Algorithmic Randomness, Computability, and Reals

Rod Downey

Victoria University

Wellington

New Zealand

The Basic Refs are van Lambalgen's Thesis, Solovay's unpublished notes, and Li-Vitanyi.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 accepted for *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)

- Presentations of computably enumerable reals, (with G. Laforte) accepted for *Theoretical Computer Science.*

- 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.

Two views of effective randomness

1 Topological:

- Random means no distinguishing features.
- 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.

- c.e. martingales

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 iff 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.*

- $\Longrightarrow$ 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 $\tau_n \in \text{ dom}M$ 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

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

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

Schnorr randomness

- One could argue that to be algorithmically random, Martin-Löf's definition is too strong.
- A *Schnorr test* is a Martin-Löf test $U_i : i \in \omega$ such that $\mu(U_i) = 2^{-i}$.
- It is also possible to give a machine characterization of Schnorr randomness.

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

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

- 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, assuming the proof is correct!) 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.).

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 Ω-numbers

- $$\Omega_M = \sum_{M(\sigma)\downarrow} 2^{-|\sigma|}$$
- Ω_M is the halting probability of M.
- Ω_M is c.e. and random.
- Such numbers are called Ω-*numbers*.
- One talks about *the* Chaitin number Ω, but it is apparently Machine dependent.

Domination, Solovay reducibility:

- $\beta \leq_S \alpha$ if there are a partial computable $\varphi : \mathbb{Q} \to \mathbb{Q}$ and a c s.t.

  $\forall q < \alpha(\varphi(q){\downarrow} < \beta \ \wedge \ \beta - \varphi(q) \leq c(\alpha - q))$.

- The idea is that however I approximate β I can also approximate α.

- Solovay's Lemma: *Let c be given. Then there is a constant d depending on c alone, such that, for $Q = H$ or K, for all n, if $|\sigma| = |\tau| = n$ and $|\sigma - \tau| \leq 2^{c-n}$, then*

$$Q(\sigma) = Q(\tau) + d.$$

- Solovay Reducibility provides a measure of relative randomness for c.e. reals:

$$\alpha \leq_S \beta \text{ implies}$$

$$\exists c \forall n (Q(\alpha \upharpoonright n) \leq Q(\beta \upharpoonright n) + c.$$

- The proof is to apply Solovay's Lemma on $\alpha \upharpoonright n$ and $\varphi(\beta \upharpoonright n) \upharpoonright n$.

Ω-like reals:

- A c.e. real is Ω-*like* if it dominates all c.e. reals.
- By the Solovay's theorem, 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.

Solovay degrees

- $\leq_S$ is reflexive and transitive. So $\equiv_S$ is an equivalence relation on the c.e. reals.
- The *Solovay degree* $[\alpha]$ of α is its $\equiv_S$-equivalence class.
- The S-degrees of c.e. reals form a distributive uppersemilattice with:
  - (i) least degree that of the computable reals,
  - (ii) greatest degree $[\Omega]$,
  - (iii) $[\alpha] \vee [\beta] = [\alpha + \beta] = [\alpha\beta]$.

- **Theorem (Downey, Hirschfeldt, and LaForte).** *The theory of the S-degrees is undecidable.*
- The proof uses Nies method of coding effectively dense boolean algebras into the appropriately complex ideals in the degree structure.
- The degree of the theory is surely what it should be but we have no proof yet.

Density and Splitting

- **Theorem** (Downey, Hirschfeldt, Nies) Let $\gamma <_S \alpha <_S \Omega$. There are β^0 and β^1 s.t. $\gamma <_S \beta^0, \beta^1 <_S \alpha$ and $\beta^0 + \beta^1 = \alpha$.

-

- **Theorem** (Downey, Hirschfeldt, Nies) Let $\gamma <_S \Omega$. There is a β s.t. $\gamma <_S \beta <_S \Omega$.

- **Corollary** The S-degrees of c.e. reals are dense.

- **Theorem** (Downey, Hirschfeldt, Nies) Suppose that $\Omega \leq_S \alpha + \beta$. Then one of α or β is Ω-like.

- (Note that, of course there are nonrandom reals α and β with $\alpha + \beta = \Omega$. But they are not c.e.)

- The proof of the result that every incomplete degree splits is very interesting and uses a finite injury argument where the injuries themselves are controlled by Ω.
  A summary:

- A c.e. real γ is random iff it cannot be written as $\alpha + \beta$ for $\alpha, \beta <_S \gamma$.

- Let $\boldsymbol{d}$ be a Solovay degree. The following are equivalent:

  (i) $\boldsymbol{d}$ is incomplete.

  (ii) $\boldsymbol{d}$ splits.

  (iii) $\boldsymbol{d}$ splits over any lesser S-degree.

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.

  (i) Restricted to c.e. reals.

  (ii) Too fine.

  (iii) Too uniform.

(joint work with Hirschfeldt and LaForte)

- Another measure of relative randomness is *sw-reducibility*:

  $\beta \leq_{sw} \alpha$ if there is a functional Γ s.t. $\Gamma^{\alpha} = \beta$ and the use of Γ is bounded by $x + c$ for some c.

- sw-reducibility is incomparable with S-reducibility.

- sw-reducibility has some nice properties, but the sw-degrees of c.e. reals are (e.g.) not an uppersemilattice.

- Would like a measure of relative randomness combining the best of S-reducibility and sw-reducibility.

Relative H reducibility:

- $\beta \leq_{rH} \alpha$ if there exist a partial computable binary function f and a constant k s.t. for each n there is a $j \leq k$ for which $f(\alpha \restriction n, j)\!\downarrow= \beta \restriction n$.
- The prefix-free complexity $H(\sigma \mid \tau)$ of σ relative to τ is $|\mu|$ for the shortest μ s.t. $M^{\tau}(\mu)\!\downarrow= \sigma$.
- $\beta \leq_{rH} \alpha$ iff $\exists c \ (\forall n \ (H(\beta \restriction n \mid \alpha \restriction n) \leq c))$.
- Both S- and sw-reducibility imply rH-reducibility.
- rH-reducibility implies Turing reducibility.

Structure

- The rH-degrees of c.e. reals are an uppersemilattice with join given by addition.
- The complete rH-degree of c.e. reals is the same as the complete S-degree.
- The rH-degrees of c.e. reals are dense.
- Every incomplete rH-degree of c.e. reals splits over any lesser degree.
- The complete rH-degree does not split.

What about

H and K reducibilities?

- Recall: for $Q \in \{H, K\}$,$\alpha \leq_Q \beta$ iff there is a c such that, for all n, $Q(\alpha \upharpoonright n) \leq Q(\beta \upharpoonright n) + c$.
- $\leq_{rH}$ and the others are examples that have this property but do not capture it for $Q = H$ since they all imply Turing reducibility:

Solovay's Theorem:

- There exist noncomputable reals α such that for all n

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

- 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

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

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

- (Question) Does $\leq_K$ imply $\leq_{rK}$ (surely not)

A proof of Solovay's Theorem

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

- (Downey, Hirschfeldt, Nies), There is a c.e. noncomputable set A such that for all n

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

- Let

$$A = \{\langle e, n\rangle : W_{e,s} \cap A_s = \emptyset \wedge \langle e, n\rangle \in W_{e,s}$$

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

- Amazingly, it turns out that A is H-trivial. (diagram)
- Note that this is injury free? Is it complete? (cf. Priority free solution to Post's Problem (Kucera).
- In general, how do $\leq_H$ and $\leq_T$ relate? DHN have shown that if α is H-trivial and $\beta \leq_{wtt} \alpha$, then β is H-trivial, and that there are T-degrees with 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) $g(n) \in D_{h(n)}$.

- Here is a proof of Kucera-Terwijn, a Martin-Löf low c.e. set.
- There is a primitive recursive function f, so that $U^A_{f(n}$ is the universal Martin-Löf test relative to A with I^A_n the corresponding Solovay test. Then X is A-random iff X is in at most finitely many I^A_n.
- We build $J_n : n \in \omega$ a Solovay test so that for each $(p, q) \in I^A_n$ is also in J_n. This is done by simple copying: if $(p, q) < s$ is in $\cup_{j \leq s} I^{A_s}_j$ is not in $J_i : i \in s$, add it. It covers I^A_n.
- We need to make A so that the "mistakes" are not too big.
- The crucial concept comes from

Kučera and Terwijn: Let $M_s(y)$ denote the collection of intervals $I_n^{A_s} : n \leq s$ which have $A_s(y) = 0$ in their use function. Then we put $y > 2e$ into $A_{s+1} - A_s$ provided that e is least with $A_s \cap W_{e,s} = \emptyset$, and

$$\mu(M_s(y)) < 2^{-e}.$$

More Questions

- How do Schnorr low and Martin Löf low sets relate? Is there a characterization of ML-low sets.
- How complicated are Schnorr random c.e. reals. (D-Griffiths) They are high, and not necessarily Martin-Löf random(Schnorr).
- What about relative Schnorr randomness.
- Test set characterizations of relative randomness?
- Randomness and structures?

- P-time, e.g. Schnorr-Lutz randomness and NP etc.
- The situation for non c.e. reals and c.e. sets. (Kummer, etc.)

- Thank you.