Open access • Journal Article • DOI:10.1137/S0097539799357441

Randomness and Recursive Enumerability — Source link

Antonín Kučera, Theodore A. Slaman

Published on: 01 Jan 2002 - SIAM Journal on Computing (Society for Industrial and Applied Mathematics)

Topics: Maximal set, Recursively enumerable set, Recursively enumerable language, Chaitin's constant and Center (category theory)

SIAM J. COMPUT.
Vol. 31, No. 1, pp. 199–211

RANDOMNESS AND RECURSIVE ENUMERABILITY*

ANTONÍN KUČERA† AND THEODORE A. SLAMAN‡

Abstract. One recursively enumerable real α dominates another one β if there are nondecreasing recursive sequences of rational numbers $(a[n] : n \in \omega)$ approximating α and $(b[n] : n \in \omega)$ approximating β and a positive constant C such that for all n, $C(\alpha - a[n]) \geq (\beta - b[n])$. See [R. M. Solovay, *Draft of a Paper (or Series of Papers) on Chaitin's Work,* manuscript, IBM Thomas J. Watson Research Center, Yorktown Heights, NY, 1974, p. 215] and [G. J. Chaitin, *IBM J. Res. Develop.*, 21 (1977), pp. 350–359]. We show that every recursively enumerable random real dominates all other recursively enumerable reals. We conclude that the recursively enumerable random reals are exactly the Ω-numbers [G. J. Chaitin, *IBM J. Res. Develop.*, 21 (1977), pp. 350–359]. Second, we show that the sets in a universal Martin-Löf test for randomness have random measure, and every recursively enumerable random number is the sum of the measures represented in a universal Martin-Löf test.

Key words. random real, Chaitin, Kolmogorov, Ω-number

AMS subject classifications. 68Q30, 03D15

PII. S0097539799357441

1. Introduction.

When is a real number effectively random? To a large extent, this question was answered by the collective efforts of Chaitin [4], Kolmogorov [11], Martin-Löf [14], Schnorr [15], Solomonoff [16], [17], and Solovay [18], among others. We present a brief historical account, based in the most part on [19]. One could also consult [1] or [13].

1.1. Characterizations of effective randomness.

To fix some notation, Σ^* denotes the set of finite binary sequences. For $a \in \Sigma^*$, $|a|$ denotes the length of a and $\langle a \rangle$ denotes the rational number with binary expansion $0.a$. We order Σ^* lexicographically.

Σ^ω denotes the set of all infinite binary sequences. As above, $\langle \alpha \rangle$ denotes the real number with binary expansion $0.\alpha$. We extend the lexicographic ordering of Σ^* to that on Σ^ω.

For $A \subseteq \Sigma^*$, $A\Sigma^\omega$ denotes the open subset of Σ^ω whose elements have an initial segment in A, and $\mu(A\Sigma^\omega)$ denotes the measure of $A\Sigma^\omega$.

We have chosen to work with Σ^* and Σ^ω, as that seemed to work best notationally. We could have worked with $\mathbb{Q}$ and $\mathbb{R}$ just as well and come to the same conclusions. We will refer to elements of $\mathbb{R}$ and to elements of Σ^ω as real numbers.

Characterization by measure. Our first characterizations of effective randomness are based on the hypothesis that an effectively random real should avoid every effectively presented set of measure 0.

DEFINITION 1.1 (Martin-Löf [14]).

1. *A* Martin-Löf randomness test *is a uniformly recursively enumerable sequence* $(A_n : n \geq 1)$ *of subsets of* Σ^* *such that for each* n, $\mu(A_n\Sigma^\omega) \leq 1/2^n$.

*Received by the editors June 21, 1999; accepted for publication (in revised form) March 12, 2001; published electronically July 25, 2001.

http://www.siam.org/journals/sicomp/31-1/35744.html

†Faculty of Mathematics and Physics, Charles University, Malostranské nám. 25, 118 00 Praha 1, Czech Republic (kucera@ksi.mff.cuni.cz).

‡Department of Mathematics, University of California, Berkeley, CA 94720-3840 (slaman@math.berkeley.edu). This author was partially supported by National Science Foundation grant DMS-9500878.

2. *An x in Σ^ω is* Martin-Löf-random *if for every Martin-Löf test $(A_n : n \geq 1)$, $x \notin \bigcap_{n\geq 1} A_n\Sigma^\omega$.*
3. *A Martin-Löf test $(U_n : n \geq 1)$ is* universal *if for every $x \in \Sigma^\omega$, if $x \notin \bigcap_{n\geq 1} U_n\Sigma^\omega$, then x is Martin-Löf-random.*

Note that when we speak of Martin-Löf tests, we will always be referring to tests which are applied to infinite binary sequences. Such tests are also known as sequential Martin-Löf tests to distinguish them from tests applied to finite strings.

A second measure theoretic criterion was proposed by Solovay.

Definition 1.2 (Solovay [18]).

1. *A* Solovay randomness test *is a uniformly recursively enumerable sequence $(A_n : n \geq 1)$ such that the sum $\sum_{n\geq 1} \mu(A_n\Sigma^\omega)$ is convergent.*
2. *An x in Σ^ω is* Solovay-random *if and only if for every Solovay randomness test $(A_n : n \geq 1)$, $\{n : x \in A_n\Sigma^\omega\}$ is finite.*

It is immediate that every Solovay-random real is Martin-Löf-random, and Solovay proved the converse.

Theorem 1.3 (Solovay [18]). *Every x in Σ^ω which is Martin-Löf-random is also Solovay-random.*

Characterization by algorithmic complexity.. Our second characterization of effective randomness is based on the hypothesis that an effectively random sequence should be unpredictable.

Suppose that f is a partial recursive function from Σ^* to Σ^*. We say that f is *self-delimiting* if for all a and b in Σ^*, if f is defined on a and on b, then a and b are incompatible; that is to say that they are not equal and neither string extends the other.

Definition 1.4 (Levin [12], Chaitin [4]). *Suppose that f is a self-delimiting recursive function. We write $f(a)\downarrow$ to indicate that f is defined on argument a.*

1. *The* halting probability *of f is $\sum_{f(a)\downarrow} 1/2^{|a|}$.*
2. *If b is in the range of f, then the* f-complexity *of b is the least length of a string a such that $f(a) = b$. If b is not in the range of f, then the f-complexity of b is ∞. Let $H_f(b)$ denote the f-complexity of b.*

Note the halting probability of a self-delimiting function is a real number between 0 and 1. Consequently, we can use its binary expansion to identify it with an element of Σ^ω. This identification is unique for irrational reals.

Convention 1.5. *In the following, we will make implicit use of the identification between $\mathbb{R}$ and Σ^ω whenever we say that a real number has a property defined only on Σ^ω.*

Definition 1.6 (Chaitin [4]). *A recursive function u is* Chaitin-universal *if and only if the following conditions hold:*

1. *u is self-delimiting.*
2. *For any self-delimiting recursive function f, there is a constant C such that for all a, $H_u(a)$ is less than or equal to $H_f(a) + C$.*

Proposition 1.7 (Chaitin [4]). *There is a recursive function which is Chaitin-universal.*

Definition 1.8 (Chaitin [4]). *An $x \in \Sigma^\omega$ is* Chaitin-random *if there is a recursive function u which is Chaitin-universal and a constant C such that for all n, $H_u(x \upharpoonright n) > n - C$. (Here $x \upharpoonright n$ is the sequence given by the first n values of x.)*

It is straightforward to check that every Martin-Löf-random real is Chaitin-random. Schnorr proved the converse; see [3].

THEOREM 1.9 (Schnorr [15]). *For every $x \in \Sigma^\omega$, if x is Chaitin-random, then x is Martin-Löf-random.*

Since all of the preceding notions of effective randomness coincide, except for historical references, we will drop the prefixes and speak of a real's being random.

Natural examples. Chaitin provided a natural class of random reals.

DEFINITION 1.10 (Chaitin [4]). *A* Chaitin Ω-number *is the halting probability of a universal function u as above.*

THEOREM 1.11.

1. (Chaitin [4]). *Every Ω-number is Chaitin-random.*
2. (Solovay [18]). *Every Ω-number is Solovay-random.*

Consequently, every Ω-number is random.

1.2. Recursive enumerability.

DEFINITION 1.12. *An α in Σ^ω is* recursively enumerable *if there is a nondecreasing sequence $(a[n] : n \in \omega)$ from Σ^* such that $\lim_{n\to\infty} a[n] = \alpha$.*

The Ω-numbers provide natural examples of recursively enumerable reals.

Solovay formulated the following notion for recursive increasing sequences of rational numbers converging to real numbers. We take the liberty of presenting his definition in terms of recursive increasing sequences from Σ^* converging to elements of Σ^ω.

DEFINITION 1.13 (Solovay [18]). *Let $(a[n] : n \in \omega)$ and $(b[n] : n \in \omega)$ be recursive monotonically (lexicographically) increasing sequences from Σ^* which converge to α and β, respectively.*

1. $(a[n] : n \in \omega)$ dominates $(b[n] : n \in \omega)$ *if there is a positive constant C such that for all n in ω, $C(\langle\alpha\rangle - \langle a[n]\rangle) \geq (\langle\beta\rangle - \langle b[n]\rangle)$.*
2. $(a[n] : n \in \omega)$ *is* universal *if it dominates every recursive monotonically increasing sequence from Σ^*.*
3. *α is Ω-like if it is the limit of a universal monotonically increasing recursive sequence from Σ^*.*

Solovay showed that every Ω-number is Ω-like. Additionally, Solovay's proof that every Ω-number is Solovay-random generalizes to Ω-like reals.

THEOREM 1.14 (Solovay [18]). *If α is Ω-like, then α is random.*

Calude et al. [2] sharpened Theorem 1.14 as follows.

THEOREM 1.15 (Calude et al. [2]). *If α is Ω-like, then α is an Ω-number.*

Thus, every Ω-like number is an Ω-number.

Calude et al. [2] posed the natural question, "Is every recursively enumerable random real an Ω-number?" In Theorem 2.1, we show that every recursively enumerable random real is Ω-like and conclude from Theorem 1.15 that the answer to this question is yes.

A second natural class of random reals. Chaitin's Ω-numbers come from universal objects in the complexity theoretic formulation of randomness. Calude et al. [2] raised the question whether the universal objects in the measure theoretic formulation of randomness are also random. They asked, "If $(U_n : n \geq 1)$ is a universal Martin-Löf test, then is $\sum_{n\geq 1} \mu(U_n\Sigma^\omega)$ random?" In Theorem 3.1, we show that the answer is yes. As we discuss below, an equivalent form of this fact was known in the context of recursive analysis.

A dual statement is also true. Theorem 3.3 states that every random recursively enumerable real number is the sum of the measures in a some universal Martin-Löf test.

This paper represents work conducted independently by the authors. Where appropriate, we have indicated places where they came to their solutions to these problems differently.

2. Random recursive enumerability implies Ω-like.

THEOREM 2.1. *Suppose that α is a random recursively enumerable element of Σ^ω. Then α is Ω-like.*

Proof. Let $(a[n] : n \in \mathbb{N})$ be a recursive nondecreasing sequence from Σ^* which converges to α. Let β be recursively enumerable, and let $(b[n] : n \in \mathbb{N})$ be a recursive lexicographically nondecreasing sequence from Σ^* which converges to β.

We show that one of the following two conditions must hold:

1. There is a uniformly recursively enumerable sequence of sets $(A_n : n \in \mathbb{N})$ such that for each n, $A_n \subseteq \Sigma^*$, $\mu(A_n\Sigma^\omega) \leq 1/2^n$, and $\alpha \in A_n\Sigma^\omega$.
2. There is a C such that for all i, $C(\langle\alpha\rangle - \langle a[i]\rangle) \geq (\langle\beta\rangle - \langle b[i]\rangle)$.

Theorem 2.1 follows. If the first condition holds, then α is not random and Theorem 2.1 is verified. Otherwise, the second condition holds and the pair β and $(b[n] : n \in \mathbb{N})$ is not a counterexample to α's being Ω-like. Since β and $(b[n] : n \in \mathbb{N})$ were arbitrary, Theorem 2.1 is verified.

We enumerate A_n by recursion on stages s. Let $A_n[s]$ be the finite set of strings that have been enumerated into A_n during earlier stages than s. Let $s^-[s]$ be the last stage during which we enumerated an element into A_n, or equal to 0, if there was no such earlier stage. If $a[s]$ has an initial segment in $A_n[s]$ or $b[s] = b[s^-[s]]$, then we let $A_n[s+1] = A_n[s]$. Otherwise, let $a[s] + (b[s] - b[s^-[s]])/2^n$ denote the string c such that $\langle c\rangle$ is equal to $\langle a[s]\rangle + (\langle b[s]\rangle - \langle b[s^-[s]]\rangle)/2^n$. We choose a finite antichain $d_1, \dots, d_k$ from Σ^* such that for every d in $[a[s], a[s] + (b[s] - b[s^-[s]])/2^n]$, there is an i such that d is compatible with d_i . We enumerate $d_1, \dots, d_k$ into A_n. In other words, we add the interval from $a[s]$ to $a[s] + (b[s] + b[s^-[s]])/2^n$ to $A_n\Sigma^\omega$. Our intention is that if the approximation to β changed by ϵ, then either α will belong to $A_n\Sigma^\omega$ or the approximation to α must change by an additional amount greater than or equal to $\epsilon/2^n$.

First, we calculate that $\mu(A_n\Sigma^\omega) \leq (\langle\beta\rangle - \langle b[0]\rangle)/2^n$: $A_n\Sigma^\omega$ is a union of a disjoint set of intervals, and the measure of $A_n\Sigma^\omega$ is the sum of the lengths of those intervals. That sum has the form

$$(\langle b[t_1]\rangle - \langle b[0]\rangle)/2^n + (\langle b[t_2]\rangle - \langle b[t_1]\rangle)/2^n + (\langle b[t_3]\rangle - \langle b[t_2]\rangle)/2^n + \dots,$$

where $t_1, t_2, \dots$ is the sequence of stages during which we enumerate intervals into $A_n\Sigma^\omega$. This is a collapsing sum with limit less than or equal to $(\langle\beta\rangle - \langle b[0]\rangle)/2^n$. The inequality could be strict when there are only finitely many terms in the sum. In any event, $\mu(A_n\Sigma^\omega) \leq 1/2^n$.

If α belongs to each $A_n\Sigma^\omega$, then we have condition 1.

Therefore, suppose that n is fixed so that α is not in $A_n\Sigma^\omega$. By our construction, if we enumerate the interval $[a[s], a[s] + (b[s] - b[s^-[s]])/2^n]$ into $A_n\Sigma^\omega$ during stage s, then there is a stage t greater than s such that $\langle a[t]\rangle$ is greater than $\langle a[s]\rangle + (\langle b[s]\rangle - \langle b[s^-[s]]\rangle)/2^n)$.

We claim that for all s, $2^n(\langle\alpha\rangle - \langle a[s]\rangle) \geq (\langle\beta\rangle - \langle b[s]\rangle)$. Fix s and let t_0 be the greatest stage t less than s such that we enumerate something into A_n during stage t or be 0 if there is no such stage. Let $t_0, t_1, \dots$ be the sequence of stages, beginning with stage t_0, during which we enumerate intervals into A_n. Then t_1 is greater than or equal to s and $\langle\alpha\rangle - \langle a[t_1]\rangle$ is greater than the sum $\Sigma_{k=1}^\infty(\langle b[t_k]\rangle - \langle b[t_{k-1}]\rangle)/2^n$. This is another collapsing sum and is equal to $(\langle\beta\rangle - \langle b[t_0]\rangle)/2^n$. Consequently, $\langle\alpha\rangle - \langle a[s]\rangle \geq \langle\alpha\rangle - \langle a[t_1]\rangle \geq (\langle\beta\rangle - \langle b[t_0]\rangle)/2^n \geq (\langle\beta\rangle - \langle b[s]\rangle)/2^n$, as required. □

3. Universal Martin-Löf tests have random measure. Subsequent to our having proven Theorem 3.1, the first author observed that a version of it appears in [6], set in the context of recursive analysis. See Remark 3.5.

THEOREM 3.1. *Let $(U_n : n \geq 1)$ be a universal Martin-Löf test. Then, for each $n \geq 1$, $\mu(U_n\Sigma^\omega)$ is random.*

Proof. We show that for each n, $\mu(U_n\Sigma^\omega)$ is Ω-like and therefore random.

Let U be one of the elements of $(U_n : n \geq 1)$. We note that $\mu(U\Sigma^\omega)$ is less than or equal to $1/2$. Let $U[s]$ denote the set consisting of the first s elements in the enumeration of U. Let $\beta \in \Sigma^\omega$ be recursively enumerable, and let $(b[s] : s \geq 1)$ be a recursive increasing sequence from Σ^* which converges to β.

We will construct a Martin-Löf test $(A_n : n \geq 1)$ so that for all n, $A_{n+1}\Sigma^\omega \subseteq A_n\Sigma^\omega$ and so that one of the following conditions holds:

1. For each n, A_n is finite and $\mu(A_n\Sigma^\omega \setminus U\Sigma^\omega) > 0$.
2. There is a C such that for each s, $C(\mu(U\Sigma^\omega) - \mu(U[s]\Sigma^\omega)) > (\langle\beta\rangle - \langle b[s]\rangle)$.

In the first case, we will obtain a contradiction by showing that $(U_n : n \geq 1)$ is not universal. In the second case, we will show that $(\mu(U[s]\Sigma^\omega) : s \geq 1)$ dominates $(b[s] : s \geq 1)$. Since β and $(b[s] : s \geq 1)$ were arbitrary, $\mu(U\Sigma^\omega)$ is Ω-like, as required.

We construct the sets A_n and several auxiliary functions by recursion on stages s. Our continuing convention is to use the suffix $[s]$ to denote the values of these objects during stage s. For example, $A_n[s]$ denotes the finite subset of Σ^* whose elements were enumerated into A_n before stage s.

In our recursion, if the recursion variable i goes to infinity, then we verify the first disjunct above. If i does not go to infinity in the limit, then its limit infimum i^* is the least index for an infinite element of $(A_n : n \geq 1)$. In this case, U must cover a nonzero fraction of the measure of A_{i^*}. We add measure to each A_n so that we can verify the second disjunct above (where C depends on i^*; see below).

We begin the construction with each A_n empty. During stage 0, we define $m_0[0] = 1/2$, define $A_0 = \{\,()\,\}$, the set whose only element is the null sequence, and say that 0 is active during stage 0. During stage s greater than 0, we begin in step 1 and follow the instructions below until reaching one which requires the end of stage s. Upon the end of stage s, we begin stage $s+1$.

1. Let $m_0[s] = 1/2$, let $A_0[s] = \{\,()\,\}$, and let $i = 1$. Go to step 2.
2. (a) If i has not been active during any previous stage or if all of its previous actions have been canceled, then let $s_i^-[s]$ equal 0.
   (b) Otherwise, let $s_i^-[s]$ be the most recent stage during which i was active.
   Go to step 3.
3. (a) If $s_i^-[s] = 0$ or if $\mu(A_i[s]\Sigma^\omega \setminus U[s]\Sigma^\omega)$ is less than or equal to $d_i[s_i^-[s]]m_{i-1}[s]/2$, then take the following actions.
      i. Set $d_i[s] = (\langle b[s]\rangle - \langle b[s_i^-[s]]\rangle)$ and $m_i[s] = d_i[s]m_{i-1}[s]/2$.

ii. Choose a finite set of strings $F_i[s]$ so that $\mu(F_i[s]\Sigma^\omega)$ is equal to $d_i[s]m_{i-1}[s]$, $F_i[s]\Sigma^\omega$ is a subset of $A_{i-1}[s]\Sigma^\omega$, and $F_i[s]\Sigma^\omega$ is disjoint from $U[s]\Sigma^\omega$. Enumerate the elements of $F_i[s]$ into A_i.

iii. Say that i is active during stage s. For each $j > i$, cancel all of the previous actions for the sake of j.

iv. End the stage s of the recursion.

(b) Otherwise, let $d_i[s] = d_i[s_i^-[s]]$ and $m_i[s] = d_i[s]m_{i-1}[s]/2$. Go to step 4.

4. (a) If i is less than s, then increase the value of i by 1, and go to step 2.

(b) Otherwise, end stage s of the recursion.

Suppose that we reach step 3(a) with $i = n$. If n is equal to 1, then we are required to find a set $F_1[s]$ such that $F_1[s]\Sigma^\omega \subset (\Sigma^\omega \setminus U[s]\Sigma^\omega)$ and $\mu(F_1[s]\Sigma^\omega) = d_1[s]m_0[s]$. Of course, $m_0[s] = 1/2$ and $d_1[s]$ is less than 1. Therefore we must find a set of measure less than $1/2$ in $\Sigma^\omega \setminus U[s]\Sigma^\omega$. Since U belongs to a Martin-Löf test, $\mu(U\Sigma^\omega) \leq 1/2$ and it is possible to find the set $F_1[s]$. If n is greater than 1, then at an earlier point in stage s, we noted that $\mu(A_{n-1}[s]\Sigma^\omega \setminus U[s]\Sigma^\omega)$ is greater than $d_{n-1}[s_{n-1}^-[s]]m_{n-2}[s]/2$. We defined $d_{n-1}[s] = d_{n-1}[s_{n-1}^-[s]]$ and defined $m_{n-1}[s] = d_{n-1}[s]m_{n-2}[s]/2$. Then $d_n[s]m_{n-1}[s] = d_n[s](d_{n-1}[s]m_{n-2}[s]/2)$. Since $d_n[s]$ is less than or equal to 1, this quantity is less than $d_{n-1}[s_{n-1}^-[s]]m_{n-2}[s]/2$, and again it is possible to find the set $F_n[s]$.

We say that n is *injured* during stage s if we cancel all of the previous actions for the sake of n during stage s. Note that 1 is never injured.

Let M_n be the set of stages during which n is active. M_n is naturally divided into intervals by injury to n. If M_n is not empty, then start by letting $\{q_j : j \in Q_n\}$ be an increasing enumeration of the stages s in M_n such that $s_n^-[s]$ is equal to 0. Note that Q_n may be finite or may be all of $\mathbb{N}$. In the case that Q_n is finite with greatest element j, we let q_{j+1} denote infinity and use it to refer to the semi-infinite interval of stages coming after the final injury to n.

To calculate a bound on the measures of the sets $A_n\Sigma^\omega$, we now compute $\sum_{s\in M_n} d_n[s]m_{n-1}[s]$, when n is greater than or equal to 1.

Divide M_n into intervals.

$$\sum_{s\in M_n} d_n[s]m_{n-1}[s] = \sum_{j\in Q_n} \sum_{s\in M_n\cap[q_j,q_{j+1})} d_n[s]m_{n-1}[s].$$

Note that $m_{n-1}[s]$ is constant between q_j and q_{j+1}.

$$= \sum_{j\in Q_n} \left(m_{n-1}[q_j] \sum_{s\in M_n\cap[q_j,q_{j+1})} d_n[s] \right).$$

Identify the collapsing sum.

$$
\begin{aligned}
&= \sum_{j \in Q_n} \left(m_{n-1}[q_j] \sum_{s \in M_n \cap [q_j, q_{j+1})} (\langle b[s] \rangle - \langle b[s_n^-[s]] \rangle) \right) \\
&\leq \sum_{j \in Q_n} m_{n-1}[q_j](\langle \beta \rangle - \langle b[0] \rangle) \\
&\leq \sum_{j \in Q_n} m_{n-1}[q_j].
\end{aligned}
$$

Note that $m_{n-1}[q_j]$ equal to $m_{n-1}[s]$, where s is the greatest stage less than q_j during which $n-1$ was active.

$$
\leq \sum_{s \in M_{n-1}} m_{n-1}[s].
$$

The last inequality could be strict, as there may be stages during which $n-1$ is active which are followed by an injury to $n-1$ before the next stage during which n is active.

We now check by induction that $\sum_{s \in M_n} m_n[s]$ is less than or equal to $1/2^{n+1}$.

Consider the case when n is equal to 0. Then, M_0 is equal to $\{0\}$ and $m_0[0]$ is equal to $1/2$. Consequently, $\sum_{s \in M_0} m_0[s] = 1/2$, as required.

Now, suppose that n is greater than 0. Then, $\sum_{s \in M_n} m_n[s]$ is given by the following:

$$
\sum_{s \in M_n} m_n[s] = \sum_{s \in M_n} d_n[s] m_{n-1}[s]/2.
$$

Move the factor $1/2$ out of the sum, and apply the previous calculation.

$$
\leq \frac{1}{2} \sum_{s \in M_{n-1}} m_{n-1}[s].
$$

Apply induction.

$$
\begin{aligned}
&\leq \frac{1}{2}(1/2^n) \\
&= 1/2^{n+1}.
\end{aligned}
$$

We have the required inequality.

Now, $\mu(A_n \Sigma^\omega)$ is less than or equal to the sum of the measures of the sets $F_n[s]\Sigma^\omega$ for $s \in M_n$. Each $F_n[s]\Sigma^\omega$ has measure $d_n[s]m_{n-1}[s]$. Therefore, $\mu(A_n \Sigma^\omega)$ is less than or equal to $\sum_{s \in M_n} d_n[s] m_{n-1}[s]$, which is less than or equal to $\sum_{s \in M_{n-1}} m_{n-1}[s]$, and hence less than or equal to $1/2^n$, as above.

Thus, $(A_n : n \geq 1)$ is a Martin-Löf test.

Suppose that for each n, n is active only finitely often. Then for each n, there is a stage s during which we execute step 3(a) for $i = n$ for the final time. Therefore, for each n, A_n is finite and $A_n \Sigma^\omega \setminus U \Sigma^\omega$ is a closed set of positive measure. Further, for each n, $A_{n+1}\Sigma^\omega \subseteq A_n\Sigma^\omega$. Since Σ^ω is compact, $\bigcap_{n\geq 1} A_n\Sigma^\omega \setminus U\Sigma^\omega$ is not empty. Thus, $\bigcap_{n\geq 1} A_n\Sigma^\omega$ is not a subset of U, contradicting the universality of $(U_n : n \geq 1)$.

Consequently, there are numbers which are active infinitely often, and we let i^* be the least such number.

The first possibility is that i^* is equal to 1. Consider the action during a stage $s \in M_1$. We add strings to A_1 so that the measure of $A_1\Sigma^\omega \setminus U[s]\Sigma^\omega$ is greater than or equal to $d_1[s]m_0[s]$, where $d_1[s]$ is the amount that the approximation to β has increased since the most recent stage $s_1^-[s]$ during which 1 was active. At the next stage $s_1^+[s]$ in M_1 after s, the measure of $A_1[s_1^+]\Sigma^\omega \setminus U[s]\Sigma^\omega$ is less than $d_1[s]m_0[s]/2 = d_1[s]m_0[0]/2$. Thus, for s in M_1, if the approximation to β increases by $d_1[s]$ during the interval $[s_1^-[s], s)$, then the measure of $U[s_1^+]\Sigma^\omega \setminus U[s]\Sigma^\omega$ is greater than or equal to $d_1[s]m_0[s]/2$. It follows that for every s, $(\langle\beta\rangle - \langle b[s]\rangle) \leq (2/m_0[0])(\mu(U\Sigma^\omega) - \mu(U[s]\Sigma^\omega))$. Thus, every increase in the approximation to β is followed by a proportional increase in the approximation to the measure of U, and so $\mu(U[s]\Sigma^\omega : s \geq 1)$ dominates $(b[s] : s \geq 1)$.

Second, i^* may be larger than 1, but the analysis is completely parallel to that of the previous case. We start from the first stage $s[0]$ in M_{i^*} after i^* is injured for the last time, we add strings to A_{i^*} so that the measure of $A_{i^*}\Sigma^\omega \setminus U[s]\Sigma^\omega$ is greater than or equal to $d_{i^*}[s]m_{i^*-1}[s] = d_{i^*}[s]m_{i^*-1}[s_0]$, and we observe that the measure of $U\Sigma^\omega$ increases by at least half that much during the interval from s to the next stage in M_n. It follows that for every m, $(\langle\beta\rangle - \langle b[m]\rangle) \leq (2/m_{i^*-1}[s_0])(\mu(U\Sigma^\omega) - \mu(U[m]\Sigma^\omega))$.

In either case, U is Ω-like and therefore random. □

The following corollary follows easily.

Corollary 3.2. *Let $(U_n : n \geq 1)$ be a universal Martin-Löf test. Then $\sum_{n\geq 1}\mu(U_n\Sigma^\omega)$ is random.*

Theorem 3.3. *For each recursively enumerable random r in Σ^ω there is a universal Martin-Löf test $(U_n : n \geq 1)$ such that $\langle r\rangle$ is equal to $\sum_{n\geq 1}\mu(U_n\Sigma^\omega)$.*

Proof. We fix a universal Martin-Löf test $(A_n : n \geq 1)$, and construct another $(U_n : n \geq 1)$ based on it so that $\langle r\rangle = \sum_{n\geq 1}\mu(U_n\Sigma^\omega)$. Let $A_n[s]$ denote the finite set of sequences which enter A_n during the first s steps of its enumeration. We may assume that for all n and s, if $s < n$, then $A_n[s]$ is empty. With analogous notation, we will make use of a universal Martin-Löf test $(V_n : n \geq 1)$ and a nondecreasing recursive sequence $(r[s] : s \geq 1)$ with limit r such that for all s, $\sum_{n\geq 1}\mu(V_n\Sigma^\omega) - \sum_{n\geq 1}\mu(V_n[s]\Sigma^\omega)$ is less than $\langle r\rangle - \langle r[s]\rangle$. We first argue that there are such sequences.

For s greater than or equal to 1, let $b[s]$ be the binary string such that the following condition holds:

$$\langle b[s]\rangle = \sum_{s\geq i\geq 1} 2^i \sum_{s\geq j\geq 1} \mu(A_{2i+j+1}[s]\Sigma^\omega).$$

Note that

$$\begin{aligned}
\sum_{s\geq i\geq 1} 2^i \sum_{s\geq j\geq 1} \mu(A_{2i+j+1}[s]\Sigma^\omega) &\leq \sum_{i\geq 1} 2^i \sum_{j\geq 1} \mu(A_{2i+j+1}\Sigma^\omega)\\
&\leq \sum_{i\geq 1} 2^i \sum_{j\geq 1} (1/2^{2i+j+1})\\
&\leq \sum_{i\geq 1} 1/2^{i+1}\\
&\leq 1/2,
\end{aligned}$$

and so there is such a $b[s]$. Let β be $\lim_{s\to\infty} b[s]$. Since r is random, Theorem 2.1 applies and we may let $(r[s] : s \geq 1)$ be a recursive nondecreasing sequence from Σ^* with limit r and let C be constant such that for all s, $\langle\beta\rangle - \langle b[s]\rangle$ is less than $C(\langle r\rangle - \langle r[s]\rangle)$. Now let k be fixed so that 2^k is greater than C. Then for all s,

$$\begin{aligned}
2^k(\langle r\rangle - \langle r[s]\rangle) &> C(\langle r\rangle - \langle r[s]\rangle)\\
&\geq \langle\beta\rangle - \langle b[s]\rangle\\
&= \sum_{i\geq 1} 2^i \sum_{j\geq 1} \mu(A_{2i+j+1}\Sigma^\omega) - \sum_{s\geq i\geq 1} 2^i \sum_{s\geq j\geq 1} \mu(A_{2i+j+1}[s]\Sigma^\omega)\\
&\geq 2^k \sum_{j\geq 1} \mu(A_{2k+j+1}\Sigma^\omega) - 2^k \sum_{s\geq j\geq 1} \mu(A_{2k+j+1}[s]\Sigma^\omega).
\end{aligned}$$

Consequently, for each s,

$$(\langle r\rangle - \langle r[s]\rangle) > \sum_{j\geq 1} \mu(A_{2k+j+1}\Sigma^\omega) - \sum_{s\geq j\geq 1} \mu(A_{2k+j+1}[s]\Sigma^\omega).$$

Then, $(A_{2k+j+1} : j \geq 1)$ is a universal Martin-Löf test such that for all s, $\sum_{j\geq 1} \mu(A_{2k+j+1}\Sigma^\omega) - \sum_{s\geq j\geq 1} \mu(A_{2k+j+1}[s]\Sigma^\omega)$ is less than $\langle r\rangle - \langle r[s]\rangle$.

We first handle the case in which $\langle r\rangle$ is less than $1/2$. Choose m so that

$$\langle r\rangle + \mu(A_{2k+m+1}\Sigma^\omega) < 1/2$$

and so that

$$\langle r\rangle > \sum_{j\geq 1} \mu(A_{2k+m+j+1}\Sigma^\omega).$$

For $n \geq 1$, let $V_n = A_{2k+m+n+1}$. For s greater than or equal to 1, let $v[s]$ be $\sum_{s\geq n\geq 1} \mu(V_n[s]\Sigma^\omega)$, and let v be $\sum_{n\geq 1} \mu(V_n\Sigma^\omega)$. By the estimates given above, for each s, $v - v[s]$ is less than or equal to $\langle r\rangle - \langle r[s]\rangle$.

We now construct our Martin-Löf test $(U_n : n \geq 1)$ so that $V_1 \subseteq U_1$ and for all n greater than 1, $V_n = U_n$.

Assuming that we establish $\sum_{n\geq 1} \mu(U_n\Sigma^\omega) = \langle r\rangle$, then since $\mu(U_1\Sigma^\omega)$ is less than or equal to $\langle r\rangle$ and $\langle r\rangle$ is less than or equal to $1/2$, $(U_n : n \geq 1)$ is a Martin-Löf test. Further, $\cap_{n\geq 1} A_n$ is a subset of $\cap_{n\geq 1} U_n$ and so $(U_n : n \geq 1)$ is universal.

We enumerate U_1 by recursion on stages s. Let $U_1[s]$ be set of strings enumerated into U_1 during stages less than s. Let $u[s]$ be $\mu(U_1[s]\Sigma^\omega) + \sum_{n>1} \mu(V_n[s]\Sigma^\omega)$, and let u be the limit of $u[s]$, as s goes to infinity.

During stage s, if $u[s]$ is less than $\langle r[s]\rangle$, then we enumerate a finite set of strings $F[s]$ into U_1 so that $F[s]\Sigma^\omega \cap U_1[s]\Sigma^\omega = \emptyset$ and $\mu(F[s]\Sigma^\omega)$ is equal to $\langle r[s]\rangle - u[s]$. (Not to ignore a fine point, since $\langle r[s]\rangle$ and $u[s]$ have finite binary expansions, there is such a finite set.) We then enumerate all of the strings that enter V_1 during stage s into U_1.

It remains to check that $u = \sum_{n\geq 1} \mu(U_n\Sigma^\omega)$ is equal to $\langle r\rangle$.

By the construction, for every s, $u[s+1]$ is greater than or equal to $\langle r[s]\rangle$. Consequently, $u \geq \langle r\rangle$.

Since $\sum_{n\geq 1} \mu(V_n\Sigma^\omega) < \langle r\rangle$, there must be a stage s such that $\langle r[s]\rangle \geq v(s)$. At the first such stage, $\langle r[s]\rangle \geq u(s)$ as well. If there are infinitely many stages s during which $\langle r[s]\rangle \geq u[s]$, then $u = \langle r\rangle$, as required. Otherwise, there are only finitely many such stages. We argue that $\langle r\rangle \geq u$ as follows. Let s_0 be the greatest stage s during which $\langle r[s]\rangle \geq u[s]$. At the beginning of stage s_0+1, we add a finite set of elements $F[s_0+1]$ to U_1 so that the measure of $U_1\Sigma^\omega$ is momentarily equal to $\langle r[s_0]\rangle$. Since $u[s] \geq \langle r[s]\rangle$ during every stage s after s_0, we do not add any further elements to U_1 other than those in V_1. Consequently U_1 is equal to $U_1[s_0] \cup F[s_0+1] \cup V_1$. Further, u, which is equal to $\sum_{n\geq 1}\mu(U_n\Sigma^\omega)$, can be written as

$$\begin{aligned} u = \mu\left(\left(U_1[s_0] \cup F[s_0+1]\right)\Sigma^\omega\right) + \sum_{n>1}\mu(V_n[s_0]\Sigma^\omega) \\ + \mu(V_1\Sigma^\omega \setminus (U_1[s_0] \cup F[s_0+1])\Sigma^\omega) + \sum_{n>1}\mu(V_n\Sigma^\omega \setminus V_n[s_0]\Sigma^\omega). \end{aligned}$$

By the choice of $F[s_0+1]$,

$$\mu((U_1[s_0] \cup F[s_0+1])\Sigma^\omega) + \sum_{n>1}\mu(V_n[s_0]\Sigma^\omega) = \langle r[s_0]\rangle.$$

Further, $V_1[s_0] \subseteq U_1[s_0]$ so

$$\begin{aligned} &\mu(V_1\Sigma^\omega \setminus (U_1[s_0] \cup F[s_0+1])\Sigma^\omega) + \sum_{n>1}\mu(V_n\Sigma^\omega \setminus V_n[s_0]\Sigma^\omega) \\ &\quad\leq \mu(V_1\Sigma^\omega \setminus V_1[s_0]\Sigma^\omega) + \sum_{n>1}\mu(V_n\Sigma^\omega \setminus V_n[s_0]\Sigma^\omega) \\ &\quad\leq \sum_{n\geq 1}\mu(V_n\Sigma^\omega) - \sum_{n\geq 1}\mu(V_n[s_0]\Sigma^\omega) \\ &\quad\leq (v - v[s_0]). \end{aligned}$$

Then, however, $u \leq \langle r[s_0]\rangle + (v - v[s_0])$. By the above, $(v - v[s_0])$ is less than or equal to $(\langle r\rangle - \langle r[s_0]\rangle)$. We conclude that u is less than or equal to $\langle r[s_0]\rangle + (\langle r\rangle - \langle r[s_0]\rangle)$; that is, $u \leq \langle r\rangle$, as required.

Next we consider the case when $\langle r\rangle$ is greater than $1/2$. Again, let $(A_n : n \geq 1)$ be a universal Martin-Löf test. Choose $m > 1$ so that $1/2 + \sum_{n>m}\mu(A_n\Sigma^\omega)$ is less than $\langle r\rangle$. Let 0^n denote the sequence with n many 0's. For $n \geq 1$, let V_n be a subset of Σ^* such that $A_{m+n}\Sigma^\omega \cup \{0^{n+1}\}\Sigma^\omega$ is equal to $V_n\Sigma^\omega \cup \{0^{n+1}\}\Sigma^\omega$, and each element of V_n is incompatible with 0^{n+1}. For each n, $\mu(A_{m+n}\Sigma^\omega \cup \{0^{n+1}\}\Sigma^\omega)$ is less than or equal to $\mu(A_{m+n}\Sigma^\omega) + 1/2^{n+1}$, which is less than or equal to $1/2^n$. Now we use the method in the previous construction to find $(U_n : n \geq 1)$ such that the following conditions hold: $\sum_{n\geq 1}\mu(U_n\Sigma^\omega) = \langle r\rangle - 1/2$; for each n, $V_n \subseteq U_n$; and every element of U_n is incompatible with 0^{n+1}.

The last constraint is only relevant to the construction of U_1. In the notation of the previous construction, we may be asked during step $s+1$ to find a set of finite sequences $F[s+1]$ such that the measure of $F[s+1]\Sigma^\omega$ is equal to $(\langle r[s]\rangle - 1/2) - u[s]$ and $F[s+1]\Sigma^\omega \cap U_1[s]\Sigma^\omega = \emptyset$. For $n = 1$, the complement of $\{0^{n+1}\}\Sigma^\omega$ has measure $3/4$, so the measure available for the choice of $F[s+1]$ is greater than or equal to $3/4 - u[s]$. Thus it is always possible to find the set $F[s]$ as required.

Finally, we let U_n^* be $U_n \cup \{0^{n+1}\}$.

Then, $\sum_{n\geq 1}\mu(U_n^*\Sigma^\omega)$ is evaluated as follows:

$$\sum_{n\geq 1}\mu(U_n^*\Sigma^\omega) = \sum_{n\geq 1}\mu(U_n\Sigma^\omega \cup \{0^{n+1}\}\Sigma^\omega).$$

Note that $U_n\Sigma^\omega \cap \{0^{n+1}\}\Sigma^\omega$ is empty.

$$\begin{aligned}
&= \sum_{n\geq 1}\mu(U_n\Sigma^\omega) + \sum_{n\geq 1}\mu(\{0^{n+1}\}\Sigma^\omega)\\
&= \sum_{n\geq 1}\mu(U_n\Sigma^\omega) + 1/2\\
&= (\langle r\rangle - 1/2) + 1/2\\
&= \langle r\rangle. \qquad \square
\end{aligned}$$

Remark 3.4. Theorem 3.1 can also be proved by using the following idea. We first observe that approximating $\mu(U_n\Sigma^\omega)$ by an open set with measure less than ϵ is at least as difficult as approximating $\langle L\rangle$, where L is the least element in Σ^ω which is not in $U_n\Sigma^\omega$. More precisely, let $\langle\alpha\rangle$ denote $\mu(U_n\Sigma^\omega)$. If we were given a Martin-Löf test $(A_n : n \geq 1)$ such that α belongs to $\bigcap_{n\geq 1} A_n\Sigma^\omega$, then we could construct another Martin-Löf test $(B_n : n \geq 1)$ such that L belongs to $\bigcap_{n\geq 1} B_n\Sigma^\omega$. By virtue of L's passing the universal Martin-Löf test $(U_n : n \geq 1)$, L is random, a contradiction. Theorem 3.1 follows.

We sketch the enumeration of $(B_n : n \geq 1)$. For any σ and s, if s is the least such that

$$\sigma \in A_n[s] \text{ and } \langle\sigma\rangle \leq \mu(U_n[s]\Sigma^\omega) < \langle\sigma\rangle + 2^{-|\sigma|},$$

take the following actions. Choose a finite set of strings $G_n[s]$ such that $G_n[s]\Sigma^\omega$ is disjoint from $U_n[s]\Sigma^\omega$, $\mu(G_n[s]\Sigma^\omega) = \langle\sigma\rangle + 2^{-|\sigma|} - \mu(U_n[s]\Sigma^\omega)$; if β is the least element in Σ^ω which is not in $U_n[s]\Sigma^\omega \cup G_n[s]\Sigma^\omega$, then

$$\langle\beta\rangle = \mu(U_n[s]\Sigma^\omega \cap \{\gamma : \gamma < \beta\}) + \mu(G_n[s]\Sigma^\omega).$$

(Observe that such set $G_n[s]$ exists.) Enumerate $G_n[s]$ into B_n.

Roughly speaking, enumerate into B_n a finite set of strings $G_n[s]$ such that $G_n[s]\Sigma^\omega$ presents the leftmost part of the complement of $U_n[s]\Sigma^\omega$ (not necessarily connected) of a total length $\langle\sigma\rangle + 2^{-|\sigma|} - \mu(U_n[s]\Sigma^\omega)$.

Remark 3.5. As we mentioned above, a recursive-analysis version of Theorem 3.1 was proven by [6]. Demuth worked in the Markov/Russian style of constructive mathematical analysis. He studied a behavior of everywhere defined constructive functions of a real variable and, among others, questions of differentiation of such functions. Since random reals from the closed unit interval

1. form a set of measure one,
2. arise by avoiding sets of measure zero from a special class, and
3. can be viewed as "generic,"

one could expect that they would be important in recursive analysis. This is the case and Demuth devoted a considerable amount of effort toward understanding their role there. He started with a rather finitistic approach, and he used a more standard terminology only in his last papers. We briefly survey Demuth's work here, taking the liberty to reformulate his definitions and results into a contemporary terminology.

Demuth [6] studied reals recursive in $\emptyset'$ and defined π_1 and π_2 numbers in that context. According to Demuth, a real x recursive in $\emptyset'$ is a π_1 number if and only if for some (equivalently, for any) recursive sequence of rational numbers $(a[n] : n \in \omega)$ converging to x there is a recursive sequence of finite recursive sets $(C_m : m \in \omega)$

such that $\mu(\bigcup_{s\notin C_m}(\min(a[s],a[s+1]),\max(a[s],a[s+1])))$ is less than 2^{-m}. Dually, x recursive in $\emptyset'$ is a π_2-number if x is not a π_1-number.

In his own terminology, Demuth constructed a universal Martin-Löf test [6, Theorem 2] and showed [6, Theorem 5] that for all x recursive in $\emptyset'$, x is a π_2 number if and only if x is random in the sense of Martin-Löf. We are omitting some details here. Later, Demuth [7] worked with arithmetical reals and defined $\mathcal{A}_1$ and $\mathcal{A}_2$ numbers as natural extensions of π_1 and π_2 numbers. Demuth was not aware that Martin-Löf had formulated these notions earlier.

Finally, Demuth [9] extended these notions to all reals under a different terminology (still not using "randomness"). In [6], he proved, among other things, the following.

(Demuth [6, Lemma 3]). If $r=\sum_{n\in\omega}r_n$, for nonnegative rationals r_n, is a π_1-number (i.e., nonrandom), then $\sum_{n\in C}r_n$ for any recursively enumerable set C is again a π_1-number (no proof was given).

(Demuth [6, Corollary]). Let Q be a recursively enumerable set of strings. If $\mu(Q\Sigma^\omega)$ is a π_1-number and $\mu(Q[s]\Sigma^\omega)$ is less than 1 for all s, then there is a π_1-number x with $0\le x\le 1$ such that $x\notin Q\Sigma^\omega$ (no proof was given).

In other words, if $\mu(Q\Sigma^\omega)$ is not random, then there is a nonrandom real not in $Q\Sigma^\omega$. It follows that if U_n appears as one of the sets in a universal Martin-Löf test, then $\mu(U_n\Sigma^\omega)$ is random.

For more on the massive work of Demuth on recursive analysis one could also consult [10], [8], or [9]. Finally, we note that Demuth also proved several interesting results from a more recursion theoretic point of view in his last papers; see [8], [9], [10]. He also studied various modifications of randomness, again motivated by problems arising in recursive analysis.

Acknowledgments. Slaman wishes to thank Cristian S. Calude and Robert M. Solovay for their advice on this project.

REFERENCES

[1] C. Calude, *Information and Randomness. An Algorithmic Perspective*, Springer-Verlag, Berlin, 1994.

[2] C. S. Calude, P. H. Hertling, B. Khoussainov, and Y. Wang, *Recursively enumerable reals and Chaitin Ω numbers*, in Proceedings of the Symposium on Theoretical Aspects of Computer Science (STACS 98), Springer, Berlin, 1998, pp. 596–606.

[3] G. J. Chaitin, *A theory of program size formally identical to information theory*, J. Assoc. Comput. Mach., 22 (1975), pp. 329–340.

[4] G. J. Chaitin, *Algorithmic information theory*, IBM J. Res. Develop., 21 (1977), pp. 350–359, 496. Reprinted in [5].

[5] G. J. Chaitin, *Information, Randomness, and Incompleteness. Papers on Algorithmic Information Theory*, 2nd ed., World Scientific, River Edge, NJ, 1990.

[6] O. Demuth, *On constructive pseudonumbers*, Comment. Math. Univ. Carolin., 16 (1975), pp. 315–331 (in Russian).

[7] O. Demuth, *On some classes of arithmetical real numbers*, Comment. Math. Univ. Carolin., 23 (1982), pp. 453–465 (in Russian).

[8] O. Demuth, *Reducibilities of sets based on constructive functions of a real variable*, Comment. Math. Univ. Carolin., 29 (1988), pp. 143–156.

[9] O. Demuth, *Remarks on the structure of tt-degrees based on constructive measure theory*, Comment. Math. Univ. Carolin., 29 (1988), pp. 233–247.

[10] O. Demuth, *Remarks on Denjoy sets*, in Proceedings of the Summer School Conference Dedication of the 90th Anniversary of Heyting, Plenum Press, New York, 1990, pp. 267–280.

[11] A. N. Kolmogorov, *Three approaches to the definition of the concept "quantity of information,"* Problemy Peredači Informacii, 1 (1965), pp. 3–11.

[12] L. A. Levin, *Laws of information conservation (non-growth) and aspects of the foundation of probability theory*, Problems Inform. Transmission, 10 (1974), pp. 206–210.
[13] M. Li and P. Vitanyi, *An Introduction to Kolmogorov Complexity and Its Applications*, 2nd ed., Springer-Verlag, New York, 1997.
[14] P. Martin-Löf, *The definition of random sequences*, Information and Control, 9 (1966), pp. 602–619.
[15] C.-P. Schnorr, *Process complexity and effective random tests*, J. Comput. System Sci., 7 (1973), pp. 376–388.
[16] R. J. Solomonoff, *A formal theory of inductive inference.* I, Information and Control, 7 (1964), pp. 1–22.
[17] R. J. Solomonoff, *A formal theory of inductive inference.* II, Information and Control, 7 (1964), pp. 224–254.
[18] R. M. Solovay, *Draft of a Paper (or Series of Papers) on Chaitin's Work ...*, manuscript, IBM Thomas J. Watson Research Center, Yorktown Heights, NY, 1974, p. 215.
[19] R. M. Solovay, *private communication,* 1999.