Journal de Théorie des Nombres
de Bordeaux **12** (2000), 531–570

Digits and continuants in Euclidean algorithms. Ergodic versus Tauberian theorems

par Brigitte VALLEE

À Jacques Martinet, meneur d'hommes et de science

Résumé. Nous faisons ici l'analyse en moyenne des principales quantités qui interviennent dans des algorithmes de type Euclide –quotients partiels (chiffres) et continuants–. L'étude de ces paramètres est en particulier essentielle quand on s'intéresse à une mesure très précise (et très réaliste) de la complexité de ces algorithmes, i.e., la complexité en bits, où l'on compte toutes les opérations sur les bits. Nous développons un cadre général pour une telle analyse, où la complexité moyenne est reliée au comportement analytique dans le plan complexe des homographies utilisées par l'algorithme. Nos méthodes sont fondées sur l'utilisation des opérateurs de transfert, objets de base de la théorie des systèmes dynamiques, que nous adaptons à nos besoins. Nous opérons dans un cadre discret, où les théorèmes Taubériens prennent le relais des théorèmes ergodiques. Ainsi, nous obtenons des résultats nouveaux sur la complexité moyenne –mesurée en bits– de toute une classe d'algorithmes de type Euclide, et ce, dans un cadre unificateur.

Abstract. We obtain new results regarding the precise average–case analysis of the main quantities that intervene in algorithms of a broad Euclidean type. We develop a general framework for the analysis of such algorithms, where the average-case complexity of an algorithm is related to the analytic behaviour in the complex plane of the set of elementary transformations determined by the algorithms. The methods rely on properties of transfer operators suitably adapted from dynamical systems theory and provide a unifying framework for the analysis of the main parameters —digits and continuants— that intervene in an entire class of gcd-like algorithms. We operate a general transfer from the continuous case (Continued Fraction Algorithms) to the discrete case (Euclidean Algorithms), where Ergodic Theorems are replaced by Tauberian Theorems.

Manuscrit reçu le 29 février 2000.

1. Introduction

The metric theory of continued fractions has been established by studies of Gauss, Lévy [26], Khinchin [22], Kuzmin [25], Wirsing [40] and Babenko [2]. These authors mainly deal with a specific density transformer that can also be used for studying the main parameters of interest, namely the quotients and the continuants. The quotients play the rôle of digits (in the related numeration system) and the continuants are the denominators of the rational approximations provided by the truncation of the continued fraction. Properties of the density transformer entail the validity of ergodic methods [8], which are both simple and powerful while providing asymptotic estimates that hold almost everywhere.

Thus, such results are not suitable for providing any information on the behaviour of the main parameters that intervene in the continued fraction expansion of a rational number, since rational inputs have zero measure. On the other hand, this particular case of a rational input is quite important in computer science since it is closely related to the average–case analysis of the Euclidean Algorithm.

The discrete counterparts of continued fraction algorithms, i.e., the Euclidean algorithms, have been less extensively studied. There are two major classical Euclidean Algorithms, that are called *Standard* (S), and *Centered* (C). The complexity of these algorithms is now well–understood, but only as regards of the number of arithmetical operations to be performed: The standard Euclidean Algorithm was analysed first in the worst case in 1733 by de Lagny, then in the average-case around 1969 independently by Heilbronn [19] and Dixon [11], and finally in distribution by Hensley [20] who proved in 1994 that the Euclidean algorithm has Gaussian behaviour. The centered algorithm was studied by Rieger [30]. Brent [6, 7] and Vallée [36] have analysed the Binary algorithm. The methods used till the early 1980's are quite varied, since they range from combinatorial (de Lagny, Heilbronn) to probabilistic (Dixon).

The more recent works [20], [35], [37] rely for a good deal on the idea of using *transfer operators*, a far-reaching generalization of density transformers, originally introduced by Ruelle [31, 32] in connection with the thermodynamic formalism and dynamical systems theory [3]. Then Mayer [29, 28] has applied such operators to the continued fraction transformation. Finally, Hensley in his study "in distribution" or Vallée in her analysis of the Binary GCD Algorithm [36], propose new methods where they use these tools, originally well–adapted to continuous models, in the discrete models of Euclidean Algorithms. Recently, these methods are proven to be quite general, and provide a unifying framework for analysing the number of steps of a whole class of Euclidean algorithms [37].

However, until now, many parameters of interest, like digits and continuants, that intervene in Euclidean Algorithm have not been studied by these methods. The average values of digits or continuants play a central rôle in the precise analysis of Euclidean Algorithms. First, the average bit–complexity of Euclidean Algorithms involves expressions where both digits and continuants intervene. Second, the continued fraction expansion of a rational number naturally provides an encoding for integer pairs that uses the digits of the continued fraction expansion. In computer systems that directly deal with continued fraction expansions [4], [39], it is important to analyse the average length of this continued fraction encoding.

In this paper, we provide new analyses of the precise expected values of the main parameters in the discrete framework. We then obtain new results about the average bit-complexity of classical Euclidean algorithms and propose a unifying framework for the analysis of the main parameters of gcd-like algorithms.

Methods. Our approach is a refinement of methods that have been already used [9, 16, 35, 36, 37, 38]: it consists in viewing an algorithm of the gcd type as a dynamical system, where each iterative step is a linear fractional transformation (LFT) of the form $z \to (az + b)/(cz + d)$. A specific set of transformations is then associated to each algorithm. It already appears from previous treatments that the computational complexity of an algorithm is in fact dictated by the collective dynamics of its associated set of transformations. More precisely, two factors intervene: the characteristics of the LFT's in the complex domain and their contraction properties, notably near fixed points.

Technically, this paper relies on a description of relevant parameters by means of generating functions, a by now common tool in the average-case of algorithms [14, 15]. As is usual in number theory contexts, the generating functions are Dirichlet series. They are first proved to be algebraically related to specific operators that encapsulate all the important informations relative to the "dynamics" of the algorithm. Their analytical properties depend on spectral properties of the operators [27], most notably the existence of a "spectral gap" that separates the dominant eigenvalue from the remainder of the spectrum. This determines the singularities of Dirichlet series of costs. The asymptotic extraction of coefficients is then achieved by means of Tauberian theorems [10, 34], a primary tool in multiplicative number theory. Average–case estimates of the main parameters (digits, continuants) finally result. The main thread of the paper is thus adequately summarized by the chain:

$$\text{Euclidean algorithm} \rightsquigarrow \text{Associated transformations} \rightsquigarrow \text{Transfer operator}$$
$$\rightsquigarrow \text{Dirichlet series of costs} \rightsquigarrow \text{Tauberian inversion}$$
$$\rightsquigarrow \text{Average-case complexity.}$$

Results and plan of the paper. Sections 2 and 3 are introductory sections where we recall descriptions of Euclidean Algorithms together with the general ergodic framework that is well-adapted to the case when inputs are random real numbers. Then, in Section 4 (that is the central technical section of the paper), we consider the case where inputs are random rational numbers. There, we develop the line of attack outlined earlier and introduce successively Dirichlet generating functions, transfer operators of the Ruelle type, and the basic elements of Tauberian theory that are adequate for our purposes. The main results of this section are summarized in Theorems 1 and 2: Theorem 1 describes the singularities of generating functions relative to the main parameters; Theorem 2 implies a general criterion for classifying behaviours of mean values relative to digits and continuants

In Section 5, we return to the solutions of our specific problems —the average bit–complexity and the average code–length— that fall as natural consequences of the present framework and are summarized in Theorems 3 and 4. These results involve entropies of both dynamical system,

$$h(\mathcal{S}) = \frac{\pi^2}{6\log 2} \approx 2.37313, \quad h(\mathcal{C}) = \frac{\pi^2}{6\log\phi} \approx 3.41831, \quad \text{with } \phi := \frac{1+\sqrt{5}}{2}$$

that are related to the analysis of continuants, together to three constants relative to binary length of digits, of Khinchin's type; the first one

$$A(\mathcal{S}) = \frac{1}{\log 2}\log\prod_{k=0}^{\infty}(1+\frac{1}{2^k}) \approx 2.25352,$$

intervenes in the analysis of parameters of Standard Algorithm, while the last two

$$A(\mathcal{C}) = 2 + \frac{1}{\log\phi}\log\prod_{k=3}^{\infty}\frac{(2^k-1)\phi^2+2\phi}{(2^k-1)\phi^2-2} \approx 3.11527$$

$$\widetilde{A}(\mathcal{C}) = \frac{1}{\log\phi}\log\prod_{k=1}^{\infty}\frac{2^k\phi^2+\phi}{2^k\phi^2-1} \approx 2.02197$$

intervene in the analysis of parameters of Centered Algorithm, together with a supplementary constant (relative to signs)

$$B(\mathcal{C}) = \frac{\log 2}{\log\phi} - 1 \approx 0.44042.$$

The average–case bit–complexity of both algorithms when applied to random integers less than N is of the form

$$C_N(\mathcal{S}) \sim \frac{\log 2}{h(\mathcal{S})}\,[A(\mathcal{S})+2]\ \log_2^2 N, \quad C_N(\mathcal{C}) \sim \frac{\log 2}{h(\mathcal{C})}\,[A(\mathcal{C})+B(\mathcal{C})+2]\ \log_2^2 N.$$

The average code–length of continued fractions when applied to random integers less than N is of the form

$$B_N(\mathcal{S}) \sim \frac{2\log 2}{h(\mathcal{S})}\,[2A(\mathcal{S})-1]\ \log_2 N, \qquad B_N(\mathcal{C}) \sim \frac{2\log 2}{h(\mathcal{C})}\,[2\widetilde{A}(\mathcal{C})+1]\ \log_2 N.$$

The numerical values for the constants of bit–complexities,

$$C_N(\mathcal{S}) \simeq 1.24237\ \log_2^2 N, \qquad C_N(\mathcal{C}) \simeq 1.12655\ \log_2^2 N,$$

prove the efficiency of Classical Euclidean Algorithms when compared to naive multiplication of numbers whose average bit–complexity is $\log_2^2 N$ on integers less than N. In the same vein, the numerical values for both constants of average code–length,

$$B_N(\mathcal{S}) \simeq 2.04868\ \log_2 N, \qquad B_N(\mathcal{C}) \simeq 2.04557\ \log_2 N,$$

prove the near-optimality of the continued–fraction encodings when compared to the minimal encoding of integer pairs whose average code–length is $2\ \log_2 N$ for integer pairs less than N.

Finally, the paper provides analyses of bit–complexities of other Euclidean Algorithms, like the Binary Algorithm (Theorem 7), the Subtractive Algorithms (Theorem 5) or other algorithms that compute the Jacobi Symbol (Theorem 6).

An extended abstract that summarizes some results of this paper and focuses on analyses of bit–complexities appeared in Proceedings of ICALP'00 [1].

2. Euclidean algorithms

We present here the Euclidean algorithms to be analysed. Then we explain the rôle of the main parameters, digits, and continuants, that appear when analysing bit-complexity. Finally, we describe the costs that will be studied.

2.1. Two Euclidean Algorithms. The standard Euclidean division of v by u ($v \geq u$), of the form $v = au + r$, produces a positive remainder r such that $0 \leq r < u$. The centered division between u and v ($v \geq u/2$), of the form $v = au + \varepsilon r$, with $\varepsilon = \pm 1$ produces a positive remainder r such that $0 \leq r < u/2$. A Euclidean algorithm is associated to each type of division, and they are respectively called the Standard Algorithm (S) and the Centered Algorithm (C).

We denote by $\ell(x)$ the number of bits in the binary representation of the positive integer x, so that $\ell(x) = \lfloor \log_2 x \rfloor + 1$. Then, the bit–cost of a division step, of the form $v = au + \varepsilon r$ is taken to be essentially $\ell(u) \times \ell(a)$, a quantity that we adopt as our bit–complexity measure. [1] It is followed

[1] There are other possible costs for a division, when some other division algorithms are used.

by exchanges which involve numbers u and r, so that the total cost of a step is $\ell(u) \times \ell(a) + \ell(u) + \ell(r)$. In the case of the centered division, there is possibly an additional subtraction (in the case when $\varepsilon = -1$) in order to obtain a remainder in the interval $[0, u/2]$.
When given an input (v_1, v_0), both algorithms perform a certain number p of divisions of the form

$$(1) \qquad v_0 = a_1 v_1 + d_1 v_2, \qquad v_1 = a_2 v_2 + d_2 v_3, \qquad \ldots v_{p-1} = a_p v_p + d_p 0$$

and decomposes the rational $x := (v_1/v_0)$ as $(v_1/v_0) = h_1 \circ h_2 \circ \ldots \circ h_p(0)$, where the h_i's are linear fractional transformations (LFT) of the form $h_i = h_{[a_i,d_i]}$ with $h_{[a,d]}(x) = 1/(a + dx)$. The pair $m := (a, d)$ is called the digit-pair of the LFT. The algorithm then computes the continued fraction expansion of rational $x = (v_1/v_0)$, (CF-expansion for short),

$$(2) \qquad \frac{v_1}{v_0} = \cfrac{1}{a_1 + \cfrac{d_1}{a_2 + \cfrac{d_2}{a_3 + \cfrac{d_3}{\ddots + \cfrac{d_{p-1}}{a_p}}}}}.$$

In both cases, the last non-zero integer v_p is the gcd of the pair (v_1, v_0). The precise form of the possible LFT's depends on the specific algorithm; there exists a special set $\mathcal{F}$ of LFT's in the final step. However, all the other steps use the same set of LFT's that is denoted by $\mathcal{H}$. For the centered algorithm (C), the rational x belongs to $\mathcal{I} = [0, 1/2]$; for the standard algorithm (S), the rational x belongs to $\mathcal{I} = [0, 1]$. Altogether, the rational inputs of each algorithm belong to the basic interval $\mathcal{I} = [0, \rho]$ with $\rho = 1$ or $\rho = 1/2$.

2.2. Bit-complexities related to Euclidean Algorithms. In both cases, when performing p divisions on the input (v_1, v_0), the bit-cost $C(v_1, v_0)$ of the algorithm is a sum of p terms, the i-th term representing the cost of the i-th division and being a product of two factors; the first factor involves the binary length $\ell(v_j)$ of integer v_j (with j possibly equal to i or $i+1$), while the second one involves a cost relative to the i-th LFT to be performed, of the form $c(h_i)$, or of the form $c(m_i)$, where m_i is the digit–pair that defines the LFT h_i. In the sequel (see Remark at the end of Section 4), we will see that we can replace the length $\ell(v)$ of integer v by its logarithm $\log_2(v)$ in base 2 and systematically consider $\log_2(v_i)$ as the first factor to be studied. In contrast, we have to work with the exact cost due to the LFT. Finally, for both algorithms, the studied bit-cost $C(v_1, v_0)$

Algorithm	*Interval $\mathcal{I}$*	*Division*	*Set $\mathcal{H}$ of LFT's*	*Final Set $\mathcal{F}$*	*Cost of the LFT*
(S)	$[0,1]$	$v = au + r$ $0 \le r < u$	$\{\frac{1}{a+x}, a \ge 1\}$	$a \ge 2$	$\ell(a) + 2$
(C)	$[0, \frac{1}{2}]$	$v = au + \varepsilon r$ $a \ge 2, \varepsilon = \pm 1,$ $0 \le r < \frac{u}{2}$	$\{\frac{1}{a+\varepsilon x}, a \ge 2,$ $\varepsilon = \pm 1,$ $(a, \varepsilon) \neq (2, -1)\}$	$\varepsilon = +1$	$\ell(a) + 2 + \frac{1-\varepsilon}{2}$

FIGURE 1. The Euclidean algorithms.

of the algorithm on the input (v_1, v_0) will be of the form

$$C(v_1, v_0) = \sum_{i=1}^{p} \log_2(v_i) \times c(m_i). \tag{3}$$

The array of Figure 1 describes the precise forms of the divisions, the generic set $\mathcal{H}$ of associated LFT's, the final set $\mathcal{F}$ and the cost of the LFT's.

It is also quite useful to describe the bit–complexity of so–called Extended Euclidean Algorithms, that compute at the same time Bezout coefficients of pair (v_1, v_0), i.e., integers r and s such that $rv_0 + sv_1 = \gcd(v_1, v_0) = v_p$. The principle is well-known, and the computation makes use of two auxiliary sequences r_i and s_i that satisfy for each index i the relation $r_i v_0 + s_i v_1 = v_i$, so that for $i = p$, the Bezout relation holds with $r := r_p$ and $s := s_p$. The sequences are initialized as $r_0 = 1, s_0 = 0, r_1 = 0, s_1 = 1$, then they are built with the help of sequence a_i,

$$d_i r_{i+1} = r_{i-1} - a_i r_i, \qquad d_i s_{i+1} = s_{i-1} - a_i s_i, \tag{4}$$

in the same way as the sequence v_i. The supplementary bit-cost due to the extension of the algorithm is thus a sum of $p-1$ terms, the i-th term representing the cost of the two multiplications of the i-th step described in (4), and being a product of two factors; the first factor involves the binary lengths $\ell(|r_i|), \ell(|s_i|)$ of integers r_i, s_i while the second one involves a cost $c(m_i)$ relative to the i-th digit–pair $m_i := (a_i, d_i)$. Finally, for the same reasons as previously (that we shall explain at the end of Section 4), the studied bit-cost $D(v_1, v_0)$ of both Extended algorithms on the input (v_1, v_0) will be of the form

$$D(v_1, v_0) = \sum_{i=1}^{p-1} [\ \log_2(|r_i|) + \log_2(|s_i|) + \log_2(v_i)\ ] \ \times c(m_i), \tag{5}$$

where the cost $c(m_i)$ is defined in Figure 1.

We are finally interested in describing the length of the binary word that encodes the pair (v_1, v_0). There are two ways for coding this pair: the first one directly uses the binary encoding $A(v_1, v_0)$ of integer pair (v_1, v_0), while the second one deals with the binary encoding $B(v_1, v_0)$ of the sequence of digits $(m_1, m_2, \ldots, m_p)$. It is important to compare the average length of these two coding words, since, in some applications that use CF-expansions in an extensive way, it may be useful to encode efficiently the sequence of CF–digits, so that this encoding can be directly used in further computations. Classical results in Information Theory entail that the mean value of $B(v_1, v_0)$ is at least equal to the mean value of $A(v_1, v_0)$. This leads us to study the length of the CF-encoding of a pair (v_1, v_0),

$$B(v_1, v_0) := \sum_{i=1}^{p} c(m_i), \tag{6}$$

related to some digit–cost c, as well as to try and find near–optimal encodings.

2.3. Main parameters for the analysis of Euclidean Algorithms. The costs to be studied, defined in (3), (5), (6), involve five main parameters: the integer p, the costs $c(m)$ of digit–pairs, and the logarithms of integers v_i defined in (1), together with the logarithms of integers $|r_i|, |s_i|$ defined in (4). The first parameter is exactly the depth of the continued fraction expansion of v_1/v_0, or the number of divisions to be performed by the algorithm on input (v_1, v_0). Its average behaviour is now well-known. The cost $c(m)$ of the digit–pair $m = (a, d)$ may involve the digit a alone or the digit d alone, or both. More generally, it is interesting to study the random behaviour of other functions of digit–pair $m = (a, d)$.

Finally, the integers v_i, r_i, s_i are related to continuants. When one "splits" the CF-expansion (2) of v_1/v_0 at depth i, one obtains two CF-expansions

(7)

$$\cfrac{1}{a_1 + \cfrac{d_1}{a_2 + \cfrac{d_2}{a_3 + \cfrac{d_3}{\ddots + \cfrac{d_{i-1}}{a_i}}}}}, \qquad \cfrac{1}{a_{i+1} + \cfrac{d_{i+1}}{a_{i+2} + \cfrac{d_{i+2}}{a_{i+3} + \cfrac{d_{i+3}}{\ddots + \cfrac{d_{p-1}}{a_p}}}}},$$

defining a rational number: the left part defines the "beginning rational" of the form

$$p_i/q_i := h_1 \circ h_2 \circ \ldots \circ h_i(0) \qquad \text{with } (p_i, q_i) \text{ coprime}, \tag{8}$$

while the right part defines the "ending rational" of the form

$$u_i/w_i := h_{i+1} \circ h_2 \circ \ldots \circ h_k(0) \qquad \text{with } (u_i, w_i) \text{ coprime}. \tag{9}$$

The beginning rationals p_i/q_i are useful for approximating the rational v_1/v_0; their numerators p_i, and their denominators q_i are called beginning

No	*Name*	*Definition*	*Type*	*Characteristics*
1	$S[c]$	$S[c](x) := \sum_{i=1}^{p(x)} c(m_i(x))$	Digit-cost	Rational x
2	Q	$Q(x) := \sum_{i=1}^{p(x)} \log q_i(x)$	Continuant	Rational x
3	W	$W(x) = \sum_{i=1}^{p(x)} \log w_i(x)$	Continuant	Rational x
4	$K[c]$	$K[c](x) := \sum_{i=1}^{p(x)} c(m_i(x)) \ \log w_i(x)$	Mixing	Rational x
5	$L[c]$	$L[c](x) := \sum_{i=1}^{p(x)} c(m_i(x)) \ \log q_i(x)$	Mixing	Rational x
6	V	$V(u,v) := \sum_{i=1}^{p(u,v)} \log v_i(u,v)$	Continuant	Integer-pair (u,v)
7	$M[c]$	$M[c](u,v) := \sum_{i=1}^{p(u,v)} c(m_i(u,v)) \ \log v_i(u,v)$	Mixing	Integer-pair (u,v)

FIGURE 2. The main costs to be studied.

continuants. They are closely related to sequences r_i and s_i that appear in the Extended Euclidean Algorithms, via the relations $p_i = |r_{i+1}|, q_i = |s_{i+1}|$. The ending continuants, i.e., the denominators w_i of the ending rationals u_i/w_i are closely related to the integers v_i that appear in the execution (1) of Euclidean algorithm on input v_1/v_0, via the relation $v_i = \gcd(v_1, v_0)\ w_i$.

When given a valid input (u, v) relative to some Euclidean Algorithm, we wish to study the behaviour of seven quantities, that fully describe the cost relative to some parameter during the execution of a Euclidean Algorithm on input (u, v). These quantities define what we call generic costs and are listed in Figure 2.

The first five quantities (1–5) of Figure 2 are expressed only in terms of depth, digits and continuants. Since the depth p, the sequence of digit-pairs $m_i = (a_i, d_i)$ and the sequence of continuants q_i or w_i only depend on rational $x := (u/v)$ and not on the pair (u, v) itself, these quantities define functions of the rational $x = (u/v)$. The first one is relative to some digit–cost defined on the sequence of digit–pairs $m_1, m_2, \dots m_p$ that appear in the continued fraction expansion of x. The second and the third ones are relative to (beginning or ending) continuants, and the fourth and fifth involve a mixing between digits and (ending or beginning) continuants w_i

or q_i. All these costs can also be viewed as functions defined on pairs on integers that we denote in the same way,

$$X(u,v) := X(\frac{u}{v}), \qquad \text{for} \quad X \in \{p, m, S[c], Q, W, K[c], L[c]\}$$

Finally, the last two quantities (6–7) to be studied involve the sequence of integers v_i that appear in the execution of Euclidean Algorithm. They depend on the pair (u,v) itself, not only on the ratio (u/v) but also on the gcd $r(u,v)$. The relation between v_i and w_i, i.e., $v_i(u,v) = r(u,v)\ w_i(u,v)$ entails that V and $M[c]$ are respectively related to W and $K[c]$,

$$\begin{aligned} V(u,v) &= p(u,v)\ \log r(u,v) + W(u,v), \\ M[c](u,v) &= \log r(u,v)\ S[c](u,v) + K[c](u,v). \end{aligned} \tag{10}$$

2.4. Average values of costs. Here, $\mathcal{I}$ denotes the basic interval. We consider the following sets

$$\widetilde{\Omega} := \{(u,v);\ \frac{u}{v} \in \mathcal{I}\}, \quad \Omega := \{(u,v); \gcd(u,v) = 1, \frac{u}{v} \in \mathcal{I}\}, \tag{11}$$

$$\widetilde{\Omega}_N := \{(u,v) \in \widetilde{\Omega}, v \le N\}, \qquad \Omega_N := \{(u,v) \in \Omega, v \le N\}, \tag{12}$$

for the possible inputs of a Euclidean algorithm. Remark that set Ω_N can be viewed as the set of irreducible rationals with denominator less than N. We denote by $X(u,v)$ one of the generic costs that are defined in Figure 2. We wish to study the mean value of X on Ω_N and $\widetilde{\Omega}_N$ that we denote by $E_N[X]$ or $\widetilde{E}_N[X]$. More precisely, we aim to evaluate the asymptotic behaviour (for $N \to \infty$) of the mean values

$$\begin{aligned} E_N[X] &= \frac{X_N}{|\Omega_N|}, \quad \text{with} \quad X_N := \sum_{(u,v)\in\Omega_N} X(u,v) \\ \widetilde{E}_N[X] &= \frac{\widetilde{X}_N}{|\widetilde{\Omega}_N|}, \quad \text{with} \quad \widetilde{X}_N := \sum_{(u,v)\in\widetilde{\Omega}_N} X(u,v). \end{aligned} \tag{13}$$

We will prove in the sequel that it is sufficient to study the first five costs (1–5) defined in Figure 2 that are relative to rational numbers. The next section analyses these costs when x is real, and gives some indications on what can be expected in the rational case.

3. Continued Fraction Algorithms. Symbolic Dynamics and Ergodic Theorems

We now relate Euclidean algorithms with continued fractions algorithms that can be viewed as continuous extensions of them. Continued fractions algorithms are important particular cases of what is usually called "expanding maps of the interval" in symbolic dynamics framework. Symbolic dynamics concerns itself with the interplay between properties of the transformation and discrete properties of trajectories of points under iteration of the transformation. There, ergodic theorems are very useful to study the main parameters of interest, when x is almost any real of the interval.

We adopt here an analytic point of view, with hypotheses stronger than usual, which entails easier proofs and is well–adapted to continued fraction systems.

3.1. Piecewise analytic maps of the interval. Here, we restrict ourselves to the particular case where the transformation is piecewise analytic.

Definition 1. [Piecewise analytic maps of the interval] *Let $\mathcal{I}$ be a real interval. A mapping $U : \mathcal{I} \to \mathcal{I}$ is piecewise analytic if there exists a (finite or denumerable) set $\mathcal{M}$, whose elements are called digits, and a partition $\{\mathcal{I}_j\}_{j\in\mathcal{M}}$ of the interval $\mathcal{I}$ in subintervals $\mathcal{I}_j$ such that the function $x \to Ux$ maps analytically each $\mathcal{I}_j$ onto $\mathcal{I}$.*

A piecewise analytic map thus consists of denumerably many branches indexed by some set $\mathcal{M}$. We let $M(x) \in \mathcal{M}$ represent the index j of the subinterval $\mathcal{I}_j$ where x falls. A coding of a real number x is then obtained by the sequence of digits of the successive iterates of x,

$$(m_1, \dots, m_k, \dots) \qquad \text{with} \qquad m_i := M(U^i x). \tag{14}$$

Here powers denote iteration, $U^2 = U \circ U$, etc. The sequence of digits of x is then produced by the following simple algorithm.

Procedure Expansion (x)
  for $k := 1$ **to** $+\infty$ **do**
    $m_k := M(x)$; $x := Ux$;

A special rôle is played by the set $\mathcal{H}$ of branches of the inverse function U^{-1} of U that are also naturally numbered by the index set $\mathcal{M}$: we denote by $h_{[m]}$ the inverse of the restriction $U|_{\mathcal{I}_m}$. If $x_k := U^k(x_0)$ and the sequence $m = (m_1, \dots, m_k)$ of the first k digits are known, the algorithm can be run backwards, and the original x_0 is recovered by

$$x_0 = h(x_k) \quad \text{where} \quad h(y) = h_{[m_1]} \circ h_{[m_2]} \circ \cdots \circ h_{[m_k]}(y).$$

The semi-group $\mathcal{H}^\star := \cup_k \mathcal{H}^k$ generated by $\mathcal{H}$ is the set of all finite compositions $h_{[m_1]} \circ h_{[m_2]} \circ \cdots \circ h_{[m_k]}$; the length of the decomposition of h is called the depth of h and denoted by $|h|$.

The scheme (14) generalizes the usual binary representation of real numbers and it constitutes also a very convenient framework for a discussion of continued fraction algorithm.

3.2. Ergodicity and Ergodic Theorem. We recall here some classical definitions cast in our particular framework. Here, $\mathcal{I}$ denotes a real interval endowed with its Lebesgue measure dt. We consider here another measure μ with a continuous density g, so that $d\mu(t) = g(t)dt$.

Definitions 2. [U-invariant measure] *Let U be a measurable mapping $U : \mathcal{I} \to \mathcal{I}$. The measure μ is said to be U–invariant if, for any subinterval $\mathcal{J} \subset \mathcal{I}$, one has $\mu(U^{-1}\mathcal{J}) = \mu(\mathcal{J})$.*
[Ergodicity] *Let U be a measurable mapping $U : \mathcal{I} \to \mathcal{I}$ and μ be a U–invariant measure. The triple $(\mathcal{I}, U, \mu)$ is ergodic if, for any subinterval $\mathcal{J} \subset \mathcal{I}$ such that $U^{-1}(\mathcal{J}) \subset \mathcal{J}$, one has $\mu(\mathcal{J}) = 0$ or 1.*
[Strongly mixing] *Let U be a measurable mapping $U : \mathcal{I} \to \mathcal{I}$ and μ be a U–invariant measure. The triple $(\mathcal{I}, U, \mu)$ is strongly mixing if, for any subinterval $\mathcal{J}, \mathcal{K} \subset \mathcal{I}$, one has $\lim_{n\to\infty} \mu(\mathcal{J} \cap U^{-n}\mathcal{K}) = \mu(\mathcal{J})\mu(\mathcal{K})$.*

Naturally, the mixing property implies the ergodic property.

Ergodic Theorems relate two different kinds of means relative to a function f: the mean value of f along an orbit of the form $(x, Ux, U^2x, \dots U^n x, \dots)$ and the mean value of f relative to measure μ.

Birkhoff's Ergodic Theorem. *Let $(\mathcal{I}, U, \mu)$ be ergodic. Then, for any $f \in \mathcal{L}^1(\mathcal{I})$, one has, for almost all x of $\mathcal{I}$,*

$$\lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n-1} f(U^i x) = \int_{\mathcal{I}} f(t)\, d\mu(t). \tag{15}$$

3.3. Strongly expanding maps of the interval and ergodicity. Clearly, the stochastic behaviour of a numbering system is closely related to the dynamics of map U on the interval $\mathcal{I}$; this dynamics is itself isomorphic to the dynamics of the semigroup $\mathcal{H}^\star$ that is generated by the set $\mathcal{H}$ of inverse branches. We now consider an important class of maps U for which this dynamics is well understood: the case of the (strongly) expanding maps.

Definition 3. [Strongly expanding maps of the interval] *Let $\mathcal{I}$ be a real interval, and let $U : \mathcal{I} \to \mathcal{I}$ be a piecewise analytic mapping whose set of inverse branches is denoted by $\mathcal{H}$. The mapping U is strongly expanding if there exist an open disk $\mathcal{V}$ whose closure contains the interval $\mathcal{I}$ and a real $\alpha < 2$ such that the following holds:*
(a) every $h \in \mathcal{H}$ has an analytic continuation on $\mathcal{V}$;
(b) h maps the closure $\bar{\mathcal{V}}$ of disk $\mathcal{V}$ inside $\mathcal{V}$;
(c) For any $h \in \mathcal{H}$, the absolute value $|h'|$ of the derivative has an analytic continuation on $\mathcal{V}$ denoted by $\widetilde{h}$;

(*d*) *For any* $h \in \mathcal{H}$*, the supremum* $\delta(h) := \sup\{|\widetilde{h}(z)|, z \in \mathcal{V}\}$ *satisfies* $\delta(h) < 1$ *and the series* $\sum_{h\in\mathcal{H}} \delta(h)^{\alpha/2}$ *converges.*

Remark 1. The quantity $\delta := \sup\{\delta(h), h \in \mathcal{H}\}$ satisfies $\delta < 1$ and defines the contraction ratio. The map U is called expanding since the derivative satisfies $|U'(x)| \geq (1/\delta) > 1$. When there exists some integer $k \geq 1$ for which U^k is strongly expansive, then U is called eventually strongly expanding. The triple $(\mathcal{V}, \alpha, \delta)$ that intervenes in Definition 3 is called the triple of U.

Remark 2. The map U is called *strongly* expanding because of two assumptions: (*i*) the various analytic continuations of h and $|h'|$ on some disk $\mathcal{V}$ that *strictly* contains interval $\mathcal{I}$, (*ii*) the fact that the real α is *strictly* less 2.

We state now the important and classical result that shows that a strongly expanding map of the interval is strong mixing (and thus ergodic) with respect to its (unique) invariant measure.

Theorem. *Let U be an eventually strongly expanding map of $\mathcal{I}$. Then there is a unique U–invariant measure μ. Moreover, the triple $(\mathcal{I}, U, \mu)$ is strongly mixing (thus ergodic) and the measure μ is of form $d\mu = \psi(t)dt$ where ψ is analytic on the neighborhood $\mathcal{V}$ of $\mathcal{I}$.*

The main tool used in the proof is the Perron-Frobenius operator that we now introduce.

3.4. The Perron-Frobenius operator relative to a strongly expanding map. As previously, the set $\mathcal{H}$ denotes the set of inverse branches of U. The Perron-Frobenius operator $\mathbf{H}$ relative to $\mathcal{H}$, together with its component operators $\mathbf{R}_h$ relative to each inverse branch h, is defined as follows:

$$\begin{aligned} &\mathbf{R}_h[f](z) := \widetilde{h}(z)\, f \circ h(z), \\ &\mathbf{H} := \sum_{h\in\mathcal{H}} \mathbf{R}_h, \qquad \mathbf{H}[f](z) = \sum_{h\in\mathcal{H}} \widetilde{h}(z)\, f \circ h(z). \end{aligned} \tag{16}$$

First, the operator $\mathbf{H}$ is a density transformer, i.e.,

$$\begin{aligned} \int_{\mathcal{I}} \mathbf{H}[f](x)dx = \sum_{h\in\mathcal{H}} \int_{\mathcal{I}} |h'(x)| f \circ h(x) dx &= \sum_{h\in\mathcal{H}} \int_{h(\mathcal{I})} f(x)dx \\ &= \int_{\mathcal{I}} f(x)dx. \end{aligned} \tag{17}$$

Second, the n-th iterate of $\mathbf{H}$ describes what happens during the n-th iteration of mapping U. Multiplicative properties of the derivative entail that the n-th iterate of $\mathbf{H}$ involves all the inverse branches of depth n,

$$\text{(18)}\qquad \begin{aligned} &\mathbf{H}^n[f](z) = \sum_{h\in\mathcal{H}^n} \widetilde{h}(z) f\circ h(z),\\ &\int_{\mathcal{I}} f(U^n(t))\ g(t)dt = \int_{\mathcal{I}} f(t)\ \mathbf{H}^n[g](t)dt. \end{aligned}$$

If U is strongly expanding, we can prove the following. Denote by $\mathcal{A}_\infty(\mathcal{V})$ the set formed with functions f that are analytic on $\mathcal{V}$ and continuous on $\bar{\mathcal{V}}$. Endowed with the sup-norm, this set is a Banach space and each component operator $\mathbf{R}_h$ is a composition operator. This type of operators was extensively studied by Shapiro [33] who proves that, under assumptions $(a),(b),(c)$, they act on $\mathcal{A}_\infty(\mathcal{V})$, are compact, and even nuclear in the sense of Grothendieck [17, 18]. Under condition (d), the operator $\mathbf{H}$ itself acts on $\mathcal{A}_\infty(\mathcal{V})$, is compact and nuclear. Furthermore, the operator $\mathbf{H}$ has positive properties that entail (via Theorems of Perron–Frobenius type due to Krasnoselsky [24]) the existence of dominant spectral objects: there exist a unique dominant eigenvalue λ strictly positive, a dominant eigenfunction denoted by ψ, strictly positive on $\mathcal{V}\cap\mathbf{R}$ and a dominant projector E. Under normalization condition $E[\psi]=1$, these last two objects are unique too. Then, compacity entails the existence of a spectral gap between the dominant eigenvalue and the remainder of the spectrum. Since $\mathbf{H}$ is a density transformer, the dominant eigenvalue satisfies $\lambda = 1$ and the dominant projector satisfies $E[f] = \int_{\mathcal{I}} f(t)dt$. Then the dominant eigenvector ψ is also an invariant function under $\mathbf{H}$ and the measure μ defined as $d\mu(t) = \psi(t)dt$ is U–invariant. Finally, the decomposition

$$\text{(19)}\qquad \mathbf{H}^n[f](x) = \psi(x)\,(\int_{\mathcal{I}} f(t)dt) + \mathbf{N}^n[f](x)\psi(x)$$

where the operator $\mathbf{N}$ relative to the remainder of the spectrum (cf a precise definition in [27]) has a spectral radius strictly less than 1, proves that

$$\lim_{n\to\infty} \mathbf{H}^n[g](x) = \psi(x)\ \int_{\mathcal{I}} g(t)dt,$$

with exponential speed, and ψ is also the the limit density on $\mathcal{I}$ when map U is iterated many times. Furthermore, the equalities,

$$\begin{aligned} \int_{\mathcal{I}} f(U^n t)\, g(t)dt &= \int_{\mathcal{I}} f(t)\, \mathbf{H}^n[g](t)dt\\ &= \int_{\mathcal{I}} f(t)[\,\psi(t)(\int_{\mathcal{I}} g(u)du) + \mathbf{N}^n[g](t)\,]dt\\ &= (\int_{\mathcal{I}} f(t)\psi(t)dt)\ (\int_{\mathcal{I}} g(u)du) + \int_{\mathcal{I}} f(t)\mathbf{N}^n[g](t)dt \end{aligned}$$

when applied to $g := \mathbf{1}_{\mathcal{J}}\,\psi$ and $f := \mathbf{1}_{\mathcal{K}}$ for some subintervals $\mathcal{J}, \mathcal{K}$ entail that measure μ defined by $d\mu(t) := \psi(t)dt$ is strong mixing (with exponential speed) and thus ergodic.

Remark. We only need in the previous proof a weak form of condition (d), i.e., the fact that the series $\sum_{h\in\mathcal{H}} \delta(h)^{\alpha/2}$ converges for $\alpha = 2$. However, the strong form of condition (d) (i.e., $\alpha < 2$) will be quite important for the sequel, particularly in Section 4.5.

3.5. Some important asymptotic mean values. Since function ψ is also the limit density on $\mathcal{I}$ when the map U is iterated many times, the mean values relative to μ can be also considered as asymptotic mean values and denoted by E_∞. Here, we give some important asymptotic mean values that play a central rôle in the sequel. They are relative to digits or to entropy of the dynamical system. If M denotes the numbering function, and c denotes a cost–digit function $c : \mathcal{M} \to \mathbf{R}^+$, then the asymptotic mean value of $c \circ M$ is

$$\begin{aligned} (20)\quad E_\infty[c(M)] := \int_{\mathcal{I}} c(M(t))\,\psi(t)dt &= \sum_{h\in\mathcal{H}} \int_{h(\mathcal{I})} c\circ M(t)\,\psi(t)dt \\ &= \sum_{m\in\mathcal{M}} c(m) \int_{h_{[m]}(\mathcal{I})} \psi(t)dt. \end{aligned}$$

The entropy $h(\mathcal{H})$ of the dynamical system is defined as the limit, if it exists, of a quantity that involves measures u_g of intervals $g(\mathcal{I})$, (for $g \in \mathcal{H}^\star$)

$$h(\mathcal{H}) := \lim_{n\to\infty} \frac{-1}{n} \sum_{g\in\mathcal{H}^n} u_g \log u_g.$$

Via a classical formula due to Rohlin, the entropy is related to the asymptotic mean value of $\log|U'|$

$$(21)\qquad E_\infty[\log|U'|] := \int_{\mathcal{I}} \log|U'(t)|\,\psi(t)dt = h(\mathcal{H}).$$

In the sequel, we describe the numeration systems relative to continued fractions, the standard continued fraction system and the centered continued fraction. In both cases, we obtain real extensions of Euclidean algorithms that give rise to expanding maps where the ergodic framework can be used.

3.6. Standard and centered continued fraction expansions. The continued fraction systems fit into the general framework of piecewise analytic maps of interval. In the basic case, the system is defined from the integer part function denoted by $x \to \lfloor x \rfloor$ and the fractional part function $x \to \{x\} := x - \lfloor x \rfloor$. It is described by the quadruple $(\mathcal{I}, U, m, \mathcal{H})$

$$\mathcal{I} = [0,1],\ U(x) = \left\{\frac{1}{x}\right\},\ m(x) = \left\lfloor \frac{1}{x} \right\rfloor,\ \mathcal{H} := \{h(z) = \frac{1}{a+z} \quad a \geq 1\}.$$

We also let $U(0) = 0, 1/0 = 0$. Centered continued fractions are obtained when one replaces truncation (integer part function) by rounding to the nearest integer $x \to [[x]]$. First introduce the notations

$$[[y]] = \left\lfloor x + \frac{1}{2} \right\rfloor,\ \{\{y\}\} = |y - [[y]]|\,,\ \varepsilon(y) = \mathrm{sign}(y - [[y]]),$$

so that the following identity holds:

$$y = [[y]] + \varepsilon(y)\{\{y\}\}.$$

Then, the centered continued fraction system is defined by the quadruple $(\mathcal{I}, U, m, \mathcal{H})$ given by

$$\mathcal{I} = [0, \frac{1}{2}],\ U(x) = \{\{\frac{1}{x}\}\},\ a(x) = [[\frac{1}{x}]],\ d(x) = \varepsilon(\frac{1}{x}),$$

$$\mathcal{H} := \left\{ h(z) = \frac{1}{a+dz} \quad a \geq 2, d = \pm 1 \quad (a,d) \neq (2,-1) \right\}.$$

with, conventionally, $U(0) = 0$, $m(0) = 0$, $1/0 = 0$.

These numeration systems provide a sequence of digits according to scheme (14) and thus continued fractions expansions, that are generally infinite. When applied to a rational x, these expansions are finite and coincide with continued fraction expansions of Section 2. In this sense, continued fractions systems can be viewed as extensions of Euclidean Algorithms, and in both cases, the rational numbers are exactly the real numbers for which the continued fraction expansion is finite. A number x is rational if and only if there exists an element h of the semi-group $\mathcal{H}^\star$ for which $x = h(0)$.

3.7. Applications of Ergodic Theorem to continued fractions systems. It is clear that both continued fraction systems are related to (eventually) strongly expanding maps. Then, the Ergodic Theorem applies to CF-expansions, and classical results entail that the invariant measure μ is of the form $d\mu(t) = \psi(t)dt$ with

$$\psi_S(t) = \frac{1}{\log 2}\frac{1}{1+t}, \qquad \psi_C(t) = \frac{1}{\log\phi}[\frac{1}{\phi+t} + \frac{1}{\phi^2 - t}].$$

The first result was conjectured by Gauss, then proven by Lévy [26]. The second result was established by Rieger [30]. The related distribution functions are

$$F_S(x) = \frac{1}{\log 2}\log\frac{1}{1+x}, \qquad F_C(x) = \frac{1}{\log\phi}\log\frac{\phi(\phi+x)}{\phi^2 - x}.$$

We consider now some asymptotic mean values that play a central rôle in the sequel. The following results are classical and can be found for instance in [5].

Digit–costs. Consider some particular digit–cost $c : \mathcal{M} \to \mathbf{R}^+$ such that $c \circ M$ is in $\mathcal{L}^1$. If $c(m)$ equals for instance the binary length of digit a, i.e., the number of binary digits in the binary expansion of digit a, one has, with general formula (20),

$$A(\mathcal{S}) := E_\infty^{[\mathcal{S}]}\,[\ell(a)] = \frac{1}{\log 2} \log \prod_{k=0}^{\infty} (1 + \frac{1}{2^k}) \approx 2.25352 \tag{22}$$

$$A(\mathcal{C}) := E_\infty^{[\mathcal{C}]}\,[\ell(a)] = 2 + \frac{1}{\log \phi} \log \prod_{k=3}^{\infty} \frac{(2^k-1)\phi^2 + 2\phi}{(2^k-1)\phi^2 - 2} \approx 3.11527. \tag{23}$$

In the case of centered continued fractions, when digit–cost equals the sign ε, one obtains

$$B(\mathcal{C}) := \Pr_\infty[\varepsilon = -1] = E_\infty^{[\mathcal{C}]}\,[\frac{1-\varepsilon}{2}] = \frac{1}{\log \phi}\ \log \frac{\phi}{2} \approx 0.44042. \tag{24}$$

Then Ergodic Theorems prove that, in both cases, and for almost all x in $\mathcal{I}$,

$$\lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n} \ell(a_i(x)) = E_\infty\,[\ell(a)] \qquad\qquad \lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n} \frac{1-\varepsilon_i(x)}{2} = E_\infty\,[\frac{1-\varepsilon}{2}].$$

Entropy. The variable $x \to |\log x|$ is quite important too, since the asymptotic mean value $E_\infty\,[|\log x|]$ is closely related to the entropy $h(\mathcal{H})$ of the dynamical system, via Rohlin's formula (21) and the fact that $|U'(x)| = 1/x^2$,

$$E_\infty\,[|\log x|] := \int_{\mathcal{I}} |\log t|\,\psi(t)dt = \frac{1}{2}\int_{\mathcal{I}} \log|U'(t)|\,\psi(t)dt = \frac{h(\mathcal{H})}{2}, \tag{25}$$

so that explicit values of entropy are obtained in both cases,

$$h(\mathcal{S}) = \frac{\pi^2}{6\log 2} \approx 2.37313, \qquad h(\mathcal{C}) = \frac{\pi^2}{6\log\phi} \approx 3.41831.$$

Continuants. This mean value intervenes also when studying the average behaviour of the parameter $\log q_n(x)$ relative to (beginning) continuant $q_n(x)$ that is well-defined for a general real number too. A real number x whose continued fraction begins with $h = h_1 \circ h_2 \circ \ldots \circ h_n$ satisfies $x = h(y) = h_1 \circ h_2 \circ \ldots \circ h_n(y)$ with some $y \in \mathcal{I}$; We relate x to the rational $x_0 := h(0) = h_1 \circ h_2 \circ \ldots \circ h_n(0)$, and the transforms $U^j(x) = h_{j+1} \circ h_2 \circ \ldots \circ h_n(y)$ to the transforms $U^j(x_0) = h_{j+1} \circ h_2 \circ \ldots \circ h_n(0)$.

The classical relation between numerator $p_j(x)$ and denominator $q_j(x)$, i.e., $p_{j+1}(x) = q_j(Ux)$ proves that

$$\frac{1}{q_n(x)} = \prod_{i=1}^{n} h_i \circ h_{i+1} \circ \ldots \circ h_n(0) = \prod_{i=0}^{n-1} U^i(x_0)$$

Since U is expanding with contraction-ratio δ, one obtains an approximate expression of $\log q_n(x)$ that involves transforms $\log U^i(x)$ instead of transforms $\log U^i(x_0)$: Since one has

$$|h(0) - h(y)| \leq \delta^k \quad \text{for any } h \text{ of depth } k \text{ and any } y \in \mathcal{I},$$

$$q_n(x) \geq (\frac{1}{\delta})^{n/2}, \quad p_n(x) \geq (\frac{1}{\delta})^{(n-1)/2},$$

there exists some constant K for which, for any x, and any integer n,

$$(26) \quad \big|\log q_n(x) - \sum_{i=1}^{n} |\log(U^i x)|\big| = \big|\sum_{i=1}^{n} |\log(U^i x_0)| - \sum_{i=1}^{n} |\log(U^i x)|\big| \leq K.$$

Now, the Ergodic Theorem (15) applies to the function $|\log x|$, implying, via (25) and (26), that

$$(27) \qquad \lim_{n\to\infty} \frac{1}{n} \log q_n(x) = \lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n} |\log(U^i x)| = \int_{\mathcal{I}} |\log t|\, \psi(t) dt = \frac{h(\mathcal{H})}{2} \qquad \text{for almost all } x \text{ of } \mathcal{I}.$$

Relations between entropy and mean binary length of digits. The asymptotic mean value relative to the binary length $E_\infty[\ell(a)]$ and the quantity $h(\mathcal{H})/(2\log 2)$ are related, since the second one is the integral of $|\log_2 t|$ with respect to ergodic measure, while the first one is the integral of the function that equals $\lfloor \log_2 a \rfloor + 1$ on the interval $h_{[a]}(\mathcal{I})$. We then obtain the relation

$$(28) \qquad E_\infty[\ell(a)] - 1 \leq \frac{h(\mathcal{H})}{2\log 2} \leq E_\infty[\ell(a)].$$

3.8. Heuristic transfer from continuous model to discrete one. With respect to asymptotic properties of continued fractions, rational numbers are very particular since their continued fraction expansion is finite. However, let us imagine that continued fractions of rational numbers and continued fractions of real numbers behave in the same way and let us suppose that the Ergodic Theorem may be applied to rational numbers with sufficiently large denominators. Then one can anticipate the following behaviours for our parameters of interest relative to rational numbers and defined in Figure 2

$$S[c](x) \sim p(x) \times E_\infty[c(M)], \qquad Q(x) \sim \frac{p(x)^2}{2} \times \frac{h}{2}$$
$$K[c](x) \sim \frac{p(x)^2}{2} \times \frac{h}{2} \times E_\infty[c(M)].$$

However, it is highly probable that this result may be true only in average on the set Ω_N defined in (12) when N tends to ∞. On the other hand, the depth $p(x)$ of a rational x of denominator N equals the rank n for which $q_n(x)$ equals N. If rational numbers of large denominator behave like generic real numbers, it is thus plausible, from (27), that $E_N[p] \sim (2/h)\log N$ for large N. This is a well-known result for which we shall give an alternative proof in the sequel. Finally, the following estimates are plausible:

$$E_N[S[c]] \sim E_N[p] \times E_\infty[c(M)], \ E_N[X] \sim E_N[p] \times \frac{\log N}{2}, \text{ for } X \in \{Q, W\},$$
$$E_N[X] \sim E_N[p] \times E_\infty[c(M)] \times \frac{\log N}{2} \quad \text{for } X \in \{K[c], L[c]\},$$

and will be proven in the sequel.

4. Generating functions, dynamical operators and Tauberian Theorems

Here, we describe general tools for analysing the main costs of interest relative to algorithms of the Euclidean type. We first introduce the Dirichlet generating functions relative to costs, so that the average cost involves partial sums of coefficients of these Dirichlet series. Tauberian Theorems are a classical tool that transfers the analytical behaviour of a Dirichlet series near its singularities into an asymptotic form for its coefficients. Then, when viewing the algorithm as a dynamical system, we relate generating functions of costs to the Ruelle operator associated to the algorithm, so that we can easily describe the singularities of generating functions. Finally, we prove the estimates of the mean values that have been previously proposed for the main parameters of algorithms.

4.1. Generating functions. We recall that we consider the following sets

$$\widetilde{\Omega} := \{(u,v);\ \frac{u}{v} \in \mathcal{I}\}, \quad \Omega := \{(u,v); \gcd(u,v) = 1, \frac{u}{v} \in \mathcal{I}\},$$
$$\widetilde{\Omega}_N := \{(u,v) \in \widetilde{\Omega}, v \leq N\}, \qquad \Omega_N := \{(u,v) \in \Omega, v \leq N\},$$

as possible inputs of a Euclidean algorithm. Our purpose is to estimate the mean value of a generic cost $X : \widetilde{\Omega} \to \mathbf{R}^+$ defined in Figure 2 on Ω_N

and $\widetilde{\Omega}_N$. More precisely, we aim to determine asymptotically (as $N \to \infty$) these mean values, denoted by $E_N[X]$ or $\widetilde{E}_N[X]$, that satisfy

$$
(29) \qquad
\begin{aligned}
E_N[X] &= \frac{X_N}{|\Omega_N|}, \quad \text{with} \quad X_N := \sum_{(u,v)\in\Omega_N} X(u,v) \\
\widetilde{E}_N[X] &= \frac{\widetilde{X}_N}{|\widetilde{\Omega}_N|}, \quad \text{with} \quad \widetilde{X}_N := \sum_{(u,v)\in\widetilde{\Omega}_N} X(u,v).
\end{aligned}
$$

The following Dirichlet generating functions of costs,

$$
(30) \qquad
\begin{aligned}
F(s) &:= \sum_{(u,v)\in\Omega} \frac{1}{v^s}, \qquad G_X(s) := \sum_{(u,v)\in\Omega} \frac{1}{v^s} X(u,v), \\
\widetilde{F}(s) &:= \sum_{(u,v)\in\widetilde{\Omega}} \frac{1}{v^s}, \qquad \widetilde{G}_X(s) := \sum_{(u,v)\in\widetilde{\Omega}} \frac{1}{v^s} X(u,v),
\end{aligned}
$$

are of the form

$$
F(s) = \sum_{n\ge 1} \frac{a_n}{n^s}, \quad \widetilde{F}(s) = \sum_{n\ge 1} \frac{\widetilde{a}_n}{n^s}, \quad G_X(s) = \sum_{n\ge 1} \frac{x_n}{n^s}, \quad \widetilde{G}_X(s) = \sum_{n\ge 1} \frac{\widetilde{x}_n}{n^s},
$$

where a_n, $\widetilde{a}_n$ are the number of pairs (u,v) of Ω or $\widetilde{\Omega}$ with fixed $v = n$, and x_n, $\widetilde{x}_n$ are the cumulative values of X on pairs (u,v) of Ω or $\widetilde{\Omega}$ with fixed $v = n$, so that the average costs in (29) to be studied

$$
E_N[X] = \frac{\sum_{n\le N} x_n}{\sum_{n\le N} a_n} \qquad \widetilde{E}_N[X] = \frac{\sum_{n\le N} \widetilde{x}_n}{\sum_{n\le N} \widetilde{a}_n}
$$

are exactly the quotient of partial sums of the coefficients of the Dirichlet series $F(s), \widetilde{F}(s), G_X(s), \widetilde{G}_X(s)$ defined in (30).

First, remark that there is an easy relation between G_X and $\widetilde{G}_X$ when cost X satisfies $X(u,v) = X(au,av)$ for any integer $a \ge 1$. Then

$$
(31) \qquad \widetilde{G}_X(s) = \zeta(s) G_X(s)
$$

where $\zeta(s)$ is the Riemann Zeta-function $\zeta(s) := \sum_{v\ge 1} \frac{1}{v^s}$.

This is the case when $X = 1$ or when X is one of the first five costs of interest defined in Figure 2. For the last two costs defined in Figure 2 that involve integers v_i, relations (10) entail that

$$
(32) \qquad
\begin{aligned}
\widetilde{G}_V(X) &= -\zeta'(s) G_p(s) + \zeta(s) G_W(s), \\
\widetilde{G}_{M[c]}(X) &= -\zeta'(s) G_{S[c]}(s) + \zeta(s) G_{K[c]}(s).
\end{aligned}
$$

Altogether, it is sufficient to analyse the first five costs on the set Ω_N.

4.2. Tauberian Theorems. In the remainder of the paper, we aim to apply the following Tauberian Theorem to the Dirichlet series F, G_X defined in (30) in order to estimate their coefficients.

Tauberian Theorem. [Delange] *Let $F(s)$ be a Dirichlet series with non negative coefficients such that $F(s)$ converges for $\Re(s) > \sigma > 0$. Assume that*
(i) $F(s)$ is analytic on $\Re(s) = \sigma, s \neq \sigma$, and
(ii) for some $\gamma \geq 0$, one has $F(s) = A(s)(s-\sigma)^{-\gamma-1} + C(s)$, *where A, C are analytic at σ, with $A(\sigma) \neq 0$.*
Then, as $N \to \infty$,

$$\sum_{n \leq N} a_n = \frac{A(\sigma)}{\sigma\Gamma(\gamma+1)}\, N^\sigma \log^\gamma N \quad [1 + \varepsilon(N)\,], \quad \varepsilon(N) \to 0.$$

We first examine the case of functions $F(s), \widetilde{F}(s)$ that are closely linked to the Riemann series $\zeta(s)$ via the equalities

$$\widetilde{F}(s) = \zeta(s)\, F(s), \qquad\qquad \widetilde{F}(s) = \rho\; \zeta(s-1)$$

Then, classical properties of ζ function entail that the Tauberian Theorem applies to $F(s)$ and $\widetilde{F}(s)$, with $\sigma = 2$ and $\gamma = 0$. More precisely, at $s = 2$, one has: $(s-2)F(s) \simeq (6\rho)/\pi^2$.

When X is one of the three costs defined in Figure 2 relative to continuants Q, V, W, it applies to $G_X(s)$ with $\sigma = 2$ and $\gamma = 3$, so that the mean value $E_N[X]$ will be of order $\log^2 N$. When X involves a digit–cost c, we will exhibit some sufficient conditions on cost c under which the Tauberian Theorem applies. In this case, the values σ and γ strongly depend on properties of the digit–cost c. In the case when c equals the binary digit–length ℓ, the mean value $E_N[S[\ell]]$ will be of order $\log N$, while the mean–value $E_N[K[\ell]]$ will be of order $\log^2 N$. We can deal with varied costs; for instance, if $c(m) = m \log^2 m$, then $E_N[S[c]]$ is of order $\log^4 N$, and if $c(m) = m^{3/2}$, then $E_N[S[c]]$ is of order $\sqrt{N}$.

It is not a priori clear how to directly apply Tauberian Theorems to $G_X(s)$. In the following, we obtain alternative expressions for $G_X(s), \widetilde{G}_X(s)$ from which the location and the nature of their singularities will become apparent. Our analysis involves suitable Ruelle operators that can be viewed as extensions of density transformers of Section 3.4 when one introduces some complex parameter s that plays the same rôle as temperature in statistical mechanic.

4.3. Algebraic properties of Ruelle operators. The Ruelle operators that we use now can be viewed as extensions of the Perron–Frobenius operator that we have introduced in Section 3.4.

The Ruelle operator $\mathbf{R}_{s,h}$ relative to a LFT h depends on some complex parameter s and is defined as

$$\mathbf{R}_{s,h}[f](x) := \frac{1}{D[h](x)^s}\ f \circ h(x), \tag{33}$$

where $D[h]$ denotes the denominator of the linear fractional transformation (LFT) h, defined for $h(x) = (ax+b)/(cx+d)$ with a, b, c, d coprime integers by $D[h](x) := |cx + d| = |\det h|^{1/2}\, |h'(x)|^{-1/2}$. Then, for a LFT h of determinant 1, the operator $\mathbf{R}_{s,h}$ is an extension of the operator $\mathbf{R}_h$ defined in (16), via the equality $\mathbf{R}_{2,h} = \mathbf{R}_h$.
Once a cost function c relative to the LFT h has been fixed, one can define another Ruelle operator relative to h,

$$\mathbf{R}^{[c]}_{s,h}[f](x) := \frac{c(h)}{D[h](x)^s}\ f \circ h(x). \tag{34}$$

Now, given an algorithm and a set $\mathcal{H}$ of LFT's used in one step of the algorithm, the Ruelle operators relative to $\mathcal{H}$ are defined by

$$\mathbf{H}_s := \sum_{h\in\mathcal{H}} \mathbf{R}_{s,h}, \qquad \mathbf{H}^{[c]}_s := \sum_{h\in\mathcal{H}} \mathbf{R}^{[c]}_{s,h}. \tag{35}$$

As previously, if the set $\mathcal{H}$ is formed of LFT's with determinant 1, the operator $\mathbf{H}_s$ is an extension of the operator $\mathbf{H}$ defined in (16), via the equality $\mathbf{H}_2 = \mathbf{H}$.
In all cases, the multiplicative property of denominator D, i.e., $D[h\circ g](x) = D[h](g(x))\, D[g](x)$ is translated into a multiplicative property on Ruelle operators: Given two LFT's, h and g, the Ruelle operator $\mathbf{R}_{s,h\circ g}$ associated to the LFT $h \circ g$ is exactly the operator $\mathbf{R}_{s,g} \circ \mathbf{R}_{s,h}$. More generally, when given two sets of LFT's, $\mathcal{L}$ and $\mathcal{K}$ and their Ruelle operators $\mathbf{K}_s, \mathbf{L}_s$, the set $\mathcal{LK}$ is formed of all $h \circ g$ with $h \in \mathcal{L}$ and $g \in \mathcal{K}$, and the Ruelle operator relative to the set $\mathcal{LK}$ is exactly the operator $\mathbf{K}_s \circ \mathbf{L}_s$. In particular, the Ruelle operator relative to the semi-group $\mathcal{H}^\star := \cup_{k\geq 0}\mathcal{H}^k$ is exactly $\sum_{k\geq 0} \mathbf{H}^k_s = (I - \mathbf{H}_s)^{-1}$. It is the quasi–inverse of the Ruelle operator $\mathbf{H}_s$ associated to the set $\mathcal{H}$.

4.4. Ruelle operators and Dirichlet generating functions. We show now how the Ruelle operators associated to the algorithms intervene in the evaluation of the generating functions of costs $G_X(s), \widetilde{G}_X(s)$. We recall that it is sufficient to study G_X for one of the first five costs of Figure 2.
We consider here a Euclidean Algorithm and its set of LFT's $\mathcal{H}$ together with its final set $\mathcal{F}$ defined in Fig.1. The Ruelle operators $\mathbf{H}_s, \mathbf{H}^{[c]}_s, \mathbf{F}_s, \mathbf{F}^{[c]}_s$ relative to $\mathcal{H}$ or $\mathcal{F}$ and defined in (33, 34, 35) will play a central rôle in the analysis.

An execution of the algorithm on the input (v_1, v_0) of Ω performing p steps of the form

$$v_0 = a_1 v_1 + d_1 v_2, \qquad v_1 = a_2 v_2 + d_2 v_3, \qquad \ldots v_{p-1} = a_p v_p + d_{p+1} 0,$$

decomposes the rational (v_1/v_0) as $(v_1/v_0) = h_1 \circ h_2 \circ \ldots \circ h_p(0)$, where the h_i's are elements of $\mathcal{H}$ (for $i \leq p-1$) or elements of $\mathcal{F}$ (for $i = p$). The choice of an index $i, 1 \leq i \leq p$, splits the LFT $h = h_1 \circ h_2 \circ \ldots \circ h_p$ into three different parts: the beginning part $b_i(h) := h_1 \circ h_2 \circ \ldots \circ h_{i-1}$, the ending part $e_i(h) := h_{i+1} \circ h_{i+2} \circ \ldots \circ h_k$, and finally the i-th component h_i. From (8) and (9) the following equalities hold:

$$D[e_i(h)](0) = w_i, \qquad D[b_{i+1}(h)][0] = q_i. \tag{36}$$

The derivative functional Δ plays an important rôle too. For some operator $\mathbf{L}_s$ that depends on parameter s, the operator $\Delta\mathbf{L}_s$ is defined by $\Delta\mathbf{L}_s := -\frac{d}{ds}\mathbf{L}_s$. When applied to $\mathbf{R}_{s,h}$ defined in (33), this functional Δ is well-suited to the problem since it produces at the numerator the logarithm $\log D[h]$. When applied to $\mathbf{R}_{s,b_i(h)}$ or to $\mathbf{R}_{s,b_i(h)}$, it produces at the numerator, via (36), the beginning or the ending continuants.

We now introduce our main operators, that are all built according to the same principles: each of them is precisely related to one of the generic costs X defined in Figure 2, and the generic operator, relative to generic cost X, is denoted by $\mathbf{X}_{s,h}$. If h is a LFT of depth p, it is expressed as a sum of p terms each of which may involve $\Delta\mathbf{R}_{s,b_i(h)}, \Delta\mathbf{R}_{s,e_i(h)}$ and $\mathbf{R}^{[c]}_{s,h_i}$; however, the precise form of $\mathbf{X}_{s,h}$ depends on cost X. Figure 3 (top) describes the operators relative to the studied costs.

We claim that, when applied to function $f = 1$ and point $x = 0$, each operator $\mathbf{X}_{s,h}$ generates the cost $X(v_1, v_0)$ of the algorithm on input (v_1, v_0) of Ω

$$\mathbf{X}_{s,h}[1](0) = \frac{1}{v_0^s} X(v_1, v_0) \qquad \text{when } (v_1, v_0) \in \Omega \text{ satisfies } \frac{v_1}{v_0} = h(0).$$

Now, when (v_1, v_0) is a general element of Ω, the LFT h defined by (2) is a general element of set $\mathcal{H}^\star\mathcal{F}$, so that we obtain alternative expressions of our main Dirichlet series F, G_X defined in (30)

$$F(s) := \sum_{(v_1,v_0)\in\Omega} \frac{1}{v_0^s} = \sum_{h\in\mathcal{H}^\star\mathcal{F}} \mathbf{R}_{s,h}[1](0)$$

$$G_X(s) := \sum_{(v_1,v_0)\in\Omega} \frac{1}{v_0^s}\, X(v_1, v_0) = \sum_{h\in\mathcal{H}^\star\mathcal{F}} \mathbf{X}_{s,h}[1](0).$$

When index i varies in $[1..p]$, beginning part $b_i(h)$ is a general element of $\mathcal{H}^\star$, ending part $e_i(h)$ is a general element of $\mathcal{H}^\star\mathcal{F}$, while the i-th component is a general element of $\mathcal{H}$ (for $i \leq p-1$) or $\mathcal{F}$ (for $i = p$), so that we obtain

Cost function X	*Operator* $\mathbf{X}_{s,h}$
1	$\mathbf{R}_{s,h}$
$S[c]$	$\sum_{i=1}^{p} \mathbf{R}_{s,e_i(h)} \circ \mathbf{R}^{[c]}_{s,h_i} \circ \mathbf{R}_{s,b_i(h)}$
W	$\sum_{i=1}^{p} \Delta\mathbf{R}_{s,e_{i+1}(h)} \circ \mathbf{R}_{s,b_i(h)}$
Q	$\sum_{i=1}^{p} \mathbf{R}_{s,e_{i+1}(h)} \circ \Delta\mathbf{R}_{s,b_i(h)}$
$K[c]$	$\sum_{i=1}^{p} \Delta\mathbf{R}_{s,e_i(h)} \circ \mathbf{R}^{[c]}_{s,h_i} \circ \mathbf{R}_{s,b_i(h)}$
$L[c]$	$\sum_{i=1}^{p} \mathbf{R}_{s,e_i(h)} \circ \mathbf{R}^{[c]}_{s,h_i} \circ \Delta\mathbf{R}_{s,b_i(h)}$

Cost function X	$\sum_{h\in\mathcal{H}^\star\mathcal{F}} \mathbf{X}_{s,h}$
1	$\mathbf{F}_s \circ (I-\mathbf{H}_s)^{-1}$
$S[c]$	$[\mathbf{F}_s \circ (I-\mathbf{H}_s)^{-1} \circ \mathbf{H}_s^{[c]} + \mathbf{F}_s^{[c]}] \circ (I-\mathbf{H}_s)^{-1}$
W	$\Delta[\mathbf{F}_s \circ (I-\mathbf{H}_s)^{-1})] \circ (I-\mathbf{H}_s)^{-1}$
Q	$\mathbf{F}_s \circ (I-\mathbf{H}_s)^{-1} \circ \Delta[(I-\mathbf{H}_s)^{-1}]$
$K[c]$	$\Delta[\mathbf{F}_s \circ (I-\mathbf{H}_s)^{-1}] \circ \mathbf{H}_s^{[c]} \circ (I-\mathbf{H}_s)^{-1}$
$L[c]$	$\mathbf{F}_s \circ (I-\mathbf{H}_s)^{-1} \circ \mathbf{H}_s^{[c]} \circ \Delta[(I-\mathbf{H}_s)^{-1}]$

Cost function X	*Main terms of* $G_X(s)$
1	$\mathbf{F}_s \circ (I-\mathbf{H}_s)^{-1}[1](0)$
$S[c]$	$\mathbf{F}_s \circ (I-\mathbf{H}_s)^{-1} \circ \mathbf{H}_s^{[c]} \circ (I-\mathbf{H}_s)^{-1}[1](0)$
W	$\mathbf{F}_s \circ (I-\mathbf{H}_s)^{-1} \circ \Delta\mathbf{H}_s \circ (I-\mathbf{H}_s)^{-2}[1](0)$
Q	$\mathbf{F}_s \circ (I-\mathbf{H}_s)^{-2} \circ \Delta\mathbf{H}_s \circ (I-\mathbf{H}_s)^{-1}[1](0)$
$K[c]$	$\mathbf{F}_s \circ (I-\mathbf{H}_s)^{-1} \circ \Delta\mathbf{H}_s \circ (I-\mathbf{H}_s)^{-1} \circ \mathbf{H}_s^{[c]} \circ (I-\mathbf{H}_s)^{-1}[1](0)$
$L[c]$	$\mathbf{F}_s \circ (I-\mathbf{H}_s)^{-1} \circ \mathbf{H}_s^{[c]} \circ (I-\mathbf{H}_s)^{-1} \circ \Delta\mathbf{H}_s \circ (I-\mathbf{H}_s)^{-1}[1](0)$

FIGURE 3. **Top**: The Ruelle operator $\mathbf{X}_{s,h}$ relative to generic cost X. **Middle**: The quantity $\sum_{h\in\mathcal{H}^\star\mathcal{F}} \mathbf{X}_{s,h}$ relative to generic cost X. **Bottom**: The main terms of Dirichlet series $G_X(s)$ relative to generic cost X.

alternative expressions of $\sum_{h\in\mathcal{H}^\star\mathcal{F}} \mathbf{X}_{s,h}$ which involves the Ruelle operators $\mathbf{H}_s, \mathbf{F}_s$ relative to the sets $\mathcal{H}, \mathcal{F}$ used by the algorithm (cf Figure 3–middle).

We finally deduce expressions for the Dirichlet series $F(s), G_X(s)$ mainly in terms of three Ruelle operators: the quasi-inverse $(I - \mathbf{H}_s)^{-1}$, the operator of costs $\mathbf{H}_s^{[c]}$, the derivative operator $\Delta\mathbf{H}_s$. For reasons that will be explained later, we only need to keep the terms of G_X that contain the largest number of occurrences of the quasi inverse $(I - \mathbf{H}_s)^{-1}$ and we call them the "main terms" of G_X (cf Figure 3–bottom). Then, main terms of Dirichlet series G_X for the two last costs of Figure 2, and the main terms of $\widetilde{G}_X$ for all the costs of interest are easily obtained from relations (32) and (31).

4.5. Functional Analysis. We come back now to the general framework of Section 3, i.e., a piecewise analytic map U of the interval $\mathcal{I}$, that we suppose strongly expanding. We have described in Section 3 the properties of the Perron–Frobenius operator $\mathbf{H}$ and explained how they entail properties related to ergodicity and strong mixing. Here, we deal with the particular case when the set $\mathcal{H}$ of the inverse branches of U is formed with LFTs of determinant 1. We recall that the operator $\mathbf{H}_s$ can be viewed as an extension of the Perron-Frobenius operator $\mathbf{H}$ since one has $\mathbf{H} = \mathbf{H}_2$. The following result shows how the general framework of Definition 3 entails all the properties that we need for applying the Tauberian Theorem to the quasi–inverse $(I - \mathbf{H}_s)^{-1}$ of the Ruelle operator relative to $\mathcal{H}$.

Theorem 1. *Let U be an eventually strongly expanding map of $\mathcal{I}$ such that the set $\mathcal{H}$ of the inverse branches of U is formed with LFTs of determinant 1. The triple of U is denoted by $(\mathcal{V}, \alpha, \delta)$ and $\mathcal{A}_\infty(\mathcal{V})$ is the set formed with functions f that are analytic on $\mathcal{V}$ and continuous on $\bar{\mathcal{V}}$. Then the following is true:*
(i) The Ruelle operator $\mathbf{H}_s$ extends the Perron-Frobenius operator $\mathbf{H}$ thanks of the relation $\mathbf{H}_2 = \mathbf{H}$. The operator $\mathbf{H}_s$ acts on $\mathcal{A}_\infty(\mathcal{V})$, is analytic on $\{\Re(s) > \alpha\}$. The dominant eigenfunction $s \to \lambda(s)$ is analytic and decreasing on the real line $s > \alpha$. For $\Re(s) = \sigma$, any eigenvalue λ of $\mathbf{H}_s$ satisfies $|\lambda| \le \lambda(\sigma)$. The derivative $-2\lambda'(2)$ equals the entropy $h(\mathcal{H})$.
(ii) The quasi–inverse $(I - \mathbf{H}_s)^{-1}$ of $\mathbf{H}_s$ is analytic on the plane $\{\Re(s) > 2\}$ and has a pole of order 1 at $s = 2$. Near $s = 2$, one has, for any function f of $\mathcal{A}_\infty(\mathcal{V})$ positive on $\mathcal{V} \cap \mathbf{R}$, and any $x \in \mathcal{V} \cap \mathbf{R}$,

$$(37) \qquad (I - \mathbf{H}_s)^{-1}[f](x) \sim \frac{1}{(s-2)}\,(\frac{-1}{\lambda'(2)})\,\psi(x)\,(\int_{\mathcal{I}} f(t)dt),$$

where ψ is the dominant eigenfunction of $\mathbf{H}$ defined by the normalization condition $\int_{\mathcal{I}} \psi(x)dx = 1$.

(iii) If the set $\mathcal{H}$ contains some subset $\{h \mid h(x) = 1/(c + x)$ with integers $c \to \infty\}$, then the quasi–inverse $(I - \mathbf{H}_s)^{-1}$ is analytic on $\Re(s) = 2, s \neq 2$.

Proof. Condition (d) of Definition entails that the Dirichlet series $\sum_{h\in\mathcal{H}} \delta(h)^{s/2}$ is convergent for $\Re(s) > \alpha$. Now, most of properties of $\mathbf{H}$ extend to $\mathbf{H}_s$ on $\{\Re(s) > \alpha\}$: There, the operator $\mathbf{H}_s$ acts on $\mathcal{A}_\infty(\mathcal{V})$ and is compact (even nuclear in the sense of Grothendieck [17, 18]). When acting on $\mathcal{A}_\infty(\mathcal{V})$, the operator $\mathbf{H}_s$ is analytic. Furthermore, for real values of parameter $s > \alpha$, it has positive properties that entail (via Theorems of Perron–Frobenius type [24]) the existence of dominant spectral objects: there exist a unique dominant eigenvalue $\lambda(s)$ positive, analytic for $s > \alpha$, a dominant eigenfunction denoted by ψ_s, and a dominant projector E_s. Under normalization condition $E_s[\psi_s] = 1$, these last two objects are unique too. Since the operator $\mathbf{H}_2 = \mathbf{H}$ is a density transformer cf (17), then one has $\lambda(2) = 1$ and $E_2[f] = \int_{\mathcal{I}} f(t)dt$. Rohlin's formula for the entropy (21) admits an alternative expression which involves the operator $\Delta\mathbf{H}$, under the form

$$h(\mathcal{H}) = \int_{\mathcal{I}} \log|U'(t)|\psi(t)dt = 2\int_{\mathcal{I}} \Delta\mathbf{H}[\psi](t)dt \tag{38}$$

Taking the derivative (with respect to s) of relation $\mathbf{H}_s[\psi_s] = \lambda(s)\psi_s$, leads to

$$\Delta\mathbf{H}_s[\psi_s] + \mathbf{H}_s[\Delta\psi_s] = -\lambda'(s)\psi_s + \lambda(s)\Delta\psi_s.$$

When choosing $s = 2$, and taking the integrals on $\mathcal{I}$, we use the fact that $\mathbf{H}_2$ is a density transformer, and Relation (38) leads to equality $-2\lambda'(2) = h(\mathcal{H})$.

Then, compacity entails the existence of a spectral gap between the dominant eigenvalue $\lambda(s)$ and the remainder of the spectrum, which splits the operator $\mathbf{H}_s$ into two parts: the "part" relative to the dominant eigensubspace and the "part" relative to the remainder of the spectrum, denoted by $\mathbf{N}_s$. By perturbation theory [21], these properties remain true in the neighborhood of the real axis, so that, for any integer $k \geq 1$ and for z in the neighborhood of the real axis, the following decomposition –that extends (19)– holds

$$\mathbf{H}_s^k[f](z) = \lambda(s)^k\psi_s(z)\, E_s[f] + \mathbf{N}_s^k[f](z), \tag{39}$$

and leads to

$$(I - \mathbf{H}_s)^{-1}[f](z) = \frac{\lambda(s)}{1-\lambda(s)}\psi_s(z)\ E_s[f] +\ (I - \mathbf{N}_s)^{-1}[f](z).$$

On a (complex) neighborhood of $s = 2$, the spectral radius of $\mathbf{N}_s$ is strictly than 1, and $(I - \mathbf{N}_s)^{-1}$ is analytic there. Now, using the derivability of

$s \to \lambda(s)$ at $s = 2$ and the equality $\lambda(2) = 1$, the residues at $s = 2$ are easily evaluated from special values at $s = 2$ and this proves the part (ii).

We next prove properties of dominant eigenvalue $\lambda(s)$ stated in (i). Here σ is real ($\sigma > \alpha$). When f is strictly positive on $\mathcal{V} \cap \mathbf{R}$, the quantity $E_\sigma[f]$ is strictly positive, and ψ_σ is strictly positive on $\mathcal{V} \cap \mathbf{R}$. Then, when taking $f = 1$ and $z = 0$ in (39), we obtain

$$\lambda(\sigma) = \lim_{k\to\infty} \Big(\sum_{h\in\mathcal{H}^k} \frac{1}{D[h](0)^\sigma} \Big)^{1/k}. \tag{40}$$

From property (d) of Definition 3, there exists $\gamma := \sqrt{\delta} < 1$ such that

$$\mathrm{Sup}\,\{\frac{1}{D[h](0)} \mid h \in \mathcal{H}\} \leq \gamma,$$

and then, for any k, $\quad \mathrm{Sup}\,\{\frac{1}{D[h](0)} \mid h \in \mathcal{H}^k\} \leq \gamma^k.$

Now, for $\beta > 0$,

$$\lambda(\sigma+\beta) = \lim_{k\to\infty} \Big(\sum_{h\in\mathcal{H}^k} \frac{1}{D[h](0)^{\sigma+\beta}} \Big)^{1/\ell} \leq \lim_{k\to\infty} \Big(\sum_{h\in\mathcal{H}^k} \gamma^{\beta k}\, \frac{1}{D[h](0)^\sigma} \Big)^{1/k}$$
$$\leq \gamma^\beta \lambda(\sigma) < \lambda(\sigma),$$

which proves that $s \to \lambda(s)$ is strictly decreasing along the real line.

Now s satisfies $\Re(s) = \sigma > \alpha$. Let λ be an eigenvalue of $\mathbf{H}_s$ and let f denote an eigenfunction relative to λ. The function f_σ denotes a dominant eigenvector relative to $\lambda(\sigma)$. Such a function is strictly positive on the segment $\mathcal{J}$, non–zero on $\mathcal{V}$ and normalized by the condition $f_\sigma(0) = 1$; moreover, the function $f(x)/f_\sigma(x)$ is supposed to be of modulus at most 1 on $[0, 1]$ and attain modulus 1 at point x_0. One always has

$$|\lambda\, f(x_0)| = |\mathbf{H}_s[f](x_0)| = |\sum_{h\in\mathcal{H}} D[h](x_0)^{-s}\ f\circ h(x_0)| \tag{41}$$
$$\leq \sum_{h\in\mathcal{H}} D[h](x_0)^{-\sigma}\ |f\circ h(x_0)|$$
$$\leq \sum_{h\in\mathcal{H}} D[h](x_0)^{-\sigma}\ f_\sigma\circ h(x_0) = \lambda(\sigma) f_\sigma(x_0), \tag{42}$$

and the definition of x_0 proves the inequality $|\lambda| \leq \lambda(\sigma)$.

On the other hand, condition of (iii) implies that the operator $\mathbf{H}_s$ has no eigenvalue equal to $\lambda(\sigma)$ on the line $\Re(s) = \sigma, s \neq \sigma$. This is an argument of Faivre [13]. Indeed, suppose that, for $s = \sigma + it, t \neq 0$, there exists an eigenvalue λ of $\mathbf{H}_s$ that satisfies $|\lambda| = \lambda(\sigma)$. Then the sequence of inequalities (41), (42) becomes a sequence of equalities. For any $h \in \mathcal{H}$, the equality

$$|f \circ h(x_0)| \;=\; f_\sigma \circ h(x_0) \tag{43}$$

holds. On the other side, the sequence $a_h := D[h](x_0)^{-\sigma-it} f \circ h(x_0)$ satisfies the equality $|\sum a_h| = \sum |a_h|$. Then, there exists θ (of modulus 1) such that $a_h = \theta|a_h|$ for any h, and the relation

$$f \circ h(x_0)\; D[h](x_0)^{-it} \;=\; \theta\; |f \circ h(x_0)| \tag{44}$$

holds. Both relations (43), (44) are in particular valid for the subset $\mathcal{D}$ of $\mathcal{H}$. Then, for $c \to \infty$, the sequence $h(x_0)$ tends to 0, and, equality (43) proves that $|f(0)| \;=\; f_\sigma(0) \neq 0$. Now, for $c \to \infty$, the relation (44) shows that the sequence

$$D[h](x_0)^{-it} = (\frac{1}{c + x_0})^{it}$$

has a limit equal to θ, which can be only true for $t = 0$. ■

4.6. Mean values of main parameters in the discrete model. Finally, Theorem 1 proves that the quasi–inverse of the Ruelle operator which intervenes in the expression of generating functions $F(s)$ and $G_X(s)$ fulfills all the hypotheses of Tauberian Theorem. Moreover, it shows that each occurrence of the quasi-inverse "brings" one pole at $s = 2$, so that the Dirichlet series $G_X(s)$ admit a pole at $s = 2$, of order at least two. The order is exactly three if cost X is relative to continuants, i.e., for $X \in \{Q, W, V\}$. In the case when cost X involves some digit–cost c, the analysis strongly depends on properties of digit–cost c.

Theorem 2. *Let $\mathcal{H}$ be a set of LFTs of determinant 1 used in one step of some Euclidean Algorithm. Assume the following:*
(i) the set $\mathcal{H}$ contains some subset $\{h(x) = 1/(c+x)$ with integers $c \to \infty\}$
(ii) the mapping U whose set of inverse branches is $\mathcal{H}$ is eventually strongly expanding.
Then the following results hold and involve the entropy $h(\mathcal{H})$ of the dynamical system and the asymptotic mean values $E_\infty[c(M)]$ of digit–cost c when the interval $\mathcal{I}$ is endowed with the invariant measure $\psi(t)dt$ relative to the dominant eigenfunction of the Perron-Frobenius operator **H**.
(a) The mean value of the number of iterations of Euclidean Algorithm on the set of inputs of denominator less than N is asymptotically of logarithmic order. It satisfies

$$\widetilde{E}_N[p] \sim E_N[p] \sim \frac{2}{h(\mathcal{H})} \log N.$$

(b) The mean values of continuant–parameters Q, W, V on the set of inputs of denominator less than N are asymptotically of log–squared order. They

satisfy

$$\widetilde{E}_N[X] \sim E_N[X] \sim \frac{1}{h(\mathcal{H})} \log^2 N \sim E_N[p] \times \frac{1}{2} \log N, \quad \text{for } X \in \{Q, V, W\}.$$

(c) Suppose that the Ruelle operator of costs $\mathbf{H}_s^{[c]}$ is analytic on $\{\Re(s) \geq 2\}$. Then the mean–value of parameter $S[c]$ on the set of inputs of denominator less than N is asymptotically of logarithmic order. It satisfies

$$\widetilde{E}_N[S[c]] \sim E_N\,[S[c]] \sim\ E_N[p] \times E_\infty[c(M)] \sim \frac{2}{h(\mathcal{H})}\ E_\infty[c(M)]\ \log N.$$

The mean–values of parameter $K[c], L[c], M[c]$ on the set of inputs of denominator less than N are asymptotically of log–squared order. They satisfy

$$\widetilde{E}_N\,[X] \sim E_N\,[X] \sim\ E_N[p] \times E_\infty[c(M)] \times \frac{1}{2} \log N \sim \frac{1}{h(\mathcal{H})}\, E_\infty[c(M)]\ \log^2 N$$

for $X \in \{K[c], L[c], M[c]\}$.

(d) Suppose that the Ruelle operator $\mathbf{H}_s^{[c]}$ of digit–costs is analytic on $\{\Re(s) \geq 2\}$ except at $s = 2$ where it has a pole of order k. Suppose that the integral $I(s) := \int_{\mathcal{I}} \mathbf{H}_s^{[c]}[\psi](t)dt$ satisfies $I(s)(s-2)^k \to A$ when $s \to 2$. Then the mean value of $S[c]$ on the set of valid inputs of denominator less than N is asymptotically of order $\log^{k+1} N$*; the mean values of $K[c], L[c], M[c]$ on the set of valid inputs of denominator less than N are asymptotically of order* $\log^{k+2} N$*. They satisfy*

$$\widetilde{E}_N[S[c]] \sim E_N[S[c]] \sim \frac{1}{(k+1)!}\,\frac{2A}{h(\mathcal{H})}\ \log^{k+1} N,$$

$$\widetilde{E}_N[X] \sim E_N[X] \sim \frac{1}{(k+2)!}\,\frac{2A}{h(\mathcal{H})}\ \log^{k+2} N, \quad \text{for}\ \ X \in \{K[c], L[c], M[c]\}.$$

(e) Suppose that there exists $\sigma > 2$ such that the Ruelle operator of digit–costs $\mathbf{H}_s^{[c]}$ is analytic on $\{\Re(s) \geq \sigma\}$ except at $s = \sigma$ where it has a pole of order k. Then the mean values of $S[c], L[c], K[c], M[c]$ on the set of valid inputs of denominator less than N are asymptotically of order $N^{\sigma-2} \log^{k-1} N$.

Proof. (b) Here X is a cost relative to continuants. Theorem 1 shows that the Dirichlet series $G_X(s)$ has a triple pole at $s = 2$, and near $s = 2$

$$F(s) \sim \frac{-1}{\lambda'(2)} \frac{\mathbf{F}[\psi](0)}{s-2}, \qquad G_X(s) \sim (\frac{-1}{\lambda'(2)})^3 \frac{\mathbf{F}[\psi](0)}{(s-2)^3} \Big(\int_{\mathcal{I}} \Delta\mathbf{H}[\psi](t)dt \Big)$$

The integral is expressed in terms of entropy via (38).

(c) Here X is a cost that involves some digit-cost. First suppose that $X = S[c]$. Since the Ruelle operator of costs is regular at $s = 2$, Theorem 1 shows that the Dirichlet series $G_X(s)$ has a double pole at $s=2$, and near $s=2$

$$F(s) \sim \frac{-1}{\lambda'(2)} \frac{\mathbf{F}[\psi](0)}{s-2}, \qquad G_X(s) \sim (\frac{-1}{\lambda'(2)})^3 \frac{\mathbf{F}[\psi](0)}{(s-2)^2} \Big(\int_{\mathcal{I}} \mathbf{H}^{[c]}[\psi](t)dt\Big).$$

The integral coincides with the asymptotic mean value of cost $c(M)$ in the continuous model (20) and is a constant of Khinchin's type.

$$\int_{\mathcal{I}} \mathbf{H}^{[c]}[\psi](t)dt = \sum_{m\in\mathcal{M}} c(m) \int_{h_{[m]}(\mathcal{I})} \psi(t)dt = E_\infty[c(M)];$$

This is true in particular for the trivial cost $c=1$, which gives the result (a) for the mean value of depth p, since $p=S[1]$.

Suppose now that $X=K[c]$. Since the Ruelle operator of costs is regular at $s=2$, Theorem 1 shows that the Dirichlet series $G_X(s)$ has a triple pole at $s=2$, and near $s=2$

$$F(s) \sim \frac{-1}{\lambda'(2)} \frac{\mathbf{F}[\psi](0)}{s-2},$$
$$G_X(s) \sim (\frac{-1}{\lambda'(2)})^3 \frac{\mathbf{F}[\psi](0)}{(s-2)^3} \Big(\int_{\mathcal{I}} \mathbf{H}^{[c]}[\psi](t)dt\Big) \Big(\int_{\mathcal{I}} \Delta\mathbf{H}[\psi](t)dt\Big).$$

The previous alternative expressions for both integrals give the result.

(d) The Dirichlet series $G_{S[c]}(s)$ has now a pole of order $k+2$ at $s=2$, and the Dirichlet series $G_{K[c]}(s)$ has now a pole of order $k+3$ at $s=2$, and near $s=2$, one has

$$G_{S[c]}(s) \sim \frac{A}{(\lambda'(2))^2} \frac{\mathbf{F}[\psi](0)}{(s-2)^{k+2}} \qquad G_{K[c]}(s) \sim \frac{A}{(\lambda'(2))^2} \frac{\mathbf{F}[\psi](0)}{(s-2)^{k+3}}.$$

(e) For $X \in \{S[c], L[c], K[c], M[c]\}$, the Dirichlet series $G_X(s)$ satisfies near $s=\sigma$, $G_X(s) \sim O((s-\sigma)^{-k})$. ∎

Remark. We can now prove why the approximation that we have made on the costs $C(v_1,v_0)$ and $D(v_1,v_0)$ are valid. When one replaces the binary length $\ell(v)$ by the logarithm $\log_2(v)$, or when one replaces $\log_2(v_i)$ by $\log_2(v_{i+1})$, one adds to Dirichlet series $G(s)$ relative to cost C some multiple of series that have a pole at $s=2$ whose order is always strictly less than $G(s)$ so that the main order term of the average cost is not modified by our approximation.

5. Average–case Analysis of Euclidean Algorithms

We now come back to the precise analysis of the two Euclidean algorithms and we focus on two main quantities: the bit–complexity of Euclidean Algorithms and the code-length of continued fractions expansions. Then we explain how our methods can be adapted to other Euclidean Algorithms.

5.1. Average bit–complexity. We recall that we wish to analyse the average behaviour of $C(v_1, v_0)$ defined in (3) or $D(v_1, v_0)$ defined in (5) when (v_1, v_0) is a random input or Ω_N or $\widetilde{\Omega}_N$. Theorem 2 (c) applies in this case to costs defined in Figure 1, and, with formulae (22), (23), (24), one obtains our first main result.

Theorem 3. *The average bit-complexities of the Standard Algorithm (S), and the Centered Algorithm (C) on the set of valid inputs of denominator less than N are asymptotically of log–squared order:*

$$\widetilde{C}_N(\mathcal{H}) \sim C_N(\mathcal{H}) \sim \frac{\log 2}{h(\mathcal{H})}\; E_\infty^{(\mathcal{H})}[c]\;\; \log_2^2 N \qquad \textit{for} \qquad \mathcal{H} \in \{\mathcal{S}, \mathcal{C}\}.$$

Here $h(\mathcal{H})$ is the entropy of the dynamical system relative to the algorithm and $E_\infty[c(M)]$ denotes the average value of digit–cost c when the interval $\mathcal{I}$ is endowed with the invariant measure. More precisely, in the standard case (S), the cost $c(m)$ equals $\ell(m) + 2$ where $\ell(m)$ is the number of bits of digit m, and

$$E_\infty^{(\mathcal{S})}[c(M)] = [2 + \frac{1}{\log 2} \log \prod_{k=0}^{\infty} (1 + \frac{1}{2^k})], \qquad h(\mathcal{S}) = \frac{\pi^2}{6 \log 2}.$$

In the centered case (C), the cost $c(m)$ relative to $m = (a, d)$ equals $\ell(a) + 2 + (1 - \varepsilon)/2$ where $\ell(a)$ is the number of bits of digit a, and $\varepsilon = \pm 1$ the sign used, so that

$$E_\infty^{(\mathcal{C})}[c(M)] = \left[3 + \frac{\log 2}{\log \phi} + \frac{1}{\log \phi} \log \prod_{k=3}^{\infty} \frac{(2^k - 1)\phi^2 + 2\phi}{(2^k - 1)\phi^2 - 2}\right], \qquad h(\mathcal{C}) = \frac{\pi^2}{6 \log \phi}.$$

The average bit-complexities of the Standard Extended Algorithm (S), and the Centered Extended Algorithm (C) on the set of valid inputs of denominator less than N satisfy

$$\widetilde{D}_N(\mathcal{H}) \sim D_N(\mathcal{H}) \sim 3\, C_N(\mathcal{H}).$$

The numerical values for the constants of bit–complexities,

$$C_N(\mathcal{S}) \simeq 1.24237\;\; \log_2^2 N, \qquad C_N(\mathcal{C}) \simeq 1.12655\;\; \log_2^2 N,$$

prove the efficiency of Classical Euclidean Algorithms when compared to naive multiplication of numbers whose average bit–complexity is $\log_2^2 N$ on integers less than N. For computing the inverse of some integer a modulo some another integer n, the Extended algorithms can be modified so that they make use of only one auxiliary sequence r_i. Then, their average bit complexity on the set of valid inputs of denominator less than N is about $2.5 \log_2^2 N$.

5.2. Average code–length of continued fractions expansions. We are now interested in describing the length $B(v_1, v_0)$ of the binary word that encodes the pair (v_1, v_0) by using the binary encoding of the sequence of digits $(m_1, m_2, \ldots, m_p)$,

$$B(v_1, v_0) := \sum_{i=1}^{p} c(m_i),$$

when digit–cost c is chosen to be near–optimal with respect to distribution of digits m_i.

The choice of a near–optimal code will follow the principles of Fano–Shannon encoding that we recall now: Assume that a source produces (independent) symbols m_i with probability p_i and the symbols are sorted with respect to decreasing probabilities. One builds a binary tree according to the recursive principle: Denote by n_0 the first index index n such that $\sum_{i \le n} p_i \ge 1/2$. Then all the symbols m_i for $i \le n_0$ are encoding by a word that begins with $'0'$ while the symbols m_i for $i > n_0$ are encoding by a word that begins with $'1'$. Then, recursively divide the first group and the second group following the same principles.

We first adopt this Fano-Shannon principle to the case of the Standard Euclidean Algorithm. We consider the approximate model where the symbol m is always emitted with the probability

$$p_m = \frac{1}{m} - \frac{1}{m+1} = \frac{1}{m(m+1)}. \tag{45}$$

Then all the digits m_i that comprise k binary digits have their code word that begins with $k-1$ times the symbol $'1'$ followed with a $'0'$. Then, we do not any more apply the Fano-Shannon process, and we use now the binary encoding of the digit. Finally, the code word of a digit m whose binary length is k is a sequence of $k-1$ symbols equal to $'1'$, then a zero, then the sequence of the binary digits of m where the most significant 1 is removed. For instance the digit 21 (in decimal expansion) is written as 10101 (in binary expansion), and will be encoded as 1111 0 0101. The process is quite easy to decode. For instance, the word 00011111100001000101 = 0 0 0 1111110000100 0 101 is decoded as $(1, 1, 1, 68, 1, 3)$. In this way, all the digits m of binary length k are encoded by a binary word of length $2k-1$, and we encounter there a code that was proposed by Elias [12] for encoding integers. We prove in this way that the Elias code appears to be quite optimal for coding a source that emits integers m with probabilities p_m defined in (45).

The asymptotic mean value of the code-length relative to a digit is just equal to $2E_\infty^{(\mathcal{S})}[\ell(M)] - 1 = 2A(\mathcal{S}) - 1$.

We can also adopt the Fano-Shannon principle to the case of the Centered Euclidean Algorithm, and we consider the approximation

$$p_{(a,\varepsilon)} \approx |\frac{1}{a} - \frac{1}{a+\varepsilon}| = \frac{1}{a(a+\varepsilon)}.$$

The order on the probabilities corresponds to the lexicographic order on the digit–pair $m = (a, \varepsilon)$. Then all the digits m that belong to interval $[(2^k, +1), (2^{k+1}, -1)]$ have their code word that begins with $k-1$ times the symbol $'1'$ followed with a $'0'$. Then, we do not any more apply the Fano-Shannon process here, and we use now the binary encoding of digit–rank inside the interval. Since there are exactly 2^{k+1} digit–pairs in the interval, this rank–encoding (from 0 to $2^{k+1}-1$) uses exactly $k+1$ bits. Finally, the code word of a digit m that belongs to the interval $[(2^k, +1), (2^{k+1}, -1)]$ is a sequence of $k-1$ symbols equal to $'1'$, then a zero, then the encoding of the digit–rank in the interval on $k+1$ bits. For instance the digit $(20, -1)$ (in decimal expansion) has rank 7 in the interval $[(16, +1), (32, -1)]$ so that it will be encoded as 111 0 00111. Decoding is quite easy too. For instance, the word 00011111110000010001011 is decoded as $(2, +1), (69, -1), (4, -1)$.

Finally all the digits of the interval $[(2^k, +1), (2^{k+1}, -1)]$ are coded on $2k+1$ bits.

Theorem 4. *The average code–lengths of the continued fraction expansions produced either by the Standard Algorithm* (S)*, or the Centered Algorithm* (C) *on the set of valid inputs of denominator less than* N *are asymptotically of logarithmic order. They satisfy*

$$\widetilde{B}_N(\mathcal{H}) \sim B_N(\mathcal{H}) \sim \frac{2\log 2}{h(\mathcal{H})}\ E_\infty^{(\mathcal{H})}[c(M)]\ \log_2 N \qquad \text{for} \qquad \mathcal{H} \in \{\mathcal{S}, \mathcal{C}\}.$$

Here $h(\mathcal{H})$ *is the entropy of the dynamical system relative to the algorithm and* $E_\infty[c(M)]$ *denotes the average value of digit–cost* c *when the interval* $\mathcal{I}$ *is endowed with the invariant measure. More precisely, in the standard case* (S)*, the cost* $c(m)$ *equals* $2\ell(m) - 1$ *where* $\ell(m)$ *is the number of bits of digit* m*, and*

$$E_\infty^{(\mathcal{S})}[c(M)] = 1 + \frac{2}{\log 2}\log\prod_{k=1}^{\infty}(1 + \frac{1}{2^k}), \qquad h(\mathcal{S}) = \frac{\pi^2}{6\log 2}$$

In the centered case (C)*, the cost* $c(m)$ *equals* $2k+1$ *when digit* m *belongs to the interval* $[(2^k, +1), (2^{k+1}, -1)]$*, so that*

$$E_\infty^{(\mathcal{C})}[c(M)] = 1 \ + \ \frac{2}{\log\phi}\log\prod_{k=1}^{\infty}\frac{2^k\phi^2 + \phi}{2^k\phi^2 - 1}, \qquad h(\mathcal{C}) = \frac{\pi^2}{6\log\phi}.$$

The numerical values for both constants of average code–length,

$$B_N(\mathcal{S}) \simeq 2.04868 \ \log_2 N, \qquad B_N(\mathcal{C}) \simeq 2.04557 \ \log_2 N,$$

prove the near-optimality of the continued–fraction encodings when compared to the minimal encoding of integer pairs whose average code–length is $2 \ \log_2 N$ for integer pairs less than N.

5.3. Other costs on digits. Theorem 2 provides a useful criterion for classifying the asymptotic behaviour of generic costs that involve digit–costs. This classification strongly depend on properties of digit–costs themselves. When Ergodic Theorems apply, Theorem 2 can be viewed as an efficient transfer from "continuous to discrete": in this case, the asymptotic mean value $E_\infty[c(M)]$ exists, and the expectation $E_N[S[c]]$ has exactly the asymptotic behaviour that one can expect if the discrete world behaves as the continuous world. However, Theorem 2 may provide a "discrete" answer whereas a "continuous" answer cannot be obtained from Ergodic methods: even if function $c \circ M$ relative to some digit–cost c is not in $\mathcal{L}^1$, Theorem 2 (d) or (e) may apply and give some precise information on $E_N[S[c]]$. For instance, if $c(m) = m \log^2 m$, then $E_N[S[c]]$ is of order $\log^4 N$, and if $c(m) = m^{3/2}$, then $E_N[S[c]]$ is of order $\sqrt{N}$.

We now focus on an important particular case that arises when the digit–cost $c_0(m)$ equals m. This digit–cost is then related to the so–called Subtractive Algorithm (T), where each Euclidean division that uses a quotient equal to a is replaced by a sequence of a subtractions. Then the value $E_N[S[c_0]]$ exactly counts the average number of subtractions of Subtractive Algorithm, while the value $E_N[M[c_0]]$ measures the average bit–complexity of the algorithm. Higher moments of the variable "number of subtractions" of the Subtractive Algorithm are associated to the values $E_N[S[c_0^k]]$. The first two mean values are analysed with Theorem 2 (d), and the higher moments are estimated with Theorem 2 (e). We obtain

Theorem 5. *The average number of subtractions performed by the Subtractive Algorithm (T) on the set of valid inputs of denominator less than N is asymptotically of log–squared order; it satisfies*

$$\mathcal{S}_N \sim \widetilde{\mathcal{S}}_N \sim \frac{6 \log^2 2}{\pi^2} \log_2^2 N.$$

The moment of order k $(k \geq 2)$ of the variable "number of iterations" is asymptotically of order N^{k-1}. The average bit-complexity of the Subtractive Algorithm (T) on the set of valid inputs of denominator less than N is asymptotically of log–cubed order:

$$\widetilde{C}_N(\mathcal{T}) \sim C_N(\mathcal{T}) \sim \frac{2 \log^2 2}{\pi^2} \log_2^3 N$$

The first assertion has been proven (with direct combinatorial methods) by Yao and Knuth in 1975 [41]. The second and third assertions provide new results.

5.4. Two Pseudo–Euclidean Algorithms related to random continued fractions. The general framework that we propose here can be easily adapted to other Euclidean Algorithms, the ones that we have called Pseudo-Euclidean in previous papers [37, 38]. These algorithms are useful for computing the Jacobi symbol and they have a structure similar to the classical Euclidean algorithms, since they perform a sequence of successive Euclidean-like divisions and exchanges. However, the Quadratic Reciprocity law being only true for a pair of odd integers, the standard Euclidean division has to be transformed into a pseudo–Euclidean division where pseudo–remainders will always be odd. A pseudo-Euclidean division on a pair (u, v) of positive odd integers

$$v = bu + \varepsilon 2^k s \qquad \text{with } \varepsilon = \pm 1,\ s \text{ odd and strictly less than } u, \tag{46}$$

creates another pair (s, u) for the following step. Then the Jacobi Symbol $J(u, v)$ is easily computed from the Jacobi symbol $J(s, u)$. The pseudo-Standard Algorithm $(\widehat{S})$ and the pseudo-Centered Algorithm $(\widehat{C})$ performs divisions where the pseudo–quotients are equal to the standard quotients or to the centered quotients; then, remainders may be even or odd, and, when they are even, powers of two are removed for obtaining the pseudo–remainders.

When performing ℓ pseudo–Euclidean divisions on a valid input (u, v) formed with two odd integers, each of the two algorithms builds a specific continued fraction of height ℓ for the rational $x = u/v$. For the pseudo–Centered algorithm $(\widehat{C})$, the rational x belongs to $\mathcal{I} = [0, 1/2]$. In the pseudo-Standard case, the rational x belongs to $\mathcal{I} = [0, 1]$.

Now, both algorithms have a Markovian flavour. In (46), if b is odd, then the remainder is even, and thus k satisfies $k \geq 1$; if b is even, then the remainder is odd, and thus k satisfies $k = 0$. This link is of Markovian type, and we consider two states: the 0 state, which means "the remainder of (u, v) is odd", i.e. $k = 0$, and the 1 state, which means "the remainder of (u, v) is even ", i.e. $k \geq 1$. Denoting by $\widehat{\mathcal{S}}_j$, resp. $\widehat{\mathcal{C}}_j$ the set of LFT's which can be used in state j, we obtain four different sets, $\widehat{\mathcal{S}}_{i|j}$, resp. $\widehat{\mathcal{C}}_{i|j}$ each of them brings rationals from state j to state i. The initial state is the 0 state and the final state is the 1 state.

It is not clear how to obtain an extension of continued fractions for real numbers. The reason is that the pseudo-divisions are related to dyadic valuation, so that continued fractions expansions are only defined for rationals numbers. However, one can define random continued fraction for real

Alg., ρ	*Division*	*LFT's*	*Initial and Final states*
$(\widehat{S})$ 1	$v = cu + 2^k s$ $s = 0$ or s odd, $k \geq 0$ $0 \leq 2^k s < u$	$\widehat{\mathcal{S}}_0 = \{\frac{1}{c+x},\ c \geq 1\}$ $\widehat{\mathcal{S}}_1 = \{\frac{2^k}{c+x},\ \geq 1, c \geq 2^k\}$ $\widehat{\mathcal{S}}_{i\mid j} = \widehat{\mathcal{S}}_j \cap \{c \equiv i \bmod 2\}$	initial state: 0 state final state: 1 state
$(\widehat{C})$ $\frac{1}{2}$	$v = cu + \varepsilon 2^k\, s$ $s = 0$ or s odd, $k \geq 0$ $0 \leq 2^k s < \frac{u}{2}$	$\widehat{\mathcal{C}}_0 = \{\frac{1}{c+\varepsilon x}\}, \varepsilon = \pm 1,$ $c \geq 2, (c, \varepsilon) \neq (2, -1)$ $\widehat{\mathcal{C}}_1 = \{\frac{2^k}{c+\varepsilon x}\}, k \geq 1, \varepsilon = \pm 1$ $c \geq 2^{k+1}, (c, \varepsilon) \neq (2^{k+1}, -1)$ $\widehat{\mathcal{C}}_{i\mid j} = \widehat{\mathcal{C}}_j \cap \{c \equiv i \bmod 2\}$	initial state: 0 state final state: 1 state

FIGURE 4. The two pseudo–Euclidean algorithms.

numbers in these cases: The state 0 is deterministic, and in the state 1, one chooses at random the dyadic valuation k of a real number, according to the law $\Pr[k = d] = 2^{-d}$ (for $d \geq 1$), that extends the natural law on even integers. In this manner, we choose the LFT of determinant 2^k with probability 2^{-k}. Now, for LFT's of determinant 2^k, the quantity

$$\frac{1}{D[h](x)^2} f \circ h(x) dx = \frac{|h'(x)|}{2^k} f \circ h(x) dx$$

represents exactly a random change of variables, so that the operator $\mathbf{H}_2$ is the Perron–Frobenius operator associated to the (random) mapping U (See [38] for more details). Then, the Ruelle operator $\mathbf{H}_s$ can be viewed as the transfer operator relative to this (random) dynamical system. Then, Theorem 2 (c) applies, and, even if the invariant eigenfunction ψ is no more explicit, the entropy and the average value $E_\infty[c]$ can be easily computed as a function of ψ.

Theorem 6. *The average bit-complexities of the Pseudo-Standard Algorithm* $(\widehat{S})$ *or the Pseudo-Centered Algorithm* $(\widehat{C})$ *on the set of odd inputs of denominator less than* N *are asymptotically of log–squared order:*

$$\widetilde{C}_N(\mathcal{H}) \sim C_N(\mathcal{H}) \sim \frac{\log 2}{h(\mathcal{H})}\ E_\infty^{(\mathcal{H})}[c]\ \log_2^2 N \qquad \textit{for} \qquad \mathcal{H} \in \{\widehat{\mathcal{S}}, \widehat{\mathcal{C}}\}.$$

Here $h(\mathcal{H})$ *is the entropy of the (random) dynamical system relative to the algorithm and* $E_\infty[c(M)]$ *denotes the average value of digit–cost* $c(m)$ *when the interval* $\mathcal{I}$ *is endowed with the invariant measure* μ *that corresponds to the dominant eigenfunction* ψ *of the Perron-Frobenius operator. More precisely, the cost* $c(m)$ *equals* $\ell(m) + 2$*, where* $\ell(m)$ *is the number of bits* *of digit m, and one has*

$$E_\infty^{(\mathcal{H})}[c(M)] = \sum_{m\in\mathcal{M}} (\ell(m)+2)\ \mu(h_{[m]}(\mathcal{I})),$$

$$h(\mathcal{H}) = 2\log 2 + 2\int_{\mathcal{I}} |\log t|\, \psi(t)dt.$$

5.5. Another pseudo-Euclidean algorithm: The Binary gcd Algorithm. There are two algorithms where no divisions are performed, the Subtractive Algorithm (T) that we have already described in 5.3. and the Binary Algorithm (B). The Binary Algorithm (B) uses only subtractions and right shifts, and it can be viewed as the pseudo-version of the Subtractive algorithm: it performs a sequence of operations of the form $v := (v-u)/2^b$, where b is the dyadic valuation of $v-u$, denoted by $b := \mathrm{Val}_2\,(v-u)$, and defined as the largest exponent b such that 2^b divides $v-u$.

This algorithm operates on odd-integer pairs and it has two nested loops: The external loop corresponds to an exchange. Between two exchanges, there is a sequence of iterations that constitutes the internal loop.

Binary Euclidean Algorithm (u, v)

While $u \neq v$ **do**
  While $u < v$ **do**
    $b := \mathrm{Val}_2\,(v-u)$;
    $v := (v-u)/2^b$;
  Exchange u and v;
Output: u (or v).

Each internal sequence consists in subtractions and (possible) shifts and can be written as

$$v = u+2^{b_1}v_1, \qquad v_1 = u+2^{b_2}v_2, \qquad v_2 = u+2^{b_3}v_3, \quad \ldots \quad v_{\ell-1} = u+2^{b_\ell}v_\ell.$$

Here v_ℓ is strictly less than u, and plays the rôle of a remainder r, so that the result of a sequence of internal loop is a decomposition of the form $v = mu + 2^s r$, with m odd, $m < 2^s$ and $r < u$, and the number of steps in the internal loop equals $b(m)$, where $b(x)$ denotes the number of ones in the binary expansion of x.

The cost of a subtractive step $v = u + (v-u)$ is equal to $\ell(v)$. The cost of a right shift $v := v/2^b$ is equal to $\ell(v)$. Then the bit–cost of a sequence of internal steps whose result is a decomposition $v = mu+dr$ equals $\ell(v)\times b(m)$ for the Binary Algorithm (B). It is followed by an exchange, so that the total cost of an external step equals $\ell(v) \times (b(m)+2)$.

This algorithm is more difficult to analyse [6, 7, 36]. The reason is that the set $\mathcal{B}$ of LFT's relative to the Binary algorithm

$$\mathcal{B} = \{h(z) = \frac{1}{m + 2^s z}, \quad m \text{ odd}, m < 2^s\}$$

is not well-behaved. First, it is not possible to find an open disk whose diameter contains the basic interval $\mathcal{I} := [0,1]$ and on which all the LFT's are analytic. The reason is that the sequence of poles of LFT's is of the form $x = -m/2^s$ and has an accumulation point at $x = 0$. As in [36], we choose for $\mathcal{V}$ an open disk of diameter $]0, \beta[$ with $1 < \beta < 2$, and a convenient functional space is then the Hardy space of order two relative to $\mathcal{V}$. It is denoted by $\mathcal{H}^2(\mathcal{V})$ and is formed with all functions f analytic inside $\mathcal{V}$ and such that $|f|^2$ is integrable along the frontier of $\mathcal{V}$. Each Ruelle operator $\mathbf{R}_{s,h}$ acts on this set and is compact, and the same is true for operator $\mathbf{H}_s$ provided that $\Re(s) > (3/2)$.

Second, as previously, the dynamical system is random, since the pseudo-division is related to dyadic valuation. However, one can define random binary continued fraction for real numbers when choosing at random the dyadic valuation k of a real number in the same way as in 5.4. Then, the Ruelle operator relative to the Binary Algorithm can be viewed as the transfer operator relative to this random dynamical system and, for $s = 2$, it is a (random) density transformer. Now, we can apply Theorem 2, version (c). As in 5.4, the invariant eigenfunction ψ is no more explicit, but the entropy and the average value $E_\infty[c]$ can be easily computed as a function of ψ and its integral F.

Theorem 7. *The average bit-complexity of the Binary Algorithm (B) on the set of valid inputs of denominator less than N is asymptotically of log–squared order:*

$$\widetilde{C}_N(\mathcal{B}) \sim C_N(\mathcal{B}) \sim \frac{\log 2}{h(\mathcal{H})}\ E_\infty^{(\mathcal{B})}[c(M)]\ \log_2^2 N.$$

Here $h(\mathcal{H})$ is the entropy of the (random) dynamical system relative to the algorithm and $E_\infty[c(M))]$ denotes the average value of digit–cost $c(m)$ when the interval $\mathcal{I}$ is endowed with the invariant measure that corresponds to the dominant eigenfunction ψ of the Perron-Frobenius operator. More precisely, the digit cost $c(m)$ is equal to $b(m) + 2$ where $b(m)$ is the number of 1 in the binary decomposition of digit m and one has

$$E_\infty^{(\mathcal{B})}[c(M)] = 2 + 2 \sum_{m \ \text{odd} \geq 1} \frac{1}{2^{\ell(m)}} F(\frac{1}{m}),$$

$$h(\mathcal{H}) = 2 \log 2 + 2 \int_{\mathcal{I}} |\log t|\, \psi(t) dt,$$

where F is the distribution function relative to invariant measure, and, as previously, $\ell(m)$ is the number of bits of integer m.

Brent [6, 7] made extensive computations for estimating the numerical value

$$\frac{2}{h(\mathcal{H})}\ E_\infty^{(\mathcal{B})}[b(M)] \approx 1.01850.$$

In a previous work [36], we have estimated the entropy by simulations, $h(\mathcal{B}) \approx 3.60$, so that

$$\widetilde{C}_N(\mathcal{B}) \sim C_N(\mathcal{B}) \simeq 0.720\ \log_2^2 N.$$

Then the average bit-complexity of the Binary Algorithm is about 60 % lower than the average bit-complexity of the Classical Euclidean Algorithms.

Acknowledgements. I wish to thank Jean Vuillemin for his interest and his questions that have been powerful motivations for this work, Julien Clément for his indications about Elias code, and Ali Akhavi for many fruitful discussions.

References

[1] A. Akhavi, B. Vallée, *Average bit–complexity of Euclidean Algorithms.* Proceedings of ICALP'00, Lecture Notes in Computer Science 1853, pp 373–387, Springer.

[2] K.I. Babenko, *On a problem of Gauss.* Soviet Mathematical Doklady **19** (1978), 136–140.

[3] T. Bedford, M. Keane, C. Series Eds, *Ergodic Theory, Symbolic Dynamics and Hyperbolic Spaces*, Oxford University Press (1991).

[4] M. Beeler, R.W. Gosper, R. Schroeppel, HAKMEM. Memorandum 239, M.I.T., Artificial Intelligence Laboratory, Feb. 1972.

[5] P. Billingsley, *Ergodic Theory and Information,* John Wiley & Sons (1965).

[6] R.P. Brent, *Analysis of the Binary Euclidean algorithm.* In: Algorithms and Complexity, New directions and recent results, ed. by J.F. Traub, Academic Press (1976), 321–355.

[7] R.P. Brent, *Further analysis of the binary Euclidean algorithm.* Report PRG-TR-7-99, Oxford University Computing Laboratory, Nov. 1999 (also reported in [23]).

[8] I.P. Cornfeld, S.V. Fomin, Y.G. Sinai, *Ergodic Theory.* A series of Comprehensive Studies in Mathematics, Springer–Verlag (1982)

[9] H. Daudé, P. Flajolet, B. Vallée, *An average-case analysis of the Gaussian algorithm for lattice reduction.* Combinatorics, Probability and Computing **6** (1997), 397–433.

[10] H. Delange, *Généralisation du Théorème d'Ikehara.* Ann. Sc. ENS **71** (1954), 213–242.

[11] J.D. Dixon, *The number of steps in the Euclidean algorithm.* Journal of Number Theory **2** (1970), 414–422.

[12] P. Elias, *Universal codeword sets and representations of the integers.* IEEE Transactions on Information Theory. Vol IT-21 , No 2, March 1975, 194–203.

[13] C. Faivre, *Distribution of Lévy's constants for quadratic numbers.* Acta Arithmetica **61** (1992), 13–34.

[14] P. Flajolet, *Analytic analysis of algorithms.* In: Proceedings of the 19th International Colloquium "Automata, Languages and Programming", Vienna, July 1992, W. Kuich, editor, Lecture Notes in Computer Science **623**, 186–210.

[15] P. Flajolet, R. Sedgewick, *Analytic Combinatorics.* Book in preparation (1999), see also INRIA Research Reports 1888, 2026, 2376, 2956.

[16] P. Flajolet, B. Vallée, *Continued fraction Algorithms, Functional operators and Structure constants.* Theoretical Computer Science **194** (1998), 1–34.

[17] A. Grothendieck, *Produits tensoriels topologiques et espaces nucléaires.* Mem. Am. Math. Soc. **16** (1955).

[18] A. Grothendieck, *La théorie de Fredholm.* Bull. Soc. Math. France **84**, 319–384.

[19] H. HEILBRONN, *On the average length of a class of continued fractions.* Number Theory and Analysis, ed. by P. Turan, New-York, Plenum (1969), 87–96.

[20] D. HENSLEY, *The number of steps in the Euclidean algorithm.* Journal of Number Theory **49** (1994), 142–182.

[21] T. KATO, *Perturbation Theory for Linear Operators.* Springer-Verlag (1980).

[22] A.I. KHINCHIN, *Continued Fractions.* University of Chicago Press, Chicago (1964). A translation of the Russian original published in 1935.

[23] D.E. KNUTH, *The art of Computer programming*, Volume 2. 3rd edition, Addison Wesley, Reading, Massachussets (1998).

[24] M. KRASNOSELSKY, *Positive solutions of operator equations.* P. Noordhoff, Groningen (1964).

[25] R.O. KUZMIN, *Sur un problème de Gauss.* Atti del Congresso Internationale dei Matematici 6 (Bologna, 1928), 83–89.

[26] P. LÉVY *Sur les lois de probabilité dont dépendent les quotients complets et incomplets d'une fraction continue.* Bull. Soc. Math. France **57** (1929), 178-194.

[27] E.R. LORCH, *Spectral Theory.* Oxford University Press, New York (1962).

[28] D.H. MAYER, *On a ζ function related to the continued fraction transformation.* Bulletin de la Société Mathématique de France **104** (1976), 195–203.

[29] D.H. MAYER, *Continued fractions and related transformations.* In: Ergodic Theory, Symbolic Dynamics and Hyperbolic Spaces, T. Bedford, M. Keane, and C. Series, Eds. Oxford University Press (1991), 175–222.

[30] G.J. RIEGER, *Über die mittlere Schrittazahl bei Divisionalgorithmen.* Math. Nachr. (1978), 157–180.

[31] D. RUELLE, *Thermodynamic formalism.* Addison Wesley (1978).

[32] D. RUELLE, *Dynamical Zeta Functions for Piecewise Monotone Maps of the Interval.* CRM Monograph Series **4**, American Mathematical Society, Providence (1994).

[33] J. SHAPIRO, *Composition operators and classical function theory.* Universitext: Tracts in Mathematics, Springer-Verlag (1993).

[34] G. TENENBAUM, *Introduction à la théorie analytique des nombres.* vol. 13. Institut Élie Cartan, Nancy, France (1990).

[35] B. VALLÉE, *Fractions continues à contraintes périodiques.* Journal of Number Theory **72** (1998), 183–235.

[36] B. VALLÉE, *Dynamics of the Binary Euclidean Algorithm: Functional Analysis and Operators.* Algorithmica **22** (1998), 660–685.

[37] B. VALLÉE, *A Unifying Framework for the analysis of a class of Euclidean Algorithms.* Proceedings of LATIN'2000, Lecture Notes in Computer Science **1776**, Springer, 343–354.

[38] B. VALLÉE, *Dynamical Analysis of a Class of Euclidean Algorithms.* Extended version of [37], to appear in Theoretical Computer Science (2001).

[39] J. VUILLEMIN, *Exact real computer arithmetic with continued fractions.* IEEE Transactions on Computers **39**, 8 (Aug. 1990), 1087–1105.

[40] E. WIRSING, *On the theorem of Gauss-Kusmin–Lévy and a Frobenius-type theorem for function spaces.* Acta Arithmetica **24** (1974), 507–528.

[41] A.C. YAO, D.E. KNUTH, *Analysis of the subtractive algorithm for greatest common divisors.* Proc. Nat. Acad. Sc. USA **72** (1975), 4720-4722.

Brigitte VALLÉE
GREYC, UMR 6072
Université de Caen
14032 Caen
France
E-mail : Brigitte.Vallee@info.unicaen.fr