Random numbers as probabilities of machine behaviour

by George Barmpalias, Douglas Cenzer and Chris Porter

Chinese Academy of Sciences - University of Florida - Drake University

Computability, Randomness and Applications, Luminy 2016

Concrete examples of random numbers?

Chaitin (CH75, 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.

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

This is an example of a c.e. 1-random real.

Zvonkin & Levin (1970) had discussed a similar example.

CH75, A theory of program size formally identical to information theory.

Zvonkin & Levin (1970) The complexity of finite objects...

Research on Chaitin's Ω

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 Ω.

Plenty of research has been devoted on the study of Ω.

Solovay (1975) Handwritten manuscript related to Chaitin's work.

Kucera & Slaman (2001) Randomness and recursive enumerability.

Calude Hertling,Khoussainov,Wang (2001) RE reals and Chaitin Ω numbers

Read Downey & Hirshfeldt (2010) Algorithmic randomness and complexity.

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

Becher & Chaitin (2002) Another Example of Higher Order Randomness.

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 (BFGM

$\Omega_U[X]$ is random but not n-random when X is Σ^0_n-complete

+ & Grigorieff (BG)

Under stronger universality for U, we have that $\Omega_U[X, k]$ is n-random, when X is Σ^0_n-complete and k large.

BFGM (2006) Randomness and halting probabilities.

BG (2007) Random reals a la Chaitin with/without prefix-freeness.

Universality probability

C.S. Wallace (W05) introduced this notion.

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

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

Wallace,Dowe (1999)Minimum Message Length and Kolmogorov Complexity

W05, Statistical and Inductive Inference by Minimum Message Length

Characterization of Universality Probability

Barmpalias and Dowe show that

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

Downey/Hirschfeldt/Miller/Nies (DHMN) show that

The degree of Ω_U^A is invariant to the choice of the universal machine U if and only if A is K trivial.

DHMN (2005) Relativizing Chaitin's halting probability.

Barmpalis & Dowe (2012) Universaility probability of a prefix-free machine.

Probability of certain events

We consider the probability of certain events when a universal oracle machine M runs on a random oracle X.

Here M(X) is a partial function from $\mathbb{N}$ into $\mathbb{N}$.

For example, $\mathrm{INF}(M) = \{X : M(X) \text{ has infinite domain}\}$
The measure of INF(M) is the probability that M(X) has infinite domain.

We show that the measure of INF(M) is a 2-random $0'$-right-c.e. real.

Conversely, every such real is the measure of INF(M) for some universal M.

Other events and machines

We also consider the propertes of totality, cofinality, computability, and completeness of the domain of M(X).

We obtain in this way characterizations of algorithmically random reals in higher randomness classes.

Thus we can give concrete examples of such reals.

We also consider monotone machines, and self-delimiting machines.

Turing degrees of probabilities of universal machines

For each type of machine, we have an enumeration $M_0, M_1, \ldots$ and U is a universal machine if, for each e, there is some σ such that $M_e(x) = U(\sigma * x)$ for all x.

The methods used by Downey/Hirschfeldt/Miller/Nies and Barmpalias and Dowe will show that the Turing degreee of the probability that, say M(X) is total, depends on the particular universal machine M.

This will be true for all of our events.

Arithmetical classes and measure

LEMMA[Measures of arithmetical classes] Let $n > 0$. The measure of a Σ^0_n class is uniformly a $0^{(n-1)}$-left c.e. real. Similarly, the measure of a Π^0_n class is uniformly a $0^{(n-1)}$-right c,e, real.

LEMMA[Measures of arithmetical classes, converse] Let $n > 0$. Given any $0^{(n-1)}$-left-c.e. real $\alpha \in [0,1]$, we can effectively produce a Σ^0_n prefix-free set of strings of measure α. Similarly, if $\beta \in [0,1]$ is a $0^{(n-1)}$-right-c.e. real, we can effectively produce a Π^0_n prefix-free set of strings of measure β.

Oracle Turing machines and events

Let M be an oracle machine, that is, $\mathrm{M} : 2^{\mathbb{N}} \times \mathbb{N} \to \mathbb{N}$. Then $\mathrm{M}(\mathrm{X})$ is the map taking n to $\mathrm{M}(\mathrm{X}, \mathrm{n})$ and $\mathrm{DOM}(\mathrm{M}(\mathrm{X})) = \{\mathrm{n} : \mathrm{M}(\mathrm{X}, \mathrm{n}) \downarrow\}$.

- $\mathtt{TOT}(\mathrm{M}) = \{\mathrm{X} \in 2^{\mathbb{N}} : \mathrm{M}(\mathrm{X})$is total;
- $\mathtt{INF}(\mathrm{M}) = \{\mathrm{X} : \mathrm{DOM}(\mathrm{M}(\mathrm{X}))$is infinite;
- $\mathtt{COM}(\mathrm{M}) = \{\mathrm{X} : \mathrm{DOM}(\mathrm{M}(\mathrm{X}))$is cofinite;
- $\mathtt{COM}(\mathrm{M}) = \{\mathrm{X} : \mathrm{DOM}(\mathrm{M}(\mathrm{X}))$is computable;
- $\mathtt{CMP}(\mathrm{M}) = \{\mathrm{X} : \mathrm{DOM}(\mathrm{M}(\mathrm{X}))$is complete.

Probabilities of events for oracle machines

LEMMA: For any Σ^0_2 set U of strings, there exists M such that M(X) is total IFF M(X) has infinite domain IFF X does not have a prefix in U.

Proof Sketch: Let $(\mathrm{U_s})$ be a computable sequence of upward closed finite sets of strings such that

(i) $\sigma \in \mathrm{U}$ IFF $\sigma \in \mathrm{U_s}$ for almost all s.

(ii) $\mathrm{U_s} \subset \mathrm{U}$ for infinitely many s.

Now define $\mathrm{M} : 2^{<\omega} \times \mathbb{N} \to \mathbb{N}$ in stages as follows. M_0 is the empty function. At stage $\mathrm{s}+1$, consider σ of length $\leq \mathrm{s}$ such that $\mathrm{M_s}(\sigma, |\sigma|$ is undefined and check if σ has a prefix in $\mathrm{U_{s+1}}$. If not, then define $\mathrm{M_{s+1}}(\sigma, |\sigma| = 0$.

LEMMA: There is an oracle machine M such that the measures of INF(M) and TOT(M) are both 2-random $\emptyset'$ right-c.e. reals.

Proof Sketch: Let U be a member of a universal ML test relative to $\emptyset'$ and let M be given by Lemma above. `TOT`(M) is a Π^0_2 class, so its measure is a $\emptyset'$-right-c.e. real. `TOT`(M) is exactly the complement of the reals that have a prefix in U. Hence `TOT`(M) is a 2-random real. Finally, it follows from Kucera-Slaman that the measure of TOT(M) is also a 2-random $\emptyset'$right-c.e. real.

Kucera, Slaman (2001) Randomness and recursive enumerability.

THEOREM: For any universal oracle machine M, the measures of TOT(M) and INF(M) are both 2-random $\emptyset'$-right-c.e. reals.

Proof Sketch: Let M be given as above and let $\mathrm{M}(\sigma) \simeq \mathrm{U}(\tau * \sigma)$. Then

$$\mathtt{TOT}(\mathrm{U}) = \tau * \mathtt{TOT}(\mathrm{M}) \cup \Big(\mathtt{TOT}(\mathrm{U}) \cap (2^\omega - [[\tau]])\Big)$$

and

$$\tau * \mathtt{TOT}(\mathrm{M}) \cap \Big(\mathtt{TOT}(\mathrm{U}) \cap (2^\omega - [[\tau]])\Big) = \emptyset.$$

Let $\mathrm{P} = \mathtt{TOT}(\mathrm{U}) \cap (2^\omega - [[\tau]])$, a Π^0_2 class, so $\mu(\mathrm{P})$ is a $\emptyset'$-right-c.e. real. Then $\mu(\mathtt{TOT}(\mathrm{U})) = 2^{-|\tau|} \cdot \mu(\mathtt{TOT}(\mathrm{M})) + \mu(\mathrm{P})$ is the sum of a 2-random $\emptyset'$-right-c.e. real and a $\emptyset'$-right-c.e. real, hence a 2-random $\emptyset'$-right-c.e. real by Demuth. A similar argument applies to $\mu(\mathtt{INF}(\mathrm{U}))$.

Demuth (1975) On constructive pseudonumbers.

The Converse

LEMMA: If $\alpha < 1$ is a $\emptyset'$-left-c.e.real and $2^{-c} < 1 - \alpha$, then there is an oracle machine M and a string ρ of length c such that $M(X, n)$ is undefined for any string X compatible with ρ , and $\mu(\mathrm{INF}(M)) = \mu(\mathrm{TOT}(M) = \alpha$.

Proof Sketch: Let $1 - \alpha - 2^{-c} = \sum_i 2^{-b_i}$. Then by Kraft-Chaitin there is a Σ^0_2 prefix-free set $S := \{\sigma_i \mid i \in \mathbb{N}\}$ of strings such that $|\sigma_0| = c$, $|\sigma_{i+1}| = b_i$ for each i. Note that $\mu([[S]]) = 1 - \alpha$. Choose a canonical Σ^0_2 approximation (S_i) to S such that $\sigma_0 \in S_i$ for all i.
Then as above we can obtain a machine M such that $M(\sigma, n)$ is not defined for any string σ compatible with σ_0 and any n. Then $mu\big(\mathtt{TOT}(M)\big) = \mu\big(\mathtt{INF}(M)\big) = \mu\big(2^\omega - [[S]]\big) = 1 - \mu\big(\big([[S]]\big) = \alpha$

THEOREM: Let α be a 2-random $\emptyset'$-right-c.e. real. Then there exists a universal oracle machine M such that $\mu(\mathrm{INF}(\mathrm{M})) = \alpha$ and there exists a universal oracle machine U such that $\mu(\mathrm{TOT}(\mathrm{U})) = \alpha$.

Proof Sketch: Let V be universal and let $\gamma = \mu(\mathrm{TOT}(\mathrm{V}))$. Then γ is a $\emptyset'$-right-c.e. real. By Downey-Hirschfeldt-Nies, there is $\mathrm{c} \in \mathbb{N}$ such that $\alpha + 2^{-\mathrm{c}} < 1$ and $\beta := \alpha - 2^{-\mathrm{c}}\gamma$ is $\emptyset'$-right-c.e. Now we have an oracle machine N and a string ρ of length c such that $\mu(\mathtt{TOT}(\mathrm{N})) = \beta$ and $\mathrm{N}(\sigma, \mathrm{n}) \uparrow$ for any σ compatible with ρ and any n. Define M so$\mathrm{M}(\sigma, \mathrm{n}) \simeq \mathrm{N}(\sigma, \mathrm{n})$ for each σ incompatible with ρ and any n; for each τ and any n let $\mathrm{M}(\rho * \tau, \mathrm{n}) \simeq \mathrm{V}(\tau, \mathrm{n})$. Then M is also universal,

$\mathtt{TOT}(\mathrm{M}) = \rho * \mathtt{TOT}(\mathrm{V}) \cup \mathtt{TOT}(\mathrm{N})$ and $\rho * \mathtt{TOT}(\mathrm{V}) \cap \mathtt{TOT}(\mathrm{N}) = \emptyset$ and so

$$\mu(\mathtt{TOT}(\mathrm{M})) = 2^{-|\rho|} \cdot \mu(\mathtt{TOT}(\mathrm{V})) + \mu(\mathtt{TOT}(\mathrm{N})) = 2^{-\mathrm{c}} \cdot \gamma + \beta = \alpha.$$

DHN (2002) Randomness, computability and density.

Cofiniteness and computability probabilities

LEMMA: For any upward closed Σ^0_3 set J of strings there is an machine M such that TFAE:

- X has a prefix in J;
- the domain of M(X) is cofinite; and
- the domain of M(X) is computable.

Moreover, the domain of M(X) is equal to its range.

LEMMA: There is an oracle machine M such that COF(M) = COM(M) and have measure a 3-random $\emptyset^{(2)}$-left-c.e. real.

THEOREM: For any universal oracle machine M, the measures of COF(M) and COM(M) are 3-random $\emptyset^{(2)}$-left-c.e. reals.

The Converse

LEMMA: If $\alpha < 1$ is a $\emptyset^{(2)}$-left-c.e. real and $2^{-c} < 1 - \alpha$, then there is an oracle machine M and a string ρ of length c such that $M(X, n)$ is undefined for any X compatible with ρ , and $\mu(COF(M)) = \alpha$.

A similar result holds for COM(M).

THEOREM: Let α be a 3-random $\emptyset^{(2)}$-left-c.e. real. Then there exists a universal oracle machines M and N such that $\mu(COF(M)) = \mu(COM(N)) = \alpha$.

Monotone machines

Monotone machines were used by Levin (1971,1973) to define the algorithmic complexity of finite objects.

A monotone machine $N : 2^{\omega} \to 2^{<\omega}$ such that if $\sigma \prec \tau$ and both $M(\sigma) \downarrow$ and $M(\tau) \downarrow$, then $M(\sigma) \preceq M(\tau)$. Then $N(X) = \bigcup_n M(X \upharpoonright n)$.

L71, Some theorems on the algorithmic approach to probability theory and information theory.

L73, The concept of a random sequence.

Events for monotone machines

We are looking at the probabilities of the following events:

- $\texttt{INF}(\mathrm{N}) = \{\mathrm{X} \in 2^{\mathbb{N}} : \mathrm{N}(\mathrm{X}) \in 2^{\mathbb{N}};$
- $\texttt{FIN}(\mathrm{N}) = 2^{\mathbb{N}} - \texttt{INF}(\mathrm{N}).$
- $\texttt{COF}(\mathrm{N}) = \{\mathrm{X} : (\exists \tau)\mathrm{N}(\mathrm{X}) = \tau * 1^{\omega}\}.$

Probabilities of events for monotone machines

LEMMA: For any Σ^0_2 set U of strings, there exists N such that N(X) is infinite IFF X does not have a prefix in U.

LEMMA: There is a monotone machine N such that the measure of INF(N) is a 2-random $\emptyset'$-left-c.e.real.

LEMMA: For any universal monotone machine N, the measure of INF(N) is a 2-random $\emptyset'$-left-c.e.real.

The Converse

LEMMA: If $\alpha < 1$ is a $\emptyset'$-left-c.e.real and $2^{-c} < 1 - \alpha$, then there is a monotone machine N and a string ρ of length c such that $N(\sigma)$ is undefined for any string σ compatible with ρ , and $\mu(\mathrm{INF}(N)) = \alpha$.

THEOREM: Let α be a 2-random $\emptyset'$-left-c.e.real. Then there exists a universal monotone machine N such that $\mu(\mathrm{INF}(N)) = \alpha$.

Infinitary self-delimiting machines

These were introduced by Chaitin and have been extensively studied by Becher, Grigorieff and others.

Let $\mathrm{M} : 2^{<\omega} \times \mathbb{N} \to 2^{<\omega}$ be a partial computable function so

(a) if $\mathrm{M}(\sigma, \mathrm{m}) \downarrow$ and $\mathrm{n} < \mathrm{m}$, then $\mathrm{M}(\sigma, \mathrm{n}) \downarrow$ and $\mathrm{M}(\sigma, \mathrm{n}) \preceq \mathrm{M}(\sigma, \mathrm{m})$;

(b) if $\mathrm{M}(\sigma, \mathrm{n}) \downarrow$, then for all strings τ, $\mathrm{M}(\sigma * \tau, \mathrm{n}) \downarrow$ and $\mathrm{M}(\sigma * \tau, \mathrm{n}) = \mathrm{M}(\sigma, \mathrm{n})$;

(c) the relation $\mathrm{M}(\sigma, \mathrm{n}) \downarrow$ is decidable.

Chaitin (1976) Algorithmic entropy of sets.

Becher & Grigorieff (2009) From index sets to randomness in $\emptyset^{(\mathrm{n})}$.

Infinitary self-delimiting machines and events

Now define the infinitary machine M^{∞} as follows.

(i) $\mathrm{M}^{\infty}(\sigma)\downarrow$ if $\mathrm{M}(\sigma, \mathrm{n})\downarrow$ for all n;

(ii) If $\mathrm{M}^{\infty}(\sigma)\downarrow$, then $\mathrm{M}^{\infty}(\sigma) = \bigcup\{\mathrm{M}(\sigma, \mathrm{n}), \mathrm{n} \in \mathbb{N}$.

Note that $\mathrm{M}(\sigma)$ may be a string or a stream.

We are looking at the probabilities of the following events:

- $\mathtt{DOM}(\mathrm{M}^{\infty} = \{\sigma : \mathrm{M}(\sigma)\downarrow\}$
- $\mathtt{INF}(\mathrm{M}^{\infty}) = \{\sigma \in \mathtt{DOM}(\mathrm{M}^{\infty}) : \mathrm{M}^{\infty}(\sigma) \in 2^{\mathbb{N}};$
- $\mathtt{FIN}(\mathrm{M}^{\infty}) = \mathtt{DOM}(\mathrm{M}^{\infty}) - \mathtt{INF}(\mathrm{M}^{\infty})$.

Probabilities for self-delimiting machines

LEMMA (a) For any upward closed Σ_2^0 set S of strings, there exists M such that $\mathrm{INF}(M) = \emptyset$ and $[[\mathrm{DOM}(M^\infty)]] = [[S]]$.
(b) For any upward closed Σ_2^0 set S of strings, there is M such that $\mathrm{FIN}(M) = \emptyset$ and $[[\mathrm{DOM}(M^\infty)]] = [[S]]$.

This yields an infinitary self-delimiting machine M such that $\mathrm{INF}(M^\infty)$ is empty and the measure of $\mathrm{DOM}(M^\infty) = \mathrm{FIN}(M^\infty)$ is a 2-random $\emptyset'$-left-c.e. real. Hence:

(Becher/Daicz/Chaitin) For any universal infinitary self-delimiting machine M, $\mathrm{FIN}(M^\infty)$ is a 2-random $\emptyset'$-left-c.e. real.

The Converse

LEMMA: If $\alpha < 1$ is a $\emptyset'$-left-c.e.real and $2^{-c} < 1 - \alpha$, then there is a machine M^{∞} and a string ρ of length c such that $M^{\infty}(\sigma)$ is undefined for any string σ compatible with ρ , $DOM(M^{\infty}) = FIN(M^{\infty}$, and $DOM(M^{\infty})$ has measure α.

THEOREM: Let α be a 2-random $\emptyset'$-left-c.e.real. Then there exists a universal infinitary self-delimiting machine M^{∞} such that $\mu(DOM(M^{\infty})) = \alpha$.

Higher randomness restrictions

LEMMA: There is no c.e. prefix-free set of strings that contains a $\Sigma^0_1(\emptyset')$ subset of 2-random measure. More generally, No Σ^0_{n+1} prefix-free set of strings has a Σ^0_{n+2} subset of $(n+2)$-random measure.

THEOREM: The measure of any subset of $\mathrm{DOM}(M^\infty)$ is not a 3-random real number.

$\mathrm{COF}(M^\infty)$ is a Σ^0_3 set of strings, and is Σ^0_3 complete if M is universal. It is also a $\emptyset'$-left-c.e.real. Hence the measure of $\mathrm{COF}(M^\infty)$ is never a 3-random real.