Merkleの基準の
SchnorrおよびKurtzランダムネス版

岐阜大学

2013年3月18日

宮部賢志

京都大学　数理解析研究所

今回の目的

アルゴリズム的ランダムネスの

基本的な定義などの紹介

話の流れ

- 計算量理論とランダムネス
- 計算可能性理論の基礎
- ランダムネスの理論の紹介
- Merkleの基準とその他のランダムネス版

ランダムの概念について

ランダムの概念の始まり

- von Mises (1919) が確率論の定式化のためにcollectiveの概念を提唱
- Martin-Löf (1966) が最初の自然なランダムの概念を定義
- Schnorr, Levin (1973) によるKolmogorov複雑性での特徴付け

ランダムの概念の使われ方

- Solomonoffによるalgorithmic probability
- Birkhoffのエルゴード定理の実効化
- 乱択アルゴリズム

計算可能性理論

- 関数 $f :\subseteq \omega \to \omega$ が計算可能であるとは，Turing マシンにより計算可能であることを言う．
- 自然数列 $\{a_n\}$ が計算可能であるとは，ある計算可能な関数 f が存在して，

$$f(n) = a_n$$

となることを言う．

- 集合 $A \subseteq \omega$ が計算可能であるとは，ある計算可能な関数 f が存在して，

$$f(n) = \begin{cases} 1 & \text{if } n \in A \\ 0 & \text{if } n \notin A \end{cases}$$

を満たすことを言う．

- 集合 $A \subseteq \omega$ が c.e. であるとは，ある計算可能な関数 f が存在して，

$$\mathrm{dom}(f) = A$$

を満たすことを言う．

- 自然数の集合の列 $\{A_n\}$ が一様に計算可能であるとは，ある計算可能な関数 f が存在して，

$$f(n,m) = \begin{cases} 1 & \text{if } m \in A_n \\ 0 & \text{if } m \notin A_n \end{cases}$$

を満たすことを言う．

- 一様に c.e. であるなど，他の概念に対しても同様に定義される．

- 実数 α が計算可能であるとは，ある計算可能な有理数列 $\{q_n\}$ が存在して，

$$|\alpha - q_n| < 2^{-n}$$

を満たすことを言う．

- 実数 α が left-c.e. であるとは，ある計算可能な単調増加列 $\{q_n\}$ が存在して，

$$\alpha = \lim_n q_n$$

を満たすことを言う．

- α が計算可能 $\iff$ α と $-\alpha$ が left-c.e.

- 2^ω に，各 $\sigma \in 2^{<\omega}$ に対して，

$$[\sigma] = \{A \in 2^\omega \ : \ \sigma \prec A\}$$

を開基として作られる topology を入れた空間を Cantor 空間と呼ぶ.

- 開集合 U が c.e. であるとは，ある c.e. 集合 $S \subseteq 2^{<\omega}$ が存在して，

$$U = \bigcup_{\sigma \in S} [\sigma]$$

を満たすことを言う.

- μ を一様測度とすると，U が c.e. 開集合なら，$\mu(U)$ は left-c.e.

ランダムネスの理論

定義 (Martin-Löf 1966)

一様に c.e. 開集合の列 $\{U_n\}$ がすべての n に対して $\mu(U_n) \leq 2^{-n}$ を満たすとき，$\{U_n\}$ を ML テストと呼ぶ．列 A が ML ランダムであるとは，すべての ML テスト $\{U_n\}$ に対して $A \notin \bigcap_n U_n$ となることを言う．

事実

$\{U_n\}$ が ML テストなら $\mu(\bigcap_n U_n) = 0$.

ML テストは可算個しかないから，ML ランダムな列の集合は測度 1.

万能 ML テスト $\{V_n\}$ が存在する，すなわち，任意の ML テスト $\{U_n\}$ に対して，

$$\bigcap_n U_n \subseteq \bigcap_n V_n$$

マシンとは，部分計算可能関数 $f :\subseteq 2^{<\omega} \to 2^{<\omega}$ の略語である．

集合 $S \subset 2^{<\omega}$ が prefix-free であるとは，

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

を満たすことを言う．マシン M が prefix-free であるとは，$\mathrm{dom}(M)$ が prefix-free であることを言う．

定義 $\sigma \in 2^{<\omega}$ の M による Kolmogorov 複雑性を，

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

で定義する．

命題

万能 prefix-free マシン U が存在する，すなわち，任意の prefix-free マシン M に対して，ある定数 $c \in \omega$ が存在して，すべての $\sigma \in 2^{<\omega}$ に対し，

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

以下，万能マシン U を固定し，$K = K_U$ とおく．

定理 (Levin 1973, Schnorr 1973, Chaitin 1975)
$X \in 2^\omega$ に関して以下は同値.

(i) X は ML ランダム.

(ii) ある $d \in \omega$ が存在して，すべての $n \in \omega$ に対して，

$$K(X \upharpoonright n) > n - d$$

.

Mekleの基準

定理 (Merkle)

$A \in 2^\omega$ に関して以下は同値.

1. A は ML ランダムでない.
2. $K(x_i) \leq |x_i| - 1$ を満たす列 $\{x_i\}$ が存在して，$A = x_0x_1x_2\cdots$ となる.
3. ある prefix-free マシン M と $K_M(x_i) \leq |x_i| - 1$ を満たす列 $\{x_i\}$ が存在して，$A = x_0x_1x_2\cdots$ となる.

証明概略

- 規則が無限回見つかるならランダムでない
- ランダムでないなら，
  どこかで規則が見つかる
- 有限桁のシフトもランダムでないから，
  やはりどこかで規則が見つかる

Merkleの基準の変形

定義 (Schnorr 1971)

$\mu(U_n)$ が一様に計算可能であるような ML テスト $\{U_n\}$ を Schnorr テストと呼ぶ．$X \in 2^\omega$ が Schnorr ランダムであるとは，すべての Schnorr テスト $\{U_n\}$ に対し $X \notin \bigcap_n U_n$ であることを言う．

事実

万能 Schnorr テストは存在しない．

定義 (Downey-Griffiths 2004)

prefix-free マシン M の測度とは

$$\mu([\![\mathrm{dom}(M)]\!]) = \sum_{\sigma \in \mathrm{dom}(M)} 2^{-|\sigma|}$$

のことを言う.

定理 (Downey-Griffiths 2004)

$X \in 2^\omega$ に関して以下は同値.

(i) X は Schnorr ランダム.

(ii) 任意の計算可能な測度を持つマシン M に対して，ある $d \in \omega$ が存在して，すべての n で

$$K_M(X \upharpoonright n) \geq n - d.$$

Schnorrランダムネス版

定理 (M.)

$A \in 2^\omega$ に関して以下は同値.

(i) A は Schnorr ランダムでない.

(ii) ある計算可能な測度を持つマシン M と $K_M(x_i) \leq |x_i| - 1$ を満たす列 $\{x_i\}$ が存在して，$A = x_0x_1x_2\cdots$ となる.

証明概略

- 基本的にはMLランダムの場合と同じだが,
  万能テストが存在しないので,
  その部分の修正が必要

- そこでシフトに関して閉じている
  Schnorrテスト（に相当するもの）を作る

Kurtzランダムネス

定義 (Kurtz '81)

列 $A \in 2^\omega$ が Kurtz ランダムであるとは，すべての測度 1 の c.e. 開集合に含まれることを言う．

例

計算可能な列 A は Kurtz ランダムではない．なぜならば，$2^\omega \setminus A$ が測度 1 の c.e. 開集合であるから．

Kurtzランダムネス版

定理 (M.)

$A \in 2^\omega$ に関して以下は同値.

(i) A は Kurtz ランダムでない.

(ii) ある計算可能な order u と決定可能な prefix-free マシン M が存在して，すべての n で

$$K_M(A \upharpoonright [u(n), u(n+1))) \leq u(n+1) - u(n) - 1$$

となる.