Correctness Proof of GC
ENE4014 Programming Languages, Spring 2019
Woosuk Lee

Definition 1. *For $m_1, m_2 \in Mem$, $m_1 \sqsubseteq m_2$ if and only if*

$$\forall l \in Dom(m_1).\ m_1(l) = m_2(l).$$

Lemma 1. *If $\rho, \sigma_0 \vdash E \Rightarrow v, \sigma_1$ and $\sigma_0 \sqsubseteq \sigma_0'$, then*

$$\rho, \sigma_0' \vdash E \Rightarrow v, \sigma_1'$$

where $\sigma_1 \sqsubseteq \sigma_1'$

Proof. By induction on E. □

Theorem 1. *If $\rho, \sigma_0 \vdash E \Rightarrow v, \sigma_1$, then*

$$\rho, \mathsf{GC}(\rho, \sigma_0) \vdash E \Rightarrow v, \sigma_1'$$

for some $\sigma_1' \in Mem$ such that $\mathsf{GC}(\rho, \sigma_1) \sqsubseteq \sigma_1'$.

Proof. By induction on E.

- Case $E = n$: we should prove

  $$\rho, \sigma_0 \vdash n \Rightarrow n, \sigma_0 \implies \rho, \mathsf{GC}(\rho, \sigma_0) \vdash n \Rightarrow n, \sigma_0'$$

  where $\mathsf{GC}(\rho, \sigma_0) \sqsubseteq \sigma_0'$.
  By the inference rule,

  $$\rho, \mathsf{GC}(\rho, \sigma_0) \vdash n \Rightarrow n, \mathsf{GC}(\rho, \sigma_0).$$

  Therefore, $\sigma_0' = \mathsf{GC}(\rho, \sigma_0) \sqsupseteq \mathsf{GC}(\rho, \sigma_0)$.

- Case $E = x$: we should prove

  $$\rho, \sigma_0 \vdash x \Rightarrow \sigma(\rho(x)), \sigma_0 \implies \rho, \mathsf{GC}(\rho, \sigma_0) \vdash x \Rightarrow \sigma(\rho(x)), \sigma_0'$$

  where $\mathsf{GC}(\rho, \sigma_0) \sqsubseteq \sigma_0'$.
  By the inference rule,

  $$\rho, \mathsf{GC}(\rho, \sigma_0) \vdash x \Rightarrow \sigma(\rho(x)), \mathsf{GC}(\rho, \sigma_0).$$

  Therefore, $\sigma_0' = \mathsf{GC}(\rho, \sigma_0) \sqsupseteq \mathsf{GC}(\rho, \sigma_0)$.

- Case $E = E_1 + E_2$: we should prove

  $$\rho, \sigma_0 \vdash E_1 + E_2 \Rightarrow v_1 + v_2, \sigma_2 \implies \rho, \mathsf{GC}(\rho, \sigma_0) \vdash E_1 + E_2 \Rightarrow v_1 + v_2, \sigma_2''$$

  where

  $$\rho, \sigma_0 \vdash E_1 \Rightarrow v_1, \sigma_1$$

  $$\rho, \sigma_1 \vdash E_2 \Rightarrow v_2, \sigma_2$$

  and $\mathsf{GC}(\rho, \sigma_2) \sqsubseteq \sigma_2''$.

  By the inductive hypothesis,

  $$\rho, \mathsf{GC}(\rho, \sigma_0) \vdash E_1 \Rightarrow v_1, \sigma_1' \tag{1}$$

  $$\rho, \mathsf{GC}(\rho, \sigma_1) \vdash E_2 \Rightarrow v_2, \sigma_2' \tag{2}$$

  where $\mathsf{GC}(\rho, \sigma_1) \sqsubseteq \sigma_1'$ and $\mathsf{GC}(\rho, \sigma_2) \sqsubseteq \sigma_2'$.

  By applying Lemma 1 into (2),

  $$\rho, \sigma_1' \vdash E_2 \Rightarrow v_2, \sigma_2'' \tag{3}$$

  where $\sigma_2' \sqsubseteq \sigma_2''$.

  By (1) and (3),

  $$\rho, \mathsf{GC}(\rho, \sigma_0) \vdash E_1 + E_2 \Rightarrow v_1 + v_2, \sigma_2''.$$

  Because $\mathsf{GC}(\rho, \sigma_2) \sqsubseteq \sigma_2'$ and $\sigma_2' \sqsubseteq \sigma_2''$, $\mathsf{GC}(\rho, \sigma_2) \sqsubseteq \sigma_2''$, which proves the case.

- Case $E = \texttt{if}\ E_1\ \texttt{then}\ E_2\ \texttt{else}\ E_3$ (when E_1 evaluates to true): we should prove

  $$\rho, \sigma_0 \vdash \texttt{if}\ E_1\ \texttt{then}\ E_2\ \texttt{else}\ E_3 \Rightarrow v, \sigma_2 \implies \rho, \mathsf{GC}(\rho, \sigma_0) \vdash \texttt{if}\ E_1\ \texttt{then}\ E_2\ \texttt{else}\ E_3 \Rightarrow v, \sigma_2''$$

  where

  $$\rho, \sigma_0 \vdash E_1 \Rightarrow \mathit{true}, \sigma_1$$

  $$\rho, \sigma_1 \vdash E_2 \Rightarrow v, \sigma_2$$

  and $\mathsf{GC}(\rho, \sigma_2) \sqsubseteq \sigma_2''$.

  By the inductive hypothesis,

  $$\rho, \mathsf{GC}(\rho, \sigma_0) \vdash E_1 \Rightarrow \mathit{true}, \sigma_1' \tag{4}$$

  $$\rho, \mathsf{GC}(\rho, \sigma_1) \vdash E_2 \Rightarrow v, \sigma_2' \tag{5}$$

  where $\mathsf{GC}(\rho, \sigma_1) \sqsubseteq \sigma_1'$ and $\mathsf{GC}(\rho, \sigma_2) \sqsubseteq \sigma_2'$.

  By applying Lemma 1 into (5),

  $$\rho, \sigma_1' \vdash E_2 \Rightarrow v_2, \sigma_2'' \tag{6}$$

where $\sigma'_2 \sqsubseteq \sigma''_2$.

By (4) and (6),

$$\rho, \mathsf{GC}(\rho, \sigma_0) \vdash \texttt{if } E_1 \texttt{ then } E_2 \texttt{ else } E_3 \Rightarrow v, \sigma''_2.$$

Because $\mathsf{GC}(\rho, \sigma_2) \sqsubseteq \sigma'_2$ and $\sigma'_2 \sqsubseteq \sigma''_2$, $\mathsf{GC}(\rho, \sigma_2) \sqsubseteq \sigma''_2$, which proves the case.

- Case $E = \texttt{if } E_1 \texttt{ then } E_2 \texttt{ else } E_3$ (when E_1 evaluates to false): Similar to the above case.

- Case $E = \texttt{proc } x\ E'$: Similar to the above case where $E = x$.

- Case $E = x := E'$: we should prove

$$\rho, \sigma_0 \vdash x := E' \Rightarrow v, \sigma_2 \implies \rho, \mathsf{GC}(\rho, \sigma_0) \vdash x := E' \Rightarrow v, \sigma''_2$$

where

$$\rho, \sigma_0 \vdash E' \Rightarrow v, \sigma_1$$
$$\sigma_2 = [\rho(x) \mapsto v]\sigma_1$$

and $\mathsf{GC}(\rho, \sigma_2) \sqsubseteq \sigma''_2$.

By the inductive hypothesis,

$$\rho, \mathsf{GC}(\rho, \sigma_0) \vdash E' \Rightarrow v, \sigma'_1 \qquad (7)$$

where $\mathsf{GC}(\rho, \sigma_1) \sqsubseteq \sigma'_1$.

By (7),

$$\rho, \mathsf{GC}(\rho, \sigma_0) \vdash x := E' \Rightarrow v, [\rho(x) \mapsto v]\sigma'_1.$$

Let $\sigma''_2 = [\rho(x) \mapsto v]\sigma'_1$.

$$\begin{array}{ll}
\mathsf{GC}(\rho, \sigma_1) \sqsubseteq \sigma'_1 & \\
[\rho(x) \mapsto v]\mathsf{GC}(\rho, \sigma_1) \sqsubseteq [\rho(x) \mapsto v]\sigma'_1 & \\
\mathsf{GC}(\rho, [\rho(x) \mapsto v]\sigma_1) \sqsubseteq [\rho(x) \mapsto v]\sigma'_1 & (\rho(x) \in \mathsf{reach}(\rho, \sigma_1)) \\
\mathsf{GC}(\rho, \sigma_2) \sqsubseteq \sigma''_2 & (\text{By the definitions of } \sigma_2, \sigma''_2)
\end{array}$$

- Other cases: Exercise.

$\square$