ON THE GROWTH RATE OF THE INPUT-OUTPUT WEIGHT DISTRIBUTION OF CONVOLUTIONAL ENCODERS*

CHIARA RAVAZZI† AND FABIO FAGNANI‡

Abstract. In this paper, exact formulæ of the input-output weight distribution function and its exponential growth rate are derived for truncated convolutional encoders. In particular, these weight distribution functions are expressed 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 the truncation lengths and the weights increase. Fortunately, a very accurate asymptotic expansion can be derived using the Multidimensional Saddle-Point method (MSP method). This approximation is substantially easier to evaluate and is used to obtain an expression of the asymptotic spectral function, and to prove continuity and concavity in its domain (convex and closed). Finally, this approach is able to guarantee that the sequence of exponential growth rates converges uniformly to the asymptotic limit, and to estimate the speed of this convergence.

Key words. Asymptotic spectral function, Convolutional coding theory, Controller canonical form, Input-output weight distribution, Maximum-likelihood decoding

AMS subject classifications. 05C21, 05C30, 13F25, 90C27, 94B10, 94B65

1. Introduction.

The estimation of weight enumerators of codes is a crucial issue in the coding theory for both application and theoretical purposes. Weight enumerators are in fact the main ingredients of all expressions that estimate error probabilities and they characterize the correction capability of the code, when maximum likelihood decoding is assumed. An extensive amount of literature exists on the bounds of weight distributions and on their use. The reader can refer to [1,2]. A particularly relevant part of this literature concerns estimating the spectral function of weight enumerators, that is 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 this paper, we focus on the estimation of input-output weight enumerators of *convolutional codes*.

1.1. State of the art.

Convolutional encoders can be considered as finite-state machines with linear updates of the state and of the output. The code sequence that emerges from the encoder depends on the previous message symbols, as well as on the present ones. Although the natural setting considers encoders that map a semi-infinite sequence into a semi-infinite stream, convolutional encoders are used in the main applications with a fixed block-length. Each block is obtained by letting the state machine evolve a finite number of steps, called *truncation lengths*. Truncated convolutional encoders are mainly used in combination with uniform random permutations in both serial and in mixed serial and parallel architectures, in order to construct high-performance schemes, known as *turbo-like codes* [3–6].

*A preliminary version of some of the results has appeared in the proceedings of the IEEE International Symposium on Information Theory 2010, held in Austin, TX, USA.

†C. Ravazzi (corresponding author) is with DET (Dipartimento di Elettronica e Telecomunicazioni), Politecnico di Torino, Corso Duca degli Abruzzi, 24, I-10129 TO (e-mail: chiara.ravazzi@polito.it)

‡F. Fagnani is with DISMA (Dipartimento di Scienze Matematiche) Politecnico di Torino, Corso Duca degli Abruzzi, 24, I-10129 TO (e-mail: fabio.fagnani@polito.it).

The average weight enumerators and the corresponding spectral functions of turbo-like code ensembles play a decisive role in the analysis of average performances under ML decoding. [7, 8]. Analyzing the weight structure of these coding schemes is not a trivial issue. A basic requirement is to determine the weight distributions of the constituent convolutional encoders. The average weight enumerators and the corresponding spectral functions can in fact be expressed in terms of weight distributions of the constituent components (see [9]). For example, in the case of repeat multiple-accumulate codes [10], an explicit analytic formula is known for the asymptotic spectral functions and it can be expressed in a recursive way [11, 12]. In [13], spectral functions are used to provide lower estimates of the noise channel parameter that allows the error probability to arbitrarily be made small. In [12], they are shown to be 0 below a threshold distance and positive beyond this distance. This threshold is shown to be the typical normalized minimum distance.

The fundamental problems of general cases remain open. First, the theoretical justification of the extension of the iterative formula of spectral function [14] requires some finer work, since the limit step needs to converge *uniformly* to the spectral function of the constituent codes. This, to the best of our knowledge, has never been proved before. Second, in order to pass from spectral functions to estimates on the noise channel parameter, or minimum distance thresholds, we need some information on the speed of convergence of the sequence of the exact exponents to the asymptotic growth rate. Finally, in theoretical analysis, the continuity and concavity of the limit function must be guaranteed [12].

The weight distribution of convolutional encoders has been studied extensively in the literature [8, 13–18]. Although analytic formulæ of weight enumerators can be derived in some cases using combinatorial techniques —i.e. for rate-1 convolutional encoders with transfer functions $(1+D)^{-1}$ and $(1+D+D^2)^{-1}$ [13]— no general method exists 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 [15]. This approach is able to precisely determine the weight enumerators for relatively small lengths, but the computation becomes prohibitively expensive as the truncation lengths increase. Bender et al. have shown, in [19], that central and local limit theorems can be derived for the growth of the components of the power of a matrix. This approach would, in principle, allow the Hayman approximation (see [20] for a survey) to be applied to the problem of the weight distribution of convolutional codes. However, the hypotheses of using these techniques are very restrictive and are not guaranteed in general cases. An overview of these methods can be found in [17] and in [21].

In [14], a numerical procedure is introduced to determine the asymptotic exponential growth rate. This method generally requires that a system of polynomial equations is solved. 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 or to guarantee continuity of the limit function.

In this paper, we address the issue of estimatig the growth rate of the weight enumerators as a function of truncation length, in order to investigate some additional properties pertaining to the asymptotic spectral function.

1.2. What is new with respect to the existing literature. Our contribution is mainly theoretical. We have improved the previous results in the following ways.

First, we have found new expressions of the weight enumerators of truncated convolutional encoders. These formulæ can be expressed as coefficients of generating functions of regular error events (sequences starting and ending in the zero state and taking the non-zero state values in-between) and truncated error events (sequences which start in the zero state and never return). Although explicit analytic expressions can be computed for relatively small truncation lengths, these expressions become computationally complex as the truncation lengths and weights increase.

The extraction of coefficients in a fixed enumerating function can be considered a crucial issue in enumerative combinatorics [22]. The Multidimensional Saddle-Point (MSP) method is a technique that is used to approximate the growth rate of the coefficients of some generating functions. This method was developed in [23, 24] and then applied in [21, 25–29] in the context of the coding theory. Our contribution consists in proving that a similar approach can also be extended to approximate coefficients of generating functions of error events. This approximation is substantially easier to evaluate, and the numerical procedure can be conveniently implemented using any standard algorithm for the unconstrained minimization of a convex function (e.g., gradient descent). We show, with some examples, that our approximation is very accurate, even for quite short truncation lengths, and we improve the estimates known from literature.

This approximation technique is used to guarantee that the sequence of exponential growth rates converges uniformly to an asymptotic limit, to estimate the speed of this convergence, and to obtain expressions of the asymptotic spectral functions. It can be proved that the expression of the asymptotic spectral function can be recast in the form given in [14]. Our new representation emphasises that the spectral function is continuous and concave in its convex and closed domain.

All these results, which were conjectured in [17], but never proved, are useful to derive information regarding the ML properties of concatenated coding schemes (see [7], [30]).

1.3. Outline of the paper. This paper is organized as follows. In addition to the specific notation introduced in the core of the text, the general notation is presented in Section 2. Preliminary facts on convolutional encoders are then introduced (Section 3). In particular, the controller canonical form is discussed; minimal realization of a convolutional encoder and the concept of error events (known also as atomic codewords) and molecular codewords are defined. In Section 4, the main results are stated formally. In particular, exact formulæ and accurate approximations of weight enumerators and of the linear term of their exponential growth rate are provided. Some examples and numerical results are shown in Section 5. Technical proofs are collected in Section 6. Section 7 contains some concluding remarks. Finally, Appendix A, which describes the asymptotic estimates of powers of series with nonnegative coefficients, completes the paper.

2. General notation. 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. The sets of nonnegative and positive reals are indicated with $\mathbb{R}_+ = [0, +\infty)$ and $\mathbb{R}^+ = (0, +\infty)$, respectively. $\mathbb{N}_0 = \{0\} \cup \mathbb{N}$ is also used. 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 largest integer $m \in \mathbb{Z}$ such that $m \leq x$. For $x \in \mathbb{R}$, $\lceil x \rceil$ is the smallest integer $m \in \mathbb{Z}$ such 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 imaginary part of the unit is denoted by $\mathrm{j} = \sqrt{-1}$. A complex number $x \in \mathbb{C}$ is represented using its absolute value and argument, i.e. $x = |x|e^{\mathrm{j}\arg(x)}$.

The log function should be considered with respect to the natural base e, unless we explicitly mention otherwise. Conventionally, we set $\exp(-\infty) = 0, \exp(+\infty) = +\infty, \inf(\emptyset) = +\infty$ and $\sup(\emptyset) = -\infty$.

This paper makes frequent use of Landau symbols. The notation "$f(N) = O(g(N))$ when $N \to \infty$" means that positive constants c and N_0 exist, so that $f(N) \le cg(N)$ 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 $\lim_{N\to\infty} f(N)/g(N) = 1$.

Boldface letters are used for the vectors and matrices. The vector of $\mathbb{R}^n$, whose elements are all equal to 1, is denoted as $\mathbf{1}_n$. Given a set $\Omega \subseteq \mathbb{R}^n$, we denote the interior, the closure and the convex hull of Ω with $\overset{\circ}{\Omega}$, $\overline{\Omega}$ and $\mathrm{co}(\Omega)$, respectively. The identity matrix in $\mathbb{R}^{n\times n}$ is denoted with $\mathbf{I}_n$. The transpose and inverse of $\mathbf{A}$ are denoted with $\mathbf{A}^T$ 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 the set of indices in which $\boldsymbol{x}$ is nonzero with $\mathrm{supp}(\boldsymbol{x})$. For $\boldsymbol{x} \in \mathbb{R}^n$, $||\boldsymbol{x}||_2 = \sqrt{\sum_{i=1}^n x_i^2}$ 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 their scalar product and their pointwise product with $\langle \boldsymbol{f}, \boldsymbol{g}\rangle = \sum_k f_k g_k^*$ and $\boldsymbol{f} \cdot \boldsymbol{g}$, respectively. 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 $\boldsymbol{x} = (x_1, \dots, x_n)$, $\boldsymbol{k} = (k_1, \dots, k_n)$, and $F(\boldsymbol{x})$ be a formal multivariate series. We denote the coefficient of $\boldsymbol{x}^{\boldsymbol{k}} = \prod_{i=1}^n x_i^{k_i}$ in $F(\boldsymbol{x})$ with $\mathrm{coeff}\{F(\boldsymbol{x}), \boldsymbol{x}^{\boldsymbol{k}}\}$ or with $F_{\boldsymbol{k}}$, i.e.

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

3. Fundamental facts on convolutional encoders.

In this section we recall some basic system-theoretic properties concerning convolutional encoders. More details can be found in [1,2], and [31].

3.1. Convolutional encoders and weight enumerators.

Let $V((D))$ be the $\mathbb{Z}_2$-vector space of the formal Laurent series with coefficients in the $\mathbb{Z}_2$-vector space V. The elements in $V((D))$ are represented as $\sum_{-\infty}^{+\infty} \boldsymbol{v}_t D^t$, with $\boldsymbol{v}_t = 0$ for a sufficiently small t. The spaces of the causal Laurent series and of the rational functions with coefficients in V are denoted with $V[[D]]$ and $V(D)$, respectively. We recall that $V[[D]]$ and $V(D)$ are subspaces of $V((D))$.

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

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

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

for each $t \in I$.

By 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 so that it is 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 exists a finite state-space realization. This means that the relationship between the input and the codewords can be described by means of a linear dynamical system with finite memory. In other words, there exist a 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 $\boldsymbol{z}(D) \in Z((D))$ that satisfies

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

Let us now consider the realization $(\mathbf{F}, \mathbf{G}, \mathbf{H}, \mathbf{L})$ of convolutional encoder $\boldsymbol{\Psi}$. By fixing $\boldsymbol{z}_0$ the sequence $\boldsymbol{z}(D)$ is uniquely determined by the input sequence $\boldsymbol{u}(D)$, through the dynamic equations in (3.1); this $\boldsymbol{z}(D)$ is called the state sequence associated with $\boldsymbol{u}(D)$. The interpretation of this representation is discussed in detail in [31]. From now on, it will always be assumed that $\boldsymbol{z}_0 = \mathbf{0}$, which is the usual assumption that means the shift register is filled with zero bits at the beginning of the encoding process.

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

Definition 3.2. *We define the trellis section at time $t \in \mathbb{Z}$ 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*

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

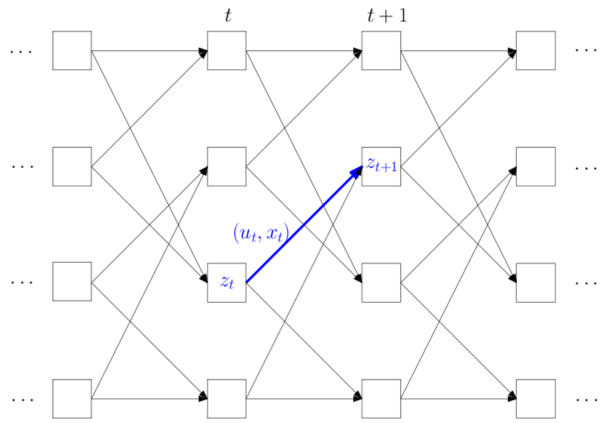


Fig. 3.1. *Trellis associated to the realization of a convolutional encoder. Given the input $\boldsymbol{u}_t$, the output and the state of the system are updated by $\boldsymbol{z}_{t+1} = \mathbf{F}\boldsymbol{z}_t + \mathbf{G}\boldsymbol{u}_t$ and $\boldsymbol{x}_t = \mathbf{H}\boldsymbol{z}_t + \mathbf{L}\boldsymbol{u}_t$*

It should be noted that the trellis is not an invariant of the code, but depends on the choice of the generator matrix as well as on the realization.

It is well-known [31] that each encoder admits a minimal realization (i.e., with observability and controllability properties and with the smallest state dimension μ). From now on, it will always be assumed that we are using the minimal trellis. This hypothesis is not necessary for the results of this paper to hold but is assumed for practical reasons.

3.2. Truncated convolutional encoders. Given a convolutional encoder $\psi \in \mathbb{Z}_2^{k\times n}(D)$ and fixed $N \in \mathbb{N}$, let us consider the block encoder $\psi_N : \mathbb{Z}_2^{kN} \to \mathbb{Z}_2^{nN}$ which is obtained by restricting the inputs of the convolutional encoder ψ to those inputs that are supported inside $[0, N-1]$, and also considering the projection of the output on the coordinates in $[0, N-1]$. Formally,

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

if

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

where we use the symbol $r(D^{N-1})$ to enclose all the terms of the whole semi-infinite sequence $\psi(\boldsymbol{u}_0 + \boldsymbol{u}_1 D + \ldots + \boldsymbol{u}_{N-1} D^{N-1})$ whose indices are not in the $[0, N-1]$ window.

We call ψ_N 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 exponential growth rate of input-output weight enumerators. For a given convolutional encoder and $(u, \delta) \in [0,1]^2$, we define the *input-output weight distribution function*

$$G_N(u, \delta; \psi) := \begin{cases} \frac{\ln A_{\lfloor ukN \rfloor, \lfloor \delta nN \rfloor}(\psi_N)}{nN} & \text{if } A_{\lfloor ukN \rfloor, \lfloor \delta nN \rfloor}(\psi_N) > 0, \\ -\infty & \text{if } A_{\lfloor ukN \rfloor, \lfloor \delta nN \rfloor}(\psi_N) = 0 \end{cases} \tag{3.2}$$

and the asymptotic growth rate as

$$G(u, \delta; \psi) := \lim_{N\to\infty} G_N(u, \delta; \psi). \tag{3.3}$$

The asymptotic growth rate of the weight distribution captures the behavior of the codewords with a linear input-output weight in the truncation length. Several authors [2, 17, 32–34] have defined a slightly weaker form of growth rate using $\limsup_{N\to\infty} G_N(u, \delta; \psi)$ instead of $\lim_{N\to\infty} G_N(u, \delta; \psi)$ in the definition. This weaker definition would only allow the input-output weight enumerators to be upper bounded by the product of a proper sub-exponential function in N and $\mathrm{e}^{NG(u,\delta)}$. Here, we adopt the stronger definition, which implies both upper and lower bound of input-output weight enumerators:

$$A_{\lfloor ukN \rfloor, \lfloor \delta nN \rfloor}(\psi_N) = \mathrm{e}^{nNG(u,\delta) + o(N)} \quad \forall (u, \delta) \in [0,1]^2.$$

3.3. Error events and their generating functions. The concatenation of the Laurent series defined in the previous section leads to the following definitions. Some of these definitions can also be found in [15, 21].

DEFINITION 3.3 (Error event). *Sequence $\boldsymbol{u} \in \mathbb{Z}_2^k((D))$ is an error event for ψ if there exists $t_b < t_e$ such that* $\operatorname{supp}(\boldsymbol{u}) \subseteq [t_b, t_e]$ *and the corresponding state sequence $\boldsymbol{z}(D) \in Z((D))$ has* $\operatorname{supp}(\boldsymbol{z}) = [t_b + 1, t_e]$. *It should be noted that this implies $\boldsymbol{u}_{t_b} \neq \boldsymbol{0}$ and* $\operatorname{supp}(\psi(\boldsymbol{u})) \subseteq [t_b, t_e]$. *We call $[t_b, t_e]$ the active window and we denote the length of the (input) error event with $l(\boldsymbol{u}) = t_e - t_b + 1$.*

Error events can be depicted as paths in the trellis that start and end in the zero state and taking non-zero state values in-between. Each non-zero codeword of a convolutional code (which is also known also as a molecular codeword) can be considered as a composition of several concatenated error events.

If we consider a truncated convolutional encoder, it could occur that the state sequence is not in the 0 state at time N. Thus it is necessary to distinguish two types of error event for the family of truncated convolutional encoders: a regular and a truncated error event.

DEFINITION 3.4 (Regular error event). *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 $\boldsymbol{u}(D) = \boldsymbol{u}_0 + \boldsymbol{u}_1 D + \ldots + \boldsymbol{u}_{N-1} D^{N-1}$ is an error event of length l for ψ.*

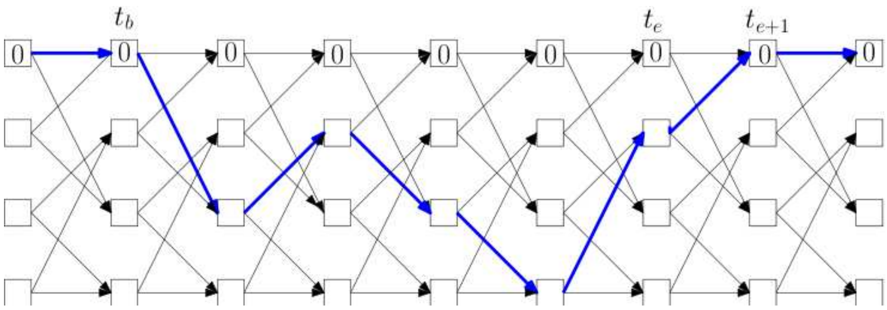


FIG. 3.2. *A regular error event with active window* $[t_b, t_e]$.

DEFINITION 3.5 (Truncated error event). *An input vector $\boldsymbol{u} \in (\mathbb{Z}_2^k)^N$ is a truncated error event for ψ_N, if there exists $t_b < N$ such that the corresponding state sequence has a support that is equal to the discrete interval* $[t_b + 1, N]$.

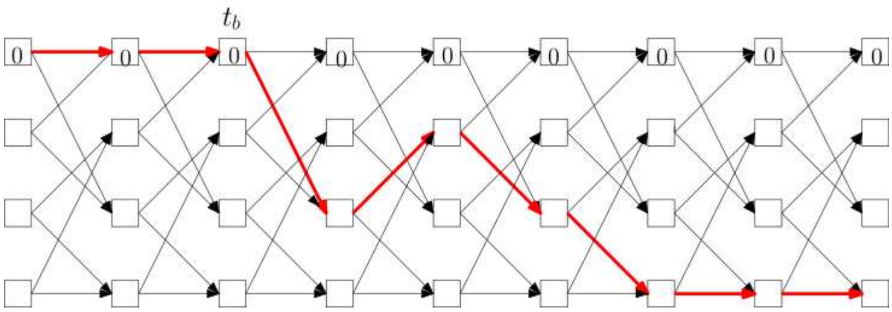


FIG. 3.3. *A truncated error event.*

These definitions lead the codewords being classified as regular or truncated.

We denote the number of input sequences with an input weight w, output weight d, and consisting exclusively of regular error events, or containing a truncated error event, respectively, with $R_{w,d}(\psi_N)$ and $T_{w,d}(\psi_N)$. We thus obtain $A_{w,d}(\psi_N) = R_{w,d}(\psi_N) + T_{w,d}(\psi_N)$.

Let ψ_N be the block encoder obtained by truncating a convolutional encoder $\psi \in \mathbb{Z}_2^{k\times n}(D) \cap \mathbb{Z}_2^{k\times n}[[D]]$ after N trellis steps. Let μ be the dimension of the state space. Let us consider a triple (w, d, l); the number of distinct error events of input weight w, output weight d and length l is denoted with $E_{w,d,l}$. We 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].

In order to display this function, we collect the information regarding the effect of the state transitions at each step, except for the zero state, in matrix form. This matrix, also known as the *transition matrix*, appears in different forms in [14,15,21,35]. We 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 a 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 $x^{\mathrm{w_H}(\boldsymbol{u})} y^{\mathrm{w_H}(\boldsymbol{x})} z$ label where $\mathrm{w_H}(\boldsymbol{u})$ is the weight of the 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. We set $M_{\boldsymbol{v},\boldsymbol{z}} = 0$ if there is not a one step transition from state $\boldsymbol{z}$ to state $\boldsymbol{v}$. Formally, we have

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

It should be noted that, once we have fixed an ordering of the states, we should 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 a similarity transformation via a permutation matrix [36].

In a 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:

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

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

$$E(x, y, z) = \sum_j \boldsymbol{b}(x, y, z)^T \mathbf{M}(x, y, z)^j \boldsymbol{a}(x, y, z). \tag{3.4}$$

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 the previous formalism we obtain

$$\widetilde{E}(x,y,z) = \sum_i \left[\sum_j \mathbf{M}^j(x,y,z)\boldsymbol{a}(x,y,z) \right]_i . \tag{3.5}$$

Other algorithms, which can be used to compute the generating function of error events, while avoiding the large transition matrix, are Viterbi's method (see [35]), or Mason's gain formula, as described in [32]. Other methods can be found in [37].

4. 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 new, or improve results that already exist in the literature. Our contribution is discussed in detail.

In the following, we present a new representation of the weight enumerators of convolutional encoders. The main tool is the use of a generating function for 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.

Let us consider the following formal power series

$$F(x,y,z) := \frac{E(x,y,z)}{(1-z)} \tag{4.1}$$

$$L(x,y,z) := \frac{1}{1-z} + \frac{\widetilde{E}(x,y,z)}{E(x,y,z)}. \tag{4.2}$$

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

THEOREM 4.1 (Weight enumerators). *The weight distribution of a truncated convolutional encoder ψ_N is given by*

$$A_{w,d}(\psi_N) = \sum_{t=1}^{N} \operatorname{coeff}\left\{ L(x,y,z)F(x,y,z)^t, x^w y^d z^N \right\}. \tag{4.3}$$

Although the computation of the expression in (4.3) is easy for reasonably sized parameters, it quickly becomes unpractical when the truncation length N grows. It should be noted that the formula in (4.3) involves powers of series with nonnegative coefficients. A technique to approximately evaluate the growth rate of the coefficients of a multivariate polynomial has been developed in [23,24] and applied in [21,25,26,38] to evaluate the weight and stopping set distribution of LDPC, and in [27,28] to study the average distance distribution of irregular doubly generalized low-density parity-check code ensembles. We will prove that a similar approach can also be extended to approximate the coefficients of the generating functions in (4.3). With this technique, we obtain the asymptotic exponential growth rate of (4.3), which can in fact be estimated much more easily.

Let us define the following set

$$\mathcal{W} := \{(u,\delta) \in [0,1]^2 | \exists N_0 \in \mathbb{N} : R_{\lfloor ukN_0 \rfloor, \lfloor \delta n N_0 \rfloor}(\psi_{N_0}) > 0\}. \tag{4.4}$$

PROPOSITION 4.2. *$\mathcal{W}$ is convex and closed.*

THEOREM 4.3 (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*

$$G(u,\delta;\psi) = \begin{cases} \frac{\max\limits_{\alpha\in[0,1]} \min\limits_{(x,y,z)\in\Sigma^+} \{\alpha \ln F(x,y,z) - uk \ln x - \delta n \ln y - \ln z\}}{n} & \text{if } (u,\delta) \in \mathcal{W} \\ -\infty & \text{otherwise} \end{cases} \tag{4.5}$$

where $\mathcal{W}$ is defined in (4.4), $\Sigma \subseteq \mathbb{R}^3$ is the region of absolute convergence of the power series $F(x,y,z)$, and $\Sigma^+ = \Sigma \cap (\mathbb{R}^+)^3$.

The espression in (4.5) highlights the following property, which was conjectured in [17], but never proved before.

COROLLARY 4.4. *$G(u,\delta;\psi)$ is continuous and concave with respect to u and δ in $\mathcal{W}$.*

An algorithm that can be used to efficiently compute the asymptotic growth rate of the weight distribution for a convolutional encoder has already been given by Sason et al. in [14]. We here improve their results in the following ways. First, the continuity and concavity of function $G(u,\delta,\psi)$ is guaranteed with our representation (4.4). 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 (4.5) 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 the unconstrained minimization of a convex function (e.g., gradient descent).

Sometimes, if the focus is on the exponential growth rate, it is not necessary to develop the full expression of the weight enumerators. Gallager [39–41] suggested to focus directly on the logarithm instead of on the weight enumerators themselves. In this way, all the sub-linear functions that multiply the exponential growth rate can be neglected. However, the exponential growth rate of the weight enumerators are often not sufficient to analyze the minimum distance properties or noise channel parameters of turbo codes and some refined estimates are required on the growth rate of the weight distribution.

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

THEOREM 4.5 (Finite length approximation). *Let us suppose that 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* $N \to \infty$

$$A_{\lfloor ukN \rfloor, \lfloor \delta n N \rfloor}(\psi_N) \sim \frac{\sqrt{2\pi\sigma^2} L(x_{\alpha^\star}, y_{\alpha^\star}, z_{\alpha^\star})}{\sqrt{(2\pi\alpha^\star N)^\nu |\mathbf{\Gamma}_{\alpha^\star}|}} \frac{F(x_{\alpha^\star}, y_{\alpha^\star}, z_{\alpha^\star})^{\alpha^\star N}}{x_{\alpha^\star}^{ukN} y_{\alpha^\star}^{\delta n N} z_{\alpha^\star}^N} \tag{4.6}$$

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

$$\begin{cases} \frac{x}{F(x,y,z)} \frac{\partial F(x,y,z)}{\partial x} = \frac{uk}{\alpha} \\ \frac{y}{F(x,y,z)} \frac{\partial F(x,y,z)}{\partial y} = \frac{\delta n}{\alpha} \\ \frac{z}{F(x,y,z)} \frac{\partial F(x,y,z)}{\partial z} = \frac{1}{\alpha} \end{cases} \tag{4.7}$$

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

$$\alpha^\star = \operatorname*{argmax}_{0 \le \alpha \le 1} \{\alpha \ln F(x_\alpha, y_\alpha, z_\alpha) - uk \ln x_\alpha - \delta n \ln y_\alpha - \ln z_\alpha\},$$

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

Theorem 4.5 largely parallels Theorem 10 in [25], in which an accurate approximation of the average weight enumerators is given for ensembles of LDPC codes. Using similar techniques (working with a formal series instead of polynomials), we are able not only to estimate the order of magnitude of weight enumerators, but also to emphasize the fundamental role played by ν.

Some of the examples given in Section 5 show that this approximation is very accurate, even for quite short truncation lengths. Explicit applications of these theorems are developed in [7] and [30].

5. 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, in some specific cases, we can improve the approximation given in Theorem 4.5.

5.1. Accumulate encoder. Let Acc_N be the block encoder obtained from 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 5.2.

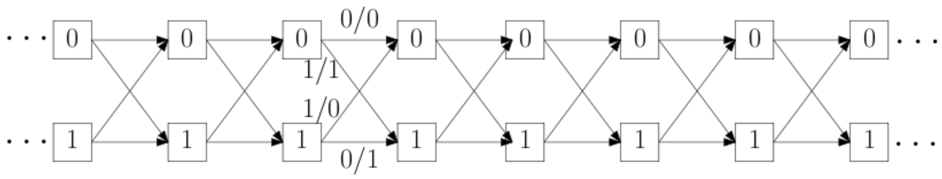


FIG. 5.1. *Trellis associated to the realization of the accumulate encoder.*

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

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

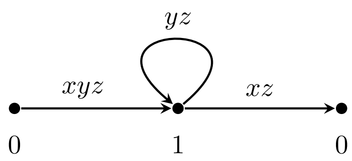


FIG. 5.2. *Accumulate encoder: weight transition diagram*

Using Theorem 4.1, we find that if w is even, then $T_{w,d}(\mathrm{Acc}_N) = 0$; otherwise, if w is odd, then $R_{w,d}(\mathrm{Acc}_N) = 0$.

The computation is now given in detail: if w is even, then

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

while, if w is odd,

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

from which

$$A_{w,d}(\mathrm{Acc}_N) = \binom{N-d}{\lfloor \frac{w}{2} \rfloor}\binom{d-1}{\lceil \frac{w}{2} \rceil - 1}, \tag{5.1}$$

a result that was also derived adopting different combinatorial techniques in [13]. The asymptotic growth rate, as shown in [13], can easily be deduced.

After some manipulations, we obtain the following solution for the set of three equations in (4.7)

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

It should be noted that the region of convergence of the generating functions of the 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 4.3 we find that

$$\begin{aligned} G(u,\delta;\text{Acc}) &= \frac{u}{2}\ln\frac{x^2yz^2}{(1-yz)(1-z)} - u\ln x - \delta\ln y - \ln z \\ &= \frac{u}{2}\ln yz - \frac{u}{2}\ln(1-yz) + \frac{u}{2}\ln\frac{z}{1-z} - u\ln x - \delta\ln y - \ln z \\ &= \frac{u}{2}\ln\left(1-\frac{u}{2\delta}\right) - \frac{u}{2}\ln\frac{u}{2\delta} + \frac{u}{2}\ln\frac{z}{1-z} - u\ln x - \delta\ln(yz) - (1-\delta)\ln z \\ &= \delta H\left(\frac{u}{2\delta}\right) + (1-\delta)H\left(\frac{u}{2(1-\delta)}\right). \end{aligned} \tag{5.2}$$

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

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

It should be noted that this approximation is better than the assertion given in Theorem 4.5. This improvement is due to the fact that when the input and output weights of the accumulate encoder are fixed, the number of error events and the overall length are automatically determined and no extra factor is needed in equation (4.6).

In Fig. 5.1, we show different results for truncation lengths $N = 80$ and $N = 200$. It should be noted that the approximation is very good, even for these low values of N and, as expected, for increasing N both the approximation and the direct calculation result approach the asymptotic growth rate.

5.2. The (4,3) Single Parity Check Code. This code can be considered as a truncated convolutional encoder $\phi \in \mathbb{Z}_2^{3\times 4}(D)$ with zero memory and $d_f(\psi) = 2$. We now focus on the output weight distribution function.

Again in this case, we can obtain an explicit expression for the output weight enumerators $A_d(\phi) = \sum_w A_{w,d}(\phi)$.

The generating function of the error events is given by

$$E(x,y,z) = (3xy^2 + 3x^2y^2 + x^3y^4)z$$

and from Theorem 4.1, we obtain

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

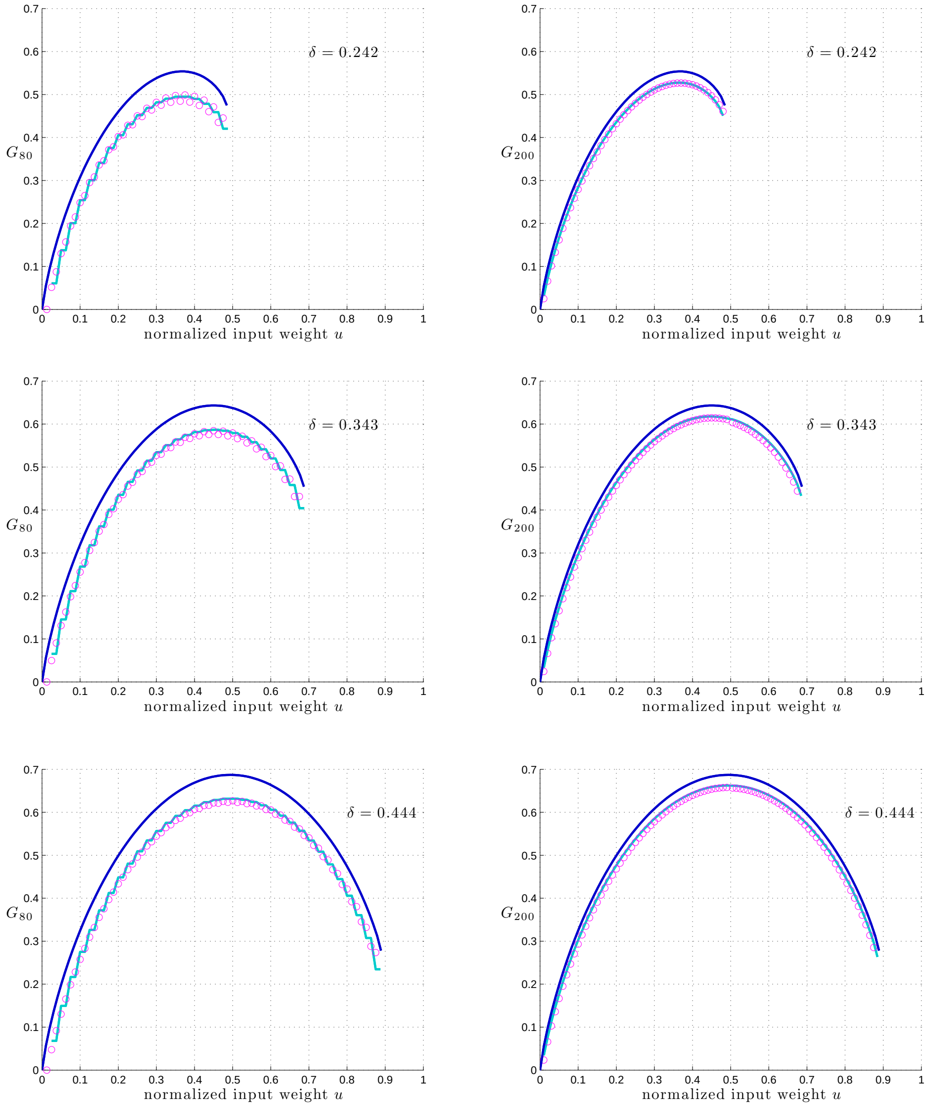


FIG. 5.3. *Accumulate encoder: once the output weight* $\delta = 0.242, 0.343, 0.444$ *has been fixed, the input-output weight distribution function* $G_N(u,\delta)$*, defined in* (3.2)*, can be plotted as a function of the normalized input weight* u *(see the dots), and compared with the exponent of* (4.6) *(bottom curve) and the asymptotic growth rate* $G(u,\delta)$ *defined in* (3.3)*. The plot is obtained for truncation lengths* $N = 80$ *(left) and* $N = 200$ *(right).*

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

$$\begin{aligned} A_d(\phi) &= \sum_{t=1}^{d/2} \binom{N}{t} \operatorname{coeff}\left\{ \sum_{i=0}^{t} \binom{t}{i} 6^i y^{t-i}, y^{d/2-2t} \right\} \\ &= \sum_{t=1}^{N} \binom{N}{t} 6^{2t-d/2} \binom{t}{2t-d/2} \end{aligned} \tag{5.3}$$

The asymptotic growth rate can easily be deduced.

In Fig. 5.2, we compare the exact weight enumerators (computed above) with the approximation obtained with Theorem 4.5 and the asymptotic spectral function provided by the method described in Theorem 4.3. The truncation lengths are taken as $N = 20$ and $N = 50$.

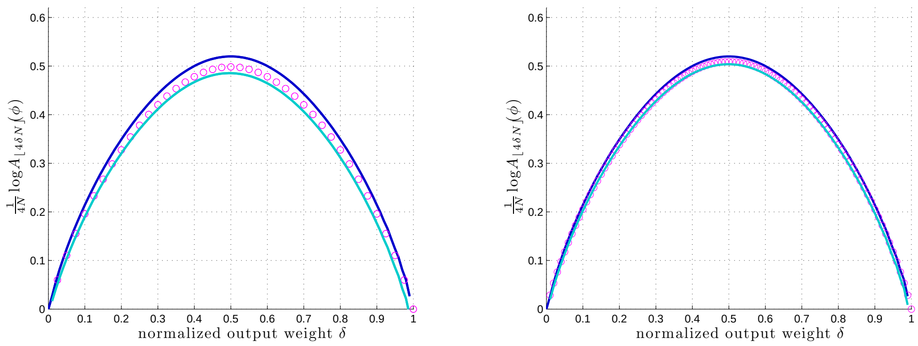


FIG. 5.4. *(4,3)-Single Parity Check Code: the exact exponent of the output weight enumerators given in* (5.3) *is compared with the exponent of the approximation using Theorem 4.5 (bottom curve) and the asymptotic growth rate (upper curve). The plot is obtained for truncation lengths* $N = 20$ *(left) and* $N = 50$ *(right).*

6. Proofs. In this section, we provide the proofs of the results listed in Section 4. Here, the proofs are outlined.

- In Subsection 6.1, we prove Theorem 4.1 by using some combinatorial results regarding convolutional codes.
- The proofs of Proposition 4.2, Theorem 4.3, and Corollary 4.4 are provided in Subsection 6.2.
- Finally, the approximation of the weight enumerators for finite length codes (Theorem 4.5) is derived in Subsection 6.3.

6.1. Exact method for the weight enumerators. Here, we prove Theorem 4.1.

Proof. [Proof of Theorem 4.1] A codeword is a concatenation of several error events. We therefore need to compute how many ways these patterns can be arranged over their total length N, so that their total input weight is w and their total output weight is d.

Given $w, d, t, l \in \mathbb{N}$, let us denote the cardinality of the set of all the input sequences $\boldsymbol{u} \in \mathbb{Z}_2^k[[D]]$ with the input weight vector w, and the output weight d, which is obtained by concatenating t full error events, and whose total length is l, with $R_{w,d,t,l}(\psi_N)$. Let us now take into consideration the combinatorics of the 0's which separate the error events (what Sason et al. call *silent periods* in [14]): it is necessary to dispose of $N - l$ elements in a maximum of $t + 1$ different blocks (see Figure 6.1).

Let $C_{N-l,t+1}$ be the number of $t+1$-combination with repetition of the finite set

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

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

FIG. 6.1. *Combinatorics of the* 0*'s which separate the error events*

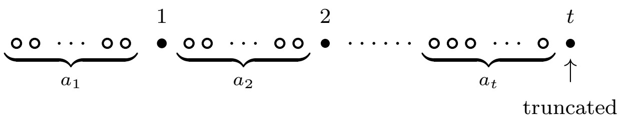
$\{1, \ldots, N-l\}$. We obtain:

$$\begin{aligned}
R_{w,d}(\psi_N) &= \sum_{t=1}^{N}\sum_{l=1}^{N} C_{N-l,t+1} R_{w,d,t,l}(\psi_N) = \sum_{t=1}^{N}\sum_{l=1}^{N} \binom{N-l+t}{t} R_{w,d,t,l}(\psi_N) \\
&= \sum_{t=1}^{N}\sum_{l=1}^{N} \binom{N-l+t}{t} \sum_{\substack{(w_1,\ldots,w_t):\\ \sum_{i=1}^{t} w_i = w}} \sum_{\substack{(d_1,\ldots,d_t):\\ \sum_{i=1}^{t} d_i = d}} \sum_{\substack{(l_1,\ldots,l_t):\\ \sum_{i=1}^{t} l_i = l}} \left(\prod_{j=1}^{t} E_{w_j,d_j,l_j} \right) \\
&= \sum_{t=1}^{N}\sum_{l=1}^{N} \operatorname{coeff}\left\{ \frac{1}{(1-z)^{t+1}}, z^{N-l} \right\} \operatorname{coeff}\left\{ [E(x,y,z)]^t, x^w y^d z^l \right\} \\
&= \sum_{t=1}^{N} \operatorname{coeff}\left\{ \frac{[E(x,y,z)]^t}{(1-z)^{t+1}}, x^w y^d z^N \right\} \qquad (6.1)
\end{aligned}$$

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

$$\begin{aligned}
&T_{w,d}(\psi_N) = \\
&= \sum_{t=1}^{N}\sum_{l=1}^{N} C_{N-l,t} \sum_{\substack{(w_1,\ldots,w_t):\\ \sum_{i=1}^{t} w_i = w}} \sum_{\substack{(d_1,\ldots,d_t):\\ \sum_{i=1}^{t} d_i = d}} \sum_{\substack{(l_1,\ldots,l_t):\\ \sum_{i=1}^{t} l_i = l}} \left(\prod_{j=1}^{t-1} E_{w_j,d_j,l_j} \right) \widetilde{E}_{w_t,d_t,l_t} \\
&= \sum_{t=1}^{N}\sum_{l=1}^{N} C_{N-l,t} \sum_{w_t=1}^{N}\sum_{d_t=1}^{N}\sum_{l_t=1}^{N} \widetilde{E}_{w_t,d_t,l_t} \times \qquad (6.2) \\
&\quad \times \sum_{\substack{(w_1,\ldots,w_{t-1}):\\ \sum_{i=1}^{t} w_i = w - w_t}} \sum_{\substack{(d_1,\ldots,d_{t-1}):\\ \sum_{i=1}^{t} d_i = d - d_t}} \sum_{\substack{(l_1,\ldots,l_{t-1}):\\ \sum_{i=1}^{t} l_i = l - l_t}} \prod_{j=1}^{t-1} E_{w_j,d_j,l_j}
\end{aligned}$$

$$
\begin{aligned}
T_{w,d}(\psi_N) &= \sum_{t=1}^{N}\sum_{l=1}^{N} C_{N-l,t} \sum_{w_t=1}^{N}\sum_{d_t=1}^{N}\sum_{l_t=1}^{N} \operatorname{coeff}\left\{\widetilde{E}(x,y,z), x^{w_t}y^{d_t}z^{l_t}\right\} \times \qquad (6.3)\\
&\quad \times \operatorname{coeff}\left\{[E(x,y,z)]^{t-1}, x^{w-w_t}y^{d-d_t}z^{l-l_t}\right\}\\
&= \sum_{t=1}^{N}\sum_{l=1}^{N} \binom{N-l+t-1}{t-1} \operatorname{coeff}\left\{\widetilde{E}(x,y,z)\,[E(x,y,z)]^{t-1}, x^{w}y^{d}z^{l}\right\}\\
&= \sum_{t=1}^{N} \operatorname{coeff}\left\{\widetilde{E}(x,y,z)\frac{[E(x,y,z)]^{t-1}}{(1-z)^t}, x^{w}y^{d}z^{N}\right\}. \qquad (6.4)
\end{aligned}
$$



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

FIG. 6.2. *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: it should be noted that, in this case, we have to dispose of $N-l$ elements in a maximum of t different blocks, since the last error event has not yet terminated (see Figure 6.2). The thesis is obtained by adding expression (6.1) to (6.4). ☐

6.2. Asymptotic growth rate of the weight enumerators. Let us now discuss how the exponential growth rate of the weight enumerators can be derived. Some other technical proofs have been deferred to Appendix A for better readability purposes.

LEMMA 6.1. *For fixed $(u,\delta) \in \mathbb{Q}^2 \cap [0,1]^2$, consider the set*

$$
\mathcal{N}_{u,\delta} = \{N \in \mathbb{N} : ukN \in \mathbb{N}, \delta nN \in \mathbb{N} \text{ and } R_{ukN,\delta nN}(\psi_N) > 0\}. \qquad (6.5)
$$

This set is either empty, or has infinite cardinality. 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 each positive integer j. In order to comprehend this fact, it should be observed 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 $\mathrm{w_H}(\psi_{N_0}(\boldsymbol{u})) = \delta nN_0$. 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 obtain $\mathrm{w_H}(\boldsymbol{w}|_{[0,jN_0-1]}) = ukjN_0$ and $\mathrm{w_H}(\psi_{jN_0}(\boldsymbol{w})) = \delta njN_0$, or equivalently $jN_0 \in \mathcal{N}_{u,\delta}$. ☐

Proof. [Proof of Proposition 4.2]

We can prove the assertion through 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 $\mathcal{W} \cap \mathbb{Q}^2$ set is dense in $\mathcal{W}$ due to the way it is defined. In fact, for each $\overline{\boldsymbol{\omega}} \in \mathcal{W}$ 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 obtain

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

In order to comprehend this fact, let $N \in \mathbb{N} \in \mathcal{N}_{\overline{\omega}_1,\overline{\omega}_2}$, as defined in (6.5), then from Lemma 6.1 we obtain $jN \in \mathcal{N}_{\overline{\omega}_1,\overline{\omega}_2}$.

It should be noted that all $\boldsymbol{\omega} \in \mathbb{Q}^2$, so 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

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

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

$$\mathrm{w_H}(\boldsymbol{u}_1|_{[0,N_1-1]}) = u_1 k N_1 \qquad \mathrm{w_H}\left(\psi_{N_1}(\boldsymbol{u}_1)\right) = \delta_1 n N_1$$

and

$$\mathrm{w_H}(\boldsymbol{u}_2|_{[0,N_2-1]}) = u_2 k N_2 \qquad \mathrm{w_H}\left(\psi_{N_2}(\boldsymbol{u}_2)\right) = \delta_2 n N_2.$$

In order to comprehend that $\mathcal{W}$ is convex, it is sufficient to prove that

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

Let us consider j_1, j_2, so that $j_1 N_1 = j_2 N_2 = N^\star$ and the following input sequences

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

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

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

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

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

From equation (6.1) we find that $(u, \delta) \in \mathcal{W}$ if, and only if, there exists $(\alpha, \beta) \in (0,1)^2$ such that the following problem is feasible

$$
\begin{aligned}
&\sum_{i,j,l} \lambda_{i,j,l} = 1, && \sum_{i} i\lambda_{i,j,l} = \frac{uk}{\alpha}, \\
&\sum_{j} j\lambda_{i,j,l} = \frac{\delta n}{\alpha}, && \sum_{k} l\lambda_{i,j,l} = \frac{\beta}{\alpha}.
\end{aligned}
\tag{6.6}
$$

It should be noted that $\lambda_{i,j,l}$ represents the limit fraction of the 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, $(\alpha, \beta) \in [0,1]^2$ exists, for which the following decision problem is feasible:

$$
\boldsymbol{\Phi\lambda} = \left(1, \frac{uk}{\alpha}, \frac{\delta n}{\alpha}, \frac{\beta}{\alpha}\right)^T \qquad \boldsymbol{\lambda} \succeq \mathbf{0}, \tag{6.7}
$$

in which the region of u and δ for which (6.6) is feasible is closed. In order to comprehend this fact, let us consider the dual problem of 6.7.

$$
\boldsymbol{\Phi}^T \boldsymbol{\zeta} \preceq \mathbf{0} \qquad \left(1, \frac{uk}{\alpha}, \frac{\delta n}{\alpha}, \frac{\beta}{\alpha}\right) \boldsymbol{\zeta} > 0 \tag{6.8}
$$

According to Farkas' lemma [42], (6.7) and (6.8) are strong alternatives, which means that only one of them holds (i.e. either (6.7) or (6.8) is feasible, but not both). On the other hand, the region of (u, δ) for which (6.8) is feasible is clearly an open set (notice that $\boldsymbol{\Phi}$ is independent of α, β, u, and δ), so that the region for which (6.6) 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 $[0,1]$, sequences $\lambda_m \in \mathbb{Q}, \boldsymbol{\omega}^1_m, \boldsymbol{\omega}^2_m \in \mathcal{W} \cap \mathbb{Q}$ exist, so 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

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

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

Now, in order to obtain 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, some notations and definitions are fixed.

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

$$
\Delta_i[F](\boldsymbol{x}) := x_i \frac{\partial \ln F}{\partial x_i} = \frac{x_i}{F}\frac{\partial F}{\partial x_i} \quad \forall i \in \{1, \ldots \eta\} \tag{6.9}
$$

$$
\Gamma_{i,j}[F](\boldsymbol{x}) := x_j \frac{\partial\left(\Delta_i[F](\boldsymbol{x})\right)}{\partial x_j} \qquad \forall i, j \in \{1, \ldots \eta\}. \tag{6.10}
$$

THEOREM 6.2. *[Multidimensional saddle-point method for large powers] Let $S(\boldsymbol{x})$ and $F(\boldsymbol{x})$ be 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

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

Let us suppose that F has the following properties:

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

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

(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 exists $\widetilde{\boldsymbol{k}}_i\in\mathscr{F}$ for $i=1,\dots,l$ such that $\widetilde{\boldsymbol{k}}_i + t\boldsymbol{k}_i\in\mathscr{F}$ for each $t\in\mathbb{N}_0$.

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

Let us assume that S satisfies the following conditions:

(P5) $S_{\boldsymbol{l}}\in\mathbb{N}_0$ for each $\boldsymbol{l}$, $S_{\boldsymbol{0}} > 0$ 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 exists $\widetilde{\boldsymbol{l}}_i\in\mathscr{S}$ for $i=1,\dots,l$ such that $\widetilde{\boldsymbol{l}}_i + t\boldsymbol{k}_i\in\mathscr{S}$ for each $t\in\mathbb{N}_0$.

Let us consider α_n and $\boldsymbol{\omega}_n$, so that there exists 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

$$\mathrm{coeff}\{S(\boldsymbol{x})[F(\boldsymbol{x})]^{\alpha_n n}, \boldsymbol{x}^{\boldsymbol{\omega}_n\alpha_n n}\} = \frac{S(\boldsymbol{x}_{\boldsymbol{\omega}})}{\sqrt{(2\pi\alpha_n n)^\nu|\boldsymbol{\Gamma}(\boldsymbol{x}_{\boldsymbol{\omega}})|}}\frac{[F(\boldsymbol{x}_{\boldsymbol{\omega}})]^{\alpha_n n}}{\boldsymbol{x}_{\boldsymbol{\omega}}^{\boldsymbol{\omega}_n\alpha_n n}}\left(1+O\left(n^{-1/10}\right)\right), \tag{6.11}$$

for $n\to\infty$, so that $n\in\mathscr{N}$, and

$$\lim_{n\in\mathscr{N}}\frac{1}{n}\ln\left(\mathrm{coeff}\{S(\boldsymbol{x})[F(\boldsymbol{x})]^{\alpha_n n}, \boldsymbol{x}^{\boldsymbol{\omega}_n\alpha_n n}\}\right) = \alpha\ln F(\boldsymbol{x}_{\boldsymbol{\omega}}) - \alpha\ \boldsymbol{\omega}\cdot\ln\boldsymbol{x}_{\boldsymbol{\omega}} \tag{6.12}$$

where $\boldsymbol{x}_{\boldsymbol{\omega}}\in(\mathbb{R}^+)^\eta$ is the unique solution to $\boldsymbol{\Delta}(\boldsymbol{x}) = \boldsymbol{\omega}$. Moreover, the convergence in (6.12) is uniform in α and $\boldsymbol{\omega}$.

Theorem 6.2, whose proof is rather technical and therefore deferred to Appendix A, may be considered as a generalization of [19, Thm. 2] and [21, Lemma D.14]. There, only the case in which the generating function is a power of a multivariate polynomial, with non-negative coefficients, was considered. Theorem 6.2 covers a more general class of generating functions, which includes the case treated in [19, Thm. 2].

Moreover, our modification allows the order of magnitude of a (convergent) sequence of coefficients to be estimated in large powers of multivariate functions and highlights the fundamental role played by ν.

LEMMA 6.3. *Let us consider function $F(x,y,z)$, which is defined in (4.1). Then (P1)-(P3) hold true. The power series $\widetilde{E}(x,y,z)$ satisfy in (3.5) and $(1-z)^{-1}$ satisfy the (P5)-(P6) properties.*

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

Let $G = (\mathcal{V}, \mathcal{E})$ be the directed graph associated with the trellis of the convolutional encoder, where $\mathcal{V} = \{v_1, v_2, \ldots v_\mu\}$ is a finite set of vertices that represent the 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. Let us now suppose that a label is assigned to each edge in the graph. If $e = (v_i, v_j) \in \mathcal{E}$, a label is assigned to the edge $f(e) = \boldsymbol{x}^{\boldsymbol{k}} = x_1^{k_1} x_2^{k_2} x_3^{k_3}$ in which k_1 is the weight of the 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 $p = (v_0, v_1), (v_1, v_2), \ldots, (v_{n-1}, v_n)$. Such a path is said to be a path of length n, and it is usually represented by the string $(v_0, v_1, \ldots v_n)$. Let us define the label of a path as the product of the labels of the component edges $f(p) = \prod_{e \in p} f(e) = \prod_{e \in p} \boldsymbol{x}^{\boldsymbol{k}_e} = \boldsymbol{x}^{\sum_{e \in p} \boldsymbol{k}_e}$. Let us define $\boldsymbol{k}_p = \sum_{e \in p} \boldsymbol{k}_e$.

With this formalism, the generating function $F(\boldsymbol{x})$ is the sum of the labels of all the paths that start and end in the zero state. A $c \in \mathscr{C}_{v|v_1,\ldots,v_n}$ cycle is a sequence that starts and ends in v with transitions in $\mathcal{V} \setminus \{v, v_1, ..., v_n\}$. Let $\mathscr{C}_{\min}$ be the set of all the minimal cycles, that is, all the cycles that start and end 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 the set of all the sequences in $\mathscr{C}_{v|v_1,\ldots,v_n}$ (and $\mathscr{C}^s_{\min}$) included in p with $\mathscr{C}^p_{v|v_1,\ldots,v_n}$ (and $\mathscr{C}^p_{\min}$).

The following lemma states that each 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 a sequence $s = (0, v_1, ..., v_n, 0)$ exists, so that $f(s) = \boldsymbol{x}^{\boldsymbol{k}}$. If v_i are all distinct values 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 the v, we can conclude the thesis. If this is not the case, it is necessary to 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 a maximum nomber of $|\mathcal{V}| = \mu$ steps, and we obtain

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

It should be noted that finally s is decomposed exlusively in terms of minimal cycles. Let us define t_c as the number of times the cycle appears in the sequence s, and we conclude that

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

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

Proof. [Proof of Theorem 4.3] If $(u,\delta) \notin \mathcal{W}$, then we trivially have that

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

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

From Theorem 4.1 (see expressions (4.1), (4.2), and (4.3)), we obtain

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

Let us define

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

and $\alpha_N = \frac{\lfloor \alpha N \rfloor}{N}$. It should be noted that $||\boldsymbol{\omega} - \boldsymbol{\omega}_N|| = O\left(N^{-1}\right)$ and $|\alpha_N - \alpha| = O(N^{-1})$. Since $(u,\delta) \in \mathcal{W}$, $\boldsymbol{\omega} \in \mathrm{co}(\mathring{\mathscr{F}})$, and from Lemma 6.3, the hypotheses of Theorem 6.2 are satisfied.

Using Theorem 6.2, we can estimate function G as follows

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

in which $(x_\alpha, y_\alpha, z_\alpha)$ is the solution of system $\boldsymbol{\Delta}[F](x,y,z) = (uk/\alpha, \delta n/\alpha, 1/\alpha)$, which is equivalent to system (4.7).

On the other hand, from Theorem 4.1 (see expression (4.3)) we obtain $\forall (x,y,z) \in$

$(\mathbb{R}^+)^3$

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

where the last step is obtained from Theorem 6.2.

We can conclude that

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

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 the proof of Lemma B.2). □

Proof. [Proof of Corollary 4.4] The continuity of function $G(u,\delta)$ in $(u,\delta) \in \mathcal{W}$ is obtained immediately from the expression in (4.5).

We can now prove that function G is also concave in its domain. It should be noted 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 a pointwise minimum over an infinite set of concave functions:

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

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

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

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

6.3. Finite length approximation of the weight distribution. The basic technique in the following proof is a direct application of Theorem 6.2 for multivariate generating functions.

Proof. [Proof of Theroem 4.5] On the basis of Theorem 6.2, we know that for $w = \lfloor ukN \rfloor$, $d = \lfloor \delta n N \rfloor$ and $N \to \infty$

$$\begin{aligned}
A_{w,d}^{\alpha N}(\psi_N) &:= \operatorname{coeff}\left\{L(x,y,z)F(x,y,z)^{\alpha N}, x^w y^d z^N\right\} \\
&\sim \frac{L(x_\alpha, y_\alpha, z_\alpha)}{\sqrt{(2\pi\alpha N)^\nu |\mathbf{\Gamma}_\alpha|}} \frac{[F(x_\alpha, y_\alpha, z_\alpha)]^{\alpha N}}{x_\alpha^w y_\alpha^d z_\alpha^N}
\end{aligned} \tag{6.13}$$

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

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

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

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

Considering 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 obtain

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

According to the assumption that $A_{w,d}^{\alpha N}(\psi_N)$ has 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 obtain

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

□

7. Concluding remarks. In this paper 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 the powers of multivariate functions, with nonnegative coefficients, can be used in the analysis of the growth rate of weight distribution as a function of the truncation length. We have investigated the connection of our estimates through a method that was previously introduced by Sason et al. in [14].

With respect to current literature, our results offer deeper insights into the problem of the spectra of truncated convolutional encoders, and they can be considered useful to derive results regarding the performance of turbo-like codes under maximum-likelihood decoding (e.g. [7], [30]).

However, we should not underestimate the importance of other analyses, such as pseudo-codewords, or stopping and trapping sets distribution, which are measures of the performance of the turbo decoder that was introduced for turbo-like codes in [43–46].

Stopping set distributions play an analogous role to that of distance spectra in ML decoding, when a binary turbo decoder is used on the binary erasure channel. Turbo decoding works on each code separately and exchanges information from one decoder to the other, until it can progress no further. When the transmitted codeword has not been recovered correctly, the set of erased positions that remain, when the decoder stops, is equal to the unique maximum-size turbo stopping set, which is also a subset of the (initial) set of erased positions.

Analyzing the stopping set distribution for these coding schemes is not a trivial issue. A basic requirement is to determine the subcode input-output support size enumerators (SIOSE) of the constituent convolutional encoders. In some cases, the SIOSE of a convolutional code can be computed using an extended trellis section of the convolutional code [45]. The extended trellis section includes and extends the trellis of the code to represent all the support vectors of the subcodes. The extended trellis section, for the convolutional encoders with $\psi(D) = 1/(1+D)$, is depicted in Fig. 7.1.

Our techniques can be adapted to compute SIOSE through the extended trellis section in the same way as the input-output weight enumerator is computed using the trellis.

8. Acknowledgments. Part of this work was conducted when the first author was visiting Massachusetts Institute of Technology. We would like to thank the Laboratory of Information and Decision Systems and Professor Devavrat Shah for their hospitality.

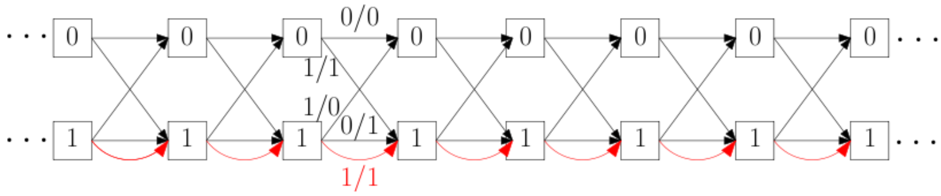


FIG. 7.1. *The extended trellis associated with the accumulate encoder $\psi(D) = (1 + D)^{-1}$. The edge labeled with $1/1$, from state 1 to state 1, is an extra edge which is not part of the original trellis section.*

REFERENCES

[1] V. S. Pless and W. C. Huffman, *Handbook of Coding Theory.* Elsevier Science, Amsterdam, Holland, 1998.

[2] R. J. McEliece, *Theory of information and coding.* Cambridge University Press, 2001.

[3] 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.

[4] C. Berrou and A. Glavieux, "Near optimum error correcting coding and decoding: turbo-codes," *IEEE Trans. Communications*, no. 44, pp. 1261–1271, 1996.

[5] S. Benedetto and G. Montorsi, "Unveiling turbo codes: some results on parallel concatenated coding schemes," *IEEE Trans. on Inform. Theory*, vol. 42, pp. 409–428, March 1996.

[6] D. V. Truhachev, M. Lentmaier, and K. S. Zigangirov, "Some results concerning the design and decoding of turbo-codes," *Problems of Information Transmission*, vol. 37, pp. 190–205, July-Sept. 2001.

[7] H. Jin and R. J. McEliece, "Coding theorems for turbo code ensembles," *IEEE Trans. on Inform. Theory*, vol. 48, pp. 1451–1461, June 2002.

[8] 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, pp. 24–47, Jan. 2000.

[9] S. Benedetto, D. Divsalar, G. Montorsi, and F. Pollara, "Analysis, design, and iterative decoding of double serially concatenated codes with interleavers," *IEEE J. Select. Areas Commun.*, vol. 16, pp. 231–244, Feb. 1998.

[10] H. Jin, *Analysis and design of turbo-like codes.* PhD thesis, Caltech, May 2001.

[11] F. Fagnani and C. Ravazzi, "Spectra and minimum distances of Repeat multiple accumulate codes," in *Proc. Inform. Theory and Applications Workshop*, (La Jolla, CA), pp. 77 – 86, January 2008.

[12] C. Ravazzi and F. Fagnani, "Spectra and minimum distances of Repeat multiple-accumulate codes," *IEEE Trans. on Inform. Theory*, vol. 55, pp. 4905–4924, November 2009.

[13] 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), pp. 201–210, September 1998.

[14] 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, pp. 3052–3061, December 2002.

[15] R. J. McEliece, *How to compute weight enumerators for convolutional codes.* Communications and Coding, Wiley, New York, NY, USA, 1998.

[16] N. Kahale and R. Urbanke, "On the minimum distance of parallel and serially concatenated codes," in *Proc. IEEE International Symposium on Information Theory*, (Cambridge, MA), Aug. 1998.

[17] H. D. Pfister, *On the capacity of the finite state channels and the analysis of convolutional accumulate-m codes.* PhD thesis, Univ. California, San Diego, La Jolla, 2003.

[18] 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*, (Austin, Texas), June 2010.

[19] 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.

[20] N. G. de Brujin, *Asymptotic Methods in Analysis.* North Holland, Amsterdam, 1981.

[21] T. Richardson and R. Urbanke, *Modern coding theory.* Cambridge University Press, 2007.

[22] P. Flajolet and R. Sedgewick, *Analytic combinatorics.* Cambridge University Press, Cambridge, UK, 2008.

[23] I. J. Good, "Saddle point methods for the multinomial distribution," *Annals of mathematical statistics*, pp. 860–881, 1956.

[24] D. Gardy, "Some results on the asymptotic behavior of coefficients of large powers of functions," *Discrete mathematics*, pp. 189–217, 1993.

[25] C. Di, T. J. Richardson, and R. L. Urbanke, "Weight distribution of low-density parity-check codes," *IEEE Trans. on Inform. Theory*, vol. 52, pp. 4839–4855, Nov. 2006.

[26] V. Rathi, "On the asymptotic weight and stopping set distribution of regular LDPC ensembles," *IEEE Trans. on Inform. Theory*, vol. 52, pp. 4212–4218, Sep. 2006.

[27] M. Flanagan, E. Paolini, M. Chiani, and M. Fossorier, "Growth rate of the weight distribution of doubly-generalized LDPC codes: General case and efficient evaluation," *Proc. IEEE Global Telecommunications Conference*, pp. 1–6, Nov.-Dec. 2009.

[28] M. Flanagan, E. Paolini, M. Chiani, and M. Fossorier, "On the growth rate of the weight distribution of irregular doubly generalized LDPC codes," *IEEE Trans. on Inform. Theory*, vol. 57, pp. 3721–3737, June 2011.

[29] D. Divsalar, "Ensemble weight enumerators for protograph-based doubly generalized ldpc codes," in *Proc. IEEE International Symposium on Information Theory*, (Seattle, WA), July 2006.

[30] 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.

[31] A. Barg and G. Forney, "Random codes: Minimum distances and error exponents," *IEEE Trans. on Inform. Theory*, vol. 48, pp. 2568–2573, Sept. 2002.

[32] S. Lin and D. J. Costello, *Error Control Coding: Fundamentals and Applications.* Prentice Hall, 1983.

[33] 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.

[34] 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*, pp. 1888–1892, July 2008.

[35] R. Johannesson and K. S. Zigangirov, *Fundamentals of Convolutional Coding.* IEEE Press, New York, NY, USA, 1999.

[36] H. Gluesing-Luerssen, "On the weight distribution of convolutional codes," *Linear algebra and its applications*, pp. 298–326, 2005.

[37] P. Fitzpatrick and G. H. Norton, "Linear recurring sequences and the path weight enumerator of a convolutional code," *Electr. Lett*, 1991.

[38] A. Orlitsky, K. Viswanathan, and J. Zhang, "Stopping set distribution of LDPC code ensembles," *IEEE Trans. on Inform. Theory*, vol. 51, pp. 929–953, Mar. 2005.

[39] R. G. Gallager, *Low-density parity-check codes.* M.I.T. Press, Cambridge, MA, 1963.

[40] R. Gallager, "A Simple Derivation of the Coding Theorem and Some Applications," *IEEE Trans. on Information Theory*, vol. IT, no. 11, pp. 3–18, 1965.

[41] R. Gallager, "The Random Coding Bound Is Tight for the Average Code," *IEEE Trans. on Information Theory*, vol. IT, pp. 244–246, March 1973.

[42] S. Boyd and L. Vandenberghe, *Convex Optimization.* Cambridge Univ. Press, 2004.

[43] E. Rosnes, M. Helmling, and A. Graell i Amat, "Pseudocodewords of linear programming decoding of 3-dimensional turbo codes," in *Proc. IEEE International Symposium on Information Theory*, (Saint Petersburg, Russia), pp. 1643–1647, August 2011.

[44] E. Rosnes and O. Ytrehus, "Turbo decoding on the binary erasure channel: Finite-length analysis and turbo stopping sets," *IEEE Trans. on Inform. Theory*, vol. 53, pp. 4059–4075, November 2007.

[45] A. Graell i Amat and E. Rosnes, "Good concatenated code ensembles for the binary erasure channel," *IEEE Journal on Selected Areas in Communications*, vol. 27, pp. 928–943, August 2009.

[46] C. Koller, A. Graell i Amat, J. Kliewer, and D. J. C. Costello, Jr., "Trapping set enumerators for repeat multiple accumulate code ensembles," in *Proc. IEEE International Symposium on Information Theory*, (Coex, Seoul, Korea), pp. 1819–1823, July 2009.

[47] H. L. Royden, *Real Analysis.* Prentice Hall, 1998.

[48] W. Rudin, *Fourier Analysis on Groups.* Wiley-Interscience, 1990.

[49] W. Rudin, *Principles of mathematical analysis.* McGraw-Hill, 1976.

[50] M. Artin, *Algebra.* Prentice Hall, 1991.

Appendix A. Multidimensional saddle-point method for large powers.

We now prove Theorem 6.2 through the use of intermediate steps. Our proof is based on multidimensional saddle-point (MSP) techniques which are used to estimate the order of magnitude of coefficients in large powers of multivariate functions.

The MSP method can be summarized as follows. The first step is to recast the problem as a 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 that crosses a saddle-point and to estimate the local integrand 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 *localizations* or *concentrations*, the contribution near the saddle-point captures the essential part of the integral. Some examples of admissible functions are multivariate polynomials (see Lemma D.14 in [21]) and univariate series (see Section VIII.8.1 in [22]). Applications of the multidimensional saddle-point method, in the context of the coding theory, can be found in [21,25,26] and can be used to study the weight/stopping sets distribution of LDPC codes.

Theorem 6.2 can be considered as an extension of Theorem 2 in [19]:

- The generating function is given by the product of two kinds of function ($S(\boldsymbol{x})$ and a large power of $F(\boldsymbol{x})$).
- It involves a multivariate series with non-negative coefficients, for which the "localization property", cited above, has never been proved.
- Theorem 6.2 estimates the order of magnitude of a (convergent) sequence of coefficients in large powers of multivariate functions.

Appendix B. Concentration property for a multivariate series.

In what follws, we will consider a multivariable formal power series of the 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 $F(\boldsymbol{x})$ has the following properties:

(P1) $F_{\boldsymbol{k}} \in \mathbb{N}_0$ for every $\boldsymbol{k}$, and $F_{\boldsymbol{0}} > 0$.

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

(P3) There exist 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 exists $\widetilde{\boldsymbol{k}}_i \in \mathscr{F}$ 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.

According to (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:

$$\Sigma = \left\{\boldsymbol{x} \in \mathbb{R}^\eta \;\middle|\; \left|\boldsymbol{x}^{\boldsymbol{k}^i}\right| < 1\ \forall i = 1, \ldots, l\right\} \tag{B.1}$$

The sum of the series on Σ is denoted by the same symbol $F(\boldsymbol{x}) := \sum_{\boldsymbol{k}\in\mathbb{N}_0^\eta} F_{\boldsymbol{k}}\boldsymbol{x}^{\boldsymbol{k}}$. Put $\Sigma^+ := \Sigma \cap (\mathbb{R}^+)^\eta$.

LEMMA B.1. *Let $\overline{\boldsymbol{x}} \in \partial\Sigma^+$ with $\overline{x}_i > 0$ for every $i = 1,\dots,\eta$. Let $\boldsymbol{x}_n \in \Sigma^+$ be a sequence, so 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 [47] yield:

$$\liminf_{n\to+\infty} F(\boldsymbol{x}_n) \geq F(\overline{\boldsymbol{x}})\,,$$

hence, to prove the result, it is sufficient to show that $F(\overline{\boldsymbol{x}}) = +\infty$ (it should be noted that the expression of $F(\overline{\boldsymbol{x}})$ is meaningful because it is the summation of a non-negative series). Let us instead suppose, ab absurdo, that $F(\overline{\boldsymbol{x}}) < +\infty$. Then, using (P3b) and (P1), for each $i = 1,\dots,l$ we obtain

$$+\infty > F(\overline{\boldsymbol{x}}) = \sum_{\boldsymbol{k}\in\mathbb{N}_0^\eta} F_{\boldsymbol{k}}\overline{\boldsymbol{x}}^{\boldsymbol{k}} \geq \sum_{t=0}^{+\infty} F_{\widetilde{\boldsymbol{k}}_i + t\boldsymbol{k}_i}\overline{\boldsymbol{x}}^{\widetilde{\boldsymbol{k}}_i}\left(\overline{\boldsymbol{x}}^{\boldsymbol{k}_i}\right)^t \geq \sum_{t=0}^{+\infty} \overline{\boldsymbol{x}}^{\widetilde{\boldsymbol{k}}_i}\left(\overline{\boldsymbol{x}}^{\boldsymbol{k}_i}\right)^t$$

This yields $\overline{\boldsymbol{x}}^{\boldsymbol{k}_i} < 1$ for every $i = 1,\dots,l$. From (B.1) it follows that $\overline{\boldsymbol{x}}$ is an interior point of Σ^+, contrarily to what was previously assumed. ◻

LEMMA B.2. *For every $\boldsymbol{\omega} \in \overset{\circ}{\mathrm{co}(\mathscr{F})}$, there exists a unique $\boldsymbol{x} \in \overset{\circ}{\Sigma^+}$ such that*

$$\Delta[F](\boldsymbol{x}) = \boldsymbol{\omega}, \tag{B.2}$$

where $\Delta[F]$ is defined in (6.9).

Proof. It should first be noted that the points that solve equation (B.2) are the stationary points 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 $\Xi = \{\boldsymbol{\xi}|(\xi_1,\dots,\xi_\eta) = (\ln x_1,\dots,\ln x_\eta), \boldsymbol{x}\in\Sigma^+\} \subseteq \mathbb{R}^\eta$. In fact,

$$\begin{aligned}
\boldsymbol{v}^T\nabla^2 f(\boldsymbol{\xi})\boldsymbol{v} &= \sum_{i=1}^{\eta}\sum_{j=1}^{\eta} v_i \frac{\partial^2 f}{\partial\xi_j\partial\xi_i} v_j \\
&= \sum_{i=1}^{\eta}\sum_{j=1}^{\eta} v_i\left(\sum_{\boldsymbol{k}} F_{\boldsymbol{k}}\mathrm{e}^{(\boldsymbol{k}-\boldsymbol{\omega})\cdot\boldsymbol{\xi}}(k_i-\omega_i)(k_j-\omega_j)\right)v_j \\
&= \sum_{\boldsymbol{k}} F_{\boldsymbol{k}}\mathrm{e}^{(\boldsymbol{k}-\boldsymbol{\omega})\cdot\boldsymbol{\xi}}\sum_{i=1}^{\eta}\sum_{j=1}^{\eta} v_i(k_i-\omega_i)(k_j-\omega_j)v_j \\
&= \sum_{\boldsymbol{k}} F_{\boldsymbol{k}}\mathrm{e}^{(\boldsymbol{k}-\boldsymbol{\omega})\cdot\boldsymbol{\xi}}||(\boldsymbol{v}\cdot(\boldsymbol{k}-\boldsymbol{\omega}))|| \geq 0
\end{aligned}$$

Since $\boldsymbol{\omega} \in \overset{\circ}{\mathrm{co}(\mathscr{F})}$, $\boldsymbol{v}^T\nabla^2 f(\boldsymbol{\xi})\boldsymbol{v} = 0 \iff \boldsymbol{v} = \boldsymbol{0}$. This implies that $f(\boldsymbol{\xi})$ is strictly convex in $\boldsymbol{\xi}\in\Xi$. Hence, uniqueness of the solution of (B.2) follows.

EXISTENCE: We now show that for any sequence of $\boldsymbol{x}_n$, whether converging to a point of $\partial\Sigma^+$ or unbounded, $\widehat{F}_{\boldsymbol{\omega}}(\boldsymbol{x}_n)$ is superiorly unbounded. This implies that $\widehat{F}_{\boldsymbol{\omega}}$ attains a global minimum in $\overset{\circ}{\Sigma^+}$ and completes the proof.

First, let us consider the case in which $\boldsymbol{x}_n \to \overline{\boldsymbol{x}} \in \partial\Sigma^+$ with $\overline{x}_i > 0$ for all i. In this case, the result easily follows from Lemma B.1. If, instead, there exists i, so that $\overline{x}_i = 0$, then,

$$\frac{F(\boldsymbol{x}_n)}{\boldsymbol{x}_n^{\boldsymbol{\omega}}} \geq \frac{F_0}{\boldsymbol{x}_n^{\boldsymbol{\omega}}} \to +\infty \qquad (n \to +\infty) \tag{B.3}$$

The case in which at least one component of $\boldsymbol{x}_n$ diverges to $+\infty$ remains to be considered. Since $\boldsymbol{\omega} \in \overset{\circ}{\mathrm{co}}(\mathscr{F})$, we find $\boldsymbol{f}^1, \dots \boldsymbol{f}^\mu \in \mathscr{F} \setminus \{\boldsymbol{0}\}$ which generate $\mathbb{R}^\mu$ and some strictly positive constants $\gamma_1, \dots, \gamma_s$ such that $\sum \gamma_j < 1$ and $\boldsymbol{\omega} = \sum \gamma_j \boldsymbol{f}^j$. If we pass to subsequences, it can always be assumed 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 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 can use the same arguments as in (B.3). Let us finally consider the case in which at least one $\alpha_l = +\infty$. It should be noted that

$$\frac{F(\boldsymbol{x}_n)}{\boldsymbol{x}_n^{\boldsymbol{\omega}}} = \frac{F(\boldsymbol{x}_n)}{\prod_l [\boldsymbol{x}_n^{\boldsymbol{f}^l}]^{\gamma^l}}$$

where $\gamma = \sum \gamma_l < 1$. Let us now put $z_l = \boldsymbol{x}_n^{\boldsymbol{f}^l} > 0$ for $l = 1, \dots, \mu$. Then,

$$\prod_l z_l^{\gamma^l} \leq \sum_l z_l^{\gamma}. \tag{B.4}$$

In order to comprehend this fact, let

$$\Gamma(z) = \frac{\prod_j z_j^{\gamma^j}}{\sum_j z_j^{\gamma}}.$$

Since $\Gamma(\lambda z) = \Gamma(z)$ for every z and $\lambda > 0$, $\Gamma(z)$ is studied, considering the z so that $\sum_j z_j^\gamma = 1$. From necessity, $z_j \leq 1$ for all j and this yields

$$\Gamma(z) = \prod_j z_j^{\gamma^j} \leq 1$$

This proves the inequality.

Using (B.4) we obtain

$$\frac{F(\boldsymbol{x}_n)}{\boldsymbol{x}_n^{\boldsymbol{\omega}}} = \frac{F(\boldsymbol{x}_n)}{\prod_l [\boldsymbol{x}_n^{\boldsymbol{f}^l}]^{\gamma^l}} \geq \frac{\sum_j \boldsymbol{x}_n^{\boldsymbol{f}^j}}{\sum_j [\boldsymbol{x}_n^{\boldsymbol{f}^j}]^{\gamma}}$$

where $\gamma = \sum \gamma_j < 1$. The expression on the left is clearly superiorly unbounded for $n \to +\infty$ and this completes the result.
$\square$

LEMMA B.3. *The matrix $\boldsymbol{\Gamma}[F](\boldsymbol{x})$ (defined in (6.10)) is symmetric and positive definite $\forall \boldsymbol{x} \in \Sigma^+$.*

Proof. In what follows, we put $\boldsymbol{\Gamma} = \boldsymbol{\Gamma}[F]$.

$$\begin{aligned} F(\boldsymbol{x})^2 \boldsymbol{v}^T \boldsymbol{\Gamma}(\boldsymbol{x}) \boldsymbol{v} &= F(\boldsymbol{x})^2 \sum_{i=1}^{\eta} \sum_{j=1}^{\eta} v_i \Gamma_{ij}(\boldsymbol{x}) v_j \\ &= F(\boldsymbol{x})^2 \sum_{i=1}^{\eta} v_i^2 \Gamma_{ii}(\boldsymbol{x}) + F(\boldsymbol{x})^2 \sum_{i=1}^{\eta} \sum_{j \neq i}^{\eta} v_i \Gamma_{ij}(\boldsymbol{x}) v_j \end{aligned}$$

$$
\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] + \\
&+ \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. \\
&\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. \\
&\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 + \\
&+ \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

$$
\begin{aligned}
F(\boldsymbol{x})^2 \boldsymbol{v}^T \boldsymbol{\Gamma}(\boldsymbol{x}) \boldsymbol{v} &= \sum_{\boldsymbol{k}} \sum_{\boldsymbol{l}} F_{\boldsymbol{k}} F_{\boldsymbol{l}} \boldsymbol{x}^{\boldsymbol{k}+\boldsymbol{l}} \left[\sum_{i=1}^{\eta} v_i \left(k_i - l_i \right) \right]^2 \\
&+ \sum_{\boldsymbol{k}} \sum_{\boldsymbol{l}} F_{\boldsymbol{k}} F_{\boldsymbol{l}} \boldsymbol{x}^{\boldsymbol{k}+\boldsymbol{l}} \left[\sum_{i=1}^{\eta} \sum_{j=1}^{\eta} v_i v_j l_i \left(k_j - l_j \right) \right] \\
&= \sum_{\boldsymbol{k}} \sum_{\boldsymbol{l}} F_{\boldsymbol{k}} F_{\boldsymbol{l}} \boldsymbol{x}^{\boldsymbol{k}+\boldsymbol{l}} \left[\sum_{i=1}^{\eta} v_i \left(k_i - l_i \right) \right]^2 \geq 0 \qquad \forall \boldsymbol{x} \in \Sigma^+
\end{aligned}
$$

Clearly, $\boldsymbol{v}^T \boldsymbol{\Gamma}(\boldsymbol{x}) \boldsymbol{v} = 0$ if, and only if, $\boldsymbol{v} = \boldsymbol{0}$. This yields the thesis. □

LEMMA B.4. *For each $\boldsymbol{r} \in (\mathbb{R}^+)^\eta$, there exists a strictly positive constant $\chi = \chi(F, \boldsymbol{r})$ such that $\forall \boldsymbol{\theta} \in [-\pi, \pi)^\eta \setminus \left[-n^{-2/5}, n^{-2/5}\right]$ the following inequality hold true*

$$
\left| \frac{F\left(\boldsymbol{r} \mathrm{e}^{\mathrm{j}\boldsymbol{\theta}} \right)}{F(\boldsymbol{r})} \right|^n \leq \chi n^{-1/5}. \tag{B.5}
$$

Proof. Let us consider

$$\left|\frac{F\left(\boldsymbol{r}\mathrm{e}^{\mathrm{j}\boldsymbol{\theta}}\right)}{F(\boldsymbol{r})}\right|^2 = \frac{\left(\sum_{\boldsymbol{k}} F_{\boldsymbol{k}}\boldsymbol{r}^{\boldsymbol{k}}\mathrm{e}^{\mathrm{j}\boldsymbol{k}^T\boldsymbol{\theta}}\right)\left(\sum_{\boldsymbol{l}} F_{\boldsymbol{l}}\boldsymbol{r}^{\boldsymbol{l}}\mathrm{e}^{-\mathrm{j}\boldsymbol{l}^T\boldsymbol{\theta}}\right)}{|F(\boldsymbol{r})|^2} = \frac{\sum_{\boldsymbol{k},\boldsymbol{l}} F_{\boldsymbol{k}}F_{\boldsymbol{l}}\boldsymbol{r}^{\boldsymbol{k}+\boldsymbol{l}}\mathrm{e}^{\mathrm{j}(\boldsymbol{k}-\boldsymbol{l})^T\boldsymbol{\theta}}}{|F(\boldsymbol{r})|^2}$$

$$= 1 - \frac{\sum_{\boldsymbol{k}\neq\boldsymbol{l}} F_{\boldsymbol{k}}F_{\boldsymbol{l}}\boldsymbol{r}^{\boldsymbol{k}+\boldsymbol{l}}\left[1-\cos\left((\boldsymbol{k}-\boldsymbol{l})^T\boldsymbol{\theta}\right)\right]}{|F(\boldsymbol{r})|^2}$$

and, by choosing $\widetilde{\boldsymbol{k}}, \widetilde{\boldsymbol{l}} \in \mathscr{F}$, we obtain

$$\left|\frac{F\left(\boldsymbol{r}\mathrm{e}^{\mathrm{j}\boldsymbol{\theta}}\right)}{F(\boldsymbol{r})}\right|^2 \leq 1 - \frac{F_{\widetilde{\boldsymbol{k}}}F_{\widetilde{\boldsymbol{l}}}\boldsymbol{r}^{\widetilde{\boldsymbol{k}}+\widetilde{\boldsymbol{l}}}\left[1-\cos\left((\widetilde{\boldsymbol{k}}-\widetilde{\boldsymbol{l}})^T\boldsymbol{\theta}\right)\right]}{|F(\boldsymbol{r})|^2}$$

$$\leq \frac{1 - F_{\widetilde{\boldsymbol{k}}}F_{\widetilde{\boldsymbol{l}}}\boldsymbol{r}^{\widetilde{\boldsymbol{k}}+\widetilde{\boldsymbol{l}}}\left[\frac{1}{2}|(\widetilde{\boldsymbol{k}}-\widetilde{\boldsymbol{l}})^T\boldsymbol{\theta}|^2 - \frac{1}{6}|(\widetilde{\boldsymbol{k}}-\widetilde{\boldsymbol{l}})^T\boldsymbol{\theta}|^3\right]}{|F(\boldsymbol{r})|^2}.$$

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 the last inequality, we find that there exists a constant $\chi = \chi(F, \boldsymbol{r}) \in \mathbb{R}^+$, that only depends on F and $\boldsymbol{r}$, such that

$$\left|\frac{F\left(\boldsymbol{r}\mathrm{e}^{\mathrm{j}\boldsymbol{\theta}}\right)}{F(\boldsymbol{r})}\right|^2 \leq 1 - \chi||\boldsymbol{\theta}||_2^2. \tag{B.6}$$

Since $\langle\mathscr{F}\rangle = \mathbb{Z}^\eta$, the standard results of Fourier analysis [48] 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 due to the fact that region $[-\pi, \pi]^\eta \setminus (-\varepsilon, \varepsilon)^\eta$ is compact and on the basis of continuity arguments we obtain 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 (B.6) is also true for $\boldsymbol{\theta} \in [-\pi, \pi)^\eta \setminus (-\varepsilon, \varepsilon)^\eta$.

From inequality (B.6), it follows that $\forall \boldsymbol{\theta} \in [-\pi, \pi)^\eta \setminus [-n^{-2/5}, n^{-2/5}]$

$$\left|\frac{F\left(\boldsymbol{r}\mathrm{e}^{\mathrm{j}\boldsymbol{\theta}}\right)}{F(\boldsymbol{r})}\right|^n \leq \left(1 - \chi||\boldsymbol{\theta}||_2^2\right)^{n/2} \leq \mathrm{e}^{-\chi n^{1/5}} \leq \chi n^{-1/5}.$$

∎

Appendix C. Proof of Theorem 6.2. In this subsection, we split the proof of Theorem 6.2 into two parts. The first considers the case of $\langle\mathscr{F}\rangle = \mathbb{Z}^\eta$. However, if $\langle\mathscr{F}\rangle = \mathbb{Z}^\nu \subset \mathbb{Z}^\eta$, the saddle-point approximation cannot be applied directly to the generating function. In the second part of the proof, we show that we can reformulate the problem in such a way that the conditions that are necessary to apply the saddle-point method are satisfied.

Proof of Theorem 6.2. *Proof.* [Proof of Theorem 6.2 with $\langle \mathscr{F} \rangle = \mathbb{Z}^\eta$] On the basis of Lemma B.2 we know that there exists a unique solution $\widetilde{\boldsymbol{x}} \in \Sigma^+ = (\mathbb{R}^+)^\eta \cap \Sigma$ to $\Delta(\boldsymbol{x}) = \boldsymbol{\omega}$, in which $\Delta = \Delta[F]$ is defined in (6.9). According to the residue theorem [49] and choosing the integration surface to be a sphere of radius $\widetilde{\boldsymbol{x}}$ we obtain

$$\begin{aligned}
&\operatorname{coeff}\left\{S(\boldsymbol{x})[F(\boldsymbol{x})]^{\alpha_n n}, \boldsymbol{\omega}_n \alpha_n n\right\}\\
&\quad= \frac{1}{(2\pi)^\eta} \int_{[-\pi,\pi]^\eta} S\left(\widetilde{\boldsymbol{x}} \mathrm{e}^{\mathrm{j}\boldsymbol{\theta}}\right) \frac{F\left(\widetilde{\boldsymbol{x}} \mathrm{e}^{\mathrm{j}\boldsymbol{\theta}}\right)^{\alpha_n n}}{\widetilde{\boldsymbol{x}}^{\alpha_n n \boldsymbol{\omega}_n} \mathrm{e}^{\mathrm{j}\alpha_n n \boldsymbol{\theta}^T \boldsymbol{\omega}_n}} \mathrm{d}\boldsymbol{\theta}\\
&\quad= \frac{1}{(2\pi)^\eta} S(\widetilde{\boldsymbol{x}}) \frac{F\left(\widetilde{\boldsymbol{x}}\right)^{\alpha_n n}}{\widetilde{\boldsymbol{x}}^{\alpha_n n \boldsymbol{\omega}}} \int_{[-\pi,\pi]^\eta} \frac{S\left(\widetilde{\boldsymbol{x}} \mathrm{e}^{\mathrm{j}\boldsymbol{\theta}}\right)}{S\left(\widetilde{\boldsymbol{x}}\right)} \frac{F\left(\widetilde{\boldsymbol{x}} \mathrm{e}^{\mathrm{j}\boldsymbol{\theta}}\right)^{\alpha_n n}}{F\left(\widetilde{\boldsymbol{x}}\right)^{\alpha_n n}} \mathrm{e}^{-\mathrm{j}\alpha_n n \boldsymbol{\theta}^T \boldsymbol{\omega}_n} \mathrm{d}\boldsymbol{\theta}.
\end{aligned}$$

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 $[-\pi, \pi]^\eta \setminus \Theta$:

$$\begin{aligned}
&\operatorname{coeff}\left\{S(\boldsymbol{x})[F(\boldsymbol{x})]^{\alpha_n n}, \boldsymbol{\omega}_n \alpha_n n\right\}\\
&= S(\boldsymbol{x}) \frac{F\left(\widetilde{\boldsymbol{x}}\right)^{\alpha_n n}}{\widetilde{\boldsymbol{x}}^{\alpha_n n \boldsymbol{\omega}_n}} \left[\frac{1}{(2\pi)^\eta} \int_{[-\pi,\pi]^\eta \setminus \Theta} \frac{S\left(\widetilde{\boldsymbol{x}} \mathrm{e}^{\mathrm{j}\boldsymbol{\theta}}\right)}{S\left(\widetilde{\boldsymbol{x}}\right)} \frac{F\left(\widetilde{\boldsymbol{x}} \mathrm{e}^{\mathrm{j}\boldsymbol{\theta}}\right)^{\alpha_n n}}{F\left(\widetilde{\boldsymbol{x}}\right)^{\alpha_n n}} \mathrm{e}^{-\mathrm{j}n\alpha_n \boldsymbol{\theta}^T \boldsymbol{\omega}_n} \mathrm{d}\boldsymbol{\theta}\right.\\
&\left.+ \frac{1}{(2\pi)^\eta} \int_{\Theta} \frac{S\left(\widetilde{\boldsymbol{x}} \mathrm{e}^{\mathrm{j}\boldsymbol{\theta}}\right)}{S\left(\widetilde{\boldsymbol{x}}\right)} \frac{F\left(\widetilde{\boldsymbol{x}} \mathrm{e}^{\mathrm{j}\boldsymbol{\theta}}\right)^{\alpha_n n}}{F\left(\widetilde{\boldsymbol{x}}\right)^{\alpha_n n}} \mathrm{e}^{-\mathrm{j}\alpha_n n \boldsymbol{\theta}^T \boldsymbol{\omega}_n} \mathrm{d}\boldsymbol{\theta}\right].
\end{aligned}$$

According to Lemma B.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 beacuse of inequality (B.6) we also have $\left|S\left(\widetilde{\boldsymbol{x}} \mathrm{e}^{\mathrm{j}\boldsymbol{\theta}}\right)/S\left(\widetilde{\boldsymbol{x}}\right)\right| < 1$. It follows that

$$\begin{aligned}
&\left|\frac{1}{(2\pi)^\eta} \int_{[-\pi,\pi]^\eta \setminus \Theta} \frac{S\left(\widetilde{\boldsymbol{x}} \mathrm{e}^{\mathrm{j}\boldsymbol{\theta}}\right)}{S\left(\widetilde{\boldsymbol{x}}\right)} \frac{F\left(\widetilde{\boldsymbol{x}} \mathrm{e}^{\mathrm{j}\boldsymbol{\theta}}\right)^{\alpha_n n}}{F\left(\widetilde{\boldsymbol{x}}\right)^{\alpha_n n}} \mathrm{e}^{-\mathrm{j}\alpha_n n \boldsymbol{\theta}^T \boldsymbol{\omega}_n} \mathrm{d}\boldsymbol{\theta}\right|\\
&\qquad \leq \frac{1}{(2\pi)^\eta} \int_{[-\pi,\pi]^\eta \setminus \Theta} \left|\frac{S\left(\widetilde{\boldsymbol{x}} \mathrm{e}^{\mathrm{j}\boldsymbol{\theta}}\right)}{S\left(\widetilde{\boldsymbol{x}}\right)}\right| \left|\frac{F\left(\widetilde{\boldsymbol{x}} \mathrm{e}^{\mathrm{j}\boldsymbol{\theta}}\right)}{F\left(\widetilde{\boldsymbol{x}}\right)}\right|^{\alpha_n n} \mathrm{d}\boldsymbol{\theta} = O\left(n^{-1/5}\right),
\end{aligned}$$

and the contribution to the integral from the $[-\pi, \pi]^\eta \setminus \Theta$ region 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 obtain

$$\begin{aligned}
&\frac{1}{(2\pi)^\eta} \int_{\Theta} \frac{S\left(\widetilde{\boldsymbol{x}} \mathrm{e}^{\mathrm{j}\boldsymbol{\theta}}\right)}{S\left(\widetilde{\boldsymbol{x}}\right)} \frac{F\left(\widetilde{\boldsymbol{x}} \mathrm{e}^{\mathrm{j}\boldsymbol{\theta}}\right)^{\alpha_n n}}{F\left(\widetilde{\boldsymbol{x}}\right)^{\alpha_n n}} \mathrm{e}^{-\mathrm{j}\alpha_n n \boldsymbol{\theta}^T \boldsymbol{\omega}_n} \mathrm{d}\boldsymbol{\theta} =\\
&= \frac{1}{(2\pi)^\eta} \int_{\Theta} \mathrm{e}^{\mathrm{j}\boldsymbol{\theta}^T \boldsymbol{\Delta}[S](\widetilde{\boldsymbol{x}}) - \frac{1}{2}\boldsymbol{\theta}^T \boldsymbol{\Gamma}[S](\widetilde{\boldsymbol{x}})\boldsymbol{\theta} + O(||\boldsymbol{\theta}||^3) + \mathrm{j}\alpha_n n \boldsymbol{\theta}^T \boldsymbol{\Delta}[F](\widetilde{\boldsymbol{x}}) - \frac{\alpha_n n}{2}\boldsymbol{\theta}^T \boldsymbol{\Gamma}[F](\widetilde{\boldsymbol{x}})\boldsymbol{\theta} + \alpha_n n O(||\boldsymbol{\theta}||^3)} \times\\
&\times \mathrm{e}^{-\mathrm{j}\alpha_n n \boldsymbol{\theta}^T \boldsymbol{\omega}_n} \mathrm{d}\boldsymbol{\theta}\\
&= \frac{1}{(2\pi)^\eta} \int_{\Theta} \mathrm{e}^{\mathrm{j}\boldsymbol{\theta}^T \boldsymbol{\Delta}[S](\widetilde{\boldsymbol{x}}) - \frac{1}{2}\boldsymbol{\theta}^T \boldsymbol{\Gamma}[S](\widetilde{\boldsymbol{x}})\boldsymbol{\theta} + O(||\boldsymbol{\theta}||^3) - \frac{\alpha_n n}{2}\boldsymbol{\theta}^T \boldsymbol{\Gamma}[F](\widetilde{\boldsymbol{x}})\boldsymbol{\theta} + \alpha_n n O(||\boldsymbol{\theta}||^3)} \times\\
&\times \mathrm{e}^{-\mathrm{j}\alpha_n n \boldsymbol{\theta}^T (\boldsymbol{\omega}_n - \boldsymbol{\omega})} \mathrm{d}\boldsymbol{\theta}
\end{aligned}$$

where the last equality is obtained from $\boldsymbol{\Delta}[F](\widetilde{\boldsymbol{x}}) = \boldsymbol{\omega}$.

It should be noted 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 $\boldsymbol{\Gamma}[S](\widetilde{\boldsymbol{x}})$ is symmetric and positive definitive (see Lemma B.3), there exist $\mathbf{P}, \boldsymbol{\Lambda}$

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 obtain

$$\begin{aligned}
&\frac{1}{(2\pi)^\eta}\int_\Theta \frac{S\left(\widetilde{\boldsymbol{x}}\mathrm{e}^{\mathrm{j}\boldsymbol{\theta}}\right)}{S\left(\widetilde{\boldsymbol{x}}\right)}\frac{F\left(\widetilde{\boldsymbol{x}}\mathrm{e}^{\mathrm{j}\boldsymbol{\theta}}\right)^{\alpha_n n}}{F\left(\widetilde{\boldsymbol{x}}\right)^{\alpha_n n}}\mathrm{e}^{-\mathrm{j}\alpha_n n\boldsymbol{\theta}^T\boldsymbol{\omega}_n}\mathrm{d}\boldsymbol{\theta} = \\
&\quad = \frac{1}{(2\pi)^\eta}\int_\Theta \mathrm{e}^{-\frac{\alpha_n n}{2}\boldsymbol{\theta}^T\mathbf{\Gamma}[F](\widetilde{\boldsymbol{x}})\boldsymbol{\theta}+O(n^{-1/5})-\mathrm{j}[\alpha_n n\boldsymbol{\theta}^T(\boldsymbol{\omega}_n-\boldsymbol{\omega})-\boldsymbol{\theta}^T\mathbf{\Delta}[S](\widetilde{\boldsymbol{x}})]}\mathrm{d}\boldsymbol{\theta} \\
&\quad = \frac{1}{(2\pi)^\eta}\int_\Theta \mathrm{e}^{-\frac{\alpha_n n}{2}\boldsymbol{\theta}^T\mathbf{\Gamma}[F](\widetilde{\boldsymbol{x}})\boldsymbol{\theta}-\mathrm{j}[\alpha_n n\boldsymbol{\theta}^T(\boldsymbol{\omega}_n-\boldsymbol{\omega})-\boldsymbol{\theta}^T\mathbf{\Delta}[S](\widetilde{\boldsymbol{x}})]}\left(1+O\left(n^{-1/5}\right)\right)\mathrm{d}\boldsymbol{\theta}.
\end{aligned}$$

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 obtain

$$\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}})|}}\left[\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}\right. \\
&\left.-\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}\right] \\
&= \frac{\left(1+O\left(n^{-1/5}\right)\right)}{\sqrt{(2\pi\alpha_n n)^\eta|\mathbf{\Gamma}(\widetilde{\boldsymbol{x}})|}}\left[\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})}\right. \\
&\left.-\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}\right].
\end{aligned}$$

Since $\mathbf{\Gamma}[F](\widetilde{\boldsymbol{x}})$ is symmetric and positive definitive (see Lemma B.3), there exists $\mathbf{Q}, \mathbf{D}$, 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

$$\begin{aligned}
&\left|\int_{\mathbb{R}^\eta\setminus\left[-(\alpha_n n)^{1/10},(\alpha_n n)^{1/10}\right]^\eta} \mathrm{e}^{-\frac{1}{2}\boldsymbol{\sigma}^T\mathbf{\Gamma}(\widetilde{\boldsymbol{x}})\boldsymbol{\sigma}-\mathrm{j}[\sqrt{\alpha_n n}\boldsymbol{\sigma}^T(\boldsymbol{\omega}_n-\boldsymbol{\omega})-\frac{1}{\sqrt{\alpha_n n}}\boldsymbol{\sigma}^T\mathbf{\Delta}[S](\widetilde{\boldsymbol{x}})]}\mathrm{d}\boldsymbol{\sigma}\right| \\
&\qquad \le \int_{||\boldsymbol{y}||^2\ge(\alpha_n n)^{1/10}} \mathrm{e}^{-\frac{1}{2}D_{\min}||\boldsymbol{y}||^2}\mathrm{d}\boldsymbol{y} = O\left(\frac{\mathrm{e}^{-(\alpha_n n)^{1/5}}}{(\alpha_n n)^{1/10}}\right) = O(n^{-1/10}).
\end{aligned}$$

We obtain

$$
\begin{aligned}
&\frac{1}{(2\pi)^\eta}\int_\Theta \frac{S\left(\widetilde{\boldsymbol{x}}\mathrm{e}^{\mathrm{j}\boldsymbol{\theta}}\right)}{S\left(\widetilde{\boldsymbol{x}}\right)}\frac{F\left(\widetilde{\boldsymbol{x}}\mathrm{e}^{\mathrm{j}\boldsymbol{\theta}}\right)^{\alpha_n n}}{F\left(\widetilde{\boldsymbol{x}}\right)^{\alpha_n n}}\mathrm{e}^{-\mathrm{j}\alpha_n n\boldsymbol{\omega}_n\boldsymbol{\theta}^T}\mathrm{d}\boldsymbol{\theta}\\
&\quad\le \frac{\left(1+O\left(n^{-1/5}\right)\right)}{\sqrt{(2\pi\alpha_n n)^\eta|\boldsymbol{\Gamma}(\widetilde{\boldsymbol{x}})|}}\left[\mathrm{e}^{-\frac{1}{2}\alpha_n n D_{\min}^{-1}||\boldsymbol{\omega}_n-\boldsymbol{\omega}||^2}+O(n^{-1/10})\right]\\
&\quad= \frac{\left(1+O\left(n^{-1/5}\right)\right)}{\sqrt{(2\pi\alpha_n n)^\eta|\boldsymbol{\Gamma}(\widetilde{\boldsymbol{x}})|}}\left[\mathrm{e}^{O\left(\frac{1}{n}\right)}+O(n^{-1/10})\right]\\
&\quad\frac{\left(1+O\left(n^{-1/5}\right)\right)}{\sqrt{(2\pi\alpha_n n)^\eta|\boldsymbol{\Gamma}(\widetilde{\boldsymbol{x}})|}}\left[1+O(n^{-1/10})\right]
\end{aligned}
$$

and we can 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

$$
\lim_{n\in\mathcal{N}}\frac{1}{n}\ln\left(\operatorname{coeff}\{S(\widetilde{\boldsymbol{x}})[F(\boldsymbol{x})]^{\alpha_n n},\boldsymbol{x}^{\boldsymbol{\omega}_n\alpha_n n}\}\right)=\alpha\ln F(\widetilde{\boldsymbol{x}})-\alpha\ \boldsymbol{\omega}\cdot\ln\widetilde{\boldsymbol{x}}
$$

It should be noted that $o(1)$ is independent of $\boldsymbol{\omega}_n$, and the convergence in (6.11) is uniform in $\boldsymbol{\omega}\in\mathring{\operatorname{co}}(\mathscr{F})$.

□

Proof. [Proof of Theorem 6.2 with $\langle\mathscr{F}\rangle\subset\mathbb{Z}^\eta$] If $\langle\mathscr{F}\rangle\subset\mathbb{Z}^\eta$, the saddle-point approximation cannot be applied directly to function $B(\boldsymbol{x})=S(\boldsymbol{x})[F(\boldsymbol{x})]^{\alpha_n n}$.

Since submodules of free modules over a Noetherian ring are free [50], there exists a basis, $\mathcal{B}=\{\boldsymbol{b}^1,\dots,\boldsymbol{b}^\nu\}$, with $|\mathcal{B}|=\nu\le\eta$ of $\langle\mathscr{F}\rangle$, and each element in $\mathscr{F}$ can be expressed in a unique way as a finite sum of the elements in $\mathcal{B}$ multiplied by some coefficients in $\mathbb{Z}$:

$$
\boldsymbol{k}=\sum_{\boldsymbol{b}\in\mathcal{B}}\gamma_{\boldsymbol{b}}(\boldsymbol{k})\boldsymbol{b},\qquad \boldsymbol{k}\in\mathscr{F}.
$$

On the basis of this hypothesis the elements in $\mathscr{S}=\{\boldsymbol{l}|S_{\boldsymbol{l}}>0\}$ can also be written as follows

$$
\boldsymbol{l}=\sum_{\boldsymbol{b}\in\mathcal{B}}\gamma_{\boldsymbol{b}}(\boldsymbol{l})\boldsymbol{b},\qquad \boldsymbol{l}\in\mathscr{S}.
$$

Let us 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 $\mathscr{G}=\{\boldsymbol{\gamma}\in\mathbb{Z}^\nu: G_{\boldsymbol{\gamma}}>0\}$.

We obtain

$$
\begin{aligned}
F(\boldsymbol{x})&=\sum_{\boldsymbol{k}\in\mathscr{F}}F_{\boldsymbol{k}}\boldsymbol{x}^{\boldsymbol{k}}=\sum_{\boldsymbol{\gamma}\in\mathscr{G}}G_{\boldsymbol{\gamma}}\boldsymbol{x}^{\sum_{\boldsymbol{b}\in\mathcal{B}}\gamma_{\boldsymbol{b}}\boldsymbol{b}}=\sum_{\boldsymbol{\gamma}\in\mathscr{G}}G_{\boldsymbol{\gamma}}\prod_{\boldsymbol{b}\in\mathcal{B}}\boldsymbol{x}^{\gamma_{\boldsymbol{b}}\boldsymbol{b}}\\
&=\sum_{\boldsymbol{\gamma}\in\mathscr{G}}G_{\boldsymbol{\gamma}}\prod_{\boldsymbol{b}\in\mathcal{B}}\left(\boldsymbol{x}^{\boldsymbol{b}}\right)^{\gamma_{\boldsymbol{b}}}=\sum_{\boldsymbol{\gamma}\in\mathscr{G}}G_{\boldsymbol{\gamma}}\boldsymbol{w}^{\boldsymbol{\gamma}}=G(\boldsymbol{w}).
\end{aligned}
$$

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 $n \to \infty$, $\boldsymbol{\xi}_n$ is a convergent sequence to $\boldsymbol{\xi}$ in which $\boldsymbol{\xi}$ satisfies $\sum_{\boldsymbol{b}\in\mathcal{B}} \xi_{\boldsymbol{b}}\boldsymbol{b} = \boldsymbol{\omega}$.

It is trivial to comprehend that if $\boldsymbol{\omega} \in \overset{\circ}{\operatorname{co}}(\mathscr{F})$, then $\boldsymbol{\xi} \in \overset{\circ}{\operatorname{co}}(\mathscr{G})$. We can conclude by means of Lemma B.2, that there exists a solution $\widetilde{\boldsymbol{w}} \in (\mathbb{R}^+)^\nu$ of $\Delta[G](\boldsymbol{w}) = \boldsymbol{\xi}$.

Moreover, 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 the 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

$$\lim_{n\to\infty} \frac{1}{n} \ln \operatorname{coeff}\left\{T(\boldsymbol{w})[G(\boldsymbol{w})]^{\alpha_n n}, \boldsymbol{w}^{\boldsymbol{\xi}_n \alpha_n n}\right\} = \alpha \ln G(\widetilde{\boldsymbol{w}}) - \alpha\, \boldsymbol{\xi} \cdot \ln \widetilde{\boldsymbol{w}}. \tag{C.1}$$

Since $\widetilde{\boldsymbol{w}}$ is a solution of $\Delta[G](\boldsymbol{w}) = \boldsymbol{\xi}$, we obtain

$$\sum_{i=1}^{\nu} \Delta_i[G](\widetilde{\boldsymbol{w}})\boldsymbol{b}^{(i)} = \sum_{i=1}^{\nu} \frac{\widetilde{w}_i}{G(\widetilde{\boldsymbol{w}})} \frac{\partial G}{\partial w_i}\bigg|_{\widetilde{\boldsymbol{w}}} \boldsymbol{b}^{(i)} = \boldsymbol{\omega}$$

from which we find 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 can conclude that

$$\Delta[G](\widetilde{\boldsymbol{w}}) = \boldsymbol{\xi} \iff \Delta[F](\widetilde{\boldsymbol{x}}) = \boldsymbol{\omega},$$

and for $n \to \infty$

$$\operatorname{coeff}\left\{S(\boldsymbol{x})[F(\boldsymbol{x})]^{\alpha_n n}, \boldsymbol{x}^{\boldsymbol{\xi}_n \alpha_n n}\right\} = \frac{S(\widetilde{\boldsymbol{x}})}{\sqrt{(2\pi\alpha_n n)^\nu |\boldsymbol{\Gamma}[F](\widetilde{\boldsymbol{x}})|}} \frac{[F(\widetilde{\boldsymbol{x}})]^{\alpha_n n}}{\widetilde{\boldsymbol{x}}^{\boldsymbol{\omega}_n \alpha_n n}}(1 + o(1)).$$

$$
\begin{aligned}
\lim_{n\to\infty} \operatorname{coeff}\left\{F(\boldsymbol{x})^{\alpha_n n}, \boldsymbol{x}^{\boldsymbol{\omega}_n \alpha_n n}\right\} &= \alpha \ln G(\widetilde{\boldsymbol{w}}) - \alpha \sum_{i=1}^{\nu} \xi_i \ln \widetilde{w}_i \\
&= \alpha \ln F(\widetilde{\boldsymbol{x}}) - \alpha \sum_{i=1}^{\nu} \xi_i \ln \widetilde{\boldsymbol{x}}^{\boldsymbol{b}^{(i)}} \\
&= \alpha \ln F(\widetilde{\boldsymbol{x}}) - \alpha \sum_{i=1}^{\nu} \xi_i \ln \left(\prod_{j=1}^{\eta} \widetilde{x}_j^{b_j^{(i)}} \right) \\
&= \alpha \ln F(\widetilde{\boldsymbol{x}}) - \alpha \sum_{i=1}^{\nu} \xi_i \sum_{j=1}^{\eta} b_j^{(i)} \ln \widetilde{x}_j \\
&= \alpha \ln F(\widetilde{\boldsymbol{x}}) - \alpha \sum_{j=1}^{\eta} \ln(\widetilde{x}_j) \sum_{i=1}^{\nu} \xi_i b_j^i \\
&= \alpha \ln F(\widetilde{\boldsymbol{x}}) - \alpha \boldsymbol{\omega} \cdot \ln \widetilde{\boldsymbol{x}}.
\end{aligned}
$$

□