ソフトウェアモデル論（2012年度）
第11回・2012/12/07

桑原 寛明
情報理工学部 情報システム学科

連絡事項

- 次回（12/14）は休講です
- 補講を 12/22（土） に行う予定です

証明系 （復習）

- 論理式が論理式集合の論理的帰結であることを、論理式（の列）に対する機械的な操作のみによって調べる方法
  - 論理式の意味（真理値）を考えない
  - 判定アルゴリズムの一種とみなしてもよい
- 証明系は、論理式（の集合）から別の論理式を導出する推論規則の集合として定義される

シークエント （復習）

- $P_1, \ldots, P_n \vdash Q$
- 論理式集合 $\{ P_1, \ldots, P_n \}$ から推論を開始し、論理式 Q が得られることを表す
  - $\{ P_1, \ldots, P_n \}$: 前提、前件
  - Q : 結論、後件
- 推論を繰り返す（推論規則を繰り返し適用する）過程が証明

推論規則の形式 （復習）

$$\frac{\text{前提1} \quad \ldots \quad \text{前提n}}{\text{結論}}\ \text{規則名}$$

- 各前提と結論は論理式
- 前提1から前提nまでのn個の論理式から結論の論理式を推論（導出）する

$$\frac{P \quad Q}{P \wedge Q}\wedge\mathrm{i}$$

論理式 P と Q から論理式 P∧Q を推論（導出）してよい

自然演繹 （復習）

- 以下の推論規則からなる証明系

$$\frac{P \quad Q}{P \wedge Q}\wedge\mathrm{i} \qquad \frac{P \wedge Q}{P}\wedge\mathrm{e}_1 \qquad \frac{P \wedge Q}{Q}\wedge\mathrm{e}_2 \qquad \frac{P}{P \vee Q}\vee\mathrm{i}_1 \qquad \frac{Q}{P \vee Q}\vee\mathrm{i}_2$$

$$\frac{P \quad P \to Q}{Q}\to\mathrm{e} \qquad \frac{\neg\neg P}{P}\neg\neg\mathrm{e} \qquad \frac{\bot}{P}\bot\mathrm{e} \qquad \frac{P \quad \neg P}{\bot}\neg\mathrm{e}$$

$$\frac{\begin{array}{c}[P]\\ \vdots \\ Q\end{array}}{P \to Q}\to\mathrm{i} \qquad \frac{P \vee Q \quad \begin{array}{c}[P]\\ \vdots \\ R\end{array} \quad \begin{array}{c}[Q]\\ \vdots \\ R\end{array}}{R}\vee\mathrm{e} \qquad \frac{\begin{array}{c}[P]\\ \vdots \\ \bot\end{array}}{\neg P}\neg\mathrm{i}$$

p∧q→r⊢p→(q→r) の証明 （復習）

$$\dfrac{\dfrac{\dfrac{\dfrac{[p]_1 \quad [q]_2}{p \wedge q}\,\wedge\mathrm{i} \qquad p \wedge q \to r}{r}\,\to\mathrm{e}}{q \to r}\,\to\mathrm{i},2}{p \to (q \to r)}\,\to\mathrm{i},1$$

正しい証明木 （復習）

- 木構造の節点は論理式
  - 根が結論
  - 葉が前提
    - 前提が集合の場合、各要素が一回以上出現する
    - 前提に含まれない葉は仮定なので [] で囲まれる
      - [] で囲む規則（→i など）がどこかで使用される
- 葉を除く各節点は、子節点にいずれかの推論規則を適用して得られる論理式
  - 適用した推論規則を記す

派生規則

- 他の推論規則を使って導出可能な推論規則
  - 証明済みの派生規則は推論規則の一つとして使ってよい
- 例えば
  - ¬¬i
  - MT（modus tollens: 後件否定）
  - PBC（proof by contradiction: 背理法）
  - LEM（law of excluded middle: 排中律）

¬¬i の導出

- P⊢¬¬Pは ¬¬i ではなく別の推論規則を使って以下のように導出可能

$$\dfrac{\dfrac{P \quad [\neg P]}{\bot}\,\neg\mathrm{e}}{\neg\neg P}\,\neg\mathrm{i}$$

MT

$$\dfrac{P \to Q \quad \neg Q}{\neg P}\,\mathrm{MT}$$

- 証明

$$\dfrac{\dfrac{\dfrac{[P] \quad P \to Q}{Q}\,\to\mathrm{e} \qquad \neg Q}{\bot}\,\neg\mathrm{e}}{\neg P}\,\neg\mathrm{i}$$

PBC

$$\dfrac{\begin{array}{c}[\neg P]\\ \vdots\\ \bot\end{array}}{P}\,\mathrm{PBC}$$

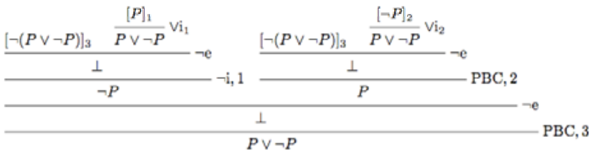
- 証明

$$\dfrac{\dfrac{\begin{array}{c}[\neg P]\\ \vdots\\ \bot\end{array}}{\neg\neg P}\,\neg\mathrm{i}}{P}\,\neg\neg\mathrm{e}$$

LEM

$$\frac{}{P \vee \neg P}\ \mathrm{LEM}$$

- 証明



矛盾

- 論理式集合 Φ から ⊥ が導出できる場合、Φ は矛盾
  - $\Phi \vdash \bot$
  - 任意の解釈について、Φ に含まれるすべての論理式が真にならない
    - モデルが存在しない
- 矛盾でない場合、無矛盾

矛盾の性質

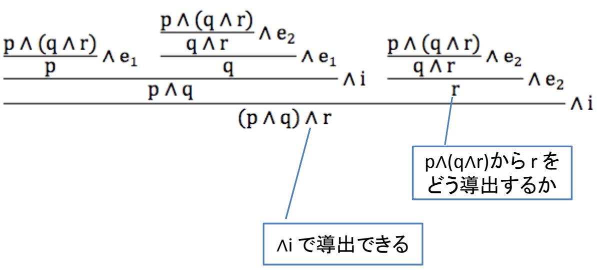
- Φ は矛盾
- 任意の論理式 P に対して Φ⊢P
- Φ⊢P かつ Φ⊢¬P なる論理式 P が存在する

自然演繹による証明の戦略 (?)

- 前提に適用できる推論規則、結論を導出できる推論規則は何か
  - 除去規則で前提を分解、導入規則で結論を合成
- ∨式の導出
  - ∨i が使えないか、∨e が使えないか
  - ∨e にLEMを組み合わせられないか
  - PBCが使えないか
- 推論規則の適用に不足する式を仮定してみる
  - 例： ¬P に ¬e を適用するために P を仮定する

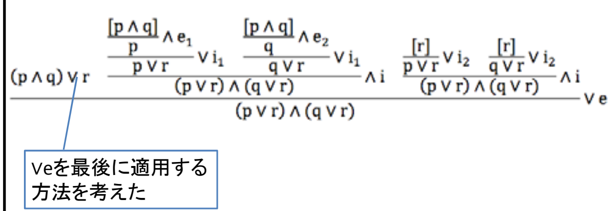
練習問題 5.21

1. p∧(q∧r) ⊢ (p∧q)∧r



練習問題 5.21

3. (p∧q)∨r ⊢ (p∨r)∧(q∨r)



※別証明もある

練習問題 5.21

7. p→q ⊢ ¬p∨q

$$\cfrac{\cfrac{}{p \vee \neg p}\,\mathrm{LEM} \qquad \cfrac{\cfrac{[p] \quad p \to q}{q} \to e}{\neg p \vee q} \vee i_2 \qquad \cfrac{[\neg p]}{\neg p \vee q} \vee i_1}{\neg p \vee q} \vee e$$

∨eとLEMの組み合わせ
p→qに→eを適用するためにp∨¬p

自然演繹の健全性

- 論理式集合 $P_1, \ldots, P_n$ から論理式 Q が導出できるならば Q は $P_1, \ldots, P_n$ の論理的帰結である
  - $P_1, \ldots, P_n \vdash Q$ ならば $P_1, \ldots, P_n \vDash Q$
- 健全でない場合、導出できたことを信じてよいかわからない
  - 導出できても論理的帰結でないことがある
  - ⇒ 導出アルゴリズムになっていない

健全性の証明

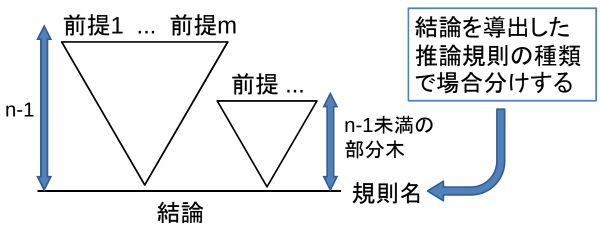
- $P_1, \ldots, P_n \vdash Q$ の証明木の高さに関する帰納法による
  - 高さが 1 の場合を示す
  - 高さが n 未満の場合に成り立つと仮定して n の場合を示す
    - 累積帰納法

基底段階

- 証明木の高さが 1 の場合
  - つまり、前提と結論が同じ場合
- これは命題変数 p に対して p⊢p の証明である
- 明らかに p⊨p である

帰納段階

- 証明木の高さが n 未満の場合に成り立つと仮定して n の場合を考える



∧i の場合

- 結論は $Q_1 \wedge Q_2$
- Q_1 と Q_2 の証明木が存在する
- つまり、論理式集合 Φ_1、Φ_2 が存在して $\Phi_1 \vdash Q_1$ および $\Phi_2 \vdash Q_2$
- Q_1 と Q_2 の証明木の高さはいずれも n 未満であるため、帰納法の仮定から $\Phi_1 \vDash Q_1$、$\Phi_2 \vDash Q_2$
- $\Phi = \Phi_1 \cup \Phi_2$ とすると $\Phi \vdash Q_1 \wedge Q_2$
- あとは $\Phi \vDash Q_1 \wedge Q_2$ を示せばよい

∧i の場合

- Φ に含まれるすべての論理式の真理値が真になるような任意の解釈 I（つまり Φ のモデル）
- $\Phi = \Phi_1 \cup \Phi_2$ ゆえ $\vDash_I \Phi_1$ かつ $\vDash_I \Phi_2$
- $\Phi_1 \vDash Q_1$ および $\Phi_2 \vDash Q_2$ ゆえ $I(Q_1) = I(Q_2) =$ 真
- よって $I(Q_1 \wedge Q_2) =$ 真
- つまり $\Phi \vdash Q_1 \wedge Q_2$ ならば $\Phi \vDash Q_1 \wedge Q_2$

証明系の無矛盾性

- 任意の論理式 P に対して、P あるいは ¬P のいずれか一方のみが証明できる
- 両方証明できる証明系は矛盾
- 自然演繹は無矛盾

自然演繹の完全性

- 論理式 Q が論理式集合 $P_1, \ldots, P_n$ の論理的帰結ならば $P_1, \ldots, P_n$ から Q が導出できる
  - $P_1, \ldots, P_n \vDash Q$ ならば $P_1, \ldots, P_n \vdash Q$
- 完全であれば、すべての論理的帰結を導出できる
  - 完全でない場合は導出できないものがある

完全性の証明

- 以下の順による

$$
\begin{aligned}
& P_1, \ldots, P_n \vDash Q \\
\Rightarrow\ & \vDash P_1 \rightarrow (P_2 \rightarrow (\ldots(P_n \rightarrow Q)\ldots)) \\
\Rightarrow\ & \vdash P_1 \rightarrow (P_2 \rightarrow (\ldots(P_n \rightarrow Q)\ldots)) \\
\Rightarrow\ & P_1, \ldots, P_n \vdash Q
\end{aligned}
$$

$P_1, \ldots, P_n \vDash Q \Rightarrow \vDash P_1 \rightarrow (P_2 \rightarrow (\ldots(P_n \rightarrow Q)\ldots))$

- 命題 5.6 による

$\vDash P \Rightarrow \vdash P$

- $\vDash P$ の定義よりすべての解釈のもとで P は真
  - P が n 種類の命題変数を含むとすると解釈は 2^n 通りあり、すべての場合で P は真
- P に含まれるすべての命題変数 p_i について $I(p_i)$ が真の場合と偽の場合がある
- $\hat{p}_i$ を $I(p_i)$ が真の場合 p_i、偽の場合 $\neg p_i$ とし、$\Phi = \{\hat{p}_1, \ldots, \hat{p}_n\}$ とすると Φ は 2^n 通り
- 補題5.32より 2^n 通りのすべての Φ について $\Phi \vdash P$
- 排中律と ∨e より $\hat{p}_1, \ldots, \hat{p}_{n-1} \vdash P$
- 以下、繰り返し

補題5.32

- 論理式 P
  - P は命題変数 $p_1,\ldots,p_m,q_1,\ldots,q_n$ を含む
- 解釈 I
  - すべての i について $I(p_i)$ = true かつ $I(q_i)$ = false
- この時、論理式集合 $\Phi = \{p_1,\ldots p_m,\neg q_1,\ldots,\neg q_m\}$（I がモデルとなるように Φ を決める）とすると

1. I(P) = true ならば $\Phi \vdash P$
2. I(P) = false ならば $\Phi \vdash \neg P$

補題5.32の証明

- 論理式 P の構造に関する帰納法による
- 基底段階

  P = p の場合
  - I(P) = true ならば、$\Phi = \{p\}$ ゆえ明らかに $p \vdash p$
  - I(P) = false ならば、$\Phi = \{\neg p\}$ ゆえ明らかに $\neg p \vdash \neg p$
- 帰納段階

  $P = \neg Q$　　$P = Q_1 \land Q_2$

  $P = Q_1 \lor Q_2$　　$P = Q_1 \to Q_2$

$P = \neg Q$ の場合

- I(P) = true ならば
  - 否定の意味より I(Q) = false
  - 論理式 Q に含まれる命題変数の集合を Φ とする
  - 帰納法の仮定より $\Phi \vdash \neg Q$ ゆえ $\Phi \vdash P$
- I(P) = false ならば
  - 否定の意味より I(Q) = true
  - 論理式 Q に含まれる命題変数の集合を Φ とする
  - 帰納法の仮定より $\Phi \vdash Q$
  - $\neg\neg$i より $\Phi \vdash \neg\neg Q$ つまり $\Phi \vdash \neg P$

$P = Q_1 \land Q_2$ の場合

- P,Q_1,Q_2 に含まれる命題変数の集合をそれぞれ Φ,Ψ_1,Ψ_2 とする
  - 明らかに $\Phi = \Psi_1 \cup \Psi_2$
- I(P) = true ならば
  - 連言の意味から $I(Q_1) = I(Q_2)$ = true
  - 帰納法の仮定から $\Psi_1 \vdash Q_1$ かつ $\Psi_2 \vdash Q_2$ ゆえ $\Phi \vdash P$

$P = Q_1 \land Q_2$ の場合

- I(P) = false ならば
  - 連言の意味から $I(Q_1)$ と $I(Q_2)$ のいずれか一方あるいは両方が false
  - $I(Q_1)$ = false, $I(Q_2)$ = true の場合
    - 帰納法の仮定より $\Psi_1 \vdash \neg Q_1$ かつ $\Psi_2 \vdash Q_2$ ゆえ $\Phi \vdash \neg Q_1 \land Q_2$
    - $\neg Q_1 \land Q_2 \vdash \neg(Q_1 \land Q_2)$ を示せばよい
  - $I(Q_1)$ = true, $I(Q_2)$ = false の場合も同様
  - $I(Q_1)$ = false, $I(Q_2)$ = false の場合も同様で、$\neg Q_1 \land \neg Q_2 \vdash \neg(Q_1 \land Q_2)$ を示せばよい

$\vdash P_1 \to (P_2 \to (\ldots(P_n \to Q)\ldots)) \Rightarrow P_1, \ldots, P_n \vdash Q$

- $\vdash P_1 \to (P_2 \to (\ldots(P_n \to Q)\ldots))$ なので P_1 を前提とすれば $\to$e 規則より $P_1 \vdash (P_2 \to (\ldots(P_n \to Q)\ldots))$
- 以下同様

モデル検査

モデル検査

- 状態遷移系として記述されたシステムが、論理式として記述された性質を満たすか否か、網羅的かつ機械的に検証する手法
- 利点
  - 網羅的、機械的、反例
- 例えば、プログラムが必ず停止すること、デッドロックしないこと、などを検証できる