Symbolic dynamics and representations

V. Berthé
IRIF-UMR 8243
Université Paris Diderot, Paris 7 - Case 7014
F-75205 Paris Cedex 13, France
berthe@irif.fr

Abstract

The object of study of symbolic dynamics are discrete dynamical systems made of infinite sequences of symbols, with the shift acting on them. They come as codings of trajectories of points in a dynamical system according to a given partition. They are used as discretization tools for analyzing such trajectories, but they also occur in a natural way in arithmetics for instance. We first will recall basic definitions concerning symbolic dynamics and illustrate them with transformations like beta-numeration and continued fractions. We then focus on orbits that are relevant in computer science, namely finite and periodic ones, together by alluding to numerical issues for the computation of orbits.

Contents

1 Introduction

The object of study of symbolic dynamics are discrete dynamical systems made of infinite sequences of symbols with values in a finite alphabet, with the shift map S acting on them: the shift S maps an infinite word $(u_n)_{n\geq 0}$ onto this infinite word from which the first letter has been taken away, that is, $S((u_n)_{n\in\mathbb{N}}) = (u_{n+1})_{n\in\mathbb{N}}$. Symbolic dynamical systems come in a natural way as codings of trajectories of points in a dynamical system according to a finite partition. They are used as discretization tools for analyzing such trajectories, but they also occur in a natural way in arithmetics for instance for the representation of numbers (real, complex), vectors, or else polynomials or Laurent formal power series with coefficients in a finite field.

Symbolic dynamics originates in the work of Jacques Hadamard [44], in 1898, through the study of geodesics on surfaces of negative curvature (see also [23]). It was then also applied by Marston Morse in 1921 in [62] to the construction of a nonperiodic recurrent geodesic and for the symbolic representations of geodesics. The study of combinatorics on words originates at the same time in papers of Axel Thue from 1906 and 1912 (see [75, pp. 139-158 and 413-477]), in particular with the study of the Thue-Morse word. Symbolic dynamics and Sturmian words then were developed by Morse and Hedlund in 1938 in [63, 64].

We first will recall basic definitions concerning symbolic dynamics in Section 2. We illustrate them with transformations like beta-numeration and continued fractions issued from arithmetic dynamics in Section 3. We focus on orbits that are relevant in computer science, namely finite and periodic ones, in Section 4. Lastly, Section 5 is devoted to Loch's theorem. Some parts of this text come from [10].

2 Discrete dynamical systems

2.1 First definitions

By *discrete dynamical system* we mean here a piecewise-continuous mapping $T\colon X \to X$ that acts on a space X that will be usually assumed to be compact.

The (one-sided) *orbit* of $x \in X$ under the action of T is defined as $\{T^n x \mid n \in \mathbb{N}\}$. If T is assumed to be invertible (e.g., if T is a homeomorphism), then the two-sided orbit of $x \in X$ under the action of T is defined as $\{T^n x \mid n \in \mathbb{Z}\}$. Orbits are also called *trajectories*.

The terminology discrete refers here to the time: we consider trajectories of points of X under the discrete-time deterministic action of the mapping T. Discrete dynamical systems can be of a geometric nature (e.g., $X = [0, 1]$), or of a symbolic nature (e.g., $X = \{0,1\}^{\mathbb{N}}$), such as described below. More precisely, as examples of dynamical systems, let us mention

- symbolic dynamical systems: these are dynamical systems defined on sets of symbols and words; we consider them in Section 2.2;
- the beta-transformation (see Section 3.1) or the Gauss map (see Section 3.2), that both act on the unit interval $[0,1]$, and that allow the representation of real numbers, as beta-expansions or as continued fractions respectively;
- the translation R_α by α on the one-dimensional torus, that is, $R_\alpha\colon x \mapsto x + \alpha \bmod 1$ (see Section 3.3).

The notion of dynamical system can be considered in a topological context (this is what we have considered so far), we get *topological dynamics*, but this notion can be extended to measurable spaces: we thus get *measure-theoretic dynamical systems*, that is, dynamical systems endowed with a probabilistic structure (an invariant measure). We will consider them in Section 2.3

2.2 Symbolic dynamical systems

For detailed introductions to symbolic dynamics and word combinatorics, see [3, 7, 19, 14, 15, 50, 55, 59, 60, 37] and the references therein.

An *alphabet* is a finite set of *symbols* (or *letters*). Let $\mathcal{A}$ be an alphabet. A *finite* word over $\mathcal{A}$ is a finite sequence of letters in $\mathcal{A}$ (that is, a word of length $n \in \mathbb{N}$ is a map u from $\{0,1,\cdots,n-1\}$ to $\mathcal{A}$). We write it as $u = u_0 \cdots u_{n-1}$ to express u as the concatenation of the letters u_i.

Let $u = u_0 \cdots u_{m-1}$ and $v = v_0 \cdots v_{n-1}$ be two words over $\mathcal{A}$. The *concatenation* of u and v is the word $w = w_0 \cdots w_{m+n-1}$ defined by $w_i = u_i$ if $0 \le i < m$, and $w_i = v_{i-m}$ otherwise. We write $u \cdot v$ or simply uv to express the concatenation of u and v. The set of all (finite) words over $\mathcal{A}$ is denoted by $\mathcal{A}^*$. Endowed with the concatenation of words as product operation, $\mathcal{A}^*$ is a monoid with ε as identity element. It is the *free* monoid generated by $\mathcal{A}$. We thus have endowed the set of finite words with an algebraic structure.

We also consider infinite words, that is, elements of $\mathcal{A}^{\mathbb{N}}$, as well as bi-infinite (also called two-sided) words in $\mathcal{A}^{\mathbb{Z}}$. All the notions defined below extend to two-sided words in $\mathcal{A}^{\mathbb{Z}}$.

A word $w_1 \cdots w_\ell$ is a *factor* of the word u (finite, infinite or bi-infinite) if there exists k such that $u_k \cdots u_{k+\ell-1} = w_1 \cdots w_\ell$. The set of factors $\mathcal{L}_u$ of an infinite word u is called its *language*. The (*factor*) *complexity function* of an infinite word u counts the number of distinct factors of a given length: there are exactly $p_u(n)$ factors of length n in u. For more on this function, see for instance [3].

The topology is given by the usual metric on infinite words in $\mathcal{A}^{\mathbb{N}}$: two infinite words are close if they coincide on their first terms. More precisely, the set $\mathcal{A}^{\mathbb{N}}$ shall be equipped with the product topology of the discrete topology on each copy of $\mathcal{A}$. Thus, this set is a compact space. This topology is also the topology defined by the following distance:

$$\text{for } u \neq v \in \mathcal{A}^{\mathbb{N}},\ d(u,v) = 2^{-\min\{n \in \mathbb{N};\ u_n \neq v_n\}}.$$

Note that the space $\mathcal{A}^{\mathbb{N}}$ is complete as a compact metric space. Furthermore, it is a *Cantor set*, that is, a totally disconnected compact set without isolated points. Note that the topology extends in a natural way to $\mathcal{A}^{\mathbb{N}} \cup \mathcal{A}^{\star}$. Indeed, let $\mathcal{B}$ be a new alphabet obtained by adding a further letter to the alphabet $\mathcal{A}$; words in $\mathcal{A}^{\star}$ can be considered as sequences in $\mathcal{B}^{\mathbb{N}}$, by extending them by the new letter in $\mathcal{B}$. The set $\mathcal{A}^{\mathbb{N}} \cup \mathcal{A}^{\star}$ is thus metric and compact, as a closed subset of $\mathcal{B}^{\mathbb{N}}$.

The mapping S acting on sets of infinite words is the (one-sided) *shift* acting on $\mathcal{A}^{\mathbb{N}}$: $S((u_n)_{n\in\mathbb{N}}) = (u_{n+1})_{n\in\mathbb{N}}$. It is continuous.

A *subshift (also called shift)* is a closed shift invariant system included in some $\mathcal{A}^{\mathbb{N}}$. If Y is a subshift, there exists a set $\mathcal{F} \subset \mathcal{A}^*$ of finite words such that an infinite word u belongs to Y if, and only if, none of its factors belongs to $\mathcal{F}$. A subshift X is called a *subshift of finite type* if one can choose the set $\mathcal{F}$ to be finite. A subshift is said to be *sofic* if the set $\mathcal{F}$ is a regular language.

As an example of a shift, take the closure in $\mathcal{A}^{\mathbb{N}}$ of $u = (u_n)_{n\geq 0}$, with u being some infinite word in $\mathcal{A}^{\mathbb{N}}$. Let $X_u := \overline{\mathcal{O}(u)}$ be the positive orbit closure of the infinite word u under the action of the shift S, i.e., the closure in $\mathcal{A}^{\mathbb{N}}$ of the set $\mathcal{O}(u) = \{S^n(u) \mid n \geq 0\}$. One checks that $\overline{\mathcal{O}(u)} = \{v \in \mathcal{A}^{\mathbb{N}},\ \mathcal{L}_v \subset \mathcal{L}_u\}$, where $\mathcal{L}_v$ is recalled to be the set of factors of the sequence v.

For a word $w = w_0 \ldots w_r$, the *cylinder set* $[w]$ is the set $\{v \in X_u \mid v_0 = w_0, \ldots, v_r = w_r\}$. The cylinder sets are *clopen* (open and closed) sets and form a basis of open sets for the topology of X_u. Indeed, if the cylinder $[w]$ is nonempty and v is a point in it, $[w]$ is identified with both the open ball $\{v' \mid d(v,v') < 2^{-n}\}$ and the closed ball $\{v' \mid d(v,v') \leq 2^{-n-1}\}$. As an exercise, prove that a clopen set is a finite union of cylinders.

Let us come back to the general case of a discrete dynamical system $T\colon X \to X$. In order to understand the behavior of trajectories, it is natural to partition the set X into a finite number (say d) of subsets $(X_i)_{1\leq i\leq d}$: $X = \cup_{i=1}^{d} X_i$. We then *code* the trajectory of a point $x \in X$ with respect to the finite partition $(X_i)_{1\leq i\leq d}$. One thus associates with each point $x \in X$ an infinite word with values in the finite alphabet $\{1, \ldots, d\}$ defined as follows:

$$\forall n \in \mathbb{N},\ u_n = i \text{ if and only if } T^n(x) \in X_i.$$

Coding trajectories allows one to go from dynamical systems (X, T) defined on 'geometric' spaces X to symbolic dynamical systems and backwards, provided the coding has been chosen in an efficient way. Section 3.3 devoted to Sturmian words, provides an example of such a fruitful coding. If the partition is well-chosen, these symbolic codings allow the statistical analysis (via ergodic theory) on the underlying dynamical systems. This is the object of next section.

2.3 Measure-theoretic dynamical systems

General references on the subject are [8, 18, 28, 46, 69, 72, 78]. See [31] for connections with number theory and Diophantine approximation.

A *measure-theoretic dynamical system* is defined as a system $(X, T, \mu, \mathcal{B})$, where μ is a probability measure defined on the σ-algebra $\mathcal{B}$ of subsets of X, and $T : X \to X$ is a measurable map which preserves the measure μ, that is, $\mu(T^{-1}(B)) = \mu(B)$ for all $B \in \mathcal{B}$. The measure μ is said to be *T-invariant*.

An invariant probability measure on X is said *ergodic* if for every set $B \in \mathcal{B}$, $T^{-1}(B) = B$ has either zero or full measure. The system $(X, T, \mu, \mathcal{B})$ is then said to be *ergodic*. This implies that almost all orbits are dense in X (almost all means that the set of elements $x \in X$ whose orbit is not dense is contained in a set of zero measure). More generally a property is said to hold *almost everywhere* (abbreviated as a.e.) if the set of elements for which the property does not hold is contained in a set of zero measure; this property is said to be *generic* (the points that satisfy this property are then also said to be generic). This helps us to give a meaning to the notion of typical behavior for a dynamical system.

Ergodicity yields furthermore the following striking convergence result. Indeed, measure-theoretic ergodic dynamical system satisfy the *Birkhoff ergodic theorem*, also called *individual ergodic theorem*, which relates spatial means to temporal means.

Theorem 1 (Birkhoff Ergodic Theorem)**.** *Let $(X, T, \mu, \mathcal{B})$ be an ergodic measure-theoretic dynamical system. Let $f \in L^1(X, \mathbb{R})$. Then*

$$\forall f \in L^1(X, \mathbb{R}) \ , \quad \frac{1}{n} \sum_{k=0}^{n-1} f \circ T^k \xrightarrow[n\to\infty]{\mu-a.e.} \int_X f \, d\mu \ .$$

Points for which this convergence property holds for a given f are generic.

In the case of a symbolic dynamical system $(\overline{\mathcal{O}(u)}, S)$ generated by an infinite word u, the following special case of the Daniell-Kolmogorov consistency theorem (see for instance [78]) provides probability measures on $(\overline{\mathcal{O}(u)}, S)$.

Theorem 2. *Let $\mathcal{A} = \{1, \ldots, d\}$ and $u \in \mathcal{A}^{\mathbb{N}}$. Consider a family of maps $(p_n)_{n\geq 1}$, where p_n is a map from $\mathcal{A}^n$ to $\mathbb{R}$, such that for any word w in $\mathcal{A}^n$, $p_n(w) \geq 0$, $p_n(w) = \sum_{i=1}^{d} p_{n+1}(w_1 \ldots w_n i)$, and $\sum_{i=1}^{d} p_1(i) = 1$. Then there exists a unique probability measure μ on $\mathcal{A}^{\mathbb{N}}$ defined on the cylinders by $\mu([w_1 \ldots w_n]) = p_n(w_1 \ldots w_n)$.*

Furthermore, if for any n and for any word $w = w_1 \ldots w_n$ in $\mathcal{A}^n$, $p_n(w) = \sum_{i=1}^{d} p_{n+1}(iw_1 \ldots w_n)$, then this measure is S-invariant (shift-invariant).

Let u be a word in $\mathcal{A}^{\mathbb{N}}$. The *frequency* $f(i)$ of a letter $i \in \mathcal{A}$ in u is defined as the limit when n tends towards infinity, if it exists, of the number of occurrences of i in $u_0u_1\cdots u_{n-1}$ divided by n. The word u has *uniform letter frequencies* if, for every letter i of u, the number of occurrences of i in $u_k\cdots u_{k+n-1}$ divided by n has a limit when n tends to infinity, uniformly in k. Similarly, we can define the frequency $f(w)$ and the uniform frequency of a factor w, and we say that u has *uniform frequencies* if all its factors have uniform frequency.

In particular, if the frequencies of all factors exist for a given $u \in \mathcal{A}^{\mathbb{N}}$, then, according to Theorem 2, there exists a unique S-invariant probability measure μ which assigns to each cylinder $[w]$ the frequency $f(w)$ of the corresponding factor $[w]$, by setting $\mu[w] := f(w)$. Thus a precise knowledge of the frequencies allows a complete description of the measure μ. One can similarly define a shift-invariant measure for a subshift $X \subset \mathcal{A}^{\mathbb{N}}$ provided that any factor w in the langage of X (i.e., the set of factors of its elements) has the same frequency in all the infinite words of X. Moreover, the property of having uniform factor frequencies for a shift is equivalent to *unique ergodicity*, that is, to have a unique invariant measure. Unique ergodicity corresponds in the case of continuous functions to uniform convergence for *all* points (and not only for a.e. point) in ergodic sums, in Birkhoff's ergodic theorem. For more details on invariant measures and ergodicity, we refer to [72] and [14, Chap. 7].

Natural questions that can be addressed now concerning discrete dynamical systems are the following. What is a good coding? How to describe the invariant measures? Can one find geometric representations of a goven symbolic dynamical system? How to measure the disorder of a dynamical system? The next sections provides some elements of answer.

2.4 Isomorphisms

Let us come back to the coding a dynamical system via a suitable partition. In order to make more precise the notion of good coding, let us see how to "compare" two dynamical systems.

Two topological dynamical systems (X, S) and (Y, T) are said to be *topologically conjugate* (or *topologically isomorphic*) if there exists an homeomorphism f from X onto Y which conjugates S and T, that is:

$$f \circ S = T \circ f.$$

Two topological dynamical systems (X, S) and (Y, T) are said to be *semi-topologically conjugate* if there exist two sets X_1 and Y_1 which are at most countable such that $B_1 = X \setminus X_1$, $B_2 = Y \setminus Y_1$, and f is a bicontinuous bijection from B_1 onto B_2 which conjugates S and T. The map f is said to be a *semi-topological conjugacy.*

Let us introduce an equivalent of the notion of topological conjugacy for measure-theoretic dynamical systems. The idea here is to remove sets of measure zero in order to conjugate the spaces via an invertible measurable transformation. For a nice exposition of connected notions of isomorphism, see [46, 78].

Two measure-theoretic dynamical systems $(X_1, T_1, \mu_1, \mathcal{B}_1)$ and $(X_2, T_2, \mu_2, \mathcal{B}_2)$ are said to be *measure-theoretically isomorphic* if there exist two sets of full measure $B_1 \in \mathcal{B}_1$, $B_2 \in \mathcal{B}_2$, a measurable map $f : B_1 \to B_2$ called *conjugacy map* such that

- the map f is one-to-one and onto,
- the reciprocal map of f is measurable,
- $f \circ T_1(x) = T_2 \circ f(x)$ for every $x \in B_1 \cap T_1^{-1}(B_1)$,
- μ_2 is the image of the measure μ_1 with respect to f, that is,

$$\forall B \in \mathcal{B}_2,\ \mu_1(f^{-1}(B \cap B_2)) = \mu_2(B \cap B_2).$$

2.5 Entropy

We briefly discuss in this section the notion of entropy which provides a measure of disorder for dynamical systems: in particular, it allows to distinguish between deterministic and chaotic dynamical systems. Deterministic systems have zero entropy, whereas chaotic systems have positive entropy. We will not enter into the details of possible definitions for chaoticity. A general reference on the subject is [32]. We just stress the fact that it is expected from chaotic dynamical systems that close initial points have divergent orbits, with the separation rate being exponential (this is called *sensitivity to initial conditions*), to have dense periodic points, as well as a topological property of mixing. The beta-transformation (see Section 3.1) and the Gauss map (see Section 3.2) are examples of chaotic systems. Indeed, the Gauss map is sensitive to initial conditions: rational initial points form a dense set and are attracted to 0, whereas quadratic irrational points are eventually attracted to a periodic orbit (which is not finite). We focus here on the case of maps of the unit circle but all these notions hold for more general dynamical systems. For more on the entropy of dynamical systems, see for instance [46, 78].

As seen before for other dynamical concepts, the notion of entropy can be defined either in a topological context, or in a measure-theoretic context. Let us start with the case of symbolic dynamical systems and topological entropy, defined with respect to the complexity function. Let X be a subshift of $\mathcal{A}^{\mathbb{N}}$. Recall that the complexity function $p_X(n)$ counts the number of factors of infinite word in X of length n. The *topological entropy* of the shift (X, S) is then defined as the exponential growth rate of the complexity function as the length increases:

$$H_{top}(X) = \lim_{n \to +\infty} \frac{\log_d(p_X(n))}{n},$$

where d denotes the cardinality of the alphabet $\mathcal{A}$. The existence of the limit follows from the subadditivity of the function $n \mapsto \log_d(p_X(n))$:

$$\forall m, n,\ \log_d(p_X(n+m)) \leq \log_d(p_X(m)) + \log_d(p_X(n)).$$

This notion also extends to more general topological dynamical systems by involving open covers.

One then can define a similar notion of measure-theoretic entropy. Let us consider the case of a symbolic dynamical system for which all elements admit factor frequencies. We assume that for any factor w of the language of X, all elements in X have the same frequency $f(w)$. Let μ be the shift-invariant measure provided by the frequencies. We recall that $\mathcal{L}_X(n)$ stands for the set of factors of length n of X. The *measure-theoretic entropy* of the shift (X, S, μ) is then defined as

$$H_\mu(X) = \lim_{n\to+\infty} \frac{1}{n} \sum_{w\in\mathcal{L}_X(n)} L(f(w)) = \lim_{n\to+\infty} \frac{1}{n} \sum_{w\in\mathcal{L}_X(n)} L(\mu[w])$$

where $L(x) = -x\log_d(x)$ for $x \neq 0$, and $L(0) = 0$ (d stands for the cardinality of the alphabet $\mathcal{A}$).

Once again, this notion extends to the case of general measure-theoretic dynamical systems through the use of pullbacks and refined partitions. In the particular case where T is a piecewise $\mathcal{C}_1$ map from the unit interval $I = [0, 1]$ into itself, natural expansion assumptions yield the existence of an absolutely continuous invariant Borel measure μ for T, then $\log|T'|$ is μ-integrable and its *metric entropy* h_μ satisfies, according to Rohlin's entropy formula:

$$h_\mu(T) = \int_I \log|T'| d\mu.$$

One recovers, under the assumption of ergodicity and through Birkhoff's ergodic theorem, the notion of *Lyapounov exponent* of a dynamical system (provided by a one-dimensional differentiable map), which measures the exponential rate of separation of orbits. It is defined for an orbit of a dynamical system (X, T), with T being piecewise differentiable, as

$$\lambda(x) = \lim_{n\to\infty} \frac{1}{n} \log\left(\prod_{i=0}^{n-1} |T'(T^i(x))|\right) = \lim_{n\to\infty} \frac{1}{n} \log\left(|(T^n(x))'|\right),$$

when this limit exists. Note that the formula given here comes from the chain rule applied to $T^n(x)$ in order to get its derivative. This allows us to get information on $|T^n(x) - T^n(y)|$. Indeed, intuitively (and as nicely explained in Chap. 9 of [24]), $|T(x) - T(y)|$ is approximatively equal to $T'(x) \cdot |x - y|$ (under suitable hypotheses such as x and y being close), whereas $|T^n(x) - T^n(y)|$ has to be compared with $\prod_{i=0}^{n-1} |T'(T^i x)| \cdot |x - y|$. This implies

$$|T^n(x) - T^n(y)| \sim \exp n\lambda(x) \cdot |x - y|,$$

which allows one to connect the rate of divergence of distinct orbits to the Lyapounov exponent. Under suitable assumptions for $(X, T, \mathcal{B}, \mu)$ (ergodicity at least), the ergodic theorem provides that for a.e. point x

$$\lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n-1} \log|T'(T^i(x))| = \int_I \log|T'| d\mu = h_\mu(T).$$

The systems associated with the beta-numeration (that is, with the beta-transformation) and with continued fractions (that is, with the Gauss map) have positive entropy, whereas the translation R_α on $\mathbb{R}/\mathbb{Z}$ has zero entropy (it is deterministic).

3 Arithmetic dynamics

We consider in this section examples of dynamical systems that all pertain to what is called 'arithmetic dynamics' in [74]. Note that the term 'arithmetic dynamics' also refers in the literature to the study of the number-theoretic properties of integer, rational, p-adic, or else algebraic points under repeated application of a polynomial or rational function (according to Wikipedia `https://en.wikipedia.org/wiki/Arithmetic_dynamics`).

The survey [74] deals with explicit arithmetic expansions of reals and vectors that have a 'dynamical' flavor. These expansions allow to (semi-)conjugate a given dynamical system and a symbolic one, with the arithmetic properties of the point x in the dynamical system X being reflected in its expansion. We focus here on classical examples of arithmetic dynamics, namely numeration dynamics, continued fractions and Sturmian shifts. Symbolic representations such as the ones described below allow for compact representations of real numbers.

3.1 Numeration dynamics

Let us use the usual base q numeration, as an illustration of a numeration system that can be described in terms of a dynamical system, where the integer q satisfies $q \geq 2$. But first recall that there are two well-known algorithmic ways of producing the digits $a_i \in \{0, \ldots, q-1\}$ of the expansion of a positive integer $N = a_k q^k + \cdots + a_0$ in base q. The greedy algorithm produces the digits of N most significant digit first: take k such that $q^k \leq N < q^{k+1}$ and set $a_k := \lfloor N/q^k \rfloor$; one then reiterates the process with N being replaced by $N - a_k q^k$ in order to get the digits in decreasing power order. Now, consider the second generation method. Let the notation $y \bmod q$ stand for the unique number in $\{0, 1, \ldots, q-1\}$ which is congruent to y modulo q. The dynamical system $(\mathbb{N}, S_q)$ with

$$S_q \colon \mathbb{N} \to \mathbb{N}, \quad n \mapsto \frac{n - (n \bmod q)}{q}$$

together with the coding map $\psi_q \colon \mathbb{N} \to \{0, 1, \ldots, q-1\}, \quad n \mapsto n \bmod q$ (which is associated with the natural partition of $\mathbb{N}$ given by the sets $k + q\mathbb{N}$, for $0 \leq k \leq q-1$), produces the digits least significant digit first: one has $a_{i+1} = \psi_q(S_q^i(N))$ for all i. Taking all sequences of digits produced by considering all integers yields a symbolic dynamical system made of infinite words that all eventually take the value 0.

Similarly, the dynamical system producing the q-ary expansions of positive real numbers is defined as $([0,1], T_q)$, with

$$T_q\colon [0,1] \to [0,1],\ x \mapsto qx - \lfloor qx \rfloor = \{qx\} = qx \pmod 1,$$

together with the coding map $\varphi_q\colon [0,1] \to \mathbb{N},\ x \mapsto \lfloor qx \rfloor$. Indeed, if $x = \sum_{i\geq 1} a_i q^{-i}$, then $\lfloor qx \rfloor = a_1 + \sum_{i\geq 1} a_{i+1} q^{-i}$, and $\{qx\} = \sum_{i\geq 1} a_{i+1} q^{-i}$. One thus has $a_i = \lfloor q T_q^{i-1}(x) \rfloor = \varphi_q(T_q^{i-1}(x))$, for all $i \geq 1$. Note that the admissible expansions produced by T_q never terminate in $(q-1)(q-1)(q-1)\cdots$. When $q = 10$ one recovers the decimal expansion, and the binary one for $q = 2$.

More generally, the so-called *beta-numeration* embraces and extends q-ary numeration. Taking a real number $\beta > 1$, it consists in expanding numbers $x \in [0,1]$ as power series in base β^{-1} with digits in the set $\{0, \ldots, \lceil \beta \rceil - 1\}$. The mapping

$$T_\beta\colon x \mapsto \{\beta x\} = \beta x \pmod 1$$

together with the coding map $\varphi_\beta\colon x \mapsto \lfloor \beta x \rfloor$ produces the digits

$$a_i = \lfloor \beta T_\beta^{i-1}(x) \rfloor = \varphi_\beta(T_\beta^{i-1}(x)),$$

for $i \geq 1$, which yields the expansion

$$x = \sum_{i\geq 1} a_i \beta^{-i}.$$

For more on beta-numeration, see e.g. [31, 38, 39]. Such expansions belong to the more general family of so-called f-expansions [73]: one expands real numbers as

$$x = \lim_{n\to\infty} f(a_1 + f(a_2 + f(a_3 + \cdots + f(a_n)\cdots))),\ \text{with } a_i \in \mathbb{N}.$$

For $\beta > 1$, the entropy of the β-transformation T_β is equal to $\log \beta$.

3.2 The Gauss map

For general references on continued fractions, see e.g. [18, 31, 45, 49].

The Gauss map T_G is defined on $[0,1]$ by

$$T_G\colon x \mapsto \{1/x\} \text{ for } x \neq 0, \quad T_G(0) = 0.$$

Together with the coding map $\varphi_G\colon x \mapsto \lfloor 1/x \rfloor$, it produces the partial quotients in the *continued fraction* expansion of a real number $x \in [0,1]$.

Let $x \in (0,1)$. If $x_1 = T_G(x) = \{1/x\} = \frac{1}{x} - \lfloor \frac{1}{x} \rfloor = \frac{1}{x} - a_1$, then $x = \frac{1}{a_1 + x_1}$. Now, set $a_n = \lfloor \frac{1}{T^{n-1}x} \rfloor = \varphi_G(T^{n-1}x)$ for $n \geq 1$. One has

$$x = \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_4 + \cdots}}}}.$$

We also will use the notation $x = [0; a_1, \cdots, a_n, \cdots]$. The digits a_n are called *partial quotients*. Continued fractions are known to provide good rational approximations of real numbers. Indeed, let $p_n/q_n = [0; a_1, \cdots, a_n]$ stand for the n-th truncation of the continued fraction of x. One has $|x - p_n/q_n| < 1/q_n^2$ for all n.

Note that continued fractions extend also to Laurent formal power series with coefficients in a finite field, see e.g. the survey [13] and the references therein. As an application, let us mention some interesting connections with pseudorandom numbers generated by the digital multistep method [65], with low-discrepancy sequences [66], or with stream cipher theory and cryptography [67].

Here, we endow $([0,1], T_G)$ with the Gauss measure μ_G which is the Borel probability measure defined as the absolutely continuous measure with respect to the Lebesgue measure by

$$\mu_G(B) = \frac{1}{\log 2} \int_B \frac{1}{1+x} dx.$$

One checks that this measure is T_G-invariant, i.e., $\mu_G(B) = \mu_G(T_G^{-1}B)$ for every Borel subset B of $[0,1]$. It is also ergodic. This measure is the unique T_G-invariant measure that is absolutely continuous with respect to Lebesgue measure.

By applying the ergodic theorem to the Gauss map, one obtains that the Lyapounov exponent is a.e. equal to $\frac{\pi^2}{6 \log 2}$, which is also equal to the entropy. The statistical properties concerning the digits in the continued fraction expansion of α are provided by the Gauss measure via the ergodic theorem. For instance, for a.e. x, one has

$$\lim_{N \to \infty} \frac{1}{N} \operatorname{Card}\{n \leq N;\ a_n = k\} = \frac{1}{\log 2} \log \left(\frac{(k+1)^2}{k(k+1)} \right).$$

Note that the continued fraction algorithm is closely related to *Euclid's algorithm*: let us start with two (coprime) positive integers u_0 et u_1; Euclid's algorithm works by subtracting as much as possible the smallest of both numbers from the largest one (that is, one performs the Euclidean division of the largest one by the smallest); this yields $u_0 = u_1 \lfloor \frac{u_0}{u_1} \rfloor + u_2$, $u_1 = u_2 \lfloor \frac{u_1}{u_2} \rfloor + u_3$, *etc.*, until we reach $u_{m+1} = 1 = \operatorname{pgcd}(u_0, u_1)$. By setting for $i \in \mathbb{N}$, $\alpha_i = \frac{u_i}{u_{i+1}}$ and $a_i = \lfloor \alpha_i \rfloor$, one gets $\alpha_{i-1} = a_{i-1} + \frac{1}{\alpha_i}$ and

$$\alpha_0 = u_0/u_1 = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cdots + \frac{1}{a_{m-1} + 1/a_m}}}}$$

3.3 Codings of rotations and Sturmian words

Sturmian words provide symbolic codings of translations R_α of the unit circle (that is, the one-dimensional torus $\mathbb{T} = \mathbb{R}/\mathbb{Z}$) with

$$R_\alpha \colon \mathbb{R}/\mathbb{Z} \to \mathbb{R}/\mathbb{Z},\ x \mapsto x + \alpha \bmod 1.$$

They have been introduced in [64] and widely studied. For more on Sturmian words, see the corresponding chapters in [60, 37] and the references therein.

The infinite word $u = (u_n)_{n\in\mathbb{N}} \in \{0,1\}^{\mathbb{N}}$ is said to be a *Sturmian word* if there exist $\alpha \in (0,1)$, $\alpha \notin \mathbb{Q}$, $x \in \mathbb{R}$ such that

$$\forall n \in \mathbb{N},\ u_n = i \Longleftrightarrow R_\alpha^n(x) = n\alpha + x \in I_i \pmod 1,$$

with either $I_0 = [0, 1-\alpha[,\ I_1 = [1-\alpha, 1[$, or $I_0 =]0, 1-\alpha],\ I_1 =]1-\alpha, 1]$.

A Sturmian word is thus a coding of the dynamical system $(\mathbb{T}, R_\alpha)$ with respect either to the two-interval partition $\{I_0 = [0, 1-\alpha[,\ I_1 = [1-\alpha, 1[\}$ or to $\{I_0 =]0, 1-\alpha],\ I_1 =]1-\alpha, 1]\}$.

The following lemma is crucial for the study of Sturmian words.

Lemma 1. *The word $w = w_1 \cdots w_n$ over the alphabet $\{0,1\}$ is a factor of the Sturmian word u if and only if $I_w := I_{w_1} \cap R_\alpha^{-1} I_{w_2} \cap \cdots R_\alpha^{-n+1} I_{w_n} \neq \emptyset$.*

Proof. By definition, one has

$$\forall i \in \mathbb{N},\ u_n = i \Longleftrightarrow n\alpha + x \in I_i \pmod 1.$$

One first notes that $u_k u_{k+1} \cdots u_{n+k-1} = w_1 \cdots w_n$ if and only if

$$\begin{cases} k\alpha + x \in I_{w_1} \\ (k+1)\alpha + x \in I_{w_2} \\ \ldots \\ (k+n-1)\alpha + x \in I_{w_n}. \end{cases}$$

One then applies the density of $(n\alpha)_{n\in\mathbb{N}}$ in $\mathbb{Z}/\mathbb{R}$ (recall that α is assumed to be an irrational number). □

One first notes that the condition of Lemma 1 does not depend on the point x whose orbit is coded but only on α. Also, it does not depend on the partition $I_0 = [0, 1-\alpha[,\ I_1 = [1-\alpha, 1[$, or $I_0 =]0, 1-\alpha],\ I_1 =]1-\alpha, 1]$. One thus can define the *Sturmian shift* (X_α, S) as the closure in $\{0,1\}^{\mathbb{N}}$ of the orbit of any Sturmian word coding R_α (and also as the closure in $\{0,1\}^{\mathbb{N}}$ of the orbit of all Sturmian words coding R_α). Indeed, since two Sturmian words coding the same rotation have the same set of factors, then one checks that the symbolic dynamical system generated by a Sturmian word coding the rotation R_α consists of *all* the Sturmian words that code the same rotation. The system (X_α, S) is *minimal*: it admits no non-trivial closed and shift-invariant subset.

One easily checks that the sets $I_{w_1} \cap R_\alpha^{-1} I_{w_2} \cap \cdots R_\alpha^{-n+1} I_{w_n}$ are intervals of $\mathbb{T} = \mathbb{R}/\mathbb{Z}$. Furthermore, the factors of u of length n are in one-to-one correspondence with the $n+1$ intervals of $\mathbb{T}$ whose end-points are given by $-k\alpha \bmod 1$, for $0 \leq k \leq n$. This implies that two Sturmian words coding the same rotation R_α have the same factors. Furthermore, Sturmian words have exactly $n+1$ factors of length n, for every $n \in \mathbb{N}$. This is even a characterization of Stumian words:

Theorem 3 (Coven-Hedlund [29]). *A word $u \in \{0,1\}^{\mathbb{N}}$ is Sturmian if and only if it has exactly $n+1$ factors of length n.*

An infinite word u is *periodic* (respectively *ultimately periodic*) if there exists a positive integer T such that $\forall n,\ u_n = u_{n+T}$.

Note that the complexity function can be considered as a good measure of the disorder of a sequence as it is smallest for periodic sequences. Namely, a basic result of [29] is the following.

Proposition 1. *If u is a periodic or ultimately periodic sequence, $p_u(n)$ is a bounded function. If there exists an integer n such that $p_u(n) \leq n$, u is an ultimately periodic sequence.*

Proof. The first part is trivial. In the other direction, we have $p_u(1) \geq 2$ otherwise u is constant, so $p_u(n) \leq n$ implies that $p_u(k+1) = p_u(k)$ for some k. For each word w of length k occurring in u, there exists at least one word of the form wa occurring in u, for some letter $a \in \mathcal{A}$. As $p_u(k+1) = p_u(k)$, there can be only one such word. Hence, if $u_i...u_{i+k-1} = u_j...u_{j+k-1}$, then $u_{i+k} = u_{j+k}$. As the set $\mathcal{L}_u(k)$ is finite, there exist $j > i$ such that $u_i...u_{i+k-1} = u_j...u_{j+k-1}$, and hence $u_{i+p} = u_{j+p}$ for every $p \geq 0$, one period being $j-i$. □

By Proposition 1, Sturmian words are non-periodic words of smallest complexity. This explains why Sturmian words are widely studied and occur in various contexts as models of aperiodic order, for quasiperidoic structures such as quasicrystals (see the books [4, 48]), or else in discrete geometry, as (Freeman) coding discrete lines in discrete geometry. More generally, for references on discrete lines, see the surveys [52, 22].

One deduces from Lemma 1 not only properties of a topological nature on the number of factors, but also information of a measure-theoretical nature, such as the expression of densities of factors [11], that can be deduced from the equidistribution of the sequence $(n\alpha)_{n\in\mathbb{N}}$. Indeed, the frequency of occurrence of the word w in the Sturmian word u is equal to the length of the interval I_w. We have seen in Section 2.3 that it allows the expression of a shift-invariant measure. Moreover, one checks that Sturmian words are uniquely ergodic: the convergence to frequencies is uniform. Frequencies of factors thus provides the unique shift-invariant measure of the Sturmian shift (X_α, S). We also deduce from the expression of the complexity function that it has zero topological entropy.

Moreover, one checks that the systems $(R_\alpha, \mathbb{T})$ and (X_α, S) are measure-theorerically isomorphic, and even semi-conjugate. We thus can consider that the chosen partition provides a good coding. One has the following commutative diagram:

$$\begin{array}{ccc} \mathbb{R}/\mathbb{Z} & \xrightarrow{R_\alpha} & \mathbb{R}/\mathbb{Z} \\ \downarrow & & \downarrow \\ X_\alpha & \xrightarrow[\mathrm{S}]{} & X_\alpha \end{array}$$

Let us consider now a combinatorial way of generating Sturmian words. A *substitution* σ is an application from an alphabet $\mathcal{A}$ into the set of nonempty finite words on $\mathcal{A}$; it extends to a morphism of the free monoid $\mathcal{A}^*$ by concatenation, that is, $\sigma(ww') = \sigma(w)\sigma(w')$ and $\sigma(\varepsilon) = \varepsilon$. It also extends in a natural way to a map defined over $\mathcal{A}^{\mathbb{N}}$ or $\mathcal{A}^{\mathbb{Z}}$.

Substitutions are very efficient tools for producing sequences. Let σ be a substitution over the alphabet $\mathcal{A}$, and a be a letter such that $\sigma(a)$ begins with a and $|\sigma(a)| \geq 2$. Then there exists a unique fixed point u of σ beginning with a. This sequence is obtained as the limit in $\mathcal{A}^{\mathbb{N}}$ (when n tends toward infinity) of the sequence of words $\sigma^n(a)$, which is easily seen to converge.

The *Fibonacci sequence* is the fixed point v beginning with a of the *Fibonacci substitution* σ defined over the two-letter alphabet $\{a, b\}$ by $\sigma(a) = ab$ and $\sigma(b) = a$.

$$v = abaababaabaababaababaabaababaabaababaababaabaababaababaaba...$$

The Fibonacci word is a particular case of a Sturmian word. It belongs to the Sturmian shift associated with the Golden ratio $\alpha = \frac{1+\sqrt{5}}{2}$.

Let us see how to generate all the Sturmian shifts with substitutions. We work now on the alphabet $\{a, b\}$. We consider the substitutions τ_a and τ_b defined over the alphabet $\mathcal{A} = \{a, b\}$ by $\tau_a \colon a \mapsto a, b \mapsto ab$ and $\tau_b \colon a \mapsto ba, b \mapsto b$. Let $(i_n) \in \{a, b\}^{\mathbb{N}}$. The following limits

$$u = \lim_{n\to\infty} \tau_{i_0}\tau_{i_1}\cdots\tau_{i_{n-1}}(a) = \lim_{n\to\infty} \tau_{i_0}\tau_{i_1}\cdots\tau_{i_{n-1}}(b) \tag{1}$$

exist and coincide whenever the directive sequence $(i_n)_n$ is not ultimately constant (it is easily shown that the shortest of the two images by $\tau_{i_0}\tau_{i_1}\ldots\tau_{i_{n-1}}$ is a prefix of the other). One checks that the infinite words thus produced are all Sturmian words: indeed, it suffices to consider and compute their factor complexity. More generally, one can prove that a Sturmian word is an infinite word whose set of factors coincides with the set of factors of a sequence u of the form (1), with the sequence $(i_n)_{n\geq 0}$ being not ultimately constant (that is, it is an element of the symbolic dynamical system X_u generated by u, since (X_u, S) is minimal). The proof relies on the fact that in a Sturmian language, either aa (the letter b occurs as an isolated letter) or bb (a is isolated) occurs: one cannot have simultaneously aa and bb since there are 3 factors of length 2. One then desubstitutes according to the isolated letter: if b is isolated in u, then one can write u as $u = \sigma_a(v)$ (one reduces the ranges of successive occurrences of a' by 1). One checks that v (possibly up to a prefix letter) is again a Sturmian word (associated with a different α). If one wants to generate a specific Sturmian word (not only a Sturmian language/shift), one can use four substitutions. One striking property of Sturmian words is the following: the way one iterates the substitutions is governed by the continued fraction expansion of α. This method can be used for the generation of discrete lines and planes in discrete geometry, as well as for the recognition of discrete planes [33]. More generally shifts with at most linear factor complexity can also be generated in terms of composition of substitutions, see e.g. the survey [12] and the references therein.

Let us see now an example of an arithmetical discrepancy property of R_α that can be proved symbolically. Let $u \in \mathcal{A}^{\mathbb{N}}$ and assume that each letter i has frequency f_i in u. The *discrepancy* of u is $\Delta(u) = \limsup_{i\in\mathcal{A},\ n\in\mathbb{N}} ||u_0u_1\dots u_{n-1}|_i - nf_i|$. The quantity $\Delta(u)$ is considered e.g. in [1, 2]. A word $u \in \mathcal{A}^{\mathbb{N}}$ is said to be C-*balanced* if for any pair v, w of factors of the same length of u, and for any letter $i \in \mathcal{A}$, one has $||v|_i - |w|_i| \le C$. It is said *balanced* if there exists $C > 0$ such that it is C-balanced. If u has letter frequencies, then u is balanced if and only if its discrepancy $\Delta(u)$ is finite. It is also said to have *bounded deviation* (the term 'deviation' refers here to the ergodic averages, that is, the Birkhoff sums associated with the indicator function of the cylinders associated with letters).

A subset A of $\mathbb{T}$ with (Lebesgue) measure $\mu(A)$ is said to be a *bounded remainder set* for the translation $R_\alpha : x \mapsto x + \alpha$ ($\alpha \in \mathbb{T}$) if there exists $C > 0$ such that for a.e. x the following holds: $\forall N,\ \ |\mathrm{Card}\{0 \le n < N\,;\, x + n\alpha \in A\} - N\mu(A)| \le C$. Let $f := \mathbf{1}_A(x) - \mu(A)\mathbf{1}$. The notation $\mathbf{1}$ stands for the constant function that takes value 1. Note that $\mathrm{Card}\{n < N\,;\, R_\alpha^n(x) \in A\} - N\mu(A) = \sum_{n<N} f(R_\alpha^n x)$. Hence, A is a bounded remainder set if and only if the Birkhoff sum $\sum_{n<N} f(R_\alpha^n x)$ is a.e. uniformly bounded.

Sturmian words are known to be 1-balanced [60] (they have bounded deviation with respect to the ergodic theorem); they even are exactly the 1-balanced infinite words that are not eventually periodic. This result can be shown with a purely combinatorial proof. One can also show a balance property for factors (instead of letters) [77]. One thus deduces from Lemma 1 that intervals of the form $\alpha\mathbb{Z} + \mathbb{Z}$ are bounded remainder sets for R_α. One recovers with a purely symbolical proof one direction of Kesten's characterization of intervals that are bounded remainder sets as intervals with length in $\alpha\mathbb{Z} + \mathbb{Z}$ [47].

4 Dynamics and computation

The aim of this section is to discuss dynamical systems and their orbits from a computational viewpoint, motivated by the question of numerical simulations in the framework of finite precision computer arithmetic, but also by applications in discrete geometry or for gcd computations.

4.1 First definitions

An orbit $(T^n(x))_{n\in\mathbb{N}}$ of the dynamical system (X, T) is said to be *eventually periodic* if there exists n such that $T^n(x) = T^{n+k}(x)$, for all $k \in \mathbb{N}$. If $n = 0$, then the orbit is said to be *purely periodic*. In order to define a stronger notion of "finiteness" for an orbit, we will assume that (X, T) has 0 as a fixed point: $0 \in X$ and $T(0) = 0$. The orbit $(T^n(x))_{n\in\mathbb{N}}$ is thus said to be *finite* if there exists n such that $T^n(x) = 0$; this yields $T^{k+n}(x) = 0$ for all $k \in \mathbb{N}$. Finite orbits are thus particular cases of periodic orbits. For instance, in base 10, rational numbers have periodic orbits, whereas decimal numbers have finite orbits.

By *finite state machine simulation* of the dynamical system (X, T), we mean the following: we consider

- a finite set $\hat{X}$, which is a set of finite sequences of, usually, binary digits, this is a *discretization* of the space X,
- a coding map $\varphi\colon X \to \hat{X}$, i.e., a projection onto the discretized space $\hat{X}$,
- and a map $\hat{T}$ that acts on $\hat{X}$ with $\hat{T}(\hat{X}) \subset \hat{X}$, whose action is defined as a finite state machine, i.e., the image of $x \in \hat{X}$ by $\hat{T}$ is computed by a finite state machine that takes as input the sequence of digits of x and then outputs the sequence of digits of $\hat{T}(x)$; we also want the behavior of $\hat{T}$ to be close to the behavior of T, that is, $\hat{T} \circ \varphi$ to be close to $\varphi \circ T$. Let us stress the fact that the transformation $\hat{T}$ acts on a discrete space whereas T acts on a continuous space.

The underlying discretization can be chosen either uniform (see e.g. [61]), or non-uniform, for instance, if one works on floating-point arithmetics, in a domain where the precision is not the same at every point of the space; it is concentrated around 0 and gets less and less accurate when the number to be represented increases. The question is now to understand what happens when the number of points N of the finite space $\hat{X}$ tends to infinity or when the precision tends to 0.

As an example, consider the floating-point simulation $\widehat{T}_G$ of the Gauss map (see e.g. [25, 26, 27]), defined as $\widehat{T}_G(0) = 0$, $\widehat{T}_G(x) = 1/x \bmod 1$ otherwise, with the operations of division and reduction modulo 1 being defined in floating-point arithmetics on the floating-point domain (i.e., on the finite set of numbers represented in this fixed-precision system).

4.2 Main issues

The following issues are thus to be considered. These questions are addressed in full generality and answers depend on the nature of the dynamical system (X, T) (the two extreme cases are usually considered, chaotic case or uniquely ergodic case, but also conservative vs. dissipative dynamics), but we use as a guideline the Gauss map acting on $[0, 1]$.

- **Periodic orbits for** (X, T) **and** $(\hat{X}, \hat{T})$ The orbits produced by a finite state machine simulation of a dynamical system are eventually periodic (the set of representable numbers $\hat{X}$ is finite). What are the finite or the periodic expansions of the dynamical system (X, T)? What is the number of periodic cycles and their lengths for $(\hat{X}, \hat{T})$? What is the size of connected components (i.e., the number of points attracted by a given cycle)? What is the time to reach it (stabilization time)?

- **Genericity and ergodic properties for periodic orbits for** (X, T) Do periodic expansions for (X, T) have a typical behavior? But what could be considered as a typical orbit? a generic orbit, but with respect to which invariant measure? What is the spatial distribution of periodic cycles for (X, T)? Indeed, since measure-theoretical dynamical systems are defined up to sets of zero measure, the relevance of the statistical properties provided by the ergodic theorem with respect to computation can be questioned. In particular, what can be said concerning the behavior of rational points under the Gauss map? We just know that their orbits are finite, and that they correspond to the application of Euclid's algorithm. We also know that points having finite, or periodic orbits are dense. This does not imply a priori that their orbits behave in a generic way.

- **Genericity and ergodic properties for periodic orbits for** $(\hat{X}, \hat{T})$ Same questions on the orbits of $(\hat{X}, \hat{T})$. What is the impact of the fact that the space $\hat{X}$ is discrete? Does discretization detect typical behavior? Are there typical orbits (with respect to (X, T)) among computable ones?

- **Rounding and truncation errors** are then to be taken care of. What can be said concerning the roundoff errors when simulating trajectories? How far are computed orbits from exact ones?

4.3 Roundoffs and shadowing

We focus here on the example of the floating-point Gauss map to illustrate this section. We follow here mainly [25, 26, 27, 40]. Orbits under the real Gauss map T_G are all finite (they reach 0) since machine-representable numbers are rational numbers. If one looks at the orbits produced by the floating-point Gauss map, it is a priori unclear to know whether they also reach 0. In the case of the Gauss map, the notion of genericity refers to the Gauss measure $\mu_G = \frac{1}{\log 2} \int \frac{1}{1+x} dx$ (see Section 3.2), that is the unique ergodic invariant measure absolutely continuous with respect to the Lebesgue measure.

As seen in the previous section, there are two levels of difficulties that have to be handled.

- First, one has to check that the roundoff errors do not accumulate. One way to handle this problem is to prove that orbits under the simulation of the dynamical system have a counterpart in the exact dynamical system, i.e., that they are uniformly close to exact orbits of T. These orbits are said to *shadow* the simulated orbits; see [70] for more on the concept of shadowing (roughly speaking, approximate orbits of a dynamical system are closely followed by exact orbits). Shadowing or pseudo-orbit tracing started with the works of Anosov and Bowen (for smooth uniformly hyperbolic systems) in the seventies, and is now a classical object of study for chaotic dynamical systems.

- But, a second problem occurs: even if orbits under a floating-point version of the dynamical system are proved to be close to exact orbits, there is no reason for these orbits to be generic with respect to T. In other words, what is the measure carried by the true orbit that shadows the computer orbit (in terms of time averages $\lim \frac{1}{N}\sum_{n=0}^{N}\delta_{T^n(x)}$)?

It is proved in [25, 27] that orbits under the floating-point Gauss map are uniformly close to exact orbits with an explicit construction of the initial point of the exact orbit. The proof relies on "backward error" analysis. As stressed in [26], "the y whose actual orbit is shadowing the numerical simulation is a quadratic irrational or rational number, and thus is from a set of zero measure." But the shadowing orbits are usually long, they thus have a tendency to behave like a generic one.

Consider now a general dynamical system (X, T). If it admits invariant measures absolutely continuous with respect to the Lebesgue measure, then among these measures, there exist a unique ergodic one. It is proved in [40], whose expressive title is "Why do computers like Lebesgue measure", that the histograms of computer simulations display the ergodic invariant measure that is absolutely continuous with respect to Lebesgue measure under the main assumption that there exist long trajectories for the computer transformation $\hat{T}$. Long means here that these orbits visit a fixed portion of the space $\hat{X}$. As stressed in [40], the very process of discretization of the spaces forces computer orbits to display only the ergodic invariant measure that is absolutely continuous.

The situation is more contrasted in the general case of conservative homeomorphisms such as highlighted and studied in detail in [43] (see also [42]), where the dynamical behavior of spacial discretizations of a generic homeomorphism of a compact manifold is investigated. The behavior of discretizations is shown to be quite erratic in the conservative case. A property is said to be generic here if it is satisfied (at least) on a countable intersection of dense open sets. It is proved that dynamical properties of a generic conservative homeomorphism cannot be detected using a single discretization, even if subsequences of discretizations allow to detect some dynamical features. The behavior in the conservative and dissipative case for homeomorphims of compact manifolds is also shown to be quite different with respect to spatial discretization.

The case of uniform discretization for circle homeomorphisms is investigated in [61]: in particular, the discrete dynamics induced by Diophantine diffeomorphisms is proved to be asymptotically random (they behave like random mappings such as described in the next section). Moreover, in [61, Proposition 8.1], uniquely ergodic homeomorphisms on a compact Riemannian manifold are considered. It is proved that the uniformly distributed measure on a periodic cycle of the discretization tends to the invariant measure when the number of points tends to infinity.

4.4 Random mappings

It is usual to compare the behaviour of a discretization of a chaotic dynamical system with the behaviour of random mappings. A *random mapping* is a map uniformly chosen randomly among all the maps from $\{1, \dots, N\}$ to itself (each map has probability $1/N^N$ to be chosen). There is an important literature devoted to random mappings, see for instance [20, 34, 51].

We represent a random mapping as a functional graph: nodes are elements of $\{1, \dots, N\}$, there is an arrow from i to j if $f(i) = j$. Note that each connected component contains one cycle. An orbit is made of a path (a tail) that connects to a cycle. A connected component is made of possibly several orbits and can be seen as trees rooted on a cycle.

The expectations of the following parameters have the asymptotics given below when N tends to infinity (note that the distributions are Gaussian).

- The mean number of nodes without antecedents is equivalent to N/e.
- The mean number of cyclic nodes is equivalent to $\sqrt{\pi N/2}$.
- The mean number of connected components is equivalent to $(1/2)\log N$.

For a random point ν, the expectations of

- the size of the component that contains ν is equivalent to $2N/3$;
- the tail length is equivalent to $\sqrt{\pi N/8}$ (i.e., the maximal length of the injective orbit);
- the cycle length is equivalent to $\sqrt{\pi N/8}$ (i.e., the average length of the period of its orbit).

In summary, one has a one giant component and few large trees. Furthermore, periods (cycles) tend to be "long".

4.5 Finite and periodic orbits of the Gauss map

Let us come back to the Gauss map. If N stands for the total number of floating-point numbers in a simulation, then the average length of the period of an orbit is thus expected to be in $\sqrt{\pi N/8} + O(1)$. The equidistribution results for quadratic irrational numbers obtained in [71], through the use of Parry's prime orbit method [68], confirm this long orbit behavior, and the fact that the periodic orbits capture some kind of genericity: taking averages on periodic orbits yields the usual ergodic limits; if each individual periodic orbit behaves in a non-generic way, the distribution of the quadratic irrational numbers ordered with respect to the lengths of their period follows the Gauss measure.

We find the same kind of paradox within the so-called framework of "dynamical analysis of algorithms" which mixes analysis of algorithms (such as initiated by D. E. Knuth) and spectral study of dynamical systems through their transfer operators, with probabilistic and ergodic methods. In particular, the dynamical analysis of Euclid's algorithm (performed in full details in [58, 5], see also

[35, 36, 76]), proves that the orbits of rational points behave indeed in a generic way.

This confirms the pertinence of a dynamical approach in contexts where only integer parameters are to be considered. Let us quote two applications fields. In discrete geometry, continued fractions and Euclid's algorithm are indeed known to describe discretizations of lines, and their possible generalizations describe discrete planes [33]. In order to understand statistical properties of such discretizations, it is useful to rely on the continuous counterpart, that is, on the Gauss map, and on its multidimensional generalizations. Continued fraction algorithms can also be used to describe gcd algorithms such as developed in [16, 17] for real numbers as well as polynomials with coefficients in a finite field. The underlying dynamical systems allow to handle a complete probabilistic analysis of the associated gcd algorithms, by providing both the average-case and the distributional analysis. In particular, the expectation of number of steps is proved to be connected to the entropy of the dynamical system.

5 Continued fractions vs. decimal expansions: Lochs' theorem

The aim of this section is to compare in average the level of information required for computing the continued fraction expansion of a positive real number x whose expansion in some numeration system (decimal, binary, base β etc.) is given. More precisely, we want to know in average the number of digits in one symbolic representation (here, the continued fraction expansion) that can be obtained from the first n digits in another representation.

We first start with decimal expansions (this is the case that has been first handled in the literature, it also yields the more striking result) and ask for the number of decimal digits required for expanding x in continued fraction. We first fix the notation. Let $x \in (0,1)$ be an irrational number with continued fraction $x = [0; a_1, \cdots, a_n, \cdots]$, and with decimal expansion $x = \sum_{i \geq 1} \frac{\varepsilon_i}{10^i}$, with $\varepsilon_i \in \{0, 1, \ldots, 9\}$ for all $i \geq 1$. For $n \geq 1$, let x_n be the lower n-th decimal approximations of x: $x_n = \sum_{i=1}^{n} \frac{\varepsilon_i}{10^i}$.

If two numbers are sufficiently close, then their respective continued fraction expansions have the same first partial quotients. Let us quantify this. For a fixed non-negative integer n, let $k_n(x)$ be the largest non-negative integer k such that the first k partial quotients of x_n are equal to the first k partial quotients of x. The following classic result by G. Lochs [56] describes the a.e. behavior of the quantity $k_n(x)$ and indicates that the n first decimals determine approximatively n of the first partial quotients, which might seem at first view non-intuitive.

Theorem 4. *[56] For almost every irrational number $x \in [0,1]$ (with respect to the Lebesgue measure)*

$$\lim_{n \to \infty} \frac{k_n(x)}{n} = \frac{6 \log 10 \log 2}{\pi^2} \sim 0.9702. \tag{2}$$

In particular, Lochs has shown in [57] that the first 1000 decimals of π give the first 968 partial quotients of the continued fraction expansion of $\pi - 3$.

Note that we recognize in (2) the Lyapounov exponent λ_G (the entropy) of the Gauss map, i.e.,

$$\lim_{n\to\infty} \frac{k_n(x)}{n} = \frac{\log 10}{\lambda_G}.$$

This is in fact not surprising to have the Lyapounov exponent λ_G intervening in the statement of Lochs' theorem. Indeed, the sensitive dependence on initial conditions (i.e., the fact of having a positive Lyapounov exponent) governs the accuracy of computations and makes it even decrease exponentially fast. As quoted from [24], "Due to the sensitive dependence on initial conditions $[\cdots]$ there is a possibility of obtaining meaningless output after many iterations of a transformation in computer experiment. Once we begin with sufficiently many digits, however, iterations can be done without paying much attention to the sensitive dependence on initial data. The optimal number of significant digits can be given in terms of the Lyapounov exponent." Still following [24], the *divergence speed* for a dynamical system (X, T), and for $0 \leq x \leq 1 - 10^{-n}$ with a fixed $n \geq 1$, is defined as

$$V_n(x) = \min\{j \geq 1 \mid |T^j(x) - T^j(x + 10^{-n})| \geq 10^{-1}\}.$$

This quantity is related to the Lyapounov exponent: $V_n(x) \sim n/\lambda(x)$, which implies that on average, the number of significant digits for $T(x)$ becomes $n - \lambda(x)$. The computations made in [24] are based on the maximal number of iterations that can be performed with no loss of precision when working with n significant digits, which can be quantified thanks to the Lyapounov exponent.

A natural question is to understand the dependence of Lochs' theorem with respect to the choice of the basis, namely, here, 10. Lochs's theorem was generalized to more general numerations and transformations in [21, 30, 54, 6], where it was shown that these generalizations of Lochs' theorem can be expressed in terms of the ratio of the entropies (i.e., of the Lyapounov exponents) of the maps involved. In particular, the question of the comparison with β-expansions ($\beta > 1$) is thoroughly answered in [6] (thus also covering the case of q-adic expansions). One expands x as $\sum_{i\geq 1} \frac{\varepsilon_i}{\beta^i}$, where $\varepsilon_i \in \{0, 1, \ldots, \lceil\beta\rceil - 1\}$ for all $i \geq 1$. Recall that the Lyapounov exponent λ_β of the β-transformation T_β is equal to $\log\beta$. Lochs' theorem becomes in this more general framework, with $k_n(x)$ being defined in a similar way as in the decimal case:

Theorem 5. *[6] For every $x \in [0, 1]$*

$$\lim_{n\to\infty} \frac{k_n(x)}{n} = \frac{\lambda_\beta(x)}{\lambda_G(x)} = \frac{6\log 2 \log\beta}{\pi^2},$$

whenever both limit exist simultaneously.

Note that the Lyapounov exponent λ_G of the Gauss map is also expressed as the following limit (when it exists):

$$\lambda_G(x) = -\lim_{n\to\infty} \frac{1}{n} \log|x - p_n/q_n|,$$

where $p_n/q_n = [0; a_1, \cdots, a_n]$. It thus also measures the exponential speed of convergence of the convergents. Theorem 5 makes Lochs' theorem more intuitive since, as underlined in [6], "if x is well approximated by rational numbers, then the amount of information about the continued fraction expansion that can be obtained from its β-expansion is small. Moreover, the larger β is (that is, the more symbols we use to code a number x), the more information about the continued fraction expansion we obtain". Moreover, [6] also provides the Hausdorff dimension of level sets via multifractal analysis and thermodynamic formalism, and proves that a similar result holds for more general Markov maps. Lochs' theorem has also been the object of further extensions for formal power series with coefficients in a finite field (see [53]).

Acknowledgement

I would like to warmly thank Delphine Boucher for her careful reading.

References

[1] B. Adamczewski, *Balances for fixed points of primitive substitutions*, Theoret. Comput. Sci. **307** (2003), 47–75.

[2] B. Adamczewski, *Symbolic discrepancy and self-similar dynamics*, Ann. Inst. Fourier (Grenoble) **54** (2004), 2201–2234.

[3] J.-P. Allouche and J. O. Shallit, *Automatic sequences: Theory and Applications*, Cambridge University Press, 2002.

[4] M. Baake, U. Grimm, Aperiodic order. *Vol. 1. A mathematical invitation*, Encyclopedia of Mathematics and its Applications **149**, Cambridge University Press, 2013.

[5] V. Baladi, B. Vallée. *Euclidean algorithms are Gaussian*, J. Number Theory **110** (2005), 331–386.

[6] L. Barreira, I. Godofredo, *Partial quotients of continued fractions and β-expansions*, Nonlinearity **21** (2008), 2211–2219.

[7] M.-P. Béal and D. Perrin, *Symbolic dynamics and finite automata*, in *Handbook of formal languages, Vol. 2*, Springer, Berlin, 1997.

[8] T. Bedford, M. Keane and C. Series (eds), *Ergodic theory, symbolic dynamics, and hyperbolic spaces*, The Clarendon Press Oxford University Press, New York, 1991.

[9] V. Berthé, *Sequences of low complexity: automatic and Sturmian sequences*, in *Topics in symbolic dynamics and applications*, F. Blanchard, A. Nogueira and A. Maas (eds), London Mathematical Society Lecture Note Series vol. 279, Cambridge University Press, 2000.

[10] V. Berthé, *Numeration and discrete dynamical systems*, Computing **94** (2012), 369–387.

[11] V. Berthé, *Fréquences des facteurs des suites sturmiennes*, Theoret. Comput. Sci. **165** (1996), 295–309.

[12] V. Berthé, V. Delecroix, *Beyond substitutive dynamical systems: S-adic expansions*, RIMS Lecture note 'Kokyuroku Bessatu' **B46** (2014), 81–123.

[13] V. Berthé, H. Nakada, *On continued fraction expansions in positive characteristic: equivalence relations and some metric properties*, Expositiones Mathematicae**18** (2000), 257–284.

[14] V. Berthé, M. Rigo (Eds), Combinatorics, Automata and Number Theory, Encyclopedia Math. Appl. **135**, Cambridge Univ. Press, Cambridge, 2010.

[15] V. Berthé, M. Rigo (Eds), Combinatorics, Words and Symbolic dynamics, Encyclopedia Math. Appl. **159**, Cambridge University Press (2016).

[16] V. Berthé, L. Lhote, B. Vallée, *A probabilistic analysis of the plain multiple gcd algorithm*, Journal of Symbolic Computation **74** (2016), 425–474.

[17] V. Berthé, L. Lhote, B. Vallée, *Analysis of the Brun Gcd Algorithm*, ISSAC 2016, ACM 2016, 87-94.

[18] P. Billingsley, *Ergodic theory and information*, John Wiley & Sons Inc., New York, 1965.

[19] F. Blanchard, A. Nogueira and A. Maas (eds), *Topics in symbolic dynamics and applications*, Cambridge University Press, 2000. London Mathematical Society Lecture Note Series, Vol. **279**.

[20] B. Bollobás, *Random graphs*, 2nd edn (Cambridge Studies in Advanced Mathematics), Cambridge University Press, 2001.

[21] W. Bosma, K. Dajani, and C. Kraaikamp, *Entropy quotients and correct digits in number-theoretic expansions*, Dynamics & stochastics, IMS Lecture Notes Monogr. Ser., **48** (2006), 176–188.

[22] V. E. Brimkov, D. Coeurjolly, and R. Klette, *Digital planarity - a review*, Discrete Applied Mathematics **155** (2007), 468–495.

[23] J. Buzzi, `https://jbuzzi.wordpress.com/2013/10/18/les-surfaces-a-courbures-opposees-et-leurs-lignes-geodesiques-jacques-hadamard-1898/`.

[24] G. H. Choe, *Computational ergodic theory*, Algorithms and Computation in Mathematics, **13**, Springer-Verlag, Berlin, 2005.

[25] R. M. Corless, *Continued fractions and chaos*, Amer. Math. Monthly **99** (1992), 203–215.

[26] R. M. Corless, *What good are numerical simulations of chaotic dynamical systems?*, Comput. Math. Appl. **28** (1994), 107–121.

[27] R. M. Corless, G. W. Frank, and J. G. Monroe, Chaos and continued fractions, Phys. D **46** (1990), 241–253.

[28] I. P. Cornfeld, S. V. Fomin and Y. G. Sinaĭ, *Ergodic theory*, Springer-Verlag, New York, 1982.

[29] E. M. Coven and G. A. Hedlund, *Sequences with minimal block growth*, Math. Systems Theory **7** (1973), 138–153.

[30] K. Dajani, A. Fieldsteel, *Equipartition of interval partitions and an application to number theory*, Proc. Amer. Math. Soc. **129** (2001), 3453–3460

[31] K. Dajani and C. Kraaikamp. *Ergodic Theory of Numbers*, The Math. Association of America, 2002.

[32] R. L. Devaney, *An introduction to chaotic dynamical systems*, Addison-Wesley Studies in Nonlinearity, Redwood City, CA, 1989.

[33] Th. Fernique, *Generation and recognition of digital planes using multi-dimensional continued fractions*, Pattern Recognition **42** (2009), 2229–2238.

[34] P. Flajolet, A. M. Odlyzko, *Random Mapping Statistics*, EUROCRYPT'89, Lecture Notes Comput. Sci. **434** (1990), 329–354.

[35] P. Flajolet, B. Vallée, *Continued fractions, comparison algorithms, and fine structure constants*, CMS Conf. Proc., **27**, 53–82, Amer. Math. Soc., Providence, RI, 2000.

[36] P. Flajolet, B. Vallée, *Continued fraction algorithms, functional operators, and structure constants*, Theoret. Comput. Sci., **194** (1998), 1–34.

[37] N. Pytheas Fogg. *Substitutions in dynamics, arithmetics and combinatorics*, volume **1794** of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 2002. Edited by V. Berthé, S. Ferenczi, C. Mauduit and A. Siegel.

[38] Ch. Frougny. Numeration systems, volume 90 of Encyclopedia of Mathematics and its Applications, chapter 7, pages 230–268. Cambridge University Press, 2002.

[39] Ch. Frougny, J. Sakarovitch, Number representation and finite automata, volume **135** of Encyclopedia of Mathematics and its Applications, chapter 2, Cambridge University Press, 2010, 34–107.

[40] P. Góra, A. Boyarsky, *Why computers like Lebesgue measure*, Comput. Math. Appl. **16** (1988), 321–329.

[41] P. Góra, Paweł, A. Boyarsky, I. Md. Shafiqul and W. Bahsoun, *Absolutely continuous invariant measures that cannot be observed experimentally*, SIAM J. Appl. Dyn. Syst., **5** (2006), 84–90.

[42] P.-A. Guihéneuf, *Gare aux erreurs d'arrondi!* `http://images.math.cnrs.fr/Gare-aux-erreurs-d-arrondi.html`

[43] P.-A. Guihéneuf, *Dynamical properties of spatial discretizations of a generic homeomorphism*, Ergodic Theory Dynam. Systems **35** (2015), 1474–1523.

[44] J. Hadamard, *Les surfaces à courbures opposées et leurs lignes géodésiques*, Journal de Mathématiques pures et appliquées 5ème série, tome 4 (1898), 27–74.

[45] G. H. Hardy and E. M. Wright, An introduction to the theory of numbers, Oxford Science Publications, 1979.

[46] A. Katok and B. Hasselblatt, *Introduction to the modern theory of dynamical systems*, Cambridge University Press, Cambridge, 1995.

[47] H. Kesten *On a conjecture of Erdös and Szüsz related to uniform distribution mod* 1, Acta Arith. **12** (1966), 193–212.

[48] J. Kellendonk, D. Lenz, J. Savinien, Mathematics of aperiodic order, Progr. Math., **309**, Birkhuser/Springer, Basel, 2015.

[49] A. Y. Khintchine, Continued fractions, Translated by Peter Wynn, P. Noordhoff Ltd., Groningen, 1963.

[50] B. P. Kitchens, *Symbolic dynamics. One-sided, two-sided and countable state Markov shifts*, Universitext. Springer-Verlag, Berlin, 1998.

[51] D. E Knuth, *The Art of Computer Programming. Volume 2: Seminumerical Algorithms*, Addison-Wesley, 1998.

[52] R. Klette and A. Rosenfeld. *Digital straightness-a review.* Discrete Applied Mathematics **139** (2004), 197–230.

[53] B. Li, J. Wu, *Beta-expansion and continued fraction expansion over formal Laurent series*, Finite Fields Appl. **14** (2008), 635–647.

[54] B. Li, J. Wu, Beta-expansion and continued fraction expansion, J. Math. Anal. Appl.**339** (2008), 1322–1331.

[55] D. Lind, B. Marcus, *An introduction to symbolic dynamics and coding*, Cambridge University Press, Cambridge, 1995.

[56] G. Lochs, *Vergleich der Genauigkeit von Dezimalbruch und Kettenbruch*, Abh. Math. Sem. Univ. Hamburg **27** (1964), 142–144.

[57] G. Lochs, *Die ersten* 968 *Kettenbruchnenner von* π, Monatsh. Math. **67** (1963), 311–316.

[58] L. Lhote, B. Vallée, *Gaussian laws for the main parameters of the Euclid algorithms*, Algorithmica, **50** (2008), 497–554.

[59] M. Lothaire, *Combinatorics on words*, Cambridge University Press, Cambridge, 1997. Second ed.

[60] M. Lothaire. *Algebraic combinatorics on words*, volume 90 of *Encyclopedia of Mathematics and its Applications*, Cambridge University Press, 2002.

[61] T. Miernowski, *Discrtisations des homomorphismes du cercle*, Ergodic Theory Dynam. Systems **26** (2006), 1867–1903.

[62] H. M. Morse, *Recurrent geodesics on a surface of negative curvature*, Trans. Amer. Math. Soc. **22** (1921), 84–100.

[63] M. Morse, G. A. Hedlund, *Symbolic Dynamics*, Amer. J. Math. **60** (1938), 815–866.

[64] M. Morse, G. A. Hedlund, *Symbolic dynamics II. Sturmian trajectories*, Amer. J. Math. **62** (1940), 1–42.

[65] H. Niederreiter, *Continued fractions for formal power series, pseudorandom numbers, and linear complexity,* Contributions to general algebra, **5** , 221–233, Hölder-Pichler-Tempsky, Vienna (1987).

[66] H. Niederreiter, *Low-discrepancy sequences and non-Archimedean Diophantine approximations*, Studia. Sci. Math. Hungar. **30** (1995), 111–122.

[67] H. Niederreiter, *Sequences with almost perfect linear complexity profile*, in “Advances in Cryptology: Proc. EUROCRYPT’87” , Springer, Berlin (1988), 37–51

[68] W. Parry, and M. Pollicott, *Zeta functions and the periodic orbit structure of hyperbolic dynamics*, Astérisque **187–188** (1990).

[69] K. Petersen, *Ergodic theory*, Cambridge University Press, Cambridge, 1989.

[70] S. Y. Pilyugin, *Shadowing in dynamical systems*, Lecture Notes in Mathematics **1706**, Berlin, Springer-Verlag, 1999.

[71] M. Pollicott, *Distribution of closed geodesics on the modular surface and quadratic irrationals*, Bull. Soc. Math. France **114** (1986), 431–446.

[72] M. Queffélec, *Substitution Dynamical Systems. Spectral Analysis*, Lecture Notes in Math. **1294**, Springer-Verlag (2010).

[73] A. Rényi, *Representations for real numbers and their ergodic properties*, Acta Math. Acad. Sci. Hungar.**8** (1957), 477–493.

[74] N. Sidorov, *Arithmetic dynamics*, in S. Bezuglyi et al., editor, Topics in dynamics and ergodic theory, volume **310** of Lond. Math. Soc. Lect. Note Ser., pages 145–189. Cambridge University Press, 2003.

[75] A. Thue, Selected mathematical papers, Universitetsforlaget, Oslo, 1977.

[76] B. Vallée, *Euclidean dynamics*, Discrete Contin. Dyn. Syst. **15** (2006), 281–352.

[77] I. Fagnot, L. Vuillon, *Generalized balances in Sturmian words*, Discrete Appl. Math. **121** (2002), 83–101.

[78] P. Walters, *An introduction to ergodic theory*, Springer-Verlag, New York, 1982.