期末テストの解答と解説
Answers of Final Exam

上原 隆平 (Ryuhei UEHARA)
uehara@jaist.ac.jp

November 30th, 2007.

Problem 1: (正の) 自然数 $\mathbb{N}$ 上の関数 $f(n), g(n)$ に対し,

$$\exists c, d > 0, \forall n \in \mathbb{N}[f(n) \leq cg(n) + d]$$

が成立するとき, $f(n) = O(g(n))$ と記述する. また, $\overset{\infty}{\forall}\, n \in \mathbb{N}$ は「有限個の例外を除くすべての自然数 n」を表す. このとき

$$\exists c > 0, \overset{\infty}{\forall}\, n \in \mathbb{N}[f(n) \leq cg(n)] \to f(n) = O(g(n))$$

を証明せよ. (Let $f(n)$ and $g(n)$ be two functions over $\mathbb{N}$, set of (positive) natural numbers. We denote by $f(n) = O(g(n))$ if we have

$$\exists c, d > 0, \forall n \in \mathbb{N}[f(n) \leq cg(n) + d].$$

Now "$\overset{\infty}{\forall}\, n \in \mathbb{N}$" describes "all natural numbers n with finite exceptions." Then prove the following:

$$\exists c > 0, \overset{\infty}{\forall}\, n \in \mathbb{N}[f(n) \leq cg(n)] \to f(n) = O(g(n)).)$$

- 定義(Definition)

$$\exists c, d > 0, \forall n \in \mathbb{N}[f(n) \leq cg(n) + d] \leftrightarrow f(n) = O(g(n))$$

- 示すこと(We have to show)

$$\exists c > 0, \overset{\infty}{\forall}\, n \in \mathbb{N}[f(n) \leq cg(n)] \to f(n) = O(g(n))$$

解答例(Ans.)

f が自然な関数なら

$$d = f(n_{\max})$$

でよい。
(If f is a natural function, we can just let above.)

- 定義(Definition)

$$\exists c, d > 0, \forall n \in \mathbb{N}[f(n) \le cg(n) + d] \leftrightarrow f(n) = O(g(n))$$

- 仮定(Assumption) $\exists c > 0, \overset{\infty}{\forall} n \in \mathbb{N}[f(n) \le cg(n)]$ （＊）
- 結論(Conclusion) $f(n) = O(g(n))$

- 仮定より、有限個の例外を除いて式（＊）が成立する。
- 例外の最大値を $n_{\max}$ とする。

$$d = \max_{1 \le n \le n_{\max}} f(n)$$

とおけば、すべての n に対して

$$f(n) \le cg(n) + d$$

をえる。よって $f(n)=O(g(n))$ となる。

- By assumption, we have (*) with finite exceptions.
- Let $n_{\max}$ be the maximum of the exceptions. Then, letting

$$d = \max_{1 \le n \le n_{\max}} f(n)$$

we have $f(n) \le cg(n) + d$

for all n, which implies $f(n)=O(g(n))$.

Problem 2: どんな正定数 k に対しても，$2^n = O(n^k)$ とはならないことを証明せよ．(For any fixed positive constant k, prove that $2^n = O(n^k)$ does not hold.)

- コメント(Comments)
  - 2^n が多項式ではないことをしっかり理解してほしい。
  - I want to understand that 2^n is not polynomial.
  - 式に対する大局観を養ってほしい。
  - I want to you to have a wide view of equations.

証明（背理法による） (Proof by contradiction)

- ある正定数 k に対して $2^n=O(n^k)$ であったとする。このとき定義より、次をえる。
- We assume $2^n=O(n^k)$ for some positive constant k. Then, by definition,

$$\exists c, d > 0, \forall n \in \mathbb{N}[2^n \le cn^k + d]$$

証明（背理法による） (Proof by contradiction)

- ある正定数 k に対して $2^n=O(n^k)$ であったとする。このとき定義より、次をえる。
- We assume $2^n=O(n^k)$ for some positive constant k. Then, by definition,

$$\exists c, d > 0, \forall n \in \mathbb{N}[2^n \le cn^k + d]$$

c, d, k は正の定数なので、n を十分大きくとれば、正定数 k' に対して次をえる。
Since c, d, and k are positive constants, we have the following for some positive constant k' for sufficiently large n;

$$cn^k + d < cn^k + cn < cn^{k+1} < n^{k+2} = n^{k'}$$

よってある n_0 が存在して、次が成立。
Thus we have the following for some n_0;

$$\forall n > n_0[2^n < n^{k'}]$$

- k' は定数なので、ある n_1 が存在して、次が成立する。
- Since k' is const., we have the following for some n_1; $\forall n > n_1[k' < \frac{n}{\log n}]$
- ところがこのとき $\left(\frac{2^n}{n^{k'}}\right) > \left(\frac{2^{k'\log n}}{n^{k'}}\right) = 1$ となり、$2^n>n^{k'}$ となるので、矛盾。
- But then, $\left(\frac{2^n}{n^{k'}}\right) > \left(\frac{2^{k'\log n}}{n^{k'}}\right) = 1$ implies $2^n>n^{k'}$, which is a contradiction.

Problem 3: 3SAT とは 3 和積形の命題論理式 F が与えられた時に，$F() = 1$ にする割当が存在するかどうかを判定する問題である．3SAT がクラス $\mathcal{NP}$ に属することを示せ．(3SAT is a problem that asks for a given formula F in 3-conjunctive normal form, if there exists an assignment that makes $F() = 1$. Show that 3SAT is in the class $\mathcal{NP}$.)

- 次を満たす *w*, *R*(*x*,*w*) を示せばよい。
- It is sufficient to show *w* and *R*(*x*,*w*) such that…

$$\text{各} x \in \Sigma^* \text{で} x \in L \leftrightarrow \exists w \in \Sigma^* : |w| \leq q(|x|)[R(x,w)]$$

R(*x*,*w*)は多項式時間計算可能、*q* は多項式

R(*x*,*w*) is poly-time computable and *q* is a polynomial.

• *R*(*x*,*w*) = (*x* は *n* 変数の3積和標準形の命題論理式*F*を符号化したもの)∧ (*w* は *n* bit の 0,1 列)∧(*F*に*w*の値を入力すると値が1になる)
と定義すれば、|*w*|=*n* であり、R(x,w) は多項式時間判定可能である。よって3SATは$\mathcal{NP}$に属する。

• Define *R*(*x*,*w*) = (*x* is a code of a 3CNF formula *F* of *n* variables)∧ (*w* is an *n* bit sequence of 0/1) ∧(*F* becomes 1 by assign. *w*).
Then, |*w*|=*n* and *R*(*x*,*w*) can be determined in poly. time. Hence 3SAT∈$\mathcal{NP}$.

Problem 4: $\mathcal{EXP}$-困難な問題 A, $\mathcal{EXP}$-完全な問題 B, $\mathcal{NP}$-困難な問題 C, $\mathcal{NP}$-完全な問題 D がある．また $\mathcal{NP} \subseteq \mathcal{EXP}$ であるが，$\mathcal{NP} \neq \mathcal{EXP}$ かどうかはわかっていない．このとき，以下の問題のペアを次の 3 つに分類せよ．

1. 一方が他方より真に困難であるもの
2. 一方が他方と同じか，より困難であるもの
3. どちらがより困難であるか，条件だけからはわからないもの

(Let A, B, C, and D are $\mathcal{EXP}$-hard problem, $\mathcal{EXP}$-complete problem, $\mathcal{NP}$-hard problem, and $\mathcal{NP}$-complete problem, respectively. We have already known that $\mathcal{NP} \subseteq \mathcal{EXP}$, but we do not know whether $\mathcal{NP} \neq \mathcal{EXP}$. Then, divide the following pairs into three groups either

1. one is properly harder than the other one,
2. one is harder th
3. we cannot deter

)

(a) A v.s. B
(b) A v.s. C
(c) B v.s. C
(d) B v.s. D

- [復習] クラス$\mathcal{R}$と問題Aに対して、
  - Aが$\mathcal{R}$困難
    ⇔ どんな $B \in \mathcal{R}$ に対しても $B \leqq_m A$
    (Aは$\mathcal{R}$のどんな問題よりも同等か困難)
  - Aが$\mathcal{R}$完全
    ⇔ A は$\mathcal{R}$困難でかつ $A \in R$
    (Aは$\mathcal{R}$の中でもっとも困難)

Problem 4: $\mathcal{EXP}$-困難な問題 A，$\mathcal{EXP}$-完全な問題 B，$\mathcal{NP}$-困難な問題 C，$\mathcal{NP}$-完全な問題 D がある．また $\mathcal{NP} \subseteq \mathcal{EXP}$ であるが，$\mathcal{NP} \neq \mathcal{EXP}$ かどうかはわかっていない．このとき，以下の問題のペアを次の 3 つに分類せよ．

1. 一方が他方より真に困難であるもの
2. 一方が他方と同じか，より困難であるもの
3. どちらがより困難であるか，条件だけからはわからないもの

(Let A, B, C, and D are $\mathcal{EXP}$-hard problem, $\mathcal{EXP}$-complete problem, $\mathcal{NP}$-hard problem, and $\mathcal{NP}$-complete problem, respectively. We have already known that $\mathcal{NP} \subseteq \mathcal{EXP}$, but we do not know whether $\mathcal{NP} \neq \mathcal{EXP}$. Then, divide the following pairs into three groups either

1. one is properly harder than the other one,
2. one is hard
3. we cannot

)

(a) A v.s. B

(b) A v.s. C

(c) B v.s. C

(d) B v.s. D

- [Review] For a class $\mathcal{R}$ and problem *A*,
  - *A* is $\mathcal{R}$-hard

    ⇔ For any $B \in \mathcal{R}$, $B \leqq_m A$

    (*A* is harder than or equal to any problem in $\mathcal{R}$)
  - *A* is $\mathcal{R}$-complete

    ⇔ *A* is $\mathcal{R}$-hard and $A \in$ R

    (*A* is the hardest in $\mathcal{R}$)

Problem 4: $\mathcal{EXP}$-困難な問題 A, $\mathcal{EXP}$-完全な問題 B, $\mathcal{NP}$ … 完全な問題 D がある．
また $\mathcal{NP} \subseteq \mathcal{EXP}$ であるが, … か … き, 以下の問題のペア
を次の 3 つに分類せよ．

1. 一方が他方より真に困難であるもの

… からはわから …

○ $\mathcal{NP} \subseteq \mathcal{EXP}$

？ $\mathcal{NP} \neq \mathcal{EXP}$

… blem, $\mathcal{EXP}$-c … P-ha …
… have already … $\mathcal{EXP}$ …
know whether $\mathcal{NP} \neq \mathcal{EXP}$. Then, divide the following … ups either

1. one is properly harder than the other one,
2. one is harder th …
3. we cannot deter …

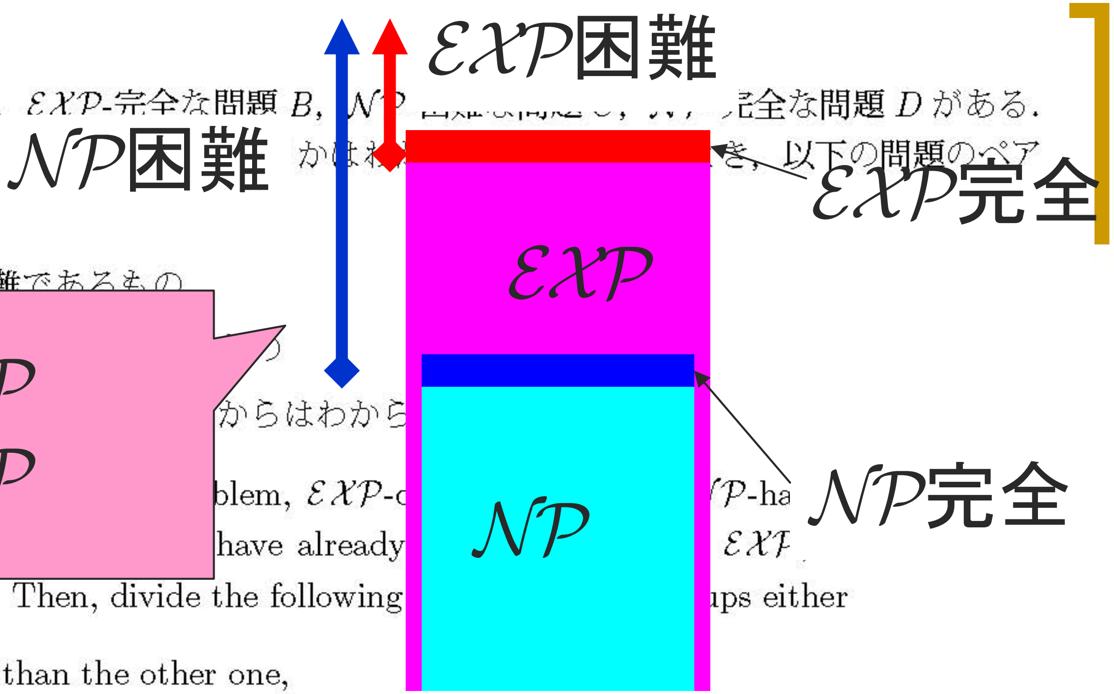
)

(a) A v.s. B

(b) A v.s. C

(c) B v.s. C

(d) B v.s. D



- [復習] クラス$\mathcal{R}$と問題Aに対して、
  - Aが$\mathcal{R}$困難

    ⇔ どんな $B \in \mathcal{R}$ に対しても $B \leq_m A$

    (Aは$\mathcal{R}$のどんな問題よりも同等か困難)
  - Aが$\mathcal{R}$完全

    ⇔ A は$\mathcal{R}$困難でかつ $A \in \mathrm{R}$

    (Aは$\mathcal{R}$の中でもっとも困難)

Problem 4: $\mathcal{EXP}$-困難な問題 A, $\mathcal{EXP}$-完全な問題 B, $\mathcal{N}$… 全な問題 D がある.
また $\mathcal{NP} \subseteq \mathcal{EXP}$ であるが, … き, 以下の問題のペア
を次の 3 つに分類せよ.

1. 一方が他方より真に困難であるもの
… からはわから…

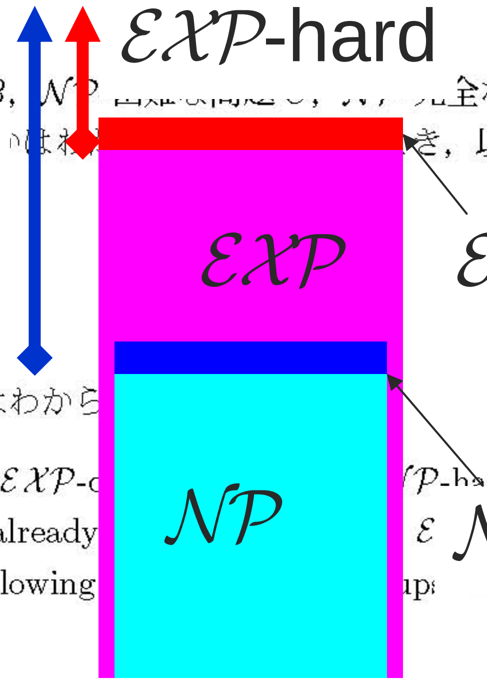
… blem, $\mathcal{EXP}$-c… $\mathcal{P}$-hard problem, and … have already … know whether $\mathcal{NP} \neq \mathcal{EXP}$. Then, divide the following … ups

1. one is properly harder than the other one,
2. one is hard…
3. we cannot …

)

(a) A v.s. B
(b) A v.s. C
(c) B v.s. C
(d) B v.s. D

○ $\mathcal{NP} \subseteq \mathcal{EXP}$
？ $\mathcal{NP} \neq \mathcal{EXP}$



- [Review] For a class $\mathcal{R}$ and problem A,
  - A is $\mathcal{R}$-hard
    ⇔ For any $B \in \mathcal{R}$, $B \leqq_m A$
    (A is harder than or equal to any problem in $\mathcal{R}$)
  - A is $\mathcal{R}$-complete
    ⇔ A is $\mathcal{R}$-hard and $A \in$ R
    (A is the hardest in $\mathcal{R}$)

Problem 4: $\mathcal{EXP}$-困難な問題 A, $\mathcal{EXP}$-完全な問題 B, $\mathcal{NP}$ ... 完全な問題 ... る.
また $\mathcal{NP} \subseteq \mathcal{EXP}$ であるが, ... かはわ ... き, 以下の問題のペア
を次の 3 つに分類せよ.

1. 一方が他方より真に困難であるもの

○ $\mathcal{NP} \subseteq \mathcal{EXP}$

? $\mathcal{NP} \neq \mathcal{EXP}$

... からはわから ...

... blem, $\mathcal{EXP}$-c ... $\mathcal{NP}$-ha ...
... have already ... $\mathcal{EXP}$ ...
know whether $\mathcal{NP} \neq \mathcal{EXP}$. Then, divide the following ... ups either

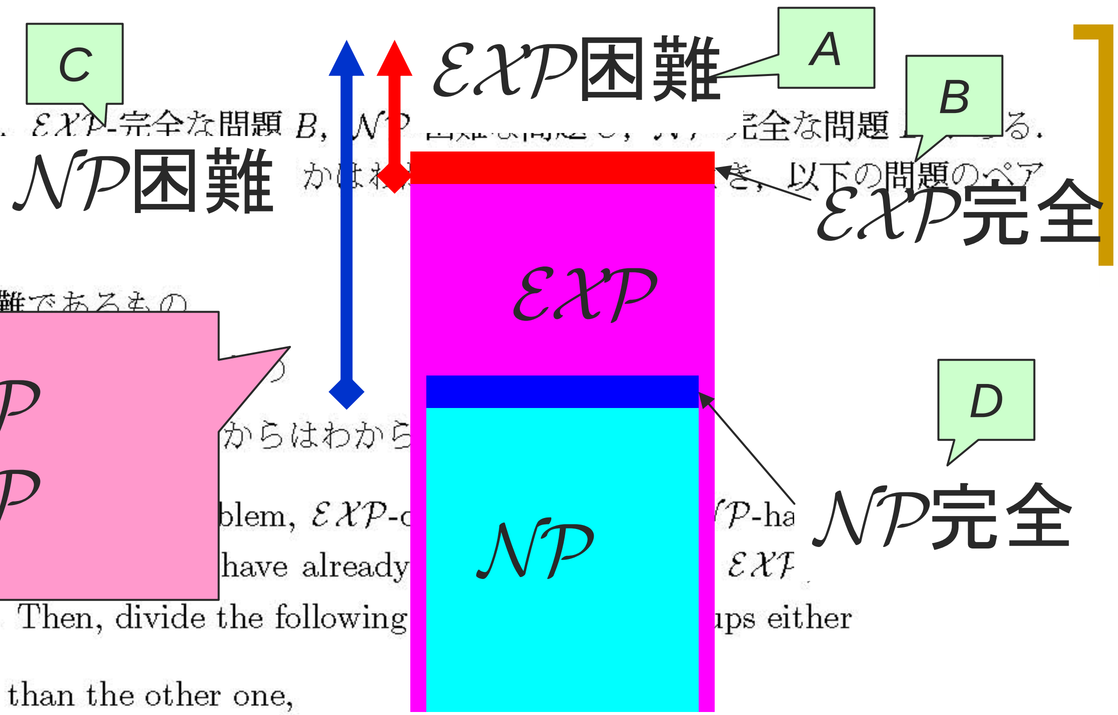
1. one is properly harder than the other one,
2. one is harder th...
3. we cannot deter...

)

(a) A v.s. B

(b) A v.s. C

(c) B v.s. C



- A($\mathcal{EXP}$-困難), B($\mathcal{EXP}$-完全), C($\mathcal{NP}$-困難), D($\mathcal{NP}$-完全)
- A v.s. B → 2. A は B と同等かより困難
- A v.s. C → 3. どちらが困難かわからない
- B v.s. C → 3. どちらが困難かわからない
- B v.s. D → 2. B は D と同等かより困難

1問正解: 1点
2問正解: 3点
3問正解: 5点

Problem 4: $\mathcal{EXP}$-困難な問題 A. $\mathcal{EXP}$-完全な問題 B, $\mathcal{N}$… …全な問題 D がある.
また $\mathcal{NP} \subseteq \mathcal{EXP}$ であるが, … …き, 以下の問題のペ…
を次の 3 つに分類せよ.

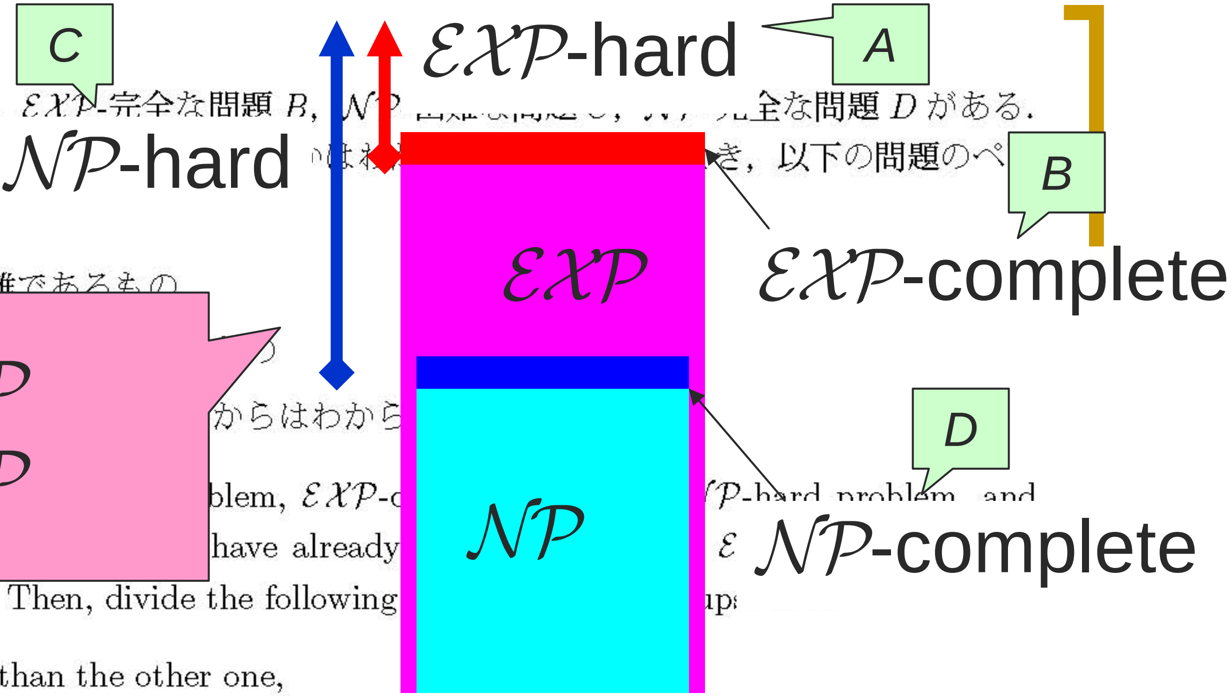
1. 一方が他方より真に困難であるもの
…からはわから…

…blem, $\mathcal{EXP}$-c… …$\mathcal{P}$-hard problem, and … have already … know whether $\mathcal{NP} \neq \mathcal{EXP}$. Then, divide the following … ups

1. one is properly harder than the other one,
2. one is harder …
3. we cannot det…

)

(a) A v.s. B
(b) A v.s. C
(c) B v.s. C



○ $\mathcal{NP} \subseteq \mathcal{EXP}$
? $\mathcal{NP} \neq \mathcal{EXP}$

- *A*($\mathcal{EXP}$-hard), *B*($\mathcal{EXP}$-complete), *C*($\mathcal{NP}$-hard), *D*($\mathcal{NP}$-complete)
- *A* v.s. *B* → 2. *A* is harder than or equal to *B*
- *A* v.s. *C* → 3. we cannot determine
- *B* v.s. *C* → 3. we cannot determine
- *B* v.s. *D* → 2. *B* is harder than or equal to *D*.

1 correct: 1 pts
2 corrects: 3 pts
3 corrects: 5 pts

Problem 5: $\mathcal{NP}$ 完全問題 A に対して，もし $A \in \mathcal{P}$ ならば $\mathcal{P} = \mathcal{NP}$ が成立することを証明せよ．(For any $\mathcal{NP}$-complete problem A, prove that $A \in \mathcal{P}$ implies $\mathcal{P} = \mathcal{NP}$.)

L

- 証明

- $\mathcal{P} \subseteq \mathcal{NP}$は自明なので、$\mathcal{NP} \subseteq \mathcal{P}$を示す。
- 任意の$L \in \mathcal{NP}$に対して$L \in \mathcal{P}$を示せばよい。
- $\mathcal{NP}$完全問題の定義より、$L \leq_m^P A$ $\quad x \in L \leftrightarrow h(x) \in A$
- よって多項式時間計算可能な関数 h が存在して
- 仮定よりAは多項式時間で判定可能。したがってLは多項式時間で判定可能なので、$L \in \mathcal{P}$.

Problem 5: $\mathcal{NP}$ 完全問題 A に対して，もし $A \in \mathcal{P}$ ならば $\mathcal{P} = \mathcal{NP}$ が成立することを証明せよ．(For any $\mathcal{NP}$-complete problem A, prove that $A \in \mathcal{P}$ implies $\mathcal{P} = \mathcal{NP}$.)

L

- Proof

• Since it is clear $\mathcal{P} \subseteq \mathcal{NP}$, we show $\mathcal{NP} \subseteq \mathcal{P}$.
• It is sufficient to show $L \in \mathcal{P}$ for any $L \in \mathcal{NP}$.
• By definition of $\mathcal{NP}$-completeness, $L \leq_m^P A$
• Thus there is a poly-time computable function *h* such that

$$x \in L \leftrightarrow h(x) \in A$$

• By assumption, *A* can be determined in poly-time. Hence *L* can be recognized in poly-time. Thus we have $L \in \mathcal{P}$.