アナウンス（覚書）

- レポート(2)：締切は5月29日
- 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

I238 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）が多すぎるとき
    - 関連する専門用語;
      クラスNP, P≠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$x \in L \Leftrightarrow R(x)$

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$x \in L \Leftrightarrow \exists w \in \Sigma^*: |w| \leqq q(|x|)[R(x,w)]$

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$x \in L \Leftrightarrow \forall w \in \Sigma^*: |w| \leqq q(|x|)[R(x,w)]$

5. Computational Complexity

- Observation of the classes

<u>Definition</u>: Class P

Set L is in the class P ⇔

There exists a poly-time computable predicate R such that

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

<u>Definition</u>: 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 $x \in \Sigma^*$, $x \in L \Leftrightarrow \exists w \in \Sigma^* : |w| \leqq q(|x|)[R(x,w)]$

<u>Definition</u>: 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 $x \in \Sigma^*$, $x \in L \Leftrightarrow \forall w \in \Sigma^* : |w| \leqq q(|x|)[R(x,w)]$

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*→*B* が多項式時間還元である

$\Longleftrightarrow$
(a) *h* はΣ^* からΣ^*への全域関数である
(b) $x \in \Sigma^*[x \in A \leftrightarrow h(x) \in B]$
(c) *h* は多項式時間計算可能である.

(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,

$\boxed{A \leq_m^P B}$ 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*→*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 poly-time reduction from *A* to *B*, we say *A* is polynomial-time reducible to *B*.

Then, we denote by $\boxed{A \leq_m^P B}$

(...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, 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) $A \le_m^P A$

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

Definition

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

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

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

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.

6. Analysis on Polynomial-Time Computability

6.1. Polynomial-time Reducibility

Theorem

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

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

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

6.2.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) $\forall L \in C\ [L \leq_m^P A]$

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. 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) $\forall L \in$ 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. 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) $A \in \mathrm{P} \rightarrow \mathrm{C} \subseteq P$　　対偶: $\mathrm{C} \not\subset \mathrm{P} \rightarrow A \notin \mathrm{P}$

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

(3) $A \in \mathrm{coNP} \rightarrow \mathrm{C} \subseteq coNP$　　対偶: $\mathrm{C} \not\subset \mathrm{coNP} \rightarrow A \notin \mathrm{coNP}$

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

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, $A \in \mathrm{P}$という仮定より$B \in \mathrm{P}$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) $A \in \mathrm{P} \rightarrow \mathrm{C} \subseteq P$ CP: $\mathrm{C} \not\subseteq \mathrm{P} \rightarrow A \notin \mathrm{P}$

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

(3) $A \in \mathrm{coNP} \rightarrow \mathrm{C} \subseteq coNP$ CP: $\mathrm{C} \not\subseteq \mathrm{coNP} \rightarrow A \notin \mathrm{coNP}$

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

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 $A \in \mathrm{P}$, we have $B \in \mathrm{P}$

(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) $A \in \mathrm{P} \rightarrow \mathrm{C} \subseteq P$　　対偶: $\mathrm{C} \not\subset \mathrm{P} \rightarrow A \notin \mathrm{P}$
(2) $A \in \mathrm{NP} \rightarrow \mathrm{C} \subseteq NP$　　対偶: $\mathrm{C} \not\subset \mathrm{NP} \rightarrow A \notin \mathrm{NP}$
(3) $A \in \mathrm{coNP} \rightarrow \mathrm{C} \subseteq coNP$　　対偶: $\mathrm{C} \not\subset \mathrm{coNP} \rightarrow A \notin \mathrm{coNP}$
(4) $A \in \mathrm{EXP} \rightarrow \mathrm{C} \subseteq EXP$　　対偶: $\mathrm{C} \not\subset \mathrm{EXP} \rightarrow A \notin \mathrm{EXP}$

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:　$\mathrm{NP} \neq \mathrm{P} \rightarrow A \notin \mathrm{P}$
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) $A \in \mathrm{P} \rightarrow \mathrm{C} \subseteq \mathrm{P}$ CP: $\mathrm{C} \not\subset \mathrm{P} \rightarrow A \notin \mathrm{P}$

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

(3) $A \in \mathrm{coNP} \rightarrow \mathrm{C} \subseteq \mathrm{coNP}$ CP: $\mathrm{C} \not\subset \mathrm{coNP} \rightarrow A \notin \mathrm{coNP}$

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

Ex. : Meaning of Theorem for class NP

Let A be NP-complete set.

By the contraposition of Theorem (1) we have

$$\mathrm{NP} \neq \mathrm{P} \rightarrow A \notin \mathrm{P}$$

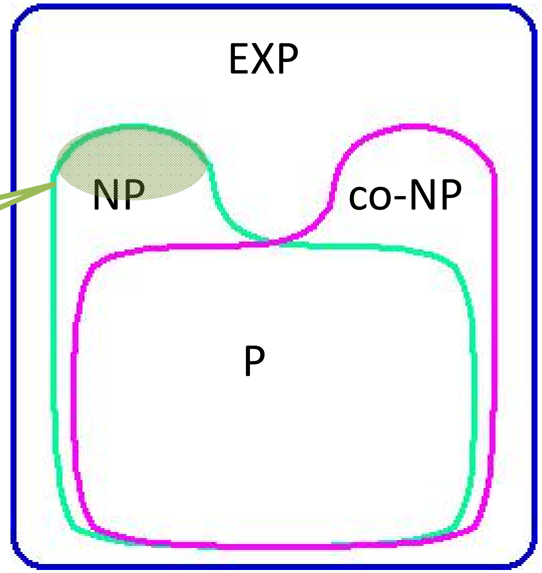
That is, NP-complete sets are NP-sets that cannot be recognized in polynomial time unless P = NP.

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≠P ➔ $A \notin$ P

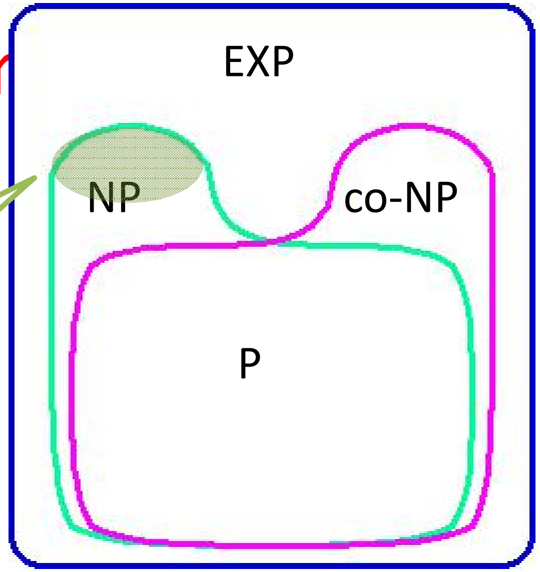
つまり，NP完全集合はP=NPでない限り，

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 proper



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

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

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) $A \le_m^P B$ → B は C困難.

(2) $A \le_m^P B$ かつ $B \in$ C → B は C完全.

証明:

定義より, $\forall L \in \mathrm{C}[L \le_m^P A]$

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

よって, $\forall L \in \mathrm{C}[L \le_m^P B]$

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

Proof :
By definition, $\forall L \in \mathrm{C}[L \le_m^P A]$
By Theorem, $L \le_m^P A \wedge A \le_m^P B \rightarrow L \le_m^P B$
Therefore, $\forall L \in \mathrm{C}[L \le_m^P B]$
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): 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)