Foundations and Trends® in Communications and
Information Theory
Vol. XX, No. XX (2017) 1–140

DOI: 10.1561/XXXXXXXXXX

Redundancy of Lossless Data Compression for Known Sources by Analytic Methods

Michael Drmota
TU Wien
michael.drmota@tuwien.ac.at

Wojciech Szpankowski
Purdue University
spa@cs.purdue.edu

Contents

Abstract

Lossless data compression is a facet of source coding and a well studied problem of information theory. Its goal is to find a shortest possible code that can be unambiguously recovered. Here, we focus on rigorous analysis of code redundancy for *known sources*. The redundancy rate problem determines by how much the actual code length exceeds the optimal code length. We present precise analyses of three types of lossless data compression schemes, namely fixed-to-variable (FV) length codes, variable-to-fixed (VF) length codes, and variable-to-variable (VV) length codes. In particular, we investigate the average redundancy of Shannon, Huffman, Tunstall, Khodak and Boncelet codes. These codes have succinct representations as trees, either as coding or parsing trees, and we analyze here some of their parameters (e.g., the average path from the root to a leaf). Such trees are precisely analyzed by analytic methods, known also as analytic combinatorics, in which complex analysis plays decisive role. These tools include generating functions, Mellin transform, Fourier series, saddle point method, analytic poissonization and depoissonization, Tauberian theorems, and singularity analysis. The term *analytic information theory* has been coined to describe problems of information theory studied by analytic tools. This approach lies on the crossroad of information theory, analysis of algorithms, and combinatorics.

M. Drmota and W. Szpankowski. *Redundancy of Lossless Data Compression for Known Sources by Analytic Methods*. Foundations and Trends$^{®}$ in Communications and Information Theory, vol. XX, no. XX, pp. 1–140, 2017.
DOI: 10.1561/XXXXXXXXXX.

1

Introduction

The basic problem of *source coding* better known as (lossless) *data compression* is to find a binary code that can be unambiguously recovered with shortest possible description either on average or for individual sequences. Thanks to Shannon's work we know that on average the number of bits per source symbol cannot be smaller than the source entropy rate. There are many codes asymptotically achieving the entropy rate, therefore one turns attention to *redundancy.* The average redundancy of a source code is the amount by which the expected number of binary digits per source symbol for that code exceeds entropy. One of the goals in designing source coding algorithms is to minimize the redundancy. In this survey, we discuss various classes of source coding and their corresponding redundancy. It turns out that such analyses often resort to studying certain intriguing trees such as Huffman, Tunstall, Khodak and Boncelet trees, as well as various algorithms such as divide-and-conquer approach. We study them using tools from the analysis of algorithms and analytic combinatorics[1] to discover precise and minute behavior of lossless compression codes.

[1] Andrew Odlyzko has argued that: "analytic methods are extremely powerful and when they apply, they often yield estimates of unparalleled precision."

Lossless data compression comes in three flavors: fixed-to-variable (FV) length codes, variable-to-fixed (VF) length codes, and finally variable-to-variable (VV) length codes. The latter includes the previous two families of codes and is the least studied among all data compression schemes. Over years we have seen a resurgence of interest in redundancy rate for *fixed-to-variable* coding (cf. [25, 28, 29, 30, 66, 90, 91, 92, 101, 103, 124, 126, 131, 133, 132, 140, 141, 152, 153, 165, 174, 181, 177, 178]). Surprisingly there are only a handful of results for variable-to-fixed codes (cf. [77, 97, 112, 134, 132, 135, 157, 162, 186]) and an almost non-existing literature on variable-to-variable codes (cf. [42, 50, 80, 97]). While there is some work on universal VF codes [157, 162, 186], to the best of our knowledge redundancy for universal VF and VV codes were not studied with the exception of some work of the Russian school [97, 96] (cf. also [99]).

In the fixed-to-variable code, discussed in Chapter 3, the encoder maps fixed length blocks of source symbols into variable-length binary code strings. Two important fixed-to-variable length coding schemes are the Shannon code and the Huffman code. In this survey we follow [153, 114]. We first discuss precise analyses of Shannon code redundancy for memoryless and Markov sources. We show that the average redundancy either converges to an explicitly computable constant, as the block length increases, or it exhibits a very erratic behavior fluctuating between 0 and 1. We also observe a similar behavior for the worst case or maximal redundancy. Then we move to the Huffman code. Despite the fact that Huffman codes have been so well known for so long, it was only relatively recently that their redundancy was fully understood. In [1] Abrahams summarizes much of the vast literature on fixed-to-variable length codes. Here, we present a precise analysis from our work [153] of the Huffman average redundancy for memoryless sources. We show that the average redundancy either converges to an explicitly computable constant, as the block length increases, or it exhibits a very erratic behavior fluctuating between 0 and 1. Following [114] we also present similar results for Markov sources.

Next, in Chapter 4 we study variable-to-fixed codes. A VF encoder partitions the source string into variable-length phrases that belong to a given dictionary $\mathcal{D}$. Often a dictionary is represented by a complete tree (i.e., a tree in which every node has maximum degree), also known as the *parsing tree*. The code assigns a fixed-length word to each dictionary entry. An important example of a variable-to-fixed code is the Tunstall code [158]. Savari and Gallager [132] present an analysis of the dominant term in the asymptotic expansion of the Tunstall code redundancy. In this survey, following [34], we describe a precise analysis of the phrase length (i.e., path from the root to a terminal node in the corresponding parsing tree) for such a code and its average redundancy. We also discuss a variant of Tunstall code known as VF Khodak code.

In the next Chapter 5 we continue analyzing VF codes due to Boncelet [15] who used the *divide-and-conquer principle* to design a practical encoding. Boncelet's algorithm is computationally fast and its practicality stems from the divide and conquer strategy: It splits the input (e.g., parsing tree) into several smaller subproblems, solving each subproblem separately, and then knitting together to solve the original problem. We use this occasion to present a careful analysis of a divide-and conquer recurrence which is at foundation of several divide-and-conquer algorithms such as heapsort, mergesort, discrete Fourier transform, queues, sorting networks, compression algorithms, and so forth [47, 86, 154].

In Chapter 6 we consider variable-to-variable codes. A variable-to-variable (VV) code is a concatenation of variable-to-fixed and fixed-to-variable codes. A variable-to-variable length encoder consists of a *parser* and a *string encoder*. The parser, as in VF codes, segments the source sequence into a concatenation of phrases from a predetermined dictionary $\mathcal{D}$. Next, the string encoder in a variable-to-variable scheme takes the sequence of dictionary strings and maps each one into its corresponding binary codeword of variable length. Aside from the special cases where either the dictionary strings or the codewords have a fixed length, very little is known about variable-to-variable length codes, even in the case of memoryless sources. In 1972 Khodak [80] described a VV scheme with small average redundancy that decreases with the growth of phrase length. He did not offer, however, an explicit VV code construction. We will remedy this situation and follow [16] to propose a transparent proof.

Finally, in Chapter 7 we discuss redundancy of one-to-one codes that are not necessarily prefix or even uniquely decodable. Recall that non-prefix codes are such codes which are not prefix free and do not satisfy Kraft's inequality. In particular, we analyze binary and non-binary one-to-one codes whose average lengths are smaller than the source entropy in defiance of the Shannon lower bound.

Throughout this survey, we study various intriguing trees describing Huffman, Tunstall, Khodak and Boncelet codes. These trees are studied by analytic techniques of analysis of algorithms [47, 85, 86, 87, 154]. The program of applying tools from analysis of algorithms to problems of source coding and in general to information theory lies at the crossroad of computer science and information theory. It is also known as *analytic information theory.* In fact, the interplay between information theory and computer science dates back to the founding father of information theory, Claude E. Shannon. His landmark paper "A Mathematical Theory of Communication" is hailed as the foundation for information theory. Shannon also worked on problems in computer science such as chess-playing machines and computability of different Turing machines. Ever since Shannon's work on both information theory and computer science, the research at the interplay between these two fields has continued and expanded in many exciting ways. In the late 1960s and early 1970s, there were tremendous interdisciplinary research activities, exemplified by the work of Kolmogorov, Chaitin, and Solomonoff, with the aim of establishing algorithmic information theory. Motivated by approaching Kolmogorov complexity algorithmically, A. Lempel (a computer scientist), and J. Ziv (an information theorist) worked together in the late 1970s to develop compression algorithms that are now widely referred to as Lempel-Ziv algorithms. Analytic information theory is a continuation of these efforts.

Finally, we point out that this survey deals only with source coding for *known sources.* The more practical *universal source coding* (in which the source distribution is unknown) is left for our future book *Analytic Information Theory.* However, at the end of this survey we provide an extensive bibliography on the redundancy rate problem, including universal source coding.

This survey is organized as follows. In the next chapter, we present some preliminary results such as Kraft's inequality, Shannon's lower bound, and Barron's lemma. In Section 3 we analyze Shannon and Huffman codes. Then we turn our attention in Section 4 to the Tunstall and VF Khodak codes. Finally, in Section 6 we discuss the VV code of Khodak and its interesting analysis. We conclude this survey with a chapter concerning the average redundancy for non-prefix codes such as one-to-one codes.

2

Preliminary Results

Let us start with some definitions and preliminary results. A *(binary) source code* is a one-to-one (or injective) mapping

$$C : \mathcal{A} \to \{0,1\}^+$$

from a finite alphabet $\mathcal{A}$ (the *source*) to the set $\{0,1\}^+$ of binary sequences.[1] Such a mapping can be directly extended to finite sequences of $x_1 \dots x_k$ by concatenation: $\widetilde{C}(x_1 \dots x_k) = C(x_1) \dots C(x_k)$, that is, to a mapping

$$\widetilde{C} : \ \mathcal{A}^+ \to \{0,1\}^+.$$

A code C is *uniquely decodable* if the extension $\widetilde{C}$ is one-to-one. In particular if C is a *prefix code* (or *instantaneous code*), that is, if no codeword $C(x)$ is a prefix of another codeword, then C is uniquely decodable.

We write $L(C,x)$ (or simply $L(x)$) for the length of $C(x)$. If $\mathcal{A}$ is of the form $\mathcal{A} = \mathcal{X}^m$ for some finite set $\mathcal{X}$ and the lengths $L(x)$ are not necessarily constant then C is called fixed-to-variable (FV) length code. Similarly if $\mathcal{A} \subset \mathcal{X}^+$ for some finite set $\mathcal{X}$ and $C(\mathcal{A}) \subset \{0,1\}^k$

[1] It is immediate to extend this concept to m-ary codes $C : \mathcal{A} \to \{0,1,\dots m-1\}^+$. However, in this survey we discuss only binary codes.

for some $k \geq 1$ then C is called variable-to-fixed (VF) length code. Accordingly, variable-to-variable (VV) length codes are defined.

We denote by P a probability distribution on the alphabet $\mathcal{A}$, The elements of the source can be then interpreted as a random variable X with probability distribution $P[X = x] = P(x)$. Such a source is also called *probabilistic source*. For example the code length $L(X)$ is then a random variable, too, and the expected code length $\mathbf{E}[L(X)]$ is an important parameter of a probabilistic source code.

The source *entropy* of a probabilistic source is defined by

$$H(P) = -\mathbf{E}[\log P(X)] = -\sum_{x \in \mathcal{A}} P(x) \log P(x),$$

where shall write log for the logarithm of unspecified base, however, throughout usually the base is equal to 2 unless specified otherwise.

Throughout, we also write $x \in \mathcal{A}^+$ for a sequence of unspecified length, and $x_i^j = x_i \dots x_j \in \mathcal{A}^{j-i+1}$ for a consecutive subsequence of length $j - i + 1$. We will also use the abbreviation $x^n = x_1^n$. Finally, throughout we write $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$ for integer, rational, and real numbers respectively.

2.1 Prefix Codes and Their Properties

As discussed, a *prefix code* is a code for which no codeword $C(x)$ for $x \in \mathcal{A}$ is a prefix of another codeword. For such codes there is a mapping between a code word $C(x)$ and a path in a tree from the root to a terminal (external) node (e.g., for a binary prefix code move to the left in the tree represents 0 and move to the right represents 1), as shown in Figure 2.1. We also point out that a prefix code and the corresponding path in a tree defines a lattice path in the first quadrant also shown in Figure 2.1. Here left L and right R traversals in the parsing tree corresponds to “left” or “up” movement in the lattice. If some additional constraints are imposed on the prefix codes, this translates into certain restrictions on the lattice path indicated as the shaded area in Figure 2.1 (see also Figure 4.2 in Chapter 4 and [38]).

The prefix condition imposes some restrictions on the code length. This fact is known as Kraft’s inequality discussed next.

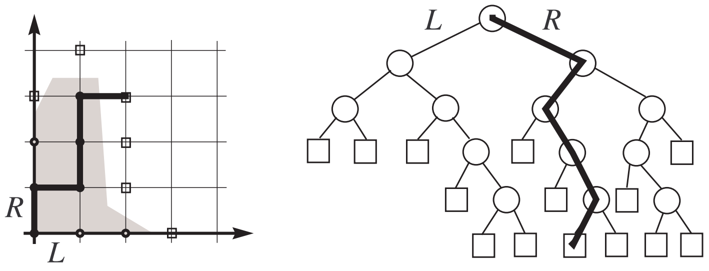


Figure 2.1: Lattice paths and binary trees

Theorem 2.1. [Kraft's Inequality] Let $|\mathcal{A}| = N$. Then for any binary prefix code the codeword lengths $\ell_1, \ell_2, \ldots, \ell_N$ satisfy the inequality

$$\sum_{i=1}^{N} 2^{-\ell_i} \leq 1. \tag{2.1}$$

Conversely, if positive integers $\ell_1, \ell_2, \ldots, \ell_N$ satisfy this inequality, then one can build a prefix code with precisely these codeword lengths.

Proof. This is an easy exercise on trees. Let $\ell_{\max}$ be the maximum codeword length. Observe that at level $\ell_{\max}$ some nodes are codewords, some are descendants of codewords, and some are neither. Since the number of descendants at level $\ell_{\max}$ of a codeword located at level ℓ_i is $2^{\ell_{\max}-\ell_i}$, we obtain

$$\sum_{i=1}^{N} 2^{\ell_{\max}-\ell_i} \leq 2^{\ell_{\max}},$$

which is the desired inequality. The converse part can also be proved, and is left for the reader. □

Using Kraft's inequality we can now prove the first theorem of Shannon (which was first established by Khinchin) that bounds from below the average code length.

Theorem 2.2. For any prefix code the average code length $\mathbf{E}[L(C, X)]$ cannot be smaller than the entropy of the source $H(P)$, that is,

$$\mathbf{E}[L(C, X)] \geq H(P)$$

where the expectation is taken with respect to the distribution P of the source sequence $X \in \mathcal{A}$ and the logarithms in the definition of $H(P)$ is the binary logarithms.

Proof. Let $K = \sum_x 2^{-L(x)} \leq 1$ and $L(x) := L(C, x)$. Then for the binary logarithm $\log = \log_2$

$$\begin{aligned}
\mathbf{E}[L(C,X)] - H(P)] &= \sum_{x\in\mathcal{A}} P(x)L(x) + \sum_{x\in\mathcal{A}} P(x)\log P(x) \\
&= -\sum_{x\in\mathcal{A}} P(x)\log\frac{2^{-L(x)}/K}{P(x)} - \log K \\
&\geq \frac{1}{\ln 2}\left(\sum_{x\in\mathcal{A}} P(x) - \frac{1}{K}\sum_{x\in\mathcal{A}} 2^{-L(x)}\right) - \log K \\
&= -\log K \geq 0
\end{aligned}$$

since $-\log_2 x \geq \frac{1}{\ln 2}(1-x)$ for all $x > 0$ and $K \leq 1$ due to Kraft's inequality. □

Observe that Khinchin's theorem implies the existence of at least one element $\widetilde{x} \in A$ such that

$$L(\widetilde{x}) \geq -\log P(\widetilde{x}). \tag{2.2}$$

In fact this follows from an obvious contradiction that arises if (2.2) is not true. A stronger statement is due to Barron [8] who proved the following result.

Lemma 2.3 (Barron)**.** Let C be a prefix code and $a > 0$. Then

$$P(L(C,X) < -\log P(X) - a) \leq 2^{-a}.$$

Proof. We argue as follows (again $\log = \log_2$):

$$\begin{aligned}
P(L(X) < -\log P(X) - a) &= \sum_{x\colon P(x) < 2^{-L(x)-a}} P(x) \\
&\leq \sum_{x\colon P(x) < 2^{-L(x)-a}} 2^{-L(x)-a} \\
&\leq 2^{-a}\sum_x 2^{-L(x)} \leq 2^{-a},
\end{aligned}$$

where we have used Kraft's inequality. □

What is the best code with respect to code length? We are now in a position to answer this question. As long as the expected code length is concerned, one needs to solve the following constrained optimization problem for:

$$\min_L \sum_x L(x)P(x) \quad \text{subject to} \quad \sum_x 2^{-L(x)} \leq 1.$$

This optimization problem has an easy real valued solution through Lagrangian multipliers, and one finds that the optimal code length is $L(x) = -\log P(x)$ provided the *integer character of the length is ignored.* If it is not ignored, then interesting things happen. First, the excess of the code length over $-\log P(x)$ is called the redundancy and discussed below. Furthermore, to minimize the redundancy, that is, to make $-\log P(x)$ as close to an integer as possible, ingenious algorithms were designed, and one of it, namely the Khodak VV code, is discussed in Chapter 6.

2.2 Redundancy

In general, one needs to round the length to an integer, thereby incurring some cost. This cost is usually known under the name *redundancy.* More precisely, redundancy is the excess of real code length over its ideal (optimal) code length which is assumed to be $-\log P(x)$. There are several possible specification of this general definition. For *known* distribution P, that we assume throughout this survey, the *pointwise redundancy* $R^C(x)$ for a code C and the *average redundancy* $\overline{R}^C$ are defined as

$$\begin{aligned} R^C(x) &= L(C,x) + \log P(x), \\ \overline{R}^C &= \mathbf{E}[L(C,X)] - H(P)]. \end{aligned}$$

Furthermore, Shtarkov introduced the *maximal* or *worst case* redundancy R^* defined as

$$R^* = \max_x [L(C,x) + \log P(x)].$$

The pointwise redundancy can be negative, but the average and worst case redundancies cannot due to the Shannon theorem and (2.2), respectively.

In this survey we analyze the average redundancy and the worst case redundancy for known sources of various prefix codes: Shannon and Huffman fixed-to-variable codes (see Chapter 3), variable-to-fixed Tunstall and Khodak codes (see Chapter 4), divide-and-conquer variable-to-fixed Boncelet code (see Chapter 5, variable-to-variable Khodak code (see Chapter 6), and non prefix one-to-one codes (see Chapter 7).

3

Redundancy of Shannon and Huffman FV Codes

We now turn our attention to fixed-to-variable length codes, in particular to Shannon and Huffman codes. In this chapter, we assume that a known source (i.e., a sequence of random variables) with distribution P generates a sequence $x^n := x_1^n = x_1 \dots x_n$ of *fixed* length n, that is, the alphabet $\mathcal{A}$ is of the form $\mathcal{A} = \mathcal{X}^n$, where we write $\mathcal{X} = \{0, 1, \dots, m-1\}$. The code words $C(x_1^n)$ may be of a variable length. We first analyze the average redundancy for Shannon and Huffman codes for memoryless sources. Then we study Shannon code redundancy for Markov sources. Finally, we consider a code that optimizes the worst case redundancy which turns out to be a generalized Shannon code.

3.1 Average Redundancy for Memoryless Sources

We now assume that a sequence of fixed length n, denoted $x^n = x_1^n$ is generated by a binary memoryless source with p being the probability of emitting 0. We also write $q := 1 - p$. This section, to a large extent, is based on [153].

3.1.1 Shannon Code

The Shannon code assigns to $x^n \in \mathcal{A} = \{0,1\}^n$ a codeword with code length

$$L(x^n) = \lceil -\log P(x^n) \rceil.$$

By Theorem 2.1 such a code always exists, since

$$\sum_{x^n \in \mathcal{A}} 2^{-\lceil -\log P(x^n) \rceil} \leq \sum_{x^n \in \mathcal{A}} P(x^n) = 1.$$

For memoryless source, we have $P(x^n) = p^k q^{n-k}$ where k is the number of 0s in x^n and recall that $q = 1 - p$. Hence, its average redundancy is then

$$\overline{R}_n^S = \sum_{k=0}^{n} \binom{n}{k} p^k q^{n-k} \left(\lceil -\log(p^k q^{n-k}) \rceil + \log p^k q^{n-k} \right).$$

We rewrite it in a slightly different form. Define $\langle x \rangle = x - \lfloor x \rfloor$ as the fractional part of real x. It is easy to see that

$$\lceil -x \rceil + x = \langle x \rangle, \quad x \in \mathbb{R} \tag{3.1}$$

for any real x. Hence we have

$$\overline{R}_n^S = \sum_{k=0}^{n} \binom{n}{k} p^k q^{n-k} \langle \alpha k + \beta n \rangle, \tag{3.2}$$

where

$$\alpha = \log_2 \left(\frac{p}{1-p} \right), \qquad \beta = \log_2 (1-p). \tag{3.3}$$

We are interested in the asymptotics of $\overline{R}_n^S$ given by (3.2). We start with a Fourier series of $\langle x \rangle$, namely (cf. [190]), for $x \in \mathbb{R}$

$$\begin{aligned} \langle x \rangle &= \frac{1}{2} - \sum_{m=1}^{\infty} \frac{\sin 2\pi m x}{m\pi} \\ &= \frac{1}{2} + \sum_{m \in \mathbb{Z} \setminus \{0\}} c_m e^{2\pi i m x}, \qquad c_m = \frac{i}{2\pi m}. \end{aligned} \tag{3.4}$$

Hereafter, we shall write

$$\sum_{m \neq 0} := \sum_{m \in \mathbb{Z} \setminus \{0\}}.$$

Observe that for $x = 0$ and $x = 1$ the right-hand and the left-hand sides of (3.4) do not agree. These are the points of discontinuity of $\langle x \rangle$.

We now continue our evaluation of the average redundancy as expressed in (3.2). Observe that its asymptotic behavior depends on rationality or irrationality of α. Indeed, if α is rational, say $\alpha = 1/2$ and $\beta = 0$, then $\langle \alpha k + \beta n \rangle$ takes only two values (i.e., 0 or 1/2), and hence the average redundancy oscillates. This is not the case when α is irrational. So let's us first deal with the case when α is irrational. Using (3.4) in (3.2) we obtain

$$\begin{aligned} \overline{R}_n^S &= \frac{1}{2} + \sum_{k=0}^{n} \binom{n}{k} p^k q^{n-k} \sum_{m \neq 0} c_m e^{2\pi i m (\alpha k + \beta n)} \\ &= \frac{1}{2} + \sum_{m \neq 0} c_m e^{2\pi i m \beta n} \left(p e^{2\pi i m \alpha} + q \right)^n . \end{aligned} \tag{3.5}$$

Our goal now is to prove that the last sum in the above is $o(1)$ when α is irrational. Of course, if α is irrational then $|pe^{2\pi i m\alpha} + q| < 1$ which implies that $\left(pe^{2\pi i m\alpha} + q\right)^n \to 0$. Hence, it is very likely that $\overline{R}_n^S \to \frac{1}{2}$ as $n \to \infty$. Unfortunately, it seems to be cumbersome to prove this fact directly from the representation (3.5) since the Fourier series does not converge absolutely. However, we can deal with the sum (3.2) directly by applying the theory of *sequences distributed modulo 1* (cf. [40, 98]) and will obtain the following result.

Theorem 3.1. Let $\overline{R}_n^S$ denote the average redundancy of the Shannon code over a binary memoryless source $\mathcal{A} = \{0,1\}^n$ of length n with parameter $p \in (0,1)$. If $p = \frac{1}{2}$, then $\overline{R}_n^S = 0$. If $p \neq \frac{1}{2}$ define α and β by (3.3). Then, as $n \to \infty$

$$\overline{R}_n^S = \begin{cases} \frac{1}{2} + o(1) & \alpha \quad \text{irrational} \\ \\ \frac{1}{2} + \frac{1}{M}\left(\langle M n \beta \rangle - \frac{1}{2} \right) + O(\rho^n) & \alpha = \frac{N}{M}, \quad \gcd(N, M) = 1 \end{cases} \tag{3.6}$$

where $\rho < 1$.

We now briefly describe elements of theory of sequences distributed modulo 1 that fits our needs and finds other applications in information theory (cf. [57]). We start with the following definition.

Definition 3.1 (B-u.d. mod 1)**.** A sequence $x_n \in \mathbb{R}$ is said to be *Bernoulli uniformly distributed modulo 1* (in short: B-u.d. mod 1) if for fixed $0 < p < 1$

$$\lim_{n\to\infty} \sum_{k=0}^{n} \binom{n}{k} p^k (1-p)^{n-k} \chi_I(\langle x_k \rangle) = \lambda(I) \tag{3.7}$$

holds for every interval $I \subset \mathbb{R}$, where $\chi_I(x_n)$ is the characteristic function of I (i.e., it equals to 1 if $x_n \in I$ and 0 otherwise) and $\lambda(I)$ is the Lebesgue measure of I.

Remark. If we replace in (3.7) the binomial distribution by the uniform distribution, then we define the *uniform distributed* sequences modulo 1, or in short u.d. mod 1. Not surprisingly, the property of $\langle x_k \rangle$ does not change when the uniform weight is replaced by the binomial weight since $\langle x_k \rangle$ stills "fills" up densely the interval $(0, 1)$ (cf. [40] for more details).

The following result summarizes the main property of B-u.d. modulo 1 sequences that we need in the analysis.

Theorem 3.2. Let $0 < p < 1$ be a fixed real number and suppose that the sequence x_n is B-uniformly distributed modulo 1. Then for every Riemann integrable function $f : [0, 1] \to \mathbb{R}$ we have

$$\lim_{n\to\infty} \sum_{k=0}^{n} \binom{n}{k} p^k (1-p)^{n-k} f(\langle x_k + y \rangle) = \int_0^1 f(t)\, dt, \tag{3.8}$$

where the convergence is uniform for all shifts $y \in \mathbb{R}$.

Proof. The proof is standard and can be found in [40, 98]. Here we only sketch the main idea. One first proves (3.8) for characteristic functions $\chi_I(x_k)$. This follows from Definition 3.1. Then, we approximate f by a step function (i.e., a combination of characteristic functions) and use the definition of the Riemann integral to bound the integral from below and above. One shows that when $n \to \infty$ these bounds coincide with the left-hand side of (3.8). □

To use Theorem 3.2 effectively, one needs a simple criterion to verify whether a sequence is B-u.d. mod 1. Such a criterion, fortunately, exists and it is basically due to Weyl. Before we formulate it, we note that we can relax the condition of Theorem 3.2 to functions f that are continuous with period 1.

Theorem 3.3 (Weyl's Criterion). A sequence x_n is B-u.d. mod 1 if and only if

$$\lim_{n\to\infty} \sum_{k=0}^{n} \binom{n}{k} p^k (1-p)^{n-k} e^{2\pi i m x_k} = 0 \tag{3.9}$$

holds for all $m \in \mathbb{Z} \setminus \{0\}$.

Proof. Again the proof is standard and the reader is referred to textbooks such as [40, 98] (cf. Chapter 8 of [154] for a brief discussion). Basically, it is based on the fact that by Weierstrass's *approximation theorem* every continuous function f of period 1 can be uniformly approximated by a trigonometric polynomial (i.e., a finite combination of functions of the type $e^{2\pi i m x}$). □

Now, we are in position to continue our derivation for the *irrational case*. Assume α is irrational. We first prove that in this case $\langle \alpha k \rangle$ is B-u.d. mod 1. Indeed, by the binomial theorem we have

$$\sum_{k=0}^{n} \binom{n}{k} p^k q^{n-k} e^{2\pi i m (k\alpha)} = \left(p e^{2\pi i m \alpha} + q\right)^n.$$

Since α is irrational we have $|pe^{2\pi i m\alpha} + q| < 1$ if $m \neq 0$. Hence it follows that

$$\lim_{n\to\infty} \sum_{k=0}^{n} \binom{n}{k} p^k q^{n-k} e^{2\pi i m (k\alpha)} = \lim_{n\to 0} \left(p e^{2\pi i m \alpha} + q\right)^n = 0 \tag{3.10}$$

so that Weyl's criterion can be applied. Hence, by Theorem 3.2, with $f(t) = t$ and $y = \beta n$, we immediately obtain

$$\lim_{n\to\infty} \sum_{k=0}^{n} \binom{n}{k} p^k q^{n-k} \langle \alpha k + \beta n \rangle = \int_0^1 t dt = \frac{1}{2}. \tag{3.11}$$

Now, we turn our attention to the case when α is rational. We assume $\alpha = M/N$ where M, N are non-zero integers such that

$\gcd(N,M) = 1$. (If $\alpha = 0$ — which is equivalent to $p = \frac{1}{2}$ — we trivially have $\overline{R}_n^S = 0$.) Let $p_{n,k} = \binom{n}{k} p^k q^{n-k}$. We proceed as follows

$$\begin{aligned}
\overline{R}_n^S &= \sum_{k=0}^{n} \binom{n}{k} p^k q^{n-k} \left\langle k\frac{N}{M} + \beta n \right\rangle = \sum_{k=0}^{n} p_{n,k} \left\langle k\frac{N}{M} + \beta n \right\rangle \\
&= \sum_{\ell=0}^{M-1} \sum_{k \equiv \ell \bmod M} p_{n,k} \left\langle \ell\frac{N}{M} + N + \beta n \right\rangle \\
&= \sum_{\ell=0}^{M-1} \sum_{k \equiv \ell \bmod M} p_{n,k} \left\langle \frac{\ell}{M} + \beta n \right\rangle \\
&= \sum_{\ell=0}^{M-1} \left\langle \frac{\ell}{M} + \beta n \right\rangle \sum_{k \equiv \ell \bmod M} \binom{n}{k} p^k (1-p)^{n-k}. \qquad (3.12)
\end{aligned}$$

To evaluate the last sum we need the following simple lemma. It asserts that if one picks every Mth term of the binomial distribution, then the total probability of this sample is “well” approximated by $1/M$.

Lemma 3.4. For fixed $\ell \le M$ and M, there exist $\rho < 1$ such that

$$\sum_{k \equiv \ell \bmod M} \binom{n}{k} p^k (1-p)^{n-k} = \frac{1}{M} + O(\rho^n). \qquad (3.13)$$

Proof. Let $\omega_k = e^{2\pi i k/M}$ for $k = 0, 1, \ldots, M-1$ be the Mth root of unity. It is well known that (cf. [154])

$$\frac{1}{M} \sum_{k=0}^{M-1} \omega_k^n = \begin{cases} 1 & \text{if } M|n \\ 0 & \text{otherwise.} \end{cases} \qquad (3.14)$$

where $M|n$ means that M divides n. In view of this, we can write

$$\begin{aligned}
\sum_{k \equiv \ell \bmod M} \binom{n}{k} p^k q^{n-k} &= \sum_{k=0}^{n} \binom{n}{k} p^k q^{n-k} \frac{1}{M} \sum_{r=0}^{M-1} \omega_r^{k-\ell} \\
&= \frac{1 + (p\omega_1 + q)^n \omega_1^{-\ell} + \cdots + (p\omega_{M-1} + q)^n \omega_{M-1}^{-\ell}}{M} \\
&= \frac{1}{M} + O(\rho^n), \qquad (3.15)
\end{aligned}$$

since $|(p\omega_r + q)| = p^2 + q^2 + 2pq\cos(2\pi r/M) < 1$ for $r \neq 0$. This proves the lemma. □

From now on, we deal only with the sum $S_n = \frac{1}{M}\sum_{\ell=0}^{M-1}\left\langle \frac{\ell}{M} + y\right\rangle$ of (3.12) ignoring the error term $O(\rho^n)$ and setting $y = \beta n$. It is clear that S_n is a periodic function in y with period $1/M$ and it is trivial to evaluate $S_n = 1/2 - 1/(2M)$ if $y = 0$. Hence, for $0 < y < 1/M$ we can use again the Fourier series (3.4) and (3.14) to obtain

$$\begin{aligned} S_n &= \frac{1}{M}\sum_{\ell=0}^{M-1}\left(\frac{1}{2} + \sum_{m\neq 0} c_m e^{2\pi i m(\ell/M+y)}\right) \\ &= \frac{1}{2} + \sum_{m\neq 0} c_m e^{2\pi i m y}\frac{1}{M}\sum_{\ell=0}^{M-1} e^{2\pi i m\frac{\ell}{M}} \\ &\overset{(3.14)}{=} \frac{1}{2} + \frac{1}{M}\sum_{m=kM\neq 0} c_{kM} e^{2\pi i k M y} \\ &\overset{(3.4)}{=} \frac{1}{2} - \frac{1}{M}\left(\frac{1}{2} - \langle yM\rangle\right). \end{aligned}$$

This leads to

$$S_n = \frac{1}{2} - \frac{1}{M}\left(\frac{1}{2} - \langle \beta n M\rangle\right) \tag{3.16}$$

for all β. Combining (3.11) and (3.16) completes then the proof of Theorem 3.1.

3.1.2 Huffman Codes

It is known that the following optimization problem over all prefix codes C

$$\overline{R}^H = \min_C \mathbf{E}[L(C,X) + \log P(X)]$$

is solved by the *Huffman code*. Recall that Huffman code is a recursive algorithm built over the associated Huffman tree, in which the two nodes with lowest probabilities are combined into a new node whose probability is the sum of the probabilities of its two children. Huffman coding is still one of the most familiar topics in information theory [1, 51, 52, 147], however, only recently a precise estimate of the average redundancy $\overline{R}^H$ of the Huffman code was derived in [153] that we review below.

We assume again that P is a memoryless source on $\mathcal{A} = \{0,1\}^n$ with parameter p, where we also assume that $p < \frac{1}{2}$. We denote by

$$P(x_1^n) = p^k q^{n-k}$$

the probability of generating a binary sequence consisting of k zeros and $n-k$ ones. The expected code length $\mathbf{E}[L_n]$ of the Huffman code is

$$E[L_n] = \sum_{k=0}^{n} \binom{n}{k} p^k q^{n-k} L(k),$$

where

$$L(k) = \frac{1}{\binom{n}{k}} \sum_{j \in \mathcal{S}_k} l_j$$

with $\mathcal{S}_k$ representing the set of all inputs having probability $p^k q^{n-k}$, and l_j being the length of the jth code in $\mathcal{S}_k$. By Gallager's sibling property [52], we know that code lengths in $\mathcal{S}_k$ are either equal to $l(k)$ or $l(k)+1$ for some integer $l(k)$. If n_k denotes the number of code words in $\mathcal{S}_k$ that are equal to $l(k)+1$, then

$$L(k) = l(k) + \frac{n_k}{\binom{n}{k}}.$$

Clearly, $l(k) = \lfloor -\log(p^k q^{n-k}) \rfloor$. Stubley [147] analyzed carefully n_k and showed

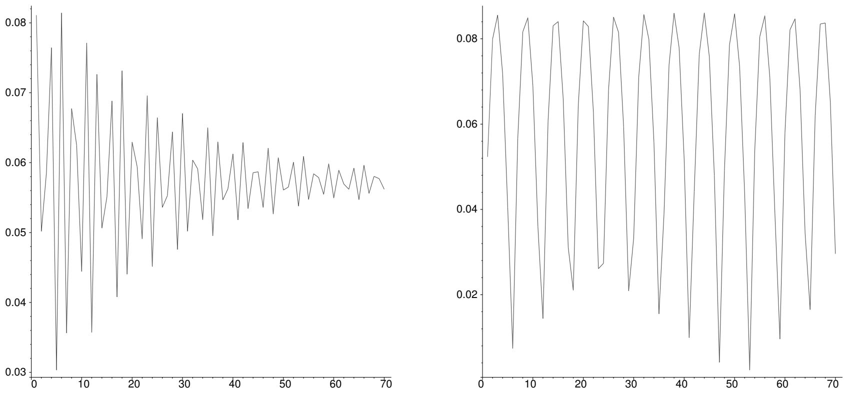
$$\begin{aligned} \overline{R}_n^H &= \sum_{k=0}^{n} \binom{n}{k} p^k q^{n-k} [\log(p^k q^{n-k}) + \lfloor -\log(p^k q^{n-k}) \rfloor] \\ &+ 2 \sum_{k=0}^{n-1} \binom{n}{k} p^k q^{n-k} (1 - 2^{(\log(p^k q^{n-k}) + \lfloor -\log(p^k q^{n-k}) \rfloor)}) + o(1). \end{aligned}$$

As before, using $\langle x \rangle = x - \lceil x \rceil$ we find

$$\log(p^k q^{n-k}) + \lfloor -\log(p^k q^{n-k}) \rfloor = -\langle \alpha k + \beta n \rangle$$

where for convenience we restate (cf. (3.3)

$$\alpha = \log_2 \left(\frac{1-p}{p} \right), \qquad \beta = \log_2 \left(\frac{1}{1-p} \right). \tag{3.17}$$



(a) (b)

Figure 3.1: The average redundancy of Huffman codes (3.18) versus block size n for: (a) irrational $\alpha = \log_2((1-p)/p)$ with $p = 1/\pi$; (b) rational $\alpha = \log_2((1-p)/p)$ with $p = 1/9$.

Thus we arrive at the following

$$\overline{R}_n^H = 2 - \sum_{k=0}^{n} \binom{n}{k} p^k q^{n-k} \langle \alpha k + \beta n \rangle - 2 \sum_{k=0}^{n} \binom{n}{k} p^k q^{n-k} 2^{-\langle \alpha k + \beta n \rangle} + o(1). \tag{3.18}$$

This is our starting formula for the average Huffman redundancy. Our main result is formulated next.

Theorem 3.5 (W. Szpankowski, 2000)**.** Consider the Huffman block code of length n over a binary memoryless source. Suppose that $0 < p < \frac{1}{2}$ and define α and β by (3.17). Then as $n \to \infty$ the average redundancy is given by

$$\overline{R}_n^H = \begin{cases} \frac{3}{2} - \frac{1}{\ln 2} + o(1) \approx 0.057304 & \alpha \notin \mathbb{Q} \\ \\ \frac{3}{2} - \frac{1}{M}\left(\langle \beta M n \rangle - \frac{1}{2} \right) - \frac{1}{M(1 - 2^{-1/M})} 2^{-\langle n \beta M \rangle / M} + o(1) & \alpha = \frac{N}{M} \end{cases}$$

where $\mathbb{Q}$ is the set of rational numbers, N, M are integers such that $\gcd(N, M) = 1$, and $\rho < 1$.

Before we present the proof, we plot in Figure 3.1 the average redundancy $\overline{R}_n^H$ presented in (3.18) as a function of n for two values of α, one *irrational* and one *rational*. In Figure 3.1(a), we consider $\alpha = \log(1-p)/p$ irrational, while in Figure 3.1(b), α is rational. Two modes of behavior are clearly visible. The function in Figure 3.1(a) converges to a constant (≈ 0.057) for large n as predicted by Theorem 3.5, while the curve in Figure 3.1(b) is quite erratic.

In the rational case, we observe that the redundancy swings from almost zero to about 0.086. To see it more precisely, and in fact to recover Gallager's upper bound [52], we set $x = \langle Mn\beta \rangle$. We first observe that $M = 1$ maximizes $\overline{R}_n^H$, and then

$$\overline{R}_n^H(x) \sim 2 - x - 2^{-x+1}. \tag{3.19}$$

This leads to

$$\max_{0 \le x < 1} 2 - x - 2^{-x+1} = 1 - \frac{1 + \ln\ln 2}{\ln 2} = \log(2(\log e)/e) = 0.08607\ldots, \tag{3.20}$$

which is the Gallager upper bound (since the most likely probability $p_1 = O(1/\sqrt{n})$ in this case). We formulate it as a corollary.

Corollary 3.6. Let $\overline{R}_n^H$ denote the average redundancy of a Huffman block code of length n over a binary memoryless source. Then

$$\limsup_{n\to\infty} \overline{R}_n^H \le 1 - \frac{1 + \ln\ln 2}{\ln 2} = \log(2(\log e)/e) \sim 0.08607\ldots, \tag{3.21}$$

Proof of Theorem 3.5. To establish Theorem 3.5 we must only deal with the asymptotics of the following sum

$$T_n = \sum_{k=0}^{n} \binom{n}{k} p^k q^{n-k} 2^{-\langle \alpha k + \beta n \rangle}. \tag{3.22}$$

We need to consider the rational and irrational case. For the irrational case, we simply use Theorem 3.2 with $f(t) = 2^{-t}$ and $y = \beta n$. For the rational case, we can use the Fourier series as before, but this time we need the following for some $a > 0$

$$2^{-\langle x \rangle / a} = C_0(a) + \sum_{m \ne 0} C_m(a) e^{2\pi i m x}, \tag{3.23}$$

where

$$C_0(a) = \frac{a}{\ln 2}\left(1 - 2^{-1/a}\right), \qquad (3.24)$$

$$C_m(a) = \frac{a}{2\pi ima + \ln 2}\left(1 - 2^{-1/a}\right), \qquad m \neq 0. \qquad (3.25)$$

In fact, for the rational case it is easier to formalize our approach and codify it in the form of the next lemma from which Theorem 3.5 follows. The proof follows the footsteps of our derivations in (3.12).

Lemma 3.7. Let $0 < p < 1$ be a fixed real number and suppose that $\alpha = \frac{N}{M}$ is a rational number with $\gcd(N, M) = 1$. Then, for every bounded function $f : [0, 1] \to \mathbb{R}$ we have

$$\sum_{k=0}^{n} \binom{n}{k} p^k (1-p)^{n-k} f(\langle k\alpha + y\rangle) = \frac{1}{M}\sum_{l=0}^{M-1} f\left(\frac{l}{M} + \frac{\langle My\rangle}{M}\right) + O(\rho^n)$$

uniformly for all $y \in \mathbb{R}$ and some $\rho < 1$.

3.1.3 Golomb Code

In this section we give a short account on Golomb's code that can be viewed as a special case of Huffman's code adapted to infinite alphabets. Our analysis in this section will differ from other sections since we perform asymptotics not with regard to the block length but rather at the limit of a code parameter.

More precisely, let

$$P(i) = (1-\theta)\theta^i, \qquad i \in \mathbb{Z}^+, \qquad (3.26)$$

be the probability assignment on the set of nonnegative integers where $0 < \theta < 1$. Golomb [54] proposed the following optimal binary code (we follow here the description from [53]): Let ℓ be an integer such that

$$\theta^\ell = \frac{1}{2}, \qquad (3.27)$$

which means that we restrict on θ that are roots of 1/2. In Golomb's code an integer i is represented as $i = \ell j + r$, where $j = \lfloor i/\ell \rfloor$ and $0 \leq r < \ell$. We encode j by a unary code (i.e., j zeros followed by a

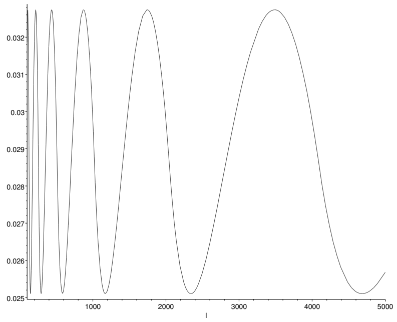


Figure 3.2: The average redundancy of Golomb codes versus ℓ.

one) while r is encoded by a Shannon code (for a uniform distribution on ℓ symbols).

In [53, 54] it is shown that the average Golomb's code length $\mathbf{E}[L]$ is

$$\mathbf{E}[L] = \lceil \log_2 \ell \rceil + \frac{\theta^{2^{\lfloor \log_2 \ell \rfloor + 1}}}{\theta^{\ell} - 1}. \tag{3.28}$$

Roughly speaking, the first term above corresponds to the Shannon code while the second term represents the unary coding. The average redundancy $\overline{R}_{\ell}^{G}$ of the Golomb code becomes

$$\overline{R}_{\ell}^{G} = \mathbf{E}[L] - H(\theta) \tag{3.29}$$

where the entropy $H(\theta)$ of the geometric distribution (3.26) can be computed as

$$H(\theta) = -\log_2(1-\theta) - \frac{\theta}{1-\theta}\log_2 \theta. \tag{3.30}$$

We will estimate $\overline{R}_{\ell}^{G}$ as $l \to \infty$ or equivalently as $\theta \to 1$ (cf. [53, 113]).

Our main result is presented next. Observe that in this case, there is *only* the oscillatory mode of $\overline{R}_{\ell}^{G}$ behavior as illustrated in Figure 3.2.

Theorem 3.8. Consider the Golomb code over the non-negative integers generated by a geometric source *Geometric*(θ) such that there exists an integer ℓ with $\theta^{\ell} = \frac{1}{2}$. Then as $\ell \to \infty$, so that $\theta \to 1$,

$$\overline{R}_{\ell}^{G} = 1 - \langle \log_2 \ell \rangle + 4 \cdot 2^{-2^{1-\langle \log_2 \ell \rangle}} - \log_2(\log_2 e) - \log_2 e - \frac{1}{2\ell} + O(\ell^{-2}). \tag{3.31}$$

Furthermore, the average redundancy $\overline{R}_\ell^G$ oscillates around $2 - \log_2(\log_2 e) - \log_2 e = 0.028538562\ldots$ with

$$\liminf_{\ell\to\infty} \overline{R}_\ell^G = 0.0251005712\ldots, \tag{3.32}$$

$$\limsup_{\ell\to\infty} \overline{R}_\ell^G = 0.0327344112\ldots. \tag{3.33}$$

Proof. We assume that $\theta^\ell = 1/2$ as in (3.28), and estimate the entropy $H(\theta)$ (cf. (3.30)) as $\ell \to \infty$ (i.e, $\theta = 2^{-1/\ell} \to 1$). Using the following Taylor's expansion

$$\log_2(1-2^{-x}) = \log_2(\ln(2) + \log_2(x) - \frac{1}{2}x + \frac{\ln(2)}{24}x^2 + O(x^3), \quad x \to 0, \tag{3.34}$$

we arrive at

$$H(\theta) = \log_2 \ell + \log_2(\log_2 e) + \frac{1}{2\ell} + O(\ell^{-2}). \tag{3.35}$$

The average redundancy $\overline{R}_\ell^G = \mathbf{E}[L] - H(\theta)$, where $\mathbf{E}[L]$ is given by (3.28), follows after some simple algebra

$$\overline{R}_\ell^G = 1 - \langle \log_2 \ell \rangle + 4 \cdot 2^{-2^{1-\langle \log_2 \ell \rangle}} - \log_2(\log_2 e) - \log_2 e - \frac{1}{2\ell} + O(\ell^{-2}) \tag{3.36}$$

as $\ell \to \infty$ or $\theta \to 1$. This proves (3.31) of Theorem 3.8. We should also point out that using the above approach we can get a full asymptotic expansion of $\overline{R}_\ell^G$ as $\ell \to \infty$.

Since $\langle \log_2 n \rangle$ is dense in $(0, 1)$ it follows by (3.36) that the average redundancy $\overline{R}_\ell^G$ asymptotically oscillates within a certain interval without reaching a limit, as observed in Figure 3.2.

To compute the magnitude of the oscillation, let us define $C = \log_2(\log_2 e) + \log_2 e = 1.971461414\ldots$. We set

$$g(x) = 1 - x + 4 \cdot 2^{-2^{1-x}} - C \tag{3.37}$$

for $0 \le x \le 1$. (Observe that $g(x)$ is asymptotically equal to R_ℓ^G when $x = \langle \log_2 n \rangle$.) One derives that $g(x)$ achieves it maximum value $g(x_1) := \max\{g(x)\} = .327344112\ldots$ at

$$x_1 = \log_2\left(\frac{-2\ln(2)}{W(-0.25\log_2 e)}\right) \tag{3.38}$$

where $W(x)$ is the Lambert-W function defined as $W(x)e^{W(x)} = x$ (cf. [21]). Similarly, the function $g(x)$ achieves its minimum value $g(x_2) := \min\{g(x)\} = .251005712\ldots$ at

$$x_2 = \log_2\left(\frac{-2\ln(2)}{W(-1, -0.25\log_2 e)}\right) \tag{3.39}$$

where $W(-1, x)$ is a branch of the Lambert-W function (cf. [21]). It is also easy to see that the average redundancy oscillates around $g(0) = g(1) = 2 - C = .0285385862\ldots$. This proves Theorem 3.8. □

3.2 Shannon Code Redundancy for Markov Sources

In this section we study the average redundancy of the Shannon code for Markov sources, that is the probability distribution on the alphabet $\mathcal{A} = \{0,1\}^n$ (or more generally on $\mathcal{A} = \{0,1,\ldots,m-1\}^n$) is given by a Markov process. This section is mostly based on [114].

Consider a source sequence $X_1, X_2, \ldots$, where for $t = 1, 2, \ldots$ the sequence $X_t \in \mathcal{X} = \{0, 1, \ldots m-1\}$ is governed by a first–order Markov chain with a given matrix $\mathbf{P}$ of state–transition probabilities $\{p(j|k)\}_{j,k=0}^{m-1}$. The initial state probabilities will be denoted by $p_k = P(X_t = k)$ for $k = 0, 1, \ldots, m-1$. We write π_k, $k = 0, 1\ldots, m-1$ for the stationary state probabilities. Thus, the probability of a given source string $x^n = (x_1, \ldots, x_n) \in \mathcal{A} = \mathcal{X}^n$, under the given Markov source, is

$$P(x^n) = p_{x_1}\prod_{t=2}^{n} p(x_t|x_{t-1}). \tag{3.40}$$

The average redundancy of the Shannon code is then

$$\overline{R}_n = \mathbf{E}[\lceil -\log P(X^n)\rceil + \log P(X^n)] = \mathbf{E}[\langle \log P(X^n)\rangle]. \tag{3.41}$$

Our main result in this section is the following theorem which is a slight extension of a result of Merhav and W. Szpankowski [114].

Theorem 3.9. Consider the Shannon code of block length n for a Markov source with a given vector $\mathbf{p} = (p_0, \ldots, p_{m-1})$ of initial state probabilities and a *positive* state transition matrix $\mathbf{P}$. Define

$$\alpha_{jk} = \log\left[\frac{p(j|0)p(j|j)}{p(k|0)p(j|k)}\right], \quad j, k \in \{0, 1, \ldots, m-1\}. \tag{3.42}$$

Then, the redundancy $\overline{R}_n$ is characterized as follows:
(a) If *not all* $\{\alpha_{jk}\}$ are rational, then

$$\overline{R}_n = \frac{1}{2} + o(1). \tag{3.43}$$

(b) If all $\{\alpha_{jk}\}$ are rational, then for every $j, k \in \{0, \ldots, m-1\}$, let

$$\zeta_{jk}(n) = M[(n-1)\log p(0|0) - \log p(j|0) + \log p(k|0) + \log p_j], \tag{3.44}$$

and

$$\Omega_n = \frac{1}{2}\left(1 - \frac{1}{M}\right) + \frac{1}{M}\sum_{j=0}^{m-1}\sum_{k=0}^{m-1} p_j \pi_k \langle \zeta_{jk}(n) \rangle, \tag{3.45}$$

where M is the smallest common integer multiple of the denominators of $\{\alpha_{jk}\}$, when each one of these numbers is represented as a ratio between two relatively prime integers. Then

$$\overline{R}_n = \Omega_n + O(\rho^n) \tag{3.46}$$

for some $\rho < 1$.

Before we prove Theorem 3.9 in the next subsection, we offer some comments. Theorem 3.9 tells us that, as in the memoryless case, $\overline{R}_n$ has two modes of behavior. In the convergent mode, which happens when at least one α_{jk} is irrational, $\overline{R}_n \to 1/2$. In the oscillatory mode, which happens when all $\{\alpha_{jk}\}$ are rational, $\overline{R}_n$ oscillates and it asymptotically coincides with Ω_n.

We also note that if $\log p(0|0)$ is irrational, then by Weyl's equidistribution Theorem 3.3, the sequences $\{\zeta_{jk}(n)\}_{n \geq 1}$ are uniformly distributed modulo 1, i.e., they fill the unit interval mod 1. If, on the other hand, $\log p(0|0)$ is rational, then $\langle \zeta_{jk}(n) \rangle$ are periodic sequences.

The expression of the oscillatory case, Ω_n, is not quite intuitive at first glance, therefore, in this paragraph, we make an attempt to give some quick insight, which captures the essence of the main points. The arguments here are informal and non-rigorous (see Section 3.2.1 for a rigorous proof). The Fourier series expansion of the periodic function $\langle \cdot \rangle$ is given by

$$\langle u \rangle = \frac{1}{2} + \sum_{h \neq 0} c_h e^{2\pi i h u} \tag{3.47}$$

and the important fact about the coefficients $c_h = i/(2\pi h)$ is that they are inversely proportional to h, so that for every two integers k and h, $c_{h\cdot k} = c_h/k$. Now, when computing $\overline{R}_n = \mathbf{E}[\langle \log P(X^n)\rangle]$, let us take the liberty of exchanging the order between the expectation and the summation, i.e.,

$$\overline{R}_n = \frac{1}{2} + \sum_{h\neq 0} c_h \mathbf{E}[e^{2\pi i h \log P(X^n)}]. \tag{3.48}$$

It turns out that under the conditions of the oscillatory mode, $\mathbf{E}[e^{2\pi i h \log P(X^n)}]$ tends to zero as $n \to \infty$ for all h, except for multiples of M, namely, $h = \ell M$, $l = \pm 1, \pm 2, \ldots$. Thus, for large n, we have

$$\begin{aligned}\overline{R}_n &\approx \frac{1}{2} + \sum_{\ell\neq 0} c_{\ell M} \mathbf{E}[e^{2\pi i \ell M \log P(X^n)}] \\ &= \frac{1}{2} + \frac{1}{M}\sum_{\ell\neq 0} c_{\ell} \mathbf{E}[e^{2\pi i \ell M \log P(X^n)}] \\ &= \frac{1}{2} + \frac{1}{M}\left[\mathbf{E}[\langle M\log P(X^n)\rangle] - \frac{1}{2}\right] \\ &= \frac{1}{2}\left(1 - \frac{1}{M}\right) + \frac{1}{M}\mathbf{E}[\langle M\log P(X^n)\rangle]. \end{aligned} \tag{3.49}$$

Now, consider the set of all $\{x^n\}$ that begin from state $x_1 = j$ and end at state $x_n = k$. Their total probability is about $p_j\pi_k$ for large n since X_n is almost independent of X_1. It turns out that all these sequences have exactly the same value of $\langle M\log P(x^n)\rangle$, which is exactly $\langle \zeta_{jk}(n)\rangle$ (or, in other words, $\langle M\log P(x^n)\rangle = \langle \zeta_{x_1 x_n}(n)\rangle$ independently of $x_2, \ldots, x_{n-1}$) and this explains the expression of Ω_n. The reason for this property of $\langle M\log P(x^n)\rangle$ is the rationality conditions $\langle M\cdot\alpha_{uv}\rangle = 0$, $u, v \in \{0, 1, \ldots, m-1\}$, which imply that $\langle M\log p(x_t|x_{t-1})\rangle = \langle M\log[p(x_t|1)p(0|0)/p(x_{t-1}|0)]\rangle$, and so,

$$\langle M\log P(x^n)\rangle = \langle M\log p_j\rangle + \sum_{t=2}^{n}\langle M\log p(x_t|x_{t-1})\rangle \mod 1$$

$$= \langle M\log p_j\rangle + \sum_{t=2}^{n}\langle M\log[p(x_t|1)p(0|0)/p(x_{t-1}|0)]\rangle \mod 1$$

which, thanks to the telescopic summation, is easily seen to coincide with the fractional part of $\zeta_{jk}(n)$, and of course, $\langle\zeta_{jk}(n)\rangle$ depends on $\zeta_{jk}(n)$ only via its fractional part.

Consider next the following example for using Theorem 3.9.

Example 3.1. Consider a Markov source for which the rows of $\mathbf{P}$ are all permutations of the first row, which is $\mathbf{p} = (p_0, \ldots, p_{m-1})$. Now, assuming that $\alpha_j := \log(p_1/p_j)$ are all rational, let M be the least common multiple of their denominators (i.e., the common denominator) when each one of them is expressed as a ratio between two relatively prime integers. Then,

$$\begin{aligned}
\langle\zeta_{jk}(n)\rangle &= \langle M(n-1)\log p(0|0) - M\log p(j|0) + M\log p(k|0) \\
&\quad +M\log p_j\rangle \\
&= \langle M(n-1)\log p_0 - M\log p_j + M\log p_k + M\log p_j\rangle \\
&= \langle M(n-1)\log p_0 + M\log p_k\rangle \\
&= \langle Mn\log p_0 - M\log p_0 + M\log p_k\rangle \\
&= \langle Mn\log p_0\rangle,
\end{aligned}$$

where in the last step, we have used the fact that $(M\log p_0 - M\log p_k)$ is integer and that $\langle\cdot\rangle$ is a periodic function with period 1. We have

$$\begin{aligned}
R_n &= \frac{1}{2}\left(1-\frac{1}{M}\right) + \frac{1}{M}\sum_{j=0}^{m-1}\sum_{k=0}^{m-1} p_j\pi_k\langle\zeta_{jk}(n)\rangle + o(1) \\
&= \frac{1}{2}\left(1-\frac{1}{M}\right) + \frac{1}{M}\sum_{j=0}^{m-1}\sum_{k=0}^{m-1} p_j\pi_k\langle nM\log p_1\rangle + o(1) \\
&= \frac{1}{2}\left(1-\frac{1}{M}\right) + \frac{1}{M}\langle nM\log p_0\rangle + o(1). \qquad (3.50)
\end{aligned}$$

If not all α_j are rational, then $\overline{R}_n \to 1/2$, as predicted by Theorem 3.9. To see why the conditions of Theorem 3.9 lead to the rationality condition herein, let us denote

$$\begin{aligned}
u_{jk} &= \langle h\log[p(j|0)/p(k|0)]\rangle\,, \\
v_{jk} &= \langle h\log[p(j|j)/p(j|k)]\rangle\,.
\end{aligned}$$

Then, the conditions of Theorem 3.9 mean that $u_{jk}+v_{jk} = 0$ and for all pairs j and k. Therefore, the number of constraints here is of the order of m^2, whereas the number of degrees of freedom that generate these variables, in this example, is $m-1$, i,e., the variables $\langle h\log(p_1/p_j)\rangle$, $j=1,2,\ldots,m-1$. Thus, we can think of this as an overdetermined set of homogeneous linear equations whose only solution is zero, meaning that all $\langle h\log(p_1/p_j)\rangle$, $j=1,2,\ldots,m-1$, vanish. Note that the memoryless source is a special case of this example, where the rows of $\mathbf{P}$ are all identical to the first row, $(p_0,\ldots,p_{m-1})$. Indeed, (3.50) coincides with the expression of the memoryless case as discussed in the first subsection of this chapter.

3.2.1 Proof of Theorem 3.9

The main idea behind the analysis of $\overline{R}_n = \mathbf{E}[\langle\log P(X^n)\rangle]$ is to approximate the periodic function $\langle\cdot\rangle$ by a sequence of trigonometric polynomials, and then to commute the expectation with the summation and analyze the various terms of the series. A sufficient condition for making this commutation rigorous is that the convergence would be uniform, but unfortunately, it cannot be uniform since the function $\langle\cdot\rangle$ is discontinuous. An alternative route that we take is to sandwich $\langle\cdot\rangle$ between two continuous periodic functions, both with period 1, and both indexed by some parameter H, which when tending to infinity, the bounds become tighter and tighter. Fejér's theorem (see, e.g., [148]), which is the trigonometric version of the Weierstrass theorem, provides a concrete sequence of trigonometric polynomials, which converges uniformly to any given periodic continuous function. The following lemma is a modern variant due to Vaaler [159] and will be used in the irrational case.

Lemma 3.10 (Vaaler, 1985). For $H\in\mathbb{N}$, $h\in\mathbb{Z}$, $1\le|h|\le H$, let

$$0<\theta_H(h) := \pi\frac{|h|}{H+1}\left(1-\frac{|h|}{H+1}\right)\cot\left(\pi\frac{|h|}{H+1}\right)+\frac{|h|}{H+1}<1.$$

Then, the trigonometric polynomial

$$\Psi_H^*(x) = \frac{1}{2}-\frac{1}{2i\pi}\sum_{1\le|h|\le H}\frac{\theta_H(h)}{h}e^{2\pi ihx}$$

satisfies

$$|\langle x\rangle - \Psi_H^*(x)| \le \frac{1}{2H+2}\sum_{|h|\le H}\left(1-\frac{|h|}{H+1}\right)e^{2\pi i h x} \qquad (x\in\mathbb{R})$$

for all H.

Define the functions ϱ_H^- and ϱ_H^+ as

$$\varrho_H^-(u) = \Psi_H^*(x) - \Delta_H(u) \tag{3.51}$$

and

$$\varrho_H^+(u) = \Psi_H^*(x) + \Delta_H(u). \tag{3.52}$$

where

$$\Delta_H(u) = \frac{1}{2H+2}\sum_{|h|\le H}\left(1-\frac{|h|}{H+1}\right)e^{2\pi i h x}. \tag{3.53}$$

Obviously, $\varrho_H^-(u)$, and $\varrho_H^+(u)$ are continuous, periodic functions, with period 1, and $\varrho_H^-(u)\le\langle u\rangle\le\varrho_H^+(u)$ for every u.

We now proceed to establish upper and lower bounds, however, we only present details for the lower bound. We have

$$\begin{aligned}\overline{R}_n &= \mathbf{E}\left[\langle\log P(X^n)\rangle\right]\\ &\ge \mathbf{E}\left[\varrho_H^-(\log P(X^n))\right]\\ &= \frac{1}{2}+\sum_{1\le|h|\le H}\frac{\theta_H(h)}{h}\mathbf{E}\left[e^{2\pi i h\log P(X^n)}\right]\\ &- \frac{1}{2H+2}\sum_{|h|\le H}\left(1-\frac{|h|}{H+1}\right)\mathbf{E}\left[e^{2\pi i h\log P(X^n)}\right].\end{aligned} \tag{3.54}$$

We next show that in the irrational case we have

$$\lim_{n\to\infty}\mathbf{E}\left[e^{2\pi i h\log P(X^n)}\right]=0 \tag{3.55}$$

for all integers $h\ne0$. If (3.55) holds then it follows that

$$\liminf_{n\to\infty}\overline{R}_n \ge \frac{1}{2}-\frac{1}{2H+2}$$

for all integers $H\ge1$ and thus $\liminf_{n\to\infty}\overline{R}_n\ge\frac{1}{2}$. Similarly we get an upper bound and consequently we have $\overline{R}_n=\frac{1}{2}+o(1)$ (as $n\to\infty$) in the irrational case.

In order to show (3.55), we define the $m \times m$ complex matrix A_h whose entries are

$$a_{jk}(h) = p(k|j) \exp\left[2\pi i h \log p(k|j)\right], \qquad j,k = 0,\dots,m-1. \tag{3.56}$$

We also define the m–dimensional column vectors

$$\boldsymbol{c}_h = (p_0 \exp[2\pi i h \log p_0)], \dots, p_{m-1} \exp[2\pi i h \log p_{m-1}])^T, \tag{3.57}$$

and $\mathbf{1} = (1,1,\dots,1)^T$, where the superscript T denotes vector/matrix transposition. Then, according to (3.40) it follows that

$$\mathbf{E}\left[e^{2\pi i h \log P(X^n)}\right] = \boldsymbol{c}_h^T A_h^{n-1} \mathbf{1}. \tag{3.58}$$

Let $\mathbf{l}_{j,h}$ and $\boldsymbol{r}_{j,h}$ be, respectively, the left eigenvector and the right eigenvector pertaining to the eigenvalue $\lambda_{j,h}$ ($j = 0,1,\dots,m-1$) of the matrix A_h. Here, we index the eigenvalues of A_h according to a non–increasing order of their modulus, that is,

$$|\lambda_{1,h}| \geq |\lambda_{2,h}| \geq \cdots \geq |\lambda_{m,h}|. \tag{3.59}$$

Since $\mathbf{P}$ is a stochastic matrix (so, its maximum modulus eigenvalue is 1) and its elements are the absolute values of the corresponding elements of A_h, it follows from [116, Theorem 8.4.5] that $|\lambda_{1,h}| \leq 1$ (and hence $|\lambda_{j,h}| \leq 1$ for all $j = 0,1,\dots,m-1$). Also, the systems of left– and right eigenvectors form a bi-orthogonal system, i.e., $\mathbf{l}_{j,h}^T \boldsymbol{r}_{k,h} = 0$, $j,k = 0,1,\dots,m-1$, $j \neq k$. We scale these vectors such that $\mathbf{l}_{j,h}^T \boldsymbol{r}_{j,h} = 1$ for all $j = 0,1,\dots,m-1$. Then by the spectral representation of matrices [116], we have

$$A_h^{n-1}\mathbf{1} = \sum_{j=0}^{m-1} \lambda_{j,h}^{n-1} \cdot \mathbf{l}_{j,h}^T \mathbf{1} \cdot \boldsymbol{r}_{j,m}, \tag{3.60}$$

and so,

$$\boldsymbol{c}_h^T A_h^{n-1}\mathbf{1} = \sum_{j=0}^{m-1} \lambda_{j,h}^{n-1} \cdot \mathbf{l}_{j,h}^T \mathbf{1} \cdot \boldsymbol{c}_h^T \boldsymbol{r}_{j,h}. \tag{3.61}$$

Now the following lemma, that appears in [116] (with minor modifications in its phrasing), and that has already been used in earlier related studies [75], [72], will be useful to show that $|\lambda_{1,h}| < 1$ in the irrational case.

For a quadratic matrix A the spectral radius is denoted by $\rho(A)$.

Lemma 3.11. [116, Theorem 8.4.5, p. 509] Let $F = \{f_{kj}\}$ and $G = \{g_{kj}\}$ be two $m \times m$ matrices. Assume that F is a real, non–negative and irreducible matrix, G is a complex matrix, and $f_{kj} \geq |g_{kj}|$ for all $k, j \in \{1, 2, \ldots, m\}$. Then, $\rho(G) \geq \rho(F)$ with equality if and only if there exist real numbers s, and $w_1, \ldots, w_m$ such that $G = e^{2\pi is} DFD^{-1}$, where $D = \mathrm{diag}\{e^{2\pi iw_1}, \ldots, e^{2\pi iw_r}\}$.

The proof of the necessity of the condition $G = e^{2\pi is} DFD^{-1}$ appears in [116] (see also [75], [72]). The sufficiency is obvious since the matrix DFD^{-1} is similar to F and hence has the same set of eigenvalues.

We wish to apply Lemma 3.11 in order to distinguish between the two aforementioned cases concerning the spectral radius of A_h. Consider the state transition probability matrix $\mathbf{P}$ in the role of F of Lemma 3.11 (i.e., $f_{kj} = p(j|k)$) and the matrix A_h in the role of G. Since $\mathbf{P}$ is assumed positive in this part, then it is obviously non–negative and irreducible. Since it is a stochastic matrix, its spectral radius is, of course, $\rho(P) = 1$. Also, by definition of A_h, as the matrix $\{p(j|k) \cdot \exp[2\pi ih \log p(j|k)]\}$, it is obvious that the elements of $\mathbf{P}$ are the absolute values of the corresponding elements of A_h, and so, all the conditions of Lemma 3.11 clearly apply. The lemma then tells us that $\rho(A_h) = \rho(P) = 1$ if and only if there exist real numbers s and $w_0, \ldots w_{m-1}$ such that for some integer h:

$$h \log p(j|k) = (s + w_k - w_j) \bmod 1, \quad j, k = 0, \ldots, m-1, \tag{3.62}$$

where $x = y \bmod 1$ means that the fractional parts of x and y are equal, that is, $\langle x \rangle = \langle y \rangle$.

To find a vector $\boldsymbol{w} = (w_0, \ldots, w_{m-1})$ and a number s with this property (if exists), we take the following approach: Consider first the choice $k = j$ in (3.62). This immediately tells us that s, if exists, must be equal to $h \log p(j|j) \pmod 1$ for every $j = 0, \ldots, m-1$. In other words, one set of conditions is that $h \log p(j|j)$ are all equal (mod 1), or equivalently,

$$\left\langle h \log \frac{p(j|j)}{p(0|0)} \right\rangle = 0, \qquad j = 0, 1, \ldots, m-1, \tag{3.63}$$

and then s is taken to be the common value of all $\langle h \log p(j|j)\rangle$. Thus, (3.62) becomes

$$-h \log \frac{p(j|j)}{p(j|k)} = (w_k - w_j) \bmod 1, \quad j,k = 0,\ldots,m-1, \tag{3.64}$$

and it remains to find the vector $\boldsymbol{w}$ if possible. To this end, observe that if $\boldsymbol{w}$ satisfies (3.64), then for every constant c, $\boldsymbol{w}+c$ also satisfies (3.64). Taking $c = -w_0$, the first component of $\boldsymbol{w}$, is arbitrary. It is apparent that if (3.64) can hold for some $\boldsymbol{w}$, then there is such a vector whose first component vanishes, and then by setting $k = 0$ in (3.64), we learn that

$$w_j = \left\langle -h \log \frac{p(j|0)}{p(j|j)} \right\rangle, \qquad j = 0,\ldots,m-1, \tag{3.65}$$

is a legitimate choice. Thus, (3.64) becomes

$$\left\langle -h \log \left[\frac{p(j|0)p(j|j)}{p(k|0)p(j|k)} \right] \right\rangle = 0 \quad j,k = 0,\ldots,m-1. \tag{3.66}$$

Note that by setting $k = 0$ in (3.66), we get (3.63) as a special case, which means that (3.66), applied to all $j,k \in \{0,1,\ldots,m-1\}$, are all the necessary and sufficient conditions needed for $\rho(A_h) = 1$. Now, a necessary and sufficient condition for (3.66) to hold for *some* integer h, is that the numbers

$$\alpha_{jk} = \log \left[\frac{p(j|0)p(j|j)}{p(k|0)p(j|k)} \right] \tag{3.67}$$

would be all rational.

Summing up, it follows that $\rho(A_h) < 1$ if at least one α_{jk} is irrational. Hence, as explained above, it follows in this case that $\overline{R}_n \sim \frac{1}{2} + o(1)$. This establishes the first part of Theorem 3.9.

If all α_{jk} are rational, then we have to argue in a different way. We have already did some heuristic calculations indicating which kind of result we can expect. Actually, we can use a method similarly to the calculations of (3.12) and Lemma 3.4, properly adapted to Markov sources, that covers the rational case.

In order to simplify the presentation, we consider just the binary case $m = 2$. The general case is just notationally more involved. First, we split up the sum according to the initial and final states

$$\begin{aligned}\mathbf{E}\left[\langle \log P(X^n)\rangle\right] &= \sum_{x_1,\ldots,x_n} P(x^n)\langle \log P(x^n)\rangle \\ &= \sum_{j=0}^{1}\sum_{k=0}^{1}\sum_{x_1=j,x_n=k} P(x^n)\langle \log P(x^n)\rangle\end{aligned}$$

Let us consider (first) the case $j = k = 0$ and denote by k_{ij} is the number of pairs (ij) in x^n. Clearly, $k_{00} + k_{01} + k_{10} + k_{11} = n - 1$. But also $k_{01} = k_{10}$ since the number of pairs ending at 1 must be equal to the number of pairs starting with 1 (see [71, 61]). We then can write $P(x^n)$ as

$$\begin{aligned}P(x^n) &= p_0 P(0|0)^{k_{00}} P(0|1)^{k_{01}} P(1|0)^{k_{10}} P(1|1)^{k_{11}}, \\ &= p_0[P(0|0)]^{n-1}\left[\frac{P(0|1)P(1|0)}{P(0|0)P(0|0)}\right]^{k_{01}}\left[\frac{P(1|1)}{P(0|0)}\right]^{k_{11}}.\end{aligned}$$

Hence, using (3.42), we can represent $\log P(x^n)$ as

$$\log P(x^n) = (n-1)\log P(0|0) + \log p_0 - k_{01}\alpha_{01} + k_{11}\alpha_{10}.$$

By assumption, we can write $\alpha_{01} = L_0/M$ and $\alpha_{10} = L_1/M$ with $\gcd(L_0, L_1, M) = 1$. Thus, $\langle \log P(x^n)\rangle$ is constant if $-k_{01}L_0 + k_{01}L_1$ is in a fixed residue class mod M. With the help of the following lemma, which generalizes Lemma 3.4 to Markov sources, we will be then able to evaluate the sum $\sum_{x_1=x_n=0} P(x^n)\langle \log P(x^n)\rangle$ asymptotically.

Lemma 3.12. Suppose that $M \geq 1$ and that L_0 and L_1 satisfy $\gcd(L_0, L_1, M) = 1$. Then, for every $0 \leq \ell < M$ and $0 \leq j, k \leq 1$ there exists $\rho < 1$ such that

$$\sum_{x_1=j,\, x_n=k,\, -k_{01}L_0+k_{01}L_1\equiv \ell \bmod M} P(x^n) = \frac{p_j\pi_k}{M} + O(\rho^n). \tag{3.68}$$

Proof. We start with the case $j = k = 0$. Let $G_{00}(z)$ and $G_{01}(z)$ be the generating function

$$G_{00}(z) = \sum_{n\geq 1}\sum_{x_1=x_n=0} P(x^n)z^n, \quad G_{01}(z) = \sum_{n\geq 1}\sum_{x_1=0,\, x_n=1} P(x^n)z^n.$$

Then these generating function satisfy the following system of linear equations (compare also with [69, 71]):

$$\begin{aligned} G_{00}(z) &= G_{00}(z)p(0|0)z + G_{01}(z)p(1|0)z + p_0 z, \\ G_{01}(z) &= G_{00}(z)p(0|1)z + G_{01}(z)p(1|1)z. \end{aligned}$$

In particular it follows that

$$\begin{aligned} G_{00}(z) &= \frac{\begin{vmatrix} p_0 z & -p(1|0)z \\ 0 & 1-p(1|1)z \end{vmatrix}}{\begin{vmatrix} 1-p(0|0)z & -p(1|0)z \\ -p(0|1)z & 1-p(1|1)z \end{vmatrix}} \\ &= \frac{p_0 z(1-p(1|1)z)}{1-(p(0|0)+p(1|1))z + (p(0|0)p(1|1) - p(0|1)p(1|0))z^2}. \end{aligned}$$

Note that this identity is also true if the $p(j|k)$ are treated as formal variables. However, if we assume that $p(0|0)+p(0|1) = p(1|0)+p(1|1) = 1$ then we have

$$G_{00}(z) = \frac{p_0 z(1-p(1|1)z)}{(1-z)(1-(p(0|0)+p(1|1)-1)z)}$$

which implies that

$$[z^n]G_{00}(z) = \frac{p_0(1-p(1|1))}{2-p(0|0)-p(1|1)} + O(|1-p(0|0)-p(1|1)|^n) = p_0\pi_0 + O(\rho^n)$$

for $\rho = |1-p(0|0)-p(1|1)| < 1$.

Furthermore, by setting $\omega_r = e^{2\pi i r/M}$ and by using (3.14), we have

$$\sum_{x_1=j,\, x_n=k,\, -k_{01}L_0+k_{01}L_1 \equiv \ell \bmod M} P(x^n) = [z^n]\frac{1}{M}\sum_{r=0}^{M-1} \omega_r^{-\ell} \cdot$$

$$\frac{p_0 z(1-p(1|1)\omega_r^{L_1} z)}{1-(p(0|0)+p(1|1)\omega_r^{L_1})z + (p(0|0)p(1|1)\omega_r^{L_1} - p(0|1)\omega_r^{L_0} p(1|0))z^2},$$

that is, we replace $p(0|1)$ by $p(0|1)\omega_r^{L_0}$ and $p(1|1)$ by $p(0|1)\omega_r^{L_1}$, $r = 0, \ldots, M-1$. Note that for $r = 0$ we already observed that $[z^n](1/M)G_{00}(z) = (1/M)p_0\pi_0 + O(\rho^n)$. Thus it remains to show that the corresponding contributions for $r = 1, \ldots, M-1$ are negligible. For this purpose we consider the matrix

$$A^{(r)} = \begin{pmatrix} p(0|0) & p(0|1)\omega_r^{L_0} \\ p(1|0) & p(1|1)\omega_r^{L_1} \end{pmatrix}.$$

For $r = 0$ we clearly have $\rho(A^{(0)}) = 1$ for the spectral radius. If we can show that $\rho(A^{(r)}) < 1$ for $r = 1, \ldots, M-1$ then the following polynomial

$$\begin{aligned} &\begin{vmatrix} 1 - p(0|0)z & -p(0|1)\omega_r^{L_0} z \\ -p(1|0)z & 1 - p(1|1)\omega_r^{L_1} z \end{vmatrix} \\ &= 1 - (p(0|0) + p(1|1)\omega_r^{L_1})z + \\ &+(p(0|0)p(1|1)\omega_r^{L_1} - p(0|1)\omega_r^{L_0} p(1|0))z^2 \end{aligned}$$

has no zeros of modulus $|z| \le 1$. Hence both poles of the corresponding generating function have modulus > 1 which implies that the n-th coefficient can be bounded by $O(\rho^n)$ for some $\rho < 1$.

In order to show that $\rho(A^{(r)}) < 1$ we just have to apply (again) Lemma 3.11 and directly observe that $\rho(A^{(r)}) = 1$ would imply that $\omega_r^{L_0} = \omega_r^{L_1} = 1$ which can only occur for $r = 0$ (here we have to use the assumption $\gcd(L_0, L_1, M) = 1$).

The other cases (where $j = 1$ or $k = 1$) can be handled in completely the same way. □

Summing up this shows that

$$R_n = \sum_{j=0}^{1} \sum_{k=0}^{1} p_j \pi_k \frac{1}{M} \sum_{\ell=0}^{M-1} \left\langle \frac{\ell + \zeta_{jk}(n)}{M} \right\rangle + O(\rho^n).$$

We should observe that the term $p_j \pi_k$ is approximately the probability of $X_1 = j$ and $X_n = k$ since for large n X_1 and X_n are almost independent.

Finally by applying (3.16) we immediately obtain (3.46) Thus we have completed the proof of Theorem 3.9.

3.2.2 Extension to Irreducible Aperiodic Markov Sources

We now discuss some extensions of Theorem 3.9. In particular, we drop the assumption that all transition probabilities must be strictly positive and assume that $\mathbf{P}$ corresponds to an irreducible aperiodic Markov source.

When some of the entries of the matrix $\mathbf{P}$ vanish, then obviously, Theorem 3.9 cannot be used as the corresponding parameters α_{jk} are no longer well defined. Lemma 3.11, which stands at the heart of the proof of Theorem 3.9, can still be used as long as $\mathbf{P}$ is irreducible, but more caution should be exercised. The key issue is still to determine whether there exist parameters s and $\boldsymbol{w}$ that satisfy

$$h \log p(j|k) = (s + w_k - w_j) \bmod 1, \tag{3.69}$$

but now these equations are imposed only for the pairs (j, k) for which $p(j|k) > 0$ (as for the other pairs $a_{jk}(h) = p(j|k) = 0$ satisfy the conditions of Lemma 3.11 automatically anyway).

For example, if one or more diagonal element of $\mathbf{P}$ is positive, and for all positive $p(j|j)$, the numbers $\langle h \log p(j|j)\rangle$ are equal, then s can still be taken to be the common value of all these numbers. If, in addition, at least one row of $\mathbf{P}$ is strictly positive, say, row number l, then w_j can be taken to be $\langle -h \log[p(l|l)/p(j|l)]\rangle$, and then the rationality condition of Theorem 3.9 is replaced by the condition that

$$\alpha'_{jk} = \log\left[\frac{p(j|0)p(0|0)}{p(k|0)p(j|k)}\right] \tag{3.70}$$

must be rational for all (j, k) with $p(j|k) > 0$.

For a general non-negative matrix $\mathbf{P}$, however, it may not be a trivial task to determine whether equations (3.69) have a solution, and if so, what this solution is. In fact, it may be simpler and more explicit to check directly if A_h has an eigenvalue on the unit circle (which thereby dictates s) and then to find $\boldsymbol{w}$ using Lemma 3.11. This would lead to the following generalized version of Theorem 3.9.

Theorem 3.13. Consider the Shannon code of block length n for an irreducible aperiodic Markov source. Let M be defined as the smallest positive integer h such that

$$\rho(A_h) \equiv |\lambda_{1,h}| = 1 \tag{3.71}$$

and set $M = \infty$ if (3.71) does not hold for any positive integer h. Then, $\overline{R}_n$ is characterized as follows:

(a) If $M = \infty$, then

$$\overline{R}_n = \frac{1}{2} + o(1). \tag{3.72}$$

(b) If $M < \infty$, then the asymptotic representation of Theorem 3.9, part (b), holds with $\zeta_{jk}(n)$ being redefined according to

$$\zeta_{jk}(n) = -M[(n-1)s + w_j - w_k - \log p_j], \tag{3.73}$$

where

$$s = \frac{\arg(\lambda_{1,M})}{2\pi} \tag{3.74}$$

and

$$w_j = \frac{\arg(x_j)}{2\pi}, \qquad j = 0, 1, \ldots, m-1, \tag{3.75}$$

x_j being the j–th component of the right eigenvector $\mathbf{x}$ of A_M, which is associated with the dominant eigenvalue $\lambda_{1,M}$.

The proof of Theorem 3.13 is very similar to that of Theorem 3.9 and hence we will not provide it here. In a nutshell, we observe that the Perron–Frobenius Theorem and Lemma 3.11 are still applicable. Then, we use the necessity of the condition $A_h = e^{2\pi i s} DPD^{-1}$ and the fact that once this condition holds, the vector

$$\mathbf{x} = D \cdot \mathbf{1} = (e^{2\pi i w_1}, \ldots, e^{2\pi i w_r})^T$$

is the right eigenvector associated with the dominant eigenvalue $\lambda_{1,m} = e^{2\pi i s}$. We again have to prove a corresponding analogue of Lemma 3.12.

Finally, we present an example with a *reducible* Markov source for which our results do not apply. In particular, in this case there is only one convergent mode of behavior.

Example 3.2. Consider the case $m = 2$, where $p(0|1) = 0$ and $\alpha := p(1|0) \in (0, 1)$, i.e.,

$$P = \begin{pmatrix} 1-\alpha & \alpha \\ 0 & 1 \end{pmatrix}. \tag{3.76}$$

Assume also that $p_0 = 1$ and $p_1 = 0$. Since this is a *reducible* Markov source (once in state 1, there is no way back to state 1), we cannot use Theorems 3.9 and 3.13, but we can still find an asymptotic expression of the redundancy in a direct manner: Note that the chain starts at state ‘0’ and remains there for a random duration, which is a geometrically distributed random variable with parameter $(1-\alpha)$. Thus, the probability of k 0’s (followed by $n-k$ 1’s) is about $(1-\alpha)^k \cdot \alpha$ (for large n) and so the argument of the function $\langle\cdot\rangle$ should be the logarithm of this probability. Taking the expectation w.r.t. the randomness of k, we readily have

$$\overline{R}_n = \sum_{k=0}^{\infty} \alpha(1-\alpha)^k \langle \log\alpha + k\log(1-\alpha)\rangle + o(1). \tag{3.77}$$

We see then that there is *no oscillatory mode* in this case, as $\overline{R}_n$ always tends to a constant that depends on α, in contrast to the convergent mode of Theorems 3.9 and 3.13, where the limit is always 1/2, independently of the source statistics. To summarize, it is observed that the behavior here is very different from that of the irreducible case, characterized by Theorems 3.9 and 3.13.

3.3 Maximal Redundancy for a Generalized Shannon Code

In this section we switch from the average redundancy to the worst case or maximal redundancy. For a given probability distribution P on an alphabet $\mathcal{A}$, we are looking for a prefix code that minimizes the maximal redundancy $R^*(P)$, that is,

$$R^*(P) = \min_C \max_{x\in\mathcal{A}} [L(C,x) + \log P(x)]. \tag{3.78}$$

To solve this optimization problem we introduce a generalized Shannon code denoted as C^{GS}. We write the code length of a generalized Shannon code as

$$L(x, C^{GS}) = \begin{cases} \lfloor \log 1/P(x) \rfloor & \text{if} \quad x\in\mathcal{L} \\ \lceil \log 1/P(x) \rceil & \text{if} \quad x\in\mathcal{U}, \end{cases}$$

where $\mathcal{L}\cup\mathcal{U} = \mathcal{A}$ is a partition of the alphabet $\mathcal{A}$. In addition, we shall postulate Kraft’s inequality is to hold, that is, for the binary case we have

$$\sum_{x\in\mathcal{L}} P(x) 2^{\langle -\log P(x)\rangle} + \frac{1}{2}\sum_{x\in\mathcal{U}} P(x) 2^{\langle -\log P(x)\rangle} \le 1.$$

Our main result of this section is to prove that there exists a generalized Shannon code that is optimal with respect to the maximal redundancy as formulated in (3.78).

Theorem 3.14 (M. Drmota and W. Szpankowski, 2004)**.** If the probability distribution P is dyadic, i.e. $\log P(x) \in \mathbb{Z}$ for all $x \in \mathcal{A}$, then $R_n^*(P) = 0$. Otherwise, let $t_0 \in T = \{\langle -\log P(x) \rangle : x \in \mathcal{A}\}$ be the largest t such that

$$\sum_{x \in \mathcal{L}_t} P(x) 2^{\langle -\log P(x) \rangle} + \frac{1}{2} \sum_{x \in \mathcal{U}_t} P(x) 2^{\langle -\log P(x) \rangle} \leq 1, \tag{3.79}$$

where

$$\mathcal{L}_t := \{x \in \mathcal{A} : \langle -\log P(x) \rangle < t\}$$

and

$$\mathcal{U}_t := \{x \in \mathcal{A} : \langle -\log P(x) \rangle \geq t\}.$$

Then

$$R^*(P) = 1 - t_0 \tag{3.80}$$

and the optimum is obtained for a generalized Shannon code with $\mathcal{L} = \mathcal{L}_{t_0}$ and $\mathcal{U} = \mathcal{U}_{t_0}$.

Proof. If P is dyadic then the numbers $l(x) := -\log P(x)$ are positive integers satisfying

$$\sum_x 2^{-l(x)} = 1.$$

Kraft's inequality holds and consequently there exists a (prefix) code C with $L(C, x) = l(x) = -\log P(x)$ for all $x \in \mathcal{A}$, and this $R^*(P) = 0$.

Now assume that P is not dyadic and let $\mathcal{C}^*$ denote the set of optimal codes, i.e.

$$\mathcal{C}^* = \{C \in \mathcal{C} : R^*(C, P) = R^*(P)\}.$$

The idea of the proof is to establish several properties of an optimal code. In particular, we will show that there exists an optimal code $C^* \in \mathcal{C}^*$ with the following two properties:

(i) For all x

$$\lfloor -\log P(x) \rfloor \leq L(C^*, x) \leq \lceil -\log P(x) \rceil \tag{3.81}$$

(ii) There exists $s_0 \in (0,1]$ such that

$$L(C^*, x) = \lfloor \log 1/P(x) \rfloor \quad \text{if} \quad \langle \log 1/P(x) \rangle < s_0 \tag{3.82}$$

and

$$L(C^*, x) = \lceil \log 1/P(x) \rceil \quad \text{if} \quad \langle \log 1/P(x) \rangle \geq s_0. \tag{3.83}$$

Observe that without losing generality we may assume that $s_0 = 1 - R^*(P)$. Thus, in order to compute $R^*(P)$ we just have to consider codes satisfying (3.82) and (3.83). As already mentioned, (3.79) is just Kraft's inequality for codes of that kind. The optimal choice is $t = t_0$ which also equals s_0. Consequently $R^*(P) = 1 - t_0$.

In view of the above, it suffices to prove properties (i) and (ii). Assume that C^* is an optimal code. First of all, the upper bound in (3.81) is obviously satisfied for C^*. Otherwise we would have

$$\max_x [L(C^*, x) + \log P(x)] > 1$$

which contradicts a simple bound applied to a regular Shannon code. Second, if there exists x such that $L(C^*, x) < \lfloor \log 1/P(x) \rfloor$, then (in view of Kraft's inequality) we can modify this code to a code $\widetilde{C}^*$ with

$$\begin{aligned} L(\widetilde{C}^*, x) &= \lceil \log 1/P(x) \rceil \quad \text{if } L(C^*, x) = \lceil \log 1/P(x) \rceil, \\ L(\widetilde{C}^*, x) &= \lfloor \log 1/P(x) \rfloor \quad \text{if } L(C^*, x) \leq \lfloor \log 1/P(x) \rfloor. \end{aligned}$$

By construction, $R^*(\widetilde{C}^*, P) = R^*(C^*, P)$. Thus, $\widetilde{C}^*$ is optimal, too. This proves (i).

Now consider an optimal code C^* satisfying (3.81) and let $\widetilde{x} \in \mathcal{A}$ with $R^*(P) = 1 - \langle -\log P(\widetilde{x}) \rangle$. Thus, $L(C^*, x) = \lfloor \log 1/P(x) \rfloor$ for all x with $\langle -\log P(x) \rangle < \langle -\log P(\widetilde{x}) \rangle$. This proves (3.82) with $s_0 = \langle -\log P(\widetilde{x}) \rangle$. Finally, if (3.83) is not satisfied, then (in view of Kraft's inequality) we can modify this code to a code $\widetilde{C}^*$ with

$$\begin{aligned} L(\widetilde{C}^*, x) &= \lceil \log 1/P(x) \rceil \quad \text{if } \langle \log 1/P(x) \rangle \geq s_0, \\ L(\widetilde{C}^*, x) &= \lfloor \log 1/P(x) \rfloor \quad \text{if } \langle \log 1/P(x) \rangle < s_0. \end{aligned}$$

By construction, $R^*(\widetilde{C}^*, P) = R^*(C^*, P)$. Thus, $\widetilde{C}^*$ is optimal, too. This proves (ii) and the lemma. □

We apply the above now to a binary Bernoulli source on the alphabet $\mathcal{A} = \{0,1\}^n$ with parameter p.

Theorem 3.15. Let P be a binary Bernoulli source on the alphabet $\mathcal{A} = \{0,1\}^n$ with parameter p and let $R_n^*(p)$ denote the corresponding maximal redundancy.
(i) If $\log \frac{1-p}{p}$ is irrational then, as $n \to \infty$,

$$R_n^*(p) = -\frac{\log\log 2}{\log 2} + o(1) = 0.5287\ldots + o(1). \tag{3.84}$$

(ii) If $\log \frac{1-p}{p} = \frac{N}{M}$ (for some coprime integers $M, N \in \mathbb{Z}$) is rational and non-zero, then as $n \to \infty$

$$R_n^*(p) =$$

$$-\frac{\lfloor M\log(M(2^{1/M}-1)) - \langle Mn\log 1/(1-p)\rangle\rfloor + \langle Mn\log 1/(1-p)\rangle}{M} + o(1).$$

Finally, if $\log \frac{1-p}{p} = 0$ then $p = \frac{1}{2}$ and $R_n^*(1/2) = 0$.

Proof. As before we set

$$\alpha = \log\frac{1-p}{p}, \qquad \beta = \log\frac{1}{1-p}.$$

Then

$$-\log(p^k(1-p)^{n-k}) = \alpha k + \beta n.$$

Since α is irrational, we know from from previous section that $\langle \alpha n\rangle$ is a Bernoulli-u.d modulo 1 sequence, and therefore for any Riemann integrable function f

$$\lim_{n\to\infty}\sum_{k=0}^{n}\binom{n}{k}p^k(1-p)^{n-k}f(\langle \alpha k + \beta n\rangle) = \int_0^1 f(x)\,dx. \tag{3.85}$$

Now set $f_{s_0}(x) = 2^x$ for $0 \le x < s_0$ and $f_{s_0}(x) = 2^{x-1}$ for $s_0 \le x \le 1$. We find

$$\lim_{n\to\infty}\sum_{k=0}^{n}\binom{n}{k}p^k(1-p)^{n-k}f_{s_0}(\langle \alpha k + \beta n\rangle) = \frac{2^{s_0-1}}{\log 2}.$$

In particular, for

$$s_0 = 1 + \frac{\log\log 2}{\log 2} = 0.4712\ldots$$

we obtain $\int_0^1 f(x)\,dx = 1$, so that the Kraft's inequality becomes equality. This implies that

$$\lim_{n\to\infty} R_n^*(p) = 1 - s_0 = 0.5287\ldots$$

which proves (3.84).

Now we establish the second part of Theorem 3.15, that is, *if* $\log\frac{1-p}{p} = \frac{N}{M}$ *is rational and non-zero (with coprime integers* N, M*) then, as* $n \to \infty$

$$R_n^*(p) =$$
$$-\frac{\lfloor M\log(M(2^{1/M}-1)) - \langle Mn\log 1/(1-p)\rangle\rfloor + \langle Mn\log 1/(1-p)\rangle}{M} + o(1).$$

We now apply Lemma 3.7 to arrive at

$$\begin{aligned}\sum_{k=0}^{n}\binom{n}{k}p^k(1-p)^{n-k}f(\langle\alpha k+\beta n\rangle) &= \frac{1}{M}\sum_{m=0}^{M-1} f\left(\left\langle\frac{mN}{M}+\beta n\right\rangle\right) + o(1)\\ &= \frac{1}{M}\sum_{m=0}^{M-1} f\left(\frac{m+\langle M\beta n\rangle}{M}\right) + o(1).\end{aligned}$$

As before, we use $f_{s_0}(x)$, where s_0 is of the form

$$s_0 = \frac{m_0 + \langle M\beta n\rangle}{M}$$

and choose m_0 maximal such that

$$\begin{aligned}\frac{1}{M}\sum_{m=0}^{M-1} f_{s_0}\left(\frac{m+\langle M\beta n\rangle}{M}\right) &= \frac{2^{\langle M\beta n\rangle}/M}{M}\left(\sum_{m=0}^{m_0-1} 2^{m/M} + \sum_{m=m_0}^{M-1} 2^{m/M-1}\right)\\ &= \frac{2^{(\langle M\beta n\rangle+m_0)/M-1}}{M(2^{1/M}-1)}\\ &\le 1.\end{aligned}$$

Thus

$$m_0 = M + \lfloor M\log(M(2^{1/M}-1)) - \langle Mn\log 1/(1-p)\rangle\rfloor,$$

and consequently

$$\begin{aligned} R_n^*(p) &= 1 - s_0 + o(1) \\ &= 1 - \frac{m_0 + \langle M\beta n\rangle}{M} + o(1) \\ &= -\frac{\lfloor M\log(M(2^{1/M}-1)) - \langle Mn\log 1/(1-p)\rangle\rfloor + \langle Mn\beta\rangle}{M} + o(1). \end{aligned}$$

This completes the proof of Theorem 3.15. □

4

Redundancy of Tunstall and Khodak VF Codes

This chapter is devoted to the analysis of the average redundancy for variable-to-fixed codes such as Khodak and Tunstall codes.

Tunstall's algorithm [158] for the construction of a VF code has been studied extensively (cf. the survey article [1]). Simple bounds for its redundancy were obtained independently by Khodak [79] and by Jelinek and Schneider [77]. Tjalkens and Willems [157] were the first to look at extensions of this code to sources with memory. Savari and Gallager [132] proposed a generalization of Tunstall's algorithm for Markov sources and used renewal theory for an asymptotic analysis of the average code word length and for the redundancy for memoryless and Markov sources. In this chapter, we restrict our analysis to memoryless sources. Our presentation here is based on an analytic approach discussed in [34, 35].

4.1 Variable-to-Fixed Codes

We now study variable-to-fixed (VF) length codes. Recall that in the VF scenario, the source string x, say over m-ary alphabet $\{0, 1, \ldots, m-1\}$, is partitioned into non-overlapping (unique) phrases, each belonging

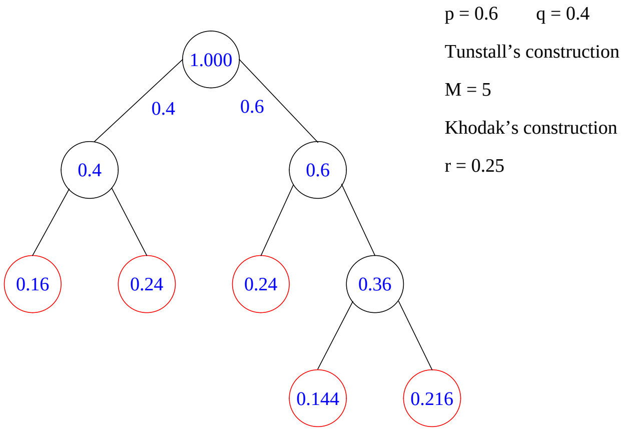


Figure 4.1: Tunstall's and Khodak's Codes for $M = 5$, $v = 4$, binary source with $p = 0.6$ (and $q = 1 - p$). Here the resulting dictionary is $\mathcal{D} = \{00, 01, 10, 110, 111\}$.

to a given *dictionary* $\mathcal{D}$ represented by a complete *parsing tree* $\mathcal{T}$. The dictionary entries $d \in \mathcal{D}$ correspond to the *leaves* of the associated parsing tree. The encoder represents each parsed string by the fixed length binary code word corresponding to its dictionary entry. If the dictionary $\mathcal{D}$ has M entries, then the code word for each phrase has $\lceil \log_2 M \rceil$ bits. The code C is, thus, a mapping $C : \mathcal{D} \to \{0,1\}^{\lceil \log_2 M \rceil}$. (It is convenient to use the notation $\mathcal{D}$ instead of $\mathcal{A}$, since in this context the letter $\mathcal{A}$ is also used to denote the source alphabet $\{0, 1, \ldots, m-1\}$.)

The best known variable-to-fixed length code is the Tunstall code [158] that is (almost) that same as the independently discovered Khodak code [79].

We first describe the Tunstall code. In such a code, edges in the parsing tree correspond to letters from the source alphabet $\{0, 1, \ldots, m-1\}$ and are labeled by the alphabet probabilities, say $p_0, \ldots, p_{m-1}$. Every vertex in such a tree is assigned the probability of the path leading to it from the root, as shown in Figure 4.1. For memoryless sources, studied here, the probability of a vertex is the product of probabilities of vertices leading to it. More precisely, the root node has m leaves corresponding to all of the symbols in $\{0, 1, \ldots, m-1\}$ and labeled by $p_0, \ldots, p_{m-1}$. The algorithms starts with the trivial tree that contains just the root that (corresponding to the empty word and) is labeled by the probability 1. At each iteration one selects the current leaf corresponding to a string of the *highest probability*, say $P_{\max}$, and grows m children out of it with probabilities $p_0 P_{\max}, \dots, p_{m-1} P_{\max}$. After J iterations, the parsing tree has J non-root *internal nodes* and $M = (m-1)J + m$ leaves, each corresponding to a distinct dictionary entry. The idea behind this algorithm is to generate a parsing tree, where all leaves have approximately the same probability, that is, distribution on $\mathcal{D}$ is close to uniform.

Another algorithm was proposed by Khodak [79] who independently discovered the Tunstall code using a rather different approach. Let $p_{\min} = \min\{p_0, \dots, p_{m-1}\}$. Khodak suggested choosing a real number $v > 1/p_{\min}$ and growing a complete parsing tree until all leaves $d \in \mathcal{D}$ satisfy

$$p_{\min}/v \le P(d) < 1/v. \tag{4.1}$$

Khodak's and Tunstall's algorithms are illustrated in Figure 4.1 with the dictionary $\mathcal{D} = \{00, 01, 10, 110, 111\}$ corresponding to strings represented by the paths from the root to all terminal nodes.

It is known (see, e.g., [132, Lemma 2]) that the parsing trees for Tunstall and Khodak algorithms are – in some instances — exactly the same, however, they react differently to the probability tie when expanding a leaf. More precisely, when there are several leaves with the same probability, the Tunstall algorithm selects *one* leaf and expands it, then selects another leaf of the same probability, and continues doing it until all leaves of the same probability are expanded. The Khodak algorithm expands *all* leaves with the same probability simultaneously, in parallel; thus there are "jumps" in the number of dictionary entries M when the parsing tree grows. For example, in Figure 4.1 two nodes marked "0.24" will be expanded simultaneously in the Khodak algorithm, and one after another by the Tunstall algorithm. We shall analyze M in this chapter.

Our goal is to present a precise analysis of the Khodak and Tunstall redundancy as well as to provide some insights into the behavior of the parsing tree (i.e., the path length distribution). In particular, we derive average redundancy *rate* $\overline{r}$ which is defined as

$$\overline{r} = \frac{\log M}{\mathbf{E}[D]} - h, \tag{4.2}$$

where $\mathbf{E}[D] = \sum_{d \in \mathcal{D}} |d| P_{\mathcal{D}}(d)$ is the average phrase length, D, of the dictionary $\mathcal{D}$ and $h := h_S = \sum_{i=0}^{m-1} p_i \log(1/p_i)$ is the entropy of the source. We note that $\mathbf{E}[D]$ is also known as the average *delay*, which is actually the average path length from the root to a terminal node in the corresponding parsing tree.

In passing we should observe that by the *Conservation of Entropy Property* [78, 134] the entropy of the dictionary $h_{\mathcal{D}}$ is related to the source entropy h_S as follows

$$h_{\mathcal{D}} = h_S \mathbf{E}[D]. \tag{4.3}$$

4.2 Redundancy of the Khodak VF Code

For Khodak's code, it follows from (4.1) that if y is a proper prefix of one or more entries of $\mathcal{D}$ (that is, y corresponds to an internal node of the parsing tree $\mathcal{T}$), then

$$P(y) \geq 1/v. \tag{4.4}$$

It is therefore easier to describe the internal nodes of the parsing tree $\mathcal{T}$ rather than its leaves. We shall follow this approach when analyzing the phrase length D of Khodak's code.

In what follows we always fix some $v > 0$ and will denote by $\mathcal{D}_v$ the dictionary of the corresponding Khodak code, by M_v the cardinality of $\mathcal{D}_v$, and by D_v the phrase lengths $|d|$ of $d \in \mathcal{D}_v$, considered as a random variable with probability distribution P on $\mathcal{D}_v$.

As mentioned above, our goal is to understand the behavior of the dictionary size M_v and the probabilistic behavior of the phrase length D_v (when the source is memoryless). Our approach throughout is analytic and we use such tools as the Mellin transform and the Tauberian theorems [47, 154]. We present our results for a general source alphabet $\{0, 1, \ldots, m-1\}$ of size m with probability p_i for $0 \leq i < m$; however, most proofs are for a binary source alphabet with $p_0 = p$ and $p_1 = q = 1 - p$.

We first deal with M_v and provide a simple relation between it and parameter v. To find an expression for M_v we introduce a new function $A(v)$ defined as the number of source strings with probability at least $1/v$, that is,

$$A(v) = \sum_{y: P(y) \geq 1/v} 1. \tag{4.5}$$

Observe that $A(v)$ represents the number of internal nodes in Khodak's construction with parameter v of a Tunstall tree. Equivalently, $A(v)$ counts the number of strings y with the self-information $-\log P(y) \leq \log v$. The function $A(v)$ satisfies the following recurrence

$$A(v) = \begin{cases} 0 & v < 1, \\ 1 + A(vp_0) + \cdots + A(vp_{m-1}) & v \geq 1. \end{cases} \tag{4.6}$$

Indeed, by definition we have $A(v) = 0$ for $v < 1$. Now suppose that $v \geq 1$. Since every m-ary string is either the empty string or a string starting with a source letter j with $0 \leq j < m$, we directly find the recurrence $A(v) = 1 + A(vp_0) + \cdots + A(vp_{m-1})$.

Since $A(v)$ represents the number of internal nodes in Khodak's construction with parameter v it follows that the dictionary size is given by

$$M_v = |\mathcal{D}_v| = (m-1)A(v) + 1.$$

Therefore, it is sufficient to obtain asymptotic expansions for $A(v)$ for $v \to \infty$.

To present these results succinctly, we need to introduce the following concept. We say that $\log(1/p_0), \ldots, \log(1/p_{m-1})$ are *rationally related* if there exists a positive real number L such that $\log(1/p_0), \ldots, \log(1/p_{m-1})$ are integer multiples of L, that is,

$$\log(1/p_j) = n_j L, \quad n_j \in \mathbb{Z}, \quad (0 \leq j < m).$$

Without loss of generality we can assume that L is as large as possible which is equivalent to $\gcd(n_0, \ldots, n_{m-1}) = 1$. For example, in the binary case $m = 2$ this is equivalent to the statement that the ratio $\log(1/p_0)/\log(1/p_1)$ is rational. Similarly we say that $\log(1/p_0), \ldots, \log(1/p_{m-1})$ are *irrationally related* if they are not rationally related.

Now are we ready to present our first result.

Theorem 4.1. We consider Khodak's VF code construction with parameter v. If $\log(1/p_0), \ldots, \log(1/p_{m-1})$ are irrationally related, then

$$M_v = (m-1)\frac{v}{h \ln 2} + o(v). \tag{4.7}$$

Otherwise, when $\log(1/p_0), \ldots, \log(1/p_{m-1})$ are rationally related, let $L > 0$ be the largest real number for which $\log(1/p_1), \ldots, \log(1/p_m)$ are integer multiples of L. Then

$$M_v = (m-1)\frac{Q_1(\ln v)}{h \ln 2} v + O(v^{1-\eta}) \tag{4.8}$$

for some $\eta > 0$ where

$$Q_1(x) = \frac{L}{1-e^{-L}} e^{-L\langle \frac{x}{L} \rangle}, \tag{4.9}$$

and, recall, $\langle x \rangle = x - \lfloor x \rfloor$ is the fractional part of the real number x.

Proof. We present a proof that is based on the Mellin transform. Furthermore, for simplicity we only present it for the binary case.

The Mellin transform $F^*(s)$ of a function $F(v)$ for complex s is defined as (see [46, 154]),

$$F^*(s) = \int_0^\infty F(v) v^{s-1} dv,$$

if it exists. Using the fact that the Mellin transform of $F(ax)$ is $a^{-s}F^*(s)$, a simple analysis of recurrence (4.6) reveals that the Mellin transform $A^*(s)$ of $A(v)$ is given by

$$A^*(s) = \frac{-1}{s(1 - p_0^{-s} - p_1^{-s})}, \qquad \Re(s) < -1.$$

In order to find asymptotics of $A(v)$ as $v \to \infty$ one can directly use the Tauberian theorem (for the Mellin transform) by Wiener-Ikehara [94, Theorem 4.1] (see also Theorem 5.6 of Chapter 5), which says that if $F(v) = 0$ for $v < 1$, $F(v) \geq 0$ for $v \geq 1$, and if $\frac{1}{s}F^*(s)$ can be represented as

$$\frac{1}{s}F^*(s) = G(s) + \frac{A_0}{s - s_0},$$

where $G(s)$ is analytic for $\Re(s) < s_0$ and has a continuous extension to the half plane $\Re(s) \le s_0$, then it follows that

$$F(v) \sim A_0 v^{-s_0}.$$

In the present context we observe that $s_0 = -1$ is the only (polar) singularity on the line $\Re(s) = -1$ and that $(s+1)A^*(s)$ can be analytically extended to a region that contains the line $\Re(s) = -1$. Namely, if $\log(p_0)/\log(p_1)$ is irrational this follows from a lemma of Schachinger and Jacquet [154] (see also Lemma 4.5 below). In particular, in the irrational case one finds

$$A(v) \sim \frac{v}{h \ln 2}, \qquad (v \to \infty).$$

This proves the first part of Theorem 4.1.

In the rational case, that is, $\log(1/p_0) = n_0 L$ and $\log(1/p_1) = n_1 L$ for coprime integers n_0, n_1 we just have to analyze the recurrence

$$G_n = 1 + G_{n-n_0} + G_{n-n_1},$$

where G_n abbreviates $A(e^{Ln})$. Equivalently we have $A(v) = G(\lfloor \log v \rfloor / L)$. Thus, from

$$G(n) = \frac{1}{(1-e^{-L})(de^{-dL} + be^{-bL})} e^{Ln} + O(e^{Ln(1-\eta)})$$

for some $\eta > 0$, we directly obtain

$$A(v) = \frac{Le^{-L\langle \log v/L \rangle}}{(1-e^{-L})} \frac{v}{h \ln 2} + O(v^{(1-\eta)})$$

where, as above, $\langle x \rangle$ is the fractional part of x. □

We add that we could have also used a Laplace transform approach presented in Choi and Golin [18].

Next we deal with our main goal, namely the analysis of the phrase length and Khodak's code redundancy. We start with deriving the moment generating function of the phrase length D_v and then its moments. Let us define the probability generating function $D(v,z)$ of the phrase length $D := D_v$ for the Khodak code with parameter v as

$$D(v,z) := \mathbf{E}[z^{D_v}] = \sum_{d \in \mathcal{D}_v} P(d) z^{|d|}.$$

However, it is better to work with another transform describing the probabilities of strings which correspond to *internal nodes* in the parsing tree $\mathcal{T}_v$. Therefore, we also define

$$S(v,z) = \sum_{y\colon\ P(y)\geq 1/v} P(y) z^{|y|}. \tag{4.10}$$

Lemma 4.2. The function $S(v,z)$ satisfies the following recurrence

$$S(v,z) = \begin{cases} 0 & v < 1, \\ 1 + p_1 S(vp_0, z) + \cdots + p_{m-1} S(vp_{m-1}, z) & v \geq 1. \end{cases} \tag{4.11}$$

Furthermore,

$$D(v,z) = 1 + (z-1) S(v,z) \tag{4.12}$$

for all complex z.

Proof. The recurrence (4.11) can be derived in the same way as for $A(v)$. The relation (4.12) follows from the following general fact on trees. Let $\widetilde{\mathcal{D}}$ be a uniquely parsable dictionary (e.g., leaves in the corresponding parsing tree) and $\widetilde{\mathcal{Y}}$ be the collection of strings which are proper prefixes of one or more dictionary entries (e.g., internal nodes). Then for all complex z (see [35])

$$\sum_{d\in\widetilde{\mathcal{D}}} P(d) \left(1 + z + \cdots z^{|d|-1}\right) = \sum_{y\in\widetilde{\mathcal{Y}}} P(y) z^{|y|}, \tag{4.13}$$

This can be deduced directly by induction and implies (4.12).

Alternatively we can use a result of [109], where it is shown that for every real-valued function G defined on strings over $\mathcal{A}$

$$\sum_{d\in\mathcal{D}} P(d) G(d) = G(\emptyset) + \sum_{y\in\mathcal{Y}} P(y) \sum_{s\in\mathcal{A}} \frac{P(ys)}{P(y)} (G(ys) - G(y))$$

where $\emptyset$ denotes an empty string, $\mathcal{D}$ the set of external nodes and $\mathcal{Y}$ the set of internal nodes. By choosing $G(x) = z^{|x|}$ we directly find

$$\begin{aligned} \sum_{d\in\mathcal{D}} P(d) z^{|d|} &= z^0 + \sum_{y\in\mathcal{Y}} P(y) \sum_{s\in\mathcal{A}} P(s) \left(z\, z^{|y|} - z^{|y|}\right) \\ &= 1 + (z-1) \sum_{y\in\mathcal{Y}} P(y), \end{aligned}$$

which again proves (4.13). □

In view of Lemma 4.2 we conclude that

$$\mathbf{E}[D] = \sum_{y\in\mathcal{Y}} P(y) = S(v,1), \qquad \mathbf{E}[D(D-1)] = 2\sum_{y\in\mathcal{Y}} P(y)|y| = S'(v,1)$$

This allows us to formulate our next main result.

Theorem 4.3. We consider Khodak's VF code construction with parameter v.
(i) If $\log(1/p_0),\ldots,\log(1/p_{m-1})$ are irrationally related, then

$$\mathbf{E}[D_v] = S(v,1) = \frac{\log v}{h} + \frac{h_2}{2h^2} + o(1), \tag{4.14}$$

where $h_2 = \sum_{i=0}^{m-1} p_i \log^2 p_i$, while in the rational case

$$\mathbf{E}[D_v] = S(v,1) = \frac{\log v}{h} + \frac{h_2}{2h^2} + \frac{Q_2(\ln v)}{h \ln 2} + O(v^{-\eta}) \tag{4.15}$$

for some $\eta > 0$, where

$$Q_2(x) = L \cdot \left(\frac{1}{2} - \left\langle \frac{x}{L} \right\rangle\right) \tag{4.16}$$

for L as defined above.
(ii) The phrase length D_v in Khodak's construction with parameter v of the Tunstall code with a dictionary of size M_v over a *biased* memoryless source (i.e., not all symbol probabilities are equal) satisfies the Central Limit Law, that is, as $M_v \to \infty$

$$\frac{D_v - \frac{1}{h}\log M_v}{\sqrt{\left(\frac{h_2}{h^3} - \frac{1}{h}\right)\log M_v}} \to N(0,1)$$

where $N(0,1)$ denotes the standard normal distribution. Furthermore, we have

$$\begin{aligned} \mathbf{E}[D_v] &= \frac{\log M_v}{h} + O(1) \\ \mathrm{Var}[D_v] &\sim \left(\frac{h_2}{h^3} - \frac{1}{h}\right)\log M_v, \end{aligned}$$

where M_v is give in Theorem 4.1.

Remark 4.1. Before we discuss any further Khodak code, we should describe another useful representation of the Khodak code using a random walk in the first quadrant. As already observed in Chapter 2, a path in the parsing tree from the root to a leaf corresponds to a random walk on a lattice in the first quadrant of the plane (see Figure 2.1). Indeed, observe that our analysis of the Khodak code boils down to studying the following sum

$$A(v) = \sum_{y:P(y)\geq 1/v} f(v)$$

for some function $f(v)$. Since $P(y) = p^{k_1}q^{k_2}$ for some nonnegative integers $k_1, k_2 \geq 0$, we conclude that the summation set of $A(v)$ can be expressed, after setting $v = 2^V$, as

$$k_1 \log(1/p) + k_2 \log(1/q) \leq V. \tag{4.17}$$

This corresponds to a random walk in the first quadrant with the linear boundary condition $ax + by = V$, where $a = \log(1/p)$ and $b = \log(1/q)$ as shown in Figure 4.2. The phrase length D_v of the Khodak code coincides with the *exit time* of such a random walk (i.e., the last step before the random walk hits the linear boundary). This correspondence is further explored in [38, 76]. In particular, in [38] we analyze the Khodak code with additional constraint on the length of the phrase length.

Finally, before presenting a proof of Theorem 4.3, let us discuss its consequences for the redundancy rate of the Khodak code. By combining (4.7) and (4.14) resp. (4.8) and (4.15) we find for the irrational case

$$\mathbf{E}[D_v] = \frac{\log M_v}{h} + \frac{\log(h \ln 2)}{h} + \frac{h_2}{2h^2} + o(1)$$

and in the rational case we have

$$\begin{aligned}\mathbf{E}[D_v] \quad = \quad & \frac{\log M_v}{h} + \frac{\log(h \ln 2)}{h} + \frac{h_2}{2h^2} + \\ & \frac{-\log L + \log(1-e^{-L}) + L\log(e)/2}{h} + O(M_v^{-\eta}).\end{aligned}$$

Recall that $L > 0$ is the largest real number for which $\log(1/p_0), \ldots, \log(1/p_{m-1})$ are integer multiples of L. As a direct consequence, we can derive a precise asymptotic formula for the average

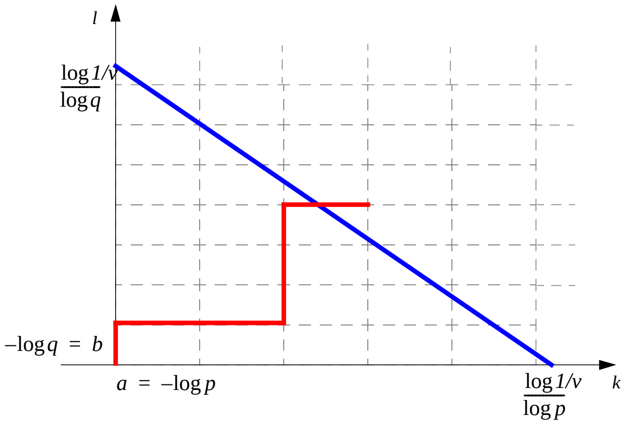


Figure 4.2: A random walk with a linear barrier; the exit time is equivalent to the phrase length in the Khodak algorithm (e.g., the exit time = 7).

redundancy of the Khodak code, that is,

$$\overline{r}_M^K = \frac{\log M}{\mathbf{E}[D]} - h\,.$$

The following result is a consequence of the above derivations.

Corollary 4.4. Let $\mathcal{D}_v$ denote the dictionary in Khodak's construction of the Tunstall code of size M_v. If $\log(1/p_0), \ldots, \log(1/p_{m-1})$ are irrationally related, then

$$\overline{r}_{M_v}^K = \frac{h}{\log M_v}\left(-\frac{h_2 \ln 2}{2h} - \log(h \ln 2)\right) + o\left(\frac{1}{\log M_v}\right).$$

In the rational case we have

$$\begin{aligned}\overline{r}_{M_v}^K \quad = \quad & \frac{h}{\log M_v}\Big(- \frac{h_2 \ln 2}{2h} - \log(h \ln 2) - \log\left(\frac{\sinh(L/2)}{L/2}\right)\Big) \\ & + O\left(\frac{1}{\log^2 M_v}\right).\end{aligned}$$

Proof of Theorem 4.3. Again we only present the proof of the binary case. In order to prove Theorem 4.3(i), we consider

$$\mathbf{E}[D_v] = \sum_{y:P(y)\geq 1/v} P(y) = S(v,1).$$

Here the Mellin transform is given by

$$D^*(s) = \int_0^\infty \mathbf{E}[D_v] v^{s-1}\, dv = \frac{-1}{s(1-p_0^{1-s}-p_1^{1-s})} \qquad (\Re(s) < 0)$$

and it leads (in the irrational case) after applying a proper extension of the Wiener-Ikehara theorem (see Theorem 5.6) to the asymptotic equivalent

$$\mathbf{E}[D_v] \sim \frac{\log(v)}{h}.$$

Note that the double pole at $s = 0$ is responsible for the log-factor Actually a more careful analysis that is based on the inverse Mellin transform – that we will develop below – determines also the second order term:

$$\mathbf{E}[D_v] = \frac{\log(v)}{h} + \frac{h_2}{2h^2} + o(1).$$

In the rational case, it is easy to see (similarly to the proof of Theorem 4.1) that

$$\mathbf{E}[D_v] = \frac{\log(v)}{h} + \frac{h_2}{2h^2} + \frac{L}{h}_e\left(\frac{1}{2} - \left\langle\frac{\log(v)}{L}\right\rangle\right) + O(r^\eta)$$

for some $\eta > 0$.

The analysis of $D(v, z)$ is more involved. Here we do not give a full proof but restrict ourselves to the irrational case and give (only) a heuristic argument bases on the Wiener-Ikehara Tauberian theorem (for rigorous proof see [35]).

We assume that z is a real number close to 1, say $|z - 1| \le \delta$. The Mellin transform $D^*(s, z)$ of $D(v, z)$ with respect to v is

$$D^*(s,z) = \frac{1-z}{s(1-zp^{1-s}-zq^{1-s})} - \frac{1}{s}, \tag{4.18}$$

for $\Re(s) < s_0(z)$, where $s_0(z)$ denotes the real solution of the characteristic equation:

$$zp^{1-s} + zq^{1-s} = 1, \tag{4.19}$$

where now we write $p := p_0$ and $q := p_1$. It is easy to see that

$$s_0(z) = -\frac{z-1}{h_e} + \left(\frac{1}{h_e} - \frac{p\ln^2 p + q\ln^2 q}{2h_e^3}\right)(z-1)^2 + O((z-1)^3)$$

as $z \to 1$ where $h_e = p \ln(1/p) + q \ln(1/q)$ is the natural entropy.

The next step is to determine the polar singularities of the meromorphic continuation of $D^*(s,z)$ right to the line $\Re(s) = s_0(z)$, that is, we have to analyze the set

$$\mathcal{Z}(z) = \{s \in \mathbf{C} : zp^{1-s} + zq^{1-s} = 1\} \tag{4.20}$$

of all complex roots of the characteristic equation (5.12). Actually there is a result due to Jacquet and Schachinger that summarizes all needed properties of the set $\mathcal{Z}(z)$. Its proof can be found in [35].

Lemma 4.5. Suppose that $0 < p < q < 1$ and that z is a real number with $|z-1| \le \delta$ for some $0 < \delta < 1$. Let

$$\mathcal{Z}(z) = \{s \in \mathbf{C} : p^{1-s} + q^{1-s} = 1/z\}.$$

(i) All $s \in \mathcal{Z}(z)$ satisfy

$$s_0(z) \le \Re(s) \le \sigma_0(z),$$

where $s_0(z) < 1$ is the (unique) real solution of $p^{1-s} + q^{1-s} = 1/z$ and $\sigma_0(z) > 1$ is the (unique) real solution of $1/z + q^{1-s} = p^{1-s}$. Furthermore, for every integer k there uniquely exists $s_k(z) \in \mathcal{Z}(z)$ with

$$(2k-1)\pi/\log p < \Im(s_k(z)) < (2k+1)\pi/\log p$$

and consequently $\mathcal{Z}(z) = \{s_k(z) : k \in \mathbf{Z}\}$.

(ii) If $\log q/\log p$ is irrational, then $\Re(s_k(z)) > \Re(s_0(z))$ for all $k \neq 0$ and also

$$\min_{|z-1|\le\delta} (\Re(s_k(z)) - \Re(s_0(z))) > 0. \tag{4.21}$$

(iii) If $\log q/\log p = r/d$ is rational, where $\gcd(r,d) = 1$ for integers $r, d > 0$, then we have $\Re(s_k(z)) = \Re(s_0(z))$ if and only if $k \equiv 0 \bmod d$. In particular $\Re(s_1(z)), \dots, \Re(s_{d-1}(z)) > \Re(s_0(z))$ and

$$s_k(z) = s_{k \bmod d}(z) + \frac{2(k - k \bmod d)\pi i}{\log p},$$

that is, all $s \in \mathcal{Z}(z)$ are uniquely determined by $s_0(z)$ and by $s_1(z), s_2(z), \dots, s_{d-1}(z)$, and their imaginary parts constitute an arithmetic progression.

In particular it follows that we can apply Wiener-Ikehara's Tauberian theorem in the irrational case and we obtain for every fixed (real) z (with $|z-1| \le \delta$)

$$D(v,z) = \frac{1-z}{zs_0(z)H(s_0(z)-1)} v^{-s_0(z)}(1+o(1)), \qquad (v \to \infty), \quad (4.22)$$

where $H(s)$ abbreviates

$$H(s) = p_1^{-s}\log(1/p_1) + p_2^{-s}\log(1/p_2).$$

Now if we assume that the error term in (4.22) is uniform in z then we can use the local expansion

$$s_0(z) = -\frac{z-1}{h_e} + \left(\frac{1}{h_e} - \frac{h_2}{2h^3}\right)(z-1)^2 + O(|z-1|^3) \qquad (4.23)$$

to obtain uniformly for $|z-1| \le \delta$ as $v \to \infty$, and then

$$\begin{aligned} D(v,z) &= v^{-s_0(z)}(1+O(s_0(z)+o(1)) \\ &= v^{\frac{z-1}{h_e}+\left(\frac{1}{h_e}-\frac{h_2}{2h^3}\right)(z-1)^2+O(|z-1|^3)}\left(1+O(|z-1|)+o(1)\right). \end{aligned}$$

Recall that $D(v,z) = \mathbf{E}[z^{D_v}]$ is the probability generating function of the dictionary length D_v and, therefore, it can be used to derive the limiting behavior. We can use the local expansion (4.23) with $z = e^{t/(\log v)^{1/2}}$ to obtain

$$\begin{aligned} v^{-s_0(z)} &= \exp\left(\log v\left(\frac{z-1}{h}_e - \left(\frac{1}{h_e} - \frac{h_2}{2h^3}\right)(z-1)^2 + O(|z-1|^3)\right)\right) \\ &= \exp\left(\frac{1}{h_e}t\sqrt{\log v} + \frac{1}{h_e}\frac{t^2}{2} - \left(\frac{1}{h_e} - \frac{h_2}{2h^3}\right)t^2 + O(t^3/\sqrt{\log v})\right) \\ &= \exp\left(\frac{1}{h_e}t\sqrt{\log v} + \left(\frac{h_2}{h^3} - \frac{1}{h_e}\right)\frac{t^2}{2} + O(t^3/\sqrt{\log v})\right) \end{aligned}$$

Hence, we arrive at

$$\mathbf{E}\left[e^{t(D_v - \frac{1}{h_e}\log v)/\sqrt{\log v}}\right] = e^{-(t/h_e)\sqrt{\log v}}\mathbf{E}\left[e^{D_v t/\sqrt{\log v}}\right] \sim e^{\frac{t^2}{2}\left(\frac{h_2}{h^3}-\frac{1}{h_e}\right)}. \quad (4.24)$$

By Laplace's theorem this would prove the normal limiting distribution as $v \to \infty$ (and also convergence of all (centralized) moments as well as exponential tail estimates).

The actual proof of Theorem 4.3 in the irrational case requires a more precise analysis that is based on the inverse Mellin transform

$$D(v,z) = \frac{1}{2\pi i} \lim_{T\to\infty} \int_{\sigma-iT}^{\sigma+iT} D^*(s,z) v^{-s}\, ds, \tag{4.25}$$

where $\sigma < s_0(z)$. In fact it turns out that the appearing integral is not absolutely convergent. To circumvent this problem, we resort to analyze another integral (see [160]), namely

$$D_1(v,z) = \int_0^v D(w,z)\, dw.$$

Clearly, the Mellin transform $D_1^*(s,z) = -D^*(s+1,z)/s$, and therefore it is of order $O(1/s^2)$. Then one can estimate its inverse Mellin by shifting the integral to the right and by taking into account the appearing residues corresponding to the zeros $\mathcal{Z}(z)$ that are described in Lemma 4.5. This finally leads to an asymptotic representation of $D_1(v,z)$ of the form

$$D_1(v,z) = \frac{1-z}{zs_0(z)(-s_0(z)+1)H(s_0(z)-1)} v^{-s_0(z)+1}(1+o(1)),$$

that is uniform in z (for $|z-1| \le \delta$). Since $D(v,z)$ is non-negative it is an easy exercise to recover from this relation (4.22), now uniformly in z and so the proof (in the irrational case) can be finished as above.

In the rational case we reduce the recurrence for $D(v,z)$ to a discrete recurrence (as is the proof of Theorem 4.1) which can be asymptotically solved uniformly in z and provides as central limit theorem by Laplace's theorem.

4.3 Analysis of the Tunstall Code

Let us now return to the Tunstall code. Recall that the parsing tree is the same as for the Khodak code, but in the case of a tie, the Tunstall code adds a phrase one at a time, while the Khodak code all at once. Nevertheless, one should expect similar results. Indeed, in the next theorem we present our findings for the Tunstall code.

Theorem 4.6. Let $\widetilde{D}_M$ denote the phrase length of the Tunstall code when the dictionary size is $M \geq 1$. Then for a biased source (i.e., when the probabilities p_i are not equal)

$$\frac{\widetilde{D}_M - \frac{1}{h}\log M}{\sqrt{\left(\frac{h_2}{h^3} - \frac{1}{h}\right)\log M}} \to N(0,1),$$

where $N(0,1)$ denotes the standard normal distribution, and

$$\begin{aligned} \mathbf{E}[\widetilde{D}_M] &= \frac{\log M}{h} + O(1), \\ \mathbf{Var}[\widetilde{D}_M] &\sim \left(\frac{h_2}{h^3} - \frac{1}{h}\right)\log M \end{aligned}$$

for $M \to \infty$.

Proof. We shall show that Theorem 4.6 can be deduced from Theorem 4.3. (The converse is obviously true.) This follows, informally, from the fact that Tunstall's code and Khodak's code are "almost equivalent" as discussed above.

Let's be more precise. Suppose that v is chosen in a way that there exists a word x with $P(x) = 1/v$. In particular the dictionary $\mathcal{D}_v$ contains all external nodes d that are adjacent to internals x with $P(x) = 1/v$. Now let $\widetilde{\mathcal{D}}_M$ be the dictionary (of size M) of any Tunstall code where only some of these internal nodes x with $P(x) = 1/v$ have been expanded. Then $\mathcal{D}_v$ is the Tunstall code where all nodes x with $P(x) = 1/v$ have been expanded. Hence, by this coupling of the dictionaries we certainly have for the dictionary lengths $|\widetilde{D}_M - D_v| \leq 1$. This also implies that $\mathbf{E}[\widetilde{D}_M] = \mathbf{E}[D_v] + O(1)$ and $\mathbf{Var}[\widetilde{D}_M - D_v] = O(1)$.

We observe that the central limit theorem is not affected by this variation. Since $\mathcal{D}_v$ satisfies a central limit theorem (see Theorem 4.3) we find

$$\frac{\widetilde{D}_M - \frac{1}{H}\log M}{\sqrt{\left(\frac{H_2}{H^3} - \frac{1}{H}\right)\log M}} \to N(0,1).$$

For the expected value and variance we have $\mathbf{E}[\widetilde{D}_M] = \frac{\log M}{H} + O(1)$ and

$$\mathbf{Var}[\widetilde{D}_M] \quad = \quad \mathbf{Var}[D_v] + O\left(\sqrt{\mathbf{Var}[D_v]}\right)$$

$$\sim \quad \left(\frac{H_2}{H^3} - \frac{1}{H}\right) \log M.$$

Indeed, more generally, let $Y_n = X_n + Z_n$ and we know that X_n satisfies a central limit theorem of the form

$$\frac{X_n - \mathbf{E}[X_n]}{\sqrt{\mathbf{Var}[X_n]}} \to N(0,1)$$

such that $\mathbf{Var}[X_n] \to \infty$ as well as $\mathbf{Var}[Z_n]/\mathbf{Var}[X_n] \to 0$ as $n \to \infty$. Then also Y_n satisfies a central limit theorem, i.e.

$$\frac{Y_n - \mathbf{E}[Y_n]}{\sqrt{\mathbf{Var}[Y_n]}} \to N(0,1),$$

and we have

$$\mathbf{Var}[Y_n] = \mathbf{Var}[X_n] + \mathbf{Var}[Z_n] + O(\sqrt{\mathbf{Var}[X_n]\mathbf{Var}[Z_n]}) \sim \mathbf{Var}[X_n]\cdot$$

which follows from Cauchy-Schwarz's inequality

$$\mathbf{E}[(X_n - \mathbf{E}[X_n])(Z_n - \mathbf{E}[Z_n])] \leq (\mathbf{Var}[X_n])^{1/2}(\mathbf{Var}[Z_n])^{1/2}.$$

This completes the proof of Theorem 4.6. □

Let us offer some final remarks. We already observed that the parsing trees for the Tunstall and Khodak algorithms are the same except when there is a “tie”. This situation can occur both, for the rational case and for the irrational case, and somewhat surprisingly leads to the cancelation of oscillation in the redundancy of the Khodak code for the rational case. As shown in [132] tiny oscillations remain in the Tunstall code redundancy for the rational case.

5

Redundancy of Divide-and-Conquer VF Arithmetic Coding

In this chapter, we consider again a variable-to-fixed code due to Boncelet [15] who used the *divide-and-conquer principle* to design a practical arithmetic encoding. Boncelet's algorithm is computationally fast and its practicality stems from the divide and conquer strategy to build a parsing tree: It splits the input (e.g., parsing tree) into several smaller subproblems, solving each subproblem separately, and then knitting together to solve the original problem. Other examples of divide-and-conquer design include heapsort, mergesort, discrete Fourier transform, queues, sorting networks, compression algorithms, and so forth [47, 86, 154].

We first describe in some details Boncelet's algorithm and present its redundancy analysis. To prove these results we need precise results about a *discrete* divide-and-conquer recurrence for some $T(n)$ which can be written as follows:

$$T(n) = a_n + \sum_{j=1}^{m} b_j T\left(\lfloor p_j n + \delta_j \rfloor\right) + \sum_{j=1}^{m} \overline{b}_j T\left(\left\lceil p_j n + \overline{\delta}_j \right\rceil\right) \qquad (5.1)$$

for some known sequence a_n and given $b_j, \overline{b}_j$, p_j and $\delta_j, \overline{\delta}_j$. The discrete nature of this recurrence (represented by the floor and ceiling functions) introduces certain oscillations not captured by traditional analysis (see

Akra and Bazzi [2] who primary studied the continuous version of the recurrence). In the second part of this chapter we present a rigorous and precise analysis of the discrete divide-and-conquer recurrence that goes beyond data compression. This chapter is based on [39].

5.1 Redundancy of Boncelet's Code

We now describe the Boncelet VF algorithm. To recall, a variable-to-fixed length encoder partitions the source string, say over a binary (or more generally over an m-ary) alphabet, into a concatenation of variable-length phrases. Each phrase belongs to a given dictionary $\mathcal{D}$ of source strings which constitutes a complete prefix free set. Such a uniquely parsable dictionary is represented by a *complete parsing tree*, i.e., a tree in which every internal node has all 2 (or more generally m) children nodes. The dictionary entries correspond to the *leaves* of the associated parsing tree. The encoder represents each parsed string by the fixed length binary code word corresponding to its dictionary entry by the code mapping $C : \mathcal{D} \to \{0,1\}^{\lceil \log_2 |\mathcal{D}| \rceil}$. Boncelet's algorithm, described next, is a practical algorithm to generate a parsing tree for a VF code, and therefore should be compared to the (asymptotically) optimal Tunstall and Khodak algorithms discussed in Chapter 4.

The main idea of Boncelet's VF code is to construct a parsing tree using a simple divide-and-conquer strategy. More precisely, let $n = |\mathcal{D}|$ denote the number of leaves in the corresponding parsing tree, hence also the size of the dictionary[1] We construct the parsing tree as follows: to build a tree with n leaves, we split n into $n = n_0 + n_1$ so that there are n_0 leaves in the left subtree and n_1 leaves in the right subtree. We accomplish it using a divide-and-conquer strategy, that is, we set

$$n_0 = \lfloor p_0 n + \delta \rfloor, \qquad n_1 = \lceil p_1 n - \delta \rceil$$

for some $\delta \in (0,1)$ (that satisfies $2p_0 + \delta < 2$, of course we assume that $p_0 + p_1 = 1$). Then the procedure is recursively applied until only 1 or 2 leaves are left. For example, if we are to build a tree with $n = 10$

[1] We should mention that in this chapter we use n to denote the number of leaves and the number of dictionary entries. Notice that in the previous chapters we used M for n which is more convenient in the context of divide-and-conquer recurrences.

leaves and $p_0 = 1/3$, we assure that there are $\lfloor 10/3 \rfloor = 3$ leaves in the left subtree and 7 in the right subtree. Recursively, 7 leaves of the root right subtree we split $7 = 2 + 5$ so that the left subtree of the root right subtree will end up with two leaves, the right subtree of the root right subtree will have 5 leaves, and so on. At the end we will build a complete pursing tree on 10 leaves.

Let $\mathcal{D} = \{v_1, \ldots v_n\}$ denote the set of phrases of the Boncelet code that are constructed in this way, that is, they correspond to the paths from the root to leaves of the Boncelet's parsing tree, and let $\ell(v_1), \ldots, \ell(v_n)$ be the corresponding phrase lengths. Clearly the probabilities p_0, p_1 induce a probability distribution $P(v_1), \ldots, P(v_n)$ on the leaves of the parsing tree and, thus, on the phrases. This fits naturally to a Bernoulli source with probabilities p_0, p_1 when the input string is partitioned according to $\mathcal{D}$. (We recall that we restrict the analysis to a binary alphabet.)

Our aim at is to understand the probabilistic behavior of the phrase length that we denote as D_n and the average redundancy. By definition the probability generating function of D_n is defined as

$$C(n, y) = \mathbf{E}[y^{D_n}] = \sum_{j=1}^{n} P(v_j) y^{\ell(v_j)}.$$

Boncelet's splitting procedure leads to the following recurrence on $C(n, y)$ for $n \geq 2$

$$C(n, y) = p_0\, y\, C\left(\lfloor p_0 n + \delta \rfloor, y\right) + p_1\, y\, C\left(\lceil p_1 n - \delta \rceil, y\right) \tag{5.2}$$

with initial conditions $C(0, y) = 0$ and $C(1, y) = 1$. We shall use this representation again in the last section of this chapter when we sketch a proof of a central limit law for the phrase length.

For now let us focus on the average phrase length and code redundancy. Let $\overline{D}_n$ denote the average phrase length

$$\overline{D}_n = \mathbf{E}[D_n] = \sum_{j=1}^{n} P(v_j)\, \ell(v_j)$$

which is also given by $\overline{D}_n = C'(n, 1)$ (where the derivative is taken with respect to y) and satisfies the recurrence

$$\overline{D}_n = 1 + p_0 \overline{D}_{\lfloor p_0 n + \delta \rfloor} + p_0 \overline{D}_{\lceil p_1 n - \delta \rceil} \tag{5.3}$$

with $\overline{D}_0 = \overline{D}_1 = 0$. This recurrence falls exactly under our divide and conquer recurrence (5.1).

We will discuss a more general recurrence in the next section where in Theorem 5.4 we give a general solution of (5.1), and in particular recurrence (5.3) discussed in Example 5.4 below. In Section 5.2 we present a sketch of the proof our our main result regarding the performance of the Boncelet algorithm.

Theorem 5.1. Consider a binary memoryless source with positive probabilities $p_0 = p$ and $p_1 = q$ and entropy $h = p\log(1/p) + q\log(1/q)$. Let $\overline{D}_n = \mathbf{E}[D_n]$ denote the expected phrase length of the binary Boncelet code with n phrases.
(i) If the ratio $(\log p)/(\log q)$ is irrational, then

$$\overline{D}_n = \frac{1}{h}\log n - \frac{\alpha}{h} + o(1), \tag{5.4}$$

where

$$\alpha = \widetilde{E}'(0) - \widetilde{G}'(0) - h - \frac{h_2}{2h}, \tag{5.5}$$

$h_2 = p\log^2 p + q\log^2 q$, and $\widetilde{E}'(0)$ and $\widetilde{G}'(0)$ are the derivatives at $s = 0$ of the Dirichlet series defined in (5.23) below.
(ii) If $(\log p)/(\log q)$ is rational, then

$$\overline{D}_n = \frac{1}{h}\log n - \frac{\alpha + \Psi(\log n)}{h} + O(n^{-\eta}), \tag{5.6}$$

where $\Psi(t)$ is a periodic function and $\eta > 0$.

Recall from Chapter 4 that for variable-to-fixed codes, the average (normalized) redundancy is expressed as

$$\overline{r}_n = \frac{\log n}{\mathbf{E}[D_n]} - h = \frac{\log n}{\overline{D}_n} - h$$

since every phrase of average length $\overline{D}_n$ requires $\log n$ bits to point to a dictionary entry. Our previous results imply immediately the following corollary.

Corollary 5.2. Let $\overline{r}_n$ denote the (normalized) average redundancy of the binary Boncelet code (with positive probabilities $p_0 = p$ and $p_1 = q$ and n phrases).

(i) If the ratio $(\log p)/(\log q)$ is irrational, then

$$\overline{r}_n = \frac{h\alpha}{\log n} + o\left(\frac{1}{\log n}\right) \tag{5.7}$$

with α defined in (5.5).
(ii) If $(\log p)/(\log q)$ is rational, then

$$\overline{r}_n = \frac{h(\alpha + \Psi(\log n))}{\log n} + o\left(\frac{1}{\log n}\right) \tag{5.8}$$

where $\Psi(t)$ is a periodic function.

Let us now compare the redundancy of Boncelet's algorithm to the asymptotically optimal Tunstall algorithm. From Corollary 4.4 we know that the redundancy of the Tunstall/Khodak code is[2]

$$\overline{r}_n^K = \frac{h}{\log n}\left(-\log(h\ln 2) - \frac{h_2 \ln 2}{2h}\right) + o\left(\frac{1}{\log n}\right)$$

(provided that $(\log p)/(\log q)$ is irrational; in the rational case there is also a periodic term in the leading asymptotics).

Example 5.1. Consider $p = 1/3$ and $q = 2/3$. Then the recurrence for $\overline{D}_n$ is precisely the same as that of Example 5.4 below. Consequently $\alpha \approx 0.0518$ while for the Tunstall code the corresponding constant in front of $h/\log n$ is equal to $-\log h - \frac{h_2}{2h} \approx 0.0496$.

It is also interesting to study the asymptotic behavior of the distribution of the phrase length D_n. Actually a precise analysis of the recurrence (5.2), proved in Section 5.3, leads to the following result.

Theorem 5.3. Consider a binary memoryless source with $p \neq q$. Then the phrase length distribution D_n of the corresponding Boncelet code with n phrases satisfies the central limit law, that is,

$$\frac{D_n - \frac{1}{h}\log n}{\sqrt{\left(\frac{h_2}{h^3} - \frac{1}{h}\right)\log n}} \to N(0,1),$$

where $N(0,1)$ denotes the standard normal distribution, and

$$\mathbf{E}[D_n] = \frac{\log n}{h} + O(1), \qquad \mathrm{Var}[D_n] \sim \left(\frac{h_2}{h^3} - \frac{1}{h}\right)\log n$$

for $n \to \infty$.

[2] Recall that we now write n for the dictionary size M.

5.2 Divide-and-Conquer Recurrence

To prove Theorem 5.1 we will rely quite heavily on a solution of the divide-and-conquer recurrence which we describe next in some generality. We shall assume that a problem of size n is split into m subproblems. It is natural to assume that there is a cost associated with combining subproblems together to find the solution. We denote such a cost by a_n. In addition, each subproblem may contribute in a different way to the final solution; we represent this by coefficients b_j and $\overline{b}_j$ for $1 \le j \le m$. Finally, we postulate that the original input n is divided into subproblems of size $\lfloor h_j(n) \rfloor$ and $\lceil \overline{h}_j(n) \rceil$, $1 \le j \le m$, where $h_j(x)$ and $\overline{h}_j(x)$ are functions that satisfy $h_j(x) \sim \overline{h}_j(x) \sim p_j x$ for $x \to \infty$ and for some $0 < p_j < 1$. We aim at presenting precise asymptotic solutions of *discrete* divide and conquer recurrences of the following form for $n \ge 2$

$$T(n) = a_n + \sum_{j=1}^{m} b_j T\left(\lfloor h_j(n) \rfloor\right) + \sum_{j=1}^{m} \overline{b}_j T\left(\left\lceil \overline{h}_j(n) \right\rceil\right). \tag{5.9}$$

A popular approach to solve this recurrence is to relax it to a *continuous* version of the following form (hereafter we assume $\overline{b}_j = 0$ for simplicity)

$$T(x) = a(x) + \sum_{j=1}^{m} b_j T(h_j(x)), \qquad x > 1, \tag{5.10}$$

where $h_j(x) \sim p_j x$ with $0 < p_j < 1$, and solve it using a Master Theorem of a divide-and-conquer recurrence. The most general solution of (5.10) is due to Akra and Bazzi [2] who proved (under certain regularity assumptions, namely that $a'(x)$ is of polynomial growth and that $h_j(x) - p_j x = O(x/(\log x)^2)$)

$$T(x) = \Theta\left(x^{s_0}\left(1 + \int_1^x \frac{a(u)}{u^{s_0+1}} du\right)\right),$$

where s_0 is a unique real root of

$$\sum_j b_j p_j^s = 1. \tag{5.11}$$

Actually this also leads directly to

$$T(n) = \Theta\left(n^{s_0}\left(1+\sum_{j=1}^{n}\frac{a_j}{j^{s_0+1}}\right)\right)$$

in the discrete version provided that $a_{n+1}-a_n$ is at most of polynomial growth.

Discrete versions of the divide and conquer recurrence, given by (5.9) are more subtle and require a different approach. We will use Dirichlet series [5] (closely related to the Mellin transform) that better captures the discrete nature of the recurrence, and then apply Tauberian theorems [94] (and also the Mellin-Perron formula presented in Theorem 5.5) to obtain asymptotics for $T(n)$. Precise results are presented in Theorem 5.4 for a particular case of sequences a_n of the form $a_n = Cn^a(\log n)^b$ (with $C > 0$ and $a, b \geq 0$). For more details see [39].

Theorem 5.4 (M. Drmota and W. Szpankowski, 2013)**.** Let $T(n)$ be the divide and conquer recurrence defined in (5.9) with $a_n = Cn^a(\log n)^b$ ($C > 0$, $a, b \geq 0$) such that:

(A1) b_j and $\overline{b}_j$ are non-negative with $b_j + \overline{b}_j > 0$,

(A2) $h_j(x)$ and $\overline{h}_j(x)$ are increasing and non-negative functions such that $h_j(x) = p_jx+O(x^{1-\delta})$ and $\overline{h}_j(x) = p_jx+O(x^{1-\delta})$ for positive $p_j < 1$ and $\delta > 0$, with $h_j(n) < n$ and $\overline{h}_j(n) \leq n-1$ for all $n \geq 2$.

Furthermore, let s_0 be the unique real solution of the equation

$$\sum_{j=1}^{m}(b_j+\overline{b}_j)p_j^{s_0} = 1. \tag{5.12}$$

Then the sequence $T(n)$ has the following asymptotic behavior:

(i) If $a > s_0$, then

$$T(n) = \begin{cases} C'n^a(\log n)^b + O\left(n^a(\log n)^{b-1}\right) & \text{if } b > 0, \\ C'n^a + O(n^{a-\delta'}) & \text{if } b = 0, \end{cases}$$

where $\delta' = \min\{a - s_0, \delta\}$ and

$$C' = \frac{C}{1-\sum_{j=1}^{m}(b_j+\overline{b}_j)p_j^a}.$$

(ii) If $a = s_0$, then

$$T(n) = C'' n^a (\log n)^{b+1} + O\left(n^a (\log n)^b\right)$$

with

$$C'' = \frac{C}{(b+1)\sum_{j=1}^{m}(b_j + \overline{b}_j) p_j^a \log(1/p_j)}.$$

(iii) If $a < s_0$ (or if we just assume that $a_n = O(n^a)$ for some $a < s_0$ as long as a_n is a non-negative and non-decreasing sequence), then for $\log p_1, \dots, \log p_m$ irrationally related (see Chapter 4)

$$T(n) \sim C''' n^{s_0},$$

where C''' is a positive constant. If $\log p_1, \dots, \log p_m$ are rationally related and if we also assume that (the so called *small growth property*)

$$T(n+1) - T(n) = O\left(n^{s_0 - \eta}\right) \tag{5.13}$$

holds for some $\eta > 1 - \delta$, then

$$T(n) = \Psi(\log n)\, n^{s_0} + O\left(n^{s_0 - \eta'}\right)$$

where $\Psi(t)$ is a positive and periodic continuous function with period L and $\eta' > 0$.

Remark 5.1. It should be remarked that the order of magnitude of $T(n)$ can be checked easily by the Akra-Bazzi theorem [2]. In particular, if we just know an upper bound for a_n which is of the form $a_n = O(n^a (\log n)^b)$ – even if a_n is not necessarily increasing – the Akra-Bazzi theorem provides an upper bound for $T(n)$ which is of form stated in Theorem 5.4. Hence the theorem can be easily adapted to cover a_n of the form

$$a_n = C n^a (\log n)^b + O((n^{a_1} (\log n)^{b_1})$$

with $a_1 < a$ or with $a_1 = a$ but $b_1 < b$. We split up the solution $T(n)$ into $T(n) = T_1(n) + T_2(n)$, where $T_1(n)$ corresponds to $a_n^{(1)} = C n^a (\log n)^b$, for which we can apply Theorem 5.4, and $T_2(n)$ corresponds to the error term $a_n^{(2)} = O((n^{a_1} (\log n)^{b_1})$, for which we apply the Akra-Bazzi theorem.

The same idea can be used for a bootstrapping procedure. Theorem 5.4 provides the asymptotic leading term for $T(n)$ that is (for example, in case (i)) of the form $C'n^a(\log n)^b$. Hence, by setting $T(n) = C'n^a(\log n)^b + S(n)$ we obtain a recurrence for $S(n)$ that is precisely of the form (5.9) with a new sequence a_n that is of smaller order than the previous one. At this step we can either apply Theorem 5.4 a second time or the Akra-Bazzi theorem.

Remark 5.2. Theorem 5.4 can be extended to the case

$$a_n = Cn^a(\log n)^b,$$

where $a > 0$ and b is an arbitrary real number. The same result holds with the only exception $a = s_0$ and $b = -1$. In this case we obtain

$$T(n) = C''n^a \log\log n + O\left(n^a(\log n)^{-1}\right)$$

with

$$C'' = \frac{C}{\sum_{j=1}^m b_j p_j^a \log(1/p_j)}.$$

Remark 5.3. The third case (iii): $a < s_0$, is of particular interest. Let us consider first the irrationally related case. Even in this case it is not immediate to describe the constant C''' explicitly. It depends heavily on a_n and also on $T(n)$ and can be written as (see [39])

$$C''' = \frac{\widetilde{A}(s_0) + \sum_{j=1}^m b_j(G_j(s_0) - E_j(s_0)) + \sum_{j=1}^m \overline{b}_j(\overline{G}_j(s_0) - \overline{E}_j(s_0))}{s_0 \sum_{j=1}^m (b_j + \overline{b}_j)p_j^{s_0} \log(1/p_j)} \tag{5.14}$$

with

$$\widetilde{A}(s) = \sum_{n=1}^{\infty} \frac{a_{n+2} - a_{n+1}}{n^s},$$

and

$$G_j(s) = \sum_{n<n_j(1)} \frac{T\left(\lfloor h_j(n+2)\rfloor\right) - T\left(\lfloor h_j(n+1)\rfloor\right)}{n^s} + \frac{T(2) - T\left(\lfloor h_j(n_j(1)+1)\rfloor\right)}{n_j(1)}, \tag{5.15}$$

$$E_j(s) = \sum_{k=1}^{\infty}(T(k+2) - T(k+1))\left(\frac{1}{(k/p_j)^s} - \frac{1}{n_j(k)^s}\right), \tag{5.16}$$

where $n_j(k) = \max\{n \geq 1 : h_j(n+1) < k+2\}$, and

$$\overline{G}_j(s) = \sum_{n<\overline{n}_j(1)} \frac{T\left(\left\lceil \overline{h}_j(n+2) \right\rceil\right) - T\left(\left\lceil \overline{h}_j(n+1) \right\rceil\right)}{n^s}$$

$$+ \frac{T(2) - T\left(\left\lceil \overline{h}_j(n_j(1)+1) \right\rceil\right)}{n_j(1)},$$

$$\overline{E}_j(s) = \sum_{k=1}^{\infty} (T(k+2) - T(k+1)) \left(\frac{1}{(k/p_j)^s} - \frac{1}{\overline{n}_j(k)^s} \right),$$

where $\overline{n}_j(k) = \min\{n \geq 1 : \overline{h}_j(n+2) > k+1\}$. We will show in the proof of Section 5.2.2 that the series $\widetilde{A}(s_0)$, $E_j(s_0)$ and $\overline{E}_j(s_0)$ actually converge. It should be also mentioned that there is no general error term in the asymptotic relation $T(n) \sim C''' n^{s_0}$.

In the rationally related case the periodic function $\Psi(t)$ has a convergent Fourier series $\Psi(t) = \sum_k c_k e^{2k\pi i x/L}$, where the Fourier coefficients are given by

$$c_k = \frac{\widetilde{A}(s_k) + \sum_{j=1}^m b_j (G_j(s_k) - E_j(s_k)) + \sum_{j=1}^m \overline{b}_j (\overline{G}_j(s_k) - \overline{E}_j(s_k))}{s_k \sum_{j=1}^m (b_j + \overline{b}_j) p_j^{s_0} \log(1/p_j)}, \tag{5.17}$$

where $s_k = s_0 + 2k\pi i/L$. In particular the constant coefficient c_0 equals C'''. Note that it cannot be deduced from this representation that the Fourier series is convergent. This makes the problem really subtle as discussed in details in [39].

We next present some applications of our main Theorem 5.4 before presenting a sketch of its proof.

5.2.1 Examples

We first illustrate our theorem on a few simple divide and conquer recurrences. Note that we only consider examples for the case (iii) and (ii), since they are more interesting.

Example 5.2. The recurrence

$$T(n) = T(\lfloor n/2 \rfloor) + 2T(\lceil n/2 \rceil) + n$$

is related to the Karatsuba algorithm [86]. Here we have

$$s_0 = \log(1/3)/\log(1/2) = 1.5849\ldots$$

and $s_0 > a = 1$. Furthermore, since $m = 1$, we are in the rationally related case. Here the small growth condition (5.13) is satisfied so that we can apply Theorem 5.4 to obtain

$$T(n) = \Psi(\log n)\, n^{\frac{\log 3}{\log 2}} \cdot (1 + o(1)) \qquad (n \to \infty)$$

with some continuous periodic function $\Psi(t)$.

In a similar manner, the Strassen algorithm [86] for matrix multiplications results in the following recurrence

$$T(n) = T(\lfloor n/2 \rfloor) + 6\, T(\lceil n/2 \rceil) + n^2.$$

Here we have $m = 1$, $s_0 = \log 7/\log 2 \approx 2.81$ and $a = 2$, and again we get an representation of the form

$$T(n) = \Psi(\log n)\, n^{\frac{\log 7}{\log 2}} \cdot (1 + o(1)) \qquad (n \to \infty)$$

with some periodic function $\Psi(t)$.

Example 5.3. The next two examples show that a small change in the recurrence might change the asymptotic behavior significantly. First let

$$T(n) = T(\lfloor n/2 \rfloor) + T(\lceil n/4 \rceil)$$

with $T(1) = 1$. Here we have $s_0 = \log((1+\sqrt{5})/2) \log 2 \approx 0.6942$ and we are in the rationally related case. Furthermore it follows easily that $T(n+1) - T(n) \le 1$. Hence the small growth condition (5.13) is satisfied and we obtain

$$T(n) \sim n^{s_0} \Psi(\log_2 n)$$

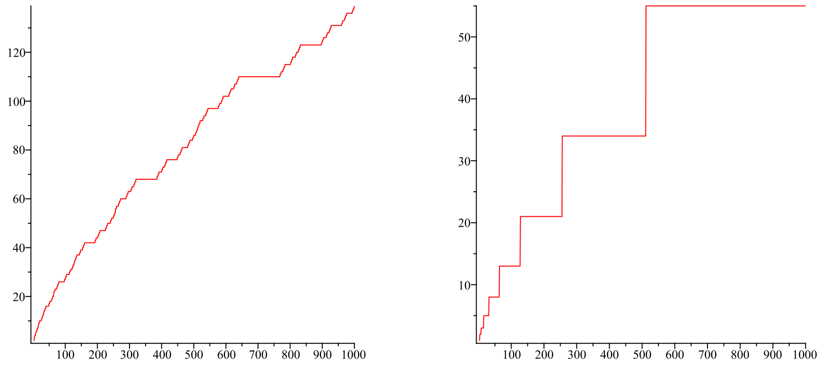
for a continuous periodic function $\Psi(t)$; see Figure 5.1(a).

However, if we just replace the appearing ceiling function by the floor function, that is,

$$\widetilde{T}(n) = \widetilde{T}(\lfloor n/2 \rfloor) + \widetilde{T}(\lfloor n/4 \rfloor) \qquad \text{for } n \ge 4$$

and $\widetilde{T}(1) = \widetilde{T}(2) = \widetilde{T}(3) = 1$, then the small growth condition (5.13) is not satisfied . We get $\widetilde{T}(n) = F_k$ for $2^{k-1} \le n < 2^k$, where F_k denotes the k-th Fibonacci number. This leads to

$$\widetilde{T}(n) \sim n^{s_0} \widetilde{\Psi}(\log_2 n),$$



(a) (b)

Figure 5.1: Illustration to Example 5.3: (a) recurrence $T(n) = T(\lfloor n/2 \rfloor) + T(\lceil n/4 \rceil)$, (b) recurrence $T(n) = T(\lfloor n/2 \rfloor) + T(\lfloor n/2 \rfloor)$.

where $\widetilde{\Psi}(t) = ((1+\sqrt{5})/2)^{1-\langle t \rangle}/\sqrt{5}$ is discontinuous for $t = 0$; see also Figure 5.1(b).

Example 5.4. Finally we consider a recurrence for the Boncelet's algorithm. Let

$$T(n) = \frac{1}{3}T\left(\left\lfloor \frac{n}{3} + \frac{1}{2} \right\rfloor\right) + \frac{2}{3}T\left(\left\lceil \frac{2n}{3} - \frac{1}{2} \right\rceil\right) + 1$$

with initial value $T(1) = 0$. Its asymptotic solution is given by

$$T(n) = \frac{1}{h}\log n + C + o(1),$$

with $h = \frac{1}{3}\log 3 + \frac{2}{3}\log\frac{3}{2} \approx 0.6365$ and some constant C. We can compute $C \approx -0.0813$. Its precise form is $C = -\alpha/h$, where

$$\begin{aligned}
\alpha &= \sum_{m\geq 1} \frac{T(m+2)-T(m+1)}{3}\left(\log\left\lceil 3m + \frac{5}{2}\right\rceil - \log(3m)\right) \\
&+ 2\sum_{m\geq 1} \frac{T(m+2)-T(m+1)}{3}\left(\log\left\lfloor \frac{3}{2}m + \frac{5}{4}\right\rfloor - \log(\frac{3m}{2})\right) \\
&+ \frac{\log 3}{3} - h - \frac{\frac{1}{3}\log^2 3 + \frac{2}{3}\log^2\frac{3}{2}}{2h} \approx 0.0518.
\end{aligned}$$

We have used this example for computing the redundancy of the binary Boncelet code with $p = 1/3$ in Example 5.1.

5.2.2 Sketch of Proof of Theorem 5.4

We present here only a part of the proof of Theorem 5.4. A complete detailed proof can be found in [39] to which we refer the interested reader.

Let us start with defining some appropriate Dirichlet series whose analysis will lead to asymptotic behavior of $T(n)$. We set

$$\widetilde{T}(s) = \sum_{n=1}^{\infty} \frac{T(n+2) - T(n+1)}{n^s},$$

provided the series is convergent. By partial summation and using a-priori upper bounds for the sequence $T(n)$, it follows that $\widetilde{T}(s)$ converges (absolutely) for $s \in \mathbb{C}$ with $\Re(s) > \max\{s_0, \sigma_a, 0\}$, where s_0 is the real solution of the equation (5.12), and σ_a is the abscissa of absolute convergence of $\widetilde{A}(s)$ defined as

$$\widetilde{A}(s) = \sum_{n=1}^{\infty} \frac{a_{n+2} - a_{n+1}}{n^s}. \tag{5.18}$$

To find a formula for $\widetilde{T}(s)$ we apply the recurrence relation (5.9). To simplify our presentation, we first assume that $\overline{b}_j = 0$, that is, we consider only the floor function on the right hand side of the recurrence (5.9); those parts that contain the ceiling function can be handled in the same way. We thus obtain

$$\widetilde{T}(s) = \widetilde{A}(s) + \sum_{j=1}^{m} b_j \sum_{n=1}^{\infty} \frac{T\left(\lfloor h_j(n+2) \rfloor\right) - T\left(\lfloor h_j(n+1) \rfloor\right)}{n^s}.$$

For $k \geq 1$ set

$$n_j(k) := \max\{n \geq 1 : h_j(n+1) < k+2\}.$$

By definition it is clear that $n_j(k+1) \geq n_j(k)$ and

$$n_j(k) = \frac{n}{p_j} + O\left(k^{1-\delta}\right). \tag{5.19}$$

Furthermore, by setting $G_j(s)$ we obtain

$$\sum_{n=1}^{\infty} \frac{T\left(\lfloor h_j(n+2)\rfloor\right) - T\left(\lfloor h_j(n+1)\rfloor\right)}{n^s}$$

$$= G_j(s) + \sum_{k=1}^{\infty} \frac{T(k+2) - T(k+1)}{n_j(k)^s}.$$

We now compare the last sum to $p_j^s \widetilde{T}(s)$:

$$\sum_{k=1}^{\infty} \frac{T(k+2) - T(k+1)}{n_j(k)^s} = \sum_{k=1}^{\infty} \frac{T(k+2) - T(k+1)}{(k/p_j)^s}$$

$$- \sum_{k=1}^{\infty} (T(k+2) - T(k+1)) \left(\frac{1}{(k/p_j)^s} - \frac{1}{n_j(k)^s} \right) = p_j^s \widetilde{T}(s) - E_j(s),$$

where $E_j(s)$ is

$$\begin{aligned} G_j(s) &= \sum_{n < n_j(1)} \frac{T\left(\lfloor h_j(n+2)\rfloor\right) - T\left(\lfloor h_j(n+1)\rfloor\right)}{n^s} \\ &\quad + \frac{T(2) - T\left(\lfloor h_j(n_j(1)+1)\rfloor\right)}{n_j(1)}, \qquad (5.20) \\ E_j(s) &= \sum_{k=1}^{\infty} (T(k+2) - T(k+1)) \left(\frac{1}{(k/p_j)^s} - \frac{1}{n_j(k)^s} \right). (5.21) \end{aligned}$$

Defining

$$E(s) = \sum_{j=1}^{m} b_j E_j(s) \quad \text{and} \quad G(s) = \sum_{j=1}^{m} b_j G_j(s)$$

we finally obtain the relation

$$\widetilde{T}(s) = \frac{\widetilde{A}(s) + G(s) - E(s)}{1 - \sum_{j=1}^{m} b_j \, p_j^s}. \qquad (5.22)$$

As mentioned above, (almost) the same procedure applies if some of the $\overline{b}_j$ are positive, that is, the ceiling function also appear in the recurrence equation. The only difference to (5.22) is that we arrive at a representation of the form

$$\widetilde{T}(s) = \frac{\widetilde{A}(s) + \widetilde{G}(s) - \widetilde{E}(s)}{1 - \sum_{j=1}^{m} (b_j + \overline{b}_j) \, p_j^s}, \qquad (5.23)$$

with a properly modified functions $\widetilde{G}(s)$ and $\widetilde{E}(s)$, however, they have the same analyticity properties as in (5.22).

For the asymptotic analysis we will only consider the irrational case for which we apply Tauberian theory (the analysis of the rational case is based on the Mellin-Perron formula and quite involved calculations; for details see [39]).

We recall that we have a representation (5.22) of the Dirichlet series $\widetilde{T}(s) = \sum_{n\ge 1}(T(n+2) - T(n+1))n^{-s}$, where $T(n+2) \ge T(n+1)$, and that we are interested in the asymptotic behavior of

$$T(n) = T(2) + \sum_{k=1}^{n-2}(T(k+2) - T(k+1)) \tag{5.24}$$

it is sufficient to get some information on the partial sums of the coefficient of the Dirichlet series $\widetilde{T}(s)$.

For the asymptotic analysis, we appeal to the Tauberian theorem by Wiener-Ikehara (see Theorem 5.6 below) and an analysis based on the Mellin-Perron formula which is presented next. Below we shall use Iverson's notation $[\![P]\!]$ which is 1 if P is a true proposition and 0 else.

Theorem 5.5 (see [5]). For a sequence $c(n)$ define the Dirichlet series

$$C(s) = \sum_{n=1}^{\infty} \frac{c(n)}{n^s}$$

and assume that the abscissa of absolute convergence σ_a is finite or $-\infty$. Then for all $\sigma > \sigma_a$ and all $x > 0$

$$\sum_{n<x} c(n) + \frac{c(\lfloor x \rfloor)}{2}[\![x \in \mathbb{Z}]\!] = \lim_{T\to\infty} \frac{1}{2\pi i}\int_{\sigma-iT}^{\sigma+iT} C(s)\frac{x^s}{s}\,ds \tag{5.25}$$

which is called the *Mellin-Perron formula.*

Now, by (5.25) and using (5.24) we find in our case

$$\begin{aligned} T(n) &= T(2) + \frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} \widetilde{T}(s)\frac{(n-\frac{3}{2})^s}{s}\,ds \qquad (5.26)\\ &= T(2) + \frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} \frac{\widetilde{A}(s) + \widetilde{G}(s) - \widetilde{E}(s)}{1 - \sum_{j=1}^{m}(b_j + \overline{b}_j)\,p_j^s}\frac{(n-\frac{3}{2})^s}{s}\,ds. \end{aligned}$$

Hence, the asymptotic behavior of $T(n)$ depends on the singular behavior of $\widetilde{A}(s)$, on the singularity at $s = 0$, and on the roots of the denominator in (5.23), that is, roots of the *characteristic equation*

$$\sum_{j=1}^{m} (b_j + \overline{b}_j)\, p_j^s = 1. \tag{5.27}$$

We denote by s_0 the unique real solution of this equation.

In summary, a master theorem for the divide-and-conquer recurrence has three major parts. In the first case the (asymptotic) behavior of a_n dominates the asymptotics of $T(n)$, in the second case, there is an *interaction* between the internal structure of the recurrence and the sequence a_n (resonance), and in the third case the behavior of the solution is driven by the recurrence and does not depend on a_n; see the three cases of Theorem 5.4. This also corresponds to an interplay between the poles $s = 0$, $s = \sigma_a$ and s_0 that determines the asymptotic behavior of the integral in (5.26) as illustrated in Figure 5.2. In fact, the pole of the largest value dictates asymptotics and determines the leading term. The oscillations will occur in the leading term in the rational case when s_0 is the dominant singularity since in this case singularities are placed periodically on the line $\Re(s) = s_0$ as shown in Figure 5.2.

Actually Dirichlet series and the partial sums of their coefficients are related via the Mellin transform. Suppose that

$$C(s) = \sum_{n \geq 1} c(n) n^{-s}$$

is a Dirichlet series and let

$$\overline{c}(v) = \sum_{n \leq v} c(n)$$

denote the partial sums of the coefficients $c(n)$. Then we have

$$C(s) = \sum_{n \geq 1} c(n) n^{-s} = s \int_1^\infty \overline{c}(v) v^{-s-1}\, dv.$$

Thus we can use Tauberian theorem like the Wiener-Ikehara theorem to recover the asymptotic behavior of $\overline{c}(v)$. We present here a general version of the Wiener-Ikehara theorem (see [39]) that is adapted to our situation.

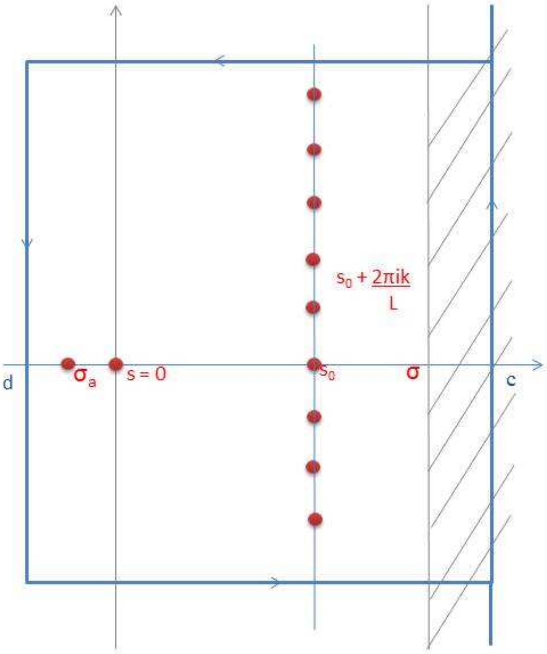


Figure 5.2: Illustration to the asymptotic analysis of the divide and conquer recurrence

Theorem 5.6. Let $\overline{c}(v)$ be non-negative and non-decreasing on $[1, \infty)$ such that transform

$$c^*(s) = \int_1^\infty \overline{c}(v) v^{-s-1}\, dv,$$

exists for $\Re(s) > s_0$ for some $s_0 \geq 0$ and suppose that there exist real constants $A_0, \ldots, A_K$ (with $A_K > 0$) such that

$$\widetilde{F}(s) = c^*(s) - \sum_{j=0}^{K} \frac{A_j}{(s - s_0)^{j+1}} \tag{5.28}$$

has a continuous extension to the closed half-plane $\Re(s) \geq s_0$. Then we have

$$\overline{c}(v) \sim \frac{A_K}{K!} (\log v)^K v^{s_0} \qquad (v \to \infty). \tag{5.29}$$

>From the representation (5.23) we observe that either $\widetilde{A}(s)$ or the factor $1/\left(1 - \sum_{j=1}^m b_j\, p_j^s\right)$ might be responsible for the abscissa of convergence of $\widetilde{T}(s)$. The functions $G(s)$ and $E(s)$ have an abscissa of

convergence that is smaller that that of $\widetilde{T}(s)$. Thus, we do not have to take care of them.

Let us suppose first that $a_n = O(n^a)$ for some $a < s_0$ which implies that the abscissa of convergence of $\widetilde{A}(s)$ is smaller than s_0. Thus $\widetilde{T}(s)$ has a simple polar singularity at $s = s_0$ that comes from the factor $1/\left(1 - \sum_{j=1}^{m} b_j\, p_j^s\right)$. Note that we have assumed that we are in the irrationally related case. Thus it follows from a direct extension of Lemma 4.5 that there is no other singularity on the line $\Re(s) = s_0$. Consequently the assumptions of Theorem 5.6 are satisfies (with $K = 0$) are it directly follows that

$$T(n) \sim C''' n^{s_0}$$

for some positive constant C'''. Note that we do not require the precise behavior of a_n. We just have to assume that a_n is non-decreasing and that $a_n = O(n^a)$ for some $a < s_0$.

However, if a_n is of larger order then the abscissa of convergence of $\widetilde{A}(s)$, then in order to apply Theorem 5.6 we need some information on the analytic behavior of $\widetilde{A}(s)$ if a_n is of the form $a_n = Cn^b(\log n)^b$ which is given in [39]) (see also [56]).

Theorem 5.7. Suppose that $a_n = n^a(\log n)^b$, where a and b are real numbers, and let $\widetilde{A}(s)$ be the Dirichlet series

$$\widetilde{A}(s) = \sum_{n\ge 1} \frac{a_{n+2} - a_{n+1}}{n^s}.$$

(i) If b is not a negative integer, then $\widetilde{A}(s)$ can be represented as

$$\widetilde{A}(s) = b\frac{\Gamma(b+1)}{(s-a)^{b+1}} + \frac{\Gamma(b+1)}{(s-a)^b} + G(s),$$

where $G(s)$ is analytic for $\Re(s) > a - 1$.
(ii) If $b = -k$ is a negative integer, then we have

$$\begin{aligned} \widetilde{A}(s) &= \sigma\frac{(-1)^k}{(k-1)!}(s-a)^{k-1}\log(s-a) \\ &+ \frac{k(-1)^k}{(k-1)!}(s-a)^k\log(s-a) + G(s), \end{aligned}$$

where $G(s)$ is analytic for $\Re(s) > a - 1$.

This theorem shows that $\widetilde{A}(s)$ is always of the form where the Tauberian theorem 5.6 is applicable. Actually the analytic behavior does not change if $\widetilde{A}(x)$ is multiplied by a function that is analytic at $s = a$. For example, if $a_n = Cn^a$ for some $a > s_0$. Then $\widetilde{A}(s)$ can be represented as

$$\widetilde{A}(s) = \frac{Ca}{(s-a)} + 1 + G(s),$$

where $G(s)$ is analytic for $\Re(s) > a - 1$. Consequently $\frac{1}{s}\widetilde{T}(s)$ can be represented as

$$\frac{1}{s}\widetilde{T}(s) = \frac{C'}{s-a} + H(s),$$

where $C' = C/\left(1 - \sum_{j=1}^{m}(b_j + \overline{b}_j)p_j^a\right)$ and $H(s)$ is analytic for $\Re(s) > \min(a-1, s_0)$. Hence, we can apply Theorem 5.6 and obtain

$$T(n) \sim C'n^a.$$

If $a_n = Cn^a(\log n)^b$ then we can argue in a similar way.

Finally the case $a = s_0$ needs some care since $\widetilde{A}(s)$ and the factor $1/\left(1 - \sum_{j=1}^{m} b_j\, p_j^s\right)$ contribute to the singular behavior of $\widetilde{T}(s)$ but even here we can apply Theorem 5.6 (in the irrationally related case).

5.3 Central Limit Law for Boncelet's Algorithms

We next provide a sketch of the proof of the the central limit theorem for the phrase length D_n of the Boncelet algorithm that is stated in Theorem 5.3. Again we only consider the irrationally related case for a binary alphabet.

To deal with $C(n, y)$, we consider the Dirichlet series

$$C(s, y) = \sum_{n=1}^{\infty} \frac{C(n+2, y) - C(n+1, y)}{n^s}.$$

For simplicity we just consider here the case $y > 1$. (The case $y \le 1$ can be handled in a similar way.) Then $C(s, y)$ converges for $\Re(s) > s_0(y)$, where $s_0(y)$ denotes the real zero of the equation (for a binary alphabet)

$$y(p^{s+1} + q^{s+1}) = 1$$

discussed in Lemma 4.5. We find

$$C(s,y) = \frac{(y-1) - \widetilde{E}(s,y)}{1 - y(p^{s+1} + q^{s+1})},$$

where

$$\widetilde{E}(s,y) = py\sum_{k=1}^{\infty}(C(k{+}2,y)){-}C(k{+}1,y))\left(\frac{1}{(k/p)^s} - \frac{1}{\left(\left\lceil\frac{k+2-\delta}{p}\right\rceil - 2\right)^s}\right)$$

$$+qy\sum_{k=1}^{\infty}(C(k+2,y)) - C(k+1,y))\left(\frac{1}{(k/q)^s} - \frac{1}{\left(\left\lfloor\frac{k+1+\delta}{q}\right\rfloor - 1\right)^s}\right)$$

converges for $\Re(s) > s_0(y) - 1$ and satisfies $\widetilde{E}(0,y) = 0$ and $\widetilde{E}(s,1) = 0$.

Then by the Wiener-Ikehara theorem only the residue at $s_0(y)$ contributes to the main asymptotic leading term. (Recall that we consider the case $y > 1$). We thus have

$$\begin{aligned} C(n,y) &\sim \operatorname{Res}\left(\frac{((y-1) - \widetilde{E}(s,y))(n-3/2)^s}{s(1 - y(p^{s+1} + q^{s+1}))}; s = s_0(y)\right) \\ &= \frac{((y-1) - \widetilde{E}(s_0(y),y))(n-3/2)^{s_0(y)}}{-s_0(y)(\log(p)p^{s_0(y)+1} + \log(q)q^{s_0(y)+1}))}(1 + o(1)). \end{aligned}$$

The essential but non-trivial observation is that this asymptotic relation holds uniform for y in an interval around 1. Let us assume that this uniformity holds. Then we are precisely in the same situation as in the case of the Tunstall code (see Chapter 4) and we obtain a central limit theorem.

In order to make the uniformity in y we have to use the Mellin-Perron formula (which is a proper reformulation of the inverse Mellin transform) and do the asymptotic treatment directly on this level. It turns out that we have to distinguish between the rationally related case and the irrationally related case which makes the analysis even more subtle (for details see [39]).

6

Redundancy of VV Khodak Codes

In the last three chapters, we discussed fixed-to-variables FV codes such as Shannon and Huffman codes (see Chapter 3), and variable-to-fixed VF codes such as Tunstall, Khodak, and Boncelet codes (see Chapters 4 and 5). We show in Theorems 3.1 and 3.5 that the *normalized* redundancy is inversely proportional to the block length n, which represents a delay and in this chapter we will denote it as $\overline{D}$. Thus for FV codes $\overline{r} = \Theta(\overline{D}^{-1})$. In Theorems 4.3 and 4.6, we analyzed Khodak and Tunstall VF codes and proved that the average redundancy (see in particular Corollary 4.4) decays like $\Theta(1/\mathbf{E}[D_v])$, where $\mathbf{E}[D_v]$ is the average phrase length that we again denote in this chapter as $\overline{D} := \mathbf{E}[D]$. In summary, for both FV and VF codes the normalized redundancy (rate) $\overline{r}$ decays inversely proportional to the average phrase length or delay $\overline{D}$.

However, it is an intriguing question whether one can construct a code with $\overline{r} = o(1/\overline{D})$. This quest was accomplished by Khodak [80] in 1972, who proved that one can find a variable-to-variable VV code with $\overline{r} = O(\overline{D}^{-5/3})$. The proof presented in [80] is rather sketchy and complicated. Here we present a transparent proof and an *explicit algorithm* to achieve this bound. We also will show that the *maximal* redundancy becomes $O(\overline{D}^{-4/3})$. Finally, in a major extension of Khodak's results we present stronger results for *almost all* sources. This chapter is based on [16].

6.1 Variable-to-Variable Codes and Redundancy Rate

Recall that a variable-to-variable (VV) length code partitions a source sequence into variable length phrases that are encoded into strings of variable lengths. While it is well known that every VV (prefix) code is a concatenation of a variable-to-fixed length code (e.g., Tunstall code) and a fixed-to-variable length encoding (e.g., Huffman code), an optimal VV code for a given dictionary size has not yet been found. Fabris [42] proved that greedy, step by step, optimization (that is, a concatenation of Tunstall and Huffman codes) does not lead to an optimal VV code.

Let us first briefly describe a VV encoder. A VV encoder has two components, a *parser* and a *string encoder*. The parser partitions the source sequence x into phrases from a predetermined dictionary $\mathcal{D}$. We shall write d or d_i for a dictionary entry, and by $\overline{D}$ we denote the average dictionary (phrase) length also known as the average delay. As argued in previous chapters, a convenient way of representing the dictionary $\mathcal{D}$ is by a complete tree also know as the *parsing tree*. Next, the string encoder in a VV scheme maps each dictionary phrase into its corresponding binary codeword $C(d)$ of length $|C(d)| = \ell(d)$. Throughout this chapter, we assume that the string encoder is a slightly modified Shannon code[1] and we concentrate on building a parsing tree for which $-\log P(d)$ $(d \in \mathcal{D})$ is close to an integer. This allows us to construct a VV code with redundancy rates (per symbol) approaching zero as the average delay increases.

In (4.2) of Chapter 4 we define the average redundancy rate as

$$\overline{r} \;=\; \frac{\sum_{d\in\mathcal{D}} P(d)\ell(d) - h_{\mathcal{D}}}{\mathbf{E}[D]} = \frac{\sum_{d\in\mathcal{D}} P(d)(\ell(d) + \log P(d))}{\mathbf{E}[D]}, \qquad (6.1)$$

[1] A variant of Shannon code that is used here assigns to $d \in \mathcal{D}$ a binary word of length $\ell(d)$ close to $-\log P(d)$ when $\log P(d)$ is slightly larger or smaller than an integer. Naturally, Kraft's inequality will not be automatically satisfied but this is handled in Lemma 6.4.

where P is the probability law of the dictionary phrases and $\mathbf{E}[D] = \sum_{d\in\mathcal{D}} |d|P(d) =: \overline{D}$. By analogy we define the *maximal* redundancy rate r^* for VV codes as follows

$$r^* = \frac{\max_{d\in\mathcal{D}}[\ell(d) + \log P(d)]}{\overline{D}}. \tag{6.2}$$

In this chapter we shall study both, the average redundancy rate and the maximal redundancy rate for VV codes.

6.2 Redundancy of the Khodak VV Code

In this section we present our main results regarding the average and maximal redundancy rates for a VV Khodak code. We also construct an explicit algorithm to achieve these bound.

We start with our main theorem of this section.

Theorem 6.1. Let $m \geq 2$ and $\mathcal{S}$ be a memoryless source over an m-ary alphabet. Then for every $D_0 \geq 1$, there exists a VV code with average dictionary length $\mathbf{E}[D] =: \overline{D} \geq D_0$ such that its average redundancy rate satisfies

$$\overline{r} = O(\overline{D}^{-5/3}), \tag{6.3}$$

and the maximal code length is $O(\overline{D}\log\overline{D})$.

The rest of this section is devoted to present a proof of Theorem 6.1. We assume an m-ary source alphabet $\mathcal{X} = \{0,\dots,m-1\}$ with probability of symbols $p_0,\dots,p_{m-1}$. Let us first give some intuition. For every $d \in \mathcal{D}$, we can represent $P(d)$ as $P(d) = p_0^{k_0}\cdots p_{m-1}^{k_{m-1}}$, where $k_i = k_i(d)$ is the number of times symbol i appears in d. In what follows we write $\text{type}(d) = (k_0, k_1, \dots, k_{m-1})$ for all strings with the same probability $P(d) = p_0^{k_0}\cdots p_{m-1}^{k_{m-1}}$. Furthermore, the string encoder of our VV code uses a slightly modified Shannon code that assigns to $d \in \mathcal{D}$ a binary word of length $\ell(d)$ close to $-\log P(d)$ when $\log P(d)$ is slightly larger or smaller than an integer. (Kraft's inequality will not be automatically satisfied but Lemma 6.4 below takes care of it.) Observe that the average redundancy of the Shannon code is (see Chapter 3)

$$\sum_{d\in\mathcal{D}} P(d)[\lceil -\log P(d)\rceil + \log P(d)] = \sum_{d\in\mathcal{D}} P(d)\langle \log P(d)\rangle$$

$$= \sum_{d\in\mathcal{D}} P(d) \cdot \langle k_0(d)\gamma_0 + k_1(d)\gamma_1 + \cdots + k_{m-1}(d)\gamma_{m-1}\rangle$$

where $\gamma_i = \log p_i$. In order to build a VV code with $\overline{r} = o(1/\overline{D})$, we are to find integers $k_0 = k_0(d), \ldots k_{m-1} = k_{m-1}(d)$ such that the linear form $k_0\gamma_0 + k_1\gamma_1 + \cdots + k_{m-1}\gamma_{m-1}$ is close to but slightly larger than an integer. In the sequel, we discuss some properties of the distribution of $\langle k_0\gamma_0 + k_1\gamma_1 + \cdots + k_{m-1}\gamma_{m-1}\rangle$ when at least one of γ_i is irrational (see [40]).

We need some additional concepts and preliminary results that we discuss next. Let $\|x\| = \min(\langle x\rangle, \langle -x\rangle) = \min(\langle x\rangle, 1 - \langle x\rangle)$ be the distance to the nearest integer. The *dispersion* $\delta(X)$ of the set $X \subseteq [0, 1)$ is defined as

$$\delta(X) = \sup_{0\le y<1} \inf_{x\in X} \|y - x\|,$$

that is, for every $y \in [0, 1)$, there exists $x \in X$ with $\|y - x\| \le \delta(X)$. Since $\|y+1\| = \|y\|$, the same assertion holds for all real y. Dispersion tells us that points of X are at most $2\delta(X)$ apart in $[0, 1]$. Therefore, there exist distinct points $x_1, x_2 \in X$ with $\langle y - x_1\rangle \le 2\delta(X)$ and $\langle y - x_2\rangle \le 2\delta(X)$.

The following property will be used throughout this chapter. This is a standard result following from Dirichlet's approximation theorem which proof can be found in [40].

Lemma 6.2. (i) Suppose that θ is an irrational number. Then there exist infinitely many integers N such that

$$\delta\left(\{\langle k\theta\rangle : 0 \le k < N\}\right) \le \frac{2}{N}.$$

(ii) In general, let $(\gamma_0, \ldots, \gamma_{m-1})$ be an m-vector of real numbers such that at least one of its coordinates is irrational. Then there exist infinitely many integers N such that the dispersion of the set

$$X = \{\langle k_0\gamma + \cdots + k_{m-1}\gamma_{m-1}\rangle : 0 \le k_j < N \ (0 \le j < m)\}$$

is bounded by

$$\delta(X) \le \frac{2}{N}.$$

The central step of all existence results is the observation that a bound on the dispersion of linear forms of $\log p_j$ implies the existence of a VV code with small redundancy. Indeed, Theorem 6.1 follows directly from the following lemma.

Lemma 6.3. Let $p_j > 0$ $(0 \le j < m)$ with $p_0 + \cdots + p_{m-1} = 1$ be given and suppose that for some $N \ge 1$ and $\eta \ge 1$ the set

$$X = \{\langle k_0 \log p_0 + \cdots + k_{m-1} \log p_{m-1}\rangle : 0 \le k_j < N \ (0 \le j < m)\},$$

has dispersion

$$\delta(X) \le \frac{2}{N^\eta}. \tag{6.4}$$

Then there exists a VV code with average phrase length $\overline{D} = \Theta(N^3)$, with maximal length of order $\Theta(N^3 \log N)$, and with average redundancy rate

$$\overline{r} \le c_m \cdot \overline{D}^{-\frac{4+\eta}{3}}$$

where c_m is a constant that may depend on m.

Clearly, Lemma 6.2 and Lemma 6.3 directly imply Theorem 6.1 by setting $\eta = 1$ if one of the $\log p_j$ is irrational. (If all $\log p_j$ are rational, then the construction is even simpler.)

We now concentrate on proving Lemma 6.3. The main thrust of the proof is to construct a complete prefix free set $\mathcal{D}$ of words (i.e., a dictionary) on m symbols such that $\log P(d)$ is *very close* to an integer $\ell(d)$ with high probability. This is accomplished by growing an m-ary tree $\mathcal{T}$ in which paths from the root to terminal nodes have $\log P(d)$ close to an integer.

In the first step, we set $k_i^0 := \lfloor p_i N^2 \rfloor$ $(0 \le i < m)$ and define

$$x = k_0^0 \log p_0 + \cdots + k_{m-1}^0 \log p_{m-1}.$$

By our assumption (6.4) of Lemma 6.3, there exist integers $0 \le k_j^1 < N$ such that

$$\left\langle x + k_0^1 \log p_0 + \cdots + k_{m-1}^1 \log p_{m-1} \right\rangle =$$

$$\left\langle (k_0^0 + k_0^1) \log p_0 + \cdots + (k_{m-1}^0 + k_{m-1}^1) \log p_{m-1} \right\rangle < \frac{4}{N^\eta}.$$

Now consider all paths in a (potentially) infinite m-ary tree starting at the root with $k_0^0 + k_0^1$ edges of type 0, $k_1^0 + k_1^1$ edges of type 1,…, and $k_{m-1}^0 + k_{m-1}^1$ edges of type $m-1$ (cf. Figure 6.1). Let $\mathcal{D}_1$ denote the set of such words. (These are the first words of our prefix free dictionary set we are going to construct.) By an application of Stirling's formula it follows that there are two positive constants c', c'' such that the probability

$$P(\mathcal{D}_1) = \binom{(k_0^0 + k_0^1) + \cdots + (k_m^0 + k_m^1)}{k_0^0 + k_0^1, \ldots, k_{m-1}^0 + k_{m-1}^1} p_0^{k_0^0 + k_0^1} \cdots p_{m-1}^{k_{m-1}^0 + k_{m-1}^1}$$

satisfies

$$\frac{c'}{N} \le P(\mathcal{D}_1) = \le \frac{c''}{N} \tag{6.5}$$

uniformly for all k_j^1 with $0 \le k_j^1 < N$. In summary, by construction all words $d \in \mathcal{D}_1$ have the property that

$$\langle \log P(d) \rangle < \frac{4}{N^\eta},$$

that is, $\log P(d)$ is very close to an integer. Note further that all words in $d \in \mathcal{D}_1$ have about the same length

$$n_1 = (k_0^0 + k_0') + \cdots + (k_{m-1}^0 + k_{m-1}') = N^2 + O(N),$$

and words in $\mathcal{D}_1$ constitute the first crop of "good words". Finally, let $\mathcal{B}_1 = \mathcal{X}^{n_1} \setminus \mathcal{D}_1$ denote all words of length n_1 not in $\mathcal{D}_1$ (cf. Figure 6.1). Then

$$1 - \frac{c''}{N} \le P(\mathcal{B}_1) \le 1 - \frac{c'}{N}.$$

In the second step, we consider all words $r \in \mathcal{B}_1$ and concatenate them with appropriately chosen words d_2 of length $\sim N^2$ such that $\log_2 P(rd_2)$ is close to an integer *with high probability.* The construction is almost the same as in the first step. For every word $r \in \mathcal{B}_1$ we set

$$x(r) = \log_2 P(r) + k_0^0 \log p_0 + \cdots + k_{m-1}^0 \log p_{m-1}.$$

By (6.4) there exist integers $0 \le k_j^2(r) < N$ $(0 \le j < m)$ such that

$$\left\langle x(r) + k_0^2(r) \log p_0 + \cdots + k_{m-1}^2(r) \log p_{m-1} \right\rangle < \frac{4}{N^\eta}.$$

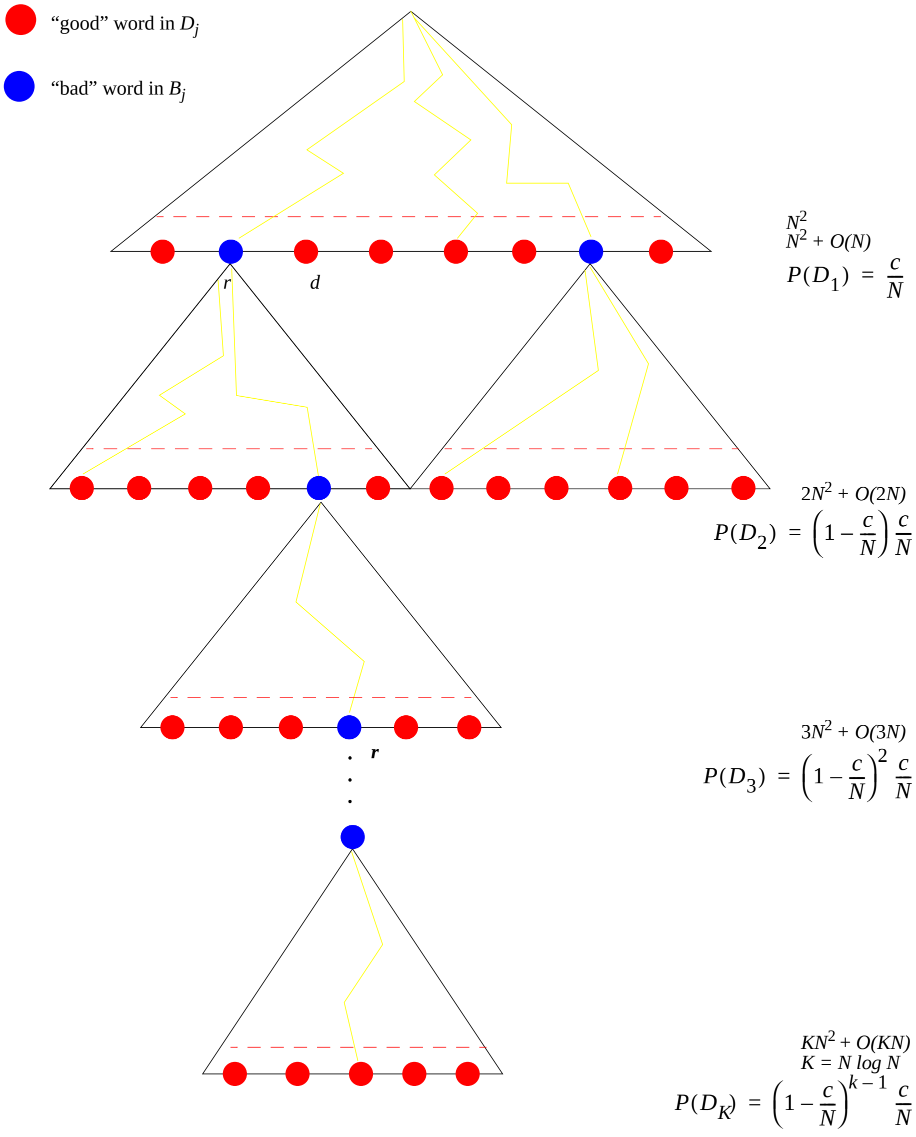

● "good" word in D_j
● "bad" word in B_j
r
d
N^2
$N^2 + O(N)$
$P(D_1) = \frac{c}{N}$
$2N^2 + O(2N)$
$P(D_2) = \left(1-\frac{c}{N}\right)\frac{c}{N}$
r
$3N^2 + O(3N)$
$P(D_3) = \left(1-\frac{c}{N}\right)^2\frac{c}{N}$
$KN^2 + O(KN)$
$K = N \log N$
$P(D_K) = \left(1-\frac{c}{N}\right)^{k-1}\frac{c}{N}$

Figure 6.1: Illustration to the construction of the VV code.

Now consider all paths (in the infinite tree $\mathcal{T}$) starting at $r \in \mathcal{B}_1$ with $k_0^0 + k_0^2(r)$ edges of type 0, $k_1^0 + k_1^2(r)$ edges of type 1, …, and $k_{m-1}^0 + k_{m-1}^2(r)$ edges of type $m-1$ (that is, we concatenated r with properly chosen words d_2) and denote this set by $\mathcal{D}_2^+(r)$. We again have that the total probability

$$P(\mathcal{D}_2(r)) = P(r) \cdot$$
$$\binom{(k_0^0 + k_0^2(r)) + \cdots + (k_{m-1}^0 + k_{m-1}^2(r))}{k_0^0 + k_0^2(r), \ldots, k_{m-1}^0 + k_{m-1}^2(r)} p_0^{k_0^0 + k_0^2(r)} \cdots p_{m-1}^{k_{m-1}^0 + k_{m-1}^2(r)}$$

of these words is bounded from below and above by

$$P(r)\frac{c'}{N} \le P(\mathcal{D}_2(r)) \le P(r)\frac{c''}{N}.$$

Furthermore, by construction we have $\langle \log_2 P(d) \rangle < \frac{4}{N^\eta}$ for all $d \in \mathcal{D}_2^+(r)$.

Similarly, we can construct a set $\mathcal{D}_2^-(r)$ instead of $\mathcal{D}_2^+(r)$ for which we have $1 - \langle \log_2 P(d) \rangle < 4/N^\eta$. We will indicate in the sequel whether we will use $\mathcal{D}_2^+(r)$ or $\mathcal{D}_2^-(r)$.

Let $\mathcal{D}_2 = \bigcup(\mathcal{D}_2^+(r) : r \in \mathcal{B}_1)$ (or $\mathcal{D}_2 = \bigcup(\mathcal{D}_2^-(r) : r \in \mathcal{B}_1)$). Then all words $d \in \mathcal{D}_2$ have almost the same length $|d| = 2N^2 + O(2N)$, their probabilities satisfy

$$\langle \log P(d) \rangle < \frac{4}{N^\eta} \quad \text{or} \quad 1 - \langle \log P(d) \rangle < \frac{4}{N^\eta}$$

and the total probability is bounded by

$$\frac{c'}{N}\left(1 - \frac{c''}{N}\right) \le P(\mathcal{D}_2) \le \frac{c''}{N}\left(1 - \frac{c'}{N}\right).$$

For every $r \in \mathcal{B}_1$, let $\mathcal{B}^+(r)$ (or $\mathcal{B}^-(r)$) denote the set of paths (resp. words) starting with r of length $2(k_0^0 + \cdots + k_{m-1}^0) + (k_1^1 + k_1^2(r) + \cdots + k_{m-1}^1 + k_{m-1}^2(r))$ that are *not* contained in $\mathcal{D}_2^+(r)$ (or $\mathcal{D}_2^-(r)$) and set $\mathcal{B}_2 = \bigcup(\mathcal{B}_2^+(r) : r \in \mathcal{B}_1)$ (or $\mathcal{B}_2 = \bigcup(\mathcal{B}_2^-(r) : r \in \mathcal{B}_1)$). Observe that the probability of $\mathcal{B}_2$ is bounded by

$$\left(1 - \frac{c''}{N}\right)^2 \le P(\mathcal{B}_2) \le \left(1 - \frac{c'}{N}\right)^2.$$

We continue this construction, as illustrated in Figure 6.1, and in step j we define sets of words $\mathcal{D}_j$ and $\mathcal{B}_j$ such that all words $d \in \mathcal{D}_j$

satisfy

$$\langle \log P(d) \rangle < \frac{4}{N^\eta} \quad \text{or} \quad 1 - \langle \log P(d) \rangle < \frac{4}{N^\eta}$$

and the length of $d \in \mathcal{D}_j \cup \mathcal{B}_j$ is then given by $|d| = jN^2 + \mathcal{O}(jN)$. The probabilities of $\mathcal{D}_j$ and $\mathcal{B}_j$ are bounded by

$$\frac{c'}{N}\left(1 - \frac{c''}{N}\right)^{j-1} \le P(\mathcal{D}_j) \le \frac{c''}{N}\left(1 - \frac{c'}{N}\right)^{j-1},$$

and

$$\left(1 - \frac{c''}{N}\right)^{j} \le P(\mathcal{B}_j) \le \left(1 - \frac{c'}{N}\right)^{j}.$$

This construction is terminated after $K = O(N \log N)$ steps so that

$$P(\mathcal{B}_K) \le c''\left(1 - \frac{c'}{N}\right)^{K} \le \frac{1}{N^\beta}$$

for some $\beta > 0$. This also ensures that

$$P(\mathcal{D}_1 \cup \cdots \cup \mathcal{D}_K) > 1 - \frac{1}{N^\beta}.$$

The complete prefix free set $\mathcal{D}$ on the m symbols is given by

$$\mathcal{D} = \mathcal{D}_1 \cup \cdots \cup \mathcal{D}_K \cup \mathcal{B}_K.$$

By the above construction, it is also clear that the average dictionary phrase length is bounded by

$$c_1 N^3 \le \overline{D} = \sum_{d \in \mathcal{D}} P(d)\,|d| \le c_2 N^3$$

for certain constants $c_1, c_2 > 0$. Notice further that the maximal code length satisfies

$$\max_{d \in \mathcal{D}} |d| = O(N^3 \log N) = O(\overline{D} \log \overline{D}).$$

Now we construct a variant of the Shannon code with $\overline{r} = o(1/\overline{D})$. For every $d \in \mathcal{D}_1 \cup \cdots \cup \mathcal{D}_K$ we can choose a non-negative integer $\ell(d)$ with

$$|\ell(d) + \log P(d)| < \frac{2}{N^\eta}.$$

In particular, we have

$$0 \le \ell(d) + \log P(d) < \frac{2}{N^\eta}$$

if $\langle \log P(d) \rangle < 2/N^\eta$ and

$$-\frac{2}{N^\eta} < \ell(d) + \log P(d) \le 0$$

if $1 - \langle \log P(d) \rangle < 2/N^\eta$. For $d \in \mathcal{B}_K$ we simply set $\ell(d) = \lceil -\log P(d) \rceil$. The final problem is now to *adjust* the choices of "+" resp. "−" in the above construction so that Kraft's inequality is satisfied. For this purpose we use the following easy property (that we adopt from Khodak [80]).

Lemma 6.4 (Khodak, 1972). Let $\mathcal{D}$ be a finite set with probability distribution P and suppose that for every $d \in \mathcal{D}$ we have $|\ell(d) + \log_2 P(d)| \le 1$ for a nonnegative integer $\ell(d)$. If

$$\sum_{d\in\mathcal{D}} P(d)(\ell(d) + \log P(d)) \ge 2 \sum_{d\in\mathcal{D}} P(d)(\ell(d) + \log P(d))^2, \qquad (6.6)$$

then there exists an injective mapping $C : \mathcal{D} \to \{0,1\}^*$ such that C is a prefix free set and $|C(d)| = \ell(d)$ for all $d \in \mathcal{D}$.

Proof. We use the local expansion $2^{-x} = 1 - x \ln 2 + \eta(x)$ for $|x| \le 1$, where $((\log 4)/4)x^2 \le \eta(x) \le (\log 4)x^2$. Hence

$$\begin{aligned}
\sum_{d\in\mathcal{D}} 2^{-\ell(d)} &= \sum_{d\in\mathcal{D}|} P(d) 2^{-(\ell(d)+\log_2 P(d))} \\
&= 1 - \ln 2 \sum_{d\in\mathcal{D}} P(d)(\ell(d) + \log P(d)) \\
&\quad + \sum_{d\in\mathcal{D}} P(d)\eta\left(\ell(d) + \log P(d)\right) \\
&\le 1 - \ln 2 \sum_{d\in\mathcal{D}} P(d)(\ell(d) + \log P(d)) \\
&\quad +2 \ln 2 \sum_{d\in\mathcal{D}} P(d)(\ell(d) + \log P(d))^2 \\
&\overset{(6.6)}{\le} 1
\end{aligned}$$

If (6.6) is satisfied, then Kraft's inequality follows, and there exists an injective mapping $C : \mathcal{D} \to \{0,1\}^*$ such that C is a prefix free set and $|C(d)| = \ell(d)$ for all $d \in \mathcal{D}$. □

We set

$$E_j = \sum_{d \in \mathcal{D}_j} P(d)(\ell(d) + \log P(d)).$$

Then $E_j > 0$ if we have chosen "+" in the above construction and $E_j < 0$ if we have chosen "−". In any case we have

$$|E_j| \le P(\mathcal{D}_j)\frac{2}{N^\eta} \le \frac{2c''}{N^{1+\eta}}\left(1 - \frac{c'}{N}\right)^{j-1} \le \frac{2c''}{N^{1+\eta}}.$$

Suppose for a moment that we have always chosen "+", that is $E_j > 0$ for all $j \ge 1$, and that

$$\sum_{j=1}^{K} E_j \le \frac{8 + 2c''}{N^{1+\eta}}. \tag{6.7}$$

We can assume that N is large enough that $2/N^\eta \le 1/2$. Hence, the assumptions of Lemma 6.4 are trivially satisfied since $0 \le \ell(d) + \log_2 P(d) < 1/2$ implies $2(\ell(d) + \log_2 P(d))^2 < \ell(d) + \log_2 P(d)$ for all $d \in \mathcal{D}$. If (6.7) does not hold (if we have chosen always "+"), then one can select "+" and "−" so that

$$\frac{8}{N^{1+\eta}} \le \sum_{j=1}^{K} E_j \le \frac{8 + 4c''}{N^{1+\eta}}.$$

Indeed, if the partial sum $\sum_{j=i}^{K} E_i \le (8 + 2c'')N^{-1-\eta}$, then the sign of E_j is chosen to be "+" and if $\sum_{j=i}^{K} E_i > (8 + 2c'')N^{-1-\eta}$ then the sign of E_j is chosen to be "−". Since

$$\sum_{d \in \mathcal{D}} P(d)(\ell(d) + \log_2 P(d))^2 \le \frac{4}{N^{2\eta}} \le \frac{4}{N^{1+\eta}} \le \sum_{d \in \mathcal{D}} P(d)(\ell(d) + \log_2 P(d))$$

the assumption of Lemma 6.4 is satisfied. Thus, there exists a prefix free coding map $C : \mathcal{D} \to \{0,1\}^*$ with $|C(d)| = \ell(d)$ for all $d \in \mathcal{D}$. Applying the above lemma, after some tedious algebra, we arrive at the following bound on the average redundancy rate

$$\overline{r} \le \frac{1}{\overline{D}} \sum_{d \in \mathcal{D}} P(d)(\ell(d) + \log P(d)) \le C\frac{1}{\overline{D}N^{1+\eta}}.$$

Since the average dictionary phrase length $\overline{D}$ is of order N^3 we have

$$\overline{r} = O\left(\overline{D}^{-1-\frac{1+\eta}{3}}\right) = O\left(\overline{D}^{-\frac{4+\eta}{3}}\right).$$

This proves the upper bound for $\overline{r}$ of Lemma 6.3 and Theorem 6.1 follows.

6.3 Explicit Construction of a Khodak VV Code

In what follows we present an algorithm for designing a VV-code with arbitrarily large average dictionary length $\overline{D}$ for memoryless sources. More precisely, we construct a code with redundancy $\overline{r} \le \varepsilon/\overline{D}$, where $\varepsilon > 0$ is given and $\overline{D} \ge c/\varepsilon^3$ (for some constant c). In fact, for some large integer N we find that $\overline{D} = N^3$ and $\varepsilon = 1/N$, so that $\overline{r} = O(\overline{D}^{-4/3})$ which does not employ the full strength of Theorem 6.1 that guarantees the existence of a code with the average redundancy smaller than $c\overline{D}^{-5/3}$. This allows, however, for some simplification of the algorithm, in particular we just use a standard Shannon code.

Before we proceed, we need some facts about *continued fractions.* A finite continued fraction expansion is a rational number of the form

$$c_0 + \cfrac{1}{c_1 + \cfrac{1}{c_2 + \cfrac{1}{c_3 + \ddots + \cfrac{1}{c_n}}}},$$

where c_0 is an integer and c_j are *positive* integers for $j \ge 1$ (see [3]). We denote this rational number as $[c_0, c_1, \ldots, c_n]$. With help of the Euclidean algorithm, it is easy to see that every rational number has a finite continued fraction expansion. Furthermore, if c_j is a given sequence of integers (that are positive for $j > 0$), then the limit $\theta = \lim_{n\to\infty}[c_0, c_1, \ldots, c_n]$ exists and is denoted by the infinite continued fraction expansion $\theta = [c_0, c_1, c_2 \ldots]$. Conversely, if θ is a real irrational number and if we recursively set

$$\theta_0 = \theta, \quad c_j = \lfloor \theta_j \rfloor, \quad \theta_{j+1} = 1/(\theta_j - c_j),$$

then $\theta = [c_0, c_1, c_2 \ldots]$. In particular, every irrational number has a unique infinite continued fraction expansion.

The *convergents* of an irrational number θ with infinite continued fraction expansion $\theta = [c_0, c_1, c_2 \ldots]$ are defined as

$$\frac{P_n}{Q_n} = [c_0, c_1, \ldots, c_n],$$

where integers P_n, Q_n are coprime. These integers can be recursively determined by

$$P_n = c_n P_{n-1} + P_{n-2}, \qquad Q_n = c_n Q_{n-1} + Q_{n-2}.$$

In particular, P_n and Q_n are growing exponentially quickly. Furthermore, the convergents $\frac{P_n}{Q_n}$ are the best rational approximations of θ in the sense that

$$|Q_n\theta - P_n| < \min_{0<Q<Q_n,\ P\in\mathbb{Z}} |Q\theta - P|.$$

In particular one has [17]

$$\left|\theta - \frac{P_n}{Q_n}\right| < \frac{1}{Q_n^2}. \tag{6.8}$$

The denominators Q_n are called *best approximation denominators.*

Now we are ready to construct a VV code with redundancy $o(1/\overline{D})$. We will also make the assumption that all symbol probabilities p_j are rational numbers; otherwise we would have to assume that p_j is known to an arbitrary precision. We then know that $\log p_j$ is either irrational or an integer (which means that $p_j = 2^{-k}$). Thus, we can immediately decide whether all $\log_2 p_j$ are rational or not. If all p_j are negative powers of 2, then we can use a perfect code with zero redundancy. Thus, we only have to treat the case where p_{m-1} is not a negative powers of 2. We also assume that the continued fraction expansion of $\log p_{m-1} = [c_0, c_1, c_2, \ldots]$ is given and one determines a convergent

$$[c_0, c_1, c_2, \ldots, c_n] = M/N$$

for which the denominator N satisfies $N > 4/\varepsilon$. The main goal of the algorithms is to construct a prefix free set of words d with the property that for *most words* $\langle \log_2 P(d) \rangle$ is small. The reason for this philosophy is that if one uses the Shannon code as the string encoder, that is, $\ell(d) = \lceil -\log_2 P(d) \rceil$, then the difference $\ell(d) - \log(1/P(d)) = \langle \log_2 P(d) \rangle$ is small and contributes negligibly to the redundancy.

The main step of the algorithm is a loop of the same subroutine. The input is a pair $\mathcal{D}$, $\mathcal{B}$ of sets of words with the property that $\mathcal{D} \cup \mathcal{B}$ is a prefix free set. Words d in $\mathcal{D}$ are already *good* in the sense that $\langle \log P(d) \rangle \le \frac{3}{4}\varepsilon$, whereas words r in $\mathcal{B}$ are *bad* because they do not satisfy this condition. In the first step of the subroutine, one chooses a word $r \in \mathcal{B}$ of minimal length and computes an integer k with $0 \le k < N$ that satisfies

$$\frac{1}{N} \le \langle kM/N + x + \log P(r) \rangle \le \frac{2}{N}.$$

Here x is an abbreviation of

$$x = \sum_{j=0}^{m-1} k_j^0 \log p_j,$$

where $k_j^0 = \lfloor p_j N^2 \rfloor$, $0 \le j < m$. The computation of k can be done by solving the congruence

$$kM \equiv 1 - \lfloor (x + \log_2 P(r))N \rfloor \bmod N$$

(e.g., with help of the Euclidean algorithm). This choice of k ensures that

$$0 \le \langle k \log p_m + x + \log_2 P(r) \rangle \le 3/N \le \frac{3}{4}\varepsilon.$$

For this k we determine the set $\mathcal{D}'$ of all words d of type$(d) = (k_0^0, \ldots, k_{m-2}^0, k_{m-1}^0 + k)$. By construction all $d' \in \mathcal{D}'$ satisfy

$$\langle \log P(r \cdot d') \rangle = \langle k \log p_{m-1} + x + \log P(r) \rangle \le \frac{3}{4}\varepsilon.$$

We now replace $\mathcal{D}$ by $\mathcal{D} \cup r \cdot \mathcal{D}'$ and $\mathcal{B}$ by $(\mathcal{B} \setminus \{r\}) \cup r \cdot (\mathcal{X}^n \setminus \mathcal{D}')$. This construction ensures that (again) all word in $d \in \mathcal{D}$ satisfy

$$\langle \log P(d) \rangle \le \frac{3}{4}\varepsilon.$$

The algorithm terminates when $P(\mathcal{D}) > 1 - \varepsilon/4$; that is, *most words* in $\mathcal{D} \cup \mathcal{B}$ are *good*. The proof of Theorem 6.1 shows that this actually occurs when the average dictionary length $\overline{D}$ is of order $O(N^3)$. In particular, the special choice of integers $k_j^0 = \lfloor p_j N^2 \rfloor$ ensures that the probability $P(\mathcal{D})$ increases step by step as quickly as possible, compare with (6.5).

As already mentioned, we finally use the Shannon code $C : \mathcal{D} \cup \mathcal{B} \to \{0,1\}^*$, that is $\ell(d) = \lceil -\log_2 P(d) \rceil$ for all $d \in \mathcal{D} \cup \mathcal{B}$. The redundancy can be estimated by

$$\begin{aligned}
\overline{r} &= \frac{1}{\overline{D}} \sum_{d \in \mathcal{D} \cup \mathcal{B}} P(d) \left(\ell(d) - \log \frac{1}{P(d)} \right) \\
&= \frac{1}{\overline{D}} \sum_{d \in \mathcal{D} \cup \mathcal{B}} P(d) \, \langle \log P(d) \rangle \\
&= \frac{1}{\overline{D}} \left(\sum_{d \in \mathcal{D}} P(d) \langle \log_2 P(d) \rangle + \sum_{d \in \mathcal{B}} P(d) \langle \log P(d) \rangle \right) \\
&\le \frac{1}{\overline{D}} \left(P(\mathcal{D}) \frac{3}{4} \varepsilon + P(\mathcal{B}) \right) \\
&\le \frac{1}{\overline{D}} \left(\frac{3}{4} \varepsilon + \frac{1}{4} \varepsilon \right) = \frac{\varepsilon}{\overline{D}}.
\end{aligned}$$

Thus this algorithm constructs a parsing tree and a VV code with a small redundancy rate. A more formal description of the algorithm follows.

Algorithm KhodCode:

Input: (i) m, an integer ≥ 2; (ii) positive rational numbers $p_0, \ldots, p_{m-1}$ with $p_0 + \cdots + p_{m-1} = 1$, p_{m-1} is not a power of 2; (iii) ε, a positive real number < 1.

Output: A VV-code, that is, a complete prefix free set $\mathcal{D}$ on m symbols and a prefix code $C : \mathcal{D} \to \{0,1\}^*$, with redundancy $\overline{r} \le \varepsilon / \overline{D}$, where the average dictionary code length $\overline{D}$ satisfies $\overline{D} \ge c(m, p_0, \ldots, p_{m-1})/\varepsilon^3$ (for some constant $c(m, p_0, \ldots, p_{m-1})$).

Notation: For a word $w \in \{0, \ldots, m-1\}^*$ that consists of k_j copies of j $(0 \le j < m)$ we set $P(w) = p_0^{k_0} \cdots p_{m-1}^{k_{m-1}}$ for the probability of w and type$(w) = (k_0, \ldots, k_{m-1})$. By ω we denote the empty word and set $P(\omega) = 1$.

```
1. **Calculate** the convergent $\frac{M}{N} = [c_0, c_1, \ldots, c_n]$ of the irrational
   number $\log p_{m-1}$ for which $N > 4/\varepsilon$.

2. **Set** $k_j^0 = \lfloor p_j N^2 \rfloor$ $(0 \le j < m)$, $x = \sum_{j=1}^{m} k_j^0 \log_2 p_j$, and $n_0 =
   \sum_{j=1}^{m} k_j^0$.

3. **Set** $\mathcal{D} = \emptyset$, $\mathcal{B} = \{\omega\}$, and $p = 0$
   **while** $p < 1 - \varepsilon/4$ **do**
         Choose $r \in \mathcal{B}$ of minimal length
         $b \leftarrow \log P(r)$
         Find $0 \le k < N$ that solves the congruence
         $kM \equiv 1 - \lfloor (x + b)N \rfloor \bmod N$
         $n \leftarrow n_0 + k$
         $\mathcal{D}' \leftarrow \{d \in A^n : \mathrm{type}(d) = (k_0^0, \ldots, k_{m-2}^0, k_{m-1}^0 + k)\}$
         $\mathcal{D} \leftarrow \mathcal{D} \cup r \cdot \mathcal{D}'$
         $\mathcal{B} \leftarrow (\mathcal{B} \setminus \{r\}) \cup r \cdot (\{0, \ldots, m-1\}^n \setminus \mathcal{D}')$
         $p \leftarrow p + P(r)P(\mathcal{D}')$, where

         $$P(\mathcal{D}') = \frac{n!}{k_0^0! \cdots k_{m-2}^0!(k_{m-1}^0 + k)!} p_0^{k_0^0} \cdots p_{m-2}^{k_{m-2}^0} p_{m-1}^{k_{m-1}^0 + k}.$$

   **end while**.

4. $\mathcal{D} \leftarrow \mathcal{D} \cup \mathcal{B}$.

5. **Construct** a Shannon code $C : \mathcal{D} \to \{0,1\}^*$ with $\ell(d) =
   \lceil -\log P(d) \rceil$ for all $d \in \mathcal{D}$.

6. **End**.
```

Example 6.1. Assume $m = 2$ with $p_0 = 2/3$ and $p_1 = 1/3$. In the first iteration of the algorithm we assume that both $\mathcal{B}$ and $\mathcal{C}$ are empty. Easy computations show that

$$\log(1/3) = [-2, 2, 2, 2, 3, \ldots], \quad \text{and} \quad [-2, 2, 2, 2] = -\frac{19}{12},$$

hence $M = -19$ and $N = 12$. Let us set $\varepsilon = 0.4$ so $4/\varepsilon = 10 < 12 = N$. Therefore, $k_0^0 = 96$, $k_1^0 = 48$ so that $n_0 = 144 = N^2$. Solving the congruence

$$-19k = 1 + 1587 \mod 12$$

gives $k = 8$ and therefore

$$\mathcal{C}' = \{d \in \{0,1\}^{152} : \text{ type}(d) = (96, 56)\}$$

with $P(\mathcal{C}') \approx 0.04425103411$. Observe that $\mathcal{B} = \{0,1\}^{152} \setminus \mathcal{C}$.

In the second iteration we can pick up any string from $\mathcal{B}$, say the string $r = 00\ldots0$ with 152 zeros. We find, solving the congruence with $b = 152\log(2/3) \approx -88.91430011$, that $k = 5$. Hence $\mathcal{C}' = \{d \in \{0,1\}^{149} : \text{ type}(d) = (96, 53)\}$ and $\mathcal{C} = \{d \in \{0,1\}^{152} : \text{ type}(d) = (96, 56)\} \cup r \cdot \mathcal{C}'$. We continue along the same path until the total probability of all "good" strings in $\mathcal{C}$ reaches the value $3/4 \cdot \varepsilon = 0.3$, which may take some time.

6.4 Khodak's Redundancy for Almost All Sources

In this section we present better estimates for the redundancy rates but valid only for *almost all* memoryless sources. This means that the set of exceptional p_j, those p_j with $\sum_{j=1}^{m} p_j = 1$ and $p_j > 0$ for all $0 \le j \le m-1$ that do not satisfy the proposed property, has zero Lebesgue measure on the $(m-1)$-dimensional hyperplane $x_0 + \cdots + x_{m-1} = 1$. From a mathematical point of view, these results are more challenging.

While Lemma 6.2 and 6.3 laid foundation for Theorem 6.1, the next lemma is fundamental for our current considerations.

Lemma 6.5. Suppose that $\varepsilon > 0$. Then for almost all p_j $(0 \le j < m)$ with $p_j > 0$ and $p_0 + p_1 + \cdots + p_{m-1} = 1$ the set

$$X = \{\langle k_0 \log p_0 + \cdots + k_{m-1} \log p_{m-1} \rangle : 0 \le k_j < N \ (0 \le j < m)\}$$

has dispersion

$$\delta(X) \le \frac{1}{N^{m-\varepsilon}} \tag{6.9}$$

for sufficiently large N. In addition, for almost all $p_j > 0$ there exists a constant $C > 0$ such that

$$\|k_0 \log p_0 + \cdots + k_{m-1} \log p_{m-1}\| \ge C \left(\max_{0 \le j < m} |k_j| \right)^{-m-\varepsilon} \tag{6.10}$$

for all non-zero integer vectors $(k_0, \ldots, k_{m-1})$.

We should point out that for $m = 2$ we can slightly improve the estimate of the lemma. Indeed, we will show that for almost all $p_0 > 0, p_1 > 0$ with $p_0 + p_1 = 1$ there exists a constant κ and infinitely many N such that the set $X = \{\langle k_0 \log p_0 + k_1 \log p_1 \rangle : 0 \le k_0, k_1 < N\}$ has dispersion

$$\delta(X) \le \frac{\kappa}{N^2}. \tag{6.11}$$

The estimate (6.11) is a little bit sharper than (6.9). However, it is only valid for infinitely many N and not for all but finitely many.[2]

By combining Lemma 6.3 and Lemma 6.5 we directly obtain our second main result valid for almost all sources.

Theorem 6.6 (Y. Bugeaud, M. Drmota, and W. Szpankowski, 2008)**.** Let $m \ge 2$ and consider a memoryless source on m symbols. Then for almost all source parameters, and for every sufficiently large D_0, there exists a VV code with the average dictionary size $\overline{D}$ satisfying $D_0 \le \overline{D} \le 2D_0$ such that its average redundancy rate is bounded by

$$\overline{r} \le \overline{D}^{-\frac{4}{3} - \frac{m}{3} + \varepsilon}, \tag{6.12}$$

where $\varepsilon > 0$ and maximal length is $O(\overline{D} \log \overline{D})$.

This theorem shows that the *typical* best possible average redundancy $\overline{r}$ can be measured in terms of negative powers of $\overline{D}$ that are linearly decreasing in the alphabet size m. However, it seems to be a very difficult problem to obtain the optimal exponent (almost surely). Nevertheless, these bounds are best possible through the methods we applied.

Before we present a proof of Lemma 6.5 and hence prove of our second main result Theorem 6.6, we complete our analysis with a lower bound for all sources. We start with a simple lemma that follows directly from our proof of Lemma 6.4

Lemma 6.7. Let $\mathcal{D}$ be a complete prefix free set with probability distribution P. Then for any code $C : \mathcal{D} \to \{0,1\}^*$ we have

$$\overline{r} \ge \frac{1}{2} \frac{1}{\overline{D}} \sum_{d \in \overline{D}} P(d) \| \log_2 P(d) \|^2.$$

[2] We point out that (6.9) and (6.11) are optimal. Since the set X consists of N^m points the dispersion must satisfy $\delta(X) \ge \frac{1}{2} N^{-m}$.

Proof. Suppose that $|x| \le 1$. Then we have $2^{-x} = 1 - x\log 2 + \eta(x)$ with $((\log 4)/4)x^2 \le \eta(x) \le (\log 4)x^2$. Actually we can represent 2^{-x} also for $|x| > 1$ and still have some positive error term $\eta(x)$ that satisfies

$$\eta(x) \ge \min\left(\eta(\langle x\rangle), \eta(1 - \langle x\rangle)\right) \ge \frac{\log 4}{4}\|x\|^2.$$

Hence by using the representation

$$x = (1 - 2^{-x} + \eta(x))/\ln 2$$

we find

$$\begin{aligned}
\overline{r} &= \frac{1}{\overline{D}}\sum_{d\in\mathcal{D}} P(d)(\ell(d) + \log P(d)) \\
&= \frac{1}{\overline{D}\ln 2}\sum_{d\in\mathcal{D}} P(d)\left(1 - 2^{-\ell(d)-\log P(d)} + \eta(\ell(d) + \log P(d))\right) \\
&= \frac{1}{\overline{D}\ln 2}\left(1 - \sum_{d\in\mathcal{D}} 2^{-\ell(d)}\right) + \frac{1}{\overline{D}\log 2}\sum_{d\in\mathcal{D}} P(d)\eta(\ell(d) + \log P(d)).
\end{aligned}$$

Hence, by Kraft's inequality and the above observation the result follows immediately. □

We are now in a position to present our finding regarding a lower bound on the redundancy rates for almost all sources.

Theorem 6.8. Consider a memoryless source on an alphabet of size $m \ge 2$. Then for almost all source parameters, and for every VV code with average dictionary length $\overline{D} \ge D_0$ (where D_0 is sufficiently large) we have

$$r^* \ge \overline{r} \ge \overline{D}^{-2m-1-\varepsilon}, \tag{6.13}$$

where $\varepsilon > 0$.

Proof. By Lemma 6.7 we have

$$\overline{r} \ge \frac{1}{2\overline{D}}\sum_{d\in\overline{D}} P(d)\|\log_2 P(d)\|^2.$$

Suppose that $P(d) = p_0^{k_0}\cdots p_{m-1}^{k_{m-1}}$ holds, that is

$$\log P(d) = k_0\log p_0 + \cdots + k_{m-1}\log p_{m-1}.$$

By Lemma 6.5, we conclude from (6.10) that for all p_j and for all non-zero integer vectors $(k_0, \ldots, k_{m-1})$

$$\|k_0 \log p_0 + \cdots + k_{m-1} \log p_{m-1}\| \geq C \left(\max_{0 \leq j < m} |k_j| \right)^{-m-\varepsilon},$$

and therefore

$$\| \log P(d)\| \geq C \left(\max_{0 \leq j < m} |k_j| \right)^{-m-\varepsilon} \geq C \left(\sum_{0 \leq j < m} k_j \right)^{-m-\varepsilon} = C|d|^{-m-\varepsilon}.$$

Consequently, by Jensen's inequality, we obtain

$$\begin{aligned} \overline{r} &\geq \frac{C}{2\overline{D}} \sum_{d \in \mathcal{D}} P(d)|d|^{-2m-2\varepsilon} \\ &\geq \frac{C}{2\overline{D}} \left(\sum_{d \in \mathcal{D}} P(d)|d| \right)^{-2m-2\varepsilon} \\ &\geq \overline{D}^{-2m-1-3\varepsilon}. \end{aligned}$$

This completes the proof of Theorem 6.8. □

6.4.1 Proof of Lemma 6.5

Lemma 6.5 states that for almost all $p_j > 0$ (with $p_1 + \cdots + p_{m-1} = 1$) the set

$$X = \{ \langle k_0 \log p_0 + \cdots + k_{m-1} \log_2 p_{m-1} \rangle : 0 \leq k_j < N \ (0 \leq j < m) \}$$

has dispersion

$$\delta(X) \leq N^{-m+\varepsilon} \tag{6.14}$$

for all sufficiently large N and for all non-zero integer vectors $(k_1, \ldots, k_m)$ we have

$$\|k_0 \log p_0 + \cdots + k_{m-1} \log_2 p_{m-1}\| \geq C \left(\max_{0 \leq j < m} |k_j| \right)^{-m-\varepsilon} \tag{6.15}$$

for some constant $C > 0$.

In view of the above, we just have to show (6.14) and (6.15) for almost all p_j. These kind of problems fall into the field of *metric Diophantine approximation* that is well established in number theory (see

[11, 17, 136, 143]). One of the problems in this field is to obtain some information about the following linear forms

$$L = k_0\gamma_0 + \cdots + k_{m-1}\gamma_{m-1} + k_m,$$

where k_j are integers and γ_j are randomly chosen real numbers. In fact, one is usually interested in lower bounds for $|L|$ in terms of $\max |k_j|$.

In our context, we have $\gamma_j = \log_2 p_j$ so that the γ_j's are related by

$$2^{\gamma_0} + \cdots + 2^{\gamma_{m-1}} = 1.$$

This means that they cannot be chosen independently. They are situated on a proper submanifold of the m-dimensional space. It has turned out that metric Diophantine approximation in this case is much more complicated than in the independent case. Fortunately, there exist now proper results that we can use for our purpose.

Theorem 6.9 (Dickinson and Dodson [31]). Suppose that $m \geq 2$ and $1 \leq k < m$. Let U be an open set in $\mathbf{R}^k$ and, for $1 \leq j \leq m$, let $\Psi_j : U \to \mathbf{R}$ be C^1 real functions. Let $\eta > 0$ be real. Then for almost all $u = (u_1, \ldots, u_k) \in U$, there exists $N_0(u)$ such that for all $N \geq N_0(u)$ we have

$$|k_0 + k_1\Psi_1(u) + \cdots + k_m\Psi_m(u)| \geq N^{-m+(m-k)\eta}(\log N)^{m-k}$$

for all non-zero integer vectors $(k_0, k_1, \ldots, k_m)$ with

$$\max_{1\leq j\leq k} |k_j| \leq N \quad \text{and} \quad \max_{k<j\leq m} |k_j| \leq N^{1-\eta}/(\log N).$$

Remark 6.1. More precisely, let us define a convex body consisting of all real vectors $(y_1, \ldots, y_m)$ with

$$\begin{aligned} |y_0 + y_1\Psi_1(u) + \ldots + y_m\Psi_m(u)| &\leq N^{-m+(m-k)\eta}(\log N)^{m-k}, \\ |y_j| &\leq N, \quad (j = 1, \ldots, k), \qquad (6.16) \\ |y_j| &\leq N^{1-\eta}\,(\log N)^{-1}, \quad (j > k). \end{aligned}$$

Dickinson and Dodson [31, p. 278] showed in the course of the proof of their Theorem 2 that the set

$$S(N) := \Big\{u \in U : \exists\ (k_0, k_1, \ldots, k_m) \in \mathbf{Z}^{m+1}\Big\}$$

with $0 < \max\limits_{1\le j\le m} |k_j| < N^{1-\eta}$ satisfying (6.16) also has the property that the set

$$\limsup_{N\to\infty} S(N) = \bigcap_{N\ge 1} \bigcup_{M\ge N} S(M)$$

has zero Lebesgue measure. This means that almost no u belongs to infinitely many sets $S(N)$. In other words, for almost every u, there exists $N_0(u)$ such that $u \notin S(N)$ for every $N \ge N_0(u)$. And this is stated in Theorem 6.9.

For $m = 2$, Theorem 6.9 can be improved as shown by Baker [7].

Theorem 6.10 (R.C. Baker [7])**.** Let Ψ_1 and Ψ_2 be C^3 real functions defined on an interval $[a,b]$. For x in $[a,b]$, set

$$k(x) = \Psi_1'(x)\Psi_2''(x) - \Psi_1''(x)\Psi_2'(x).$$

Assume that $k(x)$ is non-zero almost everywhere and that $|k(x)| \le M$ for all x in $[a,b]$ and set $\kappa = \min\{10^{-3}, 10^{-8}M^{-1/3}\}$. Then for almost all x in $[a,b]$, there are infinitely many positive integers N such that

$$|k_0 + k_1\Psi_1(x) + k_2\Psi_2(x)| \ge \kappa N^{-2}$$

for all integers k_0, k_1, k_2 with $0 < \max\{|k_1|, |k_2|\} \le N$.

Using Theorem 6.9 and Theorem 6.10 we are now in a position to prove (6.14) and (6.15).

Proof of (6.15). For this purpose we can directly apply Theorem 6.9, where $k = m - 1$ and U is an open set contained in

$$\Delta = \{u = (u_1, \dots, u_{m-1}) : u_1 \ge 0, \dots, u_{m-1} \ge 0, u_1 + \cdots + u_{m-1} \le 1\}$$

and $\Psi_j(u) = \log_2(u_j)$ $(1 \le j \le m-1)$, resp. $\Psi_m(u) = \log_2(1 - u_1 - \cdots - u_{m-1})$. We also know that, for almost all u, the numbers $1, \Psi_1(u), \dots, \Psi_m(u)$ are linearly independent over the rationals, hence,

$$L := k_0 + k_1\Psi_1(u) + \cdots + k_m\Psi_m(u) \ne 0$$

for all non-zero integer vectors $(k_0, k_1, \dots, k_m)$.

Set $J = \max_{1\le j\le m} |k_j|$ and define N by $N^{1-\eta} = J\,\log N$. Assume that J is large enough to give $N \ge N_0(u)$. We then have (for suitable constants $c_1, c_2 > 0$)

$$\begin{aligned}|L| \ge N^{-m+\eta}(\log N) &\ge c_1 J^{-m-(m-1)\eta/(1-\eta)}(\log J)^{(1-m)/(1-\eta)}\\ &\ge c_2 J^{-m-\varepsilon}\end{aligned}$$

for $\varepsilon = 2(m-1)\eta/(1-\eta)$ and J large enough. This completes the proof of (6.15).

Proof of (6.14). To simplify our presentation, we first apply Theorem 6.10 in the case of $m = 2$ and then briefly indicate how it generalizes. First of all we want to point out that Theorems 6.9 and 6.10 are lower bounds for the homogeneous linear form

$$L = k_0 + k_1\Psi_1(u) + \cdots + k_m\Psi_m(u)$$

in terms of $\max |k_j|$. Using techniques from "geometry of numbers" (see below) these lower bounds can be transformed into upper bounds for the dispersion of the set

$$X = \{\langle k_1\Psi_1(u) + \cdots + k_m\Psi_m(u)\rangle : 0 \le k_1, \ldots, k_m < N\}.$$

In particular we will use the notion of successive minima of convex bodies. Let $B \subseteq \mathbf{R}^d$ be a 0-symmetric convex body. Then the successive minima λ_j are defined by

$$\lambda_j = \inf\{\lambda > 0 : \lambda B \text{ contains } j \text{ linearly independent integer vectors}\}.$$

One of the first main results of "geometry of numbers" is *Minkowski's Second Theorem* [17, 136] stating that

$$2^d/d! \le \lambda_1 \cdots \lambda_d \mathrm{Vol}_d(B) \le 2^d.$$

Let x and N be the same as Theorem 6.10 and consider the convex body $B \subseteq \mathbf{R}^3$ that is defined by the inequalities

$$\begin{aligned}|y_0 + y_1\Psi_1(x) + y_2\Psi_2(x)| &\le \kappa N^{-2},\\ |y_1| &\le N,\\ |y_2| &\le N.\end{aligned}$$

By Theorem 6.10 the set B does not contain a non-zero integer point. Thus, the first minimum λ_1 of B is ≥ 1. Note that $\mathrm{Vol}_3(B) = 8\kappa$. Then from Minkowski's Second Theorem we conclude that the three minima of this convex body satisfy $\lambda_1\lambda_2\lambda_3 \leq 1/\kappa$. Since $1 \leq \lambda_1 \leq \lambda_2$ we thus get $\lambda_3 \leq \lambda_1\lambda_2\lambda_3 \leq 1/\kappa$ and consequently $\lambda_1 \leq \lambda_2 \leq \lambda_3 \leq 1/\kappa$. In other words, there exist constants κ_2 and κ_3, and three linearly independent integer vectors (a_0, a_1, a_2), (b_0, b_1, b_2) and (c_0, c_1, c_2) such that

$$\begin{array}{rcl} |a_0 + a_1\Psi_1(x) + a_2\Psi_2(x)| & \leq & \kappa_2 N^{-2}, \\ |b_0 + b_1\Psi_1(x) + b_2\Psi_2(x)| & \leq & \kappa_2 N^{-2}, \\ |c_0 + c_1\Psi_1(x) + c_2\Psi_2(x)| & \leq & \kappa_2 N^{-2}, \\ \max\{|a_i|, |b_i|, |c_i|\} & \leq & \kappa_3 N. \end{array}$$

Using these linearly independent integer vectors, we can show that the dispersion of

$$X = \{\langle k_1\Psi_1(x) + k_2 \log_2 \Psi_2(x)\rangle : 0 \leq k_1, k_2 \leq 7\kappa_3 N\}$$

is small.

Let ξ be a real number (that we want to approximate by an element of X) and consider the (regular) system of linear equations

$$\begin{array}{rcl} -\xi + \theta_a(a_0 + a_1\Psi_1(x) & + & a_2\Psi_2(x)) + \\ +\theta_b(b_0 + b_1\Psi_1(x) + b_2\Psi_2(x)) & + & \theta_c(c_0 + c_1\Psi_1(x) + c_2\Psi_2(x)) = 4\kappa_2 N^{-2}, \\ \theta_a a_1 + \theta_b b_1 + \theta_c c_1 & = & 4\kappa_3 N, \\ \theta_a a_2 + \theta_b b_2 + \theta_c c_2 & = & 4\kappa_3 N. \end{array} \tag{6.17}$$

Denote by $(\theta_a, \theta_b, \theta_c)$ its unique solution and set

$$t_a = \lfloor\theta_a\rfloor, \quad t_b = \lfloor\theta_b\rfloor, \quad t_c = \lfloor\theta_c\rfloor,$$

and

$$k_j = t_a a_j + t_b b_j + t_c c_j \quad (j = 0, 1, 2).$$

Of course, k_0, k_1, k_2 are integers and from the second and third equation of (6.17) combined with $\max\{|a_i|, |b_i|, |c_i|\} \leq \kappa_3 N$ it follow s that

$$\kappa_3 N \leq \min\{k_1, k_2\} \leq \max\{k_1, k_2\} \leq 7\kappa_3 N,$$

in particular, k_1 and k_2 are positive integers. Moreover, by considering the first equation of (6.17) we see that

$$\kappa_2 N^{-2} \leq -\xi + k_0 + k_1\Psi_1(x) + k_2\Psi_2(x) \leq 7\kappa_2 N^{-2}.$$

Since this estimate is independent of the choice of ξ this implies

$$\delta(X) \leq 7\kappa_2 N^{-2}.$$

Clearly, we can apply this procedure for the functions

$$\Psi_1(x) = \log_2 x$$

and

$$\Psi_2(x) = \log_2(1-x)$$

and for any interval $[a,b]$ with $0 < a < b < 1$.

This also shows that we can choose $\varepsilon = 0$ in the case $m = 2$ for infinitely many N in Lemma 3, provided that we introduce an (absolute) numerical constant.

Finally, we discuss the general case $m \geq 2$ (and prove Lemma 6.5). We consider the convex body $B \subseteq \mathbf{R}^{m+1}$ that has volume 2^{m+1} and is defined by (6.16):

$$\begin{aligned} |y_0 + y_1\Psi_1(u) + \ldots + y_m\Psi_m(u)| &\leq N^{-m+(m-k)\eta}(\log N)^{m-k}, \\ |y_j| &\leq N, \quad (j = 1, \ldots, k), \\ |y_j| &\leq N^{1-\eta}\,(\log N)^{-1}, \end{aligned}$$

for $j = k+1, \ldots, m$. By assumption, the first minimum λ_1 of B satisfies $\lambda_1 \geq N^{-\eta}$, thus, by Minkowski's Second Theorem, its last minimum λ_m is bounded by $\lambda_m \leq N^{n\eta}$. Consequently, we have $n+1$ linearly independent vectors $\mathbf{q}^{(i)}$, $i = 0, \ldots, m$, such that

$$\|\mathbf{q}^{(i)} \cdot \Psi(u)\| \leq N^{-m+(m-k)\eta+m\eta}(\log N)^k, \qquad \|\mathbf{q}^{(i)}\|_\infty \leq N^{1+m\eta}.$$

We now argue as above, and consider a system of linear equations analogous to (6.17). Hence, for any real number ξ, there are positive integers $k_1, \ldots, k_m$ such that

$$\| -\xi + k_1\Psi_1(u) + \ldots + k_m\Psi_m(u)\| < \frac{1}{N^{m-\varepsilon}}, \qquad \max k_j \leq N,$$

where $\varepsilon > 0$ can be made arbitrarily small by taking sufficiently small values of η. Applied to the functions

$$\Psi_j(u) = \log_2(u_j), \quad 1 \le j \le m-1$$

and

$$\Psi_m(u) = \log_2(1 - u_1 - \cdots - u_{m-1}),$$

this proves (6.14). This completes the proof of Lemma 6.5.

7

Redundancy of Non Prefix One-to-One Codes

In this concluding chapter, we discuss non-prefix codes, that is, codes which are not prefix free and do not satisfy Kraft's inequality. In particular, we construct a one-to-one code whose average length is smaller than the source entropy in defiance of the Shannon lower bound. To focus, we only consider fixed-to-variable codes over known memoryless sources with block size equal to n. We first present a very precise analysis of one-to-one codes for a binary source alphabet, and then extend it to a general finite source alphabet. This chapter is based on [155, 156] (see also [4, 93]).

7.1 Binary One-to-One Code

In this section we discuss codes known as *one-to-one* codes which are "one-shot" codes that assign a distinct codeword to source symbols and are not necessarily prefix codes (more generally, uniquely decodable). Therefore these codes do not satisfy the Kraft's inequality, for for such codes the Shannon lower bound doesn't apply. We quantify precisely the difference between the code length and the entropy.

We first consider a memoryless source X over the binary alphabet

$\mathcal{X} = \{0,1\}$ generating a sequence $x_1^n = x_1, \ldots, x_n \in \mathcal{A} = \mathcal{X}^n$ with probability $P(x_1^n) = p^k q^{n-k}$, where k is the number of 0's in x_1^n and p is known. We shall assume that $p \leq q$. We first list all 2^n probabilities in a nonincreasing order and assign the code length $\lfloor \log(j) \rfloor$ to the j-th binary string on this list, as shown below:

$$\begin{array}{lccccccc} \text{probabilities} & q^n \left(\frac{p}{q}\right)^0 & \geq & q^n \left(\frac{p}{q}\right)^1 & \geq & \ldots & \geq & q^n \left(\frac{p}{q}\right)^n \\ \\ \text{code lengths} & \lfloor \log_2(1) \rfloor & & \lfloor \log_2(2) \rfloor & & \ldots & & \lfloor \log_2(2^n) \rfloor. \end{array}$$

Observe that there are $\binom{n}{k}$ equal probabilities $p^k q^{n-k}$. Set

$$A_k = \binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{k}, \qquad A_{-1} = 0.$$

Starting from the position $A_{k-1} + 1$ of the above list , the next $\binom{n}{k}$ probabilities are the same and equal to $p^k q^{n-k}$. The one-to-one code assigns to x_1^n the shortest (possibly empty) binary string (ties broken with the ordering $\mathsf{0} < \mathsf{1}$) not assigned to any element y_1^n with $P(y_1^n) > P(x_1^n)$. Thus, for each $j = A_{k-1} + i$, $1 \leq i \leq \binom{n}{k}$, we assign the code length

$$\lfloor \log_2(j) \rfloor = \lfloor \log_2(A_{k-1} + i) \rfloor$$

to the jth binary string. Hence the average code length is

$$\begin{aligned} \mathbf{E}[L_n] &= \sum_{k=0}^{n} p^k q^{n-k} \sum_{j=A_{k-1}+1}^{A_k} \lfloor \log_2(j) \rfloor \qquad (7.1) \\ &= \sum_{k=0}^{n} p^k q^{n-k} \sum_{i=1}^{\binom{n}{k}} \lfloor \log_2(A_{k-1} + i) \rfloor. \end{aligned}$$

Our goal is to estimate $\mathbf{E}[L_n]$ asymptotically for large n and the average unnormalized redundancy

$$\overline{R}_n = \mathbf{E}[L_n] - nh(p)$$

where $h(p) = -p \log p - q \log q$ is the binary entropy.

Let us first simplify the formula for $\mathbf{E}[L_n]$. We need to handle the inner sum that contains the floor function. To evaluate this sum we apply partial summation: (cf. Knuth [85] Ex. 1.2.4-42)

$$\sum_{j=1}^{N} a_j = N a_N - \sum_{j=1}^{N-1} j(a_{j+1} - a_j). \tag{7.2}$$

Using this, we easily find an explicit formula for the inner sum of (7.1), namely

$$\begin{aligned} S_{n,k} &= \sum_{j=1}^{\binom{n}{k}} \lfloor \log_2(A_{k-1} + j) \rfloor \\ &= \binom{n}{k} \lfloor \log_2 A_k \rfloor - (2^{\lfloor \log_2(A_k) \rfloor + 1} - 2^{\lceil \log_2(A_{k-1}+2) \rceil}) \\ &+ (A_{k-1} + 1)(1 + \lfloor \log_2(A_k) \rfloor - \lceil \log_2(A_{k-1} + 2) \rceil). \end{aligned}$$

After some algebra, using $\lfloor x \rfloor = x - \langle x \rangle$ and $\lceil x \rceil = x + \langle -x \rangle$, we finally reduce the formula for $\mathbf{E}[L_n]$ to the following

$$\begin{aligned} \mathbf{E}[L_n] &= \sum_{k=0}^{n} \binom{n}{k} p^k q^{n-k} \lfloor \log_2 A_k \rfloor \\ &- 2 \sum_{k=0}^{n} \binom{n}{k} p^k q^{n-k} 2^{-\langle \log_2 A_k \rangle} \\ &+ \sum_{k=0}^{n} \binom{n}{k} p^k q^{n-k} \frac{1 + A_{k-1}}{\binom{n}{k}} \\ &\quad \times \left(1 + \log_2 \left(\frac{A_k}{A_{k-1} + 2} \right) - \langle -\log_2(A_{k-1} + 2) \rangle - \langle \log_2 A_k \rangle \right) \\ &- \sum_{k=0}^{n} \binom{n}{k} p^k q^{n-k} \frac{A_{k-1}}{\binom{n}{k}} \left(2^{-\langle \log_2 A_k \rangle + 1} - 2^{\langle -\log_2(A_{k-1}+2) \rangle} \right) \\ &+ 2 \sum_{k=0}^{n} p^k q^{n-k} 2^{\langle -\log_2(A_{k-1}+2) \rangle}. \end{aligned} \tag{7.3}$$

Now we are in the position to present our main result.

Theorem 7.1 (W. Szpankowski, 2008)**.** Consider a binary memoryless source and the one-to-one block code described above. Then for $p < \frac{1}{2}$

$$\begin{aligned}\overline{R}_n &= -\frac{1}{2}\log_2 n - \frac{3+\ln(2)}{2\ln(2)} + \log_2 \frac{1-p}{1-2p}\frac{1}{\sqrt{2\pi p(1-p)}} \\ &\quad + \frac{p}{1-2p}\log_2\left(\frac{2(1-p)}{p}\right) + F(n) + o(1) \qquad (7.4)\end{aligned}$$

where $\alpha = \log_2(1-p)/p$, $\beta = \log_2(1/(1-p)$. Furthermore if α is irrational then $F(n) = 0$. Conversely if $\alpha = N/M$ for some integers M, N such that $\gcd(N, M) = 1$, then

$$\begin{aligned}F(n) &= -\frac{1-p}{1-2p}H_M(n\beta)[x] - \frac{p}{1-2p}H_M(n\beta-\alpha)[-x] \\ &\quad -\frac{2(1-3p)}{1-2p}H_M(n\beta)[2^{-x}] + \frac{p}{1-2p}H_M(n\beta-\alpha)[2^x]\end{aligned}$$

where

$$\begin{aligned}H_M(y)[f] &:= \frac{1}{M\sqrt{2\pi}}\int_{-\infty}^{\infty} e^{-x^2/2}\left(\left\langle M\left(y - \log_2\left(\frac{1-2p}{1-p}\sqrt{2\pi pqn}\right)\right.\right.\right. \\ &\quad \left.\left.\left. -\frac{x^2}{2\ln 2}\right)\right\rangle - \int_0^1 f(t)dt\right)dx\end{aligned}$$

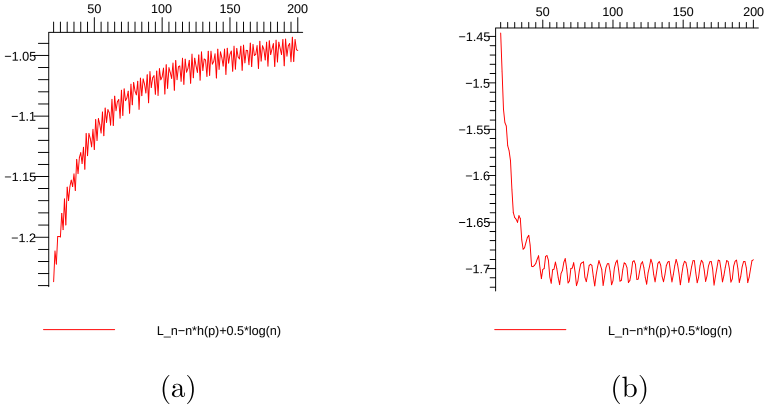
for some Riemann integrable function f.
Finally for $p = \frac{1}{2}$, we have

$$\overline{R}_n = -2 + 2^{-n}(n+2)$$

for every $n \geq 1$.

We start with some observations. First, the average redundancy $\overline{R}_n$ is *negative* for such one-to-one codes. Therefore, in [155] we coin the term anti-redundancy for $\overline{R}_n$ in this case. The fact that one-to-one codes have average code length smaller than entropy was actually known to Shannon and Huffman. However, Wyner in 1972 [174], and then Alon and Orlitsky [4], quantified more precisely this difference. Second, in view of Theorem 7.1, we again see that asymptotic behavior of the redundancy depends on the rationality/irrationality of $\alpha = \log_2(1-p)/p$ (cf. [33, 36, 153]). In Figure 7.1 we plot $\overline{R}_n + 0.5\log_2(n)$

versus n. We observe change of “mode" from a “converging mode” to a “fluctuating mode”, when switching from $\alpha = \log_2(1-p)/p$ irrational (cf. Fig. 7.1(a)) to rational (cf. Fig. 7.1(b)). Recall that we saw this already in Chapters 3 and 4 for Huffman, Shannon, and Tunstall codes.



(a) (b)

Figure 7.1: Plots of $L_n - nh(p) + 0.5\log(n)$ (y-axis) versus n (x-axis) for: (a) irrational $\alpha = \log_2(1-p)/p$ with $p = 1/\pi$; (b) rational $\alpha = \log_2(1-p)/p$ with $p = 1/9$.

We only briefly sketch the proof of Theorem 7.1. The full proof can be found in [155]. We only analyze here (7.3) which we re-write as follows

$$\sum_{k=0}^{n}\binom{n}{k}p^k q^{n-k}\lfloor\log_2 A_k\rfloor = \sum_{k=0}^{n}\binom{n}{k}p^k q^{n-k}\log_2 A_k - \sum_{k=0}^{n}\binom{n}{k}p^k q^{n-k}\langle\log_2 A_k\rangle,$$

and define

$$a_n = \sum_{k=0}^{n}\binom{n}{k}p^k q^{n-k}\log_2 A_k, \qquad b_n = \sum_{k=0}^{n}\binom{n}{k}p^k q^{n-k}\langle\log_2 A_k\rangle.$$

We first deal with a_n for which we need to derive a precise asymptotic estimate for A_n. But this is a simple exercise of the saddle point method [47, 154] as discussed below.

Lemma 7.2. For large n and $p < 1/2$

$$A_{\lfloor np \rfloor} = \frac{1-p}{1-2p} \frac{1}{\sqrt{2\pi np(1-p)}} 2^{nh(p)} \left(1 + O(n^{-1/2})\right) \tag{7.5}$$

where $h(p)$ is the binary entropy. More precisely, for every sufficiently small $\varepsilon > 0$ there exist $\delta > 0$ such that uniformly for $k = np + O(n^{1/2+\varepsilon})$

$$\begin{aligned} A_k &= \frac{1-p}{1-2p} \frac{1}{\sqrt{2\pi np(1-p)}} \left(\frac{1-p}{p}\right)^k \frac{1}{(1-p)^n} \\ &\quad \times \exp\left(-\frac{(k-np)^2}{2p(1-p)n}\right) \left(1 + O(n^{-\delta})\right) \end{aligned} \tag{7.6}$$

for some $\delta > 0$.

Proof. We use the saddle point method (see for example [154]). Let's first define the generating function of A_k, that is,

$$A_n(z) = \sum_{k=0}^{n} A_k z^k = \frac{(1+z)^n - 2^n z^{n+1}}{1-z}.$$

Thus by Cauchy's formula

$$\begin{aligned} A_k &= \frac{1}{2\pi i} \oint \frac{(1+z)^n - 2^n z^{n+1}}{1-z} \frac{dz}{z^{k+1}} \\ &= \frac{1}{2\pi i} \oint \frac{1}{1-z} 2^{n \log(1+z) - (k+1) \log z} dz. \end{aligned}$$

Define $H(z) = n \log(1+z) - (k+1) \log z$. The saddle point z_0 solves $H'(z_0) = 0$, and one finds $z_0 = (k+1)/(n-k+1) = p/(1-p) + O(1/n)$ for $k = \lfloor np \rfloor$ and $H''(z_0) = q^3/p$. Thus by the saddle point method

$$A_k = \frac{1}{1-z_0} \frac{1}{\sqrt{2\pi n H''(z_0)}} 2^{nH(z_0)} (1 + O(n^{-1/2})).$$

This proves (7.5). In a similar manner, as shown in [32], we establish (7.6), as desired. □

For b_n we need to appeal to an extension of Lemma 3.7 from Chapter 3 presented next (for a proof see [33]).

Lemma 7.3. Let $0 < p < 1$ be a fixed real number and $f : [0,1] \to \mathbb{R}$ be a Riemann integrable function.

(i) If α is irrational, then

$$\lim_{n\to\infty} \sum_{k=0}^{n} \binom{n}{k} p^k (1-p)^{n-k} f\left(\left\langle k\alpha + y - (k-np)^2/(2pqn\ln 2)\right\rangle\right) \quad (7.7)$$
$$= \int_0^1 f(t)\,dt,$$

where the convergence is uniform for all shifts $y \in \mathbb{R}$.

(ii) Suppose that $\alpha = \frac{N}{M}$ is a rational number with integers N, M such that $\gcd(N,M) = 1$. Then uniformly for all $y \in \mathbb{R}$

$$\sum_{k=0}^{n} \binom{n}{k} p^k (1-p)^{n-k} f\left(\left\langle k\alpha + y - (k-np)^2/(2pqn\ln 2)\right\rangle\right) \quad (7.8)$$
$$= \int_0^1 f(t)\,dt + G_M(y)$$

where

$$G_M(y)[f] := \frac{1}{M}\frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} e^{-x^2/2} \left(\left\langle M\left(y - \frac{x^2}{2\ln 2}\right)\right\rangle - \int_0^1 f(t)\,dt \right) dx$$

is a periodic function with period $\frac{1}{M}$.

Now, by Lemma 7.3 after observing that for $|k - pn| \le n^{1/2+\varepsilon}$

$$\log A_k = \alpha k + n\beta - \log_2 \omega\sqrt{n} - \frac{(k-np)^2}{2pqn\ln 2} + O(n^{-\delta}),$$

where $\omega = (1-2p)\sqrt{2\pi pq}/(1-p)$. Thus, we need the asymptotic behavior of

$$\sum_{k=0}^{n} \binom{n}{k} p^k q^{n-k} \left\langle \alpha k + n\beta - \log_2 \omega\sqrt{n} - \frac{(k-np)^2}{2pqn\ln 2} \right\rangle$$

that is provided by Lemma 7.3. This completes our sketch of the proof of Theorem 7.1. A full detailed proof can be found in [155].

7.2 Non-binary One-to-One Code

Finally, we consider a non-prefix codes over a general finite alphabet. Consider a probability distribution P on a set of ordered elements $\mathcal{X} = \{1, \ldots, m\}$. We define a permutation π on $\mathcal{X}$ by $\pi(a) < \pi(b)$ if $P(a) > P(b)$ or if $P(a) = P(b)$ and $a < b$. Thus, $\pi(x) = \ell$ if x is the ℓ-th most probable element in $\mathcal{X}$ according to the distribution P, with ties broken according to the ordering in $\mathcal{X}$. It is easy to verify that

$$P(x)\pi(x) \leq 1 \tag{7.9}$$

for all $x \in \mathcal{X}$: if (7.9) failed to be satisfied for $x_0 \in \mathcal{X}$, there would be at least $\pi(x_0)$ masses strictly larger than $1/\pi(x_0)$.

The one-to-one code assigns to x the shortest (possibly empty) binary string (ties broken with the ordering $\mathtt{0} < \mathtt{1}$) not assigned to any element y with $\pi(y) < \pi(x)$. Thus, we obtain (the simple but important conclusion) that the length of the encoding of x is $\lfloor \log_2 \pi(x) \rfloor$.

We are interested in finding the average code length

$$\overline{L} = \mathbf{E}[\lfloor \log_2 \pi(X) \rfloor].$$

A simple upper bound first noticed in [175] is obtained as follows

$$\begin{aligned}
\overline{L} &= \mathbf{E}[\lfloor \log_2 \pi(X) \rfloor] && (7.10)\\
&\leq \mathbf{E}[\log_2 \pi(X)] && (7.11)\\
&\leq \mathbf{E}\left[\log_2 \frac{1}{P(X)}\right] && (7.12)\\
&= H(P) && (7.13)
\end{aligned}$$

where (7.12) follows from (7.9). Note that dropping the prefix condition makes the entropy an upper bound to the minimum average length, rather than a lower bound.

As a simple example, let us compute the average code length when when P is uniform over $\mathcal{X} = \{1, \ldots, m\}$. Here we have [156]

$$\begin{aligned}
\overline{L} &= \frac{1}{m}\sum_{i=1}^{m} \lfloor \log_2 i \rfloor\\
&= \lfloor \log_2 m \rfloor + \frac{1}{m}\left(2 + \lfloor \log_2 m \rfloor - 2^{\lfloor \log_2 m \rfloor + 1}\right)
\end{aligned}$$

which is quite close to the entropy $H(P) = \log_2 m$. In the second line above we apply formula (7.2).

Our goal is to present a general result for the asymptotic behavior of average block code length for Bernoulli sources over $\mathcal{A} = \{1, \dots, m\}^n$.

Theorem 7.4 (W. Szpankowski and S. Verdu, 2011)**.** Consider a Bernoulli source on $\mathcal{A} = \{1, \dots, m\}^n$ and assume that the probability distribution $p_1, \dots p_m$ on $\mathcal{X} = \{1, \dots, m\}$ is not uniform. Then the average code length of the one-to-one code is given by

$$\overline{L}_n = nh - \frac{1}{2} \log_2 n + O(1), \tag{7.14}$$

where $h = -\sum_{i=1}^m p_i \log_2 p_1$ is the entropy. Hence, the average (anti-redundancy becomes

$$\overline{R}_n = -\frac{1}{2} \log_2 n + O(1).$$

The rest of this section is devoted to the **proof of Theorem 7.4**. Without loss of generality we assume that

$$p_1 \leq p_2 \leq \cdots \leq p_{m-1} \leq p_m. \tag{7.15}$$

We set

$$B_i = \log \frac{p_m}{p_i} \tag{7.16}$$

for $i = 1, \dots, m-1$. Note that the entropy h can be expressed as

$$h = \log \frac{1}{p_m} + \sum_{i=1}^{m-1} p_i B_i. \tag{7.17}$$

Let

$$\mathbf{k} = (k_1, \dots, k_m) \tag{7.18}$$

such that $k_1 + \cdots + k_m = n$ denote the *type* of an n-string x_1^n; the probability of each such string is equal to

$$P(x_1^n) = p^{\mathbf{k}} = p_1^{k_1} \cdots p_m^{k_m}. \tag{7.19}$$

Denote the set of all types of n-strings in $\mathcal{A} = \{1, \dots, m\}^n$ by

$$\mathcal{T}_{n,m} = \{(k_1, \dots, k_m) \in \mathbb{N}^m, k_1 + \cdots + k_m = n\}.$$

We introduce an order among types:

$$\mathbf{j} \preceq \mathbf{k} \quad \text{iff} \quad p^{\mathbf{j}} \geq p^{\mathbf{k}}$$

and we sort all types from the smallest index (largest probability) to the largest. This can be accomplished by observing that $p^{\mathbf{j}} \geq p^{\mathbf{k}}$ is equivalent to

$$j_1 B_1 + \cdots + j_{m-1} B_{m-1} \leq k_1 B_1 + \cdots + k_{m-1} B_{m-1}. \tag{7.20}$$

Therefore, to sort types $\mathbf{k}$ one needs to sort the function $S : \mathbb{R}^{m-1} \mapsto \mathbb{R}^+$

$$S(\mathbf{k}) = k_1 B_1 + \cdots + k_{m-1} B_{m-1} \tag{7.21}$$

from the smallest value $S(00 \cdots 0) = 0$ to the largest.

There are

$$\binom{n}{\mathbf{k}} = \binom{n}{k_1, \ldots, k_m} = \frac{n!}{k_1! \cdots k_m!} \tag{7.22}$$

sequences of type $\mathbf{k}$ and we list them in lexicographic order. Then, the optimum code assigns length $\lfloor \log i \rfloor$ to the ith sequence $(1 \leq i \leq m^n)$ in this list. Denote the number of sequences more probable than or equal to type $\mathbf{k}$ as

$$A_{\mathbf{k}} := \sum_{\mathbf{j} \preceq \mathbf{k}} \binom{n}{\mathbf{j}}.$$

Using somewhat informal, but intuitive, notation, $\mathbf{k}+1$ and $\mathbf{k}-1$ denote the *next* and *previous* types, respectively, in the sorted list of the elements of $\mathcal{T}_{n,m}$. Clearly, starting from position $A_{\mathbf{k}}$ the next $\binom{n}{\mathbf{k}+1}$ sequences have probability $p^{\mathbf{k}+1}$. Thus the average code length can be computed as follows

$$\begin{aligned}
\overline{L}_n &= \sum_{\mathbf{k} \in \mathcal{T}_{n,m}} p^{\mathbf{k}} \sum_{i=A_{\mathbf{k}-1}+1}^{A_{\mathbf{k}}} \lfloor \log_2 i \rfloor & (7.23)\\
&= \sum_{\mathbf{k} \in \mathcal{T}_{n,m}} p^{\mathbf{k}} \sum_{i=1}^{\binom{n}{\mathbf{k}}} \lfloor \log_2 (A_{\mathbf{k}} - i + 1) \rfloor & (7.24)\\
&= \sum_{\mathbf{k} \in \mathcal{T}_{n,m}} \binom{n}{\mathbf{k}} p^{\mathbf{k}} \log_2 A_{\mathbf{k}} + O(1), & (7.25)\\
&= \log_2 A_{\lfloor n\mathbf{p} \rfloor} + O(1), & (7.26)
\end{aligned}$$

where $\mathbf{p} = (p_1, \dots, p_m)$ with $p_m = 1 - p_1 - \cdots - p_{m-1}$. We now proceed to justify (7.25) and (7.26). Noticing that for $1 \le i \le \binom{n}{\mathbf{k}}$

$$\log_2 \left(A_{\mathbf{k}} - \binom{n}{\mathbf{k}} + 1 \right) \le \lfloor \log_2 (A_{\mathbf{k}} - i + 1) \rfloor \le \log_2 (A_{\mathbf{k}} + 1)$$

we conclude that

$$\begin{aligned} \sum_{\mathbf{k} \in \mathcal{T}_{n,m}} \binom{n}{\mathbf{k}} p^{\mathbf{k}} \log_2 A_{\mathbf{k}} \quad &+ \sum_{\mathbf{k} \in \mathcal{T}_{n,m}} \binom{n}{\mathbf{k}} p^{\mathbf{k}} \log \left(1 - \frac{\binom{n}{\mathbf{k}} - 1}{A_{\mathbf{k}}} \right) \qquad (7.27) \\ \le \overline{L}_n \quad &\le \sum_{\mathbf{k} \in \mathcal{T}_{n,m}} \binom{n}{\mathbf{k}} p^{\mathbf{k}} \log_2 (A_{\mathbf{k}} + 1). \end{aligned}$$

We first estimate the second sum on the left side of (7.27). In (7.37) and (7.39) below we establish that

$$\frac{\binom{n}{\lfloor n\mathbf{p} \rfloor}}{A_{\lfloor n\mathbf{p} \rfloor}} = O \left(n^{-(m-2)/2} \right),$$

which along with $\log(1-x) = -x + O(x^2)$ enables us to conclude that the second sum in (7.27) is of order $O(n^{-(m-2)/2})$.

In order to verify (7.25) we need asymptotics of the following *multinomial sum*

$$S_f(n) := \sum_{\mathbf{k} \in \mathcal{T}_{n,m}} \binom{n}{\mathbf{k}} p^{\mathbf{k}} f(\mathbf{k})$$

where $f(\mathbf{k})$ is a function of at most polynomial growth. In our case $f(\mathbf{k}) = \log A_{\mathbf{k}} = O(n)$, where $n = k_1 + \cdots + k_m$. In [45, 68] it is proved that such a sum grows asymptotically as $f(\lfloor n\mathbf{p} \rfloor)$. For the reader's convenience we offer a streamlined justification for functions of polynomial growth; in particular when $f(\mathbf{k})$ has an analytic continuation to a complex cone around the real positive axis [68, 154].

In general, Taylor's expansion of f around $n\mathbf{p}$ is

$$f(\mathbf{x}) = f(n\mathbf{p}) + (\mathbf{x} - \mathbf{p}) \nabla f(n\mathbf{p}) + \frac{1}{2} (\mathbf{x} - n\mathbf{p}) \nabla^2 f(\mathbf{x}') (\mathbf{x} - n\mathbf{p})$$

for some $\mathbf{x}'$ in the vicinity of $n\mathbf{p}$, where we use the same simplified notations as before. Observe now that

$$S_f(n) \quad = \quad \mathbf{E}[f(\mathbf{X})] \qquad (7.28)$$

$$\begin{aligned} &= f(n\mathbf{p}) + O(n \max_{\mathbf{x}', ij} f''_{ij}(\mathbf{x}')) && (7.29)\\ &= f(n\mathbf{p}) + O(n\xi(n)), && (7.30)\end{aligned}$$

where $\mathbf{X}$ is a multinomial distribution with parameters n and $\mathbf{p}$ and $f''_{ij}(\mathbf{x})$ is the second derivative with respect to x_i and x_j. Observe that in (7.29) we use the fact that variance of $\mathbf{X}$ is of order $O(n)$. The above asymptotic result is useful as long as the first term dominates the second term $O(n\xi(n))$, as is the case in our situation. One can argue that f has an analytic continuation in a cone around the real positive axis and polynomial growth (cf. (7.41) below). By Lemma 3 of [67] or [154] we conclude that $n\xi(n) = O(1/n)$ and $f''(\mathbf{k}) = O(1/n)$. Thus, (7.25)-(7.26) follow.

Let now

$$j_i = np_i + x_i$$

for $i = 1, \ldots, m-1$. Then, by (7.20) $p^{\mathbf{j}} \geq p^{n\mathbf{p}}$, is equivalent to

$$B_1 x_1 + \cdots + B_{m-1} x_{m-1} \leq 0. \qquad (7.31)$$

Thus[1]

$$\begin{aligned} A_{n\mathbf{p}} &= \sum_{p^{\mathbf{j}} \geq p^{n\mathbf{p}}} \binom{n}{\mathbf{j}} && (7.32)\\ &= \sum_{\mathbf{x}:\mathbf{b}^T\mathbf{x} \leq 0} \binom{n}{n\mathbf{p}+\mathbf{x}}, && (7.33)\end{aligned}$$

where

$$\begin{aligned} \mathbf{x}^T &= [x_1, \ldots, x_{m-1}],\\ \mathbf{b}^T &= [B_1, \ldots, B_{m-1}],\end{aligned}$$

and that sum runs over all vectors $\mathbf{x}$ such that $n\mathbf{p}+\mathbf{x}$ are integer vectors (we will not mention this explicitly in the sequel). The next step is to use Stirling's formula

$$n! = \sqrt{2\pi n} \cdot n^n e^{-n}(1 + O(1/n)) \qquad (7.34)$$

[1] For the sake of notational simplicity we do not distinguish between $n\mathbf{p}$ and $\lfloor n\mathbf{p} \rfloor$.

to estimate the summands in (7.33). This leads to

$$\binom{n}{n\mathbf{p}+\mathbf{x}} = \frac{n!}{(np_1+x_1)!\cdots(np_{m-1}+x_{m-1})!(np_m-x_1-\cdots-x_{m-1})!} =$$

$$\frac{\sqrt{2\pi n}n^n e^{-n} e^{np_1+x_1}\cdots e^{np_m-x_1-\cdots-x_{m-1}}(1+O(1/n))}{\prod_{i=1}^m \sqrt{2\pi(np_i+x_i)}(np_i+x_i)^{np_i+x_i}}$$

$$= \frac{1}{(2\pi)^{(m-1)/2}}\frac{1}{\sqrt{p_1\cdots p_m}}\frac{1}{n^{(m-1)/2}}\left(1+O(1/\sqrt{n})\right)\cdot$$

$$\cdot\frac{n^n}{\prod_{i=1}^m (np_i)^{np_i+x_i}(1+\frac{x_i}{np_i})^{np_i+x_i}}$$

$$= \frac{1}{(2\pi)^{(m-1)/2}}\frac{1}{\sqrt{p_1\cdots p_m}}\frac{1}{n^{(m-1)/2}}\frac{1}{p_1^{np_1}\cdots p_m^{np_m}}\left(\frac{p_m}{p_1}\right)^{x_1}\cdots\left(\frac{p_m}{p_{m-1}}\right)^{x_{m-1}}$$

$$\cdot\left(1+\frac{x_1}{np_1}\right)^{-(np_1+x_1)}\cdots\left(1-\frac{x_1+\cdots x_{m-1}}{np_m}\right)^{-(np_m-x_1\cdots-x_{m-1})}. \tag{7.35}$$

Applying now Taylor's expansion to (7.35)

$$\begin{aligned}\left(1+\frac{x}{np}\right)^{-(np+x)} &= \exp\left(-(np+x)\ln\left(1+\frac{x}{np}\right)\right)\\ &= \exp\left(-(np+x)\left(\frac{x}{np}-\frac{x^2}{2(np)^2}+O(n^{-3})\right)\right)\\ &= \exp\left(-\frac{x^2}{2np}\right)(1+O(1/n)),\end{aligned}$$

we arrive at

$$\begin{aligned}\binom{n}{n\mathbf{p}+\mathbf{x}} &= \frac{1}{(2\pi)^{(m-1)/2}}\frac{1}{\sqrt{p_1\cdots p_m}}\frac{1}{n^{(m-1)/2}}2^{nh} &(7.36)\\ &\cdot\ \left(\frac{p_m}{p_1}\right)^{x_1}\cdots\left(\frac{p_m}{p_{m-1}}\right)^{x_{m-1}}(1+O(1/\sqrt{n}))\\ &\cdot\ \exp\left(-\frac{x_1^2}{2np_1}-\cdots-\frac{x_{m-1}^2}{2np_{m-1}}-\frac{(x_1+\cdots+x_{m-1})^2}{2np_m}\right)\\ &= (1+O(1/\sqrt{n}))\,C\frac{2^{nh}}{n^{(m-1)/2}}\\ &\cdot\ \exp\left(B_1x_1+\cdots+B_{m-1}x_{m-1}\right)\\ &\cdot\ \exp\left(-\frac{1}{2n}\mathbf{x}^T\mathbf{\Sigma}^{-1}\mathbf{x}\right) &(7.37)\end{aligned}$$

where $\mathbf{\Sigma}$ is an appropriately chosen invertible covariance matrix.

We are now in the position to evaluate the sum (7.33). We need to sum over $\mathbf{b}^T\mathbf{x} \leq 0$ which we split by summing over hyperplanes $\mathbf{b}^T\mathbf{x} = -d$ for $d \geq 0$ of dimension $m-2$. We denote such a hyperplane by $\mathcal{D}^{m-2} = \{\mathbf{x} : \ \mathbf{b}^T\mathbf{x} = -d\}$. Noting that the Gaussian kernel of (7.37) when summed over the hyperplane $\mathcal{D}^{m-2}$ is of order $O(n^{(m-2)/2})$ we arrive at our final result. More precisely, plugging (7.37) into (7.33), yields

$$\begin{aligned} A_{n\mathbf{p}} &= \frac{C2^{nh}}{n^{(m-1)/2}}\left(\sum_{\mathbf{b}^T\mathbf{x}\leq 0} \exp\left(\mathbf{b}^T\mathbf{x} - \frac{1}{2n}\mathbf{x}^T\mathbf{\Sigma}^{-1}\mathbf{x}\right)\right) && (7.38) \\ &= \sum_{d\geq 0}\exp(-d)\sum_{\mathbf{b}^T\mathbf{x}=-d}\exp\left(-\frac{1}{2n}\mathbf{x}^T\mathbf{\Sigma}^{-1}\mathbf{x}\right). && (7.39) \end{aligned}$$

Noting now that

$$\sum_{\mathbf{x}\in\mathcal{D}^{m-2}}\exp\left(-\frac{1}{2n}\mathbf{x}^T\mathbf{\Sigma}^{-1}\mathbf{x}\right) \sim C(d)n^{(m-2)/2} \qquad (7.40)$$

where $C(d)$ is of at most polynomial growth of d (in fact, $C(d) = O(d^2)$). Combining (7.39) and (7.40) we finally arrive at

$$\begin{aligned} \log_2 A_{n\mathbf{p}} &\sim \log_2\left(C'\frac{2^{nh}}{n^{(m-1)/2}}n^{(m-2)/2}\right) \\ &= nh - \frac{1}{2}\log_2 n + O(1), && (7.41) \end{aligned}$$

where C' is a constant. Observe that the right order of $A_{n\mathbf{p}}$ can be obtained by considering only the hyperplane $\mathbf{b}^T\mathbf{x} = 0$. In view of (7.26), this completes the proof of Theorem 7.4.

Example 7.1. To illustrate our methodology, we explain it first for $m = 2$ and then we give some details for the case of $m = 3$ symbols with probability $p_1 < p_2 < p_3$. For $m = 2$ we have $(p < 1-p)$

$$\binom{n}{np-x} = \frac{2^{nh}}{\sqrt{2\pi p(1-p)n}}\left(\frac{p}{1-p}\right)^x \exp\left(-\frac{x^2}{2np(1-p)}\right)(1+O(1/n)).$$

Then

$$A_{np} = \sum_{x\geq 0}\binom{n}{np-x} = \frac{1}{1-\frac{p}{(1-p)}}\frac{2^{nh}}{\sqrt{2\pi p(1-p)n}}(1+O(1/n)).$$

Observe again that the order of growth of A_{np} is determined by $x = 0$. The summation of the geometric series contributes to the constant.

Let's now illustrate our calculation for $m = 3$. With $B_1 = \log(p_3/p_1)$ and $B_2 = \log_2(p_3/p_2)$, we need to evaluate

$$A_{np_1,np_2} = \sum_{k_1B_1+k_2B_2 \le np_1B_1+np_2B_2} \binom{n}{k_1, k_2}. \tag{7.42}$$

As before, we denote $k_1 = np_1 + x$ and $k_2 = np_2 + y$ to arrive at

$$\begin{aligned}\binom{n}{np_1+x, np_2+y} &= \frac{1}{\sqrt{2\pi p_1p_2p_3n}} 2^{nh(\mathbf{p})} \left(\frac{p_3}{p_1}\right)^x \left(\frac{p_3}{p_2}\right)^y \\ &\cdot \exp\left(-\frac{x^2}{2np_1} - \frac{y^2}{2np_2} - \frac{(x+y)^2}{2np_3}\right)\left(1 + O(1/\sqrt{n})\right).\end{aligned} \tag{7.43}$$

In Figure 7.2 we show the behavior of the above multinomial coefficient on the critical line $k_1B_1 + k_2B_2 = 0$ and below it. On the critical line the coefficient is well approximated by the normal distribution around the point (np_1, np_2), while for (k_1, k_2) (or equivalently for

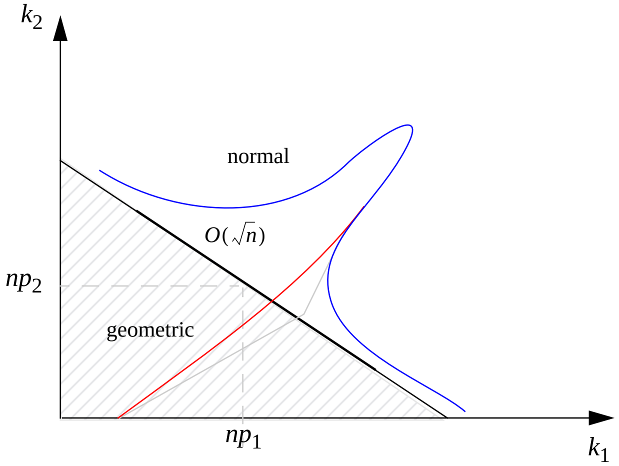


Figure 7.2: Illustration for $m = 3$. The value of the multinomial coefficient (7.43) is shown as the third dimension: The normal distribution is along the line $k_1B_1 + k_2B_2 = np_1B_1 + np_2B_2$, while away from this line the multinomial coefficient decays exponentially.

$(x, y))$ away from the critical line the coefficient decays exponentially. This leads to

$$\begin{aligned} A_{n\mathbf{p}} &= \sum_{B_1x+B_2y\le 0} \binom{n}{np_1+x, np_2+y} \qquad (7.44) \\ &\sim \frac{2^{nh}}{n\sqrt{2\pi p_1p_2p_3}} \sum_{B_1x+B_2y=0} \exp\left(-\frac{x^2}{2np_1} - \frac{y^2}{2np_2} - \frac{(x+y)^2}{2np_3}\right) \\ &= O(\sqrt{n})\frac{2^{nh}}{n} \qquad (7.45) \\ &= C\frac{2^{nh}}{\sqrt{n}}, \end{aligned}$$

where (7.45) follows from the normal approximation on the line $B_1x + B_2y = 0$.

8

Concluding Remarks

In this survey we present precise analyses of several lossless data compression schemes for *known sources* using analytic tools. We start with detailed analysis of Shannon and Huffman codes showing that their asymptotic behavior very much depends on rationality or irrationality of a certain quantity depending of the source parameters. This, among others, explains why since Huffman's code inception we could only find non-matching bounds for its performance.

After discussing fixed-to-variable codes, we move to variable-to-fixed codes such as Tunstall code and its cousin Khodak's VF code. We use sophisticated tools of analytic combinatorics such as Mellin transform and Tauberian theorems to provide detailed and precise analysis. We apply similar tools to study Boncelet VF code where we also investigate a general divide-and-conquer recurrence, a topic of great interest on its own.

At last, we consider variable-to-variable codes such as Khodak code that achieves redundancy decaying faster than linear with the average code length. We also provided explicit construction of a Khodak code. In this chapter we use different analytic methods such as analytic number theory, sequences modulo 1, and geometry of numbers.

Finally, in the last chapter we consider one-to-one codes and use analytic techniques such as the saddle point method to distill precise behavior of a one-to-one code.

We should point out a unique future of this survey. We analyze different lossless data compression schemes using tools of analytic combinatorics such as generating function, Mellin transform, depoissonization, analytic number theory, sequences modulo 1, complex asymptotics, and so on. We coin the term *analytic information theory* for solving problems of information theory using tools of analytic combinatorics and analysis of algorithms. As we mention in the introduction, Andrew Odlyzko opines that "analytic methods are extremely powerful and when they apply, they often yield estimates of unparalleled precision." We have seen it in this survey.

Finally, we should mention what we do not discuss in this survey. As pointed out in many places we focus on lossless data compression schemes for *known sources*, that is, when parameters of sources are known. We delay any discussion of universal source coding to our future book *Analytic Information Theory* which will cover many more topics including minimax redundancy, Markov types, and more.

Acknowledgment

This survey couldn't be written without able help of many of our coauthors: P. Flajolet (INRIA, France), P. Jacquet (Bell Labs, France), N. Merhav (Technion, Israel), Y. Reznik (Qualcom Inc.), S. Savari (Texas A&M, USA), G. Seroussi, S. Verdu (Princeton), M. Weinberger. We thank all of them.

Finally, we would like to thank the Associate Editor D. Neuhoff for many valuable comments that help us to improve the presentation.

References

[1] J. Abrahams. Code and parse trees for lossless source encoding. *Communications in Information and Systems*, 1:113–146, 2001.

[2] M. Akra and L. Bazzi. On the solution of linear recurrence equations. *Computational Optimization and Applications*, (10):195–201, 1998.

[3] J. Allouche and J. Shallit. *Automatic Sequences.* Cambridge University Press, 2008.

[4] N. Alon and A. Orlitsky. A lower bound on the expected length of one-to one codes. *IEEE Trans. Information Theory*, (40):1670–1672, 1994.

[5] T. Apostol. *Introduction to analytic number theory.* Springer, 1976.

[6] K. Atteson. The asymptotic redundancy of bayes rules for markov chains. *IEEE Trans. on Information Theory*, (45):2104–2109, 1999.

[7] R. C. Baker. Dirichlet's theorem on diophantine approximation. *Cambridge Philos.*, (83):37–59, 1978.

[8] A. Barron. Logically smooth density estimation. *Ph.D. Thesis*, (Stanford University):Stanford, CA, 1985.

[9] A. Barron, J. Rissanen, and B. Yu. The minimum description length principle in coding and modeling. *IEEE Trans. Information Theory*, (44):2743–2760, 1998.

[10] J. Bernardo. Reference posterior distributions for bayesian inference. *J. Roy. Stat. Soc. B.*, (41):113–147, 1979.

[11] V. Bernik and M.M. Dodson. *Metric Diophantine approximation on manifolds.* Cambridge University Press, 1999.

[12] P. Billingsley. Statistical methods in markov chains. *Ann. Math. Statistics*, (32):12–40, 1961.

[13] P. Billingsley. Convergence of probability measures. *John Wiley and Sons*, page New York, 1968.

[14] L. Biza. Asymptotically optimal tests for finite markov chains. *Ann. Math. Statistics*, (42):1992–2007, 1971.

[15] C. Boncelet. Block arithmetic coding for source compression. *IEEE Trans. Information Theory*, (39):1546–1554, 1993.

[16] Y. Bugeaud, M. Drmota, and W. Szpankowski. On the construction of (explicit) khodak's code and its analysis. *IEEE Trans. Information Theory*, (54), 2008.

[17] J. W. S. Cassels. An introduction to diophantine approximation. *Cambridge University Press*, 1957.

[18] V. Choi and M. J. Golin. Lopsided trees. *I. Analyses.*, (31):240–290, 2001.

[19] B. Clarke and A. Barron. Information-theoretic asymptotics of bayes methods. *IEEE Trans. Informational Theory*, (36):453–471, 1990.

[20] B. Clarke and A. Barron. Jeffrey's prior is asymptotically least favorable under entropy risk. *J. Stat. Planning Inference*, (41):37–61, 1994.

[21] R. Corless, G. Gonnet, D. Hare, D. Jeffrey, and D. Knuth. On the lambert w function. *Adv. Computational Mathematics*, (5):329–359, 1996.

[22] T. Cover and E. Ordentlich. Universal portfolios with side information. *IEEE Trans. Information Theory*, (42):348–363, 1996.

[23] T. M. Cover and J. A. Thomas. Elements of information theory. *John Wiley and Sons*, (New York), 1991.

[24] I. Csisz and J. Korner. Information theory: Coding theorems for discrete memoryless systems. *Academic Press*, (New York), 1981.

[25] I. Csisz and P. Shields. Redundancy rates for renewal and other processes. *IEEE Trans. Information Theory*, (42):2065–2072, 1996.

[26] L. Davisson. Universal noiseless coding. *IEEE Trans. Inform. Theory*, (19):783–795, 1973.

[27] L. Davisson and A. Leon-Garcia. A source matching approach to finding minimax codes. *IEEE Trans. Inform. Theory*, (26):166–174, 1980.

[28] A. Dembo and I. Kontoyiannis. The asymptotics of waiting times between stationary processes allowing distortion. *Annals of Applied Probability*, (9):413–429, 1999.

[29] A. Dembo and I. Kontoyiannis. Critical behavior in lossy coding. *IEEE Trans. Inform. Theory*, (47):1230–1236, 2001.

[30] A. Dembo and I. Kontoyiannis. Source coding large deviations and approximate pattern matching. *IEEE Trans. Information*, (48):1590–1615, 2002.

[31] H. Dickinson and M. M. Dodson. Extremal manifolds and hausdorff dimension. *Duke Math*, (101):271–281, 2000.

[32] M. Drmota. A bivariate asymptotic expansion of coefficients of powers of generating. *Europ. J. Combinatorics*, (15):139–152, 1994.

[33] M. Drmota, H. K. Hwang, and W. Szpankowski. Precise average redundancy of an idealized arithmetic coding. *Proc. Data Compression Conference*, (Snowbird):222–231, 2002.

[34] M. Drmota, Y. Reznik, S. Savari, and W. Szpankowski. Precise asymptotic analysis of the tunstall code. *2006 International Symposium on Information Theory*, pages 2334–2337, 2006.

[35] M. Drmota, Y. Reznik, and W. Szpankowski. Tunstall code, khodak variations, and random walks. *IEEE Trans. Inform. Theory*, (56):2928 – 2937, 2010.

[36] M. Drmota and W. Szpankowski. Precise minimax redundancy and regrets. *IEEE Trans. Information Theory*, (50):2686–2707, 2004.

[37] M. Drmota and W. Szpankowski. Variations on khodak's variable-to-variable codes. *42nd Annual Allerton Conference on Communication Control Computing*, page Urbana, 2004.

[38] M. Drmota and W. Szpankowski. On the exit time of a random walk with the positive drift. *2007 Conference on Analysis of Algorithms Juan-les-Pins France and Proc. Discrete Mathematics and Theoretical Computer Science*, (291-302), 2007.

[39] M. Drmota and W. Szpankowski. A master theorem for discrete divid and conquer recurrences. *J. of the ACM*, (60):16:1–16:49, 2013.

[40] M. Drmota and R. Tichy. Sequences discrepancies and applications. *Springer Verlag Berlin Heidelberg*, 1997.

[41] Y. Ephraim and N. Merhav. Hidden markov processes. *IEEE Trans. Inform. Theory*, (48):1518–1569, 2002.

[42] F. Fabris. Variable-length-to-variable-length source coding: A greedy step-by-step algorithm. *IEEE Trans. Info. Theory*, (38):1609–1617, 1992.

[43] J. Fan, T. Poo, and B. Marcus. Constraint gain. *IEEE Trans. Information Theory*, (50):1989–2001, 2004.

[44] M. Feder, N. Merhav, and M. Gutman. Universal prediction of individual sequences. *IEEE Trans. Information Theory*, (38):1258–1270, 1992.

[45] P. Flajolet. Singularity analysis and asymptotics of bernoulli sums. *Theoretical Computer Science*, (215):371–381, 1999.

[46] P. Flajolet, X. Gourdon, and P. Dumas. Mellin transforms and asymptotics: Harmonic sums. *Special Volume on Mathematical Analysis of Algorithms*, (144):3–58, 1995.

[47] P. Flajolet and R. Sedgewick. *Analytic Combinatorics*. Cambridge University Press, 2008.

[48] P. Flajolet and W. Szpankowski. Analytic variations on redundancy rates of renewal processes. *IEEE Trans. Information Theory*, (48):2911–2921, 2002.

[49] P. H. Flajolet and A. M. Odlyzko. Singularity analysis of generating functions. *Discrete Math.*, (3):216–240, 1990.

[50] G. H. Freeman. Divergence and the construction of variable-to-variable-length lossless codes by source-word extensions. *Data Comnpression Conference 1993*, pages 79–88, 1993.

[51] R. Gallager. Information theory and reliable communications. *New York Wiley*, 1968.

[52] R. Gallager. Variations on the theme by huffman. *IEEE Trans. Information Theory*, (24):668–674, 1978.

[53] R. Gallager and D. van Voorhis. Optimal source codes for geometrically distributed integer alphabets. *IEEE Trans. Information Theory*, (21):228–230, 1975.

[54] S. Golomb. Run-length coding. *IEEE Trans. Information Theory*, (12):399–401, 1996.

[55] G.Park, H. Hwang, P. Nicodeme, and W. Szpankowski. Profile in tries. *SIAM J. Computing*, (38):1821–1880, 2009.

[56] P. Grabner and J. Thuswaldner. Analytic continuation of a class of dirichlet series. *Abh. Math. Sem. Univ. Hamburg*, (66):281–287, 1996.

[57] R. M. Gray. Optimization noise spectra. *IEEE Trans. Information Theory*, (36):1220–1244, 1990.

[58] D. K. He and E. H. Yang. Performance anaylsis of grammer-based codes revisited. *IEEE Trans. Information Theory*, (50):1524–1535, 2004.

[59] P. Howard and J. Vitter. Analysis of arithmetic coding for data compression. *Proc. Data Compression Conference*, pages 3–12, 1991.

[60] K. H. Hwang. Large deviations for combinatorial distributions i: Central limit theorems. *Ann. Appl. Probab.*, (6):297–319, 1996.

[61] P. Jacquet, C. Knessl, and W. Szpankowski. Counting markov types, balanced matrices, and eulerian graphs. *IEEE Trans. Information Theory*, (58):4261–4272, 2012.

[62] P. Jacquet, G. Seroussi, and W. Szpankowski. On the entropy of a hidden markov process. *Data Compression Conference*, pages 362–371, 2004.

[63] P. Jacquet, G. Seroussi, and W. Szpankowski. On the entropy of a hidden markov process. *Theoretical Computer Science*, (395):203–219, 2008.

[64] P. Jacquet and W. Szpankowski. Analysis of digital tries with markovian dependency. *IEEE Trans. Information Theory*, (37):1470–1475, 1991.

[65] P. Jacquet and W. Szpankowski. Autocorrelation on words and its applicaitons. analysis of suffix trees by string-ruler approach. *Combinatorial Theory Ser A.*, (66):237–269, 1994.

[66] P. Jacquet and W. Szpankowski. Asymptotic behavior ofhte lempel-ziv parsing scheme and digital search trees. *Theoretical Computer Science*, (144):161–197, 1995.

[67] P. Jacquet and W. Szpankowski. Anaylytical depoissonization and its applications. *Theoretical Computer Science*, (201):1–62, 1998.

[68] P. Jacquet and W. Szpankowski. Entropy computations via analytic depoissonization. *IEEE Trans. Information Theory*, (45):1072–1081, 1999.

[69] P. Jacquet and W. Szpankowski. A combinatorial problem arising in information theory: Precise minimax redundancy for markov sources. In *Proc. Colloquium on Mathematics and Computer Science II: Algorithms, Trees, Combinatorics and Probabilities*, pages 311–328. Birkhauser, 2002.

[70] P. Jacquet and W. Szpankowski. Analytic approach to pattern matching applied combinatorics on words. *Cambridge University Press*, page Chapter 7, 2004.

[71] P. Jacquet and W. Szpankowski. Markov types and minimax redundancy for markov sources. *IEEE Trans. Information Theory*, (50):1393–1402, 2004.

[72] P. Jacquet and W. Szpankowski. Joint string complexity for markov sources. In *23rd International Meeting on Probabilistic, Combinatorial and Asymptotic Methods for the Analysis of Algorithms*, pages 1–12, 2012.

[73] P. Jacquet and W. Szpankowski. *Analytic Pattern Matching: From DNA to Twitter*. Cambridge University Press, Cambridge, 2015.

[74] P. Jacquet, W. Szpankowski, and I. Apostol. A universal predictor based on pattern matching. *IEEE Trans. Information Theory*, (48):1462–1472, 2002.

[75] P. Jacquet, W. Szpankowski, and J. Tang. Average profile of hte lempel-ziv parsing scheme for a markovian source. *Algorithmica*, (31):318–360, 2001.

[76] S. Janson. Moments for first passage and last exit times the minimum and related quantities for random walks with positive drift. *Adv. Appl. Probab.*, (18):865–879, 1986.

[77] F. Jelinek and K. S. Schneider. On variable-length-to-block coding. *Trans. Information Theory*, (18):765–774, 1972.

[78] G. Katona and G. Tuesnady. The principle of conservation of entropy in a noiseless channel. *Studia Sci. Math.*, (2):20–35, 1967.

[79] G. L. Khodak. Connection between redundancy and average delay of fixed-length coding. *All-Union Conference on Problems of Theoretical Cybernetics*, (Novosibirsk USSR), 1969.

[80] G. L. Khodak. Bounds of redundancy estimates for word-based encoding of sequences produced by a bernoulli source. *Problemy Peredachi Informacii*, (8):21–32, 1972.

[81] J. C. Kieffer. A unified approach to weak universal source coding. *IEEE Trans. Information Theory*, (24):340–360, 1978.

[82] J. C. Kieffer. Sample converses in source coding theory. *IEEE Trans. Information Theory*, (37):263–268, 1991.

[83] J. C. Kieffer. Strong converses in source coding relative to a fidelity criterion. *IEEE Trans. Information Theory*, (37):257–262, 1991.

[84] C. Knessl and W. Szpankowski. Enumeration of binary trees lempel-ziv '78 parsings and universal types. *Proc. the Second workshop on Analytic Algorithmics and Combinatorics*, page Vancouver, 2005.

[85] D. E. Knuth. The art of computer programming. fundmental algorithms. *Addison-Wesley Reading*, (Vol 1):Third Edition, 1997.

[86] D. E. Knuth. The art of computer programming. seminumerical algorithms. *Addison Esley Reading*, (Vol 2):Third Edition, 1998.

[87] D. E. Knuth. The art of computer programming sorting and searching. *Addison-Wesley Reading*, (Vol 3):Second Edition, 1998.

[88] D. E. Knuth. Linear probing and graphs. *Algorithmica*, (22):561–568, 1998.

[89] D. E. Knuth. Selected papers on the analysis of algorithms. *Cambridge University Press*, 2000.

[90] I. Kontoyiannis. An implementable lossy version of the lempel-ziv algorithm-part i: Optimality for memoryless sources. *IEEE Trans. Information Theory*, (45):2285–2292, 1999.

[91] I. Kontoyiannis. Pointwise redundancy in lossy data compression and universal lossy data compression. *IEEE Trans. Inform. Theory*, (46):136–152, 2000.

[92] I. Kontoyiannis. Sphere-covering measure concentration and source coding. *IEEE Trans. Inform. Theory*, (47):1544–1552, 2001.

[93] I. Kontoyiannis and S. Verdu. Optimal lossless data compression: Non-asymptotics and asymptotics. *IEEE Trans. Information Theory*, (60):777–795, 2014.

[94] J. Korevaar. A century of complex tauberian theory. *Bull. Amer. Soc.*, (39):475–531, 2002.

[95] C. Krattenthaler and P. Slater. Asymptotic redundancies for univeral quantum coding. *IEEE Trans. Information Theory*, (46):801–819, 2000.

[96] R. Krichevsky. Universal compression and retrieval. *Kluwer Dordrecht*, 1994.

[97] R. Krichevsky and V. Trofimov. The performance of universal coding. *IEEE Trans. Information Theory*, (27):199–207, 1981.

[98] L. Kuipers and H. Niederreiter. Uniform distribution of sequences. *John Wiley and Sons*, 1974.

[99] J. Lawrence. A new universal coding scheme for the biary memoryless source. *IEEE Trans. Inform. Theory*, (23):466–472, 1977.

[100] A. Lempel and J. Ziv. On the cojmplexity of finite sequences. *IEEE Information Theory*, (22):75–81, 1976.

[101] T. Linder, G. Lugosi, and K. Zeger. Fixed-rate universal lossy source coding and rates of convergence for memoryless sources. *IEEE Information Theory*, (41):665–676, 1995.

[102] S. Lonardi, W. Szpankowski, and M. Ward. Error resilient lz'77 data compression: Algorithms analysis and experiments. *IEEE Trans. Information Theory*, (53):1799–1813, 2007.

[103] G. Louchard and W. Szpankowski. Average profile and limiting distribution for a phrase size in the lempel-ziv parsing algorithm. *IEEE Trans. Information Theory*, (41):478–488, 1995.

[104] G. Louchard and W. Szpankowski. On the average redundancy rate of the lempel-ziv code. *IEEE Trans. Information Theory*, (43):2–8, 1997.

[105] G. Louchard, W. Szpankowski, and J. Tang. Average profile for the generalized digital search trees and the generalized lempel-ziv algorithms. *SIAM J. Computing*, (28):935–954, 1999.

[106] T. Luczak and W. Szpankowski. A suboptimal lossy data compression based in approximate pattern matching. *IEEE Trans. Information Theory*, (43):1439–1451, 1997.

[107] H. Mahmoud. Evolution of random search trees. *John Wiley and Sons*, 1992.

[108] K. Marton and P. Shields. The positive-divergence and blowing-up properties. *Israel J. Math*, (80):331–348, 1994.

[109] J. Massey. The entropy of a rooted tree with probabilities. In *International Symposium on Information Theory*, 1983.

[110] N. Merhav and M. Feder. A strong version of the redundancy-capacity theory of universal coding. *IEEE Trans. Information Theory*, (41):714–722, 1995.

[111] N. Merhav, M. Feder, and M. Gutman. Some properties of sequential predictors for binary markov sources. *IEEE Trans. Information Theory*, (39):887–892, 1993.

[112] N. Merhav and D. Neuhoff. Variable-to-fixed length codes provided better large deviations performance than fixed-to-variable codes. *IEEE Trans. Information Theory*, (38):135–140, 1992.

[113] N. Merhav, G. Seroussi, and M. Weinberger. Optimal prefix codes for sources with two-sided geometric distributions. *IEEE Trans. Information Theory*, (46):121–135, 2000.

[114] N. Merhav and W. Szpankowski. Average redundancy of the shannon code for markov sources. *IEEE Trans. Information Theory*, (59):7186–7193, 2013.

[115] N. Merhav and J. Ziv. On the amount of statistical side information required for lossy data compression. *IEEE Trans. Information Theory*, (43):1112–1121, 1997.

[116] R. Noble and C.R. Johnson. *Matrix Analysis*. Cambridge University Press, Cambridge, 1985.

[117] A. Odlyzk. Asymptotic enumeration. *Handbook of Cominatorics*, (II):1063–1229, 1995.

[118] A. Orlitsky and P. Santhanam. Speaking of infinity. *IEEE Trans. Information Theory*, (50):2215–2230, 2004.

[119] A. Orlitsky, Prasad Santhanam, and J. Zhang. Universal compression of memoryless sources over unknown alphabets. *IEEE Trans. Information Theory*, (50):1469–1481, 2004.

[120] D. Ornstein and P. Shields. Universal almost sure data compression. *Ann. Probab.*, (18):441–452, 1990.

[121] D. Ornstein and B. Weiss. Entropy and data compression schemes. *IEEE Informaiton Theory*, (39):78–83, 1993.

[122] E. Plotnik, M. J. Weinberger, and J. Ziv. Upper bounds on the probability of sequences emitted by finite-state sources and on the redundancy of the lempel-ziv algorithm. *IEEE Trans. Information Theory*, (38):66–72, 1992.

[123] Y. Reznik and W. Szpankowski. On average redundancy rate of the lempel-ziv codes with k-error protocol. *Information Sciences*, (135):57–70, 2001.

[124] J. Rissanen. Complexity of strings in the class of markov sources. *IEEE Trans. Information Theory*, (30):526–532, 1984.

[125] J. Rissanen. Universal coding and information and prediction and estimation. *IEEE Trans. Information Theory*, (30):629–636, 1984.

[126] J. Rissanen. Fisher information and stochastic complexity. *IEEE Trans. Information Theory*, (42):40–47, 1996.

[127] J. Rissanen and G. Furlan. Context quantization.

[128] B. Ryabko. Twice-universal coding. *Problems of Information Transmission*, pages 173–177, 1984.

[129] B. Ryabko. Prediction of random sequences and universal coding. *Problems of Information Transmission*, (24):3–14, 1988.

[130] B. Ryabko. The complexity and effectiveness of prediction algorithms. *J. Complexity*, (10):281–295, 1994.

[131] S. Savari. Redundancy of the lempel-ziv incremental parsing rule. *IEEE Trans. Information Theory*, (43):9–21, 1997.

[132] S. Savari and R. Gallager. Generalized tunstall codes for sources with memory. *IEEE Trans. Information Theory*, (43):658–668, 1997.

[133] S. A. Savari. Variable-to-fixed length codes for predictable sources. *Proc Ieee Data Compresion Conference*, pages 481–490, 1998.

[134] S. A. Savari. Variable-to-fixed length codes and the conservation of enthropy. *Trans. Information Theory*, (45):1612–1620, 1999.

[135] J. Schalkwijk. An algorithm for source coding. *IEEE Information Theory*, (18):395–399, 1972.

[136] W. M. Schmidt. *Diophantine Approximation.* Springer, 1980.

[137] R. Sedgewick and P. Flajolet. An introduction to the analysis of algorithms. *Addison-Wesley Publishing Company Reading Mass.*, 1995.

[138] G. Seroussi. On universal types. *IEEE Transactions on Informatoin Theory*, (52):171–189, 2006.

[139] P. Shields. Universal redundancy rates do not exist. *IEEE Information Theory*, (39):520–524, 1993.

[140] P. Shields. The ergodic theory of discrete sample path. *American Mathematical Society*, 1996.

[141] Y. Shtarkov. Universal sequential coding of single messages. *Problems of Information Transmission*, (23):175–186, 1987.

[142] Y. Shtarkov, T. Tjalkens, and F. M. Willems. Multi-alphabet universal coding of memoryless sources. *Problems of Information Transmission*, (31):114–127, 1995.

[143] V. G. Sprindzuk. *Metric Theory of Diophantine Approximations.* Wiley, 1979.

[144] R. Stanley. Enumerative combinatorics. *Watsworth Monterey*, 1986.

[145] R. Stanley. Enumerative combinatorics. *Cambridge University Press*, (II), 1999.

[146] Y. Steinberg and M. Gutman. An algorithm for source coding subject to a fidelity criterion based on string matching. *IEEE Trans. Information Theory*, (39):877–886, 1993.

[147] P. Stubley. On the redundancy of optimum fixed-to=variable length codes. *Proc. Data Compression Conference*, pages 90–97, 1994.

[148] B. Sury. Weierstrass's theorem - leaving no stone unturned. In *Workshop on Linear Algebra and Analysis*, 2006.

[149] W. Szpankowski. Asymptotic properties of data compress and suffix trees. *IEEE Trans. Information Theory*, (39):1647–1659, 1993.

[150] W. Szpankowski. A generalized suffix tree and its (un) expected asymptotic behaviors. *SIAM J. Compt.*, (22):1176–1198, 1993.

[151] W. Szpankowski. On asymptotics of certain sums arising in coding theory. *IEEE Trnas. Information Theory*, (41):2087–2090, 1995.

[152] W. Szpankowski. On asymptotics of certain recurrences arising in universal coding. *roblems of Information Transmission*, (34):55–61, 1998.

[153] W. Szpankowski. Asymptotic redundancy of huffman (and other) block codes. *IEEE Trans. Information Theory*, (46):2434–2443, 2000.

[154] W. Szpankowski. *Average Case Analysis of Algorithms on Sequences.* Wiley New York, New York, 2001.

[155] W. Szpankowski. A one-to-one code and its anti-redundancy. *IEEE Trans. Information Theory*, (54):4762–4766, 2008.

[156] W. Szpankowski and S. Verdu. Minimum expected length of fixed-to-variable lossless compression without prefix constraints. *IEEE Trans. Information Theory*, (57):4017–4025, 2011.

[157] T. Tjalkens and F. Willems. A universal variable-to-fixed length source code based on lawrence's algorithm. *IEEE Trans. Information Theory*, (38):247–253, 1992.

[158] B. P. Tunstall. Synthesis of noiseless compression codes. *Ph.D. dissertation*, (Georgia Inst. Technology), 1967.

[159] J. D. Vaaler. Some extremal functions in fourier analysis. *Bull. Amer. Math. Soc.*, (12):183–216, 1985.

[160] B. Vall. Dynamics of the binary euclidean algorithm functional analysis and operators. *Algorithmica*, (22):660–685, 1998.

[161] B. Vall. Dynamical sources in information theory: Fundamental intervals and word prefixes. *Algorithmica*, (29):262–306, 2001.

[162] K. Visweswariah, S. Kulkurani, and S. Verdu. Universal variable-to-fixed length source codes. *IEEE Trans. Information Theory*, (47):1461–1472, 2001.

[163] J. Vitter and P. Krishnan. Optimal prefetching via data compression. *ACM*, (43):771–793, 1996.

[164] M. Ward and W. Szpankowski. Analysis of a randomized selection algorithm motivated by the lz'77 shceme. *the First Workshop on Analytic Algorithmics and Combinatorics*, (New Orleans):153–160, 2004.

[165] M. Weinberger, N. Merhav, and M. Feder. Optimal sequential probability assignments for individual sequences. *IEEE Trans. Information Theory*, (40):384–396, 1994.

[166] M. Weinberger, J. Rissanen, and R. Arps. Applications of universal context modeling to lossless compression of gray-scale images. *IEEE Trans. Image Processing*, (5):575–586, 1996.

[167] M. Weinberger, J. Rissanen, and M. Feder. A universal finite memory sources. *IEEE Trans. Information Theory*, (41):643–652, 1995.

[168] M. Weinberger, G. Seroussi, and G. Sapiro. Loco-i: A low complexity context-based lossless image compression algorithms. *Proc. Data Compression Conference*, pages 140–149, Snowbird 1996.

[169] P. Whittle. Some distribution and moment formulae for markov chain. *J. Roy. Stat. Soc.*, (17):235–242, 1955.

[170] F. M. Willems. the context-tree weighting method: Extensions. *IEEe Trans. Information Theory*, to appear.

[171] F. M. Willems, Y. Shtarkov, and T. Tjalkens. Context weighting for general finite context sources. *IEEE Trans. Information Theory*, (42):1514–1520, 1996.

[172] F. M. Williams, Y. Shtarkov, and T. Tjalkens. The context-tree weighting method: Basic properties. *IEEE Trans. Information Theory*, (41):653–664, 1995.

[173] A. Wyner and J. Ziv. Some asymptotic properties of the entropy of a stationary ergodic data source with applications to data compression. *IEEE Trans. Information Theory*, (35):1250–1258, 1989.

[174] A. D. Wyner. An upper bound on the entropy series. *Inform. Control*, (20):176–181, 1972.

[175] A. D. Wyner. An upper bound on the entropy series. *Informiationa nd Control*, (20):176–181, 1972.

[176] A. J. Wyner. The redundancy and distribution of the phrase lengths of the fixed-database lempel-ziv algorithm. *IEEE Trans. Information Theory*, (43):1439–1465, 1997.

[177] Q. Xie and A. Barron. Minimax redundancy for the class of memoryless souces. *IEEE Trans. Information Theory*, (43):647–657, 1997.

[178] Q. Xie and A. Barron. Asymptotic minimax regret for data compression and gambling and prediction. *IEEE Trans. Information Theory*, (46):431–445, 2000.

[179] E. H. Yang and J. Kieffer. Simple universal lossy data compression schemees derived from lempel-ziv algorithm. *IEEE Trans. Information Theory*, (42):239–245, 1996.

[180] E. H. Yang and J. Kieffer. On the redundancy of the fixed-database lempel-ziv algorithm for mixing sources. *IEEE Trans. Information Theory*, (43):1101–1111, 1997.

[181] E. H. Yang and J. Kieffer. On the performance of data compression algorithms based upon string matching. *IEEE Trans. Information Theory*, page 44, 1998.

[182] E. H. Yang and Z. Zhang. The shortest common superstring problem: Average case analysis for both exact matching and approximate matching. *IEEE Trans. Information Theory*, (45):1867–1886, 1999.

[183] Y. Yang and A. Barron. Informatoin-theoretic determination of minimax rates of convergence. *The Ann. Stat.*, (27):1564–1599, 1999.

[184] Z. Zhang and V. Wei. An on-line universal lossy data compressoin algorithm via continuous codebook reinement part i: Basic results. *IEEE Trans. Information Theory*, (2):803–821, 1996.

[185] J. Ziv. Coding of source with unknown statistics part ii: Distortion relative to a fidelity criterion. *IEEE Trans. Information Theory*, (18):389–394, 1972.

[186] J. Ziv. Variable-to-fixed length codes are better than fixed-to-variable length codes for markov sources. *IEEE Trans. Information Theory*, (36):861–863, 1990.

[187] J. Ziv. Back from infinity: A constrained resouces approach to information theory. *IEEE Information Theory Society Newsletter*, (48):30–33, 1998.

[188] J. Ziv and A. Lempel. A universal algorithm for sequential data compression. *IEEE Trans. Information Theory*, (23):337–343, 1977.

[189] J. Ziv and A. Lempel. Compression of individual sequences via variable-rate coding. *IEEE Trans. Information Theory*, (24):530–536, 1978.

[190] A. Zygmund. *Trigonometric Series.* Cambridge University Press, New York, 1959.