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: $A \to B$: 多項式時間還元(polynomial-time reduction)

$\Leftrightarrow$
- (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:

$$A \leq_m^P B$$

$A \leq_m^P B$　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) $B \in$ P → $A \in$ P .
(2) $B \in$ NP → $A \in$ NP .
(3) $B \in$ co- NP → $A \in$ co- NP .
(4) $B \in$ EXP → $A \in$ EXP.

補注：クラスEは例外．一般には，$B \in$ E → $A \in$ Eとはならない．

例6.2: ONE≡ {1}と定義するとき，クラス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) $x \in \Sigma^*[x \in L \leftrightarrow h(x) \in \mathrm{ONE}]$
(3) hは多項式時間計算可能($L \in$ P→$x \in L$の判定も多項式時間内）

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

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：二和形式）
3SAT　（命題論理式充足性問題：三和形式）
SAT　（命題論理式充足性問題）
ExSAT　（拡張命題論理式充足性問題）

$$2\mathrm{SAT} \leq_m^P 3\mathrm{SAT}$$

高々k個…自明
ちょうどk個…レポート

同様に,

$$3\mathrm{SAT} \leq_m^P \mathrm{SAT} \leq_m^P \mathrm{ExSAT}$$

$$2\mathrm{SAT} \leq_m^P 3\mathrm{SAT} \leq_m^P \mathrm{SAT} \leq_m^P \mathrm{ExSAT} \quad (6.1)$$

ここで

$$\mathrm{ExSAT} \leq_m^P 3\mathrm{SAT}$$

であることを示せると,

$$3\mathrm{SAT} \equiv_m^P \mathrm{SAT} \equiv_m^P \mathrm{ExSAT}$$

となる.

例6.3: ExSATから3SATへの還元

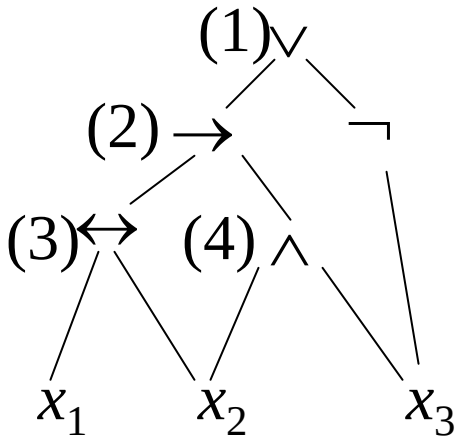
$$E_1(x_1,x_2,x_3) \equiv [[x_1 \leftrightarrow x_2] \rightarrow [x_2 \wedge x_3]] \vee \neg x_3$$

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

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



$$(1) V_1 \equiv V_2 \vee \neg x_3$$
$$(2) V_2 \equiv [V_3 \rightarrow V_4]$$
$$(3) V_3 \equiv [x_1 \leftrightarrow x_2]$$
$$(4) V_4 \equiv x_2 \wedge x_3$$

F_1を構成するために，$V_i \rightarrow U_i$とし，V_iの定義式を$\wedge$で結ぶ

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.

$$U_1 \leftrightarrow [U_2 \vee \neg x_3] = [\neg U_1 \vee U_2 \vee \neg x_3] \wedge [U_1 \vee \neg [U_2 \vee \neg x_2]]$$
$$= [\neg U_1 \vee U_2 \vee \neg x_3] \wedge [U_1 \vee [\neg U_2 \wedge x_2]]$$
$$= [\neg U_1 \vee U_2 \vee \neg x_3] \wedge [U_1 \vee \neg U_2] \wedge [U_1 \vee x_2]$$
$$= [\neg U_1 \vee U_2 \vee \neg x_3] \wedge [U_1 \vee \neg U_2 \vee \neg U_2] \wedge [U_1 \vee x_2 \vee x_2]$$

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.

6.2. 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Cに対し，集合Aが次の条件を満たすとき，
それを（$\leq_m^P$の下で）C-完全という.

(a) $\forall L \in \mathsf{C}\ [L \leq_m^P A]$

(b) $A \in \mathsf{C}$

補注：条件(a)を満たす集合はC-困難.

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

EVAL-IN-E:

入力: $< a, x, \bar{t} >$

a: 1入力プログラムのコード, $x \in \Sigma^*, \bar{t} \geq 0$

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

例6.5. クラスNPの完全集合の例

3SAT, SAT, ExSAT, DHAM, KNAP, BIN, VCなど

クラスEXPの完全集合

EVAL-IN-E, HALT-IN-Eなど

定理6.3. 任意のC-困難集合（含：C-完全集合）Aに対し，

(1) $A \in$ P → C ⊆ P　　対偶は C⊄P → $A \notin$P

(2) $A \in$ NP → C ⊆ NP　　対偶は C⊄NP → $A \notin$NP

(3) $A \in$ co-NP → C ⊆ co-NP　　対偶は C⊄co-NP → $A \notin$co-NP

(4) $A \in$ EXP → C ⊆ EXP　　対偶は C⊄ EXP → $A \notin$EXP

証明：

(1) Bを任意のC集合とすると，AはC-困難だから，

$B \leq_m^P A$　一方，$A \in$Pの仮定より，$B \in$ P（定理6.1）

(2), (3), (4)も同様

定理6.3. 任意のC-困難集合（含：C-完全集合）Aに対し，

(1) $A \in$ P → C ⊆ P　　対偶は C⊄P → $A \notin$P

(2) $A \in$ NP → C ⊆ NP　　対偶は C⊄NP → $A \notin$NP

(3) $A \in$ co-NP → C ⊆ co-NP　　対偶は C⊄co-NP → $A \notin$co-NP

(4) $A \in$ EXP → C ⊆ EXP　　対偶は C⊄ EXP → $A \notin$EXP

例6.6. 定理6.3の意味（クラスNP）

LをNP-完全集合とする.

定理6.3(1)の対偶より，

NP ≠ P ➔ $L \notin$ P

定理6.3(3)の対偶と定理5.9(1)の対偶より，

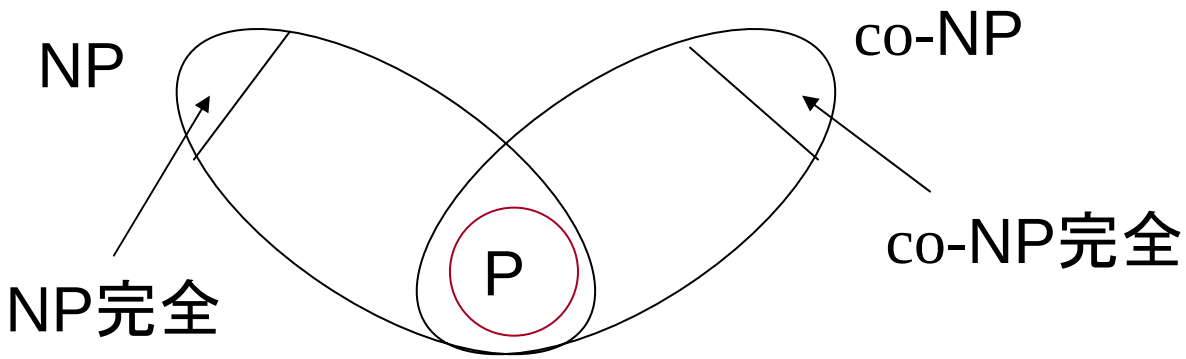
$L \notin$ co-NP

つまり，NP-完全集合はP≠NPである限り，多項式時間では認識できないNP集合である.

定理5.9.

(1) NP ⊆ co-NP → NP = co-NP

NP-完全集合はP ≠NPである限り，NP ∩ co-NPには入らない
NP集合である.



例6.7. 定理6.3の意味（クラスEXP)

DをEXP-完全集合とする.
定理6.3(1)の対偶（C$\not\subset$P → $A\notin$P , ここではEXP$\not\subset$P →$D\notin$P)
P $\neq$EXP → EXP$\not\subset$P (∵P ⊆ EXP) → $D\notin$P
定理6.3(2)の対偶（C$\not\subset$NP → $A\notin$NP ,
ここではEXP$\not\subset$ NP →$D\notin$NP)
NP $\neq$EXP → EXP$\not\subset$NP (∵ NP ⊆ EXP) → $D\notin$NP
定理6.3(3)の対偶（C$\not\subset$ co-NP → $A\notin$co- NP ,
ここではEXP$\not\subset$co- NP →$D\notin$ co- NP)
co-NP $\neq$EXP →EXP $\not\subset$co-NP →$D\notin$ co-NP
ところが, 定理5.7から, P ⊆ EXP であることを知っているから,
無条件に$D\notin$ P.
EXP-完全集合は多項式時間では計算不可能.

定理6.4. A: 任意のC-完全集合
すべての集合Bに対し,
(1) $A \leq_m^P B$ →BはC-困難.
(2) $A \leq_m^P B \ \wedge B \in \mathrm{C}$ → BはC-完全.

証明:
定義6.2より, $\forall L \in C[L \leq_m^P A]$
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, $\forall L \in C[L \leq_m^P B]$
すなわち, BはC-困難.

EXPC $\equiv \{L: L$はEXP-完全$\}$
NPC $\equiv \{L: L$はNP-完全$\}$
とすると，次の定理が成り立つ．

定理6.5.
(1) EXPC $\cap$ P $= \phi$
(2) EXP – (EXPC $\cup$ P) $\neq \phi$

定理6.6: P $\neq$ NPを仮定すると
(1) NPC $\cap$ P $= \phi$
(2) NP – (NPC $\cup$ P) $\neq \phi$