Algorithmic Randomness and Computability

Rod Downey
Victoria University
Wellington
New Zealand

References

- van Lambalgen's Thesis, Solovay's unpublished notes, and Li-Vitanyi Also new book "to appear" by Downey and Hirschfeldt prelim version on my home page, and one by Nies available (maybe) if you ask him.
- Calibrating Randomness (with Hirschfeldt, Nies and Terwijn) for BSL.
- Five Lectures on Algorithm Randomness, to appear Proceedings Computational prospects of Infinity
- Some Computability-Theoretical Aspects of Reals and Randomness, in The Notre Dame Lectures
- `www.mcs.vuw.ac.nz/research/math-pubs.shtml`

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.

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 $\mu([\sigma]) = 2^{-|\sigma|}$.
- Strings = members of $2^{<\omega} = \{0,1\}^*$.
- There are theories for more general spaces, notably by Gács, (see his web site), but this is still under development.

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 $\mu([\sigma]) = 2^{-|\sigma|}$.
- Strings = members of $2^{<\omega} = \{0,1\}^*$.
- There are theories for more general spaces, notably by Gács, (see his web site), but this is still under development.

Computability Theory

- "Computable" means $f(n)$ can be computed (in theory) by a machine.
- Objects coded as members of $\mathbb{N}$.
- $A \subseteq \mathbb{N}$ is computable means there is an algorithm to decide $n \in A$? uniformly. $\chi_A(n)$ computable.
- A is computably enumerable means $A = \{f(0), f(1), \dots\}$.
- Halting problem $\{\langle x, y\rangle : \varphi_x(y) \text{ halts } \}$ is famously c.e. but not computable.

THREE VIEWS OF EFFECTIVE RANDOMNESS FOR REALS

1. Measure-Theoretical:
   - Random means no distinguishing features. (Think of a statistical test as generating a set of tests: considered as open sets.)
   - 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 the statistician 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.

Richard von Mises:

- Actually, the first attempt to "define" randomness was by the statistician 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.. In 2^ω, $U = \{[\sigma] : \sigma \in W\}$.
- 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)

DEFINITION

α is Martin-Löf random 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 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)

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)

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)

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)

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 string σ 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, $C_U(\sigma) \leq C_N(\sigma) + d$.
- Kolmogorov showed that universal machines exist. 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 $C(\tau) \leq M_e(\tau) + e + 1$.

- A string σ 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, $C_U(\sigma) \leq C_N(\sigma) + d$.
- Kolmogorov showed that universal machines exist. 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 $C(\tau) \leq M_e(\tau) + e + 1$.

THEOREM (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.

THEOREM (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, $C(\alpha \upharpoonright n) \geq n - d$.

THEOREM (MARTIN-LÖF)

NO such real exist!

- Why? Take any α. Then, as a string $\alpha \upharpoonright n$ corresponds to some number which we can interpret as a string using llex ordering: $\alpha \upharpoonright n$ 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 $\alpha \upharpoonright n$.
- The output would be much longer, and would be $\alpha \upharpoonright m + n$, with input having length m. Thus $C(\alpha \upharpoonright m + n) < m + n - O(1)$.
- This phenomenom 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, Schnorr, Chaitin.
- Computers have alphabet $\{0, 1\}$.

DEFINITION

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.

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

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

- Fix a universal prefix-free machine M.

K-RANDOMNESS:

- Prefix freeness gets rid of the use of length as extra information:

DEFINITION
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 $|\sigma| = n$.

THEOREM (COUNTING THEOREM-CHAITIN)

$|\{\tau : |\tau| = n \wedge K(\tau) \leq n + K(n) - c\}| \leq 2^{n-c+O(1)}$.

DEFINITION (LEVIN, SCHNORR, CHAITIN)

A real 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)

K-random $\iff$ *Martin-Löf random.*

So we know that we are on a reasonable idea since the notions coincide.

The proof and Kraft-Chaitin

Theorem (Kraft Computable, Levin, Schnorr, Pippinger)

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

(II) *(*Kraft-Chaitin*) Let $d_1, d_2, \cdots$ be a computably enumerable collection of lengths (possibly with repetitions), with targets σ_i, called an axiom $\langle d_i, \sigma_i\rangle$. Then $\sum 2^{-d_i} \leq 1$ iff we can compute a prefix-free machine M with domain members τ_i and $|\tau_i| = d_i$, and $M(\tau_i) = \sigma_i$.*

LOTS OF RANDOM REALS

- $\mu\{A : A \text{ random } \} = 1$.
- 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

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 proved the following consequence:

Theorem (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 $K(\alpha \upharpoonright m) > m + f(m) - O(1)$.

Extending Schnorr's Theorem

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 proved the following consequence:

Theorem (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 $K(\alpha \upharpoonright m) > m + f(m) - O(1)$.

Extending Schnorr's Theorem

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 proved the following consequence:

Theorem (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, $M(\sigma)\downarrow[s]$.

Definition (Levin)

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.

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

- If strings to strings, you get Schnorr's process complexity.

THEOREM (LEVIN, SCHNORR)

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

Left Computably enumerable reals:

Definition

α is left 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.

Definition (Turing)

α is computable if there is a computable f s.t.

$$\forall n(\alpha - q_{f(n)} < 2^{-n}).$$

- Being a left c.e. real is not the same as being the characteristic function of a c.e. set. (Soare)

Left Computably enumerable reals:

Definition

α is left 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.

Definition (Turing)

α is computable if there is a computable f s.t.

$$\forall n(\alpha - q_{f(n)} < 2^{-n}).$$

- Being a left c.e. real is not the same as being the characteristic function of a c.e. set. (Soare)

CHAITIN'S Ω

- The most famous left c.e. real is

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

  the "halting probability."
- Left 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.

THEOREM (CHAITIN)

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 $\Omega \upharpoonright n \neq \Omega_s \upharpoonright n$.

THEOREM (CHAITIN)

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 $\Omega \upharpoonright n \neq \Omega_s \upharpoonright n$.

Plain Complexity again

- 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

Plain Complexity again

- 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 complexity a string of length n can have is
  (I) $C(\sigma) = n - O(1)$.
  (II) $K(\sigma) = n + K(n) - O(1)$.

THEOREM (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 $C(n) \geq n - O(1)$.

THEOREM (SOLOVAY)

Strongly Chaitin random and hence Kolmogorov random reals exist.

- Fundamental question: are they the same?

- The maximum complexity a string of length n can have is
  (I) $C(\sigma) = n - O(1)$.
  (II) $K(\sigma) = n + K(n) - O(1)$.

THEOREM (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 $C(n) \geq n - O(1)$.

THEOREM (SOLOVAY)

Strongly Chaitin random and hence Kolmogorov random reals exist.

- Fundamental question: are they the same?

- The maximum complexity a string of length n can have is
  (I) $C(\sigma) = n - O(1)$.
  (II) $K(\sigma) = n + K(n) - O(1)$.

THEOREM (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 $C(n) \geq n - O(1)$.

THEOREM (SOLOVAY)

Strongly Chaitin random and hence Kolmogorov random reals exist.

- Fundamental question: are they the same?

n-RANDOMNESS

- This "all" relativizes, so we can define Martin-Löf randomness relative to a set B, and n-randomness relative to $\emptyset^{(n-1)}$ which, due to the work of Kurtz, is the same as randomness for tests with Σ^0_n classes as tests.
- Thus, we can define 2-randomness as 1-randomness relative to the halting problem.

KOLMOGOROV RANDOMNESS

THEOREM (NIES-TERWIJN-STEPHAN, MILLER)

2-randomness=Kolmogorov randomness.

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

- (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.

1-RANDOMNESS AND PLAIN COMPLEXITY

- There is 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 $g : \omega \to \omega$ 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.

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.

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.

- The idea is that if we can characterize randomness by initial segment complexity, then we oght to be able to calibrate randomness by comparing initial segment complexities.

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 $q < \beta$

$$\varphi(q) \downarrow \wedge\, d(\beta - q) > |\alpha - \varphi(q)|.$$

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 $|\sigma - \tau| < 2^{-n+d}$, $K(\sigma) + c > K(\tau)$.

ONLY ONE RANDOM C.E. REAL

- 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 $K(\Omega \upharpoonright n)$ 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 $K(\Omega \upharpoonright n)$ 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.

KUČERA-SLAMAN THEOREM

THEOREM (KUČERA-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.)

KUČERA-SLAMAN THEOREM

THEOREM (KUČERA-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.)

Structure

- The c.e. reals using $\leq_S$ forms a upper semilattice, called the Solovay degrees.

Theorem (Downey, Hirschfeldt, Nies)

(I) *+ induces a join*
(II) *It is distributive*
(III) *dense*
(IV) [Ω] *is the only join inaccessible element.*

THEOREM (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 $\leq_K$

- Define $A \leq_K B$ to mean $K(A \upharpoonright n) \leq K(B \upharpoonright n) + O(1)$, all n.

Theorem (Yu, Ding, Downey)

$\mu(\{B : B \leq_K A\}) = 0$. Hence uncountably many K degrees.

- Yu, Ding In fact $2^{\aleph_0}$.

Theorem (Miller and Yu)

For almost all pairs $A|_K B$.

Theorem (Miller and Yu)

For all $n \neq m$, $\Omega^{(n)}|_K \Omega^{(m)}$.

Theorem (Miller and Yu)

However, there are random A, B with $B <_K A$.

- (Miller and Yu) Each K-degree of a random countable.
- (Miller) There is an uncountable K-degree.
- (Csima and Montalbán) There are minimal pairs of K-degrees.

K-TRIVIAL REALS:

- (Solovay) There exist noncomputable reals α such that for all n
$$K(\alpha \upharpoonright n) \leq K(1^n) + c.$$
- These are called K-trivial reals.
- Note that Chaitin proved that if $K(\alpha) \leq K(1^n) + c$, then α is Δ^0_2. It was earlier proven by Chaitin using a technique of Loveland that
$C(\alpha \upharpoonright n) \leq C(1^n) + c$ for all n, implies α is computable.

- Such A can be c.e. sets. (Zambella, then DHNS, and others)
- Solovay's 1974 proof is very complicated. Here is a simplified version proving a stronger result.
- (DHNS) There is a c.e. noncomputable set A such that for all n

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

- Let

$$A_{s+1} = A_s \cup \{x : W_{e,s} \cap A_s = \emptyset \wedge x \in W_{e,s}$$
$$\wedge \sum_{x \leq j \leq s} 2^{-K(1^j)[s]} < 2^{-(e+1)}\}.$$

THEOREM (DOWNEY, HIRSCHFELDT, NIES AND STEPHAN)
K-trivial reals are never of high degree, so this is an injury free solution to Post's problem.

Nies Theorems

- Every K-trivial is bounded by a K-trivial c.e. set.
- Every K-low is superlow, and "tracable". (and hence (Chaitin) there are only countably many.)
- (Nies and Hirschfeldt) K-trivial = low for K.
- K-trivials are closed under T-reducibility and form the only known natural Σ^0_3 ideal in the Turing degrees.
- The are bounded above by a low_2 degree.

Other classes

- K-trivials also correspond to other classes.

Theorem (Downey, Nies, Weber, Yu+Miller, Nies)

They are exactly the same as the reals low for weak 2-randomness...Randomness for generalized Martin-Löf tests, where $U_n \to 0$ but no effective convergence.

Theorem (Miller, Nies, Stephan)

They are the same as reals A such that there is an A-random B with $A \leq_T B$.

- Related to reals X with $X + R \geq_T \emptyset'$ for soem random R. (Nies)
- (Nies) They are all "jump traceable".

THEOREM (CHOLAK, DOWNEY, GREENBERG)

The strongly jump traceable c.e. reals are a proper subclass of the K-trivials, the first such defined by a cost function construction.

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.
- Also the Kučera-Gács Theorem that each real is computable in a random one suggest computational power.
- Stephan has shown that if $\mathbf{a}$ is a Turing degree containing a 1-random real which has enough information to compute a $\{0,1\}$ valued diagonal function then $\mathbf{a} \geq \mathbf{0}'$. (If $\mathbf{a}$ is 1-random and PA then $\mathbf{0}' \leq \mathbf{a}$.)

- Miller proved the following remarkable 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.

THEOREM (MILLER)

α is random and pseudo-low if α is 3-random.

- (Miller and Yu) 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.

Halting Probability

- Look at Ω^A as an operator.
- Care is needed as to exactly what this means.
- Note this is CE but not CEA.
- e.g. $\Omega|_T\Omega^\Omega$, indeed they form a minimal pair.
- Hoped to solve Martin's conjecture

Theorem (Downey, Hirschfeldt, Miller, Nies)

Alas there are $A =^* B$ such that Ω^A and Ω^B are relatively random and hence Turing incomparible.

Theorem (Downey, Hirschfeldt, Miller, Nies)

Every 2-random is Ω^B for some B. (so maybe ce reals are not red herrings)

- Compare with Kurtz's Theorem : every 2-random is properly CEA.

- many oher intersting results: eg
- Omega operators are lower semicontinuous but not continuous, and moreover, that they are continuous exactly at the 1-generic reals.

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 $\limsup_n F(\alpha \upharpoonright n) \to \infty$.
- 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 succeeds on it. Here F above should have a computable sequence of approximations $F_s \to F$.

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

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

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* $F\}$.

- The d is is effective Hausdorff dimension.
- Lutz says the following:
  "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."

Theorem (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 $\frac{K(\alpha\upharpoonright n}{n}$,
- equivalently, the infimum over all s of the values of $d^s(\alpha \upharpoonright n)$.
- 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 $\rightarrow \infty$ 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

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

  Here $\square$ 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

THEOREM (LUTZ)

There is a constant $c \in \mathbb{N}$ *such that for all* $\sigma \in 2^{<\omega}$,

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

Some ignored material

- The Russian school's work on random strings.
- Time/space bounded Komogorov complexity.
- work on Schnorr, computable and other randomness notions.
- especially the beautiful lowness material of Kučera-Terwijn-Zambella, and of Nies.
- Stochasiticity and Miller, Nies, Stephan, Merkle, etc
- complexity of c.e. sets and Kummer, Muchnik.

- Thank you.