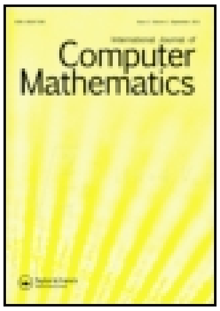

International Journal of Computer Mathematics
Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/gcom20

A relation between correctness and randomness in the computation of probabilistic algorithms

Cristian Calude [a] & Marius Zimand [a]
[a] Department of Mathematics, University of Bucharest, Str. Academiei 14, Bucharest, Romania, R- 70109

Available online: 20 Mar 2007

Intern. J. Computer Math. 1984, Vol. 16, pp. 47–53.
0020-7160/84/1601-0047 $18.50/0

A Relation Between Correctness and Randomness in the Computation of Probabilistic Algorithms

CRISTIAN CALUDE and MARIUS ZIMAND

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

(*Received March, 1984*)

Chaitin and Schwartz [4] have proved that Solovay and Strassen [12], Miller [9], and Rabin [10] probabilistic algorithms for testing primality are error-free in case the input sequence of coin tosses has maximal information content.

In this paper we shall describe conditions under which a probabilistic algorithm gives the correct output. We shall work with algorithms having the ability to make "random" decisions not necessarily binary (Zimand [13]). We shall prove that if a probabilistic algorithm is sufficiently "correct", then it is error-free on all sufficiently long inputs which are random in Kolmogorov and Martin-Löf's sense. Our result, as well as Chaitin and Schwartz's one, is only of theoretical interest, since the set of all random strings is immune (Calude and Chiţescu [2]).

KEY WORDS: Kolmogorov complexity, Martin-Löf's test, probabilistic algorithm.

C.R. CATEGORY: F.1.1, F.1.2.

1. BASIC NOTIONS

Throughout the paper $\mathbb{N}$ will be the set of all natural numbers, i.e. $\mathbb{N} = \{0, 1, 2, \ldots\}$.

If A is a finite set, then card A will be the number of elements in A.

For every non-empty sets A and B, and for every function $f: A' \to B$ (where $A' \subset A$) we shall write $f: A \xrightarrow{o} B$; we shall say that f is a *partial function* from A to B. We shall assume that $f(x)=\infty$ in case f is not defined in the point x. If $f:A\overset{o}{\rightarrow}B$ is a partial function, then $\mathrm{dom}(f)=\{x\in A \mid f(x)\neq\infty\}$ and range $(f)=\{f(x)\mid x\in\mathrm{dom}(f)\}$. In case we write $f:A\rightarrow B$ it follows that $\mathrm{dom}(f)=A$.

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 under concatenation (with λ the null string). For every x in X^* denote by $l(x)$ the length of x.

We shall consider *partial recursive functions* (*p.r. functions* in the sequel) $\varphi:X^*\times\mathbb{N}\overset{o}{\rightarrow}X^*$, $f:\mathbb{N}\times X^*\overset{o}{\rightarrow}\mathbb{N}$ or $g:\mathbb{N}\overset{o}{\rightarrow}\mathbb{N}$ (for Recursive Function Theory see [11], [7], [1]).

For every p.r. function $\varphi:X^*\times\mathbb{N}\overset{o}{\rightarrow}X^*$, the *Kolmogorov complexity* induced by φ is a function $K_\varphi:X^*\times\mathbb{N}\rightarrow\mathbb{N}\cup\{\infty\}$, defined by $K_\varphi(x\mid m)=\min\{l(y)\mid y\in X^*,\ \varphi(y,m)=x\}$ in case $x=\varphi(y,m)$ for some y in X^*, and $K_\varphi(x\mid m)=\infty$, otherwise. A p.r. function $\psi:X^*\times\mathbb{N}\overset{o}{\rightarrow}X^*$ having the property that for each p.r. function $\varphi:X^*\times\mathbb{N}\overset{o}{\rightarrow}X^*$ there exists a natural c (depending upon ψ and φ) such that $K_\psi(x\mid m)\leqq K_\varphi(x\mid m)+c$, for all x in X^* and $m\geqq 1$, is called a *Kolmogorov universal algorithm*; for the existence see Kolmogorov's Theorem [6] or [3]. Denote by $K=K_\psi$ the complexity induced by a fixed Kolmogorov universal algorithm. A string x in X^* is called *random string* (with respect to ψ) if $K(x\mid l(x))\geqq l(x)$. Random strings do exist (for every ψ and every length).

For every set $W\subset X^*\times\mathbb{N}$ and for every natural $m\geqq 1$ we shall write $W_m=\{x\in X^*\mid (x,m)\in W\}$. A non-empty recursively enumerable set $V\subset X^*\times(\mathbb{N}-\{0\})$ will be called *Martin-Löf test* (see [8] and [3]) if it possesses the following two properties:

1) For every natural $m\geqq 1$, $V_{m+1}\subset V_m$,
2) For every natural numbers m and n, $m\geqq 1$,

$$\mathrm{card}\,\{x\in X^*\mid l(x)=n,\ x\in V_m\}<p^{n-m}/(p-1).$$

We agree upon the fact that the empty set is a Martin-Löf test.

The *critical level* induced by a Martin-Löf test V is a function $m_V:X^*\rightarrow\mathbb{N}$, given by $m_V(x)=\max\{m\geqq 1\mid x\in V_m\}$, if such m exists, and $m_V(x)=0$, in the opposite case. In view of a theorem of Martin-Löf (see [8] or [3]) there exists a Martin-Löf test U (called *universal*) such that for every Martin-Löf test V we can find a natural number i (depending upon U and V) such that $V_{m+i}\subset U_m$, for every $m\geqq 1$. The last inclusion can be written as $m_V(x)\leqq m_U(x)+i$, for all x in X^*.

We shall fix a universal Martin-Löf test U and we shall write $m(x)$ instead of $m_U(x)$. A basic result of Martin-Löf asserts the existence of a natural q (depending upon ψ and U) such that

$$|l(x)-K(x|l(x))-m(x)|\leqq q,$$

for every x in X^* (see [8] or [3]).

A p.r. function $f:\mathbb{N}\times X^*\xrightarrow{o}\mathbb{N}$ is a *probabilistic algorithm* that ε-computes (ε is a recursive real in $[0,1/2]$) the p.r. function $g:\mathbb{N}\xrightarrow{o}\mathbb{N}$ if the following two conditions hold:

a) If $f(n,x)=g(n)\neq\infty$, for some n in $\mathbb{N}$ and x in X^*, then $f(n,xy)=g(n)$, for all y in X^*.

b) For every n in $\operatorname{dom}(g)$, there exists a natural number $t_{\varepsilon,n}$ (which depends upon ε and n) such that

$$\operatorname{card}\{x\in X^*|l(x)=t_{\varepsilon,n}, f(n,x)=g(n)\}>(1-\quad)p^{t_{\varepsilon,n}}.$$

(Remember that $p=\operatorname{card} X$.)

The above definition comes from [5] and [13]. A short motivation will be helpful. When writing $f(n,x)$ we denote by n the input value and by x the encoding of the "random" factor influencing the computation. Condition (a) says that if the algorithm reaches an accepting state, then further random experiments are superflous. Condition (b) asserts that in case of sufficiently long experiments the probability that f computes g is greater than $1-\varepsilon$. Choosing ε in the interval $[0,1/2]$ we assure the uniqueness of the function evaluated by f.

2. RESULTS

LEMMA 1 *Let $f:\mathbb{N}\times X^*\xrightarrow{o}\mathbb{N}$ be a probabilistic algorithm that ε-computes a p.r. function $g:\mathbb{N}\xrightarrow{o}\mathbb{N}$, for some ε in $[0,1/2]$. If n is in* $\operatorname{dom}(g)$ *and*

$$\operatorname{card}\{x\in X^*|l(x)=t, f(n,x)=g(n)\}>(1-\varepsilon)p^t,$$

then for every $r\geqq t$ we have

$$\text{card}\,\{x \in X^* \mid l(x)=r, f(n,x)=g(n)\} > (1-\varepsilon)p^r.$$

Proof We proceed by induction upon $s=r-t$. □

Now let $f:\mathbb{N}\times X^* \to \mathbb{N}$ be a probabilistic algorithm that ε-computes the recursive function $g:\mathbb{N}\to\mathbb{N}$, for some ε in $[0,1/2]$. To each recursive function $h:\mathbb{N}\to\mathbb{N}$ we associate the set

$$W(h)=\{(x,m) \mid x\in X^*, m\in\mathbb{N}-\{0\}, f(h(l(x)),x) \neq g(h(l(x))) \text{ and } \text{card}\,\{y\in X^* \mid l(y)=l(x), f(h(l(y)),y) = g(h(l(y)))\} > (1-p^{-m}/(p-1))p^{l(x)}\}.$$

LEMMA 2 *The set $W(h)$ is a Martin-Löf test.*

Proof Clearly, $W(h)$ is a recursive set. Condition (1) follows from the construction of $W(h)$. Finally,

$$\text{card}\,\{x\in X^* \mid l(x)=j, (x,m)\in W(h)\} \leqq \text{card}\,\{x\in X^* \mid l(x) =j, f(h(j),x)=g(h(j))\} < p^j - (1-p^{-m}/(p-1))p^j = p^{j-m}/(p-1). \quad \square$$

THEOREM 3 *Let $f:\mathbb{N}\times X^*\to\mathbb{N}$ and $g,h:\mathbb{N}\to\mathbb{N}$ be three recursive functions. Assume that:*

a) *The probabilistic algorithm f ε-computes g.*

b) *For every natural n there exist a natural t_n and a recursive real μ_n in $[0,2^{-1}]$ such that*

i) $\lim_n \mu_n = 0$,

ii) $\text{card}\,\{x\in X^* \mid l(x)=t_n, f(n,x)=g(n)\} \geqq (1-\mu_n)p^{t_n}$.

Then there exists a natural n_0 such that for every $n \geqq n_0$ satisfying the condition

iii) *$n=h(l(y))$ and $l(y)\geqq t_n$, for some y in X^*,*

we have

$$f(n,x)=g(n),$$

for every random string x with $n=h(l(x))$.

Proof In view of Lemma 2 one gets a natural $i \geqq 1$ such that

$$m_{W(h)}(z) \leqq m(z) + i,$$

for every z in X^*.

Let q be the constant furnished by the asymptotic relation between the complexity K and the critical level m, and put

$$a_n = [\log_p (1/\mu_n(p-1))] - (q+i+1).$$

In view of (i), there exists a natural n_0 such that $a_n > 0$, for every $n \geqq n_0$. Let $a = a_{n_0}$. We shall prove that for each $n \geqq n_0$, if we can find a string y with $h(l(y)) = n$ and $l(y) \geqq t_n$, then $f(n, x) = g(n)$, for all random strings x such that $h(l(x)) = n$.

We proceed by *reductio ad absurdum*. Suppose x is a random string with $n = h(l(x))$ and $f(n, x) \neq g(n)$. In view of Lemma 1 and (ii) we have

$$\operatorname{card} \{z \in X^* \mid l(z) = l(x), f(n, z) = g(n)\} \geqq (1 - \mu_n) p^{l(x)}.$$

From the construction of the critical level we conclude that $(x, m_{W(h)}(x) + 1) \notin W(h)$. Hence

$$\operatorname{card} \{z \in X^* \mid l(z) = l(x), f(n, z) = g(n)\}$$
$$\leqq (1 - p^{-(m_{W(h)}(x)+1)}/(p-1)) p^{l(x)}.$$

Combining the last two inequalities we obtain the relation

$$\mu_n \geqq p^{-(m_{W(h)}(x)+1)}/(p-1),$$

or equivalently,

$$m_{W(h)}(x) \geqq [\log_p (1/\mu_n(p-1))] - 1.$$

It follows that

$$m(x) \geqq [\log_p (1/\mu_n(p-1))] - (i+1).$$

Finally, again the asymptotic formula between the complexity K and the critical level m enables us to write

$$
\begin{aligned}
K(x \mid l(x)) &\leqq l(x) - m(x) + q \\
&\leqq l(x) + (q + i + 1) - [\log_p(1/\mu_n(p-1))] \\
&= l(x) - a_n \\
&< l(x),
\end{aligned}
$$

because $a_n > 0$. We contradict the randomness of x. $\square$

Remark The consistency of Theorem 3 follows from the fact that Solovay and Strassen, and Miller and Rabin primality tests satisfy the required conditions. To be more precise, we recall the common constructions of these probabilistic algorithms (see also [4]). For every natural n we take k naturals b uniformly distributed in the set $\{1, 2, \ldots, n-1\}$. For each such b we check whether some fixed predicate $w(b, n)$ holds. If so, n is composite; if not, n is prime (with the probability greater than $1-2^{-k}$).

The encoding of the "random" experiment which consists of the selection of the b's in the set $\{1, 2, \ldots, n-1\}$ is binary. For every $I \subset \{1, 2, \ldots, n-1\}$ we consider the binary string $x = x_1 x_2 \ldots x_{n-1}$, where $x_i = 1$ in case $i \in I$, and $x_i = 0$, in the opposite situation. Condition (a) in the definition of a probabilistic algorithm is obviously fulfilled. Condition (b) (for $\varepsilon = 2^{-1}$) holds too, because in case n is prime

$$
\begin{aligned}
\operatorname{card}\{x \in X^* \mid l(x) = n-1, f(n, x) = g(n)\} \\
= 2^{n-1} > (1 - 2^{-1})2^{n-1},
\end{aligned}
$$

and in case n is composite at least half of the b's between 1 and $n-1$ satisfy the predicate $w(b, n)$, i.e.

$$
\begin{aligned}
&\operatorname{card}\{x \in X^* \mid l(x) = n-1, f(n, x) = g(n)\} \\
&= \operatorname{card}\{x \in X^* \mid l(x) = n-1, x_b = 1
\end{aligned}
$$

and $w(b,n)$ holds for some b in

$$\{1,2,\ldots,n-1\}\} \geqq 2^{n-1} - \sum_{k=0}^{n-1} \binom{n-1}{k} 2^{-k}$$

$$= (1-(3/4)^{n-1})2^{n-1} > (1-2^{-1})2^{n-1},$$

for $n \geqq 4$.

Finally we consider the recursive function $h: \mathbb{N} \to \mathbb{N}$, $h(n) = n+1$, and we set for every natural n, $\mu_n = 2^{-[n/3]}$, $t_n = n-1$. Consequently, for almost all natural n and all random strings x with $l(x) = n-1$, the primality tests of Solovay and Strassen, and Miller and Rabin are error-free.

References

[1] C. Calude, *Computational Complexity, Qualitative Aspects*, Editura ştiinţifică şi enciclopedică, Bucureşti, 1982. (Romanian)

[2] C. Calude and I. Chiţescu, Strong noncomputability of random strings. *Internat. J. Comput. Math.* **11** (1982), 43–45.

[3] C. Calude and I. Chiţescu, Random strings according to A. N. Kolmogorov and P. Martin-Löf. Classical approach, *Found. Control Engrg.* **7** (1982), 73–85.

[4] G. J. Chaitin and J. T. Schwartz, A note on Monte Carlo primality tests and algorithmic information theory, *Comm. Pure Appl. Math.* **31** (1978), 521–527.

[5] J. T. Gill, Computational complexity of probabilistic Turing machines, *SIAM J. Comput.* **6** (1977), 675–695.

[6] A. N. Kolmogorov, Three approaches to the quantitative definition of information. *Problemy Peredachi Informatsii* **1** (1965), 1–7. (Russian)

[7] M. Machtey and P. Young. *An Introduction to the General Theory of Algorithms*, North-Holland, Amsterdam, 1978.

[8] P. Martin-Löf, The definition of random sequences, *Inform. and Control* **10** (1966), 602–619.

[9] G. L. Miller, Riemann's hypothesis and tests of primality, *J. Comput. System Sci.* **13** (1976), 300–317.

[10] M. O. Rabin, Probabilistic algorithms. In *Algorithms and Complexity. New Directions and Recent Results*, J. F. Traub (Ed.), Academic Press, New York, 1976, 21–39.

[11] H. Rogers, *Theory of Recursive Functions and Effective Computability*, McGraw-Hill, New York, 1967.

[12] R. Solovay and V. Strassen, A fast Monte-Carlo test for primality, *SIAM J. Comput.* **6** (1977), 84–85; Erratum **7** (1978), 118.

[13] M. Zimand, Complexity of probabilistic algorithms. Preliminary report. *Abstracts of Papers Presented to AMS*. 82 T-68-525 (1982), 547 (also in *Found. Control Engrg.* **8** (1983), 33–49).