

第6章 多項式時間計算可能性の分析

1/17

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)

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

(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:

$$A \leq_m^p B$$

Chapter 6. Analysis on Polynomial-Time Computability

1/17

6.1. Polynomial-time Reducibility

Def.6.1:

Let A and B be arbitrary sets.

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

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

(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

$$A \leq_m^p B$$

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

2/17

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 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 ($L \in \mathcal{P} \rightarrow x \in L$ 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

2/17

定理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 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 $L \in \mathcal{P} \rightarrow x \in L$)

定理6.2: A, B, C : 任意の集合

3/17

(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

Theorem 6.2: A, B, C : arbitrary sets

3/17

(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.

4/17

命題論理式の充足可能性問題の関係

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)

$2SAT \leq_m^P 3SAT$

同様に,

$3SAT \leq_m^P SAT \leq_m^P ExSAT$
 $2SAT \leq_m^P 3SAT \leq_m^P SAT \leq_m^P ExSAT$ (6.1)

ここで

$ExSAT \leq_m^P 3SAT$

であることを示せると,

$3SAT \equiv_m^P SAT \equiv_m^P ExSAT$
 となる。

高々k個... 自明
 ちょうどk個... レポート

4/17

Relation among satisfiability problems of propositional expressions

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

$2SAT \leq_m^P 3SAT$

Similarly,

$3SAT \leq_m^P SAT \leq_m^P ExSAT$
 $2SAT \leq_m^P 3SAT \leq_m^P SAT \leq_m^P ExSAT$ (6.1)

Here, if we can show

$ExSAT \leq_m^P 3SAT$

then we have

$3SAT \equiv_m^P SAT \equiv_m^P ExSAT$

at most k ... trivial
 exactly k ... report

5/17

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, $[E_1 \text{が充足可能}] \leftrightarrow [F_1 \text{が充足可能}]$ (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

(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

5/17

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

How to construct F_1

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

6/17

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

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

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

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。

6/17

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

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

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

7/17

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

7/17

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

8/17

6.2.1. 完全性の定義とその基本的性質

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

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

6.2.Completeness based on Polynomial-time Reducibility

8/17

6.2.1. Definition of Completeness and its Basic Properties

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.

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

定理6.3. 任意のC-困難集合(含: C-完全集合)Aに対し,

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

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) $A \in P \rightarrow C \subseteq P$ CP: $C \not\subseteq P \rightarrow A \notin P$
- (2) $A \in NP \rightarrow C \subseteq NP$ CP: $C \not\subseteq NP \rightarrow A \notin NP$
- (3) $A \in co-NP \rightarrow C \subseteq co-NP$ CP: $C \not\subseteq co-NP \rightarrow A \notin co-NP$
- (4) $A \in EXP \rightarrow C \subseteq EXP$ CP: $C \not\subseteq EXP \rightarrow A \notin EXP$

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

例6.6. 定理6.3の意味(クラスNP)
 Aを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, 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) $\mathcal{NP} \subseteq \text{co-}\mathcal{NP} \rightarrow \mathcal{NP} = \text{co-}\mathcal{NP}$

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

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

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 NP)

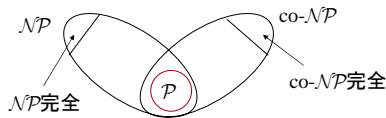
Let A be NP-complete set.

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

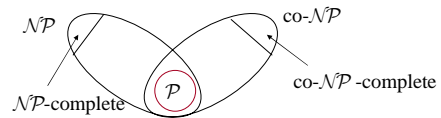
By the contraposition of Theorem 6.3(3) and that of Theorem 5.9(1),
 $A \notin \text{co-}\mathcal{NP}$

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

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 NP集合である.



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



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($C \not\subseteq \mathcal{P} \rightarrow A \notin \mathcal{P}$, 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, $D \notin \mathcal{P}$.

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)

($C \not\subseteq \mathcal{P} \rightarrow A \notin \mathcal{P}$, 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 $D \notin \mathcal{P}$.

EXP-complete sets are not computable in polynomial time.

13/17

定理6.4. A : 任意の C -完全集合

すべての集合 B に対し,
 (1) $A \leq_m^p B \rightarrow B$ は C -困難.
 (2) $A \leq_m^p B \wedge B \in C \rightarrow B$ 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, $L \leq_m^p A \wedge A \leq_m^p B \rightarrow L \leq_m^p B$
 したがって, $\forall L \in C[L \leq_m^p B]$

すなわち, B は C -困難.

13/17

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.

14/17

$\mathcal{E}\mathcal{X}\mathcal{P} \equiv \{L: L \text{ is } \mathcal{E}\mathcal{X}\mathcal{P}\text{-complete}\}$
 $\mathcal{N}\mathcal{P}\mathcal{C} \equiv \{L: L \text{ is } \mathcal{N}\mathcal{P}\text{-complete}\}$
 とすると, 次の定理が成り立つ.

定理6.5.
 (1) $\mathcal{E}\mathcal{X}\mathcal{P} \cap \mathcal{P} = \emptyset$
 (2) $\mathcal{E}\mathcal{X}\mathcal{P} - (\mathcal{E}\mathcal{X}\mathcal{P} \cup \mathcal{P}) \neq \emptyset$

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

14/17

$\mathcal{E}\mathcal{X}\mathcal{P} \equiv \{L: L \text{ is } \mathcal{E}\mathcal{X}\mathcal{P}\text{-complete}\}$
 $\mathcal{N}\mathcal{P}\mathcal{C} \equiv \{L: L \text{ is } \mathcal{N}\mathcal{P}\text{-complete}\}$
 Then, we have the following theorems.

Theorem 6.5.
 (1) $\mathcal{E}\mathcal{X}\mathcal{P} \cap \mathcal{P} = \emptyset$
 (2) $\mathcal{E}\mathcal{X}\mathcal{P} - (\mathcal{E}\mathcal{X}\mathcal{P} \cup \mathcal{P}) \neq \emptyset$

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

15/17

6.2.2 完全性の証明

定理6.7: EVAL-IN-E は $\mathcal{E}\mathcal{X}\mathcal{P}$ -完全

証明: 例5.6より, $\text{EVAL-IN-E} \in \mathcal{E}\mathcal{X}\mathcal{P}$, よって,
 $\forall L \in \mathcal{E}\mathcal{X}\mathcal{P}[L \leq_m^p \text{EVAL-IN-E}]$

を示せばよい.
 L : 任意の $\mathcal{E}\mathcal{X}\mathcal{P}$ 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,
 $x \in L \leftrightarrow A_L(x) = \text{accept}$
 $\text{time}_{A_L}(x) \leq 2^{p(|x|)}$
 L から EVAL-IN-E への還元として次の関数 h を考える.
 $h(x) \equiv \langle A_L, x, p(|x|) \rangle$ for $\forall x \in \Sigma^*$
 すると, h は全域的で, 多項式時間計算可能.

15/17

6.2.2 Proof of Completeness

Theorem 6.7: EVAL-IN-E is $\mathcal{E}\mathcal{X}\mathcal{P}$ -completeness.

Proof: By Example 5.6, we have $\text{EVAL-IN-E} \in \mathcal{E}\mathcal{X}\mathcal{P}$. Thus, it suffices to prove
 $\forall L \in \mathcal{E}\mathcal{X}\mathcal{P}[L \leq_m^p \text{EVAL-IN-E}]$
 L : any $\mathcal{E}\mathcal{X}\mathcal{P}$ 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
 $x \in L \leftrightarrow A_L(x) = \text{accept}$
 $\text{time}_{A_L}(x) \leq 2^{p(|x|)}$
 Consider the following function h to reduce from L to EVAL-IN-E.
 $h(x) \equiv \langle A_L, x, p(|x|) \rangle$ for $\forall x \in \Sigma^*$
 Then, h is total and computable in polynomial time.

16/17

また, すべての $x \in \Sigma^*$ に対し
 $x \in L \leftrightarrow A_L(x) = \text{accept}$

$\leftrightarrow \text{eval}(\overline{[A]_L}, x) = \text{accept}$

$\leftrightarrow \text{eval_in_time}(\overline{[A]_L}, x, 2^{p(|x|)}) = \text{accept}$

$\leftrightarrow \langle \overline{[A]_L}, x, 2^{p(|x|)} \rangle \in \text{EVAL-IN-E}$

$\leftrightarrow h(x) \in \text{EVAL-IN-E}$

ゆえに, h は L からEVAL-IN-Eへの多項式時間還元.

$\therefore L \leq_m^p \text{EVAL-IN-E}$ for $\forall L \in \mathcal{E}\mathcal{X}\mathcal{P}$

すなわち, EVAL-IN-Eは $\mathcal{E}\mathcal{X}\mathcal{P}$ -完全.

証明終

16/17

Moreover, for each $x \in \Sigma^*$ we have
 $x \in L \leftrightarrow A_L(x) = \text{accept}$

$\leftrightarrow \text{eval}(\overline{[A]_L}, x) = \text{accept}$

$\leftrightarrow \text{eval_in_time}(\overline{[A]_L}, x, 2^{p(|x|)}) = \text{accept}$

$\leftrightarrow \langle \overline{[A]_L}, x, 2^{p(|x|)} \rangle \in \text{EVAL-IN-E}$

$\leftrightarrow h(x) \in \text{EVAL-IN-E}$

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

$\therefore L \leq_m^p \text{EVAL-IN-E}$ for $\forall L \in \mathcal{E}\mathcal{X}\mathcal{P}$

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

Q.E.D.

17/17

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 $\mathcal{E}\mathcal{X}\mathcal{P}$ -完全.

証明:

(1) EVAL-IN-Eは $\mathcal{E}\mathcal{X}\mathcal{P}$ -完全集合で, $\mathcal{E}\mathcal{X}\mathcal{P}$ -完全集合 $\notin \mathcal{P}$.
(2) $\forall L \in \mathcal{E}\mathcal{X}\mathcal{P}$ $[A \leq_m^p \text{EVAL-IN-E}]$ と
 $\mathcal{NP} \subseteq \mathcal{E}\mathcal{X}\mathcal{P}$ より.

17/17

Theorem 6.8.

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

Proof:

(1) EVAL-IN-E is $\mathcal{E}\mathcal{X}\mathcal{P}$ -complete and any $\mathcal{E}\mathcal{X}\mathcal{P}$ -complete set $\notin \mathcal{P}$.
(2) It follows from
 $\forall L \in \mathcal{E}\mathcal{X}\mathcal{P}$ $[A \leq_m^p \text{EVAL-IN-E}]$ and
 $\mathcal{NP} \subseteq \mathcal{E}\mathcal{X}\mathcal{P}$

残りの予定(Schedule)

- 11/22 (Wed):
 - レポート(6)+ α の配布(6th report + α)
 - レポート(5)の回収(submit 5th report)
- 11/24 (Fri): 講義に関するアンケート実施(Anonymous Questionnaire)
- 11/29 (Wed):
 - 期末試験と6回目のレポートの回収(Final Exam. & 6th report submission.)
 - オフィスアワー(Office Hour): 6回目のレポートの解答と解説、期末試験の解答と解説(Answers and comments for 6th report and final exam.)
- 12/1 (Fri): 休講(No class)
- 上記以降(After that...):
 - 成績などの問い合わせはメールで(Ask by e-mail if you have any questions about records, etc.)
 - レポート、試験の返却希望者は適宜取りに行くこと(Come to my office to receive the reports and/or final exam, if you want.)