

Computability and Randomness

George Barmpalias

Victoria University of Wellington

UNT, March 4, 2009

Plan of the talk

- ▶ What do we mean by random?
- ▶ How can we formalize it?
- ▶ Using the theory of Computation
- ▶ Algorithmic randomness: Tools and results
- ▶ Interactions with classical computability
- ▶ Applications to Logic, Mathematics and modelling
- ▶ References

When should a binary sequence be called random?

- ▶ 0000000000000000000000000000...
- ▶ 011101011111010101011111101...
- ▶ 01110111111101111111011101111...

Random means . . .

- ▶ no structure or patterns
- ▶ incompressible, should not have short descriptions
- ▶ unpredictable, no betting strategy should succeed on it

0111010111110101010111111101...

- ▶ It has an obvious pattern
- ▶ it is compressible: to describe the first n bits I only need the $n/2$ bits of the odd positions
- ▶ (and an instruction saying to insert a 1 between every two digits)
- ▶ It is predictable: I can make money by betting on the even bits
- ▶ (which I am certain they are 1)

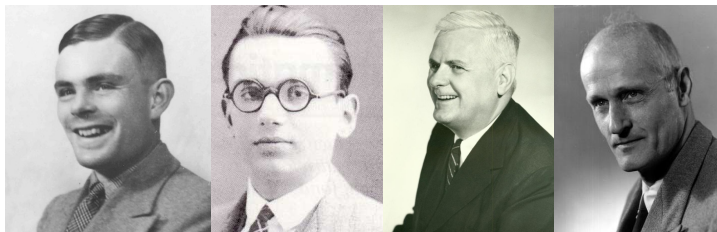
Formalization

- ▶ It is impossible to define absolute randomness
- ▶ (randomness in physics is not what we study)
- ▶ We can define it with respect to a class of compressing procedures, betting strategies, patterns etc.
- ▶ Algorithmic randomness
- ▶ This is based on the theory of computation. . .

Theory of computation

- ▶ What does it mean for a function or a set to be computable?
- ▶ When can we say that a function f can be computed from another function g ?
- ▶ What does it mean for two sets to have the same information?
- ▶ How can we classify the information content of various mathematical objects?

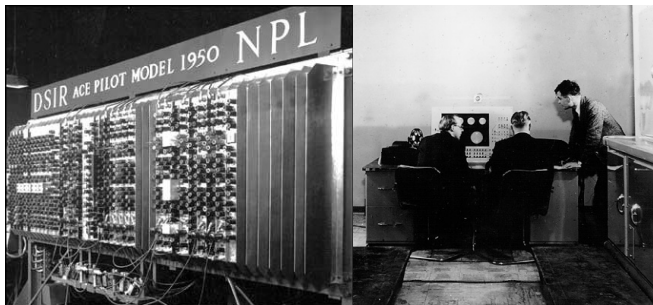
1930s



Algorithms

- ▶ Today everyone knows what computable means!
- ▶ The concept of algorithm existed long before the development of mathematical logic
- ▶ But only it was not until the 1930s when a general mathematical definition was given
- ▶ This provided a rigorous way to measure, compare and classify information
- ▶ Along with that, the concept of a universal machine was conceived

Machines



Classifying information

- ▶ The relation X is computable from Y
- ▶ Oracle Y is thought of as ROM
- ▶ Induces: X has the same information as Y
- ▶ and a natural partial order amongst the equivalence classes
- ▶ This partial order is known as the Degrees of Unsolvability or Turing degrees

Examples of problems

- ▶ Problems are coded into sets and assigned a degree of unsolvability.
- ▶ **Word problem** for finitely presented groups: given a presentation find if a word is the identity
- ▶ **Hilbert's 10th problem**: finding if a diophantine equation has an integer root.
- ▶ **Halting problem**: decide if a given machine halts on a given input

Examples of reductions

- ▶ Given a solution to Hilbert's 10th problem we can solve the word problem of any finitely presented group
- ▶ The halting problem contains the same information as Hilbert's 10th problem

Computationally Enumerable Degrees

- ▶ These problems are **Computationally enumerable**
- ▶ Solutions can be searched via effective procedures (may never halt)
- ▶ A set is computably enumerable if it can be enumerated by a machine.
- ▶ There is a complete c.e. set, one that computes all others.
- ▶ The complete c.e. degree contains many interesting problems.
- ▶ For example, the word problem, Hilbert's 10th problem and the halting problem.

Degrees of Unsolvability

- ▶ There is a **least degree**, containing the computable sets.
- ▶ Upper semi-lattice:
- ▶ $X \oplus Y = \{2n, 2m + 1 \mid n \in X \wedge m \in Y\}$
- ▶ **Countable predecessor property**
- ▶ (Spector) There is a minimal degree

Degrees of Unsolvability \mathcal{D}

- ▶ Have been studied for more than 60 years
- ▶ Very complex structure:
- ▶ Every upper semilattice of size \aleph_1 with the countable predecessor property can be embedded as an initial segment in \mathcal{D} (Abraham-Shore 1986)
- ▶ Beyond this, the problem is independent from ZFC (Slaman, Groszek 1983)

Mathematical Randomness

- ▶ Algorithmic randomness is defined with respect to computable processes of some sort.
- ▶ Randoms should have no structure which is identifiable by some effective procedure
- ▶ Be incompressible, with respect to effective compression
- ▶ Be unpredictable, with respect to effective betting functions
- ▶ Ratio of 1s over all digits should tend to $1/2$

Von Mises 1919

- ▶ **Selection rule** is a function $f : \mathbb{N} \rightarrow \mathbb{N}$ telling use which bits to look at
- ▶ $R_n^f(X) = \frac{\{m < n \mid X(f(m))=1\}}{n}$
- ▶ X is **Von Mises random** if $\lim_n R_n^f(X) = 1/2$ for all 'acceptable' selection rules
- ▶ For any countable set of selection rules, there are Von Mises random sequences (Wald)
- ▶ Ville showed that there are Von Mises random sequences X such that that $\forall n R_n(X) \geq 1/2$
- ▶ ... where $R_n(X) = \frac{\{m < n \mid X(m)=1\}}{n}$

People 1960s



Three approaches to Randomness

- ▶ **The statistician's approach:** Deal directly with rare patterns using measure theory. Random sequences should not have rare properties.
- ▶ **The coder's approach:** Rare patterns can be used to compress information. Random sequences should not be compressible (i.e., easily describable).
- ▶ **The gambler's approach:** A betting strategy can exploit rare patterns. Random sequences should be unpredictable.

Equivalence of methods

- ▶ Use measure, prefix-free machines or martingales (and semi-measures)
- ▶ Equivalence was proved by Schnorr, Chaitin in 1970s

Statistician's approach

- ▶ Martin-Löf in the 1960s
- ▶ A sequence is random if it is not contained in an effectively null G_δ set: $\cap_i U_i$
- ▶ By varying the effectivity requirement on the G_δ set we get stronger or weaker notions of randomness.
- ▶ Applications like `gzip` work by applying similar effective tests on given data

Coder's approach

- ▶ Kolmogorov, Chaitin and Levin in 1960s
- ▶ There is an **optimal (universal) machine** which gives descriptions
- ▶ The **descriptive complexity** of a string σ is the length of its shortest description
- ▶ and is denoted by $K(\sigma)$
- ▶ A sequence X is random if $K(X \upharpoonright n) \geq n - c$ for all n and a constant c
- ▶ To describe the first n bits of the sequence you need to use n bits (modulo a constant)

Relative Randomness

- ▶ Randomness notions relativize to any oracle
- ▶ Thus we can talk about a sequence X being random relative to Y
- ▶ A classic theorem is: $X \oplus Y$ is random iff X is random and Y is X -random
- ▶ Randomness relative to an oracle X refers to sequences whose 'patterns' are beyond the ability of X to recognize
- ▶ In other words, **sequences that are incompressible given information X**
- ▶ Descriptive complexity relative to X is denoted by K^X

A Remarkable Fact

A Remarkable Fact

There are certain non-computable sets that cannot compress better than a computable one.

A Remarkable Fact

There are certain non-computable sets that cannot compress better than a computable one.

*These are known as the **K-trivial** or **low for K** sets:
 $K^A =^+ K$.*

*Solovay 1976, Kummer, Kučera-Terwijn 1999, Nies
(Adv. Math. 2005)*

Kučera's Question, 1999

How many oracles can compress at most as well as a computable oracle?

Generalized Question

Given X , how many oracles compress at most as well as X ?

What is the cardinality of $\{Y \mid \forall \sigma K^X(\sigma) \leq^+ K^Y(\sigma)\}$?

Partial answers

- ▶ It can be either \aleph_0 or 2^{\aleph_0} as the set is Borel
- ▶ If X is computable, then it is \aleph_0 (Nies, 2005)
- ▶ If X sufficiently resembles the halting problem, it is 2^{\aleph_0} (Barnikolas, Lewis, Soskova 2006)
- ▶ If X is sufficiently random (i.e. random relative to the halting problem), it is \aleph_0 (Miller 2007)

Complete Characterization for an Important class

Theorem (Barnali 2007)

For the class of the sets X computable from the halting problem, the answer is

There are uncountably many oracles compressing at most as well as X iff X can compress better than a computable oracle.

Also, in terms of arithmetical complexity, this is the best possible result.

Measuring compression power of oracles

- ▶ If $\forall \sigma K^Y(\sigma) \leq^+ K^X(\sigma)$ we say that **Y has more compressing power than X**
- ▶ Similarly we can formalize **X can compress exactly as efficiently as Y**
- ▶ As with the notion of information, we get a degree structure which classifies oracles according to how well they can compress
- ▶ It is a generalization of Turing degrees
- ▶ An oracle can compress more than the halting problem iff it computes an almost everywhere dominating function (Kjos-Hanssen, Miller 2007)

Comparison of the two theories

Theorem (Barnmpalias 2008)

- ▶ *The Σ_1^0 and Δ_2^0 parts of the two structures are not equivalent.*
- ▶ *In the degrees of compressibility there are no Σ_1^0 or Δ_2^0 minimal pairs.*
- ▶ *The degrees of compressibility resemble the Turing degrees in some ways, but not in others.*

A question of S.G. Simpson and Nies

- ▶ There is a function which dominates all computable functions and has minimal degree (Cooper 1974).
- ▶ Simpson asked:

Is there a function that dominates almost all functions and has minimal degree?
- ▶ The notion of **almost everywhere domination** has played a role in the reverse mathematics of measure theory

Theorem (Barnpalias 2008)

No function of minimal degree can dominate almost all functions.

- ▶ This gives a concrete **separation of the two notions of highness**.
- ▶ The same remains to be done in local structures like the c.e. degrees.
- ▶ This is part of a more general question:
What is the role of almost everywhere domination in the Turing degrees?

An famous random by Chaitin

- ▶ **Halting probability:** $\Omega_U = \sum_{U(\sigma)\downarrow} 2^{-|\sigma|}$
- ▶ Has the same information as the Halting problem
- ▶ but much more compressed
- ▶ Complete randoms behave very differently than incomplete randoms
- ▶ large amounts of information induce order on a sequence
- ▶ **True randoms** should not have too much information

Peano Arithmetic

- ▶ Peano Arithmetic is a foundation for number theory (Peano, Dedekind 1800s)
- ▶ It is famously **undecidable** (Gödel 1931)
- ▶ A **complete model** of PA is one where for every sentence ϕ , either ϕ or $\neg\phi$ is provable
- ▶ a completion, like the algebraic closure of a field

Peano Arithmetic and Randomness

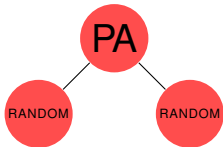
- ▶ Sets that compute a complete extension of Peano Arithmetic are related to random sets (Kučera 1980s)
- ▶ A **true random** does not compute a complete model of Peano Arithmetic (Stephan 2002)
- ▶ Dichotomy of randomness: complete randoms are very different than incomplete randoms
- ▶ Incomplete randoms are low in information
- ▶ However. . .

Peano Arithmetic and joins of randoms

Theorem (Barnmpalias, Lewis, Ng 2008)

Every degree which computes a complete model of Peano Arithmetic is the least upper bound of two random degrees.

Non-randoms and joins of randoms



Future Research

- ▶ What information can be coded into incomplete random sets and how?
- ▶ Incomplete random degrees are poorly understood
- ▶ How exactly do random sequences resemble low information?
- ▶ Effective Hausdorff dimension, packing dimension
- ▶ How about higher randomness and descriptive set theory? (Hjorth, Nies)

Applications to other fields

- ▶ **Differential Geometry:** Soare, Nabutovsky and S. Weinberger have applied the theory of Turing degrees and randomness in the construction of various manifolds that give information on the geometry of Riemannian metrics modulo diffeomorphisms.
- ▶ **Models of Arithmetic** Kučera and Slaman have answered a question of Friedman and A. McAllister on models of Peano Arithmetic and reverse mathematics, using the K-trivial sets.

Applications to other fields

- ▶ **Eff. Model theory:** Khoussainov, Semukhin, and Stephan used Kolmogorov complexity to solve a well-known open question in computable model theory
(Does there exist a computable not \aleph_0 -categorical saturated structure with a unique computable isomorphism type?)
- ▶ **brownian motion, modelling, image compression, thermodynamics etc.** In Li and Vitanyi's *An introduction to Kolmogorov Complexity and its applications*

Applications to other fields

Set theory:

- ▶ Slaman and Reimann have studied randomness relative to any continuous measure

*They showed that the classes of ‘**Never continuously random**’ oracles are countable by a game-theoretic argument using Borel Determinacy*

- ▶ and showed that the result requires Borel determinacy (2008)
- ▶ Thus it needs uncountably many iterations of the power set axiom of ZFC (Friedman 1970s)

Borel relations and automata

- ▶ Computability is in a way a miniaturization of theory of Borel relations
- ▶ Hjorth, Nies, Montalbán and Khoussainov have applied methods and results of Borel relations to the study of automata

References I

- ▶ Barmpalias, Downey, Greenberg, K-trivial degrees and the jump-traceability hierarchy, *Proc. Amer. Math. Soc.* (in press).
- ▶ Barmpalias, Downey, Greenberg, Working with strong reducibilities above totally omega-c.e. and array computable degrees *Trans. Amer. Math. Soc.* (in press).
- ▶ Barmpalias, Lewis, Stephan, Π_1^0 classes, LR degrees and Turing degrees *Ann. Pure Appl. Logic* **156** (2008)
- ▶ Barmpalias, Lewis, Soskova, Randomness, Lowness and Degrees, *J. of Symbolic Logic* **73**, Issue 2 (2008)
- ▶ Webpage: <http://www.mcs.vuw.ac.nz/~georgeb/>

References II

- ▶ Downey, Hirschfeldt, Nies, Terwijn, Calibrating randomness, *Bull. Symbolic Logic* **12** (2006)
- ▶ Nies, Lowness properties and randomness, *Adv. Math.* **197** (2005)
- ▶ Miller, Yu, On initial segment complexity and degrees of randomness, *Trans. Amer. Math. Soc.* **360** (2008)
- ▶ Cholak, Downey, Greenberg, Strong jump-traceability I: the computably enumerable case *Adv. Math.*, **217** (2008)

- ▶ Li-Vitanyi, **An introduction to Kolmogorov Complexity and its applications**, Springer-Verlag
- ▶ Nies, **Computability and Randomness**, Oxford Press
- ▶ Downey and Hirschfeldt, **Algorithmic randomness and complexity**, Springer-Verlag, to appear

Thank you!