Typing and Semantics of References

Sipho Kemkes

Jorrit de Boer

December 1 2023

References

Extending STLC with References

References

Extending STLC with References

```
  r = ref 5;
> r : Ref Nat
```

References

Extending STLC with References

```
  r = ref 5;
> r : Ref Nat

  !r;
> 5 : Nat
```

References

Extending STLC with References

```
  r = ref 5;
> r : Ref Nat

  !r;
> 5 : Nat

  r := 7;
  !r;
> 7 : Nat
```

Sequencing

```
  (r:=succ(!r); !r)
> 8 : Nat
```

Sequencing

```
  (r:=succ(!r); !r)
> 8 : Nat
```

equivalent to lambda term:

$(\lambda\_ : \text{Unit}.!r)(r := \text{succ}(!r))$

Aliasing

```
  (r = ref 8; s = r; s := succ(!s); !r)
> 9 : Nat
```

Aliasing

```
  (r = ref 8; s = r; s := succ(!s); !r)
> 9 : Nat

  (c = ref 0; incc = λ x : Unit. (c := succ(!c); !c)
> incc: Unit -> Nat
```

Aliasing

```
  (r = ref 8; s = r; s := succ(!s); !r)
> 9 : Nat

  (c = ref 0; incc = λ x : Unit. (c := succ(!c); !c)
> incc: Unit -> Nat

  incc unit;
> 1 : Nat
```

Potential problems

- References can cause type safety errors

Potential problems

- References can cause type safety errors

We will do:

- Define typing and evaluation rules
- Prove that these preserve type safety

Typing Rules

$$\frac{\Gamma \vdash t : T}{\Gamma \vdash \texttt{Ref}\ t : \texttt{Ref}\ T}\text{T-Ref}$$

$$\frac{\Gamma \vdash t : \texttt{Ref}\ T}{\Gamma \vdash !t : T}\text{T-Deref}$$

$$\frac{\Gamma \vdash t_1 : \texttt{Ref}\ T \quad \Gamma \vdash t_2 : T}{\Gamma \vdash t_1 := t_2 : \text{Unit}}\text{T-Assign}$$

Evaluation

We abstract the stack and references to that stack to:

- Locations $\mathcal{L}$
- Store $\mu : \mathcal{L} \to v$

Instead of $t \to t'$ we now get: $t \mid \mu \ \to \ t' \mid \mu'$

Evaluation

We abstract the stack and references to that stack to:

- Locations $\mathcal{L}$
- Store $\mu : \mathcal{L} \to v$

Instead of $t \to t'$ we now get: $t \mid \mu \ \to \ t' \mid \mu'$

$$(\lambda x : T.t)v \mid \mu \to [x \to v]t \mid \mu \qquad \text{(E-AppAbs)}$$

Evaluation Rules

$$\frac{t_1 \mid \mu \to t_1' \mid \mu'}{t_1\ t_2 \mid \mu \to t_1'\ t_2 \mid \mu'}\text{E-App1}$$

$$\frac{t \mid \mu \to t' \mid \mu'}{v\ t \mid \mu \to v\ t' \mid \mu'}\text{E-App2}$$

$$\frac{t \mid \mu \to t' \mid \mu'}{!t \mid \mu \to !t' \mid \mu'}\text{E-Deref}$$

$$\frac{\mu(l) = v}{!l \mid \mu \to v \mid \mu}\text{E-DerefLoc}$$

$$\frac{t_1 \mid \mu \to t_1' \mid \mu'}{t_1 := t_2 \mid \mu \to t_1' := t_2 \mid \mu'}\text{E-Assign1}$$

$$\frac{t \mid \mu \to t' \mid \mu'}{v := t \mid \mu \to v := t' \mid \mu'}\text{E-Assign2}$$

$$\frac{t \mid \mu \to t' \mid \mu'}{\texttt{Ref}\ t \mid \mu \to \texttt{Ref}\ t' \mid \mu'}\text{E-Ref}$$

$$\frac{l \notin \mathrm{dom}(\mu)}{\texttt{Ref}\ v \mid \mu \to l \mid (\mu, l \to v)}\text{E-RefV}$$

$$l := v \mid \mu \to \text{Unit} \mid [l \to v]\mu \qquad \text{E-Assign}$$

Store Typing

$$\frac{\Gamma \mid \mu \vdash \mu(l) : T}{\Gamma \mid \mu \vdash l : \texttt{Ref}\ T}$$

Store Typing

$$\frac{\Gamma \mid \mu \vdash \mu(l) : T}{\Gamma \mid \mu \vdash l : \texttt{Ref}\ T}$$

Problems

- Inefficient

Store Typing

$$\frac{\Gamma \mid \mu \vdash \mu(l) : T}{\Gamma \mid \mu \vdash l : \texttt{Ref}\ T}$$

Problems

- Inefficient
- Cyclic reference.

$$\mu = (l_1 \mapsto \lambda x : \text{Nat}.(!l_2)x,$$
$$l_2 \mapsto \lambda x : \text{Nat}.(!l_1)x,)$$

Store Typing Better Way

Solution: store typing from locations to types

$\Sigma : \mathcal{L} \to t$

Store Typing Better Way

Solution: store typing from locations to types

$\Sigma : \mathcal{L} \to t$

$$\frac{\Gamma \mid \Sigma \vdash \Sigma(l) = T}{\Gamma \mid \Sigma \vdash l : \mathsf{Ref}\ T}\text{T-Loc}$$

Store Typing Better Way

Solution: store typing from locations to types

$\Sigma : \mathcal{L} \to t$

$$\frac{\Gamma \mid \Sigma \vdash \Sigma(l) = T}{\Gamma \mid \Sigma \vdash l : \texttt{Ref}\ T}\text{T-Loc}$$

$$\frac{\Gamma \mid \Sigma \vdash t : \texttt{Ref}\ T}{\Gamma \mid \Sigma \vdash !t : T}\text{T-Deref}$$

$$\frac{\Gamma \mid \Sigma \vdash t : T}{\Gamma \mid \Sigma \vdash \texttt{ref}\ t : \texttt{Ref}\ T}\text{T-Ref}$$

$$\frac{\Gamma \mid \Sigma \vdash t_1 : \texttt{Ref}\ T \qquad \Gamma \mid \Sigma \vdash t_2 : T}{\Gamma \mid \Sigma \vdash t_1 := t_2 : \text{Unit}}\text{T-Deref}$$

Old Preservation Theorem

Theorem [Preservation]:

If $\Gamma \vdash t : T$ and $t \to t'$ then $\Gamma \vdash t' : T$

New Preservation Theorem

Theorem [Preservation]:

If $\Gamma \mid \Sigma \vdash t : T$ and $t \mid \mu \rightarrow t' \mid \mu'$ then $\Gamma \mid \Sigma \vdash t' : T$

New Preservation Theorem Attempt 2

Definition: A store is *well typed* with respect to a typing context Γ and a store typing Σ, written $\Gamma \mid \Sigma \vdash \mu$ if $dom(\mu) = dom(\sigma)$ and $\Gamma \mid \Sigma \vdash \mu(l) : \Sigma(l)$ for all $l \in dom(\mu)$.

New Preservation Theorem Attempt 2

Definition: A store is *well typed* with respect to a typing context Γ and a store typing Σ, written $\Gamma \mid \Sigma \vdash \mu$ if $dom(\mu) = dom(\sigma)$ and $\Gamma \mid \Sigma \vdash \mu(l) : \Sigma(l)$ for all $l \in dom(\mu)$.

Theorem [Preservation]:
If $\Gamma \mid \Sigma \vdash t : T$ and $t \mid \mu \rightarrow t' \mid \mu'$ and $\Gamma \mid \Sigma \vdash \mu$
then $\Gamma \mid \Sigma \vdash t' : T$

New Preservation Theorem Attempt 3

Definition: A store is *well typed* with respect to a typing context Γ and a store typing Σ, written $\Gamma \mid \Sigma \vdash \mu$ if $dom(\mu) = dom(\sigma)$ and $\Gamma \mid \Sigma \vdash \mu(l) : \Sigma(l)$ for all $l \in dom(\mu)$.

Theorem [Preservation]:
If $\Gamma \vdash t : T$ and $t \mid \mu \rightarrow t' \mid \mu'$ and $\Gamma \mid \Sigma \vdash \mu$
then there exists some $\Sigma' \supseteq \Sigma$ such that
$\Gamma \mid \Sigma \vdash t' : T$ and $\Gamma \mid \Sigma' \vdash \mu'$

Proof New Preservation Theorem

Theorem [Preservation]: If $\Gamma \vdash t : T$ and $t \mid \mu \rightarrow t' \mid \mu'$ and $\Gamma \mid \Sigma \vdash \mu$ then there exists some $\Sigma' \supseteq \Sigma$ such that $\Gamma \mid \Sigma \vdash t' : T$ and $\Gamma \mid \Sigma' \vdash \mu'$

Proof New Preservation Theorem

Theorem [Preservation]: If $\Gamma \vdash t : T$ and $t \mid \mu \to t' \mid \mu'$ and $\Gamma \mid \Sigma \vdash \mu$ then there exists some $\Sigma' \supseteq \Sigma$ such that $\Gamma \mid \Sigma \vdash t' : T$ and $\Gamma \mid \Sigma' \vdash \mu'$

Lemma [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 New Preservation Theorem

Theorem [Preservation]: If $\Gamma \vdash t : T$ and $t \mid \mu \to t' \mid \mu'$ and $\Gamma \mid \Sigma \vdash \mu$ then there exists some $\Sigma' \supseteq \Sigma$ such that $\Gamma \mid \Sigma \vdash t' : T$ and $\Gamma \mid \Sigma' \vdash \mu'$

Lemma [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 the type derivation

Proof New Preservation Theorem

Theorem [Preservation]: If $\Gamma \vdash t : T$ and $t \mid \mu \rightarrow t' \mid \mu'$ and $\Gamma \mid \Sigma \vdash \mu$ then there exists some $\Sigma' \supseteq \Sigma$ such that $\Gamma \mid \Sigma \vdash t' : T$ and $\Gamma \mid \Sigma' \vdash \mu'$

Lemma [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 the type derivation

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

Proof New Preservation Theorem

Theorem [Preservation]: If $\Gamma \vdash t : T$ and $t \mid \mu \rightarrow t' \mid \mu'$ and $\Gamma \mid \Sigma \vdash \mu$ then there exists some $\Sigma' \supseteq \Sigma$ such that $\Gamma \mid \Sigma \vdash t' : T$ and $\Gamma \mid \Sigma' \vdash \mu'$

Lemma [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 the type derivation

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

Unfolding definition of well typed store

Proof New Preservation Theorem

Theorem [Preservation]: If $\Gamma \vdash t : T$ and $t \mid \mu \rightarrow t' \mid \mu'$ and $\Gamma \mid \Sigma \vdash \mu$ then there exists some $\Sigma' \supseteq \Sigma$ such that $\Gamma \mid \Sigma \vdash t' : T$ and $\Gamma \mid \Sigma' \vdash \mu'$

Lemma [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 the type derivation

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

Unfolding definition of well typed store

Lemma: If $\Gamma \mid \Sigma \vdash t : T$ and $\Sigma' \supseteq \Sigma$ then $\Gamma \mid \Sigma' \vdash t : T$

Proof New Preservation Theorem

Theorem [Preservation]: If $\Gamma \vdash t : T$ and $t \mid \mu \rightarrow t' \mid \mu'$ and $\Gamma \mid \Sigma \vdash \mu$ then there exists some $\Sigma' \supseteq \Sigma$ such that $\Gamma \mid \Sigma \vdash t' : T$ and $\Gamma \mid \Sigma' \vdash \mu'$

Lemma [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 the type derivation

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

Unfolding definition of well typed store

Lemma: If $\Gamma \mid \Sigma \vdash t : T$ and $\Sigma' \supseteq \Sigma$ then $\Gamma \mid \Sigma' \vdash t : T$

Proof by induction on type

New Progress Theorem

Theorem [Progress]: Let t be a closed well typed term ($\emptyset \mid \Sigma \vdash t : T$) then one of the following:

- t is a value
- for any store μ such that $\emptyset \mid \Sigma \vdash \mu$ there is some term t' and store μ' with $t \mid \mu \rightarrow t' \mid \mu'$

New Progress Theorem

Theorem [Progress]: Let t be a closed well typed term ($\emptyset \mid \Sigma \vdash t : T$) then one of the following:

- t is a value
- for any store μ such that $\emptyset \mid \Sigma \vdash \mu$ there is some term t' and store μ' with $t \mid \mu \rightarrow t' \mid \mu'$

Proof by induction on the typing derivation

New Strongly Normalizing Theorem

New Strongly Normalizing Theorem

?