ソフトウェアモデル論（2010年度）
第11回・2010/12/06

桑原 寛明
情報理工学部 情報システム学科

証明系

- 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

シークェント

- $P_1, \ldots, P_n \vdash Q$
- 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

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

- 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

- 以下の推論規則からなる証明系

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

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

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

p∧q⊢q∧p の証明

$$\dfrac{\dfrac{p \wedge q}{q}\wedge\mathrm{e}_2 \qquad \dfrac{p \wedge q}{p}\wedge\mathrm{e}_1}{q \wedge p}\wedge\mathrm{i}$$

p∧q→r⊢p→(q→r) の証明

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

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）

MT

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

- 証明

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

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

$$\dfrac{}{P \vee \neg P}\,\mathrm{LEM}$$

- 証明

$$\dfrac{\dfrac{\dfrac{\dfrac{[\neg(P\vee\neg P)]_3 \quad \dfrac{[P]_1}{P\vee\neg P}\vee\mathrm{i}_1}{\bot}\neg\mathrm{e}}{\neg P}\neg\mathrm{i},1 \qquad \dfrac{\dfrac{[\neg(P\vee\neg P)]_3 \quad \dfrac{[\neg P]_2}{P\vee\neg P}\vee\mathrm{i}_2}{\bot}\neg\mathrm{e}}{P}\mathrm{PBC},2}{\bot}\neg\mathrm{e}}{P\vee\neg P}\mathrm{PBC},3$$

証明の例：演習問題 5.22 (1)

$$\dfrac{p \vee q \qquad \dfrac{\dfrac{[p] \quad \neg p}{\bot}\neg\mathrm{e}}{q}\bot\mathrm{e} \qquad [q]}{q}\vee\mathrm{e}$$

証明の例：演習問題 5.22 (2)

$$\dfrac{\dfrac{[\neg p] \quad \neg p \to p}{\to e}}{\dfrac{[\neg p] \quad p}{\neg e}}\ \dfrac{\dfrac{\bot}{p}\ PBC}{}$$

自然演繹の健全性

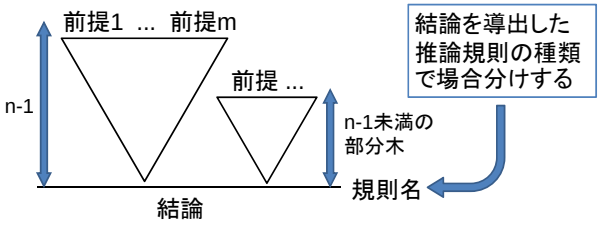
- 論理式集合 $P_1, \ldots, P_n$ から論理式 Q が導出できるならば Q は $P_1, \ldots, P_n$ の論理的帰結である
  - $P_1, \ldots, P_n \vdash Q$ ならば $P_1, \ldots, P_n \models Q$
- 証明は $P_1, \ldots, P_n \vdash Q$ の証明木の高さに関する帰納法による
  - 高さが 1 の場合を示す
  - 高さが n 未満の場合に成り立つと仮定して n の場合を示す

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 $p \vdash p$ の証明である
- 明らかに $p \models p$ 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 $\Phi_1 \models Q_1$、$\Phi_2 \models Q_2$
- $\Phi = \Phi_1 \cup \Phi_2$ とすると $\Phi \vdash Q_1 \wedge Q_2$
- あとは $\Phi \models Q_1 \wedge Q_2$ 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
- 論理的帰結の定義から $I(Q_1) = I(Q_2) = 真$
- よって $I(Q_1 \wedge Q_2) = 真$
- つまり $\Phi \vdash Q_1 \wedge Q_2$ ならば $\Phi \models Q_1 \wedge Q_2$

自然演繹の無矛盾性

- 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

自然演繹の完全性

- 論理式 Q が論理式集合 $P_1, ..., P_n$ の論理的帰結ならば $P_1, ..., P_n$ から Q が導出できる
  - $P_1, ..., P_n \models Q$ ならば $P_1, ..., P_n \vdash Q$
- 証明は以下の順

  $P_1, ..., P_n \models Q$
  $\Rightarrow \models P_1 \rightarrow (P_2 \rightarrow (...(P_n \rightarrow Q)...))$
  $\Rightarrow \vdash P_1 \rightarrow (P_2 \rightarrow (...(P_n \rightarrow Q)...))$
  $\Rightarrow P_1, ..., P_n \vdash Q$

$P_1, ..., P_n \models Q \Rightarrow \models P_1 \rightarrow (P_2 \rightarrow (...(P_n \rightarrow Q)...))$

- 命題 5.6 による

$\models P \Rightarrow \vdash P$

- $\models P$ 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、$\Phi = \{\hat{p}_1, ..., \hat{p}_n\}$ 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 Ve より $\hat{p}_1, ..., \hat{p}_{n-1} \vdash P$
- 以下、繰り返し

$\vdash P_1 \rightarrow (P_2 \rightarrow (...(P_n \rightarrow Q)...)) \Rightarrow P_1, ..., P_n \vdash Q$

- $\vdash P_1 \rightarrow (P_2 \rightarrow (...(P_n \rightarrow Q)...))$ なので P_1 を前提とすれば →e 規則より $P_1 \vdash (P_2 \rightarrow (...(P_n \rightarrow Q)...))$
- 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

モデル検査の手順

- 検査対象のシステムを状態遷移系を用いて記述する
  - 対象はプログラムや設計など
    - 「動作する」ものであれば何でも対象になる
  - 状態遷移系としてはKripke構造やオートマトンなど
- 検査したい性質を論理式を用いて記述する
  - 時相論理や様相論理を用いる
- 検査アルゴリズムを実行する
  - アルゴリズムを実装した様々なツールがある

Kripke構造

- 状態遷移系の一種
- 直観的には
  - オートマトンから記号を除去
  - オートマトンの各状態にその状態で真になる命題を追加
    - 「x の値は 1 である」など
    - 命題は命題論理の範囲内で

Kripke構造の定義

- Kripke構造 M = (S, R, L)
  - S : 状態の有限集合
  - R : 遷移関係
    - $R \subseteq S \times S$
    - R(s, s') : 状態 s から s' への遷移がある
  - L : ラベル付け関数
    - $L : S \rightarrow 2^{PV}$
    - PV は命題変数の集合
    - 各状態にその状態で真となる命題を表す命題変数を割り当てる関数