Algorithmic Randomness 3

Rod Downey

Victoria University

Wellington

New Zealand

Motivation

- Reurning to the theme of studying randomness in 2^ω and in particular the relationship of (n-) randomness to calibrations of reals by relatitive computational complexity.
- For instance, how do random reals perform as oracles?

Enumeration probabilities

- The first linkage of measure and degrees was the following: (also Spector, 1958 for hyperdegrees)
- Recall an index e for $\emptyset'$ is is universal if for all indices f and all sets S, there is a finite string σ_f such that

$$W_f^S = W_e^{\sigma_f S}.$$

- Define $P(A) = \mu\{X : W_e^X = A\}$.

de Leeuw, et. al.;Sacks

- Theorem: (de Leeuw, Moore, Shannon, Shapiro, 1956) If $P(A) > 0$ then A is computably enumerable.

- Corollary: Sacks $\mu\{X : A \leq_T X\} > 0$, iff A is computable.

- The proof uses the *majority vote* technique, which is an important standard tool. Assume $P(A) > 0$.

- For some e, $D_e = \{X : A = W_e^X\}$ has positive measure.

- There is a string σ such that the relative measure of D_e above σ is greater than $\frac{1}{2}$. (Lebesgue Density Theorem)

- Let the oracles extending σ vote on membership in D_e

- Pu n into A if more than half (by measure) say so. This enumerates A.

Solovay's Therem

- Solovay examined the relationship between $P(A) > 0$ and the least index for $W_i = A$.
- Let $H(A) = \lceil -\log P(A) \rceil$
  $I(A) = \min\{K(i) : W_i = A\}$.
- Theorem (Solovay)

$$I(A) \leq 3H(A) + K(H(A)) + O(1).$$

- The proof is combinatorial, and uses a clever lemma of Martin.

Stillwell's Therem

- Similar methods show the following due to Stillwell.

  (i) Suppose that $\mu(\{C : D \leq_T A \oplus C\}) > 0$. Then $C \leq_T A$.

  (ii) (Hence) For any $\boldsymbol{a}, \boldsymbol{b}$, $(\boldsymbol{a} \cup \boldsymbol{b}) \cap (\boldsymbol{a} \cup \boldsymbol{c}) = \boldsymbol{a}$, for almost all $\boldsymbol{c}$.

  (iii) Similarly for almost all $\boldsymbol{a}$, $\boldsymbol{a}^{(n)} \equiv \boldsymbol{a} \cup \mathbf{o}^{(\boldsymbol{n})}$. Almost all degrees are GL_n.

  (iv) For almost all $\boldsymbol{a}, \boldsymbol{b}$, $\boldsymbol{a} \cap \boldsymbol{b} = \mathbf{o}$.

- Now consider the language where variables $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}, \ldots$ vary over arbitrary degrees. Terms are built from $'$ (jump), $\cup, \cap$.

- An atomic formula $t_1 \leq t_2$ for terms t_1, t_2,

- In general build from atomic ones and $\wedge, ^{-}$ and the quantifier $\forall$ interpreted to mean "for almost all.'

- Then the above allows for the generation of normal forms, and Fubinbi's Theorem allows for treatment of quantifiers. These kinds of considerations give

- Theorem (Stillwell) The “almost all” theory of degrees is decidable.

Coding into randoms

- You might think that the above says that, in general coding into random reals should be impossible.
- The intuitive argument is, perhaps, that a random real should have information, but only in a way that if not organized enough to be able to use it. These is some truth in this as we later see.
- However, coding is possible as we now see.

The Kučera-Gács Theorem

- Every set is *wtt* reducible to a Martin-Löf random set.
- The proof uses blocks to code information, and the Gács coding is more compressed than the Kučera one. Hirschfeldt (unpublished) has yet another coding.
- One easy to understand proof is due to Merkle and Mihailovic using martingales.
- The first Lemma is folklore, more or less going back to Kučera in another form.

The Space Lemma

- (The Space Lemma) Given a rational $\delta > 1$ and $k \in \mathbb{Z}^+$, we can *compute* a length $\ell(\delta, k)$, such that for any martingale d, and any word w,

$$|\{w \in 2^{\ell(\delta,k)} : d(vw) \leq \delta d(v)\}| \geq k.$$

- It is important here that $\ell(\delta, k)$ can actually be computed.

- (Restated) For any martingale d and any interval of length k, there are at least k paths extending v of length $\ell(\delta, k)$ where d cannot increase its capitol more than a factor of δ while betting on I, no matter how d behaves.

- Proof: $d(v) = 2^{-k} \sum_{|u|=k} d(vu)$.
- (Kolmogorov) For any given ℓ and v the average of $d(vw)$ over words of length ℓ is $d(v)$.
- Thus, $\frac{|\{|w|=\ell : d(vw) > \delta d(v)\}|}{2^\ell} < \frac{1}{\delta}$.
- Since $\delta > 1$, $1 - \delta^{-1} > 0$
- Suffices to have $\ell(\delta, k) \geq \log \frac{k}{1-\delta^{-1}} = \log k + \log \delta - \log(\delta - 1)$.

Kučera-Gács

- The space lemma gives enough space for coding.
- Here is the MM proof:
- Let $\beta_i = \Pi_{j \leq i} r_j$, with $r_0 > r_1 > \cdots \in \mathbb{Q}^+$,
- Ask that β_i converge.
- Partition $\mathbb{N} = \cup\{I_s : s \in \mathbb{N}\}$; I_s of size $\ell_s = \ell(r_s, 2)$.
- The Space Lemma tells us for any word v, and any martingale d, there are at least two words w of length ℓ_s with $d(vw) \leq r_s d(v)$.

- We construct R with given $X \leq_{wtt} R$.
- At step s we will specify R on I_s.
- Say w of length I_s is *admissible* if

  (i) $s = 0$ and $d(w) \leq \beta_0$, and

  (ii) for $s > 0$, if

  $$d(vw) \leq \beta_s \text{ for } v = R \upharpoonright (I_0 \cup \cdots \cup I_{s-1})$$

- Induction and Space Lemma show at every step there are at least 2 admissible extensions.
- To specify R, from $R \upharpoonright (I_0 \cup \cdots \cup I_{s-1})$,
- choose left (lex min) if $s \notin X$ and right it $s \in X$.

Kučera Coding

- Similar left-right coding with suitable blocks allows Kučera to prove the following theorem, roughly using something like the Friedberg cupping Theorem and an intersection lemma on fat Π^0_1 classes akin to the Space Lemma.
- Theorem (Kučera, 1985) Suppose that $\boldsymbol{a} > \mathbf{0}'$. Then $\boldsymbol{a}$ is Martin-Löf random.
- Kučera's proof is in the notes. It has other applications. The theorem also follows from the last proof since if X is above $\emptyset'$ then X can compute R.

- Other positive results say that there are randoms of every possible jump (using generalized low basis theory on Π^0_1 classes which have no computable members) and
- (Kučera, Downey-Miller) randoms below $\mathbf{o}'$ of every possible jump, using basis theorems for fat Π^0_1 classes.

Random power

- All of this might lead one to suspect that randoms are in fact computationally powerful. The only explicit ones we have are above $\mathbf{o}'$, except the hyperimmune free ones. (Later we will see that almost all of them are hyperimmune, so the hyperimmune free ones are red herrings.)
- BUT Frank Stephan has shown that these random reals above $\mathbf{o}'$ are in essence the only computationally powerful reals.

- Recall that a degree is called PA if $\boldsymbol{a}$ is PA iff it is the degree of a complete extension of Peano Arithmetic.
- A function f is called *fixed-point free* if $W_{f(x)} \neq W_x$ for all x.
- By Jockusch, Lerman, Soare, and Solovay, $\boldsymbol{a}$ being FPF is equivalent to bing able to compute a DNC function: Namely g with $g(e) \neq \varphi_e(e)$ for all e.
- (Jockusch and Soare) $\boldsymbol{a}$ is PA iff it can compute a $\{0, 1\}$ valued DNC function.

Stephan's Theorem

- (Stephan) Suppose that $\boldsymbol{a}$ is PA and 1-random. Then $\mathbf{o}' \leq_T \boldsymbol{a}$.
- He concludes
  "The main result says that there are two types of Martin-Löf sets: the first type are the computationally powerful sets which permit the solving of the halting problem; the second type of random set are computationally weak in the sense that they are not [PA]. Every set not belonging to one of these two classes is not Martin-Löf random."

n-randomness

- In the same way as the arithmetical hierarchy,
- (i) A Σ^0_n test is a computable collection $\{V_n : n \in \mathbb{N}\}$ of Σ^0_n classes such that $\mu(V_k) \leq 2^{-k}$.

  (ii) A real α is Σ^0_n-random or n-random iff it passes all Σ^0_n tests.

  (iii) One can similarly define Π^0_n, Δ^0_n etc tests and randomness.

  (iv) A real α is called *arithmetically random* iff for any n, α is n-random.

Kurtz's Theorem

- We use open sets to define Martin-Löf randomness.
- Consider: the Σ^0_2 class consisting of reals that are always zero from some point onwards. It is *not* equivalent to $\cup\{[\sigma] : \sigma \in W\}$ for any W.
- Kurtz showed that n-randomness is the same as n randomness relative to open classes. (Detailed statement in the notes) The point is that:
- Theorem (Kurtz) $n+1$-randomness $= 1$-randomness *relative to* $\emptyset^{(n)}$.

- This is also implicit in Solovay's notes in the dual way he treats 2-randomness.
- Thus, for instance, if A is 2-random then $A \not\leq_T \emptyset'$. (Indeed, their degrees forma minimal pair).
- Also there is a $n+1$-random set $\Omega^{(n+1)}$ namely $\Omega^{\emptyset^{(n)}}$ which is computably enumerable relative to $\emptyset^{(n)}$.
- NOTE it is NOT CEA($\emptyset^{(n)}$). But $\Omega^{(n)} \oplus \emptyset^{(n)} \equiv_T \emptyset^{(n+1)}$.

Warning

- Similar relativization work for Schnorr, computable, etc randomness. BUT not for weak randomness.

- It is NOT true that weak-2-randomness (meaning being in every Σ^0_2 class of measure 1) is the same as being Kurtz random over $\emptyset'$. This is a genericity notion. 2-generics have this property.

- The best we can do is: $n \geq 2$, α is Kurtz n-random iff α is in every $\Sigma_2^{\emptyset^{(n-2)}}$-class of measure 1.

- weak 2-randomness is the same as "Martin-Löf randomness with no effective convergence" In fact, weak 2-randomness might best be described as *strong 1-randomness.*

A hierarchy

- Theorem

  (i) (Kurtz) Every n-random real is Kurtz n-random.

  (ii) (Kurtz) Every Kurtz $n+1$-random real is n-random.

  (iii) (Kurtz, Kautz) All containments proper.

Proof

- To get weak n+1-random not n-random prove that no weak n+1 random can be below $\emptyset^{(n)}$. But an n-random can be.

- The most difficult non-containment n-random $\neq$ weak n-random, can be shown by constructing each CEA($\emptyset^{(n)}$) degree $\boldsymbol{a} > \mathbf{o}^{(n)}$ a weakly $n+1$-random reals X $CE(\emptyset^{(n)}$, with $X \oplus \emptyset^{(n)}$ of degree $\boldsymbol{a}$ whereas any such $n+1$ random real Y must have $Y \oplus \emptyset^{(n)}$ of degree $\mathbf{o}^{(n+1)}$.

- This method is due to Downey and Hirschfeldt, and is *not* a relativization of the DGR fact that there are Kurtz randoms of all nonzero c.e. degrees..

2-randomness

- There are some relative natural examples of n-randoms using methods akin to Post's Theorem and index sets (Becher-Figueira). However, there are some really unexpected characterizations also of 2-randoms.

- Recall that 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?

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. Suppose that A is *not* 2-random. Thus, for each c there is an n with

$$K^{\emptyset'} A \upharpoonright n) < n - c.$$

- We build a plain machine M. On an input σ, M tries to parse σ as $\tau\beta$, with τ in the domain of $U^{\emptyset'}$. 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 $\emptyset'_s$ as an oracle, to compute (if anything) $\tau \prec \sigma$ with $U^{\emptyset'_s}(\tau) \downarrow$.
- If there is one, M outputs $U^{\emptyset'_s}(\tau)\beta$. From some time onwards, upon input $\nu A[n+1, m]$ with $U^{\emptyset'}(\nu) = A \upharpoonright n$, this will be $A \upharpoonright m$.
- Thus $C(A \upharpoonright m)$ is bounded away from m.
- The other direction. (Miller, NST)
- Recall from Lecture 1 that a compression function acts like U^{-1}.

- Recall that we defined $F : \Sigma^* \mapsto \Sigma^*$ to be a compression function if for all x $|F(x)| \leq C(x)$ and F is 1-1.

- Recall also that since they forma Π^0_1 class, there is a compression function F with $F' \leq_T \emptyset'$. (NST's idea)

- Namely, 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 $\exists^\infty n(F(\alpha \upharpoonright n) > n - O(1))$.

- (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.
- This still leaves strongly Chaitin random reals. Question are they 3-random, 2-random or something else. Note that the same approach won't work because *both* sides change. (To wit: $F(\alpha \restriction n) = n + F(|n|) - d$. Could to this if there was a low compression function with $K(\sigma) > K(\tau)$ implies $F(\sigma) > F(\tau)$ but this is surely false.)

Kučera strikes again

- We have seen that most random reals are not below $\mathbf{o}'$ and hence are not PA. Thus they are computationally feeble.
- However, Kučera showed that randoms do have *some* power, always.
- Kučera showed that they can compute FPF functions. Recall that this means that they can g with $g(e) \neq \varphi_e(e)$ for all e.

- The difference is that if $g(e)$ is $\{0, 1\}$-valued, (so we are dealing with PA degrees, then g computes something *positive*, whereas in the general case, g computes something *negative*.

- Actually, Kučera proved a nice generalization:
- (Jockusch, Lerman, Soare, and R. Solovay) We define a relation $A \sim_n B$ as follows.

  (i) $A = B$ if $n = 0$.

  (ii) $A =^* B$ if $n = 1$.

  (iii) $A^{(n-2)} \equiv_T B^{(n-2)}$, if $n \geq 2$.

- and a total function f is called *n-fixed point free* (n-FPF) iff for all x,

$$W_{f(x)} \not\sim_n W_x.$$

- Theorem (Kučera) Suppose that A is $n+1$ random. Then A computes an n-FPF function. (cf Generalized Arslanov's completeness criterion.)

van Lambalgen's Theorem

- A *central* (independence) result.
- Lemma (van Lambalgen, (Kučera, Kautz))

  (i) If $A \oplus B$ is n-random so is A.

  (ii) If A is n-random so is $A^{[n]}$, the n-th column of A.

  (iii) If $A \oplus B$ is n-random, then A is $n - B-$random.

  (iv) If $A \oplus B$ is random then $A \not\leq_T B$.

  (v) Hence no random degree is minimal.

- (e.g. (i)) The proof is easy. $(n = 1)$ So suppose $A \oplus B$ is random, but A is not.

- Suppose $A \in [\sigma]$ for infinitely many $[\sigma]$ in some Solovay test V.

- Then $A \oplus B$ would be in $\widehat{V}$, where $[\sigma \oplus \tau] \in \widehat{V}$ for all τ with $|\tau| = |\sigma|$ and $\sigma \in V$. (Measure the same)

- The most important fact is that the *converse* is true.
- (van Lambalgen's Theorem)

  (i) If A n-random and B is $n - A-$random, then $A \oplus B$ is n-random.

  (ii) Hence, $A \oplus B$ is n-random iff A n-random and B is $n - A-$random.

- Proof: Suppose $A \oplus B$ is not random.
- $A \oplus B \in \bigcap_n W_n$ and $\mu(W_n) \leq 1/2^{2n}$.
- Let $U_n = \{X \mid \mu(\{Y \mid X \oplus Y \in W_n\}) > 1/2^n\}$.
- Now, $\mu(U_n) \leq 1/2^n$ since otherwise, $\mu(W_n) > \mu(U_n) \cdot \frac{1}{2^n} > \frac{1}{2^n} \cdot \frac{1}{2^n} = \frac{1}{2^{2n}}$,
- Thus, $\{n \mid A \in U_n\}$ is finite. (A random)
- Hence a.a. n, $A \notin U_n$, and the measure of U_n is small.
- $V_n^A = \{Y \mid A \oplus Y \in W_n\}$ is a A-Solovay test covering B.

A pretty application

- Theorem (Miller and Yu) Suppose that A is random and B is n-random. Suppose also that $A \leq_T B$. Then A is n-random.
- Proof (We do $n = 2$.) If B is 2-random, then B is 1-Ω-random (as $\Omega \equiv_T \emptyset'$.)
- Hence by van Lambalgen's Theorem, $\Omega \oplus B$ is random.
- Thus Ω is 1-B-random.
- But $A \leq_T B$. Hence, Ω is 1-A-random. Hence $\Omega \oplus A$ is random, again by van Lambalgen's Theorem.

- Thus, A is 1-Ω-random. That is, A is 2-random.
- The general case is simlilar and relies only on van Lambalgen's Theorem and Kučera's result that all degrees above $\mathbf{o}'$ are random.
- Actually, Miller and Yu have also proven
- Theorem: For any (not necessarily random Z), any random below a Z-random is itself Z-random. (This does not use van Lambalgen)

- One nice Corollary to van Lambalgen and Sacks' Theorems is the following.
- Theorem (Kautz) Let $n \geq 2$. Then if $\boldsymbol{a}$ and $\boldsymbol{b}$ are relatively n-random, they form a minimal pair.
- Proof Suppose that $D \leq_T, A, B$. Then $A \in \{E : \Phi_e^E = D\}$. By Sacks' Theorem, this set is a Π_2^D-nullset, and hence A is not $n - D-$random, and hence not $2 - B-$random.

Effective 0-1 Laws

- Classical: Any measureable class of reals closed under finite translations has measure 0 or measure 1.
- Effective version?
- Lemma (Kučera-Kautz) Let $n \geq 1$. Let T be a Π^D_n class of positive measure. Then T contains a member of every $D-n-$random degree.
- Indeed, if A is any $n-D-$random, then there is some string σ and real B such that $A = \sigma B$ and $B \in T$.

- Proof ($n = 1, D = \emptyset$)
- T be a Π^0_1 class, $S = \overline{T} = \cup\{[\sigma] : \sigma \in W\}$ W c.e. and prefix-free.
- Let $r \in \mathbb{Q}^+$, with $\mu(S) < r$.
- Let $E_0 = S$ and $E_{s+1} = \{\sigma\tau : \sigma \in E_s \wedge \tau \in W\}$.
- $\mu(E_s) \leq r^s$
- Suppose for all B with $A = \sigma B$, $A \in S$.
- Then $B \in \cap_s E_s$ and is hence not random.
- Actually this can be gotten from the Lemma needed for Kučera coding.

- Theorem (Kurtz)

  (i) Every degree invariant Σ^0_{n+1}-class or Π^0_{n+1} either contains all n-random sets or no n-random sets.

  (ii) In fact the same is true for any such class closed under translations, and such that for all A, if $A \in S$, then for any string σ, $\sigma A \in S$.

- Examples:
- The class $\{A : A$ has non-minimal degree $\}$ has measure 1, and includes every 1-random set.
- The class $\{A \oplus B : A, B$ form a minimal pair $\}$ has measure 1, and includes all 2-random but not every 1-random set.
- The first part of this follows from the result on 2-randoms earlier.

  The second part is trickier.

below 0'

- Theorem (Kučera [**?**]) If A and B are 1-random with $A, B <_T \emptyset'$ then A and B do not form a minimal pair.

- Proof: Choose 2 randoms low and below 0' (van Lambalgen and low basis theorem) Now they are DNC and FPF. Use Kučera's Priority Free Solution to Post's Problem.

- Actually, Hirschfeldt, Nies, and Stephan have shown that the degrees below such pairs are *K-trivial.* (For those who know)

- I will look at some other almost all classes in Lecture 5, where I look at measure-theoretical injury arguments a la Kurtz' Thesis.
- In particular, I will show that almost all degrees are hyperimmune, CEA, bound 1-generics etc.

Omega Operators

- Important ignored work looks at Ω as an operator acting on Cantor space. (Downey, Hirschfeldt, Miller, Nies)
- Hopefully Miller, Nies of Hirschfeldt will present this material.
- Analog of Ω looking like $\emptyset'$ fails as badly as it can.
- We had hoped to attack Martin's conjecture about degree invariant operators on the degree.

- (“Heroic Failure”–Jan Reimann) For all such Ω there are $A =^* B$ with Ω^A and Ω^B relatively random.
- Many other results. One interesting one: Omega operators are lower semicontinuous but not continuous, and moreover, that they are continuous exactly at the 1-generic reals.