Resource-bounded randomness and differentiability

Akitoshi Kawamura (Tokyo)

CTFM, Tokyo, February 18, 2014

(Joint work with Kenshi Miyabe)

Computability and resource bounds

11011100111011110100000011010111000001111011111111010001101001......

write out bit by bit or equivalently given n, answer the n-bit prefix

nth bit in time $t(n)$

0^n

in time $t(n)$

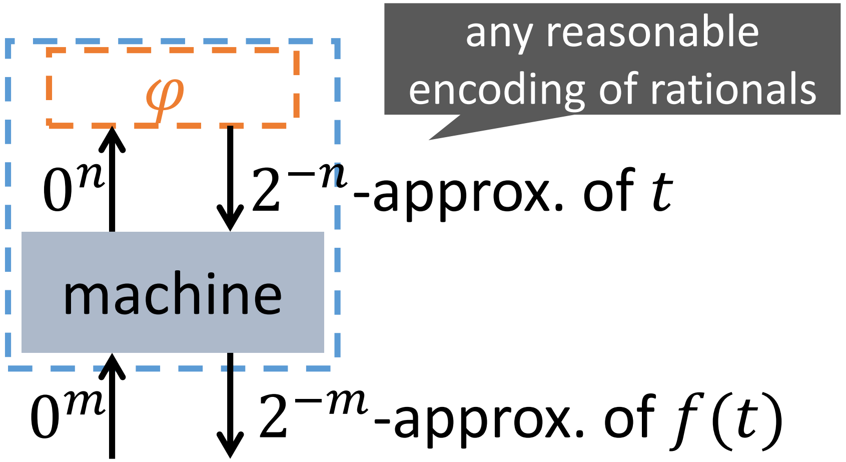
$$\mathbf{P} \subseteq \mathbf{PSPACE} \subseteq \mathbf{EXP} \subseteq \cdots \subseteq \text{Computable}$$

tally part

Computable real numbers (Turing 1936)

real $z \in [0,1]$ ←→ its binary expansion

Computable real functions



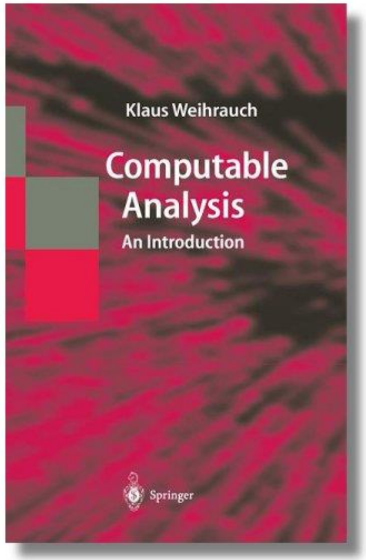
Computing $f\colon [0,1] \to \mathbf{R}$

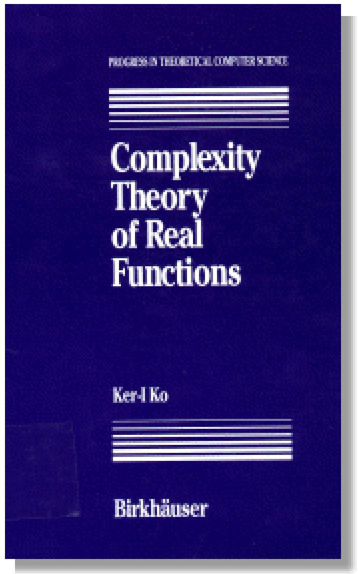
Definition (Grzegorczyk 1955, Ko-Friedman 1982)

- $\varphi\colon \Sigma^* \to \Sigma^*$ is a name of $t \in \mathbf{R}$ if
  $\varphi(0^n)$ encodes a rational within distance 2^{-n} of t.
- An oracle TM M computes $f\colon [0,1] \to \mathbf{R}$ if
  M^φ is a name of $f(t)$ for every name φ of $t \in \mathbf{R}$.

The function computed by M with oracle φ

[Equivalent to "Type-Two Machine" (infinite strings model)
+ signed digit representation]





Computability and Randomness

computability – building the sequence

1101110011101111010000001101011100000011110111111111010001101001……

randomness – (not) finding rules about the sequence

- has no rare property
- cannot predict
- cannot compress

111100110011111100000000001111111100111111……

Martin-Löf Randomness

11011100111011110100000011010111000001111011111111010001101001101010100......

- Random = no rare property

Most sequences are random.

Definition (Martin-Löf 1966)

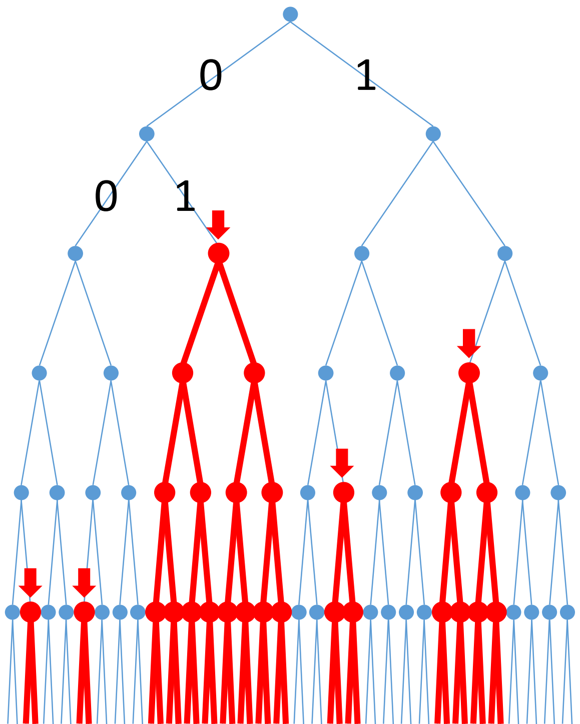
An infinite sequence $Z \in \{0,1\}^{\mathbf{N}}$ is Martin-Löf random if there is no computably enumerable test that captures Z.

$n \mapsto$ property $U_n \subseteq \{0,1\}^{\mathbf{N}}$ with $\mu(U_n) < 2^{-n}$

$Z \in \bigcap_n U_n$

U_n = sequences starting with prefixes u_{n1}, u_{n2}, ... (infinite list)

finite list → Kurtz randomness

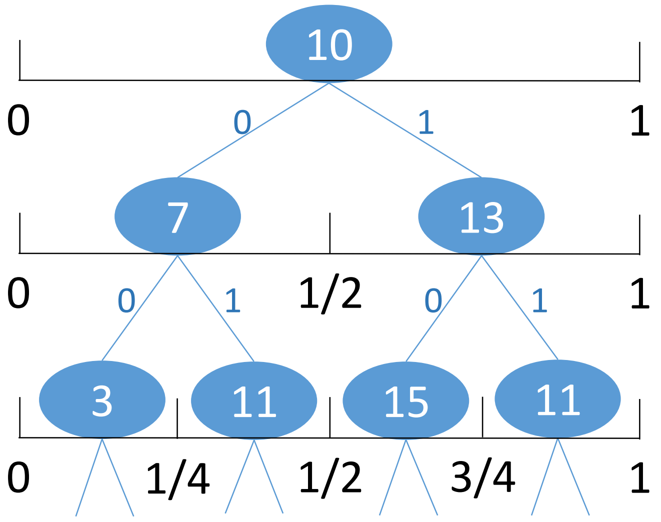


Computable randomness

110111001110111110100000011010111000001111011111111010001101001101010100......

What's the next bit?

- Random = unpredictable



Definition (Schnorr 1971)

An infinite sequence $Z \in \{0,1\}^{\mathbf{N}}$ is computably random if there is no computable martingale that succeeds on Z.

function $M: \{0,1\}^* \to \mathbf{R}_{\geq 0}$
with $M(u) = \frac{M(u0)+M(u1)}{2}$

$M(Z_{<n})$ is unbounded ($n \in \mathbf{N}$)

Definition

A real $z \in [0,1]$ is computably random if its binary expansion is.

Dependent on the base?

Resource-bounded randomness

Computable

PSPACE

P

L

Martin-Löf randomness $\subseteq$ Computable randomness $\subseteq$ Kurtz randomness

PSPACE randomness

Bounded **PSPACE** randomness

[Cenzer, Remmel 2013]

???

P randomness

L randomness

Randomness and differentiability

Theorem (Lebesgue 1904)

Every monotone function $f: [0,1] \to \mathbf{R}$ is differentiable at almost all $z \in [0,1]$.

But which z?

Poly-time version?

Theorem (Brattka, Miller, Nies 2011) **K.-Miyabe**

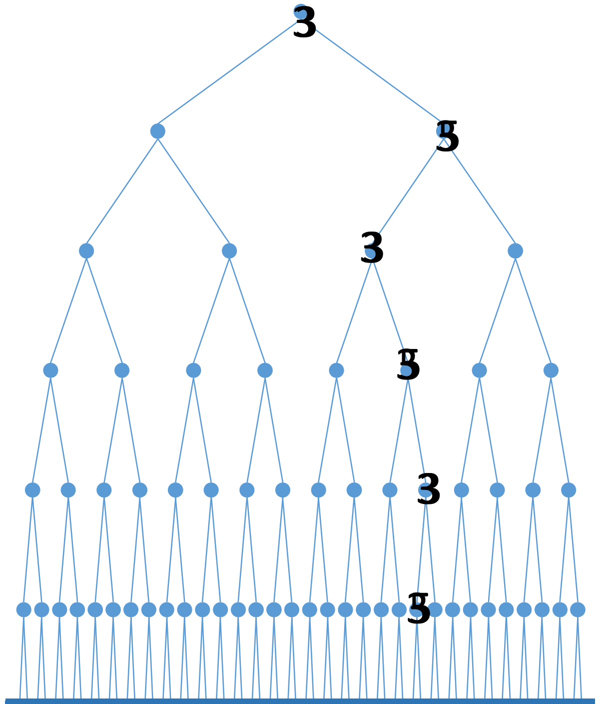
For $z \in [0, 1]$, the following are equivalent:

1. z is **poly-time** random.
2. Every **poly-time** monotone function $f: [0,1] \to \mathbf{R}$ is differentiable at z.

Not dependent on the base!

Independently by A. Nies (private communication), using the idea of *porosity*.

Martingales and real functions



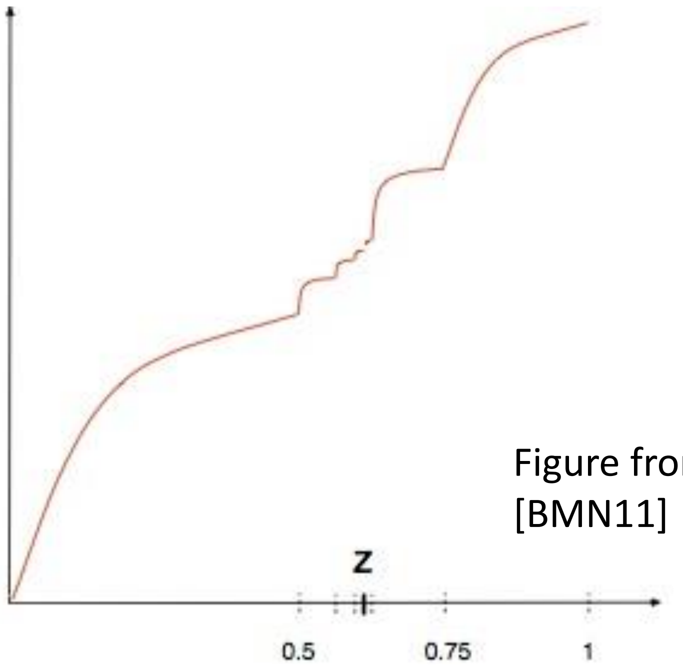


Figure from [BMN11]

M: #■☆-martingale ⟷ $f \in \mathrm{C_m}[0,1]$

non-de

poly-time ⟵ WLOG ⟶ poly-time

Succeeds at z ⟷ $f'(z) = +\infty$

??? ⟵ f not differentiable at z

$Slope_f(I) \to \infty$ no matter how intervals I approach z

Difficulties:

1. ✔ $Slope_f(I)$ may oscillate, and
2. this fact may not be observed in the martingale values.

Generalized martingales

Instead of the binary tree T_2 of intervals…

Definition

An interval tree T is pair of functions

- $children_T : \subseteq \{0\}^* \times \mathbf{Q} \times \mathbf{Q} \to \mathbf{Q}^*$
  The interval $[l, r]$ at level d is divided at level $d + 1$ at the points listed in $children(0^d, l, r)$.
- $modulus_T : \{0\}^* \to \{0\}^*$
  If $modulus(0^n) = 0^d$, every interval at depth d has length $\leq 2^{-n}$.

Lemma

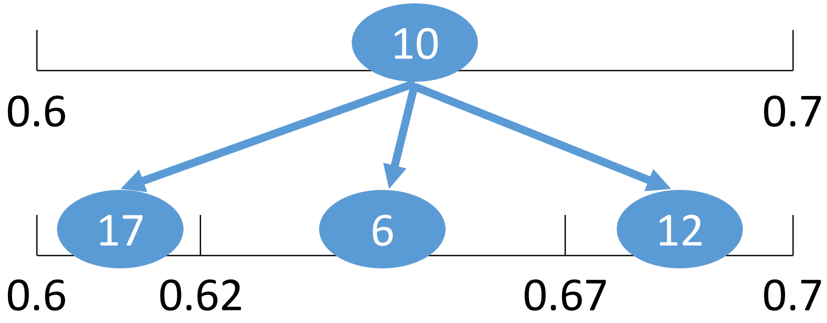
What's said so far holds for T-martingales, for any poly-time T.

- In particular, poly-time T-randomness does not depend on T.

Lemma

Any oscillation is detected on some poly-time T.

T-martingale



We may think of the tree T as being chosen by the gambler.

Work to be done

- Lipschitz → 2-D?
- Log-space
- Simplify the proofs – randomness wrt general measure
  - Done for Martin-Löf randomness since Levin (70s)
- Similar characterization of other randomness