A CONSTRUCTIVE BOREL-CANTELLI LEMMA. CONSTRUCTING ORBITS WITH REQUIRED STATISTICAL PROPERTIES.

STEFANO GALATOLO, MATHIEU HOYRUP, AND CRISTÓBAL ROJAS

Abstract. In the general context of computable metric spaces and computable measures we prove a kind of constructive Borel-Cantelli lemma: given a sequence (constructive in some way) of sets A_i with effectively summable measures, there are computable points which are not contained in infinitely many A_i.

As a consequence of this we obtain the existence of computable points which follow the *typical statistical behavior* of a dynamical system (they satisfy the Birkhoff theorem) for a large class of systems, having computable invariant measure and a certain "logarithmic" speed of convergence of Birkhoff averages over Lipschitz observables. This is applied to uniformly hyperbolic systems, piecewise expanding maps, systems on the interval with an indifferent fixed point and it directly implies the existence of computable numbers which are normal with respect to any base.

Contents

Date: 26 septembre 2008.
PARTLY SUPPORTED BY ANR GRANT 05 2452 260 OX

1. Introduction

Many results in mathematics ensure the existence of points satisfying a given property P by estimating the measure of P and proving that it is positive. In general this approach is not constructive and does not give an effective way to construct points satisfying the given property.

A key lemma in this kind of techniques is the well-known Borel-Cantelli one:
Borel-Cantelli Lemma. *Let* $\{A_n\}$ *be a sequence of subsets in a probability space* (X, μ)*. If* $\sum \mu(A_n) < \infty$*, then* $\mu(\limsup A_n) = 0$*, that is, the set of points which are contained in infinitely many* A_n *has zero measure.*

Under these conditions, $X - \limsup A_n$ is a full measure set and hence it contains "many" points of X. In this paper we give a general method to construct points in this set. This method will be applied to some nontrivial problems, as constructing numbers which are normal in every base and typical trajectories of dynamical systems.

To face this problem we will put ourself in the framework of computable metric spaces. Let us introduce and motivate this concept. It is well known that the state of a physical system can be *known* only up to some finite precision (because of measuring errors, thermal shaking, quantum phenomena, long range interactions etc...). From a mathematical point of view this knowledge is represented by a ball with positive radius in the metric space of all possible configurations of the system.

In practice, the knowledge of the state of the system up to some finite precision can be described by a sentence like "the position of the point in the phase space at time 3 is $x(3) = 0.322 \pm 0.001$". What is important here is that it admits a *finite description* (a finite string of characters).

This finite string of characters, can then be elaborated to estimate, for example the position or the distance of the system's status at time 3 with respect to other points of the space.

This kind of identification

$$Strings \leftrightarrow [Points, Geometrical\ objects]$$

if often implicit, and considered to be obvious but it underlies the concept of Computable Metric Space.

A Computable Metric Space is a metric space where a dense countable set (which will be called the set of ideal points) is identified with a set of finite strings, in a way that the distance between points in this set can be computed up to any given approximation by an algorithm having the corresponding strings as an input (see section 2.2 for precise definitions).

For example in $\mathbb{R}$ the set $\mathbb{Q}$ can be identified with the strings "p over q" in a way that the distance between rationals can be obviously calculated by an algorithm having the strings as input. We remark that if $\mathbb{R}$ is considered as a computable metric space, then beyond $\mathbb{Q}$ there are many other points which admit finite descriptions, for example π or $\sqrt{2}$ are not rationals but they can be approximated at any given precision by an algorithm, hence in some sense this points too can be identified to finite strings: π for example can be identified with the finite program which approximates it by rationals at any given precision. This set of points is called the set of *computable* real numbers (they were introduced by Turing in [Tur36]). The concept of computable point can be easily generalized to any computable metric space. Coming back to our main question, now the problem we face is the following: Given some property P about points of X (or equivalently a subset of X), can this property be observed with a computer? That is, does there exist computable points satisfying this property?

For instance, given a (non atomic) probability measure μ, let P be a subset of X of probability one: a point chosen "at random" will almost surely belong to P. But, as the set of computable points have null measure (is a countable set) the full measure of P induces *a priori* nothing upon its computable part (i.e. the set of computable points belonging to P).

We will give some results which give a positive answer to this question when P is constructed by a Borel-Cantelli technique. Let us illustrate this (for a precise statement see theorem 1):

Theorem A. *Let us consider a sequence of closed sets $(A_n)_{n\in\mathbb{N}}$ (with some effectivity condition, see definition 4) such that $\sum \mu(A_n) < \infty$ in an effective way (see Def. 10).*

If the measure μ is computable (Def. 7) then there are computable points outside $\limsup A_n$, that is lying in A_n's only finitely many times.

Computable absolutely normal numbers. As an example, a classical question where this kind of tool can be naturally applied is the normality: given a fixed enumeration base b of real numbers it it quite easy to prove that the set of b-normal numbers (the numbers where all the digits $\{0, ..., b-1\}$ appear with the same frequency) has Lebesgue-measure one. Can we find computable normal numbers? The construction proposed by Champernowne [Cha33] happens to be algorithmic, so it gives a positive answer to the question.

A natural and much more difficult problem is to construct numbers which are normal in *every* base (see sec. 4.2 for some historical comments on the problem). In section 4.2 the existence of computable absolutely normal numbers will be obtained as a quite simple corollary of Theorem A.

Computable points having typical statistical behavior. The above result on normal numbers is a particular case of the construction of computable points which follows the typical statistical behavior of a dynamical system. We will need the notion of computable dynamical systems, let us introduce it.

The notion of algorithm and computable function can be extended to functions between computable metric spaces (Def. 6). This allows to consider computable dynamical systems over metric spaces (systems whose dynamics is generated by the iteration of a computable function), and computable observables. With these definitions, all systems which can be effectively described (and used in simulations) are computable.

Computable points (as described above) are a very small invariant set, compared to the whole space. By this reason, a computable point rarely can be expected to behave as a typical point of the space and give rise to a typical statistical behavior of the dynamics. Here, "typical" behavior means a behavior which is attained for a full measure set of initial conditions. Nevertheless computable points are the only points we can use when we perform a simulation or some explicit computation on a computer.

A number of theoretical questions arise naturally from all these facts. Due to the importance of the general forecasting-simulation problem these questions also have a practical importance.

Problem 1. *Since simulations can only start with computable initial conditions, given some typical statistical behavior of a dynamical system, is there some computable initial condition realizing this behavior? how to choose such points?*

Such points could be called *pseudorandom* points. Meaningful simulations, showing typical behaviors of the dynamics can be performed if computable, pseudorandom initial conditions exist[1]. A somewhat similar problem has already been investigated in [KST94] in the setting of symbolic dynamics. They consider recursive discretisations of the system (that is a subset of computable points) and look for conditions to ensure that a *finite observer* is unable to distinguish the motion on the recursive discretisation from the original system.

In our framework, a first topological result is the following: if the system is computable and has at least a dense orbit, then there is a computable point having a dense orbit (see Thm. 3).

From the statistical point of view we can use the above Theorem A to prove the following second main result which we summarize informally below (see Thm.s 2 and 5 for precise statements).

Theorem B. *If* (X, μ, T) *is a computable dynamical system and*

(1) μ *is a computable invariant ergodic measure.*
(2) *The system* (X, T, μ) *is* $\ln^2$*-ergodic (see definition 15) for observables in some suitable functions space.*

Then there exist computable points x *for which it holds:*

$$\lim_{n\to\infty} \frac{f(x) + f(T(x)) + \ldots + f(T^{n-1}(x))}{n} = \int f \, \mathrm{d}\mu \tag{1.1}$$

for any continuous function $f : X \to \mathbb{R}$ *with compact support.*

The above theorem states that in such systems there are computable points whose time average equals the space average for any such observable on X, hence providing a set of computable points which from the statistical point of view behave as the typical points of (X, μ) in the Birkhoff pointwise ergodic theorem.

We remark that the approach taken in [KST94] is quite different, in the sense that they give sufficient conditions (in terms of Kolmogorov complexity) for a subset of computable points (a recursive discretisation) which ensure that this set satisfies a kind of finite ergodic theorem (a much weaker property than 1.1) but give no

[1]It is widely believed that computer simulations produce correct ergodic behaviour. The evidence is mostly heuristic. Most arguments are based on the various "shadowing" results(see e.g. [HK95] chapter 18). In this kind of approach (different from our), it is possible to prove that in a suitable system, any "pseudo" -trajectory, as the ones which are obtained in simulations with some computation error is near to a real trajectory of the system.

So we know that what we see in a simulation is near to some real trajectory (even if we do not know if the trajectory is typical in some sense). The main limit of this approach is however that shadowing results hold only in particular systems, having some uniform hyperbolicity, while many physically interesting systems are not like this.

We recall that in our approach we consider real trajectories instead of "pseudo" ones and we ask if there is some computable point which behaves as a typical point of the space.

method to construct such computable points (because these conditions cannot be verified in a constructive way).

To apply theorem B to concrete systems the main difficulty is to verify the points 1) and 2). In section 5 we show that these are verified for the SRB invariant measure (the natural invariant measure to be considered in this cases) in some classes of interesting systems as uniformly hyperbolic systems, piecewise expanding maps and interval maps with an indifferent fixed point.

The way we handle computability on continuous spaces is largely inspired by representation theory (see [Wei00]). However, the main goal of that theory is to study, in general topological spaces, the way computability notions depend on the chosen representation. Since we focus only on computable metric spaces we do not use representation theory in its general setting but instead present computability notions in a self-contained way, and hopefully accessible to non-specialists.

2. Computability

The starting point of recursion theory was to give a mathematical definition making precise the intuitive notions of *algorithmic* or *effective procedure* on symbolic objects. Every mathematician has a more or less clear intuition of what can be computed by algorithms: the multiplication of natural numbers, the formal derivation of polynomials are simple examples.

Several very different formalizations have been independently proposed (by Church, Kleene, Turing, Post, Markov...) in the 30's, and have proved to be equivalent: they compute the same functions from $\mathbb{N}$ to $\mathbb{N}$. This class of functions is now called the class of *recursive functions*. As an algorithm is allowed to run forever on an input, these functions may be *partial*, i.e not defined everywhere. The *domain* of a recursive function is the set of inputs on which the algorithm eventually halts. A recursive function whose domain is $\mathbb{N}$ is said to be *total*.

We now recall an important concept from recursion theory. A set $E \subseteq \mathbb{N}$ is called ***recursively enumerable (r.e.)*** if there is a (partial or total) recursive function $\varphi : \mathbb{N} \to \mathbb{N}$ enumerating E, that is $E = \{\varphi(n) : n \in \mathbb{N}\}$. If $E \neq \emptyset$, ϕ can be effectively converted into a total recursive function ψ which enumerates the same set E. We recall a useful characterization of r.e. sets: a set $E \subseteq \mathbb{N}$ is said to be ***semi-decidable*** if there is a recursive function $\varphi : \mathbb{N} \to \mathbb{N}$ whose domain is E, that is $\varphi(n)$ halts if and only if $n \in E$. A set is r.e. if and only if it is semi-decidable, and the corresponding recursive functions can be effectively converted one another. We will freely use this equivalence, using in each particular situation the most adapted characterization.

2.1. **Algorithms and uniform algorithms.** Strictly speaking, recursive functions only work on natural numbers, but this can be extended to the objects (thought as "finite" objects) of any countable set, once a numbering of its elements has been chosen. We will use the word *algorithm* instead of *recursive function* when the inputs or outputs are interpreted as finite objects. The operative power of algorithms on the objects of such a numbered set obviously depends on what can be effectively recovered from their numbers.

More precisely, let X and Y be such numbered sets such that the numbering of X is injective (it is then a bijection between $\mathbb{N}$ and X). Then any *recursive function* $\varphi : \mathbb{N} \to \mathbb{N}$ induces an *algorithm* $\mathcal{A} : X \to Y$. The particular case $X = \mathbb{N}$ will be much used.

For instance, the set $\mathbb{Q}$ of rational numbers can be injectively numbered $\mathbb{Q} = \{q_0, q_1, \ldots\}$ in an *effective* way: the number i of a rational a/b can be computed from a and b, and vice versa. We fix such a numbering: from now and beyond q_i will designate the rational number which has number i.

Now, let us consider a computability notion in the real number set, here for a number to be computable means that there is an algorithm which can approximate the number up to any precision. This notion was introduced by Turing in [Tur36].

Let x be a real number and define $\mathbb{Q}^<(x) := \{i \in \mathbb{N} : q_i < x\}$.

Definition 1. *We say that:*

- x *is* **lower semi-computable** *if the set* $\mathbb{Q}^<(x)$ *is r.e.*
- x *is* **upper semi-computable** *if the set* $\mathbb{Q}^<(-x)$ *is r.e.*
- x *is* **computable** *if it is lower and upper semi-computable.*

Equivalently, a real number is computable if and only if there exists an algorithmic enumeration of a sequence of rational numbers converging exponentially fast to x. That is:

Proposition 1. *A real number is* **computable** *if there is an algorithm* $\mathcal{A} : \mathbb{N} \to \mathbb{Q}$ *such that* $|\mathcal{A}(n) - x| \leq 2^{-n}$ *for all* n.

Uniformity.

Algorithms can be used to define computability notions on many classes of mathematical objects. The definition of computability notions will be particular to a class of objects, but they will always follow the following scheme:

An object O is ***computable*** if there is an
algorithm $\mathcal{A} :\to Y$ which computes O in some way.

Each computability notion comes with a uniform version. Let $(O_i)_{i\in\mathbb{N}}$ be a sequence of computable objects:

O_i is computable ***uniformly in i*** if there is an algorithm
$\mathcal{A} : \mathbb{N} \times X \to Y$ such that for all i, $\mathcal{A}_i = \mathcal{A}(i, .) : X \to Y$ computes O_i.

For instance, the elements of a sequence of real numbers $(x_i)_{i\in\mathbb{N}}$ are uniformly computable if there is a algorithm $\mathcal{A} : \mathbb{N} \times \mathbb{N} \to \mathbb{Q}$ such that $|\mathcal{A}(i, n) - x_i| \leq 2^{-n}$ for all i, n.

In each particular case, the computability notion may take a particular name: computable, constructive, effective, r.e., etc. so the term "computable" used above shall be replaced.

2.2. **Computable metric spaces.** A computable metric space is a metric space with an additional structure allowing to interpret input and output of algorithms as points of the metric space (for an introduction to this concept see [Wei00]). This is done in the following way: there is a dense subset (called ideal points) such that each point of the set is identified with a natural number. The choice of this set is compatible with the metric, in the sense that the distance between two such points is computable up to any precision by an algorithm getting the names of the points as input. Using this simple assumptions many constructions on metric spaces can be implemented by algorithms.

Definition 2. *A* **computable metric space** *(CMS) is a triple* $\mathcal{X} = (X, d, S)$, *where*

(i) (X, d) *is a separable metric space.*

(ii) $S = \{s_i\}_{i\in\mathbb{N}}$ *is a countable set of elements from* X *(called* **ideal points***) which is dense in* (X, d).

(iii) *The distances between ideal points* $d(s_i, s_j)$ *are all computable, uniformly in* i, j *(there is an algorithm that gets the names of two points and an allowed error as an input and outputs the distance between two points up to the given approximation).*

S is a numbered set, and the information that can be recovered from the numbers of ideal points is their mutual distances. Without loss of generality, we will suppose the numbering of S to be injective: it can always be made injective in an effective way.

We say that in a metric space (X, d), a sequence of points $(x_n)_{n\in\mathbb{N}}$ converges ***fast*** to a point x if $d(x_n, x) \leq 2^{-n}$ for all n.

Definition 3. *A point* $x \in X$ *is said to be* **computable** *if there is an algorithm* $\mathcal{A} : \mathbb{N} \to S$ *such that* $(\mathcal{A}(n))_{n\in\mathbb{N}}$ *converges fast to* x.

We define the set of ***ideal balls*** to be $\mathcal{B} := \{B(s_i, q_j) : s_i \in S, q_j \in \mathbb{Q}_{>0}\}$. We fix a numbering $\mathcal{B} = \{B_0, B_1, \dots\}$ which makes the number of a ball effectively computable from its center and radius and vice versa (this numbering may not be injective). $\mathcal{B}$ is a countable basis of the topology.

Definition 4 (Constructive open sets)**.** *We say that an open set* U *is* **constructive** *if there is an algorithm* $\mathcal{A} : \mathbb{N} \to \mathcal{B}$ *such that* $U = \bigcup_n \mathcal{A}(n)$.

Observe that an algorithm which diverges on each input n enumerates the empty set, which is then a constructive open set. Sequences of uniformly constructive open sets are naturally defined.

Example 1. *We give some example of constructive open sets:*

- *The whole space* X *is constructive open.*
- *Every finite union or intersection of ideal balls* $\{B_{n_1}, \dots, B_{n_k}\}$ *is a constructive open set, uniformly in* $\langle n_1, \dots, n_k\rangle$.
- *If* $(U_i)_{i\in\mathbb{N}}$ *is a sequence of uniformly constructive open sets, then* $\bigcup_i U_i$ *is a constructive open set.*

Remark 1. *If* U *is constructively open, belonging to* U *for an ideal point is semi-decidable: there is an algorithm* $\mathcal{A} : S \to \mathbb{N}$ *which halts only on ideal points belonging to* U*. Equivalently, the set of ideal points lying in* U *is r.e. (as a subset of* S*): there is an algorithm* $\mathcal{A} : \mathbb{N} \to S$ *enumerating* $S \cap U$*. Hence* $(U, S \cap U, d)$ *has a natural structure of computable metric space.*

Definition 5 (Constructive G_δ-set)**.** *A* **constructive G_δ-set** *is an intersection of a sequence of uniformly constructive open sets.*

Obviously, an intersection of uniformly constructive G_δ-sets is also a constructive G_δ-set.

Let $(X, S_X = \{s_1^X, s_2^X, ...\}, d_X)$ and $(Y, S_Y = \{s_1^Y, s_2^Y, ...\}, d_Y)$ be computable metric spaces. Let also B_i^X and B_i^Y be enumerations of the ideal balls in X and Y. A computable function $X \to Y$ is a function whose behavior can be computed by an algorithm up to any precision. For this it is sufficient that the preimage of each ideal ball is calculated with any precision.

Definition 6 (Computable Functions)**.** *A function $T : X \to Y$ is* **computable** *if $T^{-1}(B_i^Y)$ is a constructive open set, uniformly in i. That is, there is an algorithm $\mathcal{A} : \mathbb{N} \times \mathbb{N} \to \mathcal{B}^X$ such that $T^{-1}(B_i^Y) = \bigcup_n \mathcal{A}(i, n)$ for all i.*

A function $T : X \to Y$ is **computable on** *$D \subseteq X$ if there are uniformly constructive open sets U_i such that $T^{-1}(B_i^Y) \cap D = U_i \cap D$.*

Remark 2. *We remark that if T is computable then all $T(s_i^X)$ are computable uniformly in i: there is an algorithm $\mathcal{A} : \mathbb{N} \times \mathbb{N} \to S^Y$ such that $(\mathcal{A}(i, n))_{n \in \mathbb{N}}$ converges fast to $T(s_i^X)$ for all i.*

The algorithm just semi-decides for each ideal ball in Y if s_i^X is contained in its preimage. The process will stop for each ideal ball that contains $T(s_i^X)$, which allows to extract a sequence of ideal points of Y which converges fast to $T(s_i^X)$.

The following is a criteria to check computability of a large class of uniformly continuous functions.

Remark 3. *If T satisfies the following:*

- *all $T(s_i^X)$ are computable points, uniformly in i,*
- *T is recursively uniformly continuous: there is an algorithm $\mathcal{A} : \mathbb{Q}_{>0} \to \mathbb{Q}_{>0}$ such that for all $\epsilon \in \mathbb{Q}_{>0}$, $d(x, x') < \mathcal{A}(\epsilon) \Rightarrow d(T(x), T(x')) < \epsilon$,*

then T is computable.

Proof. Let $E = \{(i, j) \in \mathbb{N}^2 : d(T(s_i^X), s) + q_j < r\}$: this is a r.e. subset of $\mathbb{N}$ (uniformly in s, r) by the first condition. Then one can show that $T^{-1}(B(s, r)) = \bigcup_{(i,j) \in E} B(s_i, A(q_j))$. □

2.3. **Computable measures.** When X is a computable metric space, the space of probability measures over X, denoted by $\mathcal{M}(X)$, can be endowed with a structure of computable metric space. Then a computable measure can be defined as a computable point in $\mathcal{M}(X)$.

Let $\mathcal{X} = (X, d, S)$ be a computable metric space. Let us consider the space $\mathcal{M}(X)$ of measures over X endowed with weak topology, that is:

$$\mu_n \to \mu \text{ iff } \mu_n f \to \mu f \text{ for all real continuous bounded } f \tag{2.1}$$

where μf stands for $\int f \, \mathrm{d}\mu$.

If X is separable and complete, then $\mathcal{M}(X)$ is separable and complete. Let $D \subset \mathcal{M}(X)$ be the set of those probability measures that are concentrated in finitely many points of S and assign rational values to them. It can be shown that this is a dense subset ([Bil68]). Let $\mu_{n_1,..,n_k,m_1,..,m_k}$ denote the measure concentrated over the finite set $\{s_{n_1}, \ldots, s_{n_k}\}$ with q_{m_i} the weight of s_{n_i}.

We consider Prokhorov metric ρ on $\mathcal{M}(X)$ defined by:

$$\rho(\mu, \nu) := \inf\{\epsilon \in \mathbb{R}^+ : \mu(A) \leq \nu(A^\epsilon) + \epsilon \text{ for every Borel set } A\}.$$

where $A^\epsilon = \{x : d(x, A) < \epsilon\}$.

This metric induces the weak topology on $\mathcal{M}(X)$. Furthermore, it can be shown that the triple $(\mathcal{M}(X), D, \rho)$ is a computable metric space (see [Gác05], [HR07]).

Definition 7. *A measure μ is computable if there is an algorithmic enumeration of a fast sequence of ideal measures $(\mu_n)_{n \in \mathbb{N}} \subset D$ converging to μ in the Prokhorov metric and hence, in the weak topology.*

We need a criteria to check that a measure is computable. Let us then introduce (following [Gác05]) a certain fixed, enumerated sequence of Lipschitz functions. Let $\mathcal{F}_0$ be the set of functions of the form:

$$g_{s,r,\epsilon} = |1 - |d(x,s) - r|^+/\epsilon|^+ \tag{2.2}$$

where $s \in S$, $r, \epsilon \in \mathbb{Q}$ and $|a|^+ = \max\{a, 0\}$.

These are Lipschitz functions equal to 1 in the ball $B(s,r)$, to 0 outside $B(s, r+\epsilon)$ and with intermediate values in between. It is easy to see that the real valued functions $g_{s_i,r_j,\epsilon_k} : X \to \mathbb{R}$ are computable, uniformly in i, j, k.

Let $\mathcal{F}$ be the smallest set of functions containing $\mathcal{F}_0$ and the constant 1, and closed under max, min and rational linear combinations. Clearly, this is also a uniform family of computable functions. We fix some enumeration $\nu_{\mathcal{F}}$ of $\mathcal{F}$ and we write g_n for $\nu_{\mathcal{F}}(n) \in \mathcal{F}$. We remark that this set is dense in the set of continuous functions with compact support.

The following lemma, proved in [Gác05], shows that the approach to define computable measures we adopted, approximating measures with measures supported on finite ideal sets is compatible with viewing the space of measures as the dual of continuous functions, i.e. a measure is computable if and only if it is a computable function : $C_b^0 \to \mathbb{R}$.

Lemma 1. *Let $\mathcal{F} = \{g_1, g_2, ...\}$ be the set introduced above. A probability measure μ is computable if and only if $\int g_i \, d\mu$ is computable uniformly in i.*

Together with the previous lemma, the following result (see [HR07]) will be all we use about computable measures:

Lemma 2. *A probability measure μ is computable if and only if the measure of finite union of ideal balls $\mu(B_{i_1} \cup \ldots \cup B_{i_k})$ is lower semi-computable, uniformly in $i_1, \ldots, i_k$.*

2.4. **Computable probability spaces.** To obtain computability results on dynamical systems, it seems obvious that some computability conditions must be required on the system. But the "good" conditions, if any, are not obvious to specify.

A computable function defined on the whole space is necessarily continuous. But a transformation or an observable need not be continuous at every point, as many interesting examples prove (piecewise-defined transformations, characteristic functions of measurable sets,...), so the requirement of being computable everywhere is too strong. In a measure-theoretical setting, the natural weaker condition is to require the function to be computable on a set of full measure. It can be proved that such a function coincides, on its domain of computability, with a function which is computable on a full-measure constructive G_δ (see [Hoy08]).

Definition 8. *A* **computable probability space** *is a pair (X, μ) where X is a computable metric space and μ a computable Borel probability measure on X.*

Let Y be a computable metric space. A function $(X, \mu) \to Y$ is **almost everywhere computable** *(a.e. computable for short) if it is computable on a constructive G_δ-set of measure one, denoted by* $\mathrm{dom} f$ *and called the* domain of computability of f.

A **morphism** *of computable probability spaces $f : (X, \mu) \to (Y, \nu)$ is a morphism of probability spaces which is a.e. computable.*

Remark 4. *A sequence of functions f_n is uniformly a.e. computable if the functions are uniformly computable on their respective domains, which are uniformly constructive G_δ-sets. Remark that in this case intersecting all the domains provides a constructive G_δ-set on which all f_n are computable. In the following we will apply this principle to the iterates $f_n = T^n$ of an a.e. computable function $T : X \to X$, which are uniformly a.e. computable.*

3. Constructive Borel-Cantelli sets

Given a space X endowed with a probability measure μ, the well known Borel Cantelli lemma states that if a sequence of sets A_k is such that $\sum \mu(A_k) < \infty$ then the set of points which belong to finitely many A_k's has full measure. In this section we show that if the A_k are given in some "constructive" way (and μ is computable) then this full measure set contains some computable points. Hence this set contains points which can effectively be constructed.

Definition 9. *A sequence of positive numbers a_i is* effectively summable *if the sequence of partial sums converges effectively: there is an algorithm $A : \mathbb{Q} \to \mathbb{N}$ such that if $A(\epsilon) = n$ then $\sum_{i \geq n} a_i \leq \epsilon$.*

Remark 5. *A computable sequence of* positive *real numbers is effectively summable if and only if its sum is a computable real number.*

For sake of simplicity, we will focus on the complements U_n of the A_n.

Definition 10. *A* constructive Borel-Cantelli sequence *is a sequence $(U_n)_{n \in \mathbb{N}}$ of uniformly constructive open sets such that the sequence $(\mu(U_n^{\mathcal{C}}))$ is effectively summable.*

The corresponding constructive Borel-Cantelli set *is $\bigcup_k \bigcap_{n \geq k} U_n$.*

The Borel-Cantelli lemma says that every Borel-Cantelli set has full-measure: we are going to see that every *constructive* Borel-Cantelli set contains a dense subset made of computable points.

Lemma 3 (Normal form lemma)**.** *Every constructive Borel-Cantelli sequence can be effectively transformed into a constructive Borel-Cantelli sequence $(U_n)_{n \in \mathbb{N}}$ giving the same Borel-Cantelli set, with $\mu(U_n^{\mathcal{C}}) < 2^{-n}$.*

Proof. consider a constructive Borel-Cantelli sequence (V_n). As $\mu(X \setminus V_n)$ is effectively summable, an increasing sequence $(n_i)_{i \geq 0}$ of integers can be computed such that for all $i, \sum_{n \geq n_i} \mu(X \setminus V_n) < 2^{-i}$.

We now gather the V_n by blocks, setting:

$$U_i := \bigcap_{n_i \leq n < n_{i+1}} V_n$$

U_i is constructively open uniformly in i, and:

$$\mu(U_i^{\mathcal{C}}) < 2^{-i} \quad \text{and} \quad \bigcup_k \bigcap_{n \geq k} V_n = \bigcup_i \bigcap_{n \geq n_i} V_n = \bigcup_i \bigcap_{j \geq i} U_j$$

□

In the sequel we will always suppose that a constructive Borel-Cantelli sequence is put in this normal form.

Proposition 2. *Every finite intersection of constructive Borel-Cantelli sets is a constructive Borel-Cantelli set.*

Proof. let (U_n) and (V_n) be two constructive Borel-Cantelli sequences in normal form. It is easy to see that:

$$\bigcup_k \bigcap_{n\geq k} U_n \cap \bigcup_k \bigcap_{n\geq k} V_n = \bigcup_k \bigcap_{n\geq k} U_n \cap V_n$$

and $\mu((U_n \cap V_n)^{\mathcal{C}}) < 2^{-n+1}$ which is effectively summable. □

As every effectivity notion, the notion of constructive Borel-Cantelli set naturally comes with its uniform version.

Proposition 3. *The intersection of any uniform family of constructive Borel-Cantelli sets contains a constructive Borel-Cantelli set.*

Proof. suppose that $R_i = \bigcup_k \bigcap_{n\geq k} U_n^i$ is in normal form. Consider a simple bijection $\varphi : \{(n,i) : 0 \leq i \leq n\} \to \mathbb{N}$ (for instance, $\varphi(n,i) = n(n+1)/2+i$) computable in the two ways and define the sequences $(V_m)_{m\in\mathbb{N}}$ and $(a_m)_{m\in\mathbb{N}}$ by $V_m = U_n^i$ and $a_m = 2^{-n}$ where $\varphi(n,i) = m$. Obviously $\mu(V_m^{\mathcal{C}}) > a_m$.

A simple calculation shows that $\sum a_m = 4$. So (V_m) is a constructive Borel-Cantelli sequence.

Fix some i. If a point is outside U_n^i for infinitely many n, it is outside V_m for infinitely many m. That is to say:

$$\bigcup_k \bigcap_{m\geq k} V_m \subseteq \bigcup_k \bigcap_{n\geq k} U_n^i = R_i$$

As it is true for every i, the constructive Borel-Cantelli set induced by $(V_m)_m$ is included in every R_i. □

3.1. **Computable points in constructive Borel-Cantelli sets.** The Borel-Cantelli lemma can be strengthened for constructive Borel-Cantelli sequences obtaining that they contain computable points.

Theorem 1. *Let X be a complete CMS and μ a computable Borel probability measure on X.*

For every constructive Borel-Cantelli set R, the set of computable points lying in R is dense in the support of μ.

In order to the prove this theorem, we need the following lemma to construct a computable point from what could be called a *shrinking sequence of constructive open sets.*

Lemma 4 (Shrinking sequence)**.** *Let X be a complete CMS. Let V_i be a sequence of non-empty uniformly constructive open sets such that $\overline{V}_{i+1} \subseteq V_i$ and* $\mathrm{diam}(V_i)$ *converges effectively to* 0*. Then $\bigcap_i V_i$ is a singleton containing a computable point.*

Proof. As V_i is non-empty there is a computable sequence of ideal points $s_i \in V_i$. This is a Cauchy sequence, which converges by completeness. Let x be its limit: it is a computable point as $\mathrm{diam}(V_i)$ converges to 0 in an effective way. Fix some i: for all $j \geq i$, $s_j \in V_j \subseteq \overline{V}_i$ so $x = \lim_{j\to\infty} s_j \in \overline{V}_i$. Hence $x \in \bigcap_i \overline{V}_i = \bigcap_i V_i$. □

Proof of theorem 1. Let $(U_n)_n$ be a constructive Borel-Cantelli sequence, in normal form ($\mu(U_n) > 1 - 2^{-n}$, see lemma 3). Let B be an ideal ball of radius $r \leq 1$ and positive measure. In B we construct a computable point which lies in $\bigcup_n \bigcap_{k \geq n} U_k$.

To do this, let $V_0 = B$ and n_0 be such that $\mu(B) > 2^{-n_0+1}$ (such an n_0 can be effectively found from B): from this we construct a sequence $(V_i)_i$ of uniformly constructive open sets and a computable increasing sequence $(n_i)_i$ of natural numbers satisfying:

(1) $\mu(V_i) + \mu(\bigcap_{k \geq n_i} U_k) > 1$,
(2) $V_i \subseteq \bigcap_{n_0 \leq k < n_i} U_k$,
(3) $\operatorname{diam}(V_i) \leq 2^{-i+1}$,
(4) $\overline{V}_{i+1} \subseteq V_i$.

The last two conditions assure that $\bigcap_i V_i$ is a computable point (lemma 4), the second condition assures that this point lies in $\bigcap_{k \geq n_0} U_k$.

Suppose V_i and n_i have been constructed.

Claim 1. *There exist $m > n_i$ and an ideal ball B' of radius 2^{-i-1} such that*

$$\mu(V_i \cap \bigcap_{n_i \leq k < m} U_k \cap B') > 2^{-m+1}. \tag{3.1}$$

We now prove of the claim: By the first condition, $\mu(V_i \cap \bigcap_{k \geq n_i} U_k) > 0$ so there exists an ideal ball B' of radius 2^{-i-1} such that $\mu(V_i \cap \bigcap_{k \geq n_i} U_k \cap B') > 0$. There is $m > n_i$ such that $\mu(V_i \cap \bigcap_{k \geq n_i} U_k \cap B') > 2^{-m+1}$, which implies the assertion, and the claim is proved.

As inequality (3.1) can be semi-decided, such an m and a B' can be effectively found. For V_{i+1}, take any finite union of balls whose closure is contained in $V_i \cap \bigcap_{n_i \leq k < m} U_k \cap B'$ and whose measure is greater than 2^{-m+1}. Put $n_{i+1} = m$. Conditions 2., 3. and 4. directly follow from the construction, condition 1. follows from $\mu(V_{i+1}) > 2^{-m+1} > 1 - \mu(\bigcap_{k \geq m} U_k)$ (the sequence is in normal form). □

The following corollary allows to apply the above criteria to a uniform infinite sequence of constructive Borel-Cantelli sets.

Corollary 1. *Let X be a complete CMS and μ a computable Borel probability measure on X.*

Given a uniform family $(R_i)_i$ of constructive Borel-Cantelli sets, the set of computable points lying in $\bigcap_i R_i$ is dense in the support of μ.

Proof. this a direct consequence of proposition 3 and theorem 1. □

We remark that, in the particular case of Cantor spaces with an uniform measure a result of this kind can also be obtained from [Sch71] since it is possible to relate Borel Cantelli sequences to Schnorr tests. This relation is developped in [GHR08] giving some new connections between Schnorr randomness and dynamical typicality.

3.1.1. *Application to convergence of random variables.* Here, (X, μ) is a computable probability space.

Definition 11. *A* **random variable** *on (X, μ) is a measurable function $f : X \to \mathbb{R}$.*

Definition 12. *Random variables* f_n **effectively converge in probability** *to* f *if for each* $\epsilon > 0$, $\mu\{x : |f_n(x) - f(x)| < \epsilon\}$ *converges effectively to* 1, *uniformly in* ϵ. *That is, there is a computable function* $n(\epsilon, \delta)$ *such that for all* $n \geq n(\epsilon, \delta)$, $\mu[|f_n - f| \geq \epsilon] < \delta$.

Definition 13. *Random variables* f_n **effectively converge almost surely** *to* f *if* $\sup_{k \geq n} |f_n - f|$ *effectively converge in probability to* 0.

Theorem 2. *Let* f_n, f *be uniformly a.e. computable random variables. If* f_n *effectively converges almost surely to* f *then the set* $\{x : f_n(x) \to f(x)\}$ *contains a constructive Borel-Cantelli set.*

In particular, the set of computable points for which the convergence holds is dense in $\mathrm{Supp}(\mu)$.

Proof. Let $D = \bigcap_n D_n$ be a constructive G_δ-set of full measure on which all f_n, f are computable. D_n are uniformly constructive open sets, and we can suppose $D_{n+1} \subseteq D_n$ (otherwise, replace D_n by $D_0 \cap \ldots \cap D_n$).

There are uniformly constructive open sets $U_n(\epsilon)$ such that $U_n(\epsilon) \cap D = [|f_n - f| < \epsilon] \cap D$. $\mu(\bigcap_{n \geq k} U_n(\epsilon))$ converges effectively to 1, uniformly in ϵ so it is possible to compute a sequence $(k_i)_i$ such that $\mu(\bigcap_{n \geq k_i} U_n(2^{-i})) > 1 - 2^{-i}$ for all i. Put $V_i = \bigcap_{k_i \leq n < k_{i+1}} U_n(2^{-i}) \cap D_i$: V_i is constructively open uniformly in i and $\mu(V_i) > 1 - 2^{-i}$. The sets V_i form a constructive Borel-Cantelli sequence, and if a point x is in the corresponding Borel-Cantelli set then $x \in D$ and there is i_0 such that $x \in V_i$ for all $i \geq i_0$, so $|f_n(x) - f(x)| < 2^{-i}$ for all $n \geq k_i, i \geq i_0$. Hence $f_n(x) \to f(x)$. $\square$

4. Pseudorandom points and dynamical systems

Let X be a metric space, let $T : X \mapsto X$ be a Borel map. Let μ be an invariant Borel measure on X, that is: $\mu(A) = \mu(T^{-1}(A))$ holds for each measurable set A. A set a A is called T-invariant if $T^{-1}(A) = A (\mathrm{mod}\ 0)$. The system (T, μ) is said to be ergodic if each T-invariant set has total or null measure. In such systems the famous Birkhoff ergodic theorem says that time averages computed along μ typical orbits coincides with space average with respect to μ. More precisely, for any $f \in L^1(X)$ and it holds

$$\lim_{n \to \infty} \frac{S_n^f(x)}{n} = \int f \, \mathrm{d}\mu, \tag{4.1}$$

for μ almost each x, where $S_n^f = f + f \circ T + \ldots + f \circ T^{n-1}$.

If a point x satisfies equation 4.1 for a certain f, then we say that x is typical with respect to the observable f.

Definition 14. *If* x *is typical w.r.t any continuous function* $f : X \to \mathbb{R}$ *with compact support, then we call it a* $\boldsymbol{\mu}$**-typical point**.

In this section we will see how the constructive Borel-Cantelli lemma can be used to prove that in a large class of interesting systems there exists computable typical points.

Let us call (X, μ, T) a ***computable ergodic system*** if (X, μ) is a computable probability space, T is an endomorphism (i.e. an a.e. computable measure-preserving transformation) and (X, μ, T) is ergodic.

Before to enter in the main theme of typical statistical behaviors let us see an easier topological result in this line. One of the features of undecomposable (topologically transitive) chaotic systems is that there are many dense orbits, the following shows that if the system is computable then there are computable dense orbits.

We remark that this result can also be obtained as a corollary of the constructive Baire theorem [YMT99].

Theorem 3. *Let $\mathcal{X}$ be a computable complete metric space and $T : X \to X$ a transformation which is computable on a dense constructive open set. If T has a dense orbit, then it has a computable one which is dense.*

In other words, there is a computable point $x \in X$ whose orbit is dense in X. Actually, the proof is an algorithm which takes an ideal ball as input and computes a transitive point lying in this ball.

Proof. $(B_i)_{i\in\mathbb{N}}$ being an enumeration of all ideal balls, define the open sets $U_i = dom(f) \cap \bigcup_n T^{-n}B_i$ which are constructive uniformly in i. By hypothesis, U_i is also dense. $\bigcap_i U_i$ is the set of transitive points. From any ideal ball $B(s_0, r_0)$ we effectively construct a computable point in $B(s_0, r_0) \cap \bigcap_i U_i$.

If $B(s_i, r_i)$ has been constructed, as U_i is dense $B(s_i, r_i) \cap U_i$ is a non-empty constructive open set, so an ideal ball $B(s, r) \subseteq B(s_i, r_i) \cap U_i$ can be effectively found (any of them can be chosen, for instance the first coming in the enumeration). We then set $B(s_{i+1}, r_{i+1}) := B(s, r/2)$.

The sequence of balls computed satisfies:

$$\overline{B}(s_{i+1}, r_{i+1}) \subseteq B(s_i, r_i) \cap U_0 \cap \ldots \cap U_i$$

As $(r_i)_{i\in\mathbb{N}}$ is a decreasing computable sequence converging to 0 and the space is complete, $(s_i)_{i\in\mathbb{N}}$ converges effectively to a computable point x. Then $\{x\} = \bigcap_i B(s_i, r_i) \subseteq \bigcap_i U_i$. □

4.1. **Computable typical points.** We will use the results from the previous section to prove that computable typical points exist for a class of dynamical systems. Each time the set of typical points is a constructive Borel-Cantelli set, theorem 2 applies.

For instance, in the case of the shift on the Cantor space with a Bernoulli measure, the Birkhoff ergodic theorem reduces to the strong law of large numbers, which proof is simpler and makes explicit use of the Borel-Canteli lemma. This is possible thanks to the independence between the random variables involved, but strict independence is actually unnecessary: the proof can be adapted whenever the correlations between the random variables decrease sufficiently fast.

Definition 15. *We say that a system (X, T, μ) is* **$\ln^2$-ergodic** *for observables in some set of functions $\mathcal{B}$ if for each $(\phi, \psi) \in \mathcal{B}^2$ there is $c_{\phi,\psi} > 0$ such that*

$$\left| \frac{1}{n} \sum_{i<n} \int \phi \circ T^i \psi \, \mathrm{d}\mu - \int \phi \, \mathrm{d}\mu \int \psi \, \mathrm{d}\mu \right| \leq \frac{c_{\phi,\psi}}{(\ln(n))^2} \qquad \textit{for all } n \geq 2.$$

Now we can state:

Theorem 4. *Let (X, T, μ) be a dynamical system which is $\ln^2$-ergodic for observables in some set $\mathcal{B}$ of bounded observables. For each $\phi \in \mathcal{B}$, the almost-sure* *convergence:*

$$\frac{1}{n}\sum_{i<n}\phi\circ T^i \to_n \int \phi \,\mathrm{d}\mu$$

is effective.

Note that for the moment, no computability assumption is needed on the system.

As announced, the proof is an adaptation of the proof of the strong law of large numbers. We first prove two lemmas.

Lemma 5. *There exists a computable sequence n_i such that:*

- $\beta_i := \frac{n_i}{n_{i+1}}$ *converge effectively to* 1*,*
- $\frac{1}{\ln(n_i)^2}$ *is effectively summable.*

Proof. For instance, take $n_i = \lceil (1+i^{-\alpha})^i \rceil$ with $0<\alpha<1/2$. □

From now on, we denote $\frac{S_n^\phi}{n}$ by f_n.

Lemma 6. *The almost-sure convergence of the subsequence f_{n_i} to $\int \phi \,\mathrm{d}\mu$ is effective.*

Proof. For $\delta > 0$, define the deviation sets:

$$A_n^\phi(\delta) = \left\{ x \in X : \left| f_n(x) - \int \phi \,\mathrm{d}\mu \right| \geq \delta \right\}.$$

By Tchebytchev inequality,

$$\delta^2 \mu(A_n^\phi(\delta)) \leq \left\| f_n - \int \phi \,\mathrm{d}\mu \right\|_{L^2}^2 .$$

Since adding a constant to ϕ does not change this quantity, without loss of generality, let us suppose that $\int \phi \,\mathrm{d}\mu = 0$. Then

$$\left\| \frac{S_n^\phi}{n} - \int \phi \,\mathrm{d}\mu \right\|_{L^2}^2 = \int \left(\frac{S_n^\phi}{n} \right)^2 \mathrm{d}\mu = \int \left(\frac{\phi + \phi\circ T + ... + \phi \circ T^{n-1}}{n} \right)^2 \mathrm{d}\mu$$

by invariance of μ this is equal to

$$\frac{1}{n^2}\int n\phi^2 \,\mathrm{d}\mu + \frac{2}{n^2}\int \big(\sum_{i<j<n} \phi\circ T^{j-i}\phi \big) \,\mathrm{d}\mu$$

hence,

$$\begin{aligned} \delta^2 \mu(A_n^\phi(\delta)) &\leq \frac{M^2}{n} + \frac{2}{n}\sum_{k<n}\int \phi\circ T^k \phi \,\mathrm{d}\mu \\ &\leq \frac{M^2}{n} + \frac{c_{\phi,\phi}}{\ln(n)^2} \end{aligned}$$

As $\frac{M^2}{n_i} + \frac{c_{\phi,\phi}}{\ln(n_i)^2}$ is effectively summable (by choice of n_i, see lemma 5) uniformly in δ, it follows that f_{n_i} converge effectively almost-surely to $\int \phi \,\mathrm{d}\mu$. □

As n_i is not dispersed too much, the almost-sure convergence of the subsequence f_{n_i} implies that of the whole sequence f_n. Actually the effectivity is also preserved. We now make this precise.

Lemma 7. *For $n_i \leq n < n_{i+1}$ and $\beta_i := \frac{n_i}{n_{i+1}}$, one has:*

$$\|f_{n_i} - f_n\|_\infty \leq 2(1-\beta_i)\,\|\phi\|_\infty . \tag{4.2}$$

Proof. Let $M = \|\phi\|_\infty$. To see this, for any k, l, β with $\beta \leq k/l \leq 1$:

$$\begin{aligned} \frac{S_k^\phi}{k} - \frac{S_l^\phi}{l} &= \left(1 - \frac{k}{l}\right)\frac{S_k^\phi}{k} - \frac{S_{l-k}^\phi \circ T^{l-k}}{l} \\ &\leq (1-\beta)M + \frac{(l-k)M}{l} = 2(1-\beta)M, \end{aligned}$$

Taking $\beta = \beta_i$ and $k = n_i$, $l = n$ first and then $k = n$, $l = n_{i+1}$ gives the result. □

Proof of theorem 4. Let $\delta, \epsilon > 0$. To prove that f_n converge effectively almost-surely, one has to compute some p (from δ and ϵ) such that $\mu(\bigcup_{n \geq p} A_n(\delta)) < \epsilon$.

As β_i converge effectively to 1, one can compute i_0 such that if $i \geq i_0$ then $\beta_i > 1 - \delta/(4M)$. Inequality 4.2 then implies

$$\bigcup_{n_i \leq n < n_{i+1}} A_n(\delta) \subseteq A_{n_i}(\delta/2).$$

Indeed if $n_i \leq n < n_{i+1}$ and $|f_{n_i}(x) - \int \phi \, \mathrm{d}\mu| < \delta/2$ then $|f_n(x) - \int \phi \, \mathrm{d}\mu| \leq |f_n(x) - f_{n_i}(x)| + |f_{n_i}(x) - \int \phi \, \mathrm{d}\mu| \leq \delta$.

As f_{n_i} converge effectively almost-surely, one can compute some j_0 such that $\mu(\bigcup_{j \geq j_0} A_{n_j}(\delta/2)) < \epsilon$. Let $p = n_k$ where $k = \max(i_0, j_0)$: $\bigcup_{n \geq p} A_n(\delta) \subseteq \bigcup_{j \geq j_0} A_{n_i}(\delta/2)$ whose measure is less than ϵ. □

Corollary 2. *Let (X, T, μ) be a* computable *dynamical system which is* $\ln^2$*-ergodic for observables in some set $\mathcal{B}$ of bounded functions and let ϕ be a a.e. computable observable in $\mathcal{B}$.*

The set of points which are typical w.r.t ϕ contains a constructive Borel-Cantelli set. In particular, it contains computable points.

Proof. Apply theorem 2 to the sequence of uniformly a.e. computable functions $f_n = \frac{S_n^\phi}{n}$ which converge effectively almost-surely by theorem 4. □

Remark 6. *In the proof of thm 4 we see that the constructive Borel-Cantelli set depends in an effective way on $\|\phi\|_\infty$ and $c_{\phi,\phi}$. This gives the possibility to operate in a way to apply Prop. 3 and Cor. 1 to find a constructive Borel Cantelli set and computable points contained in the set of points typical with respect to a uniform family ϕ_i, T_i.*

By the above remark, to construct μ-typical points (see definition 14) using the above mentioned results, the following conditions are sufficient:

Theorem 5. *If a computable system is $\ln^2$-ergodic for observables in $\mathcal{F} = \{g_1, g_2, \dots\}$ (this set was defined in section 2.3) and the associated constants c_{g_i} (see definition 16) can be estimated uniformly in i (there is an algorithm $A : \mathbb{N} \to \mathbb{Q}$ such that $A(i) \geq c_{g_i}$) then it has a set of computable μ-typical points which is dense in the support of μ.*

Proof. We remark that $\mathcal{F}$ is dense in the set of continuous functions on X with compact support (with the sup norm) hence a computable point which is typical for each g_i is μ-typical. Such points can be found by applying theorem 2 for each g_i and using proposition 3 as explained in remark 6. $\square$

4.1.1. $\ln^2$-*mixing.* We will apply this to systems having a stronger property: they are *mixing*, with logarithmical speed. More precisely, this can be quantified using the ***correlation functions***:

$$C_n(\phi,\psi) = \left|\int \phi\circ T^n \psi \, \mathrm{d}\mu - \int \phi \, \mathrm{d}\mu \int \psi \, \mathrm{d}\mu\right|$$

which measures the dependence between observation through ϕ and ψ at times $n \gg 1$ and 0 respectively (possibly with $\psi = \phi$). Note that $C_n(\phi,\psi) = 0$ corresponds, in probabilistic terms, to $\phi\circ T^n$ and ψ being independent random variables.

Definition 16. *We say that a system (X,T,μ) has* **$\ln^2$-decay of correlations** *for observables in some set of functions $\mathcal{B}$ if for each $(\phi,\psi)\in\mathcal{B}^2$ there is $c_{\phi,\psi} > 0$ such that*

$$C_n(\phi,\psi) \le \frac{c_{\phi,\psi}}{(\ln(n))^2} \qquad \text{for all } n \ge 2.$$

Lemma 8. *If a system has $\ln^2$-decay of correlation for observables in $\mathcal{B}$ then it is $\ln^2$-ergodic for observables in $\mathcal{B}$. The ergodicity constants depend in an effective way on the mixing constants.*

Proof. We first prove that for all $n \ge 2$,

$$\sum_{k=2}^{n} \frac{1}{\ln(k)^2} \le \frac{2n}{\ln(n)^2} + 4 \tag{4.3}$$

For $n \ge 56$,

$$\begin{aligned}
\sum_{k=56}^{n} \frac{1}{\ln(k)^2} &\le \int_{x=55}^{n} \frac{\mathrm{d}x}{\ln(x)^2} \\
&\le \int_{x=55}^{n} 2\left(\frac{1}{\ln(x)^2} - \frac{2}{\ln(x)^3}\right)\mathrm{d}x \qquad (\text{as } 55 \ge \ln(4)) \\
&= \frac{2n}{\ln(n)^2} - \frac{110}{\ln(55)^2}
\end{aligned}$$

which, combined with $\sum_{k=2}^{55} \frac{1}{\ln(k)^2} \le 10$ and $\frac{110}{\ln(55)^2} \ge 6$, gives inequality (4.3).

Finally, for $n \ge 2$,

$$\begin{aligned}
\left|\frac{1}{n}\sum_{i<n}\int \phi\circ T^i\psi\,\mathrm{d}\mu - \int\phi\,\mathrm{d}\mu\int\psi\,\mathrm{d}\mu\right| &\le \frac{1}{n}\sum_{i<n} C_i(\phi,\psi) \\
&\le \frac{2c_{\phi,\psi}}{\ln(n)^2} + \frac{4c_{\phi,\psi}}{n} \\
&\le \frac{6c_{\phi,\psi}}{\ln(n)^2}
\end{aligned}$$

$\square$

4.2. **Application: computable absolutely normal numbers.** An absolutely normal (or just normal) number is, roughly speaking, a real number whose digits (in every base) show a uniform distribution, with all digits being equally likely, all pairs of digits equally likely, all triplets of digits equally likely, etc.

While a general, probabilistic proof can be given that *almost all* numbers are normal, this proof is not constructive and only very few concrete numbers have been shown to be normal. It is for instance widely believed that the numbers $\sqrt{2}$, π and e are normal, but a proof remains elusive. The first example of an absolutely normal number was given by Sierpinski in 1916, twenty years before the concept of computability was formalized. Its construction is quite complicate and is a priori unclear whether his number is computable or not. In [BF02] a recursive reformulation of Sierpinski's construction (equally complicate) was given, furnishing a computable absolutely normal number.

As an application of theorem 2 we give a simple proof that computable absolutely normal numbers are dense in $[0,1]$.

Let b be an integer ≥ 2, and X_b the space of infinite sequences on the alphabet $\Sigma_b = \{0,\dots,b-1\}$. Let $T=\sigma$ be the shift transformation on X_b, and λ be the uniform measure. A real number $r \in [0,1]$ is said to be absolutely normal if for all $b \geq 2$, its b-ary expansion $r_b \in X_b$ satisfies:

$$\lim_{n\to\infty} \frac{1}{n}\sum_{i=0}^{n-1} 1_{[w]} \circ \sigma^i(r_b) = \frac{1}{b^{|w|}} \qquad \text{for all } w \in \Sigma_b^*.$$

Theorem 6. *The set of computable reals which are absolutely normal is dense in* $[0,1]$.

Proof. for each base $b \geq 2$, consider the transformation $T_b : [0,1] \to [0,1]$ defined by $T_b(x) = bx(\text{mod } 1)$. The Lebesgue measure λ is T_b-invariant and ergodic. The partition in intervals $[k/b,(k+1)/b[$ induces the symbolic model $(\Sigma_b^{\mathcal{N}}, \sigma, \lambda)$ which is measure-theoretically isomorphic to $([0,1], T_b, \lambda)$: the interval $[k/b,(k+1)/b[$ is represented by $k \in \Sigma_b$. For any word $w \in \Sigma_b$ define $I(w)$ to be the corresponding interval $[0.\overline{w}, 0.\overline{w} + 2^{-|w|}]$.

Defining $\text{dom}T_b := [0,1] \setminus \{\frac{k}{b} : 0 \leq k \leq b\}$ (the interior of the partition) makes T_b an a.e. computable transformation. The observable $f_w := 1_{I(w)}$ is also a.e. computable, with $\text{dom}f_w = [0,1] \setminus \partial I(w)$.

Actually, since $f_w \circ \sigma^n$ and f_w are independent for $n > |w|$, theorem 2 applies to $([0,1], T_b, \lambda)$ and f_w. Therefore, the set of points (for the system (T_b, λ)) which are typical w.r.t the observable f_w contains a constructive Borel-Cantelli set $R_{b,w}$. Furthermore, $R_{b,w}$ is constructive *uniformly* in $b, w \in \Sigma_b$. Hence, by corollary 1, their intersection, which is made of absolutely normal numbers, contains a dense set of computable points. □

5. Dynamical systems having computable typical points

We will see that in a large class of dynamical systems which have a single *physically relevant* invariant measure, the computability of this measure and related c_{g_i}, for observables in $\mathcal{F}$ can be proved, hence we can apply Thm. 5 to find pseudorandom points in such systems.

5.1. **Physical measures.** In general, given (X,T) there could be infinitely many invariant measures (this is true even if we restrict to probability measures). Among this class of measures, some of them are particularly important. Suppose that we observe the behavior of the system (X, T) trough a class of continuous functions $f_i : X \to \mathbb{R}$. We are interested in the statistical behavior of f_i along typical orbits of the system. Let us suppose that the time average along the orbit of x exists

$$A_x(f_i) = \lim_{n\to\infty} \frac{1}{n} \sum f_i(T^n(x))$$

this is a real number for each f_i. Moreover $A_x(f_i)$ is linear and continuous with respect to small changes of f_i in the sup norm. Then the orbit of x acts as a measure μ_x and $A_x(f_i) = \int f_i \, \mathrm{d}\mu_x$ (moreover this measure is also invariant for T). This measure is physically interesting if it is given by a "large" set of initial conditions. This set will be called the basin of the measure. If X is a manifold, it is said that an invariant measure is *physical* (or SRB from the names of Sinai, Ruelle and Bowen) if its basin has positive Lebesgue measure (see [You02] for a survey and more precise definitions).

In what follows we will consider SRB measures in the classes of systems listed below,

(1) The class of uniformly hyperbolic system on submanifolds of $\mathbb{R}^n$.
(2) The class of piecewise expanding maps on the interval.
(3) The class of *Manneville-Pomeau* type maps (non uniformly expanding with an indifferent fixed point).

All these systems, which are rather well understood, have a unique physical measure with respect to which correlations decay is at least polynomial. Furthermore, in each case, the corresponding constants can be estimated for functions in $\mathcal{F}$. The computability of the physical measures is proved case by case, but it is always a consequence of the fact that, in one way or another, the physical measure is "approached" by iterates of the Lebesgue measure at a known speed.

5.2. **Uniformly hyperbolic systems.** To talk about SRB measures on a system whose phase space is a manifold, we have to introduce the Lebesgue measure on a manifold and check that it is computable.

5.2.1. *Computable manifolds and the Lebesgue measure.* For simplicity we will not consider general manifolds but submanifolds of $\mathbb{R}^n$.

Definition 17. *Let M be a computable metric subspace of $\mathbb{R}^n$. We say that M is a m-dimensional computable C^k submanifold of $\mathbb{R}^n$ if there exists a computable function $f : M \times B(0,1) \to M$ (where $B(0,1)$ is the unit ball of $\mathbb{R}^m$ and $M \times B(0,1)$ with the euclidean distance is a CMS in a natural way) such that for each $x \in M$, $f_x = f(x, .)$ is a C^k diffeomorphism with all k derivatives being computable.*

For each x, the above f_x is a map whose differential at any $z \in B(\mathbf{0}, 1)$ is a linear, rank m function $Df_{x,z} : \mathbb{R}^m \to \mathbb{R}^n$. This can be seen as a composition of two functions $Df_{x,z} = Df^2_{x,z} \circ Df^1_{x,z}$ such that $Df^1_{x,z} : \mathbb{R}^m \to \mathbb{R}^m$ is invertible and $Df^2_{x,z} : \mathbb{R}^m \to \mathbb{R}^n$ is an isometry.

Let us denote B_x the image of $B(0,1)$ by f_x. Then the Lebesgue measure of $D \subset B_x$ is defined as

$$m(D) = \int_{f_x^{-1}(D)} \det(Df^1_{x,z}) \, \mathrm{d}z.$$

This does not depend on the choice of B_x and f_x, and it give rise to a finite measure (Lebesgue measure) on M (see [GMS98] page 74). This measure is indeed the m dimensional Hausdorff measure on M. Moreover, the Lebesgue measure is a computable measure.

Lemma 9. *The Lebesgue measure on a computable C^k submanifold of $\mathbb{R}^n$ is computable.*

Proof (sketch). Suppose that A is a constructive open subset of some B_s, where s is an ideal point of M. Since the function $\det(Df^1_{x,z})$ is computable and the function $1_{f^{-1}(A)}(z)$ is lower semi-computable, we can lower semi-compute the value $m(A)$. In particular, there is a base of ideal balls whose measures are lower semi-computable. Let B and B' be such balls. Since these balls have zero measure boundaries, we can compute the measure of their intersection (which is a constructive open included in B). Hence any constructive open set can be decomposed into a (same measure) disjoint union of constructive open sets whose measures can be lower semi-computed. By lemma 2, m is computable. □

5.2.2. *The SRB measure of uniformly hyperbolic systems.* Let us consider a connected C^2 computable manifold M. Let us consider a dynamical system (M,T) where T is a C^2 computable diffeomorphism on M.

Let us consider a constructive open forward invariant set $Q \subset M$ (i.e. $T(\overline{Q}) \subset Q$). Let us consider the (attracting) set

$$\Lambda = \bigcap_{n\geq 0} T^n(Q).$$

Suppose that Λ contains a dense orbit and that it is an hyperbolic set for T, which means that the following conditions are satisfied.

There is a splitting of the tangent bundle of M on Λ: $T_\Lambda M = E^s_\Lambda \oplus E^u_\Lambda$ (at each point x of Λ the tangent space at x can be splitted in a direct sum of two spaces, the stable directions and the unstable ones) and a $\lambda_0 < 1$ such that

- the splitting is compatible with T, that is: $DT_x(E^s_x) = E^s_{T(x)}$ and $DT^{-1}_x(E^u_x) = E^u_{T^{-1}(x)}$.
- The dynamics expand exponentially fast in the unstable directions and contracts exponentially fast in the stable directions in an uniform way, that is: for each $x \in \Lambda$ and for each $v \in E^s_x$ and $w \in E^u_x$, $|DT_x(v)| \leq |\lambda_0 v|$ and $\left|DT^{-1}_x(w)\right| \leq |\lambda_0 w|$.

Under these assumptions it is known that

Theorem 7. *(see* [Via97] *e.g.)There is a unique invariant SRB measure μ supported on Λ. Moreover the measure is ergodic and its basin has full Lebesgue measure on Q.*

This measure has many good properties: it has exponential decay of correlations and it is stable under perturbations of T (see [Via97] e.g.). Another good property of this measure is that it is computable.

Theorem 8. *If M and T are C^2, computable and uniformly hyperbolic as above, then the SRB measure μ is computable.*

Proof. Let m be the Lebesgue measure on Q normalized by $m(Q) = 1$, clearly it is a computable measure. From [Via97] (Prop. 4.9, Remark 4.2) it holds that there are $\lambda < 1$ such that for each ν-Hölder ($\nu \in (0,1]$) continuous observable ψ, it holds

$$\left|\int \psi \circ T^n \,\mathrm{d}m - \int \psi \,\mathrm{d}\mu\right| \leq \lambda^n \ c_\psi$$

where $c_\psi = C\int |\psi| \, dm + \|\psi\|_\nu$, where C is independent from ψ and then can be estimated for each uniform sequence $\psi_i \in \mathcal{F}$ uniformly in i. This means that for each $\psi_i \in \mathcal{F}$ its integral with respect to μ can be calculated up to any given accuracy, uniformly in i. Indeed if we want to calculate $\int \psi_i \, d\mu$ up to an error of ϵ we calculate c_{ψ_i} up to an error of ϵ (this error is not really important as we will see immediately) and choose an n such that $c_{\psi_i}\lambda^n \leq \frac{\epsilon}{2}$.

By this we know that $\left|\int \psi_i \circ T^n \, dm - \int \psi_i \, d\mu\right| \leq \frac{\epsilon}{2}$. Now we have to calculate $\int \psi_i \circ T^n \, dm$ up to an error of $\frac{\epsilon}{2}$ and this will be the output. By lemma 1 then μ is computable. □

Corollary 3. *In an unif. hyp. computable system equipped with its SRB measure as above, the set of computable $\mu-$typical points is dense in the support of μ.*

Proof. μ is computable by the previous theorem, and the correlations decay is given by proposition 4.9 in [Via97] from which follows that there is $\lambda < 1$ such that for each $(g_i, g_j) \in \mathcal{F}^2$ it holds,

$$\left|\int g_i \circ T^n g_j \, \mathrm{d}m - \int g_i \, \mathrm{d}\mu \int g_j \, \mathrm{d}\mu\right| \leq \lambda^n \ c_{g_i,g_j}$$

where $c_{g_i,g_j} = C(\int |g_i| \, \mathrm{d}m + \|g_i\|_1)(\int |g_j| \, \mathrm{d}m + \|g_j\|_1)$ (C is a constant independent of $g_i \in \mathcal{F}$, $\|*\|_1$ is the Lipschitz norm, since functions in $\mathcal{F}$ are Lipschitz) are computable uniformly in i, j. Then the result follows from theorem 5. □

5.3. **Piecewise expanding maps.** We introduce a class of discontinuous maps on the interval having an absolutely continuous SRB invariant measure. The density of this measure has also bounded variation. We will show that this invariant measure is computable.

Let I be the unit interval. Let $T : I \to I$ we say that T is piecewise expanding if there is a finite partition $P = \{I_1, ..., I_k\}$ of I, such that I_i are disjoint intervals and:

(1) the restriction of T to each interval I_i can be extended to a C^1 monotonic map defined on $\overline{I_i}$ and the function $h : I \to \mathbb{R}$ defined by $h(x) = |DT(x)|^{-1}$ has bounded variation.
(2) there are constants $C > 0$ and $\sigma > 1$ such that $|DT^n(x)| > C\sigma^n$ for every $n \geq 1$ and every $x \in I$ for which the derivative is defined.
(3) For each interval $J \subset I$ there is $n \geq 1$ such that $f^n(J) = I$.

We remark that by point 1), in each interval I_i the map is Lipschitz. We remark that this restriction is not strictly necessary for what follows (see [GHR]), we suppose it for the seek of simplicity. As said before, by classical results this kind of map has an absolutely continuous invariant measure (see [Via97], chapter 3 e.g.).

Theorem 9. *If T a piecewise expanding map as above, then it has a unique ergodic absolutely continuous invariant measure μ. The basin of this SRB measure has full Lebesgue measure. Moreover μ can be written as $\mu = \phi m$ where ϕ has bounded variation and m is the Lebesgue measure.*

Moreover as before, the SRB measure is also computable

Proposition 4. *If T is an m-a.e. computable piecewise expanding map satisfying points 1),...,3) above then its SRB measure is computable.*

Proof. Let us consider $\psi \in \mathcal{F}$. In [Roj08] it is proved that the integral of a bounded a.e. computable function is computable, so the numbers $\int \psi \circ T^n \, \mathrm{d}m$ are uniformly computable.

Now, from [Via97] proposition 3.8, remark 3.2 it holds that there are $\lambda < 1, C > 0$ such that for each $\psi \in L^1$

$$\left| \int \psi \circ T^n \, \mathrm{d}m - \int \psi \, \mathrm{d}\mu \right| \leq C \ \lambda^n \ \|\psi\|_{L^1} .$$

This implies that the integral $\int \psi \, \mathrm{d}\mu$ can be calculated up to any given accuracy. As this is true for every $\psi \in \mathcal{F}$, uniformly, μ is computable by lemma 1. □

As Unif. Hyperbolic systems, also Piecewise Expanding maps can be shown to have exponential decay of correlations on bounded variation observables (see [Via97] Remark 3.2) and BV norm of functions in $\mathcal{F}$ can be estimated. Hence as in the previous section we obtain:

Corollary 4. *In an m-a.e. computable piecewise expanding system equipped with its SRB measure, the set of computable typical points is dense in* $[0,1]$.

5.4. **Manneville-Pomeau type maps.** We say that a map $T : [0,1] \to [0,1]$ is a *Manneville-Pomeau type map (MP map)* with exponent s if it satisfies the following conditions:

(1) there is $c \in (0,1)$ such that, if $I_0 = [0,c]$ and $I_1 = (c,1]$, then $T\big|_{(0,c)}$ and $T\big|_{(c,1)}$ extend to C^1 diffeomorphisms, which is C^2 for $x > 0$, $T(I_0) = [0,1]$, $T(I_1) = (0,1]$ and $T(0) = 0$;
(2) there is $\lambda > 1$ such that $T' \geq \lambda$ on I_1, whereas $T' > 1$ on $(0,c]$ and $T'(0) = 1$;
(3) the map T has the following behaviour when $x \to 0^+$

$$T(x) = x + rx^{1+s}(1 + u(x))$$

for some constant $r > 0$ and $s > 0$ and u satisfies $u(0) = 0$ and $u'(x) = O(x^{t-1})$ as $x \to 0^+$ for some $t > 0$.

In [Iso03] (see also [Gou04]) it is proved that for $0 < s < 1$ these systems have a unique absolutely continuous invariant measure, whose density f is locally Lipschitz in a neighborhood of each $x > 0$ (the density diverges at $x = 0$) the system has polynomial decay of correlations for $(1-s)$-Hölder observables. Moreover we have that:

Theorem 10. *If T is a computable MP map then its absolutely continuous invariant measure μ is computable.*

Proof. Let f be the density of μ. T is topologically conjugated to the doubling map $x \to 2x \pmod 1$ hence for each small interval I there is $k > 0$ such that $T^k(I) = [0,1]$. Since f is locally Lipschitz, there is a small interval J on which $f > \delta_1 > 0$. Let n be such that $T^n(J) = [0,1]$. Let I be some small interval, then there exist $J' \subset J$ such that $T^n(J') = I$. Since T is λ-Lipschitz, we have $m(J') \geq \frac{m(I)}{\lambda^n}$. By this, $\mu(J') \geq \frac{\delta_1 m(I)}{\lambda^n}$ and by the invariance of μ, $\frac{\mu(I)}{m(I)} \geq \frac{\delta_1}{\lambda^n}$ and then, as I is arbitrary, for each $x \in [0,1]$ we have $f(x) > \frac{\delta_1}{\lambda^n} > 0$. In particular, $\frac{1}{f}$ is $(1-s)$-Hölder. Now we use the fact that the system has polynomial decay of correlations for $(1-s)$-Hölder observables. Let us consider $\phi \in \mathcal{F}$ then we have that $\frac{1}{f} d\mu = dm$ and $\int \frac{1}{f}\,\mathrm{d}\mu = 1$, hence, by the decay of correlation of this kind of maps

$$\left|\int \phi \circ T^n \,\mathrm{d}m - \int \phi \,\mathrm{d}\mu\right| = \left|\int \phi \circ T^n \frac{1}{f}\,\mathrm{d}\mu - \int \phi \,\mathrm{d}\mu \int \frac{1}{f}\,\mathrm{d}\mu\right| \leq C \left\|\phi\right\|_{1-s} \left\|\frac{1}{f}\right\|_{1-s} n^{s-1}.$$

The norm $\|\phi\|_{1-s}$ can be estimated for functions in $\mathcal{F}$, and then, as in the previous examples we have a way to calculate $\int \phi \,\mathrm{d}\mu$ for each $\phi \in \mathcal{F}$ and again by lemma 1, μ is computable. □

Corollary 5. *In a computable Manneville-Pomeau type system, the set of computable typical points is dense in* $[0, 1]$.

Acknowledgments

The authors wish to thank Professors Giuseppe Longo and Stefano Marmi for scientific and logistic support during the elaboration of the present paper.

References

[BF02] Verónica Becher and Santiago Figueira. An example of a computable absolutely normal number. *Theor. Comput. Sci.*, 270(1-2):947–958, 2002.

[Bil68] Patrick Billingsley. *Convergence of Probability Measures*. John Wiley, New York, 1968.

[Cha33] David G. Champernowne. The construction of decimals normal in the scale of ten. *Journal of the London Mathematical Society*, 8:254–260, 1933.

[Gác05] Peter Gács. Uniform test of algorithmic randomness over a general space. *Theoretical Computer Science*, 341:91–137, 2005.

[GHR] Stefano Galatolo, Mathieu Hoyrup, and Cristóbal Rojas. Computable and non computable physical invariant measures. *In preparation.*

[GHR08] Peter Gács, Mathieu Hoyrup, and Cristóbal Rojas. Schnorr randomness–A dynamical point of view. *In preparation*, 2008.

[GMS98] Mariano Giaquinta, Giuseppe Modica, and Jiri Soucek. *Cartesian currents in the calculus of variations, I*, volume 37 of *Ergebnisse Math. Grenzgebiete (III Ser)*. Springer, 1998.

[Gou04] Sébastien Gouëzel. Sharp polynomial estimates for the decay of correlations. *Israel J. Math.*, 139:29–65, 2004.

[HK95] Boris Hasselblatt and Anatole Katok. *Introduction to the Modern Theory of Dynamical Systems*, volume 54 of *Encyclopedia of Mathematics and Its Applications*. Cambridge University Press, 1995.

[Hoy08] Mathieu Hoyrup. *Computability, randomness and ergodic theory on metric spaces*. PhD thesis, Université Paris Diderot (Paris 7), 2008.

[HR07] Mathieu Hoyrup and Cristóbal Rojas. Computability of probability measures and Martin-Löf randomness over metric spaces, Sep 2007.

[Iso03] Stefano Isola. On systems with finite ergodic degree. *Far east journal of dynamical systems*, 5:1, 2003.

[KST94] Tyll Krüger, Peter Seibt, and Serge Troubetzkoy. Complexity and Randomness of Recursive Discretizations of Dynamical Systems. *Random and Computational Dynamics*, 2:1–19, January 1994.

[Roj08] Cristóbal Rojas. *Randomness and ergodic theory: an algorithmic point of view*. PhD thesis, Ecole Polytechnique, 2008.

[Sch71] Claus-Peter Schnorr. *Zufälligkeit und Wahrscheinlichkeit. Eine algorithmische Begründung der Wahrscheinlichkeitstheorie*, volume 218 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin-New York, 1971.

[Tur36] Alan Turing. On computable numbers, with an application to the entscheidungsproblem. *Proceedings of the London Mathematical Society*, 2, 42:230–265, 1936.

[Via97] Marcelo Viana. Stochastic dynamics of deterministic systems. *Lecture Notes XXI Braz. Math. Colloq. IMPA Rio de Janeiro*, 1997.

[Wei00] Klaus Weihrauch. *Computable Analysis*. Springer, Berlin, 2000.

[YMT99] Mariko Yasugi, Takakazu Mori, and Yoshiki Tsujii. Effective properties of sets and functions in metric spaces with computability stqucture. *Theoretical Computer Science*, 219(1-2):467–486, 1999.

[You02] Lai-Sang Young. What are srb measures, and which dynamical systems have them? *J. Stat. Phys.*, 108:733–754, 2002.

Dipartimento di Matematica Applicata, Universita di Pisa
E-mail address: s.galatolo@docenti.ing.unipi.it

LIENS, Ecole Normale Supérieure, Paris
E-mail address: hoyrup@di.ens.fr

LIENS, Ecole Normale Supérieure and CREA, Ecole Polytechnique, Paris
E-mail address: rojas@di.ens.fr