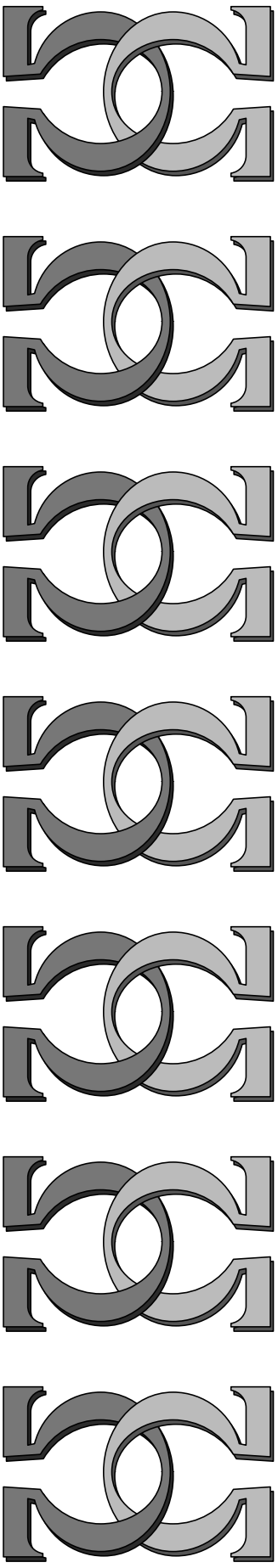

CDMTCS
Research
Report
Series

Real Numbers: From Computable to Random

C. S. Calude
University of Auckland, New Zealand

CDMTCS-141
August 2000

Centre for Discrete Mathematics and
Theoretical Computer Science

Real Numbers: From Computable to Random

Cristian S. Calude
Department of Computer Science
University of Auckland
Private Bag 92019, Auckland
New Zealand
E-mail: cristian@cs.auckland.ac.nz

Abstract

A real is computable if it is the limit of a computable, increasing, computably converging sequence of rationals. Omitting the restriction that the sequence converges computably we arrive at the notion of computably enumerable (c.e.) real, that is, the limit of a computable, increasing, converging sequence of rationals. A real is random if its binary expansion is a random sequence (equivalently, if its expansion in base $b \geq 2$ is random). The aim of this paper is to review some recent results on computable, c.e. and random reals. In particular, we will present a complete characterization of the class of c.e. and random reals in terms of halting probabilities of universal Chaitin machines, and we will show that every c.e. and random real is the halting probability of some Solovay machine, that is, a universal Chaitin machine for which ZFC (if sound) cannot determine more than its initial block of 1 bits. A few open problems will be also discussed.

1 Notation and Background

We will use notation that is standard in computability theory and algorithmic information theory; we will assume familiarity with Turing machine computations, computable and computably enumerable (c.e.) sets (see, for example, Soare [48] or Odifreddi [40]) and elementary algorithmic information theory (see, for example, Calude [7]).

By $\mathbf{N}, \mathbf{Q}, \mathbf{R}$ we denote the set of nonnegative integers (natural numbers), rationals and reals, respectively. 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.

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 $0 < 1$, that is, $\lambda < 0 < 1 < 00 < 01 < 10 < 11 < 000 < \cdots$ and let $string_n$ $(n \geq 0)$ be the nth string under this ordering. The concatenation of the strings s and t will be denoted by $s \frown t$. If j is one of 0 or 1, the string of length 1 whose sole component is j will be denoted by $\langle j \rangle$. A string s is a prefix of a string t $(s \subseteq t)$ if $t = s \frown r$, for some $r \in \Sigma^*$. A subset A of Σ^* is *prefix-free* if whenever s and t are in A and $s \subseteq t$, then $s = t$.

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. $\mathbf{x}(n) = x_0 x_1 \cdots x_{n-1} \in \Sigma^*$. Lower case letters k, l, m, n will denote nonnegative integers, and s, t, x, y, z strings. By $\mathbf{x}, \mathbf{y}, \cdots$ we denote infinite sequences from Σ^ω; finally, we reserve $\alpha, \beta, \gamma, \omega, \Omega$ for reals. Capital letters are used to denote subsets of Σ^*. We fix a standard computable bijective (pairing) function $\langle , \rangle$ defined on $\mathbf{N} \times \Sigma^*$ with values in Σ^*. For a set $A \subseteq \Sigma^*$ let $A_k = \{x \mid \langle k, x \rangle \in A\}$.

Next we move to the probabilistic part. Consider the following experiment: Pick, at random using the Lebesgue measure on $[0, 1]$, a real α in the unit interval and note that the probability that some initial prefix of the binary expansion of α lies in the prefix-free set A is the real number:

$$\Omega_A = \sum_{s \in A} 2^{-|s|}. \tag{1}$$

More formally, for $A \subseteq \Sigma^*$, $A\Sigma^\omega$ denotes the set of sequences having a prefix in A, $\{w\mathbf{x} \mid w \in A,\ \mathbf{x} \in \Sigma^\omega\}$. 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 $x_n = 1$. If A is prefix-free, then $\mu(A\Sigma^\omega) = \sum_{w \in A} 2^{-|w|} = \Omega_A$.

Following Solovay [49, 50] we say that C is a *Chaitin machine* (self-delimiting Turing machine), shortly, a machine, if C is a Turing machine processing binary strings such that its program set (domain)

$$PROG_C = \{x \in \Sigma^* \mid C(x) \text{ halts}\}$$

is an *instantaneous code*, i.e. a prefix-free set of strings. Sometimes we will write $C(x) < \infty$ when C halts on x and $C(x) = \infty$ in the opposite case. Clearly, $PROG_C$ is c.e.; conversely, every prefix-free c.e. set of strings is the domain of some 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 1 (Invariance Theorem) *We can effectively construct a machine U (called* universal*) such that for every machine C, $H_U(x) \leq H_C(x) + O(1)$.*

Note that $PROG_U$ is c.e. but not computable.

The following extension due to Chaitin [21] (see Calude and Grozea [15] for a short proof) of Kraft's inequality is very useful in constructing machines satisfying certain properties:

Theorem 2 (Kraft–Chaitin) *Given a c.e. list of "requirements" $\langle n_i, s_i\rangle$ $(s_i \in \Sigma^*, n_i \in \mathbf{N}, i \geq 0)$ such that $\sum_i 2^{-n_i} \leq 1$, we can effectively construct a 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]

2 Computable and Uncomputable Reals

The complexity of real numbers is a central topic in classical computability theory (see Turing [54], Rice [44], Calude [6], Soare [48], Odifreddi [40], Bridges [5]), computable analysis (see Martin-Löf [39], Weihrauch [56], Pour–El and Richards [43], Ko [35], Bridges [4]), algorithmic information theory (see Chaitin [24, 26, 27], Martin-Löf [37], Calude [7]) and information based complexity (see Traub, Wasilkowski, and Woźniakowski [53]).

An important class of reals is certainly the set of computable reals. In order to define them we introduce the notions of computable sequence of rationals and computable convergence rate. A sequence (a_i) of rationals a_i is called *computable* if there is a Turing machine which, given a binary name for a nonnegative integer n, computes a name for the rational a_n, with respect to a standard notation of rationals. A sequence (α_i) of reals α_i is said to *converge computably* if it converges and there is a computable function $g : \mathbf{N} \to \mathbf{N}$ such that $|\alpha_i - \lim_{k\to\infty} \alpha_k| \leq 2^{-j}$, for all i, j with $i \geq g(j)$.

A real α is called *computable* if there exists a computable sequence of rationals which converges computably to α.

Theorem 3 *Let α be a real in the unit interval. Then, the following statements are equivalent:*

1. *The real α is computable.*
2. *There exists a computable sequence (a_n) of rationals with $|\alpha - a_n| \leq 2^{-n}$, for all n.*
3. *There exists a computable function $f : \mathbf{N} \to \{0, 1\}$ such that $\alpha = \sum_{i=0}^{\infty} f(i)2^{-i}$.*
4. *The set $\{q \in \mathbf{Q} \mid q < \alpha\}$ is computable.*

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

The equivalences of 1., 2. and 3. and the implication 3. $\Rightarrow$ 4. are uniform, but the implication 4. $\Rightarrow$ 3. is not uniform.

For example, all algebraic numbers, $\log_2 3$, π, the Euler number e are computable; actually, all real numbers commonly used in numerical analysis and natural sciences are computable. Of course, not all real numbers are computable (in fact, *most reals are not computable*).[2]

Given a computable sequence (a_i) of rationals which converges computably to a computable real α, and given a computable function $g : \mathbf{N} \to \mathbf{N}$ as in the definition above, by computing $a_{g(n)}$ one obtains a rational approximation of α with precision 2^{-n}. By considering an appropriately chosen computable subsequence of the sequence (a_i) one can speed up the convergence to a great extent.

On the other hand there are also computable sequences of rationals which converge to uncomputable reals. These sequences must converge noncomputably, i.e. very slowly. The first example of an uncomputable limit of a computable sequence of rationals has been given by Specker [51].[3]

It is well-known that there are reals which can be approximated by a computable, converging sequence of rationals, but not with a computable convergence rate. For example, if h is an injective, total computable function which enumerates a c.e. set of nonnegative integers which is not computable, then the sum

$$\sum_{k=0}^{\infty} 2^{-h(k)} \tag{2}$$

is the limit of the computable sequence of partial sums $(\sum_{k=0}^{n} 2^{-h(k)})_n$, but it is not a computable real (Specker's construction [51]). A very interesting special class of numbers of this form are the Chaitin Ω numbers which will be later introduced and discussed.

We continue with a simple but intriguing example. Let $time_U(string_i)$ be the running time of the computation $U(string_i)$[4], and define the real number

$$\Upsilon_U = \sum_i 2^{-i}/time_U(string_i). \tag{3}$$

At the first glanced the analogy between (2) and (3) suggests that Υ_U is uncomputable because it is essentially defined in terms of an uncomputable set, $PROG_U$. This intuition is false: *the real Υ_U is computable.* Indeed, we can construct an algorithm computing, for every positive integer n, the nth digit of Υ_U. The idea is simple: only the terms $2^{-i}/time_U(string_i)$ for which $time_U(string_i) = \infty$ do produce perturbations in (3) because at every finite step of the computation they appear to be nonzero when, in fact, they are zero! The solution is to run all nonstopping programs $string_i$ enough time such that their cumulative contribution is too small to affect the nth digit of Υ_U.

The following results from Calude and Hertlinger [16] summarize some basic facts about computable, converging sequences of rationals, which may converge computably or noncomputably.

Proposition 4 *Let $h : \mathbf{N} \to \mathbf{N}$ be an injective, total computable function and define the sequence (a_n) of rationals by $a_n = \sum_{m=0}^{n} 2^{-h(m)}$. The sequence $(2^{-h(n)})$ is a computable sequence of rationals which converges always to zero, and the sequence (a_n) is an increasing, computable, converging sequence of rationals.*

Proposition 5 *Let $h : \mathbf{N} \to \mathbf{N}$ be an injective, total computable function and $a_n = \sum_{m=0}^{n} 2^{-h(m)}$. Then, the following conditions are equivalent:*

(a) *The range $h(\mathbf{N})$ of h is a computable set.*

(b) *The sequence $(2^{-h(n)})$ converges computably.*

(c) *The sequence (a_n) converges computably.*

[2] It is an open question whether there is any "natural phenomenon" leading to an uncomputable real number.

[3] Such numbers play an important role, for example in the construction of a continuous but uncomputable solution for the wave equation even if the initial conditions are continuous and computable, see Pour-El and Richards [43].

[4] Note that $time_U(string_i)$ is a positive integer in case $string_i \in PROG_U$, and $time_U(string_i) = \infty$, in the opposite case.

(d) *The limit of the sequence* (a_n) *is a computable real.*

We say that a sequence (a_i) of reals with limit α converges *monotonically* if there exists a constant $c > 0$ such that for all i and all $j \geq i$, $c \cdot |\alpha - a_i| \geq |\alpha - a_j|$.

For example, any converging and monotonic, i.e. either nondecreasing (e.g. $a_n = \sum_{m=0}^{n} 2^{-h(m)}$) or nonincreasing sequence of reals converges monotonically: one can take the constant $c = 1$.

Proposition 6 *Every computable sequence of rationals which converges monotonically to a computable real converges computably.*

Remark The converse of Proposition 6 is not true as the following example shows. The sequence (a_i) defined by $a_i = 2^{-i}$ if i is even and $a_i = 2^{-2i}$ if i is odd converges computably to zero, but it does not converge monotonically.

Lemma 7 *Let* (a_n) *be a computable sequence of rationals which converges computably, and let* (b_n) *be a computable sequence of rationals which converges noncomputably. Then* $(a_n + b_n)$ *is a computable sequence of rationals which converges noncomputably to the sum of the limits of* (a_n) *and* (b_n)*.*

Theorem 8 *For every computable real* α *there is a computable sequence* (a_n) *of rationals which converges to* α*, but which does not converge computably.*

Theorem 8 states that we can approximate every computable real noncomputably, that is, very slowly. Thus, *the fact, that a computable sequence of rationals converges noncomputably, does not imply that the limit is uncomputable.* Furthermore we ask whether, given a computable sequence of rationals, one can decide whether its limit is computable or not, and also, whether it converges computably or not. The answer to both these questions is *negative*.

We will use the following notation: a number i is called a *Gödel number* of a computable sequence of rationals (a_n) if $a_n = \nu_{\mathbf{Q}}(\varphi_i(n))$, for all n, where φ is a total standard numbering of the partial computable number functions and $\nu_{\mathbf{Q}}$ is a standard bijection between $\mathbf{N}$ and $\mathbf{Q}$ (see, for example, Weihrauch [56]). We say that it is impossible to decide whether the elements in a certain set A of computable sequences of rationals have a certain property, if there is no algorithm which, given a Gödel number of an element of the set A, decides whether this element has the property or not.

Theorem 9 *It is impossible to decide whether:*

- *a converging, increasing, computable sequence of rationals converges computably,*
- *a converging, increasing, computable sequence of rationals converges to a computable real or to an uncomputable real,*
- *a computable sequence of rationals which converges noncomputably converges to a computable real or to an uncomputable real.*

Theorem 8 and Theorem 9 tell us that a computable sequence of rationals which converges noncomputably may converge to a computable or an uncomputable real, and that it is impossible to decide whether the limit is computable or uncomputable. Is there still a difference between the rate of convergence of a computable sequence of rationals with computable limit and the rate of convergence of a computable sequence of rationals with uncomputable limit? We shall see later that this is indeed the case.

3 Random Reals

In this section we will introduce and study random reals in the unit interval. Reals will be written in binary, so we start by looking at random binary sequences.

> *I am convinced that the vast majority of my readers, and in fact the vast majority of scientists and even nonscientists, are convinced that they know what 'random' is. A toss of a coin is random; so is a mutation, and so is the emission of an alpha particle.... Simple, isn't it?* said Kac in [34].

Well, no! Kac knew very well that randomness could be called many things, but not simple, and in fact his essay shows that randomness is complicated, and it can be described in more than one way, even by mathematicians and scientists. According to B. Efron (cited in Kolata [36])

> *There have been heroic efforts to understand randomness. Randomness is not an easy concept to define.*

Books on probability theory do not even attempt to define it.

> *It's like the concept of a point in geometry books.*

Beltrami [2] remarked:

> *The subject of probability begins by assuming that some mechanism of uncertainty is at work giving rise to what is called randomness, but it is not necessary to distinguish between chance that occurs because of some hidden order that may exist and chance that is the result of blind lawlessness. This mechanism, figuratively speaking, churns out a succession of events, each individually unpredictable, or it conspires to produce an unforeseeable outcome each time a large ensemble of possibilities is sampled.*

In an extreme sense there is no such notion as "true randomness". Indeed, any sequence has some kind of regularity; for example, van der Waerden discovered a "universal" nontrivial property shared by all sequences:

Theorem 10 *In every binary sequence at least one of the two symbols must occur in arithmetical progressions of every length.*

The proof of van der Waerden's result (and of similar ones) is *nonconstructive*. To be more precise, there is no algorithm which will tell in a finite amount of time which alternative is true: 0 occurs in arithmetical progressions of every length or 1 occurs in arithmetical progressions of every length.

A possible approach to define random sequences is to isolate the set of all sequences having "all verifiable" properties that from the point of view of classical probability theory are satisfied with "probability one" with respect to μ.

A property P of sequences $\mathbf{x} \in \Sigma^\omega$ is *true almost everywhere in the sense of* μ in case the set of sequences not having the property P is a null set. The main example of such a property, *The Law of Large Numbers*, was discovered by Borel. For every sequence $\mathbf{x} = x_1x_2 \dots x_m \dots \in \{0,1\}^\omega$ and natural number $n \geq 1$ put $S_n(\mathbf{x}) = x_1 + x_2 + \cdots + x_n$. *Then, the limit of* S_n/n, *when* $n \to \infty$, *exists almost everywhere in the sense of* μ *and has the value* $1/2$. It is clear that a sequence satisfying a property false almost everywhere with respect to μ is very "particular". Accordingly, it is tempting to try to say that a sequence $\mathbf{x}$ is *"random"* iff it satisfies every property true almost everywhere with respect to μ. Unfortunately, we may define for every sequence $\mathbf{x}$ the property $P_\mathbf{x}$ as following: $\mathbf{y}$ *satisfies* $P_\mathbf{x}$ *iff for every* $n \geq 1$ *there exists a natural* $m \geq n$ *such that* $x_m \neq y_m$. Every $P_\mathbf{x}$ is an asymptotic property which is true almost everywhere with respect to μ and $\mathbf{x}$ does not have property $P_\mathbf{x}$. Accordingly, *no sequence can verify all properties true almost everywhere with respect to* μ. The above definition is vacuous!

However, there is a way to overcome the above difficulty: We consider not *all* asymptotic properties true almost everywhere with respect to μ, but only a *sequence* of such properties. So, the important question becomes:

What sequences of properties should be considered?

Clearly, the "larger" the chosen sequence of properties is, the "more random" will be the sequences satisfying that sequence of properties. We would like to define a notion of randomness such that at least the following properties are satisfied: *typicality*, that is, regular outcome of a random event is unlikely, and *chaoticity*, i.e. no simple law should be capable to produce a random event.

Martin-Löf [38, 37] defined random sequences by means of statistical tests. A *Martin-Löf test* is a c.e. set $A \subset \Sigma^*$ such that $\mu(A_i\Sigma^\omega) \leq 2^{-i}$, for all natural i. The set $\bigcap_{i\geq 0}(A_i\Sigma^\omega)$ is the set of all sequences which do not pass the randomness test A. With this apparatus we can say that a sequence $\mathbf{x}$ is *Martin-Löf random* if for every Martin-Löf test A, $\mathbf{x} \notin \bigcap_{\mathbf{i}\geq \mathbf{0}}(\mathbf{A_i\Sigma^\omega})$.

Martin-Löf [38] proved the existence of a *universal Martin-Löf test,* a test W with the property that for every Martin-Löf test A there is a constant c such that $A_n \subseteq W_{n+c}$, for all n. So, Martin-Löf 's definition can be rephrased as: *A sequence* $\mathbf{x}$ *is Martin-Löf random iff* $\mathbf{x}$ *passes a universal Martin-Löf test.* This result captures "typicality": for each Martin-Löf test A, the set $\bigcap_{i\geq 0}(A_i\Sigma^\omega)$ is constructively null, so

Theorem 11 *Constructively, with probability one (in the sense of* μ*), every sequence is Martin-Löf-random.*

Hence, from the probabilistic point of view, the set of random sequences is *large*. However, from a topological point of view[5] the situation is completely different (cf. Calude and Chiţescu [12]) as Martin-Löf random sequences form a small set:

Theorem 12 *The set of Martin-Löf random sequences is constructively a first Baire category set.*

Solovay [49] proposed another measure-theoretic definition of random sequences aiming to capture typicality: a sequence $\mathbf{x}$ is *Solovay random* if for every c.e. set $A \subset \Sigma^*$ such that $\sum_{i\geq 1}\mu(A_i\Sigma^\omega) < \infty$, there exists a natural N such that for all $i > N$, $\mathbf{x} \notin A_i\Sigma^\omega$.

"Chaoticity" appears in the following two complexity-theoretic definitions (see Chaitin [21]): an infinite sequence $\mathbf{x}$ is *Chaitin–Schnorr random* if there is a constant c such that $H(\mathbf{x}(\mathbf{n})) > \mathbf{n} - \mathbf{c}$, for every integer $n > 0$, and, apparently the stronger definition, an infinite sequence $\mathbf{x}$ is *Chaitin random* if $\lim_{n\to\infty} H(\mathbf{x}(\mathbf{n})) - \mathbf{n} = \infty$.

Finally, we present Hertling and Weihrauch topological approach to define randomness [32]. A *randomness space* is a triple (X, B, μ), where X is a topological space, $B : \mathbf{N} \to \mathbf{2^X}$ is a total numbering of a subbase of the topology of X, and μ is a measure defined on the σ-algebra generated by the topology of X.[6] Let (W_n) be a sequence of open subsets of X; a sequence (V_n) of open subsets of X is called *W–computable* if there is a c.e. set $A \subseteq \mathbf{N}$ such that $V_n = \bigcup_{\pi(n,i)\in A} W_i$ for all $n \in \mathbf{N}$.[7] Next we define $W'_i = W'(i) = \bigcap_{j\in D_{(1+i)}} W_j$, for all $i \in \mathbf{N}$, where $D : \mathbf{N} \to \{\mathbf{E} \mid \mathbf{E} \subseteq \mathbf{N} \text{ is finite}\}$ is the computable bijection defined by $D^{-1}(E) = \sum_{i\in E} 2^i$. Note that if B is a numbering of a subbase of a topology, then B' is a numbering of a base of the same topology. A *randomness test on* X is a B'–computable sequence (W_n) of open sets with $\mu(W_n) \leq 2^{-n}$, for all $n \in \mathbf{N}$. We say that an element $x \in X$ is called *Hertling–Weihrauch random* if $x \notin \bigcap_{n\in\mathbf{N}} W_n$, for every randomness test (W_n) on X.

Consider now the canonical topology on Σ^ω and the numbering B of a subbase (in fact a base) of the topology is given by $B_i = \{string_i\}\Sigma^\omega$. The general definition applies, so we get: *A sequence is Hertling–Weihrauch random if it is random in the space* (Σ^ω, B, μ).

All the above approaches lead to the same class of sequences:

[5] As mentioned before, Σ comes equipped with the discrete topology and Σ^ω is endowed with the product topology.

[6] Recall that a subbase of a topology is a set β of open sets such that the sets $\bigcap_{W\in E} W$, for finite, nonempty sets $E \subseteq \beta$ form a basis of the topology.

[7] The function $\pi(n, i)$ is a computable bijection, for example, $\pi(n, i) = (n + i)(n + i + 1)/2 + i$.

Theorem 13 *Let* $\mathbf{x} \in \mathbf{\Sigma}^\omega$. *The following statements are equivalent:*

1. *The sequence* $\mathbf{x}$ *is Martin-Löf random.*
2. *The sequence* $\mathbf{x}$ *is Chaitin random.*
3. *The sequence* $\mathbf{x}$ *is Chaitin–Schnorr random.*
4. *The sequence* $\mathbf{x}$ *is Solovay random.*
5. *The sequence* $\mathbf{x}$ *is Hertling–Weihrauch random.*

In what follows we will simply call "random" a sequence satisfying one of the above equivalent conditions. Theorem 13 motivates the following "randomness hypothesis" formulated in Calude [8]:

> *A sequence is "algorithmically random" if it satisfies one of the equivalent conditions in Theorem 13.*

Various arguments supporting this hypothesis, e.g. *random sequences are Borel absolutely normal*,[8] have been analyzed in the literature, e.g. Calude [7]. Here is recent argument due to Fouché [30]: *if* $X \subseteq \Sigma^\omega$ *is a measure one* Σ^0_1 *set, then it contains at least one random sequence.* In particular, if X is Π^0_1 set which contains some random sequence, then it has nonzero measure. So, if a Π^0_1 event is reflected in some random sequence, then the event must be probabilistically significant.

We are now in the position to define random reals in the unit interval: *A real* α *is random if its binary expansion* $\mathbf{x}$ *(i.e.* $\alpha = 0.\mathbf{x}$*) is random.* The choice of the binary base does not play any role, cf. Calude and Jürgensen [18], Hertling and Weihrauch [32], Staiger [52]: *randomness is a property of reals not of names of reals.*

Let us make a short digression concerning the above result. Note first that normality is not base invariant; even the weaker property of disjunctivity (a sequence is disjunctive in case any string appears in the sequence) is not base invariant (cf. Hertling [31]). Following von Mises [55] consider an arbitrary sequence $\mathbf{x} = x_1x_2 \dots x_n \dots$ over the alphabet $\Sigma = \{0, 1\}$ and define a new sequence $\mathbf{y} = y_1y_2 \dots y_n \dots$, over the alphabet $\Gamma = \{0, 1, 2\}$, by

$$y_1 = x_1, y_n = x_{n-1} + x_n, n \geq 2.$$

Then, $\mathbf{y}$ *is not random*, even if $\mathbf{x}$ is a random sequence. The motivation is simple: the strings 02 and 20 never appear in $\mathbf{y}$. (Actually, there are many other strings which do not appear in $\mathbf{y}$.)

A seemingly minor change in the above example makes a major change. For $\mathbf{x} = x_1x_2 \cdots$ with $x_1, x_2, \dots \in \{0, 1\}$ define $\mathbf{y} = y_1y_2 \cdots$ with $y_1, y_2, \dots \in \{0, 1\}$ by

$$y_i = \begin{cases} x_1, & \text{if } i = 1, \\ x_{i-1} \oplus x_i, & \text{if } i > 1. \end{cases}$$

It is not difficult to prove that $\mathbf{y}$ is random provided $\mathbf{x}$ is random.

It is immediate that no random real is computable.[9] Theorem 10 shows that every (random) sequence has some kind of regularity. Is this phenomenon symmetric, i.e. *is there any trace of computability in random reals?*

[8] Every string appears in a random sequence with the probability 2^{-n}, where n is the length of the string.

[9] Bailey and Crandall [1] discussed a hypothesis which implies the normality of many natural real numbers, e.g. π, e. A different approach was discussed in Pincus and Singer [42] and Pincus and Kalman [41]; see also Casti [20] and Beltrami [2].

4 C.E. Reals

Following Soare [47], a real α is called *c.e.* if there is a computable, increasing sequence of rationals which converges (*not necessarily computably*) to α. We will start with several characterizations of c.e. reals (cf. Calude, Hertling, Khoussainov, Wang [17]).

Recall that if $A \subseteq \Sigma^*$ is prefix-free, then, due to Kraft's inequality, the real number $\Omega_A = \sum_{x \in A} 2^{-|x|}$ lies in the interval $[0, 1]$. For a set $X \subseteq \mathbf{N}$ we define the number

$$2^{-X-1} = \sum_{n \in X} 2^{-n-1}.$$

This number also lies in the interval $[0, 1]$. If we disregard all finite sets X, which lead to rational numbers 2^{-X-1}, we get a bijection $X \mapsto 2^{-X-1}$ between the class of infinite subsets of $\mathbf{N}$ and the real numbers in the interval $(0, 1]$. If $0.\mathbf{y}$ is the binary expansion of a real α with infinitely many ones, then $\alpha = 2^{-X_\alpha - 1}$ where $X_\alpha = \{i \mid y_i = 1\}$. Clearly, if X_α is c.e., then the number $2^{-X_\alpha - 1}$ is c.e., but the converse is not true as the Chaitin Ω numbers show.[10] We characterize c.e. reals α in terms of prefix-free c.e. sets of strings and in terms of the sets X_α.

Theorem 14 *Let α be a real in $(0, 1]$. The following conditions are equivalent:*

1. *The number α is c.e.*
2. *There is a computable, nondecreasing sequence of rationals (a_n) which converges to α.*
3. *The set $\{p \in \mathbf{Q} \mid p < \alpha\}$ of rationals less than α is c.e.*
4. *There is an infinite prefix-free c.e. set $A \subseteq \Sigma^*$ with $\alpha = \Omega_A$.*
5. *There is an infinite prefix-free computable set $A \subseteq \Sigma^*$ with $\alpha = \Omega_A$.*
6. *There is a total computable function $f : \mathbf{N}^2 \to \{0, 1\}$ such that*
   (a) *If for some k, n we have $f(k, n) = 1$ and $f(k, n+1) = 0$ then there is an $l < k$ with $f(l, n) = 0$ and $f(l, n + 1) = 1$.*
   (b) *We have: $k \in X_\alpha \iff \lim_{n \to \infty} f(k, n) = 1$.*

Note the importance of the type of representation used to define c.e. reals, especially compare conditions 3. in Theorem 3 and Theorem 14, and conditions 4. and 5. in Theorem 14. Note also that according to condition 6. in Theorem 14, in the process of approximation of α the nth bit may oscillate from 0 to 1 and 1 to 0 but no more than 2^n times. In this respect, Downey and LaForte [28] proved the following interesting result:

Theorem 15 *There exists an uncomputable c.e. real α such that every prefix-free set A such that $\alpha = \Omega_A$ is computable.*

5 C.E. and Random Reals

We are now ready to answer in the affirmative, following Chaitin [21], the question posed at the end of Section 3.

Theorem 16 *If U is universal machine, then Ω_U is random.*

If C is a machine, then Ω_C represents its halting probability. When $C = U$, a universal machine, then its halting probability Ω_U is called a *Chaitin Ω real*, shortly, *Ω real*.

[10] See Theorem 16.

6 Approximating C.E. Reals

In order to compare the information contents of c.e. reals, Solovay [49] has introduced the domination relation. The real α is said to *dominate* the real β if there are a partial computable function $f : \mathbf{Q} \stackrel{o}{\to} \mathbf{Q}$ and a constant $c > 0$ with the property that if p is a rational number less than α, then $f(p)$ is (defined and) less than β, and it satisfies the inequality

$$c(\alpha - p) \geq \beta - f(p)\,.$$

In this case we write $\alpha \geq_{dom} \beta$ or $\beta \leq_{dom} \alpha$.

Roughly speaking, a real α dominates a real β if from any good approximation to α from below (say, from a rational number $p < \alpha$ with $\alpha - p < 2^{-n}$) one can effectively obtain a good approximation to β from below (a rational number $f(p) < \beta$ with $\beta - f(p) < 2^{-n+\text{constant}}$). For c.e. reals this can also be expressed as follows.

Lemma 17 *A c.e. real α dominates a c.e. real β iff there are computable, increasing (or nondecreasing) sequences (a_i) and (b_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.*

Lemma 18 *Let α, β and γ be c.e. reals. Then the following conditions hold:*

1. *The relation $\geq_{dom}$ is reflexive and transitive.*
2. *For every α, β one has $\alpha + \beta \geq_{dom} \alpha$.*
3. *If $\gamma \geq_{dom} \alpha$ and $\gamma \geq_{dom} \beta$, then $\gamma \geq_{dom} \alpha + \beta$.*
4. *For every nonnegative α and positive β one has $\alpha \cdot \beta \geq_{dom} \alpha$.*
5. *If α and β are nonnegative, and $\gamma \geq_{dom} \alpha$ and $\gamma \geq_{dom} \beta$, then $\gamma \geq_{dom} \alpha \cdot \beta$.*

Remark Every random real α can be written as

$$\alpha = \alpha' + \alpha'', \tag{4}$$

where α', α'' are nonrandom. Furthermore, $\alpha' \cdot \alpha''$ is random.

Open Question: Can we take $\alpha, \alpha', \alpha''$ c.e.?

The following result states that no computable sequence (a_i) of rationals which converges to a computable real can dominate a computable sequence of rationals converging to an uncomputable real. Hence, although we can have slow computable approximation of computable reals, we cannot slow it down arbitrarily.

Theorem 19 *Let (a_n) be a computable sequence of rationals converging to a computable real α, and let (b_n) be a computable sequence of rationals converging to an uncomputable real β. Then, for every $c > 0$ there are infinitely many i such that*

$$|\beta - b_i| > c \cdot |\alpha - a_i|\,.$$

Lemma 20 *For every $c \in \mathbf{N}$ there is a positive integer N_c such that for every $n \in \mathbf{N}$ and all strings $x, y \in \Sigma^n$ with $|0.x - 0.y| \leq c \cdot 2^{-n}$ we have*

$$|H(y) - H(x)| \leq N_c.$$

Up to now we have considered arbitrary converging and computable sequences (a_i) and (b_i) and have explicitly formulated two gaps with respect to the convergence rates, one from computable to uncomputable reals, and one from nonrandom to random reals. Both results were based on the inequality $|\beta - b_i| > c \cdot |\alpha - a_i|$ holding for infinitely many i. While we had some doubts whether in this case one can really claim that (b_i) converges slower than (a_i), we shall see now that these doubts can be cast

aside if we compare only monotonically converging sequences with computable limit and monotonically converging sequences with random limit: then we can replace the quantifier "for infinitely many i" by the quantifier "for almost all i". Certainly in this case it is justified to say that (b_i) converges slower than (a_i).

Lemma 21 *Let (b_i) be a computable sequence of rationals which converges to a random real β. Then for every $d > 0$ and almost all i we have*

$$|\beta - b_i| > 2^{d-i}\,.$$

The next result was proved in Calude and Hertling [16].

Scholium 22 *Let (a_i) be a computable sequence of rationals which converges computably to a computable real α, and let (b_i) be a computable sequence of rationals which converges monotonically to a random real β. Then for every $c > 0$ there exists a $d > 0$ such that for all $i \geq d$*

$$|\beta - b_i| > c \cdot |\alpha - a_i|\,. \tag{5}$$

Corollary 23 *Let (a_i) be a computable sequence of rationals which converges monotonically to a computable real α, and let (b_i) be a computable sequence of rationals which converges monotonically to a random real β. Then for every $c > 0$ there exists a $d > 0$ such that for all $i \geq d$*

$$|\beta - b_i| > c \cdot |\alpha - a_i|\,. \tag{6}$$

We conclude this section with a result by Solovay [49] on the relationship between the domination relation and the program-size complexity.

Theorem 24 *Let $\mathbf{x}, \mathbf{y} \in \Sigma^\omega$ be two infinite binary sequences such that both $0.\mathbf{x}$ and $0.\mathbf{y}$ are c.e. reals and $0.\mathbf{x} \geq_{dom} 0.\mathbf{y}$. Then*

$$H(\mathbf{y}(n)) \leq H(\mathbf{x}(n)) + O(1).$$

The converse implication in Theorem 24 is false (see Solovay [49], Calude and Coles [13]). A stronger version was proved in Calude and Coles [14]:

Theorem 25 *There is an uncomputable c.e. real $0.\mathbf{x}$ such that $H(\mathbf{x}_n) \leq H(string_n) + O(1)$.*

7 A Characterization of C.E. Random Reals

This section is devoted to a first characterization of c.e. random reals.

7.1 More About Domination

We consider now 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 Calude, Hertling, Khoussainov, Wang [17], we say that the set A *strongly simulates* the set B (write $B \leq_{ss} A$) if there is a partial computable function $f : \Sigma^* \xrightarrow{o} \Sigma^*$ which satisfies the following three 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 26 *If A, B are infinite prefix-free c.e. sets and $B \leq_{ss} A$, then $\Omega_B \leq_{dom} \Omega_A$.*

The following partial converse of Lemma 26 ([17]) is very important.[11]

[11] In [17] 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 $B \not\leq_{ss} A$.

Theorem 27 *Let α be a c.e. real, and B be an infinite prefix-free c.e. set. If $\Omega_B \leq_{dom} \alpha$, then there is an infinite prefix-free c.e. set $A \subset \Sigma^*$ such that $\alpha = \Omega_A$ and $B \leq_{ss} A$.*

Remark Recently Downey, Hirschfeldt and Nies [29] have obtained the following algebraic characterization of domination:

$\alpha \leq_{dom} \beta$ iff there exist an integer $c > 0$ and a c.e. real γ such that $\beta = \gamma + \frac{\alpha}{c}$.

7.2 Ω Reals Are Ω-Like

Following Solovay [49] we say that a computable increasing, and converging sequence (a_i) of rationals is *universal* if for every computable, increasing and converging sequence (b_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 Calude, Hertling, Khoussainov, Wang [17] one proves the following:

Theorem 28 *Let U be a universal machine. Every computable, increasing sequence of rationals converging to Ω_U is universal.*

7.3 Ω-like Reals Are Ω Reals

First we note that

Lemma 29 *Any Ω-like real dominates every c.e. real.*

The next theorem was proved in Calude, Hertling, Khoussainov, Wang [17].

Theorem 30 *Every Ω-like real α is an Ω real, i.e. there exists a universal machine U such that $\alpha = \Omega_U$.*

In view of Lemma 29 and Theorem 30 we get:[12]

Theorem 31 *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.*

7.4 Every C.E. Random Real Is Ω-like

Theorem 13 can be rephrased directly for reals as follows: *A real α is random iff 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) of the space Σ^ω such that $\mu(A_n) \leq 2^{-n}$. The following two important results were proved by Slaman [45, 46].

Lemma 32 *Let $(a_n), (b_n)$ 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.*

Theorem 33 *Every c.e. random real is Ω-like.*

[12] The equivalence of the statements 1 and 3 comes from Chaitin [22].

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

Theorem 34 *Let $\alpha \in (0,1)$. The following conditions are equivalent:*

1. *The real α is c.e. and random.*
2. *For some universal machine U, $\alpha = \Omega_U$.*
3. *The real α is Ω–like.*
4. *Every computable, increasing sequence of rationals with limit α is universal.*

In [46] Slaman proved the following result answering an open problem in [17]:

Theorem 35 *The measure of any section A_n of a universal Martin-Löf test A, $\mu(A_n\Sigma^\omega)$, is Ω–like, hence c.e. and random.*

8 Properties of C.E. Random Reals

C.e. random reals are dense in the unit interval. They have many other interesting properties.

Proposition 36 *The sum of a random c.e. real and a c.e. real is a random c.e. real. The product of a positive random r.e real with a positive c.e. real is a random c.e. real.*

Corollary 37 *The class of random c.e. reals is closed under addition. The class of positive random c.e. reals is closed under multiplication.*

The last Corollary contrasts with the fact that addition and multiplication do not preserve randomness. For example, if α is a random number, then $1-\alpha$ is random as well, but $\alpha + (1-\alpha) = 1$ is not random.

For two reals α and β, $\alpha =_{dom} \beta$ denotes the conjunction $\alpha \geq_{dom} \beta$ and $\beta \geq_{dom} \alpha$. For a real α, let $[\alpha] = \{\beta \in \mathbf{R} \mid \alpha =_{dom} \beta\}$; $\mathbf{R}_{r.e.} = \{[\alpha] \mid \alpha \text{ is an c.e. real}\}$.

Theorem 38 *The structure $\langle \mathbf{R}_{r.e.}; \leq_{dom} \rangle$ is an upper semilattice. It has a least element which is the $=_{dom}$-equivalence class containing exactly all computable real numbers.*

Theorem 34 proves that $\langle \mathbf{R}_{r.e.}; \leq_{dom} \rangle$ also has a greatest element, which is the equivalence class containing exactly all Chaitin Ω numbers.

Theorem 39 *Given the first n bits of Ω_U one can decide whether $U(x)$ halts or not on an arbitrary program x of length at most n.*

Remark The first 10,000 bits of Ω_U include a tremendous amount of mathematical knowledge. In Bennett's words [3]:

> *[Ω] embodies an enormous amount of wisdom in a very small space ... inasmuch as its first few thousands digits, which could be written on a small piece of paper, contain the answers to more mathematical questions than could be written down in the entire universe.*
>
> *Throughout history mystics and philosophers have sought a compact key to universal wisdom, a finite formula or text which, when known and understood, would provide the answer to every question. The use of the Bible, the Koran and the I Ching for divination and the tradition of the secret books of Hermes Trismegistus, and the medieval Jewish Cabala exemplify this belief or hope. Such sources of universal wisdom are traditionally protected from casual use by being hard to find, hard to understand when found, and dangerous to use, tending to answer more questions and deeper ones than the searcher wishes to ask. The esoteric book is, like God, simple yet undescribable. It is omniscient, and transforms all who know it ... Omega is in many senses a cabalistic number. It can be known of, but not known, through human reason. To know it in detail, one would have to accept its uncomputable digit sequence on faith, like words of a sacred text.*

It is worth noting that even if we get, by some kind of miracle, the first 10,000 digits of Ω_U, the task of solving the problems whose answers are embodied in these bits is computable but unrealistically difficult: the time it takes to find all halting programs of length less than n from $0.\Omega_0\Omega_2\ldots\Omega_{n-1}$ grows faster than any computable function of n.

We finish this section with a proof showing that c.e. random reals are wtt-complete, but not tt-complete (cf. Calude and Nies [19]). We need some more notation. For a set $A \subset \Sigma^*$ we denote by χ_A the characteristic function of A. Denote by W_x the domain of φ_x, where (φ_x) is a Gödel numbering of all partial computable string functions. We say that A is *Turing reducible* to B, and we write $A \leq_T B$, if there is an oracle Turing machine φ_w^B such that $\varphi_w^B(x) = \chi_A(x)$. We say that A is *weak truth-table reducible* to B, and we write $A \leq_{wtt} B$, if $A \leq_T B$ via a Turing reduction which on input x only queries strings of length less than $g(x)$, where $g : \Sigma^* \to \mathbf{N}$ is a fixed computable function. We say that A is *truth-table reducible* to B, and we write $A \leq_{tt} B$, if there is a computable sequence of Boolean functions $\{F_x\}_{x\in\Sigma^*}$, $F_x : \Sigma^{r_x+1} \to \Sigma$, such that for all x, we have $\chi_A(x) = F_x(\chi_B(0)\chi_B(1)\cdots\chi_B(r_x))$.[13] Let $K = \{x \in \Sigma^* \mid \varphi_x(x) < \infty\}$; a c.e. set A is *tt(wtt)-complete* if $K \leq_{tt} A$ ($K \leq_{wtt} A$). See Soare [48] or Odifreddi [40] for more details.

Theorem 40 *The set $\mathcal{H} = \{(x, n) \mid x \in \Sigma^*, n \in \mathbf{N},\ H(x) \leq n\}$ is wtt-complete.*

Theorem 41 *The set $\mathcal{H}$ is wtt-reducible to Ω_U.*

The following result belongs to Juedes, Lathrop, and Lutz [33] (we follow the direct proof in Calude and Nies [19]).

Theorem 42 *If $K \leq_{tt} \mathbf{x}$, then $\mathbf{x}$ is not random.*

9 Solovay Machines and Incompleteness

According to Theorem 34, c.e. random reals can be coded by universal machines through their halting probabilities. How "good" or "bad" are these names? In [21] (see also [22, 26]), Chaitin proved the following:

Theorem 43 *Assume that ZFC[14] is arithmetically sound.*[15] *Then, for every universal machine U, ZFC can determine the value of only finitely many bits of Ω_U.*

In fact one can give a bound on the number of bits of Ω_U which ZFC can determine; this bound can be explicitly formulated, but it *is not effective*, in the sense that it's not computable. For example, in [26] Chaitin described, in a dialect of Lisp, a universal machine U and a theory T, and proved that U can determine the value of at most $H(T) + 15,328$ bits of Ω_U; $H(T)$ is the program-size complexity of the theory T, an *uncomputable* number.

Fix a universal machine U and consider all statements of the form

$$\text{"The } n^{th} \text{ binary digit of the expansion of } \Omega_U \text{ is } k\text{"}, \tag{7}$$

for all $n \geq 0, k = 0, 1$. How many theorems of the form (7) can ZFC prove? More precisely, is there a bound on the set of non-negative integers n such that ZFC proves a theorem of the form (7)? From Theorem 43 we deduce that ZFC can prove only finitely many (true) statements of the form (7). This is Chaitin strongest information-theoretic version of Gödel's incompleteness (see [26, 27]):

Theorem 44 *If ZFC is arithmetically sound and U is a universal machine, then almost all true statements of the form (7) are unprovable in ZFC.*

[13] Note that in contrast with tt-reductions, a wtt-reduction may diverge.
[14] Zermelo set theory with choice.
[15] That is, any theorem of arithmetic proved by ZFC is *true*.

Again, a bound can be explicitly found, but not effectively computed.

Of course, for every c.e. random real α we can construct a universal machine U such that $\alpha = \Omega_U$ and ZFC is able to determine finitely (but as many as we want) bits of Ω_U. By tuning the construction of the universal machine, Solovay [50] went into the opposite direction and obtained a dramatic improvement of Theorem 43:

Theorem 45 *We can effectively construct a universal machine U such that ZFC, if arithmetically sound, cannot determine any single bit of Ω_U.*

Solovay [50] proved a sharper version of Theorem 45 by replacing ZFC with a computably axiomatizable 1-consistent theory. Theorem 43 holds true for any universal machine U (it's easy to see that the finite set of (true) statements of the form (7) which can be proven in ZFC can be arbitrarily large) while Theorem 45 constructs a specific U.

A machine U for which PA[16] can prove its universality and ZFC cannot determine more than the initial block of 1 bits of the binary expansion of its halting probability, Ω_U, will be called *Solovay machine*.[17] In view of Theorem 34 and Theorem 45, we may ask the question: *Which c.e. random reals are halting probabilities of Solovay machines?* Following Calude [10] we prove:

Theorem 46 *Assume that ZFC is arithmetically sound. Then, every c.e. random real is the halting probability of a Solovay machine.*

For example, if $\alpha \in (3/4, 7/8)$ is c.e. and random, then in the worst case ZFC can determine its first two bits (11), but no more.

Corollary 47 *Assume that ZFC is arithmetically sound. Then, every c.e. random real $\alpha \in (0, 1/2)$ is the halting probability of a Solovay machine which cannot determine any single bit of α. No c.e. random real $\alpha \in (1/2, 1)$ has the above property.*

Gödel Incompleteness Theorem is constructive, but the proof of Theorem 44 appears to be non-constructive. Is it possible to get a constructive variant of Theorem 44? The answer is affirmative and here is a possible variant:

Theorem 48 *If ZFC is arithmetically sound and U is a Solovay machine, then the statement "the 0^{th} bit of the binary expansion of Ω_U is 0" is true but unprovable in ZFC.*

In fact, one can effectively construct arbitrarily many examples of true and unprovable statements of the form (7), where U is a Solovay machine.

Consider a partial computable function ψ (depending upon two variables, a non-negative integer and a string) such that:

- for every non-negative integer n, the partial function $\psi_n(s) = \psi(n, s)$ is a machine, and
- for every φ_n with a prefix-free domain we have $\psi_n(s) = \varphi_n(s)$, for all non-negative integers n and all strings s.

Denote by D_n the domain of ψ_n and put $\Omega_n = \Omega_{D_n}$. The time relativized versions of D_n and Ω_n are defined in the usual way. Let $D_n[t]$ be the set of all elements of D_n which have appeared by time t and let $\Omega_n[t] = \Omega_{D_n[t]}$, the approximation of Ω_n computable at time t. The following facts follow directly:

1. Given n and t we can effectively compute the finite set $D_n[t]$ and the rational number $\Omega_n[t]$.
2. The sequence $(\Omega_n[t])$ increases monotonically to Ω_n.

Proposition 49 *Let U be a universal machine, $\Omega_U = 0.\omega_0\omega_1\ldots$, and let $s = s_0s_1\ldots s_m$ be a binary string. Then, we can effectively construct a universal machine W such that $\Omega_W = 0.s_0s_1\ldots s_m\omega_0\omega_1\ldots$.*

[16] PA means Peano Arithmetic.
[17] Of course, U depends on ZFC.

9.1 C.E. Random Reals Are Halting Probabilities of Solovay Machines

We fix an interpretation of Peano Arithmetic (PA) in ZFC. Each sentence of the language of PA has a translation into a sentence of the language of ZFC, determined by the interpretation of PA in ZFC. A "sentence of arithmetic" indicates a sentence of the language of ZFC that is the translation of some sentence of PA. We shall assume that ZFC is *arithmetically sound*, that is, any sentence of arithmetic which is a theorem of ZFC is true (in the standard model of PA).[18]

A *dyadic rational* is a rational number of the form $r/2^s$, where r and s are integers and $s \geq 0$; for example, $\Omega_n[t]$ is a dyadic rational. If x is a real number which is not a dyadic rational, then x has a unique binary expansion. We start numbering the digits of the binary expansion of a real α with the 0^{th} digit: $\alpha = 0.\alpha_0\alpha_1\ldots$

Every statement of the form

$$\text{"The } n^{th} \text{ binary digit of the expansion of } \Omega_l \text{ is } k\text{"}, \tag{8}$$

for all $n, l \geq 0, k = 0, 1$, can easily be formalized in PA. Moreover, if ψ_l is a machine which PA can prove universal and ZFC proves the assertion (8), then this assertion *is true*.

Theorem 50 *Assume ZFC is arithmetically sound. Let $i \geq 0$ and consider the c.e. random real*

$$\alpha = 0.\alpha_0\alpha_1\ldots\alpha_{i-1}\alpha_i\alpha_{i+1}\ldots, \text{ where } \alpha_0 = \alpha_1 = \ldots\alpha_{i-1} = 1, \alpha_i = 0.$$

Then, we can effectively construct a universal machine, U (depending upon ZFC and α), such that the following three conditions are satisfied:

a) PA proves the universality of U.

b) ZFC can determine at most i initial bits of Ω_U.

c) $\alpha = \Omega_U$.

If we set $i = 0$ in Theorem 50, then we get Corollary 47. Indeed, every c.e. random real in the interval $(0, 1/2)$ has its 0^{th} digit 0, so it can be represented as the halting probability of a Solovay machine for which ZFC cannot determine any single bit. However, if α is c.e. and random, but $\alpha > 1/2$, then ZFC can determine the 0^{th} bit of α which is 1.

9.2 Information-Theoretic Incompleteness

Theorem 48 follows directly from Corollary 47. Indeed, start with a universal machine U and effectively construct a Solovay machine U' such that $\Omega_{U'} = \frac{1}{2} \cdot \Omega_U$. Then, $\Omega_{U'}$ is less than $1/2$, so its 0^{th} bit is 0, but ZFC *cannot prove* this fact!

We can now use Chaitin's Theorem [23]

Theorem 51 *Given a universal Chaitin machine U one can effectively construct an exponential Diophantine equation $P(n, x, y_1, y_2, \ldots, y_m) = 0$ such that for every natural fixed k the equation $P(k, x, y_1, y_2, \ldots, y_m) = 0$ has an infinity of solutions iff the kth bit of Ω_U is 1.*

to effectively construct an exponential Diophantine equation which has only finitely many solutions, but this fact cannot be proven in ZFC.

In fact, for every binary string $s = s_1 s_2 \ldots s_n$ use Proposition 49 to effectively construct a Solovay machine U such that the binary expansion of Ω_U has the string $\langle 0\rangle \frown s_1 s_2 \ldots s_n$ as prefix. Consequently, *the following statements*

$$\text{"The } 0^{th} \text{ binary digit of the expansion of } \Omega_U \text{ is } 0\text{"},$$

[18] The metatheory is ZFC itself, that is, "we know" that PA itself is arithmetically sound.

"The 1^{th} binary digit of the expansion of Ω_U is s_1",

"The 2^{th} binary digit of the expansion of Ω_U is s_2",

$\vdots$

"The $(n+1)^{th}$ binary digit of the expansion of Ω_U is s_n",

are true but unprovable in ZFC.

References

[1] D. H. Bailey, R. C. Crandall. On the Random Character of Fundamental Constant expansions, `http://www.perfsci.com`, May 2000.

[2] E. Beltrami. *What is Random? Chance and Order in Mathematics and Life*, Springer-Verlag, New York, 1999.

[3] C. H. Bennett, M. Gardner. The random number omega bids fair to hold the mysteries of the universe, *Scientific American* **241** (1979) 20–34.

[4] D. S. Bridges. A constructive look at the real number line, in P. Ehrlich (ed.). *Synthèse: Real Numbers, Generalizations of the Reals and Theories of Continua*, Kluwer Academic Publishers, Amsterdam, 1994, 29–92.

[5] D. S. Bridges. *Computability—A Mathematical Sketchbook*, Springer Verlag, Berlin, 1994.

[6] C. Calude. *Theories of Computational Complexity*, North-Holland, Amsterdam, 1988.

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

[8] C. S. Calude. A glimpse into algorithmic information theory, in P. Blackburn, N. Braisby, L. Cavedon, A. Shimojima (eds.). *Logic, Language and Computation*, Volume 3, CSLI Series, Cambridge University Press, Cambridge, 2000, 65–81.

[9] C. S. Calude. A characterization of c.e. random reals, *Theoret. Comput. Sci.*, to appear.

[10] C. S. Calude, Chaitin Ω numbers, Solovay machines and incompleteness, *Theoret. Comput. Sci.*, accepted.

[11] C. S. Calude, G. J. Chaitin. Randomness everywhere, *Nature*, 400 22 July (1999), 319–320.

[12] C. Calude, I. Chiţescu. Random sequences: some topological and measure-theoretical properties, *An. Univ. Bucureşti, Mat.-Inf.* 2 (1988), 27–32.

[13] C. S. Calude, R. J. Coles. On a Theorem of Solovay, *CDMTCS Research Report* 094, 1999, 14 pp.

[14] 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, 225–237.

[15] C. Calude and C. Grozea. Kraft-Chaitin inequality revisited, *J. Univ. Comput. Sci.* 5 (1996), 306–310.

[16] C. S. Calude, P. Hertling. Computable approximations of reals: An information-theoretic analysis, *Fundamenta Informaticae* 33 (1998), 1-16.

[17] C. S. Calude, P. Hertling, B. Khoussainov, and Y. Wang. Recursively enumerable reals and Chaitin Ω 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 to appear in *Theoret. Comput. Sci.*

[18] 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.

[19] C. Calude, A. Nies. Chaitin Ω numbers and strong reducibilities, *J. Univ. Comput. Sci.* 3 (1997), 1161–1166.

[20] J. L. Casti. Truly, madly, randomly, *New Scientist* 23 Aug (1997),32–35.

[21] G. J. Chaitin. A theory of program size formally identical to information theory, *J. Assoc. Comput. Mach.* 22 (1975), 329–340. (Reprinted in: [24], 113–128)

[22] G. J. Chaitin. Algorithmic information theory, *IBM J. Res. Develop.* 21 (1977), 350–359, 496. (Reprinted in: [24], 44–58)

[23] G. J. Chaitin. *Algorithmic Information Theory*, Cambridge University Press, Cambridge, 1987. (third printing 1990)

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

[25] G. J. Chaitin. On the number of N-bit strings with maximum complexity, *Applied Mathematics and Computation* 59(1993), 97-100.

[26] G. J. Chaitin. *The Limits of Mathematics*, Springer-Verlag, Singapore, 1997.

[27] G. J. Chaitin. *The Unknowable*, Springer-Verlag, Singapore, 1999.

[28] R. G. Downey, G. L. LaForte. Presentations of Computably Enumerable Reals, *CDMTCS Research Report* 135, 2000, 23pp.

[29] R. G. Downey. Email to C. S. Calude, 6 June 2000.

[30] W. L. Fouché. Descriptive complexity and reflective properties of combinatorial configurations, *J. London. Math. Soc.* 54 (1996), 199-208.

[31] P. Hertling. Disjunctive ω-words and real numbers, *J. UCS* 2 (1996), 549-568.

[32] P. Hertling, K. Weihrauch. Randomness spaces, in K. G. Larsen, S. Skyum, and G. Winskel (eds.). *Automata, Languages and Programming, Proceedings of the 25th International Colloquium, ICALP'98* (Aalborg, Denmark), Springer-Verlag, Berlin, 1998, 796–807.

[33] D. Juedes, J. Lathrop, J. Lutz. Computational depth and reducibility, *Theoret. Comput. Sci.* 132 (1994), 37-70.

[34] M. Kac. What is random? *American Scientist* 71 (1983), 405-406.

[35] Ker-I, Ko. *Complexity of Real Functions*, Birkhauser, Berlin, 1991.

[36] G. Kolata. What does it mean to be random? *Science* 7 (1986), 1068.

[37] P. Martin-Löf. *Algorithms and Random Sequences*, Erlangen University, Nürnberg, Erlangen, 1966.

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

[39] P. Martin-Löf. *Notes on Constructive Mathematics*, Almqvist & Wiksell, Stockholm, 1967.

[40] P. Odifreddi. *Classical Recursion Theory*, North-Holland, Amsterdam, Vol.1, 1989, Vol. 2, 1999.

[41] S. Pincus, R. E. Kalman. Not all (possibly) "random" sequences are created equal, *Proc. Nat. Acad. Sci. USA* 94 (1997), 3513–3518.

[42] S. Pincus, B. H. Singer. Randomness and degrees of irregularity, *Proc. Nat. Acad. Sci. USA* 93 (1996), 2083–2088.

[43] M. B. Pour-El and J. I. Richards. *Computability in Analysis and Physics*. Springer-Verlag, Berlin, 1989.

[44] H. Rice. Recursive reals, *Proc. Amer. Math. Soc.* 5 (1954), 784–791.

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

[46] T. A. Slaman. Randomness and recursive enumerability, *SIAM J. Comput.* (to appear).

[47] R. I. Soare. Recursion theory and Dedekind cuts, *Trans. Amer. Math. Soc.* 140 (1969), 271–294.

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

[49] R. 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.

[50] R. M. Solovay. A version of Ω for which ZFC can not predict a single bit, in C.S. Calude, G. Păun (eds.). *Finite Versus Infinite. Contributions to an Eternal Dilemma*, Springer-Verlag, London, 2000, 323-334.

[51] E. Specker. Nicht konstruktiv beweisbare Sätze der Analysis, *J. Symbolic Logic* 14 (1949), 145–158.

[52] L. Staiger. The Kolmogorov complexity of real numbers, in G. Ciobanu and Gh. Păun (eds.). *Proc. Fundamentals of Computation Theory*, Lecture Notes in Comput. Sci. No. 1684, Springer–Verlag, Berlin, 1999, 536-546.

[53] J. F. Traub, G. W. Wasilkowski, and H. Woźniakowski. *Information-Based Complexity*, Academic press, New York, 1988.

[54] A. M. Turing. On computable numbers with an application to the Entscheidungsproblem, *Proc. Amer. Math. Soc.* 42 (1936-7), 230-265; a correction, ibid., 43 (1937), 544-546.

[55] R. von Mises. *Mathematical Theory of Probability and Statistics*, Edited and Complemented by Hilda Geiringer, Academic Press, New York, 1974.

[56] K. Weihrauch. *Computability*, Springer-Verlag, Berlin, 1987.