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: $A \to B$: 多項式時間還元(polynomial-time reduction)
$\Leftrightarrow$
(a) h はΣ*からΣ*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: $A \to B$: polynomial-time reduction
$\Leftrightarrow$
(a) h is a total function from Σ* onto Σ*
(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

$$A \le_m^P B$$

$A \le_m^P B$ 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) $B \in \mathcal{P} \to A \in \mathcal{P}$.
(2) $B \in \mathcal{NP} \to A \in \mathcal{NP}$.
(3) $B \in$ co-$\mathcal{NP}$ $\to A \in$ co-$\mathcal{NP}$.
(4) $B \in \mathcal{EXP} \to A \in \mathcal{EXP}$.

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

例6.2: ONE≡ {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 $L \le_m^P$ 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Σ*からΣ*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($L \in \mathcal{P} \to x \in L$の判定も多項式時間内)

$A \le_m^P B$ within polynomial time, hardness of A $\le$ that of B

定理6.1 $A \le_m^P B$ leads to,
(1) $B \in \mathcal{P} \to A \in \mathcal{P}$.
(2) $B \in \mathcal{NP} \to A \in \mathcal{NP}$.
(3) $B \in$ co-$\mathcal{NP}$ $\to A \in$ co-$\mathcal{NP}$.
(4) $B \in \mathcal{EXP} \to A \in \mathcal{EXP}$.

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

Ex.6.2: If we define ONE≡ {1}, for each set L in $\mathcal{P}$ we have
$L \le_m^P$ 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 Σ* onto Σ*.
(2) $x \in \Sigma^*[x \in L \leftrightarrow h(x) \in \text{ONE}]$
(3) h is polynomial-time computable(so is computation $L \in \mathcal{P} \to x \in L$)

定理6.2: A, B, C: 任意の集合
(1) $A \le_m^P A$
(2) $A \le_m^P B \wedge B \le_m^P C \to A \le_m^P C$

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

Theorem 6.2: A, B, C: arbitrary sets
(1) $A \le_m^P A$
(2) $A \le_m^P B \wedge B \le_m^P C \to A \le_m^P C$

Def: $A \equiv_m^P B \leftrightarrow A \le_m^P B \wedge B \le_m^P A$
$\equiv_m^P$ 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）

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

- 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…レポート(?)

同様に，

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

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

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

- at most k…trivial
- exactly k…
  - easy if you can repeat the same literal.
  - report for the other case (?)

Similarly,

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

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

Here, if we can show

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

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

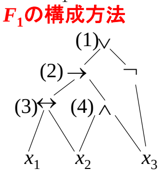
$$E_1(x_1,x_2,x_3) \equiv [[x_1 \leftrightarrow x_2] \to [x_2 \wedge x_3]] \vee \neg x_3$$

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

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)$V_2 \equiv [V_3 \to V_4]$
(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，$V_i \to U_i$とし，V_iの定義式を$\wedge$で結ぶ

Ex. 6.3: Reduction from ExSAT to 3SAT

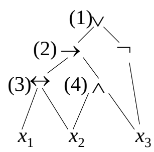
$$E_1(x_1,x_2,x_3) \equiv [[x_1 \leftrightarrow x_2] \to [x_2 \wedge x_3]] \vee \neg x_3$$

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

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)$V_2 \equiv [V_3 \to V_4]$
(3)$V_3 \equiv [x_1 \leftrightarrow x_2]$
(4)$V_4 \equiv x_2 \wedge x_3$

To construct **F_1** we let $V_i \to U_i$, 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．

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

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

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

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

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$\mathcal{C}$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)$\mathcal{C}$-完全という.
(a) $\forall L \in \mathcal{C}\ [L \le_m^P A]$
(b) $A \in \mathcal{C}$
補注：条件(a)を満たす集合は$\mathcal{C}$-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 $\mathcal{C}$, if a set A satisfies the following conditions, then it is called $\mathcal{C}$-complete (under $\le_m^P$)
(a) $\forall L \in \mathcal{C}\ [L \le_m^P A]$
(b) $A \in \mathcal{C}$
Note: Sets satisfying the condition (a) are called $\mathcal{C}$-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

例6.5. クラス$\mathcal{NP}$の完全集合の例
3SAT, SAT, ExSAT, DHAM, KNAP, BIN, VCなど
クラス$\mathcal{EXP}$の完全集合
EVAL-IN-E, HALT-IN-Eなど

EVAL-IN-E:
入力: $< a, x, \bar{t} >$
a:1入力プログラムのコード, $x \in \Sigma^*, \bar{t} \ge 0$
出力: $\textit{eval-in-time}(a, x, 2^{\bar{t}}) = \textit{accept}$?

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: $< a, x, \bar{t} >$
a: the code of a program with 1 input, $x \in \Sigma^*, \bar{t} \ge 0$
Output: $\textit{eval-in-time}(a, x, 2^{\bar{t}}) = \textit{accept}$?

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) $A \in \mathcal{P} \to \mathcal{C} \subseteq \mathcal{P}$　　対偶は $\mathcal{C} \not\subset \mathcal{P} \to A \notin \mathcal{P}$
(2) $A \in \mathcal{NP} \to \mathcal{C} \subseteq \mathcal{NP}$　　対偶は $\mathcal{C} \not\subset \mathcal{NP} \to A \notin \mathcal{NP}$
(3) $A \in$ co-$\mathcal{NP} \to \mathcal{C} \subseteq$ co-$\mathcal{NP}$　　対偶は $\mathcal{C} \not\subset$ co-$\mathcal{NP} \to A \notin$ co-$\mathcal{NP}$
(4) $A \in \mathcal{EXP} \to \mathcal{C} \subseteq \mathcal{EXP}$　　対偶は $\mathcal{C} \not\subset \mathcal{EXP} \to A \notin \mathcal{EXP}$

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，
$B \le_m^P A$　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) $A \in \mathcal{P} \to \mathcal{C} \subseteq \mathcal{P}$　　CP: $\mathcal{C} \not\subset \mathcal{P} \to A \notin \mathcal{P}$
(2) $A \in \mathcal{NP} \to \mathcal{C} \subseteq \mathcal{NP}$　　CP: $\mathcal{C} \not\subset \mathcal{NP} \to A \notin \mathcal{NP}$
(3) $A \in$ co-$\mathcal{NP} \to \mathcal{C} \subseteq$ co-$\mathcal{NP}$　　CP: $\mathcal{C} \not\subset$ co-$\mathcal{NP} \to A \notin$ co-$\mathcal{NP}$
(4) $A \in \mathcal{EXP} \to \mathcal{C} \subseteq \mathcal{EXP}$　　CP: $\mathcal{C} \not\subset \mathcal{EXP} \to A \notin \mathcal{EXP}$

Proof:　　CP: contraposition
(1) Let B be any $\mathcal{C}$-set. Then, since A is $\mathcal{C}$-hard,
$B \le_m^P A$ 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) $A \in \mathcal{P} \to \mathcal{C} \subseteq \mathcal{P}$ 対偶は $\mathcal{C} \not\subset \mathcal{P} \to A \notin \mathcal{P}$
(2) $A \in \mathcal{NP} \to \mathcal{C} \subseteq \mathcal{NP}$ 対偶は $\mathcal{C} \not\subset \mathcal{NP} \to A \notin \mathcal{NP}$
(3) $A \in$ co-$\mathcal{NP} \to \mathcal{C} \subseteq$ co-$\mathcal{NP}$ 対偶は $\mathcal{C} \not\subset$ co-$\mathcal{NP} \to A \notin$ co-$\mathcal{NP}$
(4) $A \in \mathcal{EXP} \to \mathcal{C} \subseteq \mathcal{EXP}$ 対偶は $\mathcal{C} \not\subset \mathcal{EXP} \to A \notin \mathcal{EXP}$

例6.6. 定理6.3の意味（クラス$\mathcal{NP}$）

定理5.9.
(1) $\mathcal{NP} \subseteq$ co-$\mathcal{NP} \to \mathcal{NP} =$ co-$\mathcal{NP}$

Aを$\mathcal{NP}$-完全集合とする.

定理6.3(1)の対偶より，
$\mathcal{NP} \neq \mathcal{P} \to A \notin \mathcal{P}$

定理6.3(3)の対偶と定理5.9(1)の対偶より，
$A \notin$ 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.

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

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

Theorem 5.9.
(1) $\mathcal{NP} \subseteq$ co-$\mathcal{NP} \to \mathcal{NP} =$ co-$\mathcal{NP}$

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

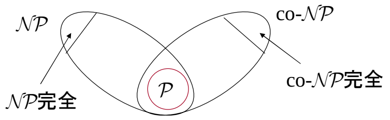
Let A be $\mathcal{NP}$-complete set.

By the contraposition of Theorem 6.3(1) we have
$\mathcal{NP} \neq \mathcal{P} \to A \notin \mathcal{P}$

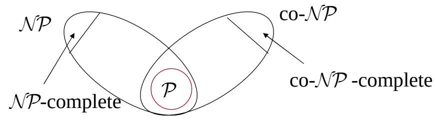
By the contraposition of Theorem 6.3(3) and that of Theorem 5.9(1),
$A \notin$ co-$\mathcal{NP}$

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

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



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



例6.7. 定理6.3の意味（クラス$\mathcal{EXP}$）

Dを$\mathcal{EXP}$-完全集合とする.

定理6.3(1)の対偶（$\mathcal{C} \not\subset \mathcal{P} \to A \notin \mathcal{P}$，ここでは$\mathcal{EXP} \not\subset \mathcal{P} \to D \notin \mathcal{P}$）
$\mathcal{P} \neq \mathcal{EXP} \to \mathcal{EXP} \not\subset \mathcal{P}$ （$\because \mathcal{P} \subseteq \mathcal{EXP}$）$\to D \notin \mathcal{P}$
定理6.3(2)の対偶（$\mathcal{C} \not\subset \mathcal{NP} \to A \notin \mathcal{NP}$，
ここでは$\mathcal{EXP} \not\subset \mathcal{NP} \to D \notin \mathcal{NP}$）
$\mathcal{NP} \neq \mathcal{EXP} \to \mathcal{EXP} \not\subset \mathcal{NP}$ （$\because \mathcal{NP} \subseteq \mathcal{EXP}$）$\to D \notin \mathcal{NP}$
定理6.3(3)の対偶（$\mathcal{C} \not\subset$co-$\mathcal{NP} \to A \notin$co-$\mathcal{NP}$，
ここでは$\mathcal{EXP} \not\subset$co-$\mathcal{NP} \to D \notin$co-$\mathcal{NP}$）
co-$\mathcal{NP} \neq \mathcal{EXP} \to \mathcal{EXP} \not\subset$co-$\mathcal{NP} \to D \notin$ co-$\mathcal{NP}$
ところが定理5.7から $\mathcal{P} \subsetneq \mathcal{EXP}$ 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.

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

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

Contraposition of Theorem 6.3(1)
（$\mathcal{C} \not\subset \mathcal{P} \to A \notin \mathcal{P}$， where $\mathcal{EXP} \not\subset \mathcal{P} \to D \notin \mathcal{P}$）
$\mathcal{P} \neq \mathcal{EXP} \to \mathcal{EXP} \not\subset \mathcal{P}$ （$\because \mathcal{P} \subseteq \mathcal{EXP}$）$\to D \notin \mathcal{P}$
Contraposition of Theorem 6.3(2)（$\mathcal{C} \not\subset \mathcal{NP} \to A \notin \mathcal{NP}$,
Here, $\mathcal{EXP} \not\subset \mathcal{NP} \to D \notin \mathcal{NP}$）
$\mathcal{NP} \neq \mathcal{EXP} \to \mathcal{EXP} \not\subset \mathcal{NP}$ （$\because \mathcal{NP} \subseteq \mathcal{EXP}$）$\to D \notin \mathcal{NP}$
Contraposition of Theorem 6.3(3)（$\mathcal{C} \notin$ co-$\mathcal{NP} \to A \not\subset$co-$\mathcal{NP}$,
here, $\mathcal{EXP} \not\subset$co-$\mathcal{NP} \to D \notin$ co-$\mathcal{NP}$）
co-$\mathcal{NP} \neq \mathcal{EXP} \to \mathcal{EXP} \not\subset$ co-$\mathcal{NP} \to D \notin$ co-$\mathcal{NP}$
But, by Theorem 5.7, since we know $\mathcal{P} \subsetneq \mathcal{EXP}$, we have $D \notin \mathcal{P}$.

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

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

証明:
定義6.2より, $\forall L \in \mathcal{C}[L \le_m^P A]$
定理6.2より, $L \le_m^P A \wedge A \le_m^P B \rightarrow L \le_m^P B$
したがって, $\forall L \in \mathcal{C}[L \le_m^P B]$

すなわち, Bは$\mathcal{C}$-困難.

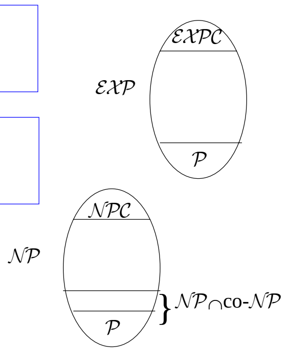
Theorem 6.4. A: any $\mathcal{C}$-complete set
For any set B we have
(1) $A \le_m^P B \rightarrow B$ is $\mathcal{C}$-hard.
(2) $A \le_m^P B \wedge B \in \mathcal{C} \rightarrow B$ is $\mathcal{C}$-complete.

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

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

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

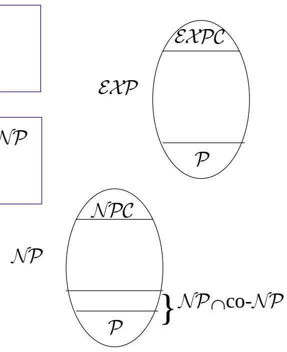
定理6.6: $\mathcal{P} \neq \mathcal{NP}$を仮定すると
(1) $\mathcal{NPC} \cap \mathcal{P} = \phi$
(2) $\mathcal{NP} - (\mathcal{NPC} \cup \mathcal{P}) \neq \phi$



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

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

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



6.2.2 完全性の証明

定理6.7: EVAL-IN-Eは$\mathcal{EXP}$-完全

証明:例5.6より, EVAL-IN-E $\in \mathcal{EXP}$, よって,
$\forall L \in \mathcal{EXP}[L \le_m^P \text{EVAL-IN-E}]$
を示せばよい.
L:任意の$\mathcal{EXP}$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($p(l)$は多項式)
そのプログラムをA_Lとする. このとき,
$x \in L \leftrightarrow A_L(x)$=accept
time_A_L $(x) \le 2^{p(|x|)}$
LからEVAL-IN-Eへの還元として次の関数hを考える.
$h(x) \equiv \langle \ulcorner A_L \urcorner, x, p(|x|) \rangle$ for $\forall x \in \Sigma^*$
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 $\mathcal{EXP}$-completeness.

Proof: By Example 5.6, we have EVAL-IN-E $\in \mathcal{EXP}$. Thus, it suffices to prove
$\forall L \in \mathcal{EXP}[L \le_m^P \text{EVAL-IN-E}]$
L: any $\mathcal{EXP}$ set.
There is a program recognizing L in time $2^{p(l)}$ ($p(l)$ is polynomial)
Let the program be A_L. Then, we have
$x \in L \leftrightarrow A_L(x)$=accept
time_A_L $(x) \le 2^{p(|x|)}$
Consider the following function h to reduce from L to EVAL-IN-E.
$h(x) \equiv \langle \ulcorner A_L \urcorner, x, p(|x|) \rangle$ for $\forall x \in \Sigma^*$
Then, h is total and computable in polynomial time.

また，すべての$x \in \Sigma^*$に対し

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

ゆえに，hはLからEVAL-IN-Eへの多項式時間還元.

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

すなわち，EVAL-IN-Eは$\mathcal{EXP}$-完全.

証明終

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

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

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

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

That is, EVAL-IN-E is $\mathcal{EXP}$-complete.

Q.E.D.

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

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

$\mathcal{NP} \subseteq \mathcal{EXP}$ より.

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

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

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

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