# CDMTCS
# Research
# Report
# Series

# Chaitin $\Omega$ Numbers, Solovay Machines, and Incompleteness

**Cristian S. Calude**
Department of Computer Science
University of Auckland

CDMTCS-114
October 1999

Centre for Discrete Mathematics and
Theoretical Computer Science

# Chaitin $\Omega$ Numbers, Solovay Machines, and Incompleteness*

**Cristian S. Calude**[†]

Draft 2.6, 7 October, 1999

**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's all over. Finally, a constructive version of Chaitin information-theoretic incompleteness theorem is proven.

## 1 Introduction

We will consider only reals in the unit interval $(0, 1)$. A real $\alpha$ 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. A real $\alpha$ is *random* if its binary expansion is a random (infinite) sequence (cf. [7, 8, 1]); the choice of base is irrelevant (cf. [6]).

In [7] (see also [8, 10, 11]), Chaitin has introduced the halting probability $\Omega_U$ of a "Chaitin universal machine" $U$–Chaitin's Omega number. He proved:

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

Are there other c.e. random reals? The answer is negative, and the proof is constructive, cf. Calude, Hertling, Khoussainov, Wang [5] and Slaman [12] (see also Calude and Chaitin [2], Calude [3]):

**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, 10]), Chaitin proved the following:

*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.

†School of Information Science, Japan Advanced Institute of Science, and Technology, JAIST, Room: I-78, Seventh Floor, Tatsunokuchi, Ishikawa 923-1292, Japan; on leave from the Department of Computer Science, University of Auckland, Private Bag 92019, Auckland, New Zealand; e-mails: `cristian@{jaist.ac.jp,cs.auckland.ac.nz}`.

**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 $\Omega_U$, and one can give a bound on the number of bits of $\Omega_U$ which ZFC can determine.*

The bound cited in Theorem 3 can be explicitly formulated, but it *is not effective*, in the sense that it's not computable. For example, in [10] 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 $\Omega_U$; $H(T)$ 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

$$\text{"The } n^{th} \text{ binary digit of the expansion of } \Omega_U \text{ is } k\text{"}, \tag{1}$$

for all $n \geq 0, k = 0, 1$. 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 [10, 11]):

**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, of course, not effectively computed.

Of course, for every c.e. random real $\alpha$ 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 $\Omega_U$.

By tuning the construction of the universal Chaitin machine, Solovay [14] went into the opposite direction and obtained a dramatic improvement of Theorem 3:

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

Solovay [14] proved sharper versions of both Theorem 3 and Theorem 5 by replacing $ZFC$ with a computably axiomatizable 1-consistent theory. Theorem 3 holds true for any universal Chaitin machine $U$ (it's 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 universal Chaitin machine $U$ for which $ZFC$ cannot determine more than the initial block of 1 bits of the binary expansion of its halting probability, $\Omega_U$, will be called *Solovay machine.*[3] In view of Theorem 2 and Theorem 5, we may ask the question:

$$\textit{Which c.e. random reals are halting probabilities of Solovay machines?} \tag{2}$$

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

[1] Zermelo set theory with choice.
[2] That is, any theorem of arithmetic proved by $ZFC$ is *true*.
[3] Of course, $U$ depends on $ZFC$.

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

**Corollary 7** *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* $\alpha$. *No c.e. random real* $\alpha \in (1/2, 1)$ *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* $\Omega_U$ *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.

## 2 Basic Definitions and Notation

Let $\Sigma = \{0, 1\}$. By $\Sigma^*$ we denote the set of binary strings (including the empty string, $\lambda$). 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 $\Sigma^*$ 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 $\Sigma^*$); see Calude [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 $A$ is the real number:

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

A *Chaitin machine (computer) U* is a partial computable string function whose domain dom($U$) is a prefix-free set.[4] Set $\Omega_U = \Omega_{\mathrm{dom}(U)}$. 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

[4] We follow Solovay's terminology [13, 14].

that for every $s, t \in \Sigma^*$, if $V(s) = t$, then $U(s') = t$, for some $s' \in \Sigma^*$ of length $|s'| \leq |s| + c$.

Universal Chaitin machines can be effectively constructed (see [9, 10, 1]). According to Theorem 1, if $U$ is universal, then $\Omega_U$ is random. As a corollary, $\Omega_U$ is irrational and does not have a computable binary expansion; however, $\Omega_U$ is c.e., that is, computable in the limit from below.

The set of Chaitin machines is c.e. Indeed, let $(\varphi_n)_{n\geq 0}$ be a Gödel numbering of all partial computable string functions. Then, there exists a partial computable function $\psi$ (depending upon two variables, a 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 $\varphi_n$ 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 $\psi_n$ and put $\Omega_n = \Omega_{D_n}$. The time relativized versions of $D_n$ and $\Omega_n$ 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 $\Omega_n$ 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 $(\Omega_n[t])_{t\geq 0}$ increase monotonically to $\Omega_n$.

This shows that every real $\Omega_n$ is c.e. (in fact, every c.e. real is an $\Omega_n$, for some $n$, cf. [5]); some $\Omega_n$'s may be even computable, but, in view of Theorem 1, if $\psi_n$ is universal, then $\Omega_n$ is random, so not computable.

# 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 $PA$).[5]

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 $\alpha$ with the $0^{th}$ digit: $\alpha = 0.\alpha_0\alpha_1\ldots$

Every statement of the form

$$\text{“The } n^{th} \text{ binary digit of the expansion of } \Omega_l \text{ is } k\text{”}, \tag{3}$$

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

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

**Theorem 9** *Assume $ZFC$ is arithmetically sound. Let $i \geq 0$ and consider the c.e. random real*

$$\alpha = 0.\underbrace{11\ldots1}_{i\ 1's}0\alpha_{i+1}\alpha_{i+2}\ldots$$

*Then, there exists a universal Chaitin machine, $U$ (depending upon $ZFC$ and $\alpha$), 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 $\Omega_U$.*

*c) $\alpha = \Omega_U$.*

A machine satisfying all conditions in Theorem 9 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 the closure under finite variations of random sequences[6] to effectively construct a universal Chaitin machine $\tilde{V}$ such that

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

if $i \geq 1$, 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`

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

`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.`

[6] If we delete (or add) a string from (to) the beginning of a random sequence, the new sequence thus obtained is still random, cf. Calude and Chiţescu [4]; see also Theorem 6.39 in Calude [1].

[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.

- `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. Otherwise, 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).

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, $|s_1| \geq 1$. 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 $i \geq 1$ 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

$$\{1, 10, 110, \ldots, \underbrace{11\ldots1}_{(i-1)\ 1's}0\},$$

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 $\Omega_U$. 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 $\Omega_U$ is irrational). Let $r' = r + 2^{-(n+1)}$.

Since $ZFC$ is arithmetically sound, the assertion "The $n^{th}$ binary bit of $\Omega_U$ 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 $\Omega_U \geq r + 2^{-(n+1)} = r'$, 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 $\Omega_U$ beyond its first $i \geq 1$ 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 $i \geq 1$, $U(01 \frown t)$ is undefined, for every string $t$. To finish the proof we notice that for $i = 0$,

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

and for $i \geq 1$,

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

If we set $i = 0$ in Theorem 9, then we get Corollary 7. 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 $\alpha$ is c.e. and random, but $\alpha > 1/2$, then $ZFC$ can determine the $0^{th}$ bit of $\alpha$ which is 1.

## 4 Incompleteness

Theorem 8 follows directly from Theorem 7: we *know* that the halting probability of a Solovay machine is less than 1/2, so its $0^{th}$ bit is 0, but $ZFC$ *cannot prove* this fact! In fact, for every binary string $s = s_1 s_2 \ldots s_n$ we can effectively construct a Solovay machine $U$ such that the binary expansion of $\Omega_U$ has the string $\langle 0 \rangle \frown s_1 s_2 \ldots s_n$ as prefix. Then, all statements

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

$$\text{“The } 1^{th} \text{ binary digit of the expansion of } \Omega_U \text{ is } s_1\text{”},$$

$$\text{“The } 2^{th} \text{ binary digit of the expansion of } \Omega_U \text{ is } s_2\text{”},$$

$$\vdots$$

$$\text{“The } (n+1)^{th} \text{ binary digit of the expansion of } \Omega_U \text{ is } s_n\text{”},$$

are true but unprovable in $ZFC$.

## Acknowledgment

I am indebted to Greg Chaitin, Bob Solovay, and Karl Svozil for helpful discussions and critique.

## References


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

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

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

[4] C. Calude and I. Chiţescu. Qualitative properties of P. Martin-Löf random sequences, *Boll. Unione Mat. Ital.* VII, Ser. B3, 240 (1989), 229-240.

[5] C.S. Calude, P. Hertling, B. Khoussainov, and Y. Wang. Recursively enumerable reals and Chaitin $\Omega$ 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. Full paper to appear in *Theoret. Comput. Sci.*

[6] 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.

[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 Limits of Mathematics*, Springer-Verlag, Singapore, 1997.

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

[12] T.A. Slaman. *Random Implies $\Omega$-Like*, manuscript, 14 December 1998, 2 pp.

[13] 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.

[14] R.M. Solovay. A version of $\Omega$ 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 (to appear).