ソフトウェアモデル論（2011年度）
第10回・2011/12/09

桑原 寛明
情報理工学部 情報システム学科

連絡事項

- 補講します
  - 12/10（土）（明日）
  - 13:00-14:30
  - F203

命題 （復習）

- 内容の真偽が確定できる文
  - 加算はチューリング機械計算可能である
  - 1と10は等しい
  - 情報理工学部の学生数は2139人である
- 命題同士が関連することもある
  - 風が吹く
  - 風が吹くと桶屋が儲かる
  - ⇒ 桶屋が儲かる

論理学 （復習）

- 命題の集まりについて、ある命題の真偽が他の命題の真偽にどのように影響するか、命題間の関連を系統的に調べる学問
- 数理論理学
  - 数学における形式手法、記号的手法を用いて行う論理学

命題論理 （復習）

- 命題の真偽に関する論証を行う
- 以下のみに着目して論証
  - 最も基本的な命題の真偽
    - 真偽が他の命題の真偽に影響されない
  - 命題の組合せ構造
- 命題の具体的内容は無視
  - 記号列として表現

論理式 （復習）

- 命題を表す記号列

1. 命題変数は論理式である
2. P, Q が論理式であれば
   - (¬P) 否定、～でない
   - (P∧Q) 連言、かつ
   - (P∨Q) 選言、または
   - (P→Q) 含意、ならば

   は論理式である
1. 1. と 2. から作られるものだけが論理式である

意味論 （復習）

- 論理式の意味とは論理式の真理値
  - 真 or 偽
- 以下の2つから決まる
  - 命題変数の真理値
  - 論理演算子（¬、∧、∨、→）の意味

解釈 （復習）

- 命題変数の真理値を定義する関数
  - true : 真、false : 偽
- 解釈を I、命題変数の集合を Σ とすると
  I : Σ → { true, false }
- すべての p∈Σ に対して I(p) = true または
  I(p) = false

解釈の例 （復習）

- Σ = { p, q, r } とすると解釈は8通りあり得る

	p	q	r
I_1	true	true	true
I_2	true	true	false
I_3	true	false	true
I_4	true	false	false
I_5	false	true	true
I_6	false	true	false
I_7	false	false	true
I_8	false	false	false

論理演算子の意味 （復習）

- 真理値関数によって定義
  - 以下の Not, And, Or, Imp がそれぞれ否定、連言、選言、含意の意味を定義

P	Not(P)
true	false
false	true

P	Q	And(P,Q)	Or(P,Q)	Imp(P,Q)
true	true	true	true	true
true	false	false	true	false
false	true	false	true	true
false	false	false	false	true

論理式の意味 （復習）

- 命題変数の集合 Σ
- 解釈 I のもとでの論理式 P の真理値 $V_I(P)$
  - 解釈は命題変数の真理値を決める

$$V_I(P) = \begin{cases} I(p) & P \text{ が命題変数 } p \in \Sigma \text{ の場合} \\ \mathrm{Not}(V_I(Q)) & P \text{ が } \neg Q \text{ の場合} \\ \mathrm{And}(V_I(Q), V_I(R)) & P \text{ が } Q \wedge R \text{ の場合} \\ \mathrm{Or}(V_I(Q), V_I(R)) & P \text{ が } Q \vee R \text{ の場合} \\ \mathrm{Imp}(V_I(Q), V_I(R)) & P \text{ が } Q \rightarrow R \text{ の場合} \end{cases}$$

モデル （復習）

- 論理式集合 Φ
- 解釈 I
- I が Φ のモデルである
  iff
  Φ に含まれるすべての論理式 P∈Φ について
  I(P) = true
- $\models_I \Phi$ あるいは $I \models \Phi$ と書く

論理的帰結 （復習）

- 論理式集合 Φ
- 論理式 P
- P は Φ の論理的帰結である
  iff
  すべての解釈 I について、I が Φ のモデルならば I は P モデルでもある
- $\Phi \models P$ と書く

論理的帰結の判定 （復習）

- 論理式 P が論理式集合 Φ の論理的帰結であるか判定したい
- 手順？
  1. すべての解釈について Φ のモデルであるか調べる
  2. Φ のモデルであるすべての解釈のもとで P が真であるか調べる
- Φ と P に含まれる命題変数が n 種類ならば 2^n 通りの解釈について調べなければならない
  ⇒ 効率が悪い

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

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

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

論理式 P と Q から論理式 P∧Q を推論（導出）してよい

証明系の健全性

- 論理式集合 Φ から論理式 P が導出（証明）できるならば P は Φ の論理的帰結である
  - $\Phi \vdash P$ ならば $\Phi \models P$
- 証明系が健全でない場合、証明できたことを信じてよいかわからない
  - 証明できても論理的帰結でないことがある
  ⇒ 証明になっていない

証明系の完全性

- 論理式 P が論理式集合 Φ の論理的帰結ならば Φ から P を導出（証明）できる
  - Φ ⊨ P ならば Φ ⊢ P
- 証明系が完全であれば、すべての論理的帰結を証明できる
  - 完全でなければ証明できないものがある

自然演繹

- 以下の推論規則からなる証明系

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

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

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

連言に関する推論規則

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

- i
  - 演算子を導入
- e
  - 演算子を除去

p∧q⊢q∧p の証明

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

証明木（導出木）

- シークェントの前提から結論を推論する過程を木構造で図示したもの（ただし根が下）
- 木構造の節点は論理式
  - 葉が前提（すべての前提が一回以上出現）
  - 根が結論
- 葉を除く各節点は、子節点の論理式に推論規則を適用して得られる論理式

二重否定に関する推論規則

$$\frac{P}{\neg\neg P}\neg\neg\mathrm{i} \qquad \frac{\neg\neg P}{P}\neg\neg\mathrm{e}$$

- ¬¬i は他の規則を用いて導出できる（例5.20）
  - なくても大丈夫

含意に関する推論規則

$$\dfrac{\begin{array}{c}[P]\\ \vdots\\ Q\end{array}}{P \to Q} \to \mathrm{i} \qquad \dfrac{P \quad P \to Q}{Q} \to \mathrm{e}$$

- [P] は論理式 P の一時的な仮定を表す
  - 仮定は推論規則（この場合は→i）の適用で消費される
  - 仮定は証明木の葉に出現する

p→(q→r)⊢p∧q→r の証明

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

p∧q→r⊢p→(q→r) の証明

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

選言に関する推論規則

$$\dfrac{P}{P \vee Q} \vee \mathrm{i}_1 \qquad \dfrac{Q}{P \vee Q} \vee \mathrm{i}_2 \qquad \dfrac{P \vee Q \quad \begin{array}{c}[P]\\ \vdots\\ R\end{array} \quad \begin{array}{c}[Q]\\ \vdots\\ R\end{array}}{R} \vee \mathrm{e}$$

否定に関する推論規則

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

- ⊥ は矛盾を表す
- 矛盾からはどのようなことでも推論できる
- 矛盾が導出された場合は前提が間違っている

¬¬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

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

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

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

- 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

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