Verifier WLP Definitions

Jenna Wise, Johannes Bader, Jonathan Aldrich, Joshua Sunshine

October 30, 2018

Weakest liberal precondition calculi definitions over self-framed formulas

$$\text{WLP}(skip, \widehat{\phi}) = \widehat{\phi}$$

$$\text{WLP}(s_1; s_2, \widehat{\phi}) = \text{WLP}(s_1, \text{WLP}(s_2, \widehat{\phi}))$$

$$\text{WLP}(T\ x, \widehat{\phi}) = \widehat{\phi}\,[\text{defaultValue}(T)/x]$$

$$\text{WLP}(x := e, \widehat{\phi}) = \max_{\Rightarrow} \left\{ \widehat{\phi}' \mid \widehat{\phi}' \Rightarrow \widehat{\phi}[e/x] \quad \wedge \quad \widehat{\phi}' \Rightarrow \text{acc}(e) \right\}$$

$$\text{WLP}(if\ (x \odot y)\ \{s_1\}\ else\ \{s_2\}, \widehat{\phi}) = undefined$$

$$\text{WLP}(x.f := y, \widehat{\phi}) = \text{acc}(x.f) * \max_{\Rightarrow} \left\{ \widehat{\phi}' \mid \widehat{\phi}' * \text{acc}(x.f) * (x.f = y) \Rightarrow \widehat{\phi} \ \wedge\ \widehat{\phi}' * \text{acc}(x.f) \in \textsc{SatFormula} \right\}$$

$$\text{WLP}(x := new\ C, \widehat{\phi}) = \max_{\Rightarrow} \left\{ \widehat{\phi}' \mid \widehat{\phi}' * (x \neq null) * \overline{\text{acc}(x.f_i) * (x.f_i = \text{defaultValue}(T_i))} \Rightarrow \widehat{\phi} \right\}$$
$$\text{where fields}(C) = \overline{T_i\ f_i}$$

$$\text{WLP}(y := z.m(\overline{x}), \widehat{\phi}) = undefined$$

$$\text{WLP}(y := z.m_C(\overline{x}), \widehat{\phi}) = \max_{\Rightarrow} \Big\{ \widehat{\phi}' \mid y \notin \text{FV}(\widehat{\phi}') \quad \wedge \quad \widehat{\phi}' \Rightarrow (z \neq null) * \text{pre}(C, m) \left[z/this, \overline{x_i/\text{params}(C, m)_i} \right]$$
$$\wedge \quad \widehat{\phi}' * \text{post}(C, m) \left[z/this, \overline{x_i/\text{old}(\text{params}(C, m)_i)}, y/result \right] \Rightarrow \widehat{\phi} \Big\}$$

$$\text{WLP}(assert\ \phi_a, \widehat{\phi}) = \max_{\Rightarrow} \left\{ \widehat{\phi}' \mid \widehat{\phi}' \Rightarrow \widehat{\phi} \quad \wedge \quad \widehat{\phi}' \Rightarrow \phi_a \right\}$$

$$\text{WLP}(release\ \phi_a, \widehat{\phi}) = undefined$$

$$\text{WLP}(hold\ \phi_a\ \{s\}, \widehat{\phi}) = undefined$$

Note:

Dynamic method calls: Dynamic method calls are left undefined, because we are not verifying programs with dynamic dispatch at this time (all method calls should be static method calls). They are included in the grammar for future implementation.

Release & hold: Release and hold are left undefined, because I need to make sure that they are necessary in the grammar since we are doing WLP instead of Hoare logic.

If: Definition coming soon.

Helpful function definitions

TBD