ランダムの概念は
どう使えるか

数学基礎論サマースクール 2012

2012年9月4日～7日　東京工業大学

宮部賢志

京都大学　数理解析研究所

ランダムの使い方

ランダムのイメージ

- でたらめ
- 不規則
- 扱いづらい
- 使えない？

ランダムとは

- ランダムな列とは
  「わずかな列しか持たないような特殊な規則を持たない」列のことである.

- ランダムな列とは
  「多くの列が持つすべての性質を持っている」列のことである.

ランダムの使われ方

- 乱拓アルゴリズム

  →ランダムであればある性質を持っていることを利用する

テーゼ

- ランダム
  - ＝うまく振る舞う（well-behaved）
  - ＝収束

大数の法則

定理 (Borel の大数の法則 1909)

$\{X_n\}$ を $P(\{0\}) = P(\{1\}) = 1/2$ を満たす独立同分布確率変数列とする．このとき，ほとんど確実に以下が成り立つ．

$$\frac{\sum_{k=1}^{n} X_k}{n} \to \frac{1}{2}.$$

重複対数の法則

定理 (Khintchine の重複対数の法則 1924)

$\{X_n\}$ を $P(\{0\}) = P(\{1\}) = 1/2$ を満たす独立同分布確率変数列とする．このとき，ほとんど確実に以下が成り立つ．

$$\limsup_{n\to\infty} \frac{\frac{\sum_{k=1}^{n} X_k}{n} - \frac{1}{2}}{\sqrt{\frac{\ln\ln n}{2n}}} = 1.$$

ランダムの階層

定理

すべての Martin-Löf ランダムな列は大数の法則および重複対数の法則を満たす.

定理

Schnorr ランダムネスに置き換えても成り立つが，Kurtz ランダムネスに置き換えると成り立たない.

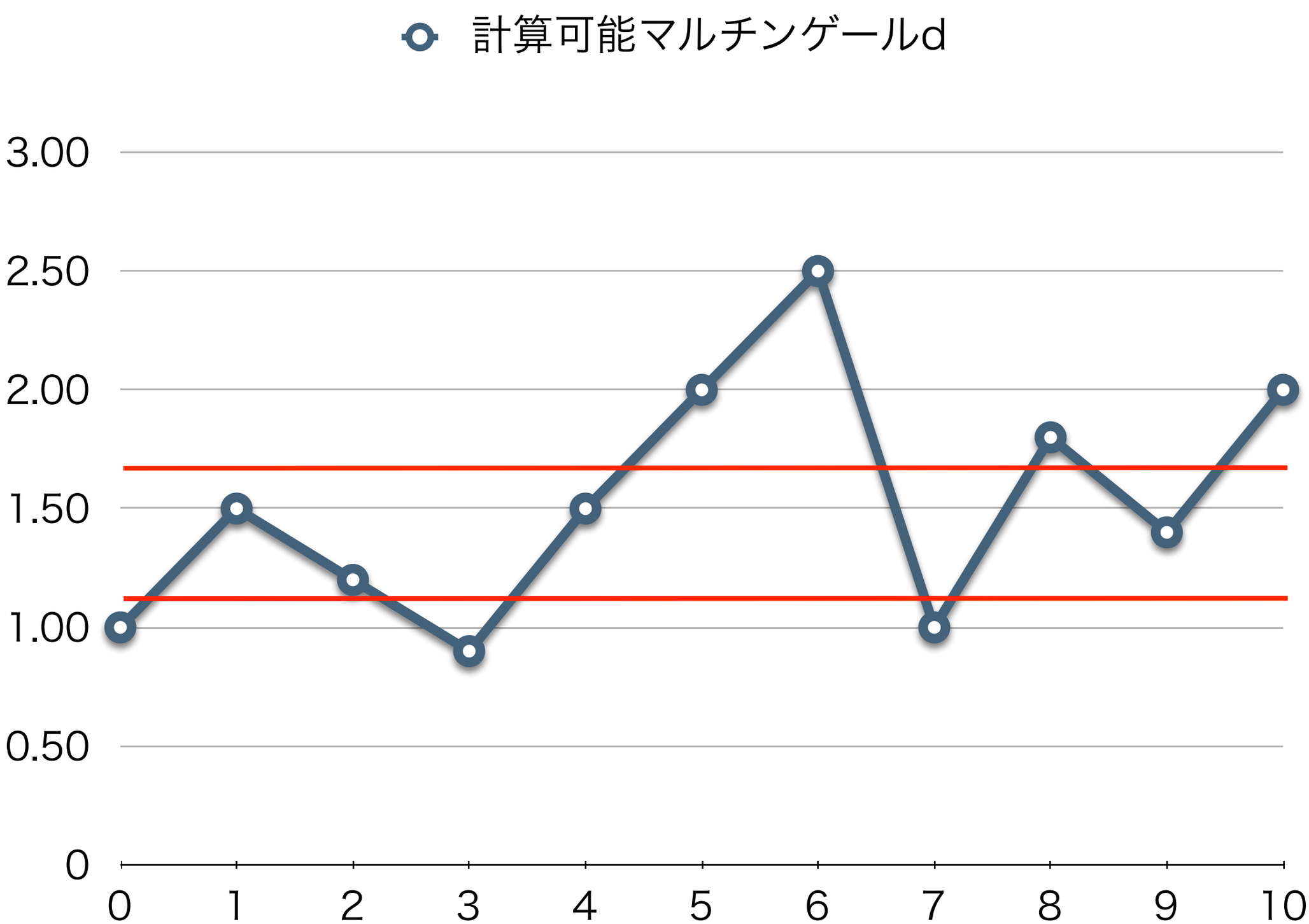
収束定理

定理 (Doob の収束定理)

$\{X_n\}$ が非負優マルチンゲールであるならば，$\lim_n X_n$ はほとんど確実に存在する.

定理 (folklore) 以下は同値.

1. $X \in 2^\omega$ が計算可能ランダム.
2. すべての計算可能マルチンゲール $d : 2^* \to \mathbb{R}^+$ に対して $\lim_n d(X \upharpoonright n)$ が存在する.

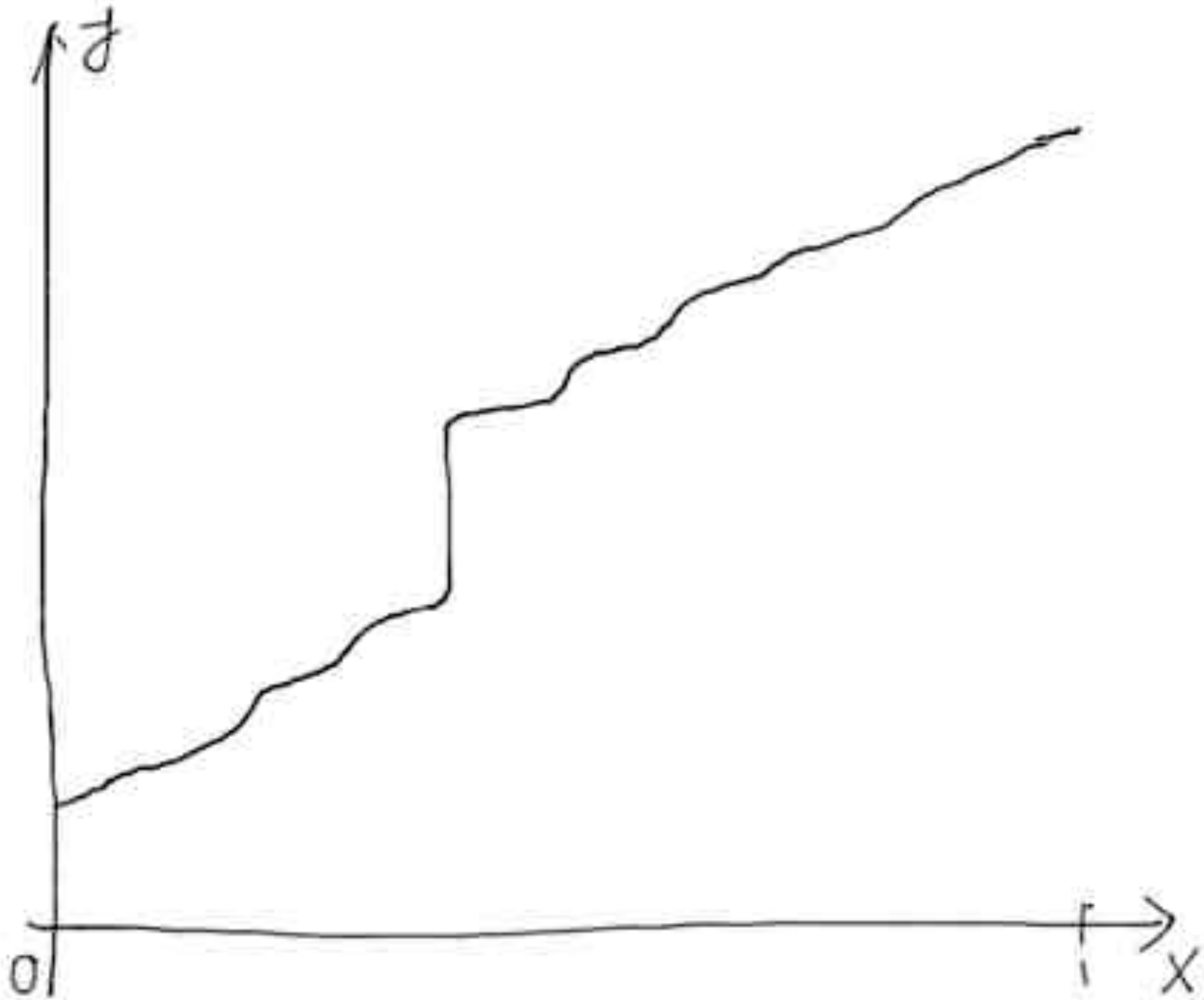

計算可能マルチンゲールd
3.00
2.50
2.00
1.50
1.00
0.50
0
0
1
2
3
4
5
6
7
8
9
10

微分可能性と
ランダムネス

Lebesgueの定理

定理 (Lebesgue 1904)

任意の単調増加関数 $f : [0, 1] \to \mathbb{R}$ はほとんど至る所微分可能.


y
0
x

Lebesgueの定理の系

定義

関数 $f : [0,1] \to \mathbb{R}$ が有界変動 (bounded variation) であるとは,

$$\sup \sum_{i=1}^{n-1} |f(t_{i+1}) - f(t_i)| < \infty.$$

ただし，$0 \leq t_1 \leq t_2 \leq \cdots \leq t_n \leq 1$.

有界変動関数は 2 つの単調増加関数の差なので,

任意の有界変動関数はほとんど至る所微分可能.

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.

Niesプログラム

弱2ランダムネス	至る所微分可能	古典的性質
MLランダムネス	有界変動	
計算可能 ランダムネス	単調 or Lipschitz	
Schnorr ランダムネス	変動ノルムで 計算可能	+計算可能性
Kurtz ランダムネス	微分が拡張実数 への計算可能	

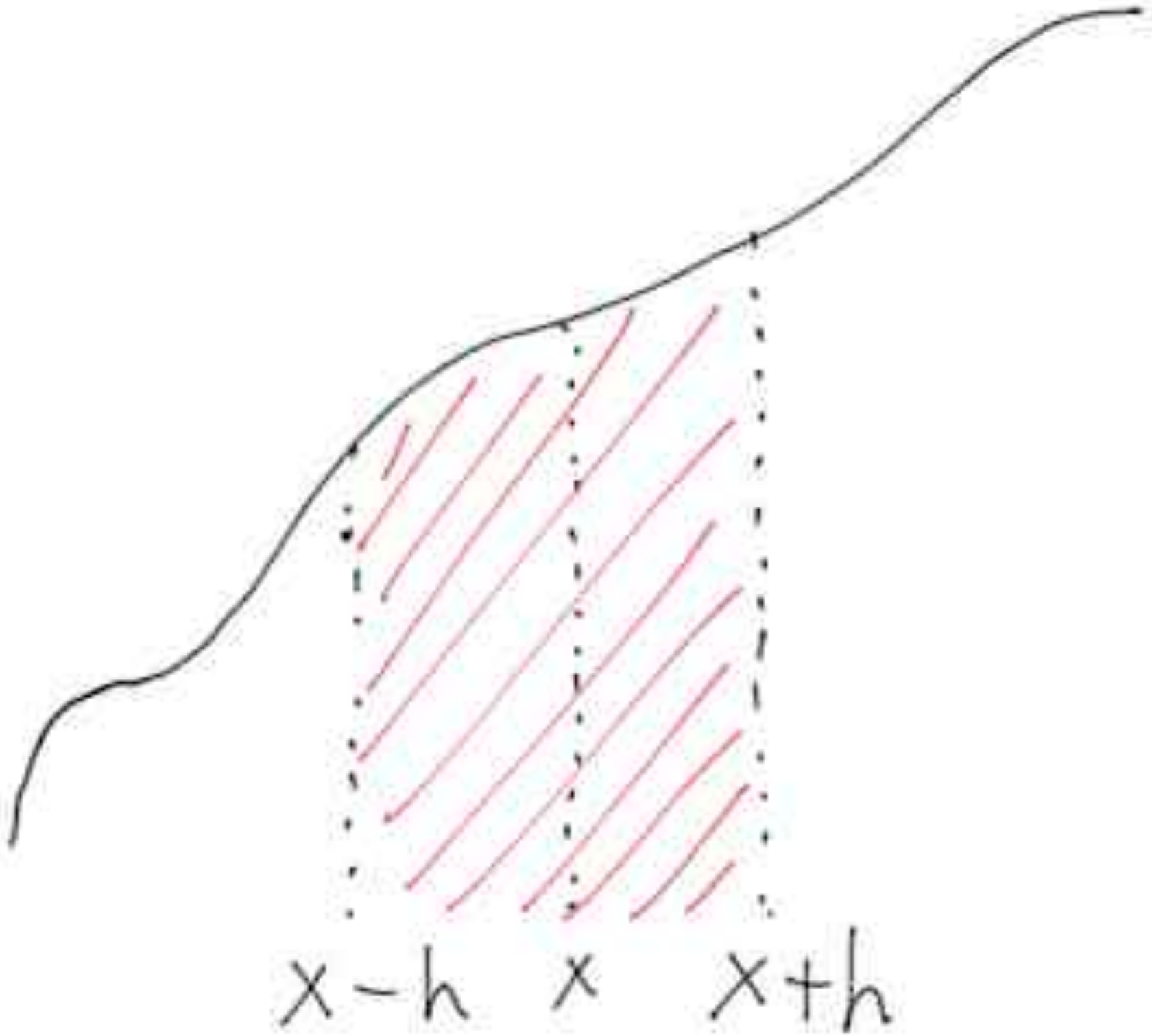
微分定理

定理 (Lebesgue 1910)

$f : [0,1] \to \mathbb{R}$ を L^1 関数とすると，ほとんど至る所の点 x で

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

ここで，$B(x,h) = (x-h, x+h)$.


x−h
x
x+h

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,

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

.

微分定理の実効化の弱い形

命題

X について以下は同値.

1. X が Schnorr ランダムである.
2. 以下を満たすような計算可能マルチンゲール M に対して，$\lim_n M(A \upharpoonright n)$ が存在する，すなわち，ある計算可能な単調増大列 $\{n_k\}$ が存在して，

$$\int |M(X \upharpoonright n_{k+1}) - M(X \upharpoonright n_k)| d\mu \leq 2^{-k}.$$

Solovayテスト

定義

Solovay テストとは，一様に c.e. 開集合の列 $\{U_n\}$ で，

$$\sum_n \mu(U_n) < \infty$$

であるものを言う.

定理

A が Martin-Löf ランダムであることと，すべての Solovay テスト $\{U_n\}$ に対して，$A \in U_n$ となる n は高々有限であることは同値.

Martin-Löf テストは Solovay テストであることから，一方向は従う.

逆を示す．ある列 A とある Solovay テスト $\{U_n\}$ があって，無限個の n で $A \in U_n$ であると仮定する.

$\sum_n \mu(U_n) \leq 1$ を仮定して良い.

$$V_m = \{X \in 2^\omega \ : \ \#\{n \ : \ X \in U_n\} \geq 2^m\}$$

とおくと，$\{V_m\}$ は一様に c.e. 開集合の列で，$\mu(V_m) \leq 2^{-m}$ であるから，ML テストであり，$A \in \bigcap_m V_m$.

Solovay for Schnorr randomness

定義

Schnorr ランダムに対する Solovay テストとは，一様に c.e. 開集合の列 $\{U_n\}$ で，

$$\sum_n \mu(U_n)$$

が計算可能であるものを言う.

定理

A が Schnorr ランダムであることと，すべての Schnorr ランダムに対する Solovay テスト $\{U_n\}$ に対して，$A \in U_n$ となる n は高々有限であることは同値.

微分定理の実効化の弱い形

命題

X について以下は同値.

1. X が Schnorr ランダムである.
2. 以下を満たすような計算可能マルチンゲール M に対して，$\lim_n M(A \upharpoonright n)$ が存在する，すなわち，ある計算可能な単調増大列 $\{n_k\}$ が存在して，

$$\int |M(X \upharpoonright n_{k+1}) - M(X \upharpoonright n_k)| d\mu \leq 2^{-k}.$$

(i)⇒(ii) A を Schnorr ランダム，M を計算可能マルチンゲールとし，命題中の式を満たす計算可能な列 $\{n_k\}$ が存在したとする．Ville の不等式より，

$$\mu(\{X \ : \max_{n_k \le n \le n_{k+1}} |M(X \upharpoonright n) - M(X \upharpoonright n_k)| > c\}) \le \frac{\int |M(X \upharpoonright n_{k+1}) - M(X \upharpoonright n_k)| d\mu}{c}.$$

$M(X \upharpoonright n) - M(X \upharpoonright n_k)$ は有限個の値しかとらないので，ある計算可能な列 $\{c_k\}$ が存在して，$2^{-k} < c_k < 2^{-k+1}$ かつ

$$U_k = \{X \ : \max_{n_k \le n \le n_{k+1}} |M(X \upharpoonright n) - M(X \upharpoonright n_k)| > c_k\}$$

が一様に計算可能になる．

U_k は一様に c.e. の開集合であり,

$$\mu(U_k) \leq \frac{2^{-2k}}{c_k} < 2^{-k}$$

であるから, $\{U_k\}$ は Schnorr テストである. A は Schnorr ランダムであるから, 有限個の k を除いて, すべての $n_k \leq n \leq n_{k+1}$ を満たす n に対し,

$$|M(A \upharpoonright n) - M(A \upharpoonright n_k)| \leq c_k < 2^{-k+1}.$$

すなわち, $\lim_n M(A \upharpoonright n)$ が存在する.

(ii)⇒(i) A は Schnorr ランダムではないとしよう．つまりある Schnorr Solovay テスト $\{[\sigma_n]\}$ に対し，無限に多くの n で $A \in [\sigma_n]$. すべての n に対し，$|\sigma_n| \leq |\sigma_{n+1}|$ を仮定する.

任意の $\sigma \in 2^*$ に対し，計算可能マルチンゲール B_σ を

$$B_\sigma(\tau) = \begin{cases} 2^{|\tau|-|\sigma|} & \tau \preceq \sigma \text{の時,} \\ 1 & \sigma \prec \tau \text{の時,} \\ 0 & \text{その他} \end{cases}$$

で定義すると，$M = \sum_n B_{\sigma_n}$ とすると，M は計算可能なマルチンゲールになる.

この M に対して上記の不等式を満たす $\{n_k\}$ を次のように定義しよう.

$$\sum_n \mu([\sigma_n])$$

は計算可能であるから，ある計算可能な列 $\{m_k\}$ が存在して,

$$\int \#\{n > m_k \ : \ X \in [\sigma_n]\} d\mu \leq 2^{-k-1}$$

となる. さらに

$$n_k = |\sigma_{m_k}|, \ M_k = \sum_{n \leq m_k} B_{\sigma_n}$$

とおく.

$$
\begin{aligned}
&|M(X \upharpoonright n_{k+1}) - M(X \upharpoonright n_k)| \\
&\qquad \leq |M(X \upharpoonright n_{k+1}) - M_k(X \upharpoonright n_k)| \\
&\qquad\qquad + |M_k(X \upharpoonright n_k) - M(X \upharpoonright n_k)|.
\end{aligned}
$$

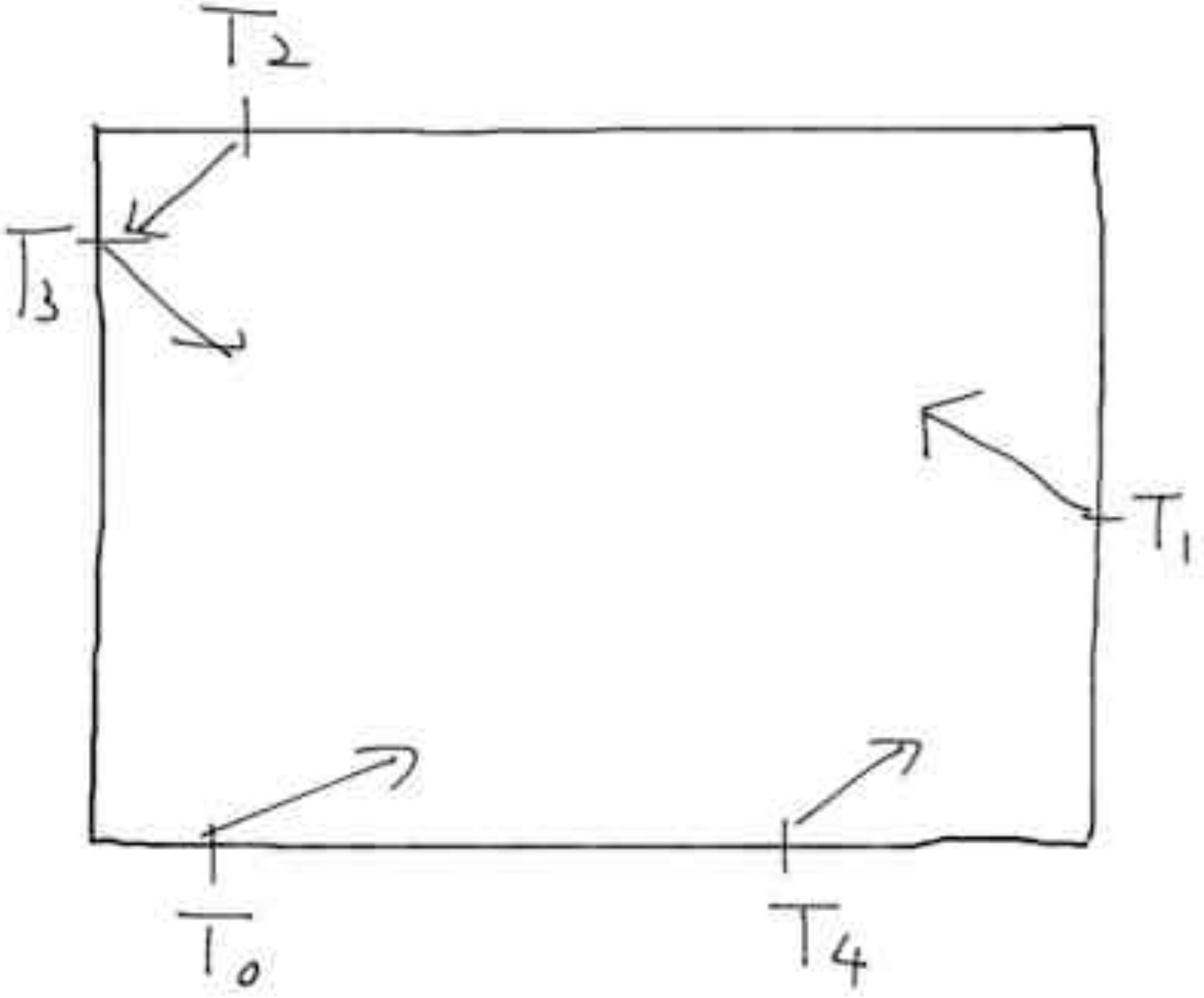
ここで $n' \in \{n_k, n_{k+1}\}$ に対して,

$$
\begin{aligned}
&\int M(X \upharpoonright n') - M_k(X \upharpoonright n_k) d\mu \\
&= \int \sum_{n > m_k} B_{\sigma_n}(X \upharpoonright n') d\mu \\
&= \int \sum_{n > m_k} B_{\sigma_n}(X \upharpoonright n_k) d\mu \\
&= \int \#\{n > m_k \ : \ X \in [\sigma_n]\} d\mu \leq 2^{-k-1}.
\end{aligned}
$$

力学系とランダムネス

Poincaréの回帰定理

- 「力学系は、ある種の条件が満たされれば、その任意の初期状態に有限時間内にほぼ回帰する」
- 「ほとんどすべての軌道が出発点の任意の近傍に無限回もどってくる」
- 「与えられた初期条件に、いくらでも近づき、かつそれを何回でも繰返すことができる」
- 出典はwikipedia参照.


T2
T3
T1
T0
T4

Poincaréの回帰定理

定理

(X, μ) を確率空間とし，$T : X \to X$ をエルゴード的関数とする．すべての正の測度を持つ $E \subseteq X$ に対して，ほとんど至る所の点 x で，無限に多くの n で $T^n(x) \in E$ となる．

定義

(X, μ) を確率空間とし，$T : X \to X$ を関数とする．$\mathcal{C}$ を X 上の可測集合族とする．点 $x \in X$ が $\mathcal{C}$ に関する T の *Poincaré* 点であるとは，すべての正の測度を持つ $E \in \mathcal{C}$ に対して，無限に多くの n で $T^n(x) \in E$ となることを言う．

Kućeraの定理

定理 (Kućera 1984)

列 A が Martin-Löf ランダムであることと，A が co-c.e. 閉集合に関するシフト演算子の Poincaré 点であることは同値である.

A を Martin-Löf ランダムでないとしよう．$\{U_n\}$ を万能 Martin-Löf テストとすると，U_1 は c.e. 開集合で

$$\mu(U_1) \leq 2^{-1} < 1$$

かつ，すべての $n \geq 1$ に対して，

$$S^n(A) \in U_1.$$

よって A は Poincaré 点ではない．

次に A を Martin-Löf ランダムとし，U を測度が 1 より小さい c.e. 開集合であるとして，無限に多くの n に対して，

$$S^n(A) \notin U$$

であることを示そう．T を c.e. prefix-free 集合で

$$U = [\![T]\!]$$

となるものとする．この時，ある k が存在して，

$$\mu([\![T^k]\!]) = (\mu([\![T]\!]))^k \leq 2^{-1}$$

である．

よって,

$$V_m = \bigcup_{l>m} [\![T^{lk}]\!]$$

とおくと，$\{V_m\}$ は Martin-Löf テストである．A は Martin-Löf ランダムであるから，ある m_0 が存在して,

$$l > m_0 \Rightarrow A \notin V_{lk} = [\![T^{lk}]\!].$$

すなわち，無限に多くの n について,

$$S^n(A) \notin [\![T]\!] = U.$$

Kućeraの定理の系

系 (Kućera 1984)

列 A が Martin-Löf ランダムでないことと，A の尾 $S^n(A)$ すべてが万能 Martin-Löf テストの第一項 U_1 に入ることは同値である.

Birkhoffのエルゴード定理

定理

(X, μ) を確率空間とし，$T : X \to X$ をエルゴード的な関数とする．f を L^1 関数とすると，ほとんど至る所の点 x で，

$$\lim_{n\to\infty} \frac{1}{n} \sum_{i<n} f(T^i(x)) = \int f d\mu.$$

Birkhoff点

定義

ある点が集合族 $\mathcal{C}$ に関する T の *Birkhoff* 点であるとは，すべての $E \in \mathcal{C}$ に対して，

$$\lim_{n\to\infty} \frac{\#\{i < n \ : \ T^i(x) \in E\}}{n} = \mu(E).$$

注意

Birkhoff 点ならば Poincaré 点である．

Birkhoff点

定理 (Gács, Hoyrup and Rojas 2011)
T を計算可能なエルゴード的関数とする．x が Schnorr ランダムであることと，x が計算可能な測度を持つ Π^1_0 集合族に対する，T の Birkhoff 点であることが同値.

定理 (Bienvenu, Day, Hoyrup, Mezhirov and Shen 2011, Franklin, Greenberg, Miller, and Ng 2012)
T を計算可能なエルゴード的関数とする．x が Martin-Löf であることと，x が Π^1_0 集合族に対する，T の Birkhoff 点であることが同値.

正規数と
計算可能な点での収束

計算可能なランダムな点

- ランダム＝収束，ではあるが，
- ランダムな点なら持つべき性質を持つ計算可能な点
- 例１）大数の法則を満たす計算可能な点
- 例２） 計算可能な正規数

例

例

大数の法則を満たす計算可能な列が存在する．例えば，

$$A = (01)^{\omega}.$$

.

正規数

定義 (Borel 1909)

$S \in \Sigma^\omega$, $w \in \Sigma^*$, $n \in \mathbb{N}$ に対し，$N_S(w,n)$ で $S \restriction n$ に w が現れる回数を表す．$S \in \Sigma^\omega$ が正規であるとは，任意の $w \in \Sigma^*$ に対し，

$$\lim_{n\to\infty} \frac{N_S(w,n)}{n} = |\Sigma|^{-|w|}$$

であることをいう．実数 x を r 進展開 $(r \geq 2)$ した時の小数点以降の文字列が正規であるとき，x は r 進正規数といい，任意の r について r 進正規数であるとき，x を単に正規数と呼ぶ．

正規数は存在する

定理 (Borel 1909)

ほとんどすべての実数は正規数.

問題 (Borel 1909)

正規数の具体例を与えよ.

10進正規数の例

例 **1.**(Champernowne 定数)

$$0.12345678910111213141516171819 20\cdots$$

例 **2.**(Copeland-Erdös 定数)

$$0.23571113171923293 1\cdots$$

問題

他の基数でも正規数か？

もっと自然な例は？

問題

以下の数は正規数か？

- π
- $\sqrt{2}$
- e
- $\log 2$

.

計算可能な正規数

定理 (Turing 1937)

計算可能な正規数は存在する.

定理

Schnorr ランダムならば正規数である. .

正規数とランダムネス

b 種類の入力での有限オートマトンによるマルチンゲールで，資金が有限にとどまる列を b-有限状態ランダムネスと呼ぶ.

定理 (Schnorr and Stimm (1972), Bourke, Hitchcock and Vinodchandran (2005))
b 進正規数であることと，b-有限状態ランダムであることは同値.

正規数を速く作る

定理

ある多項式 f が存在して，$f(n)$ 時間ランダムネスは任意の b に対し，b-有限状態ランダム．

系

多項式時間で計算できる正規数が存在する．

計算可能な点の構成

定理

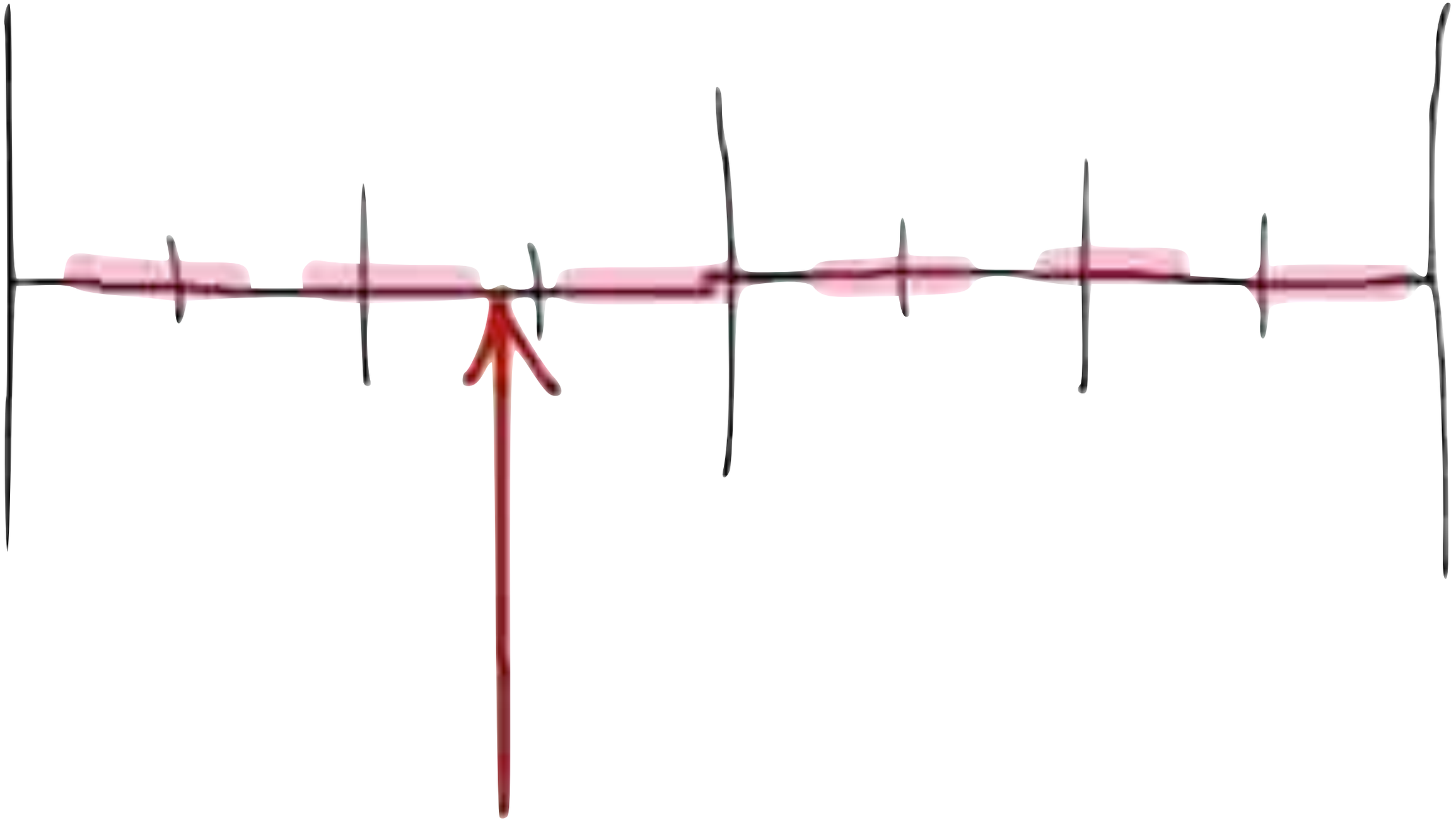
任意の計算可能マルチンゲールに対し，計算可能でそのマルチンゲールで発散しない列が存在する．

定理

任意の Schnorr テストに対し，計算可能でそのテストに合格する列が存在する．

注意

Martin-Löf ランダムネスではそのような列は構成できない．



U_1 は c.e. 開集合で $\mu(U_1) = 1/2$ を満たすとする．$A \not\in U_1$ となる計算可能な列 $A = \bigcup_n \sigma_n$ を以下のように構成する．

$\sigma_0 = \emptyset$ とする．$i \in \{0, 1\}$ に対して，どちらかは

$$\mu(U_1 \cap [i]) \leq 1/4$$

を満たすから，満たす I に対して，$\sigma_1 = i$ とする．

今，σ_n まで定まっていて，

$$\mu(U_1 \cap [\sigma_n]) \leq 2^{-n} \sum_{k=1}^{n} 2^{-k}$$

を満たしているとしよう．この時，$\mu(U_1 \cap [\sigma_n i])$ を計算することで，

$$\mu(U_1 \cap [\sigma_n i]) \leq 2^{-n-1} \sum_{k=1}^{n+1} 2^{-k}$$

を満たす i を計算可能に見つけることができて，この i に対して，$\sigma_{n+1} = \sigma_n i$ とおく．

もし，$A \in U_1$ ならば，ある n に対して，

$$[A \upharpoonright n] = [\sigma_n] \subseteq U_1$$

であるから，

$$\mu(U_1 \cap [\sigma_n]) = \mu([\sigma_n]) = 2^{-n}$$

であるはずだが，これは構成から不可能である．よって，$A \notin U_1$.