実践離散数学と計算の理論
第2回　述語論理

大阪大学大学院　工学研究科　電気電子情報通信工学専攻
王　イントウ

前回の質問

・レポートの様式について：

- wordで数式エディタを使ってpdf化or wordのまま → OK
- 紙に書いてスキャンしてpdfを提出 → OK
- 写真 → NG

・形式的証明で証明できるときは、QEDと書きますが、証明できないときはどのように記載すればいいのでしょうか？

・証明できない時は、証明できないと書いて、特に記号がない(はず)

- 証明できるかできないかを見極める一般的な方法は無い

- 特に、一般の数学だと、不完全性定理より証明も反証もできないような論理式もある

Exclusive ORとはXORのことでしょうか？

・はい

・形式的証明のとき、どのようにアプローチするのが良いのか、わからない。 CP規則、部分証明、IP規則の違い、組み合わせでの利用など、勘どころがあるでしょうか。それとも、決まった常識的なアプローチの方法があれば、教えていただきたい。

・命題の前提を小さい論理式ごとに分けて、推論規則に当てはまり、部分証明や背理法、既知の定理(次のページで示す)を用いて証明していくのが、一般的なやり方です。証明方法は一つに囚われないので、短くても長くても結論まで証明できればOKです。

- 既知の定理を利用する場合は、T （理由）とかく。TはTheoremのT

$$
\begin{array}{lll}
1. & \neg(A \vee B) & \mathrm{P} \\
2. & C \to D & \mathrm{P} \\
3. & \neg A \wedge \neg B & 1, \mathrm{T} \text{ (ド・モルガン)} \\
4. & \neg C \vee D & 2, \mathrm{T} \text{ (同値)} \\
 & \cdots &
\end{array}
$$

述語論理
（Predicate Logic）

述語（Predicate）

- 述語とは文の一部で主語にある性質を与えるもの：
  (私の娘)は<u>二歳になりました</u>。
- 命題計算では、変数 x はただの真偽値を表したが、述語計算では変数 x の性質を表現可能
  - たとえば x を変数、P を x は10歳である、Q を x は人間である、R を x は小学生であるとすると
    $P(x) \wedge Q(x) \rightarrow R(x)$
    というように性質、意味、関係について記述(コードに書く)可能

存在限量子（existential quantifier）

- ある述語を真とするような値が存在するということを記述するときに用いる
- ∃ で表す
- 例
  - 領域 $D = \{2,3,4,5\}$ とするとき、$P(x)$ を真とする値 $x \in D$ が存在するとき、
    $\exists x\ P(x)$と記号化して表す
  - すなわち、これは選言で書き下せて、$P(2) \vee P(3) \vee P(4) \vee P(5)$ が真になることを表す
- $\exists x\ P(x)$は、英語だと、There exists x such that P(x) = true.

全称限量子（universal quantifier）

- ある述語に対して、すべての値に対して真となることを記述するときに用いる
- ∀ で表す
    - 領域 $D = \{2,3,4,5\}$ とするとき、すべての値 $x \in D$ に対して $P(x)$ が真となるとき、$\forall x\ P(x)$ と表す
    - これは、連言で書き下せて、$P(2) \wedge P(3) \wedge P(4) \wedge P(5)$ が真となることを表す
- $\forall x\ P(x)$ は、英語だとFor all x, P(x) = true.

限量子の有効範囲

- $(\exists x W)$ 中の $\exists x$ の有効範囲は W である
    - $\exists x P(x, y) \rightarrow Q(x)$ は、$(\exists x P(x, y)) \rightarrow Q(x)$ と等価
    - $\exists x P(x) \wedge Q(x)$ は、$(\exists x P(x)) \wedge Q(x)$ と等価
- $\forall$ についても同じ

束縛変数と自由変数

- 論理式中の変数 x が、$\forall$ か $\exists$ で限量されているとき変数 x は束縛されていると言い（束縛変数）、そうでない場合は自由である（自由変数）という
  - 例
    - $\exists x P(x, y) \to Q(x)$
      1つ目の変数 x は束縛変数で、変数 y と2つめの変数 x は自由変数

ド・モルガンの法則

¬(A∨B)≡¬A∧¬B　（ド・モルガンの法則、選言と連言が逆の場合も同じ）

- 限量子の ∀ と ∃ は連言と選言であったことを思い出すと、ド・モルガンの規則*が適用可能であることがわかる

$$\neg(\exists x W) \equiv \forall x \neg W$$

$$\neg(\forall x W) \equiv \exists x \neg W$$

例　$x \in \{0,1,2\}$

$$\neg(\exists x P(x)) \equiv \neg(P(0) \lor P(1) \lor P(2)) \equiv \neg P(0) \land \neg P(1) \land \neg P(2) \equiv \forall x \neg P(x)$$

構文

Aは適当な述語記号(P,Q,...)

述語

$$
\begin{aligned}
P, Q \quad := \quad & \boxed{\begin{aligned} & A(T, \ldots, T) \mid \\ & \forall \mathtt{VAR}\ P \mid \\ & \exists \mathtt{VAR}\ P \mid \end{aligned}} \\
& \mathtt{T} \mid \\
& \mathtt{F} \mid \\
& P \wedge Q \mid \\
& P \vee Q \mid \\
& P \to Q \mid \\
& \neg P \mid \\
& (P)
\end{aligned}
$$

項

$$
\begin{aligned}
T \quad := \quad & \mathtt{VAR} \mid \\
& \mathtt{CONST} \mid \\
& f(T, \ldots, T)
\end{aligned}
$$

関数

$$\mathtt{VAR} \quad := \quad x \mid y \mid z \mid \ldots$$

変数

$$\mathtt{CONST} \quad := \quad a \mid b \mid c \mid \ldots$$

定数

同値性

限量子と否定

$$\neg(\forall x W) \equiv \exists x \neg W$$

$$\neg(\exists x W) \equiv \forall x \neg W$$

同じ限量子の入れ替え

$$\forall x \forall y W \equiv \forall y \forall x\ W$$

$$\exists x \exists y W \equiv \exists y \exists x\ W$$

限量子の分配

$$\exists x(p(x) \vee q(x)) \equiv \exists x\ p(x) \vee \exists x\ q(x)$$

$$\forall x(p(x) \wedge q(x)) \equiv \forall x\ p(x) \wedge \forall x\ q(x)$$

結合子→上の限量子

$$\exists x(p(x) \rightarrow q(x)) \equiv \forall x p(x) \rightarrow \exists x q(x)$$

変数名の置き換え

（yがW(x)中に無い変数のとき）

$$\exists x W \equiv \exists y W[x \mapsto y]$$

$$\forall x W \equiv \forall y W[x \mapsto y]$$

制約付き同値式

制約：論理式C中に変数xが自由に出現しないときに成り立つ

簡約

$\forall x C \equiv C$

$\exists x C \equiv C$

選言

$\forall x (C \lor A(x)) \equiv C \lor \forall x A(x)$

$\exists x (C \lor A(x)) \equiv C \lor \exists x A(x)$

連言

$\forall x (C \land A(x)) \equiv C \land \forall x A(x)$

$\exists x (C \land A(x)) \equiv C \land \exists x A(x)$

含意

$\forall x (C \to A(x)) \equiv C \to \forall x A(x)$

$\exists x (C \to A(x)) \equiv C \to \exists x A(x)$

$\forall x (A(x) \to C) \equiv \exists x A(x) \to C$

$\exists x (A(x) \to C) \equiv \forall x A(x) \to C$

解釈

- 解釈とは、論理式に意味を与える行為。領域、述語の意味を決める。
- 例
  - $\forall x P(x)$ を、$P(x)$ が x は2で割り切れるとし、 x のとる領域を整数と解釈すると、$\forall x P(x)$ はFalseとなる
  - $\forall x \exists y P(x, y)$ を $P(x, y)$ を y は x の母親であるとし、x 、y の取る範囲を人間とすると、この式はTrueである

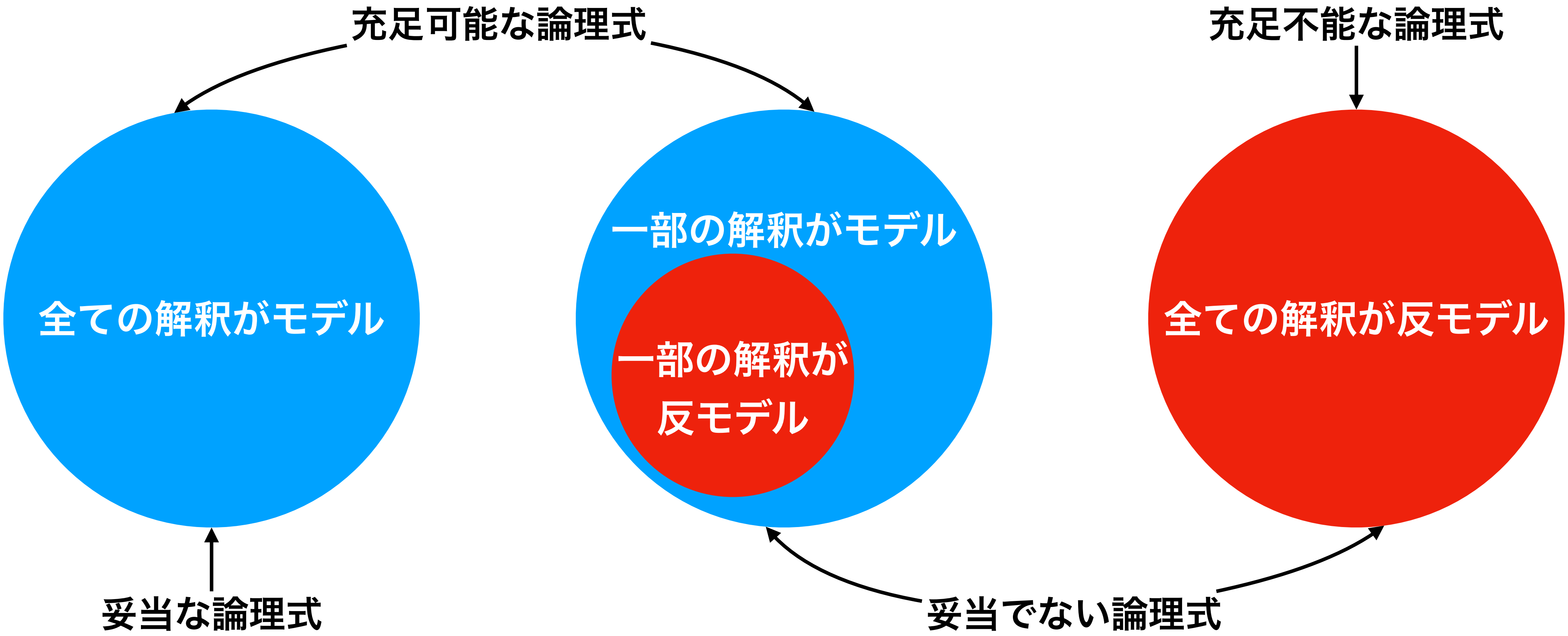
モデルと反モデル

- モデル：論理式を真とする解釈のこと
- 反モデル：論理式を偽とする解釈のこと

妥当性と充足性

- ある論理式が**妥当(valid)**であるとは、すべての解釈がモデルであることを言い、そうでない場合は**妥当でない(invalid)**と言う
- ある論理式がすべての可能な解釈について偽であれば**充足不能(unsatisfiable)**、そうでなければ**充足可能(satisfiable)**であると言う

論理式の解釈と妥当性



充足可能な論理式
充足不能な論理式
全ての解釈がモデル
一部の解釈がモデル
一部の解釈が反モデル
全ての解釈が反モデル
妥当な論理式
妥当でない論理式

モデルと反モデルの例

$\forall x P(x)$

モデルの例

x の領域を正整数として、P を x は1以上であるとする

反モデルの例

$x \in \{1, 2, 3\}$ として、P を x は2で割り切れるとする

妥当な論理式と充足不能の論理式の例

妥当な論理式の例

$$\forall x P(x) \to \exists x P(x)$$

充足不能の論理式の例

$$P(x) \land \neg P(x)$$

述語論理での形式化

- すべてのものは P である　　$\forall x P(x)$
- P なものが存在する　　$\exists x P(x)$
- すべての P は Q である　　$\forall x (P(x) \to Q(x))$
- ある P は Q である　　$\exists x (P(x) \wedge Q(x))$

述語論理での形式化の例

$P(x)$ xは政治家である

$Q(x)$ xは腹黒い

すべての政治家は腹黒い

$\forall x(P(x) \rightarrow Q(x))$

すべての政治家が腹黒いわけではない

$\exists x(P(x) \land \neg Q(x))$

述語論理の形式的証明
（Formal Proof of Predicate Logic）

自由変数への代入

- 「x は人間である」という文があったときに、x に式や値を代入することが出来る
  - x を「私」とすると、「私は人間である」となる
- $W[x \mapsto W_0]$ と書いたときには、論理式W 中の自由変数 x を項W_0に置換するということにする

代入出来ない例

- 「すべての x は y の親である」という文の y を x に置換することは出来ない
- $W[x \mapsto t]$ は、t 中の自由変数が、W によって束縛されないときに限り、W中の自由変数 x を t に置換できる

RRR法

- RRR法とは、述語論理で形式的証明を行う方法
- 限量子の除去(**R**emove)、推論(**R**eason)、復元(**R**estore)という順で行う証明方法

規則

- 限量子の除去
  - 全称実体化規則 (universal instantiation rule: UI)
  - 存在実体化規則 (existential instantiation rule: EI)
- 限量子の復元
  - 全称汎化規則 (universal generalization rule: UG)
  - 存在汎化規則 (existential generalization rule: EG)

全称実体化規則（UI）

$$\frac{\forall x W}{W[x \mapsto t]}$$

W 中の自由変数 x へ t を代入可能
（t 中の自由変数が新たに W によって束縛されない）

すべての x と言っているのだから、
x には何を代入してもよいだろうという考え

UI規則の失敗例

「すべての人間は母を持つ」

$x, y \in$ 人間　　y は x の母である $:= P(x, y)$

$$\forall x W(x) \;=\; \forall x \exists y P(x, y)$$

$$\exists y P(x, y)[x \mapsto y] = \exists y P(y, y)$$

（間違ったUI規則の適用:
yは$W(x)$に束縛されるので）

「自分が自分の母であるような人間が存在する」

存在実体化規則（EI）

$$\frac{\exists x W}{W[x \mapsto c]}$$

ただしcは証明中の命題に現れない、新しい定数

ある x が存在すると言っているのだから、
仮に c と代入してもよいだろうという考え

EI規則の失敗例

「人間には男もいて女もいる」

$x, y \in$ 人間　　　x は男 $:= P(x)$　　　x は女 $:= Q(x)$

$\exists x P(x) \land \exists y Q(y)$

$P(x)[x \mapsto c] = P(c)$

$Q(y)[y \mapsto c] = Q(c)$　　　（間違ったEI規則の適用）

$P(c) \land Q(c)$

「cは男であり女である」

存在汎化規則（EG）

$$\frac{W(t)}{\exists x W(x)}$$

$W(t)$ は式中に項 t を含む論理式

ただし、$W(x)[x \mapsto t]$ と変数代入可能な場合に限る

全称汎化規則（UG）

$$\frac{W(x)}{\forall x W(x)}$$

$W(x)$ は式中に自由変数 x を含む論理式

ただし x は前提に自由に現れず、
かつEI規則によって得られる整論理式中に自由に現れない

EIで得られた整論理式中にある自由変数にUGを適用する失敗

前提は、任意の自然数xよりも大きな自然数yが存在する

$$
\begin{array}{lll}
1. & \forall x \exists y\ (x < y) & \mathrm{P} \\
2. & \exists y\ (x < y) & 1, \mathrm{UI} \\
3. & x < c & 2, \mathrm{EI} \\
4. & \forall x\ (x < c) & 3, \mathrm{UG}\ \text{推論できない}
\end{array}
$$

全ての自然数は定数cより小さいはおかしい

形式的証明の例

$\forall x(A(x) \to B(x)) \land \forall x(B(x) \to C(x)) \to \forall x(A(x) \to C(x))$ を証明せよ

1.	$\forall x(A(x) \to B(x))$	P
2.	$\forall x(B(x) \to C(x))$	P
3.	$A(x) \to B(x)$	1, UI
4.	$B(x) \to C(x)$	2, UI
5.	$A(x) \to C(x)$	3, 4, HS
6.	$\forall x(A(x) \to C(x))$	5, UG
	QED	1-6, CP

$$\frac{\forall x W}{W[x \mapsto t]} \quad \text{(UI)}$$

$$\frac{W(x)}{\forall x W(x)} \quad \text{(UG)}$$

$$\frac{A \to B \quad B \to C}{A \to C} \quad \text{(HS)}$$

高階述語論理

- 階数
    - 命題計算を零階論理と定義
    - これまで述べてきた述語計算を一階論理と定義
    - 述語の限量化を行ったり、述語を引数に取る述語を扱うとき、それを高階論理という

述語の階数

- ある述語の引数が項であるとき、その述語の階数は1
    - 項（term）とは、変数または定数、あるいは項である引数に関数を適用したもの
    - 例：x, a, f(x, g(b))
- ある述語の引数のうち最も高い階数がnであるとき、その述語の階数はn+1
- 例
    - $A(x) \wedge B(A)$ は、Aが階数1、Bが階数2
    - $A(x) \wedge B(A) \wedge C(B)$ は、Aが階数1、Bが階数2、Cが階数3

限量子の階数

- ある限量子が変数を限量するとき、その限量子の階数は1
- ある限量子がn階の述語を限量するとき、その限量子の階数はn+1
- 例
  - $\forall x \exists A(A(B) \wedge B(x))$ はBが1階、Aが2階、∃Aが3階、∀xが1階

論理式の階数

- 論理式の階数とは、その論理式の述語と限量子のうち、最大の階数のこと
- 例
  - $S(x)$ は階数1の整論理式
  - $S(x) \wedge T(S)$ は階数2の整論理式
  - $\exists P(S(x) \wedge T(S) \wedge P(T))$ は4階の整論理式

高階関数

- プログラミング言語で関数を引数にとったり、関数を返すような関数を高階関数と呼ぶ

- 考え方は高階論理の高階とおなじ

レポート課題

レポート課題

- 本スライド中にある問題を解いてレポートとして提出せよ
- 締め切り：2023年5月30日 23:50 (JST)

以下の論理式を∀と∃を使わない論理式にせよ

$S = \{a, b, c\}, s \in S \qquad T = \{d, e\}, t \in T$

としたとき

$$\forall s (P(s) \to Q(s))$$

$$\exists s (P(s) \land Q(s))$$

$$\forall s \, \exists t R(s, t)$$

以下を形式的に証明せよ

$$\forall x(P(x) \to Q(x)) \land \neg \exists x Q(x) \to \forall x \neg P(x)$$

$$\neg Q(c) \land (\exists x P(x) \to \forall y Q(y)) \to \forall x \neg P(x)$$ (ただし、cは定数)

$$\neg \exists x \exists y (R(x, y) \land \neg P(x, y)) \land \forall x \forall y (\neg R(x, y) \to P(x, y)) \to \exists x \exists y P(x, y)$$

情報通信工学演習1：

問題：以下の論理式の階数を求めよ

$$S(x) \wedge T(S, x) \to U(T, S, x)$$

$$\forall x \exists S (S(x) \wedge T(S, x) \to U(T, S, x))$$

情報通信工学演習2：

以下を形式的に証明せよ

- 二項関係が非反射的かつ推移的ならば、非対称的であることを証明せよ

- 非反射的：　$\forall x \neg P(x,x)$
- 推移的：　$\forall x \forall y \forall z (P(x,y) \land P(y,z) \to P(x,z))$
- 非対称的：　$\forall x \forall y (P(x,y) \to \neg P(y,x))$

Hint: 部分証明、ド・モルガンの法則、命題論理の推論規則(UI, UGとか)、述語論理の推論規則(モーダス・ポネンスMP, 間接証明IP)などなど、ご活用ください