Laboratoire de l'Informatique du Parallélisme
École Normale Supérieure de Lyon
Unité Mixte de Recherche CNRS-INRIA-ENS LYON n° 5668

CENTRE NATIONAL
DE LA RECHERCHE
SCIENTIFIQUE

On randomness and infinity

Grégory Lafitte September 2001

Research Report N° 2001-36

École Normale Supérieure de Lyon
46 Allée d'Italie, 69364 Lyon Cedex 07, France
Téléphone : +33(0)4.72.72.80.37
Télécopieur : +33(0)4.72.72.80.80
Adresse électronique : `lip@ens-lyon.fr`

On randomness and infinity

Grégory Lafitte

September 2001

Abstract

In this paper, we investigate refined definitions of random sequences. Classical definitions have always the shortcome of making use of the notion of algorithm. We discuss the nature of randomness and different ways of obtaining satisfactory definitions of randomness after reviewing previous attempts at producing a non-algorithmical definition. We present alternative definitions based on infinite time machines and set theory and explain how and why randomness is strongly linked to *strong axioms of infinity*.

Keywords: Random, infinite time machines, large cardinals

Résumé

Dans ce papier, nous étudions différentes définitions de la notion de suite aléatoire. Les définitions classiques ont le défaut d'utiliser la notion d'algorithme. Après la présentation des tentatives passées de trouver une définition non-algorithmique, nous discutons de la notion d'aléatoire et envisageons différentes façons d'obtenir des définitions satisfaisantes. Nous donnons plusieurs définitions basées sur les machines à temps infini et la theorie des ensembles et nous expliquons en quoi l'aléatoire est fortement lié au *axiomes forts de l'infini*.

Mots-clés: Aléatoire, machines à temps infini, grands cardinaux

ON RANDOMNESS AND INFINITY

GRÉGORY LAFITTE

Introduction

Various attempts at outlining, understanding and formalizing randomness have been carried out. One major approach stems from probability theory and statistics. It is based essentially on statistical properties such as stability of relative frequencies. Sequences produced by fairly tossing a coin is the core idea of random sequences. This approach merely describes the properties that should have a random sequence; it does not provide a definition or notion of randomness.

It should be mentioned that many people in statistics and probability object to thinking of points in a probability space as being random and prefer to talk of random processes for pickings points instead. (This viewpoint is the one of H. Rubin as expressed to A.H. Kruse in [11].) We tend to agree totally with this. It encourages us in thinking that randomness has not much to do with the theory of probabilities apart from the trivial statistical facts concerning "random objects". Nevertheless, it is certainly worthwhile to investigate where random objects appear (e.g. Rado's graph, randomness in complexity theory, ...) and find coherent randomness definitions verified by those objects.

The other major approach is of an algorithmic nature. It is sometimes mixed with the previous approach. This approach is based on *unpredictability*. It does provide some way to define randomness but then it is rather surprising to have algorithms involved since probability theory does not use the notion of algorithm. Is it then possible to find a mathematical definition for random sequences not based on algorithmic unpredictability?

Durand et al [5] propose such a definition by opting for a randomness whose strong properties are *relatively consistent* after showing that it is impossible to get a notion of randomness having *provably* those properties. In their definition, they have to take a basis for randomness and use "arithmetical randomness" to be just that. The algorithmic nature has then not completely disappeared from the definition. Other set-theoretical approaches are those of A.H. Kruse [11], with the use of an appropriate class theory instead of ZFC, and M. van Lambalgen [16], adding to ZFC an extra atomic predicate of randomness and some axioms which govern its use.

What is randomness after all? We could define randomness as the absence of any law. The problem is again in the fact that we will want (to be able to do something from the definition and not to get an inconsistency) the avoided laws to be definable in some way and somehow we will come back to some algorithmically-based definition.

Another way of presenting randomness is the complete *independence* between any two terms, or even only between any one term and its predecessors, of a random sequence. Usually some independence is sought by using some algorithmic method. We propose a method based completely on set-theoretic independence and its strong (but still unexplained) link with the theory of large cardinals. This has prompted more and more the author to believe in a strong connection between large cardinality concepts and randomness occurrences. This idea is somehow also at the basis of M. van Lambalgen's study in [16] apart from the fact that van Lambalgen searches for new axioms, giving predicates for randomness, to add to ZFC while we think the axioms are somewhat already there in the set theory literature.

Let us now proceed to a brief description of the contents of this paper. In the first section, we discuss classical definitions of randomness through a definition, using games, of Muchnik et al and obtain a simple characterization of this classic randomness using infinite time Turing machines. This is what we call the *unfeasibility approach*.

Received by the editors September 2001.

We then continue in section 2 by giving several methods making it possible to introduce some "non provable" randomness. We present Durand et al's method, generalize it and also introduce in the same direction some randomness notions, based on *independence* from ZFC, using original infinite time machines tailored to be able to capture all the properties of sets of reals. We call this the *unprovability approach*.

Using those notions, we construct in section 3 randomness notions hopefully meeting our goal. We call this the *unknowability approach*. Our ultimate randomness notion seems to be *unknowably randomness* (randomness definition 3.4) along randomness hierarchies 2.8 or 2.12. Surely, this is the strongest form one could wish for for a randomness notion since then there is no way (in our base theory ZFC or even in ZFC+$\exists$ some large cardinal) to *connect* any one value to the other values of such a random sequence.

Notations

In this paper, a sequence (as in *random sequence*) is an infinite binary sequence, i.e. belonging to $\{0,1\}^\omega$, which can also be seen as a real, i.e. belonging to $\mathbb{R}$. $\{0,1\}^{<\omega}$ is the set of finite sequences, which can also be seen as $\mathbb{N}$. For any $s \in \{0,1\}^{<\omega}$, $\{0,1\}^\omega_s$ denotes the set of infinite binary sequences that extend s. For a sequence a, a_k denotes the $k+1$-th term of the sequence.

1. Unfeasibility-based randomness

1.1. **Algorithmic randomness ...** Muchnik et al [15] have given various temptative definitions of randomness and compared them making all the while sure that they verify several properties that everyone believes a random sequence should verify. It turns out that the two most restrictive definitions of randomness are *chaotic* and *unpredictable*. The former is based on those sequences whose initial segments' entropies grow sufficiently fast. All chaotic sequences turn out to be unpredictable, the truth of the converse is an open question. Because every other known definition of randomness reduces to the notion of unpredictableness, we will use it as our base definition and we call it *Muchnik randomness*.

1.1. **Definition.** Let a be a sequence, $\mu : \{0,1\}^{<\omega} \to \mathbb{R}^+$ a computable quasi-measure[1] that we extend to intervals $\{0,1\}^\omega_s$ by having $\mu(\{0,1\}^\omega_s) = \mu(s)$ and $C \in \mathbb{Q}^{+\star}$ called the capital[2].

A one-player gambling game is played against the sequence a using the quasi-measure μ. We call it a *μ-game*. At the start of the game, the player has his wallet W_0 equal to C. At the k-th move, the player plays by giving $n = n(k)$ and a guessed value $i = i(k)$ for $a_{n(k)}$. As this is a gambling game, he also makes a bet $w = w(k) \in \mathbb{Q}^{+\star}$ such that $w(k) \leq W_{k-1}$.

If the player was incorrect about the guessed value, he loses his bet : $W_k = W_{k-1} - w(k)$. Otherwise

$$W_k = W_{k-1} + w(k)\frac{\mu(\mathfrak{A}_{1-i(k)})}{\mu(\mathfrak{A}_{i(k)})}$$

where for $j = 0, 1$,

$$\mathfrak{A}_j = \{a' \in \{0,1\}^\omega \mid a'_{n(k)} = j \text{ and } a'_{n(l)} = a_{n(l)} \text{ for } l = 1, 2, \ldots, k-1\}$$

The sequence a is called *μ-predictable* if there is computable winning strategy for winning μ-games against a. Otherwise, it is called *μ-unpredictable*.

a is *Muchnik random* if it is μ-unpredictable for some computable μ.

1.2. **Theorem.** *A Muchnik random sequence is Martin-Löf random*[3].

Proof. See theorem 7.4 in [15]. $\square$

[1] For any $s \in \{0,1\}^{<\omega}$, $\mu(s) = \mu(s \frown 0) + \mu(s \frown 1)$ and $\mu(\epsilon) = 1$ where ϵ is the empty sequence.

[2] Without loss of generality, we can assume $C = 1$.

[3] A sequence $x \in \{0,1\}^\omega$ is *Martin-Löf random* if it avoids all effectively null sets. It is one of the classical definitions of randomness. Algorithms appear in the word 'effectively'. For more on Martin-Löf randomness, see [14].

1.2. **. . . and infinite time machines.** Finite automata on infinite sequences have been introduced by Büchi in [2] to prove the decidability of the monadic second order theory of $\langle \omega, < \rangle$. Büchi automata differ from finite automata on finite sequences only by its condition of acceptance of a word. A word is *accepted* by a Büchi automata if and only if the set of states, through which the automata goes an infinite number of times during an *execution* (there may be several executions if the automata is nondeterministic), contains at least a final state. Then Büchi introduced in [3] finite automata that are able to describe transfinite sets of sequences. Using those automata, he proved the decidability of the monadic second order theory of $\langle \alpha, < \rangle$, where α is a countable ordinal. It featured special transitions for limit ordinal stages such that the state reached at that limit stage ξ depends only on previously reached states $\{s \in S \mid \forall \beta < \xi \, \exists \gamma > \beta \, \varphi(\gamma) = s\}$. He modified again the definition, using still other special transitions for particular limit ordinal stages, to use those automata to prove the decidability of the monadic second order theory of $\langle \omega_1, < \rangle$. For a survey of Büchi automata, see [4].

In [12], we defined a variant of Büchi automata making it as powerful as infinite time Turing machines as defined by Hamkins and Lewis in [7]. We will now propose a definition of machines working with infinite time on reals but with access to transfinite tapes. It borrows ideas from Büchi automata deciding the monadic second order theory of $\langle \omega_1, < \rangle$ and $\mathcal{W}^2$-automata as studied in [12]. Much of the idea about the use of *stationary*[4] *sets* is due to Menachem Magidor.

1.3. **Definition.** Fix a $n \in \mathbb{N}$. We will work with time and tapes of cardinality[5] $\aleph_n$.

An *enhanced tape* is a function from ω_n to $\{0, 1\}$.

A *continuum machine*, or $\mathfrak{c}$-*machine*[6], is a Turing machine with $k \geq 3$ separate enhanced tapes, one for input, $k - 2$'s for scratch work, and one for output. The scratch and output tapes are filled with zeros at the beginning of any computation. At non-limit stages, it behaves like a normal Turing machine according to its transition relation. At limit stages, if the transition says so, the head is plucked from wherever it might have been racing towards, and placed on top of the first cell. Moreover, it enters a *limit state.* For a given cell of the tape, at a limit stage it takes the value of the lim sup of the cell values before the limit.

A $\mathfrak{c}$-machine distinguishes different kinds of limit states. At a limit stage, it is in a composition of limit states

$$\mathfrak{Q}_0 \times \mathfrak{Q}_1 \times \cdots \times \mathfrak{Q}_n$$

where each $\mathfrak{Q}$ is defined as

$$\mathfrak{Q}_i = \{q \in Q \mid \exists \alpha \text{ of cofinality } \omega_i \text{ with } \{\beta < \alpha \mid q_\beta = q\} \text{ stationary in } \alpha\}$$

A $\mathfrak{c}$-automaton is a $\mathfrak{c}$-machine that only reads and never writes.

The output of a $\mathfrak{c}$-machine can be considered as a real when considering only the "first" ω terms of the tape. Assuming the very reasonable "$2^{\aleph_0} < \aleph_\omega$", with this definition of continuum machines, we can effectively work on $\mathbb{R}$ using and comprehending completely its *power*, i.e. properties concerning sets of reals.

It is clearly a generalization of infinite time Turing machines[7] and by the simple techniques used in [12], has at least the same of power of computation. Hence the following theorem also applies to $\mathfrak{c}$-machines.

1.4. **Theorem.** *If $r \in \mathbb{R}$ is not writable by an infinite time Turing machine, then it is Muchnik random.*

Proof. Take $r \in \{0, 1\}^\omega$ such that it is not Muchnik random. For every computable measure μ, there is thus a strategy to win the μ-game. The strategy is necessarily computable by an infinite time Turing machine.

We translate the strategy in an infinite time Turing machine, that will be able to write r since the strategy generates winning games. □

Theorem 1.4 is our cornerstone theorem for characterizing simple randomness in terms of machine computability of reals.

---

[4] See definition 2.4.

[5] For any ordinal α : $\aleph_\alpha$ denotes the α-th cardinal and ω_α is the smallest ordinal of cardinality $\aleph_\alpha$. Following von Neumann, we identify an ordinal β with the set of ordinals $\alpha < \beta$.

[6] $\mathfrak{c}_n$-machine to indicate that we work on $\aleph_n$.

[7] An *infinite time Turing machine* is a $\mathfrak{c}$-machine (with $k = 3$) working with countable tapes and (of course) countable time. The difference with $\mathfrak{c}$-machines is in the limit stages' behaviour : It is placed in a special unique *limit state.* For a given cell of the tape, at a limit stage it takes the value of the lim sup of the cell values before the limit.

The following theorem is the Lost Melody Theorem of [7]. It shows for our purpose that Muchnik random reals are not so much *random* as they can be recognized as such.

1.5. **Theorem.** *There are random reals that are still singleton recognizable by infinite time Turing machines.*

Proof. We sketch the proof.

Consider the ordinal stages of repeat-points, that is by which it either halts or repeats, of computations with a null input. Let δ be the supremum of those repeat-points. By the nature of infinite time Turing machines, δ is a countable ordinal in L, Gödel's class of constructible sets. Let $\beta_0 = \delta$, β_n be a countable ordinal appearing first in $L_{\beta_{n+1}}$ (not in L_{β_n}) and $\beta = \sup_n \beta_n$. β is then the smallest ordinal $\geq \delta$ such that $L_{\beta+1} \models \beta$ is countable.

Since $L_{\beta+1}$ has a canonical well-ordering, there is some real $r \in L_{\beta+1}$, which is least with respect to the canonical L order, such that r codes β. r is the real we are looking for.

r is not writable because if it were, then we could solve the halting problem by searching for a real, appearing at some moment on a tape, that codes an ordinal large enough to see the repeat-point of the computation in question. Since r codes β, which is as large as δ, r is big enough and so our algorithm succeeds. And this contradicts the undecidability of the halting problem.

By usual techniques for coding the L_α's, $\{r\}$ is decidable : given a real, one must verify that it codes an ordinal, that this ordinal is larger than δ and then by the coding techniques, check whether our real really is the least code in $L_{\alpha+1}$ for some α and whether α really is the least ordinal above δ such that α is countable in $L_{\alpha+1}$. □

We now have a way of obtaining randomness through the use of infinite time machines. How can we get stronger notions of randomness, while not excluding reals that are actually random?

One way is by fixing some strong requirements for our randomness notion; so strong that there is no such notion. We then loosen up the conditions by requiring that "the randomness notion satisfies the requirements" is merely relatively consistent. This is the Durand et al approach. We can actually try to go on like this and obtain stronger and stronger notions. We will go through this method in the following section and apply it to other randomness notions than the Durand et al one. The main problem of this way of obtaining stronger randomness is that it has to be based on another randomness notion and this, of course, doesn't help in obtaining a non-algorithmical and *independence*-based randomness notion.

Another way is by having more powerful infinite time machines. We must however make sure that the gain in power is really a gain in excluding non-random reals. This will be the second part of the following section.

2. Unprovability-based randomness

2.1. **Durand et al.** Durand et al in [5] were looking for a non-algorithmically-based randomness definition. They proposed the following definition.

2.1. **Definition.** Let x be a infinite binary sequence.

x is *Solovay random* over L if it avoids any null G_δ (countable intersections of open sets) set with a code[8] in L. We note ρ_L the predicate for this randomness, and $R_L = \{x \in \{0,1\}^\omega \mid \rho_L(x)\}$.

x is *arithmetically random* if it avoids any null arithmetically coded G_δ set. We have also the similar notations ρ_A and R_A.

x is *consistently random* if $x \in R_A$ and if R_L is of full measure, then $x \in R_L$. We have also the similar notations ρ_C and R_C.

A randomness predicate ρ is said to be *consistent* if it verifies the following conditions :

- **(1):** ZFC proves that $\{x \in \{0,1\}^\omega \mid \rho(x)\}$ is a full set;
- **(2):** $\forall \Psi(x)$, if ZFC proves that $\{x \in \{0,1\}^\omega \mid \Psi(x)\}$ is null, then ZFC does not prove that there is an $x \in \{0,1\}^\omega$ satisfying $\rho(x) \wedge \Psi(x)$;
- **(3):** ZFC proves that $\forall x \in \{0,1\}^\omega$, if $\rho(x)$, then x is Martin-Löf random.

[8] $C \subseteq \omega \times 2^{<\omega}$ is a code for a G_δ set $U \subseteq \{0,1\}^\omega$ if $U = \bigcap_n \bigcup_{\langle n,u\rangle \in C} \{0,1\}^\omega_u$.

2.2. **Theorem.** *In the Solovay model*[9], R_L *is a full* G_δ *set and* ρ_L *verifies* $\mathbf{(2)}$[10].

2.3. **Corollary.** ρ_C *is a consistent randomness.*

Proof. ρ_C satisfies obviously $\mathbf{(1)}$ and $\mathbf{(3)}$ because of theorem 2.2 and of the definition of arithmetical randomness.

In the Solovay model, R_L is of full measure, so $\rho_C(x) \implies \rho_L(x)$. Hence ρ_C satisfies $\mathbf{(2)}_{\text{plain}}$. □

This study prompts a way of obtaining always finer randomness notions.

Take a randomness predicate ρ and the corresponding set of random sequences R. Set some requirements (predicates $\{P_1, P_2, \dots, P_k\}_{k\geq 2}$) for the quality of randomness desired. To be able to operate our method, R has to verify the requirements *only* in a certain model. Fix an $l \leq k$, the new randomness predicate ρ' (R') is the *consistent realisation* of ρ on top of some randomness notion ρ_{base}, noted ${\rho_{\text{base}}}^{\rho}$ and it is defined by :

$$\rho'(x) \text{ if and only if } x \in R_{\text{base}} \text{ and if } P_l(R), \text{ then } x \in R$$

This is what Durand et al did. We can go even further[11] by then defining the following randomness notion ρ^+, noted ${\rho_{\text{base}}}^{\rho}_{+}$:

$$\rho^+(x) \text{ if and only if } x \in R_{\text{base}} \text{ and if } \text{cons}(P_l(R)), \text{ then } x \in R'$$

And we can continue like that and obtain[12] ρ^{++} $({\rho_{\text{base}}}^{\rho}_{++})$, ρ^{+3} $({\rho_{\text{base}}}^{\rho}_{+3})$, ... The drawback is that we don't know much of the obtained gain in strongness for our randomness notion. We will complement this idea in the second part of this section.

The Durand et al randomness is based on unprovability on top of common randomness notion. Do we really still need this arithmetical/computational basis for randomness? We aim at answering this question in section 3. But first, we look for still stronger randomness notions with a precise measure of the gain.

2.2. **More unprovability-based randomness.** $\mathfrak{c}$-machines have very peculiar properties and we will base some new randomness notions on them. To reach those notions, we need to introduce some set-theoretical material.

An uncountable cardinal number κ is *inaccessible* if it is regular and a strong limit cardinal. An immediate consequence of inaccessibility is that V_κ, the collection of all sets of rank less than κ, is a model of ZFC; another immediate consequence is that $\kappa = \aleph_\kappa$ is a fixed point of the aleph sequence. By Gödel's second incompleteness theorem, it follows that the existence of inaccessible cardinals is unprovable in ZFC. In fact, a slightly more involved argument shows that the relative consistency of inaccessible cardinals is unprovable. Thus the existence of inaccessibles is to ZFC as the existence of an infinite set is to Peano arithmetic. For that reason, large cardinal axioms are sometimes referred to as *strong axioms of infinity*.

Modern larger cardinal theory recognizes a substantial number of large cardinal axioms. Interestingly enough, these axioms form a linearly ordered scale, on which the relation of a stronger axiom to the weaker theories is just as described above in the case of inaccessible cardinals and ZFC. This scale of large cardinals serves as a measure of consistency strength of various set theoretic assumptions.

One of those large cardinals is a *weakly compact* cardinal and we introduce them now. Every weakly compact is not only inaccessible, but on the scale of large cardinals is also above Mahlo cardinals. Among large cardinals stronger than weakly compact cardinals and even Woodin and measurable cardinals, *supercompact* cardinals are most prominent. Above supercompact and huge cardinals, the scale approaches its end with the existence of a non-trivial elementary embedding $j : V_\lambda \to V_\lambda$, as by a theorem of Kunen, $j : V \to V$ is inconsistent. For more on large cardinals and set theory at large, see [8].

2.4. **Definition.** Let κ be a regular uncountable cardinal. We call a set $C \subseteq \kappa$ *closed unbounded* in κ if

(1) for every sequence $\alpha_0 < \alpha_1 < \cdots < \alpha_\xi < \cdots$ $(\xi < \gamma)$ of elements of C, of length $\gamma < \kappa$, we have $\lim_{\xi\to\gamma} \alpha_\xi \in C$ (closed);

[9] Let $\mathcal{M}$ be a transitive model of ZFC and let κ be an inaccessible cardinal in $\mathcal{M}$. The Solovay model is $\mathcal{M}[G]$ where G is an $\mathcal{M}$-generic ultrafilter on P, the notion of forcing that collapses each $\lambda < \kappa$ onto $\aleph_0$.

[10] Actually, it verifies $\mathbf{(2)}_{\text{plain}}$: $\forall\Psi(x)$, if $\{x \in \{0,1\}^\omega \mid \Psi(x)\}$ is null, then there is no $x \in \{0,1\}^\omega$ satisfying $\rho(x) \wedge \Psi(x)$.

[11] If $P_l(R)$ is relatively consistent $(\text{cons}(P_l(R)))$, there is a model in which $P_l(R)$ is true. Living in this model, we can now consider taking R' instead of R in our "then $x \in R$". And so on...

[12] $\rho^{++}(x)$ if and only if $x \in R_{\text{base}}$ and if $\text{cons}(\text{cons}(P_l(R)))$, then $x \in R^+$

(2) for every $\alpha < \kappa$, there is $\beta > \alpha$ such that $\beta \in C$ (unbounded).

We say that $S \subseteq \kappa$ is *stationary* in κ if $S \cap C \neq \emptyset$ for every closed unbounded subset C of κ.

A cardinal κ is *weakly compact* if it is uncountable and satisfies the partition property $\kappa \to (\kappa)^2$.

Jensen [10] proved the following :

2.5. **Theorem.** *Assuming $V = L$, a regular cardinal κ is weakly compact if and only if for every stationary $A \subseteq \kappa$, such that every $\alpha \in A$ is of cofinality ω, $\{\alpha \mid cf(\alpha) > \omega, \alpha < \sup A,$ and $A \cap \alpha$ is a stationary subset of $\alpha\} \neq \emptyset$.*

Baumgartner [1] studied the question for $\kappa = \aleph_2$ and obtained a relative consistency result with ZFC+"$\exists$ weakly compact cardinal". Magidor in [13] obtained an equiconsistency result that we use to prove the following theorem.

2.6. **Theorem.** *There is a $\mathfrak{c}_2$-machine $\mathfrak{M}$ such that the ouput real $\mathfrak{r}$ of $\mathfrak{M}$ (on a blank input) is such that "$\mathfrak{r} \neq 0$" is equiconsistent with the existence of a weakly compact cardinal.*

Proof. From the study in [6], we can easily construct a $\mathfrak{c}_2$-automaton such that the language recognized by this automaton is non empty if and only if $\{\alpha < \omega_2 \mid \mathrm{cf}(\alpha) = \omega_1$ and $\alpha \cap X$ is stationary in $\alpha\}$ is non empty for every $X \subseteq \{\alpha < \omega_2 \mid \mathrm{cf}(\alpha) = \omega_0\}$. We can code this language (or a countable part of it) in a real $\mathfrak{r}$ such that $\mathfrak{r} \neq 0$ if and only if the language is not empty. Using Baumgartner's and Jensen's results (theorem 2.5), it is clear that "$\mathfrak{r} \neq 0$" is independent of ZFC.

Using Magidor's result in [13], in the same manner, we construct a $\mathfrak{c}_2$-automaton such that "$\mathfrak{r} \neq 0$" is equiconsistent with the existence of a weakly compact cardinal. □

The first part of theorem 1.5 can be extended[13] to general $\mathfrak{c}$-machines to give finer randomness definitions.

2.7. *Remark.* We can also get the other half of theorem 1.5 by using core model theory but we won't enter into such troubled waters. It is important to notice that this second part of the theorem tells us that somehow there will always be some reals non writable by such machines that will not be really random (because they are singleton recognizable) and that we always need to seek a stronger randomness. This, of course, prompts the importance of the randomness notions of the last section.

2.8. **Randomness notion.**

$$\mathfrak{r} \in \{0,1\}^\omega \text{ is } \mathfrak{c}_n\text{-random if it is not writable by a } \mathfrak{c}_n\text{-machine}$$

2.9. **Corollary.** *$\mathfrak{c}_3$-randomness is strictly stronger than $\mathfrak{c}_2$-randomness*

Proof. $\mathfrak{c}_3$ can decide and thus write $\mathfrak{r}$ from theorem 2.6. The nice thing is that the gain in randomness is quantified by a "$\exists$ weakly-compact cardinal". □

Jech and Shelah [9], using supercompact cardinals, generalized Magidor's result to $\aleph_n$ and that enables us to prove the following.

2.10. **Theorem.** *For any $n \in \mathbb{N}$, there is a $\mathfrak{c}_n$-machine $\mathfrak{M}$ such that the ouput real $\mathfrak{r}$ of $\mathfrak{M}$ (on a blank input) is such that "$\mathfrak{r} \neq 0$" is implied by the existence of n supercompact cardinals.*

Proof. In the same way as in theorem 2.6, using the generalization of Magidor's result by Jech and Shelah, we can construct for any $n \in \mathbb{N}$ a suitable $\mathfrak{c}_n$-automaton and obtain the required $\mathfrak{r}$. □

2.11. **Theorem.** *The hierarchy of randomness given by the hierarchy of $\mathfrak{c}$-machines is strict.*

Proof. "$\exists\, n+1$ supercompact cardinals" is stronger consistency-wise than "$\exists\, n$ supercompact cardinals". □

We can consider taking those mysterious reals $\mathfrak{r}$ (of theorems 2.6 and 2.10) as oracles for our $\mathfrak{c}$-machines. We are not sure if there is a gain in randomness doing this.

But one can still do as in the first part of this section and define for any $m \in \mathbb{N}$:

2.12. **Randomness notion.** ${\rho_A}^{\rho_{c_n}}_{+m}$ using as the P_l requirement: "$\exists\, n$ supercompact cardinals"

or perhaps more interestingly, ${\rho_{c_n}}^{\rho_A}_{+m}$ using as the P_l requirement: "$\nexists\, n$ supercompact cardinals".

---

[13]by replacing in the proof each occurrence of the L_α's by V_α's.

The advantage of the latter notion is that we are guaranteed, with the randomness base ρ_A, not to put aside any real that should be considered as *random*.

2.13. *Remark.* Note that ${\rho_A}^{\rho_{c_{n+1}}}$ is a stronger notion than $\rho_{A^+}^{\rho_{c_n}}$.

3. Unknowability-based randomness

The previous randomness notions still lack the *unknowability* (using *independence* from ZFC) that we are looking for.

We propose a hierarchy of randomness definitions based on the results of the previous section using the large cardinal *empirical* hierarchy.

3.1. **Randomness notion.** A real $\mathfrak{x} \in \{0,1\}^\omega$ is a large cardinal random real if there is a $\mathfrak{c}$-machine $\mathfrak{M}$ with metamathematical[14] ouput $\mathfrak{x}$ such that in ZFC, "the ouput real of $\mathfrak{M}$ is non zero" is equiconsistent with the existence of a large cardinal.

It is clearly quite, and perhaps too, restrictive but at least the notion is really of the "unknowable" nature and is not based on algorithmic notions. It has also the advantage of relying on the only well-understood notion of "objects beyond ZFC", i.e. large cardinals.

Using the "unknowable" method, the most natural definition seems to be

3.2. **Randomness notion.** Each bit is *unknowable* from the previous ones : $\mathfrak{x} \in \{0,1\}^\omega$ is *increasingly unknowably random* if there is countable family of propositions $\{Q_i\}_{i\in\mathbb{N}}$ such that

$$\forall n \in \mathbb{N}, \quad Q_n \text{ is independent of ZFC} + \bigwedge_{i<n} Q_i$$

and

$$\mathfrak{x}_i = \begin{cases} 1 & \text{if } Q_i \text{ is } \textit{true}, \\ 0 & \text{otherwise.} \end{cases}$$

It is not an effective definition but it can be in part realized using $\mathfrak{c}$-machines : let Q_i be "$\mathfrak{r}_i$ is null", where $\mathfrak{r}_i$ is the problematic real for $\mathfrak{c}_i$-machines in theorem 2.10.

We can propose a variant of this definition by requiring that

$$\forall n \in \mathbb{N}, \quad Q_n \text{ is independent of ZFC} + \bigwedge_{i\neq n} Q_i$$

but we don't know of any realization of such a strong definition.

From our different hierarchies of randomness of the previous section, we can define an *unknowable* randomness by using *generic sets*.

3.3. **Definition.** Let $\langle \mathbb{P}, \leq, \mathbf{1}\rangle$ be a partial order.

(1) $D \subset \mathbb{P}$ is *dense* in $\mathbb{P}$ iff $\forall p \in \mathbb{P}\, \exists q \leq p\, q \in D$.
(2) $G \subset \mathbb{P}$ is a *filter* in $\mathbb{P}$ iff
  (a) $\forall p, q \in G\, \exists r \in G\, r \leq p \wedge r \leq q$,
  (b) $\forall p \in G\, \forall q \in \mathbb{P}\, q \leq p \to q \in G$.
(3) G is $\mathbb{P}$-*generic* on $\mathbb{D}$ iff G is a filter on $\mathbb{P}$ and for all $\mathbb{P}$-dense $D \in \mathbb{D}$, $D \cap G \neq \emptyset$.

The existence of a generic set for a particular partial order $\mathbb{P}$ is not necessarily trivial. Nevertheless there is a much studied proposition that guarantees us (if, of course, we suppose it to hold) that most of the generic sets that we consider exists. It is called Martin's Axiom and it is independent of ZFC. See [8] for more on this.

Fix a strict randomness hierarchy $\{\rho_i^H\}_{i\in\mathbb{N}}$ ($\{R_i^H\}_{i\in\mathbb{N}}$) from the previous section. Take for partial order $\mathbb{P}$ the set $\subset \{0,1\}^\omega$ of infinite binary random sequences (somewhere in our fixed randomness hierarchy) with the order $\prec$:

$$p \prec q \text{ iff } \hat{p} > \hat{q} \text{ and there is } i > 0 \text{ such that } p \restriction_{\mathbb{N}\setminus\{0,\dots,i-1\}} = q$$

where $\hat{p}$ is the smallest n such that $p \in R_n^H$.

[14] the *truth* about the ouput of $\mathfrak{M}$.

3.4. **Randomness notion.** Fix a hierarchy of randomness notions whose strictness is according to the hierarchy of some large cardinals. $\mathfrak{x} \in \{0,1\}^\omega$ is *unknowably random along* this hierarchy if $\mathfrak{x}$ is the *union*[15] of a $\langle \mathbb{P}, \prec \rangle_{\{\rho_i^H\}_{i\in\mathbb{N}}}$-generic set.

If we take for example the randomness hierarchy definition 2.8, by the previous randomness definition, we obtain random sequences where each bit is *unknowable* from the other ones in the strong sense that the hierarchy is strict because of the supposed strictness of the hierarchy of the large cardinals used. It thus has the advantage of being in compliance with classical notions of randomness while making sure it verifies our "unknowability" requirement.

Acknowledgements

We wish to express our gratitude to Menachem Magidor for all his thoughtful ideas about infinite time machines and for pointing out the article [6] of Yuri Gurevich, Saharon Shelah and himself. We are also greatly indebted to Jacques Mazoyer for his advices, his availability and his never-failing enthusiasm.

References

1. J. E. Baumgartner, *A new class of order types*, Annals of Mathematical Logic **9** (1976), 187–222.
2. J. R. Büchi, *On a decision method in the restricted second-order arithmetic*, Logic, Methodology, and Philosophy of Science: Proc. **1960** Intern. Congr., Stanford University Press, 1962, pp. 1–11.
3. ______, *Decision methods in the theory of ordinals*, Bulletin of the American Mathematical Society **71** (1965), 767–770.
4. ______, *The monadic second-order theory of ω_1*, Decidable theories. II (Siefkes Büchi, ed.), Lecture Notes in Mathematics, vol. 328, Springer-Verlag, Berlin and New York, 1973, pp. 1–127.
5. B. Durand, V. Kanovei, V. A. Uspensky, and N. Vereshagin, *Do stronger definitions of randomness exist?*, Theoretical Computer Science (2001), to appear.
6. Y. Gurevich, M. Magidor, and S. Shelah, *The monadic theory of ω_2*, Journal of Symbolic Logic **48** (1983), no. 2, 387–398.
7. J. D. Hamkins and A. Lewis, *Infinite time Turing machines*, Journal of Symbolic Logic **65** (2000), no. 2, 567–604.
8. T. Jech, *Set theory*, Academic Press, New York, 1978.
9. T. Jech and S. Shelah, *Full reflection of stationary sets below $\aleph_\omega$*, Journal of Symbolic Logic **55** (1990), 822–830.
10. R. B. Jensen, *The fine structure of the constructible hierarchy*, Annals of Mathematical Logic **4** (1972), 229–308.
11. A. H. Kruse, *Some notions of random sequence and their set-theoretic foundations*, Zeitschift mathematische Logik und Grundlagen der Mathematik **13** (1967), 299–322.
12. G. Lafitte, *How powerful are infinite time machines?*, Thirteenth International Symposium on Fundamentals of Computation Theory (Rusins Freivalds, ed.), Lecture Notes in Computer Science, Springer-Verlag, August 2001, to appear.
13. M. Magidor, *Reflecting stationary sets*, Journal of Symbolic Logic **47** (1982), no. 4, 755–771.
14. P. Martin-Löf, *The definition of random sequences*, Information and Control **9** (1966), 602–619.
15. An. A. Muchnik, A. L. Semenov, and V. A. Uspensky, *Mathematical metaphysics of randomness*, Theoretical Computer Science **207** (1998), 263–317.
16. M. van Lambalgen, *Independence, randomness, and the axiom of choice*, Journal of Symbolic Logic **57** (1992), 1274–1304.

Ecole Normale Supérieure de Lyon,, Laboratoire de l'Informatique du Parallélisme,, 46 allée d'Italie, 69364 Lyon Cedex 07, France, Fax: (33) 4 72 72 80 80

E-mail address: glafitte@ens-lyon.fr

[15] By definition of $\prec$, all the infinite sequences are mutually compatible. There is a sequence that *contains* all of them, called the union.