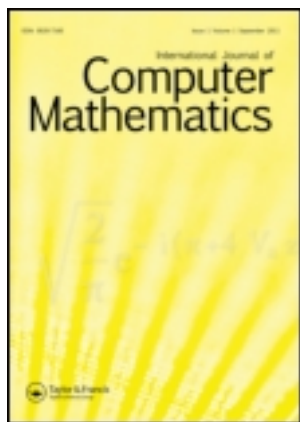


This article was downloaded by: [University of Auckland Library]

On: 27 November 2011, At: 10:41

Publisher: Taylor & Francis

Informa Ltd Registered in England and Wales Registered Number: 1072954 Registered office: Mortimer House, 37-41 Mortimer Street, London W1T 3JH, UK



International Journal of Computer Mathematics

Publication details, including instructions for authors and subscription information:
<http://www.tandfonline.com/loi/gcom20>

Strong noncomputability of random strings

Cristian Calude^a & Ion Chițescu^a

^a Department of Mathematics, University of Bucharest, Str. Academiei 14, Bucharest, R-70109, Romania

Available online: 19 Mar 2007

To cite this article: Cristian Calude & Ion Chițescu (1982): Strong noncomputability of random strings, International Journal of Computer Mathematics, 11:1, 43-45

To link to this article: <http://dx.doi.org/10.1080/00207168208803297>

PLEASE SCROLL DOWN FOR ARTICLE

Full terms and conditions of use: <http://www.tandfonline.com/page/terms-and-conditions>

This article may be used for research, teaching, and private study purposes. Any substantial or systematic reproduction, redistribution, reselling, loan, sub-licensing, systematic supply, or distribution in any form to anyone is expressly forbidden.

The publisher does not give any warranty express or implied or make any representation that the contents will be complete or accurate or up to date. The accuracy of any instructions, formulae, and drug doses should be independently verified with primary sources. The publisher shall not be liable for any loss, actions, claims, proceedings, demand, or costs or damages whatsoever or howsoever caused arising directly or indirectly in connection with or arising out of the use of this material.

Strong Noncomputability of Random Strings

CRISTIAN CALUDE and ION CHIȚESCU

Department of Mathematics, University of Bucharest, Str. Academiei 14, R-70109
Bucharest, Romania

(Received August 1981)

We prove that every infinite set of random strings is not recursively enumerable. In particular, the set of all random strings is not recursively enumerable. This property asserts that in a strong sense random strings are not constructable.

KEY WORDS: Kolmogorov complexity, random strings.

C.R. CATEGORY: 5.25, 5.26.

1) Let $X = \{a_1, a_2, \dots, a_p\}$, $p \geq 2$ be a finite alphabet. Denote by X^* the free monoid generated by X (the elements of X^* are called *strings*; the empty string is denoted by λ). If $x = x_1 x_2 \dots x_n$ is in X^* , then the length of x is $l(x) = n$; $l(\lambda) = 0$. $N = \{0, 1, 2, \dots\}$ is the set of natural numbers.

Let A and B be two sets. The notation $f: A \overset{0}{\rightarrow} B$ means that f is partially defined on A and takes its values in B . The domain of f is denoted by $\text{dom}(f)$. We shall consider *partial recursive functions* (p.r. functions in the sequel) $\varphi: X^* \times N \overset{0}{\rightarrow} X^*$, or $f: N \overset{0}{\rightarrow} X^*$. They are sometimes assumed to take the (conventional) value ∞ at points not belonging to their domain. A *recursive function* is a p.r. function which is everywhere defined. The range of a p.r. function is a *recursively enumerable set* (r.e. set in the sequel). For Recursive Function Theory see [3], [5].

For a p.r. function $\varphi: X^* \times N \overset{0}{\rightarrow} X^*$ we define the *Kolmogorov complexity* induced by φ , denoted K_φ , to be the function $K_\varphi: X^* \times N \overset{0}{\rightarrow} N \cup \{\infty\}$,

$$K_\varphi(x | n) = \begin{cases} \min \{l(y) \mid y \in X^*, \varphi(y, n) = x\}, & \text{if such } y \text{ exists,} \\ \infty, & \text{otherwise.} \end{cases}$$

It is proved in [2] the existence of a p.r. function $\psi: X^* \times N \overset{0}{\rightarrow} X^*$ (*universal algorithm in the sense of Kolmogorov*) such that: For every p.r. function $\varphi: X^* \times N \overset{0}{\rightarrow} X^*$, there exists a constant c (depending upon ψ and φ) such that $K_\psi(x|n) \leq K_\varphi(x|n) + c$, for every x in X^* and n in N . Put $K_\psi = K$, for some fixed universal algorithm ψ , and notice that K takes only finite values.

A string x is called *random (in the sense of Kolmogorov [2])* if $K(x|l(x)) \geq l(x)$. Random strings exist (for every ψ and every length).

See [2], [4], [6] for general results concerning binary random strings. For the nonbinary case see [1].

2) We rely heavily on the following result:

THEOREM 1. *Let $f: N \overset{0}{\rightarrow} X^*$ be a partial function with the following two properties:*

- 1) *dom(f) is infinite,*
- 2) *$K(f(n)|n) \geq n$, for every n in dom(f).*

Then f has no partial recursive extension (consequently f itself is not partial recursive).

Proof Suppose there exists a p.r. function $f^*: N \overset{0}{\rightarrow} X^*$ which extends f . We shall derive a contradiction.

First, we construct the auxiliary p.r. function $\varphi_{f^*}: X^* \times N \overset{0}{\rightarrow} X^*$, given by $\varphi_{f^*}(x, m) = f^*(m)$, for all x in X^* and m in N . Clearly, $\text{dom}(\varphi_{f^*}) = X^* \times \text{dom}(f^*)$.

We claim that $K_{\varphi_{f^*}}(f(n)|n) = 0$, for all n in $\text{dom}(f^*)$ (because $\varphi_{f^*}(\lambda, n) = f^*(n)$, for every n in $\text{dom}(f^*)$).

According to Kolmogorov's Theorem we get a constant c (depending upon ψ and φ_{f^*}) such that

$$K(f^*(n)|n) \leq K_{\varphi_{f^*}}(f^*(n)|n) + c = c,$$

for every n in $\text{dom}(f)$.

Using condition (1), for every n in $\text{dom}(f)$, $n > c$, we have: $K(f^*(n)|n) = K(f(n)|n) \leq c$, contradicting condition (2) which yields $K(f(n)|n) \geq n > c$. Q.E.D.

COROLLARY 1. (*P. Martin-Löf*). *There is no recursive function $f: N \rightarrow X^*$ such that $l(f(n)) = n$ and $K(f(n)|n) \geq n$, for all n in N .*

Remarks

1) Corollary 1 shows that there is no algorithm which generates for every n in N a random string of length n .

2) Corollary 1 provides a motivation for Kolmogorov's definition of "random strings". Indeed, if x is random, there are no recursive tools for recognizing this.

3) From Corollary 1 it follows that the Kolmogorov complexity is not a p.r. function.

THEOREM 2. *Every infinite set of random strings is not recursively enumerable. In particular, the set of all random strings is not recursively enumerable.*

Proof Let A be an infinite r.e. set of random strings. There exists an injective recursive function $f: N \rightarrow X^*$ such that $f(N) = A$. We can construct a p.r. function $f^*: N \rightarrow X^*$ such that $\text{dom}(f^*)$ is infinite and $K(f^*(n) | n) \geq n$, for all n in $\text{dom}(f^*)$, thus contradicting Theorem 1.

The procedure for computing f^* is the following:

1. Put $i = 0$.
2. Put $f^*(l(f(i))) = f(i)$.
3. Put $i = i + 1$.
4. If $l(f(i)) = l(f(j))$, for some $j < i$, then go to step 3.
5. Go to step 2.

Because A is infinite, the domain of f^* is also infinite. For every n in $\text{dom}(f^*)$ one has: $l(f^*(n)) = n$ and $K(f^*(n) | l(f^*(n))) \geq l(f^*(n)) = n$, because $f^*(N) \setminus \{\infty\} \subset A$. Q.E.D.

Remark Theorem 2 reinforces the non-constructivity argument in Remark (2) following Corollary 1.

References

- [1] C. Calude and I. Chişescu, Random strings according to A. N. Kolmogorov and P. Martin-Löf. Classical approach, *Foundations of Control Engineering* (to appear).
- [2] A. N. Kolmogorov, Three approaches to the quantitative definition of information. *Problems of Information Transmission* **1** (1965), 1-7.
- [3] M. Machtey and P. Young, *An introduction to the general theory of algorithms*, North-Holland, New-York, 1978.
- [4] P. Martin-Löf, *Algorithms and random sequences*, Erlagen University, Nürnberg, Erlagen, 1966.
- [5] H. Rogers, Jr. *The theory of recursive functions and effective computability*, McGraw-Hill, New-York, 1967.
- [6] A. Zvonkin and L. Levin, The complexity of finite objects and the development of the concepts of information and randomness by means of the theory of algorithms, *Uspehi. Mat. Nauk* **156** (1970), 85-127. (in Russian).