計算可能性理論特論２・講義ノート *†

木原 貴行
名古屋大学 情報学部・情報学研究科

最終更新日: 2018 年 2 月 1 日

目次

1 表現空間の理論

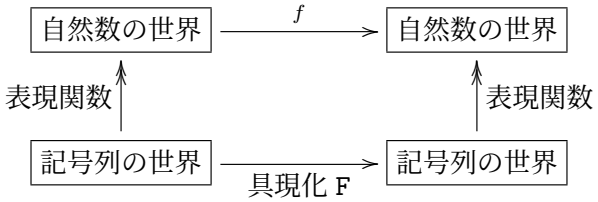
計算理論は，記号列によってコードされた数学的オブジェクトに対する計算を取り扱う分野である．この節では，文字列以外の数学的対象に関する様々な計算論を統一的に導入することを試みる．まず，自然数を記号列によって**表現**（コーディング）する，ということに立ち返って，表現（コーディング）とは何であるかの再理解を目指そう．

チューリング機械は，基本的には語上の関数 $f : (\Sigma^*)^k \to \Sigma^*$ の関数を議論するものである．し

* 本講義ノートは，2017 年度秋 2 期開講の名古屋大学大学院情報学研究科における講義「計算可能性理論特論２」の内容をまとめる予定のものである．
† 講義のページ： http://www.math.mi.i.nagoya-u.ac.jp/~kihara/teach.html

かし，2 進表現 bin によるコーディングを経由することによって，自然数上の関数 $f : \mathbb{N}^k \to \mathbb{N}$ の計算理論を展開できることは，これまでに見た通りである．これは，文字列 $\sigma \in \Sigma^*$ がどんな自然数を表しているのか，という**意味**を与えることにより，ただの文字列上の関数に自然数上の関数としての意味を与えていた，ということである．もう少し正確には，文字列 $\mathtt{bin}(n)$ が自然数 n を**表現**していたのである．この（部分）全射 $\mathtt{bin}(n) \mapsto n$ を**表現関数**と呼ぶことにしよう．

たとえば，自然数上の関数 $f : \mathbb{N}^k \to \mathbb{N}$ が計算可能であるとは，（表現関数 $\mathtt{bin}(n) \mapsto n$ を介することにより）それを記号列上の機械的操作 $\mathtt{F} :\subseteq (\Sigma^*)^k \to \Sigma^*$ として**具現化**できるということである．

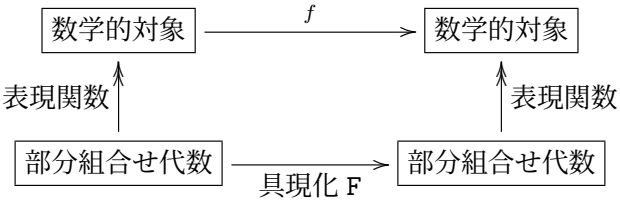


このような「**表現と具現化を経由した計算**」が計算理論の基本である．有理数や代数的数は容易に自然数でコードできるから，そのような数に関する計算論も展開できる．また，その他にも幾らかの単純な可算構造ならばコーディングできそうである．それでは，実際，どのような数学的対象ならば，記号的に表現でき，そして良い計算論を展開できるだろうか．

歴史的には，1950 年代頃に，語あるいは自然数によるコーディングという概念自体を研究対象とする**ナンバリングの理論** (*Theory of numbering*) が誕生する．また，それとは並行に，20 世紀中頃から，実数などの連続的概念を対象とする計算論である**計算可能解析学** (*computable analysis*) という分野も徐々に発展を見せた．

計算理論とはデジタル（離散的）な概念を対象とするものであり，実数や複素数などの連続的概念は計算理論の対象外である……と思われがちだが，実際はそうではない．解析学と物理学における計算可能性理論の教科書として，1989 年に Pour-El と Richards によって執筆された “Computability in Analysis and Physics” は非常に有名である

それでは，このような連続的オブジェクトを含む様々な数学的対象は如何にして計算論的に取り扱われているだろうか．その 1 つの解答は，表現と具現化に関する上の図式に少々の修正を加えるだけである．我々の記号の世界は，任意の**部分組合せ代数**であり，これによって様々な数学的対象の上の計算は，部分組合せ代数の単なる演算適用として実現される．



まず，この図式の縦方向，すなわち，部分組合せ代数による数学的対象の表現は，以下のように定式化される．

定義 1.1. $\mathbf{A}$ を(相対)部分組合せ代数とする．このとき, 集合 X と部分全射 $\nu_X :\subseteq \mathbf{A} \to X$ の対 (X, ν_X) を **$\mathbf{A}$-表現空間** ($\mathbf{A}$-*represented space*) と呼び，ν_X を X の **$\mathbf{A}$-表現** ($\mathbf{A}$-*representation*) と呼ぶ.

これは，集合 X の各要素が，部分組合せ代数 $\mathbf{A}$ の元によって名付けられたことを意味する．つまり，$\nu_X(a) = x$ であるとき，$a \in \mathbf{A}$ は x の **ν_X-コード** (*code*) または **ν_X-名** (*name*) と呼ばれる．表現関数 ν_X が文脈から明らかな場合は，単にコードまたは名と呼ぶ．1 つの元 $x \in X$ が複数のコードを持ち得る場合もあることに注意する．$\nu_X(a)$ の代わりにしばしば $[a]_X$ と書くことがある．このとき，各 $x \in X$ について，$||x||_X$ によって x のコード全体の集合を表す．つまり，以下のように定義する．

$$||x||_X = \{a \in \mathbf{A} : x = [a]_X\}.$$

注意．実現可能性理論 (*realizability theory*) では，$(X, ||\cdot||_X)$ は**モデスト集合** (*modest set*) と呼ばれる．本稿では，しばしば表現空間 $(X, [\cdot]_X)$ とモデスト集合 $(X, ||\cdot||_X)$ を同一視し，後者のことも表現空間と呼ぶ.

例 1.2. 部分組合せ代数 $\mathbf{A}$ の中で常に自然数をコードできることは定義**??**において見た通りである．これを表現空間の言葉で言い直そう．定義**??**では，自然数 $n \in \mathbb{N}$ に対して，対応する $\underline{n} \in \mathbf{A}$ を具体的に与えた．部分関数 $\nu_{\mathbb{N}} :\subseteq A \to \mathbb{N}$ を $\nu_{\mathbb{N}}(\underline{n}) \to n$ によって定義すれば，$(\mathbb{N}, \nu_{\mathbb{N}})$ は $\mathbf{A}$-表現空間をなす．各 $n \in \mathbb{N}$ の $\nu_{\mathbb{N}}$-コードは $\underline{n} \in A$ のみであり，よって $||n||_{\mathbb{N}} = \{\underline{n}\}$ である．

豆知識．表現が多価である場合もしばしば重要となる．集合 X と部分多価全射 $\delta_X :\subseteq \mathbf{A} \rightrightarrows X$ の対 (X, δ_X) を **$\mathbf{A}$-多価表現空間** ($\mathbf{A}$-*multi-represented space*) と呼ぶ．実現可能性理論においては，これと同一な概念は **アセンブリ** (*assembly*) と呼ばれる.

つづいて，上の図式における，数学的対象上の写像の部分組合せ代数上の関数による具現化の部分である．これは，以下のように定式化される.

定義 1.3. $\mathcal{X} = (X, \nu_X)$ と $\mathcal{Y} = (Y, \nu_Y)$ を $\mathbf{A}$-表現空間とする．このとき，$\mathtt{F} :\subseteq \mathbf{A} \to \mathbf{A}$ が $f : \mathcal{X} \to \mathcal{Y}$ の**具現化**であるとは，任意の $x \in X$ に対して，x のどんな ν_X-コード $\mathtt{x} \in \mathbf{A}$ が与えられても，$\mathtt{F}(\mathtt{x})$ が $f(x)$ の ν_Y-コードを与えていることを意味する.

つまり，$\mathtt{F}$ が f の具現化であるとは，以下の図式を可換にすることである.

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ {\scriptstyle \nu_X}\uparrow & & \uparrow{\scriptstyle \nu_Y} \\ \mathbf{A} & \xrightarrow[\mathtt{F}]{} & \mathbf{A} \end{array}$$

ここで，具現化 $\mathtt{F}$ として，部分組合せ代数上の関数であれば何でもよい．しかし，計算理論としては，$\mathtt{F}$ としては，部分組合せ代数上の演算として実現できるものであってほしい．ここで，定義 **??**における実現可能関数と計算可能関数のことを思い出そう．これによって，空間上の関数で，記号操作によって実現できるものと，計算できるもの，そうでないものが明確に分けられる．

定義 1.4. $\mathcal{X}$ と $\mathcal{Y}$ を $\mathbf{A}$-表現空間とする．関数 $f : \mathcal{X} \to \mathcal{Y}$ が**実現可能** (*realizable*) とは，f の実現可能な具現化 $\mathtt{F} :\subseteq \mathbf{A} \to \mathbf{A}$ が存在することを意味する．関数 $f : \mathcal{X} \to \mathcal{Y}$ が**計算可能** (*computable*) であるとは，f の計算可能な具現化 $\mathtt{F} :\subseteq \mathbf{A} \to \mathbf{A}$ が存在することを意味する．

注意. 具現化と実現可能関数の英名は realizer と realizable function であるが，本稿では 1 つの realize という単語に対して，具現と実現という 2 つの訳語を用いている．訳語は統一すべきかもしれないが，具現化と実現可能関数は定義上は大きく異なるものであり，混乱を招き得るので，あえて訳語をずらした．

例 1.5. 例 1.2 で定義した $\mathbf{A}$-表現空間 $(\mathbb{N}, \nu_{\mathbb{N}})$ において，$n \mapsto n+1$ の具現化は $\underline{n} \mapsto \underline{n+1}$ であり，これは命題**??**より $\mathtt{succ} \in \mathbf{A}$ によって実現可能である．つまり，$f : (\mathbb{N}, \nu_{\mathbb{N}}) \to (\mathbb{N}, \nu_{\mathbb{N}})$ を $f(n) = n + 1$ で定義すれば，この f は実現可能関数である．

相対部分組合せ代数 $\mathbf{A}$ に対し，しばしば $\mathsf{Mod}(\mathbf{A})$ によって $\mathbf{A}$-表現空間と計算可能関数のなす圏を表すことがある．部分組合せ代数による表現を考えるメリットは，部分組合せ代数が関数適用の抽象化であり，任意の $\mathbf{A}$-表現空間 X, Y に対して，関数空間 $[X \to Y]$ もまた $\mathbf{A}$-表現空間になるということである．専門用語を用いれば，$\mathsf{Mod}(\mathbf{A})$ は**デカルト閉圏** (*cartesian closed category*) をなすことが分かる．具体的には，以下のようにして関数空間は表現される．

定義 1.6. $\mathbf{A}$-表現空間 X, Y に対し，X から Y への $\mathbf{A}$-実現可能関数全体の空間は次の関数 $\mathtt{f} \mapsto [\![\mathtt{f}]\!]_{X \to Y}$ によって表現できる．

$$[\![\mathtt{f}]\!]_{X \to Y} = f \iff (\forall a)\ [\mathtt{f}a]_Y = f([a]_X).$$

つまり，関数 $f : X \to Y$ の名とは，f の具現化を実現する元 $\mathtt{f} \in \mathbf{A}$ である．この表現空間を $[X \to Y]_{\mathbf{A}}$ と書く．$\mathbf{A}$ が文脈から明らかな場合は，単に $[X \to Y]$ と書く．

事実，1950 年代に，クリーネは高階関数の計算理論を作り上げた．現代的な視点からは，クリーネの高階関数論の基本的な部分は，クリーネの第一または相対第二代数による表現空間の理論の一部として展開することができる．部分組合せ代数によって空間を表現することの有り難みは，その空間上の計算論を導入できるというだけでなく，様々な圏論的構成を受容できる，ということでもある．しかし，本稿では圏論についてはこれ以上深入りしない．

1.1 ナンバリングの理論

最も基本的な表現空間の理論は，クリーネの第一代数によるものである．命題**??**ではクリーネの第一代数を $\mathbb{K}_1$ と書いたが，クリーネの第一代数が単に自然数上の標準的な計算論であることを強調するため，以後，$\mathbf{N}$ によってクリーネの第一代数を表す．伝統的に，$\mathbf{N}$-表現は**部分ナンバリング** (*partial numbering*) と呼ばれ，全域 $\mathbf{N}$-表現は**ナンバリング** (*numbering*) と呼ばれる．また，$\mathbf{N}$-表現空間は**数化集合** (*numbered set*) と呼ばれることもある．しかし，本稿では用語の統一のために，これらの古典的な用語は用いない．この節では，クリーネの第一代数に基づく $\mathsf{Mod}(\mathbf{N})$ 上の計算論を概観しよう．つまり，自然数上の計算論に基づく理論によって，如何なる計算論が展開可能かを見る．

まず，命題**??**を用いると，任意の部分組合せ代数の中で有限列が 1 つの要素としてコードできる．たとえば 3 つの元 $a, b, c \in \mathbf{N}$ は，$\langle a, b, c\rangle = \langle\langle a, b\rangle, c\rangle \in \mathbf{N}$ のようにコードされる．

例 1.7 (有理数)**.** 各 $a, b \in \mathbb{N}$, $b \neq 0$ について，

$$\nu_{\mathbb{Q}}(\langle 0, a, b\rangle) = \frac{a}{b}, \qquad \nu_{\mathbb{Q}}(\langle 1, a, b\rangle) = -\frac{a}{b}$$

によって $\nu_{\mathbb{Q}} :\subseteq \mathbf{N} \to \mathbb{Q}$ を定義する．このとき，$(\mathbb{Q}, \nu_{\mathbb{Q}})$ は $\mathbf{N}$-表現空間である．

例 1.8 (計算可能関数の空間)**.** チューリング機械 M のコード e が与えられたとき，$[\![e]\!]$ によって，M によって計算される $\mathbb{N}$ 上の部分関数を表すものとする．このとき，$[\mathbb{N} \to \mathbb{N}_\perp]$ を $\mathbb{N}$ 上の部分計算可能関数全体の集合とすると，$([\mathbb{N} \to \mathbb{N}_\perp], [\![\cdot]\!])$ は $\mathbf{N}$-表現空間をなす．

例 1.9 (計算可枚挙集合の空間)**.** CE を $\mathbb{N}$ の計算可枚挙部分集合全体の集合とする．各 $e \in \mathbb{N}$ に対して，W_e を次のように定義する．

$$W_e = \{n \in \mathbb{N} : [\![e]\!](n)\downarrow\}.$$

このとき，$W : e \mapsto W_e$ に対して，(CE, W) は $\mathbf{N}$-表現空間をなす．

命題**??**の証明の直後で触れたように，クリーネの第一代数 $\mathbf{N} = (\mathbb{N}, \cdot)$ の代わりに $\Sigma^* = (\Sigma^*, \cdot)$ を考えてもよい．次の例では，Σ^*-表示空間を考えたほうが少し都合がよい．しかし，Σ^*-表示空間と $\mathbf{N}$-表示空間は計算可能性理論としては実質的に同一である．したがって，その多少の差異を気に留める必要はない．

例 1.10 (有限表示モノイド)**.** アルファベット Σ 上の関係 $R \subseteq \Sigma^* \times \Sigma^*$ が与えられたとき，各 $\sigma \in \Sigma^*$ に対して，

$$[\sigma]_R = \{\tau \in \Sigma^* : \sigma \equiv_R \tau\}$$

と定義する．ここで，$\equiv_R$ は例**??**で定義した自由モノイド Σ^* 上の合同関係である．このとき，$\sigma \mapsto [\sigma]_R$ は $\langle \Sigma \mid R\rangle$ によって与えられる商モノイド M_R の Σ^*-表現関数である．よって，$(M_R, [\cdot]_R)$ は Σ^*-表現空間をなす．

ここで，M_R の元のコードは一意ではないことに注意する．つまり，$x = [\sigma]_R \in M_R$ に対して，$\tau \equiv_R \sigma$ なる τ は全て x のコードである．

例 1.11 (有限有向グラフ)**.** $G = (V, E)$ を有限有向グラフとする．このとき，V と E は共に有限集合なので，$V = \{v(i)\}_{i \leqslant n}$ かつ $E = \{(v(a_i), v(b_i)) : i \leqslant k\}$ のように並べられるはずである．すると，定理**??**の証明中の文字列書換系と同様の方法で $G = (V, E)$ をコードできる:

$$\langle\langle a_0, b_0\rangle, \langle a_1, b_1\rangle, \langle a_2, b_2\rangle, \ldots, \langle a_k, b_k\rangle\rangle.$$

これによって，グラフ G の同型類を表しているものと考える．つまり，上のような有限有向グラフのコード $\sigma \in \Sigma^*$ が与えられたとき，$\mathrm{Gr}(\sigma)$ を σ によって表されるグラフとしたとき，

$$\sigma \simeq_{\mathrm{Graph}} \tau \iff \mathrm{Gr}(\sigma) \text{ と } \mathrm{Gr}(\tau) \text{ が有向グラフとして同型である}$$

と定義する．このとき，C_{Graphs} を有限有向グラフのコードを表している自然数全体とする，つまり $\mathrm{dom}(\mathrm{Gr})$ のこととする．$\mathsf{FinGraphs} = C_{\mathrm{Graphs}}/\simeq_{\mathrm{Graph}}$ を**有限有向グラフの同型類の N-表現空間**と呼び，**N**-表現関数は $\sigma \mapsto [\sigma]_{\mathrm{Graph}} = \{\tau : \tau \simeq_{\mathrm{Graph}} \sigma\}$ によって与えられる．

注意. 文字列書換系 $(\Sigma^*, \to)$ も有向グラフと考えられるが，これは無限グラフであることに注意する．また，例 1.10 の空間を無限グラフとして見たとき，これはあくまで 1 つの無限グラフを固定した上での連結成分全体の表現空間となり，例 1.11 のような有限グラフの同型類全体の表現空間とは全く異なるものである．

例 1.12 (遺伝的有限集合)**.** 集合 A が与えられたとき，$G_A = (\{A\}, \ni)$ を有向グラフだと思うこととする．A が**遺伝的有限集合** (*hereditarily finite set*) であるとは，G_A が有限グラフであることを意味する．したがって，例 1.11 と同じ方法で，全ての遺伝的有限集合をコードできる．つまり，有限有向グラフの同型類の **N**-表現空間 $\mathsf{FinGraphs}$ の部分空間として，遺伝的有限集合全体 $\mathbb{HF}$ は **N**-表現空間をなす．

定義 1.13. **A**-表現空間 X が**決定可能** (*decidable*) または**計算離散** (*computably discrete*) であるとは，X 上の等号 $=$ が計算可能であることを意味する．言い換えれば，

$$\{(u, v) \in \mathbf{A} \times \mathbf{A} : \nu_X(u) = \nu_X(v)\}$$

が計算可能であることを言う．

例 1.14. 有限表示モノイド $\langle \Sigma \mid R\rangle$ の**語の問題** (*word problem*) とは，以下の集合

$$\mathsf{WP}_{\langle \Sigma | R\rangle} = \{(u, v) \in \Sigma^* \times \Sigma^* : u \equiv_R v\}$$

の要素関係の決定問題である．言い換えれば，与えられた $(u, v) \in \Sigma^*$ について，$(u, v) \in \mathsf{WP}_{\langle \Sigma | R\rangle}$ かどうかを判定する問題である．有限表示モノイド $\langle \Sigma \mid R\rangle$ の語の問題が**計算可能** (*computable*)

または**可解** (*solvable*) であるとは，この判定が計算可能であることである．つまり，$\mathsf{WP}_{\langle\Sigma|R\rangle}$ が計算可能集合であることを意味する．

例 1.10 のように有限表示モノイド $\langle\Sigma \mid R\rangle$ を Σ^*-表現空間として見たとき，$\langle\Sigma \mid R\rangle$ が決定可能表現空間であることと語の問題 $\mathsf{WP}_{\langle\Sigma|R\rangle}$ が計算可能であることは同値である．

例 1.15. 例 1.11 の有限有向グラフの同型類の表示空間 FinGraphs および例 1.12 の遺伝的有限集合全体の表示空間 $\mathbb{HF}$ は決定可能空間である．なぜなら，与えられた 2 つの有限構造の間に全単射は有限種類しか存在しないので，それぞれが同型写像になっているかを順々に検証していけばよい．

さて，ナンバリングの理論の主題は，異なるナンバリングの比較である．チューリング完全な計算モデルが与えられれば，それは部分計算可能関数全体のナンバリング，つまり関数空間 $[\mathbb{N} \to \mathbb{N}_\perp]$ の $\mathbf{N}$-表現を与えるだろう．しかし，当然ながら，計算モデル毎に異なる $\mathbf{N}$-表現が作られる．重要な問題は，複数の計算モデル間の翻訳の問題である．我々が用いている計算モデル M によって，別人物が用いている計算モデル N における計算をシミュレートしたい．計算モデルを具体的なプログラミング言語に置き換えると，状況が分かりやすい．たとえば，M は Haskell で N は Java であるとすれば，Java のソースコードを Haskell のソースコードに変換するトランスコンパイラを作れるか，という問題となる．

数学的にこの翻訳問題を定式化しよう．$[\![e]\!]_M$ によって，計算モデル M においてコード e のプログラムが与える部分計算可能関数を表す．$[\![e]\!]_N$ と書いたときも同様である．$[\![\cdot]\!]_N$ から $[\![\cdot]\!]_M$ への翻訳問題は，次のような計算可能関数 $t : \mathbb{N} \to \mathbb{N}$ が存在するかどうかを尋ねるものである．

$$(\forall e \in \mathbb{N})\ [\![e]\!]_N \simeq [\![t(e)]\!]_M.$$

本稿では深入りしないが，ナンバリングの理論における最初の発見のひとつは，チューリング完全（すなわち全ての部分計算可能関数を実装できる）というだけでは，「万能機械」とは言い切れない，ということである．実際，互いに翻訳の存在しないチューリング完全な計算モデルが有り得る．これは部分組合せ代数とならないチューリング完全な計算モデルがあるということでもある．

以上は関数空間 $[\mathbb{N} \to \mathbb{N}_\perp]$ の $\mathbf{N}$-表現に関する議論であるが，一般的な $\mathbf{A}$-表現空間における翻訳概念を定義できる．

定義 1.16. ν_0, ν_1 を集合 X の $\mathbf{A}$-表現とする．ν_0 が ν_1 に**還元可能** (*reducible*) であるとは，ある計算可能関数 $t :\subseteq \mathbf{A} \to \mathbf{A}$ が存在して，次が成立することを指す．

$$(\forall a \in \mathrm{dom}(\nu_0))\ \nu_0(a) = \nu_1(t(a)).$$

このとき，$\nu_0 \leqslant \nu_1$ と書く．また，$\nu_0 \leqslant \nu_1$ かつ $\nu_1 \leqslant \nu_0$ であるとき，$\nu_0 \equiv \nu_1$ と書く．

もし $\nu_0 \equiv \nu_1$ であれば, 同値な表現であると思って良い．集合 X の表現 ν_0, ν_1 について, $\nu_0 \leqslant \nu_1$

ということは，恒等写像 $\mathrm{id} : (X, \nu_0) \to (X, \nu_1)$ が計算可能ということと同値である．

同じ集合に対して，複数の同値でない表現を与えて，それらを同時に取り扱うことが多々ある．これは，同一の集合に対して複数の異なる位相構造や代数構造などを入れることと同じようなものである．集合の表現を与えるというのは，集合に表現を介して計算可能性構造を入れるということであり，そして計算可能性構造の入れ方は一意ではない．

たとえば，2 元集合 $\{0,1\}$ の表現を幾つか見てみよう．

例 1.17 (離散 2 点空間)**.** 恒等関数の $\{0,1\}$ への制限 $\mathrm{id}_2 : \{0,1\} \to \{0,1\}$ は $\{0,1\}$ の $\mathbf{N}$-表現である．また，$\nu_2 : \mathbb{N} \to \{0,1\}$ を n が偶数ならば $\nu_2(n) = 0$ とし，n が奇数なら $\nu_2(n) = 1$ と定義すれば，$\nu_2 : \mathbb{N} \to \{0,1\}$ は $\{0,1\}$ の全域 $\mathbf{N}$-表現である．$\mathbf{N}$-表現空間 $(\{0,1\}, \mathrm{id}_2)$ と $(\{0,1\}, \nu_2)$ を離散 2 点空間と呼び，それぞれ $\mathbf{2}$ および $\mathbf{2}_\nu$ と書く．

例 1.18 (シエルピンスキ空間)**.** 2 元集合 $\{0,1\}$ に次の表現を与えたものを**シエルピンスキ空間** (*Sierpiński space*) と呼び，$\mathbb{S}$ と書く．

$$[e]_{\mathbb{S}} = \begin{cases} 1 & \text{if } [\![e]\!](0)\downarrow \\ 0 & \text{otherwise} \end{cases}$$

還元可能性証明の練習のために，以下を確認しよう．

命題 1.19. $\mathrm{id}_2 \equiv \nu_2 < [\cdot]_{\mathbb{S}}$.

Proof. $\mathrm{id}_2 \leqslant \nu_2$ であることは，任意の $i \in \{0,1\}$ について $\mathrm{id}_2(i) = \nu_2(i)$ であることから従う．$\nu_2 \leqslant \mathrm{id}_2$ について，$\nu_2 : \mathbb{N} \to \{0,1\}$ は自然数上の関数として計算可能であり，$t = \nu_2$ とすれば，任意の $n \in \mathbb{N}$ について $\nu_2(n) = \mathrm{id}_2(t(n))$ が成立する．続いて $\mathrm{id}_2 \leqslant [\cdot]_{\mathbb{S}}$ であるが，0 を入力した時に停止するプログラム e_0 と停止しないプログラム e_1 を作る．つまり，$[\![e_0]\!](0)\uparrow$ かつ $[\![e_1]\!](0)\uparrow$ であり，よって，$[e_0]_{\mathbb{S}} = 0$ かつ $[e_1]_{\mathbb{S}} = 1$ である．このとき $i \mapsto e_i$ は計算可能であり，$\mathrm{id}_2(i) = i = [e_i]_{\mathbb{S}}$ を得る．

最後に $[\cdot]_{\mathbb{S}} \not\leqslant \mathrm{id}_2$ を示す．もし $[\cdot]_{\mathbb{S}} \leqslant \mathrm{id}_2$ だとしたら，ある計算可能関数 $t : \mathbb{N} \to 2$ が存在して，任意の e について，$[e]_{\mathbb{S}} = t(e)$ となる．t は全域計算可能関数であるから，$\{e \in \mathbb{N} : t(e) = 1\}$ は計算可能である．一方，$\{e \in \mathbb{N} : [e]_{\mathbb{S}} = 1\} = \{e \in \mathbb{N} : [\![e]\!](0)\downarrow\}$ となる．演習問題**??**より，これは計算不可能である．よって $[\cdot]_{\mathbb{S}} \not\leqslant \mathrm{id}_2$ を得る． □

これらの「表現が同値でない」ということについて「同じものを違う風に表現している」と常に考えるのは少しばかり誤解を生む．「同じものの表現が異なる」というよりは，「違うものだが集合部分がたまたま一致する」と考えた方が適切な状況もある．たとえば，離散 2 点空間 $\mathbf{2}$ および $\mathbf{2}_\nu$ とシエルピンスキ空間 $\mathbb{S}$ は，そもそも想定している空間が異なる．離散 2 点空間において，0 と 1 は平等である．一方，シエルピンスキ空間 $\mathbb{S}$ においては，0 と 1 は不平等である．

シエルピンスキ表現では，計算が「停止しない」という状況を 0 で表し，「停止する」という状況を 1 で表している．「停止しない」という状況から「停止する」という状況に計算が遷移するこ

とはあっても逆は有り得ない．この意味で，0 と 1 は異なる質を持っているのである．この 0 と 1 の不平等性，あるいは 0 から 1 への一方向遷移を明示した空間がシエルピンスキ空間である．

シエルピンスキ空間は計算可枚挙性と大きく関連する．これを説明するために，表現空間の同型性の概念を導入しよう．

定義 1.20. **A**-表現空間 X, Y が**計算同型** (*computably isomorphic*) とは，ある全単射 $f : X \to Y$ で，f と f^{-1} が共に計算可能であるものが存在することを意味する．

定義 1.6 を用いて，関数空間 $[\mathbb{N} \to \mathbb{S}]$ を考えよう．我々の部分組合せ代数は $\mathbf{N}$ であるから，$[\mathbb{N} \to \mathbb{S}]$ は $\mathbb{N}$ から $\mathbb{S}$ への計算可能関数全体の空間であり，次の表現関数 $[\![\cdot]\!]_{\mathbb{N}\to\mathbb{S}}$ によって表現されている．

$$[\![\mathtt{f}]\!]_{\mathbb{N}\to\mathbb{S}} = f \iff (\forall n \in \mathbb{N})\ [[\![\mathtt{f}]\!](n)]_{\mathbb{S}} = f(n).$$

実は，この関数空間 $[\mathbb{N} \to \mathbb{S}]$ は，例 1.9 の計算可枚挙集合の空間 CE と同型である．

命題 1.21. $\mathbf{N}$-表現空間 $[\mathbb{N} \to \mathbb{S}]$ と CE は計算同型である．

Proof. 関数 $\Phi : [\mathbb{N} \to \mathbb{S}] \to \mathsf{CE}$ を次によって定義する．各 $g : [\mathbb{N} \to \mathbb{S}]$ に対して，

$$\Phi(g) = g^{-1}\{1\} = \{n \in \mathbb{N} : g(n) = 1\}.$$

この関数 Φ が計算同型写像であることを示そう．明らかに Φ は単射である．Φ の計算可能性について，$[\![p(e)]\!](n) \simeq [\![[\![e]\!](n)]\!](0)$ なる計算可能関数 $p : \mathbb{N} \to \mathbb{N}$ を取ると，任意の $e \in \mathbb{N}$ について，

$$\begin{aligned}\Phi([\![e]\!]_{\mathbb{N}\to\mathbb{S}}) = \{n \in \mathbb{N} : [[\![e]\!](n)]_{\mathbb{S}} = 1\} &= \{n \in \mathbb{N} : [\![[\![e]\!](n)]\!](0)\downarrow\} \\ &= \{n \in \mathbb{N} : [\![p(e)]\!](n)\downarrow\} = W_{p(e)}\end{aligned}$$

となるから，p は Φ を具現化する．一方，$[\![e]\!](n) \simeq [\![[\![q(e)]\!](n)]\!](0)$ なる計算可能関数 $q : \mathbb{N} \to \mathbb{N}$ を取ると，

$$W_e = \{n \in \mathbb{N} : [\![e]\!](n)\downarrow\} = \{n \in \mathbb{N} : [\![[\![q(e)]\!](n)]\!](0)\downarrow\} = \Phi([\![q(e)]\!]_{\mathbb{N}\to\mathbb{S}})$$

であるから，q は Φ^{-1} を具現化する．以上より，Φ が計算同型写像であることが示された． □

1.2 ライスの定理と空間の連結性

本節では，1953 年にヘンリー・ライス (Henry G. Rice) によって証明された**ライスの定理** (*Rice's theorem*) を取り扱う．これは，次のような驚くべき主張をする定理である．

> 部分計算可能関数に関する非自明な性質 P が任意に与えられている．このとき，与えられたプログラム e の計算する関数が P を満たすか否かを判定するアルゴリズムは存在しない．

第??節では，個々の決定問題が計算可能か計算不可能かを議論してきたが，ライスの定理は一度で大量の決定問題の計算不可能性を導く．究極の計算不可能性定理の 1 つである．

ライスの定理は，一見すると非常に興味深いが，しかし，クリーネの再帰定理などとは異なり，定理自体の有用性は低く，理論的にも深みがあるわけではない．それにも関わらず，ライスの定理は何故か伝統的に計算可能性理論入門における必須トピックとして取り扱われる．これは，その定理の衝撃的な内容に比較すると，証明が極めて簡単であるからであろう．

しかし，それだけでは，必須トピックとして扱うには少し説得力が足りない．ここでは，ライスの定理の空間的側面，つまり，これが計算可能性理論の概念を空間的に理解するためには良いトピックであることを強調する．「計算と空間」というコンテキストに置くことで，ライスの定理は特筆すべき価値を持つ．本節における我々の目標は，ライスの定理に対する以下のような幾何学的イメージを持つことである．

> 自然数や文字列の世界は離散空間（デジタル）であるが，自然数や文字列上の部分計算可能関数全体を空間として見ると，そこは連結空間のようになっている．

定義 1.1 において，表現空間 X の要素 x のコード全体の集合を $||x||_X$ と書いていたことを思い出そう．X が $\mathbf{N}$-表現空間の場合，部分集合 $S \subseteq X$ について，S の元のコード全体の集合 $||S||_X = \bigcup_{x \in S} ||x||_X$ は伝統的に**添字集合** (*index set*) と呼ばれることがある．

定義 1.22. X を全域 $\mathbf{N}$-表現空間とする．集合 $A \subseteq X$ が**計算可能開** (*computably open*) とは，添字集合 $||A||_X$ が計算可枚挙であることを意味する．

この概念は単に計算可枚挙と呼ばれることも多いが，本稿では，空間としての側面を強調するために，これを計算可能開集合と呼ぶ．計算可能開集合 A とは，与えられたコード e が A の要素を表すかどうかに関する半計算可能な手続きがあるということである．計算可能開集合全体を開基とする全域 $\mathbf{N}$-表現空間上の位相は**エルショフ位相** (*Ershov topology*) と呼ばれる．

例 1.23. 例 1.17 の離散 2 点空間 $\mathbf{2}$ において，$\varnothing, \{0\}, \{1\}, \{0,1\}$ は全て計算可能開集合である．一方，例 1.18 のシエルピンスキ空間 $\mathbb{S}$ においては，$\varnothing, \{1\}, \{0,1\}$ は計算可能開集合だが，$\{0\}$ は計算可能開集合ではない．

豆知識. シエルピンスキ空間上のエルショフ位相を考えると，位相空間論におけるシエルピンスキ空間と同相になる．

計算可枚挙集合を開集合として見ると，計算可能関数は連続関数に相当する．位相空間論において，連続関数とは，開集合の逆像が開集合となるような関数であった．

命題 1.24. X と Y を全域 $\mathbf{N}$-表現空間であり，$f : X \to Y$ を計算可能関数とする．このとき，

任意の計算可能開集合 $U \subseteq Y$ に対して，$f^{-1}[U]$ も X の計算可能開集合である．

Proof. $f : X \to Y$ が計算可能関数であれば，f を具現化する計算可能関数 $\mathtt{f} : \mathbb{N} \to \mathbb{N}$ が存在する．ν_X と ν_Y をそれぞれ X と Y の表現とすれば，つまり，$f \circ \nu_X = \nu_Y \circ \mathtt{f}$ である．このとき，$f^{-1}[U]$ のコードの集合は以下によって与えられている．

$$\begin{aligned}||f^{-1}[U]||_X = ||\{x \in X : f(x) \in U\}||_X =& \{n \in \mathbb{N} : f(\nu_X(n)) \in U\} \\ =& \{n \in \mathbb{N} : \nu_Y(\mathtt{f}(n)) \in U\} = \{n \in \mathbb{N} : \mathtt{f}(n) \in ||U||_Y\}.\end{aligned}$$

仮定より，U は計算可能開集合であるから，$||U||_Y$ は計算可枚挙である．$\mathtt{f}$ は計算可能であるから，明らかに $\{n \in \mathbb{N} : \mathtt{f}(n) \in ||U||_Y\}$ も計算可枚挙である．よって，$||f^{-1}[U]||_X$ は計算可枚挙であり，つまり $f^{-1}[U]$ が計算可能開集合であることが示された． □

豆知識． 命題 1.24 の性質を強めて，計算可能開集合 U のコードから計算可能開集合 $f^{-1}[U]$ のコードを返す計算可能関数が存在する，という主張にすると，これが f の計算可能性と同値になる．

定義 1.25. 全域 **N**-表現空間 X が**計算連結** (*computably connected*) とは，X の非自明な計算可能直和分解が存在しないことである．つまり，$X = X_0 \cup X_1$ かつ $X_0 \cap X_1 = \varnothing$ となるような空でない計算可能開部分集合 $X_0, X_1 \subseteq X$ が存在しないことを意味する．

計算連結性はライスの定理と深く関わっている．実際，以下は容易に確かめられる．

$$\text{計算連結} \iff \text{自明なものを除く添字集合が全て計算不可能.}$$

なぜなら，計算連結性は添字集合 $||X_0||_X$ と $||X_1||_X$ が共に計算可枚挙であることを述べるが，X_0 と X_1 は全体空間 X の分割なので，$||X_1||_X = \mathbb{N} \backslash ||X_0||_X$ である．よって，ポストの定理 (系 **??**) より，これは添字集合 $||X_0||_X$ と $||X_1||_X$ が共に計算可能であることと同値である．

したがって，ライスの定理とは，空間 $[\mathbb{N} \to \mathbb{N}_\perp]$ の計算連結性を述べる定理である．

例 1.26. シエルピンスキ空間 $\mathbb{S}$ は計算連結である．なぜなら，$\mathbb{S}$ の非自明な分割は $\mathbb{S} = \{0\} \cup \{1\}$ のみであるが，$\{0\}$ の添字集合は $||0||_{\mathbb{S}} = \{e \in \mathbb{N} : [e](0) \uparrow\}$ であり，これは計算可枚挙ではない．

ところで定義 1.13 において，計算離散性という概念を導入した．2 点以上を含む離散空間は不連結であるという位相空間論的事実は，計算可能性理論では次のように表される．

例 1.27. 2 点以上を含む **N**-表現空間は，もし計算離散ならば計算連結ではない．

定義 1.28. $(X, [\cdot]_X)$ を **N**-表現空間とする．このとき，X の**持ち上げ** (*lifting*) とは，集合 $X_\perp = X \cup \{\perp_X\}$ に次の表現 $[\cdot]_{X_\perp}$ を与えた **N**-表現空間である．

$$[e]_{X_\perp} = \begin{cases} [[\![e]\!](0)]_X & \text{if } [\![e]\!](0) \downarrow \\ \perp_X & \text{otherwise.} \end{cases}$$

例 1.29. 自然数全体の集合 $\mathbb{N}$ は，恒等写像によって表現することにより，自明に $\mathbf{N}$-表現空間となる．このとき，$\mathbb{N}_\perp$ の表現は

$$[e]_{\mathbb{N}_\perp} = \begin{cases} [\![e]\!](0) & \text{if } [\![e]\!](0)\downarrow \\ \perp_{\mathbb{N}} & \text{otherwise.} \end{cases}$$

によって与えられる．このような空間は**平坦領域** (*flat domain*) と呼ばれる．

シエルピンスキ空間は一点空間 $\mathbf{1} = \{\bullet\}$ の持ち上げと考えることもできる．持ち上げに関する重要な性質として，必ずレトラクション $r : X_{\perp\perp} \to X_\perp$ が存在する，ということがある．ここで，集合 X の部分集合 $S \subseteq X$ に対して，**レトラクション** (*retraction*) とは関数 $r : X \to S$ で，$r \upharpoonright S$ が恒等関数であるようなもののことである．つまり，任意の $x \in S$ に対して，$r(x) = x$ を満たす．

この性質を $X_\perp$ のような $\perp$ を持つ空間の本質であると考えよう．このアイデアを元に，$\perp$ に相当するものが既に存在している空間を次のように抽象化する．

定義 1.30. 全域 $\mathbf{N}$-表現空間 Z が **$\perp$-レトラクト** ($\perp$-*retract*) であるとは，計算可能レトラクション $r_Z : Z_\perp \to Z$ が存在することを意味する．

注意. $\perp$-レトラクトは**フォーカル集合** (*focal set*) とも呼ばれる．

演習問題 1.31. 任意の全域 $\mathbf{N}$-表現空間 X に対して，$X_\perp$ は $\perp$-レトラクトであることを示せ．

例 1.32. $\mathbb{N}$ 上の部分計算可能関数の空間 $[\mathbb{N} \to \mathbb{N}_\perp]$ は $\perp$-レトラクトである．ここで，$[\mathbb{N} \to \mathbb{N}_\perp]$ は $[\![\cdot]\!]$ によって表現されている．関数空間 $[\mathbb{N} \to \mathbb{N}_\perp]$ の持ち上げ $[\mathbb{N} \to \mathbb{N}_\perp]_\perp$ の表現を $[\![\cdot]\!]_\perp$ と書くことにする．次のような r が計算可能であることを示せばよい．任意の $f \in [\mathbb{N} \to \mathbb{N}_\perp]_\perp$ に対して，

$$r(f) = \begin{cases} f & \text{if } f \in [\mathbb{N} \to \mathbb{N}_\perp], \\ \varnothing & \text{if } f \notin [\mathbb{N} \to \mathbb{N}_\perp]. \end{cases}$$

ここで，$\varnothing$ は至る所未定義な関数を表す．このような関数 r は明らかにレトラクションである．

r の計算可能性を示すため，$d(e)$ を次のようなチューリング機械のコードとする．入力 n に対して，プログラム $[\![e]\!](0)$ が停止するのを待ち，停止したら $[\![[\![e]\!](0)]\!](n)$ を実行する．

$$\begin{aligned} &[\![e]\!](0)\downarrow \implies (\forall n)\ [\![d(e)]\!](n) \simeq [\![[\![e]\!](0)]\!](n) \implies [\![d(e)]\!] \simeq [\![[\![e]\!](0)]\!] \simeq [\![e]\!]_\perp \\ &[\![e]\!](0)\uparrow \implies (\forall n)\ [\![d(e)]\!](n)\uparrow \implies [\![d(e)]\!] = \varnothing. \end{aligned}$$

したがって，計算可能関数 $d : \mathbb{N} \to \mathbb{N}$ は明らかに r の具現化である．

例 1.33. 例 1.32 の議論を少し修正すると，任意の全域 $\mathbf{N}$-表現空間 X, Y について，X から Y への部分関数全体の空間 $[X \to Y_\perp]$ は $\perp$-レトラクトであることが示される．特に，命題 1.21 より，$\mathbb{N}$ 上の計算可枚挙集合の空間 $\mathsf{CE} \simeq [\mathbb{N} \to \mathbb{S}] \simeq [\mathbb{N} \to \mathbb{S}_\perp]$ は $\perp$-レトラクトである．

定理 1.34 (抽象ライスの定理)**.** 任意の $\bot$-レトラクトは計算連結である.

Proof. X を $\bot$-レトラクトとする. まず, 次を示す.

主張. 任意の $x \in X$ に対して, $f_x : \mathbb{S} \to X_\bot$ を $f_x(1) = x$ かつ $f_x(0) = \bot_X$ で定義すると, f_x は計算可能である.

これを確かめるためには, f の具現化 $\mathtt{f} : \mathbb{N} \to \mathbb{N}$ が計算可能であることを示せばよい. この $\mathtt{f}$ は次の性質を満たすはずである. 入力 $e \in \mathbb{N}$ に対して, もし $[\![e]\!](0)$ が停止するならば x の $X_\bot$-コードを出力し, 停止しないならば $\bot_X$ の $X_\bot$-コードを出力する.

プログラム P_e を, どんな入力が与えられても, $[\![e]\!](0)$ が停止するのを待ってから x のコードを出力するものとしよう. 入力 $e \in N$ に対して, プログラム P_e のコード $\mathtt{f}(e)$ を返す関数 $\mathtt{f}$ は容易に計算可能である. このとき, 特に

$$[e]_{\mathbb{S}} = 1 \iff [\![e]\!](0)\downarrow \iff [\![\mathtt{f}(e)]\!](0)\downarrow \in ||x||_X \iff |[\![\mathtt{f}(e)]\!](0)|_X = x \iff [\mathtt{f}(e)]_{X_\bot} = x$$
$$[e]_{\mathbb{S}} = 0 \iff [\![e]\!](0)\uparrow \iff [\![\mathtt{f}(e)]\!](0)\uparrow \iff [\mathtt{f}(e)]_{X_\bot} = \bot_X$$

であるから, $\mathtt{f}$ は f_x の計算可能な具現化となっている. ⊣ (主張)

主張. 任意の計算可能開集合 $U \subseteq X$ について,

$$r_X(\bot_X) \in U \implies U = X.$$

$r_X : X_\bot \to X$ を計算可能レトラクトとする. このとき, $r_X(\bot_X) \in U \neq X$ なる計算可能開集合 U が存在すると仮定して矛盾を導こう. まず, $x \in X \backslash U$ を取る. このとき, $r_x^{-1}[U] = U \cup \{\bot_X\}$ である. いま, $h = r_X \circ f_x$ とすると, $h^{-1}[U] = \{0\}$ である. 前の主張より, $h : \mathbb{S} \to X$ は計算可能である. U は X の計算可能開集合であるから, 命題 1.24 より, $h^{-1}[U] = \{0\}$ も $\mathbb{S}$ の計算可能開集合である. しかし, 例 1.23 で見たように, $\{0\}$ は $\mathbb{S}$ の計算可能開集合ではありえない. したがって, 任意の計算可能開集合 U について, $r_X(\bot_X) \in U \neq X$ では有り得なかった, つまり $r_X(\bot_X) \in U$ ならば $U = X$ だったということである. ⊣ (主張)

さて, 計算可能開集合 $X_0, X_1 \subseteq X$ について, もし $X = X_0 \cup X_1$ ならば, $r_X(\bot_X) \in X_0$ または $r_X(\bot_X) \in X_1$ である. よって, 上の主張により, $X_0 = X$ または $X_1 = X$ を得る. 以上より, X の計算連結性が示された. □

系 1.35 (ライスの定理)**.** 部分計算可能関数の計算可能な添字集合は自明なものだけである. つまり, $P \subseteq [\mathbb{N} \to \mathbb{N}_\bot]$ が $P \neq \varnothing$ または $P \neq [\mathbb{N} \to \mathbb{N}_\bot]$ であるものとすれば,

$$\{e \in \mathbb{N} : [\![e]\!] \in P\}$$

は計算不可能である.

Proof. 例 1.32 で見たように，$[\mathbb{N} \to \mathbb{N}_\perp]$ は $\perp$-レトラクトであるから，定理 1.34 より計算連結である．計算連結性は，非自明な添字集合が全て計算不可能であるということと同値であったから，目的の主張は示される． □

ここで，例 1.33 より，自然数上の部分計算可能関数に関する添字集合だけでなく，任意の全域 **N**-表現空間上の部分計算可能関数に関する添字集合に対して，計算可能なものは自明なものしかないことが示される．たとえば，命題 1.21 を用いれば，計算可枚挙集合の空間 CE は関数空間 $[\mathbb{N} \to \mathbb{S}]$ として表すことができるので，CE においてもライスの定理が成立する．

例 1.36. ライスの定理より，以下の集合は全て計算不可能である．

$$\begin{aligned}
\mathsf{Halt}_0 &= \{e \in \mathbb{N} : [\![e]\!](0)\downarrow\},\\
\mathsf{Fin} &= \{e \in \mathbb{N} : W_e \text{ is finite}\},\\
\mathsf{Inf} &= \{e \in \mathbb{N} : W_e \text{ is infinite}\},\\
\mathsf{Tot} &= \{e \in \mathbb{N} : (\forall n \in \mathbb{N})\ [\![e]\!](n)\downarrow\},\\
\mathsf{Cof} &= \{e \in \mathbb{N} : \mathbb{N}\backslash W_e \text{ is finite}\},\\
\mathsf{Rec} &= \{e \in \mathbb{N} : W_e \text{ is computable}\}.
\end{aligned}$$

後に確認するが，これらの添字集合の計算不可能性の度合いについて，以下が成立する．

$$\varnothing' \equiv_T \mathsf{Halt}_0 <_T \varnothing'' \equiv_T \mathsf{Fin} \equiv_T \mathsf{Inf} \equiv_T \mathsf{Tot} <_T \varnothing''' \equiv_T \mathsf{Cof} \equiv_T \mathsf{Rec}.$$

ここで，第??節で定義したように，$\leqslant_T$ はチューリング還元可能性であり，X' は X のチューリング・ジャンプである．つまり，X' は X-相対的計算に関する停止問題 Halt^X を表す．したがって，たとえば，$\varnothing''' = \mathsf{Halt}^{\mathsf{Halt}^{\mathsf{Halt}}}$ である．

注意. 位相空間論を既に学んでいる読者のために補足しておくと，抽象ライスの定理 1.34 の証明は，任意の $\perp$-レトラクトがエルショフ位相の下で（位相空間論の意味で）連結であることを述べている．なぜなら，エルショフ位相の定義より，任意の開集合は計算可能開集合を含むので，定理 1.34 の 2 つめの主張は，$r_X(\perp_X)$ を含む全ての開集合は空間全体に他ならないことを述べている．したがって，特に，ライスの定理 (系 1.35) とは，部分計算可能関数の空間 $[\mathbb{N} \to \mathbb{N}_\perp]$ がエルショフ位相の下で連結であることを主張する定理である．

ところで，唐突に現れた $\perp$-レトラクトというものの出自が気になる人もいるかもしれない．これは，ナンバリングの理論において，1960 年頃にマルツェフによって導入された**完全ナンバリング** (*complete numbering*) または**エルショフ完全ナンバリング** (*Ershov-complete numbering*) と呼ばれるものに相当する．エルショフは，この概念を **N**-表現空間と計算可能関数の圏における単射的対象の類似物として説明している．ここでは，少々，単純化したバージョンを導入しよう．

定義 1.37. 全域 **N**-表現空間 Z が **CE-絶対拡張手** (*CE-absolute extensor*) とは，与えられた全域 **N**-表現空間 X と計算可能開集合 $S \subseteq X$ について，どんな計算可能関数 $f : S \to Z$ も全域計算可能関数 $\tilde{f} : X \to Z$ に拡張できることを意味する．

注意. トポロジーの意味での絶対拡張手は，**閉**部分集合上の連続関数の拡張可能性を考えるため，実際にはかなり異なる概念となることに注意する．

命題 1.38. 全域 **N**-表現空間が CE-絶対拡張手であることと $\perp$-レトラクトであることは同値である．

Proof. 全域 **N**-表現空間 Z が CE-絶対拡張手であるとする．このとき，持ち上げ $Z_\perp$ において $Z \subseteq Z_\perp$ の添字集合は半計算可能集合 $\{e : [\![e]\!](0)\downarrow\}$ であるから，Z は $Z_\perp$ の計算可能開部分集合である．恒等関数 $\mathrm{id} : Z \to Z$ は計算可能であるから，全域計算可能関数 $\tilde{\mathrm{id}} : Z_\perp \to Z$ に拡張される．これは明らかに計算可能レトラクションである．

逆に，Z が $\perp$-レトラクトであるとする．全域 **N**-表現空間 X とその計算可能開部分集合 S が与えられているとする．I_S を S の添字集合とすると，I_S は計算可枚挙であり，つまり半計算可能であるから，次のような計算可能関数 $p : \mathbb{N} \to \mathbb{N}$ が存在する．

$$p(n) = \begin{cases} n & \text{if } n \in I_S, \\ \uparrow & \text{if } n \notin I_S. \end{cases}$$

いま，計算可能関数 $f : S \to Z$ が与えられているとする．このとき $\mathtt{f} :\subseteq \mathbb{N} \to \mathbb{N}$ を f の計算可能な具現化とする．つまり，$n \in I_S$ について $f([n]_X) = [\mathtt{f}(n)]_Z$ を満たすものとする．このとき，$\mathtt{f} \circ p$ は計算可能であるから，そのコードを q とする．つまり，$[\![q]\!](n) \simeq \mathtt{f} \circ p(n)$ である．パラメータ定理より，ある計算可能関数 $t : \mathbb{N} \to \mathbb{N}$ が存在して，$[\![t(n)]\!](0) \simeq \mathtt{f} \circ p(n)$ となる．いま，

$$\begin{aligned} n \in I_S &\implies [\![t(n)]\!](0) \simeq \mathtt{f} \circ p(n) = \mathtt{f}(n)\downarrow \implies [t(n)]_{Z_\perp} = [\mathtt{f}(n)]_Z = f([n]_X) \\ n \notin I_S &\implies [\![t(n)]\!](0) \simeq \mathtt{f} \circ p(n)\uparrow \implies \perp_X \end{aligned}$$

であるから，t は全域計算可能関数 $g : X \to Z_\perp$ で $f \upharpoonright S = g \upharpoonright S$ となるものを具現化する．いま，$r_Z : Z_\perp \to Z$ を計算可能レトラクションとすれば，$\tilde{f} = r_Z \circ g : X \to Z$ は f を拡張する全域計算可能関数である． □

豆知識. 発展的なトピックとして，ライスの定理を強めた定理が幾つかある．1950 年代半ばに証明された**マイヒル-シェファードソンの定理** (*Myhill-Shepherdson theorem*) と**ライス-シャピロの定理** (*Rice-Shapiro theorem*) はよく知られている．$\mathbb{N}$ 上の有限関数 $\theta :\subseteq \mathbb{N} \to \mathbb{N}$ に対して，$[\theta]$ を θ を拡張する部分計算可能関数全体の集合とし，有限集合 $D \subseteq \mathbb{N}$ に対して，$[D]$ を D を含む $\mathbb{N}$ の部分集合全体の集合とする．つまり，

$$[\theta] = \{\psi \in [\mathbb{N} \to \mathbb{N}_\perp] : \theta \subseteq \psi\}, \qquad [D] = \{S \subseteq \mathbb{N} : D \subseteq S\}.$$

マイヒル-シェファードソンの定理は，集合族 $\{\varnothing\} \cup \{[\theta] : \theta\text{は有限関数 }\}$ が $[\mathbb{N} \to \mathbb{N}_\perp]$ 上のエルショフ位相の開基をなすことを述べる定理である．つまり，任意の空でない計算可能開集合 $U \subseteq [\mathbb{N} \to \mathbb{N}_\perp]$ に対して，ある有限関数の族 F が存在して，$U = \bigcup_{\theta \in F}[\theta]$ と書ける．同様に，ライス-シャピロの定理は，集合族 $\{\varnothing\} \cup \{D \subseteq \mathbb{N} : D \text{ は有限集合 }\}$ が CE 上のエルショフ位相の開基をなすことを述べる．つまり，任意の空でない計算可能開集合 $U \subseteq \mathsf{CE}$ に対して，ある有限集合の族 F が存在して，$U = \bigcup_{D \in F}[D]$ と書ける．

1.3 実数の計算論

計算理論の誕生以来，実数上の計算論は計算可能性理論の中心的テーマであり続けた．しかし，もちろん，あらゆる実数を有限文字列として取り扱うということは不可能である．それでは，研究者たちは如何にして実数上の計算論を取り扱ってきただろうか．1 つの解法は，クリーネの第一代数 $\mathbf{N}$ における計算可能実数論であり，もう 1 つの解法は，クリーネの相対第二代数 $\mathbf{K} := (\mathbb{K}_2, \mathbb{K}_{2^{\emptyset}})$ における実数上の計算可能関数論である．実数の計算論の初期は前者のアプローチが主流だったように思うが，時代を経るにつれ，徐々に後者の理論の方が優れていると分かってきた．

この正確な意味を説明する前に，まず，実数の計算論の具体的なアイデアを述べよう．まず，有理数上の計算論は，例 1.7 のような有理数の表現を用いて自明に展開できる．実数の計算可能性を導入する最も簡単だが最も優れた方法は，任意精度計算（精度保証計算）である．

定義 1.39. 実数 $x \in \mathbb{R}$ が**任意精度計算可能**とは，任意の正有理数 ε 精度で x を有理近似するアルゴリズムが存在することである．つまり，ある計算可能関数 $\Phi : \mathbb{Q}_{>0} \to \mathbb{Q}$ が存在して，次を満たすことである．

$$(\forall \varepsilon \in \mathbb{Q}_{>0}) \quad |x - \Phi(\varepsilon)| < \varepsilon.$$

とりあえず，これが実数の計算可能性の妥当な定義のように思うが，少しだけ歴史的経緯を振り返ろう．チューリングが 1936 年にチューリング機械を導入した記念碑的論文「計算可能数とその決定問題への応用」では，実数の計算可能性は 2 進小数展開の計算可能性として導入されている．ここでは，その計算可能性を 2 進計算可能性と呼ぶことにする．

定義 1.40. 実数 $x \in \mathbb{R}$ が 2 **進計算可能** (*binary computable*) とは，x の任意の 2 進小数展開

$$a_0 a_1 \dots a_n . a_{n+1} a_{n+2} \dots a_{n+k} a_{n+k+1} \dots$$

に対して，関数 $i \mapsto a_i$ が計算可能であることを意味する．

しかし，すぐにチューリングは，実数の計算論を 2 進展開で導入するのは誤りだと気づいたようである．翌年にチューリングは「計算可能数とその決定問題への応用 – 訂正」を出版し，その後半部では，自身の実数の 2 進計算論を撤回した．実数の計算論の正しい与え方として，チューリングは，たとえばブラウワーの直観主義数学における縮小区間による実数の表現を挙げている．これは区間の縮小列によって実数を表現するものである．

定義 1.41. 実数 $x \in \mathbb{R}$ が**区間計算可能**とは，有理数の対の計算可能な列 $(p_n, q_n)_{n\in\mathbb{N}}$ で次のようなものが存在することである．

$$(\forall n \in \mathbb{N})\ [p_n < p_{n+1} < q_{n+1} < q_n], \text{ and } x = \lim_{n\to\infty} p_n = \lim_{n\to\infty} q_n.$$

任意精度計算との関連性に触れておくと，区間計算において，ストリーム $(p_n, q_n)_{n\in\mathbb{N}}$ の各段階

では実数を両側から挟み込んでいるため，常に近似精度の保証が可能となっている．実際，以下のように，チャーチ・チューリングの提唱の実数の計算論版のようなものも成立する．

命題 1.42. 実数について，任意精度計算可能性，2 進計算可能性，区間計算可能性はいずれも同値である．

Proof. 任意精度計算可能性と区間計算可能性の同値性は読者の演習問題とする．任意の 2 進計算可能実数が任意精度計算可能であることを確認しよう．実数の与えられた無限 2 進小数表記 $\alpha = a_0a_1 \dots a_k.a_{k+1}a_{k+2} \dots$ に対して，q_n を有限小数 $a_0a_1 \dots a_k.a_{k+1}a_{k+2} \dots a_{k+n}a_{k+n+1}$ が表す有理数とする．このとき，$q = (q_n)_{n\in\omega}$ が $[\alpha]_{\mathrm{bin}}$ の任意精度近似，つまり $[q]_A = [\alpha]_{\mathrm{bin}}$ であることは容易に分かる．

最後に，任意精度計算可能実数が 2 進計算可能実数であることを示す．有理数がどちらの意味でも計算可能であることは明らかなので，無理数 x について任意精度計算可能性が 2 進計算可能性を導くことを示せばよい．また，$x \in [0, 1]$ であると仮定しても一般性を失わない．x を任意精度計算可能な無理数とし，Φ をその任意精度近似とする．x は無理数であるから，2 進小数展開した際に，必ず 0 と 1 の両方を無限に含む．有理数 $\Phi(s)$ を 2 進小数展開した結果を $\alpha_s = 0.a^s_0a^s_1 \dots a^s_{\ell(s)}$ と書く．任意の $n \in \mathbb{N}$ について，α_s の小数点以下 $n + 1$ 桁目以降 s 桁目以前に 01 または 10 が出現するような s を探す．このとき，$\Phi(s)$ から最大 2^{-s} の誤差が発生したとしても，この 01 または 10 の出現以前の部分は変動しない．よって，$a_n = a^s_n$ と定義すれば，$[0.a_1a_2 \dots]_{\mathrm{bin}} = \lim_s \Phi(s) = x$ を得る． □

ところで，チューリングの最初の定義である「2 進計算可能性」とチューリングの第 2 の定義である「区間計算可能性」が同値であるならば，チューリングは訂正論文を出す必要は無かったのでは，と思うかもしれない．しかし，実は，チューリングが訂正論文を出した判断は正しかった．実関数の計算可能性を考える段階になると「2 進計算可能性」と「区間計算可能性」は大きく異なる．そして，そのとき「2 進計算可能性」は破綻する．なんと，実数を 3 倍するだけのごく単純な関数 $x \mapsto 3x$ ですら，2 進計算可能ではないのである．これについては，後の定理 1.45 で確認する．

このような問題を説明する前に，実数の表現について考えよう．そもそも実数の定義とは何であっただろうか．実数の集合 $\mathbb{R}$ とは，有理数の集合 $\mathbb{Q}$ の完備化，すなわちコーシー列の同値類であると学んだかもしれない．あるいは，実数とは，デデキント切断であると学んだかもしれない．

■コーシー実数: 有理**コーシー列** (*Cauchy sequence*) とは有理数列 $(q_n)_{n\in\omega} \in \mathbb{Q}^{\mathbb{N}}$ で，

$$(\forall n > 0)(\exists k \in \mathbb{N})(\forall i, j \geqslant k)\ |q_i - q_j| < 2^{-n}$$

を満たすものである．有理コーシー列 $(p_n)_{n\in\omega}$ と $(q_n)_{n\in\omega}$ が等しいとは，任意の $\varepsilon > 0$ について，十分大きな任意の $i, j \in \mathbb{N}$ について $|p_i - q_j| < \varepsilon$ が成立することである．実数の集合 $\mathbb{R}$ の**素朴コーシー表現** (*naive Cauchy representation*) とは，有理コーシー列の同値類として実数を表現す

る関数 $[\cdot]_{\mathrm{nC}} :\subseteq \mathbb{Q}^{\mathbb{N}} \to \mathbb{R}$ である．より正確には，任意の有理コーシー列 $(q_n)_{n\in\omega}$ について，

$$[(q_n)_{n\in\omega}]_{\mathrm{nC}} = \{(p_n)_{n\in\omega} : (p_n) \text{ は有理コーシー列であり，} (p_n) \text{ と } (q_n) \text{ は等しい.}\}$$

同値類 $[(q_n)_{n\in\omega}]_{\mathrm{nC}}$ のことを $\lim_{n\to\infty} q_n$ と表す．素朴コーシー表現は非常に使い勝手が悪い．本節で言及する実数の表現のうちでは最悪な表現である．コーシー列の収束速度が分からないので，コーシー列というストリームを読み込む過程で，極限の値にどれくらい近づいたか判断できないからである．素朴コーシー表現は極限概念を伴う表現であり，第**??**節で詳述するが，極限は容易に計算不可能性を生み出すのである．

そういうわけで，コーシー列と言った場合には，収束速度の情報が常に備わっていて欲しい．関数 $k : \mathbb{N} \to \mathbb{N}$ が列 $(q_n)_{n\in\omega}$ の**収束係数**とは，

$$(\forall n > 0)(\forall i, j \geqslant k(n))\ |q_i - q_j| < 2^{-n}$$

を満たすことを意味する．実数の集合 $\mathbb{R}$ の**係数付きコーシー表現**とは，有理コーシー列の正しい収束係数が与えられたとき，その有理コーシー列の同値類として実数を表現する関数 $[\cdot]_{\mathrm{mC}} :\subseteq \mathbb{Q}^{\mathbb{N}} \times \mathbb{N}^{\mathbb{N}} \to \mathbb{R}$ である．つまり，任意の有理コーシー列 $(q_n)_{n\in\omega}$ について，もし k が $(q_n)_{n\in\omega}$ の収束係数であるときのみ，$[(q_n), k]_{\mathrm{mC}}$ を定義し，$[(q_n), k]_{\mathrm{mC}} = \lim_{n\to\infty} q_n$ とする．

係数付きコーシー表現は非常に良い表現なのだが，定義が若干ごちゃごちゃするという難点がある．このため，係数付きコーシー表現の代わりに，id が収束係数となるようなコーシー列（急収束コーシー列）だけを考えて単純化することが多い．つまり，**急収束コーシー列** (*rapidly converging Cauchy sequence*) とは有理数列 $(q_n)_{n\in\omega} \in \mathbb{Q}^{\mathbb{N}}$ で，

$$(\forall n > 0)(\forall i, j \geqslant n)\ |q_i - q_j| < 2^{-n}$$

を満たすものである．このとき，実数の集合 $\mathbb{R}$ の**コーシー表現** (*Cauchy representation*) とは，急収束コーシー列の同値類として実数を表現する関数 $[\cdot]_{\mathrm{C}} :\subseteq \mathbb{Q}^{\mathbb{N}} \to \mathbb{R}$ である．つまり，$(q_n)_{n\in\omega}$ が急収束コーシー列であるときのみ，$[(q_n)]_{\mathrm{C}}$ を定義し，$[(q_n)]_{\mathrm{C}} = \lim_{n\to\infty} q_n$ とする．

■デデキント実数: 有理数の集合 $A \subseteq \mathbb{Q}$ が下方閉とは，任意の $a \in A$ と有理数 $q \leqslant a$ について $q \in A$ となることである．同様に，A が上方閉とは，任意の $a \in A$ と有理数 $q \geqslant a$ について $q \in A$ となることである．**デデキント切断** (*Dedekind cut*) とは，有理数の空でない集合の対 $L, R \subseteq \mathbb{Q}$ で，L は上方閉，R は下方閉，$L \cap R = \varnothing$ かつ $|\mathbb{Q}\backslash(L \cup R)| \leqslant 1$ となることである．この L の開部分として，$L^\circ = \{r \in \mathbb{Q} : (\exists s \in L)\ r < s\}$ と定義する．デデキント切断 (L_0, R_0) と (L_1, R_1) が等しいとは，$L_0^\circ = L_1^\circ$ となることである．

実数の集合 $\mathbb{R}$ の**デデキント表現** (*Dedekind representation*) とは，デデキント切断の枚挙の同値類として実数を表現する関数 $[\cdot]_D :\subseteq (\mathbb{Q} \times \mathbb{Q})^{\mathbb{N}} \to \mathbb{R}$ である．より正確にこの表現を定義するため，$p = (p_n)_{n\in\mathbb{N}}$ と $q = (q_n)_{n\in\mathbb{N}}$ について，p と q がそれぞれ集合 A と B の枚挙であるとき，(p, q) を (A, B) の枚挙と呼び，$\mathrm{Rng}(p, q) = (A, B)$ と書く．このとき，デデキント切断の枚挙 (p, q) に対して，同値類 $[(p, q)]_D$ を以下によって定義する．

$$[(p, q)]_D = \{(r, s) : \mathrm{Rng}(r, s) \text{ は } \mathrm{Rng}(p, q) \text{ と等しいデデキント切断である.}\}$$

(p,q) がデデキント切断 (L,R) の枚挙であるとき，$[(p,q)]_D$ のことを $\sup L$ または $\inf R$ と書く．デテキント切断を用いた表現として，他にも開デデキント表現や決定可能デデキント表現などが知られているが，いずれも計算論を展開する際にはあまり有用でないので，ここでは触れない．

豆知識．ところで，デデキント表現の等しさの定義では，L についての情報しか用いていない．このため，切断の定義は単に L だけ考えればよいのではないか，と思う人もいるかもしれない．そのような表現は**左デデキント表現**などと呼ばれるが，ユークリッド直線 $\mathbb{R}$ の表現としては正しくない．左右からしっかり挟み込まないと，実数の近似精度が評価できないため，位相的に全く異なった概念になってしまう．しかし，$\mathbb{R}$ 上のユークリッド位相の表現として正しくないだけで，$\mathbb{R}$ 上の**上半位相** (*upper topology*) と呼ばれる非 T_1 位相の表現としては正しい．これは $\{0,1\}$ を離散的なオブジェクトとして見るときはシエルピンスキ表現は誤りだが，$\{0,1\}$ を連結空間として見るときはシエルピンスキ表現が正しい，という状況と同様である．

コーシー表現では，実数は有理数のストリームとして表される．デデキント表現では，実数は有理数の対のストリームとして表される．したがって，実数の計算論を展開するための適切な舞台は，ストリーム上の計算論，つまりクリーネの相対第二代数 $\mathbf{K}$ 上の計算論 $\mathsf{Mod}(\mathbf{K})$ である．

このアイデアを用いて，任意精度表現，2 進小数表現，縮小区間表現を，実数のストリーム表現として再定義しよう．

- 2 進小数表現 $[\cdot]_{\mathrm{bin}}$ は，$\{0,1,.\}$ の記号のストリーム α で小数点記号 . が高々 1 つしか含まないものについて，$[\alpha]_{\mathrm{bin}}$ を実数の 2 進表記であると理解する表現である．
- 縮小区間表現 $[\cdot]_I$ は，$\lim_{n\to\infty}(q_n - p_n) = 0$ となるような有理数の対のストリーム $(p,q) = (p_n,q_n)_{n\in\mathbb{N}}$ が与えられたとき，$[(p,q)]_I = \lim_{n\to\infty} p_n$ を与える関数である．
- 任意精度表現 $[\cdot]_A$ は, 与えられた有理数のストリーム $(\Phi(n))_{n\in\mathbb{N}}$ について, $|x-\Phi(n)| < 2^{-n}$ なるような実数 x が存在するとき，そのような x を返す関数である．

ここで,「実数の計算可能性」を定義することと「実数の表現」を与えることの理論的な違い，そして前者よりも後者の方が重要である理屈を説明しよう．まず,「実数の計算可能性」という概念を定義しても,「実関数の計算可能性」はまた個別に定義する必要がある．しかし,「実数の表現」を与えると，そこから「実数の計算可能性」と「実関数の計算可能性」が自動的に定義される．これについて説明しよう．実数の表現を与えた，という事実は，いま $\mathbb{R}$ に $\mathbf{K}$-表現空間としての構造が与えられた，ということである．表現空間上の関数の計算可能性は定義 1.4 で与えた通りである．表現空間の点の計算可能性は以下によって与えられる．

定義 1.43. $(\mathbf{A},\mathbf{A}_\emptyset)$ を相対部分組合せ代数とする．$\mathbf{A}$-表現空間 X の点 $x\in X$ が**計算可能** (*computable*) であるとは，$x = [a]_X$ となる $a\in\mathbf{A}_\emptyset$ が存在することを意味する．

例 1.44. クリーネの相対第二代数 $\mathbf{K}$ において，$\mathbf{K}$ はストリーム全体の集合 $\mathbb{N}^{\mathbb{N}}$ であり，$\mathbf{K}_\emptyset$ は計算可能ストリーム全体の集合，つまり $\mathbb{N}$ 上の計算可能関数全体の集合であった．このとき，$\mathbf{K}$-表現空間 X の点 $x\in X$ が計算可能であるとは，x が計算可能な名を持つことを意味する．

また，実数や実関数の計算可能性だけでなく，たとえば「$\mathbb{R}$ の開部分集合の計算可能性」「$\mathbb{R}$ のコンパクト部分集合の計算可能性」などを含む無数の計算可能性概念も自動的に定義される．このように「表現」を与えるだけで，豊穣な計算可能性理論の世界が自動的に広がっていくのである．

実数の計算論は実数の表現に依存する．したがって，実数のどの表現が同値であり，どの表現が異なる計算論を与えるか，ということは計算可能解析学の初期における問題の 1 つであった．つまり，与えられた実数の計算論が異なる実数の計算論に翻訳可能かどうか，というナンバリングの理論と同様のシチュエーションに辿り着く．ナンバリングの理論のときと同様に，この問題は定義 1.16 で用いた表現の還元可能性の概念を用いて定式化できる．

定理 1.45. 任意精度表現，区間表現，コーシー表現，デデキント表現は同値である．一方，2 進小数表現および素朴コーシー表現は異なる表現であり，以下が成立する．

$$[\cdot]_{\mathrm{bin}} < [\cdot]_A \equiv [\cdot]_I \equiv [\cdot]_C \equiv [\cdot]_D < [\cdot]_{nC}.$$

Proof. $[\cdot]_{\mathrm{bin}} \leqslant [\cdot]_A$ であることは，命題 1.42 の証明において，$[\alpha]_{\mathrm{bin}} = [q]_A$ となることを示したが，$\alpha \mapsto q$ が計算可能であるから，これが $[\cdot]_{\mathrm{bin}} \leqslant [\cdot]_A$ を保証する．$[\cdot]_C \leqslant [\cdot]_{nC}$ は自明である．$[\cdot]_A \equiv [\cdot]_C$ は明らかであろう．$[\cdot]_D \leqslant [\cdot]_I$ について，与えられたデデキント切断の枚挙 $(\ell_n, r_n)_{n\in\mathbb{N}}$ に対して，各 n について $p_n = \max_{s<n} \ell_s$ かつ $q_n = \max_{s<n} r_s$ とすれば，$(p_n, q_n)_{n\in\omega}$ は区間の縮小列であり，自明に $\sup_n \ell_n = \lim_n p_n$ かつ $\inf_n r_n = \lim_n q_n$ であるから，同じ実数を与える．よって，計算可能関数 $(\ell_n, r_n)_{n\in\mathbb{N}} \mapsto (p_n, q_n)_{n\in\omega}$ によって $[\cdot]_D \leqslant [\cdot]_I$ は保証される．$[\cdot]_D \leqslant [\cdot]_I$ も容易に示せる．$[\cdot]_A \leqslant [\cdot]_I$ について，実数の任意精度近似 Φ に対して，区間 $(\Phi(n) - 2^{-n+1}, \Phi(n) + 2^{-n+1})$ を考えればよい．$[\cdot]_I \leqslant [\cdot]_A$ について，区間縮小列 $(p_n, q_n)_{n\in\mathbb{N}}$ が与えられたとき，各 n に対して $q_s - p_s < 2^{-n}$ なる $s \in \mathbb{N}$ を探し，$\Phi(n)$ をその区間 (p_s, q_s) の中点，つまり $\Phi(n) = (q_s - p_s)/2$ と定義すればよい．

次に $[\cdot]_{nC} \not\leqslant [\cdot]_A$ を示そう．H_s を停止問題の時刻 s 近似，つまり $H_s = \{e < s : [\![e]\!](e)[s] \downarrow\}$ とする．このとき $q_s = \sum_{e\in H_s} 2^{-e}$ と定義すると，$(q_s)_{s\in\mathbb{N}}$ は計算可能なコーシー列である．特に，その極限 $x = \lim_{s\to\infty} q_s$ は，素朴コーシー表現において計算可能である．しかし，x の 2 進表記を見ると，明らかに停止問題 Halt の情報を記している．停止問題の計算不可能性より，これは x が $(\mathbb{R}, [\cdot]_{\mathrm{bin}})$ で計算不可能であることを意味する．一方，命題 1.42 より，x は任意精度表現でも計算不可能である．よって，$[\cdot]_{nC} \not\equiv [\cdot]_A$ を得る．既に $[\cdot]_A \leqslant [\cdot]_{nC}$ は示してあるから，$[\cdot]_{nC} \not\leqslant [\cdot]_A$ である．

最後に，$[\cdot]_A \not\leqslant [\cdot]_{\mathrm{bin}}$ を示す．$\mathbb{R}_{\mathrm{bin}}$ を表現空間 $(\mathbb{R}, [\cdot]_{\mathrm{bin}})$ とすると，$f(x) = 3x$ で定義された関数 $f : \mathbb{R}_{\mathrm{bin}} \to \mathbb{R}_{\mathrm{bin}}$ が計算不可能であることを示す．他の表現の場合は，$x \mapsto 3x$ は容易に計算可能であることが分かるので，これが 2 進小数表現と他の表現の違いを導く．もし $f(x) = 3x$ が 2 進小数表現の元で計算可能だったとする．$1/3$ を 2 進小数展開すると $0.01010101\ldots$ という循環小数になることに注意する．f を実現するチューリング機械 M が，入力ストリーム $0.01010101\ldots$

を読み込んでいるとしよう．このとき，M は必ずある時点でストリームを出力し始めなければならない．入力ストリームの n 桁目を読み込んだ段階で，M がある文字 k を出力したとしよう．M は $x \mapsto 3x$ を計算しているはずなので，$k = 1$ であるか $k = 0$ であり，その後に小数点とそれ以下の値が続くはずである．もし $k = 1$ だったとしたら，入力ストリームの $n + 1$ 桁以降が何であろうと，M は 1 以上の実数を記述する．しかし，$n + 1$ 桁目以降ずっと 0 を返すストリーム α を考えると，$[\alpha]_{\mathrm{bin}} < 1/3$ であるから，$f([\alpha]_{\mathrm{bin}}) < 1 \leqslant [[\![M]\!](\alpha)]_{\mathrm{bin}}$ となり，M は f を正しく計算できていない．もし $k = 0$ だったとしたら，入力ストリームの $n + 1$ 桁以降が何であろうと，M は 1 以下の実数を記述する．しかし，$n + 1$ 桁目以降ずっと 1 を返すストリーム α を考えると，$[\alpha]_{\mathrm{bin}} > 1/3$ であるから，$f([\alpha]_{\mathrm{bin}}) > 1 \geqslant [[\![M]\!](\alpha)]_{\mathrm{bin}}$ となり，M は f を正しく計算できていない．よって，$x \mapsto 3x$ が 2 進小数表現の下では計算不可能であることが示された．以上より，$[\cdot]_{\mathrm{bin}}$ が他の表現と同値でないことが示されるが，既に $\leqslant [\cdot]_{\mathrm{bin}} \leqslant [\cdot]_A$ は示してあるから，$[\cdot]_A \not\leqslant [\cdot]_{\mathrm{bin}}$ を得る． □

この定理の興味深いところは，悪い表現，というものにも複数の方向性があり，表現の還元可能性概念がそれを明示してくれる点にある．つまり 2 進小数表現は，要求が厳しすぎる表現であり，素朴コーシー表現は，要求が甘すぎる表現であると言える．

豆知識．本節で述べた実数の計算モデルは，**厳格実数計算** (*exact real computation*), **誤差なし実数計算** (*error-free real computation*), あるいは**任意精度計算**などとも呼ばれる．最近は，幾つかのプログラミング言語で厳格実数計算用のライブラリが少しずつ充実しつつあるようだ．

豆知識．実数の計算論には，かつては他にも BSS 機械 (Blum-Shub-Smale machine) という計算モデルなどがあった．厳格実数計算モデルが「位相空間論的」実数の計算論と考えられるのに対し，BSS モデルは「モデル理論的」実数の計算論と思える．しかし，計算論として取り扱うとなると，BSS モデルは若干微妙なところがある．たとえば，厳格実数計算とは異なり，BSS 計算は現実のコンピュータで実装できない，実数の位相構造と相性が悪い，数学的にも美しさが足りない，などが代表的な問題点である．このため，BSS 機械は，現在ではあまり良い計算モデルとは考えられなくなってしまった．

1.4 ベール表現空間の理論 *

任意の部分組合せ代数 $\mathbf{A}$ に対して，$\mathbf{A}$-表現空間の概念を考えることができるが，近年において，最も主流な研究対象は $\mathbf{A}$ がクリーネの（相対）第二代数 $\mathbf{K}$ の場合である．クリーネの第二代数 $\mathbf{K}$ の表現空間論 $\mathsf{Mod}(\mathbf{K})$ における重要な問題は，どのような空間が良い意味で表現できるか，という問題である．たとえば，可分距離空間の計算可能性理論は極めて長い歴史を持つ．

可分距離空間であれば，第**??**節で学んだ計算可能性理論を適用可能であることは容易に分かるだろう．具体的には，可分距離空間 X の距離関数 d と可算稠密部分集合 $Q \subseteq X$ を用いて，コーシー表現を用いるなどがひとつの方法である．コーシー表現は，多くの場合に上手く行くが，しばしばより良い表現が必要になる場合もある．したがって，次の記述集合論的概念を用いた表現を考えよう．

定義 1.46. 空間 X 上の**ススリン・スキーム** (*Suslin scheme*) は $\mathbb{N}^*$ で添字付けられた集合族 $\mathcal{S} = (S_\sigma)_{\sigma\in\mathbb{N}^*}$ を表す．距離空間 X 上のススリン・スキーム $\mathcal{S}$ が**直径消失** (*vanishing diameter*) とは, 任意の $x \in \mathbb{N}^{\mathbb{N}}$ について $\lim_{n\to\infty} \operatorname{diam}(S_{x\restriction n}) = 0$ となることである．また, $\operatorname{diam}(S_{x\restriction n}) \leqslant 2^{-n}$ であれば，**急消失**であると呼ぶ．距離空間 X の**ススリン・スキーム表現**は，以下を満たす急消失ススリン・スキーム $\mathcal{S} = (S_\sigma)_{\sigma\in\mathbb{N}^*}$ である．

1. $S_\varepsilon = X$ かつ任意の $\sigma \in \mathbb{N}^*$ について S_σ は空でない開集合である．
2. 任意の $\sigma \in \mathbb{N}^*$ について，$\operatorname{cl}(S_{\sigma^\frown n}) \subseteq S_\sigma = \bigcup_n S_{\sigma^\frown n}$ である．

補題 1.47. 任意の可分距離空間はススリン・スキーム表現を持つ.

Proof. a_e を e 番目の有理点，q_n を n 番目の有理数とする．$I_\sigma = \{\langle e,k\rangle : \overline{B}(a_e;q_k) \subseteq S_\sigma \text{ and } q_k \leqslant 2^{-n-1}\}$ とし，$(e(n),k(n))$ を I_σ の n 番目の要素とする．このとき，$S_{\sigma^\frown n} = B(a_{e(n)};q_{k(n)})$ と定義する．まず $\operatorname{cl}(S_{\sigma^\frown n}) \subseteq \overline{B}(a_e;q_k) \subseteq S_\sigma$ である．任意の $x \in S_\sigma$ に対して，S_σ は開集合であるから，X の正則性より，ある $\varepsilon > 0$ が存在して，$\overline{B}(x;\varepsilon) \subseteq S_\sigma$ となる．ある $e,k \in \mathbb{N}$ について，$|x - a_e| < q_k \leqslant \varepsilon/2$ となるので，$B(a_e;q_k) \subseteq B(x;\varepsilon)$ であるから，$(e_n,k_n) = (e,k)$ なる n を取れば，$x \in S_{\sigma^\frown n}$ を得る．よって，$S_\sigma = \bigcup_n S_{\sigma^\frown n}$ である． □

距離空間 X のススリン・スキーム表現 $\mathcal{S}$ は，自明に $\mathbf{K}$-表現を誘導する．具体的には，$x \in \mathbb{N}^{\mathbb{N}}$ に対して，$\bigcap_{n\in\mathbb{N}} S_{x\restriction n}$ が空でないなら，$\nu^{\mathcal{S}}(x)$ をその唯一の元として定義する．ススリン・スキームの誘導する $\mathbf{K}$-表現 $\nu^{\mathcal{S}} :\subseteq \mathbb{N}^{\mathbb{N}} \to X$ の優れた点は，まず連続かつ**開写像** (*open map*) であるという点である．続いて，もし X が完備可分距離空間ならば，$\nu^{\mathcal{S}}$ が全域 $\mathbf{K}$-表現である．この 3 つの全域開連続性は位相的性質であるから，これは任意のポーランド空間の全域連続開 $\mathbf{K}$-表現を与えるということである．ここで，位相空間が**ポーランド空間** (*Polish space*) であるとは，完備可分距離化可能であることを意味する.

マシュー・デ・ブレクト (Matthew de Brecht) は，距離化不可能空間でも同様の表現を持ち得ることに気づいた．デ・ブレクトは**擬ポーランド空間** (*quasi-Polish space*) の概念を導入した．擬ポーランド空間とは，スミス完備擬距離化可能 (Smyth-completely quasi-metrizable) な第二可算空間である．任意のポーランド空間は擬ポーランド空間であるが，ポーランド空間でない自然な擬ポーランド空間が無数にあることが知られている．擬ポーランド空間は一般には距離化不可能でないどころか T_1-分離公理さえ満たさない．デ・ブレクトは，擬ポーランド空間の記述集合論を創始し，以下の特徴付けを与えた.

定理 1.48 (デ・ブレクトの定理)**.** 位相空間が擬ポーランド空間であることと全域開連続 $\mathbf{K}$-表現を持つことは同値である.

さて，全域開連続 **K**-表現が良い表現であることは疑いようがないが，どのような表現であれば位相空間の良い表現であるといえるだろうか．我々は良い「**位相計算構造**」を求めている．位相群であれば基本的な群演算が連続であるように，位相計算構造において基本的な計算は連続であるべきだろう．つまり，圏 $\mathsf{Mod}(\mathbf{K})$ における射と位相空間における何らかの連続性に対応があってしかるべきである．

これに対する当初の解答は，第二可算 T_0 空間に焦点を絞って考えられていた．第二可算 T_0 空間の近傍フィルター表現を考えると，十分に良い性質を持つ．したがって，任意の第二可算 T_0 空間に関する計算可能性理論が容易に展開できることは分かっていた．しかし，第二可算空間への制限は計算理論に対する強すぎる縛りだということが次第に判明する．

これは高階計算論の文脈でより明確になる．1950 年代にクリーネは高階関数空間の計算論を展開するために，**アソシエイト** (*associate*) の概念を導入した．クリーネは**主アソシエイト** (*principal associate*) というものも考えたが，これは高階関数空間においても原始的概念を開集合のように扱おうとするものであった．しかし，これは上手く行かないことが分かり，主アソシエイトの概念はすぐに放棄された．現代的な観点から，クリーネのアプローチを述べると，主アソシエイトは高階関数空間に可算開基を無理に導入し，第二可算空間のように扱おうとする試みであった．一方，アソシエイトの概念は，原始的概念が開集合であると考えることを諦め，ジェネラル・トポロジーの言葉を借りれば，ある種の「可算ネットワーク」を導入する考え方である．

このような第二可算公理を満たし得ない空間に対する計算可能性理論の展開のために，マティアス・シュレーダー (Matthias Schröder) は認容表現の概念を導入した．

定義 1.49. 位相空間 X の**認容表現** (*admissible representation*) とは，連続 **K**-表現 $\nu :\subseteq \mathbb{N}^{\mathbb{N}} \to X$ であり，次の普遍性を持つものである．任意の連続関数 $\delta :\subseteq \mathbb{N}^{\mathbb{N}} \to X$ に対して，ある $\tau :\subseteq \mathbb{N}^{\mathbb{N}} \to \mathbb{N}^{\mathbb{N}}$ が存在して，$\delta = \nu \circ \tau$ を満たす．

ススリン・スキームの誘導する表現は認容表現であることを示すことができる．したがって，擬ポーランド空間であることと全域開連続認容表現を持つことは同値である．事実，デ・ブレクトは全域認容表現を持つだけで擬ポーランド性が導かれることを示した．

それでは，どのような空間が全域とは限らない認容表現を持ち得るだろうか．ところでジェネラル・トポロジーにおいて，1959 年にアレクサンダー・アルハンゲルスキ (Alexander Arhangel'skii) は，**開基** (*open basis*) の概念を一般化する**ネットワーク** (*network*) の概念を提唱した．可算ネットワークを持つ正則 T_1 空間は，**コズミック空間** (*cosmic space*) の名の下で深く研究されている．コズミック空間という名称は言葉遊びであって，宇宙空間とはあまり関係ない．名前の由来は，コズミック空間は可分距離空間の連続像となるからである．

1960 年代以降になると，k**-ネットワーク** (k-*network*) や**収束列ネットワーク** (*cs-network*) などの変種が研究されるようになった．可算 k-ネットワークを持つ正則 T_1 空間は，$\aleph_0$**-空間** ($\aleph_0$-*space*) と呼ばれる．正則 T_1 空間が可算 k-ネットワークを持つことと可算収束列ネットワークを持つことは同値であることは知られている．

シュレーダーは，認容表現空間の基本定理とも呼べる以下の結果を示した．

表 1　様々な位相空間の関係

コズミック空間		
⇑		
$\aleph_0$ 空間	$\Longrightarrow$	認容表現空間
⇑		⇑
可分距離化可能空間	$\Longrightarrow$	第二可算 T_0 空間
⇑		⇑
ポーランド空間	$\Longrightarrow$	擬ポーランド空間

定理 1.50 (シュレーダーの定理)**.** T_0 空間 X について，以下は同値である．

1. X は認容表現を持つ．
2. X は可算収束列ネットワークを持つ．
3. X は可分距離空間の商空間となる．

したがって，現代的な計算可能性理論においては，開基よりもある種のネットワークを原始的な概念として取り扱う方が自然である．シュレーダーの定理の重要な点は，T_1-性や正則性などの強い分離公理を仮定していない点である．実際，計算可能性理論に現れる多くの空間は，そのような強い分離公理を満たさない．

豆知識．$\mathbf{K}$-表現空間の理論は，型 2 実効理論 (*type two theory of effectivity*) と呼ばれることもある．しかし，もちろん $\mathsf{Mod}(\mathbf{K})$ はデカルト閉圏をなし，高階関数空間は型 2 実効理論における中心的な研究対象の 1 つである．このため，この理論を「型 2」という名称で呼ぶのは若干，誤解を招く可能性があるように思う．似たような例として，二階算術も同様の誤解を受けることがあるようである．

2　アルゴリズム情報理論

ランダムとは何なのか，ということを理解することは，「ランダムでない」とは何なのか，というのを理解することと同等である．そういうわけで，まずは，ランダムではない列について学んでいこう．以下に挙げるのは，明らかにランダムでないバイナリ列である．

$$\underbrace{00000000000000000000000000\ldots\ldots00000000}_{1\text{ 億桁}},$$
$$\underbrace{01110111011101110111011101110\ldots\ldots01110111}_{1\text{ 億桁}}.$$

上の列は，ただの「0 が 1 億個並ぶ列」であるから，明らかにランダムでない．下の列は，すぐには気付かないかもしれないが，よく見ると，0111 を繰り返しているだけであることが分かる．つまり，下の列とは「0111 が 2500 万回並ぶ列」であるから，ランダムではない．

それでは，これらのランダムでない列が共有する性質とは何であろうか．すぐに思いつくのは，これらの列が**規則的**である，という点であろうか．ランダム性のことを無秩序性や不規則性と呼ぶこともあるし，つまり，**規則性**というものは，ランダム性の対義語と考えられている．

それでは，そもそも規則的なバイナリ列とは何であろうか．その列を記述する法則か数式か論理式のようなものがある，という感じだろうか．ここでは，もう少し漠然と，

規則性とは，そのバイナリ列を「より短い言葉で説明できる」ということである

と考えよう．たとえば，上の例では，長さ 1 億のバイナリ列を「0 が 1 億個並ぶ列」という 8 文字，「0111 が 2500 万回並ぶ列」という 14 文字で説明することができた．もう少し身近な言葉で説明すると，これは，数十メガバイトの容量を持つデータをほんの数十バイトのデータに**圧縮**したということである．

以上をまとめると，非ランダム性とは規則性であり，規則性とは圧縮可能性である．言い換えれば，

$$\text{ランダム性} = \text{不規則性} = \text{圧縮不可能性}$$

ということである．この発想を，もう少し数学的に厳密な形で定式化しよう．

2.1 コルモゴロフ複雑性

先程はバイナリ列と言ったが，これはつまりアルファベット $\{0,1\}$ 上の有限列，つまり $\{0,1\}^*$ の要素のことである．よって，$\{0,1\}^*$ はバイナリ列全体の集合を表す．また，バイナリ列 $\sigma \in \{0,1\}^*$ の長さを $|\sigma|$ によって表す．

それではデータ圧縮の概念を数学的に定式化しよう．ここで考えるのは可逆圧縮であり，不可逆圧縮は考えない．可逆圧縮で重要なのは，解凍アルゴリズムである．圧縮されたデータから元のデータを復元できなければならない．上の例で言えば，「0 が 1 億個並ぶ列」という文字列が，実際に本物の 0 が 1 億個並ぶバイナリ列を意味しているという了解があるから，「0 が 1 億個並ぶバイナリ列は『0 が 1 億個並ぶ列』という文字列で説明された」と言えるのである．

つまり，σ という記述から τ というバイナリ列を実際に生成する方法 M があって初めて，τ は σ によって説明される，τ は σ に圧縮される，のように言うことができる．この M とは，部分計算可能関数 $M :\subseteq \{0,1\}^* \to \{0,1\}^*$ であり，$M(\sigma) = \tau$ のとき，τ は σ に圧縮された，と考える．そうすると，τ は M によってどれくらい小さいデータサイズまで圧縮できるか，の限界値は以下によって与えられる．

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

この数値 $C_M(\tau)$ を τ の**平コルモゴロフ複雑性** (*plain Kolmogorov complexity*) と呼ぶ．もし $C_M(\tau) \geqslant |\tau|$ ならば，τ は決して圧縮できない列であり，したがって，ランダムな列と考えられる．まず，圧縮不可能列が存在することを見てみよう．

命題 2.1. どんな n についても，長さ n のバイナリ列 τ で，$C_M(\tau) \geqslant |\tau|$ を満たすものが存在

する．

Proof. 長さ n 未満のバイナリ列の個数を数えよう．以下，$(\sigma)_2$ によって，σ を数を 2 進表記だと思ったときのその値を表す．たとえば，$(110)_2 = 6$ である．まず、長さ n のバイナリ列の種類はちょうど 2^n 個であることに注意しよう．すると，長さ n 未満のバイナリ列の個数は

$$\sum_{i=0}^{n-1} 2^i = (\underbrace{111\ldots111}_{n\text{ 個}})_2 = (1\underbrace{000\ldots000}_{n\text{ 個}})_2 - 1 = 2^n - 1$$

である．つまり，高々 $2^n - 1$ 個のバイナリ列 τ だけが $C_M(\tau) < n$ となり得る．しかし，長さ n のバイナリ列は 2^n 種類存在するから，長さ n のバイナリ列 τ で $C_M(\tau) \geqslant n$ となるようなものが存在する．つまり，$C_M(\tau) \geqslant |\tau|$ である． □

ところで，上では M は部分計算可能関数だったら何でも良いとしたが，以後は，入力文字列 σ がいつ読み込み終わるか分からないシチュエーションを考えたい．こういう状況では，M は，適当なタイミングで文字列の読み込みが終了したと判断して，出力を返す必要がある．たとえば，入力文字列側が自身のファイルサイズを最初に記述しているとか，あるいは入力文字列の最後にエンドマークが打たれているなどすれば，M はいつ文字列の読み込みが終了したかを判断できるであろう．ここでは，その判断方法は具体的には指定せず，単に，いつ終わるか分からない文字列を入力とする関数，という概念を以下のように定義する．

定義 2.2. 接頭機械 (*prefix-free machine*) とは，次を満たす部分計算可能関数 $M :\subseteq \{0,1\}^* \to \{0,1\}^*$ である．

$$(\forall \sigma, \tau \in \{0,1\}^*)\ [\sigma \prec \tau\ \&\ \sigma \in \mathrm{dom}(M) \implies \tau \notin \mathrm{dom}(M)].$$

つまり，M は何らかの文字列を読み込み中に，ある時点 σ で出力 $M(\sigma)$ を返したならば，その時点で文字列の読み込みは打ち切っており，σ の拡張 τ については M はもはや反応を示さない．

例 2.3. $\Phi :\subseteq \{0,1\}^* \to \{0,1\}^*$ を任意の部分計算可能関数とすると，

$$M(0^{|\sigma|}1\sigma) = \Phi(\sigma)$$

で定義される関数は接頭である．

定義 2.4. 接頭機械 R が**最適** (*optimal*) であるとは，任意の接頭マシン M に対して，次の条件を満たすものである．

$$(\exists c \in \mathbb{N})(\forall \tau \in \{0,1\}^*)\ C_R(\tau) \leqslant C_M(\tau) + c.$$

定理 2.5. 最適接頭機械は存在する．

Proof. 万能チューリング機械の存在より，$\Phi(0^e1\sigma) = [\![e]\!](\sigma)$ となるような部分計算可能関数 $\Phi :\subseteq \{0,1\}^* \to \{0,1\}^*$ が存在する．最適接頭機械 R の方針は以下である．入力 $0^e1\sigma$ に対して，

$(\Phi(0^e1\tau) : \tau \sqsubseteq \sigma \text{ or } \sigma \sqsubseteq \tau)$ を同時にシミュレートし，その中で $\Phi(0^e1\sigma)$ の計算が停止するのが最速であったなら，$R(0^e1\sigma) = \Phi(0^e1\sigma)$ と出力する．より正確には，R を以下のように構成する．

入力 $0^e1\sigma$ に対して，$R(0^e1\sigma)$ の値を決めるために，まず $\Phi(0^e1\sigma)$ をシミュレートする．もし，ある s ステップで $\Phi(0^e1\sigma)$ が出力を返したならば，$s' = \max\{s, |\sigma|\}$ とする．各始切片 $\tau \sqsubset \sigma$ について，$\Phi(0^e1\tau)$ を s' ステップだけ実行し，その間に出力を返すかどうかを確かめる．もし $\Phi(0^e1\tau)$ が出力を返したならば，$R(0^e1\sigma)$ は出力を返さないと宣言する．さもなくば，続いて，各拡張 $\tau \sqsupset \sigma$ で $|\tau| < s$ なるものについて，$\Phi(0^e1\tau)$ を $s' - 1$ ステップだけ実行し，その間に出力を返すかどうかを確かめる．もし $\Phi(0^e1\tau)$ が出力を返したならば，$R(0^e1\sigma)$ は出力を返さないと宣言する．さもなくば，$R(0^e1\sigma)$ は $\Phi(0^e1\sigma)$ を出力する．

いま，d を与えられた接頭機械 M のコードとする．このとき，$\Phi(0^d1\sigma) = M(\sigma)$ であるが，M は接頭機械であるから，与えられた σ について，$(\Phi(0^d1\tau) : \tau \sqsubseteq \sigma \text{ or } \sigma \sqsubseteq \tau)$ のうちで停止する $\Phi(0^d1\tau)$ は高々 1 つしか存在しない．したがって，$M(\sigma)$ が停止するならば，$R(0^d1\sigma)$ は停止し $\Phi(0^d1\sigma) = M(\sigma)$ を出力する．

いま，$C_M(\tau) \leqslant n$ とすると，長さ n 以下のバイナリ列 σ が存在して，$M(\sigma) = \tau$ となる．よって，$R(0^d1\sigma) = \tau$ を得るが，$|0^d1\sigma| \leqslant n + d + 1$ であるから，$C_R(\tau) \leqslant n + d + 1$ である．以上より，$C_R(\tau) \leqslant C_M(\tau) + d + 1$ が得られた． □

M が最適接頭機械であるとき，$C_M(\tau)$ の代わりに $K(\tau)$ と書き，これを**接頭コルモゴロフ複雑性** (*prefix-free Kolmogorov complexity*) と呼ぶ．以下，$\leqslant^+$ によって，高々定数 c 程度の差を除いて，不等式 $\leqslant$ が成立することを意味する．

命題 2.6. $K(\tau) \leqslant^+ 2|\tau|$.

Proof. $M(0^{|\tau|}1\tau) = \tau$ と定義すれば，これは接頭機械であり，$C_M(\tau) \leqslant 2|\tau| + 1$ を得る． □

自然数 $n \in \mathbb{N}$ が与えられたとき，$\mathsf{bin}(n)$ によって，n を 2 進展開したバイナリ列を表すものとする．このとき，$|\mathsf{bin}(n)| =^+ \log n$ である．ここで，対数関数 log の底は 2 である．

命題 2.7. $K(\tau) \leqslant^+ K(0^{|\tau|}) + |\tau| \leqslant^+ 2\log|\tau| + |\tau|$.

Proof. R を最適接頭機械とする．先程のように，文字列の長さ $|\tau|$ の情報をヘッダに付与するが，それを $0^{|\tau|}1$ と記述するのは無駄が多い．代わりに，文字列の長さ情報を圧縮したデータをヘッダに付与しよう．つまり，入力バイナリ列 η が与えられたとき，$R(\sigma) = \mathsf{bin}(|\tau|)$ となるような分解 $\eta = \sigma\tau$ を探し，そのようなものが見つかったら，$M(\sigma\tau) = \tau$ と定義する．このとき，M は接頭機械であり，$C_M(\tau) \leqslant C_R(0^{|\tau|}) + |\tau|$ である．補題 2.6 より，$C_R(0^{|\tau|}) \leqslant^+ 2\log|\tau|$ である． □

次の補題は，様々なバイナリ列のコルモゴロフ複雑性の上界を求める際に便利である．

補題 2.8. M が部分計算可能関数ならば，次を満たす定数 $c \in \mathbb{N}$ が存在する．

$$(\forall \tau \in \{0,1\}^*)\ K(M(\tau)) \leqslant K(\tau) + c.$$

Proof. R を最適接頭マシンとする．このとき，$S(\sigma) = M(R(\sigma))$ によって定義すると，$\mathrm{dom}(S) \subseteq \mathrm{dom}(R)$ であるから，S は接頭機械である．与えられた τ について，長さ $K(\tau)$ のバイナリ列 σ で，$R(\sigma) = \tau$ なるものが存在する．このとき，$S(\sigma) = M(R(\sigma)) = M(\tau)$ であるから，$C_S(M(\tau)) \leqslant K(\tau)$ である．よって，R の最適性より，ある c が存在して，任意の τ に対して，$K(M(\tau)) \leqslant C_S(M(\tau)) + c \leqslant K(\tau) + c$ となる． □

2.2 チャイティンのオメガ

それでは，具体的なランダム列を記述する準備を始めよう．接頭マシンにおいて，入力はいつ終わるか分からないバイナリ列であったことを思い出そう．いま，0 と 1 が同程度に出現する公平なコイン投げの繰り返しによってバイナリ列 $x_1x_2x_3\ldots$ を作る，という状況を考える．このような入力に対して，接頭機械 M が出力を返す確率 Ω_M はどれくらいだろうか？

たとえば，ある偶数 k について 0^k1 の形である入力のみ受理し，k を出力する接頭機械 M を考えよう．コインを $2n+1$ 回投げた結果が正確に $0^{2n}1$ となる確率は $0^{-(2n+1)}$ である．したがって，コイン投げを延々繰り返した結果，そのうち，ある偶数 k について 0^k1 の形となっている確率は以下によって与えられる．

$$\Omega_M = \sum_{n=0}^{\infty} 2^{-(2n+1)} = 2/3.$$

さて，どんなバイナリ列 $\sigma \in \{0,1\}^*$ が与えられても，コインを $|\sigma|$ 回投げた結果が正確に σ と一致する確率は $2^{-|\sigma|}$ である．したがって，一般の接頭機械 M についても，M が出力を返す確率 Ω_M は次によって計算できる．

定義 2.9 (停止確率)**.** M が接頭機械であるとき，M の**停止確率** (*halting probability*) とは，以下によって定まる値である．

$$\Omega_M = \sum_{\sigma \in \mathrm{dom}(M)} 2^{-|\sigma|}.$$

ここで，$\mathrm{dom}(M)$ は M の定義域を表す．最適接頭機械 R の停止確率 $\Omega = \Omega_R$ を特に**チャイティンの定数** (*Chaitin's constant*) と呼ぶ．

演習問題 2.10. M が接頭機械であるとき，$0 \leqslant \Omega_M \leqslant 1$ であることを証明せよ．

接頭機械 M が与えられたとき，停止確率 Ω_M は，計算可能な方法で下から近似できる．これを確かめるために，M_s を M の長さ s 以下の入力に対する計算を s ステップだけ実行したものとする．つまり，$|\sigma| \leqslant s$ かつ $M(\sigma)$ が s ステップ以下で出力を返すならば，$M_s(\sigma) = M(\sigma)$ とし，さもなくば $M_s(\sigma)$ は出力を返さないものとする．すると，

$$\Omega_{M,s} = \sum_{\sigma \in \mathrm{dom}(M_s)} 2^{-|\sigma|}$$

であり，この値は有限種類の入力に対する M の計算を s ステップずつ実行することによって計算できる．さらに，

$$\Omega_{M,0} \leqslant \Omega_{M,1} \leqslant \Omega_{M,2} \leqslant \cdots \leqslant \Omega_M = \lim_{s\to\infty} \Omega_{M,s}.$$

あるバイナリ列 $\sigma \in \{0,1\}^*$ について $\sum_{i=0}^{|\sigma|-1} \sigma(i)2^{-i-1}$ と書けるような実数を**二進有理数** (*dyadic rational*) と呼ぶ．つまり，$0.\sigma 0^\omega$ の形の実数のことである．たとえば，任意の機械 M および $s \in \mathbb{N}$ について，$\mathrm{dom}(M_s)$ は有限であるから，$\Omega_{M,s}$ は二進有理数である．一方，R が最適接頭機械であれば，定義域は無限集合となり，したがって，二進有理数には成り得ない．つまり，Ω は二進有理数ではない．

演習問題 2.11. 最適接頭機械の定義域が無限集合であることを示し，したがって Ω が二進有理数でないことを結論づけよ．

二進有理数でないような実数 $x \in [0,1]$ の二進表記は一意に定まるので，x を無限バイナリ列と同一視できる．無限バイナリ列 $z \in \{0,1\}^{\mathbb{N}}$ が与えられたとき，$z \upharpoonright n$ によって，長さ n の z の始切片を表すものとする．つまり，$z = z_0 z_1 z_2 \ldots z_i z_{i+1} \ldots$ ならば，$z \upharpoonright n = z_0 z_1 z_2 \ldots z_{n-1}$ のことである．

定理 2.12. 任意の最適接頭機械の停止確率 Ω について，次が成立する．

$$(\exists c)(\forall n)\ K(\Omega \upharpoonright n) \geqslant n - c.$$

Proof. R を最適接頭機械とする．$\Omega = \Omega_R$ かつ $\Omega_s = \Omega_{R,s}$ とする．次のような（接頭とは限らない）部分計算可能関数 M を考える．各入力 σ に対して，$0.\sigma \leqslant \Omega_t < 0.\sigma + 2^{-n}$ になるまで待つ．もし，そのようなステップ t が訪れたら，R_t の値域に入っていないバイナリ列 η を返す．つまり，どんな σ についても $R_t(\sigma) \neq \eta$ であるような η を選び，$M(\sigma) = \eta$ とする．

さて，実数 x について，$\sigma = x \upharpoonright n$ であるとは，$0.\sigma \leqslant x \leqslant 0.\sigma + 2^{-n}$ であるということに注意しよう．したがって，もし $\sigma = \Omega \upharpoonright n$ ならば，$0.\sigma \leqslant \Omega \leqslant 0.\sigma + 2^{-n}$ である．$(\Omega_s)_{s\in\mathbb{N}}$ は非減少であり，$\Omega = \lim_{s\to\infty} \Omega_s$ であることと，$\Omega = 0.\sigma$ では有り得ないことを利用すると，$0.\sigma \leqslant \Omega_t < 0.\sigma + 2^{-n}$ となるような t が存在することが分かる．つまり，部分計算可能関数 M は入力 $\sigma = \Omega \upharpoonright n$ に対しては，必ず R_t の値域に入っていない η を出力する．

一方，t ステップより後では，長さ $n-1$ 以下の入力に対して R が出力を返すことはない．なぜなら，さもなくば，停止確率の定義より $\Omega \geqslant \Omega_t + 2^{-n+1}$ となるが，t の選び方より，$0.\sigma + 2^{-n+1} \leqslant \Omega_t + 2^{-n+1} \leqslant \Omega \leqslant 0.\sigma + 2^{-n}$ となり，これは矛盾を導く．

さて，η は R_t の値域に入ってなかったため，もし $R(\sigma) = \eta$ となるような σ があったとしても，その計算は t ステップよりも長い時間がかかる．したがって，上で見た t の性質より，R が入力 σ に対して出力を返しているということは，$|\sigma| \geqslant n$ を導く．これより，$K(\eta) \geqslant n$ となる．ここで $\eta = M(\sigma) = M(\Omega \upharpoonright n)$ だったことを思い出すと，$K(M(\Omega \upharpoonright n)) \geqslant n$ を得る．ところで，M は部

分計算可能関数であるから，補題 2.8 より，任意の $\sigma \in \{0,1\}^*$ に対して，$K(M(\sigma)) \leqslant K(\sigma) + c$ である．以上をまとめると，

$$n \leqslant K(M(\Omega \upharpoonright n)) \leqslant K(\Omega \upharpoonright n) + c$$

である．ここで，c は部分計算可能関数 M に依存する定数であって，n に依存しないことに注意する．以上より，任意の n について，$K(\Omega \upharpoonright n) > n - c$ を得る． □

2.3 マーティンレフ・ランダムネス

さて，最初に，ランダム性とは圧縮不可能性であると述べた．しかし，多くの人々の印象としては，ランダム性とは確率概念と大きく結びつくものである．したがって，ランダム性と圧縮不可能性の “同値性” をもう少し確率論的に理解する方法はないだろうか．

ランダム系列であれば，確率 100% で成り立つ法則を全て満たしているべきである．たとえば，ランダム系列は，ボレルの**大数の法則**を満たすし，ヒンチンの**重複対数の法則**も満たす．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．つまり，ランダムな無限列は決して α には為りえない．—**確率論的にランダムな無限列は存在しない**！

この非存在証明は数学的には正しいが，計算論的観点からすると超越的である．そもそも我々はこの無限列 α が何であるかを知らないから，如何にして事前に α について語ることが出来ようか．無限列 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．したがって，ランダム性の定義を次のように改良しよう．

> ランダム系列であれば，確率 100% で成り立つような**有限の言葉で記述できる**法則を全て満たしているべきである．

ボレルの大数の法則も，ヒンチンの重複対数の法則も，有限の言葉で記述することができる．とはいえ，「有限の言葉で記述できる」とはどういう意味なのか曖昧であるから，これでは定義になっていない．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．

以下，正確な定義を与えよう．バイナリ列の集合 $U \subseteq \{0,1\}^*$ が与えられているとしよう．このとき，U の**確率** (*probability*) または**測度** (*measure*) を，表と裏の出現確率が等しいコイン投げの試行の繰り返しによって得られるバイナリ列がいつか U に含まれる確率によって定義し，$\lambda(U)$ と書く．数学的には，U の確率 $\lambda(U)$ は以下の式によって与えられる．

$$\lambda(U) = \sum\{2^{-|\sigma|} : \sigma \in U \text{ and } (\forall \tau \sqsubseteq \sigma)\ \tau \notin U\}.$$

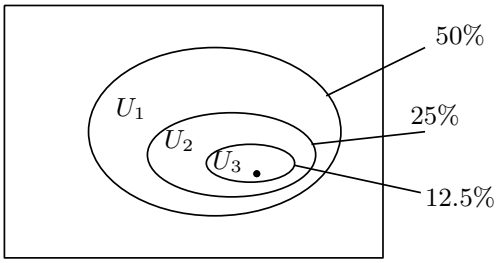


図 1　ランダムでないならば，マーティンレフ零集合によって捕捉される．

注意. λ は，公平なコイン投げから得られる $\{0,1\}^{\mathbb{N}}$ 上の確率測度 λ' と同一視できる．具体的には，バイナリ列 $\sigma \in \{0,1\}^*$ に対して，$[\sigma]$ を σ を拡張する無限バイナリ列全体，つまり $[\sigma] = \{\alpha \in \{0,1\}^{\mathbb{N}} : \sigma \sqsubseteq \alpha\}$ によって定義する．また，$[U]$ を U が生成する開集合 $[U] = \bigcup_{\sigma \in U} [\sigma]$ とする．このとき，$\lambda(U) = \lambda'([U])$ であることが分かる．

$\{0,1\}^*$ の部分集合の列 $(U_n)_{n\in\mathbb{N}}$ が与えられているとする．この集合列が**計算可枚挙**であるとは，$\{(n,\sigma) \in \mathbb{N} \times \{0,1\}^* : \sigma \in U_n\}$ が計算可枚挙であることを意味する．

定義 2.13. 集合 $N \subseteq \{0,1\}^n$ 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^0_1 集合列 $\{U_n\}_{n\in\mathbb{N}}$ で，任意の $n \in \mathbb{N}$ について $\lambda(U_n) \leqslant 2^{-n}$ 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．

上の定義の中の集合列 $(U_n)_{n\in\mathbb{N}}$ は，**マーティンレフ検定** (*Martin-Löf test*) と呼ばれる．これが意味するものは，アルゴリズム的に記述された統計的検定である．つまり，半計算可能な方法で記述された集合であり，確率 0 となることが半計算可能な方法で保証されている．無限列 $\alpha \in \{0,1\}^{\mathbb{N}}$ がマーティンレフ・ランダムであることは，どんなマーティンレフ検定 $(U_n)_{n\in\mathbb{N}}$ に対しても，$\alpha \notin \bigcap_n U_n$ となることと等しい．

さて，この統計的検定による確率的ランダム性と，圧縮不可能性によるランダム性には如何なる関わりがあるだろうか．実は，確率的にランダム性を定義しても圧縮不可能性によってランダム性を定義しても同値であることを数学的に証明できる，というのが次の定理の述べるところである．

定理 2.14. 無限バイナリ列 $\alpha \in \{0,1\}^{\mathbb{N}}$ に対して，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. 次を満たす定数 $c \in \mathbb{N}$ が存在する．

$$(\forall n \in \mathbb{N})\ K(\alpha \upharpoonright n) \geqslant n - c.$$

このために，以下の補題が必要である．集合 $L \subseteq \{0,1\}^* \times \mathbb{N}$ について，$\sum_{(\sigma,r)\in L} 2^{-r} \leqslant 1$ を**クラフトの不等式** (*Kraft's inequality*) と呼ぶ．

補題 2.15 (機械存在補題)**.** 計算可枚挙集合 $L \subseteq \{0,1\}^* \times \mathbb{N}$ がクラフトの不等式を満たすとする．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 $(\sigma, r) \in L$ 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，$K_M(\sigma) \leqslant r$ を満たす．

Proof. $L = \{(\sigma_i, r_i)\}_{i\in\mathbb{N}}$ 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，$\xi_n \in \{0,1\}^*$ 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 $\mathrm{dom}(M)$ 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 $\{\tau_k : k \leqslant n\} \cup \{\rho_{n,m} : \xi_n(m) = 1\}$ が反鎖となるように定義されるならば，結果として $\mathrm{dom}(M)$ 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．

$$2^{-r_0} = 0.\underbrace{000\ldots000}_{r_0-1}1,$$
$$0.\xi_0 = 0.\underbrace{111\ldots111}_{r_0-1}.$$

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 $\{\tau_k : k \leqslant n\} \cup \{\rho_{n,m} : \xi_n(m) = 1\}$ 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，

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

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，

$$\xi_n = \langle x_0, x_1, \ldots, x_{j-1},\ \mathbf{1}\ , 0, 0, 0, \ldots, 0, 0, 0,\ \mathbf{0}\ , x_{r_{n+1}}, \ldots\rangle,$$
$$\xi_{n+1} = \langle x_0, x_1, \ldots, x_{j-1},\ \mathbf{0}\ , 1, 1, 1, \ldots, 1, 1, 1,\ 1\ , x_{r_{n+1}}, \ldots\rangle.$$

となる．このとき，$\tau_{n+1} = \rho_{n,j}^{\frown} 0^{r_{n+1}-j}$ と定義し，各自然数 $m \in [j, r_{n+1})$ に対して，$\rho_{n+1,m} = \rho_{n,j}^{\frown} 0^{m-j} 1$ と定義する．$\{\tau_k : k \leqslant n+1\} \cup \{\rho_{n+1,m} : \xi_{n+1}(m) = 1\}$ 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，$\mathrm{dom}(M)$ は反鎖である．加えて，$|\tau_n| = r_n$ であることから，$K_M(\sigma) \leqslant r_n$ であることが従う． □

*Proof (*定理 *2.14).* $\neg(1) \Rightarrow \neg(2)$: 仮定より，ある計算可枚挙集合列 $\{U_n\}_{n\in\mathbb{N}}$ で，$\alpha \in \bigcap_n [U_n]$ かつ $\lambda(U_n) \leqslant 2^{-n}$ なるものが存在する．ある計算可枚挙な反鎖 $S_n \subseteq \{0,1\}^*$ で，$[U_n] = [S_n]$ なるものを見つけるのは難しくない．このとき，$\sum_{\sigma\in S_n} 2^{-|\sigma|} = \lambda(U_n) \leqslant 2^{-n}$ であることに注意する．後は $L = \{(\sigma, |\sigma| - n + 1) : \sigma \in S_{2n}\}$ と定義すれば，クラフトの不等式を満たす：

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

よって，機械存在補題 2.15 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，$K_M(\sigma) \leqslant |\sigma| - n + 1$ となる．このとき，$\alpha \in \bigcap_t [S_t]$ 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，$K_M(\alpha \upharpoonright n_t) \leqslant n_t - t + 1$ であるから，(2) の式の否定が得られた．

$\neg(2) \Rightarrow \neg(1)$: 各 $c \in \mathbb{N}$ について，次の集合 V_c を考える．

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

仮定より，$\alpha \in \bigcap_c [V_c]$ であるため，$\lambda(V_c) \leqslant 2^{-c}$ であることを示せば十分である．R を最適接頭機械とする．もし $\sigma \in V_c$ ならば，それを記述する有限列 $p(\sigma) \in \{0,1\}^*$ で，$|p(\sigma)| \leqslant |\sigma| - c$ かつ $R(p(\sigma)) = \sigma$ を満たすものが存在する．前者より，$\sigma \in V_c$ について，測度に関する以下の不等式を得る．

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

また，後者より，$\sigma \in V_c$ ならば $p(\sigma) \in \mathrm{dom}(R)$ である．よって，以下の不等式が導かれる．

$$2^c \cdot \lambda([V_c]) \leqslant 2^c \cdot \sum_{\sigma\in V_c} \lambda([\sigma]) \leqslant \sum_{\sigma\in V_c} \lambda([p(\sigma)]) \leqslant \sum_{\sigma\in \mathrm{dom}(R)} \lambda([\sigma]) = \Omega \leqslant 1.$$

これより，$\lambda([V_c]) \leqslant 2^{-c}$ を得る． □

2.4 ベルヌーイ測度とマルチンゲール

ここに，2 頭の馬 A と B がいるとしよう．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 $\mathcal{C}$ 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．以下，$\langle\rangle$ で空列を表す．

定義 2.16 (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 $m_p : \{0,1\}^* \to [0,1]$ 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 2.17. 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 $\sigma \in \{0,1\}^*$ 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 $\sigma \in \{0,1\}^*$ 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，それぞれの有限的条件 $[\sigma]$ 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 2.18 (カラテオドリの拡張定理)**.** $m : \{0,1\}^* \to [0,1]$ を，$m(\langle\rangle) = 1$ かつ，任意の $\sigma \in \{0,1\}^*$ について $m(\sigma) = m(\sigma 0) + m(\sigma 1)$ となる関数とする．このとき，$\{0,1\}^*$ 上のボレル確率測度 μ_m で，任意の $\sigma \in \{0,1\}^*$ について $\mu_m([\sigma]) = m(\sigma)$ 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．ある賭博戦略が与えられているとして，コイン投げの繰り返しの結果の系列が σ であった場合の現在所持金額を $d(\sigma)$ によって表すものとする．たとえば，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．

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

したがって，$p \times$ (上式) $+ (1-p) \times$ (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．一般に，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 $\mu([\sigma i]|[\sigma]) = \mu([\sigma i])/\mu([\sigma])$ によって

得られる．

J. 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，「コイン投げの繰り返しの結果が 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 $d : \{0,1\}^* \to [0,\infty)$ が Ville の意味でのマルチンゲールである．このようなマルチンゲールは，次のように形式的定義を与えることができる．

定義 2.19. μ を $\{0,1\}^{\mathbb{N}}$ 上の任意の確率測度とする．このとき，$d : \{0,1\}^*$ が任意の $\sigma \in \{0,1\}^*$ 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：

$$d(\sigma) = \frac{\mu([\sigma 0])d(\sigma 0) + \mu([\sigma 1])d(\sigma 1)}{\mu([\sigma])}.$$

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？

これに対する答えは，Ville の定理として知られる．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．つまりは，（公平なルールでゲームをする限りは）期待値よりも儲かる戦略なんてものは世の中には存在しない．

定理 2.20. μ を $\{0,1\}^{\mathbb{N}}$ 上の任意の確率測度とし，$q \geqslant 1$ 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 $d(\alpha \upharpoonright n) \geqslant q \cdot d(\langle\rangle)$ となる α 全体の集合の μ-測度は q^{-1} 以下である．

Proof. 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 $d(\sigma) \geqslant q$ を満たす極小な $\sigma \in \{0,1\}^*$ たちの集合として定義する．目標は，$\lambda([S]) \leqslant q^{-1}$ を示すことである．このとき，

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

あとは，$\sum_{\sigma \in S} \mu([\sigma])d(\sigma) \leqslant d(\langle\rangle) = 1$ 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 $a_k = \sum_{\sigma \in S[k]} \mu([\sigma])d(\sigma) \leqslant 1$ ならば，$\lim_k a_k \leqslant 1$ であるから，以下を示せば十分であることが分かる．

主張. $\tau \in \{0,1\}^*$ を任意の有限列とする．もし $F \subseteq \{0,1\}^*$ が τ を拡張する有限列たちからなる有限 $\sqsubset$-反鎖ならば，$\sum_{\sigma \in F} \mu([\sigma])d(\sigma) \leqslant \mu([\tau])d(\tau)$ 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 $\sigma \sqsupset \tau$ 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，$d(\sigma) \leqslant (\mu([\tau])/\mu([\sigma]))d(\tau)$ となることから，$\mu([\sigma])d(\sigma) \leqslant \mu([\tau])d(\tau)$ 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．τ を $F \subseteq \{\sigma : \tau \sqsubseteq \sigma\}$ 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 $F_i = \{\sigma \in F : \tau i \sqsubseteq \sigma\}$ は濃度 n 以下である．帰納的仮定より，以下が導かれる．

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

両辺に $\mu([\tau])$ を掛けることによって，$\sum_{\sigma\in F} \mu([\sigma])d(\sigma) \leqslant \mu([\tau])d(\tau)$ を得る． □

特に，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% であることが分かる．

定理 2.21 (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：

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

$\{0,1\}^{\mathbb{N}}$ 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 2.22 (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：

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

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．

以下によって，マルチンゲールとランダム性は数学的に厳密に結び付けられる．

定理 2.23. 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 $d : \{0,1\}^* \to [0,\infty)$ に対して，次の条件が成立する：

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

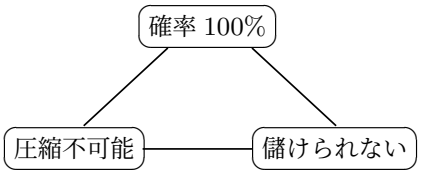


図 2　様々な発想に基づくランダム性概念は，実際には三位一体であり，一つの概念を別の視点に投影したものに他ならない (Schnorr 1971, 1973)

2.5　ハウスドルフ次元と複雑性

定理 2.23 によれば，統計的ランダム性（マーティンレフ・ランダム性）とマルチンゲールによるランダム性は，一般の確率測度においても一致する．それでは圧縮不可能性によるランダム性についてはどうだろうか．アルゴリズム情報理論としては，データ圧縮の性質を取り扱いたいため，コルモゴロフ複雑性の定義を確率測度毎に変えるのは望ましくない．したがって，素の状態のコルモゴロフ複雑性を用いて μ-ランダム列を調査したい．コルモゴロフ複雑性は公平なコイン投げによる確率測度 λ におけるランダム性との対応があったから，これは μ-ランダム列の確率測度 λ の下での振る舞いを考えるということである．

たとえば，μ として，バイアス $p = (p, p, p, \dots)$ のベルヌーイ測度 λ_p を考えよう．このとき，もちろん λ_p-ランダム列における 0 と 1 の出現確率は $p : (1-p)$ である．ところが，大数の法則から，100% の λ-確率で，0 と 1 の極限的な出現頻度は 1/2 になる．すると，0 と 1 の出現頻度が偏った無限列が得られる確率は 0% ということになる．それなら，出現頻度が $p : (1-p)$ 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，整数次元のルベーグ測度 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 2.24 (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．

$$\lambda^s(A) = \lim_{n\to\infty} \inf \left\{ \sum_{\sigma\in S} 2^{-s|\sigma|} : A \subseteq [S], \text{ and } S \subseteq \{0,1\}^{\geqslant n} \right\}.$$

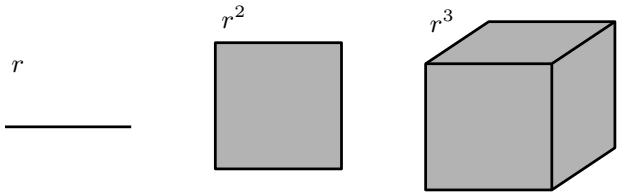


図 3　1 辺が r の s 次元立方体の s 次元ルベーグ測度は r^s である．

注意. 定義における $2^{-s|\sigma|}$ は $(\lambda([\sigma]))^s$ に等しいことに注意する．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)．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 次元ルベーグ測度は 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 2.24 が正当化される．

命題 2.25. 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 2.26. 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 2.27 (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ればいるほど，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 2.20 を思い出せば，確率 0 にまで候補を絞って

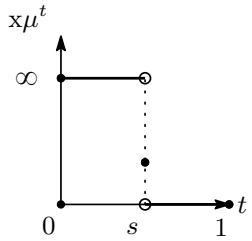


図 4　各集合には，高々 1 つの “ちょうどいい本来の次元” が存在し，それがハウスドルフ次元に他ならない．

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 2.28 (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：

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

このとき，無限列 $\alpha \in \{0,1\}^{\mathbb{N}}$ 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．

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

まず，ハウスドルフ次元とマルチンゲールがどのように関連しているのかを確認しよう．

定理 2.29. 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. α の実効ハウスドルフ次元は s 以下である*:* $\dim_H(\alpha) \leqslant s$.
2. 次の条件を満たす下半計算可能マルチンゲール $d : \{0,1\}^{<\mathbb{N}} \to [0,\infty)$ が存在する：

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

Proof. (1)⇒(2): $s > \dim_H(\alpha)$ を満たす実数 s を任意に取る．このとき，$\{\alpha\}$ は実効的 λ^s-零であるから，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．

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

ここで，U_n は反鎖とすることができる．Ville の定理 2.20 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 $\sigma \in \{0,1\}^*$ について，U_n^σ を，$\tau \sqsupseteq \sigma$ なる $\tau \in U_n$ 全体の集合とする．

このとき，$d_n(\sigma)$ として，初期資金 $d_n(\langle\rangle) = \sum_{\sigma\in U_n} 2^{-s|\sigma|}$ 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：

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

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．いま $\alpha \in \bigcap_{n\in\mathbb{N}} U_n$ 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，

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

であるから，次を得る．

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

(2)⇒(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．

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

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 $\tau \sqsubset \sigma$ 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．

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

.

ここで，最後の不等式は，定理**??**の証明中の主張による．主張 (2) の仮定より，$\alpha \in \bigcap_{n\in\mathbb{N}}[U_n]$ 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，$\dim_H(\alpha) \leqslant s$ を得る． □

つづいて，ハウスドルフ次元とコルモゴロフ複雑性の関連性である．実は，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．

定理 2.30. 無限列 $\alpha \in \{0,1\}^{\mathbb{N}}$ について，次の式が成立する．

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

Proof. まず，$\liminf_{n\to\infty} K(\alpha\upharpoonright n)/n < s$ 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，$K(\alpha\upharpoonright n) \leqslant sn - k$ が成立する．任意の $k \in \mathbb{N}$ について，

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

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??より，次を得る．

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

これより，$\sum_{\sigma\in U_k} 2^{-s|\sigma|} \leqslant 2^{-k}$ であり，$\alpha \in \bigcap_{k\in\mathbb{N}}[U_k]$ であるから，$\dim_H(\alpha) \leqslant s$ を得る．

逆に，$\dim_H(\alpha) < s$ 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，$\alpha \in \bigcap_n [U_n]$ かつ $\sum_{\sigma\in U_n} 2^{-s|\sigma|} \leqslant 2^{-n}$ を満たすものが存在する．もし，$\sigma \in \bigcup_{n\geqslant 1} U_n$ であることが分かったら，$(\sigma, s|\sigma|)$ を L に並べる．これはクラフトの不等式を満たす：

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

よって，機械存在補題 2.15 より，ある定数 $c \in \mathbb{N}$ が存在して，各 $\sigma \in \bigcup_{n\geqslant 1} U_n$ について，$K(\sigma) \leqslant s|\sigma| + c$ を得る．無限個の $t \in \mathbb{N}$ が存在して，$\alpha\upharpoonright t \in \bigcup_{n\geqslant 1} U_n$ を満たすから，

$$\liminf_{n\to\infty} \frac{K(\alpha\upharpoonright n)}{n} \leqslant s$$

を得る．よって，定理は示された． □

2.6 ランダム列のハウスドルフ次元

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 2.31. 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 2.32. 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 $\mathrm{Freq}(\alpha) = p$ 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．

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

Proof. $\sigma \in \{0,1\}^*$ と $i \in \{0,1\}$ が与えられたとき，$\#i(\sigma)$ で，$\sigma(n) = i$ なる $n \leqslant |\sigma|$ 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．$\mathrm{Freq}(\alpha) = p \geqslant 1/2 + \delta$ なので，次が成立する．

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

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，$p \geqslant 1/2+\delta$ なので，これより，

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

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，

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

であるから，次の式が成立する．

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

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． □

定理 2.33. $p \in (0,1)$ 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．

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

Proof. α が λ_p-ランダムならば，Borel の強大数の法則を分析すると，$\mathrm{Freq}(\xi) \neq p$ 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，$\mathrm{Freq}(\alpha) = p$ であることが示される．よって，定理 2.32 より，$\dim_H(\alpha) \leqslant \mathcal{H}(p)$ が成立する．後は $\dim_H(\alpha) \geqslant \mathcal{H}(p)$ 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：

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

いま，$\log \lambda_p([\sigma]) = \#0(\sigma)\log p + \#1(\sigma)\log(1-p)$ 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 $\mathrm{Freq}(\alpha) = p$ ならば，$\#0(\alpha \upharpoonright n)/n$ は p に収束するから，$\log \lambda_p([\alpha \upharpoonright n])/n$ 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，$sn + \log \lambda_p([\alpha \upharpoonright n]) < 0$ を得る．このような $n \in \mathbb{N}$ に対して，

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

が成立する．α は λ_p-ランダムなので，$\limsup_{n\to\infty} d_p(\alpha \upharpoonright n) < \infty$ 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 2.29 より，$\dim_H(\alpha) \geqslant \mathcal{H}(p)$ を得る． □