COMP3610/6361
Principles of Programming Languages

Peter Höfner

Oct 17, 2023

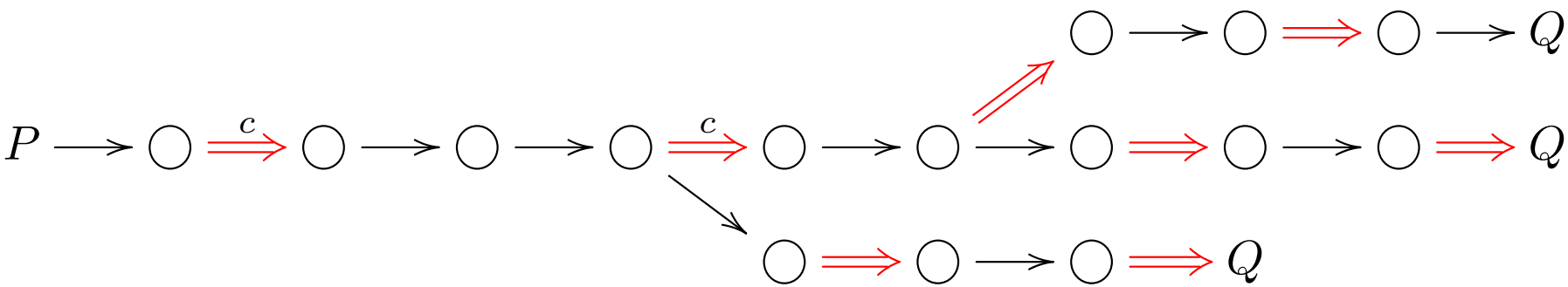
Section 24

Rely-Guarantee

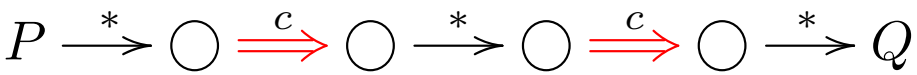
Motivation

- Owicki-Gries is *not* compositional
- generalise it to make it compositional

$$\{P\}\ c \parallel E\ \{Q\}$$



Motivation



$\xrightarrow{*}$: any state transition that can be done by *any* other thread, repeated zero or more times

Rely-Guarantee

$$\{P, R\}\ c\ \{G, Q\}$$

If

- the initial state satisfies P, and
- every state change by another thread satisfies the *rely condition* R, and

then c is executed and terminates,

then

- every final state satisfies Q, and
- every state change in c satisfies the *guarantee condition* G.

Rely-Guarantee – Parallel Rule

$$\frac{\{P_1, R \vee G_2\}\ c_1\ \{G_1, Q_1\} \qquad \{P_2, R \vee G_1\}\ c_2\ \{G_2, Q_2\}}{\{P_1 \wedge P_2, R\}\ c_1 \parallel c_2\ \{G_1 \vee G_2, Q_1 \wedge Q_2\}}$$

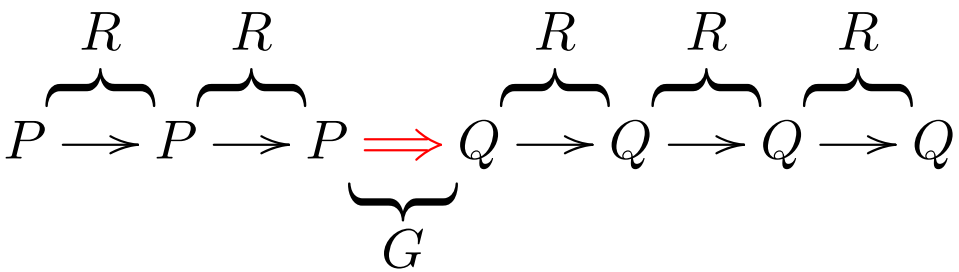
Rely-Guarantee – Consequence Rule

$$\frac{R \Rightarrow R' \qquad \{P, R'\}\ c\ \{G', Q\} \qquad G' \Rightarrow G}{\{P, R\}\ c\ \{G, Q\}}$$

Note: both rules can be packed in a single rule.

From Floyd-Hoare to Rely-Guarantee

$$\frac{\{P\}\ c\ \{Q\} \qquad ???}{\{P, R\}\ c\ \{G, Q\}}$$



Back to Stores

$$\frac{\{P\}\ c\ \{Q\} \quad P \text{ stable under } R \quad Q \text{ stable under } R \quad c \text{ is contained in } G}{\{P, R\}\ c\ \{G, Q\}}$$

P stable under R: $\forall s, s'.\ P(s) \wedge R(s, s') \Longrightarrow P(s')$

c contained in G: $\forall s, s'.\ P(s) \wedge (s, s') \in \mathcal{C}[\![c]\!] \Longrightarrow G(s, s')$

Making Assertions Stable

Assume

$$
\begin{aligned}
R &= (x \mapsto n \ \rightsquigarrow \ x \mapsto n-1) \\
&= \{(s, s') \mid \exists n.\ s(x) = n \wedge s'(x) = s + \{x \mapsto n-1\}\} \\
G &= (x \mapsto n \ \rightsquigarrow \ x \mapsto n+1) \\
&= \{(s, s') \mid \exists n.\ s(x) = n \wedge s'(x) = s + \{x \mapsto n+1\}\}
\end{aligned}
$$

$$\{x == 2, R\}\ x := x + 1\ \{G, x == 3\}$$

Making Assertions Stable

Assume

$$
\begin{aligned}
R &= (x \mapsto n \ \rightsquigarrow \ x \mapsto n-1) \\
&= \{(s, s') \mid \exists n.\ s(x) = n \wedge s'(x) = s + \{x \mapsto n-1\}\} \\
G &= (x \mapsto n \ \rightsquigarrow \ x \mapsto n+1) \\
&= \{(s, s') \mid \exists n.\ s(x) = n \wedge s'(x) = s + \{x \mapsto n+1\}\}
\end{aligned}
$$

$$\{x \leq 2, R\}\ x := x + 1\ \{G, x \leq 3\}$$

FindFirstPositive

$$i := 0 \; ; \; j := 1 \; ; \; x := |A| \; ; \; y := |A| \; ;$$
$$\{P_1 \wedge P_2\}$$

$$\begin{array}{l|l|l}
\{P_1, \mathbf{G_2}\} & & \{P_2, \mathbf{G_1}\} \\
\textbf{while} i < \min(x,y) \textbf{ do} & & \textbf{while} j < \min(x,y) \textbf{ do} \\
\quad \{P_1 \wedge i < x \wedge i < |A|\} & \| & \quad \{P_2 \wedge j < y \wedge j < |A|\} \\
\quad \ldots & & \quad \ldots \\
\quad \{P_1\} & & \quad \{P_2\} \\
\{\mathbf{G_1}, P_1 \wedge i \geq \min(x,y)\} & & \{\mathbf{G_2}, P_2 \wedge j \geq \min(x,y)\}
\end{array}$$

$$\{P_1 \wedge P_2 \wedge i \geq \min(x,y) \wedge j \geq \min(x,y)\}$$
$$r := \min(x,y)$$
$$\{r \leq |A| \wedge (\forall k.\, 0 \leq k < r \Rightarrow A[k] \leq 0) \wedge (r < |A| \Rightarrow A[r] > 0)\}$$

$$P_1 = x \leq |A| \wedge (\forall k.\, 0 \leq k < i \wedge k \text{ even} \Rightarrow A[k] \leq 0) \wedge i \text{ even} \wedge (x < |A| \Rightarrow A[x] > 0)$$
$$P_2 = y \leq |A| \wedge (\forall k.\, 0 \leq k < j \wedge k \text{ odd} \Rightarrow A[k] \leq 0) \wedge j \text{ odd} \wedge (y < |A| \Rightarrow A[y] > 0)$$
$$G_1 = \{(s, s') | s'(y) = s(y) \wedge s'(j) = s(j) \wedge s'(x) \leq s(x)\}$$
$$G_2 = \{(s, s') | s'(x) = s(x) \wedge s'(i) = s(i) \wedge s'(y) \leq s(y)\}$$

Rely-Guarantee Abstraction

Forgets

- which thread performs the action
- in what order the actions are performed
- how many times the action is performed

Usually, this is fine. . .

Verify This

$$\{x == 0\}$$

$$\{x == 0 \vee x == 1\} \qquad \{x == 0 \vee x == 1\}$$

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

$$\{x == 1 \vee x == 2\} \qquad \{x == 1 \vee x == 2\}$$

$$\{x == 2\}$$

$$G_1, G_2 = (x \mapsto n \ \rightsquigarrow \ x \mapsto n + 1)$$

Verify This

$$\{x == 0\}$$

$$\{\exists n \geq 0.\ x \mapsto n, \mathbf{G_2}\} \qquad \{\exists n \geq 0.\ x \mapsto n, \mathbf{G_1}\}$$

$$x := x + 1 \qquad \| \qquad x := x + 1$$

$$\{\mathbf{G_1}, \exists n \geq 1.\ x \mapsto n\} \qquad \{\mathbf{G_2}, \exists n \geq 1.\ x \mapsto n\}$$

$$\{\exists n \geq 1.\ x \mapsto n\}$$

$$G_1, G_2 = (x \mapsto n \ \rightsquigarrow \ x \mapsto n + 1)$$

From Floyd-Hoare to Rely-Guarantee (recap)

$$\frac{\{P\}\ c\ \{Q\} \qquad ???}{\{P, R\}\ c\ \{G, Q\}}$$

P stable under R if and only if $\{P\}\ R^*\ \{P\}$