Rely-guarantee

[Cliff Jones 1981]

Specifications are quintuples:

$$C : (P, R, G, Q)$$

precond. — rely — guarantee — postcondition

P, Q ~ assertions of a single state

R, G ~ assertions over two states (pre- & post-state)

P, R ~ assumptions

Q, G ~ conclusions.

Semantics

$C : (P, R, G, Q)$ iff $\forall s, n.\ P(s) \Rightarrow safe_n(C, s, R, G, Q)$

where:

$$safe_0(C, s, R, G, Q) \stackrel{def}{=} true$$

$$safe_{n+1}(C, s, R, G, Q) \stackrel{def}{=}$$

(I) $\quad (C = skip \Rightarrow Q(s))$

(II) $\quad \wedge\ (C, s \not\rightarrow abort)$ --- trivial.

(III) $\quad \wedge\ (\forall C', s'.\ C, s \rightarrow C', s' \Rightarrow G^*(s, s') \wedge safe_n(C', s', R, G, Q))$

(IV) $\quad \wedge\ (\forall s'.\ R(s, s') \Rightarrow safe_n(C, s', R, G, Q))$

Proof rules

$$\text{(BASIC)}\ \frac{\{P \wedge S_0 = s\}\ C\ \{Q \wedge G(S_0, s)\} \quad P \text{ stable under } R \quad Q \text{ stable under } R \quad C \text{ is an atomic command}}{C : (P, R, G, Q)}$$

$$\text{(SEQ)}\ \frac{C_1 : (P, R, G, Q) \quad C_2 : (Q, R, G, S)}{C_1 ; C_2 : (P, R, G, S)}$$

P stable under R iff $\forall s, s'.\ P(s) \wedge R(s, s') \Rightarrow P(s')$

$$\frac{C_1 : (P, R \vee G_2, G_1, Q_1) \qquad C_2 : (P, R \vee G_1, G_2, Q_2)}{C_1 \| C_2 : (P, R, G_1 \vee G_2, Q_1 \wedge Q_2)} \text{ (PAR)}$$

$R \vee G_2 \rightsquigarrow$ "The environment of thread C_1 is C_2 and the environment of the parallel composition (R)"

$G_1 \vee G_2 \rightsquigarrow$ "Each program step comes from C_1 or C_2; so satisfies G_1 or G_2 correspondingly"

$Q_1 \wedge Q_2 \rightsquigarrow$ "From the point C_1 terminates onwards Q_1 holds
—"— —"— C_2 —"— —"— Q_2 holds.
Therefore when $C_1 \| C_2$ —"— —"— $Q_1 \wedge Q_2$ —"—"

$$\frac{C : (P, R, G, Q) \qquad P' \Rightarrow P \quad Q \Rightarrow Q' \quad R' \Rightarrow R \quad G \Rightarrow G'}{C : (P', R', G', Q')} \text{ (CONSEQ)}$$

"You can strengthen the assumptions & weaken the conclusions."

Example

$\{true\}$

$\{true\}$ $\quad \| \quad$ $\{true\}$

$x := x+1$ $\quad \| \quad$ $a := x$

$\{true\}$ $\quad \| \quad$ $\{a \leq x\}$

$\| \quad b := x$

$\| \quad \{a \leq b\}$

$\{a \leq b\}$

In the PAR rule, take $R \overset{def}{=} false$, $G_1 \overset{def}{=} (x' \geq x \wedge a' = a \wedge b' = b)$ and $G_2 \overset{def}{=} (x' = x)$.

Stability checks for thread 2 : • $true \wedge G_1 \Rightarrow true$ ✓

• $a \leq x \wedge x' \geq x \wedge a' = a \wedge b' = b \Rightarrow a' \leq x'$ ✓

• $a \leq b \wedge x' \geq x \wedge a' = a \wedge b' = b \Rightarrow a' \leq b'$ ✓