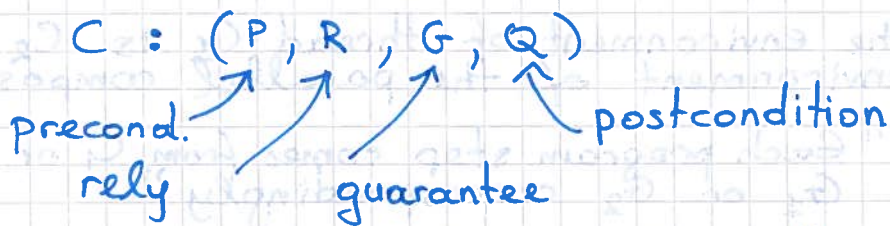


Rely-guarantee

[Cliff Jones 1981]

Specifications are quintuples :



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 $\forall s, n. P(s) \Rightarrow \text{safe}_n(C, s, R, G, Q)$

where :

$\text{safe}_0(C, s, R, G, Q) \stackrel{\text{def}}{=} \text{true}$

$\text{safe}_{n+1}(C, s, R, G, Q) \stackrel{\text{def}}{=} \dots$

- (I) $(C = \text{skip} \Rightarrow Q(s))$
- (II) $\wedge (C, s \not\rightarrow \text{abort}) \quad \text{--- trivial.}$
- (III) $\wedge (\forall C', s'. C, s \rightarrow C', s' \Rightarrow G^*(s, s') \wedge \text{safe}_n(C', s', R, G, Q))$
- (IV) $\wedge (\forall s'. R(s, s') \Rightarrow \text{safe}_n(C, s', R, G, Q))$

Proof rules

$\{ P \wedge S_0 = s \} C \{ Q \wedge G(S_0, s) \}$

P stable under R
 Q stable under R

C is an atomic command

(BASIC)

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

$C_1 : (P, R, G, Q)$

$C_2 : (Q, R, G, S)$

$C_1 ; C_2 : (P, R, G, S)$

(SEQ)

P stable under R
iff

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

$$C_1: (P, R \vee G_2, G_1, Q_1)$$

$$C_2: (P, R \vee G_1, G_2, Q_2)$$

(PAR)

$$C_1 \parallel C_2: (P, R, G_1 \vee G_2, Q_1 \wedge Q_2)$$

$R \vee G_2 \rightsquigarrow$ "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. Therefore when $C_1 \parallel C_2$ terminates $Q_1 \wedge Q_2$ holds."

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

$$P' \Rightarrow P$$

$$Q \Rightarrow Q'$$

$$R' \Rightarrow R$$

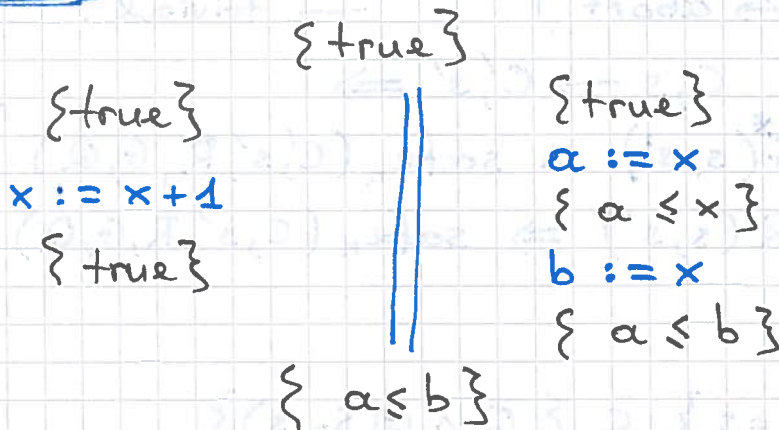
$$G \Rightarrow G'$$

(CONSEQ)

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

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

Example



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

Stability checks for thread 2: $\bullet \text{true} \wedge G_1 \Rightarrow \text{true} \checkmark$

- $\bullet a \leq x \wedge x' > x \wedge a' = a \wedge b' = b \Rightarrow a' \leq x' \checkmark$
- $\bullet a \leq b \wedge x' > x \wedge a' = a \wedge b' = b \Rightarrow a' \leq b' \checkmark$