5.2. クラス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.

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

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

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

補注 : 各 $x \in \Sigma^*$に対して, 論理式 $|w| \le q(|x|) \wedge R(x,w)$
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, $\exists w \in \Sigma^* : |w| \le q(|x|) \quad \Rightarrow \quad \exists_q w$ 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 : NP=Nondeterministic Polynomial

5.2. Class NP

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

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 NP set, and the problem of recognizing L is called an NP problem.
Also, the whole set of NP sets is called the class 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 $\exists w \in \Sigma^* : |w| \leq q(|x|) \quad \Rightarrow \quad \exists_q w$

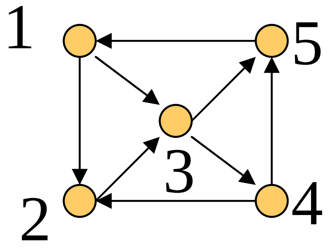
"Given a witness of polynomial length in the input size, we can determine in polynomial time whether it satisfies the condition of a given problem."

c.f.: NP=Nondeterministic Polynomial

例5.7: ハミルトン閉路問題 (DHAM) $\in$ 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

(注)全部で $n!$〜n^n 通りある

例:


証拠の候補
<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

$R_D(x, w)$ $\leftrightarrow$[xはあるグラフG(n頂点)のコード]
$\wedge$ [wは1〜nの順列$< l_1, l_2, \ldots, l_n >$]
$\wedge$[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) ∈ NP

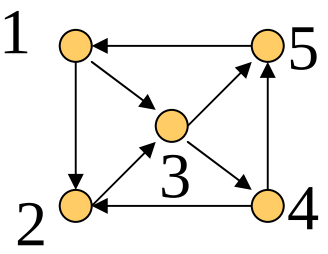
Assume graph vertices are numbered 1～*n*.

Trace on a Hamilton cycle➔ permutation of 1～*n* $< l_1, l_2, \ldots, l_n >$

This permutation is a witness of polynomial length.

(c.f.)There are $n! \sim n^n$ many candidates of witness

Ex.:



<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*:

$$x \in \text{DHAM} \leftrightarrow \exists w_G (=< l_1, \ldots, l_n >)[R_D(x, w_G)]$$

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 ∈ NP

$F(x_1, \ldots, x_n)$: 任意の拡張命題論理式

Fが充足可能 ↔ ∃$a_1, \ldots, a_n$: 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 ∈ 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

$R_E(x, w) \leftrightarrow$ [x is a code of an extended prop. express. F (n variables)]

$\wedge$ [w is an assignment to F : $< a_1, a_2, \ldots, a_n >$]

$\wedge$ $[F(a_1, \ldots, a_n) = 1]$

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.

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 $w \in \Sigma^{\leq q(|x|)}$ 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NP集合と考えてよい.

What does it mean by being an NP set?

Using q and R satisfying the predicate characterizing an 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 NP sets.

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NPに属しているとき，**co-NP集合**という．また，co-NP集合の全体を**クラスco-NP**という．

補注：co-P を定義しても 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) $L \in \text{co-NP}$

(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，

$$L = \{x : \forall w \in \Sigma^* : |w| \leq q(|x|)[Q(x, w)]\}$$

と表せる．

Classes related to NP

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

Note: It is nonsense to define co-P since it is equal to P.

Theorem 5.5. For every set L, the following conditions are equivalent.

(a) $L \in$ co-NP

(b) The set L can be represented as

$$L = \{x : \forall w \in \Sigma^* : |w| \leq q(|x|)[Q(x, w)]\}$$

by using some polynomial q and polynomial-time computable predicate Q.

例5.9: 素数判定問題

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

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，　$x \notin \mathrm{PRIME} \leftrightarrow \exists q_p w[R_p(x, w)]$

これは，$x \notin \mathrm{PRIME}$に対する証拠

よって，$\overline{\mathrm{PRIME}} \in$ NP，i.e., PRIME $\in$ co-NP

実際，$Q(x, w) \leftrightarrow \neg R_p(x, w)$ とすると

$$\mathrm{PRIME} = \{x{:} \forall q_p w\ [Q_p(x, w)]\}$$

と表せる.

PRIME $\in$ NPも示せるが，その証明はもっと複雑.

Ex.5.9: Primality testing

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

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

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

(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 $x \notin \mathrm{PRIME} \leftrightarrow \exists q_p w [R_p(x, w)]$

This is a witness to $x \notin$ PRIME

Thus, $\overline{\mathrm{PRIME}} \in$ NP, i.e., PRIME $\in$ co-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 $\in$ NP, but its proof is more complex.

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 $\sum_{i \in U_j} a_i \le b$ 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

Examples of 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).

5.3. 計算量クラス間の関係

定理5.6: P $\subseteq$ E $\subseteq$ EXP.

定義より，明らか．

定理5.7: P $\subsetneq$ E $\subsetneq$ EXP.

証明:

(1) P $\subsetneq$ 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，P $\subseteq$ $\mathrm{TIME}(2^n) \subsetneq \mathrm{TIME}(2^{3n})$ $\subseteq$ E だから，

$$\mathrm{P} \subsetneq \mathrm{E}.$$

(2)も同様．

証明終

5.3. Relation in the Complexity Class

Theorem 5.6: P $\subseteq$ E $\subseteq$ EXP.

Obvious from the definition.

Theorem 5.7: P $\subsetneq$ E $\subsetneq$ EXP.

Proof:

(1) P $\subsetneq$ 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 P $\subseteq \mathrm{TIME}(2^n) \subsetneq \mathrm{TIME}(2^{3n}) \subseteq$ E

P $\subsetneq$ E.

(2) is similar.

Q.E.D.

定理5.8.
(1) P ⊆ NP, P ⊆ co−NP (よって, P ⊆ NP ∩ co−NP)
(2) NP ⊆ EXP, co−NP ⊆ EXP (よって, NP ∪ co−NP ⊆ EXP)

証明: (1) P ⊆ NP（P ⊆ co−NP も同様）
L: 任意の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.

$$\forall x \in \Sigma^*: [x \in L \leftrightarrow P(x)] \quad \text{or} \quad P = \{x: P(x)\}$$

$R(x, w) = P(x)$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, NPの定義より, $L \in$ NP i.e., P ⊆ NP.

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

Proof:

(1) $P \subseteq NP$ ($P \subseteq co\text{-}NP$ is similar)

L: arbitrary P set

➔ L is recognizable in polynomial time

Thus, we have the following description using a polynomial-time computable predicate P.

$$\forall x \in \Sigma^* : [x \in L \leftrightarrow P(x)] \text{ or } P = \{x: P(x)\}$$

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 NP, $L \in NP$ i.e., $P \subseteq NP$.

(2) NP ⊆ EXP (co-NP ⊆ EXP)

L: 任意の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，$L \in$ EXP → NP ⊆ EXP 証明終

(2) NP $\subseteq$ EXP (co-NP $\subseteq$ EXP)

L: any 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 $R = p(|x| + |w|) \le p(l + q(l)) \longleftarrow$ polynomial of l

In total, $\{p(l+q(l)) + cq(l)\}2^{q(l)} + d = O(2^{\,l+q(l)})$

Hence, $L \in$ EXP → NP $\subseteq$ EXP Q.E.D.

定理5.9.

(1) NP ⊆ co-NP → NP = co-NP
(2) co-NP ⊆ NP → NP = co-NP
(3) NP ≠ co-NP → P ≠ NP.

補注: (3)より，NP ≠ co-NPの証明は，P≠NPの証明より難しい．

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

L ∈ co-NP → $\overline{L}$ ∈NP (定義5.3より）
→ $\overline{L}$ ∈ co-NP (NP ⊆ co-NPより）
→ L ∈NP (定義5.3と$\overline{\overline{L}}$=Lより）

Theorem 5.9

(1) NP $\subseteq$ co-NP $\rightarrow$ NP = co-NP
(2) co-NP $\subseteq$ NP $\rightarrow$ NP = co-NP
(3) NP $\neq$ co-NP $\rightarrow$ P $\neq$ NP.

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

Proof: (1) NP $\subseteq$ co-NP $\rightarrow$ NP = co-NP (proof of (2) is similar)
Since co-NP $\subseteq$ NP is shown if we prove $L \in$ NP for any $L \in$ co-NP
Combining it with the assumption NP $\subseteq$ co-NP, we have
NP = co-NP and so

$L \in$ co-NP $\rightarrow \overline{L} \in$ NP (by Definition 5.3)
$\rightarrow \overline{L} \in$ co-NP (NP $\subseteq$ co-NP)
$\rightarrow L \in$ NP (Definition 5.3 and $\overline{\overline{L}}=L$)

(3) NP $\neq$ co-NP → P $\neq$ NP.

対偶: P = NP → NP = co-NP

P＝NPと仮定すると, すべてのLに対し

$L \in$ NP $\leftrightarrow$ $L \in$ P （ P = NP より）

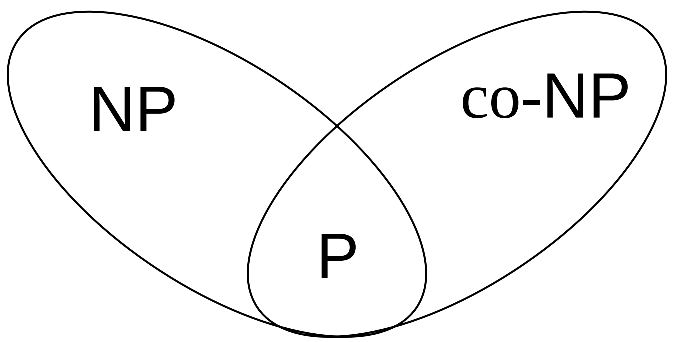
$\leftrightarrow \overline{L} \in$ P (演習問題5.5)

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

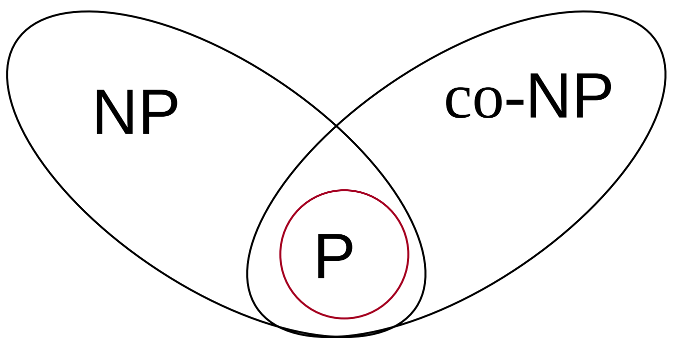
$\leftrightarrow L\ (= \overline{\overline{L}}) \in$ co- NP (定義5.3より)

$\therefore$ NP = co- NP 証明終

NP $\neq$co-NPが正しいと



or



(3) NP $\neq$ co-NP → P $\neq$ NP.

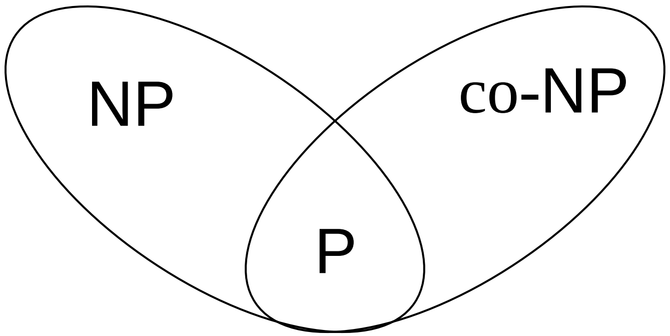
Contraposition: P = NP → NP = co-NP

If we assume P = NP, for any L we have

$$
\begin{aligned}
L \in \text{NP} &\leftrightarrow L \in \text{P} && (\text{P} = \text{NP}) \\
&\leftrightarrow \overline{L} \in \text{P} && (\text{Exercise 5.5}) \\
&\leftrightarrow \overline{L} \in \text{NP} && (\text{P} = \text{NP}) \\
&\leftrightarrow L \,(= \overline{\overline{L}}) \in \text{co-NP} && (\text{Definition 5.3})
\end{aligned}
$$

$\therefore$ NP = co-NP Q.E.D.

If NP $\neq$co-NP is true,



or