Jones's rely/guarantee logic

Aaron Turon

January 28, 2010

1 Language and operational semantics

$$S \quad ::= \quad \textbf{skip} \mid x := e \mid S; S \mid S \parallel S \mid \textbf{if } p \textbf{ then } S \textbf{ else } S \mid \textbf{while } p \textbf{ do } S$$

Recall $\sigma \in \Sigma$ is a store, mapping variables to values. We assume given semantics of expressions $[\![e]\!]^\sigma$ and predicates $[\![p]\!]$.

$$\frac{}{x := e, \sigma \longrightarrow \textbf{skip}, \sigma[[\![e]\!]^\sigma / x]} \qquad \frac{S_1, \sigma \longrightarrow S_1', \sigma'}{S_1; S_2, \sigma \longrightarrow S_1'; S_2, \sigma'} \qquad \frac{}{\textbf{skip}; S, \sigma \longrightarrow S, \sigma}$$

$$\frac{S_1, \sigma \longrightarrow S_1', \sigma'}{S_1 \parallel S_2, \sigma \longrightarrow S_1' \parallel S_2, \sigma'} \qquad \frac{S_2, \sigma \longrightarrow S_2', \sigma'}{S_1 \parallel S_2, \sigma \longrightarrow S_1 \parallel S_2', \sigma'} \qquad \frac{}{\textbf{skip} \parallel S, \sigma \longrightarrow S, \sigma} \qquad \frac{}{S \parallel \textbf{skip}, \sigma \longrightarrow S, \sigma}$$

$$\frac{\sigma \in [\![p]\!]}{\textbf{if } p \textbf{ then } S_1 \textbf{ else } S_2, \sigma \longrightarrow S_1, \sigma} \qquad \frac{\sigma \notin [\![p]\!]}{\textbf{if } p \textbf{ then } S_1 \textbf{ else } S_2, \sigma \longrightarrow S_2, \sigma}$$

$$\frac{\sigma \in [\![p]\!]}{\textbf{while } p \textbf{ do } S, \sigma \longrightarrow S; \textbf{while } p \textbf{ do } S, \sigma} \qquad \frac{\sigma \notin [\![p]\!]}{\textbf{while } p \textbf{ do } S, \sigma \textbf{skip}, \sigma}$$

2 Assertions and their semantics

We write assertions $\{p, R\}S\{G, q\}$, where p, q are predicates and R, G are relations (predicates over both primed and unprimed variables).

$\models_0 \{\sigma, R\}S\{G, q\}$ always

$\models_{n+1} \{\sigma, R\}S\{G, q\}$ iff

$$\begin{cases} \forall \sigma'.(\sigma, \sigma') \in [\![R]\!] & \implies \models_n \{\sigma', R\}S\{G, q\} \\ \forall \sigma'.S, \sigma \longrightarrow S', \sigma' & \implies (\sigma, \sigma') \in [\![G]\!]\,,\ \models_n \{\sigma', R\}S'\{G, q\} \\ S = \textbf{skip} & \implies \sigma \in [\![q]\!] \end{cases}$$

$\models \{p, R\}S\{G, q\}$ iff$\forall n. \forall \sigma \in [\![p]\!]\,.\ \models_n \{\sigma, R\}S\{G, q\}$

3 Rely/guarantee logic

Stability: p sta R iff $\forall \overline{x}, \overline{x'}.p(\overline{x}) \wedge R(\overline{x}, \overline{x'}) \Rightarrow p(\overline{x'})$.

$$\textsc{Assn}\ \frac{p \Rightarrow q[e/x] \quad (p \wedge x' = e \wedge \overline{y' = y}) \Rightarrow G \quad p, q \text{ sta } R}{\{p, R\}x := e\{G, q\}} \qquad \textsc{Skip}\ \frac{p \text{ sta } R}{\{p, R\}\textbf{skip}\{G, p\}} \qquad \textsc{Seq}\ \frac{\{p, R\}S_1\{G, q\} \quad \{q, R\}S_2\{G, r\}}{\{p, R\}S_1; S_2\{G, r\}}$$

PAR

$$\frac{(G_1 \vee G_2) \Rightarrow G \quad (R \vee G_1) \Rightarrow R_2 \quad (R \vee G_2) \Rightarrow R_1 \quad \{p, R_1\} S_1 \{G_1, q_1\} \quad \{p, R_2\} S_2 \{G_2, q_2\}}{\{p, R\} S_1 \parallel S_2 \{G, q_1 \wedge q_2\}}$$

IF

$$\frac{p \text{ sta } R \quad \{p \wedge r, R\} S_1 \{G, q\} \quad \{p \wedge \neg r, R\} S_2 \{G, q\}}{\{p, R\} \textbf{if } r \textbf{ then } S_1 \textbf{ else } S_2 \{G, q\}}$$

WHILE

$$\frac{\{p \wedge r, R\} S \{G, p\} \quad p, q \text{ sta } R \quad p \wedge \neg r \Rightarrow q}{\{p, R\} \textbf{while } r \textbf{ do } S \{G, q\}}$$

CONSEQ

$$\frac{\{p', R'\} S \{G', q'\} \quad p \Rightarrow p' \quad R \Rightarrow R' \quad q' \Rightarrow q \quad G' \Rightarrow G}{\{p, R\} S \{G, q\}}$$

4 Example proof

We will prove that $\{a = A \wedge b = B, \overline{x' = x}\} S_1 \parallel S_2 \{\text{true}, x_1 = x_2 = y_1 = y_2 = \gcd(A, B)\}$, where

$$\begin{array}{lll} S_1 = & x_1 := a; & \\ & x_2 := b; & \\ & \textbf{while } x_1 \neq x_2 \textbf{ do } S_1'; x_2 := b & \end{array} \qquad \begin{array}{lll} S_2 = & y_1 := b; & \\ & y_2 := a; & \\ & \textbf{while } y_1 \neq y_2 \textbf{ do } S_2'; y_2 := a & \end{array}$$

$$\begin{array}{lll} S_1' = & \textbf{if } x_1 > x_2 \textbf{ then} & \\ & \quad x_1 := x_1 - x_2; & \\ & \quad a := x_1 & \\ & \textbf{else skip} & \end{array} \qquad \begin{array}{lll} S_2' = & \textbf{if } y_1 > y_2 \textbf{ then} & \\ & \quad y_1 := y_1 - y_2; & \\ & \quad b := y_1 & \\ & \textbf{else skip} & \end{array}$$

We will perform a proof for S_1; the proof for S_2 is symmetric. First, we define

$$\begin{array}{rcl} p & = & \gcd(A, B) = \gcd(a, b) \\ \\ R & = & p \wedge \gcd(a, b) = \gcd(a', b') \\ & \wedge & (b \leq a \Rightarrow b' = b) \wedge a' = a \\ & \wedge & x_1' = x_1 \wedge x_2' = x_2 \\ \\ G & = & p \wedge \gcd(a, b) = \gcd(a', b') \\ & \wedge & (a \leq b \Rightarrow a' = a) \wedge b' = b \\ & \wedge & y_1' = y_1 \wedge y_2' = y_2 \\ \\ q & = & p \wedge \gcd(a, b) = \gcd(x_1, x_2) \\ I & = & p \wedge x_1 = a \wedge (x_1 > x_2 \Rightarrow x_2 = b) \end{array}$$

In the proof itself, we show only the R/G assertions that make up the derivation. The side-conditions on the rules, which are all first-order validities, are left implicit. Also, some uses of the CONSEQ rule are omitted.

First we handle the statements leading up to the loop:

$$\textsc{Seq}\ \frac{\textsc{Assn}\ \overline{\{p, R\}x_1 := a\{G, p \wedge x_1 = a\}} \qquad \textsc{Assn}\ \overline{\{p \wedge x_1 = a, R\}x_2 := b\{G, I\}}}{\{p, R\}x_1 := a; x_2 := b\{G, I\}}$$

Next, the loop itself:

$$\textsc{While}\ \frac{\textsc{Seq}\ \dfrac{\textsc{If}\ \dfrac{\textsc{Seq}\ \dfrac{\textsc{Assn}\ \overline{\{I \wedge x_1 > x_2, R\}\ x_1 := x_1 - x_2\ \{G, q \wedge x_2 = b \wedge a > b\}} \quad \textsc{Assn}\ \overline{\{q \wedge x_2 = b \wedge a > b\}\ a := x_1\ \{G, q \wedge x_1 = a\}}}{\{I \wedge x_1 > x_2, R\}x_1 := x_1 - x_2;\ a := x_1\{G, q \wedge x_1 = a\}} \quad \textsc{Skip}\ \overline{\{I \wedge x_2 > x_1, R\}\ \textbf{skip}\ \{G, q \wedge x_1 = a\}}}{\{I \wedge x_1 \neq x_2\}S_1'\{q \wedge x_1 = a\}} \quad \textsc{Assn}\ \overline{\{q \wedge x_1 = a, R\}x_2 := b\{G, I\}}}{\{I \wedge x_1 \neq x_2, R\}S_1; x_2 := b\{G, I\}}}{\{I, R\}\textbf{while}\ x_1 \neq x_2\ \textbf{do}\ S_1; x_2 := b\{G, x_1 = x_2 = \gcd(A, B)\}}$$

Putting the two together, we have

$$\{p, R\}S_1\{G, x_1 = x_2 = \gcd(A, B)\}$$

and symmetrically,

$$\{p, G\}S_2\{R, y_1 = y_2 = \gcd(A, B)\}$$

which, using PAR and CONSEQ, gives us

$$\{a = A \wedge b = B, \overline{x' = x}\}S_1 \parallel S_2\{\text{true}, x_1 = x_2 = y_1 = y_2 = \gcd(A, B)\}$$