CDMTCS
Research
Report
Series

# Chaitin $\Omega$ Numbers and Strong Reducibilities

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

**André Nies**
Department of Mathematics
University of Chicago, IL U.S.A.

CDMTCS-062
October 1997

Centre for Discrete Mathematics and
Theoretical Computer Science

# Chaitin $\Omega$ Numbers and Strong Reducibilities*

**Cristian S. Calude**[†] **and** **André Nies**[‡]

**Abstract**

We prove that any Chaitin $\Omega$ number (i.e., the halting probability of a universal self-delimiting Turing machine) is wtt-complete, but not tt-complete. In this way *we obtain a whole class of natural examples of wtt-complete but not tt-complete r.e. sets.* The proof is direct and elementary.

## 1 Introduction

Kučera [8] has used Arslanov's completeness criterion[1] to show that all random sets of r.e. T-degree are in fact T-complete. Hence, *every Chaitin* $\Omega$ *number is T-complete.* In this paper we will strengthen this result by proving that *every Chaitin* $\Omega$ *number is weak truth-table complete.* However, no Chaitin $\Omega$ number can be tt-complete as, because of a result stated by Bennett [1] (see Juedes, Lathrop, and Lutz [9] for a proof), there is no random sequence $\mathbf{x}$ such that $K \leq_{tt} \mathbf{x}$.[2] Notice that in this way *we obtain a whole class of natural examples of wtt-complete but not tt-complete r.e. sets* (a fairly complicated construction of such a set was given by Lachlan [10]).

*The first has been partially supported by AURC A18/XXXXX/62090/F3414056, 1996. The second author was partially supported by NSF Grant DMS-9500983.

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

‡Department of Mathematics, University of Chicago, Chicago IL., USA. Email: `nies@math.uchicago.edu`.

[1] *An r.e.* $X$ *is Turing equivalent to the halting problem iff there is a Turing computable in* $X$ *function* $f$ *without fixed-points, i.e.* $W_x \neq W_{f(x)}$*, for all* $x$; see Soare [12], p. 88.

[2] To keep the paper self-contained, a direct simple proof for Bennett result will be included.

We continue with a piece of notation. Let $\mathbf{N}, \mathbf{Q}$ be the sets of non-negative integers and rationals. Let $\Sigma = \{0,1\}$ denote the binary alphabet, $\Sigma^*$ is the set of (finite) binary strings, $\Sigma^n$ is the set of binary strings of length $n$; the length of a string $x$ is denoted by $|x|$. By $x|r$ we denote the prefix of length $r$ of the string $x$. Let $p(x)$ be the place of $x$ in $\Sigma^*$ ordered quasi-lexicographically. Let $\Sigma^\omega$ the set of infinite binary sequences. The prefix of length $n$ of the sequence $\mathbf{x} \in \Sigma^\omega$ is denoted by $\mathbf{x}|n$. For every $X \subset \Sigma^*$, $X\Sigma^\omega$ stands for the cylinder generated by $X$, i.e., set of all sequences having a prefix in $X$.

Fix an acceptable gödelization $(\varphi_x)_{x\in\Sigma^*}$ of all partial recursive (p.r.) functions from $\Sigma^*$ to $\Sigma^*$, and let $W_x = \mathrm{dom}(\varphi_x)$ be the domain of $(\varphi_x)$. Denote by $K$ the set $\{x \in \Sigma^* \mid x \in W_x\}$. A Chaitin computer (self-delimiting Turing machine) is a p.r. function $C : \Sigma^* \xrightarrow{o} \Sigma^*$ with a prefix-free domain $\mathrm{dom}(C)$. The program-size (Chaitin) complexity induced by Chaitin's computer $C$ is defined by $H_C(x) = \min\{|y| \mid y \in \Sigma^*, C(y) = x\}$ (with the convention $\min\emptyset = \infty$).

A Chaitin computer $U$ is *universal* if for every Chaitin computer $C$, there is a constant $c > 0$ (depending upon $U$ and $C$) such that for every $x$ there is $x'$ such that $U(x') = C(x)$ and $|x'| \le |x| + c$;[3] $c$ is the "simulation" constant of $C$ on $U$.

A Martin-Löf test is an r.e. sequence $(V_i)_{i\ge 0}$ of subsets of $\Sigma^*$ satisfying the following measure-theoretical condition:

$$\mu(V_i\Sigma^\omega) \le 2^{-i},$$

for all $i \in \mathbf{N}$. Here $\mu$ denotes the usual product measure on $\Sigma^\omega$, given by $\mu(\{w\}\Sigma^\omega) = 2^{-|w|}$, for $w \in \Sigma^*$.

An infinite sequence $\mathbf{x}$ is *random* if for every Martin-Löf test $(V_i)_{i\ge 0}$, $\mathbf{x} \notin \bigcap_{i\ge 0} A_i\Sigma^\omega$. A real $\alpha \in (0,1)$ is *random* in case its binary expansion is a random sequence.[4]

The halting probability of Chaitin's computer $C$ is

$$\Omega_C = \mu(\mathrm{dom}(U)\Sigma^\omega) = \sum_{x\in\mathrm{dom}(C)} 2^{-|x|}.$$

Any real $\Omega_C$ is recursively enumerable (r.e.) in the sense that the set $\{q \in (0,1)\cap\mathbf{Q} \mid q < \Omega_C\}$ is r.e. (see more about r.e. reals in [3]). Reals of the form $\Omega_U$, for some universal Chaitin computer $U$, are called *Chaitin* ($\Omega$) *numbers* (see [4, 6, 2]). Chaitin [4] has proved that *every Chaitin number is random.* See Calude [2] for more details.

For a set $A \subset \Sigma^*$ we denote by $\chi_A$ the characteristic function of $A$. We say that $A$ is Turing reducible to $B$, and we write $A \le_T B$, if there is an oracle Turing machine $\varphi_w^B$ such that $\varphi_w^B(x) = \chi_A(x)$. We say that $A$ is weak truth-table reducible to $B$, and we write $A \le_{wtt} B$, if $A \le_T B$ 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 recursive function. We

[3] In fact, $c$ can be effectively obtained from $U$ and $C$.

[4] Actually, the choice of base is irrelevant, cf. Theorem 6.111 in Calude [2].

say that $A$ is truth-table reducible to $B$, and we write $A \leq_{tt} B$, if there is a recursive sequence of Boolean functions $\{F_x\}_{x \in \Sigma^*}$, $F_x : \Sigma^{r_x+1} \to \Sigma$, such that for all $x$, we have $\chi_A(x) = F_x(\chi_B(0)\chi_B(1)\cdots\chi_B(r_x))$.[5] An r.e. set $A$ is tt(wtt)-complete if $K \leq_{tt} A$ ($K \leq_{wtt} A$). See Odifreddi [11] for more details.

## 2 Main Results

In what follows we will fix a universal Chaitin computer $U$ and write $H = H_U$, $\Omega = \Omega_U$.

**Theorem 2.1** *The set $\mathcal{H} = \{(x, n) \mid x \in \Sigma^*, n \in \mathbf{N},\ H(x) \leq n\}$[6] is wtt-complete.*

**Proof.** We will refine the proof by Arslanov and Calude in [7]. To this aim we will use Arslanov's Completeness Criterion (see Theorem III.8.17 in Odifreddi [11], p. 338) for wtt-reducibility

> *an r.e. set $A$ is wtt-complete iff there is a function $f \leq_{wtt} A$ without fixed-points*

and the estimation due to Chaitin [4, 5] (see Theorem 5.4 in Calude [2], pp. 77):

$$\max_{x \in \Sigma^n} H(x) = n + \mathrm{O}(\log n). \tag{1}$$

First we construct a positive integer $c > 0$ and a p.r. function $\psi : \Sigma^* \stackrel{o}{\to} \Sigma^*$ such that for every $x \in \Sigma^*$ with $W_x \neq \emptyset$,

$$U(\psi(x)) \in W_x, \tag{2}$$

and

$$|\psi(x)| \leq p(x) + c. \tag{3}$$

Consider now a Chaitin computer $C$ such that $C(0^{p(x)}1) \in W_x$ whenever $W_x \neq \emptyset$. Let $c'$ be the simulation constant of $C$ on $U$, and let $\theta$ be a p.r. function satisfying the following condition: if $C(u)$ is defined, then $U(\theta)(u) = C(u)$ and $|\theta(u)| \leq |u| + c'$. Put

[5] Note that in contrast with tt-reductions, a wtt-reduction may diverge.

[6] This set is essential in deriving Chaitin's information-theoretical version of incompleteness, [4].

$c = c' + 1$ and notice that in case $W_x \neq \emptyset$, $C(0^{p(x)}1) \in W_x$, so $\theta(0^{p(x)}1)$ is defined and and belongs to $W_x$. Finally, put $\psi(x) = \theta(0^{p(x)}1)$ and notice that

$$|\psi(x)| = |\theta(0^{p(x)}1)| \leq |0^{p(x)}1| + c' = p(x) + c.$$

Next define the function

$$F(y) = \min\{x \in \Sigma^* \mid H(x) > p(y) + c\},$$

where the minimum is taken according to the quasi-lexicographical order and $c$ comes from (3). In view of (1) it follows that

$$F(y) = \min\{x \in \Sigma^* \mid H(x) > p(y) + c, |x| \leq p(y) + c\}.$$

The function $F$ is total, $H$-recursive and $U(\psi(y)) \neq F(y)$ whenever $W_y \neq \emptyset$. Indeed, if $W_y \neq \emptyset$ and $U(\psi(y)) = F(y)$, then $\psi(y)$ is defined, so $U(\psi(y)) \in W_y$ and $|\psi(y)| \leq p(y) + c$. But, in view of the construction of $F$, $H(F(y)) > p(y) + c$, an inequality which contradicts (3): $H(F(y)) \leq |\psi(y)| \leq p(y) + c$.

Let $f$ be an $H$-recursive function satisfying $W_{f(y)} = \{F(y)\}$. To compute $f(y)$ in terms of $F(y)$ we need to perform the test $H(x) > p(y) + c$ only for those strings $x$ satisfying the inequality $|x| \leq p(y) + c$, so the function $f$ is wtt-reducible to $\mathcal{H}$.

We conclude by proving that for every $y \in \Sigma^*$, $W_{f(y)} \neq W_y$. If $W_{f(y)} = W_y$, then $W_y = \{F(y)\}$, so by (3), $U(\psi(y)) \in W_y$, that is $U(\psi(y)) = F(y)$. Consequently, by (2) $H(F(y)) \leq |\psi(y)| \leq p(y) + c$, which contradicts the construction of $F$. □

**Theorem 2.2** *The set $\mathcal{H}$ is wtt-reducible to $\Omega$.*

**Proof.** Let $g : \mathbf{N} \to \Sigma^*$ be a recursive, one-to-one function which enumerates the domain of $U$ and put $\omega_m = \sum_{i=0}^{m} 2^{-|g(i)|}$. Given $x$ and $n > 0$ we compute the smallest $t \geq 0$ such that

$$\omega_t \geq 0.\Omega_0\Omega_1 \cdots \Omega_n.$$

From the relations

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

we deduce that $|g(s)| > n$, for every $s \geq t+1$. Consequently, if $x$ is not produced by an element in the set $\{g(0), g(1), \ldots, g(t)\}$, then $H(x) > n$ as $H(x) = |g(s)|$, for some $s \geq t+1$; conversely, if $H(x) \leq n$, then $x$ must be produced via $U$ by one of the elements of the set $\{g(0), g(1), \ldots, g(t)\}$. □

Since the result in Juedes, Lathrop, and Lutz [9] is obtained in a rather indirect way, we conclude the paper by proving directly that $K \not\leq_{tt} \mathbf{x}$, for every random sequence $\mathbf{x}$.

**Theorem 2.3** *If $K \leq_{tt} \mathbf{x}$, then $\mathbf{x}$ is not random.*

**Proof.** Assume $\mathbf{x}$ is random and $K \leq_{tt} \mathbf{x}$, that is there exists a recursive sequence of Boolean functions $\{F_u\}_{u \in \Sigma^*}$, $F_u : \Sigma^{r_u+1} \to \Sigma$, such that for all $w \in \Sigma^*$, we have $\chi_A(w) = F_w(x_0 x_1 \cdots x_{r_w})$. We will construct a Martin-Löf test $V$ such that $\mathbf{x} \in \bigcap_{n \geq 0} V_n \Sigma^\omega$, which will contradict the randomness of $\mathbf{x}$.

For every string $z$ let

$$M(z) = \{u \in \Sigma^{r_z+1} \mid F_z(u) = 0\}.$$

Consider the set

$$\{z \in \Sigma^* \mid \mu(M(z)\Sigma^\omega) \geq \frac{1}{2}\}$$

of inputs to the tt-reduction of $K$ to $\mathbf{x}$ where at least half of the possible oracle strings give the output 0. This set is r.e., so let $W_{z_0}$ be a name for it. From the construction it follows that

$$z_0 \in K \Leftrightarrow F_{z_0}(x_0 x_1 \cdots x_{r_{z_0}}) = 1,$$

hence if we put $r = r_{z_0} + 1$ and

$$V_0 = \{u \in \Sigma^r \mid \mu(M(z_0)\Sigma^\omega) \geq \frac{1}{2} \Leftrightarrow F_{z_0}(u) = 1\}$$

we ensure that $V$ is r.e. and $\mu(V_0\Sigma^\omega) \leq \frac{1}{2}$. Moreover $\mathbf{x} \in V_0\Sigma^\omega$, because if $u = \mathbf{x}|r$, then

$$\mu(M(z_0)\Sigma^\omega) \geq \frac{1}{2} \Leftrightarrow z_0 \in K \Leftrightarrow F_{z_0}(u) = 1.$$

Assume now that $z_n, V_n$ have been constructed such that $\mathbf{x} \in V_n\Sigma^\omega$ and $\mu(V_n\Sigma^\omega) \leq 2^{-n-1}$. Let $z_{n+1} \notin \{z_0, z_1, \ldots, z_n\}$ be such that

$$W_{z_{n+1}} = \{u \in \Sigma^* \mid \mu(M(u)\Sigma^\omega \cap V_n\Sigma^\omega) \geq \frac{1}{2} \cdot \mu(V_n\Sigma^\omega)\}.$$

Then

$$z_{n+1} \in K \Leftrightarrow \mu(M(u)\Sigma^\omega \cap V_n\Sigma^\omega) \geq \frac{1}{2} \cdot \mu(V_n\Sigma^\omega).$$

Finally put $r = r_{z_{n+1}+1}$ and

$$V_{n+1} = \{u \in \Sigma^r \mid u|r_{z_n} \in V_n \wedge (\mu(M(z_{n+1})\Sigma^\omega \cap V_n\Sigma^\omega) \geq \frac{1}{2} \cdot \mu(V_n\Sigma^\omega) \Leftrightarrow F_{z_{n+1}}(u) = 1)\}$$

and note that $V_{n+1}$ is r.e., $\mathbf{x} \in V_{n+1}$ and

$$\mu(V_{n+1}\Sigma^\omega) \leq \frac{1}{2} \cdot \mu(V_n\Sigma^\omega) \leq 2^{-n-2}.$$

Consequently, $(V_n)_n$ is a Martin-Löf test with $\mathbf{x} \in \bigcap_{n \geq 0} V_n\Sigma^\omega$. $\square$

## References


[1] C. H. Bennett. Logical depth and physical complexity, in R. Herken (ed.). *The Universal Turing Machine. A Half-Century Survey*, Oxford University Press, Oxford, 1988, 227–258.

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

[3] C. S. Calude, P. H. Hertling, B. Khoussainov, Y. Wang. Recursively enumerable reals and Chaitin $\Omega$ numbers, *CDMTCS Research Report* 055, 1997, 22 pp.

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

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

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

[7] G. J. Chaitin, A. Arslanov, C. Calude. Program-size complexity computes the halting problem, *EATCS Bull.* 57 (1995), 198-200.

[8] A. Kučera. Measure, $\Pi_1^0$-classes and complete extensions of PA, In: H. D. Ebbinghaus and G. H. Müller (eds.) *Recursion Theory Week* (Oberwolfach, 1984), Lecture Notes in Math., 1141, Springer-Verlag, Berlin, 1985, 245-259.

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

[10] A. H. Lachlan. wtt-complete sets are not necessarily tt-complete, *Proc. Amer. Math. Soc.* 48 (1975), 429-434.

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

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