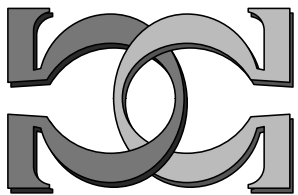
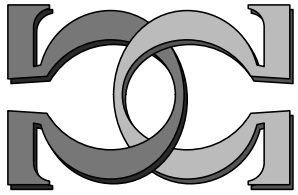
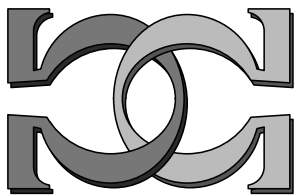


**CDMTCS  
Research  
Report  
Series**



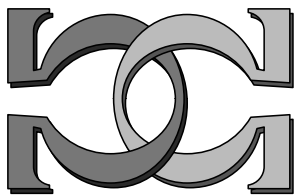
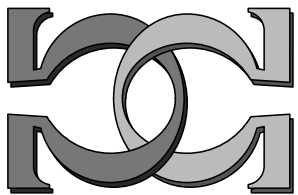
**Representation of  
Left-Computable  $\varepsilon$ -Random  
Reals**



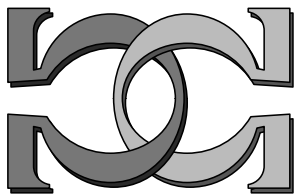
**C. S. Calude<sup>1</sup>, N. J. Hay<sup>1</sup>,  
F. C. Stephan<sup>2</sup>**

<sup>1</sup>University of Auckland

<sup>2</sup>National University of Singapore



CDMTCS-365  
May 2009



Centre for Discrete Mathematics and  
Theoretical Computer Science

# Representation of Left-Computable $\varepsilon$ -Random Reals\*

Cristian S. Calude<sup>†</sup> Nicholas J. Hay<sup>‡</sup> Frank Stephan<sup>§</sup>

7 May 2009

## Abstract

In this paper we introduce the notion of  $\varepsilon$ -universal prefix-free Turing machine and study its halting probability. The main result is the extension of the representability theorem for left-computable random reals to the case of  $\varepsilon$ -random reals: *a real is left-computable  $\varepsilon$ -random iff it is the halting probability of an  $\varepsilon$ -universal prefix-free Turing machine.* We also show that left-computable  $\varepsilon$ -random reals are provable  $\varepsilon$ -random in Peano Arithmetic. The theory developed here parallels to a large extent the classical theory, but not completely.

## 1 Introduction

A real  $\alpha$  is left-computable (or recursively/computably enumerable) if there is a computable increasing sequence of rationals which converges to  $\alpha$ . Left-computable random reals can be characterised using various tools including prefix-complexity, Martin-Löf tests, martingales, Chaitin Omega numbers and universal probability [1, 3, 5, 6, 7, 10, 14].

Some left-computable reals are not random, but “partially random”. For example, inserting a 0 in between each adjacent bits of a random sequence produces

---

\*A preliminary version of this paper was presented at the Joint AMS–NZMS Meeting, Wellington, NZ, December 2007.

<sup>†</sup>Department of Computer Science, The University of Auckland, Private Bag 92019, Auckland, New Zealand, [cristian@cs.auckland.ac.nz](mailto:cristian@cs.auckland.ac.nz). Supported in part by a Hood Fellowship.

<sup>‡</sup>Department of Computer Science, The University of Auckland, Private Bag 92019, Auckland, New Zealand, [nickjhay@gmail.com](mailto:nickjhay@gmail.com).

<sup>§</sup>Department of Mathematics and School of Computing, National University of Singapore, Singapore 117543, [fstephan@comp.nus.edu.sg](mailto:fstephan@comp.nus.edu.sg). Supported in part by NUS grant numbers R146-000-114-112 and R252-000-308-112.

a non-random sequence, having some weak randomness properties: this sequence is, as intuition suggests,  $1/2$ -random. The papers [4, 11, 15, 16, 17, 18] have studied the degree of randomness of reals (or sequences) by measuring their “degree of compression”. In what follows  $\varepsilon$  is a fixed computable real number with  $0 < \varepsilon \leq 1$  and we study the  $\varepsilon$ -randomness of reals, both intrinsically and in relation to the classical notion of randomness which corresponds to  $\varepsilon = 1$ , hence referred to as 1-randomness.

Our main tool is the  $\varepsilon$ -universal prefix-free Turing machine, a machine that can simulate any other prefix-free machine: the length of the simulating program on the  $\varepsilon$ -universal machine is bounded up to a fixed constant by the length of the simulated program divided by  $\varepsilon$ . In case  $\varepsilon = 1$  we get the classical notion of universal machine. Contrary to the situation in the classical theory, the difference between the prefix complexities induced by two  $\varepsilon$ -universal prefix-free Turing machines may not be bounded.

We show that the halting probability of an  $\varepsilon$ -universal prefix-free Turing machine is left-computable and  $\varepsilon$ -random. Generalising the corresponding representability theorem of left-computable random reals [1, 3, 7, 10] we show that the converse is also true: every left-computable  $\varepsilon$ -random is the halting probability of an  $\varepsilon$ -universal prefix-free Turing machine. A specific  $\varepsilon$ -universal Turing machine  $V_\varepsilon$  is obtained via Equation (1) below; the main principle is to “dilute” a universal Turing machine  $V$  and this machine plays an important role as the halting probability is in the least with respect to  $H$ -reducibility of all  $\varepsilon$ -random reals.

The theory developed here parallels to a large extent the classical theory, but not completely. The following two results show interesting differences: (a) the prefix-free complexities induced by universal machines differ by at most an additive constant, but the difference between prefix-free complexities induced by  $\varepsilon$ -universal machines may be unbounded, (b) random reals are Borel normal (in any base), but  $\varepsilon$ -random reals may not contain even arbitrarily long runs of 0s.

The paper is organised as follows. In Section 2 we present the necessary notation and previous results. In Section 3 we introduce and study  $\varepsilon$ -universal machines and their halting probabilities. In Section 4 we study left-computable  $\varepsilon$ -random reals and in Section 5 we present the representability theorem for left-computable  $\varepsilon$ -random reals. In Section 6 we discuss the provability in Peano Arithmetic of  $\varepsilon$ -randomness for left-computable reals. In Section 7 we disprove Stay’s conjecture regarding the 1-randomness (with respect to  $U$ ) of the halting probability of an  $\varepsilon$ -universal machine  $U$ . We conclude with a few comments and open questions.

## 2 Notation and background

Let  $\Sigma = \{0, 1\}$  and denote by  $\Sigma^n$  and  $\Sigma^*$  the set of all bit-strings of length  $n$  and the set of all bit-strings, respectively. The length of  $\sigma \in \Sigma^*$  is denoted by  $|\sigma|$ . By  $\log n$  we abbreviate the function  $\lfloor \log_2(n+1) \rfloor$ . Let  $\mathbb{N} = \{1, 2, \dots\}$  and let  $\text{bin} : \mathbb{N} \rightarrow \Sigma^*$  be the bijection which associates to every  $n \geq 1$  its binary expansion without the leading 1.

Each real  $\alpha$  with  $0 < \alpha \leq 1$  has a unique infinite binary expansion  $\alpha = 0.\alpha_1\alpha_2\cdots\alpha_n\cdots$ . We denote by  $\alpha \upharpoonright n = \alpha_1\alpha_2\cdots\alpha_n$  the prefix of length  $n$  of  $\alpha$ 's expansion. In this way, reals are identified with infinite binary sequences. Similarly, if  $\mathbf{x} = x_1x_2\cdots x_n\cdots$  is an infinite sequence,  $\mathbf{x} \upharpoonright n = x_1x_2\cdots x_n$ .

We assume that the reader is familiar with algorithmic information theory, cf. [1, 7] and present only a few notions to fix the notation.

A prefix-free (Turing) machine is a Turing machine whose domain is a prefix-free set of strings. The prefix complexity of a string induced by a prefix-free machine  $W$ ,  $H_W(\sigma)$ , is  $H_W(\sigma) = \min\{|p| : W(p) = \sigma\}$ . From now on *all Turing machines will be prefix-free and will be referred to as machines*.

We use several times the Kraft-Chaitin Theorem: given a computable enumeration of positive integers  $n_i$  such that  $\sum_i 2^{-n_i} \leq 1$ , we can effectively construct a prefix-free set of binary strings  $\{x_i\}$  such that  $|x_i| = n_i$ , for all  $i \geq 1$ .

Fix a computable  $\varepsilon$  with  $0 < \varepsilon \leq 1$  and machine  $W$ . A sequence  $\mathbf{x}$  is Chaitin  $(\varepsilon, W)$ -random if there is a constant  $c > 0$  such that for every  $n \geq 1$ ,  $H_W(\mathbf{x} \upharpoonright n) \geq \varepsilon \cdot n - c$ ;  $\mathbf{x}$  is strictly Chaitin  $(\varepsilon, W)$ -random if  $\mathbf{x}$  is Chaitin  $(\varepsilon, W)$ -random, but not Chaitin  $(\delta, W)$ -random for any  $\delta$  with  $\varepsilon < \delta \leq 1$ .

If  $W$  is universal (from now on called 1-universal), then we get Tadaki's definition of weak Chaitin  $\varepsilon$ -randomness (see [4, 17]). If  $W$  is 1-universal and  $\varepsilon = 1$ , then we get Chaitin's classical definition of randomness [5, 6]. A real is Chaitin  $(\varepsilon, W)$ -random (shortly,  $(\varepsilon, W)$ -random) if its binary expansion is Chaitin  $(\varepsilon, W)$ -random.

For any prefix-free set  $A \subset \Sigma^*$  we define  $\Omega_A = \sum_{x \in A} 2^{-|x|}$ . The halting probability of a machine  $W$  is  $\Omega_W = \sum_{x \in \text{dom}(W)} 2^{-|x|}$ .

Following Tadaki [17], for any (not necessarily prefix-free) set  $W \subseteq \Sigma^*$  and computable  $\delta > 0$  we write  $\mu^\delta(W) = \sum_{w \in W} 2^{-\delta \cdot |w|}$ . If  $\delta > 1$  and  $W$  is prefix-free, then  $\mu^\delta(W) \leq \Omega^\delta(W) \leq 1$ . However, if  $0 < \delta < 1$  then we can have  $\mu^\delta(W) = \infty$  even for prefix-free  $W$  (for example, for  $W = \{1^{\log n} 0 \text{bin}(n) : n > 0\}$ ).

## 3 $\varepsilon$ -universal machines

In this section we introduce and study the notion of  $\varepsilon$ -universal machine.

In analogy with the classical case we say, following Stay [13], that a machine

$U$  is  $\varepsilon$ -universal for  $\varepsilon$  with  $0 < \varepsilon \leq 1$  if for all machines  $T$  there exists a constant  $c_{U,T}$  such that for each program  $\sigma \in \Sigma^*$  there exists a program  $p \in \Sigma^*$  such that

$$U(p) = T(\sigma) \text{ and } \varepsilon \cdot |p| \leq |\sigma| + c_{U,T}.$$

If  $\varepsilon = 1$  we get the classical notion of universal machine. Every universal machine is  $\varepsilon$ -universal, but the converse is not true (see Theorem 2).

We fix a computable real  $\varepsilon$  with  $0 < \varepsilon \leq 1$ . A machine  $U$  is strictly  $\varepsilon$ -universal if  $U$  is  $\varepsilon$ -universal but not  $\delta$ -universal for any  $\delta$  with  $\varepsilon < \delta \leq 1$ .

**Lemma 1.** *The machine  $U$  is  $\varepsilon$ -universal iff there exists a 1-universal machine  $V$  and a constant  $c_{U,V}$  such that for all  $\sigma \in \Sigma^*$  we have  $\varepsilon \cdot H_U(\sigma) \leq H_V(\sigma) + c_{U,V}$ .*

**Theorem 2.** *Let  $V$  be a 1-universal machine and define*

$$V_\varepsilon(p0^{\lfloor(1/\varepsilon-1)|p|\rfloor}) = V(p). \quad (1)$$

*Then:*

- (a)  $V_\varepsilon$  is a machine and for all  $\sigma \in \Sigma^*$  we have  $H_{V_\varepsilon}(\sigma) = \lfloor H_V(\sigma)/\varepsilon \rfloor$ ,
- (b)  $V_\varepsilon$  is strictly  $\varepsilon$ -universal.

**Proof.** Clearly  $V_\varepsilon$  is a machine and the equality in (a) can be directly checked. From (a) and Lemma 1 we deduce the  $\varepsilon$ -universality of  $V_\varepsilon$ . If there were a constant  $c$  such that for all  $\sigma \in \Sigma^*$ ,  $\delta \cdot H_{V_\varepsilon}(\sigma) \leq H_V(\sigma) + c$ , then in view of (a) we would have  $(\delta/\varepsilon - 1) \cdot H_V(\sigma) \leq c$ , for all  $\sigma \in \Sigma^*$ , a contradiction ( $H_V$  is unbounded). So,  $V_\varepsilon$  is strictly  $\varepsilon$ -universal.  $\square$

**Theorem 3.** *Let  $V$  be a 1-universal machine. Then for every  $\varepsilon$ -universal machine  $U$ ,  $\Omega_U$  is  $(\varepsilon, V)$ -random.*

**Proof.** Let  $f$  be a computable one-to-one function which enumerates  $\text{dom}(U)$ . Let  $\omega_k = \sum_{j=1}^k 2^{-|f(j)|}$ . Clearly,  $(\omega_k)$  is a computable, increasing sequence of rationals converging to  $\Omega_U$ . Consider the binary expansion of  $\Omega_U = 0.\Omega_1\Omega_2\cdots$ .

We define a machine  $T$  as follows: on input  $\sigma \in \Sigma^*$ ,  $T$  first “tries to compute” the smallest number  $t$  with  $\omega_t \geq 0.\sigma$ . If successful,  $T(\sigma)$  is the first (in quasi-lexicographical order) string not belonging to the set  $\{U(f(1)), U(f(2)), \dots, U(f(t))\}$ ; if no such  $t$  exists then  $T(\sigma) = \infty$ .

Fix a number  $m \geq 1$  and note that  $T$  is defined on  $\Omega_U \upharpoonright m$ . Let  $t$  be the smallest number (computed in the second step of the computation of  $T$ ) with  $\omega_t \geq 0.\Omega_U \upharpoonright m$ . We have

$$0.\Omega_U \upharpoonright m \leq \omega_t < \omega_t + \sum_{s=t+1}^{\infty} 2^{-|f(s)|} = \Omega_U \leq 0.\Omega_U \upharpoonright m + 2^{-m}.$$

Hence,  $\sum_{s=t+1}^{\infty} 2^{-|f(s)|} \leq 2^{-m}$ , which implies  $|f(s)| \geq m$ , for every  $s \geq t+1$ . From the construction of  $T$  we conclude

$$H_U(T(\Omega_U \upharpoonright m)) \geq m. \quad (2)$$

Since  $T$  is a partially computable function, we get a constant  $c'$  such that for all  $\sigma \in \Sigma^*$

$$H_V(T(\sigma)) \leq H_V(\sigma) + c'. \quad (3)$$

Using (2), the  $\varepsilon$ -universality of  $U$ , and (3) we obtain

$$\begin{aligned} \varepsilon \cdot m &\leq \varepsilon \cdot H_U(T(\Omega_U \upharpoonright m)) \\ &\leq H_V(T(\Omega_U \upharpoonright m)) + c \\ &\leq H_V(\Omega_U \upharpoonright m) + c + c', \end{aligned}$$

which proves that  $\Omega_U$  is  $(\varepsilon, V)$ -random.  $\square$

**Corollary 4.** *If  $V$  be a 1-universal machine, then  $\Omega_{V_\varepsilon}$  is  $(\varepsilon, V)$ -random and  $(1, V_\varepsilon)$ -random.*

**Proof.** The halting probability  $\Omega_{V_\varepsilon}$  is  $(\varepsilon, V)$ -random because of Theorem 2, (b) and Theorem 3. Using this fact and Theorem 2, (a) we deduce that  $\Omega_{V_\varepsilon}$  is  $(1, V_\varepsilon)$ -random.  $\square$

Next we present a mechanism for producing examples of  $\varepsilon$ -universal machines. Let  $A, B$  be infinite, prefix-free (recursively/computably) enumerable sets. Generalising the strong simulation in [3], we say that the set  $A$   $\varepsilon$ -strongly simulates the set  $B$  (write  $B \leq_\varepsilon A$ ) if there is a constant  $c > 0$  and a partial computable function  $f : \Sigma^* \xrightarrow{o} \Sigma^*$  satisfying the following three conditions:

- (a)  $A = \text{dom}(f)$ ,
- (b)  $B = f(A)$  and
- (c)  $\varepsilon \cdot |\sigma| \leq |f(\sigma)| + c$  for all  $\sigma \in A$ .

The function  $f$  is called an  $\varepsilon$ -strong simulation of  $A$  onto  $B$ .

**Proposition 5.** *If  $V$  is a 1-universal machine and  $f$  is an  $\varepsilon$ -strong simulation of  $\text{dom}(V)$  onto a prefix-free enumerable set  $A$ , then  $V \circ f$  is an  $\varepsilon$ -universal machine with domain  $A$ .*

**Proof.** Recall that  $(V \circ f)(p) = V(f(p))$  for all  $p \in \Sigma^*$ . Fix a machine  $T$ . Since  $V$  is 1-universal there exists a constant  $c_T$  such that for each  $p \in \text{dom}(T)$  there exists a  $\sigma \in \text{dom}(V)$  satisfying  $|\sigma| \leq |p| + c_T$  and  $V(\sigma) = T(p)$ . Since  $f$  is onto there exists  $\tau \in A$  such that  $f(\tau) = \sigma$ . Since  $f$  is an  $\varepsilon$ -strong simulation we have  $\varepsilon \cdot |\tau| \leq |f(\tau)| + c = |\sigma| + c'$ . Combining the previous two equations we deduce that for every  $p$  there exists a  $\tau$  such that  $\varepsilon \cdot |\tau| \leq |p| + c_T + c'$  and  $V(f(\tau)) = T(p)$ , so  $V \circ f$  is  $\varepsilon$ -universal.  $\square$

It may seem that the difference between the cases  $\varepsilon = 1$  and  $0 < \varepsilon < 1$  is just technical. Here is a deeper difference. If  $V$  and  $V'$  are 1-universal machines, then their complexities  $H_V$  and  $H_{V'}$  differ by at most an additive constant [1]. *This result is not true for  $\varepsilon$ -universal machines.* To prove the claim we construct the following sequence of machines  $V_{\varepsilon,k}$  by means of a fixed 1-universal machine  $V$ . We let

$$f(p) = \begin{cases} p0^{\lfloor (1/\varepsilon - 1)|p| - k \cdot \log(|p|) \rfloor}, & \text{if } (1/\varepsilon - 1)|p| - k \cdot \log |p| \geq 1, \\ p1, & \text{otherwise,} \end{cases} \quad (4)$$

$$V_{\varepsilon,k} = V \circ f. \quad (5)$$

Note that only for finitely many strings  $p$  the value  $f(p)$  is defined by the otherwise-case. Furthermore, equation (5) means that  $V_{\varepsilon,k}(f(p)) = V(p)$  for all  $p \in \text{dom}(V)$  and  $V_{\varepsilon,k}(q)$  is undefined for all  $q \notin \{f(p) : p \in \text{dom}(V)\}$ .

**Theorem 6.** *The following properties are true:*

- (a)  $V_{\varepsilon,k}$  is a machine and  $H_{V_{\varepsilon,k}}(\sigma) = \lfloor H_V(\sigma)/\varepsilon - k \cdot \log H_V(\sigma) \rfloor$ , for almost all strings  $\sigma$ ,
- (b)  $V_{\varepsilon,k}$  is strictly  $\varepsilon$ -universal,
- (c) We have  $H_{V_{\varepsilon,k}}(\sigma) - H_{V_{\varepsilon,k+1}}(\sigma) \geq \log H_V(\sigma) - 1 \rightarrow \infty$  whenever  $|\sigma| \rightarrow \infty$ ,
- (d)  $\Omega_{V_{\varepsilon,k}}$  is  $(\varepsilon, V)$ -random.

**Proof.** Properties (a)–(c) follow from (4) and (5) using the technique presented in the proof of Theorem 2. In detail, the equality in (a) can be directly checked;  $\varepsilon$ -universality follows from (a) and Lemma 1. To show that  $V_{\varepsilon,k}$  is strictly  $\varepsilon$ -universal we suppose, by absurdity, that there exist two constants  $c, \delta$  such that

$c > 0$ ,  $1 > \delta > \varepsilon$  and  $\delta \cdot H_{V_\varepsilon}(\sigma) \leq H_V(\sigma) + c$  for all  $\sigma \in \Sigma^*$ . Then given the equality (a) we would have  $(\delta/\varepsilon - 1)H_V(\sigma) \leq \delta \cdot \log H_V(\sigma) + c + \delta$ , for all strings  $\sigma$ , a contradiction since  $H_V$  is unbounded. Property (c) follows from (a) and property (d) follows from (b) and Theorem 3.  $\square$

## 4 Left-computable $(\varepsilon, V)$ -random reals

We now study  $(\varepsilon, V)$ -random reals with the following reducibility relation: a real  $\alpha$  is *H-reducible* to a real  $\beta$ , written  $\alpha \leq_H \beta$ , if there exists a 1-universal machine  $V$  and a constant  $c > 0$  such that for all  $n \geq 1$ , we have  $H_V(\alpha \upharpoonright n) \leq H_V(\beta \upharpoonright n) + c$ . Of course, the choice of the 1-universal machine  $V$  is irrelevant. Two reals  $\alpha, \beta$  are *H-equivalent* if  $\alpha \leq_H \beta$  and  $\beta \leq_H \alpha$ .

**Theorem 7.** *Let  $V$  be a 1-universal machine. For every  $(\varepsilon, V)$ -random real  $\alpha$ ,  $\Omega_{V_\varepsilon} \leq_H \alpha$ .*

**Proof.** Tadaki [18, Theorem 4.6 (iv)] shows the following equivalence: a left-computable real  $\alpha$  is  $(\varepsilon, V)$ -random iff for every left-computable  $\varepsilon$ -convergent real  $\beta$  there exists a constant  $c$  such that for all  $n$ ,  $H_V(\beta \upharpoonright n) \leq H_V(\alpha \upharpoonright n) + c$  (recall that a real  $\gamma$  is  $\varepsilon$ -convergent if there exists an increasing computable sequence of rationals  $\{a_n\}$  such that  $\sum_{n=1}^{\infty} (a_{n+1} - a_n)^\varepsilon < \infty$  converging to  $\gamma$ ).

Now start with left-computable  $(\varepsilon, V)$ -random real  $\alpha$ . Because  $\Omega_{V_\varepsilon}$  is left-computable and  $\varepsilon$ -convergent we can apply the above mentioned equivalence to deduce the existence of a constant  $c$  such that  $H_V(\Omega_{V_\varepsilon} \upharpoonright n) \leq H_V(\alpha \upharpoonright n) + c$ , i.e.  $\Omega_{V_\varepsilon} \leq_H \alpha$ .  $\square$

**Comment 8.** Theorem 7 shows that  $\Omega_{V_\varepsilon}$  is up to  $H$ -equivalence the least of all  $(\varepsilon, V)$ -random reals. In fact, there is one left-computable real below all other  $(\varepsilon, V)$ -random reals.

**Theorem 9.** *Let  $V$  be a 1-universal machine. There exists a left-computable  $\alpha$  and a constant  $C$  such that for all  $n \geq 1$ ,  $|H_V(\alpha \upharpoonright n) - n \cdot \varepsilon| \leq C$ .*

**Proof.** In view of [11] there is a constant  $c$  such that for all  $\sigma \in \Sigma^*$ :

1.  $\sigma$  has an extension  $\tau$  of length  $|\sigma| + c$  such that  $H_V(\tau) > H_V(\sigma) + \varepsilon \cdot c + 1$ ,
2.  $H_V(\sigma) - c < H_V(\sigma 0^c) < H_V(\sigma) + \varepsilon \cdot c - 1$ .

Let  $T$  be the tree of all strings  $\sigma \in \Sigma^*$  whose all prefixes  $\eta$  with  $|\eta|$  a multiple of  $c$  have the property  $H_V(\eta) \geq \varepsilon \cdot |\eta|$ . Note that whenever  $\sigma$  is a node of length  $n \cdot c$ , by the first condition, there is an extension of  $\sigma$  in  $T$  of length  $n \cdot c + c$ .

Let  $\alpha$  be the left-most infinite branch of  $T$ , hence left-computable. If  $H_V(\alpha \upharpoonright (n \cdot c)) > n \cdot c \cdot \varepsilon + 2c + 1$ , then  $\alpha \upharpoonright (n \cdot c)0^c$  is in  $T$  as

$$H_V(\alpha \upharpoonright (n \cdot c)0^c) > n \cdot c \cdot \varepsilon + c + 1 > (n \cdot c + c) \cdot \varepsilon.$$

As  $\alpha$  is the leftmost infinite branch,  $\alpha \upharpoonright (n \cdot c + c) = \alpha \upharpoonright (n \cdot c)0^c$ . Consequently, by the second condition,  $H_V(\alpha \upharpoonright (n \cdot c + c)) < H_V(\alpha \upharpoonright (n \cdot c)) + \varepsilon \cdot c - 1$ , hence  $H_V(\alpha \upharpoonright (n \cdot c + c))$  is at least by 1 less than the target than  $H_V(\alpha \upharpoonright (n \cdot c))$ . From this it follows that  $|H_V(\alpha \upharpoonright (n \cdot c)) - n \cdot c \cdot \varepsilon|$  is bounded by a constant.  $\square$

**Comment 10.** The real  $\alpha$  in Theorem 9 is not strongly Chaitin  $(\varepsilon, V)$ -random, a slightly stronger result than [11].

It is well known that  $\Omega_V$  is Borel normal [1]. If  $\alpha = 0.\alpha_1\alpha_2\cdots$  is  $(1, V)$ -random then the real  $\beta = 0.\alpha_10\alpha_20\cdots$  is  $(1/2, V)$ -random and not Borel normal (because in its binary expansion, in the limit, the frequency of 0's is three times larger than the frequency of 1s).  $\Omega_{V_\varepsilon}$  is more than not Borel normal:

**Corollary 11** *The real  $\Omega_{V_\varepsilon}$  does not contain arbitrary long sequences of 0s.*

**Proof.** From Theorem 9 we know that  $|H_V(\Omega_{V_\varepsilon} \upharpoonright n) - \varepsilon \cdot n|$  is bounded by a constant  $c$ . There is a constant  $d$  such that for every string  $\sigma$ ,  $H_V(\sigma 0^d) < H_V(\sigma) + \varepsilon \cdot d - 3c$ . The reason is that one can code the number of 0s appended to  $\sigma$  in  $2 \cdot \log(d)$  bits so that  $H_V(\sigma 0^d) \leq H_V(\sigma) + c' + 2 \cdot \log(d)$  for some constant  $c'$ . Then, for all sufficiently large  $d$ ,  $c' + 2 \cdot \log(d) < \varepsilon \cdot d - 3c$ . It follows that for all prefixes  $\sigma$  of  $\Omega_{V_\varepsilon}$  the string  $\sigma 0^d$  is not a prefix of  $\Omega_{V_\varepsilon}$  because  $H_V(\sigma 0^d) < \varepsilon \cdot |\sigma| + c + \varepsilon \cdot d - 3c < \varepsilon \cdot (|\sigma| + d) - c$ . In particular, this is true for all prefixes of  $\Omega_{V_\varepsilon}$  which are empty or end with a 1. So there are no  $d$  consecutive 0s in  $\Omega_{V_\varepsilon}$ .  $\square$

The following result is a stronger form of Corollary 4:

**Corollary 12** *The halting probability  $\Omega_{V_\varepsilon}$  is strictly  $(\varepsilon, V)$ -random, for every 1-universal machine  $V$ .*

**Proof.** We need to show that for computable reals  $\delta, \varepsilon$  with  $0 < \varepsilon < \delta \leq 1$ ,  $\Omega_{V_\varepsilon}$  is not  $(\delta, V)$ -random. To this aim we consider a  $(1, V)$ -random real  $\alpha$ . To the string  $p_n = \alpha \upharpoonright n$  we associate the string  $q_n = \alpha_1 0^{i_1} \alpha_2 0^{i_2} \cdots \alpha_n 0^{i_n}$ , where  $i_1 = \lfloor (\frac{1}{\varepsilon} - 1) \rfloor$ ,  $i_j = \lfloor (\frac{1}{\varepsilon} - 1)j \rfloor - \sum_{t=1}^{j-1} \lfloor (\frac{1}{\varepsilon} - 1)t \rfloor$ , for  $j \in \{2, 3, \dots, n-1\}$ . Note that  $p_n$  and

$q_n$  can be effectively computed from one to the other, so there is a constant  $c$  such that for all  $n \geq 1$  we have  $|H_V(p_n) - H_V(q_n)| \leq c$ . Now denote by  $\alpha_\varepsilon$  the real whose binary expansion is  $\alpha_1 0^{i_1} \alpha_2 0^{i_2} \dots \alpha_n 0^{i_n} \dots$ . It is easy to check that  $\alpha_\varepsilon$  is strictly  $(\varepsilon, V)$ -random and, consequently, due to Theorem 7, also  $\Omega_{V_\varepsilon}$  is strictly  $(\varepsilon, V)$ -random.  $\square$

## 5 Representability of left-computable $(\varepsilon, V)$ -random reals

In this section we generalise the representability of left-computable random reals [3, 10] for the case of left-computable  $(\varepsilon, V)$ -random reals.

**Theorem 13** *Let  $V$  be a 1-universal machine. Every left-computable  $(\varepsilon, V)$ -random number is the halting probability of an  $\varepsilon$ -universal machine.*

**Proof.** Given  $V$  and  $\varepsilon$  we consider the machine  $V_\varepsilon$  defined by (1) and note that  $\Omega_{V_\varepsilon}$  is  $\varepsilon$ -convergent (see the proof of Theorem 7). By Theorem 4.6 (v) in [18], given the left-computable and  $(\varepsilon, V)$ -random real  $\alpha$  we can construct a left-computable real  $\beta \geq 0$  and a rational  $q > 0$  (in fact, we can take  $q$  to be  $2^{-m}$ , for some  $m > 0$ ) such that

$$\begin{aligned} \alpha &= \beta + 2^{-m} \cdot \Omega_{V_\varepsilon} = \beta + 2^{-m} \cdot \sum_{p \in \text{dom}(V_\varepsilon)} = 2 \cdot \sum_{r \in \text{dom}(T)} 2^{-|r|-1} + \sum_{p \in \text{dom}(V_\varepsilon)} 2^{-|s|-m} \\ &= \sum_{s \in \text{dom}(W)} 2^{-|s|} = \Omega_W, \end{aligned}$$

where the machine  $T$  is constructed from the left-computable real  $\beta$  using the Kraft-Chaitin Theorem and  $W$  is the  $\varepsilon$ -universal machine defined by the formula:

$$W(s) = \begin{cases} 0, & \text{if } s = 1s' \text{ and } s' \in \text{dom}(T), \\ V_\varepsilon(s), & \text{if } s = 0^m s' \text{ and } s' \in \text{dom}(V_\varepsilon). \end{cases}$$

This completes the proof.  $\square$

## 6 Provability of left-computable $(\varepsilon, V)$ -random reals

Peano Arithmetic (see [9], shortly, PA) is the first-order theory given by a set of 15 axioms defining discretely ordered rings, together with induction axioms for each formula  $\varphi(x, y_1, \dots, y_n): \forall \bar{y}(\varphi(0, \bar{y}) \wedge \forall x(\varphi(x, \bar{y}) \rightarrow \varphi(x+1, \bar{y})) \rightarrow \forall x(\varphi(x, \bar{y})))$ .

The proof in [2] can be adapted to show that *every left-computable  $(\varepsilon, V)$ -random real is provable  $(\varepsilon, V)$ -random in PA*. This means the following: if PA receives an algorithm for computing the computable real  $\varepsilon$  and an algorithm for a machine  $U$ , a proof that  $U$  is prefix-free and  $(\varepsilon, V)$ -universal, then it can prove that  $\Omega_U$  is left-computable and  $(\varepsilon, V)$ -random. This proof requires  $\varepsilon$  to be defined in terms of primitive recursive functions, which is always possible by a result of A. Mostowski [12].

Another representation which can be used to prove  $(\varepsilon, V)$ -randomness is the following: if PA receives an algorithm for computing the computable real  $\varepsilon$  and an algorithm for a machine  $V$ , a proof that  $V$  is prefix-free and universal, a positive integer  $c$ , and a computable increasing sequence of rationals converging to a real  $\gamma > 0$ , then PA can prove that  $\alpha = 2^{-c} \cdot \Omega_V + \gamma$  is  $(\varepsilon, V)$ -random.

Is any “representation” of a  $(\varepsilon, V)$ -random real enough to guarantee PA provability of  $(\varepsilon, V)$ -randomness? To answer this question we fix an effective enumeration of all left-computable reals in  $(0,1)$ ,  $\{\gamma_i\}$ . Such an enumeration can be based on an enumeration of all increasing primitive recursive sequences of rationals in  $(0,1)$ . Our question becomes: based solely on the index  $i$  can we always prove in PA that “ $\gamma_i$  is  $(\varepsilon, V)$ -random real” in case  $\gamma_i$  is  $(\varepsilon, V)$ -random real? We answer this question in the negative. To this aim we define the following sets:

$$\mathfrak{R}_{\text{lc}} = \{\gamma \in (0, 1) : \gamma \text{ is left-computable}\},$$

$$\mathfrak{R}_{\text{lc}}(\varepsilon, V) = \{\gamma \in \mathfrak{R}_{\text{lc}} : \gamma \text{ is } (\varepsilon, V)\text{-random}\},$$

$$\mathfrak{R}_{\text{lc}}^{\text{PA}}(\varepsilon, V) = \{\gamma \in \mathfrak{R}_{\text{lc}} : \gamma \text{ is provable}(\varepsilon, V)\text{-random in PA}\}.$$

By enumerating proofs in PA we deduce that the set  $\mathfrak{R}_{\text{lc}}^{\text{PA}}(\varepsilon, V)$  is enumerable.<sup>1</sup> Is  $\mathfrak{R}_{\text{lc}}(\varepsilon, V)$  enumerable?

We use Lemma 26 from [2]:

**Lemma 14** *If  $A \subseteq \mathfrak{R}$  is enumerable, then for all left-computable reals  $\alpha \in A$  and  $\beta > \alpha$  we have  $\beta \in A$ .*

**Theorem 15** *The set  $\mathfrak{R}_{\text{lc}}(\varepsilon, V)$  is not enumerable, so there exists  $\alpha \in \mathfrak{R}_{\text{lc}}(\varepsilon, V) \setminus \mathfrak{R}_{\text{lc}}^{\text{PA}}(\varepsilon, V)$ .*

**Proof.** Consider  $\alpha \in \mathfrak{R}_{\text{lc}}(\varepsilon, V)$  and define the left-computable real  $\beta$  in the following way. If  $\alpha \geq 1/2$ , then  $\beta = (\alpha \upharpoonright n)01 \cdots 1$  (where  $\alpha \upharpoonright (n+1) = 1^n 0$ ); if  $\alpha < 1/2$  consider the left-computable real  $\beta = (\alpha \upharpoonright n)01 \cdots 1$  (where  $\alpha \upharpoonright (n+1) =$

---

<sup>1</sup>Recall that a set  $A \subseteq \mathfrak{R}_{\text{lc}}$  is enumerable if the set  $\{i \in \mathbb{N} : \gamma_i \in A\}$  is enumerable. In such a set we enumerate all indices for all elements in  $A$ .

$0^m 1^{n-m} 0$ ). In both cases  $\beta > \alpha$  and  $\beta \notin \mathfrak{R}_{lc}(\varepsilon, V)$ , which shows, by Lemma 14, that  $\mathfrak{R}_{lc}(\varepsilon, V)$  is not enumerable, thus concluding the proof.  $\square$

In fact, a more precise result is true:

**Theorem 16** *For every  $\alpha \in \mathfrak{R}_{lc}(\varepsilon, V)$  there exists an index  $i$  such that  $\alpha = \gamma_i$  and PA cannot prove the statement “ $\gamma_i$  is  $(\varepsilon, V)$ -random”.*

**Proof.** Consider the set  $A_\alpha = \{\gamma_i : \alpha = \gamma_i\} \subset \mathfrak{R}_{lc}(\varepsilon, V)$  and repeat the above argument.  $\square$

## 7 Stay’s Conjecture

Stay [13] studied generalisations of the statement that  $\Omega_U$  is random for every 1-universal machine  $U$ . In particular he conjectured that  $\Omega_U$  is  $(1, U)$ -random for every  $\varepsilon$ -universal machine  $U$ . Although our results show that  $\Omega_U$  is  $(\varepsilon, V)$ -random (Theorem 3) and the conjecture is true for  $V_\varepsilon$  (Corollary 4), it turns out that the conjecture itself is too general and does not hold. We provide now a strong counterexample.

**Theorem 17.** *There exists an  $\frac{1}{16}$ -universal machine  $U$  such that  $\Omega_U$  is not  $(\frac{1}{2}, U)$ -random, hence not  $(1, U)$ -random.*

**Proof.** Let  $V$  be an 1-universal machine. Now we define  $U$  from  $V$  as follows:

$$U(\sigma) = \begin{cases} \tau 0^{13n}, & \text{if } \exists n > 0 \exists \tau [\sigma = 1^n 0 \tau \text{ and } |\tau| = 8n], \\ V(\tau), & \text{if } \exists n, m > 0 \exists \tau \in \text{dom}(V) \\ & [\sigma = 0\tau 0^n 1, |\sigma| = 4^{m+1} \text{ and } |\tau| \leq 4^m], \\ \infty, & \text{otherwise.} \end{cases}$$

Clearly,  $U$  is a machine. Given  $\tau \in \text{dom}(V)$ , let  $m_\tau = \min\{k > 0 : |\tau| \leq 4^k\}$  and  $n_\tau = 4^{m_\tau+1} - |\tau| - 2$ . Then  $U(0\tau 0^{n_\tau} 1) = V(\tau)$  and  $|0\tau 0^{n_\tau} 1| \leq 16 \cdot |\tau|$ , hence  $U$  is  $\frac{1}{16}$ -universal.

Now consider the binary expansion of the halting probability  $\Omega_U$ . The first bit after the dot is 1 as the strings starting with 1 contribute  $\frac{1}{2}$  to the halting probability of  $U$ . Furthermore, the strings of length  $4^{m+1}$  starting with a 0 in the domain of  $U$  contribute  $4^{-m-1} \cdot a_m$  to the halting probability of  $U$ . Here  $a_m$  is the number of strings up to the length  $4^m$  in the domain of  $V$ . Because  $a_m \leq 2^{4^m}$  it follows that  $a_m$  can be written with  $4^m$  bits. So, in the binary expansion of  $\Omega_U$ , the bits from the positions  $4^m + 2$  until  $3 \cdot 4^m + 1$  are all 0; the bits from the positions  $4^{m+1} + 1$  to  $4^m$  describe the binary value of  $a_m$ . If  $8n = 4^m + 8$  and  $\tau$  is

the string of the first  $8n$  bits of  $\Omega_U$  after the dot, then  $U(1^n0\tau) = \tau0^{13n}$  is a prefix of  $\Omega_U$  of length  $21n$  which is generated by the program  $1^n0\tau$  of length  $9n + 1$ . As this works for all  $n$  of the form  $4^m + 8$  with  $m \in \{2, 3, 4, \dots\}$ , it follows that  $\Omega_U$  is not  $(\frac{1}{2}, U)$ -random.  $\square$

## 8 Conclusion

In this paper we have introduced the notion of  $\varepsilon$ -universal machine and studied its halting probability. An  $\varepsilon$ -universal machine is capable of simulating every other machine, but less efficiently than a universal machine  $V$ . More precisely, the length of the simulating program on the universal machine is bounded up to a fixed constant by the length of the simulated program divided by  $\varepsilon$ . The halting probability of an  $\varepsilon$ -universal machine is left-computable and  $(\varepsilon, V)$ -random. The main result of this paper is the extension of the representability theorem for left-computable random reals to the case of  $\varepsilon$ -random reals: *a real is left-computable and  $(\varepsilon, V)$ -random iff it is the halting probability of an  $\varepsilon$ -universal machine*. Finally, we showed that left-computable  $\varepsilon$ -random reals are provable  $(\varepsilon, V)$ -random in Peano Arithmetic, for some, but not all of their representations. Furthermore, we refuted Stay's conjecture stating that  $\Omega_U$  is  $(1, U)$ -random provided  $U$  is  $\varepsilon$ -universal.

## Acknowledgements

We thank Mike Stay for suggesting the definition of  $\varepsilon$ -universal machine, Kohtaro Tadaki for suggesting a simplification of the definition of  $V_\varepsilon$ , and both for valuable discussions.

## References

- [1] Cristian S. Calude. *Information and Randomness. An Algorithmic Perspective*, 2nd Edition, Revised and Extended, Springer Verlag, Berlin, 2002.
- [2] Cristian S. Calude and Nicholas J. Hay. Every computably enumerable random real is provably computably enumerable random, *Logic Journal of the IGPL* (to appear). (also as *Research Report of CDMTCS*, 328, 2008)
- [3] Cristian S. Calude, Peter Hertling, Bakhadyr Khoussainov and Yongge Wang. Recursively enumerable reals and Chaitin  $\Omega$  numbers, in: M. Morvan, C. Meinel, D. Krob (eds.), *Proceedings of the 15th Symposium on Theoretical Aspects of Computer Science* (Paris), Springer-Verlag, Berlin, 1998, 596–606. Full paper in *Theoret. Comput. Sci.* 255 (2001), 125–149.

- [4] Cristian S. Calude, Ludwig Staiger and Sebastiaan A. Terwijn. On partial randomness, *Annals of Applied and Pure Logic*, 138 (2006), 20–30.
- [5] Gregory J. Chaitin. A theory of program size formally identical to information theory, *Journal of the Association of Computing Machinery* 22 (1975), 329–340.
- [6] Gregory J. Chaitin. *Algorithmic Information Theory*, Cambridge University Press, Cambridge, 1987 (3rd printing 1990).
- [7] André Nies. *Computability and Randomness*. Oxford Press, Oxford, 2009.
- [8] Piergiorgio G. Odifreddi. *Classical Recursion Theory*, vol. 1, Elsevier, 1997.
- [9] Richard Kaye. *Models of Peano Arithmetic*, Oxford Press, Oxford, 1991.
- [10] Antonin Kučera and Theodore A. Slaman. Randomness and recursive enumerability, *SIAM Journal on Computing*, 31, 1 (2001), 199–211.
- [11] Jan Reimann and Frank Stephan. On hierarchies of randomness tests, in S. S. Goncharov, H. Ono, R. Downey (eds.). *Proceedings 9th Asian Logic Conference, “Mathematical Logic in Asia”*, World Scientific, Singapore, 2006, 215–232.
- [12] Dimiter Skordev. Characterization of the computable real numbers by means of primitive recursive functions, in J. Blanck, V. Brattka, P. Hertling (eds.). *Proceedings of Computability and Complexity in Analysis 2000*, LNCS 2064, Springer-Verlag, Berlin, 2001, 296–309.
- [13] Mike Stay. Personal communication to C. Calude, 7 May 2007.
- [14] Rorbert M. Solovay. *Draft of a paper (or series of papers) on Chaitin’s work ... done for the most part during the period of Sept.–Dec. 1974*, unpublished manuscript, IBM Thomas J. Watson Research Center, Yorktown Heights, New York, May 1975, 215 pp.
- [15] Ludwig Staiger. Kolmogorov complexity and Hausdorff dimension, *Information and Computation* 103 (1993), 159–194.
- [16] Ludwig Staiger. A tight upper bound on Kolmogorov complexity and uniformly optimal prediction, *Theory of Computing Systems* 31 (1998), 215–229.
- [17] Kohtaro Tadaki. A generalization of Chaitin’s halting probability  $\Omega$  and halting self-similar sets, *Hokkaido Mathematical Journal* 31 (2002), 219–253.

- [18] Kohtaro Tadaki. Equivalent characterizations of partial randomness for recursively enumerable real, [arXiv:0805.2691](https://arxiv.org/abs/0805.2691), 2008. (also at <http://ims.nju.edu.cn/conference/randomness/tadaki.pdf>)