Phase transition between one-wayness and two-wayness[1]

Kohtaro Tadaki

Research and Development Initiative, Chuo University
JST CREST
http://www2.odn.ne.jp/tadaki/

Abstract. The statistical mechanical interpretation of algorithmic information theory (AIT, for short) was introduced and developed by our former works [2, 3, 4]. In this talk, we investigate the phase transition at temperature $T = 1$ occurring in the interpretation, from the point of view of the relative computational power between the thermodynamic quantities of AIT and the halting problem.

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 an optimal prefix-free machine to output s. Here an optimal prefix-free machine is a universal decoding algorithm. By the definition, $H(s)$ is thought to represent the amount of randomness contained in a finite binary string s, which cannot be captured in an effective manner. 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] we introduced and developed a *statistical mechanical interpretation* of AIT. We there introduced the notion of *thermodynamic quantities at temperature* T, such as partition function $Z(T)$, free energy $F(T)$, energy $E(T)$, and statistical mechanical entropy $S(T)$, into AIT. These quantities are real functions of a real argument $T > 0$. We then proved that if the temperature T is a computable real with $0 < T < 1$ then, for each of these thermodynamic quantities, the partial randomness of its value equals to T, where the notion of *partial randomness* is a stronger representation of the compression rate by means of program-size complexity. Thus, the temperature T plays a role as the partial randomness of all the thermodynamic quantities in the statistical mechanical interpretation of AIT. In [2] we further showed that the temperature T plays a role as the partial randomness of the temperature T itself, which is a thermodynamic quantity of itself. Namely, we proved *the fixed point theorem on partial randomness*, which states that, for every $T \in (0, 1)$, if the value of partition function $Z(T)$ at temperature 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., $\lim_{n\to\infty} H(T\restriction_n)/n = T$, where $T\restriction_n$ is the first n bits of the base-two expansion of T.

In our second work [3] on the interpretation, we showed that a fixed point theorem of the same form as for $Z(T)$ holds also for each of free energy $F(T)$, energy $E(T)$, and statistical mechanical entropy $S(T)$. Moreover, based on the statistical mechanical relation $F(T) = -T \log_2 Z(T)$, we showed that the computability of $F(T)$ gives completely different fixed points from the computability of $Z(T)$.

In the third work [4], we pursued the formal correspondence between the statistical mechanical interpretation of AIT and normal statistical mechanics further, and then unlocked the properties of the sufficient conditions for the fixed points on partial randomness further. The thermodynamic quantities in AIT are defined based on the halting set of an optimal prefix-free machine. In [4], we showed that there are infinitely many optimal prefix-free machines which give completely different sufficient conditions in all of the thermodynamic quantities in AIT.

[1]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.

We did this by introducing the notion of composition of prefix-free machines into AIT, which corresponds to the notion of composition of systems in normal statistical mechanics.

The work [2] also showed that the values of all the thermodynamic quantities diverge when the temperature T exceeds 1. This phenomenon may be regarded as *phase transition* in normal statistical mechanics. In this talk, we reveal a new aspect of the phase transition occurring in the statistical mechanical interpretation of AIT. Namely, we reveal the critical difference of the behavior of the thermodynamic quantities between $T = 1$ and $T < 1$, from the point of view of the relative computational power between them and the halting problem.

2 Preliminaries

We first review some basic notation and definitions which will be used in this talk. $\mathbb{N} = \{0, 1, 2, 3, \dots\}$ is the set of natural numbers, and $\mathbb{N}^+$ is the set of positive integers. $\mathbb{R}$ is the set of reals. $\{0,1\}^*$ is the set of finite binary strings. For any $s \in \{0,1\}^*$, $|s|$ is the *length* of s. 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 $\mathrm{dom}\, f$. We write "r.e." instead of "recursively enumerable." An *order function* is a non-decreasing total recursive function $f\colon \mathbb{N} \to \mathbb{N}$ such that $\lim_{n\to\infty} f(n) = \infty$.

A real α is called *computable* if there exists a computable sequence $\{a_n\}$ of rationals such that $|\alpha - a_n| < 2^{-n}$ for all $n \in \mathbb{N}$. For any $\alpha \in \mathbb{R}$ and $n \in \mathbb{N}^+$, 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 *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 any prefix-free machine C and any $s \in \{0,1\}^*$, $H_C(s)$ 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 $d \in \mathbb{N}$ such that, for every $s \in \{0,1\}^*$, $H_U(s) \leq H_C(s) + d$. 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.

Let V be an optimal prefix-free machine. The set $\mathrm{dom}\, V$ is called *the halting problem*. For each real $T > 0$, the *partition function* $Z_V(T)$ of V at temperature T is defined by

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

If $0 < T \leq 1$, then $Z_V(T)$ converges and $0 < Z_V(T) \leq 1$ due to the Kraft inequality. However, $Z_V(T)$ is shown to diverge to ∞ in the case of $T > 1$.

3 The Results

The notion of weak truth-table reducibility plays an important role in computability theory (see e.g. [1]). First we elaborate this notion as follows. This elaboration enables us to deal with the notion of asymptotic behavior in a manner like in computational complexity theory, while staying in computability theory.

Definition 3.1 (reducibility in query size f)**.** *Let $f\colon \mathbb{N} \to \mathbb{N}$, and let $A, B \subset \{0,1\}^*$. We say that A is reducible to B in query size f if there exists an oracle deterministic Turing machine M such that (i) A is Turing reducible to B via M, and (ii) on every input $s \in \{0,1\}^*$, M only queries strings of length at most $f(|s|)$.* □

For each $\alpha \in \mathbb{R}$, the *prefixes* $\mathrm{Pf}(\alpha)$ of α is the subset of $\{0,1\}^*$ defined by $\mathrm{Pf}(\alpha) = \{\alpha\restriction_n \mid n \in \mathbb{N}\}$. On the one hand, Theorem 3.2 (i) below gives a succinct equivalent characterization of f for which $Z_V(1)$ is reducible to $\mathrm{dom}\, W$ in query size f and reversely Theorem 3.2 (ii) gives a succinct equivalent characterization of f for which $\mathrm{dom}\, W$ is reducible to $Z_V(1)$ in query size f.

Theorem 3.2. *Let V and W be optimal prefix-free machines.*

(i) For every order function f, $\mathrm{Pf}(Z_V(1))$ is reducible to $\mathrm{dom}\, W$ in query size $f(n)+O(1)$ if and only if $\sum_{n=0}^{\infty} 2^{n-f(n)} < \infty$.

(ii) For every order function f, $\mathrm{dom}\, W$ is reducible to $\mathrm{Pf}(Z_V(1))$ in query size $f(n)+O(1)$ if and only if $n \leq f(n)+O(1)$. □

On the other hand, Theorem 3.3 (i) below gives a succinct equivalent characterization of f for which $Z_V(T)$ is reducible to $\mathrm{dom}\, W$ in query size f and reversely Theorem 3.3 (ii) gives a succinct equivalent characterization of f for which $\mathrm{dom}\, W$ is reducible to $Z_V(T)$ in query size f, in the case where T is a computable real with $0 < T < 1$.

Theorem 3.3. *Suppose that T is a computable real with $0 < T < 1$. Let V and W be optimal prefix-free machines.*

(i) For every order function f, $\mathrm{Pf}(Z_V(T))$ is reducible to $\mathrm{dom}\, W$ in query size $f(n)+O(1)$ if and only if $Tn \leq f(n)+O(1)$.

(ii) For every order function f, $\mathrm{dom}\, W$ is reducible to $\mathrm{Pf}(Z_V(T))$ in query size $f(n)+O(1)$ if and only if $n/T \leq f(n)+O(1)$. □

Based on the notion of reducibility in query size f, we introduce the notions of *one-wayness* and *two-wayness* between two sets A and B as follows.

Definition 3.4. *Let $A, B \subset \{0,1\}^*$. We say that the computation from A to B is one-way if the following holds: For every order functions f and g, if B is reducible to A in query size f and A is reducible to B in query size g then the function $g(f(n))-n$ of $n \in \mathbb{N}$ is unbounded. We say that the computations between A and B are two-way if the computation from A to B is not one-way and the computation from B to A is not one-way.* □

The above notions enable us to investigate the relative computational power between A and B. In particular, they can reveal a critical difference of the behavior of $Z(T)$ between $T = 1$ and $T < 1$ as follows, which cannot be captured by the original notion of weak truth-table reducibility.

Theorem 3.5 (one-wayness)**.** *Let V and W be optimal prefix-free machines. Then the computation from $\mathrm{Pf}(Z_V(1))$ to $\mathrm{dom}\, W$ is one-way and the computation from $\mathrm{dom}\, W$ to $\mathrm{Pf}(Z_V(1))$ is one-way.* □

Theorem 3.6 (two-wayness)**.** *Suppose that T is a computable real with $0 < T < 1$. Let V and W be optimal prefix-free machines. Then the computations between $\mathrm{Pf}(Z_V(T))$ and $\mathrm{dom}\, W$ are two-way.* □

References

[1] R. G. Downey and D. R. Hirschfeldt, *Algorithmic Randomness and Complexity*. Springer-Verlag, 2010.

[2] 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` An Extended Version also Available: `http://arxiv.org/abs/0801.4194v1`

[3] K. Tadaki, Fixed point theorems on partial randomness. Proceedings of the Symposium on Logical Foundations of Computer Science 2009 (LFCS'09), Lecture Notes in Computer Science, Springer-Verlag, vol. 5407, pp. 422–440, 2009.

[4] K. Tadaki, A statistical mechanical interpretation of algorithmic information theory III: Composite systems and fixed points. Proceedings of the 2009 IEEE Information Theory Workshop (ITW 2009), pp. 354–358, October 11-16, 2009, Taormina, Sicily, Italy.