

ランダムネス入門

木原 貴行

北陸先端科学技術大学院大学 (JAIST)

独立行政法人 日本学術振興会 (JSPS)

特別研究員 PD

URL: <http://researchmap.jp/kihara>

Email: kihara.takayuki.logic@gmail.com

【最終更新】 2012 年 9 月 17 日

謝辞

本稿は、2012年9月4日から7日に開催される数学基礎論サマースクール『計算可能性とランダムネス』における筆者の講義『歪んだコインとフラクタル』の講義資料として作成されたものです。2012年度数学基礎論サマースクール幹事の只木孝太郎先生、鹿島亮先生、鈴木登志雄先生、および、講師の宮部賢志氏、樋口幸治郎氏に感謝致します。また、JAISTにてセミナーに付き合っ下さった他、講義資料作成等に助言を下された、石原哉先生、根元多佳子氏、河井達治氏、吉村和人氏、伊藤成孝氏、新井規広氏に感謝致します。

記号リスト

- $\#X$ 集合 X の濃度を表す.
- X^Y 集合 Y から集合 X への関数全体の集合. たとえば $\{0, 1\}^{\mathbb{N}}$ で自然数の無限列全体の集合を表す.
- $X^{<\mathbb{N}}$ X の元の有限列全体の集合. 各 $x \in X^{<\mathbb{N}}$ は, $x = \langle x_0, x_1, \dots, x_n \rangle$ のように表す.
 $X^{\leq n}, X^{\geq n}$ でそれぞれ長さ n 以下, n 以上の有限列を表す.
- $\langle \rangle$ 空列を表す.
- $\sigma \frown \tau$ $\sigma \in X^{<\mathbb{N}}$ と $\tau \in X^{<\mathbb{N}}$ の結合 (*concatenation*) を表す.
 τ が長さ 1 の列, つまり $\tau = \langle t \rangle$ の形だった場合, $\sigma \frown \tau$ の代わりに単に σt と書く.
- $|\sigma|$ $\sigma \in X^{<\mathbb{N}}$ のとき, $|\sigma|$ によって σ の長さを表す.
- $\alpha \upharpoonright n$ 列 $\alpha = \langle a_0, a_1, \dots \rangle$ の長さ n の始切片 $\alpha \upharpoonright n = \langle a_0, a_1, \dots, a_{n-1} \rangle$ を表す.
- \preceq 列 σ, τ に対して, $\sigma \preceq \tau$ は, σ が τ の始切片, つまり $\sigma = \tau \upharpoonright |\sigma|$ であることを意味する.
- σ^- 有限列 $\sigma \in \{0, 1\}^{\mathbb{N}}$ の最後の値を削ったもの, つまり $\sigma \upharpoonright |\sigma| - 1$ を表す.
- $[[\sigma]]$ $\sigma \in X^{<\mathbb{N}}$ が生成する開閉 (*clopen*) 集合 $[[\sigma]] = \{\alpha \in X^{\mathbb{N}} : \sigma \prec \alpha\}$ を表す.
- $[S]$ $S \subseteq X^{<\mathbb{N}}$ が生成する開 (*open*) 集合 $[S] = \bigcup_{\sigma \in S} [[\sigma]]$ を表す.
- λ 確率 $(1/2, 1/2)$ の公平なコイン投げから得られる $\{0, 1\}^{\mathbb{N}}$ 上の確率測度を表す.
- $0.\alpha$ 無限列 $\alpha \in \{0, 1\}^{\mathbb{N}}$ をある実数 $r \in (0, 1)$ の小数点以下の 2 進表記とみなしたときの値 r を表す.

目次

第 1 章	測度 = 賭博 = 圧縮	1
1.1	賭博とマルチンゲール	1
1.2	博打で大金を掴める確率	3
1.3	コレクティブと頻度説 *	5
1.4	コレクティブとマルチンゲール *	9
1.5	確率過程とマルチンゲール **	11
1.6	データを圧縮できる確率	16
第 2 章	ランダムネスとは何か	19
2.1	ランダムネスの基本定理	19
2.2	チャイティンのオメガ	23
2.3	マルチンゲール vs. マルチンゲール過程 **	24
2.4	真のランダムネスと非可測集合 **	27
第 3 章	ランダムネスとフラクタル次元	29
3.1	歪んだコインとマルチンゲール	29
3.2	歪んだコインが複数あるとき	32
3.3	偏った数列の次元	35
3.4	エントロピーとハウスドルフ次元	39
3.5	超越数論とランダムネス	41
第 4 章	ランダムネス抽出と次元論	43
4.1	フォン・ノイマンのトリック	43
4.2	次元の壁を越えるのは難しい *	45
4.3	零次元よりも低次元の世界 *	48
4.4	ランダムネスと一次元の狭間 *	48
4.5	限部/ルイス強制法	52
第 5 章	普遍零集合と強零集合	59
5.1	絶対にランダムでない無限列その 1	59
5.2	絶対にランダムでない無限列その 2	61
5.3	ランダムネスと強零集合	64

第 6 章	力学系とエントロピー	67
6.1	次元 = エントロピー = 複雑性	67
第 7 章	【付録】 計算可能性理論の予備知識	72
7.1	ボレル階層と超算術的階層	72
7.2	ハウスドルフ階層と極限的学習	77
7.3	不連続関数の階層と可測関数	78
索引		80

第 1 章

測度 = 賭博 = 圧縮

1.1 賭博とマルチンゲール

問題設定. あるカジノでコイン投げゲームが行われている. このゲームのルールは以下である.

1. 各参加者は, 自由な賭け金 X ドルを支払い, 「表」または「裏」と宣言する.
2. コインが投げられた結果と宣言が一致していれば, 賭け金の倍額 $2X$ ドルを受け取る.
3. コインが投げられた結果と宣言が異なっていたら, 賭け金は没収される.

さて, 賭博師 A 氏は, このコイン投げゲームへの必勝戦略 \mathfrak{M} を考えた. それは, 第 n 回目の挑戦では 2^n ドルを賭けることである. 永遠に負け続けるということは確率的に有り得ないから, いつか第 m 回目の挑戦で勝てるはずである. 第 m 回目までの損失総額 $\sum_{t=0}^{m-1} 2^t$ ドルと, 第 m 回目での儲け額 2^m ドルを比較すると,

$$\sum_{t=0}^{m-1} 2^t = 2^m - 1 < 2^m$$

であるから, 一回勝利するだけで, それまでの負けによる損失は取り戻せる. これを儲けたい額だけ繰り返せば, 「表」「裏」のどちらに賭けるとは全く無関係に, 目標金額を稼ぐことができるはずである.

この倍プッシュ戦略 \mathfrak{M} は, 少なくとも 18 世紀においては **マルチンゲール** (*martingale*) という名で知られていた戦略である. さて, 本当にこの戦略は破綻していないだろうか.

語源とは大幅な変貌を遂げているが, マルチンゲールは現代確率論においては, 今や基本的な概念の 1 つである. 数学用語としてマルチンゲールという名を最初に用いたのは, J. Ville である. 彼は, フォン・ミーゼスの “コレクティブ” 概念の改良として, マルチンゲールを導入した. ここでは J. Ville の時代に舞い戻り, 賭博戦略としてのマルチンゲールの定義を与える.

定義 1.1. 関数 $b: \{0, 1\}^{<\mathbb{N}} \rightarrow [-1, 1]$ を **賭博戦略** (*betting strategy*) と呼ぶ. このとき, 賭博戦略 b の下での

現在資金 (*current capital*) とは、以下のように帰納的に定義される関数 $cp_b : \{0, 1\}^{<N} \rightarrow [0, \infty)$ である。

$$\begin{aligned} cp_b(\langle \rangle) &= 1, \\ cp_b(\sigma 0) &= (1 + b(\sigma)) \cdot cp_b(\sigma), \\ cp_b(\sigma 1) &= (1 - b(\sigma)) \cdot cp_b(\sigma). \end{aligned}$$

コイン投げの結果が「表」であることを 0 とし、「裏」であることを 1 によって表そう。すると、 n 回のコイン投げの結果はある有限列 $\sigma \in \{0, 1\}^{<N}$ で表される。このとき、賭博戦略 b について、現在までのコイン投げの結果が σ であるとき、 $b(\sigma)$ の値は以下の状態を表す。

- $b(\sigma) > 0$ ならば、次のコイン投げの結果が表 (0) であることに、現在資金の $|b(\sigma)|$ 倍を賭ける。
- $b(\sigma) < 0$ ならば、次のコイン投げの結果が裏 (1) であることに、現在資金の $|b(\sigma)|$ 倍を賭ける。
- $b(\sigma) = 0$ ならば、次のコイン投げ賭博には参加しない。

Ville は、賭博戦略の資金の変動過程として、マルチンゲールを定義した。つまり、「コイン投げの結果が σ であった時点での資金は $d(\sigma)$ である」ということを表す関数 $d : \{0, 1\}^{<N} \rightarrow [0, \infty)$ がマルチンゲールである。このとき、マルチンゲールは、次のように形式的定義を与えることができる。

定義 1.2. 関数 $d : \{0, 1\}^{<N} \rightarrow [0, \infty)$ がマルチンゲール (*martingale*) であるとは、任意の $\sigma \in \{0, 1\}^{<N}$ に対して、次の条件を満たすときを指す。

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

マルチンゲール d が無限列 $\alpha \in \{0, 1\}^N$ 上勝利するとは、 $\limsup_{n \rightarrow \infty} d(\alpha \upharpoonright n) = \infty$ を満たすときを指す。マルチンゲール d が集合 $A \subseteq \{0, 1\}^N$ 上完勝するとは、 d が任意の $\alpha \in A$ 上勝利するときを言う。

命題 1.1. 関数 $d : \{0, 1\}^{<N} \rightarrow [0, \infty)$ について、次の 2 条件は同値である。

1. d はマルチンゲールである。
2. ある賭博戦略 $b : \{0, 1\}^{<N} \rightarrow [-1, 1]$ と定数 $c \in [0, \infty)$ が存在して、 $d = c \cdot cp_b$ となる。

証明. (2) \Rightarrow (1): $b : \{0, 1\}^{<N} \rightarrow [-1, 1]$ を賭博戦略とする。このとき、任意の $\sigma \in \{0, 1\}^{<N}$ に対して、 $(1 \pm b(\sigma)) \geq 0$ である。よって、 $cp_b(\sigma) \in [0, \infty)$ ならば、任意の $i \in \{0, 1\}$ について、 $cp_b(\sigma i) \geq 0$ が成立する。帰納法より、任意の $\sigma \in \{0, 1\}^{<N}$ に対して、 $cp_b(\sigma) \in [0, \infty)$ を得る。また、明らかに $2 \cdot cp_b(\sigma) = cp_b(\sigma 0) + cp_b(\sigma 1)$ であるから、 $d = c \cdot cp_b$ はマルチンゲールである。

(1) \Rightarrow (2): 初期資金 (*initial capital*) は $c = d(\langle \rangle)$ によって与えられる。賭博戦略 b は次によって定義すればよい。

$$b(\sigma) = \frac{d(\sigma 0) - d(\sigma)}{d(\sigma)}.$$

このとき、マルチンゲールの定義より $0 \leq d(\sigma 0) \leq 2 \cdot d(\sigma)$ なので、 $-1 \leq b(\sigma) \leq 1$ を満たす。帰納法によって、 $d = c \cdot cp_b$ を示す。まず、 $d(\langle \rangle) = c = c \cdot cp_b(\langle \rangle)$ である。 $d(\sigma) = c \cdot cp_b(\sigma)$ が成立していると仮定する。このとき、

$$cp_b(\sigma 0) = \left(1 + \frac{d(\sigma 0) - d(\sigma)}{d(\sigma)}\right) \cdot cp_b(\sigma) = d(\sigma) + d(\sigma 0) - d(\sigma) = d(\sigma 0)$$

であり、明らかに、 $cp_b(\sigma_1) = 2 \cdot cp_b(\sigma) - cp_b(\sigma_0) = 2 \cdot d(\sigma) - d(\sigma_0) = d(\sigma_1)$ を満たす。よって、帰納法より、 $d = c \cdot cp_b$ を得る。□

以上のように、マルチンゲールとは、何らかの賭博戦略を用いたときの資金の変動過程を表す。以後は、マルチンゲールと賭博戦略を同一視する。

結論。問題設定内における倍プッシュ戦略 \mathfrak{M} の資金の変動過程は、定義 1.2 の意味でのマルチンゲールではない。何故なら、倍プッシュ戦略を実現するためには、次のどちらかの条件が満たされなければならない。

- 無限の初期資金を持っている ($\mathfrak{M}(\langle \rangle) = \infty$)。
- 多くの状況 σ で負債を背負う ($\mathfrak{M}(\sigma) < 0$)。

この負債が無利子であるときでさえ、0% の確率で、しかし無限にある可能性で、永遠に負債が増大し続ける ($\liminf_n \mathfrak{M}(\alpha \upharpoonright n) = -\infty$) ことになる。この賭博が真に確率的であればよいが、果たして、この賭博は真に確率的に行われているだろうか。

とにかく、定義 1.2 の意味で、賭博戦略あるいはマルチンゲールとして認められるためには、負債を背負うことなく、有限の所持金の中で遣り繰りしなければならないのである。

1.2 博打で大金を掴める確率

問題設定。ある賭博師 G 氏は、1 ドルを元手に、どうにか 100 万ドル以上の大金を掴んで億万長者になりたいと考えている。このために、 G 氏はある戦略 d を頼りに、コイン投げ賭博に挑むことにした。ただし、 G 氏は、現在の持ち金が 100 万ドルを超えた瞬間に、それ以上欲張らずにゲームを打ち切るとしよう。さて、 G 氏が目的を成就できる確率はどれくらいだろうか？

注意。現実では 0.01 ドル (1 セント) が金銭の最小単位であるが、ここで取り扱うものは数学的に理想的な賭博であり、「0.0000001 ドルを賭ける」といったことも許容される。

以後、 λ によって、公平なコイン投げから得られる $\{0, 1\}^{\mathbb{N}}$ 上の積測度 $\lambda = (1/2, 1/2)^{\mathbb{N}}$ を表す。

定理 1.1 (Ville 1939). $q \geq 1$ を実数とする。 d がマルチンゲールならば、ある $n \in \mathbb{N}$ で $d(\alpha \upharpoonright n) \geq q \cdot d(\langle \rangle)$ となる α 全体の集合の λ -測度は q^{-1} 以下である。

証明。単純のために初期資金は $d(\langle \rangle) = 1$ であるとする。まず、 S を $d(\sigma) \geq q$ を満たす極小な $\sigma \in \{0, 1\}^{<\mathbb{N}}$ たちの集合として定義する。目標は、 $\lambda([S]) \leq q^{-1}$ を示すことである。このとき、

$$\lambda([S]) \cdot q = \sum_{\sigma \in S} 2^{-|\sigma|} \cdot q \leq \sum_{\sigma \in S} 2^{-|\sigma|} d(\sigma).$$

あとは、 $\sum_{\sigma \in S} 2^{-|\sigma|} d(\sigma) \leq d(\langle \rangle) = 1$ であることを示せばよい。任意の数 $k \in \mathbb{N}$ について、 $S[k] = S \cap \{0, 1\}^{<k}$ と書く。もし、任意の $k \in \mathbb{N}$ について $a_k = \sum_{\sigma \in S[k]} 2^{-|\sigma|} d(\sigma) \leq 1$ ならば、 $\lim_k a_k \leq 1$ であるから、以下を示せば十分であることが分かる。

主張. $\tau \in \{0, 1\}^{<\mathbb{N}}$ を任意の有限列とする。もし $F \subseteq \{0, 1\}^{<\mathbb{N}}$ が τ を拡張する有限列たちからなる有限 \preceq -反鎖ならば、 $\sum_{\sigma \in F} 2^{-|\sigma|} d(\sigma) \leq 2^{-|\tau|} d(\tau)$ が成立する。ここで、 $F \subseteq \{0, 1\}^{<\mathbb{N}}$ が \preceq -反鎖 (antichain) であるとは、任意の異なる $\sigma, \sigma^* \in F$ が \preceq -比較不可能であることを意味する。

F の濃度に関する帰納法によって示す。 $\#F = 1$ であるときは、たとえ τ 時点での所持金 $d(\tau)$ を元手に、以後の結果が $\sigma \succeq \tau$ のように続くという確信の下で全額賭け続けたとしても、 $d(\sigma) \leq 2^{|\sigma|-|\tau|} d(\tau)$ となることから、 $2^{-|\sigma|} d(\sigma) \leq 2^{-|\tau|} d(\tau)$ となり、主張は導かれる。

$\#F = n$ のとき主張は成立していると仮定する。 F を濃度 $n+1$ の反鎖とする。 $\tau \in F \subseteq \{\sigma : \tau \preceq \sigma\}$ なる最大の長さの有限列とする。このとき、各 $i < 2$ について $F_i = \{\sigma \in F : \tau i \preceq \sigma\}$ は濃度 n 以下である。帰納的仮定より、以下が導かれる。

$$\begin{aligned} \sum_{\sigma \in F} 2^{|\tau|-|\sigma|} d(\sigma) &= \sum_{i < 2} \sum_{\sigma \in F_i} 2^{|\tau|-|\sigma|} d(\sigma) = \sum_{i < 2} \sum_{\sigma \in F_i} \frac{1}{2} \cdot 2^{|\tau i|-|\sigma|} d(\sigma) \\ &\leq \frac{1}{2} \sum_{i < 2} d(\tau i) = d(\tau). \end{aligned}$$

両辺に $2^{-|\tau|}$ を掛けることによって、 $\sum_{\sigma \in F} 2^{-|\sigma|} d(\sigma) \leq 2^{-|\tau|} d(\tau)$ を得る。 □

定理 1.2 (Ville の定理 1939). N を $\{0, 1\}^{\mathbb{N}}$ の部分集合とする。このとき、以下の2条件は同値である。

1. N は λ -測度 0 である。
2. あるマルチンゲールが N 上完勝する。

証明. (1) \Rightarrow (2): $\lambda(N) = 0$ を仮定する。このとき、ある開集合の下降列 $\{U_n\}_{n \in \mathbb{N}}$ で、 $\lambda(U_n) = 2^{-n}$ かつ $N \subseteq \bigcap_n U_n$ なるものが存在する。初期資産 1 のうち 2^{-n} を元手にしたマルチンゲール d_n を以下の条件付確率によって定義する。

$$d_n(\sigma) = \lambda(U_n | [\sigma]) = \frac{\lambda(U_n \cap [\sigma])}{\lambda([\sigma])}.$$

この d_n は明らかに以下の条件を満たす。

- $d_n(\langle \rangle) = 2^{-n}$.
- $2d_n([\sigma]) = d_n([\sigma 0]) + d_n([\sigma 1])$.
- $U_n \subseteq \{\alpha \in \{0, 1\}^{\mathbb{N}} : \lim_n d(\alpha \upharpoonright n) = 1\}$.

よって、 $d = \sum_{n=0}^{\infty} d_n$ はマルチンゲールであり、以下の性質を満たす。

$$N \subseteq \bigcap_n U_n \subseteq \{\alpha \in \{0, 1\}^{\mathbb{N}} : \lim_n d(\alpha \upharpoonright n) = \infty\}.$$

特に、 d は N 上完勝する。

(2) \Rightarrow (1): d をマルチンゲールとする. U_n を次によって定義される開集合とする.

$$U_n = \{\alpha \in \{0, 1\}^{\mathbb{N}} : (\exists n \in \mathbb{N}) d(\alpha \upharpoonright n) \geq 2^{-n}\}.$$

明らかに, 次が満たされる.

$$\bigcap_n U_n = \{\alpha \in \{0, 1\}^{\mathbb{N}} : \lim_n d(\alpha \upharpoonright n) = \infty\}.$$

定理 1.1 によって, $\lambda(U_n) \leq 2^{-n}$ であるから, $\bigcap_n U_n$ の λ -測度が 0 であることが導かれる. \square

結論. 如何なる戦略を用いようとも, 元手となる初期資金が有限である限り, 一度も借金をせずに所持金を 100 万倍に増やせる確率は, ほんの 100 万分の 1 である. そして, 如何なる戦略を用いようとも, 元手となる初期資金が有限である限り, 一度も借金をせずに “所持金を好きなだけ増やせる確率” は, 0% なのである.

1.3 コレクティブと頻度説 *

問題設定. 次の発言に注目しよう.

「あるコインを投げたとき, 表が出る確率は 70% で, 裏が出る確率は 30% である」

ごく普通の発言であるが, この発言の厳密な意味を答えるのはそう簡単ではない. 筆者は, 様々な人に「この言葉が意味するものとは何か」と尋ねてみた. すると, 多くの人はこう答えた.

「そのコインを十分多くの回数投げれば, 表が出る頻度が 70%, 裏が出る頻度が 30% に近づく」

つまり, n を十分大きくすれば, 表の出現回数が $\frac{7}{10}n$ 回, 裏の出現回数が $\frac{3}{10}n$ 回に収束するという解答だ. ……さて, この解答は正しいだろうか. 確率とは, 極限頻度だけを表すのだろうか. 表が出る頻度が 70% に収束する速度は考えなくてよいのだろうか. そもそもコインはどのように投げられるのだろうか.

無限列 $\alpha \in \{0, 1\}^{\mathbb{N}}$ が与えられたとき, α における 0 の出現頻度 $\text{Freq}(\alpha)$ を以下によって定義する.

$$\text{Freq}(\alpha) = 1 - \lim_{n \rightarrow \infty} \frac{1}{n} \sum_{i=0}^{n-1} \alpha(i) = \lim_{n \rightarrow \infty} \frac{\#\{i < n : \alpha(i) = 0\}}{n}.$$

実数 $p \in [0, 1]$ に対し, 0 と 1 の出現確率がそれぞれ p と $1 - p$ であるような確率分布から得られる積測度 $\mu_p = (p, 1 - p)^{\mathbb{N}}$ を **バイアス p のベルヌーイ測度** (Bernoulli measure with bias p) と呼ぶ. 言い換えれば, バイアス p のベルヌーイ測度 μ_p とは, 次の関数 $m_p : \{0, 1\}^{<\mathbb{N}} \rightarrow \mathbb{R}$ から誘導される $\{0, 1\}^{\mathbb{N}}$ 上の測度である:

1. $m_p(\langle \rangle) = 1$ である.
2. 任意の $\sigma \in \{0, 1\}^{<\mathbb{N}}$ に対して, $m_p(\sigma 0) = p \cdot m_p(\sigma)$ である.
3. 任意の $\sigma \in \{0, 1\}^{<\mathbb{N}}$ に対して, $m_p(\sigma 1) = (1 - p) \cdot m_p(\sigma)$ である.

定理 1.3 (Borel の強大数の法則 1909). μ_p をバイアス p のベルヌーイ測度とする. このとき, 次の等式が成立する.

$$\mu_p(\{\alpha \in \{0, 1\}^{\mathbb{N}} : \text{Freq}(\alpha) = p\}) = 1.$$

ある 2 つの可能性 A と B があったとして, A の発生確率と B の発生確率はそれぞれどの程度だろうか. ボレルの強大数の法則の述べることは, 以下である. 仮に “ランダム” に A と B を発生させ続けたとしよう.

$$\alpha = ABAAABAAABAAABAAABBAAA\dots$$

もしこの無限系列 α が本当に “ランダム” であれば, 100% の確率で, この A と B の発生頻度 $\text{Freq}(\alpha)$ は, 実際の A と B の発生確率に等しい.

フォン・ミーゼスは, このように確率概念とは, 標本を無限に採集した結果, その極限的な頻度として得られるものだと考えた. ただし, この標本の無限列は “ランダム” に選ばれなければならない. 言い換えれば, “ランダム” という概念が与えられて初めて “確率” という概念が得られるという思想である.

このような標本のランダムな無限列のことを, フォン・ミーゼスは “コレクティブ” と呼んだ. フォン・ミーゼスはあらゆる標本空間におけるコレクティブの概念を定義したが, ここでは 0 と 1 からなる無限列に対するコレクティブのみを扱う.

定義 1.3 (フォン・ミーゼス 1919). 関数 $\Theta \subseteq \{0, 1\}^{<\mathbb{N}}$ を選出規則 (*selection rule*) と呼ぶ. 与えられた無限列 $\alpha \in \{0, 1\}^{\mathbb{N}}$ に対して, Θ による α の部分列の選出 $\alpha|_{\Theta}$ とは, $(\alpha|_{\Theta})(n) = \alpha(s_n)$ によって定義される列である. ここで, s_n は $S_{\Theta} = \{k \in \mathbb{N} : \alpha \upharpoonright k+1 \in \Theta\}$ の n 番目の要素である.

\mathcal{R} を選出規則の族とする. このとき, \mathcal{R}^{α} は S_{Θ} が無限集合であるような $\Theta \in \mathcal{R}$ 全体の族として定義される. 無限列 $\alpha \in \{0, 1\}^{\mathbb{N}}$ が \mathcal{R} に関してコレクティブ (*Kollektiv*) であるとは, 任意の $\Phi, \Phi^* \in \mathcal{R}^{\alpha}$ に対して, $\text{Freq}(\alpha|_{\Phi}) = \text{Freq}(\alpha|_{\Phi^*})$ を満たすときを指す.

J. Ville は『コレクティブ概念に対する批判的研究』において, 出現頻度が極限的には落ち着いたとしても, その途中経過において到底ランダムとは思えない偏った振舞いをするのが有り得ると述べた. すなわち, コレクティブだからといって, 以下のヒンチンの重複対数の法則 (*law of the iterated logarithm*) を満たすとは限らない. この法則は, ランダムな列における 0 と 1 の出現頻度がどの程度上下に揺らぐかについて述べる.

定理 1.4 (ヒンチンの重複対数の法則 1924).

$$\lambda \left(\left\{ \alpha \in \{0, 1\}^{\mathbb{N}} : \limsup_{n \rightarrow \infty} \frac{\sum_{i=0}^{n-1} (2\alpha(i) - 1)}{\sqrt{2n \log \log n}} = 1 \right\} \right) = 1$$

例 1.1. 0110 を無限に繰り返す列 $\beta_{0110} \in \{0, 1\}^{\mathbb{N}}$ を考えよ.

$$\beta_{0110} = 011001100110011001100110\dots$$

明らかに $\text{Freq}(\beta_{0110}) = 1/2$ であるが, 如何なる n についても, $\beta_{0110} \upharpoonright 2n$ に現れる 0 と 1 の出現回数は等

しい。実際、 $\limsup_n \sum_{i=0}^{n-1} (2\beta_{0110}(i) - 1) = 1$ と、出現頻度の揺れが安定している。このため、 β_{0110} は少なくともヒンチンの重複対数の法則を満たさないという意味では、ランダムではない。

次に、与えられた関数 $h: \mathbb{N} \rightarrow \mathbb{N}$ について、 $h(t)$ 回 0 を繰り返す; $h(t+1)$ 回 1 を繰り返す; $h(t+2)$ 回 0 を繰り返す; $h(t+3)$ 回 1 を繰り返す; という操作によって構成される列 $\gamma_h \in \{0, 1\}^{\mathbb{N}}$ を考えよ。たとえば、 $h(t) = 2t + 1$ によって表される関数の場合、 γ_{2t+1} は次のような列である。

$$\gamma_{2t+1} = 01110000011111110000000011111111111\dots$$

明らかに $\text{Freq}(\gamma_{2t+1}) = 1/2$ であるが、 $\gamma_{2t+1} \upharpoonright (2n+1)^2$ において、0 は 1 よりも $(2n+1)$ 回多く出現し、 $\gamma_{2t+1} \upharpoonright (2n)^2$ において、1 は 0 よりも $(2n)$ 回多く出現する。よって $\sum_{i=0}^{4n^2-1} (2\gamma_{2t+1}(i) - 1) = 2n$ であるため、

$$1 = \limsup_{n \rightarrow \infty} \frac{\sum_{i=0}^{n-1} (2\gamma_{2t+1}(i) - 1)}{\sqrt{n}} > \limsup_{n \rightarrow \infty} \frac{\sum_{i=0}^{n-1} (2\gamma_{2t+1}(i) - 1)}{\sqrt{2n \log \log n}}$$

となり、まだ出現頻度の揺れ幅が小さすぎるようである。

今度は $h(t) = t^2$ によって定義する。同様に $\text{Freq}(\gamma_{t^2}) = 1/2$ であるが、粗い評価をすると、適当な定数 c が存在して、

$$1 < \limsup_{n \rightarrow \infty} \frac{\sum_{i=0}^{n-1} (2\gamma_{t^2}(i) - 1)}{(c \cdot n)^{\frac{2}{3}}} < \limsup_{n \rightarrow \infty} \frac{\sum_{i=0}^{n-1} (2\gamma_{t^2}(i) - 1)}{\sqrt{2n \log \log n}}$$

が成立するので、今度は出現頻度の振動が大きくなりすぎるようである。

定理 1.5 (Ville の反例 1939). \mathcal{R} が可算集合ならば、次のような無限列 $\alpha \in \{0, 1\}^{\mathbb{N}}$ が存在する:

1. α は \mathcal{R} に関してコレクティブであり、 $\text{Freq}(\alpha) = 2^{-1}$ である。
2. α は重複対数の法則を満たさない。実際、任意の $n \in \mathbb{N}$ について、 $\sum_{k=0}^{n-1} \alpha(k) \leq n/2$ を満たす。

証明. まず、 \mathcal{R} が有限集合の場合の証明を述べる。 $\mathcal{R} = \{f_i\}_{i < b}$ とする。 $A_n = \{i < b : f_i(\alpha \upharpoonright n) = 1\}$ とする。このとき、 A_n の可能性は 2^b 種類しか存在しないため、 $\{A_n\}_{n \in \mathbb{N}}$ には重複が何度も現れる。 α は以下によって定義される。

$$\alpha(n) = \begin{cases} 0, & \text{if } \{A_m\}_{m < n} \text{ 内に } A_n \text{ は偶数回現れる,} \\ 1, & \text{if } \{A_m\}_{m < n} \text{ 内に } A_n \text{ は奇数回現れる.} \end{cases}$$

まず α に 0 を加えた後しか 1 を加えることはできないので、明らかに $\sum_{k=0}^{n-1} \alpha(k) \leq n/2$ が満たされる。 α 上無限回選出する $f_i \in \mathcal{R}$ を固定する。 $\alpha|_{f_i}$ における 0 の出現頻度が偏る状況とは、ある $i \in A \subseteq \{0, \dots, b-1\}$ が $\{A_n\}_{n \in \mathbb{N}}$ 内に奇数有限回しか現れないときに限る。そのような A の種類は 2^{b-1} 個しか存在しないため、極限的には影響を与えない。言い換えれば、 $\text{Freq}(\alpha|_{f_i}) = 1/2$ が成立する。

次に、 \mathcal{R} が無限集合の場合を考える。 $\mathcal{R} = \{f_i\}_{i \in \mathbb{N}}$ とする。ここで f_0 は、任意の $\sigma \in \{0, 1\}^{<\mathbb{N}}$ について $f_0(\sigma) = 1$ であるようなものであると仮定しても一般性を失わない。前と同様に $A_n = \{i \in \mathbb{N} : f_i(\alpha \upharpoonright n) = 1\}$ を考える。ただし、ここでは A_n の適切な有限始切片 $A_n^* = A_n \upharpoonright l_n$ を考える。最初は各 A_n の極めて小さな有限始切片だけ警戒し続けておき、徐々に警戒幅を広げていく。

まずは $l_0 = 0$ とおく。各 $j \in A_n$ は要注意である。 j の警戒幅 $\hat{l}_n(j)$ を次によって定義する。

$$\hat{l}_n(j) = \min\{l \geq j : \#\{m < n : j \in A_m^* \text{ and } l_m = l\} \leq 3^l\}.$$

つまり、各選出規則 f_j の警戒幅 l であるという状況が既に $3^l + 1$ 回以上発生しているならば、次は警戒幅 $l+1$ に移行する。このとき、 l_n は次によって定義される。

$$l_n = \min\{\hat{l}_n(j) : j \in A_n\}$$

各 $l \in \mathbb{N}$ について、高々 $l \cdot 3^l$ 個の $n \in \mathbb{N}$ について $l_n = l$ と成り得る。このとき、目的の無限列 α は、次によって定義される。

$$\alpha(n) = \begin{cases} 0, & \text{if } \{A_m^*\}_{m < n} \text{ 内に } A_n^* \text{ は偶数回現れる,} \\ 1, & \text{if } \{A_m^*\}_{m < n} \text{ 内に } A_n^* \text{ は奇数回現れる.} \end{cases}$$

まず α に 0 を加えた後しか 1 を加えることはできないので、明らかに $\sum_{k=0}^{n-1} \alpha(k) \leq n/2$ が満たされる。 α 上無限回選出する $f_i \in \mathcal{R}$ を固定する。 $\{A_{t(n)}\}_{n \in \mathbb{N}}$ を $i \in A_m$ なる A_m 全体のリストとする。 $l_n \leq i$ なる n は有限個なので、ある m 以降の任意の n で、 $i \in A_{t(n)}^*$ である。与えられた $k \in \mathbb{N}$ について、 $l_{t(n)} = k$ なる最小の n と $l_{t(n+r+1)} = k+1$ なる最小の r を固定する。

$$\sigma(k) = A_{t(m)}^* A_{t(m+1)}^* \cdots A_{t(m+r)}^*$$

k として、 $\sigma(k)(0) = A_{t(m)}^*$ なる m について、任意の $n \geq m$ で $i \in A_{t(n)}^*$ となるものを固定する。 β を $\alpha|_{f_i}$ の尾で、 $t(m)$ 以降の部分からなる無限列とする。後は、 $\text{Freq}(\beta) = 1/2$ を示せば十分である。

j を $A_{t(m+j)}^*$ が $\sigma(k+1)$ 以降のブロック $\sigma(k+s(j)+1)$ に属するような十分大きい値とする。また、 $c_i[j]$ を $\beta \upharpoonright j$ の中に現れる i の出現回数とし、 p を $\alpha|_{f_i} = \sigma \frown \beta$ なる始切片 σ の長さとする。このとき、 $c_1[j] \leq c_0[j] + p$ なので、次の不等式を得る。

$$c_1[j] \leq \frac{1}{2}(c_0[j] + c_1[j] + p).$$

この p は j に依存しない定数なので、明らかに $\text{Freq}(\beta) \geq 1/2$ を導く。また、各ブロック $\sigma(k+i)$ の中には高々 2^{k+i} 個のパターンしか現れず、このブロック内における 0 と 1 の偏りは、このパターン数以下である。したがって、

$$c_0[j] \leq c_1[j] + \sum_{i=0}^{s(j)+1} 2^{k+i} \leq c_1[j] + 2^{k+s(j)+2}.$$

これより、

$$c_1[j] \geq \frac{1}{2}(c_0[j] + c_1[j] - 2^{k+s(j)+1}).$$

以上より、次の不等式を得る。

$$\frac{c_1[j]}{c_0[j] + c_1[j]} \geq \frac{c_0[j] + c_1[j] - 2^{k+s(j)+1}}{2(c_0[j] + c_1[j])} = \frac{1}{2} - \frac{2^{k+s(j)+1}}{c_0[j] + c_1[j]}.$$

いま、 $A_{t(m+j)}^*$ が属するブロックは $\sigma(k+s(j)+1)$ なので、少なくともブロック $\sigma(k+s(j))$ を跨いでいる。一方、ブロック $\sigma(k+s(j))$ の長さは、警戒幅の定義より、少なくとも $3^{k+s(j)}$ 以上である。したがって、 $j = c_0[j] + c_1[j] \geq 3^{k+s(j)}$ を得る。このため、上の不等式の右辺は $1/2$ に収束する。よって、 $\text{Freq}(\beta) \leq 1/2$ を得る。以上より、 $\text{Freq}(\alpha|_{f_i}) = \text{Freq}(\beta) = 1/2$ が示された。 \square

結論。頻度ばかりを重視し過ぎると、別の重要な確率的法則を見逃してしまうことがあるので注意しよう。

1.4 コレクティブとマルチンゲール*

問題設定. この賭博場では、いつものように数当てゲームが行われている。賭博師 H 氏は、最近、予算配分を考えるのが面倒になってきた。このため、 H 氏は、数当てゲームの各プレイに参加するときは、常に自分の所持金のうち 60% だけを用いることにした。つまり、 H 氏の選択は次のいずれかである。

1. 次の値が 0 であることに、現在の所持金の 60% を賭ける。
2. 次の値が 1 であることに、現在の所持金の 60% を賭ける。
3. どちらにも賭けず、今回のプレイは見送る。

さて、このように戦略を変えた賭博師 H 氏であるが、かつて真面目に賭け金を思案していた時期と比べると、勝利できるパターンは真に減ってしまうだろうか。

定義 1.4. マルチンゲール $d : \{0, 1\}^{<\mathbb{N}} \rightarrow [0, \infty)$ が単純 (simple) であるとは、ある実数 $q \in [0, 1]$ が存在して、任意の $\sigma \in \{0, 1\}^{<\mathbb{N}}$ および $i \in \{0, 1\}$ について次の条件を満たすことを指す。

$$d(\sigma i) \in \{(1+q)d(\sigma), d(\sigma), (1-q)d(\sigma)\}.$$

この実数 $q \in [0, 1]$ を単純マルチンゲール d の賭け率と呼ぶ。

定理 1.6 (Ambos-Spies/Mayordomo/Wang/Zheng 1996). \mathcal{R} を選出規則の集合、 \mathcal{M} を単純マルチンゲールの集合とする。もし \mathcal{R} と \mathcal{M} が共に可算集合ならば、ある可算集合 $\mathcal{R}^* \supseteq \mathcal{R}$ と $\mathcal{M}^* \supseteq \mathcal{M}$ が存在して、無限列 $\alpha \in \{0, 1\}^{\mathbb{N}}$ に関する以下の 2 つの条件は同値となる。

1. α は \mathcal{R}^* に関してコレクティブである。
2. α 上勝利する単純マルチンゲール $d \in \mathcal{M}^*$ は存在しない。

証明. α 上勝利する賭け率 q の単純マルチンゲール d が存在したと仮定する。このとき、選出関数 f_0, f_1 を次によって定義する。

$$f_i(\sigma) = \begin{cases} 1, & \text{if } d(\sigma \frown i) > d(\sigma), \\ 0, & \text{otherwise.} \end{cases}$$

このとき、次の式が満たされる。

$$\limsup_n \frac{\#\{m < n : d(\alpha \upharpoonright m) = (1+q)d(\alpha \upharpoonright m-1)\}}{\#\{m < n : d(\alpha \upharpoonright m) = (1-q)d(\alpha \upharpoonright m-1)\}} > 1.$$

もし $\text{Freq}(\alpha|_{f_i}) = 2^{-1}$ であれば、 d の α 上 i 推測時の正答率もまた 2^{-1} に収束する。よって、任意の $i < 2$ について $\text{Freq}(\alpha|_{f_i}) = 2^{-1}$ であるとすると、上式に矛盾する。これより、 α はどちらかの f_i によって、コレクティブでないことが保証される。

このようにして、各単純マルチンゲール $d \in \mathcal{M}$ 毎に 2 つの選出規則 $f_0, f_1 \in \mathcal{R}$ を準備する。このとき、 $\Phi_0(d) = f_0$ および $\Phi_1(d) = f_1$ と書く。

α のある選出規則 f が存在して、 $\text{Freq}(\alpha|_f) \neq 1/2$ であると仮定する. 各 $k \in \mathbb{N}$ と $i < 2$ について, 単純マルチンゲール d_k^i を定義する. 与えられた $\sigma \in 2^{<\mathbb{N}}$ に対して, f が σ を選出するならば, d_k^i は次の値が i であることに現在資金の 2^{-k} を賭け, さもなくば d_k^i は勝負を見送る. 形式的には, d_k^i は以下によって定義される.

$$d_k^i(\sigma \frown j) = \begin{cases} (1 + 2^{-k}) \cdot d_k^i(\sigma), & \text{if } f(\sigma) = 1 \text{ and } j = i, \\ (1 - 2^{-k}) \cdot d_k^i(\sigma), & \text{if } f(\sigma) = 1 \text{ and } j \neq i, \\ d_k^i(\sigma), & \text{if } f(\sigma) = 0. \end{cases}$$

$(\alpha|_f) \upharpoonright n+1$ における $i < 2$ の出現回数を $c_i[n]$ と書くとする. 対称性より, $\text{Freq}(\alpha|_f) = \limsup_n c_0[n]/n > 1/2$ を仮定しても一般性を失わない. このとき, ある $\varepsilon \in (0, 2^{-1})$ が存在して, $c_0[n] > (2^{-1} + \varepsilon)n$ なる n が無限個存在する. そのような n を固定する. このとき, $(\alpha|_f) \upharpoonright n+1$ までに選出している α の最大の高さに 1 を加えたものを m_n とする. このとき, 各 $k \in \mathbb{N}$ について,

$$d_k^0(\alpha \upharpoonright m_n) = (1 + 2^{-k})^{c_0[n]} (1 - 2^{-k})^{c_1[n]} \geq (1 + 2^{-k})^{(\frac{1}{2} + \varepsilon)n} (1 - 2^{-k})^{(\frac{1}{2} - \varepsilon)n}.$$

$h(x) = (1 + x)^{(\frac{1}{2} + \varepsilon)} (1 - x)^{(\frac{1}{2} - \varepsilon)}$ とおく. いま, $d_k^0(\alpha \upharpoonright m_n) \geq (h(2^{-k}))^n$ であることに注意する. 十分大きな k について, $h(2^{-k}) > 1$ が成立することを示す. まず, 対数を取る.

$$\log h(x) = \left(\frac{1}{2} + \varepsilon\right) \log(1 + x) + \left(\frac{1}{2} - \varepsilon\right) \log(1 - x).$$

$\log h(0) = 0$ かつ導関数 $(\log h)'(x)$ は次により与えられる.

$$(\log h)'(x) = \frac{\frac{1}{2} + \varepsilon}{1 + x} - \frac{\frac{1}{2} - \varepsilon}{1 - x}.$$

よって, $(\log h)'(0) = 2\varepsilon > 0$ なので, 十分小さい $x > 0$ について, $\log(x) > 0$ であり, $h(x) > 1$ である. これより, 十分大きな $k \in \mathbb{N}$ について, $\limsup_m d_k^0(\alpha \upharpoonright m) = \infty$ が満たされる.

このように, 各選出規則 $f \in \mathcal{R}$ 毎に可算個の単純マルチンゲール $d_k^i \in \mathcal{M}$ を準備する. このとき, $\Psi_k^i(f) = d_k^i$ と書く.

以上によって, 単純マルチンゲールを選出規則に変換する写像 Φ_i および選出規則を単純マルチンゲールに変換する写像 Ψ_k^j が定義された. いま, 任意の $i, j \in \{0, 1\}$ および $k \in \mathbb{N}$ について, 以下の性質は容易に示される.

$$\begin{aligned} \Phi_j \circ \Psi_k^j(f) &= f, \\ \Phi_{1-j} \circ \Psi_k^j(f) &= \emptyset. \end{aligned}$$

このとき, $\mathcal{R}^* \supseteq \mathcal{R}$ および $\mathcal{M}^* \supseteq \mathcal{M}$ を次によって定義する.

$$\begin{aligned} \mathcal{R}^* &= \mathcal{R} \cup \{\Phi_i(d) : d \in \mathcal{M}, i \in \{0, 1\}\}, \\ \mathcal{M}^* &= \mathcal{M} \cup \{\Psi_k^j(f) : f \in \mathcal{R}^*, j \in \{0, 1\}, k \in \mathbb{N}\} \end{aligned}$$

無限列 $\alpha \in \{0, 1\}^{\mathbb{N}}$ が, ある選出規則 $f \in \mathcal{R}^*$ に対してコレクティブでないならば, ある単純マルチンゲール $\Psi_k^j(f)$ は α 上勝利する. \mathcal{M}^* の定義より, $\Psi_k^j(f) \in \mathcal{M}^*$ である. 一方, ある単純マルチンゲール $d \in \mathcal{M}^*$ が無限列 $\alpha \in \{0, 1\}^{\mathbb{N}}$ 上勝利すると仮定する. このとき, α はある選出規則 $\Phi_i(d)$ を介してコレクティブではない. もし $d \in \mathcal{M}$ ならば, 定義より $\Phi_i(d) \in \mathcal{M}$ である. もし $d \in \mathcal{M}^* \setminus \mathcal{M}$ ならば, ある選出規則 $f \in \mathcal{R}$ が存在して, $d = \Psi_k^j(f)$ となる. $\Phi_i(d)$ は空関数ではありえないから, $j = i$ であり, 次を得る.

$$\Phi_i(d) = \Phi_i \circ \Psi_k^j(f) = f \in \mathcal{R} \subseteq \mathcal{R}^*$$

最後に, \mathcal{R} と \mathcal{M} が共に可算ならば, \mathcal{R}^* と \mathcal{M}^* も共に可算である. □

系 1.1. \mathcal{M} を単純マルチンゲールの可算集合とする. このとき, 次を満たす無限列 $\alpha \in \{0, 1\}^{\mathbb{N}}$ が存在する.

1. 任意の $d \in \mathcal{M}$ について, $\limsup_n d(\alpha \upharpoonright n) < \infty$ である.
2. α は重複対数の法則を満たさない.

証明. 定理 1.6 より, ある選出規則の可算集合 \mathcal{R}^* で, もし $\alpha \in \{0, 1\}^{\mathbb{N}}$ が \mathcal{R}^* に関してコレクティブであるならば, 任意の $d \in \mathcal{M}^*$ に対して $\limsup_n d(\alpha \upharpoonright n) < \infty$ なるものを得る. よって, 定理 1.5 より, そのような α で重複対数の法則を満たさないものが存在する. \square

注意. 一方, 定理 1.2, 1.3, 1.4 より, 次の条件を満たす 1 つのマルチンゲール d が存在する.

- $\limsup_n d(\alpha \upharpoonright n) < \infty$ ならば, α は大数の法則を満たす.
- $\limsup_n d(\alpha \upharpoonright n) < \infty$ ならば, α は重複対数の法則を満たす.

結論. かつて重複対数の法則を満たさない無限列相手には負けなしだった賭博師 H 氏. しかし, 怠惰な性格が災いして, 単純な戦略しか使わなくなったことにより, H 氏は重複対数の法則を満たさないような“規則的”な無限列ですら儲けられなくなってしまったのであった.

1.5 確率過程とマルチンゲール **

問題設定. さて, このカジノに, 新しい賭博が導入されたい. 『多目賭け式コイン賭博』という名で, 従来のコイン投げ賭博と類似している. ゲームの内容は, 第 $(n+1)$ 回目のコイン投げが行われた後, 現在までのコイン投げの結果 $\alpha \upharpoonright n+1 = \langle a_0, a_1, \dots, a_n \rangle$ が何であったかを予測することである.

- **【前提条件】** 第 n 回目時点でのコイン投げ $\alpha \upharpoonright n = \langle a_0, a_1, \dots, a_{n-1} \rangle$ の後, $\alpha \upharpoonright n$ の値の予想として, t 個の候補 $C_n = \{\tau_0, \dots, \tau_{t-1}\}$ に絞っている.
- **【賭博内容】** $\alpha \upharpoonright n+1$ の値の予測として, $2t$ 個の各 $\tau_s i \in \{0, 1\}^{n+1}$ に現在の所持金を割り振る. ただし, 「『 $\alpha \upharpoonright n+1$ は $\tau_0 1, \tau_2 0, \tau_2 1$ のいずれか』であることに Y ドル賭ける」のような 多目賭けも許される が, 同じ $\tau_s i$ への重ね賭けは許されない.
言い換えれば, $\{\tau_i : \tau \in C_n, i < 2\}$ の適当な有限分割 D_0, \dots, D_u を作って, 現在の所持金のうち, それぞれ金額 Y_0, \dots, Y_u ドルを賭ける, というルールである.
- **【倍率】** 選択肢が $2t$ 個なので, 通常は, 賭け金を払った後, 正解に賭けた金額 X ドルの $2t$ 倍である $2tX$ ドルを受け取る. ただし, 多目賭けの場合は, 配当金が候補数だけ除算される. つまり, 賭け金 $\sum_{w \leq u} Y_w$ ドルを失うが, $\alpha \upharpoonright n+1 \in D_v$ であれば, $2tY_v / \#D_v$ ドルを受け取る.
- **【情報開示】** 現時点での結果 $\alpha \upharpoonright n+1$ がどの D_v に属していたかという情報だけが開示される. したがって, 一目賭けをしない限り, コイン投げの正確な結果の情報は開示されない. 現在の $\alpha \upharpoonright n+1$ の候補 $C_{n+1} = D_v$ の下で, 第 $(n+2)$ 回目のコイン投げが行われる.

一目賭けを繰り返す限りは、従来のコイン投げ賭博と何ら変化はない。しかし、多目賭けが許される分、従来のコイン投げ賭博よりも、若干、客が有利なようにも思える。カジノ運営陣は、『もっと客に有利なゲームがついに登場!』と、多目賭け式コイン投げ賭博を大々的に宣伝している。さて、従来のコイン投げ賭博と比べると、客はどの程度有利になっているのだろうか。

定義 1.5. 関数 b が多目賭博戦略であるとは、任意の $n \in \mathbb{N}$ および集合 $C \subseteq \{0, 1\}^n$ に対して、

$$b(C) = \langle \langle D_0, q_0 \rangle, \langle D_1, q_1 \rangle, \dots, \langle D_u, q_u \rangle \rangle$$

の形であるときを言う。ここで、 $\{D_v\}_{v \leq u}$ は $\{\tau i : \tau \in C_n\}$ の有限分割であり、各 $v \leq u$ について $q_v \in [0, 1]$ かつ $\sum_{v \leq u} q_v \leq 1$ を満たす。 $\langle D_v, q_v \rangle$ によって、「 $\alpha \upharpoonright n + 1 \in D_v$ であることに所持金の q_v 倍を賭ける」という宣言を表す。

多目賭博戦略 b が与えられたとき、関数 $\text{cp}_b : \{0, 1\}^{<\mathbb{N}} \rightarrow [0, \infty)$ と、各 $\sigma \in \{0, 1\}^{<\mathbb{N}}$ について、 $C_\sigma^b \subseteq \{0, 1\}^{|\sigma|}$ を帰納的に定義する。

$$\text{cp}_b(\langle \rangle) = 1, \quad C_{\langle \rangle}^b = \{\langle \rangle\}.$$

$\text{cp}_b(\sigma)$ および C_σ^b が既に定義されているとし、

$$b(C_\sigma^b) = \langle \langle D_0, q_0 \rangle, \langle D_1, q_1 \rangle, \dots, \langle D_u, q_u \rangle \rangle$$

であるとする。 $v(i)$ を $\sigma i \in D_v$ なる唯一の $v \leq u$ とする。このとき、 $C_{\sigma i}^b = D_{v(i)}$ とし、 $\text{cp}_b(\sigma i)$ は以下によって定義される。

$$\text{cp}_b(\sigma i) = \left(1 + \frac{2 \cdot \#C_\sigma^b \cdot q_{v(i)}}{\#D_{v(i)}} - \sum_{w \leq u} q_w \right) \cdot \text{cp}_b(\sigma).$$

この関数 cp を、多目賭博戦略 b の下での**現在資金** (*current capital*) と呼ぶ。現在資金に関する以下の等式が成立することは容易に分かる。

$$\text{cp}_b(\sigma) = \frac{\sum_{\tau \in C_\sigma^b} \text{cp}_b(\tau 0) + \text{cp}_b(\tau 1)}{2 \cdot \#C_\sigma^b}.$$

定義 1.6 (Hitchcock/Lutz 2006). 関数 $d : \{0, 1\}^{<\mathbb{N}} \rightarrow [0, \infty)$ が与えられているとき、各 $\sigma \in \{0, 1\}^{<\mathbb{N}}$ について、 $E_\sigma^d \subseteq \{0, 1\}^{|\sigma|}$ を以下によって定義する。

$$E_\sigma^d = \{\tau \in \{0, 1\}^{|\sigma|} : (\forall n \leq |\sigma|) d(\tau \upharpoonright n) = d(\sigma \upharpoonright n)\}.$$

関数 $d : \{0, 1\}^{<\mathbb{N}} \rightarrow [0, \infty)$ が**マルチンゲール過程** (*martingale process*) とは、任意の $\sigma \in \{0, 1\}^{<\mathbb{N}}$ について、以下の条件を満たすときを言う。

$$d(\sigma) = \frac{\sum_{\tau \in E_\sigma^d} d(\tau 0) + d(\tau 1)}{2 \cdot \#E_\sigma^d}.$$

命題 1.2. 任意のマルチンゲールは、マルチンゲール過程である。

証明. 定義より自明である。 □

命題 1.3. 関数 $d: \{0, 1\}^{<\mathbb{N}} \rightarrow [0, \infty)$ について、次の 2 条件は同値である。

1. d はマルチンゲール過程である。
2. ある多目賭博戦略 b と定数 $c \in [0, \infty)$ が存在して、 $d = c \cdot \text{cp}_b$ となる。

証明. (2) \Rightarrow (1): $d = c \cdot \text{cp}_b$ によって定義する。このとき、定義 1.5 の C_σ^b と定義 1.6 の E_σ^d を考える。与えられた同じ長さの $\sigma, \tau \in \{0, 1\}^{<\mathbb{N}}$ について、もし $C_\sigma^b = C_\tau^b$ ならば、 $\langle C_{\sigma|k}^b \rangle_{k \leq |\sigma|} = \langle C_{\tau|k}^b \rangle_{k \leq |\tau|}$ が成立する。なぜならば、 $C_{\sigma|k+1}^b$ は $C_{\sigma|k}^b$ の分割であるから、 $C_{\sigma|k+1}^b \neq C_{\tau|k+1}^b$ なる最小の k について、 $C_{\sigma|k+1}^b \cap C_{\tau|k+1}^b = \emptyset$ を得る。一方、 $C_{\sigma|k}^b$ および $C_{\tau|k}^b$ は k に関する下降列であるから、 $C_\sigma^b = C_\tau^b$ とは成り得ない。これより、もし $C_\sigma^b = C_\tau^b$ でさえあれば、 σ 上と τ 上では同じ賭博戦略を行っているので、 $E_\sigma^d = E_\tau^d$ が導かれる。よって、 E_σ^d は、ある有限個の $\sigma_0, \dots, \sigma_k$ について、 $E_\sigma^d = \bigcup_{i \leq k} C_{\sigma_i}^b$ と表される。したがって、多目賭博戦略 b の現在資金に関する等式は、 $d = c \cdot \text{cp}$ のマルチンゲール過程に関する等式を導く。

(1) \Rightarrow (2): 与えられたマルチンゲール過程 d について、 $C_\sigma^b = E_\sigma^d$ となるように賭博戦略 b を構成すればよい。いま、 $A = \{\tau i : \tau \in E_\sigma^d\}$ について、 $E_{\tau_0}^d, \dots, E_{\tau_k}^d$ が異なるような有限個の $\tau_0, \dots, \tau_k \in \{0, 1\}^{|\sigma|+1}$ が存在して、 $A = \bigcup_{i \leq k} E_{\tau_i}^d$ と書ける。このとき、適当に s_0, \dots, s_k を調整して、

$$b(E_\sigma^d) = \langle \langle E_{\tau_0}^d, s_0 \rangle, \dots, \langle E_{\tau_k}^d, s_k \rangle \rangle$$

と定義すれば、 $d = c \cdot \text{cp}_b$ となるようにできる。 □

Hitchcock/Lutz のマルチンゲール過程は、コイン投げゲームの文脈での、確率論的マルチンゲールの言い換えとして導入されたものである。定義 1.2 のマルチンゲールは、第 n 回以前のコイン投げの結果の履歴 (*bit history*) が a_0, \dots, a_n であるという条件の下での、第 $(n+1)$ コイン投げの後のギャンブラーの資産 ξ_{n+1} の期待値が、その直前の資産 ξ_n に等しいという条件を表す。一方、定義 1.6 のマルチンゲール過程は、第 n 回以前のコイン投げの履歴 (*capital history*) が $\xi_0 = c_0, \dots, \xi_n = c_n$ であるという条件の下での、第 $(n+1)$ コイン投げの後のギャンブラーの資産 ξ_{n+1} の期待値が、その直前の資産 $\xi_n = c_n$ に等しいという条件を表す。

定義 1.7. 与えられた関数 $d: \{0, 1\}^{<\mathbb{N}} \rightarrow [0, \infty)$ に対して、次によって定義される確率変数 (*random variable*) $\xi_n^d: \{0, 1\}^{\mathbb{N}} \rightarrow [0, \infty)$ を考える。

$$\xi_n^d(\alpha) = d(\alpha \upharpoonright n).$$

確率変数 ξ が与えられたとき、 $\lambda(A) > 0$ なる $A \subseteq \{0, 1\}^{\mathbb{N}}$ の下での ξ の条件付期待値 (*conditional expectation*) とは、以下によって定義される $\mathbb{E}[\xi | A]$ である。

$$\mathbb{E}[\xi | A] = \frac{1}{\lambda(A)} \int_A \xi d\lambda.$$

命題 1.4. 関数 $d: \{0, 1\}^{<\mathbb{N}} \rightarrow [0, \infty)$ がマルチンゲールであることと、任意の $\sigma \in \{0, 1\}^{<\mathbb{N}}$ について、次の条件を満たすことは同値である。

$$\mathbb{E}[\xi_{|\sigma|+1}^d | \llbracket \sigma \rrbracket] = \xi_{|\sigma|}^d.$$

証明. 任意の関数 $d: \{0, 1\}^{<\mathbb{N}} \rightarrow [0, \infty)$ および任意の $\sigma \in \{0, 1\}^{<\mathbb{N}}$ について、次の等式が成立する。

$$\mathbb{E}[\xi_{|\sigma|+1}^d | \llbracket \sigma \rrbracket] = 2^{|\sigma|} \int_{\llbracket \sigma \rrbracket} \xi_{|\sigma|+1}^d d\lambda = 2^{|\sigma|} \sum_{i < 2} 2^{-|\sigma|-1} d(\sigma i) = \frac{d(\sigma 0) + d(\sigma 1)}{2}.$$

よって、マルチンゲールであることと、この値が $d(\sigma)$ に等しいことは同値である。 □

確率論における典型的なマルチンゲールとは、以下によって定義されるものである。

定義 1.8. $\vec{\xi} = (\xi_0, \xi_1, \dots)$ を可積分確率変数の列とする。 $\vec{\xi}$ が **マルチンゲール過程** (martingale process) であるとは、任意の $n \in \mathbb{N}$ および $c_0, \dots, c_n \in \mathbb{R}$ について、次の条件を満たすことである。

$$\mathbb{E}[\xi_{n+1} \mid \xi_0^{-1}\{c_0\} \cap \dots \cap \xi_n^{-1}\{c_n\}] = c_n.$$

命題 1.5 (Hitchcock/Lutz 2006). 関数 $d : \{0, 1\}^{<\mathbb{N}} \rightarrow [0, \infty)$ がマルチンゲール過程であることと、確率変数列 $\vec{\xi}^d = (\xi_0^d, \xi_1^d, \dots)$ がマルチンゲール過程であることは同値である。

これから、多目コイン賭博の勝率、つまりマルチンゲール過程で勝利できる無限列の測度を求めよう。

補題 1.1. 関数 $d : \{0, 1\}^{<\mathbb{N}} \rightarrow [0, \infty)$ が与えられているとき、 $\{0, 1\}^{<\mathbb{N}}$ 上の同値関係 \sim_d を、定義 1.6 中の E_σ^d を用いて、以下によって定義する。

$$\sigma \sim_d \tau \iff E_\sigma^d = E_\tau^d.$$

$d : \{0, 1\}^{<\mathbb{N}} \rightarrow [0, \infty)$ をマルチンゲール過程とする。 $F \subseteq \{0, 1\}^{<\mathbb{N}}$ が \sim_d で閉じた反鎖ならば、次の不等式が成立する。

$$\sum_{\sigma \in F} 2^{-|\sigma|} d(\sigma) \leq d(\langle \rangle).$$

証明. 定理 1.1 中の主張のように、有限の F のみについて補題を示せば十分である。帰納法より、 $F \subseteq \{0, 1\}^{\leq n}$ について、補題は示されていると仮定する。いま、 $F \subseteq \{0, 1\}^{\leq n+1}$ を \sim_d で閉じた反鎖とする。このとき、

$$F^- = \{\sigma \in \{0, 1\}^n : \sigma 0 \in F \text{ or } \sigma 1 \in F\}$$

とし、 F^* を F^- の \sim_d -閉包、つまり $F^* = \bigcup_{\sigma \in F^-} E_\sigma^d$ とする。 F^* が含む各 \sim_d -同値類から代表元を1つずつ適当に選んで集めたものを F_* と書く。いま、

$$G = (F \cap \{0, 1\}^{\leq n}) \cup F_*$$

とすると、 $G \subseteq \{0, 1\}^{\leq n}$ は反鎖であり、 \sim_d で閉じている。また、 F は反鎖であるから $F \cap \{0, 1\}^{\leq n} \cap F^- = \emptyset$ であり、 F が \sim_d で閉じていることから、 $F \cap \{0, 1\}^{\leq n} \cap F_* = \emptyset$ である。この性質と帰納的仮定を組み合わせ、次の式を得る。

$$d(\langle \rangle) \geq \sum_{\sigma \in G} 2^{-|\sigma|} d(\sigma) = \sum_{\sigma \in F \cap \{0, 1\}^{\leq n}} 2^{-|\sigma|} d(\sigma) + \sum_{\sigma \in F_*} 2^{-|\sigma|} d(\sigma).$$

いま、次の不等式が成立する。

$$\begin{aligned} \sum_{\sigma \in F \cap \{0, 1\}^{n+1}} 2^{-|\sigma|} d(\sigma) &= 2^{-(n+1)} \sum_{\sigma \in F \cap \{0, 1\}^{n+1}} d(\sigma) \\ &\leq 2^{-(n+1)} \sum_{\sigma \in F^-} (d(\sigma 0) + d(\sigma 1)) \\ &\leq 2^{-(n+1)} \sum_{\sigma \in F_*} \sum_{\tau \in E_\sigma^d} (d(\tau 0) + d(\tau 1)) \\ &= 2^{-(n+1)} \sum_{\sigma \in F_*} 2 \cdot \#E_\sigma^d \cdot d(\sigma) = 2^{-n} \sum_{\sigma \in F_*} d(w). \end{aligned}$$

以上より、次のようにして、目的の不等式を得る.

$$\begin{aligned} \sum_{\sigma \in F} 2^{-|\sigma|} d(\sigma) &= \sum_{\sigma \in F \cap \{0,1\}^{\leq n}} 2^{-|\sigma|} d(\sigma) + \sum_{\sigma \in F \cap \{0,1\}^{n+1}} 2^{-|\sigma|} d(\sigma) \\ &\leq \sum_{\sigma \in F \cap \{0,1\}^{\leq n}} 2^{-|\sigma|} d(\sigma) + \sum_{\sigma \in F^*} 2^{-|\sigma|} d(\sigma) \leq d(\langle \rangle). \end{aligned}$$

よって、帰納法により、補題は示された. \square

定理 1.7 (Hitchcock/Lutz 2006). $q \geq 1$ を実数とし, $d: \{0,1\}^{<\mathbb{N}} \rightarrow [0, \infty)$ をマルチンゲール過程とする. このとき, ある $n \in \mathbb{N}$ で $d(\alpha \upharpoonright n) \geq q \cdot d(\langle \rangle)$ となる α 全体の集合の λ -測度は q^{-1} 以下である. したがって, $\{0,1\}^{\mathbb{N}}$ の部分集合 N について, 以下の 3 条件は同値である.

1. N は λ -測度 0 である.
2. あるマルチンゲールが N 上完勝する.
3. あるマルチンゲール過程が N 上完勝する.

証明. d をマルチンゲール過程とする. S を $d(\sigma) \geq q \cdot d(\langle \rangle)$ を満たす極小な $\sigma \in \{0,1\}^{<\mathbb{N}}$ たちの集合として定義する. いま, $\sigma \sim_d \tau$ ならば, $d(\sigma) = d(\tau)$ なので, S は \sim_d で閉じている. これより, 補題 1.1 を S に適用できるので, 次の不等式を得る.

$$\lambda([S]) = \sum_{\sigma \in S} 2^{-|\sigma|} \leq \sum_{\sigma \in S} \left(2^{-|\sigma|} \cdot \frac{d(\sigma)}{q \cdot d(\langle \rangle)} \right) \leq \frac{d(\langle \rangle)}{q \cdot d(\langle \rangle)} = \frac{1}{q}.$$

3 条件の同値性について, (1) と (2) の同値性は Ville の定理 1.2 であり, (2) から (3) が導かれることは命題 1.2 で見た. したがって, (3) から (1) を示せば十分である. これについては, d がマルチンゲール過程であるとき, 先ほど示したように

$$\lambda(\{\alpha \in \{0,1\}^{\mathbb{N}} : (\exists n \in \mathbb{N}) d(\alpha \upharpoonright n) \geq q \cdot d(\langle \rangle)\}) \leq \frac{1}{q}$$

であることを用いて, Ville の定理 1.2 の証明と同様の議論をすればよい. \square

結論. 多目賭け式コイン賭博にしる, どんな戦略を使おうが, 所持金を 100 万倍に増やせる確率は 100 万分の 1 であり, 所持金を 1 兆倍に増やせる確率は 1 兆分の 1 なのである. そして, 所持金を好きなだけ増やせる確率は, 0% なのである. その意味で, 従来のコイン賭博も, 多目賭け式コイン賭博も変わらない. ……が, しかし! 第 2.3 節において, 公理主義的確率論では認識できない箇所において, 「多目賭け式コイン賭博の方が, 従来のコイン賭博よりも, 真に客に有利」であることが示される.

1.6 データを圧縮できる確率

問題設定 . フォン・ミーゼスのコレクティブ概念は、重複対数の法則を満たさないなど、ランダム性概念としては欠点があった。一方、「固定したマルチンゲールではあまり儲けられない」という性質をランダム性概念とみなせば、

「ランダムな無限列は不規則であり、次の値など予測不可能だから、儲けることは不可能である」

というランダム性に関する直感を反映しており、更に、コレクティブよりも性能は良さげである。

『ランダムな無限列とは、不規則（無秩序）な無限列のことである』というスローガンを認めたとしても。ところで、規則的な列、たとえば0が一億回並ぶ列などは、「0が一億回並ぶ列」という短い言葉で表現できる。ということは、

「不規則な列は、何も法則を持たないから、短い言葉で言い換えることが不可能である」

という見解はおそらく正しいであろう。言い換えれば、『ランダム = 圧縮不可能』と提唱しよう。この提唱の正当性を確かめるために、まずは文字列を圧縮できる確率を求めてみよう。

定義 1.9 (Solomonoff 1964; Kolmogorov 1965; Levin 1971; Chaitin 1975). 部分関数 $M : \subseteq \{0, 1\}^{<\mathbb{N}} \rightarrow \{0, 1\}^{<\mathbb{N}}$ が与えられたとき、有限列 $\sigma \in \{0, 1\}^{<\mathbb{N}}$ の M に関する**コルモゴロフ複雑性** (Kolmogorov complexity) とは、以下によって定義される $C_M(\sigma)$ である。

$$C_M(\sigma) = \min(\{|\tau| : M(\tau) = \sigma\} \cup \{+\infty\}).$$

$\text{dom}(M)$ が始切片関係 \preceq に関して反鎖であるとき、 M を**接頭** (prefix-free) と呼び、 C_M の代わりに K_M という記号を用いる。無限列 $\alpha \in \{0, 1\}^{\mathbb{N}}$ が M -**圧縮不可能** (M -incompressible) であるとは、以下の条件を満たすことを言う。

$$\limsup_{n \rightarrow \infty} (n - K_M(\alpha \upharpoonright n)) < \infty.$$

言い換えれば、高々定数しか圧縮できない、すなわち $K_M(\alpha \upharpoonright n) \geq n - O(1)$ を満たすことである。

補題 1.2 (Kraft の補題 1949). 任意の関数 $S : \mathbb{N} \rightarrow \mathbb{N}$ について、次の2条件は同値である。

1. ある単射 $A : \mathbb{N} \rightarrow \{0, 1\}^{<\mathbb{N}}$ で、任意の n について $|A(n)| = S(n)$ であり、 $\text{range}(A)$ が \preceq -反鎖 $A \subseteq \{0, 1\}^{<\mathbb{N}}$ であるようなものが存在する。
2. $\sum_{n=0}^{\infty} 2^{-S(n)} \leq 1$.

条件 (2) の不等式を、 S に関する **Kraft の不等式** (Kraft's inequality) と呼ぶ。

証明. (1)⇒(2): $\text{range}(A)$ が \preceq -反鎖であることから, 次の不等式が明らかに導かれる.

$$\sum_{n=0}^{\infty} 2^{-S(n)} = \sum_n \lambda(\llbracket A(n) \rrbracket) = \lambda(\llbracket \text{range}(A) \rrbracket) \leq 1.$$

(2)⇒(1): $S(n) \leq S(n+1)$ となるように S を並び替える. $A(n) \in \{0,1\}^{<\mathbb{N}}$ として, その有理数値が $0.A(n) = \sum_{k=0}^{n-1} 2^{-S(k)}$ を満たすような長さ $S(n)$ の有限列を選べばよい. \square

以後, $\{0,1\}^{<\mathbb{N}} \times \mathbb{N}$ の要素の列 $L = \{(\sigma_n, r_n)\}_{n \in \mathbb{N}}$ を **依頼状** (*request*) と呼ぶ. 各 $(\sigma, r) \in L$ によって, 「データ σ をサイズ r まで圧縮して欲しい」という依頼を表す.

系 1.2. L を依頼状とする. このとき, 次の 2 条件は同値である.

1. ある接頭関数 M が存在して, 全ての依頼 $(\sigma, r) \in L$ について, $K_M(\sigma) \leq r$ を満たす.
2. $\sum_{(\sigma, r) \in L} 2^{-r} \leq 1$.

証明. (1)⇒(2): 依頼状 $L = \{(\sigma_n, r_n)\}_{n \in \mathbb{N}}$ が与えられているとする. $S(n) = K_M(\sigma_n)$ によって定義する. 仮定より, $S(n) = K_M(\sigma_n) \leq r_n$ である. $A(n)$ を M による σ_n の最小圧縮とする, つまり, $M(\tau) = \sigma_n$ なる最小長の τ によって $A(n)$ を定義する. このとき, 明らかに A は単射であり, $\text{range}(A) \subseteq \text{dom}(M)$ である. M は接頭関数なので, $\text{dom}(M)$ は \preceq -反鎖であり, $\text{range}(A) \subseteq \text{dom}(M)$ も同様である. よって, Kraft の補題 1.2 より, 次の不等式を得る.

$$\sum_{(\sigma, r) \in L} 2^{-r} \leq \sum_{n=0}^{\infty} 2^{-S(n)} \leq 1.$$

(2)⇒(1): $L = \{(\sigma_n, r_n)\}_{n \in \mathbb{N}}$ を Kraft の不等式を満たす依頼状とする. $S(n) = r_n$ と定義すれば, S は Kraft の不等式を満たすので, Kraft の補題 1.2 より, 単射 A を得る. このとき, $M(A(n)) = \sigma_n$ によって M を定義する. すると, A の性質より, 各 n について, 以下の不等式が満たされる.

$$K_M(\sigma_n) \leq |A(n)| = S(n) = r_n.$$

さらに, $\text{range}(A)$ が \preceq -反鎖であるから M は接頭関数である. \square

定理 1.8. N を $\{0,1\}^{\mathbb{N}}$ の部分集合とする. このとき, 以下の 2 条件は同値である.

1. N は λ -測度 0 である.
2. 全ての $\alpha \in N$ を M -圧縮するような 1 つの接頭関数 $M : \subseteq \{0,1\}^{<\mathbb{N}} \rightarrow \{0,1\}^{<\mathbb{N}}$ が存在する. つまり,

$$(\forall \alpha \in N) \limsup_{n \rightarrow \infty} (n - K_M(\alpha \upharpoonright n)) = \infty.$$

証明. (1)⇒(2): 仮定より, ある開集合列 $\{U_n\}_{n \in \mathbb{N}}$ で, $N \subseteq \bigcap_n U_n$ かつ $\lambda(U_n) \leq 2^{-n}$ なるものが存在する. 開集合 U_n を生成する反鎖 $S_n \subseteq \{0,1\}^{<\mathbb{N}}$ を取る. つまり, $U_n = [S_n] = \bigcap_{\sigma \in S_n} \llbracket \sigma \rrbracket$ である. このとき, $\sum_{\sigma \in S_n} 2^{-|\sigma|} = \lambda(U_n) \leq 2^{-n}$ であることに注意する. 後は依頼状 $L = \{(\sigma, |\sigma| - n + 1) : \sigma \in S_{2n}\}$ を書けばよい. このとき, 次の不等式が成立する.

$$\sum_{(\sigma, r) \in L} 2^{-r} = \sum_{n=0}^{\infty} \sum_{\sigma \in S_{2n}} 2^{-(|\sigma| - n + 1)} = \sum_{n=0}^{\infty} 2^{n-1} \cdot \lambda(U_{2n}) \leq \sum_{n=0}^{\infty} 2^{n-1} \cdot 2^{-2n} = 1.$$

よって、系 1.2 より、ある接頭関数 M が存在して、任意の $\sigma \in S_{2n}$ について、 $K_M(\sigma) \leq |\sigma| - n + 1$ となる。もし、 $\alpha \in N$ ならば、 $N \subseteq \bigcap_t [S_t]$ なので、任意の t について、 $\alpha \upharpoonright n_t \in S_{2t}$ となる $n_t \in \mathbb{N}$ が存在する。このとき、 $K_M(\alpha \upharpoonright n_t) \leq n_t - t + 1$ であるから、 $\limsup_{n \rightarrow \infty} (n - K_M(\alpha \upharpoonright n)) = \infty$ を得る。

(2) \Rightarrow (1): M を $\text{dom}(M)$ が反鎖であり、全ての $\alpha \in N$ を M -圧縮するようなものとする。このとき、各 $c \in \mathbb{N}$ について、次の集合 V_c を考える。

$$V_c = \{\sigma \in \{0, 1\}^{<\mathbb{N}} : K_M(\sigma) \leq |\sigma| - c\}.$$

$[V_c]$ を V_c が生成する開集合とする。つまり、 $[V_c] = \bigcup_{\sigma \in V_c} [\sigma]$ とする。仮定より、 $N \subseteq \bigcap_c [V_c]$ であるため、 $\lambda(V_c) \leq 2^{-c}$ であることを示せば十分である。もし $\sigma \in V_c$ ならば、それを記述する有限列 $p(\sigma) \in \{0, 1\}^{<\mathbb{N}}$ で、 $|p(\sigma)| \leq |\sigma| - c$ かつ $M(p(\sigma)) = \sigma$ を満たすものが存在する。これより、 $\sigma \in V_c$ について、測度に関する以下の不等式を得る。

$$\lambda([p(\sigma)]) \geq 2^{|\sigma|+c} = 2^c \cdot \lambda([\sigma]).$$

いま、 $\text{dom}(M)$ は反鎖なので、次の条件を満たす。

$$\lambda([\text{dom}(M)]) = \sum_{\sigma \in \text{dom}(M)} \lambda([\sigma]) \leq 1.$$

よって、以下の不等式が導かれる。

$$2^c \cdot \lambda([V_c]) \leq 2^c \cdot \sum_{\sigma \in V_c} \lambda([\sigma]) \leq \sum_{\sigma \in V_c} \lambda([p(\sigma)]) \leq \sum_{\sigma \in \text{dom}(M)} \lambda([\sigma]) \leq 1.$$

これより、 $\lambda([V_c]) \leq 2^{-c}$ を得る。 □

結論. 100% の確率で、どんな文字列も高々定数長しか圧縮できない。

第 2 章

ランダムネスとは何か

2.1 ランダムネスの基本定理

問題設定 . ある賭博師は問うた.

「コイン投げの結果は本当にランダムなのだろうか？」

「コイン投げの結果得られる無限列 $\alpha \in \{0, 1\}^{\mathbb{N}}$ は、ランダムなのか？」

『 α である確率』は 0% だから、ランダムに無限列を選んだら、 α であるはずがない。」

「じゃあ、どんな無限列もランダムでは有り得ないのか？」

「いや、ランダムに試行を行ったとき、本当に確率 0% の事象は発生しないのか？」

「そもそも誰がどうやって“ランダム”を実現できるのか？」

「本当に“ランダム”なんてものは存在するのか？」

「そもそも“ランダム”とは一体何なんだ？」

構成的測度論によるランダムネス

.....

(前略) 最もドラマチックな功績の一つは、マーティンレフ (1966) による。彼は、構成的測度論を用いて、具体的な無限 2 進列のランダム性に関して初めて満足のいく定義を得たのである。そのような定義の探求は、20 世紀早期の確率論の基礎的研究における主目的であった。しかし、厳格な数学的基礎付けによって示されたことは、それがあまりにも捉えがたいものであり、(マーティンレフの研究の) 20 年以上過去の時点で、そのような探求は放棄されたも同然であった。(後略)

—ジャック・ルッツ, ゲールおよび具体的な列の構成次元

.....

無限列がランダムであるとは如何なる意味であろうか。出現頻度が偏っているような無限列は到底ランダムであるとは思えないし、たとえ出現頻度が偏らずとも、等頻度への収束の仕方によっては、それはランダムであるとは認められないだろう。「大数の法則 1.3 を満たす」「重複対数の法則 1.4 を満たす」このような確率 100% で成立する法則を全て満たすような無限列であれば、誰もがそれをランダムであると承認するのではないだろうか。しかし、如何なる無限列 $\alpha \in \{0, 1\}^{\mathbb{N}}$ に対しても、「 α である確率」は 0% である—ランダムな無

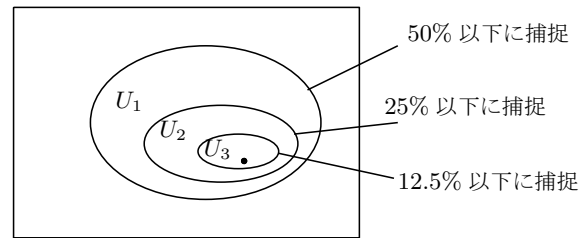


図 2.1 ランダムでないならば、マーティンレフ零集合によって捕捉される。

限列は決して α には為りえない！

だが、そもそも我々はこの α が何であるかを知らず、如何にして α について語ることが出来ようか。 α を知らずして、「 α である」などと一体どのように言及するのか。しかし、**有限の記述** e があって、それが何らかの意味で無限列 α_e を表すのであれば、「『 α_e である確率』は 0% である」という言明は、我々は実際に有限の言葉で語ることができる。このように、有限を無限に変換する規則 $e \mapsto \alpha_e$ があるならば、「 α_e である」という言及は実際に可能であるし、許されるべきだろう。

有限を無限に変換する規則の代表例は、アルゴリズムである。たとえば、素数列やフィボナッチ数列のような無限列を生成する有限長のアルゴリズムを記述することは容易であろう。また、0 と 1 の無限列であれば、たとえば円周率 π の小数点以下の値の二進表示を生成する有限長のアルゴリズムが存在する。そして、 $\{0, 1\}^{\mathbb{N}}$ の要素を適当に選んだとき、それが「 π である確率」は 0% である。よって、円周率 π はランダムな無限列ではないと結論付けてしまおう。マーティンレフが提案したことは、ランダム性概念とは、アルゴリズム概念を介して言及可能な確率 0% の条件を決して発生させないものである。

定義 2.1. 計算可能性理論の予備知識に関しては、第 7 章を見よ。集合 $V \subseteq \mathbb{N}$ が Σ_1^0 あるいは**計算的枚挙可能** (*computably enumerable*) であるとは、ある部分計算可能関数 $f : \subseteq \mathbb{N} \rightarrow \mathbb{N}$ が存在して、 $V = \text{dom}(f)$ となることを指す。 \mathbb{N} の集合列 $\{V_n\}_{n \in \mathbb{N}}$ が Σ_1^0 あるいは**計算的枚挙可能** (*computably enumerable*) であるとは、 $\{(n, x) \in \mathbb{N} \times \mathbb{N} : x \in V_n\}$ が Σ_1^0 集合であることを意味する。

定義 2.2 (マーティンレフ 1966). 集合 $N \subseteq \{0, 1\}^{\mathbb{N}}$ が**マーティンレフ零**であるとは、 $N \subseteq \bigcap_{n \in \mathbb{N}} U_n$ なる Σ_1^0 集合列 $\{U_n\}_{n \in \mathbb{N}}$ で、任意の $n \in \mathbb{N}$ について $\lambda(U_n) \leq 2^{-n}$ なるものが存在するときを言う。このとき、無限列 $\alpha \in \{0, 1\}^{\mathbb{N}}$ が**マーティンレフ・ランダム** (*Martin-Löf random*) であるとは、 $\{\alpha\}$ がマーティンレフ零集合でないときを指す。

注意. マーティンレフ・ランダムならば、計算可能選出規則たちに関してコレクティブである。それだけでなく、重複対数の法則も満たす。

圧縮不可能性によるランダムネス

第 1.6 節で述べたように、無限列がランダムであるとは、規則性を持たないということであり、言い換えれば、短い文字列に圧縮できないことであると考えられる。しかし、圧縮・解凍とは、実際のアルゴリズムと関

わるものである。したがって、計算可能関数 $M : \subseteq \{0, 1\}^{<\mathbb{N}} \rightarrow \{0, 1\}^{<\mathbb{N}}$ に関するコルモゴロフ複雑性 K_M を考察すべきであろう。

補題 2.1 (機械存在補題; Levin 1971; Schnorr 1973; Chaitin 1975). Σ_1^0 依頼状 $L \subseteq \{0, 1\}^{<\mathbb{N}} \times \mathbb{N}$ がグラフの不等式 $\sum_{(\sigma, r) \in L} 2^{-r} \leq 1$ を満たすとする。このとき、ある部分計算可能接頭関数 M が存在して、全ての依頼 $(\sigma, r) \in L$ について、長さ r のある記述 $\tau \in \{0, 1\}^r$ によって、 $M(\tau) = \sigma$ が成立する。特に、 $K_M(\sigma) \leq r$ を満たす。

証明. L は Σ_1^0 なので、 $L = \{(\sigma_i, r_i)\}_{i \in \mathbb{N}}$ と計算可能に枚挙する。反鎖 $\{\tau_n\}_{n \in \mathbb{N}}$ で、各 $n \in \mathbb{N}$ について $|\tau_n| = r_n$ なるものを計算可能な手法で構成する。各 $n \in \mathbb{N}$ について、 $\xi_n \in \{0, 1\}^{<\mathbb{N}}$ をその2進表現が次の条件を満たすものとして定義する。

$$0.\xi_n = 1 - \sum_{j=0}^n 2^{-r_j}.$$

これから、 $\xi_n(m) = 1$ なる各 $m \in \mathbb{N}$ について、補助的な有限列 $\rho_{n,m} \in \{0, 1\}^{m+1}$ を定義する。これは、 M の構成の第 n 段階時点での $\text{dom}(M)$ の利用可能領域を表し、ある $m \in \mathbb{N}$ について、 $\tau_{n+1} \succeq \rho_{n,m}$ として定義される。このとき、常に $\{\tau_k : k \leq n\} \cup \{\rho_{n,m} : \xi_n(m) = 1\}$ が反鎖となるように定義されるならば、結果として $\text{dom}(M)$ が反鎖となることが示される。

構成の第1段階として、 $\tau_0 = 0^{r_0}$ によって定義する。このとき、次が分かる。

$$\begin{aligned} 2^{-r_0} &= \underbrace{0.000\dots 000}_r 1, \\ 0.\xi_0 &= \underbrace{0.111\dots 111}_r. \end{aligned}$$

各 $m < r_0$ について、 $\rho_{0,m} = 0^m 1$ によって定義する。 $\{\tau_0\} \cup \{\rho_{0,m} : \xi_0(m) = 1\}$ が反鎖であることは明らかである。いま、反鎖 $\{\tau_k : k \leq n\} \cup \{\rho_{n,m} : \xi_n(m) = 1\}$ が既に構成されていると仮定する。

r_{n+1} が与えられたとき、 $0.\xi_{n+1} = 0.\xi_n - 2^{-r_{n+1}}$ なので、もし、 $\xi_n(r_{n+1} - 1) = 1$ ならば、 ξ_{n+1} は ξ_n の第 $r_{n+1} - 1$ 桁目を0に切り替えたものである。つまり、

$$\begin{aligned} \xi_n &= \langle x_0, x_1, x_2, x_3, \dots, x_{r_{n+1}-2}, \mathbf{1}, x_{r_{n+1}}, \dots \rangle, \\ \xi_{n+1} &= \langle x_0, x_1, x_2, x_3, \dots, x_{r_{n+1}-2}, \mathbf{0}, x_{r_{n+1}}, \dots \rangle. \end{aligned}$$

である。このとき、 $\tau_{n+1} = \rho_{n, r_{n+1}-1}$ とする。

一方、 $\xi_n(r_{n+1} - 1) = 0$ ならば、 $\xi_n(j) = 1$ なる最大の $j < r_{n+1}$ に対して、 ξ_n の第 j 桁目を0に、 $j+1$ 以上 r_{n+1} 未満の桁を1に切り替えたものが ξ_{n+1} である。つまり、

$$\begin{aligned} \xi_n &= \langle x_0, x_1, \dots, x_{j-1}, \mathbf{1}, 0, 0, 0, \dots, 0, 0, 0, \mathbf{0}, x_{r_{n+1}}, \dots \rangle, \\ \xi_{n+1} &= \langle x_0, x_1, \dots, x_{j-1}, \mathbf{0}, 1, 1, 1, \dots, 1, 1, 1, \mathbf{1}, x_{r_{n+1}}, \dots \rangle. \end{aligned}$$

となる。このとき、 $\tau_{n+1} = \rho_{n,j} \hat{\sim} 0^{r_{n+1}-j}$ と定義し、各自然数 $m \in [j, r_{n+1})$ に対して、 $\rho_{n+1,m} = \rho_{n,j} \hat{\sim} 0^{m-j} 1$ と定義する。 $\{\tau_k : k \leq n+1\} \cup \{\rho_{n+1,m} : \xi_{n+1}(m) = 1\}$ が反鎖となっていることは明らかである。

計算可能接頭関数 M を $M(\tau_n) = \sigma_n$ によって定義する。このとき、 $\text{dom}(M)$ は反鎖である。加えて、 $|\tau_n| = r_n$ であることから、 $K_M(\sigma) \leq r_n$ であることが従う。□

補題 2.2. $M : \subseteq \{0, 1\}^{\mathbb{N}} \rightarrow \{0, 1\}^{\mathbb{N}}$ が部分計算可能接頭関数ならば, $\{(\sigma, r) \in \{0, 1\}^{<\mathbb{N}} \times \mathbb{N} : K_M(\sigma) \leq r\}$ は Σ_1^0 である.

証明. $K_M(\sigma) \leq r$ であることは, $M(\tau) = \sigma$ なる長さ r 以下の $\tau \in \{0, 1\}^{<\mathbb{N}}$ が存在することと同値である. □

チューリングによる万能機械の存在定理は, 計算する対象毎に計算機を作り上げる代わりに, 1つのコンピュータの内部であらゆる計算が実現できることを述べる. つまり, 殆どの人の手許にあるコンピュータこそが, まさにチューリングによって存在の示された万能機械である. 次の命題は, データ圧縮に関しても同様の事実が成立することを述べる.

命題 2.1 (万能機械の存在). 次のような部分計算可能接頭関数 $M : \subseteq \{0, 1\}^{\mathbb{N}} \rightarrow \{0, 1\}^{\mathbb{N}}$ が存在する: 任意の部分計算可能接頭関数 $N : \subseteq \{0, 1\}^{\mathbb{N}} \rightarrow \{0, 1\}^{\mathbb{N}}$ に対して,

$$(\exists c_N \in \mathbb{N})(\forall \sigma \in \{0, 1\}^{<\mathbb{N}}) K_N(\sigma) \leq K_M(\sigma) + c$$

が成立する.

証明. $\{M_e\}_{e \in \mathbb{N}}$ を部分計算可能接頭関数全体の計算可能なリストとする. 各 $e \in \mathbb{N}$ および $\tau \in \{0, 1\}^{<\mathbb{N}}$ に対して $M(0^e \frown \tau) = M_e(\tau)$ によって定義する. このとき, M は部分計算可能接頭関数であり, 任意の $\sigma \in \{0, 1\}^{<\mathbb{N}}$ に対して $K_M(\sigma) \leq K_{M_e}(\sigma) + e$ が満たされる. □

以後, 命題 2.1 のような部分計算可能接頭関数 $M = M : \subseteq \{0, 1\}^{\mathbb{N}} \rightarrow \{0, 1\}^{\mathbb{N}}$ を固定し, 以後, K_M の代わりに単に K と書く.

マルチンゲールによるランダムネス

もし, $\alpha = \langle \alpha(0), \alpha(1), \dots \rangle$ がランダムに得られた無限列であるならば, $\alpha(n)$ の値は, これまでに与えられた系列 $\alpha \upharpoonright n = \langle \alpha(0), \alpha(1), \dots, \alpha(n-1) \rangle$ からは無関係なものであるに違いない. ならば, たとえ $\alpha \upharpoonright n$ までの値を知っていたとしても, $\alpha(n)$ の値を予測することは出来ないであろう. つまり, ランダム性とは, 次の値が何であるかの予測不可能性として与えられる.

マーティンレフの視点は『ランダム = 100%』に基づく一方, ソロモノフおよびシュノアの視点は『ランダム = 不規則』である. どちらも「ランダムネスとは何か」という疑問に対する, それぞれの自然なイメージを反映している. しかし, 100%の確率を発生させることと, 不規則であることに, 具体的には如何なる関係があるだろうか.

定理 2.1 (Schnorr 1971, 1973). 任意の無限列 $\alpha \in \{0, 1\}^{\mathbb{N}}$ について, 以下の3条件は同値である.

1. α はマーティンレフ・ランダムである.
2. α 上勝利する下半計算可能マルチンゲールは存在しない.
3. $\lim_{n \rightarrow \infty} (n - K(\alpha \upharpoonright n)) = \infty$.

証明. (1) \Leftrightarrow (2): 定理 1.2 と同じ証明が通用する. つまり, “ $\neg(1) \Rightarrow \neg(2)$ ” の証明は, 定理 1.2 の “(1) \Rightarrow (2)” の証明を模倣し, “ $\neg(2) \Rightarrow \neg(1)$ ” の証明は, 定理 1.2 の “(2) \Rightarrow (1)” の証明を模倣する. ここで, 計算可能性の条

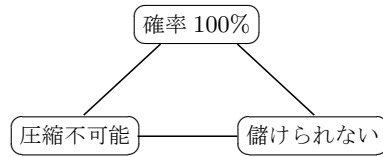


図 2.2 様々な発想に基づくランダム性概念は、実際には三位一体であり、一つ概念を別の視点に投影したものに他ならない (Schnorr 1971, 1973)

件を満たすためには、前者の証明においては条件付確率 $\lambda(U_n | \llbracket \sigma \rrbracket)$ が下半計算可能であることを注意する。

(1) \Leftrightarrow (3): 定理 1.8 と同じ証明が通用する。つまり、“ $\neg(1) \Rightarrow \neg(3)$ ” の証明は、定理 1.8 の“(1) \Rightarrow (2)”の証明を模倣し、“ $\neg(3) \Rightarrow \neg(1)$ ” の証明は、定理 1.8 の“(2) \Rightarrow (1)”の証明を模倣する。ここで、計算可能性の条件を満たすためには、前者の証明においては Kraft の補題の代わりに、機械存在補題 2.1 を用いて、部分計算可能接頭関数 M の存在を示した後、命題 2.1 を用いて、 K_M に関する式を K に関する式に置き換える。一方、後者の証明においては、補題 2.2 を用いて、 $\{V_c\}_{c \in \mathbb{N}}$ が Σ_1^0 集合列であることを保証する。□

“ランダム”という概念に、人々は様々なイメージを思い浮かべる。その全てのイメージに対して、同時に数学的な定式化を与えることは難しいかもしれない。しかし、ランダムネスという概念の孕むイメージのうち、幾らかを反映する数学的概念を定式化できたと考えてよいだろう。そして、この節で示されたことは、少なくとも、

- ランダムに選ばれるということは、あらゆる確率的法則を満たす。
- ランダムということは不規則だから、賭博で儲けられない。
- ランダムということは不規則だから、短い文字列には圧縮できない。

という 3 つの異なる観点に基づくランダム性は、いずれも同値であるということである。

2.2 チャイティンのオメガ

本稿で展開するランダムネスの理論の利点は、具体的な無限列 $\alpha \in \{0, 1\}^{\mathbb{N}}$ や実数 $0.\alpha \in \mathbb{R}$ のランダム性について語る事が出来るという点である。たとえば、我々は「円周率 π はランダムではない」「ネイピア数 e はランダムではない」という言及が可能である。それでは、**どんな定数がランダムだろうか？**

チャイティンのオメガを定義し、オメガがマーティンレフ・ランダムであることを示す。

♠: まだ書き掛けです。

2.3 マルチンゲール vs. マルチンゲール過程 **

問題設定. ある賭博師 G 氏は、多目賭けコイン投げ賭博に何度か挑戦した結果、一目賭けコイン投げ賭博より儲け易いという気分が駆られてきた。しかし、第 1.5 節で証明されたように、確率だけ見れば、多目賭けも一目賭けも勝率は同じである。そこで G 氏は考えた。きっと、確率 0% の内部には、確率では区別できない“何か”があるに違いない、と。

補題 2.3. $U \subseteq \{0,1\}^{\mathbb{N}}$ が Σ_1^0 集合であり、 $q \geq 1$ を $\lambda(U) \leq 1/q$ を満たす計算可能実数とする。このとき、 (U, q) から計算可能な手続きによって、 $d(\langle \rangle) = 1$ かつ、任意の $\alpha \in U$ について $\lim_n d(\alpha \upharpoonright n) \geq q$ なる計算可能マルチンゲール過程 d を構成できる。

証明. $U = [S]$ なる計算可能反鎖 $S \subseteq \{0,1\}^{<\mathbb{N}}$ を取る。 $S^+ = \{\tau \in \{0,1\}^{<\mathbb{N}} : \tau \succeq \sigma\}$ によって定義とし、 $s_n = \#(S^+ \cap \{0,1\}^n)$ とおく。このとき、関数 $d: \{0,1\}^{<\mathbb{N}} \rightarrow \mathbb{R}$ を以下によって定義する。

$$d(\sigma) = \begin{cases} q, & \text{if } \sigma \in S^+ \cap \{0,1\}^n, \\ 1 - \frac{(q-1) \cdot s_n}{2^n - s_n}, & \text{if } \sigma \notin S^+ \cap \{0,1\}^n. \end{cases}$$

d の計算可能性は明らかである。いま、 $\lambda(U) \leq 1/q$ より、不等式 $s_n/2^n \leq 1/q$ が成立するので、

$$\frac{(q-1) \cdot s_n}{2^n - s_n} \leq \frac{(q-1) \cdot 2^n}{q \cdot 2^n - 2^n} = 1$$

となり、 $d(\sigma) \geq 0$ を満たす。また、 $\{S^+ \cap \{0,1\}^n\}_{n \in \mathbb{N}}$ が単調増大であることと、明らかに $\sum_{\sigma \in \{0,1\}^n} d(\sigma) = 2^n$ を満たすことから、 d がマルチンゲール過程であることが従う。□

定理 2.2 (Merkle/Mihailović/Slaman 2006). 任意の $\alpha \in \{0,1\}^{\mathbb{N}}$ について、以下の 2 条件は同値である。

1. α はマーティンレフ・ランダムである。
2. α 上勝利する計算可能マルチンゲール過程は存在しない。

証明. (1) \Rightarrow (2): d を計算可能マルチンゲール過程とする。このとき、

$$U_n = \{\alpha \in \{0,1\}^{\mathbb{N}} : (\exists n) d(\alpha \upharpoonright n) \geq 2^n \cdot d(\langle \rangle)\}$$

によって定義すれば、定理 1.7 より、 $\lambda(U_n) \leq 2^{-n}$ である。また、 d の計算可能性より、 $\{U_n\}_{n \in \mathbb{N}}$ は Σ_1^0 集合列である。もし、 $\limsup_n d(\alpha \upharpoonright n) = \infty$ ならば、明らかに $\alpha \in \bigcap_n U_n$ であるから、 α はマーティンレフ・ランダムではない。

(2) \Rightarrow (1): α はマーティンレフ・ランダムでないとする。このとき、 Σ_1^0 集合列 $\{U_n\}_{n \in \mathbb{N}}$ で、 $\alpha \in \bigcap_n U_n$ かつ $\lambda(U_n) \leq 2^{-n}$ なるものが存在する。マルチンゲールとは異なり、複数のマルチンゲール過程の和がマルチ

ンゲール過程であるとは限らないことに注意する. いま, $V_\sigma = U_{|\sigma|+1} \cap \llbracket \sigma \rrbracket$ とする. $\lambda(U_{|\sigma|+1}) \leq 2^{-|\sigma|-1}$ なので, 条件付確率は $\lambda(V_\sigma | \llbracket \sigma \rrbracket) \leq 1/2$ である. これより, 定理 2.3 を用いて, マルチンゲール過程 d_σ で,

$$d_\sigma(\sigma) = 1, \text{ and } (\forall \beta \in V_\sigma)(\exists m \in \mathbb{N})(\forall n \geq m) d_\sigma(\beta \upharpoonright n) = 2$$

を満たすものを, σ から計算可能な手続きで構成できる. いま, 各 $\beta \in \{0, 1\}^{\mathbb{N}}$ と $n \in \mathbb{N}$ について, $d(\beta \upharpoonright n)$ を次の手続きによって帰納的に定義する.

- まず, $d_{\langle \rangle}(\beta \upharpoonright m) \neq 2$ ならば, $d(\beta \upharpoonright m) = d_\lambda(\beta \upharpoonright m)$ によって定義する.
- $d_{\langle \rangle}(\beta \upharpoonright n_0) = 2$ なる n_0 が存在するならば, そのような最小の n_0 について, $d(\beta \upharpoonright n_0) = 2d_{\beta \upharpoonright n_0}(\beta \upharpoonright n_0)$ によって定義する.
- 帰納的に, $n_{k+1} \geq n_k$ を以下によって定義する.

$$n_{k+1} = \min\{n \geq n_k : d_{\beta \upharpoonright n_k}(\beta \upharpoonright n) = 2\}.$$

- 各 $k \in \mathbb{N}$ および任意の $n \in [n_k, n_{k+1})$ について, $d(\beta \upharpoonright n) = 2^{k+1}d_{\beta \upharpoonright n_k}(\beta \upharpoonright n)$ によって定義する.

このように定義された d は, 明らかに $\bigcap_n U_n$ 上完勝する. この d が計算可能マルチンゲール過程であることも, 単純な議論より示される. \square

定理 2.3 (Nies/Stephan/Terwijn 2005). 以下の 2 条件を満たす無限列 $\alpha \in \{0, 1\}^{\mathbb{N}}$ は 2^{\aleph_0} 種類存在する.

1. α 上勝利する計算可能マルチンゲールは存在しない.
2. α 上勝利する計算可能マルチンゲール過程が存在する.

証明. そのような α を構成するために, ある部分写像 $\Psi : \subseteq \{0, 1\}^{\mathbb{N}} \rightarrow \{0, 1\}^{\mathbb{N}}$ を構成する. $\{M_e\}_{e \in \mathbb{N}}$ を $M_e(\langle \rangle) = 1$ を満たす部分計算可能マルチンゲールの計算可能な枚挙とする. 各 $\beta \in \{0, 1\}^{\mathbb{N}}$ は, 各セクション $\beta(e+1, *)$ で $\text{dom}(M_e)$ の大きさを推測する. ここで,

$$\beta(e+1, *) = \langle 1, 1, 1, 1, 1, 0, 0, 0, \dots \rangle$$

のような列となっており, この 1 の長さが $\text{dom}(M_e)$ の長さの予測と関連付けられる. もし, β が全ての $\text{dom}(M_e)$ に対する正しい推測を行っているならば, $\Psi(\beta)$ が目的の無限列となるようにする.

$[\sigma]^{\leq k}$ を扇 $\{\tau \in \{0, 1\}^{\leq k} : \tau \succeq \sigma\}$ を意味するものとする. 扇 $[\sigma]^{\leq k}$ 上定義されたマルチンゲール M に対して, $\tau \in \{0, 1\}^k$ が σ 以降 M を用いて n -惨敗とは, 以下の条件を満たすことである.

$$(\forall \rho \in \{0, 1\}^{< \mathbb{N}}) \sigma \preceq \rho \preceq \tau \rightarrow M(\rho) \leq (1 + 2^{-n})M(\sigma).$$

財産を $1 + 2^{-n}$ 倍に出来る確率の問題より, ある計算可能関数 $z : \mathbb{N} \rightarrow \mathbb{N}$ が存在して, 任意の $\sigma \in \{0, 1\}^n$ および, $[\sigma]^{\leq z(n)}$ 上定義されたマルチンゲール M に対して, σ 以降 M を用いて n -惨敗する少なくとも 2 つの $\tau_0, \tau_1 \in \{0, 1\}^{z(n)}$ が存在する. ここで, τ_0 の有理数表現は τ_1 未満であるとし, $\tau_{\sigma, i}^M$ を τ_i を表すものとする. $z_0 = 0$ とし, $z_{k+1} = z(z_k + 1)$ によって定義すれば, 次の性質が満たされる.

$$\sigma \in \{0, 1\}^{z_{k+1}} \implies \tau_{\sigma, i}^M \in \{0, 1\}^{z_{k+1}}.$$

いま、マルチンゲール M が与えられているとき、 $\eta \in \{0, 1\}^{z_k}$ が M -貧困であるとは、

$$(\forall j < k)(\exists b_j \in \{0, 1\}) \tau_{\eta \upharpoonright z_j + 1, b_j}^M \preceq \eta.$$

であることとし、この $\beta \upharpoonright k = (b_0, \dots, b_{k-1})$ を η の M -符号と呼ぶ。逆に、符号 $\beta \in \{0, 1\}^{\mathbb{N}}$ が与えられたとき、 $\Psi(\beta)(n) = \alpha(n)$ を以下によって定義する。

$$\alpha(z_k) = \begin{cases} 0, & \text{if } M(\alpha \upharpoonright z_k \frown 0) \leq M(\alpha \upharpoonright z_k \frown 1), \\ 1, & \text{otherwise.} \end{cases}$$

$$\alpha \upharpoonright z_{k+1} = \tau_{\alpha \upharpoonright z_k + 1, \beta(k)}^M.$$

ただし、 M は部分マルチンゲールとして与えられるため、一般に $\Psi(\beta)$ は未定義になる。一方、 β が全ての $\text{dom}(M_e)$ を正しく推測していれば、 M は $\Psi(\beta)$ 上では全ての計算可能マルチンゲール以上に優秀な部分計算可能マルチンゲールとなるように、これから M を構成する。このとき、 $\alpha = \Psi(\beta)$ の M -貧困性より、どんな計算可能マルチンゲールも α 上勝利不可能に違いない。一方、 $\alpha(z_k)$ の値は $\alpha \upharpoonright z_k$ から M を用いて予測できるので、部分計算可能な戦略によって α 上任意に財産を増やすことが可能である。これより、 α がマーティンレフ・ランダムでないことが示され、定理 2.2 より、計算可能マルチンゲール過程で α 上勝利可能となる。

部分マルチンゲールの値 $M(\sigma)$ と補助パラメータ r_σ を帰納的に定義する。まずは $M(\langle \rangle) = r_{\langle \rangle} = 1$ とする。いま、 M -貧困な $\eta \in \{0, 1\}^{z_k}$ について、 $M(\eta)$ と r_η は定義されていると仮定する。この η の M -符号を (b_0, \dots, b_{k-1}) とする。いま、 $\text{dom}(M_e)$ は全域であると η は推測しているとは、以下の条件を満たすことである。

$$\langle e+1, 0 \rangle < k, \text{ and } (\forall j \in \mathbb{N}) \langle e+1, j \rangle < k \rightarrow b_{\langle e+1, j \rangle} = 1.$$

η によって全域的であると推測されている M_e および $\tau \in [\eta]^{\leq z_{k+1}}$ について、 $M_e(\tau)$ を計算する。もし、 η の推測が正しければ、 $\tau \in \text{dom}(M_e)$ なので、計算結果は返ってくるはずである。このとき、 $M(\tau)$ を以下のように定義する。

$$M(\tau) = r_\tau + \sum_{e \in E} 2^{-2z_{\langle e+1, 0 \rangle} + 1} M_e(\tau).$$

ここで、 E は η によって全域的であると推測されているマルチンゲールの指数 e 全体の集合であり、 $r_\tau \in [0, \infty)$ は M がマルチンゲールであることを保つために適切に指定される。

補助パラメータ r_τ の値は、以下の議論によって決定される。まず、各段階 z_k に到達する度に、可能性として、以下の3つが考えられる。

1. $b_k = 1$ であり、 E は変動しない。
2. $b_k = 0$ によって、 E から高々1つの数が減らされる。
3. $k = \langle e+1, 0 \rangle + 1$ であり、 E に高々1つの数が加えられる。

可能性1の場合は特に問題ない。可能性2の場合は、マルチンゲール M の資産の達成目標が下がるため、現状維持で十分である。すなわち、現状維持分の資産を r_τ に加えて、 M がマルチンゲールであることを保つ。可能性3の場合、マルチンゲール M の資産の達成目標が増加する。この増加量を計算すると、 $M_e(\langle \rangle) = 1$ が $M_e(\eta) \leq 2^{z_k}$ を導くことから、 $2^{-2z_k - 1} M_e(\eta) \leq 2^{-z_k - 1}$ である。これより、この資金を捻出するために、 M は常に余分な財産 $2^{-|\tau|}$ を r_τ の中に貯蓄しておけばよい。

もし、符号 $\beta \in \{0, 1\}^{\mathbb{N}}$ の推測が正しければ、

$$\dots \rightarrow M \upharpoonright [\alpha \upharpoonright z_k]^{\leq z_{k+1}} \rightarrow \alpha \upharpoonright z_{k+1} \rightarrow M \upharpoonright [\alpha \upharpoonright z_{k+1}]^{\leq z_{k+2}} \rightarrow \alpha \upharpoonright z_{k+2} \rightarrow \dots$$

のようにして定義は進んでいくので、最終的に $\alpha = \Psi(\beta)$ は定義される。

いま、 $\gamma' \geq_T \emptyset''$ を満たす無限列 $\{0, 1\}^{\mathbb{N}}$ を取る。このとき、関数 $g \leq_T \gamma'$ で、全ての計算可能関数を支配するものが存在する。 $\beta \equiv_T \gamma'$ で、 $\Psi(\beta)$ が定義されるようなものを構成する。このとき、 $\beta_0 \neq \beta_1$ かつ $\Psi(\beta_0)$ と $\Psi(\beta_1)$ が共に定義されるならば、 $\Psi(\beta_0) \neq \Psi(\beta_1)$ であり、また $\gamma' \geq_T \emptyset''$ を満たす γ は 2^{\aleph_0} 個存在することから、 2^{\aleph_0} 個の異なる $\Psi(\beta)$ が定義される。いま、 $\beta \equiv_T \gamma$ は、 $\beta(0, j) = \gamma(j)$ および以下によって定義される。

$$\beta(e+1, j) = \begin{cases} 1, & \text{if } (\forall i < j) \beta(e+1, i) = 1, \text{ and} \\ & (\forall \tau \in \{0, 1\}^{\leq z(e+j+1, e+j+1)+1}) M_e(\tau)[g(e+j)] \downarrow, \\ 0, & \text{otherwise.} \end{cases}$$

このとき、 β は各 $\text{dom}(M_e)$ を小さく見積もっているため、 β に沿って M は定義され、よって $\alpha = \Psi(\beta)$ は定義される。さらに、任意の計算可能マルチンゲール M_e について、 M_e の停止時刻は g に支配されるため、ある $M_{p(e)} = M_e$ の全域性を β は正しく推測する。これより、十分小さい定数 $\varepsilon > 0$ が存在して、

$$\limsup_{n \rightarrow \infty} \varepsilon \cdot M_e(\alpha \upharpoonright n) \leq \limsup_{n \rightarrow \infty} M(\alpha \upharpoonright n)$$

が成立する。一方、 α は M -貧困な列の極限であるから、

$$\limsup_{n \rightarrow \infty} M(\alpha \upharpoonright n) \leq \prod_k 1 + 2^{-z_k} \leq \prod_k 1 + 2^{-k} < \infty$$

より、 α は計算可能マルチンゲールでは勝利できない。 □

結論。現実には博徒がアルゴリズム的な戦略しか扱えないと考えれば、一目コイン賭博よりも多目コイン賭博の方が良心的で、博徒が儲けを出せる状況は真に多いのである。

2.4 真のランダムネスと非可測集合 **

問題設定。ランダムネスという言葉に人が思い浮かべるイメージは無数にあり、本稿で扱ったランダムネスの定義は、直ちに誰もが疑いなしに受け入れるようなものではない。たとえば、ある人は次のような疑問を提起する。何故、ランダムネスを定義するためにアルゴリズム概念に言及する必要があるのだろうか。

そもそも、1970年には、マーティンレフ自身が、ランダムネスの定義の変更案を出している。マーティンレフは、ランダムネスの定義として、**実効ボレル** (*effectively Borel*) 集合の概念を用いる、いわば**超算術的ランダムネス** (*hyperarithmetically random*) を提案した。言い換えれば、変換規則 $e \mapsto \alpha_e$ として、アルゴリズムよりもむしろ**構成的無限命題論理** (*constructive infinitary propositional calculus*) を選ぶというものである。しかし、この定義も、“超算術的”や“構成的無限論理”などの特殊な概念に依存する。全ての規則(零集合)を避けるのが無理だとしても、特殊な概念に依存せず、『ありとあらゆる定義可能な規則を避ける』という概念としてランダム性を定義すればよいのでは？

定義 2.3. 条件 P が**究極のランダム性**を表すとは、以下の2条件を満たすこととする。

1. 殆ど全ての無限列が P を満たすことは、ZFC で証明可能である。
2. 集合論で定義可能な任意の集合 $N \subseteq \{0, 1\}^{\mathbb{N}}$ について、もし ZFC で N が測度 0 であることを証明可能ならば、 P を満たす無限列は N に属さないことを ZFC で証明可能である。

定理 2.4 (Durand/Kanovei/Uspensky/Vereshchagin 2003). 究極のランダム性を表す条件で、集合論によって定義可能であるものは存在しない。

証明. 真のランダム性を表す定義可能な条件 P があったと仮定する。 L をゲーデルの構成可能宇宙とすると、 L 上の定義可能整列順序 \prec_L が存在する。 $P \cap L \neq \emptyset$ ならば、 N を $P \cap L$ の \prec_L -最小元だけを含む単元集合とする。さもなくば、 N を 0 のみからなる無限列 1 つを含む単元集合とする。明らかに、 N が単元集合であることは、ZFC で証明可能である。よって、定義 2.3 の条件 (2) より、 $P \cap L \neq \emptyset$ は有り得ない。一方、ZFC と無矛盾である条件 $V = L$ の下では、定義 2.3 の条件 (1) より、ほとんどの L -無限列は P を満たすはずである。これより、矛盾が導かれる。 \square

定義 2.4. 条件 P が弱究極のランダム性を表すとは、以下の 2 条件を満たすこととする。

1. 殆ど全ての無限列が P を満たすことは、ZFC と無矛盾である。
2. 集合論で定義可能な任意の集合 $N \subseteq \{0, 1\}^{\mathbb{N}}$ について、もし ZFC で N が測度 0 であることを証明可能ならば、 P を満たす無限列は N に属さないことを ZFC で証明可能である。

L -ランダムやソロヴェイのモデルについてコメントする。

♠: まだ書き掛けです。

第3章

ランダムネスとフラクタル次元

3.1 歪んだコインとマルチンゲール

問題設定. ここに、2頭の馬 A と B がいる. この馬たち A と B が競争したとき、今の所 A の勝率が 70% であり、 B の勝率が 30% であった. さて、カジノ運営者 C 氏は、この二頭の馬を用いた競馬賭博を開催することにした. このとき、各馬券の配当額を幾らに指定すれば、公平な賭博になるだろうか.

勝率に偏りのある競馬、あるいは表裏の出現確率に偏りのあるコインが生み出す確率測度は、ベルヌーイ測度と呼ばれる. ここでは、より一般の概念として、第 n 回目の試行では、表の出現確率が p_n であり、裏の出現確率が $1 - p_n$ であるようなコイン投げから得られる確率測度としてのベルヌーイ測度を導入する.

定義 3.1 (ベルヌーイ測度). 実数列 $p = (p_n)_{n \in \mathbb{N}} \in [0, 1]^{\mathbb{N}}$ が与えられたとき、次の 3 条件を満たす $m_p : \{0, 1\}^{<\mathbb{N}} \rightarrow [0, 1]$ から得られる $\{0, 1\}^{\mathbb{N}}$ 上の確率測度 λ_p をバイアス p のベルヌーイ測度 (Bernoulli measure with bias p) と呼ぶ:

1. $m_p(\langle \rangle) = 1$ である.
2. 任意の $\sigma \in \{0, 1\}^n$ に対して、 $m_p(\sigma 0) = p_n \cdot m_p(\sigma)$ である.
3. 任意の $\sigma \in \{0, 1\}^n$ に対して、 $m_p(\sigma 1) = (1 - p_n) \cdot m_p(\sigma)$ である.

例 3.1. 実数 $p \in [0, 1]$ のみからなる実数列 (p, p, p, \dots) を単に p で表す. λ_p をバイアス p のベルヌーイ測度とし、 $\#i(\sigma)$ によって $\sigma \in \{0, 1\}^{<\mathbb{N}}$ 中に現れる $i \in \{0, 1\}$ の総数、つまり $\#\{n < |\sigma| : \sigma(n) = i\}$ を意味するものとする. このとき、各 $\sigma \in \{0, 1\}^{<\mathbb{N}}$ について、 $[\sigma]$ の λ_p -確率は以下の値となる:

$$\lambda_p([\sigma]) = m_p(\sigma) = p^{\#0(\sigma)} \cdot (1 - p)^{\#1(\sigma)}.$$

より一般に、 $\{0, 1\}^{\mathbb{N}}$ 上のどんなボレル確率測度も、それぞれの有界的条件 $[\sigma]$ が成立する確率 $m(\sigma)$ がどの程度であるかを指定することによって得られる.

定理 3.1 (カラテオドリの拡張定理). $m : \{0, 1\}^{<\mathbb{N}} \rightarrow [0, 1]$ を, $m(\langle \rangle) = 1$ かつ, 任意の $\sigma \in \{0, 1\}^{<\mathbb{N}}$ について $m(\sigma) = m(\sigma 0) + m(\sigma 1)$ となる関数とする. このとき, $\{0, 1\}^{\mathbb{N}}$ 上のボレル確率測度 μ_m で, 任意の $\sigma \in \{0, 1\}^{<\mathbb{N}}$ について $\mu_m(\llbracket \sigma \rrbracket) = m(\sigma)$ を満たすようなものが一意に存在する.

さて, 0 の出現確率が p であり, 1 の出現確率が $1-p$ であるとしよう. すると, オッズとしては, 0 の出現を当てた場合には賭け金の $1/p$ 倍, 1 の出現を当てた場合には賭け金の $1/(1-p)$ 倍の配当金が妥当であるように思える. もし, 0 が出現することに q_0 ドル, 1 が出現することに q_1 ドル賭けた場合, 資金の変動過程は, 以下のようになる.

$$\begin{aligned} d(\sigma 0) &= d(\sigma) - (q_0 + q_1) + \frac{q_0}{p}, \\ d(\sigma 1) &= d(\sigma) - (q_0 + q_1) + \frac{q_1}{1-p}. \end{aligned}$$

したがって, $p \times (\text{上式}) + (1-p) \times (\text{下式})$ を計算することによって,

$$d(\sigma) = pd(\sigma 0) + (1-p)d(\sigma 1)$$

という条件が満たされる. 確率測度 μ が与えられており, 現在までに得た 0 と 1 の列が σ であるとき, 次に $i \in \{0, 1\}$ が出現する確率は, 条件付確率 $\mu(\llbracket \sigma i \rrbracket | \llbracket \sigma \rrbracket) = \mu(\llbracket \sigma i \rrbracket) / \mu(\llbracket \sigma \rrbracket)$ によって得られるため, このような配当金指定に対応するマルチンゲールは, 以下の条件を満たすものと特徴付けられる.

定義 3.2 (任意の測度に対するマルチンゲール). μ を $\{0, 1\}^{\mathbb{N}}$ 上の任意の確率測度とする. このとき, $d : \{0, 1\}^{<\mathbb{N}}$ が任意の $\sigma \in \{0, 1\}^{<\mathbb{N}}$ に対して次の条件を満たすとき, μ -マルチンゲール (μ -martingale) と呼ばれる:

$$d(\sigma) = \frac{\mu(\llbracket \sigma 0 \rrbracket)d(\sigma 0) + \mu(\llbracket \sigma 1 \rrbracket)d(\sigma 1)}{\mu(\llbracket \sigma \rrbracket)}.$$

Ville の定理 1.1 は, 任意の測度において成立する.

定理 3.2. μ を $\{0, 1\}^{\mathbb{N}}$ 上の任意の確率測度とし, $q \geq 1$ を実数とする. d が μ -マルチンゲールならば, ある $n \in \mathbb{N}$ で $d(\alpha \upharpoonright n) \geq q \cdot d(\langle \rangle)$ となる α 全体の集合の μ -測度は q^{-1} 以下である.

証明. 基本的には, 定理 1.1 の証明と同様である. 単純のために初期資金は $d(\langle \rangle) = 1$ であるとする. まず, S を $d(\sigma) \geq q$ を満たす極小な $\sigma \in \{0, 1\}^{<\mathbb{N}}$ たちの集合として定義する. 目標は, $\lambda([S]) \leq q^{-1}$ を示すことである. このとき,

$$\mu([S]) \cdot q = \sum_{\sigma \in S} \mu(\llbracket \sigma \rrbracket) \cdot q \leq \sum_{\sigma \in S} \mu(\llbracket \sigma \rrbracket) d(\sigma).$$

あとは, $\sum_{\sigma \in S} \mu(\llbracket \sigma \rrbracket) d(\sigma) \leq d(\langle \rangle) = 1$ であることを示せばよい. 任意の数 $k \in \mathbb{N}$ について, $S[k] = S \cap \{0, 1\}^{<k}$ と書く. もし, 任意の $k \in \mathbb{N}$ について $a_k = \sum_{\sigma \in S[k]} \mu(\llbracket \sigma \rrbracket) d(\sigma) \leq 1$ ならば, $\lim_k a_k \leq 1$ であるから, 以下を示せば十分であることが分かる.

主張. $\tau \in \{0, 1\}^{<\mathbb{N}}$ を任意の有限列とする. もし $F \subseteq \{0, 1\}^{<\mathbb{N}}$ が τ を拡張する有限列たちからなる有限 \preceq -反鎖ならば, $\sum_{\sigma \in F} \mu(\llbracket \sigma \rrbracket) d(\sigma) \leq \mu(\llbracket \tau \rrbracket) d(\tau)$ が成立する.

F の濃度に関する帰納法によって示す. $\#F = 1$ であるときは, たとえ τ 時点での所持金 $d(\tau)$ を元手に, 以後の結果が $\sigma \succeq \tau$ のように続くという確信の下で全額賭け続けたとしても, $d(\sigma) \leq (\mu(\llbracket \tau \rrbracket) / \mu(\llbracket \sigma \rrbracket)) d(\tau)$ となることから, $\mu(\llbracket \sigma \rrbracket) d(\sigma) \leq \mu(\llbracket \tau \rrbracket) d(\tau)$ となり, 主張は導かれる.

$\#F = n$ のとき主張は成立していると仮定する. F を濃度 $n+1$ の反鎖とする. τ を $F \subseteq \{\sigma : \tau \preceq \sigma\}$ なる最大の長さの有限列とする. このとき, 各 $i < 2$ について $F_i = \{\sigma \in F : \tau i \preceq \sigma\}$ は濃度 n 以下である. 帰納的仮定より, 以下が導かれる.

$$\begin{aligned} \sum_{\sigma \in F} \frac{\mu(\llbracket \sigma \rrbracket)}{\mu(\llbracket \tau \rrbracket)} d(\sigma) &= \sum_{i < 2} \sum_{\sigma \in F_i} \frac{\mu(\llbracket \sigma \rrbracket)}{\mu(\llbracket \tau \rrbracket)} d(\sigma) = \sum_{i < 2} \sum_{\sigma \in F_i} \frac{\mu(\llbracket \tau i \rrbracket)}{\mu(\llbracket \tau \rrbracket)} \cdot \frac{\mu(\llbracket \sigma \rrbracket)}{\mu(\llbracket \tau i \rrbracket)} d(\sigma) \\ &\leq \sum_{i < 2} \frac{\mu(\llbracket \tau i \rrbracket)}{\mu(\llbracket \tau \rrbracket)} d(\tau i) = d(\tau). \end{aligned}$$

両辺に $\mu(\llbracket \tau \rrbracket)$ を掛けることによって, $\sum_{\sigma \in F} \mu(\llbracket \sigma \rrbracket) d(\sigma) \leq \mu(\llbracket \tau \rrbracket) d(\tau)$ を得る. \square

定理 3.3 (ボレル測度の正則性). μ を $\{0, 1\}^{\mathbb{N}}$ 上のボレル測度とする. このとき, 任意の μ -可測集合 $A \subseteq \{0, 1\}^{\mathbb{N}}$ に対して, 開集合の下降列 $\{U_n\}_{n \in \mathbb{N}}$ で, 次を満たすものが存在する:

$$\mu(A) = \inf_{n \rightarrow \infty} \mu(U_n), \text{ かつ } A \subseteq U_n.$$

$\{0, 1\}^{\mathbb{N}}$ 上のボレル測度の正則性より, 零集合を取り扱う際, 測度が 0 に収束する開集合の下降列のみを考慮すればよい.

定義 3.3 (任意の測度に対するランダムネス). μ を $\{0, 1\}^{\mathbb{N}}$ 上の任意のボレル確率測度とする. 集合 $N \subseteq \{0, 1\}^{\mathbb{N}}$ が**実効 μ -零** (effectively μ -null) であるとは, ある計算的枚挙可能集合列 $\{U_n\}_{n \in \mathbb{N}}$ で, 任意の $n \in \mathbb{N}$ に対して, 次を満たすものが存在するときを指す:

$$\mu(U_n) \leq 2^{-n}, \text{ かつ } N \subseteq U_n.$$

無限列 $\alpha \in \{0, 1\}^{\mathbb{N}}$ に対して, $\{\alpha\}$ が実効 μ -零でないとき, α は**マーティンレフ μ -ランダム** (Martin-Löf μ -random) あるいは単に **μ -ランダム** であると呼ばれる.

定理 3.4. μ を $\{0, 1\}^{\mathbb{N}}$ 上の任意の計算可能確率測度とする. このとき, 任意の無限列 $\alpha \in \{0, 1\}^{\mathbb{N}}$ に対して, 次の 2 条件は同値である.

1. α は μ -ランダムである.
2. 任意の下半計算可能 μ -マルチンゲール $d : \{0, 1\}^{<\mathbb{N}} \rightarrow [0, \infty)$ に対して, 次の条件が成立する:

$$\limsup_{n \rightarrow \infty} d(\alpha \upharpoonright n) < \infty.$$

結論. A の勝率が 70% であり, B の勝率が 30% であるとき, 配当金の倍率は, A が $10/7$ 倍, B が $10/3$ 倍としておけば公平な賭博となる.

3.2 歪んだコインが複数あるとき

問題設定．いま、手許には歪んだコインが2つあって、それぞれ A と B と呼ぼう． A と B の歪み具合は結構違うようである．さて、コイン A を投げて得られる無限列が表すランダム性と、コイン B を投げて得られる無限列が表すランダム性には、どういう違いがあるだろうか？

実数列 $(p_i)_{i \in \mathbb{N}}$ が強正であるとは、次の条件を満たすことである：

$$0 < \liminf_{n \rightarrow \infty} p_n \leq \limsup_{n \rightarrow \infty} p_n < 1.$$

定理 3.5 (角谷の定理 1948)． $(p_i)_{i \in \mathbb{N}}$ と $(q_i)_{i \in \mathbb{N}}$ を $[0, 1]$ に属す実数の強正な列とする． λ_p と λ_q をそれぞれバイアス $(p_i)_{i \in \mathbb{N}}$ および $(q_i)_{i \in \mathbb{N}}$ のベルヌーイ測度とする．このとき、以下の3条件は同値である．

1. $\sum_{i=0}^{\infty} (p_i - q_i)^2 < \infty$.
2. 任意の集合 $N \subseteq \{0, 1\}^{\mathbb{N}}$ について、 $\lambda_p(N) = 0$ であることと $\lambda_q(N) = 0$ であることは同値である．
3. $\lambda_p(N) = 0$ かつ $\lambda_q(N) = 1$ であるような集合 $N \subseteq \{0, 1\}^{\mathbb{N}}$ は存在しない．

証明．ここでは (3) から (1) の導出のみを示す．他の部分については、後に、より強い性質が示される． $\sum_{i=0}^{\infty} (p_i - q_i)^2 = \infty$ を仮定する．強正であるという仮定から、 $p_i, q_i \in [\varepsilon, 1 - \varepsilon]$ を満たす $\varepsilon > 0$ が存在する． ν をバイアス $((p_i + q_i)/2)_{i \in \mathbb{N}}$ のベルヌーイ測度とする．いま、各 $i \in \mathbb{N}$ について、次の性質が成立する．

$$\left(\frac{p_i + q_i}{2} \right)^2 = p_i q_i \left(1 + \frac{(p_i - q_i)^2}{4p_i q_i} \right) \geq p_i q_i \left(1 + \frac{(p_i - q_i)^2}{4\varepsilon^2} \right).$$

同様にして、

$$\begin{aligned} \left(\frac{(1-p_i) + (1-q_i)}{2} \right)^2 &= (1-p_i)(1-q_i) \left(1 + \frac{(p_i - q_i)^2}{4(1-p_i)(1-q_i)} \right) \\ &\geq (1-p_i)(1-q_i) \left(1 + \frac{(p_i - q_i)^2}{4\varepsilon^2} \right). \end{aligned}$$

を得る．これより、各列 $\sigma \in \{0, 1\}^{<\mathbb{N}}$ について、次を得る．

$$\nu([\sigma])^2 \geq \lambda_p([\sigma])\lambda_q([\sigma]) \prod_{i=0}^{n-1} \left(1 + \frac{(p_{|\sigma|} - q_{|\sigma|})^2}{4\varepsilon^2} \right)$$

これより、長さを無限大に発散させたとき、 $\sum_{i=0}^{\infty} (p_i - q_i)^2 = \infty$ であるという仮定より、右辺の積の項は無限大に発散する．したがって、任意の自然数 $k > 0$ に対して、十分大きな自然数 $n_k \in \mathbb{N}$ が存在して、長さ n_k の任意の列 $\sigma \in \{0, 1\}^{<\mathbb{N}}$ について、 $\nu([\sigma]) \geq k\lambda_p([\sigma])\lambda_q([\sigma])$ が成立する． N_k を $\lambda_p([\sigma]) \leq \lambda_q([\sigma])$ なる長さ n_k の列全体から生成される開閉集合とする．そのような σ について、 $\nu([\sigma])^2 \geq k\lambda_p([\sigma])^2$ であるから、

$$\lambda_p(N_k) \leq \frac{\nu(N_k)}{\sqrt{k}} \leq \frac{1}{\sqrt{k}}$$

が成立する. 同様にして, $\lambda_q(\{0,1\}^{\mathbb{N}} \setminus N_k) \leq 1/k$ が成立するため, $\lambda_q(N_k) \geq 1 - 1/k$ を得る. いま, $N = \bigcap_{n \in \mathbb{N}} \bigcup_{k > 2^{2n}} N_k$ によって定義する. このとき, $\lambda_p(\bigcup_{k > 2^{2n}} N_k) \leq 2^{-n}$ であるから, $\lambda_p(N) = 0$ を得る. また, $\lambda_q(\bigcup_{k > 2^{2n}} N_k) \geq 1 - 2^{-n}$ であり, 集合の増大列であるから, $\lambda_q(N) = \lim_{n \rightarrow \infty} \lambda_q(\bigcup_{k > 2^{2n}} N_k) = 1$ を得る. \square

定理 3.6 (Vovk 1987). λ_p と λ_q をそれぞれ強正バイアス $(p_i)_{i \in \mathbb{N}}$ および $(q_i)_{i \in \mathbb{N}}$ のベルヌーイ測度とする. もし $\sum_{n=0}^{\infty} (p_n - q_n)^2 = \infty$ ならば, 任意の無限列 $\alpha \in \{0,1\}^{\mathbb{N}}$ に対して, 次の性質が成立する.

1. α が λ_p -ランダムならば, λ_q -ランダムではない.
2. α が λ_q -ランダムならば, λ_p -ランダムではない.

補題 3.1. μ と ν を $\{0,1\}^{\mathbb{N}}$ 上の計算可能な確率測度とする. このとき, 以下の 2 条件は同値である.

1. $\mu(N) = 0$ かつ $\nu(N) = 1$ を満たす集合 $N \subseteq \{0,1\}^{\mathbb{N}}$ が存在する.
2. μ -ランダムかつ ν -ランダムであるような無限列は存在しない.

証明. (2) \Rightarrow (1): R_ν を ν -ランダム列全体の集合とすると, $\nu(R_\nu) = 1$ である. 一方, 仮定より, $R_\nu \subseteq \{0,1\}^{\mathbb{N}} \setminus R_\mu$ であり, $\mu(R_\mu) = 1$ であるから, $\mu(R_\nu) = 0$ が成立する.

(1) \Rightarrow (2): $\mu(N) = 0$ かつ $\nu(N) = 1$ を満たす集合 $N \subseteq \{0,1\}^{\mathbb{N}}$ が存在すると仮定する. このとき, 任意の $n \in \mathbb{N}$ に対して, μ の正則性より, 開集合 $U_n \supseteq N$ で, $\mu(U_n) < 2^{-n}$ なるものが存在する. また, $N \subseteq U_n$ なので, $\nu(U_n) = 1$ である. よって, ある開閉集合 $V_n \subseteq U_n$ で, $\nu(V_n) > 1 - 2^{-n}$ なるものが存在する. μ と ν は共に計算可能であるから, n からこのような開閉集合 V_n を計算する手続きが存在する. 各 $n \in \mathbb{N}$ について $W_n = \bigcup_{m > n} U_m$ によって定義すれば, $\{W_n\}_{n \in \mathbb{N}}$ は計算的枚挙可能集合列であり, $\mu(W_n) \leq 2^{-n}$ かつ $\nu(W_n) = 1$ である. したがって, $\bigcap_{n \in \mathbb{N}} W_n$ は実効 μ -零であり, 各 $\{0,1\}^{\mathbb{N}} \setminus W_n$ は実効 ν -零である. よって, α が μ -ランダムならば $\alpha \notin \bigcap_{n \in \mathbb{N}} W_n$ である一方, α が ν -ランダムならば $\alpha \in \bigcap_{n \in \mathbb{N}} W_n$ である. \square

証明 (定理 3.6). 定理 3.5 における (3) \Rightarrow (1) により, $\sum_{n=0}^{\infty} (p_n - q_n)^2 = \infty$ ならば, $\lambda_p(N) = 0$ かつ $\lambda_q(N) = 1$ であるような集合 $N \subseteq \{0,1\}^{\mathbb{N}}$ が存在する. よって, 補題 3.1 より, λ_p -ランダムかつ λ_q -ランダムであるような無限列は存在しない. \square

定理 3.7 (Vovk 1987). λ_p と λ_q をそれぞれ強正バイアス $(p_i)_{i \in \mathbb{N}}$ および $(q_i)_{i \in \mathbb{N}}$ のベルヌーイ測度とし, $\sum_{n=0}^{\infty} (p_n - q_n)^2 < \infty$ が成立していると仮定する. このとき, 無限列 $\alpha \in \{0,1\}^{\mathbb{N}}$ が λ_p -ランダムであることと λ_q -ランダムであることは同値である.

証明. 無限列 $\alpha \in \{0,1\}^{\mathbb{N}}$ が λ_p -ランダムでないとする. このとき, ある下半計算可能マルチンゲール \tilde{d} が存在して, $\lim_n \tilde{d}(\alpha \upharpoonright n) = \infty$ となる. いま, \tilde{d} を次のように分解する:

$$\tilde{d}(\sigma) = \frac{\tilde{d}(\sigma) \cdot \lambda_p(\llbracket \sigma \rrbracket)}{\lambda_q(\llbracket \sigma \rrbracket)} \cdot \frac{\lambda_q(\llbracket \sigma \rrbracket)}{\lambda_p(\llbracket \sigma \rrbracket)}.$$

単純計算により, $d_q(\sigma) = \tilde{d}(\sigma) \cdot \lambda_p(\llbracket \sigma \rrbracket) / \lambda_q(\llbracket \sigma \rrbracket)$ は下半計算可能 λ_q -マルチンゲールであることが分かる. もし $\lim_n d_q(\alpha \upharpoonright n) = \infty$ であれば, α が λ_q -ランダムでないことが従う. したがって, 後は $\lim_n d_q(\alpha \upharpoonright n) < \infty$

の場合を考えればよい. このとき, $d(\sigma) = \lambda_q([\sigma])/\lambda_p([\sigma])$ によって d を定義したとき, $\lim_n d(\alpha \upharpoonright n) = \infty$ でなければならない. 再び単純計算によって, d は計算可能 λ_p -マルチンゲールであると分かる. これから, ある計算可能 λ_q -マルチンゲール d^* で, 次を満たすものを構成する.

$$(\exists c \in \mathbb{N})(\forall n \in \mathbb{N}) \log d(\alpha \upharpoonright n) \leq d^*(\alpha \upharpoonright n) + c.$$

まずは, d^* として, 負の値を取り得るものを定義し, 後に修正を与える. いま, 各 $n \in \mathbb{N}$ について, $\alpha(n)$ の値に対して, d は所持金の η_n 倍を 0 か 1 に賭けていたとする. 言い換えれば, 各 $i \in \{0, 1\}$ について, $d(\alpha \upharpoonright n \hat{\ } i)$ の値を以下のように設定する.

$$d(\alpha \upharpoonright n \hat{\ } i) = \begin{cases} (1 - \eta_n) \cdot d(\alpha \upharpoonright n), & \text{if } d \text{ の } \alpha(n) \text{ の推測が謝っている,} \\ \left(1 + \eta_n \frac{1 - p_n}{p_n}\right) \cdot d(\alpha \upharpoonright n), & \text{if } i = 0 \text{ かつ } d \text{ の } \alpha(n) \text{ への推測が正しい,} \\ \left(1 + \eta_n \frac{p_n}{1 - p_n}\right) \cdot d(\alpha \upharpoonright n), & \text{if } i = 1 \text{ かつ } d \text{ の } \alpha(n) \text{ への推測が正しい.} \end{cases}$$

このとき, d^* は d の推測と同じ値に, 所持金のうち η_n を賭ける. つまり, d が所持金の 10% を賭けに用いたならば, d^* は所持金のうち 10 ドルを賭けに用いる. 言い換えれば, 各 $i \in \{0, 1\}$ について, $d^*(\alpha \upharpoonright n \hat{\ } i)$ の値を以下のように設定する.

$$d^*(\alpha \upharpoonright n \hat{\ } i) = \begin{cases} d^*(\alpha \upharpoonright n) - \eta_n, & \text{if } d \text{ の } \alpha(n) \text{ の推測が謝っている,} \\ \eta_n \frac{1 - q_n}{q_n} + d^*(\alpha \upharpoonright n), & \text{if } i = 0 \text{ かつ } d \text{ の } \alpha(n) \text{ への推測が正しい,} \\ \eta_n \frac{q_n}{1 - q_n} + d^*(\alpha \upharpoonright n), & \text{if } i = 1 \text{ かつ } d \text{ の } \alpha(n) \text{ への推測が正しい.} \end{cases}$$

ξ_n を d の $\alpha(n)$ への推測時の儲け額を $d(\alpha \upharpoonright n)$ で割ったもの, すなわち, それぞれの場合毎に, 順に, $-\eta_n, \eta_n \cdot ((1 - p_n)/p_n), \eta_n \cdot (p_n/(1 - p_n))$ とする. 帰納法によって, 各 $n \in \mathbb{N}$ について, 次の式を得る.

$$d(\alpha \upharpoonright n) = \prod_{k=0}^{n-1} (1 + \xi_k).$$

\bar{p} と \bar{q} は強正であることから, ある $\theta > 0$ で, 各 p_i と q_i が $[\theta, 1 - \theta]$ に入るものを取れる. $m = \lceil 1/\theta \rceil$ とする. このとき, 各 $n \in \mathbb{N}$ について $0 \leq 1/p_n, 1/(1 - p_n) \leq m$ なので, $\xi_n \in [-1, m]$ が分かる. もし $i = 0$ かつ d の $\alpha(n)$ への推測が正しい場合, 次の不等式を得る:

$$\begin{aligned} d^*(\alpha \upharpoonright n + 1) - d^*(\alpha \upharpoonright n) &= \eta_n \frac{1 - q_n}{q_n} = \xi_n - \xi_n + \eta_n \frac{1 - q_n}{q_n} = \xi_n - \frac{\eta_n(q_n - p_n)}{p_n q_n} \\ &= \xi_n - \eta_n \cdot \frac{1 - p_n}{p_n} \cdot \frac{1}{(1 - p_n)q_n} \cdot (q_n - p_n) \\ &\geq \xi_n - \xi_n \cdot m^2(q_n - p_n) \geq \xi_n - m^2|\xi_n||p_n - q_n|. \end{aligned}$$

同様の不等式を, あらゆる場合について得ることができる. これより, 帰納法によって, 任意の $n \in \mathbb{N}$ について, 次の不等式を得る:

$$\sum_{k=0}^{n-1} \xi_k - \sum_{k=0}^{n-1} m^2|\xi_k||p_k - q_k| \leq d^*(\alpha \upharpoonright n).$$

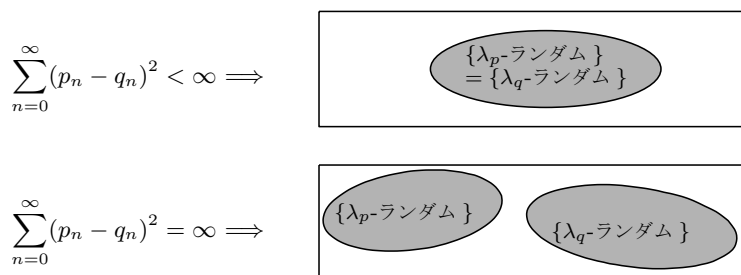


図 3.1 バルヌーイ測度の場合，ランダム性の差異は，等式 $\sum_{n=0}^{\infty} (p_n - q_n)^2 = \infty$ を満たすか否かのみ依存する。

定数 c を，任意の $\xi \in [-1, m]$ について $\log(1 + \xi) \leq \xi - c\xi^2$ なるものとする．このとき，以下の不等式が成立する：

$$\log d(\alpha \upharpoonright n) = \log \prod_{k=0}^{n-1} (1 + \xi_k) = \sum_{k=0}^{n-1} \log(1 + \xi_k) \leq \sum_{k=0}^{n-1} \xi_k - c \sum_{k=0}^{n-1} \xi_k^2.$$

いま， $\sum_{n=0}^{\infty} (p_i - q_i)^2 < \infty$ であるという仮定より，ある c^* で，任意の $t \geq 0$ について次の不等式を満たすものが存在する：

$$m^2 \sqrt{\sum_{i=0}^{\infty} (p_i - q_i)^2} \cdot \sqrt{t} \leq ct + c^*.$$

このとき，コーシー-シュワルツの不等式より，

$$\sum_{k=0}^{n-1} m^2 |\xi_k| |p_k - q_k| \leq m^2 \sqrt{\sum_{i=0}^{n-1} (p_i - q_i)^2} \sqrt{\sum_{k=0}^{n-1} \xi_k^2} \leq c \sum_{k=0}^{n-1} \xi_k^2 + c^*.$$

となるから，次を得る：

$$\log d(\alpha \upharpoonright n) \leq d^*(\alpha \upharpoonright n) + c^*.$$

仮定より， $\lim_n d(\alpha \upharpoonright n) = \infty$ であるから， $\lim_n d^*(\alpha \upharpoonright n) = \infty$ が導かれる．これより，ある自然数 $b \in \mathbb{N}$ が存在して，任意の $n \in \mathbb{N}$ について $d^*(\alpha \upharpoonright n) > -b$ となる．まず $d^{**} = d^* + \max\{c^*, b + 1\}$ によって定義し， d^* は基本的に d^{**} と同じ推測を行うが， d^{**} が資金を 1 未満に減らすような賭けを行う場合には，これに従わず，何も賭けずに見送ることとする．このとき， d^* はマルチンゲールである．さらに，もし d が計算可能ならば d^* も計算可能であり， $\lim_n d^*(\alpha \upharpoonright n) = \infty$ が成立する．□

結論．コインの歪み具合が少しでも違えば，全く別のランダム性概念が現れる。

3.3 偏った数列の次元

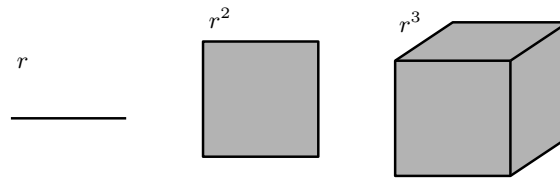


図 3.2 1 辺が r の s 次元立方体の s 次元ルベーク測度は r^s である。

問題設定 . 大数の法則から、100% の確率で、0 と 1 の極限的な出現頻度は $1/2$ になる。ということは、0 と 1 の出現頻度が偏った無限列が得られる確率は 0% だってことだ。でも、たとえば、0 と 1 の出現頻度が $1:3$ となる列を生成するアルゴリズムなんて現実に幾らでも作れるだろう。それなら、出現頻度が $1:3$ の無限列は、0% のうちのどれくらいの量を占めるだろうか？ どうにかして「0% 以下の確率」の現象を調べる方法はあるだろうか？

長さ 1 の線分の 2 次元世界における“大きさ”は 0 であるが、より低い次元の目で見れば、つまり、1 次元世界における“大きさ”は 1 である。測度 0 のものを調べるには、低次元への移行が有効であるようだ。しかし、離散的な次元では、それぞれの次元間のギャップが大きすぎるため、様々な現象の精密な分析を行うには大味すぎる。そこで、整数次元のルベーク測度 0 より精密な物差しとして、フラクタル幾何学などで頻繁に利用される、非整数次元のハウスドルフ測度の概念を持ち出すのがよい。この発想は、確率測度においても応用可能である。公平なコインによる確率測度 λ を 1 次元の確率測度と見立てよう。1 次元の確率論の代わりに今より展開するものは、**非整数次元の確率論**である。

定義 3.4 (ハウスドルフ測度 1917). 実数 $s \in [0, 1]$ を固定する。 $A \subseteq \{0, 1\}^{\mathbb{N}}$ の s 次元ハウスドルフ外測度 (s dimensional outer Hausdorff measure) は、以下によって与えられる。

$$\lambda^s(A) = \lim_{n \rightarrow \infty} \inf \left\{ \sum_{\sigma \in S} (\lambda([\sigma]))^s : A \subseteq [S], \text{ and } S \subseteq \{0, 1\}^{\geq n} \right\}.$$

注意. s 次元ハウスドルフ測度の定義の発想は、スケール則に基づく。一辺が r の線分の長さは r であり、一辺が r の正方形の面積は r^2 であり、一辺が r の立方体の体積は r^3 である (図 3.2)。より一般に、 $s \in \mathbb{N}$ について、1 辺が r の s 次元立方体の s 次元ルベーク測度は r^s である。一般の非整数 $s \in [0, \infty)$ の次元についても、図形の直径とサイズには s 乗の相関があると想定することにより、定義 3.4 が正当化される。

命題 3.1. もし $A \subseteq \{0, 1\}^{\mathbb{N}}$ が λ -可測ならば、 $\lambda(A) = \lambda^1(A)$ である。

さて、長さ 1 の線分は、1 次元の世界では大きさ 1 を持つが、2 次元世界では大きさを認識できない、すなわち面積 0 であると言えるだろう。あるいは、一辺の長さ 1 の正方形は、面積 1 であるが、体積 0 であり、さらに、正方形を充填するには長さ ∞ の曲線が必要であるから、正方形は長さ ∞ であると考えられる。このよう

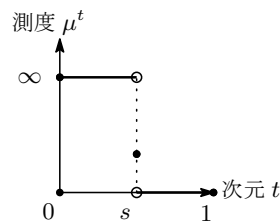


図 3.3 各集合には、高々 1 つの“ちょうどいい本来の次元”が存在し、それがハウスドルフ次元に他ならない。

に、ある図形が、本来あるべき次元より大きい次元にあるとき、その大きさは 0 であると認識され、本来あるべき次元より小さい次元にあるとき、その大きさは ∞ であると認識される。次の命題は、如何なる図形についても、0 以外の有限の大きさを取り得る次元は唯一であることを述べる。

命題 3.2. 任意の $A \subseteq \{0, 1\}^{\mathbb{N}}$ について、次のような実数 $s \in [0, 1]$ が存在する：

1. 任意の $t \in [0, s)$ について、 $\lambda^t(A) = \infty$ である。
2. 任意の $t \in (s, 1]$ について、 $\lambda^t(A) = 0$ である。

定義 3.5 (ハウスドルフ次元 1917). 集合 $A \subseteq \{0, 1\}^{\mathbb{N}}$ のハウスドルフ次元 (Hausdorff dimension) は次によって与えられる実数である。

$$\dim_H(A) = \inf\{s \in [0, 1] : \lambda^s(A) = 0\}.$$

さて、いま $\alpha \in A \subseteq \{0, 1\}^{\mathbb{N}}$ だということが分かっているとして、我々は α が何であるか知りたいとする。集合 A が小さければ小さいほど、 α が何であるかの候補が絞られている。すなわち、候補集合 A が小さく特定されていけばいるほど、 α の値を予測しやすく、そして α の値当て賭博で儲けを得ることは容易となるであろう。さて、ハウスドルフ次元が 1 未満の集合は、単純に確率 0 であるというよりも、さらに小さい。Ville の定理 1.2 を思い出せば、確率 0 にまで候補を絞っていれば、好きなだけ儲けを出せるようなマルチンゲールを構成できた。それならば、ハウスドルフ次元 1 未満にまで候補を絞っていれば、更に儲けを出せると期待できる。

定義 3.6 (実効ハウスドルフ次元). 次元として実数 $s \in [0, 1]$ を固定する。集合 $A \subseteq \{0, 1\}^{\mathbb{N}}$ が実効的に λ^s -零であるとは、ある $\{0, 1\}^{<\mathbb{N}}$ の計算的枚挙可能集合列 $\{S_n\}_{n \in \mathbb{N}}$ で、任意の $n \in \mathbb{N}$ について次を満たすものが存在するときを指す：

$$A \subseteq [S_n], \text{ かつ } \sum_{\sigma \in S_n} (\lambda([\sigma])^s \leq 2^{-n}.$$

このとき、集合 $A \subseteq \{0, 1\}^{\mathbb{N}}$ の実効ハウスドルフ次元 (effective Hausdorff dimension) は次によって与えられる実数である。

$$\text{edim}_H(A) = \inf\{s \in [0, 1] : A \text{ は実効的に } \lambda^s\text{-零である}\}.$$

また、実数 $\alpha \in \{0, 1\}^{\mathbb{N}}$ の実効ハウスドルフ次元は、 $\dim_H(\alpha) = \text{edim}_H(\{\alpha\})$ によって与えられる。

定理 3.8 (Lutz 2000). 集合 $A \subseteq \{0, 1\}^{\mathbb{N}}$ と実数 $s \in [0, 1]$ について、次の 2 条件は同値である。

1. A の実効ハウスドルフ次元は s 以下である。

2. 次の条件を満たす下半計算可能マルチンゲール $d : \{0, 1\}^{<\mathbb{N}} \rightarrow [0, \infty)$ が存在する :

$$\text{任意の } \alpha \in A \text{ および } t > s \text{ について, } \limsup_{n \rightarrow \infty} \frac{d(\alpha \upharpoonright n)}{2^{(1-t)n}} = \infty.$$

証明. (1) \Rightarrow (2): $s > \dim_H(A)$ を満たす実数 s を任意に取る. このとき, $\lambda^s(A) = 0$ であるから, ある計算的枚挙可能集合列 $\{[U_n]\}_{n \in \mathbb{N}}$ が存在して, 各 $n \in \mathbb{N}$ について, 次の性質が満たされる.

$$A \subseteq [U_n], \text{ かつ } \sum_{\sigma \in U_n} 2^{-s|\sigma|} \leq 2^{-n}.$$

ここで, U_n は反鎖とすることができる. Ville の定理 1.2 のように, マルチンゲール d_n は U_n の条件付確率を模倣する. 各 $\sigma \in \{0, 1\}^{<\mathbb{N}}$ について, U_n^σ を, $\tau \succeq \sigma$ なる $\tau \in U_n$ 全体の集合とする. このとき, $d_n(\sigma)$ とし, 初期資金 $d_n(\cdot) = \sum_{\sigma \in U_n} 2^{-s|\sigma|}$ であるような次の条件を満たすマルチンゲールを考える :

$$d_n(\sigma) = \begin{cases} 2^{|\sigma|} \sum_{\tau \in U_n^\sigma} 2^{-s|\tau|}, & \text{if } U_n^\sigma \neq \emptyset, \\ 2^{(1-s)m}, & \text{if } \sigma \upharpoonright m \in U_n \text{ for } m < |\sigma|, \\ 0, & \text{otherwise.} \end{cases}$$

このとき, $d(\sigma) = \sum_{n=1}^{\infty} d_n(\sigma)$ によって定義する. 明らかに d は下半計算可能マルチンゲールである. もし $\alpha \in A$ ならば, $A \subseteq \bigcap_{n \in \mathbb{N}} U_n$ であるから, 任意の $k \in \mathbb{N}$ について, $\alpha \upharpoonright n_k \in U_k$ なる $n_k \in \mathbb{N}$ が存在する. このとき, 任意の実数 $t > s$ について,

$$\frac{d(\alpha \upharpoonright n_k)}{2^{(1-t)n_k}} \geq \frac{d_k(\alpha \upharpoonright n_k)}{2^{(1-t)n_k}} = \frac{2^{(1-s)n_k}}{2^{(1-t)n_k}} = 2^{(t-s)n_k}$$

であるから, 次を得る.

$$\limsup_{n \rightarrow \infty} \frac{d(\alpha \upharpoonright n)}{2^{(1-t)n}} = \infty.$$

(2) \Rightarrow (1): いま, 任意の実数 $t > s$ を固定する. 各 $k \in \mathbb{N}$ について, $V_k \subseteq \{0, 1\}^{<\mathbb{N}}$ を次によって定義する.

$$V_k = \left\{ \sigma \in \{0, 1\}^{<\mathbb{N}} : \frac{d(\sigma)}{2^{(1-t)|\sigma|}} \geq 2^k \right\}.$$

このとき, U_k を V_k の極小元のなす反鎖とする. つまり, U_k として, 任意の $\tau \prec \sigma$ について $\tau \in V_k$ であるような $\sigma \in V_k$ 全体の集合とする. このとき, 次の不等式を得る.

$$\sum_{\sigma \in U_k} 2^{-t|\sigma|} \leq 2^{-k} \cdot \sum_{\sigma \in U_k} 2^{-t|\sigma|} \frac{d(\sigma)}{2^{(1-t)|\sigma|}} = 2^{-k} \cdot \sum_{\sigma \in U_k} 2^{-|\sigma|} d(\sigma) \leq 2^{-k}$$

ここで, 最後の不等式は, 定理 1.1 の証明中の主張による. 主張 (2) の仮定より, $A \subseteq \bigcap_{n \in \mathbb{N}} [U_n]$ であるから, $\lambda^t(A)$ は実効的に零である. $t > s$ は任意なので, $\text{edim}_H(A) \leq s$ を得る. \square

定理 3.9 (Ryabko 1984; Mayordomo 2002). 実数 $A \subseteq \{0, 1\}^{\mathbb{N}}$ について, 次の式が成立する..

$$\text{edim}_H(A) = \sup_{\alpha \in A} \liminf_{n \rightarrow \infty} \frac{K(\alpha \upharpoonright n)}{n}.$$

証明. まず, 任意の $\alpha \in A$ に対して $\liminf_{n \rightarrow \infty} K(\alpha \upharpoonright n)/n < s$ を満たす有理数 $s \in \mathbb{Q}$ を任意に取る. このとき, 任意の $k \in \mathbb{N}$ について, 無限個の $n \in \mathbb{N}$ が存在して, $K(\alpha \upharpoonright n) \leq sn - k$ が成立する. 任意の $k \in \mathbb{N}$ について,

$$U_k = \{\sigma \in \{0, 1\}^{<\mathbb{N}} : K(\sigma) \leq s|\sigma| - k\}$$

と定義すれば, $\{U_k\}_{k \in \mathbb{N}}$ は計算的枚挙可能集合列である. 系 1.2 より, 次を得る.

$$\sum_{\sigma \in U_k} 2^{-(s|\sigma| - k)} \leq \sum_{\sigma \in U_k} 2^{-K(\sigma)} \leq 1.$$

これより, $\sum_{\sigma \in U_k} 2^{-s|\sigma|} \leq 2^{-k}$ であり, $A \subseteq \bigcap_{k \in \mathbb{N}} [U_k]$ であるから, $\text{edim}_H(A) \leq s$ を得る.

逆に, $\text{edim}_H(A) < s$ なる有理数 $s \in \mathbb{Q}$ を取る. このとき, $\{0, 1\}^{<\mathbb{N}}$ の計算的枚挙可能集合列 $\{U_n\}_{n \in \mathbb{N}}$ で, $A \subseteq \bigcap_n [U_n]$ かつ $\sum_{\sigma \in U_n} 2^{-s|\sigma|} \leq 2^{-n}$ を満たすものが存在する. もし, $\sigma \in \bigcup_{n \geq 1} U_n$ であることが分かれば, 依頼 $(\sigma, s|\sigma|)$ を依頼状 L に書く. このとき,

$$\sum_{(\sigma, r) \in L} 2^{-r} = \sum_{\sigma \in \bigcup_{n \geq 1} U_n} 2^{-s|\sigma|} \leq \sum_{n=1}^{\infty} \sum_{\sigma \in U_n} 2^{-s|\sigma|} \leq \sum_{n=1}^{\infty} 2^{-n} = 1$$

であるから, 機械存在補題 2.1 より, 全ての依頼 $(\sigma, s|\sigma|)$ は達成され, ある定数 $c \in \mathbb{N}$ が存在して, 各 $\sigma \in \bigcup_{n \geq 1} U_n$ について, $K(\sigma) \leq s|\sigma| + c$ を得る. 任意の $\alpha \in A$ に対して, 無限個の $t \in \mathbb{N}$ が存在して, $\alpha \upharpoonright t \in \bigcup_{n \geq 1} U_n$ を満たすから,

$$\liminf_{n \rightarrow \infty} \frac{K(\alpha \upharpoonright n)}{n} \leq s$$

を得る. 以上の議論を合わせれば, 目的の等式を得る. □

系 3.1 (Mayordomo 2002). 無限列 $\alpha \in \{0, 1\}^{\mathbb{N}}$ について, 次の式が成立する.

$$\dim_H(\alpha) = \liminf_{n \rightarrow \infty} \frac{K(\alpha \upharpoonright n)}{n}.$$

結論. 確率 0% 以下の現象を調べるためには, 1 次元の確率ではなく, 次元をずらして非整数次元の確率を調べるのが有効である. このために用いられるハウスドルフ次元の概念は, コルモゴロフ複雑性の極限的増大率, つまり圧縮率と密接に結び付いている.

3.4 エントロピーとハウスドルフ次元

結論. 歪んだコインから得られるランダム列 α は, 当然ながら 0 と 1 の出現頻度が偏っており, 公平なコイン投げの意味ではランダムではない. したがって, 多くの有限部分 $\alpha \upharpoonright n$ をより短い列に圧縮できるだろう. では, 具体的には, 我々はこのランダム列 α をどれくらい圧縮できるだろうか?

定義 3.7 (Shannon 1948). 実数 $p \in [0, 1]$ のシャノン・エントロピー (*Shannon entropy*) とは、次によって定義される実数 $\mathcal{H}(p) \in [0, 1]$ である.

$$\mathcal{H}(p) = -p \log p - (1-p) \log(1-p).$$

定理 3.10 (Lutz 2000). 任意の無限列 $\alpha \in \{0, 1\}^{\mathbb{N}}$ および実数 $p \in [0, 1]$ について、もし $\text{Freq}(\alpha) = p$ ならば、 α の実効ハウスドルフ次元は $\mathcal{H}(p)$ 以下である。つまり、以下の条件を満たす。

$$\liminf_{n \rightarrow \infty} \frac{K(\alpha \upharpoonright n)}{n} \leq \mathcal{H}(p).$$

証明. $\sigma \in \{0, 1\}^{<\mathbb{N}}$ と $i \in \{0, 1\}$ が与えられたとき、 $\#i(\sigma)$ で、 $\sigma(n) = i$ なる $n \leq |\sigma|$ の数を表す。いま、 $p = 1/2$ の場合は自明なので、 $p > 1/2$ と仮定して一般性を失わない。 $\delta \in (0, p - 1/2]$ を任意の有理数とする。 $\text{Freq}(\alpha) = p \geq 1/2 + \delta$ なので、次が成立する。

$$\limsup_{n \rightarrow \infty} \frac{\#0(\alpha \upharpoonright n)}{n} \geq \frac{1}{2} + \delta.$$

マルチンゲール d を、常に次の値が 0 であることに現在資金の 2δ 倍を賭ける戦略によって与える。つまり、

$$d(\alpha \upharpoonright n) = (1 + 2\delta)^{\#0(\alpha \upharpoonright n)} \cdot (1 - 2\delta)^{\#1(\alpha \upharpoonright n)}$$

とする。このとき、次の等式が導かれる。

$$\begin{aligned} \frac{\log d(\alpha \upharpoonright n)}{n} &= \frac{\#0(\alpha \upharpoonright n)}{n} \log(1 + 2\delta) + \frac{\#1(\alpha \upharpoonright n)}{n} \log(1 - 2\delta) \\ &= 1 + \frac{\#0(\alpha \upharpoonright n)}{n} \log\left(\frac{1}{2} + \delta\right) + \frac{\#1(\alpha \upharpoonright n)}{n} \log\left(\frac{1}{2} - \delta\right). \end{aligned}$$

いま、 $p \geq 1/2 + \delta$ なので、これより、

$$\limsup_{n \rightarrow \infty} \frac{\log d(\alpha \upharpoonright n)}{n} \geq 1 + \left(\frac{1}{2} + \delta\right) \log\left(\frac{1}{2} + \delta\right) + \left(\frac{1}{2} - \delta\right) \log\left(\frac{1}{2} - \delta\right) = 1 - \mathcal{H}\left(\frac{1}{2} + \delta\right)$$

を得る。任意の正実数 $\varepsilon > 0$ に対して、 $1/2 + \delta$ が十分 p に近いような δ を取れば、 $\mathcal{H}(1/2 + \delta) < \mathcal{H}(p) + \varepsilon$ が成立する。このような $\delta \in (0, p - 1/2]$ に対して、

$$\limsup_{n \rightarrow \infty} (\log d(\alpha \upharpoonright n) - n(1 - \mathcal{H}(p) - \varepsilon)) = \infty$$

であるから、次の式が成立する。

$$\limsup_{n \rightarrow \infty} \frac{d(\alpha \upharpoonright n)}{2^{n(1 - \mathcal{H}(p) - \varepsilon)}} = \infty.$$

定数 $\varepsilon > 0$ は任意なので、これより、 α の実効ハウスドルフ次元は $\mathcal{H}(p)$ 以下である。 \square

定理 3.11 (Lutz 2003). $p \in (0, 1)$ を任意の計算可能実数とし、 λ_p をバイアス p のベルヌーイ測度とする。このとき、無限列 $\alpha \in \{0, 1\}^{\mathbb{N}}$ が λ_p -ランダムならば、 α の実効ハウスドルフ次元は、 p のシャノン・エントロピー $\mathcal{H}(p)$ に等しい。つまり、以下の性質を満たす。

$$\liminf_{n \rightarrow \infty} \frac{K(\alpha \upharpoonright n)}{n} = \mathcal{H}(p).$$

証明. α が λ_p -ランダムならば, Borel の強大数の法則 1.3 を分析すると, $\text{Freq}(\xi) \neq p$ なる $\xi \in \{0, 1\}^{\mathbb{N}}$ 全体の集合は実効的に λ_p -零であることが分かる. これより, $\text{Freq}(\alpha) = p$ であることが示される. よって, 定理 3.10 より, $\dim_H(\alpha) \leq \mathcal{H}(p)$ が成立する. 後は $\dim_H(\alpha) \geq \mathcal{H}(p)$ を示せばよい. 任意の計算可能な正実数 $s < \mathcal{H}(p)$ を固定する. いま, マルチンゲール d を任意に取る. この λ -マルチンゲールと同じ方に同じ割合の額を賭けていく場合の, λ_p による資金過程 d_p を考える. つまり, λ_p -マルチンゲール d_p を, 任意の $\sigma \in \{0, 1\}^{<\mathbb{N}}$ について, 次によって定義する:

$$d_p(\sigma) = \frac{2^{-|\sigma|}}{\lambda_p(\llbracket \sigma \rrbracket)} d(\sigma).$$

いま, $\log \lambda_p(\llbracket \sigma \rrbracket) = \#0(\sigma) \log p + \#1(\sigma) \log(1-p)$ であることに注意する. ここで, $\#i(\sigma)$ によって $\sigma \in \{0, 1\}^{<\mathbb{N}}$ 中に出現する $i \in \{0, 1\}$ の総数を表す. もし $\text{Freq}(\alpha) = p$ ならば, $\#0(\alpha \upharpoonright n)/n$ は p に収束するから, $\log \lambda_p(\llbracket \alpha \upharpoonright n \rrbracket)/n$ は $-\mathcal{H}(p)$ に収束する. これより, 十分大きな $n \in \mathbb{N}$ について, $sn + \log \lambda_p(\llbracket \alpha \upharpoonright n \rrbracket) < 0$ を得る. このような $n \in \mathbb{N}$ に対して,

$$d_p(\alpha \upharpoonright n) = \frac{2^{-n}}{\lambda_p(\llbracket \alpha \upharpoonright n \rrbracket)} d(\alpha \upharpoonright n) = \frac{1}{2^{sn + \log \lambda_p(\llbracket \alpha \upharpoonright n \rrbracket)}} \cdot \frac{d(\alpha \upharpoonright n)}{2^{(1-s)n}} > \frac{d(\alpha \upharpoonright n)}{2^{(1-s)n}}$$

が成立する. α は λ_p -ランダムなので, $\limsup_{n \rightarrow \infty} d_p(\alpha \upharpoonright n) < \infty$ であるから, 右辺の上極限の値も有限に収束する. また, $s < \mathcal{H}(p)$ は任意なので, 定理 3.8 より, $\dim_H(\alpha) \geq \mathcal{H}(p)$ を得る. \square

系 3.2 (Eggleston の定理 1949). 各 $p \in [0, 1]$ について, $\{\alpha \in \{0, 1\}^{\mathbb{N}} : \text{Freq}(\alpha) = p\}$ のハウスドルフ次元は $\mathcal{H}(p)$ である.

結論. 歪んだコインから得られるランダム列のコルモゴロフ複雑性の極限的振る舞い, すなわち実効ハウスドルフ次元は, シヤノン・エントロピーと同じ値を取る.

3.5 超越数論とランダムネス

問題設定. 実数を 2 進展開することにより, 実数 $0.\alpha \in [0, 1]$ と 0 と 1 の無限列 $\alpha \in \{0, 1\}^{\mathbb{N}}$ を同一視することができる. したがって, 無限列のランダムネスの理論は, 実数のランダムネスの理論でもある. それならば, ある種の実数のコルモゴロフ複雑性を, 具体的に計算してみよう!

定義 3.8. 実数 $\alpha \in \mathbb{R}$ に対して, $\text{Ir}(\alpha)$ を次の条件を満たす $r \in \mathbb{R}$ 全体の集合とする: 任意の正実数 $\varepsilon > 0$ に対して, ある定数 $c > 1$ が存在して, 任意の自然数 $p \leq q$ で $q \geq c$ なるものについて, r は次の不等式を満たす:

$$\left| \alpha - \frac{p}{q} \right| > \frac{1}{q^{r+\varepsilon}}.$$

実数 $\alpha \in \mathbb{R}$ の無理数度 (irrationality measure) とは, $\inf \text{Ir}(\alpha)$ によって定義される値である. ここで, $\inf \emptyset = \infty$ と定義される. 無理数度 ∞ の無理数はリウヴィル数 (Liouville number) と呼ばれる.

定理 3.12 (Staiger 1999). 任意のリウヴィル数 $\alpha \in \mathbb{R}$ は、実効ハウスドルフ次元 0 である。つまり、次の等式が成立する。

$$\liminf_{n \rightarrow \infty} \frac{K(\alpha \upharpoonright n)}{n} = 0.$$

証明. 与えられた $n \in \mathbb{N}$ に対して、コルモゴロフ複雑性に関する次の不等式を成立させる $l \geq n$ が存在することを示せば十分である。

$$\frac{K(\alpha \upharpoonright l)}{l} \leq \frac{\log n}{n}.$$

リウヴィル数をまとめて圧縮する機械を構成する。もし $\beta \in [0, 1]$ がリウヴィル数ならば、各 $n \in \mathbb{N}$ について $|\beta - \frac{p}{q}| < \frac{1}{q^n}$ なる自然数 $0 \leq p \leq q$ が存在する。このとき、 $[0, 1]$ の q 分割のある格子点周辺の幅 $\frac{2}{q^n}$ の区間 $J_{n,p,q} = [\frac{p}{q} - \frac{1}{q^n}, \frac{p}{q} + \frac{1}{q^n}]$ に β は含まれている。 $2^m \leq \frac{q^n}{2}$ なる最大の $m \in \mathbb{N}$ を取る。このとき、 $m = \lfloor n \log q - 1 \rfloor$ であることに注意する。 $[0, 1]$ を 2^m 分割したときの幅は、 $J_{n,p,q}$ の幅より大きいので、2つのブロックで $J_{n,p,q}$ を被覆できるので、それぞれの左端の点を $p_0(n, p, q)$ と $p_1(n, p, q)$ と書く。いま、ブロックは 2^{-m} 刻みであるので、 $p_0(n, p, q)$ または $p_1(n, p, q)$ は、 $\beta \upharpoonright m = \beta \upharpoonright \lfloor n \log q - 1 \rfloor$ を表すに違いない。

いま、 $p_i(n, p, q)$ は β の位置に依存せず、 (n, p, q) の値のみによって決まるから、各 (n, p, q) から $p_i(n, p, q)$ の値は計算可能である。このとき、 $[i, n, p, q]$ のような文字列で $p_i(n, p, q)$ を記述することを考える。たとえば、コンマを 11 で表記し、数字 $i < 2$ を $0i$ で表記すると考えても、これは長さ $2 + 2 \log n + 2 \log p + 2 \log q$ 程度の文字列で記述できる。 $p \leq q$ であるから、 $2 + 2 \log n + 4 \log q$ 以下であると考えてよい。これより、もし β がリウヴィル数ならば、十分大きな $n \in \mathbb{N}$ について、

$$\frac{C(\beta \upharpoonright \lfloor n \log q - 1 \rfloor)}{\lfloor n \log q - 1 \rfloor} \leq \frac{2 + 2 \log n + 4 \log q}{\lfloor n \log q - 1 \rfloor} \leq \frac{2}{\log q} \cdot \frac{\log n}{n}.$$

β が無理数でないとき、 n が無限大に発散するならば、 q も無限大に発散するので、 β の実効ハウスドルフ次元は 0 に収束する。□

系 3.3 (Oxtoby 1971). リウヴィル数全体の集合はハウスドルフ次元 0 である。

結論. どんなりウヴィル数も実効ハウスドルフ次元 0 であることを示せた。本稿では触れないが、ランダムネスの理論においてその他様々な次元概念がある。本節の結果とは対照的に、実はリウヴィル数は、正の有限状態次元 (finite state dimension) を取り得る。これを利用して、たとえば正規リウヴィル数の初等的構成を実現できる。

第4章

ランダムネス抽出と次元論

4.1 フォン・ノイマンのトリック

問題設定. N 氏は、いつものように賭博に明け暮れていた。しかし、今日の N 氏は、普段とは様子が異なり、深く眉を顰めていた。 N 氏には、どうにも C 氏の用いているコインに違和感を覚えてならなかったのだ。—あの C の野郎、イカサマしてやがる。あいつは詐欺師に違いねえ。

想像するに、コインに細工がしてあって、表が出る確率と裏が出る確率が異なっているのだろう。だが、賭博師 N 氏は、 C 氏のイカサマの証拠を掴むことができず、無根拠のイチャモンを付けるわけにもいかなかった。そこで、 N 氏は、提案をした。その怪しいコインを使ってもいいが、コイン投げは次の方法でやってくれ、と。

- コインを2回投げる。
- 結果が『表表』または『裏裏』だったら、コイン投げをやり直す。
- 結果が『表裏』だったら、それは『表』とし、結果が『裏表』だったら、それは『裏』とする。

定義 4.1 (フォン・ノイマン). $\alpha \in \{0,1\}^{\mathbb{N}}$ が与えられている。このとき、無限列 $\alpha^* \in \{0,1\}^{\mathbb{N}}$ と補助的な数 $n^* \in \mathbb{N}$ を帰納的に定義する。

- $0^* = 0$ として定義する。
- いま、 n^* および $\alpha^* \upharpoonright n^*$ が既に定義されていると仮定する。
- $\alpha(2n) = \alpha(2n+1)$ ならば、 $(n+1)^* = n^*$ と定義して、第 $(n+1)$ ステップに進む。
- $\alpha(2n) \neq \alpha(2n+1)$ ならば、 $\alpha^*(n^*) = \alpha(2n)$ および $(n+1)^* = n^* + 1$ と定義した後、第 $(n+1)$ ステップに進む。

定理 4.1 (フォン・ノイマン). 任意の実数 $p \in (0,1)$ を固定する。無限列 $\alpha \in \{0,1\}^{\mathbb{N}}$ が μ_p -ランダム列ならば、 α^* は λ -ランダム列である。

証明. いま、 μ_p^* を、 $c = \llbracket 01 \rrbracket \cup \llbracket 10 \rrbracket$ の下での条件付確率 $\mu_p^*(\llbracket 0 \rrbracket) = \mu_p(\llbracket 01 \rrbracket | c)$ および $\mu_p^*(\llbracket 1 \rrbracket) = \mu_p(\llbracket 10 \rrbracket | c)$ から得られるベルヌーイ測度とする。このとき、明らかに α^* は μ_p^* -ランダムである。 $\mu_p(\llbracket 01 \rrbracket) = \mu_p(\llbracket 10 \rrbracket) = p(1-p) > 0$ である。よって、 $\mu_p(\llbracket 01 \rrbracket | c) = \mu_p(\llbracket 10 \rrbracket | c) = 1/2$ であるから、 $\mu_p^* = \lambda$ である。□

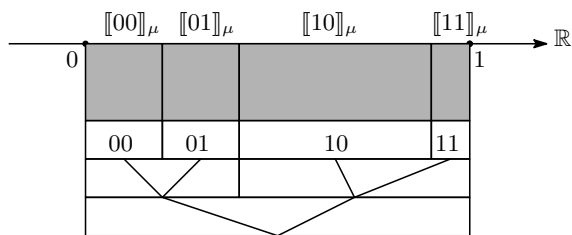
以上より、歪んだコインから得られるランダム性からならば、 λ -ランダム列の情報を抽出することができる。ランダムネス抽出 (*randomness extractor*) の研究は、計算量理論や暗号理論などで近年活発に進められている。ここでは、そのようなランダムネス抽出研究とは異なった観点に基づくランダムネス抽出の理論を展開する。すなわち、マーティンレフ・ランダム性およびコルモゴロフ複雑性に基づくランダムネス抽出の理論である。ここでは、考え得る限り最も強い意味での情報抽出であり、数学的に磐石な概念であるチューリング還元可能性 (*Turing reducibility, \leq_T*) を情報抽出の数学的形式化として用いる。この観点の下では、具体的な無限列や実数に関するランダム性およびランダム抽出を議論できる。このとき、一般に、任意の計算可能測度に関するランダム性から、公平なコイン投げにおけるランダム性を抽出することが可能である。

定義 4.2. 2つの有限列 $\sigma, \tau \in \{0, 1\}^{<\mathbb{N}}$ に対して、 $\sigma <_{\text{left}} \tau$ であることを、ある $n \in \mathbb{N}$ が存在して、 $\sigma \upharpoonright n = \tau \upharpoonright n$ かつ $\sigma(n) < \tau(n)$ であることを意味する。このとき、 $\text{Left}_\sigma = \{\tau \in \{0, 1\}^{<\mathbb{N}} : \tau <_L \sigma\}$ と定義する。有限列 $\sigma \in \{0, 1\}^{<\mathbb{N}}$ と $\{0, 1\}^{\mathbb{N}}$ 上の確率測度 μ が与えられているとする。測度 μ に基づく σ の生成する区間 $[[\sigma]]_\mu \subseteq [0, 1]$ とは、次によって定義される $[0, 1]$ の閉部分区間のことである：

$$[[\sigma]]_\mu = \left[\sum_{\tau \in \text{Left}_\sigma} \mu([\tau]), \left(\sum_{\tau \in \text{Left}_\sigma} \mu([\tau]) \right) + \mu([\sigma]) \right]$$

与えられた無限列 $\alpha \in \{0, 1\}^{\mathbb{N}}$ に対して、もし $\bigcap_{n \in \mathbb{N}} [[\alpha \upharpoonright n]]_\mu$ が1つの実数からなる単元集合ならば、その唯一の要素を α_μ と書く。

- 例 4.1.** 1. 与えられた無限列 $\alpha \in \{0, 1\}^{\mathbb{N}}$ に対して、 $0.\alpha \in [0, 1]$ によって α が表す実数を意味する。このとき、 $[[\sigma]]_\lambda = \{0.\alpha : \alpha \in [\sigma]\}$ である。
 2. 確率測度 μ を、 $\mu([[00]]) = 0.2, \mu([[01]]) = 0.2, \mu([[10]]) = 0.5, \mu([[11]]) = 0.1$ を満たすものとする。このとき、 $[[01]]_\mu = [0.2, 0.4]$ であり、 $[[11]]_\mu = [0.9, 1.0]$ である。



補題 4.1 (Levin 1970). μ が $\{0, 1\}^{\mathbb{N}}$ 上の計算可能な無原子確率測度ならば、任意の無限列 $\alpha \in \{0, 1\}^{\mathbb{N}}$ に対して、 $\alpha \equiv_T \alpha_\mu$ である。

証明. $\alpha_\mu \leq_T \alpha$ であることは、 μ の計算可能性と定義から明らかである。一方、 μ が無原子であることから、任意の $n \in \mathbb{N}$ に対して、ある $\sigma_n \in \{0, 1\}^{<\mathbb{N}}$ で $\alpha \in [[\sigma_n]]_\mu$ かつ $\mu([\sigma_n]) \leq 2^{-n}$ なるものが存在する。 μ の計算可能性より、 n から σ_n を計算できるため、 $\alpha \leq_T \alpha_\mu$ であることが従う。□

補題 4.2 (Levin 1970). μ が $\{0, 1\}^{\mathbb{N}}$ 上の計算可能な無原子確率測度ならば、任意の無限列 $\alpha \in \{0, 1\}^{\mathbb{N}}$ に対して、 α が λ -ランダムであることと α_μ が μ -ランダムであることは同値である。

証明. 前の補題のようにして、実効 λ -零集合と実効 μ -零集合の変換は容易にできる。□

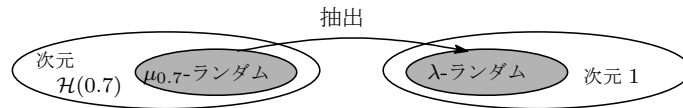


図 4.1 手許に表の出現率 70% のコインがある. このコインから得られる $\lambda_{0.7}$ ランダム列 α の次元は $\mathcal{H}(0.7)$ であるが, この α から λ -ランダムであるような次元 1 の列の情報を抽出できる.

定理 4.2 (Levin 1970). μ を $\{0, 1\}^{\mathbb{N}}$ 上の計算可能な無原子確率測度とする. このとき, 任意の μ -ランダム列 $\xi \in \{0, 1\}^{\mathbb{N}}$ に対して, ある λ -ランダム列 $\alpha \leq_T \xi$ が存在する.

証明. 測度 μ の無原子性より, 任意の $\xi \in \{0, 1\}^{\mathbb{N}}$ に対して, $0.\xi = \alpha_\mu$ となるある $\alpha \in \{0, 1\}^{\mathbb{N}}$ が存在する. 補題 4.1 より, $\alpha \leq_T \alpha_\mu$ であり, 補題 4.2 より, α は λ -ランダムである. \square

結論. 0 と 1 の列を延々生成し続ける確率的装置があったとする. もし我々がその装置が各 $[\sigma]$ を発生する確率を知っているならば, その装置から得られたランダム列から, 公平なコイン投げから得られたようなランダム列を復元することが可能である.

4.2 次元の壁を越えるのは難しい*

問題設定. 手許に表の出現率 70% のコインがある. このコインから得られる無限列, すなわち $\mu_{0.7}$ ランダム α の次元は $\mathcal{H}(0.7)$ であり, ランダムネス抽出定理 4.2 より, α から次元 1 の無限列を構成し直すことができる. とはいえ, 次元 $\mathcal{H}(0.7)$ の無限列は, 必ずしも $\mu_{0.7}$ -ランダムというわけではない.

たとえば, λ -ランダム列 $\rho = \langle \rho_0, \rho_1, \rho_2, \dots \rangle$ の各ビットの隙間に 0 を挿入する:

$$\langle \rho_0, 0, \rho_1, 0, \rho_2, 0, \rho_3, 0, \rho_4, 0, \dots \rangle$$

このような列は, 明らかに次元 $1/2$ である. このように, 各ビットの隙間に適当な数の 0 を挿入することによって, λ -ランダム列 ρ から, たとえば次元 $\mathcal{H}(0.7)$ の列を構成することは容易である. しかし, このように規則的に 0 の出現する列が $\mu_{0.7}$ -ランダムなわけではない. とはいえ, 0 の挿入によって次元を下げた列からは, 挿入した 0 を取り除くことによって, 次元 1 の列 ρ を復元することが可能である.

ある人は予想した. 「次元 $\mathcal{H}(0.7)$ の無限列がどのようにして与えられたとしても, どうにかすれば常に次元 1 の無限列を構成し直すことが出来るのではないか?」この予想は正しいだろうか?

定理 4.3 (Miller). $s \in [0, 1]$ を計算可能実数とする. 実効ハウスドルフ次元 s のある無限列 $\alpha_s \in \{0, 1\}^{\mathbb{N}}$ で, 如何なる $\xi \leq_T \alpha_s$ の実効ハウスドルフ次元も s 以下であるようなものが存在する.

定義 4.3. $S \subseteq 2^{\mathbb{N}}$ の s 次元最適被覆 (s -dimensional optimal cover) とは, S の開区間による被覆 $\{I_i\}_{i \in \mathbb{N}}$ であり, $\sum_i (\text{diam}(I_i))^s$ が最小となるもののうち, $\mu(\bigcup_i I_i)$ が最小となるものとする. このとき, $S^{\text{oc}} = \bigcup_i I_i$ と表す.

補題 4.3. S が Σ_1^0 集合ならば, S^{oc} も Σ_1^0 集合である. 実際, ある Σ_1^0 集合 $\tilde{S} \subseteq 2^{<\mathbb{N}}$ が存在して, $S^{\text{oc}} = \bigcup_{\sigma \in \tilde{S}} [\sigma]$ かつ次の条件を満たす: 任意の反鎖 $A \subseteq \tilde{S}$ について, $\text{wt}^s(A) \leq \mu_0^s(S)$.

補題 4.4. $0 \leq s < u \leq 1$ とする. $\text{wt}^u(V) \leq (1 - 2^{s-u})^{-1} \cdot \sup_n \text{wt}^s(V \cap 2^n)$.

証明. $b = \sup_n \text{wt}^s(V \cap 2^n)$ とする. このとき,

$$\text{wt}^u(V) = \sum_{\tau \in V} 2^{-u|\tau|} = \sum_n 2^{-sn} |V \cap 2^n| = \sum_n 2^{(s-u)n} \text{wt}^s(V \cap 2^n) \leq \sum_n 2^{(s-u)n} b = \frac{b}{1 - 2^{s-u}}.$$

□

補題 4.5. $0 \leq s < u \leq 1$ とし, $\{U_n\}_{n \in \mathbb{N}}$ を $U_n \subseteq 2^{>n}$ なる集合たちの族とする. このとき,

$$\sum_n \text{wt}^u(\{\sigma \in 2^n : 0 \leq \mu([U_n])\}) < \frac{\sup_n \text{wt}^s(U_n)}{1 - 2^{s-u}}.$$

証明. $b = \sup_n \text{wt}^s(U_n)$ とする. このとき, $\mu([V \cap 2^{>n}]) < 2^{-n(1-s)}b$ を得る. これより, $|\{\sigma \in 2^n : 0 \leq \mu([U_n])\}| < 2^{sn}b$ である. よって, この集合の u -次元重量は $2^{(s-u)n}b$ 未満であり, その総和は $b/(1 - 2^{s-u})$ 未満である. □

補題 4.6. 任意の Σ_1^0 集合 $S \subseteq 2^{\mathbb{N}}$ について, $\dim \mu(S^{\text{oc}}) \leq s$ である.

証明. 補題 4.3 を用い, S^{oc} の枚挙 $\tilde{S} = \{\tau_t\}_{t \in \mathbb{N}}$ を固定する. つまり, $S_{t+1}^{\text{oc}} = S_t^{\text{oc}} \cup [\tau_t]$ とする. このとき, S^{oc} の測度を次のように推測する.

1. 区間 $[\mu(S_{t+1}^{\text{oc}}), \mu(S_{t+1}^{\text{oc}}) + 2^{-|\tau_t|}]$ を V に並べる.
2. もし, ある $n, k \in \mathbb{N}$ について, $\mu(\tilde{S}_t \cap 2^{>n}) \leq k \cdot 2^{-n} < \mu(\tilde{S}_{t+1} \cap 2^{>n})$ となったら, 新たに $[\mu(S_{t+1}), \mu(S_{t+1}) + 2^{-n}]$ を V に並べる.

直感的には, 各 τ_t が並べられるたびに, それが \tilde{S} に並ぶ長さ $n = |\tau_t|$ の最後の元だと予想する. その後は測度変化 2^{-n} 刻みで考える. τ_t が並べられたタイミングで測度が残り高々 2^{-n} 程度しか増えないと予想し, その予想が覆される度に, 再び現在の測度から高々 2^{-n} 程度しか増えないと予想する. この操作によって最終測度を無限回正しく推測するのは明らかであろう. そして, 補題 4.4 および補題 4.5 より, これは s 次元ソロヴェイ検定である. □

定義 4.4. 与えられた $\sigma \in 2^{<\mathbb{N}}$ と Σ_1^0 集合 $S \subseteq [\sigma]$ について, $P_{\sigma, S} = [\sigma] \setminus S^{\text{oc}}$ によって定義する. $P_{\sigma, S} \neq \emptyset$ であるような組 (σ, S) の集まり \mathbb{P} をミラーの s -強制法 (Miller s -forcing) と呼ぶ.

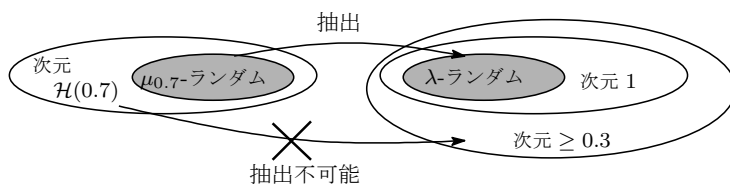


図 4.2 次元 $\mathcal{H}(0.7)$ の Miller の定数 $0. \alpha_{\mathcal{H}(0.7)} \in [0, 1]$ からは、我々が如何なる方法を取っても、たとえば次元 0.3 以上の情報を抽出することは出来ない！

補題 4.7. 以後、 $s < 1$ とする.

1. $(\sigma, S) \in \mathbb{P}$ ならば、 $\mu(P_{\sigma, S}) > 0$ かつ $\dim \mu(P_{\sigma, S}) \leq s$ である.
2. 任意の $(\sigma_0, S_0), \dots, (\sigma_n, S_n) \in \mathbb{P}$ に対して、もし $\mu(\bigcap_{i \leq n} P_{\sigma_i, S_i}) > 0$ ならば、ある $(\rho, R) \in \mathbb{P}$ で $P_{\rho, R} \subseteq \bigcap_{i \leq n} P_{\sigma_i, S_i}$ なるものが存在する.

証明. (1) s 次元観点では、 $[\sigma]$ の殆ど全てを被覆するような開集合 S は、明らかに $\mu^s(S) = \infty > 2^{-s|\sigma|}$ を満たす。よって、 $\mu(P_{\sigma, S}) = 0$ ならば $P_{\sigma, S} = \emptyset$ である。また、補題 4.6 より、 $\dim \mu(P_{\sigma, S}) = \dim \mu(S^{\text{oc}}) \leq s$ である。

(2) $P = \bigcap_{i \leq n} P_{\sigma_i, S_i}$ とし、 $\sigma = \sup_{i \leq n} \sigma_i$ とする。このとき、 $P = [\sigma] \setminus (\bigcup_{i \leq n} S_i^{\text{oc}})$ である。与えられた m に対し、 $D_m = [\sigma] \cap \bigcap_{i \leq n} \{\tau \in 2^m : P_{\tau, S_i} \neq \emptyset\}$ とする。 $[\tau] \cap P$ が空でないならば $\tau \in D_m$ なので、 $\mu(P) \leq |D_m| 2^{-m}$ である。 $\mu(P) \geq 2^{-b}$ なる b を取れば、 $|D_m| \geq 2^{m-b}$ を得る。

各 $\tau \in D_m$ について、 $R_\tau = [\tau] \cap (\bigcup_{i \leq n} S_i^{\text{oc}})$ と定義する。もし、ある m と $\tau \in D_m$ について、 $P_{\tau, R_\tau} \neq \emptyset$ であれば、 $(\rho, R) = (\tau, R_\tau)$ によって定義すればよい。いま、 $P_{\tau, R_\tau} = \emptyset$ であるとすると、 $\mu_0^s(R_\tau) = \mu_0^s([\tau]) = 2^{-sm}$ である。よって、 $\text{wt}^s(R_\tau) \geq 2^{-sm}$ であることに注意する。これより、

$$\sum_{i \leq n} \mu_s^0(S_i) = \sum_{i \leq n} \text{wt}^s(S_i^{\text{oc}}) \geq \text{wt}^s\left(\bigcup_{i \leq n} S_i^{\text{oc}}\right) \geq \sum_{\tau \in D_m} \text{wt}^s(R_\tau) \geq \sum_{\tau \in D_m} 2^{-sm} \geq 2^{m-b} 2^{-sm} = 2^{(1-s)m-b}.$$

一方、十分大きい m を取れば、 $\sum_{i \leq n} \mu_s^0(S_i) < 2^{(1-s)m-b}$ となることから、そのような m について、 $P_{\tau, R_\tau} \neq \emptyset$ なる $\tau \in D_m$ が存在する。□

各正測度 Π_1^0 集合 P に対して、 $b_P \in \mathbb{N}$ を $\mu(P) \geq 2^{-b}$ なる最小の b とする。

補題 4.8. \mathbb{P} をミラー s -強制概念とする。このとき、任意の $P \in \mathbb{P}$ および任意の $e, n \in \mathbb{N}$ に対して、 P のある部分集合 $Q \in \mathbb{P}$ が存在して、次のどちらかが満たされる：

1. 直径 $2^{b_P - n}$ 以下のある区間 I について、 $Q \subseteq \Phi_e^{-1}(I)$ となる。
2. $Q \cap \text{dom}(\Phi_e) = \emptyset$ となる。

♠: 証明まだ書きかけです。

結論 . ここで構成した次元 $\mathcal{H}(0.7)$ の具体的なある無限列 $\alpha_{\mathcal{H}(0.7)}$ からは、我々がどのように頑張っても、

$\mathcal{H}(0.7)$ より高い次元の無限列の情報を抽出できない。たとえば、 $\mathcal{H}(0.7) < 0.3$ なので、 $\alpha_{\mathcal{H}(0.7)}$ の情報をどのように利用しようとも、次元 0.3 の無限列を構成することは不可能である。

4.3 零次元よりも低次元の世界 *

次元関数 h に対するハウスドルフ h -測度。Hudelson の定理に関して書く。

4.4 ランダムネスと一次元の狭間 *

問題設定 λ -ランダムな無限列の実効ハウスドルフ次元は 1 である。一方、この逆は成り立たない。それでは、ランダムであることと実効ハウスドルフ次元 1 であることにはどれくらいの差異があるだろうか。実効ハウスドルフ次元 1 であるにも関わらず、どんな計算可能測度 μ に対しても μ -ランダムでないような無限列は存在するだろうか。

ミラーの定理に見たように、自分以下の次元の数列しか生み出さない正次元の数列が存在した。次に、同じ 1 次元の数列でも、単に実効ハウスドルフ次元 1 であることとマーティン=レフ・ランダムであることには若干のギャップがある。幾何学的測度論の言葉では、このギャップは次のように言い表されるであろう。

- ハウスドルフ次元が 1 である；つまり、任意の正実数 $\varepsilon > 0$ について、 $(1 - \varepsilon)$ 次元ハウスドルフ測度が正である。
- 1 次元ハウスドルフ測度（ルベーク測度）が正である。

フラクタル幾何学的意味だけを込めているのであれば、上の二つの違いを述べるのは極めて容易である。ここでは、それを遥かに越えて、このギャップが極めて巨大であることを述べる。

定理 4.4 (Greenberg/Miller 2011). 次のような無限列 $\alpha_{GM} \in \{0, 1\}^{\mathbb{N}}$ が存在する：

1. $\liminf_n \frac{K(\alpha_{GM} \upharpoonright n)}{n} = 1$.
2. 任意の $\xi \leq_T \alpha_{GM}$ に対して、 $\limsup_n (n - K(\xi \upharpoonright n)) = \infty$.

すなわち、 α_{GM} 自身は実効ハウスドルフ次元 1 であるにも関わらず、 α_{GM} から如何なるランダム列も構成することが出来ない。特に、定理 4.2 より、Greenberg/Miller の定数 α_{GM} は、以下の性質を持つ。

系 4.1 (Greenberg/Miller 2011). 次のような無限列 $\alpha_{GM} \in \{0, 1\}^{\mathbb{N}}$ が存在する：

1. 任意の正実数 $\varepsilon > 0$ について、 $(1 - \varepsilon)$ 次元ハウスドルフ測度において α_{GM} はランダムである。

2. どんな計算可能測度 μ の意味でも, α_{GM} は μ -ランダムではない.

Greenberg/Miller の定数 α_{GM} を記述するために, DNC 数列の概念を利用する.

定義 4.5. 与えられた非下降関数 $h: \mathbb{N} \rightarrow \mathbb{N}$ に対して, 空間 $h^{\mathbb{N}}$ を

$$h^{\mathbb{N}} = \prod_{n=0}^{\infty} \{0, 1, \dots, h(n) - 1\}$$

によって定義する. また, 有限列の集合 $h^{<\mathbb{N}}$ も同様にして定義される. このとき, 集合 $\text{DNC}[h] \subseteq h^{\mathbb{N}}$ を次によって定義する:

$$\text{DNC}[h] = \{F \in h^{\mathbb{N}} : (\forall e \in \mathbb{N}) F(e) \neq \Phi_e(e)\}.$$

各関数 $F \in \text{DNC}[h]$ は h -対角計算不可能 (h -diagonally noncomputable) であると呼ばれる. 対角計算不可能性はコルモゴロフ複雑性と深く関わっており, コルモゴロフ複雑性に関する議論を容易にするのに役に立つ.

計算可能関数 $h: \mathbb{N} \rightarrow \mathbb{N}$ が与えられているとき, $(2^h)(n) = 2^{h(n)}$ および $(\sum h)(n) = \sum_{m \leq n} h(m)$ を考える. 関数 $F \in (2^h)^{\mathbb{N}}$ について, $F^{*h} \in \{0, 1\}^{\mathbb{N}}$ によって, $F(n)$ を表す長さ $h(n)$ の 2 進列を繋げたものとする. 逆に, $\Gamma^h(X; n)$ を $\langle X(u) \rangle_{(\sum h)(n-1) \leq u < (\sum h)(n)}$ によって定義する. ここで $(\sum h)(-1) = 0$ とする. このとき, $\Gamma^h(F^{*h}; n) = F(n)$ である. さらに, 任意の $k \in \mathbb{N}$ に対して, 次の性質が満たされる.

$$(\forall u \leq k) \Gamma^h(F^{*h} \upharpoonright (\sum h)(k); u) = F(u)$$

いま, 命題 2.1 の万能機械 \mathbb{M} を固定し, $\Phi_{p(h;\sigma)}(n) = \Gamma^h(\mathbb{M}(\sigma); n)$ の計算を表す $p(h;\sigma)$ を取る. このとき, $\mathbf{p}^h(n) = \max_{\sigma \leq n} p(h;\sigma)$ として定義する. ここで, $\mathbf{p}^h: \mathbb{N} \rightarrow \mathbb{N}$ が計算可能関数であることに注意する. 定義より, 次の性質が満たされる:

$$K(F^{*h} \upharpoonright (\sum h)(k)) \leq z \implies (\exists e \leq \mathbf{p}^h(z)) (\forall u \leq k) \Phi_e(u) = F(u)$$

各 $g: \mathbb{N} \rightarrow \mathbb{N}$ について, 次の集合を考える.

$$\text{KC}[g] = \{\alpha \in \{0, 1\}^{\mathbb{N}} : (\exists c \in \mathbb{N}) (\forall n \geq c) K(\alpha \upharpoonright g(n)) \geq n\}.$$

命題 4.1. 計算可能関数 $h: \mathbb{N} \rightarrow \mathbb{N}$ を固定する.

1. 任意の $\alpha \in \text{KC}[h]$ に対して, $n \mapsto \alpha \upharpoonright h(n)$ は $\text{DNC}[2^h]$ に属す.
2. 任意の $F \in \text{DNC}[2^h]$ に対して, $F^{*h} \in \text{KC}[\sum h \circ \mathbf{p}^h]$ である.

証明. (1) もし, $\Phi_e(e) = \alpha \upharpoonright h(e)$ となるならば, $K(\alpha \upharpoonright h(e)) = K(\Phi_e(e)) \leq K(e) + O(1)$ となり矛盾する.

(2) F^{*h} が結論を満たさないと仮定する. $F(n)$ を計算するために, $F^{*h} \upharpoonright (\sum h)(n)$ の情報が必要である. いま, 無限個の n について, $K(F^{*h} \upharpoonright (\sum h \circ \mathbf{p}^h)(n)) < n$ なので, そのような n について, ある $\sigma \in 2^{<n}$ で

$$\mathbb{M}(\sigma) = F^{*h} \upharpoonright (\sum h)(\mathbf{p}^h(n))$$

となる. いま, $\mathbb{M}(\sigma)$ を基に, Γ^h を用いて, 任意の $p \leq \mathbf{p}^h(n)$ に対して, $F(p)$ を復元可能である. ここで, $p(h;\sigma) \leq \mathbf{p}^h(n)$ であるから,

$$\Phi_{p(h;\sigma)}(p(h;\sigma)) = \Gamma^h(\mathbb{M}(\sigma); p(h;\sigma)) = F(p(h;\sigma))$$

を得る．よって、 $F \notin \text{DNC}[2^h]$ が成立する． \square

以上より、DNC 数列自身はコルモゴロフ複雑性の増大度と深く関わっているものの、DNC 数列自体は一般的にはランダムではない．Greenberg/Miller の定数 α_{GM} の構成のポイントは、 h の増大速度が十分に遅い場合、任意の $\text{DNC}[h]$ 数列から、実効ハウスドルフ次元 1 の数列の情報を抽出できるという点である．まず、 h が定数関数であれば、Dana Scott, Robert Solovay, Carl Jockusch の結果を組み合わせることにより、任意の $\text{DNC}[h]$ 数列から、マーティンレフ・ランダム列の情報を抽出できる．

命題 4.2 (Scott; Solovay; Jockusch 1987)．任意の定数 $c \in \mathbb{N}$ と任意の $F \in \text{DNC}[c]$ について、あるマーティンレフ・ランダム列 $\alpha \leq_T F$ が存在する．

しかし、Jockusch が示したことは、 $c \geq 3$ について、与えられた $\text{DNC}[c]$ 数列からマーティンレフ・ランダム列を抽出するアルゴリズムが存在しないという点である．*1 言い換えれば、

- (命題 4.2) $F \in \text{DNC}[c]$ 毎に、ランダム列 $\alpha \leq_T F$ を構成するアルゴリズム Δ_F が存在する．
- $F \in \text{DNC}[c]$ からそのアルゴリズム Δ_F を発見するアルゴリズム $F \mapsto \Delta_F$ は存在しない．

一方、次の補題は、次元抽出アルゴリズムの存在を示すものである．

命題 4.3 (Greenberg/Miller 2011)．次のような計算可能関数 $\Delta : \subseteq \mathbb{N}^{\mathbb{N}} \times \mathbb{N} \rightarrow \{0, 1\}^{\mathbb{N}}$ が存在する：任意の自然数 $c \geq 2$ と関数 $F \in \text{DNC}[c]$ に対して、 $\Delta(F, c)$ は実効ハウスドルフ次元 1 である．

空間 $h^{\mathbb{N}}$ におけるマルチンゲールを考える．第 n 桁目の値の候補は $h(n)$ 種類であるため、配当金は賭け金の $h(n)$ 倍とするのが妥当であろう．言い換えれば、 d が $h^{\mathbb{N}}$ 上のマルチンゲールであるとは、各有限列 $\sigma \in \{0, 1\}^{<\mathbb{N}}$ について、次の条件を満たすときである：

$$h(|\sigma|) \cdot d(\sigma) = \sum_{n < h(|\sigma|)} d(\sigma n).$$

演習 4.1. $h^{\mathbb{N}}$ 上の普遍下半計算可能マルチンゲール d^h が存在することを示せ．ここで、 d^h が $h^{\mathbb{N}}$ 上の普遍下半計算可能マルチンゲールであるとは、 $h^{\mathbb{N}}$ 上の任意の下半計算可能マルチンゲール $d^* : \{0, 1\}^{<\mathbb{N}} \rightarrow [0, \infty)$ に対して、ある定数 $c \in \mathbb{N}$ が存在して、任意の $\sigma \in \{0, 1\}^{<\mathbb{N}}$ に対して、 $d^*(\sigma) \leq cd^h(\sigma)$ を満たす．

いま、 $h^{\mathbb{N}}$ 上の確率測度 μ_h を次によって定義する：

$$\mu_h([\sigma]) = \prod_{n < |\sigma|} h(n).$$

演習 4.2. 関数 $h : \mathbb{N} \rightarrow \mathbb{N}$ に対して、 $\dim_H^h(\alpha)$ を次の満たす $h^{\mathbb{N}}$ 上の下半計算可能マルチンゲール d が存在するような $s \in [0, 1]$ の下極限によって定義する：

$$\limsup_{n \rightarrow \infty} d(\alpha \upharpoonright n) \cdot \mu_h([\alpha \upharpoonright n])^{1-s} = \infty.$$

いま、全射 $\pi : h^{\mathbb{N}} \rightarrow [0, 1]$ を $\pi(\alpha) = \sum_{n=0}^{\infty} \alpha(n) \mu_h([\alpha \upharpoonright n+1])$ によって定義する．非下降計算可能関数 $h : \mathbb{N} \rightarrow \mathbb{N}$ を、ある定数 $k, c \in \mathbb{N}$ について、 $n \mapsto 2^{kn} + c$ によって上から抑えられるものとする．このとき、任意の $\alpha \in h^{\mathbb{N}}$ に対し

*1 樋口-木原 (201x) によれば、 $F \in \text{DNC}[c]$ からランダム列を抽出するアルゴリズム Δ_F を構成するためには、 Σ_2^0 -排中律ほどの論理学的原理があれば十分であるが、 Σ_2^0 -二重否定除去では不十分である．ここで、算術的複雑性を考慮した場合、ハイティング算術の上で、排中律 ($A \vee \neg A$) の方が二重否定除去 ($\neg\neg A \rightarrow A$) よりも真に強い論理学的原理であることに注意する．

て, $\pi(\alpha)$ の 2 進表示の実効ハウスドルフ次元は $\dim_H^h(\alpha)$ に等しいことを示せ (ヒント: 定理 3.8 による実効ハウスドルフ次元の特徴付けを用いよ).

演習 4.3 (Cenzer-Hinman 2008). 定数 $c, a \in \mathbb{N}$ に対して, $(a : c)$ -対角計算不可能関数とは, 次の集合に属す関数 $F : \mathbb{N} \rightarrow \{0, \dots, c-1\}$ である:

$$\text{DNC}[a : c] = \{F \in \{0, \dots, c-1\}^{\mathbb{N}} : (\forall e \in \mathbb{N})(\forall b < a) F(e) \neq \Phi_e(b)\}.$$

このとき, ある計算可能関数 $\Gamma : \mathbb{N}^{\mathbb{N}} \times \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}^{\mathbb{N}}$ で, 任意の $n, c \in \mathbb{N}$ および任意の $F \in \text{DNC}[c]$ に対して, $\Gamma(F, c, n) \in \text{DNC}[n : nc]$ となるようなものが存在することを示せ.

命題 4.3 の証明. $F \in \text{DNC}[c]$ および関数 $h : n \mapsto (n+1)c$ を固定する. $d : \{0, 1\}^{<\mathbb{N}} \rightarrow [0, \infty)$ を, 演習 4.1 のような $h^{\mathbb{N}}$ 上の普遍下半計算可能マルチンゲールとする. いま, 任意の $\sigma \in \{0, 1\}^{<\mathbb{N}}$ に対して,

$$\sum_{k < h(|\sigma|)} d(\sigma k) = h(|\sigma|)d(\sigma)$$

であるから, $d(\sigma k) \geq cd(\sigma)$ であるような $k < h(|\sigma|) = (|\sigma| + 1)c$ は高々 $|\sigma| + 1$ 個である. $\Phi_{m(\sigma)}$ として, $d(\sigma k) \geq c^{|\sigma|}$ なる新しい k が見つかる度に, その k を出力する関数とする. つまり, $\Phi_{m(\sigma)}(j)$ を $d(\sigma k) \geq c^{|\sigma|}$ であることが判明した j 番目の k によって定義する. いま, 演習 4.3 のような Γ を取り, 帰納的に $\alpha(n) = \Gamma(F, c, n+1)(m(\alpha \upharpoonright n))$ によって定義する. 仮定より $F \in \text{DNC}[c]$ であるから, このとき, $\alpha(n) \notin \{\Phi_{m(\alpha \upharpoonright n)}(j)\}_{j < n+1}$ が満たされる. 帰納的に, 任意の $n \in \mathbb{N}$ について, $d(\alpha \upharpoonright n) < c^n$ であることが示される.

いま, $\mu_h(\llbracket \alpha \upharpoonright n \rrbracket) = c^{-n}/n!$ であるから, 任意の $s \in [0, 1]$ に対して, 次が成立する.

$$d(\alpha \upharpoonright n) \cdot \mu_h(\llbracket \alpha \upharpoonright n \rrbracket)^{1-s} \leq \frac{a^{sn}}{(n!)^{1-s}}.$$

いま, もし $s < 1$ ならば, 定数 $p = a^{(s/1-s)}$ を考えると, 十分大きな任意の $n \in \mathbb{N}$ に対して, $n! > p^n$ であるから, そのような $n \in \mathbb{N}$ に対して, 次の不等式を得る.

$$\left(\frac{a^{sn}}{(n!)^{1-s}} \right)^{\frac{1}{1-s}} = \frac{a^{\frac{sn}{1-s}}}{n!} = \frac{p^n}{n!} < 1.$$

よって, 任意の $s < 1$ に対して, $\limsup_{n \rightarrow \infty} d(\alpha \upharpoonright n) \cdot \mu_h(\llbracket \alpha \upharpoonright n \rrbracket)^{1-s} < \infty$ を得る. これより, 演習 4.2 の \dim_H^h について, $\dim_H^h(\alpha) = 1$ を得る. 以上より, $\Delta(F, c)$ として, 演習 4.2 の $\pi(\alpha)$ の 2 進表示によって定義すれば, $\Delta(F, c) \in \{0, 1\}^{\mathbb{N}}$ の実効ハウスドルフ次元は 1 である. \square

定理 4.5 (Greenberg/Miller 2011). 次のような非下降かつ非有界な計算可能関数 $p : \mathbb{N} \rightarrow \mathbb{N}$ が存在する: 任意の $F \in \text{DNC}[p]$ に対して, ある実効ハウスドルフ次元 1 の列 $\alpha \leq_T F$ が存在する.

証明. 命題 4.3 の証明とおおよそ同様である. 関数 $h : n \mapsto (n+1)2^n$ を固定する. $d : \{0, 1\}^{<\mathbb{N}} \rightarrow [0, \infty)$ を, 演習 4.1 のような $h^{\mathbb{N}}$ 上の普遍下半計算可能マルチンゲールとする. いま, 任意の $\sigma \in \{0, 1\}^{<\mathbb{N}}$ に対して,

$$\sum_{k < h(|\sigma|)} d(\sigma k) = h(|\sigma|)d(\sigma)$$

であるから, $d(\sigma k) \geq (|\sigma| + 1)d(\sigma)$ であるような $k < h(|\sigma|) = (|\sigma| + 1)2^{|\sigma|}$ は高々 $2^{|\sigma|}$ 個である. $\Phi_{m(\sigma)}$ として, $d(\sigma k) \geq (|\sigma| + 1)!$ なる新しい k が見つかる度に, その k を出力する関数とする. つまり, $\Phi_{m(\sigma)}(j)$ を

$d(\sigma k) \geq c^{|\sigma|}$ であることが判明した j 番目の k によって定義する. いま, 演習 4.3 のような Γ を取る. このとき,

$$\Gamma(*, n+1, 2^n) : \text{DNC}[n+1] \rightarrow \text{DNC}[2^n : (n+1)2^n]$$

である. いま, $\gamma(n)$ を次の条件を満たすものとして定義する:

$$(\forall F \in \text{DNC}[n+1])(\forall \sigma \in h^n) \Gamma(F \upharpoonright \gamma(n), n+1, 2^n)(m(\sigma)) \text{ is defined.}$$

$\text{DNC}[n+1]$ のコンパクト性より, このような $\gamma(n)$ は存在する. $\gamma : \mathbb{N} \rightarrow \mathbb{N}$ は計算可能であり, 狭義単調増大であると仮定しても一般性を失わない. このとき, $p : \mathbb{N} \rightarrow \mathbb{N}$ を次のような関数として定義する:

$$p(k) = 1 + \min\{n \in \mathbb{N} : k < \gamma(n)\}.$$

このとき, $F \in \text{DNC}[p]$ ならば, $F \upharpoonright \gamma(n) \in (n+1)^{\mathbb{N}}$ であるから, $F \in \text{DNC}[n+1]$ である. よって, ある $G \leq_T F$ が存在して, 任意の $\sigma \in h^{<\mathbb{N}}$ に対して, 次の性質が成り立つ.

$$G(m(\sigma)) < h(|\sigma|), \text{ and } G(m(\sigma)) \notin \{\Phi_{m(\sigma)}(j) : j < 2^{|\sigma|}\}.$$

帰納的に, $\alpha(n) = G(m(\alpha \upharpoonright n))$ によって定義する. このとき, $\Phi_{m(\sigma)}$ の定義より, 帰納法によって, $d(\alpha \upharpoonright n) \leq n!$ であることは容易に示せる. いま, 各 $\sigma \in \{0, 1\}^{<\mathbb{N}}$ について,

$$\mu_h([\sigma]) = \frac{1}{2 \cdot 2^2 \cdots 2^{(n-1)} n!} = \frac{1}{2^{\frac{n(n-1)}{2}}}$$

が成立するから, 任意の $s < 1$ および $n \in \mathbb{N}$ について, 次が成立する:

$$d(\alpha \upharpoonright n) \mu_h([\alpha \upharpoonright n])^{1-s} \leq n! \cdot \frac{(n!)^{s-1}}{2^{(1-s)\frac{n(n-1)}{2}}} \leq \frac{n!}{2^{(1-s)\frac{n(n-1)}{2}}}.$$

ここで, $n!$ の増大速度は $2^{n \log n}$ より遅いので, この値は 0 に収束する. これより, 演習 4.2 の \dim_H^h について, $\dim_H^h(\alpha) = 1$ を得る. 以上より, $\Delta(F, c)$ として, 演習 4.2 の $\pi(\alpha)$ の 2 進表示によって定義すれば, $\Delta(F, c) \in \{0, 1\}^{\mathbb{N}}$ の実効ハウスドルフ次元は 1 である. \square

結論. この節では, DNC 数列から実効ハウスドルフ次元 1 数列の抽出可能性について議論した. 結果として, 十分に増大速度の遅い (*slow growing*) DNC 数列からは, コルモゴロフ複雑性の増大速度が十分速い (*fast growing*) 無限列の情報を抽出することが出来た. 次節では, DNC 数列からマーティンレフ・ランダム数列の抽出不可能性について議論する. このために用いるものは, 隈部/ルイスの強制法という技術的道具であり, 次節で詳細な議論を与えよう. よって, 本節の問題設定の解決は, 次節に譲る.

4.5 隈部/ルイス強制法

歴史ワンポイント

限部/ルイスの強制法は、**不動点を持たない極小次数** (*fixed point free minimal degree*) の研究の過程で誕生したものである。計算可能性理論において、1938年にスティーブン・コール・クリーネによって発見された再帰定理と呼ばれる不動点定理の一種がある。これは、コンピュータプログラムが自己複製活動を行うための理論的基盤となる重要な定理であり、日常生活においては、コンピュータウィルスという形で遭遇することが多いかもしれない。一方、計算不可能性の度合いを十分に増大させたとき、この自己複製可能性を保証する不動点が消失するという事実が古くから知られていた。これが、**不動点を持たない次数**というものである。

一方、**極小次数**は、1956年にクリフォード・スペクターによって発見されたものであり、自明な情報かそれ自身の情報しか抽出できないという特性を持つ。スペクターが極小次数の存在証明に用いた手法は、ジェラルド・サックスによってコーエン強制法と一体化され、現在は**サックス強制法** (*Sacks forcing*) として知られている。1985年、サックスは、この2つの特性を併せ持つ、不動点を持たない極小次数が存在するかどうか尋ねた。この問題は、サックス強制法の代わりに、いわゆるプリクリ強制法あるいは難波強制法の変種を用いて、1993年に限部正博 (2012年8月現在、放送大学准教授) によって解決された。

限部の強制法は、'00年代前半に、逆数学 (数学基礎論の一分野で、与えられた数学の定理に対して、それを証明するための必要最小限の公理が何であるかを探求する) において最初の応用が発見される。その後、'00年代末になって、興味深いことに、不動点の非存在という性質がコルモゴロフ複雑性に関するある種の条件と同値であることが発見される。この同値性を用いてジェラルド・サックスの問題「不動点を持たない極小次数が存在するか？」をランダムネスの言葉で翻訳すると、次のように言い表される。

問題設定 . ランダム列の特徴として、独立性概念が知られている。ランダム列

$$\alpha = \langle a_0, a_1, a_2, a_3, a_4 \dots \rangle$$

が与えられたとき、たとえば

$$\begin{aligned} \alpha_{2n} &= \langle a_0, a_2, a_4, a_6, a_8 \dots \rangle, \\ \alpha_{2n+1} &= \langle a_1, a_3, a_5, a_7, a_9 \dots \rangle \end{aligned}$$

とすれば、 α_{2n} から α_{2n+1} の情報は抽出できないし、逆に α_{2n+1} から α_{2n} の情報も抽出できない。分解された列もランダム列であるものの、そこからオリジナルのランダム列を復元することは不可能であるし、別の分解された断片の情報を知ること也不可能なのである。この分解作業を繰り返せば、1つのランダム列が無限種類の異なるランダム列の情報を内包していることが分かる。

さて、実効ハウスドルフ次元を徐々に下げていくにつれ、ランダム性は徐々に失われていく。では、実効ハウスドルフ次元をどこまで減衰させると、このような「無限種類の情報抽出可能性」という特性は失われてしまうだろうか。

限部/Lewis の定理の述べることは、任意の計算可能関数 $g : \mathbb{N} \rightarrow \mathbb{N}$ について $\liminf_{n \rightarrow \infty} \frac{K(\alpha \upharpoonright g(n))}{n} = 0$ であれば、このような無限種類の情報抽出可能性は失われる。ここでは、限部の強制法を利用し、非有界な

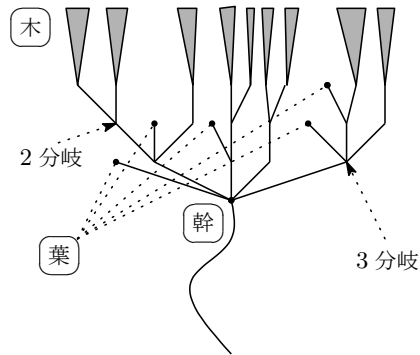


図 4.3 木に関する性質.

DNC 数列からのランダムネス抽出不可能性に関して議論する.

この節では、隈部/Lewis の強制法の解説を行う.

定理 4.6 (隈部/Lewis 2009; Greenberg/Miller 2011). $h : \mathbb{N} \rightarrow \mathbb{N}$ が計算可能な非下降かつ非有界な関数ならば、ある h -対角計算不可能関数 $F \in \text{DNC}[h]$ で、次の条件を満たすものが存在する：

$$(\forall \alpha \leq_T F) \limsup_{n \rightarrow \infty} (n - K(\alpha \upharpoonright n)) = \infty.$$

- 集合 $T \subseteq h^{<\mathbb{N}}$ が木 (tree) であるとは、 $\sigma \in T$ かつ $\tau \preceq \sigma$ ならば $\tau \in T$ であるときを言う.
- 木 $T \subseteq h^{<\mathbb{N}}$ の要素 $\sigma \in T$ が T の幹 (stem) であるとは、任意の $\tau \in T$ に対して、 $\sigma \preceq \tau$ または $\tau \preceq \sigma$ であるときを言う.
- 木 $T \subseteq h^{<\mathbb{N}}$ に対して $\rho \in T$ が葉 (leaf) であるとは、任意の $i \in \mathbb{N}$ に対して、 $\rho i \notin T$ であるときを言う. このとき Leaf_T によって、木 T の葉全体の集合を表す.
- 木 T が n -葉叢 (n -bushy) であるとは、各 $\tau \in T$ は葉であるか、さもなければ少なくとも n 個の $k \in \mathbb{N}$ について $\sigma k \in T$ であるときを言う.
- 集合 $\Lambda \subseteq h^{<\mathbb{N}}$ の σ 上叢度とは、 σ を幹とする有限 n -葉叢木 $T \subseteq h^{<\mathbb{N}}$ で $\text{Leaf}_T \subseteq \Lambda$ を満たすものが存在するような最大の $n \in \mathbb{N}$ である. ここで、 $\sigma \in \Lambda$ の場合、 Λ の σ 上叢度は任意の自然数以上となることに注意し、叢度を ∞ としておく.

定義 4.6. 以下の条件を満たす組 (σ, F, n) 全体の集合 \mathbb{P} を隈部強制法 (Kumabe forcing) と呼ぶ.

1. $\sigma \in h^{<\mathbb{N}}$ は有限列、 $F \subseteq h^{<\mathbb{N}}$ は無限木であり、 $n \leq h(|\sigma|)$ は自然数である.
2. σ は F の幹である.
3. $h^{<\mathbb{N}} \setminus F$ は σ 上叢度 n 未満である. 言い換えれば、 σ を幹とする任意の有限 n -葉叢木 $T \subseteq h^{<\mathbb{N}}$ に対して、 $\text{Leaf}_T \cap F \neq \emptyset$ である.

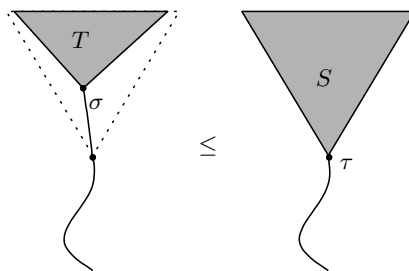


図 4.4 限部強制法.

\mathbb{P} 上の順序 \leq は以下の条件によって定義される.

$$(\sigma, T, n) \leq (\tau, S, m) \iff \sigma \succeq \tau, T \subseteq S, \text{ and } n \geq m.$$

集合 $\mathcal{D} \subseteq \mathbb{P}$ が稠密 (dense) であるとは, 任意の $p \in \mathbb{P}$ に対して, $q \leq p$ なる $q \in \mathbb{P}$ が存在するときを言う.

補題 4.9 (叢度の加法公式). $\mathbf{B}(\Lambda|\sigma)$ によって, $\Lambda \subseteq h^{<\mathbb{N}}$ の $\sigma \in h^{<\mathbb{N}}$ 上叢度を表す. このとき, 任意の $\Lambda, \Gamma \subseteq h^{<\mathbb{N}}$ と $\sigma \in h^{<\mathbb{N}}$ に対して, 次の不等式が成立する:

$$\mathbf{B}(\Lambda \cup \Gamma|\sigma) \leq \mathbf{B}(\Lambda|\sigma) + \mathbf{B}(\Gamma|\sigma).$$

次の補題は, 叢度の十分高い開集合条件は強制可能であることを保証する.

補題 4.10. $(\sigma, F, n) \in \mathbb{P}$ とする. もし $\Lambda \subseteq \{0, 1\}^{<\mathbb{N}}$ の σ 上叢度が n 以上ならば, $(\tau, F, n) \in \mathbb{P}$ なるある $\tau \in \Lambda$ が存在する.

証明. σ を幹とするある有限 n -葉叢木 $T \subseteq h^{<\mathbb{N}}$ について, $\Lambda = \text{Leaf}_T$ であると仮定しても一般性を失わない. 任意の $\tau \in \Lambda$ について, $(\tau, F, n) \notin \mathbb{P}$ であると仮定して矛盾を導く. よって, $h^{<\mathbb{N}} \setminus F$ は τ 上叢度 n 以上なので, τ を幹とする有限 n -葉叢木 $T_\tau \subseteq h^{<\mathbb{N}}$ で, 全ての葉が $h^{<\mathbb{N}} \setminus F$ に属するものが存在する. このとき, $\bigcup_{\tau \in \Lambda} T_\tau$ は σ を幹とする有限 n -葉叢木で, 全ての葉が $h^{<\mathbb{N}} \setminus F$ に属す. よって, $h^{<\mathbb{N}} \setminus F$ の σ 上叢度は n 以上である. これより, $(\sigma, F, n) \notin \mathbb{P}$ となり, 仮定に矛盾する. \square

補題 4.11. $(\langle \rangle, \text{DNC}_h, 2) \in \mathbb{P}$ である.

証明. DNC_h が無限木であることは明らかである. 任意の 2-葉叢木 $T \subseteq h^{<\mathbb{N}}$ に対して, ある T の葉が DNC_h に属することを示せばよい. これは, 各 $\sigma \in \text{DNC}_h$ に対して, 高々 1 つの $k < h(|\sigma|)$ について $\sigma k \notin \text{DNC}_h$ であることから明らかである. \square

計算可能関数 $\Phi : \subseteq h^{\mathbb{N}} \rightarrow \{0, 1\}^{\mathbb{N}}$ を固定する. $\text{dom}(\Phi)[u]$ を $\Phi(\tau) \upharpoonright u$ が定義されるような $\tau \in h^{<\mathbb{N}}$ 全体のなす Σ_1^0 集合とする. $Q_{\Phi, u} = h^{<\mathbb{N}} \setminus \text{dom}(\Phi)[u]$ として定義する. さて, 有限段で一様に Φ -計算を発散させることを強制できない, つまり各 $T \cap Q_{\Phi, u}$ が小さすぎるならば, Φ -計算の収束先を少数に特定できることを強制したい. しかし, $\text{dom}(\Phi)$ は Π_2^0 集合であるため, 直接の取り扱いが出来ないから, 叢度によって近似する.

補題 4.12. $h(|\sigma|) \geq 3n$ を仮定する. 任意の $u \in \mathbb{N}$, $\tau \succeq \sigma$ および $m \geq n$ について, $(\tau, Q_{\Phi, u}, m) \notin \mathbb{P}$ なら

ば, 任意の $\varepsilon > 0$ に対して, ある $v \in \mathbb{N}$ と σ 上叢度 n 以上の $C \subseteq \text{dom}(\Phi)[v]$ で, 次を満たすものが存在する.

$$\#\{\Phi(\tau) \upharpoonright v : \tau \in C\} \leq \varepsilon \cdot 2^v.$$

証明. いま, $(\sigma, Q_{\Phi, u}, n) \notin \mathbb{P}$ より, $\text{dom}(\Phi)[u]$ の σ 上叢度は n 以上である. いま, 記号 $\sigma \Vdash_n^0 \neg \Lambda$ と $\sigma \Vdash_n G$ を以下により定義する:

- $\sigma \Vdash_n^0 \neg \Lambda$ とは, $\Lambda \subseteq h^{< \mathbb{N}}$ の σ 上叢度が n 未満であることを意味する.
- $G = [\Lambda_G] \subseteq h^{\mathbb{N}}$ が開集合ならば, $\sigma \Vdash_n \neg G$ とは, $\sigma \Vdash_n^0 \neg \Lambda_G$ によって定義される.
- $G \subseteq h^{\mathbb{N}}$ が可算個の開集合 $\{G_u\}_{u \in \mathbb{N}}$ の共通部分 $G = \bigcap_{u \in \mathbb{N}} G_u$ ならば, $\sigma \Vdash_n G$ は次によって定義される:

$$\sigma \Vdash_n \bigcap_{u \in \mathbb{N}} G_u \iff \sigma \Vdash_{0.5n}^0 \neg \bigcup_{u \in \mathbb{N}} \{\tau : \tau \Vdash_{1.5n} \neg G_u\}.$$

このとき, $\text{dom}(\Phi) = \bigcap_{u \in \mathbb{N}} [\text{dom}(\Phi)[u]]$ に対して,

$$E = \{\sigma \in h^{< \mathbb{N}} : \sigma \Vdash_{2n} \text{dom}(\Phi)\}$$

によって定義する. いま, D をある $u \in \mathbb{N}$ について $\tau \Vdash_{3n} \neg [\text{dom}(\Phi)[u]]$ であるような $\tau \in h^{< \mathbb{N}}$ 全体の集合とする. 定義より, 各 $\sigma \in E$ について, D の σ 上叢度は n 未満である.

主張. 任意の $\eta \in E$ と $u \in \mathbb{N}$ について, $\text{dom}(\Phi)[u] \cap E$ の η 上叢度は $2n$ 以上である.

$\eta \in D$ について D の η 上叢度は ∞ なので, $\eta \in E$ ならば $\eta \notin D$ であることに注意する. これより, $\text{dom}(\Phi)[u]$ の η 上叢度は $3n$ 以上である. いま, $\eta \in E$ なので, E の定義より, D の η 上叢度は n 未満である. $D \subseteq h^{< \mathbb{N}} \setminus E$ より, $h^{< \mathbb{N}} \setminus E$ の η 上叢度もまた n 未満である. よって, 叢度の加法公式 4.9 より,

$$3n \leq \mathbf{B}(\text{dom}(\Phi)[u]|\eta) \leq \mathbf{B}(h^{< \mathbb{N}} \setminus E|\eta) + \mathbf{B}(\text{dom}(\Phi)[u] \cap E|\eta) \leq n + \mathbf{B}(\text{dom}(\Phi)[u] \cap E|\eta)$$

であるから, $\text{dom}(\Phi)[u] \cap E$ の η 上叢度は $2n$ 以上である.

主張. $\sigma \in E$ である.

$\sigma \notin E$ ならば, D の σ 上叢度は n 以上である. このとき, $\tau \in D$ で $\tau \succeq \sigma$ なるものが存在する. いま, ある $v \in \mathbb{N}$ について, $\tau \Vdash_{3n}^0 \neg \text{dom}(\Phi)[v]$ であるから, $\text{dom}(\Phi)[v]$ の τ 上叢度は $3n$ 未満となる. よって, $3n \leq h(|\sigma|) \leq h(|\tau|)$ より, $(\tau, Q_{\Phi, v}, 3n) \in \mathbb{P}$ となり, 仮定に矛盾する.

これより, 帰納的に $v_m \in \mathbb{N}$ と σ 上叢度 n 以上の有限集合 $C_m \subseteq \text{dom}(\Phi)[v_m] \cap E$ で, 次の条件を満たすものを構成していく:

$$\#\{\Phi(\tau) \upharpoonright v_m : \tau \in C_m\} \leq \left(\frac{3}{4}\right)^m \cdot 2^{v_m}.$$

まず, $v_0 = 0$ かつ $C_0 = \{\sigma\}$ と定義すれば, 明らかに上記の条件は満たされる.

いま, 既に v_m と C_m が定義されていると仮定し, $v_{m+1} = v_m + 2^{\#C_m} + 1$ によって定義する. 帰納的仮定より, $C_m \subseteq E$ なので, 任意の $\tau \in C_m$ について, $\text{dom}(\Phi)[v_{m+1}] \cap E$ は τ 上叢度 $2n$ 以上である. いま, 各 $u \in [v_m, v_{m+1})$ と $\eta \in \text{dom}(\Phi)[v_{m+1}]$ 毎に, 値 $\Phi(\eta; u) \in \{0, 1\}$ が決定する. よって, 各 $u \in [v_m, v_{m+1})$ と $\tau \in C_m$ について, ある $b(\tau, u) \in \{0, 1\}$ が存在して,

$$K(\tau, u) = \{\eta \in \text{dom}(\Phi)[v_{m+1}] \cap E : \Phi(\eta; u) = b(\tau; u)\}$$

は、叢度の加法公式 4.9 より、 τ 上叢度 n 以上である。ところで、 $2^{\#C_m} < v_{m+1} - v_m$ なので、各 u 毎に $\langle b(\tau; u) \rangle_{\tau \in C_m}$ のバリエーションは高々 $2^{\#C_m}$ 種類であることから、ある 2 つの異なる $u_m^0, u_m^1 \in [v_m, v_{m+1})$ で、 $\langle b(\tau; u_m^0) \rangle_{\tau \in C_m} = \langle b(\tau; u_m^1) \rangle_{\tau \in C_m}$ なるものが存在するはずである。いま、 A_{m+1} を次の 2 条件の両方を満たす $\eta \in \text{dom}(\Phi)[v_{m+1}] \cap E$ 全体の集合とする：

- ある $\tau \in C_m$ に対して、 $\eta \succeq \tau$ である。
- $\Phi(\eta; u_m^0) = 0$ または $\Phi(\eta; u_m^1) = 1$ である。

2 つめの条件より、各 $\tau \in C_m$ に対して、 $K(\tau, u_m^i) \subseteq A_{m+1}$ なる $i \in \{0, 1\}$ が存在するから、 A_{m+1} の τ 上叢度は n 以上である。よって、 C_m が σ 上叢度 n 以上であることから、補題 4.10 の議論を用いて、 A_{m+1} の σ 上叢度も n 以上であることが分かる。このとき、 σ を幹とする有限 n -葉叢木 T で $\text{Leaf}_T \subseteq A_{m+1}$ なるものが存在するので、 $C_{m+1} = \text{Leaf}_T$ によって定義する。

いま、任意の $\tau \in C_{m+1}$ に対して、 $\langle \Phi(\tau; u_m^0), \Phi(\tau; u_m^1) \rangle \neq \langle 1, 0 \rangle$ であるから、

$$\#\{\langle \Phi(\tau; u) : v_m \leq u < v_{m+1} \rangle : \tau \in C_m\} \leq \frac{3}{4} \cdot 2^{v_{m+1} - v_m}$$

を得る。また、 $\{\Phi(\tau) \upharpoonright v_m : \tau \in C_{m+1}\} \subseteq \{\Phi(\tau) \upharpoonright v_m : \tau \in C_m\}$ であることから、

$$\#\{\Phi(\tau) \upharpoonright v_{m+1} : \tau \in C_{m+1}\} \leq \frac{3}{4} \cdot 2^{v_{m+1} - v_m} \cdot \#\{\Phi(\tau) \upharpoonright v_m : \tau \in C_m\} \leq \left(\frac{3}{4}\right)^{m+1} \cdot 2^{v_{m+1}}$$

が成立する。よって、帰納法により、目的の主張は示された。□

各計算可能関数 $\Phi : \subseteq h^{\mathbb{N}} \rightarrow \{0, 1\}^{\mathbb{N}}$ と自然数 $c \in \mathbb{N}$ に対して、次の集合を考える：

$$\begin{aligned} \mathcal{D}_\Phi &= \bigcup_{u \in \mathbb{N}} \{(\sigma, F, n) \in \mathbb{P} : F \subseteq Q_{\Phi, u}\}, \\ \mathcal{E}_{\Phi, c} &= \bigcup_{u \in \mathbb{N}} \{(\sigma, F, n) \in \mathbb{P} : K(\Phi(\sigma) \upharpoonright u) \leq u - c\}. \end{aligned}$$

補題 4.13. 任意の $c \in \mathbb{N}$ に対して、 $\mathcal{D}_\Phi \cup \mathcal{E}_{\Phi, c}$ は \mathbb{P} で稠密である。

証明. $(\sigma, F, n) \in \mathbb{P}$ を固定する。適当に σ を伸ばすことによって、 $h(|\sigma|) \geq 3n$ を仮定できる。もし $q \leq (\sigma, F, n)$ なる $q \in \mathcal{D}_\Phi$ が存在しないなら、特に、任意の $u \in \mathbb{N}$, $\tau \succeq \sigma$ および $m \geq n$ について、 $(\tau, Q_{\Phi, u}, m) \notin \mathbb{P}$ である。よって、補題 4.12 より、与えられた $m \in \mathbb{N}$ について、自然数 $v_m \in \mathbb{N}$ と σ 上叢度 n 以上の有限集合 $C_m \subseteq \text{dom}(\Phi)[v_m]$ で、次の条件を満たすものが存在する：

$$\#\{\Phi(\tau) \upharpoonright v_m : \tau \in C_m\} \leq 2^{-2m} 2^{v_m}.$$

そのような v_m と C_m の存在を表す条件は Σ_1^0 なので、総当りによって、計算可能な手続きで、 v_m と C_m を発見できる。いま、依頼状 $L = \bigcup_{m \geq 1} L_m$ を次によって定義する：

$$L_m = \{(\Phi(\tau) \upharpoonright v_m, v_m - m) : \tau \in C_m\}$$

このとき、 L は Σ_1^0 である。いま、 L がクラフトの不等式を満たすことは、次によって確認できる：

$$\sum_{(\rho, r) \in L_m} 2^{-r} = (\#\{\Phi(\tau) \upharpoonright v_m : \tau \in C_m\}) \cdot 2^{m - v_m} \leq 2^{-2m} 2^{v_m} 2^{m - v_m} = 2^{-m}.$$

よって、補題 2.1 より、ある定数 $k \in \mathbb{N}$ が存在して、任意の $m \in \mathbb{N}$ と任意の $\tau \in C_m$ に対して、

$$K(\Phi(\tau) \upharpoonright v_m) \leq v_m - m + k$$

が成立する。よって、 $m = k + c$ なるものを選べば、 $K(\Phi(\tau) \upharpoonright v_m) \leq v_m - c$ が成立する。また、 C_m の σ 上 叢度 n 以上なので、補題 4.10 より、ある $\tau \in C_m$ について $(\tau, F, n) \in \mathbb{P}$ を満たすものが存在する。このとき、 $(\tau, F, n) \in \mathcal{E}_{\Phi, c}$ が成立する。□

結論. DNC 数列の概念を用いて、次元 1 とランダム性の情報抽出の意味で分離することができた。Greenberg/Miller の定数 α_{GM} は、次元 1 であるにも関わらず、そこから如何なるランダム性の情報も抽出できず、 α_{GM} 自身は、如何なる計算可能な無原子ボレル確率測度の意味でもランダムでない。

第 5 章

普遍零集合と強零集合

5.1 絶対にランダムでない無限列その 1

問題設定. どんな計算可能確率測度に対してもランダムでないような無限列として, 具体的にどのようなものがあるだろうか? 前章で見たように, ランダム列の情報を抽出できないような無限列がその具体例である. それでは, ランダム列の情報を抽出できるほどの情報量を持つにも関わらず, 如何なる計算可能無原子ボレル確率測度に対してもランダムでないような無限列は存在するだろうか?

定義 5.1 (Sierpiński/Szpilrajn 1936). 集合 $X \subseteq \{0, 1\}^{\mathbb{N}}$ が **普遍零** (*universal measure zero*) とは, $\{0, 1\}^{\mathbb{N}}$ 上の任意の無原子ボレル確率測度 μ に対して, $\mu(Y) = 0$ なる μ -可測集合 $Y \supseteq X$ が存在するときを言う.

演習 5.1. 以下の定理群を証明せよ.

1. (ハウスドルフ 1936) 非可算な普遍零集合が存在する.
2. (スピルレアン 1937) 集合 $X \subseteq \{0, 1\}^{\mathbb{N}}$ が普遍零であることと, 任意の同相写像 $h : \{0, 1\}^{\mathbb{N}} \rightarrow \{0, 1\}^{\mathbb{N}}$ について $h[X]$ が λ -測度 0 であることは同値である.
3. (バナッハの問題 1948) 如何なる濃度 $\kappa \leq 2^{\aleph_0}$ について, 濃度 κ の普遍零集合が存在するか?

定義 5.2. 数列 $\xi \in \{0, 1\}^{\mathbb{N}}$ が **実効普遍零** とは, $\{0, 1\}^{\mathbb{N}}$ 上の任意の計算可能な無原子ボレル確率測度 μ に対して, $\{\xi\}$ が実効 μ -零であるときを言う.

感覚的には, 実効普遍零数列とは, 如何なる計算可能な意味を持ってしても, ランダムであると言い張ることが不可能な数列である.

定理 5.1. 実効ハウスドルフ次元 1 かつ実効普遍零であるような無限列が存在する. 実際, 定理 4.4 における Greenberg/Miller の定数 α_{GM} は, 実効ハウスドルフ次元 1 かつ実効普遍零である.

証明. もし, 無限列 $\alpha \in \{0, 1\}^{\mathbb{N}}$ が実効普遍零でないならば, 定理 4.2 より, α から計算可能な λ -ランダム列

が存在する. よって, 定理 4.4 における Greenberg/Miller の定数の性質より, α_{GM} は実効普遍零では有り得ない. 一方, 定理 4.4 より, Greenberg/Miller の定数 α_{GM} の実効ハウスドルフ次元は 1 である. \square

Levin のランダムネス抽出定理 4.2 の述べることは, 実効普遍零でない無限列からは λ -ランダム列の情報を抽出できるということであった. それでは, λ -ランダム列を抽出できるにも関わらず, 実効普遍零であるということが有り得るだろうか. λ -ランダム列の情報を抽出できるが, それ自身は一見ランダム性を持っていないように思える無限列として, チューリングの停止問題がある. ここで, **停止問題 (halting problem)** とは, (万能プログラミング言語を 1 つ固定した上で) 次を意味する数列 $\theta' \in \{0, 1\}^{\mathbb{N}}$ である:

1. $\theta'(\langle e, n \rangle) = 1$ は, e 番目のプログラムに n を入力したとき, 有限時間で計算を終了することを表す.
2. $\theta'(\langle e, n \rangle) = 0$ は, e 番目のプログラムに n を入力したとき, 無限ループに陥って計算が終了しないことを表す.

補題 5.1 (Kreisel の基底定理 1955). ある λ -ランダム列 $\alpha \leq_T \theta'$ が存在する.

証明. $R_c = \{\alpha \in \{0, 1\}^{\mathbb{N}} : (\forall n \in \mathbb{N}) K(\alpha \upharpoonright n) \leq n - c\} \neq \emptyset$ であるような $c \in \mathbb{N}$ を固定する. このとき, 任意の $\alpha \in R_c$ は λ -ランダムである. いま, $P_c = \{\sigma \in \{0, 1\}^{<\mathbb{N}} : R_c \cap [\sigma] = \emptyset\}$ は Σ_1^0 集合であるから, $\sigma \in P_c$ か否かの判定を停止問題 θ' の情報を用いて行うことができる. よって, θ' の情報を用いて, $\alpha \in R_c$ を見つけ出すことができる. \square

実効零には成り得ない**停止確率 (halting probability)** Ω とは対照的に, 以下に見るように, 停止問題は普遍的な意味で規則性を持つ.

定理 5.2 (Levin 1970). 停止問題は実効普遍零である.

証明. μ を任意の計算可能確率測度とする. 各 $e \in \mathbb{N}$ について, 実効 μ -零集合 $N^e = \bigcap_n U_n^e$ とプログラム $p(e)$ を以下の手順で構成する.

- まず, $U_0^e = \{0, 1\}^{\mathbb{N}}$ とする.
 - $S_i^e = U_n^e \cap \{\xi \in \{0, 1\}^{\mathbb{N}} : \xi(\langle e, n \rangle) = i\}$ とする. n を入力したとき以下の動作を実行するプログラム $p(e)$ を書く.
 - $\mu(S_1^e) < \mu(S_0^e)$ であると分かった瞬間に, 計算を終了させる.
 - そうであると分かるまで延々計算をループさせる.
- 前者の場合は $U_{n+1}^e = S_1^e$ とし, 後者の場合は $U_{n+1}^e = S_0^e$ とする.

このとき, $\{U_n^e\}_{n \in \mathbb{N}}$ は一様に Σ_1^0 であり, $2 \cdot \mu(U_{n+1}^e) \leq \mu(S_0^e) + \mu(S_1^e) = \mu(U_n^e)$ より $\mu(U_n^e) \leq 2^{-n}$ である. よって, 任意の $e \in \mathbb{N}$ について, $N^e = \bigcap_n U_n^e$ は実効 μ -零である. 一方, 再帰定理より, $r = p(r)$ となるような $r \in \mathbb{N}$ が存在する. したがって, $\theta' \in N^r$ である. \square

系 5.1. 実効普遍零であるような無限列で, λ -ランダム列を計算可能であるものが存在する.

証明. 定理 5.2 より, 停止問題 θ' は実効普遍零であり, 補題 5.1 より, ある λ -ランダム列 $\alpha \leq_T \theta'$ が存在する. \square

結論. Greenberg/Miller の定数 α_{GM} や停止問題 \emptyset' は、如何なる計算可能性に基づく観点においてもランダムとみなすことはできない. それにも関わらず, 前者はかなり高いコルモゴロフ複雑性を持ち, 後者からはランダム列の情報を抽出できるほどの情報量を持つ.

5.2 絶対にランダムでない無限列その2

問題設定. 前節では, 如何なる計算可能な無原子ボレル確率測度に対してもランダムでない無限列の例を挙げた. それでは, 計算不可能な確率測度も考察の対象に入れてみよう. 如何なる無原子ボレル確率測度に対してもランダムでないような無限列などというものは存在するだろうか? 存在するとしたら, どのような列が, そのような条件を満たすだろうか?

定義 5.3. 無限列 $\xi \in \{0, 1\}^{\mathbb{N}}$ が **ネバー・ランダム** (*never continuously random*) とは, $\{0, 1\}^{\mathbb{N}}$ 上の任意の無原子ボレル確率測度 μ に対して, $\{\xi\}$ が実効 μ -零であるときを言う.

無限列の 0 と 1 の出現頻度が大きく偏っていれば, ランダムから程遠い. そのようなランダムから程遠い無限列であれば, ネバー・ランダムと為り得るだろうか. 単調増大な急増加関数 $F: \mathbb{N} \rightarrow \mathbb{N}$ の値域 $\text{range}(F) = \{F(n) : n \in \mathbb{N}\} \in \{0, 1\}^{\mathbb{N}}$ を無限列として見れば, 圧倒的に 0 の出現頻度が多くなる. したがって, 巨大関数の値域はネバー・ランダム列を生成することが期待できる.

定義 5.4 (ビジービーバー関数). 各 $e, n \in \mathbb{N}$ に対して,

- $\Phi_e(n)$ とは, e 番目のプログラムに n を入力したときの値を意味する.
- $s(e, n)$ は, もし $\Phi_e(n)$ が出力を返すならば, それまでに掛かる時刻を表す. もし $\Phi_e(n)$ が出力を返さないならば, $s(e, n) = 0$ とする.

ビジービーバー関数 (*Busy beaver function*) は, 各 $n \in \mathbb{N}$ について, 次のように帰納的に定義される:

$$BB(0) = 0, \text{ and } BB(n+1) = \max(\{s(e, m) : e, m \leq n\} \cup \{BB(n)\})$$

定理 5.3 (Reimann/Slaman). ビジービーバー関数 BB の値域 $\beta = \text{range}(BB) \in \{0, 1\}^{\mathbb{N}}$ は, ネバー・ランダムである.

証明. $\beta[s]$ を β の時刻 s 近似とする. 自然数 $t \in \mathbb{N}$ に対して, $\beta \upharpoonright t$ を予測したい状況を想定しよう. t に対して十分な時刻 $s_t > t$ を待ち, まずは $\beta \upharpoonright t$ を $\beta[s_t] \upharpoonright t$ であると予測する. もし $\beta \upharpoonright t \neq \beta[s_t] \upharpoonright t$ であるならば, この変化は時刻 s_t より後の時刻 $u > s_t$ に発生するため, $\beta \upharpoonright t$ 内のあるポジションから少なくとも s_t までの

間, β の値は全て 0 となる. 言い換えれば, 次のように β を捕捉できる:

$$\beta \in \llbracket \beta[s_t] \upharpoonright t \rrbracket \cup \bigcup_{\sigma \in \{0,1\}^t} \llbracket \sigma \frown 0^{s_t} \rrbracket.$$

いま, μ を $\{0,1\}^{\mathbb{N}}$ 上の無原子ボレル確率測度とする. $\{0,1\}^{\mathbb{N}}$ はコンパクトなので, 各正実数 $\varepsilon > 0$ に対して, ある $l(\varepsilon) \in \mathbb{N}$ で, 次の条件を満たすものが存在する:

$$(\forall \sigma \in \{0,1\}^{l(\varepsilon)}) \mu(\llbracket \sigma \rrbracket) \leq \varepsilon.$$

いま, 関数 l は, 測度 μ の情報を用いて計算できる. これより, $t = l(2^{-n-1})$ および $s_t = l(2^{-t} \cdot 2^{-n-1})$ と定義し, $V_n = \llbracket \beta[s_t] \upharpoonright t \rrbracket \cup \bigcup_{\sigma \in \{0,1\}^t} \llbracket \sigma \frown 0^{s_t} \rrbracket$ とする. このとき,

$$\mu(V_n) = \mu(\llbracket \beta[s_t] \upharpoonright t \rrbracket) + \sum_{\sigma \in \{0,1\}^t} \mu(\llbracket \sigma \frown 0^{s_t} \rrbracket) \leq 2^{-n-1} + 2^t \cdot 2^{-t} \cdot 2^{-n-1} = 2^{-n}$$

であるから, $\{V_n\}_{n \in \mathbb{N}}$ は実効 μ -零である. よって, 任意の無原子ボレル確率測度 μ に対して, β は μ -ランダムではない. \square

ネバー・ランダム性を導くと期待される別の概念として, K -トリビアルの概念がある. 無限列が K -トリビアルであるとは, それがコルモゴロフ複雑性の意味で 0 のみが無限に続く列が同程度に自明であることを意味する.

定義 5.5 (Chaitin 1976). 無限列 $\alpha \in \{0,1\}^{\mathbb{N}}$ が次の条件を満たすとき, K -トリビアル (K -trivial) であると呼称される.

$$\lim_n (K(\alpha \upharpoonright n) - K(0^n)) = 0$$

定理 5.4 (Kjos-Hanssen/Montalbán 2005). $P \subseteq \{0,1\}^{\mathbb{N}}$ が可算 Π_1^0 集合ならば, 任意の $\xi \in P$ はネバー・ランダムである.

証明. μ を無原子測度とする. このとき, $\mu(P) = 0$ である. P は Π_1^0 なので, 一様に Σ_1^0 な开区間たちによる P の被覆 $\{U_n\}_{n \in \mathbb{N}}$ で, $\lim_n \mu(U_n) = 0$ なるものを容易に構成できる. $\mu = \tilde{\mu}_\alpha$ なる銘 $\alpha \in \mathbb{N}^{\mathbb{N}}$ が与えられたとき, $\mu(U_n)$ は α -計算可能であるので, $\mu(U_{h(n)}) \leq 2^{-n}$ なるように選んでいけばよい. \square

定理 5.5 (Barnmpalias/Greenberg/Montalbán/Slaman 2011). 任意の K -トリビアル実数はネバー・ランダムである.

定義 5.6. $\{0,1\}^{\mathbb{N}}$ 上の無原子測度 μ が与えられているとき, $\delta_\mu : \mathbb{N} \rightarrow \mathbb{N}$ が μ の粒度 (*granularity*) であるとは, 任意の $\sigma \in \{0,1\}^{<\mathbb{N}}$ と与えられた $n \in \mathbb{N}$ に対して, 次の条件を満たすものである:

$$|\sigma| \geq \delta_\mu(n) \implies \mu(\llbracket \sigma \rrbracket) < 2^{-n}.$$

補題 5.2 (Reimann/Slaman 201X). μ を $\{0,1\}^{\mathbb{N}}$ 上の任意の無原子ボレル確率測度とする. α が μ -ランダムであり, $W \subseteq \mathbb{N}$ が $\alpha \leq_T W$ なる Σ_1^0 集合ならば, μ の粒度は W から計算可能である.

補題 5.3 (Nies 2009). 任意の K -トリビアル数はある K -トリビアル Σ_1^0 集合 $W \subseteq \mathbb{N}$ から計算可能である.

補題 5.4 (Kjos-Hanssen 2007). 実数 α について, 以下は同値である.

1. α は K -トリビアルである.
2. 普遍マーティン-レフ試験 $\{T_n\}_{n \in \mathbb{N}}$ に対して, ある λ -測度 1 未満の Σ_1^0 集合 $V \subseteq \{0, 1\}^{\mathbb{N}}$ が存在して, $T_n^\alpha \subseteq V$ となる.

補題 5.5 (Nies 2009). α を K -トリビアル数とする. $\{U_e^\alpha\}_{e \in \mathbb{N}}$ が一様 $\Sigma_1^{0,\alpha}$ 集合列ならば, 次のような計算可能関数 g と λ -測度 1 未満の Σ_1^0 集合 $V \subseteq \{0, 1\}^{\mathbb{N}}$ が存在する: 任意の e について, もし任意の $\xi \in \{0, 1\}^{\mathbb{N}}$ について $\lambda(U_e^\xi) < 2^{-g(e)}$ ならば, $U_e^\alpha \subseteq V$ である.

証明. $\{T_n\}_{n \in \mathbb{N}}$ を普遍マーティン-レフ試験とし, $\{E_n^e\}_{n \in \mathbb{N}}$ を e 番目のマーティン-レフ試験とする. $T = T_2$ とする. ある計算可能関数 f が存在して, 任意の $\xi \in \{0, 1\}^{\mathbb{N}}$ について, $E_{f(\xi)}^{e,\xi} \subseteq T^\xi$ が満たされる. Kjos-Hanssen の補題 5.4 より, T^ξ は測度 1 未満のある Σ_1^0 集合 $U \subseteq T^\xi$ に被覆される. 与えた Σ_1^0 集合 U_e に対して, マーティン-レフ試験 $\{E^{t(e)}\}_{n \in \mathbb{N}}$ で, 任意の ξ について $E_n^{t(e)} \subseteq U_e^\xi$ かつ $\lambda(E_n^{t(e)}) < 2^{-n-1}$ であり, $\lambda(U_e) < 2^{-n-1}$ ならば $U_e = E_n^{t(e)}$ なるものを返す t は容易に構成できる. よって, もし $\lambda(U_e^\xi) < 2^{-ft(e)-1}$ ならば, $U_e^\alpha = E_{ft(e)}^{t(e),\alpha} \subseteq T^\alpha \subseteq V$ が満たされる. \square

証明 (定理 5.5). β を K -トリビアル数とし, μ を任意の無原子測度とする. 補題 5.3 より, $\beta \leq_T \alpha$ なる K -トリビアル Σ_1^0 数が存在する. β が μ -ランダムであると仮定して矛盾を導く. β の収束係数は α から計算可能であるので, 補題 5.2 より, ある $s_\mu \leq_T \alpha$ によって μ のある粒度を計算できる. いま, $\beta_n[s]$ を $\beta \upharpoonright s_\mu(n)$ の時刻 s 近似とする. このとき, $\mu(\beta_n) \leq 2^{-n}$ であることが最終的には保証される. $\alpha_n[s]$ を $\beta_n[s]$ 及び $s_\mu(n)[s]$ を計算するために必要な α の時刻 s 近似の始切片とする. K -トリビアル数 α に補題 5.5 を適用して, 計算可能関数 g と Σ_1^0 集合 V を取る.

β が μ -ランダムでないことを示すために, β を捕捉する μ -ソロヴェイ試験 $\{S_n^\mu\}_{n \in \mathbb{N}}$ を構成したい. いま, 各 $r \in \mathbb{N}$ 毎に, R^r -戦略は, 以下の性質を持つ μ -ソロヴェイ試験 $\{S_n^{\mu,r}\}_{n \in \mathbb{N}}$ を作ることを目指す.

$$(\exists^\infty n) \beta \in S_n^{\mu,r} \quad \& \quad \sum_n \mu(S_n^{\mu,r}) \leq \lambda(V)$$

この要件を達成するために, 同時に R^r -戦略は $\Sigma_1^{0,\alpha}$ 集合 $U_{p(r)}^\alpha$ で $\lambda(U_{p(r)}^\alpha) \leq 2^{-g(r)}$ なるものを構成する. このとき, 再帰定理より, $U_r = U_{p(r)}$ なる r が存在するため, 補題 5.5 より $U_{p(r)}^\alpha \subseteq V$ が保証されるはずである. いま, R^r -戦略は, 無限個の部分戦略 $\{R_n^r\}_{n > g(r)}$ に分割される. 各 R_n^r -戦略は高々 2^{-n} の λ -測度を $U_{p(r)}^\alpha$ に並べることが可能である. これによって, $\lambda(U_{p(r)}^\alpha) \leq \sum_{n > g(r)} 2^{-n} \leq 2^{-g(r)}$ が保証される. R_n^r -戦略は以下の動作を行う.

1. まだ V にも $U_{p(r)}^{\alpha[s]}$ にも並べられていない λ -測度 2^{-n} の開閉集合 σ で, 他の部分戦略 $\{R_m^r\}_{m \neq n}$ によって選ばれていないものを取る.
2. この σ を使用量 $|\alpha_n[s]|$ で $U_{p(r)}^{\alpha[s]}$ に並べる. ここで s は現在時刻である.
3. 次のいずれかが満たされる時刻 $t \geq s$ まで待つ.
 - (a) α_n の変心が起こる, つまり $\alpha_n[t] \not\subseteq \alpha_n[s]$ が起こる.
 - (b) σ が V に並べられる. このとき $\lambda(V)$ が 2^{-n} 増大することに注意する.
4. もし (a) が発生したなら, この部分戦略は初期化され, 最初からやり直される. ここで (a) の発生によって, σ は $U_{p(r)}^\alpha$ から除去されていることに注意する. もし (b) が発生したなら, $\mu([\beta_n, t]) \leq 2^{-n}$ が満たされているかどうか確認し, そうであれば $\beta_{n,t}$ を S_n^μ に並べる.

この戦略は、 V の λ -測度 2^{-n} の増大を確認して初めて、 $\sum_n S_n^{\mu,r}$ の μ -測度 2^{-n} の増大を許可するため、 $\lambda(\sum_n S_n^{\mu,r}) \leq \lambda(V)$ が保証される。また、再帰定理によって得られる r について、 $U_{p(r)}^\alpha \subseteq V$ であり、最終的に $\mu([\beta_n]) \leq 2^{-n}$ となるため、全ての部分戦略 R_n^r は第4段階の動作を完遂する。 \square

定理 5.6 (Barmpalias/Greenberg/Montalbán/Slaman 2011). $\xi \leq_T W <_T 0'$ なる Σ_1^0 数 $W \subseteq \mathbb{N}$ が存在するとき、 ξ はネバー・ランダムである。

証明. μ を無原子測度とし、 ξ が μ -ランダムであると仮定して矛盾を導く。 ξ は Δ_2^0 であり、 ξ の収束係数は W から計算可能であるため、補題 5.2 より、ある $s_\mu \leq_T W$ によって μ のある粒度を計算できる。 $\Phi^{W \upharpoonright u(n)}(n) = s_\mu(n)$ なる Φ および $u \leq_T W$ を固定する。このとき、 $\mu([\Phi^{W \upharpoonright u(n)}(n)]) \leq 2^{-n}$ である。与えられた部分計算可能関数 $p: \mathbb{N} \rightarrow 2^{<\mathbb{N}}$ に対して、もし $\Phi^{p(n)}(n)$ が定義され、 $\mu([\Phi^{p(n)}(n)]) \leq 2^{-n}$ であれば、 $p(n)$ を各 $m < n$ について $U_m^{\mu,p}$ に並べる。このとき、 $\{U_n^{\mu,p}\}_{n \in \mathbb{N}}$ はマーティン-レフ μ -試験である。よって、 $\xi \notin \bigcap_n U_n^{\mu,p}$ であるから、殆ど全ての n について、 $p(n) \not\leq \alpha \upharpoonright u(n)$ である。これより、 α は自己強マーティン-レフ零ではない。しかし、これは $\alpha <_T 0'$ ならば必ず自己強マーティン-レフ零であることに矛盾する。 \square

定理 5.7 (Woodin 2008). Δ_1^1 でない無限列 $\alpha \in \{0,1\}^\mathbb{N}$ に対して、ある無限列 $\beta \in \{0,1\}^\mathbb{N}$ と、次のような全域 β -計算可能関数 $F_0, F_1: \{0,1\}^\mathbb{N} \rightarrow \{0,1\}^\mathbb{N}$ が存在する：

$$F_0(\alpha \oplus \beta) = \beta' \text{ and } F_1(\beta') = \alpha.$$

Woodin の定理は、Priky 強制法に基づき、強制法やモデル理論の知識が必要となるので、ここでは証明を省略する。

定理 5.8 (Reiman/Slaman 2008). ネバー・ランダム列 $\xi \in \{0,1\}^\mathbb{N}$ は可算種類しか存在しない。実際、任意の数列 $\xi \in \{0,1\}^\mathbb{N}$ について、もし、 ξ がネバー・ランダムならば、ある順序数 $\alpha < \omega_1^{\text{CK}}$ について、 α 回チューリングジャンプを用いて ξ を計算可能である。

結論. 如何なる意味でもランダムでないような無限列は、無限に存在する。そして、連続体濃度個存在する無限列のうち、ちょうど可算個だけが、如何なる意味でもランダムではない。

5.3 ランダムネスと強零集合

問題設定. 実数の集合論において、「ハウスドルフ次元 0 である」「普遍零である」と言った“極めて小さい”ことを意味する性質よりも、更に微小であることを意味するものとして、**強零**あるいは**強測度ゼロ**と呼ばれ

る概念がある。強零集合はあまりにも小さいため、「強零」と「可算」が等しい概念であるか否かすら、ZFC 集合論では、肯定も否定も証明できない。強零集合は、ランダムネスの理論において如何なる意味を持つだろうか？

定義 5.7 (ボレル 1919). 集合 $X \subseteq \{0,1\}^{\mathbb{N}}$ が強零 (*strongly measure zero*) であるとは、任意の正実数列 $\{\varepsilon_n\}_{n \in \mathbb{N}}$ に対して、 X を被覆する直径 ε_n 未満の区間 I_n たちの列 $\{I_n\}_{n \in \mathbb{N}}$ が存在することを言う。

演習 5.2. 以下の定理群を証明せよ。

1. (Szpilrajn 1938) 連続体仮説が真であると仮定する。このとき、非可算な強零集合が存在する (ヒント: 連続体仮説の下でルージン集合が存在することを利用せよ)。
2. (Laver 1976) ZFC が無矛盾ならば、全ての強零集合 $X \subseteq \{0,1\}^{\mathbb{N}}$ が可算であるような ZFC のモデルが存在する。したがって、ZFC の無矛盾性の仮定の下で、ZFC 集合論では、「任意の強零集合 $X \subseteq \{0,1\}^{\mathbb{N}}$ は可算である」というボレルの予想 (*Borel conjecture*) について、肯定も否定も証明できない。

定義 5.8. $\{0,1\}^{\mathbb{N}}$ 上の外測度 μ が表現可能であるとは、ある $m : \{0,1\}^{<\mathbb{N}} \rightarrow [0, \infty)$ が存在して、任意の $A \subseteq \{0,1\}^{\mathbb{N}}$ に対して、次の条件を満たすことである：

$$\mu(A) = \inf \left\{ \sum_{\sigma \in S} m(\sigma) : A \subseteq [S], \text{ and } S \subseteq \{0,1\}^{<\mathbb{N}} \right\}.$$

注意. カラテオドリの拡張定理 3.1 より、 $\{0,1\}^{\mathbb{N}}$ 上の全てのボレル測度は表現可能である。また、 s 次元ハウスドルフ測度が、表現可能な外測度の代表例である。

定義 5.9. コンパクト空間 $\{0,1\}^{\mathbb{N}}$ 上の表現可能な無原子外測度 μ が $m : \{0,1\}^{<\mathbb{N}} \rightarrow [0, \infty)$ によって表現されているとする。このとき、 $\delta_m : \mathbb{N} \rightarrow \mathbb{N}$ が表現 m の粒度 (*granularity*) であるとは、任意の $\sigma \in \{0,1\}^{<\mathbb{N}}$ と $n \in \mathbb{N}$ に対して、次の条件を満たすものである：

$$|\sigma| \geq \delta_m(n) \implies (\exists \tau \preceq \sigma) m(\tau) < 2^{-n}.$$

命題 5.1 (ベシコビッチ 1933). 集合 $X \subseteq \{0,1\}^{\mathbb{N}}$ について、以下の 3 条件は同値である。

1. X は強零集合である。
2. $\{0,1\}^{\mathbb{N}}$ 上の任意の表現可能な無原子外測度 μ について、 $\mu(X) = 0$ である。
3. 任意の次元関数 h に対して、 X の h 次元ハウスドルフ測度は 0 である。

証明. (1 \rightarrow 2) μ は表現可能なので、ある $m : \{0,1\}^{<\mathbb{N}} \rightarrow [0, \infty)$ によって表現される。 $k \in \mathbb{N}$ を固定する。表現 m の粒度 δ_m に対して、 $l_n = \delta_m(n+k+1)$ によって定義する。 X は強零なので、列 $\{l_n\}_{n \in \mathbb{N}}$ に対し、長さ l_n 以上の数列 $\sigma_n \in \{0,1\}^{l_n}$ から生成される区間列 $\{[\sigma_n]\}$ が存在して、 $X \subseteq \bigcup_n [\sigma_n]$ となる。 l_n の性質より、各 σ_n について $\rho(\tau_n) < 2^{-n-k-1}$ を満たす $\tau_n \preceq \sigma_n$ を見つけられる。このとき、 $X \subseteq \bigcup_n [\tau_n]$ なので、 $\mu(X) \leq \sum_n m(\tau_n) < 2^{-k}$ である。(2 \rightarrow 3) は明らかである。

(3 \rightarrow 1) 正整数の列 $\{l_n\}_{n \in \mathbb{N}}$ が与えられているとする。 l_{n-1} 以上 l_n 未満の長さの数列 $\sigma \in \{0,1\}^{\mathbb{N}}$ について、 $m(\sigma) = (n+1)^{-1}$ によって定義する。このとき、 m によって表現される外測度 μ に対して、あ

る次元関数 h に対する h 次元ハウスドルフ外測度 λ^h が存在して、 μ -測度 0 であることと λ^h -測度 0 であることは同値である。仮定より、 X は λ^h -零なので、ある $S \subseteq \{0,1\}^{<\mathbb{N}}$ について、 $X \subseteq \bigcup_{\sigma \in S} [\sigma]$ かつ $\sum_{\sigma \in U} m(\sigma) < 1$ を満たす。 S の元を長さが短い順に並べたものを $\{\sigma_n\}_{n \in \mathbb{N}}$ とする。もし $|\sigma_n| < l_n$ であれば、 $\sum_{i \leq n} m(\sigma_i) \geq (n+1)^{-1} \cdot (n+1) = 1$ となり矛盾を導く。よって、各 n について $|\sigma_n| \geq l_n$ を得る。 \square

系 5.2. $\{0,1\}^{\mathbb{N}}$ の任意の部分集合について、強零ならば、ハウスドルフ次元 0 であり、普遍零である。

定義 5.10. X を任意の集合とする。函数 $m : \mathcal{P}(X) \rightarrow \mathbb{R}_{\geq 0} \cup \{\infty\}$ が**外測度** (*outer measure*) であるとは、以下の条件を満たすときを言う。

1. $m(\emptyset) = 0$.
2. $A \subseteq B \subseteq X$ ならば、 $m(A) \leq m(B)$ である。
3. (劣加法性) $m(\bigcup_{i \in \mathbb{N}} A_i) \leq \sum_{i \in \mathbb{N}} m(A_i)$.

定義 5.11. 函数 $\rho : \{0,1\}^{<\mathbb{N}} \rightarrow \mathbb{R}_{\geq 0}$ が与えられたとき、外測度 $\mu_\rho^* : \mathcal{P}(X) \rightarrow \mathbb{R}_{\geq 0}$ を次によって与える：

$$\mu_\rho^*(A) = \inf \left\{ \sum_{\sigma \in U} \rho(\sigma) : A \subseteq \bigcup_{\sigma \in U} [\sigma] \right\}.$$

したがって、 $N \subseteq \{0,1\}^{\mathbb{N}}$ が μ_ρ^* -零集合であるとき、任意の n について、次を満たす $U_n \subseteq \{0,1\}^{<\mathbb{N}}$ が存在する：

$$\sum_{\sigma \in U_n} \rho(\sigma) \leq 2^{-n} \text{ \& } N \subseteq \bigcup_{\sigma \in U_n} [\sigma].$$

$N \subseteq \{0,1\}^{\mathbb{N}}$ が**マーティン=レフ μ_ρ^* -零**であるとは、次を満たす Σ_1^0 集合列 $\{U_n\}_{n \in \mathbb{N}} \in (\{0,1\}^{<\mathbb{N}})^{\mathbb{N}}$ が存在するときを言う。

$$\sum_{\sigma \in U_n} \rho(\sigma) \leq 2^{-n} \text{ \& } N \subseteq \bigcup_{\sigma \in U_n} [\sigma].$$

定義 5.12 (木原 2011; 樋口/木原 2012). 集合 $X \subseteq \{0,1\}^{\mathbb{N}}$ が**実効強零** (*effectively strongly measure zero*) であるとは、任意の計算可能正実数列 $\{\varepsilon_n\}_{n \in \mathbb{N}}$ に対して、 X を被覆する直径 ε_n 未満の区間 I_n たちの列 $\{I_n\}_{n \in \mathbb{N}}$ が存在することを言う。

♠: まだ書きかけ

第6章

力学系とエントロピー

6.1 次元 = エントロピー = 複雑性

問題設定. さて, “普通の図形” に対しては, 位相次元とハウスドルフ次元は等しい. 同様に, 実効ハウスドルフ次元もまた等しい. また, フラクタル幾何学で扱われるような “普通のフラクタル図形” に対しては, ハウスドルフ次元と実効ハウスドルフ次元は等しい. これより, フラクタル図形の次元を, コルモゴロフ複雑性の計算によって求めることが可能になる. では, 少しフラクタル図形とは少し異なる対象であるが, ある種の力学系に関しては, その位相エントロピーやハウスドルフ次元を, コルモゴロフ複雑性から求めることが可能であるという.

以後, 自然数 $k \in \mathbb{N}$ について, $\mathbf{k} = \{0, 1, \dots, k-1\}$ とする. コンパクト空間 X と, X 上の連続関数 $T: X \rightarrow X$ の組 (X, T) を **力学系** (*dynamical system*) と呼ぶ. ここでは, 各点 $x \in X$ の軌道の長期挙動 $(T^n(x): n \in \mathbb{N})$ に焦点を当てよう. 力学系のエントロピーは, 指数的増大率を定量化するために用いられる.

力学系 (X, T) を研究する方法の1つとして, それに**記号力学系** (*symbolic dynamical system*) を対応させるという方法がある. これは, X を有限個の領域 $(X_i)_{i < k}$ に分割し, 各点 $x \in X$ の軌道 $(T^n(x))_{n \in \mathbb{N}}$ の代わりに, 各時刻で訪れる領域の番号の列 $\text{It}(x) = (i[x; n]: n \in \mathbb{N}) \in \mathbf{k}^{\mathbb{N}}$ を見るというものである. ここで, $T^n(x) \in X_i$ なる i を $i[x; n]$ とする. ところで, $i[T(x); n] = i[x; n+1]$ であるから, T は $\mathbf{k}^{\mathbb{N}}$ 上の**シフト写像** (*shift map*) $\text{sh}: \mathbf{k}^{\mathbb{N}} \rightarrow \mathbf{k}^{\mathbb{N}}$ に対応する. つまり, 各 $\alpha \in \mathbf{k}^{\mathbb{N}}$ について $\text{sh}(\alpha)(n) = \alpha(n+1)$ によって定義される写像である. この $\text{It}_{X,T} = \{\text{It}(x): x \in X\}$ と sh の組 $(\text{It}_{X,T}, \text{sh})$ は代表的な記号力学系である.

例 6.1. 図 6.1 の力学系 (X, T) における位相空間 X に対して, 図 6.2 のように, たとえば4分割 $\{X_i\}_{i < 4}$ を与えることによって, 記号力学系 $(\text{It}_{X,T}, \text{sh})$ が得られる. このとき, $x \in X$ に対応するものは, その軌道 $(T^n(x))_{n \in \mathbb{N}}$ が訪れる領域番号の列 $\text{It}(x) = (2, 3, 0, 1, 1, 3, \dots)$ である.

定義 6.1 (位相エントロピー; Adler/Konheim/McAndrew 1965). コンパクト空間 X の開被覆 \mathcal{U} のエントロピーとは, 次によって与えられる値である.

$$\mathcal{H}_X(\mathcal{U}) = \log \min\{\#\mathcal{F} : \mathcal{F} \subseteq \mathcal{U}, \text{ and } X \subseteq \bigcup \mathcal{F}\}.$$

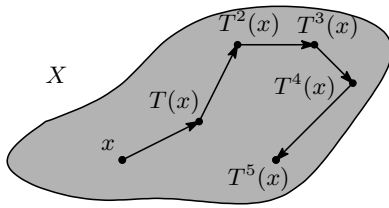


図 6.1 力学系 (X, T)

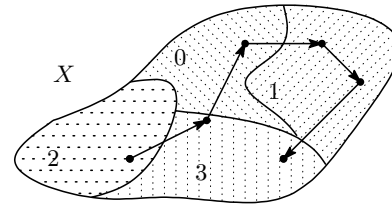


図 6.2 記号力学系 $(It_{X,T}, sh)$

いま、 X の開被覆 \mathcal{U} と \mathcal{V} が与えられているとき、

$$\mathcal{U} \vee \mathcal{V} = \{U \cap V : U \in \mathcal{U}, \text{ and } V \in \mathcal{V}\}$$

とし、 $T^{-1}\mathcal{U} = \{T^{-1}(U) : U \in \mathcal{U}\}$ によって定義する。このとき、任意の連続関数 $T : X \rightarrow X$ に対して、次の極限值は存在する。

$$\mathcal{H}(X, T, \mathcal{U}) = \lim_{n \rightarrow \infty} \frac{1}{n} \mathcal{H}_X(\mathcal{U} \vee T^{-1}\mathcal{U} \vee \dots \vee T^{-(n-1)}\mathcal{U}).$$

このとき、力学系 (X, T) の位相エントロピー (topological entropy) は、次によって定義される：

$$\text{ent}(X, T) = \sup\{\mathcal{H}(X, T, \mathcal{U}) : \mathcal{U} \text{ は } X \text{ の開被覆である}\}.$$

定義 6.2. 集合 $S \subseteq \mathbf{k}^{\mathbb{N}}$ がシフト不変 (shift invariant) であるとは、任意の $n \in \mathbb{N}$ および $\alpha \in S$ に対して、 $sh^n(\alpha) \in S$ であるときを言う。集合 $S \subseteq \mathbf{k}^{\mathbb{N}}$ がサブシフト (subshift) であるとは、 S が $\mathbf{k}^{\mathbb{N}}$ の空でない閉部分集合であり、シフト不変であるときを言う。

$S \subseteq \mathbf{k}^{\mathbb{N}}$ がサブシフトであるとき、 $(S, sh|_S)$ はコンパクト力学系である。このとき、単に $\text{ent}(S) = \text{ent}(S, sh|_S)$ と書く。

補題 6.1. $S \subseteq \mathbf{k}^{\mathbb{N}}$ がサブシフトであるならば、位相エントロピーは次によって与えられる：

$$\text{ent}(S) = \lim_{n \rightarrow \infty} \frac{\log(\#\{\alpha \upharpoonright n : \alpha \in S\})}{n}$$

定理 6.1 (Simpson 201x). $S \subseteq \mathbf{k}^{\mathbb{N}}$ をサブシフトとする。このとき、次の等式が成立する：

$$\text{ent}(S) = \dim_H(S) = \sup_{\alpha \in S} \liminf_{n \rightarrow \infty} \frac{K(\alpha \upharpoonright n)}{n}$$

補題 6.2. $S \subseteq \mathbf{k}^{\mathbb{N}}$ がサブシフトならば、 $\dim_H(S) = \text{edim}_H(S)$ である。

証明. $\dim_H(S) \leq \text{edim}_H(S)$ であることは明らかである。一方、 S の s 次元ハウスドルフ測度が 0 ならば、 S のコンパクト性と合わせて、次のような有限集合 $I \subseteq \{0, 1\}^{<\mathbb{N}}$ が存在する：

$$S \subseteq \bigcup_{\sigma \in I} [\sigma], \text{ かつ } \sum_{\sigma \in I} 2^{-s|\sigma|} \leq \frac{1}{2}.$$

$I^{(k)}$ を I の要素の k 個の組合せから構成される有限列全体の集合とする, すなわち $I^{(k)} = \{\sigma_1 \frown \dots \frown \sigma_k : \sigma_1, \dots, \sigma_k \in I\}$ によって定義する. このとき, S がサブシフトであることから, $\alpha \in S$ が $\sigma \frown \alpha^*$ と表されるとき, $\alpha^* \in S$ である. したがって, I が S を被覆することから, 任意の $\sigma \prec \alpha$ に対して, ある $\tau \in I$ が存在して, $\alpha \in [\sigma \frown \tau]$ を満たす. これより, 任意の $k \in \mathbb{N}$ について $S \subseteq [I^{(k)}]$ である. さらに,

$$\sum_{\sigma \in I^{(k)}} 2^{-s|\sigma|} = \sum_{(\sigma_1, \dots, \sigma_k) \in I^k} 2^{-s(|\sigma_1| + \dots + |\sigma_k|)} = \left(\sum_{\sigma_1 \in I} 2^{-s|\sigma_1|} \right) \dots \left(\sum_{\sigma_k \in I} 2^{-s|\sigma_k|} \right) = \left(\sum_{\sigma \in I} 2^{-s|\sigma|} \right)^k \leq 2^{-k}$$

が成立する. また, I が有限集合列であることから $\{I^{(k)}\}_{k \in \mathbb{N}}$ は計算的枚挙可能集合列なので, S の s 次元ハウスドルフ測度は実効的に零である. よって, $\text{edim}_H(S) \leq \dim_H(S)$ を得る. \square

定理 6.2 (Furstenberg 1967). $S \subseteq \mathbf{k}^{\mathbb{N}}$ がサブシフトならば, $\text{ent}(S) = \dim_H(S)$ である.

補題 6.3. 任意のサブシフト $S \subseteq \mathbf{k}^{\mathbb{N}}$ について, $\text{ent}(S) \geq \dim_H(S)$ である.

証明 (定理 6.2). いま, \mathcal{U} を S の有限被覆とする. このとき, ある有限集合 $I \subseteq \{0, 1\}^{<\mathbb{N}}$ が存在して, $\mathcal{U} = \{[\sigma] : \sigma \in I\}$ を満たすと仮定して一般性を失わない. \mathcal{U} が被覆であり, S がサブシフトであることから, 任意の $\alpha \in S$ に対して, I の要素の列 $\{\sigma_i\}_{i \in \mathbb{N}} \subseteq I$ が存在して,

$$\alpha = \sigma_0 \frown \sigma_1 \frown \sigma_2 \frown \dots$$

と表すことができる. このとき, 各 $n \in \mathbb{N}$ について, 次のような $k \in \mathbb{N}$ を取る.

$$\sigma_0 \frown \dots \frown \sigma_{k-1} \prec \alpha \upharpoonright n \preceq \sigma_0 \frown \dots \frown \sigma_k.$$

$m = \max\{|\sigma| : \sigma \in I\}$ とすれば, 任意の $n \in \mathbb{N}$ について, $S \upharpoonright n$ は, I の有限個の組合せで, 長さが $n+m$ 未満のものだけを用いて網羅することができる.

いま, S の s 次元ハウスドルフ測度が 0 であると仮定する. このとき, S の位相エントロピーが s 以下であることを示せばよい. つまり, $\lim_{n \rightarrow \infty} 2^{-sn} \#S \upharpoonright n$ が有界であることを示す. さて, $\lambda^s(S) = 0$ および S のコンパクト性より, 次のような有限集合 $I \subseteq \{0, 1\}^{<\mathbb{N}}$ が存在する:

$$S \subseteq \bigcup_{\sigma \in I} [\sigma], \text{ かつ } \sum_{\sigma \in I} 2^{-s|\sigma|} < 1.$$

このとき, スケール s での I の要素の有限組合せ全体の重みは次のように有界であることが分かる:

$$\sum_{(\sigma_0, \dots, \sigma_k) \in I^{<\mathbb{N}}} 2^{-s(|\sigma_0| + \dots + |\sigma_k|)} = \sum_{j=1}^{\infty} \left(\sum_{\sigma \in I} 2^{-s|\sigma|} \right)^j < \infty$$

この有限の値を M とおく. $S \upharpoonright n$ の各要素に対して, I の要素の有限組合せ $(\sigma_0, \dots, \sigma_k)$ が対応し, さらに $2^{-sn} < 2^{ms} 2^{-s(|\sigma_0| + \dots + |\sigma_k|)}$ が満たされる. これより, $2^{-sn} \#S \upharpoonright n < 2^{ms} M$ が成立する. よって, $\lim_{n \rightarrow \infty} 2^{-sn} \#S \upharpoonright n$ が有界となることから, $\text{ent}(S) \leq s$ となることが示された. \square

証明 (定理 6.1). 定理 3.9, 補題 6.2, および定理 6.2 による. \square

定義 6.3 (測度論的エントロピー). (X, μ) を確率空間とする. 関数 $T: X \rightarrow X$ が保測 (*measure-preserving*) であるとは, 任意の μ -可測集合 $P \subseteq X$ に対して $\mu(T^{-1}(P)) = \mu(P)$ を満たすことである. このような組 (X, T, μ) を保測力学系 (*measure-preserving dynamical system*) と呼ぶ. 空間 X の μ -可測集合による有限分割 \mathcal{P} を可測分割と呼ぶ. 可測分割 \mathcal{P} のエントロピーを次によって定義する:

$$\mathcal{H}_{X, \mu}(\mathcal{P}) = - \sum_{P \in \mathcal{P}} \mu(P) \log \mu(P).$$

いま, \mathcal{P} と \mathcal{Q} が X の可測分割ならば, $\mathcal{P} \vee \mathcal{Q}$ や $T^{-1}(\mathcal{P})$ は以前と同様にして定義される. このとき,

$$\mathcal{H}(X, T, \mu, \mathcal{P}) = \lim_{n \rightarrow \infty} \frac{1}{n} \mathcal{H}_{X, \mu}(\mathcal{P} \vee T^{-1}\mathcal{P} \vee \dots \vee T^{-(n-1)}\mathcal{P})$$

としたとき, 保測力学系 (X, T, μ) の測度論的エントロピー (*measure-theoretic entropy*) とは, 次によって定義される値である:

$$\text{ent}(X, T, \mu) = \sup\{\mathcal{H}(X, T, \mu, \mathcal{P}) : \mathcal{P} \text{ は } X \text{ の可測分割である}\}.$$

定義 6.4. $S \subseteq \mathbf{k}^{\mathbb{N}}$ をサブシフトとする. S 上のボレル確率測度 μ がエルゴード的 (*ergodic*) とは, 任意の μ -可測集合 $P \subseteq S$ で $\text{sh}^{-1}(P) \subseteq P$ なるものについて, $\mu(P) \in \{0, 1\}$ となることである. μ がシフト不変 (*shift-invariant*) であるとは, 任意のボレル集合 $P \subseteq S$ に対して, $\mu(\text{sh}^{-1}(P)) = \mu(P)$ となるときを言う. この場合, $(S, \text{sh}|_S, \mu)$ は保測力学系となり, その測度論的エントロピーを単に $\text{ent}(S, \mu)$ と書く.

定理 6.3 (Shannon/McMillan/Breiman). $S \subseteq \mathbf{k}^{\mathbb{N}}$ がサブシフトで, μ が S 上のエルゴード的シフト不変確率測度であるならば, μ -殆ど全ての $\alpha \in S$ について, 次の等式が成立する:

$$\text{ent}(S, \mu) = \lim_{n \rightarrow \infty} \frac{-\log \mu(\llbracket \alpha \upharpoonright n \rrbracket)}{n}. \quad \square$$

定理 6.4 (変分原理). 任意のサブシフト $S \subseteq \mathbf{k}^{\mathbb{N}}$ に対して, 次が成立する.

$$\text{ent}(S) = \max\{\text{ent}(S, \mu) : \mu \text{ は } \mathbf{k}^{\mathbb{N}} \text{ 上のエルゴード的シフト不変確率測度である}\}. \quad \square$$

定理 6.5 (Simpson 201x). $S \subseteq \mathbf{k}^{\mathbb{N}}$ をサブシフトとする. このとき, 次の等式を満たす一点 $\alpha \in S$ が存在する.

$$\text{ent}(S) = \dim_H(S) = \dim_H(\alpha) = \liminf_{n \rightarrow \infty} \frac{K(\alpha \upharpoonright n)}{n}.$$

証明. 変分原理 6.4 より, S 上のあるエルゴード的シフト不変確率測度 μ で, $\text{ent}(S) = \text{ent}(S, \mu)$ となるものが存在する. 実数 $s < \text{ent}(S)$ を任意に取る. いま, $s + \varepsilon < \text{ent}(S)$ なる正実数 $\varepsilon > 0$ を任意に取る. このとき, Shannon/McMillan/Breiman の定理 6.3 より, μ -殆ど全ての $\alpha \in S$ と十分大きい任意の $n \in \mathbb{N}$ に対して,

$$\frac{-\log \mu(\llbracket \alpha \upharpoonright n \rrbracket)}{n} > s + \varepsilon$$

が成立する。よって、

$$T_n = \{\sigma \in \mathbf{k}^n : \mu([\sigma]) < 2^{-(s+\varepsilon)|\sigma|}\}$$

と定義すると、 μ -殆ど全ての $\alpha \in S$ に対して、十分大きな $n \in \mathbb{N}$ について $\alpha \in [T_n]$ である。各 $n \in \mathbb{N}$ に対して、次の集合 U_n を考える：

$$U_n = \{\sigma \in \mathbf{k}^n : K(\sigma) < s|\sigma|\}.$$

このとき、明らかに $\#U_n \leq 2^{sn}$ である。よって、各 $n \in \mathbb{N}$ に対して、

$$\mu([U_n] \cap [T_n]) = \mu([U_n \cap T_n]) < 2^{sn} 2^{-(s+\varepsilon)n} = 2^{-\varepsilon n}$$

が成立するから、

$$\sum_{n=1}^{\infty} \mu([U_n] \cap [T_n]) < \infty$$

を得る。ボレル/カンテリの補題より、 μ -殆ど全ての $\alpha \in S$ と十分大きな $n \in \mathbb{N}$ に対して、 $\alpha \notin [U_n] \cap [T_n]$ である。これより、 μ -殆ど全ての $\alpha \in S$ と十分大きな $n \in \mathbb{N}$ に対して、 $\alpha \notin [U_n]$ を得る。つまり、 $K(\alpha \upharpoonright n) \geq sn$ である。任意の $s < \text{ent}(S)$ について、次の集合 Q_s を考える：

$$Q_s = \{\alpha \in S : (\exists c \in \mathbb{N})(\forall n) K(\alpha \upharpoonright n) \geq sn - c\}.$$

ここまでに、任意の $s < \text{ent}(S)$ について、 $\mu(Q_s) = 1$ であることを示した。よって、

$$Q = \bigcap \{Q_s : s \in \mathbb{Q}, \text{ and } s < \text{ent}(S)\}$$

は μ -測度 1 であり、定理 3.9 より、任意の $\alpha \in Q \subseteq S$ は $\text{ent}(S) \leq \dim_H(\alpha)$ を満たす。明らかに $\dim_H(\alpha) \leq \text{edim}_H(S)$ であるから、定理 6.1 と組み合わせることによって、目的の等式を得る。□

結論。サブシフトと呼ばれる特殊な力学系においては、その空間の位相エントロピーやハウスドルフ次元といった大域的情報は、その空間内のたった一点に全て取り込まれる。つまり、サブシフトの位相エントロピーとハウスドルフ次元を求めるためには、その空間内の具体的な一点の圧縮率、すなわち実効ハウスドルフ次元、を求めればよい。

第 7 章

【付録】 計算可能性理論の予備知識

ここに計算論の予備知識をまとめる。第 7 節で挙げる定理の証明は、大抵の計算可能性理論の入門書に載っているの、ここでは結果を述べるだけにする。

7.1 ボレル階層と超算術的階層

問題設定。ボレル集合って、測度論や確率論でよく出てくるけど、その正体は一体なんだろう。ボレル集合が構成可能性と関係があると聞いたことがあるけれど、計算可能性とはどういう関係があるのかな？

定義 7.1 (ボレル 1898). 集合 S の部分集合の族 $\mathcal{F} \subseteq \mathcal{P}(S)$ が、補集合演算と可算和を取る操作で閉じているとき、 σ -加法族 (σ -algebra) であると言う。位相空間 S が与えられたとき、 \mathcal{B} を、 S の開集合全体を含む最小の σ -加法族を表すものとし、各 $B \in \mathcal{B}$ はボレル集合 (Borel set) と呼ばれる。

定義 7.2 (ボレル階層; ハウスドルフ 1914). $U \subseteq \{0, 1\}^{\mathbb{N}}$ が開 (open) または Σ_1^0 であるとは、ある $S \subseteq \{0, 1\}^{<\mathbb{N}}$ が存在して、 $U = [S]$ となることである。開集合の補集合は閉 (closed) または Π_1^0 と呼ばれる。可算個の閉集合 $\{F_n\}_{n \in \mathbb{N}}$ の和 $\bigcup_{n \in \mathbb{N}} F_n$ は、 \mathbf{F}_σ または Σ_2^0 と呼ばれる。可算個の開集合 $\{G_n\}_{n \in \mathbb{N}}$ の共通部分 $\bigcap_{n \in \mathbb{N}} G_n$ は、 \mathbf{G}_δ または Π_2^0 と呼ばれる。 Π_2^0 集合であることと Σ_2^0 集合の補集合であることは同値である。より一般に、順序数 ξ について、

- $\Sigma_{\xi+1}^0$ 集合とは、可算個の Π_ξ^0 集合の和である。
- $\Pi_{\xi+1}^0$ 集合とは、 $\Sigma_{\xi+1}^0$ 集合の補集合である。
- ξ が極限順序数ならば、 Σ_ξ^0 集合とは、ある $\zeta_0, \zeta_1, \dots < \xi$ について $\Pi_{\zeta_n}^0$ 集合たちの可算和である。
- Σ_ξ^0 かつ Π_ξ^0 であるような集合を Δ_ξ^0 集合と呼ぶ。

注意。可算和 \bigcup が自然数への存在量化 ($\exists n \in \mathbb{N}$)、可算共通部分 \bigcap が自然数への全称量化 ($\forall n \in \mathbb{N}$)、補集合演算が否定 \neg に対応しているように、位相空間のボレル階層 (Borel hierarchy) は、述語論理 (predicate logic) の \forall と \exists の累積の階層、すなわち算術的階層 (arithmetical hierarchy) および超算術的階層 (hyperarithmetical hierarchy) に対応している。たとえば、無限列空間 $\{0, 1\}^{\mathbb{N}}$ の部分集合 V が Σ_5^0 であるとは、

$$V = \{\alpha \in \{0, 1\}^{\mathbb{N}} : (\exists n_1 \in \mathbb{N})(\forall n_2 \in \mathbb{N})(\exists n_3 \in \mathbb{N})(\forall n_4 \in \mathbb{N})(\forall n_5 \in \mathbb{N}) \theta(\alpha, n_0, \dots, n_5)\}$$

のような \exists と \forall の 5 回の累積で表されることと同値である.

例 7.1. ボレル階層は, より一般の位相空間に対して定義される.

1. 有理数全体の集合 \mathbb{Q} と代数的実数全体の集合 $\mathbb{R} \cap \overline{\mathbb{Q}}$ は, 共に \mathbb{R} の Σ_2^0 集合である.
2. $\text{Freq}(\alpha) = 1/2$ なる $\alpha \in \{0, 1\}^{\mathbb{N}}$ 全体の集合は, λ -測度 1 の Π_3^0 集合である.
3. f が $[0, 1]$ 上の連続関数ならば, f の微分可能点全体の集合は, $[0, 1]$ の Π_3^0 集合である.
4. $K(\{0, 1\}^{\mathbb{N}})$ を $\{0, 1\}^{\mathbb{N}}$ のコンパクト部分集合全体のなすヴィトリリス位相による空間とする. このとき, λ -測度 0 のコンパクト集合 $K \subseteq \{0, 1\}^{\mathbb{N}}$ 全体の集合は $K(\{0, 1\}^{\mathbb{N}})$ の Π_2^0 集合である.

命題 7.1 (ルベーク 1905). 如何なる非可算な完備可分距離空間においても, 任意の $1 \leq \xi < \omega_1$ について, Σ_ξ^0 であるが Π_ξ^0 でない集合, および Π_ξ^0 であるが Σ_ξ^0 でない集合が存在する.

定義 7.3. $n \in \mathbb{N}$ とする. 射影階層 (*projective hierarchy*) あるいはルジン階層 (*Lusin hierarchy*) は, 以下によって定義される.

1. ボレル集合 B の連続関数による像を Σ_1^1 集合と呼ぶ.
2. Σ_n^1 集合の補集合を Π_n^1 集合と呼ぶ.
3. Π_n^1 集合の連続関数による像を Σ_{n+1}^1 集合と呼ぶ.
4. Σ_n^1 かつ Π_n^1 であるような集合を Δ_n^1 集合と呼ぶ.

注意. 射影階層は, ボレル階層に加え, 射影に対応する存在量化 ($\exists \alpha \in \{0, 1\}^{\mathbb{N}}$) または ($\exists X \subseteq \mathbb{N}$) と, 余射影に対応する全称量化 ($\forall \alpha \in \{0, 1\}^{\mathbb{N}}$) または ($\forall X \subseteq \mathbb{N}$) が加わり, 論理的には, 二階算術 (*second-order arithmetic*) に関係している.

例 7.2.

1. \mathbb{R}^2 の単連結部分集合全体の集合は, 共に $K(\mathbb{R}^n)$ の Π_1^1 集合である.
2. $n \geq 3$ について, \mathbb{R}^n の単連結部分集合全体の集合は, 共に $K(\mathbb{R}^n)$ の Π_2^1 集合である.
3. $n \geq 2$ について, \mathbb{R}^n の弧状連結部分集合全体の集合は, 共に $K(\mathbb{R}^n)$ の Π_2^1 集合である.

定理 7.1 (Suslin の定理 1917). 任意の集合 $B \subseteq \{0, 1\}^{\mathbb{N}}$ について, 以下の 3 条件は同値である.

1. B はボレル集合である.
2. ある順序数 $\xi < \omega_1$ について, B は Σ_ξ^0 集合である.
3. B は Δ_1^1 集合である.

命題 7.2 (Suslin 1917). 如何なる非可算な完備可分距離空間においても, 任意の自然数 $n \geq 1$ について, Σ_n^1 であるが Π_n^1 でない集合, および Π_n^1 であるが Σ_n^1 でない集合が存在する. よってボレル集合でないような Σ_1^1 集合が存在する.

定理 7.2 (ゲーデル 1938;). 「ルベーク非可測な Δ_2^1 集合が存在する」という主張は ZFC と無矛盾である.

定理 7.3 (Martin/Solovay 1970). Σ_2^1 集合は, \aleph_1 個のボレル集合の和である. 逆に, \aleph_1 個のボレル集合の和が Σ_2^1 集合であるかどうかは, ZFC では肯定も否定も証明できない.

定義 7.4. $\varphi(\vec{p})$ を自然数変数記号 $\{x, y, z, \dots\}$, 自然数上の演算/関係/定数記号 $\{+, \times, \leq, =, 0, 1\}$, および述

語論理記号 $\{\vee, \wedge, \neg, \rightarrow, \forall, \exists\}$ の有限個の組合せで構成される論理式で、有限個の自然数パラメータ \vec{p} を持ち得るものとする。このとき、

1. $\varphi(\vec{p})$ が Σ_0^0 あるいは Π_0^0 であるとは、 φ に現れる量化記号が全て有界である、つまり $\forall x < t \exists y < u$ の形であるときを指す。
2. $\varphi(\vec{p})$ が Σ_{n+1}^0 であるとは、ある Π_n^0 論理式 $\psi(\vec{p}, q)$ について、 $(\exists x \in \mathbb{N}) \psi(\vec{p}, x)$ の形であるときを指す。
3. $\varphi(\vec{p})$ が Π_{n+1}^0 であるとは、ある Σ_n^0 論理式 $\psi(\vec{p}, q)$ について、 $(\forall x \in \mathbb{N}) \psi(\vec{p}, x)$ の形であるときを指す。

このような形の論理式を**算術的論理式 (arithmetical formula)**と呼び、特にパラメータを持たない論理式を**文 (sentence)**と呼ぶ。 $\Gamma \in \{\Sigma_n^0, \Pi_n^0\}_{n \in \mathbb{N}}$ とする。 Γ 論理式 $\varphi(n)$ によって定義される集合 $A = \{n \in \mathbb{N} : \varphi(n)\}$ を Γ 集合と呼ぶ。 $A \subseteq \mathbb{N}$ が Σ_n^0 かつ Π_n^0 であるとき、 Δ_n^0 であると呼ばれる。 また、 $\Gamma \in \{\Sigma_n^0, \Pi_n^0, \Delta_n^0\}_{n \in \mathbb{N}}$ に対して、無限列 $\alpha \in \{0, 1\}^{\mathbb{N}}$ が Γ であるとは、 $\hat{\alpha} = \{n \in \mathbb{N} : \alpha(n) = 1\}$ が Γ 集合であるときを指す。

例 7.3.

1. ゴールドバッハ予想とフェルマーの最終定理は共に Π_1^0 文である。
2. リーマン予想と同値な Π_1^0 文が存在する。
3. $P = NP$ は Π_2^0 文である。

定義 7.5. 本稿では、計算可能性の厳密な数学的定義は述べないが、以下のようなものと想定しておけば十分である。部分関数 $f : \subseteq X \rightarrow Y$ が**計算可能 (computable)** であるとは、あるプログラム \mathcal{A} で、任意の $x \in X$ について、以下の2条件を満たすものが存在することである。

1. $x \in \text{dom}(f) \iff \mathcal{A}$ に x を入力したときの計算が有限時間で出力を返す。
2. $x \in \text{dom}(f)$ ならば、 \mathcal{A} に x を入力したときの出力が $f(x)$ である。

有限文字列を自然数 $e \in \mathbb{N}$ によってコードすれば、あらゆるプログラムは自然数に置き換わる。自然数 e が表すプログラムによって表される計算可能関数を Φ_e と書く。

以後、通常の入力 $x \in X$ の他に、何らかの無限列 $\alpha \in \{0, 1\}^{\mathbb{N}}$ を徐々に読み込む計算も考える。この場合、プログラム内に “ $y := \text{Oracle}(x)$ ” の形の命令を用いてよい。無限列を読み込んでない場合には、単にこの命令は無視されるが、もし無限列 $\alpha \in \{0, 1\}^{\mathbb{N}}$ を読み込んでいる場合、“ $y := \text{Oracle}(x)$ ” は「変数 y に $\alpha(x)$ の値を代入せよ」という命令と解釈される。自然数 e が表すプログラムに無限列 $\alpha \in \{0, 1\}^{\mathbb{N}}$ を読み込ませることによって表される計算可能関数を Φ_e^α と書く。

ある $e \in \mathbb{N}$ について、 $\Phi_e^\alpha = \beta$ であるとき、 β は α に**チューリング還元可能 (Turing reducible)** あるいは β は α から**計算可能である** と言い、 $\beta \leq_T \alpha$ と書く。

命題 7.3 (Post 1943). 任意の $\alpha, \beta \in \{0, 1\}^{\mathbb{N}}$ について、次の性質が成り立つ。

1. α が計算可能 $\iff \alpha$ は Δ_1^0 である。
2. $\alpha \leq_T \beta \iff \alpha$ は $\Delta_1^0(\beta)$ である。

定義 7.6. 無限列 $\alpha \in \{0, 1\}^{\mathbb{N}}$ に対して、 α -**相対的停止問題 (halting problem relative to α)** とは、次によって定義される無限列 $\alpha' \in \{0, 1\}^{\mathbb{N}}$ である。

$$\alpha'(\langle e, n \rangle) = 1 \iff n \in \text{dom}(\Phi_e^\alpha).$$

このとき、自然数 $n \in \mathbb{N}$ について、帰納的に、 $\alpha^{(0)} = \alpha$, $\alpha^{(n+1)} = (\alpha^{(n)})'$ と定義する. $\alpha^{(n)}$ を α の n 回 チューリングジャンプ (*the n -th Turing jump*) と呼ぶ.

注意. 停止問題 \emptyset' を \mathbb{N} の部分集合として見たとき、これは Σ_1^0 である. Σ_1^0 集合はしばしば**再帰的可算** (*recursively enumerable*) または**計算的枚挙可能** (*computably enumerable*) と呼ばれる.

命題 7.4 (Post の定理 1943). 任意の $\alpha, \beta \in \{0, 1\}^{\mathbb{N}}$ について、次の性質が成り立つ.

1. $\alpha \leq_T \emptyset^{(n)} \iff \alpha$ は Δ_{n+1}^0 である.
2. $\alpha \leq_T \beta^{(n)} \iff \alpha$ は $\Delta_{n+1}^0(\beta)$ である.

命題 7.5 (Shoenfield の極限補題). 任意の $\alpha, \beta \in \{0, 1\}^{\mathbb{N}}$ について、以下の 3 条件は同値である.

1. $\alpha \leq_T \beta^{(n)}$;
2. $\alpha \in \Delta_{n+1}^0(\beta)$;
3. ある $\gamma \leq_T \beta$ なる $\gamma \in \{0, 1\}^{\mathbb{N} \times \mathbb{N} \times \dots \times \mathbb{N}}$ が存在して、任意の $k \in \mathbb{N}$ について、次が成立する.

$$\alpha(u) = \lim_{v_0 \rightarrow \infty} \lim_{v_1 \rightarrow \infty} \dots \lim_{v_{n-1} \rightarrow \infty} \gamma(u, v_0, v_1, \dots, v_{n-1}).$$

注意. Shoenfield の極限補題より、特に Δ_2^0 であることを**極限計算可能** (*limit computable*) と呼ぶことがある.

注意. 最小の計算不可能順序数を**チャーチ・クリーネ順序数** (*Church-Kleene ordinal*) と呼び、 ω_1^{CK} と書く. 本稿では詳細を述べないが、構成的無限命題論理を用いることによって、順序数 $\xi < \omega_1^{\text{CK}}$ について、 Σ_ξ^0 , Π_ξ^0 , Δ_ξ^0 を定義できる. また、任意の順序数 $\xi < \omega_1^{\text{CK}}$ に対して、 ξ 回チューリングジャンプを定義することも可能である. ただし、順序数回のチューリングジャンプが矛盾なく定義できることは、あくまで定理である. たとえば、エルショフによれば、変心の階層の順序数回の累積、あるいは、フェフターマンによれば、再帰的公理化可能理論 T に対する無矛盾性述語 $\text{Con}(T)$ の順序数回の累積などを矛盾なしに定義することは不可能である. したがって、計算可能性/定義可能性等が問題となる状況では、順序数回累積の概念には注意を払わなければならない. 彼等は、順序数に対して累積を定義するのではなく、記法に対する分岐型の累積を定義することによって、矛盾を避けている.

命題 7.6 (チューリング). 任意の $\alpha \in \{0, 1\}^{\mathbb{N}}$ に対して、 α' は α から計算不可能である. よって、任意の順序数 $\xi < \omega_1^{\text{CK}}$ に対して、 Σ_ξ^0 だが Π_ξ^0 でない無限列、および Π_ξ^0 だが Σ_ξ^0 でない無限列が存在する.

例 7.4 (数学基礎論における例).

1. ZFC で証明可能な算術的文全体の集合 $\{[\varphi] : \text{ZFC} \vdash \varphi\}$ は Σ_1^0 である (ZFC でなくとも、任意の再帰的公理化可能理論についてこの性質は満たされる).
2. **算術の真理** (*true arithmetic*), つまり「与えられた算術的文の真偽を決定せよ」という問題 $\text{Th}(\mathbb{N})$ は Σ_ω^0 であり、さらに、この問題の難易度 (次数) に関して、 $\emptyset^{(\omega)} \leq_T \text{Th}(\mathbb{N})$ が成立する.
3. Σ_1^0 と Σ_ω^0 には大幅な差があることから、いま、「算術を表現できる ω -無矛盾な再帰的公理化可能理論が不完全である」ということを言う**ゲーデルの不完全性定理** (*Gödel incompleteness theorem*) は自明に導かれる.
4. 無限列 $\alpha \in \{0, 1\}^{\mathbb{N}}$ が **PA 次数** (*PA degree*) を持つとは、「ペアノ算術を含む無矛盾かつ完全な理論」を α から計算できることを指す (ペアノ算術を ZFC などの算術を表現できる別の理論に変えても、定義は同一になる). ゲーデルの不完全性定理より、PA 次数を持つ無限列は Δ_1^0 ではない.
5. $\alpha <_T \emptyset'$ を満たす PA 次数の無限列 $\alpha \in \{0, 1\}^{\mathbb{N}}$ が存在する. よって、 Δ_2^0 であるような PA 次数を持つ無限列が存在する.

6. $[0, 1]^{\mathbb{N}}$ 上の連続関数の不動点を見つける問題（ブラウワーの不動点定理）と、PA 次数を持つ無限列を見つける問題は、チューリング次数の意味で正確に等しい。この他にも、チューリング次数が PA 次数と本質的に同値な数学的命題は無数にある。

定義 7.7. この定義内で数集合と言った場合、 \mathbb{N} の部分集合を指すこととする。 $\varphi(\vec{p}, \vec{P})$ を自然数変数記号 $\{x, y, z, \dots\}$, 数集合変数記号 $\{X, Y, Z, \dots\}$, 自然数上の演算/関係/定数記号 $\{+, \times, \leq, =, 0, 1\}$, 要素関係を表す関係記号 $\{\in\}$, および述語論理記号 $\{\vee, \wedge, \neg, \rightarrow, \forall, \exists\}$ の有限個の組合せで構成される論理式で、有限個の自然数パラメータ \vec{p} および数集合パラメータ \vec{P} を持ち得るものとする。このような論理式を二階算術 (*second-order arithmetic*) の論理式と呼ぶ。このとき、

1. $\varphi(\vec{p}, \vec{P})$ が Σ_0^1 あるいは Π_0^1 とは、 φ に現れる量化記号が全て自然数変数に対するものであるとき、つまり、 $\forall x \in \mathbb{N} \exists y \in \mathbb{N}$ の形であるときを指す。 Σ_n^0, Π_n^0 等は以前と同様にして定義される。
2. $\varphi(\vec{p}, \vec{P})$ が Σ_{n+1}^1 であるとは、ある Π_n^1 論理式 $\psi(\vec{p}, \vec{P}, Q)$ について、 $(\exists X \subseteq \mathbb{N}) \psi(\vec{p}, \vec{P}, X)$ の形であるときを指す。
3. $\varphi(\vec{p}, \vec{P})$ が Π_{n+1}^1 であるとは、ある Σ_n^1 論理式 $\psi(\vec{p}, \vec{P}, Q)$ について、 $(\forall X \subseteq \mathbb{N}) \psi(\vec{p}, \vec{P}, X)$ の形であるときを指す。

与えられた無限列 $\alpha \in \{0, 1\}^{\mathbb{N}}$ に対して、 $\hat{\alpha} = \{n \in \mathbb{N} : \alpha(n) = 1\}$ と書く。 $\Gamma \in \{\Sigma_n^i, \Pi_n^i\}_{n \in \mathbb{N}}^{i < 2}$ とする。無限列 $\alpha \in \{0, 1\}^{\mathbb{N}}$ が Γ であるとは、自然数パラメータ n を持つ Γ 論理式 $\varphi(n)$ が存在して、 $\hat{\alpha} = \{n \in \mathbb{N} : \varphi(n)\}$ を満たすことである。また、無限列の集合 $S \subseteq \{0, 1\}^{\mathbb{N}}$ が Γ であるとは、数集合パラメータ A を持つ Γ 論理式 $\varphi(A)$ が存在して、 $S = \{\alpha \in \{0, 1\}^{\mathbb{N}} : \varphi(\hat{\alpha})\}$ を満たすことである。前と同様に、 Σ_n^i かつ Π_n^i であるとき、 Δ_n^i であると呼ばれる。

定理 7.4 (Kleene の定理 1955). 任意の無限列 $\alpha \in \{0, 1\}^{\mathbb{N}}$ について、以下の 3 条件は同値である。

1. ある順序数 $\xi < \omega_1^{CK}$ について、 $\alpha \leq_T \emptyset^{(\xi)}$ である。
2. ある順序数 $\xi < \omega_1^{CK}$ について、 α は Σ_ξ^0 である。
3. α は Δ_1^1 である。

定理 7.5 (Kleene 1952, 1955). $\{0, 1\}^{\mathbb{N}}$ の部分集合の階層について、以下の性質が成り立つ。

$$\begin{aligned} \tilde{\Delta}_1^0 &= \Delta_1^0; & \tilde{\Delta}_\xi^0 &= \bigcup_{\alpha \in \{0, 1\}^{\mathbb{N}}} \Delta_\xi^0(\alpha); \\ \tilde{\Sigma}_\xi^0 &= \bigcup_{\alpha \in \{0, 1\}^{\mathbb{N}}} \Sigma_\xi^0(\alpha); & \tilde{\Pi}_\xi^0 &= \bigcup_{\alpha \in \{0, 1\}^{\mathbb{N}}} \Pi_\xi^0(\alpha). \end{aligned}$$

さらに、ボレル集合は以下によって特徴付けられる。

$$\{A \subseteq \{0, 1\}^{\mathbb{N}} : A \text{ はボレル}\} = \tilde{\Delta}_1^1 = \bigcup_{\alpha \in \{0, 1\}^{\mathbb{N}}} \Delta_1^1(\alpha).$$

命題 7.7 (Kurtz 1981). $1 \leq \alpha < \omega_1^{CK}$ とする。 Σ_α^0 集合が与えられたとき、 $S \subseteq \{0, 1\}^{\mathbb{N}}$ の λ -測度は Σ_α^0 実

数である.

証明. n 上の帰納法によって示す. まず, $n = 1$ のとき, Σ_1^0 集合 $U \subseteq \{0, 1\}^{\mathbb{N}}$ を生成する Σ_1^0 反鎖 $W \subseteq \{0, 1\}^{<\mathbb{N}}$ を考える. このとき, $\lambda(U) = \lim_{t \rightarrow \infty} \sum_{\sigma \in W[t]} 2^{-|\sigma|}$ である. ここで, $\sum_{\sigma \in W[t]} 2^{-|\sigma|}$ は t で一様に計算可能かつ, t に関して単調増大であるから, $\lambda(U)$ は Σ_1^0 実数である.

いま, Σ_n^0 集合の λ -測度は, 与えられた Σ_n^0 集合の指数から一様に Σ_n^0 であると仮定する. $U \subseteq \{0, 1\}^{\mathbb{N}}$ を Σ_{n+1}^0 集合とする. このとき, Σ_n^0 集合の下降列 $\{V_k\}_{k \in \mathbb{N}}$ が存在して, $U = \{0, 1\}^{\mathbb{N}} \setminus \bigcap_k V_k$ となる. このとき, $\lambda(S) = 1 - \lim_{k \rightarrow \infty} \lambda(V_k)$ である. ここで, $s_k = 1 - \lambda(V_k)$ は Δ_{n+1}^0 実数であり, $\{s_k\}_{k \in \mathbb{N}}$ は単調増大列であるから, その極限である $\lambda(S)$ は Σ_{n+1}^0 実数である. \square

命題 7.8 (Kurtz 1981, Kautz 1991). $1 \leq \alpha < \omega_1^{CK}$ とする. このとき, 与えられた Σ_{n+1}^0 集合 $U \subseteq \{0, 1\}^{\mathbb{N}}$ と実数 $\varepsilon > 0$ に対して, $\Sigma_1^0(\emptyset^{(n)})$ 集合 $V \supseteq U$ で $\lambda(V) - \lambda(U) < \varepsilon$ なるものを構成できる.

7.2 ハウスドルフ階層と極限的学習

定義 7.8 (ハウスドルフの差の階層 (Hausdorff difference hierarchy)). $\theta, \xi > 0$ を任意の順序数とする.

1. Σ_{ξ}^0 集合 $A_0 \subseteq \{0, 1\}^{\mathbb{N}}$ を, $\{A_0\}$ を介して $(\Sigma_{\xi}^0)_1$ 集合であると呼ぶ.
2. $A \subseteq \{0, 1\}^{\mathbb{N}}$ が $\{A_{\eta}\}_{\eta < \theta+1}$ を介して $(\Sigma_{\xi}^0)_{\theta+1}$ 集合であるとは, $\{A_{\eta}\}_{\eta < \theta}$ は Σ_{ξ}^0 集合の上昇列であり, $\{A_{\eta}\}_{\eta < \theta}$ を介して $(\Sigma_{\xi}^0)_{\theta}$ 集合であるような $B \subseteq \{0, 1\}^{\mathbb{N}}$ が存在して, $A = A_{\theta} \setminus B$ となることである.
3. ξ が極限順序数のとき, $A \subseteq \{0, 1\}^{\mathbb{N}}$ が $\{A_{\eta}\}_{\eta < \theta}$ を介して $(\Sigma_{\xi}^0)_{\theta}$ 集合であるとは, $\{A_{\eta}\}_{\eta < \theta}$ は Σ_{ξ}^0 集合の上昇列であり, $A = \bigcup_{\eta < \theta} (A_{2\eta+1} \setminus A_{2\eta})$ となることである.

命題 7.9. $\bigcup_{n \in \mathbb{N}} (\Sigma_1^0)_n$ は, 開集合全体を含む最小の有限加法族である. より一般に, 任意の順序数 ξ について, $\bigcup_{n \in \mathbb{N}} (\Sigma_{\xi}^0)_n$ は, Σ_{ξ}^0 集合全体を含む最小の有限加法族である.

命題 7.10. 如何なる非可算な完備可分距離空間においても, 任意の順序数 $\theta, \xi \in [1, \omega_1)$ について, $(\Sigma_{\xi}^0)_{\theta}$ であるが, どんな $\eta < \theta$ についても $(\Sigma_{\xi}^0)_{\eta}$ でないような集合が存在する.

定理 7.6 (ハウスドルフ, クラトフスキ). 任意の順序数 $1 \leq \xi < \omega_1$ および任意の集合 $A \subseteq \{0, 1\}^{\mathbb{N}}$ に対して, 以下の 2 条件は同値である.

1. A は $\Delta_{\xi+1}^0$ 集合である.
2. ある $1 \leq \theta < \omega_1$ について, A は $(\Sigma_{\xi}^0)_{\theta}$ 集合である.

♠ 後で書くもののリスト:

- エルショフ階層 (Ershov hierarchy)
- ワッジ次数 (Wadge degree)
- ゴールドの極限同定 (identification in the limit) から機械学習の理論へ

7.3 不連続関数の階層と可測関数

定義 7.9. 関数 $F : \{0, 1\}^{\mathbb{N}} \rightarrow \{0, 1\}^{\mathbb{N}}$ が \mathcal{A} -可測 (\mathcal{A} -measurable) であるとは、任意の Σ_1^0 集合 U について、 $F^{-1}[U] \in \mathcal{A}$ となることである。 \mathcal{A} が λ -可測集合全体の族であるときは、単に F は可測 (measurable) であると言う。

例 7.5.

1. 関数が連続であることと Σ_1^0 -可測であることは同値である。
2. ヘヴィサイドの階段関数は Σ_1^0 -可測でないが、 Δ_2^0 -可測である。
3. ディリクレの関数 $\lim_{n \rightarrow \infty} \lim_{m \rightarrow \infty} (\cos n! \pi x)^{2m}$ は Σ_2^0 -可測でない。

上記の例の関数はいずれも可算的連続である、つまり、定義域の可算分割 $\{X_i\}_{i \in \mathbb{N}}$ が存在して、そこへの制限 $F \upharpoonright X_i$ は連続となる。

定義 7.10. $\Gamma, \Gamma^* \in \{\Sigma_n^i, \Pi_n^i, \Delta_n^i\}_{n \in \mathbb{N}, i < 2}$ とする。関数 $F : \{0, 1\}^{\mathbb{N}} \rightarrow \{0, 1\}^{\mathbb{N}}$ が実効 (Γ, Γ^*)-可測 (effectively Γ -measurable) であるとは、与えられた無限列 $\alpha \in \{0, 1\}^{\mathbb{N}}$ と $\Gamma(\alpha)$ 集合 U に対して、 $F^{-1}[U]$ が $\Gamma^*(\alpha)$ 集合であり、その $\Gamma^*(\alpha)$ 集合の指数を計算できることを指す。実効 (Σ_1^0, Γ)-可測関数を、単に実効 Γ -可測であるという。

例 7.6. Lusin は、可算的連続でないボレル可測関数が存在するか否かと尋ねた。そのような例として、チューリングジャンプ (Turing jump) は可算的連続でない Σ_2^0 -可測関数である。一方、Jayne/Rojas の定理 (1984) によれば、任意の Δ_2^0 -可測関数は可算的連続である。

例 7.7. ハイパージャンプ (hyperjump) は可測関数であるが、ボレル可測ではない。

定義 7.11 (ベール 1898). 連続関数列の各点極限であるような関数をベール第 1 類 (Baire class 1) と呼ぶ。各順序数 $1 < \xi < \omega_1$ に対して、関数 $f : \{0, 1\}^{\mathbb{N}} \rightarrow \{0, 1\}^{\mathbb{N}}$ が、 $\xi_n < \xi$ についてベール第 ξ_n 類関数 f_n たちの列 $\{f_n\}_{n \in \mathbb{N}}$ の各点極限であるとき、 f をベール第 ξ 類 (Baire class ξ) であると呼ぶ。

命題 7.11 (ルベーク 1905). 非可算な完備可分距離空間において、任意の順序数 $1 \leq \xi < \omega_1$ に対して、ベール第 ξ 類であるが、どんな $\zeta < \xi$ についてもベール第 ζ 類でないような関数が存在する。

定理 7.7 (ルベーク 1905; ハウスドルフ 1914). $1 \leq \xi < \omega_1$ とする。 $f : \{0, 1\}^{\mathbb{N}} \rightarrow \{0, 1\}^{\mathbb{N}}$ がベール第 ξ 類であることと $\Sigma_{\xi+1}^0$ -可測であることは同値である。

定義 7.12. 関数 $f : \{0, 1\}^{<\mathbb{N}} \rightarrow \{0, 1\}^{<\mathbb{N}}$ が \preceq -準同型 (\preceq -homomorphism) であるとは、任意の $\sigma, \tau \in \{0, 1\}^{<\mathbb{N}}$ に対して、もし $\sigma \preceq \tau$ ならば $f(\sigma) \preceq f(\tau)$ を満たすことを言う。部分関数 $F : \subseteq \{0, 1\}^{\mathbb{N}} \rightarrow \{0, 1\}^{\mathbb{N}}$ が計算可能 (computable) であるとは、ある計算可能 \preceq -準同型 $f : \{0, 1\}^{<\mathbb{N}} \rightarrow \{0, 1\}^{<\mathbb{N}}$ が存在して、以下の 2 条件を満たすことである。

1. $\xi \in \text{dom}(F) \iff \lim_{n \rightarrow \infty} |f(\xi \upharpoonright n)| = \infty$.
2. $\xi \in \text{dom}(F)$ ならば、 $F(\xi) = \lim_{n \rightarrow \infty} f(\xi \upharpoonright n)$.

命題 7.12. $\{0, 1\}^{\mathbb{N}}$ 上の計算可能関数は連続である。

定義 7.13. $\Phi(e)$ で自然数 $e \in \mathbb{N}$ によってコードされた $\{0, 1\}^{\mathbb{N}}$ 上の計算可能関数とする。部分関数 $F : \subseteq$

$\{0, 1\}^{\mathbb{N}} \rightarrow \{0, 1\}^{\mathbb{N}}$ が学習可能 (*learnable*) であるとは、次の条件を満たす計算可能関数 $\Psi : \{0, 1\}^{<\mathbb{N}} \rightarrow \mathbb{N}$ が存在することである.

$$(\forall \xi \in \text{dom}(F)) \quad F(\xi) = \Phi \langle \lim_{n \rightarrow \infty} \Psi(\xi \upharpoonright n) \rangle (\xi).$$

定理 7.8 (Pauly/de Brecht 2012). 関数 $F : \subseteq \{0, 1\}^{\mathbb{N}} \rightarrow \{0, 1\}^{\mathbb{N}}$ が実効 (Σ_2^0, Σ_2^0) 可測であることと学習可能であることは同値である.

証明. F は実効 (Σ_2^0, Σ_2^0) 可測なので、任意の $y \in \{0, 1\}^{\mathbb{N}}$ に対して、 $F^{-1}(\{y\})$ は $\Sigma_2^0(y)$ 集合である. さらに、 $F^{-1}(\{y\}) = \bigcup_n P_n^y$ なる Π_1^0 集合列の指数を y で一様に計算可能である. よって、 $x \in P_n^y$ を表す Σ_2^0 論理式 $\varphi(x, y, n)$ が存在する. いま、各 $x \in \text{dom}(F)$ に対して、 $(\exists n) \varphi(x, y, n)$ なる $y \in \{0, 1\}^{\mathbb{N}}$ は唯一である. これより、 $\Pi_1^0(x)$ 集合 $Q^x = \{n \frown y : \varphi(x, y, n)\}$ と各自然数 $n \in \mathbb{N}$ について、 $\#(Q^x \cap \llbracket n \rrbracket) \leq 1$ である. 学習者は、第 n 回目の推測で、 $\#(Q^x \cap \llbracket n \rrbracket) = 1$ と推測し、その孤立点を計算することを試みる. この手続きによって、 $F(x)$ の値は学習される. \square

定理 7.9 (Császár/Laczkovich 1975, 1979, 1990). ベール離散第一類関数は、 Π_1^0 -区分的連続である. ベール離散第 ξ 類関数は、 Π_ξ^0 -区分的連続である.

索引

- Δ_2^0 , 72
- Freq(α), 5
- K-トリビアル, 59
- \leq_T , 42, 71
- $\#i(\sigma)$, 28
- ω_1^{CK} , 72
- Σ_1^0 , 20, 59, 72
- 位相エントロピー, 65
- 依頼状, 16
- エルゴード的, 67
- エルショフ階層, 74
- 外測度, 62
- 可測関数, 74
- カラテオドリの拡張定理, 29
- 究極のランダム性, 27
- 強大数の法則, 5
- 強零, 62
- 極限計算可能, 72
- 計算可能, 20, 71
- 計算的枚挙可能, 20, 72
- コルモゴロフ複雑性, 16, 20, 65
- コレクティブ, 6
- 再帰的可算, 72
- サブシフト, 65
- 実効 (Γ, Γ^*) 可測関数, 75
- 実効強零, 63
- 実効ハウスドルフ次元, 35, 65
- 実効普遍零, 56
- 射影階層, 70
- シャノン・エントロピー, 37
- 接頭関数, 16
- 測度論的エントロピー, 67
- 単純マルチンゲール, 9
- チャーチ・クリネ順序数, 72
- チューリング還元可能, 42, 71
- チューリングジャンプ, 71
- 超算術的, 27
- 重複対数の法則, 6
- 停止確率, 57
- 停止問題, 57, 71
- 二階算術, 73
- ネバー・ランダム, 58
- ハウスドルフ外測度, 34
- ハウスドルフ次元, 35, 62, 65
- ハウスドルフの差の階層, 74
- 反鎖, 3, 16
- PA 次数, 72
- 普遍マルチンゲール, 48
- 普遍零, 56
- ベール第 1 類関数, 75
- ベルヌーイ測度, 5, 28
- 変分原理, 67
- 保測力学系, 66
- ボレル階層, 69
- ボレル集合, 69
- マーティンレフ・ランダム, 20, 30, 63
- マルチンゲール, 2, 22, 29
- マルチンゲール過程, 12, 13, 23
- 有限状態次元, 40
- ランダムネス抽出, 42
- 力学系, 64
- ワッジ次数, 74