CDMTCS Research Report Series

A Characterization of C.E. Random Reals

Cristian S. Calude
Department of Computer Science
University of Auckland
Auckland, New Zealand

CDMTCS-095
March 1999

Centre for Discrete Mathematics and
Theoretical Computer Science

A Characterization of C.E. Random Reals*

Cristian S. Calude

Department of Computer Science
University of Auckland
Private Bag 92019, Auckland
New Zealand
Email: cristian@cs.auckland.ac.nz

Abstract

A real α is computably enumerable if it is the limit of a computable, increasing, converging sequence of rationals; α is random if its binary expansion is a random sequence. Our aim is to offer a self-contained proof, based on the papers [7, 14, 4, 13], of the following theorem: *a real is c.e. and random if and only if it a Chaitin Ω real, i.e., the halting probability of some universal self-delimiting Turing machine.*

1 Introduction

We will consider only reals in the unit interval. A real α is computably enumerable (c.e.) if it is the limit of a computable, increasing, converging sequence of rationals. A real α is random if its binary expansion is a random (infinite) sequence (cf. [7, 8, 1]); the choice of base is irrelevant (cf. [5]).

The halting probability of a universal self-delimiting Turing machine (Chaitin's Ω real, [7, 8, 10]) is a random c.e. real. Are there other c.e. random reals? We will show that the answer is negative: *the set of c.e. random reals coincides with the set of Chaitin's Ω reals.*

The proof uses an intermediate class of c.e. reals, Solovay's Ω-like reals, and shows that this class coincides with the class of Ω reals, on one hand, and with the class of c.e. reals, on the other hand.

Chaitin [7] proved that every Ω real is c.e. and random. Solovay [14] proved that Ω-like reals are c.e. and random. Solovay also showed that every Chaitin Ω real is Ω-like. In [4] Calude, Hertling, Khoussainov and Wang showed that the converse implication is true as well: every Ω-like real in the unit interval is the halting probability of a universal self-delimiting Turing machine. Finally, Slaman [13] proved that every c.e. random real is Ω-like.

The paper is organised as follows. Section 2 is devoted to basic notation; in Section 3 we introduce self-delimiting Turing machines, program-size complexity, Chaitin's Ω

*This paper was written during the author's visit to the Department of Mathematics, University of Chicago and was presented on 19 February 1999 to "Soare's Logic Seminar". I wish to thank Bob Soare for encouraging me to write this paper.

reals, and c.e. reals. In Section 4 we prove that every Ω real is c.e. and random. Section 5 introduces Solovay's domination relation and proves some basic facts about it. In Section 6 we prove that every Ω real is Ω-like. In the next section we prove the converse implication, namely, that every Ω-like real is the halting probability of some universal self-delimiting Turing machine. Section 8 shows that every c.e. random real is Ω-like. Finally, Section 9 is dedicated to some comments.

2 Notation

By $\mathbf{N}$ we denote the set of nonnegative integers. A sequence $q_0, q_1, q_2, \ldots$ of numbers (integers, rationals, or reals) is said to be increasing (non-decreasing) if $q_i < q_{i+1}$ (if $q_i \leq q_{i+1}$) for all i. If f and g are natural number functions, the formula $f(n) \leq g(n) + O(1)$ means that there is a constant $c > 0$ with $f(n) \leq g(n) + c$, for all n. If X and Y are sets, then $f : X \stackrel{o}{\to} Y$ denotes a partial function defined on a subset of X.

Let $\Sigma = \{0, 1\}$ denote the binary alphabet. Let Σ^* be the set of (finite) binary strings, and Σ^ω the set of infinite binary sequences. The length of a string x is denoted by $|x|$; λ is the empty string. Let $<$ be the quasi-lexicographical order on Σ^* induced by $0 < 1$ and let $string_n$ $(n \geq 0)$ be the nth string under this ordering. For strings $x, y \in \Sigma^*$, xy is the concatenation of x and y. For a sequence $\mathbf{x} = x_0 x_1 \cdots x_n \cdots \in \Sigma^\omega$ and an integer number $n \geq 1$, $\mathbf{x}(n)$ denotes the initial segment of length n of $\mathbf{x}$ and x_i denotes the ith digit of $\mathbf{x}$, i.e., $\mathbf{x}(n) = x_0 x_1 \cdots x_{n-1}$. Lower case letters k, l, m, n will denote nonnegative integers, and x, y, z strings. By $\mathbf{x}, \mathbf{y}, \cdots$ we denote infinite sequences from Σ^ω; finally, we reserve α, β, γ for reals. Capital letters are used to denote subsets of Σ^*. We fix a standard computable pairing function $\lambda k, y\langle k, y\rangle$ defined on $\mathbf{N} \times \Sigma^*$ with values in Σ^*. For a set $A \subseteq \Sigma^*$ let $A_k = \{x \mid \langle k, x\rangle \in A\}$. For $A \subseteq \Sigma^*$, $A\Sigma^\omega$ denotes the set of sequences $\{w\mathbf{x} \mid w \in A, \mathbf{x} \in \Sigma^\omega\}$. The sets $A\Sigma^\omega$ are the open sets in the natural topology on Σ^ω. Computably enumerable (c.e.) open sets are sets of the form $A\Sigma^\omega$, where $A \subseteq \Sigma^*$ is c.e. Let μ denote the usual product measure on Σ^ω, given by $\mu(\{w\}\Sigma^\omega) = 2^{-|w|}$, for $w \in \Sigma^*$. For a measurable set $\mathbf{C}$ of infinite sequences, $\mu(\mathbf{C})$ is the probability that $\mathbf{x} \in \mathbf{C}$ when $\mathbf{x}$ is chosen by a random experiment in which an independent toss of a fair coin is used to decide whether $x_n = 1$. A set $A \subseteq \Sigma^*$ is prefix-free if no string in A is a proper prefix of another. If A is prefix-free, then $\mu(A\Sigma^\omega) = \sum_{w \in A} 2^{-|w|}$.

We assume familiarity with Turing machine computations, cf. Soare [12].

3 C.E. Reals

A self-delimiting Turing machine C has a program tape, an output tape, and a work tape. Only 0's, 1's and blanks can ever appear on a tape. The program tape and the output tape are infinite to the right, while the worktape is infinite in both directions. Each tape has a scanning head. The program and output tape heads cannot move left, but the worktape head can move in both directions. The program tape is read-only, the output tape is write-only, and the worktape is read/write.

The machine C starts in the initial state with a program $x \in \Sigma^*$ on its program tape, the output tape blank, and the worktape blank. The left-most cell of the program tape is blank and the program tape head initially scans this cell. The program x lies immediately to the right of this cell and the rest of the program tape is blank. The output tape head initially scans the left-most cell of the output tape.

During each cycle of operation the machine reads the content of the scanned program tape cell and of the scanned worktape cell; it may halt, move the read head of the program tape one cell to the right, write a 0, a 1, or a blank on the scanned worktape cell, move the read/write head of the worktape one cell to the left or to the right, and write a 0 or a 1 on the scanned output tape cell and move the write head of the output tape one cell to the right. The machine changes state: the action performed and the next state are both functions of the present state and the contents of the two cells being scanned by the program tape head and the worktape head.

If, after finitely many steps, C halts with the program tape head scanning the last bit of x, then the computation is a success, and we write $C(x) < \infty$; the output of the computation is the string $C(x) \in \Sigma^*$ appearing on the output tape. Otherwise, the computation is a failure, we write $C(x) = \infty$, and there is no output.

A successful computation must end with the program tape head scanning the last bit of the program. Since the program tape head is read-only and cannot move left, the program set

$$PROG_C = \{x \in \Sigma^* \mid C(x) < \infty\}$$

is an *instantaneous code*, i.e., a prefix-free set of strings; of course, $PROG_C$ is c.e. Conversely, every prefix-free c.e. set set of strings is the domain of some self-delimiting Turing machine. It follows by Kraft's inequality that, for every self-delimiting Turing machine C,

$$\Omega_C = \mu(PROG_C \Sigma^\omega) = \sum_{x \in PROG_C} 2^{-|x|} \leq 1.$$

The number Ω_C is called the halting probability of C.

Let C be a self-delimiting Turing machine. The *program-size complexity* of the string $x \in \Sigma^*$ (relatively to C) is $H_C(x) = \min\{|y| \mid y \in \Sigma^*,\ C(y) = x\}$, where $\min \emptyset = \infty$.

Theorem 3.1 (Invariance Theorem; Chaitin [7]) *There is a self-delimiting Turing machine U such that for every self-delimiting Turing machine C, $H_U(x) \leq H_C(x) + O(1)$.*

A self-delimiting Turing machine U satisfying Theorem 3.1 is called *universal.*

Clearly, every universal self-delimiting machine produces every string. We denote by x^* the *canonical program* of x, i.e., $x^* = \min\{y \in \Sigma^* \mid U(y) = x\}$, where the minimum is taken on strings according to the quasi-lexicographical order.

The halting probability Ω_U of a universal self-delimiting machine U is called a *Chaitin Ω real.*

The following extension due to Chaitin [7] (see Calude, Grozea [3] for a short proof) of Kraft's inequality is very useful to construct self-delimiting Turing machines satisfying certain properties:

Theorem 3.2 (Kraft-Chaitin) *Given a c.e. list of "requirements" $\langle n_i, s_i \rangle$ ($i \geq 0, s_i \in \Sigma^*, n_i \in \mathbf{N}$) such that $\sum_i 2^{-n_i} \leq 1$, we can effectively construct a self-delimiting Turing machine C and a computable one-to-one enumeration $x_0, x_1, x_2, \ldots$ of strings x_i of length n_i such that $C(x_i) = s_i$ for all i and $C(x) = \infty$ if $x \notin \{x_i \mid i \in \mathbf{N}\}$.*[1]

Random (infinite) sequences were defined by Martin-Löf [11] using "randomness tests". A Martin-Löf test is a c.e. set $A \subseteq \Sigma^*$ satisfying the inequality

$$\mu(A_i \Sigma^\omega) \leq 2^{-i},$$

[1]Notice that $\Omega_C = \sum_i 2^{-n_i}$.

for all $i \in \mathbf{N}$. An alternative characterization can be obtained using program-size complexity (see Calude [1] for more details).

Theorem 3.3 *Let $\mathbf{x} \in \Sigma^\omega$. The following statements are equivalent:*

1. *There is a constant c such that $H_U(\mathbf{x}(n)) > n - c$, for every integer $n > 0$.*
2. *For every Martin-Löf test A, $\mathbf{x} \notin \bigcap_{i \geq 0}(A_i\Sigma^\omega)$.*
3. *We have: $\lim_{n\to\infty} H(\mathbf{x}(n)) - n = \infty$.*

A real α is called c.e. if it is the limit of a computable increasing sequence of rationals; equivalently, α is if the set of all rationals less than α is c.e.

A sequence $\mathbf{x} \in \Sigma^\omega$ is *random* if it satisfies one of the equivalent conditions in Theorem 3.3.[2] A real α is *random* if its binary expansion $\mathbf{x}$ (i.e., $\alpha = 0.\mathbf{x}$) is random.[3]

4 Ω Reals Are C.E. and Random

This section is devoted to the following result:

Theorem 4.1 (Chaitin [7]) *The halting probability Ω_U, of a universal self-delimiting machine U, is random.*

Proof. Let f be a computable one-to-one function which enumerates $PROG_U$, the domain of U. Let $\omega_k = \sum_{j=0}^{k} 2^{-|f(j)|}$. Clearly, (ω_k) is a computable, increasing sequence of rationals converging to Ω_U, so Ω_U is c.e. Consider the binary expansion of $\Omega_U = 0.\Omega_0\Omega_1\cdots$

We define a self-delimiting Turing machine C as follows: on input $x \in \Sigma^*$ C first "tries to compute" $y = U(x)$ and the smallest number t with $\omega_t \geq 0.y$. If successful, $C(x)$ is the first (in quasi-lexicographical order) string not belonging to the set $\{U(f(0)), U(f(1)), \ldots, U(f(t))\}$; otherwise, $C(x) = \infty$ if $U(x) = \infty$ or t does not exist.

If $x \in PROG_C$ and x' is a string with $U(x) = U(x')$, then $C(x) = C(x')$. Applying this to $x \in PROG_C$ and the canonical program $x' = (U(x))^*$ of $U(x)$ yields

$$H_C(C(x)) \leq |x'| = H_U(U(x)).$$

Furthermore, by the universality of U, for all $x \in PROG_C$:

$$H_U(C(x)) \leq H_C(C(x)) + O(1) \leq H_U(U(x)) + O(1). \tag{1}$$

Now, fix a number n and assume that x is a string with $U(x) = \Omega_0\Omega_1\cdots\Omega_{n-1}$. Then $C(x) < \infty$. Let t be the smallest number (computed in the second step of the computation of C) with $\omega_t \geq 0.\Omega_0\Omega_1\cdots\Omega_{n-1}$. We have

$$0.\Omega_0\Omega_1\cdots\Omega_{n-1} \leq \omega_t < \omega_t + \sum_{s=t+1}^{\infty} 2^{-|f(s)|} = \Omega_U \leq 0.\Omega_0\Omega_1\cdots\Omega_{n-1} + 2^{-n}.$$

[2] Note that the program-size complexities of every two universal self-delimiting machines U and V are asymptotically equal: $H_U(x) = H_V(x) + O(1)$. Hence the choice of the underlying universal self-delimiting Turing machine is irrelevant in the above characterization.

[3] The choice of the binary base does not play any role, cf. Calude, Jürgensen [5]: randomness is a property of reals not of names of reals.

Hence, $\sum_{s=t+1}^{\infty} 2^{-|f(s)|} \leq 2^{-n}$, which implies $|f(s)| \geq n$, for every $s \geq t+1$.

¿From the construction of C we conclude that $H_U(C(x)) \geq n$. Using (1) we obtain

$$n \leq H_U(C(x)) \leq H_C(C(x)) + O(1) \leq H_U(U(x)) + O(1) = H_U(\Omega_0\Omega_1 \cdots \Omega_{n-1}) + O(1).$$

which proves that the sequence $\Omega_0\Omega_1 \cdots$ is random, i.e., Ω_U is random. □

5 Domination and Ω-like Reals

In order to compare the information contents of c.e. reals, Solovay [14] has introduced the following definition (see also Chaitin [8]): a c.e. real α *dominates* a c.e. real β (write $\beta \leq_{dom} \alpha$) if there are two computable, increasing (or non-decreasing) sequences $(a_i)_i$ and $(b_i)_i$ of rationals and a constant c with $\lim_{n\to\infty} a_n = \alpha$, $\lim_{n\to\infty} b_n = \beta$, and $c(\alpha - a_n) \geq \beta - b_n$, for all n.

The relation $\leq_{dom}$ is transitive and reflexive, hence it naturally defines a partially ordered set whose elements are the $=_{dom}$-equivalence classes of c.e. reals.[4][5]

We continue by considering a relation between c.e. sets which is very close, but not equivalent, to the domination relation. Let A, B be infinite, prefix-free c.e. sets. Following [4], we say that the set A *strongly simulates* the set B (write $B \leq_{ss} A$) if there is a partial computable function $f : \Sigma^* \stackrel{o}{\to} \Sigma^*$ which satisfies the following conditions:

1. $A = dom(f)$,
2. $B = f(A)$,
3. $|x| \leq |f(x)| + O(1)$, for all $x \in A$.

Note that $\leq_{ss}$ is reflexive and transitive.

Lemma 5.1 *If A, B are infinite prefix-free c.e. sets and $B \leq_{ss} A$, then $\mu(B\Sigma^\omega) \leq_{dom} \mu(A\Sigma^\omega)$.*

Proof. Let (x_i) be a one-to-one computable enumeration of A. Let f be a function and $c > 0$ be a constant as in the above definition. For each n and each $y \in B \setminus \{f(x_0), \ldots, f(x_n)\}$ there is a string $x \in A \setminus \{x_0, \ldots, x_n\}$ with $y = f(x)$ and $|x| \leq |f(x)| + c$. Hence,

$$\begin{aligned} 2^{-B} - 2^{-\{f(x_0),\ldots,f(x_n)\}} &= 2^{-(B\setminus\{f(x_0),\ldots,f(x_n)\})} \\ &\leq 2^c \cdot 2^{-(A\setminus\{x_0,\ldots,x_n\})} \\ &= 2^c \cdot (2^{-A} - 2^{-\{x_0,\ldots,x_n\}}). \end{aligned}$$

[4] This partially ordered set has a minimum element which is the equivalence class containing exactly all computable reals. It has a maximum element which is the equivalence class containing exactly all Chaitin Ω reals. In fact, it is an upper semilattice: the least upper bound of any two classes containing c.e. reals α and β, respectively, is the class containing the c.e. real $\alpha+\beta$; cf. Calude, Hertling, Khoussainov, Wang [4].

[5] There is an important relationship between domination and randomness. If $\alpha \leq_{dom} \beta$, then β is "more random" than α in the sense that the program-size complexity of the first n digits of α does *not* exceed the complexity of the first n digits of β by more than a constant, cf. Solovay [14]. The more random an effective object is, the closer it is to Chaitin Ω numbers; the less random an effective object is, the closer it is to computable reals. The converse implication is false, namely there are c.e. reals $0.\mathbf{x}$ and $0.\mathbf{y}$ such that $H(\mathbf{x}(n)) \leq H(\mathbf{y}(n)) + O(1)$ and $0.\mathbf{y}$ does not dominate $0.\mathbf{x}$, cf. Calude, Coles [2].

We conclude that $\mu(B\Sigma^\omega) \leq_{dom} \mu(A\Sigma^\omega)$. □

The following partial converse implication in Lemma 5.1 is true and very important, cf. Calude, Hertling, Khoussainov, Wang [4].[6]

Theorem 5.2 *Let α be a c.e. real, and B be an infinite prefix-free c.e. set. If $\mu(B\Sigma^\omega) \leq_{dom} \alpha$, then there is an infinite prefix-free c.e. set $A \subset \Sigma^*$ such that $\alpha = \mu(A\Sigma^\omega)$ and $B \leq_{ss} A$.*

Proof. Assume that $\mu(B\Sigma^\omega) \leq_{dom} \alpha$. Let (y_i) be a one-to-one computable enumeration of B and $(a_n)_n$ be an increasing computable sequence of positive rationals converging to α. In view of the domination property of α, there are an increasing, total computable function $f : \mathbf{N} \to \mathbf{N}$ and a constant $c \in \mathbf{N}$ such that, for each $n \in \mathbf{N}$,

$$2^c \cdot (\alpha - a_n) \geq \mu(B\Sigma^\omega) - \sum_{i=0}^{f(n)} 2^{-|y_i|}. \tag{2}$$

Without loss of generality, we may assume that

$$a_0 > \sum_{i=0}^{f(0)} 2^{-|y_i|-c} \tag{3}$$

(otherwise we increase c). We construct a computable sequence $(n_i)_{i\geq 0}$ of numbers and a computable double sequence $(m_{i,j})_{i,j\geq 0}$ of elements in $\mathbf{N} \cup \{\infty\}$. These numbers n_i and the numbers $m_{i,j} \neq \infty$ will be the lengths of the strings in the set A which will be constructed. The numbers n_i will guarantee that $B \leq_{ss} A$. The numbers $m_{i,j}$ will be used "to fill" the set A up in order to get exactly $\alpha = \mu(A\Sigma^\omega)$. This will follow directly from Equation (4) below.

Construction of (n_i): Put $n_i = |y_i| + c$, for all i.

Begin of construction of $(m_{i,j})$.

Stage 0. Let $m_{i,j} = \infty$, for all $i < f(0)$ and $j \in \mathbf{N}$, and define the positive integers $(m_{f(0),j})_{j\geq 0}$ inductively in such a way that

$$\sum_{j=0}^{\infty} 2^{-m_{f(0),j}} = a_0 - \sum_{i=0}^{f(0)} 2^{-n_i}.$$

Stage s $(s \geq 1)$. If

$$a_s \leq \sum_{i=0}^{f(s)} 2^{-n_i} + \sum_{i=0}^{f(s-1)} \sum_{j=0}^{\infty} 2^{-m_{i,j}},$$

[6] In [4] one proves the existence of two infinite prefix-free c.e. sets A and B such that $\mu(A\Sigma^\omega) = \mu(B\Sigma^\omega) = 1$ but $A \not\leq_{ss} B$ and $B \not\leq_{ss} A$.

then let $m_{i,j} = \infty$, for all i with $f(s-1) < i \leq f(s)$ and $j \in \mathbf{N}$. Otherwise, let $m_{i,j} = \infty$, for all i with $f(s-1) < i < f(s)$ and $j \in \mathbf{N}$, and let positive integers $(m_{f(s),j})_{j \geq 0}$ be inductively defined in such a way that

$$\sum_{j=0}^{\infty} 2^{-m_{f(s),j}} = a_s - \left(\sum_{i=0}^{f(s)} 2^{-n_i} + \sum_{i=0}^{f(s-1)} \sum_{j=0}^{\infty} 2^{-m_{i,j}} \right).$$

End of construction of $(m_{i,j})$.

Next we prove the equality:

$$\alpha = \sum_{i=0}^{\infty} \left(2^{-n_i} + \sum_{j=0}^{\infty} 2^{-m_{i,j}} \right), \tag{4}$$

by distinguishing the following two cases.

Case 1. If there are infinitely many stages s such that

$$a_s = \sum_{i=0}^{f(s)} \left(2^{-n_i} + \sum_{j=0}^{\infty} 2^{-m_{i,j}} \right),$$

then (4) holds.

Case 2. Assume the inequality $a_s < \sum_{i=0}^{f(s)} \left(2^{-n_i} + \sum_{j=0}^{\infty} 2^{-m_{i,j}} \right)$ holds true for almost all $s \in \mathbf{N}$ and we notice that

$$\alpha = \lim_{s \to \infty} a_s \leq \sum_{i=0}^{\infty} \left(2^{-n_i} + \sum_{j=0}^{\infty} 2^{-m_{i,j}} \right). \tag{5}$$

For the inverse estimate, we define s_0 to be the largest stage such that

$$a_{s_0} = \sum_{i=0}^{f(s_0)} \left(2^{-n_i} + \sum_{j=0}^{\infty} 2^{-m_{i,j}} \right).$$

Such a stage s_0 exists because of (3) and the construction. By (2) we have

$$\alpha - a_{s_0} \geq \sum_{i=f(s_0)+1}^{\infty} 2^{-|y_i|-c}.$$

Hence, by the construction,

$$\alpha \geq \sum_{i=0}^{\infty} \left(2^{-n_i} + \sum_{j=0}^{\infty} 2^{-m_{i,j}} \right). \tag{6}$$

By combining (5) and (6) we obtain the equality (4) also in this case.

Let $h : \mathbf{N} \to \{(i,j) \in \mathbf{N}^2 \mid m_{i,j} \neq \infty\}$ be a computable bijection (note that by construction the set $\{(i,j) \in \mathbf{N}^2 \mid m_{i,j} \neq \infty\}$ is infinite) and define a computable sequence $(m'_i)_i$ of numbers by $m'_i = m_{h(i)}$. Using this sequence we define $(n'_i)_i$ by $n'_{2i} = n_i$ and $n'_{2i+1} = m'_i$. By Kraft-Chaitin Theorem 3.2 and (4), combined with $0 < \alpha \leq 1$, we can construct a one-to-one computable sequence $(x_i)_i$ of strings with $|x_i| = n'_i$ such that the set $\{x_i \mid i \in \mathbf{N}\}$ is prefix-free. Set $A = \{x_i \mid i \in \mathbf{N}\}$ and, using (4), obtain

$$\mu(A\Sigma^\omega) = \sum_{i=0}^{\infty} 2^{-n'_i} = \sum_{i=0}^{\infty} 2^{-n_i} + \sum_{i=0}^{\infty} 2^{-m'_i} = \alpha\,.$$

Finally we define a computable function $g : A \to B$ by $g(x_{2i}) = y_i$ and such that $|g(x_{2i+1})| \geq |x_{2i+1}|$, for all i. This is possible because B is infinite. Obviously, $g(A) = B$, and $|x| \leq |g(x)| + c$, for all $x \in A$, showing that $B \leq_{ss} A$. □

6 Ω Reals Are Ω-Like

Following Solovay ([14]) we say that a computable increasing, and converging sequence $(a_i)_i$ of rationals is *universal* if for every computable, increasing and converging sequence $(b_i)_i$ of rationals there exists a number $c > 0$ such that $c(\alpha - a_n) \geq \beta - b_n$, for all n, where $\alpha = \lim_{n\to\infty} a_n$ and $\beta = \lim_{n\to\infty} b_n$. Solovay called a real *Ω-like* if it is the limit of a universal computable, increasing sequence of rationals.

In [4] one proves the following:

Theorem 6.1 (Solovay) *Let U be a universal self-delimiting Turing machine. Every computable, increasing sequence of rationals converging to Ω_U is universal.*

Proof. Let (a_n) be an increasing, computable sequence of rationals with limit Ω_U, and let (b_n) be an increasing, computable, converging sequence of rationals. Set $\beta = \lim_{n\to\infty} b_n$. We have to show that there is a constant $c > 0$ with $c(\Omega_U - a_n) \geq \beta - b_n$ for all n.

Let (x_i) be a one-to-one, computable enumeration of $PROG_U$, and $\Omega_{U,n} = \sum_{i=0}^{n} 2^{-|x_i|}$. We define a total computable, increasing function $g : \mathbf{N} \to \mathbf{N}$, where we also define $g(-1) = -1$, by

$$g(n) = \min\{j > g(n-1) \mid \Omega_{U,j} \geq a_n\}\,.$$

The sequence $(\Omega_{U,g(n)})$ is an increasing, computable sequence with limit Ω_U. In view of the inequality $\Omega_U - a_n \geq \Omega_U - \Omega_{U,g(n)}$, it is sufficient to prove that there is a constant $c > 0$ with $c(\Omega_U - \Omega_{U,g(n)}) \geq \beta - b_n$ for all n.

For each $i \in \mathbf{N}$, let y_i be the first string (with respect to the quasi-lexicographical ordering) which is not in the set $\{U(x_j) \mid j \leq g(i)\} \cup \{y_j \mid j < i\}$. Furthermore, put $n_i = [-\log(b_{i+1} - b_i)] + 1$. Since $\sum_{i=0}^{\infty} 2^{-n_i} \leq \beta - b_0 < 1$, by Kraft-Chaitin Theorem 3.2 we can construct a self-delimiting Turing machine C such that, for every $i \in \mathbf{N}$, there is a string $u_i \in \Sigma^{n_i}$ satisfying $C(u_i) = y_i$. Hence, there is a constant c_C such that $H_U(y_i) \leq n_i + c_C$. In view of the choice of y_i, there is a string $x'_i \in PROG_U \setminus \{x_j \mid j \leq g(i)\}$ such that $|x'_i| \leq n_i + c_C$ and $U(x'_i) = y_i$. For different i and j we have $y_i \neq y_j$, whence $x'_i \neq x'_j$. Finally we obtain

$$\begin{aligned}\Omega_U - \Omega_{U,g(n)} &= \textstyle\sum_{i=g(n)+1}^{\infty} 2^{-|x_i|} \geq \sum_{i=n}^{\infty} 2^{-|x'_i|} \\ &\geq \textstyle\sum_{i=n}^{\infty} 2^{-n_i - c_C} \geq 2^{-c_C-1} \sum_{i=n}^{\infty} (b_{i+1} - b_i) = 2^{-c_C-1}(\beta - b_n),\end{aligned}$$

which proves the assertion. □

7 Ω-like Reals Are Ω Reals

First we note that

Lemma 7.1 *An Ω-like real dominates every c.e. real.*

Theorem 7.2 (Calude, Hertling, Khoussainov, Wang [4]) *Every Ω-like real α is an Ω real, i.e., there exists a universal self-delimiting Turing machine U such that $\alpha = \Omega_U$.*

Proof. Let V be a universal self-delimiting Turing machine. Since α is Ω-like it dominates every c.e. real, in particular, $\mu(PROG_V\Sigma^\omega) \leq_{dom} \alpha$. By Theorem 5.2 there exist an infinite prefix-free c.e. set A with $\mu(A\Sigma^\omega) = \alpha$, a computable function $f : A \to PROG_V$ with $A = dom(f)$, $f(A) = PROG_V$, and a constant $c > 0$ such that $|x| \leq |f(x)| + c$, for all $x \in A$. We define a self-delimiting Turing machine U by $U(x) = V(f(x))$. The universality of V implies the universality of U and

$$\alpha = \mu(A\Sigma^\omega) = \mu(PROG_U\Sigma^\omega) = \Omega_U.$$

□

In view of Lemma 7.1 and Theorem 7.2 we get:[7]

Theorem 7.3 *Let α be a c.e. real. The following statements are equivalent:*

1. *There exists a universal computable, increasing sequence of rationals converging to α.*
2. *Every computable, increasing sequence of rationals with limit α is universal.*
3. *The real α dominates every c.e. real.*

8 Every C.E. Random Real Is Ω-like

Theorem 3.3 can be re-phrased directly for reals as follows: *A real α is random if and only if for every Martin-Löf test A, $\alpha \notin \bigcap_{i\geq 0} A_i$.* In the context of reals, a Martin-Löf test A is a uniformly c.e. sequence of c.e. open sets $(A_n)_n$ of the space Σ^ω such that $\mu(A_n) \leq 2^{-n}$.

Lemma 8.1 (Slaman [13]) *Let $(a_n)_n, (b_n)_n$ be two computable, increasing sequences of rationals converging to α and β, respectively. One of the following two conditions hold:*

A) *There is a Martin-Löf test A such that $\alpha \in \bigcap_{i\geq 0} A_i$.*

B) *There is a rational constant $c > 0$ such that $c(\alpha - a_i) \geq \beta - b_i$, for all i.*

Proof. We enumerate the Martin-Löf set A by stages. Let $A_n[s]$ be the union of finitely many open c.e. sets that have been enumerated into A_n during stages less than s. Put $A_n[0] = \emptyset$ and $A_n[s+1] = A_n[s] \cup (a_s, a_s + (b_s - b_{s_0})2^{-n})$, in case $a_s \notin A_n[s]$ and $b_s \neq b_{s_0}$; here s_0 is the last stage during which we enumerated a c.e. open set into A_n or

[7] The equivalence of the statements 1 and 3 comes from Chaitin [8].

$s_0 = 0$ if there was no such stage; otherwise, $A_n[s+1] = A_n[s]$. Clearly, $A_n = \bigcup_s A_n[s]$ is a disjoint union of c.e. open sets.

Let $t_1, t_2, \ldots, t_n, \ldots$ be the sequence of stages during which we do enumerate open sets into A_n. Then,

$$\begin{aligned}\mu(A_n) &= \mu(\bigcup_s A_n[s]) = \sum_{i\geq 1} \mu(A_n[t_i]) \\ &= \frac{1}{2^n}(b_{t_1} - b_0) + (b_{t_2} - b_{t_1}) + (b_{t_3} - b_{t_2}) + \cdots \\ &= \frac{1}{2^n}(\beta - b_0) \leq \frac{1}{2^n}\end{aligned}$$

If $\alpha \in \bigcap_{i\geq 0} A_i$, then A) holds. Assume that $\alpha \notin A_n$, for some n. We shall prove that $2^i(\alpha - a_i) \geq \beta - b_i$, for almost all i, so B) holds.

If the open set $(a_s, a_s + (b_s - b_{s_0})2^{-n})$ is enumerated into A_n at stage s, then there is a stage $t > s$ such that $a_t > a_s + (b_s - b_{s_0})2^{-n}$. Fix $i > 0$ and let t_0 be the greatest stage $t \leq i$ such that we enumerate something into A_n during stage t or $t_0 = 0$, otherwise. Let $t_0, t_1, t_2, \ldots, t_n, \ldots$ be the sequence of stages during which we do enumerate open sets into A_n. Clearly, $t_0 < i \leq t_1$. As

$$\alpha - a_{t_1} > a_{t_k} - a_{t_1} + (b_{t_k} - b_{t_{k-1}})2^{-n},$$

for all k and $a_{t_k} \notin A_n[t_1] \cup A_n[t_2] \cup \cdots \cup A_n[t_{k-1}]$, it follows that

$$a_{t_k} - a_{t_1} > a_{t_{k-1}} - a_{t_1} + (b_{t_{k-1}} - b_{t_{k-2}})2^{-n},$$

so

$$\alpha - a_{t_1} \geq \sum_{k\geq 1}(b_{t_k} - b_{t_{k-1}})2^{-n} = (\beta - b_{t_0})2^{-n}.$$

Finally, for every $i \geq \max\{t_0, t_1\}$,

$$\alpha - a_i \geq \alpha - a_{t_1} \geq (\beta - b_{t_0})2^{-n} \geq (\beta - b_i)2^{-n},$$

because $(a_n)_n, (b_n)_n$ are increasing. □

Theorem 8.2 (Slaman [13]) *Every c.e. random real is Ω-like.*

Proof. Apply Lemma 8.1: if A) holds, then α is not random; if B) holds, then $\beta \leq_{dom} \alpha$, and the theorem follows as β has been arbitrarily chosen. □

9 Final Comments

The following theorem summarizes the characterization of c.e. and random reals:

Theorem 9.1 *Let α be a c.e. real. The following conditions are equivalent:*

1. *The real α is c.e. and random.*

2. *For some universal self-delimiting Turing machine U, $\alpha = \Omega_U$.*

3. *The real α is Ω-like.*

4. *There exists a universal computable, increasing sequence of rationals converging to α.*

5. *Every computable, increasing sequence of rationals with limit α is universal.*

C.e. random reals have many interesting properties; for example, they are wtt-complete, but not tt-complete (cf. Calude and Nies [6]).

References

[1] C. Calude. *Information and Randomness. An Algorithmic Perspective.* Springer-Verlag, Berlin, 1994.

[2] C. S. Calude, R. J. Coles. Program-size complexity of initial segments and domination relation reducibility, in J. Karhumäki, H. A. Maurer, G. Păun, G. Rozenberg (eds.). *Jewels Are Forever*, Springer-Verlag, Berlin, 1999. (in press)

[3] C. Calude and C. Grozea. Kraft-Chaitin inequality revisited, *J. UCS* 5 (1996), 306–310.

[4] C. S. Calude, P. Hertling, B. Khoussainov, and Y. Wang. Recursively enumerable reals and Chaitin Ω numbers, in: M. Morvan et al. (eds.), *Proceedings of the 15th Symposium on Theoretical Aspects of Computer Science (Paris)*, Springer–Verlag, Berlin, 1998, 596–606.

[5] C. Calude, H. Jürgensen. Randomness as an invariant for number representations, in H. Maurer, J. Karhumäki, G. Rozenberg (eds.). *Results and Trends in Theoretical Computer Science*, Springer-Verlag, Berlin, 1994, 44-66.

[6] C. Calude, A. Nies. Chaitin Ω numbers and strong reducibilities, *J. UCS* 3 (1997), 1161–1166.

[7] G. J. Chaitin. A theory of program size formally identical to information theory, *J. Assoc. Comput. Mach.* 22 (1975), 329–340. (Reprinted in: [9], 113–128)

[8] G. J. Chaitin. Algorithmic information theory, *IBM J. Res. Develop.* 21 (1977), 350–359, 496. (Reprinted in: [9], 44–58)

[9] G. J. Chaitin. *Information, Randomness and Incompleteness, Papers on Algorithmic Information Theory*, World Scientific, Singapore, 1987. (2nd ed., 1990)

[10] G. J. Chaitin. *The Unknowable*, Springer-Verlag, Singapore, 1999 (in press).

[11] P. Martin-Löf. The definition of random sequences, *Inform. and Control* 9 (1966), 602–619.

[12] R. I. Soare. *Recursively Enumerable Sets and Degrees*, Springer-Verlag, Berlin, 1987.

[13] T. A. Slaman. *Random Implies Ω-Like*, manuscript, 14 December 1998, 2 pp.

[14] R. 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.