UNIVERSITE PARIS.
DIDEROT (Paris 7)

UNIVERSITÀ
DI PISA

Ecole Doctorale de Sciences Mathématiques de Paris Centre

Doctorat en informatique

–

Mathieu HOYRUP

Calculabilité, aléatoire et théorie ergodique sur les espaces métriques

Calcolabilità, aleatorio e teoria ergodica in spazi metrici

–

Thèse dirigée par

Giuseppe LONGO / Stefano GALATOLO

Soutenue le 17 juin 2008

Rapporteurs

Olivier BOURNEZ
Abbas EDALAT
Peter GÁCS

JURY

Olivier BOURNEZ	rapporteur
Roberto DI COSMO	président
Abbas EDALAT	rapporteur
Bassam FAYAD	examinateur
Stefano GALATOLO	directeur
Giuseppe LONGO	directeur

Remerciements

Je tiens tout d'abord à remercier Giuseppe Longo d'avoir encadré cette thèse. Merci pour le rôle essentiel qu'il a joué dans mon éducation scientifique, pour ses encouragements constants et sa confiance. Merci à Stefano Galatolo d'avoir co-dirigé cette thèse, de m'avoir tant apporté dans mon apprentissage de la théorie ergodique, et de m'avoir appris qu'il arrive un moment où il faut arrêter de retoucher les articles et les soumettre.

Merci aux membres du jury: à Olivier Bournez et Abbas Edalat d'avoir accepté, en plus d'être rapporteurs, de faire le déplacement pour la soutenance, à Roberto Di Cosmo d'avoir bien voulu présider le jury, à Bassam Fayad d'avoir accepté d'en faire partie.

Merci à Peter Gács d'avoir accepté d'être rapporteur, merci pour sa visite à Paris et pour l'intérêt qu'il a manifesté pour notre travail.

Un grand merci à Cristóbal Rojas d'avoir été un si agréable collaborateur, d'avoir été une source si intarissable de réponses à mes questions et de questions à mes réponses. Sa compagnie a fait de ce travail une réelle partie de plaisir.

Je remercie tous les enseignants et moniteurs de Paris 7 avec qui j'ai collaboré, et tous les étudiants qui m'ont servi de cobayes et m'ont donné la sensation d'être utile, lorsque la recherche fondamentale n'y parvenait pas.

Je remercie également les secrétaires Michelle Angely, Lise-Marie Bivart, Sylvia Imbert, Joëlle Isnard, Valérie Mongiat, et Michèle Wasse ainsi que les documentalistes de la bibliothèque de l'ENS et les membres du SPI pour leur compétence, leur patience, leur pédagogie et leur bonne humeur.

Merci à Andreï Nikolaïevitch, sans qui cette aventure n'aurait pu avoir lieu. Merci à la lettre μ, sans laquelle cette thèse perdrait tout son sens. Merci à toutes celles et ceux qui ont fait semblant de comprendre mon sujet de thèse quand moi-même ne savais pas trop où j'en étais. Merci au CIES de m'avoir appris à faire des recherches sur Google au bout de deux années de thèse.

Merci, pour leur soutien et leur compagnie, à mes parents, à Aude et Manu, à Laurent, Rémy, Fabien, Sébastien, Nicolas, Pierre, Marie, Michaël, Martin, Maël, Arda, Boris, Aurélien, Matteo, Pierre-Emmanuel, Jonathan, Dan et tous les autres.

Et bien sûr, tous mes remerciements vont à Caroline, sans qui ces années n'auraient pas eu le même parfum.

Résumé

L'objectif général de cette thèse est d'étudier les notions d'aléatoire et d'information algorithmiques – jusqu'ici restreints aux espaces symboliques – sur des espaces plus généraux, précisément les espaces métriques calculables, et d'appliquer ces notions à la théorie des systèmes dynamiques. Les principaux apports sont : (1) le développement d'un cadre robuste pour l'étude d'objets mathématiques (mesures de probabilité, systèmes dynamiques et leurs modèles symboliques) d'un point de vue algorithmique, notamment l'introduction et l'étude détaillée des treillis d'énumération effective; (2) l'extension de l'aléatoire algorithmique aux espaces métriques calculables, améliorant ainsi l'extension menée par Gács qui imposait une condition supplémentaire à l'espace, et l'étude de quelques notions des probabilités classiques du point de vue de l'aléatoire; (3) un apport à la théorie des systèmes dynamiques, établissant des relations entre l'aléatoire algorithmique et l'aléatoire dynamique. Nous étudions notamment deux notions de complexité algorithmique des orbites, l'une $\mathcal{K}_\mu$ utilisant la mesure, l'autre $\mathcal{K}$ inspirée du point de vue topologique. Nous montrons que la complexité $\mathcal{K}_\mu$ des orbites partant des points aléatoires est l'entropie du système au sens de la mesure, que la borne supérieure des complexités $\mathcal{K}$ des orbites est l'entropie topologique, et que $\mathcal{K}_\mu$ et $\mathcal{K}$ coïncident pour les points aléatoires. Ce travail enrichit les résultats de Brudno et White.

Sommario

L'obiettivo di fondo di questa tesi è lo studio delle nozioni di aleatorio e d'informazione algoritmici – usualmente limitati alle sequenze simboliche – a spazi più generali, e di interesse per la fisica-matematica, quali gli spazi metrici calcolabili. E questo, con lo scopo di applicare tali nozioni alle teoria dei sistemi dinamici. I contributi principali della tesi sono: (1) lo sviluppo di un quadro robusto per lo studio di strutture matematiche (misure di probablilità, sistemi dinamici e loro modelli simbolici) dal punto di vista algoritmico, in particolare l'introduzione e lo studio dettagliato di reticoli d'enumerazione effettivi; (2) l'estensione dell'aleatorio algoritmico agli spazi metrici calcolabili, migliorando con cosi' l'approccio di Gacs che imponeva una non ovvia condizione supplementare allo spazio, nonché lo studio di alcune nozioni di probabilità classica dal punto di vista dell'aleatorio algoritmico; (3) un contributo alla teoria dei sistemi dinamici, grazie ad alcune correlazioni fra aleatorio algoritmico e aleatorio dinamico. Sono state parimenti studiate due nozioni di complessità algoritmica delle orbite, l'una ($\mathcal{K}_\mu$) basata sulla misura, l'altra ($\mathcal{K}$) inspirata da un punto di vista topologico. Si dimostra allora che la complessità $\mathcal{K}_\mu$ delle orbite che iniziano da punti aleatori coincide con l'entropia del sistema, nel senso della misura, che il limite superiore della complessità $\mathcal{K}$ delle orbite è l'entropia topologica, e che $\mathcal{K}_\mu$ e $\mathcal{K}$ coincidono sui per i punti aleatori. Questi ultimi risultati arricchiscono quelli di Brudno e White.

Summary

The general aim of this thesis is the study of the notions of algorithmic randomness and information, which are defined on symbolic spaces, to more general spaces – namely computable metric spaces – allowing their applications to dynamical systems theory. The main results are: (1) the development of a robust framework to study classical mathematical objects (probability measures, dynamical systems and their symbolic models) from an algorithmic point of view, in particular the introduction and detailed study of the structure of enumerative lattice; (2) the extension of algorithmic randomness to all computable metric spaces, improving the previous extension by Gacs which required an additive assumption on the space, and the study of some classical probability notions from the point of view of randomness; (3) contributions to dynamical systems theory, establishing relations between algorithmic and dynamical randomness. In particular, we study two notions of algorithmic orbit complexity, the one ($\mathcal{K}_\mu$) using an invariant probability measure, the other ($\mathcal{K}$) inspired from the topological approach. We prove that the complexity $\mathcal{K}_\mu$ of the orbits of random points equal the measure-theoretical entropy of the system, that the supremum of the complexity $\mathcal{K}$ among all the orbits is the topological entropy, and that $\mathcal{K}_\mu$ and $\mathcal{K}$ coincide on random points. This work improves results established by Brudno and White.

Introduction

Modeling regularities

A good model grasps all regularities...

Suppose one tosses a coin a large number of times and observes that heads tend to appear more than tails: there are at least two possible interpretations: (1) it is a manifestation of Luck, (2) it is a manifestation of the biased character of the coin. According to the first one, the observed regularity (the number of heads dominates) is specific to the particular sequence of tosses. According to the second one, the regularity is a generic property that is shared by most sequences of tosses with this coin. This can be made precise by the use of a probabilistic model which provides a mathematical definition of genericity for a property (generic = of probability one).

We feel that the second model enables us to explain, or understand what happened. More generally, one could say that understanding a natural phenomenon consists in providing a model – which will be mathematical here – which grasps all the regularities that have as yet been observed. Believing in such a model offers an explanation *a posteriori* of what has been observed in the past, and allows one to predict *a priori* the regularities that will be observed in the future.

Once it has been assumed that a model is adequate with a phenomenon, what remains is called "randomness". The actual evolution of the system is expected to occupy all the space that is left available inside the frame provided by the model, and to explore all the degrees of freedom in a random way: all the regular part of the system has been injected into the structure, and only the random part remains to the particular realizations. If one expects other regularities, the model shall be refined so that they can be derived from it.

These considerations are "physical": what is concerned there is the relation between the model and reality. Let us discuss the mathematical counterpart.

...but creates artificial ones.

In many mathematical spaces, one often distinguishes a class of elements which are "easily describable": the rational numbers in the real line, simple functions in functions spaces, etc. They are used in order to carry out constructions, to approximate more complex elements, to structure the space. If the space underlies a model of a natural process, these elements may seem to be artificial as they have no physical meaning, but they are often essential for the understanding of the system. A classical example is given by the periodic solutions of a differential system: even if they are unstable, they are essential to the mathematical study of the system, as Poincaré says:

> D'ailleurs, ce qui nous rend ces solutions périodiques si précieuses, c'est qu'elles sont, pour ainsi dire, la seule brèche par où nous puissions essayer de pénétrer dans une place jusqu'ici réputée inabordable.[1]

Through these simple elements, some particular regularities might not be forbidden by the model whereas they are not physically plausible. Probability theory, providing a mathematical notion of "plausibility" (high or full probability) is a way of getting rid of the artificial behaviors that are introduced by the model.

This can even be refined: computability theory provides a sound and general setting to talk about description and regularities. Using this it is possible to give a precise meaning to "easily describable" and "regularities". This is the aim of algorithmic randomness, which enables one to reject those elements which have more regularities than expected, labeling them as "non-random". The elements that remain are called "random" and classical theorems like:

$$\text{property } P \text{ holds for } \mu\text{-almost every element}$$

are to be converted into:

$$\text{property } P \text{ holds for every } \mu\text{-random element.}$$

(where μ is a probability measure).

The ideas underlying this notion go back to Laplace and several definitions have been suggested along the twentieth century (Von Mises, Church, Kolmogorov), but the first sound definition of algorithmically random binary sequences is due to Martin-Löf in

[1] Henri Poincaré, *Les méthodes nouvelles de la mécanique céleste.*

[ML66]. Extensions to other spaces have been recently proposed (see [HW98], [HW03], [Gác05]. A first aim of this thesis is to improve these extensions and establish a framework which makes possible the investigation of classical probability theory – which takes place in general spaces – from the algorithmic point of view.

Quantifying regularities

Let us come back for a while to physical considerations. Once a model has been defined in such a way that it integrates all regularities which are expected to appear, what remains is randomness, disorder, uncertainty. Boltzmann defined a notion of *entropy* to quantify the degree of uncertainty left by the statistical model. Along the second half of the twentieth century this idea has been a source of several notions of entropies in different mathematical contexts. The expression *information content* is also used in place of entropy, as uncertainty can be thought as lack of information. The theories which deal with these quantities are consequently called *information theories*.

The static setting The space may be endowed with different structures, which lead to different notions of entropy:

1. The topological point of view: a topological entropy measures the size of the space, i.e. the number of distinguishable points. This is the idea underlying the ϵ-entropy, defined by Kolmogorov and Tikhomirov in 1959 ([KT59]).

2. The probabilistic point of view: taking advantage of the non-uniformity of the space modeled by probabilities, Shannon defined in 1948 his famous entropy. To each point is actually attributed an individual information content, of which the entropy is the mean. In the topological framework, which is blind to non-uniformity, all points had the same information content.

3. The algorithmic point of view: in 1965, Kolmogorov ([Kol65]) comes back to the entropy notions mentioned above and makes use of computability theory in order to define an algorithmic notion. The idea is simple: in each context, topological or probabilistic, one can interpret information content of a point as its minimal description length, relative to some fixed description system; the entropy is then the mean description length of points. Computability theory provides a very general description

system: universal Turing machines are able to simulate all effective decoding procedures. The *Kolmogorov complexity* of a point is then its minimal description length by a universal machine, and is also called algorithmic information content.

The dynamical setting The situation described above is "static": what is observed is only the state of a system, not its evolution. Time evolution of systems is mainly modeled by dynamical systems. The fact that such systems are deterministic does not prevent randomness from appearing: randomness is indeed thought as unpredictability (in classical mechanics). The ideas that underlie information theory, which attempt is to quantify uncertainty, have been applied to dynamical systems to quantify their degree of unpredictability. Each static entropy has a dynamical version, which is its growth rate along the time-evolution of the system. The dynamical versions of the ϵ-entropy, the Shannon entropy and the Kolmogorov complexity are respectively:

1. The topological entropy of a system (defined in 1965 by Adler, Konheim and McAndrew in [AKM65]),
2. The Kolmogorov-Sinaï entropy (defined in 1958, 1959, [Kol58], [Sin59]),
3. The algorithmic complexity of the orbits of a system (defined in 1983 by Brudno, [Bru83], improved later by Galatolo [Gal00]).

As in the static case, these different notions are strongly related. Let us remark that the algorithmic approach gives an *individual* (attributed to each single orbit) and *intrinsic* notion (independent of the measure for instance).

The theory of dynamical systems provides a setting in which classical randomness, understood as deterministic unpredictability, can be investigated. On the other hand, probability theory[2] is the natural framework to talk about randomness (note that this theory is not concerned with the way randomness is generated). A very natural idea is to mix these two settings: this is the object of *ergodic theory*, which deals with dynamical systems from a probabilistic point of view, studying them as particular stochastic processes.

Another aim of this thesis is to establish a robust framework in order to handle ergodic theory from an algorithmic point of view. We then establish strong relations between randomness, ergodic theorems, orbit complexities and entropies. Some of our results had

[2] whose axiomatization was achieved in 1933 by Kolmogorov

already been stated on the Cantor space (especially [V'y98]); this extension to more "natural" setting for dynamics relates then to actual physical systems.

Articles

- [Hoy07]: *Dynamical systems: stability and simulability*, appeared in Mathematical Structures in Computer Science. This was a preliminary work on dynamical systems and computability.

- [HR07]: *Computability of probability measures and Martin-Löf randomness over metric spaces*, submitted to Information and Computation, available at `http://arxiv.org/abs/0709.0907`. It contains parts of chapters 1, 2 and 3 and was written in collaboration with Cristóbal Rojas.

- [GHR07c]: *Algorithmically random points in measure preserving systems, statistical behavior, complexity and entropy*, submitted to Information and Computation, available at `http://arxiv.org/abs/0801.0209`. It is a joint work with Stefano Galatolo and Cristóbal Rojas, and contains parts of chapters 4 and 5.

- [GHR07b]: *An effective Borel-Cantelli lemma. Constructing orbits with required statistical properties*, submitted to the Journal of the European Mathematical Society, available at `http://arxiv.org/abs/0711.1478`. This article was written with Stefano Galatolo and Cristóbal Rojas. Only the application to absolutely normal numbers is included in the thesis. An improved version of this article can be found in Cristóbal Rojas's thesis [Roj08].

- [GHR08]: *Schnorr randomness–A dynamical point of view*, in preparation. It is a joint work with Peter Gács and Cristóbal Rojas. An improved version of this article can be found in [Roj08].

- [GHR07a]: *Computable invariant measures*, in preparation. This joint work with Stefano Galatolo and Cristóbal Rojas is not finished yet.

The articles [HR07], [GHR07c] and [GHR07b] are following the submission process at the time this thesis is written.

Contents

Chapter 1

Computability

There are mainly two frameworks to carry out computability investigations over general spaces. The one is domain theory, the other is representation theory. The first one (see [Eda97] for instance) uses order theory and has nice categorical properties, but does not handle mathematical objects from the classical point of view. The second one (see [Wei00]) applies to topological spaces but uses a rather heavy language, everything being expressed in terms of Turing machines and symbols (representations are ways to encode objects into symbolic sequences).

Our goal is to develop a language which is closer to the classical mathematical one, in order to take advantage of the mathematical intuitions one has when starting to work in computability theory. Of course, our framework is much inspired by the two frameworks mentioned above which are rich in ideas and results. We are guided by the following principle: a mathematical space shall be handled from the first or the second point of view, depending on the natural structure which comes with it (an order or a topology).

We introduce the rather elementary structure of *enumerative lattice* from which all constructivity notions on general spaces can be derived. It enables one to express computability proofs in a more algebraic fashion, freeing oneself from coding questions. The structure of enumerative lattice enables one to carry out important constructions in a straightforward way:

1. construction of effective enumerations. Effective enumerations are recurrent in computer science (the first one being the enumeration of Turing machines) and can be reduced to a general abstract result,

2. conversion of algorithms into extensional algorithms,

3. extension of partial functions to total functions,

4. constructivity relative to non-constructive objects can be easily expressed.

1.1 Background from recursion theory

We assume that the reader is familiar with recursion theory on the natural numbers. We recall some basic concepts that will be intensively used along this thesis. For more details, we refer the reader to a standard text [Rog87].

On the set of natural numbers, recursion theory provides a robust notion of *recursive function* i.e. possibly partial functions which can be "effectively computed". There are bijective functions $\langle\rangle : \mathbb{N}^k \to \mathbb{N}$ which are effective in the sense that the projections $\pi_i^k : \mathbb{N} \to \mathbb{N}$ defined by $\pi_i^k(\langle n_1, \dots, n_k \rangle) = n_i$ are recursive. An essential property of recursive functions is their *effective enumerability*: there is an enumeration $\{\phi_e : e \in \mathbb{N}\}$ of this set such that not only ϕ_e is recursive, but the function $f : \langle e, n\rangle \mapsto \phi_e(n)$ is recursive. In other words, there is a *universal* recursive function ϕ_u which simulates all recursive functions. We will say that ϕ_e is recursive *uniformly* in e: there is a single recursive function which computes ϕ_e when it is provided with e.

One of the most important notions of recursion theory is the notion of *recursively enumerable* (r.e.) subset of $\mathbb{N}$. $E \subseteq \mathbb{N}$ is recursively enumerable if there is a recursive function ϕ such that $E = \mathrm{im}\phi = \{\phi(n) : n \in \mathbb{N}\}$. The effective enumeration of all the recursive functions induces an effective enumeration: $E_e = \mathrm{im}\varphi_e$. We recall some well-known facts which prove to be very useful:

1. If $E = \mathrm{im}\phi$ it is possible to construct, in a uniform way, a recursive function ψ such that $E = \mathrm{dom}\psi$. In other words, there is a total recursive function f such that $\mathrm{im}\phi_e = \mathrm{dom}\phi_{f(e)}$. We say that $\phi_{f(e)}$ *semi-decides* E: it can be thought of as an algorithm which tests if an element belongs to E and stops exactly when it is true.

2. The conversion is also possible in the other direction: there is a total recursive function g such that $\mathrm{dom}\phi_e = \mathrm{im}\phi_{g(e)}$.

3. There is a total recursive function h such that $\mathrm{im}\phi_e = \mathrm{im}\phi_{h(e)}$ and $\phi_{h(e)}$ is total when E_e is non-empty.

The existence of a universal recursive function ϕ_u induces the existence of a r.e. set E which is universal in the sense that $E_e = \{n : \langle n, e\rangle \in E\}$ for all e. Indeed, let $E = \mathrm{im} f$ where f is the recursive function defined by $f(\langle e, n\rangle) = \langle n, \varphi_e(n)\rangle$.

1.1.1 Numbered sets

Among the historical models of effective procedures, some work on the natural numbers (recursive functions), some work on finite symbolic sequences (Turing machines). Modulo effective encoding, these two classes of mathematical objects are equivalent. Gödel initiated this by encoding logical formulas into integers in order for encoding and decoding to be effective (he modeled effectivity by primitive recursion). This is now a very common principle, intensively used by programmers: expressive programming languages internally represent discrete objects as graphs, trees, formulas by binary strings. Fortunately the particular representation system is hidden to the reader: we will try to follow this principle as soon as possible, namely from section 1.2.

Definition 1.1.1.1. A ***numbered set*** is a countable set S with a total surjective function $\nu_S : \mathbb{N} \to S$, called the ***numbering***. If a generic element of S is denoted by s, s_n will denote $\nu_S(n)$.

Whenever it is possible, we will choose a bijective numbering, for which we define:

Definition 1.1.1.2. Suppose the numberings of S and S' are bijective. A (possibly partial) function $f : S \to S'$ is ***computable*** if there is a recursive function ψ such that $f(s_n) = s'_{\psi(n)}$ for all $n \in \mathbb{N}$. In other words, the following diagram commutes:

$$\begin{array}{ccc} \mathbb{N} & \xrightarrow{\psi} & \mathbb{N} \\ \nu_S \downarrow & & \downarrow \nu_{S'} \\ S & \xrightarrow{f} & S' \end{array}$$

A set $A \subseteq S$ is ***recursively enumerable (r.e.)*** if there is a r.e. subset E of $\mathbb{N}$ such that $A = \{s_n : n \in E\}$.

The computability of functions between two numbered sets S, S' depends on what information can be effectively recovered about an object from its number. For most countable sets encountered in mathematics, everybody agree on what is the relevant information. In this thesis, a few numbered sets will be used. For each one, a particular numbering will be fixed once for all.

Examples. 1. $\mathbb{N}^k$ is a numbered set, with the inverse of $\langle\rangle_k$ as numbering,

2. $\mathbb{N}^*$ is a numbered set, with the inverse of $\langle\rangle$ as numbering,

3. we fix some bijective numbering of the set $\mathcal{F}$ of finite subsets of $\mathbb{N}$, which makes the function from $\mathbb{N}^*$ to $\mathcal{F}$, mapping $(n_1, \ldots, n_k)$ to $\{n_1, \ldots, n_k\}$ computable, with a computable right-inverse. F_i will denote the finite subset of $\mathbb{N}$ with number i.

4. we fix some effective bijective numbering of $\mathbb{Z}$ (for instance $z_{2n} = n$ and $z_{2n+1} = -n-1$),

5. we fix some bijective numbering of $\mathbb{Q}$ which makes the function $\mathbb{Z} \times \mathbb{N} \to \mathbb{Q}, (a, b) \mapsto a/b$ computable, with a computable right-inverse. q_n will denote the rational number with number n.

6. we also fix some effective bijective numbering of the set $\mathbb{Q}_{>0}$ of positive rational numbers, such that $\mathbb{N} \times \mathbb{N} \to \mathbb{Q}, (a, b) \mapsto a/b$ is computable and has a computable right-inverse. When it will be clear from the context that we use positive rational numbers, we will also write q_n for the positive rational number with number n.

In a natural way, any finite product of numbered sets is also a numbered set, its numbering being induced by that of $\mathbb{N}^k$. The set of finite subsets of a numbered set is a numbered set: its numbering is now induced by the numbering of $\mathcal{F}$. The disjoint union $S'' = S \uplus S'$ of two numbered sets has a canonical natural numbering: $s''_{2n} = s_n$ and $s''_{2n+1} = s'_n$.

1.2 Enumerative Lattices

Enumerative lattices are a generalization of the set of subsets of $\mathbb{N}$ with the inclusion as order. Their name comes from the fact that they inherit an intersecting property: all the r.e. subsets of $\mathbb{N}$ can be *enumerated* in a uniform way. They are effective versions of complete lattices (see appendix B.2 for preliminaries on complete lattices).

Definition 1.2.0.3 (Enumerative lattice)**.** An ***enumerative lattice*** $(L, \leq, \mathcal{P})$ is a complete lattice $(L, \leq)$ with a numbered set $\mathcal{P} \subseteq L$ such that every element of L is the supremum of a subset of $\mathcal{P}$.

$\mathcal{P}$ is called the set of ***ideal elements***. The numberings of $\mathcal{F}$ (the set of finite subsets of $\mathbb{N}$) and $\mathcal{P}$ induce a numbering of the directed set $\mathcal{D}$ of suprema of finite subsets of $\mathcal{P}$: $d_{\langle i_1,\ldots,i_n\rangle} = \sup\{p_{i_1}, \ldots, p_{i_n}\}$. The numbered set $\mathcal{D}$ will be intensively used in the following.

Examples. 1. The Sierpiński space $\mathbb{S} = \{\bot, \top\}$ with $\bot < \top$ and $\mathcal{P} = \{\top\}$ is an enumerative lattice (take for instance $\nu_{\mathcal{P}}(n) = \top$ for all $n \in \mathbb{N}$). The two elements $\bot$ and$\top$ shall be interpreted as false/true, reject/accept, diverge/stop. In particular, we will use the following notation: if ϕ is a logical proposition, intended to be right or wrong, "ϕ" will be $\top$ if ϕ is right, $\bot$ if ϕ is wrong (it will be clear on examples),

2. The set $(P(\mathbb{N}), \subseteq, \text{singletons})$ is an enumerative lattice, and more generally,

3. If S is a numbered set, then $(2^S, \subseteq, \text{singletons})$ is an enumerative lattice,

4. Let $\overline{\mathbb{R}} = \mathbb{R} \cup \{-\infty, +\infty\}$: $(\overline{\mathbb{R}}, \leq, \mathbb{Q})$ is an enumerative lattice. Similarly, $([0,1], \leq, \mathbb{Q} \cap [0,1])$ and $(\overline{\mathbb{R}}^+, \leq, \mathbb{Q}_{>0})$ are enumerative lattices, where $\overline{\mathbb{R}}^+ = [0, +\infty) \cup \{+\infty\}$,

5. If $(L, \leq, \mathcal{P})$ and $(L', \sqsubseteq, \mathcal{P}')$ are enumerative lattices, their product $(L \times L', \leq_\times, \mathcal{P} \times \mathcal{P}')$ is an enumerative lattice, with $(x, x') \leq_\times (y, y')$ if $x \leq y$ and $x' \sqsubseteq y'$,

6. Let $(L_i, \leq_i, \mathcal{P}_i)_{i \in \mathbb{N}}$ be a family of enumerative lattices. Their product $(\Pi_i L_i, \leq, \mathcal{P})$ with $(l_i)_i \leq (l'_i)_i \iff l_i \leq l'_i \forall i$ and $(l_i)_i \in \mathcal{P} \iff$ there is some i such that $l_i \in \mathcal{P}_i$ and $l_j = \bot_j$ for $j \neq i$.

Scott-topology vs sequential topology

We recall that in every topological space, the sequential topology is finer than the topology (see appendix A.1.1). As the following proposition shows, enumerative lattices with the Scott-topology are sequential spaces: the sequential topology coincides with the Scott-topology.

Proposition 1.2.0.1 (Scott-topology). *For a subset $U \subseteq L$ the following are equivalent:*

1. *U is Scott-open,*

2. *for all $A \subseteq \mathcal{P}$, $[\sup A \in U \iff$ there exists a finite set $A_0 \subseteq A$ such that $\sup A_0 \in U]$,*

3. *for every sequence x_n satisfying $x_n \leq x_{n+1}$,*

$$\sup_n x_n \in U \iff \exists n, x_n \in U$$

4. *U is sequentially open.*

In conditions 2 and 3 the equivalence can be replaced by an implication $\Rightarrow$, assuming that U is an upper set ($x \in U$ and $x \leq y \implies y \in U$). Actually, in conditions 2 and 3, the implication $\Leftarrow$ is equivalent to the fact that U is an upper set (take $x \in U, x \leq y$, $A = \{x, y\}$ in condition 2, $x_0 = x$ and $x_n = y$ for $n \geq 1$ in condition 3).

The implication $1 \Rightarrow 4$ is true in any topological space.

Proof of $2 \Rightarrow 1$. We use the characterization of the Scott topology for a complete lattice (proposition B.2.0.4). Let $U \subseteq X$ satisfying 2. First, U is an upper set: if $x \in U$ and $x \leq y$, then $y = \sup\{x, y\} \in U$. Let $A \subseteq X$ such that $\sup A \in U$. For each $a \in A$, there is some set $\mathcal{P}_a \subseteq \mathcal{P}$ such that $a = \sup \mathcal{P}_a$. Define $\mathcal{P}_A := \bigcup_{a \in A} \mathcal{P}_a$: $\sup \mathcal{P}_A = \sup A \in U$ so there is a finite subset $\{p_{i_1}, \ldots, p_{i_n}\}$ of $\mathcal{P}_A$ whose supremum is in U. For each $k \leq n$, there is $a_k \in A$ such that $p_{i_k} \in \mathcal{P}_{a_k}$: define $A_0 = \{a_1, \ldots, a_n\} \subseteq A$. As $\sup A_0 \geq \sup\{p_{i_1}, \ldots, p_{i_n}\} \in U$ which is an upper set, it follows that $\sup A_0 \in U$. U is then Scott-open. $\square$

Proof of $3 \Rightarrow 2$. Suppose U satisfies condition 3. Let $A \subseteq \mathcal{P}$ such that $\sup A \in U$. A is countable: $A = \{p_{i_1}, p_{i_2}, \ldots\}$. Let $d_k = \sup\{p_{i_1}, \ldots, p_{i_k}\}$. As $d_k \leq d_{k+1}$ and $\sup d_k = \sup A \in U$, there is k such that $d_n \in U$ for all $n \geq k$: $d_k = \sup A_0$ for some finite subset A_0 of A. $\square$

Proof of $4 \Rightarrow 3$. First, if U is sequentially open, then it is an upper set: indeed, let $x \leq y$ with $x \in U$. The sequence defined by $x_{2n} = x, x_{2n+1} = y$ converges to its $\liminf$ which is $x \in U$ (see proposition B.2.0.7), so there is k such that $x_n \in U$ for all $n \geq k$. Hence, $y \in U$. This induces the implication $\exists n, x_n \in U \implies \sup_n x_n \in U$.

Now, any sequence satisfying $x_n \leq x_{n+1}$ converges to its supremum (see proposition B.2.0.7), so if U is sequentially open, then $\sup_n x_n \in U \implies \exists n, x_n \in U$. $\square$

Scott-continuity vs sequential continuity

The preceding proposition directly induces characterizations of Scott-continuous functions between enumerative lattices:

Proposition 1.2.0.2 (Scott-continuity)**.** *For a function $f : L \to L'$ the following are equivalent:*

1. *f is Scott-continuous,*

2. *for all* $A \subseteq \mathcal{P}$, $f(\sup A) = \sup\{f(\sup A_0) : A_0$ *finite subset of* $A\}$,

3. *for every sequence* x_n *satisfying* $x_n \leq x_{n+1}$, $f(\sup_n x_n) = \sup_n f(x_n)$,

4. f *is sequentially continuous.*

1.2.1 Constructivity

The distinguished ideal elements are chosen to be constructive, and generate a wider class of constructive elements.

Definition 1.2.1.1 (Constructive element)**.** An element $x \in L$ is ***constructive*** if there is some r.e. set $E \subseteq \mathbb{N}$ such that $x = \sup\{p_i : i \in E\}$.

Naturally, we say that elements x_n are uniformly constructive if there are uniformly r.e. sets $E_n \subseteq \mathbb{N}$ such that $x_n = \sup\{p_i : i \in E_n\}$. In other words, there is a r.e. set $E \subseteq \mathbb{N}^2$ such that $x_n = \sup\{p_i : (n, i) \in E\}$.

Examples.

1. If S is a numbered set with a bijective numbering, then the constructive elements of $(2^S, \subseteq, \text{singletons})$ are the r.e. subsets of S,

2. The constructive elements of $(\overline{\mathbb{R}}, \leq, \mathbb{Q})$ are called the ***lower semi-computable*** real numbers,

3. The constructive elements of the infinite product $(L^{\mathbb{N}}, \leq, \mathcal{P})$ are the sequences of uniformly constructive elements of L.

Here is the interesting property of enumerative lattices which justifies their name:

Proposition 1.2.1.1 (Effective enumeration)**.** *Let* $(L, \leq, \mathcal{P})$ *be an enumerative lattice. There is an effective enumeration of the constructive elements of L, that is a sequence* $(x_e)_{e \in \mathbb{N}}$ *of uniformly constructive elements exhausting the set of constructive elements of L.*

Proof. The effective enumeration $(E_e)_{e \in \mathbb{N}}$ of the r.e. subsets of $\mathbb{N}$ induces an effective enumeration of the constructive elements of L: $x_e = \sup\{p_i : i \in E_e\}$. □

The set $[L \to L']$ of Scott-continuous functions endowed with the point-wise ordering is a complete lattice, but not an enumerative lattice in general. It is nevertheless possible to define a natural notion of constructive Scott-continuous function.

Definition 1.2.1.2 (Constructive function $L \to L'$)**.** A function $f : L \to L'$ is ***constructive*** if it is Scott-continuous and $f(d_k)$ is constructive uniformly in k.

If $f : L \to L'$ and $g : L' \to L''$ are constructive functions, their composition $g \circ f$ is easily constructive.

The topology τ_L is a complete lattice which is isomorphic to the set $[L \to \mathbb{S}]$ of Scott-continuous functions from L to $\mathbb{S}$: an open set $U \subseteq L$ can be identified with its (continuous) characteristic function $\mathbf{1}_U : L \to \mathbb{S}$ defined by $\mathbf{1}_U(x) =$ "$x \in U$" (i.e. $\mathbf{1}_U(x) = \top$ if $x \in U$, $\perp$ otherwise). It enables to define:

Definition 1.2.1.3 (Constructive open set)**.** Let $(L, \leq, \mathcal{P})$ be an enumerative lattice. A Scott-open set $U \in \tau_L$ is ***constructively open*** or is a ***constructive open set*** if $\mathbf{1}_U : L \to \mathbb{S}$ is a constructive function.

The open sets $\emptyset, L$ are obviously constructive. In $(\overline{\mathbb{R}}, \leq, \mathbb{Q})$, the constructive open sets are $(x, +\infty)$ where x is upper semi-computable. In $(2^{\mathbb{N}}, \subseteq, \{\text{singletons}\})$, the basic open sets $\Uparrow F_i = \{E \subseteq \mathbb{N} : F_i \subseteq E\}$ (where F_i is finite) are constructive and the constructive open sets are the r.e. unions of such basic open sets.

Characterizations using $P(\mathbb{N})$

As mentioned above, $(P(\mathbb{N}), \subseteq, \text{singletons})$ is an enumerative lattice. The set $\mathcal{C}(P(\mathbb{N}), P(\mathbb{N}))$ of continuous functions from $P(\mathbb{N})$ to $P(\mathbb{N})$ is a complete lattice with the point-wise ordering. For each finite set $F \subseteq \mathbb{N}$ and $j \in \mathbb{N}$, let us define the ***step function*** $\mathrm{St}_F^j : P(\mathbb{N}) \to P(\mathbb{N})$ by:

$$\mathrm{St}_F^j(E) = \begin{cases} \{j\} & \text{if } F \subseteq E \\ \emptyset & \text{otherwise} \end{cases}$$

which is Scott-continuous. The numberings of $\mathcal{F}$ and $\mathbb{N}$ induce a canonical numbering of the step functions.

Proposition 1.2.1.2 (Constructive element vs constructive function)**.** *$\mathcal{C}(P(\mathbb{N}), P(\mathbb{N}))$ is an enumerative lattice with the point-wise ordering and the step functions as ideal elements. The constructive elements of $\mathcal{C}(P(\mathbb{N}), P(\mathbb{N}))$ are exactly the constructive functions from $P(\mathbb{N})$ to $P(\mathbb{N})$.*

Proof. If $\Phi : P(\mathbb{N}) \to P(\mathbb{N})$ is Scott-continuous, then one easily has $\Phi = \sup\{\mathrm{St}_F^j : F \in \mathcal{F}, j \in \Phi(F)\}$. If Φ is moreover a constructive function, then the set $A = \{(i, j) : j \in \Phi(F_i)\}$

is r.e., as $\Phi(F_i)$ is r.e. uniformly in i. So $\Phi = \sup\{\mathrm{St}^j_{F_i} : (i,j) \in A\}$ is a constructive element of $\mathcal{C}(P(\mathbb{N}), P(\mathbb{N}))$.

Conversely, if Φ is a constructive element of $\mathcal{C}(P(\mathbb{N}), P(\mathbb{N}))$, i.e. if $\Phi = \sup_{(i,j)\in A} \mathrm{St}^j_{F_i}$ for some r.e. set $A \subseteq \mathbb{N}^2$, then $\Phi(F_k) = \{j : \exists i, (i,j) \in A, F_i \subseteq F_k\}$ is r.e. uniformly in k. $\square$

Let $(L, \leq, \mathcal{P})$ be an enumerative lattice. Let us define the function $\sup_{\mathcal{P}} : P(\mathbb{N}) \to L$. By hypothesis on L, it is surjective: every element of L is the image of a subset of $\mathbb{N}$ by $\sup_{\mathcal{P}}$. Moreover, for every function $f : L \to L'$, there is $\Phi : P(\mathbb{N}) \to P(\mathbb{N})$ such that the following diagram commutes:

$$\begin{tikzcd} P(\mathbb{N}) \arrow[r, "\Phi"] \arrow[d, "\sup_{\mathcal{P}}"'] & P(\mathbb{N}) \arrow[d, "\sup_{\mathcal{P}'}"] \\ L \arrow[r, "f"] & L' \end{tikzcd}$$

i.e. $f \circ \sup_{\mathcal{P}} = \sup_{\mathcal{P}'} \circ \Phi$. Indeed, by surjectivity of $\sup_{\mathcal{P}'}$, for each $E \subseteq \mathbb{N}$ there is E' such that $f \circ \sup_{\mathcal{P}}(E) = \sup_{\mathcal{P}'}(E')$: put $\Phi(E) = E'$. Let us call such a Φ a ***realization*** of f.

Proposition 1.2.1.3 (Realizability). *Let $(L, \leq, \mathcal{P})$ be $(L', \leq, \mathcal{P}')$ be enumerative lattices and $f : L \to L'$ a function.*

1. *f is Scott-continuous if and only if it has a Scott-continuous realization $\Phi : P(\mathbb{N}) \to P(\mathbb{N})$.*

2. *f is constructive if and only if it has a constructive realization $\Phi : P(\mathbb{N}) \to P(\mathbb{N})$.*

Proof. If f has a Scott-continuous realization Φ, from $\Phi(E) = \sup_{F\subseteq E} \Phi(F)$ one easily derives$f(A) = \sup_{A_0 \subseteq A} f(A_0)$ (where F, A_0 are finite), so f is Scott-continuous. If Φ is moreover constructive, then $f(d_k) = f \circ \sup_{\mathcal{P}}(F_k) = \sup_{\mathcal{P}'} \circ \Phi(F_k)$ is constructive uniformly in k, as $\Phi(F_k)$ is r.e. uniformly in k.

Conversely, suppose f is Scott-continuous. As $\sup_{\mathcal{P}'}$ is surjective, for each finite set $F_i \subseteq \mathbb{N}$ there is a set $E_i \subseteq \mathbb{N}$ such that $f \circ \sup_{\mathcal{P}}(F_i) = \sup_{\mathcal{P}'}(E_i)$. As f is Scott-continuous, the element Φ of $\mathcal{C}(P(\mathbb{N}), P(\mathbb{N}))$ defined by $\Phi = \sup\{\mathrm{St}^j_{F_i} : i \in \mathbb{N}, j \in E_i\}$ is a realization of f. If f is moreover constructive, E_i can be chosen to be r.e. uniformly in i, which implies that Φ is a constructive element of $\mathcal{C}(P(\mathbb{N}), P(\mathbb{N}))$. $\square$

Morphism of enumerative lattices

Definition 1.2.1.4. Let $(L, \leq, \mathcal{P})$ and $(L', \sqsubseteq, \mathcal{P}')$ be two enumerative lattices. A ***morphism*** from L to L' is a constructive function $f : L \to L'$ which commutes with all suprema: for all $A \subseteq L$, $f(\sup A) = \sup f(A)$.

An ***isomorphism*** is a bijective morphism $f : L \to L'$ ($f^{-1} : L' \to L$ is then automatically a morphism). The fact that L and L' are isomorphic is denoted $L \equiv L'$.

Here are some easy but useful observations:

Proposition 1.2.1.4 (Basic facts about morphisms)**.**

1. *A morphism $f : L \to L'$ of complete lattices is a morphism of enumerative lattices if and only if $f(p_i)$ is constructive uniformly in i.*
2. *Every bijective constructive function $f : L \to L'$ is an isomorphism.*
3. *If $f : L \to L'$ is an isomorphism, $x \in L$ is constructive if and only if $f(x) \in L'$ is constructive.*
4. *If $f : L \to L'$ and $f' : L' \to L''$ are morphisms, $f' \circ f : L \to L''$ is a morphism. If f and f' are isomorphisms, so is $f' \circ f$.*

Product of enumerative lattices

If $(L, \leq, \mathcal{P})$ and $(L', \sqsubseteq, \mathcal{P}')$ are enumerative lattices, then their product $L \times L'$ is an enumerative lattice with the product order $\leq \times \sqsubseteq$ and with ideal elements $(\mathcal{P} \times \{\perp'\}) \cup (\{\perp\} \times \mathcal{P}')$ (this numbered set can be thought as the disjoint union $\mathcal{P} \uplus \mathcal{P}'$).

The projections $\pi_L : L \times L' \to L$ and $\pi_{L'} : L \times L' \to L'$ defined by $\pi_L(x, x') = x$ and $\pi_{L'}(x, x') = x'$ are morphisms, and for every constructive elements x, x', their right-inverses $\lambda_{x'} : L \to L \times L'$ and $\lambda_x : L' \to L \times L'$ defined by $\lambda_{x'}(x) = (x, x')$ and $\lambda_x(x') = (x, x')$ are morphisms.

It follows that if $f : L \times L' \to L''$ is constructive (where $(L'', \subseteq, \mathcal{P}'')$ is another enumerative lattice) and $x \in L$ is constructive, then $f_x : L' \to L''$ defined by $f_x(x') = f(x, x') = f \circ \lambda_x(x')$ is constructive.

The function $\sup : L \times L \to L$ defined by $\sup(x, x') = \sup\{x, x'\}$ is a morphism. However, the function $\inf : L \times L \to L$ which maps (x, y) to $\inf\{x, y\}$ is never a morphism of complete lattices, unless $L = \{\perp\}$: indeed, $\inf\{\sup\{\mathcal{P} \times \{\perp\} \cup \{\perp\} \times \mathcal{P}\}\} = \top$ and $\sup\{\inf\{x, x'\} : (x, x') \in \mathcal{P} \times \{\perp\} \cup \{\perp\} \times \mathcal{P}\} = \perp$.

In all the enumerative lattices we will encounter in this thesis, the function $\inf : L \times L \to L$ is Scott-continuous and even constructive. Its Scott-continuity lies in its distributivity on $\sup$. Its constructivity happens for different reasons.

Note that $\inf$ need not be distributive on $\sup$ to be constructive: consider the "diamond" enumerative lattice, where $p_1 \wedge (p_2 \vee p_3) = p_1$ and $(p_1 \wedge p_2) \vee (p_1 \wedge p_3) = \bot$ (as the lattice is finite, every directed set contains its supremum, so every monotonic function is Scott-continuous and even constructive):

$$\begin{tikzcd}
 & \top \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
p_1 \arrow[dr, dash] & p_2 \arrow[d, dash] & p_3 \arrow[dl, dash] \\
 & \bot &
\end{tikzcd}$$

Replacing $P(\mathbb{N})$ by $P(\mathbb{N}) \times P(\mathbb{N})$

The fact that $\mathbb{N}$ and $\mathbb{N} \uplus \mathbb{N}$ are effectively bijective implies that the enumerative lattices $P(\mathbb{N})$ and $P(\mathbb{N}) \times P(\mathbb{N})$ are isomorphic. The set $\mathcal{P}$ of ideal elements of $P(\mathbb{N}) \times P(\mathbb{N})$, which consists of the elements $(\{n\}, \emptyset)$ and $(\emptyset, \{n\})$ for $n \in \mathbb{N}$, can be identified with $\mathbb{N} \uplus \mathbb{N}$. The function $\sup_{\mathcal{P}} : P(\mathbb{N}) \to P(\mathbb{N}) \times P(\mathbb{N})$, defined by $\sup_{\mathcal{P}}(E) = (\{n : 2n \in E\}, \{n : 2n+1 \in E\})$ is an isomorphism.

From this, it follows that in proposition 1.2.1.3, realizations can be defined on $P(\mathbb{N}) \times P(\mathbb{N})$ or take values in $P(\mathbb{N}) \times P(\mathbb{N})$. If one wants to prove that a function $f : L \times L' \to L''$ is constructive, it may be more natural to exhibit a constructive realization $\Phi : P(\mathbb{N}) \times P(\mathbb{N}) \to P(\mathbb{N})$.

1.3 Effective Topological Spaces

Most of the definitions of this section are now classical and can be found in [Wei00] using representation theory.

We know that if (X, τ) is a topological space, its topology has a natural complete lattice structure $(\tau, \subseteq)$. If X has a countable basis $\mathcal{B}$ with a fixed numbering, then $(\tau, \subseteq, \mathcal{B})$ is an enumerative lattice. As $\cap$ distributes on unions, $\cap : \tau \times \tau \to \tau$ is Scott-continuous (see B.2.0.6). Usually, an effective topological space is defined as a T_0 second-countable topological space (X, τ) with a countable sub-basis σ. Taking the finite intersections of elements of σ provides a countable basis $\mathcal{B}$ with the canonical numbering: $B_{\langle i_1,\dots,i_n\rangle} = \sigma_{i_1} \cap \ldots \cap \sigma_{i_n}$. As $\mathcal{B}$ is closed under finite intersections, and because of the effectivity of the numbering, it automatically makes $\cap$ constructive.

However, we will mainly work in topological spaces where a countable basis that is not closed under finite intersections comes naturally. We then adapt the definition, requiring explicitly the constructivity of $\cap$.

Definition 1.3.0.5. An ***effective topological space*** is a triple $\mathcal{X} = (X, \tau, \mathcal{B})$ where:

1. (X, τ) is a T_0 second-countable topological space,
2. $\mathcal{B}$ is a countable basis with a numbering,
3. $\cap : \tau \times \tau \to \tau$ is constructive.

The numbered set $\mathcal{B}$ will be called the set of ***ideal open sets***. The functions $\cup : \tau\times\tau \to \tau$ and $\bigcup : \tau^{\mathbb{N}} \to \tau$ are constructive, as $\cup$ is the supremum for the inclusion order.

Examples.

1. $\mathbb{N}$ with the discrete topology and the singletons as basis is an effective topological space. Its topology is actually $P(\mathbb{N})$, and the induced enumerative lattice structure $(P(\mathbb{N}), \subseteq, \{\text{singletons}\})$ is the one that we already met,
2. If Σ is a finite alphabet, the product topology on $\Sigma^{\mathbb{N}}$ is effective: to each finite string u on Σ we associate the cylinder $[u] := \{\omega : u \text{ prefix of } \omega\}$. The cylinders form a countable basis.

Definition 1.3.0.6 (Constructive open sets)**.** An open subset U of X is ***constructively open*** or is a ***constructive open set*** if it is a constructive element of the enumerative lattice $(\tau, \subseteq, \mathcal{B})$, i.e. if there is a r.e. set $E \subseteq \mathbb{N}$ such that $U = \bigcup_{i\in E} B_i$.

Let $(U_e)_{e\in\mathbb{N}}$ be the canonical enumeration of all the constructive open subsets of X, given by the general construction on enumerative lattices. For $x \in X$, we define the Scott-continuous function $\delta_x : \tau \to \mathbb{S}$ by $\delta_x(U) =$ "$x \in U$".

Definition 1.3.0.7 (Constructive points)**.** Let $(X, \tau, \mathcal{B})$ be an effective topological space. A point $x \in X$ is said to be ***constructive*** if the function $\delta_x : \tau \to \mathbb{S}$ is constructive (it is then a morphism of enumerative lattices).

In other words, x is constructive if the set $\{i : x \in B_i\}$ is r.e.

We recall that τ, being an enumerative lattice, has a canonical topology, namely the Scott-topology. But this topology has no countable basis in general, so τ is not an effective topological space. Let us give an example of Scott-open subset of τ: when K is a compact subset of X, the set $\mathcal{U}_K = \{U \in \tau : K \subseteq U\}$ is a Scott-open. If x is a constructive point, the subset $\mathcal{U}_x = \{U \in \tau : x \in U\}$ of τ is a constructive open subset of τ (see definition 1.2.1.3): indeed, its indicator function $\mathbf{1}_{\mathcal{U}_x} : \tau \to \mathbb{S}$ is exactly δ_x.

As a continuous function from X to X' can be characterized by its inverse $f^{-1} : \tau' \to \tau$, the notion of constructive function between enumerative lattices directly gives a notion of constructively continuous function between effective topological spaces:

Definition 1.3.0.8 (Constructively continuous functions)**.** Let $(X, \tau, \mathcal{B})$ and $(X', \tau', \mathcal{B}')$ be two effective topological spaces. A function $f : X \to Y$ is ***constructively continuous*** if it is continuous and $f^{-1} : \tau' \to \tau$ is constructive.

We will use two useful characterizations: as f^{-1} is a morphism of complete lattices, it is a morphism of enumerative lattice when it is constructive, and f is constructively continuous if and only if all $f^{-1}(B_i)$ are uniformly constructive open sets.

As constructivity of functions between enumerative lattices is stable by composition, so is constructive continuity of functions between effective topological spaces. As a closed subset A of X can be characterized by the Scott-continuous function $\iota_A : \tau \to \mathbb{S}$ defined by $\iota_A(U) =$ "$A \cap U \neq \emptyset$", it gives a notion of constructive closed set.

Definition 1.3.0.9. A closed subset A of X is a ***constructive closed set*** if the function $\iota_A : \tau \to \mathbb{S}$ defined by $\iota_A(U) =$ "$A \cap U \neq \emptyset$" is constructive (it is then a morphism of enumerative lattices).

Remark that X, as a closed subset of X, has no reason to be constructive in general: the non-emptiness of the basic open sets need not be semi-decidable.

Morphisms of effective topological spaces

Definition 1.3.0.10. Let $(X, \tau, \mathcal{B})$ and $(X', \tau', \mathcal{B}')$ be two effective topological spaces. A ***morphism*** from X to X' is a constructively continuous function $f : X \to X'$.

An ***isomorphism*** is a bijective morphism $f : X \to X'$ such that $f^{-1} : X' \to X$ is a morphism. That X and X' are isomorphic is denoted $X \equiv X'$.

Here are some easy but useful observations:

Proposition 1.3.0.5 (Basic facts about morphisms)**.**

1. *The image of a constructive point by a morphism is a constructive point.*

2. *If $f : X \to X'$ is an isomorphism $x \in X$ is constructive if and only if $f(x) \in X'$ is constructive.*

3. *If $f : X \to X'$ and $f' : X' \to X''$ are morphisms, $f' \circ f : X \to X''$ is a morphism. If f and f' are isomorphism, so is $f' \circ f$.*

Proof. Everything follows from the same proposition for enumerative lattices (proposition 1.2.1.4). If $\delta_x : \tau \to \mathbb{S}$ and $f^{-1} : \tau' \to \tau$ are constructive, so is $\delta_{f(x)} = \delta_x \circ f^{-1}$. If f^{-1} and f'^{-1} are constructive, so is $(f' \circ f)^{-1} = f^{-1} \circ f'^{-1}$. □

Product of effective topological spaces

If $(X, \tau, \mathcal{B})$ and $(X', \tau', \mathcal{B}')$ are effective topological space, then their product $(X \times X', \tau \times \tau', \mathcal{B} \times \mathcal{B}')$ is an effective topological space with the product topology.

As for enumerative lattices, the projections $\pi_X : X \times X' \to X$ and $\pi_{X'} : X \times X' \to X'$ are morphisms, and for every constructive points x, x', their right-inverses $\lambda_{x'} : X \to X \times X'$ and $\lambda_x : X' \to X \times X'$ are morphisms.

It follows that if $f : X \times X' \to Y$ is a morphism (where $(Y, \tau_Y, \mathcal{B}_Y)$ is another effective topological space) and $x \in X$ is constructive, then $f_x : X' \to Y$ defined by $f_x(x') = f(x, x') = f \circ \lambda_x(x')$ is a morphism.

The function $X \to X \times X$ mapping x to (x, x) is a morphism: the preimage of $B_i \times B_j$ is $B_i \cap B_j$.

1.3.1 Functions which are continuous on a subset

Let $(X, \tau, \mathcal{B})$ be an effective topological space and D be any subset of X. D is an effective topological space, with the induced topology $\tau_D = \tau_X \cap D = \{U \cap D : U \in \tau_X\}$ and the induced basis $\mathcal{B}_D = \mathcal{B} \cap D = \{B_i \cap D\}$. Remark that D may be any subset: in particular, there may be no way to distinguish non-empty basic open sets of $\mathcal{B}_D$ from empty ones, in a constructive way.

The topology on D then receives its canonical enumerative lattice structure. The constructive open subsets of D are exactly the constructive open subsets of X, intersected with D.

Proposition 1.3.1.1. *Let $D \subseteq X$.*

1. *The projection $\pi_D : \tau_X \to \tau_D$ defined by $\pi_D(U) = U \cap D$ is a morphism of enumerative lattices,*

2. *$x \in D$ is a constructive point of $(D, \tau_D, \mathcal{B}_D)$ if and only if x is a constructive point of $(X, \tau, \mathcal{B})$,*

As $\mathrm{id} : D \to X$ satisfies $\mathrm{id}^{-1} = \pi_D$, the first point can be rephrased: $\mathrm{id} : D \to X$ is a morphism of effective topological spaces.

Proof.

1. π_D is realized by $\mathrm{id} : P(\mathbb{N}) \to P(\mathbb{N})$: $\pi_D \circ \sup_{\mathcal{B}} = \sup_{\mathcal{B}_D} \circ \mathrm{id}$,

2. so the realizations of $\delta_x^D : \tau_D \to \mathbb{S}$ are exactly the realizations of $\delta_x^X = \delta_x^D \circ \pi_D$, and hence they are constructive at the same time.

□

It follows that any constructive function $F : \tau_Y \to \tau_X$ induces a constructive function $\pi_D \circ F : \tau_Y \to \tau_D$, but not every constructive function from τ_Y to τ_D may be obtained this way.

Definition 1.3.1.1. A function $f : X \to Y$ is ***constructively continuous on D*** if $f|_D : D \to Y$ is constructively continuous.

A set $A \subseteq X$ is ***constructively open on D*** if $A \cap D$ is a constructive open subset of $(D, \tau_D, \mathcal{B}_D)$.

In other words, A is constructively open on D if and only if there is a constructive open subset U of X such that $A \cap D = U \cap D$. f is constructively continuous on D if and only if $f^{-1}(B_i)$ are uniformly constructive open sets on D, i.e. there are uniformly constructive open subsets V_i of X such that $f^{-1}(B_i) \cap D = V_i \cap D$.

Definition 1.3.1.2 (Relative constructivity)**.** Let X, Y be effective topological spaces. A point $y \in Y$ is ***x-constructive*** if the function $f : \{x\} \to Y$ defined by $f(x) = y$ is constructively continuous on $\{x\}$.

1.3.2 The enumerative lattice $\mathcal{C}(X, L)$

Let $(X, \tau, \mathcal{B})$ be an effective topological space and $(L, \leq, \mathcal{P})$ an enumerative lattice. The set $[X \to L]$ of continuous functions from X to L with the point-wise order is a complete lattice, but does not have a canonical enumerative lattice structure in general. We then consider a subclass of $[X \to L]$, generated by the family of *step functions* (the author has been informed that this idea was also used in [Eda07b]).

For any open set $U \subseteq X$ and element $l \in L$, we define the ***step function*** $\mathrm{St}_U^l : X \to L$ by:

$$\mathrm{St}_U^l(x) = \begin{cases} l & \text{if } x \in U \\ \perp & \text{otherwise} \end{cases}$$

Step functions are continuous. ***Ideal step functions*** are step functions $\mathrm{St}_{B_i}^{p_j}$ where B_i is an ideal open set and p_j an ideal element. The set $\mathcal{S}\mathrm{tep}$ of ideal step functions is a numbered set (in bijection with $\mathcal{B} \times L$). We will sometimes denote $\mathrm{St}_{B_i}^{p_j}$ by $\mathrm{St}_{\langle i,j \rangle}$. We define $\mathcal{C}(X, L)$ as the set of point-wise suprema of step functions: it is an enumerative lattice.

Suprema and infima The order on $\mathcal{C}(X, L)$ is the point-wise order, and the supremum of a subset $\mathcal{G}$ of $\mathcal{C}(X, L)$ for this order coincides with the point-wise supremum of functions in $\mathcal{G}$:

$$(\sup \mathcal{G})(x) = \sup\{g(x) : g \in \mathcal{G}\}$$

The same thing holds for finite infima: $\inf\{f, g\}(x) = \inf\{f(x), g(x)\}$. However, the infimum of a set $\mathcal{G} \subseteq \mathcal{C}(X, L)$ is not in general the point-wise infimum of functions in $\mathcal{G}$, which is not in general continuous. One only has:

$$(\inf \mathcal{G})(x) \leq \inf\{g(x) : g \in \mathcal{G}\}$$

as $\inf \mathcal{G} \leq \inf g$ for all $g \in \mathcal{G}$. A simple example is $\mathcal{C}(X, \mathbb{S})$, which can be identified with τ_X (they are isomorphic complete lattices). The infimum of a family $\{U_i\}_{i \in I}$ of open subsets of X is not their intersection (which is not in general an open set), but instead the *interior* of their intersection: the characteristic function of their intersection is the point-wise infimum of the characteristic functions of the U_i.

The functions of $\mathcal{C}(X, L)$ share a common property, which is not true in general for all continuous functions from X to L (see section 1.4.3 for a counter-example).

Proposition 1.3.2.1. *Let $f \in \mathcal{C}(X, L)$. For every $x \in X$ and every sequence x_n converging to x,*

$$f(x) \leq \liminf f(x_n)$$

Proof. It is true of any step function $\mathrm{St}_{B_i}^{p_j}$: if $x \in B_i$, x_n eventually falls in B_i, so $\liminf f(x_n) = f(x)$. If $x \notin B_i$, $f(x) = \perp$.

If the condition is satisfied by a sequence of functions (f_i), then it is also satisfied by $f = \sup_i f_i$: $f(x) = \sup_i f_i(x) \leq \sup_i \liminf f_i(x_n) = \sup_i \sup_k \inf_{n \geq k} f_i(x_n) = \sup_k \sup_i \inf_{n \geq k} f_i(x_n)$. For all $n \geq k$, $\sup_i \inf_{n \geq k} f_i(x_n) \leq \sup_i f_i(x_n)$, so $\sup_i \inf_{n \geq k} f_i(x_n) \leq \inf_{n \geq k} \sup_i f_i(x_n)$. Hence $f(x) \leq \liminf f(x_n)$. □

Back to $\mathcal{C}(P(\mathbb{N}), P(\mathbb{N}))$ We know that $(P(\mathbb{N}), \subseteq, \{\text{singletons}\})$ is an enumerative lattice, on which the Scott-topology is naturally defined. Actually it makes $P(\mathbb{N})$ an effective topological space: to each finite set $F \subseteq \mathbb{N}$ we associate the Scott-open set $\Uparrow F$ defined as $\{E \in P(\mathbb{N}) : F \subseteq E\}$. The family $\{\Uparrow F : F \text{ finite subset of } \mathbb{N}\}$ is a basis of the Scott-topology on $P(\mathbb{N})$.

Taking $X = P(\mathbb{N})$ as an effective topological space and $L = P(\mathbb{N})$ as an enumerative lattice, the step functions defined here coincide with the step functions defined in section 1.2.1, but the notation is a bit different: ideal open sets are $\Uparrow F := \{E \in P(\mathbb{N}) : F \subseteq E\}$ where $F \subseteq \mathbb{N}$ is finite, and $\mathrm{St}_{\Uparrow F}^{\{j\}}$ was written St_F^j.

Constructivity on $\mathcal{C}(X, L)$

We now define and study the constructive functions from X to L.

Definition 1.3.2.1. Let $(X, \tau, \mathcal{B})$ be an effective topological space and $(L, \leq, \mathcal{P})$ an enumerative lattice. A function $f : X \to L$ is ***constructive*** if it is a constructive element of $\mathcal{C}(X, L)$.

Proposition 1.3.2.2 (Some constructive functions)**.**

1. *The function $\mathbf{1} : \tau \to \mathcal{C}(X, \mathbb{S})$ defined by $\mathbf{1}(U) = \mathbf{1}_U$ is an isomorphism of enumerative lattice,*

2. *The function $\mathrm{St} : \tau \times L \to \mathcal{C}(X, L)$ defined by $\mathrm{St}(U, l) = \mathrm{St}_U^l$ is constructive,*

3. *If $x \in X$ is constructive then the function $\mathrm{Eval}_x : \mathcal{C}(X, L) \to L$ defined by $\mathrm{Eval}_x(f) = f(x)$ is a morphism. The image of x by a constructive function is then constructive.*

Proof.

1. $\mathbf{1}$ commutes with suprema. As it is bijective, $\mathbf{1}^{-1}$ also commutes with suprema. $\mathbf{1}$ is a constructive bijection between the ideal sets: $\mathbf{1}(B_i) = \mathrm{St}^{\top}_{B_i}$.

2. $\mathrm{St}(\bigcup_{i\in E} B_i, \sup_{j\in E'} p_j) = \sup_{i\in E, j\in E'} \mathrm{St}^{p_j}_{B_i}$, so St is realized by the constructive function defined by $\Phi(E, E') = \{\langle i, j\rangle : i \in E, j \in E'\}$.

3. Eval_x commutes with suprema, and $\mathrm{Eval}_x(\mathrm{St}^{p_j}_{B_i})$ is constructive uniformly in $\langle i, j\rangle$. Indeed, it is p_j if $x \in B_i$, $\perp$ otherwise.

□

$\mathbb{N}$ with the discrete topology can be seen as an effective topological space, the basis being of course the set of singletons. Its topology is the enumerative lattice $2^{\mathbb{N}}$. $L^{\mathbb{N}}$ and $\mathcal{C}(\mathbb{N}, L)$ are isomorphic, so a sequence (l_n) of uniformly constructive elements, or constructive sequence, can be seen as a constructive element of $\mathcal{C}(\mathbb{N}, L)$.

Proposition 1.3.2.3 (Composition)**.** *Let X, Y be effective topological spaces, L, L' be enumerative lattices, and $f : X \to Y$ and $h : L \to L'$ be continuous functions.*

1. *For every $g \in \mathcal{C}(Y, L)$, $g \circ f \in \mathcal{C}(X, L)$ and $h \circ g \in \mathcal{C}(Y, L')$.*

$$\begin{tikzcd}
X \arrow[r, "f"] \arrow[dr, "g\circ f"'] & Y \arrow[d, "g"] \arrow[dr, "h\circ g"] & \\
& L \arrow[r, "h"] & L'
\end{tikzcd}$$

2. *Moreover, the following functions are Scott-continuous:*

$$\begin{array}{rcl} \mathrm{Comp}_f : C(Y, L) & \to & C(X, L) \\ g & \mapsto & g \circ f \end{array} \qquad \begin{array}{rcl} \mathrm{Comp}^h : C(Y, L) & \to & C(Y, L') \\ g & \mapsto & h \circ g \end{array}$$

3. *If f is constructively continuous and h is constructive, then Comp^f and Comp_h are constructive.*

Proof. Let $\mathrm{St}^{p_j}_{B_i} \in \mathcal{C}(Y, L)$: $\mathrm{Comp}_f(\mathrm{St}^{p_j}_{B_i}) = \mathrm{St}^{p_j}_{f^{-1}(B_i)}$ belongs to $\mathcal{C}(X, L)$. If f is constructively continuous, it is even constructive, uniformly in $\langle i, j\rangle$. As $\mathcal{C}(X, L)$ is closed under suprema and Comp_f commutes with suprema, the three results follow.

Let F_k be a finite subset of $\mathbb{N}$:

$$\mathrm{Comp}^h\left(\sup\left\{\mathrm{St}^{p_j}_{B_i} : \langle i, j\rangle \in F_k\right\}\right) = \sup\left\{\mathrm{St}\left(\bigcap_{\langle i,j\rangle\in I} B_i, h\left(\sup_{\langle i,j\rangle\in I} p_j\right)\right) : I \subseteq F_k\right\}$$

belongs to $\mathcal{C}(Y, L')$ and is constructive uniformly in k if h is constructive. As $\mathcal{C}(Y, L')$ is closed under suprema, and Comp^h is Scott-continuous, the three results follow. $\square$

Note that Comp_f is also a morphism of complete lattices, and a morphism of enumerative lattices when f is constructively continuous. If h is a morphism, then Comp^h is also a morphism. If f and h are isomorphisms, so are Comp_f and Comp^h.

Proposition 1.3.2.4 (Some isomorphisms)**.** *Let X, Y be effective topological spaces and L, L' be enumerative lattices. The following holds:*

$$\begin{array}{rrcll} & \mathcal{C}(X \times Y, L) & \equiv & \mathcal{C}(X, \mathcal{C}(Y, L)) & \textit{(curryfication)} \\ & \mathcal{C}(X, L \times L') & \equiv & \mathcal{C}(X, L) \times \mathcal{C}(X, L') & \textit{(vector functions)} \\ X \equiv Y \textit{ implies} & \mathcal{C}(X, L) & \equiv & \mathcal{C}(Y, L) & \textit{(left composition)} \\ L \equiv L' \textit{ implies} & \mathcal{C}(Y, L) & \equiv & \mathcal{C}(Y, L') & \textit{(right composition)} \end{array}$$

The first isomorphism is called $\mathrm{Curry} : C(X \times Y, L) \to C(X, C(Y, L))$, its inverse is called $\mathrm{Uncurry} : C(X, C(Y, L)) \to C(X \times Y, L)$.

Proof. Curry commutes with suprema. We recall that $\mathcal{B}_{X\times Y} = \{B_i \times B_j : B_i \in \mathcal{B}_X, B_j \in \mathcal{B}_Y\}$. The ideal step functions $\mathrm{St}(B_i \times B_j, p_k) \in \mathcal{C}(X \times Y, L)$ and $\mathrm{St}(B_i, \mathrm{St}(B_j, p_k)) \in \mathcal{C}(X, \mathcal{C}(Y, L))$ are both constructive uniformly in i, j, k: Curry and $\mathrm{Uncurry}$ simply exchange them.

$\mathrm{St}_{B_i}^{(p_j, \perp')} \in \mathcal{C}(X, L \times L')$ and $(\mathrm{St}_{B_i}^{p_j}, \perp') \in \mathcal{C}(X, L) \times \mathcal{C}(X, L')$ are constructive uniformly in i, j, and in correspondence via the isomorphism. Similarly for $\mathrm{St}_{B_i}^{(\perp, p'_j)}$ and $(\perp, \mathrm{St}_{B_i}^{p'_j})$.

The last two assertions are corollaries of proposition 1.3.2.3. $\square$

Two simple but useful observations can be made, taking $L = \mathbb{S}$.

1. Every constructively continuous function from X to Y induces a morphism $f^{-1} : \tau_Y \to \tau_X$, which is "conjugated" to $\mathrm{Comp}_f : \mathcal{C}(Y, \mathbb{S}) \to \mathcal{C}(X, \mathbb{S})$ in the following way: $\mathbf{1}_{f^{-1}U} = \mathbf{1}_U \circ f$, i.e. the following diagram commutes:

$$\begin{tikzcd} \mathcal{C}(Y, \mathbb{S}) \arrow[r, "\circ f"] & \mathcal{C}(X, \mathbb{S}) \\ \tau_Y \arrow[u, "\mathbf{1}"] \arrow[r, "f^{-1}"] & \tau_X \arrow[u, "\mathbf{1}"'] \end{tikzcd} \qquad (\circ f \text{ denotes } \mathrm{Comp}_f)$$

2. If $x \in X$ and $U \in \tau_{X \times Y}$ are constructive then the projection $U_x = \{y \in Y : (x, y) \in X\}$ is a constructive open set. Moreover, the function:

$$\begin{array}{rcl} \tau_{X \times Y} & \to & \mathcal{C}(X, \tau_Y) \\ U & \mapsto & (x \mapsto U_x) \end{array}$$

is an isomorphism, which is "conjugated" to Curry in the following way: $\mathbf{1}_{U_x} = \mathrm{Curry}(\mathbf{1}_U)(x)$, i.e. the following diagram commutes:

$$\begin{tikzcd} \mathcal{C}(X \times Y, \mathbb{S}) \arrow[r, "\mathrm{Curry}"] & \mathcal{C}(X, \mathcal{C}(Y, \mathbb{S})) \\ \tau_{X \times Y} \arrow[u, "\mathbf{1}"] \arrow[r] & \mathcal{C}(X, \tau_Y) \arrow[u, "\mathrm{Comp}^h"'] \end{tikzcd}$$

with $h = \mathbf{1} : \tau_Y \to \mathcal{C}(Y, \mathbb{S})$ (as h is an isomorphism, so is Comp^h).

Corollary 1.3.2.1. *If* $\inf : L \times L \to L$ *is constructive, then* $\inf : \mathcal{C}(X, L) \times \mathcal{C}(X, L) \to \mathcal{C}(X, L)$ *is constructive.*

Proof. If $\inf : L \times L \to L$ is constructive, then $\mathrm{Comp}^{\inf} : \mathcal{C}(X, L \times L) \to \mathcal{C}(X, L)$ is constructive. Using the isomorphism $\mathcal{C}(X, L) \times \mathcal{C}(X, L) \equiv \mathcal{C}(X, L \times L)$ gives the result. □

Restriction of functions

If D is a subset of X, a function $f : D \to L$ is constructive if it is a constructive element of $\mathcal{C}(D, L)$ where D has the induced effective topology. Actually, as $\mathrm{id} : D \to X$ is a morphism, the canonical surjection $\mathrm{Comp}_{\mathrm{id}} : \mathcal{C}(X, L) \to \mathcal{C}(D, L)$ which maps f to $f|_D$ is a morphism of enumerative lattices, so the constructive functions from D to L are exactly the constructive functions from X to L, restricted to D.

Relative constructivity

Definition 1.3.2.2 (Relative constructivity)**.** Let X be an effective topological space, L an enumerative lattice and $x \in X$. An element $y \in L$ is ***x-constructive*** if the function $f : \{x\} \to Y$ defined by $f(x) = y$ is constructive, which is equivalent to the existence of a constructive function $f \in \mathcal{C}(X, L)$ such that $f(x) = y$.

Via isomorphisms, the enumerative lattice $\mathcal{C}(\{x\}, L)$ can be interpreted in several equivalent ways, allowing to express nicely x-constructivity.

Consider the enumerative lattice $\mathcal{C}(\{x\}, L)$. As a complete lattice, it is isomorphic to L: to $f \in \mathcal{C}(\{x\}, L)$ is associated $f(x) \in L$, and to $y \in L$ is associated the function $x \mapsto y$. But as enumerative lattices, they are not isomorphic in general, unless x is constructive. There is a way of defining an alternative enumerative lattice structure on L to make it isomorphic to $\mathcal{C}(\{x\}, L)$: consider $(L, \leq, \mathcal{P}^x)$ where $\mathcal{P}^x = \{\mathrm{St}_{B_i}^{p_j}(x) : i, j \in \mathbb{N}\}$ inherits the numbering of step functions. We denote this enumerative lattice by L^x. The enumerative lattices L^x and $\mathcal{C}(\{x\}, L)$ are now isomorphic, and the constructive elements of L^x are the x-constructive elements of L.

When $L = \mathbb{S}$, one shall interpret $\mathbb{S}^x$ as the space of semi-decidability relative to x. Let us illustrate this: if X, Y are effective topological spaces, $x \in X$ and $y \in Y$, we defined

$$y \text{ is constructive} \iff \text{the function } \delta_y : \tau \to \mathbb{S} \text{ is constructive.}$$

We can state:

$$y \text{ is } x\text{-constructive} \iff \text{the function } \delta_y : \tau \to \mathbb{S}^x \text{ is constructive.}$$

which can be expressed as the semi-decidability relative to x of the the relation "$y \in U$". Indeed, let $f : \{x\} \to Y$ be the function defined by $f(x) = y$: by definition y is x-constructive if and only if f is constructively continuous. As $\tau_{\{x\}} \equiv \mathcal{C}(\{x\}, \mathbb{S}) \equiv \mathbb{S}^x$, δ_y is "conjugated" to $f^{-1} : \tau_Y \to \tau_{\{x\}}$ in the following way:

$$\begin{tikzcd}
\tau_Y \arrow[d, "f^{-1}"] & = & \tau_Y \arrow[d, "\delta_y"] \\
\tau_{\{x\}} & \equiv & \mathbb{S}^x
\end{tikzcd}$$

so f is constructively continuous if and only if $\delta_y : \tau_Y \to \mathbb{S}^x$ is constructive.

The isomorphic enumerative lattices $\mathcal{C}(Y, L)^x \equiv \mathcal{C}(\{x\}, \mathcal{C}(Y, L)) \equiv \mathcal{C}(Y, \mathcal{C}(\{x\}, L)) \equiv \mathcal{C}(Y, L^x)$ induces three equivalent notions:

1. constructive elements of $\mathcal{C}(Y, L)^x$,
2. x-constructive elements of $\mathcal{C}(Y, L)$,
3. constructive elements of $\mathcal{C}(Y, L^x)$,

which we call x-constructive functions from Y to L.

1.4 More on enumerative lattices

1.4.1 Computable enumerative lattice

Generally, the Scott-topology on an enumerative lattice is not second-countable (it is always T_0), so it cannot be made an effective topological space.

For $x \in L$, define $\uparrow x = \{y \in L : x \leq y\}$. These sets have no reason to be Scott-open sets (in $\overline{\mathbb{R}}$ for instance, $\uparrow x = [x, +\infty]$ is not Scott-open). A candidate for a countable basis of the topology is the family $\{\mathrm{Int}(\uparrow d) : d \in \mathcal{D}\}$, where $\mathrm{Int}(A)$ is the interior of A, i.e. the union of all open sets contained in A and $\mathcal{D}$ is the set of finite supremum of simple elements of $\mathcal{P}$ (see what follows definition 1.2.0.3). Let us try to understand these sets.

If $y \in \mathrm{Int}(\uparrow x)$, then for every directed set A with $y \leq \sup A$, $\sup A \in \mathrm{Int}(\uparrow x)$ so there is $a \in A \cap \mathrm{Int}(\uparrow x)$, so $x \leq a$. It follows that $x \ll y$, where $\ll$ is the ***way-below*** relation, defined as:

Definition 1.4.1.1 (Way-below). $x \ll y$ if for any directed set A, $[y \leq \sup A \implies \exists a \in A, x \leq a]$.

This relation is a classical concept in domain theory, see [AJ94].

The characterization of the Scott-topology on an enumerative lattice (see proposition 1.2.0.1) gives a characterization of the way-below relation: $x \ll y$ if and only if for all $A \subseteq \mathcal{P}$,

$$y \leq \sup A \implies \text{there is a finite set } A_0 \subseteq A \text{ such that } x \leq \sup A_0.$$

Define $\mathrel{\Uparrow} x := \{y \in L : x \ll y\}$ and $\mathrel{\Downarrow} x := \{d \in \mathcal{D} : d \ll x\}$. The way-below relation satisfies the following properties:

1. $x \ll y \implies x \leq y$,
2. $x' \leq x \ll y \leq y' \implies x' \ll y'$,
3. $x, x' \ll y \iff \sup\{x, x'\} \ll y$.

Point 1 implies that $\sup \mathrel{\Downarrow} x \leq x$. Point 3 implies that $\mathrel{\Uparrow} \sup\{x, x'\} = \mathrel{\Uparrow} x \cap \mathrel{\Uparrow} x'$.

Examples.
1. On $(\mathbb{S}, \leq, \{\top\})$, $\ll$ is $<$,
2. On $(\overline{\mathbb{R}}, \leq, \mathbb{Q})$: $\ll$ is $<$,
3. On $(P(\mathbb{N}), \subseteq, \{singletons\})$, $\ll$ is $\subseteq$,

4. The Euclidean topological space $(\mathbb{R}, \tau_{\mathbb{R}}, \mathcal{B})$ is effective, with the rational open intervals as ideal open sets. On the enumerative lattice $(\tau_{\mathbb{R}}, \subseteq, \mathcal{B})$, $U \ll V \iff \overline{U} \subseteq V$ and $\overline{U}$ is compact.

We now define the notion of computable enumerative lattice, which is like an effective given continuous domain (see [ES99]) in the case when the poset is a complete lattice. Let us recall that the set $\mathcal{D}$ of finite suprema of simple elements has a natural numbering $\{d_i : i \in \mathbb{N}\}$.

Definition 1.4.1.2. A ***computable enumerative lattice*** is an enumerative lattice $(L, \leq, \mathcal{P})$ satisfying:

1. $x = \sup \mathop{\downarrow\!\!\!\!\downarrow} x$ for all $x \in L$,
2. the set $\{(i, j) : p_i \ll d_j\}$ is r.e.

To prove the first point, one just has to show that $x \leq \sup \mathop{\downarrow\!\!\!\!\downarrow} x$. On a computable enumerative lattice, the set $\{(i, j) : d_i \ll d_j\}$ is also r.e: $\sup\{p_{i_1}, \ldots, p_{i_k}\} \ll d_j \iff p_{i_1} \ll d_j, \ldots, p_{i_k} \ll d_j$.

The first three examples given above are computable enumerative lattices. If $(X, \tau, \mathcal{B})$ is any effective topological space, its topology is not in general a computable enumerative lattice.

On a computable enumerative lattice, one has the interpolation property, which is a classical result on continuous domains (see [AJ94]) (wee write the proof for completeness):

Lemma 1.4.1.1 (Interpolation). *If $d \ll y$ there exists $d' \in \mathcal{D}$ with $d \ll d' \ll y$.*

Proof. As $\mathop{\downarrow\!\!\!\!\downarrow} d$ is directed for all d, so is $D = \bigcup_{d \ll y} \mathop{\downarrow\!\!\!\!\downarrow} d$. Hence, if $d \ll \sup D$ there is $d' \in D$ such that $d \leq d'$, so $d \in D$. Now, $\sup D = \sup\{\sup \mathop{\downarrow\!\!\!\!\downarrow} d : d \ll y\} = \sup\{d : d \ll y\} = \sup \mathop{\downarrow\!\!\!\!\downarrow} y = y$. It follows that $\mathop{\downarrow\!\!\!\!\downarrow} y \subseteq D$, which gives the result. □

Proposition 1.4.1.1 (Effective topology). *Let $(L, \leq, \mathcal{P})$ be a computable enumerative lattice. The family $\mathcal{B} = \{\mathop{\uparrow\!\!\!\!\uparrow} d = Int(\uparrow d) : d \in \mathcal{D}\}$ is a basis of the Scott-topology, the family $\{\mathop{\uparrow\!\!\!\!\uparrow} p = Int(\uparrow p) : p \in \mathcal{P}\}$ being a sub-basis: $\mathop{\uparrow\!\!\!\!\uparrow} \sup\{p_{i_1}, \ldots, p_{i_n}\} = \mathop{\uparrow\!\!\!\!\uparrow} p_{i_1} \cap \ldots \cap \mathop{\uparrow\!\!\!\!\uparrow} p_{i_n}$. It makes $(L, \tau_{Scott}, \mathcal{B})$ an effective topological space.*

Proof. First, $\mathop{\uparrow\!\!\!\!\uparrow} d$ is Scott-open: if A is directed and $\sup A \in \mathop{\uparrow\!\!\!\!\uparrow} d$, by the interpolation lemma there is $d' \in \mathcal{D}, d \ll d' \ll \sup A$, so there is some $a \in A$ with $d' \leq a$, which implies $a \in \mathop{\uparrow\!\!\!\!\uparrow} d$. We already know that $\mathrm{Int}(\uparrow d) \subseteq \mathop{\uparrow\!\!\!\!\uparrow} d$: as $\mathop{\uparrow\!\!\!\!\uparrow} d \subseteq \uparrow d$ is Scott-open, they actually coincide.

Now, the family $\mathcal{B} = \{\Uparrow d : d \in \mathcal{D}\}$ is a basis: for every Scott-open set U, $U = \bigcup_{d \in U} \Uparrow d$. Indeed, if $x \in U$, as $x = \sup \Downarrow x$ and $\Downarrow x$ is directed, there is $d \in \Downarrow x \cap U$: then $x \in \Uparrow d$. As this basis is closed under finite intersections in a constructive way, $(L, \tau, \mathcal{B})$ is an effective topological space. □

Remark that $x \in L$ is a constructive point of the effective topological space $(L, \tau, \mathcal{B})$ if and only if $\{i : p_i \ll x\}$ is r.e. Indeed, $d_k \ll x \iff \forall i \in F_k, p_i \ll x$, so if the latter is true, then $\{k : x \in \Uparrow d_k\}$ is r.e.

On a computable enumerative lattice, convergence of sequences has a nice characterization:

Proposition 1.4.1.2 (Limits of a sequence). *In a computable enumerative lattice, x_n converges to x if and only if $x \leq \liminf x_n$.*

Proof. We already know that in a complete lattice, if $x \leq \liminf x_n$ then x_n converges to x (see proposition B.2.0.7).

If x_n converges to x, then for each $d \in \Downarrow x$, $\liminf x_n \geq d$. Indeed, x belongs to the Scott-open set $\Uparrow d$ so there is k such that $x_n \in \Uparrow d$ for all $n \geq k$. It follows that $\inf\{x_n : n \geq k\} \geq d$, so $\liminf x_n \geq d$. Hence, $\liminf x_n \geq \sup \Downarrow x = x$. □

Constructivity in $(L, \leq, \mathcal{P})$ vs constructivity in $(L, \tau, \mathcal{B})$

We now compare the different notions of constructivity provided by the enumerative and the effective topological structures. We will use the following lemma (in the title of the lemma, L^{comp} means that the enumerative lattice L is computable):

Lemma 1.4.1.2 (Constructivities of $\mathrm{id} : L^{\text{comp}} \to L^{\text{comp}}$). *Let L be a computable enumerative lattice (and then also an effective topological space). The identity function $\mathrm{id} : L \to L$ is:*

1. *a constructive element of $\mathcal{C}(L, L)$,*
2. *a morphism of enumerative lattices,*
3. *a morphism of effective topological spaces.*

Proof. 1. $\mathrm{id} = \sup\{\mathrm{St}^{d_i}_{\Uparrow d_i} : d_i \in \mathcal{D}\} = \sup\{\mathrm{St}^{p_i}_{\Uparrow p_i} : p_i \in \mathcal{P}\}$. 2. 3. are obvious (they are already true when L is a plain enumerative lattice or an effective topological space). □

Proposition 1.4.1.3 (Constructive element of L^{comp})**.** *Let $(L, \leq, \mathcal{P})$ be a computable enumerative lattice. $x \in L$ is a constructive element of the enumerative lattice $(L, \leq, \mathcal{P})$ if and only if it is a constructive point of the effective topological space $(L, \tau, \mathcal{B})$.*

Proof. If x is a constructive point, i.e. $\{i : x \in \Uparrow d_i\}$ is r.e., then $x = \sup \Downarrow x = \sup\{p_j : p_j \ll x\}$ is a constructive element.

If x is a constructive element, there is a r.e. set $E \subseteq \mathbb{N}$ such that $x = \sup\{p_j : j \in E\}$. Then, $d_i \ll x$ if and only if E has a finite subset F_k such that $d_i \ll d_k = \sup_{j \in F_k} p_j$, which is semi-decidable (i.e. $\{i : d_i \ll x\}$ is r.e.). □

Proposition 1.4.1.4 (Functions from L^{comp} to L')**.** *Let L, L' be enumerative lattices, where L is computable. For a function $f : L \to L'$, the following are equivalent:*

1. *f is Scott-continuous,*
2. *$f(x) = \sup f(\Downarrow x)$ for all x,*
3. *$f \in \mathcal{C}(L, L')$.*

The following are equivalent:

i) f is a constructive function between enumerative lattices,

ii) f is a constructive element of $\mathcal{C}(L, L')$.

Proof. $[1 \Rightarrow 2]$: as $\Downarrow x$ is a directed set, the Scott-continuity of f directly implies $f(x) = f(\sup \Downarrow x) = \sup f(\Downarrow x)$. $[2 \Rightarrow 3]$: $f = \sup\{\mathrm{St}(\Uparrow d_i, f(d_i)) : i \in \mathbb{N}\}$. Indeed, $f(x) = \sup f(\Downarrow x) = \sup\{f(d_i) : x \in \Uparrow d_i\}$. $[3 \Rightarrow 1]$: we already know that elements of $\mathcal{C}(X, L')$ are continuous functions, for any topological space X.

Remark that $[1 \Rightarrow 3]$ is a direct consequence of proposition 1.3.2.3, applied to $h = f : L \to L'$ and $g = \mathrm{id} \in \mathcal{C}(L, L)$: $h \circ g = f \in \mathcal{C}(L, L')$, using that f is continuous. When f is constructive, the same proposition gives $[(i) \Rightarrow (ii)]$.

$[(ii) \Rightarrow (i)]$: if f is a constructive element of $\mathcal{C}(L, L')$, then $f = \sup\{\mathrm{St}^{p_j}_{\Uparrow d_i} : (i, j) \in E\}$ for some r.e. set E. So $f(d_k) = \sup\{p_j : (i, j) \in E, d_i \ll d_k\}$ is constructive, uniformly in k. □

Proposition 1.4.1.5 (Functions from X to L^{comp})**.** *Let X be an effective topological space and L a computable enumerative lattice. For a function $f : X \to L$, the following are equivalent:*

1. *f is continuous,*

2. *$f(x) \leq \liminf f(x_n)$ for every sequence x_n converging to x,*

3. *$f \in \mathcal{C}(X, L)$.*

The following are equivalent:

i) *f is constructively continuous,*

ii) *f is a constructive element of $\mathcal{C}(X, L)$.*

Proof. $[1 \Rightarrow 3]$ and its constructive version $[(i) \Rightarrow (ii)]$ follow again from proposition 1.3.2.3, applied to $f : X \to L$ and $g = \mathrm{id} \in \mathcal{C}(L, L)$: $g \circ f = f \in \mathcal{C}(X, L)$.

$[3 \Rightarrow 1]$: we already know that every function in $\mathcal{C}(X, L)$ is continuous.

$[1 \Leftrightarrow 2]$: as L with the Scott-topology is a sequential space (proposition 1.2.0.1), f is continuous if and only if it is sequentially continuous. By proposition 1.4.1.2, point 2 can be read "f is sequentially continuous".

$[(ii) \Rightarrow (i)]$: if f is a constructive element of $\mathcal{C}(X, L)$, then $f = \sup\{\mathrm{St}_{B_i}^{p_j} : \langle i, j \rangle \in E\}$ for some r.e. set E. $f^{-1}(\Uparrow d_k) = \bigcup\{B_{i_1} \cap \ldots \cap B_{i_n} : d_k \ll \sup\{p_{j_1}, \ldots, p_{j_n}\}, \langle i_1, j_1 \rangle, \ldots, \langle i_n, j_n \rangle \in E\}$ is a constructive open set, uniformly in k. □

It follows from this proposition that when L is a computable enumerative lattice, every continuous function $f : D \to L$ can be extended to a continuous function on the whole space X. Indeed, if $f : D \to L$ is continuous then $f \in \mathcal{C}(D, L)$ by the preceding proposition, so it can be extended to a continuous function from X to L.

On a computable enumerative lattice, one has the following property, which is already established for bounded complete continuous domains (see [AJ94]). We write the proof for self-containedness.

Proposition 1.4.1.6 (Constructivity of $\inf$)**.** *If $(L, \leq, \mathcal{P})$ is a computable enumerative lattice, then* $\inf : L \times L \to L$ *is constructive.*

Proof. The product $L \times L$ is a computable enumerative lattice, and $(x, y) \ll (x', y') \iff x \ll x', y \ll y'$. To avoid confusions, let us denote the function $\inf$ by $f : L \times L \to L$. We use the characterization given by proposition 1.4.1.4 and show that $f(x, y) = \sup\{f(d, d') : (d, d') \ll (x, x')\}$.

First, $f(x,y) = \sup(\twoheaddownarrow x \cap \twoheaddownarrow y)$: indeed, $f(x,y) = \sup \twoheaddownarrow(f(x,y)) \leq \sup(\twoheaddownarrow x \cap \twoheaddownarrow y)$ as $d \ll \inf\{x,y\} \implies d \ll x, y$, and $\sup(\twoheaddownarrow x \cap \twoheaddownarrow y) \leq x, y$. Then, $\twoheaddownarrow x \cap \twoheaddownarrow y = (\bigcup_{d \ll x} \twoheaddownarrow d) \cap (\bigcup_{d' \ll x} \twoheaddownarrow d') = \bigcup_{(d,d') \ll (x,x')} (\twoheaddownarrow d \cap \twoheaddownarrow d')$. So,

$$\begin{aligned} f(x,y) &= \sup(\twoheaddownarrow x \cap \twoheaddownarrow y) \\ &= \sup\{\sup(\twoheaddownarrow d \cap \twoheaddownarrow d') : (d,d') \ll (x,x')\} \\ &= \sup\{f(d,d') : (d,d') \ll (x,x')\} \end{aligned}$$

As $\twoheaddownarrow d_i \cap \twoheaddownarrow d'_j$ is r.e. uniformly in in $\langle i,j \rangle$, $f(d_i, d_j)$ is constructive uniformly in i. $\square$

Note that $\inf$ is never a morphism of complete lattices, unless $L = \{\bot\}$: $\inf\{\sup(\mathcal{P} \times \{\bot\} \cup \{\bot\} \times \mathcal{P})\} = (\top, \top)$ and $\sup\{\inf\{x,x'\} : (x,x') \in \mathcal{P} \times \{\bot\} \cup \{\bot\} \times \mathcal{P}\} = (\bot, \bot)$. Note also that $\inf$ need not be distributive on $\sup$: consider the following computable enumerative lattice ($\ll$ is exactly $\leq$), where $p_1 \wedge (p_2 \vee p_3) = p_1$ and $(p_1 \wedge p_2) \vee (p_1 \wedge p_3) = \bot$:

$$\begin{tikzcd}[arrows=-] & \top \arrow[dl] \arrow[d] \arrow[dr] & \\ p_1 \arrow[dr] & p_2 \arrow[d] & p_3 \arrow[dl] \\ & \bot & \end{tikzcd}$$

As a computable enumerative lattice is also an effective topological space, definition 1.3.0.9 gives a notion of constructive closed subset: a closed set $A \subseteq L$ is constructive if the function $\iota_A : \tau_L \to \mathbb{S}$ defined by $\iota_A(U) =$ "$A \cap U \neq \emptyset$" is constructive. For instance, $A = \downarrow x = \{y \leq x\}$ is a constructive closed set when x is constructive. Indeed, $A \cap \twoheaduparrow d \neq \emptyset \iff d \ll x \iff x \in \twoheaduparrow d$ by the interpolation lemma, and more generally $A \cap U \neq \emptyset \iff x \in U$, so $\iota_A = \delta_x$. As x is a constructive element of a computable enumerative lattice, it is a constructive point of the corresponding effective topological space (proposition 1.4.1.3) i.e. δ_x is constructive.

Proposition 1.4.1.7 (Effective enumeration in constructive closed sets)**.** *Let $(L, \leq, \mathcal{P})$ be a computable enumerative lattice and A a constructive closed subset of L. There is a effective enumeration of all the constructive elements of A.*

Proof. Let $(E_e)_{e \in \mathbb{N}}$ be the enumeration of the r.e. subsets of $\mathbb{N}$. There is a total recursive function φ such that $E_e = \bigcup_n F_{\varphi(e,n)}$ with $F_{\varphi(e,n)} \subseteq F_{\varphi(e,n+1)}$.

Define $x_e = \sup\{d_{\varphi(e,n)} : A \cap \Uparrow d_{\varphi(e,n)} \neq \emptyset\}$. As $d_{\varphi(e,n)} \leq d_{\varphi(e,n+1)}$ and all $d_{\varphi(e,n)}$ belong to A, there supremum belongs to A.

Now, if x is a constructive point of A, then $E = \{i : p_i \in \Downarrow x\}$ is r.e, so there is e such that $E = E_e$. We claim that $x = x_e$. Indeed, for every n, $d_{\varphi(e,n)} \ll x$ so $x \in A \cap \Uparrow d_{\varphi(e,n)} \neq \emptyset$, so $x_e = \sup_n d_{\varphi(e,n)} = x$. □

This proposition can be used to derive a well-known result in randomness and complexity theory: the effective enumerability of semi-measures on $\mathbb{N}$, i.e. sequences of uniformly lower semi-computable real numbers whose sum is ≤ 1:

Proposition 1.4.1.8. *The enumerative lattice $\mathcal{C}(\mathbb{N}, [0,1])$ of sequences of real numbers is computable. The subset of sequences $(x_n)_n$ satisfying $\sum_n x_n \leq 1$ is a constructive closed set.*

Proof. For $x, y \in \mathcal{C}(\mathbb{N}, [0,1])$, $x \ll y \iff x_n = 0$ or $x_n < y_n$ for all n, which is semi-decidable when x is a simple element (null at each n but one).

Let x be a finite supremum of simple elements: $x_n = 0$ for all $n \notin I$ where I is a finite subset of $\mathbb{N}$. $\Uparrow x \cap A \neq \emptyset \iff \exists y \in A$ with $x_n < y_n$ for $n \in I$, which is equivalent to $\sum_n x_n < 1$, which can be semi-decided. □

Another application will be the effective enumerability of randomness tests on the Cantor space (see section 3.1.1).

1.4.2 Pseudo-computable enumerative lattice

The computability of an enumerative lattice is a strong condition, which is not satisfied in general by topologies. For instance, we saw that the Euclidean topology on $\mathbb{R}$ is a computable enumerative lattice. The induced topology on $\mathbb{Q}$ is an effective topological space, so the induced topology is an enumerative lattice, which is no more computable. However, the underlying topology on $\mathbb{R}$ makes this enumerative lattice "pseudo-computable".

We will see that for a large class of effective topological spaces, namely computable metric spaces, the topology as an enumerative lattice is pseudo-computable.

Definition 1.4.2.1. An enumerative lattice $(L, \leq, \mathcal{P})$ is ***pseudo-computable*** if there is a binary relation $\lhd$ on $\mathbb{N}$ satisfying:

1. $i \lhd j \implies p_i \leq p_j$,

2. for all i, j, $\inf\{p_i, p_j\} = \sup_{\mathcal{P}}(\Downarrow i \cap \Downarrow j)$, where $\Downarrow i = \{k \in \mathbb{N} : k \lhd i\}$,

3. $\{(i, j) : i \lhd j\}$ is r.e.

We will sometimes write $p_i \lhd p_j$ for $i \lhd j$, which makes sense when the indexes of p_i and p_j are written. If $(L, \leq, \mathcal{P})$ and $(L', \sqsubseteq, \mathcal{Q})$ are pseudo-computable enumerative lattices, in the expressions $p_i \lhd p_j$ and $q_i \lhd q_j$, two different relations on $\mathbb{N}$ are actually involved (one for each enumerative lattice).

Every computable enumerative lattice is pseudo-computable: take $i \lhd j$ if and only if $p_i \ll p_j$.

Let $x \in L$: $x = \sup_{i \in E} p_i$ for some set $E \subseteq \mathbb{N}$. Defining $\Downarrow E = \bigcup_{i \in E} \Downarrow i$, one has $x = \sup_{\mathcal{P}}(\Downarrow E)$. Indeed, $\sup_{\mathcal{P}}(\Downarrow E) = \sup_{i \in E} \sup_{\mathcal{P}}(\Downarrow i) = \sup_{i \in E} p_i = x$.

Proposition 1.4.2.1 (Constructivity of $\inf$)**.** *Let $(L, \leq, \mathcal{P})$ be a pseudo-computable enumerative lattice. If $\inf$ distributes over $\sup$ then $\inf : L \times L \to L$ is constructive.*

Proof. $\inf\{x, y\} = \inf\{\sup_{i \in E} p_i, \sup_{i \in E'} p_i\} = \sup\{\inf\{p_i, p_j\} : i \in E, j \in E'\} = \sup\{\sup_{\mathcal{P}}(\Downarrow i \cap \Downarrow j) : i \in E, j \in E'\} = \sup_{\mathcal{P}}(\bigcup_{i,j} \Downarrow i \cap \Downarrow j) = \sup_{\mathcal{P}}(\Downarrow E \cap \Downarrow E')$.

By the third condition, the function $\Downarrow : P(\mathbb{N}) \to P(\mathbb{N})$ is constructive. As $\cap : P(\mathbb{N}) \times P(\mathbb{N}) \to P(\mathbb{N})$ is constructive, $\inf$ is realized by the constructive function $\cap \circ (\Downarrow, \Downarrow) : P(\mathbb{N}) \times P(\mathbb{N}) \to P(\mathbb{N})$. □

Proposition 1.4.2.2. *Let $(X, \tau, \mathcal{B})$ be an effective topological space and $(L, \leq, \mathcal{P})$ be an enumerative lattice. If τ_X and L are pseudo-computable enumerative lattices, then so is $\mathcal{C}(X, L)$.*

Proof. Define $\mathrm{St}_{B_i}^{p_j} \lhd \mathrm{St}_{B_{i'}}^{p_{j'}} \iff B_i \lhd B_{i'}$ and $p_j \lhd p_{j'}$. This relation is obviously r.e. As $\mathrm{St} : \tau_X \times L \to \mathcal{C}(X, L)$ is monotonic, the first condition on $\lhd$ come directly from the same condition for τ_X and L. For the second condition,

$$\begin{aligned}
\inf\{\mathrm{St}_{B_i}^{p_j}, \mathrm{St}_{B_{i'}}^{p_{j'}}\} &= \mathrm{St}_{B_i \cap B_{i'}}^{\inf\{p_j, p_{j'}\}} \\
&= \mathrm{St}(\sup_{\mathcal{B}}(\Downarrow i \cap \Downarrow i'), \sup_{\mathcal{P}}(\Downarrow j \cap \Downarrow j')) \\
&= \sup\{\mathrm{St}_{B_k}^{p_l} : k \in \Downarrow i \cap \Downarrow i', l \in \Downarrow j \cap \Downarrow j'\} \\
&= \sup\{\mathrm{St}_{B_k}^{p_l} : \langle k, l\rangle \in \Downarrow \langle i, j\rangle \cap \Downarrow \langle i', j'\rangle\}
\end{aligned}$$

□

Definition 1.4.2.2 (Constructive closed set)**.** In a pseudo-computable enumerative lattice $(L, \leq, \mathcal{P})$, a closed subset A is ***constructive*** if the set $\{i : A \cap \Uparrow F_i \neq \emptyset\}$ is r.e.

We extend the relation $\lhd$ to $P(\mathbb{N}) \times P(\mathbb{N})$: $E \lhd E'$ if for every $i \in E$ there is $j \in E$ with $i \lhd j$. For a finite set F, $F \lhd E$ if and only if there is $F' \subseteq E$ of same cardinality such that $F \lhd F'$. We define $\Uparrow F = \{\sup\{p_i : i \in F'\} : F \lhd F'\}$.

Theorem 1.4.2.1 (Uniform numeration in constructive closed sets)**.** *Let L be a pseudo-computable enumerative lattice and A a constructive closed subset of L. There is a constructive enumeration of* all *the constructive elements of A.*

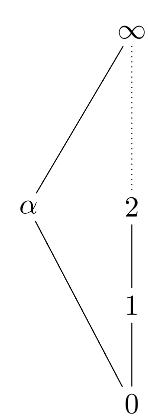
Proof. Let $p_i \in A$. For each $F \lhd \{i\}$, $p_i \in A \cap \Uparrow F \neq \emptyset$. So $p_j = \sup\{d_F : F \lhd \{i\}, A \cap \Uparrow F \neq \emptyset\}$. If $x \in A$ is constructive, $x = \sup_{i \in E} p_i$ for some r.e. set E. So $x = \sup\{d_F : F \lhd E, A \cap \Uparrow F \neq \emptyset\}$.

Let $(E_e)_{e \in \mathbb{N}}$ be the enumeration of the r.e. subsets of $\mathbb{N}$. There is a total recursive function φ such that $E_e = \bigcup_n F_{\varphi(e,n)}$ with $F_{\varphi(e,n)} \subseteq F_{\varphi(e,n+1)}$.

Define $x_e = \sup\{d_{\varphi(e,n)} : A \cap \Uparrow F\varphi(e,n) \neq \emptyset\}$. As $d_{\varphi(e,n)} \leq d_{\varphi(e,n+1)}$ and all $d_{\varphi(e,n)}$ belong to F, their supremum belongs to F. If $x \in A$ is constructive, $x = \sup_{i \in E} p_i$ for some r.e. set E. Let $E' = \bigcup_{i \in E} \Downarrow i$. E' is r.e, so $E' = E_e$ for some e. We claim that $x = x_e$. Indeed, for each $F \subseteq E'$, there is $F' \subseteq E$ with $F \lhd F'$. As $d'_F \leq x$, $d'_F \in A \cap \Uparrow F \neq \emptyset$. So $x_e = \sup\{d_{\varphi(e,n)} : n \in \mathbb{N}\} = x$. $\square$

1.4.3 An enumerative lattice which is not computable

We give an example of enumerative lattice which is not computable and is a source of counter-examples. This example already appeared in [AJ94]. Consider the following enumerative lattice $L = \mathbb{N} \cup \{\alpha, \infty\}$ with $\mathcal{P} = \mathbb{N} \cup \{\alpha\}$ for instance.



The way-below relation is $0 \ll x$ for all x, $n \ll x$ for all $x \in [n, +\infty]$. But α is not way-below ∞ (and then, not way-below itself): $\alpha \leq \infty = \sup \mathbb{N}$ but $\alpha \not\ll n$ for all $n \in \mathbb{N}$. It implies that $\sup \Downarrow\alpha = 0 < \alpha$, so L is not a computable enumerative lattice.

The Scott-open sets are $[n, \infty]$ for $n \in \mathbb{N}$, $n > 0$ and $\{\alpha\} \cup [n, \infty]$ for $n \in \mathbb{N}$. The Scott-open sets $\Uparrow x$ are not a basis of the topology, as they do not generate the sets $\{\alpha\} \cup [n, \infty]$ for $n > 0$.

Nevertheless, L is an effective topological space, with all the open sets as a countable basis.

Convergence Define the sequence $x_{2n} = n$ and $x_{2n+1} = \alpha$: x_i converges to α, as every open set containing α is one of the sets $\{\alpha\} \cup [n, +\infty]$ which contains x_i for all $i \geq 2n$. But $\alpha \not\leq \liminf x_i = 0$.

Continuity $\mathrm{id} : L \to L$ is of course continuous, but is not in $\mathcal{C}(L, L)$. Indeed, the preceding sequence x_n converges to α, but $\mathrm{id}(\alpha) \not\leq \liminf \mathrm{id}(x_n)$.

We also exhibit an example of a continuous function from $[0, 1]$ to L which is not in $\mathcal{C}(X, L)$. Let us define $g : [0, 1] \to L$ in the following way: $g(0) = \alpha$, $g = n$ on $[2^{-(n+1)}, 2^{-n})$ for $n \in \mathbb{N}$ and $g(1) = 0$. g is continuous, but once again $g \notin \mathcal{C}([0, 1], L)$: defining $y_{2n} = 2^{-(n+1)}$ and $y_{2n+1} = 0$, one has $y_n \to 0$ and $g(y_n) = x_n$.

The function $\inf : L \times L \to L$ is not continuous: $\mathbb{N}$ is directed, but $\inf\{\alpha, \sup \mathbb{N}\} = \alpha$ and $\sup\{\inf\{\alpha, n\} : n \in \mathbb{N}\} = 0$.

Constructivity $\mathrm{id} : L \to L$ is obviously a morphism of enumerative lattices and a morphism of effective topological spaces. As $\mathrm{id} \notin \mathcal{C}(L, L)$, id is *a fortiori* not a constructive element of $\mathcal{C}(L, L)$.

1.5 Computability on $\mathbb{R}$

In this section, we present the different well-known notions of computability on the set of real numbers, expressed with the computability structures developed so far.

Computability

The Euclidean topology on $\mathbb{R}$ is effective: the rational open intervals form a countable basis. A real number or a function from some set to $\mathbb{R}$ is ***computable*** if it is constructive, $\mathbb{R}$

being endowed with the effective Euclidean topology.

The Euclidean topology $\tau_{\mathbb{R}}$ on $\mathbb{R}$ is a computable enumerative lattice, the way-below relation being $U \ll V \iff \overline{U}$ compact and $\overline{U} \subseteq V$.

Lower semi-computability

$\mathbb{R}$ can also be endowed with the right-topology, or topology of lower semi-continuity, given by the open sets $(x, +\infty)$. $\mathbb{R}$ is also an effective topological space for this topology, but this can be expressed in the following way.

We add the infinites to $\mathbb{R}$: $\overline{\mathbb{R}} = \mathbb{R} \cup \{-\infty, +\infty\}$ and endow it with the natural order $\leq$. It is a computable enumerative lattice, with $\mathbb{Q}$ as set of ideal elements, the way-below relation being the strict order $<$.

To express that a real number is constructive as an element of this enumerative lattice, we will say that it is a ***lower semi-computable*** real number. In a similar way, we will say that a function from some set to $\overline{\mathbb{R}}$ is lower semi-computable if it is a constructive function when $\overline{\mathbb{R}}$ is endowed with this enumerative lattice structure.

We will sometimes restrict ourselves to $\overline{\mathbb{R}}^+ = [0, +\infty) \cup \{+\infty\}$ or to $[0, 1]$, which are also computable enumerative lattices.

Upper semi-computability

Reversing the order gives another computable enumerative lattice, whose constructive elements are the ***upper semi-computable*** real numbers.

Relations

The topology of lower semi-continuity $\tau_{\leq}$ on $(\overline{\mathbb{R}}, \leq, \mathbb{Q})$, is a computable enumerative lattice which is isomorphic to $(\overline{\mathbb{R}}, \geq, \mathbb{Q})$. In particular, the constructive open subsets of $(\overline{\mathbb{R}}, \leq, \mathbb{Q})$ are the sets $(x, +\infty]$ where x is upper semi-computable.

Conversely, the topology of upper semi-continuity $\tau_{\geq}$ on $(\overline{\mathbb{R}}, \leq, \mathbb{Q})$, is isomorphic to $(\overline{\mathbb{R}}, \leq, \mathbb{Q})$: the constructive open sets are the sets $[-\infty, x)$ where x is lower semi-computable.

The function $\mathrm{id} : \mathbb{R} \to \mathbb{R}$ is both lower and upper semi-computable: it means that id is a constructive or recursively continuous function from the effective topological space $\mathbb{R}$ to the computable enumerative lattice $(\overline{\mathbb{R}}, \leq, \mathbb{Q})$ (resp. $(\overline{\mathbb{R}}, \geq, \mathbb{Q})$).

On a totally ordered set X, the *order topology* can be defined (not to be confused with the Scott-topology !): it is the topology generated by the sub-base of "open rays" $\{x : a < x\}, \{x : x < b\}$ for all $a, b \in X$. The open rays together with the intervals $\{x : a < x < b\}$ form a basis of the order topology.

This can be applied to $\mathbb{R}$ with the natural order: the order topology is then the euclidean topology. This can also be applied to $\overline{\mathbb{R}}$ or $\overline{\mathbb{R}}^+$, still with the natural order: the order topology is the euclidean topology together with the sets $[-\infty, x)$, $(x, +\infty]$. It is also the refinement of $\tau_{\leq}$ and $\tau_{\geq}$. It makes $\overline{\mathbb{R}}$ and $\overline{\mathbb{R}}^+$ compact effective topological spaces: their bases are the unions of the bases of $\tau_{\mathbb{R}}$, $\tau_{\leq}$ and $\tau_{\geq}$. A function from an effective topological space X to $\overline{\mathbb{R}}$ or $\overline{\mathbb{R}}^+$ is constructively continuous if and only if it is lower and upper semi-computable.

Actually, the spaces $\overline{\mathbb{R}}$, $\overline{\mathbb{R}}^+$ and $[0, 1]$ with the order topology are isomorphic effective topological spaces, the functions $e^x : \overline{\mathbb{R}} \to \overline{\mathbb{R}}^+$ and $-\ln(1 - x) : [0, 1] \to \overline{\mathbb{R}}^+$ being examples of isomorphisms. Remark that they are also isomorphisms of computable enumerative lattices.

1.6 Computable Metric Spaces

1.6.1 Basics

Computable metric spaces were studied in [Wei93], [BP03] using representation theory, in [Hem02] using oracle machines, in [EH98] using domain theory.

A metric on a set X is a way to transfer automatically the Euclidean topology on $\mathbb{R}$ to X. Generally, the advantages drawn from defining a metric exceed the fact that a topology is automatically defined, and the metric structure yields strong results which are not true of any topological space. When a metric space is separable (i.e. has a countable dense subset) the topology has a countable basis, which enables one to endow it with an effective topology. The choice of a particular countable dense subset induces particular notions of constructive points, functions, etc. To make the use of the metric interesting from a computability point of view, it shall be chosen in order for the distance to be computable, as a function from the effective topological space to $\mathbb{R}$. Precisely, it gives:

Definition 1.6.1.1. A ***computable metric space (CMS)*** is a triple $(X, d, \mathcal{S})$ where:

1. (X, d) is a separable complete metric space,

2. $\mathcal{S}$ is a countable dense subset of X, with a numbering such that

3. $d(s_i, s_j)$ is computable, uniformly in i, j.

$\mathcal{S}$ is called the set of ***ideal points***. It is a numbered set, whose numbering makes the mutual distances between ideal points uniformly computable. Let $\mathcal{B} = \{B(s,q) : s \in \mathcal{S}, q \in \mathbb{Q}, q > 0\}$ be the set of ***ideal balls***. It is a basis of the topology induced by the metric d. The numberings of $\mathcal{S}$ and of the set of positive rational numbers induce a numbering of the collection of ideal balls, which is then a numbered set. Precisely, $B_{\langle i,j\rangle} := B(s_i, q_j)$. The topology $(\tau, \subseteq, \mathcal{B})$ is an enumerative lattice, which is not computable in general. Nevertheless:

Proposition 1.6.1.1. *The topology of a computable metric space is a pseudo-computable enumerative lattice, with:*

$$\langle i_1, j_1\rangle \lhd \langle i_2, j_2\rangle \quad \stackrel{def.}{\Longleftrightarrow} \quad d(s_{i_1}, s_{i_2}) + q_{j_1} < q_{j_2}$$

As $\cap$ distributes over unions, $\cap : \tau \times \tau \to \tau$ is constructive.

Proof. As the distance between ideal points is computable, the relation $\lhd$ is r.e. Clearly, $n \lhd p$ implies $B_n \subseteq B_p$.

We finally have to show that $B(s_{i_1}, q_{j_1}) \cap B(s_{i_2}, q_{j_2}) = \bigcup\{B(s_i, q_j) : \langle i,j\rangle \lhd \langle i_1, j_1\rangle, \langle i_2, j_2\rangle\}$: if $x \in B(s_{i_1}, q_{j_1}) \cap B(s_{i_2}, q_{j_2})$, take a positive rational number $q_j < \frac{1}{2}(q_{j_1} - d(x, s_{i_1})), \frac{1}{2}(q_{j_2} - d(x, s_{i_2}))$. Then $s_i \in B(x, q_j)$: $x \in B(s_i, q_j)$ and $\langle i,j\rangle \lhd \langle i_1, j_1\rangle, \langle i_2, j_2\rangle$. $\square$

The relation $\lhd$ is related to the way-below relation on the domain of formal balls, as defined in [EH98].

As $\cap$ is constructive, $(X, \tau, \mathcal{B})$ is then an effective topological space (see definition 1.3.0.5).

Product of computable metric spaces

If $(X, d, \mathcal{S})$ and $(X', d', \mathcal{S}')$ are computable metric spaces, there are two ways to endow their product with an effective topology: (1) as X and X' are automatically effective topological spaces, so is their product, the countable basis being the product $\mathcal{B} \times \mathcal{B}'$, (2) $X \times X'$ can be endowed with the product metric $d_\infty((x, x'), (y, y')) = \max\{d(x, y), d'(x', y')\}$, with $\mathcal{S} \times \mathcal{S}'$ as ideal points: it is a computable metric space, and then an effective topological space. The induced topology is also the product topology, but the countable basis is a bit different: it is the set of ideal balls $\{B((s,s'),q) : (s,s') \in \mathcal{S} \times \mathcal{S}', q \in \mathbb{Q}\}$.

Actually, these two different effective topological spaces are isomorphic, so we may use one construction or the other according to circumstances.

The metric and the constructive points

The constructivity of a point can be characterized in an algorithmic way: $x \in X$ is constructive if and only if there is an algorithm which outputs a Cauchy sequence of ideal points converging exponentially fast to x. Precisely, x is constructive if and only if there is a total recursive function φ such that $d(x, s_{\varphi(n)}) < 2^{-n}$ for all n.

For this reason, the constructive points of computable metric spaces will be called ***computable points***: they can be computed by an algorithm, up to any precision. Constructive functions arriving in a computable metric space will be called ***computable functions***.

Proposition 1.6.1.2. *The function $d : X \times X \to \mathbb{R}$ is computable. For all $x \in X$, the following are equivalent:*

1. *x is a computable point,*
2. *the function $d_x : X \to \mathbb{R}$, $d_x(y) = d(x,y)$ is computable,*
3. *$d(x, s_i)$ is computable, uniformly in i,*
4. *$d(x, s_i)$ is upper semi-computable, uniformly in i.*

Proof. $d^{-1}(a,b) = \bigcup\{B(s,q) \times B(s',q') : a + q + q' < d(s,s') < b - q - q'\}$ is a constructive open set, uniformly in a, b. $[1 \Rightarrow 2]$ follows from the computability of d, $[2 \Rightarrow 3 \Rightarrow 4]$ is immediate, $[4 \Rightarrow 1]$: $\delta_x : \tau \to \mathbb{S}$ is constructive: $\delta_x(B(s_i, q_j)) = \top \iff d(x, s_i) < q_j$. $\square$

In particular, if r is a positive lower semi-computable real number and x a computable point of X, the ball $B(x,r)$ is a constructive open set: d_x is upper semi-computable and $B(x,r) = d_x^{-1}[0,r)$.

For $x \in X$ and $r \geq 0$, let $\overline{B}(x,r)$ be the closed ball $\{y : d(x,y) \leq r\}$. It contains the closure of the open ball $B(x,r)$ but is not equal when there are isolated points are at distance r from x. $\overline{B}_n$ denotes $\overline{B}(s_i, q_j)$ where $n = \langle i, j \rangle$. The complement of $\overline{B}_n$ is a constructive open set, uniformly in n. Remark that $n \lhd p$ implies $\overline{B}_n \subseteq B_p$.

Computable metric subspace

As every computable metric space is also an effective topological space, there is a notion of effective topological subspace: given any subset D of X, the topology on X induces a topology on D, which is an effective topological subspace of X. D is also a metric subspace, with the induced metric, but D is not in general a computable metric space: it should at least be closed in order to be a complete metric space.

Definition 1.6.1.2. Let $(X, d, \mathcal{S})$ be a computable metric space. A ***computable metric subspace*** of X is a computable metric space $(D, d, \mathcal{S}')$ where D is a subset of X, d is the induced metric and such that $\mathrm{id} : D \to X$ is computable.

Theorem 1.6.1.1. *A subset D of X can be made a computable metric subspace of X if and only if D is a constructive closed set.*

Before proving it we state another theorem which will be used later and from which theorem 1.6.1.1 directly follows.

Theorem 1.6.1.2. *Let $(X, d, \mathcal{S})$ be a computable metric space. A closed subset A is constructive if and only if it contains a dense sequence of uniformly computable points.*

Proof. The "if" part is direct: if A contains such a sequence $(x_k)_k$, then $A \cap U \neq \emptyset \iff \exists k, x_k \in U$.

The "only if" part requires more attention. Let $B = B(s, r)$ be an ideal ball intersecting A: we construct a fast Cauchy sequence of ideal points $s(i)$ whose limit is in $A \cap B$. Put $s(0) = s$ and $r(0) = r$. If $s(i), r(i)$ have been constructed and satisfy $B(i) = B(s(i), r(i)) \cap A \neq \emptyset$, put $r(i+1) = r(i)/2$: as $B(i) \subseteq \cup_{s' \in B(i)} B(s', r(i)/2)$ there is $s(i+1) \in B(i)$ such that $B(s(i+1), r(i+1))$ intersects A. $s(i+1)$ can be effectively found. The sequence $s(i)$ is a Cauchy sequence, so it converges, and its limit is in A, which is a closed set. As everything is uniform in the number of the ideal ball B, any numbering $(B_k)_k$ of the ideal balls intersecting A gives a constructive sequence $(x_k)_k$ of uniformly computable points with $x_k \in B_k \cap A$. □

Remark that the closure of any constructive open set is then a constructive closed set. Indeed, the ideal points of U can be enumerated in a uniform way, and they are dense in $\overline{U}$.

Proof. (of theorem 1.6.1.1) The proof of the theorem is then a consequence of this: any dense sequence of uniformly computable points contained in F can be used as set of ideal points of the subspace F. Conversely, if $(F, d, \mathcal{S}^F)$ is a computable metric subspace, then s_i^F is a computable point of F, uniformly in i, so $s_i^F = \mathrm{id}(s_i^F)$ is also a computable point of X, uniformly in i. □

Computable Baire theorem

The technique used in the proof of theorem 1.6.1.2 can be adapted to get a computable version of Baire's theorem.

Definition 1.6.1.3. In an effective topological space $(X, \tau, \mathcal{B})$, a constructive G_δ, or Π_2^0 is an intersection of uniformly constructive open sets.

One of the forms of the classical Baire category theorem states that every non-empty complete metric space is a Baire space, i.e. every countable intersection of dense open sets is dense. Its proof is actually constructive, and a computable version has been proved in [YMT99], [Bra01]. We recall the proof, which uses the following lemma:

Lemma 1.6.1.1. *Let X be a computable metric space. Let V_i be a sequence of non-empty uniformly constructive open sets such that $\overline{V}_{i+1} \subseteq V_i$ and $\mathrm{diam}(V_i)$ effectively tends 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 $\mathrm{diam}(V_i)$ tends 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 $x \in \bigcap_i \overline{V}_i = \bigcap_i V_i$. □

Theorem 1.6.1.3 (Computable Baire theorem)**.** *Every dense constructive G_δ contains a dense sequence of uniformly computable points.*

Proof. $A = \bigcap_i U_i$ where U_i is constructive uniformly in i. Let B be an ideal ball: we construct a shrinking sequence of ideal balls $(B(i))_i$ such that $B(i+1) \subseteq U_i$. 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. It follows that $\bigcap_i B(i)$ is a singleton $\{x\}$ consisting of a computable point. As everything is uniform in the ideal ball B, the numbering $(B_k)_k$ of $\mathcal{B}$ gives a constructive sequence $(x_k)_k$ of uniformly computable points with $x_k \in B_k$. □

The technique used in the proof of Baire's theorem is a generalization of the diagonalization technique used in Cantor's argument to prove that the set of real numbers is not countable. Actually, Baire's theorem implies that $\mathbb{R}$ is non-countable: given a sequence $(x_n)_n$ of real numbers, the open sets $U_n = \mathbb{R} \setminus \{x_n\}$ are dense, so their intersection is dense by Baire's theorem and then non-empty. In other words, from any sequence $(x_n)_n$ of real numbers, one can construct a number x which does not belong to the sequence. This construction is effective, as illustrated by the computable Baire's theorem. It implies that in a computable metric space without isolated point, there is no constructive enumeration of all its computable points: from every constructive sequence can be computed a point which does not appear in the sequence.

Corollary 1.6.1.1. *There is a sequence $(r_n)_n$ of uniformly computable positive real numbers which is dense in $[0, +\infty)$, such that $d(s_i, s_j) \neq r_n$ for all i, j, n. It makes the relation $s_i \in B(s_j, r_n)$ decidable.*

Proof. $[0, +\infty)$ is obviously a computable metric space. Define the uniformly constructive open subsets of $[0, +\infty)$: $U_{i,j} = (0, +\infty) \setminus \{d(s_i, s_j)\}$. Then $R = \bigcap_{i,j} U_{i,j}$ is a constructive dense G_δ, so the preceding theorem allows to conclude. □

Computable dense orbits Let us briefly present a direct consequence of this theorem for topological dynamical systems. 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.

Definition 1.6.1.4. Let (X, τ) be a topological space and $T : X \to X$ a continuous map. T is ***topologically transitive*** if for all open sets U, V, there is n such that $U \cap f^{-n}V \neq \emptyset$.

A sufficient condition is the existence of a dense trajectory. In complete separable metric spaces, it is also a necessary condition:

Proposition 1.6.1.3. *Let X be a complete separable metric space and $T : X \to X$ a continuous map. T is topologically transitive if and only if it has a dense trajectory.*

The proof relies on the Baire category theorem. Its computable version gives:

Theorem 1.6.1.4 (Computable dense orbits)**.** *Let X be a computable metric space and $T : X \to X$ a transformation which is computable on a constructive dense G_δ. If T has a dense orbit, then it has a* computable *dense one.*

Proof. This is a direct consequence of the computable Baire theorem (theorem 1.6.1.3). Let D be the domain of computability of T: then $R = D \cap \bigcap_i \bigcup_n T^{-n} B_i$ is a constructive dense G_δ. Indeed, as T is computable on D, $T^{-n} B_i \cap D = U_{n,i} \cap D$ where $U_{n,i}$ is a constructive open set, uniformly in n, i. Hence, $R = D \cap \bigcap_i \bigcup_n U_{n,i}$. By computable Baire's theorem R contains computable points, whose orbits are dense by definition of R. □

1.6.2 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.

In [Hem02] it is proved that between computable metric spaces, the domain of functions which are computable in a stronger sense is a constructive G_δ, 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 1.6.2.1. *Let X be an effective topological space and Y a computable metric space. 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.*

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 Π^0_2-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. 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. 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 $d(x', x) + r' < r$. If $(x', r') < (x, r)$ then $\overline{B}(x', r') \subseteq B(x, r)$ (the converse does not hold in general, but for connected 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 recursively 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, $x \in \psi(B(s,q))$. □

1.7 Representation theory

In representation theory, the Cantor space $\{0,1\}^{\mathbb{N}}$ is chosen as a primitive space: a notion of computable function from $\{0,1\}^{\mathbb{N}}$ to $\{0,1\}^{\mathbb{N}}$ is defined using a kind of Turing machines (called type-two machines), and is used to define computability notions on general spaces through *representations*. A representation on a set X is a partial surjective function $\rho : \{0,1\}^{\mathbb{N}} \to X$. If (X, ρ) and (X', ρ') are represented spaces, an element $x \in X$ is ρ-computable if it is the image by ρ of a computable sequence, a function $f : X \to X'$ is (ρ, ρ')-computable if there is a computable function $F : \mathrm{dom}(\rho) \to \{0,1\}^{\mathbb{N}}$ such that $f \circ \rho = \rho' \circ F$ on $\mathrm{dom}(\rho)$.

$\{0,1\}^{\mathbb{N}}$ is an effective topological space, which the topology generated by the cylinders, which form a countable basis $\mathcal{B}$. It is an easy fact that a function $F : D \subseteq \{0,1\}^{\mathbb{N}} \to \{0,1\}^{\mathbb{N}}$ is computable by a type-two machine if and only if it is constructively continuous on D.

The set $P(\mathbb{N})$ is represented this way: if $\omega \in \{0,1\}^{\mathbb{N}}$,

$$\mathrm{En}(\omega) = \{n \in \mathbb{N} : \mathtt{110}^{n+1}\mathtt{11} \text{ is a sub-word of } \omega\}.$$

It induces a canonical representation $\rho_L = \sup_{\mathcal{P}} \circ \mathrm{En}$ for any enumerative lattice $(L, \leq, \mathcal{P})$, which is a constructive element of $\mathcal{C}(\{0,1\}^{\mathbb{N}}, L)$.

When $(X, \tau, \mathcal{B})$ is an effective topological space, the standard representation is defined by $\rho_X(\omega) = x$ if $\mathrm{En}(\omega) = \{i : x \in B_i\}$: it is a constructively continuous function from $\{0,1\}^{\mathbb{N}}$ to X.

It can be shown that:

1. Constructive functions from $P(\mathbb{N})$ to $P(\mathbb{N})$ as defined here are exactly the functions which are (En,En)-computable (and this extends to functions between enumerative lattices).

2. Between effective topological spaces X and Y, it is well-known that constructively continuous functions are exactly the (ρ_X, ρ_Y)-computable functions.

3. Constructive elements of $\mathcal{C}(X, L)$ are exactly the (ρ_X, ρ_L)-computable functions.

See [Wei00] for details.

1.8 Kolmogorov complexity

We briefly recall the notion of Kolmogorov complexity and some useful properties. For complete introductions to the subject, we refer to [LV93], [Cal94], [Gác].

In the context of information theory, Kolmogorov defined in [Kol65] a notion of *algorithmic information content* of discrete objects. Information theory is about transmission of discrete data, and particularly, their encoding into binary sequences. A central question is to find coding systems which minimize the length of the transmitted message. Until Kolmogorov, the *effective computability* of the coding systems studied (Shannon-Fano coding, Huffman coding) was always implicit, attention being even focused on their practical implementation. Kolmogorov took advantage of computability theory, which grasps what it means for a procedure to be effectively computable, defining the algorithmic information content of discrete objects as the minimal codeword length by computable codings (once the objects have been identified with integers, or finite words).

The so-called *Kolmogorov complexity* is universal in the sense that it does not depend on structures underlying the objects (for instance, Huffman coding depends on the probabilities that are put on the objects). From this universality Kolmogorov complexity draws a very general statute and intimate relations with many mathematical concepts (as probabilities, dimension). As a drawback, Kolmogorov complexity is not computable, and makes sense only up to additive constants (which may be as large as possible), so its interesting features appear at the asymptotic limit.

We recall the variant of Kolmogorov complexity, defined independently by Chaitin and Levin, which is closer to classical information theory, as it is concerned with *prefix codes*. For a complete introduction to Kolmogorov complexity we refer to standard texts [LV93], [Gác].

1.8.1 Definitions

Given a discrete data set, there are many ways to encode its objects into binary strings. We require the code to be *prefix*: no code is prefix of another code, which enables one to decode a concatenation of codes into a sequence of data. Let us make it precise.

Let $\{0,1\}^{\mathbb{N}}$ be the Cantor space of infinite binary sequences, and $\{0,1\}^*$ be the set of finite binary words. A word $w \in \{0,1\}^*$ defines the ***cylinder*** $[w] \subset \{0,1\}^{\mathbb{N}}$ of all possible continuations of w. A set $D = \{w_1, w_2, ...\} \subset \{0,1\}^*$ defines an open set $[D] = \cup_i [w_i] \subset \{0,1\}^{\mathbb{N}}$. D is called ***prefix-free*** if no word of D is prefix of another one, that is if the cylinders $[w_i]$ are pairwise disjoint.

We define the prefix Kolmogorov complexity of objects of a numbered set whose numbering is bijective (typically, $\mathbb{N}$ or Σ^* where Σ is a finite alphabet).

Definition 1.8.1.1. Let S be a numbered set. An ***interpreter*** is a partial recursive function $I : \{0,1\}^* \to S$ which has a prefix-free domain.

The prefix Kolmogorov complexity (or algorithmic information content) of $s \in S$ relative to an interpreter I is

$$K_I(s) := \begin{cases} |p| & \text{if } p \text{ is a shortest input such that } I(p) = s \\ \infty & \text{if there is no } p \text{ such that } I(p) = s \end{cases}$$

As for recursive functions, there exists an effective enumeration of all interpreters, which entails the existence of a universal interpreter U which is asymptotically optimal in the sense that the *invariance theorem* holds:

Theorem 1.8.1.1 (Invariance theorem)**.** *For every interpreter I there exists $c_I \in \mathbb{N}$ such that for all $s \in S$ we have $K_U(s) < K_I(s) + c_I$.*

All universal interpreters then give the same complexity to objects of S, up to additive constants. We fix a universal interpreter U and we let $K(w) = K_U(w)$ be the ***prefix Kolmogorov complexity*** of s. In this thesis, we never use the original definition by Kolmogorov, sometimes called *plain* complexity, so we will often omit the adjective *prefix*. As the set of words p satisfying $U(p) = s$ is r.e. uniformly in s (indeed, we suppose the numbering to be bijective), the function $K : S \to \mathbb{N}$ is upper semi-computable.

1.8.2 Simple estimates

Let f, g be real-valued functions. We say that g ***additively dominates*** f and write $f \overset{+}{<} g$ if there is a constant c such that $f \leq g + c$. As codes are always *binary* words, we use base-2 logarithms, which we denote by $\log$.

Binary words. Let $S = \{0,1\}^*$ be the numbered set of finite binary strings. We define an interpreter I by $I(a_1 0 a_2 \dots 0 a_k 1 w) = w$ if $a_1 a_2 \dots a_k$ is the binary expansion of $|w|$. The domain where I is defined is prefix-free, and $K_I(w) = |w| + 2\lfloor \log(|w| + 2) \rfloor$. Hence,

$$K(w) \overset{+}{<} |w| + 2\log|w| \quad \text{for } w \in \{0,1\}^* \tag{1.1}$$

Natural numbers. Let $S = \mathbb{N}$: from (1.1), we derive

$$K(n) \overset{+}{<} \log n + 2\log(\log n) \quad \text{for } n \in \mathbb{N} \tag{1.2}$$

as n can be identified with a binary word of length $\lfloor \log(n+1) \rfloor$.

Cartesian product. If S, S' are numbered sets, $S \times S'$ has a canonical numbering. If I, I' are interpreters from $\{0,1\}^*$ to S, S' respectively, we define the function $I'' : \{0,1\}^* \to S \times S'$ by $I''(pq) = (I(p), I(q))$ (where pq is the concatenation of p and q), which makes sense as the domains of I, I' are prefix-free. I'' is computable and has prefix-free domain, so it is an interpreter. From this, we derive:

$$K(s, s') \overset{+}{<} K(s) + K(s') \quad \text{for } (s, s') \in S \times S' \tag{1.3}$$

Finite sequences. If S is a numbered set then the set S^* of finite sequences of elements of S is also a numbered set. Using the same argument,

$$K(s_1,\ldots,s_n) \overset{+}{<} K(s_1)+\ldots+K(s_n) \quad \text{for } (s_1,\ldots,s_n)\in S^* \tag{1.4}$$

1.8.3 Shannon information content

When a finite set S is endowed with a probability measure $P=(p_s)_{s\in S}$, that is $p_s \in [0,1]$ and $\sum_s p_s = 1$, Shannon proved that the mean codeword length of a prefix code is bounded from below by the *entropy* of the distribution $H(P) = -\sum_s p_s \log p_s$, the quantity $-\log p_s$ being called the *information content* of s. Moreover, there is an optimal prefix code (Huffman coding) for which the codeword length of s is $\lceil -\log p_s \rceil$, so the mean codeword length is between $H(P)$ and $H(P)+1$.

This can be extended to countable sets. If S is a numbered set, and P is computable (p_s is computable uniformly in s), then the associated optimal prefix code is also computable, i.e. it can be decoded by an interpreter. It implies that $K(s) \overset{+}{<} -\log p_s$. This can be improved by the so-called *coding theorem*.

Theorem 1.8.3.1 (Coding theorem)**.** *Let $P : S \to \overline{\mathbb{R}}^+$ be a lower semi-computable function such that $\sum_s P(s) \leq 1$. Then $K(s) \overset{+}{<} -\log P(s)$, i.e. there is a constant c such that $K(s) \leq -\log P(s) + c$ for all $s \in S$.*

Such a function P is often called a *semi-measure* (it is nearly a probability measure). As the domain of the universal interpreter U is prefix-free, $\sum_i 2^{-K(i)}$ is the (Lebesgue) measure of its domain, so is less than one. Hence, the function m: $\mathbb{N} \to [0,1]$ defined by $\mathrm{m}(i) = 2^{-K(i)}$ is itself a semi-measure, which is *universal*, in the sense that it multiplicatively dominates all semi-measures: for all P, there is a constant $c'(=2^{-c})$ such that m$\geq c'P$.

Let us consider a simple application: the sequence $\frac{1}{n(\log(n))^2}$ is summable, which can be proved using that it is the derivative of $\frac{-\ln(2)}{\log(x)}$, which is integrable on $[2,+\infty)$. From the coding theorem, one derives $K(n) \overset{+}{<} \log n + 2\log(\log n)$ (inequality 1.2).

Define $J(x) = x+1+2\log(x+1)$ for real $x \geq 0$: $\sum_n 2^{-J(\log n)} < \infty$ and $K(n) \overset{+}{<} J(\log n)$.

The following property is a version of a result attributed to Kolmogorov, stated in terms of prefix complexity instead of plain complexity.

Proposition 1.8.3.1. *Let $E \subseteq \mathbb{N} \times S$ be a r.e. set such that $E_n = \{s : (n, s) \in E\}$ is finite for all n. Then for (s, n) with $s \in E_n$,*

$$K(s) \overset{+}{<} J(\log |E_n|) + K(n)$$

Proof. Let $\varphi : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ be a total injective recursive function enumerating E. Define $P(n, s_{\varphi(n,i)}) = 2^{-K(n)-J(\log(i))}$ and $P(n, s) = 0$ if $s \notin E_n$. P is lower semi-computable and $\sum_{(n,s)} P(n, s) \leq \sum_{(n,i)} 2^{-K(n)-J(\log(i))} \leq 1$, so applying the coding theorem, one has $K(n, s_{\varphi(n,i)}) \overset{+}{<} K(n) + J(\log(i))$. As $i \leq |E_n|$ and J is non-decreasing, $K(n, s) \overset{+}{<} K(n) + J(\log |E_n|)$ for $s \in E_n$. $\square$

Chapter 2

Probability measures and computability

The Cantor space, or space of infinite binary sequences, is a friendly place for computability. Its total disconnection has numerous consequences: cylinders are decidable sets, their measure is computable, the space has open covers which are also partitions, etc. General metric spaces do not share these features with the Cantor space, which raises important problems when dealing with measures, or symbolic models of dynamical systems.

Computability of probability measures on general spaces was already studied, identifying measures with valuations, in [Eda96] using domain theory and in [Sch07] using refined representation theory. The problem was studied in [Wei99] for the unit real interval, from several points of view. In [Gác05] probability measure are seen as points of a metric space, on which computability notions are well developed.

We study the computability of probability measures on a computable metric space, seeing measures as points of a metric space, as valuations on open sets, as integration operators. We show that these approaches are equivalent, which relates the works mentioned above. We then introduce the computable version of probability spaces, and show:

Theorem. *Every computable probability space is isomorphic to the Cantor space endowed with the uniform measure.*

This result allows one to transfer algorithmic probability concepts (as algorithmic randomness) from the Cantor space to any computable probability space. The computability assumption on the measure is fundamental, as there are non-computable probability measures for which the theorem does not hold.

Most of this work together with a part of section 3 on algorithmic randomness are gathered in an article [HR07] which is following the submission process at the time this thesis is written.

2.1 The space $\mathcal{M}(X)$ of probability measures

Following [Gác05] we endow the space $\mathcal{M}(X)$ with a computable metric space structure compatible with the weak topology.

2.1.1 Background

Let us recall bases of measure theory for probability measures, partially taken from [Bil68].

Let (X, d) be a metric space. A σ-field on X is a class of subsets of X containing X, which is closed under complement and countable unions. The Borel σ-field is the σ-field generated by the topology, i.e. the smallest σ-field containing the open sets. A Borel probability measure μ on X is a set function from the Borel sets to $[0, 1]$ which is (i) countably additive set ($\mu(\cup_{k=1}^{\infty} A_k) = \sum_k \mu(A_k)$ for disjoint Borel sets A_k), and satisfies (ii) $\mu(X) = 1$. Let μ_n, μ be Borel probability measures on X: we say that μ_n ***converges weakly*** to μ if $\int f d\mu_n \to \int f d\mu$ for every bounded, continuous real function f on X.

Let us recall the Portmanteau theorem. We say that a Borel set A is ***μ-continuous*** if $\mu(\partial A) = 0$, where $\partial A = \overline{A} \cap \overline{X \setminus A}$ is the boundary of A.

Theorem 2.1.1.1 (Portmanteau theorem)**.** *Let μ_n, μ be Borel probability measures on a separable metric space (X, d). The following are equivalent:*

1. *μ_n converges weakly to μ,*

2. $\limsup_n \mu_n(F) \leq \mu(F)$ *for all closed sets F,*

3. $\liminf_n \mu_n(G) \geq \mu(G)$ *for all open sets G,*

4. $\lim_n \mu_n(A) = \mu(A)$ *for all μ-continuous sets A.*

When (X, d) is a separable metric space, weak convergence can be proved using the following criterion:

Proposition 2.1.1.1. *Let $\mathcal{A}$ be a countable basis of the topology which is closed under the formation of finite unions. If $\mu_n(A) \to \mu(A)$ for every $A \in \mathcal{A}$, then μ_n converges weakly to μ.*

Proof. Let G be an open set: it can be expressed as a countable union of elements of $\mathcal{A}$: $G = \bigcup_i A_i$. Let $G_i = A_0 \cup \ldots \cup A_i \in \mathcal{A}$: as $G_i \subseteq G$, $\mu_n(G_i) \leq \mu_n(G)$ so $\mu(G_i) = \lim_n \mu_n(G_i) \leq \liminf_n \mu_n(G)$. It follows that $\mu(G) = \sup_i \mu(G_i) \leq \liminf_n \mu_n(G)$, so condition (iii) of the preceding theorem holds. □

We then endow the set $\mathcal{M}(X)$ of Borel probability measures over X with the *weak topology*, which is the topology of weak convergence (i.e. the finest topology for which all sequences μ_n converging weakly to μ converge to μ for the topology, see appendix A.1.1). The implication $1 \Rightarrow 3$ in the portmanteau theorem can then be read as the lower semi-continuity of the function ($\mathcal{M}(X)$ is a sequential space by definition):

$$\begin{array}{rccc} v(U): & \mathcal{M}(X) & \to & \overline{\mathbb{R}}^+ \\ & \mu & \mapsto & \mu(U) \end{array}$$

When (X, d) is a metric space, the weak topology on $\mathcal{M}(X)$ is metrizable:

Definition 2.1.1.1. The ***Prokhorov metric*** ρ on $\mathcal{M}(X)$ is defined by:

$$\rho(\mu, \nu) := \inf\{\epsilon \in \mathbb{R}^+ : \mu(A) \leq \nu(A^\epsilon) + \epsilon \text{ for every Borel set } A\}. \tag{2.1}$$

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

It is known that it is indeed a metric, which induces the weak topology on $\mathcal{M}(X)$. When X is separable, $\mathcal{M}(X)$ is also separable: fixing a countable dense set $\mathcal{S} \subseteq X$, we define the set $\mathcal{N} \subset \mathcal{M}(X)$ of finite linear combinations of Dirac measures (measures concentrated in one point) concentrated on points of $\mathcal{S}$, with rational coefficients. It can be shown that this is a dense subset.

Moreover, when (X, d) is complete, $(\mathcal{M}(X), \rho)$ is also complete, see [Bil68].

2.1.2 The computable metric space $\mathcal{M}(X)$

Let $(X, d, \mathcal{S})$ be a computable metric space. From what precedes, we know that $(\mathcal{M}(X), \rho, \mathcal{N})$ is a separable complete metric space. Following [Gác05], we show that it is even a *computable* metric space.

We call $\mathcal{N}$ the set of ***ideal measures***. As every ideal measure can be described by a finite subset of $\mathcal{S} \times \mathbb{Q}_{>0}$, the numberings of $\mathcal{S}$ and $\mathbb{Q}_{>0}$ induce a canonical numbering $\{\nu_i : i \in \mathbb{N}\}$ of $\mathcal{N}$ (which can be taken injective). We start with the following lemma:

Lemma 2.1.2.1. *The valuation $v_{\nu_i} : \tau \to [0, 1]$ mapping U to $\nu_i(U)$ is lower semi-computable, uniformly in i.*

Proof. For a Dirac measure d_s concentrated on an ideal point s, $v_{d_s} : \tau \to [0, 1]$ is lower-semi-continuous, as s is constructive (v_{d_s} is actually $\delta_s : \tau \to \mathbb{S}$, with 0 and 1 in place of $\perp$ and $\top$ respectively). Now, if ν is a finite linear combination $\sum q d_s$ of Dirac measures, v_ν is $\sum q v_{d_s}$, which is lower semi-computable, uniformly in the number of ν.

□

Proposition 2.1.2.1. $(\mathcal{M}(X), \rho, \mathcal{N})$ *is a computable metric space.*

Proof. We have to show that the real numbers $\rho(\nu_i, \nu_j)$ are all computable, uniformly in $\langle i, j\rangle$.

Observe that if ν_i is an ideal measure concentrated over a finite set $S \subseteq \mathcal{S}$, then (2.1) becomes $\rho(\nu_i, \nu_j) = \inf\{\epsilon \in \mathbb{Q} : \forall A \subset S, \nu_i(A) < \nu_j(A^\epsilon) + \epsilon\}$. First, $\nu_i(A)$ is computable. Since A^ϵ is a finite union of ideal open balls, the number $\nu_j(A^\epsilon)$ is lower semi-computable. As everything is uniform, $\rho(\nu_i, \nu_j)$ is upper semi-computable. To see that $\rho(\nu_i, \nu_j)$ is lower-semi-computable, observe that $\rho(\nu_i, \nu_j) = \sup\{\epsilon \in \mathbb{Q} : \exists A \subset S, \nu_i(A) > \nu_j(A^{\bar{\epsilon}}) + \epsilon\}$, where $A^{\bar{\epsilon}} = \{x : d(x, A) \leq \epsilon\}$ is a finite union of ideal closed balls when $A \subset S$, and then is the complement of a constructive open set. $\nu_j(A^{\bar{\epsilon}})$ is then upper semi-computable, which allows to conclude. Note that everything is uniform. □

Definition 2.1.2.1. A Borel probability measure μ is ***computable*** if it is a computable point of the computable metric space $(\mathcal{M}(X), \rho, \mathcal{N})$.

2.1.3 The Wasserstein metric

In the particular case when the metric space X is bounded, an alternative metric due to Wasserstein in [Was69] can be defined on $\mathcal{M}(X)$. When f is a real-valued function, μf denotes $\int f d\mu$.

Definition 2.1.3.1. The *Wasserstein metric* on $\mathcal{M}(X)$ is defined by:

$$W(\mu, \nu) = \sup_{f \in \text{1-Lip}(X)} (|\mu f - \nu f|) \tag{2.2}$$

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

As with the Prokhorov metric, the topology induced by W on $\mathcal{M}(X)$ is the weak topology, and $(\mathcal{M}(X), W)$ is separable and complete as soon as X is separable and complete.

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

Proposition 2.1.3.1. $(\mathcal{M}(X), W, \mathcal{N})$ *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 (2.2) over 1-Lip$^*(X) := \{f \in$ 1-Lip$(X) : f(s^*) = 0\}$. Given some precision ϵ we construct an ϵ-net of 1-Lip$^*(X)$, that is a finite set $\mathcal{G}_\epsilon \subseteq$ 1-Lip$^*(X)$ made of uniformly computable functions such that for each $f \in$ 1-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-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 $\phi^+_{s,k}(x) := a + d(s,x)$ and $\phi^-_{s,k}(x) := a - d(s,x)$. Then it is not difficult to see that $\mathcal{G}_\epsilon$ defined as the set of all possible combinations of $\max$ and $\min$ made with the $\phi^\pm_{s,k}(x)$ satisfy 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 effectivisation using the Prokhorov or the Wasserstein metrics turn out to be equivalent.

Theorem 2.1.3.1. *The Prokhorov and the Wasserstein metrics are effectively equivalent. That is, the identity function* $id : (\mathcal{M}(X), \rho, \mathcal{N}) \to (\mathcal{M}(X), W, \mathcal{N})$ *is an isomorphism of effective topological spaces.*

Proof. Let M be an integer bound on the diameter of X. We show that $\rho(\mu,\nu)^2 \leq W(\mu,\nu) \leq (M+1)\rho(\mu,\nu)$.

For the second inequality, suppose $\rho(\mu,\nu) < \epsilon/(M+1)$. By the coupling theorem [Bil68], for every $f \in$ 1-Lip(X) it holds $|\mu f - \nu f| \leq \epsilon$, so $W(\mu,\nu) < \epsilon$. For the first inequality, suppose $W(\mu, \nu) < \epsilon^2$. Let A be a Borel set: we define $g(x) := [1 - d(x, A)/\epsilon]^+$ where $[r]^+ = \max(r, 0)$: g equals 1 on A, 0 outside A^ϵ, so $\mu(A) \leq \mu g \leq \mu(A^\epsilon)$. As $\epsilon g \in$ 1-Lip(X), $\epsilon \mu g < \epsilon \nu g + \epsilon^2$, which, simplifying by ϵ, gives $\mu(A) \leq \nu(A^\epsilon) + \epsilon$. As this is true for all Borel sets A, it follows that $\rho(\mu, \nu) < \epsilon$.

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.

□

The effectivisation 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 ?

2.1.4 Measures as valuations

We know from the portmanteau theorem (theorem 2.1.1.1) that for each open set U, the function:

$$\begin{array}{rccc} v(U): & \mathcal{M}(X) & \rightarrow & \overline{\mathbb{R}}^+ \\ & \mu & \mapsto & \mu(U) \end{array}$$

is lower semi-continuous. As $\overline{\mathbb{R}}^+$ is a computable enumerative lattice, $v(U)$ is an element of $\mathcal{C}(\mathcal{M}(X), \overline{\mathbb{R}}^+)$. Moreover, it is a basic property of measures that $\sup_n \mu(U_n) = \mu(\bigcup_n U_n)$ when $U_n \subseteq U_{n+1}$. This implies the Scott-continuity of the function

$$\begin{array}{rccc} v: & \tau & \rightarrow & \mathcal{C}(\mathcal{M}(X), \overline{\mathbb{R}}^+) \\ & U & \mapsto & v(U) \end{array} \tag{2.3}$$

Indeed, if $U_n \subseteq U_{n+1}$, $v(\bigcup_n U_n)$ is the function which maps μ to $\mu(\bigcup_n U_n) = \sup_n \mu(U_n) = \sup_n(v(U_n)(\mu))$ so it is the point-wise supremum of the functions $v(U_n)$ which is exactly $\sup_n v(U_n)$. Proposition 1.2.0.2 then enables to conclude.

Proposition 2.1.4.1. *The valuation operator $v : \tau \rightarrow \mathcal{C}(\mathcal{M}(X), \overline{\mathbb{R}}^+)$ defined in (2.3) is constructive.*

Proof. We have to show that $v(B_{n_1} \cup \ldots \cup B_{n_k})$ is constructive, uniformly in $\langle n_1, \ldots, n_k \rangle$.

We define the ϵ-interior of U: $U(\epsilon) = B(s_{i_1}, q_{j_1} - \epsilon) \cup \ldots \cup B(s_{i_k}, q_{j_k} - \epsilon)$: we will use $U(2\epsilon)^\epsilon \subseteq U(\epsilon)$ and $U(\epsilon)^\epsilon \subseteq U$. Let $B_n = B^{\mathcal{M}}(\mu_i, q_j)$ be an ideal ball of $\mathcal{M}(X)$. Define $y_n = \mu_i(U(q_j)) - q_j$. We claim that:

$$v(U) = \sup_n \mathrm{St}_{B_n}^{y_n}$$

Indeed, for every measure $\mu \in B_n = B^{\mathcal{M}}(\mu_i, q_j)$, $\mu_i(U(q_j)) \leq \mu(U) + q_j$ by definition of the Prokhorov distance, so $\mathrm{St}_{B_n}^{y_n}(\mu) \leq v(U)(\mu)$.

Let $\mu \in \mathcal{M}(X)$ and $q < \mu(U)$: as $\mu(U) = \sup_j\{\mu(U(q_j)) - 2q_j\}$, there is $q_j > 0$ such that $\mu(U(q_j)) - 2q_j > q$. As v_U is continuous, $v_U^{-1}(q, 1]$ is open, so there is an ideal measure $\mu_i \in v_U^{-1}(q, 1] \cap B(\mu, q_j)$. Then, $q < \mu(U(2q_j)) - 2q_j \leq \mu_i(U(q_j)) - q_j$, so $q < \mathrm{St}_{B_n}^{y_n}(\mu)$.

Finally, as $U(q_j)$ is recursively open, uniformly in j, y_n is lower semi-computable uniformly in n, so $v(U)$ is constructive. And everything is uniform in $\langle n_1, \ldots, n_k \rangle$. □

Here is a simple consequence: if $B_i = B(s, r)$ is an ideal ball, denoting by $\overline{B}_i$ the closed ball $\overline{B}(s, r) = \{x : d(x, s) \leq r\}$, its complement is a constructive open set, uniformly in i. Then the function $\mu \mapsto \mu(\overline{B}_{i_1} \cup \ldots \cup \overline{B}_{i_k})$ is upper semi-computable, uniformly in $\langle i_1, \ldots, i_k \rangle$. In particular, if the measure of the boundary of any ideal ball is null, the quantities $\mu(B_{i_1} \cup \ldots \cup B_{i_k})$ are uniformly computable.

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

Theorem 2.1.4.1. *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 2.1.4.1. $[2 \Rightarrow 3]$ Trivial. $[3 \Rightarrow 1]$ We show that $\rho(\mu_n, \mu)$ is upper semi-computable uniformly in n, and then use proposition 1.6.1.2. Since $\rho(\mu_n, \mu) < \epsilon$ 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) $\rho(\mu_n, \mu) < \epsilon$ is semi-decidable, uniformly in n and ϵ.

□

It could be formulated in terms of representations: representing a measure 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 lead to the same constructivity notions. This is the approach taken in [Wei99] for the special case $X = [0,1]$ and in [Sch07] on arbitrary sequential spaces. 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 [Eda96], the Scott topology being proved to induce the weak topology.

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 have:

Corollary 2.1.4.1. *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 2.1.4.2. *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*.

2.1.5 Measures as integrals

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

The effective topology on X and the enumerative lattice structure of $\overline{\mathbb{R}}^+$ induce in a canonical way the enumerative space $\mathcal{C}(X, \overline{\mathbb{R}}^+)$ (see section 1.3.2). As $\overline{\mathbb{R}}^+$ is a computable enumerative lattice, $\mathcal{C}(X, \overline{\mathbb{R}}^+)$ is exactly the set of lower semi-continuous functions from X

to $\overline{\mathbb{R}}^+$, and its constructive elements are the constructively continuous functions from X to $\overline{\mathbb{R}}^+$ (proposition 1.4.1.5).

The Portmanteau theorem (theorem 2.1.1.1) can be easily extended: μ_n converges weakly to μ if and only if for all $f \in \mathcal{C}(X, \overline{\mathbb{R}}^+)$, $\liminf_n \int f d\mu_n \geq \int f d\mu$ (lower semi-continuous functions behave as open sets). In other words, the function:

$$\begin{array}{rccc} I(f): & \mathcal{M}(X) & \to & \overline{\mathbb{R}}^+ \\ & \mu & \mapsto & \int f d\mu \end{array}$$

is lower semi-continuous (as $\mathcal{M}(X)$ is a sequential space), i.e. belongs to $\mathcal{C}(\mathcal{M}(X), \overline{\mathbb{R}}^+)$.

The monotone convergence theorem states that $\int (\sup_n f_n) d\mu = \sup_n \int f_n d\mu$ when f_n is an increasing sequence of non-negative measurable functions (see [Bil79]). As the enumerative lattice $\mathcal{C}(X, \overline{\mathbb{R}}^+)$ is a sequential space, it implies by proposition 1.2.0.2 that the function:

$$\begin{array}{rccc} I_\mu: & \mathcal{C}(X, \overline{\mathbb{R}}^+) & \to & \overline{\mathbb{R}}^+ \\ & f & \mapsto & \int f d\mu \end{array}$$

is Scott-continuous. Actually, this can be strengthen. The function:

$$\begin{array}{rccc} I: & \mathcal{C}(X, \overline{\mathbb{R}}^+) & \to & \mathcal{C}(\mathcal{M}(X), \overline{\mathbb{R}}^+) \\ & f & \mapsto & I(f) \end{array} \tag{2.4}$$

is Scott-continuous. Indeed, taking an increasing sequence f_n, $I(\sup_n f_n)$ is the function which maps μ to $\int (\sup_n f_n) d\mu = \sup_n \int f_n d\mu = \sup_n I(f_n)(\mu)$ so it is the point-wise supremum of the functions $I(f_n)$, which is exactly $\sup_n I(f_n)$. Again, proposition 1.2.0.2 allows to establish the Scott-continuity of I.

Proposition 2.1.5.1. *The integral operator $I : \mathcal{C}(X, \overline{\mathbb{R}}^+) \to \mathcal{C}(\mathcal{M}(X), \overline{\mathbb{R}}^+)$ defined at (2.4) is constructive.*

Proof. Consider a finite supremum of step functions $f_n = \sup\{\mathrm{St}_{B_{i_1}}^{q_{j_1}}, \ldots, \mathrm{St}_{B_{i_k}}^{q_{j_k}}\}$. The functions can be reordered so that $q_{j_1} \geq q_{j_1} \geq \ldots \geq q_{j_k}$. The integral $\int f_n d\mu$ can be expressed using the valuation operator v, by induction on k:

$$\begin{array}{rcl} \displaystyle\int \sup\{\mathrm{St}_{B_{i_1}}^{q_{j_1}}, \ldots, \mathrm{St}_{B_{i_k}}^{q_{j_k}}\} d\mu & = & q_{j_k} \mu(B_{i_1} \cup \ldots \cup B_{i_k}) + \\ & & \displaystyle\int \sup\{\mathrm{St}_{B_{i_1}}^{q_{j_1} - q_{j_k}}, \ldots, \mathrm{St}_{B_{i_{k-1}}}^{q_{j_{k-1}} - q_{j_k}}\} d\mu \end{array}$$

When only one function remains, the integral is simply $\int \mathrm{St}_{B_i}^{q_j} d\mu = q_j \mu(B_i)$. Replacing $\int \ldots d\mu$ by $I(\ldots)$ and $\mu(\ldots)$ by $v(\ldots)$, and using the fact that v is constructive (proposition 2.1.4.1), we obtain that $I(f_n)$ is a lower semi-computable function, uniformly in n. So I is constructive. □

Remark 2.1.5.1. Here is a simple corollary which will be used in the construction of the uniform randomness test (see section 3.1.2). We recall that C_i is the complement of $\overline{B}_i$. We define the upper semi-computable functions $\mathrm{St}_{\overline{B}_i}^{q_j} = q_j - \mathrm{St}_{C_i}^{q_j}$, which will also be denoted by $\overline{\mathrm{St}_{\langle i,j \rangle}}$. If F_k is a finite subset of $\mathbb{N}$, we define $\overline{f}_k = \sup\{\mathrm{St}_{\overline{B}_i}^{q_j} : \langle i,j \rangle \in F_k\}$. The function $\mu \mapsto \int \overline{f}_k d\mu$ is then upper semi-computable, uniformly in k. Indeed, let q be the maximal q_j enumerated by F_k: $q - \overline{f}_k = \inf\{\mathrm{St}_{C_i}^{q_j} + q - q_j\}$ is a constructive element of $\mathcal{C}(X, \overline{\mathbb{R}}^+)$, uniformly in k, and $\int \overline{f}_k d\mu = q - \int (q - \overline{f}_k) d\mu$.

Another corollary can easily be inferred:

Corollary 2.1.5.1. *Let f_i be uniformly computable real functions such that $|f_i| \leq M_i$ where M_i are uniformly computable bounds. Then the functions $\mu \mapsto \int f_i d\mu$ are uniformly computable.*

Proof. The functions $f_i + M_i$ (resp. $M_i - f_i$) are uniformly lower (resp. upper) semi-computable, so $\int f_i d\mu = \int (f_i + M_i) d\mu - M_i = M_i - \int (M_i - f_i) d\mu$. Proposition 2.1.5.1 allows to conclude. □

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

Proposition 2.1.5.2. *Given a measure $\mu \in \mathcal{M}(X)$, the following are equivalent:*

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

Proof. $[1 \Rightarrow 2]$ is a direct consequence of proposition 2.1.5.1, $[2 \Rightarrow 1]$ is a direct consequence of theorem 2.1.4.1: $\mathbf{1} : \tau \to \mathcal{C}(X, \overline{\mathbb{R}}^+)$ mapping U to $\mathbf{1}_U$ is constructive, so the constructivity of $I\mu$ implies that of $v_\mu = I_\mu \circ \mathbf{1}$, which implies the computability of μ, $[2 \Leftrightarrow 3]$ holds by Scott-continuity of the operator.

□

2.2 Computable Probability Spaces

In this section, we study in details the following class of spaces:

Definition 2.2.0.1. 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.

On a probability space, restricting oneself to continuous functions is too much limited and does not even makes sense: the space L^1 of integrable functions is actually a quotient space, identifying functions which differ on a null set.

On a computable probability space a natural idea is to require functions to be computable *almost everywhere*. Theorem 1.6.2.1 states that functions between computable metric spaces which are computable on a dense set can be extended to functions which are computable on a dense constructive G_δ. So assuming that the measure is supported on the whole space, any function which is computable on a full-measure set can be extended to a function which is computable on a full-measure constructive G_δ. We will see above that the assumption on the support of the measure can be suppressed.

Definition 2.2.0.2.

1. Let (X, μ) be a probability space and Y a computable metric space. A function $f : X \to Y$ is ***almost computable*** if it is constructively continuous on a constructive G_δ of full measure, which we denote by D_f.
2. A ***morphism of probability spaces*** $f : (X, \mu) \to (Y, \nu)$, is an almost computable function $f : X \to Y$ such that $\nu = \mu f^{-1}$.
3. An ***isomorphism*** $(f, g) : (X, \mu) \rightleftarrows (Y, \nu)$ is a pair (f, g) of morphisms such that $g \circ f = id$ on $f^{-1}(D_g)$ and $f \circ g = id$ on $g^{-1}(D_f)$.

If (f, g) is an isomorphism, it can be converted into a bijection $h : D_1 \to D_2$ between full-measure constructive G_δ, such that h and h^{-1} are morphisms. Indeed, put $D_2 = g^{-1}(D_f)$ and $D_1 = f^{-1}(D_2) = g(D_2)$: $h = f|_{D_1} : D_1 \to D_2$ is a bijection and $g|_{D_2}$ is its inverse.

Let (X, μ) be a computable probability space and Y a computable metric space. If $f : X \to Y$ is an almost computable function, then the induced probability measure $\nu = \mu F^{-1}$ is computable, and $f : (X, \mu) \to (Y, \nu)$ is a morphism of computable probability spaces.

Here is a simple example of an isomorphism. Let (X, μ) be a computable probability space. The support $\mathrm{Supp}(\mu)$ of μ (the smallest closed set of full measure) is a constructive closed set: $U \cap \mathrm{Supp}(\mu) \neq \emptyset \iff \mu(U) > 0$. It follows that $\mathrm{Supp}(\mu)$ is a computable metric subspace of X (see theorem 1.6.1.1). The induced measure is μ itself, which is a computable probability measure, as element of $\mathcal{M}(\mathrm{Supp}(\mu))$, and the computable probability spaces (X, μ) and $(\mathrm{Supp}(\mu), \mu)$ are isomorphic. From this, it is possible to assume that the measure is supported on the whole space when necessary.

2.2.1 Generalized binary representations

When studying computability over the reals, the first step is generally to get convinced that the base-two numeral representation of real numbers is not adequate to define computable functions. This relies in the fact that the space $\mathbb{R}$ of real numbers and the Cantor space of binary representations are not homeomorphic.

But many interesting issues on the unit interval $[0, 1]$ arise in a probabilistic context instead of a topological one (think of Borel normality). For this purpose, the numeral system is suitable, and may even be preferred: almost every real has a unique expansion. Moreover, the Cantor space is a privileged place for computability, due to its symbolic nature. For instance belonging to a basic open set (cylinder) can be decided: it boils down to a simple pattern-matching. This is possible only because cylinders are at the same time closed and open.

This idea has already been implicitly used to extend algorithmic randomness from the Cantor space to the unit interval with the Lebesgue measure: algorithmic randomness being at the boundary between probability theory and computability, the numeral system is perfectly appropriate to carry out this extension.

We propose a generalization of the binary representation of real numbers, and prove that every computable probability space admits such a representation. It will have important consequences in the application to dynamical systems, where the use of symbolic models is essential.

To carry out this generalization, let us briefly scrutinize the binary numeral system on the unit interval: $\mathrm{bin} : 2^{\mathbb{N}} \to [0, 1]$ is a total surjective computable function. Every non-dyadic real has a unique expansion, and the inverse of bin, 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 dense G_δ) and has full Lebesgue measure. $(\mathrm{bin}, \mathrm{bin}^{-1})$ 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 2.2.1.1. A ***binary representation*** of a computable probability space (X, μ) is a constructively continuous surjective function $\rho : 2^\omega \to X$ such that, calling $\rho^{-1}(x)$ the set of ***expansions*** of $x \in X$:

- there is a constructive dense G_δ of full measure $D \subseteq X$ of points having a unique expansion,
- $\rho^{-1} : D \to \rho^{-1}(D)$ is constructively continuous.

Remark that a constructive G_δ of full measure is always dense in the support of the measure. Also remark that a binary representation ρ induces an isomorphism (ρ, ρ^{-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 2.2.1.1. *Every computable probability space (X, μ) has a binary representation.*

First remark that if there is such a binary representation, the domain D of the isomorphism is then totally disconnected: the pre-images of the cylinders form a basis of clopen and even *decidable* sets. As subsets of the whole space X, they are generally not decidable, but *almost decidable* instead.

Definition 2.2.1.2. A set A is said to be ***almost decidable*** if there are two constructive open sets U and V such that:

$$U \subset A, \quad V \cap A = \emptyset, \quad U \cup V \text{ is dense and has measure one}$$

Remark that, as for subsets of $\mathbb{N}$, a set is almost decidable if and only if its complement is almost decidable. An almost decidable set is always a continuous 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 at distance r from s, then $B(s, r)$ is almost decidable: take $U = B(s, r)$ and $V = X \setminus \overline{B}(s, r)$. The indicator $\mathbf{1}_A : X \to [0, 1]$ of an almost decidable set A is an almost computable function.

We say that the elements of a sequence $(A_i)_{i \in \mathbb{N}}$ are uniformly almost decidable if there are uniformly constructive open sets U_i, V_i satisfying the conditions of the definition.

Proposition 2.2.1.1. *If A is almost decidable then $\mu(A)$ is a computable real number.*

Proof. Since U and V are constructive open sets, by proposition 2.1.4.1 their measures are lower semi-computable. As $\mu(U) + \mu(V) = 1$, their measures are also upper semi-computable. $\square$

Consequences of Baire's theorem

We present a series of lemma which follow from the computable Baire theorem (theorem 1.6.1.3).

Lemma 2.2.1.1. *Let (Y, μ) be a computable probability space with no isolated point. Then there is a sequence of uniformly computable points $(y_n)_n$ which is dense in X satisfying $\mu(\{y_n\}) = 0$ for all n.*

Proof. The set $R = \{y \in Y : \mu(\{y\}) = 0\}$ is a constructive G_δ: $R = \bigcap_n \bigcup_{i:\mu(\overline{B}_i)<2^{-n}} B_i$. If Y has no isolated point, R is moreover dense in Y. $\square$

Corollary 2.2.1.1. *Let (X, μ) be a computable probability space and Y be a computable metric space without isolated point. Let $f_i : X \to Y$ be a sequence of uniformly computable functions. Then there is a sequence $(y_n)_n$ of uniformly computable points of Y which is dense in Y and such that for all i, n, $f_i^{-1}(y_n)$ is a μ-null set.*

Proof. Define the uniformly computable measures $\mu_i = \mu f_i^{-1}$ and apply the previous lemma to the computable measure $\mu = \sum_i 2^{-i}\mu_i$ (or intersect the uniform sequence of constructive G_δ, which gives a constructive G_δ). $\square$

We can strengthen this requiring these sets to be also negligible from a topological point of view. We recall that a set A is nowhere dense if the interior of its closure is empty; if A is a closed set, A is nowhere dense if and only if its complement is dense.

Corollary 2.2.1.2. *Under the same hypotheses, there is a sequence $(y_n)_n$ of uniformly computable points of Y which is dense in Y and such that for all i, n, $f_i^{-1}(y_n)$ is a nowhere dense μ-null set.*

Proof. Intersect the constructive G_δ from the preceding corollary with $\bigcap_{i,j} Y \setminus \{f_i(s_j)\}$. The y_n constructed are such that every ideal point is outside $f_i^{-1}(y_n)$, so the complement of $f_i^{-1}(y_n)$ is a dense open set. $\square$

Theorem 2.2.1.2. *There is a sequence $(r_n)_{n\in\mathbb{N}}$ of uniformly computable positive real numbers such that $(B(s_i, r_n))_{\langle i,n\rangle}$ is a basis of uniformly almost decidable balls.*

Proof. Apply the preceding corollary to $f_i : X \to \mathbb{R}^+$ defined by $f_i(x) = d(s_i, x)$. □

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 2.2.1.3. For $w \in 2^*$, 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.

We are now able to prove theorem 2.2.1.1.

Proof of theorem 2.2.1.1. We construct an encoding function $b : D \to 2^\omega$, a decoding function $\rho : D_\rho \to X$, and show that ρ is a binary representation, with $b = \rho^{-1}$.

Encoding. Let $D = \bigcap_i B^\mu_i \cup C^\mu_i$: this is a dense full-measure constructive G_δ. Define the computable function $b : D \to 2^\omega$ by:

$$b(x)_i = \begin{cases} 1 & \text{if } x \in B^\mu_i \\ 0 & \text{if } x \in C^\mu_i \end{cases}$$

Let $x \in D$: $\omega = b(x)$ is also characterized by $\{x\} = \bigcap_i \Gamma(\omega_{0..i-1})$. Let μ_ρ be the image measure of μ by b: $\mu_\rho = \mu \circ b^{-1}$. b is then a morphism from (X, μ) to $(2^\omega, \mu_\rho)$.

Decoding. Let D_ρ 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 $\rho : D_\rho \to X$ by:

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

ω is called an expansion of x. Remark 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, $b = \rho^{-1} : \rho^{-1}(D) \to D$ and $\mu_\rho(D_\rho) = \mu(D) = 1$.

We now show that $\rho : D_\rho \to X$ is a surjective morphism. For 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_ρ is a Π_2^0-set: we show that $D_\rho = \bigcap_n \{\omega \in 2^\omega : \omega \text{ has a } n\text{-witness}\}$.

Let $\omega \in D_\rho$ and $x = \rho(\omega)$. 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 of 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.

• $\rho : D_\rho \to X$ 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 $\rho(\omega)$.

• ρ is surjective: we show that each point $x \in X$ has at least one expansion. To do this, we construct by induction a sequence $\omega = \omega_0\omega_1\ldots$ such that for all i, $x \in \overline{\Gamma(\omega_0 \ldots \omega_i)}$. Let $i \geq 0$ and suppose that $\omega_0 \ldots \omega_{i-1}$ (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.

□

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 2.1.4.1). Let us say that two bases $(U_i)_i$ and $(V_i)_i$ of the topology τ are constructively equivalent if the corresponding effective topological spaces are isomorphic.

Corollary 2.2.1.3. *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 the basis $\mathcal{B}$ of ideal balls 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 almost 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 constructive open sets are uniformly constructive 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 2.1.4.1. □

2.2.2 Computable Lebesgue space

It is a classical result that metric spaces endowed with a probability measure are *Lebesgue spaces*, i.e. isomorphic to the unit interval with the Lebesgue measure together with a countable set of mass points (see [Bil68]). We define:

Definition 2.2.2.1. A computable probability space is a ***computable Lebesgue space*** if it is isomorphic to the computable probability space $([0,1], \lambda)$ where λ is the Lebesgue measure.

and prove:

Theorem 2.2.2.1. *Every computable probability space with no atom is a computable Lebesgue space.*

We first prove the result for $(I = [0,1], \mu)$.

Lemma 2.2.2.1. *The interval endowed with a non-atomic computable probability measure is a computable Lebesgue space.*

Proof. We define the morphism of computable probability spaces $F(x) = \mu([0,x])$. As μ has no atom and is computable, F is computable and surjective.

As F is surjective, it has right inverses. Two of them are $G_<(y) = \sup\{x : F(x) < y\}$ and $G_>(y) = \inf\{x : F(x) > y\}$, and satisfy $F^{-1}(y) = [G_<(y), G_>(y)]$. They are increasing and respectively left and right-continuous. As F is computable, they are even lower and upper semi-computable respectively.

Let us define $D = \{y : G_<(y) = G_>(y)\}$: every $y \in D$ has a unique pre-image by F, which is then injective on $F^{-1}(D)$. The restriction of F on $F^{-1}(D)$ has a left-inverse, which is given by the restriction of $G_<$ and $G_>$ on D. Let us call it $G : D \to I$. By lower and upper semi-computability of $G_<$ and $G_>$, G is computable.

Now, D is a Π^0_2-set: $D = \cap_n\{y : G_>(y) - G_<(y) < 1/n\}$. We show that $I \setminus D$ is a countable set. The family $\{[G_<(y), G_>(y)] : y \in I\}$ indexed by I is a family of disjoint closed intervals, included in $[0,1]$. Hence, only countably many of them have positive length. Those intervals are indexed by points y belonging to $I \setminus D$, which is then countable. It follows that D has Lebesgue measure one.

(F, G) is then an isomorphism between (I, μ) and (I, λ).

□

Proof of the theorem. We know from theorem 2.2.1.1 that every computable probability space (X, μ) has a binary representation, which is in particular an isomorphism with the Cantor space $(2^{\mathbb{N}}, \nu_\rho)$. Using the classical binary representation of real numbers, the latter is isomorphic to the unit interval (I, μ_I) with the induced measure μ_I. If μ is non-atomic, so is μ_I. By the previous lemma, (I, μ_I) is isomorphic to (I, λ). □

2.3 When the measure is not computable

Let X be a computable metric space and μ a (not necessarily computable) Borel probability measure. We can consider, for a Borel probability μ on X, the enumerative lattice τ^μ. The topologies τ and τ^μ are the same, only their associated countable bases $\mathcal{B}$ and $\mathcal{B}^\mu$ differ: the constructive open sets of $(X, \tau^\mu, \mathcal{B}^\mu)$ are the μ-constructive open sets of $(X, \tau, \mathcal{B})$.

We recall that $\tau^\mu \equiv \mathcal{C}(\{\mu\}, \tau)$. τ^μ is a pseudo-computable enumerative lattice, and makes $(X, \tau^\mu, \mathcal{B}^\mu)$ an effective topological space. When μ is computable, $(X, \tau^\mu, \mathcal{B}^\mu)$ is isomorphic to $(X, \tau, \mathcal{B})$.

The G_δ sets are the elements of the enumerative lattice $(\tau^\mu)^{\mathbb{N}}$: its constructive elements are the μ-constructive G_δ sets. It may be useful to remark that $(\tau^\mu)^{\mathbb{N}} \equiv \mathcal{C}(\mathbb{N}, \tau^\mu) \equiv \mathcal{C}(\mathbb{N} \times \{\mu\}, \tau) \equiv \mathcal{C}(\{\mu\}, \tau^{\mathbb{N}}) \equiv (\tau^{\mathbb{N}})^\mu$.

It gives a direct notion of μ-constructivity for functions: a function f from X to an effective topological space Y is μ-constructively continuous if $f^{-1} : \tau_Y \to (\tau_X)^\mu$ is constructive. It is equivalent to the existence of a constructively continuous function $g : \{\mu\} \times X \to Y$ such that $f(x) = g(\mu, x)$.

From this, we could consider probability spaces (X, μ) for non-computable measures, and define the associated notions of morphisms. But the computability of the measure was essential in the construction of the binary representation. First, the construction of

μ-continuity points (lemma 2.2.1.1) cannot be made uniform in the measure:

Proposition 2.3.0.1. *There is no continuous function $f : \mathcal{M}([0,1]) \to [0,1]$ such that $\mu(\{f(\mu)\}) = 0$ for all μ.*

Proof. The function $\delta : x \to \delta_x$ is continuous, so $f \circ \delta$ is a continuous function from $[0,1]$ to $[0,1]$, so it has a fixed point x_0: $\delta_{x_0}(\{f(\delta_{x_0})\}) = 1$. $\square$

Proposition 2.3.0.2. *There is no continuous function $f : \mathcal{M}(\mathbb{R}) \to \mathbb{R}$ such that $\mu(\{f(\mu)\}) = 0$ for all μ.*

Proof. If such an f exists, let $g : \mathbb{R} \to \mathbb{R}$ be the continuous function defined by $g(x) = f(\delta_x)$. As in the preceding proof, we prove that g must have a fixed point, which contradicts the hypothesis on f.

Let us suppose that g has no fixed point: replacing g by $x \mapsto -g(-x)$, we can assume without loss of generality that $g(x) > x$ for all x. Let $\alpha = g(0) + 1$. The function $h : \lambda \mapsto f((1-\lambda)\delta_0 + \lambda\delta_\alpha)$ is continuous and $h(\lambda) \neq \alpha$ for all $\lambda \in (0,1]$. As $h(0) = g(0) < \alpha$, $h(1) < \alpha$ and hence $g(\alpha) = h(1) < \alpha$. As $g(0) > 0$, g has a fixed point in $(0, \alpha)$. $\square$

Moreover, the construction which was possible for a computable measure is not possible in general:

Proposition 2.3.0.3. *There exists a (non-computable) Borel probability measure μ on $[0,1]$ which has no μ-computable continuity point.*

Sketch of the proof. The space $[0,1]^{\mathbb{N}}$ of sequences of real numbers with the product topology has a computable metric. In [Mil04], Miller proved the existence of a sequence $\alpha = (\alpha_n)_n \in [0,1]^{\mathbb{N}}$ such that there is no x which is α-computable and which does not belong to α. Such a sequence has no "computable diagonalization", i.e. there is no way to construct a point $x \notin \alpha$ from α. In particular, α contains all computable reals, as every computable real is also α-computable.

Let $\mu = \sum_i 2^{-i}\delta_{\alpha_i}$ be the mixture of the Dirac measures concentrated on the points of this sequence. μ is α-computable, so μ has no μ-computable continuity point (which should not belong to α and be α-computable). $\square$

The reason lies in the fact that μ has no minimal degree, i.e. there is no binary sequence ω which is μ-computable and such that μ is ω-computable. Such a sequence would be a representative for μ, which could be computed from any Cauchy sequence of ideal measures converging exponentially fast to μ.

When μ has a minimal degree, the construction of continuity points can be made extensional, i.e. independent of the particular Cauchy sequence converging to μ, describing μ by ω. Hence, such a measure has μ-computable continuity points.

Chapter 3

Algorithmic probability theory

Probability theory enables one to formulate and prove sentences like “property P holds with probability one”, or “property P holds almost surely”. An idea which was already addressed by Laplace, and later by Von Mises, is to identify the properties that an infinite binary sequence should satisfy to be qualified “random”. Church and later Kolmogorov proposed a definition using computability theory, but Martin-Löf ([ML66]) was the first one who defined a sound notion: a binary sequence is random if it satisfies all properties of probability one which can be presented in an *algorithmic way*. A characterization of Martin-Löf randomness in terms of Kolmogorov complexity was later proved, conferring robustness to this notion.

3.1 Algorithmic randomness

Still recently, algorithmic randomness was only defined on the space of binary sequences (or sequences on a finite alphabet). We first recall the classical setting.

3.1.1 Martin-Löf randomness on the Cantor space

Let $\Sigma^{\mathbb{N}}$ be the space of infinite sequences on a finite alphabet Σ.

A finite string is easily describable if its Kolmogorov complexity is low. Kolmogorov tried to define a notion of algorithmic random sequence as whose prefixes have maximal complexity. Martin-Löf showed in [ML71] that this definition did not work: no infinite sequence could be random in this sense. This lead him to propose in [ML66] a sound notion using tests:

Definition 3.1.1.1. Let μ be a computable probability measure on $\Sigma^{\mathbb{N}}$. A μ-***Martin-Löf test*** is a sequence of uniformly constructive open sets U_n satisfying $\mu(U_n) < 2^{-n}$.

A sequence ω ***passes*** such a test if $\omega \notin \bigcap_n U_n$.

A sequence is μ-***Martin-Löf random*** if it passes all μ-Martin-Löf tests.

In other words, the property "being in $\bigcap_n U_n$" has null probability, in an effective way: $\bigcap_n U_n$ is called an ***effective*** μ***-null set***.

He proved the following remarkable result:

Theorem. *There is a universal μ-Martin-Löf test, i.e. a test that is passed exactly by random sequences.*

Later, Chaitin and Levin independently proposed the prefix variant of the Kolmogorov complexity (see section 1.8) which enables to define a sound notion of individual algorithmic randomness. It was then proved that this notion coincides with Martin-Löf's one.

Theorem 3.1.1.1 (Schnorr, Levin)**.** *Let μ be a computable measure on $\Sigma^{\mathbb{N}}$. A sequence ω is μ-Martin-Löf random if and only if there is a constant c such that for all n,*

$$K(\omega_{0..n-1}) > -\log \mu[\omega_{0..n-1}] - c.$$

($\omega_{0..n-1}$ is the word which consists of the first n symbols of ω). The minimal such c, called the ***randomness deficiency*** of ω, and defined by:

$$d_\mu(\omega) := \sup_n \{-\log \mu[\omega_{0..n-1}] - K(\omega_{0..n-1})\}$$

for all ω, is then finite exactly on random sequences.

Moreover, the coding theorem provides a simple upper bound on the complexity of words, when the space is endowed with a computable measure. The function $P : \Sigma^* \to [0,1]$ defined by $P(w) = 2^{-K(|w|)}\mu([w])$ is a semi-measure (see theorem 1.8.3.1): $P(w)$ is lower semi-computable uniformly in w, and $\sum_w P(w) = \sum_n 2^{-K(n)} \leq 1$, so the coding theorem gives:

Proposition 3.1.1.1. *Let μ be a computable measure on $\Sigma^{\mathbb{N}}$. For all $w \in \Sigma^*$,*

$$K(w) \stackrel{+}{<} -\log \mu([w]) + K(|w|)$$

Another presentation of tests is possible: a μ-randomness test is defined as a positive lower semi-computable function $t : \{0,1\}^{\mathbb{N}} \to \mathbb{R}$ satisfying $\int t d\mu \leq 1$ (see [VV93] for an interpretation of such tests). The associated effective null set is $\{x : t(x) = +\infty\} = \bigcap_n \{x : t(x) > 2^n\}$.

If U_n is a Martin-Löf test then $t(\omega) = \sup\{n : \omega \in U_n\}$ is a randomness test. Conversely, if t is a randomness test, then the sequence $U_n = \{x : t(x) > 2^n\}$ is a Martin-Löf test.

Gács proved in [Gác79] that 2^{d_μ} is a universal randomness test: it multiplicatively dominates all randomness tests, i.e. for all test t, there is a constant c such that $2^{d_\mu} \geq ct$.

The proof of the existence of a universal test lies on the effective enumeration of all tests. Using this presentation of tests, we show how to derive this enumeration from proposition 1.4.1.7:

Proposition 3.1.1.2. *The enumerative lattice $\mathcal{C}(2^{\mathbb{N}}, \overline{\mathbb{R}}^+)$ is computable. If μ is a computable measure on $2^{\mathbb{N}}$, the subset of functions f satisfying $\int f d\mu \leq 1$ is a constructive closed set.*

Proof. $\mathrm{St}^q_{[w]} \ll f \iff q < \inf_{\omega \in [w]} f(\omega) \iff [w] \subseteq f^{-1}(q, +\infty]$ which is semi-decidable, as $[w]$ is compact in a constructive way.

Let f be a finite supremum of step functions. $\Uparrow f \cap A \neq \emptyset \iff \exists g \in A, f \ll g \iff \int f d\mu < 1$, which is semi-decidable as $\int f d\mu$ is computable (on the Cantor space). □

3.1.2 Martin-Löf randomness on a computable metric space

A first extension to more general spaces was proposed in [HW98] and [HW03], but a sound theory of computable measures was lacking and in some sense the assumptions put on the probability measure are not stable. A suitable extension to computable metric spaces was carried out in [Gác05], generalizing at the same time Levin's theory: algorithmic randomness is also defined for non-computable probability measures. We improve this work removing a computability condition for the existence of a universal randomness test. Our work is currently submitted to a journal ([HR07]).

As testing a statistical property may require computations using the probability measure μ, they are generally not constructive when μ is not computable. Instea, they are constructive *relatively* to μ. We briefly recall how relative contructivity can be expressed in a simple way, when dealing with objects in an enumerative lattice.

Let L be an enumerative lattice and x a point of an effective topological space X. An element $l \in L$ is x-constructive if there is a constructive function $f \in \mathcal{C}(\{x\}, L)$ such that $f(x) = l$, which is equivalent to the existence of a constructive function $f \in \mathcal{C}(X, L)$ such that $f(x) = l$ (we recall that constructive functions from $D \subseteq X$ to L are exactly the restrictions to D of constructive functions from X to L) (see section 1.3.2 for more details).

We also recall that lower semi-computable functions from X to $\overline{\mathbb{R}}^+$ are defined as constructive elements of $\mathcal{C}(X, \overline{\mathbb{R}}^+)$. Mixing these two remarks gives the notion of a μ-lower semi-computable function from X to $\overline{\mathbb{R}}^+$: it is a μ-constructive element of $\mathcal{C}(X, \overline{\mathbb{R}}^+)$.

Definition 3.1.2.1. Given a probability measure μ, a ***μ-randomness test*** is a μ-lower semi-computable function $t : X \to \overline{\mathbb{R}}^+$ such that $\int t d\mu \leq 1$.

A ***uniform randomness test*** is a lower semi-computable function $t : \mathcal{M}(X) \times X \to \overline{\mathbb{R}}^+$ such that for all $\mu \in \mathcal{M}(x)$, $\int t_\mu d\mu \leq 1$ where t_μ denotes $t(\mu, .)$.

Definition 3.1.2.2. A point $x \in X$ is said to be ***μ-random with respect to t*** if $t_\mu(x) < \infty$. A point is ***μ-random*** if it is random w.r.t every test t. The set of μ-random points is denoted by R_μ.

A set $N \subseteq X$ is a ***μ-effective null set*** if there is a randomness test t such that $N \subseteq \{x \in X : t_\mu(x) = +\infty\}$.

By definition, a uniform test t is a constructive element of $\mathcal{C}(\mathcal{M}(X) \times X, \overline{\mathbb{R}}^+)$ and can also be seen, by curryfication, as a constructive element of $\mathcal{C}(\mathcal{M}(X), \mathcal{C}(X, \overline{\mathbb{R}}^+))$.

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

We show an important result which holds on any computable metric space: there is a *universal* uniform randomness test (theorem 3.1.2.1). This result was already obtained in [Gác05] but only on spaces which have recognizable Boolean inclusions, which is an additional computability property on the basis of ideal balls.

Proposition 3.1.2.1. *There is a sequence $(t_e)_{e \in \mathbb{N}}$ of uniformly lower semi-computable functions from $\mathcal{M}(X) \times X$ to $\overline{\mathbb{R}}^+$ satisfying:*

1. *t_e is a uniform randomness test for all e,*

2. *if f is a lower semi-computable function, then there is e such that for all μ which satisfies $\int f(\mu, .) d\mu \leq 1$, it holds $t_e(\mu, .) = f(\mu, .)$.*

Proof. For each finite subset F_k of $\mathbb{N}$, consider the functions from $\mathcal{M}(X) \times X$ to $\overline{\mathbb{R}}^+$: $f_k = \sup_{i \in F_k} \mathrm{St}_i$ and $\overline{f}_k = \sup_{i \in F_k} \overline{\mathrm{St}_i}$ (see remark 2.1.5.1), which are respectively lower and upper semi-computable. The function $m_k : \mathcal{M}(X) \to [0,1]$ defined by $m_k(\mu) = \int \overline{f}_k(\mu, .) d\mu$ is upper semi-computable by remark 2.1.5.1, so the sets $W_k := m_k^{-1}[0,1)$ are uniformly constructive open subsets of $\mathcal{M}(X)$. If $\mu \in W_k$ then $\int f_k(\mu) d\mu \leq m_k(\mu) < 1$.

Consider the effective enumeration $(E_e)_{e \in \mathbb{N}}$ of the r.e. subsets of $\mathbb{N}^2$: there is a recursive function $\varphi : \mathbb{N}^2 \to \mathbb{N}$ such that $E_e = \bigcup_n F_{\varphi(e,n)}$ and $F_{\varphi(e,n)} \subseteq F_{\varphi(e,n+1)}$. Define

$$t_e = \sup_n f_{\varphi(e,n)}.\mathbf{1}_{W_{\varphi(e,n)} \times X}$$

The functions t_e are uniformly constructive and are uniform tests. Indeed, as $f_{\varphi(e,n)} \leq f_{\varphi(e,n+1)}$, $\int t_e(\mu, .) d\mu = \sup\{\int f_{\varphi(e,n)}(\mu, .) : \mu \in W_{\varphi(e,n)}\} \leq 1$.

Now, let f be a lower semi-computable function from $\mathcal{M}(X) \times X$ to $\overline{\mathbb{R}}^+$. There is a r.e. set $E \subseteq \mathbb{N}$ such that $f = \sup_{j \in E} \mathrm{St}_j$. Let $E' = \{i : \exists j \in E, \mathrm{St}_i \lhd \mathrm{St}_j\}$. E' is r.e. so there is e such that $E' = E_e$: we prove that $t_e(\mu, .) = f(\mu, .)$ for each μ such that $\int f(\mu, .) d\mu \leq 1$.

By definition of $E_e = E'$, $f = \sup_n f_{\varphi(e,n)} = \sup_n \overline{f}_{\varphi(e,n)}$, so $m_{\varphi(e,n)}(\mu) = \int \overline{f}_{\varphi(e,n)}(\mu, .) \leq \int f(\mu, .) d\mu$. Moreover, $\overline{f}_{\varphi(e,n)}(\mu, x) < f(\mu, x)$ as soon as $f(\mu, x) > 0$, so $\int f(\mu, .) d\mu = 0$ or $\int \overline{f}_{\varphi(e,n)}(\mu, .) d\mu < f(\mu, .) d\mu$. In both cases, $\mu \in W_{\varphi(e,n)}$ whenever $\int f(\mu, .) d\mu \leq 1$. Hence, $t_e(\mu, .) = \sup_n f_{\varphi(e,n)}(\mu, .) = f(\mu, .)$. □

It has two important consequences:

Corollary 3.1.2.1. *Let t be a μ-test: there is a uniform test t' such that $t'_\mu = t$.*

Proof. $t : \{\mu\} \times X \to \overline{\mathbb{R}}^+$ can be extended to a lower semi-computable function $f : \mathcal{M} \times X \to \overline{\mathbb{R}}^+$. Applying the preceding proposition to f gives a uniform test t' which coincides with f on μ: $t'_\mu = f_\mu = t$. □

Theorem 3.1.2.1 (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 with $t_u \geq ct$.*

Let μ be a probability measure on X. A point $x \in X$ is μ-random if and only if it is μ-random with respect to t_u.

Proof. It is defined by $t_u := \sum_e 2^{-e-1} t_e$. □

3.1.3 Weaker notions of randomness

Martin-Löf random points are points which pass a large class of tests, but for some theorems, this class is broader than necessary. In [Sch71], Schnorr proposed a smaller class of tests which induce a strictly weaker notion of randomness, which are sufficiently random to satisfy many classical probability theorems, as for instance the strong law of large numbers (on the Cantor space with a Bernoulli measure). Schnorr tests may not be suitable on computable metric spaces with non-computable measures. We introduce the class of *Borel-Cantelli* tests which we will prove later to be equivalent to Schnorr tests when the measure is computable.

The weak notion of Kurtz-randomness can be straightforwardly extended to metric spaces, and happens to be very useful. We refer the reader to [HW97], [DG] for characterizations of Schnorr and Kurtz randomness on the Cantor space.

First, let us recall the celebrated Borel-Cantelli lemma.

Theorem (Borel-Cantelli). *Let (X, μ) be a probability space and A_n be measurable sets.*

If $\sum_n \mu(A_n) < \infty$ then for μ-almost every x, $x \in A_n$ only finitely many times.

If $\sum_n \mu(A_n) = \infty$ and the A_n's are pairwise independent, then for μ-almost every x, $x \in A_n$ infinitely many times.

From now, we suppose that X is a computable metric space and μ is a Borel probability measure on X (for the moment, we do not require μ to be computable). We denote by Π_1^μ the set of complements of μ-constructive open sets (see section 2.3).

A sequence x_n of non-negative real numbers is said to be ***effectively summable*** if there is a total recursive function $\phi : \mathbb{N} \to \mathbb{N}$ such that $\sum_{n \geq \phi(i)} x_n < 2^{-i}$.

Definition 3.1.3.1. A ***Borel-Cantelli test*** (BC-test for short) is a sequence $(A_n)_{n\in\mathbb{N}}$ of uniformly Π_1^μ-sets such that the sequence $\mu(A_n)$ is effectively summable.

A point x ***passes a Borel-Cantelli test*** if it belongs to A_n only finitely many times, i.e. if $x \notin \limsup_n A_n$.

A point is ***Schnorr random*** if it passes all BC-tests.

If $P(x)$ is a property of points of X, we will say that P is ***tested by a BC-test*** $(A_n)_n$ if $P(x)$ holds for all points x that pass the test: passing the test is a guarantee that P will be satisfied (but it may not be an equivalence). Let us point out simple properties of BC-tests, which follow from the fact that the class Π_1^μ is closed under finite unions, in a constructive way.

Normal form If $(A_n)_n$ is a BC-test, it can be converted into a BC-test $(B_n)_n$ such that $\mu(B_n) < 2^{-n}$. Indeed, there is a computable sequence of natural numbers k_i such that $\mu(\sum_{n\geq k_i} \mu(A_n)) < 2^{-i}$. Put $B_i = \bigcup_{k_i \leq n < k_{i+1}} A_n$. Obviously, a point belongs to A_n infinitely often if and only if it belongs to B_i infinitely often. This construction is uniform in the primitive test.

Finite conjunction If properties P, P' can be tested by BC-tests $(A_n)_n$ and $(A'_n)_n$, then the conjunction $P \wedge P'$ can be tested by a single BC-test: the sequence defined by $A''_n = A_{n+1} \cup A'_{n+1}$ is a BC-test, and $\limsup_n A''_n = \limsup_n A_n \cup \limsup_n A'_n$.

Countable conjunction If property P_i can be tested by BC-test $(A^i_n)_n$ and if the tests are uniform in i, then the conjunction of all P_i can be tested by a single BC-test $A'_n = \bigcup_{i<n} A^i_{n+1+i}$: it is easy to check that $\bigcup_i \limsup_n A^i_n \subseteq \limsup_n A'_n$. Indeed, for each i, $\bigcap_k \bigcup_{n>k} A^i_n = \bigcap_k \bigcup_{n>k} A^i_{n+1+i} \subseteq \bigcap_k \bigcup_{n>k} A'_n$.

We will also use a smaller class of tests (see [DGR04] for more information):

Definition 3.1.3.2. A ***Kurtz-test*** is a sequence of uniformly Π_1^μ sets A_n satisfying $\mu(A_n) = 0$.

A point ***passes a Kurtz-test*** if $x \notin \bigcup_n A_n$.

A point is ***Kurtz-random*** if it passes all Kurtz-tests.

Actually, $(A_n)_n$ is a Kurtz test if and only if $\bigcap_n (X \setminus A_n)$ is a μ-constructive G_δ of full measure.

Proposition 3.1.3.1. *Every Kurtz random point is in the support of the measure.*

Proof. $\mathrm{Supp}(\mu)$ is a μ-constructive G_δ: $B \cap \mathrm{Supp}(\mu) \neq \emptyset \iff \mu(B) > 0$. And it has full measure. □

On the Cantor space with a computable measure, it is well-known that Martin-Löf randomness implies Schnorr-randomness which implies Kurtz-randomness, the first implication being straightforward as Schnorr-tests are defined as a particular class of Martin-Löf tests. We establish a generalization of this theorem. This time, the second implication is direct. For the first one, one has to be careful: as in the construction of the universal test, extensionality with respect to the measure is a problem which did not exist for computable measures.

Theorem 3.1.3.1. *Martin-Löf-randomness ⇒ Schnorr-randomness ⇒ Kurtz-randomness.*

Proof of the first implication. Let $A_n = X \setminus U_n$ be a BC-test. We enclose A_n in a μ-constructive open set T_n of measure $\leq 2^{-n}$. We first make the description of U_n independent of μ: $U_n = V_n(\mu)$ where V_n are uniformly constructive open subsets of $\mathcal{M}(X) \times X$: $V_n = \bigcup_{i \in E_n} B_i$ where E_n are uniformly r.e. sets. We now describe V_n by closed balls: defining $E'_n = \{j : \exists i \in E_n, B_j \triangleleft B_i\}$, $V_n = \bigcup_{j \in E'_n} B_j = \bigcup_{j \in E'_n} \overline{B}_j$. As E'_n is r.e. uniformly in n, there is a total recursive function $\varphi : \mathbb{N}^2 \to \mathbb{N}$ such that $E'_n = \bigcup_p F_{\varphi(p,n)}$ with $F_{\varphi(p,n)} \subseteq F_{\varphi(p+1,n)}$. Denoting the complement of $\overline{B}_j$ by C_j, we define the uniformly constructive open sets:

$$V_{p,n} = \bigcup_{j \in F_{\varphi(p,n)}} B_j \quad \text{and} \quad W_{p,n} = \bigcap_{j \in F_{\varphi(p,n)}} C_j$$

By construction, (i) $V_n = \bigcup_p V_{p,n}$, (ii) $V_{p,n} \cap W_{p,n} = \emptyset$ and (iii) $A_n \subseteq W_{p,n}$. We finally define $T_n = \bigcup_{p:\mu(V_{p,n}(\mu))>1-2^{-n}} W_{p,n}(\mu)$ which is, by construction, a μ-ML-test. As $\mu(V_n(\mu)) = \mu(U_n) > 1 - 2^{-n}$, there is p such that T_n contains $W_{p,n}(\mu)$, which contains A_n. It follows that $\limsup_n A_n \subseteq \limsup_n T_n$, so $(\bigcup_{n>k} T_n)_k$ is a μ-ML-test containing $\limsup_n A_n$. □

Proof of the second implication. Let $(A_n)_n$ be a Kurtz-test. Define $B_n = \bigcap_{k \geq n} A_k$ which is also a Kurtz-test and hence a BC-test, and $\limsup_n B_n = \bigcap_n A_n$. □

The three notions enable us to state a sharp Borel-Cantelli lemma for algorithmic random points (see [Dav01] for similar results for Martin-Löf random sequences).

Proposition 3.1.3.2 (Borel-Cantelli for random points)**.** *Let X be a computable metric space and μ a Borel probability measure on X. Let A_n be Borel sets.*

i) If A_n is a μ-constructive open set, uniformly in n, and $\sum_n \mu(A_n) < \infty$ then every μ-Martin-Löf random point belongs to only finitely many A_n.

ii) If A_n is a Π_1^μ-set, uniformly in n, and the sequence $\mu(A_n)$ is effectively summable then every μ-Schnorr random point belongs to only finitely many A_n.

iii) If A_n is a μ-constructive open set, uniformly in n, the A_n's are independent events and $\sum_n \mu(A_n) = \infty$, then every μ-Kurtz random point belongs to infinitely many A_n.

Proof.

i) Such a sequence $(A_n)_n$ is usually called a Solovay test. Solovay tests are known to be equivalent to Martin-Löf tests. Indeed, define $t(x) = \#\{n : x \in A_n\}$: t is μ-lower semi-computable and $\int t d\mu = \sum_n \mu(A_n) < \infty$, so t is a Martin-Löf test, and $\limsup_n A_n = \{x : t(x) = \infty\}$.

ii) By definition of Borel-Cantelli tests.

iii) It is a direct corollary of the classical theorem: $\limsup_n A_n = \bigcap_n \bigcup_{k\geq n} A_k$ has measure one, so the sets $B_n = X \setminus (\bigcup_{k\geq n} A_k)$ form a Kurtz-test.

□

3.1.4 Application to random variables

We briefly investigate convergence of random variables for algorithmic random points. An attempt toward this direction can be found in [V'y97]. The results established here are rather simple but clarifying, and seem to be new.

Background

Let $(X, d, \mathcal{S})$ be a computable metric space and μ a (not necessarily computable) Borel probability measure on X: it makes (X, μ) a probability space (we do not mention the σ-field, which is always supposed to be the Borel one).

Definition 3.1.4.1. A ***random variable*** on (X, μ) is a measurable function $f : X \to \overline{\mathbb{R}}$.

Definition 3.1.4.2. Random variables f_n ***converge in probability*** to f, written $f_n \to_P f$, if

$$\lim_n \mu[|f_n - f| \geq \epsilon] = 0$$

for each positive ϵ, where $[|f_n - f| \geq \epsilon]$ denotes $\{x : |f_n(x) - f(x)| \geq \epsilon\}$.

Definition 3.1.4.3. Random variables f_n ***converge almost surely*** to f if for almost every point $x \in X$, $f_n(x) \to f(x)$. It is equivalent to the convergence in probability to 0 of $\sup_{k\geq n} |f_n - f|$.

Effective versions

Definition 3.1.4.4. Random variables f_n ***effectively converge in probability*** to f if for each $\epsilon > 0$, $\mu\{x : |f_n(x) - f(x)| < \epsilon\}$ effectively tends 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 3.1.4.5. Random variables f_n ***effectively converge almost surely*** to f if $\sup_{k \geq n} |f_n - f|$ effectively converge in probability to 0.

Proposition 3.1.4.1 (Convergence for Schnorr-random points)**.** *Let f_n, f be uniformly almost computable random variables. If f_n effectively converges almost surely to f then the convergence of $f_n(x)$ to $f(x)$ can be tested by a Borel-Cantelli test. In particular, convergence holds for μ-Schnorr-random points.*

Proof. Define the uniformly constructive open sets $U_n(\epsilon) = [|f_n - f| < \epsilon]$. $\mu(\bigcap_{n \geq k} U_n(\epsilon))$ 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 $V_i = \bigcap_{k_i \leq n < k_{i+1}} U_n(2^{-i})$: V_i is constructively open uniformly in i and $\mu(V_i) > 1 - 2^{-i}$. The complements of the sets V_i form a Borel-Cantelli test, and if a point x passes the test, 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 $n \geq k_i, i \geq i_0$. Remark that the convergence of $f_n(x)$ is effective. □

Proposition 3.1.4.2 (Convergence for Martin-Löf random points)**.** *Let $f_n : X \to \overline{\mathbb{R}}^+$ be a decreasing sequence of uniformly lower semi-computable random variables which effectively converge in probability to 0. Then f_n converges to 0 on Martin-Löf random points.*

Proof. Let ϵ be a positive rational number. By hypothesis $U_n = [f_n > \epsilon]$ are uniformly constructive open sets whose measures converge effectively to 0. □

When the convergence is not effective, a version for random points can still be stated, even if it is weaker.

Proposition 3.1.4.3 (Kurtz-random points)**.** *Let f_n be uniformly lower semi-computable random variables which converge almost surely to a constant c. Then $\limsup_n f_n \geq c$ on Kurtz-random points.*

Proof. Let $a < c$ be a rational number: with probability one, $\limsup_n f_n \geq c$ so $f_n > a$ infinitely many times. In other words the set $\bigcap_k \bigcup_{n > k} [f_n > a]$ has measure one: it is a Kurtz-test. □

Note that the convergence is not supposed to be effective, and the constant c need not be computable.

When the almost sure convergence is not effective, one cannot expect convergence for all Martin-Löf random points. For instance, let Ω be Chaitin's number (it is a lower semi-computable real number in $[0, 1]$, which is Martin-Löf random for the Lebesgue measure λ, see [LV93]). Let $(q_n)_n$ be an increasing computable sequence of rational numbers converging to Ω, and let $U_n = (q_n, \Omega + 1/n)$. $f_n = \mathbf{1}_{U_n}$ is uniformly lower semi-computable and converges λ-almost surely to 0, but $f_n(\Omega) = 1$.

Lemma 3.1.4.1. *Let f be an almost computable random variable. There is a lower semi-computable function $g : X \to \overline{\mathbb{R}}$ such that $f = g$ on D_X.*

Proof. $f : D_f \to \overline{\mathbb{R}}$ is computable, i.e. constructively continuous, so it is also constructively continuous as a function from D_f to $\overline{\mathbb{R}}$ with the order topology. Hence, it is constructively continuous for the lower and upper topologies: as $\mathbb{R}$ is a computable enumerative lattice, f is then a constructive element of $\mathcal{C}(D_f, \overline{\mathbb{R}}_{\leq})$ and $\mathcal{C}(D_f, \overline{\mathbb{R}}_{\geq})$. So it has a lower semi-computable extension g on X. □

Corollary 3.1.4.1. *Let f_n be uniformly almost computable random variables which converge almost surely to a constant c. Then $\limsup_n f_n \geq c \geq \liminf_n f_n$ on Kurtz-random points.*

Proof. Apply the previous lemma to f_n and $-f_n$ (which can be extended to lower semi-computable random variables, which coincide with f_n and $-f_n$ on the domain of computability of f_n, and hence on Kurtz-random points). □

Corollary 3.1.4.2. *Let f_n, f be uniformly almost computable random variables. If f_n converge almost surely to f, then $\limsup_n f_n \geq f \geq \liminf_n f_n$ on Kurtz-random points.*

Proof. Apply the previous lemma to the sequence $f_n - f$ which converges almost surely to 0. □

Rudiments of algorithmic integration theory

Proposition 3.1.4.2 directly induces a result we could be a starting point for an algorithmic version of the classical integration theory, as algorithmic randomness is an algorithmic version of probability theory.

It is a basic result from measure theory that on a metric space X endowed with a Borel probability measure μ, for every Borel set A and every $\epsilon > 0$ there is an open set G and closed set F such that $F \subseteq A \subseteq G$ and $\mu(G \setminus F) < \epsilon$ (see [Bil68]). From this, one easily derives: for every integrable function $h : X \to \overline{\mathbb{R}}^+$ and every $\epsilon > 0$ there is a lower semi-continuous function g and an upper semi-continuous function f such that $f \leq h \leq g$ and $\int (g - f) d\mu < \epsilon$. This approach has been used [Eda07a] to build a computable theory of measure and integration.

Definition 3.1.4.6. An integrable function $h : X \to \overline{\mathbb{R}}^+$ is ***effectively integrable*** if there is a decreasing sequence g_n of uniformly lower semi-computable functions and an increasing sequence f_n of uniformly upper semi-computable functions such that $f_n \leq f \leq g_n$ and $\int (g_n - f_n) d\mu < 2^{-n}$.

A similar definition of effectively measurable set is possible: the effective measurable sets of measure zero are exactly the effective null sets. Consequently, this fits very well with algorithmic randomness:

Proposition 3.1.4.4. *If h is effectively integrable, then $\sup_n f_n(x) = h(x) = \inf_n g_n(x)$ for all Martin-Löf random points x.*

Proof. By Tchebychev inequality, $\mu[g_n - f_n \geq \epsilon] \leq \frac{1}{\epsilon} \int (g_n - f_n) d\mu$ effectively converges to 0, so $\bigcap_n [g_n - f_n > \epsilon]$ is an effective null set. One could also apply proposition 3.1.4.2 to $g_n - f_n$. □

A unified algorithmic theory of measure, integration and randomness should be investigated in the future.

The value of lower semi-computable functions on random points

Here is a rather surprising consequence: lower semi-computable random variables which coincide on a full-measure set actually coincide on an *effective* full-measure set (effective in Kurtz sense).

Proposition 3.1.4.5. *Let $f, g : X \to \overline{\mathbb{R}}$ be lower semi-computable functions. f and g coincide almost everywhere if and only if they coincide on μ-Kurtz random points.*

Proof. Suppose f and g coincide almost everywhere.

There is a r.e. set E such that $g = \sup\{\mathrm{St}_i : i \in E\}$. Define the r.e. set $E' = \{j : \exists i \in E, \mathrm{St}_j \lhd \mathrm{St}_i\}$. Then $g = \sup\{\mathrm{St}_j : j \in E'\} = \sup\{\overline{\mathrm{St}_j} : j \in E'\}$. Enumerating E' and taking finite suprema, we can construct an increasing sequence g_n of uniformly upper semi-computable functions such that $g = \sup g_n$. Applying proposition 3.1.4.3 to $f - g_n$, which are uniformly lower semi-computable and converge almost everywhere to 0, gives $f \geq \liminf_n g_n = g$ on μ-Kurtz random points. Exchanging f and g gives the result. □

Given a lower semi-continuous function $f : X \to \overline{\mathbb{R}}$ and a point x, dropping the value of f on x leaves f lower semi-continuous: for each $a \leq f(x)$, the function g defined by $g(x) = a$ and $g = f$ elsewhere is lower semi-continuous. When f is moreover lower semi-computable and x is a computable point, dropping $f(x)$ to a lower semi-computable number a leaves f lower semi-computable.

The following proposition says that when x is μ-Kurtz random and $\mu(\{x\}) = 0$, $f(x)$ is the maximal possible value.

Proposition 3.1.4.6. *Let f be a lower semi-computable random variable and x a μ-Kurtz random point such that $\mu(\{x\}) = 0$. For each $a \in \overline{\mathbb{R}}$, define $g_a(x) = f(x) + a$ and $g_a = f$ elsewhere. For each $\epsilon > 0$, g_ϵ is not lower semi-continuous at x and $g_{-\epsilon}$ is not lower semi-computable at x.*

Proof. As $g_{-\epsilon}$ coincides almost everywhere with f but at x, it cannot be lower semi-computable by the preceding proposition.

Suppose g_ϵ is lower semi-continuous. Let α be a rational number such that $f(x) < \alpha < g_\epsilon(x)$. As g is lower semi-continuous, there is an ideal ball B containing x such that $g_\epsilon \geq \alpha$ on B. Let $B' \lhd B$ containing x, and $C' = X \setminus \overline{B}'$. As x is μ-Kurtz random, the full-measure open set $U = X \setminus \{x\}$ cannot be constructive. However, U is exactly $C' \cup f^{-1}(\alpha, +\infty]$: contradiction. □

3.2 Randomness on a computable probability space

When fixing a computable probability measure, the enumeration of randomness tests is a consequence of theorem 1.4.2.1 applied to the pseudo-computable enumerative lattice $\mathcal{C}(X, \overline{\mathbb{R}}^+)$.

Proposition 3.2.0.7. *Let (X, μ) be a computable probability space. Consider the pseudo-computable enumerative lattice $\mathcal{C}(X, \overline{\mathbb{R}}^+)$. The set of lower semi-continuous functions $f : X \to \overline{\mathbb{R}}^+$ which satisfy $\int f d\mu \leq 1$ is a constructive closed subset of $\mathcal{C}(X, \overline{\mathbb{R}}^+)$.*

Proof. $A = \{t : \int t d\mu \leq 1\}$ is closed. To a finite set $F_k \subset \mathbb{N}$ corresponds a finite supremum of step functions $f_k = \sup\{\mathrm{St}_{B_i}^{q_j} : \langle i,j\rangle \in F_k\}$. Define $\overline{f}_k = \sup\{\mathrm{St}_{\overline{B}_i}^{q_j} : \langle i,j\rangle \in F_k\}$.

One has the interesting property that if $f_k \lhd f_{k'}$ then $\int f_k d\mu = 0$ or $\int f_k d\mu < \int f_{k'} d\mu$. Indeed, there is $\epsilon > 0$ such that $f_k + \epsilon \leq f_{k'}$ on the set U where f_k is supported, so $\int f_k d\mu + \epsilon\mu(U) \leq \int_U f_{k'} d\mu \leq \int f_{k'} d\mu$. If $\int f_k d\mu > 0$ then $\mu(U) > 0$.

We claim that $A \cap \Uparrow f_k \neq \emptyset \iff \int \overline{f}_k d\mu < 1$. Indeed, if there is k' with $f_k \lhd f_{k'} \in A$, there is j such that $f_k \lhd f_j \lhd f_{k'}$. As $\overline{f}_k \leq f_{k'}$, $\int \overline{f}_k d\mu \leq \int f_j d\mu < \int f_{k'} d\mu \leq 1$. Conversely, suppose that $\int \overline{f}_k d\mu < 1$: as $\overline{f}_k$ is the point-wise infimum of $\{f_j : f_k \lhd f_j\}$, by the monotone convergence theorem $\int \overline{f}_k d\mu = \inf\{\int f_j d\mu : f_k \lhd f_j\}$ so there is $f_j \lhd f_k$ such that $\int f_j d\mu < 1$. $\square$

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 3.2.0.8. *Morphisms of computable probability spaces are defined on Martin-Löf, random points and preserve randomness.*

Proof. Let $F : D \subseteq X \to Y$ be a morphism. Every Kurtz random (and hence every ML-random, Schnorr-random) point is in D.

Let $t_\nu : Y \to \overline{\mathbb{R}}^+$ be the universal ν-test. The function $t_\nu \circ F : D \to \overline{\mathbb{R}}^+$ is lower semi-computable, i.e. it is a constructive element of $\mathcal{C}(D, \overline{\mathbb{R}}^+)$. It is the restriction to D of a constructive function $f \in \mathcal{C}(X, \overline{\mathbb{R}}^+)$. As $\mu(D) = 1$, $\int t_\nu \circ F d\mu$ is well defined and equals $\int f d\mu$. As F is measure-preserving, $\int t_\nu \circ F d\mu = \int t_\nu d\nu \leq 1$. Hence f is a μ-test. Let $x \in X$ be a μ-random point: as $x \in D$, $t_\nu(F(x)) = f(x) < +\infty$, so $F(x)$ is ν-random. $\square$

Corollary 3.2.0.3. *Let $(F,G) : (X,\mu) \rightleftarrows (Y,\nu)$ 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 3.2.0.4. *Let ρ be a binary representation on a computable probability space (X,μ). Each point having a μ_ρ-random expansion is μ-random and each μ-random point has a unique expansion, which is μ_ρ-random.*

On a computable probability space, Borel-Cantelli tests are equivalent to Schnorr random tests (this is why we called Schnorr random points those points which pass all Borel-Cantelli tests).

Definition 3.2.0.7. A ***Schnorr-test*** is a sequence of uniformly constructive open sets U_n such that $\mu(U_n) < 2^{-n}$ and $\mu(U_n)$ are uniformly computable real numbers.

Proposition 3.2.0.9 (Schnorr tests vs Borel-Cantelli tests)**.** *On a computable probability space, Schnorr-tests and Borel-Cantelli tests are equivalent. More precisely, for every Schnorr-test $(V_n)_n$, there is a BC test $(A_n)_n$ such that $\bigcap_n V_n \subseteq \limsup_n A_n$; for every BC test $(A_n)_n$, there is a Schnorr-test $(V_n)_n$ such that $\limsup_n A_n \subseteq \bigcap_n V_n$.*

Proof. Let (A_n) be a BC test, and $U_n = X \setminus A_n$. Expressing U_n as a constructive union of almost decidable balls, one can construct a sequence of sets $A'_n \subseteq U_n$ which are finite unions of almost decidable closed balls, such that $\mu(A'_n) > 1 - 2^{-n}$. Let $V_n = X \setminus A'_n$: $(V_n)_n$ is a Schnorr-test, and $\limsup_n A_n \subseteq \limsup_n V_n$. The sets $\bigcup_{k>n} V_k$ form a Schnorr-test.

Conversely, let $(V_n)_n$ be a Schnorr-test: if $V_k = \emptyset$ for some k, then take $A_n = X$ for all n. Otherwise, we express V_n as a union of almost decidable sets which are disjoint up to null sets. There is a total recursive function φ such that $V_n = \bigcup_i B^{\mu}_{\varphi(i,n)} = \bigcup_i \overline{B}^{\mu}_{\varphi(i,n)}$ (B^{μ}_k are almost decidable balls). Let us define $U_{\langle k,n\rangle} = \bigcup_{i\leq k} B^{\mu}_{\varphi(i,n)}$ and

$$A_{\langle 0,n\rangle} = \overline{B}^{\mu}_{\varphi(0,n)} \qquad A_{\langle k+1,n\rangle} = \overline{B}^{\mu}_{\varphi(k+1,n)} \setminus U_{\langle k,n\rangle}$$

One has $U_{\langle k,n\rangle} \subseteq A_{\langle 0,n\rangle} \cup A_{\langle 1,n\rangle} \cup \ldots \cup A_{\langle k,n\rangle}$ (easy by induction on k) and $V_n = \bigcup_k U_{\langle k,n\rangle} = \bigcup_k A_{\langle k,n\rangle}$.

All $A_{\langle k,n\rangle}$ are almost decidable sets so their measures are uniformly computable. If $k \neq k'$ then $A_{\langle k,n\rangle}$ and $A_{\langle k',n\rangle}$ are disjoint up to a null set, so $\sum_{k,n} \mu(A_{\langle k,n\rangle}) = \sum_n \mu(V_n)$ is computable. It follows that the sequence $\mu(A_i)$ is effectively summable. As A_i are uniformly Π_1 sets, (A_i) is a Borel-Cantelli test.

Now, $\bigcap_n V_n \subseteq \limsup_i A_i$. Indeed, if $x \in \bigcap_n V_n$ then for each n there is k such that $x \in A_{\langle k,n\rangle}$, so x is in infinitely many A_i's. $\square$

Combination of measures

We denote the set of μ-Martin-Löf random points by R_μ. We state simple observations on the decomposition of the set of random points induced by the decomposition of a probability measure. The same results hold for Schnorr and Kurtz random points.

Lemma 3.2.0.2. *Let μ_1, μ_2 be computable probability measures and $\alpha \in (0,1)$ a computable real number. Let $\mu = \alpha\mu_1 + (1-\alpha)\mu_2$. Let R_μ be the set of μ-Martin-Löf random points: $R_\mu = R_{\mu_1} \cup R_{\mu_2}$.*

Proof. $\alpha\mu_1 \leq \mu$ so for every μ-test t, αt is a μ_1-test. It implies that $R_{\mu_1} \subseteq R_\mu$. If t_1 is a μ_1-test and t_2 a μ_2-test, then $\min(t_1, t_2)$ is a μ-test and $\min(t_1(x), t_2(x)) < \infty \iff t_1(x) < \infty$ or $t_2(x) < \infty$. So $R_\mu \subseteq R_{\mu_1} \cup R_{\mu_2}$. $\square$

When μ is a probability measure on X and A is a subset of X with positive measure, the induced measure μ_A is defined by $\mu_A(B) = \mu(B|A) = \mu(B \cap A)/\mu(A)$.

Lemma 3.2.0.3. *Let μ be a computable measure and U be a constructive open set such that $\mu(U)$ is a computable real number. Let $F = X \setminus U$: then μ_U and μ_F are computable measures, and $R_\mu = R_{\mu_U} \uplus R_{\mu_F}$.*

Proof. Indeed, $\mu_U(V) = \mu(U \cap V)/\mu(U)$ and $\mu_F(V) = \mu(U \cup V)/\mu(U) - 1$.

$\mu = \alpha\mu_U + (1-\alpha)\mu_F$ where $\alpha = \mu(U)$, so $R_\mu = R_{\mu_U} \cup R_{\mu_F}$ by lemma 3.2.0.2. Moreover, $R_{\mu_U} \subseteq U$ as $\mu_U(U) = 1$, and $R_{\mu_F} \subseteq \mathrm{Supp}(\mu_F) \subseteq F$ as $\mu_F(F) = 1$. So $R_{\mu_U} \cap R_{\mu_F} = \emptyset$. $\square$

A characterization using Kolmogorov complexity ? The binary representation enables one to get a notion of Kolmogorov complexity of points in a computable metric space. The characterization of Martin-Löf randomness in terms of complexity directly follows. For points x which have a unique expansion ω, define:

$$K_n(x) = K(\omega_{0..n-1}) \text{ and } \Gamma_n(x) = \rho([\omega_{0..n-1}])$$

Corollary 3.2.0.5. *Let ρ be a binary representation on a computable probability space (X, μ). Then x is μ-Martin-Löf random if and only if there is c such that for all n:*

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

However, the meaning of this complexity is not clear and depends on the particular binary representation that is involved. On a computable metric space, it is possible to define the algorithmic complexity of x up to ϵ as the minimal complexity of an ideal ball of radius ϵ containing x, which is the local algorithmic version of the ϵ-entropy defined by Kolmogorov and Tikhomirov in [KT59], [KV61]. This was proposed by Galatolo in [Gal99], where a link is proved between this local algorithmic entropy and dimension.

On the Cantor space where ideal balls are cylinders, this approach has been intensively studied during the past ten years, defining constructive versions of Hausdorff, packing, box counting dimension and relating Kolmogorov complexity with these constructive dimensions (see for instance [May01], [Lut03], [Rei04], [Sta05]). It is possible to extend these ideas to computable metric spaces. Lacking time, we do not address this here; however, in the last section, we will apply these ideas to dynamical systems, in order to relate the algorithmic complexity of orbits to the topological entropy of the system.

Difficulties appear when trying to relate this algorithmic complexity to computable measures, and it is hardly possible to get a characterization of randomness using complexity, like the one given by theorem 3.1.1.1 on the Cantor space: the fact that the latter is totally disconnected is an essential feature.

3.2.1 Pseudo-random points

Here, (X, μ) is a computable probability space. Although computable points are generally not algorithmically random at all (unless the measure is concentrated on it), computable points may be random relatively to a particular probabilistic law.

Definition 3.2.1.1. Let T be a (Kurtz, Schnorr, Borel-Cantelli or Martin-Löf) randomness test. A point x is ***pseudo-random*** for T if x passes the test and is a computable point.

The existence of pseudo-random points is desirable if one wants to carry out reliable simulations of a probabilistic process on a computer. We briefly investigate this question from an abstract point of view: in particular, we do not wonder if such pseudo-random points can be computed in practice. We prove the following result:

Theorem 3.2.1.1. *Every Kurtz test admits a sequence of uniformly pseudo-random points which is dense in* $\mathrm{Supp}(\mu)$.

Every Borel-Cantelli test admits a sequence of uniformly pseudo-random points which is dense in $\mathrm{Supp}(\mu)$.

Proof. The proofs essentially use the computable Baire's theorem (theorem 1.6.1.3).

Of course, the first point is directly implied by the second one. Nevertheless, it can be directly proved in a simple manner: the support of μ is a constructive closed set ($U \cap \mathrm{Supp}(\mu) \neq \emptyset \iff \mu(U) > 0$) and hence a computable metric subspace (theorem 1.6.1.1);

every Kurtz test induces, in the subspace $\mathrm{Supp}(\mu)$, a dense constructive G_δ, to which the computable Baire's theorem can be applied.

By proposition 3.2.0.9, the second point is true for Borel-Cantelli tests if and only if it is true for Schnorr-tests. We prove it for a Schnorr test $(V_n)_n$. The restriction of μ to $X \setminus V_n$, defined by $\nu_n(A) = \mu(V_n \cap A)/\mu(V_n)$ is a computable measure (lemma 3.2.0.3) so again its support is a constructive closed set. By theorem 1.6.1.2 there is a computable sequence $(x^n_k)_k$ which is dense in $\mathrm{Supp}(\nu_n)$. Note that everything is uniform in n, so we can mix these sequences into a computable sequence $y_{\langle n,k\rangle} = x^n_k$, which is dense in the support of μ: indeed, as $\mu(\mathrm{Supp}(\nu_n)) = \mu(X \setminus V_n) \geq 1 - 2^{-n}$, $\bigcup_n \mathrm{Supp}(\nu_n)$ has μ-measure one so it is dense in $\mathrm{Supp}(\mu)$. □

We also present an alternative proof, which does not use Schnorr-tests.

Proof. Let $(A_n)_n$ be a Borel-Cantelli test. There is a computable non-increasing sequence of rational numbers $(a_n)_n$ which converges to 0, such that $\mu(\bigcup_{k\geq n} A_n) < a_n$. Let $U_n = X \setminus A_n$: U_n is a constructive open set, uniformly in n. Let B be an ideal ball of radius 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 such that $\mu(B) + \mu(\bigcap_{k\geq n_0} U_k) > 1$ (such an n_0 can be effectively found): 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. $\mathrm{diam}(V_i) \leq 2^{-i+1}$,
4. $\overline{V}_{i+1} \subseteq V_i$.

The last two conditions assure that $\bigcap_i V_i$ is a computable point (lemma 1.6.1.1), the second condition assures that this point lies in $\bigcap_k U_k$.

Suppose V_i and n_i have been constructed.

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

$$\mu(V_i \cap \bigcap_{n_i \leq k < m} U_k \cap B') > a_m. \tag{3.1}$$

Proof 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 $\mu(V_i \cap \bigcap_{k \geq n_i} U_k \cap B') > 0$. As a_m converges to 0 as m grows, there is $m > n_i$ such that $\mu(V_i \cap \bigcap_{k \geq n_i} U_k \cap B') > a_m$, which implies the assertion. □

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 a_m. Put $n_{i+1} = m$. Conditions 2., 3. and 4. directly follow from the construction, condition 1. follows from $\mu(V_{i+1}) > a_m > 1 - \mu(\bigcap_{k \geq m} U_k)$. □

Corollary 3.2.1.1. *Let f_n, f be almost computable random variables. If f_n converge effectively almost surely to f, then there is a sequence of uniformly computable points $(x_i)_i$ which is dense in* $\mathrm{Supp}(\mu)$*, such that $f_n(x_i) \to f(x_i)$.*

Proof. The convergence can be Borel-Cantelli tested (proposition 3.1.4.1), so we can apply theorem 3.2.1.1. □

Application: computable absolutely normal numbers

Theorem 3.2.1.1 can be applied to prove the existence of computable absolutely normal numbers, in an elementary way. We extended this to prove the existence of computable μ-typical points for a class of dynamical systems. This extension is presented in [Roj08] and in an article [GHR07b] that is currently submitted.

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 ([Bor09]), 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 1917 ([Sie17]), twenty years before the concept of computability was formalized. Its construction is quite complicated and is a priori unclear whether his number is computable or not. In [BF02] a recursive reformulation of Sierpinski's construction (equally complicated) was given, furnishing a computable absolutely normal number.

As an application of theorem 3.2.1.1 we give a simple proof that computable absolutely normal numbers are dense in $[0,1]$.

For $b \geq 2$ let D_b be the set of real numbers in $[0,1]$ which are not b-adic: it is a constructive dense G_δ with Lebesgue full measure. Let $w \in \{0,1,\dots,b-1\}^*$. For $n \geq 0$ and $x \in D_b$ define $f_n(x)$ to be the mean number of occurrences of w in the first n digits of its b-ary expansion ω:

$$f_n(x) = \frac{1}{n}\#\{i \leq n : \omega_{i..i+|w|-1} = w\}$$

f_n are uniformly computable on D_b. The fact that λ-almost every real $x \in [0,1]$ is normal in base b is expressed by the almost sure convergence of f_n to the constant function $f = b^{-|w|}$. The proof of this is a slight modification of the proof of the strong law of large numbers, which originally requires the independence of the random variables involved.

Here, f_n and f_p are independent if $|n-p| \geq |w|$. One can prove the following:

$$P\left[|f_n - f| \geq \epsilon\right] \leq \frac{2|w|}{\epsilon^2 n} \tag{3.2}$$

which only implies the effective convergence *in probability* of f_n to f. Furthermore, using the particular form of f_n (a mean of eventually independent random variables), it can be proved that $f_n(x) \to f(x)$ if and only if $f_{n^2}(x) \to f(x)$. The random variables f_{n^2} effectively converge almost surely to f, and this is uniform in b, w.

It follows that the convergence of f_n to f can be Borel-Cantelli tested, uniformly in b, w, so the simultaneous convergence of all $f_n^{b,w}$ to $f^{b,w}$ for every $b \geq 2, w \in \{0,\dots,b-1\}^*$ can be Borel-Cantelli tested. Hence, there is a dense computable sequence of real numbers which are absolutely normal.

Proof of (3.2). If X is a random variable, $\mathbf{E}X$ is the expectation of X, $\mathbf{V}X = E(X^2) - E(X)^2$ its variance. Let $X_i(x) = 1$ if the b-expansion of x between ranks i and $i+|w|-1$ is w,

$X_i(x) = 0$ otherwise. $\mathbf{E}X_i = \mathbf{E}X_i^2 = \beta := b^{-|w|}$ and X_i, X_j are independent if $|i-j| \geq |w|$.

$$\begin{aligned}
\sum_{i<j<n} \mathbf{E}X_iX_j &= \sum_{i=0}^{n-2}\sum_{j=i+1}^{n-1} \mathbf{E}X_iX_j \\
&\leq \sum_{i=0}^{n-2}\sum_{j=i+1}^{i+|w|-1} \mathbf{E}X_iX_j + \sum_{i=0}^{n-2}\sum_{j=i+|w|}^{n-1} \mathbf{E}X_iX_j \\
&= \sum_{i=0}^{n-2}\sum_{j=1}^{|w|-1} \mathbf{E}X_0X_j + \sum_{i=0}^{n-|w|-1}\sum_{j=|w|}^{n-i-1} \beta^2 \\
&= (n-1)\sum_{j=1}^{|w|-1} \mathbf{E}X_0X_j + \frac{(n-|w|)(n-|w|+1)}{2}\beta^2 \\
&\leq (n-1)(|w|-1) + \frac{(n-|w|)(n-|w|+1)}{2}\beta^2
\end{aligned}$$

Let $S_n = X_0 + \ldots + X_{n-1}$.

$$\begin{aligned}
\mathbf{V}S_n &= \sum_{i<n} \mathbf{E}X_i^2 + 2\sum_{i<j<n} \mathbf{E}X_iX_j - (\mathbf{E}S_n)^2 \\
&= n\beta + 2\sum_{i<j<n} \mathbf{E}X_iX_j - (n\beta)^2 \\
&\leq (\beta + 2|w| - 2 - (2|w|-1)\beta^2)n + (|w|-1)(|w|\beta^2 - 2) \leq 2|w|n
\end{aligned}$$

By Tchebychev inequality, $P[|f_n - f| \geq \epsilon] \leq \mathbf{V}f_n/\epsilon^2$. As $f_n = S_n/n$, (3.2) follows. $\square$

Chapter 4

Algorithmic ergodic theory

In a classical world, randomness is understood as deterministic unpredictability. The world evolves deterministically, and our limited knowledge of the present state of nature prevent us to predict what will happen in the future, so everything happens as if the evolution had a random component. The model of determinism is the theory of dynamical systems, while probability theory is a model of pure randomness. The goal of ergodic theory is to look at dynamical systems from a probabilistic point of view. It talks about global properties of a system, or generic behavior, instead of prediction of orbits.

The algorithmic theory of randomness, which is among others an attempt to improve probability theory giving a notion of random object, is then to be applied to ergodic theory. Part of this chapter and the following are gathered in an article [GHR07c] which is following the submission process.

4.1 Background

We recall the bases of ergodic theory. More details can be found in standard references [Bil65], [Wal82], [Pet83], [HK95], [HK02].

Let (X, d) be a metric space: the topology generates the Borel σ-field, which makes X a measurable space. Let $T : X \to X$ be a measurable map. A probability measure μ on X is invariant under T if for all Borel set A, $\mu(A) = \mu(T^{-1}A)$, that is μ is a fixed point of the operator $\mu \mapsto \mu_*$ defined by $\mu_* = \mu T^{-1}$. We also say that T preserves μ, or that T is an endomorphism of the probability space (X, μ). Given such an endomorphism, a Borel set A is T-invariant if $T^{-1}A = A$ (mod 0), i.e. the symmetric difference $A \Delta T^{-1}A$

has μ-measure 0. The system (X, μ, T) (or the measure μ) is said to be ***ergodic*** if every T-invariant set has measure 0 or 1: the system has no proper subsystem (where proper means "of non-trivial measure"). Another characterization is that every observable $f \in L^1(X, \mu)$ which is invariant under T, i.e. satisfying $f = f \circ T$ almost everywhere, is constant almost everywhere (think of the particular case when f is the characteristic function of some Borel set A).

Poincaré recurrence theorem Let T be an endomorphism of a probability space (X, μ). If A is a measurable set with positive measure, then for μ-almost every point $x \in A$, there is $i \geq 1$ such that $T^i x \in A$. In other words, $\mu(A \cap \bigcup_{i \geq 1} T^{-i}A) = \mu(A)$. From this it is easy to derive that the orbit of μ-almost every point $x \in A$ comes back to A infinitely often.

Birkhoff ergodic theorem Let T be an endomorphism of a probability space (X, μ). The Birkhoff ergodic theorem states that for any $f \in L^1(X, \mu)$ and for μ-almost every $x \in X$, the following limit exists:

$$f^*(x) := \lim_{n \to \infty} \frac{1}{n} \sum_{i=0}^{n-1} f \circ T^i(x), \tag{4.1}$$

Moreover, $f^* \in L^1(X, \mu)$, f^* is T-invariant and $\int f^* d\mu = \int f d\mu$. If the system is moreover ergodic, it follows that $f^* = \int f d\mu$ almost everywhere.

In general there is no point x for which the limit exists for every $f \in L^1(X, \mu)$: for each x one can construct a pathological f making the Birkhoff mean oscillate. Nevertheless, for any countable family $\{f_i\}$ of such functions, there is a full-measure set of points for which the convergence holds for each f_i. When the system is ergodic, defining:

$$\mu_n^x = \frac{1}{n} \sum_{i=0}^{n-1} \delta_{T^i x}$$

the convergence of the Birkhoff mean (4.1) can be reformulated as $\mu_n^x f \to \mu f$. When X is a separable metric space, it is possible to find a countable family $\{f_i\}$ such that the weak convergence of μ_n^x to μ is characterized by the convergence $\mu_n^x f_i \to \mu f_i$ for every f_i in this family (see proposition 2.1.1.1).

Definition 4.1.0.2 (μ-typical points)**.** Let (X, d) be a separable metric space, μ a probability measure and T an endomorphism of (X, μ). A point $x \in X$ is μ-typical with respect to T if

$$\lim_{n \to \infty} \frac{1}{n} \sum_{i=0}^{n-1} f \circ T^i(x) = \int f d\mu$$

for all continuous bounded real function f. Equivalently, x is μ-typical if μ_n^x converges weakly to μ.

From the discussion above, the set of μ-typical points for T has measure one when the system is ergodic. In giving full weight to the set of μ-typical points, the measure μ selects those orbits whose statistics reproduce μ.

Symbolic model Let T be an endomorphism of a (Borel) probability space (X, μ). A classical idea is to simplify the dynamics watching it through a discrete filter. A finite measurable partition is a finite collection $\xi = \{C_1, \dots, C_k\}$ of pairwise disjoint Borel sets, called cells or atoms, such that $\mu(\cup_i C_i) = 1$. To (X, μ, T) is then associated a symbolic dynamical system, in the following way. Let $\Sigma^{\mathbb{N}}$ be the set of infinite sequences of elements of $\Sigma = \{1, \dots, k\}$. To a point $x \in X$ corresponds an infinite sequence $\omega = (\omega_i)_{i\in\mathbb{N}} = \phi_\xi(x) \in \Sigma^{\mathbb{N}}$ defined by:

$$\omega_j = i \iff T^j(x) \in C_i$$

The image X_ξ of X by ϕ_ξ is a subset of $\Sigma^{\mathbb{N}}$ which is invariant under the *shift* transformation $\sigma : \Sigma^{\mathbb{N}} \to \Sigma^{\mathbb{N}}$ defined by $\sigma(\omega)_i = \omega_{i+1}$ for all i. The measure μ induces a probability measure $\mu_\xi = \mu\phi_\xi^{-1}$ on X_ξ, which is invariant under σ. The system (X_ξ, μ_ξ, σ) is then called the *symbolic model* associated to (X, μ, T, ξ).

Symbolic models are of great importance when dealing with information theory. They are mainly used to see the dynamical system as a source of strings in order to investigate transmission problems as compression, and relating them to global properties of the system.

4.2 Ergodic theory on computable probability spaces

4.2.1 Effective symbolic dynamics

The requirement of ξ being measurable makes the symbolic model appropriate from the measure-theoretic point of view. On a computable probability space, symbolic models shall be moreover constructive.

Definition 4.2.1.1. Let T be an endomorphism of a computable probability space (X, μ) and $\xi = \{C_1 \dots, C_k\}$ a finite measurable partition. The associated symbolic model (X_ξ, μ_ξ, σ)

is said to be ***an effective symbolic model*** if the map $\phi_\xi : X \to \{1,\dots,k\}^{\mathbb{N}}$ is a morphism of computable probability spaces (here the space $\{1,\dots,k\}^{\mathbb{N}}$ is endowed with the standard computable structure).

We denote by $\xi(x)$ the atom containing x (if there is one). Observe that ϕ_ξ is constructively continuous on its domain only if the atoms are constructive open sets (in the domain):

Definition 4.2.1.2 (Computable partitions)**.** A measurable partition ξ is said to be a ***computable partition*** if its atoms are constructive open sets.

Conversely:

Proposition 4.2.1.1. *Let (X,μ) be a computable probability space and $T : X \to X$ an endomorphism. If $\xi = \{C_1 \dots, C_k\}$ is a finite computable partition, then the associated symbolic model is effective.*

Proof. Define the full-measure constructive G_δ:

$$D = \bigcap_{n\in\mathbb{N}} T^{-n}(C_1 \cup \ldots \cup C_k)$$

The sets $\phi_\xi^{-1}([i_0,\dots,i_n]) = C_{i_0} \cap T^{-1}C_{i_1} \cap \ldots \cap T^{-n}C_{i_n}$ are uniformly constructive open in D, so ϕ_ξ is constructively continuous on D.

□

The results obtained in section 2.2 directly give the following:

Corollary 4.2.1.1. *On every computable probability space, there exists a family of uniformly computable partitions which generates the Borel σ-field.*

Proof. From the family of uniformly almost decidable balls $\{B_k^\mu\}$ provided by theorem 2.2.1.2, we consider the computable partitions $\xi_k = \{B_k^\mu, X \setminus \overline{B}_k^\mu\}$: as the almost decidable balls form a basis of the topology, the σ-field generated by the P_k is the Borel σ-field. □

4.2.2 Dynamics of random points

In this section we study two examples of probabilistic theorems from ergodic theory and give their version for algorithmic random points: recurrence and statistical typicality.

Recurrence

Definition 4.2.2.1. Let X be a metric space. A point $x \in X$ is said to be ***recurrent*** for a transformation $T : X \to X$, if $\liminf_{n\to\infty} d(x, T^n x) = 0$.

The version of the recurrence theorem for random points can be made very short, using the classical theorem instead of making its proof constructive.

Proposition 4.2.2.1 (Random points are recurrent)**.** *Let (X, μ) be a computable probability space. If x is μ-Kurtz random, then it is recurrent with respect to* every *endomorphism T on (X, μ).*

Proof. Let x be μ-Kurtz random and B an almost decidable neighborhood of x. As x is μ-Kurtz random, one necessarily has $\mu(B) > 0$. The measure $\mu_B(.) = \mu(.|B)$ is computable and x is also μ_B-Kurtz random by lemma 3.2.0.3. Let T be an endomorphism: there is a constructive open set U such that:

$$\bigcup_{n\geq 1} T^{-n} B = U \cap D$$

where D is the domain of computability of T. By the Poincaré recurrence theorem, this set has full measure for μ_B, so x, which is μ_B-Kurtz random, belongs to U. As x also belongs to D, there is $n \geq 1$ such that $T^n x \in B$. As T preserves μ-randomness, $T^n x$ is μ-Kurtz random, so the orbit of x visits B infinitely many times. And this holds for every almost decidable B neighborhood of x. $\square$

It implies that for every open set U of positive measure, every μ-Kurtz random point which belongs to U comes back infinitely often to U.

Statistical typicality This problem has already been studied by V'yugin ([V'y97]) on the Cantor space and for computable observables. Using effective symbolic dynamics, it is possible to extend this result in a straightforward way to computable probability spaces.

We will use the particular case of V'yugin's theorem:

Lemma 4.2.2.1. *Let μ be a computable shift-invariant ergodic measure on the Cantor space $\{0,1\}^\omega$. Then for each μ-Martin-Löf random sequence ω:*

$$\lim_n \frac{1}{n} \sum_{i=0}^{n-1} \omega_i = \mu([1]) \tag{4.2}$$

We are now able to prove:

Theorem 4.2.2.1 (Random points are typical)**.** *Let (X, μ) be a computable probability space. Then each μ-Martin-Löf random point x is μ-typical for every ergodic endomorphism T.*

Proof. Let f_A be the characteristic function of the set A. First, let us show that if A is an almost decidable set then for all μ-random point x:

$$\lim_n \frac{1}{n} \sum_{i=0}^{n} f_A \circ T^i(x) = \mu(A) \tag{4.3}$$

Indeed, consider the *computable partition* defined by $\mathcal{P} := \{U, V\}$ with U and V as in definition 2.2.1.2 and the associated symbolic model $(X_{\mathcal{P}}, \sigma, \mu_{\mathcal{P}})$. By proposition 4.2.1.1, $\phi_{\mathcal{P}}(x)$ is a well defined $\mu_{\mathcal{P}}$-random infinite sequence, so lemma 4.2.2.1 applies and gives the result.

Now we apply proposition 2.1.1.1to prove that $\mu_n = \frac{1}{n}\sum_{i<n}\delta_{T^i x}$ converges weakly to μ: the countable family of almost decidable sets is a basis of the topology, closed under finite unions, and $\mu_n(A) \to \mu(A)$ for every almost decidable set A. $\square$

It means that for any bounded continuous function $f : X \to \mathbb{R}$ and any μ-Martin-Löf random point x,

$$\lim_n \frac{1}{n} \sum_{i=0}^{n} f \circ T^i(x) = \int f d\mu$$

with no computability assumption required on f.

Martin-Löf randomness, Schnorr randomness and typicality Martin-Löf randomness is then strong enough to assure the convergence of the Birkhoff mean. Several questions remain open: is Martin-Löf randomness too strong for this purpose? Is Schnorr randomness strong enough? In [GHR08] we show that Schnorr randomness assures typicality for a particular class of dynamical systems (namely mixing systems) and that it is tight: if a point is not Schnorr random, there is a mixing system for which it is not typical (see [Roj08] for a complete presentation).

In [V'y98] V'yugin constructs a computable shift-invariant measure μ for which the convergence of the Birkhoff mean is not effective: hence proposition 3.1.4.1 cannot be applied in order to prove that the convergence holds for μ-Schnorr random points. Actually, the constructed measure μ is a combination $\sum_i \alpha_i\mu_i$ of computable ergodic measures for which the shift is mixing. The set of μ-Schnorr random points is then the union of the sets of μ_i-Schnorr random points (generalization of lemma 3.2.0.2), so the convergence holds for μ-Schnorr random points.

It would be worth investigating the following problem: is there a computable shift-invariant ergodic measure for which the convergence is not effective? If there is such a measure μ, are there μ-Schnorr random points which are not μ-typical?

4.3 When the measure is not computable

Let X be a compact metric space and $T : X \to X$ a continuous map. The Krylov-Bogoliubov theorem states that the set $\mathcal{M}_T(X)$ of T-invariant Borel probability measures is non-empty. It can also be shown that it is a compact and convex subset of $\mathcal{M}(X)$, whose extremal points are the ergodic T-invariant measures.

When X is a (still compact) computable metric space and T is computable, it is not known yet if there exist computable T-invariant probability measures. It can be shown that the complement of $\mathcal{M}_T(X)$ is a constructive open subset of $\mathcal{M}(X)$. In particular, when X is compact in a constructive way, so are $\mathcal{M}(X)$ and $\mathcal{M}_T(X)$. In this context, the only invariant measure of a uniquely ergodic computable map is always computable.

But in general, the computability of invariant measures is an open issue. In [GHR07b] and [GHR07a] we solve the problem for classes of dynamical systems (namely mixing systems) for which we prove the existence of a computable invariant measure. This is developed in [Roj08].

But in general, the computability of invariant measures is an open issue. Another problem which should be investigated is the ergodic decomposition of invariant measures: ergodic measures are the extremal points of the convex set $\mathcal{M}_T(X)$, so every invariant measure can be decomposed as a mixture of ergodic measures (which corresponds to a decomposition of a system into “minimal” subsystems). If an invariant measure is computable, is this decomposition also computable ?

If a system has few computable invariant measures, what has been developed in this chapter cannot be applied. We show how V’yugin’s result can be extended to non-computable invariant measures.

Theorem 4.3.0.2 (Birkhoff ergodic theorem for random points)**.** *Let X be a computable metric* *space and μ be a probability measure on X. Let $T : X \to X$ be a measure-preserving map and $f : X \to \overline{\mathbb{R}}$ an integrable function. Suppose T and f are computable on a full-measure constructive G_δ.*

1. *For every μ-random point x, the following limit exists:*

$$f^*(x) := \lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n-1} f \circ T^i x$$

2. *If μ is ergodic, then $f^*(x) = \int f d\mu$ for every μ-random point x.*

V'yugin's proof is based on the constructive proof of Birkhoff's theorem by Bishop, defining a function which measures the number of oscillations of the Birkhoff mean. Let us outline his proof of the first point.

Outline of V'yugin's proof. Let $f_n = \frac{1}{n}\sum_{i<n} f \circ T^i$. For rational numbers $\alpha < \beta$, define

$$\sigma(\omega, \alpha, \beta) := \sup\left\{N : \exists n_1 < n_2 < \ldots n_{2N} \text{ with } f_{n_{2k-1}}(x) < \alpha, f_{n_{2k}}(x) > \beta\right\}$$

which is infinite when $\liminf_n f_n(\omega) < \alpha < \beta < \limsup_n f_n(\omega)$. Using the invariance of the measure, he proves that $\int \sigma(\omega, \alpha, \beta) d\mu$ is finite. If f and T are computable, then $\sigma(\omega, \alpha, \beta)$ is lower semi-computable, and hence is a test (up to a multiplicative constant).

It follows that $\sigma(\omega, \alpha, \beta) < \infty$ for every μ-Martin-Löf random sequence. As $\alpha < \beta$ are arbitrary, $f_n(x)$ converges for all μ-Martin-Löf random point x. $\square$

Let us now remark some facts:

1. everything is defined as well on a computable metric space X,

2. the function σ does not depend on μ, and is a μ-test for every invariant measure μ, even if μ is not computable,

3. it is not necessary to assume that f and T are computable *everywhere*, but on a constructive full-measure G_δ instead. Indeed, from this there is a constructive G_δ of full measure, D where all f_n are computable: $\sigma(x, \alpha, \beta)$ is then lower semi-computable on D and can be extended to a lower semi-computable function t on all X: t is then a μ-test, which coincides with $\sigma(x, \alpha, \beta)$ on D.

These remarks allow to obtain the first result: as every μ-Martin-Löf random point x is also μ-Kurtz random, x belongs to D so $t(x) = \sigma(x, \alpha, \beta) < \infty$ and hence $f_n(x)$ converges (α, β are arbitrary).

The second result cannot be so simply obtained: when μ is ergodic, the test used to prove that $f^*(x) = \int f d\mu$ for each μ-random point depends on μ. Fortunately, we can use proposition 3.1.4.3 to conclude: as f_n converges almost surely to the constant $c = \int f d\mu$, and f_n are uniformly almost computable, $\liminf_n f_n(x) \leq \int f d\mu \leq \limsup_n f_n(x)$ for all μ-Kurtz random point x. As every μ-Martin-Löf random point x is μ-Kurtz random and $f_n(x)$ converges by the first result, the limit must be $\int f d\mu$.

Chapter 5

Entropy and orbit complexity

In [Bru83], Brudno defined an algorithmic complexity $K(x, T)$ for the orbits of a continuous dynamical system on a compact space, and proved the following results:

Theorem (Brudno)**.** *Let X be a compact topological space and $T : X \to X$ a continuous map.*

1. *For any ergodic probability measure μ the equality $K(x, T) = h_\mu(T)$ holds for μ-almost all $x \in X$.*
2. *For all $x \in X$, $K(x, T) \leq h(T)$.*

where $h_\mu(T)$ is the Kolmogorov-Sinaï entropy of (X, T) with respect to μ and $h(T)$ is the topological entropy of T. This result seems miraculous as no computability assumption is required on the space or on the transformation T. Actually, this miracle lies in the compactness of the space, which makes it finite when observations are made with finite precision (open covers of the space can be reduced to *finite* open covers). Indeed, when the space is not compact, it is possible to construct systems for which the algorithmic complexity of orbits is correlated in no way to their dynamical complexity (see [WB96]). In [Gal00], Galatolo generalized Brudno's definition to non-compact spaces endowed with a computable structure (computable metric spaces), and requiring the transformation to be computable. He shows that his definition coincides with Brudno's one in the compact case.

Brudno and Galatolo's definitions are actually inspired from the topological approach of dynamical systems. We show that the measure-theoretic setting provides a natural notion of algorithmic complexity $\mathcal{K}_\mu(x, T)$ defined almost everywhere (in particular on Kurtz random points) and for which the first result in Brudno's theorem comes easily. We go further in showing:

Theorem (5.1.4.2). *Let T be an ergodic endomorphism of the computable probability space (X, μ),*

$$\mathcal{K}_\mu(x, T) = h_\mu(T) \quad \textit{for all ML-random point } x.$$

In the topological context, we then use Galatolo's definition of algorithmic complexity of orbits $\overline{\mathcal{K}}(x, T)$, and strengthen the second part of Brudno's theorem, showing:

Theorem (5.2.3.1). *Let T be a computable map on a compact computable metric space X,*

$$\sup_{x \in X} \overline{\mathcal{K}}(x, T) = h(T)$$

Remark that this was already implied by Brudno's theorem, using the variational principle: $h(T) = \sup\{h_\mu(T) : \mu\ T\text{-invariant}\}$. Nevertheless, our proof uses purely topological and algorithmic arguments and no measures. In particular, it does not use the variational principle, and can be thought as an alternative proof of it.

We finally prove that the two notions of algorithmic complexity of orbits coincide on Martin-Löf random points:

Theorem (5.3.0.3). *Let T be an ergodic endomorphism of the computable probability space (X, μ), where X is compact,*

$$\mathcal{K}_\mu(x, T) = \overline{\mathcal{K}}(x, T) \quad \textit{for all ML-random point } x.$$

5.1 The measure point of view

Suppose discrete objects (symbolic strings for instance) are produced by some source. The tendency of the source toward producing such objects more than others can be modeled by a probability distribution, which gives more information than the crude set of possible outcomes. The Shannon entropy of the probabilistic source measures the degree of uncertainty that lasts when taking the probability distribution into account.

Any ergodic dynamical system (X, T, μ) can be seen as a source of outputs. Kolmogorov and Sinaï adapted Shannon's theory to dynamical systems in order to measure the degree of unpredictability or chaoticity of an ergodic system. The first step consists in discretizing the space X using finite partitions. Let $\xi = \{C_1, \ldots, C_n\}$ be a finite measurable partition of X. Then let $T^{-1}\xi$ be the partition whose atoms are the pre-images $T^{-1}C_i$. Then let

$$\xi_n = \xi \vee T^{-1}\xi \vee T^{-2}\xi \vee \ldots \vee T^{-(n-1)}\xi$$

be the partition given by the sets of the form

$$C_{i_0} \cap T^{-1}C_{i_1} \cap \ldots \cap T^{-(n-1)}C_{i_{n-1}},$$

varying C_{i_j} among all the atoms of ξ. Knowing which atom ξ_n a point x belongs to comes to knowing which atoms of the partition ξ the orbit of x visits up to time $n-1$.

The measure-theoretical entropy of the system w.r.t the partition ξ can then be thought as the rate (per time unit) of gained information (or removed uncertainty) when observations of the type "$T^n(x) \in C_i$" are performed. This is of great importance when classifying dynamical systems: it is a measure-theoretical invariant, which enables one to distinguish non-isomorphic systems.

We briefly recall the definition. For more details, we refer the reader to [Bil65], [Wal82], [Pet83], [HK95].

5.1.1 Entropy with Shannon information

Given a partition ξ and a point x, $\xi(x)$ denotes the atom of the partition x belongs to. Let us consider the ***Shannon information function*** relative to the partition ξ_n (the information which is gained by observing that $x \in \xi_n(x)$),

$$I_\mu(x|\xi_n) := -\log \mu(\xi_n(x))$$

and its mean, the entropy of the partition ξ_n,

$$H_\mu(\xi_n) := \int_X I_\mu(.|\xi_n)d\mu = \sum_{C\in\xi_n} -\mu(C)\log\mu(C)$$

The ***measure-theoretical*** or ***Kolmogorov-Sinaï entropy*** of T relative to the partition ξ is defined as:

$$h_\mu(T,\xi) = \lim_{n\to\infty} \frac{1}{n} H_\mu(\xi_n).$$

(which exists and is an infimum, since the sequence $H_\mu(\xi_n)_n$ is sub-additive). With the Shannon information function, it is possible to define a kind of point-wise notion of entropy with respect to a partition ξ:

$$\limsup_n \frac{1}{n} I_\mu(x|\xi_n).$$

This local entropy is related to the global entropy of the system by the celebrated Shannon-McMillan-Breiman theorem:

Theorem (Shannon-McMillan-Breiman)**.** *Let T be an ergodic endomorphism of the probability space $(X, \mathscr{B}, \mu)$ and ξ a finite measurable partition. Then for μ-almost every x,*

$$\lim_{n\to\infty} \frac{1}{n} I_\mu(x|\xi_n) = h_\mu(T, \xi). \tag{5.1}$$

The convergence also holds in $L^1(X, \mathscr{B}, \mu)$.

Now we suppress the partition-dependency: the ***Kolmogorov-Sinaï entropy*** of (X, T, μ) is

$$h_\mu(T) := \sup\{h_\mu(T, \xi) : \xi \text{ finite measurable partition}\}$$

We recall the following two results that we will need later. The first proposition follows directly from the definitions.

Proposition 5.1.1.1. *If $(\Sigma^{\mathbb{N}}, \mu_\xi, \sigma)$ is the symbolic model associated to (X, μ, T, ξ) then $h_\mu(T, \xi) = h_{\mu_\xi}(\sigma)$.*

The next proposition is taken from [Pet83]:

Proposition 5.1.1.2. *If $(\xi_i)_{i\in\mathbb{N}}$ is a family of finite measurable partitions which generates the Borel σ-field up to sets of measure 0, then $h_\mu(T) = \sup_i h_\mu(T, \xi_0 \vee ... \vee \xi_i)$.*

5.1.2 Entropy with Kolmogorov information

In this section, T is an endomorphism of the computable probability space (X, μ) and $\xi = \{C_1, \dots, C_k\}$ is a computable partition. Let $(\Sigma^{\mathbb{N}}, \mu_\xi, \sigma)$ be the effective symbolic model of (X, μ, T, ξ) where $\Sigma = \{1, \dots, k\}$ (see section 4.2.1).

Kolmogorov introduced algorithmic complexity as a quantity of information, on the same level as Shannon information. When the measure, the transformation and the partition are computable, it makes sense to define the algorithmic equivalents of the notions defined above. It turns out that the two points of view are strongly related.

An atom C of the partition ξ_n can then be seen as a word of length n on the alphabet Σ, which allows one to consider its Kolmogorov complexity $K(C)$. For those points whose iterates are covered by ξ (they form a constructive dense G_δ of full measure), we define the ***Kolmogorov information function*** relative to the partition ξ_n:

$$\mathcal{I}(x|\xi_n) := K(\xi_n(x))$$

which is independent of μ (this was originally defined by Brudno, for a not necessarily computable partition). We then define the ***algorithmic entropy*** of the partition ξ_n as the mean of $\mathcal{I}$:

$$\mathcal{H}_\mu(\xi_n) := \int_X \mathcal{I}(.|\xi_n)d\mu = \sum_{C\in\xi_n} \mu(C)K(C).$$

We also define a local notion of algorithmic entropy, which we call symbolic orbit complexity:

Definition 5.1.2.1 (Symbolic orbit complexity)**.** Let T be an endomorphism of the computable probability space (X, μ). For any finite computable partition ξ, we define $\mathcal{K}_\mu(x, T|\xi) := \limsup_n \frac{1}{n}\mathcal{I}(x|\xi_n)$. Then,

$$\mathcal{K}_\mu(x, T) := \sup\{\mathcal{K}_\mu(x, T|\xi) : \xi \text{ computable partition}\}$$

As there are only countably many computable partitions, $\mathcal{K}_\mu(x, T)$ is defined almost everywhere (at least on Kurtz random points). The quantity $\mathcal{K}_\mu(x, T|\xi)$ was introduced by Brudno in [Bru83] without any computability restriction on the space, the measure nor the transformation. He proved:

Theorem 5.1.2.1 (Brudno)**.** *$\mathcal{K}_\mu(x, T|\xi) = h_\mu(T, \xi)$ for μ-almost every point.*

Taking the supremum of $\mathcal{K}_\mu(x, T|\xi)$ over all – not necessarily computable – finite partitions ξ generally gives an infinite quantity, that is why Brudno did not go further (he did not have a computable structure at his disposal), and proposed a topological definition using open covers instead of partitions.

As we now show, the hypothesis of definition 5.1.2.1 enables one to derive Brudno's theorem in a rather simple manner.

5.1.3 Equivalence

The theory of randomness and Kolmogorov complexity on the space of symbolic sequences provides powerful results (theorem 3.1.1.1 and proposition 3.1.1.1) which enable us to relate the algorithmic entropies $\mathcal{I}_\mu$ and $\mathcal{H}_\mu$ to the Shannon entropies I_μ and H_μ (inequalities (5.3), (5.5)). We recall these two results: if $\Sigma^{\mathbb{N}}$ is endowed with a computable probability measure ν, then for all $\omega \in \Sigma^{\mathbb{N}}$,

$$-\log \nu[\omega_{0..n-1}] - d_\nu(\omega) \quad \leq \quad K(\omega_{0..n-1}) \quad \overset{+}{<} \quad -\log \nu[\omega_{0..n-1}] + K(n) \tag{5.2}$$

where d_ν is the deficiency of randomness, which satisfies $\int_{\Sigma^{\mathbb{N}}} d_\nu d\nu < 1$ and is finite exactly on Martin-Löf random sequences (the constant in $\overset{+}{<}$ does not depend on ω and n).

Equivalence between local entropies Applying (5.2) to $\nu = \mu_\xi$ directly gives:

$$I_\mu(.|\xi_n) - d_\mu \circ \phi_\xi \quad \leq \quad \mathcal{I}(.|\xi_n) \quad \overset{+}{<} \quad I_\mu(.|\xi_n) + K(n) \tag{5.3}$$

where it is defined (almost everywhere, at least on Kurtz random points). Every μ-Martin-Löf random point x is mapped by ϕ_ξ on a μ_ξ-Martin-Löf random sequence (see proposition 3.2.0.8), whose randomness deficiency is finite. It then follows that the local entropies using Shannon information and Kolmogorov information coincide on μ-random points:

$$\mathcal{K}_\mu(x, T|\xi) = \limsup_n \frac{1}{n} I(x|\xi_n) \quad \text{for every } \mu\text{-Martin-Löf random point } x \tag{5.4}$$

This equality together with the Shannon-McMillan-Breiman theorem (5.1) give directly Brudno's theorem (theorem 5.1.2.1).

Equivalence between global entropies Now, the Kolmogorov-Sinaï entropy, originally expressed using Shannon entropy, can be expressed using algorithmic entropy. Taking the mean in (5.3), one obtains:

$$H_\mu(\xi_n) - 1 \quad \leq \quad \mathcal{H}_\mu(\xi_n) \quad \overset{+}{<} \quad H_\mu(\xi_n) + K(n) \tag{5.5}$$

So,

$$h_\mu(T|\xi) = \lim_n \frac{H_\mu(\xi_n)}{n} = \lim_n \frac{\mathcal{H}_\mu(\xi_n)}{n}$$

As the collection of computable partitions is generating (see corollary 4.2.1.1), the Kolmogorov-Sinaï entropy of (X, μ, T) can be characterized by:

$$h_\mu(T) = \sup \left\{ \lim_n \frac{\mathcal{H}_\mu(\xi_n)}{n} : \xi \text{ finite computable partition} \right\}.$$

It then follows that $\mathcal{K}_\mu(x, T) = h_\mu(T)$ for μ-almost every x. We now strengthen this, proving that it holds for all Martin-Löf random points.

5.1.4 Symbolic orbit complexity of random points

On the Cantor space, V'yugin ([V'y97]) and later Nakamura ([Nak05]) proved a slightly weaker version of the Shannon-McMillan-Breiman for Martin-Löf random sequences. In particular, we will use:

Theorem 5.1.4.1 (V'yugin)**.** *Let μ be a computable shift-invariant ergodic measure on $\Sigma^{\mathbb{N}}$. Then, for any μ-Martin-Löf random sequence ω,*

$$\limsup_{n\to\infty} -\frac{1}{n}\log \mu([\omega_{0..n-1}]) = h_\mu(\sigma).$$

Note that it is not known yet if the limit exists for all random sequences.

Using effective symbolic models, this can be easily extended to any computable probability space.

Corollary 5.1.4.1 (Shannon-McMillan-Breiman for random points)**.** *Let T be an ergodic endomorphism of the computable probability space (X,μ), and ξ a computable partition. For every μ-Martin-Löf random point x,*

$$\limsup_{n\to\infty} -\frac{1}{n}\log \mu(\xi_n(x)) = h_\mu(T,\xi).$$

Proof. Since ξ is computable, the symbolic model (X_ξ,μ_ξ,σ) is effective. Every μ-Martin-Löf random point x is mapped by proposition 3.2.0.8 to a μ_ξ-Martin-Löf random sequence ω, for which the preceding theorem holds. Using the facts that $\mu(\xi_n(x)) = \mu_\xi([\omega_{0..n-1}])$ and $h_\mu(T,\xi) = h_{\mu_\xi}(\sigma)$ allows to conclude. □

Finally, this implies our first announced result:

Theorem 5.1.4.2. *Let T be an ergodic endomorphism of the computable probability space (X,μ). For every μ-Martin-Löf random point x:*

$$\mathcal{K}_\mu(x,T) = h_\mu(T).$$

Proof. We use equality (5.4): for every random point x, $\mathcal{K}_\mu(x,T|\xi) = \limsup_n \frac{1}{n} I_\mu(x|\xi_n)$ which equals $h_\mu(T,\xi)$ by the preceding result. Since the collection of all computable partitions generates the Borel σ-field (corollary 4.2.1.1), $\sup\{h_\mu(T,\xi) : \xi \text{ computable partition}\} = h_\mu(T)$ (see proposition 5.1.1.2). □

5.2 The topological point of view

Let X be a compact metric space and $T : X \to X$ a continuous map. The topological entropy of the system (X, T) measures the growth rate of the number of distinguishable orbits of the system. It is a topological invariant, in particular it does not depend on the metric inducing the topology. The original definition by Adler, Konheim and McAndrew ([AKM65]) uses open covers of the space. Brudno's definition of algorithmic complexity of orbits is underlay by this definition, and then is defined only for compact spaces.

Bowen ([Bow71],[Bow73]) gave a characterization of the topological entropy of a system inspired of the ϵ-entropy of Kolmogorov and Tikhomirov ([KT59]), which makes sense for non-compact spaces. Using this idea, Galatolo extended the notion of algorithmic complexity of orbits to the non-compact case ([Gal00]). We denote by $\overline{\mathcal{K}}(x, T)$ the algorithmic complexity of the orbit of x under T.

Using topological and algorithmic arguments, we prove:

Theorem. *Let X be a compact computable metric space and $T : X \to X$ a computable map. Then,*

$$h(T) = \sup_{x \in X} \overline{\mathcal{K}}(x, T).$$

where $h(T)$ is the topological entropy of the system.

5.2.1 Topological entropy

Bowen's definition is reminiscent of the capacity (or box counting dimension) of a totally bounded subset of a metric space. In order to prove the theorem mentioned above, we will also use a characterization of topological entropy, expressing it as a kind of Hausdorff dimension. We first present Bowen's definition.

In this section, X is a metric space and $T : X \to X$ a continuous map.

Entropy as a capacity

For $n \geq 0$, let us define the distance $d_n(x, y) = \max\{d(T^i x, T^i y) : 0 \leq i < n\}$ and the Bowen ball $B_n(x, \epsilon) = \{y : d_n(x, y) < \epsilon\}$, which is open by continuity of T. Given a totally bounded set $Y \subseteq X$ and numbers $n \geq 0, \epsilon > 0$, let $N(Y, n, \epsilon)$ be the minimal cardinality of a cover of Y by Bowen balls $B_n(x, \epsilon)$. A set of points E such that $\{B_n(x, \epsilon) : x \in E\}$ is a cover of Y is also called an (n, ϵ)-spanning set of Y. One then defines:

$$h_1(T, Y, \epsilon) = \limsup_{n \to \infty} \frac{\log N(Y, n, \epsilon)}{n}$$

which is non-decreasing as $\epsilon \to 0$, so the following limit exists:

$$h_1(T, Y) = \lim_{\epsilon \to 0} h_1(Y, T, \epsilon).$$

When X is compact, the ***topological entropy*** of T is $h(T) = h_1(T, X)$. It measures the exponential growth-rate of the number of distinguishable orbits of the system.

The topological entropy can be defined using separated sets instead of open covers: a subset A of X is (n, ϵ)-separated if for any distinct points $x, y \in A$, $d_n(x, y) > \epsilon$. Let us define $M(Y, n, \epsilon)$ as the maximal cardinality of an (n, ϵ)-separated subset of Y. It is easy to see that $M(Y, n, 2\epsilon) \leq N(Y, n, \epsilon) \leq M(Y, n, \epsilon)$, and hence $h_1(T, Y)$ can be alternatively defined using $M(Y, n, \epsilon)$ in place of $N(Y, n, \epsilon)$.

Entropy as a dimension

Pesin instead defined a topological entropy which is an analog of Hausdorff dimension. His definition coincides with the classical one in the compact case. Hausdorff dimension has stronger stability properties than box dimension, which has important consequences, as we will see in what follows. We refer the reader to [Pes98], [HK02] for more details.

Let X be a metric space and $T : X \to X$ a continuous map. The ϵ-size of $E \subseteq X$ is 2^{-s} where

$$s = \sup\{n \geq 0 : \mathrm{diam}(T^i E) \leq \epsilon \text{ for } 0 \leq i < n\}.$$

It measures how long the orbits starting from E are ϵ-close. As ϵ decreases, the ϵ-size of E is non-decreasing. The 2ϵ-size of a Bowen ball $B_n(x, \epsilon)$ is less than 2^{-n}.

In a way that is reminiscent from the definition of Hausdorff measure, let us define

$$m^s_\delta(Y, \epsilon) = \inf_{\mathcal{G}} \left\{ \sum_{U \in \mathcal{G}} (\epsilon\text{-size}(U))^s \right\}$$

where the infimum is taken over all countable covers $\mathcal{G}$ of Y by open sets of ϵ-size $< \delta$. This quantity is monotonically increasing as δ tends to 0, so the limit $m^s(Y, \epsilon) := \lim_{\delta \to 0^+} m^s_\delta(Y, \epsilon)$ exists and is a supremum. There is a critical value s_0 such that $m^s(Y, \epsilon) = \infty$ for $s < s_0$ and $m^s(Y, \epsilon) = 0$ for $s > s_0$. Let us define $h_2(T, Y, \epsilon)$ as this critical value:

$$h_2(T, Y, \epsilon) := \inf\{s : m^s(Y, \epsilon) = 0\} = \sup\{s : m^s(Y, \epsilon) = \infty\}.$$

As less and less covers are allowed when $\epsilon \to 0$ (the ϵ-size of sets does not decrease), the following limit exists

$$h_2(T,Y) := \lim_{\epsilon \to 0^+} h_2(T,Y,\epsilon)$$

and is a supremum. In [Pes98], it is proved that:

Theorem 5.2.1.1. *When Y is a T-invariant compact set, $h_1(T,Y) = h_2(T,Y)$.*

In particular, if the space X is compact, then $h(T) = h_1(T,X) = h_2(T,X)$.

5.2.2 Orbit complexity

In this section, $(X,d,\mathcal{S})$ is a computable metric space and $T : X \to X$ a transformation (for the moment, no continuity or computability assumption is put on T). Galatolo ([Gal00]) defined an algorithmic complexity of the orbits of a dynamical system, which quantifies the algorithmic information needed to describe the orbit of x with finite but arbitrarily accurate precision. He proved it to coincide with Brudno's definition on compact spaces.

Given $\epsilon > 0$ and $n \in \mathbb{N}$, the algorithmic information needed to follow the n first iterates of x up to ϵ is:

$$\mathcal{K}_n(x,T,\epsilon) := \min\{K(i_0,\ldots,i_{n-1}) : d(s_{i_j}, T^j x) < \epsilon \text{ for } j = 0,\ldots,n-1\}$$

where K is the self-delimiting Kolmogorov complexity. We then define the maximal and minimal growth-rates of this quantity:

$$\begin{aligned}
\overline{\mathcal{K}}(x,T,\epsilon) &:= \limsup_{n\to\infty} \frac{1}{n}\mathcal{K}_n(x,T,\epsilon) \\
\underline{\mathcal{K}}(x,T,\epsilon) &:= \liminf_{n\to\infty} \frac{1}{n}\mathcal{K}_n(x,T,\epsilon).
\end{aligned}$$

As ϵ tends to 0, these quantities increase (or at least do not decrease), hence they have limits (which can be infinite).

Definition 5.2.2.1. The ***upper*** and ***lower orbit complexities*** of x under T are defined by:

$$\begin{aligned}
\overline{\mathcal{K}}(x,T) &:= \lim_{\epsilon\to 0^+} \overline{\mathcal{K}}(x,T,\epsilon) \\
\underline{\mathcal{K}}(x,T) &:= \lim_{\epsilon\to 0^+} \underline{\mathcal{K}}(x,T,\epsilon).
\end{aligned}$$

Remark 5.2.2.1. If T is computable, and assuming that ϵ takes only rational values, the n first iterates of x could be ϵ-shadowed by the orbit of a single ideal point instead of a pseudo-orbit of n ideal points. Actually it is easy to see that it gives the same quantities $\overline{\mathcal{K}}(x,T,\epsilon)$ and $\underline{\mathcal{K}}(x,T,\epsilon)$: let $\mathcal{K}'_n(x,T,\epsilon)=\min\{K(i):d(T^j s_i,T^j x)<\epsilon \text{ for } j<n\}$, one has:

$$\begin{aligned}\mathcal{K}'_n(x,T,2\epsilon) &\overset{+}{<} \mathcal{K}_n(x,T,\epsilon)+K(\epsilon)\\ \mathcal{K}_n(x,T,\epsilon) &\overset{+}{<} \mathcal{K}'_n(x,T,\epsilon/2)+K(n,\epsilon)\end{aligned}$$

Indeed, from ϵ and $i_0,\dots,i_{n-1}$ some ideal point can be algorithmically found in the constructive open set $B(s_{i_0},\epsilon)\cap\ldots\cap T^{-(n-1)}B(s_{i_{n-1}},\epsilon)$, uniformly in $i_0,\dots,i_{n-1}$. Its n first iterates 2ϵ-shadow the orbit of x, which proves the first inequality. For the second inequality, some $i_0,\dots,i_{n-1}$ can be algorithmically found from n, ϵ, and a point s_i whose n first iterates $\epsilon/2$-shadow the orbit of x, taking any $s_{i_j}\in B(T^j s_i,\epsilon/2)$.

Remark 5.2.2.2. Under the same assumptions, one could define $K(B_n(s_i,\epsilon))$ to be $K(i,n,\epsilon)$, and replace $K(i)$ by $K(B_n(s_i,\epsilon))$ in the definition of $\mathcal{K}'_n(x,T,\epsilon)$, without changing the quantities $\overline{\mathcal{K}}(x,T,\epsilon)$ and $\underline{\mathcal{K}}(x,T,\epsilon)$. Indeed,

$$K(i)\overset{+}{<}K(B_n(s_i,\epsilon))\overset{+}{<}K(i)+K(n)+K(\epsilon)$$

5.2.3 Relation between orbit complexity and topological entropy

In this section, we prove the following theorem:

Theorem 5.2.3.1 (Topological entropy vs orbit complexity)**.** *Let X be a compact computable metric space, and $T:X\to X$ a computable map. Then*

$$h(T)=\sup_{x\in X}\underline{\mathcal{K}}(x,T)=\sup_{x\in X}\overline{\mathcal{K}}(x,T).$$

In order to prove this theorem, we define an effective version of the topological entropy, which is strongly related to the complexity of orbits. The idea is not new and has been deeply studied on the Cantor space, defining effective versions of many types of dimensions and relating them to Kolmogorov complexity (see [CH94], [May01], [Lut03], [Rei04], [Sta05]).

Effective entropy as an effective dimension

Before defining an effective version, we give a simple characterization which will accommodate to effectivization.

Definition 5.2.3.1. A ***null s-cover*** of $Y \subseteq X$ is a set $E \subseteq \mathbb{N}^3$ such that:

1. $\sum_{(i,n,p)\in E} 2^{-sn} < \infty$,
2. for each $k, p \in \mathbb{N}$, the set $\{B_n(s_i, 2^{-p}) : (i,n,p) \in E, n \geq k\}$ is a cover of Y.

The idea is simple: every null s-cover induces open covers of arbitrary small size and arbitrary small weight. Remark that any null s-cover of Y is also a null s'-cover for all $s' > s$.

Lemma 5.2.3.1. $h_2(T, Y) = \inf\{s : Y \textit{ has a null } s\textit{-cover}\}$.

Proof. Suppose $s > h_2(T, Y)$. We fix $p, k \in \mathbb{N}$ and put $\epsilon = 2^{-p}$ and $\delta = 2^{-k}$. As $m^s_\delta(Y, \epsilon) = 0$, there is a cover $(U_{j,k,p})_j$ of Y by open sets of ϵ-size $\delta_{j,k,p} < \delta$ with $\sum_j \delta^s_{j,k,p} < 2^{-(k+p)}$. Let s_i be any ideal point in $U_{j,k,p}$. If $\delta_{j,k,p} > 0$, then $\delta_{j,k,p} = 2^{-n}$ for some n. If $\delta_{j,k,p} = 0$, take any $n \geq (j + k + p)/s$. In both cases, $U_{j,k,p}$ is included in the Bowen ball $B_n(s_i, \epsilon)$. We define $E_{k,p}$ as the set of (i, n, p) obtained this way, and $E = \bigcup_{k,p} E_{k,p}$. By construction, for each k, p, $\{B_n(s_i, 2^{-p}) : (i, n, p) \in E, n \geq k\}$ is a cover of Y. Moreover, $\sum_{(i,n,p)\in E_{k,p}} 2^{-sn} \leq \sum_j \delta^s_{j,k,p} + \sum_j 2^{-(j+k+p)} \leq 2^{-(k+p)+2}$, so $\sum_{(i,n,p)\in E} 2^{-sn} < \infty$.

Conversely, if Y has a null s-cover E, take $\epsilon, \delta > 0$ and p, k such that $\epsilon > 2^{-p+1}$ and $\delta > 2^{-k}$. For all $k' \geq k$, the family $\{B_n(s_i, 2^{-p}) : (i, n, p) \in E, n \geq k'\}$ is a cover of Y by open sets of ϵ-size smaller than $2^{-n} \leq \delta$. Moreover, $\sum_{(i,n,p)\in E, n\geq k'} 2^{-sn}$ tends to 0 as k' grows, so $m^s_\delta(Y, \epsilon) = 0$. It follows that $s \geq h_2(T, Y)$. □

By an *effective* null s-cover, we mean a null s-cover E which is a r.e. subset of $\mathbb{N}^3$.

Definition 5.2.3.2. The ***effective topological entropy*** of T on Y is defined by

$$h_2^{\text{eff}}(T, Y) = \inf\{s : Y \text{ has an effective null } s\text{-cover}\}$$

As less null s-covers are allowed in the effective version, $h_2(T, Y) \leq h_2^{\text{eff}}(T, Y)$. Of course, if $Y \subseteq Y'$ then $h_2^{\text{eff}}(T, Y) \leq h_2^{\text{eff}}(T, Y')$. Hausdorff dimension has an important stability property: $\dim Y = \sup_{i\in\mathbb{N}} \dim Y_i$ when $\bigcup_{i\in\mathbb{N}} Y_i = Y$. This property has a much stronger counterpart in the effective version: $\dim^{\text{eff}} Y = \sup_{y\in Y} \dim^{\text{eff}}\{y\}$, which has sense because the effective dimension of a point is generally positive. This remarkable result, which has been proved on the Cantor space, can be extended on any computable metric space and also holds for the effective topological dimension.

Theorem 5.2.3.2 (Effective topological entropy vs lower orbit complexity)**.** *Let X be an effective metric space and $T : X \to X$ a continuous map. For all $Y \subseteq X$,*

$$h_2^{\text{eff}}(T, Y) = \sup_{x \in Y} \underline{\mathcal{K}}(x, T)$$

This theorem is a direct consequence of the two following lemmas.

Lemma 5.2.3.2. *Let $\alpha \geq 0$ and $Y_\alpha = \{x : \underline{\mathcal{K}}(x, T) \leq \alpha\}$. One has $h_2^{\text{eff}}(T, Y_\alpha) \leq \alpha$.*

Proof. Let $\beta > \alpha$ be a rational number. We define the r.e. set $E = \{(i, n, p) : K(i, n, p) < \beta n\}$. Let $p \in \mathbb{N}$ and $\epsilon = 2^{-p}$. If $x \in Y_\alpha$ then $\underline{\mathcal{K}}(x, T, \epsilon) \leq \alpha < \beta$ so for infinitely many n, there is some s_i such that $x \in B_n(s_i, \epsilon)$ and $K(i, n, p) < \beta n$. So for all k, $\{B_n(s_i, 2^{-p}) : (i, n, p) \in E, n \geq k\}$ covers Y_α. Moreover, $\sum_{(i,n,p)\in E} 2^{-\beta n} \leq \sum_{(i,n,p)\in E} 2^{-K(i,n,p)} \leq 1$.

E is then an effective null β-cover of Y_α, so $h_2^{\text{eff}}(T, Y_\alpha) \leq \beta$. And this is true for every rational $\beta > \alpha$. □

Lemma 5.2.3.3. *Let $Y \subseteq X$. For all $x \in Y$, $\underline{\mathcal{K}}(x, T) \leq h_2^{\text{eff}}(T, Y)$.*

Proof. Let $s > h_2^{\text{eff}}(T, Y)$: Y has an effective null s-cover E. As $\sum_{(i,n,p)\in E} 2^{-sn} < \infty$, by the coding theorem $K(i, n, p) \leq sn + c$ for some constant c, which does not depend on i, n, p. If $x \in Y$, then for each p, k, x is in a ball $B_n(s_i, 2^{-p})$ for some $n \geq k$ with $(i, n, p) \in E$. Then $\mathcal{K}_n(x, T, 2^{-p}) \leq sn + c$ for infinitely many n, so $\underline{\mathcal{K}}(x, T, 2^{-p}) \leq s$. As this is true for all p, $\underline{\mathcal{K}}(x, T) \leq s$. As this is true for all $s > h_2^{\text{eff}}(T, Y)$, we can conclude. □

Proof of theorem 5.2.3.2. By lemma 5.2.3.3, $\alpha := \sup_{x\in Y} \underline{\mathcal{K}}(x, T) \leq h_2^{\text{eff}}(T, Y)$. Now, as $Y \subseteq Y_\alpha$, $h_2^{\text{eff}}(T, Y) \leq h_2^{\text{eff}}(T, Y_\alpha) \leq \alpha$ by lemma 5.2.3.2. □

The definition of an effective null α-cover involves a summable computable sequence. The universality of the sequence $2^{-K(i)}$ among summable lower semi-computable sequences is at the core of the proof of the preceding theorem, which states that there is a universal effective null α-cover, for every $\alpha \geq 0$. In other words, there is a maximal set of effective topological entropy $\leq \alpha$, and this set is $Y_\alpha = \{x \in X : \underline{\mathcal{K}}(x, T) \leq \alpha\}$.

The definition of the topological entropy as a capacity could be also made effective. Classical capacity does not share with Hausdorff dimension the countable stability. For the same reason, its effective version is not related with the orbit complexity as strongly as the effective topological entropy is. Nevertheless, a weaker relation holds, which is sufficient for our purpose: the upper complexity of orbits is bounded by the effective capacity. We do not develop this and only state the needed property (which implicitly uses the fact that the effective capacity coincides with the classical capacity for a compact computable metric space):

Lemma 5.2.3.4. *Let X be a compact computable metric space. For all $x \in X$, $\overline{\mathcal{K}}(x,T) \leq h_1(T,X)$.*

Proof. We first construct a r.e. set $E \subseteq \mathbb{N}^3$ such that for each n, p, $\{s_i : (i,n,p) \in E\}$ is a $(n, 2^{-p})$-spanning set and a $(n, 2^{-p-2})$-separated set. Let us fix n and p and enumerate $E_{n,p} = \{i : (i,n,p) \in E\}$, in a uniform way. The algorithm starts with $S = \emptyset$ and $i = 0$. At step i it analyzes s_i and decides to add it to S or not, and goes to step $i+1$. $E_{n,p}$ is the set of points which are eventually added to S.

Step i for each ideal point $s \in S$, test in parallel $d_n(s_i, s) < 2^{-p-1}$ and $d_n(s_i, s) > 2^{-p-2}$: at least one of them must stop. If the first one stops first, reject s_i and go to Step $i+1$. If the second one stops first, go on with the other points $s \in S$: if all S has been considered, then add s_i to S and go to Step $i+1$.

By construction, the set of selected ideal points forms a $(n, 2^{-p-2})$-separated set. If there is $x \in X$ which is at distance at least 2^{-p} from every selected point, then let s_i be an ideal point s_i with $d_n(x, s_i) < 2^{-p-1}$: s_i is at distance at least 2^{-p-1} from every selected point, so at step i it must have been selected, as the first test could not stop. This is a contradiction: the selected points form a $(n, 2^{-p})$-spanning set.

From the properties of $E_{n,p}$ it follows that $N(X, n, 2^{-p}) \leq |E_{n,p}| \leq M(X, n, 2^{-p-2})$, and then

$$\sup_p \left(\limsup \frac{1}{n} \log |E_{n,p}| \right) = h_1(T,X)$$

If $\beta > h_1(T,X)$ is a rational number, then for each p, there is $k \in \mathbb{N}$ such that $\log |E_{n,p}| < \beta n$ for all $n \geq k$.

Now, for $s_i \in E_{n,p}$, $K(i) \stackrel{+}{<} \log |E_{n,p}| + 2 \log \log |E_{n,p}| + K(n,p)$ by proposition 1.8.3.1. Take $x \in X$: x is in some $B_n(s_i, 2^{-p})$ for each n, so $\overline{\mathcal{K}}(x, T, 2^{-p}) \leq \limsup_n \frac{1}{n} \log |E_{n,p}| \leq \beta$ as $\log |E_{n,p}| < \beta n$ for all $n \geq k$. As this is true for all p and all $\beta > h_1(T,X)$, $\overline{\mathcal{K}}(x,T) \leq h_1(T,X)$ and this for all $x \in X$. □

We are now able to prove the main theorem, combining the several results established above:

$$\begin{array}{ccccc} h_1(T,X) = h_2(T,X) & \leq & h_2^{\text{eff}}(T,X) = \sup_{x\in X} \underline{\mathcal{K}}(x,T) & \leq & \sup_{x\in X} \overline{\mathcal{K}}(x,T) \leq h_1(T,X) \\ \text{(theorem 5.2.1.1)} & & \text{(theorem 5.2.3.2)} & & \text{(lemma 5.2.3.4)} \end{array}$$

5.3 Equivalence of the two notions of orbit complexity for random points

We now prove:

Theorem 5.3.0.3. *Let T be an ergodic endomorphism of the computable probability space (X, μ), where X is compact. Then for every Martin-Löf random point x,*

$$\overline{\mathcal{K}}(x,T) = \mathcal{K}_\mu(x,T).$$

Proof of $\overline{\mathcal{K}}(x,T) \leq \mathcal{K}_\mu(x,T)$. Let $\epsilon > 0$. Choose a computable partition ξ of diameter $< \epsilon$ (this is why we require X to be compact). To every cell of ξ, associate an ideal point which is inside (as ξ is computable, this can be done in a computable way, but we actually do not need that). The translation of symbolic sequences in sequences of ideal points through this finite dictionary is constructive, and transforms the symbolic orbit of a point x into a sequence of ideal points which is ϵ-close to the orbit of x. So $\overline{\mathcal{K}}(x,T,\epsilon) \leq \mathcal{K}_\mu(x,T|\xi)$. The inequality follows letting ϵ tend to 0. □

To prove the other inequality, we recall some technical stuff. The self-delimiting Kolmogorov complexity of natural numbers $k \geq 1$ satisfies

$$K(k) \overset{+}{<} f(k)$$

where $f(x) = \log x + 1 + 2\log(\log x + 1)$ for all $x \in \mathbb{R}, x \geq 1$. f is a concave increasing function and $x \mapsto x f(1/x)$ is an increasing function on $]0,1]$ which tends to 0 as $x \to 0$.

We recall that for finite sequences of natural numbers $(k_1, \ldots, k_n)$, one has

$$K(k_1, \ldots, k_n) \overset{+}{<} K(k_1) + \ldots + K(k_n)$$

as the shortest descriptions for $k_1, \ldots, k_n$ can be extracted from their concatenation (this is one reason to use the self-delimiting complexity instead of the plain complexity).

Lemma 5.3.0.5. *Let Σ be a finite alphabet and $n \in \mathbb{N}$. Let $u, v \in \Sigma^n$ and $0 < \alpha < 1/2$ such that the density of the set of positions where u and v differ is less than α, that is:*

$$\frac{1}{n}\#\{i \leq n : u_i \neq v_i\} < \alpha < 1/2$$

Then $\left|\frac{1}{n}K(u) - \frac{1}{n}K(v)\right| < \alpha f(1/\alpha) + \frac{c}{n}$ where c is a constant independent of u, v and n.

Proof. Let $(i_1, \ldots, i_p)$ be the ordered sequence of indices where u and v differ. By hypothesis, $p/n < \alpha$. Put $k_1 = i_1$ and $k_j = i_j - i_{j-1}$ for $2 \leq j \leq p$.

We now show that u can be recovered from v and roughly $\alpha f(1/\alpha)n$ bits more. Indeed u can be computed from $(v, k_1, \ldots, k_p)$, constructing the string which coincides with v everywhere but at positions $k_1, k_1 + k_2, \ldots, k_1 + \ldots + k_p$, so $K(u) \overset{+}{<} K(v) + K(k_1) + \ldots + K(k_p) \overset{+}{<} K(v) + f(k_1) + \ldots + f(k_p)$.

Now, as f is a concave increasing function, one has:

$$\frac{1}{p}\sum_{j \leq p} f(k_j) \leq f\left(\frac{1}{p}\sum_{j \leq p} k_j\right) = f\left(\frac{i_p}{p}\right) \leq f\left(\frac{n}{p}\right)$$

As a result,

$$\frac{1}{n}K(u) \leq \frac{1}{n}K(v) + \frac{p}{n}f\left(\frac{n}{p}\right) + \frac{c}{n}$$

where c is some constant independent of u, v, n, p. As $p/n < \alpha < 1/2$ and $x \mapsto xf(1/x)$ is increasing for $x \leq 1/2$, one has:

$$\frac{1}{n}K(u) \leq \frac{1}{n}K(v) + \alpha f(1/\alpha) + \frac{c}{n}$$

Switching u and v gives the result (c may be changed). □

We are now able to prove the other inequality.

Proof of $\mathcal{K}_\mu(x, T) \leq \overline{\mathcal{K}}(x, T)$. Fix some computable partition ξ. We show that for any $\beta > 0$ there is some $\epsilon > 0$ such that for every Martin-Löf random point x, $\mathcal{K}_\mu(x, T|\xi) \leq \overline{\mathcal{K}}(x, T, \epsilon) + \beta$. As $\overline{\mathcal{K}}(x, T, \epsilon)$ increases as $\epsilon \to 0^+$ and β is arbitrary, the inequality follows.

First take $\alpha < 1/2$ such that $\alpha f(1/\alpha) < \beta$, and remark that

$$\lim_{\epsilon \to 0^+} \mu\left(\overline{(\partial\xi)^\epsilon}\right) = \mu(\partial\xi) = 0$$

Hence there is some ϵ such that $\mu\left(\overline{(\partial\xi)^{2\epsilon}}\right) < \alpha$. From a sequence of ideal points we will reconstruct the symbolic orbit of a random point with a density of errors less than α. Lemma 5.3.0.5 will then allow to conclude.

We define an algorithm $\mathcal{A}(\epsilon, i_0, \ldots, i_{n-1})$ with $\epsilon \in \mathbb{Q}_{>0}$ and $i_0, \ldots, i_{n-1} \in \mathbb{N}$ which outputs a word $a_0 \ldots a_{n-1}$ on the alphabet ξ. To compute a_j, $\mathcal{A}$ semi-decides in a dovetail picture:

- $s_{i_j} \in C$ for every $C \in \xi$,
- $s \in C$ for every $s \in B(s_{i_j}, \epsilon)$ and every $C \in \xi$.

The first test which stops provides some $C \in \xi$: put $a_j = C$.

Let x be a random point whose iterates are covered by ξ, and $s_{i_0}, \ldots, s_{i_{n-1}}$ be ideal points which ϵ-shadow the first n iterates of x. We claim that $\mathcal{A}$ will halt on $(\epsilon, i_0, \ldots, i_{n-1})$. Indeed, as $T^j x$ belongs to some $C \in \xi$, $C \cap B(s_{i_j}, \epsilon)$ is a non-empty open set and then contains at least one ideal point s, which will be eventually dealt with.

We now compare the symbolic orbit of x with the symbolic sequence computed by $\mathcal{A}$. A discrepancy at rank j can appear only if $T^j x \in (\partial\xi)^{2\epsilon}$. Indeed, if $T^j x \notin (\partial\xi)^{2\epsilon}$ then $B(T^j x, 2\epsilon) \subseteq C$ where C is the cell $T^j x$ belongs to. As $d(s_{i_j}, T^j x) < \epsilon$, $B(s_{i_j}, \epsilon) \subseteq B(x, 2\epsilon) \subseteq C$, so the algorithm gives the right cell.

Now, as x is typical,

$$\limsup_{n\to\infty} \frac{1}{n} \#\{j < n : T^j x \in (\partial\xi)^{2\epsilon}\} \leq \mu\left(\overline{(\partial\xi)^{2\epsilon}}\right) < \alpha$$

so there is some n_0 such that for all $n \geq n_0$, $\frac{1}{n}\#\{j < n : T^j x \in (\partial\xi)^{2\epsilon}\} < \alpha$. This implies that for all $n \geq n_0$ and ideal points $s_{i_0}, \ldots, s_{i_{n-1}}$ which ϵ-shadow the first n iterates of x and with minimal complexity, the algorithm $\mathcal{A}(\epsilon, i_0, \ldots, i_{n-1})$ produces a symbolic string u which differs from the symbolic orbit v of x of length n with a density of errors $< \alpha$. As $K(u) \overset{+}{<} K(\epsilon) + \mathcal{K}_n(x, T, \epsilon)$ and $\alpha f(1/\alpha) < \beta$, applying lemma 5.3.0.5 gives:

$$\begin{aligned} \frac{1}{n} K(\xi_n(x)) = \frac{1}{n} K(v) &\leq \frac{1}{n} K(u) + \alpha f(1/\alpha) + \frac{c}{n} \\ &\leq \frac{1}{n}\left(\mathcal{K}_n(x, T, \epsilon) + K(\epsilon) + c'\right) + \beta + \frac{c}{n} \end{aligned}$$

where c' is independent of n. Taking the $\limsup$ as $n \to \infty$ gives:

$$\mathcal{K}_\mu(x, T|\xi) \leq \overline{\mathcal{K}}(x, T, \epsilon) + \beta$$

□

Combining theorem 5.3.0.3 and corollary 5.1.4.2, we obtain a version of Brudno's theorem (theorem 5) for Martin-Löf random points.

Corollary 5.3.0.1. *Let T be an ergodic endomorphism of the computable probability space (X, μ), where X is compact. Then for every Martin-Löf random point x:*

$$\overline{\mathcal{K}}(x, T) = h_\mu(T)$$

Bibliography

[AJ94] Samson Abramsky and Achim Jung. Domain theory. In S. Abramsky, D. Gabbay, and T. S. E. Maibaum, editors, *Handbook of Logic in Computer Science Volume 3*, pages 1–168. Oxford University Press, 1994.

[AKM65] R. L. Adler, A. G. Konheim, and M. H. McAndrew. Topological entropy. *Transactions of the American Mathematical Society*, 114:309–319, February 1965.

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

[Bil65] Patrick Billingsley. *Ergodic Theory and Information*. John Wiley, New York, 1965.

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

[Bil79] Patrick Billingsley. *Probability and Measure*. John Wiley, New York, 1979.

[Bor09] Emile Borel. Les probabilités dénombrables et leurs applications arithmétiques. *Rendiconti del Circolo Matematico di Palermo*, 27:247–271, 1909.

[Bow71] Rufus Bowen. Entropy for group endomorphisms and homogeneous spaces. *Transactions of the American Mathematical Society*, 153:401–414, January 1971.

[Bow73] Rufus Bowen. Topological entropy for noncompact sets. *Transactions of the American Mathematical Society*, 184:125–136, October 1973.

[BP03] Vasco Brattka and Gero Presser. Computability on subsets of metric spaces. *Theoretical Computer Science*, 305(1-3):43–76, 2003.

[Bra01] Vasco Brattka. Computable versions of baire's category theorem. In *MFCS '01: Proceedings of the 26th International Symposium on Mathematical Foundations of Computer Science*, pages 224–235, London, UK, 2001. Springer-Verlag.

[Bru83] A.A. Brudno. Entropy and the complexity of the trajectories of a dynamical system. *Transactions of the Moscow Mathematical Society*, 2:127–151, 1983.

[Cal94] Cristian Calude. *Information and Randomness: An Algorithmic Perspective*. Springer-Verlag New York, Inc., Secaucus, NJ, USA, 1994.

[CH94] Jin-Yi Cai and Juris Hartmanis. On Hausdorff and topological dimensions of the Kolmogorov complexity of the real line. In *Proceedings of the 30th IEEE symposium on Foundations of computer science*, pages 605–619, Orlando, FL, USA, 1994. Academic Press, Inc.

[Dav01] George Davie. The Borel-Cantelli lemmas, probability laws and kolmogorov complexity. *Annals of Probability*, 29(4):1426–1434, 2001.

[Dav04] George Davie. Characterising the Martin-Löf random sequences using computably enumerable sets of measure one. *Information Processing Letters*, 92(3):157–160, 2004.

[DG] R. Downey and E. Griths. On Schnorr randomness.

[DGR04] Rodney G. Downey, Evan J. Griffiths, and Stephanie Reid. On Kurtz randomness. *Theoretical Computer Science*, 321(2-3):249–270, 2004.

[Eda96] Abbas Edalat. The Scott topology induces the weak topology. In *LICS '96: Proceedings of the 11th Annual IEEE Symposium on Logic in Computer Science*, page 372, Washington, DC, USA, 1996. IEEE Computer Society.

[Eda97] Abbas Edalat. Domains for computation in mathematics, physics and exact real arithmetic. *The Bulletin of Symbolic Logic*, 3(4):401–452, 1997.

[Eda07a] Abbas Edalat. A computable approach to measure and integration theory. In *LICS '07: Proceedings of the 22nd Annual IEEE Symposium on Logic in Computer Science*, pages 463–472, Washington, DC, USA, 2007. IEEE Computer Society.

[Eda07b] Abbas Edalat. A continuous derivative for real-valued functions. In S. Barry Cooper, Benedikt Löwe, and Andrea Sorbi, editors, *CiE*, volume 4497 of *Lecture Notes in Computer Science*, pages 248–257. Springer, 2007.

[EH98] Abbas Edalat and Reinhold Heckmann. A computational model for metric spaces. *Theoretical Computer Science*, 193:53–73, 1998.

[ES99] Abbas Edalat and Philipp Sünderhauf. A domain-theoretic approach to computability on the real line. *Theoretical Computer Science*, 210(1):73–98, 1999.

[Gác] Peter Gács. Lecture notes on descriptional complexity and randomness. http://www.cs.bu.edu/faculty/gacs/papers/ait-notes.pdf.

[Gác79] Péter Gács. Exact expressions for some randomness tests. In *Proceedings of the 4th GI-Conference on Theoretical Computer Science*, pages 124–131, London, UK, 1979. Springer-Verlag.

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

[Gal99] Stefano Galatolo. Pointwise information entropy for metric spaces. *Nonlinearity*, 12(5):1289–1298, 1999.

[Gal00] Stefano Galatolo. Orbit complexity by computable structures. *Nonlinearity*, 13:1531–1546, 2000.

[GHR07a] Stefano Galatolo, Mathieu Hoyrup, and Cristóbal Rojas. Computable invariant measures. *In preparation*, 2007.

[GHR07b] Stefano Galatolo, Mathieu Hoyrup, and Cristóbal Rojas. An effective Borel-Cantelli lemma. Constructing orbits with required statistical properties. *Submitted to JEMS*, 2007. Available on arxiv.

[GHR07c] Stefano Galatolo, Mathieu Hoyrup, and Cristóbal Rojas. Effective symbolic dynamics, random points, statistical behavior, complexity and entropy. *Submitted to Information and Computation*, 2007. Available on arxiv.

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

[Hem02] Armin Hemmerling. Effective metric spaces and representations of the reals. *Theor. Comput. Sci.*, 284(2):347–372, 2002.

[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.

[HK02] Boris Hasselblatt and Anatole Katok. *Handbook of Dynamical Systems*, volume 1A, chapter Principle Structures. Elsevier, 2002.

[Hoy07] Mathieu Hoyrup. Dynamical systems: stability and simulability. *Mathematical Structures in Computer Science*, 17(2):247–259, 2007.

[HR07] Mathieu Hoyrup and Cristóbal Rojas. Computability of probability measures and Martin-Löf randomness over metric spaces. *Submitted to Information and Computation*, 2007. Available on arxiv.

[HW97] Peter Hertling and Yongge Wang. Invariance properties of random sequences. *Journal of Universal Computer Science*, 3(11):1241–1249, 1997.

[HW98] Peter Hertling and Klaus Weihrauch. Randomness spaces. In Kim G. Larsen, Sven Skyum, and Glynn Winskel, editors, *Automata, Languages and Programming*, volume 1443 of *Lecture Notes in Computer Science*, pages 796–807, Berlin, 1998. Springer. 25th International Colloquium, ICALP'98, Aalborg, Denmark, July 1998.

[HW03] Peter Hertling and Klaus Weihrauch. Random elements in effective topological spaces with measure. *Information and Computation*, 181(1):32–56, 2003.

[Kol58] A.N. Kolmogorov. A new metric invariant of transitive dynamical systems, and Lebesgue space automorphisms. *Doklady Akademii Nauk*, 119(5):861–864, 1958. In Russian.

[Kol65] A.N. Kolmogorov. Three approaches to the quantitive definition of information. *Problems of Information Transmission*, 1:1–17, 1965.

[KT59] A.N. Kolmogorov and V.M. Tikhomirov. ϵ-entropy and ϵ-capacity. *Uspekhi Mat. Nauk*, 14:3–86, 1959. English transl. AMS Translations, 17:2 (1961), 277-364.

[KV61] A.N. Kolmogorov and Tikhomirov V.M. ϵ-entropy and ϵ-capacity of sets in functional spaces. *AMS Translations, Series 2*, 17:277–364, 1961.

[Lut03] Jack H. Lutz. The dimensions of individual strings and sequences. *Information and Computation*, 187(1):49–79, 2003.

[LV93] Ming Li and Paul M. B. Vitanyi. *An Introduction to Kolmogorov Complexity and Its Applications*. Springer-Verlag, Berlin, 1993.

[May01] Elvira Mayordomo. A Kolmogorov complexity characterization of constructive Hausdorff dimension. *Electronic Colloquium on Computational Complexity (ECCC)*, 8(059), 2001.

[Mil04] Joseph S. Miller. Degrees of unsolvability of continuous functions. *Journal of Symbolic Logic*, 69(2):555–584, 2004.

[ML66] Per Martin-Löf. The definition of random sequences. *Information and Control*, 9(6):602–619, 1966.

[ML71] Per Martin-Löf. Complexity oscillations in infinite binary sequences. *Z. Wahrscheinlichkeit*, 19:225–230, 1971.

[Nak05] Masahiro Nakamura. Ergodic theorems for algorithmically random sequences. *Proceedings of the Symposium on Information Theory and Its Applications*, 2005.

[PER89] Marian B. Pour-El and J. Ian Richards. *Computability in Analysis and Physics*. Perspectives in Mathematical Logic. Springer, Berlin, 1989.

[Pes98] Yakov B. Pesin. *Dimension Theory in Dynamical Systems: Contemporary Views and Applications*. Chicago Lectures in Mathematics. The University of Chicago Press, 1998.

[Pet83] Karl Petersen. *Ergodic Theory*. Cambridge Univ. Press, 1983.

[Rei04] Jan Reimann. *Computability and fractal dimension*. PhD thesis, Ruprecht-Karls Universität Heidelberg, 2004.

[Rog87] Hartley Jr. Rogers. *Theory of Recursive Functions and Effective Computability*. MIT Press, Cambridge, MA, USA, 1987.

[Roj06] Cristóbal Rojas. Computability and information in models of randomness and chaos. *To appear in Mathematical Structures in Computer Science*, 2006.

[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.

[Sch07] Matthias Schröder. Admissible representations of probability measures. *Electronic Notes in Theoretical Computer Science*, 167:61–78, 2007.

[Sie17] M.W. Sierpiński. Démonstration élémentaire du théorème de M. Borel sur les nombres absolument normaux et détermination effective d'un tel nombre. *Bulletin de la Société Mathématique de France*, 47:127–132, 1917.

[Sin59] Yakov G. Sinai. On the notion of entropy of dynamical systems. *Doklady Akademii Nauk*, 124(4):768–771, 1959. In Russian.

[Sta05] Ludwig Staiger. Constructive dimension equals Kolmogorov complexity. *Information Processing Letters*, 93(3):149–153, 2005.

[vL87] M. van Lambalgen. *Random sequences*. PhD thesis, Department of Mathematics, University of Amsterdam, 1987.

[VV93] Vladimir G. Vovk and Vladimir V. Vyugin. On the empirical validity of the bayesian method. *Journal of the Royal Statistical Society*, B 55(1):253–266, 1993.

[V'y97] Vladimir V. V'yugin. Effective convergence in probability and an ergodic theorem for individual random sequences. *SIAM Theory of Probability and Its Applications*, 42(1):39–50, 1997.

[V'y98] Vladimir V. V'yugin. Ergodic theorems for individual random sequences. *Theoretical Computer Science*, 207(4):343–361, 1998.

[V'y01] Vladimir V. V'yugin. Non-robustness property of the individual ergodic theorem. *Problems of Information Transmission*, 37(2):27–39, 2001.

[Wal82] Peter Walters. *An Introduction to Ergodic Theory*, volume 79 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1982.

[Was69] L.N. Wasserstein. Markov processes over denumerable products of spaces describing large systems of automata. *Problems of Information Transmission*, 5:47–52, 1969.

[WB96] H. White and R.W. Batterman. Chaos and algorithmic complexity. *Foundations of Physics*, 26(3):307–336, 1996.

[Wei93] Klaus Weihrauch. Computability on computable metric spaces. *Theoretical Computer Science*, 113(2):191–210, 1993.

[Wei99] Klaus Weihrauch. Computability on the probability measures on the borel sets of the unit interval. *Theoretical Computer Science*, 219:421–437, 1999.

[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 structure. *Theoretical Computer Science*, 219(1-2):467–486, 1999.

Appendix A

Background from topology

Definition A.0.0.3 (Topology)**.** Let X be a set. A ***topology*** on X is a class τ of subsets of X which contains $\emptyset$ and X and is closed under the formation of unions and finite intersections. (X, τ) is called a ***topological space***.

Definition A.0.0.4 (Continuity)**.** Let (X, τ^X) and (Y, τ^Y) be topological spaces. A function $f : X \to Y$ is ***continuous*** if for every $U \in \tau_Y$, $f^{-1}(U) \in \tau_X$.

A.1 Convergence

A.1.1 Sequences

Definition A.1.1.1 (Convergence)**.** Let (X, τ) be a topological space. Let $(x_n)_{n\in\mathbb{N}}$ be a sequence of elements of X. We say that x_n ***converges*** to x, or that x is a ***limit*** of x_n if for every open set U,

$$x \in U \implies \exists k, x_n \in U \text{ for all } n \geq k$$

We denote it by $x_n \to x$.

In a space where the limit is unique, we can write $\lim_{n\to\infty} x_n = x$. But we will meet topological space in which a sequence may have many limits.

Conversely, any notion of convergence induces a topology.

Definition A.1.1.2 (Topology of convergence)**.** Let X be a set, and $\to \subseteq X^{\mathbb{N}} \times X$ a relation between sequences and elements of X. The ***topology of*** $\to$***-convergence*** is the topology $\tau_\to$

defined by:

$$U \in \tau_{\to} \iff \text{for all } x \in U \text{ and all sequence } x_n \text{ such that } x_n \to x, \exists k, \forall n \geq k, x_n \in U$$

It is indeed a topology. Now, let (X, τ) be a topological space: definition A.1.1.1 gives a canonical convergence relation $\to$ on X. Definition A.1.1.2 in turn provides a topology $\tau_{\to}$, called the ***sequential topology***.

By definition of convergence, the sequential topology is finer than the primitive topology: $\tau \subseteq \tau_{\to}$ so $id : (X, \tau_{\to}) \to (X, \tau)$ is continuous. The notion of convergence provided by $\tau_{\to}$ coincides with $\to$.

Definition A.1.1.3 (Sequential continuity)**.** Let (X, τ^X) and (Y, τ^Y) be topological spaces. A function $f : X \to Y$ is ***sequentially continuous*** if for all sequence x_n converging to some x, $f(x_n)$ converges to $f(x)$.

f is sequentially continuous if and only if $f : (X, \tau^X_{\to}) \to (Y, \tau^Y)$ is continuous, if and only if $f : (X, \tau^X_{\to}) \to (Y, \tau^Y_{\to})$ is continuous.

Proposition A.1.1.1. *Continuity implies sequential continuity.*

Proof. If f is continuous, then $f = f \circ id_X : (X, \tau^X_{\to}) \to (Y, \tau^Y)$ is continuous. □

A topological space (X, τ) is ***sequential*** if the sequential topology coincides with τ. A function from a sequential space to a topological space is continuous if and only if it is sequentially continuous. Every second-countable topological space (space with a countable basis) is sequential.

A.1.2 Nets

There is a generalization of the notions of sequence and converging sequence: nets and converging nets. A sequence is indexed by the total order $\mathbb{N}$, a net is indexed by a partial order.

Definition A.1.2.1. Let X be a set. A ***net*** is a family $(x_d)_{d \in D}$ of elements of X indexed by a directed set $(D, \leq)$. We denote by Nets the set of nets.

Definition A.1.2.2. A ***net-convergence space*** is a set X with a relation $\to \subseteq \mathrm{Nets} \times X$ between nets and elements, called the ***net-convergence relation***.

Every net-convergence relation induces a topology τ_{net}, called the ***topology of net-convergence***, defined by:

$$A \in \tau_{\text{net}} \iff \forall (x_d)_{d \in D} \to x \in A, \exists d \in D, x_{d'} \in U \text{ for all } d' \geq d$$

It is indeed a topology. Now, let X be a set: every topology τ on X induces a net-convergence relation, defined by:

$$(x_d)_{d \in D} \to x \iff [\forall U \in \tau, x \in U \implies \exists d \in D, x_{d'} \in U \text{ for all } d' \geq d]$$

which in turn induces a topology τ_{net}. By definition, $\tau \subseteq \tau_{\text{net}}$. Actually,

Proposition A.1.2.1. *Let (X, τ) be a topological space. Then $\tau = \tau_{net}$.*

Proof. Let $A \in \tau_{\text{net}}$ and $x \in A$: we have to show that there is $U \in \tau$ such that $x \in U \subseteq A$. Define $D = \{U \in \tau : x \in U\}$ endowed with the order of reverse inclusion: $U \leq V$ if $U \supseteq V$. D is a directed set. Now, suppose that for each $U \in D$, $U \nsubseteq A$: there exists $y_U \in U \setminus A$. The net $(y_U)_{U \in D}$ converges to x: if $x \in U \in \tau$, then $U \in D$ and for all $V \geq U$, $y_V \in V \subseteq U$. As $x \in A \in \tau_{\text{net}}$, there is $U \in D$ such that $y_U \in A$: contradiction. $\square$

Appendix B

Background from order theory

In section 1.2 we introduce the notion of *enumerative lattice*. This appendix is intended to place this notion in a wider context. We refer to [AJ94] for a complete introduction.

B.1 Directed complete partial order

Definition B.1.0.3. A ***directed complete partial order (dcpo)*** is a partial order $(X, \leq)$ such that that every non-empty directed subset of X has a supremum in X.

Definition B.1.0.4 (Scott-topology)**.** Let $(X, \leq)$ be a directed complete partial order. The ***Scott-topology*** on X is defined by: $U \subseteq X$ is ***Scott-open*** if and only if:

1. it is an upper set: $x \in U, x \leq y \implies y \in U$,
2. for every directed set $D \subseteq X$, $\sup D \in U \implies D \cap U \neq \emptyset$.

The Scott-topology is made for the suprema to be seen as limits. This can be made precise. For each directed set D, D can be seen as a net, indexed by itself: put $x_d = d$ for each $d \in D$. The ***canonical net-convergence relation*** is then defined by:

$$D \to x \iff x \leq \sup D$$

In other words, $\to$ is $\{(D, x) : D \text{ directed}, x \leq \sup D\} \subseteq \mathrm{Nets} \times X$. The Scott-topology is then the topology of net-convergence induced by the canonical net-convergence relation.

Definition B.1.0.5 (Scott-continuity)**.** Let $(X, \sqsubseteq)$ and $(Y, \leq)$ be two directed complete partial orders. A function $f : X \to Y$ is ***Scott-continuous*** if:

1. it is monotonic: $x \sqsubseteq x' \implies f(x) \leq f(x')$,
2. it commutes with directed suprema: if D is a directed subset of X, then $f(\sup_{\sqsubseteq} D) = \sup_{\leq} f(D)$.

Proposition B.1.0.2. *A function $f : X \to Y$ is Scott-continuous if and only if it is continuous for the Scott-topologies on X and Y.*

Proof. Use the fact that $U_{y_0} = \{y \in Y : y \not\leq y_0\}$ is Scott-open for each $y_0 \in Y$. □

Using these particular open sets directly gives:

Proposition B.1.0.3. $x \leq y \iff [\forall U \text{ Scott-open}, x \in U \implies y \in U]$

The induced topological space is Kolmogorov or T_0: for each $x \neq y$, there is an open set U with $x \in U$ and $y \notin U$ or the converse (take $U = U_x$ or U_y).

B.2 Complete lattice

Definition B.2.0.6 (Complete lattice)**.** A ***complete lattice*** $(X, \leq, \perp)$ is a partial order $(X, \leq)$ with a least element $\perp$ such that every subset of X has a supremum.

In a complete lattice, there is a greatest element $\top$, and every subset of X has also an infimum. Any complete lattice is in particular a directed complete partial order, on which the Scott-topology is defined, and can be characterized in the following way:

Proposition B.2.0.4 (Scott-topology)**.** *Let $(X, \leq, \perp)$ be a complete lattice. A subset U of X is Scott-open if and only if for every $A \subseteq X$, the following are equivalent:*

1. $\sup A \in U$,
2. *there exists a finite subset A_0 of A such that* $\sup A_0 \in U$

Proof. Easy (the set of suprema of finite subsets of A is directed). □

Every complete lattice is compact for the Scott-topology: if X is covered by a family of Scott-open sets, one of them contains $\perp$ and then it contains the whole set X.

The characterization of the Scott-topology induces a characterization of Scott-continuity:

Proposition B.2.0.5. *Let $(X, \sqsubseteq)$ and $(Y, \leq)$ be two complete lattices. A function $f : X \to Y$ is Scott-continuous if and only if for every $A \subseteq X$,*

$$f(\sup A) = \sup\{f(\sup A_0) : A_0 \textit{ finite subset of } A\}$$

The set of Scott-continuous functions between complete lattices L, L' is a complete lattice, with the pointwise ordering $f \leq g \iff \forall E, f(E) \leq g(E)$. The supremum of a set of Scott-continuous function $\mathcal{G}$ for this order is their pointwise supremum, i.e. the function defined by $f(x) = \sup_{g \in \mathcal{G}} g(x)$ for each x.

Let X be a set: $(2^X, \subseteq, \emptyset, X)$ is a complete lattice. Let $\mathcal{F}$ be the collection of all finite subsets of X. For $F \in \mathcal{F}$, define $U_F = \{A \subseteq X : F \subseteq A\}$: this is a Scott-open, and the collection $\{U_F : F \in \mathcal{F}\}$ is even a basis of the Scott-topology.

Proposition B.2.0.6. *If finite infima distribute over arbitrary suprema, that is*

$$\inf\{x, \sup A\} = \sup\{\inf\{x, a\} : a \in A\}$$

for all subsets A of L, then $\inf : L \times L \to L$ *is Scott-continuous.*

Proof. For seek of clarity, the function $\inf : L \times L \to L$ will be called f: $f(x, y) = \inf\{x, y\} = x \wedge y$. f is monotonic: if $(d_1, d_2) \leq (d'_1, d'_2)$, i.e. $d_1 \leq d'_1$ and $d_2 \leq d'_2$, then $d_1 \wedge d_2 \leq d'_1 \wedge d'_2$.

Let $D \subseteq L \times L$ be a directed set: we want to show that $f(\sup D) = \sup f(D) = \sup\{f(d) : d \in D\}$. Let $D_1 = \{d_1 : \exists d_2, (d_1, d_2) \in D\}$ and $D_2 = \{d_2 : \exists d_1, (d_1, d_2) \in D\}$: $\sup D = (\sup D_1, \sup D_2)$, so $f(\sup D) = f(\sup D_1, \sup D_2) = \sup f(D_1 \times D_2)$ by distributivity of $\inf$ on $\sup$.

As $D \subseteq D_1 \times D_2$, $\sup f(D) \leq \sup f(D_1 \times D_2)$. Now, if $(d_1, d'_2) \in D_1 \times D_2$, there are d_2, d'_1 such that $(d_1, d_2) \in D$ and $(d'_1, d'_2) \in D$. As D is directed, there is $(d''_1, d''_2) \in D$ with $d_1, d'_1 \leq d''_1$ and $d_2, d'_2 \leq d''_2$. As f is monotonic, $f(d_1, d'_2) \leq f(d''_1, d''_2)$. Hence, $\sup f(D_1 \times D_2) \leq \sup f(D)$. $\square$

A morphism of complete join-semilattices is a function which commutes with all suprema. An isomorphism is a bijective morphism: its inverse is then necessarily a morphism (and then an isomorphism). Between complete lattices, homeomorphisms (i.e. isomorphisms of topological spaces) and isomorphisms of complete lattices are the same (although not every continuous function is a morphism of complete lattices).

Convergence in a complete lattice

Proposition B.2.0.7. *Let $(L, \leq)$ be a complete lattice. Let $(x_n)_{n \in \mathbb{N}}$ be a sequence of elements of L. We define:*

$$\liminf x_n = \sup\{\inf\{x_n : n \geq k\} : k \in \mathbb{N}\}$$

If $x \leq \liminf x_n$ then x_n converges to x in the Scott-topology.

Moreover, if $x_n \leq x_{n+1}$ this is equivalent: x_n converges to x if and only if $x \leq \sup_n x_n = \liminf x_n$.

Proof. Let U be a Scott-open such that $x \in U$: then $\liminf x_n \in U$, so there is k such that $\inf\{x_n : n \geq k\} \in U$, which implies $x_n \in U$ for all $n \geq k$.

Suppose $x_n \leq x_{n+1}$ and x_n converges to x. As $U = \{y : y \not\leq \sup_n x_n\}$ is Scott-open, if $x \in U$ then there is some $x_n \in U$, which is impossible. □

In a complete lattice, every sequence converges (in particular to its $\liminf$), but it has many different limits.

B.2.1 Topology as a complete lattice

The Sierpiński space $\mathbb{S} = \{\perp, \top\}$ is the set with two elements, endowed with the order $\perp < \top$: it is a complete lattice, on which the Scott-topology is $\tau_{\mathbb{S}} = \{\emptyset, \{\top\}, \{\perp, \top\}\}$. Now, the set $[X \to \mathbb{S}]$ of continuous functions from X to $\mathbb{S}$ is in turn a complete lattice, with the pointwise ordering: we endow it with the Scott-topology. τ_X and $[X \to \mathbb{S}]$ are homeomorphic (or isomorphic): $\mathbf{1} : \tau \to [X \to \mathbb{S}]$ defined by $\mathbf{1}(U)(x) = \top$ if $x \in U$, $\perp$ otherwise is an homeomorphism.

Index