数理解析研究所講究録
第1691巻 2010年 120-126

Chaitin Ω and halting problems II

中央大学 研究開発機構　只木孝太郎 (Kohtaro Tadaki)*
Research and Development Initiative, Chuo University

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, $H(s)$ is thought to represent the amount of randomness of a finite binary string s. 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 [2] Chaitin introduced the halting probability Ω_U as a concrete example of random real. His Ω_U is defined as the probability that the optimal prefix-free machine U halts, and is shown to be random, based on the following fact:

Fact 1 (Chaitin [2]). *The first n bits of the base-two expansion of Ω_U solve the halting problem of U for inputs of length at most n.* □

In our former work [7], we investigated the relationship between the base-two expansion of Ω_U and the halting problem of U further. On the one hand, we considered the following converse problem of Fact 1 in a general setting. Let V and W be arbitrary optimal prefix-free machines.

Problem 1. *Find a succinct equivalent characterization of a total recursive function $f\colon \mathbf{N}^+ \to \mathbf{N}$ which satisfies the condition: For all $n \in \mathbf{N}^+$, if n and the list of all halting inputs for V of length at most n are given, then the first $n - f(n) - O(1)$ bits of the base-two expansion of Ω_W can be calculated.* □

Theorem 3.1 below is one of the main results of the work [7]. It gives to Problem 1 a solution that the total recursive function f must satisfy $\sum_{n=1}^{\infty} 2^{-f(n)} < \infty$, which is the Kraft inequality in essence. Note that the condition $\sum_{n=1}^{\infty} 2^{-f(n)} < \infty$ holds for $f(n) = \lfloor (1+\varepsilon) \log_2 n \rfloor$ with an arbitrary computable real $\varepsilon > 0$, while this condition does not hold for $f(n) = \lfloor \log_2 n \rfloor$. On the other hand, it is also important to consider whether the bound n on the length of halting inputs given in Fact 1 is tight or not. In the work [7], we considered this problem as well in the following form:

Problem 2. *Find a succinct equivalent characterization of a total recursive function $f\colon \mathbf{N}^+ \to \mathbf{N}$ which satisfies the condition: For all $n \in \mathbf{N}^+$, if n and the first n bits of the base-two expansion of Ω_W are given, then the list of all halting inputs for V of length at most $n + f(n) - O(1)$ can be calculated.* □

Theorem 3.2 below, which is also one of the main results of the work [7], gives to Problem 2 a solution that the total recursive function f must be bounded to the above. Thus, we see that the bound n on the length of halting inputs given in Fact 1 is tight up to an additive constant.

It is well known that the base-two expansion of Ω_U and the halting problem of U are Turing equivalent. The results in the work [7] can be thought of as an elaboration of the Turing equivalence. Namely, in the work [7], we studied the relationship between the base-two expansion of Ω_U and the halting problem of U using a more rigorous and insightful notion than the notion of Turing equivalence. As a result, we revealed computational one-wayness between the base-two expansion of Ω_U and the halting problem of U in the form of Theorems 3.1 and 3.2 together.

In this paper, based on the same setting, we investigate the relationship between the base-two expansion of $Z_U(T)$ and the halting problem of U. Here, $Z_U(T)$ is the partition function at temperature $T \in (0, 1]$ [5]. It is one of the thermodynamic quantities in the statistical mechanical interpretation of AIT [6], and results in Ω_U in the case of $T = 1$, i.e., $Z_U(1) = \Omega_U$. In the case where T is a computable real with $0 < T < 1$, we reveal computational equivalence, i.e., computational two-wayness, between

*E-mail: tadaki@kc.chuo-u.ac.jp, Website: http://www2.odn.ne.jp/tadaki/

the base-two expansion of $Z_U(T)$ and the halting problem of U. This contrasts the computational one-wayness between the base-two expansion of Ω_U and the halting problem of U.

2 Preliminaries

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

$\{0,1\}^* = \{\lambda, 0, 1, 00, 01, 10, 11, 000, \dots\}$ 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 subset S of $\{0,1\}^*$ and any $n \in \mathbb{Z}$, we denote by $S\restriction_n$ the set $\{s \in S \mid |s| \leq n\}$. Note that $S\restriction_n = \emptyset$ for every subset S of $\{0,1\}^*$ and every negative integer $n \in \mathbb{Z}$. For any function f, the domain of definition of f is denoted by $\mathrm{dom}\, f$. 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 $\alpha = 5/8$, $\alpha\restriction_6 = 101000$. On the other hand, for any non-positive integer $n \in \mathbb{Z}$, we set $\alpha\restriction_n = \lambda$.

A real α is called *r.e.* if there exists a computable, increasing sequence of rationals which converges to α. An r.e. real is also called a *left-computable* real. On the other hand, a real α is called *right-computable* if $-\alpha$ is left-computable. We say that a real α is *computable* if there exists a computable sequence $\{a_n\}_{n\in\mathbb{N}}$ of rationals such that $|\alpha - a_n| < 2^{-n}$ for all $n \in \mathbb{N}$. It is then easy to see that, for every $\alpha \in \mathbb{R}$, α is computable if and only if α is both left-computable and right-computable.

2.1 Algorithmic Information Theory

In the following we concisely review some definitions and results of AIT [2, 3]. A *prefix-free machine* is a partial recursive function $C\colon \{0,1\}^* \to \{0,1\}^*$ such that $\mathrm{dom}\, C$ 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 $p \in \mathrm{dom}\, C$, then there is $q \in \mathrm{dom}\, U$ for which $U(q) = C(p)$ and $|q| \leq |p| + d$. 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 or the *Kolmogorov complexity* of s. It follows that for every prefix-free machine C there exists $d \in \mathbb{N}$ such that, for every $s \in \{0,1\}^*$,

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

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 $s \in \mathrm{dom}\, \Psi$,

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

For any $s, t \in \{0,1\}^*$, we define $H(s,t)$ as $H(b(s,t))$, where $b\colon \{0,1\}^* \times \{0,1\}^* \to \{0,1\}^*$ is a particular bijective total recursive function.

For any optimal prefix-free machine V, *Chaitin's halting probability* Ω_V of V is defined as $\sum_{p\in\mathrm{dom}\, V} 2^{-|p|}$. The real Ω_V is also called *Chaitin* Ω *number*. 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 $n \in \mathbb{N}^+$ [2, 3]. Based on Fact 1, Chaitin [2] showed that Ω_V is weakly Chaitin random for every optimal prefix-free machine V.

2.2 Partial randomness

In the work [5], 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 (e.g. [4]), can be characterized by a real T with $0 < T \leq 1$ as follows.

Definition 2.1 (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 $d \in \mathbb{N}$ such that $Tn - d \leq H(\alpha\restriction_n)$ for all $n \in \mathbb{N}^+$.* □

Definition 2.2 (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 $H(\alpha\restriction_n) \leq Tn + d$ for all $n \in \mathbb{N}^+$.* □

Note that, in the case where $T = 1$, the weak Chaitin T-randomness results in weak Chaitin randomness. If a real 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. Note, however, that the converse does not hold. Thus, the notion of partial randomness is a stronger representation of compression rate.

In the work [5], we generalized Chaitin Ω number to $Z(T)$ as follows.[1] For each optimal prefix-free machine V and each real $T > 0$, the *partition function* $Z_V(T)$ of V at temperature T is defined as $\sum_{p\in\mathrm{dom}\, V} 2^{-|p|/T}$. 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 2.3 (Tadaki [5]). *Let V be an optimal prefix-free machine and let $T \in \mathbb{R}$. If $0 < T \leq 1$ and T is computable, then $Z_V(T)$ is an r.e. real which is weakly Chaitin T-random and T-compressible.* □

An r.e. real has a special property on partial randomness, as shown in Theorem 2.5 below. For any r.e. reals α and β, we say that α *dominates* β if there are computable, increasing sequences $\{a_n\}$ and $\{b_n\}$ of rationals and $c \in \mathbb{N}^+$ such that $\lim_{n\to\infty} a_n = \alpha$, $\lim_{n\to\infty} b_n = \beta$, and $c(\alpha - a_n) \geq \beta - b_n$ for all $n \in \mathbb{N}$.

Definition 2.4 (T-convergence and $\Omega(T)$-likeness, Tadaki [8]). *Let $T \in (0,1]$. An increasing sequence $\{a_n\}$ of reals is called T-convergent if $\sum_{n=0}^{\infty}(a_{n+1} - a_n)^T < \infty$. An r.e. real α is called T-convergent if there exists a T-convergent computable, increasing sequence of rationals which converges to α. An r.e. real α is called $\Omega(T)$-like if it dominates all T-convergent r.e. reals.* □

Theorem 2.5 (equivalent characterizations of partial randomness for an r.e. real, Tadaki [8]). *Let $T \in (0,1]$, and let α be an r.e. real. Then the following three conditions are equivalent: (i) The real α is weakly Chaitin T-random. (ii) The real α is $\Omega(T)$-like. (iii) For every T-convergent r.e. real β there exists $d \in \mathbb{N}$ such that, for all $n \in \mathbb{N}^+$, $H(\beta\restriction_n) \leq H(\alpha\restriction_n) + d$.* □

3 The Former Result: Computational One-Wayness

Theorem 3.1 (Tadaki [7]). *Let V and W be optimal prefix-free machines, and let $f\colon \mathbb{N}^+ \to \mathbb{N}$ be a total recursive function. Then the following two conditions are equivalent:*

(i) There exist an oracle deterministic Turing machine M and $c \in \mathbb{N}$ such that, for all $n \in \mathbb{N}^+$, $M^{\mathrm{dom}\, V\restriction_n}(n) = \Omega_W\restriction_{n-f(n)-c}$.

(ii) $\sum_{n=1}^{\infty} 2^{-f(n)} < \infty$. □

Theorem 3.2 (Tadaki [7]). *Let V and W be optimal prefix-free machines, and let $f\colon \mathbb{N}^+ \to \mathbb{N}$ be a total recursive function. Then the following two conditions are equivalent:*

(i) There exist an oracle deterministic Turing machine M and $c \in \mathbb{N}$ such that, for all $n \in \mathbb{N}^+$, $M^{\{\Omega_W\restriction_n\}}(n) = \mathrm{dom}\, V\restriction_{n+f(n)-c}$, where the finite subset $\mathrm{dom}\, V\restriction_{n+f(n)-c}$ of $\{0,1\}^*$ is represented as a finite binary string in a certain format.

(ii) The function f is bounded to the above. □

[1] In [5], $Z(T)$ is denoted by Ω^T.

4 T-Convergent R.E. Reals

Let T be an arbitrary computable real with $0 < T \leq 1$ throughout the rest of the present paper. The parameter T plays a crucial role in the present paper.[2] In this section, we investigate the relation of the halting problems to T-convergent r.e. reals. In particular, Theorem 4.6 below is used to show the main result I in the next section. Recently, Calude, Hay, and Stephan [1] showed the existence of an r.e. real which is weakly Chaitin T-random and strictly T-compressible, in the case of $T < 1$, as follows.

Theorem 4.1 (Calude, Hay, and Stephan [1]). *Suppose that $T < 1$. Then there exist an r.e. real $\alpha \in (0,1)$ and $d \in \mathbb{N}$ such that, for all $n \in \mathbb{N}^+$, $|H(\alpha\restriction_n) - Tn| \leq d$.* □

We show that the same r.e. real α as in Theorem 4.1 has the following property.

Theorem 4.2. *Suppose that $T < 1$. Let V be an optimal prefix-free machine. Then there exist an r.e. real $\alpha \in (0,1)$, an oracle deterministic Turing machine M, and $c \in \mathbb{N}$ such that α is weakly Chaitin T-random and, for all $n \in \mathbb{N}^+$, $M^{\mathrm{dom}\, V\restriction_{\lceil Tn \rceil}}(n) = \alpha\restriction_{n-c}$.* □

Calude, et al. [1] uses Lemma 4.3 below to show Theorem 4.1. We also use it to show Theorem 4.2.

Lemma 4.3 (Reimann and Stephan [4] and Calude, Hay, and Stephan [1]). *Let V be an optimal prefix-free machine. Suppose that $T < 1$. Then there exists $c \in \mathbb{N}^+$ such that, for every $s \in \{0,1\}^*$, there exists $t \in \{0,1\}^c$ for which $H_V(st) \geq H_V(s) + Tc$.* □

Proof of Theorem 4.2. Suppose that $T < 1$. Let V be an optimal prefix-free machine. Then it follows from Lemma 4.3 that there exists $c \in \mathbb{N}^+$ such that, for every $s \in \{0,1\}^*$, there exists $t \in \{0,1\}^c$ for which

$$H_V(st) \geq H_V(s) + Tc. \tag{3}$$

For each prefix-free machine D and each $s \in \{0,1\}^*$, we denote by $S(D;s)$ the set $\{\, u \in \{0,1\}^{|s|+c} \mid s \text{ is a prefix of } u \;\&\; H_D(u) > T\,|u| \,\}$.

Now, we define a sequence $\{a_k\}_{k\in\mathbb{N}}$ of finite binary strings recursively on $k \in \mathbb{N}$ by $a_k := \lambda$ if $k = 0$ and $a_k := \min S(V; a_{k-1})$ otherwise. First note that a_0 is properly defined as λ and therefore satisfies $H_V(a_0) > T\,|a_0|$. For each $k \geq 1$, assume that $a_0, a_1, a_2, \ldots, a_{k-1}$ are properly defined. Then $H_V(a_{k-1}) > T\,|a_{k-1}|$ holds. It follow from (3) that there exists $t \in \{0,1\}^c$ for which $H_V(a_{k-1}t) \geq H_V(a_{k-1}) + Tc$, and therefore $a_{k-1}t \in \{0,1\}^{|a_{k-1}|+c}$ and $H_V(a_{k-1}t) \geq T\,|a_{k-1}t|$. Thus $S(V; a_{k-1}) \neq \emptyset$, and therefore a_k is properly defined. Hence, a_k is properly defined for every $k \in \mathbb{N}$. We thus see that, for every $k \in \mathbb{N}$, $a_k \in \{0,1\}^{ck}$, $H_V(a_k) > T\,|a_k|$, and a_k is a prefix of a_{k+1}. Therefore, it is easy to see that, for every $m \in \mathbb{N}^+$, there exists $k \in \mathbb{N}$ such that a_k contains m zeros. Thus, we can uniquely define a real $\alpha \in [0,1)$ by the condition that $\alpha\restriction_{ck} = a_k$ for all $k \in \mathbb{N}^+$. It follows that $H_V(\alpha\restriction_{ck}) > T\,|\alpha\restriction_{ck}|$ for all $k \in \mathbb{N}^+$. Note that there exists $d_0 \in \mathbb{N}$ such that, for every $s, t \in \{0,1\}^*$, if $|t| \leq c$ then $|H_V(st) - H_V(s)| \leq d_0$. Therefore, there exists $d_1 \in \mathbb{N}$ such that, for every $n \in \mathbb{N}^+$, $H_V(\alpha\restriction_n) > Tn - d_1$, which implies that α is weakly Chaitin T-random and therefore $\alpha \in (0,1)$.

Next, we show that there exists an oracle deterministic Turing machine M such that, for all $n \in \mathbb{N}^+$, $M^{\mathrm{dom}\, V\restriction_{\lceil Tn \rceil}}(n) = \alpha\restriction_{n-c}$. For each $k \in \mathbb{N}$, we denote by F_k the set $\{s \in \{0,1\}^* \mid H_V(s) \leq \lfloor Tck \rfloor\}$. It follows that

$$a_k = \min\{\, u \in \{0,1\}^{ck} \mid a_{k-1} \text{ is a prefix of } u \;\&\; u \notin F_k \,\} \tag{4}$$

for every $k \in \mathbb{N}^+$. By the following procedure, we see that such an oracle deterministic Turing machine M exists.

Given n and $\mathrm{dom}\, V\restriction_{\lceil Tn \rceil}$ with $n \geq c$, one first calculates the k_0 finite sets $F_1, F_2, \ldots, F_{k_0}$, where $k_0 = \lfloor n/c \rfloor$. This can be possible because $\mathrm{dom}\, V\restriction_{\lceil Tn \rceil}$ is available and $\lfloor Tck_0 \rfloor \leq \lceil Tn \rceil$. One then calculates $a_1, a_2, \ldots, a_{k_0}$ in this order one by one from $a_0 = \lambda$ based on the relation (4) and $F_1, F_2, \ldots, F_{k_0}$. Finally, one calculates $\alpha\restriction_{n-c}$ from a_{k_0} and outputs it. This is possible since $\alpha\restriction_{ck_0} = a_{k_0}$ and $n - c < ck_0$.

Finally, we show that α is an r.e. real. Let $p_1, p_2, p_3, \ldots$ be a particular recursive enumeration of the infinite r.e. set $\mathrm{dom}\, V$. For each $l \in \mathbb{N}^+$, we define a prefix-free machine $V^{(l)}$ by the following two conditions (i) and (ii): (i) $\mathrm{dom}\, V^{(l)} = \{p_1, p_2, \ldots, p_l\}$. (ii)$V^{(l)}(p) = V(p)$ for every $p \in \mathrm{dom}\, V^{(l)}$. It is easy to see that such prefix-free machines $V^{(1)}, V^{(2)}, V^{(3)}, \ldots$ exist. For each $l \in \mathbb{N}^+$ and each $s \in \{0,1\}^*$, note

[2] The parameter T corresponds to the notion of "temperature" in the statistical mechanical interpretation of AIT introduced by Tadaki [6].

that $H_{V^{(l)}}(s) \geq H_V(s)$ holds, where $H_{V^{(l)}}(s)$ may be ∞. For each $l \in \mathbb{N}$, we define a sequence $\{a_k^{(l)}\}_{k\in\mathbb{N}}$ of finite binary strings recursively on $k \in \mathbb{N}$ by $a_k^{(l)} := \lambda$ if $k = 0$ and $a_k^{(l)} := \min(S(V^{(l)}; a_{k-1}^{(l)}) \cup \{a_{k-1}^{(l)} 1^c\})$ otherwise. It follows that $a_k^{(l)}$ is properly defined for every $k \in \mathbb{N}$. Note, in particular, that $a_k^{(l)} \in \{0,1\}^{ck}$ and $a_k^{(l)}$ is a prefix of $a_{k+1}^{(l)}$ for every $k \in \mathbb{N}$.

Let $l \in \mathbb{N}^+$. We show that $a_k^{(l)} \leq a_k$ for every $k \in \mathbb{N}^+$. To see this, assume that $a_{k-1}^{(l)} = a_{k-1}$. Then, since $H_{V^{(l)}}(s) \geq H_V(s)$ holds for every $s \in \{0,1\}^*$, based on the constructions of $a_k^{(l)}$ and a_k from $a_{k-1}^{(l)}$ and a_{k-1}, respectively, we see that $a_k^{(l)} \leq a_k$. Thus, based on the constructions of $\{a_k^{(l)}\}_{k\in\mathbb{N}}$ and $\{a_k\}_{k\in\mathbb{N}}$ we see that $a_k^{(l)} \leq a_k$ for every $k \in \mathbb{N}^+$.

We define a sequence $\{r_k\}_{k\in\mathbb{N}}$ of rationals by $r_k = 0.a_k^{(k)}$. Obviously, $\{r_k\}_{k\in\mathbb{N}}$ is a computable sequence of rationals. Based on the result in the previous paragraph, we see that $r_k \leq \alpha$ for every $k \in \mathbb{N}^+$. Based on the constructions of prefix-free machines $V^{(1)}, V^{(2)}, V^{(3)}, \ldots$ from V, it is also easy to see that $\lim_{k\to\infty} r_k = \alpha$. Thus we see that α is an r.e. real. □

Note that, using Theorem 4.2 and Theorem 5.4 below, we can give to Theorem 4.1 a different proof from Calude, et al. [1].

Theorem 4.4. *Suppose that $T < 1$. For every r.e. real β, if β is T-convergent then β is strictly T-compressible.*

Proof. Suppose that $T < 1$. Let β be a T-convergent r.e. real. Using Theorem 4.1 we see that there exists an r.e. real α such that α is weakly Chaitin T-random and strictly T-compressible. Since α is weakly Chaitin T-random, using the implication (i) $\Rightarrow$ (iii) of Theorem 2.5 we see that, for every T-convergent r.e. real γ, there exists $d \in \mathbb{N}$ such that, for all $n \in \mathbb{N}^+$, $H(\gamma\restriction_n) \leq H(\alpha\restriction_n) + d$. Since β is a T-convergent r.e. real, it follows that $H(\beta\restriction_n) \leq H(\alpha\restriction_n) + O(1)$ for all $n \in \mathbb{N}^+$. Thus, since α is strictly T-compressible, β is also strictly T-compressible. □

Calude, et al. [1], in essence, showed the following result.

Theorem 4.5 (Calude, Hay, and Stephan [1]). *If a real β is weakly Chaitin T-random and strictly T-compressible, then there exists $d \geq 2$ such that a base-two expansion of β has neither a run of d consecutive zeros nor a run of d consecutive ones.* □

Theorem 4.6. *Suppose that $T < 1$. Let V be an optimal prefix-free machine. For every r.e. real β, if β is T-convergent and weakly Chaitin T-random, then there exist an oracle deterministic Turing machine M and $d \in \mathbb{N}$ such that, for all $n \in \mathbb{N}^+$, $M^{\mathrm{dom}\, V\restriction_{\lceil Tn\rceil}}(n) = \beta\restriction_{n-d}$.*

Proof. Suppose that $T < 1$. Let V be an optimal prefix-free machine. Then, by Theorem 4.2, there exist an r.e. real α, an oracle deterministic Turing machine M_0, and $d_0 \in \mathbb{N}$ such that α is weakly Chaitin T-random and, for all $n \in \mathbb{N}^+$, $M^{\mathrm{dom}\, V\restriction_{\lceil Tn\rceil}}(n) = \alpha\restriction_{n-d_0}$. Since α is an r.e. real which is weakly Chaitin T-random, it follow from the implication (i) $\Rightarrow$ (ii) of Theorem 2.5 that α is $\Omega(T)$-like.

Now, for an arbitrary r.e. real β, assume that β is T-convergent and weakly Chaitin T-random. Then, by Theorem 4.4, β is strictly T-compressible. It follows from Theorem 4.5 that there exists $c \geq 2$ such that the base-two expansion of β has neither a run of c consecutive zeros nor a run of c consecutive ones. On the other hand, since the r.e. real α is weakly Chaitin T-random, from the definition of $\Omega(T)$-likeness we see that α dominates β. Therefore, there are computable, increasing sequences $\{a_k\}_{k\in\mathbb{N}}$ and $\{b_k\}_{k\in\mathbb{N}}$ of rationals and $d_1 \in \mathbb{N}$ such that $\lim_{k\to\infty} a_k = \alpha$ and $\lim_{k\to\infty} b_k = \beta$ and, for all $k \in \mathbb{N}$, $\alpha - a_k \geq 2^{-d_1}(\beta - b_k)$ and $\lfloor\beta\rfloor = \lfloor b_k\rfloor$. Then, by the following procedure, we see that there exists an oracle deterministic Turing machine M such that, for all $n \in \mathbb{N}^+$, $M^{\mathrm{dom}\, V\restriction_{\lceil Tn\rceil}}(n) = \beta\restriction_{n-(d_0+d_1+c+2)}$.

Given n and $\mathrm{dom}\, V\restriction_{\lceil Tn\rceil}$ with $n > d_0 + d_1 + c + 2$, one first calculates $\alpha\restriction_{n-d_0}$ by simulating the computation of M_0 with the input n and the oracle $\mathrm{dom}\, V\restriction_{\lceil Tn\rceil}$. One then find $k_0 \in \mathbb{N}$ such that $0.(\alpha\restriction_{n-d_0}) < a_{k_0}$. This is possible since $0.(\alpha\restriction_{n-d_0}) < \alpha$ and $\lim_{k\to\infty} a_k = \alpha$. It follows that $2^{-(n-d_0)} > \alpha - 0.(\alpha\restriction_{n-d_0}) > \alpha - a_{k_0} \geq 2^{-d_1}(\beta - b_{k_0})$. Thus, $0 < \beta - b_{k_0} < 2^{-(n-d_0-d_1)}$. Let t_n be the first n bits of the base-two expansion of the rational number $b_{k_0} - \lfloor b_{k_0}\rfloor$ with infinitely many zeros. Then, $|\, b_{k_0} - \lfloor b_{k_0}\rfloor - 0.t_n\,| \leq 2^{-n}$. It follows from $|\,\beta - \lfloor\beta\rfloor - 0.(\beta\restriction_n)\,| < 2^{-n}$ that $|\,0.(\beta\restriction_n) - 0.t_n\,| < (2^{d_0+d_1} + 2)2^{-n} < 2^{d_0+d_1+2}2^{-n}$. Hence, $|\,\beta\restriction_n - t_n\,| < 2^{d_0+d_1+2}$, where $\beta\restriction_n$ and t_n in $\{0,1\}^n$ are regarded as a dyadic integer. Thus, t_n is obtained by adding to $\beta\restriction_n$ or subtracting from $\beta\restriction_n$ a $d_0 + d_1 + 2$ bits dyadic integer. Since the base-two expansion of β has neither a run of c consecutive zeros nor a

run of c consecutive ones, it can be checked that the first $n-(d_0+d_1+2+c)$ bits of t_n equals the first $n-(d_0+d_1+2+c)$ bits of $\beta\restriction_n$. Thus one can output $\beta\restriction_{n-(d_0+d_1+c+2)}$ by calculating the first $n-(d_0+d_1+c+2)$ bits of t_n. □

5 Main Results

Let V and W be optimal prefix-free machines. The following two theorems together show computational equivalence, i.e., computational two-wayness, between the base-two expansion of $Z_W(T)$ and the halting problem of V in the case of $T<1$.

Theorem 5.1 (main result I). *Suppose that $T<1$. Let V and W be optimal prefix-free machines, and let $f\colon \mathbb{N}^+\to\mathbb{N}$ be a total recursive function. Then the following two conditions are equivalent:*

(i) There exist an oracle deterministic Turing machine M and $c\in\mathbb{N}$ such that, for all $n\in\mathbb{N}^+$, $M^{\mathrm{dom}\,V\restriction_{\lceil Tn\rceil}}(n)=Z_W(T)\restriction_{n+f(n)-c}$.

(ii) The function f is bounded to the above. □

Theorem 5.2 (main result II). *Let V and W be optimal prefix-free machines, and let $f\colon \mathbb{N}^+\to\mathbb{N}$ be a total recursive function. Then the following two conditions are equivalent:*

(i) There exist an oracle deterministic Turing machine M and $c\in\mathbb{N}$ such that, for all $n\in\mathbb{N}^+$, $M^{\{Z_W(T)\restriction_n\}}(n)=\mathrm{dom}\,V\restriction_{\lceil Tn\rceil+f(n)-c}$, where the finite subset $\mathrm{dom}\,V\restriction_{\lceil Tn\rceil+f(n)-c}$ of $\{0,1\}^*$ is represented as a finite binary string in a certain format.

(ii) The function f is bounded to the above. □

Due to the 7-page limit, we only prove Theorem 5.1 in what follows. Let W be an optimal prefix-free machine. By Theorem 7 of Tadaki [8], $Z_W(T)$ is a T-convergent r.e. real. Moreover, by Theorem 2.3, $Z_W(T)$ is weakly Chaitin T-random. Thus, the implication (ii) $\Rightarrow$ (i) of Theorem 5.1 follows immediately from Theorem 4.6.

On the other hand, the implication (i) $\Rightarrow$ (ii) of Theorem 5.1 follows immediately from Theorem 5.3 below and Theorem 2.3. In order to prove Theorem 5.3, we need Theorem 5.4 below.

Theorem 5.3. *Let β be a real which is weakly Chaitin T-random, and let V be an optimal prefix-free machine. For every function $f\colon \mathbb{N}^+\to\mathbb{Z}$, if there exists an oracle deterministic Turing machine M such that, for all $n\in\mathbb{N}^+$, $M^{\mathrm{dom}\,V\restriction_{\lceil Tn\rceil}}(n)=\beta\restriction_{n+f(n)}$, then the function f is bounded to the above.* □

Let M be a deterministic Turing machine with the input and output alphabet $\{0,1\}$, and let C be a prefix-free machine. We say that M *computes* C if the following holds: for every $p\in\{0,1\}^*$, when M starts with the input p, (i) M halts and outputs $C(p)$ if $p\in\mathrm{dom}\,C$; (ii) M does not halt forever otherwise. We use this convention on the computation of a prefix-free machine by a deterministic Turing machine throughout the rest of this paper. Thus, we exclude the possibility that there is $p\in\{0,1\}^*$ such that, when M starts with the input p, M halts but $p\notin\mathrm{dom}\,C$. For any $p\in\{0,1\}^*$, we denote the running time of M on the input p by $T_M(p)$ (may be ∞). Thus, $T_M(p)\in\mathbb{N}$ for every $p\in\mathrm{dom}\,C$ if M computes C.

We define $L_M=\min\{\,|p|\mid p\in\{0,1\}^*\ \&\ M \text{ halts on input } p\}$ (may be ∞). For any $n\geq L_M$, we define I_M^n as the set of all halting inputs p for M with $|p|\leq n$ which take longest to halt in the computation of M, i.e., as the set $\{\,p\in\{0,1\}^*\mid |p|\leq n\ \&\ T_M(p)=T_M^n\,\}$ where T_M^n is the maximum running time of M on all halting inputs of length at most n. In the work [7], we slightly strengthened the result presented in Chaitin [3] to obtain the following (see Note in Section 8.1 of Chaitin [3]).

Theorem 5.4 (Chaitin [3] and Tadaki [7]). *Let V be an optimal prefix-free machine, and let M be a deterministic Turing machine which computes V. Then $n=H(n,p)+O(1)=H(p)+O(1)$ for all (n,p) with $n\geq L_M$ and $p\in I_M^n$.* □

Proof of Theorem 5.3. Let β be a real which is weakly Chaitin T-random. Let V be an optimal prefix-free machine, and let M be a deterministic Turing machine which computes V. For each n with $\lceil Tn\rceil\geq L_M$, we choose a particular p_n from $I_M^{\lceil Tn\rceil}$. For an arbitrary function $f\colon \mathbb{N}^+\to\mathbb{Z}$, assume that there exists an

oracle deterministic Turing machine M_0 such that, for all $n \in \mathbb{N}^+$, $M_0^{\mathrm{dom}\, V\restriction_{\lceil Tn\rceil}}(n) = \beta\restriction_{n+f(n)}$. Then, by the following procedure, we see that there exists a partial recursive function $\Psi\colon \mathbb{N} \times \{0,1\}^* \to \{0,1\}^*$ such that, for all n with $\lceil Tn\rceil \geq L_M$,

$$\Psi(n, p_n) = \beta\restriction_{n+f(n)}\,. \tag{5}$$

Given (n, p_n) with $\lceil Tn\rceil \geq L_M$, one first calculates the finite set $\mathrm{dom}\, V\restriction_{\lceil Tn\rceil}$ by simulating the computation of M with the input q until at most the time step $T_M(p_n)$, for each $q \in \{0,1\}^*$ with $|q| \leq \lceil Tn\rceil$. This can be possible because $T_M(p_n) = T_M^{\lceil Tn\rceil}$ for every n with $\lceil Tn\rceil \geq L_M$. One then calculates $\beta\restriction_{n+f(n)}$ by simulating the computation of M_0 with the input n and the oracle $\mathrm{dom}\, V\restriction_{\lceil Tn\rceil}$.

It follows from (5) and (2) that

$$H(\beta\restriction_{n+f(n)}) \leq H(n, p_n) + O(1) \tag{6}$$

for all n with $\lceil Tn\rceil \geq L_M$.

On the other hand, given $\lceil Tn\rceil$ with $n \in \mathbb{N}^+$, one only need to specify one of $\lceil 1/T\rceil$ possibilities of n in order to calculate n, since T is a computable real and $T \neq 0$. Thus, there exists a partial recursive function $\Phi\colon \mathbb{N}^+ \times \{0,1\}^* \times \mathbb{N}^+ \to \mathbb{N}^+ \times \{0,1\}^*$ such that, for every $n \in \mathbb{N}^+$ and every $p \in \{0,1\}^*$, there exists $k \in \mathbb{N}^+$ with the properties that $1 \leq k \leq \lceil 1/T\rceil$ and $\Phi(\lceil Tn\rceil, p, k) = (n, p)$. It follows from (2) and (1) that $H(n,p) \leq H(\lceil Tn\rceil, p) + \max\{H(k) \mid k \in \mathbb{N}^+ \,\&\, 1 \leq k \leq \lceil 1/T\rceil\} + O(1)$ for all $n \in \mathbb{N}^+$ and all $p \in \{0,1\}^*$. Hence, using (6) and Theorem 5.4 we have

$$H(\beta\restriction_{n+f(n)}) \leq H(\lceil Tn\rceil, p_n) + O(1) \leq \lceil Tn\rceil + O(1) \leq Tn + O(1) \tag{7}$$

for all n with $\lceil Tn\rceil \geq L_M$.

On the other hand, since β is weakly Chaitin T-random, we have $Tn + Tf(n) \leq H(\beta\restriction_{n+f(n)}) + O(1)$ for all $n \in \mathbb{N}^+$. Combining this with (7), we see that f is bounded to the above. □

Acknowledgments

The author is grateful to Prof. Marius Zimand for the valuable discussions. 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, 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`

[2] G. J. Chaitin, "A theory of program size formally identical to information theory," *J. Assoc. Comput. Mach.*, vol. 22, pp. 329–340, 1975.

[3] G. J. Chaitin, *Algorithmic Information Theory*. Cambridge University Press, Cambridge, 1987.

[4] 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.

[5] K. Tadaki, "A generalization of Chaitin's halting probability Ω and halting self-similar sets," *Hokkaido Math. J.*, vol. 31, pp. 219–253, 2002.

[6] 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`

[7] K. Tadaki, Chaitin Ω numbers and halting problems. *Proc. CiE 2009*, Lecture Notes in Computer Science, Springer-Verlag, Vol.5635, pp.447–456, 2009.

[8] K. Tadaki, Partial randomness and dimension of recursively enumerable reals. *Proc. MFCS 2009*, Lecture Notes in Computer Science, Springer-Verlag, Vol.5734, pp.687–699, 2009.