Algorithmic Randomness and computability

Rod Downey

Victoria University

Wellington

New Zealand

Joint work with

- Evan Griffiths
  Denis Hirschfeldt
  Andre Nies
  Frank Stephan
  Stephanie Reid
  Geoff LaForte

The Basic Refs are van Lambalgen's Thesis, Solovay's unpublished notes, and Li-Vitanyi. 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.*
- Density, randomness and computability, with D. Hirschfeldt and A. Nies, to appear 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)
- On computable randomness (with Griffiths and Laforte)
- Presentations of computably enumerable reals, (with G. Laforte) accepted for *Theoretical Computer Science.*
- Martingales and reducibility (with Hirschfeldt and Griffiths)
- Some of the papers can be found in

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

Motivation

- What is "random"?
- How can we calibrate levels randomness?
- How does this relate to classical computability notions, which calibrate levels of complexity?
- Von Mises, Church, Solomonoff, Chaitin, Kolmogorov, Shannon, etc.

Notation

- "real" is taken without comment as "real in $(0, 1]$."
- for uniformity, a real is always nonrational.

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:
- In effective terms:
  - Initial segments cannot be output by short programs.

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

  - martingales
  - $F : 2^{<\omega} \mapsto \mathbb{R}^+ \cup \{0\}$, with $F(\sigma) = \frac{F(\sigma 1)+F(\sigma 0)}{2}$.
  - F succeeds on α iff $\limsup_n F(\alpha \upharpoonright n) \to \infty$.
- Think of a real where every 6th 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.
$$\forall i(\mu(U_i) \leq 2^{-i}).$$
- 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.

Self-delimiting universal computers

- Computers have alphabet $\{0,1\}$.
- A computer M is *self-delimiting* if
$$(M(\sigma)\downarrow \ \wedge \ \sigma' \supsetneq \sigma) \Rightarrow M(\sigma')\uparrow .$$
- A self-delimiting M is *universal* if for every self-delimiting N there is a c s.t.
$$N(\sigma)\downarrow \to \exists\tau(|\tau| \leq |\sigma| + c \ \wedge$$
$$M(\tau)\downarrow = N(\sigma)).$$
- Fix a universal machine N, and a self-delimiting universal computer M.

Kolmogorov-Chaitin randomness:

- The *Kolmogorov complexity* $K(\sigma)$ of $\sigma \in \{0,1\}^*$ is $|\tau|$ for the shortest τ s.t. $N(\tau)\downarrow = \sigma$.

- The *prefix-free complexity* $H(\sigma)$ of $\sigma \in \{0,1\}^*$ is $|\tau|$ for the shortest τ s.t. $M(\tau)\downarrow = \sigma$.

- α is *random* if there is a c s.t.

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

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

Schnorr's Theorem

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

- The proof uses Kraft's inequality in the following guise. (Chaitin-Kraft) *Suppose that we have a c.e. list of pairs of the form* n_i, σ_i *with* $\sigma_i \in \{0,1\}^*$, *and* $n_i \in \omega$. *Suppose also that* $\sum_i 2^{-n_i} \leq 1$. *Then there is a prefix free machine* M *and a list of strings* τ_i *with* $|\tau_i| = n_i$ *such that* $M(\tau_i) = \sigma_i$ *for all* i. (diagram)

- $\Longrightarrow$ Suppose that α is not Martin-Löf random and $\alpha \in \cap_i U_i$, with $\mu(U_i) \leq 2^{-i}$. We use Chaitin-Kraft. Let $n \geq 3$. For all strings σ of length n^2 with extensions in U_{n^2}, enumerate the pair n, σ into B. Note that $\sum_B 2^{-n} \leq \sum_{n\geq 3} 2^{-n}(\mu(U_{n^2}) \leq \sum_{n\geq 3} 2^{n-n^2} \leq 1$. Thus by Kraft-Chaitin there is a machine M and strings $\tau_n \in \operatorname{dom} M$ with $M(\tau_n) = \sigma_n$ and $|\tau_n| = n, |\sigma_n| = n^2$. Since $\alpha \in \cap_n U_{n^2}$, this means that α is not Chaitin random.

- $\Longleftarrow$ Suppose that α is Martin-Löf random. Consider

$$U_k = \{\beta : \exists n(H(\beta \upharpoonright n) \leq n - 2^k\}.$$

Then $\mu(U_k) \leq 2^{-k}$ and hence, as $\alpha \notin \cap_K U_k$, we are done.

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.

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

- α is *strongly c.e.* if $\alpha = 0.\chi_A$ for a c.e. A.

- Soare was the first to observe that there are c.e. reals that are not strongly c.e..

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

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

  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 centreal 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** α is Schnorr random iff for all computable prefix free machines M, there is a c such that for all n,

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

- A *total Solovay test* is a computable collection of c.e. open sets V_i: $i \in \omega$, such that the sum $\Sigma_{i=0}^{\infty}\mu(V_i)$ is finite and a computable real. A real α passes a total Solovay test if $\alpha \in V_i$ for at most finitely many V_i.

- (Downey and Griffiths) y is Schnorr random iff y passes all total Solovay tests

- Suppose z is Schnorr random. For any f given by a computable machine, suppose for the sake of contradiction that $(n - K_f(z \upharpoonright n))$ is unbounded as a function of n. Let $M = \Sigma_{x \in dom(f)} 2^{-|x|}$.

- Define

$U_k = \{x : \exists n K_f(x \upharpoonright n) \leq n - k\}.$

- Then $\mu(U_k) \leq M2^{-k}$. and $\mu(U_k)$ is a computable function of k
- Hence $(n - K_f(z \upharpoonright n))$ must be bounded for any such f: $(\exists d) n - K_f(z \upharpoonright n) \leq d$, so $K_f(x \upharpoonright n) \geq n - d$.
- The other direction we suppose z is not Schnorr random. Let U_k be a Schnorr test such that $z \in \cap_k U_k$, $U_{k+1} \subset U_k$, and $\mu(U_k) = 2^{-k}$. and use Kraft Chaitin.

- 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.).

- Other results
- For ML-randomness can calibrate via $A \leq_H B$ iff for all n, $H(A \upharpoonright n) \leq H(B \upharpoonright n) + \mathcal{O}(1)$.
- $A \leq SchB$ 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.
- Schnorr implies computable imples ML.
- recently Downey, Griffiths and LaForte have a test characterization of computable randomness in terms of computably graded tests.
- lots of questions

Kurtz Randomness

- Stuart Kurtz suggested that a read 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*:

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

- S-reducibility is a measure of relative randomness, but not the only one, and it has some problems.

How do H and T reducibilities interact?

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

Solovay's Theorem:

- There exist noncomputable reals α such that for all n

$$H(\alpha \restriction n) \leq H(1^n) + c.$$

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

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

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

A proof of Solovay's Theorem

- 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

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

- Let

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

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

- Amazingly, it turns out that A is H-trivial. (diagram)
- Note that this is injury free. (Post's problem)
- H-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

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

for all n.

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

Some other related work:

- One can relativize the definition of H or K-complexity.
- (Kucera-Terwijn) There exist c.e. noncomputable sets, A such that $RAND^A = RAND$.
- (Terwijn-Zambella) This is not true for Schnorr randomness, 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.

  A set X is Schnorr low iff there is a computable function p, such that, for all functions $g \leq_X$, there is a function h where, for all n,

(i) $|H_{h(n)}| < p(n)$,

(ii) $g(n) \in D_{h(n)}$.

Nies Theorems

Nies has some new material here:

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

Martingales again

- A supermartingale is like a martingale except that $f(\sigma) \geq \frac{f(\sigma 0)+f(\sigma 1)}{2}$
- There is a multiplicatively optinal universal sm:

$$f(\sigma) = \sum_e 2^{-e} f_e(\sigma).$$

- (DGH) There in no universal multiplicatively optimal martingale.
- Recently with Hirschfeldt and Griffiths we have looked at "supermartingale reducibility;" that is $A \leq_{su} B$ iff for some constant c,

for all n, $cf(B \upharpoonright n) \geq f(A \upharpoonright n)$. ($f$ universal)

- (e.g.) $\leq_{rH}$ implies $\leq_{su}$.
- The zero degree is the computables, the top is the randoms.
- dense + is a join etc.

- Thank you.