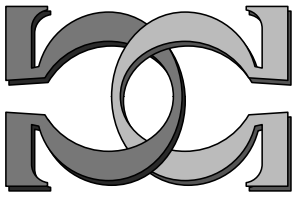

CDMTCS
Research
Report
Series

A New Representation of Chaitin Ω Number Based on Compressible Strings

Kohtaro Tadaki
Chuo University, Japan

CDMTCS-380
April 2010

Centre for Discrete Mathematics and
Theoretical Computer Science

A New Representation of Chaitin Ω Number Based on Compressible Strings

Kohtaro Tadaki

Research and Development Initiative, Chuo University
JST CREST
1–13–27 Kasuga, Bunkyo-ku, Tokyo 112-8551, Japan
E-mail: tadaki@kc.chuo-u.ac.jp
http://www2.odn.ne.jp/tadaki/

Abstract. In 1975 Chaitin introduced his Ω number as a concrete example of random real. The real Ω is defined based on the set of all halting inputs for an optimal prefix-free machine U, which is a universal decoding algorithm used to define the notion of program-size complexity. Chaitin showed Ω to be random by discovering the property that the first n bits of the base-two expansion of Ω solve the halting problem of U for all binary inputs of length at most n. In this paper, we introduce a new representation Θ of Chaitin Ω number. The real Θ is defined based on the set of all compressible strings. We investigate the properties of Θ and show that Θ is random. In addition, we generalize Θ to two directions $\Theta(T)$ and $\overline{\Theta}(T)$ with real $T > 0$. We then study their properties. In particular, we show that the computability of the real $\Theta(T)$ gives a sufficient condition for a real $T \in (0, 1)$ to be a fixed point on partial randomness, i.e., to satisfy the condition that the compression rate of T equals to T.

Key words: algorithmic information theory, Chaitin Ω number, randomness, partial randomness, fixed point, program-size complexity

1 Introduction

Algorithmic information theory (AIT, for short) is a framework for applying information-theoretic and probabilistic ideas to recursive function theory. One of the primary concepts of AIT is the *program-size complexity* (or *Kolmogorov complexity*) $H(s)$ of a finite binary string s, which is defined as the length of the shortest binary input for a universal decoding algorithm U, called an *optimal prefix-free machine*, to output s. By the definition, $H(s)$ can be thought of as the information content of the individual finite binary string s. In fact, AIT has precisely the formal properties of classical information theory (see Chaitin [5]). In particular, the notion of program-size complexity plays a crucial role in characterizing the *randomness* of an infinite binary string, or equivalently, a real. In [5] Chaitin introduced the halting probability Ω as an example of random real. His Ω is defined based on the set of all halting inputs for U, and plays a central role in the metamathematical development of AIT [7]. The first n bits of the

base-two expansion of Ω solve the halting problem of U for inputs of length at most n. Based on this property, Chaitin showed that Ω is random.

In this paper, we introduce a new representation Θ of Chaitin Ω number. The real Θ is defined based on the set of all compressible strings, i.e., all finite binary strings s such that $H(s) < |s|$, where $|s|$ is the length of s. The first n bits of the base-two expansion of Θ enables us to calculate a random finite string of length n, i.e., a finite binary string s for which $|s| = n$ and $|s| \leq H(s)$. Based on this property, we show that Θ is random.

In the works [14, 15] we introduced the notion of *partial randomness* for a real as a stronger representation of the compression rate of a real by means of program-size complexity. At the same time, we generalized the halting probability Ω to $Z(T)$ so that the partial randomness of $Z(T)$ can be controlled by a real T with $0 < T \leq 1$.[1] As T becomes larger, the partial randomness of $Z(T)$ increases. When $T = 1$, $Z(T)$ becomes a random real, i.e., $Z(1) = \Omega$. Later on, in the work [16] we revealed a special significance of the computability of the value $Z(T)$. Namely, we proved *the fixed point theorem on partial randomness*,[2] which states that, for every $T \in (0, 1)$, if $Z(T)$ is a computable real, then the partial randomness of T equals to T, and therefore the compression rate of T equals to T, i.e., $\lim_{n\to\infty} H(T\upharpoonright_n)/n = T$, where $T\upharpoonright_n$ is the first n bits of the base-two expansion of T.

In a similar manner to the generalization of Ω to $Z(T)$, in this paper we generalize Θ to two directions $\Theta(T)$ and $\overline{\Theta}(T)$. We then show that the reals $\Theta(T)$ and $\overline{\Theta}(T)$ both have the same randomness properties as $Z(T)$. In particular, we show that the fixed point theorem on partial randomness, which has the same form as for $Z(T)$, holds for $\Theta(T)$.

The paper is organized as follows. We begin in Section 2 with some preliminaries to AIT and partial randomness. In Section 3 we introduce Θ and study its property. Subsequently, we generalize Θ to two directions $\Theta(T)$ and $\overline{\Theta}(T)$ in Section 4 and Section 5, respectively. In Section 6, we prove the fixed point theorem on partial randomness based on the computability of $\Theta(T)$.

2 Preliminaries

We start with some notation about numbers and strings which will be used in this paper. $\#S$ is the cardinality of S for any set S. $\mathbb{N} = \{0, 1, 2, 3, \dots\}$ is the set of natural numbers, and $\mathbb{N}^+$ is the set of positive integers. $\mathbb{Q}$ is the set of rationals, and $\mathbb{R}$ is the set of reals. A sequence $\{a_n\}_{n\in\mathbb{N}}$ of numbers (rationals or reals) is called *increasing* if $a_{n+1} > a_n$ for all $n \in \mathbb{N}$. Normally, $O(1)$ denotes any function $f\colon \mathbb{N}^+ \to \mathbb{R}$ such that there is $C \in \mathbb{R}$ with the property that $|f(n)| \leq C$ for all $n \in \mathbb{N}^+$. On the other hand, $o(n)$ denotes any function $g\colon \mathbb{N}^+ \to \mathbb{R}$ such that $\lim_{n\to\infty} g(n)/n = 0$.

[1] In [14, 15], $Z(T)$ is denoted by Ω^T.

[2] The fixed point theorem on partial randomness is called a fixed point theorem on compression rate in [16].

$\{0,1\}^* = \{\lambda, 0, 1, 00, 01, 10, 11, 000, \dots\}$ is the set of finite binary strings where λ denotes the *empty string*, and $\{0,1\}^*$ is ordered as indicated. We identify any string in $\{0,1\}^*$ with a natural number in this order, i.e., we consider $\varphi\colon \{0,1\}^* \to \mathbb{N}$ such that $\varphi(s) = 1s - 1$ where the concatenation $1s$ of strings 1 and s is regarded as a dyadic integer, and then we identify s with $\varphi(s)$. For any $s \in \{0,1\}^*$, $|s|$ is the *length* of s. For any $n \in \mathbb{N}$, we denote by $\{0,1\}^n$ the set $\{\, s \mid s \in \{0,1\}^* \ \&\ |s| = n\}$. A subset S of $\{0,1\}^*$ is called *prefix-free* if no string in S is a prefix of another string in S. For any function f, the domain of definition of f is denoted by $\operatorname{dom} f$. We write "r.e." instead of "recursively enumerable."

Let α be an arbitrary real. For any $n \in \mathbb{N}^+$, we denote by $\alpha\restriction_n \in \{0,1\}^*$ the first n bits of the base-two expansion of $\alpha - \lfloor\alpha\rfloor$ with infinitely many zeros, where $\lfloor\alpha\rfloor$ is the greatest integer less than or equal to α. For example, in the case of $\alpha = 5/8$, $\alpha\restriction_6 = 101000$. A real α is called *right-computable* if there exists a total recursive function $f\colon \mathbb{N}^+ \to \mathbb{Q}$ such that $\alpha \le f(n)$ for all $n \in \mathbb{N}^+$ and $\lim_{n\to\infty} f(n) = \alpha$. On the other hand, a real α is called *left-computable* if $-\alpha$ is right-computable. A left-computable real is also called a *r.e.* real. It is then easy to show the following theorem.

Theorem 1. *Let $\alpha \in \mathbb{R}$.*

(i) α is computable if and only if α is both right-computable and left-computable.
(ii) α is right-computable if and only if the set $\{\, r \in \mathbb{Q} \mid \alpha < r \,\}$ is r.e. □

2.1 Algorithmic Information Theory

In the following we concisely review some definitions and results of AIT [5, 7]. A *prefix-free machine* is a partial recursive function $C\colon \{0,1\}^* \to \{0,1\}^*$ such that $\operatorname{dom} C$ is a prefix-free set. For each prefix-free machine C and each $s \in \{0,1\}^*$, $H_C(s)$ is defined by $H_C(s) = \min\{\, |p| \mid p \in \{0,1\}^* \,\&\, C(p) = s \,\}$ (may be ∞). A prefix-free machine U is said to be *optimal* if for each prefix-free machine C there exists $d \in \mathbb{N}$ with the following property; if $p \in \operatorname{dom} C$, then there is $q \in \operatorname{dom} U$ for which $U(q) = C(p)$ and $|q| \le |p| + d$. It is easy to see that there exists an optimal prefix-free machine. We choose a particular optimal prefix-free machine U as the standard one for use, and define $H(s)$ as $H_U(s)$, which is referred to as the *program-size complexity* of s, the *information content* of s, or the *Kolmogorov complexity* of s [9, 11, 5]. It follows that for every prefix-free machine C there exists $d \in \mathbb{N}$ such that, for every $s \in \{0,1\}^*$,

$$H(s) \le H_C(s) + d. \tag{1}$$

Based on this we can show that, for every partial recursive function $\Psi\colon \{0,1\}^* \to \{0,1\}^*$, there exists $d \in \mathbb{N}$ such that, for every $s \in \operatorname{dom}\Psi$,

$$H(\Psi(s)) \le H(s) + d. \tag{2}$$

Based on (1) we can also show that there exists $d \in \mathbb{N}$ such that, for every $s \ne \lambda$,

$$H(s) \le |s| + 2\log_2|s| + d. \tag{3}$$

For any $s \in \{0,1\}^*$, we define s^* as $\min\{\, p \in \{0,1\}^* \mid U(p) = s\}$, i.e., the first element in the ordered set $\{0,1\}^*$ of all strings p such that $U(p) = s$. Then, $|s^*| = H(s)$ for every $s \in \{0,1\}^*$.

Chaitin [5] introduced Ω number as follows. For each optimal prefix-free machine V, the halting probability Ω_V of V is defined by

$$\Omega_V = \sum_{p \in \mathrm{dom}\, V} 2^{-|p|}.$$

For every optimal prefix-free machine V, since $\mathrm{dom}\, V$ is prefix-free, Ω_V converges and $0 < \Omega_V \leq 1$. For any $\alpha \in \mathbb{R}$, we say that α is *weakly Chaitin random* if there exists $c \in \mathbb{N}$ such that $n - c \leq H(\alpha\restriction_n)$ for all $n \in \mathbb{N}^+$ [5, 7]. Chaitin [5] showed that Ω_V is weakly Chaitin random for every optimal prefix-free machine V. Therefore $0 < \Omega_V < 1$ for every optimal prefix-free machine V.

2.2 Partial Randomness

In the works [14, 15], we generalized the notion of the randomness of a real so that *the degree of the randomness*, which is often referred to as *the partial randomness* recently [3, 12, 4], can be characterized by a real T with $0 < T \leq 1$ as follows.

Definition 1 (weak Chaitin T-randomness). *Let $T \in (0,1]$ and let $\alpha \in \mathbb{R}$. We say that α is weakly Chaitin T-random if there exists $c \in \mathbb{N}$ such that, for all $n \in \mathbb{N}^+$, $Tn - c \leq H(\alpha\restriction_n)$.* □

In the case where $T = 1$, the weak Chaitin T-randomness results in weak Chaitin randomness.

Definition 2 (T-compressibility and strict T-compressibility). *Let $T \in (0,1]$ and let $\alpha \in \mathbb{R}$. We say that α is T-compressible if $H(\alpha\restriction_n) \leq Tn + o(n)$, namely, if $\limsup_{n\to\infty} H(\alpha\restriction_n)/n \leq T$. We say that α is strictly T-compressible if there exists $d \in \mathbb{N}$ such that, for all $n \in \mathbb{N}^+$, $H(\alpha\restriction_n) \leq Tn + d$.* □

For every real α, if α is weakly Chaitin T-random and T-compressible, then $\lim_{n\to\infty} H(\alpha\restriction_n)/n = T$, i.e., the *compression rate* of α equals to T.

In the works [14, 15], we generalized Chaitin Ω number to $Z(T)$ as follows. For each optimal prefix-free machine V and each real $T > 0$, the *generalized halting probability* $Z_V(T)$ of V is defined by

$$Z_V(T) = \sum_{p \in \mathrm{dom}\, V} 2^{-\frac{|p|}{T}}.$$

Thus, $Z_V(1) = \Omega_V$. If $0 < T \leq 1$, then $Z_V(T)$ converges and $0 < Z_V(T) < 1$, since $Z_V(T) \leq \Omega_V < 1$. The following theorem holds for $Z_V(T)$.

Theorem 2 (Tadaki [14, 15]). *Let V be an optimal prefix-free machine.*

(i) *If* $0 < T \leq 1$ *and* T *is computable, then* $Z_V(T)$ *is a left-computable real which is weakly Chaitin* T*-random and* T*-compressible.*
(ii) *If* $1 < T$*, then* $Z_V(T)$ *diverges to* ∞*.* □

The computability of the value $Z_V(T)$ has a special implication on T as follows.

Theorem 3 (fixed point theorem on partial randomness, Tadaki [16]). *Let* V *be an optimal prefix-free machine. For every* $T \in (0,1)$*, if* $Z_V(T)$ *is computable, then* T *is weakly Chaitin* T*-random and* T*-compressible, and therefore*

$$\lim_{n\to\infty} \frac{H(T\restriction_n)}{n} = T. \tag{4}$$

The equality (4) means that the compression rate of T equals to T itself. Intuitively, we might interpret the meaning of (4) as follows: Consider imaginarily a file of infinite size whose content is

"The compression rate of this file is $0.100111001\ldots\ldots$"

When this file is compressed, the compression rate of this file actually equals to $0.100111001\ldots\ldots$, as the content of this file says. This situation is self-referential and forms a fixed point. For a simple and self-contained proof of Theorem 3, see Section 5 of Tadaki [18].

A left-computable real has a special property on partial randomness, as shown in Theorem 4 below. For completeness, we include the proof of Theorem 4 in Appendix A.

Definition 3 (T-convergence, Tadaki [17]). *Let* $T \in (0,1]$*. An increasing sequence* $\{a_n\}$ *of reals is called* T*-convergent if* $\sum_{n=0}^{\infty}(a_{n+1}-a_n)^T < \infty$*. A left-computable real* α *is called* T*-convergent if there exists a* T*-convergent computable, increasing sequence of rationals which converges to* α*.* □

Theorem 4 (Tadaki [19]). *Let* T *be a computable real with* $0 < T < 1$*. For every left-computable real* α*, if* α *is* T*-convergent then* α *is strictly* T*-compressible.* □

3 New Representation of Chaitin Ω Number

In this section, we introduce a new representation Θ of Chaitin Ω number based on the set of all compressible strings, and investigate its property.

Definition 4. *For any optimal prefix-free machine* V*,* Θ_V *is defined by*

$$\Theta_V = \sum_{H_V(s)<|s|} 2^{-|s|},$$

where the sum is over all $s \in \{0,1\}^*$ *such that* $H_V(s) < |s|$*.* □

For each optimal prefix-free machine V, we see that

$$\Theta_V < \sum_{H_V(s)<|s|} 2^{-H_V(s)} \leq \sum_{s\in\{0,1\}^*} 2^{-H_V(s)} \leq \sum_{p\in\mathrm{dom}\, V} 2^{-|p|} = \Omega_V.$$

Thus, Θ_V converges and $0 < \Theta_V < \Omega_V$ for every optimal prefix-free machine V. It is important to evaluate how many strings s satisfy the condition $H_V(s) < |s|$. For that purpose, we define $S_V(n) = \{\, s \in \{0,1\}^* \mid |s| = n \;\&\; H_V(s) < n \,\}$ for each optimal prefix-free machine V and each $n \in \mathbb{N}$. We can then show the following theorem.

Theorem 5. *Let V be an optimal prefix-free machine. Then $S_V(n) \subsetneqq \{0,1\}^n$ for every $n \in \mathbb{N}$. Moreover $\#S_V(n) = 2^{n-H(n)+O(1)}$ for all $n \in \mathbb{N}^+$, i.e., there exists $d \in \mathbb{N}$ such that (i) $\#S_V(n) \leq 2^{n-H(n)+d}$ for all $n \in \mathbb{N}$, and (ii) $2^{n-H(n)-d} \leq \#S_V(n)$ for all sufficiently large $n \in \mathbb{N}$.* □

The first half of Theorem 5 is easily shown by counting the number of binary strings of length less than n. Solovay [13] showed that $\#\{\, s \in \{0,1\}^* \mid H_V(s) < n \,\} = 2^{n-H(n)+O(1)}$ for every optimal prefix-free machine V. The last half of Theorem 5 slightly improves this result. For completeness, we include the proof of Theorem 5 in Appendix B.

Theorem 6. *For every optimal prefix-free machine V, Θ_V is a left-computable real which is weakly Chaitin random.* □

Theorem 6 results from each of Theorem 7 (i) and Theorem 8 (i) below by setting $T = 1$. Thus, we here omit the proof of Theorem 6. For completeness, however, we include a proof specific to Theorem 6 in Appendix C.

The works of Calude, et al. [1] and Kučera and Slaman [10] showed that, for every $\alpha \in (0,1)$, α is left-computable and weakly Chaitin random if and only if there exists an optimal prefix-free machine V such that $\alpha = \Omega_V$. Thus, it follows from Theorem 6 that, for every optimal prefix-free machine V, there exists an optimal prefix-free machine W such that $\Theta_V = \Omega_W$. However, it is open whether the following holds or not: For every optimal prefix-free machine W, there exists an optimal prefix-free machine V such that $\Omega_W = \Theta_V$.

In the subsequent two sections, we generalize Θ_V to two directions $\Theta_V(T)$ and $\overline{\Theta}_V(T)$ with a real $T > 0$. We see that the reals $\Theta_V(T)$ and $\overline{\Theta}_V(T)$ both have the same randomness properties as $Z_V(T)$ (i.e., the properties shown in Theorem 2 for $Z_V(T)$).

4 Generalization of Θ to $\Theta(T)$

Definition 5. *For any optimal prefix-free machine V and any real $T > 0$, $\Theta_V(T)$ is defined by*

$$\Theta_V(T) = \sum_{H_V(s)<|s|} 2^{-\frac{|s|}{T}}.$$ □

Thus, $\Theta_V(1) = \Theta_V$. If $0 < T \leq 1$, then $\Theta_V(T)$ converges and $0 < \Theta_V(T) < 1$, since $\Theta_V(T) \leq \Theta_V < 1$. The following theorem holds for $\Theta_V(T)$.

Theorem 7. *Let V be an optimal prefix-free machine, and let $T > 0$.*

(i) If T is computable and $0 < T \leq 1$, then $\Theta_V(T)$ is a left-computable real which is weakly Chaitin T-random.
(ii) If T is computable and $0 < T < 1$, then $\Theta_V(T)$ is strictly T-compressible.
(iii) If $1 < T$, then $\Theta_V(T)$ diverges to ∞. □

Proof. Let V be an optimal prefix-free machine. We first note that, for every $s \in \{0,1\}^*$, $H_V(s) < |s|$ if and only if there exists $p \in \operatorname{dom} V$ such that $V(p) = s$ and $|p| < |s|$. Thus, the set $\{\, s \in \{0,1\}^* \mid H_V(s) < |s| \,\}$ is r.e. and, obviously, infinite. Let $s_1, s_2, s_3, \ldots$ be a particular recursive enumeration of this set.

(i) Suppose that T is a computable real and $0 < T \leq 1$. Then, since $\Theta_V(T) = \sum_{i=1}^{\infty} 2^{-|s_i|/T}$, it is easy to see that $\Theta_V(T)$ is left-computable.

For each $n \in \mathbb{N}^+$, let α_n be the first n bits of the base-two expansion of $\Theta_V(T)$ with infinitely many ones. Then, since $0.\alpha_n < \Theta_V(T)$ for every $n \in \mathbb{N}^+$, $\sum_{i=1}^{\infty} 2^{-|s_i|} = \Theta_V(T)$, and T is computable, there exists a partial recursive function $\xi\colon \{0,1\}^* \to \mathbb{N}^+$ such that, for every $n \in \mathbb{N}^+$, $0.\alpha_n < \sum_{i=1}^{\xi(\alpha_n)} 2^{-|s_i|/T}$. It is then easy to see that $\sum_{i=\xi(\alpha_n)+1}^{\infty} 2^{-|s_i|/T} = \Theta_V(T) - \sum_{i=1}^{\xi(\alpha_n)} 2^{-|s_i|/T} < \Theta_V(T) - 0.\alpha_n < 2^{-n}$ for every $n \in \mathbb{N}^+$. It follows that, for all $i > \xi(\alpha_n)$, $2^{-|s_i|/T} < 2^{-n}$ and therefore $Tn < |s_i|$. Thus, given α_n, by calculating the set $\{\, s_i \mid i \leq \xi(\alpha_n) \;\&\; |s_i| = \lfloor Tn \rfloor \,\}$ and picking any one finite binary string of length $\lfloor Tn \rfloor$ which is not in this set, one can obtain $s \in \{0,1\}^{\lfloor Tn \rfloor}$ such that $|s| \leq H_V(s)$. This is possible since $\{\, s_i \mid i \leq \xi(\alpha_n) \;\&\; |s_i| = \lfloor Tn \rfloor \,\} = S_V(\lfloor Tn \rfloor) \subsetneqq \{0,1\}^{\lfloor Tn \rfloor}$, where the last proper inclusion is due to the first half of Theorem 5.

Hence, there exists a partial recursive function $\Psi\colon \{0,1\}^* \to \{0,1\}^*$ such that $\lfloor Tn \rfloor \leq H_V(\Psi(\alpha_n))$. Using the optimality of V, we then see that $Tn \leq H(\Psi(\alpha_n)) + O(1)$ for all $n \in \mathbb{N}^+$. On the other hand, it follows from (2) that there exists $c_\Psi \in \mathbb{N}$ such that $H(\Psi(\alpha_n)) \leq H(\alpha_n) + c_\Psi$. Therefore, we have

$$Tn \leq H(\alpha_n) + O(1) \tag{5}$$

for all $n \in \mathbb{N}^+$. This inequality implies that $\Theta_V(T)$ is not computable and therefore the base-two expansion of $\Theta_V(T)$ with infinitely many ones has infinitely many zeros also. Hence $\alpha_n = \Theta_V(T)\restriction_n$ for every $n \in \mathbb{N}^+$. It follows from (5) that $\Theta_V(T)$ is weakly Chaitin T-random.

(ii) Suppose that T is a computable real and $0 < T < 1$. Note that $\Theta_V(T) = \sum_{i=1}^{\infty} 2^{-|s_i|/T}$ and $\sum_{i=1}^{\infty} (2^{-|s_i|/T})^T = \sum_{i=1}^{\infty} 2^{-|s_i|} = \Theta_V < \infty$. Thus, since T is computable, it is easy to show that $\Theta_V(T)$ is a T-convergent left-computable real. It follows from Theorem 4 that $\Theta_V(T)$ is strictly T-compressible.

(iii) Suppose that $T > 1$. We then choose a particular computable real t satisfying $1 < t \leq T$. Let us first assume that $\Theta_V(t)$ converges. Based on an argument similar to the proof of Theorem 7 (i), it is easy to show that $\Theta_V(t)$ is

weakly Chaitin t-random, i.e., there exists $c \in \mathbb{N}$ such that $tn - c \leq H(\Theta_V(t)\restriction_n)$ for all $n \in \mathbb{N}^+$. It follows from (3) that $tn - c \leq n + o(n)$. Dividing by n and letting $n \to \infty$ we have $t \leq 1$, which contradicts the fact $t > 1$. Thus, $\Theta_V(t)$ diverges to ∞. By noting $\Theta_V(t) \leq \Theta_V(T)$ we see that $\Theta_V(T)$ diverges to ∞. □

5 Generalization of Θ to $\overline{\Theta}(T)$

Definition 6. *For any optimal prefix-free machine V and any real $T > 0$, $\overline{\Theta}_V(T)$ is defined by*

$$\overline{\Theta}_V(T) = \sum_{H_V(s)<T|s|} 2^{-|s|},$$

where the sum is over all $s \in \{0,1\}^*$ such that $H_V(s) < T\,|s|$. □

Thus, $\overline{\Theta}_V(1) = \Theta_V$. For each optimal prefix-free machine V and each real T with $0 < T \leq 1$, we see that

$$\overline{\Theta}_V(T) < \sum_{H_V(s)<T|s|} 2^{-\frac{H_V(s)}{T}} \leq \sum_{s\in\{0,1\}^*} 2^{-\frac{H_V(s)}{T}} \leq \sum_{p\in\mathrm{dom}\,V} 2^{-\frac{|p|}{T}} = Z_V(T).$$

Thus, $\overline{\Theta}_V(T)$ converges and $0 < \overline{\Theta}_V(T) < Z_V(T)$ for every optimal prefix-free machine V and every real T with $0 < T \leq 1$. We define $S_{V,T}(n) = \{\, s \in \{0,1\}^* \mid |s| = n \;\&\; H_V(s) < Tn \,\}$ for each optimal prefix-free machine V, each $T \in (0,1]$, and each $n \in \mathbb{N}$. It follows from Theorem 5 that $S_{V,T}(n) \subset S_V(n) \subsetneqq \{0,1\}^n$ for every optimal prefix-free machine V, every $T \in (0,1]$, and every $n \in \mathbb{N}$. The following theorem holds for $\overline{\Theta}_V(T)$.

Theorem 8. *Let V be an optimal prefix-free machine, and let $T > 0$.*

(i) If T is left-computable and $0 < T \leq 1$, then $\overline{\Theta}_V(T)$ is a left-computable real which is weakly Chaitin T-random.
(ii) If T is computable and $0 < T < 1$, then $\overline{\Theta}_V(T)$ is strictly T-compressible.
(iii) If $1 < T$, then $\overline{\Theta}_V(T)$ diverges to ∞. □

Proof. Let V be an optimal prefix-free machine.

(i) Suppose that T is a left-computable real and $0 < T \leq 1$. We first note that, for every $s \in \{0,1\}^*$, $H_V(s) < T\,|s|$ if and only if there exists $p \in \mathrm{dom}\,V$ such that $V(p) = s$ and $|p| < T\,|s|$. Thus, since T is left-computable, the set $\{\, s \in \{0,1\}^* \mid H_V(s) < T\,|s| \,\}$ is r.e. and, obviously, infinite. Let $s_1, s_2, s_3, \ldots$ be a particular recursive enumeration of this set. Then, since $\overline{\Theta}_V(T) = \sum_{i=1}^{\infty} 2^{-|s_i|}$, it is easy to see that $\overline{\Theta}_V(T)$ is left-computable.

For each $n \in \mathbb{N}^+$, let α_n be the first n bits of the base-two expansion of $\overline{\Theta}_V(T)$ with infinitely many ones. Then, since $0.\alpha_n < \overline{\Theta}_V(T)$ for every $n \in \mathbb{N}^+$ and $\sum_{i=1}^{\infty} 2^{-|s_i|} = \overline{\Theta}_V(T)$, there exists a partial recursive function $\xi\colon \{0,1\}^* \to \mathbb{N}^+$ such that, for every $n \in \mathbb{N}^+$, $0.\alpha_n < \sum_{i=1}^{\xi(\alpha_n)} 2^{-|s_i|}$. It is then easy to see that $\sum_{i=\xi(\alpha_n)+1}^{\infty} 2^{-|s_i|} = \overline{\Theta}_V(T) - \sum_{i=1}^{\xi(\alpha_n)} 2^{-|s_i|} < \overline{\Theta}_V(T) - 0.\alpha_n < 2^{-n}$ for

every $n \in \mathbb{N}^+$. It follows that, for all $i > \xi(\alpha_n)$, $2^{-|s_i|} < 2^{-n}$ and therefore $n < |s_i|$. Thus, given α_n, by calculating the set $\{\, s_i \mid i \leq \xi(\alpha_n) \;\&\; |s_i| = n, \}$ and picking any one finite binary string of length n which is not in this set, one can obtain $s \in \{0,1\}^n$ such that $T\,|s| \leq H_V(s)$. This is possible since $\{\, s_i \mid i \leq \xi(\alpha_n) \;\&\; |s_i| = n \,\} = S_{V,T}(n) \subsetneqq \{0,1\}^n$.

Hence, there exists a partial recursive function $\Psi\colon \{0,1\}^* \to \{0,1\}^*$ such that $Tn \leq H_V(\Psi(\alpha_n))$. Using the optimality of V, we then see that $Tn \leq H(\Psi(\alpha_n)) + O(1)$ for all $n \in \mathbb{N}^+$. On the other hand, it follows from (2) that there exists $c_\Psi \in \mathbb{N}$ such that $H(\Psi(\alpha_n)) \leq H(\alpha_n) + c_\Psi$. Therefore, we have

$$Tn \leq H(\alpha_n) + O(1) \tag{6}$$

for all $n \in \mathbb{N}^+$. This inequality implies that $\overline{\Theta}_V(T)$ is not computable and therefore the base-two expansion of $\overline{\Theta}_V(T)$ with infinitely many ones has infinitely many zeros also. Hence $\alpha_n = \overline{\Theta}_V(T)\restriction_n$ for every $n \in \mathbb{N}^+$. It follows from (6) that $\overline{\Theta}_V(T)$ is weakly Chaitin T-random.

(ii) Suppose that T is a computable real and $0 < T < 1$. Note that

$$\begin{aligned}\sum_{H_V(s)<T|s|} (2^{-|s|})^T = \sum_{H_V(s)<T|s|} 2^{-T|s|} &< \sum_{H_V(s)<T|s|} 2^{-H_V(s)} \\ &\leq \sum_{s\in\{0,1\}^*} 2^{-H_V(s)} \leq \sum_{p\in\operatorname{dom} V} 2^{-|p|} = \Omega_V < \infty.\end{aligned}$$

Thus, since T is computable, it is easy to show that $\overline{\Theta}_V(T)$ is a T-convergent left-computable real. It follows from Theorem 4 that $\overline{\Theta}_V(T)$ is strictly T-compressible.

(iii) Suppose that $T > 1$. Using (3), it is easy to show that there exists $n_0 \in \mathbb{N}$ such that, for every $s \in \{0,1\}^*$, if $|s| \geq n_0$ then $H_V(s) < T\,|s|$. Thus, obviously, $\overline{\Theta}_V(T)$ diverges to ∞. □

6 Fixed Point Theorem on Partial Randomness by $\Theta_V(T)$

In this section, we prove the following form of fixed point theorem on partial randomness, which is based on the computability of $\Theta_V(T)$. Note that this theorem has the same form as Theorem 3.

Theorem 9 (fixed point theorem on partial randomness by $\Theta_V(T)$). *Let V be an optimal prefix-free machine. For every $T \in (0,1)$, if $\Theta_V(T)$ is computable, then T is weakly Chaitin T-random and T-compressible.* □

Let V be an arbitrary optimal prefix-free machine in what follows. Theorem 9 follows immediately from Theorem 10, Theorem 11, and Theorem 12 below, as well as from Theorem 1 (i). Let $s_1, s_2, s_3, \ldots$ be a particular recursive enumeration of the infinite r.e. set $\{\, s \in \{0,1\}^* \mid H_V(s) < |s| \,\}$. For each $k \in \mathbb{N}^+$ and each real $x > 0$, we define $Z_k(x)$ as $\sum_{i=1}^{k} 2^{-|s_i|/x}$. Note then that $\lim_{k\to\infty} Z_k(x) = \Theta_V(x)$ for every $x \in (0,1]$.

Theorem 10. *For every $T \in (0,1)$, if $\Theta_V(T)$ is right-computable then T is weakly Chaitin T-random.*

Proof. First, we define $W_k(x)$ as $\sum_{i=1}^{k} |s_i|\, 2^{-|s_i|/x}$ for each $k \in \mathbb{N}^+$ and each real $x > 0$. We show that, for each $x \in (0,1)$, $W_k(x)$ converges as $k \to \infty$. Let x be an arbitrary real with $x \in (0,1)$. Since $x < 1$, there is $l_0 \in \mathbb{N}^+$ such that $(\log_2 l)/l \leq 1/x - 1$ for all $l \geq l_0$. Then there is $k_0 \in \mathbb{N}^+$ such that $|s_i| \geq l_0$ for all $i > k_0$. Thus, we see that, for each $i > k_0$,

$$|s_i|\, 2^{-\frac{|s_i|}{x}} = 2^{-(\frac{1}{x} - \frac{\log_2 |s_i|}{|s_i|})|s_i|} \leq 2^{-|s_i|}.$$

Hence, for each $k > k_0$, $W_k(x) - W_{k_0}(x) = \sum_{i=k_0+1}^{k} |s_i|\, 2^{-|s_i|/x} \leq \sum_{i=k_0+1}^{k} 2^{-|s_i|} < \Theta_V$. Therefore, since $\{W_k(x)\}_k$ is an increasing sequence of reals bounded to the above, it converges as $k \to \infty$, as desired. For each $x \in (0,1)$, we define a positive real $W(x)$ as $\lim_{k\to\infty} W_k(x)$.

On the other hand, since $\Theta_V(T)$ is right-computable by the assumption, there exists a total recursive function $f\colon \mathbb{N}^+ \to \mathbb{Q}$ such that $\Theta_V(T) \leq f(m)$ for all $m \in \mathbb{N}^+$, and $\lim_{m\to\infty} f(m) = \Theta_V(T)$.

We choose a particular real t with $T < t < 1$. Then, for each $i \in \mathbb{N}^+$, using the mean value theorem we see that

$$2^{-\frac{|s_i|}{x}} - 2^{-\frac{|s_i|}{T}} < \frac{\ln 2}{T^2}\, |s_i|\, 2^{-\frac{|s_i|}{t}} (x - T)$$

for all $x \in (T,t)$. We then choose a particular $c \in \mathbb{N}$ with $W(t) \ln 2/T^2 \leq 2^c$. Here, the limit value $W(t)$ exists, since $0 < t < 1$. It follows that

$$Z_k(x) - Z_k(T) < 2^c (x - T) \tag{7}$$

for all $k \in \mathbb{N}^+$ and $x \in (T,t)$. We also choose a particular $n_0 \in \mathbb{N}^+$ such that $0.(T\restriction_n) + 2^{-n} < t$ for all $n \geq n_0$. Such n_0 exists since $T < t$ and $\lim_{n\to\infty} 0.(T\restriction_n) + 2^{-n} = T$. Since $T\restriction_n$ is the first n bits of the base-two expansion of T with infinitely many zeros, we then see that $T < 0.(T\restriction_n) + 2^{-n} < t$ for all $n \geq n_0$. In addition, we choose a particular $n_1 \in \mathbb{N}^+$ such that $(n-c)2^{-n} \leq 1$ for all $n \geq n_1$. For each $n \geq 1$, since $|T - 0.(T\restriction_n)| < 2^{-n}$, we see that that $|T(n-c) - 0.(T\restriction_n)(n-c)| < (n-c)2^{-n} \leq 1$. Hence, we have

$$\lfloor 0.(T\restriction_n)(n-c) \rfloor \leq T(n-c) \quad \& \quad T(n-c) - 2 \leq \lfloor 0.(T\restriction_n)(n-c) \rfloor \tag{8}$$

for every $n \geq n_1$. We define $n_2 = \max\{n_0, n_1, c+1\}$.

Now, given $T\restriction_n$ with $n \geq n_2$, one can find $k_0, m_0 \in \mathbb{N}^+$ such that $f(m_0) < Z_{k_0}(0.(T\restriction_n) + 2^{-n})$. This is possible from $Z(T) < Z(0.(T\restriction_n) + 2^{-n})$,

$$\lim_{k\to\infty} Z_k(0.(T\restriction_n) + 2^{-n}) = Z(0.(T\restriction_n) + 2^{-n}),$$

and the properties of f. It follows from $Z(T) \leq f(m_0)$ and (7) that

$$\sum_{i=k_0+1}^{\infty} 2^{-|s_i|/T} = Z(T) - Z_{k_0}(T) < Z_{k_0}(0.(T\restriction_n) + 2^{-n}) - Z_{k_0}(T) < 2^{c-n}.$$

Hence, for every $i > k_0$, $2^{-|s_i|/T} < 2^{c-n}$ and therefore $T(n-c) < |s_i|$. Thus, by calculating the set $\{\, s_i \mid i \leq k_0 \;\&\; |s_i| = \lfloor 0.(T\restriction_n)(n-c) \rfloor \,\}$ and picking any one finite binary string of length $\lfloor 0.(T\restriction_n)(n-c) \rfloor$ which is not in this set, one can obtain $s \in \{0,1\}^{\lfloor 0.(T\restriction_n)(n-c) \rfloor}$ such that $|s| \leq H_V(s)$. This is possible since $\{\, s_i \mid i \leq k_0 \;\&\; |s_i| = \lfloor 0.(T\restriction_n)(n-c) \rfloor, \} = S_V(\lfloor 0.(T\restriction_n)(n-c) \rfloor) \subsetneqq \{0,1\}^{\lfloor 0.(T\restriction_n)(n-c) \rfloor}$, where the first equality follows from the first inequality in (8) and the last proper inclusion is due to the first half of Theorem 5.

Hence, there exists a partial recursive function $\Psi\colon \{0,1\}^* \to \{0,1\}^*$ such that $\lfloor 0.(T\restriction_n)(n-c) \rfloor \leq H(\Psi(T\restriction_n))$ for all $n \geq n_2$. Using (2), there is $c_\Psi \in \mathbb{N}$ such that $H(\Psi(T\restriction_n)) \leq H(T\restriction_n) + c_\Psi$ for all $n \geq n_2$. Thus, it follows from the second inequality in (8) that $Tn - Tc - 2 - c_\Psi < H(T\restriction_n)$ for all $n \geq n_2$, which implies that T is weakly Chaitin T-random. □

Theorem 11. *For every $T \in (0,1)$, if $\Theta_V(T)$ is right-computable, then T is also right-computable.*

Proof. Since $\Theta_V(T)$ is right-computable, there exists a total recursive function $f\colon \mathbb{N}^+ \to \mathbb{Q}$ such that $\Theta_V(T) \leq f(m)$ for all $m \in \mathbb{N}^+$, and $\lim_{m\to\infty} f(m) = \Theta_V(T)$. Thus, since $\Theta_V(x)$ is an increasing function of $x \in (0,1]$, we see that, for every $x \in \mathbb{Q}$ with $0 < x < 1$, $T < x$ if and only if there are $m, k \in \mathbb{N}^+$ such that $f(m) < Z_k(x)$. It follows from Theorem 1 (ii) that T is right-computable. □

Theorem 12. *For every $T \in (0,1)$, if $\Theta_V(T)$ is left-computable and T is right-computable, then T is T-compressible.*

Proof. For each $i \in \mathbb{N}^+$, using the mean value theorem we see that

$$2^{-\frac{|s_1|}{t}} - 2^{-\frac{|s_1|}{T}} > (\ln 2)\,|s_1|\,2^{-\frac{|s_1|}{T}}(t-T)$$

for all $t \in (T,1)$. We choose a particular $c \in \mathbb{N}^+$ such that $(\ln 2)\,|s_1|\,2^{-\frac{|s_1|}{T}} \geq 2^{-c}$. Then, it follows that

$$Z_k(t) - Z_k(T) > 2^{-c}(t-T) \tag{9}$$

for all $k \in \mathbb{N}^+$ and $t \in (T,1)$.

Since T is a right-computable real with $T < 1$ by the assumption, there exists a total recursive function $f\colon \mathbb{N}^+ \to \mathbb{Q}$ such that $T < f(l) < 1$ for all $l \in \mathbb{N}^+$, and $\lim_{l\to\infty} f(l) = T$. On the other hand, since $\Theta_V(T)$ is left-computable by the assumption, there exists a total recursive function $g\colon \mathbb{N}^+ \to \mathbb{Q}$ such that $g(m) \leq \Theta_V(T)$ for all $m \in \mathbb{N}^+$, and $\lim_{m\to\infty} g(m) = \Theta_V(T)$. By Theorem 6, Θ_V is weakly Chaitin random and therefore $\Theta_V \notin \mathbb{Q}$. Thus, the base-two expansion of Θ_V is unique and contains infinitely many ones, and $0 < \Theta_V < 1$ in particular.

Given n and $\Theta_V\restriction_{\lceil Tn \rceil}$ (i.e., the first $\lceil Tn \rceil$ bits of the base-two expansion of Θ_V), one can find $k_0 \in \mathbb{N}^+$ such that $0.(\Theta_V\restriction_{\lceil Tn \rceil}) < \sum_{i=1}^{k_0} 2^{-|s_i|}$. This is possible since $0.(\Theta_V\restriction_{\lceil Tn \rceil}) < \Theta_V$ and $\lim_{k\to\infty} \sum_{i=1}^{k} 2^{-|s_i|} = \Theta_V$. It is then easy to see that $\sum_{i=k_0+1}^{\infty} 2^{-|s_i|} = \Theta_V - \sum_{i=1}^{k_0} 2^{-|s_i|} < 2^{-\lceil Tn \rceil} \leq 2^{-Tn}$. Using the inequality $a^d + b^d \leq (a+b)^d$ for any reals $a, b > 0$ and $d \geq 1$, it follows that

$$\Theta_V(T) - Z_{k_0}(T) = \sum_{i=k_0+1}^{\infty} 2^{-\frac{|s_i|}{T}} < 2^{-n}. \tag{10}$$

Note that $\lim_{l\to\infty} Z_{k_0}(f(l)) = Z_{k_0}(T)$. Thus, since $Z_{k_0}(T) < \Theta_V(T)$, one can then find $l_0, m_0 \in \mathbb{N}^+$ such that $Z_{k_0}(f(l_0)) < g(m_0)$. It follows from (10) and (9) that $2^{-n} > g(m_0) - Z_{k_0}(T) > Z_{k_0}(f(l_0)) - Z_{k_0}(T) > 2^{-c}(f(l_0) - T)$. Thus, $0 < f(l_0) - T < 2^{c-n}$. Let t_n be the first n bits of the base-two expansion of the rational number $f(l_0)$ with infinitely many zeros. Then, $|\, f(l_0) - 0.t_n \,| < 2^{-n}$. It follows from $|\, T - 0.(T\restriction_n) \,| < 2^{-n}$ that $|\, 0.(T\restriction_n) - 0.t_n \,| < (2^c + 2)2^{-n}$. Hence, $T\restriction_n = t_n$, $t_n \pm 1$, $t_n \pm 2$, $\ldots$, $t_n \pm (2^c + 1)$, where $T\restriction_n$ and t_n are regarded as a dyadic integer. Thus, there are still $2^{c+1} + 3$ possibilities of $T\restriction_n$, so that one needs only $c + 2$ bits more in order to determine $T\restriction_n$.

Thus, there exists a partial recursive function $\Phi\colon \mathbb{N}^+ \times \{0,1\}^* \times \{0,1\}^* \to \{0,1\}^*$ such that

$$\forall\, n \in \mathbb{N}^+ \quad \exists\, s \in \{0,1\}^* \quad |s| = c + 2 \ \ \&\ \ \Phi(n, \Theta_V\restriction_{\lceil Tn \rceil}, s) = T\restriction_n \,. \tag{11}$$

Let us consider a prefix-free machine D which satisfies the following two conditions (i) and (ii): (i) For each $p, q \in \mathrm{dom}\, U$ and $v, s \in \{0,1\}^*$, $pqvs \in \mathrm{dom}\, D$ if and only if $|v| = U(q)$ and $|s| = c + 2$. (ii) For each $p, q \in \mathrm{dom}\, U$ and $v, s \in \{0,1\}^*$ such that $|v| = U(q)$ and $|s| = c + 2$, $D(pqvs) = \Phi(U(p), v, s)$. It is easy to see that such a prefix-free machine D exists. For each $n \in \mathbb{N}^+$, note that $n = U(n^*)$ and $\left|\Theta_V\restriction_{\lceil Tn \rceil}\right| = U(\lceil Tn \rceil^*)$. Thus, it follows from (11) that there exists $s \in \{0,1\}^*$ with $|s| = c + 2$ such that $D(n^*\lceil Tn \rceil^* \Theta_V\restriction_{\lceil Tn \rceil} s) = \Phi(n, \Theta_V\restriction_{\lceil Tn \rceil}, s) = T\restriction_n$. Hence, $H_D(T\restriction_n) \leq |n^*| + |\lceil Tn \rceil^*| + \left|\Theta_V\restriction_{\lceil Tn \rceil}\right| + |s| = H(n) + H(\lceil Tn \rceil) + \lceil Tn \rceil + c + 2$. It follows from (3) that $H_D(T\restriction_n) \leq Tn + 2\log_2 n + 2\log_2\log_2 n + O(1)$ for all $n \in \mathbb{N}^+$. Using (1) we see that T is T-compressible. □

Acknowledgments. This work was supported by KAKENHI, Grant-in-Aid for Scientific Research (C) (20540134), by SCOPE from the Ministry of Internal Affairs and Communications of Japan, and by CREST from Japan Science and Technology Agency.

References

1. C. S. Calude, P. H. Hertling, B. Khoussainov, and Y. Wang, "Recursively enumerable reals and Chaitin Ω numbers," *Theoret. Comput. Sci*, vol. 255, pp. 125–149, 2001.
2. C. S. Calude, N. J. Hay, and F. C. Stephan, "Representation of left-computable ε-random reals," Research Report of CDMTCS, 365, May 2009. Available at: `http://www.cs.auckland.ac.nz/CDMTCS/researchreports/365cris.pdf`
3. C. S. Calude, L. Staiger, and S. A. Terwijn, "On partial randomness," *Annals of Pure and Applied Logic*, vol. 138, pp. 20–30, 2006.
4. C. S. Calude and M. A. Stay, "Natural halting probabilities, partial randomness, and zeta functions," *Inform. and Comput.*, vol. 204, pp. 1718–1739, 2006.
5. G. J. Chaitin, "A theory of program size formally identical to information theory," *J. Assoc. Comput. Mach.*, vol. 22, pp. 329–340, 1975.
6. G. J. Chaitin, "Algorithmic entropy of sets," *Computers & Mathematics with Applications*, vol. 2, pp. 233–245, 1976.

7. G. J. Chaitin, *Algorithmic Information Theory*. Cambridge University Press, Cambridge, 1987.
8. R. G. Downey and D. R. Hirschfeldt, *Algorithmic Randomness and Complexity*. Springer-Verlag, To appear.
9. P. Gács, "On the symmetry of algorithmic information," *Soviet Math. Dokl.*, vol. 15, pp. 1477–1480, 1974; correction, ibid. vol. 15, pp. 1480, 1974.
10. A. Kučera and T. A. Slaman, "Randomness and recursive enumerability," *SIAM J. Comput.*, vol. 31, No. 1, pp. 199–211, 2001.
11. L. A. Levin, "Laws of information conservation (non-growth) and aspects of the foundations of probability theory," *Problems of Inform. Transmission*, vol. 10, pp. 206–210, 1974.
12. J. Reimann and F. Stephan, On hierarchies of randomness tests. Proceedings of the 9th Asian Logic Conference, World Scientific Publishing, August 16-19, 2005, Novosibirsk, Russia.
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. K. Tadaki, Algorithmic information theory and fractal sets. Proceedings of 1999 Workshop on Information-Based Induction Sciences (IBIS'99), pp. 105–110, August 26-27, 1999, Syuzenji, Shizuoka, Japan. In Japanese.
15. K. Tadaki, "A generalization of Chaitin's halting probability Ω and halting self-similar sets," *Hokkaido Math. J.*, vol. 31, pp. 219–253, 2002.
16. K. Tadaki, A statistical mechanical interpretation of algorithmic information theory. Local Proceedings of Computability in Europe 2008 (CiE 2008), pp. 425–434, June 15-20, 2008, University of Athens, Greece. Electronic Version Available: `http://www.cs.swan.ac.uk/cie08/cie2008-local.pdf`
17. K. Tadaki, Partial randomness and dimension of recursively enumerable reals. Proceedings of the 34th International Symposium on Mathematical Foundations of Computer Science (MFCS 2009), Lecture Notes in Computer Science, Springer-Verlag, Vol.5734, pp.687–699, August 24-28, 2009, Novy Smokovec, High Tatras, Slovakia. An Earlier Full Version Available: `http://arxiv.org/abs/0805.2691v1`
18. K. Tadaki, Fixed points on partial randomness. Proceedings of the 6th Workshop on Fixed Points in Computer Science (FICS 2009), pp. 100–107, September 12-13, 2009, Coimbra, Portugal. Electronic Version Available: `http://cs.ioc.ee/fics09/fics09proc.pdf`
19. K. Tadaki, One-wayness and two-wayness in algorithmic randomness. Submitted to the 35th International Symposium on Mathematical Foundations of Computer Science (MFCS 2010), Lecture Notes in Computer Science, Springer-Verlag, August 23-27, 2010, Brno, Czech Republic.
20. A. K. Zvonkin and L. A. Levin, "The complexity of finite objects and the development of the concepts of information and randomness by means of the theory of algorithms," *Russian Math. Surveys*, vol. 25, no. 6, pp. 83–124, 1970.

A The proof of Theorem 4

For completeness, we here prove Theorem 4 using the following two theorems.

Theorem 13 (Tadaki [17]). *Let T be a computable real with $0 < T \leq 1$, and let α be a left-computable real. Then the following conditions are equivalent:*

(i) The real α is weakly Chaitin T-random.
(ii) For every T-convergent left-computable real β there exists $d \in \mathbb{N}$ such that, for all $n \in \mathbb{N}^+$, $H(\beta\restriction_n) \leq H(\alpha\restriction_n) + d$. □

Theorem 14 (Calude, Hay, and Stephan [2]). *Let T be a computable real with $0 < T < 1$. Then there exist a left-computable real α and $d \in \mathbb{N}$ such that $|H(\alpha\restriction_n) - Tn| \leq d$ for all $n \in \mathbb{N}^+$, i.e., the real α is weakly Chaitin T-random and strictly T-compressible.* □

Theorem 13 is the equivalence between the conditions (i) and (iv) in Theorem 8 of Tadaki [17]. On the other hand, Theorem 14 is Theorem 9 of Calude, Hay, and Stephan [2]. The proof of Theorem 4 is then given as follows.

Proof (of Theorem 4). Let T be a computable real with $0 < T < 1$, and let α be a left-computable real. Assume that α is T-convergent. Using Theorem 14 we see that there exist a left-computable real β such that β is weakly Chaitin T-random and

$$H(\beta\restriction_n) \leq Tn + O(1) \tag{12}$$

for all $n \in \mathbb{N}^+$. Since β is weakly Chaitin T-random, using the implication (i) $\Rightarrow$ (iv) of Theorem 13 we see that, for every T-convergent left-computable real γ, there exists $d \in \mathbb{N}$ such that, for all $n \in \mathbb{N}^+$, $H(\gamma\restriction_n) \leq H(\beta\restriction_n) + d$. Since α is a T-convergent left-computable real, it follows that $H(\alpha\restriction_n) \leq H(\beta\restriction_n) + d$ for all $n \in \mathbb{N}^+$. Thus, using (12) we see that $H(\alpha\restriction_n) \leq Tn + O(1)$ for all $n \in \mathbb{N}^+$, which implies that α is strictly T-compressible. □

B The proof of Theorem 5

We here prove Theorem 5. For that purpose, we need the notion of universal probability.

The program-size complexity $H(s)$ is originally defined using the concept of program-size, as stated in Subsection 2.1. However, it is possible to define $H(s)$ without referring to such a concept, i.e., as in the following, we first introduce a *universal probability* m, and then define $H(s)$ as $-\log_2 m(s)$. A universal probability is defined as follows [20].

Definition 7 (universal probability). *A function $r\colon \{0,1\}^* \to [0,1]$ is called a lower-computable semi-measure if $\sum_{s\in\{0,1\}^*} r(s) \leq 1$ and the set $\{(a,s) \in \mathbb{Q} \times \{0,1\}^* \mid a < r(s)\}$ is r.e. We say that a lower-computable semi-measure m is a universal probability if for every lower-computable semi-measure r, there exists $c \in \mathbb{N}^+$ such that, for all $s \in \{0,1\}^*$, $r(s) \leq cm(s)$.* □

The following theorem can be then shown (see e.g. Theorem 3.4 of Chaitin [5] for its proof).

Theorem 15. *For every optimal prefix-free machine V, the function $2^{-H_V(s)}$ of s is a universal probability.* □

By Theorem 15, we see that $H(s) = -\log_2 m(s) + O(1)$ for every universal probability m. Thus it is possible to define $H(s)$ as $-\log_2 m(s)$ with a particular universal probability m instead of as $H_U(s)$. Note that the difference up to an additive constant is nonessential to algorithmic information theory.

Now the proof of Theorem 5 is given as follows.

Proof (of Theorem 5). Let V be an optimal prefix-free machine. First, for each $n \in \mathbb{N}$, it is easy to show that $\#S_V(n) \leq 2^n - 1$ by counting the number of binary strings of length less than n. Thus we have $S_V(n) \subsetneqq \{0,1\}^n$ for every $n \in \mathbb{N}$.

Next, we show that there exists $d_1 \in \mathbb{N}$ such that $\#S_V(n) \leq 2^{n-H(n)+d_1}$ for all $n \in \mathbb{N}$. For that purpose, we define a function $f\colon \mathbb{N} \to [0,\infty)$ by $f(n) = \#S_V(n)2^{-n}$. It follows that $\sum_{n=0}^{\infty} f(n) = \Omega_V < 1$. On the other hand, note that, for every $n \in \mathbb{N}$ and every $s \in \{0,1\}^n$, $H_V(s) < n$ if and only if there exists $p \in \mathrm{dom}\, V$ such that $V(p) = s$ and $|p| < n$. Based on these facts, we see that f is a lower-computable semi-measure. Recall here that we identify $\{0,1\}^*$ with $\mathbb{N}$. It follows from Theorem 15 that there exists $d_1 \in \mathbb{N}$ such that $f(n) \leq 2^{d_1}2^{-H(n)}$ for all $n \in \mathbb{N}$, which implies that $\#S_V(n) \leq 2^{n-H(n)+d_1}$ for all $n \in \mathbb{N}$, as desired.

Finally, we show that there exists $d_2 \in \mathbb{N}$ such that $2^{n-H(n)-d_2} \leq \#S_V(n)$ for all sufficiently large $n \in \mathbb{N}$. Let us consider a prefix-free machine C which satisfies the following two conditions (i) and (ii): (i) For each $p, q \in \mathrm{dom}\, U$ and $s \in \{0,1\}^*$, $pqs \in \mathrm{dom}\, C$ if and only if $|pqs| = U(p) - U(q)$. (ii) For each $p, q \in \mathrm{dom}\, U$ and $s \in \{0,1\}^*$ such that $|pqs| = U(p) - U(q)$, $C(pqs) = pq0^{U(q)}s$. Here $U(p)$ and $U(q)$ are regarded as a natural number. It is easy to see that such a prefix-free machine C exists. It follows from (1) that there exists $d \in \mathbb{N}$ such that, for every $s \in \{0,1\}^*$,

$$H(s) \leq H_C(s) + d. \tag{13}$$

For each $n \in \mathbb{N}$ and $s \in \{0,1\}^*$, if $|s| = n-d-H(n)-H(d)$, then $|n^*d^*s| = n-d = U(n^*) - U(d^*)$ and therefore $C(n^*d^*s) = n^*d^*0^ds$ and $\left|n^*d^*0^ds\right| = n$. Thus, for each $n \in \mathbb{N}$, if $n - d - H(n) - H(d) \geq 0$ then $\#\{\, s \mid |s| = n \,\&\, H_C(s) \leq n-d \,\} \geq 2^{n-H(n)-d-H(d)}$. It follows from (13) that, for each $n \in \mathbb{N}$, if $n-H(n)-d-H(d) \geq 0$ then $2^{n-H(n)-d-H(d)} \leq \#S_V(n)$. Since $n - H(n) - d - H(d) \geq 0$ holds for all sufficiently large $n \in \mathbb{N}$, the result follows. □

C The proof of Theorem 6

Proof (of Theorem 6). Let V be an optimal prefix-free machine. We first note that, for every $s \in \{0,1\}^*$, $H_V(s) < |s|$ if and only if there exists $p \in \mathrm{dom}\, V$ such that $V(p) = s$ and $|p| < |s|$. Thus, the set $\{\, s \in \{0,1\}^* \mid H_V(s) < |s| \,\}$ is r.e. and, obviously, infinite. Let $s_1, s_2, s_3, \ldots$ be a particular recursive enumeration of this set. Then, since $\Omega_V = \sum_{i=1}^{\infty} 2^{-|s_i|}$, it is easy to see that Ω_V is left-computable.

For each $n \in \mathbb{N}^+$, let α_n be the first n bits of the base-two expansion of Ω_V with infinitely many ones. Then, since $0.\alpha_n < \Omega_V$ for every $n \in \mathbb{N}^+$ and

$\sum_{i=1}^{\infty} 2^{-|s_i|} = \Theta_V$, there exists a partial recursive function $\xi\colon \{0,1\}^* \to \mathbb{N}^+$ such that, for every $n \in \mathbb{N}^+$,

$$0.\alpha_n < \sum_{i=1}^{\xi(\alpha_n)} 2^{-|s_i|}.$$

It is then easy to see that

$$\sum_{i=\xi(\alpha_n)+1}^{\infty} 2^{-|s_i|} = \Theta_V - \sum_{i=1}^{\xi(\alpha_n)} 2^{-|s_i|} < \Theta_V - 0.\alpha_n < 2^{-n}$$

for every $n \in \mathbb{N}^+$. It follows that, for all $i > \xi(\alpha_n)$, $2^{-|s_i|} < 2^{-n}$ and therefore $n < |s_i|$. Thus, given α_n, by calculating the set $\{\, s_i \mid i \leq \xi(\alpha_n) \;\&\; |s_i| = n \,\}$ and picking any one finite binary string of length n which is not in this set, one can obtain $s \in \{0,1\}^n$ such that $|s| \leq H_V(s)$. This is possible since $\{\, s_i \mid i \leq \xi(\alpha_n) \;\&\; |s_i| = n \,\} = S_V(n) \subsetneqq \{0,1\}^n$, where the last proper inclusion is due to the first half of Theorem 5.

Hence, there exists a partial recursive function $\Psi\colon \{0,1\}^* \to \{0,1\}^*$ such that $n \leq H_V(\Psi(\alpha_n))$. Using the optimality of V, we then see that $n \leq H(\Psi(\alpha_n)) + O(1)$ for all $n \in \mathbb{N}^+$. On the other hand, it follows from (2) that there exists $c_\Psi \in \mathbb{N}$ such that $H(\Psi(\alpha_n)) \leq H(\alpha_n) + c_\Psi$. Therefore, we have

$$n \leq H(\alpha_n) + O(1) \tag{14}$$

for all $n \in \mathbb{N}^+$. This inequality implies that Θ_V is not computable and therefore the base-two expansion of Θ_V with infinitely many ones has infinitely many zeros also. Hence $\alpha_n = \Theta_V{\restriction}_n$ for every $n \in \mathbb{N}^+$. It follows from (14) that Θ_V is weakly Chaitin random. □