Preservation

Statement

if

- $\Gamma \models s$
- $\Gamma, s \vdash t : T$
- $t \mid s \longrightarrow t' \mid s'$

then $\exists \Gamma', T'$ such that

- $\Gamma \subseteq \Gamma'$
- $\Gamma' \models s'$
- $\Gamma', s' \vdash t' : T'$
- $\Gamma', s' \vdash T' \equiv T$

Proof Sketch

By induction on the derivation of $t \mid s \longrightarrow t' \mid s'$.

Case Red-New

$t = \mathbf{val}\, x = \mathbf{new}\, c; t'$ where $c = T_c\{\, \overline{def_i}^{\,i} \,\}$.

For $\Gamma, s \vdash t : T$, only the **Typ-New** rule applies.

We assume x is fresh, without loss of generality thanks to alpha-conversion.

$s' = s, x \mapsto c$

$\Gamma' = \Gamma, x : T_c$

By construction, $\Gamma \subseteq \Gamma'$ and $\Gamma' \models s'$.

Through the **Typ-New** rule, we know that

$\Gamma', s \vdash t' : T$

so $\Gamma', s' \vdash t' : T$, since $s \subseteq s'$, and the same derivation is possible.

Thus $T = T'$ and we are done.

Case Red-VSel

$t = v.l$ where $x \mapsto T_c\{\ \overline{def_i}^{\,i}\ \} \in s$, def_i **is** $l = v'$, $v \downarrow x$, $s \vdash v.l \,|\, v' \uparrow_v v''$.

$\Gamma' = \Gamma$ and $s' = s$.

$t' = v''$.

For $\Gamma, s \vdash v.l : T$, only the **Typ-VSel** rule applies, with premise: $\Gamma, s \vdash v \ni l : T$.

By $\Gamma \models s$: $\exists T'$, such that

- $\Gamma, s \vdash v' : T'$
- $\Gamma, s \vdash T' \equiv T$

Because we propagate the widening, $\exists T''$, such that

- $\Gamma, s \vdash v'' : T'$
- $\Gamma, s \vdash T'' \equiv T'$

Case Red-MSel

$t = v\, m\, v'$ where $x \mapsto T_c\{\ \overline{def_i}^{\,i}\ \} \in s$, def_i **is** $m(x_i) = t_i$, $v \downarrow x$, $s \vdash v.m(v') \,|\, \lambda x_i.t_i \uparrow_m t'$.

$s' = s$.

For $\Gamma, s \vdash v\, m\, v' : T$, only the **Typ-MSel** rule applies. Premises:

- $\Gamma, s \vdash v \ni m : S \to T$
- $\Gamma, s \vdash v' : S'$
- $\Gamma, s \vdash S' \equiv S$

By $\Gamma \models s$: $\exists W$, such that

- $\Gamma, x_i : S, s \vdash t_i : W$
- $\Gamma, x_i : S, s \vdash W \equiv T$

Because we propagate the widening, $\exists T'$, such that * $\Gamma, s \vdash t' : T'$ * $\Gamma, s \vdash T' \equiv W$

$\equiv$ Lemma

If

- $\Gamma, x_i : S, s \vdash t_i : W$
- $\Gamma, x_i : S, s \vdash S' \equiv S$

then $\exists W'$ such that

- $\Gamma, x_i : S', s \vdash t_i : W'$
- $\Gamma, x_i : S', s \vdash W' \equiv W$
- If $\Gamma, x_i : S, s \vdash W \equiv T$, then $\Gamma, x_i : S', s \vdash W' \equiv T$.

Substitution lemma

If

- $\Gamma, x_i : S', s \vdash t_i : W'$
- $\Gamma, s \vdash v' : S'$

then $\exists W''$ such that

- $\Gamma, s \vdash [v'/x_i]t_i : W''$
- $\Gamma, x_i : S', s \vdash W'' \equiv W'$

The $\equiv$ and substitution lemmas apply. $T' = W''$.

Case Red-Ctx

There are four cases:

1. $t_1.l \mid s \longrightarrow t_1'.l \mid s'$
2. $t_1\ m\ t_2 \mid s \longrightarrow t_1'\ m\ t_2 \mid s'$
3. $v_1\ m\ t_2 \mid s \longrightarrow v_1\ m\ t_2' \mid s'$
4. $t_1 : T \mid s \longrightarrow t_1' : T \mid s'$

For case 1, only the **Typ-VSel** rule applies, with premise: $\Gamma, s \vdash t_1 \ni l : T$. By induction hypothesis, $\exists \Gamma', s', T_1'$ such that $\Gamma', s' \vdash t_1' : T_1'$ and $\Gamma', s' \vdash T_1' \equiv T_1$ where $\Gamma, s \vdash t_1 : T_1$. The conclusion follows by the membership-$\equiv$ lemma.

For cases 2 and 3, only the **Typ-Sel** rule applies. Premises:

- $\Gamma, s \vdash t_1 \ni m : S_1 \to T$
- $\Gamma, s \vdash t_2 : T_2$
- $\Gamma, s \vdash T_2 \equiv S_1$

For case 3, by induction hypothesis, $\exists \Gamma', s', T_2'$ such that $\Gamma', s' \vdash t_2' : T_2'$ and $\Gamma', s' \vdash T_2' \equiv T_2$. By transitivity of $\equiv$ on T_2 (with strengthening of context), $\Gamma', s' \vdash T_2' \equiv S_1$. So the **Typ-Sel** rule applies with the result $T' = T$.

For case 2, by induction hypothesis, $\exists \Gamma', s', T_1'$ such that $\Gamma', s' \vdash t_1' : T_1'$ and $\Gamma', s' \vdash T_1' <: T_1$ where $\Gamma, s \vdash t_1 : T_1$. The conclusion follows by the membership-$\equiv$ lemma.

For case 4, only the **Typ-Wid** rule applies with premises:

- $\Gamma, s \vdash t_1 : T_1$
- $\Gamma, s \vdash T_1 <: T$

By induction hypothesis, $\exists \Gamma', s', T_1'$ such that $\Gamma', s' \vdash t_1' : T_1'$ and $\Gamma', s' \vdash T_1' \equiv T_1$. So, $\Gamma', s' \vdash T_1' <: T$, and the **Typ-Wid** rule applies again with result $T' = T$.

Membership-$\equiv$ lemma

If

- $\Gamma, s \vdash t_1 : T_1$
- $\Gamma, s \vdash t_1' : T_1'$
- $\Gamma, s \vdash T_1' \equiv T_1$

and if

- $\Gamma, s \vdash t_1 \ni m : S_1 \to T$

then $\exists S_1', T'$ such that

- $\Gamma, s \vdash t_1' \ni m : S_1' \to T'$
- $\Gamma, s \vdash S_1 \equiv S_1'$
- $\Gamma, s \vdash T' \equiv T$

or if

- $\Gamma, s \vdash t_1 \ni l : T$

then $\exists T'$ such that

- $\Gamma, s \vdash t_1' \ni l : T'$
- $\Gamma, s \vdash T' \equiv T$

Substitution Lemma

Statement

If

- $\Gamma, x : S, s \vdash t : T$
- $\Gamma, s \vdash v : S$

then $\exists T'$ such that

- $\Gamma, s \vdash [v/x]t : T'$
- $\Gamma, x : S, s \vdash T' \equiv T$

Proof Sketch

By induction on the derivation of $\Gamma, x : S, s \vdash t : T$.

Case Typ-Var

$t = z$. Premise: $z : T \in \Gamma, x : S$.

If $z = x$, then $T = S = T'$, since $[v/x]z = [v/x]x = x$. If $z \neq x$, then $[v/x]z = z$, so $T = T'$.

Case Typ-VSel

$t = t_1.l$ with premises $\Gamma, s \vdash t_1 \ni l : T$ and $\Gamma, x : S, s \vdash t_1 : T_1$.

Let $[v/x]t = t' = t_1'.l = [v/x]t_1.l$.

By induction hypothesis, $\Gamma, x : S, s \vdash t_1 : T_1$ implies $\Gamma, s \vdash t_1' : T_1'$ and $\Gamma, x : S, s \vdash T_1' \equiv T_1$.

By the **membership-$\equiv$ lemma**, $\Gamma, s \vdash t_1' \ni l : T'$ and $\Gamma, x : S, s \vdash T' \equiv T$.

The **Typ-VSel** rule applies with result T'.

Case Typ-MSel

$t = t_1\ m\ t_2$. Premises:

- $\Gamma, x : S, s \vdash\ t_1\ \ni\ m_1 : S_1 \to T$
- $\Gamma, x : S, s \vdash\ t_1 : T_1$
- $\Gamma, x : S, s \vdash\ t_2 : T_2$
- $\Gamma, x : S, s \vdash\ T_2 \equiv S_1$

Let $[v/x]t = t' = t'_1\ m\ t'_2 = [v/x]t_1\ m\ [v/x]t_2$.

By induction hypothesis:

- $\Gamma, x : S, s \vdash\ t_2 : T_2$ implies
- $\Gamma, s \vdash\ t'_2 : T'_2$
- $\Gamma, x : S, s \vdash\ T'_2 \equiv T_2$
- $\Gamma, x : S, s \vdash\ t_1 : T_1$ implies
- $\Gamma, s \vdash\ t'_1 : T'_1$
- $\Gamma, x : S, s \vdash\ T'_1 \equiv T_1$

By the **membership-$\equiv$ lemma**:

- $\Gamma, s \vdash\ t'_1\ \ni\ m : S'_1 \to T'$
- $\Gamma, x : S, s \vdash\ S_1 \equiv S'_1$
- $\Gamma, x : S, s \vdash\ T' \equiv T$

The **Typ-MSel** rule applies with result T'.

Case Typ-New

$t = \mathbf{val}\, z = \mathbf{new}\, T_c\{\ \overline{def_i}^{\,i}\ \}; t_0$

$t' = [v/x]t = \mathbf{val}\, z = \mathbf{new}\, [v/x]T_c\{\ \overline{[v/x]def_i}^{\,i}\ \}; [v/x]t_0$

For the **Typ-New** rule to apply again, we need substitution to preserve the properties checked by the **Typ-New** rule. In particular, substitution must preserve good bounds and well-formed and expanding types. We rely on the fact that two $\equiv$-equivalent types are indistingushable by judgements.

Case Typ-Wid

$t = t_1 : T$ with premises $\Gamma, s \vdash t_1 : T_1$ and $\Gamma, s \vdash T_1 <: T$.

Let $[v/x]t = t' = t'_1 : T' = [v/x]t_1 : [v/x]T$.

If $x \notin fn(T)$, then straightforward by induction hypothesis.

Otherwise, is $\Gamma, x : S, s \vdash [v/x]T \equiv T$? TODO: is this case possible? TODO: then what?

$\equiv$ Lemma

Statement

If

- $\Gamma, x : S, s \vdash t : T$
- $\Gamma, s \vdash S' \equiv S$

then $\exists T'$ such that

- $\Gamma, x : S', s \vdash t : T'$
- $\Gamma, x : S', s \vdash T' \equiv T$

Proof Sketch

TODO.

Membership-$\equiv$ Lemma

Statement

If

- $\Gamma, s \vdash t : T$
- $\Gamma, s \vdash t' : T'$
- $\Gamma, s \vdash T' \equiv T$
- $\Gamma, s \vdash T'$ **wfe**

and if

- $\Gamma, s \vdash t \ni m : S_1 \to T_1$

then $\exists S_1', T_1'$ such that

- $\Gamma, s \vdash t' \ni m : S_1' \to T_1'$
- $\Gamma, s \vdash S_1 \equiv S_1'$
- $\Gamma, s \vdash T_1' \equiv T_1$

or if

- $\Gamma, s \vdash t \ni l : T_1$

then $\exists T_1'$ such that

- $\Gamma, s \vdash t' \ni l : T_1'$
- $\Gamma, s \vdash T_1' \equiv T_1$

Proof Sketch

TODO.