論理学
第5回「証明(演習)」

萩野　達也
hagino@sfc.keio.ac.jp

lecture URL

https://vu5.sfc.keio.ac.jp/slide/

前回まで

- 命題
  - 論理結合子（∧, ∨, →, ¬）
  - 真理値表
  - トートロジー
- 標準形
  - 論理和標準形
  - 論理積標準形
  - 論理結合子の制限
- 証明
  - 公理と定理
  - LK体系

式の構文的な意味

定理: 次の3つは同値である.

1. 式 $A_1, \ldots, A_m \vdash B_1, \ldots, B_n$ がLKで証明可能である.
2. 式 $A_1 \land \cdots \land A_m \vdash B_1 \lor \cdots \lor B_n$ がLKで証明可能である.
3. 論理式 $A_1 \land \cdots \land A_m \to B_1 \lor \cdots \lor B_n$ がLKで証明可能である.

証明: かんたんにするために, $m = n = 2$ の場場合を示す.

- まず, (1)が成り立てば, (2)であることを示す.

$$\begin{array}{c l}
A_1, A_2 \vdash B_1, B_2 & \\ \hline
A_1, A_2 \vdash B_1, B_1 \lor B_2 & (\lor\mathrm{R}_2) \\ \hline
A_1, A_2 \vdash B_1 \lor B_2, B_1 & (\mathrm{ER}) \\ \hline
A_1, A_2 \vdash B_1 \lor B_2, B_1 \lor B_2 & (\lor\mathrm{R}_1) \\ \hline
A_1, A_2 \vdash B_1 \lor B_2 & (\mathrm{CR}) \\ \hline
A_1 \land A_2, A_2 \vdash B_1 \lor B_2 & (\land\mathrm{L}_1) \\ \hline
A_2, A_1 \land A_2 \vdash B_1 \lor B_2 & (\mathrm{EL}) \\ \hline
A_1 \land A_2, A_1 \land A_2 \vdash B_1 \lor B_2 & (\land\mathrm{L}_2) \\ \hline
A_1 \land A_2 \vdash B_1 \lor B_2 & (\mathrm{CL})
\end{array}$$

証明(つづき)

定理:次の3つは同値である.

1. 式 $A_1, \dots, A_m \vdash B_1, \dots, B_n$ がLKで証明可能である.
2. 式 $A_1 \land \cdots \land A_m \vdash B_1 \lor \cdots \lor B_n$ がLKで証明可能である.
3. 論理式 $A_1 \land \cdots \land A_m \to B_1 \lor \cdots \lor B_n$ がLKで証明可能である.

証明(つづき):

- 次に, (2)が成り立てば, (3)であることを示す.

$$\dfrac{A_1 \land A_2 \vdash B_1 \lor B_2}{\vdash A_1 \land A_2 \to B_1 \lor B_2}\ (\to\mathrm{R})$$

証明（つづき）

定理 : 次の3つは同値である.

1. 式 $A_1, \ldots, A_m \vdash B_1, \ldots, B_n$ がLKで証明可能である.
2. 式 $A_1 \land \cdots \land A_m \vdash B_1 \lor \cdots \lor B_n$ がLKで証明可能である.
3. 論理式 $A_1 \land \cdots \land A_m \to B_1 \lor \cdots \lor B_n$ がLKで証明可能である.

証明（つづき）:

- 最後に, (3)が成り立てば, (1)であることを示す.
- (1)ならば(2), (2)ならば(3), (3)ならば(1)なので, 3つ同値である.

$$
\begin{prooftree}
\AxiomC{$\vdash A_1 \land A_2 \to B_1 \lor B_2$}
\AxiomC{}
\RightLabel{(I)}
\UnaryInfC{$A_1 \vdash A_1$}
\RightLabel{(WL)}
\UnaryInfC{$A_2, A_1 \vdash A_1$}
\RightLabel{(EL)}
\UnaryInfC{$A_1, A_2 \vdash A_1$}
\AxiomC{}
\RightLabel{(I)}
\UnaryInfC{$A_2 \vdash A_2$}
\RightLabel{(WL)}
\UnaryInfC{$A_1, A_2 \vdash A_2$}
\RightLabel{(∧R)}
\BinaryInfC{$A_1, A_2 \vdash A_1 \land A_2$}
\AxiomC{}
\RightLabel{(I)}
\UnaryInfC{$B_1 \vdash B_1$}
\RightLabel{(WR)}
\UnaryInfC{$B_1 \vdash B_1, B_2$}
\AxiomC{}
\RightLabel{(I)}
\UnaryInfC{$B_2 \vdash B_2$}
\RightLabel{(WR)}
\UnaryInfC{$B_2 \vdash B_2, B_1$}
\RightLabel{(ER)}
\UnaryInfC{$B_2 \vdash B_1, B_2$}
\RightLabel{(∨L)}
\BinaryInfC{$B_1 \lor B_2 \vdash B_1, B_2$}
\RightLabel{(→L)}
\BinaryInfC{$A_1 \land A_2 \to B_1 \lor B_2, A_1, A_2 \vdash B_1, B_2$}
\RightLabel{(Cut)}
\BinaryInfC{$A_1, A_2 \vdash B_1, B_2$}
\end{prooftree}
$$

LKの式の意味

- LK式（sequent）を用いる

$$A_1, \ldots, A_m \vdash B_1, \ldots, B_n$$

- 直観的な意味
  - A_1からA_mを仮定すると，B_1からB_nのどれかが導かれる．
- 構文的な意味
  - $A_1 \land \cdots \land A_m \vdash B_1 \lor \cdots \lor B_n$
  - $A_1 \land \cdots \land A_m \to B_1 \lor \cdots \lor B_n$
- 構文の解釈
  - 「$A_1, \ldots, A_m$」前件の「,」は「かつ」
  - 「$B_1, \ldots, B_n$」後件の「,」は「または」
  - 「$\vdash$」は「ならば」

式（sequent）に関するトートロジー

- 論理式のトートロジーを式（sequent）に拡張する.

- Γ を論理式の列 $A_1, \ldots, A_m$ としたとき,

$$\Gamma^* = \begin{cases} A_1 \vee \cdots \vee A_m & m > 0 \text{ のとき} \\ \perp & m = 0 \text{ のとき} \end{cases}$$

$$\Gamma_* = \begin{cases} A_1 \wedge \cdots \wedge A_m & m > 0 \text{ のとき} \\ \top & m = 0 \text{ のとき} \end{cases}$$

- 式 $\Gamma \vdash \Delta$ がトートロジーである ⇔ $\Gamma_* \to \Delta^*$ がトートロジーである

式

$$\Gamma \vdash \Delta$$

=

論理式

$$\Gamma_* \to \Delta^*$$

推論の拡張

- 式の左端右端以外への推論規則の適用
  - exchange規則を使うことで，適用させたい式を左端あるいは右端に移動させることができる.
  - どの位置の論理式に対しても，contraction, weakening, 論理結合に関する推論規則を適用することができる.

- 補題（lemma）
  - $S_1, S_2, \ldots, S_n$ からLKの推論規則を使ってSを推論することができるとき，下記は補題としてLKの証明において用いることができる.

$$\frac{S_1 \quad S_2 \quad \ldots \quad S_n}{S}$$

- 補題の例

$$\frac{\Gamma \vdash \Delta_1, A, B, \Delta_2}{\Gamma \vdash \Delta_1, A \vee B, \Delta_2} \qquad \frac{\Gamma_1, A, \Gamma_2 \vdash \Delta \qquad \Gamma_1, B, \Gamma_2 \vdash \Delta}{\Gamma_1, A \vee B, \Gamma_2 \vdash \Delta}$$

練習問題

- 次の命題を証明しなさい.
  - $A \to (B \to A)$
  - $\bigl(A \to (B \to C)\bigr) \to \bigl((A \to B) \to (A \to C)\bigr)$
  - $(A \to B) \to \bigl((B \to C) \to (A \to C)\bigr)$
  - $(A \to C) \to \bigl((B \to C) \to (A \lor B \to C)\bigr)$
  - $(A \to B) \to \bigl((A \to \neg B) \to \neg A\bigr)$
  - $(A \land B) \land C \to A \land (B \land C)$
  - $(A \lor B) \lor C \to A \lor (B \lor C)$
  - $\neg(A \land B) \to (\neg A \lor \neg B)$
  - $(\neg A \lor \neg B) \to \neg(A \land B)$
  - $(A \to B) \to (\neg B \to \neg A)$
  - $(\neg B \to \neg A) \to (A \to B)$

ボトムアップとトップダウンの証明

- ボトムアップ証明
  - 正しいと証明された式からはじめて，目的の式まで推論規則を適用していく.
  - 始式から始める通常の証明.
  - 途中段階も，すべて証明.
- トップダウン証明
  - 終式から始めて，その式に至る推論規則を探す.
  - 最終的に始式に到達すると証明が完成する.
  - 途中段階では補題でしかない.

$$\dfrac{\dfrac{}{A \vdash A}\,(\mathrm{I}) \qquad \dfrac{}{B \to C \vdash B \to C}\,(\mathrm{I})}{A \to (B \to C), A \vdash B \to C}\,(\to\mathrm{L})$$

$$\dfrac{\dfrac{}{B \vdash B}\,(\mathrm{I}) \qquad \dfrac{}{C \vdash C}\,(\mathrm{I})}{B \to C, B \vdash C}\,(\to\mathrm{L})$$

ボトムアップ

$$\dfrac{\dfrac{\dfrac{A, A \to B, A \to (B \to C) \vdash C}{A \to B, A \to (B \to C) \vdash A \to C}\,(\to\mathrm{R})}{A \to (B \to C) \vdash (A \to B) \to (A \to C)}\,(\to\mathrm{R})}{\vdash \big(A \to (B \to C)\big) \to \big((A \to B) \to (A \to C)\big)}\,(\to\mathrm{R})$$

トップダウン

まとめ

- LK式
  - 構文的意味
  - トートロジー

- 推論
  - 補題