Algorithmic Randomness 2

Rod Downey

Victoria University

Wellington

New Zealand

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 have high Kolmogorov complexity.

3. Other views: e.g. random means unpredictable. No effective betting strategy succeeds on α.

Richard von Mises:

- Actually, the first attempt to “define” randomness was by von Mises 1919.
- Stochastic approach: $\alpha = a_1 a_2 \ldots$, “select” some subsequence assuming “acceptable” selection rules,
- say positions $f(1) < f(2) \ldots$, then $n \to \infty$, the number of $a_{f(i)} = 1$ divided by those with $a_{f(i)} = 0$ for $i \leq n$ should be 1.
- generalization of the law of large numbers.
- What are acceptable selection rules?

- Some problems (later). Solved by Martin-Löf who said we should view effective statistical tests as effective null sets.

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..
  $U = \{[\sigma] : \sigma \in W\}$.
- 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.

Universal Tests

- Enumerate all c.e. tests, $\{W_{e,j,s} : e, j, s \in \mathbb{N}\}$, stopping should one threated to exceed its bound.
- $U_n = \cup_{e\in\mathbb{N}} W_{e,n+e+1}$.
- A passes this test iff it passes all tests. It is a *universal martin-Löf test.* (Martin-Löf)
- There are other clever constructions we may need later. (Kučera)

Kolmogorov Complexity, again

- From this point of view we should have all the initial segments of a real to be random.
- (Can also use selected places and factor in the complexity of the selection.)

- First try α, a real, is random iff for all n, $C(\alpha \upharpoonright n) \geq n - d$.
- By complexity oscillations (Lecture 1) no such real can exist. The reason as we have seen is that C lacks the intentional meaning of Komogorov complexity.

Levin-Chaitin (K-)

randomness:

- Recall from Lecture 1: prefix freeness gets rid of the use of length as extra information:
- α is K-*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 $\iff$ Martin-Löf random.

Kraft-Chaitin

- Recall from Lecture 1, KC:
  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 $\tau_n \in \mathrm{dom} M$ 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.

Levin and monotone complexity

- Recall from Lecture 1, that for a 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 $Km(A \upharpoonright n) = n - O(1)$.

K and C

- Recall from Lecture 1, we had a notion of weakly Chaitin random string : $K(x) > |x|$.
- (Corollary) For all c, there are infinitely many weakly K random strings σ with $C(\sigma) < |\sigma| - c$.
- (Proof) Consider the initial segments of a random real and C-oscillations.
- Actually with a more refied analysis of the complexity oscillations, you can have $C(x) \leq n - \log n$.

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. (Kučera)
- There are ones of all jumps and even Δ^0_2 ones of all jumps (Kučera, Downey-Miller)

Chaitin's Ω

- The most famous random real is

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

  the "halting probability."

- 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 $K_s(\Omega_s \upharpoonright n) < n - c - 1$, enumerate $\langle n - c, \Omega_s \upharpoonright n\rangle$ into KC, and hence $\Omega \upharpoonright n \neq \Omega_s \upharpoonright n$.

Ω and halting

- Solovay looked at basic properties of Ω, in terms of computability. e.g.
- Let $D_n = \{x : |x| \leq n \wedge U(x) \downarrow\}$.
- (Solovay) $K(D_n) = n + O(1)$.
- (Solovay)

  (i) $K(D_n | \Omega \upharpoonright n) = O(1)$. (Indeed $D_n \leq_{wtt} \Omega \upharpoonright n$ via a weak truth table reduction with identity use.)

  (ii) $K(\Omega \upharpoonright n | D_{n+K(n)}) = O(1)$.
- (i) is easy. Wait till $\Omega_s =_{\text{def}} \sum_{U(\sigma)\downarrow[s]} 2^{-|\sigma|}$ is correct on its first n bits. Then we can compute D_n.

- (ii) is more difficult and is in the notes.

Extending Schnorr's Theorem

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

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.
- It was known that there were *sufficient* conditions on on $C(\alpha \upharpoonright n)$ to guarantee randomness. To wit:
- Say that it is Kolmogorov random if there are infinitely many n with $C(n) \geq n - O(1)$.
- (Solovay) They exist.

1-randomness and plain complexity

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

Martingales

- von Mises again. This time think about predicting the next bit of a sequence. Then you bet on the outcome. You should not win!

- (Levy) A *martingale* is a function $f : 2^{<\omega} \mapsto \mathbb{R}^+ \cup \{0\}$ such that for all σ,
$$f(\sigma) = \frac{f(\sigma 0) + f(\sigma 1)}{2}.$$

- the martingale *succeeds* on a real α, if $\limsup_n F(\alpha \upharpoonright n) \to \infty$.

- Think of betting on sequence where you know that every 2nd bit was 1. Then every second bit you could double you stake. This martingale exhibits exponential growth and that can be used to characterize computable reals.
- Ville proved that null sets correspond to success sets for martingales. They were used extensively by Doob in the study of stochastic processes.

- A *supermartingale* is a function $f : 2^{<\omega} \mapsto \mathbb{R}^+ \cup \{0\}$ such that for all σ,
$$f(\sigma) \geq \frac{f(\sigma 0) + f(\sigma 1)}{2}.$$
- Schnorr showed that Martin-Löf randomness corresponded to effective (super-)martingales failing to succeed.
- f as being *effective* or *computably enumerable* if $f(\sigma)$ is a c.e. real, and at every stage we have effective approximations to f in the sense that $f(\sigma) = \lim_s f_s(\sigma)$, with $f_s(\sigma)$ a computable increasing sequence of rationals.

Schnorr, Again

- Theorem: A real α is Martin-Löf random iff no effective (super-)martingale. succeeds on α.
- The proof uses a basic fact about (super-)martingales.
- (Kolmogorov's inequality)

(i) Let f be a (super-) martingale. For any string σ and prefix-free set $X \subseteq \{x : \nu \preceq x\}$,

$$2^{-|\nu|} f(\nu) \geq \sum_{x \in X} 2^{-|x|} f(x).$$

(ii) Let $S^k(f) = \{\sigma : f(\sigma) \geq k\}$, then

$$\mu(S^k(f)) \leq f(\lambda)\frac{1}{k}.$$

- That is the stake must be shared fairly at level n.

- Proof of Schnorr's Theorem: We show that test sets and martingales are essentially the same. (Ville effectivized). Firstly suppose that f is an effective (super-)martingale.

- Let $V_n = \cup\{\beta : f(\beta) \geq 2^n\}$.

- V_n is a c.e. open set and $\mu(V_n) \leq 2^{-n}$ by Kolmogorov's Inequality.

- Thus $\{V_n : n \in \mathbb{N}\}$ is a Martin-Löf test.

- And $\alpha \in \cap_n V_n$ iff $\limsup_n f(\alpha \upharpoonright n) = \infty$.

- Hence a martingales succeeds on α iff it fails the derived test.

- The other direction.

- Build a martingale from a Martin-Löf test. Let $\{U_n : n \in \mathbb{N}\}$ be a Martin-Löf test.

- We represent U_n by extensions of a prefix-free set of strings σ, and whenever such a σ is enumerated into $\cup_{n,s} U_n^s$, increase $F(\sigma)[s]$ by one.

- To maintain the martingale nature of F, we also increase F by 1 on all extensions of σ, and by 2^{-t} on the substring of σ of length $(|\sigma| - t)$.)

Universal martingales

- (Corollary) There is a universal martingale. For all martingales g, and reals α, f succeeds on α implies g succeeds on α.
- Use the construction above in a universal Martin-Löf test.

Optimal supermartingales

- (Schnorr) We can do better. There is a multiplicatively optimal supermartingale.
- An effective supermartingale f such that for all effective supermartingales g, there is a constant c such that, for all σ,
$$cf(\sigma) \geq g(\sigma).$$
- No such martingale exists.
- This is implicit in Levin's work since $\delta(\sigma) = 2^{-|\sigma|}F(\sigma)$ is the optimal continuous effective semimeasure.

- Proof: construct a computable enumeration of all effective supermartingales, g_i for $i \in \mathbb{N}$. (Stop the enumeration when it threatens to fail the supermartingale condition.)
- Then we can define

$$f(\sigma) = \sum_{i \in \mathbb{N}} 2^{-i} g_i(\sigma).$$

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.
- (i) A martingale f is called computable iff $f : 2^{<\omega} \mapsto \mathbb{R}^+ \cup \{0\}$ is a computable function with $f(\sigma)$ (the index of functions representing the effective convergence of) a computable real. (That is, we will be given indices for a computable sequence of rationals $\{q_i : i \in \mathbb{N}\}$ so that $f(\sigma) = \lim_s q_s$ and $|f(\sigma) - q_s| < 2^{-s}$.)

  (ii) A real α is called *computably* *random* iff for no computable martingale succeeeds on it.

- 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 $\{U_i\}$.
- There is a machine characterization of Schnorr randomness, solving an old question of Ambos-Spies and others.

- Recall that a real is called *computable* if it has a computable dyadic expansion.
- (Stop the enumeration when it threatens to fail the supermartingale condition.) Then we can define

$$f(\sigma) = \sum_{i \in \mathbb{N}} 2^{-i} g_i(\sigma).$$

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

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

is a computable real.
- The domains of prefix-free machines are, in general, only *computably*

enumerable or *left computable* in the sense that they are limits of computable nondecreasing sequences of rations.

- For example $\Omega = \lim_s \Omega_s = \sum_{U(\sigma)\downarrow[s]} 2^{-|\sigma|}$.
- Computably enumerable reals play the same role in this theory as computably enumerable set do in classical computalility theory, and will be deal with in more detail later.
- 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,

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

- Proof. For instance, suppose that α is not Schnorr random. Thus we have $\alpha \in \cap_n V_n$ a Schnorr test.
- We mimic the proof for Martin-Löf dropping complexity of σ by k should $[\sigma]$ occur in the test.
- Now the point is that the proof of KC would give a computable machine if the requirements were computable, which they are.
- the other direction is similar.

Kurtz Randomness

- Another related notion of relevance to this story is: Kurtz or weak 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 $\alpha \in U$.
- Some would suggest that this is not really a randomness notion at all, since it can be shown to be not stochastic, but it will be relvant later.
- There is a null set characterization of this notion.

- (Wang) A *Kurtz null test* is a collection $\{V_n : n \in \mathbb{N}\}$ of c.e. open sets, such that

  (i) $\mu(V_n) \leq 2^{-n}$, and

  (ii) There is a computable function $f : \mathbb{N} \mapsto (\Sigma^*)^{<\omega}$ such that $f(n)$ is a canonical index for a finite set of σ's, say, $\sigma_1, \ldots, \sigma_n$ and $V_n = \{[\sigma_1], \ldots, [\sigma_n]\}$.

- Theorem (Wang, implict in Kurtz's Thesis) A real α is Kurtz random iff it passes all Kurtz null tests.

- Proof Let U be a c.e. open set with $\mu(U) = 1$. We define V_n.

- To define V_1, enumerate U until a stage s is found with $\mu(U_s) > 2^{-1}$.

The let $V_1 = \overline{U_s}$. Continue in the obvious way.

- Theorem (Downey, Grifiths, Reid) A real α is weakly random iff for ever "computably layered" machine M,

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

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

- Soon we will show that all c.e. random reals are Turing complete.

- (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.

- (Downey, Griffiths and Reid) Each c.e. degree contains a c.e. Kurtz random real.

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

Martingale characterizations

- (Wang) A real α is Kurtz random iff there is no computable martingale F and nondecreasing function h, such that for *almost all* n,

$$F(\alpha \upharpoonright n) > h(n).$$

- (Schnorr) We say that a computable martingale *strongly* succeeds on a real x iff there is a computable unbounded nondecreasing function $h : \mathbb{N} \mapsto \mathbb{N}$ such that $F(x \upharpoonright n) \geq h(n)$ infinitely often.
- (Schnorr) A real x is Schnorr random iff no computable martingale strongly succeeds on x.

The full characterization

- Martin-Löf implies computable implies Schnorr implies Kurtz. (randomness)
- The following very attractive result gives the full picture.
- (Nies, Stephan and Terwijn) For every set A, the following are equivalent.

  (I) A is high.

  (II) $\exists B \equiv_T A$, B is computably random but not Martin-Löf random.

  (III) $\exists C \equiv_T A$, C is Schnorr random but not computably random.

- Moreover, for c.e. degrees, the examples can be chosen to be c.e.

Outside the high degrees

- (Nies, Stephan and Terwijn) Suppose that a set A is Schnorr random and does not have high degree. (That is, $A' \not\geq_T \emptyset''$. Then A is Martin-Löf random.

- (Nies, Stephan, Terwijn) Suppose that A is of hyperimmune-free degree. Then A is Kurtz random iff A is Martin-Löf random.

- Both proofs use domination properties.
- The high case.
- Suppose that A is not of high degree and covered by the Martin-Löf test $A \subset \cap_i U_i$. Let $f(n)$ be the stage by which U_n has enumerated a $[\sigma] \in U_{n,s}$ with $A \in [\sigma]$. Note that f is A-computable, and hence computable relative to an oracle which is not high. It follows that there is a computable function g such that $g(n) > f(n)$ for infinitely many n. Then consider the test $\{V_i : i \in \mathbb{N}\}$, found by setting $V_i = U_{i,g(i)}$. The $\cup_i V_i$ is a Schnorr-Solovay test, and hence A is not Schnorr random.

- Proof of the hyperimmune case .
- Suppose that A has hyperimmune free degree, and A is Kurtz random. Suppose that A is not Martin-Löf random. Then since Then there is a Martin-Löf test $\{V_n : n \in \mathbb{N}\}$, such that $A \in \cap_n V_n$. Using A we can compute A-computably compute a stage $g(n)$ such that $A \in V_{g(n)}$, and without loss of generality we can suppose that $V_{g(n+1)} \supseteq V_{g(n)}$. But as A has hyperimmune free degree, we can choose a computable function f so that $f(n) > g(n)$ for all n. Then if we define $W_n = V_{f(n)}$, being a Kurtz null test such that $A \in \cap_n W_n$, a contradiction.

- Actually this works for weakly 2-random reals.

von Mises strikes back

- There has been a lot of work recently on nonmonotonic selection, and nonmonotomic martingales, which might address Schnorr's critique.
- Briefly, we get toselect position $f(0), f(1), \ldots$ and bet on thse bits, but now the selction on the places can be nonmonotonic.
- Important open question (Muchnik, Uspensky, Semenov)
- Is randomness relative to computable nonmonotonic supermartingales the same as Martin-Löf randomness. (also see MMNRS)

Hausdorff Dimension

- Actually Schnorr called the function h and *order*.
- If F is a martingale and h is an order the *h-success* set of F is the set:

$$S_h(F) = \{\alpha : \limsup_{n\to\infty} \frac{F(\alpha \upharpoonright n)}{h(n)} \to \infty\}.$$

- Thus, A real α is Schnorr random iff for all computable orders h and all computable martingales F, $\alpha \notin S_h(F)$.
- Exponential orders offer a special place in this subject.

- (Lutz) An s-*gale* is a function $F : 2^{<\omega} \mapsto \mathbb{R}$ such that

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

- The basic idea here is that not betting on one outcome or the other is bad.
- Usually, decide that we are not prepared to favour one side or the other in our bet. Thus we make $F(\sigma i) = F(\sigma)$ at some node σ.In the case of an s-gale, then we will be unable to do this, without *automatically losing money due to inflation.*
- Lutz has shown that effective Hausdorff dimension can be

characterized using these notions.

- It is not important exactly what the definition is but we get the following.
- (Lutz, Hitchcock) 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 $F\}$.

  (iii) $s = \inf\{s \in \mathbb{Q} : X \subseteq S_{2^{(1-s)n}}[d]$ for some martingale $d\}$.

- Lutz comment:
- "Informally speaking, the above theorem says the the dimension 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."
- While Schnorr did not do any of this, he did look at exponential orders. He comments:
- "To our opinion the important statistical laws correspond to null sets with fast growing orders. Here the exponentially growing orders are

of special significance."