

1 Discussion: Type Safety For References

It was hard proving type safety for references in combination with the Hindley Milner type system. Tofte designed a type system extension, which was wrong. Therefore, his proof of soundness was also wrong. Tofte's experience gave rise to a syntactic approach to type safety. Wright and Felleisen in 1992 presented a proof technique based on small-step semantics.

As a first attempt to state the type safety theorem, consider the following:

Theorem 1.1 $\Sigma, \Gamma \vdash e : t_1 \wedge \mu, e \mapsto \mu', e' \Rightarrow \Sigma, \Gamma \vdash e' : t_1$

The statement of Theorem 1.1 is wrong because of this counter-example: $l : \text{int}, \Gamma \vdash !l : \text{int} \wedge l \rightarrow \lambda x.x, !l \mapsto \mu', \lambda x.x \Rightarrow \Sigma, \Gamma \vdash \lambda x.x : \text{int}$. We can never produce a derivation tree that ends with $\Sigma, \Gamma \vdash \lambda x.x : \text{int}$.

To address the counterexample, we need a notion of $\Sigma \vdash \mu$.

$$\frac{\cdot, \cdot \vdash \mu(l) : \Sigma(l)}{\Sigma \vdash \mu}$$

The above notion does not work. If $\mu = \{l \rightarrow \text{ref } l'\} \uplus \{l' \rightarrow \text{ref } 17\}$, then $\mu(l) = \text{ref } l'$, but since Σ is not passed above the line, we cannot type $\text{ref } l'$. Correcting this, we have

$$\frac{\Sigma, \cdot \vdash \mu(l) : \Sigma(l)}{\Sigma \vdash \mu}$$

The latter is enough to talk about closed terms.

In Theorem 1.1 we captured an invariant that is not broken (type preservation), but we missed progress. Incorporating this observation and the definition of $\Sigma \vdash \mu$, we come to a new version of Theorem 1.1:

Theorem 1.2 $\forall \Sigma : L \rightarrow T. \forall \mu : L \rightarrow V, \forall e, t_1. \Sigma, \cdot \vdash e : t_1 \wedge \mu, e \mapsto \mu', e' \Rightarrow \Sigma, \cdot \vdash e' : t_1 \wedge \Sigma \vdash \mu'$

We don't use Γ as our terms are closed. The induction hypothesis would not get stuck because of adding to the environment (check all eval rules).

Does Theorem 1.2 work? Consider the example:

$\forall \Sigma : L \rightarrow T. \forall \mu : L \rightarrow V. \forall e, t_1. \cdot, \cdot \vdash \text{ref } 17 : \text{int ref} \wedge \cdot, \text{ref } 17 \mapsto l_1 \rightarrow 17, l_1 \Rightarrow \cdot, \cdot \vdash l_1 : \text{int ref} \wedge \Sigma \vdash \mu'$. This is wrong. We need a new Σ on the right side of Theorem 1.2. So finally, we have

Theorem 1.3 $\forall \Sigma : L \rightarrow T. \forall \mu : L \rightarrow V. \forall e, t_1. \Sigma, \cdot \vdash e : t_1 \wedge \Sigma \vdash \mu \wedge \mu, e \mapsto \mu', e' \Rightarrow \exists \Sigma'. \Sigma', \cdot \vdash e' : t_1 \wedge \Sigma' \vdash \mu' \wedge \Sigma' \geq \Sigma$

where

$$\frac{\forall l \in \text{dom}(\mu) . \Sigma, \cdot \vdash \mu(l) : \Sigma(l)}{\Sigma \vdash \mu} \quad \frac{\forall l \in \text{dom}\Sigma. \Sigma(l) = \Sigma'(l)}{\Sigma' \geq \Sigma}$$

Gregory observed that the last part of the theorem statement, $\text{dom}(\Sigma') = \text{dom}(\mu')$ is not possible to prove, as we don't know if $\text{dom}(\Sigma) = \text{dom}(\mu)$. Thus we should either remove that result or assume that $\text{dom}(\Sigma) = \text{dom}(\mu)$ in the premises.