Randomness, probabilities and machines

by George Barmpalias and David Dowe

Chinese Academy of Sciences - Monash University

CCR 2015, Heidelberg
Concrete examples of random numbers?

Chaitin (1975) introduced the halting probability of a machine.

Take a universal prefix-free machine $U$.
Feed as input a long stream of random bits until it halts.
The probability that it halts is the halting probability of $U$.

$$\Omega = \sum_{U(\sigma)\downarrow} 2^{-|\sigma|}$$

This is an example of a c.e. 1-random real.
Zvonkin & Levin (1970) had discussed a similar example.

Chaitin (1975) A theory of program size formally identical to information theory.
Zvonkin & Levin (1970) The complexity of finite objects...
Research on Chaitin’s $\Omega$

Halting probability

A machine $U$ halts on a real, if it halts on a prefix of it. The measure of reals on which $U$ halts is $\Omega$.

Plenty of research has been devoted on the study of $\Omega$.

Solovay (1975) Handwritten manuscript related to Chaitin’s work.
Calude, Hertling, Khoussainov & Wang (2001) R. e. reals and Chaitin $\Omega$ numbers
Downey, Hirschfeldt, Miller & Nies (2005) Relativizing Chaitin’s halting probability.

Other examples of random numbers?

Random probabilities stemming from infinite computations:

Becher, Daicz, and Chaitin (2001)
Probability that $U$ prints finitely many symbols is 2-random.

Becher & Chaitin (2002)
Probability that $U$ prints finitely many zeros is 2-random

Becher, Daicz & Chaitin. (2001) A highly random number
Generalized Chaitin numbers

Probability $\Omega_U[X]$ that output belongs to $X$.
Probability $\Omega_U[X,k]$ that output on inputs $> k$ belongs to $X$.

Becher, Figueira, Grigorieff & Miller (2006)
$\Omega_U[X]$ is random but not $n$-random when $X$ is $\Sigma^0_n$-complete

Becher & Grigorieff (2007)
Under stronger universality for $U$, we have that $\Omega_U[X,k]$ is $n$-random, when $X$ is $\Sigma^0_n$-complete and $k$ large.

A real $X$ preserves the universality of $U$ if $\sigma \mapsto U(X \upharpoonright n \ast \sigma)$ is universal for all $n$.

Universality probability of $U$ is the measure of reals that preserve the universality of $U$. 

Wallace (2005) Statistical and Inductive Inference by Minimum Message Length 
Dowe (2008) Foreword re C. S. Wallace (Special issue of the Computer Journal)
Chris Wallace

Wallace is known for his work on \textit{inductive inference} and his approach known as \textit{minimum message length}.

This is different than but comparable to the \textit{minimum description length} approach to inductive inference.

Li & Vitanyi. \textit{An Introduction to Kolmogorov Complexity and Its Applications}
A first observation

**Proposition**

The universality prob. of a universal machine is in $(0, 1)$.

- $K(X \upharpoonright_n) \geq n - c$ for some real $X$ and all $n$
- $N_c = \{\sigma_s\}$ is the c.e. set of strings $\rho$ such that $K(\rho) < n - c$
- At stage $s$ set $M(\sigma_s \ast \tau) := U(\tau)$ for all $\tau$ unless $\sigma_s$ is comparable with some $\sigma_i, i < s$
- $M$ is well-defined and prefix free
- Every string has a $c$-compressible finite extension
- So all $c$-incompressible reals preserve the universality of $M$. 
Next steps

So the universality probability $P_U$ is non-trivial.

How about its arithmetical complexity?

It does not seem to be simpler than $\Pi^0_4$

We found that it is hard to code useful information to $P_U$.

This gave us a hint that it might be very random.

The 4-randomness of $P_U$ would show that it is in $\Pi^0_4 - \Sigma^0_4$. 
Coding a $\Pi_4^0$ set into the machine

Given a $\Sigma_4^0$ set of strings $J$, $e \in \mathbb{N}$ we can construct:

- a prefix-free machine $V$
- a c.e. set of strings $Q$
- a program computing $\mu(Q) < 2^{-e}$

such that:

Reals in the complement of $[Q]$ preserves universality of $V$ exactly when it does not have a prefix in $J$;

The reals in $[Q]$ that preserve $V$-universality have measure that can be $\emptyset^{(3)}$-approximated from above.
The special machine

Let $J$ be a member of the universal $\emptyset^{(3)}$-Martin-Löf test.

Let $V$ be the coded machine given the $\Sigma_4^0$ set of strings $J$.

Then $P_V$ is 4-random.

$P_V$ is the sum of the probabilities conditional on $[Q]$ and $\overline{[Q]}$.

The first one is $\emptyset^{(3)}$-right-c.e.

The second one is 4-random and $\emptyset^{(3)}$-right-c.e.

So the sum is also 4-random and $\emptyset^{(3)}$-right-c.e.
Any universal machine

Let $U$ be a universal prefix-free machine.

Then $P_U = P_V + P_*$ for some $\emptyset^{(3)}$-right-c.e. number $P_*$.

The universality probability of any universal machine is 4-random and $\emptyset^{(3)}$-right-c.e.

By the arithmetical complexity restrictions on highly random sets:

The universality probability of a universal machine is $\Delta^0_5$ but not $\Pi^0_4$ or $\Sigma^0_4$. 
More consequences

Given any universal machine $U$ there exists a universal $V$ such that $P_U + \Omega_V^{(3)} = 1$.

We know that $\Omega_V^{(3)} \oplus \emptyset^{(3)} \equiv_T \emptyset^{(4)}$

and $\Omega_V^{(3)}$ does not compute any non-trivial $\Delta_4^0$ set

The degree of $P_U$ and $\emptyset^{(3)}$ have sup $\emptyset^{(4)}$ and inf $\emptyset$. 
Characterization

The universality probabilities are exactly the 4-random numbers that are right-c.e. relative to $0^{(3)}$.

Downey/Hirschfeldt/Miller/Nies show that

The degree of $\Omega^A_U$ is invariant to the choice of the universal machine $U$ if and only if $A$ is $K$ trivial.

Their methods actually show that

If $A$ is not $K$ trivial, there exist $U, V$ universal such that the degrees of $\Omega^A_U, \Omega^A_V$ are incomparable.
Consequences of characterization

Given any universal machine $V$ there exists a universal $U$ such that $P_U + \Omega_V^{(3)} = 1$.

So using Downey/Hirschfeldt/Miller/Nies

There exist universal $U, V$ such that the degrees of $P_U, P_V$ are incomparable.
Proof of the characterization from the main lemma

Given a $\Sigma^0_4$ set of strings $J$, $e \in \mathbb{N}$ we can construct:

- a prefix-free machine $V$
- a c.e. set of strings $Q$
- a program computing $\mu(Q) < 2^{-e}$

such that:

- Reals in the complement of $[Q]$ preserves universality of $V$ exactly when it does not have a prefix in $J$;
- The reals in $[Q]$ that preserve $V$-universality have measure that can be $\emptyset^{(3)}$-approximated from above.
Given a 4-random $\emptyset^{(3)}$-right-c.e. $\gamma$ we can find a $\Pi_1^0(\emptyset^{(3)})$ class with measure $\gamma$.

Let $\Omega_N$ be a 1-random left c.e. real.

Given a left-c.e. index $c$ of a real $\beta$ we can compute $t$ such that if $\beta < 2^{-c}$ then $t$ is a left-c.e. index of $\Omega_N - \beta$.

This relativizes:

Given a $\emptyset^{(3)}$-right-c.e. index $c$ of a real $\beta$ we can compute $t$ such that if $\beta < 2^{-c}$ then $t$ is a $\emptyset^{(3)}$-right-c.e. index of $1 - \Omega_N^{\emptyset^{(3)}} - \beta$.

This gives a computable function $c \mapsto h(c)$. 
Algorithm on parameters \((i, c)\)

Fix a 4-random and \(\emptyset^{(3)}\)-right-c.e. number \(1 - \Omega_N^{\emptyset^{(3)}}\).
Let \(\gamma_i\) be an effective enumeration of all \(\emptyset^{(3)}\)-right-c.e. reals.

Feed into the lemma a \(\Sigma_1^0(\emptyset^{(3)})\) class with measure \(1 - \gamma_i\), and \(c\).

Get \(V, Q\) and an index \(e\) for approximating the measure \(\beta\) of reals in \(Q\) which preserve \(V\)-universality.

Output \(e\) and output \(h(e)\).

This gives \((i, c) \mapsto f(i, c)\) and \((i, c) \mapsto g(i, c)\).

There is a fixed point \((i, c)\) such that:

(a) \(f(i, c) \simeq c\): \(\beta\) has an index \(c\) such that \(\beta \leq 2^{-c}\);
(b) \(g(i, c) \simeq i\): the reals preserving \(V\)-universality outside \(Q\) have measure \(1 - \Omega_N^{\emptyset^{(3)}} - \beta\).
The machine $V$ of the double fixed-point $(i, c)$

The reals outside $Q$ which preserve $V$-universality have measure

$$1 - \Omega_N^{\emptyset} - \beta.$$ 

The reals inside $Q$ which preserve $V$-universality have measure $\beta$.

Hence the universality probability of $V$ is

$$(1 - \Omega_N^{\emptyset} - \beta) + \beta = 1 - \Omega_N^{\emptyset}.$$
Thank you for your attention!