高级数理逻辑

杨雅君

yjyang@tju.edu.cn

智能与计算学部

2024

涉及的数学分支

- 证明论
- 模型论
- 递归论
- 集合论
- 推演系统

概述

- 数理逻辑的含义
  - 用数学的方法研究逻辑问题
- 逻辑的核心内容
  - 推理理论：本课程仅仅研究演绎（有效）推理
- 演绎推理
  - 前提与结论存在可推导性关系
  - 由前提的真，可得结论的真
  - 前提 $\Rightarrow$ 结论
  - 前提 $\rightarrow$ 结论为永真式

怎样的前提和结论存在可推导性关系？

例子

- 所有 3 的倍数的数字之和是 3 的倍数。
- 10^{10} 的数字之和不是 3 的倍数。
- 10^{10} 不是 3 的倍数。

- 所有中学生打网球。
- 王君不打网球。
- 王君不是中学生。

可推导性关系的内因

- 前提、结论的真值
  - 语义范畴
- 内因：前提、结论的逻辑形式
  - 语法范畴
- 两个例子的逻辑形式相同
  - S 中的所有元有 R 性质。
  - a 没有 R 性质。
  - a 不是 S 中的元。

数理逻辑的研究内容

- 形式语言
  - 无二义性、精确的、普遍适用的符号语言
  - 自然语言存在二义性、不精确
  - 语义：涉及符号、表达式的具体涵义
  - 语法：仅涉及表达式的形式结构
- 推理演算

历史

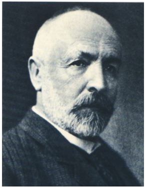
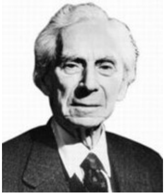
- 公元前 3 世纪，Aristotle 创立了逻辑学。
- 数理逻辑是数学的基础问题。
- 17 世纪，Leibniz 提出建立形式语言、推理方法的思想，以解决数学证明等问题的一致性问题。
- 1847 年，Bool 发表了《逻辑的数学分析》，建立了布尔代数，初步创建了符号系统。
- 1887 年，Frege 出版《数论基础》，成功的实现了 Leibniz 的思想。
- 1928 年，Hilbert 提出 4 个急需解决的数理逻辑问题。
- 从 1929 年开始的短时期内，Godel 全部解决了这四个问题。

课程的主要内容

- 经典逻辑
  - 命题逻辑
  - 谓词（一阶）逻辑
- 非经典逻辑
  - 构造型逻辑
  - 模态逻辑

集合论

- 19世纪下半叶，Cantor提出朴素集合论
- 1903年，Russel提出集合论悖论，产生数学的第三次危机
- 1908年，Zermelo提出公理化集合论(ZF体系)


集合论

- 集合论是数学的基石之一
- 基本概念
  - 集合 & 元素
  - 序偶 & 笛卡尔积
  - 关系
    - 映射
    - 等价关系
    - 相容关系
    - 序关系

集合 & 元素

- 若干事物组成的整体被称为集合，集合中的每个事物被称为元素。
- 元素 a 属于集合 A，记为 $a \in A$
- 在确定性数学中，$a \notin A$ iff $\neg(a \in A)$
- 集合的表示方法
  - 枚举法
  - 谓词法
  - 归纳法

元素的一些说明

- 无序性：$\{a, b\} = \{b, a\}$
- 可区分：$\{a, b\} = \{a, a, b\}$
- 或具体或抽象，$\{1, 2, \&, *, \text{天津大学}, \mathsf{CMU}\}$
- 或有联系或无联系
- 特别的，集合的元素可以是一个集合：$\{\{1, 2\}, 1, 2\}$

集合悖论

Russel（理发师）悖论

某城市中有一位理发师，他的招牌是这样写的：“本人将为本城所有不给自己刮脸的人刮脸，且只给这些人刮脸。”

这位理发师能不能给他自己刮脸呢？

如果他不给自己刮脸，他就属于“不给自己刮脸的人”，他就要给自己刮脸，而如果他给自己刮脸呢？他又属于“给自己刮脸的人”，他就不该给自己刮脸。

ZF 公理体系

- 外延公理：$S = T$ iff $(\forall x)(x \in S \leftrightarrow x \in T)$ 为真
- 子集公理：$S \subseteq T$ iff $(\forall x)(x \in S \to x \in T)$ 为真
- 空集存在公理：存在一个没有任何元素的集合 $\emptyset$
- 幂集公理：集 A 的幂集 $P(A) = \{a|a$ 为 A 的子集$\}$

集合论

集合的运算：对于集合 S, T

- 并：$S \cup T = \{x | x \in S \vee x \in T\}$
- 交：$S \cap T = \{x | x \in S \wedge x \in T\}$
- 差：$S - T = \{x | x \in S \wedge x \notin T\}$
- 补：$\bar{S} = E - S = \{x \notin S\}$，$E$ 为全集
- 对称差：$S \oplus T = (S - T) \cup (T - S)$

序偶 & 笛卡尔积

- 序偶
  - 元素 a 与 b 构成的序偶，简记为 $< a, b >$。
  - $< a, b >=< x, y >$ iff $a = x$ 且 $b = y$
- 笛卡尔积：$S \times T = \{< x, y > | x \in S \wedge x \in T\}$
- 扩展（$n > 2$）
  - 有序 n 元组：
    $< a_1, a_2, \cdots, a_n >=<< a_1, a_2, \cdots, a_{n-1} >, a_n >$
  - n 阶笛卡尔积：
    $S_1 \times S_2 \times \cdots \times S_n = \{< x_1, x_2, \cdots, x_n > | x_1 \in S_1 \wedge \cdots \wedge x_n \in S_n\}$

集合论

关系

- R 是从集 S 到集 T 的一个二元关系 iff $R \subseteq S \times T$
- R 是集 S 上的一个二元关系 iff $R \subseteq S \times S = S^2$
- 几个特殊关系
  - 从集 S 到集 T 的全域关系：$S \times T$
  - 空关系：$\emptyset$
  - 集 S 上的恒等关系：$I_S = \{< x, x > | x \in S\}$
- 关系的表示
  - 关系矩阵
  - 关系图

关系的运算

- 定义域（前域）、值域、域：设 R 是由 A 到 B 的一个二元关系，则
  $dom(R) = \{x|\exists y \in B, < x, y > \in R\}$ 称为 R 的定义域。
  $ran(R) = \{y|\exists x \in A, < x, y > \in R\}$ 称为 R 的值域。
  $FLD(R) = dom(R) \cup ran(R)$ 称为 R 的域。
- 复合关系：设 R 是由 A 到 B 的一个二元关系，S 是由 B 到 C 的一个二元关系，则
  $R \circ S = \{< x, z > |\exists y \in B, < x, y > \in R$ 且 $< y, z > \in S\}$ 称为 R 与 S 的复合关系。
- 逆关系：设 R 是由 A 到 B 的一个二元关系，则
  $R^{-1} = \{< y, x > | < x, y > \in R\}$ 称为 R 的逆关系。

关系的性质：设 R 是 A 上的一个二元关系

- 自反：R 在 A 上自反，iff 对于任何 $x \in A, xRx$。
- 对称：R 在 A 上对称，iff 对于任何 $x, y \in A$，若 xRy，则 yRx。
- 传递：R 在 A 上对称，iff 对于任何 $x, y, z \in A$，若 xRy 且 yRz，则 xRz。
- 反自反
- 反对称

等价关系

- 等价关系：若 R 在 A 上自反、对称、传递，则称 R 为 A 上的一个等价关系。
- 等价类：设 R 为 A 上的一个等价关系，则对于 $a \in A$，$[a]_R = \{x| < a, x >\in R\}$ 称为 a 关于 R 的等价类。
- 商集：设 R 为 A 上的一个等价关系，则 $A/R = \{[a]_R|a \in A\}$ 称为 A 关于 R 的商集。
- 等价类的性质
  - $\cup[a]_R = A$
  - $[a]_R = [b]_R$ iff aRb
  - $[a]_R \neq \emptyset$
- A/R 是 A 的一个划分。

集合论

- 映射：设 f 是由集 A 到集 B 的一个二元关系。若满足:
  1. 对于任何 x, y, z，若 $<x, y> \in f$ 且 $<x, z> \in f$，则 $y = z$；
  2. $dom(f) = A$。

  则称 f 为从 A 到 B 的一个映射，记为 $f : A \to B$。若 $<x, y> \in f$，则称 y 为 x 的像，x 为 y 的原像，记为 $y = f(x)$。
- 运算：若 f 是由 A^n 到 B 的一个映射，则称 f 为 A 上的一个 n 元运算。
- 单射、满射、双射
  - 设 f 为从 A 到 B 的一个单射，当且仅当对于任何 x, y，若 $f(x) = f(y)$，则 $x = y$。
  - 设 f 为从 A 到 B 的一个满射，当且仅当 $ran(f) = B$。
  - 既是单射又是满射的映射称为双射（或一一映射）。

集合的基数

- 等势、同浓：若集合 A 和 B 间存在一一映射，则称 A 与 B 等势（或同浓），记作 $A \sim B$。
- 单射、满射、双射等势作为集合间的关系是等价关系。
- 基数：与集合 A 等势的全体集合所组成的集合，称为 A 的基数，记为 $|A|$。
  - 有限集合的基数，记为其元素个数。
  - $|N|$ 记为 $\aleph_0$，$|R|$ 记为 $\aleph_1$
- 可数集、不可数集：若 $|A| \leq |N|$，则称 A 为可数集。否则为不可数集。

自然数集的归纳定义

自然数的后继。

两种等价定义。

定义一：

1. $0 \in N$
2. 对于任何 n，若 $n \in N$，则 $n' \in N$ (n' 为 n 的后继)
3. 只有由（有限次使用）(1) 和 (2) 生成的 $n \in N$。

定义二：N 是满足以下 (1) 和 (2) 的 S 中的最小集：

1. $0 \in S$
2. 对于任何 n，若 $n \in S$，则 $n' \in S$ (n' 为 n 的后继)

基于自然数集的归纳证明原理

定理

1. $R(0)$；
2. 对于任何 $n \in N$，如果 $R(n)$，则 $R(n')$。

则对于任何 $n \in N$， $R(n)$。

归纳命题、变元、基始、步骤、假设

3. 对于任何 $n \in N$，如果 $R(0), \cdots, R(n)$，则 $R(n')$。
4. 对于任何 $n \in N$，如果对于所有 $m < n$， $R(m)$，则 $R(n)$。

$1 + 3 = 1 + 2 = 4$

自然数集上函数的递归定义原理

定理

设 g 和 h 是 N 上的已知函数，则必存在唯一的 N 上函数 f，使得

1. $f(0) = g(0)$；
2. $f(n') = h(f(n))$ (或 $f(n') = h(n, f(n))$)，其中 n' 为 n 的后继。

$g(n) = 1, h(n, m) = (n+1) \times m$

$f(0) = g(0)$

$f(n+1) = h(n, f(n))$

集合归纳定义的一般情况

设 M 为集合，g_i 为 n_i 元运算，$i = 1, 2, \cdots, k$。两种等价定义：

1. $M \subseteq S$
2. 对于任何 $x_1, x_2, \cdots, x_{n_i}$，若 $x_1, x_2, \cdots, x_{n_i} \in S$，则 $g_i(x_1, x_2, \cdots, x_{n_i}) \in S$
3. 只有由（有限次使用）(1) 和 (2) 生成的元素才是 S 中元素。

集合 S 是满足以下 (1) 和 (2) 的 T 中的最小集：

1. $M \subseteq S$
2. 对于任何 $x_1, x_2, \cdots, x_{n_i}$，若 $x_1, x_2, \cdots, x_{n_i} \in T$，则 $g_i(x_1, x_2, \cdots, x_{n_i}) \in T$

归纳证明原理的一般情况

设 S 为上述定义的集合。如果

1. 对于任何 $x \in M$，$R(x)$;
2. 对于任何 $x_1, x_2, \cdots, x_{n_i} \in S$，如果 $R(x_1), R(x_2), \cdots, R(x_{n_i})$，则 $R(g_i(x_1, x_2, \cdots, x_{n_i}))$。

则对于任何 $x \in S$, $R(x)$。

函数递归定义原理的一般情况

设 S 为上述定义的集合。设 $h : M \to S$，$h_i : S^{n_i} \to S$，$i = 1, 2, \cdots, k$，为已知函数。则存在唯一的 S 上的函数 f，使得

- $f(x) = h(x)$，对于任何 $x \in M$，
- $f(g_i(x_1, x_2, \cdots, x_{n_i})) = h_i(f(x_1), f(x_2), \cdots, f(x_{n_i}))$，对于任何 $x_1, x_2, \cdots, x_{n_i} \in S$

经典命题逻辑

- 命题：具有唯一真值的陈述句。
- 联结词（命题运算符）
  - 否定："不"
  - 析取："或"
  - 合取："与"
  - 条件："若...，则..."
  - 双条件："...当且仅当..."
- 复合命题 & 简单命题
- 在命题逻辑中，逻辑形式由联结词决定

命题语言

- 命题语言 $\mathcal{L}^P$ 是经典命题逻辑的形式语言
- 命题语言 $\mathcal{L}^P$ 是符号的集合
  - 命题符号：$p, q, r, \cdots$
  - 联结符号：$\neg, \wedge, \vee, \rightarrow, \leftrightarrow$
  - 标点符号：$(,)$
- 命题语言 $\mathcal{L}^P$ 的含义本质上不涉及语义，而只有语法。

表达式

表达式：$\mathcal{L}^P$ 中有限个符号组成的字符串

- 表达式的长度：表达式中的符号数目
- 空表达式：长度为 0 的表达式，记为 $\emptyset$
- 表达式相等：$U = V$ iff 表达式 U 和 V 中符号依次相同
- 表达式 U 和 V 依次并列形成新的表达式 UV，且 $U\emptyset = \emptyset U = U$
- 若表达式 $U = W_1VW_2$，则 V 是 U 的段。若 V 是 U 的段且 V 和 U 不相等，则 V是 U 的真段。
- 初始段、结尾段、真初始段、真结尾段

公式集的归纳定义

- 并不是所有表达式都是研究对象
- 研究对象必须符合语法
- 原子公式集 $Atom(\mathcal{L}^P) = \{U|U$ 是由单个命题符号构成的表达式$\}$
- 合式公式集 $Form(\mathcal{L}^P)$
  1. $Atom(\mathcal{L}^P) \subseteq Form(\mathcal{L}^P)$
  2. 若 $A \in \mathcal{L}^P$，则 $(\neg A) \in Form(\mathcal{L}^P)$
  3. 若 $A, B \in Form(\mathcal{L}^P)$，则 $(A * B) \in Form(\mathcal{L}^P)$。其中 $*$ 表示 $\wedge, \vee, \rightarrow, \leftrightarrow$ 中的任何一个
  4. A 是能由有限次应用 (1)-(3) 形成的表达式 iff $A \in Form(\mathcal{L}^P)$

公式集的归纳定义

- 合式公式集 $Form(\mathcal{L}^P)$·是满足的以下 (1)-(3) 的 S 中的最小集
  1. $Atom(\mathcal{L}^P) \subseteq S$
  2. 若 $A \in S$，则 $(\neg A) \in S$
  3. 若 $A, B \in S$，则 $(A * B) \in S$。其中 $*$ 表示 $\wedge, \vee, \rightarrow, \leftrightarrow$ 中的任何一个

公式集的归纳证明

定理：设 R 是一个性质，若

1. 对于任何 $p \in Atom(\mathcal{L}^P)$，$R(p)$；
2. 对于任何 $A \in Form(\mathcal{L}^P)$，若 $R(A)$，则 $R((\neg A))$；
3. 对于任何 $A, B \in Form(\mathcal{L}^P)$，若 $R(A)$ 且 $R(B)$，则 $R((A * B))$，其中 $*$ 表示 $\wedge, \vee, \rightarrow, \leftrightarrow$ 中的任何一个；

则对于任何 $A \in Form(\mathcal{L}^P)$，$R(A)$。

公式结构

引理：对于任何 $A \in Form(\mathcal{L}^P)$，有

- A 为不空的表达式。
- A 中的左括号与右括号的数目相同。
- A 的任何不空的真初始段中，左括号的数目比右括号的数目多；A 的任何不空的真结尾段中，左括号的数目比右括号的数目少。

定理

$\mathcal{L}^P$ 的每一公式恰好具有以下 6 种形式之一：原子公式，$(\neg A)$，$(A \wedge B)$，$(A \vee B)$，$(A \to B)$，$(A \leftrightarrow B)$，并且在各种情形公式所具有的那种形式是唯一的。

公式的语法分类

- 原子公式
- 复合公式：设 A, B 为公式，则
    - 否定式：$\neg A$
    - 合取式：$(A \wedge B)$
    - 析取式：$(A \vee B)$
    - 蕴含式：$(A \rightarrow B)$，其中 A 为前件，B 为后件
    - 等值式：$(A \leftrightarrow B)$

辖域

- 设 A, B, C 为公式
- 若 $(\neg A)$ 是 C 的段，则称 A 为它左方的 $\neg$ 在 C 中的辖域
- 若 $(A * B)$ 是 C 的段，则称 A 和 B 分别为它们之间的 $*$ 在 C 中的左辖域和右辖域。其中 $*$ 表示 $\wedge, \vee, \rightarrow, \leftrightarrow$ 中的任何一个。

定理

任何 A 中的任何 $\neg$（如果有）有唯一的辖域；任何 A 中的任何 $*$（如果有）有唯一的左辖域和右辖域

定理

若 A 是 $(\neg B)$ 的段，则 $A = (\neg B)$ 或 A 是 B 的段；若 A 是 $(B * C)$ 的段，则 $A = (B * C)$ 或 A 是 B 的段或 A 是 C 的段

语义

- 函数 v：$\{\mathcal{L}^P$中所有命题符号$\} \to \{1,0\}$，被称为一个真假赋值。
- 真假赋值 v 给公式 A 指派的真假值，记为 A^v。其定义为：
  1. $p^v \in \{0,1\}$
  2. 若 $A^v = 0$，则 $(\neg A)^v = 1$；否则，$(\neg A)^v = 0$
  3. 若 $A^v = B^v = 1$，则 $(A \wedge B)^v = 1$；否则，$(A \wedge B)^v = 0$
  4. 若 $A^v = B^v = 0$，则 $(A \vee B)^v = 0$；否则，$(A \vee B)^v = 1$
  5. 若 $A^v = 1$ 且 $B^v = 0$，则 $(A \to B)^v = 1$；否则，$(A \to B)^v = 1$
  6. 若 $A^v = B^v$，则 $(A \leftrightarrow B)^v = 1$；否则，$(A \leftrightarrow B)^v = 0$
- 这是一个递归定义函数。
- 对于一个公式，列出所有真假赋值指派的真假值，就形成了该公式真值表。

例子

$p \vee q \to \neg q \wedge r$

p	q	r	p	$\vee$	q	$\to$	$\neg$	q	$\wedge$	r
1	1	1	1	1	1	0	0	1	0	1
1	1	0	1	1	1	0	0	1	0	0
1	0	1	1	1	0	1	1	0	1	1
1	0	0	1	1	0	0	1	0	0	0
0	1	1	0	1	1	0	0	1	0	1
0	1	0	0	1	1	0	0	1	0	0
0	0	1	0	0	0	1	1	0	1	1
0	0	0	0	0	0	1	1	0	0	0

公式的语义分类

- 若对于所有 $B \in \Sigma$，$B^v = 1$，则 $\Sigma^v = 1$，否则，$\Sigma^v = 0$。
- Σ 是可满足的，当且仅当存在真假赋值 v，使得 $\Sigma^v = 1$。特别地，若 $\{A\}$ 是可满足的，则称 A 为可满足式。
- A 是重言式，当且仅当对于任何的真假赋值 v， $A^v = 1$。
- A 是矛盾式，当且仅当对于任何的真假赋值 v， $A^v = 0$。

逻辑推论

- 设 $\Sigma \subseteq Form(\mathcal{L}^P)$，$A \in Form(\mathcal{L}^P)$。$A$ 是 Σ 的逻辑推论，记作 $\Sigma \models A$，当且仅当对于任何真假赋值 v，$\Sigma^v = 1$ 蕴涵 $A^v = 1$ ($A^v = 0$ 蕴涵 $\Sigma^v = 0$)
  - $\emptyset \models A$ 表示 A 为重言式。
  - $\models$ 不是 $\mathcal{L}^P$ 中符号。
  - $\Sigma \models A$ 不是公式。
  - A 和 B 是逻辑等值的，即 $A \models B$ 并且 $B \models A$。

逻辑推论

证明：$A \to B, B \to C \models A \to C$。

证法 1：对于任何真假赋值 v，

若 $\{A \to B, B \to C\}^v = 1$。可得

1. $(A \to B)^v = 1$
2. $(B \to C)^v = 1$

若 $A^v = 1$，则由 (1) 可得，$B^v = 1$。再由 (2) 可得，$C^v = 1$。所以，$(A \to C)^v = 1$。

若 $A^v = 0$，则 $(A \to C)^v = 1$。

逻辑推论

证明：$A \to B, B \to C \models A \to C$。

证法 2：设任何真假赋值 v，

若 $\{A \to C\}^v = 0$，可得

1. $A^v = 1$
2. $C^v = 0$

若 $B^v = 1$，则由 (2) 可得，$(B \to C)^v = 0$。所以，$(A \to B, B \to C)^v = 0$。

若 $B^v = 0$，则由 (2) 可得，$(A \to B)^v = 0$。所以，$(A \to B, B \to C)^v = 0$。

定理

- 等值公式替换：如果 B 和 C 逻辑等值，且 A 中将 B 的某些出现替换为 C 而得到 A'，则 A 和 A' 逻辑等值。
- 对偶性：设 A 为 $\mathcal{L}^P$ 的原子公式和联结符号 $\neg, \wedge, \vee$ 使用相关规则而形成的公式。若对 A 中的 $\wedge$ 与 $\vee$，原子公式与它的否定式进行交换而得到 A'（称为 A 的对偶），则 $\neg A$ 和 A' 逻辑等值。

形式可推演

- 用 Σ 表示任何公式集，即 $\Sigma \subseteq Form(\mathcal{L}^P)$。
  - $\Sigma \cup \{A\}$ 可以记为 Σ, A。
  - $\Sigma \cup \Sigma'$ 可以记为 Σ, Σ'。
  - $\Sigma = \{A_1, A_2, \cdots, \}$，则 Σ 可以记为 $A_1, A_2, \cdots$。
- $\Sigma \vdash A$ 表示 A 由 Σ 形式可推演（形式可证明）的。其中，Σ 为前提，A 为结论。
  - $\vdash$ 不是 $\mathcal{L}^P$ 中符号。
  - $\Sigma \vdash A$ 不是公式。
  - $A \vdash\dashv B$ 表示 $A \vdash B$ 并且 $B \vdash A$，并称 A 和 B 是语法等值的。

形式可推演

- 用 Σ 表示任何公式集，即 $\Sigma \subseteq Form(\mathcal{L}^P)$。
  - $\Sigma \cup \{A\}$ 可以记为 Σ, A。
  - $\Sigma \cup \Sigma'$ 可以记为 Σ, Σ'。
  - $\Sigma = \{A_1, A_2, \cdots,\}$，则 Σ 可以记为 $A_1, A_2, \cdots$。
- $\Sigma \vdash A$ 表示 A 由 Σ 形式可推演（形式可证明）的。其中，Σ 为前提，A 为结论。
  - $\vdash$ 不是 $\mathcal{L}^P$ 中符号。
  - $\Sigma \vdash A$ 不是公式。
  - $A \vdash\dashv B$ 表示 $A \vdash B$ 并且 $B \vdash A$，并称 A 和 B 是语法等值的。

命题逻辑的推演规则

共11条，A, B, C 为公式

- (Ref)：$A \vdash A$
- $(+)$：若 $\Sigma \vdash A$，则 $\Sigma, \Sigma' \vdash A$
- $(\neg-)$：若 $\Sigma, \neg A \vdash B$ 且 $\Sigma, \neg A \vdash \neg B$，则 $\Sigma \vdash A$
- $(\to -)$：若 $\Sigma \vdash A \to B$ 且 $\Sigma \vdash A$，则 $\Sigma \vdash B$
- $(\to +)$：若 $\Sigma, A \vdash B$，则 $\Sigma \vdash A \to B$
- $(\wedge-)$：若 $\Sigma \vdash A \wedge B$，则 $\Sigma \vdash A$，$\Sigma \vdash B$

命题逻辑的推演规则

共11条，A, B, C 为公式

- $(\wedge +)$：若 $\Sigma \vdash A$，$\Sigma \vdash B$，则 $\Sigma \vdash A \wedge B$
- $(\vee -)$：若 $\Sigma, A \vdash C$ 且 $\Sigma, B \vdash C$，则 $\Sigma, A \vee B \vdash C$
- $(\vee +)$：若 $\Sigma \vdash A$，则 $\Sigma \vdash A \vee B$，$\Sigma \vdash B \vee A$
- $(\leftrightarrow -)$：若 $\Sigma \vdash A \leftrightarrow B$ 且 $\Sigma \vdash A$，则 $\Sigma \vdash B$；
  若 $\Sigma \vdash A \leftrightarrow B$ 且 $\Sigma \vdash B$，则 $\Sigma \vdash A$
- $(\leftrightarrow +)$：若 $\Sigma, A \vdash B$ 且 $\Sigma, B \vdash A$，则 $\Sigma \vdash A \leftrightarrow B$

形式推演的定义

- A 是在命题逻辑中由 Σ 形式可推演（形式可证明）的，记为 $\Sigma \vdash A$，当且仅当 $\Sigma \vdash A$ 能有限次使用形式推演规则生成。
- 这是一个归纳定义。定义了以下集合：
  $\{\Sigma \vdash A | \Sigma \subseteq Form(\mathcal{L}^P)\check{}A \in Form(\mathcal{L}^P)\}$
- 关于归纳证明（定理2.6.2）
- 一个有限序列 $\Sigma_1 \vdash A_1, \Sigma_2 \vdash A_2, \cdots, \Sigma_n \vdash A_n$ 被称为 $\Sigma_n \vdash A_n$ 的形式证明。其中， $\Sigma_k \vdash A_k, (1 \leq k \leq n)$ 由使用某一推演规则而生成。

$\in$ 规则

证明：$A, \Sigma \vdash A$。

证：

1. $A \vdash A$ (Ref)
2. $A, \Sigma \vdash A$ $(+)(1)$

例子

证明：$\neg A \to B \vdash \neg B \to A$。

证：

1. $\neg A \to B, \neg B, \neg A \vdash \neg A \to B$ $\quad (\in)$
2. $\neg A \to B, \neg B, \neg A \vdash \neg A$ $\quad (\in)$
3. $\neg A \to B, \neg B, \neg A \vdash B$ $\quad (\to -)(1)(2)$
4. $\neg A \to B, \neg B, \neg A \vdash \neg B$ $\quad (\in)$
5. $\neg A \to B, \neg B, \vdash \neg A$ $\quad (\neg -)(3)(4)$
6. $\neg A \to B \vdash \neg B \to A$ $\quad (\to +)(5)$

Tr 规则

证明：若 $\Sigma \vdash \Sigma'$，$\Sigma' \vdash A$，则 $\Sigma \vdash A$。

证：

1. $\Sigma' \vdash A$ (前提)
2. $A_1, A_2, \cdots, A_n \vdash A$，其中 $A_1, A_2, \cdots, A_n \in \Sigma'$ (定理2.6.2)(1)
3. $\Sigma, A_1, A_2, \cdots, A_n \vdash A$ $(+)(2)$
4. $\Sigma, A_1, A_2, \cdots, A_{n-1} \vdash A_n \to A$ $(\neg+)(3)$
5. $\Sigma \vdash A_n$ (前提)
6. $\Sigma, A_1, A_2, \cdots, A_{n-1} \vdash A$ $(\neg-)(4)(5)$
7. $\Sigma \vdash A$ (同理(6))

例子

证明：$A \to B, B \to C \vdash A \to C$。

证：

1. $A \to B, B \to C, A \vdash A \to B$ $(\in)$
2. $A \to B, B \to C, A \vdash A$ $(\in)$
3. $A \to B, B \to C, A \vdash B$ $(\to -)(1)(2)$
4. $A \to B, B \to C, A \vdash B \to C$ $(\in)$
5. $A \to B, B \to C, A \vdash C$ $(\to -)(4)(3)$
6. $A \to B, B \to C \vdash A \to C$ $(\to +)(5)$

例子

证明：$A \to (B \to C), A \to B \vdash A \to C$。

证：

1. $A \to (B \to C), A \to B, A \vdash A \to (B \to C)$ $(\in)$
2. $A \to (B \to C), A \to B, A \vdash A$ $(\in)$
3. $A \to (B \to C), A \to B, A \vdash B \to C$ $(\to -)(1)(2)$
4. $A \to (B \to C), A \to B, A \vdash A \to B$ $(\in)$
5. $A \to (B \to C), A \to B, A \vdash B$ $(\to -)(4)(2)$
6. $A \to (B \to C), A \to B, A \vdash C$ $(\to -)(3)(5)$
7. $A \to (B \to C), A \to B \vdash A \to C$ $(\to +)(6)$

例子

证明：$\neg\neg A \vdash A$。

证：

1. $\neg\neg A, \neg A \vdash \neg A$ $(\in)$
2. $\neg\neg A, \neg A \vdash \neg\neg A$ $(\in)$
3. $\neg\neg A \vdash A$ $(\neg-)(1)(2)$

$(\neg+)$ 归谬律

证明：若 $\Sigma, A \vdash B$，$\Sigma, A \vdash \neg B$，则 $\Sigma \vdash \neg A$。

证：

1. $\Sigma, \neg\neg A \vdash \Sigma$ $\qquad (\in)$
2. $\neg\neg A \vdash A$ $\qquad$ (已证)
3. $\Sigma, \neg\neg A \vdash A$ $\qquad (+)(2)$
4. $\Sigma, A \vdash B$ $\qquad$ (前提)
5. $\Sigma, \neg\neg A \vdash B$ $\qquad (\mathrm{Tr})(1)(3)(4)$
6. $\Sigma, A \vdash \neg B$ $\qquad$ (前提)
7. $\Sigma, \neg\neg A \vdash \neg B$ $\qquad (\mathrm{Tr})(1)(3)(6)$
8. $\Sigma \vdash \neg A$ $\qquad (\neg-)(5)(7)$

例子

证明：$A \vdash \neg\neg A$。

证：

1. $A, \neg A \vdash A$ $(\in)$
2. $A, \neg A \vdash \neg A$ $(\in)$
3. $A \vdash \neg\neg A$ $(\neg+)(1)(2)$

范式

- 单式
  - 原子公式和原子公式的否定称为单式。
- 析（合）取子式
  - 以单式为析（合）取项的析（合）取式称为析（合）取子式。
- 析取范式
  - 以合取子式为析取项的析取式称为析取范式。
- 合取范式
  - 以析取子式为合取项的合取式称为合取范式。
- 主析取范式和主合取范式

例子

求 $(p \to q) \wedge r$ 的析取范式和合取范式

解:

$$
\begin{aligned}
& (p \to q) \wedge r \\
\Leftrightarrow\ & (\neg p \vee q) \wedge r \\
\Leftrightarrow\ & (\neg p \wedge r) \vee (q \wedge r) \\
\Leftrightarrow\ & (\neg p \vee q) \wedge (r \vee q) \wedge (\neg p \wedge r) \wedge r
\end{aligned}
$$

翻译

符号化下列命题，并进行推理。

公安人员审查一件盗窃案，事实如下：

- 张平或王磊盗窃了机房的计算机一台；
- 若张平盗窃了计算机，则作案时间不可能发生在午夜之前；
- 若王磊的证词正确，则午夜时机房里的灯未灭；
- 若王磊的证词不正确，则作案时间发生在午夜之前；
- 午夜时机房的灯光灭了。

问：谁盗窃了该台计算机。

翻译

- p：张平盗窃了机房的计算机一台。
- q：王磊盗窃了机房的计算机一台。
- r：作案时间发生在午夜之前。
- s：王磊的证词正确。
- t：午夜时机房的灯光灭了。

例子

$p \vee q, p \to \neg r, s \to \neg t, \neg s \to r, t \vdash ?$

1. $p, \neg q \vdash p$ $(\in)$
2. $p, \neg q, \neg p \vdash \neg q$ $(\in)$
3. $p, \neg q, \neg p \vdash q$ $(\in)$
4. $p, \neg q \vdash p$ $(\neg -)(2)(3)$
5. $p \vee q, \neg q \vdash p$ $(\vee -)(1)(4)$
6. $p \vee q, \neg q, p \to \neg r \vdash p$ $(+)(5)$
7. $p \vee q, \neg q, p \to \neg r \vdash p \to \neg r$ $(\in)$
8. $p \vee q, \neg q, p \to \neg r \vdash \neg r$ $(\to -)(6)(7)$

例子

$p \vee q, p \to \neg r, s \to \neg t, \neg s \to r, t \vdash ?$

9. $s \to \neg t, \neg s \to r, s, t \vdash s$ $(\in)$
10. $s \to \neg t, \neg s \to r, s, t \vdash s \to \neg t$ $(\in)$
11. $s \to \neg t, \neg s \to r, s, t \vdash \neg t$ $(\to -)(9)(10)$
12. $s \to \neg t, \neg s \to r, s, t \vdash t$ $(\in)$
13. $s \to \neg t, \neg s \to r, t \vdash \neg s$ $(\neg +)(11)(12)$
14. $s \to \neg t, \neg s \to r, t \vdash \neg s \to r$ $(\in)$
15. $s \to \neg t, \neg s \to r, t \vdash r$ $(\to -)(13)(14)$
16. $p \vee q, p \to \neg r, s \to \neg t, \neg s \to r, t, \neg q \vdash \neg r$ $(+)(8)$
17. $p \vee q, p \to \neg r, s \to \neg t, \neg s \to r, t, \neg q \vdash r$ $(+)(15)$
18. $p \vee q, p \to \neg r, s \to \neg t, \neg s \to r, t \vdash q$ $(\neg -)(16)(17)$