一様Kurtzランダムネスに対する独立性定理

東京工業大学

2013年1月25日

宮部賢志

京都大学　数理解析研究所

話の流れ

- Kurtzランダムネス
- Merkleの基準
- 独立性定理

Kurtz ランダムネス

- 2進無限列がランダムであるとは どういうことか？
- 規則が全く見つからない
- 規則がなかなか見つからない
- 規則がすぐに見つかる

ランダムの諸概念の関係

- Demuth ランダムネス
- Martin-Löf ランダムネス
- 計算可能ランダムネス
- Schnorr ランダムネス
- Kurtz ランダムネス

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．

テスト型の特徴付け

定義 (Wang ’96)

Kurtz null test とは ML-test $\{U_n\}$ で，ある計算可能な関数 $f : \omega \to (2^{<\omega})^{<\omega}$ が存在してすべての n で $U_n = [f(n)]$ となるものを言う.

定理 (Wang ’96)

Kurtz ランダムであることと，すべての Kurtz null test に合格することが同値.

証明

証明

A が Kurtz ランダムでないとしよう．

U を測度 1 の c.e. 開集合で $A \notin U$ となるものとする．

それぞれの n に対して，$\mu(U_s) > 1 - 2^n$ となる最小の s に対して，$V_n = 2^\omega \setminus U_s$ とおく．

$\{V_n\}$ は Kurtz null test で，$A \in \bigcap_n V_n$.

$\{V_n\}$ を Kurtz null test で，$A \in \bigcap_n V_n$ とする．

$U = \bigcup_n (2^\omega \setminus V_n)$ とすれば，U は測度 1 の c.e. 開集合で，

$A \notin U$ だから，A は Kurtz ランダムでない．

マルチンゲール

定義

マルチンゲールとは, 関数 $d : 2^{<\omega} \to \mathbb{R}^+$ で, すべての $\sigma \in 2^{<\omega}$ で，$d(\sigma) = \frac{d(\sigma 0)+d(\sigma 1)}{2}$ を満たすものを言う.

定理 (Wang '96)

$A \in 2^\omega$ に関して以下は同値.

1. A は Kurtz ランダムでない.
2. ある計算可能なマルチンゲール d と計算可能な order h が存在して，すべての n で $d(A \upharpoonright n) > h(n)$ となる.

計算可能な測度を持つマシン

定義

prefix-free マシン M の測度とは，$\mu(\mathrm{dom}(M))$ のことを言う．

定理 (Downey, Griffiths and Reid '04)

$A \in 2^\omega$ に関して以下は同値．

1. A は Kurtz ランダムでない．
2. ある計算可能な測度を持つマシン M と計算可能な関数 F が存在して，$K_M(A \upharpoonright f(n)) < f(n) - n$ となる．

決定可能なマシン

定理 (Bienvenu and Merkle '07)

$A \in 2^\omega$ に関して以下は同値.

1. A は Kurtz ランダムでない.
2. ある決定可能な prefix-free マシン M と計算可能な order f が存在して，すべての n で $K_M(A \upharpoonright f(n)) \leq f(n) - n$ となる.
3. ある決定可能なマシン M と計算可能な order f が存在して，すべての n で $C_M(A \upharpoonright f(n)) \leq f(n) - n$ となる.

Merkleの基準

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，$A = x_0 x_1 x_2 \cdots$ 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，$A = x_0 x_1 x_2 \cdots$ となる.

Schnorrランダムネス版

定理 (M.)

$A \in 2^\omega$ に関して以下は同値.

1. A は Schnorr ランダムでない.
2. 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，$A = x_0 x_1 x_2 \cdots$ となる.

Kurtz ランダムネス版

定理 (M.)

$A \in 2^\omega$ に関して以下は同値.

1. A は Kurtz ランダムでない.
2. 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.

A は Kurtz ランダムではないとしよう.

A が合格しない Kurtz null test $\{[\![f(n)]\!]\}$ が存在する.

すなわち，計算可能な関数 $f:\omega\to(2^{<\omega})^{<\omega}$ と計算可能な order u が存在して，すべての n で $f(n)\subseteq 2^{u(n)}$, $|f(n)|=2^{u(n)-n}$, $A\restriction u(n)\in f(n)$ となる.

さらに，$u(0)=0$ で，u は単調増加とする.

計算可能な単調増加関数 k を，$k(0)=0$,

$$k(n+1)=u(k(n))+n+2$$

で定義し，$l(n)=u(k(n))$ に対して，命題を満たすようなマシン M を作ろう.

KC 集合を

$$\langle l(n+1) - l(n) - 1, \sigma \restriction [l(n), l(n+1))\rangle \text{ for } \sigma \in f(k(n+1))$$

で定義する．ここで,

$$\sigma \in f(k(n+1)) \Rightarrow |\sigma| = u(k(n+1)) = l(n+1)$$

であることに注意しよう．この weight は,

$$\begin{aligned}
&\sum_n \sum_{\sigma \in f(k(n+1))} 2^{-(l(n+1)-l(n)-1)} \\
&= \sum_n 2^{u(k(n+1))-k(n+1)} \cdot 2^{-u(k(n+1)+u(k(n))+1} \\
&= \sum_n 2^{-n-1} = 1.
\end{aligned}$$

この KC 集合から作られるマシン M は計算可能な測度を持つ.

すべての n に対して,

$$\sigma_n = X \upharpoonright u(n) \in f(n)$$

だから，各 n に対して,

$$M(\tau_n) = X \upharpoonright [l(n), l(n+1))$$

となる $\tau_n \in 2^{l(n+1)-l(n)-1}$ が存在する．よって,

$$K_M(X \upharpoonright [l(n), l(n+1))) \leq l(n+1) - l(n) - 1.$$

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

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

となったとしよう．Kurtz null test を次のように作る．$S_0 = \{\lambda\}$,

$$S_{n+1} = \{M(\sigma) \,:\, \sigma \in 2^{<l(n+1)-l(n)},\ M(\sigma) = l(n+1) - l(n)\}.$$

M は prefix-free なので，$\mu([\![S_{n+1}]\!]) \leq 2^{-1}$.

$f : \omega \to (2^{<\omega})^{<\omega}$ を次で定義する.

$$f(n) = \{x_1 \cdots x_n \ : \ x_i \in S_i \text{ for } i = 1, \cdots, n\}.$$

すると,

$$\mu([\![f(n)]\!]) = \prod_{i=1}^{n} \mu([\![S_i]\!]) \leq 2^{-n}.$$

よって, $\{[\![f(n)]\!]\}_n$ は Kurtz null test. すべての n で $A \in [\![f(n)]\!]$ であるから, A は Kurtz ランダムではない.

独立性定理

独立性定理

定理 (van Lambalge ’87)

A, B に関して以下は同値.

1. $A \oplus B$ が ML ランダム.
2. A が ML ランダム, かつ, B が A-ML ランダム.

(1)⇒(2) は, ”easy direction”

(2)⇒(1) は, ”difficult direction” と呼ばれる.

- Kolmogorov-Loveland randomnessでは弱い形で成立（Merkle-Miller-Nies-Reimann-Stephan ’06）
- 計算可能ランダムでは不成立（MMNRS ’06）
- Schnorrランダムネスでは不成立（Yu ’07）
- 一様Schnorrランダムでは成立（M. ’11, M.-Rute submitted）
- 一様計算可能ランダムでは弱い形で成立（M. ’11, M.-Rute submitted）
- Demuthランダムでは不成立，Demuth_BLRランダムでは成立（Diamondstone-Greenberg-Turetsky submitted）

Kurtzランダムネスでは？

定理 (Franklin-Stephan '11)

- A が Kurtz ランダムで，B が A-Kurtz ランダムなら，$A \oplus B$ は Kurtz ランダム．
- $A \oplus B$ は Kurtz ランダムだが，A, B は互いに Kurtz ランダムでない A, B が存在する．

つまり，"difficult direction" は成り立つが，"easy direction" は成り立たない．

一様Kurtzランダムネス

1. X が Kurtz random
   $\iff$ すべての測度 1 の c.e. 開集合に含まれる.
2. X が Kurtz random relative to A
   $\iff$ すべての測度 1 の A-c.e. 開集合に含まれる.
3. X が Kurtz random uniformly relative to A
   $\iff$ 次を満たすすべての計算可能な $f : 2^\omega \to \tau$ に関して $X \in f(A)$. すべての $Z \in 2^\omega$ に対して $\mu(f(Z)) = 1$.

easy direction

定理 (M.)

$A \oplus B$ が Kurtz ランダムならば,

B は Kurtz random uniformly relative to A.

B は Kurtz random uniformly relative to A でないとしよう.

ある計算可能な関数 $f : 2^\omega \to \tau$ が存在して,

すべての $Z \in 2^\omega$ で $\mu(f(Z)) = 1$ かつ $B \notin f(A)$.

ここで, c.e. 開集合 U を

$$U = \{X \oplus Y \ : \ Y \in f(X)\}.$$

とおくと, $\mu(U) = 1$ かつ, $A \oplus B \notin U$.

すなわち $A \oplus B$ は Kurtz ランダムではない.

定理 (Frankline and Stephan '11)

A が Kurtz ランダムかつ，B が A-Kurtz ランダムならば，

$A \oplus B$ は Kurtz ランダム.

証明

A を Kurtz ランダム，U を任意の c.e. 開集合で測度 1 のものとする.

任意の有理数 $r < 1$ に対し，

$$U_r = \{P \ : \ \mu(\{Q \ : \ P \oplus Q \in U\}) > r\}$$

とおくと，U_r は c.e. 開集合.

また任意の r に対して，$\mu(U_r) = 1$.

A は Kurtz ランダムだから，すべての r に対して $A \in U_r$.

$$T = \{Q \ : \ A \oplus Q \in U\}$$

は測度 1 の A-c.e. 開集合.

B は A-Kurtz ランダムだから，$B \in T$，すなわち $A \oplus B \in U$.

U は任意だったから，$A \oplus B$ は Kurtz ランダム.

difficult direction

定理 (M.)

A, B は互いに一様 Kurtz ランダムだが,

$A \oplus B$ は Kurtz ランダムではないような A, B が存在する.

つまり, ”easy direction”は成り立つが, ”difficult direction” は成り立たない！

定理 (木原-M.)

A, B に関して以下は同値.

1. A は Kurtz random uniformly relative to B.
2. すべての有理数値マルチンゲール $d \leq_{tt} B$ と計算可能な order h に対して，$d(A \upharpoonright n) \leq h(n)$ となる n が存在する.

命題

すべての n で $A(n) = 0$ または $B(n) = 0$ ならば，$A \oplus B$ は Kurtz ランダムではない.

すべての n で $A(n)=0$ または $B(n)=0$ とする．

すべての n で $d(A\oplus B\upharpoonright n)>h(n)$ となる計算可能なマルチンゲール d と計算可能な order h を作ろう．

$d(\lambda)=1$ かつ，任意の偶数長の σ と長さが 2 の τ に対して，

$$d(\sigma\tau)=\begin{cases}0 & \tau=11\\ \frac{4}{3} & \text{o.w.}\end{cases}$$

と定義すると，d は計算可能なマルチンゲールとなる．すると，

$$d(A\oplus B\upharpoonright 2m+i)\geq\left(\frac{4}{3}\right)^m.$$

$\{\Phi_i\}$ をすべての $Z \in 2^\omega$ に対して Φ^Z がマルチンゲールとなるようなすべての有理数値 truth-table functional Φ の数え上げとする.

また, $\{h_j\}$ を計算可能な order の数え上げとする.

各ステージ s で, $A \restriction m_s$, $B \restriction m_s$ を定義する.

s が偶数なら $A \restriction m_s = (A \restriction m_{s-1})0^{m_s - m_{s-1}}$ とし,

s が奇数なら $B \restriction m_s = (B \restriction m_{s-1})0^{m_s - m_{s-1}}$ とする.

$s = 2\langle i, j\rangle$ の時, $\Phi_i^A(B \restriction m'_s) \leq h_j(m'_s)$ となるような $m'_s \leq m_s$ が存在するように $B \restriction m_s$ を作り,

$s = 2\langle i, j\rangle + 1$ の時は, $\Phi_i^B(A \restriction m'_s) \leq h_j(m'_s)$ となるような $m'_s \leq m_s$ が存在するように $B \restriction m_s$ を作る.

$$\Phi_i^{(A\upharpoonright m_{s-1})0^\omega}(B\upharpoonright m_{s-1}) \leq h_j(n)$$

を満たす最小の $n \geq m_{s-1}$ を m'_s とする.

$B\upharpoonright m'_s$ を $B\upharpoonright m_{s-1} \preceq B\upharpoonright m'_s$ かつ

$$\Phi_i^{(A\upharpoonright m_{s-1})0^\omega}(B\upharpoonright m'_s) \leq \Phi_i^{(A\upharpoonright m_{s-1})0^\omega}(B\upharpoonright m_{s-1}) \leq h_j(m'_s)$$

を満たすように定義する. m_s を $\Phi_i^{(A\upharpoonright m_{s-1})0^\omega}(B\upharpoonright m'_s)$ の計算で使う oracle の長さと m'_s 大きい方として,

$$\begin{aligned} A\upharpoonright m_s =& (A\upharpoonright m_{s-1})0^{m_s - m_{s-1}} \\ B\upharpoonright m_s =& (B\upharpoonright m'_s)0^{m_s - m'_s} \end{aligned}$$

と定義する.

再考

- なぜ一様Kurtzランダムネスでは独立性定理が成り立たないのか？

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.

Schnorrランダムネス版

定理 (M.)

$A \in 2^\omega$ に関して以下は同値.

1. A は Schnorr ランダムでない.
2. 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，$A = x_0 x_1 x_2 \cdots$ となる.

Kurtzランダムネス版

定理 (M.)

$A \in 2^\omega$ に関して以下は同値.

1. A は Kurtz ランダムでない.
2. 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.

つまり

- A+Bで計算可能な桁数内で規則を見つけることができたとしても，A,Bそれぞれは計算可能な桁数内で桁数を見つけることができないかもしれない．
- しかし，上手く分ければ見つけられる！

計算可能な結合

定義 (M.)

$h, g : \omega \to \omega$ を計算可能な単調増加関数で

$$\omega = \{h(n) \ : \ n \in \omega\} \cup \{g(n) \ : \ n \in \omega\}$$

を満たすものとする．この時，$A, B \in 2^\omega$ に対して，$A \oplus_h B = X$ を，

$$X(h(n)) = A(n), \ X(g(n)) = B(n)$$

で定義し，そのような h, g が存在するとき，$\oplus_h$ を計算可能な結合と呼ぶ.

一様Kurtzランダムネスに対する独立性定理

定理 (M.)

$X \in 2^\omega$ に関して以下は同値.

1. X は Kurtz ランダム
2. すべての計算可能な結合 $\oplus_h$ に対し，$X = A \oplus_h B$ と置くと，A, B は互いに一様 Kurtz ランダム.