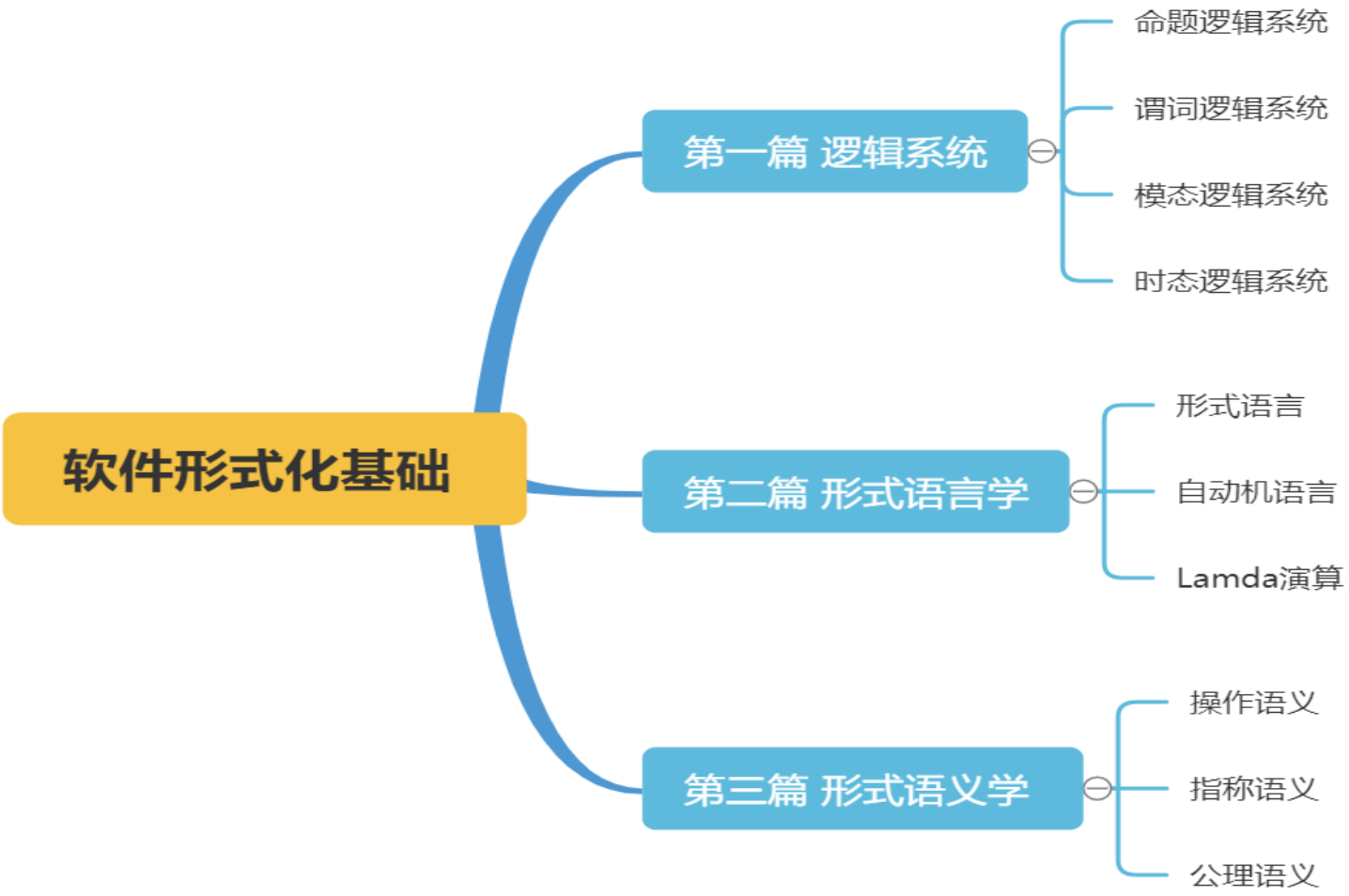
软件理论基础


软件形式化基础
第一篇 逻辑系统
命题逻辑系统
谓词逻辑系统
模态逻辑系统
时态逻辑系统
第二篇 形式语言学
形式语言
自动机语言
Lamda演算
第三篇 形式语义学
操作语义
指称语义
公理语义

Course Outline

- 软件理论基础框架
- 命题逻辑
  - 命题逻辑框架
  - 命题逻辑特质
  - 命题逻辑的证明系统
- 一阶谓词逻辑
  - 一阶谓词逻辑框架
  - 一阶谓词逻辑特质
  - 一阶谓词逻辑的证明系统
- 模态逻辑
  - 模态逻辑语法
  - 模态逻辑语义结构
  - 模态逻辑的推理理论
- 时态逻辑
  - 时态逻辑语法
  - 时态逻辑语义结构
  - 时态逻辑的推理理论

Course Outline

- Lambda演算
  - Lambda演算规则
  - Lambda演算应用
- 操作语义
  - 操作语义规则
  - 操作语义应用

软件理论基础：逻辑篇

为什么要学习逻辑？

数理逻辑是一门以**数学方法**为基础，用**符号系统**的形式来研究思维结构及规律的学科.

- 数理逻辑在计算机软件硬件设计中的应用
  - 开关电路---布尔代数
  - 搜索引擎---索引
  - 关系数据库 ---谓词逻辑
  - ……

为什么要学习逻辑？

数理逻辑是**规范语言、定理证明器、模型检测器**的基础

$$\mathcal{M} \models \phi$$

其中，$\mathcal{M}$-模型；ϕ--规范语言（用户需求），以逻辑的形式表示。

中心：设计好的算法计算$\models$

题外话—学得东西都是有用的

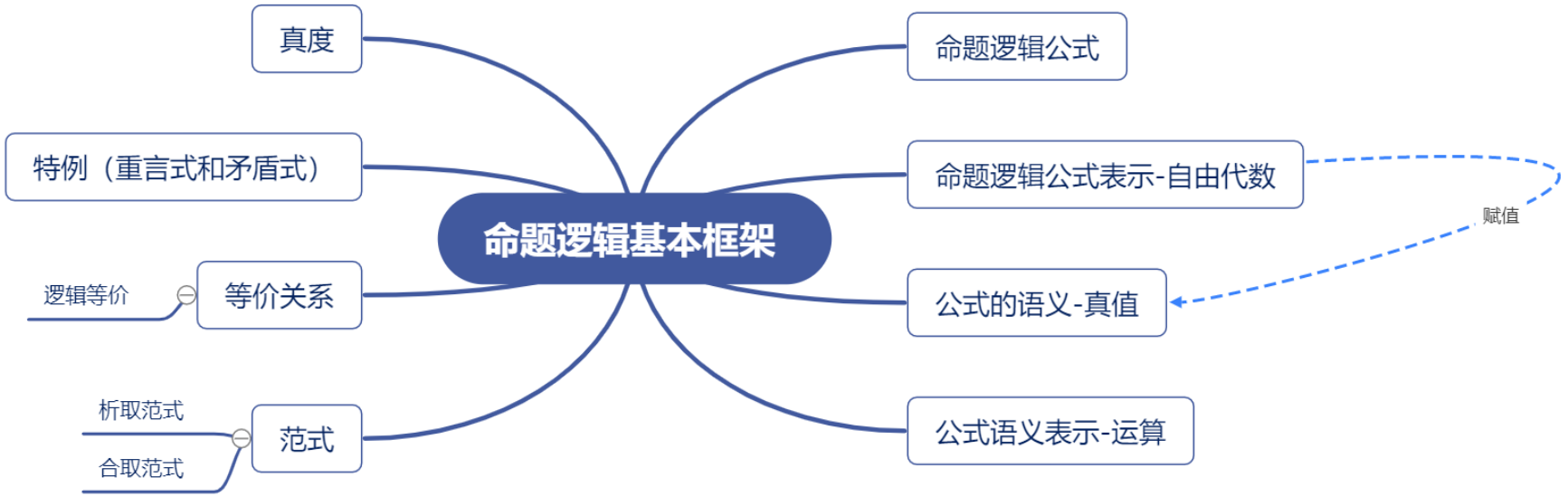
1. Google 2002年推出了自己的``新闻"服务。和传统媒体的做法不同，这些新闻不是记者写的，也不是人工编辑的，而是由计算机整理、分类和聚合各个新闻网站的内容，一切都是自动生成的。这里面关键的技术就是新闻的自动分类----**背后的数学（余弦定理）**

2. Google的网页排名技术。其``PageRank"网页排名算法是革命性的发明--公认的文献检索中最大的贡献之一，有人甚至认为整个公司的成功都是基于这个算法。创始人：拉里.佩奇、谢尔盖.布林. 佩奇也是因为这个算法在30岁时当选为美国工程院院士,是继乔布斯, 盖茨之后有一位当院士的辍学生. 其背后的数学---**线性代数**.

中国的大部分软件工程师在一个未知领域都是从直观感觉出发,用``凑"的方法来解决问题,说的不好听,就是山寨. Google招揽理论基础优异的工程师.-----吴军《数学之美》

命题逻辑系统

命题逻辑系统


真度
特例（重言式和矛盾式）
逻辑等价
等价关系
析取范式
合取范式
范式
命题逻辑基本框架
命题逻辑公式
命题逻辑公式表示-自由代数
赋值
公式的语义-真值
公式语义表示-运算

命题逻辑系统的语法结构

- 如何构造命题逻辑公式？

定义：命题是陈述句

陈述句可以分为

- 简单句
- 复合句： 简单句+连接词

陈述句有真假之分： 陈述句表达的含义是真或假。

- 命题： 简单命题，复合命题
- 真命题和假命题
- 命题变元： 表示命题的变元， 用字母$p, q, \ldots\ldots, p_1, p_2, \ldots\ldots$表示。
- 复合命题： 命题变元+连接符组合

命题逻辑公式

- 字母表
- 命题变元: $p, q, \ldots\ldots, p_1, p_2, \ldots\ldots$表示
- 连接符： $\wedge, \vee, \rightarrow, \neg,$
- 辅助符：), (,
- 命题逻辑公式 用符号A表示：

$$A::=p|A\wedge A|\mathrm{A}\vee A|\neg A|A\longrightarrow A$$

定义　　设$S=\{p_1，\ p_2, \ldots, p_n, \ldots\ldots\}$是命题变元集,

F(S)表示S上的命题公式集， 其元素用A表示，其归纳定义如下：

- $S\subseteq F(S)$, 即， 每个命题变元都是命题逻辑公式，称为原子命题公式
- 若$A, B\in F(S)$， 则 $\neg\mathrm{A}, \mathrm{A}\wedge\mathrm{B}, \mathrm{A}\vee\mathrm{B}, \mathrm{A}\longrightarrow\mathrm{B}\in\mathrm{F(S)}$。

注:F(S)是S生成的$(\neg,\wedge,\vee,\longrightarrow)$型 的自由代数。

例子：下列都是命题公式

$$p_1 \to p_2, (p_1 \to p_2) \vee (p_2 \wedge \neg p_3), \neg p_1 \to p_2$$

但这些都不是命题逻辑公式： $p_1 \to$， $((p_2 \wedge)$ $\vee p_3)$

命题逻辑系统的语义结构

命题有真假含义之分，

即有真命题和假命题之分。用$1(T)$表示真值真，

而$0(F)$表示真值假。

真值

- 原子命题公式的真值可以指定为真或假

定义　真值指派是指对命题变元指定真值，即S到$\{0,1\}$的一个映射.

例子：考虑命题变元p_1, p_2, p_3, p_4. 真值组$(0,1,1,0)$是p_1, p_2, p_3, p_4的一个真值指派。

- 命题逻辑的连接符构成了一个真值$\{0,1\}$上的一元或二元运算:

1. 一元运算$\neg$:

$$\begin{array}{rccc} \neg: & \{0,1\} & \longrightarrow & \{0,1\} \\ & 0 & \mapsto & 1 \\ & 1 & \mapsto & 0 \end{array}$$

2. 二元运算$\wedge$:

$$\begin{array}{rccc} \wedge: & \{0,1\}^2 & \longrightarrow & \{0,1\} \\ & (0,0) & \mapsto & 0 \\ & (0,1) & \mapsto & 0 \\ & (1,0) & \mapsto & 0 \\ & (1,1) & \mapsto & 1 \end{array}$$

真值

3. 二元运算$\vee$:

$$\begin{array}{rccc} \vee: & \{0,1\}^2 & \longrightarrow & \{0,1\} \\ & (0,0) & \mapsto & 0 \\ & (0,1) & \mapsto & 1 \\ & (1,0) & \mapsto & 1 \\ & (1,1) & \mapsto & 1 \end{array}$$

4. 二元运算$\rightarrow$:

$$\begin{array}{rccc} \rightarrow: & \{0,1\}^2 & \longrightarrow & \{0,1\} \\ & (0,0) & \mapsto & 1 \\ & (0,1) & \mapsto & 1 \\ & (1,0) & \mapsto & 0 \\ & (1,1) & \mapsto & 1 \end{array}$$

- 由命题变元的真值指派以及连接符所确定的真值运算可得到命题逻辑公式的真值.

如：给定命题变元p_1, p_2, p_3, p_4.

真值

公式	$(0,1,1,0)$	$(1,1,0,1)$	$(1,1,1,1)$
$(p_1 \to p_2) \vee p_3$	1	1	1
$\neg(p_1 \wedge p_3) \to p_4$	0	1	1
$p_1 \to p_1$			
$(p_5 \wedge p_2) \to p_1$	×	×	×

赋值

定义　$F(S)$的一个赋值v是一个映射$F(S) \longrightarrow \{0,1\}$, 并满足下面条件：

1. $v(\neg A) = \neg v(A)$
2. $v(A \vee B) = v(A) \vee v(B)$
3. $v(A \wedge B) = v(A) \wedge v(B)$
4. $v(A \to B) = v(A) \to v(B)$.

用符号Ω表示所有赋值集.

注1：同态映射—

注2：定义中等式中左边符号$\wedge, \vee, \neg, \to$是命题逻辑连接符，而右边符号$\wedge, \vee, \neg, \to$是真值集$\{0,1\}$上的一元或二元运算。

注3：这是归纳定义：定义复杂公式的赋值是通过复杂公式中的简单公式的赋值经过运算得到。因此，复杂公式的赋值完全命题变元的赋值确定。

如：计算公式$(p_1 \to p_2) \to p_3$的赋值：$v((p_1 \to p_2) \to p_3) = (v(p_1) \to v(p_2)) \to v(p_3)$.

赋值

注4：假设A含有n个命题变元，则A的赋值有2^n个。

定理　赋值可以诱导一个真值指派，而真值指派也可以诱导一个赋值。

证明：设v是$F(S)$上的一个赋值，即v是$F(S)$到$\{0,1\}$的一个函数。由于命题变元集S是$F(S)$的一个子集，因此，v在S上的限制$v|_S$是命题变元的真值指派。反之，设V是S的一个真值指派，则V可以诱导一个$F(S)$的赋值v_V:

设$A \in F(S)$, 若A是命题变元p，则定义$v_V(p) = V(p)$. 若A是一个复合公式$A_1 \vee A_2$，则定义$v_V(A) = v_V(A_1) \vee v_V(A_2)$. 类似地，定义其他的三种复合公式$A$是$A_1 \wedge A_2$, $A_1 \to A_2$以及$\neg A_1$情形。这样定义的映射v_V是$F(S)$的一个赋值。 □

真度

定义　设逻辑公式A含有n个命题变元，设$T(A)=\{v\in\Omega\mid v(A)=1\}$. 公式$A$的真度$\tau(A)$定义为：

$$\tau(A)=\frac{|T(A)|}{2^n}.$$

例子：计算$\tau(p_1\to p_2),\tau(p_1\vee p_2),\tau(p_1\wedge p_2),\tau(\neg p)$.
$\tau((p_1\to p_2)\to p_1)$.

注：说明$F(S)$中每个公式的真度都是一个以2的方幂为分母的非负数。反过来，是不是每个这种分数都是$F(S)$中的某个公式呢？回答是肯定的，见下面定理。

定理　设$H=\{\tau(A)\mid A\in F(S)\}$，则

$$H=\{\frac{k}{2^n}\mid k=0,1,\cdots,2^n;n=1,2,\cdots\}.$$

重言式与矛盾式

定义　设$A \in F(S)$,若$\tau(A) = 1$，则称A为重言式（永真式），若$\tau(A) = 0$则称A为矛盾式（永假式）.用符号$\models A$表示A是重言式.

例子：永真式$p \to p$, 矛盾式$p \wedge \neg p$。

注：（1）上述定义等价于：设$A \in F(S)$,若对每个赋值$v \in \Omega$ 都有$v(A) = 1$，则称A为重言式（永真式），若对每个赋值$v \in \Omega$ 都有$v(A) = 0$，则称A为矛盾式（永假式）。

（2）在计算机科学中，若$\models A$，则称A是**有效的**；若**存在**一个赋值$v \in \Omega$使得$v(A) = 1$,则称A是**可满足的**。显然有效蕴含可满足。

（3）A是可满足的当且仅当$\neg A$ 是无效的。

例子：$p \vee q \to p$的有效性和可满足性。

逻辑等价与真值等价

定义 设$A, B \in F(S)$，若对于$v \in \Omega$都有$v(A) = v(B)$，则称A与B是逻辑等价的，记作$A = B$.

例子：$A \vee B = \neg A \to B$, $A \to B = \neg(A \wedge \neg B)$.

定理 $\{\neg, \to\}, \{\neg, \vee\}, \{\neg, \wedge\}$是连接符集$\{\neg, \vee, \wedge, \to\}$的充足集。

定理 性质：

交换律	$A \vee B = B \vee A$	$A \wedge B = B \wedge A$
结合律	$A \vee (B \vee C) = (A \vee B) \vee C$	$A \wedge (B \wedge C) = (A \wedge B) \wedge C$
分配律	$A \vee (B \wedge C) = (A \vee B) \wedge (A \vee C)$	$A \wedge (B \vee C) = (A \wedge B) \vee (A \wedge C)$
de Morgan律	$\neg(A \vee B) = \neg A \wedge \neg B$	$\neg(A \wedge B) = \neg A \vee \neg B$
吸收律	$A \vee (A \wedge B) = A$	$A \wedge (A \vee B) = A$
幂等律	$A \vee A = A$	$A \wedge A = A$
对合律	$\neg\neg A = A$	

范式

定义

- （标准）析取范式：$(Q_{11} \wedge Q_{12} \wedge \cdots Q_{1n}) \vee \cdots \vee (Q_{m1} \wedge Q_{m2} \wedge \cdots \wedge Q_{mn})$,
- （标准）合取范式：$(Q_{11} \vee Q_{12} \vee \cdots Q_{1n}) \wedge \cdots \wedge (Q_{m1} \vee Q_{m2} \vee \cdots \vee Q_{mn})$,

其中Q_{ij}或是命题变元，或是命题变元的非。

定理　任何非矛盾式的公式都逻辑等价于一个析取范式，
任何非重言式的公式都逻辑等价于一个合取范式.

注：限制条件实际都可以去掉。因为矛盾式逻辑等价于一个析取范式$\neg p \wedge p$; 重言式逻辑等价于一个合取范式$\neg p \vee p$.

例子

$$(p \to \neg q) \to (q \vee \neg p)$$

的合取范式和吸取范式。

范式

p	q	$\neg p$	$\neg q$	$p \to \neg q$	$q \vee \neg p$	$(p \to \neg q) \to (q \vee \neg p)$
1	1	0	0	0	1	1
1	0	0	1	1	0	0
0	1	1	0	1	1	1
0	0	1	1	1	1	1

合取范式：$\neg p \vee q$

析取范式：$(p \wedge q) \vee (\neg p \wedge q) \vee (\neg p \wedge \neg q)$

(1)合取范式考虑计算结果为FALSE, 析取范式考虑计算结果TRUE.

(2)合取范式作用是方便有效性检查：$\models \varphi$。其中：$\varphi = (Q_{11} \vee Q_{12} \vee \cdots Q_{1n}) \wedge \cdots \wedge (Q_{m1} \vee Q_{m2} \vee \cdots \vee Q_{mn})$，$Q_{ij}$或是命题变元，或是命题变元的非。等价于$\models Q_{i1} \vee Q_{m2} \vee \cdots \vee Q_{in}\ (i = 1, \cdots, m)$。

(3) $\models Q_{i1} \vee Q_{m2} \vee \cdots \vee Q_{in}$ 是有效的当且仅当存在$1 \leq k, j \leq n$使得Q_{ik} 是$\neg Q_{ij}$.

课堂练习一

1. 证明下列公式是重言式:

(a) $A \to (\neg A \to B)$

(b) $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$

2. 证明下列各条成立

(a) $(A \vee B) \to C = (A \to C) \wedge (B \to C)$


命题逻辑的推理机制
公理
推理规则
定理
推演
推演方法
三段论规则
可证等价关系
子式替换定理

命题逻辑系统的推理机制

建立命题逻辑系统的推理机制，由公理和推理规则组成，回答一个公式是否可以由其他公式推出，即是否其他公式的结论？

形式系统

定义： 命题逻辑形式系统L：命题逻辑公式集$F(S)$+三条公理L_1, L_2, L_3，+一条推理规则MP。

- 三条公理：

  L1: $A \to (B \to A)$

  L2: $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$

  L3: $(\neg A \to \neg B) \to (B \to A)$

- 一条推理规则: Modus Ponens 规则（MP规则），分离规则

  MP：从$A \to B$与A可以得到B.

$$\frac{A, A \to B}{B}$$

注：L1, L2, L3是公理模式，由此可以得到无穷多个公理，如: $(p \to (q \to p)), (p \to (p \to p)), (p \to ((q \vee r) \to p)$ 都是公理。

L中的证明与定理

定义　L 中的一个证明是一有限公式序列$A_1, A_2, \cdots, A_n$,其中每个A_i或是公理，或存在$j, k < i$使得A_i是A_j和A_k使用MP规则推导的结果。其中最后一项公式A_n称为L中的一个定理，记作$\vdash_L A_n$ 或$\vdash A_n$. n叫做证明的长度。

注：定理可当公理使用与证明中：
若有限公式序列$A_1, A_2, \ldots, A_n$中每个A_i 或是公理，或是定理，或是存在$j, k < i$ 使得A_i是A_j和A_k使用MP规则推导的结果，则$A_1, A_2, \ldots, A_n$是一个证明。

例子：证明：

1. $\vdash (p_1 \to p_2) \to (p_1 \to p_1)$
2. $\vdash (A \to A)$

推演

定义 设$\Gamma \subset F(S)$, 从Γ 出发的L 中一个推演是一有限公式序列$A_1, A_2, \cdots, A_n$,其中每个A_i或是公理，或是Γ中成员，或存在$j, k < i$使得A_i是A_j和A_k使用MP规则推导的结果。其中最后一项公式A_n称为Γ-结论，记作$\Gamma \vdash_L A_n$ 或$\Gamma \vdash A_n$. n叫做推演的长度。

注：当$\Gamma = \emptyset$时，Γ-结论就是定理，即$\emptyset \vdash A$ 就是$\vdash A$.

例子：证明: $\{A, B \to (A \to C)\} \vdash B \to C$

定理 (演绎定理)

设$\Gamma \subset F(S), A, B \in F(S)$.则$\Gamma \cup \{A\} \vdash B$ 当且仅当$\Gamma \vdash A \to B$.

证明：”$\Rightarrow$”设$\Gamma \cup \{A\} \vdash B$，则有一个从$\Gamma \cup \{A\}$ 得到B的推演。

$$\begin{array}{ll} (1) & A_1 \\ (2) & A_2 \\ \vdots & \vdots \\ (n) & A_n \end{array}$$

其中A_n就是B.

对推演长度n使用数学归纳法，构造$\Gamma \vdash A \to B$的推演.

证明步骤：

1. 奠基步：$n=1$ 此时，B或是公理，或是Γ中成员，或是A。

(a) B是公理，

(1)	B	公理
(2)	$B \to (A \to B)$	$L1$
(3)	$A \to B$	$MP(1,2)$

所以$\vdash A \to B$，进而$\Gamma \vdash A \to B$.

(b) $B \in \Gamma$

(1)	B	Γ
(2)	$B \to (A \to B)$	$L1$
(3)	$A \to B$	$MP(1,2)$

所以$\Gamma \vdash A \to B$.

(c) B就是A.

因为$\vdash A \to A$，所以$\vdash A \to B$.

2. 归纳步：假定当推演长度小于n是结论成立，即当$\Gamma \cup \{A\} \vdash B$的推演长度小于$n$时，都有$\Gamma \vdash A \to B$成立。现假定$\Gamma \cup \{A\} \vdash B$的推演长度等于$n$.从而有$\Gamma \cup \{A\} \vdash B$的推演：

$$\begin{array}{ll} (1) & A_1 \\ (2) & A_2 \\ \vdots & \vdots \\ (n) & A_n(\text{就是}B) \end{array}$$

当B是公理，或是Γ中成员，或是A时，从前面的证明可以得到$\Gamma \vdash A \to B$. 因此，我们直接假定B 是两项C与$C \to B$使用MP规则得到,即存在$i, j < n$使得A_i是C，而A_j是$C \to B$，如下所示：

$$\begin{array}{ll} (1) & A_1 \\ (2) & A_2 \\ \vdots & \vdots \\ (i) & A_i(C) \\ \vdots & \vdots \\ (j) & A_j(C \to B) \\ \vdots & \vdots \\ (n) & A_n(B) \end{array}$$

由此有$\Gamma \cup \{A\} \vdash C$ 以及$\Gamma \cup \{A\} \vdash C \to B$，它们的推演长度分别是$i$和$j$，都小于$n$。故而，由归纳假设得到$\Gamma \vdash A \to C$

与$\Gamma \vdash A \to (C \to B)$都成立。因而，可得到推演：

$$
\begin{array}{lll}
(1) & & \\
\vdots & & (\Gamma \vdash A \to C) \\
(k) \quad A \to C & & \\
(k+1) & & \\
\vdots & & (\Gamma \vdash A \to (C \to B)) \\
(l) \quad A \to (C \to B) & & \\
(l+1) \quad (A \to (C \to B)) \to ((A \to C) \to (A \to B)) & & L2 \\
(l+2) \quad (A \to C) \to (A \to B) & & MP(l, l+1) \\
(l+3) \quad A \to B & & MP(k, l+2)
\end{array}
$$

所以，我们得到了$\Gamma \vdash A \to B$.

”$\Leftarrow$”设$\Gamma \vdash A \to B$，则存在一推演：

$$
\begin{array}{ll}
(1) & A_1 \\
(2) & A_2 \\
\vdots & \vdots \\
(n) & A_n (A \to B)
\end{array}
$$

其中，每个A_i或是公理，或是Γ中成员，或存在 $j,k<i$ 使得A_i是A_j和A_k使用规则MP得到。

在这个推演基础上构造一个序列如下：

$$
\begin{array}{lll}
(1) & A_1 & \\
(2) & A_2 & \\
\vdots & \vdots & \\
(n) & A_n(A \to B) & \\
(n+1) & A & (\text{假设}) \\
(n+2) & B & MP(n, n+1)
\end{array}
$$

这个序列是$\Gamma \cup \{A\}$到B的一个推演，故有，$\Gamma \cup \{A\} \vdash B$. □

注：使用演绎定理可以简化证明。

例子：证明：$\vdash A \to A$.

例子：证明：$\vdash \neg A \to (A \to B)$.

HS规则：

定理　(三段论规则–HS规则)

$\{A \to B, B \to C\} \vdash A \to C.$

证明：构造推演序列如下：

(1)	$A \to B$	Γ
(2)	$B \to C$	Γ
(3)	A	假设
(4)	B	$MP(1,3)$
(5)	C	$MP(2,4)$

所以有，$\{A, A \to B, B \to C\} \vdash C$.这样，由演绎定理得到，$\{A \to B, B \to C\} \vdash A \to C$. □

推论　设$\vdash A \to B$ 且$\vdash B \to C$，则$\vdash A \to C$.

可证等价关系：

定义　设$A, B \in F(S)$，若$\vdash A \to B$且$\vdash B \to A$成立，则称A与B可证等价,记作$A \approx B$.

例子：设$A \in F(S)$，则$\neg\neg A \approx A$.

例子：设$A, B \in F(S)$，则$(A \to B) \approx (\neg B \to \neg A)$.

证明：由L3得到$\vdash (\neg B \to \neg A) \to (A \to B)$. 现在需要证明$\vdash (A \to B) \to (\neg B \to \neg A)$. 由演绎定理只须证明$\{A \to B\} \vdash (\neg B \to \neg A)$.

定理　可证等价关系$\approx$是$F(S)$上的同余关系.

证明：

1. $\approx$ 是$F(S)$上的等价关系.
2. $\approx$对$F(S)$的逻辑运算非$\neg$是同余的,即若$A \approx B$则$\neg A \approx \neg B$.
3. $\approx$对$F(S)$的逻辑运算$\to$是同余的,即若$A \approx B$且$C \approx D$，则$(A \to C) \approx (B \to D)$.

□

子式替换定理

定理　设A中含有子式A_1，且$A_1 \approx B_1$,若A中的一处或多处出现的A_1换成B_1所得的公式记为B，则有$A \approx B$.

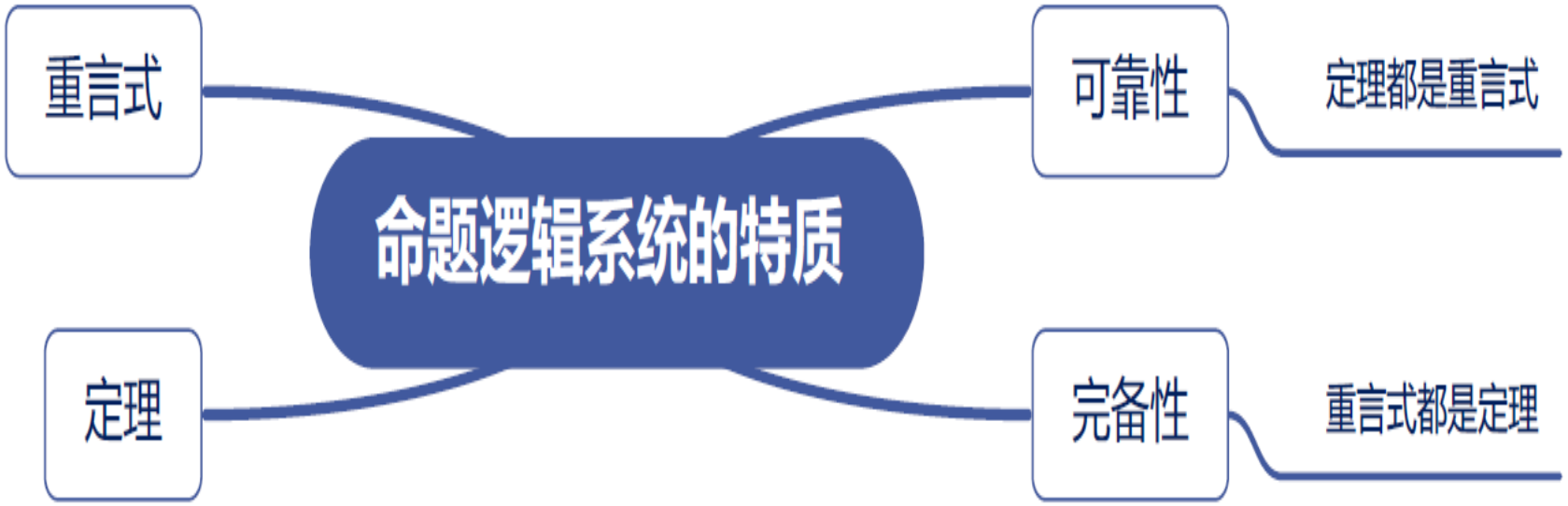
课堂练习二

(1). 试证：

1. $\vdash A \to (B \to (A \to B))$.

(2) 试证：

1. $(A \to (B \to C)) \approx (B \to (A \to C))$


命题逻辑系统的特质
重言式
定理
可靠性
定理都是重言式
完备性
重言式都是定理

命题逻辑系统的可靠性与完备性

给定命题变元集S，使用逻辑连接词$\neg, \vee, \wedge, \rightarrow$构造$S$上的命题逻辑公式集$F(S)$，它是$S$上的$(\neg, \vee, \wedge, \rightarrow\}$型的自由代数，在赋值语义考虑下有逻辑公式真度以及重言式概念，符号$\models A$表明命题逻辑公式A是重言式，而从逻辑推理考虑下有证明和定理概念，符号$\vdash A$表明A是一个定理。本段解决$\vdash A$与$\models A$的关系：

$$\forall A \in F(S), \models A \text{ 当且仅当} \vdash A.$$

(1) 反映了“可证”和“真”之间的关系。通常“真”大于“可证”，但在命题逻辑中二者一致。

(2)希尔伯特的第二问题：算术公理系统的无矛盾性。希尔伯特提出用形式主义计划的证明论方法加以证明。

(3)哥德尔不完全性定理：“20世纪最有意义的数学真理”

第一定理：任意一个包含一阶谓词逻辑与初等数论的形式系统，都存在一个命题，它在这个系统中既不能被证明为真，也不能被证明为否。说明了“真”大于“可证”。

第二定理：如果系统S含有初等数论，当S无矛盾时，它的无矛盾性不可能在S内证明。

命题逻辑系统的可靠性

定理　(可靠性定理) 命题逻辑系统L中的定理都是重言式，即

$$若\vdash A则\models A.$$

证明：依赖于下面两个引理.

(1) L中的公理都是重言式。

(2)MP规则保重言式，即设$A, B \in \mathcal{F}(S)$.如果$A \to B \in Tau$且$A \in Tau$,则$B \in Tau$.

□

命题逻辑系统的完备性

命题逻辑系统L的完备性证明需要一些准备工作.

引理　$\vdash (\neg A \to A) \to A.$

定义　(扩张)

设L^*是系统L的基础上改变L的公理或给L添加新的公理而得到的系统，若L中的定理都是L^*的定理,则称L^*是L的扩张.

例子：在L中增加新公理$A \to A$得到L的一个扩张L^*. 但L的定理与L^*的定理相同.

例子：在L中增加新公理$A \to \neg A$得到L的一个扩张L^*, L^*是L的真扩张，因为$A \to \neg A$不是L的定理，但是L^*的定理.

例子：设$A \in F(S)$，若A不是L中的定理，增加公理$\neg A$则得到L的扩张L^*。

注：L是其自身的扩张。

相容性

定义　L的扩张L^*称为相容的，若$F(S)$中不存在公式A使得A与$\neg A$都是L^*的定理。

例子：L是相容的。

引理　L的扩张L^*是相容的当且仅当$F(S)$中有一公式不是L^*中的定理.

证明：$\Rightarrow$设L^*是相容的，若再设$F(S)$中的任何公式都是L^*的定理，则对于任何的公式A都有A与$\neg A$均是L^*的定理，与L^*的相容性矛盾。

$\Leftarrow$ 设L^*是不相容的，则存在公式$A \in F(S)$使得A和$\neg A$均是L^*中的定理。下面证明$F(S)$中的任何公式B都是L^*的定理。

完全性

定义　系统L的扩张S称为完全的，若对$F(S)$中的每个公式A都有$\vdash_S A$或$\vdash_S \neg A$成立.

注：系统L是不完全的，因为$\vdash_L p$与$\vdash_L \neg p$均不成立.

引理　相容系统L^*都有一个相容的完全扩张S.

证明：设相容系统L^*是不完全的，则有$A \in F(S)$使得$\vdash_{L^*} A$不成立。以$\neg A$作为新公理加到L^*中得到L^*的一个扩张L^{**}，则L^{**}是相容的。若L^{**}是不完全的，则存在公式$B \in F(S)$使得$\vdash_{L^{**}} B$不成立。以$\neg B$作为新公理加到L^{**}中得到L^{**}的一个扩张L^{***}. 这个过程可以一直下去。一般地叙述如下.

由于$F(S)$是可数集，可设为$A_0, A_1, \ldots, A_n, \ldots$

现在构造L^*的扩张序列$J_0, J_1, \ldots, J_n, \ldots$

令$J_0 = L^*$

若$\vdash_{J_0} A_0$，则令$J_1 = J_0$,

若$\vdash_{J_0} A_0$不成立，则增加$\neg A_0$为新公理从J_0得到J_1,则J_1是J_0的相容扩张。一般地，对于$n \geq 1$, 由J_{n-1}构造J_n:

$$J_n = \begin{cases} J_{n-1} & \text{若} \vdash_{J_{n-1}} A_{n-1}\text{成立} \\ J_{n-1} + \{\neg A_{n-1}\} & \text{若} \vdash_{J_{n-1}} A_{n-1}\text{不成立} \end{cases}$$

其中$J_{n-1} + \{\neg A_{n-1}\}$表示$J_{n-1}$增加新公理$\neg A_{n-1}$所得到的$J_{n-1}$的公理.

定义L^*的扩张S: S的公理集是$J_n(n = 0, 1, 2, \ldots)$的公理集之并，则S是L^*的相容完全扩张. □

L的完备性定理

定理 命题逻辑系统L中的重言式都是定理，即若$\models A$则$\vdash A$.

证明：假设A不是L中的定理，则把$\neg A$添加为新公理得到相容系统L^*。取L^*的相容完全扩张S，定义映射$v: F(S) \longrightarrow \{0,1\}$为$v(B)=1$当且仅当$\vdash_S B(B \in F(S))$. 则$v$是$F(S)$上的一个赋值. 由$v$的定义可以得到$v(\neg A)=1$与$A$是重言式矛盾. 所以$A$是L的定理.

注：重言式是从形式系统的外部来描述公式的特点。而定理是从形式系统的内部来描述公式的特点。因而,可靠性定理说明了形式系统内部描述，从外部来看是合理的，是可靠的。完备性定理反映了外部的描述是恰当的，没有多余的信息。

课堂练习三

1. 利用L的完备性定理证明以下各式成立:

(a) $\vdash (\neg A \to A) \to A$