# 第6章 多項式時間計算可能性の分析

## 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 $h$: $A$→$B$: 多項式時間還元(polynomial-time reduction)

⇔
(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:

$$A \le_m^P B$$

# Chapter 6. Analysis on Polynomial-Time Computability

## 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 $\boxed{A \leq_m^P B}$

$A \le_m^P B$　多項式時間の範囲内では，$A$の難しさ$\le$ $B$の難しさ

**定理6.1.** $A \le_m^P B$ のとき，

(1) $B \in$ P → $A \in$ P .
(2) $B \in$ NP → $A \in$ NP .
(3) $B \in$ co- NP → $A \in$ co- NP .
(4) $B \in$ EXP → $A \in$ EXP.

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

例6.2: ONE$\equiv$ {1}と定義するとき，クラスPのすべての集合$L$について　$L \le_m^P$ 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) $\forall x \in \Sigma^*[x \in L \leftrightarrow h(x) \in \mathrm{ONE}]$
(3) $h$は多項式時間計算可能($L\in$ P→$x \in L$の判定も多項式時間内）

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

**定理6.1** $A \leq_m^P B$ leads to,

(1) $B \in$ P → $A \in$ P .
(2) $B \in$ NP → $A \in$ NP .
(3) $B \in$ co- NP → $A \in$ co- NP .
(4) $B \in$ EXP → $A \in$ EXP.

Note : class E is exceptional. Generally, $B \in$ E → $A \in$ E is not true.

Ex.6.2: If we define ONE$\equiv \{1\}$, for each set $L$ in 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) $\forall x \in \Sigma^*[x \in L \leftrightarrow h(x) \in \text{ONE}]$
(3) $h$ is polynomial-time computable(so is computation $L \in$ P→$x \in L$)

**定理6.2:** $A, B, C$: 任意の集合

(1) $A \leq_m^P A$

(2) $A \leq_m^P B \wedge B \leq_m^P C \to A \leq_m^P C$

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

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

(1) $A \leq_m^P A$

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

$$\text{Def}: A \equiv_m^P B \leftrightarrow A \leq_m^P B \wedge B \leq_m^P A$$

$\equiv_m^P$ is an equivalence relation.

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

$$2\mathrm{SAT} \le_m^P 3\mathrm{SAT}$$

高々$k$個…自明
ちょうど$k$個…レポート

同様に，

$$3\mathrm{SAT} \le_m^P \mathrm{SAT} \le_m^P \mathrm{ExSAT}$$

$$2\mathrm{SAT} \le_m^P 3\mathrm{SAT} \le_m^P \mathrm{SAT} \le_m^P \mathrm{ExSAT} \quad (6.1)$$

ここで

$$\mathrm{ExSAT} \le_m^P 3\mathrm{SAT}$$

であることを示せると，

$$3\mathrm{SAT} \equiv_m^P \mathrm{SAT} \equiv_m^P \mathrm{ExSAT}$$

となる．

## Relation among satisfiability problems of propositional expressions

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

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

at most $k$ … trivial
exactly $k$ … report

Similarly,

$$3\mathrm{SAT} \leq_m^P \mathrm{SAT} \leq_m^P \mathrm{ExSAT}$$

$$2\mathrm{SAT} \leq_m^P 3\mathrm{SAT} \leq_m^P \mathrm{SAT} \leq_m^P \mathrm{ExSAT} \quad (6.1)$$

Here, if we can show

$$\mathrm{ExSAT} \leq_m^P 3\mathrm{SAT}$$

then we have

$$3\mathrm{SAT} \equiv_m^P \mathrm{SAT} \equiv_m^P \mathrm{ExSAT}$$

## 例6.3: ExSATから3SATへの還元

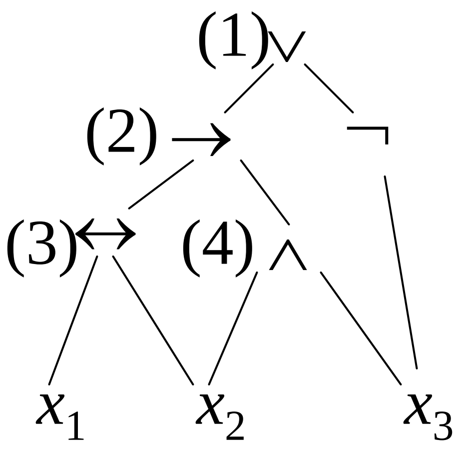
$$E_1(x_1, x_2, x_3) \equiv [[x_1 \leftrightarrow x_2] \rightarrow [x_2 \wedge x_3]] \vee \neg x_3$$

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

このとき, [$E_1$が充足可能] $\leftrightarrow$ [$F_1$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




$$(1) V_1 \equiv V_2 \vee \neg x_3$$

$$(2) V_2 \equiv [V_3 \rightarrow V_4]$$

$$(3) V_3 \equiv [x_1 \leftrightarrow x_2]$$

$$(4) V_4 \equiv x_2 \wedge x_3$$

$F_1$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

## Ex. 6.3: Reduction from ExSAT to 3SAT

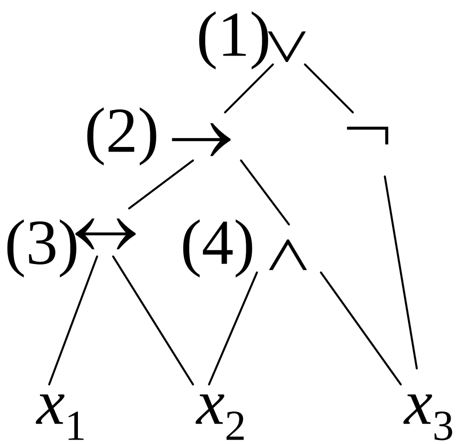
$$E_1(x_1, x_2, x_3) \equiv [[x_1 \leftrightarrow x_2] \rightarrow [x_2 \wedge x_3]] \vee \neg x_3$$

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

Then, [$E_1$ is satisfiable] $\leftrightarrow$ [$F_1$ is satisfiable] (6.2)

$F_1$ is easier to be converted to 3SAT form.

**How to construct $F_1$**




(1) $V_1 \equiv V_2 \vee \neg x_3$

(2) $V_2 \equiv [V_3 \rightarrow V_4]$

(3) $V_3 \equiv [x_1 \leftrightarrow x_2]$

(4) $V_4 \equiv x_2 \wedge x_3$

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

$F_1$ の構成方法より，
(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

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

$$
\begin{aligned}
U_1 \leftrightarrow [U_2 \vee \neg x_3] &= [\neg U_1 \vee U_2 \vee \neg x_3] \wedge [U_1 \vee \neg [U_2 \vee \neg x_2]] \\
&= [\neg U_1 \vee U_2 \vee \neg x_3] \wedge [U_1 \vee [\neg U_2 \wedge x_2]] \\
&= [\neg U_1 \vee U_2 \vee \neg x_3] \wedge [U_1 \vee \neg U_2] \wedge [U_1 \vee x_2] \\
&= [\neg U_1 \vee U_2 \vee \neg x_3] \wedge [U_1 \vee \neg U_2 \vee \neg U_2] \wedge [U_1 \vee x_2 \vee x_2]
\end{aligned}
$$

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．

From the construction of $F_1$
(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

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

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

$$
\begin{aligned}
U_1 \leftrightarrow [U_2 \vee \neg x_3] &= [\neg U_1 \vee U_2 \vee \neg x_3] \wedge [U_1 \vee \neg [U_2 \vee \neg x_2]] \\
&= [\neg U_1 \vee U_2 \vee \neg x_3] \wedge [U_1 \vee [\neg U_2 \wedge x_2]] \\
&= [\neg U_1 \vee U_2 \vee \neg x_3] \wedge [U_1 \vee \neg U_2] \wedge [U_1 \vee x_2] \\
&= [\neg U_1 \vee U_2 \vee \neg x_3] \wedge [U_1 \vee \neg U_2 \vee \neg U_2] \wedge [U_1 \vee x_2 \vee x_2]
\end{aligned}
$$

Others are similar.

Thus, every 3SAT form is converted.

# 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

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（$\le_m^P$の下で）C-完全という.

(a) $\forall L \in$ C $[L \le_m^P A]$

(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

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

## 6.2.1. 完全性の定義とその基本的性質

EVAL-IN-E:

入力: $< a, x, \bar{t} >$

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

出力: $\mathit{eval\text{-}in\text{-}time}(a, x, \overline{2^{\bar{t}}}) = \mathit{accept}$ ?

例6.5. クラスNPの完全集合の例

3SAT, SAT, ExSAT, DHAM, KNAP, BIN, VCなど

クラスEXPの完全集合

EVAL-IN-E, HALT-IN-Eなど

# 6.2.Completeness based on Polynomial-time Reducibility

## 6.2.1. Definition of Completeness and its Basic Properties

$\mathrm{EVAL\text{-}IN\text{-}E}:$

$\mathrm{Input}: < a, x, \bar{t} >$

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

$\mathrm{Output}: \mathit{eval\text{-}in\text{-}time}(a, x, \overline{2^{\bar{t}}}) = \mathit{accept}\,?$

Ex.6.5. Examples of NP-complete sets

3SAT, SAT, ExSAT, DHAM, KNAP, BIN, VC, etc

EXP-complete sets

EVAL-IN-E, HALT-IN-E, etc.

**定理6.3.** 任意のC-困難集合(含:C-完全集合)$A$に対し,

(1) $A \in$ P → C ⊆ P　対偶は C ⊄ P → $A \notin$ P

(2) $A \in$ NP → C ⊆ NP　対偶は C ⊄ NP → $A \notin$ NP

(3) $A \in$ co-NP → C ⊆ co-NP　対偶は C ⊄ co-NP → $A \notin$ co-NP

(4) $A \in$ EXP → C ⊆ EXP　対偶は C ⊄ EXP → $A \notin$ EXP

証明:

(1) $B$を任意のC集合とすると, $A$はC-困難だから,

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

(2), (3), (4)も同様

**Theorem 6.3.** For any C-hard (or C-complete) set $A$,

(1) $A \in \mathsf{P} \rightarrow \mathsf{C} \subseteq \mathsf{P}$ CP: $\mathsf{C} \not\subset \mathsf{P} \rightarrow A \notin \mathsf{P}$

(2) $A \in \mathsf{NP} \rightarrow \mathsf{C} \subseteq \mathsf{NP}$ CP: $\mathsf{C} \not\subset \mathsf{NP} \rightarrow A \notin \mathsf{NP}$

(3) $A \in$ co-NP $\rightarrow \mathsf{C} \subseteq$ co-NP CP: $\mathsf{C} \not\subset$ co-NP $\rightarrow A \notin$ co-NP

(4) $A \in \mathsf{EXP} \rightarrow \mathsf{C} \subseteq \mathsf{EXP}$ CP: $\mathsf{C} \not\subset \mathsf{EXP} \rightarrow A \notin \mathsf{EXP}$

Proof: CP: contraposition

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

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

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

**定理6.3.** 任意のC-困難集合（含：C-完全集合）$A$に対し，

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

**定理5.9.**
(1) $\mathrm{NP} \subseteq \text{co-NP} \rightarrow \mathrm{NP} = \text{co-NP}$

**例6.6.** 定理6.3の意味（クラスNP）
$L$をNP-完全集合とする．

定理6.3(1)の対偶より，

$$\mathrm{NP} \neq \mathrm{P} \Rightarrow L \notin \mathrm{P}$$

定理6.3(3)の対偶と定理5.9(1)の対偶より，

$$L \notin \text{co-NP}$$

つまり，NP-完全集合はP≠NPである限り，多項式時間では認識できないNP集合である．

**Theorem 6.3.** For any C-hard (or C-complete) set $A$,

(1) $A \in$ P → C ⊆ P  CP: C ⊄ P → $A \notin$ P
(2) $A \in$ NP → C ⊆ NP  CP: C ⊄ NP → $A \notin$ NP
(3) $A \in$ co-NP → C ⊆ co-NP  CP: C ⊄ co-NP → $A \notin$ co-NP
(4) $A \in$ EXP → C ⊆ EXP  CP: C ⊄ EXP → $A \notin$ EXP

**Theorem 5.9.**
(1) NP ⊆ co-NP → NP = co-NP

**Ex.6.6:** Meaning of Theorem 6.3 (class NP)

Let $L$ be NP-complete set.

By the contraposition of Theorem 6.3(1) we have

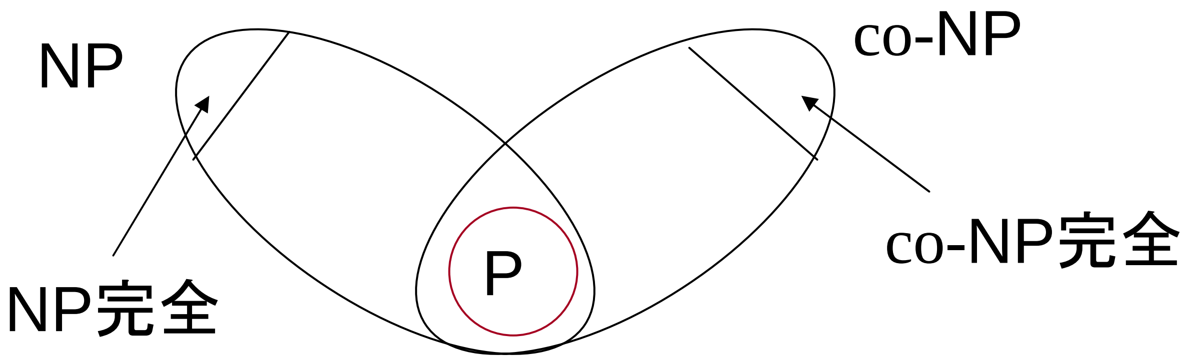
NP ≠ P → $L \notin$ P

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

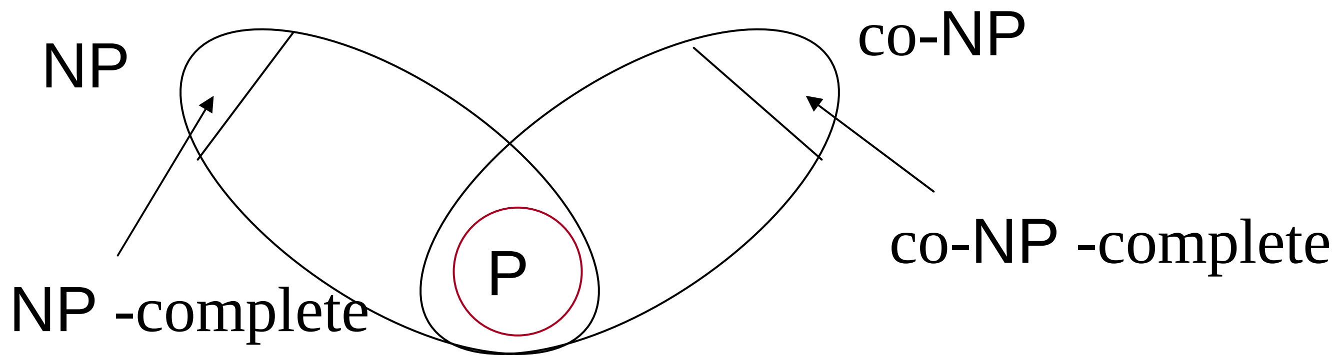
$L \notin$ co-NP

That is, NP-complete sets are NP-sets that cannot be recognized in polynomial time unless P = NP.

NP-完全集合はP $\neq$NPである限り，NP $\cap$ co-NPには入らないNP集合である.



NP-compete sets are NP-sets that do not belong to NP $\cap$ co-NP unless P = NP.



**例6.7.** 定理6.3の意味(クラスEXP)

$D$をEXP-完全集合とする.
定理6.3(1)の対偶(C $\not\subset$ P → $A \notin$ P， ここではEXP $\not\subset$ P →$D \notin$ P )
P $\neq$ EXP → EXP $\not\subset$ P (∵P ⊆ EXP ) → $D \notin$ P
定理6.3(2)の対偶(C $\not\subset$ NP → $A \notin$ NP ,
ここではEXP $\not\subset$ NP →$D \notin$ NP )
NP $\neq$ EXP → EXP $\not\subset$ NP (∵ NP ⊆ EXP ) → $D \notin$ NP
定理6.3(3)の対偶(C $\not\subset$ co-NP → $A \notin$ co- NP ,
ここではEXP $\not\subset$ co- NP →$D \notin$ co- NP )
co-NP $\neq$ EXP →EXP $\not\subset$ co-NP →$D \notin$ co-NP
ところが，定理5.7から，P ⊆ EXP であることを知っているから，
無条件に$D \notin$ P.
EXP-完全集合は多項式時間では計算不可能.

**Ex. 6.7.** Meaning of Theorem 6.3 (class EXP)

Let $D$ be an EXP-complete set.
Contraposition of Theorem 6.3(1)
(C $\not\subset$ P $\rightarrow$ $A \notin$ P , where EXP $\not\subset$ P $\rightarrow D \notin$ P )
P $\neq$ EXP $\rightarrow$ EXP $\not\subset$ P ($\because$ P $\subseteq$ EXP ) $\rightarrow$ $D \notin$ P
Contraposition of Theorem 6.3(2) (C $\not\subset$ NP $\rightarrow$ $A \notin$ NP ,
Here, EXP $\not\subset$ NP $\rightarrow D \notin$ NP )
NP $\neq$ EXP $\rightarrow$ EXP $\not\subset$ NP ($\because$ NP $\subseteq$ EXP ) $\rightarrow$ $D \notin$ NP
Contraposition of Theorem 6.3(3) (C $\notin$ co-NP $\rightarrow$ $A \not\subset$ co- NP ,
here, EXP $\not\subset$ co-NP $\rightarrow D \notin$ co- NP )
co-NP $\neq$ EXP $\rightarrow$ EXP $\not\subset$ co-NP $\rightarrow D \notin$ co-NP
But, by Theorem 5.7, since we know P $\subseteq$ EXP, we have
$D \notin$ P.
EXP-complete sets are not computable in polynomial time.

**定理6.4.** $A$: 任意のC-完全集合
すべての集合$B$に対し,
(1) $A \leq_m^P B$ → $B$はC-困難.
(2) $A \leq_m^P B \wedge B \in$ C → $B$はC-完全.

証明:
定義6.2より, $\forall L \in C[L \leq_m^P A]$
定理6.2より, $L \leq_m^P A \wedge A \leq_m^P B \to L \leq_m^P B$
したがって, $\forall L \in C[L \leq_m^P B]$
すなわち, $B$はC-困難.

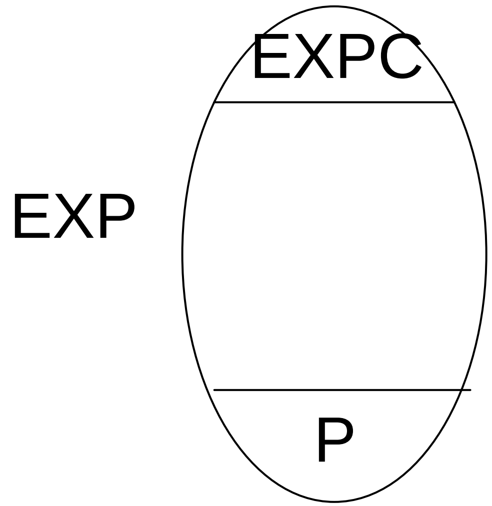
**Theorem 6.4.** $A$: any C-complete set
For any set $B$ we have
(1) $A \leq_m^P B \rightarrow B$ is C-hard..
(2) $A \leq_m^P B \wedge B \in$ C $\rightarrow$ $B$ is C-complete.

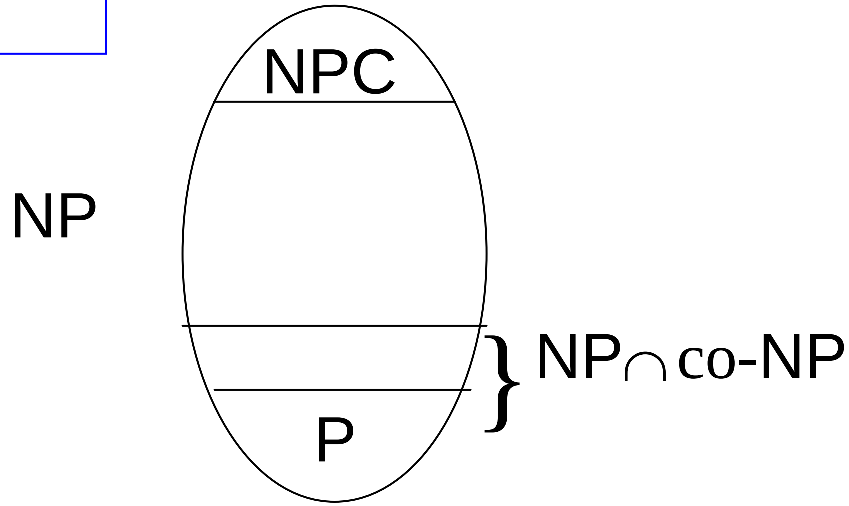
Proof:
By Def. 6.2 $\forall L \in C[L \leq_m^P A]$
By Theorem 6.2, $L \leq_m^P A \wedge A \leq_m^P B \rightarrow L \leq_m^P B$
Therefore, $\forall L \in C[L \leq_m^P B]$
That is, $B$ is C-hard.

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

**定理6.5.**
(1) EXPC $\cap$ P $= \phi$
(2) EXP – (EXPC $\cup$ P) $\neq \phi$

**定理6.6:** P $\neq$ NPを仮定すると
(1) NPC$\cap$P $= \phi$
(2) NP – (NPC$\cup$ P) $\neq \phi$



EXPC $\equiv \{L: L$ is EXP-complete$\}$

NPC $\equiv \{L: L$ is NP-complete$\}$

Then, we have the following theorems.

**Theorem 6.5.**

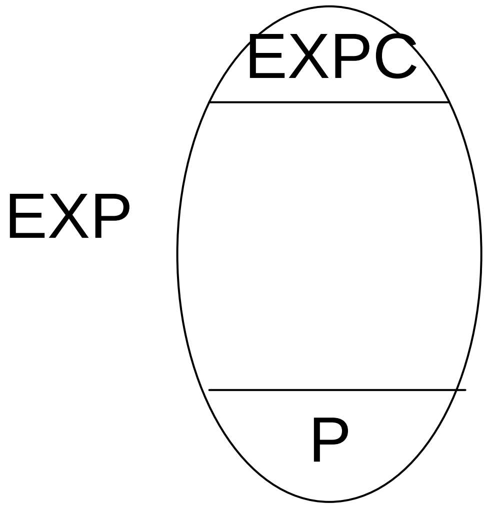
(1) $\mathrm{EXPC} \cap \mathrm{P} = \phi$

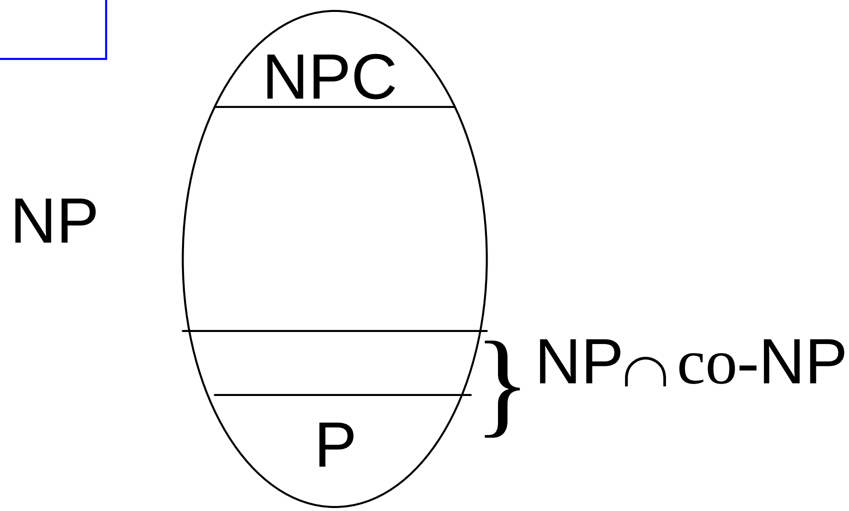
(2) $\mathrm{EXP} - (\mathrm{EXPC} \cup \mathrm{P}) \neq \phi$

**Theorem 6.6: Assuming** $\mathrm{P} \neq \mathrm{NP}$

(1) $\mathrm{NPC} \cap \mathrm{P} = \phi$

(2) $\mathrm{NP} - (\mathrm{NPC} \cup \mathrm{P}) \neq \phi$



## 6.2.2 完全性の証明

**定理6.7:** EVAL-IN-EはEXP-完全

証明：例5.6より，EVAL-IN-E $\in$ EXP, よって，

$$\forall L \in \mathrm{EXP}[\, L \leq_m^P \mathrm{EVAL\text{-}IN\text{-}E}]$$

を示せばよい．

$L$：任意のEXP集合とする．

$L$を$2^{p(l)}$時間で認識するプログラムが存在($p(n)$は多項式)

そのプログラムを**L**とする．このとき，

$x \in L \;\leftrightarrow\; \mathbf{L}(x)$=accept

time_**L** $(x) \;\leq 2^{p(|x|)}$

$L$からEVAL-IN-Eへの還元として次の関数$h$を考える．

$$h(x) \;\equiv < \ulcorner \mathbf{L} \urcorner, x, \overline{p(|x|)} > \quad \text{for} \quad \forall x \in \Sigma^*$$

すると，$h$は全域的で，多項式時間計算可能．

# 6.2.2 Proof of Completeness

**Theorem 6.7:** EVAL-IN-E is EXP-completeness.

Proof: By Example 5.6, we have EVAL-IN-E ∈ EXP. Thus, it suffices to prove

$$\forall L \in \mathrm{EXP}[\, L \le_m^P \text{EVAL-IN-E}]$$

$L$: any EXP set.

There is a program recognizing $L$ in time $2^{p(l)}$ ($p(n)$ is polynomial)

Let the program be **L**. Then, we have

$x \in L \leftrightarrow \mathbf{L}(x)$=accept

time_**L** $(x) \le 2^{p(|x|)}$

Consider the following function $h$ to reduce from $L$ to EVAL-IN-E.

$$h(x) \equiv \, < \ulcorner \mathbf{L} \urcorner, x, \overline{p(|x|)} > \quad \text{for} \quad \forall x \in \Sigma^*$$

Then, $h$ is total and computable in polynomial time.

また，すべての$x \in \Sigma^*$に対し

$$
\begin{aligned}
x \in L \leftrightarrow\ & \mathsf{L}(x) = \mathrm{accept} \\
\leftrightarrow\ & \mathrm{eval}(\lceil \mathsf{L} \rceil,\ x) = \mathrm{accept} \\
\leftrightarrow\ & \mathrm{eval\_in\_time}(\lceil \mathsf{L} \rceil,\ x,\ \overline{2^{p(|x|)}}) = \mathrm{accept} \\
\leftrightarrow\ & < \lceil \mathsf{L} \rceil,\ x,\ \overline{2^{p(|x|)}} > \in \text{EVAL-IN-E} \\
\leftrightarrow\ & h(x) \in \text{EVAL-IN-E}
\end{aligned}
$$

ゆえに，$h$は$L$からEVAL-IN-Eへの多項式時間還元.

$$\therefore L \leq_m^P \text{EVAL-IN-E} \ \ \text{for } \forall L \in \mathrm{EXP}$$

すなわち，EVAL-IN-EはEXP-完全.

証明終

Moreover, for each $x \in \Sigma^*$ we have

$$
\begin{aligned}
x \in L \leftrightarrow\ & \mathbf{L}(x) = \text{accept} \\
\leftrightarrow\ & \text{eval}(\lceil \mathbf{L} \rceil,\ x) = \text{accept} \\
\leftrightarrow\ & \text{eval\_in\_time}(\lceil \mathbf{L} \rceil,\ x,\ \overline{2^{p(|x|)}}) = \text{accept} \\
\leftrightarrow\ & <\lceil \mathbf{L} \rceil,\ x,\ \overline{2^{p(|x|)}}> \in \text{EVAL-IN-E} \\
\leftrightarrow\ & h(x) \in \text{EVAL-IN-E}
\end{aligned}
$$

Thus, *h* is a polynomial-time reduction from *L* to EVAL-IN-E.

$$\therefore L \leq_m^P \text{EVAL-IN-E} \ \text{ for } \forall L \in \mathsf{EXP}$$

That is, EVAL-IN-E is EXP-complete.

Q.E.D.

**定理6.8.**
(1) EVAL-IN-E $\notin$ P
(2) EVAL-IN-EはNP-困難
(3) HALT-IN-EはEXP-完全.

証明:
(1) EVAL-IN-EはEXP-完全集合で, EXP-完全集合 $\notin$ P.
(2) $\forall L \in \mathrm{EXP} \quad [A \leq_m^P \mathrm{EVAL\text{-}IN\text{-}E}]$ と

NP ⊆ EXP より.

**Theorem 6.8.**
(1) EVAL-IN-E $\notin$ P
(2) EVAL-IN-E is NP-hard.
(3) HALT-IN-E is EXP-complete.

Proof:
(1) EVAL-IN-E is EXP-complete and any EXP-complete set $\notin$ P.
(2) It follows from

$$\forall L \in \text{EXP} \quad [A \leq_m^P \text{EVAL-IN-E}] \quad \text{and}$$

$$\text{NP} \subseteq \text{EXP}$$

# 残りの予定

- 7月22日(金): 講義に関するアンケート実施
- 7月27日(水):
  - 授業は休講
  - オフィスアワー: 6回目のレポートの回収、解答と解説
- 7月29日(金):
  - 期末試験(大講義室にて。遅刻厳禁)
- それ以降:
  - 成績などの問い合わせはメールで
  - レポート、試験の返却希望者は適宜取りにくること
- おまけ:
  - 上原は7月25日(月)~7月27日(水) は出張
  - TAの寺本君も7月25日(月)~7月26日(火)は出張