Algorithmic Randomness and Complexity

Rod Downey

Victoria University

Wellington

New Zealand

Joint work with

- Evan Griffiths
  Denis Hirschfeldt
  Andre Nies
  Frank Stephan
  Stephanie Reid
  Geoff LaForte
  Yu Liang
  Wu Guohua
  Jan Reimann

  and others..

The Basic Refs are van Lambalgen's Thesis, Solovay's unpublished notes, and Li-Vitanyi. Also a new book "to appear" by Downey and Hirschfeldt prelim version on my home page.

And *Calibrating Randomness* (with Hirschfeldt, Nies and Terwijn) for BSL, soon on my web page.

The new material can be found in:

- Randomness and reducibility, (with G. Laforte and D. Hirschfeldt) extended abstract in *Mathematical Foundations of Computer Science, 2001.* to appear in *Journal of Comput. and Sys. Sci.*
- Density, randomness and

computability, with D. Hirschfeldt and A. Nies, SIAM J. Comput. (Extended abstract appeared in *Symposium for Theoretical Aspects of Computer Science, STACS'01* January, 2001.)

- Some Computability-Theoretical Aspects of Reals and Randomness, to appear, in a *Lecture Notes in Logic* volume edited by Cholak. et. al.
- On Schnorr Randomness, (with Evan Griffiths) to appear JSL
- On computable randomness (with Griffiths and Laforte)
- papers by Miller, Yu Liang, Stephan, Reimann, Terwijn, Merkle.

- Some of the papers can be found in

  `www.mcs.vuw.ac.nz/`
  `research/math-pubs.shtml`

  Nies home page, Hirschfeldt's home page.

Motivation

- What is “random”?
- How can we calibrate levels randomness? Among randoms?, Among non-randoms?
- How does this relate to classical computability notions, which calibrate levels of computational complexity?
- Von Mises, Church, Solomonoff, Levin, Chaitin, Kolmogorov, Shannon, etc.

Notation

- Real is a member of Cantor space 2^ω with topology with basic clopen sets $[\sigma] = \{\sigma\alpha : \alpha \in 2^\omega\}$ whose measure is $2^{-|\sigma|}$.

- for uniformity, a real is always nonrational.

- Strings = members of $2^{<\omega} = \{0, 1\}^*$.

Computability Theory

- "Computable" functions $f : \mathbb{N} \mapsto \mathbb{N}$ means that we have an algorithm for computing $f(n)$ from n.
- Things like strings, rationals etc are coded as integers, so no loss of generality using $\mathbb{N}$.
- A set B is called *computably enumerable* c.e. if it is the range of a computable function.
  $B = \{f(0), f(1), \ldots\}$.

- Equivalently B is the *domain* of a computable *partial* function meaning that it is a function whose domain is a *subset* of $\mathbb{N}$. (Put n into the range of f once it is in the domain of $\varphi_s = \{x \leq s : \varphi(x) \downarrow [s]$ (that is, halts at stage s.)$\}$)
- Think of these sets as those for which we have an algorithm that "in theory" would list all the members, but not *in order*. We don't seem to be able to know if the set is *computable* in th sense that we can also list the complement.
- The most famous c.e. set : The halting problem $Halt = \{\langle x, y\rangle :$ the x-program halts on input $y\}$.

- This set is c.e. but non-computable by a simple diagonal argument. (Gödel, Turing, Post, etc.)

Three views of effective randomness

1 Measure-Theoretical:

- Random means no distinguishing features. (Think of a statistical test as generating a set of tests: e.g. the law of large numbers $\limsup n \frac{a_1+\cdots+a_n}{n} \to \frac{1}{2}$. Then consider $U = \{x : x \text{ fails the law }\}$. The U is a null open set.)
- In effective terms:
  - Avoids all effective sets of measure 0.

2. Algorithmic:

- Random means hard to describe, incompressible: e.g. 1010101010.... (10000 times) would have a short program.

- In effective terms:

  - Initial segments cannot be output by short programs.

3. Other views: e.g. random means unpredictable.

- martingales=betting strategies (Doob etc)
– $F : 2^{<\omega} \mapsto \mathbb{R}^+ \cup \{0\}$, with $F(\sigma) = \frac{F(\sigma 1)+F(\sigma 0)}{2}$.
– F succeeds on α iff $\limsup_n F(\alpha \restriction n) \to \infty$.

- Think of a real where every 3rd bit was 1. You could win betting on the bits.

- In effective terms, no effective martingale succeeds on α.

Martin-Löf randomness:

- A *c.e. open set* is one of the form $\bigcup_i (q_i, r_i)$ where $\{q_i : i \in \omega\}$ and $\{r_i : i \in \omega\}$ are c.e..
- A *Martin-Löf test* is a uniformly c.e. sequence $U_1, U_2, \ldots$ of c.e. open sets s.t.
$$\forall i (\mu(U_i) \leq 2^{-i}).$$
(Computably shrinking to measure 0)
- α is *Martin-Löf random* if for every Martin-Löf test,
$$\alpha \notin \bigcap_{i>0} U_i.$$

Solovay Randomness

- We call a real α *Solovay random* iff for all c.e. sets of open intervals $\{I_n : n \in \omega\}$, with $\sum_n |I_n| < \infty$, $\alpha \in I_n$ for at most finitely many n.
- (Solovay) α is Martin-Löf random iff α is Solovay random.
- The proof is not difficult: A Martin-Löf test is a Solovay test, naturally. For the other direction, given a Solovay test as above and wlog the sum is ≤ 1, let $U_k = \{\beta : \beta \in I_n \text{ for at least } 2^k n\}$. Then $\mu(U_k) \leq 2^{-k}$ and hence if α is Martin=Löf random we are done.

Kolmogorov Complexity

- Capture the incompressibility paradigm.
- A string σ is random iff the only way to describe it is by hardwiring it.
- For a fixed machine N, we can define
- The *Kolmogorov complexity* $C(\sigma)$ of $\sigma \in \{0,1\}^*$ with respect to N, is $|\tau|$ for the shortest τ s.t. $N(\tau)\downarrow = \sigma$. (Kolmogorov, Solomonov)

- A real is N-random iff $C_N(\sigma) \geq |\sigma|$.
- A machine U is called universal iff for all N, there is a d such that for all σ, $C_U(\sigma) \leq C_N(\sigma) + d$.
- They exist (Kolmogorov). Hence there is a notion of Kolmogorov randomness for strings up to a constant.

A first attempt for *reals*

- The above works for *strings*.
- For *reals* problems occur because a string τ gives "$|\tau| + \tau$" much information.
- First try α, a real, is random iff for all n, $C(\alpha \restriction n) \geq n - d$.
- (Martin-Löf) NO such real exist!

- Why? Take any α. Then, as a string $\alpha \upharpoonright n$ corresponds to some number which we can interpret as a string using llex ordering: $\alpha \upharpoonright n$ is the m-th string.

- Now consider the program that does the following. It takes a strings ν, interprets its length $m_\nu = |\nu$ as a string, $\sigma = \sigma_m$ and outputs $\sigma\nu$.

- Apply this to the string τ whose length is m th code of $\alpha \upharpoonright n$.

- The output would be much longer, and would be $\alpha \upharpoonright m + n$, with input having length m. Thus $C(\alpha \upharpoonright m + n) < m + n - O(1)$.

Prefix free

universal computers

- Computers have alphabet $\{0,1\}$.
- A computer M is *prefix-free* if

$$(M(\sigma)\downarrow \ \wedge \ \sigma' \supsetneq \sigma) \Rightarrow M(\sigma')\uparrow .$$

- A prefix-free M is *universal* if for every prefix-free N there is a c s.t.

$$N(\sigma)\downarrow \rightarrow \exists\tau(|\tau| \leq |\sigma| + c \ \wedge$$

$$M(\tau)\downarrow = N(\sigma)).$$

- Fix a universal prefix-free machine M.

Kolmogorov-Levin-Chaitin

randomness:

- Prefix freeness gets rid of the use of length as extra information:
- The *prefix-free complexity* $K(\sigma)$ of $\sigma \in \{0,1\}^*$ is $|\tau|$ for the shortest τ s.t. $M(\tau)\downarrow = \sigma$.
- Note now $K(\sigma) \leq |\sigma| + K(|\sigma|) + d$, about $n + 2\log n$, for $\sigma| = n$.
- α is *random* if there is a c s.t.

$$\forall n (K(\alpha \upharpoonright n) > n - c).$$

This happens if there is a c such that for infinitely many n,
$C(\alpha \upharpoonright n) > n - c$.

Schnorr's Theorem

Theorem[Schnorr]
Chaitin random $\Longleftrightarrow$ Martin-Löf random.

Computably enumerable reals:

- α is *c.e.* if there is a computable sequence of rationals

  $$q_0 < q_1 < \ldots \longrightarrow \alpha.$$

  Equivalently, the lower cut of α is a c.e. set of rationals.

- α is *computable* if there is a computable f s.t.

  $$\forall n(\alpha - q_{f(n)} < 2^{-n}).$$

- Being a c.e. real is *not* the same as being the characteristic function of a c.e. set. (Soare)

- Chaitin's Omega
- The most famous c.e. real is

$$\Omega = \mu \operatorname{dom}(M) = \sum_{M(\sigma)\downarrow} 2^{-|\sigma|},$$

the "halting probability."

- c.e. reals are the relevant effetive sets for randomness (as they are the measures of domains of prefix free machines) in the same way that c.e sets are the central objects in classical computabiltity theory.

Schnorr randomness

- One could argue that to be algorithmically random, Martin-Löf's definition is too strong.
- For instance, α is ML-random iff no c.e. Martingale succeeds on α. (That is the betting startegy $F : 2^{<\omega} \mapsto \mathbb{R}^+ \cup \{0\}$ is a c.e. function.)
- Schnorr argued that ML randomness is intrinsically c.e. not defeating "effectively"=*computably* given objects.

More effective randomness

- Schnorr proposed two notions of more computable randomness.
- Computable randomness where we used martingales with F a computable function. (more later) and Schnorr randomness below.
- A *Schnorr test* is a Martin-Löf test $U_i : i \in \omega$ such that $\mu(U_i) = 2^{-i}$.
- α is Schnorr random iff $\alpha \notin \cap_i U_i$ for all Schnorr tests $\{U_i\}$.
- We give a machine characterization of Schnorr randomness, solving an old question of Ambos-Spies and others.

- A real is called *computable* if it has a computable dyadic expansion.

- A *computable prefix free machine* is a prefix free machine M such that,

$$\sum_{M(\sigma)\downarrow} 2^{-|\sigma|}$$

is a computable real.

- **Theorem**(Downey and Griffiths) α is Schnorr random iff for all computable prefix free machines M, there is a c such that for all n,

$$H_M(\alpha \upharpoonright n) \geq n - c.$$

- Schnorr used martingales and a kind of forcing argument to prove that there are Schnorr random reals that are not Martin-Löf random.

- (Downey-Griffiths) All Schnorr random c.e. reals are of "high" c.e. degree.

- (Downey-Griffiths) There are c.e. reals that are Schnorr random that have incomplete T-degree. Contrast with the fact that all Martin-Löf random reals are wtt complete (but not tt-complete by work of Kummer and Slaman-Kucera.).

- (Downey-Griffiths-LaForte, Nies-Stephan-Terwijn) All high c.e. degrees contain Schnorr random c.e. reals.
- NST have a stronger result for copmputably random c.e. reals and high degrees.

- Other results
- For ML-randomness can calibrate via $A \leq_K B$ iff for all n, $K(A \upharpoonright n) \leq K(B \upharpoonright n) + \mathcal{O}(1)$.
- $A \leq SchB$ iff for all computable machines M, with $B \in \mathrm{ra}(M)$ there is a computable N such that

$$H_N(A \upharpoonright n) \leq H_M(B \upharpoonright n) + \mathcal{O}(1).$$

- There are "Schnorr trivial reals"
- Structure is largely unknown.

- α is Schnorr random iff no computable martingale "strongly" succeeds on α.(Namely there is a nondecreasing computable $f : \omega \mapsto \omega$ such that $F(\alpha \restriction n) \geq f(n)$ infinitely often.
- ML implies computable imples Schnorr.
- Recently Downey, Griffiths and LaForte (and independently Merkle, Mihailovic and Slaman) have a test characterization of computable randomness in terms of computably graded tests.
- lots of questions

Kurtz Randomness

- Stuart Kurtz suggested that a real should be random if it obeyed all positive laws: that is α is Kurtz random iff for all c.e. open sets U, if $\mu(U) = 1$ then $\alpha \in U$.
- We have seen that all ML-random sets are complete, all Schnorr ones have high degree, surprisingly:
- (Downey, Griffiths and Reid) Each c.e. degree contains a c.e. Kurtz random real.

Measures of Relative Randomness

- A reducibility $\leq$ on reals is a *measure of relative randomness* if it satisfies the *Solovay property*:

$$\text{If } \beta \leq \alpha \text{ then}$$
$$\exists c\ (\forall n\ (K(\beta \upharpoonright n) \leq K(\alpha \upharpoonright n) + c)).$$

- Can also use C, and others.

Solovay Reducibility

- We talk about *the* halting problem, whereas of course we really mean HALT_U for a universal U. But... they are all the same (Myhill)
- Solovay introduced a reduction to address this for randomness.
- ($\alpha \leq_S \beta$) α is Solovay or domination reducible to β iff there is a constant d, and a partial computable φ, such that for all rationals $q < \beta$

$$\varphi(q) \downarrow \wedge\ d(\beta - q) > |\alpha - \varphi(q)|.$$

- Intuitively, however well I can approximate β, I can approximate α just as well.
- S-reducibility is a measure of relative randomness (Solovay)

Kucera-Slaman Theorem

- A c.e. real is Ω-*like* if it dominates all c.e. reals.
- (Solovay) Any Ω-like real is random.
- **Theorem** (Calude, Hertling, Khoussainov, and Wang) If a c.e. real is Ω-like then it is an Ω-number.
- **Theorem** [Kucera-Slaman] If a c.e. real is random then it is Ω-like.
- ie all random c.e. reals are the "same" and are halting probabilities. (even though it might be possible for it to be as high as $n + 2\log n$ all oscillations occur at the "same" n's.)

Structure

- The c.e. reals using $\leq_S$ forms a upper semilarttice, called the Solovay degrees.
- (Downey, Hirschfeldt, Nies) (i) $+$ induces a join
  (ii) It is distributive
  (iii) dense
  (iv) $[\Omega]$ is the only join inaccessible element.

- (Downey, Hirschfeldt, Laforte) The structure of the S-degrees of c.e. reals has an undecidable theory.
- S-reducibility is a measure of relative randomness, but not the only one, and it has some problems.
- However, structure of $\leq_K$ and $\leq_C$, except on c.e. reals, is largely unknown. On the randoms, we lack techniques.

Results on $\leq_K$

- Question: are there two *random* A, B with $A <_K B$?
- Yu, Ding, Downey $\mu(\{A \leq_K A\}) = 0$. Hence uncountably many K degrees.
- Yu, Ding In fact $2^{\aleph_0}$.
- (Miller and Yu) for almost all pairs $A|_K B$.
- (Miller) Each K-degree of a random countable. Unknown if there is an uncountable K-degree.

How do K and T reducibilities interact?

- It is known that if $\alpha \leq_C \mathbb{N}$ then α is computable.
- is this true of $\leq_K$? Intuitively, yes, but.....

Solovay's Theorem:

- There exist noncomputable reals α such that for all n

$$K(\alpha \upharpoonright n) \leq K(1^n) + c.$$

- Note that Chaitin proved that if $K(\alpha) \leq K(1^n) + c$, then α is Δ^0_2. It was earlier by Loveland proved that

  $C(\alpha \upharpoonright n) \leq C(1^n) + c$ *for all* n, *implies* α *is computable.*
  In fact:

  (Stephan) Suppose that we have c.e. α, β with $\alpha \leq_C \beta$. Then $\alpha \leq_T \beta$.

- Solovay's 1974 proof is very complicated. Here is a simplified version proving a stronger result.

- There is a c.e. noncomputable set A such that for all n

$$K(A \upharpoonright n) \leq K(n) + \mathcal{O}(1).$$

- Let

$$A_{s+1} = A_s \cup \{x : W_{e,s} \cap A_s = \emptyset \wedge x \in W_{e,s}$$

$$\wedge \sum_{x \leq j \leq s} 2^{-K(1^j)[s]} < 2^{-(e+1)}\}.$$

- Amazingly, it turns out that A is K-trivial. (diagram)
- Note that this is injury free. (Post's problem)
- K-trivial reals are never of high degree, so this is an injury free solution to Post's problem.

Other Facts

- (Zambella) For each c there are only $\mathcal{O}(2^c)$ many reals with

  $$K(A \upharpoonright n) \leq K(n) + c,$$

  for all n.
- The K-trivial reals are closed under wtt-reducibility and under $+$.
- There are low c.e. degrees containing no K-trivials.

Some other related work:

- One can relativize the definition of C or K-complexity.
- (Kucera-Terwijn) There exist c.e. noncomputable sets, A such that $RAND^A = RAND$. Call these ML-low.
- (Terwijn-Zambella+Nies-Bedregal) This is not true for Schnorr randomness for tests, but there are sets below $\mathbf{o}''$ where for Schnorr Randomness, $RAND^A = RAND$. These sets can be characterized by certain properties similar to being hyperimmune free.

- Downey, Griffiths and Reid showed that Schnorr low=Kurtz low for tests.
- Nies proved that Computable lowness= computable!

Nies Theorems

Nies has some new material here:

- Every K-trivial is bounded by a K-trivial c.e. set.
- Every K-low is low$_2$ and "tracable". hence there are only countably many.
- trivial implies low for K.
- K-trivials are closed under T-reducibility.

n-randomness

- Replace ML tests by ML tests relative to $\emptyset^{(n)}$ and you get $n+1$ randomness.
- (Nies,Stephan, Terwijn; Miller) 2-random = Kolmogorov random where α is Kolmogorov random iff $\exists^\infty n(C(\alpha \upharpoonright n) \geq n - d$.
- Call α strong Chaitin random iff $\exists^\infty n(K(\alpha \upharpoonright n) \geq n + K(n) - d)$. Question ?2-random=SC random?
- Ω^A is very interesting. Question: is it degree invariant... Martin's conjecture.

Cereals are red herrings

- In some sense, the c.e. reals and Ω make us think of randomness as "like" the halting problem, and more random=more information. This seems false.
- Stephan has shown that if $\boldsymbol{a}$ is a Turing degree conatining a 1-random real which has enough information to compute a $\{0,1\}$ valued diagonal function then $\boldsymbol{a} \geq \mathbf{o}'$.
- Miller proved the remarkable following result. Say α is "pseudo-low" if $(\exists^\infty n)[K(n) \leq K^\alpha(n) + O(1)]$.

- The intuition is that α is so computationally useless that it gives no help in computing such n.
- (Miller) α is random and pseudo-low iff α is 3-random.

Some ignored material

- supermartingale reducibility
- Lutz, Schnorr and Hausdorff dimension of reals and strings.
- $\leq_{vL}$ and Miller-Yu.
- Stochasiticity and Merkle-Slaman-Ambos-Spies etc.
- complexity of c.e. sets and Kummer.
- Kucera coding

- Thank you.