論理学
第4回「証明」

萩野　達也
hagino@sfc.keio.ac.jp

lecture URL

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

前回まで

- 命題
  - 真偽が決まっている文
  - 命題変数
  - 論理結合子（∧，∨，→，¬）
  - 論理式
  - 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

推論

- 真理値表を用いた命題の正しさの定義
  - 基本的な命題（命題変数）の真偽値から，命題の真偽を計算する.

- 推論
  - すでに正しいと分かっている命題から，別の正しい命題を導く
  - 推論規則を繰り返し用いて，前提となる命題から，命題導く
  - 「前提$B_1, . . . , B_n$からAが推論される」

- 推論規則（inference rule）
  - 正しい命題から正しい命題を導く規則

- 例
  - A と$A \rightarrow B$ からB を導く
  - モーダスポネンス（modus ponens）
  - 三段論法（syllogism）とも呼ばれる
  - 「人間は死すべきもの」であり「ソクラテスは人間である」，ゆえに「ソクラテスは死すべきもの」である.

公理と定理

- 公理(axiom)
  - 正しいと考える前提
  - 「異なった2点を通る直線はただ一つ存在する」
  - 「平行線は交わらない」

- 定理(theorem)
  - 公理から推論規則を使って得られた命題
  - 定理を導く推論の過程を証明(proof)という
  - 「3 角形の内角の和は180 度である」
  - 「ピタゴラスの定理」

形式論理体系

- 扱っている論理学を形式的に扱う体系
  - 論理式の構文や操作に関する体系
  - 公理と推論規則からなる

- 古典命題論理(classical propositional logic)の形式体系
  - ヒルベルト(Hilbert)の体系
    - 公理中心で推論規則はモーダスポネンスだけ
  - ゲンツェン(Gentzen)の自然演繹(natural deduction)の体系
    - 日常の推論に近いもの
    - NK体系
  - ゲンツェンのsequent計算の体系
    - 形式的な表現にすぐれている
    - LK体系

LKの式

- LK 体系では次の式(sequent)を用いる

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

- 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」

- 「 ⊢ 」の読み方
  - ターンスタイル(turnstyle, 回転扉)
  - ティー(tee)

- $A_1, \dots, A_m \vdash B_1, \dots, B_n$
  - 「$A_1, \dots, A_m$」前件(antecedent)
  - 「$B_1, \dots, B_n$」後件(succedent)
  - 「前件から後件が導かれる」

式の特別な場合

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

- mやnは0でもかまわない
  - $\vdash B_1, \ldots, B_n$
    - 仮定は必要なく「B_1からB_nのどれかが導かれる」
  - $\vdash B$
    - 「Bが導かれる」
  - $A_1, \ldots, A_m \vdash$
    - 導かれるものがないので，「A_1からA_mを仮定すると矛盾する」
    - 「A_1からA_mのすべてを仮定してはいけない」
  - $A \vdash$
    - 「Aから導かれるものはない」
    - 「Aではない」
  - $\vdash$
    - 仮定は必要がないのに，導くものがない
    - 「矛盾している」

LKの推論規則

$$\frac{A, A, \Gamma \vdash \Delta}{A, \Gamma \vdash \Delta}\ (\mathrm{CL})$$

前提の式

推論規則の名前

結論の式

- 前提(premise)の式から，結論(conclusion)の式を得る
  - A は論理式
  - Γ, Δ は論理式の列
    - 空でも構わない

- 例

$$\frac{A, A, B, C \vdash D}{A, B, C \vdash D}\ (\mathrm{CL}) \qquad \frac{A, A \vdash A \wedge B}{A \vdash A \wedge B}\ (\mathrm{CL}) \qquad \frac{A \vee B, A \vee B \vdash A \wedge B}{A \vee B \vdash A \wedge B}\ (\mathrm{CL})$$

$$\frac{p \to q \vee r, p \to q \vee r, p \wedge s \vdash s \to t}{p \to q \vee r, p \to q \vdash s \to t}\ (\mathrm{CL})$$

LKの公理と推論規則

- 公理：始式（initial sequent）と定数

$$\frac{}{A \vdash A}\ (\mathrm{I}) \qquad \frac{}{\vdash \top}\ (\top) \qquad \frac{}{\bot \vdash}\ (\bot)$$

- 構造に関する推論規則：weakening, contraction, exchange, cut

$$\frac{\Gamma \vdash \Delta}{A, \Gamma \vdash \Delta}\ (\mathrm{WL}) \qquad \frac{\Gamma \vdash \Delta}{\Gamma \vdash \Delta, A}\ (\mathrm{WR})$$

$$\frac{A, A, \Gamma \vdash \Delta}{A, \Gamma \vdash \Delta}\ (\mathrm{CL}) \qquad \frac{\Gamma \vdash \Delta, A, A}{\Gamma \vdash \Delta, A}\ (\mathrm{CR})$$

$$\frac{\Gamma_1, A, B, \Gamma_2 \vdash \Delta}{\Gamma_1, B, A, \Gamma_2 \vdash \Delta}\ (\mathrm{EL}) \qquad \frac{\Gamma \vdash \Delta_1, A, B, \Delta_2}{\Gamma \vdash \Delta_1, B, A, \Delta_2}\ (\mathrm{ER})$$

$$\frac{\Gamma_1 \vdash \Delta_1, A \qquad A, \Gamma_2 \vdash \Delta_2}{\Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2}\ (\mathrm{Cut})$$

（ここでΓ, Δは論理式の列）

推論規則（つづき）

- 論理結合子に関する**推論規則**

$$\frac{A, \Gamma \vdash \Delta}{A \wedge B, \Gamma \vdash \Delta} \ (\wedge \mathrm{L}_1)$$

$$\frac{\Gamma \vdash \Delta, A}{\Gamma \vdash \Delta, A \vee B} \ (\vee \mathrm{R}_1)$$

$$\frac{B, \Gamma \vdash \Delta}{A \wedge B, \Gamma \vdash \Delta} \ (\wedge \mathrm{L}_2)$$

$$\frac{\Gamma \vdash \Delta, B}{\Gamma \vdash \Delta, A \vee B} \ (\vee \mathrm{R}_2)$$

$$\frac{A, \Gamma_1 \vdash \Delta_1 \quad B, \Gamma_2 \vdash \Delta_2}{A \vee B, \Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2} \ (\vee \mathrm{L})$$

$$\frac{\Gamma_1 \vdash \Delta_1, A \quad \Gamma_2 \vdash \Delta_2, B}{\Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2, A \wedge B} \ (\wedge \mathrm{R})$$

$$\frac{\Gamma_1 \vdash \Delta_1, A \quad B, \Gamma_2 \vdash \Delta_2}{A \to B, \Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2} \ (\to \mathrm{L})$$

$$\frac{A, \Gamma \vdash \Delta, B}{\Gamma \vdash \Delta, A \to B} \ (\to \mathrm{R})$$

$$\frac{\Gamma \vdash \Delta, A}{\neg A, \Gamma \vdash \Delta} \ (\neg \mathrm{L})$$

$$\frac{A, \Gamma \vdash \Delta}{\Gamma \vdash \Delta, \neg A} \ (\neg \mathrm{R})$$

LKの公理

$$\frac{}{A \vdash A}\,(\mathrm{I})$$

- 意味
  - 「A から A を導くことができる」

- LKでは公理は実質一つだけ
  - A は任意の論理式なので，実際には無数にある
  - A が任意なので， A を実際の論理式に当てはめる必要がある

- 例

$$\frac{}{p \vdash p}\,(\mathrm{I}) \qquad \frac{}{p \land q \vdash p \land q}\,(\mathrm{I}) \qquad \frac{}{p \to q \lor r \vdash p \to q \lor r}\,(\mathrm{I})$$

$$\frac{}{A \lor B \vdash A \lor B}\,(\mathrm{I})$$

LKの定数に関する公理

$$\cfrac{}{\vdash \top}\ (\top) \qquad \cfrac{}{\bot \vdash}\ (\bot)$$

- 意味
  - 「真を導くことができる」
  - 「偽からは何も導くことはできない」

Weakening, Contraction, Exchange推論規則

$$\frac{\Gamma \vdash \Delta}{A, \Gamma \vdash \Delta}\ (\mathrm{WL}) \qquad \frac{\Gamma \vdash \Delta}{\Gamma \vdash \Delta, A}\ (\mathrm{WR})$$

- weakening
  - 前件や後件に任意の論理式を付け加えても構わない

$$\frac{A, A, \Gamma \vdash \Delta}{A, \Gamma \vdash \Delta}\ (\mathrm{CL}) \qquad \frac{\Gamma \vdash \Delta, A, A}{\Gamma \vdash \Delta, A}\ (\mathrm{CR})$$

- contraction
  - 同じ論理式は1つに縮約することができる

$$\frac{\Gamma_1, A, B, \Gamma_2 \vdash \Delta}{\Gamma_1, B, A, \Gamma_2 \vdash \Delta}\ (\mathrm{EL}) \qquad \frac{\Gamma \vdash \Delta_1, A, B, \Delta_2}{\Gamma \vdash \Delta_1, B, A, \Delta_2}\ (\mathrm{ER})$$

- exchange
  - 前件内あるいは後件内の論理式の順序を入れ替えても構わない

Cut推論規則

$$\frac{\Gamma_1 \vdash \Delta_1, A \qquad A, \Gamma_2 \vdash \Delta_2}{\Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2}\ (\mathrm{Cut})$$

- cut
  - A を後件に持つ式と，A を前件に持つ式から，A を切り離した式を推論する
  - $\Gamma_2 \vdash \Delta_2$ を直接示すことが難しい
    - A を別に示しておいて
    - $A, \Gamma_2 \vdash \Delta_2$ を推論する

左と右の推論規則

- 規則の結論部分に論理結合子がある

$$\frac{A, \Gamma \vdash \Delta}{A \land B, \Gamma \vdash \Delta}\ (\land L_1)$$

$$\frac{B, \Gamma \vdash \Delta}{A \land B, \Gamma \vdash \Delta}\ (\land L_2)$$

$$\frac{A, \Gamma_1 \vdash \Delta_1 \quad B, \Gamma_2 \vdash \Delta_2}{A \lor B, \Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2}\ (\lor L)$$

$$\frac{\Gamma_1 \vdash \Delta_1, A \quad B, \Gamma_2 \vdash \Delta_2}{A \to B, \Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2}\ (\to L)$$

$$\frac{\Gamma \vdash \Delta, A}{\neg A, \Gamma \vdash \Delta}\ (\neg L)$$

$$\frac{\Gamma \vdash \Delta, A}{\Gamma \vdash \Delta, A \lor B}\ (\lor R_1)$$

$$\frac{\Gamma \vdash \Delta, B}{\Gamma \vdash \Delta, A \lor B}\ (\lor R_2)$$

$$\frac{\Gamma_1 \vdash \Delta_1, A \quad \Gamma_2 \vdash \Delta_2, B}{\Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2, A \land B}\ (\land R)$$

$$\frac{A, \Gamma \vdash \Delta, B}{\Gamma \vdash \Delta, A \to B}\ (\to R)$$

$$\frac{A, \Gamma \vdash \Delta}{\Gamma \vdash \Delta, \neg A}\ (\neg R)$$

左：前件に論理結合子

右：後件に論理結合子

「∧」の推論規則

$$\frac{A, \Gamma \vdash \Delta}{A \land B, \Gamma \vdash \Delta}\,(\land \mathrm{L}_1)$$

$$\frac{B, \Gamma \vdash \Delta}{A \land B, \Gamma \vdash \Delta}\,(\land \mathrm{L}_2)$$

$$\frac{\Gamma_1 \vdash \Delta_1, A \quad \Gamma_2 \vdash \Delta_2, B}{\Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2, A \land B}\,(\land \mathrm{R})$$

- 2つの左の規則（$\land \mathrm{L}_1$, $\land \mathrm{L}_2$）
  - 前件に「∧」を追加する
  - 「A を $A \land B$ にする」
  - 「B を $A \land B$ にする」

- 1つの右の規則（∧R）
  - 後件に「∧」を追加する
  - 「A と B をあわせて $A \land B$ にする」
  - 前提の2つの式から結論の式を推論する

「∨」の推論規則

$$\frac{A, \Gamma_1 \vdash \Delta_1 \quad B, \Gamma_2 \vdash \Delta_2}{A \vee B, \Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2}\ (\vee L)$$

$$\frac{\Gamma \vdash \Delta, A}{\Gamma \vdash \Delta, A \vee B}\ (\vee R_1)$$

$$\frac{\Gamma \vdash \Delta, B}{\Gamma \vdash \Delta, A \vee B}\ (\vee R_2)$$

- 1つの左の規則（∨L）
  - 前件に「∨」を追加する
  - 「A と B をあわせて $A \vee B$ にする」
  - 前提の2つの式から結論の式を推論する
- 2つの右の規則（$\vee R_1$, $\vee R_2$ ）
  - 後件に「∨」を追加する
  - 「A を $A \vee B$ にする」
  - 「B を $A \vee B$ にする」

「→」の推論規則

$$\frac{\Gamma_1 \vdash \Delta_1, A \quad B, \Gamma_2 \vdash \Delta_2}{A \to B, \Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2}\ (\to\mathrm{L}) \qquad \frac{A, \Gamma \vdash \Delta, B}{\Gamma \vdash \Delta, A \to B}\ (\to\mathrm{R})$$

- 1つの左の規則（→L）
  - 前件に「→」を追加する
  - 「後件の A と，前件の B をあわせて $A \to B$ にする」
  - 前提の2つの式から結論の式を推論する
- 1つの右の規則（→R）
  - 後件に「→」を追加する
  - 「前件の A と，後件の B をあわせて $A \to B$ にする」

「¬」の推論規則

$$\frac{\Gamma \vdash \Delta, A}{\neg A, \Gamma \vdash \Delta}\ (\neg\mathrm{L}) \qquad \frac{A, \Gamma \vdash \Delta}{\Gamma \vdash \Delta, \neg A}\ (\neg\mathrm{R})$$

- 1つの左の規則（¬L）
  - 前件に「¬」を追加する
  - 「後件の A を前件の $\neg A$ にする」

- 1つの右の規則（¬R）
  - 後件に「¬」を追加する
  - 「前件の A を後件の $\neg A$ にする」

LKの証明図

- LK の証明図（proof figure）
  - 始式から出発し，推論規則を次々に適用していく過程を記述したもの
  - 証明図の一番下にある式を，その証明図の終式（end sequent）という.

- 例: 証明図

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{A \vdash A}\,(\mathrm{I})}{\vdash A, \neg A}\,(\neg\mathrm{R})}{\vdash A, A \vee \neg A}\,(\vee\mathrm{R}_2)}{\vdash A \vee \neg A, A}\,(\mathrm{ER})}{\vdash A \vee \neg A, A \vee \neg A}\,(\vee\mathrm{R}_1)}{\vdash A \vee \neg A}\,(\mathrm{CR})$$

終式

- S を終式とする証明図が存在する時，S はLKで証明可能である（provable）という.

練習問題

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

まとめ

- 推論
  - 公理
  - 定理

- LK体系
  - 始式
  - LK推論規則

- 証明
  - 証明図