ランダムの概念について

宮部賢志[*1]

2012 年 9 月 20 日

[*1] 京 都 大 学　数 理 解 析 研 究 所,　E-mail:　kmiyabe@kurims.kyoto-u.ac.jp,　URL: http://kenshi.miyabe.name/wordpress/

はじめに

本ノートは「数学基礎論サマースクール 2012」における筆者の講義の講義録である．

数学基礎論サマースクール[*1] は，日本数学会[*2] の「数学基礎論および歴史分科会」の補助を受け，毎年開催されるものである．2012 年は Turing 生誕 100 年にあたり，Turing year と呼ばれ，特にイギリスでは様々なイベントが開催された．数学基礎論サマースクール 2012 [*3] でもこれを記念し，基礎コースとして入門講座「計算可能性の理論」，発展コースとして「アルゴリズム的ランダムネスと数学」の講義が行われた．

筆者はその発展コースの一部を担当し，90 分の講義を 2 つ行った．1 つ目は「ランダムの概念はどう使えるか」というタイトルで，アルゴリズム的ランダムネスの理論と他の理論との関係について講義した．この内容は第 1 章にまとめられている．2 つ目は「ランダムの概念はどう発展してきたか」というタイトルの講演を行い，この内容は第 2 章にまとめられている．

本文では，計算可能性の理論とアルゴリズム的ランダムネスの理論の基礎的な知識を仮定している．数学基礎論サマースクール 2012 では，前者については基礎コースの講師であった鹿島亮先生が，後者については発展コースの他の講師であった樋口幸治郎氏および木原貴行氏[*4] が講演しているためである．アルゴリズム的ランダムネスの理論の教科書としては [19, 9] が挙げられる．

この場を借りて，数学基礎論サマースクール 2012 の幹事をされた只木孝太郎先生，鹿島亮先生，鈴木登志雄先生および共に発展コースの講師をつとめた樋口幸治郎氏，木原貴行氏に感謝の意を表したい．

[*1] http://mathsoc.jp/section/logic_and_history/SummerSchool.html

[*2] http://mathsoc.jp/

[*3] http://www2.odn.ne.jp/tadaki/LSS2012.html

[*4] http://researchmap.jp/kihara/

目次

第 1 章

ランダムの概念はどう使えるか

1.1　ランダムの使い方

1.1.1　ランダムは使えるか

ランダムと言えば，でたらめであり，不規則であり，扱いづらいものというイメージがあるらしい．更にそれに関連して，使えないものというイメージもあるらしい．ランダムな列は「わずかな列しか持たないような特殊な規則を持たない」が，「多くの点が持つ性質はランダムな点ならば必ず持つ」はずである．このことから，乱拓アルゴリズムなどに応用されることがある．このように実用的な意味でも，ランダムな点は「使える」点である．

このことをアルゴリズム的ランダムネスの言葉で書くとどうなるだろうか．以下では

ランダム＝うまく振る舞う (well-behaved) ＝収束

という形の定理をいくつか紹介することにする．ここでは，実用的な意味での「使える」ではなく，他の分野と関連を持ち，そして発展に貢献できるという意味で「使える」という言葉を使っていることをご了承願いたい．

1.1.2　大数の法則と重複対数の法則

「ランダムな点ならば必ず持つべき性質」は，確率論では極限定理として長らく研究されてきた．その代表例が大数の法則である．ここでは最も単純な場合を挙げる．

定理 1.1.1. *(Borel の大数の法則 1909 [3])* $\{X_n\}$ を $P(\{0\}) = P(\{1\}) = 1/2$ を満たす独立

同分布確率変数列とする．このとき，ほとんど確実に以下が成り立つ．

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

その収束の速さは重複対数の法則として，知られている．

定理 1.1.2. *(Khintchine* の重複対数の法則 *1924 [14])* $\{X_n\}$ を $P(\{0\}) = P(\{1\}) = 1/2$ を満たす独立同分布確率変数列とする．このとき，ほとんど確実に以下が成り立つ．

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

この定理に相当するものをアルゴリズム的ランダムネスの言葉で書くと以下のようになる．

定理 1.1.3 ([26, 18])**.** すべての *Martin-Löf* ランダムな列は大数の法則および重複対数の法則を満たす．

これらはランダムならば「うまく振る舞う」ことの例である．更に次のことも成り立つ．

定理 1.1.4. すべての *Schnorr* ランダムな列は大数の法則および重複対数の法則を満たす．*Kurtz* ランダムな列で大数の法則を満たさない列が存在する．

このことは同じ「多くの列について成り立つ」性質であってでも，その性質が成り立つことがどれくらい難しいかについて，ランダムの概念に応じて階層を作れることを意味している．

上記の例は，「ランダムならばうまく振る舞う」という一方向のみの成立であった．逆は成り立たない．つまり Martin-Löf ランダムではない列で大数の法則を満たす列が存在する．（例えば，$X = (01)^\omega$ など．）以下ではこの逆方向も成り立つ定理を取り上げる．

1.1.3　収束定理と計算可能ランダムネス

確率論において重要な収束定理の 1 つが以下である．

定理 1.1.5 (Doob の収束定理 (の系))**.** $\{X_n\}$ が非負マルチンゲールであるならば，$\lim_n X_n$ はほとんど確実に存在する．

この定理に対応するアルゴリズム的ランダムネスの定理として以下がよく知られている．

定理 1.1.6 (folklore)**.** 以下は同値．

1. $X \in 2^\omega$ が計算可能ランダム．

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

計算可能ランダムな点での収束は，Doob の収束定理の実効化と見ることができる．証明のアイディアも Doob の収束定理と基本的には同じである．逆は古典的な定理には対応するものが存在しない．

証明．2. $\Rightarrow$ 1. は自明である．

逆を示そう．$d : 2^* \to \mathbb{R}^+$ を計算可能マルチンゲール，$X \in 2^\omega$ を計算可能ランダムとする．$\lim_n d(X \upharpoonright n)$ が存在しないと仮定して，矛盾を示す．$\lim_n d(X \upharpoonright n)$ が存在しないので，ある有理数 $r < s$ に対して，無限に多くの n で $d(X \upharpoonright n) < r$ となり，かつ，無限に多くの n で $d(X \upharpoonright n) > s$ となる．

新しい計算可能マルチンゲール f を以下のように定義する．λ を空文字として，$f(\lambda) = 1$ とする．それぞれの列 $A \in 2^\omega$ に対して，次のように賭ける．最初は 0,1 に均等に賭ける．$d(A \upharpoonright n_0) < r$ となる n_0 が存在したらその後は，d の賭け方に従って賭ける．次に $d(A \upharpoonright n_1) > s$ となる n_1 が見つかったら, その後はまた均等に賭ける．その次に $d(A \upharpoonright n_2) < r$ となる n_2 があれば，また d の賭け方に従う．という賭け方を繰り返す．このように定義された f は計算可能マルチンゲールになる．

X と d に対する仮定より，$A = X$ に対して無限列 $n_0, n_1, \cdots$ が存在する．n_{2i} と n_{2i+1} の間で，資金を $\frac{s}{r}$ 倍にできる．一方，n_{2i+1} と n_{2i+2} の間では，資金が変化しない．よって，$\lim_n f(X \upharpoonright n) = \infty$ であり，これは X が計算可能ランダムであることに矛盾する． □

問題 **1.1.7.** この定理の変形版を考えてみよう．*c.e.* マルチンゲールにしたら *Martin-Löf* ランダムネスを特徴付けるだろうか？ *Schnorr* ランダムネス版はどうなるだろうか？

1.2 微分可能性とランダムネス

1.2.1 Demuth プログラム

確率論で知られている極限定理を Martin-Löf ランダムの列について示そうという試みを提案したのは O. Demuth であり，今日この流れの研究は Demuth プログラムと呼ばれている．代表的な成果が以下で見る Martin-Löf ランダムネスの微分可能性による特徴付けである．まず，古典的な定理を思い出しておこう．

定理 1.2.1 (Lebesgue 1904 [16])**.** 任意の単調増加関数 $f : [0, 1] \to \mathbb{R}$ はほとんど至る所微分

可能.

この定理は有界変動関数に自然に拡張される.

定義 1.2.2. 関数 $f : [0,1] \to \mathbb{R}$ が 有界変動*(bounded variation)* であるとは,

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

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

有界変動関数は 2 つの単調増加関数なので，任意の有界変動関数はほとんど至る所微分可能であることが導かれる．この実効化として，計算可能な関数に限ると Martin-Löf ランダムネスを特徴付ける.

定理 1.2.3 (Demuth [8])**.** 実数 $x \in [0,1]$ について以下は同値.

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

Nies はこの定理の他のランダムネス版を考えることを提案し，以下の様な結果を得ている.

定理 1.2.4 (Brattka, Miller and Nies [5])**.** 実数 $x \in [0,1]$ について以下は同値.

1. x は計算可能ランダムである.
2. すべての単調な計算可能関数 $f : [0,1] \to \mathbb{R}$ に対して，f が x で微分可能.
3. すべての *Lipschitz* 連続な計算可能関数 $f : [0,1] \to \mathbb{R}$ に対して，f が x で微分可能.

定理 1.2.5 (Brattka et al. [5])**.** 実数 $x \in [0,1]$ について以下は同値.

1. x は弱 *2* ランダムである.
2. すべての至る所微分可能な計算可能関数 $f : [0,1] \to \mathbb{R}$ に対して，f が x で微分可能.

この方向の研究として，これまでに様々な結果が知られている.

1.2.2　微分定理と Schnorr ランダムネス

微分可能性ではなく，微分定理の実効化の研究も行われている.

定理 1.2.6 (Lebesgue 1910 [17])**.** $f : [0,1] \to \mathbb{R}$ を L^1 関数とすると，ほとんど至る所の点 x

で

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

ここで，$B(x,h) = (x-h, x+h)$.

この定理の実効化として，Pathak ら（独立に Rute) は以下の結果を得ている.

定理 1.2.7 (Pathak, Rojas and Simpson [20], Rute)**.** 実数 $x \in [0,1]$ について以下は同値.

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

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

ここではこの定理の弱い形である主張を証明しよう.

命題 1.2.8. 列 $A \in 2^\omega$ について以下は同値.

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

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

この証明を与えるために，少し準備をする.

定義 1.2.9. 一様に *c.e.* 開集合の列 $\{U_n\}$ が

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

を満たすとき，$\{U_n\}$ を *Solovay* テスト と呼ぶ.

定理 1.2.10. A が *Martin-Löf* ランダムであることと，すべての *Solovay* テスト $\{U_n\}$ に対して，$A \in U_n$ となる n は高々有限個であることは同値.

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

逆を示す．ある列 A とある Solovay テスト $\{U_n\}$ があって，無限個の n で $A \in U_n$ であると仮定する．$\sum_n \mu(U_n) \leq 1$ を仮定して良い.

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

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

定義 1.2.11. $\{U_n\}$ が一様に *c.e.* 開集合の列で，$\sum_n \mu(U_n)$ が計算可能な実数であるとき，$\{U_n\}$ を *Schnorr Solovay* テスト と呼ぶ.

定理 1.2.12. A が *Schnorr* ランダムであることと，すべての *Schnorr Solovay* テスト $\{U_n\}$ に対して，$A \in U_n$ となる n は高々有限個であることは同値.

証明は Solovay テストの場合と同様である.

命題 *1.2.8* の証明. (i)⇒(ii) A を Schnorr ランダム，M を計算可能マルチンゲールとし，

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

を満たす計算可能な列 $\{n_k\}$ が存在したとする．Ville の不等式より，

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

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

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

が一様に計算可能になる．U_k は一様に c.e. の開集合であり，

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

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

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

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

(ii)⇒(i) A は Schnorr ランダムではないとしよう．つまりある Schnorr Solovay テスト $\{[\sigma_n]\}$ に対し，無限に多くの n で $A \in [\sigma_n]$.

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

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

で定義する．ここで

$$M = \sum_n B_{\sigma_n}$$

とすると，M は計算可能なマルチンゲールになる．

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

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

は計算可能であるから，ある計算可能な列 $\{m_k\}$ が存在して，

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

となる．さらに

$$n_k = \max\{|\sigma_n| \ : \ n \leq m_k\}$$

とおく．

$$M_k = \sum_{n \leq m_k} B_{\sigma_n}$$

とおくと，

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

ここで $n' \in \{n_k, n_{k+1}\}$ に対して，

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

であるから，上記の不等式は成立する． □

1.3　力学系とランダムネス

1.3.1　Poincaré の回帰定理

ランダムネスの理論の応用として最近特に盛んに研究されているのが力学系である．力学系の分野では数値シミュレーションが盛んに行われており，計算した値が正しい値に収束しているかは大きな問題であった．ランダムネスの理論はそれに対し数学的に厳密な道具立てを提供する．

最初に取り上げるのは，Poincaré の回帰定理である．この定理は「適当な条件の満たされた力学系は，その初期状態の任意の近傍に無限回もどってくる」などと表現される．

定理 1.3.1 (Poincaré 1890)**.** (X,μ) を確率空間とし，$T : X \to X$ をエルゴード的関数とする．すべての正の測度を持つ $E \subseteq X$ に対して，ほとんど至る所の点 x で，無限に多くの n で $T^n(x) \in E$ となる．

後の定理のために，用語を用意しよう．

定義 1.3.2. (X,μ) を確率空間とし，$T : X \to X$ を関数とする．$\mathcal{C}$ を X 上の可測集合族とする．点 $x \in X$ が $\mathcal{C}$ に関する T の *Poincaré* 点であるとは，すべての正の測度を持つ $E \in \mathcal{C}$ に対して，無限に多くの n で $T^n(x) \in E$ となることを言う．

この時，Poincaré 点により Martin-Löf ランダムネスを特徴づけることができる．

定理 1.3.3 (Kućera [15])**.** 列 A が *Martin-Löf* ランダムであることと，A が *co-c.e.* 閉集合に関するシフト演算子 S の *Poincaré* 点であることは同値である．

補題 1.3.4. *c.e. prefix-free* 集合 T と非負の整数 k に対し，*c.e. prefix-free* 集合 T^k を

$$T^k = \{\sigma_1\sigma_2\cdots\sigma_k \ : \ \sigma_i \in T\}$$

で定義する．この時,

$$\mu([\![T^k]\!]) = (\mu([\![T]\!]))^k.$$

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

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

かつ，すべての $n \geq 1$ に対して，

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

よって A は Poincaré 点ではない．

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

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

であることを示そう．T を c.e. prefix-free 集合で

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

となるものとする．この時，ある k が存在して，

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

である．よって，

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

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

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

すなわち，無限に多くの n について，

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

□

この定理から次の不思議な結果が得られる．Martin-Löf ランダムネスは万能 Martin-Löf テストの第一項 U_1 のみで特徴づけられる．

系 1.3.5. *A が Martin-Löf ランダムでないことと，A の尾 $S^n(A)$ すべてが U_1 に入ることは同値.*

1.3.2 Birkhoff のエルゴード定理

Poincaré の回帰定理よりも強い結果として，Birkhoff のエルゴード定理が知られている．

定理 1.3.6 (Birkhoff のエルゴード定理)**.** (X, μ) を確率空間とし，$T : X \to X$ をエルゴード的な関数とする．f を L^1 関数とすると，ほとんど至る所の点 x で，

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

定義 1.3.7. ある点が集合族 $\mathcal{C}$ に関する T の *Birkhoff* 点 であるとは，すべての $E \in \mathcal{C}$ に対して，

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

Birkhoff 点ならば Poincaré 点である．以下のような Birkhoff 点によるランダムの概念の特徴付けが知られている．

定理 1.3.8 (Gács, Hoyrup and Rojas [11])**.** T を計算可能なエルゴード的関数とする．x が *Schnorr* ランダムであることと，x が計算可能な測度を持つ Π^1_0 集合族に対する，T の *Birkhoff* 点であることが同値．

定理 1.3.9 (Bienvenu, Day, Hoyrup, Mezhirov and Shen [2], Franklin, Greenberg, Miller, and Ng [10])**.** T を計算可能なエルゴード的関数とする．x が *Martin-Löf* であることと，x が Π^1_0 集合族に対する，T の *Birkhoff* 点であることが同値．

1.4　正規数と計算可能な点での収束

これまで見てきたように，収束とランダムは深い関係がある．収束する点はある意味でランダムな点であるが，万能テストが存在しないランダムネスの場合，計算可能で収束する（すなわちランダムに見える）点を明示的に構成できる．

例 1.4.1. 大数の法則を満たす計算可能な列が存在する．例えば，

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

しかしこの列では 01 の文字列が多く出てくる反面，00 や 11 の文字列は全く出てこない．そこですべての文字列がしかるべき頻度で出てくる文字列を考えよう．

定義 1.4.2 (Borel 1909 [3])**.** 実数 $x \in b^\omega$ と基数 b に対し，$S(x, b, w, k)$ で $x \upharpoonright k$ に $w \in b^*$ が現れる回数を表す，すなわち，

$$S(x, b, w, k) = \#\{i \ : \ 1 \le i \le k - |w| + 1 \text{ かつ } x_{i:i+|w|-1} = w\}.$$

すべての w に対し，

$$\lim_{k\to\infty} \frac{S(x,b,w,k)}{k} = b^{-|w|}$$

であるとき，x は b 進正規数 であるという．任意の $b \geq 2$ について b 進正規であるとき，x を単に 正規数 と呼ぶ．

Borel が示したことは以下のことであった．

定理 1.4.3 (Borel 1909 [3])**.** ほとんどすべての実数は正規数．

よく知られている Borel の大数の法則はこの定理の系として導かれる．その証明は測度論的であり，Borel は正規数の具体例を与えるという問題を提示した．これに関連して以下の様な例が知られている．例えば，Champernowne 定数は，10 進少数表示において自然数が順に連なっている実数である，すなわち，

$$0.12345678910111213141516171819 20\cdots$$

これは 10 進正規数であることが知られている [6] が，他の基数に関しては正規か否かは分かっていない．また，Copeland-Erdös 定数は，10 進少数表示において素数が順に連なっている実数である，すなわち，

$$0.2357111317192329313741 43\cdots$$

これも 10 進正規数であることが知られている [7]．人工的に作られたものではない数たちの正規数についてはよく分かっていない．例えば，

$$\sqrt{2},\ \pi,\ e,\ \log 2$$

などの数が正規数であるかどうかは知られていない．

一方で，Turing は以下の結果を示している．測度論的な議論では導かれないことに注意しよう．

定理 1.4.4 (Turing [25][*1])**.** 計算可能な正規数は存在する．

その証明をランダムネスの言葉で書き直すと以下のことも分かる．

定理 1.4.5 ([1] 参照)**.** *Schnorr* ランダムネスならば正規数である．

[*1] 実際に出版されたのは 1992 年だが 1938 年ごろに書かれたと考えられている

更に強い結果として，以下の結果が知られている．b 種類の入力において，任意の有限オートマトンによるマルチンゲールで，資金が有限にとどまる列を $\underline{b\text{-有限状態ランダム}}$ であるという．

定理 1.4.6 (Schnorr and Stimm [21], Bourke, Hitchcock and Vinodchandran [4])**.** b 進正規数であることと，b-有限状態ランダムであることとは同値．

有限状態オートマトンを多項式時間で模倣することにより，以下の系が得られる．

系 1.4.7. 多項式時間で計算可能な正規数が存在する．

この系の背景にある基本的な考え方を紹介しておこう．

定理 1.4.8. 任意の計算可能マルチンゲールに対し，計算可能でそのマルチンゲールで発散しない列が存在する．

定理 1.4.9. 任意の *Schnorr* テストに対し，計算可能でそのテストに合格する列が存在する．

証明. $\{U_n\}$ を Schnorr テストとする．U_1 は c.e. 開集合で $\mu(U_1) = 1/2$ を満たすとして良い．$A \notin U_1$ となる計算可能な列 $A = \bigcup_n \sigma_n$ を以下のように構成する．

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

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

を満たすから，満たす i に対して，$\sigma_1 = i$ とする．

今，σ_n まで定まっていて，

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

を満たしているとしよう．この時，$i \in \{0, 1\}$ に対し $\mu(U_1 \cap [\sigma_n i])$ を計算することで，

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

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

もし，$A \in U_1$ ならば，ある n に対して，

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

であるから，

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

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

注意 **1.4.10.** *Martin-Löf* ランダムネスではそのような列は構成できない．

また，Hoyrup らにより「Birkhoff のエルゴード定理の性質を満たすような計算可能な点が存在する」ことも示されているが，上記と同じ考え方で得られた定理である．

第 2 章

ランダムの概念はどう発展してきたか

前半では，「ランダムであるとは，ほとんど至るところ成り立つ性質を持つ点」という見方をした．これは言うまでもなく，ランダムを典型的な点として見ている．しかしこのような「確率的プロセスの実現系列」いわゆる「サンプルパス」としての使い方は，アルゴリズム的ランダムネスの発展の歴史からすれば，技術的応用にすぎない．後半では，先人たちがランダム，確率，予測などの概念をどのように捉えていたかを紹介した後，ランダムネスの正当な使われ方として，アルゴリズム的確率，Vitányi による分類への応用の 2 つを紹介する．

2.1　ランダムおよび確率の歴史

2.1.1　理論の目的は何か

科学理論，ここでは特に数学で記述される理論の目的は何であろうか．この問題は科学哲学でよく論じられ，現象の記述，説明，予測などいくつかの提案がなされている．特にランダムに見える現象をどう定式化するという問題において，大きな問題になる．

例えば，科学の目的の 1 つを予測することだとすれば，科学は万人が従うべき正しい予測を与えていると，期待する人があるかもしれない．繰り返し同じ実験ができるような場合は，予測が正しかったかどうかある程度判定できる．そうでない場合は，どのようにして予測が正しかったかどうか判定できるのだろうか？事故が起こる確率が 1% であると予測して，事故が起こった場合，その予測は間違っていたのだろうか？どのような場合なら，正しい予測はできるのか，科学の範囲は何か？

ここでは，先人たちが「自らの理論の正当化のために，ランダムの概念をどう定義したか」を見ていく．

2.1.2　古代の偶然論

最初に取り上げるのは Aristotle である．Aristotle (B.C. 384-322) は偶然に関して確固とした考えを持っていたようである．Aristotle によれば，自己偶発的な現象にも原因が存在し，それを”Tyche” または”automaton” などと呼んでいる．そして，科学の中での偶然性の研究を否定する．

> 偶然的なものは科学的に取り扱えないとみなさなければならない．『形而上学』

ここでは，科学が取り扱える範囲を規定している．非常に分かりやすい議論である．

神学者もまた偶然に関して確固とした考えを持っている人々であった．それは Augustine (354-430) の次の言葉に象徴される．

> その原因は至るところにある神の手により操作されるもので，その意味で無作為な (random) ものは何もないし，遇運 (chance) なるものは存在しない．『八十三の問題について』

> すべては神の摂理に従う．『神の国』

Atistotle と Augustine では，偶然に対する態度は全く異なるが，この 2 つが，17 世紀まで確率計算の発生を抑止した原因を作った（『確率論の黎明』（安藤洋美）参照）と言われる．

2.1.3　古典確率の成立まで

上記のような考え方は現実的には問題を引き起こす．例えば，裁判などで確信の度合いという考え方が必要になる．これに対し，Thomas Aquinas (1225-1274) の態度は以下のようなものであった．

> 聖なる教え（神学）は，哲学者たちが自然理性により真理を知り得た場合には，彼らの権威をも用いる・・・しかし，聖なる教えはかかる権威をいわば教えの外の蓋然的論拠（Argumenta probabilia）として用いるにすぎない．『神学大全』

ここでは科学の有用性を認めながらも，「用いるにすぎない」ため，正当化する必要がない．しかし，この変化は確率概念の成立に向けた一歩であったように思われる．

しばらくして，有名な Pascal と Fermat の往復書簡（1654）が行われる．その中で「掛金をどう配分するのが適当か」という問題が取り上げられる．ここでは probability という言葉は出てこない．最初に Pascal が「公平な賭け」を基盤に問題を解いた．すなわち「ランダムであるとは予測不可能であることだ」と考えて，自らの回答に正当性を与えたのである．一方，Fermat は「組み合わせ」を基盤に問題を解いている．ここでは「ランダムであるとは多くの場合が平等に表れることだ」と考えている．Fermat の方法のほうが数学的に明らかに簡単であり，Pascal もその有効性を認めた．

このやりとりをおそらくは聞いていた Arnauld（1612-1694）により確率概念が作られる．

> 10 人の人が各人 1 クラウン賭けるゲームがあり，彼らのうちの 1 人だけが買って全部をせしめ，他の人々が皆失うとしよう．（中略）彼が 1 クラウン失い，9 クラウンを得ないのは，各々の場合 9 倍も確からしい．“The Port Royal Logic”

Fermat と Pascal の問題では，掛金の配分というルールの問題であったのに対し，Arnauld の表現では，それを予測の正当化に用いている．これは 1 つの考え方である．実際，Arnauld は蓋然性の根拠に，external evidence と internal evidence の区別を行なっている．これが，epistemic probability と aleatory probability の区別につながり，現在の主観確率と客観確率の区別につながっていると言われる．

しかし，大勢としてはこのような区別は無視される．その原因の 1 つには Bernoulli による大数の弱法則から，確率と頻度が同一視されるようになったことが挙げられる．Bernoulli 自身は主観確率を支持していただけに皮肉な結果であった．詳細は，Shafer [22], Hacking [12] などを参照して欲しい．

このような背景のもと，Laplace (1749-1827) により古典確率が完成する．

> 一定数の同等に可能な場合，すなわしそれらが存在するかどうかについてわれわれが決めかねる程度が同じである場合に帰着させ・・・『確率の哲学的試論』

Laplace 自身は決定論者であり，「確率は我々の無知に起因する」と考え，確率の計算は，「同等に可能な場合」を基盤に行えるとした．これは大きな一歩であったが，「同等に可能な場合」とは一体何を意味するのかは不明確のままであり，「ランダムの概念」がこの言葉に隠されていることに注意しよう．

2.2　von Mises と Kolmogorov による確率論

「同等に可能な場合」が見つけられない場合には，どう確率を定義したら良いだろうか？ 19 世紀末には物理において確率の取り扱いに困難が生じていた．Hilbert (1862-1943) の有名な 1900 年の国際数学者会議における「23 の問題」の中で，次のような問題を提出した．

第 6 問題「物理学は公理化できるか」

確率の厳密な取り扱いとして，幾何学のような公理化を求めたのであった．これに対して候補として挙げられた 2 つの理論が，von Mises による確率論と Kolmogorov による公理主義的確率論であった．

2.2.1　公理主義的確率論

Kolmogorov (1903-1987) は，『確率論の基礎概念』(1933) により今でも一般的に使われている「公理主義的確率論」を提唱した．では，公理化されている確率とは一体何か．Kolmogorov 自身の説明を，Kolmogorov 自身が頻度論者であることに注意しながら聞いてみよう．

確率論は，経験的な現実世界に以下のように適用される．

1. 何回でも繰り返すことができる，何らかの試行があるとする．
2. 試行が実現した結果として起こりうる事象の，ある定まった集まりを考える．この集まりの事象には，個々の実現では起こるものもあれば，起こらないものもある．起こるものも起こらないものも含めた，考えられる全ての事象の集合を Ω とする．
3. 試行の結果として現実に起こった事象が，ある集合 A に含まれるならば，そのとき事象 A が起こったという．
4. ある条件のもと，試行の実現の後に，起こることも起こらないこともありうる事象 A に対して，次の性質をもつ実数 $P(A)$ を定めることができる．

原理 A　試行が非常に多くの回数 (n 回) 繰り返されたとして，その結果事象 A の起こった回数が m 回であるとき，m と n の比 $\frac{m}{n}$ がほぼ $P(A)$ に等しいと事実上確信できる．

原理 B　$P(A)$ が非常に小さい場合には，試行が 1 回だけ実現したときには事象 A は起こらないと事実上確信できる．

『確率論の基礎概念』 (Kolmogorov)

この見方は Popper により傾向説へと移行させられる.

> しかしこれは，わたしたちがその条件について，確率に等しい頻度を持つ連続性を生み出す傾向性，性質，傾向を備えたものとして，具体化しなければならないことを意味する．そしてそれはまさに，傾向説の主張である．(Popper 1959)

この文脈において「ランダムである」とは,「事実上確信できる事象」であり,「確率 1 で起こる事象」に他ならない．しかし，この「事実上確信できる」とはいかなる意味であるのか．ここに数学と物理の違いがあるという考え方もある.

> 物理的に不可能な現象とは，その確率が無限に小さいもののことである．(Cournot の架け橋)

「ランダム」のこのような見方は 1 つの見方であるが，まだ曖昧さが残る.

Kolmogorov は 1933 年の時点から 1960 年代まで,「確率論の現実への応用」のためには, von Mises の理論のようなものが必要だと考えており，これがアルゴリズム的ランダムネスの成立につながるのである.

> 既に述べてきたように，数学的確率論の結果を現実の「ランダムな現象」に応用するには，何らかの形で確率の頻度論が必要であろう．そしてその避けられない部分はすでに von Mises の精力的な努力により確立されている．(Kolmogorov 1963; 筆者訳)

2.2.2 von Mises の確率論

von Mises の確率論において特筆すべきことは，（その数学的複雑さではなく,）自らの理論の範囲，そして科学の範囲について明確に表明していることであろう.

- 我々の確率論は「ドイツが未来にリベリアと戦争する確率はあるか？」というような問題とは何の関係もない.
- 物理の言葉を使うなら，確率論を適用するためには，実際上無限に長い一様な観察がなければならないと言えるだろう.
- 他のすべての自然科学のように，確率論は観察から始まり，それらを並べ，分類し，そこからある基本的な概念や法則を導き，最後に，一般的な普遍的に適用可能な論理を使って，実験結果と比較することで検定可能な結論を導くのである．すな

わち，我々の見方では，確率論は普通の科学であり，テーマとして際立ってはいるが，推論の方法として特別なわけではない．

- ある数学者が「君は私が次の列車に乗り遅れる確率を計算できるか？」と言ってからかうならば，解答を丁重に断らなければならない．それはちょうど「君はあの 2 つの山の頂上の距離を計算できるか？」と彼が聞かれたら，彼は断るように．つまり，もし適当な距離と角度が分かってさえいれば，距離は計算できる．同じように確率が分かるのは，依存する確率が分かっている時だけである．
- 「確率」という言葉は，ランダムの条件を満たす真の collective の極限頻度という意味だけで使う．

(“Probability, Statistics and Truth” by R. von Mises; 筆者訳)

von Mises の考え方は，次の言葉に要約される．

まず Collective ありき，そして確率がある．
(“Probability, Statistics and Truth” by R. von Mises; 筆者訳)

von Mises の理論では，ランダムの概念は，確率が定義できるための条件として使われている．

Kolmogorov による公理的確率論も，von Mises による確率論も，いずれも（いわゆる）独立同分布が想定されている．この場合には，確率も頻度も予測も，大きくは違わない．しかし，独立同分布が想定できない場合はどうであろうか？このような問題意識の元でアルゴリズム的情報理論の基礎が作られて行くのである．

2.3　ランダムネスの応用

2.3.1　アルゴリズム的確率

単純のために，2 進有限列が与えられたときに，次の文字を予測することを考える．十分長い列ならば，じっとその文字列を眺めると，いくつかの規則が見つかるだろう．その規則を「理論」と呼ぼう．互いに矛盾する理論もあるかもしれないし，互いに整合的な理論もあるかもしれない．この時，どのように予測を作ったら良いだろうか？

1 つの考え方は次の言葉に表現される．

もしいくつかの理論がデータと整合的であれば，それらすべてを保持せよ．
(Epicurus, B.C. 341?-)

しかし，同時に次のような考え方もよく使われる．

> 観察されたデータに整合的な最も単純な理論を保持せよ．
> (William of Ockham, 1288-1348)

この互いに矛盾する 2 つの考え方を組み合わせることを考える．

> 単純な規則には多くの，複雑な規則には少ない，金額を賭けた賭け戦略は良い戦略に違いない．

定義 2.3.1 (Solomonoff 1964)**.** 関数 $M : 2^\omega \to \mathbb{R}^+$ を以下で定義する．

$$M(\sigma) = \sum_{p:\sigma \preceq U(p)} 2^{-|p|}.$$

ここで U は万能マシンである．

この戦略はある意味で最善である．その意味を正確に述べよう．

定義 2.3.2. 関数 $M : 2^* \to \mathbb{R}^+$ が，$M(\epsilon) \leq 1$,

$$M(\sigma) \geq M(\sigma 0) + M(\sigma 1)$$

を満たす時，M を 半測度 と呼ぶ．*c.e.* 半測度 M が以下を満たす時，最善 *(optimal)* であると言う．任意の *c.e.* 半測度 N に対して，ある定数 C が存在し，すべての σ で,

$$C \cdot M(\sigma) \geq N(\sigma).$$

命題 2.3.3. 上記で定義された関数 M は，最善の *c.e.* 半測度である．

異なる最善の c.e. 半測度の作り方も存在する．

命題 2.3.4. $\{\mu_n\}$ をすべての *c.e.* 半測度の計算可能な数え上げとする．関数 M を

$$M = \sum_n 2^{-n} \mu_n$$

で定義すると，M は最善の *c.e.* 半測度となる．

c.e. 半測度の概念が，c.e. 優マルチンゲールと本質的に同じことに注意しておこう．すなわち，M を半測度とすると，

$$d(\sigma) = 2^{|\sigma|} M(\sigma)$$

とおけば，d は c.e. 優マルチンゲールであり，c.e. 優マルチンゲール d に対して，

$$M(\sigma) = 2^{-|\sigma|} d(\sigma)$$

とすれば，M は c.e. 半測度である．このことから，Martin-Löf ランダムネスは c.e. 半測度によっても特徴付けられる．

定理 2.3.5 (Levy 1973)**.** μ を 2^ω 上の計算可能測度，M を任意の最善の *c.e.* 半測度とする．ある列 $x_{1:\infty}$ が *μ-Martin-Löf* ランダムであることと，ある定数 c が存在してすべての n で $M(x_{1:n}) \leq c \cdot \mu(x_{1:n})$ となることは同値.

さて，最善の c.e. 半測度によれば，$x_{<n}$ までの文字列が与えられたときには，次に $i \in \{0,1\}$ が出る方に，

$$\frac{M(x_{<n}i)}{M(x_{<n})} =: M(x_{<n}i|x_{<n})$$

の割合で所持金を賭けるべきだということになる．一方で，列 $x_{1:\infty}$ が確率 μ によって「確率的に」振る舞うのであれば，$x_{<n}$ までの文字列が与えられたときには，次に $i \in \{0,1\}$ が出る方に，

$$\frac{\mu(x_{<n}i)}{\mu(x_{<n})} =: \mu(x_{<n}i|x_{<n})$$

の割合で所持金を賭けるべきだということになる．この 2 つの値は次の意味で近い．

定理 2.3.6 (Solomonoff [24])**.** M を最善の *c.e.* 半測度とすると，任意の計算可能な測度 μ に対して，μ についてほとんど確実に，

$$M(x_{1:n}|x_{<n}) - \mu(x_{1:n}|x_{<n}) \to 0.$$

ここで任意の μ についてこの式が成り立つことに注意しよう．すなわち μ が予め分からなかったとしても，最善の c.e. 半測度 M は μ を正しく予測できるのである．このことから Solomonoff は $M(x_n|x_{<n})$ を「確率」と呼ぶことを提唱するのである．ここで μ が計算可能でさえあれば，独立同分布でなくても成り立つことに注意しよう．しかし，残念ながら $M(x_n|x_{<n})$ は計算可能ではない．このことはアルゴリズム的確率の理論の最も大きな欠点と見られている．

この定理の証明を行う．

証明. Hellinger 距離を以下で定義する．

$$h_\sigma = \sum_{i\in\{0,1\}} \left(\sqrt{M(\sigma i|\sigma)} - \sqrt{\mu(\sigma i|\sigma)}\right)^2.$$

すると，

$$h_\sigma \leq 2 - 2 \sum_{i \in \{0,1\}} \sqrt{M(\sigma i|\sigma)\mu(\sigma i|\sigma)}$$

であるから，

$$N_\sigma = \sum_{i \in \{0,1\}} \sqrt{M(\sigma i|\sigma)\mu(\sigma i|\sigma)}$$

とおけば，

$$N_\sigma \leq 1 - \frac{h_\sigma}{2} \leq \exp\left(-\frac{h_\sigma}{2}\right).$$

ここで関数 $d : 2^* \to \mathbb{R}^+$ を以下で定義する．

$$d(\sigma) = \sqrt{\frac{M(\sigma)}{\mu(\sigma)}} \cdot \exp\left(\sum_{i=1}^{|\sigma|-1} h_{\sigma_{1:i}}\right).$$

ここで，M は最善であるから，$M(\sigma)/\mu(\sigma) > c > 0$ と仮定して良い．すると，

$$\begin{aligned}
\sum_{i \in \{0,1\}} \mu(\sigma i) d(\sigma i) &= \sum_{i \in \{0,1\}} \sqrt{M(\sigma i)\mu(\sigma i)} \cdot \exp\left(\sum_{i=1}^{|\sigma|} h_i\right) \\
&= \sum_{i \in \{0,1\}} \sqrt{M(\sigma i|\sigma)\mu(\sigma i|\sigma)} \cdot \exp\left(h_\sigma\right) \times \sqrt{M(\sigma)\mu(\sigma)} \cdot \exp\left(\sum_{i=1}^{|\sigma|-1} h_{\sigma_{1:i}}\right) \\
&\leq \sqrt{M(\sigma)\mu(\sigma)} \cdot \exp\left(\sum_{i=1}^{|\sigma|} h_{\sigma_{1:i}}\right) \\
&= \mu(\sigma) d(\sigma).
\end{aligned}$$

よって，d は μ-優マルチンゲール．つまり，μ に関してほとんど確実に，

$$\limsup_n d(x_{1:n}) < \infty.$$

これより，

$$\sum_{i=1}^{\infty} h_{x_{1:n}} < \infty.$$

よって，

$$M(x_{1:n}|x_{<n}) - \mu(x_{1:n}|x_{<n}) \to 0.$$

□

さて，上記の定理において「ほとんど確実に」を「μ-Martin-Löf ランダムな列に対して」で，置き換えることができるか，という問題は自然に思いつくであろう．この問題は最近否定的に解決された．

命題 2.3.7 (Hutter and Muchnik [13])**.** ある計算可能な測度 μ とある最善の予測 M およびある μ*-Martin-Löf* ランダムな列に対して，

$$M(x_n|X_{<n}) - \mu(x_n|x_{<n}) \not\to 1.$$

更に μ として一様測度を取ることができる．

アルゴリズム的確率の理論では「ランダムの概念」が「これ以上規則が見つけられない」という予測の最善性を保証するものとして使われている．アルゴリズム的確率の理論はランダムの概念の正当な使われ方として注目すべきものであるが，数学的な問題が多く存在している．

最後に Solomonoff [23] が亡くなる直前に書いた以下の言葉を紹介しよう．

> For quite some time I felt that the dependence of ALP (Alogrithmic Probability) on the reference machine (universal machine) was a serious flaw in the concept, and I tried to find some "objective" universal device, free from the arbitrariness of choosing a particular universal machine. When I though I finally found a device of this sort, I realized that I really didn't want it - that I had no use for it at all!

この見方の変更によってアルゴリズム的確率の理論は数学的にどう修正すべきなのか，今後の研究が待たれるところである．

2.3.2　分類

新しい規則が見つかると予測は変わるだろう．同じように新しい規則が見つかると似ているという概念も変わる．このような「ランダムの概念」は分類にも応用される．

通常，分類は分類するものの固有の性質に着目して分類される．遺伝子による動物種の分類，本の分類，音楽の分類，Linux 上の実行ファイルの分類などは基本的にそれぞれ違う分類の仕方で分類されるだろう．しかしどれも「文字列」と見ることで，統一的な単純な分類方法を与えることができないだろうか．

2 つの文字列の類似度を定義しよう．x^* で x を出力するプログラムの中で最小のもの (の 1 つ) を表す．

定義 2.3.8. y の x に含まれる 情報量 を

$$I(x:y) = K(y) - K(y|x^*)$$

で定義する.

命題 2.3.9. 定数を除いて，以下が成り立つ.

1. $I(x:y) \geq 0$.
2. $I(x:x) = K(x)$.

y の x に含まれる情報量は，x の y に含まれる情報量と同じであろうか？

定理 2.3.10. 定数を除いて，以下が成り立つ.

$$K(x,y) = K(x) + K(y|x^*).$$

系 2.3.11. 定数を除いて，以下が成り立つ.

$$I(x:y) = K(y) - K(y|x^*) = K(x) + K(y) - K(x,y) = I(y:x).$$

定義 2.3.12. $I(x:y)$ を x と y の 相互情報量 と呼ぶ.

上記の定理を示すのに，以下の概念を使う．prefix-free マシン M に対し，

$$Q_M(\sigma) = \mu([\![\{\tau \ : \ M(\tau) = \sigma\}]\!])$$

とすると，

$$K(\sigma) = -\log Q(\sigma).$$

定理 *2.3.10* の証明. $\leq$ は自明なので逆を示す.

$\{\nu_s\}$ を U の定義域の計算可能な数え上げとし，σ_s, τ_s を $U(\nu_s) = \langle \sigma_s, \tau_s \rangle$ とする．また

$$W_\sigma = \{s \ : \ \sigma_s = \sigma\}$$

とおく．任意の n と σ に対し，

$$s \in W_\sigma \text{に対して } \langle |\nu_s| - n, \tau_s \rangle$$

を request として KC 集合を作る．ただしその request の重さは 1 を超えないようにする．その KC 集合から作られた prefix-free マシンを $M_{n,\sigma}$ と呼ぼう.

次のような prefix-free マシン V を考える．ある τ について $U(\nu) = \langle \sigma, \tau \rangle$ となるときに，$V(\nu) = \sigma$ とする．このとき，

$$Q_V(\sigma) = \sum_\tau Q(\langle \sigma, \tau \rangle).$$

よって，

$$\sum_\tau Q(\langle \sigma, \tau \rangle) \leq Q(\sigma) + O(1).$$

これからある c があって，すべての σ で，

$$2^{K(\sigma)-c} \sum_\tau Q(\langle \sigma, \tau \rangle) \leq 1.$$

よって

$$\sum_{s \in W_\sigma} 2^{-|\nu_s| - |\sigma^*| + c} = 2^{K(\sigma)-c} \sum_\tau Q(\langle \sigma, \tau \rangle) \leq 1.$$

これより，$M_{K(\sigma)-c,\sigma}$ は関係するすべての request が数え上げられている．

次のような prefix-free マシン M を定義しよう．神託 ρ に対して，$U(\rho) = \sigma$ となる σ を探し，その後 $M_{|\rho|-c,\sigma}$ を模倣する．

神託が σ^* であれば，M は $M_{K(\sigma)-c,\sigma}$ を模倣する．任意の τ に対し，$\langle \sigma, \tau \rangle^* = \nu_s$ となる $s \in W_\sigma$ が存在し，$\langle K(\sigma, \tau) - K(\sigma) + c, \tau \rangle$ が request されるから，

$$K(\tau | \sigma^*) \leq K_M(\tau | \sigma^*) \leq K(\sigma, \tau) - K(\sigma) + O(1).$$

□

これを現実の分類に応用しようとしたとき，問題になるのが K の計算不可能性である．そこで思い切って通常の圧縮プログラムで近似しよう．また最大が 1 となるように正規化を行う．

定義 2.3.13 (Vitányi 2006)**.** x, y の 正規圧縮距離*(normalized compression distance)* を以下で定義する．

$$\mathrm{NCD}(x, y) = \frac{C(yx) - \min\{C(x), C(y)\}}{\max\{C(x), C(y)\}}.$$

この距離に基づいて分類を行う実験は既に行われ，遺伝子，文学作品，音楽，Linux 実行ファイル，Java オブジェクトファイルを bzip2 や gzip により適切に分類することに成功している．

更に「赤」「馬」のような概念の分類を行う実験もなされている．アイデアは単純で，それらの概念に対して，Google のような検索エンジンの結果に対し，NCD を適用するのである．

最後に

ランダムという一見捉えどころのない概念に対して，数学的な特徴付けを与えることで，様々な概念が数学の問題に置き換わる．他の例を挙げると，

- 最小記述長の理論
- ゲーム論的確率論
- 杉田洋先生によるモンテカルロ法の解析

などがある．今後，ますますランダムネスの理論が，様々な理論の基礎として使われることを期待している．

参考文献

[1] V. Becher. Turing's Normal Numbers: Towards Randomness. In S. B. Cooper, A. Dawar, and B. Löwe, editors, *CiE 2012*, volume 7318 of *LNCS*, pages 35–45, Heidelberg, 2012. Springer.

[2] L. Bienvenu, A. Day, M. Hoyrup, I. Mezhirov, and A. Shen. A constructive version of Birkhoffs ergodic theorem for Martin-Löf random points. *Information and Computation*, 2011.

[3] E. Borel. Les probabilités Dénombrables et leurs applications arithmétiques. *Rendiconti del Circolo Matematico di Palermo*, 27:247–270, 1909.

[4] C. Bourke, J. M. Hitchcock, and N. V. Vinodchandran. Entropy rates and finite-state dimension. *Theoretical Computer Science*, 349:392–406, 2005.

[5] V. Brattka, J. S. Miller, and A. Nies. Randomness and differentiability. Submitted.

[6] D. G. Champernowne. The Construction of Decimals Normal in the Scale of Ten. *Journal of the London Mathematical Society*, 8:254–260, 1933.

[7] A. H. Copeland and P. Erdös. Note on normal numbers. *Bulletin of the American Mathematical Society*, 52:857–860, 1946.

[8] O. Demuth. The differentiability of constructive functions of weakly bounded variation on pseudo numbers. *Comment. Math. Univ. Carolin.*, 16(3):583–599, 1975.

[9] R. Downey and D. R. Hirschfeldt. *Algorithmic Randomness and Complexity*. Springer, Berlin, 2010.

[10] J. Franklin, N. Greenberg, J. Miller, and K. Ng. Martin-Löf random points satisfy Birkhoff's ergodic theorem for effectively closed sets. *Proceedings of the AMS*, 140:3623–3628, 2012.

[11] P. Gács, M. Hoyrup, and C. Rojas. Randomness on Computable Probability Spaces - A Dynamical Point of View. *Theory of Computing System*, 48(3):465–485, 2011.

[12] I. Hacking. *The Emergence of Probability*. Cambridge University Press, London, 1975.

[13] M. Hutter and A. Muchnik. On semimeasures predicting Martin-Löf random sequences. *Theoretical Computer Science*, 382:247–261, 2007.

[14] A. Y. Khinchin. Über einen Satz der Wahrscheinlichkeitrechnung. *Fund. Mat.*, 6:9–20, 1924.

[15] A. Kučera. Measure, Π^0_1 classes, and complete extensions of PA. In *Recursion Theory Week*, volume 1141 of *Lecture Notes in Mathematics*, pages 245–259, Berlin, 1984, 1985. Springer.

[16] H. Lebesgue. *Leçons sur l'Intégration et la recherche des fonctions primitives*. Gauthier-Villars, Paris, 1904.

[17] H. Lebesgue. Sur l'intégration des fonctions discontinues. *Annales scientifiques de l'École Normale Supérieure*, 27:361–450, 1910.

[18] M. Li and P. Vitányi. *An introduction to Kolmogorov complexity and its applications*. Graduate Texts in Computer Science. Springer-Verlag, New York, third edition edition, 2009.

[19] A. Nies. *Computability and Randomness*. Oxford University Press, USA, 2009.

[20] N. Pathak, C. Rojas, and S. G. Simpson. Schnorr randomness and the Lebesgue Differentiation Theorem. To appear in Proceedings of the American Mathematical Society.

[21] C. P. Schnorr and H. Stimm. Endliche Automaten und Zufallsfolgen. *Acta Informatica*, 1:345–359, 1972.

[22] G. Shafer. Non-Additive Probabilities in the Work of Bernoulli and Lambert. *Archive for History of Exact Sciences*, 19(4):309–370, 1978.

[23] R. Solomonoff. Algorithmic probability: Theory and applications. *Information Theory and Statistical Learning*, pages 1–23, 2009.

[24] R. J. Solomonoff. Complexity-based induction systems: Comparisons and convergence theorems. *IEEE Transaction on Information Theory*, IT-24:422–432, 1978.

[25] A. M. Turing. A note on normal numbers. In J. L. Britton, editor, *Collected Works of A. M. Turing: Pure Mathematics*, pages 263–265. North Holland, Amsterdam, 1992. with notes of the editor in 265-265.

[26] V. G. Vovk. The law of the iterated logarithm for random Kolmogorov, or chaotic,

sequences. *Theory of Probability and Its Applications*, 32:413–425, 1987.