Some results on effective randomness

(Preliminary version September 2003)

Wolfgang Merkle[1], Nenad Mihailović[1], and Theodore A. Slaman[2]

[1] Ruprecht-Karls-Universität Heidelberg, Institut für Informatik, INF 294, D–69120 Heidelberg, Germany, {merkle|mihailovic}@math.uni-heidelberg.de
[2] University of California, Department of Mathematics, slaman@math.berkeley.edu

Classification: Computational and structural complexity (random sequences, effective measure).

Abstract. We investigate the characterizations of effective randomness in terms of Martin-Löf covers and martingales. First, we address a question of Ambos-Spies and Kučera [1], who asked for a characterization of computable randomness in terms of covers. We argue that computable randomness randomness can be characterized in term of Martin-Löf covers and effective mass distributions on Cantor space.
Second, we show that the class of Martin-Löf random sets coincides with the class of sets of reals that are random with respect to computable martingale processes. This improves on results of Hitchcock and Lutz [14], who showed that the later class is contained in the class of Martin-Löf random sets and is a strict superset of the class of rec-random sets.
Third, we analyze the sequence of measures of sets in a universal Martin-Löf test. Kučera and Slaman [17] showed that any set which appears as the component of a universal Martin-Löf test has measure which is Martin-Löf random. Further, since the sets in a Martin-Löf test are uniformly computably enumerable, so is their sequence of measures. We prove an an exact converse and hence a characterization. We show that if $\alpha_0, \alpha_1, \ldots$ is a uniformly computably enumerable sequence such that for each i, α_i is Martin-Löf random and less than 2^{-i}, then there is a universal Martin-Löf test $M_0, M_1, \ldots$ such that for each i, M_i has measure α_i.

1 Introduction

We investigate into characterizations of effective randomness concepts in terms of Martin-Löf tests and martingales.

After reviewing concepts of effective randomness and measure in Section 2, we consider in Section 3 a question of Ambos-Spies and Kučera [1], who ask for a characterization of computable randomness in terms of tests. We give such a characterization in terms of Martin-Löf tests such that there is an effective probability measure μ where for any index k and any word w, the Lebesgue measure of the kth component of the test within the cylinder generated by w is bounded from above by $\mu(w)/k$.

In Section 4, we show that the class of Martin-Löf random sequences coincides with the class of sequences that are random with respect to computable martingale processes. This improves on one of the main results of Hitchcock and Lutz [ICALP 2002, pp. 549–560], who showed that the latter class is contained in the class of Martin-Löf random sequences and is a strict superclass of the class of rec-random sequences.

Finally, in Section 5, we demonstrate that in the characterization of Martin-Löf randomness by universal Martin-Löf tests, the measure of the individual sets in the universal test can be chosen according to any given sequence of uniformly c.e. and Martin-Löf random reals, i.e., for any such sequence $r_0, r_1, \ldots$ there is a universal Martin-Löf test such that the measure of the kth component is just r_k. This assertion complements the result of Kučera and Slaman [11] that for any universal Martin-Löf test the measure of every component of the test is a Martin-Löf random real (where, trivially, these reals form a uniformly c.e. sequence). In summary, a sequence of reals $r_0, r_1, \ldots$ is random and uniformly c.e. if and only if there is a universal Martin-Löf test $U_0, U_1, \ldots$ such that the measure of $U_k\{0,1\}^\infty$ is r_k. The latter has a similar flavor as the characterization of the Martin-Löf random c.e. reals as the reals that are the halting probability of a universal prefix machine; see Calude [5] for further discussion and references.

1.1 Notation

The notation used in the following is mostly standard, for unexplained notation refer to the surveys and textbooks cited in the bibliography [2, 3, 14].

We consider words over the binary alphabet $\{0,1\}$, the empty word is denoted by λ. If not explicitly stated differently, SETS are sets of words, SEQUENCES are infinite binary sequences and the term CLASS refers to a set of sequences. For any sequence A, let A be equal to $A(0)A(1)\ldots$, i.e., $A(i)$ denotes the $(i+1)$th bit of A. The class of all sequences is referred to as CANTOR SPACE and is denoted by $\{0,1\}^\infty$. The class of all sequences that have a word x as common prefix is called the CYLINDER GENERATED BY x and is denoted by $x\{0,1\}^\infty$. For a set of words W, let $W\{0,1\}^\infty$ be the union of all the cylinders $x\{0,1\}^\infty$ where the word x is in W.

Recall the definition of the LEBESGUE MEASURE (or UNIFORM MEASURE) λ on Cantor space, which describes the distribution obtained by choosing the individual bits of a sequence according to independent tosses of a fair coin.

2 Random sequences

In this section, we review effective random sequences and related concepts that are used in the following. For more comprehensive accounts of effective random sequences and effective measure theory, we refer to the surveys cited in the bibliography [1, 2, 14].

Imagine a player who successively places bets on the individual bits of the characteristic sequence of an unknown sequence A. The betting proceeds in rounds $i = 1, 2, \ldots$. During round i, the player receives as input the length $i-1$ prefix of A and then, first, decides whether to bet on the ith bit being 0 or 1 and, second, determines the stake that shall be bet. The stake might be any fraction between 0 and 1 of the capital accumulated so far, i.e., in particular, the player is not allowed to incur debts. Formally, a player can be identified with a BETTING STRATEGY

$$b : \{0,1\}^* \to [-1,1]$$

where on input w the absolute value of $b(w)$ is the fraction of the current capital that shall be at stake and the bet is placed on the next bit being 0 or 1 depending on whether $b(w)$ is negative or nonnegative.

The player starts with strictly positive, finite capital $d_b(\lambda)$. At the end of each round, in case the current guess has been correct, the capital is increased by this round's stake and, otherwise, is decreased by the same amount. So given a betting strategy b and the initial capital, we can inductively determine the corresponding PAYOFF FUNCTION, or MARTINGALE, d_b by applying the equations

$$d_b(w0) = d_b(w) - b(w) \cdot d_b(w), \qquad d_b(w1) = d_b(w) + b(w) \cdot d_b(w) .$$

Intuitively speaking, the payoff $d_b(w)$ is the capital the player accumulates till the end of round $|w|$ by betting on a sequence that has the word w as a prefix.

Conversely, any function d from words to nonnegative reals that for all words w satisfies the fairness condition

$$d(w) \;=\; \frac{d(w0) + d(w1)}{2} \tag{1}$$

determines an initial capital $d(\lambda)$ and a betting function b.

Definition 1. *A martingale d SUCCEEDS on a sequence A if d is unbounded on the prefixes of A, i.e., if*

$$\limsup_{m\to\infty} \; d(A|\{0,\dots,m\}) \;=\; \infty \; .$$

A martingale d is COMPUTABLE if it is confined to rational values and there is a Turing machine that on input w outputs an appropriate finite representation of $d(w)$. Computable martingales are considered in recursion-theoretical settings [1, 19, 20, 23], while in connection with complexity classes one considers martingales that in addition are computable within appropriate resource-bounds [2, 13, 14, 16].

Definition 2. *A sequence is REC-RANDOM if no computable martingale succeeds on it.*

Definition 3. *A martingale d has the EFFECTIVE SAVINGS PROPERTY if there is a computable function on words such that*

(i) $f(w) \le d(w)$ *for all words* w,
(ii) f *is nondecreasing, i.e.,* $f(w) \le f(v)$ *whenever* w *is a prefix of* v,
(iii) d *wins on a sequence iff* f *is unbounded on the prefixes of the sequence.*

Remark 4 *For every computable martingale d_0 there is a computable martingale d with initial capital 1 that is equivalent to d, i.e., succeeds on exactly the same sequences and has the effective savings property via some computable monotonic function f.*

The construction of the martingale d is well-known and works, intuitively speaking, by putting aside one unit of capital every time the capital reaches a certain threshold, while from then on using the remainder of the capital in order to bet according to the initial martingale.

Besides rec-random sequences, we consider Martin-Löf random sequences [15]. We denote by $\mathrm{W}_0, \mathrm{W}_1, \ldots$ the standard enumeration of the computably enumerable sets [21].

Definition 5. *A class $\mathcal{N}$ is a MARTIN-LÖF NULL CLASS if there exists a computable function $g\colon \mathbb{N} \to \mathbb{N}$ such that for all i*

$$\mathcal{N} \subseteq \mathrm{W}_{g(i)}\{0,1\}^\infty \quad \textit{and} \quad \lambda(\mathrm{W}_{g(i)}\{0,1\}^\infty) \le \frac{1}{2^i} \; . \tag{2}$$

A sequence is MARTIN-LÖF RANDOM if it is not contained in any Martin-Löf null class.

In the situation of Definition 5, we say that the W_i form a MARTIN-LÖF TEST that covers the class $\mathcal{N}$, i.e., a class is covered by a Martin-Löf test if and only if it is a Martin-Löf null class.

By definition, a class $\mathcal{N}$ has uniform measure 0 if there is a sequence of sets $V_0, V_1, \ldots$ such that (2) is satisfied with $\mathrm{W}_{g(i)}$ replaced by V_i. Thus the concept of a Martin-Löf null class is indeed an effective variant of the classical concept of a class that has uniform measure 0 and, in particular, any Martin-Löf null class has uniform measure 0. By σ-additivity and since there are only countably many computable functions, also the union of all Martin-Löf null classes has uniform measure 0, hence the class of Martin-Löf random sequences has uniform measure 1. In fact, it can be shown that the union of all Martin-Löf null classes is again a Martin-Löf null class [5, Section 6.2]. Equivalently, there is a UNIVERSAL MARTIN-LÖF TEST $U_0, U_1, \ldots$ that covers the class of all sequences that are not Martin-Löf random.

3 Characterizing computable randomness by tests

By definition, a sequence is Martin-Löf random if it cannot be covered by a Martin-Löf test $U_0, U_1, \ldots$, i.e., is not contained in the intersection of the classes $U_k\{0,1\}^\infty$. For such a test, for given index k and word w the value

$$m_k^w = \lambda(w\{0,1\}^\infty \cap U_k\{0,1\}^\infty) \tag{3}$$

can be effectively approximated from below by simply enumerating the words in U_k that extend w. In fact, by a result of Kučera [9, 10, Lemma 8.1 and Lemma 2], we can compute a nontrivial upper bound on m_k^w, i.e., one that is strictly less than $1/2^{|w|}$, in case m_k^w is indeed strictly smaller than the latter number. On the other hand, it is known that in case one requires in addition that the m_k^w can be effectively approximated to any given precision, one obtains a characterization of the concept of Schnorr randomness, where the Schnorr random sequences are a strict superclass of the computable random sequences [1, 20, 24].

We show in this section that the concepts of computable random sequence and of computable null class can be characterized by Martin-Löf tests where the m_k^w can be appropriately bounded from above by means of a computable mass distribution on Cantor space. This gives a positive answer to a question of Ambos-Spies and Kučera, who have asked whether computable randomness can be characterized in terms of Martin-Löf tests [1, Open Problem 2.6].

Definition 6. *A* MASS DISTRIBUTION *on Cantor space is a mapping μ from words to reals such that for any word w holds $\mu(w) = \mu(w0) + \mu(w1)$. A* PROBABILITY MEASURE *(on Cantor space) is a mass distribution μ where $\mu(\lambda) = 1$. A mass distribution μ is* COMPUTABLE *if μ is rational-valued and there is an effective procedure that on input w computes $\mu(w)$.*

Mass distributions and martingales are essentially the same concept [8] where, in particular, the additivity condition $\mu(w) = \mu(w0) + \mu(w1)$ corresponds to the fairness condition (1). More precisely, given a mass distribution μ, the function $w \mapsto 2^{|w|}\mu(w)$ is a martingale with initial capital $\mu(\lambda)$ and conversely, given a martingale d, the function $w \mapsto d(w)/2^{|w|}$ is a mass distribution.

Proposition 7. *A class $\boldsymbol{C}$ has computable measure* 0 *if and only if there is a Martin-Löf test $U_0, U_1, \ldots$ and a computable probability measure μ such that*

(i) $\boldsymbol{C}$ is contained in the intersection of the classes $U_k\{0,1\}^\infty$,

(ii) for any k and any word w, the Lebesgue measure of the intersection of the cylinder generated by w with $U_k\{0,1\}^\infty$ is at most $\mu(w)/k$, i.e.,

$$\lambda(w\{0,1\}^\infty \cap U_k\{0,1\}^\infty) \leq \frac{\mu(w)}{k} \; . \tag{4}$$

Proof. First, assume that we are given a class $\boldsymbol{C}$ that has computable measure 0. By Remark 4, pick a computable martingale d that succeeds on every sequence in $\boldsymbol{C}$ and has the effective savings property via some computable, nondecreasing function f. In order to obtain a Martin-Löf test $U_0, U_1, \ldots$ and a probability distribution μ as required, let

$$U_k = \{w | f(w) \geq k, \text{ while } f(v) < k \text{ for all proper prefixes } v \text{ of } w\}, \; \mu(w) = \frac{d(w)}{2^{|w|}}.$$

In order to prove assertion (i), fix any sequence X in $\boldsymbol{C}$. Then d succeeds on X and, in particular, f is unbounded on the prefixes of X; hence for all k there is some prefix of X in U_k and X is contained in the intersection of the $U_k\{0,1\}^\infty$.

In order to prove assertion (ii), fix any index k and word w. First assume that w has some prefix w_0 in U_k. In this case assertion (ii) holds because by construction and assumption on f, we have

$$k \leq f(w_0) \leq f(w) \leq d(w), \qquad \text{hence } \frac{1}{2^{|w|}} \leq \frac{\mu(w)}{k} \; . \tag{5}$$

Next consider any word w that does not have a prefix in U_k and let U_k^w be the set of all words in U_k that extend w. Then assertion (ii) holds because we have

$$\lambda(w\{0,1\}^\infty \cap U_k\{0,1\}^\infty) \leq \sum_{v \in U_k^w} \frac{1}{2^{|v|}} \leq \sum_{v \in U_k^w} \frac{\mu(v)}{k} \leq \frac{\mu(w)}{k} \; ,$$

where the inequalities hold, from left to right, because U_k and hence U_k^w is prefix-free, by (5), and by additivity of probability measures.

Next assume that we are given a Martin-Löf test $U_0, U_1, \ldots$ and a probability measure μ as in the proposition. By the discussion following Definition 6, the function $w \mapsto \mu(w)2^{|w|}$ is a computable martingale, which succeeds on any sequence in $\boldsymbol{C}$ because by assumption any such sequence is contained in the intersection of the $U_k\{0,1\}^\infty$, i.e., has prefixes in all the U_k, where for all words w in U_k we have $\mu(w)2^{|w|} \geq k$ according to (4). □

4 The power of martingale processes

Hitchcock and Lutz [7] remark that the term martingale has different meanings in probability theory and theoretical computer science. In order to compare the two notions, consider Lebesgue measure on Cantor space and for a given function d from words to the real numbers, let ξ_m^d be the random variable defined by $\xi_m^d(X) = d(X(0)\ldots X(m-1))$, i.e., for a a martingale d and a random sequence X chosen uniformly at random, $\xi_0^d(X), \xi_1^d(X), \ldots$ is just the sequence of capital values that are reached on the prefixes of X when betting according to d. The martingale concept from Section 2, which the one usually considered in theoretical computer, can then be equivalently characterized by reformulating the fairness condition (1) as follows. A function d from words to reals is a martingale iff for any word w, the conditional expectation of $\xi^d_{|w|+1}$, given that X extends w, is equal to $\xi^d_{|w|}$, i.e.,

$$\mathbf{E}[\xi^d_{|w|+1} \mid w\{0,1\}^\infty] = \xi^d_{|w|} \tag{6}$$

On the other hand, in probability theory, a sequence $\xi_0, \xi_1, \ldots$ of random variables is called a martingale if for all m, the expectation of ξ_m is finite and

$$\mathbf{E}[\xi^d_{m+1} \mid \xi^d_0 = c_0, \ldots, \xi^d_m = c_m] = \xi^d_m \qquad \text{for all reals } c_0, \ldots, c_{m-1}. \tag{7}$$

Hitchcock and Lutz call a function d from words to reals a MARTINGALE PROCESS iff the sequence $\xi^d_0, \xi^d_1, \ldots$ is a martingale in the sense of probability theory; they remark that in the fairness conditions (6) and (7) for martingales and martingale processes, the average is taken over all sequences with the same *bit history* and the same *capital history*, respectively. Two words have the same bit history if they are identical. With a martingale d understood, two words v and w have the same capital history, $v \approx_d w$ for short, if both words have the same length and we have $d(v') = d(w')$ for any two prefixes v' of v and w' of w that have the same length. The relation $\approx_d$ is an equivalence relation on words and will be called d-equivalence. Condition (8) is an equivalent reformulation of the fairness condition (7) for martingale processes in terms of d-equivalence [7].

$$2 \sum_{\{v\colon v \approx_d w\}} d(v) \quad = \quad \sum_{\{v\colon v \approx_d w\}} [d(v0) + d(v1)] \qquad \text{for all words } w\ . \tag{8}$$

Among other results, Hitchcock and Lutz derive the following facts about martingale processes. Every class that can be covered by a martingale processes is also a Martin-Löf null class. On the other hand, every computable martingale is by definition also a martingale process, and there is a rec-random sequence on which a computable martingale process succeeds. The latter assertion is obtained by proving that the following result of An. A. Muchnik [17, Theorem 9.1] remains true with computable martingale processes in place of nonmonotonic partial computable martingales. If almost all prefixes w of a sequence have Kolmogorov complexity of at most $|w| - \log|w|$, then some nonmonotonic partial computable martingale succeeds on the sequence. These results of Lutz and Hitchcock show that computable martingales are strictly less powerful than computable martingale processes where in turn the latter are at most as powerful as Martin-Löf tests, and that accordingly the concepts of random sequence and of class of measure zero defined in terms of martingale processes are intermediate between the corresponding concepts for computable martingales and Martin-Löf tests. We state in Theorem 9 that martingale processes are in fact as powerful as Martin-Löf tests, hence the corresponding concepts of randomness and measure are the same. In the proof of this theorem, we use a construction of martingale processes that is described in Remark 8.

Remark 8 *Given a computably enumerable set U such that $U\{0,1\}^\infty$ has Lebesgue measure at most $1/2$, there is a computable martingale process d that doubles its initial capital $d(\lambda) = 1$ on every sequence in $U\{0,1\}^\infty$, i.e., every such sequence has a prefix w where $d(w) = 2$. Furthermore, an index for d can be computed from a c.e. index for U.*

In order to construct a martingale process d as required, let $w_1, w_2, \dots$ be an effective enumeration of U and let $\widetilde{U}$ be the set of all words w such that some prefix of w is enumerated into U within at most $|w|$ steps of this enumeration. The set $\widetilde{U}$ is computable and closed under extensions, and $U\{0,1\}^\infty$ coincides with $\widetilde{U}\{0,1\}^\infty$. The martingale process d is defined inductively for words of length $m = 0, 1, \dots$, where $d(\lambda) = 1$. For any word w of length m that is in $\widetilde{U}$, let $d(w) = 2$, while all other words w of length m are assigned identical values $d(w)$ in such a way that the fairness condition for martingale processes is not violated. The latter is alway possible because the Lebesgue measure of $U\{0,1\}^\infty$ is at most $1/2$, details are left to the reader.

It remains to show that d is a martingale process, which amounts to show for any given word w that the equation in the fairness condition (7) is satisfied. By construction, first, we have $d(v) = 2$ for all extensions of v of any word w where $d(w) = 2$, hence if $d(w) = 2$, then $d(w0) = d(w1) = 2$ and the same holds for all words v that are d-equivalent to w; the equation in the fairness condition follows. Second, an easy induction shows that all strings w of the same length such that $d(w)$ differs from 2 are d-equivalent. But for the words w in such an equivalence class, the values $d(w0)$ and $d(w1)$ are simply chosen such that the fairness condition is not violated.

Theorem 9. *A class can be covered by a martingale process if and only if it is Martin-Löf null class. In particular, a sequence is random with respect to martingale processes if and only if it is Martin-Löf random.*

Proof. The second assertion in the theorem follows from the first one because for both concepts of randomness involved, a sequence R is random iff the singleton class $\{R\}$ can be covered by an admissible martingale. Concerning the first assertion, recall that Lutz and Hitchcock [7] have shown that any class on which a martingale process succeeds is a Martin-Löf null class. So it suffices to show that there is a martingale process d that succeeds on the class covered by some universal Martin-Löf test $U_0, U_1, \dots$.

For any word w, let

$$V_w = \{u \in U_{|w|+1} \colon u = wv \text{ for some } v\}\ , \qquad V_w^- = \{v \colon wv \in V_w\}\ . \tag{9}$$

The Lebesgue measure of $U_{|w|+1}\{0,1\}^\infty$ is at most $1/2^{|w|+1}$, thus the Lebesgue measure of V_w^- is at most $1/2$ and similar to the construction in Remark 8 we obtain a martingale process d_w^- that doubles its initial capital 2^k on all words in V_w^-. Then

$$d_w^k(u) = \begin{cases} d_w^-(v) & \text{in case } u = wv, \\ 2^k & \text{in case } w \text{ is not a prefix of } w. \end{cases}$$

is a computable martingale process that attains on λ, as well as on w the value 2^k and which doubles the latter capital on any sequence in $V_w\{0,1\}^\infty$. In fact attains $d_w^-(v)$ attains the value 2^{k+1} on any sequence in $U_{|w|+1}\{0,1\}^\infty$ that extends w because $U_{|w|+1}$ cannot contain words of length less than $|w| + 1$.

The martingale process d we are looking for can be viewed as working in phases $s = 1, 2, \dots$, where during phase k it copies the values of some martingale process of the form $d(w, k)$. For a given sequence X, the phases are as follows. During the first phase, d agrees with $d(0, \lambda)$, this phase lasts up to and including the least prefix w_2 of X such that the latter martingale attains the value 2, i.e., has doubled its initial capital. The second phase starts at w_1, there overlapping with the first phase; the second phase lasts up to and including the least prefix w_2 of X on which $d(w_1, 1)$ has doubled. The further phases are similar, i.e., during phase k, the martingale process d agrees with $d(w_k, k)$, and phase k ends and phase $k+1$ starts as soon as the capital has reached 2^{k+1} at word w_{k+1}. By construction, d is computable and is unbounded on any sequence that is contained in all the $U_k\{0,1\}^\infty$.

It remains to show that d is a martingale process. Any d-equivalence class is the disjoint union of finitely many $d(w_k, k)$-equivalence classes where d agrees on each such class with the corresponding martingale process $d(w_k, k)$; hence d satisfies the fairness condition for martingale processes because all these $d(w_k, k)$ satisfy this condition. □

5 Universal Martin-Löf tests

Definition 10. *A* COMPUTABLY ENUMERABLE REAL, C.E. REAL *for short, is a real which is the limit of a nondecreasing computable sequence of rational numbers.*

A real is MARTIN-LÖF RANDOM, RANDOM *for short, if its binary expansion has the form $0.R(0)R(1)\ldots$ for some Martin-Löf random sequence R.*

A real is a CHAITIN Ω REAL *if it is the halting probability of some universal prefix-free Turing machine.*

Definition 11 (Solovay [22]). *Let $(a^s : s \geq 0)$ and $(b^s : s \geq 0)$ be computable sequences of rationals which converge nondecreasingly to α and β, respectively.*

1. $(a^s : s \geq 0)$ DOMINATES $(b^s : s \geq 0)$ *if there is a positive constant c such that for all $s \geq 0$, $c(\alpha - a^s) > (\beta - b^s)$.*
2. $(a^s : s \geq 0)$ *is* UNIVERSAL *if it dominates every computable nondecreasing sequence of rationals.*
3. α *is* Ω-LIKE *if it is the limit of a universal nondecreasing computable sequence if rationals.*

By a celebrated result, which Calude [5] attributes to work of Calude, Hertling, Khoussainov, and Wang, of Chaitin, of Kučera and Slaman, and of Solovay, a c.e. real is random iff it is Chaitin Ω real iff it is Ω-like; for proofs and references see Calude [5].

Among other results, Kučera and Slaman [11] show, first, that for any universal Martin-Löf test $U_0, U_1, \ldots$, the Lebesgue measure of the classes $U_k\{0,1\}^\infty$ are Martin-Löf random reals and, second, that given any c.e. Martin-Löf random real r there is a universal Martin-Löf test such that the sum of the measures $U_k\{0,1\}^\infty$ is r. These results are complemented by Theorem 15 below, the main result of this section, which states that for any sequence $r_0, r_1, \ldots$ of reals that are random and uniformly c.e., there is a universal Martin-Löf test $U_0, U_1, \ldots$ such that the Lebesgue measure of $U_k\{0,1\}^\infty$ is just r_k. Furthermore, the proof of Theorem 15 can be adapted to yield a simplified proof of the second mentioned result by Kučera and Slaman.

Remark 12. In their proof that every c.e. random real is Ω-like, Kučera and Slaman [11, Theorem 2.1] actually show that for any real r that is random and c.e. there is not just some computable universal sequence that converges nondecreasingly to r but in fact any computable universal sequence that converges nondecreasingly to r is universal.

With an enumeration of a computably enumerable set U understood, we write U^s for the set of words that enter U during the first U steps of the enumeration, and we write u and u^s for the Lebesgue measure of $\lambda(U\{0,1\}^\infty)$ and $\lambda(U^s\{0,1\}^\infty)$, respectively.

Lemma 13. *Let r be a c.e. random real and let $(r^s : s \geq 0)$ be any universal sequence that converges to r. Let $(U_j : j \geq 1)$ be a universal Martin-Löf test with uniform computable enumerations $(U_j^s : j \geq 1)$ such that U_j^s is empty in case $s \leq j$. Then there is an index k such that for every stage s,*

$$r - r^s > \sum_{j \geq k} (u_j - u_j^s).$$

Proof. Choose a computable, nondecreasing, and unbounded sequence $(c_j : j \geq 1)$ of positive rationals such that

$$\sum_{j \geq 1} c_j 2^{-j} < \infty \ , \text{ hence } \sum_{j \geq 1} c_j u_j < \infty$$

by the measure condition on the components of a Martin-Löf test. We then have that $\widetilde{u} = \sum_j c_j u_j$ is finite and thus is a c.e. real with approximation

$$\widetilde{u}^s = \sum_{j=1}^{s} c_j u_j^s = \sum_{j=1}^{\infty} c_j u_j^s \ .$$

Accordingly, by Remark 12 and assumption on r and the r^s, there is a nonzero constant c such that for every stage s,

$$c(r - r^s) > u - \widetilde{u}^s = \sum_{j=1}^{\infty} c_j u_j - \sum_{j=1}^{\infty} c_j u_j^s = \sum_{j=1}^{\infty} c_j (u_j - u_j^s)$$

Since the sequence $(c_j : j \geq 1)$ is unbounded, we may let k be the minimal index such that $c < c_k$. Then we have

$$r - r^s > \frac{1}{c} \sum_{j \geq k} c_j (u_j - u_j^s) > \frac{c_k}{c} \sum_{j \geq k} (u_j - u_j^s) > \sum_{j \geq k} (u_j - u_j^s),$$

and the lemma is proved. □

Remark 14 *The assertion of Lemma 13 does not depend on the special bounds $1/2^k$ on the measure u_k of the sets $U_k\{0,1\}^\infty$; indeed, the Lemma holds by essentially the same proof for any uniformly c.e. sequence $(U_k : k \geq 0)$ of sets such that there are computable sequences $(q^k : k \geq 1)$ and $(c^k : k \geq 1)$ such that the c^k are nondecreasing and unbounded,*

$$u^k < q^k \text{ for all } k \ , \qquad \text{and} \qquad \sum_{k \geq 1} c^k q^k < \infty \ .$$

Theorem 15. *Let $(r_n : n \geq 1)$ be a uniformly c.e. sequence of random reals with $r_n < 2^{-n}$ for every n. Then there is a universal Martin-Löf test $(A_n : n \geq 1)$ such that for each n, $\lambda(A_n\{0,1\}^\infty) = r_n$.*

Proof. We enumerate the components of the universal test $(A_n : n \geq 1)$ by recursion such that the enumeration is uniform in the enumeration of the given random reals $(r_n : r \geq 1)$. Hence, for the sake of notational simplicity, in the construction of a component A_n we drop the index n and just write A. Also r_n is abbreviated to r.

By Remark 12, we may let $(r^s : s \geq 0)$ be a universal nondecreasing computable sequence of rationals that converges to r. Fix a universal Martin-Löf test $(U_k : k \geq 0)$. It may be assumed that for all k and s, if $s < k$, then U_k^s is empty.

We enumerate A by recursion on stages s. The construction can be roughly described as follows. At each stage s, we try to enumerate as many words from U into A as possible such that the measure of $A\{0,1\}^\infty$ does not become greater than r^s. More precisely, try to enumerate all of U_s^s, then all of U_{s-1}^s etc. into A. Consider the case in which $m \geq 1$ is the greatest index such that the measure of the union of $A\{0,1\}^\infty$ and $U_m^s\{0,1\}^\infty$ is greater than r^s. Then we compute a subclass of $U_m^s\{0,1\}^\infty$ that, after entering A, increases the measure of $A\{0,1\}^\infty$ to r^s.

At stage s, let $m \leq s$ be the minimal index such that

$$l^s := \lambda\left(\left(A^{s-1} \cup \bigcup_{j\geq 0} U_{m+j}^s\right)\{0,1\}^\infty\right) \leq r^s.$$

Enumerate $U_m^s, U_{m+1}^s, \ldots, U_s^s$ into A. If $l^s = r^s$, then we are done. Now suppose otherwise. Then we have to make the set A bigger in order to make the measure of $A^s\{0,1\}^\infty$ equal to r^s.

We first handle the case in which $m = 1$. Choose any set $F(s)$ of measure $r^s - l^s$ such that each word contained in it is incomparable with any word enumerated into A so far. We enumerate $F(s)$ into A.

Next consider the case where $m > 1$. If possible, let w be a word in U_{m-1}^s such that the measure of the union of $A\{0,1\}^\infty$ and $w\{0,1\}^\infty$ is greater than r^s. If there is no such word w, we can easily enlarge A in a finite number of steps such that there is one. Namely, successively enumerate words from U_{m-1}^s into A such that the measure of $A\{0,1\}^\infty$ is increased but never exceeds r^s. Now fix a word w in U_{m-1}^s such that the measure of the union of $A\{0,1\}^\infty$ and $w\{0,1\}^\infty$ is greater than r^s. Let d denote the difference between r^s and the measure of (the enlarged set) $A\{0,1\}^\infty$. We may suppose that the rational d is given by its dyadic representation, in which there are only finitely many digits different from zero. Now it is easy to see that there is a set E of words of equal length which extend w such that for a suitable subset E' of E, the measure of $(A \cup E')\{0,1\}^\infty$ is r^s. Note that it suffices to choose the set E such that the words contained in it are longer than any word in A and longer than t, where 2^t is the denominator of the dyadic representation of d. Enumerate E' into A. This concludes the construction of the set A, and hence of $(A_n : n \geq 1)$.

By the hypothesis above, the construction of A is based on a universal nondecreasing computable sequence $(r^s : s \geq 0)$ of rationals that converges to r. By construction, the measure of $A\{0,1\}^\infty$ is increased at every stage s by $r^s - r^{s-1}$, hence we have

$$\lambda(A\{0,1\}^\infty) = r. \tag{10}$$

We now argue that there is an index k such that

$$A\{0,1\}^\infty \supseteq \bigcup_{j\geq 0} U_{k+j}\{0,1\}^\infty. \tag{11}$$

Observe that it is enough to show that there are an index k and infinitely many stages s such that

$$A^s\{0,1\}^\infty \supseteq \bigcup_{j\geq 0} U_{k+j}^s\{0,1\}^\infty. \tag{12}$$

Since $(U_k : k \geq 0)$ is a universal Martin-Löf test and $(r^s : s \geq 0)$ is a universal sequence of rationals, we may apply Lemma 13. Hence, let k be an index such that at every stage s,

$$r - r^s > \sum_{j \geq k} \Big(\lambda\big(U_j\{0,1\}^\infty\big) - \lambda\big(U_j^s\{0,1\}^\infty\big) \Big). \tag{13}$$

Certainly $s = k - 1$ is a number such that (12) is satisfied. Now let s be any such number. Then there is a $t > s$ such that (12) with s replaced by t is also true. Namely, let $v > s$ be minimal such that

$$r^v - r^s > \sum_{j \geq k} \Big(\lambda\big(U_j^v\{0,1\}^\infty\big) - \lambda\big(U_j^s\{0,1\}^\infty\big) \Big).$$

Note that such a number v exists by (13) and because the sequence $(r^s : s \geq 0)$ converges to r. Then either for $t = v$ we have

$$A^t\{0,1\}^\infty \supseteq \bigcup_{j \geq 0} U_{k+j}^t\{0,1\}^\infty, \tag{14}$$

or there is an index $j \geq k$ such that $A^v\{0,1\}^\infty \not\supseteq U_j^v\{0,1\}^\infty$. But then there must be a stage t between s and v such that a word not in any of the sets $U_k^t\{0,1\}^*, U_{k+1}^t\{0,1\}^*, \ldots$ is enumerated into A during stage t. This can only be the case if also all components $U_k^t, U_{k+1}^t, \ldots$ are enumerated into A during stage t, i.e., (14) is satisfied again. This shows that there are infinitely many stages s such that (12) is satisfied, which in turn shows that (11) is true.

In summary, a uniformly c.e. sequence $(A_n : n \geq 1)$ was constructed such that for each set $A = A_n$ and for the corresponding random real $r = r_n$, the conditions (10) and (11) are satisfied. By (11), the intersection of all $U_k\{0,1\}^\infty$ is a subclass of the intersection of all $A_n\{0,1\}^\infty$. Since $(U_k : k \geq 1)$ is a universal test by hypothesis, we thus have that $(A_n : n \geq 1)$ is a universal Martin-Löf test, too. By (10), the measure of each $A_n\{0,1\}^\infty$ is equal to r_n. □

Remark 16 *From the proof of Theorem 15, we obtain a somewhat simpler proof of the result of Kučera and Slaman [11] that given any c.e. Martin-Löf random real r there is a universal Martin-Löf test such that the sum of the measures $U_k\{0,1\}^\infty$ is r. Such a test can be constructed similar to the construction of the set A in in the proof of Theorem 15, except that now words that correspond to different components U_k are put into different components of the constructed test and that we can assume that we know the index k, hence we never have to add words corresponding to components with an index less than k.*

References

1. K. Ambos-Spies and A. Kučera. Randomness in computability theory. In P. A. Cholak et al. (eds.), *Computability Theory and Its Applications. Current Trends and Open Problems.* Contemporary Mathematics 257:1–14, American Mathematical Society (AMS), 2000.
2. K. Ambos-Spies and E. Mayordomo. Resource-bounded measure and randomness. In A. Sorbi (ed.), *Complexity, Logic, and Recursion Theory*, p. 1-47. Dekker, New York, 1997.
3. J. L. Balcázar, J. Díaz, and J. Gabarró. *Structural Complexity I*, Springer, 1995.
4. C. S. Calude, *Information and Randomness*, Springer-Verlag, 1994.
5. C. S. Calude. *A characterization of c.e. random reals.* Theoretical Computer Science 271:3-14, 2002.
6. R. Durrett. *Essentials of Stochastic Process*, Springer, 1999.
7. J. M. Hitchcock and J. H. Lutz Why computational complexity requires stricter martingales. Theory of computing systems, to appear. A preliminary version appeared in P. Widmayer et al. (eds.), 29th International Colloquium on Automata, Languages and Programming, Lecture Notes in Computer Science 2380:549–560, Springer, 2002.
8. J. M. Hitchcock. Small Spans in Scaled Dimension. Technical report cs.CC/0304030, Computing Research Repository, 2003.
9. A. Kučera. Measure, Π^0_1-classes and complete extensions of PA. In: H.-D. Ebbinghaus et al. (eds.), *Recursion Theory Week.* Lecture Notes in Mathematics 1141:245-259, Springer, 1985.
10. A. Kučera. On the use of diagonally nonrecursive functions. In: H.-D. Ebbinghaus et al. (eds.), *Logic Colloquium '87.* Studies in Logic and the Foundations of Mathematics 129:219-239, North-Holland, 1989.
11. A. Kučera and T. A. Slaman. *Randomness and recursive enumerability.* SIAM Journal on Computing, 31(1):199–211, 2001.
12. M. Li and P. Vitányi. *An Introduction to Kolmogorov Complexity and Its Applications*, second edition. Springer, 1997.
13. J. H. Lutz. Almost everywhere high nonuniform complexity. *Journal of Computer and System Sciences*, 44:220–258, 1992.
14. J. H. Lutz. The quantitative structure of exponential time. In L. A. Hemaspaandra and A. L. Selman (eds.), *Complexity Theory Retrospective* II, p. 225–260, Springer, 1997.
15. P. Martin-Löf. The definition of random sequences. *Information and Control* 9(6):602–619, 1966.
16. E. Mayordomo. *Contributions to the Study of Resource-Bounded Measure.* Doctoral dissertation, Universitat Politècnica de Catalunya, Barcelona, Spain, 1994.
17. An. A. Muchnik, A. L. Semenov, and V. A. Uspensky. Mathematical metaphysics of randomness. *Theoretical Computer Science* 207:263–317, 1990.
18. P. Odifreddi. *Classical Recursion Theory.* North-Holland, Amsterdam, 1989.
19. C.-P. Schnorr. A unified approach to the definition of random sequences. *Mathematical Systems Theory*, 5:246–258, 1971.
20. C.-P. Schnorr. *Zufälligkeit und Wahrscheinlichkeit.* Lecture Notes in Mathematics 218, Springer, 1971.
21. R. I. Soare. *Recursively Enumerable Sets and Degrees.* Springer, 1987.
22. 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.
23. S. A. Terwijn. *Computability and Measure.* Doctoral dissertation, Universiteit van Amsterdam, Amsterdam, Netherlands, 1998.
24. Y. Wang. A Separation of two randomness concepts. *Information Processing Letters*, 69:115–118, 1999.