情報論理学
(第４回)

基礎工学部情報科学科　泉 泰介

命題論理の論理式(第2回より再掲)

- 命題論理の構成要素(記号集合)
  1. 命題記号の集合Π
  2. 論理記号→，¬
  3. 補助記号(,)

定義(命題論理)

Πに基づく論理式$L(\Pi)$とは，以下の条件のいずれかを満たすもの(=b.およびc.の操作の繰り返しで得られるもの)すべての集合

a. Π中の各記号$p \in \Pi$
b. 2つの論理式p, qに対する$(p) \to (q)$
c. 論理式pに対する$\neg(p)$

- 再帰的な定義になっていることに注意

意味論と自然演繹(第2回より再掲)

- 定義上論理式はただの記号の列
  - **そこに真とか偽とか，$P \to Q$の真理値表とか，そういう概念は存在しない**
  - 論理式を用いて実際に論理を議論するためには，論理式を何らかの形で操作したり，そこから別の(意味のある)論理式を帰結したりするような方法が必要になる

- 2つのアプローチが存在：**意味論 / 自然演繹**
  - 対立する概念ではない
  - 別のことをやろうとしているわけでもない(得手不得手はある)
  - が，実際に2つを勉強すると毛色は結構違う

今回と次回の内容

- 前回までは命題論理の意味論的なアプローチに基づいて議論
- 今回からは自然演繹的(記号処理的)アプローチについて説明
  - 論理式を記号処理的に取り扱う
  - 真理値ベースでの同値変形等に基づかない
- 最終的に2つのアプローチは等価であることが示される
- 2つのアプローチによる議論を混同しないように
  - 意味をとれば自明なことも，演繹的な証明では自明でないことがある(逆も然り)

Part1 ：命題論理の公理系と証明

命題論理の公理系S

- P, Q, Rを任意の論理式を表す変数とする．Sは以下の3つの公理(axiom) A1～A3と1つの推論規則B1から構成される
  - (A1) $P \to (Q \to P)$
  - (A2) $\big(P \to (Q \to R)\big) \to ((P \to Q) \to (P \to R))$
  - (A3) $(\neg P \to \neg Q) \to ((\neg P \to Q) \to P)$
  - (B1) 任意の論理式PとQに対して，Pと$P \to Q$からQを得る

- この公理系はヒルベルト流のシステムと呼ばれたりする
  - 公理系は「証明」を形式化するために役って立つ「基本パーツ」のようなものを定めており，何を基本と思うかによっていくつかの流儀がある

公理のインスタンス

- (A1) $P \to (Q \to P)$
- (A2) $(P \to (Q \to R)) \to ((P \to Q) \to (P \to R))$
- (A3) $(\neg P \to \neg Q) \to ((\neg P \to Q) \to P)$
- (B1) 任意の論理式PとQに対して，
  Pと$P \to Q$からQを得る

- 公理A1～A3の記号P, Q, Rを任意の論理式で置き換えたものを公理のインスタンス(instance)と呼ぶ
- 例：(A1) $P \to (Q \to P)$　に対してPへX，Qへ$Y \to Z$を代入
  - 得られるインスタンスは$X \to ((Y \to Z) \to X)$
- 元の公理と，それから得られるインスタンスを一緒くたにして公理と呼ぶこともある
  - そのとき，元の(A1)～(A3)を公理のスキーム(scheme)と呼んだりもする

(形式的)証明

- Γ：論理式の集合(仮定・仮説:Hypothesis)
- 各P_iが以下のいずれかに該当するような論理式の有限長系列$P_1, P_2, \ldots P_n = P$が存在するとき，公理系SにおいてPが導かれる(deduced)という
  1. P_iはΓに含まれる
  2. P_iはSの公理(のインスタンス)
  3. P_iはあるP_j, P_k $(j, k < i)$ からSの推論規則B1によって導かれる論理式
- このとき，系列$P_1, P_2, \ldots P_n$をΓからPの演繹(deduction)と呼ぶ
  - nはこの演繹の長さと呼ばれる

(形式的)証明

- 仮定ΓよりPを導くことが可能(そのような演繹が存在)することを

$$\Gamma \vdash P$$

と書く．仮定が存在しない(Γが空集合)ときは特に

$$\vdash P$$

と書き，このときの演繹を証明(proof)と呼ぶ

- 演繹と証明を区別せずに，すべて証明と呼ぶ場合もある(この授業も証明で統一する)

証明の例(1)

- (A1) $P \to (Q \to P)$
- (A2) $(P \to (Q \to R)) \to ((P \to Q) \to (P \to R))$
- (A3) $(\neg P \to \neg Q) \to ((\neg P \to Q) \to P)$
- (B1) 任意の論理式PとQに対して，
  Pと$P \to Q$からQを得る

□ $\vdash X \to X$ の証明を書いてみる

1. $(X \to ((X \to X) \to X)) \to ((X \to (X \to X)) \to (X \to X))$ A2($P = R = X, Q = (X \to X)$)
2. $X \to ((X \to X) \to X)$ A1($P = X, Q = (X \to X)$)
3. $(X \to (X \to X)) \to (X \to X)$ B1(式2, 1より)
4. $(X \to (X \to X))$ A1($P = Q = X$)
5. $X \to X$ B1(式4,3より)

？？？

- 素朴な疑問：いったい何をやっているのか？
  - $X \to X$なぞ当たり前ではないか！！！

  → 当たり前ではありません

- 論理式は記号の列であり，証明は単なる記号列の列であることに注意
  - **我々は→にも¬にも一切意味(真理値表)を与えていない！**
  - 公理や推論規則による記号列の生成方法のみを与えている

- 公理系Sのもとで，(記号列としての)所望の論理式が導くことができるかどうかは全く明らかではない

？？？？？

- さらなる疑問
  - 意味を与えていないのであれば，所望の論理式が導かれるということにも意味はないのでは？

  → その通り

- **証明の構成は（今のところ）単なる記号処理パズルでしかない！**

- …が，「ちゃんと意味を与えられる」ことを実際には示せる
  (完全性定理．証明は次週)

$$\vdash P \quad \Leftrightarrow \quad \vDash P$$

がすべての論理式Pについて成り立つ

「記号操作パズルで導ける」の意

「論理的な帰結として(恒真式として)導ける」の意

実際には仮定を設けても成り立つ
すなわち $\Gamma \vdash P \Leftrightarrow \Gamma \vDash P$

証明における基本的な性質

- 証明の定義より，以下のような性質が(ほぼ自明に)成り立つ
  1. Pが公理(のインスタンス)のとき，$\vdash P$　(${P}$だけからなる証明が存在)
  2. $P \in \Gamma$ならば$\Gamma \vdash P$　(${P}$だけからなる証明が存在)
  3. $\Gamma \vdash P$かつ$\Gamma' \supseteq \Gamma$ならば$\Gamma' \vdash P$　($\Gamma \vdash P$の証明は$\Gamma' \vdash P$の証明でもある)
  4. $\Gamma \vdash P$かつ$P \vdash Q$ならば$\Gamma \vdash Q$
  5. $\Gamma \vdash P_1$, $\Gamma \vdash P_2$, $\{P_1, P_2\} \vdash Q$ならば$\Gamma \vdash Q$

- 4.は，$\Gamma \vdash P$の証明(の列)をWとして，$P \vdash Q$の証明の列を$Q_1, Q_2, \dots Q_n$としたとき，$Q_j = P$となるようなQ_jすべてを列Wで置き換えた列が$\Gamma \vdash Q$の証明になる

- 5.も4.と同様の考え方で示せる

証明における基本的な性質

- ある論理式$f(P_1, P_2, \ldots, P_n)$が証明可能，すなわち$\vdash f(P_1, P_2, \ldots, P_n)$とすると$P_1, P_2, \ldots, P_n$を任意の論理式で置き換えたもの$f'$も同様に証明可能
  - fの証明における各命題記号を当該の論理式で置き換えればf'の証明になる
  - 論理記号はすべて公理から出発していることに注意

演繹定理

- 実際の証明においては，ゼロからの証明の代わりに，仮定をベースに証明を構成することが有用(証明のモジュール化)
  - 仮定は自然な形で含意に置き換えることができる→演繹定理
    - 意味論的な文脈では第2週で既に示した($\Gamma, P \vDash Q$ならば$\Gamma \vDash P \to Q$)
    - 自然演繹的な文脈でも同様の事実が示せる

定理(演繹定理:Deduction Theorem)
$\Gamma, P \vdash Q$ならば$\Gamma \vdash P \to Q$ (Γは空でもよい)

演繹定理の証明

- $\Gamma, P \vdash Q$の証明を$Q_1, Q_2, \ldots Q_n$とする．証明は$\Gamma \vdash P \to Q_i$が任意のiについて成り立つことを，iについての(強)帰納法によって示す

- (基底段階)$i = 1$のとき，Q_1は公理(のインスタンス)か$\Gamma \cup \{P\}$中の論理式のいずれか.
  - $Q_1 = P$のとき，前述の$X \to X$の証明より$\vdash P \to P \Rightarrow \Gamma \vdash P \to P \Rightarrow \Gamma \vdash P \to Q_1$
  - それ以外のとき，$\Gamma \vdash Q_1$である(Q_1だけからなる列が証明になる).
    公理A1を用いるとインスタンス$Q_1 \to (P \to Q_1)$が得られるので，
    これと推論規則B1より$(P \to Q_1)$が得られる，形式的には，

1. Q_1 （Q_1はΓより導けるので）
2. $\mathrm{Q}_1 \to (P \to Q_1)$ （公理A1より）
3. Q_1 (推論規則B1より) がΓ$\vdash P \to Q_1$の証明になる

演繹定理の証明

- (帰納段階)$i' < i$なるすべてのi'について$\Gamma \vdash P \rightarrow Q_{i'}$であると仮定して，$\Gamma \vdash P \rightarrow Q_i$を示す
  - $Q_i \in \Gamma \cup P$またはQ_iが公理のインスタンスのときは，$i = 1$のときと同様に証明可能
  - Q_iが推論規則により得られているときは，ある$j, k < i$が存在して$Q_k = Q_j \rightarrow Q_i$である
  - 帰納法の仮定より$\Gamma \vdash P \rightarrow Q_k \Leftrightarrow \Gamma \vdash P \rightarrow (Q_j \rightarrow Q_i)$であり，公理A2より

$$\Gamma \vdash \left(P \rightarrow (Q_j \rightarrow Q_i)\right) \rightarrow \left((P \rightarrow Q_j) \rightarrow (P \rightarrow Q_i)\right)$$

が得られるので，推論規則を用いて$\Gamma \vdash (P \rightarrow Q_j) \rightarrow (P \rightarrow Q_i)$を得る
さらに帰納法の仮定より$\Gamma \vdash (P \rightarrow Q_j)$であるので，推論規則を再度適用して

$$\Gamma \vdash (P \rightarrow Q_i)$$

が得られる　(終)

演繹定理の利用例

- $X \to Y, Y \to Z \vdash X \to Z$ を証明せよ(いわゆる三段論法)
- 直接説明するのではなく，まず$X \to Y, Y \to Z, X \vdash Z$を示す
  1. $X \to Y$　　仮定
  2. $Y \to Z$　　仮定
  3. X　　仮定
  4. Y　　B1(式3,1より)
  5. Z　　B1(式4,2より)
- 最後に演繹定理を用いて$X \to Y, Y \to Z, X \vdash Z$から$X \to Y, Y \to Z \vdash X \to Z$を得る(終)

演繹定理の一般性

- 公理系にはさまざまなバリエーションがあることは既に述べた
- どのような公理系ならば演繹定理は利用可能か？
  - 証明自体は公理A1，推論規則しか使っていない→この2つがあれば十分?
  - No. それ以外に$X \to X$を使っており，そこでA2が使われている
- 結論：A3以外の公理と推論規則を備えた公理系は演繹定理が成り立つ
  - そのような別の公理系の例は次週に説明する

Part 2: 証明の練習

テキスト例2.1.2(2)

- (A1) $P \to (Q \to P)$
- (A2) $(P \to (Q \to R)) \to ((P \to Q) \to (P \to R))$
- (A3) $(\neg P \to \neg Q) \to ((\neg P \to Q) \to P)$
- (B1) 任意の論理式PとQに対して，
  Pと$P \to Q$からQを得る

- $X \to (Y \to Z), Y \vdash X \to Z$ の証明を与えよ
  - $X \to (Y \to Z), Y, X \vdash Z$を示して演繹定理を用いる

1.	$X \to (Y \to Z)$	仮定
2.	X	仮定
3.	$Y \to Z$	B1(式1,2)
4.	Y	仮定
5.	Z	B1(式3,4)

テキスト問2.1.2より

- (A1) $P \to (Q \to P)$
- (A2) $(P \to (Q \to R)) \to ((P \to Q) \to (P \to R))$
- (A3) $(\neg P \to \neg Q) \to ((\neg P \to Q) \to P)$
- (B1) 任意の論理式PとQに対して，
  Pと$P \to Q$からQを得る

- (1) $\vdash \neg X \to (X \to Y)$ の証明を与えよ
  - 演繹定理の適用を考える．すなわち，$\neg X, X \vdash Y$をまず示したのち，演繹定理×2で証明を完了する

1. $\neg X$	(仮定)	6. $\neg Y \to X$	B1(式2,5)
2. X	(仮定)	7. $(\neg Y \to \neg X) \to ((\neg Y \to X) \to Y)$	(A3)
3. $\neg X \to (\neg Y \to \neg X)$	A1		
4. $\neg Y \to \neg X$	B1(式1,3)	8. $(\neg Y \to X) \to Y$	B1(4,7)
5. $X \to (\neg Y \to X)$	A1	9. Y	B1(式6,8)

  - 最後に演繹定理より$\neg X \vdash X \to Y$を得，さらに$\vdash \neg X \to (X \to Y)$ を得る (終)

テキスト問2.1.2より

- (A1) $P \to (Q \to P)$
- (A2) $(P \to (Q \to R)) \to ((P \to Q) \to (P \to R))$
- (A3) $(\neg P \to \neg Q) \to ((\neg P \to Q) \to P)$
- (B1) 任意の論理式PとQに対して，
  Pと$P \to Q$からQを得る

- (3) $\vdash \neg\neg X \to X$ の証明を与えよ
  - これも$\neg\neg X \vdash X$を示して演繹定理を用いる

1. $\neg\neg X$ 仮定
2. $\neg\neg X \to (\neg X \to \neg\neg X)$ A1
3. $(\neg X \to \neg\neg X)$ B1(式1,2)
4. $(\neg X \to \neg\neg X) \to \big((\neg X \to \neg X) \to X\big)$ A3
5. $((\neg X \to \neg X) \to X)$ B1(式3,4)
6. $\neg X \to \neg X$ 例1より
7. X B1(式5,6)

  - 演繹定理より$\vdash \neg\neg X \to X$を得る (終)

テキスト問2.1.2より

- (A1) $P \to (Q \to P)$
- (A2) $(P \to (Q \to R)) \to ((P \to Q) \to (P \to R))$
- (A3) $(\neg P \to \neg Q) \to ((\neg P \to Q) \to P)$
- (B1) 任意の論理式PとQに対して，
  Pと$P \to Q$からQを得る

5. $\Gamma \vdash P_1,\ \Gamma \vdash P_2,\ \{P_1, P_2\} \vdash Q$ならば$\Gamma \vdash Q$

- (5) $\vdash (\neg Y \to \neg X) \to (X \to Y)$ の証明を与えよ
  - $(\neg Y \to \neg X) \vdash (X \to Y)$を示して演繹定理を使う

1. $(\neg Y \to \neg X)$　仮定
2. $(\neg Y \to \neg X) \to ((\neg Y \to X) \to \neg Y)$　A3
3. $(\neg Y \to X) \to Y$　B1(式1,2)
4. $(X \to (\neg Y \to X))$　A1
5. $X \to Y$　式3,4+例2.1.2(2)+演繹の性質5

- 演繹定理より$\vdash (\neg Y \to \neg X) \to (X \to Y)$を得る．(終)