Do stronger definitions of randomness exist ?

Bruno Durand * Vladimir Kanovei †
Vladimir A. Uspensky ‡ Nikolai Vereshchagin‡§

September 9, 2002

Abstract

In this paper, we investigate refined definition of random sequences. Classical definitions (Martin-Löf tests of randomness, uncompressibility, unpredictability, or stochasticness) make use of the notion of algorithm. We present alternative definitions based on set theory and explain why they depend on the model of **ZFC** that is considered. We also present a possible generalisation of the definition when small infinite regularities are allowed.

Prolegomena

It is rather surprising that algorithms are involved for defining random sequences since probability theory does not use the notion of algorithm. Thus we try in this paper to propose definitions based only on set theory. We first explain why it is not so easy: we prove that direct definitions (based on the notion of provably null sets) cannot exist. Thus we propose a definition based on consistency. With this definition the set of random sequences depends upon the model of **ZFC** we consider. We also propose a notion of invariant rondomness in which small infinite regularities are allowed to occur. Although some techniques and tools of set theory (Solovay models, *etc.*) are involved, this paper is not focused

* L.I.P., Ecole Normale Supérieure de Lyon, 46 Allée d'Italie, 69364 Lyon Cedex 07, France. `Bruno.Durand@ens-lyon.fr`.

† Moscow Transport Engineering Institute, `kanovei@mech.math.msu.su`. Supported by DFG and University of Wuppertal.

‡ Dept. of Mathematical Logic and Theory of Algorithms, Faculty of Mechanics and Mathematics, Lomonosov Moscow State University, Vorobjyovih Gorih, Moscow 119899, Russia, `uspensky@lpcs.math.msu.ru`.

§ Work done at L.I.P., Ecole Normale Supérieure de Lyon. `ver@mech.math.msu.su`.

on set theory. Even sketching some arguments (mostly known in set theoretic literature), we are confident that it is not necessary to be an expert on set theory to take benefit of the theorems and notions considered. Our goal will be to understand how far the notion of algorithm is necessary to define randomness and what kind of other definition can be or cannot be proposed.

1 Introduction

If somebody tells us that he has tossed a coin infinitely many times getting the sequence

$$0001000101000100000001000101000001000101010... \qquad (*)$$

where each even term is 0, we will most likely be ready to suspect fraudulence. Why? Our disbelief that the sequence is really random can be expressed in different terms: for instance, it contains too much regularities to be really random, or that it is "predictable" [1], or that it has more zeros than ones thus violating the Law of Large Numbers, but essentially any explanation amounts to the following: *the sequence is not random because it belongs to a simply defined set of strings of Lebesgue measure* 0.

Towards more rigorous presentation, let us define $\Omega = 2^{\mathbb{N}}$, the set of all infinite binary sequences. The Lebesgue, or uniform, measure in Ω, denoted by $\mathtt{mes}$, is the product of $\mathbb{N}$-many copies of the measure on the 2-element set $\{0,1\}$ giving the value $1/2$ to both $\{0\}$ and $\{1\}$. A *null set* is any set $X \subseteq \Omega$ with $\mathtt{mes}\, X = 0$. Complements of null sets, *i. e.*, sets of measure 1, are *full sets*.

Coming back to the discussion above, we may conclude that a reasonable notion of a random element of Ω must infer that random sequences avoid all "essential" null sets in Ω, or, what is the same, must belong to all "essential" full sets. The key issue is which sets should be viewed as "essential" here. Of course those cannot be all (null and full) sets, because then there would be no random sequences at all. As a matter of fact, there is no other reasonable opportunity to provide the existence of random sequences except for taking a *countable* family E of "essential" subsets of Ω. Then, we can define a sequence $x \in \Omega$ to be *random in the sense of* E iff it avoids any null set $X \in E$. The set R of all random sequences is, of course, full. The larger family E we take the more refined notion of randomness we obtain and the stronger is our belief that any random sequence can be obtained by fair coin tossing.

An important definition of this kind, given by Martin-Löf [8], is as follows. Let Ω_u denote the set of all infinite continuations of a finite string u. Recall that

[1] For example, if a casino plays this sequence in a gambling where we can bet any amount of money within $\$1$ on the next term of the sequence, we shall win as much as we want after sufficient number of moves.

$A \subseteq \Omega$ is a null set if it can be covered by an open set (in Cantor's topology) of arbitrarily small measure, that is, for any n, there is a set B_n of finite strings such that 1) $A \subseteq \bigcup_{u \in B_n} \Omega_u$ and 2) $\sum_{u \in B_n} \mathtt{mes}\,(\Omega_u) = \sum_{u \in B_n} 2^{-l(u)} < 1/n$. A set A is called *effectively null* if there exists a sequence B_n satisfying 1) and 2) such that the set $\{\langle u, n\rangle : u \in B_n\}$ is recursively enumerable. According to Martin-Löf, a sequence in Ω is *random* if it avoids all [2] effectively null sets. For instance the sequence $(*)$ above is not random: indeed, it belongs to the effectively null set of all sequences x such that $x(n) = 0$ for all even n. Note that the family of all effectively null sets is countable, as any its element is identified by an algorithm and the number of algorithms is countable.

It turns out that usual laws of probability theory, *e. g.*, the law of large numbers (the frequency of zeros among first n terms tends to $1/2$) or the law of the iterated logarithm, are satisfied by any Martin-Löf random sequence, simply because the set of all counterexamples can be covered by an effectively null set. Yet the Martin-Löf definition does not encounter all possible infinite regularities which a really random sequence should avoid. For instance a simple diagonal construction yields a particular, definable Martin-Löf random sequence while our intuition refuses to accept any definable sequence to be random.

The aim of our paper is to present more refined definitions of randomness, in part known from modern set theory. We shall assume some surface acquaintance with Zermelo – Fraenkel set theory **ZFC**, including a belief that it is an adequate foundation of mathematics. It will be a separate chapter (Section 5) which introduces some different opportunities in the study of the notion of randomness, related to *invariant* randomness.

2 Set theoretic approach to randomness

The Martin-Löf definition is an example of randomness definitions which describe the "essential" null sets (*i. e.*, those to be avoided) in terms of a fixed notion of definability. (We treat "to be a r. e. set" as a kind of definability.) Taking more broad concepts of definability, we obtain, generally speaking, stronger notions of randomness. For instance, one defines a sequence $x \in \Omega$ to be *arithmetically random* iff it avoids all arithmetically coded null sets (see Section 4). Then many Martin-Löf random sequences, in particular all aritmetically definable among them, become arithmetically non-random.

However we shall still have *hyperarithmetically* definable arithmetically random sequences. Moreover, whichever particular notion of definability we take, there will be random, in this sense, sequences, definable in some other sense.

[2] One can consider only some particular effectively null sets here. This restricted approach leads to notions of *chaotic*, *unpredictable*, and *stochastic* sequences, see [9, 11, 12].

This persuades us to think how to incorporate the most general set theoretic definability as a whole. In view of this discussion, a perfect notion $\rho(x)$ of a random sequence would be a notion satisfying two principles:

(1) **ZFC** proves that the set of all random sequences is a full set.

(2) For any formula $\Psi(x)$ such that **ZFC** proves that the set $\{x \in \Omega : \Psi(x)\}$ is null, it is provable, in **ZFC**, that no random sequence satisfies $\Psi(x)$.

(*Formula* means a set theoretic formula unless otherwise indicated.) However

Theorem 1 *There does not exist a formula ρ satisfying both* (1) *and* (2).

Proof [3] Suppose that ρ is such a formula.

The argument is based on ideas connected with the Gödel constructibility. Gödel defined in 1938 a class L of sets called *constructible sets* and proved that L is a model of **ZFC**. The statement that all sets are constructible is called *the axiom of constructibility* and formally abbreviated by the equality $\mathrm{V} = \mathrm{L}$, where V denotes the universe of all sets. The axiom $\mathrm{V} = \mathrm{L}$ was proved to be consistent with **ZFC** by Gödel (the key fact is that $\mathrm{V} = \mathrm{L}$ is true in the class L) and independent from **ZFC** by Cohen in 1961. [4]

The most important here property of L is that there is a well-ordering $<_{\mathrm{L}}$ of L, definable by a concrete set theoretic formula.

Let $\psi(x)$ say the following: $x \in \Omega$ is the $<_{\mathrm{L}}$-least element x_0 of the set $\{x \in \Omega \cap \mathrm{L} : \rho(x)\}$, if the latter is non-empty, and $x(n) = 0$ for all n otherwise. Obviously **ZFC** proves that there is only one $x \in \Omega$ satisfying $\psi(x)$; hence, by (2), **ZFC** proves that $\psi(x)$ contradicts $\rho(x)$. However the axiom $\mathrm{V} = \mathrm{L}$ (which is consistent with **ZFC**) implies, by (1) [5], that there is a sequence x satisfying $\rho(x)$ and $\psi(x)$ — namely, the x_0 defined above. □

This drawback can be fixed at the cost of employment of non-**ZFC** means. This can be, for instance, an appropriate class theory, as in [5]. Myhill (see [7]) handled the problem adding to **ZFC** an extra atomic predicate of randomness and some axioms which govern its use. Another, even more exotic opportunity

[3] A modification of an argument by Myhill which shows that (1) is incompatible with a stronger version of (2) saying that, for any set theoretic formula $\Psi(x)$, **ZFC** proves that if the set $\{x \in \Omega : \Psi(x)\}$ is of full measure then all random sequences satisfy $\Psi(x)$. The argument first appeared in [5], p. 321; see [7] for more on Myhill's approach.

[4] We refer to [3, 6] in matters of all general set theoretic facts used below as well as in matters of the history of related set theoretic studies.

[5] We actually need only that **ZFC** proves the existence of at least one random sequence.

is to employ a nonstandard set theory estending **ZFC**, to define a sequence to be random iff it avoids any *standard* null set, as in [4].

However, our requirements should be moderated, as long as we keep committment not to leave the **ZFC** ground. Our proposal to this end, which seems to be a new one, is to consider the following weaker form of principle (2):

(2′) For any formula $\Psi(x)$, if **ZFC** proves the set $\{x : \Psi(x)\}$ to be null, then **ZFC** does <u>not</u> prove that there <u>is</u> a random sequence satisfying $\Psi(x)$.

Informally, the principle states that no one will ever prove that a particular law of probability theory is not satisfied by some random sequence. In particular, any notion of random sequence satisfying (2′) is resistant to the above critics of Martin-Löf randomness. These are, however, not all the requirements we find necessary to impose on a notion of randomness. The point is that the principles (1) and (2′) do not imply, that the sequence (say) 000000000000000...... is not random. Principle (2′) implies, of course, that one cannot prove that it is random. But we expect that such laws as "not to be identically zero" should be proved. This leads us to the third principle:

(3) **ZFC** proves that any random sequence is arithmetically random, hence, Martin-Löf random, too.

We face here the same problem: the choice of arithmetical randomness, as the bottom level, is not well motivated. However, our construction applies to any previously specified amount of definability: for any definable provably countable family of provablynull sets there is a notion of randomness satisfying (1) and (2′), and such that is is provable that any random sequence avoids all those sets.

Our main result (see Section 4) will be a notion of randomness which satisfies (1), (2′), (3). This notion will comprise two distinct notions: the Solovay randomness and the arithmetical randomness. The key point is that is is *consistent* that the Solovay randomness satisfies both (1) and (2). This allows to define the "aggregate" notion by cases, *i. e.*, as the Solovay randomness whenewer it satisfies (1) and (2), and the arithmetical randomness otherwise. This will result in a notion of randomness also satisfying the common closure properties, for instance, stable with respect to finite changes.

3 Solovay random sequences

The aim of this Section is to describe a notion of randomness which has the following properties, apparently even stronger than those of (1) and (2), but only in the sense of *consistency*:

(1*) The set of all random sequences is a full set.

(2*) For any formula $\Psi(x)$, if the set $\{x \in \Omega : \Psi(x)\}$ is null then no random sequence satisfies $\Psi(x)$.

It immediately follows from Theorem 1 that there is no set theoretic formula which, *provably in* **ZFC**, satisfies (1*) and (2*) as a notion of randomness. Yet there is a notion of randomness which *consistently* satisfies (1*) and (2*).

Recall that $\mathbf{G}_\delta$ sets are countable intersections of open sets. Define $\mathbb{S} = 2^{<\mathbb{N}}$, the set of all finite binary strings. Let us say that a set $C \subseteq \mathbb{N}\times\mathbb{S}$ is a *code* for a $\mathbf{G}_\delta$ set $U \subseteq \Omega$ iff $U = \bigcap_n \bigcup_{\langle n,u\rangle \in C} \Omega_u$, where, as above, $\Omega_u = \{x \in \Omega : u \subset x\}$.

Definition 2 A sequence $x \in \Omega$ is *Solovay random over* L iff it avoids any null $\mathbf{G}_\delta$ set with a code in L, the class of all Gödel constructible sets.

The formula saying that $x \in \Omega$ is Solovay random over L is denoted by $\rho_{\mathrm{L}}(x)$. Put $\mathcal{R}_{\mathrm{L}} = \{x \in \Omega : \rho_{\mathrm{L}}(x)\}$ (all Solovay random over L sequences). □

In fact it will not be different to say: whenever $X \subseteq \Omega$ is a null *Borel* set with a code in L. [6] Indeed, it is a classical fact of measure theory that any null Borel set $X \subseteq \Omega$ can be covered by a null $\mathbf{G}_\delta$ set $U \subseteq \Omega$. The construction of the covering set U can be maintained effectively enough to show that any null Borel set coded in L can be covered by a null $\mathbf{G}_\delta$ set coded in L.

It occurs that basic properties of $\mathcal{R}_{\mathrm{L}}$ depend on the structure of the set universe: **ZFC** alone does not prove much, so that one either considers special models or proves consistency theorems. In particular, it is consistent with **ZFC** that $\mathcal{R}_{\mathrm{L}}$ is empty, just because $\mathcal{R}_{\mathrm{L}} = \emptyset$ is a (trivial) consequence of the axiom of constructibility $\mathrm{V} = \mathrm{L}$. On the other hand, we have

Theorem 3 (Solovay) *It is consistent with* **ZFC** *that the formula* $\rho_{\mathrm{L}}(x)$ *satisfies both* (1*) *and* (2*).

Proof The method of proof will be to demonstrate that $\rho_{\mathrm{L}}(x)$ satisfies (1*) and (2*) in a particular model of **ZFC**, called *the Solovay model*.

To obtain this model, one has to fix an inaccessible cardinal ϑ in the constructible universe L. Then one defines a *generic extension* of L, which is a model of **ZFC** where each ordinal $\alpha < \vartheta$ is made countable by adding an

[6] It would be difficult to fully present here the involved mechanism of coding Borel subsets of Ω. It is based on the observation that construction of a Borel subset of Ω from sets of the form $\Omega_u = \{x \in \Omega : u \subset x\}$, where u is a finite binary sequence, needs only countably many applications of the operations of countable union and countable intersection. This can be adequately coded *e.g.* by a sequence $c \in \Omega$. Sequences which code Borel sets this way are called *Borel codes*. The set of all Borel codes is a co-analytic subset of Ω.

appropriate *collapse function* $f_\alpha : \mathbb{N}$ onto $\alpha = \{\beta : \beta < \alpha\}$. The model has a lot of applications in set theory, for instance it is true in this model that all projective sets of sequences are Lebesgue measurable. This result is based on the following key fact (we refer to [3, 6] for proof):

Proposition 4 *In the Solovay model, if a set* $X \subseteq \Omega$ *is definable by a set theoretic formula containing only sets in* L *as parameters then there is a Borel set* $B \subseteq \Omega$ *with a code* [7] *in* L *such that* $X \cap \mathcal{R}_{\mathrm{L}} = B \cap \mathcal{R}_{\mathrm{L}}$. □

The following lemma is another key ingredient of the proof of Theorem 3.

Lemma 5 *In the Solovay model,* $\mathcal{R}_{\mathrm{L}}$ *is a full* $\mathbf{G}_\delta$ *set.*

Proof Codes $C \subseteq \mathbb{N} \times \mathbb{S}$ for $\mathbf{G}_\delta$ sets, defined above, can themselves be effectively coded by sequences in Ω. Thus it suffices to prove that the set $\Omega \cap \mathrm{L}$ of all constructible sequences is countable in the Solovay model.

To show this recall that $\aleph_1$ is the least uncountable cardinal, or, that is the same, the least cardinal bigger than $\aleph_0 = \mathtt{card}\,\mathbb{N}$, the countable cardinality. By $\aleph_1^{\mathrm{L}}$ they denote "$\aleph_1$ in the sense of L", that is, the object defined, in L, as the least uncountable cardinal. Clearly $\aleph_1^{\mathrm{L}} < \vartheta$, where ϑ is the L-inaccessible cardinal which participates, as above, in the construction of the Solovay model. It follows that $\aleph_1^{\mathrm{L}}$ is countable, in the Solovay model. On the other hand, it is known that, in L, the continuum hypothesis $2^{\aleph_0} = \aleph_1$ holds; hence, sequences in $\Omega \cap \mathrm{L}$ admit $1-1$ correspondence with L-countable ordinals, *i.e.*, those smaller than $\aleph_1^{\mathrm{L}}$. It follows that the set $\Omega \cap \mathrm{L}$ is really countable. □

Thus, in the Solovay model, $\mathcal{R}_{\mathrm{L}}$ has full measure, so that every set of sequences, definable by a formula with parameters in L, is a Borel set modulo a null set – hence, it is Lebesgue measurable. (This remains true even if we allow, in addition, arbitrary parameters in Ω in definitions of sets.) In other words, we have (1*). We easily prove (2*), too. Indeed, suppose that, in the Solovay model, $X \subseteq \Omega$ is a null set, definable by a formula containing only sets in L as parameters. By Proposition 4, we can assume that X is a *Borel* null set, coded in L. It follows from observation after Definition 2, that X is covered by a null $\mathbf{G}_\delta$ set $U \subseteq \Omega$, coded in L. However $U \cap \mathcal{R}_{\mathrm{L}} = \emptyset$. □

The use of the Solovay model in this proof needs to be commented upon. Recall that the construction of this model starts with a model with an inaccessible cardinal. It is known that the existence of such a cardinal cannot be proved in **ZFC**, moreover, it implies the formal consistency of **ZFC**, so that a

[7] See Footnote 6 above.

set theory with an inaccessible cardinal is much stronger than **ZFC**. Therefore, it is important to figure out whether the existence of inaccessible cardinal can be eliminated from the proof of Theorem 3.

In many similar cases, the use of inaccessible cardinals is inavoidable (sometimes it is very difficult to prove this !), but in this case the Solovay model can be replaced by models not based on inaccessibles. One of them is a model obtained as an extension $\mathrm{L}[f]$ of the constructible universe L by a generic map $f : \mathbb{N}$ onto $\aleph_1^{\mathrm{L}}$. Another one, much more sophisticated but not using a cardinal collapse (which means that all L-cardinals remain cardinals in the extension) is described in [10], p. 315. (We shall not stop at set theoretic details related to those models.) Neither of the two needs inaccessible cardinals or anything else beyond **ZFC**. However the Solovay model has another advantage.

Indeed, consider the notion of *relative standardness*, which naturally arises in the study of some probabilistic phenomena like the Fubini theorem (see [7]). This would be a binary formula $R(x,y)$ (reads: x *is random relative to* y) satisfying the two following requirements

(1°) If $y \in \Omega$ then the set $\{x : R(x,y)\}$ is a full set.

(2°) For any formula $\Psi(x,y)$, if $y \in \Omega$ and the set $\{x \in \Omega : \Psi(x,y)\}$ is null then no sequence $x \in \Omega$ satisfies $R(x,y)$ & $\Psi(x,y)$.

For instance, let, following [7], $R(x,y)$ be the formula saying that $x \in \Omega$ is Solovay random over $\mathrm{L}[y]$, the class of all sets sets constructible relative to y : in other words, that x avoids any null $\mathbf{G}_\delta$ set with a code in $\mathrm{L}[y]$. A minor modification of the proof of Theorem 3 shows that it is consistent with **ZFC** that this formula R satisfies both (1°) and (2°), and in fact R satisfies (1°) and (2°) in the Solovay model. However, unlike the "simple" randomness above, it is not known whether the consistency of (1°) and (2°) can be established on the base of **ZFC** alone. (This problem was formulated in [7].)

4 The "consistent" randomness

Recall that a code for a $\mathbf{G}_\delta$ set is, as defined in Section 3, a subset of $\mathbb{S} \times \mathbb{N}$, where $\mathbb{S}$ is the set of all finite binary strings. Let us fix a recursive bijection $\beta : \mathbb{S} \times \mathbb{N}$ onto $\mathbb{N}$. We say that a $\mathbf{G}_\delta$ code C is *arithmetically definable* iff its β-image c is an arithmetical subset of $\mathbb{N}$ in the ordinary sense, *i.e.*, it can be defined by a formula written in terms of addition and multiplication, with quantifiers over natural numbers. We say that a set $G \subseteq \Omega$ is *an arithmetically coded* $\mathbf{G}_\delta$ *set* iff it has an arithmetically definable code.

Definition 6 A sequence $x \in \Omega$ is *an arithmetically random* iff it avoids any null arithmetically coded $\mathbf{G}_\delta$ set. [8] The formula saying that $x \in \Omega$ is arithmetically random is denoted by $\rho_{\rm A}(x)$. Put $\mathcal{R}_{\rm A} = \{x \in \Omega : \rho_{\rm A}(x)\}$ (all arithmetically random sequences). □

One easily proves, in **ZFC**, that $\mathcal{R}_{\rm L} \subseteq \mathcal{R}_{\rm A}$, or, in other words, $\rho_{\rm L}(x)$ implies $\rho_{\rm A}(x)$. Unlike $\mathcal{R}_{\rm L}$, the set $\mathcal{R}_{\rm A}$ is, provably in **ZFC**, a set of full measure. Clearly any Martin-Löf random sequence $x \in \Omega$ belongs to $\mathcal{R}_{\rm A}$.

Let $\rho(x)$ be the formula saying:

- $x \in \mathcal{R}_{\rm A}$, and if $\mathcal{R}_{\rm L}$ is a set of full measure then $x \in \mathcal{R}_{\rm L}$.

Thus ρ defines the set $\mathcal{R}_{\rm L}$ of all Solovay random sequences over L — provided this is a set of full measure, while otherwise it defines simply the set $\mathcal{R}_{\rm A}$ of all arithmetically random sequences. It easily follows that ρ satisfies (1) and (3). To see that $\rho(x)$ also satisfies (2′), consider a set theoretic formula $\Psi(x)$ such that **ZFC** proves that it defines a null set. Note that, by definition, **ZFC** proves $\rho(x) \Longrightarrow \rho_{\rm L}(x)$; hence, by Theorem 3, it is consistent with **ZFC** that ρ satisfies (2*). It follows that $\forall\, x\, (\rho(x) \Longrightarrow \neg\, \Psi(x))$ also is consistent, so that **ZFC** does not prove that there is a random sequence x satisfying $\Psi(x)$.

5 Invariant randomness

Any reasonable notion of randomness of a sequence in Ω (including those considered above) informally amounts to the requirement that the sequence cannot include infinite regularities of some kind. What happens if we do not mind to allow "small" infinite regularities ? Let is make a few steps in this direction.

Let I be an ideal on $\mathbb{N}$ whose elements (subsets of $\mathbb{N}$) will be thought of as "small" infinite sets. The following examples are of interest:

$$\begin{aligned} \mathtt{Fin} &= \text{all finite subsets of } \mathbb{N} \quad ; \\ \mathcal{D} &= \text{all density 0 subsets of } \mathbb{N} \quad . \end{aligned}$$

(A set $X \subseteq \mathbb{N}$ is *of density* 0 iff the frequency of elements of X among first n natural numbers tends to 0 as n tends to ∞.) Define E_I to be the associated equivalence relation on Ω, so that $x \,\mathsf{E}_I\, y$ iff the set $\{n : x(n) \neq y(n)\}$ belongs to I : informally, x and y "differ not too much" from each other.

Note that $\mathsf{E}_{\mathtt{Fin}}$ is usually denoted by E_0.

[8] See [1] on this notion. A similar approach, which includes arithmetical randomness as a very particular case, was proposed in [2]. It can be proved that this definition is equivalent to uncompressibility when computations are relativised to arithmetical oracles.

If E is an equivalence relation on Ω then let $[x]_{\mathsf{E}} = \{y : y \mathrel{\mathsf{E}} x\}$ (the E-*class* of $x \in \Omega$) and $[X]_{\mathsf{E}} = \{y : \exists x \in X\, (y \mathrel{\mathsf{E}} x)\}$ and $]X[_{\mathsf{E}} = \complement\,[\complement X]_{\mathsf{E}}$ (the E-*saturation* and the E-*kernel* of $X \subseteq \Omega$; $\complement X$ is the complement of X, as usual). Any set X satisfying $X = [X]_{\mathsf{E}}$ is called E-*invariant*.

Let us take the *arithmetical* randomness as the basic notion, but the following definition makes sense for any other one (*e. g.*, the Solovay randomness).

Definition 7 Let E be an equivalence relation on Ω. A sequence $x \in \Omega$ is *arithmetically* E-*invariant random* iff it avoids any set of the form $]X[_{\mathsf{E}}$, where X is a null arithmetically coded $\mathbf{G}_\delta$ set. □

(It is not clear that this is equivalent to the requirement that x avoids any null E-invariant arithmetically coded $\mathbf{G}_\delta$ set: note that $[X]_{\mathsf{E}}$ may be not Borel, even assuming that E, X are Borel.) The definition makes sense formally for any equivalence relation E, but lacks motivation if E is not of the form E_I [9].

Then "arithmetically random" is clearly the same as "arithmetically $=$-invariant random" (the equality can be considered as an equivalence relation). Moreover, this is the same as "arithmetically E_0-invariant random", because the E_0-saturation $[X]_{\mathsf{E}_0}$ of any set X is the union of countably many simple shifts of X. On the other hand, the case of $\mathsf{E}_{\mathcal{D}}$ is different !

Indeed, the set of all arithmetically $\mathsf{E}_{\mathcal{D}}$-invariant random sequences is clearly $\mathsf{E}_{\mathcal{D}}$-invariant. It follows that there is an arithmetically $\mathsf{E}_{\mathcal{D}}$-invariant random sequence x such that $x(2^n) = 0$ for all n : note that the set $\{2^n : n \in \omega\}$ belongs to $\mathcal{D}$! Such an x is not arithmetically random, of course. Thus, arithmetically random sequences form a proper subclass of arithmetically $\mathsf{E}_{\mathcal{D}}$-invariant random ones. In fact for any arithmetically random x there exist many arithmetically $\mathsf{E}_{\mathcal{D}}$-invariant random but not arithmetically random sequences $y \mathrel{\mathsf{E}_{\mathcal{D}}} x$. We would be interested to know if any arithmetically $\mathsf{E}_{\mathcal{D}}$-invariant random y satisfies $y \mathrel{\mathsf{E}_{\mathcal{D}}} x$ for some arithmetically random x .

Another question is how the known forms of relationship between ideals over $\mathbb{N}$ reflect in the associated notions of invariant randomness.

References

[1] B. Durand, A. Shen, N. Vereshagin. *Arithmetical randomness*. (Manuscript), 1998.

[9] In the latter case, the definition may reflect the procedure of coin tossing which allows to toss packets of infinitely many coins simultaneously, to determine the values of $x(n)$, where $n \in X$ and $X \subseteq \mathbb{N}$ belongs to I, a given ideal.

[2] H. Gaifman, M. Snir, Probabilities over rich languages, randomness and testing, *J. of Symbolic Logic*, 1982, 47, pp. 495 – 548.

[3] T. Jech, *Set Theory*, Academic Press, 1978.

[4] V. Kanovei and M. Reeken, Mathematics in a nonstandard world, *Math. Japonica* 1997, 45, no 2, pp. 369 – 408.

[5] A. H. Kruse, Some notions of random sequence and their set-theoretic foundations, *Z. math. L. Grundl. Math.*, 1967, 13, pp. 299 – 322.

[6] K. Kunen, *Set Theory, an introduction to independence proofs*, North–Holland, 1980.

[7] M. van Lambalgen, Independence, randomness, and the axiom of choice, *J. of Symbolic Logic*, 1992, 57, pp. 1274 – 1304.

[8] P. Martin-Löf. The definition of random sequences, *Information and Control*, 1966, 9, pp. 602–619.

[9] An. A. Muchnik, A. L. Semenov, V. A. Uspensky. Mathematical methaphysics of randomness, *Theoretical Computer Science*, 1998, 207, pp. 263–317.

[10] J. Stern, Regularity properties of definable sets of reals, *Annals of Pure and Applied Logic*, 1985, 29, pp. 289 – 324.

[11] V. A. Uspensky, A. L. Semenov, and A. Kh. Shen. Can an individual sequence of zeros and ones be random ? *Russian Math. Surveys*, 1990, 45, 1, pp. 121–189.

[12] V. A. Uspensky and A. L. Semenov. *Algorithms: main ideas and applications*. Kluwer Acad. Publ., Dordrecht, 1993.