

LEMMA [Inversion of the Typing Relation]:

1. If  $\Gamma \mid \Sigma \vdash x : R$ , then  $x : R \in \Gamma$
2. If  $\Gamma \mid \Sigma \vdash \lambda x : T_1. t_2 : R$ , then  $R = T_1 \rightarrow R_2$  for some  $R_2$ , with  $\Gamma, x : T_1 \vdash t_2 : R_2$ .
3. If  $\Gamma \mid \Sigma \vdash t_1 t_2 : R$ , then there is some type  $T_{11}$  such that  $\Gamma \mid \Sigma \vdash t_1 : T_{11} \rightarrow R$  and  $\Gamma \mid \Sigma \vdash t_2 : T_{11}$ .
4. If  $\Gamma \mid \Sigma \vdash \text{ref } t : R$ , then  $R = \text{Ref } T_1$  for some  $T_1$  and  $\Gamma \mid \Sigma \vdash t_1 : T_1$ .
5. If  $\Gamma \mid \Sigma \vdash !t : R$ , then  $\Gamma \mid \Sigma \vdash t : \text{Ref } R$ .
6. If  $\Gamma \mid \Sigma \vdash t_1 := t_2 : R$ , then  $R = \text{Unit}$ ,  $\Gamma \mid \Sigma \vdash t_1 : \text{Ref } T_1$ , for some  $T_1$  and  $\Gamma \mid \Sigma \vdash t_2 : T_1$ .
7. If  $\Gamma \mid \Sigma \vdash l : R$ , then  $R = \text{Ref } T_1$ , for some  $T_1$ , and  $\Sigma(l) = T_1$ .

*Proof* : Immediate from the definition of the typing relation.

LEMMA [Canonical Forms]:

1. If  $v$  is a value of type  $T_1 \rightarrow T_2$ , then  $v = \lambda x : T_1. t_2$ .
2. If  $v$  is a value of type  $\text{Unit}$ , then  $v = \text{unit}$ .
3. If  $v$  is a value of type  $\text{Ref } T$ , then  $v = l$ .

*Proof* : Straightforward.

THEOREM [Progress]: Suppose  $t$  is a closed, well-typed term (that is,  $\emptyset \mid \Sigma \vdash t : T$  for some  $T$ ). Then either  $t$  is a value or else, for any store  $\mu$  such that  $\emptyset \mid \Sigma \vdash \mu$ , there is some term  $t'$  with  $t \mid \mu \longrightarrow t' \mid \mu'$ .

*Proof*: Straightforward induction on typing derivations.

1. The variable case cannot occur (because  $t$  is closed).
2. The abstraction case is immediate, since abstractions are values.
3. For application, where  $t = t_1 t_2$ , with  $\emptyset \mid \Sigma \vdash t_1 : T_{11} \rightarrow T_{12}$  and  $\emptyset \mid \Sigma \vdash t_2 : T_{11}$ , for the inversion lemma. Then, by the induction hypothesis, either  $t_1$  is a value or else it can make a step of evaluation, and likewise  $t_2$ . If  $t_1$  can take a step, then rule  $EApp1$  applies to  $t$ . If  $t_1$  is a value and  $t_2$  can take a step, then rule  $EApp2$  applies. Finally, if both  $t_1$  and  $t_2$  are values, then the canonical forms lemma tells us that  $t_1$  has the form  $\lambda x : T_{11}. t_{12}$ , and so rule  $EAppAbs$  applies to  $t$ .
4. The *unit* case is immediate, since *unit* is a value.
5. If  $t = \text{Ref } t_1$ , then  $T = \text{Ref } T_1$ , for some  $T_1$ , and  $\emptyset \mid \Sigma \vdash t_1 : T_1$ . By the induction hypothesis, either  $t_1$  is a value or else it can make a step of evaluation. If  $t_1$  can take a step, then for any store  $\mu$  such that  $\emptyset \mid \Sigma \vdash \mu$ , there is some term  $t'_1$  with  $t_1 \mid \mu \longrightarrow t'_1 \mid \mu'$ . For this reason, for any store  $\mu$  such that  $\emptyset \mid \Sigma \vdash \mu$ , the rule  $ERef$  applies to  $t$ , which guarantees the existence of  $t'$  and  $\mu'$ . If  $t_1$  is a value ( $t_1 = \text{Ref } v_1$ ) then the rule  $ERefV$  applies to  $t$ , obtaining that  $t' = l$ , with  $l \notin \text{dom}(\mu)$  and  $\mu' = (\mu, l \mapsto v_1)$ .

6. If  $t = !t_1$ , then  $\emptyset \mid \Sigma \vdash t_1 : \text{Ref } T$ . By the induction hypothesis, either  $t_1$  is a value or else it can make a step of evaluation. If  $t_1$  can take a step, then for any store  $\mu$  such that  $\emptyset \mid \Sigma \vdash \mu$ , there is some term  $t'_1$  with  $t_1 \mid \mu \longrightarrow t'_1 \mid \mu'$ . For this reason, for any store  $\mu$  such that  $\emptyset \mid \Sigma \vdash \mu$ , the rule  $EDeref$  applies to  $t$ , which guarantees the existence of  $t'$  and  $\mu'$ . If  $t_1$  is a value ( $t_1 = l$ , for the Canonical Forms Lemma) then the rule  $EDerefLoc$  applies to  $t$  (since  $\emptyset \mid \Sigma \vdash l : \text{Ref } T$  and  $\emptyset \mid \Sigma \vdash \mu$  then  $\mu(l)$  is defined), obtaining that  $t' = \mu(l)$ , and  $\mu' = \mu$ .
7. If  $t = t_1 := t_2$ , then then  $T = \text{Unit}$ ,  $\emptyset \mid \Sigma \vdash t_1 : \text{Ref } T_1$ , for some  $T_1$  and  $\emptyset \mid \Sigma \vdash t_2 : T_1$ . By the induction hypothesis, either  $t_1$  is a value or else it can make a step of evaluation, and likewise  $t_2$ . If  $t_1$  can take a step, then for any store  $\mu$  such that  $\emptyset \mid \Sigma \vdash \mu$ , there is some term  $t'_1$  with  $t_1 \mid \mu \longrightarrow t'_1 \mid \mu'$ . For this reason, for any store  $\mu$  such that  $\emptyset \mid \Sigma \vdash \mu$ , the rule  $EAssing1$  applies to  $t$ , which guarantees the existence of  $t'$  and  $\mu'$ . If  $t_2$  can take a step, is the same, but with the rule  $EAssing2$ . Finally, if both  $t_1$  and  $t_2$  are values, then the canonical forms lemma tells us that  $t_1$  has the form  $l$ . Then the rule  $EAssing$  applies to  $t$ , which guarantees the existence of  $t'$  and  $\mu'$ .
8. If  $t = l$ , then it is immediate, since locations are values.

LEMMA[Permutation]: If  $\Gamma \mid \Sigma \vdash t : T$  and  $\Delta$  is a permutation of  $\Gamma$ , then  $\Delta \mid \Sigma \vdash t : T$ .

*Proof:* Straightforward induction on typing derivations.

LEMMA[Weakening]: If  $\Gamma \mid \Sigma \vdash t : T$  and  $x \notin \text{dom}(\Gamma)$ , then  $\Gamma, x : S \mid \Sigma \vdash t : T$ .

*Proof:* Straightforward induction on typing derivations.

LEMMA [Preservation of types under substitution]: If  $\Gamma, x : S \mid \Sigma \vdash t : T$  and  $\Gamma \mid \Sigma \vdash s : S$ , then  $\Gamma \mid \Sigma \vdash [x \mapsto s]t : T$ .

*Proof:* By induction on a derivation of the statement  $\Gamma, x : S \vdash t : T$ . For a given derivation, we proceed by cases on the final typing rule used in the proof.

LEMMA [1]: If  $\Gamma \mid \Sigma \vdash \mu$ ,  $\Sigma(l) = T$  and  $\Gamma \mid \Sigma \vdash v : T$  then  $\Gamma \mid \Sigma \vdash [l \mapsto v]\mu$ .

*Proof:* Straightforward induction.

LEMMA [2]: If  $\Gamma \mid \Sigma \vdash t : T$  and  $\Sigma \subseteq \Sigma'$  then  $\Gamma \mid \Sigma' \vdash t : T$ .

*Proof:* Straightforward induction.

LEMMA[Preservation]: If  $\Gamma \mid \Sigma \vdash t : T$ ,  $\Gamma \mid \Sigma \vdash \mu$  and  $t \mid \mu \longrightarrow t' \mid \mu'$ , then for some  $\Sigma' \supseteq \Sigma$ ,  $\Gamma \mid \Sigma \vdash t' : T$  and  $\Gamma \mid \Sigma' \vdash \mu'$ .

*Proof:*

1. *Case TVar:*  $\dots$
2. *Case TAbs:*  $\dots$
3. *Case TApp:*  $\dots$
4. *Case TLoc:* If the last rule in the derivation is  $TLoc$ , then we know from the form of this rule that  $t$  must be a location  $l$ , then  $t$  is a value, so it cannot be the case that  $t \mid \mu \longrightarrow t' \mid \mu'$  for any  $t'$ , and the requirements of the theorem are vacuously satisfied.

5. *Case TUnit*: If the last rule in the derivation is *TUnit*, then we know from the form of this rule that  $t$  must be *unit*, then  $t$  is a value, so it cannot be the case that  $t \mid \mu \longrightarrow t' \mid \mu'$  for any  $t'$ , and the requirements of the theorem are vacuously satisfied.
6. *Case TRef*:  $t = \text{ref } t_1$ ,  $\Gamma \mid \Sigma \vdash \text{ref } t_1 : \text{Ref } T_1$ , for some  $T_1$  and  $\Gamma \mid \Sigma \vdash t_1 : T_1$ . If the last rule in the derivation is *TRef*, then we know from the form of this rule that  $t$  must have the form  $\text{ref } t_1$ , for some  $t_1$ . Now, looking at the evaluation rules with this form on the left-hand side, we find that there are two rules by which  $t \mid \mu \longrightarrow t' \mid \mu'$  can be derived: *ERefV* and *ERef*. We consider each case separately.
  - *Subcase ERef*:  $t_1 \mid \mu \longrightarrow t'_1 \mid \mu'$ ,  $t' = \text{ref } t'_1$ . By the induction hypothesis,  $\Gamma \mid \Sigma' \vdash t'_1 : T_1$ , for some  $\Sigma'$ , where  $\Gamma \mid \Sigma' \vdash \mu'$ . Then we can apply rule *TRef*, to conclude that  $\Gamma \mid \Sigma' \vdash \text{ref } t'_1 : \text{Ref } T_1$ , that is  $\Gamma \mid \Sigma' \vdash t' : T$ , where  $\Gamma \mid \Sigma' \vdash \mu'$ .
  - *Subcase ERefV*:  $t = \text{ref } v_1$ ,  $t' = l$  and  $l \notin \text{dom}(\mu)$ . For  $\Sigma' = \Sigma \cup (l, T_1)$ , for the rule *TLoc*, is true that  $\Gamma \mid \Sigma' \vdash l : \text{Ref } T_1$ , and  $\Gamma \mid \Sigma' \vdash (\mu, l \mapsto v_1)$ .
7. *Case TAssing*:  $t = t_1 := t_2$ ,  $T = \text{Unit}$ ,  $\Gamma \mid \Sigma \vdash t_1 : \text{Ref } T_1$ , for some  $T_1$ , and  $\Gamma \mid \Sigma \vdash t_2 : T_1$ . If the last rule in the derivation is *TAssing*, then we know from the form of this rule that  $t$  must have the form  $t_1 := t_2$ , for some  $t_1$  and  $t_2$ . Now, looking at the evaluation rules with this form on the left-hand side, we find that there are three rules by which  $t \mid \mu \longrightarrow t' \mid \mu'$  can be derived: *EAssing1*, *EAssing2* and *EAssing*. We consider each case separately.
  - *Subcase EAssing1*:  $t_1 \mid \mu \longrightarrow t'_1 \mid \mu'$ ,  $t' = t'_1 := t_2$ . By the induction hypothesis,  $\Gamma \mid \Sigma' \vdash t'_1 : \text{Ref } T_1$ , for some  $\Sigma'$ , where  $\Gamma \mid \Sigma' \vdash \mu'$ . Moreover,  $\Gamma \mid \Sigma' \vdash t_2 : T_1$ , for Lemma[2]. Then we can apply rule *TAssing*, to conclude that  $\Gamma \mid \Sigma' \vdash t'_1 := t_2 : \text{Unit}$ , that is  $\Gamma \mid \Sigma' \vdash t' : T$ , where  $\Gamma \mid \Sigma' \vdash \mu'$ .
  - *Subcase EAssing2*: Similar to the above.
  - *Subcase EAssing*:  $t = l := v$  and  $t' = \text{unit}$ . Then for  $\Sigma$ , it is satisfied that  $\Gamma \mid \Sigma \vdash t' : \text{Unit}$ , that is  $\Gamma \mid \Sigma \vdash t' : T$ , and for  $\mu' = [l \mapsto v]\mu$  is true that  $\Gamma \mid \Sigma \vdash [l \mapsto v]\mu$  for Lemma[1].
8. *Case TDeref*:  $t = !t_1$  and  $\Gamma \mid \Sigma \vdash t_1 : \text{Ref } T$ . If the last rule in the derivation is *TDeref*, then we know from the form of this rule that  $t$  must have the form  $t = !t_1$ , for some  $t_1$ . Now, looking at the evaluation rules with this form on the left-hand side, we find that there are two rules by which  $t \mid \mu \longrightarrow t' \mid \mu'$  can be derived: *EDeref* and *EDerefLoc*. We consider each case separately.
  - *Subcase EDeref*:  $t_1 \mid \mu \longrightarrow t'_1 \mid \mu'$ ,  $t' = !t'_1$ . By the induction hypothesis,  $\Gamma \mid \Sigma' \vdash t'_1 : \text{Ref } T$ , for some  $\Sigma'$ , where  $\Gamma \mid \Sigma' \vdash \mu'$ . Then we can apply rule *TDeref*, to conclude that  $\Gamma \mid \Sigma' \vdash !t'_1 : T$ , that is  $\Gamma \mid \Sigma' \vdash t' : T$ , where  $\Gamma \mid \Sigma' \vdash \mu'$ .
  - *Subcase EDerefLoc*:  $t_1 = l$ ,  $\mu(l) = v$ , for some  $v$  and  $t' = v$ . We know that  $\Gamma \mid \Sigma \vdash l : \text{Ref } T$ , then for the inversion lemma,  $\Sigma(l) = T$ . We know too, that  $\Gamma \mid \Sigma \vdash \mu$ , then  $\Gamma \mid \Sigma \vdash \mu(l) : \Sigma(l)$ , that is  $\Gamma \mid \Sigma \vdash v : T$ .