ELSEVIER

Theoretical Computer Science 284 (2002) 269–277

Theoretical Computer Science

www.elsevier.com/locate/tcs

Chaitin Ω numbers, Solovay machines, and Gödel incompleteness

Cristian S. Calude

Department of Computer Science, University of Auckland, Private Bag 92019, Auckland, New Zealand

Abstract

Computably enumerable (c.e.) reals can be coded by Chaitin machines through their halting probabilities. Tuning Solovay's construction of a Chaitin universal machine for which *ZFC* (if arithmetically sound) cannot determine any single bit of the binary expansion of its halting probability, we show that every c.e. random real is the halting probability of a universal Chaitin machine for which *ZFC* cannot determine more than its initial block of 1 bits—as soon as you get a 0, it is all over. Finally, a constructive version of Chaitin information-theoretic incompleteness theorem is proven.

Keywords: Computably enumerable real; Chaitin machine; Random real; Information-theoretic incompleteness

1. Introduction

We will consider only reals in the unit interval $(0,1)$. A real α is *computably enumerable* (c.e.) if it is the limit of a computable, increasing, converging sequence of rationals. In contrast with the case of a computable real, whose digits are given by a computable function, during the process of approximation of a c.e. real one may never know how close one is to the final value. See [13] for a recent study on computably enumerable reals. 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, 14, 20]). C.e. random reals have many other interesting properties; for example, they are wtt-complete, but not tt-complete (cf. [6]). For computation theory see [16].

In [7] (see also [8, 11, 12]), Chaitin has introduced the halting probability Ω_U of a "Chaitin universal machine" U–Chaitin's Omega number. He proved:

Theorem 1. *For every Chaitin universal machine U, Ω_U is a c.e. random real.*

E-mail address: cristian@cs.auckland.ac.nz (C.S. Calude).

0304-3975/02/$ - see front matter
PII: S0304-3975(01)00068-8

Are there other c.e. random reals? The answer is negative, and the proof is constructive, cf. [4, 17] (full paper will appear in [15]; see also [3, 2]):

Theorem 2. *The set of c.e. random reals coincides with the set of Chaitin Omega numbers.*

So, computably enumerable (c.e.) reals can be coded by Chaitin universal machines through their halting probabilities. How "good" or "bad" are these names? In [7] (see also [8, 11]), Chaitin proved the following:

Theorem 3. *Assume that ZFC*[1] *is arithmetically sound.*[2] *Then, for every Chaitin universal machine U, ZFC can determine the value of only finitely many bits of Ω_U, and one can give a bound on the number of bits of Ω_U which ZFC can determine.*

The bound cited in Theorem 3 can be explicitly formulated, but it *is not effective*, in the sense that it is not computable. For example, in [11] 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 Chaitin machine U and consider all statements of the form

"The nth binary digit of the expansion of Ω_U is k", (1)

for all $n \geqslant 0$, $k = 0, 1$. How many theorems of the form (1) 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 (1)? From Theorem 3 we deduce that *ZFC* can prove only finitely many (true) statements of the form (1). This is Chaitin strongest information-theoretic version of Gödel's incompleteness (see [11, 12]):

Theorem 4. *If ZFC is arithmetically sound and U is a Chaitin universal machine, then almost all true statements of the form* (1) *are unprovable in ZFC.*

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

Of course, for every c.e. random real α we can construct a Chaitin 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 Chaitin machine, Solovay [19] went into the opposite direction and obtained a dramatic improvement of Theorem 3:

Theorem 5. *We can effectively construct a universal Chaitin machine U such that ZFC, if arithmetically sound, cannot determine any single bit of Ω_U.*

[1] Zermelo set theory with choice.

[2] That is, any theorem of arithmetic proved by *ZFC* is *true*.

Solovay [19] proved a sharper version of Theorem 5 by replacing *ZFC* with a computably axiomatizable 1-consistent theory. Theorem 3 holds true for any universal Chaitin machine U (it is easy to see that the finite set of (true) statements of the form (1) which can be proven in *ZFC* can be arbitrarily large) while Theorem 5 constructs a specific U.

A Chaitin machine U for which PA[3] 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.*[4] In view of Theorems 2 and 5, we may ask the question:

Which c.e. random reals are halting probabilities of Solovay machines? (2)

The main result of this note answers question (2):

Theorem 6. *Assume that ZFC is arithmetically sound. Then, every c.e. random real is the halting probability of a Solovay machine.*

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

Corollary 7. *Assume that ZFC is arithmetically sound. Then, every c.e. random real* $\alpha \in (0, \frac{1}{2})$ *is the halting probability of a Solovay machine which cannot determine any single bit of* α. *No c.e. random real* $\alpha \in (\frac{1}{2}, 1)$ *has the above property.*

Gödel Incompleteness Theorem is constructive, but the proof of Theorem 4 appears to be non-constructive. Is it possible to get a constructive variant of Theorem 4? The answer is affirmative and here is a possible variant:

Theorem 8. *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 (1), where U is a Solovay machine.

The rest of this paper is organised as follows. Section 2 contains a review of the basic definitions of algorithmic information theory that we need. In Section 3, we present the proof of Theorem 6. Section 4 is devoted to incompleteness.

[3] *PA* means Peano Arithmetic.
[4] Of course, U depends on *ZFC*.

2. Basic definitions and notation

Let $\Sigma = \{0,1\}$. By Σ^* we denote the set of binary strings (including the empty string, λ). If s is a binary string, we write $|s|$ for the length of s. 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 $s = t$.

We will work with the usual theory of partial computable string functions (i.e., partial functions whose domains and ranges are subsets of Σ^*); see [1].

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

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

A *Chaitin machine* (*computer*) V computes a partial string function whose domain $\mathrm{dom}(V)$ is a prefix-free set.[5] Set $\Omega_V = \Omega_{\mathrm{dom}(V)}$. A Chaitin machine U is *universal* if it can simulate any other Chaitin machine. More precisely, U is universal if for every Chaitin machine V there is a constant c (depending upon U and V) such that for every $s, t \in \Sigma^*$, if $V(s) = t$, then $U(s') = t$, for some $s' \in \Sigma^*$ of length $|s'| \leqslant |s| + c$.

Universal Chaitin machines can be effectively constructed (see [10, 11, 1]). According to Theorem 1, if U is universal, then Ω_U is random. As a corollary, Ω_U is irrational and does not have a computable binary expansion; however, Ω_U is c.e., that is, computable in the limit from below.

The set of Chaitin machines is c.e. Indeed, let $(\varphi_n)_{n \geqslant 0}$ be a Gödel numbering of all partial computable string functions. Then, there exists 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 Chaitin 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 $(\Omega_n[t])_{t \geqslant 0}$ increases monotonically to Ω_n.

[5] We follow Solovay's terminology [18, 19].

This shows that every real Ω_n is c.e. (in fact, every c.e. real is an Ω_n, for some n, cf. [4]); some Ω_n's may be even computable, but, in view of Theorem 1, if ψ_n is universal, then Ω_n is random, so not computable.

Proposition 9. *Let U be a universal Chaitin 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 Chaitin machine W such that $\Omega_W = 0.s_0s_1\ldots s_m\omega_0\omega_1\ldots$.*

For every universal Chaitin machine U we can effectively construct two universal Chaitin machines V_1 and V_2 such that $\Omega_{V_1} = \frac{1}{2}\Omega_U$ and $\Omega_{V_2} = \frac{1}{2}(1+\Omega_U)$: put $V_1(0x) \simeq U(x)$ and $V_2(0x) \simeq U(x)$, $V_2(1) = 0$, respectively.

3. Solovay's theorem revisited

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*).[6]

A *dyadic rational* is a rational number of the form $r/2^s$, where r and s are integers and $s \geqslant 0$; 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 0th digit: $\alpha = 0.\alpha_0\alpha_1\ldots$.

Every statement of the form

"The nth binary digit of the expansion of Ω_l is k", (3)

for all $n, l \geqslant 0$, $k = 0, 1$, can easily be formalized in *PA*. Moreover, if ψ_l is a Chaitin machine which *PA* can prove universal and *ZFC* proves the assertion (3), then this assertion *is true*.

Theorem 10. *Assume ZFC is arithmetically sound. Let $i \geqslant 0$ and consider the c.e. random real*

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

Then, we can effectively construct a universal Chaitin 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) $\alpha = \Omega_U$.

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

A machine satisfying all conditions in Theorem 10 will be called *Solovay machine*.

We start by fixing a universal Chaitin machine V such that the universality of V is provable in PA and $\Omega_V = \alpha$. Use Theorem 2 and Proposition 9 to effectively construct a universal Chaitin machine $\tilde{V}$ such that

$$\Omega_{\tilde{V}} = 0.\underbrace{00\ldots0}_{i\,0's}\alpha_{i+1}\alpha_{i+2}\ldots,$$

if $i \geqslant 1$, and a universal Chaitin machine $\hat{V}$ such that

$$\Omega_{\hat{V}} = 0.\alpha_1\alpha_2\ldots,$$

in case $i = 0$. Next we construct, by cases, a partial computable function $W(l,s)$ (l is a non-negative integer and $s \in \Sigma^*$) as follows:

Step 1: Set $W(l,\lambda)$ to be undefined.

Step 2: If $i = 0$, then go to Step 6. Otherwise, set

$$W(l,\langle 1\rangle) = W(l,10) = \ldots = W(l,\underbrace{11\ldots1}_{i\,1's}0) = \lambda.$$

Step 3: If $s = 00 \frown t$, for some $t \in \Sigma^*$, then set

$$W(l,s) \simeq \tilde{V}(t),$$[7]

and stop.

Step 4: If $s = 01 \frown t$, for some $t \in \Sigma^*$, then go to Step 5.

Step 5: List all theorems of *ZFC*, in some definite order, not depending on t, and search for a theorem of the form (3). If no such theorem is found, then $W(l,s)$ is undefined, and stop. If such a theorem is found, then let n,l,k be its parameters.

- If $|t| \neq n$, then $W(l,s)$ is undefined, and stop.
- If $|t| = n$, then let r be the unique dyadic rational, in $[0,1)$, whose binary expansion is $t \frown \langle k\rangle$ and set $r' = r + 2^{-(n+1)}$. Search for the least integer m such that $\Omega_l[m] \in (r,r')$. If this search fails, or $s \in D_l[m]$, then $W(l,s)$ is undefined, and stop. In the opposite case set $W(l,s) = \lambda$, and stop.

Step 6: If $s = \langle 0\rangle \frown t$, for some string t, then set

$$W(l,s) \simeq \hat{V}(t),$$

and stop.

Step 7: If $s = \langle 1\rangle \frown t$, for some string t, then go to Step 5.

The Recursion Theorem provides a j such that $\varphi_j(s) \simeq W(j,s)$. We fix such a j and set $U = \varphi_j$. We will show that U is a universal Chaitin machine which satisfies conditions (a)–(c).

[7] As usual $x \simeq y$ holds between two partially defined objects x and y if (a) x is defined iff y is defined and (b) if they are both defined, then they are equal.

First we prove that U is a Chaitin machine. Let $i=0$. Suppose that s_1 and s_2 are in the domain of U and $s_1 \subseteq s_2$. Since U is undefined on the empty string, $|s_1| \geqslant 1$. Let k be the first bit of s_1. Let $s_i = \langle k \rangle \frown t_i$. Clearly $t_1 \subseteq t_2$. If $k=0$, then t_1 and t_2 are in the domain of the Chaitin machine V, hence $t_1 = t_2$ and $s_1 = s_2$. If $k=1$ and $U(s_1)$ and $U(s_2)$ are defined, then the integer n has to be defined in the course of the computation; n *is* the same for both s_1 and s_2 as the enumeration of theorems of *ZFC* does not depend upon t_i. But then $|t_1| = |t_2| = n$, so $|s_1| = |s_2| = n+1$ and $s_1 = s_2$. Now assume that $i \geqslant 1$ and, again, s_1 and s_2 are in the domain of U and $s_1 \subseteq s_2$. Let k be the first bit of s_1. If $k=1$, then according to Step 2, s_1, s_2 belong to the prefix-free set

$$\{1, 10, 110, \ldots, \underbrace{11\ldots1}_{i1's}0\},$$

so $s_1 = s_2$. If $k=0$, then two cases may appear. If $s_i = 00 \frown t_i$, then t_1, t_2 belong to the domain of the Chaitin machine $\tilde{V}$ (see Step 3), so $t_1 = t_2$ and $s_1 = s_2$. If $s_i = 01 \frown t_i$, then in view of Step 5, a similar argument as in case $i=0$ shows that $s_1 = s_2$.

It follows that U is a Chaitin machine, i.e., $U = \psi_j$ and $\Omega_j = \Omega_U$. The universality of U follows from the definition of $W(l,s)$ on Steps 3 and 6 as $\tilde{V}$ and $\hat{V}$ are universal. More, U inherits from $\tilde{V}(\hat{V})$ the fact that its universality is provable in *PA*.

Assume now that $i=0$ and *ZFC* can determine some bit of Ω_U. Then, in the course of the computation the integers n and k are defined. Let r be a dyadic rational with denominator 2^{n+1} such that

$$r < \Omega_U < r + 2^{-(n+1)},$$

(r exists because Ω_U is irrational). Let $r' = r + 2^{-(n+1)}$.

Since *ZFC* is arithmetically sound, the assertion "The nth binary bit of Ω_U is k" is *true*. Hence the first $n+1$ bits of the binary expansion of r have the form $t \frown \langle k \rangle$ where t is a string of length n. For all sufficiently large m, $\Omega_j[m]$ will lie in the interval (r, r').

Let $s = \langle 1 \rangle \frown t$ and consider the computation of $U(s)$. The rationals r and r' involved in that computation are exactly the ones just defined above. The search for an m such that $\Omega_j[m] \in (r, r')$ will succeed and $s \notin D_j[m]$. Reason: if $s \in D_j[m]$, then $U(s)$ is undefined. But $D_j[m] \subseteq D_j$, so $s \in D_j$, the domain of U, a contradiction.

Consequently, $U(s)$ is defined, and D_j contains in addition to the members of $D_j[m]$ the string s of length $n+1$. It follows that $\Omega_U \geqslant r + 2^{-(n+1)} = r'$, which contradicts the definition of r.

With a similar argument as above one can show that the assumption that *ZFC* can determine some bit of Ω_U beyond its first $i \geqslant 1$ bits leads to a contradiction.

The analysis just described above shows that for $i=0$, $U(\langle 1 \rangle \frown t)$ is undefined, and in case $i \geqslant 1$, $U(01 \frown t)$ is undefined, for every string t. To finish the proof we notice that for $i=0$,

$$\Omega_V = \tfrac{1}{2}\Omega_{\hat{V}} = \Omega_U,$$

and for $i \geqslant 1$,

$$\Omega_V = (1 - 2^{-i}) + \tfrac{1}{4}\Omega_{\tilde{V}} = \Omega_U.$$

If we set $i = 0$ in Theorem 10, then we get Corollary 7. Indeed, every c.e. random real in the interval $(0, \frac{1}{2})$ has its 0th 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 $\alpha > \frac{1}{2}$, then *ZFC* can determine the 0th bit of α which is 1.

4. Incompleteness

Theorem 8 follows directly from Corollary 7. Indeed, start with a universal Chaitin machine U and effectively construct a Solovay machine U' such that $\Omega_{U'} = \frac{1}{2}\Omega_U$. Then, $\Omega_{U'}$ is less than $\frac{1}{2}$, so its 0th bit is 0, but *ZFC cannot prove* this fact!

We can now use Chaitin's theorem [9]

Theorem 11. *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 9 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*

"The 0th binary digit of the expansion of Ω_U is 0",
"The 1st binary digit of the expansion of Ω_U is s_1",
"The 2nd 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.

Acknowledgements

I wish to thank the Japan Advanced Institute for Science and Technology and Monbusho (Japan Ministry of Education, Science, Sports and Culture) for providing the excellent environment where this paper was written. I am indebted to Greg Chaitin, Bob Solovay, Karl Svozil and an anonymous referee for helpful comments and critique.

References

[1] C. Calude, Information and Randomness. An Algorithmic Perspective, Springer, Berlin, 1994.
[2] C.S. Calude, A characterization of c.e. random reals, Theoret. Comput. Sci., to appear.
[3] C.S. Calude, G.J. Chaitin, Randomness everywhere, Nature 400 (22) (1999) 319–320.
[4] C.S. Calude, P. Hertling, B. Khoussainov, Y. Wang, Recursively enumerable reals and Chaitin Ω numbers, in: M. Morvan, C. Meinel, D. Krob (Eds.), Proc. 15th Symp. on Theoretical Aspects of Computer Science (Paris), Springer, Berlin, 1998, pp. 596–606; Theoret. Comput. Sci. 255 (2001) 125–149.
[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, Berlin, 1994, pp. 44–66.
[6] C. Calude, A. Nies, Chaitin Ω numbers and strong reducibilities, J. Univ. Comput. Sci. 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: [10], 113–128).
[8] G.J. Chaitin, Algorithmic information theory, IBM J. Res. Develop. 21 (1977) 350–359, 496 (Reprinted in: [10], 44–58).
[9] G.J. Chaitin, Algorithmic Information Theory, Cambridge University Press, Cambridge, 1987 (Third printing 1990).
[10] G.J. Chaitin, Information, Randomness and Incompleteness, Papers on Algorithmic Information Theory, World Scientific, Singapore, 1987 (2nd ed., 1990).
[11] G.J. Chaitin, The Limits of Mathematics, Springer, Singapore, 1997.
[12] G.J. Chaitin, The Unknowable, Springer, Singapore, 1999.
[13] R.G. Downey, G.L. LaForte, Presentations of computably enumerable reals, CDMTCS Research Report 135, 2000, 23pp.
[14] P. Hertling, K. Weihrauch, Randomness spaces, in: K.G. Larsen, S. Skyum, G. Winskel (Eds.), Automata, Languages and Programming, Proc. 25th Int. Colloq. ICALP'98, Springer, Berlin, 1998, pp. 796–807.
[15] A. Kuçera, T.A. Slaman, Randomness and recursive enumerability, SIAM J. Comput. 31 (1) (2001) 199–211.
[16] P. Odifreddi, Classical Recursion Theory, North-Holland, Amsterdam, vol.1, 1989, vol. 2, 1999.
[17] T.A. Slaman, Random Implies Ω-Like, manuscript, 14 December 1998, 2 pp.
[18] 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.
[19] R.M. Solovay, A version of Ω for which *ZFC* cannot predict a single bit, in: C.S. Calude, G. Păun (Eds.), Finite Versus Infinite. Contributions to an Eternal Dilemma, Springer, London, 2000, pp. 323–334.
[20] L. Staiger, The Kolmogorov complexity of real numbers, in: G. Ciobanu, Gh. Păun (Eds.), Proc. Fundamentals of Computation Theory, Lecture Notes in Computer Science 1684, Springer, Berlin, 1999, pp. 536–546.