Theory of Programming Languages
程序设计语言理论

张昱

School of Computer Science and Technology
University of Science and Technology of China

December, 2009

第6章　命题和类型

[PFPL Ch32,33][TPL Ch9]

本章介绍:

- **Curry-Howard**同构
  命题和类型相对应，证明和程序相对应.
  构造逻辑：不支持排中率
- 经典逻辑：支持排中率

6.1 引言-1

- 类型与程序
  - 类型规范行为，程序实现所规范的行为
  - 静态语义把程序关联到其所实现的类型
  - 动态语义通过逐步执行程序把程序关联到它的化简
- 命题与证明
  - 命题陈述问题，证明解答所陈述的问题
  - 形式逻辑系统把证明关联到其所证明的命题
  - 证明化简把等价的证明联系起来
- Curry-Howard同构

  命题等同于类型，证明等同于程序

6.1 引言-2

❖ Curry-Howard同构

- 对每个命题ϕ，存在一个关联的类型τ，使得对ϕ的每个证明，存在一个对应的类型为τ的表达式。

- 命题是其证明的类型，一个证明是相应类型的一个程序
- 证明有可计算的内容，程序是证明的一种形式。

程序语言中的概念可以引起逻辑中的概念，相反亦然。

最初的同构由Curry、Howard观测到，适用于构造逻辑；后来得到扩展和丰富。

6.1 引言-3

❖构造逻辑和经典逻辑的区别

例 定理：存在两个无理数a和b，使得a^b是有理数。

该定理在经典逻辑中可证，但是在构造逻辑中不可证明.

经典逻辑：若$\sqrt{2}^{\sqrt{2}}$是有理数，取$a = b = \sqrt{2}$，因$\sqrt{2}$是无理数，故所取的a和b满足定理.

若$\sqrt{2}^{\sqrt{2}}$是无理数，取$a = \sqrt{2}^{\sqrt{2}}$，$b = \sqrt{2}$，则a和b都是无理数且 $a^b = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = (\sqrt{2})^2 = 2$ 是有理数，故所取的a和b满足定理.

该证明依据排中率来肯定$\sqrt{2}^{\sqrt{2}}$是有理数或者是无理数.

构造逻辑：不支持排中率，由于不能证明$\sqrt{2}^{\sqrt{2}}$究竟是有理数还是无理数，故不能指出如何构造满足定理的a和b.

6.2 构造逻辑-1

❖ 构造逻辑(直觉主义逻辑)的语义

- 构造逻辑关心两种断言
  - ϕ **prop**: 表示ϕ是一个命题
  - ϕ **true**: 表示ϕ是一个真命题
- 命题是描述要解决的问题的规范
- 对命题所引起的问题的解是证明

  如果命题有一个证明，则称该命题为真。
- 构造逻辑的特征：只有存在命题的证明，才能判断该命题为真——可构造性。
- 如何评判命题为假？用反证法证明(假设命题为真,推出已知事实和假设相矛盾)

6.2 构造逻辑-2

❖ 构造逻辑的语义

- 构造逻辑不接受排中律，即不接受 $\phi \vee \neg\phi$ 为定理
  对于一个命题，不一定是真、假之一。

Why? 总是存在一些尚未解决的命题！

未解决：表示尚没有对此命题的证明或反驳
  例如，P=NP?

- 命题ϕ是可判定的是指存在对ϕ的证明或反驳.

例：如果ϕ表示两个自然数的不相等命题，则ϕ是可判定的。因为对于给定的自然数m和n，总可以算出$m= n$或者$m\neq n$。

6.2 构造逻辑-3

❖构造逻辑的语义

- 断言ϕ **prop**和ϕ **true**是基本的，是直言断言
- 一般地，会关注假言断言 ϕ_1 true, ..., ϕ_n true $\vdash \phi$ true 表示ϕ为真是以$\phi_1, \ldots, \phi_n$都为真为假设的。
- 假言断言满足以下结构性质(Γ是一组命题为真的假设)

$$\frac{}{\Gamma, \phi \text{ true} \vdash \phi \text{ true}}$$

$$\frac{\Gamma \vdash \phi \text{ true} \quad \Gamma, \phi \text{ true} \vdash \psi \text{ true}}{\Gamma \vdash \psi \text{ true}}$$

$$\frac{\Gamma \vdash \psi \text{ true}}{\Gamma, \phi \text{ true} \vdash \psi \text{ true}}$$

$$\frac{\Gamma, \phi \text{ true}, \phi \text{ true} \vdash \theta \text{ true}}{\Gamma, \phi \text{ true} \vdash \theta \text{ true}}$$

$$\frac{\Gamma, \psi \text{ true}, \phi \text{ true}, \Gamma' \vdash \theta \text{ true}}{\Gamma, \phi \text{ true}, \psi \text{ true}, \Gamma' \vdash \theta \text{ true}}$$

6.2 构造逻辑-4

❖命题逻辑

- 命题逻辑的联结词：永真(truth)、永假(falsehood)、合取(conjunction)、析取(disjunction)、蕴涵(implication)、否(negation)
- 命题逻辑的语法：$\phi ::= \top \mid \bot \mid \phi_1 \wedge \phi_2 \mid \phi_1 \vee \phi_2 \mid \phi_1 \Rightarrow \phi_2$
  也可以用以下推导形如ϕ **prop**的断言的规则给出

$$\frac{}{\top\ \mathbf{prop}} \qquad \frac{}{\bot\ \mathbf{prop}} \qquad \frac{\phi\ \mathbf{prop} \quad \psi\ \mathbf{prop}}{\phi \wedge \psi\ \mathbf{prop}}$$

$$\frac{\phi\ \mathbf{prop} \quad \psi\ \mathbf{prop}}{\phi \vee \psi\ \mathbf{prop}} \qquad \frac{\phi\ \mathbf{prop} \quad \psi\ \mathbf{prop}}{\phi \Rightarrow \psi\ \mathbf{prop}}$$

6.2 构造逻辑-5

❖命题逻辑

➢ 用于证明的规则

引入规则:由给定的连接词构成命题的“直接”证明

消去规则:由其他命题的“间接”证明构成命题的证明

证明守恒(conservation of proof)原理

这些规则是互逆的:

– 消去规则只能抽取引入规则所引入的信息（证明形式）

– 可以使用引入规则构造证明，供消去形式使用。

➢ 永真规则：只有引入形式，没有消去形式

$$\frac{}{\Gamma \vdash \top \ \text{true}}$$

6.2 构造逻辑-6

❖ 命题逻辑

➢ 合取规则

– 引入规则

$$\frac{\Gamma \vdash \phi \text{ true} \quad \Gamma \vdash \psi \text{ true}}{\Gamma \vdash \phi \wedge \psi \text{ true}}$$

– 消去规则

$$\frac{\Gamma \vdash \phi \wedge \psi \text{ true}}{\Gamma \vdash \phi \text{ true}} \qquad \frac{\Gamma \vdash \phi \wedge \psi \text{ true}}{\Gamma \vdash \psi \text{ true}}$$

➢ 蕴涵规则

– 引入规则

$$\frac{\Gamma, \phi \text{ true} \vdash \psi \text{ true}}{\Gamma \vdash \phi \Rightarrow \psi \text{ true}}$$

– 消去规则

$$\frac{\Gamma \vdash \phi \Rightarrow \psi \text{ true} \quad \Gamma \vdash \phi \text{ true}}{\Gamma \vdash \psi \text{ true}}$$

6.2 构造逻辑-7

❖ 命题逻辑

➢ 永假规则：没有引入形式，只有消去形式

$$\frac{\Gamma \vdash \perp \text{ true}}{\Gamma \vdash \phi \text{ true}}$$

➢ 析取规则

– 引入规则

$$\frac{\Gamma \vdash \phi \text{ true}}{\Gamma \vdash \phi \vee \psi \text{ true}} \qquad \frac{\Gamma \vdash \psi \text{ true}}{\Gamma \vdash \phi \vee \psi \text{ true}}$$

– 消去规则

$$\frac{\Gamma \vdash \phi \vee \psi \text{ true} \quad \Gamma, \phi \text{ true} \vdash \theta \text{ true} \quad \Gamma, \psi \text{ true} \vdash \theta \text{ true}}{\Gamma \vdash \theta \text{ true}}$$

6.2 构造逻辑-8

- 使证明显式化——Curry-Howard同构的关键
  - 断言ϕ **true**表示ϕ有一个证明
  - 可用断言$p : \phi$取代ϕ **true**，表示p是ϕ的一个证明
  - 假言断言修改为 $x_1 : \phi_1, \ldots, x_n : \phi_n \vdash p : \phi$
  - 构造逻辑的规则可以用证明项重写如下

    Γ是一组形如$x_i : \phi_i$的假设，且Γ中不存在重复的变量x_i
    - 永真规则 $$\frac{}{\Gamma \vdash \mathtt{trueI} : \top}$$
    - 合取规则

$$\frac{\Gamma \vdash p : \phi \quad \Gamma \vdash q : \psi}{\Gamma \vdash \mathbf{andI}(p, q) : \phi \wedge \psi} \qquad \frac{\Gamma \vdash p : \phi \wedge \psi}{\Gamma \vdash \mathbf{andE}[\mathbf{l}](p) : \phi} \qquad \frac{\Gamma \vdash p : \phi \wedge \psi}{\Gamma \vdash \mathbf{andE}[\mathbf{r}](p) : \psi}$$

6.2 构造逻辑-9

- 构造逻辑的规则可以用证明项重写如下

  Γ是一组形如$x_i : \phi_i$的假设，且Γ中不存在重复的变量x_i

  – 蕴涵规则

$$\frac{\Gamma, x:\phi \vdash p:\psi}{\Gamma \vdash \mathbf{impI}[\phi](x.p) : \phi \Rightarrow \psi} \qquad \frac{\Gamma \vdash p:\phi \Rightarrow \psi \quad \Gamma \vdash q:\phi}{\Gamma \vdash \mathbf{impE}(p,q) : \psi}$$

  – 永假规则

$$\frac{\Gamma \vdash p:\perp}{\Gamma \vdash \mathtt{falseE}[\phi](p) : \phi}$$

  – 析取规则

$$\frac{\Gamma \vdash p:\phi}{\Gamma \vdash \mathbf{orI}[\mathrm{l}][\psi](p) : \phi \vee \psi} \qquad \frac{\Gamma \vdash p:\psi}{\Gamma \vdash \mathbf{orI}[\mathrm{r}][\phi](p) : \phi \vee \psi}$$

$$\frac{\Gamma \vdash p:\phi \vee \psi \quad \Gamma, x:\phi \vdash q:\theta \quad \Gamma, y:\psi \vdash r:\theta}{\Gamma \vdash \mathbf{orE}[\phi;\psi](p, x.q, y.r) : \theta}$$

6.2 构造逻辑-命题作为类型-1

❖命题ϕ和其类型ϕ^*之间的对应关系

命题	类型	
$\top$	*unit*	空积类型
$\bot$	*void*	空和类型
$\phi \wedge \psi$	$\phi^* \times \psi^*$	二元积类型
$\phi \vee \psi$	$\phi^* \to \psi^*$	函数类型
$\phi \Rightarrow \psi$	$\phi^* + \psi^*$	二元和类型

6.2 构造逻辑-命题作为类型-2

❖ 证明和程序之间的对应关系

证明	程序	
trueI	*	空积的引入
falseE[ϕ](p)	$Zero^{\phi *}(p^*)$	空和的消去
andI(p, q)	$\langle p^*, q^*\rangle$	二元积的引入
andE[l](p)	$\mathbf{Proj}_1(p^*)$	二元积的消去
andE[r](p)	$\mathbf{Proj}_2(p^*)$	二元积的消去
impI[ϕ]($x.p$)	$\lambda x{:}\phi^*.p^*$	函数类型的引入
impE[ϕ](p, q)	$p^*\ q^*$	函数类型的消去
orI[l][ψ](p)	**Inleft**(p^*)	二元和的引入
orI[r][ϕ](p)	**Inright**(p^*)	二元和的引入
orE[ϕ; ψ](p, $x.q$,$y.t$)	**Case** $p^*(\lambda x{:}\phi^*.q^*)(\lambda y{:}\psi^*.r^*)$	二元和的消去

6.2 构造逻辑-命题作为类型-3

❖ 定理 Curry-Howard同构

1. 如果ϕ **prop** ，则ϕ^* **type**;

2. 如果$\Gamma \vdash p : \phi$，则$\Gamma^* \vdash p^* : \phi^*$。

➢ 上述定理反映出命题和类型,以及证明和程序之间的静态对应关系

➢ 进一步扩展得到动态对应关系：消去形式是引入形式的后逆

$$\mathbf{andE[l](andI(}p, q\mathbf{))} \equiv p$$

$$\mathbf{andE[r](andI(}p, q\mathbf{))} \equiv q$$

$$\mathbf{impE[}\phi\mathbf{](impI[}\phi\mathbf{](}x.p\mathbf{)}, q\mathbf{)} \equiv [q/x]p$$

$$\mathbf{orE[}\phi;\psi\mathbf{](orI[l][}\psi\mathbf{](}p\mathbf{)}, x.q, y.r\mathbf{)} \equiv [p/x]q$$

$$\mathbf{orE[}\phi;\psi\mathbf{](orI[r][}\phi\mathbf{](}p\mathbf{)}, x.q, y.r\mathbf{)} \equiv [p/y]r$$

6.3 经典逻辑-1

构造逻辑：不接受排中律，判断命题为真的唯一标准是要为该命题构造一个证明。

命题ϕ的一个反驳由假言断言ϕ **true** $\vdash \perp$ **true**的证据构成.

经典逻辑：接受排中律，即$\phi \vee \neg\phi$ true。

经典逻辑比构造逻辑所能表达的要弱。

例如，在经典逻辑中，命题$\phi \vee \neg\phi$不能说明存在ϕ的一个证明或反例，而只能说明不可能同时存在对ϕ的证明和反驳。

6.3 经典逻辑-2

❖经典逻辑

- 关心三种断言
  - ϕ **true**：表示ϕ是一个真命题
  - ϕ **false**：表示ϕ是一个假命题
  - #：表示一个已经推导出的矛盾
- 假言断言 $\phi_1\ \text{false}, \cdots, \phi_m\ \text{false}; \psi_1\ \text{true}, \cdots, \psi_n\ \text{true} \vdash J$

  J是上述三种断言之一，用Γ表示为真的假设集，Δ表示为假的假设集

$$\frac{\Delta\Gamma \vdash \phi\ \text{false} \qquad \Delta\Gamma \vdash \phi\ \text{true}}{\Delta\Gamma \vdash \#}$$

$$\frac{}{\Delta, \phi\ \text{false}\ \Gamma \vdash \phi\ \text{false}}$$

$$\frac{}{\Delta\ \Gamma, \phi\ \text{true} \vdash \phi\ \text{true}}$$

6.3 经典逻辑-3

❖经典逻辑

$$\frac{\Delta, \phi \text{ false } \Gamma \vdash \#}{\Delta\Gamma \vdash \phi \text{ true}} \qquad \frac{\Delta\ \Gamma, \phi \text{ true} \vdash \#}{\Delta\Gamma \vdash \phi \text{ false}} \qquad \frac{}{\Delta\Gamma \vdash \top \text{ true}} \qquad \frac{}{\Delta\Gamma \vdash \bot \text{ false}}$$

$$\frac{\Delta\Gamma \vdash \phi \text{ true} \quad \Delta\Gamma \vdash \psi \text{ true}}{\Delta\Gamma \vdash \phi \wedge \psi \text{ true}} \qquad \frac{\Delta\Gamma \vdash \phi \text{ false}}{\Delta\Gamma \vdash \phi \wedge \psi \text{ false}} \qquad \frac{\Delta\Gamma \vdash \psi \text{ false}}{\Delta\Gamma \vdash \phi \wedge \psi \text{ false}}$$

$$\frac{\Delta\Gamma, \phi \text{ true} \vdash \psi \text{ true}}{\Delta\Gamma \vdash \phi \Rightarrow \psi \text{ true}} \qquad \frac{\Delta\Gamma \vdash \phi \text{ true} \quad \Delta\Gamma \vdash \psi \text{ false}}{\Delta\Gamma \vdash \phi \Rightarrow \psi \text{ false}}$$

$$\frac{\Delta\Gamma \vdash \phi \text{ true}}{\Delta\Gamma \vdash \phi \vee \psi \text{ true}} \qquad \frac{\Delta\Gamma \vdash \psi \text{ true}}{\Delta\Gamma \vdash \phi \vee \psi \text{ true}} \qquad \frac{\Delta\Gamma \vdash \phi \text{ false} \quad \Delta\Gamma \vdash \psi \text{ false}}{\Delta\Gamma \vdash \phi \vee \psi \text{ false}}$$

$$\frac{\Delta\Gamma \vdash \phi \text{ false}}{\Delta\Gamma \vdash \neg\phi \text{ true}}$$

6.3 经典逻辑-4

❖经典逻辑

$$\frac{\Delta\Gamma \vdash \perp \text{ false}}{\Delta\Gamma \vdash \phi \text{ true}} \qquad \frac{\Delta\Gamma \vdash \phi \wedge \psi \text{ true}}{\Delta\Gamma \vdash \phi \text{ true}} \qquad \frac{\Delta\Gamma \vdash \phi \wedge \psi \text{ true}}{\Delta\Gamma \vdash \psi \text{ true}}$$

$$\frac{\Delta\Gamma \vdash \phi \vee \psi \text{ true} \quad \Delta\Gamma, \phi \text{ true} \vdash \theta \text{ true} \quad \Delta\Gamma, \psi \text{ true} \vdash \theta \text{ true}}{\Delta\Gamma \vdash \theta \text{ true}}$$

$$\frac{\Delta\Gamma \vdash \phi \Rightarrow \psi \text{ true} \quad \Delta\Gamma \vdash \phi \text{ true}}{\Delta\Gamma \vdash \psi \text{ true}}$$

$$\frac{\Delta\Gamma \vdash \neg\phi \text{ true} \quad \Delta\Gamma \vdash \phi \text{ false}}{\Delta\Gamma \vdash \theta \text{ false}}$$

6.3 经典逻辑-5

❖ 经典逻辑

➢ 三种断言的显式证明表示

– $p : \phi$ 表示 p 是 ϕ 的一个证明

– $k \div \phi$ 表示 k 是 ϕ 的一个反驳

– $k \# p$ 表示 k 和 p 相矛盾

➢ 假言断言改为 $\underbrace{u_1 \div \phi_1, \cdots, u_m \div \phi_m}_{\Delta}; \underbrace{x_1 : \psi_1, \cdots, x_n : \psi_n}_{\Gamma} \vdash J$

J: 是上述显式证明形式之一

6.3 经典逻辑-6

❖ 静态语义

- 矛盾产生于证明和反驳之间的冲突

$$\frac{\Delta;\Gamma \vdash k \div \phi \quad \Delta;\Gamma \vdash p : \phi}{\Delta;\Gamma \vdash k \# p}$$

- 自反性

$$\overline{\Delta, u \div \phi;\Gamma \vdash u \div \phi} \qquad \overline{\Delta;\Gamma, x : \phi \vdash x : \phi}$$

- 永真与永假互补

ccr: call with current refutation
ccp: call with current proof

$$\frac{\Delta, u \div \phi;\Gamma \vdash k \# p}{\Delta;\Gamma \vdash \mathtt{ccr}(u \div \phi . k \# p) : \phi} \qquad \frac{\Delta;\Gamma, x : \phi \vdash k \# p}{\Delta;\Gamma \vdash \mathtt{ccp}(x : \phi . k \# p) \div \phi}$$

- 联结词规则组织成永真和永假的引入规则，后者相当于构造逻辑中的消去规则

$$\overline{\Delta;\Gamma \vdash \langle\rangle : \top} \qquad \overline{\Delta;\Gamma \vdash \mathtt{abort} \div \bot}$$

6.3 经典逻辑-7

❖ 静态语义

➢ 联结词规则组织成永真和永假的引入规则，后者相当于构造逻辑中的消去规则

$$\frac{\Delta;\Gamma \vdash p:\phi \quad \Delta;\Gamma \vdash q:\psi}{\Delta;\Gamma \vdash \langle p,q\rangle : \phi \wedge \psi}$$

$$\frac{\Delta;\Gamma \vdash k \div \phi}{\Delta;\Gamma \vdash \mathtt{fst};k \div \phi \wedge \psi}$$

$$\frac{\Delta;\Gamma \vdash k \div \psi}{\Delta;\Gamma \vdash \mathtt{snd};k \div \phi \wedge \psi}$$

$$\frac{\Delta\Gamma, x:\phi \vdash p:\psi}{\Delta\Gamma \vdash (\lambda x:\phi.p):\phi \Rightarrow \psi}$$

$$\frac{\Delta\Gamma \vdash p:\phi \quad \Delta\Gamma \vdash k \div \psi}{\Delta\Gamma \vdash \mathrm{app}(p);k \div \phi \Rightarrow \psi}$$

$$\frac{\Delta;\Gamma \vdash p:\phi}{\Delta;\Gamma \vdash \mathtt{inl}(p):\phi \vee \psi}$$

$$\frac{\Delta;\Gamma \vdash p:\psi}{\Delta;\Gamma \vdash \mathtt{inr}(p):\phi \vee \psi}$$

$$\frac{\Delta;\Gamma \vdash k \div \phi \quad \Delta;\Gamma \vdash l \div \psi}{\Delta;\Gamma \vdash \mathtt{case}(k,l) \div \phi \vee \psi}$$

$$\frac{\Delta;\Gamma \vdash k \div \phi}{\Delta;\Gamma \vdash \mathtt{not}(k):\neg\phi}$$

$$\frac{\Delta;\Gamma \vdash p:\phi}{\Delta;\Gamma \vdash \mathtt{not}(p) \div \neg\phi}$$

6.3 经典逻辑-8

❖ 动态语义：识别冲突的过程

➢ 抽象机的状态： ***k* # *p***

➢ 执行：对***k* # *p***约简

用矛盾状态之间的转换关系来归纳定义

$\texttt{fst};k \# \langle p,q\rangle \mapsto k \# p$	合取（二元积）
$\texttt{snd};k \# \langle p,q\rangle \mapsto k \# q$	合取（二元积）
$\texttt{case}(k,l) \# \texttt{inl}(p) \mapsto k \# p$	析取（二元和）
$\texttt{case}(k,l) \# \texttt{inr}(q) \mapsto l \# q$	析取（二元和）
$\texttt{app}(p);k \# \lambda(x{:}\phi.q) \mapsto k \# [p/x]q$	蕴涵（函数）
$\texttt{not}(p) \# \texttt{not}(k) \mapsto k \# p$	否定
$\texttt{ccp}(x{:}\phi.\underline{k \# p}) \# q \mapsto [q/x]k \# [q/x]p$	
$k \# \texttt{ccr}(u \div \phi.\underline{l \# p}) \mapsto [k/u]l \# [k/u]p$	

6.3 经典逻辑- 9

❖ 动态语义：识别冲突的过程

$$\mathrm{ccp}(x:\phi.k\ \#\ p)\ \#\ q \mapsto [q/x]k\ \#\ [q/x]p$$

$$k\ \#\ \mathrm{ccr}(u \div \phi.l\ \#\ p) \mapsto [k/u]l\ \#\ [k/u]p$$

- 上面的规则会导致对 $\mathrm{ccp}(x:\phi.k\ \#\ p)\ \#\ \mathrm{ccr}(u \div \phi.l\ \#\ q)$ 有两种状态转换
  - 第一种 $[r/x]k\ \#\ [r/x]p \quad r \text{ is } \mathrm{ccr}(u \div \phi.l\ \#\ q)$
  - 第二种 $[m/u]l\ \#\ [m/u]q \quad m \text{ is } \mathrm{ccp}(x:\phi.k\ \#\ p)$
- 如何看待上述情况
  - 将动态语义视为是非确定性的，即上述两种情况都可能
  - 确定的动态语义：规定优先级
    - 选择第一种：惰性证明语义
    - 选择第二种：急切证明语义

6.3 经典逻辑- 10

❖ 动态语义：识别冲突的过程

- 执行的初始状态或结束状态是什么？
  - 对证明的急切解释
    假定初始(或终结)的反驳为halt，然后形成
    halt # p
  - 对反驳的急切解释
    假定初始(或终结)的证明为halt，然后形成
    k # halt

习题

1. [TPL]