5.2. クラス$\mathcal{NP}$

定義5.2: 集合 L に対して次の条件を満たす多項式 q と多項式時間計算可能述語 R が存在したとする.

$$各x \in \Sigma^* でx \in L \leftrightarrow \exists w \in \Sigma^* :|w| \leq q(|x|)[R(x,w)] \quad (5.1)$$

つまり, $L = \{x : \exists w \in \Sigma^* [|w| \leq q(|x|) \wedge R(x,w)]\}$

このとき, Lを$\mathcal{NP}$集合といい, Lの認識問題を$\mathcal{NP}$問題という.
また, $\mathcal{NP}$集合の全体をクラス$\mathcal{NP}$という.

補注:各 $x \in \Sigma^*$に対して, 論理式 $|w| \leq q(|x|) \wedge R(x,w)$ を満たす $w_x \in \Sigma^*$をxの(多項式長の)証拠という.
以下では, $\exists w \in \Sigma^* : |w| \leq q(|x|) \quad \Rightarrow \quad \exists_q w$ と略記.

「入力サイズの多項式長の証拠が与えられたとき, これが問題の条件を満たすかどうかを多項式時間で判定できる. 」

補足:$\mathcal{NP}$=**N**ondeterministic **P**olynomial

5.2. Class $\mathcal{NP}$

Def. 5.2: Suppose that we have a polynomial q and polynomial time computable predicate R for a set L such that

$$\text{for each } x \in \Sigma^*, x \in L \leftrightarrow \exists w \in \Sigma^* :|w| \leq q(|x|)[R(x,w)]$$

i.e., $L = \{x : \exists w \in \Sigma^* [|w| \leq q(|x|) \wedge R(x,w)]\}$ (5.1)

Then, L is called an $\mathcal{NP}$ set, and the problem of recognizing L is called an $\mathcal{NP}$ problem.
Also, the whole set of $\mathcal{NP}$ sets is called the class $\mathcal{NP}$.

Note: For each $x \in \Sigma^*$, $w_x \in \Sigma^*$ satisfying the predicate $|w| \leq q(|x|) \wedge R(x,w)$ is called (polynomial) witness of x.
Hereafter, we use notation $\exists w \in \Sigma^* : |w| \leq q(|x|) \quad \Rightarrow \quad \exists_q w$

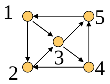
"Given a witness of polynomial length in the input size, we can determine in polynomial time whether it satisfies the condition of a given problem."

c.f.:$\mathcal{NP}$=**N**ondeterministic **P**olynomial

例5.7: ハミルトン閉路問題 (DHAM) $\in \mathcal{NP}$

グラフの頂点は1～nと番号づけされていると仮定.
ハミルトン閉路の辿り方➔ 1～n の順列$< l_1, l_2, \ldots, l_n >$
この順列が多項式長の証拠

例:



証拠の候補 (注)全部で $n!$～n^n 通りある
<1,2,3,4,5> ➔ハミルトン閉路 ➔証拠
<1,2,3,5,4> ➔ハミルトン閉路でない
<1,4,3,2,5> ➔ハミルトン閉路でない

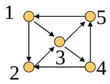
$R_D(x, w)$ ↔[xはあるグラフG(n頂点)のコード]
∧[wは1～nの順列$< l_1, l_2, \ldots, l_n >$]
∧[wはGのハミルトン閉路を表している]

すべての $x \in \Sigma^*$について次の関係が成り立つ.
xがあるグラフGのコードになっているとき:
$x \in \mathrm{DHAM} \leftrightarrow \exists w_G (=< l_1, \ldots, l_n >)[R_D(x, w_G)]$
xがグラフのコードになっていないとき: $\forall w[\neg R_D(x,w)]$

Ex.5.7: Hamilton Cycle Problem (DHAM) $\in \mathcal{NP}$

Assume graph vertices are numbered 1～n.
Trace on a Hamilton cycle➔ permutation of 1～n $< l_1, l_2, \ldots, l_n >$
This permutation is a witness of polynomial length.

Ex.:



candidates of witness (*c.f.*)There are $n!$～n^n many
<1,2,3,4,5> ➔Hamilton cycle ➔witness
<1,2,3,5,4> ➔not Hamilton cycle
<1,4,3,2,5> ➔not Hamilton cycle

$R_D(x, w)$ ↔[x is a code of a graph G(with n vertices)]
∧[w is a permutation of 1～n: $< l_1, l_2, \ldots, l_n >$]
∧[w represents a Hamilton cycle in G]

For each $x \in \Sigma^*$ we have
if x is a code of a graph G:
$x \in \mathrm{DHAM} \leftrightarrow \exists w_G (=< l_1, \ldots, l_n >)[R_D(x, w_G)]$
if x is not a code of any graph: $\forall w[\neg R_D(x,w)]$

例5.8: 命題論理式充足性問題(3SAT, SAT, ExSATなど)
目標:ExSAT $\in \mathcal{NP}$

$F(x_1, \ldots, x_n)$: 任意の拡張命題論理式
Fが充足可能 ↔ $\exists a_1, \ldots, a_n$: 各a_iは1か0 $[F(a_1, \ldots, a_n) = 1]$

証拠の長さq_E
Fへの真偽値の割り当てを$< a_1, \ldots, a_n >$で表す.
→ 長さは $3(n+n+1)=6n+3 \leq 6|\lceil F \rceil| + 3$
$q_E(l) = 6l+3$

述語R_E
$R_E(x, w)$ ↔ [xはある拡張命題論理式F (n変数)のコード]
∧[wはFへの割り当て$< a_1, a_2, \ldots, a_n >$]
∧$[F(a_1, \ldots, a_n) = 1]$

計算木を用いると$F(a_1, \ldots, a_n)$ の値は多項式時間で計算可能.
よって, R_Eも多項式時間で計算可能.

Ex.5.8: Satisfiability Problem of Prop. Express. (3SAT, SAT, ExSAT)
Goal:ExSAT $\in \mathcal{NP}$

$F(x_1, \ldots, x_n)$: arbitrary extended prop. logic. expression
F is satisfiable↔ $\exists a_1, \ldots, a_n$: each a_i is 0 or 1 $[F(a_1, \ldots, a_n) = 1]$

length of a witness q_E
Truth assignment to F is denoted by $< a_1, \ldots, a_n >$.
→ its length is $3(n+n+1)=6n+3 \leq 6|\lceil F \rceil| + 3$
$q_E(l) = 6l+3$

predicate R_E
$R_E(x, w)$ ↔[x is a code of an extended prop. express. F (n variables)]
∧ [w is an assignment to F : $< a_1, a_2, \ldots, a_n >$]
∧ $[F(a_1, \ldots, a_n) = 1]$

Using a computation tree, the value of $F(a_1, \ldots, a_n)$ is computed in polynomial time. Thus, R_E is also computable in polynomial time.

$\mathcal{NP}$集合であることの意味は何か?

(5.1)を満たすq, Rを用いると, $x \in L$? を次のように判定できる.

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

長さが$q(|x|)$以下の文字列をすべて列挙して調べれば, acceptかrejectか判定できる. ただ, そのような文字列は2の$q(|x|)$乗個(指数関数)存在することに注意.

上記の計算方式で認識できる集合を$\mathcal{NP}$集合と考えてよい.

What does it mean by being an $\mathcal{NP}$ set?

Using q and R satisfying the predicate characterizing an $\mathcal{NP}$ set, we can determine $x \in L$? in the following way.

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

If we enumerate and check all possible strings of length at most $q(|x|)$, then we can accept or reject them. Here note that there are 2 to the $q(|x|)$ (exponentially many) such strings.

We may think that those sets recognizable as above are $\mathcal{NP}$ sets.

$\mathcal{NP}$に関連したクラス

定義5.3. 集合Lは, その補集合$\overline{L}$が$\mathcal{NP}$に属しているとき, **co-$\mathcal{NP}$集合**という. また, co-$\mathcal{NP}$集合の全体を**クラスco-$\mathcal{NP}$**という.

補注: co-$\mathcal{P}$ を定義しても $\mathcal{P}$ と同じなので無意味.

定理5.5. すべての集合 L に対し, 次の条件は同値.
(a) $L \in$ co-$\mathcal{NP}$
(b) 集合 L を, 適当な多項式 q と多項式時間計算可能述語Qを用いて,
$$L = \{x : \forall w \in \Sigma^* : |w| \le q(|x|)[Q(x, w)]\}$$
と表せる.

Classes related to $\mathcal{NP}$

Def.5.3. A set L is called a **co-$\mathcal{NP}$** set if its complement $\overline{L}$ belongs to $\mathcal{NP}$. The whole family of co-$\mathcal{NP}$ sets is called the class **co-$\mathcal{NP}$**.

Note: It is nonsense to define co-$\mathcal{P}$ since it is equal to $\mathcal{P}$.

Theorem 5.5. For every set L, the following conditions are equivalent.
(a) $L \in$ co-$\mathcal{NP}$
(b) The set L can be represented as
$$L = \{x : \forall w \in \Sigma^* : |w| \le q(|x|)[Q(x, w)]\}$$
by using some polynomial q and polynomial-time computable predicate Q.

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.

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$< a_1, a_2, \dots, a_n, b >$
質問：$\sum_{i\in S} a_i = b$ となる添字の集合 $S \subseteq \{1, \dots, n\}$があるか？

・**箱詰め問題**(BIN)
入力：自然数の組$< a_1, a_2, \dots, a_n, b, k >$
質問：添字の集合$U=\{1, \dots, n\}$を$U_1, \dots, U_k$のk個に分割し，
各jで $\sum_{i\in U_j} a_i \le b$ 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 $< a_1, a_2, \dots, a_n, b >$
question：Is there a set of indices $S \subseteq \{1, \dots, n\}$ s.t. $\sum_{i\in S} a_i = b$?

・**Bin Packing Problem**(BIN)
input：n+2 tuple of natural numbers $< a_1, a_2, \dots, a_n, b, k >$
question：Is there a partition of a set of indices $U=\{1, \dots, n\}$ into $U_1, \dots, U_k$ such that $\sum_{i\in U_j} a_i \le b$ 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、
$\forall c > 0, \overset{\infty}{\forall} n[c t_1(n)^2 \le t_2(n)]$
$\to \mathrm{TIME}(t_1) \subsetneq \mathrm{TIME}(t_2)$

証明:
(1) $\mathcal{P} \subsetneq \mathcal{E}$.
$t_1(n)=2^n$, $t_2(n)=2^{3n}$とすると，<u>階層定理</u>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 ,
$\forall c > 0, \overset{\infty}{\forall} n[c t_1(n)^2 \le t_2(n)]$
$\to \mathrm{TIME}(t_1) \subsetneq \mathrm{TIME}(t_2)$

Proof:
(1) $\mathcal{P} \subsetneq \mathcal{E}$.
For $t_1(n)=2^n$, $t_2(n)=2^{3n}$, from the <u>hierarchy theorem</u> 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-$\mathcal{NP}$ (よって，$\mathcal{P} \subseteq \mathcal{NP} \cap$ co-$\mathcal{NP}$)
(2) $\mathcal{NP} \subseteq \mathcal{EXP}$, co-$\mathcal{NP} \subseteq \mathcal{EXP}$ (よって，$\mathcal{NP} \cup$ 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-$\mathcal{NP}$ (thus, $\mathcal{P} \subseteq \mathcal{NP} \cap$ co-$\mathcal{NP}$)
(2)$\mathcal{NP} \subseteq \mathcal{EXP}$, co-$\mathcal{NP} \subseteq \mathcal{EXP}$ (thus, $\mathcal{NP} \cup$ 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., $\mathcal{P} \subseteq \mathcal{NP}$.

(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

(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

$L = \{x : \exists_q w[R(x,w)]\} = \{x : \exists_q w[|w| \le q(|x|) \wedge R(x,w)]\}$

program recognizing L using q and R

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

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

$L \in \mathcal{NP}$ ↔ $\overline{L} \in \mathcal{P}$ ($\mathcal{P} = \mathcal{NP}$ より)

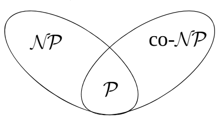
↔ $\overline{L} \in \mathcal{P}$ (演習問題5.5)

↔ $\overline{L} \in \mathcal{NP}$ ($\mathcal{P} = \mathcal{NP}$ より)

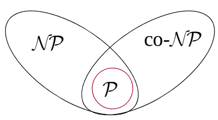
↔ $L\ (= \overline{\overline{L}}) \in$ co-$\mathcal{NP}$ (定義5.3より)

∴ $\mathcal{NP}$ = 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

$L \in \mathcal{NP}$ ↔ $\overline{L} \in \mathcal{P}$ ($\mathcal{P} = \mathcal{NP}$)

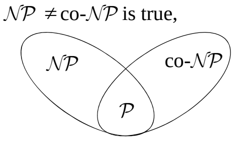
↔ $\overline{L} \in \mathcal{P}$ (Exercise 5.5)

↔ $\overline{L} \in \mathcal{NP}$ ($\mathcal{P} = \mathcal{NP}$)

↔ $L\ (= \overline{\overline{L}}) \in$ co-$\mathcal{NP}$ (Definition 5.3)

∴ $\mathcal{NP}$ = co-$\mathcal{NP}$ Q.E.D.

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



or