Trivial Reals

Rod Downey

Victoria University

Wellington

New Zealand

- Joint work with Denis Hirschfeldt (Chicago) Andre Nies (Auckland) and Frank Stephan (Heidelberg)

The Basic Refs are van Lambalgen's Thesis, Solovay's unpublished notes, and Li-Vitanyi.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

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.

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

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

Kraft's Theorem

- (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.

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.

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

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

- 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 $\alpha \leq_T \beta$.

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

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

- 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. (proof?)

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

- 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.