Things to do in and with algorithmic randomness

Tohoku University
22 Feb 2013

Kenshi Miyabe
RIMS, Kyoto University

An introduction to algorithmic randomness

Topics in algorithmic randomness

- Three paradigm - tests, martingales, complexity
- Randomness notions - Schnorr, Kurtz, Demuth
- Turing reducibility - Kučera-Gács Theorem
- Relative randomness - van Lambalgen, lowness

Which sequence is random?

- 00000 00000 00000 00000 00000 00000 00000
- 11001 00100 00111 11101 10101 01000 10001
- 00000 01000 00010 00001 10001 00001 10100

Question 1:
How do we define a randomness notion?

Three paradigm

- Typical - not in effectively constructed null
- Unpredictable - impossible to increase money in a fair betting game
- Incompressible - impossible to be produced by short strings

Turing machine

- Turing machine has
  - input tape (finite or infinite)
  - output tape (finite or infinite but one-way)
- The set of symbols = {0,1}

Kolmogorov complexity

machine = partial computable function from $2^{<\omega}$ to $2^{<\omega}$

$$K_M(\sigma) = \min\{|\tau| \ : \ M(\tau) = \sigma\}$$

There is a universal one U, that is, for each machine M, there is a constant $d \in \omega$ such that

$$K_U(\sigma) \leq K_M(\sigma) + d$$

for each $\sigma \in 2^{<\omega}$.

prefix-free Kolmogorov complexity

$S \subseteq 2^{<\omega}$ is prefix-free if

$$\sigma, \tau \in S \Rightarrow \sigma \not\prec \tau.$$

A machine is called prefix-free if its domain is prefix-free.

Example

$\{0, 01\}$ not prefix-free, $\{0, 10\}$ is prefix-free.

Intuitively, a prefix-free machine recognizes when an input is over.

Basic property

We sometimes write n to mean 0^n.

Proposition

$$K(\sigma) \leq |\sigma| + 2\log|\sigma| + O(1).$$

Proposition (Chaitin 1975)

$$K(\sigma) \leq |\sigma| + K(|\sigma|) + O(1).$$

Martin-Löf randomness

Theorem (Levin 1973, Schnorr 1973, Chaitin 1975)

Let U be a universal prefix-free machine. $A \in 2^\omega$ is Martin-Löf random (or 1-random) iff

$$K_U(A \upharpoonright n) > n - O(1).$$

Other randomness notions

- Demuth randomness
- Weak 2-randomness
- Martin-Löf randomness
- Schnorr randomness
- Kurtz randomness

Question 2:
Is a random set computationally weak?

Chaitin's Omega

Definition (Chaitin)

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

Proposition

If U is a universal prefix-free machine, Ω_U is Martin-Löf random and $\Omega_U \equiv_T \emptyset'$.

Kućera-Gács Theorem

Theorem (Kučera 1984, Gács 1986)

Every set is wtt-reducible to a 1-random set. Furthermore, every Turing degree above the halting problem contains a 1-ranom set.

Definition

A degree is 1-random if it contains 1-random set.

PA degree

Definition

A Turing degree a is called PA if each partial computable $\{0,1\}$-valued function has a-computable total extension.

Theorem (Stephan)

If $\mathbf{a}$ degree is PA and 1-random, then $\mathbf{a} \geq \mathbf{0}'$.

Two types of random sets

- Stupidity Tests
- First: so smart that they know how to be stupid
- Second: really stupid

Difference randomness

Difference randomness is introduced by Franklin and Ng (2011).

Theorem

A set is difference random

iff it is Martin-Löf random and incomplete.

Question 3:
What do you mean by saying that
a set is more random than another?

Measures of randomness

- Relative randomness
- K-reducibility

Relative randomness

- B is (Turing) computable relative to A
- B is (ML-)randomness relative to A

n-random

Definition (Kurtz 1981, Kautz 1991)

A set is called n-random if it is 1-random relative to $\emptyset^{(n-1)}$.

Theorem (Miller 2010)

A set X is 2-random iff it is infinitely often K-random, that is,

$$K(X \upharpoonright n) \geq n + K(n) - O(1)$$

for infinitely many n.

K-reducibility and K-triviality

$X \leq_K Y$ if $K(X \upharpoonright n) \leq K(Y \upharpoonright n) + O(1)$.

Definition

A set X is called K-trivial if $X \leq_K \emptyset$, that is,

$$K(X \upharpoonright n) \leq K(n) + O(1).$$

Lowness

Theorem (Nies and Hirschfeldt, see Nies 2005)

The following are equivalent for a set A:

(i) A is low for ML-randomness, that is, every ML-random set is ML-random relative to A.

(ii) A is K-trivial, that is,

$$K(A \upharpoonright n) < K(n) + O(1).$$

van Lambalgen's Theorem

Theorem (van Lambalgen 1987)

$A \oplus B$ is ML-random

iff A is ML-random and B is ML-random relative to A.

K and vL reducibility

$X \leq_K Y$ if $K(X \upharpoonright n) \leq K(Y \upharpoonright n) + O(1)$.

Definition (Miller and Yu 2008)

$X \leq_{vL} Y$ if, for all Z, that $X \oplus Z$ is ML-random implies $Y \oplus Z$ is ML-random.

Theorem (Miller and Yu 2008)

If $X \leq_K Y$, then $X \leq_{vL} Y$.

Theorem (Miller and Yu 2008)

If $Y \leq_T X$ and Y is 1-random, then $X \leq_{vL} Y$.

$X \oplus Y$ is 1-random, then $X \oplus Y <_{vL} X, Y$. .

Question 4:
How about other randomness notions?

Schnorr randomness

A machine M is called computable measure machine (c.m.m.) if

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

is computable.

Theorem (Downey and Griffiths 2004)

A is Schnorr random

iff $K_M(A \upharpoonright n) > n - O(1)$ for each c.m.m. M.

K does not work well

Theorem (See Theorem 7.4.8 in Nies's book)

For each order function h, there is a computably (so Schnorr) random set Z such that $\forall^\infty n K(Z \upharpoonright n|n) \leq h(n)$.

Schnorr reducibility

Definition (Downey and Griffiths)

$A \leq_{Sch} B$ if, for each c.m.m. M, there is a c.m.m. N such that

$$K_N(A \upharpoonright n) \leq K_M(B \upharpoonright n) + O(1).$$

A is called Schnorr trivial if $A \leq_{Sch} \emptyset$.

Schnorr and truth-table

- Every high degree contains a Schnorr trivial set. (Franklin)
- K-trivial reals form an ideal in the Turing degrees.
- Schnorr trivial reals form an ideal in the tt-degrees.

Definition A set A is anti-complex if, for every order function f, $C(A \upharpoonright f(n)) \leq n$ for almost all n.

Theorem (Franklin Greenberg Stephan Wu)

The following are equivalent for a set A:

(i) A is weak truth-table reducible to a Schnorr trivial set.

(ii) $\deg_{wtt} A$ is c.e. traceable.

(iii) A is anti-complex.

(iv) There is a set B such that $A \leq_{T(tu)} B$.

Theorem

The following are equivalent for a set A:

(i) A is a Schnorr trivial set.

(ii) A is computably tt-traceable.

(iii) A is totally anti-complex.

(iv) There is a set B such that $A \leq_{tt(tu)} B$.

(i) $\iff$ (ii) by Franklin-Stephan.

(i) $\iff$ (iii) by Hölzl-Merkle.

(i) $\iff$ (iv) by Franklin-Greenberg-Stephan-Wu.

Definition (Hölzl and Merkle)

A set A is totally i.o. complex if there is a computable function g such that for all total machines M there are infinitely many n where $C_M(A \upharpoonright h(n)) \leq n$.

Definition

A set A is totally anti-complex if it is not totally i.o. complex, that is, for any order h there exists a total machine M such that $C_M(A \upharpoonright h(n)) \leq n$ for almost all n.

Uniform relativization

- B is truth-table computable relative to A
- B is Schnorr random uniformly relative to A

Turing and truth-table reducibility

B is Turing computable relative to A
iff there is a partial computable function $f :\subseteq 2^\omega \to 2^\omega$ such that $f(A) = B$.

B is truth-table computable relative to A
iff there is a total computable function $f :\subseteq 2^\omega \to 2^\omega$ such that $f(A) = B$.

computable analysis

Consider a sequence $\{q_n\}$ of rationals such that $|q_{n+1} - q_n| \leq 2^{-n}$ for all n.

We say $\{q_n\}$ represents a real x is $\lim_n q_n = x$.

A real x is called computable if a computable sequence represents the real x.

(We also say x has a computable representation.)

Then computability of a function $f :\subseteq 2^\omega \to \mathbb{R}$ is naturally induced.

Uniform relativization

$\alpha \in \mathbb{R}$ is computable relative to $A \in 2^\omega$ if there is a (partial) computable function $f :\subseteq 2^\omega \to \mathbb{R}$ such that $f(A) = \alpha$.

$\alpha \in \mathbb{R}$ is computable uniformly relative to $A \in 2^\omega$ if there is a total computable function $f : 2^\omega \to \mathbb{R}$ such that $f(A) = \alpha$.

Uniform relativization

B is Schnorr random relative to A

if $K_{M^A}(B \upharpoonright n) > n - O(1)$ for each oracle machine M such that $\mu(\mathrm{dom}(M^A))$ is computable from A.

B is Schnorr random uniform relative to A

if $K_{M^A}(B \upharpoonright n) > n - O(1)$ for each oracle machine M such that $Z \mapsto \mu(\mathrm{dom}(M^Z))$ is a total computable function.

Remark

Full relativization and partial relativization.

vL-theorem for Schnorr

Theorem (Merkle et al. 2006, Yu 2007, Kjos-Hanssen)
Van Lambalgen's theorem does not hold for Schnorr randomness.

Theorem (M., M.-Rute (accepted last week!))
Van Lambalgen's theorem does hold for uniform Schnorr randomness.

Lowness and triviality

Theorem (essentially due to Franklin and Stephan 2010)
The following are equivalent for a set A:

(i) A is low for Schnorr randomness, that is, every Schnorr random set is Schnorr random uniformly relative to A.

(ii) A is Schnorr trivial, that is, for each c.m.m. M, there is a c.m.m. N such that

$$K_N(A \restriction n) < K_M(n) + O(1).$$

A slogan

Study uniform relativization more!

vL-theorem

- Done -
  Demuth by Diamondstone et al.,
  Schnorr and Kurtz by M.
  Bounded Primitive Recursive Randomness by Cenzer and Remmel
- Not done -
  weak 2, difference, bounded

Lowness

- Done -
  Demuth by Bienvenu et al.,
  Schnorr by Franklin et al.,
  Kurtz by Kihara and M.
- Not done -
  comp., weak 2, bounded, Π^1_1-MLR and others

Kučera-Gács theorem for tt-reducibility does not hold!

Theorem (Calude and Nies 1997)

No ML-random set Z satisfies $\emptyset' \leq_{tt} Z$.

Actually, no Kurtz random set Z satisfies $\emptyset' \leq_{tt} Z$.

Question

Which tt-degree contains a (Schnorr, Kurtz etc.) random set?

Is it really a natural question?

Theorem

A is K-trivial iff $\{Z : A \leq_T Z\}$ contains an A-ML-random set.

Theorem (Franklin-Stephan)

There is a Schnott trivial set that $\{Z : A \leq_{tt} Z\}$ does not contain a Schnorr random set uniformly relative to A.

Theorem (M.)

A is Schnorr trivial iff, for each uniform Schnorr test $\{U_n\}$, there is Z such that $Z \notin \bigcap_n U_n^A$ and $A \leq_{tt} Z$.

Questions

- Other randomness versions of vL-reducibility
- Infinitely often maximally complex for c.m.m.
- Randomness extraction
- Solovay reducibility revisited
- Omega operator
- Resource-bounded randomness

Things to do with algorithmic randomness

- The basic idea is to replace "almost everywhere" with "all sufficiently random points".

- Two big topics are "differentiability" and "ergodic theorem".

- Interesting because
  - one sometimes needs a new notion
  - randomness notions can be understood by classical notions

Completely different interpretations via algorithmic randomness!

Ergodic theory

Set $A = [0, 1/2)$ and $B = [1/2, 1]$.

Consider

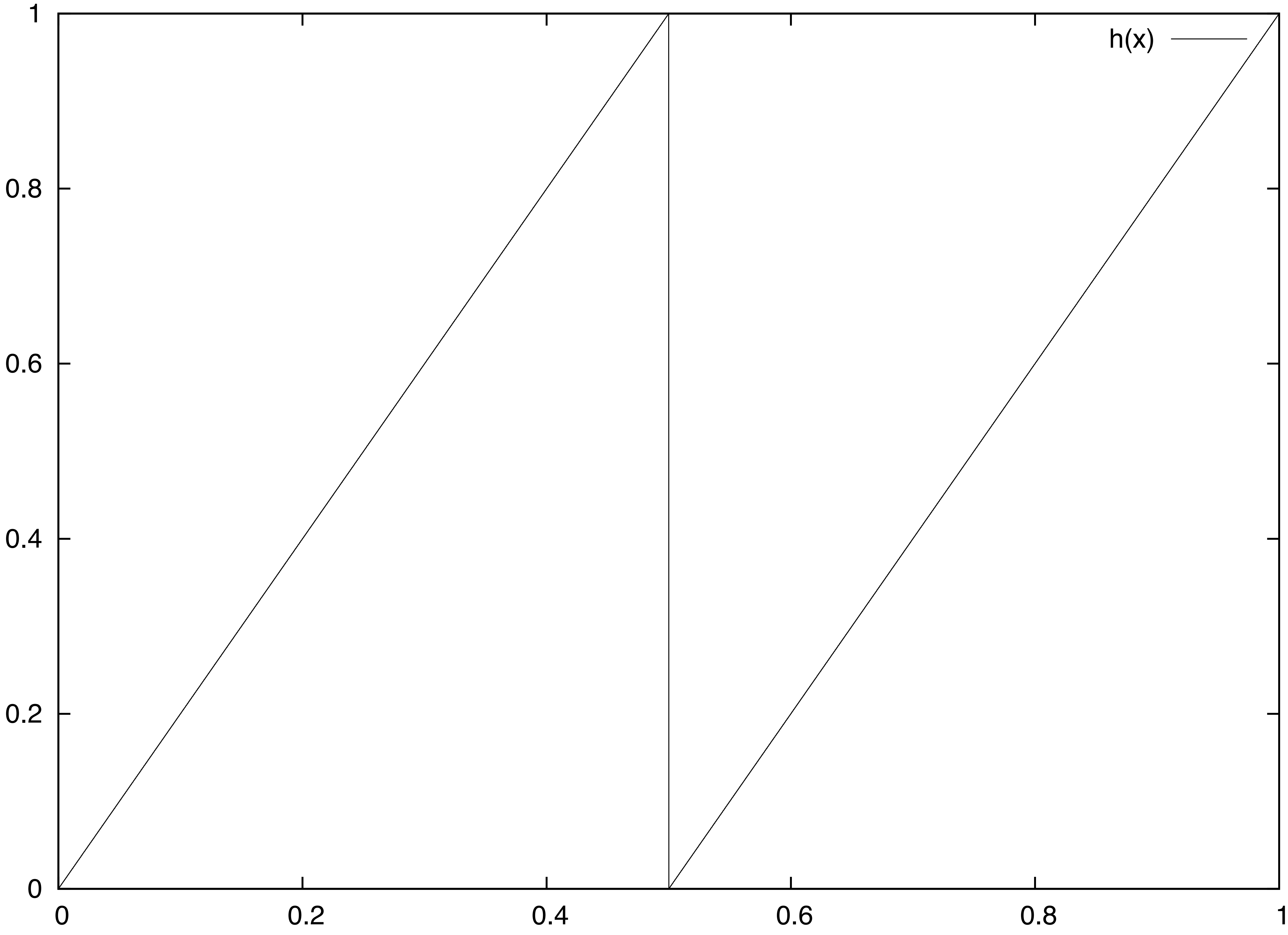
$$f(x) = \begin{cases} 2x & \text{if } x \in A \\ 2x - 1 & \text{if } x \in B \end{cases}$$

Question

Given an initial point x_0, how often $f^n(x_0) \in A$?

More precisely, evaluate the following value:

$$\lim_{N \to \infty} \frac{\#\{n \leq N \ : \ f^n(x_0) \in A\}}{N}.$$


h(x)
1
0.8
0.6
0.4
0.2
0
0
0.2
0.4
0.6
0.8
1

Birkhoff's ergodic theorem (SLLN is enough in this case) says that

$$\lim_{N\to\infty} \frac{\#\{n \le N \ : \ f^n(x_0) \in A\}}{N} = 1/2$$

almost everywhere.

Interpretation via probability

Because of the sensitivity of initial condition, the points move randomly, so the frequency goes to the measure of the set.

More natural interpretation

The unpredictability (randomness) of the initial value corresponds the unpredictability of the orbit, so the frequency goes to the measure of the set. Furthermore, the set of such points has measure 1. This also explains the sensitivity of initial condition.

Such interpretation via deterministic randomness was made possible due to Poincaré, but in what sense a determined initial value is unpredictable or random?

Hoyrup et al. showed that

$$\lim_{N\to\infty} \frac{\#\{n \leq N \ : \ f^n(x_0) \in A\}}{N} = 1/2$$

for all Schnorr random points.

Actually, they showed that Schnorr randomness can be characterized via effective version of Birkhoff's ergodic theorem.

- “Randomness and Determination, from Physics and Computing towards Biology”
- “Incomputability in Physics and Biology”
- by Giuseppe Longo in CNRS.

Use randomness as a resource

- Randomized algorithm such as Monte Carlo
- The relation with L^1-computability?
- Which randomness is needed?
- Which property of randomness is used?

- “Monte Carlo Method, Random Number, and Pseudorandom Number”
- by Hiroshi Sugita in Osaka Univ.

Justification of scientific method

- How to deal with uncertainties?
- Justification of induction seems to need the notion of randomness rather than Ockham's razor.
- The relation between mathematics and science?

- "Algorithmic Probability -- Its Discovery -- Its Properties and Application to Strong AI" and "Algorithmic Probability: Theory and Applications" by Solomonoff

- "Universal Artificial Intelligence"
  by Marcus Hutter
  in Australia's national university

- “Ockham Efficiency Theorem”
  in “Ockham’s Razor, Truth, and Information”
  by Kevin T. Kelly in Carnegie Mellon Univ.

Other random phenomena?

- Brownian motion by Fouch and Kjos-Hanssen
- Statistical mechanics by Tadaki and others
- Quantum mechanics by Calude and Svozil
- Statistics?

Computability everywhere

- computable analysis
- computable measure theory
- computable information theory?
- computable statistics?
- computable quantum mechanics?

Thanks!