ELSEVIER

Information Processing Letters 69 (1999) 115–118

Information Processing Letters

A separation of two randomness concepts ☆

Yongge Wang [1]

Department of Computer Science and Electrical Engineering, University of Wisconsin-Milwaukee, P.O. Box 784, Milwaukee, WI 53201, USA

Received 10 November 1997; received in revised form 10 December 1998
Communicated by P.M.B. Vitányi

Abstract

In this paper we give an affirmative answer to a conjecture by Lutz (1992). That is, we will show that there is a Schnorr random sequence which is not rec-random.

Keywords: Randomness; Martingales

1. Introduction and notation

Schnorr [3] used the martingale concept to give a uniform description of various notions of randomness. In particular, he gave a characterization of Martin-Löf's randomness concept in these terms. Moreover, he criticized Martin-Löf's concept as being too strong and proposed a less restrictive concept as an adequate formalization of the notion of a random sequence. In addition Schnorr introduced an intermediate notion between Martin-Löf and Schnorr randomness which we call rec-randomness. Schnorr left open the question whether rec-randomness is a proper refinement of Schnorr randomness, which was conjectured to be true by Lutz [2]. We will show that rec-randomness is strictly stronger than Schnorr randomness, thereby proving Lutz's conjecture. This question was also mentioned by van Lambalgen [1].

For the most part our notation is standard. We assume that the reader is familiar with the basics of recursion theory.

$\mathbb{N}$, $\mathbb{Q}^+$ and $\mathbb{R}^+$ are the set of natural numbers, the set of nonnegative rational numbers and the set of nonnegative real numbers, respectively. $\Sigma = \{0, 1\}$ is the binary alphabet, Σ^* is the set of (finite) binary strings, Σ^n is the set of binary strings of length n, and Σ^∞ is the set of infinite binary sequences. The length of a string x is denoted by $|x|$. λ is the empty string. For strings $x, y \in \Sigma^*$, xy is the concatenation of x and y. For a sequence $x \in \Sigma^* \cup \Sigma^\infty$ and an integer number $n \geqslant -1$, $x[0..n]$ denotes the initial segment of length $n+1$ of x ($x[0..n] = x$ if $|x| \leqslant n+1$) and $x[i]$ denotes the ith bit of x, i.e.,

$$x[0..n] = x[0] \ldots x[n].$$

Lower case letters $\ldots, k, l, m, n, \ldots, x, y, z$ from the middle and the end of the alphabet will denote numbers and strings, respectively. The letter b is reserved for elements of Σ, and lower case Greek letters $\xi, \eta, \ldots$ denote infinite sequences from Σ^∞. A subset of Σ^* is called a language or simply a set. Italic capital letters are used to denote subsets of Σ^*.

☆ The work reported here is a part of the author's Ph.D. Thesis (Wang, 1996) under the direction of Professor Ambos-Spies at the University of Heidelberg, Germany.

[1] Email: wang@cs.uwm.edu.

0020-0190/99/$ – see front matter
PII: S0020-0190(98)00202-6

2. Definitions

Definition 1. A *martingale* is a function $F:\Sigma^* \to \mathbb{R}^+$ such that, for all $x \in \Sigma^*$,

$$F(x) = \frac{F(x1) + F(x0)}{2}. \tag{1}$$

A martingale F *succeeds* on an infinite sequence $\xi \in \Sigma^\infty$ if $\limsup_n F(\xi[0..n-1]) = \infty$.

Note that in the above definition, the martingales are defined as real-valued functions. In this paper we will mainly use rational-valued martingales unless specified explicitly.

Definition 2 (Schnorr [3]). A *rec-test* is a recursive martingale $F:\Sigma^* \to \mathbb{Q}^+$. An infinite sequence ξ *does not withstand* the rec-test F if F succeeds on ξ. A sequence ξ is *rec-random* if it withstands all rec-tests.

Definition 3 (Schnorr [3]). A *Schnorr test* is a pair (F, h) of functions such that $F:\Sigma^* \to \mathbb{Q}^+$ is a recursive martingale and $h:\mathbb{N} \to \mathbb{N}$ is an unbounded, nondecreasing, recursive function. A sequence ξ *does not withstand* the Schnorr test (F, h) if $F(\xi[0..n-1]) \geqslant h(n)$ i.o. A sequence ξ is *Schnorr random* if it withstands all Schnorr tests.

Theorem 4 (Schnorr [3]). *Every rec-random sequence is also Schnorr random.*

Proof. This follows immediately from the definitions. □

3. Separation of rec-randomness from Schnorr randomness

Theorem 5. *There is a Schnorr random sequence which is not rec-random.*

Proof. We start with some notation. Call a Schnorr test (F, h) *standard* if $F(\lambda) = 1$ and $h(0) = 0$. Let $(F_0, h_0), (F_1, h_1), \ldots$ be an effective enumeration of all pairs of partial recursive functions satisfying, for each $e \in \mathbb{N}$,

$$F_e:\Sigma^* \to \mathbb{Q}^+ \quad \text{and} \quad h_e:\mathbb{N} \to \mathbb{N},$$

and let $(M_0', M_0''), (M_1', M_1''), \ldots$ be the corresponding Turing machines computing those functions. Let $n_0, n_1, \ldots$ be a sequence of numbers such that $(F_{n_0}, h_{n_0}), (F_{n_1}, h_{n_1}), \ldots$ is an enumeration (not effective) of all standard Schnorr tests among the sequence $(F_0, h_0), (F_1, h_1), \ldots$. For the sequence $n_0, n_1, \ldots$, define a "universal" martingale Φ by letting

$$\Phi(x) = \sum_{i=0}^{\infty} 2^{-n_i} F_{n_i}(x).$$

In what follows we will construct a recursive martingale F and a sequence ξ such that, for each e, the following requirements are satisfied.

R: F succeeds on ξ.

N_e: If (F_e, h_e) is a standard Schnorr test, then there exists $c \in \mathbb{N}$ such that, for all $n > c$, $F_e(\xi[0..n-1]) < h_e(n)$.

Note that the requirement R ensures that ξ is not rec-random and the requirements N_e ensure that ξ is Schnorr random. Namely, if ξ is not Schnorr random, then there exists a standard Schnorr test (F_{e_1}, h_{e_1}) such that $F_{e_1}(\xi[0..n-1]) \geqslant h_{e_1}(n)$ i.o., which contradicts the requirement N_{e_1}.

Using the knowledge of the "universal" martingale Φ, it is easy to construct the Schnorr random sequence ξ. However, during our construction, we also want to construct a recursive martingale F which will succeed on ξ. And we cannot effectively decide whether (F_e, h_e) is a standard Schnorr test or not. Hence we cannot decide the construction of ξ recursively. In order to solve this problem, we will use some bits of ξ to code assumptions whether certain (F_e, h_e)'s are standard Schnorr tests or not. That is, in the construction, we define a partial recursive function $d:\Sigma^* \to \Sigma^*$ such that, for a string x on which d is defined, $d(x)$ denotes the following assumptions: For $e < |d(x)|$, we assume that (F_e, h_e) is a standard Schnorr test if and only if $d(x)[e] = 1$. Then ξ will be a "true path", that is, $d(\xi)[m] = 1$ if and only if $m = n_i$ for some $i \in \mathbb{N}$. So it suffices to construct the recursive martingale F in such a way that F succeeds on all sequences η such that there are infinitely many ones in $d(\eta)$.

Construction of ξ, F and d.

Stage 0. Let $F(\lambda) = 1$ and $d(\lambda) = \lambda$.

Stage 1. Let $F(0) = F(1) = 1$, $d(0) = 0$ and $d(1) = 1$. If (F_0, h_0) is a standard Schnorr test then let $\xi[0] = 1$ else let $\xi[0] = 0$.

Stage $s + 1$ ($s > 0$). For each string $x \in \Sigma^s$ such that neither $F(x0)$ nor $F(x1)$ has been defined before stage $s + 1$, we distinguish the following two cases.

Case 1. $d(x)$ has not been defined. Let $F(x0) = F(x1) = F(x)$.

Case 2. $d(x) = b_0 \dots b_k$ has been defined. If, for each $j \leqslant k$ satisfying $b_j = 1$, there exists $m_j \leqslant |x|$ such that $M_j''(m_j)$ stops in $s + 1$ steps and

$$2^{j+|d(x)|+3} F(x) < h_j(m_j), \tag{2}$$

then go to Process 1, else go to Process 2.

Process 1. Let $F(x0) = 0, F(x1) = F(x10) = F(x11) = 2F(x)$, $d(x1) = d(x)$, $d(x10) = d(x)0$, $d(x11) = d(x)1$. If $\xi[0..s-1] = x$, then let $\xi[0..s+1] = \xi[0..s-1]1b$, where $b = 1$ if (F_{k+1}, h_{k+1}) is a standard Schnorr test and $b = 0$ otherwise.

Process 2. Let $F(x0) = F(x1) = F(x)$, $d(x0) = d(x1) = d(x)$. If $\xi[0..s-1] = x$, then let $\xi[0..s] = \xi[0..s-1]b$, where $b = 1$ if $\Phi(x1) \leqslant \Phi(x0)$ and $b = 0$ otherwise.

Note that it is clear by inspection that, prior to each stage $s + 1$, $F(x)$ is defined for all $|x| \leqslant s$, $d(\xi[0..s-1])$ and $\xi[0..s]$ are defined, and for all $e < |d(\xi[0..s-1])|$, $d(\xi[0..s-1])[e] = 1$ if and only if (F_e, h_e) is a standard Schnorr test. Thus F is a rec-test and d is monotone, so the sequence $d(\xi) \in \Sigma^* \cup \Sigma^\infty$ is well-defined.

It remains to verify that the above-constructed F and ξ satisfy the requirements. We establish this by proving a sequence of claims.

Claim 6. *There are infinitely many stages s such that $F(\xi[0..s-1])$ is defined in Process* 1 *of Case* 2.

Proof. We prove this by induction. Given s_0, we have to show that there exists a stage $s > s_0$ such that $F(\xi[0..s-1])$ is defined in Process 1 of Case 2. For each $i < |d(\xi[0..s_0])|$ satisfying $d(\xi[0..s_0])[i] = 1$, (F_i, h_i) is a standard Schnorr test, hence h_i is an unbounded, nondecreasing, recursive function, which implies that there exists some $s > s_0$ such that, at stage $s + 1$, the condition (2) holds for $x = \xi[0..s-1]$. Let s_1 be the least such s. Then $F(\xi[0..s_1])$ is defined in Process 1 of Case 2. This completes the proof of the claim. □

Claim 7. *$d(\xi)[e]$ is defined for all $e \in \mathbb{N}$, and $d(\xi)[e] = 1$ if and only if (F_e, h_e) is a standard Schnorr test. $m = n_i$ for some $i \in \mathbb{N}$.*

Proof. This follows immediately from Claim 6 and the preliminary observation after the construction. □

Claim 8. $\lim_n F(\xi[0..n-1]) = \infty$.

Proof. By Claim 7, $d(\xi[0..s])$ is defined for all $s \in \mathbb{N}$. Hence, at each stage $s + 1$, $F(\xi[0..s])$ is defined in Case 2 of the construction. At stage $s+1$, if $F(\xi[0..s])$ is defined in Process 1 of Case 2, then $F(\xi[0..s]) = 2F(\xi[0..s-1])$; Otherwise $F(\xi[0..s]) = F(\xi[0..s-1])$. By Claim 6, there are infinitely many stages s such that $F(\xi[0..s-1])$ is defined in Process 1 of Case 2. This completes the proof. □

Claim 9. *For each $s \in \mathbb{N}$,*

$$\Phi(\xi[0..s-1]) \leqslant 2^{|d(\xi[0..s-1])|+1} F(\xi[0..s-1]).$$

Proof. We prove the claim by induction on s. For $s = 0$, since $\Phi(\lambda) \leqslant 2$, it is straightforward that $\Phi(\lambda) \leqslant 2^{0+1} F(\lambda)$. The case for $s = 1$ is also similarly straightforward.

For the inductive step, we distinguish the following two cases.

Case 1. At stage $s + 1$, $\xi[0..s]$ is defined in Process 1. Then

$$\begin{aligned}\Phi(\xi[0..s]) &\leqslant 2\Phi(\xi[0..s-1]) \\ &\leqslant 2^{|d(\xi[0..s-1])|+1} 2 \cdot F(\xi[0..s-1]) \\ &= 2^{|d(\xi[0..s])|+1} F(\xi[0..s])\end{aligned}$$

and

$$\begin{aligned}\Phi(\xi[0..s+1]) &\leqslant 2\Phi(\xi[0..s]) \\ &\leqslant 2^{|d(\xi[0..s])|+2} F(\xi[0..s]) \\ &\leqslant 2^{|d(\xi[0..s+1])|+1} F(\xi[0..s+1]).\end{aligned}$$

Case 2. At stage $s + 1$, $\xi[0..s]$ is defined in Process 2. Then

$$\begin{aligned}\Phi(\xi[0..s]) &\leqslant \Phi(\xi[0..s-1]) \\ &\leqslant 2^{|d(\xi[0..s-1])|+1} F(\xi[0..s-1]) \\ &= 2^{|d(\xi[0..s])|+1} F(\xi[0..s]).\end{aligned}$$ □

Claim 10. *For each e, if (F_e, h_e) is a standard Schnorr test, then*

$$2^{e+|d(\xi[0..n-1])|+1}F(\xi[0..n-1]) < h_e(n) \quad a.e.$$

Proof. Let c_1 be large enough such that $|d(\xi[0..c_1-1])| > e$. By the construction, there exist $c_0 > m_e > c_1$ such that

$$2^{e+|d(\xi[0..c_0-1])|+3}F(\xi[0..c_0-1]) < h_e(m_e) \leqslant h_e(c_0).$$

In the following we show by induction that the inequality of the claim holds for all $n > c_0$. For each $s+1 > c_0$, we distinguish the following two cases.

Case 1. At stage $s+1$, $\xi[0..s]$ is defined in Process 1. Then, by the construction, there exists $s_e < s+1$ such that

$$2^{e+|d(\xi[0..s-1])|+3}F(\xi[0..s-1]) < h_e(s_e).$$

So

$$2^{e+|d(\xi[0..s])|+1}F(\xi[0..s]) = 2^{e+|d(\xi[0..s-1])|+2}F(\xi[0..s-1]) < h_e(s_e) \leqslant h_e(s+1)$$

and

$$2^{e+|d(\xi[0..s+1])|+1}F(\xi[0..s+1]) = 2^{e+|d(\xi[0..s-1])|+3}F(\xi[0..s-1]) < h_e(s_e) \leqslant h_e(s+2).$$

Case 2. At stage $s+1$, $\xi[0..s]$ is defined in Process 2. Then

$$2^{e+|d(\xi[0..s])|+1}F(\xi[0..s]) = 2^{e+|d(\xi[0..s-1])|+1}F(\xi[0..s-1]) < h_e(s) \leqslant h_e(s+1). \quad \square$$

Claim 11. *For each e, the requirement N_e is met.*

Proof. If (F_e, h_e) is not a standard Schnorr test, then N_e is met trivially. Otherwise, by Claim 10, let c_0 be large enough so that $2^{e+|d(\xi[0..n-1])|+1}F(\xi[0..n-1]) < h_e(n)$ for all $n \geqslant c_0$.

Then for all $s \geqslant c_0$,

$$F_e(\xi[0..s-1]) \leqslant 2^e\Phi(\xi[0..s-1]) \leqslant 2^{e+|d(\xi[0..s-1])|+1}F(\xi[0..s-1]) \quad \text{(by Claim 9)} < h_e(s). \quad \square$$

These claims taken together complete the proof of Theorem 5. $\square$

Acknowledgements

I would like to thank Professor K. Ambos-Spies, Professor S. Kautz, Professor J. Lutz and Professor E. Mayordomo for many useful discussions and for many useful remarks on a preliminary draft of this paper.

References

[1] M. van Lambalgen, Random sequences, Ph.D. Thesis, University of Amsterdam, 1987.
[2] J.H. Lutz, Almost everywhere high nonuniform complexity, J. Comput. System Sci. 44 (1992) 220–258.
[3] C.P. Schnorr, Zufälligkeit und Wahrscheinlichkeit, Lecture Notes in Math., Vol. 218, Springer, Berlin, 1971.
[4] Y. Wang, Randomness and complexity, Ph.D. Thesis, Universität Heidelberg, 1996.