Handling loops

Semantics of commands: The meaning of a command $\Gamma \vdash S$ is a function $[\![\Gamma]\!] \to [\![\Gamma]\!]_\perp$ that takes a store η, and returns a possibly updated store or returns $\perp$ which indicates divergence.

$$[\![\Gamma \vdash \text{while } e \text{ do } S]\!] \quad = \quad \mathrm{lub}\ f \quad \text{where}$$

$$f_0\ \eta \ = \perp$$

$$\begin{aligned} f_{i+1}\ \eta = {} & \text{let } b = [\![\Delta^\dagger \vdash e : \mathtt{bool}]\!]\eta \text{ in} \\ & \text{if } b = 0 \text{ then } \eta \text{ else} \\ & \text{let } \hat{\eta} = [\![\Delta^\dagger \vdash S]\!]\eta \text{ in } f_i\ \hat{\eta} \end{aligned}$$

We assume that the (metalanguage) construct, let $x = e_1$ in e_2, is strict: If the value of e_1 is $\perp$ then that is the value of the entire let expression; otherwise, its value is the value of e_2 with x bound to the value of e_1.

Predicates

The predicate $wconf$ on $[\![\Gamma]\!] \rightarrow [\![\Gamma]\!]_\perp$ is defined as:

$$wconf\ \mathsf{f} \quad \Longleftrightarrow \quad \forall \eta \in [\![\Gamma]\!] \bullet \mathsf{f}\eta \neq \perp \ \Rightarrow \ \eta \sim_{[\![\Gamma]\!]} \mathsf{f}\eta$$

The predicate $nonint$ on $[\![\Gamma]\!] \rightarrow [\![\Gamma]\!]_\perp$ is defined as:

$$nonint\ \mathsf{f} \quad \Longleftrightarrow \quad \forall (\eta, \eta') \bullet (\eta \sim \eta') \wedge (\mathsf{f}\eta \neq \perp \neq \mathsf{f}\eta') \ \Rightarrow \ \mathsf{f}\eta \sim \mathsf{f}\eta'$$

Technical results revisited

Lemma (write confinement of commands) Suppose $\Delta \vdash S : (\mathtt{com}\ \kappa)$. Then $\kappa = H \Rightarrow \mathit{wconf}[\![\Delta^\dagger \vdash S]\!]$.

Theorem (safe commands are noninterfering) Suppose $\Delta \vdash S : (\mathtt{com}\ \kappa)$. Then $\mathit{nonint}[\![\Delta^\dagger \vdash S]\!]$.

The proofs of the above require additional lemmas for the while case:

1. $\forall i \bullet \mathit{wconf}\ f_i$
2. $(\forall i \bullet \mathit{wconf}\ f_i) \Rightarrow \mathit{wconf}\ (\mathrm{lub}\ f)$
3. $\forall i \bullet \mathit{nonint}\ f_i$
4. $(\forall i \bullet \mathit{nonint}\ f_i) \Rightarrow \mathit{nonint}\ (\mathrm{lub}\ f)$