LOWNESS FOR THE CLASS OF SCHNORR RANDOM REALS

BJØRN KJOS-HANSSEN

Department of Mathematics
University of Connecticut
Storrs, CT 06269, USA

ANDRÉ NIES

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

FRANK STEPHAN

School of Computing, 3 Science Drive 2, and
Department of Mathematics, 2 Science Drive 2
National University of Singapore
Singapore 117543, Republic of Singapore

ABSTRACT

We answer a question of Ambos-Spies and Kučera in the affirmative. They asked whether, when a real is low for Schnorr randomness, it is already low for Schnorr tests.

Keywords: lowness, randomness, Schnorr randomness, Turing degrees, recursion theory, computability theory

1. Introduction

In an influential 1966 paper [9], Martin-Löf proposed an algorithmic formalization of the intuitive notion of randomness for infinite sequences of 0's and 1's. His formalization was based on an effectivization of a test concept from statistics, by means of uniformly computably enumerable (c.e.) sequences of open sets. Martin-Löf's proposal addressed some insufficiencies in an earlier algorithmic concept of randomness proposed by Church [3], who had formalized a notion now called computable stochasticity. However, Schnorr [13] criticized Martin-Löf's notion as too strong, because it was based on a c.e. test concept rather than a computable notion of tests. He suggested that one should base a formalization of randomness on computable betting strategies (also called martingales), in way that would still overcome the problem that Church's concept was too weak. In present terminology, a real Z is computably random if no computable betting strategy succeeds along Z; that is, for each computable betting strategy there is a finite upper bound on the capital that it reaches. The real Z is Schnorr random if no martingale succeeds *effectively.* Here effective success means that the capital at $Z\upharpoonright n$ exceeds $f(n)$ infinitely often, for some unbounded computable function f. See [1] for more on the history of this.

We recall some definitions. The Cantor space 2^ω is the set of infinite binary sequences; these are called *reals* and are identified with set of integers, i.e., subsets of ω. If $\sigma \in 2^{<\omega}$, that is, σ is a finite binary sequence, then we denote by $[\sigma]$ the set of reals that extend σ. These form a basis of clopen sets for the usual discrete topology on 2^ω. Write $|\sigma|$ for the length of $\sigma \in 2^{<\omega}$. The Lebesgue measure μ on 2^ω is defined by stipulating that $\mu[\sigma] = 2^{-|\sigma|}$. With every set $U \subseteq 2^{<\omega}$ we associate the open set $[U]^{\preceq} = \bigcup_{\sigma \in U}[\sigma]$. The empty sequence is denoted λ. If $\sigma, \tau \in 2^{<\omega}$ and σ is a prefix of τ, then we write $\sigma \preceq \tau$. If $\sigma \in 2^{<\omega}$ and $i \in \{0,1\}$ then σi denotes the string of length $|\sigma|+1$ extending σ whose final entry is i. The concatenation of two strings σ and τ is denoted $\sigma\tau$. The empty set is denoted $\emptyset$ and inclusion of sets is denoted by $\subseteq$. If A is a real and $n \in \omega$ then $A\upharpoonright n$ is the prefix of A consisting of the first n bits of A. Letting $A(n)$ denote bit n of A, we have $A\upharpoonright n = A(0)A(1)\cdots A(n-1)$.

Given $\alpha \in 2^{<\omega}$ and a measurable set $C \subseteq 2^\omega$, we let $\mu_\alpha C = \frac{\mu(C \cap [\alpha])}{\mu[\alpha]}$. For an open set W we let

$$W|\sigma = \bigcup \left\{ [\tau] : \tau \in 2^{<\omega}, [\sigma\tau] \subseteq W \right\}.$$

Note in particular that $\mu_\sigma W = \mu(W|\sigma)$ and $\mu_\lambda W = \mu W$.

Fixing some effective correspondence between the set of finite subsets of ω and ω, we let D_e be the eth finite subset of ω under this correspondence. In other words, e is a strong, or canonical, index for the finite set D_e. Similarly, we let S_e be the eth finite subset of $2^{<\omega}$ under a suitable correspondence. So S_e is a finite set of strings, and $[S_e]^{\preceq} = \cup_{\sigma \in S_e}[\sigma]$ is then the clopen set coded by $e \in \omega$. We use the Cantor pairing function, the bijection $p : \omega^2 \to \omega$ given by $p(n,s) = \frac{(n+s)^2+3n+s}{2}$, and write $\langle n, s \rangle = p(n,s)$.

A *Martin-Löf test* is a set $U \subseteq \omega \times 2^\omega$ such that $\mu U_n \leq 2^{-n}$, where U_n denotes the nth section of U, and U_n is a Σ^0_1 class, uniformly in n. If in addition μU_n is a computable real, uniformly in n, then U is called a *Schnorr test.* Z is *Martin-Löf random* if for each Martin-Löf test U there is an n such that $Z \notin U_n$, and *Schnorr random* if for each Schnorr test U there is an n such that $Z \notin U_n$. The notion of Schnorr randomness is unchanged if we instead define a Schnorr test to be a Martin-Löf test for which $\mu U_n = 2^{-n}$ for each $n \in \omega$.

Concepts encountered in computability theory are usually based on some notion of computation, and therefore have relativized forms. For instance, we may relativize the tests and randomness notions above to an oracle A. If $\mathcal{C} = \{X : X$ is

Martin-Löf random} then the relativization is $\mathcal{C}^A = \{X : X$ is Martin-Löf random relative to $A\}$ (meaning that Σ^0_1 classes are replaced by $\Sigma^{0,A}_1$ classes). In general, if $\mathcal{C}$ is such a relativizable class, we say that A is *low for* $\mathcal{C}$ if $\mathcal{C}^A = \mathcal{C}$. If $\mathcal{C}$ is a randomness notion, more computational power means a smaller class, namely, $\mathcal{C}^A \subseteq \mathcal{C}$ for any A. Being low for $\mathcal{C}$ means to have small computational power (in a sense that depends on $\mathcal{C}$). In particular, the low for $\mathcal{C}$ reals are closed downward under Turing reducibility.

The randomness notions for which lowness was first considered are Martin-Löf and Schnorr randomness. Kučera and Terwijn [6] constructed a non-computable c.e. set of integers A which is low for Martin-Löf randomness, answering a question of Zambella [16]. In the paper [14] it is shown that there are continuum many reals that are low for Schnorr randomness.

An important difference between the two randomness notions is that for Martin-Löf randomness, but not for Schnorr randomness, there is a universal test R. Thus, Z is not Martin-Löf random iff $Z \in \bigcap_{b \in \omega} R_b$. Therefore, in the Schnorr case, an apparently stronger lowness notion is being *low for Schnorr tests*, or S_0*-low* in the terminology of [1]: A is low for Schnorr tests if for each Schnorr test U^A relative to A, there is an unrelativized Schnorr test V such that $\bigcap_n U^A_n \subseteq \bigcap_n V_n$. This implies that A is low for Schnorr randomness, or S*-low* in the terminology of [1]. Ambos-Spies and Kučera asked if the two notions coincide. We answer this question in the affirmative.

Terwijn and Zambella [14] actually constructed oracles A which are low for Schnorr tests. They first gave a characterization of this lowness property, via a notion of traceability, a restriction on the possible sequence of values of the functions computable from A. They showed that A is low for Schnorr tests iff A is computably traceable (see formal definition in the next section). Then they constructed continuum many computably traceable reals. We answer the question of Ambos-Spies and Kučera by showing that each real which is low for Schnorr randomness is in fact computably traceable.

Towards this end, it turns out to be helpful to have a more general view of lowness. We consider lowness for any pair of randomness notions $mathcalC$, $\mathcal{D}$ with $\mathcal{C} \subseteq \mathcal{D}$.

Definition 1.1. *A is in* $\mathrm{Low}(\mathcal{C}, \mathcal{D})$ *if* $\mathcal{C} \subseteq \mathcal{D}^A$*. We write* $\mathrm{Low}(\mathcal{C})$ *for* $\mathrm{Low}(\mathcal{C}, \mathcal{C})$*.*

Clearly, if $\mathcal{C} \subseteq \widetilde{\mathcal{C}} \subseteq \widetilde{\mathcal{D}} \subseteq \mathcal{D}$ are randomness notions, and the inclusions relativize (so $\widetilde{\mathcal{D}}^A \subseteq \mathcal{D}^A$ for each real A), then $\mathrm{Low}(\widetilde{\mathcal{C}}, \widetilde{\mathcal{D}}) \subseteq \mathrm{Low}(\mathcal{C}, \mathcal{D})$. That is, we make the class $\mathrm{Low}(\widetilde{\mathcal{C}}, \widetilde{\mathcal{D}})$ larger by decreasing $\mathcal{C}$ or increasing $\mathcal{D}$. Let MR, CR and SR denote the classes of Martin-Löf random, computably random (defined below) and Schnorr random reals, respectively. Thus for instance $\mathrm{Low}(\mathsf{MR}, \mathsf{CR})$ is the class of oracles A such that each Martin-Löf random real is computably random in A. We will characterize lowness for any pair of randomness notions $\mathcal{C} \subseteq \mathcal{D}$ with $\mathcal{C}, \mathcal{D} \in \{\mathsf{MR}, \mathsf{CR}, \mathsf{SR}\}$.

Recall that Ω denotes the halting probability of a universal prefix machine. Ω is a Martin-Löf random *computably enumerable real*, i.e., a real that can be effectively approximated from below. Given $\mathcal{D} \supseteq \mathsf{MR}$, an interesting lowness notion obtained by weakening $\mathrm{Low}(\mathsf{MR}, \mathcal{D})$ is $\mathrm{Low}(\{\Omega\}, \mathcal{D})$. That is, instead of $\mathsf{MR} \subseteq \mathcal{D}^A$ one merely requires that $\Omega \in \mathcal{D}^A$. We denote this class by $\mathrm{Low}(\Omega, \mathcal{D})$. In [11], the case $\mathcal{D} = \mathsf{MR}$ is studied. They show that the class coincides with $\mathrm{Low}(\mathsf{MR})$ on the Δ^0_2 reals, but not in general. In fact, a Martin-Löf random real is 2-random iff it is in $\mathrm{Low}(\Omega, \mathsf{MR})$.

Here we investigate the class $\mathrm{Low}(\Omega, \mathsf{SR})$. We show that A is $\mathrm{Low}(\mathsf{MR}, \mathsf{SR})$ iff A is c.e. traceable. Moreover, the weaker assumption $\Omega \in \mathsf{SR}^A$ still implies that A is array computable (there is a function $f \leq_{wtt} \emptyset'$ bounding all functions computable from A, on almost all inputs). So for c.e. sets of integers A, A being $\mathrm{Low}(\mathsf{MR},\mathsf{SR})$ is in fact equivalent to $\Omega \in \mathsf{SR}^A$ by Ishmukhametov [5]. We also provide an example of a real A which is array computable but not $\mathrm{Low}(\Omega, \mathsf{SR})$.

2. Main concepts

2.1. *Martingales*

For our purposes, a *martingale* is a function $M : 2^{<\omega} \mapsto \mathbb{Q}$ (where $\mathbb{Q}$ is the set of rational numbers) such that (i) the domain of M is $2^{<\omega}$, or $2^{\leq n} = \{\sigma \in 2^{<\omega} : |\sigma| \leq n\}$ for some n, (ii) $M(\lambda) \leq 1$, and (iii) M has the martingale property $M(x0) + M(x1) = 2M(x)$ whenever the strings $x0, x1$ belongs to the domain of M. A martingale M *succeeds* on a sequence $Z \in 2^\omega$ if

$$\limsup_{n\to\infty} M(Z\lceil n) = \infty.$$

A real is *computably random* if no computable martingale succeeds on it.

A martingale M *effectively succeeds* on a sequence Z if there is a nondecreasing and unbounded computable function $h : \omega \longrightarrow \omega$ such that

$$\limsup_{n\to\infty} M(Z\lceil n) - h(n) > 0.$$

Equivalently (since we are considering integer-valued functions), $\exists^\infty n \ M(Z\lceil n) > h(n)$. We can now state the characterization of Schnorr randomness in terms of martingales: a real Z is Schnorr random if and only if no computable martingale effectively succeeds on Z.

2.2. *Traceability*

Let W_e denote the eth c.e. set of integers in some standard list. A real A is *c.e. traceable* if there is a computable function p, called a *bound*, such that for every $f \leq_T A$, there is a computable function r such that for all x, we have $|W_{r(x)}| \leq p(x)$ and $f(x) \in W_{r(x)}$.

The following is a stronger notion than c.e. traceability. A is *computably traceable* if there is a computable p such that for every $f \leq_T A$, there is a computable r such that for all x, we have $|D_{r(x)}| \leq p(x)$ and $f(x) \in D_{r(x)}$.

It is interesting to notice that it does not matter what bound p one chooses as a witness for traceability:

Proposition 2.1 (Terwijn and Zambella [14])**.** *Let A be a real that is computably traceable with bound p. Then for any monotone and unbounded computable function p', A is computably traceable with bound p'. The same holds for c.e. traceability.*

The result of Terwijn and Zambella is

Theorem 2.2 ([14])**.** *A real A is low for Schnorr tests iff A is computably traceable.*

3. Statement of the main result

Theorem 3.1.

(I) A is $\mathrm{Low}(\mathsf{MR}, \mathsf{SR})$ *iff A is c.e. traceable.*

(II) A is $\mathrm{Low}(\mathsf{CR}, \mathsf{SR})$ *iff A is* $\mathrm{Low}(\mathsf{SR})$ *iff A is computably traceable.*

We make some remarks about the proofs, and fill in the details in the next Section. We obtain Theorem 3.1(I) by modifying the methods in [14] to the case of c.e. traces instead of computable ones.

As for Theorem 3.1(II), by Theorem 2.2 if A is computably traceable then A is low for Schnorr tests. Hence A is certainly $\mathrm{Low}(\mathsf{SR})$, and therefore also $\mathrm{Low}(\mathsf{CR}, \mathsf{SR})$. It remains only to show that each real $A \in \mathrm{Low}(\mathsf{CR}, \mathsf{SR})$ is computably traceable. To see that this is so, take the following three steps:

1. Recall that A is *hyperimmune-free* if for each $g \leq_T A$, there is a computable f such that for all x, we have $g(x) \leq f(x)$. As a first step towards proving Theorem 3.1(II), Bedregal and Nies [2] showed that each $A \in \mathrm{Low}(\mathsf{CR}, \mathsf{SR})$ is hyperimmune-free (see Lemma 4.9 below). To see this, assume that A is not, so there is a function $g \leq_T A$ not dominated by any computable function f. Define a martingale $L \leq_T A$ which succeeds in the sense of Schnorr, with the computable lower bound $h(n) = n/4$, on some $Z \in \mathsf{CR}$. One uses here that g is infinitely often above the running time of each computable martingale. (Special care has to be taken with the partial martingales, which results in a real Z that is only Δ^0_3.)

2. If A is hyperimmune-free and c.e. traceable, then A is computably traceable. For let $g \leq_T A$, then the first stage where $g(x)$ appears in a given trace for g can be computed relative to A.

3. Now each A in $\mathrm{Low}(\mathsf{CR}, \mathsf{SR})$ is c.e. traceable by Theorem 3.1(I), hence by the above computably traceable, and Theorem 3.1(II) follows.

We discuss lowness for the remaining pairs of randomness notions. Nies has shown that A is $\mathrm{Low}(\mathsf{MR}, \mathsf{CR})$ iff A is $\mathrm{Low}(\mathsf{MR})$ iff A is K-trivial, where A is K-trivial if $\forall n\ K(X \upharpoonright n) \leq K(n) + O(1)$ (see [10]). Here $K(\sigma)$ denotes the prefix-free Kolmogorov complexity of $\sigma \in 2^{<\omega}$. Finally, he shows that a real A which is $\mathrm{Low}(\mathsf{CR})$ is computable. Namely, A is both K-trivial and hyperimmune-free. Since all K-trivial reals are Δ^0_2, and all hyperimmune-free Δ^0_2 reals are computable, the conclusion follows.

4. Proof of the Main Result

We first need to develop a few useful facts from measure theory.

Definition 4.1. *A measurable set A has density d at a real X if*

$$\lim_{n\to\infty} \mu_{(X\upharpoonright n)} A = d.$$

A basic result is the following

Theorem 4.2 (Lebesgue Density Theorem)**.** *Let $\Xi(A) = \{X : A$ has density 1 at $X\}$. If A is a measurable set then so is $\Xi(A)$, and the measure of the symmetric difference of A and $\Xi(A)$ is zero.*

Corollary 4.3. *Let C be a measurable subset of 2^ω with $\mu C > 0$. Then for each $\delta < 1$, there is an $\alpha \in 2^{<\omega}$ such that $\mu_\alpha C \geq \delta$.*

We will use the following consequence of Corollary 4.3.

Lemma 4.4. *Let $0 < \epsilon \leq 1$. If U_n, $n \in \omega$ and V are open subsets of 2^ω with $\bigcap_{n\in\omega} U_n \subseteq V$ and $\mu V < \epsilon$, then there exist σ and n such that $\mu_\sigma(U_n - V) = 0$ and $\mu_\sigma V < \epsilon$.*

Proof. Suppose otherwise; we shall obtain a contradiction by constructing a real in $\bigcap_{n\in\omega} U_n - V$. Let $\sigma_0 = \lambda$ and assume we have defined σ_n such that $\mu_{\sigma_n} V < \epsilon$. By hypothesis $\mu_{\sigma_n}(U_n - V) > 0$, so there is a $[\tau] \subseteq U_n$ such that $\mu_{\sigma_n}([\tau] - V) > 0$. In particular $\tau \succeq \sigma_n$ and $\mu_\tau V < 1$. Let $C = 2^\omega - V$, a closed and hence measurable set. By Corollary 4.3 applied to C (and with 2^ω replaced by $[\tau]$), there exists $\sigma_{n+1} \succeq \tau$ such that $\mu_{\sigma_{n+1}} V < \epsilon$. Let X be the real that extends all σ_n's constructed in this way. Since $[\sigma_{n+1}] \subseteq U_n$ for all n we have that $X \in \bigcap_{n\in\omega} U_n$. But $[\sigma_n] \not\subseteq V$ for every n, so, since V is open, $X \notin V$. This contradiction completes the proof. $\square$

We now get to the proof of Theorem 3.1. First we show Theorem 3.1(I), namely, A is Low(MR, SR) iff A is c.e. traceable. We start with the "$\Leftarrow$" direction.

Lemma 4.5. *If A is c.e. traceable then A is* Low(MR, SR).

Proof. Assume that A is c.e. traceable and U^A is a Schnorr test relative to A. Let $U^A_{n,s}$, $n, s \in \omega$ be clopen sets, $U^A_{n,s} \subseteq U^A_{n,s+1}$, $U^A_n = \bigcup_{s\in\omega} U^A_{n,s}$, such that the $U^A_{n,s}$ are $\Delta^{0,A}_1$ classes uniformly in n and s. As $\mu U^A_n = 2^{-n}$, we may assume that $\mu U^A_{n,s} > 2^{-n}(1 - 2^{-s})$. Let f be an A-computable function such that $[S_{f(\langle n,s\rangle)}]^{\preceq} = U^A_{n,s}$. Since A is c.e. traceable and $f \leq_T A$, we can let T be a c.e. trace of f. By Proposition 2.1, we may choose T such that in addition $|T_x| \leq x$ for each $x > 0$.

We now want to define a sub-trace $\hat{T}$ of T, i.e., $\hat{T}_{\langle n,s\rangle} \subseteq T_{\langle n,s\rangle}$ for each n, s. The intent is that the open sets defined via $\hat{T}$ are small enough to give us a Martin-Löf test containing $\cap_{n\in\omega} U^A_n$, and nothing important is in $T_{\langle n,s\rangle} - \hat{T}_{\langle n,s\rangle}$. So let $\hat{T}_{\langle n,s\rangle}$ be the set of $e \in T_{\langle n,s\rangle}$ such that $2^{-n}(1 - 2^{-s}) \leq \mu[S_e]^{\preceq} \leq 2^{-n}$ and $[S_e]^{\preceq} \supseteq [S_d]^{\preceq}$ for some $d \in \hat{T}_{\langle n,s-1\rangle}$, where $\hat{T}_{\langle n,-1\rangle} = \omega$. Let

$$V_n = \bigcup \left\{ [S_e]^{\preceq} : e \in \hat{T}_{\langle n,s\rangle},\ s \in \omega \right\}.$$

Then $\mu V_n \leq 2^{-n}|\hat{T}_{\langle n,0\rangle}| + \sum_{s\in\omega} 2^{-s}2^{-n}|\hat{T}_{\langle n,s\rangle}|$. Since $|\hat{T}_{\langle n,s\rangle}| \leq |T_{\langle n,s\rangle}| \leq \langle n,s\rangle$ for $\langle n,s\rangle \neq 0$, and $\langle n,s\rangle$ has only polynomial growth in n and s, it is clear that

$\sum_{s\in\omega} 2^{-s}2^{-n}|\hat{T}_{\langle n,s\rangle}|$ is finite and goes effectively to 0 as $n\to\infty$, hence the same can be said of μV_n. Hence there is a recursive function f such that $\mu V_{f(n)} \le 2^{-n}$. Let $\tilde{V}_n = V_{f(n)}$. Then $\tilde{V}$ is a Martin-Löf test, and $\bigcap_n U_n^A \subseteq \bigcap_n \tilde{V}_n$. That is, each Schnorr test relative to A is contained in a Martin-Löf test. It follows that each real that is Martin-Löf random is Schnorr random relative to A, and the proof is complete. $\square$

Next we will show the "⇒" direction of Theorem 3.1(I). The proof is similar to the "⇒" of Theorem 2.2.

Definition 4.6. *For $k,l\in\omega$ define the clopen set*

$$B_{k,l} = \bigcup \left\{[\tau 1^k] : \tau \in 2^{<\omega}, |\tau| = l\right\},$$

where 1^k is a string of 1's of length k.

Note that $\mu B_{k,l} = 2^{-k}$ for all l.

Lemma 4.7. *If $A\in 2^\omega$ is* $\mathrm{Low}(\mathsf{MR},\mathsf{SR})$ *then A is c.e. traceable.*

Proof. Note that A is $\mathrm{Low}(\mathsf{MR},\mathsf{SR})$ iff for every Schnorr test U^A relative to A, $\bigcap_{n\in\omega} U_n^A \subseteq \bigcap_{b\in\omega} R_b$ (recall that R is a universal Martin-Löf test).

Oversimplifying a bit, one can say that the proof below goes as follows. We code a given $g\le_T A$ into a Schnorr test U^g relative to A. Then by hypothesis, $\bigcap_n U_n^g \subseteq \bigcap_n R_n$; in fact we will only use the fact that $\bigcap_n U_n^g \subseteq R_3$. We then define a c.e. trace T, namely T_k is the set of l such that $B_{k,l} - R_3$ has small measure in some sense. Since R_3 has rather small measure, $B_{k,l} - R_3$ will tend to have big measure, which means that there will be only a few l for which $B_{k,l} - R_3$ has small measure; in other words, T_k has small size. Moreover we make sure T is a trace for g and so A is c.e. traceable.

We now give the proof details. Suppose we want to find a trace for a given function $g\le_T A$. We define the test U^g by stipulating that

$$U_n^g = \bigcup_{k>n} B_{k,g(k)}.$$

It is easy to see that μU_n^g can be approximated computably in A, so after taking a subsequence of U_n^g, $n\in\omega$, we may assume U^g is a Schnorr test relative to A. Hence by assumption $\bigcap U^g \subseteq \bigcap_{b\in\omega} R_b$. Thus $V = R_3$ contains $\bigcap U^g$ and $\mu V < \frac{1}{4}$. We may assume throughout that $g(k)\ge k$ for every k because from a trace for $g(k)+k$ one can obtain a trace for g with the same bound. By Lemma 4.4, there exist σ and n such that $\mu_\sigma(U_n^g - V) = 0$ and $\mu_\sigma V < 1/4$. As $U_0^g \supseteq U_1^g \supseteq \cdots$, we can choose σ and n with the additional property $n\ge|\sigma|$. Hence for each $k>n$, we have $g(k)\ge k>n\ge|\sigma|$ and hence $g(k)\ge|\sigma|$.

Let $\tilde{V} = V|\sigma$, let $\tilde{g}(k) = \max\{0, g(k)-|\sigma|\}$, and

$$T_k = \left\{ l : \mu(B_{k,l} - \tilde{V}) < 2^{-(l+3)} \right\}.$$

Note that for each $l\in\omega$, if $l\ge|\sigma|$ then $B_{k,l}|\sigma = B_{k,l-|\sigma|}$. So since $g(k)\ge|\sigma|$,

$$U_n^g|\sigma = \bigcup_{k>n} B_{k,g(k)}|\sigma = \bigcup_{k>n} B_{k,g(k)-|\sigma|} = U_n^{\tilde{g}},$$

so $\mu(U_n^{\tilde{g}} - \tilde{V}) = \mu_\sigma(U_n^g - V) = 0$. Hence $\tilde{g}(k) \in T_k$ for all $k > n$.

Since $\tilde{V}$ is a Σ_1^0 class, it is evident that T is a c.e. set of integers; indeed $B_{k,l} - \tilde{V}$ is a Π_1^0 class, so we can enumerate the fact that certain basic open sets $[\sigma]$ are disjoint from it, until the measure remaining is as small as required. A trace for g is obtained as follows:

$$G_k = \begin{cases} \{l + |\sigma| : l \in T_k\} & \text{if } k > n; \\ \{g(k)\} & \text{if } k \leq n. \end{cases}$$

We now show that G is a trace for g, i.e. for all $k \in \omega$, $g(k) \in G_k$. If $k \leq n$ then this holds by definition of G_k; so suppose $k > n$. Then $g(k) > k > n > |\sigma|$, so $\tilde{g}(k) = g(k) - |\sigma|$ so $g(k) = \tilde{g}(k) + |\sigma|$. As $k > n$, $\tilde{g}(k) \in T_k$ and hence $g(k) \in G_k$.

Clearly G is c.e.; so it remains to show that $|G_k|$ is computably bounded, independently of g. As $|G_k| = |T_k|$ for $k > n$ and $|G_k| = 1$ for $k \leq n$, this is a consequence of Lemma 4.8 below. □

Lemma 4.8. *If $\tilde{V}$ is a measurable set with $\mu\tilde{V} < \frac{1}{4}$, and $T_k = \{l : \mu(B_{k,l} - \tilde{V}) < 2^{-(l+3)}\}$, then for $k \geq 1$, $|T_k| < 2^k k$.*

Proof. Observe that by definition of T_k,

$$\sum_{l \in T_k} \mu(B_{k,l} - \tilde{V}) < \sum_{l \in T_k} 2^{-(l+3)} \leq \frac{1}{8} \sum_{l \in \omega} 2^{-l} = \frac{1}{4},$$

so

$$\mu \bigcup_{l \in T_k} B_{k,l} - \mu\tilde{V} \leq \mu \bigcup_{l \in T_k} (B_{k,l} - \tilde{V}) \leq \frac{1}{4}.$$

As $\mu\tilde{V} < \frac{1}{4}$ we obtain that

$$\mu \bigcup_{l \in T_k} B_{k,l} < \frac{1}{2}.$$

As observed above $\mu B_{k,l} = 2^{-k}$. Moreover, for k fixed, the $B_{k,l}$'s are mutually independent as soon as the l's are taken sufficiently far apart. In fact sufficiently far here means a distance of k. So for $k \geq 1$, we let T_k^* be a subset of T_k consisting of $\left\lfloor \frac{|T_k|}{k} \right\rfloor$ elements all of which are sufficiently far apart. (Here $\lfloor a \rfloor$ is the greatest integer $\leq a$.) To show such a set exists we may assume we are in the worst case, where the elements of T_k are closest together: say $T_k = \{0, \ldots, |T_k| - 1\}$. Then let $T_k^* = \{mk : 0 \leq m \leq \left\lfloor \frac{|T_k|}{k} \right\rfloor - 1\}$. As $\left(\left\lfloor \frac{|T_k|}{k} \right\rfloor - 1\right) k \leq |T_k| - k \leq |T_k| - 1 \in T_k$, this makes $T_k^* \subseteq T_k$. Write $\alpha = \left\lfloor \frac{|T_k|}{k} \right\rfloor$. We now have

$$\mu \bigcap_{l \in T_k} (2^\omega - B_{k,l}) \leq \mu \bigcap_{l \in T_k^*} (2^\omega - B_{k,l}) = (1 - 2^{-k})^\alpha$$

and hence

$$1-(1-2^{-k})^{\alpha} \leq 1-\mu \bigcap_{l\in T_k}(2^{\omega}-B_{k,l}) = \mu 2^{\omega} - \mu \bigcap_{l\in T_k}(2^{\omega}-B_{k,l})$$

$$\leq \mu\left(2^{\omega}-\bigcap_{l\in T_k}(2^{\omega}-B_{k,l})\right) = \mu \bigcup_{l\in T_k} B_{k,l} < \frac{1}{2}.$$

From the inequality above we obtain, letting $m = 2^k - 1$,

$$\left(1-\frac{1}{m+1}\right)^{\alpha} = (1-2^{-k})^{\alpha} > \frac{1}{2}$$

or $\left(\frac{m+1}{m}\right)^{\alpha} < 2$. Now suppose $\alpha \geq m$. Then $\left(\frac{m+1}{m}\right)^{\alpha} \geq \left(\frac{m+1}{m}\right)^{m} \geq 2$ as $(m+1)^m \geq m^m + m^{m-1}\binom{m}{1} = 2m^m$. So we conclude $\alpha < m = 2^k - 1$. Now by definition of α, we have $\frac{T_k}{k} \leq \alpha + 1 < 2^k$ and so $|T_k| < 2^k k$; this completes the proof. $\square$

In order to prove Theorem 3.1(II), recall that, by Theorem 2.2, each computably traceable real is Low(SR). Thus it suffices to show that each Low(CR, SR) real is computably traceable. The first ingredient to show this is the following result from [2].

Lemma 4.9. *If A is* Low(CR, SR) *then A is hyperimmune-free.*

Proof. Suppose A is not hyperimmune-free, so there is a function $g \leq_T A$ not dominated by any computable function. Thus for each computable f, $\exists^{\infty} x\ f(x) \leq g(x)$. We will define a computably random real X and an A-computable martingale L which succeeds on X in the sense of Schnorr, so A is not Low(CR, SR). In the following α, β, γ denote finite subsets of ω, and $n_\alpha = \sum_{i\in\alpha} 2^i$ (here $n_\emptyset = 0$).

Let $\{M_e\}_{e\in\omega}$ be an effective listing of all partial computable martingales with range included in $[1/2, \infty)$. At stage t, we have a finite portion $M_e[t]$ whose domain is a subset of some set of the form $2^{\leq n}$ for some n. If X is not computably random, then $\lim_{n\to\infty} M_e(X\restriction n) = \infty$ for some total M_e by [13]. Let

$$TMG = \{e : M_e \text{ is total}\}.$$

For finite sets α, β, let us in this proof say that α is a *strong subset* of β (denoted $\alpha \subseteq^{+} \beta$) if $\alpha \subseteq \beta$ and moreover for each $i \in \omega$, if $i \in \beta - \alpha$ then $i > \max(\alpha)$. So the possibility that β contains an element smaller than some element of α is ruled out.

For certain α, and all those included in TMG, we will define strings x_α, in such a way that $\alpha \subseteq^{+} \beta \Rightarrow x_\alpha \preceq x_\beta$. We choose the strings in such a way that $M_e(x_\alpha)$ is bounded by a fixed constant (depending on e), for each total M_e and each α containing e. Then the set of integers

$$X = \bigcup_{e\in\omega} x_{TMG\cap[0,e]}$$

is a computably random real. On the other hand we are able to define an A-computable martingale L which Schnorr succeeds on X. We give an inductive definition of the strings x_α, "scaling factors" $p_\alpha \in \mathbb{Q}^{+}$ (positive rationals) (we do not define $p_\emptyset$) and partial computable martingales M_α such that, if x_α is defined then

$$M_\alpha(x_\alpha) \text{ converges in } g(|x_\alpha|) \text{ steps and } M_\alpha(x_\alpha) < 2. \tag{1}$$

It will be clear that A can decide if $y = x_\alpha$ given inputs y and α.

Let $x_\emptyset = \lambda$, and let $M_\emptyset$ be the constant zero function (we may assume g is such that $M_\emptyset(\lambda)$ converges in $g(0)$ steps). Now suppose $\alpha = \beta \cup \{e\}$ where $e > \max(\beta)$, and inductively suppose that (1) holds for β. Let

$$p_\alpha = \tfrac{1}{2} 2^{-|x_\beta|}(2 - M_\beta(x_\beta)),$$

and let $M_\alpha = M_\beta + p_\alpha M_e$. Since M_e is a martingale on its domain, $M_e(z) \le 2^{|z|}$ for any z. So writing $b = M_\beta(x_\beta)$, we have $M_\alpha(x_\beta) = b + p_\alpha M_e(x_\beta) < b + p_\alpha 2^{|x_\beta|} = b + \frac{1}{2}(2-b) = 1 + \frac{b}{2} < 1 + \frac{2}{2} = 2$ if $M_\alpha(x_\beta)$ is defined.

To define x_α, we look for a sufficiently long $x \succeq x_\beta$ such that M_α does not increase from x_β to x and $M_\alpha(x)$ converges in $g(|x|)$ steps. In detail, for larger and larger $m > |x_\beta|$, $m \ge 4n_\alpha$, if no string y, $|y| < m$ has been designated to be x_α as yet, and if $M_\alpha(z)$ (i.e., each $M_e(z), e \in \alpha$) converges in $g(m)$ steps, for each string z of length $\le m$, then choose x_α of length m, $x_\beta \prec x_\alpha$ such that M_α does not increase anywhere from x_β to x_α.

Claim 4.10. *If $\alpha \subseteq TMG$, then x_α and p_α (the latter only if $\alpha \neq \emptyset$) are defined.*

Proof. The lemma is trivial for $\alpha = \emptyset$. Suppose it holds for β, and $\alpha = \beta \cup \{e\} \subseteq TMG$, where $e > \max(\beta)$. Since the function

$$f(m) = \mu s \forall e \in \alpha \forall x\, [\, |x| \le m \Rightarrow M_e(x) \textit{ converges in } s \textit{ steps}]$$

is computable, there is a least $m \ge 4n_\alpha$, $m > |x_\beta|$ such that $g(m) \ge f(m)$. Since there is a path down the tree starting at x_β where M_α does not increase, the choice of x_α can be made. □

Claim 4.11. *If $\beta \subseteq^+ \alpha$ are finite sets then $M_\beta(x) \le M_\alpha(x)$ for all x.*

Proof. This is clear by induction from the case $\alpha = \beta \cup \{e\}$, i.e., the case where $\alpha - \beta$ has only one element. □

Claim 4.12. *X is computably random.*

Proof. Suppose M_e is total. Let $\alpha = TMG \cap [0, e]$. Suppose $\alpha \subseteq \gamma$, $\gamma' = \gamma \cup \{i\}$, $\max(\gamma) < i$ and $\gamma' \subseteq TMG$. Then $\alpha \subseteq^+ \gamma \subseteq^+ \gamma'$. Hence by Claim 4.11, for each x with $x_\gamma \preceq x \preceq x_{\gamma'}$, we have

$$p_\alpha M_e(x) \le M_\alpha(x) \le M_{\gamma'}(x) \le M_{\gamma'}(x_\gamma) < 2,$$

hence $M_e(x) < 2/p_\alpha$ for each $x \prec X$, and so the capital of M_e on X is bounded. □

Claim 4.13. *There is a martingale $L \le_T A$ which effectively succeeds on X. In fact,*

$$\exists^\infty x \prec X \ L(x) \ge \lfloor |x|/4 \rfloor.$$

Proof. For a string z, let $r(z) = \lfloor |z|/2 \rfloor$. We let $L = \sum_\alpha L_\alpha$, where L_α is a martingale with initial capital $L_\alpha(\lambda) = 2^{-n_\alpha}$ which bets everything along x_α from $x_\alpha \upharpoonright r(x_\alpha)$ on. More precisely, if x_α is undefined then L_α is constant with value 2^{-n_α}. Otherwise, for convenience we let $x = x_\alpha \upharpoonright 2r(x_\alpha)$ and work with x instead of x_α; and define L_α on a string y as follows.

- If y does not contain "half of x", i.e. if $x \upharpoonright r(x) \not\preceq y$ then just let $L_\alpha(y) = 2^{-n_\alpha}$.

- If y does contain "half of x" but y and x are incompatible, then let $L_\alpha(y) = 0$.
- If y contains "half of x" and x and y are compatible, then let $L_\alpha(y) = 2^{-n_\alpha} 2^{\min(|y|-r(x), r(x))}$.

So if y contains x then $L_\alpha(y) = 2^{r(x)-n_\alpha}$, so we make no more bets once we extend x_α, and if x contains y then $L_\alpha(y) = 2^{|y|-r(x)-n_\alpha}$, i.e. we double the capital for each correct bit of x beyond $x \upharpoonright r(x)$.

Note that $L(\lambda) = \sum_\alpha 2^{-n_\alpha}$ and, as each $k \in \omega$ has a unique binary expansion and hence is equal to n_α for a unique finite set α, we have $L(\lambda) = \sum_{k\in\omega} 2^{-k} = 2$. Moreover it is clear that each L_α satisfies the martingale property $L_\alpha(x0)+L_\alpha(x1) = 2L_\alpha(x)$ hence so does L.

L effectively succeeds on X. Indeed, as $|x_\alpha| \geq 4n_\alpha$, we have $L_\alpha(x_\alpha) = 2^{r(x_\alpha)-n_\alpha} \geq 2^{\lfloor |x_\alpha|/2 \rfloor - \lfloor |x_\alpha|/4 \rfloor} \geq 2^{\lfloor |x_\alpha|/4 \rfloor} \geq \lfloor |x_\alpha|/4 \rfloor$ since $2^q \geq q$ for each $q \in \omega$.

Finally, we show that $L \leq_T A$. Given input y, we use g to see if some string x, $|x| \leq 2|y|$ is x_α. If not, $L_\alpha(y) = 2^{-n_\alpha}$. Else we determine $L_\alpha(y)$ from x using the definition of L_α. $\square$

The second ingredient to the proof of Theorem 3.1(II) is the following fact of independent interest.

Proposition 4.14. *If A is hyperimmune-free and c.e. traceable, then A is computably traceable.*

Proof. Let $f \leq_T A$ and let h be as in the definition of c.e. traceability. Let $g(x) = \mu s. f(x) \in W_{h(x),s}$ (where $W_{e,s}$ is the approximation at stage s to the c.e. set W_e). Then $g \leq_T A$ and so since A is hyperimmune-free, g is dominated by a computable function r. So if we replace $W_{h(x)}$ by $W_{h(x),r(x)}$, we obtain a computable trace for f. $\square$

Lemma 4.9 and Proposition 4.14 together establish Theorem 3.1(II): if A is Low$(\mathsf{CR}, \mathsf{SR})$, then A is c.e. traceable by Theorem 3.1(I), and hyperimmune-free by Lemma 4.9. Thus by Proposition 4.14, A is computably traceable.

As a corollary, we obtain an answer to the question of Ambos-Spies and Kučera.

Corollary 4.15. *A real A is S-low if and only if it is S_0-low.*

Proof. This follows by Theorem 2.2 and Theorem 3.1(II), since each computably traceable real is S_0-low. $\square$

5. Lowness notions related to Chaitin's halting probability

Recall that A is array computable if there is a function $f \leq_{wtt} \emptyset'$ bounding all functions computable from A on almost all inputs.

Theorem 5.1. *If $\Omega \in \mathsf{SR}^A$ then A is array computable.*

Proof. We show that the function $\beta(x) = \mu s\ \Omega_s \upharpoonright 3x = \Omega \upharpoonright 3x$ dominates each function $\alpha \leq_T A$. Since $\beta \leq_{wtt} \Omega \leq_{wtt} 0'$, this shows that A is array computable.

Given $\alpha \leq_T A$, consider the A-computable martingale $M = \sum_p M_p$, where M_p is the martingale which is has the value 2^{-p} on all strings of length up to p, and then doubles the capital along the string $y = \Omega_{\alpha(p)} \upharpoonright 3p$, so that $M_p(y) = 2^p$. Note that $M(z)$ is rational for each z. If $\alpha(p) > \beta(p)$ for infinitely many p, then M Schnorr succeeds on Ω, contradiction. $\square$

Corollary 5.2. *If A is c.e. then $\Omega \in \mathsf{SR}^A$ iff A is c.e. traceable.*

Proof. For c.e. A, array computable implies c.e. traceable by Ishmukhametov [5]. $\square$

In [12] it is shown that c.e. traceable degrees do not contain diagonally non-computable functions, hence by a result of Kučera [7], the c.e. traceable degrees have measure zero. On the other hand every real A which is Martin-Löf random relative to Ω satisfies that Ω is MR^A, by van Lambalgen's theorem [15], and hence the measure of the set of A such that Ω is SR^A is one; so A c.e. traceable is not equivalent to $\Omega \in \mathsf{SR}^A$. Also, $\Omega \in \mathsf{SR}^A$ is not equivalent to A being array computable, as we now show.

The following notion of forcing appears implicitly in [4].

Definition 5.3. *A tree T is a set of strings $\sigma \in 2^{<\omega}$ such that if $\sigma \in T$ and τ is a substring of σ then $\tau \in T$. A tree T is full on a set $F \subseteq \omega$ if whenever $\sigma \in T$ and $|\sigma| \in F$, then $\sigma 0 \in T$ and $\sigma 1 \in T$. Let F_n, $n \in \omega$ be finite sets such that each F_n is an interval of ω, $|F_{n+1}| > |F_n|$ and $\bigcup_n F_n = \omega$. The sequence F_n, $n \in \omega$ is called a* very strong array*. Let P be the set of computable perfect trees T such that T is full on F_n for infinitely many n. Order P by $T_1 \leq_P T_2$ if $T_1 \subseteq T_2$. The partial order $(P, \leq_P)$ is a notion of forcing we call very strong array forcing.*

Theorem 5.4. *For each real X there is a hyperimmune-free real A such that no real computable from X is in SR^A. In particular, as hyperimmune-free implies array computable, there is an array computable real A such that $\Omega \notin \mathsf{SR}^A$.*

Proof. Let A be sufficiently generic for very strong array forcing. Then A is hyperimmune-free, as may be proved by modifying the standard construction of a hyperimmune-free degree [8] to work with trees that are full on infinitely many F_n, $n \in \omega$.

Moreover, for each real B computable from X, there is an n (hence infinitely many n) such that A agrees with B on F_n. Indeed, given a condition T a condition extending T and ensuring the existence of such an n is obtained as a full subtree of T.

Hence no real B computable from X is Schnorr random relative to A. Indeed the measure of the set of those oracles B that agree with A on infinitely many F_n is zero, and it is easy to see that the measure of those B such that for some $k > n$, A and B agree on F_k, goes to zero effectively as $n \to \infty$. Hence there is a Schnorr test relative to A which is failed by any such B, as desired. $\square$

Question 5.5. *Characterize the (c.e.) sets of integers A such that Ω is computably random relative to A. Does this depend on the version of Ω used?*

Acknowledgements

The first author was supported by a Marie Curie Fellowship of the European Community Programme "Improving Human Potential" under contract number HPMF-

CT-2002-01888. The second author was partially supported by University of Auckland New Staff research grant, No 3603229/9343, and by the Marsden fund of New Zealand, No 03-UOA-130.

References

[1] Klaus Ambos-Spies and Antonín Kučera. Randomness in computability theory. In *Computability theory and its applications (Boulder, CO, 1999)*, volume 257 of *Contemp. Math.*, pages 1–14. Amer. Math. Soc., Providence, RI, 2000.

[2] B. Bedregal and A. Nies. Lowness properties of reals and hyper-immunity. In *Wollic 2003*, volume 84 of *Electronic Notes in Theoretical Computer Science*. Elsevier, 2003. http://www.elsevier.nl/locate/entcs/volume84.html.

[3] A. Church. On the concept of a random sequence. *Bull. Amer. Math. Soc*, 46:130–135, 1940.

[4] R. G. Downey, Carl G. Jockusch, Jr., and M. Stob. Array nonrecursive sets and genericity. In T. A. Slaman S. B. Cooper and S. S. Wainer, editors, *Computability, Enumerability, Unsolvability: Directions in Recursion Theory*, London Mathematical Society Lecture Notes Series, pages 93–104. Cambridge University Press, 1996.

[5] Shamil Ishmukhametov. Weak recursive degrees and a problem of Spector. In *Recursion theory and complexity (Kazan, 1997)*, volume 2 of *de Gruyter Ser. Log. Appl.*, pages 81–87. de Gruyter, Berlin, 1999.

[6] A. Kucera and S. Terwijn. Lowness for the class of random sets. *J. Symbolic Logic*, 64:1396–1402, 1999.

[7] Antonín Kučera. Measure, Π^0_1-classes and complete extensions of PA. In *Recursion theory week (Oberwolfach, 1984)*, volume 1141 of *Lecture Notes in Math.*, pages 245–259. Springer, Berlin, 1985.

[8] D. A. Martin and W. Miller. The degrees of hyperimmune sets. *Z. Math. Logik Grundlag. Math.*, 14:159–166, 1968.

[9] P. Martin-Löf. The definition of random sequences. *Inform. and Control*, 9:602–619, 1966.

[10] A. Nies. Lowness properties and randomness. To appear in Advances in Mathematics.

[11] André Nies, Frank Stephan, and Sebastiaan Terwijn. Randomness, relativization and turing degrees. To appear in the Journal of Symbolic Logic.

[12] Bjørn Kjos-Hanssen, Wolfgang Merkle, and Frank Stephan. Kolmogorov Complexity and the Recursion Theorem. To appear.

[13] Claus-Peter Schnorr. *Zufälligkeit und Wahrscheinlichkeit. Eine algorithmische Begründung der Wahrscheinlichkeitstheorie*. Springer-Verlag, Berlin, 1971. Lecture Notes in Mathematics, Vol. 218.

[14] Sebastiaan A. Terwijn and Domenico Zambella. Computational randomness and lowness. *Journal of Symbolic Logic*, 66(3):1199–1205, 9 2001.

[15] Michiel van Lambalgen. The axiomatization of randomness. *J. Symbolic Logic*, 55(3):1143–1167, 1990.

[16] D. Zambella. On sequences with simple initial segments. ILLC technical report ML 1990 -05, Univ. Amsterdam, 1990.