

オラクルと P 対 NP 問題

ごたんとう (@mathonigori)

2019 年 6 月 28 日

定理 1. $P^A = NP^A$ をみたすオラクル A が存在する.

証明. A として PSPACE 完全な言語をとる. A は PSPACE 完全なので多項式時間で PSPACE 問題を A へ帰着でき, $PSPACE \subseteq P^A$ が成立する. また, $P^A \subseteq NP^A$ が定義よりわかる. さらに, オラクル A への問い合わせに対する答えを計算する非決定性多項式領域 Turing 機械が存在することと $NP \subseteq NPSpace$ より $NP^A \subseteq NPSpace$ である. また, Savitch の定理より $NPSpace \subseteq PSPACE$. 以上より,

$$PSPACE \subseteq P^A \subseteq NP^A \subseteq NPSpace \subseteq PSPACE$$

であり, $P^A = NP^A$ と分かる. □

定理 2. $P^B \neq NP^B$ をみたすオラクル B が存在する.

証明. $M_1^?, M_2^?, \dots$ をすべてのオラクル付き Turing 機械が現れる列であって, 任意の $i \in \mathbb{N}$ について $M_i^?$ と同じ機械が無限回現れるものとする. 以下では再帰的に B_n, X_n を定義し, 最終的に $B = \bigcup B_n, L = \{0^n \mid \exists x \in B \text{ s.t. } |x| = n\}$ と定めることで $L \in NP^B \setminus P^B$ であることを示す.

(1) $n = 0$ のとき

$B_0 = X_0 = \emptyset$ と定める.

(2) $n = i - 1$ まで B_n, X_n が定まっているとき

まず, $X_i = X_{i-1}$ としておく. $M_i^{B_{i-1}}$ に入力として 0^i を与えて, $i^{\log i}$ ステップまで動作させる. 動作の中でオラクルへ文字列 x が B_{i-1} に入っているかの問い合わせがあるとき, $|x| \geq i$ であれば X_i を $X_i \cup \{x\}$ とする.

① $i^{\log i}$ ステップ以内に $M_i^{B_{i-1}}$ が 0^i を拒否した場合

$B_i := B_{i-1} \cup \{x \in \{0, 1\}^* \mid |x| = i, x \notin X_i\}$ と定義する. $\sum_{j=1}^i j^{\log j} < 2^i$ より $\{x \in \{0, 1\}^* \mid |x| = i, x \notin X_i\} \neq \emptyset$ をみたすので, あとで定義する L が $0^i \in L$ をみたすようになる.

② $i^{\log i}$ ステップ以内に $M_i^{B_{i-1}}$ が 0^i を受理した場合

$B_i := B_{i-1}$ と定義する. この定め方によって, あとで定義する L が $0^i \notin L$ をみたすようになる.

③ $i^{\log i}$ ステップ以内に $M_i^{B_{i-1}}$ が停止しなかった場合

$B_i := B_{i-1}$ と定義する.

(1), (2) から再帰的に B_n, X_n が定義された. ここで,

$$B := \bigcup B_n, L := \{0^n \mid \exists x \in B \text{ s.t. } |x| = n\}$$

と定義しよう. すると, 多項式時間 $p(n)$ で動く任意の M_i^B について, $L(M_i^B) \neq L$ が言える. まず, $n = i$ での定義を与えるときに①か②の場合であったならば, 入力を 0^i としたときを考えることで $L(M_i^B) \neq L$ が分かる. では, ③の場合ではどうだろうか. この場合は,

$$\exists I \in \mathbb{N} \text{ s.t. } I^{\log I} > p(I) \text{ かつ } M_I^B = M_i^B$$

であることから, $n = I$ で①か②の場合の定義をすることになり, 同じ機械 M_I^B について $L(M_I^B) \neq L$ と言える. よって任意の多項式時間オラクル Turing 機械が L を判定しないと分かり, $L \notin P^B$. また, 非決定的にある長さの文字列が A の元であるか問い合わせをすることができることから $L \in NP^B$ が言える. 以上から $P^B \neq NP^B$ が示された. \square

定理 1 と定理 2 より, オラクルの有無が影響しない手法では P 対 NP 問題を解くことができないとわかる.

参考文献

- [1] Christos H. Papadimitriou, "Computational Complexity. Addison-Wesley", pp.339 - 343, 1994.
- [2] Michael Sipser, "Introduction to the Theory of Computation", PWS Publishing, pp.318 - 321, 1997.