



软件理论基础与实践

STLCPROP: Properties of STLC

熊英飞
北京大学



Progress

Theorem progress : forall t T,
empty |- t \in T ->
value t \ / exists t', t --> t'.

- 证明概要：在 $\text{empty} \vdash t \in T$ 上做归纳
 - 不可能是 T_Var
 - T_True , T_False 和 T_Abs 的时候 t 都是 $value$
 - T_App 的时候， t 为 $t_1 t_2$ ，根据归纳假设
 - t_1 或者 t_2 能往下约简，则整体可以往下约简
 - t_1 和 t_2 都是 $value$ ，因为 t_1 是函数类型，则 t_1 必然是 $lambda$ 抽象，所以根据 ST_AppAbs 可以往下约简
 - T_If 的时候， t 为 $\text{if } t_1 \text{ then } t_2 \text{ else } t_3$ ，根据归纳假设
 - 如果 t_1 是 $value$ ，则 t_1 为 $true$ 或者 $false$ ，整体可以约简
 - 如果 t_1 可以往下约简，整体可以往下约简



Preservation

Theorem `preservation` : forall t t' T,
empty |- t \in T ->
t --> t' ->
empty |- t' \in T.

- 因为需要对application进行分析，即需要保证替换不影响类型，先证明两个引理。



弱化引理

```
Lemma weakening_empty : forall Gamma t T,  
  empty |- t \in T ->  
  Gamma |- t \in T.
```

- 证明思路：在推导关系上做归纳，将归纳假设应用到目标上



替换引理

Lemma substitution_preserves_typing : forall

$$\begin{aligned} & \text{Gamma } x \ U \ t \ v \ T, \\ & x \mid\rightarrow U ; \text{Gamma} \mid\text{- } t \ \text{in } T \rightarrow \\ & \text{empty} \mid\text{- } v \ \text{in } U \rightarrow \\ & \text{Gamma} \mid\text{- } [x:=v]t \ \text{in } T. \end{aligned}$$

- 证明概要：在 t 上做归纳
 - 如果 t 是变量且为 x ，则 $U=T$ ，用归纳假设和弱化引理可以证明
 - 如果 t 是变量且不为 x ，则替换不改变任何内容
 - 如果 t 是 $\lambda y:S, t_0$ ，则 $T=S \rightarrow T_1$ 且 $y \mid\rightarrow S ; x \mid\rightarrow U ; \text{Gamma} \mid\text{- } t_0 \ \text{in } T_1$ 。同时有归纳假设 $\forall \text{Gamma}' , x \mid\rightarrow U ; \text{Gamma}' \mid\text{- } t_0 \ \text{in } T_0 \rightarrow \text{Gamma}' \mid\text{- } [x:=v]t_0 \ \text{in } T_0$.
 - 如果 $x=y$ ，则替换之后还是 t ，根据T-Abs我们需要证明 $y \mid\rightarrow S ; \text{Gamma} \mid\text{- } t_0 \ \text{in } T_1$ 。上述类型假设变为 $y \mid\rightarrow S ; y \mid\rightarrow U ; \text{Gamma} \mid\text{- } t_0 \ \text{in } T_1$ 。二者等价
 - 如果 $x \neq y$ ，则需要证明 $y \mid\rightarrow S ; \text{Gamma} \mid\text{- } [x:=v]t_0 \ \text{in } T_1$ 。令归纳假设中 $\text{Gamma}' = y \mid\rightarrow S ; \text{Gamma}$ 可得
 - 其他情况应用归纳假设可得。



证明Preservation

Theorem preservation : forall t t' T,
empty |- t \in T ->
t --> t' ->
empty |- t' \in T.

- 在 $\text{empty} \vdash t \in T$ 上做归纳
 - T_Var, T_Abs, T_True, T_False的情况都不会往下计算
 - T_App的情况，则 $t = t_1 t_2$
 - 如果 t_1 或 t_2 可以往下约简，则应用归纳假设可得
 - 如果 t_1 和 t_2 都是 value，则应用替换引理可得
 - T_If的情况，则 $t = \text{if } t_1 \text{ then } t_2 \text{ else } t_3$
 - 如果 t_1 可以往下约简，应用归纳假设可得
 - 如果 t_1 不能往下约简，则整体约简为 t_2 或者 t_3 ，类型保持



Preservation的逆是否成立

```
forall t t' T,  
  empty |- t' \in T ->  
  t --> t' ->  
  empty |- t \in T.
```

- 不成立，因为类型有错的项可能规约成类型正确的项，如 $(\lambda x:\text{Bool}, x) (\lambda x:\text{Bool} x)$



类型系统正确性

Definition `stuck` ($t:tm$) : `Prop` :=
(`normal_form step`) t /\ \sim `value` t .

Corollary `soundness` : `forall` t t' T ,
`empty` |- t \in T ->
 t -->* t' ->
 \sim (`stuck` t').



类型唯一性

Theorem `unique_types` : `forall` Gamma e T T',
Gamma |- e \in T ->
Gamma |- e \in T' ->
T = T'.

证明留作作业



练习

- 如果给STLC添加了如下操作语义规则和类型推导规则，progress和preservation是否还成立？

$$\frac{}{t \rightarrow \text{zap}} \quad (\text{ST_Zap})$$

$$\frac{}{\text{Gamma} \vdash \text{zap} \in \mathbb{T}} \quad (\text{T_Zap})$$



作业

- 完成progress_from_term_ind和unique_types
 - 请使用最新英文版教材