提纲

- 4.1 形式系统
- 4.2 命题逻辑公理系统
- 4.3 一阶谓词逻辑公理系统
- 4.4 一阶理论公理系统*
- 4.5 命题逻辑证明
- 4.6 一阶谓词逻辑证明
- 4.7 理论证明*

逻辑公理—表达思想的初始概念

- 自然数公理
  - $\forall x(s(x) \neq x)$
  - $\forall x \forall y\ (x \neq y \rightarrow s(x) \neq s(y))$
  - $\forall x(x + 0 = x)$
  - $\forall x \forall y(x + s(y) = s(x + y))$
  - $\forall x(x \circ 0 = 0)$
  - $\forall x \forall y(x \circ s(y) = x \circ y + x$
- 自然数公理是实质公理
  - 具体概念：后继(s)，0，$+$，$\circ$，Q
- 自然数公理是所有的自然数命题真值的依据.
- 从自然数公理能推导出所有的自然数命题真值.

Giuseppe Peano
（1858-1932）

形式系统

- 一个形式系统应当包括以下几部分.
  - (1)**各种初始符号**. 初始符号是一个形式系统的“字母”，经解释后其中一部分是初始概念.
  - (2)**形成规则**. 规定初始符号组成各种合适符号序列的规则. 经解释后合式符号序列是一子句，称为系统里的合式公式或命题.
  - (3)**公理**. 把某些所要肯定的公式选出，作为推导其它所要肯定的公式的出发点，这些作为出发点的公式称为公理.
  - (4)**变形规则**. 变形规则规定如何从公理和已经推导出的一个或几个公式经过符号变换而推导出另一公式. 经过解释，变形规则就是推理规则.
  - 应用变形规则进行推导可以得到一系列公式，这些公式经过解释是系统的定理.
- 形式系统完全由一套**表意符号**建立，它能**克服日常语言的歧义性，使概念、判断、推理精确化**.

希尔伯特证明论

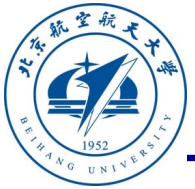
David Hilbert
1862-1943

- 通过形式化第一次使证明本身成为数学研究对象.
- 给出**初始符号**集合
- 构造**合式公式**规则
- **$\Gamma \vdash Q$的证明**，构造出$1 \sim m$个合式公式序列，其中，第m个合式公式是A，并且$1 \sim m$合式公式
  - 或者是前提
  - 或者是公理
  - 或者是推导规则
- 形式证明的正确性是可验证的.

公理系统

定义4.1.1 从一些公理出发，根据演绎定理，推导出一系列定理，由此形成的演绎体系，称为公理系统.

- 公理系统的组成：
  - **符号集**；
  - **公式集**，公式是用于表达命题的符号串；
  - **公理集**，是公式集的真子集
    - 公理是用于表达推理由之出发的初始肯定命题；
  - **推理规则集**
    - 推理规则是由公理及已证定理得出新定理的规则；
  - **定理集**，表达了本系统肯定的所有命题.



提纲

- 4.1 形式系统
- 4.2 命题逻辑公理系统
- 4.3 一阶谓词逻辑公理系统
- 4.4 一阶理论公理系统*
- 4.5 命题逻辑证明
- 4.6 一阶谓词逻辑证明
- 4.7 理论证明*

主要内容

- 命题逻辑公理系统
  - 公理系统
  - 形式推演
  - 演绎定理

命题逻辑公理系统

命题逻辑的公理系统定义如下:

(1) 符号集合：

- **命题变元：** $p_1, p_2, \cdots,$
- **联结词符号：** $\neg, \rightarrow$
- **括号：** $(,)$

(2) 形成规则(公式定义)：

- 若Q是**命题变元**，则Q是公式；
- 若Q是公式，则$\neg Q$是公式；
- 若Q, R是公式，则 $Q \rightarrow R$ 是公式.

命题逻辑公理系统

命题逻辑的公理系统定义如下：

(3) 公理：设Q, R, P为任意公式

- 公理模式$\mathscr{A}_1$：$Q \to (R \to Q)$　肯定后件律
- 公理模式$\mathscr{A}_2$：$(P \to (Q \to R)) \to ((P \to Q) \to (P \to R))$　蕴含词分配律
- 公理模式$\mathscr{A}_3$：$(\neg Q \to \neg R) \to (R \to Q)$　换位律

(4) 推理规则：(分离规则，MP(Modus Ponents)规则)

- 若Q和$Q \to R$成立，则R成立.
- Q和$Q \to R$称为**前提**，R称为**结论**.

(5) 定理集

- 公理集和推理规则集给定后，定理集就完全确定了，因此可省略定理集

命题逻辑公理系统

命题逻辑的公理系统定义如下:

(1) 符号集合：

- **命题变元：** $p_1, p_2, \ldots,$
- **联结词符号：** $\neg, \rightarrow$
- **括号：** $(,)$

(2) 形成规则(公式定义)：

- 若p是**命题变元**，则p是公式；
- 若Q是公式，则$\neg Q$是公式；
- 若Q, R是公式，则$Q \rightarrow R$是公式

(3) 公理： 设Q, R, P为任意公式

- 公理模式$\mathscr{A}_1$：$Q \rightarrow (R \rightarrow Q)$ **肯定后件律**
- 公理模式$\mathscr{A}_2$：$(P \rightarrow (Q \rightarrow R)) \rightarrow ((P \rightarrow Q) \rightarrow (P \rightarrow R))$ **蕴含词分配律**
- 公理模式$\mathscr{A}_3$：$(\neg Q \rightarrow \neg R) \rightarrow (R \rightarrow Q)$ **换位律**

(4) 推理规则： (分离规则，MP(Modus Ponents)规则)

- 若Q和$Q \rightarrow R$成立，则R成立．其中，Q和$Q \rightarrow R$称为前提，R称为结论.

(5) 定理集（公理集和推理规则集给定后，定理集就完全确定了，因此可省略定理集）

缩写定义

- 命题公理系统中仅使用了¬、→联结词符号，

而其他联结词符号∨,∧, ↔,⊕**可以认为是缩写公式**，

用≡表示缩写定义

$(1)\ Q \vee R \equiv \neg Q \rightarrow R$

$(2)\ Q \wedge R \equiv \neg(Q \rightarrow \neg R)$

$(3)\ Q \leftrightarrow R \equiv (Q \rightarrow R) \wedge (R \rightarrow Q)$

$(4)\ Q \oplus R \equiv \neg(Q \leftrightarrow R)$

公理模式

- 公理模式是**相同形式的公式的集合**

公理：设Q, R, P为任意公式

公理模式$\mathscr{A}_1$：$Q \to (R \to Q)$

公理模式$\mathscr{A}_2$：$(P \to (Q \to R)) \to ((P \to Q) \to (P \to R))$

公理模式$\mathscr{A}_3$：$(\neg Q \to \neg R) \to (R \to Q)$

- 公理都是**永真式**，是不加证明而肯定的永真式
- 除了以上公理外，有时还需要**其他推理前提**，记为**公式集合Γ**.
- 已证明过的定理可以用作以后推理的前提.

记号：用Γ或加下标的Γ表示公式集，用Q, R, P或加下标的Q, R, P表示公式.

公理系统

- 弗雷格公理系统
  - $Q \to (R \to Q)$
  - $(P \to (Q \to R)) \to ((P \to Q) \to (P \to R))$
  - $(P \to (Q \to R)) \to (Q \to (P \to R))$
  - $(Q \to R) \to (\neg R \to \neg Q)$
  - $\neg\neg Q \to Q$
  - $Q \to \neg\neg Q$
- 卢卡西维茨公理系统
  - $Q \to (R \to Q)$
  - $(P \to (Q \to R)) \to ((P \to Q) \to (P \to R))$
  - $(\neg Q \to \neg R) \to (R \to Q)$
- 罗素公理系统
  - $Q \vee Q \to Q$
  - $Q \to Q \vee R$
  - $Q \vee R \to R \vee Q$
  - $(P \to Q) \to (P \vee R \to Q \vee R)$

推演(演绎)

- 设Γ是合式公式集合，Q是合式公式

(1) **如果Γ成立，则Q必然成立**，则称**Γ推演(演绎)出Q**，记为**$\Gamma \vdash Q$**

(2) Γ称为推演的**前提集**，称Q为**结论.**

- 推演（演绎）
  - 命题逻辑公理系统
  - 谓词逻辑公理系统

证明

- **证明（Proof）**是指**从前提开始必然到达结论的一系列推理步骤**
  - 推理步骤可以是前提、公理、或由推导规则推演出的公式.
- **有效证明**的特征：
  - 如果前提成立，则结论必然成立.
- **可靠证明**的特征：
  - 前提是成立，并且推理有效.

形式推演

定义4.2.1 设Γ是公式集．若公式序列$A_1, A_2, \ldots, A_n$中的每个公式A_i满足以下条件之一：

(1) A_i是公理；

(2) $A_i \in \Gamma$；

(3) 有j，$k < i$，使A_i由A_j，A_k用MP规则推出．

若A_j和$A_k = A_j \to A_i$成立，则A_i成立

则称该序列为公式A_n的从公式集Γ的一个推演，记为$\Gamma \vdash A_n$．其中，Γ称为推演的前提集，A_n称为结论．

形式推演

定义4.2.1 设Γ是公式集．若公式序列$A_1, A_2, \ldots, A_n$中的每个公式A_i满足以下条件之一：

(1) A_i是公理；

(2) $A_i \in \Gamma$；

(3) 有j，$k < i$，使A_i由A_j，A_k用MP规则推出．

则称该序列为公式A_n的从公式集Γ的一个推演，

记为$\Gamma \vdash A_n$．其中，Γ称为推演的前提集，A_n称为结论．

- 每个公理本身即是它的一个证明
- 每个公理都是定理
- Γ中每个公式A本身即是它的一个从Γ的推演
- 如果公式Q和$Q \to R$ 都是Γ的逻辑推论，则R也是Γ的逻辑推论

引理4.5.1 $Q \to (P \to R), P \vdash Q \to R$

证明：

证据：

$A_1 = (Q \to (P \to R)) \to ((Q \to P) \to (Q \to R))$ $\mathscr{A}_2$

$A_2 = Q \to (P \to R)$ $A_2 \in \Gamma$

$A_3 = (Q \to P) \to (Q \to R)$ $\mathrm{MP}(A_1, A_2)$

$A_4 = P \to (Q \to P)$ $\mathscr{A}_1$

$A_5 = P$ $A_5 \in \Gamma$

$A_6 = Q \to P$ $\mathrm{MP}(A_4, A_5)$

$A_7 = Q \to R$ $\mathrm{MP}(A_3, A_6)$

证毕

逻辑公理系统

- 公理系统是指从事先给定的公理系统出发，根据推理规则推导出一系列定理，形成的演绎体系叫作公理系统。
- 公理系统把表达某些肯定命题的公式称为定理
- 公理分成两类：
- 逻辑公理：都是永真式，是各公理系统（几何学、数论公理系统）通用公理
- 非逻辑公理（公设）：一般不是永真式，只有在特定解释下才为真，在数理逻辑中，只关心由给定公设集能推出哪些定理。

命题逻辑的公理系统的四个要素

- （1）符号集合
  - 命题变元：$p_1, p_2, \cdots, p_n$
  - 联结词符号：$\rightarrow$，$\neg$
  - 括号：（，）
- （2）公式集（形成规则）
  - 若P是命题变元，则P是公式；
  - 若P是公式，则¬P是公式；
  - 若P，Q是公式，则(P $\rightarrow$Q)是公式

命题逻辑公理系统四个要素

- (3).公理模式：P,Q,R为任意合式公式
- 1). $\mathscr{A}_1$： R→ (Q→R)　　肯定后件律
- 2). $\mathscr{A}_2$： (P→ (Q→R))→((P→Q)→ (P→R))　　蕴含词分配律
- 3). $\mathscr{A}_3$： (¬Q→¬R)→(R→Q)　　换位律
- (4).推理规则：变形规则 (分离规则，MP规则)

  若Q和Q→R成立，则R成立。
  - 其中，Q和Q→R称为前提，R称为结论。

公理系统的组成

- 应当包括以下几部分。
  - (1) 符号集。形式系统的“字母表”，经解释后其中一部分是初始概念。
  - (2) 公式集（形成规则）。用于表达命题的符号串，规定组成各种合适符号序列的规则。经解释后合式符号序列是一子句，称为系统里的合式公式或命题。
  - (3)公理集。把某些所要肯定的公式选出，作为推导其它所要肯定的公式的出发点，这些作为出发点的公式称为公理。
  - (4)推理规则（变形规则）。变形规则规定如何从公理和已经推导出的一个或几个公式经过符号变换而推导出另一公式。经过解释，变形规则就是推理规则。
  - 应用变形规则进行推导可以得到一系列公式，这些公式经过解释是系统的定理。
- 公理系统系统完全由一套表意符号建立，它能克服日常语言的歧义性，使概念、判断、推理精确化。

特点分析1：缩写定义

- 谓词公理系统中仅使用了¬和→联结词符号，而其他联结词符号∨,∧,↔,⊕可以认为是缩写公式，用≡表示缩写定义。
  - (1).Q∨R≡(¬Q→R)
  - (2).Q∧R≡¬ (Q→¬R)
  - (3).Q↔R≡(Q→R) ∧(R→Q)
  - (4).Q⊕R≡¬ (Q↔R)

特点分析2:模式化的

- 公理模式：P、Q、R代表任意命题公式
- 例如：
- $(Q \rightarrow R) \rightarrow (P \rightarrow (Q \rightarrow R))$ A_1
- $(P \rightarrow (Q \rightarrow R)) \rightarrow ((P \rightarrow Q) \rightarrow (P \rightarrow R))$ A_2

特点分析3:可解的、可判定的

- 命题逻辑系统中，公式集合与公理集合的判定问题都是可解的，即可用计算机判定一个符号串是公式还是公理
- 命题逻辑的推演正确定是可以通过计算机程序进行判定的
- 例如航电系统、区块链系统的可信性与可靠性

特点分析4:公理与定理

- 三条公理是逻辑公理，是永真式
- 分离规则能保证结论的永真性，即由永真的前提得到的结论还是永真式
- 从逻辑公理出发，使用MP分离规则推出的定理都是永真式（确保了推理演绎的正确性）
- 但除了逻辑公理外有时候还需要其它推理前提，如牛顿三大定律，将这些推理前提符号化为数理逻辑公式，他们往往不是永真式。
- 这些推理前提成为非逻辑公理，用Γ表示
- 已经证明的可以做定理，可以作为以后的前提

形式推演

定义4.2.1 设Γ是公式集．若公式序列$A_1, A_2, \ldots, A_n$中的每个公式A_i满足以下条件之一：

(1) A_i是公理；

(2) $A_i \in \Gamma$；

(3) 有j，$k < i$，使A_i由A_j，A_k用MP规则推出．

则称该序列为公式A_n的从公式集Γ的一个推演，

记为$\Gamma \vdash A_n$．其中，Γ称为推演的前提集，A_n称为结论．

- 每个公理本身即是它的一个证明
- 每个公理都是定理
- Γ中每个公式A本身即是它的一个从Γ的推演
- 如果公式Q和$Q \to R$ 都是Γ的逻辑推论，则R也是Γ的逻辑推论

推论关系（回顾）

- **定义3.2.1** 设Q和R是合式公式，若对于任意指派函数σ，都有$\sigma(Q) \vDash \sigma(R)$，则称$R$是$Q$的逻辑推论，或称$Q$语义推出$R$，记为：$Q \vDash R$

- **定义3.2.2** 设Γ是合式公式集合，R是合式公式，若对于任意指派函数σ，都有$\sigma(Q) \vDash \sigma(R)$，则称$R$是$\Gamma$的逻辑推论，或称$\Gamma$语义推出$R$，记为$\Gamma \vDash R$

- **定义3.2.3** 设$Q_1, \ldots, Q_n$是谓词命题，若$\Gamma = \{Q_1, \ldots, Q_n\}$，则$\Gamma \vDash R$，也可记为$Q_1, \ldots, Q_n \vDash R$。若$\Gamma$是空集合，则记为：$\vDash R$。

推演(演绎)

- 定义：设Γ是合式公式集合，Q是合式公式
  如果Γ成立，则Q必然成立，则称Γ推演(演绎)出Q，
  记为$\Gamma \vdash Q$。
- Γ 称为推演的前提集，称Q为结论。

- 推演（演绎）
  - 命题逻辑公理系统
  - 谓词逻辑公理系统

推演和推论区别与联系？

推演(演绎)

■ 推演和推论的关系

	推论	推演
结论	成立/不成立	存在/不存在
表现形式	所有满足公式集前提的真值赋值满足结论	存在从前提到结论的推理公式序列
前提	前提集合是约束条件，越多越复杂	前提集合是推演条件，越多越简单
	公式集Γ	公式集Γ;公理;由MP规则推出的公式
推理过程	逻辑运算(化成蕴含式) 穷举运算(真值表)	用公式集和公理系统进行逻辑推理(证明)
$\models A;\vdash A$	A是永真式	A是定理

可靠性定理

- 可靠性定理：若$\Gamma \vdash A$，则$\Gamma \vDash A$
- 证明：

  设$A_1, \cdots, A_n$是Q的从Γ的一个推演，归纳证明$\Gamma \vDash A_i, i = 1, 2, \cdots, n$，其中
  - 若A_i是公理，则A_i是永真式，必然有$\Gamma \vDash A_i$
  - 若$A_i \in \Gamma$，必然有$\Gamma \vDash A_i$
  - 若A_i由A_j, A_k用MP规则推出，其中$j, k < i$，A_k为$A_j \to A_i$，由归纳假设知，$\Gamma \vDash A_j, \Gamma \vDash A_j \to A_i$，
  - 对于任意真值赋值v满足Γ，都有$v(A_j) = v(A_j \to A_i) = 1$，此时$v(A_i) = 1$，所以$\Gamma \vDash A_i$
  - 由于$A_n = Q$，可知$\Gamma \vDash Q$

  推论：若$\vdash A$，则$\vDash A$

定理4.2.2（传递律）$P \to Q, Q \to R \vdash P \to R$

证明：

	证据：
$A_1 = (Q \to R) \to (P \to (Q \to R))$	$\mathscr{A}_1$
$A_2 = Q \to R$	$A_2 \in \Gamma$
$A_3 = P \to (Q \to R)$	$\mathrm{MP}(A_1, A_2)$
$A_4 = (P \to (Q \to R)) \to ((P \to Q) \to (P \to R))$	$\mathscr{A}_2$
$A_5 = (P \to Q) \to (P \to R)$	$\mathrm{MP}(A_4, A_3)$
$A_6 = P \to Q$	$A_6 \in \Gamma$
$A_7 = P \to R$	$\mathrm{MP}(A_5, A_6)$

证毕

定理4.2.3 $\vdash \neg Q \rightarrow (Q \rightarrow R)$

证明：

$A_1 = \neg Q \rightarrow (\neg R \rightarrow \neg Q)$

$A_2 = (\neg R \rightarrow \neg Q) \rightarrow (Q \rightarrow R)$

$A_3 = \neg Q \rightarrow (Q \rightarrow R)$

证毕

证据：

$\mathscr{A}_1$

$\mathscr{A}_3$

$A_1, A_2 \vdash A_3$

例4.2.1

若$\Gamma \vdash Q \to R$且$\Gamma \vdash Q \to (R \to P)$, 则$\Gamma \vdash Q \to P$.

解：设$B_1, \dots, B_n, Q \to R$是从Γ到$Q \to R$的推演，

$C_1, \dots, C_m, Q \to (R \to P)$是从$\Gamma$到$Q \to (R \to P)$的推演.

则可如下构造从Γ到$Q \to P$的推演：

$B_1, \dots, B_n, Q \to R$,	$\Gamma \vdash Q \to R$
$C_1, \dots, C_m, Q \to (R \to P)$,	$\Gamma \vdash Q \to (R \to P)$
$A_1 = (Q \to (R \to P)) \to ((Q \to R) \to (Q \to P))$,	$\mathscr{A}_2$
$A_2 = (Q \to R) \to (Q \to P)$,	$\mathrm{MP}(A_1, C_{m+1})$
$A_3 = Q \to P$	$\mathrm{MP}(A_2, B_{n+1})$

证毕

定理4.5.1 （三段论）$Q, Q \to R \vdash R$

证明：

$A_1 = Q \to R$

$A_2 = Q$

$A_3 = R$

证毕

证据：

$A_1 \in \Gamma$

$A_2 \in \Gamma$

$A_1 = A_2 \to A_2$

定理4.5.3 $\vdash (Q \to R) \to ((P \to Q) \to (P \to R))$

证明：　　证据：

$A_1 = (Q \to R) \to (P \to (Q \to R))$　　$\mathscr{A}_1$

$A_2 = (P \to (Q \to R)) \to ((P \to Q) \to (P \to R))$　　$\mathscr{A}_2$

$A_3 = (Q \to R) \to ((P \to Q) \to (P \to R))$　　$A_1, A_2 \vdash A_3$

证毕

定理4.5.6 $\vdash Q \to Q$

证明：

证据：

$A_1 = (Q \to ((Q \to Q) \to Q)) \to ((Q \to (Q \to Q)) \to (Q \to Q))$ $\mathscr{A}_2$

$A_2 = Q \to ((Q \to Q) \to Q)$ $\mathscr{A}_1$

$A_3 = (Q \to (Q \to Q)) \to (Q \to Q)$ $A_1 = A_2 \to A_3$

$A_4 = Q \to (Q \to Q)$ $\mathscr{A}_1$

$A_5 = Q \to Q$ $A_3 = A_4 \to A_5$

证毕

定理4.5.7 $\vdash \neg\neg Q \to Q$

证明：

$A_1 = \neg\neg Q \to (\neg\neg\neg\neg Q \to \neg\neg Q)$ $\mathscr{A}_1$

$A_2 = (\neg\neg\neg\neg Q \to \neg\neg Q) \to (\neg Q \to \neg\neg\neg Q)$ $\mathscr{A}_3$

$A_3 = (\neg Q \to \neg\neg\neg Q) \to (\neg\neg Q \to Q)$ $\mathscr{A}_3$

$A_4 = \neg\neg Q \to (\neg\neg Q \to Q)$ $A_1, A_2, A_3 \vdash A_4$

$A_5 = (\neg\neg Q \to (\neg\neg Q \to Q)) \to ((\neg\neg Q \to \neg\neg Q) \to (\neg\neg Q \to Q))$ $\mathscr{A}_2$

$A_6 = (\neg\neg Q \to \neg\neg Q) \to (\neg\neg Q \to Q)$ $A_5 = A_4 \to A_6$

$A_7 = (\neg\neg Q \to \neg\neg Q)$ $\vdash Q \to Q$

$A_8 = \neg\neg Q \to Q$ $A_6 = A_7 \to A_8$

证据：

证毕

定理4.5.8 $\vdash Q \to \neg\neg Q$

证明：

$A_1 = (\neg\neg\neg Q \to \neg Q) \to (Q \to \neg\neg Q)$

$A_2 = (\neg\neg\neg Q \to \neg Q)$

$A_3 = Q \to \neg\neg Q$

证毕

证据：

$\mathscr{A}_3$

$\vdash \neg\neg Q \to Q$

$A_1 = A_2 \to A_3$

例4.5.1 若$\Gamma \vdash R$，则$\Gamma \vdash Q \to R$.

证明：因为$\Gamma \vdash R$，所以存在从Γ到R的推演$A_1, \ldots, A_k$，使得$A_k = R$.

证据：

$A_1 = \alpha_1$

……

$A_{k-1} = \alpha_{k-1}$

$A_k = R$	$\Gamma \vdash R$
$A_{k+1} = R \to (Q \to R)$	$\mathscr{A}_1$
$A_{k+2} = Q \to R$	$A_{k+1} = A_k \to A_{k+2}$

所以，$\Gamma \vdash Q \to R$

证毕

例4.5.2

- 若$\Gamma \vdash A \to B$，且$\Gamma \vdash A \to (B \to C)$，则$\Gamma \vdash A \to C$
- 证明：设$P_1, \cdots, P_{n-1}, A \to B$是$A \to B$的从$\Gamma$的推演，$Q_1, \cdots, Q_{n-1}, A \to (B \to C)$是$A \to (B \to C)$的从$\Gamma$的推演

	证据：
(1)$P_1, \cdots, P_{n-1}$	…
(2)$A \to B$	序列1
(3)$Q_1, \cdots, Q_{n-1}$	…
(4)$A \to (B \to C)$	序列2
(5)$\big(A \to (B \to C)\big) \to \big((A \to B) \to (A \to C)\big)$	公理二
(6)$(A \to B) \to (A \to C)$	MP(4)(5)
(7)$A \to C$	MP(2)(6)

证毕

定理4.5.2 $\vdash (P \to (Q \to R)) \to (Q \to (P \to R))$

证明：

证据：

$A_1 = (P \to (Q \to R)) \to ((P \to Q) \to (P \to R))$ $\mathscr{A}_2$

$A_2 = ((P \to Q) \to (P \to R)) \to (Q \to ((P \to Q) \to (P \to R)))$ $\mathscr{A}_1$

$A_3 = (Q \to ((P \to Q) \to (P \to R))) \to ((Q \to (P \to Q)) \to (Q \to (P \to R)))$ $\mathscr{A}_2$

$A_4 = ((P \to (Q \to R)) \to ((Q \to (P \to Q)) \to (Q \to (P \to R))))$ $A_1, A_2, A_3 \vdash A_4$

$A_5 = ((P \to (Q \to R)) \to ((Q \to (P \to Q)) \to (Q \to (P \to R)))) \to ((P \to (Q \to R)) \to (Q \to (P \to Q)) \to (P \to (Q \to R)) \to (Q \to (P \to R)))$ $\mathscr{A}_2$

$A_6 = ((P \to (Q \to R)) \to (Q \to (P \to Q)) \to (P \to (Q \to R)) \to (Q \to (P \to R))$

$A_5 = A_4 \to A_6$

$A_7 = Q \to (P \to Q)$ $\mathscr{A}_1$

$A_8 = (Q \to (P \to Q)) \to ((P \to (Q \to R)) \to (Q \to (P \to Q)))$ $\mathscr{A}_1$

$A_9 = (P \to (Q \to R)) \to (Q \to (P \to Q))$ $A_8 = A_7 \to A_9$

$A_{10} = (P \to (Q \to R)) \to (Q \to (P \to R))$ $A_6 = A_9 \to A_{10}$

证毕

定理4.3.2 演绎定理

- $\Gamma \cup \{A\} \vdash B$当且仅当$\Gamma \vdash A \to B$
- 证明：
  - 充分性：设$A_1, A_2, \cdots, A_n$是B的从$\Gamma \cup \{A\}$的推演，则$A_n = B$，归纳证明$\Gamma \vdash A \to A_i$
    - 若A_i是公理，则$\Gamma \vdash A_i$，由例4.5.1可知，$\Gamma \vdash A \to A_i$；
    - 若$A_i \in \Gamma$，则$\Gamma \vdash A_i$，由4.5.1例可知，$\Gamma \vdash A \to A_i$；
    - 若A_i由A_j, A_k用MP规则推出，其中$j, k < i, A_k = A_j \to A_i$，
    - 由归纳假设知$\Gamma \vdash A \to A_j, \Gamma \vdash A \to (A_j \to A_i)$，
    - 由例4.5.2可知$\Gamma \vdash A \to A_i$
    - 因此有$\Gamma \vdash A \to A_n$，即$\Gamma \vdash A \to B$
  - 必要性：
    - 设$\Gamma \vdash A \to B$，则$\Gamma \cup \{A\} \vdash A \to B$，
    - 又因为$\Gamma \cup \{A\} \vdash A$，所以根据三段论有$\Gamma \cup \{A\} \vdash B$

定理3.2 演绎定理说明

- 要证明$\Gamma \vdash A_1 \to (A_2 \to \cdots \to (A_n \to B))$
- 可以把前件变为前提$\Gamma \cup \{A_1, A_2, \ldots, A_n\} \vdash B$
- 因为证明$\Gamma \cup \{A_1, A_2, \ldots, A_n\} \vdash B$比证明
- $\Gamma \vdash A_1 \to (A_2 \to \cdots \to (A_n \to B))$容易

定理4.3.2 $\Gamma \cup \{Q\} \vdash R$当且仅当$\Gamma \vdash Q \to R$

证明: (必要性) 假设$\Gamma \cup \{Q\} \vdash R$，用关于$\Gamma \cup \{Q\}$到$R$的推演长度$n$作归纳证明.

(1) 当$n = 1$时，R或为公理，或属于Γ，或R是Q.

(a) 若R是公理，则

$A_1 = R$　　R是公理

$A_2 = R \to (Q \to R)$　　$\mathscr{A}_1$

$A_3 = Q \to R$　　$A_2 = A_1 \to A_3$

所以$\vdash Q \to R$，从而$\Gamma \vdash Q \to R$

定理4.3.2 $\Gamma \cup \{Q\} \vdash R$当且仅当$\Gamma \vdash Q \to R$

证明: (必要性) 假设$\Gamma \cup \{Q\} \vdash R$，用关于$\Gamma \cup \{Q\}$到$R$的推演长度$n$作归纳证明.

(1) 当$n = 1$时，R或为公理，或属于Γ，或R是Q.

(b) 若 $R \in \Gamma$，则

证明	证据
$A_1 = R$	$R \in \Gamma$
$A_2 = R \to (Q \to R)$	$\mathscr{A}_1$
$A_3 = (Q \to R)$	$A_2 = A_1 \to A_3$

所以，$\Gamma \vdash Q \to R$

(c) 若$R = Q$，则由前面例子知$\vdash Q \to Q$.

所以$\Gamma \vdash Q \to Q$

定理4.3.2 $\Gamma \cup \{Q\} \vdash R$当且仅当$\Gamma \vdash Q \to R$

证明 (续) 假设$\Gamma \cup \{Q\}$到R的推演长度小于n时定理成立.

(2) 归纳证明：当$\Gamma \cup \{Q\}$到R的推演长度等于n时，

并且R由分离规则推出，则有推演$A_1, \dots, A_n = R$，且存在$i, j < n$，使得$A_i = P$，$A_j = P \to R$.

因为$i, j < n$且$\Gamma \cup \{Q\} \vdash P$，且$\Gamma \cup \{Q\} \vdash P \to R$.

由归纳假设知，$\Gamma \vdash Q \to P$且$\Gamma \vdash Q \to (P \to R)$.

因此，存在从Γ到$Q \to P$的推演$B_1, \dots, B_m = Q \to P$，和

从Γ到$Q \to (P \to R)$的推演$C_1, \dots, C_p = Q \to (P \to R)$.

如下构造从Γ到$Q \to R$的推演：

$B_1, \dots, B_m = Q \to P, C_1, \dots, C_p = Q \to (P \to R),$

$C_{p+1} = (Q \to (P \to R)) \to ((Q \to P) \to (Q \to R))$ $\mathscr{A}_2$

$C_{p+2} = (Q \to P) \to (Q \to R)$ $C_{p+1} = C_p \to C_{p+2}$

$C_{p+3} = Q \to R$ $C_{p+2} = B_m \to C_{p+3}$

因此，$\Gamma \vdash Q \to R$.

定理4.3.2 $\Gamma \cup \{Q\} \vdash R$当且仅当$\Gamma \vdash Q \to R$

证明 (续) (充分性)：假设$\Gamma \vdash Q \to R$，则存在从Γ到$Q \to R$的推演$A_1, A_2, \ldots, A_m = Q \to R$.

如下构造从$\Gamma \cup \{Q\}$到R的推演：

证据：

A_1

……

$A_m = Q \to R$

$A_{m+1} = Q$　　$Q \in \Gamma \cup \{Q\}$

$A_{m+2} = R$　　$A_m = A_{m+1} \to A_{m+2}$

因此，$\Gamma \cup \{Q\} \vdash R$.

演绎定理

定理4.3.2 $\Gamma \cup \{Q\} \vdash R$当且仅当$\Gamma \vdash Q \to R$

- 如果要推演的公式是一个**蕴涵式**，则可**把前件作为附加前提添加至前提集Γ，去推导后件**
- 一般来说，前提越多，推导起来更容易

再证定理4.5.2 $\vdash (P \to (Q \to R)) \to (Q \to (P \to R))$

证明：由演绎定理知，只需证明$P \to (Q \to R) \vdash Q \to (P \to R)$

同样由演绎定理知，只需证明$P \to (Q \to R), Q \vdash P \to R$

同理得，只需证明$P \to (Q \to R), Q, P \vdash R$

	证据
$A_1 = P \to (Q \to R)$	$A_1 \in \Gamma$
$A_2 = P$	$A_2 \in \Gamma$
$A_3 = Q \to R$	$A_1 = A_2 \to A_3$
$A_4 = Q$	$A_4 \in \Gamma$
$A_5 = R$	$A_3 = A_4 \to A_5$

证毕

例4.5.3 $\vdash \neg A \to (A \to B)$

- 证明：
  - 首先找出$A \to B$的一个从$\{\neg A\}$的推演如下

	证据：
(1)$\neg A$	前提
(2)$\neg A \to (\neg B \to \neg A)$	公理一
(3)$\neg B \to \neg A$	MP(1)(2)
(4)$(\neg B \to \neg A) \to (A \to B)$	公理三
(5)$A \to B$	MP(3)(4)

  - 由演绎定理得出$\vdash \neg A \to (A \to B)$

- 这个例子表明，如果有一对矛盾A与$\neg A$，就可以和上式结合用两次MP规则得到任何公式。

定理4.5.9 $\vdash (\neg\neg Q \to \neg\neg R) \to (Q \to R)$

证明：

$A_1 = (\neg\neg Q \to \neg\neg R) \to (\neg R \to \neg Q)$

$A_2 = (\neg R \to \neg Q) \to (Q \to R)$

$A_3 = (\neg\neg Q \to \neg\neg R) \to (Q \to R)$

证毕

证据：

$\mathscr{A}_3$

$\mathscr{A}_3$

$A_1, A_2 \vdash A_3$

定理4.5.14 $\vdash \neg Q \to (Q \to R)$

证明：

$A_1 = \neg Q \to (\neg R \to \neg Q)$

$A_2 = (\neg R \to \neg Q) \to (Q \to R)$

$A_3 = \neg Q \to (Q \to R)$

证毕

证据：

$\mathscr{A}_1$

$\mathscr{A}_3$

$A_1, A_2 \vdash A_3$

定理4.5.16 $\vdash (\neg Q \to Q) \to (R \to Q)$

证明：

	证据：
$A_1 = \neg Q \to (\neg\neg R \to \neg Q)$	$\mathscr{A}_1$
$A_2 = (\neg\neg R \to \neg Q) \to (Q \to \neg R)$	$\mathscr{A}_3$
$A_3 = \neg Q \to (Q \to \neg R)$	$A_1, A_2 \vdash A_3$
$A_4 = (\neg Q \to (Q \to \neg R)) \to ((\neg Q \to Q) \to (\neg Q \to \neg R))$	$\mathscr{A}_2$
$A_5 = (\neg Q \to Q) \to (\neg Q \to \neg R)$	$A_4 = A_3 \to A_5$
$A_6 = (\neg Q \to \neg R) \to (R \to Q)$	$\mathscr{A}_3$
$A_7 = (\neg Q \to Q) \to (R \to Q)$	$A_5, A_6 \vdash A_7$

证毕

定理4.5.15 $\vdash (\neg Q \to Q) \to Q$

证明：

$A_1 = (\neg Q \to Q) \to ((\neg Q \to Q) \to Q)$

$A_2 = ((\neg Q \to Q) \to ((\neg Q \to Q) \to Q)) \to (((\neg Q \to Q) \to (\neg Q \to Q)) \to ((\neg Q \to Q) \to Q)))$

$A_3 = ((\neg Q \to Q) \to (\neg Q \to Q)) \to ((\neg Q \to Q) \to Q)$

$A_4 = (\neg Q \to Q) \to (\neg Q \to Q)$

$A_5 = (\neg Q \to Q) \to Q$

证毕

证据：

$\vdash (\neg Q \to Q) \to (R \to Q)$

$\mathscr{A}_2$

$A_2 = A_1 \to A_3$

$\vdash Q \to Q$

$A_3 = A_4 \to A_5$

定理4.5.21 $\vdash Q \vee Q \rightarrow Q$

证明：

$A_1 = (\neg Q \rightarrow Q) \rightarrow Q$

$A_2 = Q \vee Q \rightarrow Q$

证毕

证据：

$\vdash (\neg Q \rightarrow Q) \rightarrow Q$

$Q \vee R \equiv \neg Q \rightarrow R$

定理4.5.22 $\vdash \neg(Q \wedge \neg Q)$

证明：

$A_1 = Q \rightarrow \neg\neg Q$

$A_2 = (Q \rightarrow \neg\neg Q) \rightarrow \neg\neg(Q \rightarrow \neg\neg Q)$

$A_3 = \neg\neg(Q \rightarrow \neg\neg Q)$

$A_4 = \neg(Q \wedge \neg Q)$

证毕

证据：

$\vdash Q \rightarrow \neg\neg Q$

$\vdash Q \rightarrow \neg\,\neg Q$

$A_2 = A_1 \rightarrow A_3$

$Q \wedge R \equiv \neg(Q \rightarrow \neg R)$

定理4.5.23 $\vdash (Q \vee \neg Q)$

证明：

$A_1 = \neg Q \to \neg Q$

$A_2 = (Q \vee \neg Q)$

证毕

证据：

$\vdash Q \to Q$

$Q \vee R \equiv \neg Q \to R$

定理4.5.32 $\vdash Q \to R \vee Q$

证明：

$A_1 = Q \to (\neg R \to Q)$

$A_2 = Q \to R \vee Q$

证毕

证据：

$\mathscr{A}_1$

$Q \vee R \equiv \neg Q \to R$

定理4.5.41 $\vdash \neg Q \to (Q \to R)$

证明：

$A_1 = \neg Q \to (\neg R \to \neg Q)$

$A_2 = (\neg R \to \neg Q) \to (Q \to R)$

$A_3 = \neg Q \to (Q \to R)$

证毕

证据：

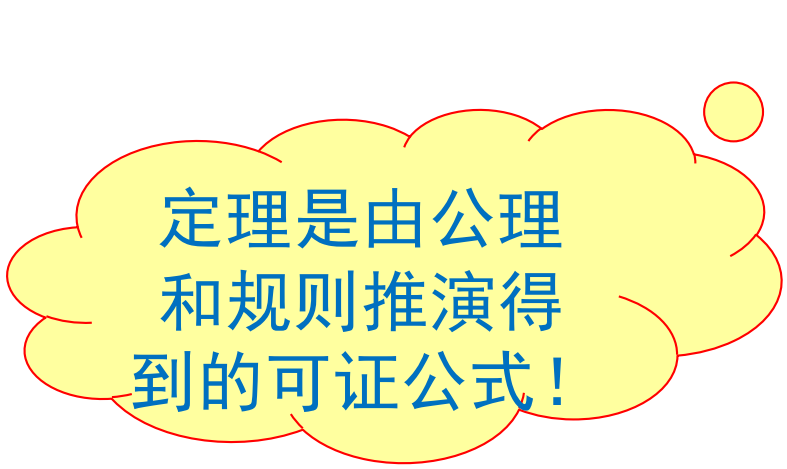
$\mathscr{A}_1$

$\mathscr{A}_3$

$A_1, A_2 \vdash A_3$

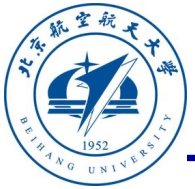
- 如果存在R的从Γ的推演，则记为 $\Gamma \vdash R$.
- 将$\{A_1, \ldots, A_n\} \vdash R$简记为$A_1, \ldots, A_n \vdash R$，
- 将$\emptyset \vdash R$简记为$\vdash R$，此时称R为**定理.**
- 如果$A_1, \ldots, A_n$是R的从$\emptyset$的推演，则称$A_1, \ldots, A_n$为定理R的**证明.**

从系统的公理出发，根据系统允许的推理规则推得的合式公式称为**可证公式**，或称系统里的**定理**.



小结

- 命题逻辑公理系统
  - 公理系统
  - 形式推演
  - 演绎定理



提纲

- 4.1 形式系统
- 4.2 命题逻辑公理系统
- 4.3 一阶谓词逻辑公理系统
- 4.4 一阶理论公理系统*
- 4.5 命题逻辑证明
- 4.6 一阶谓词逻辑证明
- 4.7 理论证明*

公理系统

- 是指**从事先给定的公理**出发，根据**推理规则**推导出一系列**定理**，由此形成的演绎系统.
- 公理系统的组成：
  - **符号集**；
  - **公式集**，公式是用于表达命题的符号串；
  - **公理集**，是公式集的真子集
    - 公理是用于表达推理由之出发的初始肯定命题；
  - **推理规则集**
    - 推理规则是由公理及已证定理得出新定理的规则；
  - **定理集**，表达了本系统肯定的所有命题.

主要内容

- 谓词逻辑公理系统的证明与推演：
  - 5条公理+2条规则（MP+UG）
  - 演绎定理
  - 替换定理

谓词逻辑公理系统

(1) 符号集合：

- **个体变元：** $p_1, p_2, \cdots$
- **个体常元：** $c_1, c_2, \cdots$
- **函词符号：** 对每个正整数n，n元函词符号 $f_1^n, f_2^n, \cdots$
- **谓词符号：** 对每个正整数n，n元谓词符号 $P_1^n, P_2^n, \cdots$
- **联结词符号：** $\neg, \rightarrow$
- **量词符号：** $\forall$
- **逗　号：** ,
- **括　号：** (,)

谓词逻辑公理系统（续）

(2) 项定义：

- **个体常元**是项；
- **个体变元**是项；
- 若$t_1, \ldots, t_n$是项，则$f_i^n(t_1, \ldots, t_n)$是项.

(3) 公式集合：

- 若$t_1, \ldots, t_n$是项，则$P_i^n(t_1, \ldots, t_n)$是公式.
- 若Q是公式，则$\neg Q$是公式；
- 若Q和R是公式，则$Q \to R$是公式；
- 若Q是公式，则$\forall x Q$是公式.

谓词逻辑公理系统（续）

(4) 公理集合： 令Q, R, P为任意公式

公理模式$\mathscr{A}_1$：$Q \to (R \to Q)$

公理模式$\mathscr{A}_2$：$(P \to (Q \to R)) \to ((P \to Q) \to (P \to R))$

公理模式$\mathscr{A}_3$：$(\neg Q \to \neg R) \to (R \to Q)$

公理模式$\mathscr{A}_4$： $\forall x Q \to Q_t^x$

其中**项t对于Q中的x可代入**.

公理模式$\mathscr{A}_5$： $\forall x(Q \to R) \to (Q \to \forall x R)$，（量词分配）

其中**x不是Q中自由变元**.

(5) 推理规则:

- 分离规则（简称MP规则）：从Q和$Q \to R$推出R.
- **综合规则**（简称UG规则）：从Q推出$(\forall x Q)$.

回顾：可代入

- 可代入：设t是项，y是t中任一自由变元，Q是合式公式，x是Q中自由变元，如果Q中x的任何自由出现都不在∀y(∃y)的辖域内，则称项t是对Q中自由变元x可代入的(substitutable)。

- 特别指出：若 $x_1,\ldots,x_n$ 在 A 中没有自由出现，则 $A_{t_1,\cdots,t_n}^{x_1,\cdots,x_n}$ 和 A相同，显然 $t_1,\ldots,t_n$ 对于 A 中的 $x_1,\ldots,x_n$ 是可代入的

缩写定义

谓词公理系统中仅使用了¬和→联结词符号，
而其他联结词符号∨,∧, ↔,⊕可以认为是缩写公式，
用≡表示缩写定义.

- $(1)\ Q \vee R \equiv \neg Q \rightarrow R$
- $(2)\ Q \wedge R \equiv \neg(Q \rightarrow \neg R)$
- $(3)\ Q \leftrightarrow R \equiv (Q \rightarrow R) \wedge (R \rightarrow Q)$
- $(4)\ Q \oplus R \equiv \neg(Q \leftrightarrow R)$

谓词公理系统中仅使用了量词∀，**存在量词∃**是缩写公式，由定义给出，用≡表示缩写定义.

- $\exists x Q(x) \equiv \neg \forall x \neg Q(x)$

推演

定义4.2.1 设Γ是**语句集**. 如果公式序列$A_1, \ldots, A_n$中的每个公式A_i满足以下条件之一：

1. A_i是公理，
2. $A_i \in \Gamma$，
3. 有$j, k < i$使得用**MP规则**由A_j, A_k可推出A_i，
4. **有$j < i$使得用UG规则由A_j可推出A_i；**

则称$A_1, \ldots, A_n$为A_n的从Γ的一个**推演**.

称Γ为推演的前提集，A_n为推演的结论.

例4.6.1 若$\Gamma \vdash \forall x_i Q$且$t$对于公式$Q$中的$x_i$可代入，则$\Gamma \vdash Q_t^{x_i}$

证明：　　证据

$A_1 = \forall x_i Q$　　$\Gamma \vdash \forall x_i Q$

$A_2 = \forall x_i Q \to Q_t^{x_i}$　　$\mathscr{A}_4$

$A_3 = Q_t^{x_i}$　　$A_2 = A_1 \to A_3$

证毕

- 说明：若取t为x_i，则$Q_t^{x_i}$即为公式Q.

  所以有：**若$\Gamma \vdash \forall x_i Q$，则$\Gamma \vdash Q$.**

命题逻辑定理

- $\vdash (Q \to (R \to P)) \to (R \to (Q \to P))$
- $\vdash (R \to P) \to ((Q \to R) \to (Q \to P))$
- $\vdash (Q \to R) \to ((R \to P) \to (Q \to P))$
- $\vdash ((Q \to R) \to (Q \to P)) \to (Q \to (R \to P))$

- $\vdash Q \to Q$
- $\vdash \neg\neg Q \to Q$
- $\vdash R \to \neg\neg R$

命题逻辑定理

- $\vdash (\neg\neg Q \to \neg\neg R) \to (Q \to R)$
- $\vdash (Q \to R) \to (\neg\neg Q \to \neg\neg R)$
- $\vdash (Q \to R) \to (\neg R \to \neg Q)$
- $\vdash (\neg Q \to R) \to (\neg R \to Q)$
- $\vdash (Q \to \neg R) \to (R \to \neg Q)$

- $\vdash \neg Q \to (Q \to R)$
- $\vdash (\neg Q \to Q) \to (R \to Q)$
- $\vdash (\neg Q \to Q) \to Q$
- $\vdash (\neg Q \to R \wedge \neg R) \to Q$
- $\vdash (\neg Q \to R) \to ((\neg Q \to \neg R) \to Q)$
- $\vdash (Q \to R) \to ((Q \to \neg R) \to \neg Q)$

命题逻辑定理

- $\vdash Q \to ((Q \to R) \to R)$
- $\vdash Q \wedge (Q \to R) \to R$

- $\vdash (P \wedge Q \to R) \to (P \to (Q \to R))$
- $\vdash Q \to (R \to (Q \wedge R))$
- $\vdash (P \to Q) \wedge (P \to R) \to (P \to Q \wedge R)$
- $\vdash (P \to R) \to ((Q \to R) \to ((P \vee Q) \to R))$

- $Q, R \vdash Q \wedge R$

命题逻辑定理

- $\vdash \boldsymbol{Q} \vee \boldsymbol{Q} \rightarrow \boldsymbol{Q}$
- $\vdash \boldsymbol{Q} \wedge \boldsymbol{Q} \rightarrow \boldsymbol{Q}$
- $\vdash (\boldsymbol{Q} \rightarrow \boldsymbol{R}) \vee (\boldsymbol{R} \rightarrow \boldsymbol{Q})$
- $\vdash (\boldsymbol{Q} \rightarrow \boldsymbol{R}) \vee (\boldsymbol{Q} \rightarrow \neg \boldsymbol{R})$

- 单调性：$(\boldsymbol{Q} \rightarrow \boldsymbol{R}) \rightarrow (\boldsymbol{Q} \wedge \boldsymbol{P} \rightarrow \boldsymbol{R} \wedge \boldsymbol{P})$

例4.6.2 $\vdash \forall x(Q(x) \vee \neg Q(x))$

证明：

$A_1 = \neg Q(x) \rightarrow \neg Q(x)$

$A_2 = Q(x) \vee \neg Q(x)$

$A_3 = \forall x(Q(x) \vee \neg Q(x))$

证毕

证据：

$\vdash Q \rightarrow Q$

$Q \vee R \equiv \neg Q \rightarrow R$

$\mathrm{UG}(A_2)$

定理4.6.1 $\vdash \forall x Q(x) \to \forall y Q(y)$, ($y$不在Q中自由出现)

- 证明定理：$\vdash \forall x Q(x) \to \forall y\, Q(y)$ 其中 y不在Q中自由出现，且 y可代入
  - 此处，$Q(x)$ 理解为参数化公式：
  - 例如：$Q(x) = P(x,z) \to R(x,a) \wedge \forall y P(x,y)$ 不可代入！
  - 例如：$Q(x) = P(x,z) \to R(x,a)$ 则有：

    $Q(y) = P(y,z) \to R(y,a)$ 可代入！

    证明： 证据：

定理4.6.1 $\vdash \forall x Q(x) \to \forall y Q(y)$, ($y$不在Q中自由出现)

- 证明定理：$\vdash \forall x Q(x) \to \forall y\, Q(y)$ 其中 y不在Q中自由出现，且 y可代入
  - 此处，$Q(x)$ 理解为参数化公式：
  - 例如：$Q(x) = P(x,z) \to R(x,a) \wedge \forall y P(x,y)$ 不可代入！
  - 例如：$Q(x) = P(x,z) \to R(x,a)$ 则有：

    $Q(y) = P(y,z) \to R(y,a)$ 可代入！

    证明： 证据：
  - $A_1 = \forall x Q(x) \to Q(y)$ 公理$\mathcal{A}_4$
  - $A_2 = \forall y\big(\forall x Q(x) \to Q(y)\big)$ UG A_1
  - $A_3 = \forall y\big(\forall x Q(x) \to Q(y)\big) \to \big(\forall x Q(x) \to \forall y Q(y)\big)$ 公理$\mathcal{A}_5$
  - $A_4 = \forall x Q(x) \to \forall y\, Q(y)$

    MPA_3 A_2

证毕。

例4.6.4 $\vdash Q(c) \to \exists x Q(x)$

证明 证据

$A_1 = \forall x \neg Q(x) \to \neg Q(c)$ $\mathscr{A}_4$

$A_2 = \neg\neg\forall x \neg Q(x) \to \forall x \neg Q(x)$ $\vdash (\neg\neg Q \to Q)$

$A_3 = \neg\neg\forall x \neg Q(x) \to \neg Q(c)$ $A_2, A_1 \vdash A_3$

$A_4 = (\neg\neg\forall x \neg Q(x) \to \neg Q(c)) \to (Q(c) \to \neg\forall x \neg Q(x))$ $\mathscr{A}_3$

$A_5 = Q(c) \to \neg\forall x \neg Q(x)$ $A_4 = A_3 \to A_5$

$A_6 = Q(c) \to \exists x A(x)$ $\exists x Q(x) \equiv \neg\forall x \neg Q(x)$

证毕

定理4.6.6 $\vdash \forall x\forall y R(x,y) \to \forall y\forall x R(x,y)$

证明：

	证据：
$A_1 = \forall x\forall y R(x,y) \to \forall y R(x,y)$	$\mathscr{A}_4$
$A_2 = \forall y R(x,y) \to R(x,y)$	$\mathscr{A}_4$
$A_3 = \forall x\forall y R(x,y) \to R(x,y)$	$A_1, A_2 \vdash A_3$
$A_4 = \forall x(\forall x\forall y R(x,y) \to R(x,y))$	$\mathrm{UG}(A_3)$
$A_5 = \forall x(\forall x\forall y R(x,y) \to R(x,y)) \to (\forall x\forall y R(x,y) \to \forall x R(x,y))$	$\mathscr{A}_5$
$A_6 = (\forall x\forall y R(x,y) \to \forall x R(x,y))$	$A_5 = A_4 \to A_6$
$A_7 = \forall y(\forall x\forall y R(x,y) \to \forall x R(x,y))$	$\mathrm{UG}(A_6)$
$A_8 = \forall y(\forall x\forall y R(x,y) \to \forall x R(x,y)) \to (\forall x\forall y R(x,y) \to \forall y\forall x R(x,y))$	$\mathscr{A}_5$
$A_9 = \forall x\forall y R(x,y) \to \forall y\forall x R(x,y)$	$A_8 = A_7 \to A_9$

证毕

演绎定理

定理4.3.3 若Q是语句，则

$$\Gamma \cup \{Q\} \vdash R \text{当且仅当} \Gamma \vdash Q \to R.$$

证明：(必要性) 设$A_1, \ldots, A_n$是R的从$\Gamma \cup \{Q\}$的推演.

归纳证明：$\Gamma \vdash Q \to Q_i$，$i = 1, \ldots, n$.

(1) 若A_i是公理或者$A_i \in \Gamma$，则$\Gamma \vdash A_i$，此时

$A_1 = A_i$	$\Gamma \vdash A_i$
$A_2 = A_i \to (Q \to A_i)$	$\mathscr{A}_1$
$A_3 = Q \to A_i$	$A_2 = A_1 \to A_3$.

- **回顾：语句** A 中没有自由变元，所以对于解释 I 中的任意赋值 v_1 和 v_2，$I(A)(v_1) = I(A)(v_2)$，即**语句的意义与赋值无关**，将 $I(A)(v)$ 简记为 $I(A)$。

演绎定理

定理4.3.3 若Q是语句，则

$$\Gamma \cup \{Q\} \vdash R \text{当且仅当} \Gamma \vdash Q \to R.$$

证明：(必要性)设$A_1, \ldots, A_n$是R的从$\Gamma \cup \{Q\}$的推演.

归纳证明：$\Gamma \vdash Q \to Q_i$，$i = 1, \ldots, n$.

(2) 若A_i是Q，由$\vdash Q \to Q$知，$\Gamma \vdash A_i \to Q_i$.

演绎定理

定理4.3.3 若Q是语句，则

$$\Gamma \cup \{Q\} \vdash R \text{当且仅当} \Gamma \vdash Q \to R.$$

证明：(必要性)设$A_1, \ldots, A_n$是R的从$\Gamma \cup \{Q\}$的推演.

归纳证明：$\Gamma \vdash Q \to Q_i$，$i = 1, \ldots, n$.

(3) 若A_i由A_j, Q_k用MP规则推出$(j, k < i), A_k = Q_j \to A_i$.

由归纳假设知，$\Gamma \vdash Q \to A_j$且$\Gamma \vdash Q \to (Q_j \to Q_i)$，

由例4.2.1得出$\Gamma \vdash Q \to A_i$.

(例4.2.1：$\Gamma \vdash Q \to R$且$\Gamma \vdash Q \to (R \to P)$，则$\Gamma \vdash (Q \to P)$

演绎定理

定理4.3.3 若Q是语句，则

$$\Gamma \cup \{Q\} \vdash R \text{当且仅当} \Gamma \vdash Q \to R.$$

证明：(续) (4)若A_i由A_j用UG规则推出，其中$j < i$，A_i为$\forall x A_j$.

由归纳假设知，$\Gamma \vdash Q \to A_j$. 由UG规则得出

$$\Gamma \vdash \forall x(Q \to A_j) \quad (A_i \text{为} \forall x A_j)$$

因Q是语句，x不是Q的自由变元，由公理$\mathscr{A}_5$,

$$\Gamma \vdash \forall x(Q \to A_j) \to (Q \to \forall x Q_j)$$

再用MP规则得出

$$\Gamma \vdash Q \to \forall x Q_j, \text{ 此即为} \Gamma \vdash Q \to Q_i.$$

因此，$\Gamma \vdash Q \to Q_n$，即$\Gamma \vdash Q \to R$.

演绎定理

定理4.3.3 若Q是语句，则

$$\Gamma \cup \{Q\} \vdash R \text{当且仅当} \Gamma \vdash Q \to R.$$

证明: (续) (充分性) 已知$\Gamma \vdash Q \to R$,

由$\Gamma \cup \{Q\} \vdash Q$且$\Gamma \cup \{Q\} \vdash Q \to R$,

根据MP规则，得到$\Gamma \cup \{Q\} \vdash R$.

演绎定理

定理4.3.3 若Q是**语句**，则

$$\Gamma \cup \{Q\} \vdash R \text{当且仅当} \Gamma \vdash Q \to R.$$

- 如果要证明$\Gamma \vdash Q \to R$，只有**当Q是语句时，才能使用演绎定理**将Q移至左边去证明$\Gamma \cup \{Q\} \vdash R$.

例：$\vdash \forall x(Q(x,y) \to R(x,y)) \to (\forall xQ(x,y) \to \forall xR(x,y))$

定理4.6.18 $\vdash \forall x(P(x) \wedge Q(x)) \rightarrow (\forall x P(x) \wedge \forall x Q(x))$

证明：由演绎定理知, 仅需证$\forall x(P(x) \wedge Q(x)) \vdash \forall x P(x) \wedge \forall x Q(x)$.

设 $\Gamma = \{\forall x(P(x) \wedge Q(x))\}$.

	证据：
$A_1 = \forall x(P(x) \wedge Q(x))$	$A_1 \in \Gamma$
$A_2 = \forall x(P(x) \wedge Q(x)) \rightarrow P(x) \wedge Q(x)$	$\mathscr{A}_4$
$A_3 = P(x) \wedge Q(x)$	$A_2 = A_1 \rightarrow A_3$
$A_4 = P(x) \wedge Q(x) \rightarrow P(x)$	$\vdash Q \wedge R \rightarrow Q$（重言式）
$A_5 = P(x)$	$A_4 = A_3 \rightarrow A_5$
$A_6 = \forall x P(x)$	$\mathrm{UG}(A_5)$
$A_7 = P(x) \wedge Q(x) \rightarrow Q(x)$	$\vdash Q \wedge R \rightarrow R$ （重言式）
$A_8 = Q(x)$	$A_7 = A_3 \rightarrow A_8$
$A_9 = \forall x Q(x)$	$\mathrm{UG}(A_8)$
$A_{10} = \forall x P(x) \wedge \forall x Q(x)$	$A_6, A_9 \vdash A_6 \wedge A_9$

证毕

小结

- 谓词逻辑公理系统的证明与推演：
  - 5条公理+2条规则（**MP+UG**）
  - 演绎定理（定理4.3.3）

下面给出这些谓词定理的
参考证明：

定理4.6.4 $\vdash Q(c) \to \exists x Q(x)$

证明：

$A_1 = \forall x \neg Q(x) \to \neg Q(c)$

$A_2 = (\forall x \neg Q(x) \to \neg Q(c)) \to (Q(c) \to \neg \forall x \neg Q(x))$

$A_3 = Q(c) \to \neg \forall x \neg Q(x)$

$A_4 = Q(c) \to \exists x Q(x)$

证毕

证据：

$\mathscr{A}_4$

$\vdash (R \to \neg P) \to (P \to \neg R)$

$A_2 = A_1 \to A_3$

$\exists x R(x) \equiv \neg \forall x \neg R(x)$

定理4.6.5 $\vdash \neg Q(c) \to \neg \forall x Q(x)$

证明：

$A_1 = \forall x Q(x) \to Q(c)$ $\mathscr{A}_4$

$A_2 = \left(\forall x Q(x) \to Q(c)\right) \to \left(\neg Q(c) \to \neg \forall x Q(x)\right)$

$\vdash (R \to \neg P) \to (P \to \neg R)$

$A_3 = \neg Q(c) \to \neg \forall x Q(x)$ $A_2, A_1 \vdash A_3$

证毕

证据：

定理4.6.6 $\vdash \forall x\forall y R(x,y) \to \forall y\forall x R(x,y)$

证明：

证据：

$A_1 = \forall x\forall y R(x,y) \to \forall y R(x,y)$ $\mathscr{A}_4$

$A_2 = \forall y R(x,y) \to R(x,y)$ $\mathscr{A}_4$

$A_3 = \forall x\forall y R(x,y) \to R(x,y)$ $A_1, A_2 \vdash A_3$

$A_4 = \forall x(\forall x\forall y R(x,y) \to R(x,y))$ $\mathrm{UG}(A_3)$

$A_5 = \forall x(\forall x\forall y R(x,y) \to R(x,y)) \to (\forall x\forall y R(x,y) \to \forall x R(x,y))$ $\mathscr{A}_5$

$A_6 = (\forall x\forall y R(x,y) \to \forall x R(x,y))$ $A_5 = A_4 \to A_6$

$A_7 = \forall y(\forall x\forall y R(x,y) \to \forall x R(x,y))$ $\mathrm{UG}(A_6)$

$A_8 = \forall y(\forall x\forall y R(x,y) \to \forall x R(x,y)) \to (\forall x\forall y R(x,y) \to \forall y\forall x R(x,y))$ $\mathscr{A}_5$

$A_9 = (\forall x\forall y R(x,y) \to \forall y\forall x R(x,y))$ $A_8 = A_7 \to A_9$

证毕

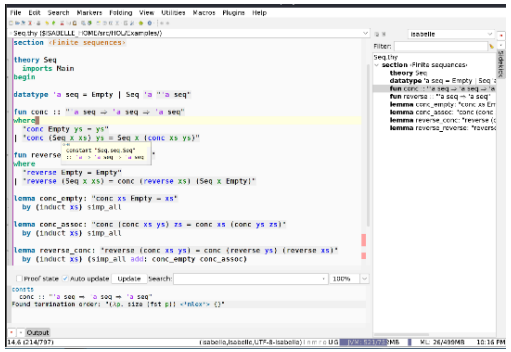
公理系统的应用

- 数学理论体系的起点
  - 皮亚诺算术公理
  - 塔尔斯基实数公理系统
  - 欧几里得几何公理
  - Zermelo-Fraenkel集合论
  - 柯尔莫果洛夫概率论公理

- 程序形式化验证
  - 形式验证使用**数学方法**证明系统**不存在bug**或**符合规范**
  - 常用的形式验证软件：Coq/Isabelle/TLA+等

定理证明辅助工具——Isabelle

- Isabelle定理证明器
  - Isabelle是一种**支持高阶逻辑**的通用定理证明器
  - Isabelle由剑桥大学和慕尼黑工业大学的学者于1986年共同开发完成
  - 支持谓词公理系统、Zermelo-Fraenkel集合论、嵌入式操作系统验证等
- 操作系统形式化验证
  - seL4是世界上最小的内核之一，但**性能不弱于**当前性能最好的微内核
  - seL4是**完全形式验证**的
  - seL4验证使用Isabelle/HOL进行**形式化数学证明**



```
— ‹The combinator K›
lemma ‹P ⟶ (Q ⟶ P)›
  by fast

— ‹The combinator S›
lemma ‹(P ⟶ Q ⟶ R) ⟶ (P ⟶ Q) ⟶ (P ⟶ R)›
  by fast


— ‹Converse is classical›
lemma ‹(P ⟶ Q) ∨ (P ⟶ R) ⟶ (P ⟶ Q ∨ R)›
  by fast

lemma ‹(P ⟶ Q) ⟶ (¬ Q ⟶ ¬ P)›
  by fast
```


谢谢