ランダムの概念が
持つべき自然な性質

日本数学会　数学基礎論および歴史

2012年9月21日　九州大学

宮部賢志

京都大学　数理解析研究所

はじめに

計算可能

- Q. 計算可能とは？
- A. Church-Turingのテーゼで
  Turingマシンの計算可能性と同一視

ランダム

- Q. ある列がランダムであるとは？
- A. Martin-Löf - Chaitinのテーゼで
  Martin-Löfランダムネスと同一視

ランダム

- Q. ある列がランダムであるとは？
- A. Martin-Löf - Chaitinのテーゼで
  Martin-Löfランダムネスと同一視

してよいのか？

これまで

- 1966年以降，主な研究対象は
  Martin-Löfランダムネスであった．
- 特に2000年代以降，他のランダムネスについても良い性質をもつことが示されてきた．
- 中でも特にSchnorrランダムネスは良い性質を持っている！

話の流れ

- Martin-Löfランダムネスはどんな性質を持つか．なぜ自然であると考えられてきたか．
- Schnorrランダムネスの欠点と見られてきたことは何であったか．どう克服されたか．
  特に独立性定理を中心に．

ランダムの概念を
定義する

どれがランダムでしょう？

- 1111111111111111111111111111111111...
- 0101010101010101010101010101010101...
- 0101110101110101010111111111111110111...
- 0010010000111111011010101000100010000...

Martin-Löf(1966)の提案

- すべての
  （ある意味で計算可能な）

統計的検定に合格する列として，
ランダムネスを定義したらどうか？

計算可能性

- 集合 $S \subseteq 2^*$ が計算可能であるとは，関係 $\sigma \in S$ が決定可能であることを言う．
- S が c.e. であるとは，$\sigma \in S$ を満たす σ を計算可能に数え上げることができることを言う．
- 実数 α に対し，$L(\alpha) = \{q \in \mathbb{Q} \ : \ q < \alpha\}$ と定義する．
- α が計算可能であるとは，$L(\alpha)$ が計算可能であることを言う．
- α が c.e. であるとは，$L(\alpha)$ が c.e. であることを言う．

Cantor空間

- Cantor 空間 2^ω
- $[\sigma] = \{A \in 2^\omega \ : \ \sigma \preceq A\}$
- 開集合 $U \subseteq 2^\omega$ が c.e. であるとは,

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

を満たす c.e. 集合 S が存在することをいう.

.

Martin-Löfランダムネス

定義 (Martin-Löf 1966)

μ を Cantor 空間上の一様測度とする.

一様に c.e. の開集合の列 $\{U_n\}$ がすべての n で $\mu(U_n) \leq 2^{-n}$ であるとき，$\{U_n\}$ を Martin-Löf テストであると言う.

列 $A \in 2^\omega$ がすべての Martin-Löf テストに対して合格する，すなわち，$A \notin \bigcap_n U_n$ であるとき，A は Martin-Löf ランダムであると言う.

Schnorrの批判

- c.e.開集合の測度はc.e.で,
  一般には計算可能ではない.
- 計算可能なものだけに制限すべきだと主張

Schnorrランダムネス

定義 (Schnorr 1971)

一様に c.e. の開集合の列 $\{U_n\}$ がすべての n で $\mu(U_n)=2^{-n}$ であるとき，$\{U_n\}$ を Schnorr テストであると言う．

列 $A \in 2^\omega$ がすべての Schnorr テストに対して合格するとき，A は Schnorr ランダムであると言う．

大数の法則と重複対数の法則

- Martin-Löfランダムネス もSchnorrランダムネスも，多くの統計的法則を満たすことが知られている.
- 例えば，どちらのランダムネスも大数の法則と重複対数の法則を満たす.

Martin-Löfランダムネス

万能テスト

あるランダムネスに対してあるテストが万能であるとは，ある列がそのテストに合格することとその列がランダムであることが同値であることを言う．

定理 (Martin-Löf 1966)

万能 Martin-Löf テストは存在する．

定理 (Schnorr 1971)

万能 Schnorr テストは存在しない．

3つの同値な定義

- 典型性　－　統計的性質
- 予測不可能性　－　マルチンゲール
- 圧縮不可能性　－　複雑性

マルチンゲール

定義

関数 $d : 2^* \to \mathbb{R}^+$ が

$$d(\sigma) = \frac{d(\sigma 0) + d(\sigma 1)}{2}$$

を満たす時，d をマルチンゲールと呼ぶ.

特徴付け

定理 (Schnorr 1971)

A が Martin-Löf ランダムであることと，すべての c.e. マルチンゲール d に対して，

$$\limsup_n d(A \upharpoonright n) < \infty$$

となることは同値である.

特徴付け

定理 (Schnorr 1971)

A が Schnorr ランダムダムであることと，すべての計算可能なマルチンゲール d と計算可能な order h に対して，

$$\limsup_n \frac{d(A \upharpoonright n)}{h(n)} < \infty$$

となることは同値である.

Kolmogorov複雑性

部分計算可能関数のことをマシンとも言う.

あるマシン $f :\subseteq 2^* \to 2^*$ が prefix-free であるとは，任意の異なる $\sigma, \tau \in \mathrm{dom}(f)$ に対し，$\sigma \not\preceq \tau$ かつ $\tau \not\preceq \sigma$ となることを言う.

定義 (Kolmogorov 複雑性)

$$K(\sigma) = \min\{|\tau| \ : \ U(\tau) = \sigma\}.$$

ここで U は万能 prefix-free マシンである.

特徴付け

定理 (Levin 1973, Schnorr 1973, Chaitin 1975)

A が Martin-Löf ランダムであることと，ある $d \in \mathbb{N}$ が存在して，すべての n に対し，

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

となることは同値である.

独立性定理

定理 (van Lambalgen 1987)

以下は同値.

- $A \oplus B$ が Martin-Löf ランダムである.
- A が Martin-Löf ランダムかつ

  B が A から見て Martin-Löf ランダムである.

.

ここまでのまとめ

	MLランダム	Schnorrランダム
万能テスト	存在する	存在しない
マルチンゲール	存在する	存在する
複雑性	存在する	?
独立性定理	成立	?

Schnorrランダムネス

最初の困難

- Schnorrランダムネスの複雑性による特徴付けは存在するか？

マシンの測度

文字列の集合 $S \subseteq 2^*$ に対し，

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

と定義し，prefix-free マシン M の測度を

$$\mu([\![\mathrm{dom}(M)]\!])$$

で定義する．

複雑性による特徴付け

定理 (Downey and Griffiths 2004)

A が Schnorr ランダムであることと，すべての計算可能な測度を持つマシン M に対して，

$$K_M(A \upharpoonright n) > n - O(1)$$

であることは同値.

次の困難

- Schnorrランダムネスに対して，
  独立性定理は成立するか？

独立性定理の不成立

定理 (Merkle et al. 2006, Yu 2007)

Schnorr ランダムネスに対しては独立性定理の一方向が成り立たない．$A \oplus B$ が Schnorr ランダムで，B が A-Schnorr ランダムでない組 A, B が存在する

積分テスト

定義

関数 $t : 2^\omega \to \mathbb{R}$ が下側半計算可能であるとは，$t^{-1}(> p)$ が $p \in \mathbb{Q}$ に関して一様に c.e. 開集合となることをいう.

関数 t が積分テストであるとは，$t : 2^\omega \to \mathbb{R}^+$ が下側半計算可能で積分可能であることをいう.

定理

A に関して以下は同値.

1. A が Martin-Löf ランダムである.
2. すべての積分テスト t に対して，$t(A) < \infty$.

独立性定理の一方向の証明

定理

$A \oplus B$ が ML ランダムならば，B は A-ML ランダムである．

証明

B は A-ML ランダムでないとする．

下側半計算可能関数 $t : 2^\omega \times 2^\omega \to \mathbb{R}^+$ が存在して，$\int t(A, Y)d\mu \leq 1$ かつ $t(A, B) = \infty$.

ここで，各 X について，$\int t(X, Y)d\mu \leq 1$ となるように制限した t を f とする．

すると $\int f(X, Y)d\mu \leq 1$ かつ $t(A, B) = \infty$ より，$A \oplus B$ は ML ランダムではない．

Schnorr積分テスト

定義

関数 t が Schnorr 積分テストであるとは，$t : 2^\omega \to \mathbb{R}^+$ が下側半計算可能で $\int t d\mu$ が計算可能であることをいう.

定理 (宮部)

A に関して以下は同値.

1. A が Schnorr ランダムである.
2. すべての Schnorr 積分テスト t に対して，$t(A) < \infty$.

一様Schnorrランダムネス

A-Schnorr 積分テスト

$\Longrightarrow$ t^A が下側半計算可能で $\int t^A d\mu$ が A 計算可能.

一様 Schnorr 積分テスト

$\Longrightarrow$ $X \mapsto t^X$ が一様下側半計算可能で $X \mapsto \int t^X d\mu$ が計算可能.

独立性定理の一方向

定理 (宮部)

$A \oplus B$ が Schnorr ランダムならば,

B は A 一様 Schnorr ランダムである.

独立性定理のもう一方向

定理 (Franklin & Stephan)

A が Schnorr ランダムかつ B が A-Schnorr ランダム

$\Longrightarrow A \oplus B$ は Schnorr ランダムである.

定理 (宮部 & Rute)

A が Schnorr ランダムかつ B が A 一様 Schnorr ランダム

$\Longrightarrow A \oplus B$ は Schnorr ランダムである.

$A \oplus B$ は ML ランダムでなく，A は ML ランダムとする．
積分テスト t があって，$t(A \oplus B) = \infty$ である．

$$f(X) = \int t(X \oplus Y) d\mu$$

とすると，f は積分テストなので，$f(A) < \infty$.

$$g(Y) = t(A \oplus Y)$$

とおくと，g は A 下側半計算可能であり，

$$\int g d\mu = f(A) < \infty \text{ かつ } g(B) = t(A \oplus B) = \infty$$

より，B は A-ML ランダムではない．

Schnorr積分テストの性質 1

命題

t を Schnorr 積分テスト，A を Schnorr ランダムとすると，

$$t(A) \leq_T A.$$

証明概略

t_n を t の計算可能近似列で，$||t - t_n||_1 \leq 2^{-2n}$ を満たすものとすれば，測度 2^{-n} の部分以外では，$|t - t_n| \leq 2^{-n}$.

Schnorr積分テストの性質２

命題

t を Schnorr 積分テストとすると，

一様な全域計算可能関数列 $\{h_n\}$ が存在して，

- 至る所，$h_n \leq t$ かつ
- A が Schnorr ランダムなら，ある n が存在して，$h_n(A) = t(A)$

正しい相対化

$R(X)$ である X から見てランダムである列の集合とする.

今, $R(\emptyset)$ が決まっているとすると, 独立性定理を満たすならば,

$$A \oplus B \in R(\emptyset) \iff A \in R(\emptyset) \text{ かつ } B \in R(A)$$

であるから，$A \in R(\emptyset)$ である A に対して，$R(A)$ はただ一つに決まる.

このことは，各ランダムの概念に対して，(実質的に) ただ一つの正しい相対化が存在することを意味する.

外のランダムネスでは？

ランダムの概念	相対化
n-ランダムネス	通常
弱2ランダムネス	部分
Demuthランダム	部分
MLランダム	通常
計算可能ランダム	一様
Schnorrランダム	一様
Kurtzランダム	一様

ランダムは使えないはず

定義 (Chaitin 1975)

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

Ω は c.e.,Martin-Löf ランダム, 停止問題と T-同値.

これほど規則的で，使える数が，ランダムであるというのは，非常に直感に反する.
このことから，自然なランダムの概念は，もっと強いランダムネスであると主張する人もいる.

やっぱりランダムは使えない

定理 (Calude and Nies 1997)

A が Schnorr ランダムならば,

$$\emptyset' \not\leq_{\mathrm{tt}} A.$$

注意

実は Kurtz ランダムネスでも同じことが成り立つ.

L^1計算可能性

定義 (Pour-El et al.; Pathak et al.)

関数 $f :\subseteq [0,1] \to \mathbb{R}$ が実効化 L^1 計算可能であるとは，有理数係数の多項式の計算可能な列 f_n が存在して，

$$\int |f - f_n| d\mu \leq 2^{-n} \text{かつ } f(x) = \lim_n f_n(x)$$

となることを言う.

定理 (Pathak et al.)

$x \in [0,1]$ が Schnorr ランダムであることと，すべての実効化 L^1 計算可能関数 f に対して $f(x)$ が存在することは同値.

解析との架け橋

定理 (宮部)

実効化 L^1 計算可能＝ 2 つの Schnorr 積分テストの差

Schnorr テスト $\Longrightarrow$Schnorr 積分テスト $\Longrightarrow L^1$ 計算可能関数

Demuthプログラム

定理 (Demuth 1975)

実数 $x \in [0,1]$ について以下は同値.

1. x は Martin-Löf ランダムである.
2. すべての有界変動な計算可能関数 $f : [0,1] \to \mathbb{R}$ に対して，f が x で微分可能.

微分定理の実効化

定理 (Pathak, Rojas and Simpson; Rute)
実数 $x \in [0,1]$ について以下は同値.

1. x は Schnorr ランダムである.
2. すべての実効化 L^1 計算可能関数 f について,

$$\frac{\int_{B(x,h)} f d\mu}{2h} \to f(x)$$

.

まとめ&その他

	MLランダム	Schnorrランダム
万能テスト	存在する	存在しない
マルチンゲール	存在する	存在する
複雑性	存在する	存在する
独立性定理	成立	成立
lowの概念	一致	一致
相性の良い関数族	弱L^1計算可能	L^1計算可能

注意

- 私は，MLランダムネスよりもSchnorrランダムネスの方が自然な概念であると主張しているのではありません！

まとめ

- MLランダムネスはSchnorrランダムネスと比較して非常によく調べられており，どちらが自然かを判断する状況にはない.
- けれどもSchnorrランダムネスはこれまで考えられてきたよりも自然な概念であることが最近分かってきた.

補足

- 「自然なランダムの概念が1つ存在する」という考え方には根拠がない.
- 状況に応じて必要なランダムの概念が変わってもよいはず.
- ランダムの概念が「自然」である必要はあるか？