COMPSCI 3MI3

Assignment 9

1 Solution Set

1.1 Q1

We will prove the property of progress for our simply typed λ-Calculus augmented with *Unit*, the sequencing operator and referencing operations. Formally we prove: if $\emptyset \mid \Sigma \vdash t : T$ for some term t, type T and typing store Σ, then t is a value, or else, for any μ with $\emptyset \mid \Sigma \vdash \mu$ there exists some term t' and store μ' such that $t \mid \mu \to t' \mid \mu'$. We will prove progress holds by induction on the typing derivation $\emptyset \mid \Sigma \vdash t : T$.

By augmenting our previously defined simply typed λ-Calculus with *Unit*, sequencing and referencing, we do not modify our previous terms defined in our calculus, thus our previously proved progress property theorem will hold for existing cases in our augmented calculus. Therefore we focus on proving new cases unique to our augmented calculus.

We also extend the cannonical forms lemma to include cases for `ref` t and `unit` with the following definitions:

(1) If v is a value of type *Unit*, then v is `unit`.

(2) If v is a value of type *Ref* T, then v is a memory location l.

Base case. Our base case denotes all typing derivations for which there do not exist any further sub-typing derivations. The possible typing derivations are of the following cases:

Case: T-Unit
If T-Unit is the final typing derivation then $t =$ `unit` and $T = Unit$. Thus t is a value and our property holds.

Case: T-Loc
If T-Loc is the final typing derivation then $t = l$, with l a memory location and $T = Ref\, T_1$ with the premise $\Sigma(l) = T_1$. Since l is a value, t is a value and our property holds.
Thus our base case holds.

Induction step. We assume for all typing sub-derivations that the progress property holds. We prove for the remaining typing derivations that the progress property holds.. The typing derivation must one of the following cases:

Case: T-Seq
If T-Seq was the final typing derivation then $t = t_1; t_2$ and $T = T_2$ with the premises $\emptyset \,|\, \Sigma \vdash t_1 : \mathit{Unit}$ and $\emptyset \,|\, \Sigma \vdash t_2 : T_2$. By our induction hypothesis on t_1 for some store μ we know t_1 is either a value or we have $t_1 \,|\, \mu \rightarrow t_1' \,|\, \mu'$. If t_1 is a value, by the cannonical forms lemma we know $t_1 = \texttt{unit}$, thus we can apply E-SeqNext to t with store μ. Otherwise if we have $t_1 \mid \mu \rightarrow t_1' \mid \mu'$ then we can apply E-Seq to t with μ. Therefore, in all cases t is either a value or we have $t \mid \mu \rightarrow t' \mid \mu'$, thus our progress property holds for the T-Seq case.

Case: T-Ref
If T-Ref was the final typing derivation then $t = \texttt{ref}\, t_1$, $T = \mathit{Ref}\ T_1$ and we have the premise $\emptyset \mid \Sigma \vdash t_1 : T_1$. By our induction hypothesis on t_1 for some store μ we know t_1 is either a value or we have $t_1 \mid \mu \rightarrow t_1' \mid \mu'$. If t_1 is a value then by assigning new memory location $l \notin \mathit{dom}(\mu)$ to store the reference for t_1 we can apply E-RefV to t with μ, thus obtaining $\mu' = \mu, l \mapsto t_1$ and $\Sigma' = \Sigma, l \mapsto T_1$ with $t \,|\, \mu \rightarrow t' \mid \mu'$. Otherwise, if we have $t_1 \mid \mu \rightarrow t_1' \mid \mu'$ then we can apply E-Ref to t with μ. Therefore, in all cases t is either a value or we have $t \,|\, \mu \rightarrow t' \mid \mu'$, thus our progress property holds for the T-Ref case.

Case: T-Deref
If T-Deref was the final typing derivation then $t =!t_1$, $T = T_1$ with the premise $\emptyset \mid \Sigma \vdash t_1 : \mathit{Ref}\ T_1$. By our induction hypothesis on t_1 for some store μ we know t_1 is either a value or we have $t_1 \mid \mu \rightarrow t_1' \mid \mu'$. If t_1 is a value by the cannonical forms lemma we know $t_1 = l$ a memory location with the premise $\Sigma(l) = T_1$. Since μ is well typed with respect to Σ we know $\mathit{dom}(\mu) = \mathit{dom}(\Sigma)$ and $\mu(l) : \Sigma(l)$. Thus, we have the premise $\mu(l) = v : \Sigma(l)$ for some value v. We can then say that we can apply E-DerefLoc to t with store μ. Otherwise, if we have $t_1 \,|\, \mu \rightarrow t_1' \,|\, \mu'$ we can apply E-Deref to t with μ. Therefore, in all cases t is either a value or we have $t \mid \mu \rightarrow t' \mid \mu'$, thus our progress property holds for the T-Deref case.

Case: T-Assign
If T-Assign was the final typing derivation then $t = t_1 := t_2$, $T = \mathit{Unit}$ and we have the premises $\emptyset \mid \Sigma \vdash t_1 : \mathit{Ref}\ T_1$ and $\emptyset \mid \Sigma \vdash t_2 : T_1$. By our induction hypothesis for t_1 for some store μ we know t_1 is either a value or we have $t_1 \mid \mu \rightarrow t_1' \mid \mu'$, with similar being said for t_2. We then have 3 cases. If both t_1 and t_2 are values, by the cannonical forms lemma we know $t_1 = l$ a memory location with the premise $\Sigma(l) = T_1$. Since t_2 is also a value we can apply E-Assign to t with μ. If t_1 is a value and we have $t_2 \mid \mu \rightarrow t_2' \mid \mu'$ we can apply E-Assign2 to t with μ. Lastly, if we have $t_1 \mid \mu \rightarrow t_1' \mid \mu'$, regardless of t_2 we can apply E-Assign1 to t with μ. Therefore, in all cases t is either a value or we have $t \mid \mu \rightarrow t' \mid \mu'$, thus our progress property holds for the T-Assign case.

Therefore our induction step holds. We have shown for all possible typing derivations the progress property holds.

Thus we've shown that the progress property holds for our augmented simply typed λ-Calculus. □

1.2 Q2

We will prove the property of preservation holds for our simply typed λ-Calculus augmented with *Unit*, the sequencing operator and referencing operations. Formally, we prove:

$$(\Gamma \mid \Sigma \vdash t : T) \wedge (t \mid \mu \to t' \mid \mu') \wedge (\Gamma \mid \Sigma \vdash \mu) \implies (\exists \Sigma' \supseteq \Sigma \mid (\Gamma \mid \Sigma' \vdash t' : T) \wedge (\Gamma \mid \Sigma' \vdash \mu'))$$

We will prove the above holds by induction on the evalution derivation $t \mid \mu \to t' \mid \mu'$, assuming μ is well typed with respect to a typing context Γ and typing store Σ.

By augmenting our previously defined simply typed λ-Calculus with *Unit*, sequencing and referencing, we do not modify our previous terms defined in our calculus. Thus our previously defined argument for proving the property of preservation, augmented with the lemma of Preservation Over Substitution, will hold for existing cases in our augmented calculus. Therefore we focus on proving new cases unique to our augmented calculus.

We also extend our definition of the inversion lemma previously defined in the slides, deriving new definitions from our new typing rules:

(1) $\Gamma \mid \Sigma \vdash \texttt{unit} : R \implies R = \mathit{Unit}$

(2) $\Gamma \mid \Sigma \vdash (t_1; t_2) : R \implies \Gamma \mid \Sigma \vdash t_1 : \mathit{Unit} \wedge \Gamma \mid \Sigma \vdash t_2 : R$

(3) $\Gamma \mid \Sigma \vdash l : R \implies R = \mathit{Ref}\, T_1 \wedge \Sigma(l) = T_1$

(4) $\Gamma \mid \Sigma \vdash \texttt{ref}\, t_1 : R \implies R = \mathit{Ref}\, T_1 \wedge \Gamma \mid \Sigma \vdash t_1 : T_1$

(5) $\Gamma \mid \Sigma \vdash !t : R \implies R = T_1 \wedge \Gamma \mid \Sigma \vdash t : \mathit{Ref}\, T_1$

(6) $\Gamma \mid \Sigma \vdash t_1 := t_2 : R \implies R = \mathit{Unit} \wedge \Gamma \mid \Sigma \vdash t_1 : \mathit{Ref}\, T_1 \wedge \Gamma \mid \Sigma \vdash t_2 : T_1$

Base case. Our base case denotes the final evalutation derivation where $t \mid \mu \to t' \mid \mu'$ will yield a value. The possible evaluation derivations that could yield a value are of the following:

Case: E-SeqNext
If E-SeqNext was the last derivation we know $t = \texttt{unit}; t_2$ and $t' = t_2$ with $\mu = \mu'$. The only typing derivation we can apply is T-Assign, thus we have $\Gamma \mid \Sigma \vdash \texttt{unit}; t_2 : T_2$ and $T = T_2$ with the premises $\Gamma \mid \Sigma \vdash \texttt{unit} : \mathit{Unit}$ and $\Gamma \mid \Sigma \vdash t_2 : T_2$. Setting $\Sigma' = \Sigma$ we've shown for $\Sigma' \supseteq \Sigma$ we have $\Gamma \mid \Sigma' \vdash t' : T$ and $\Gamma \mid \Sigma' \vdash \mu'$. Thus, the E-SeqNext case holds.

Case: E-RefV
If E-RefV was the last derivation we know $t = \texttt{ref}\, v_1$, $t' = l$, $\mu' = \mu, l \mapsto v_1$ and $\Sigma' = \Sigma, l \mapsto T_1$ with v_1 some value and l a memory location. We also have the premises $l \notin \mathit{dom}(\mu)$ and $\Gamma \mid \Sigma \vdash v_1 : T_1$. By T-Ref with the premise $\Gamma \mid \Sigma \vdash v_1 : T_1$ we know $\Gamma \mid \Sigma \vdash \texttt{ref}\, v_1 : \mathit{Ref}\, T_1$, thus $T = \mathit{Ref}\, T_1$. By T-Loc with our premise $\Sigma'(l) = T_1$ we know $\Gamma \mid \Sigma' \vdash l : \mathit{Ref}\, T_1$. Lastly, by our premises $\Gamma \mid \Sigma \vdash \mu$ and $l \notin \mathit{dom}(u)$ we know by adding l to our stores μ' and Σ' will not violate $\Gamma \mid \Sigma' \vdash \mu'$. Therefore, we've shown for $\Sigma' \supseteq \Sigma$ we have $\Gamma \mid \Sigma' \vdash t' : T$ and $\Gamma \mid \Sigma' \vdash \mu'$. Thus, the E-RefV case holds.

Case: E-Assign
If E-Assign was the last derivation we know $t = l := v_2$ and $t' = \texttt{unit}$ with $\mu' = [l \mapsto v_2]\mu$. The only typing derivation we can apply is T-Assign, thus we have $\Gamma \mid \Sigma \vdash l := v_2 : \mathit{Unit}$ and $T = \mathit{Unit}$ with the premises $\Gamma \mid \Sigma \vdash l : \mathit{Ref}\, T_1$ and $\Gamma \mid \Sigma \vdash v_2 : T_1$. It follows then by the 3rd clause of the extended inversion lemma we know $\Sigma(l) = T_1$. Then by Preservation Over Storage with our premises $\Gamma \mid \Sigma \vdash \mu$, $\Sigma(l) = T_1$ and $\Gamma \mid \Sigma \vdash v_2 : T_1$ we know $\Gamma \mid \Sigma \vdash \mu'$. Lastly, by T-Unit we know $\Gamma \mid \Sigma \vdash \texttt{unit} : \mathit{Unit}$. Setting $\Sigma' = \Sigma$ we've shown for $\Sigma' \supseteq \Sigma$ we have $\Gamma \mid \Sigma' \vdash t' : T$ and $\Gamma \mid \Sigma' \vdash \mu'$. Thus, the E-Assign case holds.

Case: E-DerefLoc
If E-DerefLoc was the last derivation we know $t =!l$, $t' = v$ and $\mu' = \mu$ with l a memory locations and v some value. We also have the premise that $\mu(l) = v$. The only typing derivation we can apply is T-Deref, thus we know $\Gamma \mid \Sigma \vdash !l : T_1$ with $T = T_1$, and have the premise $\Gamma \mid \Sigma \vdash l : \mathit{Ref}\, T_1$. It then follows that by the 3rd clause of the extended inversion lemma $\Sigma(l) = T_1$. Since we know μ is well-typed with respect to Γ and Σ, by the definition of $\Gamma \mid \Sigma \vdash \mu$ we have $\mu(l) : \Sigma(l)$. Thus with $\mu(l) = v$ we have $\Gamma \mid \Sigma \vdash v : T_1$. Setting $\Sigma' = \Sigma$, we've shown for Σ', $\Gamma \mid \Sigma' \vdash t' : T$ and $\Gamma \mid \Sigma' \vdash \mu$. Thus, the E-DerefLoc case holds.

Thus our base cases hold.

Induction step. We assume for all sub-derivations of $t \mid \mu \to t' \mid \mu'$ the property of preservation holds. We will prove that for all possible derivations $t \to t'$ our property holds. We remaining possible derivations are the following:

Case: E-Seq
If E-Seq was the last derivation we know $t = t_1; t_2$, $t' = t_1'; t_2$ and have the premise $t_1 \mid \mu \to t_1' \mid \mu'$. The only typing derivation we can apply to t is T-Seq thus we know t is typed T_2 for some context Γ and typing store Σ, thus $T = T_2$, and we have the premises $\Gamma \mid \Sigma \vdash t_1 : \mathit{Unit}$ and $\Gamma \mid \Sigma \vdash t_2 : T_2$. By our induction hypothesis on t_1 with our premises $t_1 \mid \mu \to t_1' \mid \mu'$, $\Gamma \mid \Sigma \vdash t_1 : \mathit{Unit}$ and $\Gamma \mid \Sigma \vdash \mu$ we know there exists $\Sigma' \supseteq \Sigma$ such that $\Gamma \mid \Sigma' \vdash t_1' : \mathit{Unit}$ and $\Gamma \mid \Sigma' \vdash \mu'$. With $\Sigma' \supseteq \Sigma$ and $\Gamma \mid \Sigma \vdash t_2 : T_2$, by Weakening Over Typing Stores we know $\Gamma \mid \Sigma' \vdash t_2 : T_2$. Thus, by T-Seq with our premises $\Gamma \mid \Sigma' \vdash t_1' : \mathit{Unit}$

and $\Gamma \,|\, \Sigma' \vdash t_2 : T_2$ we know $\Gamma \,|\, \Sigma' \vdash t_1'; t_2 : T_2$. Therefore we've shown there exists $\Sigma' \supseteq \Sigma$ such that $\Gamma \,|\, \Sigma' \vdash t' : T$ with $\Gamma \,|\, \Sigma' \vdash \mu'$, so our E-Seq case holds.

Case: E-Ref
We prove the E-Ref case similarly to E-Seq. With E-Ref we know $t = \texttt{ref}\ t_1$, $t' = \texttt{ref}\ t_1'$ and have the premise $t_1 \,|\, \mu \rightarrow t_1' \,|\, \mu'$. The only typing derivation we can apply to t is T-Ref thus we know $\Gamma \,|\, \Sigma \vdash \texttt{ref}\ t_1 : \mathit{Ref}\ T_1$, $T = \mathit{Ref}\ T_1$ and have the premise $\Gamma \,|\, \Sigma \vdash t_1 : T_1$. By our induction hypothesis on t_1 with our premises $t_1 \,|\, \mu \rightarrow t_1' \,|\, \mu'$, $\Gamma \,|\, \Sigma \vdash t_1 : T_1$ and $\Gamma \,|\, \Sigma \vdash \mu$ we know there exists $\Sigma' \supseteq \Sigma$ such that $\Gamma \,|\, \Sigma' \vdash t_1' : T_1$ and $\Gamma \,|\, \Sigma' \vdash \mu'$. By T-Ref with the premise $\Gamma \,|\, \Sigma' \vdash t_1' : T_1$ we have $\Gamma \,|\, \Sigma' \vdash \texttt{ref}\ t_1' : \mathit{Ref}\ T_1$. Therefore we've shown there exists $\Sigma' \supseteq \Sigma$ such that $\Gamma \,|\, \Sigma' \vdash t' : T$ with $\Gamma \,|\, \Sigma' \vdash \mu'$, so our E-Ref case holds.

Case: E-Assign1
We prove the E-Assign1 case similarly to E-Seq. With E-Assign1 we know $t = t_1 := t_2$, $t' = t_1' := t_2$ and have the premise $t_1 \,|\, \mu \rightarrow t_1' \,|\, \mu'$. The only typing derivation we can apply to t is T-Assign thus we know $\Gamma \,|\, \Sigma \vdash t_1 := t_2 : \mathit{Unit}$, $T = \mathit{Unit}$ and have the premises $\Gamma \,|\, \Sigma \vdash t_1 : \mathit{Ref}\, T_1$ and $\Gamma \,|\, \Sigma \vdash t_2 : T_1$. By our induction hypothesis on t_1 with our premises $t_1 \,|\, \mu \rightarrow t_1' \,|\, \mu'$, $\Gamma \,|\, \Sigma \vdash t_1 : \mathit{Ref}\ T_1$ and $\Gamma \,|\, \Sigma \vdash \mu$ we know there exists $\Sigma' \supseteq \Sigma$ such that $\Gamma \,|\, \Sigma' \vdash t_1' : \mathit{Ref}\ T_1$ and $\Gamma \,|\, \Sigma' \vdash \mu'$. With $\Sigma' \supseteq \Sigma$ and $\Gamma \,|\, \Sigma \vdash t_2 : T_1$, by Weakening Over Typing Stores we know $\Gamma \,|\, \Sigma' \vdash t_2 : T_1$. By T-Assign with the premises $\Gamma \,|\, \Sigma' \vdash t_1' : \mathit{Ref}\, T_1$ and $\Gamma \,|\, \Sigma' \vdash t_2 : T_1$ we have $\Gamma \,|\, \Sigma' \vdash t_1' := t_2 : \mathit{Unit}$. Therefore we've shown there exists $\Sigma' \supseteq \Sigma$ such that $\Gamma \,|\, \Sigma' \vdash t' : T$ with $\Gamma \,|\, \Sigma' \vdash \mu'$, so our E-Assign1 case holds.

Case: E-Assign2
We prove the E-Assign2 case similarly to E-Seq. With E-Assign2 we know $t = v_1 := t_2$, $t' = v_2 := t_2'$ with v_1 some value. We also have the premise $t_2 \,|\, \mu \rightarrow t_2' \,|\, \mu'$. The only typing derivation we can apply to t is T-Assign thus we know $\Gamma \,|\, \Sigma \vdash v_1 := t_2 : \mathit{Unit}$, $T = \mathit{Unit}$ and have the premises $\Gamma \,|\, \Sigma \vdash v_1 : \mathit{Ref}\, T_1$ and $\Gamma \,|\, \Sigma \vdash t_2 : T_1$. By our induction hypothesis on t_2 with our premises $t_2 \,|\, \mu \rightarrow t_2' \,|\, \mu'$, $\Gamma \,|\, \Sigma \vdash t_2 : T_1$ and $\Gamma \,|\, \Sigma \vdash \mu$ we know there exists $\Sigma' \supseteq \Sigma$ such that $\Gamma \,|\, \Sigma' \vdash t_2' : T_1$ and $\Gamma \,|\, \Sigma' \vdash \mu'$. With $\Sigma' \supseteq \Sigma$ and $\Gamma \,|\, \Sigma \vdash v_1 : \mathit{Ref}\ T_1$, by Weakening Over Typing Stores we know $\Gamma \,|\, \Sigma' \vdash v_1 : \mathit{Ref}\ T_1$. By T-Assign with the premises $\Gamma \,|\, \Sigma' \vdash v_1 : \mathit{Ref}\, T_1$ and $\Gamma \,|\, \Sigma' \vdash t_2' : T_1$ we have $\Gamma \,|\, \Sigma' \vdash v_1 := t_2' : \mathit{Unit}$. Therefore we've shown there exists $\Sigma' \supseteq \Sigma$ such that $\Gamma \,|\, \Sigma' \vdash t' : T$ with $\Gamma \,|\, \Sigma' \vdash \mu'$, so our E-Assign2 case holds.

Case: E-Deref
We prove the E-Deref case similarly to E-Ref. With E-Deref we know $t =!t_1$, $t' =!t_1'$ and have the premise $t_1 \,|\, \mu \rightarrow t_1' \,|\, \mu'$. The only typing derivation we can apply to t is T-Deref thus we know $\Gamma \,|\, \Sigma \vdash !t_1 : T_1$, $T = T_1$ and have the premise $\Gamma \,|\, \Sigma \vdash t_1 : \mathit{Ref}\ T_1$. By our induction hypothesis on t_1 with our premises $t_1 \,|\, \mu \rightarrow t_1' \,|\, \mu'$, $\Gamma \,|\, \Sigma \vdash t_1 : \mathit{Ref}\ T_1$ and $\Gamma \,|\, \Sigma \vdash \mu$ we know there exists $\Sigma' \supseteq \Sigma$ such that $\Gamma \,|\, \Sigma' \vdash t_1' : \mathit{Ref}\ T_1$ and $\Gamma \,|\, \Sigma' \vdash \mu'$. By T-Deref with the premise $\Gamma \,|\, \Sigma' \vdash t_1' : \mathit{Ref}\ T_1$ we have $\Gamma \,|\, \Sigma' \vdash !t_1' : T_1$. Therefore we've

shown there exists $\Sigma' \supseteq \Sigma$ such that $\Gamma \mid \Sigma' \vdash t' : T$ with $\Gamma \mid \Sigma' \vdash \mu'$, so our E-Deref case holds.

Therefore our induction step holds. We have shown for all possible typing derivations the preservation property holds.
Thus we've shown that the property of preservation holds for our augmented simply typed λ-Calculus.