Algorithmic Randomness

Rod Downey
Victoria University
Wellington
New Zealand

Darmstadt, 2018

- Lets begin by examining the title:

- Algorithmic
- Randomness

Algorithmic

- Etymology : Al-Khwārizmī, Persian astronomer and mathematician, wrote a treatise in 825 AD, On Calculation with Hindu Numerals, together with an error in the Latin translation.
- What we intuitively mean
- From a set of basic instructions (ingredients) specify a mechanical method to obtain the desired result.

Computable functions and Church's Thesis

- The notion of a Computable Function can be made precise and was done in the 1930's by people like Church, Gödel, Turing and others.
- Became implemented by the work of Turing, von Neumann and others.
- Commonly accepted is Church's Thesis that the intuitively computable functions are the same as those defined by Turing machine (or your favourite programming language, such as JAVA, C++, etc.)
- The point of this is we are able to delineate precisely when something is computable or not. (NB Turing's analysis.)
- Trickier when we talk about complexity theory. (feasible is a subset of polynomial time on a Turing Machine)

Randomness

- The idea is to use algorithmic means to ascribe meaning to the apparent randomness of individual objects.
- Something is random if it is e.g. "unpredictable" where "unpredictable" is interpreted to be somehow "computably predictable".
- This idea goes against the tradition, since Kolmogorov, of assigning all strings of the same length equal probability. That is, 000000000000... does not seem random.
- Nevertheless, we'd expect that the behaviour of an "algorithmically random" string should be typical.

The great men

- Turing 1950:

  > *" An interesting variant on the idea of a digital computer is a "digital comput er with a random element." These have instructions involving the throwing of a die or some equivalent electronic process; one such instruction might for instance be, "Throw the die and put the-resulting number into store 1000." Sometimes such a machine is described as having free will (though I would not use this phrase myself)."*

- von Neumann 1951:

  > *"Any one who considers arithmetical methods of producing random digits is, of course, in a state of sin."*

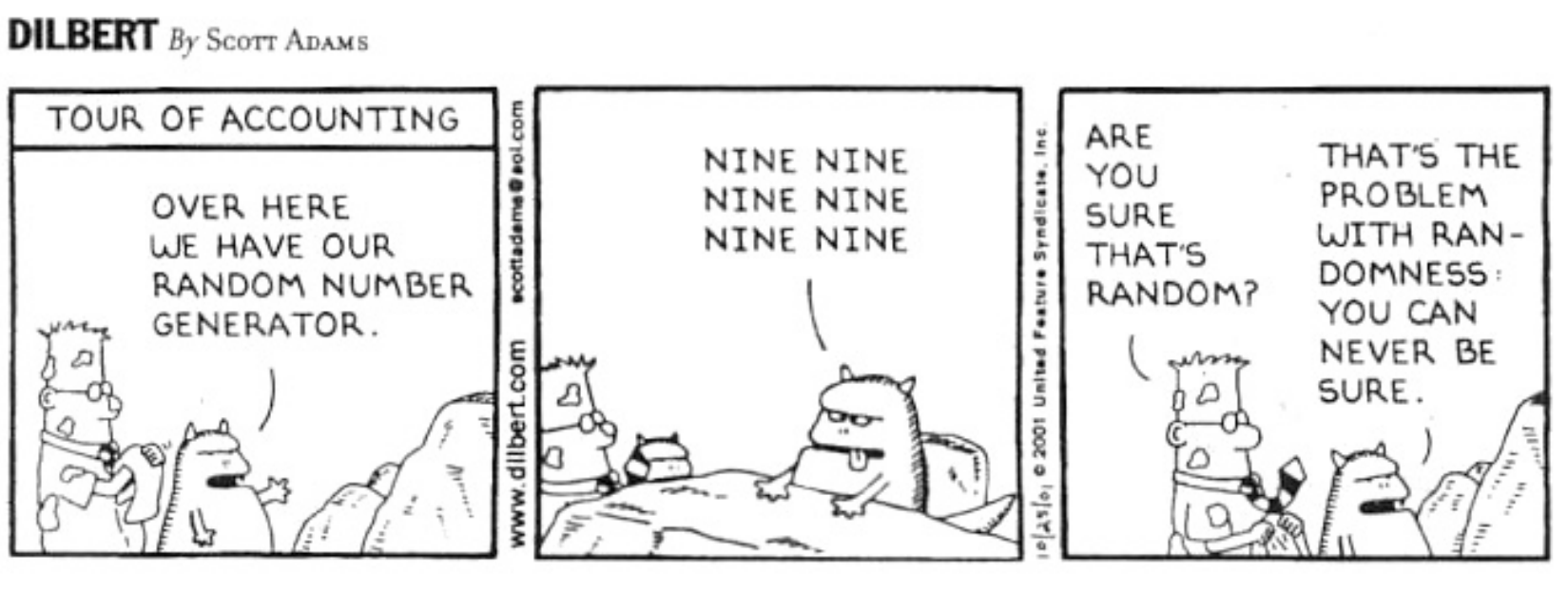
- It is fair to say that both had the idea of "pseudo-random" numbers with no formalization.

Randomness

Even earlier:

> *"How dare we speak of the laws of chance?*
> *Is not chance the antithesis of all law?"*
>
> — *Joseph Bertrand, Calcul des Probabilités, 1889*

Intuitive Randomness



Intuitive Randomness

Which of the following binary sequences seem random?

A 00000000000000000000000000000000000000000000000000

B 00110100110100110100110100110100110100110100110100

C 01000110110000010100111001011101110000000100100011010001010101

D 00100110110110001000111101010011101100100110000000101101010100

E 01010111011011110111001001101011011100110110100001101111011101

F 01110111110011011001101001000011111100110110000001101101010101

G 00000110001011100010000000010100001011010100000010000000100

H 01010011011110110111010101000001011110000001010111010101000101

Intuitive Randomness

Non-randomness: increasingly complex patterns.

A 00000000000000000000000000000000000000000000000000

B 00110100110100110100110100110100110100110100110101

C 01000110110000010100111001011101110000000100100011010001010101

D 00100110110110001000111101010011101100100110000000101101010100

E 01010111011011110111001001101011011100110110100001101111011101

F 01110111110011011001101001000011111100110110000001101101010101

G 00000110001011100010000000010100001011010100000010000000010000

H 01010011011110110111010101000001011110000001010111010101000101

Intuitive Randomness

Randomness: bits coming from atmospheric patterns.

A 00000000000000000000000000000000000000000000000000

B 00110100110100110100110100110100110100110100110100

C 01000110110000010100111001011101110000000100100011010001010101

D 00100110110110001000111101010011101100100110000000101101010100

E 01010111011011110111001001101011011100110110100001101111011101

F 01110111110011011001101001000011111100110110000001101101010101

G 00000110001011100010000000010100001011010100000010000000100

H 01010011011110110111010101000001011110000001010111010101000101

Intuitive Randomness

Partial Randomness: mixing random and nonrandom sequences.

A 00000000000000000000000000000000000000000000000000

B 00110100110100110100110100110100110100110100110101

C 01000110110000010100111001011101110000000100100011010001010 1

D 00100110110110001000111101010011101100100110000001011010100

E 01010111011011110111001001101011011100110110100001101111011 1

F 01110111110011011001101001000011111100110110000001101101010 1

G 00000110001011100010000000010100001011010100000100000000100

H 01010011011110110111010101000001011110000001010111010101000 1

Intuitive Randomness

Randomness relative to other measures: biased coins.

A 00000000000000000000000000000000000000000000000000

B 00110100110100110100110100110100110100110100110101

C 01000110110000010100111001011101110000000100100011010001010101

D 00100110110110001000111101010011101100100110000000101101010100

E 01010111011011110111001001101011011100110110100001101111011101

F 01110111110011011001101001000011111100110110000001101101010101

G 00000110001011100010000000010100001011010100000010000000010000

H 01010011011110110111010101000001011110000001010111010101000101

Historical Roots

- Borel around 1900 looked at normality.
- If we toss an unbiased coin, we ought to get the same number of 0's and 1's on average, and the same for any fixed subsequence like 0100111.

Definition

1. A real (sequence) $\alpha = a_1 a_2 \ldots$ is normal base n iff for each m, and any sequence $\sigma \in \{0, \ldots, n-1\}^m$, if $\lim_s \frac{|\{i \leq n | x(i) \ldots x(i+m-1) = \sigma\}|}{n} \to \frac{1}{n^m}$.
2. α is absolutely normal iff α is normal to every base $n \geq 2$.

- E.g. The Champernowne number .0123456789101112... is normal base 10. Is it normal base 2?
- Borel observed that almost every real is absolutely normal.
- Lebesgue and Sierpinskyg gave an explicit "constructions" of an absolutely normal number.
- Widely believed that e, π, and any algebraic irrational is absolutely normal. None proven normal to any base.

- We now know that (Schnorr and Stimm) that normality is algorithmic randomness relative to finite state machines.... more on this story later.

Three Approaches to Randomness at an Intuitive Level

- The statistician's approach: Deal directly with rare patterns using measure theory. Random sequences should not have effectively rare properties. (von Mises, 1919, finally Martin-Löf 1966)
- Computably generated null sets represent effective statistical tests.
- The coder's approach: Rare patterns can be used to compress information. Random sequences should not be compressible (i.e., easily describable) (Kolmogorov, Levin, Chaitin 1960-1970's).
- Kolomogorov complexity; the complexity of σ is the length of the shortest description of σ.
- The gambler's approach: A betting strategy can exploit rare patterns. Random sequences should be unpredictable. (Solomonoff, 1961, Scnhorr, 1975, Levin 1970)
- No effective martingale (betting) can make an infinite amount betting of the bits.

The statisticians approach

- von Mises, 1919. A random sequence should have as many 0's as 1's. But what about 1010101010101010.....
- Indeed, it should be *absolutely normal*.
- von Mises idea: If you select a subsequence $\{a_{f(1)}, a_{f(2)}, \dots\}$ (e.g. $f(1) = 3, f(2) = 10, f(3) = 29,000$, so the 3rd, the 10th, the 29,000 th etc) then the number of 0's and 1's divided by the number of elements selected should end to $\frac{1}{2}$. (Law of Large Numbers)
- But what selection functions should be allowed?
- Church: computable selections.
- Ville, 1939 showed no countable collection for selection possible. Essentially not enough statistical tests.

Ville's Theorem

Theorem (Ville)

Given any countable collection of selection functions, there is a real passing every member of the test yet the number of zero's less than or equal to n in the $A \upharpoonright n$ (the first n bits of the real A) is always less than or equal to the number of 1's.

Martin-Löf

- Martin-Löf, 1966 suggests using shrinking effective null sets as representing effective tests. Basis of modern effective randomness theory.
- For this discussion, use Cantor Space 2^ω.
- We use measure. For example, the event that the sequence begins with 101 has having probability 2^{-3}, which is the measure of the cylinder $[101] = \{101\beta \mid \beta \in 2^\omega\}$.
- The idea is to exclude computably "rare" properties, and interpret this as measure 0.
- For example, each second bit was a 0.
- So we could test $T_1 = \{[00], [10]\}$ first. A real α would not be looking good if $\alpha \in [00]$ or $\alpha \in [10]$ This first "test" had measure $\frac{1}{2}$.
- Then we could test if α is in $T_2 = \{[0000], [0010], [1000], [1010]\}$(having measure $\frac{1}{4}$).
- α fails the test if $\alpha \in \cap_n T_n$.

Martin-Löf tests

- We visualize the most general statistical test as being effectively generated by considerations of this kind. A c.e. set is the output of a computable function.
- A c.e. open set is one of the form $U = \{[\sigma] : \sigma \in W\}$, where W is a c.e. set of strings in $2^{<\omega}$.
- 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* (MLR) if for every Martin-Löf test,

$$\alpha \notin \bigcap_{i>0} U_i.$$

Universal Tests

- Enumerate all c.e. tests, $\{W_{e,j,s} : e, j, s \in \mathbb{N}\}$, stopping should one threatened 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)

The Coder's Approach

- Have a Turing machine $U(\tau) = \sigma$ is a U-description of σ. The length of the shortest τ is the Kolmogorov Complexity of σ relative to U. $C_U(\sigma)$.
- There are universal machines in the sense that for all M, $C_U(\sigma) \leq_C^K (\sigma) =_{\text{def}} K_M(\sigma) + d_m$. We write C for this.
- We think of strings as being C-random if $C(\sigma) \geq |\sigma|$. The only way to describe σ is to hard code it. It lacks exploitable regularities.
- For example "write 101010 100 times" is a short description of a long string.

reals

- From this point of view we should have all the initial segments of a real to be random.
- First try α, a real, is random iff for all n, $C(\alpha \upharpoonright n) \geq n - d$.
- Complexity oscillations: Take a very long string. It will contain an initial segment $\sigma\tau$ where $|\tau|$ is a code for σ, e.g. in the Ilex ordering. So that τ is a C-description of $\sigma\tau$.
- By complexity oscillations no random real so described can exist. The reason as is that C lacks the intentional meaning of Kolmogorov complexity. This meaning is that the bits of τ encode the information of the bits of σ. Because C really uses $\tau + |\tau|$ as we know it halts there.

Prefix free complexity

- K is the same except we use prefix-free complexity (Think telephone numbers.) i.e. $U(\tau)$ halts implies $U(\tau')$ does not for all τ comparable (but not equal to) τ.
- (Levin, later Schnorr and Chaitin) Now define α is K-random if there is a c s.t.

$$\forall n(K(\alpha \upharpoonright n) > n - c).$$

And...

- They all give the same class of randoms!

Theorem (Schnorr)

A is Martin-Löf random iff A is K-random.

- It is possible that $\exists^\infty n C(X \upharpoonright n) =^+ n$, for some real X.

Theorem (Nies, Stephan, and Terwijn, Nies)

Such reals are exactly the 2-randoms.

- Here A is n-random iff A is random relative to $\emptyset^{(n)}$. Thus, by e.g. the relatives Schnorr theorem, $K^{\emptyset^{(n)}}(A \upharpoonright n) \geq^+ n$ for all n.
- Amazingly, n-randoms are all definable in terms of K and C. (Bienvenu, Muchnick, Shen, Vereshchagin)

- Similar ideas using martingales were you bet on the nest bit. A is random iff no "effective" martingale succeeds in achieving infinite winnings betting on the bits of A.
- $f(\sigma) = \frac{f(\sigma 0)+f(\sigma 1)}{2}$. (fairness)
- Many variations depending of sensitivity of the tests. Implementations approximate the truth: ZIP, GZIP, RAR and other text compression programmes.
- Notice no claims about randomness "in nature" But very interesting question as to e.g. how much is needed for physics etc.
- We have given up on a metaphysical notion of randomness, but only have a notion determined by the complexity of the tests. Stronger tests mean "more random".
- Interesting experiments can be done. E.g. ants. (or children) (Reznikova and Yu, 1986)

Turing, around 1938

- Borel asked for an explicit example of an absolutely normal number.
- Turing interpreted this to mean a construction of a computable real; one with a computably converging Cauchy sequence.

> *Although it is known that almost all numbers are [absolutely] normal no example of [an absolutely] normal number has ever been given. I pro- pose to show how [absolutely] normal numbers may be constructed and to prove that almost all numbers are [absolutely] normal constructively.*

- Turing invented Martin-Löf type tests of sufficient sensitivity to test for absolute normality, but coarse enough to all a computable real to pass.

- Jack Lutz (Cambridge 2012, Turing Year)

  Placing computability constraints on a nonconstructive theory like Lebesgue measure seems a priori to weaken the theory, but it may strengthen the theory for some purposes. This vision is crucial for present-day investigations of individual random sequences, dimensions of individual sequences, measure and category in complexity classes, etc.

- So Turing had the machinery to be able to generate the theory of algorithmic randomness.
- We might speculate why he did not do this.
- We have already seen that he though of randomness as a physical phenomenom.
- Certainly he recognized that difficulty of recognizing randomness from predictability:

> *" It is not normally possible to determine from observing a machine whether it has a random element, for a similar effect can be produced by such devices as making choices depend on the digits of the decimal for π. "*

- It is clear that Turing regarded randomness as a computational resource. For example, in artificial intelligence Turing consider learning algorithms. Turing says in

  > *"It is probably wise to include a random element in a learning machine.... A random element is rather useful when searching for the solution of some problem."*

- Turing then gives an example of search for the solution to some numerical problem, pointing out that if we do this systematically, we will often have a lot of overhead corresponding to our previous searches. However, if the problem has solutions reasonably densely in the sample space random methods should succeed.
- Actually, you can buy hardware randomness: Based on belief that Quantum Mechanics delivers "true randomness"
- Even Swiss-made: Quandis Random Number Generator

Normality, again

- Schnorr and Stimm used martingales generated by automata, and we see α is normal base d if no automata based martingale can succeed on it.
- Hence, exponential time contains absolutely normal reals.
- Much work here by Mayordomo, Becher, Slaman, Bugeaud, Heiber, we know that these examples can be in time $n \log n$ (for the n-th bit in binary) and have deep relationships with Diophantine approximation, discrepancies etc.
- This is an area of significant recent progress, see Veronica Becher's home page for some references.

Some other recent themes

- What is "random"? What level of randomness is necessary for applications.
- Suppose I have a source of weak randomness, how can I amplify this to get better randomness?
- 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? If a real is random does it have strong or weak computational power?
- Can we use computational randomness to give classical results; or at least insight into classical theorems?

Randoms should be computationally weak

- We now know that there are two kinds of randoms, those which resemble Chaitin's $\Omega = \sum_\sigma 2^{-K(\sigma)}$ and more typical ones.
- There has been a lot of popular press about the "number of knowledge" etc, which is random, but has high computational power.
- We would theorize randoms would be stupid: computationally weak.
- However

Theorem (Kucera-Gacs)

If X is an set, there is a MLR real Y with $X \leq_T Y$.

Smart randoms are rare

- Stupidity Tests
- There are two ways to convince someone you are stupid:
- The first are random as they pass the stupidity test as they are so smart that they know how to be stupid, the second really are stupid.

Theorem (Stephan)

A random real can compute a DNC function (we say the real has PA degree) iff A computes the halting problem.

- f is DNC iff for all x, $f(x) \neq \varphi_x(x)$, and $f(x) \in \{0, 1\}$.

Theorem (Barmpalias, Lewis, Ng)

Every PA degree is the join of two random degrees.

- But if a real Y is 2-random, then already it cannot have any information in commong with the halting problem. (Specifically, their Turing degrees form a minimal pair.)

Halting probabilities

- One would think therefore that Ω has nothing to do with most randoms, but:

Theorem (Downey, Hirschfeldt, Miller, Nies)

Almost every random A is Ω^B for some B.

- One would think that the fact that Ω is of computably enumerable degree is rare, but, again:

Theorem (Kurtz)

Almost every random A is computably enumerable relative to some $B <_T A$.

Initial segment complexity

- Lots of work relating initial segment Kolmogorov complexity and algorithmic complexity.
- an order is a computable nondecreasing function h with infinite limit. We say that A is complex if there is an order h such that $C(A \upharpoonright n) \geq h(n)$ for all n.

Theorem (Kjos-Hanssen, Merkle, Stephan)

A is complex iff there is a DNC function $f \leq_{tt} A$.

- A very striking set of results were on an amazing natural class of reals called "K" trivials.

K-Trivials

Theorem (Chaitin)

If $C(A \upharpoonright n) \leq^+ C(n)$ for all n, then A is computable.

- This is proven using the fact that a Π^0_1 class with a finite number of paths has computable paths, combined with the Counting Theorem $\{\sigma : C(\sigma) \leq C(n) + d \wedge |\sigma| = n\} \leq A2^d$.
- What is $K(A \upharpoonright n) \leq^+ K(n)$ for all n? We call such reals K-trivial. Does A K-trivial imply A computable?
- Chaitin proved that the K-trivials are all Δ^0_2. (I.e. computable from the halting problem.)

K-triviality

Theorem (Solovay, 1975, unpubl)

There are noncomputable K-trivial reals.

- Let t be any function dominating all primitive recursive functions, or at least the overhead in the Recursion Theorem. We define a computably enumerable set:
- Put x into $A_{t(s+1)} - A_{t(s)}$ if it is the least z with $K_{t(s+1)}(z) \neq K_{t(s)}(z)$.

Theorem (Downey, Hirschfeldt, Nies, Stephan)

1. *B is K-trivial and noncomputable implies $\emptyset <_T B <_T \emptyset'$,*
2. *and hence the A above solves Post's problem.*

- That is, an injury and requirement free solution to Post's Problem.

K-Trivials

- Proven to be an amazing class.

Theorem

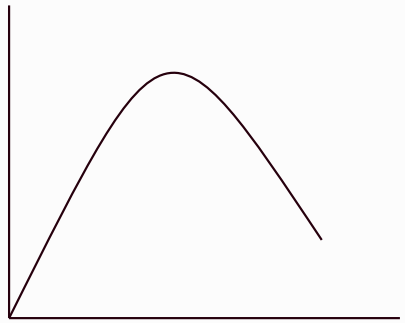
The following are equivalent.

1. *A is K-trivial.*
2. *A is low for ML randomness, MLR^A=MLR (Nies)*
3. *A is low for K, $K^A =^+ K$ (up to a constant). (Nies and Hirschfeldt)*
4. *$A \leq_T B$ with B MLR relative to A (Nies and Stephan)*

- (Nies) There are only a countable number of K-trivials, they are each computable from an incomplete K-trivial c.e. set. They are all superlow. (i.e. $A' \equiv_{tt} \emptyset'$)
- So they are essentially and enumerable phenomenon. This means they cannot be constructed from forcing, for instance.

Computational power

Heuristic graph, horizontal axis represents randomness and verticical useful information content (computational power)



Some applications

- Famously, Chaitin showed proved the First Incompleteness Theorem using K-complexity.

Theorem (Chaitin)

For any sufficiently strong, computably axiomatizable, consistent theory T, there is a number c such that T cannot prove that $C(\sigma) > c$ for any given string σ. (This also follows by interpreting an earlier result of Barzdins, see Li-Vitanyi.)

- Kritchman and Raz (2010) used such methods to give a proof of the Second Incompleteness Theorem as well. (Their paper also includes an account of Chaitin's proof.)
- We could ask could we improve proof theoretical power by adding randomness: Bienvenu, Romashchenko, Shen, Taveneaux, and Vermeeren showed that the answer is no.

Complexity

- Things seem different if we have a source of random strings when we consider running times:
- Bienvenu and Downey (STACS 2018) showed that a random source will *always* speed up some computation in exponential time. (Specifically, a Schnorr random is never "low for speed").
- (For those who know what genericity is) Interestingly, for category the answer depends on whether $P \neq NP$. Bayer (2012) showed that if $P = NP$ every 2-generic is LFS, and if $P \neq NP$ no 1-generic is.
- Sometimes, complexity assumptions are needed: Bienvenu, Romashchenko, Shen, Taveneaux, and Vermeeren showed that if $P \neq PSPACE$ then additional axioms asserting certain certain strings are random does make proofs much shorter.
- Many questions related to whether $BPP = P$?, e.g. polynomial identity testing.

Applications of Kolmogorov complexity

- There are many coming from incompressibility method
- Algorithmically random strings should exhibit typical behaviour on computable processes.
- Give average running times for sorting, by showing that if the outcome is not what we would expect we can compress a random input (which is now a single algorithmically random string).
- Li-Vitanyi, Ch. 6 is completely devoted to this technique applying it to areas as diverse as combinatorics, formal languages, compact routing, circuit complexity and many others.

Mutual information

- $C(x|y)$ of a string x given y as an oracle is an absolute measure of how complex x is in y's opinion.
- Hence comparing two sequences x, y of e.g. DNA, or two phylogenic trees, or two languages, or two bits of music, "Google" distance, we have invented many distance metrics such as "maximum parsimony" in the DNA example. But it is natural to use a measure like $\max\{C(x,y), C(y,x)\}$, if the have the same length, or some normalized version if they don't.
- Then we know absolutely what information the strings
- Use compression packages in practice.

High up Low down

Allender and others began a program under the idea that random oracles can't be useful under efficient reductions..

Theorem (Buhrman, Fortnow, Koucký and Loff; Allender, Buhrman, Koucký, van Melkebeek and Ronneburger 2006; Allender, Buhrman and Koucký 2006)

Let R be the set of all random strings for either plain or prefix-free complexity. (i.e. $R = \{x \mid C(x) > |x| - 1\}$ for example.)

- $\mathrm{BPP} \subseteq \mathrm{P}^R_{tt}$.
- $\mathrm{PSPACE} \subseteq \mathrm{P}^R$.
- $\mathrm{NEXP} \subseteq \mathrm{NP}^R$.

In this tt refers to truth-table (non-adaptive) reductions.

Theorem (Allender, Friedman and Gasarch)

- $\Delta_1^0 \cap \bigcap_U \mathrm{P}_{tt}^{R_{K_U}} \subseteq \mathrm{PSPACE}$.
- $\Delta_1^0 \cap \bigcap_U \mathrm{NP}^{R_{K_U}} \subseteq \mathrm{EXPSPACE}$. *Here U ranges over universal prefix-free machines, K_U is prefix-free complexity as determined by U, and R_{K_U} is the corresponding set of random strings.*

Theorem (Cai,D,Epstein,Lempp,Miller)

For any universal U there is a noncomputable set $X \not\leq_{tt} R_K^U$. Hence if $X \leq_{tt}$ all R_K^V's it is computable. So the "$\Delta_1^0\cap$" can be removed.

Computable Analysis

- Roots go back to Turing's original paper!

Definition (Kleene, essentially)

f is computable it there is a uniform algorithm taking fast converging Cauchy sequences (i.e. $q_k \in B(q_n, 2^{-n})$ for all $k > n$) to fast converging Cauchy sequences.

(This is in, e.g., a separable metric space with a countable computable base, like the reals and the base $\mathbb{Q}$.)

- In fact "f continuous" $=$ "f computable relative to an oracle".

Theorem (Pour-E and Richards)

In this setting an operator is computable iff it is bounded.

- Thus there is a computable ODE with computable initial conditions but no computable solution. (Myhill)

- Some things are perhaps surprisingly computable. For example, the graph G of a computable function on a closed interval is computable as a set, in the sense that the distance function $d(x, G)$ is computable from it.
- It is also possible to look at effective L^p-computability, Fine computability, ...
- New initiatives in computable structures in Polish spaces, e.g. Pontryagin duality. (Melnikov, etc)

Derivatives

- If you look at e.g. the Dini derivative the correct way, then it looks like a martingale. This observation was by Demuth.

Theorem (Demuth-Brattka, Miller, Nies-TAMS)

A computable f of bounded variation is differentiable at each Martin-Löf random set, and this is tight.

- That is "differentiable=random"
- Westrick has shown that the differentiation/continuity hierarchy aligns exactly with the arithmetic/analytic hierarchy.
- Lots of new work on computational aspect of Ergodic Theorems, Brownian motion and the like. But no time.
- Think about the "almost everywhere" behaviour you have seen...

Dimensions

- There have been a lot of interesting applications of algorithmic randomness to classical areas; particularly Ergodic theory, sofic shifts (i.e. iterative systems whose actions will be computable, entropies correspond to halting probabilities), and understanding levels of randomness necessary for almost everywhere behaviour in analysis. Here is one nice example

Theorem (Hochman and Meyerovitch)

The values of entropies of subshifts of finite type over $\mathbb{Z}^d$ for $d \geq 2$ are exactly the complements of halting probabilities.

- (Specifically) V is finite set, and $V^{\mathbb{Z}}$ with the shift operator T, acting with $(T(\mathbf{x})) = x_{j+1}$.
- A subshift is a subspace of the full shift space and has finite type if it is characterized by a finite transition matrix. ("Markov" shift)
- Lots of work relating to Sofic subshifts characterized by forbidden strings being a regular language.

Dimensions

- But I will finish with one nice example: algorithmic dimension.
- Classically points have dimension 0, lines 1, etc.
- Beginning with Hausdorff use a modification of outer measure to define fractions dimension. E.g. the Koch curve has Hausdorff dimension $\log_3(4)$.
- For Hausdorff dimension use a modified notion of outer measure to refine measure 0, e.g. on the line. ($[\sigma]$ counts for $2^{(1-s)|\sigma|}$, with $0 \leq s < 1$.
- Packing dimension using inner measure.
- Huge amount of modern mathematics and lots of attractive pictures.

- Jack Lutz in the early 2000's discovered there are
  1. natural definitions of effective dimensions initial segment Kolmogorov complexity (Lutz, Mayordomo)
  2. in many situations, tight relationships between effective dimensions and classical dimensions. (Hitchcock, Lutz and Lutz)
- The "point to set" principles allow for proving results about classical dimensions using effective dimensions of individual sequences.

Effective dimensions

- Replace each second bit of a random sequence by a 1. The result is "$\frac{1}{2}$ random": Think of $\frac{K(X\upharpoonright n)}{n}$ as a measure of the "partial randomness" of X.
- Look at

$$\liminf_{n\to\infty} \frac{K(X \upharpoonright n)}{n} \qquad \text{and} \qquad \limsup_{n\to\infty} \frac{K(X \upharpoonright n)}{n},$$

- The first above is the effective Hausdorff dimension, dim and the second effective packing dimension. Dim.
- Using relativizations, for a set $\mathcal{S}$ the classical e.g. Hausdorff dimension is also

$$\min\{\dim^Y(X) \mid X \in \mathcal{S} \wedge Y \in 2^\omega\}.$$

Examples

- In the setting of "topological entropy" Simpson proved that the classical dimension equals the entropy (generalizing a difficult result of Furstenburg 1967) using effective methods.
- Day gave a new proof of the Kolmogorov-Sinai Theorem classifying Ergodic systems for Bernoulli measures in terms of Shannon entropy using effective packing dimension.
- Lutz and Lutz and Lutz and Stull gave new simpler proofs and proved new theorems in fractal geometry.
- This is an area in its infancy.

Randomness amplification

- Can randomness be extracted from a partially random source?
- We can use dimensions to measure the partial randomness in our setting.
- Fortnow, Hitchcock, Pavan, Vinochandran, and Wang showed that if X has nonzero effective packing dimension and $\varepsilon > 0$, then there is a Y that is (poly time) computable from X such that the effective packing dimension of Y is at least $1 - \varepsilon$.
- Joe Miller showed that this not true for Hausdorff dimension. There are Turing degrees with of dimension $\frac{1}{2}$ for example.
- Zimand showed two independent sources are enough for Hausdorff dimension.
- Nevertheless, we feel that a real of Hausdorff dimension 1 should be somehow close to a random.
- In exciting recent work, Greenberg, Miller, Shen, and Westrick showed that if $\dim(X) = 1$, then there is a MLR Y with the density of $S = (X \setminus Y) \cup (Y \setminus X)$ equal to 0. (i.e. $\lim_{n\to\infty} \frac{|S\upharpoonright n|}{n} = 0$)

Want to know more?

- My homepage : just type Rod Downey into google.
- and I am the one who is not the author of gay Lolita.