2024年度 数理論理学

講義資料(15)

青戸 等人 (知能情報システムプログラム)

目次

述語推論の擬似証明コード：$\forall$Eの推論

命題論理において，2次元的な図形である証明図と1次元的な文章である証明の中間的な形態として，証明図を1次元的な命令の列に翻訳した擬似証明コードを紹介した．ここでは，それを述語論理へ拡張する．命題論理で用いた擬似証明コードの命令は，そのまま述語論理でも用いる．

まず，次の証明図に対する擬似証明コードを示す．

$$\dfrac{\dfrac{[\forall \mathrm{x}\,(\mathrm{P}(\mathrm{x},\mathrm{a}) \vee \mathrm{P}(\mathrm{x},\mathrm{b}))]^3}{\mathrm{P}(\mathrm{a},\mathrm{a}) \vee \mathrm{P}(\mathrm{a},\mathrm{b})}\,\forall\mathrm{E} \quad \dfrac{\dfrac{[\neg\mathrm{P}(\mathrm{a},\mathrm{a})]^2 \quad [\mathrm{P}(\mathrm{a},\mathrm{a})]^1}{\bot}\,\neg\mathrm{E}}{\mathrm{P}(\mathrm{a},\mathrm{b})}\,\bot \quad [\mathrm{P}(\mathrm{a},\mathrm{b})]^1}{\dfrac{\mathrm{P}(\mathrm{a},\mathrm{b})}{\neg\mathrm{P}(\mathrm{a},\mathrm{a}) \to \mathrm{P}(\mathrm{a},\mathrm{b})}\,\to\mathrm{I}^2}\,\vee\mathrm{E}^1}{\forall \mathrm{x}\,(\mathrm{P}(\mathrm{x},\mathrm{a}) \vee \mathrm{P}(\mathrm{x},\mathrm{b})) \to \neg\mathrm{P}(\mathrm{a},\mathrm{a}) \to \mathrm{P}(\mathrm{a},\mathrm{b})}\,\to\mathrm{I}^3$$

```
assume 1 : ∀x (P(x, a) ∨ P(x, b))
assume 2 : ¬P(a, a)
from 1 have 3 : P(a, a) ∨ P(a, b) by ∀E
show P(a, b) as follows:
  distinguish cases by 3
  case P(a, a)
    hence ⊥ using 2 by ¬I
    hence P(a, b) by ⊥E
  case P(a, b)
    hence P(a, b) trivially
  hence claim by ∨E
hence ¬P(a, a) → P(a, a) by →I[2]
hence ∀x (P(x, a) ∨ P(x, b))→¬P(a, a)→P(a, a) by →I[1]
```

$\forall$の除去規則に対する擬似証明コードは，命題論理のときと同様である: $\forall x A$から，任意の項tを用いて，$[x := t](A)$を導出する．もちろん，代入については，束縛変数の名前替えの便宜法を忘れないこと．

演習 **15.1.** 以下の証明図を参考にして，$\forall \mathtt{x}\,(\mathtt{P}(\mathtt{x}) \to \mathtt{Q}(\mathtt{x})) \to \mathtt{P}(\mathtt{a}) \vee \mathtt{P}(\mathtt{b}) \to \mathtt{Q}(\mathtt{a}) \vee \mathtt{Q}(\mathtt{b})$ の擬似証明コードを記せ．

$$\dfrac{\dfrac{\dfrac{[\forall \mathtt{x}\,(\mathtt{P}(\mathtt{x}) \to \mathtt{Q}(\mathtt{x}))]^3}{\mathtt{P}(\mathtt{a}) \to \mathtt{Q}(\mathtt{a})}\forall\mathrm{E} \quad [\mathtt{P}(\mathtt{a})]^1}{\mathtt{Q}(\mathtt{a})}\to\mathrm{E} \qquad \dfrac{\dfrac{\dfrac{[\forall \mathtt{x}\,(\mathtt{P}(\mathtt{x}) \to \mathtt{Q}(\mathtt{x}))]^3}{\mathtt{P}(\mathtt{b}) \to \mathtt{Q}(\mathtt{b})}\forall\mathrm{E} \quad [\mathtt{P}(\mathtt{b})]^1}{\mathtt{Q}(\mathtt{b})}\to\mathrm{E}}{\mathtt{Q}(\mathtt{a}) \vee \mathtt{Q}(\mathtt{b})}\vee\mathrm{I}}{\dfrac{[\mathtt{P}(\mathtt{a}) \vee \mathtt{P}(\mathtt{b})]^2 \qquad \mathtt{Q}(\mathtt{a}) \vee \mathtt{Q}(\mathtt{b})}{\mathtt{Q}(\mathtt{a}) \vee \mathtt{Q}(\mathtt{b})}\vee\mathrm{E}^1}$$

$$\dfrac{\dfrac{\mathtt{P}(\mathtt{a}) \vee \mathtt{P}(\mathtt{b}) \to \mathtt{Q}(\mathtt{a}) \vee \mathtt{Q}(\mathtt{b})}{\forall \mathtt{x}\,(\mathtt{P}(\mathtt{x}) \to \mathtt{Q}(\mathtt{x})) \to \mathtt{P}(\mathtt{a}) \vee \mathtt{P}(\mathtt{b}) \to \mathtt{Q}(\mathtt{a}) \vee \mathtt{Q}(\mathtt{b})}\to\mathrm{I}^3}{}$$

```
assume 1 : ∀x (P(x) → Q(x))
assume 2 : P(a) ∨ P(b)
show Q(a) ∨ Q(b) as follows:
  distinguish cases by 2
  case 3 : P(a)
    from 1 have P(a) → Q(a) by ∀E
    hence Q(a) using 3 by →E
    hence Q(a) ∨ Q(b) by ∨I
  case 4 : P(b)
    from 1 have P(b) → Q(b) by ∀E
    hence Q(b) using 4 by →E
    hence Q(a) ∨ Q(b) by ∨I
  hence claim by ∨E
hence ∀x (P(x) → Q(x)) → P(a) ∨ P(b) → Q(a) ∨ Q(b) by →I[1, 2]
```

述語推論の擬似証明コード：$\forall$Iの推論

次に，$\forall$の導入規則を用いる擬似証明コードについて説明する．$\forall$の導入規則を用いる場合は，新たなブロック構造を考える．まず，次の証明図を考えてみよう．

$$\dfrac{\dfrac{\dfrac{\dfrac{[\forall y\, P(y) \wedge \forall z\, Q(z)]^1}{\forall y\, P(y)}\wedge E}{P(x)}\forall E \qquad \dfrac{\dfrac{[\forall y\, P(y) \wedge \forall z\, Q(z)]^1}{\forall z\, Q(z)}\wedge E}{Q(x)}\forall E}{P(x) \wedge Q(x)}\wedge I}{\dfrac{\forall x\,(P(x) \wedge Q(x))}{\forall y\, P(y) \wedge \forall z\, Q(z) \to \forall x\,(P(x) \wedge Q(x))}\to I^1}\forall I$$

この証明図を擬似証明コードを変換してみる．

```
assume 1 : ∀y P(y) ∧ ∀z Q(z)
hence 2 : ∀y P(y) and 3 : ∀z Q(z) by ∧E
{ fix x
   from 2 have 4 : P(x) by ∀E
   from 3 have 5 : Q(x) by ∀E
   from 4 5 have P(x) ∧ Q(x) by ∧I
} hence ∀x (P(x) ∧ Q(x)) by ∀I
hence ∀y P(y) ∧ ∀z Q(z) → ∀x (P(x) ∧ Q(x)) by →I[1]
```

∀の導入規則で束縛される変数をxとすると，∀の導入規則の直前まで，その変数xが自由に出現する論理式を用いた推論が用いられている．

このように，自由変数xを用いるときには，{と}を用いて，その変数の有効範囲(スコープ)を指定する．

スコープの最初では，fix 命令で，これから用いる変数を宣言する．

∀の導入規則による証明の基本的な形は次の通り．

{ fix x
  ...
  ... have A
} hence $\forall x\, A$ by $\forall$I

変数xは，{と }で囲まれたブロック構造の中で，局所変数として使われる．

fix は，”固定する”という意味の単語だが，この意味の通り，直観的には，この変数は(考えている対象を表わす変数として)固定されている，という気持ちである．

```
{ fix x
  ...
  ... have A
} hence ∀x A by ∀I
```

このとき，変数 x は，(固定されているが)どのような対象も取り得るということに注意．つまり，もし，x に言及するような仮定を {} ブロックの中で導入する場合には，その仮定は，{} ブロックの中で除去を済ませておく必要がある．(これが，∀ の導入規則の条件であった．)

よりわかりやすい証明のためには，x とは関係しない仮定は，{} ブロックの中でなく，プロックに入る前に assume 命令で導入しておくとよい．

演習 **15.2.**　以下の証明図を参考にして，次の述語論理式に対する擬似証明コードを示せ：

$$\forall \mathtt{x}\,(\mathtt{P}(\mathtt{x}) \to \mathtt{Q}(\mathtt{x})) \to \forall \mathtt{x}\,\mathtt{P}(\mathtt{x}) \to \forall \mathtt{x}\,\mathtt{Q}(\mathtt{x})$$

$$\dfrac{\dfrac{\dfrac{\dfrac{[\forall \mathtt{x}\,(\mathtt{P}(\mathtt{x}) \to \mathtt{Q}(\mathtt{x}))]^2}{\mathtt{P}(\mathtt{x}) \to \mathtt{Q}(\mathtt{x})}\,\forall\mathrm{E} \quad \dfrac{[\forall \mathtt{x}\,\mathtt{P}(\mathtt{x})]^1}{\mathtt{P}(\mathtt{x})}\,\forall\mathrm{E}}{\mathtt{Q}(\mathtt{x})}\,{\to}\mathrm{E}}{\forall \mathtt{x}\,\mathtt{Q}(\mathtt{x})}\,\forall\mathrm{I}}{\forall \mathtt{x}\,\mathtt{P}(\mathtt{x}) \to \forall \mathtt{x}\,\mathtt{Q}(\mathtt{x})}\,{\to}\mathrm{I}^1}{\forall \mathtt{x}\,(\mathtt{P}(\mathtt{x}) \to \mathtt{Q}(\mathtt{x})) \to \forall \mathtt{x}\,\mathtt{P}(\mathtt{x}) \to \forall \mathtt{x}\,\mathtt{Q}(\mathtt{x})}\,{\to}\mathrm{I}^2$$

(解答例)

```
assume 1 : ∀x (P(x) → Q(x))
assume 2 : ∀x P(x)
{ fix x
   from 1 have 3 : P(x) → Q(x) by ∀E
   from 2 have 4 : P(x) by ∀E
   from 3 4 have Q(x) by →E
} hence ∀x Q(x) by ∀I
hence ∀x (P(x) → Q(x)) → ∀x P(x) → ∀x Q(x) by →I[1, 2]
```

目次

述語推論の擬似証明コード：$\exists$Iの推論

次に，$\exists$Iの推論に対する擬似証明コードを紹介する．以下の証明図を考える．

$$\dfrac{\dfrac{\dfrac{[\forall \mathrm{x}\, \mathrm{P}(\mathrm{x},\mathrm{x})]^1}{\mathrm{P}(\mathrm{y},\mathrm{y})}\forall\mathrm{E}}{\exists \mathrm{z}\, \mathrm{P}(\mathrm{y},\mathrm{z})}\exists\mathrm{I}}{\forall \mathrm{y}\, \exists \mathrm{z}\, \mathrm{P}(\mathrm{y},\mathrm{z})}\forall\mathrm{I}}{\forall \mathrm{x}\, \mathrm{P}(\mathrm{x},\mathrm{x}) \to \forall \mathrm{y}\, \exists \mathrm{z}\, \mathrm{P}(\mathrm{y},\mathrm{z})}\to\mathrm{I}^1$$

この証明図を擬似証明コードに直してみる．

```
assume 1 : ∀x P(x, x)
{ fix y
   from 1 have P(y, y) by ∀E
   hence ∃z P(y, z) by ∃I
} hence ∀y ∃z P(y, z) by ∀I
hence ∀x P(x, x) → ∀y ∃z P(y, z) by →I[1]
```

∃の導入規則では，$[x := t]A$の形になっているときに，$\exists x\, A$を導出するが，これは擬似証明コードでも同じである．

演習 **15.3.**　以下の証明図を参考にして，次の述語論理式に対する擬似証明コードを示せ：

$$\forall \mathtt{x}\, \mathtt{P}(\mathtt{x}) \vee \mathtt{Q}(\mathtt{a}) \to \exists \mathtt{x}\, (\mathtt{P}(\mathtt{x}) \vee \mathtt{Q}(\mathtt{x}))$$

$$\dfrac{\dfrac{[\forall \mathtt{x}\, \mathtt{P}(\mathtt{x}) \vee \mathtt{Q}(\mathtt{a})]^2 \quad \dfrac{\dfrac{\dfrac{[\forall \mathtt{x}\, \mathtt{P}(\mathtt{x})]^1}{\mathtt{P}(\mathtt{a})}\forall \mathrm{E}}{\mathtt{P}(\mathtt{a}) \vee \mathtt{Q}(\mathtt{a})}\vee \mathrm{I}}{\exists \mathtt{x}\, (\mathtt{P}(\mathtt{x}) \vee \mathtt{Q}(\mathtt{x}))}\exists \mathrm{I} \quad \dfrac{\dfrac{[\mathtt{Q}(\mathtt{a})]^1}{\mathtt{P}(\mathtt{a}) \vee \mathtt{Q}(\mathtt{a})}\vee \mathrm{I}}{\exists \mathtt{x}\, (\mathtt{P}(\mathtt{x}) \vee \mathtt{Q}(\mathtt{x}))}\exists \mathrm{I}}{\exists \mathtt{x}\, (\mathtt{P}(\mathtt{x}) \vee \mathtt{Q}(\mathtt{x}))}\vee \mathrm{E}^1}{\forall \mathtt{x}\, \mathtt{P}(\mathtt{x}) \vee \mathtt{Q}(\mathtt{a}) \to \exists \mathtt{x}\, (\mathtt{P}(\mathtt{x}) \vee \mathtt{Q}(\mathtt{x}))} \to \mathrm{I}^2$$

```
assume 1 : ∀x P(x) ∨ Q(a)
show ∃x (P(x) ∨ Q(x)) as follows:
  distinguish cases by 1
  case ∀x P(x)
    hence P(a) by ∀E
    hence P(a) ∨ Q(a) by ∨I
    hence ∃x(P(x) ∨ Q(x)) by ∃I
  case P(b)
    hence P(b) ∨ Q(b) by ∨I
    hence ∃x(P(x) ∨ Q(x)) by ∃I
  hence claim by ∨E
hence ∀x P(x) ∨ Q(a) → ∃x (P(x) ∨ Q(x)) by →I[1]
```

$\exists$Iによって，自由変数がなくなる場合もある．そのように，自由変数のスコープを閉じるだけのときは，単に}でスコープを閉じて，そのまま推論を続ければよい．

例として，以下の証明図に対する擬似証明コードを考えてみよう．

$$\dfrac{\dfrac{\dfrac{\dfrac{[\forall \mathrm{x}\,\mathrm{P}(\mathrm{x},\mathrm{x})]^{1}}{\mathrm{P}(\mathrm{y},\mathrm{y})}\forall\mathrm{E}}{\exists \mathrm{z}\,\mathrm{P}(\mathrm{y},\mathrm{z})}\exists\mathrm{I}}{\exists \mathrm{y}\,\exists \mathrm{z}\,\mathrm{P}(\mathrm{y},\mathrm{z})}\exists\mathrm{I}}{\forall \mathrm{x}\,\mathrm{P}(\mathrm{x},\mathrm{x}) \to \exists \mathrm{y}\,\exists \mathrm{z}\,\mathrm{P}(\mathrm{y},\mathrm{z})}\to\mathrm{I}^{1}$$

```
assume 1 : ∀x P(x, x)
{ fix y
   from 1 have P(y, y) by ∀E
   hence ∃z P(y, z) by ∃I
} hence ∃y ∃z P(y, z) by ∃I
hence ∀x P(x, x) → ∃y ∃z P(y, z) by →I[1]
```

∃Iによって，自由変数yはなくなるので，そのスコープは閉じてよい．

自由変数のスコープは，ネストしてもよい．次ページに，スコープのネストが必要になる例を示す．

$$\dfrac{\dfrac{\dfrac{[\forall y\, P(x,y)]^1}{P(x,y)}\,\forall E}{\exists y\, P(x,y)}\,{\to}I}{\forall y\, P(x,y) \to \exists y\, P(x,y)}\,{\to}I^1}{\forall x\, (\forall y\, P(x,y) \to \exists y\, P(x,y))}\,\forall I$$

{ fix x
  assume 1 : $\forall y\, P(x,y)$
  { fix y
    from 1 have $P(x,y)$ by $\forall E$
  } hence $\exists y\, P(x,y)$ by $\exists I$
  hence $\forall y\, P(x,y) \to \exists y\, P(x,y)$ by $\to I[1]$
} hence $\forall x\, (\forall y\, P(x,y) \to \exists y\, P(x,y))$ by $\forall I$

述語推論の擬似証明コード：$\exists$Eの推論

次に，$\exists$の除去規則に対する擬似証明コードを紹介する．以下の証明図に対する擬似証明コードを考えてみる．

$$\dfrac{\dfrac{\dfrac{[\mathrm{P}(\mathrm{z}) \wedge \neg \mathrm{P}(\mathrm{z})]^{1}}{\neg \mathrm{P}(\mathrm{z})} \wedge \mathrm{E} \quad \dfrac{[\mathrm{P}(\mathrm{z}) \wedge \neg \mathrm{P}(\mathrm{z})]^{1}}{\mathrm{P}(\mathrm{z})} \wedge \mathrm{E}}{\dfrac{[\exists \mathrm{x}\,(\mathrm{P}(\mathrm{x}) \wedge \neg \mathrm{P}(\mathrm{x}))]^{2} \qquad \bot}{\bot} \neg \mathrm{E}} \exists \mathrm{E}^{1}}{\neg \exists \mathrm{x}\,(\mathrm{P}(\mathrm{x}) \wedge \neg \mathrm{P}(\mathrm{x}))} \neg \mathrm{I}^{2}$$

```
assume 1 : ∃x (P(x) ∧ ¬P(x))
{ fix z
   assume 2 : P(z) ∧ ¬P(z)
   from 2 have P(z) and ¬P(z) by ∧E
   hence ⊥ by ¬E
} hence ⊥ using 1 by ∃E[2]
hence ¬∃x (P(x) ∧ ¬P(x)) by ¬I[1]
```

∃の除去規則においても，自由変数が導入される．やり方は，∀の除去規則のときと同様.

∃の除去規則では，スコープのなかにある仮定が除去されることに注意．むろん，∃の除去規則の適用に際しては，変数条件のチェックが必要.

演習 **15.4.**　以下の証明図を参考にして，次の述語論理式に対する擬似証明コードを示せ：

$$\forall \mathrm{x}\,(\mathrm{P}(\mathrm{x}) \to \mathrm{Q}(\mathrm{x})) \to \exists \mathrm{x}\,\mathrm{P}(\mathrm{x}) \to \exists \mathrm{x}\,\mathrm{Q}(\mathrm{x})$$

$$\dfrac{\dfrac{\dfrac{\dfrac{[\forall \mathrm{x}\,(\mathrm{P}(\mathrm{x}) \to \mathrm{Q}(\mathrm{x}))]^3}{\mathrm{P}(\mathrm{z}) \to \mathrm{Q}(\mathrm{z})}\forall\mathrm{E} \quad [\mathrm{P}(\mathrm{z})]^1}{\mathrm{Q}(\mathrm{z})}\to\mathrm{E}}{\exists \mathrm{x}\,\mathrm{Q}(\mathrm{x})}\exists\mathrm{I} \qquad [\exists \mathrm{x}\,\mathrm{P}(\mathrm{x})]^2}{\exists \mathrm{x}\,\mathrm{Q}(\mathrm{x})}\exists\mathrm{E}^1}{\exists \mathrm{x}\,\mathrm{P}(\mathrm{x}) \to \exists \mathrm{x}\,\mathrm{Q}(\mathrm{x})}\to\mathrm{I}^2}{\forall \mathrm{x}\,(\mathrm{P}(\mathrm{x}) \to \mathrm{Q}(\mathrm{x})) \to \exists \mathrm{x}\,\mathrm{P}(\mathrm{x}) \to \exists \mathrm{x}\,\mathrm{Q}(\mathrm{x})}\to\mathrm{I}^3$$

```
assume 1 : ∀x (P(x) → Q(x))
assume 2 : ∃x P(x)
{ fix z
   assume 3 : P(z)
   from 1 have P(z) → Q(z) by ∀I
   hence Q(z) by →E
   hence ∃x Q(x) by ∃I
} hence ∃x Q(x) using 2 by ∃E[3]
hence ∀x (P(x) → Q(x)) → ∃x P(x) → ∃x Q(x) by →I[1, 2]
```

目次

述語推論の擬似証明コードから数学の証明へ

前にも述べたように，数学の証明は，述語論理に基づいている．我々の見てきた擬似証明コードは，証明図よりは，数学の証明に近いものとなっていると思われる．とはいえ，実際の数学の証明とは，まだ差分も多い．

述語推論を使った証明で注意すべき点を2点あげておく：

- 1番外側の$\forall$や最後の$\forall$Iの推論は省略されることが多い．つまり，「$A(x,y)$が成立する」という意味は，「$\forall x \forall y\, A(x,y)$が成立する」という意味である．

- $\forall$や$\exists$の使い方がもっと柔軟．(我々の学習してきた述語論理は第一階述語論理とよばれるものだが，数学で用いられる述語論理は，高階述語論理のため．)

等号の推論の利用

擬似証明コードでは，等号の推論については取り上げなかった．ただ，等号の推論については，自然演繹法の推論を特に意識しないでも使えると思う．

すでに示したように，等号の公理から，等号の反射性，対称性，推移性が証明できる．これらの性質は暗黙のうちに使われることが多い．特に，“等しい”ものを繋げていって，“等しい”ことを示す，のはよく用いられる手法．

また，$s = t$のとき，以下の性質もよく用いる：

- sを使ってもtを使っても計算した値は等しい．
- 命題$A(s)$が成立$\Leftrightarrow$命題$A(t)$が成立．

定義について

前にも触れたように，定義は(少なくても論理的な観点からは)言葉の置き換えにすぎない．しかし，定義を用いた，

用語	$\Rightarrow$	用語の意味する項や論理式	$(unfolding)$
用語	$\Leftarrow$	用語の意味する項や論理式	$(folding)$

の両方向の変換は，数学の証明の多くの部分を占めることも確かである．

したがって，定義を知らないと証明ができない，のは明らかだろう．つまり，使われている用語の定義がわからない場合には，まず定義を知る必要がある．

用語の定義がわからない場合という状況をもう少し詳しく解析すると，以下のように，いくつかのケースがあるだろうか.

ケース (1): その定義をその著者が与えているか，説明している場合. 通常，その用語を用いるのに先だって，用語を説明しているか，もしくは，定義を与えているはずである. 従って，どこかに定義がないか，関連する所を探してみる必要があるだろう. 例えば，この講義であれば，これまでの講義資料をさらってみる，ということになる.

ケース (2): 定義が省略されている場合. その分野の基本的な用語であったりすれば，定義が省略されている場合もある. その場合は，その分野の専門書なり論文なりで，その用語の定義を調べる必要がある. 実際には，説明がないよ

うな，基本的な用語がわかっていない場合には，その分野の基礎的な教科書を少し勉強する必要があるだろう..

ケース (3): 省略すべきでない定義なのに，著者が失念して記述していない場合．この場合も非常に多い．書き手をあまり信じてはいけない．

一般には，同じ用語であっても，分野によって，あるいは，使う人によって，定義はさまざま．であることにも注意.

(擬似証明コードから)数学の証明へ(例1)

これまでの説明を，具体的に見てみるために，ここでは昔に見た次の命題の証明を考えてみよう．

定理 **15.5.** (再掲) 命題論理式上の論理的同値性$\cong$は同値関係である．

同値関係の定義より，“$\cong$が反射的，かつ，$\cong$が対称的，かつ，$\cong$が推移的”，示せばよい．

これには，“$\cong$が反射的”と，“$\cong$が対称的”と，“$\cong$が推移的”とを，それぞれ示せばよい．そうすれば，$\wedge$Iの推論から命題が得られる．

(証明)

(1) 反射性

「$\cong$が反射的である $\overset{\text{def}}{\Longleftrightarrow} \forall A\ (A \cong A)$」であるから，$\cong$の反射性を示すには，$\forall A\ (A \cong A)$を示せばよい．したがって，$A$を任意にとり **(**擬似コードでの`fix`命令**)**，$A \cong A$を示せばよい．**(**最後の$\forall$Iの推論は，もちろん省略．**)**

「 Aを任意の命題論理式とする．vを任意の付値とする．このとき，$[\![A]\!]_v = [\![A]\!]_v$が成立する．よって，任意の付値$v$について，$[\![A]\!]_v = [\![A]\!]_v$が成立する．よって，論理的同値性の定義より，$A \cong A$. したがって，任意の命題論理式$A$について，$A \cong A$. すなわち，$\cong$は反射的.」

緑文字にした部分は，普通に省略されそうな箇所.

(2) 対称性

「$\cong$が対称的である $\overset{\text{def}}{\Longleftrightarrow} \forall A \forall B\,(A \cong B \Rightarrow B \cong A)$」．したがって，$A, B$を任意にとり **(fix命令)**，“$A \cong B \Rightarrow B \cong A$”を示せばよい．“$A \cong B \Rightarrow B \cong A$”には，$\to$Iの推論より，“$A \cong B$”を仮定して，“$B \cong A$”を導けばよい．

「A, Bを任意の命題論理式とする．$A \cong B$と仮定する．すると，論理的同値性の定義より，任意の付値vについて，$[\![A]\!]_v = [\![B]\!]_v$．いま，$v$を任意の付値とする．すると，$[\![A]\!]_v = [\![B]\!]_v$．よって，等号の性質から，$[\![B]\!]_v = [\![A]\!]_v$．したがって，任意の付値$v$について，$[\![B]\!]_v = [\![A]\!]_v$．したがって，論理的同値性の定義より，$B \cong A$．以上より，$A \cong B$ならば$B \cong A$．よって，任意の命題論理式$A, B$について，$A \cong B$ならば$B \cong A$が成り立つ．よって，定義より，$\cong$は対称的である．」

(3) 推移性

「$\cong$が推移的である $\overset{\text{def}}{\Longleftrightarrow}$ $\forall A \forall B \forall C\,(A \cong B$かつ$B \cong C \Rightarrow A \cong C)$」．したがって，$A, B, C$を任意にとり **(`fix`命令)**，“$A \cong B$かつ$B \cong C \Rightarrow A \cong C$”を示せばよい．

「A, B, Cを任意の命題論理式とする．$A \cong B$，$B \cong C$と仮定する．すると，論理的同値性の定義より，任意の付値vについて，$[\![A]\!]_v = [\![B]\!]_v$，$[\![B]\!]_v = [\![C]\!]_v$．今，$v$を任意の付値とする．このとき，$[\![A]\!]_v = [\![B]\!]_v$かつ$[\![B]\!]_v = [\![C]\!]_v$．よって，等号の性質から，$[\![A]\!]_v = [\![C]\!]_v$．ゆえに，任意の付値$v$について，$[\![A]\!]_v = [\![C]\!]_v$．よって，論理的同値性の定義より，$A \cong C$．以上より，$A \cong B$かつ$B \cong C$ならば$A \cong C$．したがって，任意の命題論理式$A, B, C$について，$A \cong B$かつ$A \cong B$ならば$B \cong C$が成立する．よって，推移性の定義から，$\cong$は推移的である．」

(擬似証明コードから)数学の証明へ(例2)

次に，もう少し複雑な述語推論を使っている例として，関数の性質に関する証明を眺めてみよう．

命題 **15.6.** 関数 $f : A \to B, g : B \to C$ が全射であるとき，f と g の合成 $g \circ f : A \to C$ も全射となる．

ここで，命題の**1**番外側の$\forall$である”任意の f, g について”が省略されていることに注意.

関数の全射性の定義は「 関数 $f : A \to B$ が全射 $\overset{\text{def}}{\iff}$ $\forall y \in B\ \exists x \in A\ f(x) = y$」であることに注意すると，任意の全射関数 $f : A \to B, g : B \to C$ をとり，「 任意の $z \in C$ について，ある $x \in A$ が存在して，$(g \circ f)(x) = z$ となること」を示せばよい．

関数$f : A \to B, g : B \to C$が全射であると仮定する.
任意の$z \in C$をとる **(fix z)**.
このとき，$g : B \to C$が全射であること **($\forall z \in C\ \exists y \in B\ (g(y) = z)$，つまり，$\forall z(z \in C \Rightarrow \exists y \in B\ (g(y) = z))$)**
から，ある$y \in B$が存在して，$g(y) = z$が成立する．よって，**(fix y)** $g(y) = z$なる$y \in B$が得られる.
次に，$f : A \to B$が全射であることから，ある$x \in A$が存在して，$f(x) = y$が成立する.
よって，**(fix x)** $f(x) = y$なる$x \in A$が得られる.
このとき，関数合成の定義から，$(g \circ f)(x) = g(f(x)) = g(y) = z$が成立.
したがって，よって，ある$x \in A$が存在して$(g \circ f)(x) = z$が成立.
以上より，任意の$z \in C$について，$x \in A$が存在して，$(g \circ$

$f)(x) = z$となる．よって，$g \circ f : A \to C$が全射であることが示された． □

もっとも，普通は，以下ぐらいの証明に圧縮される：

(証明)
任意の$z \in C$をとる．このとき，$g : B \to C$が全射であることから，$g(y) = z$なる$y \in B$が存在する．よって，$f : A \to B$が全射であることから，$g(y) = z$なる$y \in B$が存在する．このとき，関数合成の定義から，$(g \circ f)(x) = g(f(x)) = g(y) = z$が成立．よって，$g \circ f : A \to C$が全射であることが示された． □

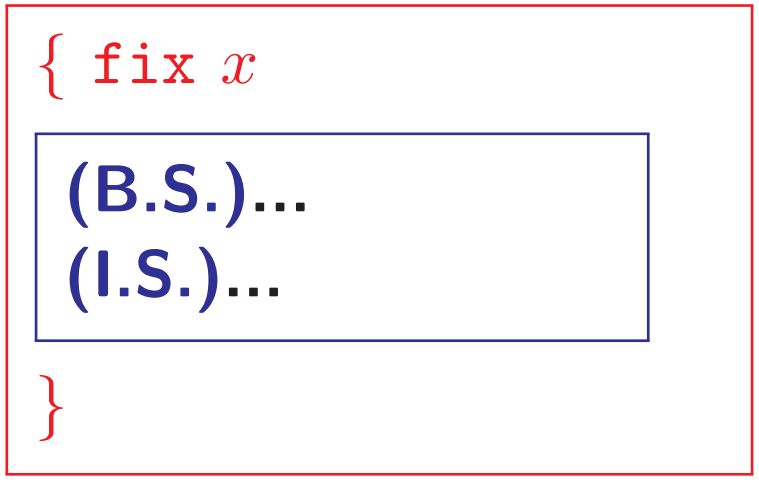
帰納法と∀Iの順序

$\forall x, y \in \mathbb{N}.\, A(x, y)$を$y$に関する帰納法で示すことを考える．
このとき，2種類の証明構造があることに注意しよう：

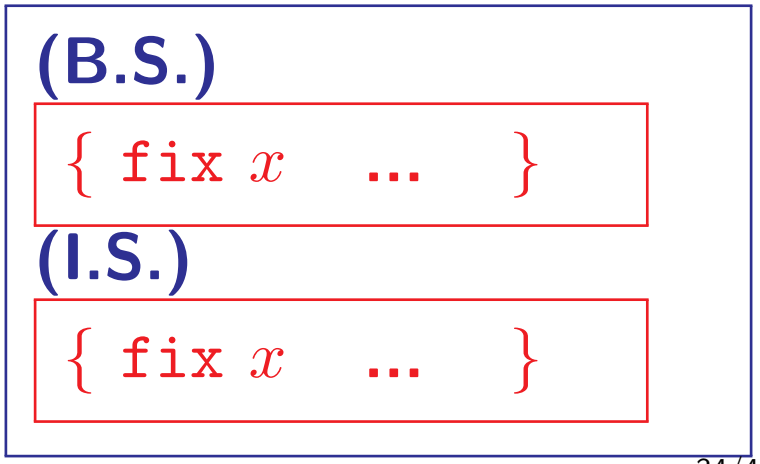
形式(I)：∀Iのブロックの中で，帰納法が使われる．

形式(II)：帰納法のブロックの中で，∀Iが使われる．

形式(I)



形式(II)



形式 (I)

{ x を固定する．

$A(x,y)$ を y に関する帰納法で証明
基本ステップ： $A(x,0)$ を示す．
帰納ステップ：
$A(x,k)$ を仮定して (帰納法の仮定)，
$A(x,k+1)$ を示す．
$A(y,k)$ $(x \neq y)$ は仮定として使えない．

よって，任意の y について $A(x,y)$ が成立．
} ゆえに，任意の x,y について $A(x,y)$ が成立．

形式 (II)

$\forall x.A(x,y)$ を，y に関する帰納法で証明

基本ステップ：$\forall x.A(x,0)$ を示す．

{ x を固定する．
x の取り方によらず，$A(x,0)$ が成立を示す
} よって，任意の x について $A(x,0)$ が成立．

帰納ステップ：$\forall x A(x,k) \Rightarrow \forall x A(x,k+1)$ を示す．

$\forall x A(x,k)$ を仮定する (帰納法の仮定)．
{ x を固定する．
x の取り方によらず，$A(x,k+1)$ が成立を示す．このとき，$A(y,k)$ $(x \neq y)$ も仮定として使えることに注意．
} ゆえに，任意の x,y について $A(x,y)$ が成立．

目次

数学の言葉と論理の言葉

数学の証明においては，論理推論の他にも，さまざまな数の性質や集合の性質が用いられる．

論理	数学
省略方法の約束	定義
論理式	命題 (真偽は問わないで使う場合)
恒真	定理/補題/命題 (使い方で区別する)
$\wedge, \vee, \rightarrow, \neg$	かつ，または，ならば，〜でない
証明図	証明
$\forall, \exists$	任意の〜について $(\forall)$，〜が存在して $(\exists)$
仮定集合を明示	適切な仮定 (公理) を暗黙に仮定

集合論の公理からその他の公理は導けるので，集合論の公理が仮定されていると考えればよい．

公理系と数学の体系

定義 15.7. [公理系] 閉じた述語論理式の集合を公理系とよぶ.

例. 体の公理系

$$\forall x\,\forall y\,\forall z((x+y)+z \approx x+(y+z))$$
$$\forall x\,\forall y(x+y \approx y+x)$$
$$\forall x\,\forall y\,\forall z((x\times y)\times z \approx x\times(y\times z))$$
$$\forall x\,\forall y\,\forall z(x\times(y+z) \approx (x\times y)+(x\times z))$$
$$\forall x(x+0 \approx x)$$
$$\forall x(x+(-x) \approx 0)$$
$$\forall x(1\times x \approx x)$$
$$\forall x\,\forall y(x\times y \approx y\times x)$$
$$0 \not\approx 1$$
$$\forall x(\neg(x \approx 0) \to \exists y(x\times y \approx 1)$$

自然数論の公理系(ペアノ 算術)

$$\forall \mathtt{x}\,(\neg \mathtt{S}(\mathtt{x}) \approx \mathtt{0})$$
$$\forall \mathtt{x}\,\forall \mathtt{y}\,(\mathtt{S}(\mathtt{x}) \approx \mathtt{S}(\mathtt{y}) \to \mathtt{x} \approx \mathtt{y})$$
$$\forall \mathtt{x}\,(\mathtt{x}{+}\mathtt{0} \approx \mathtt{x})$$
$$\forall \mathtt{x}\,\forall \mathtt{y}\,(\mathtt{x}{+}\mathtt{S}(\mathtt{y}) \approx \mathtt{S}(\mathtt{x}{+}\mathtt{y}))$$
$$\forall \mathtt{x}\,(\mathtt{x}{\times}\mathtt{0} \approx \mathtt{0})$$
$$\forall \mathtt{x}\,\forall \mathtt{y}\,(\mathtt{x}{\times}\mathtt{S}(\mathtt{y}) \approx (\mathtt{x}{\times}\mathtt{y}){+}\mathtt{x})$$

および，以下の形をしたすべての L 上の閉じた述語論理式

$$[x := \mathtt{0}](A) \wedge \forall x\,(A \to [x := \mathtt{S}(x)](A)) \to \forall x\,A$$

ペアノ 算術は自然数論の公理系となっている.

集合論の公理系(ZFC集合論)

外延性の公理　$\forall \mathrm{x}, \mathrm{y}\,(\forall \mathrm{z}\,(\mathrm{z} \in \mathrm{x} \leftrightarrow \mathrm{z} \in \mathrm{y}) \to \mathrm{x} \approx \mathrm{y})$

分出公理　$\forall \mathrm{x} \exists \mathrm{y} \forall \mathrm{z} (\mathrm{z} \in \mathrm{y} \leftrightarrow \mathrm{z} \in \mathrm{x} \wedge A(\mathrm{z}))$

空集合の公理　$\exists \mathrm{x}\, \forall \mathrm{y}\, (\mathrm{y} \notin \mathrm{x})$

対集合の公理　$\forall \mathrm{x}, \mathrm{y}\, \exists \mathrm{u} \forall \mathrm{z} (\mathrm{z} \in \mathrm{u} \leftrightarrow \mathrm{z} \approx \mathrm{x} \vee \mathrm{z} \approx \mathrm{y})$

合併集合の公理　$\forall \mathrm{u} \exists \mathrm{z} \forall \mathrm{x} (\mathrm{x} \in \mathrm{z} \leftrightarrow \exists \mathrm{y} \in \mathrm{u}\, (\mathrm{x} \in \mathrm{y}))$

. . . . . .

(ZFC集合論では10つの公理がある．)

集合論の公理から，さまざまな集合の性質が証明されることや，(その他の)専門的な内容は，公理的集合論というキーワードの入っている本を勉強するとよい．

(近代的な)数学は，集合論上に，数論や群論など他の理論を展開する形で形式化される．(例えば，自然数$0, 1, 2, \ldots$は$\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \ldots$と表わし，ペアノの公理が導かれることを示す．)

集合論の公理から，数学でよく使う基本的な命題がどのように証明できるのかを勉強するには，以下の文献が大変お勧め:

島内 剛一，数学の基礎，日本評論社,**1971**年.

なお，本講義の次の段階として勉強するレベルとしても適切な本と思います.

“明らか”，“自明”とは？

証明のなかで，“明らか”や“自明”といった言葉が用いられているのを見たことがあるかもしれない．証明のなかで用いられる“明らか”や“自明”は，日常の言葉で用いる“明らか”や“自明”とは異なる意味をもっている．

一般的な意味:
「いろいろ想像しても間違っているように思えない．」
「それが成り立たないようなケースはなさそうに思える．」

証明で用いられる意味:
「少々の作業量で証明を書き下せる．」

証明中に，“明らか”や“自明”と書かれている場合，その証明を自分で補完できなければいけない．

証明するのに必要なもの

(1) どうして成立するのか，どうやって証明できるかのアイデア

これを得るには創造性が必要．パズルを解くのと同じ．
(でも，実際に証明をきちんと書いてみると穴が見つかることも...)

(2) 証明を書く技術

(2-1) 正しい証明を書く技術
これは身につけることのできる技術．この講義が役立つのはこのレベル．

(2-2) 読みやすい証明を書く技術
正しいことがまず条件だが，人に読んでもらうには読みやすさも重要．文章を書くのと同じで，改善にはキリがない．

もっと証明に上達したい方へ

理論的な内容を取り扱った教科書を，何冊かきちんとした指導者のもとで読むのが，近道でしょう．

以下の本は，英語ですが，無料の**PDF**もあるので，内容もきちんとしていて，初心者が勉強するのには，お勧めできます．

Richard Hammack, Book of Proof (3rd ed.), Published by Richard Hammack, 2018, https://richardhammack.github.io/BookOfProof/.

この講義の内容をひと通り理解した人は十分読めるでしょう．

まとめ

- 述語推論の擬似証明コード
  - `fix`, {, }ブロック
- 証明図から，数学の証明へ
  - 等号推論の利用，定義
  - 帰納法と $\forall$ の導入規則の順序に関する注意
  - 公理系と数学の証明