10.3.1 $P \neq NP$ 予想とランダムオラクル

オラクルによって $P^A \neq NP^A$ であつたり $P^B = NP^B$ であつたりするという事実は $P \stackrel{?}{=} NP$ 問題の難しさをあらためて示しただけ、なのであろうか？ それとも、第 II 巻第 16 章の定理 16.5 で証明するように $IP = PSPACE$ が成り立つのに、一方で $IP^A = PSPACE^A$ となるオラクル A が存在することも証明できることを鑑みると、相対化ができない（すなわち、ある命題の証明を相対化したものが元の命題と真偽を同じくするとは限らない）ような証明法があることも事実であるから、相対化できないような証明法によって $P \neq NP$ が証明できるかもしれない。そんなわけでは、この項では $P \stackrel{?}{=} NP$ 問題について相対化の観点からもう少しだけ考察してみよう。

はじめに考察したいのは、 $P = NP$ が成り立つことと $P \neq NP$ が成り立つことは独立であるのか、すなわち、一方が成り立たないからといって他方が成り立つとは限らないのではないかと、いう観点である。数学の世界は形式的に定義された公理系によって記述できる（例えば、自然数も、自然数を基にして定義される整数、有理数、実数、複素数も、集合論をはじめとする数学の諸理論も形式的体系 (formal system) として定義することができる（その辺りのことについては概略ではあるが第 II 巻の第 19 章を参照されたい。以下では最小限のことだけを説明する）が、ゲーデルの不完全性定理のように、 $P = NP$ も $P \neq NP$ も証明することができないようなこと（形式的体系）があるのであろうか？

Σ を有限アルファベットとし、 $W \subseteq \Sigma^*$ を帰納的言語とする。 W の元はなんらかの陳述（命題）を表す式（論理式と考えよ）を Σ 上の文字列として表したもの（符号化ではなく、例えば $\forall x(P(f(x), a) \wedge \exists y Q(y))$ のような、構文 (syntax) だけが定まっていて意味 (semantics) が定まっていない文字列）である。 $T \subseteq W$ を帰納的可算言語とし、 T の元を定理と呼ぶ。これは、すべての定理を列挙する（生成する）アルゴリズムが存在することを意味する。 $F := (\Sigma, W, T)$ を公理化可能理論 (axiomatizable theory) という。特に、 T が帰納的言語であるとき、 F は決定可能 (decidable) であるという。これは、任意に与えられた命題 (W の元) が F の定理であるかどうかを判定するアルゴリズムが存在することを意味する。こういった形式的理論のなかでも、TM に関する基本的性質すべてが上述の‘定理’になり、かつ矛盾を含まないもの（すなわち、命題 A とその否定の両方が定理になることがないような理論。そういった形式的理論は健全 (sound) であるという）を考えたい。換言すると、TM が F のモデルの一部を成し（すなわち、TM に関する命題は F においてすべて成り立つ（=定理となる））、かつ F のすべての定理 (T の元) が証明できると仮定する^{†1}。

次の定理は、上述の間‘ $P = NP$ も $P \neq NP$ も成り立たないような形式的理論が存在するか’に対する‘ある種の’解答である。 $\{M_i\}_{i \in \mathbb{N}}$ を多テープ TM の列挙とする。

定理 10.6.^{†2} TM がモデルの一部を成すような任意の公理化可能理論 F に対し、 $L(M_i) = \emptyset$ かつ $P^{L(M_i)} = NP^{L(M_i)}$ も $P^{L(M_i)} \neq NP^{L(M_i)}$ も F において証明できないような DTM M_i を求

^{†1} 形式的理論 F の論理式 (W の元) の中に現れるすべての記号（すなわち、アルファベット Σ の元) に具体的な意味を与えることを解釈 (interpretation) あるいは構造 (structure) というが、その解釈の下ですべての定理 (T の元) が真になる（=成り立つ）とき、その解釈をモデル (model) という。 F における証明 (proof) とは、公理 (axiom) と呼ばれる論理式 (T の部分集合) からなんらかの論理的に妥当な推論の仕方によって定理 (T の元) を導く過程のことである（ここでは、どのような推論を許すのかは明示していない）。証明によって導かれたものが定理であるが、証明できる (provable) とは証明が存在することである。

^{†2} J.Hartmanis and J.Hopcroft, Independence results in computer science, *ACM SIGACT News*, 8, pp.13–23, 1976.

めるアルゴリズムが存在する. □

証明 定理 10.5 より, $\mathbf{P}^A = \mathbf{NP}^A$, $\mathbf{P}^B \neq \mathbf{NP}^B$ となる A, B が存在する. TM M を次のように定義する:

M が (j, x) を受理する $\iff F$ における証明を枚挙したうちの最初の x 個の中に
 $[\mathbf{P}^{L(M_j)} = \mathbf{NP}^{L(M_j)} \text{ かつ } x \in B]$ の証明が存在するか, または
 $[\mathbf{P}^{L(M_j)} \neq \mathbf{NP}^{L(M_j)} \text{ かつ } x \in A]$ の証明が存在する.

帰納定理 (第 7 章 7.2 節の問 7.5 参照) より, $x \in L(M_{j_0}) \iff (j_0, x) \in L(M)$ を満たす j_0 が存在する.

もし $[\mathbf{P}^{L(M_{j_0})} = \mathbf{NP}^{L(M_{j_0})}]$ の証明が F に存在するとすると, $(j_0, x) \in L(M) \iff x \in B$ が有限個の例外を除くすべての x に対して成り立つ. すなわち, $L(M_{j_0})$ と B は有限個の元以外では等しいので, $\mathbf{P}^B \neq \mathbf{NP}^B$ とすると $\mathbf{P}^{L(M_{j_0})} \neq \mathbf{NP}^{L(M_{j_0})}$ である. 同様に, もし $[\mathbf{P}^{L(M_{j_0})} \neq \mathbf{NP}^{L(M_{j_0})}]$ の証明が F に存在するとすると, $L(M_{j_0})$ と A は有限個の元以外では等しいので, $\mathbf{P}^A = \mathbf{NP}^A$ とすると $\mathbf{P}^{L(M_{j_0})} = \mathbf{NP}^{L(M_{j_0})}$ である. F は健全であるとした仮定から, $\mathbf{P}^{L(M_{j_0})} = \mathbf{NP}^{L(M_{j_0})}$ も $\mathbf{P}^{L(M_{j_0})} \neq \mathbf{NP}^{L(M_{j_0})}$ も F では証明できないということが導かれる.

さらに, $\mathbf{P}^{L(M_{j_0})} = \mathbf{NP}^{L(M_{j_0})}$ も $\mathbf{P}^{L(M_{j_0})} \neq \mathbf{NP}^{L(M_{j_0})}$ も F では証明できないことから, M_{j_0} はどんな入力 x も受理しない. すなわち, $L(M_{j_0}) = \emptyset$ である. □

$L(M_{j_0}) = \emptyset$ であるからといって $\mathbf{P} = \mathbf{NP}$ であることや $\mathbf{P} \neq \mathbf{NP}$ であることが F で証明できるとは限らないので, $\mathbf{P} = \mathbf{NP}$ が成り立つかどうかは F と独立である. それゆえ, この定理は「合理性のある任意の形式的証明系 F に対して, F と独立な, 計算量理論の観点から少しばかり興味深い事実が成り立つ」ことを示しただけで, $\mathbf{P} \stackrel{?}{=} \mathbf{NP}$ 問題の解決に貢献するものではない.

定理 10.5 (2) の証明において, L_B を受理する NTM M は $x \in B$ か否かの計算においてたった 1 回しかオラクルに質問していないのに対し, DTM M^B は指数関数的回数も質問をしている. 一般に, $t(n)$ 時間限定の NTM の計算木は指数関数 $O(2^{t(n)})$ 個の様相を含みうるのでオラクル NTM ならば B に指数関数回の質問をすることによってオラクル DTM よりも能力を高くできるが, オラクル NTM とオラクル DTM の関係を通常の NTM と DTM の関係に近づけるには NTM が無制限にオラクルに質問できないように制限する必要がある. 例えば, オラクル NTM はたかだか多項式回の質問しかできないように制約してもオラクル NTM の方がまだオラクル DTM よりも能力が高いであろうか? 実は, こういった制約をオラクル NTM に課すと, 相対化版の $\mathbf{P} \stackrel{?}{=} \mathbf{NP}$ 問題は非相対化版の $\mathbf{P} \stackrel{?}{=} \mathbf{NP}$ 問題と同値になることが証明できる. このことは, 定理 10.5 が成り立つのは, オラクル NTM が (質問によって) 過剰なまでの情報にアクセスできることにあるといえる. したがって, 定理 10.5 のような相対化版の結果は, 元々の相対化されていない問題に影響を及ぼすものではない, という見方もできる. この種の結果を正の相対化 (positive relativization) という. その一例を次に示す.

集合 A に対し,

$$\mathbf{NP}_b^A := \{ B \mid \exists \text{多項式時間限定のオラクル NTM } M, \exists \text{多項式 } p, \\ \forall x [x \in B \iff x \in L(M^A) \text{ かつ } M(x) \text{ がする質問総数} \leq p(|x|)] \}$$

と定義する.

定理 10.7.¹³ $P = NP$ が成り立つ必要十分条件は、任意の A に対して $P^A = NP_b^A$ が成り立つことである。□

したがって、 $P \neq NP$ が証明できない限りどんな A に対しても $P^A \neq NP_b^A$ となることはない。一方、任意の $PSPACE$ 完全な A に対して $P^A = NP^A = PSPACE$ であるから、 $P^A \neq NP_b^A$ となる A は存在する。しかし、これは $PSPACE$ がオラクルとして強力であることを示しているだけであり、 $P \stackrel{?}{=} NP$ 問題についてそれ以上の情報を与えるものではない。

最後に、この節のタイトルになっているランダムなオラクルについて考察しよう。

はじめに、位相や測度に関する基本的事項について簡単に述べておく。以下に述べる程度のことがわかれば十分で、位相空間や測度論に精通している必要はない。

① 位相空間について

距離空間（距離が定義されている集合）において極限とか連続という概念は‘開集合’ (open set) という概念によってより抽象的に記述することができ、このことから開集合の族が定義された集合を位相空間 (topological space) と呼んで研究されるようになった。集合 S の位相 (topology) とは次の条件

1. $S \in \mathcal{O}, \emptyset \in \mathcal{O}$.
2. 任意の有限個の $U_1, \dots, U_n \in \mathcal{O}$ に対して、それらの共通部分も $U_1 \cap \dots \cap U_n \in \mathcal{O}$ である。
3. Λ を任意の有限または無限の添字集合とすると、 $U_\lambda \in \mathcal{O}$ ($\lambda \in \Lambda$) ならばそれらの和集合も $\bigcup_{\lambda \in \Lambda} U_\lambda \in \mathcal{O}$ である。

を満たす S の部分集合の族 $\mathcal{O}$ のことである。 $\mathcal{O}$ に属す集合を開集合という。空でない集合 S の部分集合すべてからなる集合 $\mathcal{O}$ は位相の条件を満たしている。この位相を離散位相 (discrete topology) という。

位相空間 S の部分集合族 $\mathcal{B}$ で、 S の位相 $\mathcal{O}$ (すなわち、 S の開集合すべてから成る集合族) に属す任意の開集合が $\mathcal{B}$ の元の和として表せるものを開集合の基底とか開基 (開基底) (base, basis) といい、開基 $\mathcal{B}$ は位相 $\mathcal{O}$ を生成するという。

$a \in S$ に対し、 a を含む開集合を a の近傍 (neighbour) といい、 a の近傍の全体を $\mathcal{N}(a)$ と書いて全近傍系 (neighbourhood system) という。全近傍系 $\mathcal{N}(a)$ の一部分からなる集合族 $\mathcal{B}(a)$ で、任意の $U \in \mathcal{N}(a)$ に対して $V \subseteq U \wedge V \in \mathcal{B}(a)$ を満たす V が存在するものを a の基本近傍系 (fundamental system of neighbourhoods) という。基本近傍系を用いて、2つの位相空間 S と T の直積 $S \times T$ の位相を次のように定義する。各 $a \in S$ の基本近傍系を $\mathcal{B}(a)$ 、各 $b \in T$ の基本近傍系を $\mathcal{B}(b)$ とするとき、 $(a, b) \in S \times T$ の基本近傍系を

$$\mathcal{B}(a, b) := \{V \times W \mid V \in \mathcal{B}(a), W \in \mathcal{B}(b)\}$$

と定義すると $S \times T$ は位相空間になる (これを S と T の積空間といい、この位相を直積位相という)。

② 測度について

測度 (measure) とは、面積、体積、長さ、個数といった「大きさ」に関する概念を精緻化・一般化した‘量を測る尺度’である。特に、ルベーグ測度 (Lebesgue measure) は、「互いに素な複数の集

¹³ R.Book, T.Long and A.Selman, Quantitative relativizations of complexity classes, *J. Comput. Sys. Sci.* 13, pp.461–487, 1984.

合の長さ・面積・体積はそれぞれの長さ・面積・体積の和に等しい」という‘加法性’を保ちながら、ユークリッド空間上の長さ・面積・体積の概念を拡張したものである。

もう少し具体的にいうと、集合 X 上の測度とは X の部分集合に実数（その部分集合の「大きさ」）を割り当てる写像である。可能ならば‘加法性’が成り立つことが望ましいが残念ながら不可能であるため、測度が定義できるような、 X の部分集合からなるより小さな集合族を代わりに考え、このような集合を可測集合と呼ぶ。すなわち、集合 X に対し、次の条件を満たす空でない集合族 $\Sigma \subseteq 2^X$ を X 上の σ -集合代数 (σ -algebra) といひ（完全加法族 (completely additive class)、可算加法族 (countably additive class) とか σ -加法族とか σ -集合体 (σ -field) ともいう)、 Σ に属す集合を可測集合 (measurable set) という：

1. $\Sigma \neq \emptyset$.
2. Σ は補集合で閉じている： $A \in \Sigma \implies X - A \in \Sigma$.
3. Σ は可算個の和で閉じている： $A_1, A_2, \dots \in \Sigma \implies (A_1 \cup A_2 \cup \dots) \in \Sigma$.
4. したがって、 $\emptyset, X \in \Sigma$ であり、共通部分でも閉じている： $A_1, A_2, \dots \in \Sigma \implies (A_1 \cap A_2 \cap \dots) \in \Sigma$.

ルベーグ測度については、まず $\mathbb{R}^n$ 内の区間 (box) を、1次元区間の直積 $B := \prod_{i=1}^n [a_i, b_i]$ と定義し、この区間 B の容積 (volume) を $\text{vol}(B) := \prod_{i=1}^n (b_i - a_i)$ と定義する。 $\mathbb{R}^n$ の任意の部分集合 A に対し、 $\mathbb{R}^n$ のたかだか可算個の区間からなる区間族を $\mathcal{B}$ とするとき、 A の外測度 (outer measure) $\lambda^*(A)$ を

$$\lambda^*(A) := \inf_{\mathcal{B}} \left\{ \sum_{B \in \mathcal{B}} \text{vol}(B) \right\}$$

と定義する（下限は、その和が A を被覆するような $\mathcal{B}$ すべてに対して取る）。さらに、 $\mathbb{R}^n$ の部分集合 A がルベーグ可測 (Lebesgue measurable) であることを、 $\mathbb{R}^n$ の任意の部分集合 S に対して

$$\lambda^*(S) = \lambda^*(A \cap S) + \lambda^*(S - A) \quad (\text{カラテオドリの条件})$$

が成り立つこと、と定義する。ルベーグ可測な集合全体は完全加法族を成し、その上のルベーグ測度 λ は、任意のルベーグ可測集合 A に対して $\lambda(A) := \lambda^*(A)$ と定義する。

確率測度 (probability measure) は‘確率を測る尺度’であり、‘加法性’のような測度の性質を満たすもので、確率空間において事象の集合上で定義された実数値関数のことである。一般の測度と確率測度の違いは、確率測度は全空間に対する値が1であるということである。すなわち、標本空間 Ω と σ -集合体 $\mathcal{F}$ が与えられたとき、 $(\Omega, \mathcal{F})$ 上の確率 (測度) とは、以下を満たす $\mathcal{F}$ 上の関数 μ のことである：

1. $\mathcal{F}$ の元 E のそれぞれについて関数値 $\mu[E]$ が定まり、かつ
2. 全ての $E \in \mathcal{F}$ に対して $0 \leq \mu[E] \leq 1$ であり、
3. $\mu[\emptyset] = 0, \mu[\Omega] = 1$ かつ
4. $E_1, E_2, \dots \in \mathcal{F}$ が互いに排反、すなわち $i \neq j \implies E_i \cap E_j = \emptyset$ を満たすとき、 $\mu[\bigcup_{i=1}^{\infty} E_i] = \sum_{i=1}^{\infty} \mu[E_i]$ が成り立つ。

2つの確率空間 $(\Omega_i, \mathcal{F}_i, \mu_i)$ ($i = 1, 2$) の直積確率空間 $(\Omega, \mathcal{F}, \mu)$ を次のように定義する。

1. Ω は Ω_1 と Ω_2 の直積集合： $\Omega = \Omega_1 \times \Omega_2$.
2. $\mathcal{F}$ は次のように段階的に定義する：

- (a) $C := \{A_1 \times A_2 \mid A_1 \in \mathcal{F}_1, A_2 \in \mathcal{F}_2\}$.
 (b) C の互いに素な元の有限和を $\mathcal{A}$ とする.
 (c) $\mathcal{A}$ を含む最小の σ -集合体を $\mathcal{F}$ とする.

3. μ は,

- (a) $A_1 \times A_2$ という形の集合 ($A_1 \in \mathcal{F}_1, A_2 \in \mathcal{F}_2$) に対しては, $\mu[A_1 \times A_2] := \mu[A_1]\mu[A_2]$ と定義する.
 (b) より一般の $\mathcal{F}$ の元 ($A_1 \times A_2$ の和集合や, $\mathcal{F}$ が σ -集合体であることによる「極限」的な集合など) に対しては, P に σ -加法性を課すことで拡張して定義する (例えば, $A \cap B = \emptyset \implies \mu[A \cap B] := \mu[A] + \mu[B]$ とする, など).

さて, 本題に戻ろう.

$C := \{C \mid C \subseteq \{0, 1\}^*\}$ とし, C の部分クラス

$$\mathcal{A} := \{A \in C \mid \mathbf{P}^A = \mathbf{NP}^A\}, \quad \mathcal{B} := \{B \in C \mid \mathbf{P}^B \neq \mathbf{NP}^B\}$$

を考える. $\mathcal{A}$ と $\mathcal{B}$ のどちらが‘大きい’だろうか? 確率論の観点からこの問題を考察しよう.

C 上の確率を定義するために, $X \in C$ とその特性数列

$$\alpha_X := \chi_X(\lambda)\chi_X(0)\chi_X(1)\chi_X(00)\cdots$$

とを同一視する. ここで, $\lambda, 0, 1, 00, \dots$ は $\{0, 1\}^*$ の元を辞書式順序で並べたものであり,

$$\chi_X(x) = 1 \quad (\chi_X(x) = 0) \stackrel{\text{def}}{\iff} x \in X \quad (x \notin X)$$

である. C をこのように定義された無限 2 進数列の集合, すなわち $\{0, 1\}$ の可算無限直積 $\{0, 1\}^\infty$ とみなす. C を位相空間として扱うために, $\{0, 1\}$ の離散位相の可算無限直積を C の位相と定義する. この位相空間はカントール空間 (Cantor space) と呼ばれ, よく知られたカントール集合 (閉区間 $[0, 1]$ に属す実数のうちその 3 進数展開のどの桁にも 1 が含まれないような表示ができるものからなる集合. カントールの 3 進集合ともいう. 図形的にはフラクタルの一種と見ることができ) の位相空間論的抽象化である.

C 上の一様確率測度 (uniform probability measure) μ を $\{0, 1\}$ 上の等確率測度 (すなわち, $\mu\{0\} = \mu\{1\} = \frac{1}{2}$) の可算無限直積として定義する. すなわち, 任意の n に対し, ランダムな 2 進数列 $\alpha \in C$ の第 n ビットが 0 になる確率と 1 になる確率は等しく $\frac{1}{2}$ である. 区間 $[0, 1]$ の実数とその 2 進数展開とを同一視したとき, この μ は $[0, 1]$ のルベーグ測度である.

任意の $u \in \{0, 1\}^*$ に対し, $\Gamma_u := \{u\beta \mid \beta \in \{0, 1\}^\infty\}$ と定義する. Γ_u をシリンダー (cylinder) という. すべてのシリンダー Γ_u ($u \in \{0, 1\}^*$) は直積位相の下で位相空間 C の開集合基になる. 明らかに, 任意の $u \in \{0, 1\}^*$ に対し, $\mu(\Gamma_u) = 2^{-|u|}$ である. すべての Γ_u ($u \in \{0, 1\}^*$) を含む最小の σ -集合体をボレル集合体 (Borel field, Borel algebra) という. ボレル集合体の元 (ボレル集合 (Borel set) という) は可測である.

以上述べたような設定の下で $\mathcal{A}$ と $\mathcal{B}$ のどちらが‘大きい’ ($\mu(\mathcal{A})$ と $\mu(\mathcal{B})$ のどちらが大きい) であろうか? 実は後述するように $\mu(\mathcal{A}) = 0$ であるが, その証明は次の補題が重要な役割を演じる:

補題 10.1 (コルモゴロフの 0-1 律). ボレル集合 $\Gamma \subseteq C$ が有限の変更の下で不変 (すなわち $\alpha \in \Gamma$ かつ α と β が有限個のビット位置においてしか異ならないならば $\beta \in \Gamma$ である) とすると, $\mu(\Gamma)$ は 1 か 0 である.

略証 Γ が有限の変更の下で不変ならば, 全空間 $\mathcal{C}$ における Γ の分布は任意の u について部分空間 Γ_u における分布と等しい. なぜなら, 任意の長さが同じ $u, v \in \{0, 1\}^*$ に対して, 写像 $f(u\alpha) = v\alpha$ は Γ の元は変えずに部分空間 Γ_u を部分空間 Γ_v へ写し, かつ条件付き確率を保存する (すなわち, $\mu(\Gamma \cap \Gamma_u) = \mu(\Gamma \cap \Gamma_v)$ を満たす). したがって, 任意の $u \in \{0, 1\}^*$ に対して

$$(*) \quad \mu(\Gamma \cap \Gamma_u) = \mu(\Gamma)\mu(\Gamma_u)$$

が成り立つ. このことと $\{\Gamma_u \mid u \in \{0, 1\}^*\}$ がすべてのボレル集合を生成することから, $(*)$ は任意のボレル集合, したがって特に Γ に対しても成り立つ. よって, $\mu(\Gamma) = \mu(\Gamma)^2$ であり, ゆえに $\mu(\Gamma)$ は 0 か 1 である. $\square$

定理 10.8.ⁱ⁴ $\mu(\mathcal{B}) = 1$ である. すなわち, 任意の $B \in \mathcal{B}$ に対し $\mathbf{P}^B \neq \mathbf{NP}^B$ が確率 1 で成り立つ. $\square$

この定理の証明は難解なので省略するが,

$$L_B := \{0^n \mid \exists x [|x| = n \wedge x_1, x_{11}, \dots, x_{1^n} \in B]\}$$

と定義すると, $L_B \in \mathbf{NP}^B$ であることは明らかなので, $L_B \in \mathbf{P}^B$ を満たすオラクル B は非常に少ない (存在する確率が 0 である) ことを証明すればよい.

ⁱ⁴ C.Bennet and J.Gill, Relative to a random oracle A , $\mathbf{P}^A \neq \mathbf{NP}^A \neq \mathbf{coNP}^A$ with probability 1, *SIAM J. Comput.* 10, pp.96–113, 1981.