Discrete Mathematics and Theoretical Computer Science **(subm.)**, by the authors, 1–rev

The Lyapunov Tortoise and the dyadic Hare

Benoît Daireaux[1] and Véronique Maume-Deschamps[2] and Brigitte Vallée[1]

[1] *CNRS UMR 6072, GREYC, Université de Caen, F-14032 Caen, France*
[2] *Institut de mathematiques de Bourgogne Universite de Bourgogne - UMR 5584 du CNRS 9,Avenue Alain Savary B.P. 47870 21078 Dijon Cedex France*

We study a gcd algorithm directed by Least Significant Bits, the so–called LSB algorithm, and provide a precise average–case analysis of its main parameters [number of iterations, number of shifts, etc. . .]. This analysis is based on a precise study of the dynamical systems which provide a continuous extension of the algorithm, and, here, it is proved convenient to use both a 2–adic extension and a real one. This leads to the framework of products of random matrices, and our results thus involve a constant γ which is the Lyapunov exponent of the set of matrices relative to the algorithm. The algorithm can be viewed as a race between a dyadic hare with a speed of 2 bits by step and a "real" tortoise with a speed equal to $\gamma/\log 2 \sim 0.05$ bits by step. Even if the tortoise starts before the hare, the hare easily catches up with the tortoise [unlike in Aesop's fable [1]. . .], and the algorithm terminates.

1 Introduction

Like any gcd algorithm, the LSB algorithm performs a sequence of divisions and exchanges, and the divisions are used to "shorten" the integers. However, the LSB division aims to create zeroes on the right of the binary extension [whereas usual ones create zeroes on the left], which right–shifts then easily suppress. At a first glance, it resembles the Binary Algorithm. However, both algorithms are quite different: in the Binary Algorithm, the exchange is performed as soon as the remainder r becomes smaller than the divisor u, whereas the LSB algorithm performs an exchange as soon as the remainder r has a dyadic norm smaller than u. In this sense, the Binary algorithm tends to shorten integers both on the right and on the left, while the LSB algorithm is totally dyadic, only shortens on the right, and may even increases the size on the left...

To the best of our knowledge, the LSB algorithm was introduced for the first time by Stehl´e and Zimmermann [21], who use it in their improvement of the recursive gcd algorithm. This algorithm appears to be interesting, because it is more "stable" than other gcd–algorithms. The authors provided a worst–case analysis of the algorithm, which proves that, for a fixed input–size, the maximal number of iterations grows linearly with the size of data. They also made experimental observations [20]; for instance, they remark that the size of remainders is not generally decreasing, a quotient of ± 1 occurs with probability 1/3, and the average number of iterations appears to be linear with respect to size.

We succeed to prove these experimental observations. The analyses provided here are instances of dynamical analysis, [described in [23] for instance], where one proceeds in three main steps: First, the (discrete) algorithm is extended into a continuous process, which can be defined in terms of a dynamical system, where executions of the gcd algorithm are then described by particular trajectories [i.e., trajectories of "rational" points]. Second, the main parameters of the algorithm are extended and studied in this continuous framework: the study of particular trajectories is replaced by the study of generic trajectories. Finally, one operates a transfer "from continuous to discrete", and proves that the probabilistic behaviour of gcd algorithms [related to "rational" trajectories] is quite similar to the behaviour of their continuous counterparts [related to generic trajectories].

Particulars of the LSB Algorithm. In the LSB case, the analysis will be more involved. We have to record the number of zeroes produced on the left of integers, and this is easily done by the 2–adic valuation. But, we also have to take into account the total size of integers, and this cannot be done in the dyadic framework. In short, the topology is ultrametric, but the size is archimedean.
It will prove convenient to use the set of matrices $\mathcal{N}$,

$$\mathcal{N} := \{N_{[q]} = \begin{pmatrix} 0 & 1 \\ 1 & q \end{pmatrix}; q = \frac{a}{2^k}; k \geq 1, a \text{ odd}, a \in [-2^k+1, 2^k-1]\}, \tag{1}$$

where each matrix $N_{[q]}$ is drawn with probability $\delta_q := 1/|q|_2^2 = 2^{-2k}$. The choice of probabilities is related to the 2–adic topology, while the Euclidean norm of matrix N is used to deal with the usual notion of size. Then, the Lyapunov exponent γ of this set of matrices plays a fundamental rôle in our paper. It is classically defined as the limit

$$\gamma := \frac{1}{n} \lim_{n\to\infty} \mathbb{E}\,[\log ||N_1 \cdot N_2 \cdot \ldots \cdot N_n||],$$

[when each matrix N_k is independently drawn in $\mathcal{N}$]. More precisely, the exponent $\gamma_0 := \gamma/\log 2$ measures the average increase of integer size at each step. On the other hand, the integer k in (1) is equal to the right–shift, and thus the decrease of the integer size; in our probabilistic model inherited from the dyadic topology, its average value is equal to 2. We have then explained our title: our tortoise lives in the real world, and moves [on average] according to the Lyapunov exponent, while the move of our hare is directed by dyadic rules.

Random matrices and iterated functions systems. In summary, our first step transforms the analysis of the LSB algorithm into a study of the set $\mathcal{N}$ of random matrices. The subject of random matrices has been widely studied in works of Furstenberg [12], Guivarc'h and Raugi [14], Le Page [18], and is well summarized in the book of Bougerol and Lacroix [3]. In particular, Chapter II of Part A of this book and the whole Part B are devoted to the case of matrices of order 2. We are now in the "real" world, and the dyadic topology is just translated on probabilities. Like in [3], we then consider the action of matrices $N_{[q]}$ on the real projective line, and it proves more convenient to transport the whole framewok on the compact torus $J := \mathbb{R}/\pi\mathbb{Z}$ [via the "tangent" map]. Our set $\mathcal{N}$ is now transformed into a set $\mathcal{L}$ of random functions $\ell : J \to J$ (where each function ℓ is drawn with dyadic probability δ_ℓ), and we find ourselves within the framework of Iterated Functions Systems (IFS), where it is classical to deal with transfer operators $\mathbf{G}_z$, defined as

$$\mathbf{G}_z[f](x) := \sum_{\ell\in\mathcal{L}} \delta_\ell \cdot |\ell'(x)|^z \cdot f \circ \ell(x),$$

which depend on a parameter z, act on functions $f : J \to \mathbb{C}$ and "summarize" all the properties of the set $\mathcal{N}$. Note that parameter z "marks" the "real" size (symbolized by our tortoise).

In our study, we need a double generalization of these transfer operators, and introduce two new parameters, a parameter t, which "marks" the dyadic size (symbolized by our hare), and a (third) parameter w, which marks the step–cost c that we wish to study. Accordingly, the whole paper deals with the operator

$$\mathbf{G}_{t,z,w}[f] := \sum_{\ell\in\mathcal{L}} \delta_\ell^t \cdot \exp[wc(\ell)] \cdot |\ell'|^z \cdot f\circ\ell.$$

Like in previous dynamical analyses[†], we prove that this operator plays the rôle of a generating operator, which itself generates all the objects of "classical" analysis of algorithms —namely (Dirichlet) generating functions, or the moment generating functions. The main properties of set $\mathcal{N}$ of matrices can be "read" on the (dominant) spectral objects of the operator, namely its dominant eigenvalue $\lambda(t,z,w)$. Notably, the Lyapounov exponent γ is related to the derivative of $z \to \lambda(1,z,0)$ at $z=0$,

$$\gamma = -\frac{1}{2}\lambda_z'(1,0,0).$$

The main results. Our first result confirms and proves all the experimental facts observed in [20, 21], and, more generally, describes, in a very precise way, a generic execution of the LSB–algorithm. On an integer input (u,v), the LSB algorithm performs $P(u,v)$ iterations, with a total number $K(u,v)$ of right-shifts, a total number $S(u,v)$ of subtractions; during the execution, a quotient a occurs $C_a(u,v)$ times. It performs a total of $B(u,v)$ elementary operations on bits [$B(u,v)$ is often called the bit-complexity]. What are the average values of these parameters when (u,v) is a random pair of binary length N, for sufficiently large N? We prove, in Theorem 1, that all the mean values of these parameters [except the bit–complexity] are of asymptotic order N, and the mean value of the bit–complexity is of asymptotic order N^2. Furthermore, all the constants that appear in the dominant terms involve the Lyapunov exponent in base 2, namely $\gamma_0 := \gamma/\log 2$,

$$\mathbb{E}_N[P] \sim \frac{1}{2-\gamma_0}\cdot N, \qquad \mathbb{E}_N[K] \sim 2\cdot\mathbb{E}_N[P], \qquad \mathbb{E}_N[S] \sim \frac{5}{2}\mathbb{E}_N[P], \qquad \mathbb{E}_N[B] \sim \mathbb{E}_N[S+K]\cdot\frac{N}{2}$$

$$\text{and, for a quotient } a \text{ with } \ell(a) \text{ binary digits,} \qquad \mathbb{E}_N[C_a] \sim \frac{1}{3}\cdot\frac{1}{4^{\ell(a)-1}}\cdot\mathbb{E}_N[P].$$

A numerical value for constant γ_0 is $\gamma_0 \sim 0.0344/\log 2 \sim 0.0497$. Then, we obtain

$$\mathbb{E}_N[P] \sim 0.51\cdot N \qquad \mathbb{E}_N[K+S] \sim 2.30\cdot N, \qquad E_N[B] \sim 1.15\cdot N^2.$$

This must be compared to the behaviour of the Binary Algorithm, which has already been analyzed in [22], where it is proven that

$$\mathbb{E}_N[P] \sim 0.39\cdot N, \qquad \mathbb{E}_N[K+B] \sim 2.11\cdot N, \qquad E_N[B] \sim 1.10\cdot N^2.$$

Then, it appears that the behaviour of LSB algorithm is quite similar to the Binary Algorithm.

Our second result provides an analysis of the continuous extension of the LSB algorithm. Since the LSB algorithm is based on the 2-adic norm, this extension is quite naturally a 2-adic extension, and we

[†] Remark that all previous dynamical analyses used dynamical systems, not iterated functions systems.

then work in the field $\mathbb{Q}_2$ of 2-adic numbers. This extension generates the (2–adic) continued fraction expansion of a dyadic number x, and in particular provides after n steps a rational approximation Q_n of x, its n-th convergent. Theorem 2 studies the size $L(Q_n)$ of the n–th convergent, and proves that it asymptotically follows a Gaussian Law. Notably, the expectation of the size satisfies

$$\mathbb{E}[L(Q_n)] \sim (2+\gamma_0)\cdot n.$$

Plan of the paper. We present in Section 2 the LSB algorithm, the 2-adic continued fraction expansion and state our main results, Theorems 1 and 2. Section 3 introduces the LSB dynamical system, which is further extended into an iterated functions system (IFS). We present the main actor, the transfer operator relative to this IFS. Then, Propositions 1 and 2 perform transfers "from continuous to discrete", and relate the transfer operator to generating functions. Finally, Theorem 3 [proved in section 5] describes the main analytical properties of the operator which make possible to apply the Tauberian theorem and the Quasi-Power theorem for proving Theorems 1 and 2.

2 The LSB algorithm.

This section is devoted to describing the general framework of this paper. First, we present the LSB algorithm, and make precise the probabilistic model used in our analysis. Then, we state our first main result [Theorem 1] which provides the mean values of the main parameters of the LSB algorithm. In a second stage, we extend this algorithm into a continuous process, namely the 2-adic (centered) continued fraction expansion. Our second main result [Theorem 2] exhibits the Gaussian behaviour of the length of continuants.

2.1 The LSB Division.

The division directed by the least significant bits [LSB's] of integers resembles the usual one, which is directed by the most significant bits [MSB's]; however it aims to create zeroes on the right of the binary expansion of the integers, whereas the usual division creates them on the left of this expansion. Since the 2–adic valuation equals the number of zeroes on the right, it is then quite natural to describe the LSB division with the help of the 2-adic norm : Indeed, the LSB division can be defined by replacing the usual norm by the 2-adic one in the definition of the classical Euclidean division.
Let us first recall some facts about the 2-adic valuation. The 2-adic valuation of an integer $a \in \mathbb{Z}$, denoted by $\nu(a)$, is the largest k such that 2^k divides a. The valuation of the rational $a/b \in \mathbb{Q}$ is then defined by: $\nu(a/b) = \nu(a) - \nu(b)$. From this valuation, one defines the 2-adic absolute value of a rational x:

$$|x|_2 = 2^{-\nu(x)}.$$

The 2-adic distance between two integers x and y is then closely related to the number of significant bits which are common between x and y. This is why it is very useful in the case when the division between u and v is directed by the least significant bits of u and v. It is a ultrametric absolute value, and the relations

$$|x+y|_2 \leq \max(|x|_2, |y|_2), \qquad |x+y|_2 = \max(|x|_2, |y|_2) \quad \text{if } |x|_2 \neq |y|_2$$

always hold.

First, we denote by $\widetilde{\Omega}$ the set of valid inputs of the division,

$$\widetilde{\Omega} := \{(u,v) \in \mathbb{Z}^2; v \text{ odd}, u \text{ even}\}. \tag{2}$$

Given a valid input $(u,v) \in \widetilde{\Omega}$, the centered LSB division returns a remainder r smaller (with respect to the 2-adic norm) than u and a quotient q such that

$$v = uq + r, \qquad \text{with} \qquad |q| < 1, \quad 0 \le |r|_2 \le \frac{1}{2}|u|_2. \tag{3}$$

Since the pair (r,u) satisfies $\nu(r) > \nu(u)$, the shifted pair $(r',u') := (2^{-\nu(u)} \cdot r, 2^{-\nu(u)} \cdot u)$ belongs to the set $\widetilde{\Omega}$: this will be the new pair for the next step.
For instance, the division between $v = 29 = 11101_2$ and $u = 12 = 1100_2$ is naively made as follows, in order to obtain a remainder r with at least three zeroes on the right: with a right binary shift, we "forget" the two zeroes on the right of u and the difference between 11101_2 and 11_2 equals 11010_2. There is only one zero on the right, then we "forget" it and we continue; the difference $1101_2 - 11_2 = 1010$ creates one supplementary zero on the right: we "forget" it and we continue; finally the difference $101_2 - 11_2 = 10_2$ creates a third zero on the right. Then, we stop and finally the division can be written as

$$11101_2 = 1100_2 \times \frac{1_2 + 10_2 + 100_2}{100_2} + 1000_2, \qquad \textit{i.e.}, \quad 29 = \frac{7}{4}12 + 8.$$

Such a process leads to a division of the form

$$v = uq + r,\ 0 < q < 2 \text{ and } 0 \le |r|_2 \le \frac{1}{2}|u|_2. \tag{4}$$

Since we wish to obtain a division of type (3), we finally center the quotient q and write

$$29 = \frac{-1}{4}12 + 32, \qquad 11101_2 = 1100_2 \times \frac{-1_2}{100_2} + 100000_2,$$

and the pair (r,u) is $(32,12)$. The new pair (r',u') is then obtained by right-shifting the pair (r,u). Finally, the new pair generated by the division of 29 by 12 is $(8,3)$.

Generally speaking, the (centered) quotient (also called the "digit") q is of the form

$$q = \frac{a}{2^k} \qquad \text{with} \quad k := \nu(u), \quad a = v \cdot \left(\frac{u}{2^{\nu(u)}}\right)^{-1} \text{cmod } 2^{k+1}.$$

Here $x \operatorname{cmod} y$ denotes the centered remainder of x mod y. Remark that a is odd and belongs to $[-2^k + 1, 2^k - 1]$. It is easy to prove that the set of possible digits relative to all valid pairs (u,v) is

$$\mathcal{Q} := \{\frac{a}{2^k}; k \ge 1, a \text{ odd}, a \in [-2^k + 1, 2^k - 1]\}. \tag{5}$$

Remark that, in the LSB division $v = qu + r$, the absolute value $|r|$ of the remainder may be strictly larger than $|u|$; It can be true even for the shifted r'. Of course, this situation cannot occur with the classical division.

Input : $(u,v) = (72001, 2011176)$
In base 2 $(u,v) = (111101011000000101000_2, 10001100101000001_2)$.

i	u_i [base 2]	u_i[base 10]	continuant r_{i+1}	continuant p_{i+1}	quotient $a_i/2^{k_i}$
0	**10001100101000001**	72001	1	0	
1	**111101011000000101**000	2011176	-11	1000	-3 / 8
2	**1100100110110101**0000	826192	1101	1000	1 / 2
3	**11000011000101**0000000	1598080	-100011	10001000	1 / 8
4	**100110001111**00000000	626432	11110011	-1000	-1 / 2
5	**111010010101**000000000	1911296	-101111111	1000101000	-1 / 2
6	**11000001001**0000000000	1582080	1001001101	1000001000	1 / 2
7	**1000100011**00000000000	1120256	-100001001001	11010011000	-1 / 2
8	**1000001011**000000000000	2142208	11101011	111010111000	1 / 2
9	**11**00000000000000	49152	-100000101011101	100001101111000	1 / 4
10	**1000001**000000000000000	2129920	100100010110101	11001001001000	-1 / 2
11	**10001**0000000000000000	1114112	-1011110010111111	10100000000101000	1 / 2
12	**11**0000000000000000000	1572864	10000011101100001011	-110001110001001000	-5 / 8
13	**1**000000000000000000000	2097152	10001100101000001	111101011000000101000	3 / 4

Fig. 1: An execution of the LSB Algorithm.

In the sequel, we will make a deep use of the matrix representation of the division: if we define for $q \in \mathcal{Q}$, the matrices

$$M_{[q]} = \begin{pmatrix} 0 & 2^k \\ 2^k & a \end{pmatrix}, \qquad N_{[q]} = \begin{pmatrix} 0 & 1 \\ 1 & q \end{pmatrix} = 2^{-k} M_{[q]}, \tag{6}$$

then the old pair (u,v), the intermediate pair (r,u) and the new pair (r',u') satisfy

$$\begin{pmatrix} u \\ v \end{pmatrix} = N_{[q]} \begin{pmatrix} r \\ u \end{pmatrix}, \qquad \begin{pmatrix} u \\ v \end{pmatrix} = M_{[q]} \begin{pmatrix} r' \\ u' \end{pmatrix}.$$

We denote by $\mathcal{M}$, [resp. $\mathcal{N}$] the set of matrices $M_{[q]}$ [resp. $N_{[q]}$] when $q \in \mathcal{Q}$. The set $\mathcal{N}$ plays an essential rôle in the paper.

2.2 The LSB Algorithm.

On the valid input (u,v) of $\widetilde{\Omega}$, the LSB algorithm performs a sequence of steps, each step being composed by a LSB division, followed by a binary shift and an exchange. The total execution on the input $(u_0 := v, u_1 := u)$ is described as follows

$$\left\{ \begin{array}{lll} u_0 = q_1 u_1 + r_1, & u_2 := 2^{-\nu(u_1)} \cdot r_1, & u_1 := 2^{-\nu(u_1)} \cdot u_1, \\ u_1 = q_2 u_2 + r_2, & u_3 := 2^{-\nu(u_2)} \cdot r_2, & u_2 := 2^{-\nu(u_2)} \cdot u_2, \\ \dots & \dots & \dots \\ u_{i-1} = q_i u_i + r_i, & u_{i+1} := 2^{-\nu(u_i)} \cdot r_i, & u_i := 2^{-\nu(u_i)} \cdot u_i \\ \dots & \dots & \dots \end{array} \right\}$$

and stops at the p-th iteration with $u_{p+1} = 0$. Figure 1 describes an instance of such an execution.

On an input (u,v) whose gcd equals d, the previous execution creates matrix products of the form

$$\begin{pmatrix} u \\ v \end{pmatrix} = M \begin{pmatrix} 0 \\ d \end{pmatrix} = N \begin{pmatrix} 0 \\ 2^k d \end{pmatrix}, \qquad \text{with} \quad M := M_{[q_1]} \cdot M_{[q_2]} \cdot \ldots \cdot M_{[q_p]}, \quad N := \frac{1}{2^k} M, \tag{7}$$

where $k = k_1 + \cdots + k_p$ is the total number of shifts performed. It also creates the continued fraction expansion of the rational u/v,

$$\frac{u}{v} = \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{\ddots + \cfrac{1}{q_p + 0}}}} \tag{8}$$

If $h_{[q]}(x)$ denotes the linear fractional transformation (LFT) associated to matrix $M_{[q]}$ [or $N_{[q]}$], defined as

$$h_{[q]}(x) := \frac{1}{q+x} = \frac{2^k}{a + 2^k x}, \tag{9}$$

then the previous continued fraction expansion can be written as

$$\frac{u}{v} = h_{[q_1]} \circ h_{[q_2]} \circ \ldots h_{[q_p]}(0) = h(0). \tag{10}$$

Remark that the LFT h and the matrix M are of the form

$$h(x) = \frac{\alpha x + \beta}{\gamma x + \delta}, \qquad M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

with $\alpha, \beta, \gamma, \delta$ coprime integers. When the algorithm performs p iterations, it thus gives rise to a continued fraction of depth p.

2.3 Probabilistic behaviour of the LSB Algorithm.

We wish to study this algorithm from a probabilistic point of view, and then provide a theory which explains the experimental facts already observed by Stelh´e and Zimmermann in [21] or [20]. These authors have studied this algorithm from the worst–case point of view. They have established that the algorithm runs in quadratic time (in the worst–case) and they have exhibited the precise worst–case number of iterations: It arises when each division–step uses the minimal–size quotient, equal to $1/2$, and involves the absolute value of the smallest eigenvalue of the matrix $M_{[1/2]}$ equal to $(\sqrt{17}-1)/2$. Then, the maximum number of iterations of the LSB Algorithm on a pair (u,v) with $\max(|u|,|v|) \le N$, is asymptotic to

$$\log_{\frac{\sqrt{17}-1}{2}} N.$$

They have also observed that the sequence of remainders $(u_0, u_1, u_2, \ldots, u_p)$ is not generally decreasing. Here, we wish to describe the probabilistic behaviour of some important parameters related to this algorithm, in order to compare them with already known results concerning other gcd algorithms.

In fact, we consider two sets Ω and $\widetilde{\Omega}$: the second one is formed with all the valid inputs of the algorithm, while the first one only contains the valid inputs that are coprime. We mainly deal with the set Ω. It may seem strange —at least from an algorithmic point of view— to study the sets of inputs for which the answer of the algorithm is trivial! However, we shall see that this (trivial) set is in a sense generic, and it will be easy to transfer the results on Ω to the (more natural) set $\widetilde{\Omega}$.

For the LSB Algorithm, the sets $\widetilde{\Omega}$ and Ω are

$$\widetilde{\Omega} := \{(u,v) \in \mathbb{Z}^2; v \text{ odd}, u \text{ even}\}, \qquad \Omega := \{(u,v) \in \widetilde{\Omega},\ \gcd(u,v) = 1\}.$$

We then endow these sets with a size. It is convenient here to deal with the Euclidean norm $||.||$, so that the square of the norm of the input (u,v) is (u^2+v^2). We then choose as the size of the input the quantity $L(u,v)$ defined from the binary length ℓ, $[\ell(x) := \lfloor \log_2 x \rfloor + 1]$,

$$L(u,v) := \frac{1}{2}\ell(u^2+v^2). \tag{11}$$

Finally, the sets

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

gather valid inputs of size N and are endowed with uniform probabilities denoted by $\mathbb{P}_N, \widetilde{\mathbb{P}}_N$. We wish to analyze the probabilistic behavior of the main observables (as digits or continuants) on the set Ω_N, when the size N of the input becomes large. We then (easily) return to $\widetilde{\Omega}_N$.

The complexity analysis of each algorithm first aims to quantify the number of iterations that are performed during the execution (3). More generally, we wish to study general additive parameters which only depend on the sequence of the digits q_i. We consider a cost c defined on the set Q, and we attach to the execution (3) of the LSB algorithm on the input (u,v) the total cost $C(u,v)$ defined by

$$C(u,v) := \sum_{i=1}^{p} c(q_i). \tag{13}$$

Here, we consider a large class of digit-costs c for which the average

$$\mu[c] := \sum_{q \in Q} \frac{1}{|q|_2^2} \cdot c(q) \tag{14}$$

is finite. This class contains some particular parameters which are are of great algorithmic interest. For instance, if $c = 1$, then $C = P$ is the number of iterations. If c is the characteristic function of some particular quotient q_0, then C is the number of occurrences of this particular quotient during the execution of the algorithm. If c is the digit–size ℓ, then C is the length of the binary encoding of the continued fraction. If $c(q) := k$, then $C = K$ is the total number of binary shifts performed by the algorithm. If $c(q) := s(a)$ isthe number of ones in the binary representation of a, then S is the total number of subtractions performed by the algorithm. If $c(u,q) := \ell(u) \cdot [k(q) + s(a)]$ then

$$B(u,v) = \sum_{i=1}^{p} \ell(u_i)[k(q_i) + s(a_i)]$$

is the complexity in bits of one execution of the algorithm.

2.4 The first result.

As is usual in probabilistic analysis of algorithms, generating functions are the basic tools in our study. When interested in a total cost C, we deal with the bivariate generating function $S_C(s,w)$,

$$S_C(s,w) := \sum_{(u,v)\in\Omega} \frac{\exp[wC(u,v)]}{(u^2+v^2)^s},$$

and we look for an alternative expression for it [see Proposition 1]. Then, the Dirichlet series $T_C(s)$ and $T_1(s)$,

$$T_C(s) := \sum_{(u,v)\in\Omega} \frac{C(u,v)}{(u^2+v^2)^s} = \sum_{n\geq 1} \frac{t_n}{n^s}, \qquad T_1(s) = \sum_{(u,v)\in\Omega} \frac{1}{(u^2+v^2)^s} = \sum_{n\geq 1} \frac{|\Omega_n|}{n^s}$$

satisfy

$$T_C(s) = \frac{\partial}{\partial w} S_C(s,w)]_{w=0}, \qquad T_1(s) = S_C(s,0),$$

and they inherit the alternative expression obtained for $S_C(s,w)$. On the other hand, t_n is the cumulated cost C on the set of pairs (u,v) for which (u^2+v^2) equals n. Then, the expectation of cost C on Ω_N can be expressed with the partial sums of the coefficients of the two series

$$\mathbb{E}_N[C] := \frac{\sum_{n=2^{2N-1}}^{2^{2N}} t_n}{\sum_{n=2^{2N-1}}^{2^{2N}} |\Omega_n|}.$$

Finally, Tauberian Theorems will be used for "extracting" coefficients from a Dirichlet series [see Theorem A].
Remark that the series $\widetilde{S}_C(s,w)$ [the analogue of $S(s,w)$ on $\widetilde{\Omega}$] is closely related to $S_C(s,w)$. This is due to the fact that, for $(u,v)\in\Omega$, the two costs $C(du,dv)$ and $C(u,v)$ are equal. Then,

$$\widetilde{S}(s,w) = Z(s)\cdot S(s,w), \qquad \text{where} \quad Z(s) := \sum_{(u,v)\in\widetilde{\Omega}} \frac{1}{(u^2+v^2)^s}$$

is a Zeta function closely related to the Zeta function on $\mathbb{Z}[i]$.

Consider the set $\mathcal{N} := \{N_{[q]};\quad q\in\mathcal{Q}\}$, where each matrix $N_{[q]}$ is chosen with probability $|q|_2^{-2}$. This is a set of random matrices, and we can define the binary Lyapunov exponent of this set $\mathcal{N}$,

$$\gamma_0 := \frac{1}{n}\lim_{n\to\infty} \mathbb{E}[\log_2 ||N_1\cdot N_2\cdot\ldots N_n||].$$

This quantity will be proved to exist and to be strictly positive. Extensive computations [11] have shown that γ_0 is small, and close to 0.0497. This quantity will play a central rôle in the whole paper.

Our first theorem provides the asymptotic behaviour of the expectation of a general additive cost C on sets $\Omega_N, \widetilde{\Omega}_N$, and we focus on particular parameters of algorithmic interest, namely the number P of iterations, the total number K of binary shifts, the number S of subtractions. We obtain also the asymptotic behoviour of the compexity in bits B.

Theorem 1. *Consider an additive cost C associated to a digit–cost c. On the sets $\Omega_N, \widetilde{\Omega}_N$, endowed with the uniform probability, the average value of C is asymptotically linear with respect to the input size N,*

$$\mathbb{E}_N[C] \sim \widetilde{\mathbb{E}}_N[C] \sim \frac{1}{2-\gamma_0} \cdot \mu[C] \cdot N,$$

Here γ_0 is the binary Lyapunov exponent of set $\mathcal{N}$ and $\mu[C]$ is [by definition] equal to the average $\mu[c]$ of digit–cost c

$$\mu[C] := \mu[c] := \sum_{q \in Q} \frac{1}{|q|_2^2} \cdot c(q).$$

For costs P (number of iterations), K(number total of shifts), S (number of subtractions), C_a (number of occurrences of quotients with numerator equal to a), the constants are

$$\mu[P] = 1, \qquad \mu[K] = 2, \qquad \mu[S] = \frac{5}{2}, \qquad \mu[C_a] = \frac{4}{3} \cdot 4^{-\ell(a)}.$$

On the sets $\Omega_N, \widetilde{\Omega}_N$, endowed with the uniform probability, the average value of the bit–complexity B is asymptotically linear with respect to the input size N,

$$\mathbb{E}_N[B] \sim \widetilde{\mathbb{E}}_N[B] \sim \frac{1}{2-\gamma_0} \cdot \mu[K+S] \cdot \frac{N^2}{2}.$$

Remark. This theorem perfectly fits the following heuristic model. An execution of the algorithm is a race between the Lyapounov Tortoise and the Dyadic Hare. At any step of the algorithm, the hare is on the right of the number, while the tortoise is on the left. At the beginning, the tortoise is thus N bits ahead the hare. The average speed of the tortoise is γ_0 bits by step, and the hare runs much faster since its average speed is 2 bits by step. The hare thus wins $2-\gamma_0$ bits by step to the tortoise and finally catches with it after $N/(2-\gamma_0)$ steps.

2.5 Extension of the LSB algorithm.

Our second result provides an analysis of the continuous extension of the LSB algorithm. Since the LSB algorithm is based on the 2-adic norm, this extension is quite naturally a 2-adic extension, and we then work in the field $\mathbb{Q}_2$ of 2-adic numbers. We refer to Gouvea [13] and Koblitz [17] for a good introduction on p-adic numbers. The set $\mathbb{Q}_2$ is the completion of $\mathbb{Q}$ with respect to the 2-adic absolute value. It is an ultrametric locally compact space and the set $\mathbb{Q}$ is dense in $\mathbb{Q}_2$. The Hensel expansion provides a natural representation of 2-adic numbers : Each $y \in \mathbb{Q}_2$ has a unique expansion of the form

$$y = \sum_{n \geq n_0} a_n 2^n, \quad \text{with } a_n \in \{0,1\} \text{ and } n_0 \in \mathbb{Z}. \tag{15}$$

This expansion is in a sense dual to the binary expansion of a real x. However, in the Hensel expansion, the exponents n belong to a set of the form $\{n \in \mathbb{Z}; n \geq n_0\}$ and may tend to $+\infty$ while in the binary expansion, the exponents belong to a set of the form $\{n \in \mathbb{Z}; n \leq n_0\}$ and may tend to $-\infty$.

From the Hensel expansion, it is easy to define the 2-adic (non–centered) integer part $\lfloor x \rfloor_2$ and the (non–centered) fractional part $\{x\}_2$ of a 2-adic number x

$$\lfloor x \rfloor_2 = \sum_{n=\nu(x)}^{0} \alpha_n 2^n, \qquad \text{and } \{x\}_2 := \sum_{n \geq 1} \alpha_n 2^n.$$

Then, $\lfloor x \rfloor_2$ is a rational of the form $a/2^k$, with a odd and $1 \leq a < 2^{k+1}$ so that $\lfloor x \rfloor_2$ belongs to $]0,2[$. The quantity $\{x\}_2$ defines a 2–adic number which belongs to the open unit ball $\mathcal{B}$ of $\mathbb{Q}_2$, (it is also the closed ball of radius $1/2$),

$$\mathcal{B} := \{x \in \mathbb{Q}_2,\ |x|_2 < 1\} = \left\{x \in \mathbb{Q}_2,\ |x|_2 \leq \frac{1}{2}\right\}. \tag{16}$$

We can "center" the rational $\lfloor x \rfloor_2$ in order to get a rational $\lceil x \rfloor_2$ which belong to $]-1,+1[$:

If $\lfloor x \rfloor_2 > 1$, **then** $\lceil x \rfloor_2 := \lfloor x \rfloor_2 - 2, \quad \{\{x\}\}_2 := \{x\}_2 + 2,$
else $\lceil x \rfloor_2 := \lfloor x \rfloor_2, \quad \{\{x\}\}_2 := \{x\}_2.$

Then, each 2- adic number x admits a unique decomposition of the form

$$x = \lceil x \rfloor_2 + \{\{x\}\}_2, \qquad \text{with} \quad \lceil x \rfloor_2 \in \mathbb{Q}, |\lceil x \rfloor_2| < 1, \{\{x\}\}_2 \in \mathcal{B}.$$

Remark that, when the integer pair (u,v) belongs to $\widetilde{\Omega}$, the rational u/v belongs to $\mathcal{B}$, and the previous decomposition, applied to the rational v/u is closely related to the LSB division on the integer pair (u,v) of the form $v = uq + r$ given in (3):

$$\left\lceil \frac{v}{u} \right\rfloor_2 = q, \qquad \left\{\left\{\frac{v}{u}\right\}\right\}_2 = \frac{r}{u} = \frac{r'}{u'}.$$

Then, the mapping $T : \mathcal{B} \to \mathcal{B}$ defined as

$$T(x) := \frac{1}{x} - \left\lceil \frac{1}{x} \right\rfloor_2 = \left\{\left\{\frac{1}{x}\right\}\right\}_2 \qquad \text{if } x \neq 0, \quad T(0) = 0, \tag{17}$$

extends one step of the LSB algorithm: on a rational u/v of $\mathcal{B}$, it produces the rational $r/u = r'/u'$.

This mapping is for instance described by Browkin in [5, 6]. With this mapping, we can define the (infinite) trajectory $(y, T(y), T^2(y), \ldots, T^i(y), \ldots)$ of any $y \in \mathcal{B}$, and also its 2-adic continued fraction expansion, of the form

$$y = \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{\ddots \cfrac{1}{q_n + \ddots}}}}, \tag{18}$$

where each digit $q_i = q_i(y) = \lfloor T^{i-1}(y) \rceil$ belongs to the set $\mathcal{Q}$.

Our second main result deals with the probabilistic analysis of this continuous process. We deal with the Haar measure η defined on the ball $\mathcal{B}$, and we are interested in the behaviour of truncated trajectories

$(y, T(y), \ldots T^n(y))$ at a fixed depth n, for a randomly chosen y. We wish to describe the evolution of parameters of these (truncated) trajectories, when the truncation depth becomes large. There are two main types of parameters.
First, we consider, as previously, a digit–cost c, and attach the total cost on the truncated trajectory $(y, T(y), \ldots T^n(y))$ defined as

$$C^{(n)}(y) := \sum_{i=1}^{n} c(q_i(y)).$$

Such costs have already been analysed by Daireaux in [7] for digit–costs of moderate growth, and they are proved to follow an asymptotic gaussian law. In the more general case when $\mu[c]$ (defined in (14)) is finite, the Ergodic Theorem shows that

$$\mathbb{E}[C^{(n)}] \sim \mu[c] \cdot n.$$

Remark. Our Theorem 1 also proves that rational trajectories behave (on average) as generic trajectories.

2.6 The second result

Here, we are interested in a second type of parameters, the so–called continuants, which are more difficult to analyse. Consider a 2-adic number $y \in \mathcal{B}$ and its CFE expansion, given in (18), truncated at depth n. This defines a vector $Q_n(y) := (p_n(y), r_n(y))$, via the relation

$$\begin{pmatrix} p_n(y) \\ r_n(y) \end{pmatrix} = M_{[q_1]} \cdot M_{[q_2]} \cdot \ldots \cdot M_{[q_n]} \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \tag{19}$$

and the rational $p_n(y)/r_n(y) = h_{[q_1]} \circ h_{[q_2]} \circ \ldots \circ h_{[q_n]}(0)$ approximates the 2-adic number y [with respect to the 2−adic norm]. We wish to study the random variable $\log||Q_n(y)||$ when the ball $\mathcal{B}$ is endowed with the Haar measure η. This quantity is equal to the size of the n–th approximant of y. We shall deal with the L´evy Moment Generating Function, $\mathbb{E}[\exp(w \log||Q||)]$, which is defined by

$$\mathbb{E}[\exp(w \log||Q_n||)] = \int_{\mathcal{B}} \exp[w \log||Q_n(y)||] \, d\eta(y). \tag{20}$$

where η is the Haar measure defined on the ball $\mathcal{B}$.
Our second main result proves that the random variable $\log||Q_n||$ follows an asymptotic gaussian law.

Theorem 2. *Consider any x in the open unit ball $\mathcal{B}$ of $\mathbf{Q}_2$ and denote by $Q_n(x) := (p_n(x), r_n(x))$ the vector of $\mathbf{Z}^2$ whose components form the n-th convergent p_n/r_n of the dyadic x. Denote by $||.||$ the Euclidean norm. When $\mathcal{B}$ is endowed with the uniform density with respect to the Haar measure η, the random variable $\log||Q_n||$ asymptotically follows a Gaussian Law, with an optimal speed of convergence in $O(1/\sqrt{n})$. Moreover, the mean and the variance satisfy*

$$\mathbb{E}[\log_2||Q_n||] = (2+\gamma_0) \cdot n + a + O(\tau^{-n}), \qquad \mathbb{V}[\log_2||Q_n||] = b \cdot n + c + O(\tau^{-n})$$

Here, γ_0 is the binary Lyapunov exponent of set of matrices $\mathcal{N}$, where each matrix $N_{[q]}$ is chosen with probability $|q|_2^{-2}$, and a, b, c, τ are constants, with $b > 0, \tau < 1$.

Remark. If we wish to deal with the size L defined in (11), we obtain

$$\mathbb{E}[L(Q_n)] = (2+\gamma_0) \cdot n + O(1).$$

Once again, this result can be explained by our heuristic Aesop's model. Here, the tortoise and the hare no longer race one against each other, but work together and add their respective speeds. Then the total speed is $2+\gamma_0$ bits per step, and, after n steps, they have performed a $(2+\gamma_0)\cdot n$ long run.

2.7 Comparison of the two results.

Comparing our two Theorems leads to a rather surprising phenomenon. If a rational number of size N behaves as a generic dyadic number, the size of its n–th convergent would be equal to $(2+\gamma_0)\cdot n$ [from Theorem 2]. On the other side, [from Theorem 1], the LSB algorithm terminates after $P(N) := N/(2-\gamma_0)$ steps, the length of the $P(N)$–th convergent should be equal to

$$N\cdot\frac{2+\gamma_0}{2-\gamma_0},$$

whereas it must be equal to N. In all the previously known cases (see [23]), the constant involved in Theorem 1 is the inverse of the constant of Theorem 2. Here, the difference suggests (and shows) that the continuants of a rational number do not behave in the same way as the continuants of a generic dyadic number. We have never seen this situation before, and, at the moment, we do not have a good explanation of this phenomenon.

3 Dynamical systems relative to the LSB algorithm

We first present the dynamical system underlying the 2-adic CFE, and explain why it is necessary to perform a further extension which both considers real trajectories in addition to 2-adic ones. We then introduce our main tool, the transfer operator, which we use as a generating operator. Finally, we state Theorem 3, which describes the main analytical properties of our transfer operators, and explain how to "transfer" analytical properties from the operator to our problem.

3.1 The LSB Dynamical System.

We recall that a dynamical system is a pair (X,S) formed by a compact set X and a mapping $S : X \to X$ for which there exist a suitable countable partition of X such that the restriction of S to each element of the partition is C^2 and invertible. Here, the pair $(\mathcal{B},T)$ (defined in (16, 17) defines a dynamical system which extends the LSB Algorithm. We now describe its main characteristics, and list some of its important properties.

Let $q\in\mathcal{Q}$ be an allowed digit defined in (5). We denote by $\mathcal{B}_q$ the open ball of center $1/q$ and of radius $|1/q|_2^2$:

$$\mathcal{B}_q := \left\{x\in\mathcal{B},\ \left|x-\frac{1}{q}\right|_2 < \left|\frac{1}{q}\right|_2^2\right\} = \left\{x\in\mathcal{B},\ \left|x-\frac{1}{q}\right|_2 \le \frac{1}{2}\left|\frac{1}{q}\right|_2^2\right\}.$$

When q varies in $\mathcal{Q}$, the balls $\mathcal{B}_q$ are disjoint and form a partition of $\mathcal{B}\setminus\{0\}$:

$$\bigcup_{q\in\mathcal{M}} \mathcal{B}_q = \mathcal{B}\setminus\{0\},\ \text{and}\ \mathcal{B}_q\cap\mathcal{B}_{q'} = \emptyset\ \text{for}\ q'\neq q.$$

For all $q\in\mathcal{Q}$, the restriction $T_{[q]} : \mathcal{B}_q \to \mathcal{B}$ of T to the ball $\mathcal{B}_q$ is of the form

$$T_{[q]}(x) = \frac{1}{x} - q,$$

and defines a surjective mapping : $T_{(q]}(\mathcal{B}_q) = \mathcal{B}$. Its inverse branch is the LFT $h_{[q]} : \mathcal{B} \mapsto \mathcal{B}_q$ already defined in (9)

$$h_{[q]}(x) = \frac{1}{q+x} = \frac{2^k}{2^k x + a} \qquad \text{if } q = \frac{a}{2^k}.$$

Remark that for $x \in \mathcal{B}$, its denominator $2^k x + a$ has a 2-adic norm equal to $|2^k x + a|_2 = |a|_2 = 1$. Then, the 2-adic norm of the derivative $h'_{[q]}$ is constant on $\mathcal{B}$,

$$|h'_q(x)|_2 = |\frac{2^{2k}}{(2^k x + a)^2}|_2 = 2^{-2k} = \frac{1}{|\det h|}, \qquad \forall x \in \mathcal{B}. \tag{21}$$

This property will be central in our study [see Section 3.2].
We denote by $\mathcal{H}$ the set of the inverse branches

$$\mathcal{H} := \{h_{[q]}, q \in \mathcal{Q}\},$$

by $\mathcal{H}^n$ the set formed by all possible composition of n elements of $\mathcal{H}$ and by $\mathcal{H}^*$ the semi-group generated by $\mathcal{H}$.

3.2 The transfer operator.

The main study in dynamical systems concerns itself with the interplay between properties of the transformation T and properties of trajectories –or encoded trajectories– under iteration of the transformation. The behaviour of typical trajectories of dynamical systems is more easily explained by examining the flow of densities.
Here, the set $\mathcal{B}$ is endowed with some initial distribution relative to some density $f = f_0$ with respect to the Haar measure η. The time evolution governed by the map T modifies the density, and the successive densities $f_1, f_2, \ldots, f_n, \ldots$ describe the global evolution of the system. Since the laws governing change do not change with time, there exists an operator $\mathbf{H}$ for which $f_1 = \mathbf{H}[f_0]$, $f_2 = \mathbf{H}[f_1]$, and more generally $f_n = \mathbf{H}[f_{n-1}] = \mathbf{H}^n[f_0]$ for all n. This operator is called the density transformer, or the Perron-Frobenius operator. It can be defined as

$$\mathbf{H}[f](x) = \sum_{h \in \mathcal{H}} |h'(x)|_2 \cdot f \circ h(x). \tag{22}$$

In previous dynamical analyses, which deal with real extensions, the quantity $|h'(0)|$ is the square of the denominator of $h(0)$ and thus the operator can be used as a generating operator for the input sizes. Now, the equality (21), $|h'(x)|_2 = 1/|\det h|$ entails an alternative form for the transfer operator

$$\mathbf{H}[f](x) = \sum_{h \in \mathcal{H}} |\det h|^{-1} \cdot f \circ h(x).$$

We observe two main facts. First, good news: since each branch h has a constant derivative, this dynamical system is "memoryless" : if the initial density f_0 is 1, then each step is independent on the previous history and chooses the matrix $M_{[q]}$ [or the LFT $h_{[q]}$] with probability $|q|_2^{-2}$. Second, bad news: we have "lost" the input sizes ..., and we are led to perform a new extension of the dynamical system where the (extended) transfer operator generates input sizes.

3.3 A new dynamical system.

Indeed, we aim generating, for $q \in \mathcal{Q}$, the quantities

$$\frac{||(u,v)||^2}{||M_{[q]}(u,v)||^2}, \qquad \text{with} \quad M_{[q]} = \begin{pmatrix} 0 & 2^k \\ 2^k & a \end{pmatrix} = 2^k N_{[q]} = 2^k \begin{pmatrix} 0 & 1 \\ 1 & q \end{pmatrix}. \tag{23}$$

These are real objects, that we wish to generate according to the 2–adic rules, and we are now in the context of products of random (independent) matrices; we adopt the point of view described in [3], and we consider the projective real line, endowed with the usual projective topology [not the real topology]. It is homeomorphic [via the map "tangent"] to the torus $J := \mathbb{R}/\pi\mathbb{Z}$ which can be identified with the interval $]-\pi/2,+\pi/2[$ (where the two points $-\pi/2$ and $+\pi/2$ are the same).

Consider now, for each branch $T_{[q]}$ of the LSB dynamical system, the map $\underline{T}_{[q]} : J \rightarrow J$ which is conjugate of $T_{[q]}$ by the map "tangent" and by $\underline{h}_{[q]}$ the inverse of $\underline{T}_{[q]}$,

$$\underline{T}_{[q]}(y) = \arctan\left(\frac{1}{\tan y} - q\right), \qquad \underline{h}_{[q]}(y) = \arctan\left(\frac{1}{\tan y + q}\right).$$

For $u/v = w = \tan y$, the equality

$$\frac{||(u,v)||^2}{||N_{[q]}(u,v)||^2} = \frac{1+w^2}{1+(w+q)^2} = |\underline{h}'_{[q]}(y)|$$

entails that, for any $x \in \mathcal{B}$,

$$\frac{||(u,v)||^2}{||M_{[q]}(u,v)||^2} = \frac{1}{2^{2k}} \frac{||(u,v)||^2}{||N_{[q]}(u,v)||^2} = |h'_{[q]}(x)|_2 \cdot |\underline{h}'_{[q]}(y)|. \tag{24}$$

We are then led to introduce the following dynamical system $(\mathcal{B} \times J, V)$ defined as follows: the partition is $((\mathcal{B}_q \times J)_{q \in \mathcal{Q}})$, the restriction of V to $\mathcal{B}_q \times J$ is the surjection $(T_{[q]}, \underline{T}_{[q]}) : \mathcal{B}_q \times J \rightarrow \mathcal{B} \times J$, and the set of inverse branches is the set of $(h_{[q]}, \underline{h}_{[q]})$. The Jacobian of the map $(x,y) \mapsto (h(x), \underline{h}(y))$ is the product $|h'(x)]_2 \cdot |\underline{h}'(y)| = \delta_h \cdot |\underline{h}'(y)|$, where δ_h is equal to $|\det h|^{-1}$. Then, the transfer operator related to the dynamical system

$$\mathbf{G}_{s,s}[F](x,y) := \sum_{h \in \mathcal{H}} \delta_h^s \cdot |\underline{h}'(y)|^s \cdot F(h(x), \underline{h}(y))$$

is, with (24), a generating operator for the quantities (23).

3.4 A system of iterated functions.

We need in fact a slightly different operator which depends on two parameters t and z, but acts on functions of the unique variable y,

$$\mathbf{G}_{t,z}[f](y) := \sum_{h \in \mathcal{H}} \delta_h^t \cdot |\underline{h}'(y)|^z \cdot f(\underline{h}(y)).$$

If $\mathcal{L}$ denotes the set $\mathcal{L} := \{\underline{h}; h \in \mathcal{H}\}$ and if we let $\delta_{\underline{h}} := \delta_h$[‡], we adopt the final expression:

$$\mathbf{G}_{t,z}[f](y) := \sum_{\ell \in \mathcal{L}} \delta_\ell^t \cdot |\ell'(y)|^z \cdot f \circ \ell(y), \qquad \mathbf{G}_s := \mathbf{G}_{s,s}. \tag{25}$$

[‡] We extend the quantity δ with multiplicativity and use it with an index $q \in \mathcal{Q}^\star$, or with an index in $\mathcal{M}^\star$, or in $\mathcal{L}^\star$ ...

In this operator, the probabilities δ_ℓ contain all the informations which come from the 2–adic topology, while the functions ℓ contain all the informations on the input sizes.
Remark that Equation (24) can be extended (with multiplicative properties) to any triple (ℓ, M, N) whose components are relative to the same element $q = (q_1, q_2, \ldots, q_n) \in \mathcal{Q}^\star$. For any (u,v,y) with $u/v = \tan y$, [and notably for $(0,1,0)$], and for any $q \in \mathcal{Q}^\star$, one has

$$|\ell'(y)| \cdot \delta_\ell = \frac{||(u,v)||^2}{||M(u,v)||^2}, \qquad |\ell'(0)| \cdot \delta_\ell = \frac{1}{||M(0,1)||^2}. \tag{26}$$

If we wish also generate the total cost $C(u,v)$ of the algorithm on the input (u,v), we use a weighted transfer operator. This operator depends on digit–cost c, and involves a third parameter w, which is used to “mark” the cost c,

$$\mathbf{G}_{t,z,w}[f](y) := \sum_{\ell \in \mathcal{L}} \delta_\ell^t \cdot \exp[wc(\ell)] \cdot |\ell'(y)|^z \cdot f \circ \ell(y). \tag{27}$$

Remark: Since $\ell = \ell_{[q]}$ for some $q \in \mathcal{Q}$, the digit–cost can be also defined directly on $\mathcal{L}$, and it can be extended on $\mathcal{L}^\star$ by additivity:

$$c(\ell) := c(q) \quad \text{for} \quad \ell = \ell_{[q]}, \qquad c(\ell_1 \circ \ell_2 \circ \ldots \circ \ell_n) := c(\ell_1) + c(\ell_2) + \ldots + c(\ell_n). \tag{28}$$

3.5 Transfer operator viewed as a generating operator.

The transfer operators defined in (25,27) can be viewed as generating operators for data size and/or for costs. The n-th iterate of the operator has exactly the same expression as the operator itself, except that the sum is now taken over the n–th power of the initial set, namely $\mathcal{L}^n$,

$$\mathbf{G}^n_{t,z,w}[f](y) := \sum_{\ell \in \mathcal{L}^n} \delta_\ell^t \cdot \exp[wc(\ell)] \cdot |\ell'(y)|^z \cdot f \circ \ell(y), \tag{29}$$

and the n-th iterate of the transfer operator describes the data sizes after n iterations.
When we wish to describe the evolution of data sizes during all the possible executions of the algorithm, which correspond to the semi–group $\mathcal{L}^\star$, we are led to work with the quasi-inverse of the transfer operator, which generates all the possible iterations, and, in a quite general framework, the quasi-inverse

$$(I - \mathbf{G}_{t,z,w})^{-1}[1](0)$$

will generate all the input sizes together with execution costs.

More precisely, the following results provide alternative forms for the two main objects involved in our analyses.

Proposition 1. *The bivariate Dirichlet series relative to an additive cost C relative to a digit–cost c satisfies*

$$S_C(s,w) = (I - \mathbf{G}_{s,s,w})^{-1}[1](0),$$

and the (univariate) Dirichlet series of cost C satisfies

$$T_C(s) = (I - \mathbf{G}_s)^{-1} \circ \mathbf{G}_s^{[c]} \circ (I - \mathbf{G}_s)^{-1}[1](0). \tag{30}$$

Here the operator $\mathbf{G}_s^{[c]}$ is the derivative of operator $\mathbf{G}_{s,s,w}$ at $w = 0$,

$$\mathbf{G}_s^{[c]}[f] := \sum_{\ell \in \mathcal{L}} \delta_\ell^s \cdot c(\ell) \cdot |\ell'|^s \cdot f \circ \ell. \tag{31}$$

The (univariate) Dirichlet series of bit–complexity B satisfies

$$T_B(s) = (I - \mathbf{G}_s)^{-1} \circ \mathbf{G}_s^{[k+s]} \circ (I - \mathbf{G}_s)^{-1} \circ \frac{d}{ds}\mathbf{G}_s \circ (I - \mathbf{G}_s)^{-1}[1](0). \tag{32}$$

Proof. This proof is a particular instance of a generic proof which can be found in [23] or in [7]. Notice that relation (10) defines a bijection between the subset Ω and the set $\mathcal{H}^\star$, and thus $\mathcal{L}^\star$. And, for any input $(u,v) \in \Omega$, relative to a function $\ell \in \mathcal{L}^\star$, the rational (u/v), the Euclidean norm $||(u,v)||^2$ and the cost $C(u,v)$ can be expressed by means of function ℓ, with (26) and (28),

$$\frac{u}{v} = \arctan \ell(0), \qquad \frac{1}{||(u,v)||^2} = \delta_\ell \cdot |\ell'(0)|, \qquad C(u,v) = c(\ell).$$

Thus, the bivariate generating function $S_C(s,w)$ satisfies

$$S_C(s,w) = \sum_{(u,v)\in\Omega} \frac{\exp[wC(u,v)]}{(u^2+v^2)^s} = \sum_{\ell\in\mathcal{L}^\star} \delta_\ell^s \cdot \exp[wc(\ell)] \cdot |\ell'(0)|^s = (I - \mathbf{G}_{s,s,w})^{-1}[1](0)$$

Then the alternative expression of $T_C(s)$ is obtained by taking the derivative (with respect to w) at $w = 0$ of the quasi-inverse.
For the bit-complexity, the proof is similar to the original proof provided in [2] or in [25], ■

Proposition 2. *Consider any x in the open unit ball $\mathcal{B}$ of $\mathbf{Q}_2$ and denote by $Q_n(x) := (p_n(x), q_n(x))$ the vector of $\mathbf{Z}^2$ whose components form the n-th convergent p_n/q_n of the dyadic x. Denote by $||.||$ the Euclidean norm. When $\mathcal{B}$ is endowed with the uniform density with respect to the Haar measure η, the moment generating function of the logarithm of the continuant norm $||Q_n||$ satisfies*

$$\mathbb{E}[\exp(2w \log ||Q_n||)] = \mathbf{G}^n_{1-w,-w}[1](0).$$

Proof. With the expression (19) of the continuant, and definition of the moment generating function in (20), one has:

$$\mathbb{E}[\exp(2w \log ||Q_n||)] = \sum_{q\in\mathcal{Q}^n} ||M_{[q]}(1,0)||^{2w} \cdot \eta[h_{[q]}(\mathcal{B})].$$

Using the fact that the measure of the ball $h_{[q]}(\mathcal{B})$ equals δ_q, and Equality (26), one obtains

$$\mathbb{E}[\exp(2w \log ||Q_n||)] = \sum_{q\in\mathcal{Q}^n} \delta_q \cdot |\ell'_{[q]}(0)|^{-w} \cdot \delta_q^{-w} = \mathbf{G}^n_{1-w,-w}[1](0). \qquad ■$$

4 Two main theorems.

Proofs of Theorems 1 and 2 are obtained from Propositions 1 and 2 by applying two main theorems. We prove Theorem 1 by using the alternative expression of the Dirichlet series $T_C(s)$ obtained in Proposition 1, together with the following Tauberian theorem, due to Delange, which extracts coefficients of Dirichlet series.

Theorem A. [Tauberian Theorem.] [8] *Let $T(s) := \sum_{n\geq 1} t_n n^{-s}$ be a Dirichlet series with non negative coefficients such that $T(s)$ converges for $\Re(s) > \sigma_0 > 0$. Assume that*
(i) $T(s)$ is analytic on $\Re(s) = \sigma, s \neq \sigma$, and
(ii) for some $\gamma \geq 0$, one has $T(s) = A(s)(s-\sigma)^{-\gamma-1} + C(s)$, where A, C are analytic at σ, with $A(\sigma) \neq 0$. Then,

$$\sum_{n=2^{2N-1}}^{2^{2N}} t_n = \frac{A(\sigma)}{\sigma\Gamma(\gamma+1)}(1-2^{-\sigma})(2\log 2)^{\gamma}\cdot 2^{2N\sigma}N^{\gamma}\cdot[1+\varepsilon(N)], \qquad \lim_{N\to\infty}\varepsilon(N) = 0,$$

We prove Theorem 2, by using the alternative expression of the L ́evy moment generating function obtained in Proposition 2, together with the following Theorem, due to Hwang, which proves the Gaussian behavior of a sequence of random variables as soon as their moment generating functions behave like quasi- powers.

Theorem B. [Quasi-Power Theorem.] [16] *Assume that the moment generating functions $\mathbb{E}[\exp(wR_n)]$ for a sequence of functions R_n are analytic in a complex neighborhood $\mathcal{W}$ of $w = 0$, and satisfy*

$$\mathbb{E}[\exp(wR_n)] = \exp[\beta_n U(w) + V(w)]\left(1 + O(\kappa_n^{-1})\right), \tag{33}$$

with β_n, $\kappa_n \to \infty$ as $n \to \infty$, $U(w)$, $V(w)$ analytic on $\mathcal{W}$ and the O–term uniform in $\mathcal{W}$. Then, the mean and the variance satisfy

$$\mathbb{E}[R_n] = U'(0)\cdot\beta_n + V'(0) + O(\kappa_n^{-1}), \qquad \mathbb{V}[R_n] = U''(0)\cdot\beta_n + V''(0) + O(\kappa_n^{-1}).$$

Furthermore, if $U''(0) \neq 0$, the distribution of R_n is asymptotically Gaussian, with speed of convergence $O(\kappa_n^{-1} + \beta_n^{-1/2})$,

$$\mathbb{P}_\nu\left[x \;\middle|\; \frac{R_n(x) - U'(0)n}{\sqrt{U''(0)n}} \leq Y\right] = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{Y} e^{-y^2/2}\,dy + O(\kappa_n^{-1} + \beta_n^{-1/2}).$$

4.1 Our main result in Functional Analysis.

We now state the following result [proved in Section 5] which will allow us to apply respectively the Tauberian Theorem [Theorem A] [8] and the Quasi-Power Theorem [Theorem B] [16] in order to obtain Theorems 1 and 2.

Theorem 3. *Denote by $\mathcal{A} := \{(t,z) \in \mathbb{C}^2; \Re t > 1/2\}$, by $\mathcal{D}_0$ a suitable (complex) neighborhood of $(1,0)$ and by $\mathcal{D}_1$ a suitable (complex) neighborhood of $(1,1)$. The following is true:*

(i) *For* $(t,z) \in \mathcal{A}$, *the operators* $\mathbf{G}_{t,z}, \mathbf{G}_{t,z}^{[c]}$ *[defined in (25, 31)] act on the functional space* $\mathcal{C}^1(J)$. *Moreover the map* $(t,z) \mapsto \mathbf{G}_{t,z}$ *is analytic.*

(ii) *For* $(t,z) \in \mathcal{D}_0 \cup \mathcal{D}_1$, *the operator* $\mathbf{G}_{t,z}$, *when it acts on* $\mathcal{C}^1(J)$ *admits a unique dominant eigenvalue* $\lambda(t,z)$ *separated from the remainder of the spectrum by a spectral gap.*

(iii) *The dominant eigenvalue* $\lambda(t,z)$ *satisfies the following relations*

$$\lambda(t,0) = \frac{2^{1-2t}}{1-2^{1-2t}}, \qquad \lambda(t,z) = \lambda(t,1-z), \qquad \lambda(1,0) = 1 = \lambda(1,1),$$

and the Lyapunov exponent γ *of the set* $\mathcal{N}$ *satisfies*

$$2\gamma = \lambda_z'(1,1) = -\lambda_z'(1,0).$$

(iv) *The map* $w \mapsto \log\lambda(1-w,-w)$ *has a second derivative which is non zero at* $w=0$.

(v) *On the punctured plane* $\Re s \geq 1, s \neq 1$, *the spectral radius* $R(s)$ *of* $\mathbf{G}_s$ *is strictly less than 1.*

4.2 Proofs of Theorems 1 and 2.

As we already said, we prove Theorems 1 and 2 with applying Theorems A and B to the series $T_C(s)$, and $\mathbb{E}[\exp(2w\log||Q_n||)]$. The link provided in Propositions 1 and 2 between these series and the transfer operator extends to the properties of these objects: Analytic properties of the generating functions can be deduced from spectral properties of the operator, so that Theorems A and B finally apply. We precise this in the next two propositions, whose proofs are in the appendix.

Proposition 3. *With Theorem 3, the Dirichlet series* $T_C(s)$ *and* $T_0(s)$ *fulfill the hypotheses of Tauberian Theorem [Theorem A] (at* $\sigma = 1$*).*

Proof. From Proposition 1, the operators relative to Dirichlet series $T_C(s)$, and $T_0(s)$ involve (one or two) occurrences of the quasi-inverse $(I-\mathbf{G}_s)^{-1}[f](y)$ [see (30)]. First, Property (v) of Theorem 3 entails that the quasi-inverse is analytic when s belongs to the punctured half-plane $\Re(s) \geq 1, s \neq 1$, so that Hypothesis (i) of Theorem A is satisfied. Second, Property (ii) of Theorem 3 entails, for $(s,s) \in \mathcal{D}_1$, the following spectral decomposition

$$(I-\mathbf{G}_s)^{-1}[f](y) = \frac{\lambda(s)}{1-\lambda(s)}\mathbf{P}_s[f](y) + (I-\mathbf{N}_s)^{-1}[f](y),$$

where $\mathbf{P}_s$ is the dominant projector and $\mathbf{R}_s$ is the operator "for the remainder of the spectrum" whose spectral radius is less than $\rho|\lambda(s)|$ (with $\rho < 1$). Then, for $(s,s) \in \mathcal{D}_1$, one has

$$(I-\mathbf{G}_s)^{-1}[f](y) \sim \frac{1}{(s-1)}\frac{-1}{\lambda'(1)}\mathbf{P}_1[f](y) \qquad \text{when} \quad s \to 1$$

and, since $\mathbf{G}_1$ is a density transformer, the dominant projector $\mathbf{P}_1$ satisfies

$$\mathbf{P}_1[f](y) = \varphi(y)\int_J f(t)dt$$

where φ is the dominant eigenfunction for $\mathbf{G}_1$ [i.e., the invariant density]. Then, for $(s,s) \in \mathcal{D}_1$, the dominant part of $T_C(s)$ is

$$T_C(s) \sim \frac{1}{(s-1)^2}\frac{1}{\lambda'(1)^2}\mathbf{P}_1 \circ \mathbf{G}_1^{[c]} \circ \mathbf{P}_1[1](0) \sim \frac{1}{(s-1)^2}\frac{1}{\lambda'(1)^2} \cdot A \cdot \varphi(0),$$

for some constant A, and the series $T_C(s)$ thus has a pole of order 2 at $s=1$, while $T_0(s)$ has a simple pole at $s=1$,

$$T_0(s) \sim \frac{1}{(s-1)}\frac{-1}{\lambda'(1)}\mathbf{P}_1[1](0) = \frac{1}{(s-1)}\frac{-1}{\lambda'(1)}\cdot\varphi(0).$$

Then, hypotheses of Theorem A are fulfilled for $T_C(s)$ and $T_0(s)$. Remark furthermore that

$$A = \int_J \mathbf{G}_1^{[c]}[\varphi](y)dy = \sum_{\ell\in\mathcal{L}} \delta_\ell \cdot c(\ell)\int_J |\ell'(y)|\cdot\varphi\circ\ell(y) = \sum_{\ell\in\mathcal{L}}\delta_\ell\cdot c(\ell),$$

and, with Theorem 3 (iii), one has :

$$|\lambda'(1)| = |\lambda'_t(1,1)+\lambda'_z(1,1)| = 4\log 2+\lambda'_z(1,0) = 4\log 2 - 2\gamma. \qquad \blacksquare$$

Proposition 4. *With Theorem 3, the moment generating functions* $\mathbb{E}[2\exp(w\log||Q_n||)]$ *fulfill the hypotheses of Quasi-Powers Theorem [Theorem B].*

Proof. Let $\mathcal{W}$ be a complex neighborhood of zero such that $(1-w,-w)$ belongs to the set $\mathcal{D}_0$ of Theorem 3. Then Property (i) of Theorem 3 implies that the moment generating functions $\mathbb{E}[\exp(2w\log||Q_n||)]$ are analytic for $w\in\mathcal{W}$. Theorem 3 (ii) entails a spectral decomposition of the form

$$\mathbf{G}^n_{1-w,-w}[f](x) = \lambda^n(1-w,-w)\mathbf{P}_{1-w,-w}[f](x) + \mathbf{R}^n_{1-w,-w}[f](x)$$

where $\mathbf{P}_{z,t}$ is the projector on the dominant eigensubspace and $\mathbf{R}_{z,t}$ is the operator for the remainder of the spectrum, whose spectral radius is less than $\rho|\lambda(z,t)$ [with $\rho<1$ for $(t,z)=(1-w,-w)\in\mathcal{D}_0$]. Then $||\mathbf{R}_{1-w,-w}||_1^n \le \tau^n|\lambda(1-w,-w)|^n$ for $\rho<\tau<1$, and

$$\mathbf{G}^n_{1-w,-w}[1](x) = \exp\left[n\log\lambda(1-w,-w)+\log\mathbf{P}_{1-w,-w}[1](x)\right]\left(1+O(\tau^{-n})\right).$$

Then, from Theorem 3 (iv), Theorem B can be applied with

$$U(w) = \log\lambda(1-w,-w), \quad V(w) = \log\mathbf{P}_{1-w,-w}[1](0) \quad \text{and } \kappa_n = \tau^{-n}.$$

With Theorem 3 (iii), the derivative $U'(0)$ is equals to

$$U'(0) = \lambda'_t(1,0) - \lambda'_z(1,0) = 4\log 2 + 2\gamma. \qquad \blacksquare$$

5 Functional Analysis: Proof of Theorem 3

This last Section is devoted to the proof of Theorem 3. We first introduce another set of matrices, formed by the inverses of the matrices $N_{[q]}$. Then, we recall the main results needed on random matrices, which we summarize in Theorem D. These results are a first step for proving Theorem 3. We explain why they are not sufficient for our purpose, and we establish in Propositions 6, 7, 8, the main steps that are necessary for proving Theorem 3.

5.1 Sets $\mathcal{N}$ and $\mathcal{N}^{-1}$

As we previously remarked in Section 3.4, the dynamics of the LSB Algorithm is closely related to the set $\mathcal{N}$ of random matrices

$$\mathcal{N} := \{N_{[q]}; \quad N_{[q]} := \begin{pmatrix} 0 & 1 \\ 1 & q \end{pmatrix}, \quad q \in \mathcal{Q}\},$$

relative to the set $\mathcal{Q}$ of dyadic rational numbers

$$\mathcal{Q} := \{q = \frac{a}{2^k}; k \geq 1, a \text{ odd}, a \in [-2^k+1, 2^k-1]\},$$

where q is drawn with probability $|q|_2^{-2}$. It is also related to set $\mathcal{L}$ of functions,

$$\mathcal{L} := \{\ell_{[q]}; \quad \ell_{[q]} : J \to J, \quad \ell_{[q]}(x) = \arctan\left(\frac{1}{q+\tan x}\right), \quad q \in \mathcal{Q}\},$$

where q is drawn with probability $|q|_2^{-2}$. Quite often, we omit the index q, and a generic element of $\mathcal{L}$ is denoted by ℓ, and its probability is denoted by δ_ℓ.
We shall need another set of matrices, the set

$$\mathcal{N}^{-1} := \{N_{[q]}^{-1} : q \in \mathcal{Q}\},$$

where each matrix $N_{[q]}^{-1}$ is chosen with probability δ_q. For an element $\ell \in \mathcal{L}$, relative to some matrix $N_{[q]}$, the element ℓ^{-1} is associated to matrix $N_{[q]}^{-1}$, with a relative probability δ_ℓ. The involution $(x,1) \mapsto (-1,x)$ of the projective line is exactly expressed by the involutive map Tilde on the torus J, defined as

$$\widetilde{y} : y \mapsto y + \pi/2. \tag{34}$$

Then, the expressions of matrices $N_{[q]}, N_{[q]}^{-1}$

$$N_{[q]}^{-1}(-1,x) = (x+q,-1); \qquad N_{[q]}(x,1) = (1,x+q)$$

lead to the following relation between ℓ and ℓ^{-1}

$$\ell^{-1}(\widetilde{y}) = \widetilde{\ell(y)}, \qquad [\ell^{-1}(\widetilde{y})]' = \ell'(y). \tag{35}$$

As it is mentionned in [3] [Part B, Proposition III. 2.5 page 243], this will provide nice relations between $\mathbf{G}_{t,z}$ and the operator $\widehat{\mathbf{G}}_{t,1-z}$ relative to sets $\mathcal{N}^{-1}, \mathcal{L}^{-1}$, defined by

$$\widehat{\mathbf{G}}_{t,z}[f](y) := \sum_{\ell \in \mathcal{L}^{-1}} \delta_\ell^t \cdot |\ell'(y)|^z \cdot f \circ \ell(y). \tag{36}$$

The transfer operator $T(z)$ introduced by Bougerol in [3] is defined as

$$T(z)[f](x) := \sum_{M \in \mathcal{M}} \delta_M \left(\frac{||M(u,v)||}{||(u,v)||}\right)^z \cdot f \circ h(x),$$

where h is the LFT relative to matrix M and (u,v) is any vector of $\mathbb{R}^2$ associated to point x of the projective line $\mathbf{P}(\mathbb{R})$. Remark that, with (26), $T(z)$ is just the conjugate [via the tangent map] of our operator $\mathbf{G}_{1-z/2,-z/2}$.

We shall use the results obtained in [3] for the operator $\mathbf{G}_{1-z,-z}$ for z near 0 in order to derive the analysis of operators $\mathbf{G}_{s,t}$ for s and t near 1. In [3], it is proven that $\mathbf{G}_{1-z,-z}$, when acting on the space $\mathbb{H}_\alpha(J)$ of α Hölder functions, is quasi-compact for z near 0 [see Theorem D]. Here, we shall prove that such a result holds on the space $\mathcal{C}^1(J)$ when (s,t) is near $(1,0)$ or $(1,1)$. We also need studying operators $\mathbf{G}_{s,s}$ in the half plane $\{s;\ \Re(s) \geq 1\}$.

5.2 Quasi–compactness.

We first recall the main notions about spectrum, essential spectrum and quasi–compactness.

For an operator $\mathbf{L}$ acting on a Banach space $\mathcal{F}$, the spectrum $\sigma(\mathbf{L})$ is the set of elements λ for which $\mathbf{L}-\lambda I$ is not inversible. There are two types of spectral values: an element of $\sigma(\mathbf{L})$ for which $\mathbf{L}-\lambda 1$ is not injective is called an eigenvalue and is of type 1; a spectral value which is not an eigenvalue is a spectral value of type 2: for such a spectral value λ, the operator $\mathbf{L}-\lambda I$ is not surjective.

The notion of essential spectrum was introduced by Nussbaum [19]. An element λ of $\sigma(\mathbf{L})$ belongs to the essential spectrum denoted by $\sigma^{[e]}(\mathbf{L})$ if it satisfies at least one of the three following properties:
(A) λ is an eigenvalue of infinite multiplicity,
(B) λ is not isolated in the spectrum
(C) The image of $\mathbf{G}-\lambda I$ is not closed.
Moreover, an eigenvalue which belongs to the essential spectrum is either of type (A) or of type (B) [19].

The spectral radius $R(\mathbf{L})$ is the supremum of moduli $|\lambda|$ when λ is an element of $\sigma(\mathbf{L})$, and the essential spectral radius $R^{[e]}(\mathbf{L})$ is the supremum of moduli $|\lambda|$ when λ is an element of $\sigma^{[e]}(\mathbf{L})$. For compact operators, the essential radius equals 0.

An operator $\mathbf{L}$ is quasi-compact if the strict inequality $R^{[e]}(\mathbf{L}) < R(\mathbf{L})$ holds. Then, except for the part of the spectrum inside the closed disk of radius $R^{[e]}(\mathbf{L})$, the operator behaves just like a compact operator (in the sense that its spectrum consists of isolated eigenvalues of finite multiplicity).

The following theorem, due to Hennion [15] is a generalisation of previous theorems due to Ionescu-Tulcea and Marinescu, or Lasota-Yorke. It provides an upper bound for the essential spectral radius. It deals with two norms, a weak norm $|.|_{\mathcal{F}}$ and a strong norm $||.||_{\mathcal{F}}$, for which the unit ball of $(\mathcal{F},||.||)$ is compact in $(\mathcal{F},|.|)$.

Theorem C. [Hennion, Ionescu-Tulcea and Marinescu, Lasota-Yorke]. *Suppose that the Banach space $\mathcal{F}$ is endowed with two norms $|.|$ and $||.||$, and the unit ball of $(\mathcal{F},||.||)$ is compact in $(\mathcal{F},|.|)$. Let $\mathbf{L}$ be a bounded operator on $(\mathcal{F},||.||)$. Assume that there exist two sequences $\{r_n\}$ and $\{t_n\}$ of positive numbers such that, for all $n \geq 1$, one has*

$$||\mathbf{L}^n[f]|| \leq r_n \cdot ||f|| + t_n \cdot |f|. \tag{37}$$

Then, the essential spectral radius of the operator $\mathbf{L}$ on $(\mathcal{F},||.||)$ satisfies $R^{[e]}(\mathbf{L}) \leq \lim_{n\to\infty} \inf (r_n)^{1/n}$.

We use this Theorem C for an alternative proof of Theorem D, with the space $\mathbb{H}_\alpha(J)$ of α Hölder functions; the strong norm is the α-Hölder norm $|.|_\alpha$, and the weak norm is the L^1 norm. We also use this Theorem in Proposition 6 (iii) with the space $\mathcal{C}^0(J)$ of continuous functions; the strong norm is the sup norm $||.||_0$, and the weak norm is the L^1 norm.

We shall often use the following Lemma which makes precise the relations between the spectrum and the essential spectrum of an operator acting on two spaces $\mathcal{F}_1 \subset \mathcal{F}_2$.

Lemma 1. *Let* $\mathbf{L}$ *be a linear operator acting on two Banach spaces* $\mathcal{F}_1$ *and* $\mathcal{F}_2$*, and denote by* σ_i*,* $\sigma_i^{[e]}$ *the spectrum, and the essential spectrum of* $\mathbf{L}$ *as an operator on* $\mathcal{F}_i$*,* $i = 1,2$*.*
(a) *Suppose that* $\mathcal{F}_1, \mathcal{F}_2$ *satisfy the following three properties:* (i) $\mathcal{F}_1 \subset \mathcal{F}_2$*, and* $\mathcal{F}_1$ *is dense in* $\mathcal{F}_2$ *–* (ii) *The injection* $\mathcal{F}_1 \to \mathcal{F}_2$ *is continuous –* (iii) *the unit ball of* $\mathcal{F}_1$ *is* $\mathcal{F}_2$*–compact in* $\mathcal{F}_2$*. Then, the inclusion* $\sigma_1 \subset \sigma_2$ *holds.*
(b) *If, in addition,* $\mathcal{F}_1, \mathcal{F}_2$ *satisfy* (iv) *the unit ball of* $\mathcal{F}_1$ *is* $\mathcal{F}_2$*–compact in* $\mathcal{F}_1$*, then the inclusion* $\sigma_1^{[e]} \subset \sigma_2^{[e]}$ *holds.*

Proof. We denote by $\mathbf{G}$ the operator $\mathbf{G} := \mathbf{L} - \lambda I$. In this proof, we use twice the following sublemma.

Sublemma. *Let the spaces* $\mathcal{F}_1$ *and* $\mathcal{F}_2$ *satisfy hypothesis* (ii) *of the Lemma. Let* $\mathbf{G}$ *be a linear operator acting on both spaces. Assume that there are* $g \notin \mathbf{G}[\mathcal{F}_1]$ *and a sequence* (f_n) *of functions of* $\mathcal{F}_2$ *for which the* $\mathcal{F}_2$*–limit of the sequence* $\mathbf{G}[f_n]$ *is* g*. Then, there exists a sequence* (ψ_n) *in* $\mathcal{F}_1$ *with* $\|\psi_n\|_1 = 1$ *such that* $\|\mathbf{G}[\psi_n]\|_2$ *goes to* 0*.*

Proof of the sublemma. Because g is not in $\mathbf{G}[\mathcal{F}_1]$, the sequence (f_n) has no limit points for the $\mathcal{F}_1$-topology : since the convergence in $\mathcal{F}_1$ implies the convergence in $\mathcal{F}_2$, any $\mathcal{F}_1$–limit point h would satisfy $\mathbf{G}[h] = g$. In particular, (f_n) is not a Cauchy sequence. Thus, there exists $\varepsilon > 0$ and a subsequence n_k such that for all $k \in \mathbb{N}$, one has $\|f_{n_k} - f_{n_{k+1}}\|_1 > \varepsilon$. Define $\phi_k := f_{n_k} - f_{n_{k+1}}$ and $\psi_k = \frac{\phi_k}{\|\phi_k\|_1}$. Now, $\|\psi_k\|_1 = 1$ and the inequality $\|\phi_k\|_1 > \varepsilon$ proves that the sequence $\mathbf{G}[\psi_k]$ goes to 0 in $\mathcal{F}_2$. ∎

We now return to the proof of Lemma 1.

(a) *Inclusion* $\sigma_1 \subset \sigma_2$. If λ is an eigenvalue of $\mathbf{L}$ as an operator on $\mathcal{F}_1$, then it is also an eigenvalue of $\mathbf{L}$ as an operator on $\mathcal{F}_2$.
Let λ be an element of σ_1 of type 2, which is not an element of σ_2. Then $\mathbf{G}$ is not surjective on $\mathcal{F}_1$ but is surjective on $\mathcal{F}_2$: there exists $g \in \mathcal{F}_1$ which is not in $\mathbf{G}[\mathcal{F}_1]$. But g belongs to $\mathbf{G}[\mathcal{F}_2]$ and there is $f \in \mathcal{F}_2$ such that $g = \mathbf{G}[f]$. Since $\mathcal{F}_1$ is dense in $\mathcal{F}_2$, there is a sequence f_n of functions of $\mathcal{F}_1$ which converges to f in $\mathcal{F}_2$. Then the sequence $\mathbf{G}[f_n]$ converges to $\mathbf{G}[f] = g$ in $\mathcal{F}_2$. Now, using the sublemma and hypothesis (iii) shows that the sequence ψ_k has a non zero limit point ψ (for the $\mathcal{F}_2$ topology) which belongs to $\mathcal{F}_2$ and satisfies $\mathbf{G}[\psi] = 0$. This means that λ is an eigenvalue of $\mathbf{L}$ in $\mathcal{F}_2$, which provides a contradiction. So, we have proven that any element of σ_1 belongs to σ_2.

(b) *Inclusion* $\sigma_1^{[e]} \subset \sigma_2^{[e]}$. If λ is an essential spectral value of type (A) or (B) of $\mathbf{L}$ as an operator on $\mathcal{F}_1$, then it is also an essential spectral value of type (A) or (B) of $\mathbf{L}$ as an operator on $\mathcal{F}_2$.
Suppose now that λ is an essential spectral value of $\mathbf{L}$ as an operator on $\mathcal{F}_1$ of type (C). Then, the set $\mathbf{G}[\mathcal{F}_1]$ is not $\mathcal{F}_1$–closed and there exists $g \notin \mathbf{G}[\mathcal{F}_1]$ which is the $\mathcal{F}_1$–limit of a sequence $\mathbf{G}[f_n]$, with $f_n \in \mathcal{F}_1$. Then g is also the $\mathcal{F}_2$–limit of the sequence $\mathbf{G}[f_n]$. Now, using the sublemma and hypothesis (iv) shows that there exists a non zero limit point ψ of the sequence ψ_k (for the $\mathcal{F}_2$ topology) which belongs to $\mathcal{F}_1$ and satisfies $\mathbf{G}[\psi] = 0$. This means that λ is an eigenvalue of $\mathbf{L}$ in $\mathcal{F}_1$. Since λ is an element of $\sigma_1^{[e]}$, we know that it is either of type (A) or of type (B). Then, it is also an essential spectral value of type (A) or (B) of $\mathbf{L}$ as an operator on $\mathcal{F}_2$. So, we have proven that any element of $\sigma_1^{[e]}$ belongs to $\sigma_2^{[e]}$ ∎

In the sequel, we consider the four spaces $\mathcal{C}^1(J) \subset \mathbb{H}_\alpha(J) \subset \mathcal{C}^0(J) \subset L^1(J)$. We apply Lemma 1 (a) to the following pairs: $\mathcal{C}^1(J)$ and $\mathbb{H}_\alpha(J)$ [in Prop. 6 (ii)], $\mathcal{C}^0(J)$ and $L^1(J)$ [in Prop. 8 (i)]. We apply Lemma 1 (b) to the pair $\mathcal{C}^1(J)$ and $\mathcal{C}^0(J)$ [Prop. 6 (iii)].

5.3 Classical results for random matrices.

We shall deal with the general framework of random matrices and use many results from [3]: we consider a denumerable set $\mathcal{S}$ of random matrices 2×2 with determinant 1, and, we associate to each element S of $\mathcal{S}$ its LFT h, and also the map $\ell : J \to J$ conjugated to h with the tangent map [i.e., $\ell := \arctan \circ h \circ \tan$]. We denote by $\overline{\mathcal{S}}$ the semi–group generated by $\mathcal{S}$. Let

$$L^+(S) := \sup\{\log^+ ||S||, \log^+ ||S^{-1}||\} \qquad \text{with} \quad \log^+ x := \sup(0, \log x).$$

We now define some important properties for such a set $\mathcal{S}$.

$(P1)$ [Contraction] *There exists a sequence (S_n) of $\overline{\mathcal{S}}$ for which $||S_n||^{-1} \cdot S_n$ converges to a rank one matrix.*

$(P2)$ [Strong Irreducibility] *There does not exist a finite union W of lines $V_1, V_2, \ldots V_k$ which is invariant by all S in $\mathcal{S}$.*

$(P3)$ $\mathbb{E}[\exp(wL^+(S))] < \infty$ *for w positive real small enough.*

We shall apply in the sequel three main theorems, due to Furstenberg [12], Guivarc'h and Raugi [14] and Le Page [18], and well–summarized in the book of Bougerol [see [3] pages 66, 67, 105, 119], which we gather into the next theorem, where we use our notations. The original proof of Bougerol does not use Theorem C, but it is possible to use Theorem C to get a shorter proof of Theorem D.

Theorem D. [Product of random matrices.] [Furstenberg, Guivarc'h and Raugi, Le Page] *Suppose that a set $\mathcal{S}$ of random matrices fulfills $(P1, P2, P3)$. Then,*
(i) the Lyapunov exponent of $\mathcal{S}$ defined as

$$\gamma := \frac{1}{n} \lim_n \mathbb{E}[\log ||S_1 S_2 \ldots S_n||]$$

is strictly positive.
(ii) Denote by $\mathbb{H}_\alpha(J)$ the space of α-H¨older functions on J. For sufficiently small α, z, the transfer operator $\mathbf{G}_{1,z} : \mathbb{H}_\alpha(J) \to \mathbb{H}_\alpha(J)$ is quasi-compact, and admits a unique dominant eigenvalue $\lambda(1,z)$; the Lyapounov exponent γ of set $\mathcal{S}$ satisfies $2\gamma = -\lambda'_z(1,0)$.

5.4 The LSB matrices.

We now show that we can apply Theorem D to the LSB framework. We also prove three supplementary properties $(P4, P5, P6)$ which will be useful in the sequel, and make precise properties $(P1, P3)$.

Proposition 5. *Consider the set $\mathcal{N}, \mathcal{L}$ associated to the LSB Algorithm. The set of matrices $\mathcal{N}$ fulfills hypotheses $(P1, P2, P3)$. Moreover, the set of functions $\mathcal{L}$ satisfies the following:*
$(P4)$ [Fixed point] *There exists $\ell \in \mathcal{L}$ and $x \in J$ such that $\ell(x) = x$.*
$(P5)$ [Bounds on derivatives] *For any $\ell \in \mathcal{L}$, and any $x \in J$, one has $\phi^{-2} \le |\ell'(x)| \le \phi^2$.*
$(P6)$ [Bounded Distortion] *For any $x \in J$ and any $\ell \in \mathcal{L}$, one has $|\ell''(x)| \le \sqrt{5}\,|\ell'(x)|$.*

Remark. It is clear, with (35), that the sets $\mathcal{N}^{-1}, \mathcal{L}^{-1}$ also satisfy all these properties. It is also clear that the set $\mathcal{M}$ fulfills $(P1, P2, P3)$.

Proof. Any matrix $N_{[q]}$ in $\mathcal{N}$ is symmetric, with determinant equal to -1. It has two distinct eigenvalues, λ_q^+ (the dominant one) and λ_q^-, with

$$|\lambda_q^+| = \frac{1}{2}(|q| + \sqrt{q^2+4}) = |\lambda_q^-|^{-1}.$$

Then, the Euclidean norm of matrix $N_{[q]}$ is equal to $|\lambda_q^+|$. Since any q of $\mathcal{Q}$ satisfies $|q| < 1$, one has

$$||N_{[q]}|| \le \phi, \qquad ||N_{[q]}^{-1}|| \le \phi, \qquad L^+(N_{[q]}) \le \log \phi.$$

This proves $(P3)$. Then Relation (26) entails $(P5)$. Now, choose as S_n the n-th power of any matrix $N_{[q]}$, whose eigenvalues have moduli $|\lambda_q^+|^n, |\lambda_q^-|^n$. Then Lemma III.1.4 of Bougerol [page 45] entails $(P1)$. Finally, the existence of eigenvectors for N entails the existence of fixed points for h, and thus for ℓ: This proves $(P4)$.

Proof of $(P2)$. Suppose that such a W exists. Then, for any $S \in \mathcal{S}$, there exists a permutation σ_S of $[1..k]$ for which $S(V_i) = V_{\sigma_S(i)}$, so that each V_i is invariant by all the matrices $N^{k!}$ relative to $N \in \mathcal{N}$. This implies that $k = 2$, and that $\{V_1, V_2\}$ is a common eigenbase for all the matrices N^2. This would entail that any pair of matrices N_1^2, N_2^2 commute, which is not true.

Proof of $(P6)$. Fix $q \in \mathcal{Q}$. The quantity $\gamma_q(x) := \ell_q''(x)/\ell_q'(x)$ relative to the distortion of $\ell_{[q]}$ is

$$\gamma_q(x) = \frac{2q(\tan^2 x + q \tan x - 1)}{1 + (q + \tan x)^2},$$

and the extremal values of γ_q are equal to $\pm q\sqrt{q^2+4}$. Since any q of $\mathcal{Q}$ satisfies $-1 < q < 1$, one deduces $|\gamma_q(x)| \le \sqrt{5}, \quad \forall q \in \mathcal{Q}$ and $x \in J$. ■

Then, Proposition 5 entails that Theorem D can be applied to sets $\mathcal{N}, \mathcal{N}^{-1}, \mathcal{M}$, so that the operators $\mathbf{G}_{1,z}$, $\widehat{\mathbf{G}}_{1,z}, \mathbf{G}_{1-z,-z}$ are quasi-compact on the set $\mathbb{H}_\alpha(J)$ when α and z are small. However, it is not sufficient for our purpose, since we need quasi–compacity for $\mathbf{G}_{t,z}$ for z near to 1.

5.5 Action of the transfer operator on $\mathcal{C}^0(J)$ and $\mathcal{C}^1(J)$.

We mainly work in both spaces $\mathcal{C}^1(J)$ and $\mathcal{C}^0(J)$, endowed with the norms

$$||f||_0 := \sup_{x \in J} |f(x)| \qquad ||f||_1 = ||f||_0 + ||f'||_0,$$

and we shall often use Lemma 1 with intermediary spaces $\mathbb{H}_\alpha(J)$ and $L^1(J)$.

Proposition 6. *The following holds:*

(i) *Denote by* $\mathcal{A} := \{(t,z) \in \mathbb{C}^2; \Re t > 1/2\}$. *When* $(t,z) \in \mathcal{A}$, *the operators* $\mathbf{G}_{t,z}$, $\widehat{\mathbf{G}}_{t,z}$ *and* $\mathbf{G}_{z,z}^{(c)}$ *act on* $\mathcal{C}^1(J)$ *and* $\mathcal{C}^0(J)$ *; Moreover, the maps* $(t,z) \mapsto \mathbf{G}_{t,z}$, $(t,z) \mapsto \widehat{\mathbf{G}}_{t,z}$ *are analytic.*

(ii) *The operators* $\mathbf{G}_{1,0}$ *and* $\widehat{\mathbf{G}}_{1,0}$ *are quasi-compact on the space* $\mathcal{C}^1(J)$. *More precisely, the decomposition holds :*

$$\mathbf{G}_{1,0}^n[f] = \int f d\nu + \mathbf{R}_{1,0}^n[f],$$

where ν *is a probability measure on* J, *invariant by the dual operator* $\mathbf{G}_{1,0}^*$ *and* $\mathbf{R}_{1,0}$ *is a continuous operator on* $\mathcal{C}^1(J)$ *whose spectral radius is strictly less than* 1. *The same decomposition holds for* $\widehat{\mathbf{G}}_{1,0}$ *on* $\mathcal{C}^1(J)$ *(with* $\widehat{\nu}$ *and* $\widehat{\mathbf{R}}_{1,0}$*).*

(iii) *The essentiel spectral radius of the operator* $\mathbf{G}_{1,1}$ *when it acts on the space* $\mathcal{C}^1(J)$ *or* $\mathcal{C}^0(J)$ *is strictly less than 1.*

(iv) *On each of the two spaces* $\mathcal{C}^1(J)$*or* $\mathcal{C}^0(J)$*, the following decomposition holds :*

$$\mathbf{G}_1^n[f] = \varphi \int f \, dt + \mathbf{R}_{1,1}^n[f].$$

Here, $\varphi \in \mathcal{C}^1(J)$ *is a density of probability and* $\mathbf{R}_{1,1}$ *is a continuous operator on* $\mathcal{C}^1(J)$ *[and* $\mathcal{C}^0(J)$*] whose spectral radius is strictly less than* 1.

(v) *There exists complex neighborhoods* $\mathcal{D}_0$ *of* $(1,0)$ *and* $\mathcal{D}_1$ *of* $(1,1)$ *for which the following is true: for* $(t,z) \in \mathcal{D}_0 \cup \mathcal{D}_1$ *the operators* $\mathbf{G}_{t,z}, \widehat{\mathbf{G}}_{t,z}$*, when acting on* $\mathcal{C}^1(J)$*, admit a unique dominant eigenvalue denoted by* $\lambda(t,z)$*,* $\widehat{\lambda}(t,z)$ *separated from the remainder of the spectrum by a spectral gap. For* $(t,z) \in \mathcal{D}_1$*, the operators* $\mathbf{G}_{t,z}, \widehat{\mathbf{G}}_{t,z}$ *[when acting on* $\mathcal{C}^0(J)$*] admit a unique dominant eigenvalue denoted by* $\lambda(t,z)$*,* $\widehat{\lambda}(t,z)$ *separated from the remainder of the spectrum by a spectral gap.*

Proof.
(i) Consider $(t,z) \in \mathcal{A}$, and let $\sigma := \Re z, \tau := \Re t$. Remark first that, if $(t,z) \in \mathcal{A}$, the series of weighted probabilities δ_ℓ is convergent when $(t,z) \in \mathcal{A}$, and satisfies

$$S(\tau) := \sum_{\ell \in \mathcal{L}} \delta_\ell^\tau = \sum_{k \geq 1} [2^{1-2\tau}]^k = \frac{2^{1-2\tau}}{1 - 2^{1-2\tau}}.$$

Each component term $\mathbf{G}_{t,z,(\ell)}$ of $\mathbf{G}_{t,z}$ defined as $\mathbf{G}_{t,z,(\ell)}[f] := |\ell'|^z \cdot f \circ \ell$ satisfies, with $(P5)$,

$$||\mathbf{G}_{t,z,(\ell)}[f]||_0 \leq \phi^{2|\sigma|} \cdot ||f||_0,$$

$$\left(\mathbf{G}_{t,z,(\ell)}[f]\right)'(x) = z \cdot \ell''(x) \cdot \ell'(x)^{z-1} \cdot f \circ \ell(x) + \ell'(x)^{z+1} \cdot f' \circ \ell(x),$$

so that

$$||\left(\mathbf{G}_{t,z,\ell}[f]\right)'||_0 \leq \sqrt{5} \cdot \phi^{2|\sigma|} \cdot [z| \cdot \|f\|_0 + \phi^{2|\sigma+1|} \|f'\|_0,$$

and finally

$$||\mathbf{G}_{t,z}||_0 \leq \phi^{2|\sigma|} \cdot S(\tau), \qquad ||\mathbf{G}_{t,z}||_1 \leq |z| \cdot \phi^{2|\sigma|+2} \cdot S(\tau). \tag{38}$$

This proves that the sum defining $\mathbf{G}_{t,z}$ converges normally on all compact subset of $\mathcal{A}$ both in $\mathcal{C}^0(J)$ and in $\mathcal{C}^1(J)$. Then, $\mathbf{G}_{t,z}$ is a bounded operator on $\mathcal{C}^0(J)$ and on $\mathcal{C}^1(J)$, and the maps $(t,z) \mapsto \mathbf{G}_{t,z}$ are analytic. The proofs for operators $\widehat{\mathbf{G}}_{t,z}$ are of the same spirit.

(ii) Theorem C (ii) entails that the decompositions hold in $\mathbb{H}_\alpha(J)$. To see that they hold on $\mathcal{C}^1(J)$, we first recall that the operators $\mathbf{G}_{1,0}$ and $\widehat{\mathbf{G}}_{1,0}$ act on $\mathcal{C}^1(J)$. Then, from relations

$$\mathbf{R}_{1,0}[f] = \mathbf{G}_{1,0}[f] - \int f d\nu, \qquad \widehat{\mathbf{R}}_{1,0}[f] = \widehat{\mathbf{G}}_{1,0}[f] - \int f d\widehat{\nu}$$

the operators $\mathbf{R}_{1,0}$ and $\widehat{\mathbf{R}}_{1,0}$ act also on $\mathcal{C}^1(J)$. Now, Lemma 1 proves that $\mathbf{R}_{1,0}$, when it acts on $\mathcal{C}^1(J)$, has a spectral radius strictly less than 1.

(iii) We study now the operator $\mathbf{G}_1 := \mathbf{G}_{1,1}$ on $\mathcal{C}^0(J)$ and prove that it fulfills the hypotheses of Theorem D: we choose as the strong norm the norm $||.||_0$ and as the weak norm the norm $||.||_{L^1}$.

First, the unit ball $\mathcal{B} = \{g \in \mathcal{C}^0(J); \quad ||g||_0 \le 1\}$ is compact in $L^1(J)$: Since functions of $\mathcal{B}$ are uniformly bounded, they are L^1-bounded and uniformly equi-integrable.

Second, consider a function f in $\mathcal{C}^0(J)$, denote by $I(f) := \int_J f(u)du$, and decompose $f = g + I(f)$ with $g := f - I(f)$. Then, g satisfies $I(g) = 0$, and any primitive F of g is a $\mathcal{C}^1(J)$ function on J [i.e., it satisfies $F(\frac{\pi}{2}) = F(-\frac{\pi}{2})$]. We fix a point a in J and we consider the operator $\mathbf{F}_n$ defined as

$$\mathbf{F}_n[g](x) := \int_a^x \mathbf{G}_1^n[g](u)du = \sum_{\ell \in \mathcal{L}^n} \delta_\ell \int_a^x |\ell'(u)| g \circ \ell(u) du = \sum_{\ell \in \mathcal{L}^n} \delta_\ell \int_{\ell(a)}^{\ell(x)} g(u)du$$

$$= \sum_{\ell \in \mathcal{L}^n} \delta_\ell [F \circ \ell(x) - F \circ \ell(a)] = \mathbf{G}_{1,0}^n[F](x) - \mathbf{G}_{1,0}^n[F](a) = \mathbf{R}_{1,0}^n[F](x) - \mathbf{R}_{1,0}^n[F](a).$$

Now, since $\mathbf{R}_{1,0} : \mathcal{C}^1(J) \to \mathcal{C}^1(J)$ has a spectral radius $\rho < 1$, we have, for any $\rho < \kappa < 1$, and some constant K_1,

$$||\mathbf{F}_n[g]||_1 \le 2||\mathbf{R}_{1,0}^n[F]||_1 \le K_1 \cdot \kappa^n ||F||_1.$$

Since F is a primitive of g, we have $||F||_1 \le (\pi + 1)||g||_0$. Since $\mathbf{F}_n[g]$ is a primitive of $\mathbf{G}_1^n[g]$, one has $||\mathbf{F}_n[g]||_1 \ge ||\mathbf{G}_1^n[g]||_0$, and finally

$$||\mathbf{G}_1^n[g]||_0 \le K_2 \cdot \kappa^n ||g||_0. \tag{39}$$

Now, we return to function f, with $||g||_0 \le (\pi+1)||f||_0$ and $|I(f)| \le ||f||_{L^1}$. Then, for some constant K_3,

$$||\mathbf{G}_1^n[f]||_0 \le ||\mathbf{G}_1^n[g]||_0 + |I(f)| \cdot ||\mathbf{G}_1^n[\mathbf{1}]||_0 \le K_3 \,[\kappa^n ||f||_0 + t_n \cdot ||f||_{L^1}] \tag{40}$$

with $t_n = ||\mathbf{G}_1^n[\mathbf{1}]||_0$. This relation shows that the operator $\mathbf{G}_1$, when it acts on $\mathcal{C}^0(J)$, fulfills the hypotheses of Theorem C, and its essential spectral radius is strictly less than 1. Now, Lemma 1 (b) proves that the same holds in $\mathcal{C}^1(J)$.

(iv) The relation $\int \mathbf{G}_1^n[f](u)du = \int f(u)du$ proves that the spectral radius equals 1. Together with the fact that the essential spectral radius is strictly less than 1, this shows the existence of an eigenvalue of modulus 1.

Let λ be an eigenvalue of modulus 1 with an eigenfunction f. Then, using the relation $\int \mathbf{G}_1[|f|](u)du = \int |f(u)|du$ together with the triangular inequality, we deduce that $\mathbf{G}_1[|f|] = |f|$. Then, f equals $\alpha\varphi$ with α of modulus 1, and φ an eigenfunction relative to $\lambda = 1$. Now, the relation $\mathbf{G}_1[f] = \lambda f$ entails that, for any $\ell \in \mathcal{L}$, and any $x \in J$, the equality $\alpha \circ \ell(x) \cdot \varphi \circ \ell(x) = \lambda\alpha(x) \cdot \varphi(x)$. Now, with $(P4)$, we use as x a fixed point for some function ℓ, and we conclude that $\lambda = 1$.

Let us prove that 1 is simple as an eigenvalue of $\mathbf{G}_1$ on $\mathcal{C}^1(J)$. Let φ and ψ be two eigenfunctions associated to 1 with $I(\varphi) = I(\psi) = 1$. Then $I(\varphi - \psi) = 0$. Applying (39) to the function $\varphi - \psi$:

$$||\varphi - \psi||_0 = ||\mathbf{G}_1^n[\varphi - \psi]||_0 \le K_2 \cdot \kappa^n ||\varphi - \psi||_0 \tag{41}$$

provides the equality $\varphi = \psi$, so that 1 is a simple eigenvalue.

(v) Follows from perturbation theory, see e.g. Dunford-Schwartz VII.6 ([10]). ■

5.6 Duality between $\widehat{\mathbf{G}}_{t,1-z}$ and $\mathbf{G}_{t,z}$.

For z near 0 and t near 1, we now make precise the relations between the dominant eigenvalue $\lambda(t,z)$ of $\mathbf{G}_{t,z}$ on $\mathcal{C}^1(J)$ and the dominant eigenvalue $\lambda(t,1-z)$ of $\mathbf{G}_{t,1-z}$ on $\mathcal{C}^0(J)$ or on $\mathcal{C}^0(J)$. [see also [3]]

Proposition 7. *One has:*

(i) For $(t,z)\in\mathcal{D}_0\cup\mathcal{D}_1$, $\lambda(t,z)=\widehat{\lambda}(t,z)$.

(ii) For a real pair $(t,z)\in\mathcal{D}_0$, the following relation between $\widehat{\mathbf{G}}_{t,z}$ and $\mathbf{G}_{t,1-z}$ holds : for all $f\in\mathcal{C}^1(J)$, $g\in\mathcal{C}^0(J)$, for all $n\in\mathbb{N}$,

$$\int \widehat{\mathbf{G}}^n_{t,z}[f]\cdot g dx = \int \mathbf{G}^n_{t,1-z}[g]\cdot f dx. \tag{42}$$

and entails the equality : $\lambda(t,1-z)=\widehat{\lambda}(t,z)$.

Proof. (i) Using the involution Tilde defined in (34), we denote by $\widetilde{f}$ the mapping $J\to J$ which is defined from $f:J\to J$ by $\widetilde{f}(y)=f(\widetilde{y})$. Then, with (35),

$$\widehat{\mathbf{G}}_{t,z}[f](\widetilde{y}) = \sum_{\ell\in\mathcal{L}} \delta^t_\ell\cdot|(\ell^{-1}(\widetilde{y}))'|^z\cdot f\circ\ell^{-1}(\widetilde{y}) = \sum_{\ell\in\mathcal{L}} \delta^t_\ell\cdot|\ell'(y)|^z\cdot f(\widetilde{\ell(y)})$$

$$= \sum_{\ell\in\mathcal{L}} \delta^t_\ell\cdot|\ell'(y)|^z\cdot \widetilde{f}\circ\ell(y) = \mathbf{G}_{t,z}[\widetilde{f}](y).$$

This proves, for (t,z) near $(1,0)$ or $(1,1)$, the equality between the dominant eigenvalue $\lambda(t,z)$ of $\mathbf{G}_{t,z}$ and the dominant eigenvalue $\widehat{\lambda}(t,z)$ of $\widehat{\mathbf{G}}_{t,z}$.
(ii) Consider $f\in\mathcal{C}^1(J)$, $g\in\mathcal{C}^0(J)$, and $n\in\mathbb{N}$. The following relation holds

$$\int_J \mathbf{G}^n_{t,z}[f](u)\cdot g(u)du = \sum_{\ell\in\mathcal{L}^n}\delta^t_\ell\int_J|\ell'(u)|^z f(\ell(u))g(u)du = \sum_{\ell\in\mathcal{L}^n}\delta^t_\ell\int_J|\ell'(\ell^{-1}(v))|^{z-1}\cdot g\circ\ell^{-1}(v)\cdot f(v)dv$$

$$= \sum_{\ell\in\mathcal{L}^n}\delta^t_\ell\int_J|(\ell^{-1})'(v))|^{1-z}\cdot g\circ\ell^{-1}(v)\cdot f(v)dv = \int_J \widehat{\mathbf{G}}^n_{t,1-z}[g](v)\cdot f(v)dv.$$

Now, for (t,z) near (1, 0), the quasi-compacity of operators $\mathbf{G}_{t,z}$ on $\mathcal{C}^1(J)$ and $\mathbf{G}_{t,1-z}$ [on $\mathcal{C}^0(J)$ or on $\mathcal{C}^1(J)$] entails the relation

$$\lambda(t,z)^n = \widehat{\lambda}(t,1-z)^n\cdot[1+O(\kappa^n)],$$

which proves (ii).

Finally, we have proven that $\lambda(t,z)=\lambda(t,1-z)$, [for (t,z) near (1, 0)]. This entails, with Theorem D(ii) the equality $2\gamma=-\lambda'_z(1,0)=\lambda'_z(1,1)$. ■

5.7 Aperiodicity and strict convexity.

Finally, we have to check supplementary spectral properties.

Proposition 8. *(1) For the operator $\mathbf{G}_s$ when acting on $\mathcal{C}^1(J)$ or $\mathcal{C}^0(J)$, the following holds*

(i) For any s with $\Re s>1$, the spectral radius $R(s)$ of $\mathbf{G}_s$ is stricly less than 1.

(ii) On the line $\Re s=1, s\neq 1$, the spectral radius $R(s)$ of $\mathbf{G}_s$ is stricly less than 1.

(2) *The dominant eigenvalue* $l(s) := \lambda(1-s,-s)$ *of the operator* $\mathbf{G}_{1-s,-s}$ *on* $\mathcal{C}^1(J)$ *has its second derivative* $l''(0)$ *which is non zero.*

Proof. $(1)(i)$ We have, for $\sigma := \Re s \geq 1$,

$$||\mathbf{G}_s[f]||_{L^1} = \int_J |\mathbf{G}_s[f](y)|\,dy \leq \sum_{\ell\in\mathcal{L}} \delta_\ell^\sigma \int_J |\ell'(y)|^\sigma |f(\ell(y))|dy \leq \sum_{\ell\in\mathcal{L}} \delta_\ell^\sigma \int_J |\ell'(\ell^{-1}(x))|^{\sigma-1}|f(x)|dx$$

$$\leq \phi^{2(\sigma-1)} \sum_{\ell\in\mathcal{L}} \delta_\ell^\sigma \cdot ||f||_{L^1} = \phi^{2(\sigma-1)} \frac{2^{1-2\sigma}}{1-2^{1-2\sigma}} ||f||_{L^1} \leq \left(\frac{\phi}{2}\right)^{2(\sigma-1)} \cdot ||f||_{L^1}.$$

Then, the spectral radius of $\mathbf{G}_s$ on L^1 is at most $(\phi/2)^{2(\sigma-1)}$, which is strictly less than 1 for $\Re s > 1$. With Lemma 1, the same holds for $\mathbf{G}_s$ acting on $\mathcal{C}^0(J)$ or on $\mathcal{C}^1(J)$.

$(1)(ii)$ The previous argument implies that, for $s = 1+it$, the spectral radius of $\mathbf{G}_s$ on $\mathcal{C}^0(J)$ is at most 1. There are now two main steps in the proof. We first prove in (a) that the essential spectral radius of $\mathbf{G}_s$ on $\mathcal{C}^0(J)$ is strictly less than 1. Then, we prove in (b) that there is no eigenvalue of modulus 1.

(a) The inequality $||\mathbf{G}^n_{1+it}[f]||_0 \leq ||\mathbf{G}^n_1[|f|]||_0$, the relation (40) applied to the function $f_1 := |f|$ and Theorem D prove that the essential spectral radius of $\mathbf{G}_{1+it}$ [when acting on $\mathcal{C}^0(J)$] is strictly less than 1.

(b) Suppose now that, for $s = 1+it, t \neq 0$, the spectral radius of $\mathbf{G}_s$ is equal to 1. Since the essential spectral radius is strictly less than 1, $\mathbf{G}_s$ has an eigenvalue of modulus one. Following the proof of Proposition 9 in [24] entails the existence of a function μ with $|\mu| = 1$ such that for all $n \in \mathbb{N}$, for all $\ell \in \mathcal{L}^n$,

$$\delta_\ell^{it} \cdot |\ell'|^{it} \cdot \mu \circ \ell = \mu. \tag{43}$$

Then, there is a bounded function ξ, such that, for any $\ell \in \mathcal{L}^n$, there exists an integer $J(\ell)$ for which,

$$\log \delta_\ell + \log |\ell'| = \xi - \xi \circ \ell + \frac{2\pi}{t} J(\ell).$$

This entails that J is additive, i.e., $J(\ell_1 \circ \ell_2) = J(\ell_1) + J(\ell_2)$, and $\mathbb{E}_n[J] = n\mathbb{E}[J]$. Denote by Γ the Lyapounov exponent of set $\mathcal{M}$, that equals $\Gamma = 2\log 2 + \gamma$. Then Theorem C (ii), and (26) imply that

$$\frac{2\pi}{t}\mathbb{E}[J] = -2\Gamma, \qquad \mathbb{E}[(\log ||M_1 \cdot M_2 \cdot \ldots \cdot M_n|| - n\Gamma)^2] < K,$$

for some constant K. This contradicts Lemma 5.3 p.123 in [3] and ends the proof of Assertion (ii) on $\mathcal{C}^0(J)$. With Lemma 1 (a), the same is true on $\mathcal{C}^1(J)$.

(2) The quantity $l(s) = \lambda(1-s,-s)$ is the dominant eigenvalue of the operator $\mathbf{G}_{1-s,-s}$ which is exactly the Bougerol transfer operator related to set $\mathcal{M}$. Applying [3], Lemmas 5.2 and 5.3 p. 122 proves that $l''(0) > \Gamma^2$.■

6 Open problems and Conclusion.

The non-centered LSB Algorithm. This analysis can also be applied to the non-centered LSB algorithm. In its actual version, this algorithm does not always terminate, notably on inputs (u,v) of the form $v =$

$-2^k u$. It is quite easy to add a supplementary stopping condition in order to avoid this problem. Then, the analysis of this version of the non–centered LSB algorithm deals with a new set $\overline{\mathcal{N}}$ of matrices, of the form

$$\overline{\mathcal{N}} := \{\overline{N}_{[q]} = \begin{pmatrix} 0 & 1 \\ 1 & q \end{pmatrix}; q = \frac{a}{2^k}; k \geq 1, a \text{ odd}, 0 < a < 2^{k+1}\}. \tag{44}$$

The numerical value of the binary Lyapounov exponent $\overline{\gamma}_0$ relative to set $\overline{\mathcal{N}}$ is $\overline{\gamma}_0 \sim 0.651$ [11] and is more than 13 times bigger than γ_0. Then, even if it is modified in order to always terminate, the non-centered LSB algorithm is certainly slower than the centered version which is studied in this paper.

Continuants behaviour. It would be interesting to study the length of the k-th convergent of a rational number, when k is a given fraction of the total number P of iterations of the LSB algorithm, of the form $k = \lfloor \delta P \rfloor$, for a fixed $\delta \in [0, 1]$. This study should explain the apparent contradiction between our two main results.

Towards distribution results. Finally, our "dream" is to adapt methods of Baladi and Vall´ee [4] in order to prove Gaussian laws for the main parameters of the LSB algorithm. This is indeed why we chose to study the operators in the space $\mathcal{C}^1(J)$, where the arguments developped in [4], based on previous works of Dolgopyat [9] may [perhaps] apply.

Acknowledgements. We wish to thank Damien Stehl´e for introducing us to the LSB algorithm, and Philippe Flajolet for performing computations of the Lyapounov exponents.

References

[1] AESOP. The hare and the tortoise. `http://www.umass.edu/aesop/haretortoise/index.html`

[2] AKHAVI, A., VALLÉE, B. Average bit–complexity of Euclidean Algorithms, *Proceedings of ICALP'2000, Lecture Notes in Computer Science* 1853, pp 373-387, Springer.

[3] BOUGEROL, P. AND LACROIX, J. *Products of random matrices with applications to Schrödinger operators.* Progress in Probability and Statistics, 8. Birkhäuser Boston, Inc., Boston, MA, 1985.

[4] BALADI, V., AND VALLÉE, B. Euclidean Algorithms are Gaussian, to appear in *Journal of Number Theory*. Short version: BALADI, V., AND VALLÉE, B. Distributional analyses of Euclidean algorithms, *Proceedings of Alenex–ANALCO'04*, pp 170–184.

[5] BROWKIN, J. Continued fractions in local fields. II, Math. Comp. 70 (2001), no. 235, pp.1281-1292 .

[6] BROWKIN, J. Continued fractions in local fields. I, Demonstratio Math. 11 (1978), no. 1, pp.67-82.

[7] DAIREAUX, B. Analyse des algorithmes d'Euclide: une approche dynamique., PhD Thesis, University of Caen, June 05.

[8] DELANGE, H. G´en´eralisation du Th´eorème d'Ikehara, *Ann. Sc. ENS*, (1954) 71, pp 213–242.

[9] DOLGOPYAT, D. On decay of correlations in Anosov flows, *Ann. of Math.* 147 (1998) pp 357–390.

[10] DUNFORD, N. AND SCHWARTZ, J. *Linear Operators. Part I. General Theory.* Pure and Applied Mathematics, Vol. 7 Interscience Publishers, Inc., New York; Interscience Publishers, Ltd., London 1958

[11] FLAJOLET, P. Personal communication.

[12] FURSTENBERG, H. Non commuting random products, Trans. amer. Math. Soc (108) pp 377–428.

[13] GOUVEA, F.Q. *p-Adic Numbers: an Introduction*

[14] GUIVARC'H, Y, AND RAUGI, A. Frontières de Furstenberg, propri´et´es de contraction et th´eorèmes de convergence. Zeit. fur Wahrscheinlichkeitstheorie und Verw. Gebiete (69) pp 187–242.

[15] HENNION, H. AND HERVÉ, L. *Limit theorems for Markov chains and stochastic properties of dynamical systems by quasi-compactness.* Lecture Notes in Mathematics, 1766. Springer-Verlag, Berlin, 2001.

[16] HWANG H. K. On convergence rates in the central limit theorem for combinatorial structures *European Journal of Combinatorics*, 19, (1998), pp 329–343.

[17] KOBLITZ, N. *p-adic Numbers, p-adic Analysis, and Zeta-Functions* 2nd edition, Springer-Verlag, 19.

[18] LE PAGE, E. Th´eorèmes limites pour les produits de matrices al´eatoires, in *Probability measures on groups*, pp 258–303, ed. H. Meyer, Lectures Notes in Math. 928, Springer, New-York,

[19] NUSSBAUM,R. The radius of the essential spectrum. *Duke Math. J.* 37 1970 473–478.

[20] STEHLÉ, D. Web page: `http://www.loria.fr/~stehle/BINARY.html`

[21] STEHLÉ, D. AND ZIMMERMANN, P. A Binary Recursive Gcd Algorithm, Proceedings of ANTS'04, Lecture Notes in Computer Science.

[22] VALLÉE, B. Dynamics of the Binary Euclidean Algorithm: Functional Analysis and Operators., *Algorithmica* (1998) vol 22 (4) pp 660–685.

[23] VALLÉE, B. Euclidean dynamics Web page: `http://users.info.unicaen.fr/~brigitte/index.html/`

[24] VALLÉE, B. Dynamical sources in information theory: fundamental intervals and word prefixes *Algorithmica,* **29**, 262-306, (2001).

[25] VALLÉE, B. Digits and Continuants in Euclidean Algorithms. Ergodic Versus Tauberian Theorems, *Journal de Théorie des Nombres de Bordeaux* 12 (2000) pp 531-570.