計算量クラス(前回の復習)

$$\mathsf{P} \equiv \bigcup_{p:\text{多項式}} \mathrm{TIME}(p(l))$$

$$\mathsf{E} \equiv \bigcup_{c>1} \mathrm{TIME}(2^{cl})$$

$$\mathsf{EXP} \equiv \bigcup_{p:\text{多項式}} \mathrm{TIME}(2^{p(l)})$$

(定義5.2) 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$x \in L \Leftrightarrow \exists w \in \Sigma^* : |w| \leqq q(|x|)[R(x,w)]$

略記: $\exists_q w \in \Sigma^* : [R(x,w)]$

(定理5.5) 集合Lがクラスco-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$x \in L \Leftrightarrow \forall w \in \Sigma^* : |w| \leqq q(|x|)[R(x,w)]$

略記: $\forall_q w \in \Sigma^* : [R(x,w)]$

Complexity Classes

$$\mathsf{P} \equiv \bigcup_{p:\text{polynomial}} \mathrm{TIME}(p(l))$$

$$\mathsf{E} \equiv \bigcup_{c>1} \mathrm{TIME}(2^{cl})$$

$$\mathsf{EXP} \equiv \bigcup_{p:\text{polynomial}} \mathrm{TIME}(2^{p(l)})$$

(Def 5.2) Set L is in the class NP$\Leftrightarrow$

There exists a poly q and a poly-time computable pred. R s.t.

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

Abbr. $\exists_q w \in \Sigma^* : [R(x,w)]$

(Theorem 5.5) Set L is in the class co-NP$\Leftrightarrow$

There exists a poly q and a poly-time computable pred. R s.t.

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

Abbr. $\forall_q w \in \Sigma^* : [R(x,w)]$

5.3. 計算量クラス間の関係

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

定義より，明らか.

定理5.7: $\mathrm{P} \subsetneqq \mathrm{E} \subsetneqq \mathrm{EXP}$.

証明:

(1) $\mathrm{P} \subsetneqq \mathrm{E}$.

$t_1(n)=2^n$, $t_2(n)=2^{3n}$とすると，階層定理より，

$$\mathrm{TIME}(2^n) \subsetneqq \mathrm{TIME}(2^{3n})$$

一方，$\mathrm{P} \subseteq \mathrm{TIME}(2^n) \subsetneqq \mathrm{TIME}(2^{3n}) \subseteq \mathrm{E}$ だから，

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

(2)も同様.

証明終

5.3. Relation in the Complexity Class

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

Obvious from the definition.

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

Proof:

(1) $\mathsf{P} \subsetneq \mathsf{E}$.

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

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

(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 ⊆ NP, P ⊆ co−NP (thus, P ⊆ NP ∩ co−NP)
(2)NP ⊆ EXP, co−NP ⊆ EXP (thus, NP ∪ co−NP ⊆ EXP)

Proof:

(1) P ⊆ NP （P ⊆ co−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.

$\forall x \in \Sigma^*:[x \in L \leftrightarrow P(x)]$ 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 ⊆ 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,

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

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$=p(|x| + |w|) \leq p(l + q(l))$ ⟵ 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

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

```
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 $R = p(|x| + |w|) \leq p(l + q(l))$ ← polynomial of l

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

Hence, $L \in$ 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$L \in$co-NPに対して$L \in$ 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.

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

Theorem 5.9.

(1) NP ⊆ co-NP → NP = co-NP

(2) co-NP ⊆ NP → NP = co-NP

(3) NP ≠ co-NP → P ≠ NP

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

Proof: (1) NP ⊆ co-NP → NP = co-NP (proof of (2) is similar)

Since co-NP ⊆ NP is shown if we prove $L \in$ NP for any $L \in$ co-NP

Combining it with the assumption NP ⊆ co-NP, we have NP = co-NP and so

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

$\rightarrow \overline{\overline{L}} \in$ co-NP (NP ⊆ co-NP)

$\rightarrow L \in$ NP (Definition 5.3 and $\overline{\overline{L}} = L$)

(3) NP ≠ co-NP → P ≠ 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)

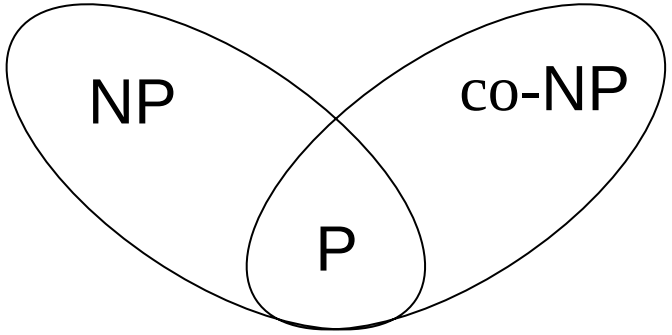
$\leftrightarrow \overline{L} \in$ NP (P = NP より)

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

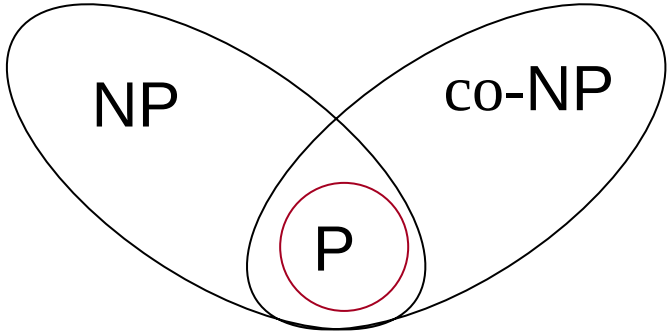
$\therefore$ NP = co- NP

証明終

NP ≠co-NPが正しいと



or



(3) NP ≠ co-NP → P ≠ NP.

Contraposition: P = NP → NP = co-NP

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

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

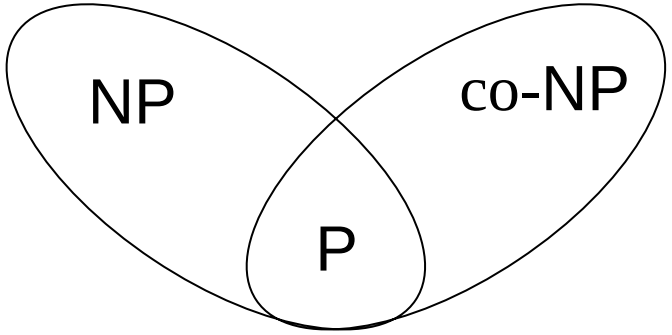
$\leftrightarrow \overline{L} \in$ P (Exercise 5.5)

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

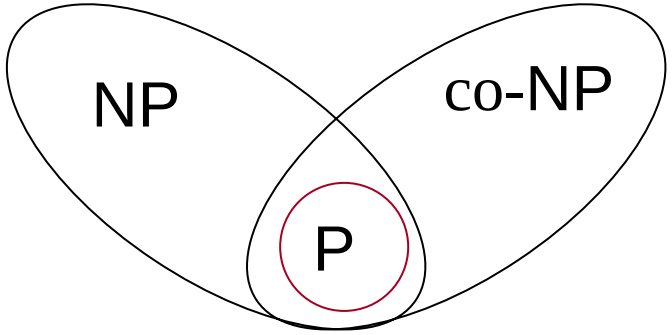
$\leftrightarrow L\ (= \overline{\overline{L}}) \in$ co- NP (Definition 5.3)

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

If NP ≠co-NP is true,



or



計算量クラス間の定義を概観すると…

クラスPの定義(5章)
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(定義5.2)
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co-NPの定義(定理5.5)
集合Lがクラスco-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 P (Chapter 5)
Set L is in the class P⇔
There exists a poly-time computable predicate R such that
for each $x \in \Sigma^*$, $x \in L \Leftrightarrow R(x)$

Def: Class NP (Def 5.2)
Set L is in the class 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-NP (Theorem 5.5)
Set L is in the class co-NP⇔
There exists a poly q and a poly-time computable pred. R s.t.
for each $x \in \Sigma^*$, $x \in L \Leftrightarrow \forall w \in \Sigma^* : |w| \leqq q(|x|)[R(x,w)]$

$\exists x_1 \exists x_2 \exists x_3 \, [R(x_1,x_2,x_3)] \Leftrightarrow \exists w(=<x_1,x_2,x_3>)[R'(w)]$

$\forall x_1 \forall x_2 \forall x_3 \, [R(x_1,x_2,x_3)] \Leftrightarrow \forall w(=<x_1,x_2,x_3>)[R'(w)]$

…たとえば $\exists x \forall y \exists w[R(x,y,w)]$ は??

クラス $\Sigma_k^p : L = \{x : \exists_q w_1 \forall_q w_2 \ldots \Phi_q w_k [R(x, w_1, \ldots, w_k)]$

クラス $\Pi_k^p : L = \{x : \forall_q w_1 \exists_q w_2 \ldots \Phi_q w_k [R(x, w_1, \ldots, w_k)]$

(比較的)すぐわかる関係:

$\Sigma_0^p = \Pi_0^p = \mathrm{P}$

$\Sigma_1^p = \mathrm{NP}$

$\Pi_1^p = \text{co-NP}$

$\Pi_k^p \subseteq \Pi_{k+1}^p \cap \Sigma_{k+1}^p$

$\Sigma_k^p \subseteq \Pi_{k+1}^p \cap \Sigma_{k+1}^p$

$\exists x_1 \exists x_2 \exists x_3 [R(x_1,x_2,x_3)] \Leftrightarrow \exists w(=<x_1,x_2,x_3>)[R'(w)]$

$\forall x_1 \forall x_2 \forall x_3 [R(x_1,x_2,x_3)] \Leftrightarrow \forall w(=<x_1,x_2,x_3>)[R'(w)]$

…How about, e.g., $\exists x \forall y \exists w[R(x,y,w)]$??

$$\text{Class } \Sigma_k^p : L = \{x : \exists w_1 \forall w_2 ... \Phi w_k [R(x, w_1, ..., w_k)]$$

$$\text{Class } \Pi_k^p : L = \{x : \forall w_1 \exists w_2 ... \Phi w_k [R(x, w_1, ..., w_k)]$$

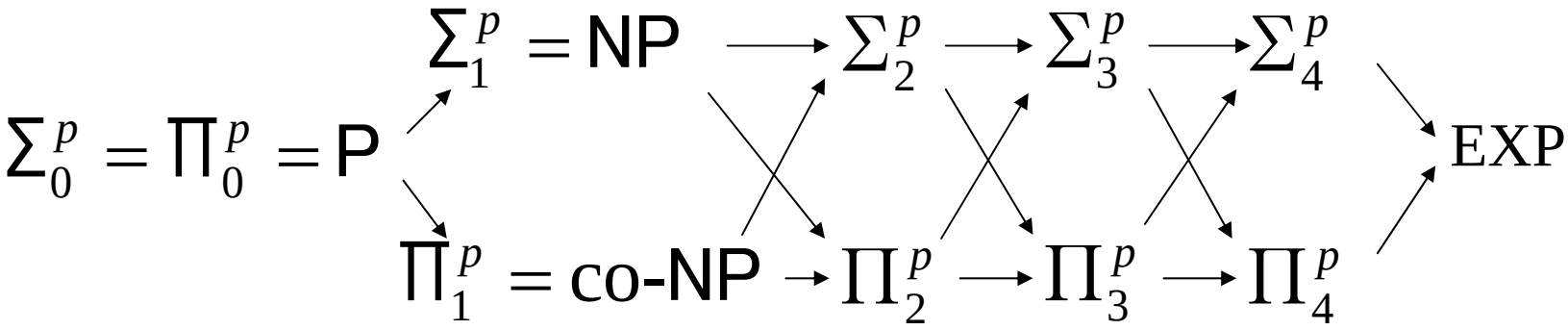
It is not difficult to see that…

$$\Sigma_0^p = \Pi_0^p = \mathsf{P} \qquad \Pi_k^p \subseteq \Pi_{k+1}^p \cap \Sigma_{k+1}^p$$

$$\Sigma_1^p = \mathsf{NP} \qquad \Sigma_k^p \subseteq \Pi_{k+1}^p \cap \Sigma_{k+1}^p$$

$$\Pi_1^p = \text{co-NP}$$

(比較的)すぐわかる関係:

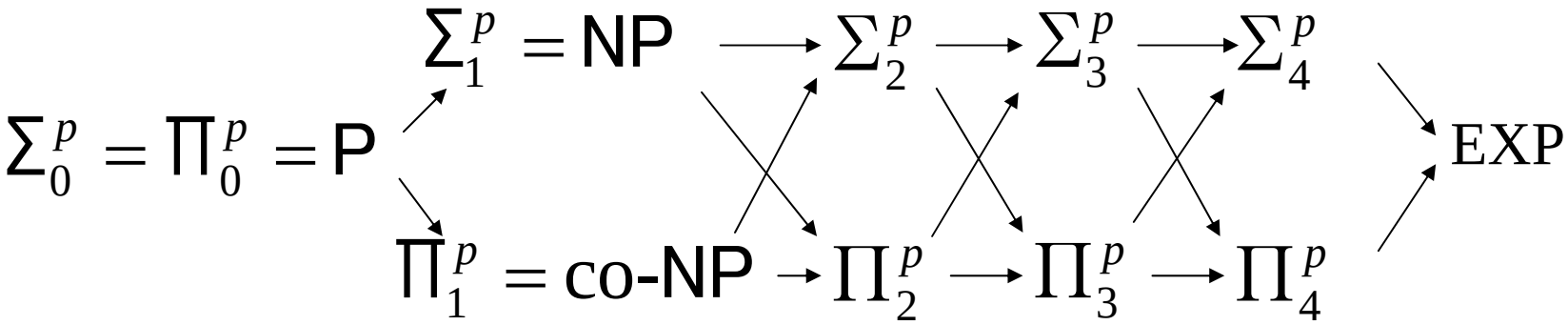


$$\mathrm{PH} \equiv \bigcup_k \Sigma_k^p = \bigcup_k \Pi_k^p$$

戸田の定理: $\mathrm{PH} \subseteq \mathrm{P}^{\mathrm{PP}}$

祝!!
ゲーデル賞

It is not difficult to see that…



$$\mathsf{PH} \equiv \bigcup_k \Sigma_k^p = \bigcup_k \Pi_k^p$$

Toda's Theorem: $\mathsf{PH} \subseteq \mathsf{P}^{\mathsf{PP}}$

Gödel Prize!!