Algorithmic Randomness

Rod Downey

Victoria University

Wellington

New Zealand

The Basic Refs are van Lambalgen's Thesis, Solovay's unpublished notes, and Li-Vitanyi.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

Some Computability-Theoretical Aspects of Reals and Randomness, to appear, in a *Lecture Notes in Logic* volume edited by Cholak. et. al.

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.
  $B = \{f(0), f(1), \dots\}$.

- 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 $\limsup_n F(\alpha \upharpoonright n) \to \infty$.

- 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. (Formalizing the Berry paradox)
- 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)

- 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.
- Proof: We can enumerate the Turing machines $\{M_e : e \in \mathbb{N}\}$. Define

  $$U(1^e 0\sigma) = M_e(\sigma).$$

  This particular coding gives $C(\tau) \leq M_e(\tau) + e + 1$.

- (Plain Counting Theorem-Kolmogorov) $|\{\tau : C(\tau) \leq |\tau| - d\}| \leq O(1)2^{|\tau|-d}$.
- Proof: pigeonhole principle.
- Thus plain complexity is a *combinatorial fact* This is important when we look at compression functions later.

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, $C(\alpha \upharpoonright n) \geq n - d$.
- (Martin-Löf) NO such real exist!

- Why? Take any α. Then, as a string $\alpha \restriction n$ corresponds to some number which we can interpret as a string using llex ordering: $\alpha \restriction n$ 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 $\alpha \restriction n$.
- The output would be much longer, and would be $\alpha \restriction m + n$, with input having length m. Thus $C(\alpha \restriction m + n) < m + n - O(1)$.
- This pehnomenom is fundamental in

our understanding of Kolmogorov complexity and is called *complexity oscillations*.

- There are several known ways to get round this problem to cause only to get the information provided by the *bits* of the strings.

Prefix free

universal computers

- Levin, Gaćs, Chaitin.
- 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.

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

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

- They exist, same proof.
- Fix a universal prefix-free machine M.

Levin-Gaćs-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 $\sigma| = n$.
- (Counting Theorem-Chaitin) $|\{\tau : |\sigma| = |\tau| = n \wedge K(\sigma) \leq K(\tau) + d - c\}| \leq O(2^d)2^{n+K(n)-c}$.

- 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.

The proof and Kraft-Chaitin

- Theorem(Kraft)

  (i) If A is prefix-free then $\sum_{n \in A} 2^{-|n|} \leq 1$.

  (ii) (This part is now called Kraft-Chaitin, or Chaitin simulation) Let $d_1, d_2, \cdots$ be a collection of lengths, possibly with repetitions, Then $\Sigma 2^{-d_i} \leq 1$ iff there is a prefix-free set A with members σ_i and σ_i has length d_i. Furthermore from the sequence d_i we can effectively compute the set A.

- Proof: On direction of Kraft-Chaitin

is clear. This is because of the topological correspondence $\Delta : [\sigma] \mapsto [0.\sigma, 0.\sigma + 2^{-|\sigma|})$ taking the string σ to an interval of size $2^{-|\sigma|}$, gives a correspondence between a set of disjoint intervals in $[0, 1)$ and a prefix-free set.

- The noneffective case:
- Given lengths $\{d_i : i \in \mathbb{N}\}$ in some random order.
- Arrange in increasing order, say $l_1 \leq l_2 \leq \ldots$.
- Choose disjoint intervals I_j, with the right end-point of I_n as the left endpoint of I_{n+1} and the length of I_{n+1} being $2^{-l_{n+1}}$. Then we can

again use the correspondence by setting $[\sigma_n] = \Delta^{-1}(I_n)$.

- Chaitin's process: (Using a trick of Joe Miller) The idea is that, at each stage n, we have a mapping $d_i \mapsto [\sigma_i]$, $|\sigma_i| = d_i$, together with a binary string $x[n] = .x_1 x_2 \dots x_m$ representing the length $1 - \sum_{j \leq n} 2^{-d_j}$.
- Ensure for 1 in the expansion that there is a string of precisely that length in $2^{<\omega} - \{\sigma_j : j \leq n\}$.
- To continue the induction, at stage $n+1$, when a new length d_{n+1} enters,
- position $x_{d_{n+1}}$ is a 1. Then we can find the corresponding string $\tau_{d_{n+1}}$ in

$2^{<\omega} - \{\sigma_j : j \leq n\}$ and set $\sigma_{n+1} = \tau_{d_{n+1}}$. Then of course we make $x_{d_{n+1}} = 0$ in $x[n+1]$.

- If position $x_{d_{n+1}}$ is a 0, find the largest $j < d_{n+1}$ with $x_j = 1$, find the lexicographically least string τ extending τ_j of length d_{n+1}, let $\sigma_{n+1} = \tau$, and let $x[n+1] = x[n] - .\nu$ where ν is the string which is zero except for 1 in position d_{n+1}.

- Notice that nothing changes in $x[n+1]$ from $x[n]$ except in positions j to d_{n+1}, and these all change to 1, with the exception of x_j which changes to 0. Since τ was chosen as the lexicographically least string in the cone $[\tau_j]$, there will be corresponding strings in $[\tau_j]$ of lengths $j-1, \ldots, d_{n+1}$, as required to complete the induction.

- (Restatement) Suppose that we are effectively given a set of "requirements" $\langle n_k, \sigma_k \rangle$ for $k \in \omega$ with $\sum_k 2^{-n_k} \leq 1$. Then we can (primitive recursively) build a prefix-free machine M and a collection of strings τ_k with $|\tau_k| = n_k$ and $M(\tau_k) = \sigma_k$.

Proof of Schnorr's Theorem

- $\Longrightarrow$ Suppose that α is not Martin-Löf random and $\alpha \in \cap_i U_i$, with $\mu(U_i) \leq 2^{-i}$.
- We use Kraft-Chaitin.
- Let $n \geq 3$. For all strings σ in U_{n^2}, enumerate the pair $|\sigma| - n, \sigma$ into B.
- By prefix-freeness, 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 $\tau_n \in$ dom$M$ with $M(\tau_n) = \sigma_n$ and $|\tau_n| = |\sigma| - n$.

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

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

Then $\mu(U_k) \leq 2^{-k}$ (as the domain of M is prefix-free) and hence, as $\alpha \notin \cap_K U_k$, we are done.

Lots of random reals

- $\mu\{A : A \text{ random } \} = 1$.
- Consider the Σ^0_2 class $\{A : \exists k \forall n K(A \upharpoonright n > n - k\}$ contains all random reals.
- Hence there are ones of low Turing degree (low basis theorem) and hyperimmune free degree.
- There are ones of all jumps and even Δ^0_2 ones of all jumps (Kučera, Downey-Miller)

Extending Schnorr's Theorem

- (Miller and Yu) α is Martin-Löf random iff $\sum_{n \in \mathbb{N}} 2^{n-K(\alpha \upharpoonright n)} < \infty$.
- This says that whilst the K-complexity is above n, mostly it is "pretty far" from n.
- (Miller and Yu) 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 $K(\alpha \upharpoonright m) > m + f(m) - O(1)$.

Monotone Complexity

- Levin's original idea here was to try to assign a complexity to the *real itself.* That is, think of the complexity of the real as the shortest machine that outputs the real. Hence now we are thinking of machines that take a program σ and might perhaps output a real α. (Nonsense unless α is computable)
- The following definition can be applied to Turing machines with potentially infinite output, and to discrete ones mapping strings to strings. In this definition, we regard

$M(\sigma)\downarrow$ to mean that at some stage s, $M(\sigma)\downarrow [s]$.

- We say that a machine M is *monotone* if its action is continuous. That is, for all $\sigma \preceq \tau$, if $M(\sigma)\downarrow$ and $M(\tau)\downarrow$ then

$$M(\sigma) \preceq M(\tau).$$

- Levin's (standard) monotone complexity Km is defined as follows. Fix a universal monotone machine U.

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

- (Levin's Theorem) A is Martin-Löf random iff $Km(A \upharpoonright n) > n - O(1)$.

  (One direction holds since every prefix-free machine is monotone, the other we again put $[\sigma]$ into U_k iff $Km_M(sigma) \leq |\sigma| - k$. where M is a universal monotone machine, and

$$\mu(U_k) = \sum\{2^{-|\sigma|} : K_M(\sigma) \leq |\sigma| - k \wedge$$

$$\forall \tau \prec \sigma (K_M \tau) > |\tau| - k)\} \leq 2^{-k}.$$

- In fact A is Martin-Löf random iff $Km(A \upharpoonright n) = n - O(1)$.

The Coding Theorem

- There is another important characterization in terms of *discrete semimeasures.*

- A discrete semimeasure is function $m : 2^\omega \mapsto \mathbb{R}^+ \cup \{0\}$ such that
$$\sum_{\sigma \in 2^\omega} m(\sigma) \leq 1.$$

- An equivalent way to think of a discrete semimeasure is to identify 2^ω with $\mathbb{N}$ and think of $\mathbb{N}$ as being our measure space.

- The discrete Lebesgue measure is $\lambda(\sigma) = 2^{-2|\sigma|-1}$.

- There is a universal multiplicatively minimal discrete c.e. semimeasure. Fix one, say m.

- The Coding Theorem (Levin, Gaćs, Chaitin) Given a prefix-free machine D, let $Q_D(\sigma) = \mu(D^{-1}(\sigma))$ Fix D to be a universal prefix-free machine. Then $-\log m(\sigma) =$ $-\log Q(\sigma) + O(1) = K(\sigma) + O(1)$.

- Proof: Kraft-Chaitin again.

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 effective 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.
- Ω is random.
- Proof. We use Kraft-Chaitin: We build a Kraft-Chaitin set with coding constant c given by the recursion

theorem. If, at stage s, we see $K_s(\Omega_s \restriction n) < n - c - 1$, enumerate $\langle n - c, \Omega_s \restriction n \rangle$ into KC, and hence $\Omega \restriction n \neq \Omega_s \restriction n$.

Plain Complexity again

- In spite of the fact that we have this natural characterization in terms of K or Km, it was a longstanding question whether there was a plain complexity charcaterization of randomness.

- the relationship between plain and prefix-free complexities is complicated.

- (Solovay)

  $$K(x) = C(x) + C^{(2)}(x) + \mathcal{O}(C^{(3)}(x)).$$

  $$C(x) = K(x) - K^{(2)}(x) + \mathcal{O}(K^{(3)}(x)).$$

- The 3's are *sharp*
- The maximum a string of length n can be is (i) $C(\sigma) = n - O(1)$. (ii) $K(\sigma) = n + K(n) - O(1)$.
- (Solovay) (ii) implies (i), but not conversely.
- Say that a real is strongly Chaitin random iff there are infinitely many n with $K(\alpha \upharpoonright n) \geq n + K(n) - O(1)$.
- Say that it is Kolmogorov random if there are infinitely many n with $C(n) \geq n - O(1)$.
- (Solovay) They exist.
- Fundamental question: are they the same?

- Can define 2-randomness as 1-randomness relative to the halting problem.

Kolmogorov randomness

- Theorem Nies-Terwijn-Stephan, Miller 2-randomness=Kolmogorov randomness.
- Proof We fix a universal machine U which is universal and prefix-free for all oracles. we use H to denote the halting set. Suppose that A is *not* 2-random. Thus, for each c there is an n with

$$K^H(A \upharpoonright n) < n - c.$$

- We build a plain machine M. On an input σ, M tries to parse σ as $\tau\beta$, with τ in the domain of U^H. Note that as K^X is prefix-free for all oracles X, there is at most one $\tau \prec \sigma$.

- Let $s = |\sigma|$.
- First it assumes that s is sufficiently large that H_s is correct on the use of $A \upharpoonright n$. It assumes that It then uses H_s as an oracle, to compute (if anything) $\tau \prec \sigma$ with $U^{H_s}(\tau) \downarrow$.
- If there is one, M outputs $U^{H_s}(\tau)\beta$. From some time onwards, upon input $\nu A[n+1, m]$ with $U^H(\nu) = A \upharpoonright n$, this will be $A \upharpoonright m$.
- Thus $C(A \upharpoonright m)$ is bounded away from m.
- The other direction. (Miller, NST)

- A compression function acts like U^{-1}.
- We say that $F : \Sigma^* \mapsto \Sigma^*$ is a compression function if for all x $|F(x)| \leq C(x)$ and F is 1-1.
- Nies, Stephan, and Twerijn There is a compression function F with $F' \leq_T \emptyset'$.
- Consider the Π^0_1 class of functions $|\widehat{F}(\sigma)| \leq C(\sigma)$.
- The main idea is that most of the basic facts of plain complexity can be re-worked with any compression function. For a compression function F we can define F-Kolmogorov complexity: α is F-Kolmogorov

random iff
$\exists^\infty n(F(\alpha \restriction n) > n - O(1))$.

- (NST) If Z is 2-random relative a compression function F, then Z is Kolmogorov F-random.

- Now we can save a quantifier using a low compression function.

1-randomness and plain complexity

- Theorem (Miller and Yu) x is Martin-Löf random iff $(\forall n)\, C(x \upharpoonright n) \geq n - g(n) - \oplus O(1)$, for every computable $g\colon \omega \to \omega$ such that $\sum_{n\in\omega} 2^{-g(n)}$ is finite.

Measures of Relative Randomness

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

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

- Notice that if α is random and $\alpha \leq \beta$ then by Schnorr's Theorem, β is random too.

- 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. Clearly $\leq_S$ implies $\leq_T$.
- S-reducibility is a measure of relative randomness (Solovay)
- This follows by : Let d be given. Then there is a constant $c = c(d)$ such that for all n: if σ and τ have length n and $|\sigma - \tau| < 2^{-n+d}$, $K(\sigma) + c > K(\tau)$.

Kucera-Slaman Theorem

- A c.e. real is Ω-*like* if it dominates all c.e. reals.

- (Solovay) Any Ω-like real is random.
- Proof : By Schnorr.

  Solovay proved that Ω-like reals posessed many of the properties that Ω posessed. He remarks:

  "It seems strange that we will be able to prove so much about the behavior of $K(\Omega \restriction n)$ when, a priori, the definition of Ω is thoroughly model dependent. What our discussion has shown is that our results hold for a class of reals (that include the value of the universal measures of ...) and that the function $K(\Omega \restriction n)$ is model independent to within $O(1)$."

- **Theorem** (Calude, Hertling, Khoussainov, and Wang) If a c.e. real is Ω-like then it is an Ω-number. That is, a halting probability.

- Proof: We have $\Omega \leq_S \alpha$ with enumerations $\Omega_s \to \Omega$, $\alpha_s \to \alpha$

- We know that if we use a stage by stage approximation, then essentially $c(\alpha - \alpha_s) \geq \Omega - \Omega_s$.

- Use Kraft-Chaitin. If $U(\tau) = \sigma$ then $2^{-|\tau|}$ enters the domain of $U - U_s$. We re-cycle this by defining $M(\tau) = \sigma$ with $2^{-|\tau|}$ entering $\alpha - \alpha_s$, this keeping $K_M(\sigma) \leq K_U(\sigma) + c$. etc.

- **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.)

- Proof: Suppose that α is random and β is a c.e. real. We need to show that $\beta \leq_S \alpha$. We enumerate a Martin-Löf test $F_n : n \in \omega$ in stages. Let $\alpha_s \to \alpha$ and $\beta_s \to \beta$ computably and monotonically. We assume that $\beta_s < \beta_{s+1}$.

- At stage s if $\alpha_s \in F_n^s$, do nothing, else put $(\alpha_s, \alpha_s + 2^{-n}(\beta_{s+1} - \beta_{t_s}))$

into F_n^{s+1}, where t_s denotes the last stage we put something into F_n.

- One verifies that $\mu(F_n) < 2^{-n}$. Thus the F_n define a Martin-Löf test. As α is random, there is a n such that for all $m \geq n$, $\alpha \notin F_m$. This shows that $\beta \leq_S \alpha$ with constant 2^n.

Structure

- The c.e. reals using $\leq_S$ forms a upper semilattice, 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.

A unified approach

- For $x, y \in 2^\omega$, write $x \leq_{vL} y$ if $(\forall z \in 2^\omega)\ x øplus z$ is 1-random $\implies$ $y \oplus z$ is 1-random.
- is the same as Define $y \leq_{\mathcal{L}R} x$ if $(\forall z \in 2^\omega)\ z$ is 1-x-random $\implies$ z is 1-y-random, on the randoms.
- inspired by van Lambalgen: $A \oplus B$ is random iff A is B-random and B is A-random.
- (Miller and Yu) If $x \leq_{vL} y$ and x is n-random, then y is n-random.
- (Miller and Yu) If $y \leq_T x$ and y is 1-random, then $x \leq_{vL} y$.

- (Miller and Yu) If $m \neq n$, then $\Omega^{\emptyset^{(m)}}$ and $\Omega^{\emptyset^{(n)}}$ have no upper bound in the vL-degrees.

- (Miller and Yu) If x is n-random and $y \leq_T x$ is 1-random, then y is n-random.

- (Miller and Yu) $x \leq_K y \implies x \leq_{vL} y$.

- (Hence)(Yu, Ding, Downey) $\mu(\{\beta : \beta \leq_K \alpha\}) = 0$.

- Proof: If β is 1-α-random, then $\beta \not\leq_{vL} \alpha$ and hence, since $\mu(\{\beta : \beta$ is 1-α-random $\}) = 1$, we get $\mu(\{\beta : \beta \leq_K \alpha\}) = 0$, by applying Corollary **??**.

Martingales

- 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.
- also have *supermartingales* where we only ask $F(\sigma) \geq \frac{F(\sigma 1)+F(\sigma 0)}{2}$.
- Supermartingales have an advantage that they can be enumerated, and

there is a multiplicatively optimal minimal one. (Levin)

- (Schnorr) a real is 1-random iff no computably enumerable (super-)martingale succeeeds on it. Here F above should have a computable sequence of approximations $F_s \to F$.

- Proof; (Idea) Let $U_k : k \in \omega$ be a Martin-Löf test. Initially define $F_0(\sigma) = 1$ for all σ. If we see $[\sigma] \in U_k[s]$ raise $F_{s+1}(\widehat{\sigma}) = F_s(\widehat{\sigma}) + 1$ for all $\sigma \preceq \widehat{\sigma}$. Propogate this down to λ losing powers of 2. (fig) Then $A \in \cap_k U_k$ iff $F(A \upharpoonright n) \to \infty$.

  The other direction is similar. When $F(\sigma) > 2^k$ put $[\sigma] \in U_k$.

Continuous semimeasures

- Yet another view is provided by Levin's continuous semimeasures.
- A *continuous semimeasure* is a function $\delta : [2^{<\omega}] \mapsto \mathbb{R}^+ \cup \{0\}$ satisfying

  (i) $\delta([\lambda]) \leq 1$, and

  (ii) $\delta([\sigma]) \geq \delta([\sigma 0]) + \delta([\sigma 1])$.

  We need (ii) because we are no longer giving Cantor space a discrete topology, but its usual one.
- In the words of Li and Vitanyi, a semimeasure is a "defective" measure, as it is only *subadditive*. Of

course we can talk about effective semimeasures, as c.e. semimeasures (and hence "effective defective measures"!).

- These correspond: F be a supermartingale. Define

$$\delta([\sigma]) = 2^{-|\sigma|}F(\sigma).$$

Then δ is a semimeasure, and F is multiplicatively optimal iff δ is.

- We can also associate a version of Kolmogorov complexity to a semimeasure.

$$KM(\sigma) = -\log \delta([\sigma]),$$

where δ is the optimal semimeasure.

- Notice that

$$KM(\sigma) = -\log F(\sigma) + |\sigma| + O(1),$$

where F is an optimal supermartingale.

- The notation KM is similar to the notation Km used for (continous) monotone Kolmogorov complexity

- If α is random then the universal supermartingale is eventually constant on it and hence

$$KM(\alpha \upharpoonright n) = n + O(1) = Km(\alpha \upharpoonright n).$$

- If α is computable, then the universal supermartingale is, up to a multiplicative constant, 2^n on initial segments of length n upon it. Hence KM like Km is constant on computable reals.

- It was a longstanding open question whether KM and Km differed on strings. That is, whether a natural analog of the Coding Theorem, Theorem **??**, held for continuous measures.

- Levin conjectured that indeed it did, and $Km(\sigma) = KM(\sigma)$ for all σ. This question was finally solved in 1983 by P. Gács.

- This also shows that supermartingale reducibility and monotone reducibility differ.

Hausdorff dimension

- 1895 Borel, Jordan
- Lebesgue 1904 measure
- In any n-dimesnional Euclidean space, Carathéodory 1914

$$\mu^s(A) = \inf\{\sum_i |I_i|^s : A \subset \cup_i I_i\},$$

where each I_i is an interval in the space.

- 1919 Hausdorff s fractional. and refine measure 0.
- For $0 \leq s \leq 1$, the s-measure of a clopen set $[\sigma]$ is

$$\mu_s([\sigma]) = 2^{-s|\sigma|}.$$

- Lutz has the folllwijg characterization of effective Hausdorff dimension:
- An *s-gale* is a function $F : 2^{<\omega} \mapsto \mathbb{R}$ such that

$$F(\sigma) = 2^s(F(\sigma 0) + F(\sigma 1)).$$

Similarly we can define s-supergale, etc.

- Theorem (Lutz) For a class X the following are equivalent:

(i) $\dim(X) = s$.

(ii) $s = \inf\{s \in \mathbb{Q} : X \subseteq S[d]$ for some s-gale $F\}$.

- Lutz says the folllowing:

"Informally speaking, the above theorem says the the dimennsion of a set is the *most hostile environment* (i.e. most unfavorable payoff schedule, i.e. the infimum s) in which a single betting strategy can *achieve infinite winnings* on every element of the set."

- Thm Lutz, Mayordomo: The Hausdorff dimension of a real α is

$$\liminf_{n\to\infty} \frac{K(\alpha \upharpoonright n)}{n} = (\liminf_{n\to\infty} \frac{C(\alpha \upharpoonright n)}{n})$$

Dimensions of strings

- Lutz has introduced a method of assigning dimensions to strings.
- liminf $\frac{K(\alpha\restriction n}{n}$,
- equivalently, the infimum over all s of the values of $d^s(\alpha \restriction n)$.
- To discreteize this characterization, Lutz used three devices:

  (i) He replaced supergales by *termgales*, which resemble supergales, yet have modifications to deal with the terminations of strings. This is done first via s-termgales and then later by termgales, which are uniform families of s-termgales.

(ii) He replaced $\to \infty$ by a finite threshold.

(iii) He replaced optimal s-supergale by and optimal termgale.

- For $s \in [0, \infty)$, an s-*termgale* is a function d from the collection of terminated strings T to $\mathbb{R}^+ \cup \{0\}$, such that $d(\lambda) \leq 1$, and

$$d(\sigma) \geq 2^{-s}[d(\sigma 0) + d(\sigma 1) + d(\sigma \Box)].$$

Here $\Box$ is a delimiting symbol, and has vanishing probability as $n \to \infty$.

- (i) A *termgale* is a family $d = \{d^s : s \in [0, \infty)\}$ of

s-termgales such that

$$2^{-s|\sigma|}d^s(\sigma) = 2^{-s'|\sigma|}d'(\sigma),$$

for all s, s' and $\sigma \in 2^{<\omega}$.

(ii) We say that a termgale is *constructive* or Σ^0_1, if d^0 is a Σ^0_1 function.

- Now introduce optimal termgales etc.
- filtering through discrete semimeasures and the Coding theorem, you get
- There is a constant $c \in \mathbb{N}$ such that for all $\sigma \in 2^{<\omega}$,

$$|K(\sigma) - |\sigma| \dim(\sigma)| \leq c.$$

How do K and T reducibilities interact?

- It is known that if $\alpha \leq_C \mathbb{N}$ then α is computable. (Chaitin)
- 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

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

- 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.
- 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.

Recall n-randomness

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

Answer NO: there are $A =^* B$ with $\Omega^A|_T\Omega^B$.

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 if α is 3-random.

- (DHNM) also if $A \leq_T B$ and A, B are random with B n-=random, then A is also n-random. Thus randomness is a *lowness* property.

- (DHNM) On the other hand every 2-random is Ω^B for some B.

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.