

アナウンス(覚書)

- レポート(2):出題は5月22日, 締切は5月29日
- 5月24日のチュートリアルアワーは補講をします
- 期末試験:5月31日チュートリアルアワー
 - 前回と同じ形式?
 - 出題範囲は「計算量」のみにする予定

1238 計算の理論

上原 隆平

2018年I-1期(4-5月)

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

5. 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

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 $x \in L \iff R(x)$

クラスNPの定義

集合LがクラスNPに入る

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 $x \in L \iff \exists w \in \Sigma^* : |w| \leq q(|x|) \wedge R(x, w)$

クラスcoNPの定義

集合LがクラスcoNPに入る

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 $x \in L \iff \forall w \in \Sigma^* : |w| \leq q(|x|) \wedge R(x, w)$

5. Computational Complexity

- Observation of the classes

Definition: Class P

Set L is in the class P

There exists a poly-time computable predicate R such that

for each $x \in \Sigma^*$, $x \in L \iff R(x)$

Definition: Class NP

Set L is in the class NP

There exists a poly q and a poly-time computable predicate R such that

for each $x \in \Sigma^*$, $x \in L \iff \exists w \in \Sigma^* : |w| \leq q(|x|) \wedge R(x,w)$

Definition: Class coNP

Set L is in the class coNP

There exists a poly q and a poly-time computable predicate R such that

for each $x \in \Sigma^*$, $x \in L \iff \forall w \in \Sigma^* : |w| \leq q(|x|) \implies R(x,w)$

6. 多項式時間計算可能性の解析手法

6.1. 多項式時間還元可能性

定義

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,

$A \leq_m^P B$ とかく.

(...多項式時間程度の差を無視すれば, A の難しさ B の難しさ)

6. Analysis on Polynomial-Time Computability

6.1. Polynomial-time Reducibility

Definition

Let A and B be arbitrary sets.

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

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

(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 that of B)

6. 多項式時間計算可能性の解析手法

6.1. 多項式時間還元可能性

定理 $A \leq_m^P B$ 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: $\text{ONE} \equiv \{1\}$ 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 $h(x) \equiv \begin{cases} 1, & \text{if } x \in L \\ 0, & \text{otherwise} \end{cases}$

6. Analysis on Polynomial-Time Computability

6.1. Polynomial-time Reducibility

Theorem $A \leq_m^P B$ 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.: When we define $\text{ONE} \equiv \{1\}$, for each set L in P we have

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

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

6. 多項式時間計算可能性の解析手法

6.1. 多項式時間還元可能性

定理 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

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

\equiv_m^P は同値関係.

6. Analysis on Polynomial-Time Computability

6.1. Polynomial-time Reducibility

Theorem 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

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

\equiv_m^P is an equivalence relation.

6. 多項式時間計算可能性の解析手法

6.1. 多項式時間還元可能性

定理

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

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

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, 特を示すことはない.

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

(c) 各項 $(x \ y)$ に対して新しい変数を導入して

$$(x \ y \ z) \quad (x \ y \ \bar{z}).$$

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.

6. Analysis on Polynomial-Time Computability

6.1. Polynomial-time Reducibility

Theorem

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

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

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.

6. 多項式時間計算可能性の解析手法

6.1. 多項式時間還元可能性

定理

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

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

証明 (概略)

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

6. Analysis on Polynomial-Time Computability

6.1. Polynomial-time Reducibility

Theorem

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

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

Proof (Outline)

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

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 .

6. 多項式時間計算可能性の解析手法

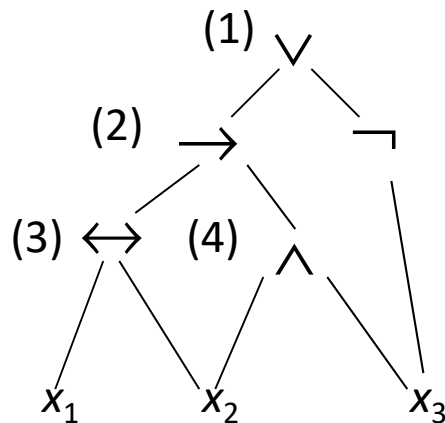
6.1. 多項式時間還元可能性

定理 (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:

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



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

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

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

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

6. Analysis on Polynomial-Time Computability

6.1. Polynomial-time Reducibility

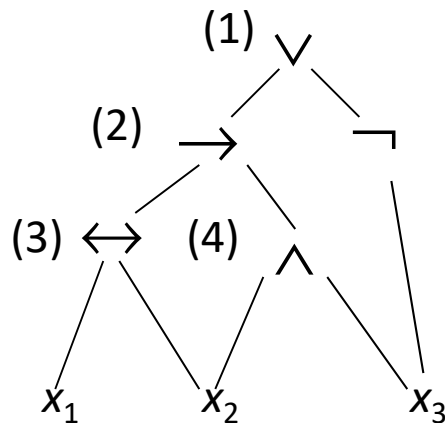
Theorem (2) $3\text{SAT} \equiv_m^P \text{SAT} \equiv_m^P \text{ExSAT}$

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:

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



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

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

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

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

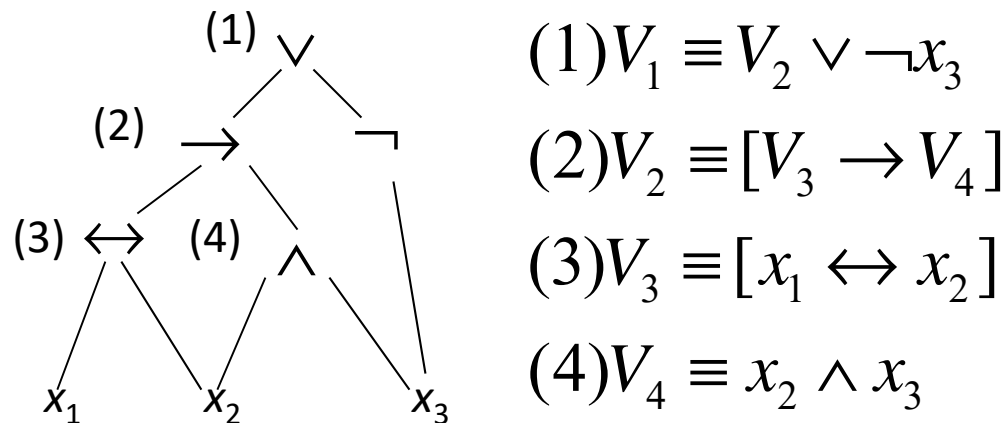
6. 多項式時間計算可能性の解析手法

6.1. 多項式時間還元可能性

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

ExSAT から 3SAT への還元を例で示す:

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



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

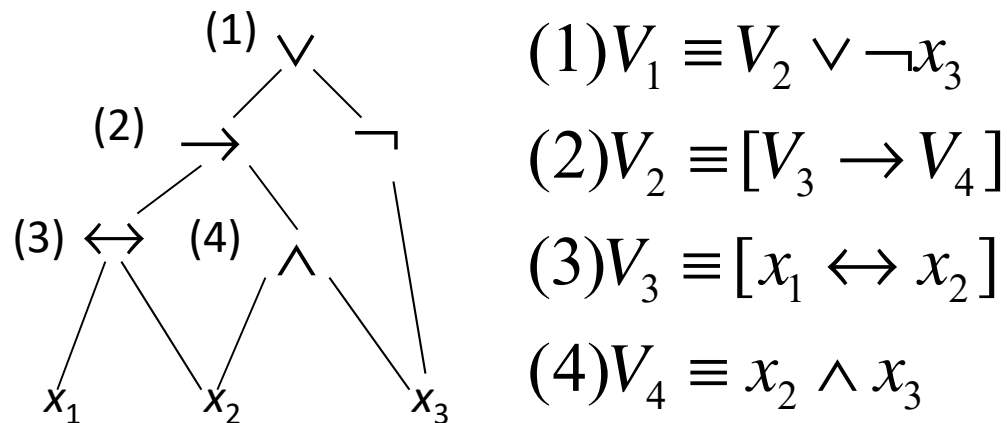
6. Analysis on Polynomial-Time Computability

6.1. Polynomial-time Reducibility

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

Reduction from ExSAT to 3SAT by an example:

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



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

6. 多項式時間計算可能性の解析手法

6.1. 多項式時間還元可能性

定理 (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 $F''()$ 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.

6. Analysis on Polynomial-Time Computability

6.1. Polynomial-time Reducibility

Theorem (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.

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

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

6. 多項式時間計算可能性の解析手法

6.2. 完全性

6.2.1. 定義と基本性質

定義

クラスCに対して, 集合Aが次を満たすとき

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

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

$$(b) \quad A \in C$$

Aは**C完全**であるという.

例. NP完全集合の例

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

6. Analysis on Polynomial-Time Computability

6.2. Completeness

6.2.1. Definition and basic properties

Definition

For a class C , if a set A satisfies

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

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. Examples of NP-complete sets

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

6. 多項式時間計算可能性の解析手法

6.2. 完全性

6.2.1. 定義と基本性質

定理 C 困難(または C 完全)な任意の集合 A に対して,

- | | |
|---|---|
| (1) $A \in P \rightarrow C \in P$ | 対偶: $C \notin P \rightarrow A \notin P$ |
| (2) $A \in NP \rightarrow C \in NP$ | 対偶: $C \notin NP \rightarrow A \notin NP$ |
| (3) $A \in coNP \rightarrow C \in coNP$ | 対偶: $C \notin coNP \rightarrow A \notin coNP$ |
| (4) $A \in EXP \rightarrow C \in EXP$ | 対偶: $C \notin EXP \rightarrow A \notin EXP$ |

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.

6. Analysis on Polynomial-Time Computability

6.2. Completeness

6.2.1. Definition and basic properties

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

- | | |
|---|---|
| (1) $A \in P \rightarrow C \in P$ | CP: $C \notin P \rightarrow A \notin P$ |
| (2) $A \in NP \rightarrow C \in NP$ | CP: $C \notin NP \rightarrow A \notin NP$ |
| (3) $A \in \text{coNP} \rightarrow C \in \text{coNP}$ | CP: $C \notin \text{coNP} \rightarrow A \notin \text{coNP}$ |
| (4) $A \in \text{EXP} \rightarrow C \in \text{EXP}$ | CP: $C \notin \text{EXP} \rightarrow A \notin \text{EXP}$ |

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.

6. 多項式時間計算可能性の解析手法

6.2. 完全性

6.2.1. 定義と基本性質

定理 C 困難(または C 完全)な任意の集合 A に対して,

- | | |
|---|---|
| (1) $A \in P \rightarrow C \in P$ | 対偶: $C \notin P \rightarrow A \notin P$ |
| (2) $A \in NP \rightarrow C \in NP$ | 対偶: $C \notin NP \rightarrow A \notin NP$ |
| (3) $A \in coNP \rightarrow C \in coNP$ | 対偶: $C \notin coNP \rightarrow A \notin coNP$ |
| (4) $A \in EXP \rightarrow C \in EXP$ | 対偶: $C \notin EXP \rightarrow A \notin EXP$ |

例: 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.

6. Analysis on Polynomial-Time Computability

6.2. Completeness

6.2.1. Definition and basic properties

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

- | | | | |
|-------|----------------------|------|--|
| (1) A | $P \rightarrow C$ | P | CP: $C \not\subseteq P \rightarrow A \notin P$ |
| (2) A | $NP \rightarrow C$ | NP | CP: $C \not\subseteq NP \rightarrow A \notin NP$ |
| (3) A | $coNP \rightarrow C$ | coNP | CP: $C \not\subseteq coNP \rightarrow A \notin coNP$ |
| (4) A | $EXP \rightarrow C$ | EXP | CP: $C \not\subseteq EXP \rightarrow A \notin EXP$ |

Ex. : Meaning of Theorem for class NP

Let A be NP-complete set.

By the contraposition of Theorem (1) we have

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

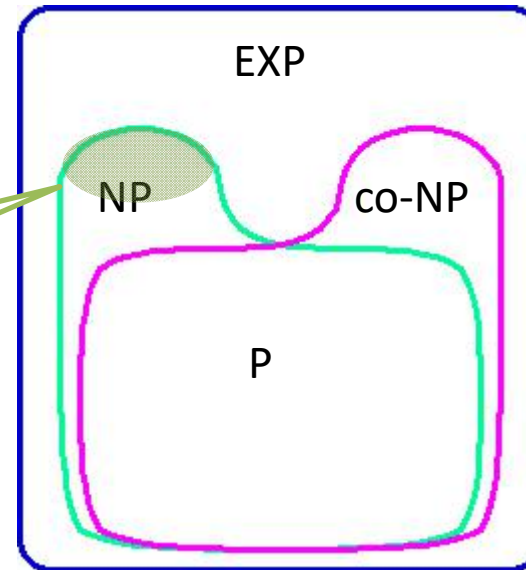
That is, NP-complete sets are NP-sets that cannot be recognized in polynomial time unless $P = NP$.

6. 多項式時間計算可能性の解析手法

6.2. 完全性

6.2.1. 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：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、

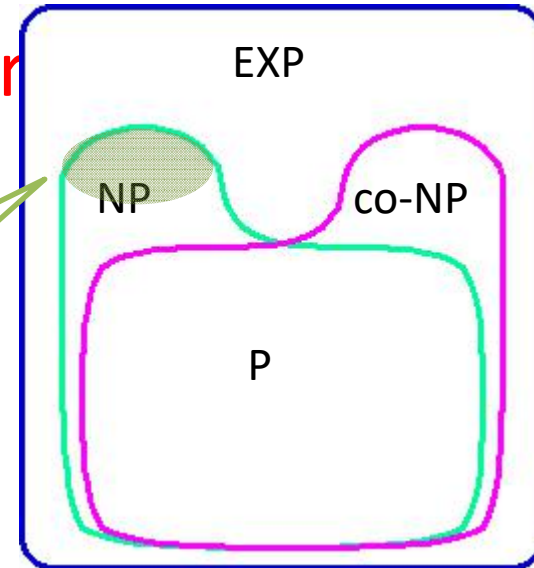
多項式時間では認識できないNP集合である。

6. Analysis on Polynomial-Time Computability

6.2. Completeness

6.2.1. Definition and basic properties

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



Ex. : 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 $P = NP$.

6. 多項式時間計算可能性の解析手法

6.2. 完全性

6.2.1. 定義と基本性質

定理 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, $\forall L \in C [L \leq_m^P A]$

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

よって, $\forall L \in C [L \leq_m^P B]$

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。

6. Analysis on Polynomial-Time Computability

6.2. Completeness

6.2.1. Definition and basic properties

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) $A \leq_m^P B$ 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

残りの予定 (Schedule)

5/29(Tue): 多項式時間還元性に基づく完全性

- レポート提出, 解答と解説

5/31(Thu): (たぶん終わらないので) 上記の続き & 補足

- 講義アンケート
- 残った時間は質問など.

5/31(Thu)のチュートリアルアワー: 期末試験(Final Exam)

- 30点満点
- 範囲は後半の「計算量の理論」から
- 選択肢(Choices); 5月29日に多数決で決めましょう.
 - 教科書/スライド/ノート (Textbooks, copy of slides, and hand written notes)
 - スライドのコピー/手書きノート/筆記用具のみ(Copy of slides, hand-written note, and pens/pencils)
 - 筆記用具のみ(Only pens and pencils)