LETTER

Complexity Oscillations in Random Reals

ChenGuang LIU[†a)], ***Student Member and*** **Kazuyuki TANAKA**[†], ***Nonmember***

SUMMARY The C-oscillation due to Martin-Löf shows that $\{\alpha | \forall n[C(\alpha \upharpoonright n) \geq n - O(1)]\} = \emptyset$, which also follows $\{\alpha | \forall n[K(\alpha \upharpoonright n) \geq n + K(n) - O(1)]\} = \emptyset$. By generalizing them, we show that there does not exist a real α such that $\forall n (K(\alpha \upharpoonright n) \geq n + \lambda K(n) - O(1))$ for any $\lambda > 0$.

key words: *algorithmic randomness, C-oscillation, Kolmogorov complexity*

1. Introduction

Most notations used in this letter are standard. We use C and K for plain Kolmogorov complexity and prefix-free Kolmogorov complexity, respectively. Let $2^{<\omega}$ be the set of finite binary sequences and 2^{ω} the set of infinite binary sequences. We use $\sigma, \tau, \ldots$ to denote the elements of $2^{<\omega}$, and $\alpha, \beta, \ldots$ to denote the elements of 2^{ω}. Occasionally, we write $\sigma \cdot \tau = \sigma\tau$ to denote the concatenation of the strings σ and τ. $|\sigma|$ is the length of sequence σ. $\alpha \upharpoonright n$ is the prefix of α with length n. We write 2^i for the set $\{\sigma \in 2^{<\omega} : |\sigma| = i\}$. By $\nu \sqsubset \upsilon$ we mean that ν is a prefix of υ.

We also say a member of Cantor space 2^{ω} by a *real*. Any real member in $[0,1]$ can be associated with a real $\alpha = \alpha_{[1]}\alpha_{[2]} \ldots \alpha_{[n]} \ldots$ via the function $\varphi : 2^{\omega} \to [0,1]$ where $\varphi(\alpha) = \sum_{i=1}^{\infty} \alpha_{[i]} 2^{-i}$. Let $bin : \mathbb{N}_+ \to 2^{<\omega}$ be the bijection which associates to every $n \geq 1$ its binary expansion without the leading 1, i.e., the binary expansion of n is $1bin(n)$.

We assume the reader is acquainted with the basic definitions and results of recursion theory and algorithmic randomness. We refer to the textbooks of Soare [7], Calude [1], and Li and Vitányi [3] for this background.

2. C-Oscillation

The main idea behind the theory of algorithmic randomness for finite strings is that a string σ is random if and only if it is *incompressible*, that is, the only way to generate the random string σ by an algorithm is to essentially hardwire it into the algorithm. Therefore, the minimal length of a program to generate the random string σ is essentially the same as that of σ itself.

Random reals should be those whose initial segments are all hard to compress. With such considerations, the first attempt to define a random real would be to say that α is random if $C(\alpha \upharpoonright n) \geq n - O(1)$ for all n. Unfortunately, no real satisfies this condition.

Theorem 1 (Martin-Löf [5], [6]): There does not exist a real α such that

$$\forall n (C(\alpha \upharpoonright n) \geq n - O(1)).$$

This is a fundamental observation of Martin-Löf. This reasoning is refined in the following theorem.

Theorem 2: For any real α, we have $C(\alpha \upharpoonright n) \leq n - \log n + O(1)$ for infinitely many n.

Proof: Let $\sigma_1, \sigma_2, \ldots$ be an effective listing of all strings, with $|\sigma_n| = \lfloor \log n \rfloor$. If $\alpha \upharpoonright m = \sigma_n$, then from the length of $\alpha \upharpoonright n$ we can recover $\alpha \upharpoonright m$. Thus, to generate $\alpha \upharpoonright n$, we need only generate the string τ such that $\alpha \upharpoonright n = \sigma\tau$ and compute n from $|\tau| = n - \log n$, which gives us σ_n. This shows that for any α, $\exists^{\infty} n (C(\alpha \upharpoonright n) \leq n - \log n + O(1))$. □

The highest prefix-free Kolmogorov complexity of string with length n can have $n + K(n) + O(1)$. However, it is impossible for a real to have $K(\alpha \upharpoonright n) \geq n + K(n) - O(1)$ for all n.

Theorem 3: There does not exist a real α such that

$$\forall n (K(\alpha \upharpoonright n) \geq n + K(n) - O(1)).$$

Proof: (Downey and Hirshfeldt [2]) From the definition of plain Kolmogorov complexity, we have $C(\sigma) \leq |\sigma| + O(1)$ for any $\sigma \in 2^{<\omega}$.

Let $m_c(\sigma) = |\sigma| - C(\sigma) + O(1)$. It is clear that $C(\sigma) = |\sigma| - m_c(\sigma) + O(1)$. Then, we have

$$\begin{aligned} K(C(\sigma)) &= K(|\sigma| - m_c(\sigma) + O(1)) \\ &\leq K(|\sigma|) + K(m_c(\sigma) - O(1)) \\ &\leq K(|\sigma|) + O(\log m_c(\sigma)). \end{aligned}$$

By the theorem $C(\sigma) \geq K(\sigma) - K(C(\sigma)) - O(1)$. Consequently, for any σ,

$$K(\sigma) \leq |\sigma| - m_c(\sigma) + K(|\sigma|) + O(\log m_c(\sigma)).$$

Rearranging this inequality, we get

$$|\sigma| + K(|\sigma|) - K(\sigma) \geq m_c(\sigma) - O(\log m_c(\sigma)).$$

For any $\sigma \in 2^{<\omega}$, $K(\sigma) \leq |\sigma| + K(|\sigma|) + O(1)$. Let $m_k(\sigma) = |\sigma| + K(|\sigma|) - K(\sigma) + O(1)$. Suppose there is real

Manuscript received February 18, 2008.
[†]The authors are with Tohoku University, Sendai-shi, 980–0815 Japan. The first author is also with Xi'an University of Technology, Xi'an 710054 China.
a) E-mail: liu@mail.tains.tohoku.ac.jp
DOI: 10.1093/ietisy/e91–d.10.2517

α with $\exists c \forall n (K(\alpha \upharpoonright n) \geq n + K(n) - c)$. Set $\sigma \sqsubset \alpha$, say $\sigma = \alpha \upharpoonright n$. Hence, $m_K(\sigma) = m_K(\alpha \upharpoonright n) \leq c$ for some fixed c (independent of σ). By $m_K(\sigma) \geq m_c(\sigma) - O(\log m_c(\sigma))$, we have $m_c(\alpha \upharpoonright n) - O(\log m_c(\alpha \upharpoonright n)) \leq c$, which clearly implies that $m_c(\alpha \upharpoonright n) \leq c'$ for some fixed c'. Hence, $\exists c \forall n (C(\alpha \upharpoonright n) \geq n - c')$, a contraction. □

3. The Generalization of C-Oscillation

In this section, we provide a generalization of C-oscillation. More precisely, we have the following theorem.

Theorem 4: For any $\lambda > 0$, there does not exist a real α such that

$$\forall n \, (K(\alpha \upharpoonright n) \geq n + \lambda K(n) - O(1)) .$$

In proving this theorem, we will use the following theorem.

Theorem 5: For any n, we have

$$K(n) \leq \log n + O(\log \log n).$$

Proof: Since the length of the binary representation of n is $1 + |bin(n)|$ and $|bin(n)| = \lfloor \log n \rfloor$, we have $C(n) \leq \log n + O(1)$.

Recall $K(\sigma) \leq C(\sigma) + C^{(2)}(\sigma) + C^{(3)}(\sigma) + \ldots + C^{(n)}(\sigma) + O(C^{(n+1)}(\sigma))$ for any n. Hence, we have $K(n) \leq \log n + O(\log \log n)$. □

Now, we prove Theorem 4 below.

Proof of Theorem 4: Suppose not. Let $\lambda > 0$ and $\alpha \in 2^{\omega}$ be a real such that

$$\forall n \, (K(\alpha \upharpoonright n) \geq n + \lambda K(n) - O(1)) .$$

1) For $\lambda = 1$, this was proved in Theorem 3.

2) For $\lambda > 1$. Recall $K(\sigma) \leq |\sigma| + K(|\sigma|) + O(1)$ for any $\sigma \in 2^{<\omega}$. Consequently,

$$K(\alpha \upharpoonright n) \leq n + K(n) + O(1).$$

Then, we have

$$n + \lambda K(n) \leq n + K(n) + O(1).$$

Since $K(n) > 0$, this is a contraction.

3) For $1 > \lambda > 0$. In the proof of Theorem 3, we have proved that, for any σ,

$$K(\sigma) \leq C(\sigma) + K(|\sigma|) + O(\log m_c(\sigma)).$$

Set $\sigma \sqsubset \alpha$, say $\sigma = \alpha \upharpoonright n$. Hence, we have

$$K(\alpha \upharpoonright n) \leq C(\alpha \upharpoonright n) + K(n) + O(\log(n - C(\alpha \upharpoonright n))).$$

With respect the supposition, we have

$$\forall n (n - C(\alpha \upharpoonright n) - O(\log(n - C(\alpha \upharpoonright n))) \leq (1 - \lambda) K(n)).$$

Fix δ with $1 - \lambda < \delta < 1$. Then, we have

$$\forall^{\infty} n \left(\frac{\delta}{1 - \lambda} (n - C(\alpha \upharpoonright n)) \leq K(n) \right).$$

Recall Theorem 2 $\exists^{\infty} n (n - C(\alpha \upharpoonright n) + O(1) \geq \log n)$ and Theorem 5 $\forall n (K(n) \leq \log n + O(\log \log n))$. So,

$$\exists^{\infty} n \left(\frac{\delta}{1 - \lambda} \log n < \log n + O(\log \log n) \right),$$

which is a contradiction.

Sum up the the above three cases, we have $\{\alpha | \forall n (K(\alpha \upharpoonright n) \geq n + \lambda K(n) - O(1))\} = \emptyset$ for any $\lambda > 0$.

The proof completes. □

This generalization is very useful in exploring the relations between the various definitions of partial randomness, for details to see [4].

Acknowledgments

This research is supported in part by the Mitsubishi Foundation. The first author is also partially supported by a grant-in-aid for special research of the 21st century Center of Excellence (COE) program "Exploring new Science by Bridging Particle-Matter Hierarchy" from Ministry of Education, Culture, Sports, Science and Technology, Japan.

References

[1] C.S. Calude, Information theory and randomness: An algorithmic perspective, 2nd ed., Springer-Verlag, 2002.

[2] R. Downey and D. Hirshfeldt, "Algorithmic randomness and complexity," in Monographs in mathematical logic, Springer-Verlag, in preparation.

[3] M. Li and P. Vitányi, An introduction to Kolmogorov complexity and its applications, 2nd ed., Springer-Verlag, 1997.

[4] C.G. Liu, Computational aspects of randomness, Doctor Thesis, Tohoku University, Dec. 2007.

[5] P. Martin-Löf, "The definition of random sequences," Information and Control, vol.9, no.6, pp.602–619, 1966.

[6] P. Martin-Löf, "Complexity oscillations in infinite binary sequences," Z. Wahrscheinlichkeit—Theorie Verw, Gebiete, vol.19, pp.225–230, 1971.

[7] R.I. Soare, Recursively enumerable sets and degrees, Springer-Verlag, 1987.