

1238 計算の理論

上原 隆平

2018年I-1期(4-5月)

Announce

- Report 2: 出題は5月23日, 締切は6月4日10:50
(Distributed today; Deadline is 10:50am, June 4.)
- 5月23日のチュートリアルアワーは補講
(Today, I'll give supplemental lecture on 13:30-15:10.)
- 5月28日, 30日は出張のため休講
(Lectures will be cancelled on May 28 and May 30.)

I238 Computation Theory

by

Prof. Ryuhei Uehara

Term I-1, April-May, 2018

計算量の理論

- ゴール1:
 - “計算可能な関数/問題/言語/集合”
- ゴール2:
 - 「問題の困難さ」を示す方法を学ぶ
 - 計算可能な問題であっても、手におえない場合がある！
 - 計算に必要な資源(時間・領域)が多すぎる時
 - 関連する専門用語;
 - クラスNP, $P \neq NP$ 予想, NP困難性, 還元

Computational Complexity

- Goal 1:
 - “*Computable Function/Problem/Language/Set*”
- Goal 2:
 - How can you show “*Difficulty of Problem*”
 - There are *intractable* problems even if they are computable!
 - because they require too many resources (time/space)!
 - Technical terms;
 - The class NP, P≠NP conjecture, NP-hardness, reduction

6. 計算量の理論

• 計算量クラスの定義を概観すると...

クラスPの定義

集合Lがクラス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NPの定義

集合Lがクラス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coNPの定義

集合LがクラスcoNP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 $x \in L \Leftrightarrow \forall w \in \Sigma^* : |w| \leq q(|x|) [R(x,w)]$

6. Computational Complexity

- Observation of the classes

Definition: Class P

Set L is in the class P \Leftrightarrow

There exists a poly-time computable predicate R such that
for each $x \in \Sigma^*$, $x \in L \Leftrightarrow R(x)$

Definition: Class NP

Set L is in the class NP \Leftrightarrow

There exists a poly q and a poly-time computable predicate R such that
for each $x \in \Sigma^*$, $x \in L \Leftrightarrow \exists w \in \Sigma^* : |w| \leq q(|x|)[R(x,w)]$

Definition: Class coNP

Set L is in the class coNP \Leftrightarrow

There exists a poly q and a poly-time computable predicate R such that
for each $x \in \Sigma^*$, $x \in L \Leftrightarrow \forall w \in \Sigma^* : |w| \leq q(|x|)[R(x,w)]$

7. 多項式時間計算可能性の解析手法

7.1. 多項式時間還元可能性

定義7.1:

A と B を任意の集合とする.

(1) 関数 $h: A \rightarrow B$ が 多項式時間還元 である

- \Leftrightarrow $\left\{ \begin{array}{l} \text{(a) } h \text{ は } \Sigma^* \text{ から } \Sigma^* \text{ への全域関数である} \\ \text{(b) } x \in \Sigma^* [x \in A \leftrightarrow h(x) \in B] \\ \text{(c) } h \text{ は多項式時間計算可能である.} \end{array} \right.$

(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 であるといい,

$$A \leq_m^P B \quad \text{とかく.}$$

(...多項式時間程度の差を無視すれば, A の難しさ \leq B の難しさ)

7. Analysis on Polynomial-Time Computability

7.1. Polynomial-time Reducibility

Definition 7.1:

Let A and B be arbitrary sets.

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

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

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

Then, we denote by

$$A \leq_m^P B$$

(...within polynomial time, hardness of $A \leq$ that of B)

7. 多項式時間計算可能性の解析手法

7.1. 多項式時間還元可能性

定理7.1: $A \leq_m^P B$ のとき次が成立する

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

注意: クラス E は例外. 一般に $B \in E \rightarrow A \in E$ は成立しない.

例7.1: $\text{ONE} \equiv \{1\}$ と定義すると, P の各集合 L に対して,

$$L \leq_m^P \text{ONE}$$

である. ここで $h(x) \equiv \begin{cases} 1, & \text{if } x \in L \\ 0, & \text{otherwise} \end{cases}$

7. Analysis on Polynomial-Time Computability

7.1. Polynomial-time Reducibility

Theorem 7.1: $A \leq_m^P B$ leads to

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

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

Ex. 7.1: When we define $\text{ONE} \equiv \{1\}$, for each set L in P we have

$$L \leq_m^P \text{ONE}$$

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

7. 多項式時間計算可能性の解析手法

7.1. 多項式時間還元可能性

定理7.2: A, B, C を任意の集合とする.

$$(1) A \leq_m^P A$$

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

定義7.2:

$$A \equiv_m^P B \leftrightarrow A \leq_m^P B \wedge B \leq_m^P A$$

\equiv_m^P は同値関係.

7. Analysis on Polynomial-Time Computability

7.1. Polynomial-time Reducibility

Theorem 7.2: A, B, C : arbitrary sets

$$(1) A \leq_m^P A$$

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

Definition 7.2:

$$A \equiv_m^P B \leftrightarrow A \leq_m^P B \wedge B \leq_m^P A$$

\equiv_m^P is an equivalence relation.

7. 多項式時間計算可能性の解析手法

7.1. 多項式時間還元可能性

定理 7.3:

$$(1) 2SAT \leq_m^P 3SAT \leq_m^P SAT \leq_m^P \text{ExSAT}$$

$$(2) 3SAT \equiv_m^P SAT \equiv_m^P \text{ExSAT}$$

証明

(1) 定義によっていくつかの証明が考えられる:

(a) 定義が「各項に高々3リテラル」の場合は, 2SATの入力は 3SATの入力としても有効なので, 特に示すことはない.

(b) 各項 $(x \vee y)$ を単に $(x \vee y \vee y)$ で置き換えればよい.

(c) 各項 $(x \vee y)$ に対して新しい変数を導入して

$$(x \vee y \vee z) \wedge (x \vee y \vee \bar{z}).$$

と置き換えてもよい.

どの場合も多項式時間還元で, 元の論理式が充足可能である必要十分条件は, 新しい式が充足可能であること.

7. Analysis on Polynomial-Time Computability

7.1. Polynomial-time Reducibility

Theorem 7.3:

$$(1) 2SAT \leq_m^P 3SAT \leq_m^P SAT \leq_m^P \text{ExSAT}$$

$$(2) 3SAT \equiv_m^P SAT \equiv_m^P \text{ExSAT}$$

Proof

(1) we have some proofs depending on definition:

(a) each instance of 2SAT is also in 3SAT if the definition is “at most 3 literals in a clause”.

(b) each clause $(x \vee y)$ can be replaced by $(x \vee y \vee y)$.

(c) each clause $(x \vee y)$ can be replaced by $(x \vee y \vee z) \wedge (x \vee y \vee \bar{z})$.

In any case, they are poly-time reduction, and the original formula is satisfiable iff so is the resulting formula.

7. 多項式時間計算可能性の解析手法

7.1. 多項式時間還元可能性

定理7.3:

$$(1) 2SAT \leq_m^P 3SAT \leq_m^P SAT \leq_m^P \text{ExSAT}$$

$$(2) 3SAT \equiv_m^P SAT \equiv_m^P \text{ExSAT}$$

証明 (概略)

(2) (1)より, $\text{ExSAT} \leq_m^P 3SAT$ が成立することを示せばよい.

基本戦略:

ExSATの式 F が与えられたら, それに基づいて3SATの式 F' を構成する. ただしここで F が充足可能である必要十分条件が F' が充足可能であるようにする. そのために, まず F の計算木を構築し, 次に F の計算手順を表現する論理式 F' を構築する.

7. Analysis on Polynomial-Time Computability

7.1. Polynomial-time Reducibility

Theorem 7.3:

$$(1) \text{ 2SAT} \leq_m^P \text{ 3SAT} \leq_m^P \text{ SAT} \leq_m^P \text{ ExSAT}$$

$$(2) \text{ 3SAT} \equiv_m^P \text{ SAT} \equiv_m^P \text{ ExSAT}$$

Proof (Outline)

(2) It is sufficient to show that $\text{ExSAT} \leq_m^P \text{ 3SAT}$ by (1).

Strategy:

For any given F in ExSAT, we construct another F' in 3SAT such that F is satisfiable iff F' is satisfiable.

To do that, we first construct the computation tree of F , and construct F' that represents the computation process of F .

7. 多項式時間計算可能性の解析手法

7.1. 多項式時間還元可能性

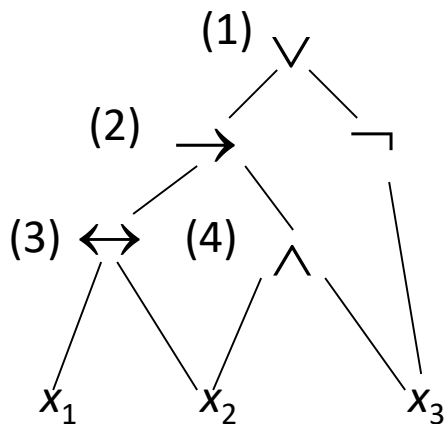
定理7.3 (2) $3\text{SAT} \equiv_m^P \text{SAT} \equiv_m^P \text{ExSAT}$

証明 (概略)

(2) $\text{ExSAT} \leq_m^P 3\text{SAT}$ が成立することを示せばよい.

ExSAT から 3SAT への還元を例で示す:

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



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

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

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

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

7. Analysis on Polynomial-Time Computability

7.1. Polynomial-time Reducibility

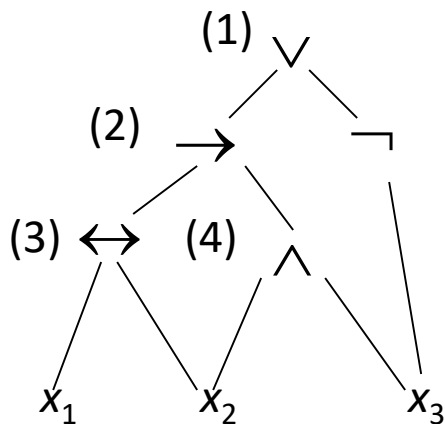
Theorem 7.3: (2) $3\text{SAT} \equiv_m^P \text{SAT} \equiv_m^P \text{ExSAT}$

Proof (Outline)

(2) It is sufficient to show that $\text{ExSAT} \leq_m^P 3\text{SAT}$ by (1).

Reduction from ExSAT to 3SAT by an example:

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



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

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

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

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

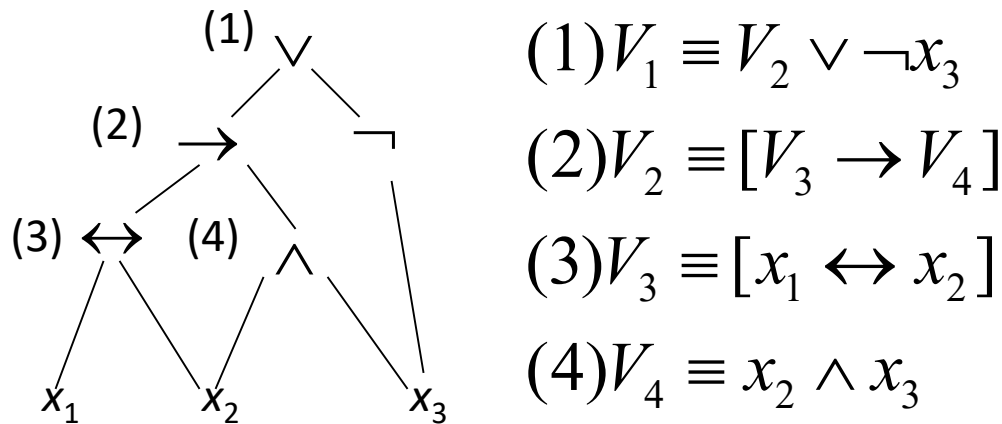
7. 多項式時間計算可能性の解析手法

7.1. 多項式時間還元可能性

定理7.3: (2) $3SAT \equiv_m^P SAT \equiv_m^P ExSAT$

ExSAT から 3SAT への還元を例で示す:

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



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

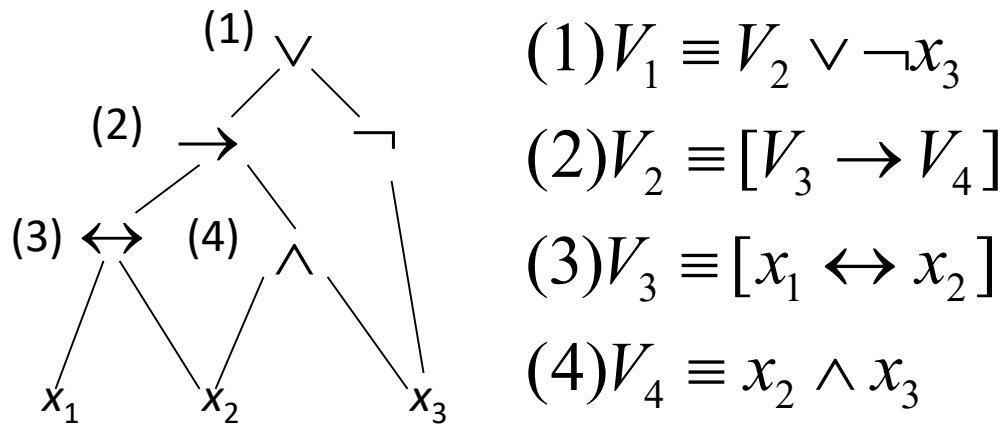
7. Analysis on Polynomial-Time Computability

7.1. Polynomial-time Reducibility

Theorem 7.3: (2) $3\text{SAT} \equiv_m^P \text{SAT} \equiv_m^P \text{ExSAT}$

Reduction from ExSAT to 3SAT by an example:

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



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

7. 多項式時間計算可能性の解析手法

7.1. 多項式時間還元可能性

定理7.3: (2) $3SAT \equiv_m^P SAT \equiv_m^P ExSAT$

ExSAT から 3SAT への還元を例で示す:

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

このとき構成から, $F()$ は充足可能 $\Leftrightarrow F''()$ は充足可能.
 $F''()$ をこれと同値な 3SAT の要素 $F'()$ で表現する.

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

他のケースも同様に変形でき, $F'()$ は 3SAT の要素となる.

7. Analysis on Polynomial-Time Computability

7.1. Polynomial-time Reducibility

Theorem 7.3: (2) $3\text{SAT} \equiv_m^P \text{SAT} \equiv_m^P \text{ExSAT}$

Reduction from ExSAT to 3SAT by an example:

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

Then, by construction, $F()$ is satisfiable iff $F''()$ is satisfiable.

We show $F''()$ can be represented by an equivalent $F'()$ in 3SAT.

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

The other cases are similar, and $F'()$ is in 3SAT.

7. 多項式時間計算可能性の解析手法

7.2. 完全性

7.2.1. 定義と基本性質

定義7.3:

クラスCに対して, 集合Aが次を満たすとき

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

集合Aは(\leq_m^P のもとで) **C困難**であるという.

さらに次を満たすなら

$$(b) A \in C$$

Aは**C完全**であるという.

例7.2: NP完全集合の例

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

7. Analysis on Polynomial-Time Computability

7.2. Completeness

7.2.1. Definition and basic properties

Definition 7.3:

For a class C , if a set A satisfies

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

the set A is called **C-hard** (under \leq_m^P).

Moreover, if we have

(b) $A \in C$,

then A is called **C-complete**.

Ex. 7.2: Examples of NP-complete sets

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

7. 多項式時間計算可能性の解析手法

7.2. 完全性

7.2.1. 定義と基本性質

定理7.4: C 困難(または C 完全)な任意の集合 A に対して,

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

証明:

(1) 任意の C 集合を B とする. A が C 困難であることから,

$B \leq_m^P A$ であり, $A \in P$ という仮定より $B \in P$ をえる.

(2), (3), (4) も同様.

7. Analysis on Polynomial-Time Computability

7.2. Completeness

7.2.1. Definition and basic properties

Theorem 7.4: 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) $A \in \text{coNP} \rightarrow C \subseteq \text{coNP}$ | CP: $C \not\subseteq \text{coNP} \rightarrow A \notin \text{coNP}$ |
| (4) $A \in \text{EXP} \rightarrow C \subseteq \text{EXP}$ | CP: $C \not\subseteq \text{EXP} \rightarrow A \notin \text{EXP}$ |

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 $B \in P$

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

7. 多項式時間計算可能性の解析手法

7.2. 完全性

7.2.1. 定義と基本性質

定理7.4: C 困難(または C 完全)な任意の集合 A に対して,

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

例7.3: クラス NP に関する定理の意味するところ

NP 完全集合を A とする.

定理(1)の対偶より: $NP \neq P \rightarrow A \notin P$

つまり, NP 完全集合は $P=NP$ でない限り,

多項式時間では認識できない NP 集合である.

7. Analysis on Polynomial-Time Computability

7.2. Completeness

7.2.1. Definition and basic properties

Theorem 7.4: 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) $A \in \text{coNP} \rightarrow C \subseteq \text{coNP}$ | CP: $C \not\subseteq \text{coNP} \rightarrow A \notin \text{coNP}$ |
| (4) $A \in \text{EXP} \rightarrow C \subseteq \text{EXP}$ | CP: $C \not\subseteq \text{EXP} \rightarrow A \notin \text{EXP}$ |

Ex. 7.3: Meaning of Theorem for class NP

Let A be NP-complete set.

By the contraposition of Theorem (1) we have

$$NP \neq P \rightarrow A \notin P$$

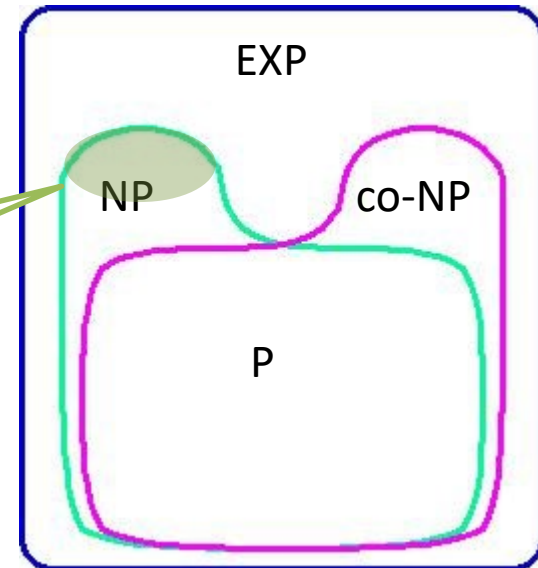
That is, NP-complete sets are NP-sets that cannot be recognized in polynomial time unless $P = NP$.

7. 多項式時間計算可能性の解析手法

7.2. 完全性

7.2.1. 定義と基本性質

NP完全問題とは、クラスNPの中で最も難しい問題群を構成しているといえる。



例7.3: クラスNPに関する定理の意味するところ

NP完全集合をAとする。

定理(1)の対偶より: $NP \neq P \rightarrow A \notin P$

つまり, NP完全集合は $P=NP$ でない限り,

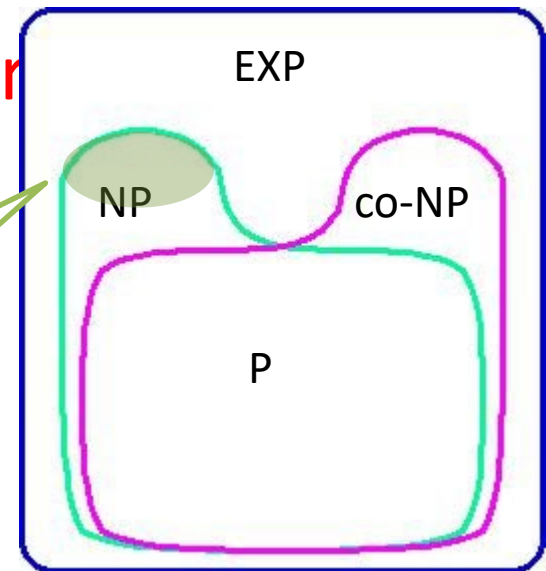
多項式時間では認識できないNP集合である。

7. Analysis on Polynomial-Time Computability

7.2. Completeness

7.2.1. Definition and basic properties

NP-complete problems form the most difficult problems in the class NP.



Ex. 7.3: Meaning of Theorem for class NP

Let A be NP-complete set.

By the contraposition of Theorem (1) we have

$$NP \neq P \rightarrow A \notin P$$

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

7. 多項式時間計算可能性の解析手法

7.2. 完全性

7.2.1. 定義と基本性質

定理7.5: A :任意のC完全集合
任意の集合 B に対して以下が成立
(1) $A \leq_m^P B \rightarrow B$ は C 困難.
(2) $A \leq_m^P B$ かつ $B \in C \rightarrow B$ は C 完全.

証明:

定義より, $\forall L \in \mathcal{Q}[L \leq_m^P A]$

定理より, $L \leq_m^P A \wedge A \leq_m^P B \rightarrow L \leq_m^P B$

よって, $\forall L \in \mathcal{Q}[L \leq_m^P B]$

つまり B は C 困難.

ひとたび NP 完全問題 A が得られたら, これを使って他の問題の困難性を「測定」できる.

7. Analysis on Polynomial-Time Computability

7.2. Completeness

7.2.1. Definition and basic properties

Theorem 7.5: A : any C-complete set

For any set B we have

(1) $A \leq_m^P B \rightarrow B$ is C-hard.

(2) $A \leq_m^P B$ and $B \in C \rightarrow B$ is C-complete.

Proof:

By definition, $\forall L \in C [L \leq_m^P A]$

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

Therefore, $\forall L \in C [L \leq_m^P B]$

That is, B is C-hard.

Once you have an NP-complete problem A , it can be used to measure to the other problems