

**Observation of the definitions of the classes...**

Def: Class  $\mathcal{P}$  (Chapter 5)  
 Set  $L$  is in the class  $\mathcal{P} \Leftrightarrow$   
 There exists a poly-time computable predicate  $R$  such that  
 for each  $x \in \Sigma^*$ ,  $x \in L \Leftrightarrow R(x)$

Def: Class  $\mathcal{NP}$  (Def 5.2)  
 Set  $L$  is in the class  $\mathcal{NP} \Leftrightarrow$   
 There exists a poly  $q$  and a poly-time computable pred.  $R$  s.t.  
 for each  $x \in \Sigma^*$ ,  $x \in L \Leftrightarrow \exists w \in \Sigma^*: |w| \leq q(|x|)[R(x,w)]$

Def: Class  $\text{co-}\mathcal{NP}$  (Theorem 5.5)  
 Set  $L$  is in the class  $\text{co-}\mathcal{NP} \Leftrightarrow$   
 There exists a poly  $q$  and a poly-time computable pred.  $R$  s.t.  
 for each  $x \in \Sigma^*$ ,  $x \in L \Leftrightarrow \forall w \in \Sigma^*: |w| \leq q(|x|)[R(x,w)]$

**計算量クラス間の定義を概観すると...**

クラス  $\mathcal{P}$  の定義 (5章)  
 集合  $L$  がクラス  $\mathcal{P}$  に入る  $\Leftrightarrow$   
 以下を満たす多項式時間計算可能述語  $R$  が存在:  
 各  $x \in \Sigma^*$  で  $x \in L \Leftrightarrow R(x)$

クラス  $\mathcal{NP}$  の定義 (定義 5.2)  
 集合  $L$  がクラス  $\mathcal{NP}$  に入る  $\Leftrightarrow$   
 以下を満たす多項式  $q$  と多項式時間計算可能述語  $R$  が存在:  
 各  $x \in \Sigma^*$  で  $x \in L \Leftrightarrow \exists w \in \Sigma^*: |w| \leq q(|x|)[R(x,w)]$

クラス  $\text{co-}\mathcal{NP}$  の定義 (定理 5.5)  
 集合  $L$  がクラス  $\text{co-}\mathcal{NP}$  に入る  $\Leftrightarrow$   
 以下を満たす多項式  $q$  と多項式時間計算可能述語  $R$  が存在:  
 各  $x \in \Sigma^*$  で  $x \in L \Leftrightarrow \forall w \in \Sigma^*: |w| \leq q(|x|)[R(x,w)]$

**Theorem 5.9**

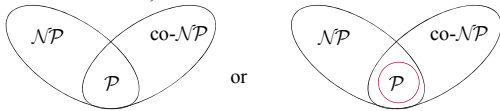
- (1)  $\mathcal{NP} \subseteq \text{co-}\mathcal{NP} \rightarrow \mathcal{NP} = \text{co-}\mathcal{NP}$
- (2)  $\text{co-}\mathcal{NP} \subseteq \mathcal{NP} \rightarrow \mathcal{NP} = \text{co-}\mathcal{NP}$
- (3)  $\mathcal{NP} \neq \text{co-}\mathcal{NP} \rightarrow \mathcal{P} \neq \mathcal{NP}$

12/12

Contraposition:  $\mathcal{P} = \mathcal{NP} \rightarrow \mathcal{NP} = \text{co-}\mathcal{NP}$

If we assume  $\mathcal{P} = \mathcal{NP}$ , for any  $L$  we have  
 $L \in \mathcal{NP} \Leftrightarrow L \in \mathcal{P} \quad (\mathcal{P} = \mathcal{NP})$   
 $\Leftrightarrow L \in \mathcal{P} \quad (\text{Exercise 5.5})$   
 $\Leftrightarrow L \in \underline{\mathcal{NP}} \quad (\mathcal{P} = \mathcal{NP})$   
 $\Leftrightarrow L (= \underline{L}) \in \text{co-}\mathcal{NP} \quad (\text{Definition 5.3})$   
 $\therefore \mathcal{NP} = \text{co-}\mathcal{NP}$  Q.E.D.

If  $\mathcal{NP} \neq \text{co-}\mathcal{NP}$  is true,



**定理 5.9.**

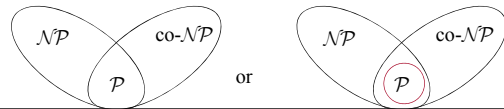
- (1)  $\mathcal{NP} \subseteq \text{co-}\mathcal{NP} \rightarrow \mathcal{NP} = \text{co-}\mathcal{NP}$
- (2)  $\text{co-}\mathcal{NP} \subseteq \mathcal{NP} \rightarrow \mathcal{NP} = \text{co-}\mathcal{NP}$
- (3)  $\mathcal{NP} \neq \text{co-}\mathcal{NP} \rightarrow \mathcal{P} \neq \mathcal{NP}$ .

12/12

対偶:  $\mathcal{P} = \mathcal{NP} \rightarrow \mathcal{NP} = \text{co-}\mathcal{NP}$

$\mathcal{P} = \mathcal{NP}$  と仮定すると、すべての  $L$  に対し  
 $L \in \mathcal{NP} \Leftrightarrow L \in \mathcal{P} \quad (\mathcal{P} = \mathcal{NP} \text{ より})$   
 $\Leftrightarrow L \in \mathcal{P} \quad (\text{演習問題 5.5})$   
 $\Leftrightarrow L \in \underline{\mathcal{NP}} \quad (\mathcal{P} = \mathcal{NP} \text{ より})$   
 $\Leftrightarrow L (= \underline{L}) \in \text{co-}\mathcal{NP} \quad (\text{定義 5.3 より})$   
 $\therefore \mathcal{NP} = \text{co-}\mathcal{NP}$  証明終

$\mathcal{NP} \neq \text{co-}\mathcal{NP}$  が正しいと



**Chapter 6. Analysis on Polynomial-Time Computability**

1/14

**6.1. Polynomial-time Reducibility**

**Def.6.1:**

Let  $A$  and  $B$  be arbitrary sets.

(1) function  $h: A \rightarrow B$ : **polynomial-time reduction**

- $\Leftrightarrow$  (a)  $h$  is a total function from  $\Sigma^*$  onto  $\Sigma^*$
- (b)  $x \in \Sigma^*[x \in A \leftrightarrow h(x) \in B]$
- (c)  $h$  is polynomial-time computable.

(2) When there is a polynomial-time reduction from  $A$  to  $B$ , we say  $A$  is **polynomial-time reducible to  $B$** .

Then, we denote by

$$A \leq_m^p B$$

**第6章 多項式時間計算可能性の分析**

1/14

**6.1. 多項式時間還元可能性**

**定義 6.1:**

$A$  と  $B$  を任意の集合とする.

(1) 関数  $h: A \rightarrow B$ : **多項式時間還元** (polynomial-time reduction)

- $\Leftrightarrow$  (a)  $h$  は  $\Sigma^*$  から  $\Sigma^*$  への全域的関数
- (b)  $x \in \Sigma^*[x \in A \leftrightarrow h(x) \in B]$
- (c)  $h$  は多項式時間計算可能.

(2)  $A$  から  $B$  への多項式時間還元が存在するとき,

$A$  は  $B$  へ **多項式時間還元可能** という (polynomial time reducible).

このとき、次のように書く:

$$A \leq_m^p B$$

2/14

$A \leq_m^P B$  within polynomial time, hardness of  $A \leq$  that of  $B$

**Theorem 6.1**  $A \leq_m^P B$  leads to,

- (1)  $B \in \mathcal{P} \rightarrow A \in \mathcal{P}$ .
- (2)  $B \in \mathcal{NP} \rightarrow A \in \mathcal{NP}$ .
- (3)  $B \in \text{co-}\mathcal{NP} \rightarrow A \in \text{co-}\mathcal{NP}$ .
- (4)  $B \in \mathcal{EXPTIME} \rightarrow A \in \mathcal{EXPTIME}$ .

Note: class  $\mathcal{E}$  is exceptional. Generally,  $B \in \mathcal{E} \rightarrow A \in \mathcal{E}$  is not true.

**Ex.6.2:** If we define  $\text{ONE} \equiv \{1\}$ , for each set  $L$  in  $\mathcal{P}$  we have  $L \leq_m^P \text{ONE}$

If we define  $h(x) \equiv \begin{cases} 1, & \text{if } x \in L, \\ 0, & \text{otherwise} \end{cases}$

- (1)  $h$  is a total function from  $\Sigma^*$  onto  $\Sigma^*$ .
- (2)  $x \in \Sigma^* [x \in L \leftrightarrow h(x) \in \text{ONE}]$
- (3)  $h$  is polynomial-time computable (so is computation  $L \in \mathcal{P} \rightarrow x \in L$ )

2/14

$A \leq_m^P B$  多項式時間の範囲内では、 $A$ の難しさ  $\leq$   $B$ の難しさ

**定理6.1.**  $A \leq_m^P B$  のとき,

- (1)  $B \in \mathcal{P} \rightarrow A \in \mathcal{P}$ .
- (2)  $B \in \mathcal{NP} \rightarrow A \in \mathcal{NP}$ .
- (3)  $B \in \text{co-}\mathcal{NP} \rightarrow A \in \text{co-}\mathcal{NP}$ .
- (4)  $B \in \mathcal{EXPTIME} \rightarrow A \in \mathcal{EXPTIME}$ .

補注: クラス  $\mathcal{E}$  は例外. 一般には,  $B \in \mathcal{E} \rightarrow A \in \mathcal{E}$  とはならない.

**例6.2:**  $\text{ONE} \equiv \{1\}$  と定義するとき, クラス  $\mathcal{P}$  のすべての集合  $L$  について  $L \leq_m^P \text{ONE}$  が成り立つ.

$h(x) \equiv \begin{cases} 1, & x \in L \text{ のとき,} \\ 0, & \text{その他のとき} \end{cases}$

と定義すると, (1)  $h$  は  $\Sigma^*$  から  $\Sigma^*$  への全域的関数.  
 (2)  $x \in \Sigma^* [x \in L \leftrightarrow h(x) \in \text{ONE}]$   
 (3)  $h$  は多項式時間計算可能 ( $L \in \mathcal{P} \rightarrow x \in L$  の判定も多項式時間内)

3/14

**Theorem 6.2:**  $A, B, C$ : arbitrary sets

- (1)  $A \leq_m^P A$
- (2)  $A \leq_m^P B \wedge B \leq_m^P C \rightarrow A \leq_m^P C$

Def:  $A \equiv_m^P B \leftrightarrow A \leq_m^P B \wedge B \leq_m^P A$   
 $\equiv_m^P$  is an equivalence relation.

3/14

**定理6.2:**  $A, B, C$ : 任意の集合

- (1)  $A \leq_m^P A$
- (2)  $A \leq_m^P B \wedge B \leq_m^P C \rightarrow A \leq_m^P C$

定義:  $A \equiv_m^P B \leftrightarrow A \leq_m^P B \wedge B \leq_m^P A$   
 $\equiv_m^P$  は同値関係

4/14

**Relation among satisfiability problems of propositional expressions**

2SAT (propositional satisfiability problem)  
 3SAT  
 SAT  
 ExSAT (extended propositional satisfiability problem)

$2\text{SAT} \leq_m^P 3\text{SAT}$

- at most  $k$ ...trivial
- exactly  $k$ ...
- easy if you can repeat the same literal.
- the other case ... good exercise!

Similarly,  
 $3\text{SAT} \leq_m^P \text{SAT} \leq_m^P \text{ExSAT}$   
 $2\text{SAT} \leq_m^P 3\text{SAT} \leq_m^P \text{SAT} \leq_m^P \text{ExSAT}$  (6.1)

Here, if we can show  
 $\text{ExSAT} \leq_m^P 3\text{SAT}$

then we have  
 $3\text{SAT} \equiv_m^P \text{SAT} \equiv_m^P \text{ExSAT}$

4/14

**命題論理式の充足可能性問題の間の関係**

2SAT (命題論理式充足性問題: 二和積形式)  
 3SAT (命題論理式充足性問題: 三和積形式)  
 SAT (命題論理式充足性問題)  
 ExSAT (拡張命題論理式充足性問題)

$2\text{SAT} \leq_m^P 3\text{SAT}$

- 高々  $k$  個 ... 自明
- ちょうど  $k$  個 ...
- 同じリテラルを使ってよいなら簡単。
- だめなら... 考えてみよう!

同様に,  
 $3\text{SAT} \leq_m^P \text{SAT} \leq_m^P \text{ExSAT}$   
 $2\text{SAT} \leq_m^P 3\text{SAT} \leq_m^P \text{SAT} \leq_m^P \text{ExSAT}$  (6.1)

ここで  
 $\text{ExSAT} \leq_m^P 3\text{SAT}$

であることを示せると,  
 $3\text{SAT} \equiv_m^P \text{SAT} \equiv_m^P \text{ExSAT}$   
 となる.

Ex. 6.3: Reduction from ExSAT to 3SAT

5/14

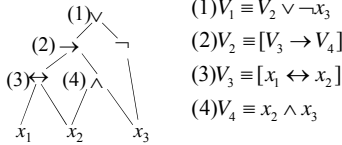
$$E_1(x_1, x_2, x_3) \equiv [[x_1 \leftrightarrow x_2] \rightarrow [x_2 \wedge x_3]] \vee \neg x_3$$

$$F_1(x_1, x_2, x_3) \equiv U_1 \wedge [U_1 \leftrightarrow [U_2 \vee \neg x_3]] \wedge [U_2 \leftrightarrow [U_3 \rightarrow U_4]]$$

$$\wedge [U_3 \leftrightarrow [x_1 \leftrightarrow x_2]] \wedge [U_4 \leftrightarrow [x_2 \wedge x_3]]$$

Then,  $[E_1 \text{ is satisfiable}] \leftrightarrow [F_1 \text{ is satisfiable}]$  (6.2)  
 $F_1$  is easier to be converted to 3SAT form.

How to construct  $F_1$



To construct  $F_1$  we let  $V_i \rightarrow U_i$ , and connect expressions of  $V_i$  by  $\wedge$

例6.3: ExSATから3SATへの還元

5/14

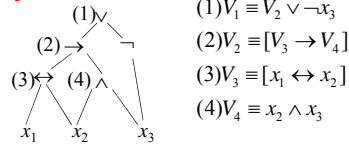
$$E_1(x_1, x_2, x_3) \equiv [[x_1 \leftrightarrow x_2] \rightarrow [x_2 \wedge x_3]] \vee \neg x_3$$

$$F_1(x_1, x_2, x_3) \equiv U_1 \wedge [U_1 \leftrightarrow [U_2 \vee \neg x_3]] \wedge [U_2 \leftrightarrow [U_3 \rightarrow U_4]]$$

$$\wedge [U_3 \leftrightarrow [x_1 \leftrightarrow x_2]] \wedge [U_4 \leftrightarrow [x_2 \wedge x_3]]$$

このとき,  $[E_1 \text{が充足可能}] \leftrightarrow [F_1 \text{が充足可能}]$  (6.2)  
 $F_1$ は三和積形式に直しやすい形になっている.

$F_1$ の構成方法



$F_1$ を構成するために,  $V_i \rightarrow U_i$ とし,  $V_i$ の定義式を  $\wedge$ で結ぶ

From the construction of  $F_1$

6/14

- (1)  $F_1$  is never true unless each  $U_i$  is  $V_i(x_1, x_2, x_3)$ .
- (2) If each  $U_i$  is  $V_i(x_1, x_2, x_3)$ , we have  $F_1 = E_1$

The above properties are proved by using induction.  
 proof is omitted.

Conversion to 3SAT form

$$a \rightarrow b = \neg a \vee b$$

$$a \leftrightarrow b = (a \rightarrow b) \wedge (b \rightarrow a) = [\neg a \vee b] \wedge [\neg b \vee a]: \text{useful relations}$$

$$U_1 \leftrightarrow [U_2 \vee \neg x_3] = [\neg U_1 \vee U_2 \vee \neg x_3] \wedge [U_1 \vee \neg [U_2 \vee \neg x_3]]$$

$$= [\neg U_1 \vee U_2 \vee \neg x_3] \wedge [U_1 \vee [\neg U_2 \wedge x_2]]$$

$$= [\neg U_1 \vee U_2 \vee \neg x_3] \wedge [U_1 \vee \neg U_2] \wedge [U_1 \vee x_2]$$

$$= [\neg U_1 \vee U_2 \vee \neg x_3] \wedge [U_1 \vee \neg U_2] \wedge [U_1 \vee x_2 \vee x_2]$$

Others are similar.  
 Thus, every 3SAT form is converted.

$F_1$ の構成方法より,

6/14

- (1) 各  $U_i$  の値を  $V_i(x_1, x_2, x_3)$  としない限り,  $F_1$  は真にはならない.
- (2) 各  $U_i$  の値を  $V_i(x_1, x_2, x_3)$  としたとき,  $F_1 = E_1$

上の性質が成り立つことは, 帰納法を用いるなどして証明可能.  
 証明は省略.

三和積形式への変換

$$a \rightarrow b = \neg a \vee b$$

$$a \leftrightarrow b = (a \rightarrow b) \wedge (b \rightarrow a) = [\neg a \vee b] \wedge [\neg b \vee a] \text{であることを用いる.}$$

$$U_1 \leftrightarrow [U_2 \vee \neg x_3] = [\neg U_1 \vee U_2 \vee \neg x_3] \wedge [U_1 \vee \neg [U_2 \vee \neg x_2]]$$

$$= [\neg U_1 \vee U_2 \vee \neg x_3] \wedge [U_1 \vee [\neg U_2 \wedge x_2]]$$

$$= [\neg U_1 \vee U_2 \vee \neg x_3] \wedge [U_1 \vee \neg U_2] \wedge [U_1 \vee x_2]$$

$$= [\neg U_1 \vee U_2 \vee \neg x_3] \wedge [U_1 \vee \neg U_2] \wedge [U_1 \vee x_2 \vee x_2]$$

他も同様.  
 よって, すべて三和積形式に変形できることがわかる.

6.2. Completeness based on Polynomial-time Reducibility

7/14

6.2.1. Definition of Completeness and its Basic Properties

Def.6.2: For a class  $C$ , if a set  $A$  satisfies the following conditions, then it is called  $C$ -complete (under  $\leq_m^P$ )

- (a)  $\forall L \in C [L \leq_m^P A]$
- (b)  $A \in C$

Note: Sets satisfying the condition (a) are called  $C$ -hard.

6.2. 多項式時間還元可能性に基づく完全性

7/14

6.2.1. 完全性の定義とその基本的性質

定義6.2: 計算量クラス  $C$  に対し, 集合  $A$  が次の条件を満たすとき, それを ( $\leq_m^P$  の下で)  $C$ -完全という.

- (a)  $\forall L \in C [L \leq_m^P A]$
- (b)  $A \in C$

補注: 条件(a)を満たす集合は  $C$ -困難.

## 6.2. Completeness based on Polynomial-time Reducibility

### 6.2.1. Definition of Completeness and its Basic Properties

Ex.6.5. Examples of  $\mathcal{NP}$ -complete sets

3SAT, SAT, ExSAT, DHAM, KNAP, BIN, VC, etc  
 $\mathcal{EXP}$ -complete sets  
 EVAL-IN-E, HALT-IN-E, etc.

EVAL - IN - E:

Input :  $\langle a, x, \bar{t} \rangle$

$a$  : the code of a program with 1 input,  $x \in \Sigma^*, \bar{t} \geq 0$

Output :  $eval-in-time(a, x, \bar{t}) = accept?$

## 6.2. 多項式時間還元可能性に基づく完全性

### 6.2.1. 完全性の定義とその基本的性質

例6.5. クラス  $\mathcal{NP}$  の完全集合の例

3SAT, SAT, ExSAT, DHAM, KNAP, BIN, VC など  
 $\mathcal{EXP}$  の完全集合  
 EVAL-IN-E, HALT-IN-E など

EVAL - IN - E:

入力 :  $\langle a, x, \bar{t} \rangle$

$a$  : 1入力プログラムのコード,  $x \in \Sigma^*, \bar{t} \geq 0$

出力 :  $eval-in-time(a, x, \bar{t}) = accept?$

Theorem 6.3. For any  $\mathcal{C}$ -hard (or  $\mathcal{C}$ -complete) set  $A$ ,

- |   |  |
|---|--|
| (1) $A \in \mathcal{P} \rightarrow \mathcal{C} \subseteq \mathcal{P}$                       | CP: $\mathcal{C} \not\subseteq \mathcal{P} \rightarrow A \notin \mathcal{P}$                       |
| (2) $A \in \mathcal{NP} \rightarrow \mathcal{C} \subseteq \mathcal{NP}$                     | CP: $\mathcal{C} \not\subseteq \mathcal{NP} \rightarrow A \notin \mathcal{NP}$                     |
| (3) $A \in \text{co-}\mathcal{NP} \rightarrow \mathcal{C} \subseteq \text{co-}\mathcal{NP}$ | CP: $\mathcal{C} \not\subseteq \text{co-}\mathcal{NP} \rightarrow A \notin \text{co-}\mathcal{NP}$ |
| (4) $A \in \mathcal{EXP} \rightarrow \mathcal{C} \subseteq \mathcal{EXP}$                   | CP: $\mathcal{C} \not\subseteq \mathcal{EXP} \rightarrow A \notin \mathcal{EXP}$                   |

Proof:

CP: contraposition

(1) Let  $B$  be any  $\mathcal{C}$ -set. Then, since  $A$  is  $\mathcal{C}$ -hard,

$B \leq_m^P A$  and by the assumption  $A \in \mathcal{P}$  we have  $B \in \mathcal{P}$  (Th. 6.1)

(2), (3), (4) are similar.

定理6.3. 任意の  $\mathcal{C}$ -困難集合 (含:  $\mathcal{C}$ -完全集合)  $A$  に対し,

- |   |  |
|---|--|
| (1) $A \in \mathcal{P} \rightarrow \mathcal{C} \subseteq \mathcal{P}$                       | 対偶は $\mathcal{C} \not\subseteq \mathcal{P} \rightarrow A \notin \mathcal{P}$                       |
| (2) $A \in \mathcal{NP} \rightarrow \mathcal{C} \subseteq \mathcal{NP}$                     | 対偶は $\mathcal{C} \not\subseteq \mathcal{NP} \rightarrow A \notin \mathcal{NP}$                     |
| (3) $A \in \text{co-}\mathcal{NP} \rightarrow \mathcal{C} \subseteq \text{co-}\mathcal{NP}$ | 対偶は $\mathcal{C} \not\subseteq \text{co-}\mathcal{NP} \rightarrow A \notin \text{co-}\mathcal{NP}$ |
| (4) $A \in \mathcal{EXP} \rightarrow \mathcal{C} \subseteq \mathcal{EXP}$                   | 対偶は $\mathcal{C} \not\subseteq \mathcal{EXP} \rightarrow A \notin \mathcal{EXP}$                   |

証明:

(1)  $B$  を任意の  $\mathcal{C}$  集合とすると,  $A$  は  $\mathcal{C}$ -困難だから,

$B \leq_m^P A$  一方,  $A \in \mathcal{P}$  の仮定より,  $B \in \mathcal{P}$  (定理6.1)

(2), (3), (4) も同様

Theorem 6.3. For any  $\mathcal{C}$ -hard (or  $\mathcal{C}$ -complete) set  $A$ ,

- |   |  |
|---|--|
| (1) $A \in \mathcal{P} \rightarrow \mathcal{C} \subseteq \mathcal{P}$                       | CP: $\mathcal{C} \not\subseteq \mathcal{P} \rightarrow A \notin \mathcal{P}$                       |
| (2) $A \in \mathcal{NP} \rightarrow \mathcal{C} \subseteq \mathcal{NP}$                     | CP: $\mathcal{C} \not\subseteq \mathcal{NP} \rightarrow A \notin \mathcal{NP}$                     |
| (3) $A \in \text{co-}\mathcal{NP} \rightarrow \mathcal{C} \subseteq \text{co-}\mathcal{NP}$ | CP: $\mathcal{C} \not\subseteq \text{co-}\mathcal{NP} \rightarrow A \notin \text{co-}\mathcal{NP}$ |
| (4) $A \in \mathcal{EXP} \rightarrow \mathcal{C} \subseteq \mathcal{EXP}$                   | CP: $\mathcal{C} \not\subseteq \mathcal{EXP} \rightarrow A \notin \mathcal{EXP}$                   |

Theorem 5.9.

- (1)  $\mathcal{NP} \subseteq \text{co-}\mathcal{NP}$   
 $\rightarrow \mathcal{NP} = \text{co-}\mathcal{NP}$

Ex.6.6: Meaning of Theorem 6.3 (class  $\mathcal{NP}$ )

Let  $A$  be  $\mathcal{NP}$ -complete set.

By the contraposition of Theorem 6.3(1) we have

$\mathcal{NP} \neq \mathcal{P} \rightarrow A \notin \mathcal{P}$

By the contraposition of Theorem 6.3(3) and that of Theorem 5.9(1),

$A \notin \text{co-}\mathcal{NP}$

That is,  $\mathcal{NP}$ -complete sets are  $\mathcal{NP}$ -sets that cannot be recognized in polynomial time unless  $\mathcal{P} = \mathcal{NP}$ .

定理6.3. 任意の  $\mathcal{C}$ -困難集合 (含:  $\mathcal{C}$ -完全集合)  $A$  に対し,

- |   |  |
|---|--|
| (1) $A \in \mathcal{P} \rightarrow \mathcal{C} \subseteq \mathcal{P}$                       | 対偶は $\mathcal{C} \not\subseteq \mathcal{P} \rightarrow A \notin \mathcal{P}$                       |
| (2) $A \in \mathcal{NP} \rightarrow \mathcal{C} \subseteq \mathcal{NP}$                     | 対偶は $\mathcal{C} \not\subseteq \mathcal{NP} \rightarrow A \notin \mathcal{NP}$                     |
| (3) $A \in \text{co-}\mathcal{NP} \rightarrow \mathcal{C} \subseteq \text{co-}\mathcal{NP}$ | 対偶は $\mathcal{C} \not\subseteq \text{co-}\mathcal{NP} \rightarrow A \notin \text{co-}\mathcal{NP}$ |
| (4) $A \in \mathcal{EXP} \rightarrow \mathcal{C} \subseteq \mathcal{EXP}$                   | 対偶は $\mathcal{C} \not\subseteq \mathcal{EXP} \rightarrow A \notin \mathcal{EXP}$                   |

例6.6. 定理6.3の意味 (クラス  $\mathcal{NP}$ )

$A$  を  $\mathcal{NP}$ -完全集合とする.

定理6.3(1)の対偶より,

$\mathcal{NP} \neq \mathcal{P} \rightarrow A \notin \mathcal{P}$

定理6.3(3)の対偶と定理5.9(1)の対偶より,

$A \notin \text{co-}\mathcal{NP}$

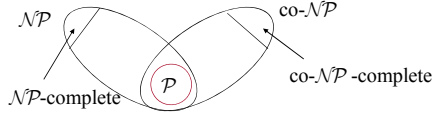
つまり,  $\mathcal{NP}$ -完全集合は  $\mathcal{P} \neq \mathcal{NP}$  である限り,  
 多項式時間では認識できない.

定理5.9.

- (1)  $\mathcal{NP} \subseteq \text{co-}\mathcal{NP} \rightarrow \mathcal{NP} = \text{co-}\mathcal{NP}$

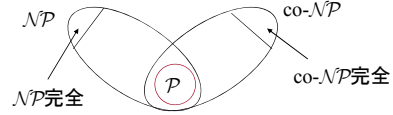
$\mathcal{NP}$ -complete sets are  $\mathcal{NP}$ -sets that do not belong to  $\mathcal{NP} \cap \text{co-}\mathcal{NP}$  unless  $\mathcal{P} = \mathcal{NP}$ .

11/14



$\mathcal{NP}$ -完全集合は  $\mathcal{P} \neq \mathcal{NP}$  である限り、 $\mathcal{NP} \cap \text{co-}\mathcal{NP}$  には入らない  $\mathcal{NP}$  集合である。

11/14



**Ex. 6.7.** Meaning of Theorem 6.3 (class  $\mathcal{EXP}$ )

12/14

Let  $D$  be any  $\mathcal{EXP}$ -complete set.

Contraposition of Theorem 6.3(1)

$(C \not\subseteq \mathcal{P} \rightarrow A \notin \mathcal{P}, \text{ where } \mathcal{EXP} \not\subseteq \mathcal{P} \rightarrow D \notin \mathcal{P})$

$\mathcal{P} \neq \mathcal{EXP} \rightarrow \mathcal{EXP} \not\subseteq \mathcal{P} (\because \mathcal{P} \subseteq \mathcal{EXP}) \rightarrow D \notin \mathcal{P}$

Contraposition of Theorem 6.3(2)  $(C \not\subseteq \mathcal{NP} \rightarrow A \notin \mathcal{NP},$

Here,  $\mathcal{EXP} \not\subseteq \mathcal{NP} \rightarrow D \notin \mathcal{NP})$

$\mathcal{NP} \neq \mathcal{EXP} \rightarrow \mathcal{EXP} \not\subseteq \mathcal{NP} (\because \mathcal{NP} \subseteq \mathcal{EXP}) \rightarrow D \notin \mathcal{NP}$

Contraposition of Theorem 6.3(3)  $(C \not\subseteq \text{co-}\mathcal{NP} \rightarrow A \notin \text{co-}\mathcal{NP},$

here,  $\mathcal{EXP} \not\subseteq \text{co-}\mathcal{NP} \rightarrow D \notin \text{co-}\mathcal{NP})$

$\text{co-}\mathcal{NP} \neq \mathcal{EXP} \rightarrow \mathcal{EXP} \not\subseteq \text{co-}\mathcal{NP} \rightarrow D \notin \text{co-}\mathcal{NP}$

But, by Theorem 5.7, since we know  $\mathcal{P} \subseteq \mathcal{EXP}$ , we have  $D \notin \mathcal{P}$ .

$\mathcal{EXP}$ -complete sets are not computable in polynomial time.

**例6.7.** 定理6.3の意味(クラス $\mathcal{EXP}$ )

12/14

$D$ を $\mathcal{EXP}$ -完全集合とする。

定理6.3(1)の対偶  $(C \not\subseteq \mathcal{P} \rightarrow A \notin \mathcal{P}, \text{ここでは } \mathcal{EXP} \not\subseteq \mathcal{P} \rightarrow D \notin \mathcal{P})$

$\mathcal{P} \neq \mathcal{EXP} \rightarrow \mathcal{EXP} \not\subseteq \mathcal{P} (\because \mathcal{P} \subseteq \mathcal{EXP}) \rightarrow D \notin \mathcal{P}$

定理6.3(2)の対偶  $(C \not\subseteq \mathcal{NP} \rightarrow A \notin \mathcal{NP},$

ここでは  $\mathcal{EXP} \not\subseteq \mathcal{NP} \rightarrow D \notin \mathcal{NP})$

$\mathcal{NP} \neq \mathcal{EXP} \rightarrow \mathcal{EXP} \not\subseteq \mathcal{NP} (\because \mathcal{NP} \subseteq \mathcal{EXP}) \rightarrow D \notin \mathcal{NP}$

定理6.3(3)の対偶  $(C \not\subseteq \text{co-}\mathcal{NP} \rightarrow A \notin \text{co-}\mathcal{NP},$

ここでは  $\mathcal{EXP} \not\subseteq \text{co-}\mathcal{NP} \rightarrow D \notin \text{co-}\mathcal{NP})$

$\text{co-}\mathcal{NP} \neq \mathcal{EXP} \rightarrow \mathcal{EXP} \not\subseteq \text{co-}\mathcal{NP} \rightarrow D \notin \text{co-}\mathcal{NP}$

ところが定理5.7から  $\mathcal{P} \subseteq \mathcal{EXP}$  であるから、 $D \notin \mathcal{P}$ .

$\mathcal{EXP}$ -完全集合は多項式時間では計算不可能。

**Theorem 6.4.**  $A$ : any  $\mathcal{C}$ -complete set

13/14

For any set  $B$  we have

(1)  $A \leq_m^p B \rightarrow B$  is  $\mathcal{C}$ -hard.

(2)  $A \leq_m^p B \wedge B \in \mathcal{C} \rightarrow B$  is  $\mathcal{C}$ -complete.

Proof:

By Def. 6.2  $\forall L \in \mathcal{C}[L \leq_m^p A]$

By Theorem 6.2,  $L \leq_m^p A \wedge A \leq_m^p B \rightarrow L \leq_m^p B$

Therefore,  $\forall L \in \mathcal{C}[L \leq_m^p B]$

That is,  $B$  is  $\mathcal{C}$ -hard.

**定理6.4.**  $A$ : 任意の $\mathcal{C}$ -完全集合

13/14

すべての集合 $B$ に対し、

(1)  $A \leq_m^p B \rightarrow B$ は $\mathcal{C}$ -困難。

(2)  $A \leq_m^p B \wedge B \in \mathcal{C} \rightarrow B$ は $\mathcal{C}$ -完全。

証明:

定義6.2より,  $\forall L \in \mathcal{C}[L \leq_m^p A]$

定理6.2より,  $L \leq_m^p A \wedge A \leq_m^p B \rightarrow L \leq_m^p B$

したがって,  $\forall L \in \mathcal{C}[L \leq_m^p B]$

すなわち,  $B$ は $\mathcal{C}$ -困難。

14/14

$\mathcal{EXPC} \equiv \{L: L \text{ is } \mathcal{EXP}\text{-complete}\}$   
 $\mathcal{NPC} \equiv \{L: L \text{ is } \mathcal{NP}\text{-complete}\}$   
 Then, we have the following theorems.

**Theorem 6.5.**  
 (1)  $\mathcal{EXPC} \cap \mathcal{P} = \emptyset$   
 (2)  $\mathcal{EXP} - (\mathcal{EXPC} \cup \mathcal{P}) \neq \emptyset$

**Theorem 6.6: Assuming  $\mathcal{P} \neq \mathcal{NP}$**   
 (1)  $\mathcal{NPC} \cap \mathcal{P} = \emptyset$   
 (2)  $\mathcal{NP} - (\mathcal{NPC} \cup \mathcal{P}) \neq \emptyset$

14/14

$\mathcal{EXPC} \equiv \{L: L \text{ is } \mathcal{EXP}\text{-完全}\}$   
 $\mathcal{NPC} \equiv \{L: L \text{ is } \mathcal{NP}\text{-完全}\}$   
 とすると、次の定理が成り立つ.

**定理6.5.**  
 (1)  $\mathcal{EXPC} \cap \mathcal{P} = \emptyset$   
 (2)  $\mathcal{EXP} - (\mathcal{EXPC} \cup \mathcal{P}) \neq \emptyset$

**定理6.6:  $\mathcal{P} \neq \mathcal{NP}$ を仮定すると**  
 (1)  $\mathcal{NPC} \cap \mathcal{P} = \emptyset$   
 (2)  $\mathcal{NP} - (\mathcal{NPC} \cup \mathcal{P}) \neq \emptyset$

### Schedule(残りの予定)

- 10/25(Mon):
  - Submission of the report (レポート提出)
- 10/28(Thu): Last class (前半最後の講義)
  - Course Evaluation Questionnaire (授業アンケート)
  - Misc. (その他)
- 11/ 1(Mon): mid-term exam (中間試験)
  - 40 points ✖ Textbook, Copy, Printout,...
  - You can bring your own hand-written notebook  
(手書きノートのみ持ち込み可)
  - Lesson 3~Lesson 6 (講義3~講義6)