Verifier Well-formed Definitions

Jenna Wise, Jonathan Aldrich, Cameron Wong

February 2, 2019

1 Type synthesis rules for expressions

Γ is the context mapping variables to their declared types, Δ is the context mapping classes and field names to the associated types.

$$\frac{\Gamma[x] = \tau}{\Gamma, \Delta \vdash x : \tau} \qquad \frac{}{\Gamma, \Delta \vdash n : \mathit{int}} \qquad \frac{}{\Gamma, \Delta \vdash \mathit{null} : \top}$$

$$\frac{\Gamma, \Delta \vdash e : C \quad \Delta[C.f] = \tau}{\Gamma, \Delta \vdash e.f : \tau} \qquad \frac{\Gamma, \Delta \vdash e_1 : \mathit{int} \quad \Gamma, \Delta \vdash e_2 : \mathit{int}}{\Gamma, \Delta \vdash e_1 \oplus e_2 : \mathit{int}}$$

2 Well-formed rules for concrete contracts

Missing rule for abstract predicates.

$$\frac{}{\Gamma, \Delta \vdash \mathrm{true}\ \text{OK}} \qquad \frac{\Gamma, \Delta \vdash e_1 : \mathit{int} \quad \Gamma, \Delta \vdash e_2 : \mathit{int}}{\Gamma, \Delta \vdash e_1 \odot e_2\ \text{OK}} \qquad \frac{\Gamma, \Delta \vdash e.f : \tau}{\Gamma, \Delta \vdash \mathrm{acc}(e.f)\ \text{OK}}$$

$$\frac{\Gamma, \Delta \vdash \phi_1\ \text{OK} \quad \Gamma, \Delta \vdash \phi_2\ \text{OK}}{\Gamma, \Delta \vdash \phi_1 * \phi_2\ \text{OK}}$$

3 Well-formed rules for gradual contracts

TODO

4 Well-formed rules for statements

$\Gamma, \Delta \vdash s \dashv \Gamma'$ is the judgment stating that s is well-formed under contexts Γ, Δ and that the variable type context is Γ' after s.

TODO: if, method calls, release, hold

$$\frac{}{\Gamma, \Delta \vdash skip \dashv \Gamma} \qquad \frac{\Gamma, \Delta \vdash s_1 \dashv \Gamma' \quad \Gamma, \Delta \vdash s_2 \dashv \Gamma''}{\Gamma, \Delta \vdash s_1; s_2 \dashv \Gamma''} \qquad \frac{\Gamma, \Delta \vdash e : T}{\Gamma, \Delta \vdash T\ x := e \dashv \Gamma[x \mapsto T]}$$

$$\frac{\Gamma, \Delta \vdash x : C \quad \Delta[C.f] = \tau \quad \Gamma, \Delta \vdash y : \tau}{\Gamma, \Delta \vdash x.f := y \dashv \Gamma} \qquad \frac{}{\Gamma, \Delta \vdash x := newC \dashv \Gamma[x \mapsto C]} \qquad \frac{\Gamma, \Delta \vdash \phi\ \textsc{ok}}{\Gamma, \Delta \vdash assert\ \phi \dashv \Gamma}$$