LOWNESS AND Π_2^0 NULLSETS

ROD DOWNEY, ANDRE NIES, REBECCA WEBER, AND LIANG YU

Abstract. We prove that there exists a noncomputable c.e. real which is low for weak 2-randomness, a definition of randomness due to Kurtz, and that all reals which are low for weak 2-randomness are low for Martin-Löf randomness.

1. Introduction

In this paper we are concerned with a concept of randomness due to Kurtz in his thesis [9]. Instead of defining randomness as avoidance of measure-zero sets, as in the work of Martin-Löf, Kurtz defined it in terms of membership in measure-one sets, an idea of having all typical properties rather than lacking all special properties.[1]

Definition 1.1 (Kurtz [9]). *A real α is* weakly n-random *(w-n-random, Kurtz n-random) if it is a member of all Σ_n^0 classes of measure one.*

The name reflects that in the $n = 1$ case this is a weaker condition than Martin-Löf randomness. In fact, weak $(n+1)$-randomness implies n-randomness (the relativization of Martin-Löf randomness) and n-randomness implies weak n-randomness, and neither converse holds. Note that Gaifman and Snir's definition of Σ_n-randomness [5], made independently, is the same as weak n-randomness when restricted to the appropriate language and coin-toss probability. They give a similarly broadened version of Martin-Löf randomness, and state that the relationship above between the two holds for the fully general definitions.

The work of Downey, Griffiths and Reid [1], of Kurtz and of Jockusch in [9] extensively explores characterizations of w-1-randomness, Turing degrees of w-1-random reals, and reals which are low for w-1-randomness (defined below). However, w-n-randomness is less well-studied, with the primary results in the theses of Kurtz [9] and later Kautz [6] and Wang [16].

This paper is concerned with weak 2-randomness, which perhaps should be called *strong 1-randomness*, since it seems the first level in the Kurtz hierarchy where *typical* randomness behavior occurs. From the definition above α will be weakly 2-random iff α is in all Σ_2^0 classes of measure 1.

The first and third authors' research was supported by the Marsden Fund of New Zealand, via postdoctoral fellowships. The second author was partially supported by Marsden Fund grant No. 03-UOA-130. The fourth author was supported by NZIMA CoRE and by postdoctoral fellowships for computability theory and algorithmic randomness R-146-000-054-123 of Singapore and NSF of China No. 10471060 and No. 10420130638. Special thanks to the IMS at NUS and the workshop "Computational Prospects of Infinity 2005", at which some of this work was done.

[1] We use *real* to mean an element of Cantor space, 2^ω. This space is equipped with the usual topology with the basis of clopen sets $[\sigma] = \{\sigma\alpha : \sigma \in 2^{<\omega} \ \&\ \alpha \in 2^\omega\}$, with Lebesgue measure $\mu([\sigma]) = 2^{-|\sigma|}$.

An equivalent definition is to say α is weakly 2-random iff α avoids all Π^0_2 nullsets. Compare this to Martin-Löf randomness, which is equivalent to avoiding all Π^0_2 nullsets with effective convergence.

Martin-Löf randomness is sufficiently weak to allow for quite "nonrandom" behavior. For example, Kučera and Gács [4, 7] showed that every real is computable from a Martin-Löf random real. Also from their work it follows that every Turing degree above $\mathbf{0'}$ contains a Martin-Löf random real. On the other hand, Frank Stephan [15] showed that if a degree is Martin-Löf random and is sufficiently powerful to be able to compute a $\{0,1\}$-valued fixed point free function (i.e., it is PA) then it *must be* above $\mathbf{0'}$. Thus, such reals are quite atypical random reals, which in general must have low computational power. Similarly Sacks [14] showed that if A is noncomputable then $\mu(\{B : A \leq_T B\}) = 0$. We would expect any real which is random relative to A not to be above A in the Turing degrees. Again for each e, $\{X : A = \varphi_e^X\}$ is a Π^A_2-nullset (by Sacks's Theorem, because for each e, if the Π^A_2 set $\{X : A = \varphi_e^X\}$ has nonzero measure, A must be recursive) and hence if B is weakly 2-random relative to A, then $B \notin \{X : A = \varphi_e^X\}$. Thus $A \not\leq_T B$ if B is weakly-2-A-random.

We prove that in fact if A is weakly 2-random then the Turing degree of A and **0'** form a minimal pair. However, the main thrust of the present paper is to explore lowness for weak 2-randomness. This is especially interesting in that if a real A is low for weak 1-randomness then A is hyperimmune free, whereas if A is low for Martin-Löf randomness then A must be of low Turing degree.

We prove that there indeed do exist reals that are low for weak 2-randomness. Indeed there are computably enumerable sets which are low for weak 2-randomness. Technically this is much more demanding than the result for Martin-Löf randomness since a consequence of our first result, that weak 2-randoms form minimal pairs with **0'**, shows that there are no universal Π^0_2 nullsets. As our final result we prove that if A is low for weak 2-randomness then A is low for Martin-Löf randomness. We leave open the question whether they are the same, but conjecture they are not. We remark that there are a number of other possible proper subclasses of the low for Martin-Löf random reals, such as the reals which are Martin-Löf non-cuppable reals (Nies [13]), and the strongly jump traceable reals (Figueira, Nies, Stephan [3]). We believe that these classes are all related.

2. Preliminaries

We recall the definition of Martin-Löf randomness.

Definition 2.1 (Martin-Löf [10])**.** *A* Martin-Löf test *(ML test) is a computable sequence of c.e. open sets $\{U_n\}_{n\in\omega}$ such that for all n, $\mu(U_n) \leq 2^{-n}$. A real α* passes *such a test if $\alpha \notin \bigcap_n U_n$; α is* Martin-Löf random *(also* 1-random*) if it passes all ML tests.*

We have stated that weak 2-randomness is equivalent to avoidance of Π^0_2 nullsets, whose definition is below. For any n, weak n-randomness may be characterized in terms of exclusion from nullsets; we give the definition only for $n = 2$ and refer to the forthcoming book by Downey and Hirschfeldt [2] for the full version.

Definition 2.2. *A* generalized Martin-Löf test *(GML test) is a Π^0_2 nullset. That is, a computable sequence of c.e. open sets $\{U_n\}_{n\in\omega}$ such that $U_n \supseteq U_{n+1}$ for all n*

and $\lim_n \mu(U_n) = 0$. *In other words it is a Martin-Löf test without the restriction on speed of convergence.*

Theorem 2.3 (Kautz [6], Wang [16], after Kurtz [9]). *A real is weakly 2-random iff it passes all GML tests.*

For the proof of Theorem 2.3, see Downey and Hirschfeldt [2]. Relative randomness is obtained in the usual way, by adding an oracle to the tests.

We next show that the w-2-random degrees are not Δ^0_2. In fact, each forms a minimal pair with $\mathbf{0'}$, and as a consequence we obtain the result that there is no universal GML test.[2]

Theorem 2.4. *Each weakly 2-random degree forms a minimal pair with* $\mathbf{0'}$.

Proof. Suppose not, so there is a non-computable Δ^0_2 set Z and a weakly 2-random set A so that $Z = \Phi^A_e$. Since Z is Δ^0_2, there is an effective approximation $Z[s]$ so that $\lim_s Z(n)[s] = Z(n)$ for all n. Define

$$S_e = \{X | (\forall n)(\forall s)(\exists t > s)(\Phi^X_e(n)[t] \downarrow = Z(n)[t])\}.$$

S_e is Π^0_2 and $A \in S_e$. Since A is weakly 2-random, $\mu(S_e) > 0$. Thus there is a finite set $\Sigma \subseteq 2^{<\omega}$ and an open set $U = \bigcup_{\sigma\in\Sigma} V_\sigma$ so that

$$\mu(U \cap S_e) > \frac{3}{4}\mu(U).$$

To effectively compute $Z(n)$, we simply need to search for a finite set $\Xi \subseteq 2^{<\omega}$ with

$$\mu(\bigcup_{\tau\in\Xi} V_\tau) > \frac{1}{2}\mu(U) \text{ and } \bigcup_{\tau\in\Xi} V_\tau \subseteq U$$

so that for any $\tau_0, \tau_1 \in \Xi$,

$$\Phi^{\tau_0}_e(n) \downarrow = \Phi^{\tau_1}_e(n) \downarrow .$$

Then $Z(n) = \Phi^{\tau_0}_e(n)$. Thus Z is computable, contradiction. □

Corollary 2.5. *There is no universal GML test.*

Proof. Suppose there is a universal GML test. Then there is a non-empty Π^0_1 class containing only weakly 2-random reals. Then, by the Kreisel Basis Theorem, there is a weakly 2-random set computed by $\mathbf{0'}$. This contradicts Theorem 2.4. □

A noncomputable set A is *low* for a concept of randomness if all random reals are random relative to A. A stronger condition, meaningful for randomness concepts defined by passing tests, is for A to be *low for tests.* Such an A produces oracle tests which are individually covered by non-oracle tests; that is, for every test $\{U^A_n\}_{n\in\omega}$,

[2] Denis Hirschfeldt (personal communication to Downey) has shown that if $\{U_n : n \in \omega\}$ is a generalized Martin-Löf test, then there is a computably enumerable noncomputable set B such that $B \leq_T A$ for every Martin-Löf random set $A \in \cap_n U_n$. A corollary to this and our theorem is that *A real A is weakly 2-random iff A is 1-random and its degree forms a minimal pair with* $\mathbf{0'}$. The proof of Hirschfeldt's theorem is not difficult (but it is clever). We define $c(n, s) = \mu(U_n)[s]$, here assuming that tests are nested and each U_n is presented by an antichain. We put x into $B[s]$ if $W_e \cap B = \emptyset[s]$, $x \in W_e[s]$ and $c(x, s) < 2^{-e}$. We define a functional Γ as follows. If $\sigma \in U_{n, \text{ at } s}$, declare $\Gamma^\sigma(n) = B(n)[s]$. Finally we will define a Solovay test by saying that if $x \in B_{\text{at } s}$, put $U_x[s]$ into S. Then one verifies (i) $\mu(S) \leq 1$ (since we use the cost function 2^{-e}), (ii) B is noncomputable as $\mu(U_n) \to 0$, obtaining that if $A \in \cap_n U_n$ and A is 1-random, then since A will avoid S, $\Gamma^A =^* B$.

there is a non-oracle test $\{\widetilde{U}_n\}_{n\in\omega}$ such that $\bigcap_n U_n^A \subseteq \bigcap_n \widetilde{U}_n$. It is a uniform version of, and implies, "low for random." There is no definition of randomness where the two versions of lowness are known to differ, though the question is open in several cases. In particular, for Martin-Löf randomness the two are equivalent and for weak 2-randomness the equivalence is open. The low for w-2-random real we construct in §3 is low for tests, and in §4 we show the (possibly) larger class of low for w-2-randoms is contained in the class of low for ML-randoms.

3. There is a low for w-2-random

While it is possible to computably list exactly the Martin-Löf tests, it is not possible to do the same with GML tests. Any such list will include sequences of nested sets whose measure does not limit to zero. We will let $\{U_{e,n}\}_{n,e\in\omega}$ denote a canonical list of all *potential* (oracle) GML tests, where the measure of each $U_{e,n}$ is less than $\frac{1}{2}$ and for every e, n, $U_{e,n+1} \subseteq U_{e,n}$.

Theorem 3.1. *There is a noncomputable low for weakly 2-random c.e. set.*

Proof. We build a set A which is low for weak 2-random tests. As above, let $\{U_{e,n}^A\}$ be a canonical list of all potential oracle GML tests. We will build a simple c.e. set A and sequences $\{\widetilde{U}_{e,n}\}$ (not dependent on A) witnessing the lowness of A. That is, for all e we ensure $\bigcap_n \widetilde{U}_{e,n} \supseteq \bigcap_n U_{e,n}^A$, and if the latter is a GML test the former is as well.

Let W_f be an enumeration of all c.e. sets. The containment $\bigcap_n U_{e,n}^A \subseteq \bigcap_n \widetilde{U}_{e,n}$ will be implicit in the construction. For the rest, we have the following requirements.

$$P_f: \quad |W_f| = \omega \ \Rightarrow\ W_f \cap A \neq \emptyset.$$
$$R_e: \quad \lim_k \mu(U_{e,k}^A) = 0 \ \Rightarrow\ \lim_k \mu(\widetilde{U}_{e,k}) = 0.$$

We meet R_e by selecting values $n(e,k)$ indexing a subsequence of $U_{e,k}^A$ and setting $\widetilde{U}_{e,n(e,k)} = \bigcup_s U_{e,n(e,k)}^A[s]$, where sets with indices i, $n(e,k) < i \leq n(e,k+1)$, are equal to the set of index $n(e,k)$. The intention is that $U_{e,n(e,k)}^A$ is the first set of the e^{th} potential GML test to have measure less than 2^{-k}. Of course, since the construction is dynamic, we will have to guess the subsequence and will often be incorrect. Hence in reality $n(e,k) = \lim_s n(e,k,s)$ and sets may have more content than simply the union $\bigcup_s U_{e,n(e,k)}^A[s]$. We will ensure that if $\{U_{e,k}^A\}_{k\in\omega}$ is truly a GML test, the limit $n(e,k)$ will exist and (therefore) the additional content will be bounded.

However, that is not all of the difficulty. If changes to A cause $U_{e,n(e,k)}^A$ to enumerate and then remove too much measure, setting $\widetilde{U}_{e,n(e,k)} = \bigcup_s U_{e,n(e,k)}^A[s]$ may prohibit $\lim_k \mu(\widetilde{U}_{e,k}) = 0$. Likewise, temporary addition of measure to $U_{e,n(e,k)}^A$ may lead us to believe falsely that $U_{e,n(e,k)}^A$ is not the first set of measure less than 2^{-k} and define $n(e,k,s+1) \neq n(e,k,s)$. Finitely often that is not a problem, but if it occurs infinitely often $\lim_s n(e,k,s)$ will fail to exist.

We answer both difficulties by splitting R_e into subrequirements.

$$R_{e,k,d}: \quad [n(e,k) \text{ defined with } \mu(\widetilde{U}_{e,n(e,k)}) < 2^{1-k}] \ \vee\ [\mu(U_{e,d}^A) \geq 2^{-k}].$$

For a fixed e, k, meeting these requirements means either $n(e,k)$ is eventually defined or $(\forall\, n)\ [\mu(U_{e,n}^A) \geq 2^{-k} > 0]$, and hence $\{U_{e,n}^A\}$ is not a test. To meet $R_{e,k,d}$ we restrain enumeration into A. The requirements which are still attempting to define $n(e,k)$ will not actively impose restraint; each P_f requirement will have restrictions on its enumeration into A that without injury will keep $\mu(\widetilde{U}_{e,n(e,k)}) < 2^{1-k}$. Those $R_{e,k,d}$ which see $\mu(U^A_{e,d}) \geq 2^{-k}$ at stage s will attempt to keep the measure high by imposing restraint $r(e,k,d,s) = s$ with priority $\langle e,k,d\rangle$. For all $\langle e,k,d\rangle$, $r(e,k,d,0) = 0$.

After Kučera and Terwijn [8], we define

$$\alpha(y,e,k,s) = \mu\left(\bigcup\{[\sigma] : y < u([\sigma], A_s, \langle e, n(e,k,s)\rangle, s)\}\right),$$

the measure of the part of $U^A_{e,n(e,k)}[s]$ which has y below its use (we follow the convention that all uses are bounded by the current stage of the construction). The requirement P_f *requires attention with witness* x at stage s if $W_{f,s} \cap A_s = \emptyset$ and there is some $x > 2f$ in $W_{f,s}$ such that

$$\alpha(x,e,k,s) < 2^{-(k+f+1)} \text{ for all } \langle e,k\rangle < f$$

and

$$x > r(e,k,d,s) \text{ for all } \langle e,k,d\rangle < f.$$

Construction

Set the convention that at stage s only $U^A_{e,k}$ with $e,k \leq s$ are nonempty. Set $\widetilde{U}_{e,k,0} = \emptyset$ and $n(e,k,0) = k$ for all e,k. To *re-index* with $n(e,k,s+1) = m$ means to set $n(e,k+i,s+1) = m+i$ for $i \geq 0$ and $n(e,j,s+1) = n(e,j,s)$ for $j < k$.

Stage s:

Step 1. If any P_f requires attention, pick the highest-priority such and least witness x and let $A_{s+1} = A_s \cup \{x\}$.

Step 2. For each e do the following:

(i) If there are k,d such that $\mu(U^A_{e,d}[s]) \geq 2^{-k}$ but $\mu(U^A_{e,d}[s-1]) < 2^{-k}$, set $r(e,k,d,s+1) = s$.

(ii) If (i) occurred for some k,d pair such that $d \geq n(e,k,s)$ or if there is a k such that $\widetilde{U}_{e,n(e,k)}[s] > 2^{1-k}$, pick the least such k and re-index with $n(e,k,s+1) = s+1$.

Step 3. For any value which has not been explicitly reset, let the stage $s+1$ value be the same as the stage s value. Let $\widetilde{U}_{e,n(e,k)}[s+1] = \widetilde{U}_{e,n(e,k)}[s] \bigcup U^A_{e,n(e,k)}[s+1]$.

Verification

Lemma 3.2. *All* $r(e,k,d) = \lim_s r(e,k,d,s)$ *exist.*

Proof. Suppose $r(e',k',d')$ exists for all $\langle e',k',d'\rangle < \langle e,k,d\rangle$, and stage s is such that all those limits have been attained and all requirements P_f with $f \leq \langle e,k,d\rangle$ have stopped acting (s exists because every P_f acts at most once).

If $\mu(U^A_{e,d}[s]) \geq 2^{-k}$, then (if not set already) $r(e,k,d)$ will be set at stage $s+1$ and never injured, which means that $\mu(U^A_{e,d}[t]) \geq 2^{-k}$ for all $t > s$, and hence $r(e,k,d)$ has reached its limit at stage $s+1$. Likewise if $\mu(U^A_{e,d})$ should become too large at a later stage. If $\mu(U^A_{e,d}) < 2^{-k}$ for all stages $s' \geq s$, then $r(e,k,d)$ is never reset after stage s and has reached its limit. □

Lemma 3.3. *If* $\lim_n \mu(U^A_{e,n}) = 0$*, then for all* k*,* $n(e,k,s)$ *has a finite limit.*

Proof. Suppose the lemma does not hold for e, and fix some least k such that $n(e,k,s)$ does not have a finite limit. Since we only reset $n(e,k,s)$ when either

(i) $\mu(U^A_{e,n(e,k)}[s]) \geq 2^{-k}$ or
(ii) $\mu(\widetilde{U}_{e,n(e,k)}[s]) \geq 2^{1-k}$,

at least one of these must happen infinitely often.

Assume $n(e,k,s)$ is reset because of (i) infinitely often. We claim $\lim_n \mu(U^A_{e,n}) \geq 2^{-k}$. Because $U^A_{e,n} \supseteq U^A_{e,n+1}$ for all n, every time (i) occurs any sets of index less than the current $n(e,k)$ must also have measure at least 2^{-k}. Let $U^A_{e,d}$ be any such set. Further enumerations into A may cause $\mu(U^A_{e,d})$ to drop below 2^{-k} again, but by assumption it will later grow back. Since every time $\mu(U^A_{e,d})$ grows from below 2^{-k} to above $r(e,k,d)$ is reset, by Lemma 3.2 it must happen only finitely many times for any fixed d. Therefore all $\mu(U^A_{e,n})$ eventually grow to at least 2^{-k} and stay there.

We will show that if (i) happens only finitely often, so does (ii). If all instances of (i) have passed at stage s, then $r(e,k,d)$ for $d \geq s$ will never be changed again. Only finitely-many such restraints will have been set to a nonzero value. Let d' be the first d such that $r(e,k,d) = 0$ permanently. By choice of k to be minimal, all $n(e,k',s)$ with $k' < k$ will reach a limit; let t be a stage such that those limits have been reached, all instances of (i) have passed, and all P_f with $f \leq \langle e,k,d'\rangle$ have stopped acting. We claim $n(e,k)$ can change at most once more after stage t. It may be that actions from above have increased the measure of $\widetilde{U}_{e,n(e,k)}[t]$ sufficiently that even obeying restraint, the actions of lower-priority P_f requirements push that measure to at least 2^{-k}. However, at such a stage t', $n(e,k)$ will be reset to $t'+1$; $U^A_{e,t'+1}$ is empty at stage t' and by assumption has measure less than 2^{-k} at all stages thereafter. The total injury to $\widetilde{U}_{e,n(e,k)}$ by lower-priority P_f will be less than

$$\sum_{i=0}^{\infty} 2^{-(k+i+1)} = 2^{-k},$$

so $\mu(\widetilde{U}_{e,n(e,k)}) < 2^{-k} + 2^{-k} = 2^{1-k}$ and (ii) never happens again. □

Corollary 3.4. *All $R_{e,k,d}$ are satisfied, and thus all R_e are satisfied.*

Lemma 3.5. *All P_f are satisfied.*

Proof. Suppose W_f is infinite. Since by Lemma 3.2 all restraints $r(e,k,d)$ reach a finite limit, and P_f need respect only finitely many such restraints, there will be $x \in W_f$ respecting all such restraints as well as the requirement that $x > 2f$.

We must show there will eventually be an eligible x with $\alpha(x,e,k,s) < 2^{-(k+f+1)}$ for all $\langle e,k\rangle < f$. Note that there are only finitely many intervals with size at least $2^{-(k+f+1)}$, so if each has bounded use within each $U^A_{e,k}$, the maximum of those uses will be finite and all large enough x will satisfy the α restraint. Therefore the only potential problem is if for some σ with $\mu[\sigma] \geq 2^{-(k+f+1)}$, the computation "$\sigma \in U^A_{e,k}$" is broken and reformed infinitely many times, each time with a use higher than all elements enumerated into W_f in the meantime. However, only requirements $P_{f'}$ with $f' < f$ may be allowed to break a computation for σ, and there are only finitely many of them. Therefore all the uses reach a finite limit and P_f will eventually be allowed to act. □

As A is clearly c.e., this completes the proof of Theorem 3.1. □

4. Each low for w-2-random is low for ML-random

Given multiple definitions of randomness, their relationship to each other is of interest. In particular, if $\mathcal{C} \subseteq \mathcal{D}$ are sets of reals random with respect to two different notions of randomness, we can ask whether the reals low for those notions have the same containment relationship. One means of approaching that question is by considering lowness for the *pair* $\mathcal{C}, \mathcal{D}$. Since relativizing $\mathcal{D}$ usually makes it smaller, one would expect that in general $\mathcal{C} \not\subseteq \mathcal{D}^A$ even if $\mathcal{C} \subseteq \mathcal{D}$. The following class consists of the sets A for which the inclusion still holds.

Definition 4.1. *A set A is in* $\mathrm{Low}(\mathcal{C}, \mathcal{D})$ *if* $\mathcal{C} \subseteq \mathcal{D}^A$.

If $\mathcal{C} \subseteq \widetilde{\mathcal{C}} \subseteq \widetilde{\mathcal{D}} \subseteq \mathcal{D}$ are randomness notions for which containment is preserved under relativization (a property true of all reasonable randomness notions), then $\mathrm{Low}(\widetilde{\mathcal{C}}, \widetilde{\mathcal{D}}) \subseteq \mathrm{Low}(\mathcal{C}, \mathcal{D})$. That is, we make the class $\mathrm{Low}(\mathcal{C}, \mathcal{D})$ larger by decreasing $\mathcal{C}$ or increasing $\mathcal{D}$. Note that $\mathrm{Low}(\mathcal{C}, \mathcal{D})$ always contains $\mathrm{Low}(\mathcal{D})$, the set of reals low for the randomness notion $\mathcal{D}$.

Let $\mathsf{MLRand}, \mathsf{W2Rand}$ denote the classes of ML-random and weakly 2-random sets, respectively.

Theorem 4.2. $\mathrm{Low}(\mathsf{W2Rand}, \mathsf{MLRand}) = \mathrm{Low}(\mathsf{MLRand})$. *In other words, if each weakly 2 random is ML-random relative to A, then A is in fact low for ML-random.*

Since every ML test is a GML test, $\mathsf{W2Rand}^A \subseteq \mathsf{MLRand}^A$ for any A. Thus having $A \in \mathrm{Low}(\mathsf{W2Rand}) - \mathrm{Low}(\mathsf{MLRand})$ would contradict Theorem 4.2 and a corollary to the theorem is that every real which is low for w-2-random is low for ML-random. Note that here we mean the broader notion of low for random, rather than the (possibly) more restrictive low for tests.

We begin with several preliminaries, primarily notational. A Turing machine M is *prefix-free* if $M(\sigma)\downarrow$ means $M(\tau)\uparrow$ for any proper initial segment $\tau \subset \sigma$. Otherwise we call M a *prefix machine*. Fix a universal prefix-free Turing machine U, here and below. We use $K(n)$ to denote the prefix-free Kolmogorov complexity of n; that is, the length of the shortest input σ such that $U(\sigma)\downarrow = n$. The input σ is also called a *U-description* of n. A real Z is Martin-Löf random iff there is a constant $b \in \omega$ such that

$$(\forall n)\ [K(Z \upharpoonright n) > n - b]. \tag{4.1}$$

See Downey and Hirschfeldt [2] for more details.

The following simple criterion for being non-ML-random is due to Merkle (see [12]). By $a \leq^+ b$ we mean $a \leq b + c$ where c is a constant independent of a and b.

Lemma 4.3. *If $Z = z_0 z_1 z_2 \dots$ where $K(z_i) \leq |z_i| - 1$ for each i, then $Z \notin \mathsf{MLRand}$.*

Proof. Fix n and consider the prefix machine M which, on an input σ, searches for an initial segment $\rho \subseteq \sigma$ such that $U(\rho)\downarrow = n$, and then for $\nu_0, \dots, \nu_{n-1} \in \mathrm{dom}(U)$ such that $\rho\nu_0 \dots \nu_{n-1} = \sigma$. If the search is successful, it prints $U(\nu_0) \dots U(\nu_{n-1})$. Given a string $z_0 \dots z_{n-1}$, let σ be a concatenation of a shortest U-description of n followed by shortest U-descriptions of $z_0, \dots, z_{n-1}$. Then $M(\sigma) = z_0 \dots z_{n-1}$, and so $K(z_0 \dots z_{n-1}) \leq^+ K(n) + \sum_{i<n} K(z_i) \leq K(n) + |z_0 \dots z_{n-1}| - n$. Since $K(n) \leq^+ 2 \log n$, we obtain $K(z_0 \dots z_{n-1}) \leq^+ |z_0 \dots z_{n-1}| - (n - 2 \log n)$, failing to meet (4.1) and thus showing $Z \notin \mathsf{MLRand}$. $\square$

We also use a characterization of Low(MLRand) due to Nies and Stephan (see [11, Thm 3.3], or [12]).

Theorem 4.4. *A is low for ML-randomness iff*

$$\exists R \text{ c.e. open } (\mu(R) < 1 \;\wedge\; \forall z \in 2^{<\omega}[K^A(z) \le |z| - 1 \;\Rightarrow\; [z] \subseteq R]). \tag{4.2}$$

We will use a consequence of the failure of (4.2). For an open set V and a string w, the conditional measure $\mu(V \mid w)$ is $2^{|w|}\mu(V \cap [w])$.

Claim 4.5. *Suppose (4.2) fails for A. Let β, γ be rationals such that $\beta < \gamma < 1$. For each c.e. open set V and each string w, if $\mu(V \mid w) \le \beta$, then there is z such that $K^A(z) \le |z| - 1$ and $\mu(V \mid wz) \le \gamma$.*

Proof. Suppose that no such z exists, and consider the c.e. set of strings

$$G = \{z : \mu(V \mid wz) > \gamma\}.$$

Whenever $K^A(z) \le |z| - 1$ then $z \in G$. Let R be the c.e. open set generated by G. Note that $z0, z1 \in G \;\Rightarrow\; z \in G$. So if $(z_i)_{i<N}$ is a listing of the minimal strings in G ($N \le \infty$), then $R = \bigcup_{i<N}[z_i]$.

Now

$$\beta \ge \mu(V \mid w) \ge \sum_{i<N} 2^{-|z_i|}\mu(V \mid wz_i) \ge \mu(R)\cdot\gamma.$$

Thus $1 > \beta/\gamma \ge \mu R$ and (4.2) holds, contradiction. □

Proof of Theorem 4.2. Suppose that A is not low for ML-random. Thus the hypothesis of Claim 4.5 is satisfied. We show that $\mathsf{W2Rand} \subseteq \mathsf{MLRand}^A$ fails, by building a set $Z \in \mathsf{W2Rand}$ that is not ML-random relative to A. We define (non-effectively) a sequence of strings $z_0, z_1, \dots$ such that $K^A(z_i) \le |z_i| - 1$ and let $Z = z_0 z_1 z_2 \dots$, so that Z is not ML-random relative to A by Lemma 4.3 relativized to A. As in §3 let $\{U_{e,n}\}_{e,n\in\omega}$ be an enumeration of all potential GML tests. For $Z \in \mathsf{W2Rand}$, for each actual GML test $\{U_{e,n}\}$ we define a number n_e and ensure $Z \notin U_{e,n_e}$. At the beginning of Step e, $z_0, \dots, z_{e-1}$ have been defined, and we let

$$V_e = \bigcup_{\substack{i<e \\ n_i \text{ defined}}} U_{i,n_i},$$

and $w_e = z_0 \dots z_{e-1}$. We ensure inductively that

$$\mu(V_e \mid w_e) \le \gamma_e := 1 - 2^{-e}. \tag{4.3}$$

In particular, since $\mu(V_e|w_e) < 1$, $[w_e] \not\subseteq V_e$ for each e. Since the V_e are open and nested, $V_e \subseteq V_{e+1}$ for all e, this is sufficient to give $Z \notin U_{e,n_e}$ whenever $\{U_{e,n}\}$ is a test, as required. To see this, note that $Z \in U_{e,n_e}$ requires some initial segment $w_m \subset Z$ be such that $[w_m] \subseteq U_{e,n_e}$ (WLOG and in fact necessarily $m > n_e$). However, our guarantee of $[w_{m+1}] \not\subseteq V_{m+1}$, $w_{m+1} \supset w_m$, contradicts $[w_m] \subseteq U_{e,n_e} \subseteq V_{m+1}$, so $Z \notin U_{e,n_e}$.

Note that w_0 is the empty string and $V_0 = \emptyset$, so that (4.3) holds for $e = 0$.

Step $e \ge 0$. If $\{U_{e,n}\}_{n\in\omega}$ is not a test (i.e., $\lim_n \mu(U_{e,n}) \ne 0$), then leave n_e undefined. Otherwise, choose n_e so large that

$$\mu(U_{e,n_e}) \le 2^{-|w_e|-e-2}.$$

In particular, $\mu(U_{e,n_e}|w_e) \le 2^{-(e+2)}$.

Then letting $V_{e+1} = V_e \cup U_{e,n_e}$, we get

$$\mu(V_{e+1} \mid w_e) \leq \gamma_e + 2^{-(e+2)} = 1 - 2^{-e} + 2^{-(e+2)} < 1.$$

Applying Claim 4.5 to $V = V_{e+1}$, $w = w_e$, $\beta = \gamma_e + 2^{-(e+2)}$, and $\gamma = \gamma_{e+1} > \beta$, there is $z = z_e$ such that $K^A(z) \leq |z| - 1$ and $\mu(V_{e+1} \mid w_e z) \leq \gamma_{e+1}$. Thus (4.3) holds for $e + 1$. □

Postscript, 27 March 2006. After this paper was accepted for publication, Miller and Nies independently proved that every K-trivial real is in fact low for weak 2-randomness. Together with our work, this gives yet another characterization of the robust class of K-trivial reals. The Miller-Nies material will appear elsewhere.

References

[1] Downey, R., E. Griffiths, and S. Reid, *On Kurtz randomness.* Theoretical Computer Science **321** (2004) 249–270.

[2] Downey, R., and D. Hirschfeldt, *Algorithmic Randomness and Complexity.* Springer-Verlag, to appear. Current version available at `http://www.mcs.vuw.ac.nz/~downey`.

[3] Figueira, S., A. Nies, and F. Stephan. *Lowness properties and approximations of the jump.* Proceedings of the Twelfth Workshop of Logic, Language, Information and Computation (WoLLIC 2005). Electronic Lecture Notes in Theoretical Computer Science **143** (2006), 45–57.

[4] Gács, P., *Every set is reducible to a random one.* Information and Control **70** (1986), 186–192.

[5] Gaifman, H., and M. Snir, *Probabilities over rich languages, testing and randomness.* J. Symbolic Logic **47** (1982), 495–548.

[6] Kautz, S., *Degrees of Random Sets.* Ph.D. thesis, Cornell University, 1991.

[7] Kučera, A., *Measure, Π_1^0 classes, and complete extensions of PA.* In Springer Lecture Notes in Mathematics **1141** (1985), 245–259.

[8] Kučera, A. and S. Terwijn, *Lowness for the class of random sets.* J. Symbolic Logic **64** (1999), no. 4, 1396–1402.

[9] Kurtz, S., *Randomness and Genericity in the Degrees of Unsolvability.* Ph.D. thesis, University of Illinois at Urbana-Champaign, 1981.

[10] Martin-Löf, P., *The definition of random sequences.* Information and Control [9] (1966), 602–619.

[11] Nies, A., *Low for random sets: the story.* Preprint, available at `http://www.cs.auckland.ac.nz/~nies`.

[12] Nies, A., *Computability and Randomness.* To appear.

[13] Nies, A., *Non-cupping and randomness.* Proc. Amer. Math. Soc., to appear.

[14] G. Sacks, *Degrees of Unsolvability*, Princeton University Press, 1963.

[15] Stephan, F., personal communication.

[16] Wang, Y., *Randomness and Complexity.* Ph.D. thesis, University of Heidelberg, 1996.

School of Mathematics, Statistics and Computer Science, Victoria University, P.O. Box 600, Wellington, New Zealand

E-mail address: `Rod.Downey@vuw.ac.nz`

Department of Computer Science, The University of Auckland, Private Bag 92019, Auckland, New Zealand

E-mail address: `nies@cs.auckland.ac.nz`

Department of Mathematics, Dartmouth College, 6188 Bradley Hall, Hanover, NH 03755 USA

E-mail address: `rweber@math.dartmouth.edu`

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

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