THESIS IN COMPUTER SCIENCE
–
COMPUTABILITY, RANDOMNESS AND ERGODIC THEORY ON METRIC SPACES
–
SUM UP

MATHIEU HOYRUP

CONTEXT

Entropies. Several notions of *entropies* have been defined along the twentieth century. The role of an entropy is to quantify the uncertainty one has about the state of a – physical as well as mathematical – system, whose states are modeled as points of a mathematical space. 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 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 (see [LV93], [Cal94] for details on Kolmogorov complexity).

Entropies of dynamical systems. 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),
(2) The Kolmogorov-Sinaï entropy (defined in 1958, 1959),
(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).

Probability theory[1] is the natural framework to talk about randomness (note that this theory is not concerned with the way randomness is generated). On the other hand, as classical randomness is understood as deterministic unpredictability, the theory of dynamical systems provides another setting in which randomness can be investigated. 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 (see [Pet83]).

Algorithmic randomness. 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.

Algorithmic randomness then provides a model which enables one to prove stronger results than probability theory: as each single infinite binary sequence gets the attribute "random" or "non-random", classical theorems like:

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

shall be converted into:

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

Algorithmic randomness theory was still recently restricted to the Cantor space of binary sequences (or sequences over a finite alphabet) (see [HW03], [Gác05] for extensions to other spaces).

Results of the thesis. Our general goal is to establish a robust framework in order to handle probability theory as well as ergodic theory from an algorithmic point of view. Much work has previously been achieved on the Cantor space; but restricting oneself to this space is very limitative, by comparison with the wide range of spaces in which probabilistic and dynamical systems issues generally take place: a theory on more general spaces is needed. We study computable metric spaces, which are metric spaces with a

[1] which axiomatization was achieved in 1933 by Kolmogorov

computability feature allowing one to talk about computable points, functions, subsets, etc. On such spaces, we give different characterizations of computability for probability measures, and extend algorithmic randomness. This work is an improvement of a recent article ([Gác05]). We then establish strong relations between randomness, ergodic theorems, orbit complexities and entropies. Our work is partially based on results which had already been stated on the Cantor space (especially [V'y98]).

In what follows, we present the content of the chapters.

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) has nice categorical properties, but is less general than the second one (see [Wei00]), which in turn uses a rather heavy language. In particular, everything is expressed in terms of Turing machines and coding issues (representations are ways to encode objects into symbolic sequences).

Introducing the notion of *enumerative lattice*, we propose an approach inspired from both of these settings, as general as the second one but focusing more on structures than on machines. The quite elementary enumerative lattice structure can be used to induce all constructivity notions on general space. It enables one to express computability proofs in a more algebraic fashion, freeing oneself from coding questions. The most interesting feature of enumerative lattices is that they grasp the structure needed to construct *effective enumerations*. Effective enumerations are recurrent in computer science (the first one being the enumeration of Turing machines): we prove a general abstract result from which each single effective enumeration shall be derived. In particular, we will use this result to enumerate uniform randomness tests.

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.

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 several works previously achieved. We then introduce the computable version of probability spaces, and show:

Theorem 1. *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.

3. Algorithmic randomness

The preceding section directly provides a notion of algorithmic randomness on computable probability spaces. However, following an approach by Levin, and later Gács ([Gác05]), we define randomness with respect to *any* probability measure (i.e. not necessarily computable), and show that it coincides with the one induced by the isomorphism with the Cantor space whenever the measure is computable. The probability measure is not fixed anymore, but instead becomes a parameter, or argument of randomness tests, which are then called *uniform*. We show two important results:

Theorem 2. *Let X be a computable metric space.*

(1) *Let μ be a probability measure on X: every randomness test for μ can be extended to a uniform test.*
(2) *There exists a* universal *randomness test.*

The first point is important when one constructs a function and proves that it is a test for some measure, using particular properties of this measure (invariant, ergodic, Bernoulli, etc): as random points are those points which pass all uniform tests, it is not clear *a priori* that random points pass this test, which is not uniform.

The second point extends the classical result proved by Martin-Löf on the Cantor space endowed with a computable probability measure. It strengthens Gács result, which holds for computable metric spaces which satisfy an additional computability condition. Our construction is made very synthetic by the use of an appropriate enumerative lattice.

4. Algorithmic ergodic theory

Ergodic theory provides many probability theorems. Let us recall two classical ones: let (X, μ) be a probability space and $T : X \to X$ an endomorphism (or measure-preserving map), (1) the Poincaré recurrence theorem states that the trajectory of μ-almost every point returns arbitrarily close to its initial condition, (2) the Birkhoff ergodic theorem states that for every integrable function $f : X \to \mathbb{R}$, the mean of f along the trajectory of μ-almost every point converges. We say that a point is *generic* if this convergence holds for every bounded continuous observable f.

We state their algorithmic counterpart:

Theorem 3. *Let X be a computable metric space endowed with a (not necessarily computable) probability measure μ. Every μ-random point is recurrent and generic for every endomorphism $T : X \to X$.*

Part of the proof of the ergodic theorem for random points is an extension of a result previously stated on the Cantor space with a computable measure and for computable observables ([V'y98]).

We then study the following problem: the use of a computer is often necessary to catch a glimpse of the behaviour of a dynamical system, when mathematical analysis reaches its limits. But machines can only compute... computable objects, which constitute a tiny subsystem (it is countable and has null measure). The question is then: are the trajectories drawn on the screen representative of the system ? The problem is not related to round-off errors: our computation model enables exact computations, so the trajectories appearing on the screen are indeed trajectories of the system. But may it happen that

every computable orbit is periodic ? or that no computable orbit satisfies the Birkhoff ergodic theorem ? Let us call *pseudo-random* orbits those orbits which are computable and typical in the sense of the Birkhoff ergodic theorem: they are generally not algorithmically random, as they are computable, but they have statistical properties of typical orbits.

We give two positive answers:

Theorem 4. *Let X be a computable metric space and $T : X \to X$ a computable map. If T has a dense orbit, then T has a* computable *dense orbit.*

Let (X, μ) be a computable probability space. Every mixing *endomorphism $T : X \to X$ has a pseudo-random orbit.*

The mixing property is stronger than ergodicity: the state of the system at time t is quasi-independent of the state at time 0, whenever t is sufficiently large. An immediate corollary is the existence of computable real numbers which are normal in every base. This result was already obtained in 2002, but in a rather technical way.

A question is still open: are there computable dynamical systems for which no pseudo-random orbit exist ?

5. Entropy and orbit complexity

In 1998, V'yugin ([V'y98]) proved a version of the Shannon-McMillan-Breiman theorem for random points on the Cantor space endowed with a computable probability measure. This result can be easily transferred to computable probability spaces, using the isomorphism, and then strengthens Brudno's result ([Bru83]): the complexity of the orbit of each random point equals the Kolmogorov-Sinaï entropy of the system. To do this, we use two notions of orbit complexity, the one using computable partitions, the other using the metric, and prove that they coincide for random points. Using topological and algorithmic arguments, we then prove:

Theorem 5. *Let X be a compact computable metric space and $T : X \to X$ a computable map. The supremum of the algorithmic complexity of orbits coincides with the topological entropy of the system.*

These two results put together are related to the variational principle: the topological entropy is the supremum of Kolmogorov-Sinaï entropies, the measure varying among invariant measures.

Some References

[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.

[Eda97] Abbas Edalat. Domains for computation in mathematics, physics and exact real arithmetic. *The Bulletin of Symbolic Logic*, 3(4):401–452, 1997.

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

[Gal00] Stefano Galatolo. Orbit complexity by computable structures. *Nonlinearity*, 13:1531–1546, 2000.

[HW03] Peter Hertling and Klaus Weihrauch. Random elements in effective topological spaces with measure. *Information and Computation*, 181(1):32–56, 2003.

[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.

[LV93] Ming Li and Paul M. B. Vitanyi. *An Introduction to Kolmogorov Complexity and Its Applications*. Springer-Verlag, Berlin, 1993.

[ML66] Per Martin-Löf. The definition of random sequences. *Information and Control*, 9(6):602–619, 1966.

[Pet83] Karl Petersen. *Ergodic Theory*. Cambridge Univ. Press, 1983.

[V'y98] Vladimir V. V'yugin. Ergodic theorems for individual random sequences. *Theoretical Computer Science*, 207(4):343–361, 1998.

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