Available online at www.sciencedirect.com
ScienceDirect
Theoretical Computer Science 385 (2007) 193–201
Theoretical Computer Science
www.elsevier.com/locate/tcs

Random reals à la Chaitin with or without prefix-freeness

Verónica Becher[a,b,*], Serge Grigorieff[c]

[a] *Departamento de Computación, FCEyN, Universidad de Buenos Aires, Argentina*
[b] *Consejo Nacional de Investigaciones Científicas y Técnicas (CONICET), Argentina*
[c] *LIAFA, CNRS and Université Paris 7, 2, pl. Jussieu 75251 Paris Cedex 05, France*

Received 16 October 2006; received in revised form 7 June 2007; accepted 24 June 2007

Communicated by F. Cucker

Abstract

We give a general theorem that provides examples of n-random reals à la Chaitin, for every $n \geq 1$; these are halting probabilities of partial computable functions that are universal *by adjunction* for the class of *all* partial computable functions, The same result holds for the class functions of partial computable functions with prefix-free domain. Thus, the usual technical requirement of prefix-freeness on domains is an option which we show to be non-critical when dealing with universality by adjunction. We also prove that the condition of universality by adjunction (which, though particular, is a very natural case of optimality) is essential in our theorem.

Keywords: Algorithmic randomness; Random reals; Kolmogorov complexity; Omega numbers

1. Introduction

Partial computable functions with prefix-free domain have been considered to get deep relations between Martin-Löf randomness and algorithmic information theory; namely,

- Schnorr's characterization [15] of random sequences of $\mathbf{2}^\omega$ via the prefix-free (also called self-delimited) variant $K : \mathbf{2}^{<\omega} \to \mathbb{N}$ of Kolmogorov complexity (Chaitin [5] and Levin [11]).
- Chaitin's Omega numbers as significant random reals (Chaitin [5]; cf. Theorem 1.6 below).

The role of prefix-freeness in these results is that of a key technical tool, but one can argue that there is no decisive conceptual argument in favor of the prefix-free restriction on domains: recently, Miller and Yu [13] have obtained a plain Kolmogorov complexity characterization of random sequences. In this short paper, we give examples of n-random reals à la Chaitin, for every $n \geq 1$, namely, the probability $\Omega_U[A]$ that U maps into a given Σ^0_n-complete set A (or simply non-empty Σ^0_1 in the case of $n = 1$); cf. Theorem 2.4. Their significance is twofold. Firstly, unlike

* Corresponding author at: Departamento de Computación, FCEyN, Universidad de Buenos Aires, Argentina. Tel.: +54 11 4576 3359; fax: +54 11 4576 3359.
E-mail addresses: vbecher@dc.uba.ar (V. Becher), seg@liafa.jussieu.fr (S. Grigorieff).

0304-3975/$ - see front matter
doi:10.1016/j.tcs.2007.06.007

the classical Chaitin Omega numbers, these reals are the halting probabilities of universal functions *with no prefix-free condition on their domains*. Secondly, there were no known examples of n-random reals arising from halting probabilities other than the classical Chaitin Omega numbers of optimal partial functions recursive in oracle $\emptyset^{n-1}$, for $n \geq 1$. However, the price to pay is that:

(a) though the notion of optimality we use—the so called *universality by adjunction*—is most usual, it is more restrictive than the classical notion; and
(b) the probability $\Omega_U[A]$ that we use is only subadditive in A; cf. Proposition 1.5.

1.1. Optimality, universality and universality by adjunction

We denote by $\mathbf{2}^{<\omega}$ the set of all finite words on the alphabet $\{0, 1\}$ and by $\mathbf{2}^{\leq n}$ the set of all words up to size n. The length of a word a is denoted as $|a|$. We write $\preceq$ for the prefix relation between words. Let $\varphi : \mathbf{2}^{<\omega} \to \mathbf{2}^{<\omega}$. We denote by $\varphi_e : \mathbf{2}^{<\omega} \to \mathbf{2}^{<\omega}$ the map such that $dom(\varphi_e) = \{p \mid 0^e 1p \in dom(\varphi)\}$ and $\varphi_e(p) = \varphi(0^e 1p)$ for all p in its domain. We shall use the next definition when $\mathcal{C}$ is the class of partial computable functions (resp. with prefix-free domains) or partial computable with oracle $\emptyset^{(n-1)}$.

Definition 1.1 (*Universality and Universality by Adjunction*). Let $\mathcal{C}$ be a class of partial functions $\mathbf{2}^{<\omega} \to \mathbf{2}^{<\omega}$.

(1) U is *universal* (resp. *partial universal*) in $\mathcal{C}$ if $U \in \mathcal{C}$ and there is a total (resp. partial) computable function $c : \mathbb{N} \times \mathbf{2}^{<\omega} \to \mathbf{2}^{<\omega}$ such that

$$\mathcal{C} = \{\lambda p.U(c(e, p)) \mid e \in \mathbb{N}\}$$

where $\lambda p.U(c(e, p))$ denotes the partial function $p \mapsto U(c(e, p))$ with domain $\{p \mid c(e, p) \in dom(U)\}$.
(2) U is *universal by adjunction* in the case of $c(e, p) = 0^e 1p$, i.e.

$$U \in \mathcal{C} \ \wedge \ \mathcal{C} = \{U_e \mid e \in \mathbb{N}\}.$$

Let us recall the classical notion of optimality.

Definition 1.2. (1) Let $\varphi : \mathbf{2}^{<\omega} \to \mathbf{2}^{<\omega}$. We denote by $C_\varphi : \mathbf{2}^{<\omega} \to \mathbb{N} \cup \{+\infty\}$ the map such that $C\varphi(u) = \min\{|p| \mid \varphi(p) = u\}$ (with the convention $\min \emptyset = +\infty$).
(2) $U : \mathbf{2}^{<\omega} \to \mathbf{2}^{<\omega}$ is optimal for $\mathcal{C}$ if

$$U \in \mathcal{C} \ \wedge \ (\forall \varphi \in \mathcal{C}\ \exists a\ \forall x \in \mathbf{2}^{<\omega}\ [C_U(x) \leq C_\varphi(x) + a]).$$

As is well known,

Proposition 1.3. *If $U : \mathbf{2}^{<\omega} \to \mathbf{2}^{<\omega}$ is partial universal for $\mathcal{C}$ with respect to a partial computable map c such that*

$$(\dagger) \qquad \forall e\ \exists a_e\ \forall p\ ((e, p) \in dom(c) \Rightarrow |c(e, p)| \leq |p| + a_e)$$

then U is also optimal for $\mathcal{C}$. In particular, universality by adjunction implies optimality.

1.2. Generalized Chaitin reals

We shall deal with Martin-Löf randomness (cf. textbooks [3,12,7]) and n-randomness (i.e. randomness in oracle $\emptyset^{(n-1)}$), for $n \geq 1$. Recall that a real is left c.e. (resp. n-left c.e.) if it is the limit of a bounded monotone increasing computable (resp. computable in oracle $\emptyset^{(n-1)}$) sequence of rational numbers. We use $\mu(\mathcal{X})$ to denote the Lebesgue measure of a subset $\mathcal{X}$ of the Cantor space $\mathbf{2}^\omega$ of all infinite binary words of length ω. For a set $S \subseteq \mathbf{2}^{<\omega}$, we write $S\mathbf{2}^\omega$ to denote the set $\{sg \mid s \in \mathbf{2}^{<\omega} \wedge g \in \mathbf{2}^\omega\}$. In the case where S is a singleton $\{s\}$ we drop the braces and simply write $s\mathbf{2}^\omega$.

Definition 1.4. Let $f : \mathbf{2}^{<\omega} \to \mathbf{2}^{<\omega}$ and $A \subseteq \mathbf{2}^{<\omega}$. We denote by $\Omega_f[A]$ and $\Omega_f[k, A]$ the reals

$$\Omega_f[A] = \mu(\{p \in dom(f) \mid f(p) \in A\}\mathbf{2}^\omega)$$
$$\Omega_f[k, A] = \mu(\{p \in dom(f) \mid |p| \geq k \wedge f(p) \in A\}\mathbf{2}^\omega)$$

Thus, $\Omega_f[A]$ (resp. $\Omega_f[k, A]$) is the probability that an infinite word has at least one prefix (resp. prefix of length $\geq k$) which is mapped into A by f.

The lack of prefix-freeness prevents $\Omega_f[A]$ from being additive in A; it is merely subadditive.

Proposition 1.5. (1) *If $A, B \subseteq \mathbf{2}^{<\omega}$ then $\Omega_f[A \cup B] \leq \Omega_f[A] + \Omega_f[B]$.*
(2) *In the case where f has prefix-free domain and A, B are disjoint then*

$$\Omega_f[A \cup B] = \Omega_f[A] + \Omega_f[B].$$

Since there are finitely many p's with length $< k$, the real $\mu(\{|p| < k \mid f(p) \in A\}\mathbf{2}^\omega)$ is rational. In the case where f has prefix-free domain, we have $\Omega_f[A] = \Omega_f[k, A] + \mu(\{|p| < k \mid f(p) \in A\}\mathbf{2}^\omega)$ and Chaitin's celebrated theorem [5] (see the Note on page 141 of [6]) can be stated as follows.

Theorem 1.6 (*Chaitin [5]*). *Let $U : \mathbf{2}^{<\omega} \to \mathbf{2}^{<\omega}$ be optimal for the class of partial computable functions with prefix-free domains. For every $k \in \mathbb{N}$ and every infinite computably enumerable set $A \subseteq \mathbf{2}^{<\omega}$, the real $\Omega_U[k, A]$ is random left c.e.*

Let us also recall the extension obtained for Σ^0_n sets A in [1].

Theorem 1.7 (*Becher, Figueira, Grigorieff and Miller [1]*). *Let $U : \mathbf{2}^{<\omega} \to \mathbf{2}^{<\omega}$ be optimal for the class of partial computable functions with prefix-free domains. For every $k \in \mathbb{N}$ and $n \geq 2$ and every Σ^0_n-complete set $A \subseteq \mathbf{2}^{<\omega}$, the real $\Omega_U[k, A]$ is random.*

Remark 1.8. As shown in [1], the above results cannot be extended:

– for any optimal U there exists a Δ^0_2 set A such that $\Omega_U[A]$ is rational,
– there exists an optimal U such that $\Omega_U[A]$ is rational for all finite sets A.

However, we shall extend them with the extra hypothesis of universality by adjunction. In particular, randomness is extended to n-randomness in Theorem 2.7.

2. Universality by adjunction and randomness of generalized Chaitin reals

2.1. Partial many–one reducibility

The following extension of many–one reducibility is the pertinent tool for addressing the main Theorem 2.4. It was introduced by Ershov, 1968 [8], and is related to Kleene index sets and enumeration reducibility (cf. [8], page 23, point 6 of Corollaries and [14] and [10], Remark 4).

Definition 2.1 (*[8]*). (1) Let $A, B \subseteq \mathbf{2}^{<\omega}$. We say that A is partial many–one reducible to B if $A = f^{-1}(B)$ for some partial computable $f : \mathbf{2}^{<\omega} \to \mathbf{2}^{<\omega}$.
(2) For $\mathcal{C} \subseteq P(\mathbf{2}^{<\omega})$, the notion of partial many–one $\mathcal{C}$-completeness is defined in the usual way.

The following result was noticed in [8] (Example on p. 21).

Proposition 2.2. *A set S is partial many–one Σ^0_1-complete if and only if it is Σ^0_1 and non-empty.*

Proof. Let $f : \mathbf{2}^{<\omega} \to \mathbf{2}^{<\omega}$ be a constant function with value an element of S and domain the set to be reduced to S.

2.2. Randomness of $\Omega_U[k, A]$ for k large enough

The following proposition is straightforward.

Proposition 2.3. *Suppose that*

(1) *$\widetilde{X}$ and $\widetilde{Y}$ are disjoint subsets of $\mathbf{2}^{<\omega}$,*
(2) *$\widetilde{X} \cup \widetilde{Y}$ is prefix-free,*
(3) *$X \subseteq \widetilde{X}\mathbf{2}^{<\omega}$ and $Y \subseteq \widetilde{Y}\mathbf{2}^{<\omega}$.*

Then $X\mathbf{2}^\omega$ and $Y\mathbf{2}^\omega$ are disjoint and $\mu((X \cup Y)\mathbf{2}^\omega) = \mu(X\mathbf{2}^\omega) + \mu(Y\mathbf{2}^\omega)$.

We can now prove our main theorem.

Theorem 2.4. *Let $U : \mathbf{2}^{<\omega} \to \mathbb{N}$ be universal by adjunction for the class of partial computable functions (no prefix-free condition on domains).*

Let $n \geq 1$. If $A \subseteq \mathbb{N}$ is partial many–one Σ^0_n complete then, for all k large enough, the real $\Omega_U[k, A]$ is n-random left n-c.e.

Note 2.5. Let $\ell > 0$, $a \in A$ and define V from U as follows: $V(q) = a$ if $|q| < \ell$ and $V(qp) = U(p)$ for all $|q| = \ell$. If U is optimal (resp. universal, resp. universal by adjunction) for the class of partial computable functions then so is V. Also, $\mu(\{p \mid |p| = k \wedge V(p) = a\}\mathbf{2}^{\omega}) = 1$ for all $k < \ell$. Thus $\Omega_V[k, \{a\}] = 1$ for all $k < \ell$. Since $\{a\}$ is partial many–one Σ^0_1 complete (cf. Proposition 2.2), the condition "k large enough" cannot be removed in Theorem 2.4.

Proof. Let φ_n be universal by adjunction for the class of functions with prefix-free domains which are partial computable with oracle $\emptyset^{(n-1)}$. Let $Z_n = dom(\varphi_n)$. Chaitin's Theorem 1.6 (and its oracular version, for the case $n \geq 2$) insures that $Z_n \subset \mathbf{2}^{<\omega}$ is a prefix-free Σ^0_n set such that $\mu(Z_n\mathbf{2}^{\omega})$ is n-random left n-c.e. The assumed partial many–one Σ^0_n-completeness of A yields a partial computable $f : \mathbf{2}^{<\omega} \to \mathbb{N}$ such that $f^{-1}(A) = Z_n$. Since U is universal by adjunction, there exists $i \in \mathbb{N}$ such that $f = U_i$. Thus,

$$\begin{aligned} Z_n &= U_i^{-1}(A) = \{p \in \mathbf{2}^{<\omega} \mid 0^i 1p \in U^{-1}(A)\} \\ 0^i 1 Z_n &= U^{-1}(A) \cap 0^i 1\mathbf{2}^{<\omega}. \end{aligned}$$

Let k be any integer $> i$ and let

$$\begin{aligned} X &= \widetilde{X} = U^{-1}(A) \cap 0^i 12^{<k-i-1} \\ Y &= \widetilde{Y} = U^{-1}(A) \cap 0^i 12^{\geq k-i-1}. \end{aligned}$$

Since $0^i 1 Z_n = U^{-1}(A) \cap 0^i 1\mathbf{2}^{<\omega}$ is prefix-free, the conditions of Proposition 2.3 are satisfied. Since $X \cup Y = U^{-1}(A) \cap 0^i 1\mathbf{2}^{<\omega} = 0^i 1 Z_n$, we get

$$\mu(0^i 1 Z_n \mathbf{2}^{\omega}) = \mu((U^{-1}(A) \cap 0^i 12^{<k-i-1})\mathbf{2}^{\omega}) + \mu(U^{-1}(A) \cap 0^i 12^{\geq k-i-1})\mathbf{2}^{\omega}).$$

Now, $0^i 12^{<k-i-1}$ is finite; hence the real $\mu((U^{-1}(A) \cap 0^i 12^{<k-i-1})\mathbf{2}^{\omega})$ is rational. Since $\mu(0^i 1 Z_n \mathbf{2}^{\omega}) = 2^{-i-1}\mu(Z_n\mathbf{2}^{\omega})$ is n-random, so is $\mu((U^{-1}(A) \cap 0^i 12^{\geq k-i-1})\mathbf{2}^{\omega})$. Finally, letting

$$\begin{aligned} \widetilde{X} &= 0^i 12^{k-i-1} & X &= U^{-1}(A) \cap \widetilde{X}\mathbf{2}^{<\omega} \\ \widetilde{Y} &= \{u \mid |u| = k \wedge 0^i 1 \not\preceq u\} & Y &= U^{-1}(A) \cap \widetilde{Y}\mathbf{2}^{<\omega} \end{aligned}$$

we have $X \cup Y = U^{-1}(A) \cap 2^{\geq k}$ and the conditions of Proposition 2.3 are satisfied, so that

$$\begin{aligned} \Omega_U[k, A] &= \mu((U^{-1}(A) \cap 2^{\geq k})\mathbf{2}^{\omega}) \\ &= \mu((U^{-1}(A) \cap 0^i 12^{\geq k-i-1})\mathbf{2}^{\omega}) + \sum_{|u|=k, 0^i 1 \not\preceq u} \mu((U^{-1}(A) \cap u\mathbf{2}^{<\omega})\mathbf{2}^{\omega}). \end{aligned}$$

Both terms on the right are left n-c.e. and the first one is n-random. Using the fact that the sum of two left n-c.e. reals is n-random whenever one of them is n-random ([4]; cf. also [2], Prop. 3.6, or Downey and Hirschfeldt's book [7]), we conclude that our sum is n-random, completing the proof of Theorem 2.4.

Using Proposition 2.2, we get:

Corollary 2.6. *Let $U : \mathbf{2}^{<\omega} \to \mathbb{N}$ be universal by adjunction for the class of partial computable functions (no prefix-free condition on domains).*

(1) *If $A \subseteq \mathbb{N}$ is computably enumerable and non-empty, then, for all k large enough, the real $\Omega_U[k, A]$ is 1-random left c.e.*
(2) *If $n \geq 2$ and $A \subseteq \mathbb{N}$ is many–one Σ^0_n complete then, for all k large enough, the real $\Omega_U[k, A]$ is n-random left n-c.e.*

2.3. Prefix-freeness and randomness of $\Omega_U[A]$

The argument of the proof of Theorem 2.4 also applies mutatis mutandis to prefix-free partial computable maps (it is even simpler since there is no need for large k). Under the hypothesis of universality by adjunction, this extends Chaitin's Theorem 1.6 and also Theorem 3.2 of [1].

Theorem 2.7. *Let $U : \mathbf{2}^{<\omega} \to \mathbb{N}$ be universal by adjunction for the class of partial computable functions with prefix-free domains. Let $n \geq 1$. If $A \subseteq \mathbb{N}$ is partial many–one Σ^0_n complete, then $\Omega_U[A]$ is n-random left n-c.e.*

3. On the role of the hypothesis of universality by adjunction

3.1. Optimal partial universality is not enough

Proposition 3.1 below stresses the essential role of universality by adjunction in Theorem 2.4. Point (i) is a non-prefix-free version of the weaker analog statement in [1, Proposition 2.1]. We construct an optimal partial universal machine V such that $\Omega_V[k, A]$ is not random, for the choices of $A \subset \mathbf{2}^{<\omega}$ in Points (ii) and (iii). These are the counterparts of the weaker analogs [1, Corollary 2.2 and Remark 2.3] (also cf. Figueira, Stephan and Wu [9]). In particular, Point (iii) constructs a Π^0_1 set A, and disproves randomness of $\Omega_V[k, B]$ for every $B \subseteq A$, by showing lack of Borel normality in base 2. We provide the full proof.

Let us recall that a real r is Borel normal in base $t \geq 2$, if for every word $w \in \{0, 1, \ldots, (t-1)\}^{<\omega}$,

$$\lim_{n\to\infty} \frac{\text{number of occurrences of } w \text{ in } r\restriction n \text{ in base } t}{n} = \frac{1}{t^{|w|}}.$$

r is *absolutely normal* if it is normal to every base $t \geq 2$. Absolute normality is an effective measure 1 property, so all random reals possess it.

Proposition 3.1. *There exists a partial computable function $V : \mathbf{2}^{<\omega} \to \mathbf{2}^{<\omega}$ such that*

(i) *V is partial universal and satisfies property (†) of Proposition 1.3. In particular, V is optimal.*
(ii) *If $A \subset \mathbf{2}^{<\omega}$ is finite then $V^{-1}(A)$ is finite, and hence $\Omega_V[k, A]$ is dyadic rational for every k,*
(iii) *There is an infinite Π^0_1 set $A \subseteq \mathbf{2}^{<\omega}$ such that, for every k and every subset $B \subseteq A$, the real $\Omega_V[k, A]$ is not Borel normal, and hence not 1-random.*

3.2. Proof of Proposition 3.1

3.2.1. Construction of V

Let $U : \mathbf{2}^{<\omega} \to \mathbf{2}^{<\omega}$ be partial computable universal by adjunction. Modify U so that the empty word ε is not in the domain of U. This does not affect universality which involves programs of the form 0^i1p which are all $\neq \varepsilon$. We transform U into another partial computable function V by removing from the domain of U as many "useless" programs as we can: we remove any program p which is not shorter than some program which is already known to be in the domain of U and gives the same image as p does. Namely, let $(p_i)_{i\in\mathbb{N}}$ be a computable enumeration of $dom(U)$. Define a total computable function $f : \mathbb{N} \to \mathbb{N}$ such that $f(i)$ is the smallest $j \leq i$ satisfying

$$U(p_j) = U(p_i), \quad |p_j| = \min\{|p_\ell| : \ell \leq i,\ U(p_\ell) = U(p_i)\}.$$

Let V be the partial computable restriction of U to the computably enumerable set $\{p_{f(i)} \mid i \in \mathbb{N}\}$.

3.2.2. Proof of point (i) of Proposition 3.1

To simplify notation we write $\Omega_V[a]$ and $\Omega_V[k, a]$ in place of $\Omega_V[\{a\}]$ and $\Omega_V[k, \{a\}]$ for singleton sets $\{a\}$. Define a partial computable $c : \mathbb{N} \times \mathbf{2}^{<\omega} \to \mathbf{2}^{<\omega}$ as follows:

$$dom(c) = \{(e, p) \mid 0^e1p \in dom(U)\}$$
$$c(e, p) = p_{f(i)} \text{ where } i \text{ is such that } p_i = 0^e1p.$$

Clearly, $0^e1p \in dom(U) \Leftrightarrow c(e, p) \in dom(V)$ and $U(0^e1p) = V(c(e, p))$. Since U is universal by adjunction, we see that V is partial universal. Finally, inequality $|c(e, p)| \leq |0^e1p|$ yields property (†).

3.2.3. Proof of point (ii) of Proposition 3.1

To get point (ii) of Proposition 3.1, apply equality $V^{-1}(A) = \bigcup_{a\in A} V^{-1}(a)$ and the following claim.

Claim 3.2. *Let $a \in \mathbf{2}^{<\omega}$. The set $V^{-1}(a)$ is finite non-empty of the form $V^{-1}(a) = \{q_0, \ldots, q_n\}$ where $|q_0| > |q_1| > \cdots > |q_n| = C_U(a)$. In particular, $C_V = C_U$.*

Proof. Let j be least such that $U(p_j) = a$ and $|p_j| = C_U(a)$. Then $f(i) = j$ for every $i \geq j$ such that $U(p_i) = a$. This proves finiteness of $V^{-1}(a)$ and that its smallest element has length $C_U(a)$. To conclude, observe that, by construction of V, two elements of $V^{-1}(a)$ cannot have the same length.

3.2.4. Some more properties of V

The length of a dyadic rational in [0, 1] is the number of digits of its shortest representation in base 2.

Claim 3.3. *There exists a total computable function $\ell : \mathbf{2}^{<\omega} \to (\mathbb{N} \setminus \{0\})$ such that, for all $a \in \mathbf{2}^{<\omega}$,*

(1) *the longest word in $V^{-1}(a)$ has length $\ell(a)$; hence $2^{-\ell(a)} \leq \Omega_V[a]$;*
(2) *the real $\Omega_V[a]$ is dyadic rational with length $\leq \ell(a)$.*

Proof. Let $\ell(a)$ be the length of the element q_0 of $V^{-1}(a)$ which comes first in the enumeration of $dom(U)$. Since the empty word is not in $dom(U)$ (cf. Section 3.2.1), ℓ takes values in $\mathbb{N} \setminus \{0\}$. The construction of V insures that q_0 is the longest element of $V^{-1}(a)$, which proves point 1. Observe that $\Omega_V[a] = \sum_{q\in M_a} 2^{-|q|}$ where M_a is the set of minimal elements of the finite set $V^{-1}(a)$ (minimality is with respect to the prefix ordering on words). Thus, point 1 implies point 2.

Note 3.4. In the case where the longest element of $V^{-1}(a)$ has a prefix in $V^{-1}(a)$, it does not appear in M_a, so that the length of $\Omega_V[a]$ may be $< \ell(a)$.

Claim 3.5. $\lim_{|a|\to+\infty} \Omega_V[a] = 0$.

Proof. Claim 3.2 yields $\Omega_V[a] < \sum_{j\geq C_U(a)} 2^{-j} = 2^{-C_U(a)+1}$. To conclude, recall that $\lim_{|a|\to+\infty} C_U(a) = +\infty$ for any U.

3.2.5. A sufficient condition for failing normality

We shall use the following lemma to prove that $\Omega_V[k, A]$ is not Borel normal.

Lemma 3.6. *Let $\alpha = \sum_{n\in\mathbb{N}} \alpha_n$ where the α_n's are strictly positive dyadic rational numbers. Suppose there is some $g : \mathbb{N} \to (\mathbb{N} \setminus \{0\})$ such that, for all n, α_n has length $\leq g(n)$ (as a dyadic rational) and $\alpha_{n+1} < 2^{-3g(n)}$. Then α is not Borel normal in base 2 (and hence not 1-random).*

Proof. Observe that the hypotheses imply that $2^{-g(n+1)} \leq \alpha_{n+1} < 2^{-3g(n)}$; hence, $g(n+1) > 3g(n)$. In particular, $g(n)$ is strictly monotone increasing unbounded. Let $\beta = \sum_{n\in\mathbb{N}} \alpha_{n+1}$. The contribution of α_{n+1} to β is for digits with ranks in $\{3g(n)+1, \ldots, g(n+1)\}$. All digits of β between $g(n+1)+1$ and $3g(n+1)$ are 0. Let us denote by $\#_i(x)$ the number of digits i ($i = 0, 1$) in the initial segment of β up to rank x;

$$
\begin{aligned}
\#_1(3g(N+1)) &\leq [g(1) - 3g(0)] + \cdots + [g(N+1) - 3g(N)] \\
&= g(N+1) - 2[g(1) + \cdots + g(N)] - 3g(0) \\
\#_0(3g(N+1)) &\geq [3g(1) - g(1)] + \cdots + [3g(N+1) - g(N+1)] \\
&= 2g(1) + \cdots + 2g(N+1).
\end{aligned}
$$

Thus, $\#_0(3g(N+1)) \geq 2\#_1(3g(N+1))$, i.e. the $3g(N+1)$ first digits of β contain more than twice as many 0's as 1's. Since $g(N+1)$ is unbounded, this proves that β is not normal in base 2. Finally, α is also not normal since it is the sum of β and the dyadic rational α_0.

3.2.6. Construction of the Π^0_1 set A

We now define the set A which satisfies property (ii) of Proposition 3.1. Fix some enumeration $(p_i)_{i\in\mathbb{N}}$ of $dom(V)$ and associate with it the computable bijective enumeration $E : \mathbb{N} \to \mathbf{2}^{<\omega}$ such that the $E(i)$'s are the distinct elements of the sequence $(V(p_i))_{i\in\mathbb{N}}$ in their order of first appearance. Let $<_E$ be the order on $\mathbf{2}^{<\omega}$ induced by E : $u <_E v \Leftrightarrow E^{-1}(u) < E^{-1}(v)$. We give a construction of an infinite Π^0_1 set $A = \bigcap_{t\geq 0} A_t$. To force failure of Borel normality of $\Omega_V[k, A]$ in base 2, we make the construction so that the following property will hold, where $\ell : \mathbf{2}^{<\omega} \to \mathbb{N}$ is the total computable function from Claim 3.3:

$$\forall n \geq 1 \ \ (\Omega_V[a_n] < 2^{-3\ell(a_{n-1})}) \quad \text{where } a_0, a_1, \ldots \text{ is the enumeration of } A \text{ induced by } E. \tag{1}$$

The computable sequence of cofinite sets $(A_t)_{t\in\mathbb{N}}$ is inductively defined as follows.
Initial step. Let $a^0_0 = E(0)$ (the $<_E$ least word) and $A_0 = \mathbf{2}^{<\omega}$.
Inductive step: from t to $t+1$. Let $\Omega^t_V[a]$ denote the approximation of $\Omega_V[a]$ at step t. The set A_{t+1} is defined as follows.

Let $a^t_0 <_E a^t_1 <_E \ldots <_E a^t_{m_t}$ be the distinct elements in $A_t \cap \{V(p_i) \mid 0 \leq i \leq t\}$. Set $A_{t+1} = A_t$ in the case where for every $n = 1, \ldots, m_t$,

$$\Omega^t_V[a^t_n] < 2^{-3\ell(a^t_{n-1})} \tag{2}$$

Otherwise let a^t_j be the first among $a^t_1, \ldots, a^t_{m_t}$ such that condition (2) fails and set $A_{t+1} = A_t \setminus \{a^t_j\}$.

Clearly, the A_t's are cofinite and decreasing and $A = \bigcap_{t\geq 0} A_t$ is Π^0_1.

3.2.7. A has the wanted properties

Claim 3.7. *A is infinite and, letting $a_0 <_E a_1 <_E \ldots$ be the enumeration of A, for every $n \in \mathbb{N}$, conditions $m_t \geq n$ and $a^t_n = a_n$ hold for all t large enough.*

Proof. Let $\mathcal{P}(n)$ be the following property:

$$\begin{aligned} \exists a_0 \ldots \exists a_n \quad & [a_0 <_E a_1 <_E \ldots <_E a_n \wedge \\ & (\forall a \in A_t \setminus \{a_0, \ldots, a_n\}\ a_n <_E a) \wedge \\ & (\exists \tau\ \forall t \geq \tau\ (m_t \geq n \ \wedge\ \textstyle\bigwedge_{i=0,\ldots,n} a^t_i = a_i))]. \end{aligned}$$

To prove the claim, it suffices to show $\forall n\ \mathcal{P}(n)$. By induction on n. *Initial step $n = 0$.* Observe that a^t_0 is never removed since the a^t_j to be removed is selected among $a^t_1, \ldots, a^t_{m_t}$. Thus, one can take $a_0 = a^0_0$ and $\tau = 0$.

Inductive step: from n to $n+1$. Let $a_0, \ldots, a_n$ and τ witness condition $\mathcal{P}(n)$. First, observe that, since A_t is cofinite and $domain(U)$ is infinite, the set $T = \{t \geq \tau \mid m_t > n\}$ is infinite. If $\mathcal{P}(n+1)$ failed then, for every $t \in T$, the element a^t_{n+1} is removed at some step $t' > t$. Thus, we can extract an infinite subset $S \subseteq T$ such that the a^t_{n+1}'s, $t \in S$, are pairwise distinct. The removal at step t' of $a^t_{n+1} = a^{t'}_{n+1}$ means that $\Omega^{t'}_V[a^t_{n+1}] \geq 2^{-3\ell(a_n)}$. Since, $\Omega_V[a^t_{n+1}] \geq \Omega^{t'}_V[a^t_{n+1}]$, we get

$$\Omega_V[a^t_{n+1}] \geq 2^{-3\ell(a_n)} \quad \text{for all } t \in S. \tag{3}$$

Now, the infinite sequence $(a^t_{n+1})_{t\in S}$ is made of pairwise distinct elements, and hence the lengths of its elements tend to $+\infty$ and Claim 3.5 says that $\Omega_V[a^t_{n+1}]$ tends to 0 when t tends to $+\infty$. But, according to (3), the sequence is bounded from below by $2^{-3\ell(a_n)}$. A contradiction.

Claim 3.8. *Condition* (1) *holds for every infinite subset B of A.*

Proof. Condition (1) from the construction holds for A. Let τ be such that $m^t \geq n$ and $a_n = a^t_n$ and $\Omega^t_V[a_n] = \Omega_V[a_n]$ for all $t \geq \tau$. Since a^t_n is not removed, we have $\Omega^t_V[a_n] < 2^{-3\ell(a_{n-1})}$. Hence $\Omega_V[a_n] < 2^{-3\ell(a_{n-1})}$.

To get condition (1) for any infinite subset B of A, it suffices to prove that $\Omega_V[a_{n+1+k}] < 2^{-3\ell(a_n)}$ holds for all n and k. We prove it by induction on k.

Initial step $k = 0$. Apply condition (1) for A (cf. point 1 of this proof).

Inductive step: from k to $k+1$. Observe that

$$\begin{aligned} \Omega_V[a_{n+1+k+1}] &< 2^{-3\ell(a_{n+1+k})} && \text{(condition (1) for } A\text{)} \\ &< 2^{-\ell(a_{n+1+k})} \\ &\le \Omega_V[a_{n+1+k}] && \text{(Claim 3.3)} \\ &< 2^{-3\ell(a_n)} && \text{(induction hypothesis).} \end{aligned}$$

3.2.8. *Proof of point (iii) of Proposition 3.1*

Consider some infinite subset B of A and some fixed k. Let $b_0 <_E b_1 <_E \ldots$ be the elements of B. Then $\Omega_V[k, B] = \sum_{n\in\mathbb{N}} \alpha_n$ where

$$\begin{aligned} \alpha_0 &= \Omega_V[k, b_0] \\ \alpha_{n+1} &= \Omega_V[k, \{b_0, \ldots, b_{n+1}\}] - \Omega_V[k, \{b_0, \ldots, b_n\}]. \end{aligned}$$

Case 1: $\{n \mid \alpha_n = 0\}$ *is cofinite.* Then $\Omega_V[k, B]$ is rational and hence not normal.

Case 2: $I = \{n \mid \alpha_n > 0\}$ *is infinite.* Let $i_0 < i_1 < \ldots$ be the elements of I. Then $\Omega_V[k, \{b_j \mid j \le i_m\}] = \Omega_V[k, \{b_{i_j} \mid j \le m\}]$. Let $B' = \{b_{i_j} \mid j \in \mathbb{N}\}$. Then B' is an infinite subset of A and $\Omega_V[k, B] = \Omega_V[k, B']$ and the α'_n's associated with B' are all strictly positive. Thus, we reduce to the case where all α_n's are strictly positive.

By Claim 3.8, condition (1) is true for B. Thus, $\Omega_V[b_{n+1}] < 2^{-3\ell(b_n)}$, so that

$$\text{All programs in } V^{-1}(b_{n+1}) \text{ have length} \ge 3\ell(b_n). \tag{4}$$

From Claim 3.3 we have $2^{-\ell(b_{n+1})} \le \Omega_V[b_{n+1}]$. In particular, $2^{-\ell(b_{n+1})} < 2^{-3\ell(b_n)}$, so that $\ell(b_{n+1}) > 3\ell(b_n)$ and the sequence $(\ell(b_n))_{n\in\mathbb{N}}$ is strictly increasing.

Using Claim 3.3 and the monotonicity of the $\ell(b_n)$, we see that

$$\text{All programs in } V^{-1}(\{b_0, \ldots, b_n\}) \text{ have length} \le \ell(b_n). \tag{5}$$

Using conditions (4) and (5) we see that no program in $V^{-1}(b_{n+1})$ is shorter than some program in $V^{-1}(\{b_0, \ldots, b_n\})$. In particular, $\alpha_{n+1} = \mu(M_n\mathbf{2}^\omega)$ where M_n is the family of programs in $V^{-1}(b_{n+1})$ which have length $\ge k$ and have no prefix in $V^{-1}(\{b_0, \ldots, b_n\}) \cap 2^{\ge k}$. Since $\alpha_{n+1} > 0$, the set M_n is not empty. Now, $M_n \subseteq V^{-1}(b_{n+1})$ and Claim 3.3 states that the longest element of M_n has length $\le \ell(b_{n+1})$. As a consequence, the length of the dyadic rational $\alpha_{n+1} = \mu(M_n\mathbf{2}^\omega)$ is $\le \ell(b_{n+1})$.

Inclusion $M_n \subseteq V^{-1}(b_{n+1})$ and inequality $\Omega_V[b_{n+1}] < 2^{-3\ell(b_n)}$ (condition (1) for B) imply that $\alpha_{n+1} = \mu(M_n\mathbf{2}^\omega) \le \Omega_V[b_{n+1}] < 2^{-3\ell(b_n)}$.

The hypotheses of Lemma 3.6 are satisfied taking g to be the map $n \mapsto \ell(b_n)$. The application of this lemma concludes the proof of point (iii) of Proposition 3.1.

References

[1] V. Becher, S. Figueira, S. Grigorieff, J.S. Miller, Randomness and halting probabilities, Journal of Symbolic Logic 71 (4) (2006) 1394–1410.
[2] V. Becher, S. Grigorieff, Random reals and possibly infinite computations. Part I: Randomness in $\emptyset'$, Journal of Symbolic Logic 70 (3) (2005) 891–913.
[3] C. Calude, Information and Randomness, Springer, 1994.
[4] C. Calude, P. Hertling, B. Khoussainov, Y. Wang, Recursively enumerable reals and Chaitin Ω numbers, in: STACS 98, Paris, 1998, in: Lecture Notes in Computer Science, vol. 1373, Springer-Verlag, 1998, pp. 596–606.
[5] G. Chaitin, A theory of program size formally identical to information theory, Journal of the ACM 22 (1975) 329–340. Available on Chaitin's home page.
[6] G. Chaitin, Algorithmic Information Theory, 1st edition, Cambridge University Press, 1987.
[7] R. Downey, D. Hirschfeldt, Algorithmic Randomness and Complexity, Springer, 2006 (in press). Preliminary version, April 5th 2007, available on Downey's home page.
[8] Yu.L. Ershov, On a hierarchy of sets. III, Algebra and Logic 9 (1970) 20–31.
[9] S. Figueira, F. Stephan, G. Wu, Randomness and universal machines, in: Second International Conference on Computability and Complexity in Analysis, CCA 2005, Fernuniversität Hagen, Informatik Berichte, vol. 326, 2005, pp. 103–116, Journal of Complexity 22 (6) (2006) 738–751.
[10] C.M. Harris, On the symmetric enumeration degrees, Notre Dame Journal of Formal Logic 48 (2) (2007) 175–204.

[11] L. Levin, On the notion of random sequence, Soviet Mathematics Doklady 14 (5) (1973) 1413–1416.
[12] M. Li, P. Vitanyi, An Introduction to Kolmogorov Complexity and its Applications, 2nd edition, Springer, 1997.
[13] J. Miller, L. Yu, On initial segment complexity and degrees of randomness, Transactions of the American Mathematical Society (in press).
[14] J.-L. Mohrherr, Kleene index sets and functional m-degrees, Journal of Symbolic Logic 48 (3) (1983) 829–840.
[15] C.P. Schnorr, A unified approach to the definition of random sequences, Mathematical Systems Theory 5 (1971) 246–258.