > 0\}$$

generates $\mathbb{Z}^\nu$ as an abelian group. Then, for $N \to \infty$

$$A_{\lfloor ukN \rfloor, \lfloor \delta nN \rfloor}(\psi_N) \sim \frac{\sqrt{2\pi\sigma^2}\, L(x_{\alpha^\star}, y_{\alpha^\star}, z_{\alpha^\star})}{\sqrt{(2\pi\alpha^\star N)^\nu |\mathbf{\Gamma}_{\alpha^\star}|}} \, \frac{F(x_{\alpha^\star}, y_{\alpha^\star}, z_{\alpha^\star})^{\alpha^\star N}}{x_{\alpha^\star}^{ukN}\, y_{\alpha^\star}^{\delta nN}\, z_{\alpha^\star}^{N}} \tag{3.9}$$

where $(x_\alpha, y_\alpha, z_\alpha) \in (\mathbb{R}^+)^3$ is the unique solution of the following system

$$\begin{cases} \frac{x}{F(x,y,z)} \frac{\partial F(x,y,z)}{\partial x} = \frac{uk}{\alpha} \\ \frac{y}{F(x,y,z)} \frac{\partial F(x,y,z)}{\partial y} = \frac{\delta n}{\alpha} \\ \frac{z}{F(x,y,z)} \frac{\partial F(x,y,z)}{\partial z} = \frac{1}{\alpha} \end{cases} \tag{3.10}$$

and $\alpha^\star$ and $\Gamma_{\alpha^\star}$ are defined by

$$\alpha^\star = \underset{0 \le \alpha \le 1}{\mathrm{argmax}} \left\{\alpha \ln F(x_\alpha, y_\alpha, z_\alpha) - uk \ln x_\alpha - \delta n \ln y_\alpha - \ln z_\alpha\right\},$$

$$\mathbf{\Gamma}_{\alpha^\star} = \left.\begin{pmatrix} x\frac{\partial}{\partial x}\left(\frac{x}{F}\frac{\partial F}{\partial x}\right) & y\frac{\partial}{\partial y}\left(\frac{x}{F}\frac{\partial F}{\partial x}\right) & z\frac{\partial}{\partial z}\left(\frac{x}{F}\frac{\partial F}{\partial x}\right) \\ x\frac{\partial}{\partial x}\left(\frac{y}{F}\frac{\partial F}{\partial y}\right) & y\frac{\partial}{\partial y}\left(\frac{y}{F}\frac{\partial F}{\partial y}\right) & z\frac{\partial}{\partial z}\left(\frac{y}{F}\frac{\partial F}{\partial y}\right) \\ x\frac{\partial}{\partial x}\left(\frac{z}{F}\frac{\partial F}{\partial z}\right) & y\frac{\partial}{\partial y}\left(\frac{z}{F}\frac{\partial F}{\partial z}\right) & z\frac{\partial}{\partial z}\left(\frac{z}{F}\frac{\partial F}{\partial z}\right) \end{pmatrix}\right|_{(x_{\alpha^\star}, y_{\alpha^\star}, z_{\alpha^\star})}.$$

Some examples in Section 3.4 show that this approximation is very accurate even for quite short truncation lengths. Explicit applications of these theorems are developed in [19] and [61].

3.4 Some examples

We discuss our theorems and we use them to compute enumerating functions of some convolutional encoders. We now show that our method provides explicit analytic expressions and we can improve the approximation given in Theorem 3.3 in some specific cases.

3.4.1 Accumulate encoder

Let Acc_N be the block encoder obtained by the truncation after N trellis steps of the convolutional encoder with transfer function $G(D) = (1 + D)^{-1}$. The weight transition diagram is depicted in Figure 3.1.

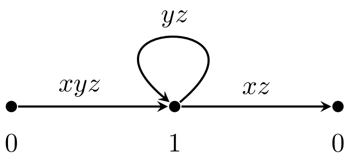


Figure 3.1: Accumulate encoder: weight transition diagram

In this case the generating functions of error events are given by the following formal power series

$$E(x,y,z) = x^2yz^2\sum_{k=0}^{+\infty}(yz)^k = \frac{x^2yz^2}{(1-yz)} \qquad \widetilde{E}(x,y,z) = xyz\sum_{k=0}^{+\infty}(yz)^k = \frac{xyz}{1-yz}.$$

Using Theorem 3.1, we get that if w is even then $T_{w,d}(\mathrm{Acc}_N) = 0$; otherwise, if w is odd then $R_{w,d}(\mathrm{Acc}_N) = 0$.

We now give the computation in detail: if w is even, then

$$\begin{aligned}
R_{w,d}(\mathrm{Acc}_N) &= \sum_{t=1}^{N} \mathrm{coeff}\left\{\frac{x^{2t}y^tz^{2t}}{(1-z)^{t+1}(1-yz)^t}, x^wy^dz^N\right\} \\
&\overset{t=w/2}{=} \mathrm{coeff}\left\{\frac{1}{(1-z)^{w/2+1}(1-yz)^{w/2}}, y^{d-w/2}z^{N-w}\right\} \\
&= \mathrm{coeff}\left\{\frac{1}{(1-z)^{w/2+1}(1-s)^{w/2}}, s^{d-w/2}z^{N-d-w/2}\right\} \\
&= \mathrm{coeff}\left\{\frac{1}{(1-s)^{w/2}}, s^{d-w/2}\right\}\mathrm{coeff}\left\{\frac{1}{(1-z)^{w/2+1}}, z^{N-d-w/2}\right\} \\
&= \binom{N-d}{\frac{w}{2}}\binom{d-1}{\frac{w}{2}-1};
\end{aligned}$$

if w is odd, then

$$\begin{aligned}
T_{w,d}(\mathrm{Acc}_N) &= \sum_{t=1}^{N} \mathrm{coeff}\left\{\frac{x^{2t-1}y^t z^{2t-1}}{(1-z)^t(1-yz)^t}, x^w y^d z^N\right\} \\
&\overset{t=(w+1)/2}{=} \mathrm{coeff}\left\{\frac{1}{(1-z)^{(w+1)/2}(1-yz)^{(w+1)/2}}, y^{d-(w+1)/2}z^{N-w}\right\} \\
&= \mathrm{coeff}\left\{\frac{1}{(1-z)^{(w+1)/2}(1-s)^{(w+1)/2}}, s^{d-(w+1)/2}z^{N-d-(w-1)/2}\right\} \\
&= \mathrm{coeff}\left\{\frac{1}{(1-s)^{(w+1)/2}}, s^{d-(w+1)/2}\right\} \mathrm{coeff}\left\{\frac{1}{(1-z)^{(w+1)/2}}, z^{N-d-(w-1)/2}\right\} \\
&= \binom{N-d}{\frac{w-1}{2}}\binom{d-1}{\frac{w+1}{2}-1},
\end{aligned}$$

from which

$$A_{w,d}(\mathrm{Acc}_N) = \binom{N-d}{\lfloor \frac{w}{2} \rfloor}\binom{d-1}{\lceil \frac{w}{2} \rceil - 1} \tag{3.11}$$

as derived with different combinatorial techniques in [48]. The asymptotic growth rate, as stated in [48], can be deduced easily.

After some manipulations, we have the following solution for the set of three equations in (3.10)

$$\alpha = \frac{u}{2} \qquad yz = 1 - \frac{u}{2\delta} \qquad z = 1 - \frac{u}{2(1-\delta)}.$$

Notice that the region of convergence of generating functions of error events is given by $\Sigma^+ = \{(x,y,z) \in (\mathbb{R}^+)^3 : 0 \le z < 1, 0 \le yz < 1\}$. Equivalently, the domain $\mathcal{W} = \{(u,\delta) \in [0,1]^2 | u \in [0, \min\{2\delta, 2(1-\delta)\}]$, which is convex and closed.

From Theorem 3.2 we get that

$$\begin{aligned}
G(u,\delta;\mathrm{Acc}) &= \frac{u}{2}\ln\frac{x^2yz^2}{(1-yz)(1-z)} - u\ln x - \delta\ln y - \ln z \\
&= \frac{u}{2}\ln yz - \frac{u}{2}\ln(1-yz) + \frac{u}{2}\ln\frac{z}{1-z} - u\ln x - \delta\ln y - \ln z \\
&= \frac{u}{2}\ln\left(1-\frac{u}{2\delta}\right) - \frac{u}{2}\ln\frac{u}{2\delta} + \frac{u}{2}\ln\frac{z}{1-z} - u\ln x - \delta\ln(yz) - (1-\delta)\ln z \\
&= \delta H\left(\frac{u}{2\delta}\right) + (1-\delta)H\left(\frac{u}{2(1-\delta)}\right).
\end{aligned} \tag{3.12}$$

Finally, following the procedure given in Section 5.3, one gets the following approximation:

$$G_N(u,\delta;\mathrm{Acc}) \sim -\frac{1}{2}\ln\left(\pi u N\frac{yz(1-z)^2}{(1-yz)^2}\right) + G(u,\delta) \qquad N \to \infty.$$

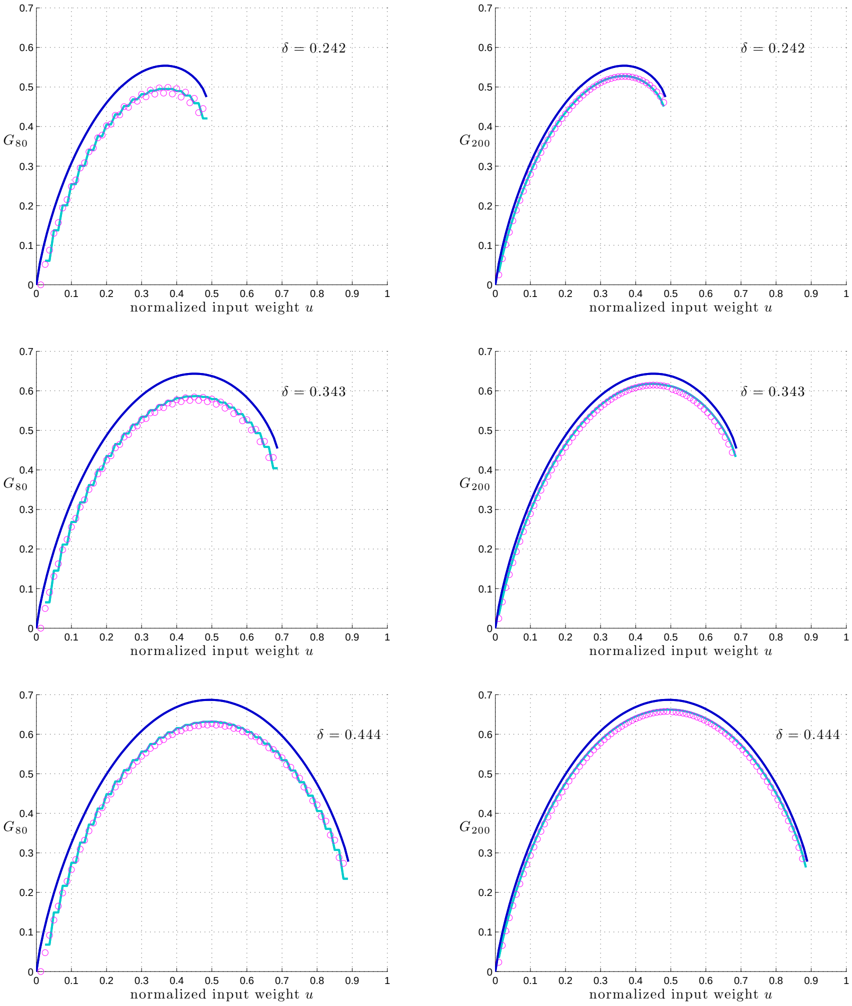


Figure 3.2: Fixed the output weight $\delta = 0.242, 0.343, 0.444$, the x-axis is the normalized input weight, the y-axis is the exponent of the weight distribution. The dots are the exact exponents of the weight enumerators. The bottom curve is the approximation using Theorem 3.3 while the upper curve is the asymptotic exponent. The plot is obtained for the truncation length $N = 80$ and $N = 200$.

Notice that this approximation is better compared with the assertion given in Theorem 3.3. This improvement comes from the fact that when we fix the input and output weight of the accumulate encoder the number of error events and the overall length is automatically determined and we do not need any extra factor in equation (3.9).

In Fig. 3.4.1 we show different results for truncation lengths $N = 80$ and $N = 200$. Notice that the approximation is very good even for these low values of N and, as to be expected, for increasing N both approximation and direct calculation result approach the asymptotic growth rate.

3.4.2 The (4,3) Single Parity Check Code

This code can be thought of as a truncated convolutional encoder $\psi \in \mathbb{Z}_2^{3\times 4}(D)$ with zero memory and $d_f(\psi) = 2$. We now focus on the output weight distribution function.

Also in this case we obtain explicit expression for weight enumerators.

The generating function of error events is given by

$$E(y,z) = (6y^2 + y^4)z$$

and from Theorem 3.1 we get

$$\begin{aligned} A_d(\psi) &= \sum_{t=1}^{N} \text{coeff}\left\{\frac{E(y,z)^t}{(1-z)^{t+1}}, y^d z^N\right\} = \sum_{t=1}^{N} \text{coeff}\left\{(6y^2+y^4)^t \frac{z^t}{(1-z)^{t+1}}, y^d z^N\right\} \\ &= \sum_{t=1}^{N} \text{coeff}\left\{(6y^2+y^4)^t, y^d\right\} \text{coeff}\left\{\frac{1}{(1-z)^{t+1}}, z^{N-t}\right\} \\ &= \sum_{t=1}^{N} \binom{N}{t} \text{coeff}\left\{(6+y^2)^t, y^{d-2t}\right\} = \sum_{t=1}^{N} \binom{N}{t} \text{coeff}\left\{(6+y)^t, y^{d/2-2t}\right\} \end{aligned}$$

from which $A_d(\psi) = 0$ if d is odd. If d is even

$$\begin{aligned} A_d(\psi) &= \sum_{t=1}^{d/2} \binom{N}{t} \text{coeff}\left\{\sum_{i=0}^{t} \binom{t}{i} 6^i y^{t-i}, y^{d/2-2t}\right\} \\ &= \sum_{t=1}^{N} \binom{N}{t} 6^{2t-d/2} \binom{t}{2t-d/2} \end{aligned}$$

The asymptotic growth rate can be deduced easily.

In Fig. 3.4.2 we compare the exact weight enumerators (computed above) with approximation obtained in Theorem 3.3 and the asymptotic spectral function provided by method described in Theorem 3.2. The truncation lengths are taken $N = 30$ and $N = 50$.

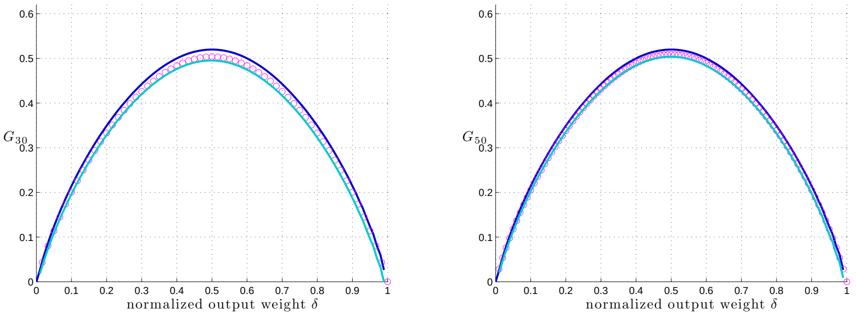


Figure 3.3: The x-axis is the normalized output weight, the y-axis is the exponent of the output weight distribution. The dots are the exact exponents of the weight enumerators. The bottom curve is the approximation using Theorem 3.3 while the upper curve is the asymptotic exponent. The plot is obtained for the truncation length $N = 30$ and $N = 50$.

3.5 Proofs

In this section we provide the proofs of results listed in Section 3.3. Here, the outline of the proofs.

- In Subsection 3.5.1 we prove Theorem 3.1 by using some combinatorial results about convolutional codes.
- Proofs of Proposition 3.1, Theorem 3.2, and Corollary 3.1 are provided in Subsection 3.5.2.
- Finally, the approximation of weight enumerators for finite length codes (Theorem 3.3) is derived in Subsection 3.5.3.

3.5.1 Exact method for weight enumerators

Here, we prove Theorem 3.1.

Proof of Theorem 3.1. A codeword is a concatenation of several error events, then we need to compute in how many ways one can arrange these patterns in their total length N such that their total input weight is w and their total output weight is d.

Given $w, d, t, l \in \mathbb{N}$, denote with $R_{w,d,t,l}(\psi_N)$ the cardinality of the set of all the input sequences $\boldsymbol{u} \in \mathbb{Z}_2^k[[D]]$ with input weight vector w, output weight d, obtained by concatenating t full error events, and whose total length is l. Take now into consideration the combinatorics of the 0's which separate the error events (what Sason et al. call *silent periods* in [49]): we have to dispose $N-l$ elements in at most $t+1$ different blocks (see Figure 3.4).

$$\underbrace{\circ\circ\cdots\circ\circ}_{a_1}\ \overset{1}{\bullet}\ \underbrace{\circ\circ\cdots\circ\circ}_{a_2}\ \overset{2}{\bullet}\ \cdots\cdots\ \overset{t}{\bullet}\ \underbrace{\circ\circ\cdots\circ\circ}_{a_{t+1}}$$

$$\begin{cases} \sum_{i=1}^{t+1} a_i = N-l \\ a_i \geq 0 \end{cases} \Longrightarrow C_{N-l,t+1} = \binom{N-l+t}{t}$$

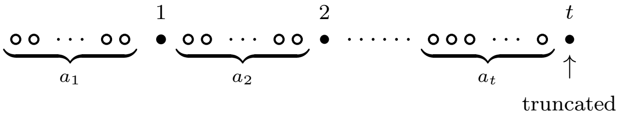
Figure 3.4: Combinatorics of the 0's which separate the error events

Let $C_{N-l,t+1}$ be the number of $t+1$-combination with repetition of the finite set $\{1,\ldots,N-l\}$. We get that

$$\begin{aligned}
R_{w,d}(\psi_N) &= \sum_{t=1}^{N}\sum_{l=1}^{N} C_{N-l,t+1} R_{w,d,t,l}(\psi_N) = \sum_{t=1}^{N}\sum_{l=1}^{N}\binom{N-l+t}{t} R_{w,d,t,l}(\psi_N) \\
&= \sum_{t=1}^{N}\sum_{l=1}^{N}\binom{N-l+t}{t} \sum_{\substack{(w_1,\ldots,w_t):\\ \sum_{i=1}^{t} w_i = w}} \sum_{\substack{(d_1,\ldots,d_t):\\ \sum_{i=1}^{t} d_i = d}} \sum_{\substack{(l_1,\ldots,l_t):\\ \sum_{i=1}^{t} l_i = l}} \left(\prod_{j=1}^{t} E_{w_j,d_j,l_j}\right) \\
&= \sum_{t=1}^{N}\sum_{l=1}^{N} \operatorname{coeff}\left\{\frac{1}{(1-z)^{t+1}}, z^{N-l}\right\} \operatorname{coeff}\left\{[E(x,y,z)]^t, x^w y^d z^l\right\} \\
&= \sum_{t=1}^{N} \operatorname{coeff}\left\{\frac{[E(x,y,z)]^t}{(1-z)^{t+1}}, x^w y^d z^N\right\} \qquad (3.13)
\end{aligned}$$

Through similar arguments, we get that the number of input sequences having input weight w output weight d and containing a truncated error event is given by

$$
\begin{aligned}
&T_{w,d}(\psi_N) = \\
&= \sum_{t=1}^{N}\sum_{l=1}^{N} C_{N-l,t} \sum_{\substack{(w_1,\dots,w_t):\\ \sum_{i=1}^t w_i = w}} \ \sum_{\substack{(d_1,\dots,d_t):\\ \sum_{i=1}^t d_i = d}} \ \sum_{\substack{(l_1,\dots,l_t):\\ \sum_{i=1}^t l_i = l}} \left(\prod_{j=1}^{t-1} E_{w_j,d_j,l_j}\right) \widetilde{E}_{w_t,d_t,l_t} \\
&= \sum_{t=1}^{N}\sum_{l=1}^{N} C_{N-l,t} \sum_{w_t=1}^{N}\sum_{d_t=1}^{N}\sum_{l_t=1}^{N} \widetilde{E}_{w_t,d_t,l_t} \times \qquad (3.14)\\
&\qquad \times \sum_{\substack{(w_1,\dots,w_{t-1}):\\ \sum_{i=1}^t w_i = w-w_t}} \ \sum_{\substack{(d_1,\dots,d_{t-1}):\\ \sum_{i=1}^t d_i = d-d_t}} \ \sum_{\substack{(l_1,\dots,l_{t-1}):\\ \sum_{i=1}^t l_i = l-l_t}} \prod_{j=1}^{t-1} E_{w_j,d_j,l_j} \\
&= \sum_{t=1}^{N}\sum_{l=1}^{N} C_{N-l,t} \sum_{w_t=1}^{N}\sum_{d_t=1}^{N}\sum_{l_t=1}^{N} \mathrm{coeff}\left\{\widetilde{E}(x,y,z), x^{w_t}y^{d_t}z^{l_t}\right\} \times \qquad (3.15)\\
&\qquad \times \mathrm{coeff}\left\{[E(x,y,z)]^{t-1}, x^{w-w_t}y^{d-d_t}z^{l-l_t}\right\} \\
&= \sum_{t=1}^{N}\sum_{l=1}^{N} \binom{N-l+t-1}{t-1} \mathrm{coeff}\left\{\widetilde{E}(x,y,z)\,[E(x,y,z)]^{t-1}, x^w y^d z^l\right\} \\
&= \sum_{t=1}^{N} \mathrm{coeff}\left\{\widetilde{E}(x,y,z)\frac{[E(x,y,z)]^{t-1}}{(1-z)^t}, x^w y^d z^N\right\}. \qquad (3.16)
\end{aligned}
$$



$$
\begin{cases} \sum_{i=1}^t a_i = N-l \\ a_i \ge 0 \end{cases} \Longrightarrow C_{N-l,t+1} = \binom{N-l+t-1}{t-1}
$$

Figure 3.5: Combinatorics of the 0's which separate the error events

The term $C_{N-l,t}$ takes into consideration the combinatorics of the 0's which separate the error events: notice that in this case we have to dispose $N-l$ elements in at most t different blocks, since the last error event is not yet terminated (see Figure 3.5).

The assertion follows by adding expression (3.13) to (3.16). □

3.5.2 Asymptotic growth rate of weight enumerators

Now we discuss how the exponential growth rate of weight enumerators can be derived. Due to better readability, some more technical proofs are postponed in Appendix A.

Lemma 3.1. *For fixed $(u, \delta) \in \mathbb{Q}^2 \cap [0,1]^2$, consider the set*

$$\mathcal{N}_{u,\delta} = \{N \in \mathbb{N} : ukN \in \mathbb{N}, \delta nN \in \mathbb{N} \textit{ and } R_{ukN,\delta nN}(\psi_N) > 0\}. \tag{3.17}$$

Then either this set is empty, or has infinite cardinality. In particular, if $N_0 \in \mathcal{N}_{u,\delta}$ then $jN_0 \in \mathcal{N}_{u,\delta}$ for all $j \in \mathbb{N}$.

Proof. : if $N_0 \in \mathcal{N}_{u,\delta}$, then $jN_0 \in \mathcal{N}_{u,\delta}$ for every positive integer j. To see this fact, observe that if $N_0 \in \mathcal{N}_{u,\delta}$ then there exists an input sequence $\boldsymbol{u}(D) \in \mathbb{Z}_2^k((D))$ such that $\boldsymbol{u}|_{[0,N_0-1]}$ consists exclusively of regular error events, $\mathrm{w_H}(\boldsymbol{u}|_{[0,N_0-1]}) = ukN_0$ and $\mathrm{w_H}\left(\psi_{N_0}(\boldsymbol{u})\right) = \delta nN_0$. By considering the sequence

$$\boldsymbol{w}(D) = \boldsymbol{u}(D) \vee_{N_0} D^{N_0}\boldsymbol{u}(D) \vee_{2N_0} \dots \vee_{(j-1)N_0} D^{(j-1)N_0}\boldsymbol{u}(D),$$

we get $\mathrm{w_H}(\boldsymbol{w}|_{[0,jN_0-1]}) = ukjN_0$ and $\mathrm{w_H}\left(\psi_{jN_0}(\boldsymbol{w})\right) = \delta njN_0$, or equivalently $jN_0 \in \mathcal{N}_{u,\delta}$. □

Proof of Proposition 3.1. We prove the assertion by showing the following steps:

1. $\mathcal{W} \cap \mathbb{Q}^2$ is dense in $\mathcal{W}$;
2. $\mathcal{W} \cap \mathbb{Q}^2$ is convex;
3. $\mathcal{W}$ is closed;
4. $\mathcal{W}$ is convex.

1) The set $\mathcal{W} \cap \mathbb{Q}^2$ is dense in $\mathcal{W}$ by the way it is defined. In fact, for every $\overline{\boldsymbol{\omega}} \in \mathcal{W}$ and open ball

$$\mathcal{B}_1(\overline{\boldsymbol{\omega}}, \varepsilon) = \{\boldsymbol{\omega} : |\omega_1 - \overline{\omega}_1| < \varepsilon_1, |\omega_2 - \overline{\omega}_2| < \varepsilon_2\} \cap \mathcal{W},$$

we have

$$\mathcal{B}_1(\overline{\boldsymbol{\omega}}, \varepsilon) \cap \mathcal{W} \cap \mathbb{Q}^2 \neq \emptyset.$$

To see this fact let $N \in \mathbb{N} \in \mathcal{N}_{\overline{\omega}_1,\overline{\omega}_2}$ defined in (3.17), then from Lemma 3.1 $jN \in \mathcal{N}_{\overline{\omega}_1,\overline{\omega}_2}$.

Notice that all $\boldsymbol{\omega} \in \mathbb{Q}^2$ such that $|\omega_1 - \overline{\omega}_1| < \frac{1}{2j_1kN}$ and $|\omega_2 - \overline{\omega}_2| < \frac{1}{2j_2nN}$ with $j_1 \geq \frac{1}{2\varepsilon_1 kN}$ and $j_2 \geq \frac{1}{2\varepsilon_2 kN}$ are in $\mathcal{B}_1(\overline{\boldsymbol{\omega}}, \varepsilon) \cap \mathcal{W} \cap \mathbb{Q}^2$ since

$$R_{\lfloor\omega_1 kN\rfloor,\lfloor\omega_2 nN\rfloor}(\psi_N) = R_{\lfloor\overline{\omega}_1 kN\rfloor,\lfloor\overline{\omega}_2 nN\rfloor}(\psi_N) > 0.$$

2) Let $(u_1,\delta_1),(u_2,\delta_2) \in \mathcal{W} \cap \mathbb{Q}^2$ and

$$N_1 = \min\{N | N \in \mathcal{N}_{u_1,\delta_1}\} \qquad N_2 = \min\{N | N \in \mathcal{N}_{u_2,\delta_2}\} \qquad N^\star = \operatorname{lcm}(N_1,N_2).$$

From above it follows that $jN^\star \in \mathcal{N}_{u_1,\delta_1} \cap \mathcal{N}_{u_2,\delta_2}$ for all positive integer j and there exist input sequences $\boldsymbol{u}_1,\boldsymbol{u}_2 \in \mathbb{Z}_2^k((D))$ such that

$$\mathrm{w_H}(\boldsymbol{u}_1|_{[0,N_1-1]}) = u_1kN_1 \qquad \mathrm{w_H}\left(\psi_{N_1}(\boldsymbol{u}_1)\right) = \delta_1 nN_1$$

and

$$\mathrm{w_H}(\boldsymbol{u}_2|_{[0,N_2-1]}) = u_2kN_2 \qquad \mathrm{w_H}\left(\psi_{N_2}(\boldsymbol{u}_2)\right) = \delta_2 nN_2.$$

To see that $\mathcal{W}$ is convex, it is sufficient to prove that

$$(\vartheta u_1 + (1-\vartheta)u_2, \vartheta\delta_1 + (1-\vartheta)\delta_2) \in \mathcal{W} \qquad \forall \vartheta \in [0,1] \cap \mathbb{Q}.$$

Consider j_1, j_2 such that $j_1N_1 = j_2N_2 = N^\star$ and the following input sequences

$$\begin{aligned}\boldsymbol{w}_1(D) &= \boldsymbol{u}_1(D) \vee_{N_1} D^{N_1}\boldsymbol{u}_1(D) \vee_{2N_1} \dots \vee_{(j_1-1)N_1} D^{(j_1-1)N_1}\boldsymbol{u}(D),\\ \boldsymbol{w}_2(D) &= \boldsymbol{u}_2(D) \vee_{N_2} D^{N_2}\boldsymbol{u}_2(D) \vee_{2N_2} \dots \vee_{(j_2-1)N_2} D^{(j_2-1)N_2}\boldsymbol{u}(D).\end{aligned}$$

Let q be an integer such that $q\vartheta \in \mathbb{N}$ then the sequence

$$\boldsymbol{v} = \boldsymbol{w}_1 \vee_{N^\star} \dots \vee_{(q\vartheta-1)N^\star} D^{(q\vartheta-1)N^\star}\boldsymbol{w}_1 \vee_{q\vartheta N^\star} D^{q\vartheta N^\star}\boldsymbol{w}_2 \vee_{(q\vartheta+1)N^\star} \dots \vee_{qN^\star-1} D^{qN^\star-1}\boldsymbol{w}_2$$

has the following properties

$$\mathrm{w_H}(\boldsymbol{v}|_{[0,qN^\star-1]}) = (\vartheta u_1 + (1-\vartheta)u_2)qkN^\star \qquad \mathrm{w_H}\left(\psi_{qN^\star}(\boldsymbol{v})\right) = (\vartheta\delta_1 + (1-\vartheta)\delta_2)qnN^\star.$$

We conclude $qN^\star \in \mathcal{N}_{\vartheta u_1+(1-\vartheta)u_2, \vartheta\delta_1+(1-\vartheta)\delta_2}$ and $\vartheta(u_1,\delta_1) + (1-\vartheta)(u_2,\delta_2) \in \mathcal{W}$.

3) We now show that the region $\mathcal{W}$ is also closed.

From equation (3.13) $(u,\delta) \in \mathcal{W}$ if and only if there exist $(\alpha,\beta) \in (0,1)^2$ such that the following problem is feasible

$$\begin{aligned} &\sum_{i,j,l} \lambda_{i,j,l} = 1, && \sum_i i\lambda_{i,j,l} = \frac{uk}{\alpha},\\ &\sum_j j\lambda_{i,j,l} = \frac{\delta n}{\alpha}, && \sum_k l\lambda_{i,j,l} = \frac{\beta}{\alpha}. \end{aligned} \tag{3.18}$$

Notice that $\lambda_{i,j,l}$ represents the limit fraction of error events in a linear fashion with input weight i, output weight j and length l. Equivalently, $(u,\delta) \in \mathcal{W}$ if and only if there exist $\alpha,\beta \in [0,1]$ for which the following decision problem is feasible:

$$\boldsymbol{\Phi\lambda} = \left(1, \frac{uk}{\alpha}, \frac{\delta n}{\alpha}, \frac{\beta}{\alpha}\right)^T \qquad \boldsymbol{\lambda} \succeq \boldsymbol{0}, \tag{3.19}$$

where the region of u and δ for which (3.18) is feasible is closed. To see this fact, consider the dual problem of 3.19.

$$\boldsymbol{\Phi}^T\boldsymbol{\zeta} \preceq \mathbf{0} \qquad \left(1, \frac{uk}{\alpha}, \frac{\delta n}{\alpha}, \frac{\beta}{\alpha}\right)\boldsymbol{\zeta} > 0 \tag{3.20}$$

By Farka's lemma [72], (3.19) and (3.20) are strong alternatives, which means that exactly one of them holds (i.e. either 3.19 or 3.20 is feasible but not both). On the other hand, the region of (u, δ) for which (3.20) is feasible is clearly an open set (notice that $\boldsymbol{\Phi}$ is independent on α, β, u, δ), so that the region for which (3.18) is feasible is closed.

4) Let $\boldsymbol{\omega}^1, \boldsymbol{\omega}^2 \in \mathcal{W}$ and $\lambda \in [0, 1]$. Since $\mathcal{W} \cap \mathbb{Q}$ is dense in $\mathcal{W}$ (see point 1)) and $\mathbb{Q} \cap [0, 1]$ in $[0, 1]$, there exist sequences $\lambda_m \in \mathbb{Q}, \boldsymbol{\omega}^1_m, \boldsymbol{\omega}^2_m \in \mathcal{W} \cap \mathbb{Q}$ such that $\lambda_m \to \lambda$, $\boldsymbol{\omega}^1_m \to \boldsymbol{\omega}^1$ and $\boldsymbol{\omega}^2_m \to \boldsymbol{\omega}^2$. As $\mathcal{W} \cap \mathbb{Q}$ is convex, then $\lambda_m\boldsymbol{\omega}^1_m + (1 - \lambda_m)\boldsymbol{\omega}^2_m \in \mathbb{Q} \cap \mathcal{W}$ and

$$\lambda_m\boldsymbol{\omega}^1_m + (1 - \lambda_m)\boldsymbol{\omega}^2_m \overset{m\to\infty}{\longrightarrow} \lambda\boldsymbol{\omega}^1 + (1 - \lambda)\boldsymbol{\omega}^2 \in \mathcal{W}$$

follows from the fact that $\mathcal{W}$ is closed and $\mathcal{W}$ is clearly convex. □

Now to get a closed form expression for the asymptotic spectral function $G(u, \delta)$ we use the multidimensional saddle point method for large powers. Before illustrating this method, we fix some notation and definitions.

Given a function $F(\boldsymbol{x})$ of class C^2 of η variables $\boldsymbol{x} = (x_1, \dots, x_\eta)$ define the following operators:

$$\Delta_i[F](\boldsymbol{x}) := x_i\frac{\partial \ln F}{\partial x_i} = \frac{x_i}{F}\frac{\partial F}{\partial x_i} \qquad \forall i \in \{1, \dots \eta\} \tag{3.21}$$

$$\Gamma_{i,j}[F](\boldsymbol{x}) := x_j\frac{\partial\left(\Delta_i[F](\boldsymbol{x})\right)}{\partial x_j} \qquad \forall i, j \in \{1, \dots \eta\}. \tag{3.22}$$

Theorem 3.4. *[Multidimensional saddle point method for large powers] Let $S(\boldsymbol{x})$ and $F(\boldsymbol{x})$ power series of the type*

$$S(\boldsymbol{x}) = \sum_{\boldsymbol{l}\in\mathbb{N}_0^\eta} S_{\boldsymbol{l}}\boldsymbol{x}^{\boldsymbol{l}} = \sum_{\boldsymbol{l}\in\mathscr{S}} S_{\boldsymbol{l}}\boldsymbol{x}^{\boldsymbol{l}}$$

$$F(\boldsymbol{x}) = \sum_{\boldsymbol{k}\in\mathbb{N}_0^\eta} F_{\boldsymbol{k}}\boldsymbol{x}^{\boldsymbol{k}} = \sum_{\boldsymbol{k}\in\mathscr{F}} F_{\boldsymbol{k}}\boldsymbol{x}^{\boldsymbol{k}}$$

where $\boldsymbol{x} = (x_1, \dots, x_\eta)$, $\boldsymbol{x}^{\boldsymbol{k}} = \prod_{i=1}^{\eta} x_i^{k_i}$, and

$$\mathscr{F} := \{\boldsymbol{k} \in \mathbb{N}_0^\eta \mid F_{\boldsymbol{k}} > 0\} \qquad \mathscr{S} := \{\boldsymbol{l} \in \mathbb{N}_0^\eta \mid S_{\boldsymbol{l}} > 0\}\ .$$

Suppose F has the following properties:

(P1) $F_{\boldsymbol{k}} \in \mathbb{N}_0$ *for every* $\boldsymbol{k}$*,* $F_{\boldsymbol{0}} > 0$ *and* $|\mathscr{F}| \geq 2$.

(P2) There exists $C \in \mathbb{R}^+$ *and* $s \in \mathbb{N}$ *such that* $F_{\boldsymbol{k}} \leq C|\boldsymbol{k}|^s$ *for every* $\boldsymbol{k}$.

(P3) There exists a finite subset $\mathscr{F}_0 \subseteq \mathscr{F}$ *and* $\boldsymbol{k}^1, \dots \boldsymbol{k}^l \in \mathbb{N}_0^\eta$ *such that:*

(P3a) $\mathscr{F} \subseteq \{\boldsymbol{k}^0 + \sum_{i=1}^l t_i \boldsymbol{k}^i \mid \boldsymbol{k}^0 \in \mathscr{F}_0,\ t_i \in \mathbb{N}\}$.

(P3b) There exist $\widetilde{\boldsymbol{k}}_i \in \mathscr{F}$ *for* $i = 1, \dots, l$ *such that* $\widetilde{\boldsymbol{k}}_i + t\boldsymbol{k}_i \in \mathscr{F}$ *for every* $t \in \mathbb{N}_0$.

(P4) $\mathscr{F}$ *generates* $\mathbb{Z}^\nu$ *as an Abelian group.*

Assume S *satisfies the following conditions:*

(P5) $S_{\boldsymbol{l}} \in \mathbb{N}_0$ *for every* $\boldsymbol{l}$*,* $S_{\boldsymbol{0}} > 0$ *and* $|\mathscr{S}| \geq 2$.

(P6) There exists a finite subset $\mathscr{S}_0 \subseteq \mathscr{S}$ *such that:*

(P6a) $\mathscr{S} \subseteq \{\boldsymbol{l}^0 + \sum_{i=1}^l t_i \boldsymbol{k}^i \mid \boldsymbol{l}^0 \in \mathscr{S}_0,\ t_i \in \mathbb{N}\}$.

(P6b) There exist $\widetilde{\boldsymbol{l}}_i \in \mathscr{S}$ *for* $i = 1, \dots, l$ *such that* $\widetilde{\boldsymbol{l}}_i + t\boldsymbol{k}_i \in \mathscr{S}$ *for every* $t \in \mathbb{N}_0$.

Consider α_n *and* $\boldsymbol{\omega}_n$ *such that there exist* α *and* $\boldsymbol{\omega} \in \overset{\circ}{\mathrm{co}}(\mathscr{F})$ *with* $|\alpha_n - \alpha| = O(n^{-1})$ *and* $||\boldsymbol{\omega}_n - \boldsymbol{\omega}|| = O\left(n^{-1}\right)$ *when* $n \to \infty$*. Let*

$$\mathscr{N} = \{n \in \mathbb{N} | \boldsymbol{\omega}_n \alpha_n n \in \mathbb{N}^\eta, \alpha_n n \in \mathbb{N}\}.$$

Then we have for $n \to \infty$ *such that* $n \in \mathscr{N}$

$$\mathrm{coeff}\{S(\boldsymbol{x})[F(\boldsymbol{x})]^{\alpha_n n}, \boldsymbol{x}^{\boldsymbol{\omega}_n \alpha_n n}\} = \frac{S(\boldsymbol{x}_{\boldsymbol{\omega}})}{\sqrt{(2\pi\alpha_n n)^\nu |\boldsymbol{\Gamma}(\boldsymbol{x}_{\boldsymbol{\omega}})|}} \frac{[F(\boldsymbol{x}_{\boldsymbol{\omega}})]^{\alpha_n n}}{\boldsymbol{x}_{\boldsymbol{\omega}}^{\boldsymbol{\omega}_n \alpha_n n}} \left(1 + O\left(n^{-1/10}\right)\right) \tag{3.23}$$

and

$$\lim_{n \in \mathscr{N}} \frac{1}{n} \ln\left(\mathrm{coeff}\{S(\boldsymbol{x})[F(\boldsymbol{x})]^{\alpha_n n}, \boldsymbol{x}^{\boldsymbol{\omega}_n \alpha_n n}\}\right) = \alpha \ln F(\boldsymbol{x}_{\boldsymbol{\omega}}) - \alpha\ \boldsymbol{\omega} \cdot \ln \boldsymbol{x}_{\boldsymbol{\omega}} \tag{3.24}$$

where $\boldsymbol{x}_{\boldsymbol{\omega}} \in (\mathbb{R}^+)^\eta$ *is the unique solution to* $\boldsymbol{\Delta}(\boldsymbol{x}) = \boldsymbol{\omega}$*. Moreover, the convergence in* (3.24) *is uniform in* α *and* $\boldsymbol{\omega}$*.*

Theorem 3.4, whose proof is rather technical and therefore deferred to Appendix A, may be thought of as a generalization of [52, Thm. 2] and [21, Lemma D.14]. There, only the case when the generating function is a power of a multivariate polynomial with non-negative coefficients was considered. Theorem 3.4 covers a more general class of generating functions, which includes the case treated in [52, Thm. 2]. Moreover, our modification allows to estimate the order of magnitude of a (convergent) sequence of coefficients in large powers of multivariate functions and unveils the fundamental role played by ν.

Lemma 3.2. *Let $F(x,y,z)$ as defined in (3.4). Then (P1)-(P3) hold true. The power series $\widetilde{E}(x,y,z)$ in (3.3) and $(1-z)^{-1}$ satisfy properties (P5)-(P6).*

Proof. The condition $F_{\mathbf{0}} > 0$ is obtained by taking common factors out. Properties (P1)-(P2) can be verified trivially and we only prove condition (P3).

Let $G = (\mathcal{V}, \mathcal{E})$ be the directed graph associated to the trellis of the convolutional encoder, where $\mathcal{V} = \{v_1, v_2, \dots v_\mu\}$ is a finite set of vertices representing states of the convolutional encoder and $\mathcal{E} \subseteq \mathcal{V} \times \mathcal{V}$ with $(v_i, v_j) \in \mathcal{E}$ if there is one step transition from state v_i to state v_j. Suppose now that a label is assigned to every edge in the graph. If $e = (v_i, v_j) \in \mathcal{E}$, a label is assigned to the edge $f(e) = \boldsymbol{x}^{\boldsymbol{k}} = x_1^{k_1} x_2^{k_2} x_3^{k_3}$ where k_1 is the weight of input sequence that takes the machine from state v_i to state v_j, k_2 is the corresponding output weight and k_3 is the length of the input sequence. A path in such a graph is a sequence of edges of the form $p = (v_0, v_1), (v_1, v_2), \dots, (v_{n-1}, v_n)$. Such a path is said to be a path of length n and it is usually represented by the string $(v_0, v_1, \dots v_n)$. Let us define the label of a path the product of the labels of the component edges $f(p) = \prod_{e \in p} f(e) = \prod_{e \in p} \boldsymbol{x}^{\boldsymbol{k}_e} = \boldsymbol{x}^{\sum_{e \in p} \boldsymbol{k}_e}$. We denote with $\boldsymbol{k}_p = \sum_{e \in p} \boldsymbol{k}_e$.

With this formalism the generating function $F(\boldsymbol{x})$ is the sum of the labels of all paths starting and ending in the zero state. A cycle $c \in \mathscr{C}_{v|v_1,\dots,v_n}$ is a sequence starting and ending in v with transitions in $\mathcal{V} \setminus \{v, v_1, ..., v_n\}$. Let $\mathscr{C}_{\min}$ be the set of all minimal cycles, namely all cycles starting and ending in a generic vertex v and taking distinct values in between. Since the encoder has a fixed memory, then $|\mathscr{C}_{\min}|$ is finite. Given a path p we denote with $\mathscr{C}^p_{v|v_1,\dots,v_n}$ (and $\mathscr{C}^p_{\min}$) the set of all sequences in $\mathscr{C}_{v|v_1,\dots,v_n}$ (and $\mathscr{C}^s_{\min}$) included in p.

The following lemma states that every multi-index $\boldsymbol{k} \in \mathscr{F} \neq \{\boldsymbol{k} | F_{\boldsymbol{k}} > 0\}$ can be written in terms of minimal cycles.

Let $\boldsymbol{k} \in \mathscr{F}$. Then there exists a sequence $s = (0, v_1, ..., v_n, 0)$ such that $f(s) = \boldsymbol{x}^{\boldsymbol{k}}$. If v_i are all distinct then $s \in \mathscr{C}_{\min}$, $\boldsymbol{k} = \boldsymbol{k}_s$ and the assertion is verified. Otherwise $f(s) = \prod_{c_0 \in \mathscr{C}^s_0} f(c_0)$.

$$f(s) = \prod_{c_0 \in \mathscr{C}^s_0} \prod_{v \in c_0} \prod_{c_1 \in \mathscr{C}^s_{v|0}} f(c_1)$$

If $\mathscr{C}^s_{v|0} = \mathscr{C}_{\min}$ for all v we conclude the thesis. If this is not the case, proceed as before:

$$f(s) = \prod_{c_0 \in \mathscr{C}^s_0} \prod_{v \in c_0} \prod_{c_1 \in \mathscr{C}^s_{v|0} \cap \mathscr{C}^s_{\min}} f(c_1) \prod_{c_1' \in \mathscr{C}^s_{v|0} \setminus \mathscr{C}^s_{\min}} f(c_1')$$

The process halts after at most $|\mathcal{V}| = \mu$ number of steps and we get

$$f(s) = \prod_{c_0 \in \mathscr{C}^s_0} \prod_{v_1 \in c_0} \prod_{c_1 \in \mathscr{C}_{v_1|0} \cap \mathscr{C}_{\min}} f(c_1) \dots \prod_{v_\mu \in c_{\mu-1}} \prod_{c_\mu \in \mathscr{C}_{v_\mu | v_{\mu-1},\dots,v_1,0} \cap \mathscr{C}_{\min}} f(c_\mu).$$

Notice that s is finally decomposed exlusively in terms of minimal cycles. Define t_c be the number of times the cycle appears in the sequence s and we conclude

$$f(s) = \prod_{c \in \mathscr{C}_{\min}} f(c)^{t_c} = \boldsymbol{x}^{\sum_c t_c \boldsymbol{k}_c}.$$

Similar arguments are used to prove conditions (P5)-(P6) for $\widetilde{E}(x, y, z)$. Finally (P5)-(P6) are trivially verified for $(1-z)^{-1}$. □

Proof of Theorem 3.2. If $(u, \delta) \notin \mathcal{W}$ then we have trivially that

$$R_{\lfloor ukN \rfloor, \lfloor \delta nN \rfloor}(\psi_N) = 0 \quad \forall N \in \mathbb{N},$$

and functions G_N are not defined in those points, and we set conventionally $G_N(u, \delta) = -\infty$ $\forall N \in \mathbb{N}$.

From Theorem 3.1 (see expressions (3.4), (3.5), and (3.6)) we have

$$\begin{aligned} G_N(u,\delta) &\geq \frac{1}{nN} \ln \operatorname{coeff}\left\{L(x,y,z)F(x,y,z)^{\lfloor \alpha N \rfloor}, x^{\lfloor ukN \rfloor} y^{\lfloor \delta nN \rfloor} z^N\right\} \quad \forall \alpha \in [0,1] \\ &= \frac{1}{nN} \ln \operatorname{coeff}\left\{\frac{1}{1-z} F(x,y,z)^{\lfloor \alpha N \rfloor}, x^{\lfloor ukN \rfloor} y^{\lfloor \delta nN \rfloor} z^N\right\} + \\ &+ \frac{1}{nN} \ln \operatorname{coeff}\left\{\frac{\widetilde{E}(x,y,z)}{1-z} F(x,y,z)^{\lfloor \alpha N \rfloor - 1}, x^{\lfloor ukN \rfloor} y^{\lfloor \delta nN \rfloor} z^N\right\} \quad \forall \alpha \in [0,1] \end{aligned}$$

Define now

$$\boldsymbol{\omega}_N = \left(\frac{\lfloor ukN \rfloor}{\lfloor \alpha N \rfloor}, \frac{\lfloor \delta nN \rfloor}{\lfloor \alpha N \rfloor}, \frac{N}{\lfloor \alpha N \rfloor}\right) \qquad \boldsymbol{\omega} = \left(\frac{uk}{\alpha}, \frac{\delta n}{\alpha}, \frac{1}{\alpha}\right)$$

and $\alpha_N = \frac{\lfloor \alpha N \rfloor}{N}$. Notice that $||\boldsymbol{\omega} - \boldsymbol{\omega}_N|| = O\left(N^{-1}\right)$ and $|\alpha_N - \alpha| = O(N^{-1})$. Since $(u, \delta) \in \mathcal{W}$, $\boldsymbol{\omega} \in \overset{\circ}{\operatorname{co}}(\mathscr{F})$ and from Lemma 3.2 the hypotheses of Theorem 3.4 are satisfied.

Using Theorem 3.4, we can estimate the function G as follows

$$\lim_{N \to \infty} G_N(u,\delta) \geq \frac{1}{n} \left\{\alpha \ln F(x_\alpha, y_\alpha, z_\alpha) - uk \ln x_\alpha - \delta n \ln y_\alpha - \ln z_\alpha\right\} \quad \forall \alpha \in [0,1]$$

$$\lim_{N \to \infty} G_N(u,\delta) \geq \frac{1}{n} \max_{\alpha \in [0,1]} \left\{\alpha \ln F(x_\alpha, y_\alpha, z_\alpha) - uk \ln x_\alpha - \delta n \ln y_\alpha - \ln z_\alpha\right\}$$

with $(x_\alpha, y_\alpha, z_\alpha)$ solution of system $\boldsymbol{\Delta}[F](x, y, z) = (uk/\alpha, \delta n/\alpha, 1/\alpha)$, which is equivalent to system (3.10).

On the other hand, from Theorem 3.1 (see expression (3.6)) we have $\forall (x,y,z) \in (\mathbb{R}^+)^3$

$$\begin{aligned}
G_N(u,\delta) \leq{}& \frac{\ln N}{nN} + \max_\alpha \frac{1}{nN} \ln \operatorname{coeff}\left\{L(x,y,z)F(x,y,z)^{\lfloor \alpha N \rfloor}, x^{\lfloor ukN \rfloor} y^{\lfloor \delta n N \rfloor} z^N\right\} \\
\leq{}& \frac{\ln N}{nN} + \max_\alpha \left\{ \frac{1}{nN} \ln \operatorname{coeff}\left\{L(x,y,z)F(x,y,z)^{\lfloor \alpha N \rfloor}, x^{\lfloor ukN \rfloor} y^{\lfloor \delta n N \rfloor} z^N\right\} + \right. \\
& - \frac{1}{n}\left[\alpha \ln F(x_\alpha, y_\alpha, z_\alpha) - uk \ln x_\alpha - \delta n \ln y_\alpha - \ln z_\alpha\right] + \\
& \left. + \frac{1}{n}\left[\alpha \ln F(x_\alpha, y_\alpha, z_\alpha) - uk \ln x_\alpha - \delta n \ln y_\alpha - \ln z_\alpha\right] \right\} \\
\leq{}& \frac{\ln N}{nN} + \max_\alpha \left\{ \frac{1}{nN} \ln \operatorname{coeff}\left\{L(x,y,z)F(x,y,z)^{\lfloor \alpha N \rfloor}, x^{\lfloor ukN \rfloor} y^{\lfloor \delta n N \rfloor} z^N\right\} + \right. \\
& \left. - \frac{1}{n}\left[\alpha \ln F(x_\alpha, y_\alpha, z_\alpha) - uk \ln x_\alpha - \delta n \ln y_\alpha - \ln z_\alpha\right] \right\} + \\
& + \frac{1}{n} \max_\alpha \left[\alpha \ln F(x_\alpha, y_\alpha, z_\alpha) - uk \ln x_\alpha - \delta n \ln y_\alpha - \ln z_\alpha\right].
\end{aligned}$$

where the last step follows from Theorem 3.4.

We conclude that

$$\lim_{N\to\infty} G_N(u,\delta) \leq \frac{1}{n} \max_\alpha \left[\alpha \ln F(x_\alpha, y_\alpha, z_\alpha) - uk \ln x_\alpha - \delta n \ln y_\alpha - \ln z_\alpha\right].$$

The assertion is then obtained by observing that

$$(x_\alpha, y_\alpha, z_\alpha) = \operatorname*{argmin}_{x,y,z} \left\{\alpha \ln F(x,y,z) - uk \ln x - \delta n \ln y - \ln z\right\}$$

(see proof of Lemma A.2). □

Proof of Corollary 3.1. The continuity of function $G(u,\delta)$ in $(u,\delta) \in \mathcal{W}$ follows immediately from the expression in (3.8).

We now prove that the function G is also concave in its domain. Notice that the function

$$f(u,\delta,\alpha) = \min_{x,y,z} \left\{\alpha \ln F(x,y,z) - uk \ln x - \delta n \ln y - \ln z\right\}$$

is concave in $(u,\delta,\alpha) \in \mathcal{W} \times [0,1]$ as pointwise minimum over an infinite set of concave functions:

$$\begin{aligned}
&\theta f(u_1,\delta_1,\alpha_1) + (1-\theta) f(u_2,\delta_2,\alpha_2) = \\
&\quad = \min_{x,y,z} \left[\theta\alpha_1 \ln F(x,y,z) - \theta u_1 k \ln x - \theta\delta_1 n \ln y - \theta \ln z\right] + \\
&\quad + \min_{x,y,z} \left[(1-\theta)\alpha_2 \ln F(x,y,z) - (1-\theta)u_2 k \ln x - (1-\theta)\delta_2 n \ln y - (1-\theta) \ln z\right] \\
&\quad \leq \min_{x,y,z} \left[(\theta\alpha_2 + (1-\theta)\alpha_2) \ln F(x,y,z) - (\theta u_1 + (1-\theta)u_2) k \ln x + \right. \\
&\quad \left. -(\theta\delta_2 + (1-\theta)\delta_2) n \ln y - \ln z\right] \\
&\quad = f(\theta u_1 + (1-\theta)u_2, \theta\delta_1 + (1-\theta)\delta_2, \theta\alpha_1 + (1-\theta)\alpha_2).
\end{aligned}$$

Let $\alpha_i = \operatorname*{argmax}_{\alpha} f(u_i, \delta_i, \alpha)$ then

$$\begin{aligned}
\theta G(u_1, \delta_1) &+ (1-\theta) G(u_2, \delta_2) \\
&= \theta \max_{\alpha} f(u_1, \delta_1, \alpha) + (1-\theta) \max_{\alpha} f(u_2, \delta_2, \alpha) \\
&= \theta f(u_1, \delta_1, \alpha_1) + (1-\theta) f(u_2, \delta_2, \alpha_2) \\
&\leq f(\theta u_1 + (1-\theta) u_2, \theta\delta_1 + (1-\theta)\delta_2, \theta\alpha_1 + (1-\theta)\alpha_2) \\
&\leq \max_{\alpha} f(\theta u_1 + (1-\theta) u_2, \theta\delta_1 + (1-\theta)\delta_2, \alpha) \\
&= G(\theta u_1 + (1-\theta) u_2, \theta\delta_1 + (1-\theta)\delta_2).
\end{aligned}$$

We conclude that $G(u, \delta)$ is concave in $(u, \delta) \in \mathcal{W}$. □

3.5.3 Finite length approximation of weight distribution

The basic technique in the following proof is a direct application of Theorem 3.4 for multivariate generating functions.

Proof of Theroem 3.3. From Theorem 3.4 we know that for $w = \lfloor ukN \rfloor$, $d = \lfloor \delta n N \rfloor$ and $N \to \infty$

$$\begin{aligned}
A_{w,d}^{\alpha N}(\psi_N) &:= \operatorname{coeff}\left\{L(x,y,z)F(x,y,z)^{\alpha N}, x^w y^d z^N\right\} \\
&\sim \frac{L(x_\alpha, y_\alpha, z_\alpha)}{\sqrt{(2\pi\alpha N)^\nu |\mathbf{\Gamma}_\alpha|}} \frac{[F(x_\alpha, y_\alpha, z_\alpha)]^{\alpha N}}{x_\alpha^w y_\alpha^d z_\alpha^N} \qquad (3.25)
\end{aligned}$$

where $(x_\alpha, y_\alpha, z_\alpha)$ is the solution of system

$$\begin{cases}
\frac{x}{F(x,y,z)} \frac{\partial F(x,y,z)}{\partial x} = \frac{uk}{\alpha} \\
\frac{y}{F(x,y,z)} \frac{\partial F(x,y,z)}{\partial y} = \frac{\delta n}{\alpha} \\
\frac{z}{F(x,y,z)} \frac{\partial F(x,y,z)}{\partial z} = \frac{1}{\alpha}
\end{cases}$$

Assume that $A_{w,d}^{\alpha N}(\psi_N)$ attains its maximum in α_N then

$$\begin{aligned}
A_{w,d}(\psi_N) = A_{w,d}^{\alpha_N N}(\psi_N) \int_0^1 \frac{A_{w,d}^{\alpha N}(\psi_N)}{A_{w,d}^{\alpha_N N}(\psi_N)} \mathrm{d}\alpha \\
= A_{w,d}^{\alpha_N N}(\psi_N) \int_0^1 \frac{\frac{L(x_\alpha, y_\alpha, z_\alpha)}{\sqrt{(2\pi\alpha N)^\nu |\mathbf{\Gamma}_\alpha|}} \frac{[F(x_\alpha, y_\alpha, z_\alpha)]^{\alpha N}}{x_\alpha^w y_\alpha^d z_\alpha^N}}{\frac{L(x_{\alpha_N}, y_{\alpha_N}, z_{\alpha_N})}{\sqrt{(2\pi\alpha_N N)^\nu |\mathbf{\Gamma}_{\alpha_N}|}} \frac{[F(x_{\alpha_N N}, y_{\alpha_N}, z_{\alpha_N N})]^{\alpha_N}}{x_{\alpha_N}^w y_{\alpha_N}^d z_{\alpha_N}^N}} (1 + o(1)) \mathrm{d}\alpha
\end{aligned}$$

Taking the Taylor expansion of function

$$K_N(\alpha) = -\frac{1}{2} \ln\left((2\pi\alpha N)^\nu |\Gamma_\alpha|\right) + \ln L(x_\alpha, y_\alpha, z_\alpha) + \alpha N \ln F(x_\alpha, y_\alpha, z_\alpha) - w \ln x_\alpha - d \ln y_\alpha - \ln z_\alpha$$

at $\alpha = \alpha_N$ we have

$$A_{w,d}(\psi_N) = A_{w,d}^{\alpha_N N}(\psi_N) \int_0^1 \mathrm{e}^{K_N'(\alpha_N)(\alpha - \alpha_N) + \frac{1}{2} K_N''(\overline{\alpha})(\alpha - \alpha_N)^2} (1 + o(1)) \mathrm{d}\alpha$$

According to the assumption that $A_{w,d}^{\alpha N}(\psi_N)$ takes its maximum value at $\alpha = \alpha_N$, we know that $K'_N(\alpha_N) = 0$ and

$$A_{w,d}(\psi_N) = A_{w,d}^{\alpha_N N}(\psi_N) \int_{-\infty}^{\infty} \mathrm{e}^{-\frac{x^2}{2\sigma^2}}(1 + o(1))\mathrm{d}x$$

where $\frac{1}{\sigma^2} = -\frac{K''_N(\alpha^\star)}{N^2}$. Since $|\alpha_N - \alpha^\star| = O(1/N)$ we have

$$\begin{aligned} A_{w,d}(\psi_N) &= A_{w,d}^{\lfloor \alpha_N N \rfloor}(\psi_N)\sqrt{2\pi\sigma^2}(1 + o(1)) \\ &\sim \frac{\sqrt{2\pi\sigma^2}L(x_{\alpha^\star}, y_{\alpha^\star}, z_{\alpha^\star})}{\sqrt{(2\pi\lfloor \alpha^\star N \rfloor)^\nu |\mathbf{\Gamma}_{\alpha^\star}|}} \frac{[F(x_{\alpha^\star}, y_{\alpha^\star}, z_{\alpha^\star})]^{\alpha^\star N}}{x_{\alpha^\star}^w y_{\alpha^\star}^d z_{\alpha^\star}^N}(1 + o(1)). \end{aligned}$$

□

3.6 Concluding remarks

In this chapter we have analyzed the weight distribution of truncated convolutional encoders. In particular, we have derived exact formulæ of weight enumerators in terms of generating functions of regular and truncated error events. We have shown how asymptotic estimates of powers of multivariate functions with nonnegative coefficients can be used in the analysis of the growth rate of weight distribution as a function of truncation length. We have investigated the connection of our estimates with a method previously introduced by Sason et al. Our estimates are useful for deriving results regarding ML properties (see [19]) and minimum distance properties of concatenated coding schemes.

We believe that our techniques could be also used to analyze the weight spectrum of turbo-stopping-sets, a measure of the performance of a binary turbo decoder on the BEC introduced for turbo-like codes in [73].

Multiple serial turbo-coding ensemble 4

Brief—In this chapter, the ensembles of multiple-serial turbo codes, obtained by coupling an outer code with a cascade of m rate-1 recursive convolutional encoders through uniform random interleavers, are studied. The parameters that make the ensemble asymptotically good are identified. In particular, it is proved that the average spectral functions of these code ensembles are equal to 0 below a positive threshold distance δ_m. Moreover, if $m = 2$ and the free distance of the outer encoder $d_f \geq 3$, or if $m \geq 3$ and $d_f \geq 2$, then the minimum distance scales linearly in the code length with high probability and δ_m provides a lower bound on the growth rate coefficient.
Finally, under a weak algebraic condition on the outer encoder, it is proved that the sequence of average spectral functions converge uniformly, when $m \to \infty$, to a limit function which is equal to the maximum between 0 and the asymptotic spectra of the classical linear random ensemble. Consequently the sequence δ_m converges to the Gilbert–Varshamov (GV) distance. Combining these results it is possible to conclude that the normalized minimum distances of these concatenated coding schemes converge to the GV-distance when m goes to infinity.

4.1 Introduction and outline of the chapter

In this chapter we study in detail average spectra and minimum distances of multiple-serial turbo coding ensembles, which are obtained by interconnecting an outer code with m rate-1 recursive convolutional encoders through uniform random permutations.

As a first result, we find exact expressions in terms of constituent encoders and we prove that the asymptotic spectra can be obtained through a dynamical system (dependent on the inner encoder) with initial condition equal to the asymptotic spectra of the outer encoder. This iterative formula coincides with those obtained in [46,49,57]. However, its theoretical justification requires MSP-techniques for weight enumerators of constituent encoders, developed in the previous chapter. Inspired both by the the tail estimations of [36] and by the bounding approach used in [46], it is proved that if $m \geq 2$ the average spectral functions of these code ensembles are equal to 0 below a strictly positive threshold distance δ_m (see Theorem 4.5).

Coupling this study with an ad hoc analysis for the low-weight average weight enumerators inspired by the the tail estimations of [36], we finally propose upper bounds to the repartition function of the minimum distance. The key ingredient in order to prove the achievement of the distance thresholds δ_m is MSP-approximation of weight enumerators of constituent encoders, derived in Theorem 3.2. This allows us to show that if $m = 2$ and the free distance of the outer encoder $d_f \geq 3$, or if $m \geq 3$ and $d_f \geq 2$, minimum distance scales linearly in the truncation lengths with high probability (see Theorem 4.6): in the coding terminology this means that such codes are asymptotically good with probability close to 1. More precisely, we obtain with high probability lower bounds on the asymptotic normalized minimum distance of the serial ensembles. Proving the tightness of these bounds would require second-moment estimations for the enumerating functions, and is a problem left for future research. However, numerical results and concentration results available in the literature for the distance-spectra of regular ensembles of binary LDPC codes (see [42,43]) make us optimistic about the tightness of our bounds for multiple concatenated codes as well. Moreover, numerical results suggest that minimum distance is strictly monotonic increasing in the number of inner encoders. The theoretical proof is given just in the case of Repeat multiple-accumulate codes (RA^m, see Section 4.8).

Finally, under a weak algebraic condition on the outer encoder, it is proved that average spectra are equicontinuous (equi-Lipshitz in the case of RA^m) and converge uniformly when $m \to \infty$ to a limit function which is equal to the maximum between 0 and the asymptotic spectra of the classical linear random ensemble (see Theorem 4.7). Consequently the sequence δ_m converges to the Gilbert–Varshamov (GV) distance. Combining these results it is possible to conclude that the normalized minimum distances of these concatenated coding schemes converge to the GV-distance when m goes to infinity in probability. These results passes through the use of new mathematical tools which do not show up in the Markov chain based analysis of average weight enumerators proposed in [44]. In particular we need results coming from non smooth analysis and fixed points study of non-linear dynamical systems.

The remainder of this chapter is organized as follows. Section 4.2 is devoted to the description of multiple serial concatenation of rate-1 codes and its weight structure; then the family of repeat multiple-accumulate codes is introduced as example. In Section 4.3 we review main results known in literature. The stress is given to results collected in [44] and we show how to connect them within our analysis. Section 4.4 presents, in a formal way, all the original contributions presented in this chapter together with some numerical results. Sections 4.5, 4.6, and 4.7 are technical sections whose results are proved in details. Finally, Section 4.8, containing some stronger results in the case of repeat multiple accumulate codes, completes the chapter.

Preliminary versions of this work have been presented at the ITA-2008 workshop [54], at the ISTC-2010 [61]. The study of RA^m ensemble has been published in [55].

4.2 Problem setting

4.2.1 Ensemble description

In this section, we consider a general class of concatenated coding systems of the type depicted in Fig. 4.1.

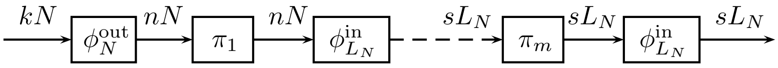


Figure 4.1: Coding scheme: Multiple serial concatenated codes.

Fixed the convolutional encoders $\phi^{\text{out}} \in \mathbb{Z}_2^{k\times n}(D)$ and $\phi^{\text{in}} \in \mathbb{Z}_2^{s\times s}(D)$, we consider their block truncations and we couple them in a multiple serial concatenation through permutations π_i of length nN (which act on symbols) by the map composition

$$\mathcal{S} = \phi_{L_N}^{\text{in}} \circ \pi_m \circ \ldots \circ \phi_{L_N}^{\text{in}} \circ \pi_1 \circ \phi_N^{\text{out}}. \tag{4.1}$$

where L_N is such that $sL_N = nN$. The resulting code has rate $R = k/n$.

In order to avoid extremely cumbersome notation, we will at first expose our results in full detail under some assumptions, and later we will discuss how most of the assumptions can be weakened.

Assumption 4.1. *In our setting we assume that:*

- ϕ^{out} *is non-catastrophic with free distance* d_f^o*;*
- ϕ^{in} *is non-catastrophic (with parameter* μ^i*, see Definition 3.4) and recursive (see Definition 3.5).*
- ϕ^{in} *has scalar input* $(s = 1)$

In Theorem 4.7 we will make a further assumption.

Assumption 4.2. *The convolutional encoder $\phi^{\text{out}}(D) \in \mathbb{Z}_2(D)^{k\times n}$ has all k-minors invertible.*

Let $\mathscr{S}_N^m$ be the ensemble of all serial encoders $\mathcal{S}$ in (4.1) obtained by choosing $\pi_1, \dots, \pi_m$ with uniform probability over the set of all possible permutations of nN elements.

Denote with

$$d_{\min}(\mathscr{S}_N^m) := \min_{\boldsymbol{u}\in\mathbb{Z}_2^{kN}\setminus\{\mathbf{0}\}} \left\{ \mathrm{w_H}(\phi_{L_N}^{\text{in}} \circ \pi_m. \circ \dots \circ \phi_N^{\text{out}}(\boldsymbol{u})) \right\},$$

We focus on the minimum distance distribution of these coding schemes, namely on the high-probability behavior of $d_{\min}(\mathscr{S}_N^m)$ as a function of N.

The analysis is undertaken by a detailed study of asymptotic average spectra of this ensemble.

4.2.2 Weight Enumerators and average spectra

Before showing results known in literature and our contribution, we fix some notations.

We consider the *average output weight enumerators* of $\mathscr{S}_N^m$

$$\overline{A}_d\left(\mathscr{S}_N^m\right) := |\mathscr{S}_N^m|^{-1} \textstyle\sum_{\mathcal{S}\in\mathscr{S}_N^m} A_d(\mathcal{S}).$$

They can be expressed in terms of the input-output weight distribution of its component codes (see [17, 18]). We have the following results.

Proposition 4.1.

$$\overline{\mathbf{A}}(\mathscr{S}_N^m) = \mathbf{A}(\phi_N^{\text{out}})\mathbf{P}(\phi_{L_N}^{\text{in}})^m \tag{4.2}$$

where $\mathbf{P}(\phi_{L_N}^{\text{in}})$ is a finite dimensional matrix given by

$$P_{w,d}(\phi_{L_N}^{\text{in}}) := \frac{A_{w,d}(\phi_{L_N}^{\text{in}})}{\binom{nN}{w}}.$$

The entry $P_{w,d}(\phi_{L_N}^{\text{in}})$ can be interpreted as the probability that a randomly chosen input sequence of weight w is mapped by the inner encoder to an output sequence of weight d and for this reason is known as *input-output weight transition probability*. Notice that $\mathbf{P}(\phi_{L_N}^{\text{in}})$ is thus a stochastic matrix. Consider the coefficients $P_{w,d}(\phi_{L_N}^{\text{in}})$ for $w \geq 1$ and $d \geq 1$, since the inner encoder is non-catastrophic (see Assumption 4.1) $P_{w,d}(\phi_{L_N}^{\text{in}})$ is zero if $w > \mu^i d$.

We denote *N-th spectral function* of $\mathscr{S}_N^m$

$$r_N^{(m)}(\delta) := \frac{1}{nN} \ln \overline{A}_{\lfloor \delta nN \rfloor}(\mathscr{S}_N^m), \quad \text{for } \delta \in [0,1].$$

and the *asymptotic spectral function*

$$\widehat{r}^{(m)}(\delta) := \limsup_{N\to\infty} r_N^{(m)}(\delta), \quad \text{for } \delta \in [0,1].$$

Example 4.1 (Repeat Multiple-Accumulate codes)**.** *Repeat Multiple-Accumulate codes, denoted by RA^m and introduced by Jin and McEliece in [48], are the simplest non trivial example of a serial concatenation of rate-1 codes through uniform random interleavers, where the outer encoder is the repeat code and inner encoders are truncated recursive convolutional accumulate codes.*

Given $q \in \mathbb{N}$ and $N \in q\mathbb{N}$, the outer encoder $\mathrm{Rep}_N^q : \mathbb{Z}_2^N \to \mathbb{Z}_2^{qN}$ repeats the information block q-times

$$\mathrm{Rep}_N^q([v_1,\dots,v_N]) = \underbrace{[v_1,\dots,v_N,\dots,v_1,\dots,v_N]}_{q\ times}.$$

and the accumulator $\mathrm{Acc}_N : \mathbb{Z}_2^{qN} \to \mathbb{Z}_2^{qN}$ can be interpreted as the block encoder defined by

$$\mathrm{Acc}_N([u_1,\dots,u_{qN}]) = [u_1, u_1+u_2, \dots, u_1+\dots+u_{qN}].$$

In this case $\mathbf{A}(\mathrm{Rep}_N^q)$ and $\mathbf{P}(\mathrm{Acc}_N)$ can be explicitly computed (see Section 3.4) and we obtain

$$A_{w,d}(\mathrm{Rep}_N^q) = \begin{cases} \binom{N}{w} & qw = d \\ 0 & otherwise \end{cases}$$

$$P_{w,d}(\mathrm{Acc}_N) = \begin{cases} 1 & w = h = 0 \\ \frac{\binom{qN-d}{\lfloor w/2 \rfloor}\binom{d-1}{\lceil w/2 \rceil -1}}{\binom{qN}{w}} & w \geq 1 \text{ and } d \geq 1 \\ 0 & otherwise. \end{cases}$$

Consider the coefficients $P_{w,d}(\mathrm{Acc}_N)$ for $w \geq 1$ and $d \geq 1$ and notice that $P_{w,d}(\mathrm{Acc}_N)$ is non-zero if and only if

$$\lceil w/2 \rceil \leq d \quad and \quad \lfloor w/2 \rfloor \leq n - d,$$

as one of the binomial coefficients in the numerator is zero if either condition is not satisfied.

4.3 Previous results: analysis and design

In this section we state previous results on the minimum distance.

Kahale and Urbanke show that for $m = 1$ the typical minimum distance of such coding schemes scales only sublinearly in N with probability approaching one. Precisely, they prove the following result.

Theorem 4.1 (Theorem 2.a in [36])**.** *If $d = o(N^\beta)$ for $N \to \infty$ with $\beta = 1 - 2/d_f^o$, then there exists a constant C (independent on d and N) such that*

$$\mathbb{P}\left(d_{\min}(\mathscr{S}_N^1) < d\right) \leq C d^{\frac{d_f^o}{2}} N^{1-\frac{d_f^o}{2}} + o\left(d^{\frac{d_f^o}{2}} N^{1-\frac{d_f^o}{2}}\right)$$

and so, in particular, $\mathbb{P}\left(d_{\min}(\mathscr{S}_N^1) < d\right) \overset{N\to\infty}{\longrightarrow} 0$.

Notice that the free distance d_f^o plays a crucial role in the estimation of the minimum distance: the more the parameter d_f^o is large, the more the minimum distance growth rate is close to be linear with high probability.

The picture of $d_{\min}(\mathscr{S}_N^1)$ given in Theorem 4.1 is completed in [36] by proving that if $d/N^\beta \to \infty$ then $\mathbb{P}\left(d_{\min}(\mathscr{S}_N^1) < d\right) \to 1$ when $N \to \infty$ (see Theorem 2.b in [36]). Their proof, based on a second-order method, does not underline how fast is the convergence. However a much stronger result holds true: deterministically (i.e. for any given permutation π), the minimum distance cannot grow more than $CN^\beta \ln N$ for some constant C. This deterministic upper bound is obtained by Bazzi, Mahdian and Spielman for Repeat-Convolute codes (see Theorem 2 in [45]), and generalized later in [74] for a more general setting. We state formally this result.

Theorem 4.2 (Theorem 2 in [74])**.** *There exist constants $C, N_0 \in \mathbb{N}$ such that for all $N \geq N_0$ the following inequality is true*

$$d_{\min}(\mathscr{S}_N^1) \leq CN^\beta \ln(N).$$

In the theoretical analysis of the minimum distance distribution for $m \geq 2$ we can distinguish two main lines. On the one hand, we take fixed truncation lengths and we let m go to ∞. On the other hand, fixed the number of inner encoders, we study the minimum distance as a function of N.

The first approach is exploited in [44]. In particular, the authors prove the following theorem with arguments coming from the spectral theory of stochastic matrices, applied to $\mathbf{P}(\phi_{L_N}^{\text{in}})$.

Theorem 4.3 (Theorem 3 in [44])**.** *For every $N \in \mathbb{N}$, it holds*

$$\overline{A}_d\left(\mathscr{S}_N^\infty\right) := \lim_{m\to\infty} \overline{A}_d\left(\mathscr{S}_N^m\right) = \begin{cases} 1, & \textit{if } d = 0 \\ \binom{nN}{d}\frac{2^{kN}-1}{2^{nN}-1}, & \textit{if } d \geq 1. \end{cases} \tag{4.3}$$

Notice that expressions (2.11) and (4.3) are not identical. The main difference between them comes from the fact that all of the encoders in $\mathscr{S}_N^m$ are invertible for all m, whereas the $\mathscr{L}_N$ contains a small fraction of noninvertible encoders. However, both ensembles behave quite similarly: it can be verified that for any $\epsilon > 0$ there exists N_0 such that $\forall N \geq N_0$

$$|\overline{A}_d\left(\mathscr{L}_N\right) - \overline{A}_d\left(\mathscr{S}_N^\infty\right)| < \epsilon.$$

Theorem 4.3 yields the following result.

Corollary 4.1. *There exists $\{m_N\}_{N\in\mathbb{N}}$ such that for any $\epsilon > 0$*

$$\mathbb{P}\left(d_{\min}(\mathscr{S}_N^{m_N}) < (\delta_{GV} - \epsilon)N\right) \overset{N\to\infty}{\longrightarrow} 0.$$

Proof. Fix η such that $0<\eta<1/2^{1-R}$. It follows from Theorem 4.3 that, for every N and d, there exists $m_N(d)$ such that

$$\left|\overline{A}_d(\mathscr{S}_N^m)-\overline{A}_d(\mathscr{S}_N^\infty)\right|\le\eta^N\qquad\forall N\in\mathbb{N},\ \forall d\ge1,\ \forall m\ge m_N(d)$$

Let now $m_N:=\max\{m_N(d):\ 1\le d\le N\}$. Then,

$$\left|\overline{A}_d(\mathscr{S}_N^{m_N})-\overline{A}_d(\mathscr{S}_N^\infty)\right|\le\eta^N\quad\forall N\in\mathbb{N},\ \forall d\ge1.$$

Equivalently,

$$\frac{\ln\left(\overline{A}_d(\mathscr{S}_N^\infty)-\eta^N\right)}{nN}\le\frac{\ln\overline{A}_d(\mathscr{S}_N^{m_N})}{nN}\le\frac{\ln\left(\overline{A}_d(\mathscr{S}_N^\infty)+\eta^N\right)}{nN}$$
$$\forall N\in\mathbb{N},\ \forall d\ge1\,.$$

Denoting $r_N^{(m_N)}(\delta)=\frac{1}{nN}\ln\overline{A}_{\lfloor\delta nN\rfloor}(\mathscr{S}_N^{m_N})$ we have that

$$r_N^{(m_N)}(\delta)\ge\frac{\ln\overline{A}_{\lfloor\delta nN\rfloor}(\mathscr{S}_N^\infty)}{nN}+\frac{1}{nN}\ln\left(1-\frac{\eta^N}{\overline{A}_{\lfloor\delta nN\rfloor}(\mathscr{S}_N^\infty)}\right)\tag{4.4}$$
$$r_N^{(m_N)}(\delta)\le\frac{\ln\overline{A}_{\lfloor\delta nN\rfloor}(\mathscr{S}_N^\infty)}{nN}+\frac{1}{nN}\ln\left(1+\frac{\eta^N}{\overline{A}_{\lfloor\delta nN\rfloor}(\mathscr{S}_N^\infty)}\right)\tag{4.5}$$

From Stirling approximation [62] we get the following estimations

$$\overline{A}_{\lfloor\delta nN\rfloor}(\mathscr{S}_N^\infty)\ge\frac{\exp\left\{nN\left[H(\delta)-(1-R)\ln2\right]\right\}}{nN+1}\tag{4.6}$$
$$\overline{A}_{\lfloor\delta nN\rfloor}(\mathscr{S}_N^\infty)\le\exp\left\{nN\left[H(\delta)-(1-R)\ln2\right]\right\}.\tag{4.7}$$

From (4.4), (4.5), (4.6) and (4.7) we finally obtain

$$\begin{aligned}r_N^{(m_N)}(\delta)&\ge H(\delta)-(1-R)\ln2-\frac{1}{nN}\ln(nN+1)\\&\quad+\frac{1}{nN}\ln\left[1-\left(\frac{\eta}{\mathrm{e}^{H(\delta)-(1-R)\ln2}}\right)^{nN}(nN+1)\right]\\r_N^{(m_N)}(\delta)&\le H(\delta)-(1-R)\ln2\\&\quad+\frac{1}{nN}\ln\left[1+\left(\frac{\eta}{\mathrm{e}^{H(\delta)-(1-R)\ln2}}\right)^{nN}(N+1)\right].\end{aligned}$$

By the way η has been chosen, we have that $\eta/\mathrm{e}^{H(\delta)-(1-R)\ln2}<1$ for any $\delta\in[0,1]$. Therefore we can conclude that

$$\lim_{N\to\infty}r_N^{(m_N)}(\delta)=H(\delta)-(1-R)\ln2.$$

The assertion is now a straightforward application of (2.13). □

This result is very encouraging, as it puts into evidence that there exists a sequence of codes whose minimum distance converges to the GV bound. Moreover Theorem 4.3 holds for all the convolutional inner encoders (recursive or not recursive). However, this argument does not give any information about the minimum distance distribution for the case of a finite number of inner encoders and it does not guarantee that the typical distance of all serial codes converges to the GV limit.

For this reason our analysis will concern with the computation of the minimum distance distribution for the specific ensemble of $\mathscr{S}^m$ for fixed m.

Regarding this second approach, it is proved in [37] that in the case of RA_N^2 the typical minimum distance scales linearly in N with high probability. An estimation of the linear growth rate is given in [46]. The result is summarized in the following theorem.

Theorem 4.4 (Section 3.6.7 in [46])**.** *For any arbitrary small $\epsilon > 0$ and $\eta > 0$, there exists a constant $C, N_0 \in \mathbb{N}$ such that for all $N \geq N_0$ it holds*

$$\mathbb{P}\left(d_{\min}(RA_N^2) \leq (\overline{\delta} - \epsilon)N\right) \leq CN^{1-\lceil q/2\rceil+\eta} + o\left(N^{1-\lceil q/2\rceil+\eta}\right),$$

where $\overline{\delta} = (4e^{8/q})^{-1}$. This implies that if $q \geq 3$ then $\mathbb{P}(d_{\min}(RA_N^2) \to 0$ when $N \to \infty$.

If we serially concatenate any encoder, whose minimum distance is growing like $\overline{\delta}N$, with an accumulate encoder through a uniform random interleaver, the minimum distance of the new encoder must grow faster than $\overline{\delta}N/2$ as $P_{h,d}(\mathrm{Acc}_N)$ is zero for every $d \leq \lceil h/2\rceil$. Then Theorem 4.2 implies that if the minimum distance behaves linearly in N for $m = 2$ then so must hold for every $m \geq 2$: for any $\epsilon > 0$

$$\mathbb{P}\left(d_{\min}(RA_N^m) \leq (\overline{\delta}/2^{m-2} - \epsilon)N\right) \overset{N\to\infty}{\longrightarrow} 0.$$

Although this argument allows us to conclude that the typical minimum distance is growing linearly in N, it does not allow to prove that the minimum distance grows when m increases. We will improve this estimate and prove that these thresholds are strictly increasing in m.

4.4 Summary of our results

We summarize our main results in the next theorems.

Theorem 4.5 shows that for $m \geq 2$ asymptotic spectral functions exhibit some different features as compared to the case where $m = 1$. The main difference is that for $m \geq 2$ there exists a positive point such that the function is zero below it and positive beyond it.

Theorem 4.5. *Under Assumption 4.1 , there exists a sequence of points $\{\delta_m\}_{m\in\mathbb{N}}$ such that*

$$\max_{\sigma\leq\delta_m}\left\{\widehat{r}^{(m)}(\sigma)\right\}=0,$$

We have to note that Theorem 4.5 corrects some wrong statements in [56], partially revised in [59]. Results presented in [56], [57] are affected by some numerical errors and induce the authors to believe that the spectral function is negative before some threshold and conclude that such point is the normalized minimum distance with high probability. Actually, Theorem 4.5 guarantees that the floor of the spectral functions $\widehat{r}^{(m)}(\delta)$ is zero. Therefore we can not apply Lemma 2.2, in order to estimate the minimum distance distribution.

Nevertheless we shall prove the following theorem.

Theorem 4.6. *For any arbitrarily small $\epsilon>0$ and $\eta>0$, there exists a constant $\chi>0$ and $N_0\in\mathbb{N}$ such that for all $N\geq N_0$ it holds*

$$\mathbb{P}\left(\frac{d_{\min}(\mathscr{S}_N^m)}{nN}<\delta_m-\epsilon\right)\leq\chi N^{\alpha_m+\eta}+o\left(N^{\alpha_m+\eta}\right)$$

where $\alpha_m=1-\sum_{i=1}^{m-1}\lceil d_f^o/2^i\rceil$.

Theorem 4.6 guarantees that, if $m=2$ and the free distance of the outer encoder $d_f^o\geq3$, or if $m\geq3$ and $d_f^o\geq2$, the typical minimum distance scales linearly in the code length with high probability and the distance threshold δ_m is a lower bound of the linear growth.

Let us denote the function

$$H_+^R(\delta)=\begin{cases}H(\delta)-(1-R)\ln2 & \text{if } \delta\in(\delta_{GV},1-\delta_{GV})\\ 0 & \text{otherwise.}\end{cases}$$

where $\delta_{GV}=\delta_{GV}(R)$ is the GV-distance defined in (2.9).

Theorem 4.7. *Under Assumption 4.1 and 4.2 the functions $\widehat{r}^{(m)}(\delta)$ are equicontinuous in $\delta\in[0,1]$ and converge uniformly when $m\to\infty$ to $\widehat{r}^{(\infty)}(\delta)=H_+^R(\delta)$.*

By combining Theorem 4.6 and 4.7 together we have that, if we choose an outer encoder satisfying the algebraic condition in Theorem 3, the sequence of coefficients of the linear growth δ_m converges to the limit implied by GV-bound when m tends to infinity. Notice that the hypothesis on outer encoder is not very restrictive and includes all block encoders obtained by concatenating together N successive codewords of a (n,k) block code (as considered in [47, 54]) and a huge class of convolutional encoders (see [44, 49]).

The normalized minimum distances δ_m are listed in Table I for various Convolutional Multiple-Accumulate (CA^m) ensembles (see also Fig. 4.2, 4.3, 4.4, 4.5) . These numerical results have been found using the MSP-techniques to compute growth rates of the weight distributions of convolutional encoders. Notice that convergence looks quite fast: it is sufficient to put a small number of accumulate codes to get very close to the limit, i.e., to approach the normalized Gilbert-Varshamov distance.

Summarizing, Theorems 4.5 and 4.6 generalize those in [44], improve the earlier estimations of the growth rates in [37] and [46] for $m = 2$, and give a deeper insight into the problem of the aymptotic spectra of $\mathscr{S}^m$.

The achievability of the Gilbert-Varshamov limit when m goes to infinity were conjectured but never analytically proved. Moreover if the inner encoders are accumulators we can strengthen Theorem 4.7: the asymptotic spectra are equi-Lipshitz and form a monotonic decreasing sequence in m.

In Sections 4.5, 4.6, and 4.7 we shall prove respectively Theorem 4.5, 4.6 and 4.7 through intermediate steps.

4.5 Spectral function analysis

This section is devoted to the study of the asymptotic spectral functions for a fixed number of inner encoders m.

4.5.1 Dynamical system formulation

Let define $\Psi : C\left([0,1]\right) \longrightarrow C\left([0,1]\right)$ as follows

$$\Psi[g](\delta) = \max_{0\leq u\leq 1}\{g(u) + f(u,\delta)\}, \quad \forall\delta \in [0,1] \tag{4.8}$$

where

$$f_N(u,\delta) := \frac{1}{nN}\ln P_{\lfloor unN\rfloor,\lfloor\delta nN\rfloor}(\phi^{\text{in}}_{L_N})$$

and

$$f(u,\delta) := \limsup_{N\to\infty} f_N(u,\delta) \tag{4.9}$$

From the fact that $P_{w,d}(\phi^{\text{in}}_{L_N})$ represents a probability, it follows that both functions f_N and f are not positive.

Starting from (4.2) it can be easily seen that the sequence of asymptotic spectral functions can be obtained recursively by applying the operator Ψ to the initial condition

$$\widehat{r}^{(0)}(\delta) := \limsup_{N\to\infty}\frac{1}{nN}\ln A_{\lfloor\delta nN\rfloor}(\phi^{\text{out}}_N). \tag{4.10}$$

However, the theoretical justification of this iterative formula requires to prove uniformity in the convergence of limits in (4.9) and (4.10). This difficulty can be overcome by applying MSP-techniques to the weight enumerators of constituent encoders, devised in the previous chapter.

Table 4.1: Numerical values of linear growth rates δ_m for various ensembles and $m = 2, 3, 4$ ($C(n, k)$ outer code, δ_m normalized distance threshold with m accumulate codes, δ_{GV} normalized GV-distance). Rep=Repeat, Par=Single parity check, Ham=Hamming code, Ham$_e$=extended Hamming, Mlc=Maximum length code

ϕ^{out}	Rep-$(2,1)$	Rep-$(3,1)$	Par-$(3,2)$	Par-$(4,3)$	Ham-$(7,4)$	Ham$_e$-$(8,4)$	Mlc-(3,2)	$\left(1, \frac{1}{1+D}\right)$	$\left(1+D^2, 1+D+D^2\right)$
δ_2	–	0.133	–	–	0.061	0.090	–	0.083	0.104
δ_3	0.103	0.174	0.054	0.035	0.080	0.110	0.055	0.109	0.110
δ_4	0.109	0.174	0.061	0.042	0.087	0.110	0.061	0.110	0.110
δ_{GV}	0.110	0.174	0.061	0.042	0.087	0.110	0.061	0.110	0.110

Theorem 4.8.
$$\widehat{r}^{(m+1)} = \Psi\left[\widehat{r}^{(m)}\right] = \Psi^m\left[\widehat{r}^{(0)}\right]. \tag{4.11}$$

Proof. From expression (4.2) we get

$$r_N^{(m)}(\delta) \geq r_N^{(m-1)}(u) + f_N(u,\delta) \qquad \forall u \in [0,1]$$

and by letting N go to infinity

$$\widehat{r}^{(m)}(\delta) \geq \widehat{r}^{(m-1)}(u) + f(u,\delta) \qquad \forall u \in [0,1]$$
$$\widehat{r}^{(m)}(\delta) \geq \max_{0\leq u\leq 1}\left\{\widehat{r}^{(m-1)}(u) + f(u,\delta)\right\} = \Psi[r^{m-1}](\delta).$$

We prove now by induction on m that $r_N^{(m)}(\delta)$ converges uniformly in $\delta \in [0,1]$ to $\Psi[r^{m-1}](\delta)$ when $N \to \infty$.

From Theorem 3.3 we have that $r_N^{(0)}$ and f_N converge to $\widehat{r}^{(0)}$ and f, respectively, when $N \to \infty$.

By inductive step, assume $r_N^{(m)}$ converges uniformly to $\widehat{r}^{(m)}$ when $N \to \infty$.

Starting from (4.2) we have

$$r_N^{(m+1)}(\delta) \leq \frac{\ln(nN)}{nN} + \max_{u\in[0,1]}\{r_N^{(m)}(u) + f_N(u,\delta)\}$$

from which

$$\begin{aligned}
&\left| r_N^{(m+1)}(\delta) - \max_{0\leq u\leq 1}\left[\widehat{r}^{(m)}(u) + f(u,\delta)\right]\right| \leq \\
&\quad\leq \frac{1}{nN}\ln(nN) + \left|\max_{0\leq u\leq 1}\left[r_N^{(m)}(u) - \widehat{r}^{(m)}(u)\right]\right| + \left|\max_{0\leq u\leq 1}\left[f_N(u,\delta) - f(u,\delta)\right]\right| \\
&\quad\leq \frac{1}{nN}\ln(nN) + \max_{0\leq u\leq 1}\left|r_N^{(m)}(u) - \widehat{r}^{(m)}(u)\right| + \max_{0\leq u\leq 1}\left|f_N(u,\delta) - f(u,\delta)\right|.
\end{aligned}$$

By letting N go to infinity we get

$$\begin{aligned}
0 &\leq \limsup_{N\to\infty}\max_{\delta\in[0,1]}|r_N^{(m+1)}(\delta) - \max_{0\leq u\leq 1}\left[\widehat{r}^{(m)}(u) + f(u,\delta)\right]| \leq \\
&\leq \limsup_{N\to\infty}\frac{1}{nN}\ln(nN) + \limsup_{N\to\infty}\max_{0\leq u\leq 1}\left|r_N^{(m)}(u) - \widehat{r}^{(m)}(u)\right| + \\
&+ \limsup_{N\to\infty}\max_{\delta\in[0,1]}\max_{0\leq u\leq 1}|f_N(u,\delta) - f(u,\delta)| = 0
\end{aligned}$$

and the assertion is verified also for the case $m+1$.

□

Notice that:

- the dynamical system we have defined depends exclusively on the inner encoder and it would be different if we replace it with another convolutional encoder;

- the influence of the outer encoder is in the initial condition.

Moreover, we have that the asymptotic spectral functions are uniformly bounded and continuous.

Proposition 4.2. *The following facts are true:*

1. *the sequence of functions* $\{\widehat{r}^{(m)}\}_{m\in\mathbb{N}}$ *is uniformly bounded. In particular the following inequalities hold*

$$0 \leq \widehat{r}^{(m)}(\delta) \leq R\ln 2 \quad \forall\delta \tag{4.12}$$

2. *Functions* $\widehat{r}^{(m)}(\delta)$ *are continuous in* δ

Proof. 1. We prove it by induction on m. Consider the case with $m = 0$ and notice that $\widehat{r}^{(0)}(\delta) \geq 0$ (see Theorem 3.2) and $\widehat{r}^{(0)}(\delta) \leq R\ln 2$ (the outer encoder has rate R).

Suppose now that the inequalities hold also for m. Using the inductive assumption on $\widehat{r}^{(m)}$ and the fact that f is non-positive, we get that the lower bound holds also for $m+1$

$$\widehat{r}^{(m+1)}(\delta) \geq \max_u\{0 + f(u,\delta)\} = 0\,.$$

On the other hand, as $f(u,\delta)$ is non-negative

$$\widehat{r}^{(m+1)}(\delta) \leq \max_{0\leq u\leq 1}\{\widehat{r}^{(m)}(u)\} \leq R\ln 2$$

where the last inequality is obtained using the inductive hypothesis. The proof is thus complete.

2. The asymptotic spectral function $\widehat{r}^{(0)}(\delta)$ is continuous in its domain, as the asymptotic spectral function of a convolutional encoder is continuous (see Corollary 3.1). The general case can be proved by induction on m, using expression (4.11) and the continuity of $f(u,\delta)$ in both variables (consequence of Corollary 3.1). □

Next two lemmas have been proved in [36] just for systematic terminated convolutional codes but the general case is a straightforward generalization (see [46]).

Lemma 4.1 (Lemma 3 in [36]). *Let* $\psi \in \mathbb{Z}_2(D)^{k\times n}$ *be non-catastrophic. If* $\lfloor d/d_f(\psi)\rfloor \leq N/2$, *there exists a constant* χ_1 *such that*

$$A_d(\psi_N) \leq \chi_1^d \binom{N}{\lfloor d/d_f(\psi)\rfloor}$$

Lemma 4.2 (Lemma 1 in [36]). *Given a non catastrophic and recursive convolutional encoder* ψ, *there exist constants* χ_2, η *such that*

$$A_{w,\leq d}(\psi_N) \leq \chi_2^w \tbinom{N}{\lfloor w/2\rfloor}\tbinom{\eta d}{\lceil w/2\rceil}$$

Lemma 4.3. *Under the Assumption 4.1, there exists a constant $C > 0$ such that*

$$\lim_{\delta\to 0^+} \frac{\widehat{r}^{(1)}(\delta)}{\delta} \leq C.$$

Proof. It follows immediately from expression in (4.2), estimating the enumerating coefficients of the constituent encoders with Lemmas 4.1 and 4.2, so that we get there exist constants $\eta, \chi_1, \chi_2, \chi, C$ independent on w, d, N

$$\begin{aligned}
\overline{A}_{\leq d}(\mathscr{S}_N^1) &= \sum_{w=d_f^o}^{\mu_i d} A_w(\phi_N^{\text{out}}) \frac{A_{w,\leq d}(\phi_{L_N}^{\text{in}})}{\binom{nN}{w}} \\
&\leq \sum_{w=d_f^o}^{\mu_i d} \chi_1^w \binom{N}{\lfloor w/d_f^o\rfloor} \chi_2^w \frac{\binom{L_N}{\lfloor w/2\rfloor}\binom{\eta d}{\lceil w/2\rceil}}{\binom{nN}{w}} \\
&\leq \sum_{w=d_f^o}^{\mu_i d} \binom{N}{\lfloor w/d_f^o\rfloor} \left(\chi\frac{d}{nN}\right)^{\lceil \frac{w}{2}\rceil}
\end{aligned}$$

If $d/nN < 1/\chi$ then

$$\overline{A}_{\leq d}(\mathscr{S}_N^1) \leq d_f^o \sum_{j=1}^{\lfloor \mu_i d/d_f^o\rfloor} \binom{N}{j}\left(\chi\frac{d}{nN}\right)^{\frac{j d_f^o}{2}} \leq \left[1+\left(\chi\frac{d}{nN}\right)^{\frac{d_f^o}{2}}\right]^N - 1$$

from which it follows that

$$\frac{\widehat{r}^{(1)}(\delta)}{\delta} \leq C\delta^{d_f^o/2-1} + o\left(\delta^{d_f^o/2-1}\right) \xrightarrow{\delta\to 0^+} \begin{cases} C \text{ if } d_f^o = 2 \\ 0 \text{ if } d_f^o \geq 3 \end{cases}$$

where C is a constant independent on N. □

Theorem 4.9. *Under the Assumption 4.1, if $m \geq 2$ there exists a threshold $\delta \in (0, 1/2)$ such that*

$$\max_{\sigma\leq\delta}\left\{\widehat{r}^{(m)}(\sigma)\right\} = 0$$

Proof. We prove the assertion by induction on m.

As initial case we can take $m = 2$. From Lemma 4.2 and Stirling's approximation [62] there exist constants η, κ such that

$$F(u,\delta) = \max_{\sigma\leq\delta}\{f(u,\sigma)\} \leq \delta\eta H\left(\frac{u}{2\delta\eta}\right) + u\kappa + H(u/2) - H(u).$$

As $F(0,\delta) = f(0,\delta) = 0$ it follows that there exists a constant c such that

$$\limsup_{u\to 0^+} \frac{F(u,\delta)}{u} \leq \frac{1}{2}\ln\delta + c + o(1) \quad \delta\to 0.$$

and by Lemma 4.3 we have for any sufficiently small δ

$$\lim_{u\to 0^+} \frac{\widehat{r}^{(1)}(u) + F(u,\delta)}{u} < 0 \quad \forall u \in (0, \mu^i \delta).$$

Being $\widehat{r}^{(1)}(0) + f(0,\delta) = 0$, the assertion is verified for $m = 2$.

For the inductive step, assume the statement is true for m: there exists a threshold $\tilde{\delta} \in (0, 1/2)$ such that $\max_{\sigma\leq\tilde{\delta}} \left\{\widehat{r}^{(m)}(\sigma)\right\} = 0$. If we take $\delta = \tilde{\delta}/\mu^i \in (0, 1/2)$ we have

$$\begin{aligned}\max_{\sigma\leq\delta}\left\{\widehat{r}^{(m+1)}(\sigma)\right\} &= \max_{\sigma\leq\tilde{\delta}/\mu^i}\left\{\max_{u\leq\mu^i\sigma}[\widehat{r}^{(m)}(u) + f(u,\sigma)]\right\}\\ &= \max_{u\leq\tilde{\delta}}\left\{\widehat{r}^{(m)}(u) + \max_{\sigma\leq\tilde{\delta}/\mu^i}[f(u,\sigma)]\right\} = 0\end{aligned}$$

where the last equality follows from the inductive hypothesis and from negativity of function f. □

Define the sequence of points $\{\delta\}_{m\geq 1}$ such that

$$\delta_m = \max\{\epsilon \in [0, 1/2) : \max_{\sigma\leq\epsilon} \widehat{r}^{(m)}(\sigma) = 0\}. \tag{4.13}$$

Proposition 4.3. $\widehat{r}^{(m)}(\delta) \geq H_+^R(\delta), \forall\delta.$

Proof. From Theorem 3.3 we have that $\widehat{r}^{(0)}(\delta) \geq H(\delta) - (1 - R)\ln 2$ for all δ. The general case can be proved by induction on m. Putting together this fact with point 1. of Proposition 4.2 we get the assertion. □

Corollary 4.2. *Let $\{\delta_m\}_{m\in\mathbb{N}}$ be the sequence defined in (4.13). We have that $\delta_m \leq \delta_{GV}$, $\forall m$.*

It can actually be shown that the sequence of points $\{\delta_m\}$ is monotonic and strictly increasing in the case of Repeat-convolute codes (see Section 4.8 for details).

We have to note that Theorem 4.5 corrects some wrong statements in [56], partially revised in [59]. Indeed, the authors in [56] overlook the fact that the maximizing value of

$$G^{(m)}(u,\delta) = \widehat{r}^{(m-1)}(u) + f(u,\delta)$$

with respect to the variable u can occur on the boundary. In fact, they only verify numerically that the function at the local maximum is negative. Therefore they claim that the spectral function is negative before some threshold δ_m and conclude that such point δ_m is the normalized minimum distance with high probability.

4.6 Estimation of minimum distance distribution

As we have already noticed, the floor of the spectral functions is zero and we can not apply Lemma 2.2, in order to estimate the minimum distance distribution.

We prove that $\forall \epsilon > 0$ the probability of the event $\{d_{\min}(\mathscr{S}_N^m) \leq (\delta_m - \epsilon) nN\}$ decreases to zero polinomially in N. Inspired by asymptotic techniques devised in [19], we split the computation of the probability into two parts. The first part considers the contribution of the codewords with small weight in the last inner encoder $h < h_N$ and the second part refers to those codewords with weight $h \geq h_N$. The sequence $\{h_N\}_{N \in \mathbb{N}}$ can be chosen in such a way that the first term dominates the behavior of the overall probability.

The bounding approach in the following lemma has been proposed in the case of Convolutional-accumulate codes [46, 55] and we adapt the proof for the general case.

Lemma 4.4. *Let $\{h_N\}_{N\in\mathbb{N}}$ be a sequence of integers such that for all $\xi > 0$*

$$\lim_{N\to\infty} \frac{h_N}{N^\xi} = 0. \tag{4.14}$$

Then

$$\sum_{h=1}^{h_N - 1} \overline{A}_h\left(\mathscr{S}_N^m\right) = O\left(N^{\alpha_m + \xi}\right) \tag{4.15}$$

where $\alpha_m = 1 - \sum_{i=1}^m \lceil d_f^o / 2^i \rceil$.

Proof. We prove the assertion by induction on m. Consider the case $m = 1$ as initial step: from Lemma 4.1 and 4.2 we have that there exist constants χ, c such that

$$\begin{aligned}
\overline{A}_{\leq h_N}\left(\mathscr{S}_N^1\right) &= \sum_{h=1}^{h_N} \sum_{w=d_f^o}^{\mu^i h_N} A_w(\phi_N^{\text{out}}) P_{w,h}(\phi_{L_N}^{\text{in}}) \\
&= \sum_{w=d_f^o}^{\mu^i h_N} A_w(\phi_N^{\text{out}}) \sum_{h=1}^{h_N} P_{w,h}(\phi_{L_N}^{\text{in}}) \\
&\leq \sum_{w=d_f^o}^{\mu^i h_N} \chi^w \binom{N}{\left\lfloor \frac{w}{d_f^o} \right\rfloor} P_{w,\leq h_N}(\phi_{L_N}^{\text{in}}) \\
&\leq \sum_{w=d_f^o}^{\mu^i h_N} c^w N^{\left\lfloor \frac{w}{d_f^o} \right\rfloor} \left(\frac{h_N}{N}\right)^{\left\lceil \frac{w}{2} \right\rceil} \\
&\leq \mu^i h_N \max_{d_f^o \leq w \leq \mu^i h_N} \left\{ N^{\frac{w}{\log_c N} + \left\lfloor \frac{w}{d_f^o} \right\rfloor} \left(\frac{h_N}{N}\right)^{\left\lceil \frac{w}{2} \right\rceil} \right\}
\end{aligned}$$

Choose now an arbitrary small number $\xi > 0$ and define $\hat{\xi} = \frac{\xi}{1+2\lceil d_f^o/2\rceil}$. From (4.14), then we get

$$\lim_{N\to\infty} \frac{h_N}{N^{\hat{\xi}}} = 0.$$

Notice that

$$\begin{aligned}\mu^i h_N \left(\frac{h_N}{N}\right)^{\lceil w/2\rceil} &= \mu^i N^{\hat{\xi}} \left(\frac{h_N}{N^{\hat{\xi}}}\right) \left(\frac{h_N}{N^{\hat{\xi}} N^{1-\hat{\xi}}}\right)^{\lceil w/2\rceil} \\ &= \mu^i N^{\hat{\xi}} \left(\frac{h_N}{N^{\hat{\xi}}}\right)^{\lceil w/2\rceil+1} N^{-(1-\hat{\xi})\lceil w/2\rceil}\end{aligned}$$

then we have

$$\begin{aligned}&\mu^i h_N \max_{d_f^o \le w \le \mu^i h_N} \left\{ N^{w/\log_c N + \lfloor w/d_f^o \rfloor} \left(\frac{h_N}{N}\right)^{\lceil w/2\rceil} \right\} \\ &\quad = N^{\hat{\xi}} \max_{d_f^o \le w \le \mu^i h_N} \left\{ \mu^i N^{\frac{w}{\log_c N} + \lfloor w/d_f^o \rfloor - (1-\hat{\xi})\lceil \frac{w}{2}\rceil} \left(\frac{h_N}{N^{\hat{\xi}}}\right)^{\lceil \frac{w}{2}\rceil+1} \right\}.\end{aligned}$$

Let $C > 0$ be a constant. Since $h_N/N^{\hat{\xi}} \overset{N\to\infty}{\longrightarrow} 0$, we have that for $w \ge d_f^o$ and N large enough

$$\mu^i \left(\frac{h_N}{N^{\hat{\xi}}}\right)^{1+\lceil w/2\rceil} \le \mu^i \left(\frac{h_N}{N^{\hat{\xi}}}\right)^{1+\lceil d_f^o/2\rceil} \le C.$$

Also for $d_f^o \le w \le \mu^i h_N$ and N large enough

$$\frac{w}{\log_c N} + \left\lfloor \frac{w}{d_f^o} \right\rfloor - (1-\hat{\xi}) \left\lceil \frac{w}{2} \right\rceil \le \left\lfloor \frac{w}{d_f^o} \right\rfloor - (1-2\hat{\xi}) \left\lceil \frac{w}{2} \right\rceil \le 1 - (1-2\hat{\xi}) \left\lceil \frac{d_f^o}{2} \right\rceil.$$

Hence, for fixed $C > 0$ and for N large enough we get that

$$\begin{aligned}\sum_{h=1}^{h_N} \overline{A}_h(\mathscr{S}_N^1) &\le \mu^i h_N \max_{d_f^o \le w \le \mu^i h_N} \left\{ N^{w/\log_c N + \lfloor w/d_f^o \rfloor} \left(\frac{h_N}{N}\right)^{\lceil w/2\rceil} \right\} \\ &\le C N^{\hat{\xi}+1-(1-2\hat{\xi})\lceil d_f^o/2\rceil} \\ &= C N^{1-\lceil d_f^o/2\rceil + \hat{\xi}\left(1+2\lceil d_f^o/2\rceil\right)} \\ &= C N^{1-\lceil d_f^o/2\rceil+\xi}\end{aligned}$$

Assume now that this statement is true for the case $m-1$: we have

$$\begin{aligned}\sum_{h=1}^{h_N} \overline{A}_h(\mathscr{S}_N^m) &= \sum_{h=1}^{h_N} \sum_{w=1}^{\mu^i h_N} \overline{A}_w(\mathscr{S}_N^{m-1}) P_{w,h}(\phi_{L_N}^{\text{in}}) \\ &= \sum_{w=1}^{\mu^i h_N} \overline{A}_w(\mathscr{S}_N^{m-1}) \sum_{h=1}^{h_N} P_{w,h}(\phi_{L_N}^{\text{in}}).\end{aligned}$$

Let now $\xi > 0$ be an arbitrary small number and $\hat{\xi} = \xi/(1 + 2\lceil d_f^o/2^m \rceil)$. From inductive hypothesis we have that for fixed $C > 0$ and for large enough N

$$\sum_{h=1}^{\mu^i h_N} \overline{A}_h(\mathscr{S}_N^{m-1})) \leq C N^{1-\sum_{i=1}^{m-1} \lceil d_f^o/2^i \rceil + \hat{\xi}}$$

It follows that

$$\begin{aligned}\sum_{h=1}^{h_N} \overline{A}_h(\mathscr{S}_N^m) &\leq C N^{1-\sum_{i=1}^{m-1} \lceil d_f^o/2^i \rceil + \hat{\xi}} \sum_{w=\lceil d_f^o/2^{m-1} \rceil}^{\mu^i h_N} c^w \left(\frac{h_N}{N}\right)^{\lceil w/2 \rceil} \\ &\leq C N^{1-\sum_{i=1}^{m-1} \lceil d_f^o/2^i \rceil + \hat{\xi}} \mu^i h_N \max_{\lceil d_f^o/2^{m-1} \rceil \leq w \leq \mu^i h_N} c^w N^{-\lceil w/2 \rceil} h_N^{\lceil w/2 \rceil} \\ &\leq C N^{1-\sum_{i=1}^{m} \lceil d_f^o/2^i \rceil + \xi}.\end{aligned}$$

Then the statement is proved also for m. □

Lemma 4.5. *There exists a constant χ (independent on N) such that*

$$r_N^{(m)}(\delta) \leq \chi \frac{\ln N}{N} + \widehat{r}^{(m)}(\delta)$$

Proof. We give the proof by induction on m. As an initial step, we take $m = 0$: by using Theorem 3.1, 3.3 and 3.4 we get there exists χ such that

$$\widehat{r}_N^{(0)}(\delta) = \frac{1}{nN} \ln A_{\lfloor \delta n N \rfloor}(\phi_N^{\text{out}}) \leq \chi \frac{\ln N}{N} + \widehat{r}^{(0)}(\delta)$$

and the statement is trivially verified.

For the inductive step, assume that the statement of this lemma is true for $m - 1$: from Stirling approximation [62] we have

$$\begin{aligned}\overline{A}_d(\mathscr{S}_N^m) = \sum_{h=1}^{\mu^i d} \overline{A}_h(\mathscr{S}_N^{m-1}) P_{h,d}(\phi_{L_N}^{\text{in}}) &\leq \mu^i d \max_{1 \leq h \leq \mu^i d} \{\overline{A}_h(\mathscr{S}_N^{m-1}) P_{h,d}(\phi_{L_N}^{\text{in}})\} \\ &\leq \mu^i d \max_{\frac{h}{nN} \in \left[\frac{1}{nN}, \frac{\mu^i d}{nN}\right]} \left\{ e^{nN\left[\widehat{r}^{(m-1)}\left(\frac{h}{nN}\right) + \chi \frac{\ln N}{N}\right]} (nN+1) \frac{e^{nN\left[\frac{1}{nN} \ln A_{h,d}(\phi_{L_N}^{\text{in}})\right]}}{e^{nNH\left(\frac{h}{nN}\right)}} \right\} \\ &\leq \exp\left\{ nN \left[\max_{\frac{h}{nN} \in \left[\frac{1}{nN}, \mu^i \frac{d}{nN}\right]} \left[\widehat{r}^{(m-1)}\left(\frac{h}{nN}\right) + f\left(\frac{h}{nN}, \frac{d}{nN}\right) \right] + \tilde{\chi} \frac{\ln N}{N} \right] \right\} \\ &\leq \exp\left\{ nN \left[\widehat{r}^{(m)}\left(\frac{d}{nN}\right) + \tilde{\chi} \frac{\ln N}{N} \right] \right\}\end{aligned}$$

where the last equality follows from (4.11). Then statement is proved also for m. □

4.6.1 Proof of Theorem 4.6

Proof. Fix $\epsilon > 0$ and let $d_N = (\delta_m - \epsilon)nN$. Pick a sequence of integers $\{h_N\}_{N\in\mathbb{N}}$ satisfying condition (4.14) and such that

$$\lim_{N\to\infty} \frac{\ln N}{h_N} = 0. \tag{4.16}$$

From (2.13) we have

$$\begin{aligned}
\mathbb{P}(d_{\min}(\mathscr{S}_N^m) \leq d_N) &\leq \sum_{d=1}^{d_N} \sum_{h=1}^{\mu^i d} \overline{A}_h\left(\mathscr{S}_N^{m-1}\right) P_{h,d}(\phi_{L_N}^{\text{in}}) \\
&\leq \sum_{h=1}^{\mu^i d_N} \sum_{d=1}^{d_N} \overline{A}_h\left(\mathscr{S}_N^{m-1}\right) P_{h,d}(\phi_{L_N}^{\text{in}}) \\
&= \sum_{h=1}^{h_N-1} \overline{A}_h\left(\mathscr{S}_N^{m-1}\right) \sum_{d=1}^{d_N} P_{h,d}(\phi_{L_N}^{\text{in}}) + \\
&+ \sum_{h=h_N}^{\mu^i d_N} \sum_{d=1}^{d_N} \overline{A}_h\left(\mathscr{S}_N^{m-1}\right) P_{h,d}(\phi_{L_N}^{\text{in}}) \\
&\leq \sum_{h=1}^{h_N-1} \overline{A}_h(\mathscr{S}_N^{m-1}) + B_N^m
\end{aligned} \tag{4.17}$$

where the last step is obtained from the fact that $\mathbf{P}(\phi_{L_N}^{\text{in}})$ is a stochastic matrix and defining

$$B_N^m = \sum_{h=h_N}^{\mu^i d_N} \sum_{d=1}^{d_N} \overline{A}_h(\mathscr{S}_N^{m-1}))P_{h,d}(\phi_{L_N}^{\text{in}}).$$

Let $G_m(x,y) = \widehat{r}^{(m-1)}(x) + \max_{\sigma\in[1/nN,y]} f(x,\sigma)$.

From Lemma 4.5 and Stirling approximation [62] we can estimate as follows:

$$\begin{aligned}
B_N^m &= \sum_{h=h_N}^{\mu^i d_N} \sum_{d=1}^{d_N} \overline{A}_h(\mathscr{S}_N^{m-1}) P_{h,d}(\phi_{L_N}^{\text{in}}) \\
&\leq \sum_{h=h_N}^{\mu^i d_N} \sum_{d=1}^{d_N} \mathrm{e}^{nNr_N^{(m-1)}\left(\frac{h}{nN}\right)} (nN+1) \frac{\mathrm{e}^{nN\left[\frac{1}{nN}\ln A_d(\phi_{L_N}^{\text{in}}))\right]}}{\mathrm{e}^{nNH\left(\frac{h}{nN}\right)}} \\
&\leq (nN+1) \sum_{h=h_N}^{\mu^i d_N} \sum_{d=1}^{d_N} \mathrm{e}^{nN\left[\widehat{r}^{(m-1)}\left(\frac{h}{nN}\right)+\chi\frac{\ln N}{N}+f\left(\frac{h}{nN},\frac{d}{nN}\right)\right]} \\
&= N^{\tilde{\chi}} \sum_{h=h_N}^{\mu^i d_N} \sum_{d=1}^{d_N} \mathrm{e}^{nN\left[\widehat{r}^{(m-1)}\left(\frac{h}{nN}\right)+f\left(\frac{h}{nN},\frac{d}{nN}\right)\right]} \\
&\leq d_N N^{\tilde{\chi}} \sum_{h=h_N}^{\mu^i d_N} \mathrm{e}^{nN\max_{d\in[1/nN,d_N/nN]}\left[\widehat{r}^{(m-1)}\left(\frac{h}{nN}\right)+f\left(\frac{h}{nN},\frac{d}{nN}\right)\right]} \\
&= N^{\hat{\chi}} \sum_{h=h_N}^{\mu^i d_N} \mathrm{e}^{nNG^{(m)}\left(\frac{h}{nN},\frac{d_N}{nN}\right)} \\
&= N^{\hat{\chi}} \sum_{h=h_N}^{\mu^i d_N} \mathrm{e}^{nNG^{(m)}\left(\frac{h}{nN},\delta_m-\epsilon\right)}
\end{aligned}$$

For $h_N \leq h \leq \mu^i d_N$ it holds that

$$nNG_m(h/nN, \delta_m - \epsilon) \leq h\tau.$$

where

$$\tau = \max_{h_N/(nN)<u\leq\mu^i(\delta_m-\epsilon)} \frac{G_m(u,\delta_m-\epsilon)}{u}$$

Using the fact that $\widehat{r}^{(m-1)}$ and f are both continuous (and so is G) and by the way δ_m has been defined (4.13), we obtain that

$$G_m(u,\delta_m-\epsilon) < 0 \quad \text{for } u \in [h_N/(nN), \mu^i(\delta_m-\epsilon)].$$

Hence,

$$\tau \leq \lim_{N\to\infty} \frac{G_m(h_N/(nN),\delta_m-\epsilon)}{h_N/(nN)} = \frac{\partial G(u,\delta_m-\epsilon)}{\partial u} < 0\,. \tag{4.18}$$

We get

$$B_N^m \leq N^{\tilde{\chi}} \sum_{h=h_N}^{\mu^i d_N} \mathrm{e}^{\tau h} \leq N^{\hat{\chi}} \frac{\mathrm{e}^{h_N\tau}}{1-e^{\tau}}.$$

It follows from the condition (4.16) that

$$\begin{aligned} B_N^m &\leq \exp\left[\tilde{\chi}\ln N + \tau h_N\right] \\ &= \exp\left[h_N\left(\frac{\tilde{\chi}\ln N}{h_N} + \tau\right)\right] \overset{N\to\infty}{\longrightarrow} 0. \end{aligned}$$

From (4.17) and Lemma 4.4, we conclude that $\forall \eta > 0$

$$\mathbb{P}(d_{\min}(\mathscr{S}_N^m) \leq (\delta_m - \epsilon)nN) = O\left(N^{\alpha_{m-1}+\eta}\right), \tag{4.19}$$

from which, if we choose η sufficiently small, it follows that

$$\lim_{N\to\infty} \mathbb{P}(d_{\min}(\mathscr{S}_N^m) \leq (\delta_m - \epsilon)nN) = 0$$

for $m \geq 3$ and $q \geq 2$ or $m = 2$ and $q \geq 3$. □

4.7 Asymptotic analysis

In Section 4.5 we have studied the properties of the asymptotic spectral function for a fixed number of inner encoders m. We now analyze the behavior for $m \to +\infty$.

The dynamical system formulation allows us to track the evolution of the spectral function as it passes through each inner encoder. Through some techniques of non smooth analysis and the study of fixed points of dynamical systems, we will be able to study the convergence of the sequence of spectral functions and to complete the proof of Theorem 4.7.

4.7.1 Spectral function evolution

We start with some simple properties:

Lemma 4.6. *Let $g, h \in C([0,1])$, then,*

1. $\|\Psi[g] - \Psi[h]\|_\infty \leq \|g - h\|_\infty$.
2. *If* $g(\delta) \leq h(\delta)$ $\forall\delta \in [0,1]$, *then* $\Psi[g](\delta) \leq \Psi[h](\delta)$ $\forall\delta \in [0,1]$.
3. $\Psi[g + C] = C + \Psi[g]$, *for any* $C \in \mathbb{R}$.

Proof. 1. The result is an immediate consequence of the following fact

$$\begin{aligned} \Psi[g](\delta) \leq \max_{u\in[0,1]}[g(u) - h(u)] + \max_{u\in[0,1]}[h(u) + f(u,\delta)] = \\ = \max_{u\in[0,1]}[g(u) - h(u)] + \Psi[h](\delta). \end{aligned}$$

2. and 3. are obvious. □

We say that $g \in C([0,1])$ is a *fixed point* for Ψ if $g = \Psi[g]$. It follows from 3. of Lemma 4.6 that, if g is a fixed point for Ψ, then the same holds for $g + C$. Another interesting way to modify fixed points is illustrated in the following result.

Proposition 4.4. *If g is a fixed point for Ψ, then $g_+(x) = [0 \vee g](x)$ is a fixed point for Ψ.*

Proof. Consider the subset of maximizing points

$$\Gamma^+(\delta) = \operatorname*{argmax}_{u\in[0,1]} [g_+(u) + f(u,\delta)].$$

For each $\delta \in [0,1]$ choose $u^+(\delta) \in \Gamma^+(\delta)$. We have

$$\begin{aligned}\Psi[g_+](\delta) &= g_+(u^+(\delta)) + f(u^+(\delta),\delta) = \\ &= f(u^+(\delta),\delta) \vee [g(u^+(\delta)) + f(u^+(\delta),\delta)] \leq \\ &\leq f(u^+(\delta),\delta) \vee \left\{ \max_{u\in[0,1]} [g(u) + f(u,\delta)] \right\} = \\ &= f(u^+(\delta),\delta) \vee g(\delta). \end{aligned} \tag{4.20}$$

Suppose now that $\delta \in [0,1]$ is such that $g(\delta) \leq 0$. Then, from (4.20) we have

$$0 \leq \Psi[g_+](\delta) \leq f(u^+(\delta),\delta) \vee g(\delta) \leq 0.$$

We conclude that $\Psi[g_+](\delta) = 0 = g_+(\delta)$.

If instead δ is such that $g(\delta) > 0$, we have

$$g(u) \leq g_+(u) \Longrightarrow g = \Psi[g] \leq \Psi[g_+].$$

As f is non-positive, it follows that

$$g(\delta) \leq \Psi[g_+](\delta) \leq f(u^+(\delta),\delta) \vee g(\delta) = g(\delta),$$

and we conclude that $\Psi[g_+](\delta) = g(\delta) = g_+(\delta)$. This completes the proof. □

Proposition 4.5. *The following functions are fixed points for Ψ, for any arbitrary constant C:*

1. $g(\delta) = C$;
2. $g(\delta) = H(\delta) + C$.

Proof. 1. The result follows trivially by noticing that $g = 0$ is a fixed point for Ψ as $f(u,\delta)$ is non-positive. It then follows from property 3. of Lemma 4.6.

2. Since $\phi^{\text{in}}_{L_N}$ has unitary rate then $\operatorname{Im}(\phi^{\text{in}}_{L_N}) = \mathbb{Z}_2^{nN}$ then

$$\sum_{w=1}^{nN} A_{w,d}(\phi^{\text{in}}_{L_N}) = \binom{nN}{d}.$$

It is straightforward to verify that $\max_{u\in[0,1]} f(u,\delta) = H(\delta)$. □

An important consequence of Propositions 4.4 and 4.5 is that both $H(\delta) - (1-R)\ln 2$ and $H_+^R(\delta) = [H(\delta) - (1-R)\ln 2]_+$ are fixed points for Ψ.

Proposition 4.6. *If all k-minors of $\psi^{\text{out}}(D) \in \mathbb{Z}_2(D)^{k\times n}$ are invertible, then*

$$\widehat{r}^{(0)}(\delta) \leq RH(\delta) = y^{(0)}(\delta).$$

Proof. Let C_k^n be the set of k-combination of the finite set $\{1,\dots,n\}$ and $\boldsymbol{x} \in [0,1]^n$ such that $||\boldsymbol{x}||_1 = n\delta$. If all k-minors of $\psi^{\text{out}}(D) \in \mathbb{Z}_2(D)^{k\times n}$ are invertible then

$$\widehat{r}^{(0)}(\delta) \leq \tfrac{1}{n} \bigwedge\nolimits_{\mathcal{I}\in C_k^n} \sum\nolimits_{i\in\mathcal{I}} H(x_i)$$

or equivalently

$$\widehat{r}^{(0)}(\delta) \leq \tfrac{k}{n} \sum\nolimits_{i=1}^k \tfrac{1}{k} H(x_i) \leq RH\left(\tfrac{1}{k}\sum\nolimits_{i=1}^k x_i\right)$$

where $x_1 \leq x_2 \leq \dots \leq x_n$ and $||\boldsymbol{x}||_1 = n\delta$. Suppose ab absurdo that $\sum_{i=1}^k x_i > k\delta$ then $\delta < x_k \leq \dots \leq x_n$ and

$$n\delta = \sum\nolimits_{i=1}^k x_i + \sum\nolimits_{i=k+1}^n x_i \geq \sum\nolimits_{i=1}^k x_i + (n-k)\delta$$

from which we get the contradiction and we conclude the thesis. □

From Lemma 4.6 and Proposition 4.3 we get

$$H_+^R(\delta) \leq \widehat{r}^{(m)}(\delta) \leq \Psi^m\left[y^{(0)}(\delta)\right] = y^{(m)}(\delta). \tag{4.21}$$

Theorem 4.10. *The following facts are true:*

1. *$\{y^{(m)}(\delta)\}_{m\in\mathbb{N}}$ is decreasing in m.*
2. *$\{y^{(m)}\}_{m\in\mathbb{N}}$ is a sequence of equicontinuous functions.*
3. *The sequence $\{y^{(m)}\}_{m\in\mathbb{N}}$ converges uniformly to a limit function $y^{(\infty)}$.*

Proof. 1. Let us suppose by contradiction that there exists $\overline{\delta} \in [0,1]$ such that $y^{(1)}(\overline{\delta}) > y^{(0)}(\overline{\delta})$. Since the function f is non-positive we have that

$$\begin{aligned} y^{(1)}(\overline{\delta}) &= \max_{\overline{\delta}\leq u\leq 1-\overline{\delta}} \{RH(u) + f(u,\overline{\delta})\} \\ &\leq \max_{\overline{\delta}\leq u\leq 1-\overline{\delta}} \{RH(u) - H_+^R(u)\} + \Psi[H_+^R](\overline{\delta}) \end{aligned}$$

Since the inner encoder has rate equal to 1 we have $\Psi[H_+^R](\overline{\delta}) = H_+^R(\overline{\delta})$. We conclude that $y^{(1)}(\overline{\delta}) \leq y^{(0)}(\overline{\delta})$, which contradicts the previous assumption.

The general case is then proved by induction on m. For the inductive step, we assume that the statement is true for m: from the recursive expression (4.11) and inductive hypothesis we have

$$\begin{aligned}\widehat{r}^{(m+1)}(\delta) &= \max_{0\leq u\leq 1}\left\{\widehat{r}^{(m)}(u)+f(u,\delta)\right\}\\ &\leq \max_{0\leq u\leq 1}\left\{\widehat{r}^{(m-1)}(u)+f(u,\delta)\right\}\\ &= \widehat{r}^{(m)}(\delta) \qquad \forall\delta\in[0,1]\end{aligned}$$

and the statement is proved also for $m+1$.

2. From Corollary 3.1 we know that the function $f(u,\delta)$ is continuous in both variables as sum of continuous functions: for any arbitrary $\epsilon>0$ there exists $\eta>0$ such that for all $|\delta-\tilde{\delta}|<\eta$ it holds

$$f(u,\tilde{\delta})-\epsilon\leq f(u,\delta)\leq f(u,\tilde{\delta})+\epsilon$$

from which

$$\begin{aligned}y^{(m)}(\delta) &= \max_{0\leq u\leq 1}[y^{(m-1)}(u)+f(u,\delta)]\\ &\leq \max_{0\leq u\leq 1}[y^{(m-1)}(u)+f(u,\tilde{\delta})+\epsilon]\\ &= y^{(m)}(\tilde{\delta})+\epsilon,\end{aligned}$$

and

$$\begin{aligned}y^{(m)}(\delta) &= \max_{0\leq u\leq 1}[y^{(m-1)}(u)+f(u,\delta)]\\ &\geq \max_{0\leq u\leq 1}[y^{(m-1)}(u)+f(u,\tilde{\delta})-\epsilon]\\ &= y^{(m)}(\tilde{\delta})-\epsilon.\end{aligned}$$

Notice that η only depends on f and ϵ and not on m.

3. Since the sequence of functions $\{y^{(m)}\}_{m\geq 1}$ is decreasing in m and is lower bounded, it converges to the limit function $y^{(\infty)}$. Let

$$a_m=\max_{\delta\in[0,1]}\left[y^{(m)}(\delta)-y^{(\infty)}(\delta)\right].$$

Then, the sequence $\{a_m\}_{m\in\mathbb{N}}$ is monotonically decreasing in m and has a limit when $m\to\infty$.

The family $\{y^{(m)}\}_{m\geq 1}$ consists of uniformly bounded equicontinuous functions. Therefore Ascoli Arzelá's theorem (see [75]) guarantees that there exists a subsequence $\{m_j\}_{j\in\mathbb{N}}$ such that $a_{m_j}\to 0$ when $j\to\infty$. For the uniqueness of this limit we conclude that $a_m\to 0$. □

Corollary 4.3. *$y^{(\infty)}(\delta)$ is a fixed point for Ψ.*

Proof. It follows from Theorem 4.10, equation (4.11) and Lemma 4.6. □

4.7.2 Analysis of limit function $y^{(\infty)}(\delta)$

As we know the family $\{y^{(m)}\}_{m\geq 1}$ consists of a sequence of continuous and nonnegative functions converging uniformly to the limit function $y^{(\infty)}$. The next proposition characterizes some properties of it.

Proposition 4.7. *The following facts are true*

1. $y^{(\infty)}(\delta) : [0,1] \to \mathbb{R}^+$ *is continuous.*
2. *There exists* $\delta_\infty > 0$ *such that* $y^{(\infty)}(\delta) = 0$, $\forall \delta \leq \delta_\infty$*;*

Proof. These are trivial consequences of Theorem 4.10. □

Notice that we already know a fixed point of Ψ satisfying all properties stated in Proposition 4.7: it is the function $H_+^R(\delta)$. For the moment, from Proposition 4.2 and Theorem 4.10, we only know that, for any $\delta \in [0,1]$, $y^{(\infty)}(\delta) \geq [H(\delta) - (1-R)\ln 2]_+$. In the rest of this section we will prove that they are in fact equal.

Let us define the following function:

$$t^{(\infty)}(\delta) := \begin{cases} \max\limits_{\sigma\leq\delta} y^{(\infty)}(\sigma) \vee \max\limits_{\sigma\leq\delta} y^{(\infty)}(1-\sigma) & \delta \leq 1/2 \\ \max\limits_{\sigma\leq 1-\delta} y^{(\infty)}(\sigma) \vee \max\limits_{\sigma\leq 1-\delta} y^{(\infty)}(1-\sigma) & \delta > 1/2 \end{cases} \tag{4.22}$$

Proposition 4.8. *The following facts are true*

1. $t^{(\infty)}(\delta)$ *is continuous in* $\delta \in [0,1]$.
2. $t^{(\infty)}(\delta) = t^{(\infty)}(1-\delta)$.
3. $t^{(\infty)}(\delta)$ *is increasing in* $\delta \in [0,1/2]$.

Proof. 1. It follows trivially from property 1. in Proposition 4.8. 2. and 3. follow trivially by definition. □

Let

$$q(u,\delta) := \begin{cases} \max\limits_{\sigma\leq\delta} [f(u,\sigma)] \vee \max\limits_{\sigma\leq\delta} [f(u,1-\sigma)] & \delta \leq 1/2 \\ \max\limits_{\sigma\leq 1-\delta} [f(u,\sigma)] \vee \max\limits_{\sigma\leq 1-\delta} [f(u,1-\sigma)] & \delta > 1/2 \end{cases}$$

and define

$$\Upsilon[g](\delta) = \max_{0\leq u\leq 1} \{g(u) + q(u,\delta)\}, \quad \forall \delta \in [0,1].$$

Proposition 4.9. *It holds true*

1. $\Upsilon[H](\delta) = H(\delta)$
2. $\Upsilon[H(\delta) + C] = H(\delta) + C$

3. $\Upsilon[H_+^R](\delta) = [H_+^R](\delta)$

Proof. 1. We have the following equalities

$$\begin{aligned}
\Upsilon[H](\delta) &= \max_{0\leq u\leq 1}\{H(u)+q(u,\delta)\} = \max_{0\leq u\leq 1}\left\{H(u)+\left[\max_{\sigma\leq\delta} f(u,\sigma)\vee \max_{\sigma\leq 1-\delta} f(u,1-\sigma)\right]\right\}\\
&= \max_{0\leq u\leq 1}\left\{\max_{\sigma\leq\delta}[H(u)+f(u,\sigma)]\vee \max_{\sigma\leq 1-\delta}[H(u)+f(u,1-\sigma)]\right\}\\
&= \max_{\sigma\leq\delta}\left\{\max_{0\leq u\leq 1}[H(u)+f(u,\sigma)]\right\}\vee \max_{\sigma\leq 1-\delta}\left\{\max_{0\leq u\leq 1}[H(u)+f(u,1-\sigma)]\right\}\\
&= \max_{\sigma\leq\delta}\{H(\sigma)\}\vee\max_{\sigma\leq\delta}\{H(1-\sigma)\} = H(\delta) \qquad \forall\delta\leq 1/2.
\end{aligned}$$

The equality $H(\delta)=\Upsilon[H](\delta)$ follows from the fact that $q(u,\delta)=q(u,1-\delta)$.

2. It follows from the fact that $q(u,\delta)\leq 0 \quad \forall u,\delta$.

3. The proof is analogous to that of Lemma 4.4 and is a consequence of 2. □

With this formalism we have the following chain of inequalities $\forall\delta\in[0,1]$

$$\Upsilon[H_+^R](\delta) = H_+^R(\delta) \leq \widehat{r}^{(\infty)}(\delta) \leq y^{(\infty)}(\delta) \leq t^{(\infty)}(\delta) = \Upsilon[y^{(\infty)}](\delta) \leq \Upsilon[t^{(\infty)}](\delta). \tag{4.23}$$

In order to prove Theorem 3, it is sufficient to show that this series of inequalities are in fact equalities.

Define

$$\Gamma_\infty(\delta) = \operatorname*{argmax}_{0\leq u\leq 1}\{t^{(\infty)}(u)+q(u,\delta)\} \tag{4.24}$$

Then, for any $u\in\Gamma_\infty(\delta)$ it clearly holds

$$\Upsilon[t^{(\infty)}](\delta) = t^{(\infty)}(u)+q(u,\delta)\,. \tag{4.25}$$

We start with a technical result.

Lemma 4.7. *The following facts are true.*

1. *For any $\delta\in(\delta_\infty,1/2)$ and $u\in\Gamma_\infty(\delta)$, we have $u\in[\delta,1-\delta]$. Moreover, $\delta\in\Gamma_\infty(\delta)$ if and only if $\delta\in\{0,1/2\}$.*

2. *If $\delta_n \overset{n\to\infty}{\longrightarrow} \delta_\infty$ and, $u_n\in\Gamma_\infty(\delta_n)$ is such that $u_n \overset{n\to\infty}{\longrightarrow} u_\infty$, then $u_\infty\in\Gamma_\infty(\delta_\infty)$*

Proof. 1. Since $q(u,\delta)\leq 0$ for any u and δ, it follows from (4.25) that, necessarily,

$$t_\infty(\delta)\leq \max_{0\leq u\leq 1}\{t_\infty(u)+q(u,\delta)\}\leq t_\infty(u)=t_\infty(1-u) \quad \forall u\in\Gamma_\infty(\delta).$$

It now follows by property 2. of Proposition 4.8, that, $u\in[\delta,1-\delta]$. Finally notice that (4.25) holds with $u=\delta$ if and only if $q(\delta,\delta)=0$, and this happens if and only if $\delta\in\{0,1/2\}$.

2. Let $\tilde{u} \in [0,1]$, then

$$t_\infty(\tilde{u}) + q(\tilde{u}, \delta_n) \leq t_\infty(u_n) + q(u_n, \delta_n)\,.$$

By letting $n \to \infty$ and from the continuity of t_∞ and q we get

$$t_\infty(\tilde{u}) + q(\tilde{u}, \delta_\infty) \leq t_\infty(u_\infty) + q(u_\infty, \delta_\infty)\,.$$

This yields the result.

□

Theorem 4.11.

$$t^{(\infty)}(\delta) = H_+^R(\delta), \forall \delta.$$

Proof. Take $\delta \in [\delta_{GV}, 1/2]$, there exists $\delta_1 \in \Gamma_\infty(\delta) \cap (\delta, 1/2]$ such that

$$\begin{aligned} t^{(\infty)}(\delta) &\leq t^{(\infty)}(\delta_1) + q(\delta_1, \delta) \\ &= t^{(\infty)}(\delta_1) - H_+^R(\delta_1) + H_+^R(\delta_1) + q(\delta_1, \delta) \\ &\leq t^{(\infty)}(\delta_1) - H_+^R(\delta_1) + \Upsilon[H_+^R](\delta) \\ &= t^{(\infty)}(\delta_1) - H_+^R(\delta_1) + H_+^R(\delta). \end{aligned}$$

from which

$$0 \leq t^{(\infty)}(\delta) - H_+^R(\delta) \leq t^{(\infty)}(\delta_1) - H_+^R(\delta_1).$$

Repeating the argument k times we get

$$0 \leq t^{(\infty)}(\delta) - H_+^R(\delta) \leq t^{(\infty)}(\delta_{k+1}) - H_+^R(\delta_{k+1}).$$

where $\delta_{k+1}(\delta) \in \Gamma_\infty(\delta_k))$ and

$$0 \leq t^{(\infty)}(\delta) - H_+^R(\delta) \leq \lim_{k\to\infty} \left[t^{(\infty)}(\delta_k) - H_+^R(\delta_k) \right].$$

Since $t^{(\infty)}$ and H_+^R are both continuous, we get

$$0 \leq t^{(\infty)}(\delta) - H_+^R(\delta) \leq t^{(\infty)}\left(\lim_{k\to\infty} \delta_k\right) - H_+^R\left(\lim_{k\to\infty} \delta_k\right).$$

By the way δ_k have been constructed we know that the sequence $\{\delta_k\}_{k\in\mathbb{N}}$, is upper bounded by $1/2$ and increasing in k. Using the fact that $\delta \in \Gamma_\infty(\delta)$ if and only if $\delta = \{0, 1/2\}$, we conclude it converges to $1/2$ and we conclude $t^\infty(\delta) = H_+^R(\delta)$ for every $\delta \in [\delta_{GV}, 1/2]$. Since the functions $t^\infty(\delta)$ and $H_+^R(\delta)$ are both symmetric with respect $\delta = 1/2$, continuous,

$$t^\infty(\delta) = H_+^R(\delta) \quad \forall \delta \in [\delta_{GV}, 1 - \delta_{GV}].$$

□

Corollary 4.4. *We have*

$$y^{(\infty)} = \hat{r}^{(\infty)}(\delta) = H_+^R(\delta)$$

and consequently $\delta_{GV} = \delta_\infty$.

4.8 A particular case: RA^m

Some of the previous results can be strengthen for RA^m. This section is devoted to the study of the asymptotic spectral functions for a fixed number of accumulators m in order to estimate thresholds δ_m.

4.8.1 Average spectral functions

Given $\delta \in [0,1]$, define the interval $\Omega_\delta = [0, 2\delta \wedge 2(1-\delta)]$. It can be verified that the asymptotic spectral functions satisfy the iterative relation in (4.11) with

$$\begin{aligned} f(u,\delta) \doteq f(u,\delta;\mathrm{Acc}) = \\ = \begin{cases} -H(u) + (1-\delta)H\left(\frac{u}{2(1-\delta)}\right) + \delta H\left(\frac{u}{2\delta}\right) \\ \qquad\qquad\qquad u \in \Omega_\delta \text{ and } \delta \in [0,1] \\ -\infty \qquad \text{otherwise} \end{cases} \end{aligned} \tag{4.26}$$

and

$$\widehat{r}^{(0)}(\delta) = H(\delta)/q. \tag{4.27}$$

Proposition 4.10. *The following facts are true*

1. $\widehat{r}^{(m)}(\delta) = \widehat{r}^{(m)}(1-\delta)$*;*
2. $\widehat{r}^{(m)}(\delta)$ *is increasing in* $\delta \in [0,1/2]$ *and* $\widehat{r}^{(m)}\left(\frac{1}{2}\right) = R\ln 2$.

Proof. 1. From (4.27) we have that $\widehat{r}^{(0)}(\delta) = \widehat{r}^{(0)}(1-\delta)$. Consider now the case $m \geq 1$. From (4.11) we get that

$$\begin{aligned} \widehat{r}^{(m)}(1-\delta) &= \max_{u\in[0,1]} \{\widehat{r}^{(m-1)}(u) + f(u,1-\delta)\} \\ &= \max_{u\in[0,1]} \{\widehat{r}^{(m-1)}(u) + f(u,\delta)\} = \widehat{r}^{(m)}(\delta) \end{aligned}$$

where the second equality follows from the fact that $f(u,\delta) = f(u,1-\delta)$, $\forall u \in [0,1]$ (see (4.26)).

2. From (4.27) we have that $\widehat{r}^{(0)}(\delta)$ is strictly increasing in $\delta \in [0,1/2]$. Since

$$\begin{aligned} \frac{\partial}{\partial\delta} f(u,\delta) = H\left(\frac{u}{2\delta}\right) - H\left(\frac{u}{2(1-\delta)}\right) \\ - \frac{u}{2\delta}\ln\frac{1-\frac{u}{2\delta}}{\frac{u}{2\delta}} + \frac{u}{2(1-\delta)}\ln\left(\frac{1-\frac{u}{2(1-\delta)}}{\frac{u}{2(1-\delta)}}\right) \\ = \ln\left(1-\frac{u}{2(1-\delta)}\right) - \ln\left(1-\frac{u}{2\delta}\right) \geq 0 \\ \forall \delta \in [0,1/2],\ u \in \Omega_\delta, \end{aligned} \tag{4.28}$$

if $0 \leq \delta_1 \leq \delta_2 \leq 1/2$ then we have that

$$\begin{aligned}
\widehat{r}^{(m)}(\delta_1) &= \max_{u\in[0,1]} \left\{\widehat{r}^{(m-1)}(u) + f(u,\delta_1)\right\} \\
&= \max_{u\in[0,2\delta_1]} \left\{\widehat{r}^{(m-1)}(u) + f(u,\delta_1)\right\} \\
&\leq \max_{u\in[0,2\delta_1]} \left\{\widehat{r}^{(m-1)}(u) + f(u,\delta_2)\right\} \\
&\leq \max_{u\in[0,2\delta_2]} \left\{\widehat{r}^{(m-1)}(u) + f(u,\delta_2)\right\} = \widehat{r}^{(m)}(\delta_2).
\end{aligned}$$

Moreover, from (4.27) we have that $\widehat{r}^{(0)}(1/2) = R\ln 2$. The general case can be proved by induction on m, using the fact that $f(u,1/2) = 0$.

□

Lemma 4.8. *$\widehat{r}^{(1)}(\delta)$ is differentiable in δ.*

Proof. By concavity of $H(u)$ and by the fact that

$$\begin{aligned}
\frac{\partial^2}{\partial u^2} f(u,\delta) &= \frac{1}{1-u} - \frac{1}{2(2\delta-u)} - \frac{1}{2\left[2(1-\delta)-u\right]} \\
&= \frac{1}{1-u} - \frac{1-u}{(2\delta-u)\left[2(1-\delta)-u\right]} \\
&= \frac{1}{1-u}\left[1 - \frac{(1-u)^2}{(2\delta-u)\left[2(1-\delta)-u\right]}\right] \\
&= \frac{1}{1-u}\left[\frac{(2\delta-u)\left[2(1-\delta)-u\right] - (1-u)^2}{(2\delta-u)\left[2(1-\delta)-u\right]}\right] \\
&= \frac{1}{1-u}\left[\frac{4\delta(1-\delta) - 2u + u^2 - (1-u)^2}{(2\delta-u)\left[2(1-\delta)-u\right]}\right] \\
&= -\frac{1-4\delta(1-\delta)}{(1-u)(2\delta-u)\left[2(1-\delta)-u\right]} \leq 0, \\
&\qquad\qquad \forall\delta,\ u \in \Omega_\delta
\end{aligned}$$

and

$$\frac{\partial^2}{\partial u^2} f(u,\delta) = 0 \iff \delta = 1/2,$$

we conclude that, for fixed δ, $G^{(1)}(u,\delta)$ is strictly concave in $u \in \Omega_\delta$. As

$$\frac{\partial}{\partial u} G^{(1)}(u,\delta)\Big|_{u=0} = +\infty \qquad \frac{\partial}{\partial u} G^{(1)}(u,\delta)\Big|_{u=2\delta} = -\infty,$$

we deduce that the maximizing value $u^{(1)}$ of the function $G^{(1)}(u,\delta)$ is unique and $u^{(1)} \in (0, 2\delta \wedge 2-2\delta)$.

Define the function

$$u^{(1)}(\delta) = \operatorname*{argmax}_{u\in\Omega_\delta} G^{(1)}(u,\delta).$$

If we differentiate $G^{(1)}(u,\delta)$ with respect to u, we get that $u^{(1)}(\delta)$ must satisfy the following condition

$$\begin{aligned}\frac{\partial}{\partial u}G^{(1)}(u,\delta) = -\left(1-\frac{1}{q}\right)\ln(1-u) - \frac{1}{q}\ln u + \\ + \frac{1}{2}\ln(2-2\delta-u) + \frac{1}{2}\ln(2\delta-u) = 0.\end{aligned} \tag{4.29}$$

Rearranging and defining

$$F(u,\delta) = (u^2-2u+4\delta(1-\delta))^{q/2} - (1-u)^{q-1}u$$

we have that $F(u^{(1)}(\delta),\delta) = 0$.

It can be verified that $F(0,0) = 0$, $\frac{\partial}{\partial u}F(u,\delta) < 0$ and F is C^1, then the theorem of implicit function guarantees that $u_q^{(1)}(\delta)$ is C^1, $\forall q \in \mathbb{N}$. □

Theorem 4.12. *There exists a constant $K \in \mathbb{R}$ such that*

$$|\widehat{r}^{(m)}(\delta_2) - \widehat{r}^{(m)}(\delta_1)| \le K|\delta_2-\delta_1| \qquad \forall\delta_1,\delta_2,\forall m.$$

In order to prove Lemma 4.12 we need to establish some intermediate results. Lemma 4.9 allows us to get some information about the monotony of non-smooth functions. The result is surely not original but we give the assertion, as we don't have any reference.

Lemma 4.9. *Let $y : \mathbb{R} \to \mathbb{R}$ be a bounded Lipschitz function such that*

$$\limsup_{\eta\to 0} \frac{y(x+\eta)-y(x)}{\eta} \le 0 \tag{4.30}$$

for all $x \in \mathbb{R}$. Then $y(x)$ is a monotonically decreasing function.

Proof. Notice first that Rademacher's theorem (see [76]) guarantees that y is differentiable at almost every point in $\mathbb{R}$. Let $y' : \mathbb{R} \to \mathbb{R}$ be any bounded measurable function coinciding with the derivative of y when this exists. Clearly $y' \le 0$ almost surely and it is also easy to see that y' coincides with the distributional derivative of y.

Let now $\{\psi_n\}_{n\in\mathbb{N}}$ be a sequence of C^∞ functions such that

$$\mathrm{supp}(\psi_n) = \left[-\frac{1}{n},\frac{1}{n}\right] \qquad \int_{-\infty}^{\infty}\psi_n(x)\,\mathrm{d}x = 1,$$

where $\mathrm{supp}(\psi_n)$ is the set of points where the function ψ_n is not zero. Clearly,

$$\int_{-\infty}^{\infty}\psi_n(x)y(x)\,\mathrm{d}x \overset{n\to\infty}{\longrightarrow} y(0).$$

Fix $a < b$ and consider now the sequence of functions $\{J_n(x)\}_{n\in\mathbb{N}}$ defined by

$$J_n(x) = \int_{-\infty}^{x}[\psi_n(s-b)-\psi_n(s-a)]\,\mathrm{d}s \qquad \forall x\,.$$

We have that the functions $J_n(x)$ are C^∞, compactly supported and $J_n(x) \leq 0$ for every n. We now have

$$\begin{aligned}0 \leq \int_{-\infty}^{\infty} J_n(x)y'(x)\,\mathrm{d}x &= -\int_{-\infty}^{\infty} J_n'(x)y(x)\,\mathrm{d}x = \\ &= -\int_{-\infty}^{\infty} \psi_n(x-b)y(x)\,\mathrm{d}x + \int_{-\infty}^{\infty} \psi_n(x-a)y(x)\,\mathrm{d}x \\ &\overset{n\to\infty}{\longrightarrow} -y(b) + y(a).\end{aligned}$$

Hence, $y(a) \geq y(b)$. This proves the result. □

For every δ, define the following set

$$\Gamma^{(m)}(\delta) = \operatorname*{argmax}_{u\in\Omega_\delta} \{\widehat{r}^{(m-1)}(u) + f(u,\delta)\} \tag{4.31}$$

and choose $u^{(m)}(\delta) \in \Gamma^{(m)}(\delta)$. Moreover we know that $u^{(1)}(\delta)$ is unique.

Lemma 4.10. *For any arbitrary $\epsilon \in]0, 1/2]$, we have:*

1. *if $u^{(m)}(\delta) \leq 2\delta(1-\delta)$ and $\widehat{r}^{(m)}(\delta)$ is Lipschitz in $\delta \in [\epsilon, 1/2]$, then $\widehat{r}^{(m)}(\delta) - H(\delta)$ is decreasing in $\delta \in [\epsilon, 1/2]$;*

2. *if $\widehat{r}^{(m)}(\delta) - H(\delta)$ decreases in $\delta \in [\epsilon, 1/2]$, then $u^{(m+1)}(\delta) \leq 2\delta(1-\delta)$ and $\widehat{r}^{(m+1)}(\delta)$ is Lipschitz in $\delta \in [\epsilon, 1/2]$;*

Proof. 1. From the hypothesis we know that $u^{(m)}(\delta) \leq 2\delta(1-\delta)$ and we can write that for any arbitrary $\eta > 0$

$$\widehat{r}^{(m)}(\delta+\eta) = \max_{0\leq u\leq 2(\delta+\eta)(1-\delta-\eta)} [\widehat{r}^{(m-1)}(u) + f(u,\delta+\eta)].$$

Using the fact that $\frac{\partial^2}{\partial\delta^2} f(u,\delta) \leq 0$, and $\frac{\partial^2}{\partial\delta\partial u} f(u,\delta) \geq 0$ $\forall\delta \leq 1/2$, $\forall u \in \Omega_\delta$, we can estimate, for $u \leq 2(\delta+\eta)(1-\delta-\eta)$,

$$\begin{aligned}f(u,\delta+\eta) &\leq f(u,\delta) + f_\delta(u,\delta)\eta \\ &\leq f(u,\delta) + f_\delta(2(\delta+\eta)(1-\delta-\eta),\delta)\eta\end{aligned}$$

Hence,

$$\begin{aligned}\widehat{r}^{(m)}(\delta+\eta) \leq &\max_{0\leq u\leq 2(\delta+\eta)(1-\delta-\eta)} [\widehat{r}^{(m-1)}(u) + f(u,\delta)+ \\ &\qquad + f_\delta(2(\delta+\eta)(1-\delta-\eta),\delta)\eta] \\ &\leq \widehat{r}^{(m)}(\delta) + f_\delta(2(\delta+\eta)(1-\delta-\eta),\delta)\eta,\end{aligned}$$

where the last inequality follows by the fact that $u^{(m)}(\delta) \leq 2\delta(1-\delta)$. So we have

$$\frac{\widehat{r}^{(m)}(\delta+\eta) - \widehat{r}^{(m)}(\delta)}{\eta} \leq f_\delta(2(\delta+\eta)(1-\delta-\eta),\delta)$$

and

$$\limsup_{\eta\to 0}\frac{\widehat{r}^{(m)}(\delta+\eta)-\widehat{r}^{(m)}(\delta)}{\eta}\leq f_{\delta}(2\delta(1-\delta),\delta)=H'(\delta).$$

From Lemma 4.9 we conclude that $\widehat{r}^{(m)}(\delta)-H(\delta)$ decreases in $\delta\in[\epsilon,1/2]$.

2. We prove it by contradiction.

If we assume that, for some $\delta\in[\epsilon,1/2]$, it holds $u^{(m+1)}(\delta)>2\delta(1-\delta)$, then

$$\begin{aligned}\widehat{r}^{(m+1)}(\delta)&=\widehat{r}^{(m)}(u^{(m+1)}(\delta))+f(u^{(m+1)}(\delta),\delta)=\\&=\widehat{r}^{(m)}(u^{(m+1)}(\delta))-H(u^{(m+1)}(\delta))+\\&\qquad+H(u^{(m+1)}(\delta))+f(u^{(m+1)}(\delta),\delta).\end{aligned}$$

From the hypothesis it can be upper bounded as follows

$$\begin{aligned}\widehat{r}^{(m+1)}(\delta)&<\widehat{r}^{(m)}(2\delta(1-\delta))-H(2\delta(1-\delta))+\\&\qquad+H(2\delta(1-\delta))+f(2\delta(1-\delta),\delta)=\\&=\widehat{r}^{(m)}(2\delta(1-\delta))+f(2\delta(1-\delta),\delta)\end{aligned}$$

This is absurd by the definition of $\widehat{r}^{(m+1)}$.

We now prove the second part of 2). Let $\delta_1<\delta_2\in[\epsilon,1/2]$. We have

$$u^{(m+1)}(\delta_2)\in[0,2\delta_2(1-\delta_2)].$$

Since

$$\frac{\partial}{\partial\delta}f(u,\delta)=\ln\left(1-\frac{u}{2(1-\delta)}\right)-\ln\left(1-\frac{u}{2\delta}\right)$$

is continuous in $\delta\in[\epsilon,1/2]$ and $u\in[0,2\delta(1-\delta)]$, Weierstrass's theorem guarantees that $|\frac{\partial f}{\partial\delta}|$ attains its maximum $K\in\mathbb{R}$ over a closed bounded domain. By applaying Lagrange's theorem in the variable δ we have that $\exists\ \xi\in(\delta_1,\delta_2)$ such that

$$\begin{aligned}|f(u,\delta_2)-f(u,\delta_1)|&=\left|\frac{\partial f}{\partial\delta}(u,\xi)(\delta_2-\delta_1)\right|\\&=\left|\frac{\partial f}{\partial\delta}(u,\xi)\right||\delta_2-\delta_1|\leq K|\delta_2-\delta_1|\end{aligned}$$

and we conclude that $f(u,\delta)$ is Lipschitz in $\delta\in[\epsilon,1/2]$ uniformly in $u\in[0,2\delta(1-\delta)]$.

It follows that

$$\begin{aligned}\widehat{r}^{(m+1)}(\delta_2)&=\max_{0\leq u\leq 2\delta_2(1-\delta_2)}\{\widehat{r}^{(m)}(u)+f(u,\delta_2)\}\\&\leq\max_{0\leq u\leq 2\delta_1(1-\delta_1)}\{\widehat{r}^{(m)}(u)+f(u,\delta_1)\}+K|\delta_2-\delta_1|\\&=\widehat{r}^{(m+1)}(\delta_1)+K|\delta_2-\delta_1|\,.\end{aligned}$$

Similarly, we can estimate,

$$\widehat{r}^{(m+1)}(\delta_2) \geq \widehat{r}^{(m+1)}(\delta_1) - K|\delta_2 - \delta_1|$$

We conclude that

$$|\widehat{r}^{(m+1)}(\delta_2) - \widehat{r}^{(m+1)}(\delta_1)| \leq K|\delta_2 - \delta_1| \qquad \forall \delta_1, \delta_2 \in [\epsilon, 1/2].$$

Notice that the constant K only depends on f and ϵ, and not on m. □

Proof of Theorem 4.12: We first consider the case $m = 1$. Let

$$u_q^{(1)}(\delta) = \underset{u \in \Omega_\delta}{\operatorname{argmax}} [H(u)/q + f(u, \delta)].$$

If we consider the case $q = 2$, we find the analytical expression

$$u_2^{(1)}(\delta) = \frac{3 - \sqrt{9 - 32\delta(1-\delta)}}{4} \qquad \forall \delta \in [0, 1/2],$$

by which $u_2^{(1)}(\delta) \leq 2\delta(1-\delta)$ and $u_2^{(1)}(\delta) = 2\delta(1-\delta) \iff \delta = 0$ or $\delta = 1/2$.

We prove now that $\{u_q^{(1)}(\delta)\}_{q \in \mathbb{N}}$ is a decreasing sequence of functions in q. Supposing ab absurdo that $u_q^{(1)}(\delta) < u_{q+1}^{(1)}(\delta)$,

$$\begin{aligned}
\widehat{r}_q^{(1)}(\delta) &= \tfrac{H(u_q^{(1)}(\delta))}{q} + f(u_q^{(1)}(\delta), \delta) + \\
&\qquad + \tfrac{H(u_q^{(1)}(\delta))}{q+1} - \tfrac{H(u_q^{(1)}(\delta))}{q+1} \leq \\
&\leq \tfrac{H(u_q^{(1)}(\delta))}{q} - \tfrac{H(u_q^{(1)}(\delta))}{q+1} + \\
&\qquad + f(u_{q+1}^{(1)}(\delta), \delta) + \tfrac{H(u_{q+1}^{(1)}(\delta))}{q+1} \leq \\
&\leq \tfrac{H(u_{q+1}^{(1)}(\delta))}{q} - \tfrac{H(u_{q+1}^{(1)}(\delta))}{q+1} \\
&\qquad + f(u_{q+1}^{(1)}(\delta), \delta) + \tfrac{H(u_{q+1}^{(1)}(\delta))}{q+1} = \\
&= f(u_{q+1}^{(1)}(\delta), \delta) + \tfrac{H(u_{q+1}^{(1)}(\delta))}{q}
\end{aligned}$$

we get that $u_q^{(1)}(\delta) \neq \underset{u \in \Omega_\delta}{\operatorname{argmax}} [r^{(1)}(u) + f(u, \delta)]$.

So we have $u_q^{(1)}(\delta) \leq u_2^{(1)}(\delta) \leq 2\delta(1-\delta)$, $\forall q \in \mathbb{N}$.

Notice that $\widehat{r}^{(1)}(\delta)$ is differentiable and $u^{(1)}(\delta) \leq 2\delta(1-\delta)$. Applying, inductively, Lemma 4.10 for some $\epsilon \in (0, \epsilon_2)$ we obtain that $\widehat{r}^{(m)}(\delta)$ are all Lipschitz in $\delta \in [\epsilon, 1/2]$, $\forall m$. As $\widehat{r}^{(m)}(\delta)$ is symmetric respect to axis $\delta = 1/2$ and $\widehat{r}^{(m)}(\delta) = 0$ $\forall \delta \leq \epsilon$, $\widehat{r}^{(m)}(\delta)$ is Lipschitz in every point in $[0, 1]$, $\forall m$.

Notice that the Lipschitz's constant K is the same for every spectral function.

Proposition 4.11. *The sequence of functions $\{\widehat{r}^{(m)}(\delta)\}_{m \geq 1}$ is decreasing in m.*

See proof of property 1. of Theorem 4.10.

Define the sequence of points $\{\epsilon_m\}_{m \geq 1}$ such that

$$\epsilon_m = \max\{\epsilon \in [0, 1/2) : \ \widehat{r}^{(m)}(\delta) = 0 \ \forall \ \delta \leq \epsilon\}. \tag{4.32}$$

4.8.2 Strict monotonicity of ϵ_m

From Theorem 4.5 it is trivial to see that $\{\epsilon_m\}_{m\geq 1}$ is increasing in m. It can actually be shown that monotonicity is strict.

Lemma 4.11. *Let $\delta < 1/2$ and $\Gamma^{(m)}(\delta)$ the set of points such that*

$$\Gamma^{(m)}(\delta) = \operatorname*{argmax}_{0\leq u\leq 2\delta}\{\widehat{r}^{(m-1)}(u) + f(u,\delta)\}. \tag{4.33}$$

If $\tilde{u} \in \Gamma^{(m)}(\delta)$ then $\tilde{u} \leq 1/2$.

Proof. The statement is trivially proved if $\delta \leq 1/4$. Consider the case with $1/4 < \delta < 1/2$ and suppose at the contrary that $\tilde{u} \in (1/2, 2\delta]$. As $\widehat{r}^{(m-1)}(u) = \widehat{r}^{(m-1)}(1-u)$ then there exists a point $y \in [1/2-(2\delta-1/2), 1/2]$ such that

$$\widehat{r}^{(m-1)}(\tilde{u}) = \widehat{r}^{(m-1)}(y)$$

and by the fact that $f(u,\delta)$ is decreasing in u we get that

$$\widehat{r}^{(m-1)}(\tilde{u}) + f(\tilde{u},\delta) < \widehat{r}^{(m-1)}(y) + f(y,\delta)$$

and therefore $\tilde{u} \notin \Gamma^{(m)}(\delta)$, which contradicts our assumption. □

Proposition 4.12. *Let $\{\epsilon_m\}_{m\in\mathbb{N}}$ be the sequence of points such that*

$$\epsilon_m = \max\{\epsilon \in [0,1/2):\ \widehat{r}^{(m)}(\delta) = 0, \forall\delta \leq \epsilon\}.$$

The sequence is strictly increasing in $m \in \mathbb{N}$.

Proof. From Proposition 4.11 follows that $\epsilon_{m+1} \geq \epsilon_m$. We now prove by induction on m that a strictly inequality holds.

As first step, choose $m = 2$. Consider

$$G^{(1)}(u,\delta) = \frac{H(u)}{q} + f(u,\delta), \qquad u \in [0,1],\ \delta \in [0,1].$$

Differentiating the function $G^{(1)}(u,\delta)$ with respect to the variable u, we get that

$$\frac{\mathrm{d}}{\mathrm{d}u}\left(\frac{H(u)}{q}\right) = \frac{1}{q}\ln\frac{1-u}{u} \overset{u\to 0^+}{\longrightarrow} +\infty.$$

and

$$\begin{aligned}\frac{\partial}{\partial u} f(u,\delta) &= \frac{\partial}{\partial u}\left(-H(u) + (1-\delta)H\left(\frac{u}{2(1-\delta)}\right)\right.\\ &\left. + \delta H\left(\frac{u}{2\delta}\right)\right)\\ &= -\ln\left(\frac{1-u}{u}\right) + \frac{1}{2}\ln\left(\frac{2(1-\delta)-u}{u}\right)\\ &+ \frac{1}{2}\ln\left(\frac{2\delta - u}{u}\right)\\ &= \ln u - \ln(1-u) + \frac{1}{2}\ln(2(1-\delta)-u)\\ &- \frac{1}{2}\ln u + \frac{1}{2}\ln(2\delta - u) - \frac{1}{2}\ln u\\ &= -\ln(1-u) + \frac{1}{2}\ln(2(1-\delta)-u)\\ &+ \frac{1}{2}\ln(2\delta - u)\\ &= \frac{1}{2}\ln\frac{(2(1-\delta)-u)(2\delta-u)}{(1-u)^2}\\ &= \frac{1}{2}\ln\frac{4\delta(1-\delta) - 2u + u^2}{(1-u)^2} \qquad (4.34)\end{aligned}$$

from which we have

$$\begin{aligned}\frac{\partial}{\partial u} f(u,\delta)\Big|_{u=0} &= \frac{1}{2}\ln(2\delta) + \frac{1}{2}\ln[2(1-\delta)]\\ &= \frac{1}{2}\ln\left(4\delta(1-\delta)\right) \le 0 \qquad \forall\delta\in(0,1).\end{aligned}$$

As $G^{(1)}(0,\delta) = 0$ and there exists ϵ_δ such that

$$\frac{\partial}{\partial u} G^{(1)}(u,\delta) > 0,\ \forall u \in (0,\epsilon_\delta)$$

then $G^{(1)}(u,\delta) > 0,\ \forall\delta$ and for u sufficiently small. From the recursive expression in (4.11) we conclude that

$$\begin{aligned}\widehat{r}^{(1)}(\delta) &= \max_{0\le u\le 1}\{\widehat{r}^{(0)}(u) + f(u,\delta)\}\\ &= \max_{0\le u\le 1}\{G^{(1)}(u,\delta)\} > 0, \quad \forall\delta\in(0,1).\end{aligned}$$

From Theorem 4.5 it is proved that $\epsilon_2 > 0 = \epsilon_1$.

For the inductive step, assume the statement is true for m, namely $\epsilon_m > \epsilon_{m-1}$.

Let $\Gamma^{(m+1)}(\delta)$ be the set of points defined in (4.33) and we prove preliminarily that $\Gamma^{(m+1)}(\epsilon_m) = \{0\}$. From Lemma 4.11, we have that if $u^{(m+1)} \in$

$\Gamma^{(m+1)}(\epsilon_m)$ then $u^{(m+1)} < \frac{1}{2} \wedge 2\epsilon_m$. Suppose at the contrary that $u^{(m+1)} \in (\epsilon_{m-1}, 1/2 \wedge 2\epsilon_m]$ then

$$0 = \widehat{r}^{(m+1)}(\epsilon_m) = \widehat{r}^{(m)}(u^{(m+1)}) + f(u^{(m+1)}, \epsilon_m) = 0$$

From Proposition 1 and from the inductive hypothesis we get

$$\begin{aligned} 0 = \widehat{r}^{(m+1)}(\epsilon_m) &< \widehat{r}^{(m-1)}(u^{(m+1)}) + f(u^{(m+1)}, \epsilon_m) \\ &\leq \max_{0 \leq u \leq 2\epsilon_m} \widehat{r}^{(m-1)}(u) + f(u, \epsilon_m) = \widehat{r}^{(m)}(\epsilon_m) \end{aligned}$$

then

$$\epsilon_m \neq \max\{\epsilon \in [0, 1/2) : \ \widehat{r}^{(m)}(\delta) = 0, \forall \delta \leq \epsilon\}.$$

which contradicts the definition of ϵ_m.

As $\widehat{r}^{(m)}(u) = 0$, for every $u \in [0, \epsilon_m]$ and the function $f(u, \epsilon_m)$ is decreasing in $u \in [0, \epsilon_{m-1}]$ then $\Gamma^{(m+1)}(\epsilon_m) = \{0\}$. We conclude that there exists $\eta > 0$ for which

$$\widehat{r}^{(m)}(u) + f(u, \epsilon_m) \leq -\eta \quad \forall u \in (\epsilon_{m-1}, 2\epsilon_m].$$

Using the fact that $\widehat{r}^{(m)}$ and f are both continuous and $f(u, \delta)$ is strictly increasing in $\delta < 1/2$, by the way ϵ_m has been defined (4.13), we get that there exists $\epsilon' > 0$ such that

$$\widehat{r}^{(m)}(u) + f(u, \epsilon_m + \epsilon') \leq 0 \quad \forall u \in (\epsilon_{m-1}, 2(\epsilon_m + \epsilon')]$$

and the statement is proved also for $m + 1$. □

4.8.3 Analytical bounds

The next results provide, respectively, a lower bound and an upper bound on the thresholds ϵ_m.

Proposition 4.13. *If $\widehat{r}^{(m-1)}(\delta) \leq c\delta$ with $c \in \mathbb{R}$ then $\widehat{r}^{(m)}(\delta) = 0$, $\forall \delta \leq \frac{1}{2}(1 - \sqrt{1 - \mathrm{e}^{-2c}})$.*

Proof.

$$\begin{aligned} \widehat{r}^{(m)}(\delta) &= \max_{u \in \Omega_\delta} \{\widehat{r}^{(m-1)}(u) + f(u, \delta)\} \\ &\leq \max_{u \in \Omega_\delta} \{cu + f(u, \delta)\} \end{aligned}$$

As $\frac{\partial^2}{\partial u^2} f(u, \delta) \leq 0$, $\forall \delta$, $u \in \Omega_\delta$ then for any fixed δ the maximizing value $\tilde{u}$ is unique:

$$\tilde{u}(\delta) = 1 - \frac{1 - 2\delta}{\sqrt{1 - \mathrm{e}^{-2c}}} \in \Omega_\delta \iff \delta \leq \frac{1}{2}(1 - \sqrt{1 - \mathrm{e}^{-2c}}).$$

It can be easily verified that

$$c\tilde{u}(\delta) + f\left(\tilde{u}(\delta), \delta\right) \leq 0 \qquad \forall \delta \leq \frac{1}{2}(1 - \sqrt{1 - \mathrm{e}^{-2c}}).$$

The statement is proved, by using the fact that $\widehat{r}^{(m)}(\delta) \geq 0$. □

Proposition 4.14.

$$\widehat{r}^{(1)}(\delta) \leq \frac{1}{q}\ln\left[1+\left(2\sqrt{\delta(1-\delta)}\right)^q\right]$$

Proof. From the expression in (4.26) we have

$$\begin{aligned}
f(u,\delta) &= -H(u)+(1-\delta)H\left(\frac{u}{2(1-\delta)}\right)+\delta H\left(\frac{u}{2\delta}\right)\\
&= u\ln u+(1-u)\ln(1-u)\\
&+(1-\delta)\left[-\frac{u}{2(1-\delta)}\ln\left(\frac{u}{2(1-\delta)}\right)\right.\\
&\left.-\left(1-\frac{u}{2(1-\delta)}\right)\ln\left(1-\frac{u}{2(1-\delta)}\right)\right]\\
&+\delta\left[-\frac{u}{2\delta}\ln\left(\frac{u}{2\delta}\right)-\left(1-\frac{u}{2\delta}\right)\ln\left(1-\frac{u}{2\delta}\right)\right]\\
&= u\ln u+(1-u)\ln(1-u)-\frac{u}{2}\ln\left(\frac{u}{2(1-\delta)}\right)\\
&-\frac{2(1-\delta)-u}{2}\ln\left(\frac{2(1-\delta)-u}{2(1-\delta)}\right)\\
&-\frac{u}{2}\ln\left(\frac{u}{2\delta}\right)-\frac{2\delta-u}{2}\ln\left(\frac{2\delta-u}{2\delta}\right)\\
&= u\ln u+(1-u)\ln(1-u)-\frac{u}{2}\ln u+\frac{u}{2}\ln\left(2(1-\delta)\right)\\
&-\frac{2-2\delta-u}{2}\ln\left(\frac{2-2\delta-u}{2(1-\delta)}\right)-\frac{u}{2}\ln u+\frac{u}{2}\ln(2\delta)\\
&-\frac{2\delta-u}{2}\ln\left(\frac{2\delta-u}{2\delta}\right)\\
&= u\ln\left(2\sqrt{\delta(1-\delta)}\right)+(1-u)\ln(1-u) \qquad (4.35)\\
&-\frac{2\delta-u}{2}\ln\left(\frac{2\delta-u}{2\delta}\right)-\frac{2-2\delta-u}{2}\ln\left(\frac{2-2\delta-u}{2-2\delta}\right).
\end{aligned}$$

Jensen's inequality and the fact that $g(u)=u\ln u$ is strictly convex imply that

$$\begin{aligned}
(1-u)\ln(1-u) &= g(1-u)\\
&= g\left(\frac{2\delta-u}{2\delta}\delta+\frac{2-2\delta-u}{2(1-\delta)}(1-\delta)\right)\\
&\leq \delta g\left(\frac{2\delta-u}{2\delta}\right)+(1-\delta)g\left(\frac{2-2\delta-u}{2(1-\delta)}\right)\\
&= \frac{2\delta-u}{2}\ln\left(\frac{2\delta-u}{2\delta}\right)\\
&+\frac{2-2\delta-u}{2}\ln\left(\frac{2-2\delta-u}{2(1-\delta)}\right)
\end{aligned}$$

from which it follows that

$$f(u,\delta) \le u \ln\left(2\sqrt{\delta(1-\delta)}\right) \tag{4.36}$$

and equality holds if and only if $u = 0$ or $\delta = 1/2$.

By (4.36) we get that

$$\begin{aligned}
\widehat{r}^{(1)}(\delta) &= \max_{0\le u\le 1} \{\widehat{r}^{(0)}(u) + f(u,\delta)\} \\
&= \max_{0\le u\le 1} \left\{\frac{H(u)}{q} + f(u,\delta)\right\} \\
&\le \max_{0\le u\le 1} \left\{\frac{H(u)}{q} + u\ln\left(2\sqrt{\delta(1-\delta)}\right)\right\} \\
&= \max_{0\le u\le 1} \left\{\frac{H(u)}{q} + \frac{u}{q}\ln\left(2\sqrt{\delta(1-\delta)}\right)^q\right\}. \qquad (4.37)
\end{aligned}$$

Differentiating this expression with respect to the variable u

$$\begin{aligned}
&\frac{\mathrm{d}}{\mathrm{d}u}\left\{\frac{H(u)}{q} + \frac{u}{q}\ln\left(2\sqrt{\delta(1-\delta)}\right)^q\right\} \\
&\quad = \frac{1}{q}\ln\left(\frac{1-u}{u}\right) + \frac{1}{q}\ln\left(2\sqrt{\delta(1-\delta)}\right)^q = 0
\end{aligned}$$

we get

$$\frac{1-u}{u} = \frac{1}{\left(2\sqrt{\delta(1-\delta)}\right)^q}$$

from which the optimizing value in the computation is

$$u = \frac{1}{1+\frac{1}{\left(2\sqrt{\delta(1-\delta)}\right)^q}} = \frac{\left(2\sqrt{\delta(1-\delta)}\right)^q}{1+\left(2\sqrt{\delta(1-\delta)}\right)^q}.$$

Substituting it in the right-hand side of (4.37) gives

$$\begin{aligned}
\widehat{r}^{(1)}(\delta) \leq{} & \frac{1}{q} H \left(\frac{\left(2\sqrt{\delta(1-\delta)}\right)^q}{1+\left(2\sqrt{\delta(1-\delta)}\right)^q} \right) \\
& + \frac{1}{q} \frac{\left(2\sqrt{\delta(1-\delta)}\right)^q}{1+\left(2\sqrt{\delta(1-\delta)}\right)^q} \ln \left(2\sqrt{\delta(1-\delta)}\right)^q \\
={} & -\frac{1}{q} \frac{\left(2\sqrt{\delta(1-\delta)}\right)^q}{1+\left(2\sqrt{\delta(1-\delta)}\right)^q} \ln \left(\frac{\left(2\sqrt{\delta(1-\delta)}\right)^q}{1+\left(2\sqrt{\delta(1-\delta)}\right)^q} \right) \\
& - \frac{1}{q} \frac{1}{1+\left(2\sqrt{\delta(1-\delta)}\right)^q} \ln \left(\frac{1}{1+\left(2\sqrt{\delta(1-\delta)}\right)^q} \right) \\
& + \frac{1}{q} \frac{\left(2\sqrt{\delta(1-\delta)}\right)^q}{1+\left(2\sqrt{\delta(1-\delta)}\right)^q} \ln \left(2\sqrt{\delta(1-\delta)}\right)^q \\
={} & \frac{1}{q} \frac{\left(2\sqrt{\delta(1-\delta)}\right)^q}{1+\left(2\sqrt{\delta(1-\delta)}\right)^q} \ln \left(1+\left(2\sqrt{\delta(1-\delta)}\right)^q\right) \\
& + \frac{1}{q} \frac{\ln \left(1+\left(2\sqrt{\delta(1-\delta)}\right)^q\right)}{1+\left(2\sqrt{\delta(1-\delta)}\right)^q} \\
={} & \frac{1}{q} \ln \left[1+\left(2\sqrt{\delta(1-\delta)}\right)^q\right]
\end{aligned}$$

□

Corollary 4.5. $\widehat{r}^{(m)}(\delta) = 0 \ \forall \delta \leq \frac{1}{2}(1-\sqrt{1-\mathrm{e}^{-4}}), m \geq 2.$

Proof. Consider the case with $m = 2$ and $q = 2$. From Proposition (4.14) and by the fact that $\{R_q(\delta)\}_{q\in\mathbb{N}}$ form a non-increasing sequence of functions in q, we have that

$$\widehat{r}^{(1)}(\delta) \leq R_2(\delta) = \frac{1}{2} \ln \left[1+4\delta(1-\delta)\right] \leq 2\delta \qquad \forall \delta.$$

From Proposition 4.13 we get that

$$\widehat{r}^{(2)}(\delta) = 0 \qquad \forall \delta \leq \frac{1}{2}(1-\sqrt{1-\mathrm{e}^{-4}}).$$

The statement also holds for $m > 2$ from Proposition 4.11.

□

4.9 Concluding remarks

In this chapter we have studied some properties of the spectral functions for uniformly interleaved serially concatenated codes and their relation to the minimum distance growth rate. In particular we have shown that for $m \geq 2$, the asymptotic spectral functions exhibit some different features as compared to the case where $m = 1$. The main difference is that for $m \geq 2$ there exists a positive point δ_m such that the function is zero below it and positive beyond it. Moreover, by tracking the evolution of the asymptotic spectral functions, we have shown that these functions converge uniformly, when m tends to infinity, to that of random linear code ensemble for $\delta \in [\delta_{GV}, 1 - \delta_{GV}]$.

Although the floor of the spectral functions is zero, by combining the asymptotic spectral functions with the use of the union bound we have proved that the mutilple-serial coding ensemble is asymptotically good, in the sense that the typical minimum distance grows linearly in N with probability one. Moreover we have provided a numerical method to estimate with arbitrarily small accuracy the linear growth rate: except for the case of $d_f^o = 2$ and $m = 2$, we have proved that the growth rate is at least δ_m. This implies that the normalized minimum distance increases monotonically with m and meets the limit implied by the Gilbert-Varshamov bound on the minimum distance when m tends to infinity. Notice that the minimum distance ratios computed using this method are quite close to the empirical growth rates listed in [44].

Theoretically, our mathematical tools provide a new general framework for estimating the minimum distance distribution of multiple serially concatenated codes.

This chapter leaves some open problems to study:

- How fast the sequence of the spectral functions converges to the limit function?

- What is the effect of the inner encoders of the encoding scheme on this convergence?

The results presented in this chapter are very encouraging and suggest that even a few number of inner encoders are sufficient to approach the asymptotic behavior. Since for Repeat mutiple-convolute codes the sequence of threshold δ_m is strictly increasing, then this convergence should not be in finite time for general cases.

Moreover the dynamical system we have defined depends exclusively on the inner encoder and it would be different if we replace it with another convolutional encoder. The numerical results and the fact that Theorem 4.7 hold for any choice of the convolutional encoder (as long it was not the identity) lead us to conjecture that the dynamical systems analysis is likely to hold true for all convolutional encoders both recursive and not recursive.

Instead for the final part on the estimation of distances, the role of recursivity must necessarily come up since, if it is not recursive can not certainly exhibit linear growth of minimum distances. Indeed, it is easy to verify that for any nonrecursive rate-1 convolutional encoder with an impulse response of weight d the output weight will be at most d times the input weight. If the desired output weight is γN and the input weight is 1, then the minimum numbers of concatenations needed is $\log_d \gamma N$. We conclude that, for fixed m and asymptotically large N, the convolutional encoder never maps an input word of weight 1 to an output word of weight γN and we expect that the ensemble has low weight codewords.

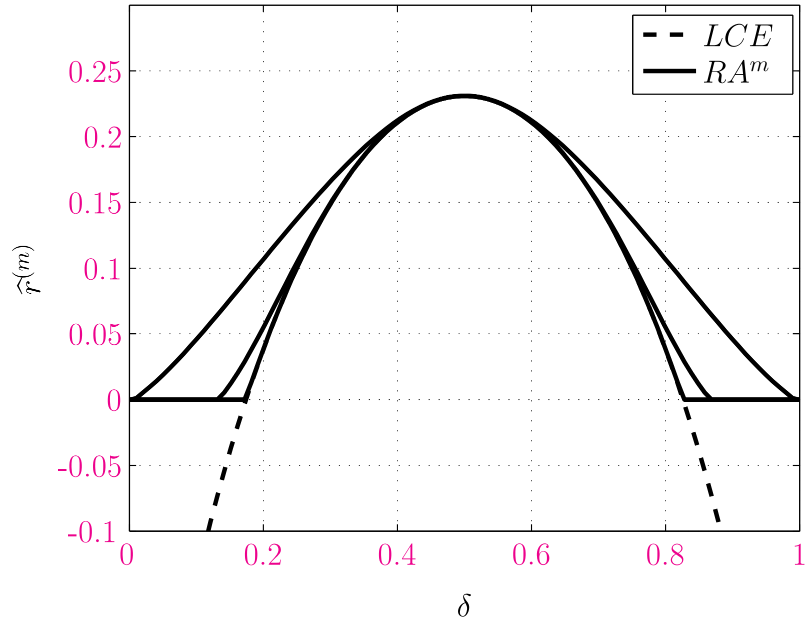


Figure 4.2: Asymptotic spectral functions for ensembles of RA^m with $m = 1, 2, 3$ (from top to bottom) and comparison to that of random linear coding ensemble (LCE).

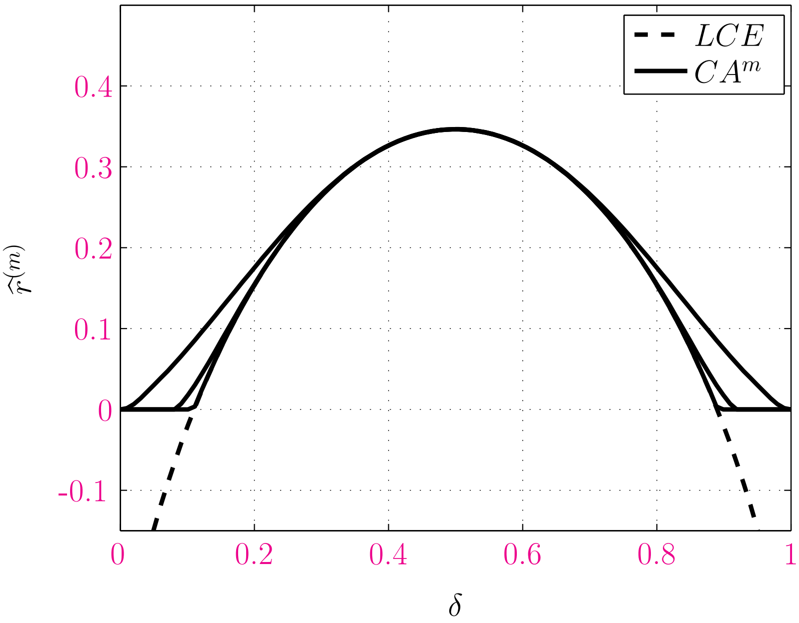


Figure 4.3: Asymptotic spectral functions corresponding to the ensembles of CA^m with $m = 1, 2, 3$ (from top to bottom) and outer convolutional encoder $G_1(D) = [1, 1 + D]$ (thick lines) and comparison to that of linear coding ensemble (dashed line).

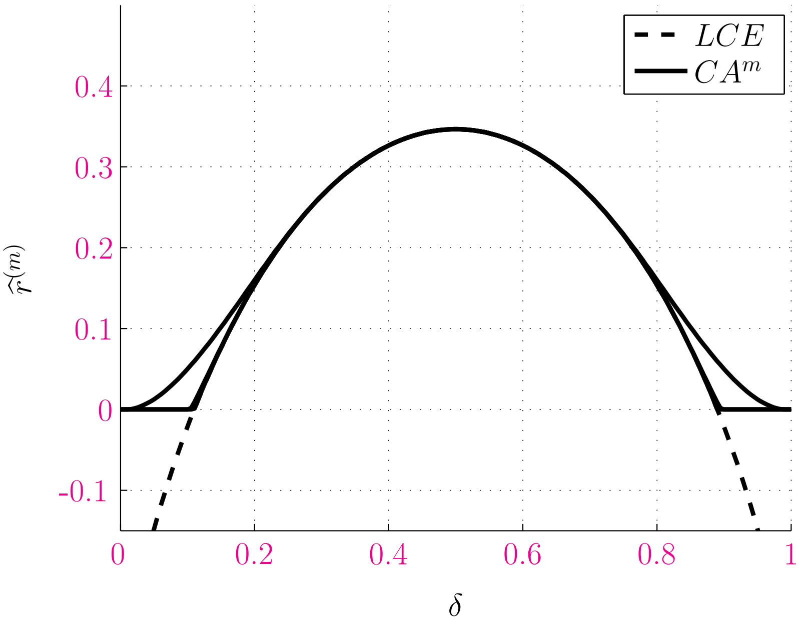


Figure 4.4: Asymptotic spectral functions corresponding to the ensembles of CA^m with $m = 1, 2, 3$ (from top to bottom) and outer convolutional encoder $G_2(D) = [1 + D^2, 1 + D + D^2]$ (thick lines) and comparison to that of linear coding ensemble (dashed line).

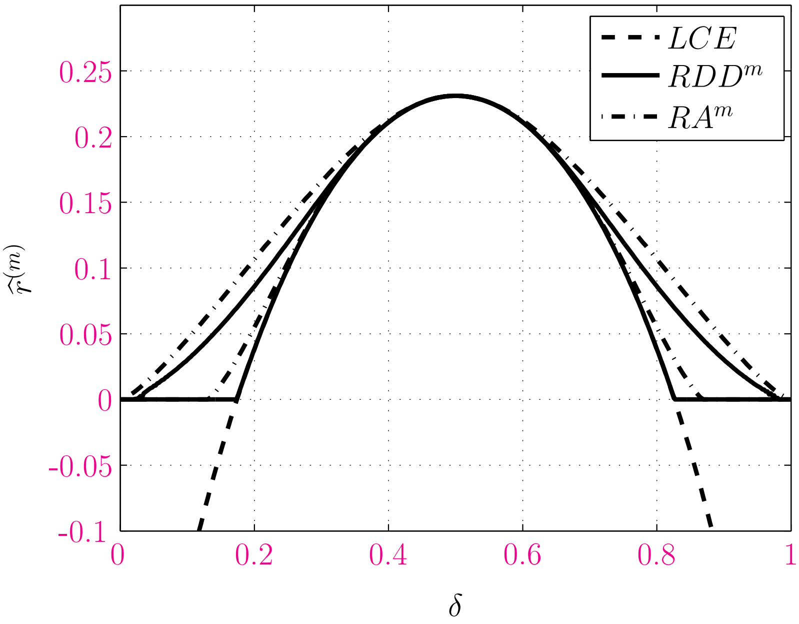


Figure 4.5: Asymptotic spectral functions of RDD^m with $m = 1, 2$ (thick lines from top to bottom) and comparison to those of RA^m (dashed-dot lines) and linear coding ensemble (dashed line).

Irregular Repeat-Convolute codes

5

Brief—This chapter deals with a family of codes that generalize Repeat-Convolute codes, and can be seen both as particular systematic serial turbo codes and as structured LDPC codes. Their minimum distance distribution is studied. First, we prove that deterministically the minimum distance cannot grow linearly. Inspired by the the tail estimations of [36], we identify parameters allowing the typical minimum distance to grow sub-linearly in the codewords length with high probability.

5.1 Introduction and outline of the chapter

In this chapter, we develop the study of Irregular Repeat-Convolute codes, a family of codes which are a generalization of Repeat-Convolute codes, and which can be seen both as serial turbo schemes and as structured Low Density Parity Check (LDPC) codes.

We recall that one of the main problems of Low Density Parity Check (LDPC) codes is their encoding complexity, which is generally quadratic in the block length, as the generating matrix is not sparse. Constraining the parity check matrix to have a particular structure can a priori guarantee easy encoding. A successful construction uses matrices with a staircase part (i.e. a sub-matrix with ones on the diagonal and on the lower diagonal, and zeros everywhere else), so that the encoder can be seen as the serial concatenation of a repetition code, an interleaver and an accumulator. They are known as Repeat-Accumulate (RA) [23] codes or, if repetition is not uniform, Irregular Repeat-Accumulate (IRA) codes [22].

There is a huge literature on the analysis and design of IRA codes (we refer to [77] and references therein). In [78] the possibility to vary the structured part of the parity matrix is investigated. This is equivalent to choosing an inner encoder different from the accumulator.

Theoretical results in [78] enlighten the effect of the choice of the inner encoder on the performances under maximum-likelihood (ML) decoding assumption.

Here, we focus on minimum distance distribution and we follow the approach to study these codes as a serial turbo structure. First, we prove that deterministically the minimum distance cannot grow linearly, using deterministic upper bounding techniques devised in [37]. Inspired by the the tail estimations of [36], we identify parameters allowing the typical minimum distance to grow sub-linearly in the codewords length with high probability.

The remainder of the chapter is organized as follows. Section 5.2 is devoted to the description of the coding scheme. Section 5.3 presents, in a formal way, all the original contributions presented in this chapter. Sections 5.4, 5.5, 5.6 are technical sections whose results are proved in details. Finally, Section 5.7 containing concluding remarks completes the chapter.

5.2 Ensemble description

We consider the ensemble of Irregular-Repeat Convolute codes (IRC codes), obtained by the serial concatenation of an irregular Low Density Generator Matrix (LDGM) code with an arbitrary rate-1 convolutional encoder.

These codes are defined as follows.

- Let $(u_1, \ldots, u_N)$ be a sequence of N information bits. These bits form the systematic part of the codeword.

- To generate the parity part, repeat the i-th bit q_i times, where $(q_1, \ldots, q_N)$ is a sequence of integers such that $q_{\min} \le q_i \le q_{\max}$.

- Order this sequence according to a permutation π. Then group this sequence in M irregular blocks of size $(s_1, \ldots, s_M)$ with $s_{\min} \le s_i \le s_{\max}$ and take the modulo-2 sum of every block. These give the check bits.

- Finally, the sequence emerging form the LDGM code is then encoded using a rate-1 recursive convolutional encoder $\phi^{\text{in}}(D) \in \mathbb{Z}_2(D)$.

These coding schemes use all bits (systematic part and parity part) as its codeword and we have rate $R = N/(N + M)$.

LDGM code can be represented as a bipartite graph $\mathcal{G} = (\mathcal{I} \cup \mathcal{J}, \mathcal{E})$ where $\mathcal{I} = \{1, \ldots, N\}, \mathcal{J} = \{1, \ldots, M\}$ and $(i, j) \in \mathcal{E}$ if the i-th information bit is involved in the determination of the j-th parity bit. Figure 5.1 shows this graphical representation.

It is convenient to introduce the following notation. Let Q_i (respectively S_j) be the fraction of information (check) bits that are connected to i check (j information) bits. The following polynomials with non-negative coefficients

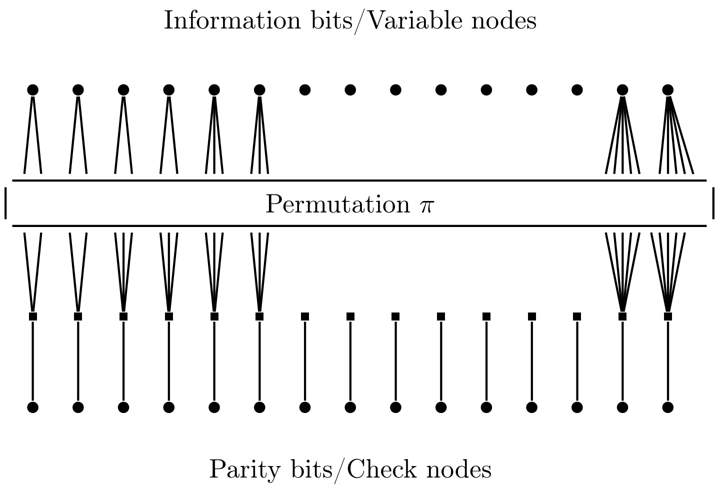


Figure 5.1: Graphical representation of LDGM code

are used to specify the ensembles of IRC codes

$$Q(x) = \sum_{i=q_{\min}}^{q_{\max}} Q_i x^i \qquad S(x) = \sum_{j=s_{\min}}^{s_{\max}} S_j x^j.$$

We denote

$$\begin{aligned} q_{\min} &= \operatorname{ldeg}[Q(x)] & q_{\max} &= \deg[Q(x)] \\ s_{\min} &= \operatorname{ldeg}[S(x)] & s_{\max} &= \deg[S(x)]. \end{aligned}$$

Notice that the total number of edges between information and parity nodes are equal to $\overline{q}N = \overline{s}M$ where $\overline{q} = \sum_i iQ_i$ and $\overline{s} = \sum_j jS_j$.

We can interpret the overall coding scheme as the following map composition (see Fig. 5.2)

$$\psi_N : \boldsymbol{u} \mapsto (\boldsymbol{u}, \phi_M^{\text{in}} \circ \text{Sum}_M^S \circ \pi \circ \text{Rep}_N^Q(\boldsymbol{u}))$$

where

- $\mathrm{Rep}_N^Q : \mathbb{Z}_2^N \to \mathbb{Z}_2^{\overline{q}N}$ is the irregular repetition encoder

$$\mathrm{Rep}_N^Q([u_1,\dots,u_N]) = (\underbrace{u_1,\dots,u_1}_{q_1 \text{ times}},\underbrace{u_2,\dots,u_2}_{q_2 \text{ times}},\dots,\underbrace{u_N,\dots,u_N}_{q_N \text{ times}})$$

- π is a random permutation in the group of permutation on $\overline{q}N$ elements $S_{\overline{q}N}$.
- the $\mathrm{Sum}_M^S : \mathbb{Z}_2^{\overline{q}N} \to \mathbb{Z}_2^M$ is the irregular summator

$$\mathrm{Sum}_M^S([x_1,x_2,\dots,x_{\overline{q}N}]) = \left(\sum_{i=1}^{s_1} x_i, \sum_{i=s_1+1}^{s_1+s_2} x_i, \dots, \sum_{i=\sum_{l=1}^{M-1} s_l+1}^{\sum_{l=1}^{M} s_l} x_i\right)$$

- $\phi^{\mathrm{in}}(D) : \mathbb{Z}_2((D)) \to \mathbb{Z}_2((D))$ is a rate-1 scalar non-catastrophic and recursive convolutional encoder, and $\phi_M : \mathbb{Z}_2^M \to \mathbb{Z}_2^M$ is the block encoder obtained by truncating the trellis at depth M.

We denote with $\mathcal{C}_N = \mathrm{Im}(\psi_N)$ the associated code.

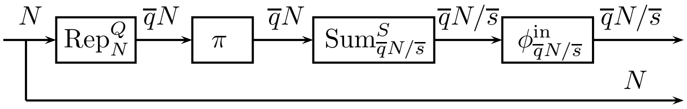

N
Rep_N^Q
$\overline{q}N$
π
$\overline{q}N$
$\mathrm{Sum}_{\overline{q}N/\overline{s}}^S$
$\overline{q}N/\overline{s}$
$\phi_{\overline{q}N/\overline{s}}^{\mathrm{in}}$
$\overline{q}N/\overline{s}$
N

Figure 5.2: Coding scheme: Irregular-repeat convolute codes.

This scheme generalizes Repeat convolute encoders, which are the particular case when $s_{\max} = 1$. The LDGM encoder $\phi_N^{\mathrm{out}} = \mathrm{Sum}_M^S \circ \pi \circ \mathrm{Rep}_N^Q$ can be considered as the truncation of a proper convolutional encoder, which is not injective, but the systematic branch guarantees injectivity and non-catastrophicity of the overall coding scheme.

Irregular Repeat-Accumulate (IRA), introduced in [22], are obtained by fixing the inner encoder to be the accumulator. The choice to have scalar inner encoder (as in the previous chapter) does not affect our analysis.

These codes can be seen be seen also as LDPC codes: a parity check matrix can be constructed in the following way. Notice that a pair $(\boldsymbol{u},\boldsymbol{x}) \in \mathbb{Z}_2^N \times \mathbb{Z}_2^{\overline{q}N/\overline{s}}$ belongs to $\mathcal{C}_N$ if and only if

$$\mathrm{Sum}_M^S \circ \pi \circ \mathrm{Rep}_N^Q(\boldsymbol{u}) + \phi_M^{-1}(\boldsymbol{x}) = \mathbf{0}$$

and can be represented with parity check matrices of the type $[\mathbf{H}_N, \mathbf{K}_N]$, where $\mathbf{H}_N$ is a sparse matrix with at most $s_{\max}$ 1's per row and $q_{\max}$ 1's per column, while $\mathbf{K}_N$ is a matrix depending on the inner encoder $\phi^{\text{in}}(D)$. Notice that also $\mathbf{K}_N$ is a low density matrix with a number of 1's depending on the degree of $[\phi^{\text{in}}(D)]^{-1}$. For example if $\phi^{\text{in}}(D) = \frac{1}{(1+D)}$ we obtain the staircase LDPC codes: $\mathbf{K}_N$ has 1's on the diagonal and on the lower diagonal, and zeros elsewhere:

$$\mathbf{K}_N = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & \dots \\ 1 & 1 & 0 & 0 & 0 & 0 & \dots \\ 0 & 1 & 1 & 0 & 0 & 0 & \dots \\ 0 & 0 & 1 & 1 & 0 & 0 & \dots \\ 0 & 0 & 0 & 1 & 1 & 0 & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \end{bmatrix}$$

If ϕ is the scalar encoder $\phi(D) = \frac{1}{1+D+D^3}$ the block matrix $\mathbf{K}_N$ is given by:

$$\mathbf{K}_N = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & \dots \\ 1 & 1 & 0 & 0 & 0 & 0 & \dots \\ 0 & 1 & 1 & 0 & 0 & 0 & \dots \\ 1 & 0 & 1 & 1 & 0 & 0 & \dots \\ 0 & 1 & 0 & 1 & 1 & 0 & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \end{bmatrix}$$

5.3 Main contribution

The behavior of the minimum distance for these type of codes is not yet completely understood. Regarding the case of IRA code ensembles (which is a particular case of our setting) the results are not precise. By viewing some similarity with LDPC codes, Di et al. assert that if $q_{\min} \geq 3$ for all but most a fraction $O(N^{-1})$ of codes in these ensembles minimum distances scale linearly in the code length (see Theorem 23 in [42]).

In this chapter, by viewing IRA codes as serial turbo codes we prove the contrary: deterministically (i.e. for any given permutation π) the minimum distance cannot grow linearly. We can extend the proof also for generic inner encoders with the additional assumption to have a regular summator.

Theorem 5.1. *Suppose one of the following conditions are satisfied:*

- $\phi^{\text{in}}(D) = (1+D)^{-1}$
- $S(x) = x^s$

then there exist constants $C_1, C_2, N_0 \in \mathbb{N}$ such that for all $N \geq N_0$ the following inequality is true

$$d_{\min}(\psi_N) \leq C_1 N^{\beta} \ln(N) + C_2 \ln N$$

with $\beta = 1 - 1/\lceil q_{\min}/2 \rceil$.

As a second step we derive the average weight enumerators of structured LDPC codes, which are used to study minimum distance distribution. In particular, we get that minimum distance grows at least sub-linearly in N, with probability approaching one as N goes to infinity. We formally have the following theorem.

Theorem 5.2. *Let $d = o(N^{\beta})$ for $N \to \infty$ with $\beta = 1 - 2/q_{\min}$. If $q_{\min} \geq 3$ then*

$$\mathbb{P}\left(d_{\min}(\psi_N) < d\right) \overset{N\to\infty}{\longrightarrow} 0.$$

5.4 Deterministic upper bound

We now prove that the ensemble of IRC codes has minimum distance growing at most like $O\left(N^{1-\frac{1}{\lceil q_{\min}/2\rceil}}\right)$.

Before starting, we recall some notation and properties of recursive convolutional encoders.

Definition 5.1. *Let d_{e} be the effective free distance of the recursive convolutional encoder $\phi(D)$, namely the minimum Hamming weight among its codewords corresponding to input weight 2:*

$$d_{\mathrm{e}}(\phi) := \min\{\mathrm{w_H}(\phi(\boldsymbol{u})) = 2\}$$

Our proof will make use of the following fact.

Lemma 5.1. *Suppose one of the following conditions are satisfied:*

- $\phi^{\mathrm{in}}(D) = (1+D)^{-1}$
- $S(x) = x^s$.

There exists a constant $\overline{\zeta} \in \mathbb{N}$ such that

$$\mathrm{w_H}\left(\phi^{\mathrm{in}}\left(\mathrm{Sum}_M^S\left([\ldots 010^{a\overline{\zeta}-1}10\ldots]\right)\right)\right) \leq a d_e(\phi^{\mathrm{in}}).$$

Proof. 1. If $\phi^{\mathrm{in}}(D) = (1+D)^{-1}$ we have $d_{\mathrm{e}} = 1$ and $\mathrm{w_H}(\phi^{\mathrm{in}}(1+D^a)) = a$, for every $a \in \mathbb{N}$ (see trellis transitions in Section 3.4). The assertion is proved with $\overline{\zeta} = 1$. To see this fact, suppose a sequence of the form $\ldots 010^{a-1}10\ldots$ is fed in the summator. We distinguish two cases:

- if the pair of 1's falls in the same group of summation, then the output weight is clearly zero
- if the two 1's fall in different blocks then the sequence entering in the accumulate encoder is of the form $\ldots 010^{b-1}10\ldots$ with $b \leq a$. We conclude that the sequence emerging from the accumulate encoder has weight not greater than a.

2. As $\phi^{\text{in}}(D)$ is recursive with scalar input, there exists $t \in \mathbb{N}$ such that $\mathrm{w_H}(\phi^{\text{in}}(1+D^t))$ (see Lemma 1 in [37]). Let $\bar{t} = \min\{t \in \mathbb{N} : \mathrm{w_H}(\phi(1+D^t)) < \infty\}$ then $\mathrm{w_H}(\phi^{\text{in}}(1+D^t)) < \infty$ if and only if $t = j\bar{t}, j \in \mathbb{N}$. Notice that the inner encoder is also proper $\phi^{\text{in}}(D) = \frac{p(D)}{q(D)}$ with $\deg[p] < \deg[q]$, then $\mathrm{w_H}(\phi^{\text{in}}(1+D^{j\bar{t}})) = j\mathrm{w_H}(\phi^{\text{in}}(1+D^{\bar{t}}))$. To make sure that this is true, consider

$$(1+D^{j\bar{t}})\frac{p(D)}{q(D)} = \sum_{r=0}^{j-1} D^{r\bar{t}}(1+D^{\bar{t}})\frac{p(D)}{q(D)}.$$

As $\deg[p] < \deg[q]$, the error events $D^{r\bar{t}}(1+D^{\bar{t}})\frac{p(D)}{q(D)}$ have disjoint supports so that $\mathrm{w_H}\left(\sum_{r=0}^{j-1} D^{r\bar{t}}(1+D^{\bar{t}})\frac{p(D)}{q(D)}\right)$ is the sum of the individual weights of the j error events, which are all equal to $\mathrm{w_H}\left(\phi^{\text{in}}(1+D^{\bar{t}})\right) = d_{\text{e}}$.

If the summator is regular with grouping factor equal to s then the assertion is proved with $\bar{\zeta} = s\bar{t}$. In particular, we have

$$\begin{aligned}
&\mathrm{w_H}\left(\phi^{\text{in}}\left(\mathrm{Sum}_M^S\left([\ldots 010^{a\bar{\zeta}-1}10\ldots]\right)\right)\right) = \\
&\quad = \mathrm{w_H}\left(\phi^{\text{in}}\left(\mathrm{Sum}_M^S\left([\ldots 010^{as\bar{t}-1}10\ldots]\right)\right)\right) \\
&\quad = \mathrm{w_H}\left(\phi^{\text{in}}\left([\ldots 010^{a\bar{t}-1}10\ldots]\right)\right) = ad_{\text{e}}.
\end{aligned}$$

□

Definition 5.2. *A hypergraph $\mathcal{H}$ is a pair $\mathcal{H} = (\mathcal{V}, \mathcal{E})$ where $\mathcal{V}$ is a set of elements, called nodes or vertices, and $\mathcal{E}$ is a set of non-empty subsets of $\mathcal{V}$ called hyperedges or links. A q-uniform hypergraph is a hypergraph such that all its hyperedges have size q.*

Definition 5.3. *The degree of a vertex in a hypergraph is the number of hyperedges that contain that vertex.*

Lemma 5.2. *[Lemma 3 in [37]] If $\mathcal{H} = (\mathcal{V}, \mathcal{E})$ is q-partite, q-uniform with b vertices in each part and $4b^{\lceil q/2 \rceil} \leq |\mathcal{E}|$ then there exists a non-empty subset $\mathcal{S} \subset \mathcal{E}$ such that $1 \leq |\mathcal{S}| \leq 2q \ln b$ and every vertex has even degree in the induced subgraph $(\mathcal{V}, \mathcal{S})$.*

Proof of Theorem 5.2. The key idea, first introduced in [37], consists in finding, for any interleaver, a suitable subset of sequences, such that the corresponding output has a small weight. We describe here the construction adapting the procedure from [37] to our setting.

Let $\bar{\zeta}$ be the number defined in Lemma 5.1 and $Q_{\min} = Q_{q_{\min}}$ be the fraction of information nodes with repetition parameter $q_{\min}$. To construct a suitable input sequence, we first note that every bit of the input $\boldsymbol{u}$ corresponding to information nodes with repetition parameter $q_{\min}$ appears exactly $q_{\min}$ times in the string $\pi\left(\mathrm{Rep}_N^Q(\boldsymbol{u})\right)$. For every $i \in \{1, \dots, Q_{\min}N\}$ and every index $j \in \{1, \dots, q_{\min}\}$ we set $\tau_j(i)$ with the position (after the permutation) of the j-th copy of the i-th input bit and $\sigma_j(i) = \tau_j(i) \bmod \overline{\zeta}$. Since there are at most $\overline{\zeta}^{q_{\min}}$ such possible sequences and $Q_{\min}N$ input bits, by the pigeonhole principle clearly there exists a set $\mathcal{U} \subseteq \{1, \dots, Q_{\min}N\}$ of size at least $|\mathcal{U}| \geq \left\lceil \frac{Q_{\min}N}{\overline{\zeta}^{q_{\min}}} \right\rceil$ such that $\boldsymbol{\sigma}(i) = \boldsymbol{\sigma}(j)$ for all $i, j \in \mathcal{U}$.

From now on we take input bits with indices in $\mathcal{U}$. The remark is that as all the 1's in these sequences are permuted to positions at a distance multiple of $\overline{\zeta}$, when applying the map $\phi_M^{\mathrm{in}} \circ \mathrm{Sum}_M^S$ any pair of them gives bounded output weight. We now construct a low weight codeword by setting some of positions in $\mathcal{U}$ to 1.

Let

$$b \leq \left\lfloor \left(\frac{1}{4} \left\lceil \frac{Q_{\min}N}{\overline{\zeta}^{q_{\min}}} \right\rceil \right)^{1/\lceil q_{\min}/2 \rceil} \right\rfloor \tag{5.1}$$

and split the set $\{1, \dots, q_{\min}N\}$ into b consecutive intervals $I_1, \dots, I_b$, each of length $\lfloor q_{\min}N/b \rfloor$ (except eventually the last interval with size $\lceil q_{\min}N/b \rceil$).

We construct now an hypergraph $\mathcal{H} = (\mathcal{V}, \mathcal{E})$ as follows: $\mathcal{H}$ is $q_{\min}$-partite, in the sense that it has $q_{\min}$ parts. $\mathcal{V}$ is the union of $q_{\min}$ disjoint copies of $W = \{I_1, \dots, I_b\}$. The set of hyperedges $\mathcal{E}$ has cardinality $|\mathcal{U}|$ and is $q_{\min}$-uniform, in the sense that $\mathcal{E} \in W^{q_{\min}}$ (each hyperedge contains exactly $q_{\min}$ vertices, each from a different part). Every hyperedge $e \in \mathcal{E}$ corresponds to an index $i \in \mathcal{U}$ and is of the form $e_i = (I_{h_1}, \dots, I_{h_{q_{\min}}}) \in W^{q_{\min}}$ where h_j is such that $\tau_j(i) \in I_{h_j}$. By the way b has been chosen in (5.1), we have

$$4b^{\lceil q_{\min}/2 \rceil} \leq \left\lceil \frac{Q_{\min}N}{\overline{\zeta}^{q_{\min}}} \right\rceil \leq |\mathcal{U}| = |\mathcal{E}|$$

and from Lemma 5.2 there exists a subset $\mathcal{S} \subset \mathcal{E}$ with $1 \leq |\mathcal{S}| \leq 2q_{\min} \ln b$ such that every vertex in the induced subhypergraph $(\mathcal{V}, \mathcal{S})$ has even degree. Take now the set $\widetilde{\mathcal{U}} \subseteq \mathcal{U}$ corresponding to the hyperedges in $\mathcal{S}$. Clearly we have $1 \leq |\widetilde{\mathcal{U}}| \leq 2q_{\min} \ln b$. Construct now the input sequence $\boldsymbol{u}$ as follows

$$u_i = \begin{cases} 1 & \text{if } i \in \widetilde{\mathcal{U}} \\ 0 & \text{otherwise.} \end{cases}$$

By construction $\pi(\mathrm{Rep}_N^Q(\boldsymbol{u}))$ has $|\widetilde{\mathcal{U}}|q_{\min}/2$ pairs of 1's and each pair is in the same interval I_j and at distance which is a multiple of $\overline{\zeta}$. Then we have

$$\begin{aligned}
&\mathrm{w}_{\mathrm{H}}(\boldsymbol{u}, \phi_M^{\mathrm{in}}(\mathrm{Sum}_M^S(\pi(\mathrm{Rep}_N^Q(\boldsymbol{u})))))\\
&\quad= \mathrm{w}_{\mathrm{H}}(\boldsymbol{u}) + \mathrm{w}_{\mathrm{H}}(\phi_M^{\mathrm{in}}(\mathrm{Sum}_M^S(\pi(\mathrm{Rep}_N^Q(\boldsymbol{u})))))\\
&\quad\leq |\widetilde{\mathcal{U}}| + \frac{|\widetilde{\mathcal{U}}| q_{\min}}{2} d_{\mathrm{e}} \left\lceil \frac{q_{\min} N}{b} \right\rceil\\
&\quad\leq 2 q_{\min} \ln b + q_{\min}^2 d_{\mathrm{e}} \left\lceil \frac{q_{\min} N}{b} \right\rceil \ln b\\
&\quad\leq \frac{4}{q_{\min}} \ln N + 2 d_{\mathrm{e}} \left\lceil \frac{q_{\min} N}{b} \right\rceil \ln N\\
&\quad\leq \frac{4}{q_{\min}} \ln N + 2 d_{\mathrm{e}} \left(\frac{q_{\min} N}{b} + 1 \right) \ln N\\
&\quad= \left(\frac{4}{q_{\min}} + 2 d_{\mathrm{e}} \right) \ln N + 2 d_{\mathrm{e}} \frac{q_{\min} N}{b} \ln N\\
&\quad= \left(\frac{4}{q_{\min}} + 2 d_{\mathrm{e}} \right) \ln N + 2 d_{\mathrm{e}} q_{\min} N \left(\left(\frac{Q_{\min} N}{4 \overline{\zeta}^{q_{\min}}} \right)^{1/\lceil q_{\min}/2 \rceil} - 1 \right)^{-1} \ln N\\
&\quad= \left(\frac{4}{q_{\min}} + 2 d_{\mathrm{e}} \right) \ln N + 2 d_{\mathrm{e}} q_{\min} N \left(\frac{\overline{\zeta}^{q_{\min}}}{Q_{\min} N} \right)^{1/\lceil q_{\min}/2 \rceil} \times\\
&\quad\times \left(\left(\frac{1}{4} \right)^{1/\lceil q_{\min}/2 \rceil} - \left(\frac{\overline{\zeta}^{q_{\min}}}{Q_{\min} N} \right)^{1/\lceil q_{\min}/2 \rceil} \right)^{-1} \ln N
\end{aligned}$$

If $N \geq N_0 = 8 \overline{\zeta}^{q_{\min}} / Q_{\min}$ we get

$$\begin{aligned}
&\mathrm{w}_{\mathrm{H}}(\boldsymbol{u}, \phi_M^{\mathrm{in}}(\mathrm{Sum}_M^S(\pi(\mathrm{Rep}_N^Q(\boldsymbol{u})))))\\
&\quad\leq \left(\frac{4}{q_{\min}} + 2 d_{\mathrm{e}} \right) \ln N + 2 d_{\mathrm{e}} q_{\min} N \left(\frac{\overline{\zeta}^{q_{\min}}}{Q_{\min} N} \right)^{1/\lceil q_{\min}/2 \rceil} 8 \lceil q_{\min}/2 \rceil \ln N\\
&\quad\leq \left(\frac{4}{q_{\min}} + 2 d_{\mathrm{e}} \right) \ln N + 8 d_{\mathrm{e}} q_{\min} (q_{\min} + 1) N^{1 - 1/\lceil q_{\min}/2 \rceil} \left(\overline{\zeta}^2 / Q_{\min} \right) \ln N
\end{aligned}$$

where the last inequality follows from $q_{\min} \geq 2$. We conclude there exist constants $C_1, C_2, N_0 \in \mathbb{N}$ such that for all $N \geq N_0$

$$d_{\min}(\psi_N) \leq C_1 N^{\beta} \ln(N) + C_2 \ln N$$

with $\beta = 1 - 1/\lceil q_{\min}/2 \rceil$.

□

5.5 Weight enumerators

In this section we present exact formulæ of average weight enumerators for IRC code ensembles and we present an analytical bound, which will be useful to analyze the minimum distance distribution.

5.5.1 Exact formulæ

The analysis of average weight enumerators is not affected if we assume a uniform interleaver between the inner and outer codes. This fact comes exclusively from the randomness of the LDGM ensemble construction.

Remark 5.1. *Consider the non-systematic branch of the coding scheme. The map obtained by adding an extra interleaver between the summator and the inner encoder*

$$\boldsymbol{x} = \phi_M \circ \pi_2 \circ \mathrm{Sum}_M^S \circ \pi_1 \circ \mathrm{Rep}_N^Q(\boldsymbol{u}) \tag{5.2}$$

is equivalent to the original coding scheme (see Fig. 5.3).

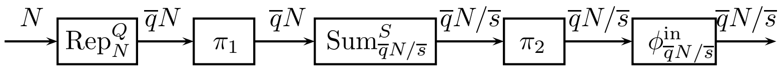

N
Rep_N^Q
$\overline{q}N$
π_1
$\overline{q}N$
$\mathrm{Sum}^S_{\overline{q}N/\overline{s}}$
$\overline{q}N/\overline{s}$
π_2
$\overline{q}N/\overline{s}$
$\phi^{\mathrm{in}}_{\overline{q}N/\overline{s}}$
$\overline{q}N/\overline{s}$

Figure 5.3: Non-systematic branch: equivalent map composition.

In fact, rewriting (5.2) as follows

$$\phi_M^{-1}(\boldsymbol{x}) = \pi_2 \circ \mathrm{Sum}_M^S \circ \pi_1 \circ \mathrm{Rep}_N^Q(\boldsymbol{u}),$$

it can be found a permutation $\widetilde{\pi}_2$ in the group $S_{\overline{q}N}$, such that $\pi_2 \circ \mathrm{Sum}_M^S = \mathrm{Sum}_M^S \circ \widetilde{\pi}_2$ and, consequently,

$$\phi_M^{-1}(\boldsymbol{x}) = \mathrm{Sum}_M^S \circ \widetilde{\pi}_2 \circ \pi_1 \circ \mathrm{Rep}_N^Q(\boldsymbol{u}).$$

The schemes considered are equivalent if the probability of the permutation $\widetilde{\pi}_2 \circ \pi_1 = \pi$ is uniform over $S_{\overline{q}N}$. Notice that

$$\begin{aligned}
\mathbb{P}(\widetilde{\pi}_2 \circ \pi_1 = \pi) &= \sum_{\sigma \in S_{\overline{q}N/\overline{s}}} \mathbb{P}(\widetilde{\pi}_2 \circ \pi_1 = \pi | \pi_2 = \sigma) \mathbb{P}(\pi_2 = \sigma) \\
&= \left(\frac{\overline{q}N}{\overline{s}}\right)^{-1} \sum_{\sigma \in S_{\overline{q}N/\overline{s}}} \mathbb{P}(\widetilde{\pi}_2 \circ \pi_1 = \pi | \pi_2 = \sigma) \\
&= \left(\frac{\overline{q}N}{\overline{s}}\right)^{-1} \sum_{\sigma \in S_{\overline{q}N/\overline{s}}} \mathbb{P}(\pi_1 = \widetilde{\pi}_2^{-1} \circ \pi | \pi_2 = \sigma) \\
&= \left(\frac{\overline{q}N}{\overline{s}}\right)^{-1} \sum_{\sigma \in S_{\overline{q}N/\overline{s}}} \mathbb{P}(\pi_1 = \widetilde{\sigma}^{-1} \circ \pi) \\
&= \left(\frac{\overline{q}N}{\overline{s}}\right)^{-1} \left(\frac{\overline{q}N}{\overline{s}}\right) \frac{1}{\overline{q}N!} = \frac{1}{\overline{q}N!}
\end{aligned}$$

where the last equality comes from the fact that π_1 is uniformly distributed over $S_{\overline{q}N}$ and we conclude that these two map compositions are equivalent.

From Remark 5.1 we deduce the following proposition.

Proposition 5.1. *The average weight enumerators of the ensemble are given by*

$$\overline{A}_{w,d}(\psi_N) = \sum_{h=0}^{q_{\max} w} \overline{A}_{w,h}\left(\phi_N^{\text{out}}\right) P_{h,d-w}(\phi^{\text{in}}_{\overline{q}N/\overline{s}})$$

where

$$P_{i,j} = \frac{A_{i,j}(\phi^{\text{in}}_{\overline{q}N/\overline{s}})}{\binom{\overline{q}N/\overline{s}}{i}}.$$

Proposition 5.2. *The average weight enumerators of LDGM code ensemble are given by*

$$\begin{aligned}\overline{A}_{w,d}(\phi_N^{\text{out}}) = \sum_{e=q_{\min} w}^{q_{\max} w} \frac{1}{\binom{\overline{q}N}{e}} \text{coeff}\left\{\prod_i (1+x^i y)^{NQ_i}, x^e y^w\right\} \times \\ \times \text{ coeff}\left\{\prod_j [\alpha_0(x,j)+\alpha_1(x,j)z]^{MS_j}, x^e z^d\right\}\end{aligned}$$

where $\alpha_0(x;j) = \frac{1}{2}\left[(1+x)^j + (1-x)^j\right]$ *and* $\alpha_1(x;j) = \frac{1}{2}\left[(1+x)^j - (1-x)^j\right]$.

Proof. Consider the bipartite graph based ensemble, in which there are N variables nodes and M check nodes. Denote by W and D the random variables denoting the input output weight, of a randomly chosen codeword of a code drawn randomly from the ensemble. Let E be the number of edges emanating from variable nodes equal to 1. We have

$$\begin{aligned}A_{w,d}(\phi_N^{\text{out}}) &= \binom{N}{w}\mathbb{P}(D=d|W=w) = \binom{N}{w}\sum_{e=0}^{\overline{q}N}\mathbb{P}(E=e, D=d|W=w) \\ &= \binom{N}{w}\sum_{e=0}^{\overline{q}N}\mathbb{P}(D=d|E=e, W=w)\mathbb{P}(E=e|W=w). \qquad (5.3)\end{aligned}$$

We get that

$$\begin{aligned}\mathbb{P}(E=e|W=w) &= \frac{\text{coeff}\left\{\prod_{i=q_{\min}}^{q_{\max}}\left(\sum_i \binom{Q_i N}{w_i} x^{iw_i} y^{w_i}\right), x^e y^w\right\}}{\binom{N}{w}} \\ &= \frac{\text{coeff}\left\{\prod_{i=q_{\min}}^{q_{\max}} (1+x^i y)^{Q_i N}, x^e y^w\right\}}{\binom{N}{w}}\end{aligned}$$

and, given the number of edges emanating from variable nodes equal to 1, we have to compute the probability that d parity nodes are connected to exactly an odd number of these edges and $M-d$ to an even number of them. Notice that $\alpha_0(x;j)$ counts in how many way we can choose j edges such that each check node has an even number of chosen sockets and, in analogous way, $\alpha_1(x;j)$ is the generating function counting in how many way we can choose j edges such that each check node has an odd number of chosen edges. Therefore, we obtain

$$\mathbb{P}(D=d|E=e,W=w)=\frac{\text{coeff}\left\{\prod_{j=s_{\min}}^{s_{max}}[\alpha_0(x;j)+\alpha_1(x;j)z]^{S_jM},x^ez^d\right\}}{\binom{\overline{q}N}{e}}$$

where $\binom{\overline{q}N}{e}$ is the number of ways to dispose e 1's in $\overline{q}N$ positions. We conclude that

$$\begin{aligned}\overline{A}_{w,d}(\phi_N^{\text{out}})=&\sum_{e=q_{\min}w}^{q_{\max}w}\frac{1}{\binom{\overline{q}N}{e}}\text{coeff}\left\{\prod_i(1+x^iy)^{NQ_i},x^ey^w\right\}\times\\ &\times\text{coeff}\left\{\prod_j[\alpha_0(x,j)+\alpha_1(x,j)z]^{MS_j},x^ez^d\right\}.\end{aligned}$$

□

In particular the weight spectrum is simplified if we consider a regular LDGM.

Corollary 5.1. *For (q,s)-regular LDGM code we have*

$$\overline{A}_{w,d}(\phi_N^{\text{out}})=\binom{N}{w}\binom{qN/s}{d}\text{coeff}\left\{\alpha_0^{qN/s-d}(x;s)\alpha_1^d(x;s),x^{qw}\right\}\binom{qN}{qw}^{-1},$$

5.5.2 Analytical bounds

Now, we consider a useful bound on the weight enumerator of the LDGM code. This bound is derived using bounding techniques devised in [39] to compute the weight enumerators of LDPC codes.

Lemma 5.3.

$$A_{w,d}(\phi_N^{\text{out}})\le\sum_{e=q_{\min}w}^{q_{\max}w}\frac{1}{\binom{\overline{q}N}{e}}\binom{N}{w}\binom{\overline{q}N/\overline{s}}{d}s_{\max}^d\binom{\overline{q}N/\overline{s}}{(e-d)/2}\binom{s_{\max}(e-d)/2}{e-d}\mathbb{1}_{\{(e-d)\in2\mathbb{N}\}}$$

Proof. Consider the expression in (5.3). Since $\mathbb{P}(E=e|W=w)\le1$ we have

$$\begin{aligned}\overline{A}_{w,d}(\phi_N^{\text{out}})&=\binom{N}{w}\sum_{e=0}^{\overline{q}N}\mathbb{P}(D=d|E=e,W=w)\mathbb{P}(E=e|W=w)\\ &\le\binom{N}{w}\sum_{e=0}^{\overline{q}N}\mathbb{P}(D=d|E=e,W=w)\\ &=\binom{N}{w}\sum_{e=0}^{\overline{q}N}\frac{\text{coeff}\left\{\prod_j[\alpha_0(x,j)+\alpha_1(x,j)z]^{MS_j},x^ez^d\right\}}{\binom{\overline{q}N}{e}}\end{aligned}$$

Notice that $\forall l$ the following inequalities hold

$$\begin{aligned}\operatorname{coeff}\left\{\alpha_1(x;j), x^l\right\} = \operatorname{coeff}\left\{\sum_{i=0}^{\lfloor j/2\rfloor}\binom{j}{2i+1}x^{2i+1}, x^l\right\} = \operatorname{coeff}\left\{jx\sum_{i=0}^{\lfloor j/2\rfloor}\frac{1}{j}\binom{j}{2i+1}x^{2i}, x^l\right\}\\ \leq \operatorname{coeff}\left\{jx\sum_{i=0}^{\lfloor j/2\rfloor}\binom{j}{2i}x^{2i}, x^l\right\} = \operatorname{coeff}\left\{s_{\max}x\alpha_0(x;j), x^l\right\}\end{aligned}$$

then we have

$$\begin{aligned}
&\operatorname{coeff}\left\{\prod_j[\alpha_0(x,j)+\alpha_1(x,j)z]^{MS_j}, x^e z^d\right\} =\\
&\leq \operatorname{coeff}\left\{\prod_j[\alpha_0(x,j)+s_{\max}x\alpha_0(x;j)z]^{MS_j}, x^e z^d\right\}\\
&= \operatorname{coeff}\left\{\prod_j[\alpha_0(x,j)(1+s_{\max}xz)]^{MS_j}, x^e z^d\right\}\\
&= \operatorname{coeff}\left\{\prod_j[\alpha_0(x,j)]^{MS_j}(1+s_{\max}xz)^{M\sum_j S_j}, x^e z^d\right\}\\
&= \operatorname{coeff}\left\{\prod_j[\alpha_0(x,j)]^{MS_j}, x^{e-d}\right\}\operatorname{coeff}\left\{(1+s_{\max}xz)^{\overline{q}N/\overline{s}}, x^d z^d\right\}\\
&= s_{\max}^d\binom{\overline{q}N/\overline{s}}{d}\operatorname{coeff}\left\{\prod_j[\alpha_0(x,j)]^{MS_j}, x^{e-d}\right\}\\
&\leq s_{\max}^d\binom{\overline{q}N/\overline{s}}{d}\operatorname{coeff}\left\{[\alpha_0(x;s_{\max})]^{M\sum_j S_j}, x^{e-d}\right\}\\
&= s_{\max}^d\binom{\overline{q}N/\overline{s}}{d}\operatorname{coeff}\left\{[\alpha_0(x;s_{\max})]^{\overline{q}N/\overline{s}}, x^{e-d}\right\}.
\end{aligned}$$

It is clear that if $e-d$ is odd, $\operatorname{coeff}\left\{[\alpha_0(x;s_{\max})]^{\overline{q}N/\overline{s}}, x^{e-d}\right\}$ is zero. To estimate this coefficient when $e-d$ is even, consider the following experiment. Consider a binary matrix with r rows and $\overline{q}N/\overline{s}$ columns. Each column corresponds to a copy of polynomial $\alpha_0(x;s_{\max})$. Set the element (i,j) in the matrix to 1 if the i-th coefficient of the j-th polynomial is chosen. Notice that the matrix has $e-d$ 1's and that each column contains an even number of 1's. Specifically, we have

$$\operatorname{coeff}\{\alpha_0(x;s_{\max})^{\overline{q}N/\overline{s}}, x^{e-d}\} = \sum_{k_0,k_2,\ldots\in\mathcal{K}}\binom{\overline{q}N/\overline{s}}{k_0,k_2,\ldots}\prod_{i\text{ even}}\binom{s_{\max}}{i}^{k_i}, \quad (5.4)$$

where

$$\mathcal{K} = \{(k_0, k_2, ...) \in \mathbb{N} : \sum_{i \text{ even}} k_i = \overline{q}N/\overline{s}, \ \sum_{i \text{ even}} ik_i = e - d\}.$$

The mutinomial coefficient enumerates all possibilities of dividing the $\overline{q}N/\overline{s}$ columns into subsets of size $l_0, l_2, \ldots$ and the binomial coefficient $\binom{s_{max}}{i}$ corresponds to choosing the i bits which are set to one in each column. So we are looking for an upper bound on the expected weight distribution. Notice that each of populated columns contains at least two 1's. Since there are $e - d$ 1's in the matrix, then there are at most $(e - d)/2$ populated columns. Then we get

$$\text{coeff}\{\alpha_0(x; s_{\max})^{\overline{q}N/\overline{s}}, x^{e-d}\} \leq \binom{\overline{q}N/\overline{s}}{(e-d)/2}\binom{s_{\max}(e-d)/2}{e-d}, \tag{5.5}$$

where $\binom{\overline{q}N/\overline{s}}{(e-d)/2}$ is the number of ways of choosing the populated columns and $\binom{s_{\max}(e-d)/2}{e-d}$ the number of ways of arranging $e-d$ 1's only in those populated columns. This completes the proof. □

5.6 Minimum distance distribution

In this section, we state and prove our main results on the minimum distance of the irregular repeat-convolute code. Our results indicates that, with high probability, $d_{\min}$ scales as N^{β}, where $\beta = 1 - 2/q_{\min}$

Lemma 5.4. *If $dq_{\max} \leq N$, there exist constants $\widetilde{C}_1, \widetilde{C}_2$ (independent on d, N) such that*

$$\mathbb{P}(d_{\min}(\psi_N) \leq d) \leq \sum_{h=0}^{q_{\max}d} \sum_{e=\max\{q_{\min},h\}}^{q_{\max}d} a_{e,h}\frac{\widetilde{C}_2^h}{h^h}d^{\lceil h/2 \rceil}$$

where

$$a_{e,h} = \widetilde{C}_1^e\left(\frac{e}{N}\right)^{\lceil e/2 \rceil - e/q_{\min}} e^{\lfloor h/2 \rfloor}$$

Proof. We start by estimating the minimum distance distribution with the union bound:

$$\mathbb{P}(d_{\min}(\psi_N) \leq d) \leq \sum_{w=1}^{d}\sum_{h=0}^{q_{\max}w}\binom{\overline{q}N/\overline{s}}{h}^{-1}\overline{A}_{w,h}(\phi_N^{\text{out}})A_{h,\leq d-w}(\phi_{\overline{q}N/\overline{s}}^{\text{in}}).$$

Lemma 4.2 ensures that there exists a constant C (independent on h, d, N) such that

$$\mathbb{P}(d_{\min}(\psi_N) \leq d) \leq \sum_{w=1}^{d}\sum_{h=0}^{q_{\max}w}\binom{\overline{q}N/\overline{s}}{h}^{-1}\overline{A}_{w,h}(\phi_N^{\text{out}})\frac{C^h}{h^h}N^{\lfloor h/2 \rfloor}d^{\lceil h/2 \rceil}$$

Using Lemma 5.3, the usual bounds $(a/b)^b \leq \binom{a}{b} \leq (a\mathrm{e}/b)^b$ and noticing that when $e-h$ is even $\frac{e-h}{2} = \lfloor e/2 \rfloor - \lfloor h/2 \rfloor$ we get there exist C_1, C_2

$$\binom{\overline{q}N/\overline{s}}{h}^{-1} \overline{A}_{w,h}(\phi_N^{\mathrm{out}}) \leq \sum_{e=q_{\min}w}^{q_{\max}w} \binom{N}{w} C_1^e C_2^h N^{-\lceil e/2 \rceil - \lfloor h/2 \rfloor} e^{\lceil e/2 \rceil + \lfloor h/2 \rfloor} \mathbb{1}_{\{(e-h)\in 2\mathbb{N}\}}.$$

Putting together these estimates and exchanging the order of summation we have

$$\begin{aligned}
&\mathbb{P}(d_{\min}(\psi_N) \leq d) \leq \\
&\leq \sum_{w=1}^{d} \sum_{e=q_{\min}w}^{q_{\max}w} \sum_{h=0}^{e} \binom{N}{w} C_1^e \widetilde{C}_2^h N^{-\lceil e/2 \rceil} e^{\lceil e/2 \rceil + \lfloor h/2 \rfloor} \frac{d^{\lceil h/2 \rceil}}{h^h} \mathbb{1}_{\{(e-h)\in 2\mathbb{N}\}} \\
&= \sum_{h=0}^{q_{\max}d} \sum_{e=q_{\min}h}^{q_{\max}d} \sum_{w=e/q_{\max}}^{e/q_{\min}} \binom{N}{w} C_1^e \widetilde{C}_2^h N^{-\lceil e/2 \rceil} e^{\lceil e/2 \rceil + \lfloor h/2 \rfloor} \frac{d^{\lceil h/2 \rceil}}{h^h} \mathbb{1}_{\{(e-h)\in 2\mathbb{N}\}} \\
&\leq \sum_{h=0}^{q_{\max}d} \sum_{e=q_{\min}h}^{q_{\max}d} \sum_{w=e/q_{\max}}^{e/q_{\min}} \binom{N}{\lfloor e/q_{\min} \rfloor} C_1^e \widetilde{C}_2^h N^{-\lceil e/2 \rceil} e^{\lceil e/2 \rceil + \lfloor h/2 \rfloor} \frac{d^{\lceil h/2 \rceil}}{h^h} \mathbb{1}_{\{(e-h)\in 2\mathbb{N}\}} \\
&\leq \sum_{h=0}^{q_{\max}d} \sum_{e=q_{\min}h}^{q_{\max}d} \widetilde{C}_1^e \widetilde{C}_2^h N^{-\lceil e/2 \rceil + \lfloor e/q_{\min} \rfloor} e^{\lceil e/2 \rceil + \lfloor h/2 \rfloor - \lfloor e/q_{\min} \rfloor} \frac{d^{\lceil h/2 \rceil}}{h^h} \mathbb{1}_{\{(e-h)\in 2\mathbb{N}\}}
\end{aligned}$$

for some constants $\widetilde{C}_1, \widetilde{C}_2$. From hypothesis $e \leq q_{\max}d \leq N$ and $(e/N)^{-\lfloor e/q_{\min} \rfloor} \leq (e/N)^{-e/q_{\min}}$ □

Lemma 5.5. *If $q_{\min} \geq 3$ and $d = o(N)$ for $N \to \infty$, for any $c \in (0,1)$, there exists N_0 such that, for all $N \geq N_0$*

$$a_{e+2,h} \leq c a_{e,h}$$

Proof. We prove the assertion by showing that when $e = o(N)$ then the ratio $a_{e+2,h}/a_{e,h} \to 0$ when $N \to 0$:

$$\begin{aligned}
\frac{a_{e+2,h}}{a_{e,h}} &= \widetilde{C}_1^2 \left(\frac{e+2}{e}\right)^{\lceil e/2 \rceil - e/q_{\min} - \lfloor h/2 \rfloor} \left(\frac{e+2}{N}\right)^{1-2/q_{\min}} \\
&\leq \widetilde{C}_1^2 \left(\frac{e+2}{e}\right)^{e} \left(\frac{e+2}{N}\right)^{1-2/q_{\min}} \\
&\leq \widetilde{C}_1^2 \mathrm{e}^2 \left(\frac{e+2}{N}\right)^{1-2/q_{\min}}.
\end{aligned}$$

If $e = o(N)$ for $N \to \infty$ then $\lim_{N\to\infty} \frac{a_{e+2,h}}{a_{e,h}} = 0$. □

Proof of Theorem 5.2. From Lemma 5.4 we get

$$\mathbb{P}(d_{\min}(\psi_N) \leq d) \leq \sum_{h=0}^{q_{\min}-1} \sum_{e=q_{\min}}^{q_{\max}d} a_{e,h} \frac{\widetilde{C}_2}{h^h} d^{\lceil h/2 \rceil} + \sum_{h=q_{\min}}^{q_{\max}d} \sum_{e=h}^{q_{\max}d} a_{e,h} \frac{\widetilde{C}_2}{h^h} d^{\lceil h/2 \rceil}$$

and from Lemma 5.5 we obtain under the assumption $d = o(N)$ that for any $c \in (0,1)$ there exists $N_0 \in \mathbb{N}$ such that $\forall N \geq N_0$

$$\begin{aligned}
\mathbb{P}(d_{\min}(\psi_N) \leq d) &\leq \sum_{h=0}^{q_{\min}-1} \sum_{l=0}^{+\infty} c^l (a_{q_{\min},h} + a_{q_{\min}+1,h}) \frac{\widetilde{C}_2}{h^h} d^{\lceil h/2 \rceil} \\
&+ \sum_{h=q_{\min}}^{q_{\max} d} \sum_{l=0}^{+\infty} c^l (a_{h,h} + a_{h+1,h}) \frac{\widetilde{C}_2}{h^h} d^{\lceil h/2 \rceil} \\
&= \sum_{h=0}^{q_{\min}-1} \frac{(a_{q_{\min},h} + a_{q_{\min}+1,h})}{1-c} \frac{\widetilde{C}_2}{h^h} d^{\lceil h/2 \rceil} \\
&+ \sum_{h=q_{\min}}^{q_{\max} d} \frac{(a_{h,h} + a_{h+1,h})}{1-c} \frac{\widetilde{C}_2}{h^h} d^{\lceil h/2 \rceil}
\end{aligned}$$

For the first summation we have the following estimate:

$$\begin{aligned}
&\sum_{h=0}^{q_{\min}-1} \frac{(a_{q_{\min},h} + a_{q_{\min}+1,h})}{1-c} \frac{\widetilde{C}_2}{h^h} d^{\lceil h/2 \rceil} \\
&\leq \frac{1}{1-c} \sum_{h=0}^{q_{\min}-1} \left[\widetilde{C}_1^{q_{\min}} \left(\frac{q_{\min}}{N} \right)^{\lceil q_{\min}/2 \rceil - 1} q_{\min}^{\lfloor h/2 \rfloor} \right. \\
&\left. + C_1^{q_{\min}+1} \left(\frac{q_{\min}+1}{N} \right)^{\lceil (q_{\min}+1)/2 \rceil - 1} (q_{\min}+1)^{\lfloor h/2 \rfloor} \right] \frac{\widetilde{C}_2}{h^h} d^{\lceil h/2 \rceil} \\
&\leq \widetilde{C} \left(N^{-\lceil q_{\min}/2 \rceil + 1} d^{\lceil (q_{\min}-1)/2 \rceil} + N^{-\lceil (q_{\min}+1)/2 \rceil + 1 + \frac{1}{q_{\min}}} d^{\lceil (q_{\min}-1)/2 \rceil} \right).
\end{aligned}$$

Consider separately the upper bound for $q_{\min}$ even and odd

- if $q_{\min}$ is even

$$\begin{aligned}
&\sum_{h=0}^{q_{\min}-1} \frac{(a_{q_{\min},h} + a_{q_{\min}+1,h})}{1-c} \frac{\widetilde{C}_2}{h^h} d^{\lceil h/2 \rceil} \\
&\leq \widetilde{C} \left(N^{-q_{\min}/2+1} d^{q_{\min}/2} + N^{-(q_{\min}+2)/2+1+\frac{1}{q_{\min}}} d^{q_{\min}/2} \right) \\
&= \widetilde{C} N^{-q_{\min}/2+1} d^{q_{\min}/2} \left(1 + N^{-1+\frac{1}{q_{\min}}} \right) \leq 2\widetilde{C} N^{-q_{\min}/2+1} d^{q_{\min}/2}
\end{aligned}$$

- if $q_{\min}$ is odd

$$\begin{aligned}
&\sum_{h=0}^{q_{\min}-1} \frac{(a_{q_{\min},h} + a_{q_{\min}+1,h})}{1-c} \frac{\widetilde{C}_2}{h^h} d^{\lceil h/2 \rceil} \\
&\leq \widetilde{C} \left(N^{-(q_{\min}+1)/2+1} d^{(q_{\min}-1)/2} + N^{-(q_{\min}+1)/2+1+\frac{1}{q_{\min}}} d^{(q_{\min}-1)/2} \right) \\
&= \widetilde{C} N^{-(q_{\min}+1)/2+1} d^{(q_{\min}+1)/2} \left(\frac{1}{N} + N^{-\frac{1}{2}+\frac{1}{q_{\min}}} \right) \\
&\leq 2\widetilde{C} N^{-(q_{\min}+1)/2+1} d^{(q_{\min}+1)/2}.
\end{aligned}$$

We conclude that the upper bound for the overall first summation is given by

$$\sum_{h=0}^{q_{\min}-1} \frac{(a_{q_{\min},h} + a_{q_{\min}+1,h})}{1-c} \frac{\widetilde{C}_2}{h^h} d^{\lceil h/2 \rceil} \leq \overline{C} N^{1-\lceil q_{\min}/2 \rceil} d^{\lceil q_{\min}/2 \rceil}. \tag{5.6}$$

For the second summation, instead, we have

$$\begin{aligned}
&\sum_{h=q_{\min}}^{q_{\max}d} \frac{(a_{h,h} + a_{h+1,h})}{1-c} \frac{\widetilde{C}_2}{h^h} d^{\lceil h/2 \rceil} \leq \\
&\quad \leq \frac{1}{1-c} \sum_{h=q_{\min}}^{q_{\max}d} \left(\widetilde{C}_1^h \left(\frac{h}{N}\right)^{\lceil \frac{h}{2} \rceil - \frac{h}{q_{\min}}} h^{\lfloor \frac{h}{2} \rfloor} \frac{\widetilde{C}_2^h}{h^h} d^{\lceil \frac{h}{2} \rceil} + \right. \\
&\quad \left. + \widetilde{C}_1^{h+1} \left(\frac{h+1}{N}\right)^{\lceil \frac{h+1}{2} \rceil - \frac{h+1}{q_{\min}}} (h+1)^{\lfloor \frac{h+1}{2} \rfloor} \frac{\widetilde{C}_2^h}{h^h} d^{\lceil \frac{h}{2} \rceil} + \right) \\
&\quad \leq \frac{1}{1-c} \sum_{h=q_{\min}}^{q_{\max}d} \left(\overline{C}_1^h N^{\frac{h}{q_{\min}} - \lceil \frac{h}{2} \rceil} d^{\lceil \frac{h}{2} \rceil} + \widetilde{C}_1^h (h+1) \mathrm{e} N^{\frac{h+1}{q_{\min}} - \lceil \frac{h+1}{2} \rceil} \widetilde{C}_2^h d^{\lceil \frac{h}{2} \rceil} \right) \\
&\quad \leq \frac{1}{1-c} \sum_{h=q_{\min}}^{q_{\max}d} \left(\overline{C}_1^h N^{\frac{h}{q_{\min}} - \lceil \frac{h}{2} \rceil} d^{\lceil \frac{h}{2} \rceil} + \overline{C}_2^h N^{\frac{h+1}{q_{\min}} - \lceil \frac{h+1}{2} \rceil} d^{\lceil \frac{h}{2} \rceil} \right)
\end{aligned}$$

for some constants $\overline{C}_1, \overline{C}_2$.

We get for the second summation

$$\begin{aligned}
\sum_{h=q_{\min}}^{q_{\max}d} \frac{(a_{h,h} + a_{h+1,h})}{1-c} \frac{\widetilde{C}_2}{h^h} d^{\lceil h/2 \rceil} &\leq \sum_{h=q_{\min}}^{q_{\max}d} C^h d^{\lceil \frac{h}{2} \rceil} \left(N^{\frac{h}{q_{\min}} - \lceil \frac{h}{2} \rceil} + N^{\frac{h+1}{q_{\min}} - \lceil \frac{h+1}{2} \rceil} \right) \\
&= \sum_{h=q_{\min}, h \in 2\mathbb{N}}^{q_{\max}d} C^h d^{\frac{h}{2}} \left(N^{\frac{h}{q_{\min}} - \frac{h}{2}} + N^{\frac{h+1}{q_{\min}} - \frac{h+2}{2}} \right) \\
&+ \sum_{h=q_{\min}, h \notin 2\mathbb{N}}^{q_{\max}d} C^h d^{\frac{h+1}{2}} \left(N^{\frac{h}{q_{\min}} - \frac{h+1}{2}} + N^{\frac{h+1}{q_{\min}} - \frac{h+1}{2}} \right) \\
&= \sum_{h=q_{\min}, h \in 2\mathbb{N}}^{q_{\max}d} C^h d^{\frac{h}{2}} N^{\frac{h}{q_{\min}} - \frac{h}{2}} \left(1 + N^{\frac{1}{q_{\min}} - 1} \right) \\
&+ \sum_{h=q_{\min}, h \notin 2\mathbb{N}}^{q_{\max}d} C^h d^{\frac{h+1}{2}} N^{\frac{gh}{q_{\min}} - \frac{h}{2}} \left(N^{1/q_{\min} - \frac{1}{2}} + N^{-\frac{1}{2}} \right) \\
&\leq 2 \sum_{h=q_{\min}, h \in 2\mathbb{N}}^{q_{\max}d} \left(C d^{\frac{1}{2}} N^{\frac{1}{q_{\min}} - \frac{1}{2}} \right)^h \\
&+ d^{\frac{1}{2}} \left(N^{1/q_{\min} - \frac{1}{2}} + N^{-\frac{1}{2}} \right) \sum_{h=q_{\min}, h \notin 2\mathbb{N}}^{q_{\max}d} \left(C d^{\frac{1}{2}} N^{\frac{1}{q_{\min}} - \frac{1}{2}} \right)^h
\end{aligned}$$

If $d = o(N)$, for sufficiently large N we have

$$d^{\frac{1}{2}}\left(N^{1/q_{\min}-\frac{1}{2}} + N^{-\frac{1}{2}}\right) \leq 2d^{\frac{1}{2}}N^{1/q_{\min}-\frac{1}{2}}$$

We conclude that

$$\begin{aligned}\mathbb{P}(d_{\min}(\psi_N) \leq d) \leq{} & \overline{C}N^{1-\lceil q_{\min}/2\rceil}d^{\lceil q_{\min}/2\rceil} + 2\sum_{h=q_{\min},h\in 2\mathbb{N}}^{q_{\max}d}\left(Cd^{\frac{1}{2}}N^{-\frac{1}{2}+\frac{1}{q_{\min}}}\right)^{h} \\ & + 2\sum_{h=q_{\min},h\notin 2\mathbb{N}}^{q_{\max}d}\left(Cd^{\frac{1}{2}}N^{-\frac{1}{2}+\frac{1}{q_{\min}}}\right)^{h+1} \\ \leq{} & \overline{C}N^{1-\lceil q_{\min}/2\rceil}d^{\lceil q_{\min}/2\rceil} + \\ & + 2CN^{1-\frac{q_{\min}}{2}}d^{\frac{q_{\min}}{2}}\left(1 + d^{\frac{1}{2}}N^{-\frac{1}{2}+\frac{1}{q_{\min}}}\right)\sum_{h=0}^{+\infty}\left(Cd^{\frac{1}{2}}N^{-\frac{1}{2}+\frac{1}{q_{\min}}}\right)^{h}\end{aligned}$$

Notice that if $d = o(N^{\beta})$ then $N^{-\frac{1}{2}+\frac{1}{q_{\min}}}d^{\frac{1}{2}} \to 0$ when $N \to \infty$, the above series is convergent and $\mathbb{P}(d_{\min}(\psi_N) \leq d)$ is asymptotically vanishing. □

5.7 Concluding remarks

This chapter has analyzed the behavior of the minimum distance of a family of linear-time encodable LDPC codes. The design parameter, provided through this analysis, for the constituents encoders of the scheme are perfectly matching with the ones suggested by the analysis of the average error probability [19,78].

Further investigations will be devoted to the case of multiple inner encoders. The minimum distance analysis is a straightforward generalization of results in Chapter 4, while the convergence to the Gilbert-Varshamov distance looks a hard task.

6 Conclusions

In this thesis, we developed a theoretical analysis of turbo-like coding ensembles, where convolutional encoders are concatenated through permutations.

First, we focused on truncated convolutional encoders. We derived exact formulæ of the weight enumerators and showed how asymptotic estimates of powers of multivariate functions with nonnegative coefficients can be used to study their growth rate in the code length. Then, we obtained an explicit expression of the asymptotic spectral function and proved its continuity and concavity.

Building upon these results, we analyzed average spectra and minimum distance of multiple concatenated coding schemes. We identified sufficient conditions allowing minimum distances to scale linearly in the code length with high probability, and we obtained lower bounds for their typical normalized minimum distance. The design parameter for the constituents encoders of the scheme, provided through this analysis, perfectly match with the ones suggested by the analysis of the average error probability [19] and observed from simulations [44].

Moreover, we derived a very mild condition on the outer encoder, which guarantees the convergence of the minimum distance to the GV-distance when the number of interconnections goes to infinity. The question whether this assumption can be removed is still an open problem. Another open problem is to find mathematical tools to estimate how fast the typical minimum distances converge to the GV-limit.

We also considered another binary ensemble fitting in the general scheme discussed above. It is a generalization of Repeat-Convolute codes, and it can be interpreted as a family of structured linear-time encodable and decodable LDPC codes, generalizing staircase LDPC codes. The inner encoder is itself the composition of two maps, and in order to find a design criterion we presented the minimum distance analysis. We showed that minimum distances can grow at most sub-linearly in the code length and that this happens with probability close to one.

Some of the main problems left for future research are:

- proving concentration results for the spectra of turbo-like code ensembles using a second order method;
- analyzing the weight spectrum of turbo-stopping-sets, a measure of the performance of a binary turbo decoder on the BEC introduced for turbo-like codes in [73].

The mathematical tools used in this thesis should help addressing these issues.

Multidimensional saddle-point method for large powers A

We prove now Theorem 3.4 through intermediate steps. Our proof is based on multidimensional saddle-point (MSP) techniques to estimate order of magnitude of coefficients in large powers of multivariate functions.

We can summarize the MSP-method as follows. The first step is to recast the problem as computation of a Cauchy integral and to apply the residue theorem. In order to estimate complex integrals of an analytic function, it is often a good strategy to choose a path crossing a saddle-point and estimate the integrand locally near this saddle-point (i.e. where the modulus of the integrand achieves its maximum on the contour). If the generating function satisfies some "nice" properties, which go under the name of *localization* or *concentration*, the contribution near the saddle-point captures the essential part of the integral. Some examples of admissible functions are multivariate polynomial (see Lemma D.14 in [21]) and univariate series (see Section VIII.8.1 in [62]). Applications of multidimensional saddle point method in the context of coding theory can be found in [21, 42, 43] to study weight/stopping set distribution of LDPC codes.

Theorem 3.4 can be thought as an extension of Theorem 2 in [52]:

- The generating function is given by the product of two kinds of functions ($S(\boldsymbol{x})$ and a large power of $F(\boldsymbol{x})$).

- It involves multivariate series with non-negative coefficients, for which the "localization property", cited above, has never been proved.

- Theorem 3.4 estimates the order of magnitude of a (convergent) sequence of coefficients in large powers of multivariate functions.

A.1 Concentration property for multivariate series

In the sequel we will consider multivariable formal power series of type

$$F(\boldsymbol{x}) = \sum_{\boldsymbol{k}\in\mathbb{N}_0^\eta} F_{\boldsymbol{k}}\boldsymbol{x}^{\boldsymbol{k}}$$

where $\boldsymbol{x} = (x_1, \ldots, x_\eta)$, and $\boldsymbol{x}^{\boldsymbol{k}} = \prod_{i=1}^{\eta} x_i^{k_i}$ and we recall the notation:

$$\mathscr{F} := \{\boldsymbol{k} \in \mathbb{N}_0^\eta \,|\, F_{\boldsymbol{k}} > 0\} \;.$$

Throughout this section we will assume that $F(\boldsymbol{x})$ possesses the following properties:

(P1) $F_{\boldsymbol{k}} \in \mathbb{N}_0$ for every $\boldsymbol{k}$, and $F_{\boldsymbol{0}} > 0$.

(P2) There exists $C \in \mathbb{R}^+$ and $s \in \mathbb{N}$ such that $F_{\boldsymbol{k}} \le C|\boldsymbol{k}|^s$ for every $\boldsymbol{k}$.

(P3) There exists a finite subset $\mathscr{F}_0 \subseteq \mathscr{F}$ and $\boldsymbol{k}^1, \ldots \boldsymbol{k}^l \in \mathbb{N}_0^\eta$ such that:

(P3a) $\mathscr{F} \subseteq \{\boldsymbol{k}^0 + \sum_{i=1}^{l} t_i\boldsymbol{k}^i \mid \boldsymbol{k}^0 \in \mathscr{F}_0,\ t_i \in \mathbb{N}\}$.

(P3b) There exist $\widetilde{\boldsymbol{k}}_i \in \mathscr{F}$ for $i = 1, \ldots, l$ such that $\widetilde{\boldsymbol{k}}_i + t\boldsymbol{k}_i \in \mathscr{F}$ for every $t \in \mathbb{N}_0$.

(P4) $\mathscr{F}$ generates $\mathbb{Z}^\mu$ as an Abelian group.

From (P1), (P2) and (P3) it follows that the region of absolute convergence $\Sigma \subseteq \mathbb{R}^\eta$ of $F(\boldsymbol{x})$ is given by the open set:

$$\Sigma = \left\{\boldsymbol{x} \in \mathbb{R}^\eta \;\middle|\; \left|\boldsymbol{x}^{\boldsymbol{k}^i}\right| < 1 \;\forall i = 1, \ldots, l\right\} \tag{A.1}$$

The sum of the series on Σ will be denoted by the same symbol $F(\boldsymbol{x}) := \sum\limits_{\boldsymbol{k}\in\mathbb{N}_0^\eta} F_{\boldsymbol{k}}\boldsymbol{x}^{\boldsymbol{k}}$. Put $\Sigma^+ := \Sigma \cap (\mathbb{R}^+)^\eta$.

Lemma A.1. *Let $\overline{\boldsymbol{x}} \in \partial\Sigma^+$ with $\overline{x}_i > 0$ for every $i = 1, \ldots, \eta$. Let $\boldsymbol{x}_n \in \Sigma^+$ be a sequence such that $\boldsymbol{x}_n \to \overline{\boldsymbol{x}}$ for $n \to +\infty$. Then,*

$$F(\boldsymbol{x}) = \lim_{n\to+\infty} F(\boldsymbol{x}_n) = +\infty\,.$$

Proof. (P1) and Fatou's lemma [79] yield:

$$\liminf_{n\to+\infty} F(\boldsymbol{x}_n) \ge F(\overline{\boldsymbol{x}})\,,$$

hence, to prove the result, it is sufficient to show that $F(\overline{\boldsymbol{x}}) = +\infty$ (notice that the expression $F(\overline{\boldsymbol{x}})$ is meaningful because it is the summation of a non-negative series). Suppose, by contradiction, that instead $F(\overline{\boldsymbol{x}}) < +\infty$. Then, using (P3b) and (P1), for every $i = 1, \ldots, l$ we obtain

$$+\infty > F(\overline{\boldsymbol{x}}) = \sum_{\boldsymbol{k}\in\mathbb{N}_0^\eta} F_{\boldsymbol{k}}\overline{\boldsymbol{x}}^{\boldsymbol{k}} \ge \sum_{t=0}^{+\infty} F_{\widetilde{\boldsymbol{k}}_i+t\boldsymbol{k}_i}\overline{\boldsymbol{x}}^{\widetilde{\boldsymbol{k}}_i}\left(\overline{\boldsymbol{x}}^{\boldsymbol{k}_i}\right)^t \ge \sum_{t=0}^{+\infty} \overline{\boldsymbol{x}}^{\widetilde{\boldsymbol{k}}_i}\left(\overline{\boldsymbol{x}}^{\boldsymbol{k}_i}\right)^t$$

This yields $\overline{\boldsymbol{x}}^{\boldsymbol{k}_i} < 1$ for every $i = 1, \dots, l$. From (A.1) it follows that $\overline{\boldsymbol{x}}$ is an interior point of Σ^+ contrarily to what was assumed. □

Lemma A.2. *For every $\boldsymbol{\omega} \in \overset{\circ}{\mathrm{co}(\mathscr{F})}$, there exists a unique $\boldsymbol{x} \in \overset{\circ}{\Sigma^+}$ such that*

$$\Delta[F](\boldsymbol{x}) = \boldsymbol{\omega}, \tag{A.2}$$

where $\Delta[F]$ is defined in (3.21).

Proof. Notice first of all that points solving (A.2) are the stationary point in $\overset{\circ}{\Sigma^+}$ of $\widehat{F}_{\boldsymbol{\omega}}(\boldsymbol{x}) = \ln\left(F(\boldsymbol{x})/\boldsymbol{x}^{\boldsymbol{\omega}}\right)$.

UNIQUENESS: Consider the function $f_{\boldsymbol{\omega}}(\boldsymbol{\xi}) = \widehat{F}_{\boldsymbol{\omega}}(\mathrm{e}^{\xi_1}, \mathrm{e}^{\xi_2}, \dots, \mathrm{e}^{\xi_\eta})$. It is strictly convex on the set $\Xi = \{\boldsymbol{\xi} | (\xi_1, \dots, \xi_\eta) = (\ln x_1, \dots, \ln x_\eta), \boldsymbol{x} \in \Sigma^+\} \subseteq \mathbb{R}^\eta$. Indeed,

$$\begin{aligned}
\boldsymbol{v}^T \nabla^2 f(\boldsymbol{\xi}) \boldsymbol{v} &= \sum_{i=1}^{\eta} \sum_{j=1}^{\eta} v_i \frac{\partial^2 f}{\partial \xi_j \partial \xi_i} v_j \\
&= \sum_{i=1}^{\eta} \sum_{j=1}^{\eta} v_i \left(\sum_{\boldsymbol{k}} F_{\boldsymbol{k}} \mathrm{e}^{(\boldsymbol{k}-\boldsymbol{\omega})\cdot\boldsymbol{\xi}} (k_i - \omega_i)(k_j - \omega_j) \right) v_j \\
&= \sum_{\boldsymbol{k}} F_{\boldsymbol{k}} \mathrm{e}^{(\boldsymbol{k}-\boldsymbol{\omega})\cdot\boldsymbol{\xi}} \sum_{i=1}^{\eta} \sum_{j=1}^{\eta} v_i (k_i - \omega_i)(k_j - \omega_j) v_j \\
&= \sum_{\boldsymbol{k}} F_{\boldsymbol{k}} \mathrm{e}^{(\boldsymbol{k}-\boldsymbol{\omega})\cdot\boldsymbol{\xi}} ||(\boldsymbol{v} \cdot (\boldsymbol{k} - \boldsymbol{\omega}))|| \geq 0
\end{aligned}$$

Since $\boldsymbol{\omega} \in \overset{\circ}{\mathrm{co}(\mathscr{F})}$ then $\boldsymbol{v}^T \nabla^2 f(\boldsymbol{\xi}) \boldsymbol{v} = 0 \iff \boldsymbol{v} = \boldsymbol{0}$. This implies that $f(\boldsymbol{\xi})$ is strictly convex in $\boldsymbol{\xi} \in \Xi$. Uniqueness of the solution of (A.2) hence follows.

EXISTENCE: We now show that for any sequence $\boldsymbol{x}_n$ either converging to a point of $\partial\Sigma^+$ or unbounded, it holds that $\widehat{F}_{\boldsymbol{\omega}}(\boldsymbol{x}_n)$ is superiorly unbounded. This will imply that $\widehat{F}_{\boldsymbol{\omega}}$ attains global minimum in $\overset{\circ}{\Sigma^+}$ and will complete the proof.

Consider first the case when $\boldsymbol{x}_n \to \overline{\boldsymbol{x}} \in \partial\Sigma^+$ with $\overline{x}_i > 0$ for all i. In this case the result easily follows from Lemma A.1. If, instead, there exists i such that $\overline{x}_i = 0$, then,

$$\frac{F(\boldsymbol{x}_n)}{\boldsymbol{x}_n^{\boldsymbol{\omega}}} \geq \frac{F_0}{\boldsymbol{x}_n^{\boldsymbol{\omega}}} \to +\infty \qquad (n \to +\infty) \tag{A.3}$$

It remains to consider the case when at least one component of $\boldsymbol{x}_n$ diverges to $+\infty$. Since $\boldsymbol{\omega} \in \overset{\circ}{\mathrm{co}(\mathscr{F})}$, we can find $\boldsymbol{f}^1, \dots \boldsymbol{f}^\mu \in \mathscr{F} \setminus \{\boldsymbol{0}\}$ generating $\mathbb{R}^\mu$ and strictly positive constants $\gamma_1, \dots, \gamma_s$ such that $\sum \gamma_j < 1$ and $\boldsymbol{\omega} = \sum \gamma_j \boldsymbol{f}^j$. Passing possibly to subsequences, we can always assume that $\boldsymbol{x}_n^{\boldsymbol{f}^l} \to \alpha_l \in [0, +\infty]$ for all $l \in \{1, \dots, \mu\}$. If $\alpha_l \in]0, +\infty[$ for all l, then this would easily imply that $\boldsymbol{x}_n$ is bounded. If $\alpha_l \in [0,+\infty[$ for all l and at least one of them is 0, then, since $\boldsymbol{x}_n^{\boldsymbol{\omega}} = \prod_l [\boldsymbol{x}_n^{\boldsymbol{f}^l}]^{\gamma_l}$, we would have $\boldsymbol{x}_n^{\boldsymbol{\omega}} \to 0$ and we could argue as in (A.3). Consider finally the case when at least one $\alpha_l = +\infty$.

We can write as follows:

$$\frac{F(\boldsymbol{x}_n)}{\boldsymbol{x}_n^{\boldsymbol{\omega}}} = \frac{F(\boldsymbol{x}_n)}{\prod_l [\boldsymbol{x}_n^{\boldsymbol{f}^l}]^{\gamma^l}}$$

where $\gamma = \sum \gamma_l < 1$. Let now $z_l = \boldsymbol{x}_n^{\boldsymbol{f}^l} > 0$ for $l = 1, \dots, \mu$. Then,

$$\prod_l z_l^{\gamma^l} \le \sum_l z_l^{\gamma}. \tag{A.4}$$

To see this fact let

$$\Gamma(z) = \frac{\prod_j z_j^{\gamma^j}}{\sum_j z_j^{\gamma}}.$$

It satisfies $\Gamma(\lambda z) = \Gamma(z)$ for every z and $\lambda > 0$. Let us restrict it to the z such that $\sum_j z_j^{\gamma} = 1$. Necessarily, $z_j \le 1$ for all j and this yields

$$\Gamma(z) = \prod_j z_j^{\gamma^j} \le 1$$

This proves the inequality.

Using (A.4) we have

$$\frac{F(\boldsymbol{x}_n)}{\boldsymbol{x}_n^{\boldsymbol{\omega}}} = \frac{F(\boldsymbol{x}_n)}{\prod_l [\boldsymbol{x}_n^{\boldsymbol{f}^l}]^{\gamma^l}} \ge \frac{\sum_j \boldsymbol{x}_n^{\boldsymbol{f}^j}}{\sum_j [\boldsymbol{x}_n^{\boldsymbol{f}^j}]^{\gamma}}$$

where $\gamma = \sum \gamma_j < 1$. The expression on the left is clearly superiorly unbounded for $n \to +\infty$ and this completes the result.

□

Lemma A.3. *The matrix $\boldsymbol{\Gamma}[F](\boldsymbol{x})$ (defined in (3.22)) is symmetric and definite positive $\forall \boldsymbol{x} \in \Sigma^+$.*

Proof. In the sequel we put $\boldsymbol{\Gamma} = \boldsymbol{\Gamma}[F]$.

$$\begin{aligned} F(\boldsymbol{x})^2 \boldsymbol{v}^T \boldsymbol{\Gamma}(\boldsymbol{x}) \boldsymbol{v} &= F(\boldsymbol{x})^2 \sum_{i=1}^{\eta} \sum_{j=1}^{\eta} v_i \Gamma_{ij}(\boldsymbol{x}) v_j \\ &= F(\boldsymbol{x})^2 \sum_{i=1}^{\eta} v_i^2 \Gamma_{ii}(\boldsymbol{x}) + F(\boldsymbol{x})^2 \sum_{i=1}^{\eta} \sum_{j \ne i}^{\eta} v_i \Gamma_{ij}(\boldsymbol{x}) v_j \end{aligned}$$

$$
\begin{aligned}
F(\boldsymbol{x})^2\boldsymbol{v}^T\boldsymbol{\Gamma}(\boldsymbol{x})\boldsymbol{v} &= \sum_{i=1}^{\eta} v_i^2 \left[\sum_{\boldsymbol{k}}\sum_{\boldsymbol{l}} \left(k_i^2 - k_i l_i\right) F_{\boldsymbol{k}} F_{\boldsymbol{l}} \boldsymbol{x}^{\boldsymbol{k}+\boldsymbol{l}}\right] + \\
&\quad + \sum_{i=1}^{\eta}\sum_{j\neq i}^{\eta} v_i v_j \left[\sum_{\boldsymbol{k}}\sum_{\boldsymbol{l}} \left(k_i k_j - k_i l_j\right) F_{\boldsymbol{k}} F_{\boldsymbol{l}} \boldsymbol{x}^{\boldsymbol{k}+\boldsymbol{l}}\right] \\
&= \sum_{\boldsymbol{k}}\sum_{\boldsymbol{l}} F_{\boldsymbol{k}} F_{\boldsymbol{l}} \boldsymbol{x}^{\boldsymbol{k}+\boldsymbol{l}} \left[\sum_{i=1}^{\eta} v_i^2 \left(k_i^2 - k_i l_i\right) + \sum_{i=1}^{\eta}\sum_{j\neq i}^{\eta} v_i v_j \left(k_i k_j - k_i l_j\right)\right] \\
&= \sum_{\boldsymbol{k}}\sum_{\boldsymbol{l}} F_{\boldsymbol{k}} F_{\boldsymbol{l}} \boldsymbol{x}^{\boldsymbol{k}+\boldsymbol{l}} \left[\sum_{i=1}^{\eta} v_i^2 \left(k_i - l_i\right)^2 + \sum_{i=1}^{\eta} v_i^2 l_i \left(k_i - l_i\right) + \right. \\
&\quad \left. + \sum_{i=1}^{\eta}\sum_{j\neq i}^{\eta} v_i v_j \left(k_i k_j - k_i l_j - k_j l_i + l_i l_j\right) + \sum_{i=1}^{\eta}\sum_{j\neq i}^{\eta} v_i v_j l_i \left(k_j - l_j\right)\right] \\
&= \sum_{\boldsymbol{k}}\sum_{\boldsymbol{l}} F_{\boldsymbol{k}} F_{\boldsymbol{l}} \boldsymbol{x}^{\boldsymbol{k}+\boldsymbol{l}} \left[\sum_{i=1}^{\eta} v_i^2 \left(k_i - l_i\right)^2 + \sum_{i=1}^{\eta} v_i^2 l_i \left(k_i - l_i\right) + \right. \\
&\quad \left. + \sum_{i=1}^{\eta}\sum_{j\neq i}^{\eta} v_i v_j \left(k_i - l_i\right)\left(k_j - l_j\right) + \sum_{i=1}^{\eta}\sum_{j\neq i}^{\eta} v_i v_j l_i \left(k_j - l_j\right)\right] \\
&= \sum_{\boldsymbol{k}}\sum_{\boldsymbol{l}} F_{\boldsymbol{k}} F_{\boldsymbol{l}} \boldsymbol{x}^{\boldsymbol{k}+\boldsymbol{l}} \left[\sum_{i=1}^{\eta} v_i \left(k_i - l_i\right)\right]^2 + \\
&\quad + \sum_{\boldsymbol{k}}\sum_{\boldsymbol{l}} F_{\boldsymbol{k}} F_{\boldsymbol{l}} \boldsymbol{x}^{\boldsymbol{k}+\boldsymbol{l}} \left[\sum_{i=1}^{\eta} v_i l_i \left(v_i(k_i - l_i) + \sum_{j\neq i}^{\eta} v_j \left(k_j - l_j\right)\right)\right],
\end{aligned}
$$

from which

$$
\begin{aligned}
F(\boldsymbol{x})^2\boldsymbol{v}^T\boldsymbol{\Gamma}(\boldsymbol{x})\boldsymbol{v} &= \sum_{\boldsymbol{k}}\sum_{\boldsymbol{l}} F_{\boldsymbol{k}} F_{\boldsymbol{l}} \boldsymbol{x}^{\boldsymbol{k}+\boldsymbol{l}} \left[\sum_{i=1}^{\eta} v_i \left(k_i - l_i\right)\right]^2 \\
&\quad + \sum_{\boldsymbol{k}}\sum_{\boldsymbol{l}} F_{\boldsymbol{k}} F_{\boldsymbol{l}} \boldsymbol{x}^{\boldsymbol{k}+\boldsymbol{l}} \left[\sum_{i=1}^{\eta}\sum_{j=1}^{\eta} v_i v_j l_i \left(k_j - l_j\right)\right] \\
&= \sum_{\boldsymbol{k}}\sum_{\boldsymbol{l}} F_{\boldsymbol{k}} F_{\boldsymbol{l}} \boldsymbol{x}^{\boldsymbol{k}+\boldsymbol{l}} \left[\sum_{i=1}^{\eta} v_i \left(k_i - l_i\right)\right]^2 \geq 0 \qquad \forall \boldsymbol{x} \in \Sigma^+
\end{aligned}
$$

Clearly, $\boldsymbol{v}^T\boldsymbol{\Gamma}(\boldsymbol{x})\boldsymbol{v} = 0$ if and only if $\boldsymbol{v} = \boldsymbol{0}$. This yields the result. □

Lemma A.4. *For each $\boldsymbol{r} \in (\mathbb{R}^+)^\eta$, there exists a strictly positive constant $\chi = \chi(F, \boldsymbol{r})$ such that $\forall \boldsymbol{\theta} \in [-\pi, \pi)^\eta \setminus \left[-n^{-2/5}, n^{-2/5}\right]$ it holds the following inequality*

$$
\left|\frac{F\left(\boldsymbol{r}\mathrm{e}^{\mathrm{j}\boldsymbol{\theta}}\right)}{F(\boldsymbol{r})}\right|^n \leq \chi n^{-1/5}. \tag{A.5}
$$

Proof. We have that

$$\left|\frac{F\left(\boldsymbol{r}\mathrm{e}^{\mathrm{j}\boldsymbol{\theta}}\right)}{F(\boldsymbol{r})}\right|^2 = \frac{\left(\sum_{\boldsymbol{k}} F_{\boldsymbol{k}}\boldsymbol{r}^{\boldsymbol{k}}\mathrm{e}^{\mathrm{j}\boldsymbol{k}^T\boldsymbol{\theta}}\right)\left(\sum_{\boldsymbol{l}} F_{\boldsymbol{l}}\boldsymbol{r}^{\boldsymbol{l}}\mathrm{e}^{-\mathrm{j}\boldsymbol{l}^T\boldsymbol{\theta}}\right)}{|F(\boldsymbol{r})|^2} = \frac{\sum_{\boldsymbol{k},\boldsymbol{l}} F_{\boldsymbol{k}}F_{\boldsymbol{l}}\boldsymbol{r}^{\boldsymbol{k}+\boldsymbol{l}}\mathrm{e}^{\mathrm{j}(\boldsymbol{k}-\boldsymbol{l})^T\boldsymbol{\theta}}}{|F(\boldsymbol{r})|^2}$$

$$= 1 - \frac{\sum_{\boldsymbol{k}\neq\boldsymbol{l}} F_{\boldsymbol{k}}F_{\boldsymbol{l}}\boldsymbol{r}^{\boldsymbol{k}+\boldsymbol{l}}\left[1-\cos\left((\boldsymbol{k}-\boldsymbol{l})^T\boldsymbol{\theta}\right)\right]}{|F(\boldsymbol{r})|^2}$$

and, by choosing $\widetilde{\boldsymbol{k}},\widetilde{\boldsymbol{l}} \in \mathscr{F}$, we get

$$\left|\frac{F\left(\boldsymbol{r}\mathrm{e}^{\mathrm{j}\boldsymbol{\theta}}\right)}{F(\boldsymbol{r})}\right|^2 \leq 1 - \frac{F_{\widetilde{\boldsymbol{k}}}F_{\widetilde{\boldsymbol{l}}}\boldsymbol{r}^{\widetilde{\boldsymbol{k}}+\widetilde{\boldsymbol{l}}}\left[1-\cos\left((\widetilde{\boldsymbol{k}}-\widetilde{\boldsymbol{l}})^T\boldsymbol{\theta}\right)\right]}{|F(\boldsymbol{r})|^2}$$

$$\leq \frac{1 - F_{\widetilde{\boldsymbol{k}}}F_{\widetilde{\boldsymbol{l}}}\boldsymbol{r}^{\widetilde{\boldsymbol{k}}+\widetilde{\boldsymbol{l}}}\left[\frac{1}{2}|(\widetilde{\boldsymbol{k}}-\widetilde{\boldsymbol{l}})^T\boldsymbol{\theta}|^2 - \frac{1}{6}|(\widetilde{\boldsymbol{k}}-\widetilde{\boldsymbol{l}})^T\boldsymbol{\theta}|^3\right]}{|F(\boldsymbol{r})|^2}.$$

If we assume $\boldsymbol{\theta} \in (-\varepsilon,\varepsilon)^\eta$ with $\varepsilon \leq 3/(2||\widetilde{\boldsymbol{k}}-\widetilde{\boldsymbol{l}}||_1)$ and $\boldsymbol{r} \in (\mathbb{R}^+)^\eta$, then from last inequality we get that there exists a constant $\chi = \chi(F,\boldsymbol{r}) \in \mathbb{R}^+$ only depending on F and $\boldsymbol{r}$ such that

$$\left|\frac{F\left(\boldsymbol{r}\mathrm{e}^{\mathrm{j}\boldsymbol{\theta}}\right)}{F(\boldsymbol{r})}\right|^2 \leq 1 - \chi||\boldsymbol{\theta}||_2^2. \tag{A.6}$$

Since $\langle\mathscr{F}\rangle = \mathbb{Z}^\eta$, standard results on Fourier analysis [80] show that

$$\langle\mathscr{F}\rangle\cdot\boldsymbol{\theta} = 0 \pmod{2\pi} \iff \boldsymbol{\theta} = 0 \pmod{2\pi}.$$

Since $F(\boldsymbol{r}) > 0\ \forall\boldsymbol{r} \in (\mathbb{R}^+)^\eta$ and by the fact that the region $[-\pi,\pi]^\eta \setminus (-\varepsilon,\varepsilon)^\eta$ is compact and by continuity argument we have that there exists a constant $\tau \in \mathbb{R}^+$ such that

$$\frac{\sum_{\boldsymbol{k}\neq\boldsymbol{l}} F_{\boldsymbol{k}}F_{\boldsymbol{l}}\boldsymbol{r}^{\boldsymbol{k}+\boldsymbol{l}}\left[1-\cos\left((\boldsymbol{k}-\boldsymbol{l})^T\boldsymbol{\theta}\right)\right]}{F(\boldsymbol{r})} > \tau.$$

This proves that the inequality (A.6) is true also for $\boldsymbol{\theta} \in [-\pi,\pi)^\eta \setminus (-\varepsilon,\varepsilon)^\eta$.

It follows from inequality (A.6) that $\forall\boldsymbol{\theta} \in [-\pi,\pi)^\eta \setminus [-n^{-2/5}, n^{-2/5}]$

$$\left|\frac{F\left(\boldsymbol{r}\mathrm{e}^{\mathrm{j}\boldsymbol{\theta}}\right)}{F(\boldsymbol{r})}\right|^n \leq \left(1-\chi||\boldsymbol{\theta}||_2^2\right)^{n/2} \leq \mathrm{e}^{-\chi n^{1/5}} \leq \chi n^{-1/5}.$$

□

A.2 Proof of Theorem 3.4

In this subsection we split the proof of Theorem 3.4 into two parts. The first considers the case with $\langle\mathscr{F}\rangle = \mathbb{Z}^\eta$. Otherwise, if $\langle\mathscr{F}\rangle = \mathbb{Z}^\nu \subset \mathbb{Z}^\eta$, the saddle point approximation cannot be applied directly to the generating function. However, in the second part of the proof we show that we can reformulate the problem in such a way the conditions, required to apply the saddle point method, are satisfied.

Proof of Theorem 3.4

Proof of Theorem 3.4 with $\langle \mathscr{F} \rangle = \mathbb{Z}^\eta$. From Lemma A.2 we know that there exists a unique solution $\widetilde{\boldsymbol{x}} \in \Sigma^+ = (\mathbb{R}^+)^\eta \cap \Sigma$ to $\Delta(\boldsymbol{x}) = \boldsymbol{\omega}$, where $\Delta = \Delta[F]$ is defined in (3.21). By the residue theorem and by choosing the integration surface to be a sphere of radius $\widetilde{\boldsymbol{x}}$ we have

$$\begin{aligned}
&\operatorname{coeff}\left\{S(\boldsymbol{x})[F(\boldsymbol{x})]^{\alpha_n n}, \boldsymbol{\omega}_n \alpha_n n\right\} \\
&\quad = \frac{1}{(2\pi)^\eta} \int_{[-\pi,\pi]^\eta} S\left(\widetilde{\boldsymbol{x}} \mathrm{e}^{\mathrm{j}\boldsymbol{\theta}}\right) \frac{F\left(\widetilde{\boldsymbol{x}} \mathrm{e}^{\mathrm{j}\boldsymbol{\theta}}\right)^{\alpha_n n}}{\widetilde{\boldsymbol{x}}^{\alpha_n n \boldsymbol{\omega}_n} \mathrm{e}^{\mathrm{j}\alpha_n n \boldsymbol{\theta}^T \boldsymbol{\omega}_n}} \mathrm{d}\boldsymbol{\theta} \\
&\quad = \frac{1}{(2\pi)^\eta} S(\widetilde{\boldsymbol{x}}) \frac{F\left(\widetilde{\boldsymbol{x}}\right)^{\alpha_n n}}{\widetilde{\boldsymbol{x}}^{\alpha_n n \boldsymbol{\omega}}} \int_{[-\pi,\pi]^\eta} \frac{S\left(\widetilde{\boldsymbol{x}} \mathrm{e}^{\mathrm{j}\boldsymbol{\theta}}\right)}{S\left(\widetilde{\boldsymbol{x}}\right)} \frac{F\left(\widetilde{\boldsymbol{x}} \mathrm{e}^{\mathrm{j}\boldsymbol{\theta}}\right)^{\alpha_n n}}{F\left(\widetilde{\boldsymbol{x}}\right)^{\alpha_n n}} \mathrm{e}^{-\mathrm{j}\alpha_n n \boldsymbol{\theta}^T \boldsymbol{\omega}_n} \mathrm{d}\boldsymbol{\theta}.
\end{aligned}$$

By splitting the integration region $[-\pi, \pi]^\eta$ into $\Theta = \left[-(\alpha_n n)^{-2/5}, (\alpha_n n)^{-2/5}\right]^\eta$ and its complement $[-\pi, \pi]^\eta \setminus \Theta$:

$$\begin{aligned}
&\operatorname{coeff}\left\{S(\boldsymbol{x})[F(\boldsymbol{x})]^{\alpha_n n}, \boldsymbol{\omega}_n \alpha_n n\right\} \\
&\quad = S(\boldsymbol{x}) \frac{F\left(\widetilde{\boldsymbol{x}}\right)^{\alpha_n n}}{\widetilde{\boldsymbol{x}}^{\alpha_n n \boldsymbol{\omega}_n}} \left[\frac{1}{(2\pi)^\eta} \int_{[-\pi,\pi]^\eta \setminus \Theta} \frac{S\left(\widetilde{\boldsymbol{x}} \mathrm{e}^{\mathrm{j}\boldsymbol{\theta}}\right)}{S\left(\widetilde{\boldsymbol{x}}\right)} \frac{F\left(\widetilde{\boldsymbol{x}} \mathrm{e}^{\mathrm{j}\boldsymbol{\theta}}\right)^{\alpha_n n}}{F\left(\widetilde{\boldsymbol{x}}\right)^{\alpha_n n}} \mathrm{e}^{-\mathrm{j}n\alpha_n \boldsymbol{\theta}^T \boldsymbol{\omega}_n} \mathrm{d}\boldsymbol{\theta} \right. \\
&\quad \left. + \frac{1}{(2\pi)^\eta} \int_{\Theta} \frac{S\left(\widetilde{\boldsymbol{x}} \mathrm{e}^{\mathrm{j}\boldsymbol{\theta}}\right)}{S\left(\widetilde{\boldsymbol{x}}\right)} \frac{F\left(\widetilde{\boldsymbol{x}} \mathrm{e}^{\mathrm{j}\boldsymbol{\theta}}\right)^{\alpha_n n}}{F\left(\widetilde{\boldsymbol{x}}\right)^{\alpha_n n}} \mathrm{e}^{-\mathrm{j}\alpha_n n \boldsymbol{\theta}^T \boldsymbol{\omega}_n} \mathrm{d}\boldsymbol{\theta} \right].
\end{aligned}$$

From Lemma A.4 there exists a constant χ such that $\left|F\left(\widetilde{\boldsymbol{x}} \mathrm{e}^{\mathrm{j}\boldsymbol{\theta}}\right)/F\left(\widetilde{\boldsymbol{x}}\right)\right| \leq \chi n^{-1/5}$ and from inequality (A.6) we have also $\left|S\left(\widetilde{\boldsymbol{x}} \mathrm{e}^{\mathrm{j}\boldsymbol{\theta}}\right)/S\left(\widetilde{\boldsymbol{x}}\right)\right| < 1$. It follows that

$$\begin{aligned}
&\left| \frac{1}{(2\pi)^\eta} \int_{[-\pi,\pi]^\eta \setminus \Theta} \frac{S\left(\widetilde{\boldsymbol{x}} \mathrm{e}^{\mathrm{j}\boldsymbol{\theta}}\right)}{S\left(\widetilde{\boldsymbol{x}}\right)} \frac{F\left(\widetilde{\boldsymbol{x}} \mathrm{e}^{\mathrm{j}\boldsymbol{\theta}}\right)^{\alpha_n n}}{F\left(\widetilde{\boldsymbol{x}}\right)^{\alpha_n n}} \mathrm{e}^{-\mathrm{j}\alpha_n n \boldsymbol{\theta}^T \boldsymbol{\omega}_n} \mathrm{d}\boldsymbol{\theta} \right| \\
&\quad \leq \frac{1}{(2\pi)^\eta} \int_{[-\pi,\pi]^\eta \setminus \Theta} \left| \frac{S\left(\widetilde{\boldsymbol{x}} \mathrm{e}^{\mathrm{j}\boldsymbol{\theta}}\right)}{S\left(\widetilde{\boldsymbol{x}}\right)} \right| \left| \frac{F\left(\widetilde{\boldsymbol{x}} \mathrm{e}^{\mathrm{j}\boldsymbol{\theta}}\right)}{F\left(\widetilde{\boldsymbol{x}}\right)} \right|^{\alpha_n n} \mathrm{d}\boldsymbol{\theta} = O\left(n^{-1/5}\right),
\end{aligned}$$

and the contribution to the integral from the region $[-\pi, \pi]^\eta \setminus \Theta$ is negligible.

On the other hand, by expanding the function $\ln\left(F\left(\widetilde{\boldsymbol{x}} \mathrm{e}^{\mathrm{j}\boldsymbol{\theta}}\right)/F\left(\widetilde{\boldsymbol{x}}\right)\right)$ up to second order terms we have

$$\begin{aligned}
&\frac{1}{(2\pi)^\eta} \int_{\Theta} \frac{S\left(\widetilde{\boldsymbol{x}} \mathrm{e}^{\mathrm{j}\boldsymbol{\theta}}\right)}{S\left(\widetilde{\boldsymbol{x}}\right)} \frac{F\left(\widetilde{\boldsymbol{x}} \mathrm{e}^{\mathrm{j}\boldsymbol{\theta}}\right)^{\alpha_n n}}{F\left(\widetilde{\boldsymbol{x}}\right)^{\alpha_n n}} \mathrm{e}^{-\mathrm{j}\alpha_n n \boldsymbol{\theta}^T \boldsymbol{\omega}_n} \mathrm{d}\boldsymbol{\theta} = \\
&= \frac{1}{(2\pi)^\eta} \int_{\Theta} \mathrm{e}^{\mathrm{j}\boldsymbol{\theta}^T \boldsymbol{\Delta}[S](\widetilde{\boldsymbol{x}}) - \frac{1}{2}\boldsymbol{\theta}^T \boldsymbol{\Gamma}[S](\widetilde{\boldsymbol{x}})\boldsymbol{\theta} + O(||\boldsymbol{\theta}||^3) + \mathrm{j}\alpha_n n \boldsymbol{\theta}^T \boldsymbol{\Delta}[F](\widetilde{\boldsymbol{x}}) - \frac{\alpha_n n}{2}\boldsymbol{\theta}^T \boldsymbol{\Gamma}[F](\widetilde{\boldsymbol{x}})\boldsymbol{\theta} + \alpha_n n O(||\boldsymbol{\theta}||^3)} \times \\
&\times \mathrm{e}^{-\mathrm{j}\alpha_n n \boldsymbol{\theta}^T \boldsymbol{\omega}_n} \mathrm{d}\boldsymbol{\theta} \\
&= \frac{1}{(2\pi)^\eta} \int_{\Theta} \mathrm{e}^{\mathrm{j}\boldsymbol{\theta}^T \boldsymbol{\Delta}[S](\widetilde{\boldsymbol{x}}) - \frac{1}{2}\boldsymbol{\theta}^T \boldsymbol{\Gamma}[S](\widetilde{\boldsymbol{x}})\boldsymbol{\theta} + O(||\boldsymbol{\theta}||^3) - \frac{\alpha_n n}{2}\boldsymbol{\theta}^T \boldsymbol{\Gamma}[F](\widetilde{\boldsymbol{x}})\boldsymbol{\theta} + \alpha_n n O(||\boldsymbol{\theta}||^3)} \times \\
&\times \mathrm{e}^{-\mathrm{j}\alpha_n n \boldsymbol{\theta}^T (\boldsymbol{\omega}_n - \boldsymbol{\omega})} \mathrm{d}\boldsymbol{\theta}
\end{aligned}$$

where the last equality follows from $\mathbf{\Delta}[F](\widetilde{\boldsymbol{x}}) = \boldsymbol{\omega}$.

Notice that $\alpha_n n ||\boldsymbol{\theta}||^3 = O(n^{-1/5})$ if $\boldsymbol{\theta} \in \Theta = [-(\alpha_n)^{-2/5}, (\alpha_n)^{-2/5}]$. Since $\mathbf{\Gamma}[S](\widetilde{\boldsymbol{x}})$ is symmetric definite positive (see Lemma A.3) then there exist $\mathbf{P}, \mathbf{\Lambda}$ such that $\mathbf{\Gamma}[S] = \mathbf{P}^T \mathbf{\Lambda} \mathbf{P}$ where $\mathbf{\Lambda}$ is a diagonal matrix with positive entries $\{\lambda_i\}_{i=1}^{\eta}$ and

$$\frac{1}{2}\boldsymbol{\theta}^T \mathbf{\Gamma}[S](\widetilde{\boldsymbol{x}})\boldsymbol{\theta} = \frac{1}{2}\boldsymbol{\theta}^T \mathbf{P}^T \mathbf{\Lambda} \mathbf{P} \boldsymbol{\theta} = \frac{1}{2}\sum_i \lambda_i ||(\mathbf{P}\boldsymbol{\theta})_i||_2^2 = O(n^{-4/5}) = O(n^{-1/5}).$$

We get

$$\begin{aligned}
&\frac{1}{(2\pi)^\eta}\int_\Theta \frac{S\left(\widetilde{\boldsymbol{x}}\mathrm{e}^{\mathrm{j}\boldsymbol{\theta}}\right)}{S\left(\widetilde{\boldsymbol{x}}\right)} \frac{F\left(\widetilde{\boldsymbol{x}}\mathrm{e}^{\mathrm{j}\boldsymbol{\theta}}\right)^{\alpha_n n}}{F\left(\widetilde{\boldsymbol{x}}\right)^{\alpha_n n}} \mathrm{e}^{-\mathrm{j}\alpha_n n \boldsymbol{\theta}^T \boldsymbol{\omega}_n} \mathrm{d}\boldsymbol{\theta} = \\
&= \frac{1}{(2\pi)^\eta}\int_\Theta \mathrm{e}^{-\frac{\alpha_n n}{2}\boldsymbol{\theta}^T \mathbf{\Gamma}[F](\widetilde{\boldsymbol{x}})\boldsymbol{\theta} + O(n^{-1/5}) - \mathrm{j}[\alpha_n n \boldsymbol{\theta}^T(\boldsymbol{\omega}_n - \boldsymbol{\omega}) - \boldsymbol{\theta}^T \mathbf{\Delta}[S](\widetilde{\boldsymbol{x}})]} \mathrm{d}\boldsymbol{\theta} \\
&= \frac{1}{(2\pi)^\eta}\int_\Theta \mathrm{e}^{-\frac{\alpha_n n}{2}\boldsymbol{\theta}^T \mathbf{\Gamma}[F](\widetilde{\boldsymbol{x}})\boldsymbol{\theta} - \mathrm{j}[\alpha_n n \boldsymbol{\theta}^T(\boldsymbol{\omega}_n - \boldsymbol{\omega}) - \boldsymbol{\theta}^T \mathbf{\Delta}[S](\widetilde{\boldsymbol{x}})]} \left(1 + O\left(n^{-1/5}\right)\right) \mathrm{d}\boldsymbol{\theta}.
\end{aligned}$$

By defining $\boldsymbol{\sigma} = \sqrt{\alpha_n n}\boldsymbol{\theta}$ and $\Sigma = \left[-(\alpha_n n)^{1/10}, (\alpha_n n)^{1/10}\right]^\eta$ we get that

$$\begin{aligned}
&\frac{1}{(2\pi)^\eta}\int_\Theta \frac{S\left(\widetilde{\boldsymbol{x}}\mathrm{e}^{\mathrm{j}\boldsymbol{\theta}}\right)}{S\left(\widetilde{\boldsymbol{x}}\right)} \frac{F\left(\widetilde{\boldsymbol{x}}\mathrm{e}^{\mathrm{j}\boldsymbol{\theta}}\right)^{\alpha_n n}}{F\left(\widetilde{\boldsymbol{x}}\right)^{\alpha_n n}} \mathrm{e}^{-\mathrm{j}\alpha_n n \boldsymbol{\theta}^T \boldsymbol{\omega}_n} \mathrm{d}\boldsymbol{\theta} = \\
&= (\alpha_n n)^{-\eta/2} \frac{\left(1 + O\left(n^{-1/5}\right)\right)}{(2\pi)^\eta} \int_\Sigma \mathrm{e}^{-\frac{1}{2}\boldsymbol{\sigma}^T \mathbf{\Gamma}(\widetilde{\boldsymbol{x}})\boldsymbol{\sigma} - \mathrm{j}[\sqrt{\alpha_n n}\boldsymbol{\sigma}^T(\boldsymbol{\omega}_n - \boldsymbol{\omega}) - \frac{1}{\sqrt{\alpha_n n}}\boldsymbol{\sigma}^T \mathbf{\Delta}[S](\widetilde{\boldsymbol{x}})]} \mathrm{d}\boldsymbol{\sigma} \\
&= \frac{\left(1 + O\left(n^{-1/5}\right)\right)}{\sqrt{(2\pi\alpha_n n)^\eta |\mathbf{\Gamma}(\widetilde{\boldsymbol{x}})|}} \int_\Sigma \sqrt{\frac{|\mathbf{\Gamma}(\widetilde{\boldsymbol{x}})|}{(2\pi)^\eta}} \mathrm{e}^{-\frac{1}{2}\boldsymbol{\sigma}^T \mathbf{\Gamma}(\widetilde{\boldsymbol{x}})\boldsymbol{\sigma} - \mathrm{j}[\sqrt{\alpha_n n}\boldsymbol{\sigma}^T(\boldsymbol{\omega}_n - \boldsymbol{\omega}) - \frac{1}{\sqrt{\alpha_n n}}\boldsymbol{\sigma}^T \mathbf{\Delta}[S](\widetilde{\boldsymbol{x}})]} \mathrm{d}\boldsymbol{\sigma} \\
&= \frac{\left(1 + O\left(n^{-1/5}\right)\right)}{\sqrt{(2\pi\alpha_n n)^\eta |\mathbf{\Gamma}(\widetilde{\boldsymbol{x}})|}} \Bigg[\int_{\mathbb{R}^\eta} \sqrt{\frac{|\mathbf{\Gamma}(\widetilde{\boldsymbol{x}})|}{(2\pi)^\eta}} \mathrm{e}^{-\frac{1}{2}\boldsymbol{\sigma}^T \mathbf{\Gamma}(\widetilde{\boldsymbol{x}})\boldsymbol{\sigma} - \mathrm{j}[\sqrt{\alpha_n n}\boldsymbol{\sigma}^T(\boldsymbol{\omega}_n - \boldsymbol{\omega}) - \frac{1}{\sqrt{\alpha_n n}}\boldsymbol{\sigma}^T \mathbf{\Delta}[S](\widetilde{\boldsymbol{x}})]} \mathrm{d}\boldsymbol{\sigma} \\
&- \int_{\mathbb{R}^\eta \setminus \Sigma} \sqrt{\frac{|\mathbf{\Gamma}(\widetilde{\boldsymbol{x}})|}{(2\pi)^\eta}} \mathrm{e}^{-\frac{1}{2}\boldsymbol{\sigma}^T \mathbf{\Gamma}(\widetilde{\boldsymbol{x}})\boldsymbol{\sigma} - \mathrm{j}[\sqrt{\alpha_n n}\boldsymbol{\sigma}^T(\boldsymbol{\omega}_n - \boldsymbol{\omega}) - \frac{1}{\sqrt{\alpha_n n}}\boldsymbol{\sigma}^T \mathbf{\Delta}[S](\widetilde{\boldsymbol{x}})]} \mathrm{d}\boldsymbol{\sigma}\Bigg] \\
&= \frac{\left(1 + O\left(n^{-1/5}\right)\right)}{\sqrt{(2\pi\alpha_n n)^\eta |\mathbf{\Gamma}(\widetilde{\boldsymbol{x}})|}} \Big[\mathrm{e}^{-\frac{1}{2}\alpha_n n(\boldsymbol{\omega}_n - \boldsymbol{\omega})^T \mathbf{\Gamma}^{-1}(\widetilde{\boldsymbol{x}})(\boldsymbol{\omega}_n - \boldsymbol{\omega})} \\
&- \int_{\mathbb{R}^\eta \setminus \Sigma} \sqrt{\frac{|\mathbf{\Gamma}(\widetilde{\boldsymbol{x}})|}{(2\pi)^\eta}} \mathrm{e}^{-\frac{1}{2}\boldsymbol{\sigma}^T \mathbf{\Gamma}(\widetilde{\boldsymbol{x}})\boldsymbol{\sigma} - \mathrm{j}[\sqrt{\alpha_n n}\boldsymbol{\sigma}^T(\boldsymbol{\omega}_n - \boldsymbol{\omega}) - \frac{1}{\sqrt{\alpha_n n}}\boldsymbol{\sigma}^T \mathbf{\Delta}[S](\widetilde{\boldsymbol{x}})]} \mathrm{d}\boldsymbol{\sigma}\Bigg].
\end{aligned}$$

Since $\mathbf{\Gamma}[F](\widetilde{\boldsymbol{x}})$ is symmetric definite positive (see Lemma A.3) then there exist $\mathbf{Q}, \mathbf{D}$ such that $\mathbf{\Gamma} = \mathbf{Q}^{\mathbf{T}}\mathbf{D}\mathbf{Q}$ where $\mathbf{D}$ is a diagonal matrix with positive entries $\{D_i\}_{i=1}^{\eta}$ and $D_{\min} = \min_i D_i$. Then, by defining $\boldsymbol{y} = \mathbf{Q}\boldsymbol{\sigma}$, we have

$$\left| \int_{\mathbb{R}^\eta \setminus \left[-(\alpha_n n)^{1/10}, (\alpha_n n)^{1/10}\right]^\eta} \mathrm{e}^{-\frac{1}{2}\boldsymbol{\sigma}^T \boldsymbol{\Gamma}(\widetilde{\boldsymbol{x}})\boldsymbol{\sigma} - \mathrm{j}[\sqrt{\alpha_n n}\boldsymbol{\sigma}^T(\boldsymbol{\omega}_n - \boldsymbol{\omega}) - \frac{1}{\sqrt{\alpha_n n}}\boldsymbol{\sigma}^T \boldsymbol{\Delta}[S](\widetilde{\boldsymbol{x}})]} \mathrm{d}\boldsymbol{\sigma} \right|$$
$$\leq \int_{||\boldsymbol{y}||^2 \geq (\alpha_n n)^{1/10}} \mathrm{e}^{-\frac{1}{2}D_{\min}||\boldsymbol{y}||^2} \mathrm{d}\boldsymbol{y} = O\left(\frac{\mathrm{e}^{-(\alpha_n n)^{1/5}}}{(\alpha_n n)^{1/10}}\right) = O(n^{-1/10}).$$

We get that

$$\frac{1}{(2\pi)^\eta} \int_\Theta \frac{S\left(\widetilde{\boldsymbol{x}}\mathrm{e}^{\mathrm{j}\boldsymbol{\theta}}\right)}{S\left(\widetilde{\boldsymbol{x}}\right)} \frac{F\left(\widetilde{\boldsymbol{x}}\mathrm{e}^{\mathrm{j}\boldsymbol{\theta}}\right)^{\alpha_n n}}{F\left(\widetilde{\boldsymbol{x}}\right)^{\alpha_n n}} \mathrm{e}^{-\mathrm{j}\alpha_n n \boldsymbol{\omega}_n \boldsymbol{\theta}^T} \mathrm{d}\boldsymbol{\theta}$$
$$\leq \frac{\left(1 + O\left(n^{-1/5}\right)\right)}{\sqrt{(2\pi\alpha_n n)^\eta |\boldsymbol{\Gamma}(\widetilde{\boldsymbol{x}})|}} \left[\mathrm{e}^{-\frac{1}{2}\alpha_n n D_{\min}^{-1}||\boldsymbol{\omega}_n - \boldsymbol{\omega}||^2} + O(n^{-1/10})\right]$$
$$= \frac{\left(1 + O\left(n^{-1/5}\right)\right)}{\sqrt{(2\pi\alpha_n n)^\eta |\boldsymbol{\Gamma}(\widetilde{\boldsymbol{x}})|}} \left[\mathrm{e}^{O\left(\frac{1}{n}\right)} + O(n^{-1/10})\right]$$
$$\frac{\left(1 + O\left(n^{-1/5}\right)\right)}{\sqrt{(2\pi\alpha_n n)^\eta |\boldsymbol{\Gamma}(\widetilde{\boldsymbol{x}})|}} \left[1 + O(n^{-1/10})\right]$$

and we conclude that for $n \to \infty$

$$\operatorname{coeff}\left\{S(\boldsymbol{x})[F(\boldsymbol{x})]^{\alpha_n n}, \boldsymbol{\omega}_n \alpha_n n\right\} = \frac{S(\widetilde{\boldsymbol{x}})}{\sqrt{(2\pi\alpha_n n)^\eta |\boldsymbol{\Gamma}[F](\widetilde{\boldsymbol{x}})|}} \frac{F(\widetilde{\boldsymbol{x}})^{\alpha_n n}}{\widetilde{\boldsymbol{x}}^{\boldsymbol{\omega}_n \alpha_n n}}(1 + o(1))$$

and

$$\lim_{n \in \mathcal{N}} \frac{1}{n} \ln\left(\operatorname{coeff}\{S(\widetilde{\boldsymbol{x}})[F(\boldsymbol{x})]^{\alpha_n n}, \boldsymbol{x}^{\boldsymbol{\omega}_n \alpha_n n}\}\right) = \alpha \ln F(\widetilde{\boldsymbol{x}}) - \alpha\ \boldsymbol{\omega} \cdot \ln \widetilde{\boldsymbol{x}}$$

Notice that $o(1)$ is independent on $\boldsymbol{\omega}_n$ and the convergence in (3.23) is uniform in $\boldsymbol{\omega} \in \overset{\circ}{\operatorname{co}}(\mathscr{F})$.

□

Proof of Theorem 3.4 with $\langle\mathscr{F}\rangle \subset \mathbb{Z}^\eta$. If $\langle\mathscr{F}\rangle \subset \mathbb{Z}^\eta$ then the saddle point approximation cannot be applied directly to the function $B(\boldsymbol{x}) = S(\boldsymbol{x})[F(\boldsymbol{x})]^{\alpha_n n}$.

Since submodules of free modules over a Noetherian ring are free [81], there exists a basis $\mathcal{B} = \{\boldsymbol{b}^1, \ldots, \boldsymbol{b}^\nu\}$ with $|\mathcal{B}| = \nu \leq \eta$ of $\langle\mathscr{F}\rangle$ and every element in $\mathscr{F}$ can be expressed in a unique way as a finite sum of elements in $\mathcal{B}$ multiplied by coefficients in $\mathbb{Z}$:

$$\boldsymbol{k} = \sum_{\boldsymbol{b} \in \mathcal{B}} \gamma_{\boldsymbol{b}}(\boldsymbol{k})\boldsymbol{b}, \qquad \boldsymbol{k} \in \mathscr{F}.$$

From hypothesis also elements in $\mathscr{S} = \{\boldsymbol{l} | S_{\boldsymbol{l}} > 0\}$ can be written as combination of basis elements:

$$\boldsymbol{l} = \sum_{\boldsymbol{b} \in \mathcal{B}} \gamma_{\boldsymbol{b}}(\boldsymbol{l})\boldsymbol{b}, \qquad \boldsymbol{l} \in \mathscr{S}.$$

Define $\boldsymbol{w}_{\boldsymbol{b}} = \boldsymbol{x}^{\boldsymbol{b}}$, $\forall \boldsymbol{b} \in \mathcal{B}$, set $G_{\boldsymbol{\gamma}(\boldsymbol{k})} = F_{\boldsymbol{k}}$, $T_{\boldsymbol{\gamma}(\boldsymbol{l})} = S_{\boldsymbol{l}}$ and let $\mathscr{G} = \{\boldsymbol{\gamma} \in \mathbb{Z}^{\nu} : G_{\boldsymbol{\gamma}} > 0\}$.

Then we have

$$\begin{aligned} F(\boldsymbol{x}) &= \sum_{\boldsymbol{k}\in\mathscr{F}} F_{\boldsymbol{k}} \boldsymbol{x}^{\boldsymbol{k}} = \sum_{\boldsymbol{\gamma}\in\mathscr{G}} G_{\boldsymbol{\gamma}} \boldsymbol{x}^{\sum_{\boldsymbol{b}\in\mathcal{B}} \gamma_{\boldsymbol{b}} \boldsymbol{b}} = \sum_{\boldsymbol{\gamma}\in\mathscr{G}} G_{\boldsymbol{\gamma}} \prod_{\boldsymbol{b}\in\mathcal{B}} \boldsymbol{x}^{\gamma_{\boldsymbol{b}} \boldsymbol{b}} \\ &= \sum_{\boldsymbol{\gamma}\in\mathscr{G}} G_{\boldsymbol{\gamma}} \prod_{\boldsymbol{b}\in\mathcal{B}} \left(\boldsymbol{x}^{\boldsymbol{b}}\right)^{\gamma_{\boldsymbol{b}}} = \sum_{\boldsymbol{\gamma}\in\mathscr{G}} G_{\boldsymbol{\gamma}} \boldsymbol{w}^{\boldsymbol{\gamma}} = G(\boldsymbol{w}). \end{aligned}$$

and for the same reason $S(\boldsymbol{x}) = T(\boldsymbol{w})$.

If $\boldsymbol{k} \in \mathscr{B}$ then there exists $\boldsymbol{q} \in \mathscr{S}$ such that $\boldsymbol{k} = \sum_{\boldsymbol{l}\in\mathscr{F}} a_{\boldsymbol{l}} \boldsymbol{l} + \boldsymbol{q}$ with $\sum_{\boldsymbol{l}\in\mathscr{F}} a_{\boldsymbol{l}} = \alpha_n n$ and, equivalently,

$$\boldsymbol{k} = \sum_{\boldsymbol{l}\in\mathscr{F}} a_{\boldsymbol{l}} \sum_{\boldsymbol{b}\in\mathcal{B}} \gamma_{\boldsymbol{b}}(\boldsymbol{l}) \boldsymbol{b} + \sum_{\boldsymbol{b}\in\mathcal{B}} \gamma_{\boldsymbol{b}}(\boldsymbol{q}) \boldsymbol{b} = \sum_{\boldsymbol{b}\in\mathcal{B}} \sum_{\boldsymbol{l}\in\mathscr{F}} a_{\boldsymbol{l}} [\gamma_{\boldsymbol{b}}(\boldsymbol{l}) + \gamma_{\boldsymbol{b}}(\boldsymbol{q})] \boldsymbol{b}$$

with $\sum_{\boldsymbol{l}\in\mathscr{F}} a_{\boldsymbol{l}} = \alpha_n n$. Let

$$\xi_{n,\boldsymbol{b}} = (\alpha_n n)^{-1} \sum_{\boldsymbol{l}\in\mathscr{F}} a_{\boldsymbol{l}} [\gamma_{\boldsymbol{b}}(\boldsymbol{l}) + \gamma_{\boldsymbol{b}}(\boldsymbol{q})],$$

then

$$\operatorname{coeff}\left\{S(\boldsymbol{x})[F(\boldsymbol{x})]^{\alpha_n n}, \boldsymbol{x}^{\boldsymbol{\omega}_n \alpha_n n}\right\} = \operatorname{coeff}\left\{T(\boldsymbol{w})[G(\boldsymbol{w})]^{\alpha_n n}, \boldsymbol{w}^{\boldsymbol{\xi}_n \alpha_n n}\right\}.$$

If $\boldsymbol{\omega}_n \to \boldsymbol{\omega}$ when $n \to \infty$ then $\boldsymbol{\xi}_n$ is a convergent sequence to $\boldsymbol{\xi}$ where $\boldsymbol{\xi}$ satisfies $\sum_{\boldsymbol{b}\in\mathcal{B}} \xi_{\boldsymbol{b}} \boldsymbol{b} = \boldsymbol{\omega}$.

It is trivial to see that if $\boldsymbol{\omega} \in \overset{\circ}{\operatorname{co}}(\mathscr{F})$ then $\boldsymbol{\xi} \in \overset{\circ}{\operatorname{co}}(\mathscr{G})$. We conclude by Lemma A.2 that there exists a solution $\widetilde{\boldsymbol{w}} \in (\mathbb{R}^+)^{\nu}$ of $\Delta[G](\boldsymbol{w}) = \boldsymbol{\xi}$.

Moreover we have that since $||\boldsymbol{\omega}_n - \boldsymbol{\omega}|| = O(\frac{1}{n})$ then $||\boldsymbol{\xi}_n - \boldsymbol{\xi}|| = O(\frac{1}{n})$. Since $\langle \mathscr{G} \rangle = \mathbb{Z}^{\nu}$, we can apply multidimensional saddle point method:

$$\operatorname{coeff}\left\{T(\boldsymbol{w})[G(\boldsymbol{w})]^{\alpha_n n}, \boldsymbol{w}^{\boldsymbol{\xi}_n \alpha_n n}\right\} = \frac{T(\widetilde{\boldsymbol{w}})}{\sqrt{(2\pi\alpha_n n)^{\nu} |\boldsymbol{\Gamma}[G](\widetilde{\boldsymbol{w}})|}} \frac{[G(\widetilde{\boldsymbol{w}})]^{\alpha_n n}}{\widetilde{\boldsymbol{w}}^{\boldsymbol{\xi}_n \alpha_n n}} (1+o(1)) \quad n \to \infty.$$

and

$$\lim_{n\to\infty} \frac{1}{n} \ln \operatorname{coeff}\left\{T(\boldsymbol{w})[G(\boldsymbol{w})]^{\alpha_n n}, \boldsymbol{w}^{\boldsymbol{\xi}_n \alpha_n n}\right\} = \alpha \ln G(\widetilde{\boldsymbol{w}}) - \alpha \, \boldsymbol{\xi} \cdot \ln \widetilde{\boldsymbol{w}}. \tag{A.7}$$

Since $\widetilde{\boldsymbol{w}}$ is solution of $\Delta[G](\boldsymbol{w}) = \boldsymbol{\xi}$, we get

$$\sum_{i=1}^{\nu} \Delta_i[G](\widetilde{\boldsymbol{w}}) \boldsymbol{b}^{(i)} = \sum_{i=1}^{\nu} \frac{\widetilde{w}_i}{G(\widetilde{\boldsymbol{w}})} \frac{\partial G}{\partial w_i}\bigg|_{\widetilde{\boldsymbol{w}}} \boldsymbol{b}^{(i)} = \boldsymbol{\omega}$$

from which we get that $\forall j = 1, \ldots, \eta$

$$\sum_{i=1}^{\nu} \frac{\widetilde{w}_i}{G(\widetilde{\boldsymbol{w}})} \frac{\partial G}{\partial w_i}\bigg|_{\widetilde{\boldsymbol{w}}} b_j^{(i)} = \frac{x_j}{F(\boldsymbol{x})} \sum_{i=1}^{\nu} \frac{\partial G}{\partial w_i} \frac{\boldsymbol{x}^{\boldsymbol{b}^{(i)}} b_j^{(i)}}{x_j} = \frac{x_j}{F(\boldsymbol{x})} \sum_{i=1}^{\nu} \frac{\partial G}{\partial w_i} \frac{\partial w_i}{\partial x_j} = \frac{x_j}{F(\boldsymbol{x})} \frac{\partial F}{\partial x_j} = \omega_j.$$

We conclude that

$$\Delta[G](\widetilde{\boldsymbol{w}}) = \boldsymbol{\xi} \iff \Delta[F](\widetilde{\boldsymbol{x}}) = \boldsymbol{\omega},$$

and for $n \to \infty$

$$\operatorname{coeff}\left\{S(\boldsymbol{x})[F(\boldsymbol{x})]^{\alpha_n n}, \boldsymbol{x}^{\boldsymbol{\xi}_n \alpha_n n}\right\} = \frac{S(\widetilde{\boldsymbol{x}})}{\sqrt{(2\pi\alpha_n n)^\nu |\boldsymbol{\Gamma}[F](\widetilde{\boldsymbol{x}})|}} \frac{[F(\widetilde{\boldsymbol{x}})]^{\alpha_n n}}{\widetilde{\boldsymbol{x}}^{\boldsymbol{\omega}_n \alpha_n n}} (1 + o(1)).$$

$$\begin{aligned}
\lim_{n\to\infty} \operatorname{coeff}\{F(\boldsymbol{x})^{\alpha_n n}, \boldsymbol{x}^{\boldsymbol{\omega}_n \alpha_n n}\} &= \alpha \ln G(\widetilde{\boldsymbol{w}}) - \alpha \sum_{i=1}^{\nu} \xi_i \ln \widetilde{w}_i \\
&= \alpha \ln F(\widetilde{\boldsymbol{x}}) - \alpha \sum_{i=1}^{\nu} \xi_i \ln \widetilde{\boldsymbol{x}}^{\boldsymbol{b}^{(i)}} \\
&= \alpha \ln F(\widetilde{\boldsymbol{x}}) - \alpha \sum_{i=1}^{\nu} \xi_i \ln \left(\prod_{j=1}^{\eta} \widetilde{x}_j^{b_j^{(i)}} \right) \\
&= \alpha \ln F(\widetilde{\boldsymbol{x}}) - \alpha \sum_{i=1}^{\nu} \xi_i \sum_{j=1}^{\eta} b_j^{(i)} \ln \widetilde{x}_j \\
&= \alpha \ln F(\widetilde{\boldsymbol{x}}) - \alpha \sum_{j=1}^{\eta} \ln(\widetilde{x}_j) \sum_{i=1}^{\nu} \xi_i b_j^i \\
&= \alpha \ln F(\widetilde{\boldsymbol{x}}) - \alpha \boldsymbol{\omega} \cdot \ln \widetilde{\boldsymbol{x}}.
\end{aligned}$$

□

Bibliography

[1] C. E. Shannon, "A mathematical theory of communication," *Bell System Technical Journal*, no. 27, pp. 379–423 and 623–656, October 1948.

[2] ——, "Certain results in coding theory for noisy channels," *Information and control*, no. 1, pp. 6–25, 1957.

[3] R. M. Fano, *Transmission of information. A Statistical Theory of Communication.* The M.I.T. Press and John Wiley & Sons, 1961.

[4] N. Alon and J. H. Spencer, *The probabilistic method.* Wiley, New York, 2000.

[5] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes.* North Holland, 1988.

[6] G. D. Forney, "Convolutional codes I: Algebraic structure," *IEEE Trans. on Inform. Theory*, vol. 16, 1970.

[7] ——, "Convolutional codes II: Maximum-likelihood decoding," *Inform. Contr.*, vol. 25, 1974.

[8] ——, "Convolutional codes III: Sequential decoding," *Inform. Contr.*, vol. 25, 1974.

[9] C. Berrou, A. Glavieux, and P. Thitimajshima, "Near Shannon limit error-correcting coding and decoding: Turbo codes," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Geneva, Switzerland, May 1993.

[10] C. Berrou and A. Glavieux, "Near optimum error correcting coding and decoding: turbo-codes," *IEEE Trans. Communications*, no. 44, pp. 1261–1271, 1996.

[11] R. G. Gallager, *Low-density parity-check codes.* M.I.T. Press, Cambridge, MA, 1963.

[12] D. J. C. MacKay and R. M. Neal, "Good codes based on very sparse matrices," *Cryptography and coding. 5th IMA Conf., LNCS 1025.*, pp. 100–111. Berlin: Springer, 1995.

[13] R. J. McEliece, D. J. C. MacKay, and J. Cheng, "Turbo decoding as an instance of Pearl's "belief propagation" algorithm," *IEEE Journal on selected areas in communications*, vol. 16, no. 2, Feb. 1998.

[14] S. M. Aji and R. J. McEliece, "The generalized distributive law," *IEEE Trans. on Information Theory*, vol. 46, no. 2, March 2000.

[15] S. Benedetto and G. Montorsi, "Design of parallel concatenated convolutional codes," *IEEE Trans. on Information Theory*, vol. 44, no. 5, pp. 591–600, May 1996.

[16] ——, "Unveiling turbo codes: some results on parallel concatenated coding schemes," *IEEE Trans. on Inform. Theory*, vol. 42, no. 2, pp. 409–428, March 1996.

[17] S. Benedetto, D. Divsalar, G. Montorsi, and F. Pollara, "Serial concatenation of interleaved codes: Performance analysis, design, and iterative decoding," *IEEE Trans. on Inform. Theory*, vol. 44, no. 3, pp. 909–926, May 1998.

[18] ——, "Analysis, design, and iterative decoding of double serially concatenated codes with interleavers," *IEEE J. Select. Areas Commun.*, vol. 16, no. 2, pp. 231–244, Feb. 1998.

[19] H. Jin and R. J. McEliece, "Coding theorems for turbo code ensembles," *IEEE Trans. on Inform. Theory*, vol. 48, no. 6, pp. 1451–1461, June 2002.

[20] H. D. Pfister and P. H. Siegel, "Coding theorems for generalized Repeat accumulate codes," in *Proc. of Int. Symp. Inform. Theory and Its Appl.*, vol. 1, Honolulu, HI, USA, Nov. 2000, pp. 21–25.

[21] T. Richardson and R. Urbanke, *Modern coding theory.* Cambridge University Press, 2007.

[22] H. Jin, A. Khandekar, and R. J. McEliece, "Irregular repeat-accumulate codes," in *Proc. of the 2nd International Symposium on Turbo Codes*, Brest, France, September 2000.

[23] H. Jin, "Analysis and design of turbo-like codes," Ph.D. dissertation, Caltech, May 2001.

[24] V. S. Pless and W. C. Huffman, *Handbook of Coding Theory.* Elsevier Science, Amsterdam, Holland, 1998.

[25] R. J. McEliece, *Theory of information and coding.* Cambridge University Press, 2001.

[26] T. Ericson, *Bounds on the Size of a Code (Lecture Notes in Control and Information Sciences)*, G. S.-V. Berlin, Heidelberg, Ed., 1989, vol. 128.

[27] T. Jiang and A. Vardy, "Asymptotic improvement of the Gilbert-Varshamov bound on the size of binary codes," *IEEE Trans. on Inform. Theory*, vol. 50, no. 8, Aug. 2004.

[28] P. Gaborit and G. Zémor, "Asymptotic improvement of the Gilbert-Varshamov bound for binary linear codes," in *IEEE International Symposium on Information Theory*, Seattle, USA, July 2006.

[29] A. Barg and G. Forney, "Random codes: Minimum distances and error exponents," *IEEE Trans. on Inform. Theory*, vol. 48, no. 9, pp. 2568–2573, Sept. 2002.

[30] J. N. Pierce, "Limit distrubution of the minimum distance of random linear codes," *IEEE Trans. on Inform. Theory*, vol. IT-13, no. 4, pp. 595–599, Oct. 1967.

[31] V. Guruswami and P. Indyk, "Efficiently decodable codes meeting Gilbert-Varshamov bound for low rates," in *Proceedings of SODA*, 2004.

[32] T. Kasami, "A Gilbert-Varshamov bound for quasi cyclic codes of rate 1/2," *IEEE Trans. on Inform. Theory*, vol. 48, no. 5, pp. 679–679, 1974.

[33] M. Breiling, "A logarithmic upper bound on the minimum distance of turbo codes," *IEEE Trans. on Inform. Theory*, vol. 50, pp. 1692–1710, 2004.

[34] M. Breiling and J. B. Huber, "Combinatorial analysis of the minimum distance of turbo codes," *IEEE Trans. on Inform. Theory*, vol. 47, pp. 2737–2750, 2001.

[35] A. Perotti and S. Benedetto, "An upper bound on the minimum distance of serially concatenated convolutional codes," *IEEE Trans. Inform. Theory*, vol. 52, no. 12, pp. 5501–5509, Dec. 2006.

[36] N. Kahale and R. Urbanke, "On the minimum distance of parallel and serially concatenated codes," in *Proc. IEEE International Symposium on Information Theory (ISIT '98)*, Cambridge, MA, Aug. 1998.

[37] L. Bazzi, M. Mahdian, and A. Spielman, "The minimum distance of turbo-like codes," *IEEE Trans. on Inform. Theory*, vol. 55, no. 1, pp. 6–15, Jan. 2009.

[38] L. Bazzi and S. Mitter, "Encoding complexity versus minimum distance," *IEEE Trans. on Information Theory*, vol. 50, pp. 2010–2021, 2005.

[39] G. Miller and D. Burshtein, "Asymptotic enumeration methods for analyzing LDPC codes," *IEEE Trans. on Inform. Theory*, vol. 50, no. 6, pp. 1115–1131, Nov. 2004.

[40] R. Gallager, *Information theory and reliable communication.* New York: Wiley, 1968.

[41] S. Litsyn and V. Shevelev., "On ensembles of low-density parity-check codes: Asymptotic distance distributions," *IEEE Trans. on Inform. Theory*, Apr. 2002.

[42] C. Di, T. J. Richardson, and R. L. Urbanke, "Weight distribution of low-density parity-check codes," *IEEE Trans. on Inform. Theory*, vol. 52, no. 11, pp. 4839–4855, Nov. 2006.

[43] V. Rathi, "On the asymptotic weight and stopping set distribution of regular LDPC ensembles," *IEEE Trans. on Inform. Theory*, vol. 52, no. 9, pp. 4212–4218, Sep. 2006.

[44] H. D. Pfister and P. H. Siegel, "The serial concatenation of rate-1 codes through uniform random interleavers," *IEEE Trans. on Inform. Theory*, vol. 49, no. 6, pp. 1425–1438, June 2003.

[45] L. Bazzi, "Minimum Distance of Error Correcting Codes versus Complexity, Simmetry and Pseudorandomness," Ph.D. dissertation, Massachusetts Institute of Technology, Sept. 2003.

[46] H. D. Pfister, "On the capacity of the finite state channels and the analysis of convolutional accumulate-m codes," Ph.D. dissertation, Univ. California, San Diego, La Jolla, 2003.

[47] A. Graell i Amat and R. L. Bidan, "Minimum distance and convergence analysis of Hamming-accumulate-acccumulate codes," *IEEE Trans. on Comm*, vol. 57, no. 12, December 2009.

[48] D. Divsalar, H. Jin, and R. McEliece, "Coding theorems for 'turbo-like codes'," in *Proc. 36th Annu. Allerton Conf. Communication, Control and Computing*, Monticello, IL, September 1998, pp. 201–210.

[49] I. Sason, E. Telatar, and R. Urbanke, "On the asymptotic input output weight distributions and thresholds of convolutional and turbo-like encoders," *IEEE Trans. on Inform. Theory*, vol. 48, no. 12, pp. 3052–3061, December 2002.

[50] R. J. McEliece, *How to compute weight enumerators for convolutional codes.* Communications and Coding, Wiley, New York, NY, USA, 1998.

[51] I. Sason and S. Shamai, "Improved upper bounds on the ML decoding error probability of parallel and serial concatenated turbo codes via their ensemble distance spectrum," *IEEE Trans. on Inform. Theory*, vol. 46, no. 1, pp. 24–47, Jan. 2000.

[52] E. A. Bender, L. B. Richmond, and S. G. Williamson, "Central and local limit theorem applied to asymptotic enumeration III: Matrix recursions," *J. Combin. Theory*, pp. 263–278, 1983.

[53] N. G. de Brujin, *Asymptotic Methods in Analysis.* North Holland, Amsterdam, 1981.

[54] F. Fagnani and C. Ravazzi, "Spectra and minimum distances of Repeat multiple accumulate codes," in *Proc. Inform. Theory and Applications Workshop*, La Jolla, CA, January 2008, pp. 77 – 86.

[55] C. Ravazzi and F. Fagnani, "Spectra and minimum distances of Repeat multiple-accumulate codes," *IEEE Trans. on Inform. Theory*, vol. 55, no. 11, pp. 4905–4924, November 2009.

[56] J. Kliewer, K. S. Zigangirov, and D. J. Costello, "New results on the minimum distance of Repeat multiple accumulate codes," in *Proc. Forty-Fifth Annual Allerton Conference on Communication, Control, and Computing*, Monticello, IL, Sept. 2007.

[57] D. J. Costello, C. Koller, J. Kliewer, and K. S. Zigangirov, "On the distance growth properties of double serially concatenated convolutional codes," in *Proc. Inform. Theory and Applications Workshop*, Jan. 2008.

[58] C. Koller, J. Kliewer, K. S. Zigangirov, and D. J. Costello, "Minimum distance bounds for multiple-serially concatenated code ensembles," in *Proc. IEEE Int. Symp. on Inform. Theory, Toronto, Canada*, July 2008, pp. 1888–1892.

[59] J. Kliewer, K. S. Zigangirov, C. Koller, and D. J. Costello, "Coding theorems for Repeat multiple accumulate codes," *[Online.] Available: arXive.org*, Oct. 2008.

[60] C. Ravazzi and F. Fagnani, "Hayman-like techniques for computing input–output weight distribution of convolutional encoders," in *Proc. IEEE International Symposium on Information Theory*, June 2010.

[61] C. Ravazzi and F. Fagnani, "Minimum distance properties of multiple-serially concatenated codes," in *Proceedings of IEEE International Symposium on 6th International symposium on turbo codes and iterative information processing*, Brest, France, Sept. 2010.

[62] P. Flajolet and R. Sedgewick, *Analytic combinatorics.* Cambridge University Press, Cambridge, UK, 2008.

[63] V. Borkar, *Probability Theory.* New York: Springer-Verlag, 1995.

[64] T. Cover and J. Thomas, *Elements of information theory.* New York: Wiley Series in Telecommunications, 1991.

[65] A. Viterbi and J. Omura, *Principles of digital communications and coding.* McGraw Hill, New York, 1979.

[66] I. J. Good, "Saddle point methods for the multinomial distribution," *Annals of mathematical statistics*, pp. 860–881, 1956.

[67] D. Gardy, "Some results on the asymptotic behavior of coefficients of large powers of functions," *Discrete mathematics*, pp. 189–217, 1993.

[68] R. Johannesson and K. S. Zigangirov, *Fundamentals of Convolutional Coding.* IEEE Press, New York, NY, USA, 1999.

[69] H. Gluesing-Luerssen, "On the weight distribution of convolutional codes," *Linear algebra and its applications*, pp. 298–326, 2005.

[70] S. Lin and D. J. Costello, *Error Control Coding: Fundamentals and Applications.* Prentice Hall, 1983.

[71] P. Fitzpatrick and G. H. Norton, "Linear recurring sequences and the path weight enumerator of a convolutional code," *Electr. Lett*, 1991.

[72] S. Boyd and L. Vandenberghe, *Convex Optimization.* Cambridge Univ. Press, 2004.

[73] O. Y. E. Rosnes, "Turbo decoding on the binary erasure channel: Finite-length analysis and turbo stopping sets," *IEEE Trans. on Inform. Theory*, vol. 53, no. 11, pp. 4059–4075, November 2007.

[74] F. Garin, G. Como, and F. Fagnani, "The performance of serial turbo codes does not concentrate," *Submitted*, 2010.

[75] W. Rudin, *Principles of mathematical analysis.* McGraw-Hill, 1976.

[76] R. T. Rockafellar and R. J. B. Wets, *Variational Analysis.* Springer, 1998, vol. 317.

[77] A. Roumy, S. Guemghar, G. Caire, and S. Verdú, "Design methods for irregular repeat-accumulate codes," *IEEE Trans. on Inform. Theory*, vol. 50, no. 8, Aug. 2005.

[78] F. Garin, G. Como, and F. Fagnani, "Staircase and other structured linear-time encodable LDPC codes: analysis and design," in *Proc. of International Symposium on Information Theory*, Sep. 2007.

[79] H. L. Royden, *Real Analysis.* Prentice Hall, 1998.

[80] W. Rudin, *Fourier Analysis on Groups.* Wiley-Interscience, 1990.

[81] M. Artin, *Algebra.* Prentice Hall, 1991.