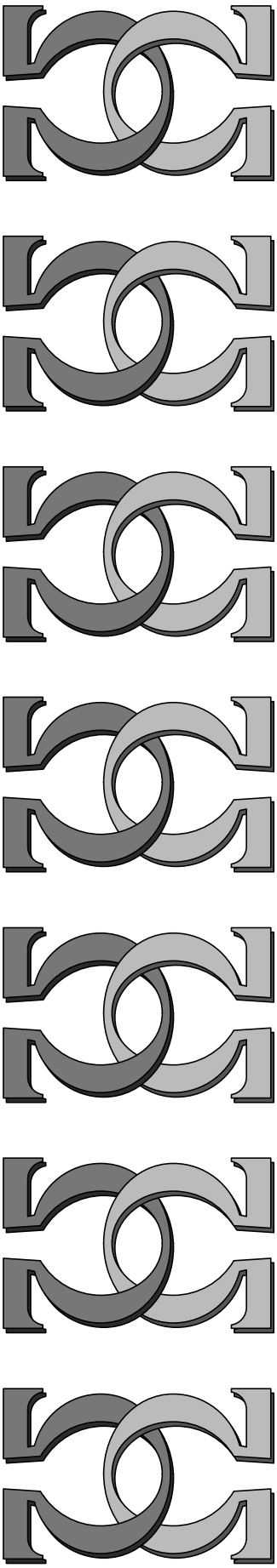

CDMTCS
Research
Report
Series

A Version of Ω for which ZFC can not Predict a Single Bit

Robert M. Solovay
University of California at Berkeley

CDMTCS-104
May 1999

Centre for Discrete Mathematics and
Theoretical Computer Science

A version of Ω for which ZFC can not predict a single bit

Robert M. Solovay*
solovay@math.berkeley.edu

May 16, 1999

1 Introduction

In [2], Chaitin introduced the real Ω and proved the following:

Theorem 1 *Assume that ZFC is arithmetically sound. [That is, any theorem of arithmetic proved by ZFC is* true.*] Then ZFC can determine the value of only finitely many bits of Ω. In fact we can explicitly compute a bound on the number of bits of Ω which ZFC can determine.*

Chaitin's theorem is much more general than what we have stated. ZFC can be replaced by any recursively axiomitizable theory in which Peano arithmetic can be interpreted.

The real Ω depends on the choice of "universal Chaitin machine". It is natural to suspect that by tuning this choice one can improve Chaitin's result.

Here is the main theorem of this paper:

Theorem 2 *We can choose the universal Chaitin computer U so that ZFC [if arithmetically sound] can not determine any bit of the Ω associated to U.*

The rest of this paper is organized as follows. Section 2 contains a review of the basic definitions of Chaitin's theory that we use. In section 3, we recall the notion of "1-consistent". [The hypothesis that ZFC is arithmetically sound can be sharpened, in both my theorem and Chaitin's, to merely asserting that ZFC is 1-consistent.] Section 4 gives a more detailed discussion of Chaitin's theorem. The remaining sections of the paper are devoted to a proof of our theorem.

I am grateful to Greg Chaitin for giving me a copy of his book [1] which started me thinking about this circle of ideas.

*I wish to thank the Isaac Newton Institute for providing the environment where this paper was written.

2 Preliminary definitions and notation

2.1 Bit strings

ω is the set of non-negative integers. I follow von Neumann so that each integer n is equal to the set $\{m \in \omega \mid m < n\}$ of integers less than n.

Σ^* is the set of finite sequences of 0's and 1's. Thus an element of Σ^* is just a function whose domain is in ω and whose range is included in $\{0, 1\}$.

The concatenation of the two bit strings s and t will be denoted by $s \frown t$. If j is one of 0 or 1, the bit string of length 1 whose sole component is j will be denoted by $\langle j \rangle$. Of course $\emptyset$ is the unique string of length 0.

If s is a bit string, we write $|s|$ for the length of s.

The usual theory of partial recursive functions is done considering functions whose domain and range are subsets of ω. We want to import this theory over to functions whose domain and range are subsets of Σ^* and for that, it is convenient to fix a canonical bijection between Σ^* and ω. This is done as follows:

We linearly order Σ^* by putting $s < t$ if either:

1. $|s| < |t|$ *or*
2. $|s| = |t|$ and s lexicographically precedes t.

With this ordering, there is a unique order isomorphism of Σ^* with ω [which will serve as the "canonical bijection" between the two sets.]

2.2 Prefix-free codes

A subset A of Σ is a prefix-free-code if whenever s and t are members of A such that $s \subseteq t$ then $s = t$.

Associated to any prefix-free code, A, is a real number Ω_A defined thus:

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

This has the following probabilistic interpretation: Pick a real x in $[0, 1]$ at random using the Lebesgue measure on $[0, 1]$. Then Ω_A is the probability that some initial prefix of the binary expansion of x lies in A.

2.3 Chaitin machines

A *Chaitin machine* is a partial recursive function whose domain and range are subsets of Σ^* and whose domain is a prefix-free code.

Let U be a Chaitin machine with domain A. Then we set $\Omega_U = \Omega_A$.

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 bit string π_V such that the equality

$$U(\pi_V \frown s) \simeq V(s)$$

holds for any bit string s.

Here, 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.

It is proved in [2] that universal Chaitin machines exist. Moreover, if U is universal, then Ω_U has a strong randomness property. [It is now know that Ω_U is Martin-Lof random.] As a corollary, Ω_U is irrational and does not have a recursive binary expansion.

2.4 Gödel numbering Chaitin machines

We fix one of the usual Gödel numberings $\{\varphi_i \mid i \in \omega\}$ of all partial recursive functions from Σ^* to Σ^*. Then the function $\Phi : \omega \times \Sigma^* \mapsto \Sigma^*$ given by

$$\Phi(i, s) \simeq \varphi_i(s)$$

is partial recursive.

It follows that the domain of Φ is recursively enumerable. Since it is clearly infinite, we fix a recursive enumeration without repetitions of the domain of Φ: $\langle \langle n_i, s_i \rangle \mid i \in \omega \rangle$. We can certainly arrange that this enumeration is primitive recursive.

We are going to construct a new function $\Psi : \omega \times \Sigma^* \mapsto \Sigma^*$. Defining $\psi_i : \Sigma^* \mapsto \Sigma^*$ (for $i \in \omega$) by

$$\psi_i(s) \simeq \Psi(i, s)$$

will yield the desired Gödel numbering of Chaitin machines.

Ψ will be the restriction of Φ to a certain subset of its domain. We proceed by induction on i to determine if the pair $\langle n_i, s_i \rangle$ will be placed in the domain of Ψ:

Place $\langle n_i, s_i \rangle$ in the domain of Ψ iff for no $j < i$ for which $\langle n_j, s_j \rangle$ has been placed in the domain of Ψ do we have $n_j = n_i$ and s_j compatible with s_i. [That is, $s_j \subseteq s_i$ or $s_i \subseteq s_j$.]

This construction has the following properties (whose proof is left to the reader):

1. The domain of ψ_i is prefix-free.

2. If the domain of φ_i is prefix-free, then $\psi_i = \varphi_i$.

2.5 Timing

We let D_n be the domain of ψ_n. Let $\Omega_n = \Omega_{D_n}$.

Intuitively, $D_n[t]$ is those elements of D_n which have appeared by time t. More precisely,

$$D_n[t] = \{s : (\exists j \leq t)(n_j = n \text{ and } s_j = s \text{ and } \langle n_j, s_j \rangle \text{ was placed into Dom}(\Psi) \text{ at stage } j\}$$

We put $\Omega_n[t] = \Omega_{D_n[t]}$. Intuitively, this is the approximation to Ω_n computable at time s.

The following facts are evident:

1. $\Omega_n[t]$ is a rational number with denominator a power of 2.
2. Given n and t we can compute [by a primitive recursive function] the finite set $D_n[t]$ and the rational number $\Omega_n[t]$.
3. As t increases to infinity, the $\Omega_n[t]$ increase monotonically to the limit Ω_n.

3 1-consistency

Throughout this section T is a theory with a recursive set of axioms in which Peano Arithmetic is relatively interpretable. We fix a relative interpretation of PA in T. Of course, the basic example we have in mind is ZFC equipped with the usual relative interpretation of PA in ZFC.

For brevity in what follows, we say "interpretation" rather than "relative interpretation".

Our main theorem will use the hypothesis that "ZFC is 1-consistent". In this first part of this section, we review known results without proof that describe the relationship of the notion of 1-consistency to other notions of soundness.

In the second part of this section, we derive from the assumption that ZFC is 1-consistent that any determination that ZFC makes about one of the binary digits of Ω_U [for some *universal* Chaitin computer U] is *true*. This will be the only use we make of the 1-consistency hypothesis.

3.1 A spectrum of soundness hypotheses

3.1.1 ω-models

Since there is a fixed interpretation of PA in T, any model of T determines a model of PA. We say that a model M of T is an ω-model if the associated model of PA is isomorphic to the standard model of PA.

Our first soundness assumption is that T has an ω-model.

3.1.2 Arithmetic soundness

Each sentence of the language of PA has a translation into a sentence of the language of T, determined by the interpretation of PA in T. We shall blur the distinction between a sentence of PA and its translation. We use the phrase "sentence of arithmetic" to indicate a sentence of the language of T that is the translation of some sentence of PA.

Our second soundness assumption is that T is arithmetically sound. That is, if ϑ is a sentence of arithmetic which is a theorem of T, then ϑ is true [in the standard model of PA].

Remark: Our metatheory is ZFC. So we know that PA itself is arithmetically sound.

3.1.3 ω-consistency

The notion of ω-consistency was introduced by Gödel in connection with his incompleteness theorems.

It is easiest to define when a theory T is *not* ω-consistent. [I.e., is ω-inconsistent.] This happens if there is a formula of the language of T, $\theta(x)$, [having only the indicated free variable x] such that the following happens:

1. T proves "There is an $x \in \omega$ such that $\theta(x)$."
2. For each natural number n, T proves "$\neg\theta(\mathbf{n})$".

In theories like PA which have a canonical term to denote each natural number, $\mathbf{n}$ is the canonical term that denotes the integer n. In theories like ZFC that lack such terms the explication of what the formula $\theta(\mathbf{n})$ is, is a little more subtle, but we presume the reader will be familiar with the details.

3.1.4 1-consistency

A theory T is 1-consistent, if whenever it proves a Σ^0_1 sentence, θ, then θ is true,

There is a notion of when a formula of PA is "primitive recursive". Basically these are the formulas that arise in implementing Gödel's proof that every primitive recursive predicate is expressible in PA.

A sentence of PA is Σ^0_1 if it has the form $(\exists x)P(x)$ where P is primitive recursive.

A special case of Σ^0_1 sentences are the formalizations of assertions that a particular Turing machine halts if started [in its canonical "start state"] on an empty tape. Indeed, every Σ^0_1 sentence is provably equivalent in PA to such a "halting statement".

3.1.5 Consistency

T is consistent if it does not prove the assertion "$0 = 1$". Equivalently, T is consistent if it does not prove every sentence in the language of T.

3.1.6 Positive relations between the different notions of soundness

These claims are all trivial: Every theory T that has an ω model is arithmetically sound and ω-consistent. If $T$is arithmetically sound or ω-consistent, then T is 1-consistent. If T is 1-consistent, then T is consistent.

3.1.7 Negative relations between the different notions of soundness

The claims that follow are not entirely trivial, but are all well-known. Details will not be given. The proof of our main theorem does not depend on these results.

There are theories T_1, T_2, T_3, and T_4, all in the language of ZFC and all extending ZC [Zermelo set theory with choice] such that:

1. T_1 is arithmetically sound but not ω-consistent.
2. T_2 is ω-consistent but not arithmetically sound.
3. T_3 is consistent, but not 1-consistent.
4. T_4 is not consistent.

3.1.8

From now on, when we say that a theory T is 1-consistent, it is implied that the theory has a recursive set of axioms and comes equipped with some definite interpretation of PA in T.

3.2 Proving facts about Ω

3.2.1 Binary expansions

A *dyadic rational* is a rational number of the form $r/2^s$ where r and s are integers and $s \geq 0$.

If x is a real number which is not a dyadic rational, then x has a unique binary expansion. If x is a dyadic rational, it has two distinct binary expansions. In this paper, we shall always pick the one that ends in an infinite sequence of 0's.

With this convention in place, the following can easily be formalized in PA: "The i^{th} binary digit of Ω_j is k." [Here $k < 2$, of course, if the assertion is true.]

We start numbering the digits of the binary expansion of a real with the 0^{th} digit. Thus the 0^{th} digit of the binary expansion of 1/3 is 0; the 1^{st} digit is 1; the 2^{nd} digit is 0, etc.

Lemma 3 *Let ψ_j be a Chaitin machine which PA can prove universal. Let T be 1-consistent, and let T prove the assertion "The i^{th} binary digit of Ω_j is k". Then this assertion is true.*

Our proof of this lemma will proceed in two steps. We first show that any Π^0_2 sentence proved by T is true. We then show the sentence in question in the lemma is provably equivalent in PA to a Π^0_2 sentence.

3.2.2 Π^0_2 sentences

A Π^0_2 sentence is a sentence of PA of the form $\forall x \exists y P(x, y)$, where P is primitive recursive.

Suppose then, towards a contradiction, that T proves the translation of such a Π^0_2 sentence, and that the sentence is false. Then for some particular integer n, the sentence $\exists y P(\mathbf{n}, y)$ is false and provable in T. But this latter sentence is Σ^0_1, and this contradicts the assumption that T is 1-consistent.

3.2.3 Proof of the lemma

We work in PA. We know that Ω_j is irrational. hence, we can express the fact that the i^{th} digit of Ω_j is k as follows:

$$(\forall m)(\exists n > m)\ [\text{the } i^{th} \text{ digit of } \Omega_j[n] \text{ is } k]$$

[The proof of this claim is easy and left to the reader.] But the assertion just displayed is visibly Π^0_2. The lemma is proved.

4 Chaitin's results about predicting bits of Ω

The results of this section, which are stated without proof, are not needed for the proof of the main theorem.

Throughout this section we fix a universal Chaitin machine U. [In the later parts of this section, we even implicitly specialize to a particular such U.]

We fix a j such that $U = \psi_j$. Formal assertions about U refer to this j.

We write Ω for Ω_U. As discussed in section 3.2.1, we can easily formalize in PA the assertion "The i^{th} binary digit of Ω is k". [This formalization uses the Gödel number, j, of Ω.]

Now let T be a 1-consistent theory of the sort discussed in section 3. Following Chaitin, we want to give an upper bound on the set of $i \in \omega$ such that T proves a theorem of the form "The i^{th} bit of the binary expansion of Ω is k" for some $k \leq 1$. We refer to this cardinality as "the number of bits of Ω that T can determine". Of course, a priori, this cardinality might be infinite; however, it will turn out to be finite.

4.1 $H(T)$

We wish to give a definition of the number of bits it takes to describe the arithmetical theorems of T.

We fix a Gödel numbering of the sentences of PA.

Now consider a theory T of the sort described above. We proceed to associate an r. e. set of strings W_T to T. Let $s \in \Sigma^*$. Then s corresponds to an integer n_s as discussed in section 2.1. Then $s \in W_T$ iff n_s is the Godel number of a sentence of PA whose translation is a theorem of T.

Now let $s \in \Sigma^*$. We say that s is a program for W_T if

1. $U(s)$ is defined and has the value t. Let n be the integer corresponding to t. [Cf. section 2.1.]

2. The domain of φ_n is W_T.

Finally, let $H(T)$ be the length of the shortest program for W_T.

We can now state Chaitin's theorem [proved in [2]].

Theorem 4 *Let U be a universal Chaitin computer. Then there is a positive constant C [depending only on U] such that [for T a 1-consistent theory] T can determine at most $C + H(T)$ bits of Ω.*

In [1], Chaitin describes a particular universal computer [whose implementation is done in a dialect of Lisp that Chaitin devised.] For a definition of $H(T)$ which is similar in spirit to the one I have given above, Chaitin proves the following:

Theorem 5 *Let U be the particular universal Chaitin computer defined in [1]. Let T be a 1-consistent theory. Then T determines at most $H(T)+15328$ bits of Ω_U.*

5 Precise statement of the main theorem. Outline of the proof.

Theorem 6 *Let T be a 1-consistent theory. Then there is a universal Chaitin computer, U [$= \psi_j$] such that:*

1. *PA proves the fact that U is universal.*

2. *T can not determine even a single bit of Ω_U.*

In particular, our theorem applies to ZFC provided that ZFC is 1-consistent.

Of course, the U provided by the theorem depends on T.

Here is a sketch of the proof. [Some technical details have been omitted from this sketch. They will be provided in the following sections where the proof will be presented in detail.]

We fix a standard Chaitin universal computer V such that the universality of V is provable in PA.

Our computer U will be undefined on the string $\emptyset$. For strings of the form $\langle 0\rangle \frown s$, we will have:

$$U(\langle 0\rangle \frown s) \simeq V(s)$$

This will ensure the universality claims made about U.

We are still free to define U on strings of the form $\langle 1\rangle \frown s$ as we wish. We will use this freedom to prevent T from guessing a single bit of Ω_U.

Thanks to the magic of the recursion theorem, we can assume that when defining U we know the Gödel number of U. Our algorithm when given a string of the form $\langle 1\rangle \frown s$ first begins an enumeration of the arithmetical theorems of T, looking for the first one of the form "The n^{th} bit of Ω_U is k". This search may go on forever without finding such a sentence. If it does succeed, we note the particular values of n and k. If s does not have length n, then $U(\langle 1\rangle \frown s)$ is undefined.

Let r be the dyadic rational whose dyadic expansion begins with $s \frown \langle k\rangle$ followed by an infinite string of 0's. Let $r' = r + 2^{-(n+1)}$. We search for a t such that $\Omega[t]$ lies in the interval (r, r'). If we find such, we make $U(\langle 1\rangle \frown s)$ be defined with the value $\emptyset$.

It seems reasonable that the final value of Ω should be at least $\Omega[t] + 2^{-(n+1)}$ since we have just added a new string of length $n+1$ to the domain of Ω. Thus the action we have just taken prevents Ω from being in the interval $(r.r')$.

But clearly, if T has correctly predicted the value of the n^{th} bit of Ω then Ω will lie in an interval of the form (r, r') for some length n bit string s. Thus our assumption that T can predict a single bit of Ω has led to a contradiction.

There are two points where we have to amplify the sketch to turn it into a correct proof.

1. We must check that the self-reference in the sketch can indeed be handled by the recursion theorem. [This is routine, but we shall treat this carefully in the final proof.]

2. The phrase "It seems reasonable" probably could be turned into a rigorous argument. But the detailed proof will proceed differently at this point.

6 Description of the construction

We will be defining a function $U : \Sigma^* \mapsto \Sigma^*$ that depends on an integer parameter j. [Intuitively, j is a guess at the Gödel number of U.] We will specify the value of j presently

U can be viewed as coming from a function $U_1 : \omega \times \Sigma^* \mapsto \Sigma^*$. [So $U(s0 \simeq U_1(j, s)$.] Our construction will be such that U_1 is partial recursive.

6.1

As discussed in the sketch, we fix a universal Chaitin computer V such that the universality of V is provable in PA.

We proceed to define $U(s)$ by cases:

Case 1: $s = \emptyset$.

Then $U(s)$ is undefined.

Case 2: $s = \langle 0 \rangle \frown t$ for some bit string t.

Then we set $U(s) \simeq V(t)$.

6.2 Case 3

This is the case where $s = \langle 1 \rangle \frown t$ for some bit string t.

Our construction begins with an preliminary calculation to determine certain constants n and k. This preliminary calculation may not converge. In that case U will be undefined at s for any s falling under Case 3.

The preliminary calculation lists the theorems of T in some definite order [not depending on t] searching for a theorem of the form "The n^{th} binary digit of Ω_j is k". If it finds such a theorem, then the value of n and k for the rest of the construction are those given by the first such theorem.

We will only define $U(\langle 1 \rangle \frown t)$ if $|t| = n$.

Suppose then that $|t| = n$. We define dyadic rationals r and r' as follows. r is the unique dyadic rational [in $[0, 1)$] whose binary expansion starts with $t \frown \langle k \rangle$ and whose digits [after the n^{th} one] are all 0. $r' = r + 2^{-(n+1)}$.

We now proceed to search for the least integer m such that $\Omega_j[m]$ lies in the open interval (r, r'). [Of course, this search might fail. If so, $U(s)$ is undefined.]

Recall that $D_j[m]$ is the finite set of strings in the domain of Ω_j that have contributed to the computation of $\Omega_j[m]$. [Cf. section 2.5.] If s appears in $D_j[m]$, then $U(s)$ is undefined. Otherwise, we set $U(s) = \emptyset$.

6.3 The recursion theorem applied

The recursion theorem assures us that there is a value of j such that $\varphi_j(s) \simeq U_1(j, s)$. We fix such a j and set $U = \varphi_j$. Thus in the definition of U just given, the value of the parameter j was the Gödel number of U.

7 Analysis of the construction

7.1 U is a Chaitin machine

Suppose that s_1 and s_2 are two elements of the domain of U such that $s_1 \subseteq s_2$. We have to see that $s_1 = s_2$.

Since U is undefined on the empty string, $|s_1| \geq 1$. Let $r = s_1(0)$. Let $s_i = \langle r \rangle \frown t_i$. Clearly $t_1 \subseteq t_2$. If $r = 0$, then t_1 and t_2 are in the domain of the Chaitin computer V. Hence $t_1 = t_2$. So $s_1 = s_2$.

If $r = 1$, then for $U(s_1)$ and $U(s_2)$ to be defined, we must have the integer n defined in the course of the construction. But then $|s_1| = |s_2| = n + 1$. So $s_1 = s_2$ as desired.

It follows that $U = \psi_j$ and that the real Ω_j used in the course of the construction is Ω_U. [Cf. section 2.4.]

7.2 U is universal

This follows from the definition of U on strings beginning with a 0. It is also clear that U inherits from V the fact that its universality is provable in PA.

Note that it follows that Ω_U is irrational. [Cf. section 2.3.]

7.3

Now, towards a contradiction, assume that T can determine some bit of Ω_U. Then in the course of the construction the integers n and k are defined.

Let r be a dyadic rational with denominator 2^{n+1} such that $r < \Omega_U < r + 2^{-(n+1)}$. [We use here the fact that Ω_U is irrational.] Let $r' = r + 2^{-(n+1)}$.

Since T is 1-consistent, the assertion "The n^{th} 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 bit string of length n. For all sufficiently large m, $\Omega_j[m]$ will lie in the interval (r, r').

Let $s = \langle 1 \rangle \frown t$. Consider now the computation of $U(s)$. The r and the r' involved in that computation are the ones we have just defined. The search for an m such that $\Omega_j[m] \in (r.r')$ will succeed.

Could it be that $s \in D_j[m]$? No, for then $U(s)$ would not be defined. But $D_j[m] \subseteq D_j$, so we would have $s \in D_j$. I.e. s *would* be in the domain of U after all, a contradiction.

So $U(s)$ 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 $\Omega_U \geq r + 2^{-(n+1)} = r'$. But this contradicts the definition of r. The proof of the main theorem is complete.

References

[1] G. J. Chaitin. *The limits of mathematics*, Springer-Verlag, Singapore, 1998.

[2] G. J. Chaitin. A theory of program size formally identical to information theory, *ACM Journal* 22 (1975), 329–340.