Algorithmic Randomness and Computability
Rod Downey

Abstract. We examine some recent work which has made significant progress in out understanding of algorithmic randomness, relative algorithmic randomness and their relationship with algorithmic computability and relative algorithmic computability.

1. Introduction

In the last few years we have seen some very exciting progress in our understanding of algorithmic randomness and its relationship with computability and complexity. These results have centered around a programme which attempts to answer questions of the following form: when is one real more random than another? How should this be measured? How would such measures of calibration relate to other measures of complexity of reals, such as the traditional measures of relative complexity like Turing degrees, which measure relative computability? These investigations have revealed deep and hitherto unexpected properties of randomness, anti-randomness and algorithmic complexity, as well as pointing at analogs in other areas, and answering questions from apparently completely unrelated areas.

In this paper I will attempt to give a brief (and biased) overview of some of the more recent highlights. I apologize for ignoring important work relating the collection of random strings with complexity theory such as [1, 2], and work on randomness for computably enumerable sets such as Kummer [48, 49] and Muchnik and Positelsky [71], purely for space reasons. This overview will be too short to give a complete account of the all of the progress. For a fuller picture, I refer the reader to the long surveys of Downey, Hirschfeldt, Nies and Terwijn [28], Downey [16, 15, 17], Terwijn [96] and the upcoming monographs Downey and Hirschfeldt [22][1], and Nies [77].

We will look at various methods of calibration by initial segment complexity such as those introduced by Solovay [89], Downey, Hirschfeldt, and Nies [26], Downey, Hirschfeldt, and LaForte [23], Downey [16], as well as other methods such as lowness notions of Kučera and Terwijn [47], Terwijn and Zambella [97], Nies [75, 76], Downey, Griffiths and Reid [21], and methods such as higher level randomness notions going back to the work of Kurtz [50], Kautz [38], and Solovay [89], and other calibrations of randomness based on changing definitions along the lines of Schnorr, computable, s-randomness, etc. Particularly fascinating is the recent work on lowness, which began with Downey, Hirschfeldt, Nies and Stephan, and developed in a series of deep papers by Nies [75, 76] and his co-authors.

---

[1]Available in prelimininary form at `www.mcs.vuw.ac.nz/∼downey`

2. Preliminaries

Since most of our results are concerned with effectiveness/computability, we assume that the reader is familiar with the basic facts concerning computability theory/recursion theory. Thus, we will regard countable sets as effectively coded in the natural numbers and consider effective processes on them as computable ones. For example, an effective prediction function would be classified according to it computability. We assume that the reader is also familiar with semi-computable (computably enumerable) processes such as the computably enumerable set coding the halting problem $\emptyset' = \{(e, x) : \text{the } e\text{-th program halts on input } x\}$. Such computable enumerable problems can be represented by sets W defined as $x \in W$ iff $\exists y R(x, y)$, where R is a computable relation. We will call a set in the form $\exists y R(x, y)$, Σ_1^0. If $\mathbb{N} - A$ is Σ_1^0, then we say that A is Π_1^0. If A is both Σ_1^0 and Π_1^0 we say that A is Δ_1^0 (and this is the same as being computable). This process can be extended to the *arithmetical hierarchy*. We will say that A is Σ_n^0 iff there is a Π_{n-1}^0 relation R such that $x \in A$ iff $\exists y R(x, y)$. (Equivalently, x is in A iff $\exists y \forall z \ldots$ (with n alternations)$Q(x, y, z, \ldots)$ and Q computable.) Analogously, we can define Π_n^0 and Δ_n^0. We will also assume that the reader is familiar with the process of *relativization* which means that we put oracles (allowing for "read only memory") on our machines. These oracles allow for computations in which a finite number of effectively generated membership queries of the oracle set are allowed. Thus, for instance, $A' = \{(e, x) : \text{the } e\text{-th program halts on input } x \text{ when given oracle } A\}$. This is the halting problem *relativized to A*, usually pronounced "A-jump". If we classify sets under the preordering $\leq_T$ we will write $A \leq_T B$ to mean that membership of A can be computed by a program with access to B as an oracle. (Here we identify sets with their characteristic functions, and hence as reals: members of Cantor space 2^ω.) The equivalence classes of $\leq_T$, which calibrate countable sets into classes of "equi-computability" are called Turing degrees, after the famous Alan Turing. We remark that the simplest kind of Turing reduction is called an m-reduction (for many-one) and is defined as follows: $A \leq_m B$ means that there is a computable function f such that $x \in A$ iff $f(x) \in B$. Thus to figure out if x is in A from B, the algorithm simply says : compute $f(x)$ and ask B if $f(x)$ is in B. It is easy to show that for any computably enumerable set A, $A \leq_m \emptyset'$, so that the halting problem $\emptyset'$ if m-complete, in that it is the most complicated computably enumerable set as measured by m-reducibility[2]. We remark that the relativization of the halting problem be algorithmically unsolvable is that $A' \not\leq_T A$ for any set A. The relativization of the halting problem is intrinsically tied with the halting problem. Namely, $\emptyset''$, which is defined as the halting problem gained with the halting problem as an oracle is a natural Σ_2^0 set and it can compute any Π_2^0 set and any Σ_2^0 set, and similarly for $\emptyset^{(n+1)}$.

Any other notions from computability needed are introduced in context. We also refer the reader to Soare [86] for further background material in computabil-

---

[2]Additionally, it might seem that there might be various versions of the halting problem depending of which programming language, or which encoding, is used. It can be shown that that are all of the same m-degree, and hence are basically all the same. More on this in the context of randomness later.

ity, and to Li-Vitanyi [56] or Calude [6] for general background in algorithmic randomness.

In this paper "real" will be interpreted as a member of Cantor space 2^ω with sub-basic clopen sets $[\sigma] = \{\sigma\alpha : \alpha \in 2^\omega\}$, for $\sigma \in 2^{<\omega}$. This space is equipped with the standard Lebesgue measure, where, for $\sigma \in 2^{<\omega}$, $\mu([\sigma]) = 2^{-|\sigma|}$. There have been investigations on other measures than the uniform one, and on other spaces (the latter notably by Gács [34]), but space precludes a thorough discussion here. For Cantor space up to degree things, speaking loosely, it does not matter measure is used, so long as it is not atomic. Finally, the initial segment of a real α (or a string) of length n will be denoted by $\alpha \restriction n$.

3. Three approaches to randomness

In terms of measure a any two reals occur with probability zero, yet we would argue that a real $\alpha = 01010101\ldots$ would not seem random. How should we understand this?

3.1. Martin-Löf randomness. The first author to attempt to grapple with trying to "define" randomness was von Mises [101]. Von Mises was a statistician and attempted to define randomness in terms of statistical laws. For instance, he argued that a random real should pass all statistical tests. Thus, he argued, if one "selected" from a real $\alpha = a_0 a_1 \ldots$ some subsequence $a_{i_0}, a_{i_1}, \ldots$, then $\lim_{n\to\infty} \frac{|\{j : a_{i_j} = 1 \wedge 1 \leq j \leq n\}|}{n}$ should be $\frac{1}{2}$. Naturally, von Mises lacked the language needed to suggest which selection rules should be considered. That awaited the development of computable function theory in the 1930's by Church and others, which then allowed us to argue that a random real should be "computably stochastic" in the sense of von Mises.

Unfortunately, Wald and others showed that there are some significant problems (see van Lambalgen [99] for a discussion) with this approach, known as computable stochasticity. Here I refer the reader to Ambos-Spies [3], Merkle [62, 63], and Uspensky, Semenov and Shen [98]. The first really acceptable version of von Mises idea was developed by Per Martin-Löf in [60]. He argued that any effective statistical test was an effective null set and a random real should be one that simply avoids any effective null set.

The notion of an effective collection of reals is are called effective classes. As a direct analog of the arithmetical hierarchy. A Σ_1^0 class U is a "c.e. set of reals" in the sense that there is a computable relation R such that for each real α, $\alpha \in U$ iff $\exists x R^\alpha(x)$, where R^α denotes R with oracle α. An equivalent definition is that U is a Σ_1^0 class iff there is a c.e. set of intervals W such that $U = \cup\{[\sigma] : \sigma \in W\}$. Now we can make our intuition of avoiding all effective statistical tests more precise, as follows.

Definition 3.1. (Martin-Löf [60]) A set of reals $A \subseteq 2^\omega$ is Martin-Löf null (or Σ_1-null) if there is a uniformly c.e. sequence $\{U_i\}_{i\in\omega}$ of Σ_1^0-classes (called a *Martin-*

Löf test) such that $\mu(U_i) \leq 2^{-i}$ and $A \subseteq \bigcap_i U_i$. $\alpha \in 2^\omega$ is Martin-Löf random, or 1-random, if $\{\alpha\}$ is not Σ_1-null.

This definition and variations form common bases for the theory of algorithmic randomness. There are also two other approaches aside from the measure-theoretical. These include the incompressibility paradigm and the unpredictability paradigm.

It is possible to calibrate randomness in a method similar to the arithmetical hierarchy, by defining n-randomness exactly as above, except that Σ_1^0 null sets are replaced by Σ_n^0 null sets. It can be shown (Kurtz [50]) that $n+1$-randomness is 1-randomness relative to $\emptyset^{(n)}$, Stuart Kurtz [50] was the first meaning that if $\emptyset'$ is given as an oracle, what is the analog of Martin-Löf randomness. to systematically examine the relationship between n-randomness and the computability, although some unpublished work was to be found in Solovay [89], and 2-randomness was already to be found in Gaifman and Snir [35], in implicit form.

There has been quite some work clarifying the relationship between Turing reducibility and n-randomness. For example, it has long been known that if **a** is $n+1$-random then **a** is GL_n, meaning that $\mathbf{a} \cup \mathbf{0}^n = (\mathbf{a} \cup \mathbf{0})^n$, and that the "almost all" theory of degrees is decidable (Stillwell [93]). Recently some lovely new work has emerged. As an illustration, we mention the following unexpected result.

Theorem 3.2 (Miller and Yu [69]). *Suppose that $A \leq_T B$ and B is n-random and A is 1-random. Then A is n-random.*

3.2. Kolmogorov complexity. The key idea here is that a random string (as generated by a coin toss, say) should not be easily described by a short program. Thus, 10^{100} is easily described by a description much shorter than its length. This incompressibility idea was the famous approach pioneered by Kolmogorov [41] (also cf. Solomonoff [88]). For our programming language (which we take as Turing machines) we consider the lengths of strings σ producing a string τ. Think of σ as a description of τ under the action of the machine N. Then the N-complexity of the τ is the *length* of the shortest σ from which N produces τ. Since we can enumerate the machines $M_0, M_1, \ldots$, we can make a universal machine M which acts as $M(1^{e+1}0\sigma) = M_e(\sigma)$. Thus, there is canonical choice for the choice of machine up to a constant, and we define the (plain) *Kolmogorov complexity* of τ as

$$C(\tau) = \min\{|\sigma| : M(\sigma) = \tau\}.$$

The we would say that τ is C-random iff $C(\tau) \geq |\tau|$. We will also need conditional versions of this (and other) measures. We will write $C(\sigma|\nu)$ as the conditional plain complexity of σ given ν as an oracle. (We will use analogous notation for K below.)

Plain Kolmogorov complexity produces a nice theory of randomness for strings, but as Martin-Löf argued, plain complexity fails to capture the intentional meaning of "the bits of σ producing the bits of τ". This is the length of σ itself can be used in the program, giving $\tau + |\tau|$ many bits of information. Thus, it is easily shown that if α is sufficiently long then there is some n such that $C(\alpha \upharpoonright n) < n$,

meaning that there are *no* random reals if we take randomness to mean that all initial segments should be random[3].

This problem was overcome by Levin [51, 54], Schnorr [84], and Chaitin [10]), using monotone, process and prefix-free complexities. Here we focus on the prefix-free complexity. Recall that A of intervals is called *prefix-free* iff for all σ, τ, if $\sigma \prec \tau$, then $[\sigma] \in A$ implies $[\tau] \notin A$. Note that for such a set A,

$$\mu(A) = \sum \{2^{-|\sigma|} : [\sigma] \in A\}.$$

Levin and then Chaitin defined prefix-free Kolmogorov complexity using machines whose domains were prefix free. Again there is a universal one U (same argument) and we define

$$K(\tau) = \min\{|\sigma| : U(\sigma) = \tau\}.$$

Finally we can define a real to be K-random iff for all n, $K(\alpha \restriction n) \geq n - O(1)$. The concepts of Martin-Löf randomness and K-randomness are tied together as follows.

Theorem 3.3 (Schnorr, see Chaitin [10, 12]). *$A \in 2^\omega$ is Martin-Löf random if and only if it is K-random.*

Given Schnorr's Theorem, Solovay had asked whether $\liminf_s K(\Omega \restriction n) - n \to \infty$. This was solved affirmatively by Chaitin. However, there is a very attractive generalization of this due to Miller and Yu who show that the complexity of a random real must be above n eventually by "quite a bit."

Theorem 3.4 (Ample Excess Lemma, Miller and Yu [69]). *A real α is random iff*

$$\sum_{n \in \mathbb{N}} 2^{n - K(\alpha \restriction n)} < \infty.$$

Corollary 3.5 (Miller and Yu [70]). *Suppose that f is an arbitrary function with $\sum_{m \in \mathbb{N}} 2^{-f(m)} = \infty$. Suppose that α is 1-random. Then there are infinitely many m with $K(\alpha \restriction m) > m + f(m)$.*

Ther reader might wonder whether plain compelxity could be used to charcterize 1-randomness. There had been some natural "C-conditions" which had been shown to guarantee randomness. Martin-Löf showed that if a real had infinitely often maximal C-complexity then it would be random. That is, Kolmogorov observed that the greatest plain complexity a string σ can have is $|\sigma|$. We will say that a real is *Kolmogorov random* iff $\exists^\infty n[C(\alpha \restriction n) = n - O(1)$. If A is Kolmogorov random it is 1-random. But recently more has been shown. Chaitin showed that

---

[3]Specifically, every string ν corresponds to some number (string) in the length/lexicographic ordering of $2^{<\omega}$. Given a long string α, take any initial segment $\alpha \restriction n$. This corresponds to a number m in this way. Now consider the programme which, on input ρ interprets ρ's length as a string γ and outputs $\gamma\rho$. If this programme is enacted on $\alpha \restriction^{n+m}_{n+1}$ the segment of α of length m beginning after α, it will output $\alpha \restriction n + m$, allowing for compression of arbitrary segments.

the highest prefix-free complexity a string can have is $|\sigma| + K(|\sigma|)$, and we define α to be strongly Chaitin random iff $\exists^\infty n[(K(\alpha \restriction n) > n + K(n) - O(1)]$. Solovay [89] (see Yu, Ding, Downey [107]) showed that each 3-random is strongly Chaitin random, and every strongly Chaitin random real is Kolmogorov random and hence 1-random. It is not known if every Kolmogorov random real is strongly Chaitin random. The following remarkable result shows that Kolmogorov randomness can be characterized in terms of the randomness hierarchy.

Theorem 3.6 (Nies, Stephan and Terwijn [78]). *Suppose that α is Kolmogorov random. Then α is 2-random.*

Theorem 3.7 (Miller [66], Nies, Stephan and Terwijn [78]). *A real α is 2-random iff α is Kolmogorov random.*

We remark that there seems no *prima facie* reason for 2-randomness to be the same as Kolmogorov randomness! The question of whether there was a natural condition in terms of plain complexity which characterized 1-randomness was finally solved by Miller and Yu, having been open for 40 years.

Definition 3.8. (Miller and Yu [69]) Define a computable function $G \colon \omega \to \omega$ by

$$G(n) = \begin{cases} K_{s+1}(t), & \text{if } n = 2^{\langle s,t \rangle} \text{ and } K_{s+1}(t) \neq K_s(t) \\ n, & \text{otherwise.} \end{cases}$$

Theorem 3.9 (Miller and Yu [69]). *For $x \in 2^\omega$, the following are equivalent:*

(i) x is 1-random.

(ii) (One direction of this is in Gács [32]) $(\forall n)\, C(x \restriction n) \geq n - K(n) \pm O(1)$.

(iii) $(\forall n)\, C(x \restriction n) \geq n - g(n) \pm O(1)$, for every computable $g \colon \omega \to \omega$ such that t $\sum_{n \in \omega} 2^{-g(n)}$ is finite.

(iv) $(\forall n)\, C(x \restriction n) \geq n - G(n) \pm O(1)$.

While it is not hard to show that almost all reals are random (as one would hope), Schnorr's Theorem allows us to easily show that there are explicit random reals. The halting probabilities of prefix-free Turing machines occupy the same place in algorithmic randomness as computably enumerable sets (the domains of partial computable functions) do in classical computability theory. They are called *left-computably enumerable reals* (left-c.e.) and are defined as the limits of increasing computable sequences of rationals. A special left-c.e. real is $\Omega = \sum_{U(\sigma)\downarrow} 2^{-|\sigma|}$ where U is a universal prefix free machine.

Theorem 3.10 (Chaitin [10, 12]). *Ω is Martin-Löf random.*

Chaitin's Ω has had a lot of popular attention. It allows us to prove Gödel's incompleteness theorem and the like using Kolmogorov complexity. Solovay [89] was the first to look at basic computability-theoretical aspects of Ω. For instance, consider $D_n = \{x : |x| \leq n \wedge U(x) \downarrow\}$. Solovay proved that $K(D_n) = n + O(1)$, where $K(D_n)$ is the K-complexity for an index for D_n. Solovay also proved the following basic relationships between D_n and $\Omega \restriction n$.

Theorem 3.11 (Solovay [89]).   *(i)* $K(D_n|\Omega \restriction n) = O(1)$[4].

(ii) $K(\Omega \restriction n|D_{n+K(n)}) = O(1)$.

The reader should note that in classical computability theory, we usually talk of *the* halting problem, whereas here the definition of Ω seems thoroughly machine dependent. To try to address this issue, Solovay [89] introduced the following definition, which is a kind of analytic version of *m*-reducibility.

Definition 3.12 (Solovay [89]). We say that a real α is *Solovay reducible* to β (or β *dominates* α), $\alpha \leq_S \beta$, iff there is a constant c and a partial computable function f, so that for all $q \in \mathbb{Q}$, with $q < \beta$,

$$c(\beta - q) > \alpha - f(q).$$

The intuition here is a sequence converging to β can generate one converging to α at the same rate, as clarified by Calude, Hertling, Khoussainov, Wang [9]. It is easy to see that $\leq_S$ implies $\leq_T$ for reals. Since there are only $O(2^{2d})$ many reals within a radius of 2^{-n+d} of a string representing a rational whose dyadic expansion has length n, it follows that $\leq_S$ has the *Solovay Property*

Lemma 3.13 (Solovay [89]). *If $\alpha \leq_S \beta$ then there is a c such that, for all n,*

$$K(\alpha \restriction n) \leq K(\beta \restriction n) + c.$$

The same also holds for C in place of K.

This lemma shows that, if $\Omega \leq_S \beta$, then β is Martin-Löf random. The next result says the being Ω-like means that a left-c.e. real look like Ω.

Theorem 3.14 (Calude, Hertling, Khoussainov, Wang [9]). *Suppose that β is a left-c.e. real and that $\Omega \leq_S \beta$. Then β is a halting probability. That is, there is a universal machine $\widehat{U}$ such that $\mu(\mathrm{dom}(\widehat{U})) = \beta$.*

The final piece of the puzzle was provided by the following lovely result of Kučera and Slaman.

Theorem 3.15 (Kučera and Slaman [46]). *Suppose that α is random and a left-c.e. real. Then for all left-c.e. reals β, $\beta \leq_S \alpha$, and hence α is a halting probability.*

We know that all reals have complexity oscillations. The Kučera-Slaman Theorem says that for left-c.e. random reals, they all happen in the same places. Downey, Hirschfeldt and Nies [26], and Downey, Hirschfeldt and LaForte [24] were motivated to look at the structure of computably enumerable reals under Solovay reducibility. The structure remains largely unexplored.

Theorem 3.16 (Downey, Hirschfeldt and Nies [26]).   *(i) The Solovay degrees of left-c.e. reals forms a distributive upper semilattice, where the operation of join is induced by +, arithmetic addition (or multiplication) (namely $[x] \vee [y] \equiv_S [x + y].$)*

---

[4]Indeed, $D_n \leq_{wtt} \Omega \restriction n$ via a weak truth table reduction with identity use, where a Turing reduction is a weak truth table one if there is a computable bound on the size of the queries used.

(ii) This structure is dense.[5] In fact if $\mathbf{a} < \mathbf{b} < [\Omega]$ then there exist incomparable $\mathbf{b_1}, \mathbf{b_2}$ with $\mathbf{a} < \mathbf{b_1} \vee \mathbf{b_2} = \mathbf{b}$.

(iii) However, if $[\Omega] = \mathbf{a} \vee \mathbf{b}$ then either $[\Omega] = \mathbf{a}$ or $[\Omega] = \mathbf{b}$.

Theorem 3.17 (Downey and Hirschfeldt [22]). *There exist left-c.e. sets A and B such that the Solovay degrees of A and B have no infimum in the (global) Solovay degrees.*

Theorem 3.18 (Downey, Hirschfeldt, and LaForte [24]). *The first order theory of the uppersemilattice of the Solovay degrees of left-c.e. reals is undecidable.*

We can view Ω as a fundamental operator on reals in the same way as we do for the jump operator. However, we need real care when dealing with relativizing Ω. We will take the notion of *universal machine* to mean that the machine U should be universal (and hence prefix-free) for all oracles, and if M_e is any machine, then M_e should be effectively coded in U, meaning that for some τ, $M_e(\sigma) = U(\tau\sigma)$. This definition avoids pathological machines.

The properties of omega operators acting on Cantor space and their relationship with, for instance, Turing reducibility was really initiated by Downey, Hirschfeldt, Miller and Nies [25]. It had been hoped, for instance, that these might be degree invariant operators on 2^ω. This hope failed about as badly as it could.

Theorem 3.19 (Downey, Hirschfeldt, Miller, Nies [25]). *For any omega operator Ω, there are reals $A =^* B$ (meaning that they differ only by a finite amount) such that Ω^A and Ω^B are relatively random (and hence $\Omega^A |_T \Omega^B$).*

One the other hand, omega operators do have some fascinating properties.

Theorem 3.20 (Downey, Hirschfeldt, Miller, Nies [25]). *Omega operators are lower semicontinuous but not continuous, and moreover, that they are continuous exactly at the 1-generic reals[6].*

In some sense Ω is kind of a red herring amongst random reals. It gives the impression that random reals have high computational power. Also results such as the famous Kučera-Gács Theorem below say that some random reals have high computational power.

Theorem 3.21 (Kučera [42], Gács [33]). *Every set is Turing (wtt-) reducible to a Martin-Löf random set.*

We remark that it is by no means clear this result should be true. After all, the very first result connecting measure and computability was the following:

---

[5]In fact, Downey and Hirschfeldt [22] have sown the Density Theorem holds for the left-c.e. reals for any measure of relative randomness which has a Σ_3^0 definition, has a top degree of $[\Omega]$, $+$ is a join, and where the computable sets are in the zero degree.

[6]Here recall that x is 1-generic means that it is Cohen generic for 1 quantifier arithmetic.

Theorem 3.22 (de Leeuw, Moore, Shannon, and Shapiro [14]). *Define the* enumeration probability *of A as*

$$P(A) = \mu(\{X \in 2^\omega : U^X = A\}),$$

where U is some universal machine. Then if $P(A) > 0$, A is a computably enumerable set.

An immediate corollary is the result first stated by Sacks [81] that $\mu(\{Y : A \leq_T Y\}) > 0$ iff A is computable.

The question is : "How do we reconcile the notions of high computational power and high randomness?". Frank Stephan gave a clarification to this dichotomy. We say that a function f is fixed point free iff for all partial computable functions φ_e, $f(e) \neq \varphi_e(e)$. We will say a set A has PA if it has the computational power to compute $\{0, 1\}$ valued fixed point free function[7] Whilst Kučera [44, 45] had shown that random reals can always compute fixed point free functions[8], Stephan showed that the randoms above the degree of the halting problem are the only ones with sufficient computational power to be able to compute a $\{0, 1\}$-valued one[9].

Theorem 3.23 (Stephan [91]). *Suppose that **a** is PA and 1-random. Then $\mathbf{0}' \leq_T$ **a**.*

All of this might leads the reader to guess that Ω, and hence all halting probabilities, have little to do with algorithmic randomness in general. Again this is not the case.

Theorem 3.24 (Downey, Hirschfeldt, Miller, Nies [25]). *Suppose that A is 2-random. Then there is a universal machine U and set B such that $A = \Omega_U^B$.*

That is, almost all randoms are halting probabilities. Notice that $\overline{\Omega}$ is random, but cannot be a halting probability relative to any oracle.

By analyzing the "majority vote" proof of Sacks Theorem, it is easy to show that if A is 2-random and $B \leq_T A$, then A is *not* random relative to B. Thus Theorem 3.24 stands in contrast the classical theorem from Kurtz' regrettably unpublished Thesis. (Proofs of this result and others from Kurtz's Thesis, and from Solovay's notes can be found in Downey and Hirschfeldt [22].)

Theorem 3.25 (Kurtz [50]). *Suppose that A is 2-random. Then there is a set $B \leq_T A$ such that A is computably enumerable relative to B.*

3.3. Martingales and the prediction paradigm. The last major approach to the concept of algorithmic randomness uses the intuition that random reals should be *hard to predict*. This can be formalized by imagining you had some

---

[7]They are called PA degrees since the coincide with the degrees bounding complete extensions of Peano Arithmetic. (Scott [85], Solovay)

[8]Additionally, Kučera proved that if A is n-random, then A bounds an n-FPF function. We refer the reader to [45] or [22] for definitions and details.

[9]Also, Kjos-Hanssen, Merkle, and Stephan [39] give a variant of in terms of Kolmogorov complexity and is in some sense an explanation why it is true.

"*effective*" betting strategy which worked on the bits of a real α. At each stage you get to try to predict the next bit of α, knowing the previous n bits. This idea leads to the following concept.

Definition 3.26 (Levy [55]). A *martingale* (*supermartingale*) is a function $f : 2^{<\omega} \mapsto \mathbb{R}^+ \cup \{0\}$ such that for all σ,

$$f(\sigma) = \frac{f(\sigma 0) + f(\sigma 1)}{2} \big(\text{resp.} f(\sigma) \geq \frac{f(\sigma 0) + f(\sigma 1)}{2} \big).$$

We say that the (super-)martingale *succeeds* on a real α, if $\limsup_n F(\alpha \upharpoonright n) \to \infty$.

Martingales were introduced by Levy [55], and Ville [102] proved that null sets correspond to success sets for martingales. They were used extensively by Doob in the study of stochastic processes. Schnorr [82, 83] effectivized the notion of a (super-)martingale.

Definition 3.27. We will define a (super-)martingale f as being *effective* or *computably enumerable* if $f(\sigma)$ is a c.e. real, and at every stage we have effective approximations to f in the sense that $f(\sigma) = \lim_s f_s(\sigma)$, with $f_s(\sigma)$ a computable increasing sequence of rationals.

We remark that the reader might have expected that an effective martingale would be one with f a computable function rather than one with computable *approximations*. This is an important point and we return to it later.

Theorem 3.28 (Schnorr [82]). *A real α is Martin-Löf random iff α does not succeed on any effective (super-)martingale.*

Thus, we have nice evidence that we have captured a reasonable notion of algorithmic randomness in that the three approaches, measure-theoretical, compressional, and predictability, all give the same class.

3.4. Schnorr's critique. In [82, 83], Schnorr argued that Theorem 3.28 demonstrated a clear failure of the intuition behind the definition of algorithmic randomness in that it we had *computable enumerable* betting strategies corresponding to Martin-Löf randomness rather than *computable* ones. Schnorr proposed the two variations below, and these have had attracted considerable interest recently. The first is to replace computably enumerable martingales by computable martingales and obtain the concept of *computably random* meaning that no computable martingale can succeed on the real. The second is to take the definition of Martin-Löf randomness (Definition 3.1) and replace $\mu(U_i) \leq 2^{-i}$ by $\mu(U_i) = 2^{-i}$ so that we know exactly the measure of the test sets, and hence can decide if $[\sigma] \in U_i$ by waiting until we know the measure of U_i to within $2^{-|\sigma|}$. Some clarification of the relationships between these two concepts was obtained by Schnorr.

Definition 3.29. We say that a computable martingale *strongly* succeeds on a real x iff there is a computable unbounded nondecreasing function $h : \mathbb{N} \mapsto \mathbb{N}$ such that $F(x \upharpoonright n) \geq h(n)$ infinitely often.

Theorem 3.30 (Schnorr [82]). *A real x is Schnorr random iff no computable martingale strongly succeeds on x.*

Thus Martin-Löf randomness implies computable randomness which implies Schnorr randomness. None of the implications can be reversed (van Lambalgen [99]). These concepts were somewhat ignored for maybe 20 years after Schnorr defined them, possibly because Martin-Löf randomness sufficed for many tasks, and because they were rather more difficult to handle. There are no universal tests, for instance, for Schnorr randomness. Recently, Downey and Griffiths [19] gave a nice characterization of Schnorr randomness in terms of *computable* machines. Here prefix-free M is called computable iff the measure of its domain is a computable real.

Theorem 3.31 (Downey and Griffiths [19]). *A real α is Schnorr random iff for all computable machines M, there is a constant c such that, for all n, $K_M(\alpha \restriction n) \geq n - c$.*

Related here is yet another notion of randomness called Kurtz or weak randomness. We define a *Kurtz test* (resp. Kurtz n-test) to be a a Σ_1^0 (resp. Σ_n^0-) class of measure 1. Then a real A is called *weakly $(n-)$random* or *Kurtz n-random*[10] if it passes all Kurtz $(n-)$tests, meaning that $A \in U$ for all such U. There is a null test version.

Definition 3.32 (Wang [103]). A *Kurtz null test* is a collection $\{V_n : n \in \mathbb{N}\}$ of c.e. open sets, such that

(i) $\mu(V_n) \leq 2^{-n}$, and

(ii) There is a computable function $f : \mathbb{N} \to (\Sigma^*)^{<\omega}$ such that $f(n)$ is a canonical index for a finite set of σ's, say, $\sigma_1, \ldots, \sigma_n$ and $V_n = \{[\sigma_1], \ldots, [\sigma_n]\}$.

Theorem 3.33 (Wang [103], after Kurtz [50]). *A real α is Kurtz random iff it passes all Kurtz null tests.*

Wang also gave a martingale version of Kurtz randomness.

Theorem 3.34 (Wang [103]). *A real α is Kurtz random iff there is no computable martingale F and nondecreasing computable function h, such that for* almost all n,

$$F(\alpha \restriction n) > h(n).$$

This should be directly compared with Schnorr's characterization of Schnorr randomness in terms of martingales and computable orders. Downey, Griffith and Reid [21] gave a machine characterization of Kurtz randomness, and showed that each computably enumerable non-zero degree contained a Kurtz random left-c.e. real. This contrasted with the theorem of Downey, Griffiths and LaForte [20]

---

[10]Now it could be argued that weak randomness is not really a randomness notion at all, but rather a genericity notion. However, for $n \geq 2$ it is certainly a randomness notion, and $n = 2$ corresponds to "Martin-Lóf tests with no effective rate of convergence."

who showed that if a left-c.e. real was Kurtz random, then its Turing degree must resemble the halting problem in that it must be high (i.e. $A' \equiv_T \emptyset'$). The definitive (and rather difficult) result here is the following which builds on all of this work.

Theorem 3.35 (Nies, Stephan and Terwijn [78]). *For every set A, the following are equivalent.*

(I) *A is high (i.e. $A' \geq_T \emptyset''$).*

(II) *There exists $B \equiv_T A$, such that B is computably random but not Martin-Löf random.*

(III) *There exists $C \equiv_T A$, such that C is Schnorr random but not computably random.*

Moreover, the examples can be chosen as left-c.e. reals if the degrees are computably enumerable.

Remarkably, outside of the high degrees the notions coincide.

Theorem 3.36 (Nies, Stephan and Terwijn [78]). *Suppose that a set A is Schnorr random and does not have high degree. Then A is Martin-Löf random.*

An even more unexpected collapse occurs for the special class of degrees called hyprimmune-free degrees. Following Miller and Martin [73], we say that A is *hyperimmune-free* iff for all functions $f \leq_T A$, there is a computable function g such that for all x, $f(x) \leq g(x)$.

Theorem 3.37 (Nies, Stephan, Terwijn [78]). *Suppose that A is of hyperimmune-free degree. Then A is Kurtz random iff A is Martin-Löf random.*

Space precludes me for discussing a very attractive possible refutation of Schnorr's critique proposed by Muchnik, Semenov, and Uspensky [72] who looked at *non-monotonic* betting strategies, where now we no longer pick the bits of the real in order. The open question is whether using computable nonmonotonic super-martingales, we might capture the notion of Martin-Löf randomness. We refer the reader to the paper of Merkle, Miller, Nies, Reimann and Stephan [65] and [72].

3.5. Hausdorff dimension. Whilst I don't really have enough space to do justice to the area, there has been a lot of very interesting work concerning effective Hausdorff dimension of even single reals and strings. For instance, we would expect that if $\Omega = w_0 w_1 \ldots$ then somehow $w_0 00 w_1 00 w_2 00 \ldots$ should be "$\frac{1}{3}$ random." A refinement of the class of measure zero sets is given by the theory of Hausdorff Dimension. In 1919 Hausdorff [36] generalized earlier work of Carathéodory to define a notion of an s-dimensional measure to include non-integer values. The basic idea is that you replace measure by a kind of generalized measure, where $\mu([\sigma])$ is replaced by $2^{-s|\sigma|}$ where $0 < s \leq 1$. With $s = 1$ we get normal Lebesgue measure. For $s < 1$ we get a refinement of measure zero. We can translate this cover version into a s-gale (a version of martingales, namely $f(\sigma) = 2^{-s}(f(\sigma 0) + f(\sigma 1))$.)

definition in the same way that it is possible to frame Lebesgue measure in terms of martingales.

Here we are viewing betting strategies in a *hostile environment* (a model of Jack Lutz), where "inflation" is acting so *not winning* means that we automatically lose money. (For normal martingales, we are to choose not to bet on some bit saving our funds for later bits and this has not effect. Here failing to bit means that our capital shrinks. The most hostile environment where we can win will be the effective Hausdorff dimension.) That is, roughly speaking, it can be shown that there is some limsup where the s-measure is not zero, and this is called the Hausdorff dimension of the set.

The study of effective dimension was pioneered through the work of Jack Lutz though as with much of the area of randomness there is a lot of history. In any case, for the effective version through the work of Lutz, Mayordomo, Hitchcock, Staiger and others we find that the notion corresponds to $\liminf_n \frac{K(A \restriction n)}{n}$, and can take that as a *working definition* of effective Hausdorff dimension. (Here I must refer the reader to Lutz [58, 59] for more details and history.)

With this definition, it can easily be shown that the "00" version of Ω above really has Hausdorff dimension $\frac{1}{3}$ and in fact is $\frac{1}{3}$ random as in Tadaki [94].

Terwijn [95, 96] and Reimann [80] have very nice results here relating Hausdorff dimension to degree structures. The latter as well and Lutz and Mayordomo have also looked at other dimensions, such as effective packing dimension, which can be characterized as $\limsup_n \frac{K(A \restriction n)}{n}$. Again it is possible to examine these concepts for stronger and weaker randomness notions such as Schnorr dimension. For instance, Downey, Merkle and Reimann [30] have shown that it is possible to have computably enumerable *sets* with nonzero Schnorr packing dimension, whereas their Schnorr Hausdorff dimension is 0. Much work remains to be done here with a plethora of open questions.

We finish this section by remarking that Lutz [58, 59] has even developed a notion of dimension for individual *strings*. The approach is to replace s-gales by "termgales" which are the analogues of s-gales for terminated strings. In essence he has characterized dimension for individual strings exactly in terms of prefix-free Kolmogorov complexity. Space does not allow for the development of this theory and we refer the reader to Lutz [58, 59] or Downey and Hirschfeldt [22] for further details.

4. Calibrating randomness

We have seen that we can classify randomness in terms of initial segment complexity. Thus it seems reasonable to think that we should also be able to classify *relative* randomness in terms of *relative* initial segment complexity. This motivates the following definition.

Definition 4.1 (Downey, Hirschfeldt, and LaForte [23]). We say a pre-ordering $\preceq$ is am Q-*initial segment measure of relative randomness* iff it obeys the Solovay property met earlier: $A \preceq B$ means that for all n, $Q(A \restriction n) \leq Q(B \restriction n) + O(1)$.

Here we are thinking of Q as C or K. We have already seen that Solovay reducibility is a measure of relative randomness and can be used to characterize the left-c.e. random reals. However, Solovay reducibility has a number of limitations such as being too fine and only really relating to left-c.e. reals.

There are a number of other interesting measures of relative randomness. They include segment ones $\leq_C$ and $\leq_K$ which are defined in the obvious way. Others include the following introduced by Downey, Hirschfeldt and LaForte [23]:

(i) $A \leq_{sw} B$ iff there is a c and a wtt procedure Γ with use $\gamma(n) = n + c$, and $\Gamma^B = A$. If $c = 0$, then this is called ibT-reducibility and is the one used by Soare and Csima in differential geometry, such as Soare [87].

(ii) $A \leq_{rK} B$ means that there there is a c such that for all n,

$$K((A \restriction n)|(B \restriction n + c)) = O(1).$$

The reducibility (i) is also called effective Lipschitz reducibility and This reducibility has been analyzed by Yu and Ding [105], Barmpalias and Lewis (e.g. [4]), and Raichev and Stephan (e.g. [79]). While I don't really have space to discuss these reducibilities in detail, I would like to point out that they do give nice insight into relative computability. We briefly consider sw. The idea of this reducibility is that if $A \leq_{sw} B$, then there is an *efficient* way to convert the *bits* of B into those of A. The Kučera-Slaman Theorem says that all versions of Ω are the same in terms of their S-degrees. But we may ask whether there is a "bit" version of this result? Yu and Ding [105] established the following.

Theorem 4.2 (Yu and Ding [105]). *(i) There is no sw-complete c.e. real.*

(ii) There are two c.e. reals β_0 and β_1 so that there is no c.e. real α with $\beta_0 \leq_{sw} \alpha$ and $\beta_1 \leq_{sw} \alpha$.

There are other assorted results and reducibilities. However, things are still in their infancy here. We will simply refer the reader to Downey [17], or Downey and Hirschfeldt [22] for the current situation.

We return to looking at the basic measures $\leq_C$ and $\leq_K$. The reader should note that these are not really reducibilities but simply transitive pre-orderings. (Though following tradition we will continue to refer to them as reducibilities.)

Theorem 4.3 (Yu, Ding, Downey [107]). *For $Q \in \{K, C\}$, $\{X : X \leq_Q Y\}$ has size $2^{\aleph_0}$ and has members of each degree, whenever Y is random.*

The replacement for this theorem is a measure-theoretical one:

Theorem 4.4 (Yu, Ding, Downey [107]). *For any real A, $\mu(\{B : B \leq_K A\}) = 0$. Hence there are uncountably many K degrees.*

We had hoped that there might be nice hierarchies related to levels of randomness. We will denote by $\Omega^{(m+1)}$ to be Ω relative to $\emptyset^{(m)}$. We might have hoped that $\Omega^{(2)}$ was K-above Ω, but that hope turns out to be folourn.

Theorem 4.5 (Yu, Ding, Downey [107]). *For all c and $n < m$,*

$$(\exists^\infty k)\big[\, K(\Omega^{(n)} \restriction k) < K(\Omega^{(m)} \restriction k) - c\,\big].$$

For $n = 0, m = 1$ Theorem 4.5 was proven by Solovay [89], using totally different methods.

Miller and Yu have made really significant progress in our understanding here by introducing yet more measures of relative randomness. They are based around van Lambalgen's Theorem which states that for all A, B, *B n-random and A is B-n-random iff $A \oplus B$ is n-random.*

Definition 4.6 (Miller and Yu [69]). We say that $\alpha \leq_{vL} \beta$, α is *van Lambalgen*[11] reducible to β if for all $x \in 2^\omega$, $\alpha \oplus x$ is random implies $\beta \oplus x$ is random.

Miller and Yu's basic result were as follows.

Theorem 4.7 (Miller and Yu [69]). *For all random α, β,*

  (i) *α n-random and $\alpha \leq_{vL} \beta$ implies β is n-random.*

  (ii) *If $\alpha \oplus \beta$ is random then α and β have no upper bound in the vL-degrees.*

  (iii) *If $\alpha \leq_T \beta$ and α is 1-random, then $\beta \leq_{vL} \alpha$.*

  (iv) *There are random $\alpha \equiv_{vL} \beta$ of different Turing degrees.*

  (v) *There are no maximal or minimal random vL-degrees, and no join.*

  (vi) *If $\alpha \oplus \beta$ is random then $\alpha \oplus \beta <_{vL} \alpha, \beta$.*

  (vii) *The Σ_1^0 theory of the vL-degrees is decidable.*

Miller and Yu show that $\Omega^{(n)}$ and $\Omega^{(m)}$ have no upper bound in the vL degrees for $n \neq m$. This improves the Yu, Ding, Downey (Theorem 4.5) result above. All of this is filters through an interesting relationship between $\leq_{vL}$ and $\leq_C, \leq_K$.

Lemma 4.8 (Miller and Yu [69]). *For random α, β,*

  (i) *Suppose that $\alpha \leq_K \beta$. Then $\alpha \leq_{vL} \beta$.*

  (ii) *Suppose that $\alpha \leq_C \beta$. Then $\alpha \leq_{vL} \beta$.*

We state the following for $\leq_K$ but they hold equally for $\leq_C$, as has been shown by Miller and Yu.

Corollary 4.9 (Miller and Yu [69]).   (i) *Suppose that $\alpha \leq_K \beta$, and α is n-random and β is random. Then β is n-random.*

  (ii) *If $\alpha \oplus \beta$ is 1-random, then $\alpha|_K \beta$ and have no upper bound in the K-degrees.*

---

[11]This is closely related to a relation introduced by Nies: He defined $A \leq_{LR} B$ if for all Z, Z is 1-B-random implies Z is 1-A-random. If A and B are both random then $A \leq_{LR} B$ iff $B \leq_{LR} A$.

(iii) For all $n \neq m$, the K-degrees of $\Omega^{(n)}$ and $\Omega^{(m)}$ have no upper bound.

Miller and Yu have many other very interesting results on the K degrees of c.e. reals. For instance, they show that if $\alpha \oplus \beta$ is 1-random, then $\alpha|_K \alpha \oplus \beta$. Miller has proven the following.

Theorem 4.10 (Miller [67]).   *(i) If α, β are random, and $\alpha \equiv_K \beta$, then $\alpha' \equiv_{tt} \beta'$. As a consequence, every K-degree of a random real is countable.*

(ii) If $\alpha \leq_K \beta$, and α is 3-random, then $\beta \leq_T \alpha \oplus \emptyset'$.

Notice that (ii) implies that the cone of K-degrees above a 3-random is countable. On the other hand, Miller and Yu have constructed a 1-random whose K-upper cone is uncountable. The construction of an uncountable random K-degree uses their method of constructing K-comparable reals. Its proof uses the following clever lemma. The current proof of Theorem 4.11 is quite difficult.

Theorem 4.11 (Miller and Yu [70]). *Suppose that $\sum_n 2^{-f(n)} < \infty$, then there is a 1-random Y with*

$$K(Y \restriction n) < n + f(n),$$

for almost all n.

To finish this section, we mention further evidence that randomness is a "lowness" notion. Miller has shown that if α is 3-random then its often useless as an oracle. We will call α *weakly-low for K* if $(\exists^\infty n)[K(n) \leq K^\alpha(n) + O(1)]$. Thus in a weakly-low real, the information in α is so useless that it cannot help to compress n. The following result echoes the theme articulated by Stephan that most random reals have little *usable* information in them.

Theorem 4.12 (Miller [67]).   *(i) If α is 3-random it is weakly-low.*

(ii) If α is weakly-low, and random, then α is strongly Chaitin random in that

$$(\exists^\infty n)\big[K(\alpha \restriction n) \geq n + K(n) - O(1)\big].$$

5. Lowness and triviality

There have been some truly dramatic results in what has now become known as lowness and triviality. If Q is a measure of relative randomness then we can say that A is *Q-trivial* iff $A \leq_Q 1^\omega$. Thus using Q we cannot distinguish A from a computable set. We will say that A is *Q-low* if $Q^A(\sigma) = Q(\sigma) + O(1)$, for all σ. Thus, for instance A is K-low would mean that $K^A(\sigma) = K(\sigma) + O(1)$ for all σ.

We say that a set A is low for a randomness notion V iff the randoms relative to A remain the same. (One would usually expect that fewer sets would be random.) An apparently weaker notion is that of being low for V tests. That is, every if $\{U_i : i \in \mathbb{N}\}$ is a V^A test, then there is a V-test $\{\hat{U}_i : i \in \mathbb{N}\}$ such that $\cap_i U_i \subseteq \cap_i \hat{U}_i$. We remark that since there are universal Martin-Löf tests the test set notion and the lowness notion are the same.

5.1. The remarkable Martin-Löf case. There have been a series of amazing results in the case of 1-randomness. Historically, these results began with triviality. An old result of Loveland [57] shows that $Q(\alpha \upharpoonright n|n) = O(1)$ for all n, $(Q \in \{C, K\})$ iff α is computable. This result was generalized by Chaitin [11], who proved the following.

Theorem 5.1 (Chaitin [11]). *α is computable iff $\alpha \leq_C 1^\omega$. (That is, iff α is C-trivial.)*

I think this squares with our intuition that should α be indistinguishable from a computable string in terms of its initial segment complexity it should itself be computable. Chaitin also noted that essentially the same proof shows that if α is K-trivial, the α is Δ_2^0 and hence computable from the halting problem. The breakthrough was again by Solovay.

Theorem 5.2 (Solovay [89]). *There are noncomputable α which are K-trivial.*

Solovay's argument was complex and mysterious. It turned out that the example α could even be chosen as a computably enumerable *set* (Calude and Coles [7], Downey, Hirschfeldt, Nies and Stephan [27], Kummer (unpubl), An A. Muchnik (unpubl.)). The paper [27] gave a very simple construction of a computably enumerable K-trivial set along the lines of the Dekker deficiency set. What is remarkable is that such K-trivial sets solve Post's problem.

Theorem 5.3 (Downey, Hirschfeldt, Nies and Stephan [27]). *Suppose that α is K-trivial. Then $\alpha <_T \emptyset'$.*

The method of proof of Theorem 5.3 uses what has become known as the "decanter method"(terminology of Nies) and is unfortunately very complicated, though it does *not* use the priority method. No easy proof of Theorem 5.3 is known.

It was noted that the short [27] proof constructing a K-trivial set strongly resembled and earlier construction of a computably enumerable set A which was low for Martin-Löf randomness by Kučera and Terwijn [47]. It was conjectured that perhaps these classes might have something to do with each other. In a ground breaking series of papers, Nies (and Hirschfeldt) proved some completely unexpected facts.

Theorem 5.4 (Nies (and Hirschfeldt for some), [75, 76]). *(a) The following classes of reals coincide.*

> *(i) K-low.*
>
> *(ii) K-trivial.*
>
> *(iii) low for Martin-Löf randomness.*

(b) All the members A of this class $\mathcal{C}$ are superlow *in that $A' \equiv_{wtt} \emptyset'$.*

(c) The class $\mathcal{C}$ forms a natural Σ_3^0 ideal in the Turing degrees. There is a low$_2$ computably enumerable degree $\mathbf{a}$ such that if $\mathbf{c} \in \mathcal{C}$, the $\mathbf{c} < \mathbf{a}$.

    (d) If A is a K-trivial real, then there is a computably enumerable set $\hat{A}$ with $A \leq_T \hat{A}$.

The K-trivials form the only known natural nontrivial Σ_3^0 ideal in the (computably enumerable) Turing degrees. Item (c) in the above is a special case of a general unpublished Theorem of Nies that every Σ_3^0 ideal in the computably enumerable degrees is bounded by a low$_2$ computably enumerable degree. (A proof can be found in Downey and Hirschfeldt [22].) It is possible that there is a low (non-computably enumerable) degree **a** which bounds $\mathcal{C}$, and even possible that such a degree could be random. This problem seems hard.

Subsequently, other quite deep results have been proven. For instance, we have seen that if A is noncomputable then $\mu(\{X : A \leq_T X\}) = 0$, but since there are K-low reals, there must be reals A and randoms X such that X is A-random and $A \leq_T X$. In that case, we say that A is a *base of Martin-Löf randomness.*

Theorem 5.5 (Hirschfeldt, Nies, Stephan [37]). *A is K-trivial iff it is a base of Martin-Löf randomness.*

We remark that Slaman has used the class of K-trivials to solve a longstanding problem in computable model theory. As a final result in this area we mention some interesting results of Csima and Montalbán. These results are related to the enumeration of the K-trivials.

Theorem 5.6 (Chaitin [11], Zambella [108]). *There are only $O(2^d)$ members of $KT(d)$. They are all Δ_2^0.*

The reader might wonder with the nice computable bound how many K-trivial reals there are. Let $G(d) = |\{X : X \in KT(d)\}|$. Then there is a crude estimate that $G(d) \leq_T \emptyset'''$. This is the best upper bound known. In unpublished work, Downey, Miller and Yu have shown that $G(d) \not\leq_T \emptyset'$, using the fact that $\sum_d \frac{G(d)}{2^d}$ is convergent. This is all related to the Csima-Montalbán functions. We say that f is a *Csima-Montalbán function* if f is nondecreasing and

$$K(A \restriction n) \leq K(n) + f(n) + O(1)$$

implies that $A \restriction n$ is K-trivial. Such functions can be constructed from $\emptyset'' \oplus G$. We define f to be *weakly* Csima-Montalbán, if we weaken the hypothesis to be that $\liminf_n f(n) \to \infty$. Little is known here. It is not known if the arithmetical complexity of f depends upon the universal machine chosen. We remark that the original use of Csima-Montalbán functions was to construct a minimal pair of K-degrees: K-degrees **a**, **b** such that $\mathbf{a} \wedge \mathbf{b} = \mathbf{0}$.

In other more recent work, Downey, Nies, Weber and Yu [29] have also looked at lowness for weak 2-randomness. Here it has been shown that such degrees do exist, and are all K-trivial. It is not known if the converse holds.

5.2. Other lowness and triviality.
One thing which this work has brought (back) to the fore is the use of domination properties in classical computability. This was first recognized in the study of lowness for Schnorr randomness. Terwijn

and Zambella [97] defined a degree $\mathbf{a}$ to be computably traceable iff there is a single computable function f such that for all functions $g \leq_T \mathbf{a}$, there is a computable collection of canonical finite sets $\{D_{p(x)} : x \in \mathbb{N}\}$, such that

(i) $|D_{p(x)}| < f(x)$, and

(ii) $g(x) \in D_{p(x)}$ for almost all x.

Being computably traceable is a strong form of being hyperimmune-free. Terwijn and Zambella showed that there are $2^{\aleph_0}$ many degrees that are hyperimmune-free yet not computably traceable. There are also $2^{\aleph_0}$ degrees that are computably traceable. The following theorem completely classifies the low for Schnorr random reals. Its proof is far from easy.

Theorem 5.7 (Terwijn and Zambella [97]). *A is low for Schnorr random null sets iff A is computably traceable.*

It is clear that if A is low for tests then A is low for Schnorr randoms. But the converse is not at all clear and had been an open question of Ambos-Spies and Kučera [3]. The question was finally solved by Kjos-Hanssen, Stephan, and Nies [40], using Bedregal and Nies [5]. Summarizing the results proven there, we have:

Theorem 5.8 (Kjos-Hanssen, Stephan, and Nies [40]). *$\mathbf{a}$ is low for Schnorr null sets iff $\mathbf{a}$ is low for Schnorr randomness.*

I remark in passing that I am not aware of any lowness notion that differs for null sets and for the randomness notion. In other work, Nies has examined lowness for polynomial time randomness, and lowness for computable randomness. For computable randomness, the answer is rather surprising.

Theorem 5.9 (Nies [76]). *Suppose that A is low for computable randomness. Then A is computable.*

Finally there has been a little work on triviality notions here. Recall that Downey and Griffiths [19] proved that A is Schnorr trivial iff for all *computable* machines M, $K_M(A \upharpoonright n) \geq n - O(1)$. This definition naturally allows us to define a reducibility notion.

Definition 5.10 (Downey and Griffiths [19]). We say that α is Schnorr reducible to β, $\alpha \leq_{Sch} \beta$, iff for all computable machines M, there is a computable machine $\widehat{M}$ such that $K_M(\beta \upharpoonright n) - O(1) > K_{\widehat{M}}(\alpha \upharpoonright n)$, for all n.

This definition allows us to say that a real α is *Schnorr trivial* iff $\alpha \leq_{Sch} 1^{\omega}$. Schnorr trivial reals behave quite differently than do Schnorr low reals and the K-trivials. Downey and Griffiths constructed a Schnorr trivial real and Downey, Griffiths and LaForte [20] showed that they can even be Turing complete, though they do not occur in every computably enumerable Turing degree. Subsequently, they have been investigated by Johanna Franklin [31] Her results are summarized below.

Theorem 5.11 (Franklin [31]). *(i) There is a perfect set of Schnorr trivials (and thus some are not Δ_2^0.)*

(ii) Every degree above $\mathbf{0}'$ contains a Schnorr trivial.

(iii) Every Schnorr low is Schnorr trivial.

(ii) The Schnorr lows are not closed under join.

Finally, we mention that other lowness notions both in randomness and in other contexts have been analyzed. Yu [104] (also Miller and Greenberg (unpubl)) proved that there are no sets low for 1-genericity. Sets low for Kurtz randomness were first constructed by Downey, Griffiths and Reid. They were shown there to be all hyperimmune-free and were implied by Schnorr lowness. Stephan and Yu [92] have shown that lowness for Kurtz randomness differs from lowness for Schnorr randomness and lowness for weak genericity. To wit, they have shown the following.

Theorem 5.12 (Stephan and Yu [92]). *(i) Low for weakly generic is the same hyperimmune-free plus not of diagonally noncomputable degree.*

(ii) There is a set of hyperimmune-free degree which is neither computably traceable traceable nor diagonally noncomputable.

(iii) Low for weakly generic implies low for Kurtz random.

(iv) In particular, low for weakly generic and hence low for Kurtz randomness is not the same as Schnorr low.

The topic of lowness for such concepts remains in its infancy, and promises fascinating results.

References

[1] Allender, E., H. Buhrman, M. Koucký, D. van Melkebeek, and D. Ronneburger, *Power from Random Strings,* in *FOCS 2002,* IEEE (2002), 669-678.

[2] Allender, E., H. Buhrman, and M. Koucký, *What Can be Efficiently Reduced to the Kolmogorov-Random Strings?,* Annals of Pure and Applied Logic, 2006 to appear.

[3] Ambos-Spies K., and A. Kučera, *Randomness in computability theory*, in *Computability Theory and its Applications*, (Cholak, Lempp, Lerman, Shore, eds) Contemporary Mathematics Vol. 257 (2000), 1-14.

[4] Barmpalias, G., and A. Lewis, *Randomness and the Lipschitz degrees of computability*, submitted.

[5] Bedregal, B., 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.

[6] Calude, C., *Information Theory and Randomness, an Algorithmic Perspective,* Springer-Verlag, Berlin, 1994. Second revised edition 2002.

[7] Calude, C., and Coles, R. *Program size complexity of initial segments and domination relation reducibility,* in *Jewels are Forever,* (J. Karhümaki, H. Mauer, G. Paŭn, G. Rozenberg, eds.) Springer-Veralg, New York, 1999, 225-237.

[8] Calude, C., Coles, R., Hertling, P., Khoussainov, B., *Degree-theoretic aspects of computably enumerable reals,* in *Models and Computability,* (ed. Cooper and Truss) Cambridge University Press, 1999.

[9] Calude, C., Hertling, P., Khoussainov, B., Wang, Y., *Recursively enumerable reals and Chaitin's Ω number,* in STACS '98, Springer Lecture Notes in Computer Science, Vol 1373, 1998, 596-606.

[10] Chaitin, G., *A theory of program size formally identical to information theory,* Journal of the Association for Computing Machinery 22 (1975), pp. 329-340.

[11] Chaitin, G. *Information-theoretical characterizations of recursive infinite strings,* Theoretical Computer Science, vol. 2 (1976), 45-48.

[12] Chaitin, G. *Incompleteness theorems for random reals,* Adv. in Appl. Math Vol. 8 (1987), 119-146.

[13] Chaitin, G., *Information, Randomness & Incompleteness,* 2nd edition, Series in Computer Science 8, World Scientific, River Edge, NJ, 1990.

[14] de Leeuw, K., Moore, E. F., Shannon, C. E., and Shapiro, N. *Computability by probabilistic machines,* Automata studies, pp. 183–212. Annals of mathematics studies, no. 34. Princeton University Press, Princeton, N. J., 1956.

[15] Downey, R., *Some recent progress in algorithmic randomness,* in *Proceedings of the 29 th Annual Conference on Mathematical Foundations of Computer Scence, Prague, August 2004* (invited paper) (J. Fiala, V. Koubek and J. Kratochvil eds), Springer-Verlag, Lecture Notes in Computer Science, Vol. 3153 (2004), 42-81.

[16] Downey, R., *Some Computability-Theoretical Aspects of Reals and Randomness,* in *The Notre Dame Lectures,* (Peter Cholak, ed.) Vol. 18 in the *Lecture Notes in Logic* series published by the Association for Symbolic Logic. (2005) 97-146.

[17] Downey, R., *Five lectures on algorithmic randomness,* to appear in *Proceedings of "Computational Prospects of Inifinity,"* World Scientific, (edited by Chong et. al.)

[18] Downey, R., Ding Decheng, Tung Shi Ping, Qiu Yu Hui, Mariko Yasuugi, and Guohua Wu (eds), *Proceedings of the 7th and 8th Asian Logic Conferences,* World Scientific, 2003, viii+471 pages.

[19] Downey, R. and E. Griffiths, *On Schnorr randomness,* Journal of Symbolic Logic, Vol 69 (2) (2004), 533-554.

[20] Downey, R., E. Griffiths and G. LaForte, *On Schnorr and computable randomness, martingales, and machines,* Mathematical Logic Quarterly, Vol. 50, No 6 (2004), 613-627.

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

[22] Downey, R., and D. Hirschfeldt, *Algorithmic Randomness and Complexity,* Springer-Verlag Monographs in Computer Science, to appear (preliminary version www.mcs.vuw.ac.nz/∼downey).

[23] R. Downey, D. Hirschfeldt, and G. LaForte, *Randomness and reducibility*, extended abstract appeared in *Mathematical Foundations of Computer Science, 2001* J. Sgall, A. Pultr, and P. Kolman (eds.), Mathematical Foundations of Computer Science 2001, Lecture Notes in Computer Science 2136 (Springer, 2001), 316–327). final version in *Journal of Computing and System Sciences.* Vol. 68 (2004), 96-114.

[24] Downey, R., D. Hirschfeldt, and G. LaForte, *Undecidability of Solovay degrees of c.e. reals*, in preparation.

[25] Downey, R., D. Hirschfeldt, J. Miller, and A. Nies, *Relativizing Chaitin's halting probability*, to appear Journal of Mathematical Logic.

[26] Downey, R., D. Hirschfeldt, and A. Nies, *Randomness, computability and density* SIAM Journal on Computing, 31 (2002) 1169–1183 (extended abstract in proceedings of STACS 2001 January, 2001. Lecture Notes in Computer Science, Springer-Verlag, (Ed A. Ferriera and H. Reichel, 2001, 195-201)).

[27] Downey, R., D. Hirschfeldt, A. Nies, and F. Stephan, *Trivial reals*, extended abstract in *Computability and Complexity in Analysis* Malaga, (Electronic Notes in Theoretical Computer Science, and proceedings, edited by Brattka, Schröder, Weihrauch, FernUniversität, 294-6/2002, 37-55),July, 2002. Final version appears in [18] 2003, 103-131.

[28] Downey, R., D. Hirschfeldt, A. Nies, and S. Terwijn, *Calibrating randomness,* to appear, Bulletin Symbolic Logic.

[29] Downey, R., A. Nies, R. Weber, and Yu Liang, *Lowness and Π_2^0-Nullsets*, in preparation.

[30] Downey, R., J. Reimann, and W. Merkle, *Schnorr dimension*, to appear, Proceedings *Computability in Europe.*

[31] Franklin, J., Ph. D. Dissertation, University of California at Berkeley, in preparation.

[32] Gács, P., *Exact Expressions for some Randomness Tests* Z. Math. Log. Grdl. M., Vol. 26 (1980), 385-394. (Short version: Springer Lecture Notes in Computer Science 67 (1979) 124-131)

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

[34] Gács, P., *Uniform Test of Algorithmic Randomness Over a General Space,* online manuscript.

[35] Gaifmann, H., and M. Snir, *Probabilities over rich languages*, J. Symb. Logic, Vol. 47, (1982), 495-548.

[36] Hausdorff, F., *Dimension und äußeres Maß*, Mathematische Annalen 79 (1919) 157–179.

[37] Hirschfeldt, D, A. Nies, and F. Stephan, *Using random sets as oracles*, in preparation.

[38] Kautz, S., *Degrees of Random Sets,* Ph.D. Diss. Cornell, 1991.

[39] Kjos-Hanssen, B., W. Merkle, and F. Stephan, *Kolmogorov complexity and the Recursion Theorem*, to appear.

[40] Kjos-Hanssen, B., F. Stephan, and A. Nies. *On a question of Ambos-Spies and Kučera*, to appear.

[41] Kolmogorov, A.N., *Three Approaches to the Quantitative Definition of Information*, in *Problems of Information Transmission (Problemy Peredachi Informatsii)*, 1965, Vol. 1, 1-7.

[42] Kučera, A., *Measure, Π_1^0 classes, and complete extensions of PA,* in *Springer Lecture Notes in Mathematics,* Vol. 1141, 245-259, Springer-Verlag, 1985.

[43] Kučera, A., *An alternative priority-free solution to Post's Problem, Proceedings, Mathematical Foundations of Computer Science,* (Ed. J. Gruska, B. Rovan, and J. Wiederman), Lecture Notes in Computer Science, Vol. 233, Springer-Verlag, (1986).

[44] Kučera, A., *On the use of diagonally nonrecursive functions,* in *Logic Colloquium, '87,* North-Holland, Amsterdam, 1989, 219-239.

[45] Kučera, A., *Randomness and generalizations of fixed point free functions,* in *Recursion Theory Week, Proceedings Oberwolfach 1989,* (K. Ambos-Spies, G. H. Müller and G. E. Sacks, eds.) Springer-Verlag, LNMS 1432 (1990), 245-254.

[46] Kučera, A. and T. Slaman, *Randomness and recursive enumerability,* SIAM Journal of Computing, Vol. 31 (2001), 199-211.

[47] Kučera, A., and S. Terwijn, *Lowness for the class of random sets,* Journal of Symbolic Logic, vol. 64 (1999), 1396-1402.

[48] Kummer, M., *Kolmogorov complexity and instance complexity of recursively enumerable sets,* SIAM Journal of Computing, Vol. 25 (1996), 1123-1143.

[49] Kummer, M., *On the complexity of random strings,* (extended abstract) in *STACS, '96,* Springer-Verlag Lecture Notes in Computer Science, Vol 1046 (11996), 25-36.

[50] Kurtz, S., *Randomness and Genericity in the Degrees of Unsolvability,* Ph. D. Thesis, University of Illinois at Urbana, 1981.

[51] Levin, L., *Some Theorems on the Algorithmic Approach to Probability Theory and Information Theory,* Dissertation in Mathematics, Moscow, 1971.

[52] Levin. L., *On the notion of a random sequence,* Soviet Math. Dokl. 14 (1973) 1413–1416.

[53] Levin, L., *Laws of information conservation (non-growth) and aspects of the foundation of probability theory,* Problems Informat. Transmission, Vol. 10 (1974), ' 206-210.

[54] Levin, L., *Measures of complexity of finite objects (axiomatic description),* Soviet Mathematics Dolkady, vol. 17 (1976), 552-526.

[55] Levy, P., *Theorie de l'Addition des Variables Aleantoires,* Gauthier-Villars, 1937.

[56] Li, Ming and Vitanyi, P., *Kolmogorov Complexity and its Applications,* Springer-Verlag, 1993.

[57] Loveland, D. *A variant of the Kolmogorov concept of complexity,* Information and Control, vol. 15 (1969), 510-526.

[58] Lutz, J., *The dimensions of individual strings and sequences,* Information and Computation, Vol 187 (2003), pp. 49-79. (Preliminary version: *Gales and the constructive dimension of individual sequences,* in: U. Montanari, J. D. P. Rolim, E. Welzl (eds.), Proc. 27th International Colloquium on Automata, Languages, and Programming, 902–913, Springer, 2000.)

[59] Lutz, J., *Effective fractal dimensions,* Mathematical Logic Quarterly Vol. 51 (2005), pp. 62-72.

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

[61] Martin-Löf, P., *Complexity oscillations in infinite binary sequences,* Z. Wahrscheinlichkeittheorie verw. Gebiete, Vol. 19 (1971), 225-230.

24

[62] Merkle W., *The complexity of stochastic sequences,* Preliminary version in CCC2003, final version to appear.

[63] Merkle W., *The Kolmogorov-Loveland stochastic sequences are not closed under selecting subsequences,* J. Symbolic Logic, Vol. 68 (2003), 1362-1376.

[64] Merkle W., and N. Mihailovic, *On the construction of effective random sets*, in Proceedings MFCS 2002, (ed. Diks and Rytter) Springer-Verlag LNCS 2420.

[65] Merkle, W., J. Miller, A. Nies, J. Reimann, and F. Stephan, *Kolmogorov-Loveland randomness and stochasticity*, to appear, Annals of Pure and Applied Logic.

[66] J. S. Miller, *Kolmogorov random reals are 2-random*, J. Symbolic Logic, to appear.

[67] Miller, J., *The K-degrees, low for K degrees, and weakly low for K oracles,* in preparation.

[68] Miller, J. *Contrasting plain and prefix-free Kolmogorov complexity,* in preparation.

[69] Miller, J., and L. Yu, *On initial segment complexity and degrees of randomness*, to appear, Trans. Amer. Math. Soc.

[70] Miller, J., and L. Yu, *Oscillation in the initial segment complexity of random reals,* in preparation.

[71] Muchnik, An. A., and S. P. Positelsky, *Kolmogorov entropy in the context of computability theory*, Theor. Comput. Sci., Vol. 271 (2002), 15-35.

[72] Muchnik, An. A., A. Semenov, and V. Uspensky, *Mathematical metaphysics of randomness,* Theor. Comput. Sci., Vol 207(2), (1998), 263-317.

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

[74] Ng Keng Meng, F. Stephan, and G. Wu, *The Degrees of Weakly Computable Reals,*

[75] Nies, A., *Reals which compute little*, to appear, *Proceedings of CL 2002.*

[76] Nies, A., *Lowness properties and randomness*, Advances in Mathematics 197, 1 (2005), 274-305..

[77] Nies, A., *Computability and Randomness,* monograph in preparation.

[78] Nies, A., F. Stephan and S. A. Terwijn, *Randomness, relativization, and Turing degrees*, to appear, Journal of Symbolic Logic.

[79] Raichev, A., Ph.D. thesis, University of Wisconsin-Madison, in progress.

[80] Reimann, J., *Computability and Dimension,* PhD Thesis, University of Heidelberg, 2004

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

[82] Schnorr, C. P., *A unified approach to the definition of a random sequence,* Mathematical Systems Theory, 5 (1971), 246-258.

[83] Schnorr, C. P., *Zufälligkeit und Wahrscheinlichkeit*, Springer-Verlag Lecture Notes in Mathematics, Vol 218, 1971, Springer-Verlag, New York.

[84] Schnorr, C. P., *Process complexity and effective random tests*, Journal of Computer and System Sciences, vol. 7 (1973), 376-388.

[85] Scott, D., *Algebras of sets binumerable in complete extensions of arithmetic,* in Proc. Symp. Pure and Appl. Math., Vol. 5 (1962), 357-366.

[86] Soare, R., *Recursively enumerable sets and degrees* (Springer, Berlin, 1987).

[87] R. Soare, *Computability Theory and Differential Geometry*, Bulletin Symbolic Logic, to appear.

[88] Solomonoff, R., *A formal theory of inductive inference, part 1 and part2,* Information and Control, 7 (1964), 224-254.

[89] Solovay, R., *Draft of paper (or series of papers) on Chaitin's work*, unpublished notes, May, 1975, 215 pages.

[90] Staiger, L., *Kolmogorov complexity and Hausdorff dimension,* Information and Computation, Vol. 103 (1993), 159-194.

[91] Stephan, F., *Martin-Löf random sets and PA-complete sets,* to appear.

[92] Stephan, F, and Yu Liang, *Lowness for weakly 1-generic and Kurtz random*, in preparation.

[93] Stillwell, J., *Decidability of "almost all" theory of degrees,* J. Symb. Logic, Vol. 37 (1972), 501-506.

[94] Tadaki, K., *A generalization of Chaitin's halting probability Ω and halting self-similar sets,* Hokkaido Math. J., Vol. 32 (2002), 219-253.

[95] Terwijn, S. *Computability and Measure*, Ph. D. Thesis, University of Amsterdam, 1998.

[96] S. A. Terwijn, *Complexity and Randomness,* Notes for a course given at the University of Auckland, March 2003. Published as research report CDMTCS-212, University of Auckland.

[97] S. A. Terwijn and D. Zambella, *Computational randomness and lowness*, Journal of Symbolic Logic 66(3) (2001) 1199–1205.

[98] Uspensky, V., A. Semenov and A.Kh. Shen, *Can an Individual Sequence of Zeros and Ones be Random?*, Russian Math. Surveys, Vol. 45 (1990), 121-189.

[99] van Lambalgen, M., *Random Sequences,* Ph. D,. Diss. University of Amsterdam, 1987.

[100] van Lambalgen, M., *The axiomatization of randomness,* Journal of Symbolic Logic, 55 (1990), 1143-1167.

[101] von Mises, R., *Grundlagen der Wahrscheinlichkeitsrechnung*, Math. Z., vol. 5 (1919), 52-99.

[102] Ville, J., *Ětude critique de la concept du collectif*, Gauthier-Villars, 1939.

[103] Wang, Y., *Randomness and Complexity*, PhD Diss, University of Heidelberg, 1996.

[104] Yu, Liang, *Lowness for genericity,* Archive for Mathematical Logic, to appear.

[105] Yu Liang and Ding Decheng, *There is no sw-complete c.e. real*, J. Symbolic Logic Vol. 69 (2004), no. 4, 1163-1170.

[106] Yu Liang and Ding Decheng, *There are $2^{\aleph_0}$ many H-degrees in the random reals.* Proc. Amer. Math. Soc. 132 (2004), no. 8, 2461–2464

[107] Yu Liang, Ding Decheng, and R. Downey, *The Kolmogorov complexity of the random reals*, *Annals of Pure and Applied Logic* Volume 129, Issues 1-3 , (2004), 163-180

[108] Zambella, D., *On sequences with simple initial segments*, ILLC technical report, ML-1990-05, University of Amsterdam, 1990.

[109] Zvonkin A. K., and L.A. Levin, *The complexity of finite objects and the development of concepts of information and randomness by the theory of algorithms*, Russian Math. Surveys, 25(6):83-124 (1970).

Rod Downey
School of Mathematical and Computing Sciences
Victoria University
PO Box 600, Wellington
New Zealand.
www.mcs.vuw.ac.nz/∼downey
E-mail: rod.downey@vuw.ac.nz