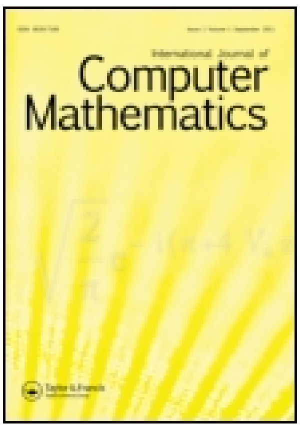


International Journal of Computer Mathematics
Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/gcom20

# Strong noncomputability of random strings

Cristian Calude [a] & Ion Chiţescu [a]

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

Available online: 19 Mar 2007

*Intern. J. Computer Math* 1982, Vol. 11, pp. 43–45
0020-7160/82/1101-0043 $06.50/0

Printed in Great Britain



# 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 $X=\{a_1, a_2, \ldots, a_p\}$, $p \geqq 2$ 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 $\lambda$). If $x=x_1x_2\ldots x_n$ is in $X^*$, then the length of $x$ is $l(x)=n$; $l(\lambda)=0$. $N=\{0,1,2,\ldots\}$ is the set of natural numbers.

Let $A$ and $B$ be two sets. The notation $f\colon A \overset{0}{\to} B$ means that $f$ is partially defined on $A$ and takes its values in $B$. The domain of $f$ is denoted by dom $(f)$. We shall consider *partial recursive functions* (*p.r. functions* in the sequel) $\varphi\colon X^* \times N \overset{0}{\to} X^*$, or $f\colon N \overset{0}{\to} X^*$. They are sometimes assumed to take the (conventional) value $\infty$ 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 $\varphi\colon X^* \times N \overset{0}{\to} X^*$ we define the *Kolmogorov complexity* induced by $\varphi$, denoted $K_\varphi$, to be the function $K_\varphi\colon X^* \times N \overset{0}{\to} N \cup \{\infty\}$,

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

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

A string $x$ is called *random* (*in the sense of Kolmogorov* [2]) if $K(x \mid l(x)) \geqq l(x)$. Random strings exist (for every $\psi$ 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 $f$: $N \xrightarrow{0} X^*$ be a partial function with the following two properties:*

*1) dom$(f)$ is infinite,*

*2) $K(f(n) \mid n) \geqq n$, 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 $f^*: N \xrightarrow{0} X^*$ which extends $f$. We shall derive a contradiction.

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

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

According to Kolmogorov's Theorem we get a constant $c$ (depending upon $\psi$ and $\varphi_{f*}$) such that

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

for every $n$ in dom$(f)$.

Using condition (1), for every $n$ in dom$(f)$, $n > c$, we have: $K(f^*(n) \mid n) = K(f(n) \mid n) \leqq c$, contradicting condition (2) which yields $K(f(n) \mid n) \geqq n > c$. Q.E.D.

COROLLARY 1. (*P. Martin-Löf*). *There is no recursive function $f$: $N \to X^*$ such that $l(f(n)) = n$ and $K(f(n) \mid n) \geqq n$, 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 $f: N \to X^*$ such that $f(N) = A$. We can construct a p.r. function $f^*: N \xrightarrow{0} X^*$ such that dom$(f^*)$ is infinite and $K(f^*(n) \mid n) \geqq n$, for all $n$ in 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 dom$(f^*)$ one has: $l(f^*(n))=n$ and $K(f^*(n) \mid l(f^*(n))) \geqq l(f^*(n))=n$, 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. Chiţescu, 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).