Computability of probability measures and Martin-Löf randomness over metric spaces☆

Mathieu Hoyrup

DI, Ecole Normale Supérieure, Paris

Cristóbal Rojas

DI, Ecole Normale Supérieure and CREA, Ecole Polytechnique, Paris

Abstract

In this paper we investigate algorithmic randomness on more general spaces than the Cantor space, namely computable metric spaces. To do this, we first develop a unified framework allowing computations with probability measures. We show that any computable metric space with a computable probability measure is isomorphic to the Cantor space in a computable and measure-theoretic sense. We show that any computable metric space admits a universal uniform randomness test (without further assumption).

Key words: Computability, computable metric space, computable probability measure, almost computable function, enumerative lattice, Kolmogorov-Chaitin complexity, algorithmic randomness, universal test.
2000 MSC: 03D45, 03D75, 03D80, 03F60, 68Q30

1. Introduction

The theory of algorithmic randomness begins with the definition of individual random infinite sequences introduced in 1966 by Martin-Löf (see [26]). Since then, many efforts have contributed to the development of this theory which is now well established and intensively studied, though mostly restricted to the Cantor space. In order to carry out an extension of this theory to more general infinite objects as encountered in most mathematical models of physical random phenomena, a necessary step is to understand what it means for a probability measure on a general space to be computable (this is very simply expressed on the Cantor Space). Only then algorithmic randomness can be extended.

☆partly supported by ANR Grant 05 2452 260 ox.

Email addresses: `hoyrup@di.ens.fr` (Mathieu Hoyrup), `rojas@di.ens.fr` (Cristóbal Rojas)

The problem of computability of (Borel) probability measures over more general spaces has been investigated by several authors: by Edalat in [9] for compact spaces using domain-theory; by Weihrauch in [31] for the unit interval and by Schröder in [27] for sequential topological spaces both using representations; and by Gács in [13] for computable metric spaces. Probability measures can be seen from different points of view and those works develop, each in its own framework, the corresponding computability notions. Mainly, Borel probability measures can be regarded as points of a metric space, as valuations on open sets or as integration operators. We express the computability counterparts of these different views in a unified framework, and show them to be equivalent.

Extensions of the algorithmic theory of randomness to other objects have been proposed: on the space of continuous real functions in [3, 11, 12] for the study of Brownian motion, on the space of compact subsets of the Cantor space in [8]. Extensions ot abstract spaces has also been proposed: on effective topological spaces in [18], [19] and on computable metric spaces in [13], both of them generalizing the notion of randomness tests and investigating the problem of the existence of a universal test. In [19], to prove the existence of such a test, ad hoc computability conditions on the measure are required, which *a posteriori* turn out to be incompatible with the notion of computable measure. The second one ([13]), carrying the extension of Levin's theory of randomness, considers *uniform tests* which are tests parametrized by measures. A computability condition on the basis of ideal balls (namely, recognizable Boolean inclusions) is needed to prove the existence of a universal uniform test.

In this article, working in computable metric spaces with any probability measure, we consider both uniform and non-uniform tests and prove the following points:

- uniformity and non-uniformity do not essentially differ,
- the existence of a universal test is assured without any further condition.

Another issue addressed in [13] is the characterization of randomness in terms of Kolmogorov-Chaitin Complexity (a central result in Cantor Space). There, this characterization is proved to hold (for an *effectively compact* computable metric space X with a computable measure) under the assumption that there exists a computable injective encoding of a full-measure subset of X into binary sequences (in the formalism of that paper this is expressed by requiring the existence of a *cell decomposition*). In the real line for example, the base-two numeral system (or binary expansion) constitutes such an encoding for the Lebesgue measure. This fact was already been (implicitly) used in the definition of random reals (reals with a random binary expansion, w.r.t. the uniform measure), in [25] for instance.

We introduce, for computable metric spaces with a computable measure, a notion of binary representation generalizing the base-two numeral system of the reals, and prove that:

- such a binary representation always exists,

- a point is random if and only if it has a unique binary expansion that is random.

Moreover, our notion of binary representation allows to identify any computable probability space with the Cantor space (in a computable-measure-theoretic sense). It provides a tool to directly transfer elements of algorithmic randomness theory from the Cantor space to any computable probability space. In particular, the characterization of randomness in terms of Kolmogorov-Chaitin complexity, even in a non-compact space, is a direct consequence of this.

The way we handle computability on continuous spaces is largely inspired by Weihrauch and Kreitz's theory of representations, which formalizes the ways mathematical objects are represented by symbolic sequences. 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 (see [17] for instance) and *Enumerative Lattices* (introduced in Section 2.2) we shall consider only one *canonical* representation for each set, so we do not use representation theory in its general setting.

Our study of measures and randomness, although restricted to computable metric spaces, involves computability notions on various sets which do not have natural metric structures. Fortunately, all these sets become enumerative lattices in a very natural way and the canonical representation provides in each case the right computability notions.

In Section 2, we develop a language intended to express computability concepts, statements and proofs in a rigorous but still (we hope) transparent way. The structure of computable metric space is then recalled. In Section 3, we introduce the notion of enumerative lattices and present two important examples to be used in the paper. Section 4 is devoted to the detailed study of computability on the set of probability measures. In Section 5 we define the notion of binary representation on any computable metric space with a computable measure and show how to construct such a representation. In Section 6 we apply all this machinery to algorithmic randomness.

2. Basic definitions

2.1. Recursive functions.

The starting point of recursion theory was the mathematization of the intuitive notion of function computable by an *effective procedure* or *algorithm*. The different systems and computation models formalizing *mechanical* procedures on natural numbers or symbols have turned out to coincide, and therefore have given rise to a robust mathematical notion which grasps (this is Church-Turing thesis) what means for a (partial) function $\varphi : \mathbb{N} \to \mathbb{N}$ to be *algorithmic*, and which can be made precise using any one of the numerous formalisms proposed. Following the usual denomination, we call such a function a ***(partial) recursive function***. To show that a function $\varphi : \mathbb{N} \to \mathbb{N}$ is recursive, we will exhibit an algorithm $\mathcal{A}$ which on input n halts and outputs $\varphi(n)$ when it is defined, runs forever otherwise.

In the same vein, a robust notion of (partial) recursive function $F : \mathbb{N}^\mathbb{N} \to \mathbb{N}^\mathbb{N}$ can be characterized by different formal definitions, which are equivalent:

Via domain theory (see [1]). This approach takes the notion of recursive function as primitive, which avoids the definition of a new computation model. A partial function $F : \mathbb{N}^\mathbb{N} \to \mathbb{N}^\mathbb{N}$ is recursive if there is a recursive function $F' : \mathbb{N}^* \to \mathbb{N}^*$ which is monotone for the prefix ordering, such that for all $\sigma \in \mathrm{dom}(F)$, $F(\sigma)$ is the infinite sequence obtained at the limit by computing F' on the finite prefixes of σ (precisely, the Baire space can be embedded into the set of finite and infinite sequences of integers ordered by the prefix relation, which is an ω-algebraic domain).

Via oracle Turing machines (used by Ko and Friedman, see [23], [22]). An oracle Turing machine $\mathcal{M}^{[\sigma]}$ is a Turing machine which works with a sequence $\sigma \in \mathbb{N}^\mathbb{N}$ provided as oracle and is allowed to read elements σ_n of the oracle sequence. On an input $n \in \mathbb{N}$, it may stop and output a natural number, interpreted as $F(\sigma)_n$.

Via type-two Turing machines (defined by Weihrauch, see [32]). Expressed differently, it is essentially the same computation model (it works on symbols instead of integers).

Again, to show that a function $F : \mathbb{N}^\mathbb{N} \to \mathbb{N}^\mathbb{N}$ is recursive, we will exhibit an algorithm $\mathcal{A}$ which given $\sigma \in \mathbb{N}^\mathbb{N}$ as oracle and n as input, halts and outputs $F(\sigma)_n$. The algorithm together with σ in the oracle is denoted $\mathcal{A}^{[\sigma]}$.

A sequence $\sigma \in \mathbb{N}^\mathbb{N}$ is ***recursive*** if the function $n \mapsto \sigma_n$ is recursive. Given a family $(\sigma_i)_{i\in\mathbb{N}}$ of recursive sequences, σ_i is ***recursive uniformly in i*** if the function $\langle i, n\rangle \mapsto \sigma_{i,n}$ is recursive, where $\langle , \rangle$ denotes some computable bijection between tuples and natural numbers.

2.2. Representations and constructivity

A representation on a set X is a surjective (partial) function $\rho : \mathbb{N}^\mathbb{N} \to X$. Let X and Y be sets with fixed representations ρ_X and ρ_Y. The following notions depend on the chosen representations, but we do not mention them when it is clear from the context.

Definition 2.2.1 (Constructivity notions).

1. An element $x \in X$ is ***constructive*** if there is a recursive sequence σ such that $\rho_X(\sigma) = x$.
2. The elements of a sequence $(x_i)_{i\in\mathbb{N}}$ are ***uniformly constructive*** if there is a family $(\sigma_i)_i$ of uniformly recursive sequences such that $\rho_X(\sigma_i) = x_i$ for all i.
3. A function $f :\subseteq X \to Y$ is ***constructive*** on $D \subseteq X$ if there exists a recursive function $F : \mathbb{N}^\mathbb{N} \to \mathbb{N}^\mathbb{N}$ such that the following diagram commutes

on $\rho_X^{-1}(D)$:

$$\begin{array}{ccc} \mathbb{N}^{\mathbb{N}} & \xrightarrow{F} & \mathbb{N}^{\mathbb{N}} \\ \rho_X \downarrow & & \downarrow \rho_Y \\ X & \xrightarrow{f} & Y \end{array} \qquad \text{(that is, } f \circ \rho_X = \rho_Y \circ F \text{ on } \rho_X^{-1}(D))$$

We say that y is ***x-constructive*** if there is a function $f :\subseteq X \to Y$ constructive on $\{x\}$ with $f(x) = y$. If x is constructive, x-constructivity and constructivity are equivalent. Note that two sequences of natural numbers can be merged into a single one, so the product $X \times Y$ of two represented sets has a canonical representation. In particular, it makes sense to speak about (x, y)-constructive elements.

2.3. Objects

There is a canonical way of defining a representation on a set X when 1) some collection of *elementary objects* of X can be encoded into natural numbers and 2) any element of X can be described by a sequence of these elementary objects. Once encoded into natural numbers, the elementary objects inherit their finite character and may be output by algorithms. Let us make it precise:

Definition 2.3.1. A ***numbered set*** $\mathcal{O}$ is a countable set together with a total surjection $\nu_{\mathcal{O}} : \mathbb{N} \to \mathcal{O}$ called the ***numbering***. We write o_n for $\nu(n)$.

An algorithm may then be seen as outputting objects, via their numbers.

A numbered set $\mathcal{O}$ and a (partial) surjection $\delta : \mathcal{O}^{\mathbb{N}} \to X$ induce canonically a representation $\rho : \mathbb{N}^{\mathbb{N}} \to X$ defined by $\rho(n_1, n_2, \ldots) = \delta(o_{n_1}, o_{n_2}, \ldots)$. At least in this paper, all representations will be obtained in this way. A sequence of finite objects which is mapped by δ to x is called a ***description*** of x.

Given a numbered set $\mathcal{O}$, we say that an algorithm (plain or with oracle) ***enumerates*** a sequence of objects $(o_{n_i})_{i\in\mathbb{N}}$ if on input i it outputs o_{n_i}. Given a representation $(\mathcal{O}, \delta)$ on a set X, an algorithm enumerating a description of $x \in X$ is said to ***describe*** x.

An algorithm may also take objects as inputs, with a restriction:

Definition 2.3.2. An algorithm $\mathcal{A}$ is said to be ***extensional*** on an element $x \in X$ if for all σ such that $\rho_X(\sigma) = x$, $\mathcal{A}^{[\sigma]}$ describes the same element $y \in Y$.

We then say that $\mathcal{A}$ x-describes y or that $\mathcal{A}^{[x]}$ describes y.

The constructivity notions of Definition 2.2.1 can then be expressed using this language, which will be used throughout this paper.

1. An element $x \in X$ is constructive if there is an algorithm describing x,
2. The elements of a sequence $(x_i)_{i\in\mathbb{N}}$ are uniformly constructive if there is an algorithm $\mathcal{A}$ such that $\mathcal{A}(\langle i, . \rangle)$ describes x_i,
3. A function $f :\subseteq X \to Y$ is constructive on $D \subseteq X$ if there exists an algorithm which x-describes $f(x)$ for all $x \in D$.

An x-constructive element y may be x-described by an algorithm which is extensional only on x, and thus induce a function which is defined only at x.

2.3.1. The example of the real numbers

The set $\mathbb{R}$ of real numbers can be endowed with several non-equivalent representations. Let $\mathbb{Q}$ be the numbered set of rational numbers. A sequence $(x_n)_{n\in\mathbb{N}}$ of real numbers is said to be a ***fast Cauchy*** sequence, or simply a ***fast*** sequence if $|x_n - x_{n+1}| < 2^{-n}$ for all n.

Let $\delta_C : \mathbb{Q}^{\mathbb{N}} \to \mathbb{R}$ be the partial surjection which maps every fast sequence of rational numbers to its limit. A real number is said to be ***computable*** if it is constructive relative to δ_C.

Let $\delta_{\leq} : \mathbb{Q}^{\mathbb{N}} \to \mathbb{R}$ be the total surjection which maps every sequence of rational numbers to its supremum. A real number is said to be ***lower semi-computable*** if it is constructive relative to $\delta_{\leq}$.

Let $\delta_{\geq} : \mathbb{Q}^{\mathbb{N}} \to \mathbb{R}$ be the total surjection which maps every sequence of rational numbers to its infimum. A real number is said to be ***upper semi-computable*** if it is constructive relative to $\delta_{\geq}$.

We recall that a real number x is computable if and only if x is both lower and upper semi-computable.

2.4. Computable Metric Spaces

Plain computability (as opposed to semi-computability) on the real numbers can be extended to a large class of metric spaces, called computable metric spaces. These spaces have been introduced and studied in [30], [10], [17] among others.

Definition 2.4.1. A ***computable metric space*** is a triple $\mathcal{X} = (X, d, \mathcal{S})$, where:

- (X, d) is a separable complete metric space (polish metric space),
- $\mathcal{S} = \{s_i : i \in \mathbb{N}\}$ is a countable dense subset of X,
- The real numbers $d(s_i, s_j)$ are all computable, uniformly in $\langle i, j\rangle$.

The elements of $\mathcal{S}$ are called the ***ideal points***. The numbering $\nu_{\mathcal{S}}$ defined by $\nu_{\mathcal{S}}(i) := s_i$ makes $\mathcal{S}$ a numbered set. Without loss of generality, $\nu_{\mathcal{S}}$ can be supposed to be injective: as $d(s_i, s_j) > 0$ can be semi-decided, ν_S can be effectively transformed into an injective numbering. Then a sequence of ideal points can be uniquely identified with the sequence of their names.

For $x \in X$ and $r > 0$, let $B(x, r)$ be the metric ball $\{y \in X : d(x, y) < r\}$. The numbered sets $\mathcal{S}$ and $\mathbb{Q}_{>0}$ induce the numbered set of ***ideal balls*** $\mathcal{B} := \{B(s_i, q_j) : s_i \in \mathcal{S}, q_j \in \mathbb{Q}_{>0}\}$, the numbering being $\nu_{\mathcal{B}}(\langle i, j\rangle) := B(s_i, q_j)$. We write $B_{\langle i,j\rangle}$ for $\nu_{\mathcal{B}}(\langle i, j\rangle)$. The closed ball $\{x \in X : d(s, x) \leq q\}$ is denoted $\overline{B}(s, q)$ and may not coincide with the closure of the open ball $B(s, q)$ (typically, if the space is disconnected).

We now recall some important examples of computable metric spaces:

Examples:

1. The Cantor space $(\Sigma^{\mathbb{N}}, d, \mathcal{S})$ where Σ is a finite alphabet, $d(\omega, \omega') := 2^{-\min\{n\in\mathbb{N}:\omega_n \neq \omega'_n\}}$ if $\omega = \omega'$ and $d(\omega, \omega) = 0$ and $\mathcal{S} := \{w000\ldots : w \in \Sigma^*\}$ where Σ^* is the set of finite words on Σ and 0 a distinguished element of Σ.

2. The euclidean space $(\mathbb{R}^n, d_{\mathbb{R}^n}, \mathbb{Q}^n)$ with the euclidean metric and the standard numbering of $\mathbb{Q}^n$,
3. The product $(X \times Y, d, \mathcal{S}_X \times \mathcal{S}_Y)$ of two computable metric spaces has a canonical computable metric space structure, with $d((x,y),(x',y')) = \max\{d_X(x,x'), d_Y(y,y')\}$.

For further examples, like functions spaces $C[0,1]$ and L^p for computable $p \geq 1$ we refer to [Weihrauch]. As on $\mathbb{R}$, a sequence $(x_n)_{n\in\mathbb{N}}$ of points of X is said to be a ***fast Cauchy*** sequence, or simply a ***fast*** sequence if $d(x_n, x_{n+1}) < 2^{-n}$ for all n.

Definition 2.4.2. On a computable metric space $(X, d, \mathcal{S})$, the canonical representation is the Cauchy representation $(\mathcal{S}, \delta_C)$ defined by $\delta_C(\overrightarrow{s}) = x$ for all fast sequences $\overrightarrow{s}$ of ideal points converging to x.

Again, each set X with a computable metric structure $(X, d, \mathcal{S})$ will be implicitly represented using the Cauchy representation. Then canonical constructivity notions derive directly from Definition 2.2.1. It is usual to call a constructive element of X a ***computable point***, and a constructive function between computable metric spaces, a ***computable function***. Remark that the computable real numbers are the computable points of the computable metric space $(\mathbb{R}, d, \mathbb{Q})$.

The choice of this representation is justified by the classical result: every computable function between computable metric spaces is continuous (on its domain of computability).

Proposition 2.4.1. *Let $(X, d, \mathcal{S})$ be a computable metric space. The distance $d : X \times X \to \mathbb{R}$ is a computable function.*

Proposition 2.4.2. *For a point $x \in X$, the following statements are equivalent:*
- *x is a computable point,*
- *all $d(x, s_i)$ are upper semi-computable uniformly in i,*
- *$d_x := d(x, .) : X \to \mathbb{R}$ is a computable function.*

Several metrics and effectivisations of a single set are possible, and induce in general different computability notions: two computable metric structures $(d, \mathcal{S})$ and $(d', \mathcal{S}')$ are said to be *effectively equivalent* if $id : (X, d, \mathcal{S}) \to (X, d', \mathcal{S}')$ is a computable homeomorphism (with computable inverse). In this case, all computability notions are preserved replacing one structure by the other (see [17] for details).

3. Enumerative Lattices

3.1. Definition

We introduce a simple structure using basic order theory, on which a natural representation can be defined. The underlying ideas are those from domain theory, but the framework is lighter and (hence) less powerful. Actually, it is sufficient for the main purpose: Proposition 3.1.1. This will be applied in the last section on randomness.

Definition 3.1.1. An ***enumerative lattice*** is a triple $(X, \leq, \mathcal{P})$ where $(X, \leq)$ is a complete lattice and $\mathcal{P} \subseteq X$ is a numbered set such that every element x of X is the supremum of some subset of $\mathcal{P}$.

We then define $\mathcal{P}_{\downarrow}(x) := \{p \in \mathcal{P} : p \leq x\}$ (note that $x = \sup \mathcal{P}_{\downarrow}(x)$). Any element of X can be described by a sequence $\overrightarrow{p}$ of elements of $\mathcal{P}$. Note that the least element $\perp$ need not belong to $\mathcal{P}$: it can be described by the empty set, of which it is the supremum.

Definition 3.1.2. The canonical representation on an enumerative lattice $(X, \leq, \mathcal{P})$ is the induced by the partial surjection $\delta_{\leq}(\overrightarrow{p}) = \sup \overrightarrow{p}$ (where the sequence $\overrightarrow{p}$ may be empty).

From here and beyond, each set X endowed with an enumerative structure $(X, \leq, \mathcal{P})$ will be implicitly represented using the canonical representation. Hence, canonical constructivity notions derive directly from Definition 2.2.1. Let us focus on an example: the identity function from X to X is computed by an algorithm outputting exactly what is provided by the oracle. Hence, when the oracle is empty, which describes $\perp$, the algorithm runs forever and outputs nothing, which is a description of $\perp$.

Examples:

1. $(\overline{\mathbb{R}}, \leq, \mathbb{Q})$ with $\overline{\mathbb{R}} = \mathbb{R} \cup \{-\infty, +\infty\}$: the constructive elements are the so-called *lower semi-computable* real numbers,
2. $(2^{\mathbb{N}}, \subseteq, \{\text{finite sets}\})$: the constructive elements are the r.e. sets from classical recursion theory,
3. $(\{\perp, \top\}, \leq, \{\top\})$ with $\perp < \top$.

One of the most important features of enumerative lattices for our purposes is the following.

Proposition 3.1.1. *Let $(X, \leq, \mathcal{P})$ be an enumerative lattice. There is an enumeration $(x_i)_{i \in \mathbb{N}}$ of all the constructive elements of X such that x_i is constructive uniformly in i.*

Proof. let φ be a universal partial recursive function. It induces an enumeration of all the r.e. subsets of $\mathbb{N}$: for every r.e. set $E \subseteq \mathbb{N}$, there is some i such that $E = E_i := \{\varphi(\langle i, n \rangle) : n \in \mathbb{N}\}$. Moreover, we can take φ such that whenever $E_i \neq \emptyset$ the function $\varphi(\langle i, . \rangle) : \mathbb{N} \to \mathbb{N}$ is total (this is a classical construction from recursion theory, see [16]). Then consider the associated algorithm $\mathcal{A}_{\varphi} = \nu_{\mathcal{P}} \circ \varphi$: for every constructive element x there is some i such that $\mathcal{A}_{\varphi}(\langle i, . \rangle) : \mathbb{N} \to \mathcal{P}$ enumerates x ($\emptyset$ is a description of $\perp$).

The Scott continuity can be defined on every directed complete partial order (see [1]). On enumerative lattices, the definition can be sharpened, taking advantage of the additional structure.

Definition 3.1.3. Let Y, Z have enumerative lattice structures. A function $f : Y \to Z$ is said to be ***Scott-continuous*** if it is monotonic and commutes with suprema of increasing sequences.

Scott continuity happens to be very useful to prove constructivity of functions between enumerative lattices. The following (easy) proposition will be intensively used.

Proposition 3.1.2. *If a function $f : Y \to Z$ is Scott-continuous and all $f(\sup\{p_{n_1}, \ldots, p_{n_k}\})$ are constructive uniformly in $\langle n_1, \ldots, n_k\rangle$, then f is constructive.*

Proof. Let $\overrightarrow{p} = (p_{n_1}, p_{n_2}, \ldots)$ be a sequence whose supremum is an element $y \in Y$. The algorithm describing $f(y)$ works as follows: on oracle $\overrightarrow{p}$, it enumerates in dovetail all the descriptions of $f(\sup\{p_{n_1}, \ldots, p_{n_k}\})$ for all $k \geq 1$ (this is possible because all the $f(\sup\{p_{n_1}, \ldots, p_{n_k}\})$ are constructive uniformly in $\langle n_1, \ldots, n_k\rangle$, by hypothesis). The supremum of the enumerated sequence is then $\sup_k f(\sup\{p_{n_1}, \ldots, p_{n_k}\})$ which is $f(y)$ by Scott-continuity. Thus, the enumerated sequence is a description of $f(y)$.

Actually, one can also prove the converse implication, using classical technics. But we do not need this in the present paper.

3.2. Functions from a computable metric space to an enumerative lattice

Given a computable metric space $(X, d, \mathcal{S})$ and an enumerative lattice $(Y, \leq, \mathcal{P})$, we define the numbered set $\mathcal{F}$ of ***step functions*** from X to Y:

$$f_{\langle i,j\rangle}(x) = \begin{cases} p_j & \text{if } x \in B_i \\ \perp & \text{otherwise} \end{cases}$$

We then define $\mathcal{C}(X, Y)$ as the closure of $\mathcal{F}$ under pointwise suprema, with the pointwise ordering $\sqsubseteq$. We have directly:

Proposition 3.2.1. $(\mathcal{C}(X, Y), \sqsubseteq, \mathcal{F})$ *is an enumerative lattice.*

example: the set $\overline{\mathbb{R}}^+ = [0, +\infty) \cup \{+\infty\}$ has an enumerative lattice structure $(\overline{\mathbb{R}}^+, \leq, \mathbb{Q}^+)$, which induces the enumerative lattice $\mathcal{C}(X, \overline{\mathbb{R}}^+)$ of positive lower semi-continuous functions from X to $\overline{\mathbb{R}}^+$. Its constructive elements are the positive *lower semi-computable* functions.

We now show that the constructive elements of $\mathcal{C}(X, Y)$ are exactly the constructive functions from X to Y.

To each algorithm $\mathcal{A}$ we associate a constructive element of $\mathcal{C}(X, Y)$, enumerating a sequence of step functions: enumerate all $\langle n, i_0, \ldots, i_k\rangle$ with $d(s_{i_j}, s_{i_{j+1}}) < 2^{-(j+1)}$ for all $j < k$ (prefix of a fast sequence). Keep only those for which the computation of $\mathcal{A}^{[i_0,\ldots,i_k,0,0,\ldots]}(n)$ halts without trying to read beyond i_k. For each one, the latter computation outputs some element p_l: then output the step function $f_{\langle i,l\rangle}$ where $B_i = B(s_{i_k}, 2^{-k})$. We denote by $f_{\mathcal{A}}$ the supremum of the enumerated sequence of step functions.

Lemma 3.2.1. *For all x on which $\mathcal{A}$ is extensional, $f_{\mathcal{A}}(x)$ is the element of Y described by $\mathcal{A}^{[x]}$.*

PROOF. let y be the element described by $\mathcal{A}^{[x]}$.

For all $\langle n, i_0, \ldots, i_k \rangle$ for which some $f_{\langle i,j \rangle}$ is enumerated with $x \in B_i$, there is a fast sequence $\overrightarrow{s}$ converging to x starting with $s_{i_0}, \ldots, s_{i_k}$, for which $\mathcal{A}^{[\overrightarrow{s}]}(n) = p_j$. Then $y \geq p_j = f_{\langle i,j \rangle}(x)$. Hence $y \geq f_{\mathcal{A}}(x)$.

There is a fast sequence $\overrightarrow{s}$ converging to x: for all n, $\mathcal{A}^{[\overrightarrow{s}]}(n)$ stops and outputs some p_{j_n}, so there is some i_n with $x \in B_{i_n}$ such that $f_{\langle i_n, j_n \rangle}$ is enumerated. Hence, $y = \sup_n p_{j_n} = \sup f_{\langle i_n, j_n \rangle}(x) \leq f_{\mathcal{A}}(x)$.

Proposition 3.2.2. *The constructive elements of $\mathcal{C}(X, Y)$ are exactly the (total) constructive functions from X to Y.*

PROOF. The supremum of an r.e. subset E of $\mathcal{F}$ is a total constructive function: semi-decide in dovetail $x \in B_i$ for all $f_{\langle i,j \rangle} \in E$, and enumerate p_j each time a test stops.

Given a total constructive function f, there is an algorithm $\mathcal{A}$ which on each $x \in X$ is extensional and describes $f(x)$, so $f = f_{\mathcal{A}}$.

The proof even shows that the equivalence is constructive: the evaluation of any $f : X \to Y$ on any $x \in X$ can be achieved by an algorithm having access to any description of $f \in \mathcal{C}(X, Y)$, and any algorithm evaluating f can be converted into an algorithm describing $f \in C(X, Y)$. More precisely:

Proposition 3.2.3. *Let X, X' be computable metric spaces and Y be an enumerative lattice:*

Evaluation: *The function Eval: $\mathcal{C}(X, Y) \times X \to Y$ defined by Eval$(f, x) = f(x)$ is constructive,*

Curryfication: *If a function $f : X' \times X \to Y$ is constructive then the function from X' to $C(X, Y)$ mapping $x' \in X'$ to $f(x', .)$ is constructive.*

Finally, the enumerative lattice structure has important properties, which will be used later:

Proposition 3.2.4. *Let $f : D \subseteq X \to Y$ be a function which is constructive on D. f can be extended to a* total *constructive function.*

The x-constructive elements of Y are exactly the images of x by total *constructive functions from X to Y.*

PROOF. Let $\mathcal{A}$ be an algorithm which, for each $x \in D$, x-describes $f(x)$. $f_{\mathcal{A}}$ is a total constructive function by proposition 3.2.2. Let $x \in D$: as $\mathcal{A}$ is extensional on x, it x-describes $f_{\mathcal{A}}(x)$ by lemma 3.2.1. By hypothesis, it x-describes $f(x)$, so $f_{\mathcal{A}}$ coincides with f on D.

The second part is a direct consequence of the first one, with $D = \{x\}$.

3.3. The Open Subsets of a computable metric space

Following [7], [6], we define constructivity notions on the open subsets of a computable metric space. The topology τ induced by the metric has the numbered set $\mathcal{B}$ of ideal balls as a countable basis: any open set can then be described as a countable union of ideal balls. Actually $(\tau, \subseteq, \mathcal{B})$ is an enumerative lattice (cf Section 3), the supremum operator being union. The canonical representation on enumerative lattices (Definition 3.1.2) induces constructivity notions on τ, a constructive open set being called a ***recursively enumerable (r.e) open set***.

In order to prove that some set of natural numbers is recursively enumerable, it is often more natural to prove that it is semi-decidable, which is an equivalent notion. This notion can be extended to subsets of a computable metric space, and it happens to be very useful in the applications. We recall from Section 3 that $\{\perp, \top\}$ is an enumerative lattice, which induces canonically the enumerative lattice $\mathcal{C}(X, \{\perp, \top\})$.

Definition 3.3.1. A subset A of X is said to be ***semi-decidable*** if its indicator function $1_A : X \to \{\perp, \top\}$ (mapping $x \in A$ to $\top$ and $x \notin A$ to $\perp$) is constructive.

In other words, A is semi-decidable if there is a recursive function φ such that for all $x \in X$ and all descriptions $\overrightarrow{s}$ of x, $\varphi^{\lceil \overrightarrow{s} \rceil}$ stops if and only if $x \in A$. It is a well-known result (see [6]) that the two notions are effectively equivalent:

Proposition 3.3.1. *A subset of X is semi-decidable if and only if it is an r.e. open set. Moreover, the enumerative lattices $(\tau, \subseteq, \mathcal{B})$ and $\mathcal{C}(X, \{\perp, \top\})$ are constructively isomorphic.*

The isomorphism is the function $U \mapsto 1_U$ and its inverse $f \mapsto f^{-1}(\top)$. In other words, $f^{-1}(\top)$ is f-r.e. uniformly in f and 1_U is U-lower semi-computable uniformly in U. It implies in particular that:

Corollary 3.3.1. *The intersection $(U, V) \mapsto U \cap V$ and union $(U, V) \mapsto U \cup V$ are constructive functions from $\tau \times \tau$ to τ.*

For computable functions between computable metric spaces, we have the following useful characterization:

Proposition 3.3.2. *Let (X, d_X, S_X) and (Y, d_Y, S_Y) be computable metric spaces. A (partial) function $f : D \subset X \to Y$ is computable if and only if the preimages of ideal balls are uniformly r.e. open (in D) sets. That is, for all i, $f^{-1}(B_i) = U_i \cap D$ where U_i is an r.e. open set uniformly in i.*

We will use the following notion:

Definition 3.3.2. A ***constructive G_δ-set*** is a set of the form $\bigcap_n U_n$ where $(U_n)_n$ is a sequence of uniformly r.e. open sets.

3.3.1. Extension of computable functions

It is a classical result that if $f : X \to Y$ is a function from a topological space to a metric space, then the set of points of continuity of f is a G_δ-set.

In [17] it is proved that between computable metric spaces, the domain of functions which are computable in a stronger sense is a constructive G_δ-set, when the space has finite topological dimension in an effective way (existence of a finitary stratification). We prove a related result, which holds for any computable metric space.

Theorem 3.3.1. *Let X, Y be computable metric spaces. Let $f : D \subseteq X \to Y$ be a function computable on a dense set D. Then f can be extended to a computable function on a constructive G_δ-set.*

Proof. There is a computable function $\phi : \mathcal{B}_Y \to \tau_X$ such that $f^{-1}(B) = D \cap \phi(B)$ for all ideal ball B of Y. We define the domain of the extension of f:

$$G = \bigcap_{q \in \mathbb{Q}, q>0} \bigcup_{s \in \mathcal{S}_Y} \phi(B(s,q))$$

which is a constructive G_δ-set. By continuity of $f : D \to Y$, one easily has $D \subseteq G$.

We now define $g : G \to Y$ extending f. Let $x \in G$: as D is dense, there is a sequence $(x_k)_k$ of points of D converging to x: we define $g(x) = \lim_k f(x_k)$.

Claim 1. *g is well-defined.*

The limit exists: for each $\epsilon > 0$, x is in some $\phi(B(s,\epsilon))$ which is open, so there is k_0 such that $x_k \in \phi(B(s,\epsilon))$ for $k \geq k_0$. As $x_k \in D$, $f(x_k) \in B(s,\epsilon)$ for all $k \geq k_0$. $(f(x_k))_k$ is then a Cauchy sequence, which converges by completeness of Y.

The limit is uniquely defined. Indeed, let $(x_k)_k$ and $(x'_k)_k$ be two sequences of points of D converging to x. Mix these two sequences: $x''_{2k} = x_k$ and $x''_{2k+1} = x'_k$. $(x''_k)_k$ is a sequence of points of D converging to x, so $f(x''_k)$ converges. Consequently, $\lim_k f(x_k) = \lim_k f(x'_k)$.

As f is continuous on D, g coincides with f on D.

Claim 2. *g is computable.*

In general, one does not have $g^{-1}(B) = G \cap \phi(B)$ for an ideal ball B. Instead, the following holds: $g^{-1}(B) \subseteq G \cap \overline{\phi(B)}$ and $G \cap \phi(B) \subseteq g^{-1}(\overline{B})$ (easy from the definition of g).

We define the strict order $<$ on $Y \times \mathbb{R}_+$ by $(x', r') < (x, r)$ if $d(x', x) + r' < r$ (this order is also used in [10]). If $(x', r') < (x, r)$ then $\overline{B}(x', r') \subseteq B(x, r)$ (the converse does not hold in general, but for normed vector spaces like $\mathbb{R}$). Let $B(s,q)$ be some ideal ball of Y. We define:

$$\psi(B(s,q)) = \bigcup_{(s',q')<(s,q)} \phi(B(s',q'))$$

and show that $g^{-1}(B(s,q)) = G \cap \psi(B(s,q))$ which implies that g is computable, as $\psi(B_i)$ is r.e. open, uniformly in i.

First, note that $B(s,q) = \bigcup_{(s',q')<(s,q)} B(s',q') = \bigcup_{(s',q')<(s,q)} \overline{B}(s',q')$.

If $x \in G \cap \psi(B(s,q))$ then $x \in \phi(B(s',q'))$ for some $(s',q') < (s,q)$, so $g(x) \in \overline{B}(s',q') \subseteq V$.

Conversely, if $x \in G$ and $g(x) \in V$, $g(x) \in B(s',q')$ for some $(s',q') < (s,q)$. Take some positive rational δ such that $d(g(x),s') < q' - \delta$: as $x \in G$, there is s'' such that $x \in \phi(B(s'',\delta/2))$. It follows that $g(x) \in \overline{B}(s'',\delta/2)$, which implies $(s'',\delta/2) < (s,q)$. Hence, $x \in \psi(B(s,q))$.

Observe that the result still holds when X is any effective topological space (the proof does not use the metric in X).

4. Computing with probability measures

4.1. Measures as points of the computable metric space $\mathcal{M}(X)$

Here, following [13], we define computable measures in the following way: first the space $\mathcal{M}(X)$ is endowed with a computable metric space structure compatible with the weak topology and then computable measures are defined as the constructive points.

Given a metric space (X,d), the set $\mathcal{M}(X)$ of Borel probability measures over X can be endowed with the *weak topology*, which is the finest topology for which $\mu_n \to \mu$ if and only if $\int f \, \mathrm{d}\mu_n \to \int f \, \mathrm{d}\mu$ for all continuous bounded function $f : X \to \mathbb{R}$. This topology is metrizable and when X is separable and complete, $\mathcal{M}(X)$ is also separable and complete (see [4]). Moreover, a computable metric structure on X induces in a canonical way a computable metric structure on $\mathcal{M}(X)$.

Let $\mathcal{D} \subset \mathcal{M}(X)$ be the set of those probability measures that are concentrated in finitely many points of $\mathcal{S}$ and assign rational values to them. It can be shown that this is a dense subset (see [4]). The numberings $\nu_{\mathcal{S}}$ of ideal points of X and $\nu_{\mathbb{Q}}$ of the rationals numbers induce a numbering $\nu_{\mathcal{D}}$ of ideal measures: $\mu_{\langle\langle n_1,\dots,n_k\rangle,\langle m_1,\dots,m_k\rangle\rangle}$ is the measure concentrated over the finite set $\{s_{n_1},\dots,s_{n_k}\}$ where q_{m_i} is the weight of s_{n_i}.

4.1.1. The Prokhorov metric

Let us consider the particular metric on $\mathcal{M}(X)$:

Definition 4.1.1. The ***Prokhorov metric*** π on $\mathcal{M}(X)$ is defined by:

$$\pi(\mu,\nu) := \inf\{\epsilon \in \mathbb{R}^+ : \mu(A) \leq \nu(A^\epsilon) + \epsilon \text{ for every Borel set } A\}. \tag{1}$$

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

It is known that it is indeed a metric, which induces the weak topology on $\mathcal{M}(X)$ (see [4]). Moreover, as proved in [13] we have that:

Proposition 4.1.1. *$(\mathcal{M}(X),\mathcal{D},\pi)$ is a computable metric space.*

PROOF. We have to show that the real numbers $\pi(\mu_i, \mu_j)$ are all computable, uniformly in $\langle i, j \rangle$. First observe that if U is a r.e. open subset of X, $\mu_i(U)$ is lower semi-computable uniformly in i and U. Indeed, if $(s_{n_1}, q_{m_1}), \ldots, (s_{n_k}, q_{m_k})$ are the mass points of μ_i together with their weights (recoverable from i) then $\mu_i(U) = \sum_{s_{n_j} \in U} q_{m_j}$. As the s_{n_j} which belong to U can be enumerated from any description of U, this sum is lower semi-computable. In particular, $\mu_i(B_{i_1} \cup \ldots \cup B_{i_k})$ is lower semi-computable and $\mu_i(\overline{B}_{i_1} \cup \ldots \cup \overline{B}_{i_k})$ is upper semi-computable, both of them uniformly in $\langle i, i_1, \ldots, i_k \rangle$

Now we prove that $\pi(\mu_i, \mu_j)$ is computable uniformly in $\langle i, j \rangle$.

Observe that if μ_i is an ideal measure concentrated over S_i, then (1) becomes $\pi(\mu_i, \mu_j) = \inf\{\epsilon \in \mathbb{Q} : \forall A \subset S_i,\ \mu_i(A) < \mu_j(A^\epsilon) + \epsilon\}$. Since μ_j is also an ideal measure and A^ϵ is a finite union of open ideal balls, the number $\mu_j(A^\epsilon)$ is lower semi-computable (uniformly in ϵ and j) and then $\pi(\mu_i, \mu_j)$ is upper semi-computable, uniformly in $\langle i, j \rangle$. To see that $\pi(\mu_i, \mu_j)$ is lower semi-computable, uniformly in $\langle i, j \rangle$, observe that $\pi(\mu_i, \mu_j) = \sup\{\epsilon \in \mathbb{Q} : \exists A \subset S_i,\ \mu_i(A) > \mu_j(A^{\overline{\epsilon}}) + \epsilon\}$, where $A^{\overline{\epsilon}} = \{x : d(x, A) \leq \epsilon\}$ (a finite union of closed ideal balls when $A \subset S_i$) and use the upper semi-computability of $\mu_j(A^{\overline{\epsilon}})$.

Definition 4.1.2. A measure μ is ***computable*** if it is a constructive point of $(\mathcal{M}(X), \mathcal{D}, \pi)$.

The effectivization of the space of Borel probability measures $\mathcal{M}(X)$ is of theoretical interest, and opens the question: what kind of information can be (algorithmically) recovered from a description of a measure as a point of the computable metric space $\mathcal{M}(X)$? The two most current uses of a measure are to give weights to measurable sets and means to measurable functions. Can these quantities be computed?

4.1.2. The Wasserstein metric

In the particular case when the metric space X is bounded, an alternative metric can be defined on $\mathcal{M}(X)$. When f is a real-valued function, μf denotes $\int f \, \mathrm{d}\mu$.

Definition 4.1.3. The *Wasserstein metric* on $\mathcal{M}(X)$ is defined by:

$$W(\mu, \nu) = \sup_{f \in 1\text{-Lip}(X)} (|\mu f - \nu f|) \tag{2}$$

where 1-Lip(X) is the space of 1-Lipschitz functions from X to $\mathbb{R}$.

We recall (see [2]) that W has the following properties:

Proposition 4.1.2.

1. *W is a distance and if X is separable and complete then $\mathcal{M}(X)$ with this distance is a separable and complete metric space.*
2. *The topology induced by W is the weak topology and thus W is equivalent to the Prokhorov metric.*

Moreover, if $(X, \mathcal{S}, d)$ is a computable metric space (and X bounded), then:

Proposition 4.1.3. *$(\mathcal{M}(X), \mathcal{D}, W)$ is a computable metric space.*

PROOF. We have to show that the distance $W(\nu_i, \nu_j)$ between ideal measures is uniformly computable. Let $S_{i,j} = \mathrm{Supp}(\nu_i) \cup \mathrm{Supp}(\nu_j)$ be the finite set of ideal points on which ν_i and ν_j are concentrated. We fix some $s^* \in S_{i,j}$: we can take the supremum in (2) only over $1\text{-Lip}^*(X) := \{f \in 1\text{-Lip}(X) : f(s^*) = 0\}$, as the difference $|\mu f - \nu f|$ remains unchanged when adding a constant to f. Given some precision ϵ we construct an ϵ-net of $1\text{-Lip}^*(X)$, that is a finite set $\mathcal{G}_\epsilon \subseteq 1\text{-Lip}^*(X)$ made of uniformly computable functions such that for each $f \in 1\text{-Lip}^*(X)$ there is some $g \in \mathcal{G}_\epsilon$ satisfying $\sup\{|f(x) - g(x)| : x \in S_{i,j}\} < \epsilon$. Let $M \in \mathbb{N}$ be greater than the diameter of X: $|f| < M$ for every $f \in 1\text{-Lip}^*(X)$. Compute $n \in \mathbb{N}$ such that $M < 2\epsilon n$. For each $s \in S_{i,j}$ and $a \in \{\frac{kM}{n}\}_{k=-m}^{m}$ let us consider the functions defined by $d^+_{s,k}(x) := a + d(s, x)$ and $d^-_{s,k}(x) := a - d(s, x)$. Let D be the finite set of such functions and $\mathcal{G}_\epsilon = \{\max(f_1, \ldots, f_p) : f_i \in D, p \geq 1\} \cup \{\min(f_1, \ldots, f_p) : f_i \in D, p \geq 1\}$. It is not difficult to see that the set $\mathcal{G}_\epsilon$ satisfies the required condition.

Therefore, since $\sup(|f - g|) < \epsilon$ implies $|\mu(f - g)| < \epsilon$ we have that:

$$\sup_{g \in \mathcal{G}_\epsilon} (|\mu_i g - \mu_j g|) \leq W(\mu_i, \mu_j) \leq \sup_{g \in \mathcal{G}_\epsilon} (|\mu_i g - \mu_j g|) + 2\epsilon$$

where the $\mu_i g$ are computable, uniformly in i. The result follows.

When X is bounded, the effectivisations using the Prokhorov or the Wasserstein metrics turn out to be equivalent.

Theorem 4.1.1. *The Prokhorov and the Wasserstein metrics are computably equivalent. That is, the identity function $id : (\mathcal{M}(X), \mathcal{D}, \pi) \to (\mathcal{M}(X), \mathcal{D}, W)$ is a computable isomorphism, as well as its inverse.*

PROOF. Let M be an integer such that $\sup_{x,y \in X} d(x, y) < M$. Suppose $\pi(\mu, \nu) < \epsilon/(M + 1)$. Then, by the coupling theorem(see [4]), for every $f \in 1 - \mathrm{Lip}(X)$ it holds $|\mu f - \nu f| \leq \epsilon$, hence $W(\mu, \nu) < \epsilon$. Conversely, suppose $W(\mu, \nu) < \epsilon^2 < 1$. Let A be a Borel set and define $g^A_\epsilon := |1 - d(x, A)/\epsilon|^+$. Then $\epsilon g^A_\epsilon \in 1 - \mathrm{Lip}(X)$. $W(\mu, \nu) < \epsilon^2$ implies $\mu\epsilon g^A_\epsilon < \nu\epsilon g^A_\epsilon + \epsilon^2$ and since $\mu(A) \leq \mu g^A_\epsilon$ and $\nu g^A_\epsilon \leq \nu(A^\epsilon)$, we conclude $\mu(A) \leq \nu(A^\epsilon) + \epsilon$ and then $\pi(\mu, \nu) < \epsilon$. Therefore, given a fast sequence of ideal measures converging to μ in the Prokhorov metric, we can construct a fast sequence of ideal measures converging to μ in the W metric and vice-versa.

This equivalence offers an alternative method to prove computability of measures. It is used for example in [14] to show the computability of *physical measures* (measures which are "physically relevent" in some sense, see [34] for precise definitions) for some classes of dynamical systems.

4.2. Measures as valuations

We now investigate the first problem: can the measure of sets be computed from the Cauchy description of a measure? Actually, the answer is positive for a very small part of the Borel sigma-field. It is a well-known fact that a Borel (probability) measure μ is characterized by the measure of open sets, which generate the Borel sigma-field. That is, by the valuation $v_\mu : \tau \to [0,1]$ which maps an open set to its μ-measure. A basic property of measures is continuity from below, which directly implies the Scott-continuity of v_μ (see Definition 3.1.3).

The question is then to study this characterization from a computability viewpoint. The first result is that the measure of open sets can be lower semi-computed, using the Cauchy description of the measure.

Proposition 4.2.1. *The valuation operator $v : \mathcal{M}(X) \times \tau \to [0,1]$ mapping (μ, U) to $\mu(U)$ is lower semi-computable.*

PROOF. as $v_\mu = v(\mu, .)$ is Scott-continuous, it suffices to show that it is uniformly lower semi-computable on finite unions of balls by Proposition 3.1.2

We first restrict to ideal measures μ_i: we have already seen (proof of Proposition 4.1.1) that all $\mu_i(B_{i_1} \cup \ldots \cup B_{i_k})$ are lower semi-computable real numbers, uniformly in $\langle i, i_1, \ldots, i_k \rangle$.

Now let $(\mu_{k_n})_{n\in\mathbb{N}}$ a description of a measure μ, that is a fast sequence converging to μ for the Prokhorov distance: then $\pi(\mu_{k_n}, \mu) \leq \epsilon_n$ where $\epsilon_n = 2^{-n+1}$. For $n \geq 1$, and $U = B(s_{i_1}, q_{j_1}) \cup \ldots \cup B(s_{i_k}, q_{j_k})$ define:

$$U_n = \bigcup_{m \leq k} B(s_{i_m}, q_{j_m} - \epsilon_n)$$

note that $U_{n-1}^{\epsilon_n} \subseteq U_n$ and $U_n^{\epsilon_n} \subseteq U$. We show that $\mu(U) = \sup_n(\mu_{j_n}(U_n) - \epsilon_n)$:

- $\mu_{j_n}(U_n) \leq \mu(U) + \epsilon_n$ for all n, so $\mu(U) \geq \sup_n(\mu_{j_n}(U_n) - \epsilon_n)$.
- $\mu(U_{n-1}) \leq \mu_{j_n}(U_n) + \epsilon_n$ for all n. As U_{n-1} increases towards U as $n \to \infty$, $\mu(U) = \sup_n(\mu(U_{n-1}) - 2\epsilon_n) \leq \sup_n(\mu_{j_n}(U_n) - \epsilon_n)$.

As the quantity $\mu_{j_n}(U_n) - \epsilon_n$ is lower semi-computable uniformly in n, we are done (observe that everything is uniform in the finite description of U).

The second result is stronger: the lower semi-computability of the measure of the r.e. open sets even characterizes the computability of the measure.

Theorem 4.2.1. *Given a measure $\mu \in \mathcal{M}(X)$, the following are equivalent:*

1. *μ is computable,*
2. *$v_\mu : \tau \to [0,1]$ is lower semi-computable,*
3. *$\mu(B_{i_1} \cup \ldots \cup B_{i_k})$ is lower semi-computable uniformly in $\langle i_1, \ldots, i_k \rangle$.*

PROOF. [1 $\Rightarrow$ 2] Direct from Proposition 4.2.1. [2 $\Rightarrow$ 3] Trivial. [3 $\Rightarrow$ 1] We show that $\pi(\mu_n, \mu)$ is upper semi-computable uniformly in n, and then use Proposition 2.4.2. Since $\pi(\mu_n, \mu) < \epsilon$ iff $\mu_n(A) < \mu(A^\epsilon) + \epsilon$ for all $A \subset S_n$ where S_n is the finite support of μ_n, and $\mu(A^\epsilon)$ is lower semi-computable (A^ϵ is a finite union of open ideal balls) $\pi(\mu_n, \mu) < \epsilon$ is semi-decidable, uniformly in n and ϵ. This allows to construct a fast sequence of ideal measures converging to μ.

It means that a representation which would be “tailor-made” to make the valuation constructive, describing a measure μ by the set of integers $\langle i_1, \ldots, i_k, j\rangle$ satisfying $\mu(B_{i_1} \cup \ldots \cup B_{i_k}) > q_j$, would be constructively equivalent to the Cauchy representation. This is the approach taken in [31] for the special case $X = [0, 1]$ and in [27] on an arbitrary sequential topological space. In both case, the topology on $\mathcal{M}(X)$ induced by this representation is proved to be equivalent to the weak topology. A domain theoretical approach was also developed in [9] on a compact space, the Scott topology being proved to induce the weak topology.

In [35] the measure of finite union of basic balls is assumed to be computable in order to prove the existence of a universal randomness test. The results stated above show that this assumption is at first sight too strong. Nevertheless we will see later in this section that it is still reasonable (corollary 5.2.1).

4.2.1. The examples of the Cantor space and the unit interval.

On the Cantor space $\Sigma^{\mathbb{N}}$ (where Σ is a finite alphabet) with its natural computable metric space structure, the ideal balls are the cylinders. As a finite union of cylinders can always be expressed as a disjoint (and finite) union of cylinders, and the complement of a cylinder is a finite union of cylinders, we get the notion of computable measure that is usually used on the Cantor space (in [26] for instance):

Corollary 4.2.1. *A measure $\mu \in \mathcal{M}(\Sigma^{\mathbb{N}})$ is computable iff the measures of the cylinders are uniformly computable.*

On the unit real interval, ideals balls are open rational intervals. Again, a finite union of such intervals can always be expressed as a disjoint (and finite) union of open rational intervals. Then:

Corollary 4.2.2. *A measure $\mu \in \mathcal{M}([0, 1])$ is computable iff the measures of the rational open intervals are uniformly lower semi-computable.*

If μ has no atoms, a rational open interval is the complement of at most two disjoint open rational intervals, up to a null set. In this case, μ is then computable iff the measures of the rational intervals are uniformly *computable.*

4.3. Measures as integrals

We now answer the second question: is the integral of functions computable from the description of a measure ?

The computable metric space structure of X and the enumerative lattice structure of $\overline{\mathbb{R}}^+$ induce in a canonical way the enumerative lattice $\mathcal{C}(X, \overline{\mathbb{R}}^+)$ (see Section 3.2), which is actually the set of lower semi-continuous functions from X to $\overline{\mathbb{R}}^+$. We have:

Proposition 4.3.1. *The integral operator $\int : \mathcal{M}(X) \times \mathcal{C}(X, \overline{\mathbb{R}}^+) \to \overline{\mathbb{R}}^+$ is lower semi-computable.*

Proof. the integral of a finite supremum of step functions can be expressed by induction on the number of functions: first, $\int f_{\langle i,j\rangle}\,\mathrm{d}\mu = q_j\mu(B_i)$ and

$$\begin{aligned}\int \sup\{f_{\langle i_1,j_1\rangle},\ldots,f_{\langle i_k,j_k\rangle}\}\,\mathrm{d}\mu &= q_{j_m}\mu(B_{i_1}\cup\ldots\cup B_{i_k}) + \\ &\qquad \int \sup\{f_{\langle i_1,j'_1\rangle},\ldots,f_{\langle i_k,j'_k\rangle}\}\,\mathrm{d}\mu\end{aligned}$$

where q_{j_m} is minimal among $\{q_{j_1},\ldots,q_{j_k}\}$ and $q_{j'_1} = q_{j_1} - q_{j_m}, q_{j'_2} = q_{j_2} - q_{j_m}$, *etc.* Note that $f_{\langle i_m,j'_m\rangle}$ being the zero function can be removed.

Now, m can be computed and by Proposition 4.2.1 the measure of finite unions of ideal balls can be uniformly μ-lower semi-computed, so the integral above can be uniformly μ-lower semi-computed. For any fixed measure μ, the integral operator $\int \mathrm{d}\mu : \mathcal{C}(X,\overline{\mathbb{R}}^+) \to \overline{\mathbb{R}}^+$ is Scott-continuous, so it is lower semi-computable.

Again, the lower semi-computability of the integral of lower semi-computable functions characterizes the computability of the measure:

Corollary 4.3.1. *Given a measure $\mu \in \mathcal{M}(X)$, the following are equivalent:*

1. *μ is computable,*
2. *$\int \mathrm{d}\mu : \mathcal{C}(X,\overline{\mathbb{R}}^+) \to \overline{\mathbb{R}}^+$ is lower semi-computable,*
3. *$\int \sup\{f_{i_1},\ldots,f_{i_k}\}\,\mathrm{d}\mu$ is lower semi-computable uniformly in $\langle i_1,\ldots,i_k\rangle$.*

Proof. [2 $\Leftrightarrow$ 3] holds by Scott-continuity of the operator,

[1 $\Rightarrow$ 2] is a direct consequence of proposition 4.3.1,

[2 $\Rightarrow$ 1] is a direct consequence of Theorem 4.2.1, composing the integral operator with the function from τ to $\mathcal{C}(X,\overline{\mathbb{R}}^+)$ mapping an open set to its indicator function (which is computable, see Proposition 3.3.1).

It means that a representation of measures which would be "tailor-made" to make the integration constructive, describing a measure by the set of integers $\langle i_1,\ldots,i_k,j\rangle$ satisfying $\int \sup\{f_{i_1},\ldots,f_{i_k}\}\,\mathrm{d}\mu > q_j$, would be constructively equivalent to the Cauchy representation.

Proposition 4.3.1 directly implies the following result, which will be used in the last section.

Corollary 4.3.2. *Let $(f_i)_i$ be a sequence of uniformly computable functions, i.e. such that the function $(i,x) \mapsto f_i(x)$ is computable. If moreover f_i has a bound M_i computable uniformly in i, then the function $(\mu,i) \to \int f_i\,\mathrm{d}\mu$ is computable.*

Proof. $f_i + M_i$ and $M_i - f_i$ are uniformly lower semi-computable, so $\int f_i\,\mathrm{d}\mu = \int (f_i+M_i)\,\mathrm{d}\mu - M_i = M_i - \int (M_i - f_i)\,\mathrm{d}\mu$ is both lower and upper-computable by Proposition 4.3.1 allow to conclude.

5. Computable Probability Spaces

The representation induced by the binary numeral system of real numbers is generally presented as not adequate for computability purposes since simple functions as $x \mapsto 3x$ are not computable with respect to it. This lies in the fact that the real interval and the space of sequences are not homeomorphic.

On the other hand, if we are insterested in probabilistic issues, the binary representation is actually suitable, and may even be preferred: almost every real has a unique binary expansion.

More generally, computability notions from computable analysis are effective versions of topological ones (semi-decidable sets are open, computable functions are continuous, etc). What about effective versions of measure-theoretical/probabilistic notions?

In this section we study a computable version of probability spaces, that is, metric spaces equipped with a fixed computable Borel probability measure. This will give us a framework allowing to talk about *almost everywhere* computability or decidability notions. Let us then introduce:

Definition 5.0.1. A ***computable probability space*** is a pair $(\mathcal{X}, \mu)$ where $\mathcal{X}$ is a computable metric space and μ a computable Borel probability measure on X.

On a computable probability space a natural idea is to require functions to be computable *almost everywhere*, i.e. on a full-measure set. Let us assume that the measure is supported on the whole space. By Theorem 3.3.1 any function which is computable on a full-measure (hence dense) set can be extended to a function which is computable on a full-measure constructive G_δ-set (actually, the assumption about the support of the measure is not necessary, as one can first restrict the function to the support of the measure, see [20] for more details).

From this argument, the following definition is in a sense as general as requiring a function to be computable almost everywhere. As we will see in the last section, its advantage is that such a function behaves well on Martin-Löf random points.

Definition 5.0.2. Let $(\mathcal{X}, \mu)$ be a computable probability space and $\mathcal{Y}$ a computable metric space. A function $f :\subset (\mathcal{X}, \mu) \to Y$ is ***almost computable*** if it is computable on a constructive G_δ-set (denoted as D_f) of measure one.

Example1. Let m be the Lebesgue measure on $[0, 1]$. The binary expansion of reals defines a function from non-dyadic numbers to infinite binary sequences which induces an almost computable function from $([0, 1], m)$ to $\{0, 1\}^{\mathbb{N}}$.

Remark 5.0.1. Given a uniform sequence of almost computable functions $(f_i)_i$, any computable operation $\odot_{i=0}^{n} f_i$ (adition, multiplication, composition, etc...) is almost computable too, uniformly in n.

We recall that $F : (\mathcal{X}, \mu) \to (\mathcal{Y}, \nu)$ is measure-preserving if $\mu(F^{-1}(A)) = \nu(A)$ for all Borel sets A.

Definition 5.0.3. A ***morphism of computable probability spaces*** $F : (\mathcal{X}, \mu) \to (\mathcal{Y}, \nu)$, is an almost computable measure-preserving function $F : D_F \subseteq X \to Y$.

An ***isomorphism*** $(F, G) : (\mathcal{X}, \mu) \rightleftarrows (\mathcal{Y}, \nu)$ is a pair (F, G) of morphisms such that $G \circ F = id$ on $F^{-1}(D_G)$ and $F \circ G = id$ on $G^{-1}(D_F)$.

Example2. Let $(\{0,1\}^{\mathbb{N}}, \lambda)$ be the Cantor space with the uniform measure. The binary expansion (see example 1) creates an isomorphism of computable probability spaces between the spaces $([0,1], m)$ and $(\{0,1\}^{\mathbb{N}}, \lambda)$.

Remark 5.0.2. To every isomorphism of computable probability spaces (F, G) one can associate the canonical invertible morphism $\varphi = F|_{D_\varphi}$ with $\varphi^{-1} = G|_{D_{\varphi^{-1}}}$, where $D_\varphi = F^{-1}(G^{-1}(D_F))$ and $D_{\varphi^{-1}} = G^{-1}(D_F)$. Of course, (φ, φ^{-1}) is an isomorphism of CPS's as well.

5.1. Generalized binary representations

The Cantor space $\{0,1\}^{\mathbb{N}}$ is a privileged place for computability. This can be understood by the fact that it is the countable product (with the product topology) of a finite space (with the discrete topology). A consequence of this is that membership of a basic open set (cylinder) boils down to a pattern-matching and is then *decidable*. As decidable sets must be clopen, this property cannot hold in connected spaces. As a result, a computable metric space is not in general constructively homeomorphic to the Cantor space.

Nevertheless, the real unit interval $[0,1]$ is not so far away from the Cantor space. The binary numeral system provides a correspondence between real numbers and binary sequences, which is certainly not homeomorphic, unless we remove the small set of dyadic numbers. In particular, the remaining set is totally disconnected, and the dyadic intervals form a basis of clopen sets.

Actually, this correspondence makes the computable probability space $[0,1]$ with the Lebesgue measure isomorphic to the Cantor space with the uniform measure. This fact has been implicitly used, for instance, to extend algorithmic randomness from the Cantor space with the uniform measure to Euclidean spaces with the Lebesgue measure (see [25] for instance).

We generalize this to any computable probability space, over which we define the notion of *binary representation*. We show that every computable probability space has a binary representation. This implies, in particular, that every computable probability space is isomorphic to the Cantor space with a computable measure. To carry out this generalization, let us briefly scrutinize the binary numeral system on the unit interval:

$\delta : \{0,1\}^{\mathbb{N}} \to [0,1]$ is a total surjective morphism. Every non-dyadic real has a unique expansion, and the inverse of δ, defined on the set D of non-dyadic numbers, is computable. Moreover, D is large both in a topological and measure-theoretical sense: it is a residual (a countable intersection of dense open sets) and has measure one. (δ, δ^{-1}) is then an isomorphism.

In our generalization, we do not require every binary sequence to be the expansion of a point, which would force X to be compact.

Definition 5.1.1. A ***binary representation*** of a computable probability space $(\mathcal{X}, \mu)$ is a pair (δ, μ_δ) where μ_δ is a computable probability measure on $\{0,1\}^{\mathbb{N}}$ and $\delta : (\{0,1\}^{\mathbb{N}}, \mu_\delta) \to (\mathcal{X}, \mu)$ is a surjective morphism such that, calling $\delta^{-1}(x)$ the set of ***expansions*** of $x \in X$:

- there is a dense full-measure constructive G_δ-set D of points having a unique expansion,
- $\delta^{-1} : D \to \delta^{-1}(D)$ is computable.

Observe that when the support of the measure (the smallest closed set of full measure) is the whole space X, like the Lebesgue measure on the interval, a full-measure constructive G_δ-set is always a residual, but in general it is only dense on the support of the measure: that is the reason why we explicitly require D to be dense. Also observe that a binary representation δ always induces an isomorphism (δ, δ^{-1}) between the Cantor space and the computable probability space.

The sequel of this section is devoted to the proof of the following result:

Theorem 5.1.1. *Every computable probability space $(\mathcal{X}, \mu)$ has a binary representation.*

The space, restricted to the domain D of the isomorphism, is then totally disconnected: the preimages of the cylinders form a basis of clopen and even *decidable* sets. In the whole space, they are not decidable any more. Instead, they are *almost decidable.*

In particular, this theorem implies the existence of a cell decomposition of the space (as defined in [13]) for *every* computable probability measure.

Definition 5.1.2. A set A is said to be ***almost decidable*** if there are two r.e. open sets U and V such that:

$$U \subset A, \quad V \subseteq A^{\mathcal{C}}, \quad U \cup V \text{ is dense and has measure one}$$

Definition 5.1.3. A measurable set A is said to be ***μ-continuous*** or a ***μ-continuity set*** if $\mu(\partial A) = 0$ where $\partial A = \overline{A} \cap \overline{X \setminus A}$ is the boundary of A.

Observe that a set is almost decidable if and only if its complement is almost decidable. This is the analogue that a subset of $\mathbb{N}$ is decidable if and only if its complement is decidable. An almost decidable set is always a continuity set. Let $B(s,r)$ be a μ-continuous ball with computable radius: in general it is not an almost decidable set (for instance, isolated points may be at distance exactly r from s). But if there is no ideal point is at distance r from s, then $B(s,r)$ is almost decidable: take $U = B(s,r)$ and $V = X \setminus \overline{B}(s,r)$.

We say that the elements of a sequence $(A_i)_{i\in\mathbb{N}}$ are uniformly almost decidable if there are two sequences $(U_i)_{i\in\mathbb{N}}$ and $(V_i)_{i\in\mathbb{N}}$ of uniformly r.e. sets satisfying the conditions above.

Lemma 5.1.1. *There is a sequence $(r_n)_{n\in\mathbb{N}}$ of uniformly computable reals such that $(B(s_i, r_n))_{\langle i,n\rangle}$ is a basis of uniformly almost decidable balls.*

To prove this we will use the computable Baire Category Theorem (proved in [33], [5]), applied to the set of real numbers.

Theorem 5.1.2 (Computable Baire theorem). *On a computable metric space, every dense constructive G_δ-set contains a dense sequence of uniformly computable points.*

Proof. Let $A = \bigcap_i U_i$ where U_i is constructive uniformly in i. Let B be an ideal ball: we construct a sequence of ideal balls $(B(i))_i$ such that $\overline{B}(i+1) \subseteq U_i \cap B(i)$. Put $B(0) = B$. If $B(i)$ has been constructed, as U_i is dense $B(i) \cap U_i$ is a non-empty open set, so we can find some ball $B' \subseteq B(i) \cap U_i$. $B(i+1)$ is obtained dividing the radius of $B'$by 2. By completeness of the space $\bigcap_i B(i)$ is non-empty. It is even a singleton $\{x\}$ where x is a computable point which, of course, belongs to $A \cap B$.

As everything is uniform in the ideal ball B, the numbering $(B_k)_k$ of ideal balls gives a constructive sequence $(x_k)_k$ of uniformly computable points with $x_k \in A \cap B_k$.

Now we can prove the lemma.

Proof. define $U_{\langle i,k\rangle} = \{r \in \mathbb{R}^+ : \mu(\overline{B}(s_i, r)) < \mu(B(s_i, r)) + 1/k\}$: by computability of μ, this is a r.e open subset of $\mathbb{R}^+$, uniformly in $\langle i, k\rangle$. It is furthermore dense in $\mathbb{R}^+$: the spheres $S_r = \overline{B}(s_i, r) \setminus B(s_i, r)$ are disjoint for different radii and μ is finite, so the set of r for which $\mu(S_r) \geq 1/k$ is finite.

Define $V_{\langle i,j\rangle} = \mathbb{R}^+ \setminus \{d(s_i, s_j)\}$: this is a dense r.e open set, uniformly in $\langle i, j\rangle$.

Then by the computable Baire Theorem, the dense constructive G_δ-set

$$\bigcap_{\langle i,k\rangle} U_{\langle i,k\rangle} \cap \bigcap_{\langle i,j\rangle} V_{\langle i,j\rangle}$$

contains a sequence $(r_n)_{n\in\mathbb{N}}$ of uniformly computable real numbers which is dense in $\mathbb{R}^+$. In other words, all r_n are computable, uniformly in n. By construction, for any s_i and r_n, $B(s_i, r_n)$ is almost decidable.

We will denote $B(s_i, r_n)$ by B^μ_k where $k = \langle i, n\rangle$. Note that different algorithmic descriptions of the same μ may yield different sequences $(r_n)_{n\in\mathbb{N}}$, so B^μ_k is an abusive notation. It is understood that some algorithmic description of μ has been chosen and fixed. This can be done only because the measure μ is computable, which is then a crucial hypothesis. We denote $X \setminus \overline{B}(s_i, r_n)$ by C^μ_k and define:

Definition 5.1.4. For $w \in \{0, 1\}^*$, the ***cell*** $\Gamma(w)$ is defined by induction on $|w|$:

$$\Gamma(\epsilon) = X, \quad \Gamma(w0) = \Gamma(w) \cap C^\mu_i \quad \text{and} \quad \Gamma(w1) = \Gamma(w) \cap B^\mu_i$$

where ϵ is the empty word and $i = |w|$.

This an almost decidable set, uniformly in w.

PROOF. (of Theorem 5.1.1). We construct an encoding function $b : D \to \{0,1\}^{\mathbb{N}}$, a decoding function $\delta : D_\delta \to X$, and show that δ is a binary representation, with $b = \delta^{-1}$.

Encoding.

Let $D = \bigcap_i B_i^\mu \cup C_i^\mu$: this is a dense full-measure constructive G_δ-set. Define the computable function $b : D \to \{0,1\}^{\mathbb{N}}$ by:

$$b(x)_i = \begin{cases} 1 & \text{if } x \in B_i^\mu \\ 0 & \text{if } x \in C_i^\mu \end{cases}$$

Let $x \in D$: $\omega = b(x)$ is also characterized by $\{x\} = \bigcap_i \Gamma(\omega_{0..i-1})$. Let μ_δ be the image measure of μ by b: $\mu_\delta = \mu \circ b^{-1}$. b is then a morphism from (X, μ) to $(\{0,1\}^{\mathbb{N}}, \mu_\delta)$.

Decoding.

Let D_δ be the set of binary sequences ω such that $\bigcap_i \overline{\Gamma(\omega_{0..i-1})}$ is a singleton. We define the decoding function $\delta : D_\delta \to X$ by:

$$\delta(\omega) = x \text{ if } \bigcap_i \overline{\Gamma(\omega_{0..i-1})} = \{x\}$$

ω is called an expansion of x. Observe that $x \in B_i^\mu \Rightarrow \omega_i = 1$ and $x \in C_i^\mu \Rightarrow \omega_i = 0$, which implies in particular that if $x \in D$, x has a unique expansion, which is $b(x)$. Hence, $b = \delta^{-1} : \delta^{-1}(D) \to D$ and $\mu_\delta(D_\delta) = \mu(D) = 1$.

We now show that $\delta : D_\delta \to X$ is a surjective morphism. For the sake of clarity, the center and the radius of the ball B_i^μ will be denoted s_i and r_i respectively. Let us call i an *n-witness* for ω if $r_i < 2^{-(n+1)}, \omega_i = 1$ and $\Gamma(\omega_{0..i}) \neq \emptyset$.

• D_δ is a constructive G_δ-set: we show that $D_\delta = \bigcap_n \{\omega \in \{0,1\}^{\mathbb{N}} : \omega$ has a n-witness$\}$.

Let $\omega \in D_\delta$ and $x = \delta(\omega)$. For each n, $x \in B(s_i, r_i)$ for some i with $r_i < 2^{-(n+1)}$. Since $x \in \overline{\Gamma(\omega_{0..i})}$, we have that $\Gamma(\omega_{0..i}) \neq \emptyset$ and $\omega_i = 1$ (otherwise $\overline{\Gamma(\omega_{0..i})}$ is disjoint from B_i^μ). In other words, i is an n-witness for ω.

Conversely, if ω has a n-witness i_n for all n, since $\overline{\Gamma(\omega_{0..i_n})} \subseteq \overline{B_{i_n}^\mu}$ whose radius tends to zero, the nested sequence $(\overline{\Gamma(\omega_{0..i_n})})_n$ of closed cells has, by completeness of the space, a non-empty intersection, which is a singleton.

• $\delta : D_\delta \to X$ is computable. For each n, find some n-witness i_n of ω: the sequence $(s_{i_n})_n$ is a fast sequence converging to $\delta(\omega)$.

• δ is surjective: we show that each point $x \in X$ has at least one expansion. To do this, we construct by induction a sequence $\omega = \omega_0\omega_1\dots$ such that for all i, $x \in \overline{\Gamma(\omega_0 \dots \omega_i)}$. Let $i \geq 0$ and suppose that $\omega_0 \dots \omega_{i-1}$ (empty when $i = 0$) has been constructed. As $B_i^\mu \cup C_i^\mu$ is open dense and $\Gamma(\omega_{0..i-1})$ is open, $\overline{\Gamma(\omega_{0..i-1})} = \overline{\Gamma(\omega_{0..i-1}) \cap (B_i^\mu \cup C_i^\mu)}$ which equals $\overline{\Gamma(\omega_{0..i-1}0)} \cup \overline{\Gamma(\omega_{0..i-1}1)}$. Hence, one choice for $\omega_i \in \{0,1\}$ gives $x \in \overline{\Gamma(\omega_{0..i})}$.

By construction, $x \in \bigcap_i \overline{\Gamma(\omega_{0..i-1})}$. As $(B_i^\mu)_i$ is a basis and $\omega_i = 1$ whenever $x \in B_i^\mu$, ω is an expansion of x.

5.2. Another characterization of the computability of measures

The existence of a basis of almost decidable sets also leads to another characterization of the computability of measures, which is reminiscent of what happens on the Cantor space (see corollary 4.2.1). Let us say that a basis $(U_i)_i$ of the topology τ is constructively equivalent to the basis of ideal balls $\mathcal{B}$ if both $id_\tau : (\tau, \subseteq, \mathcal{B}) \to (\tau, \subseteq, \mathcal{U})$ and its inverse are constructive functions between enumerative lattices.

Corollary 5.2.1. *A measure $\mu \in \mathcal{M}(X)$ is computable if and only if there is a basis $\mathcal{U} = (U_i)_{i\in\mathbb{N}}$ of uniformly almost decidable open sets which is constructively equivalent to $\mathcal{B}$ and such that all $\mu(U_{i_1} \cup \ldots \cup U_{i_k})$ are computable uniformly in $\langle i_1, \ldots, i_k\rangle$.*

Proof. if μ is computable, the decidable balls $U_{\langle i,n\rangle} = B(s_i, r_n)$ are basis which is constructively equivalent to $\mathcal{B}$: indeed, $B(s_i, r_n) = \bigcup_{q_j<r_n} B(s_i, q_j)$ and $B(s_i, q_j) = \bigcup_{r_n<q_j} B(s_i, r_n)$, and r_n is computable uniformly in n.

For the converse, the valuation function f_μ is lower semi-computable. Indeed, the r.e open sets are uniformly r.e relatively to the basis $\mathcal{U}$, so their measures can be lower semi-computed, computing the measures of finite unions of elements of $\mathcal{U}$. Hence μ is computable by Theorem 4.2.1.

This result shows that the assumption on the measure used in [35] (namely the measures of finite unions of basic open sets are computable) can always be achieved for a computable measure.

6. Algorithmic randomness

On the Cantor space with a computable measure μ, Martin-Löf originally defined the notion of an individual random sequence as a sequence passing all μ-randomness tests. A μ-randomness test *à la Martin-Löf* is a sequence of uniformly r.e. open sets $(U_n)_n$ satisfying $\mu(U_n) \leq 2^{-n}$. The set $\bigcap_n U_n$ has null measure, in an effective way: it is then called an effective null set.

Equivalently, a μ-randomness test can be defined as a positive lower semi-computable function $t : \{0,1\}^{\mathbb{N}} \to \mathbb{R}$ satisfying $\int t d\mu \leq 1$ (see [28] for instance). The associated effective null set is $\{x : t(x) = +\infty\} = \bigcap_n \{x : t(x) > 2^n\}$. Actually, every effective null set can be put in this form for some t. A point is then called μ-random if it lies in no effective null set.

Following Gács, we will use the second presentation of randomness tests which is more suitable to express uniformity.

6.1. Randomness w.r.t. any probability measure

Definition 6.1.1. Given a measure $\mu \in \mathcal{M}(X)$, a ***μ-randomness test*** is a μ-constructive element t of $\mathcal{C}(X, \overline{\mathbb{R}}^+)$, such that $\int t d\mu \leq 1$. Any subset of $\{x \in X : t(x) = +\infty\}$ is called a ***μ-effective null set***.

A ***uniform randomness test*** is a constructive function T from $\mathcal{M}(X)$ to $\mathcal{C}(X, \overline{\mathbb{R}}^+)$ such that for all $\mu \in \mathcal{M}(x)$, $\int T^\mu d\mu \leq 1$ where T^μ denotes $T(\mu)$.

Note that T can be also seen as a lower semi-computable function from $\mathcal{M}(X) \times X$ to $\overline{\mathbb{R}}^+$ (see Section 3.2).

A presentation *à la Martin-Löf* can be directly obtained using the constructive functions $F : \mathcal{C}(X, \overline{\mathbb{R}}^+) \to \tau^{\mathbb{N}}$ and $G : \tau^{\mathbb{N}} \to \mathcal{C}(X, \overline{\mathbb{R}}^+)$ defined by: $F(t)_n := t^{-1}(2^n, +\infty)$ and $G((U_n)_n)(x) := \sup\{n : x \in \bigcap_{i \leq n} U_i\}$. They satisfy $F \circ G = id : \tau^{\mathbb{N}} \to \tau^{\mathbb{N}}$ and preserve the corresponding effective null sets.

A uniform randomness test T induces a μ-randomness test T^μ for all μ. We show two important results which hold on any computable metric space:

- the two notions are actually equivalent (Theorem 6.1.1),
- there is a *universal* uniform randomness test (Theorem 6.1.2).

The second result was already obtained by Gács, but only on spaces which have recognizable Boolean inclusions, which is an additional computability property on the basis of ideal balls. Gács' idea was to use a basic set of computable functions $H_i : \mathcal{M}(X) \times X \to \overline{\mathbb{R}}^+$, and to check for each one if the following condition holds:

$$\sup_{\mu} \int H_i(\mu, .)\, \mathrm{d}\mu < 1. \tag{3}$$

As this cannot be tested in general, this led him to the need of the recognizable Boolean inclusions property[1].

Here, condition (3) is replaced by a condition which depends on μ: given μ as oracle, the algorithm tests $\int H_i(\mu, .)\, \mathrm{d}\mu < 1$ so that the decision of keeping H_i or not depends on μ. In a sense, instead of *checking* condition (3) we *build* a function that satisfies it.

By Proposition 3.2.2, constructive functions from $\mathcal{M}(X)$ to $\mathcal{C}(X, \overline{\mathbb{R}}^+)$ can be identified to constructive elements of the enumerative lattice $\mathcal{C}(\mathcal{M}(X), \mathcal{C}(X, \overline{\mathbb{R}}^+))$. Let $(H_i)_{i \in \mathbb{N}}$ be an enumeration of all its constructive elements (Proposition 3.1.1): $H_i = \sup_k f_{\varphi(i,k)}$ where $\varphi : \mathbb{N}^2 \to \mathbb{N}$ is some recursive function and the f_n are step functions.

Lemma 6.1.1. *There is a constructive function $T : \mathbb{N} \times \mathcal{M}(X) \to \mathcal{C}(X, \overline{\mathbb{R}}^+)$ satisfying:*

- *for all i, $T_i = T(i, .)$ is a uniform randomness test,*
- *if $\int H_i(\mu)\, \mathrm{d}\mu < 1$ for some μ, then $T_i(\mu) = H_i(\mu)$.*

Proof. To enumerate only tests, we would like to be able to semi-decide $\int \sup_{k<n} f_{\varphi(i,k)}(\mu)\, \mathrm{d}\mu < 1$. But $\sup_{k<n} f_{\varphi(i,k)}(\mu)$ is only lower semi-computable (from μ). To overcome this problem, we use another class of basic functions.

Let $\mathcal{Y}$ be a computable metric space: for an ideal point s of Y and positive rationals q, r, ϵ, define the *hat* function:

$$h_{q,s,r,\epsilon}(y) := q.[1 - [d(y, s) - r]^+/\epsilon]^+$$

[1] It can be shown that if X is compact in a constructive way then so is $\mathcal{M}(X)$, in which case the supremum over $\mathcal{M}(X)$ is computable. Actually, in this case X has recognizable Boolean inclusions.

where $[a]^+ = \max\{0, a\}$. This is a continuous function whose value is q in $B(s,r)$, 0 outside $B(s, r+\epsilon)$. The numberings of $\mathcal{S}$ and $\mathbb{Q}_{>0}$ induce a numbering $(h_n)_{n\in\mathbb{N}}$ of all the hat functions. They can be taken as an alternative to step functions in the enumerative lattice $\mathcal{C}(Y, \overline{\mathbb{R}}^+)$: they yield the same computable structure. Indeed, step functions can be constructively expressed as suprema of such functions: $f_{\langle i,j\rangle} = \sup\{h_{q_j,s,r-\epsilon,\epsilon} : 0 < \epsilon < r\}$ where $B_i = B(s,r)$, and conversely.

We apply this to $Y = \mathcal{M}(X) \times X$ endowed with the canonical computable metric structure. By Curryfication it provides functions $h_n \in \mathcal{C}(\mathcal{M}(X), \mathcal{C}(X, \overline{\mathbb{R}}^+))$ with which the H_i can be expressed: there is a recursive function $\psi : \mathbb{N}^2 \to \mathbb{N}$ such that for all i, $H_i = \sup_k h_{\psi(i,k)}$.

Furthermore, $h_n(\mu)$ (strictly speaking, $\mathrm{Eval}(h_n, \mu)$, see Proposition 3.2.3) is bounded by a constant computable from n and independent of μ. Hence, the integration operator $\int : \mathcal{M}(X) \times \mathbb{N} \to [0,1]$ which maps $(\mu, \langle i_1, \ldots, i_k\rangle)$ to $\int \sup\{h_{i_1}(\mu), \ldots, h_{i_k}(\mu)\}\,\mathrm{d}\mu$ is computable (Corollary 4.3.2).

We are now able to define T: $T(i,\mu) = \sup\{H_i^k(\mu) : \int H_i^k(\mu)\,\mathrm{d}\mu < 1\}$ where $H_i^k = \sup_{n<k} h_{\psi(i,n)}$. As $\int H_i^k(\mu)\,\mathrm{d}\mu$ can be computed from i, k and a description of μ, T is a constructive function from $\mathbb{N} \times \mathcal{M}(X)$ to $\mathcal{C}(X, \overline{\mathbb{R}}^+)$.

As a consequence, every randomness test for a particular measure can be extended to a uniform test:

Theorem 6.1.1 (Uniformity vs non-uniformity). *Let μ_0 be a measure. For every μ_0-randomness test t there is a uniform randomness test $T : \mathcal{M}(X) \to \mathcal{C}(X, \overline{\mathbb{R}}^+)$ with $T(\mu_0) = \frac{1}{2}t$.*

Proof. let μ_0 be a measure and t a μ_0-randomness test: $\frac{1}{2}t$ is then a μ_0-constructive element of the enumerative lattice $\mathcal{C}(X, \overline{\mathbb{R}}^+)$, so by lemma 3.2.1 there is a constructive element H of $\mathcal{C}(\mathcal{M}(X), \mathcal{C}(X, \overline{\mathbb{R}}^+))$ such that $H(\mu_0) = \frac{1}{2}t$. There is some i such that $H = H_i$: T_i is a uniform randomness test satisfying $T_i(\mu_0) = \frac{1}{2}t$ because $\int H_i(\mu_0)d\mu_0 = \frac{1}{2}\int t d\mu_0 < 1$.

Theorem 6.1.2 (Universal uniform test). *There is a universal uniform randomness test, that is a uniform test T_u such that for every uniform test T there is a constant c_T with $T_u \geq c_T T$.*

Proof. it is defined by $T_u := \sum_i 2^{-i-1} T_i$: as every T_i is a uniform randomness test, T_u is also a uniform randomness test, and if T is a uniform impossibility test, then in particular $\frac{1}{2}T$ is a constructive element of $\mathcal{C}(\mathcal{M}(X), \mathcal{C}(X, \overline{\mathbb{R}}^+))$, so $\frac{1}{2}T = H_i$ for some i. As $\int H_i(\mu)d\mu = \frac{1}{2}\int T(\mu)d\mu < 1$ for all μ, $T_i(\mu) = H_i(\mu) = \frac{1}{2}T(\mu)$ for all μ, that is $T_i = \frac{1}{2}T$. So $T_u \geq 2^{-i-2}T$.

Definition 6.1.2. Given a measure μ, a point $x \in X$ is called ***μ-random*** if $T_u^\mu(x) < \infty$. Equivalently, x is μ-random if it lies in no μ-effective null set.

The set of μ-random points is denoted by R_μ. This is the complement of the maximal μ-effective null set $\{x \in X : T_u^\mu(x) = +\infty\}$.

6.2. Randomness on a computable probability space

We study the particular case of a computable measure. As a morphism of computable probability spaces is compatible with measures and computability structures, it shall be compatible with algorithmic randomness. Indeed:

Proposition 6.2.1. *Morphisms of computable probability spaces are defined on random points and preserve randomness.*

To prove it, we shall use the following lemma. This was proved in [24] on the Cantor space. On computable metric spaces, the proof must be slightly adapted as the measure of ideal balls is not computable in general.

Lemma 6.2.1. *In a computable probability space $(\mathcal{X}, \mu)$, every random point lies in every r.e. open set of full measure.*

Proof. let $U = \bigcup_{\langle i,j\rangle \in E} B(s_i, q_j)$ be a r.e. open set of measure one, with E a r.e. subset of $\mathbb{N}$. Let F be the r.e. set $\{\langle i,k\rangle : \exists j, \langle i,j\rangle \in E, q_k < q_j\}$. Define:

$$U_n = \bigcup_{\langle i,k\rangle \in F\cap[0,n]} B(s_i, q_k) \quad \text{and} \quad V_n^{\mathcal{C}} = \bigcup_{\langle i,k\rangle \in F\cap[0,n]} \overline{B}(s_i, q_k)$$

Then U_n and V_n are r.e. uniformly in n, $U_n \nearrow U$ and $U^{\mathcal{C}} = \bigcap_n V_n$. As $\mu(U_n)$ is lower semi-computable uniformly in n, a sequence $(n_i)_{i\in\mathbb{N}}$ can be computed such that $\mu(U_{n_i}) > 1 - 2^{-i}$. Then $\mu(V_{n_i}) < 2^{-i}$, and $U^{\mathcal{C}} = \bigcap_i V_{n_i}$ is a μ-Martin-Löf test. Therefore, every μ-random point is in U.

Proof. (of Proposition 6.2.1) let $(\mathcal{X}, \mu)$ and $(\mathcal{Y}, \nu)$ be computable probability spaces and $F : D \subseteq X \to Y$ a morphism. From Lemma 6.2.1, every random point is in D which is an intersection of full-measure r.e open sets.

Let $t : Y \to \overline{\mathbb{R}}^+$ be the universal ν-test. The function $t \circ F : D \to \overline{\mathbb{R}}^+$ is lower semi-computable. Let $\mathcal{A}$ be any algorithm lower semi-computing it: the associated lower semi-computable function $f_{\mathcal{A}} : X \to \overline{\mathbb{R}}^+$ extends $t \circ F$ to the whole space X (see Lemma 3.2.1). As $\mu(D) = 1$, $\int t \circ F d\mu$ is well defined and equals $\int f_{\mathcal{A}} d\mu$. As F is measure-preserving, $\int t \circ F d\mu = \int t d\nu \leq 1$. Hence $f_{\mathcal{A}}$ is a μ-test. Let $x \in X$ be a μ-random point: as $x \in D$, $t(F(x)) = f_{\mathcal{A}}(x) < +\infty$, so $F(x)$ is ν-random.

The following statement is implicitely present in [35] and [21] on the Cantor space.

Corollary 6.2.1. *Let $(F, G) : (\mathcal{X}, \mu) \rightleftarrows (\mathcal{Y}, \nu)$ be an isomorphism of computable probability spaces. Then $F_{|R_\mu}$ and $G_{|R_\nu}$ are total computable bijections between R_μ and R_ν, and $(F_{|R_\mu})^{-1} = G_{|R_\nu}$.*

In particular:

Corollary 6.2.2. *Let δ be a binary representation on a computable probability space $(\mathcal{X}, \mu)$. Each point having a μ_δ-random expansion is μ-random and each μ-random point has a unique expansion, which is μ_δ-random.*

This proves that algorithmic randomness over a computable probability space could have been defined encoding points into binary sequences using a binary representation: this would have led to the same notion of randomness. Using this principle, a notion of Kolmogorov complexity characterizing Martin-Löf randomness comes for free. This was already done in [13] assuming (i) the existence of a cell decomposition of the space and (ii) that the space is compact, in a constructive way. For $x \in D$, define:

$$H_n(x) = H(\omega_{0..n-1}) \text{ and } \Gamma_n(x) = \delta([\omega_{0..n-1}])$$

where ω is the expansion of x and H is the prefix Kolmogorov-Chaitin complexity.

Corollary 6.2.3. *Let δ be a binary representation on a computable probability space $(\mathcal{X}, \mu)$. Then x is μ-random if and only if there is c such that for all n:*

$$H_n(x) \geq -\log \mu(\Gamma_n(x)) - c$$

All this allows to treat algorithmic randomness within probability theory over general metric spaces. In [15] for instance, it is applied to show that in ergodic systems over metric spaces, algorithmically random points are well-behaved: they are *typical* with respect to any ergodic endomorphism of computable probability space, generalizing what has been proved in [29] for the Cantor space.

Acknowledgements

We would like to thank Stefano Galatolo, Peter Gács, Giuseppe Longo and the anonymous referees for useful comments and remarks.

References

[1] Abramsky, S., Jung, A., 1994. Domain theory. In: Abramsky, S., Gabbay, D., Maibaum, T. S. E. (Eds.), Handbook of Logic in Computer Science Volume 3. Oxford University Press, pp. 1–168.
URL `citeseer.ist.psu.edu/abramsky94domain.html`

[2] Ambrosio, L., Gigli, N., Savaré, G., 2005. Gradient flows: in metric spaces and in the space of probability measures. Birkhauser, Zürich.

[3] Asarin, E., Prokovskii, A., 1986. Use of the kolmogorov complexity in analyzing control system dynamics. Automation and Remote Control 47, 21–28.

[4] Billingsley, P., 1968. Convergence of Probability Measures. John Wiley, New York.

[5] Brattka, V., 2001. Computable versions of baire's category theorem. In: MFCS '01: Proceedings of the 26th International Symposium on Mathematical Foundations of Computer Science. Springer-Verlag, London, UK, pp. 224–235.

[6] Brattka, V., Presser, G., 2003. Computability on subsets of metric spaces. Theoretical Computer Science 305, 43–76.

[7] Brattka, V., Weihrauch, K., 1999. Computability on subsets of euclidean space i: Closed and compact subsets. Theoretical Computer Science 219 (1-2), 65–93.

[8] Brodhead, P., Cenzer, D., Dashti, S., 2006. Random closed sets. In: CiE. pp. 55–64.

[9] Edalat, A., 1996. The Scott topology induces the weak topology. In: LICS '96: Proceedings of the 11th Annual IEEE Symposium on Logic in Computer Science. IEEE Computer Society, Washington, DC, USA, p. 372.

[10] Edalat, A., Heckmann, R., 1998. A computational model for metric spaces. Theoretical Computer Science 193, 53–73.

[11] Fouché, W. L., 2000. Arithmetical representations of brownian motion i. Journal of Symbolic Logic 65 (1), 421–442.

[12] Fouché, W. L., 2008. Dynamics of a generic brownian motion: Recursive aspects. Theoretical Computer Science 394 (3), 175–186.

[13] Gács, P., 2005. Uniform test of algorithmic randomness over a general space. Theoretical Computer Science 341, 91–137.

[14] Galatolo, S., Hoyrup, M., Rojas, C., 2007. A constructive Borel-Cantelli lemma. Constructing orbits with required statistical properties. To appear in Theoretical Computer Science.
URL http://arxiv.org/abs/0709.0907

[15] Galatolo, S., Hoyrup, M., Rojas, C., 2007. Effective symbolic dynamics, random points, statistical behavior, complexity and entropy. Submitted.
URL http://arxiv.org/abs/0801.0209

[16] Hartley Rogers, J., 1987. Theory of Recursive Functions and Effective Computability. MIT Press, Cambridge, MA, USA.

[17] Hemmerling, A., 2002. Effective metric spaces and representations of the reals. Theor. Comput. Sci. 284 (2), 347–372.

[18] Hertling, P., Weihrauch, K., 1998. Randomness spaces. In: Larsen, K. G., Skyum, S., Winskel, G. (Eds.), Automata, Languages and Programming. Vol. 1443 of Lecture Notes in Computer Science. Springer, Berlin, pp. 796–807, 25th International Colloquium, ICALP'98, Aalborg, Denmark, July 1998.

[19] Hertling, P., Weihrauch, K., 2003. Random elements in effective topological spaces with measure. Information and Computation 181 (1), 32–56.

[20] Hoyrup, M., 2008. Computability, Randomness and Ergodic Theory on metric spaces. Ph.D. thesis, Université Denis Diderot, Paris.

[21] Kautz, S., 1991. Degrees of random sets. Ph.D. thesis, Cornell.

[22] Ko, K.-I., 1991. Complexity Theory of Real Functions. Birkhauser Boston Inc., Cambridge, MA, USA.

[23] Ko, K.-I., Friedman, H., 1982. Computational complexity of real functions. Theoretical Computer Science 20 (3), 323–352.

[24] Kurtz, S., 1981. Randomness and genericity in the degrees of unsolvability. Ph.D. thesis, University of Illinois at Urbana.

[25] Lutz, J. H., Weihrauch, K., 2008. Connectivity properties of dimension level sets. Electronic Notes in Theoretical Computer Science 202, 295–304.

[26] Martin-Löf, P., 1966. The definition of random sequences. Information and Control 9 (6), 602–619.

[27] Schröder, M., 2007. Admissible representations of probability measures. Electronic Notes in Theoretical Computer Science 167, 61–78.

[28] Vovk, V., Vyugin, V., 1993. On the empirical validity of the bayesian method. Journal of the Royal Statistical Society B 55 (1), 253–266.

[29] V'yugin, V. V., 1997. Effective convergence in probability and an ergodic theorem for individual random sequences. SIAM Theory of Probability and Its Applications 42 (1), 39–50.

[30] Weihrauch, K., 1993. Computability on computable metric spaces. Theoretical Computer Science 113, 191–210, fundamental Study.

[31] Weihrauch, K., 1999. Computability on the probability measures on the Borel sets of the unit interval. Theoretical Computer Science 219, 421–437.

[32] Weihrauch, K., 2000. Computable Analysis. Springer, Berlin.

[33] Yasugi, M., Mori, T., Tsujii, Y., 1999. Effective properties of sets and functions in metric spaces with computability structure. Theoretical Computer Science 219 (1-2), 467–486.

[34] Young, L.-S., 2002. What are SRB measures, and which dynamical systems have them? J. Stat. Phys. 108, 733–754.

[35] Zvonkin, A., Levin, L., 1970. The complexity of finite objects and the development of the concepts of information and randomness by means of the theory of algorithms. Russian Mathematics Surveys 256, 83–124.