软件理论基础与实践

STLCPROP: Properties of STLC

胡振江 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|- 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t1 t2，根据归纳假设
    - t1或者t2能往下约简，则整体可以往下约简
    - t1和t2都是value，因为t1是函数，则t1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if t1 then t2 else t3，根据归纳假设
    - 如果t1是value，则t1为true或者false，整体可以约简
    - 如果t1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 G
amma x U t v T,
  x |-> U ; Gamma |- t \in T ->
  empty |- v \in U   ->
  Gamma |- [x:=v]t \in T.
```

- 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\y:S,t0，则T=S->T1且有归纳假设∀Gamma’, x|->U; Gamma’ |- t0 in T0 → Gamma’ |- [x:=v]t0 in T0.
    - 如果x=y，则我们需要证明y|->S; Gamma |- t0 in T1，等价于y|->S; x|->U; Gamma |- t0 in T1，根据归纳假设可得
    - 如果x≠y，则我们需要证明y|->S; Gamma |- [x:=v]t0 in T1。令归纳假设中Gamma’=y|-S;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|-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=t1 t2
    - 如果t1或t2可以往下约简，则应用归纳假设可得
    - 如果t1和t2都是value，则应用替换引理可得
  - T_If的情况，则t=if t1 then t2 else t3
    - 如果t1可以往下约简，应用归纳假设可得
    - 如果t1不能往下约简，则整体约简为t2或者t3，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，如(\x:Bool, (\y:Bool->Bool, y) x) (\z:Bool, z)
  - 类型检查不能证明有错误的例子

类型系统正确性

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

Corollary soundness : forall t t' T,
  empty |- t \in T ->
  t -->* t' ->
  ~(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

作业

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