

# Verifier Well-formed Definitions

Jenna Wise, Jonathan Aldrich, Cameron Wong

February 1, 2019

## 1 Type synthesis rules for expressions

$\Gamma$  is the context mapping variables to their declared types,  $\Delta$  is the context mapping classes and field names to the associated types.

$$\begin{array}{c} \frac{\Gamma[x] = \tau}{\Gamma, \Delta \vdash x : \tau} \qquad \frac{}{\Gamma, \Delta \vdash n : int} \qquad \frac{}{\Gamma, \Delta \vdash null : \top} \\[10pt] \frac{\Gamma, \Delta \vdash e : C \quad \Delta[C.f] = \tau}{\Gamma, \Delta \vdash e.f : \tau} \qquad \frac{\Gamma, \Delta \vdash e_1 : int \quad \Gamma, \Delta \vdash e_2 : int}{\Gamma, \Delta \vdash e_1 \oplus e_2 : int} \end{array}$$

## 2 Well-formed rules for concrete contracts

Missing rule for abstract predicates.

$$\begin{array}{c} \frac{}{\Gamma, \Delta \vdash \text{true OK}} \qquad \frac{\Gamma, \Delta \vdash e_1 : int \quad \Gamma, \Delta \vdash e_2 : int}{\Gamma, \Delta \vdash e_1 \odot e_2 \text{ OK}} \qquad \frac{\Gamma, \Delta \vdash e.f : \tau}{\Gamma, \Delta \vdash \text{acc}(e.f) \text{ OK}} \\[10pt] \frac{\Gamma, \Delta \vdash \phi_1 \text{ OK} \quad \Gamma, \Delta \vdash \phi_2 \text{ OK}}{\Gamma, \Delta \vdash \phi_1 * \phi_2 \text{ OK}} \end{array}$$

## 3 Well-formed rules for gradual contracts

TODO

## 4 Well-formed rules for statements

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

TODO: if, method calls, release, hold

$$\begin{array}{c}
\overline{\Gamma, \Delta \vdash \text{skip} >: \Gamma} \qquad \frac{\Gamma, \Delta \vdash s_1 >: \Gamma' \quad \Gamma, \Delta \vdash s_2 >: \Gamma''}{\Gamma, \Delta \vdash s_1; s_2 >: \Gamma''} \qquad \frac{\Gamma, \Delta \vdash e : T}{\Gamma, \Delta \vdash T \ x := e >: \Gamma[x \mapsto T]} \\
\\
\frac{\Gamma, \Delta \vdash x : C \quad \Delta[C.f] = \tau \quad \Gamma, \Delta \vdash y : \tau}{\Gamma, \Delta \vdash x.f := y >: \Gamma} \qquad \overline{\Gamma, \Delta \vdash x := \text{new} C >: \Gamma[x \mapsto C]} \qquad \frac{\Gamma, \Delta \vdash \phi \text{ OK}}{\Gamma, \Delta \vdash \text{assert } \phi >: \Gamma}
\end{array}$$