2007年度 情報数学
証明論入門

2007年7月6日
情報理工学科　上田 和紀

復習：議論（argument）の例

- If the train arrives late and there are no taxis at the station, then John is late for his meeting.
- John is not late for his meeting.
- The train did arrive late.
- *Therefore*, there were taxis at the station.

If *P* and not *Q*, then *R*.　Not *R*.　*P*.　*Therefore*, *Q*.

- これが議論として正当であることを形式的（機械的）に証明したい.

形式的証明とは

- 形式的証明とは，与えられた演繹体系（＝ 公理と推論規則の組）の下で，いくつかの前提 $A_1, ..., A_n$ から結論 B を機械的に導き出すこと.
  - 論理式の意味や内容には踏み込まない.
- 与えられた公理と推論規則の下で $A_1, ..., A_n$ から B を導き出せることを $A_1, ..., A_n \vdash B$ と書く.
- 公理の一例：$A_1, ..., A_n \vdash A_i \quad (i = 1, ..., n)$
  - 仮定したことは（当然）導いてよい

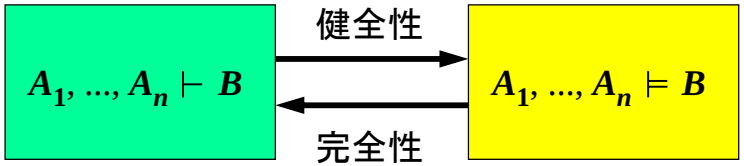
復習と比較：論理的帰結

- 論理式 $A_1, ..., A_n$ が真となるようなすべての付値／構造の下で B が真になるとき，論理式 B が論理式 $A_1, ..., A_n$ の論理的帰結であるといい，$A_1, ..., A_n \models B$ と書く.
- “論理的帰結”は，各論理式の内容（意味）に言及した概念
  - 証明の“正しさ”を論じるための道具立て
- 比較
  - A: A という命題自身
    - 解釈（真偽）は付値や構造によってきまる
  - $\models A$: A は恒真である
  - $\vdash A$: A が導ける

命題 A に関するメタレベルの主張

演繹体系の健全性と完全性

- ⊢ と ⊨ は違う概念だが深く関係している



（計算の世界）　　（意味の世界）

- 健全性(soundness，証明できたことは正しい）は，ないと使い物にならない
- 完全性(completeness，正しいことは証明できる）は，あると望ましい

復習：論理的帰結の証明

- If *P* and not *Q*, then *R*.　Not *R*.　*P*.　*Therefore*, *Q*. が正しい議論であることを示すいくつかの方法：
  - (1) 真理値表を作って確かめる
  - (2) 式変形によって，⊨ の左辺を ∧ でつなげたものが Q ∧ ... の形になることを確かめる
  - (3) 式変形によって，⊨ の左辺および ¬Q を ∧ でつなげたものが ⊥ になることを確かめる
- これらは，論理式を“意味の世界”に翻訳して議論の当否を確かめる方法である（cf. 三段論法）
  - 力ずくのやり方（brute-force method）
  - 一階述語論理では意味の世界に無限集合が出てくる

三段論法（modus ponens）

- *P* と *P* ⇒ *Q* から（機械的に）*Q* を導く
- “⇒”の直感的な意味にしたがった推論
  - 真理値表を見たり，*P* ⇒ *Q* を ¬ と ∨ を使って書き換えたりするよりも直截（ちょくせつ）的
- “⇒”以外の各演算子にも推論規則を与えてゆくと，演繹体系ができあがる
  - 代表的な演繹体系として自然演繹法 (natural deduction) とシーケント計算 (sequent calculus) とがある．情報系の学生が学ぶにはどちらにもそれぞれ利点があるが，本講義では後者を扱う．

シーケント（sequent）

- $A_1, ..., A_m \vdash B_1, ..., B_n$ の形（A_i, B_i は命題論理式または一階述語論理式）をシーケントという．
  - $n = 1$：前提 $A_1, ..., A_m$ から B_1 が導かれる（既出）
  - $n > 1$：前提 $A_1, ..., A_m$ から $B_1, ..., B_n$ のどれか一つ以上が導かれる
  - $n = 0$：前提 $A_1, ..., A_m$ から矛盾が導かれる
    - $A \vdash$ は「A ではない」と同じこと
  - $m = 0$：（前提なしに）$B_1, ..., B_n$ のどれかが導かれる
  - $m = n = 0$ ：（前提なしに）矛盾（が導かれる）
    - ⊢ （矛盾）が証明できるような体系は使えない．⊢ が証明できない体系は無矛盾であるという．

シーケント計算（sequent calculus）

- シーケントに関する演繹体系のこと
  1. 正当性が自明なシーケントを定義する
     cf. *P*. *Q*. ...(他の前提)... . Therefore, *Q*.
  2. 複雑なシーケントがどのような場合に成立するかを，より簡単なシーケントに還元して定義する
     cf. *P*. *Q*. ...(他の前提)... . Therefore, *R*.
     が正当な議論ならば
     P and *Q*. ...(他の前提)... . Therefore, *R*
     も正当な議論のはず
     - 前者の方が論理演算子が少ないという意味で簡単

命題論理のシーケント計算

- 【準備】シーケント $A_1, ..., A_m \vdash B_1, ..., B_n$ において，前提および結論の並びの順序は重要ではないはず．つまり，$A_1, ..., A_m$ と $B_1, ..., B_n$ はそれぞれ多重集合（マルチ集合，multiset）とみなしてよい．以下では，論理式の多重集合を $\Gamma, \Delta, \Pi, \Sigma$ などのギリシャ文字で表わす．A, Γ は多重集合 $\{A\}$ と多重集合 Γ との和を表わす．
  - 注：本講義の範囲（古典命題論理，古典一階述語論理）では，シーケントの前提と結論は通常の集合としてもよいが，別の論理体系（線形論理など）を考えるときのために，多重集合と考えておいたほうがよい．

命題論理のシーケント計算

- 公理と推論規則からなる．
  - 公理：前提なしに正しいと認めるシーケント．
    Initial sequent ともいう．具体的には

    $$A, \Gamma \vdash A, \Delta$$

    が initial sequent（A は任意の命題論理式）．
  - 推論規則：すでに正しいとわかっているシーケントから新たな正しいシーケントを得るための規則．

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

    の形をとる．

シーケント内部の“前提”や“結論”とは，レベルが一段異なることに注意！

命題論理のシーケント計算

- 推論規則（その１）

$$\frac{A, \Gamma \vdash \Delta}{\Gamma \vdash \Delta, \neg A}\ (\neg\text{右}) \qquad \frac{\Gamma \vdash \Delta, A}{\neg A, \Gamma \vdash \Delta}\ (\neg\text{左})$$

$$\frac{\Gamma \vdash \Delta, A \quad \Gamma \vdash \Delta, B}{\Gamma \vdash \Delta, A \wedge B}\ (\wedge\text{右}) \qquad \frac{A, B, \Gamma \vdash \Delta}{A \wedge B, \Gamma \vdash \Delta}\ (\wedge\text{左})$$

$$\frac{\Gamma \vdash \Delta, A, B}{\Gamma \vdash \Delta, A \vee B}\ (\vee\text{右}) \qquad \frac{A, \Gamma \vdash \Delta \quad B, \Gamma \vdash \Delta}{A \vee B, \Gamma \vdash \Delta}\ (\vee\text{左})$$

- 上から下に読むことも下から上に読むことも可能

命題論理のシーケント計算

- 推論規則（その２）

$$\frac{A, \Gamma \vdash \Delta, B}{\Gamma \vdash \Delta, A \Rightarrow B} (\Rightarrow 右)$$

$$\frac{\Gamma \vdash \Delta, A \quad B, \Gamma \vdash \Delta}{A \Rightarrow B, \Gamma \vdash \Delta} (\Rightarrow 左)$$

- 最後の規則“⇒左”は，三段論法の一般化
- 以上の（G. Gentzen による）演繹体系を LK と呼ぶことがある．
  - 注意：LK の定式化にはいくつかの流儀がある．

証明図

- 推論規則の適用過程を積み重ねて記述したものを証明図という．

例：

$$\frac{\dfrac{P \vdash Q, P \quad Q \vdash Q, P}{P \vee Q \vdash Q, P} (\vee 左)}{P \vee Q \vdash Q \vee P} (\vee 右)$$

- 証明図は木構造をなす．木の分岐係数はたかだか２である．木の葉はすべて initial sequent でなければならない．Initial sequent は単独でも証明図となる．

シーケント計算の健全性（soundness）

- 論理式 $A_1 \wedge \ldots \wedge A_m \Rightarrow B_1 \vee \ldots \vee B_n$ を，シーケント $A_1, \ldots, A_m \vdash B_1, \ldots, B_n$ に対応する論理式と呼ぶ．
- $A_1 \wedge \ldots \wedge A_m \Rightarrow B_1 \vee \ldots \vee B_n$ が恒真であるとき，そしてそのときに限り，シーケント $A_1, \ldots, A_m \vdash B_1, \ldots, B_n$ が正しいという．
- Initial sequent は正しい（ことが容易にわかる）
- 各推論規則の前提がすべて正しいシーケントならば，対応する結論も正しいシーケントである（こともちょっと頑張ればわかる）．
- したがって，証明できるシーケントは正しい．つまり体系 LK は健全（sound）である．

シーケント計算の完全性（completeness）

- 正しいシーケントはすべて証明可能か？
  - 答えは Yes, すなわち命題論理のシーケント計算の体系 LK は完全である．
- まず論理記号（¬, ∧, ∨, ⇒）をもたないシーケントを考えると，正しいシーケントは必ず initial sequent なので証明可能．
- 論理記号を含むシーケントは，シーケントの中に出てくる論理記号の個数に関する帰納法で考える．
  - １つの推論規則の上のシーケントは，下のシーケントより論理記号の個数が少なくとも１個少ない
  - １つの推論規則の下のシーケントが正しければ，上のシーケントもすべて正しい．
  - 帰納法の仮定から，上のシーケントはすべて証明可能で，それらから下のシーケントが推論できる

Wang のアルゴリズム

- シーケントの証明図は一番下（木の根）から上向きに作ってゆく．
- 証明図を１段上に伸ばすと論理記号が少なくとも１つ減るので，証明図の高さは有限．幅も有限．
- 証明図を１段上に伸ばす方法は複数ありうるが，結論が正しければ前提のシーケントもすべて正しい（ことは各推論規則を見て確かめることができる）．
- 前提のシーケントが正しければ，同様にして証明図を上に伸ばしてゆけば，すべての枝が最終的には initial sequent に到達するはず．
  - 上に伸ばす作業が行き詰まることはない

一階述語論理のシーケント

- シーケント $A_1, ..., A_m \vdash B_1, ..., B_n$ に出現する自由変数を $x_1, ..., x_k$ とする．
- 論理式が自由変数を含む場合，その値がわからない限り，論理式の真偽を決めることは一般にできない．
- しかしたとえば loves(X,Y) ⊢ loves(X,Y) は，X と Y の値が何であっても正しいと認めることができる．
- 以上の考察から，$A_1, ..., A_m \vdash B_1, ..., B_n$ が正しいとは，「$\forall x_1 ... \forall x_k\, (A_1 \wedge ... \wedge A_m \Rightarrow B_1 \vee ... \vee B_n)$ が恒真であること」と定義する．「 」内の論理式を，このシーケントに対応する論理式という．

一階述語論理のシーケント計算

- Initial sequent は命題論理のときと同じ
- ¬, ∧, ∨, ⇒ に関する規則も命題論理のときと同じ
- ∀, ∃ に関する規則と重ね合せ規則が追加される．まず

$$\frac{A, A, \Gamma \vdash \Delta}{A, \Gamma \vdash \Delta}\ (\text{重ね合せ左})$$

$$\frac{\Gamma \vdash \Delta, A, A}{\Gamma \vdash \Delta, A}\ (\text{重ね合せ右})$$

一階述語論理のシーケント計算

- ∀, ∃ に関する規則．$A[x]$ で，自由変数 x を含むかもしれない論理式 A を表し，$A[t]$ で，A 中の自由変数 x に項 t を代入したものを表す．

$$\frac{A[t], \Gamma \vdash \Delta}{\forall x(A[x]), \Gamma \vdash \Delta}\ (\forall\text{左}) \qquad \frac{\Gamma \vdash \Delta, A[a]}{\Gamma \vdash \Delta, \forall x(A[x])}\ (\forall\text{右})$$

$$\frac{A[a], \Gamma \vdash \Delta}{\exists x(A[x]), \Gamma \vdash \Delta}\ (\exists\text{左}) \qquad \frac{\Gamma \vdash \Delta, A[t]}{\Gamma \vdash \Delta, \exists x(A[x])}\ (\exists\text{右})$$

- t は任意の項
- a は Γ や Δ に現れない変数 (eigenvariable)

一階述語論理のシーケント計算

- Eigenvariable 条件の必要性

$$\frac{A[a], \Gamma \vdash \Delta}{\exists x(A[x]), \Gamma \vdash \Delta}\ (\exists 左) \qquad \frac{\Gamma \vdash \Delta, A[a]}{\Gamma \vdash \Delta, \forall x(A[x])}\ (\forall 右)$$

★ a は Γ や Δ に現れない変数 (eigenvariable)

$$\dfrac{\dfrac{p(A) \vdash p(A)}{p(A) \vdash \forall X(p(X))}\ (\forall 右) \leftarrow 誤り}{\exists X(p(X)) \vdash \forall X(p(X))}\ (\exists 左)$$

一階述語論理のシーケント計算

- 証明の例

$$\dfrac{\dfrac{p(1) \vdash p(1)}{\forall X(p(X)) \vdash p(1)}\ (\forall 左)}{\forall X(p(X)) \vdash \exists X(p(X))}\ (\exists 右)$$

$$\dfrac{\dfrac{\dfrac{\dfrac{p(A) \vdash p(A), q(A)}{\forall X(p(X)) \vdash p(A), q(A)}\ (\forall 左) \quad \dfrac{q(A) \vdash p(A), q(A)}{\forall X(q(X)) \vdash p(A), q(A)}\ (\forall 左)}{\forall X(p(X)) \vee \forall X(q(X)) \vdash p(A), q(A)}\ (\vee 左)}{\forall X(p(X)) \vee \forall X(q(X)) \vdash p(A) \vee q(A)}\ (\vee 右)}{\forall X(p(X)) \vee \forall X(q(X)) \vdash \forall X(p(X) \vee q(X))}\ (\forall 右)$$

一階述語論理のシーケント計算

- 重ね合せ規則を要する証明の例

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{p(0), p(s(0)) \vdash p(s(0)), p(s(s(0)))}{p(0), p(s(0)), p(s(0)) \Rightarrow p(s(s(0))) \vdash p(s(s(0)))}\ (右半分略)}{p(0), p(s(0)), \forall X(p(X) \Rightarrow p(s(X))) \vdash p(s(s(0)))}\ (左半分略)}{p(0), p(0) \Rightarrow p(s(0)), \forall X(p(X) \Rightarrow p(s(X))) \vdash p(s(s(0)))}}{p(0), \forall X(p(X) \Rightarrow p(s(X))), \forall X(p(X) \Rightarrow p(s(X))) \vdash p(s(s(0)))}}{p(0), \forall X(p(X) \Rightarrow p(s(X))) \vdash p(s(s(0)))}$$

健全性と完全性

- 一階述語論理のシーケント計算も，健全かつ完全
  - 完全性の証明は少々複雑なので省略
- しかし，与えられた一階述語論理のシーケントが LK によって証明できるか否かは決定不能.
  - cf. 命題論理式の場合は決定可能.