計算量クラス間の定義を概観すると…

クラス$\mathcal{P}$の定義(5章)
集合Lがクラス$\mathcal{P}$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$\mathcal{NP}$の定義(定義5.2)
集合Lがクラス$\mathcal{NP}$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co-$\mathcal{NP}$の定義(定理5.5)
集合Lがクラスco-$\mathcal{NP}$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$x \in L \Leftrightarrow \forall w \in \Sigma^*: |w| \leqq q(|x|)[R(x,w)]$

Observation of the definitions of the classes…

Def: Class $\mathcal{P}$ (Chapter 5)
Set L is in the class $\mathcal{P}$ ⇔
There exists a poly-time computable predicate R such that
for each $x \in \Sigma^*$, $x \in L \Leftrightarrow R(x)$

Def: Class $\mathcal{NP}$ (Def 5.2)
Set L is in the class $\mathcal{NP}$ ⇔
There exists a poly q and a poly-time computable pred. R s.t.
for each $x \in \Sigma^*$, $x \in L \Leftrightarrow \exists w \in \Sigma^*: |w| \leqq q(|x|)[R(x,w)]$

Def: Class co-$\mathcal{NP}$ (Theorem 5.5)
Set L is in the class co-$\mathcal{NP}$ ⇔
There exists a poly q and a poly-time computable pred. R s.t.
for each $x \in \Sigma^*$, $x \in L \Leftrightarrow \forall w \in \Sigma^*: |w| \leqq q(|x|)[R(x,w)]$

6/12

例5.9: 素数判定問題

$$\lceil n \rceil \notin \text{PRIME} \leftrightarrow \exists m{:}1 < m < n[\ n \bmod m = 0]$$

したがって，$q_p(n) = n$とし，

$$R_p(x,w) \leftrightarrow [x \notin \mathrm{N}] \vee [[w \in \mathrm{N}] \wedge [1 < m < n] \wedge [n \bmod m = 0]]$$

(ただし，n, mは各々x, wが表す自然数，
Nは自然数の2進表記全体）
と定義すると，
すべての $x \in \Sigma^*$ に対し，　$x \notin \text{PRIME} \leftrightarrow \exists q_p w[R_p(x,w)]$
これは，$x \notin$ PRIMEに対する証拠
よって，$\overline{\text{PRIME}} \in \mathcal{NP}$, i.e., PRIME $\in$ co-$\mathcal{NP}$
実際，$Q(x, w) \leftrightarrow \neg R_p(x, w)$ とすると
PRIME = $\{x{:}\ \forall q_p w\ [Q_p(x, w)]\}$
と表せる.

PRIME $\in \mathcal{NP}$ も示せるが，その証明はもっと複雑.

6/12

Ex.5.9: Primality testing

$$\lceil n \rceil \notin \text{PRIME} \leftrightarrow \exists m{:}1 < m < n[\ n \bmod m = 0]$$

Therefore, for $q_p(n) = n$,

$$R_p(x,w) \leftrightarrow [x \notin \mathrm{N}] \vee [[w \in \mathrm{N}] \wedge [1 < m < n] \wedge [n \bmod m = 0]]$$

(where, n and m are natural numbers represented by x and w.
N is a set of all natural numbers in the binary form)
This definition leads to
for every $x \in \Sigma^*$ we have $x \notin \text{PRIME} \leftrightarrow \exists q_p w[R_p(x,w)]$
This is a witness to $x \notin$ PRIME
Thus, $\overline{\text{PRIME}} \in \mathcal{NP}$, i.e., PRIME $\in$ co-$\mathcal{NP}$
In fact, using $Q(x, w) \leftrightarrow \neg R_p(x, w)$, PRIME can be expressed as
PRIME = $\{x{:}\ \forall q_p w\ [Q_p(x, w)]\}$

We can also show that PRIME $\in \mathcal{NP}$, but its proof is more complex.

7/12

$\mathcal{NP}$問題の例

・**合成数判定問題**(COMPOSITE)
入力：自然数n
質問：nは合成数か？（素数でないか？）

・**ナップサック問題**(KNAP)
入力：自然数の組$< a_1, a_2, \ldots, a_n, b >$
質問：$\sum_{i \in S} a_i = b$ となる添字の集合 $S \subseteq \{1, \ldots, n\}$があるか？

・**箱詰め問題**(BIN)
入力：自然数の組$< a_1, a_2, \ldots, a_n, b, k>$
質問：添字の集合$U=\{1, \ldots, n\}$を$U_1, \ldots, U_k$のk個に分割し，
各jで $\sum_{i \in U_j} a_i \leq b$ とすることは可能か？

・**頂点被覆問題**(VC)
入力：無向グラフGと自然数kの組$<G, k>$
質問：Gにk頂点の頂点被覆が存在するか？

頂点被覆S:
どの辺(u,v)も
u,vの一方は
Sに含まれる

7/12

Examples of $\mathcal{NP}$ problems

・**Composite Number Testing Problem**(COMPOSITE)
input：natural number n
question：Is n composite? (Is it not prime?)

・**Knapsack Problem**(KNAP)
input：n+1 tuple of natural numbers $< a_1, a_2, \ldots, a_n, b>$
question：Is there a set of indices $S \subseteq \{1, \ldots, n\}$ s.t. $\sum_{i \in S} a_i = b$?

・**Bin Packing Problem**(BIN)
input：n+2 tuple of natural numbers $< a_1, a_2, \ldots, a_n, b, k>$
question：Is there a partition of a set of indices $U=\{1, \ldots, n\}$
into $U_1, \ldots, U_k$ such that $\sum_{i \in U_j} a_i \leq b$ for each j?

・**Vertex Cover Problem**(VC)
input：pair of undirected graph G and natural number k $<G, k>$
question： Is there a vertex cover of k vertices over G?

Vertex Cover S contains at least one of u and v for each edge (u,v).

8/12

5.3. 計算量クラス間の関係

定理5.6: $\mathcal{P} \subseteq \mathcal{E} \subseteq \mathcal{EXP}$.

定義より，明らか.

定理5.7: $\mathcal{P} \subsetneq \mathcal{E} \subsetneq \mathcal{EXP}$.

階層定理(定理4.4):
任意の制限時間 t_1, t_2 に対し、
$\forall c > 0, \overset{\infty}{\forall} n[ct_1(n)^2 \le t_2(n)]$
$\rightarrow \mathrm{TIME}(t_1) \subsetneq \mathrm{TIME}(t_2)$

証明:
(1) $\mathcal{P} \subsetneq \mathcal{E}$.
$t_1(n)=2^n$, $t_2(n)=2^{3n}$とすると，階層定理より，
$\mathrm{TIME}(2^n) \subsetneq \mathrm{TIME}(2^{3n})$
一方，$\mathcal{P} \subseteq \mathrm{TIME}(2^n) \subsetneq \mathrm{TIME}(2^{3n}) \subseteq \mathcal{E}$だから，
$\mathcal{P} \subsetneq \mathcal{E}$.
(2)も同様.

証明終

8/12

5.3. Relation in the Complexity Class

Theorem 5.6: $\mathcal{P} \subseteq \mathcal{E} \subseteq \mathcal{EXP}$.

Obvious from the definition.

Theorem 5.7: $\mathcal{P} \subsetneq \mathcal{E} \subsetneq \mathcal{EXP}$.

Hierarchy Thm. (Thm. 4.4):
For any times t_1, t_2 ,
$\forall c > 0, \overset{\infty}{\forall} n[ct_1(n)^2 \le t_2(n)]$
$\rightarrow \mathrm{TIME}(t_1) \subsetneq \mathrm{TIME}(t_2)$

Proof:
(1) $\mathcal{P} \subsetneq \mathcal{E}$.
For $t_1(n)=2^n$, $t_2(n)=2^{3n}$, from the hierarchy theorem we have
$\mathrm{TIME}(2^n) \subsetneq \mathrm{TIME}(2^{3n})$
On the other hand, since $\mathcal{P} \subseteq \mathrm{TIME}(2^n) \subsetneq \mathrm{TIME}(2^{3n}) \subseteq \mathcal{E}$
$\mathcal{P} \subsetneq \mathcal{E}$.
(2) is similar.

Q.E.D.

9/12

定理5.8.
(1) $\mathcal{P} \subseteq \mathcal{NP}$, $\mathcal{P} \subseteq$ co-$\mathcal{NP}$ ($\therefore \mathcal{P} \subseteq \mathcal{NP} \cap$ co-$\mathcal{NP}$)
(2) $\mathcal{NP} \subseteq \mathcal{EXP}$, co-$\mathcal{NP} \subseteq \mathcal{EXP}$ ($\therefore \mathcal{NP} \cup$ co-$\mathcal{NP} \subseteq \mathcal{EXP}$)

証明: (1) $\mathcal{P} \subseteq \mathcal{NP}$ （$\mathcal{P} \subseteq$ co-$\mathcal{NP}$ も同様）
L: 任意の$\mathcal{P}$集合
➔ Lは多項式時間で認識可能
よって，多項式時間計算可能述語Pを用いて次のように書ける.
$\forall x \in \Sigma^*: [x \in L \leftrightarrow P(x)]$ or $P = \{x: P(x)\}$
$R(x, w) = P(x)$と定義 （第2引数は無視）
→ 任意の多項式qについて，
$L = \{x: \exists_q w[\ R(x,w)]\}$
よって，$\mathcal{NP}$の定義より，$L \in \mathcal{NP}$ i.e., $\mathcal{P} \subseteq \mathcal{NP}$.

9/12

Theorem 5.8.
(1) $\mathcal{P} \subseteq \mathcal{NP}$, $\mathcal{P} \subseteq$ co-$\mathcal{NP}$ ($\therefore \mathcal{P} \subseteq \mathcal{NP} \cap$ co-$\mathcal{NP}$)
(2) $\mathcal{NP} \subseteq \mathcal{EXP}$, co-$\mathcal{NP} \subseteq \mathcal{EXP}$ ($\therefore \mathcal{NP} \cup$ co-$\mathcal{NP} \subseteq \mathcal{EXP}$)

Proof:
(1) $\mathcal{P} \subseteq \mathcal{NP}$ （$\mathcal{P} \subseteq$ co-$\mathcal{NP}$ is similar）
L: arbitrary $\mathcal{P}$ set
➔ L is recognizable in polynomial time
Thus, we have the following description using a polynomial-time computable predicate P.
$\forall x \in \Sigma^*: [x \in L \leftrightarrow P(x)]$ or $P = \{x: P(x)\}$

We define $R(x, w) = P(x)$ （neglecting the second argument）
→ for any polynomial q,
$L = \{x: \exists_q w[\ R(x,w)]\}$
Thus, from the definition of $\mathcal{NP}$, $L \in \mathcal{NP}$ i.e., $\mathcal{P} \subseteq \mathcal{NP}$.

10/12

(2) $\mathcal{NP} \subseteq \mathcal{EXP}$ (co-$\mathcal{NP} \subseteq \mathcal{EXP}$)
L: 任意の$\mathcal{NP}$集合
➔多項式qと多項式時間計算可能述語Rが存在して，
$L = \{x : \exists_q w[R(x,w)]\} = \{x : \exists_q w[|\ w| \le q(|\ x\ |) \wedge R(x,w)]\}$
qとRを用いて，Lを認識するプログラムを作る.

```
prog L(input x);
begin
    for each w ∈ Σ^{≤q(|x|)} do
      if R(x, w) then accept end-if
    end-for;
    reject
end.
```

長さlの入力に対するプログラムの時間計算量:
Rは多項式時間計算可能だったから，ある多項式pに対し，
Rの計算時間$=p(|x| + |w|) \le p(l + q(l))$ ⟵ l の多項式
全体では，$\{p(l+q(l)) + cq(l)\}2^{q(l)} + d = O(2^{\,l+q(l)})$
よって，$L \in \mathcal{EXP}$ → $\mathcal{NP} \subseteq \mathcal{EXP}$

証明終

10/12

(2) $\mathcal{NP} \subseteq \mathcal{EXP}$ (co-$\mathcal{NP} \subseteq \mathcal{EXP}$)
L: any $\mathcal{NP}$ set
➔There is some polynomial q and polynomial-time computable predicate R such that
$L = \{x : \exists_q w[R(x,w)]\} = \{x : \exists_q w[|\ w| \le q(|\ x\ |) \wedge R(x,w)]\}$

```
prog L(input x);
begin
    for each w ∈ Σ^{≤q(|x|)} do
      if R(x, w) then accept end-if
    end-for;
    reject
end.
```

program recognizing L using q and R

time complexity of the program for an input of length l:
Since R is polynomial-time computable, for some polynomial q
time of $R=p(|x| + |w|) \le p(l + q(l))$ ⟵ polynomial of l
In total, $\{p(l+q(l)) + cq(l)\}2^{q(l)} + d = O(2^{\,l+q(l)})$
Hence, $L \in \mathcal{EXP}$ → $\mathcal{NP} \subseteq \mathcal{EXP}$

Q.E.D.

定理5.9.
(1) $\mathcal{NP} \subseteq$ co-$\mathcal{NP}$ → $\mathcal{NP}$ = co-$\mathcal{NP}$
(2) co-$\mathcal{NP} \subseteq \mathcal{NP}$ → $\mathcal{NP}$ = co-$\mathcal{NP}$
(3) $\mathcal{NP} \neq$ co-$\mathcal{NP}$ → $\mathcal{P} \neq \mathcal{NP}$.

補注: (3)より, $\mathcal{NP} \neq$co-$\mathcal{NP}$の証明は, $\mathcal{P} \neq \mathcal{NP}$の証明より難しい.

証明: (1) $\mathcal{NP} \subseteq$ co-$\mathcal{NP}$ → $\mathcal{NP}$ = co-$\mathcal{NP}$ ((2)の証明も同様)
任意の$L \in$ co-$\mathcal{NP}$に対して$L \in \mathcal{NP}$が示せれば,
co-$\mathcal{NP} \subseteq \mathcal{NP}$が証明できるので,
仮定の$\mathcal{NP} \subseteq$ co-$\mathcal{NP}$と合わせて$\mathcal{NP}$ = co-$\mathcal{NP}$が言える.

$L \in$ co-$\mathcal{NP}$ → $\overline{L} \in \mathcal{NP}$ (定義5.3より)
→ $\overline{L} \in$ co-$\mathcal{NP}$ ($\mathcal{NP} \subseteq$ co-$\mathcal{NP}$より)
→ $L \in \mathcal{NP}$ (定義5.3と$\overline{\overline{L}}=L$より)

Theorem 5.9
(1) $\mathcal{NP} \subseteq$ co-$\mathcal{NP}$ → $\mathcal{NP}$ = co-$\mathcal{NP}$
(2) co-$\mathcal{NP} \subseteq \mathcal{NP}$ → $\mathcal{NP}$ = co-$\mathcal{NP}$
(3) $\mathcal{NP} \neq$ co-$\mathcal{NP}$ → $\mathcal{P} \neq \mathcal{NP}$.

Note: from (3) the proof for $\mathcal{NP} \neq$ co-$\mathcal{NP}$ is harder than that for $\mathcal{P} \neq \mathcal{NP}$.

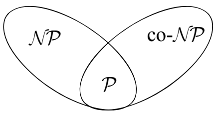
Proof: (1) $\mathcal{NP} \subseteq$ co-$\mathcal{NP}$ → $\mathcal{NP}$ = co-$\mathcal{NP}$ (proof of (2) is similar)
Since co-$\mathcal{NP} \subseteq \mathcal{NP}$ is shown if we prove $L \in \mathcal{NP}$ for any $L \in$ co-$\mathcal{NP}$
Combining it with the assumption $\mathcal{NP} \subseteq$ co-$\mathcal{NP}$, we have
$\mathcal{NP}$ = co-$\mathcal{NP}$ and so
$L \in$ co-$\mathcal{NP}$ → $\overline{L} \in \mathcal{NP}$ (by Definition 5.3)
→ $\overline{L} \in$ co-$\mathcal{NP}$ ($\mathcal{NP} \subseteq$ co-$\mathcal{NP}$)
→ $L \in \mathcal{NP}$ (Definition 5.3 and $\overline{\overline{L}}=L$)

(3) $\mathcal{NP} \neq$ co-$\mathcal{NP}$ → $\mathcal{P} \neq \mathcal{NP}$.

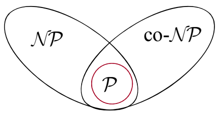
対偶: $\mathcal{P} = \mathcal{NP}$ → $\mathcal{NP}$ = co-$\mathcal{NP}$

$\mathcal{P}$=$\mathcal{NP}$と仮定すると, すべてのLに対し
$L \in \mathcal{NP}$ ↔ $L \in \mathcal{P}$ ($\mathcal{P} = \mathcal{NP}$より)
↔ $\overline{L} \in \mathcal{P}$ (演習問題5.5)
↔ $\overline{L} \in \mathcal{NP}$ ($\mathcal{P} = \mathcal{NP}$より)
↔ L (= $\overline{\overline{L}}$) $\in$ co-$\mathcal{NP}$ (定義5.3より)
∴ $\mathcal{NP}$ = co-$\mathcal{NP}$ 証明終

$\mathcal{NP} \neq$co-$\mathcal{NP}$が正しいと



or

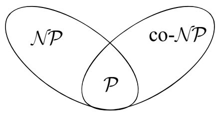


(3) $\mathcal{NP} \neq$ co-$\mathcal{NP}$ → $\mathcal{P} \neq \mathcal{NP}$.

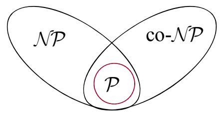
Contraposition: $\mathcal{P} = \mathcal{NP}$ → $\mathcal{NP}$ = co-$\mathcal{NP}$

If we assume $\mathcal{P}$=$\mathcal{NP}$, for any L we have
$L \in \mathcal{NP}$ ↔ $L \in \mathcal{P}$ ($\mathcal{P} = \mathcal{NP}$)
↔ $\overline{L} \in \mathcal{P}$ (Exercise 5.5)
↔ $\overline{L} \in \mathcal{NP}$ ($\mathcal{P} = \mathcal{NP}$)
↔ L (= $\overline{\overline{L}}$) $\in$ co-$\mathcal{NP}$ (Definition 5.3)
∴ $\mathcal{NP}$ = co-$\mathcal{NP}$ Q.E.D.

If $\mathcal{NP} \neq$co-$\mathcal{NP}$ is true,



or



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→B: 多項式時間還元(polynomial-time reduction)
⇔
(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: $A \leq_m^P B$

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→B: polynomial-time reduction
⇔
(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 $A \leq_m^P B$

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

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) $B \in \mathcal{EXP} \rightarrow A \in \mathcal{EXP}$.

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: 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　$L \leq_m^P$ 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

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) $B \in \mathcal{EXP} \rightarrow A \in \mathcal{EXP}$.

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 ONE$\equiv$ {1}, for each set L in $\mathcal{P}$ we have
$L \leq_m^P$ 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 $L \in \mathcal{P} \rightarrow x \in L$)

定理6.2: A, B, C: 任意の集合
(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
(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.

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)

2SAT $\leq_m^P$ 3SAT

- 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…考えてみよう！

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．

Relation among satisfiability problems of propositional expressions

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

2SAT $\leq_m^P$ 3SAT

- at most k…trivial
- exactly k…
  - ➢easy if you can repeat the same literal.
  - ➢the other case … good exercise!

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

5/14

例6.3: ExSATから3SATへの還元

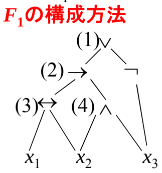
$$E_1(x_1,x_2,x_3) \equiv [[x_1 \leftrightarrow x_2] \to [x_2 \wedge x_3]] \vee \neg x_3$$

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

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 ∧で結ぶ

5/14

Ex. 6.3: Reduction from ExSAT to 3SAT

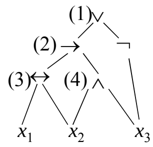
$$E_1(x_1,x_2,x_3) \equiv [[x_1 \leftrightarrow x_2] \to [x_2 \wedge x_3]] \vee \neg x_3$$

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

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 ∧

6/14

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．

$$\begin{aligned} U_1 \leftrightarrow [U_2 \vee \neg x_3] &= [\neg U_1 \vee U_2 \vee \neg x_3] \wedge [U_1 \vee \neg[U_2 \vee \neg x_2]] \\ &= [\neg U_1 \vee U_2 \vee \neg x_3] \wedge [U_1 \vee [\neg U_2 \wedge x_2]] \\ &= [\neg U_1 \vee U_2 \vee \neg x_3] \wedge [U_1 \vee \neg U_2] \wedge [U_1 \vee x_2] \\ &= [\neg U_1 \vee U_2 \vee \neg x_3] \wedge [U_1 \vee \neg U_2 \vee \neg U_2] \wedge [U_1 \vee x_2 \vee x_2] \end{aligned}$$

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．

6/14

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

$$\begin{aligned} U_1 \leftrightarrow [U_2 \vee \neg x_3] &= [\neg U_1 \vee U_2 \vee \neg x_3] \wedge [U_1 \vee \neg[U_2 \vee \neg x_2]] \\ &= [\neg U_1 \vee U_2 \vee \neg x_3] \wedge [U_1 \vee [\neg U_2 \wedge x_2]] \\ &= [\neg U_1 \vee U_2 \vee \neg x_3] \wedge [U_1 \vee \neg U_2] \wedge [U_1 \vee x_2] \\ &= [\neg U_1 \vee U_2 \vee \neg x_3] \wedge [U_1 \vee \neg U_2 \vee \neg U_2] \wedge [U_1 \vee x_2 \vee x_2] \end{aligned}$$

Others are similar.
Thus, every 3SAT form is converted.

7/14

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($\leq^P_m$の下で)$\mathcal{C}$-完全という．
(a) $\forall L \in \mathcal{C}\ [L \leq^P_m A]$
(b) $A \in \mathcal{C}$
補注：条件(a)を満たす集合は$\mathcal{C}$-困難．

7/14

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 $\leq^P_m$)
(a) $\forall L \in \mathcal{C}\ [L \leq^P_m A]$
(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: $\textit{eval-in-time}(a, x, \bar{2}^{t}) = \textit{accept}$?

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: $\textit{eval-in-time}(a, x, \bar{2}^{t}) = \textit{accept}$?

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

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

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

例6.6. 定理6.3の意味(クラス$\mathcal{NP}$)

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

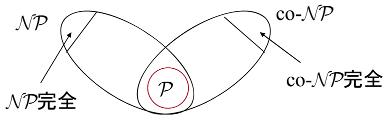
Aを$\mathcal{NP}$-完全集合とする.
定理6.3(1)の対偶より,
$\mathcal{NP} \neq \mathcal{P} \rightarrow A \notin \mathcal{P}$
定理6.3(3)の対偶と定理5.9(1)の対偶より,
$A \notin$ co-$\mathcal{NP}$
つまり, $\mathcal{NP}$-完全集合は$\mathcal{P} \neq \mathcal{NP}$である限り,
多項式時間では認識できない.

Theorem 6.3. For any $\mathcal{C}$-hard (or $\mathcal{C}$-complete) set A,
(1) $A \in \mathcal{P} \rightarrow \mathcal{C} \subseteq \mathcal{P}$ CP: $\mathcal{C} \not\subset \mathcal{P} \rightarrow A \notin \mathcal{P}$
(2) $A \in \mathcal{NP} \rightarrow \mathcal{C} \subseteq \mathcal{NP}$ CP: $\mathcal{C} \not\subset \mathcal{NP} \rightarrow A \notin \mathcal{NP}$
(3) $A \in$ co-$\mathcal{NP} \rightarrow \mathcal{C} \subseteq$ co-$\mathcal{NP}$ CP: $\mathcal{C} \not\subset$ co-$\mathcal{NP} \rightarrow A \notin$ co-$\mathcal{NP}$
(4) $A \in \mathcal{EXP} \rightarrow \mathcal{C} \subseteq \mathcal{EXP}$ CP: $\mathcal{C} \not\subset \mathcal{EXP} \rightarrow A \notin \mathcal{EXP}$

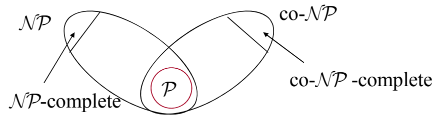
Theorem 5.9.
(1) $\mathcal{NP} \subseteq$ co-$\mathcal{NP} \rightarrow \mathcal{NP} =$ co-$\mathcal{NP}$

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
$\mathcal{NP} \neq \mathcal{P} \rightarrow A \notin \mathcal{P}$
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（$\mathcal{C}\not\subset\mathcal{P}\rightarrow A\notin\mathcal{P}$，ここでは$\mathcal{EXP}\not\subset\mathcal{P}\rightarrow D\notin\mathcal{P}$)
$\mathcal{P}\neq\mathcal{EXP}\rightarrow\mathcal{EXP}\not\subset\mathcal{P}$ $(\because\mathcal{P}\subseteq\mathcal{EXP})\rightarrow D\notin\mathcal{P}$
定理6.3(2)の対偶（$\mathcal{C}\not\subset\mathcal{NP}\rightarrow A\notin\mathcal{NP}$,
ここでは$\mathcal{EXP}\not\subset\mathcal{NP}\rightarrow D\notin\mathcal{NP}$)
$\mathcal{NP}\neq\mathcal{EXP}\rightarrow\mathcal{EXP}\not\subset\mathcal{NP}$ $(\because\mathcal{NP}\subseteq\mathcal{EXP})\rightarrow D\notin\mathcal{NP}$
定理6.3(3)の対偶（$\mathcal{C}\not\subset$co-$\mathcal{NP}\rightarrow A\notin$co-$\mathcal{NP}$,
ここでは$\mathcal{EXP}\not\subset$co-$\mathcal{NP}\rightarrow D\notin$co-$\mathcal{NP}$)
co-$\mathcal{NP}\neq\mathcal{EXP}\rightarrow\mathcal{EXP}\not\subset$co-$\mathcal{NP}\rightarrow D\notin$ 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)
（$\mathcal{C}\not\subset\mathcal{P}\rightarrow A\notin\mathcal{P}$，where $\mathcal{EXP}\not\subset\mathcal{P}\rightarrow D\notin\mathcal{P}$)
$\mathcal{P}\neq\mathcal{EXP}\rightarrow\mathcal{EXP}\not\subset\mathcal{P}$ $(\because\mathcal{P}\subseteq\mathcal{EXP})\rightarrow D\notin\mathcal{P}$
Contraposition of Theorem 6.3(2)（$\mathcal{C}\not\subset\mathcal{NP}\rightarrow A\notin\mathcal{NP}$,
Here，$\mathcal{EXP}\not\subset\mathcal{NP}\rightarrow D\notin\mathcal{NP}$)
$\mathcal{NP}\neq\mathcal{EXP}\rightarrow\mathcal{EXP}\not\subset\mathcal{NP}$ $(\because\mathcal{NP}\subseteq\mathcal{EXP})\rightarrow D\notin\mathcal{NP}$
Contraposition of Theorem 6.3(3)（$\mathcal{C}\notin$ co-$\mathcal{NP}\rightarrow A\not\subset$co-$\mathcal{NP}$,
here，$\mathcal{EXP}\not\subset$co-$\mathcal{NP}\rightarrow D\notin$ co-$\mathcal{NP}$)
co-$\mathcal{NP}\neq\mathcal{EXP}\rightarrow\mathcal{EXP}\not\subset$ co-$\mathcal{NP}\rightarrow D\notin$ 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) $A\leq_m^P B\rightarrow B$は$\mathcal{C}$-困難.
(2) $A\leq_m^P B\wedge B\in\mathcal{C}\rightarrow B$は$\mathcal{C}$-完全.

証明:
定義6.2より，$\forall L\in\mathcal{C}[L\leq_m^P A]$
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，$\forall L\in\mathcal{C}[L\leq_m^P B]$

すなわち，Bは$\mathcal{C}$-困難.

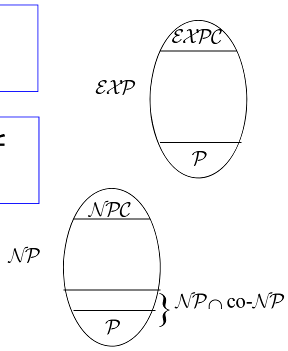
Theorem 6.4. A: any $\mathcal{C}$-complete set
For any set B we have
(1) $A\leq_m^P B\rightarrow B$ is $\mathcal{C}$-hard.
(2) $A\leq_m^P B\wedge B\in\mathcal{C}\rightarrow B$ is $\mathcal{C}$-complete.

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

$\mathcal{EXPC}$ ≡{L: Lは$\mathcal{EXP}$-完全}
$\mathcal{NPC}$ ≡{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) $\mathcal{EXP} - (\mathcal{EXPC} \cup \mathcal{P}) \neq \phi$

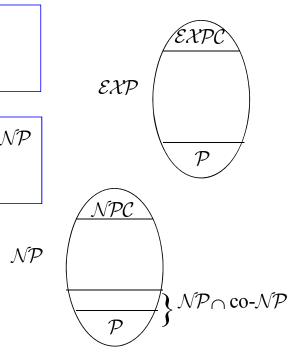
定理6.6: $\mathcal{P} \neq \mathcal{NP}$**を仮定すると**
(1) $\mathcal{NPC} \cap \mathcal{P} = \phi$
(2) $\mathcal{NP} - (\mathcal{NPC} \cup \mathcal{P}) \neq \phi$



$\mathcal{EXPC}$ ≡{L: L is $\mathcal{EXP}$-complete}
$\mathcal{NPC}$ ≡{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) $\mathcal{NP} - (\mathcal{NPC} \cup \mathcal{P}) \neq \phi$



残りの予定(Schedule)

- 4/23(Thu) Office Hour:
  - レポート(1)の解答と解説(Comments on report(1))
- 4/27(Mon): 最後の講義(Last class)
- 4/30(Thu): Office Hour:
  - レポート(2)の解答と解説(Comments on report(2))
  - 試験に対する希望調査（持ち込み/範囲）
  - その他
- 5/7(Thu): 中間試験(Mid term exam)
  - 4題40点満点