PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 135, Number 3, March 2007, Pages 861–864
S 0002-9939(06)08541-8
Article electronically published on September 15, 2006

WHEN VAN LAMBALGEN'S THEOREM FAILS

LIANG YU

(Communicated by Julia Knight)

ABSTRACT. We prove that van Lambalgen's Theorem fails for both Schnorr randomness and computable randomness.

To characterize randomness, various definitions of randomness for individual elements of Cantor space have been introduced. The most popular (and maybe the most important) definitions of randomness are Martin-Löf randomness, Schnorr randomness and computable randomness.

We use μ to denote Lebesgue measure on Cantor space 2^ω.

Definition 0.1 (Martin-Löf [7]). (i) Given a set $X \subseteq \omega$, an X-Martin-Löf test is a computable collection $\{V_n : n \in \mathbb{N}\}$ of computably enumerable open sets such that $\mu(V_n) \leq 2^{-n}$.

(ii) Given a set $X \subseteq \omega$, a set Y is said to pass the X-Martin-Löf test if $Y \notin \bigcap_{n\in\mathbb{N}} V_n$.

(iii) Given a set X, a set Y is said to be X-ML-random if it passes all X-Martin-Löf tests.

(iv) A set Y is said to be ML-random if it is $\emptyset$-ML-random.

Definition 0.2 (Schnorr [9]). (i) Given a set $X \subseteq \omega$, an X-Schnorr test $\{V_n : n \in \mathbb{N}\}$ is an X-ML-test such that there is an increasing X-computable function $g : \omega \mapsto \omega$ with $\lim_n g(n) = \infty$ so that $\mu(V_n) = 2^{-g(n)}$.

(ii) Given a set $X \subseteq \omega$, a set Y is said to pass the X-Schnorr test if $Y \notin \bigcap_{n\in\mathbb{N}} V_n$.

(iii) Given a set X, a set Y is said to be X-ML-random if it passes all X-Schnorr tests.

Note one can replace "$Y \notin \bigcap_{n\in\mathbb{N}} V_n$" with "$Y \in V_n$ for at most finitely many V_n's" in item (ii) above. A proof can be found in [4].

Definition 0.3 (Schnorr [9]). (i) Given a set $X \subseteq \omega$, a function $f : 2^{<\omega} \mapsto 2^\omega$ is X-computable if there is an X-computable function $g : \omega \times 2^{<\omega} \mapsto 2^{<\omega}$ so that for each $\sigma \in 2^{<\omega}$, $\lim_n g(n,\sigma) = f(\sigma)$ and for each n and m, $|g(n,\sigma) - g(n+m,\sigma)| < 2^{-n}$.[1]

Received by the editors July 11, 2005 and, in revised form, August 21, 2005 and October 17, 2005.

2000 *Mathematics Subject Classification.* Primary 03D28, 68Q30.

The author was supported by a postdoctoral fellowship from computability theory and algorithmic randomness R-146-000-054-123 in Singapore, NSF of China No.10471060 and No.10420130638. The author thanks the referee for kindly correcting numerous English errors.

[1] One should think of $2^{<\omega}$ as the set of rationals and 2^ω as the set of reals in the interval [0,1].

(ii) A martingale is a function $f : 2^{<\omega} \mapsto 2^{\omega}$ such that for all $\sigma \in 2^{<\omega}$, $f(\sigma) = \frac{f(\sigma^\frown 0)+f(\sigma^\frown 1)}{2}$.
(iii) Given a set $X \subseteq \omega$, a martingale f is called X-computable iff f is an X-computable function.
(iv) Given a set $X \subseteq \omega$, the X-computable martingale f is said to succeed on Y if $\limsup_n f(Y \upharpoonright n) = \infty$.
(v) Given a set $X \subseteq \omega$, a set Y is called X-computably random if no X-computable martingale succeeds on Y.

The motivation for the introduction of these definitions is complex. For further discussion of these reasons and of the controversy on the advantages and disadvantages of the various notions of randomness, see [7], [9], [10], [2]. Each definition has its own reason for being. The problem is which one is the best. Van Lambalgen proved the following result which is well known now as van Lambalgen's Theorem.

Theorem 0.4 (van Lambalgen [10])**.** *If $X, Y \subseteq \omega$, then $X \oplus Y$ is ML-random iff X is ML-random and Y is X-ML-random.*

In both the mathematical and philosophical sense, van Lambalgen's Theorem is extremely important. Mathematically, there exist a large number of applications of van Lambalgen's Theorem in the theory of randomness. Readers can find these in the forthcoming book [3]. Philosophically, a random set should have the property that no information about any part of it can be obtained from another part. In particular, no information about "the left part" of a random set should be obtained from "the right part" and vice versa. In other words, "the left part" of a random set should be "the right part"—random and vice versa.

Hence one way to finish the controversy on which notion of randomness is best is to check which definitions satisfy van Lambalgen's Theorem. We show that Martin-Löf randomness is the only one among the definitions mentioned here that does.

We use "randomness" without any prefix to denote "Martin-Löf randomness" and use "(Schnorr, computable)-randomness" to denote "$\emptyset$-(Schnorr, computable)-randomness". Readers can find all of the necessary material in [3] and [5].

We need some technical results.

Theorem 0.5 (Martin [6])**.** *Let $A_0 \leq_T A_1$. Then $A_0'' \leq_T A_1'$ iff there is an A_1-computable function which dominates every A_0-computable function.*

Theorem 0.6 (Nies, Stephan, Terwijn [8])**.** *For every set A, the following are equivalent.*

- $A' \geq_T \emptyset''$.
- *There is a computably random but not random set $B \equiv_T A$.*
- *There is a Schnorr random but not computably random set $B \equiv_T A$.*

Theorem 0.7 (Schnorr [9])**.** *For any set $X \subseteq \omega$, X-randomness implies X-computable randomness implies X-Schnorr randomness.*

The following lemma is a relativized version of a result in [8].

Lemma 0.8. *If A_0 is A_1-Schnorr-random and $A_1'' \not\leq_T (A_0 \oplus A_1)'$, then A_0 is A_1-random.*

Proof. If not, then $A_0 \in \bigcap_n U_n^{A_1}$ where $\{U_n^{A_1}\}_{n\in\omega}$ is an A_1-Martin-Löf test. Let f be a total $A_0 \oplus A_1$-computable function so that $A_0 \in U_n^{A_1}[f(n)]$ ($U_n^{A_1}[f(n)]$ is a subset of $U_n^{A_1}$ into which each membership is enumerated no later than the stage $f(n)$). By Theorem 0.5, there is an A_1-computable function g so that $g(n) > f(n)$ for infinitely many n's. Define a Schnorr test $\{V_n^{A_1}\}_{n\in\omega}$ so that $V_n^{A_1} = U_n^{A_1}[g(n)]$ for each n. Then $A_0 \in V_n^{A_1}$ for infinitely many n's. So A is not A_1-Schnorr-random. A contradiction. □

A function $f : \omega \mapsto \omega$ is said to be DNC (diagonally noncomputable) if $f(n) \neq \Phi_n(n)$ for each n where $\{\Phi_n : n \in \omega\}$ is an effective enumeration of the partial computable functions.

Theorem 0.9. *Let $B <_T \emptyset'$ be a c.e. set.*

(i) *If $A = A_0 \oplus A_1 \leq_T B$ is Schnorr-random but not random, then A_i is not A_{1-i}-Schnorr-random for each $i \leq 1$.*
(ii) *If $A = A_0 \oplus A_1 \leq_T B$ is computably-random but not random, then A_i is not A_{1-i}-computably-random for each $i \leq 1$.*

Proof. (i) Suppose not. Say A_0 is A_1-Schnorr-random. It is easy to see that both A_i's are Schnorr-random. Note that by Theorem 0.6, $A' \geq_T \emptyset''$. Since $A \leq_T \emptyset'$, in fact, $A' \equiv_T \emptyset''$. Since every random set computes a DNC-function and no DNC-function can be computed by an incomplete c.e. set (Arslanov [1]), neither A_i's can be random. By Theorem 0.6, $A_i' \equiv_T \emptyset''$ for each $i \leq 1$. Hence $A_1'' \equiv_T \emptyset''' >_T \emptyset'' \equiv_T A' \equiv_T (A_0 \oplus A_1)'$. By Lemma 0.8, A_0 is random. Hence $B \equiv_T \emptyset'$. A contradiction.

(ii) By the relativized form of Theorem 0.7, for any set X, every X-computably-random set Y is X-Schnorr-random. So if A is computably random, then A is Schnorr-random. By (i), A_i is not A_{1-i}-Schnorr-random for each $i \leq 1$. So A_i is not A_{1-i}-computably-random for each $i \leq 1$. □

By Theorem 0.6, for every c.e. set B with $B' \geq_T \emptyset''$, there is a set $A \equiv_T B$ which satisfies the assumption in Theorem 0.9. So van Lambalgen's Theorem fails for both Schnorr randomness and computable randomness.

Finally we remark that the other direction of van Lambalgen's Theorem is true for both Schnorr randomness and computable randomness. In other words, if X is Schnorr (computably)-random and Y is X-Schnorr (computably)-random, then $X \oplus Y$ is Schnorr (computably)-random. The proof is just a straightforward modification of the proof of van Lambalgen's Theorem.

References

[1] M. M. Arslanov. Some generalizations of a fixed-point theorem. *Izv. Vyssh. Uchebn. Zaved. Mat.*, (5):9–16, 1981. MR0630478 (82j:03050)

[2] G. J. Chaitin. *Information, randomness & incompleteness*, volume 8 of *World Scientific Series in Computer Science*. World Scientific Publishing Co. Inc., River Edge, NJ, 1990. MR1153671 (92m:01094)

[3] R. Downey and D. Hirschfeldt. *Algorithmic randomness and complexity*. Springer-Verlag, Berlin. To appear.

[4] Rodney G. Downey and Evan J. Griffiths. Schnorr randomness. *J. Symbolic Logic*, 69(2):533–554, 2004. MR2058188 (2005b:03106)

[5] Rodney G. Downey, Denis R. Hirschfeldt, André Nies, and Sebastiaan A. Terwijn. Calibrating randomness. *Bull. Symbolic Logic*. To appear.

[6] Donald A. Martin. Classes of recursively enumerable sets and degrees of unsolvability. *Z. Math. Logik Grundlagen Math.*, 12:295–310, 1966. MR0224469 (37:68)

[7] Per Martin-Löf. The definition of random sequences. *Information and Control*, 9:602–619, 1966. MR0223179 (36:6228)

[8] André Nies, Frank Stephan, and Sebastiaan A. Terwijn. Randomness, relativization and Turing degrees. *J. Symbolic Logic*, 70(2):515–535, 2005. MR2140044

[9] C.-P. Schnorr. A unified approach to the definition of random sequences. *Math. Systems Theory*, 5:246–258, 1971. MR0354328 (50:6808)

[10] M. van Lambalgen. *Random sequences*. Ph.D. Dissertation, University of Amsterdam, 1987.

Department of Mathematics, Faculty of Science, National University of Singapore, Lower Kent Ridge Road, Singapore 117543

E-mail address: yuliang.nju@gmail.com

Current address: Institute of Mathematical Science, Nanjing University, 210093, JiangSu Province, People's Republic of China