多項式時間計算可能クラスについて

TANAKA, Hisao / 田中, 尚夫

(出版者 / Publisher)
法政大学工学部
(雑誌名 / Journal or Publication Title)
Bulletin of the Faculty of Engineering, Hosei University / 法政大学工学部研究集報
(巻 / Volume)
33
(開始ページ / Start Page)
11
(終了ページ / End Page)
15
(発行年 / Year)
1997-03
(URL)
https://doi.org/10.15002/00003803

多項式時間計算可能クラスについて

田中　尚夫*

On Polynomial Time Computable Classes

Hisao TANAKA*

Abstract

We define the notion of polynomial time computability for classes of language and discuss some relation between the complexity of Lebesgue measure of such classes and the **P=? BPP** question. Thus we have shown :

THEOREM : If the assumption **PTH** holds,then **P=BPP** holds. For the description of the assumption **PTH**, see the following.

§1　序　　論

Strings の集合たちのクラスたちを考える。これらを今後単にクラスという。著者は以前に

定理．［Ta 67］Σ_1^1 クラスのルベーグ測度は Σ_1^1- 実数である。

という結果を証明した。ここでは計算量問題の観点から、これより遥かに低いクラスの測度を考察する。即ちパラメタをもつ多項式時間計算可能クラスの概念を定義し、その測度がパラメタに関してどんな計算量になるのかを考察するのである。パラメタを取り入れるのは以下の理由による：パラメタなしの多項式時間計算可能クラスは帰納的クラスとなるから、basic open sets の有限個の和集合となり、その測度は2進有理数であり、当然多項式時間で計算できる。よって問題が自明になってしまう。そこで多項式時間計算可能クラスの或“列”を取り扱わなければならないのである。

$\{C_k\}$ を多項式時間計算可能クラスの1つの列（定義は次節を参照）とする。r を2進 string $r=r_1 r_2 \ldots r_n$ とし、r と2進小数 $0.r_1 r_2 \ldots r_n$ とを同一視する。**PTH** は次の主張である（正確な記述は次節で述べる）：

PTH（Polynomial Time Hypotheis on Measure）：

“$r < \mu(C_k)$” は r，k に関する多項式時間計算可能な関係である。

*工学部システム制御工学科

このとき本論文の主定理は次のように述べられる：

定理 3.2.　仮定 **PTH** の下で **P＝BPP** が成り立つ。□

大方は **P≠BPP** という予想であるから、われわれの仮定 **PTH** は証明が困難であろう。

§2　準　　備

本論文は計算理論の標準的な用語と記号法に従う。例えば、文献 [Pa 94]、[Ta 96] etc. を参照されたい。　$\Sigma=\{0,1\}$ とし、Σ 上の有限列（語ともいう）全体の集合 Σ^* の部分集合を言語といい、言語たちの集合をクラスという。Σ^* の要素全体を標準的に並べて

$$\lambda, 0, 1, 00, 01, 10, 11, 000, \ldots$$

とし、それらをその番号である自然数と同一視する。§1 の k は番号 k をもつ語と考えてよい。

言語　$Y \subseteq \Sigma^*$ はその特性関数と同一視される：

$$Y = Y(0)Y(1)Y(2)\ldots Y(n)\ldots$$

ここで、$n \in Y$ ならば $Y(n)=1$、$n \notin Y$ ならば $Y(n)=0$ である。また、$Y \mid n = Y(0)Y(1)\ldots Y(n-1)$ とおき、Y の n-始切片という。

$w = w(0)w(1)\ldots w(n-1) \in \Sigma^*$ に対し

$$N_w = \{Y \subseteq \Sigma^* : Y \mid n = w\}$$

とし、すべての N_w たちを basic open sets として空間 2^{Σ^*} へ位相を入れると所謂カントル空間になる。

$P_{\tilde{e}}$ を e- 番目の多項式時間限定 oracle チューリングマシン、$p_e(n)$ をその時間限定多項式とする。これは、e に関して帰納的であるようにできる。

定義 2.1.　クラス **A** が多項式時間計算可能であるとは、

$$Y \in \mathbf{A} \Leftrightarrow P_e^Y(x) = 1$$

が成り立つような、$e, x \in \Sigma^*$ が存在すること。□

序論で述べたように、パラメタを導入しよう。

$e, x \in \Sigma^*$ に対しクラスの列 $\mathbf{A}_{e,x}$ を次のように定義する：

$$Y \in \mathbf{A}_{e,x} \Leftrightarrow P_e^Y(x) = 1$$

各クラス $\mathbf{A}_{e,x}$ は勿論帰納的であるから、それは有限個の basic open sets の和集合であり、従ってそのルベーク測度 $\mu(\mathbf{A}_{e,x})$ は 2 進有限小数である。そうして明らかに

$$r < \mu(\mathbf{A}_{e,x}) \qquad (1)$$

は、r,e,x の関係として、帰納的である。しかしながら我々はこれが多項式時間計算可能であると望みたい。そこで次の仮定的主張を立てる：

PTH：関係 (1) は多項式時間計算可能である。□

§3 主　定　理

簡単のため、oracle A に対し、P_e^A とそれが受理する言語

$$\{x \in \Sigma^* : P_e^A(x) = 1\}$$

とを同一視して、

$$\mathbf{P}[A] = \{P_e^A : e = 0, 1, 2 \ldots\}$$

と定義する、これは所謂クラス **P** の oracle A による相対化であり、$\mathbf{P} = \mathbf{P}[\phi]$ である。そこで言語 A、B に対し、BがAに多項式時間チューリング還元可能ということを、$B \in \mathbf{P}[A]$ によって定義し、$B \leqq_{PT} A$ で表す。

定理 3.1.　もし **PTH** が成り立つならば、任意の言語 B に対し

$$\mu(\{Y : B \leqq_{PT} Y\}) > 0 \Leftrightarrow B \in \mathbf{P}$$

証明.　十分性は明らかであるから、必要性を証明する。よって

$$\mu(\{Y : B \leqq_{PT} Y\}) > 0$$

と仮定する。$\mathbf{B}_e = \{Y : B = P_e^Y\}$ とおくと

$$\{Y : B \leqq_{PT} Y\} = \cup\{\mathbf{B}_e : e = 0, 1, 2 \ldots\}$$

であるから、$\mu(\mathbf{B}_e) > 0$ となる index e がある。簡単のため、$\mathbf{B}_e$の代わりに **B** と書き、$\mu(\mathbf{B}) = 3\varepsilon$ とおく。そのとき、補集合 $\neg\mathbf{B}$ を含む開集合 **G** で $\mu(\mathbf{G} \cap \mathbf{B}) < \varepsilon$ をみたすものがある。よって、**G** に含まれる有限個の basic open sets $\mathbf{N}_{w1}, \mathbf{N}_{w2}, \ldots, \mathbf{N}_{wm}$ を見つけて

$$\mathbf{D} = \mathbf{N}_{w1} \cup \mathbf{N}_{w2} \cup \ldots \cup \mathbf{N}_{wm}, \qquad \mu(\mathbf{G} - \mathbf{D}) < \varepsilon \tag{2}$$

が成立するようにできる。そのとき、

$$\mu(\mathbf{B} - \mathbf{D}) > 2\varepsilon \tag{3}$$

そこで、j = 0, 1 に対し $\mathbf{K}_j(x) = \{Y : P_e^Y(x) = j\}$ とおくと、すべての x について $\mathbf{B} \subseteq \mathbf{K}_{B(x)}(x)$ となる。(3)により、

$$\mu(\mathbf{K}_{B(x)}(x) - \mathbf{D}) > 2\varepsilon \tag{4}$$

他方で、もし $j \neq B(x)$ ならば $\mathbf{K}_j(x) \subseteq \neg\mathbf{B}$ 。よって $\neg\mathbf{B} \subseteq \mathbf{G}$ と(2)から

$$j \neq B(x) \Rightarrow \mu(\mathbf{K}_j(x) - \mathbf{D}) < \varepsilon \tag{5}$$

従って、$\varepsilon < r < 2\varepsilon$ をみたす2進有限小数 **r** をとると(3)によって

$$\mu(\mathbf{K}_j(x) - \mathbf{D}) > \mathbf{r} \Rightarrow j = B(x) \tag{6}$$

が得られる。ここで (4) を使うと

$$\forall x \; \exists j \in \{0, 1\}[\mu(\mathbf{K}_j(x) - \mathbf{D}) > \mathbf{r}] \tag{7}$$

明らかに次の関係をみたす index d と stirng w とが存在する：

$$Y \in \mathbf{K}_j(x) - \mathbf{D} \Leftrightarrow P_e^Y \text{ は } \langle x, j, w\rangle \text{ を受理する}$$

$$\Leftrightarrow Y \in \mathbf{A}_{d, \langle x,j,w\rangle}$$

故に、(7) は

$$\forall x \exists j \in \Sigma[r < \mu(A_{d,\langle x,j,w\rangle})] \tag{8}$$

が成立することを言っている。

ここで一つの補題を述べる：

補題 3.2. $R(x,j)$ が多項式時間計算可能な関係で、条件

$$\forall x \exists j \in \Sigma\, R(x,j) \tag{9}$$

をみたすとする。このとき、

$$\forall x\, R(x,f(x)) \tag{10}$$

が成り立つような多項式時間計算可能関数 $f:\Sigma^* \to \Sigma$ が存在する。□

証明は明らかであろう。

定理の証明を続ける。$R(x,j)$ として "$r<\mu(A_{d,\langle x,j,w\rangle})$" をとる。我々は **PTH** を仮定しているから、この $R(x,j)$ は多項式時間計算可能である。故に 補題 3.2 が適用できて、

$$\forall x[\mu(K_{f(x)}(x)-D)>r]$$

をみたす多項式時間計算可能関数 $f(x)$ が存在することになる。よって(6)から

$$\forall x[f(x)=B(x)]$$

が成立し、$B \in P$ が証明された。□

定理 3.1 の Baire category version は1980年代からの folklore-type の事実である：

$$\{Y : B \leqq_{PT} Y\} \text{ が meager でない} \Leftrightarrow B \in P$$

ところで、[BG 81] [AS 86] は次の結果を証明した：

$$B \in BPP \Leftrightarrow \mu(\{Y : B \leqq_{PT} Y\}) = 1$$

ここで、**BPP** は誤り確率が $1/2$ より小さく制限された多項式時間限定確率チューリングマシンによって受理される言語全体のクラスである。$\{Y : B \leqq_{PT} Y\}$ は tail set であるから、Kolmogorov の zero-one 法則によって

$$\mu(\{Y : B \leqq_{PT} Y\}) > 0 \Leftrightarrow \mu(\{Y : B \leqq_{PT} Y\}) = 1$$

である。これらと定理3.1.とから我々の主定理が得られる：

定理 3.3. **PTH** ならば **P=BPP** が成立する。□

PTH を証明することは困難である。次の結果は関係 "$r<\mu(A_{e,x})$" の一つの評価を与えるものである。

定理 3.4. "$r<\mu(A_{e,x})$" は r, e, x に関し $DTIME(2^{poly})$ である。□

紙数の関係上その証明は省略する。より良い評価が望まれる。

文　　献

[AS 86] Ambos-Spies, K., Randomness, relativizations, and polynomial reducibilities, L.N. in C. S., 223 (1986), 23-34.

[BG 81] Bennett, C.H., and Gill, J., Relative to a random oracle A, $P^A \neq NP^A \neq co-NP^A$ with

probability 1, SIAM J. Computing. 10 (1981), 96-113.

[Pa 94] Papadimitriou, C.H., Computational Complexity, Addison-Wesley, Reading (1994), 523 pp.

[Ta 67] Tanaka, H., Some results in effective descriptive set theory, Publ. RIMS. Kyoto Univ., Ser. A, Vol. 3 (1967), 11-52.

[Ta 96] 田中尚夫，数学基礎論的手法の計算量理論への応用，数学，第48巻第4号（1996），372-384.