ランダム概念の階層とその改良としての還元可能性

宮部賢志(明治大学理工学部)

鈴木研・宮部研合同ゼミ

首都大学東京

2015年2月23日(月)

ランダムとは何か

ランダムな有限列

- 00000000000000000000000000000000000000
- 01010101010101010101010101010101010101010
- 01010001101010001010111101011111100000110

Kolmogorov複雑性

定義

マシンとは部分計算可能関数 $M :\subseteq 2^{<\omega} \to 2^{<\omega}$ のことを言う.

定義

2 進有限列 σ に対して，そのマシン M に対する複雑性を,

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

によって定義する．そのような τ が存在しない場合は ∞ とする.

万能マシン U を 1 つ固定して，$C = C_U$ とする．

命題

ある定数 $c \in \mathbb{N}$ が存在して，すべての $\sigma \in 2^{<\omega}$ に対して，

$$C(\sigma) \leq |\sigma| + c.$$

任意の $n \in \mathbb{N}$ に対して，ある $\sigma \in 2^n$ が存在して，

$$C(\sigma) \geq n.$$

マシンの定義域を prefix-free に制限した場合の複雑性を K で表す．ファイルの終了が判定できるものと思って良い．

命題

ある定数 $c \in \mathbb{N}$ が存在して，すべての $\sigma \in 2^{<\omega}$ に対して，

$$K(\sigma) \leq |\sigma| + K(|\sigma|) + c.$$

任意の $n \in \mathbb{N}$ に対して，ある $\sigma \in 2^n$ が存在して，

$$K(\sigma) \geq n + K(n).$$

MLランダムネス

定義

$A \in 2^\omega$ が ML ランダムであるとは，ある定数 $c \in \mathbb{N}$ が存在して，すべての $n \in \mathbb{N}$ に対して，

$$K(A \upharpoonright n) > n - c$$

となることを言う．

- MLランダムな列の集合は測度1

- すべてのMLランダムな列は大数の法則，重複対数の法則を満たす

- 統計検定や予測不可能性による同値な特徴付けも知られている

ランダム概念の階層

2ランダムネス

↓

MLランダムネス

↓

Schnorrランダムネス

↓

Kurtzランダムネス

ランダムさの還元可能性

Motivation

- ある列が別の列よりも
  よりランダムであるとは？

ハーフランダム

定義

$A \in 2^\omega$ がハーフランダムであるとは，ある定数 $c \in \mathbb{N}$ が存在して，すべての $n \in \mathbb{N}$ に対して，

$$K(A \upharpoonright n) > \frac{n}{2} - c$$

となることを言う．

例えば，A を ML ランダムとして，$B = A \oplus \emptyset$ など．$\frac{1}{2}$ を s に変えると，s ランダムと呼ばれる．

K-reducibility

定義

$A \leq_K B$ を,

$$K(A \upharpoonright n) \leq K(B \upharpoonright n) + O(1)$$

により定義する.

Theorem (Miller 2009)

A が 2 ランダム $\iff$ $K(A \upharpoonright n) > n + K(n) - O(1)$ i.o.

Theorem (Levin-Schnorr 1973)

A が ML ランダム $\iff$ $K(A \upharpoonright n) > n - O(1)$.

Theorem (Nies 本の Theorem 7.4.11)

計算可能ランダムな列 A で任意の計算可能な order h に対して，ほとんどすべての n で $K(A \upharpoonright n|n) \leq h(n)$ となるものが存在する.

問題

- K-reducibilityではMLランダムと2ランダムとは整合性があるが，計算可能ランダム以下はつぶれてしまって，階層を保っていない
- C-reducibilityも同じ問題が起こる
- ランダムの階層を保つ還元可能性はないのか？

全域マシンは定義域が全域となるマシン.

prefix-free 判定可能マシンは定義域が prefix-free で計算可能なマシン.

計算可能測度マシンは $\sum_{\sigma\in\mathrm{dom}(M)} 2^{-|\sigma|}$ が計算可能となるような prefix-free マシン.

それぞれから導かれる還元可能性を，$\leq_{tm}$, $\leq_{dm}$, $\leq_{Sch}$ と書く.

「$A \leq_r B$ かつ A が R ランダムであるとき，B が R ランダムである」この条件が満たされるとき，還元可能性 $\leq_r$ は R ランダムネスと整合性があるということにする．

例えば，K, C-reducibility は ML ランダムネスと 2 ランダムネスとは整合性があるが，計算可能ランダムネス，Schnorr ランダムネス，Kurtz ランダムネスとは整合性がない．

定理 (Nies, Stephan and Terwijn 2005)
十分速く発散する関数 g に対して,
X が 2 ランダム $\iff$ $C^g(X \upharpoonright n) > n - O(1)$ i.o.

よって $\leq_{tm}$ は 2 ランダムネスと整合性がある.

定理 (Bienvenu and Merkle 2007 の結果から)
X が Kurtz ランダム $\iff$ すべての全域マシン M と計算可能なオーダー f に対して, $C_M(X \upharpoonright n) > n - f(n)$ i.o.

よって $\leq_{tm}$ は Kurtz ランダムネスと整合性がある.

定理 (M.)

X が Schnorr ランダム $\iff$ すべての計算可能測度マシン M と全域マシン N に対して，$C_N(X \upharpoonright n) > n - K_M(n) - O(1)$.

よって $\leq_{tm}$ は Schnorr ランダムネスと整合性がある.

Downey-Griffiths(2004) より,
$\leq_{Sch}$ は Schnorr ランダムネスと整合性がある.

Bienvenu-Merkle(2007) より,
$\leq_{wm}$ は Schnorr ランダムネスと整合性があり,
$\leq_{wm}$ と $\leq_{Sch}$ は Kurtz ランダムネスと整合性があり,
$\leq_{wm}$ は ML ランダムネスと整合性がある.

Bienvenu の博士論文の Theorem 2.3.24 より,
$\leq_{wm}$ は 2 ランダムネスと整合性がある.

$$Q_M(\sigma) = \mu(\llbracket \{\tau \ : \ M(\tau) \downarrow = \sigma\} \rrbracket)$$

Theorem (Coding theorem)

$$K(\sigma) = -\log Q(\sigma).$$

$$Q_M(\in 2^n) = \mu(\llbracket \{\tau \ : \ M(\tau) \downarrow \in 2^n\} \rrbracket)$$

Theorem (M.)

$$K(n) = -\log Q(\in 2^n).$$

.

Extended counting theorem

Theorem (Counting theorem)

$$|\{\sigma \ : \ |\sigma| = n \wedge K(\sigma) \leq n + K(n) - r\}| \leq 2^{n-r+O(1)}.$$

Theorem (Extended counting theorem, M.)

$$|\{\sigma \ : \ |\sigma| = n \wedge K_M(\sigma) \leq n - \log(Q_M(\in 2^n)) - r\}| \leq 2^{n-r+O(1)}.$$

2-randomness and c.m.m.

Theorem (M.)

A sequence $X \in 2^\omega$ is 2-random iff, for every computable measure machine M,

$$K_M(X \upharpoonright n) \geq n - \log(Q_M(\in 2^n)) - O(1)$$

for infinitely many n.

Corollary

If $X \leq_{Sch} Y$ and X is 2-random, then Y is 2-random.

Plain machines (C)	X	X	MLR	2R
Prefix-free machines (K)	X	X	MLR	2R
Comp. measure machines	WR	SR	?	2R
Prefix-free decidable mach.	WR	SR	MLR	2R
Total machines	WR	SR	?	2R