COMP3151/COMP9154: Owicki-Gries Exercises

Johannes Åman Pohjola

June 20, 2022

1 Exercise 1

Consider the following program:

var $n := 0$			
p_1:	**var** $x := n$;	q_1:	**var** $y := n$;
p_2:	$n := x + 1$;	q_2:	$n := y + 1$;

1. Transcribe the program above into transition diagrams for P and Q.
2. Find an inductive assertion network to prove the Hoare triple $\{n = 0\}\ P||Q\ \{n > 0\}$.
3. Find another assertion network to prove $\{n = 0\}\ P||Q\ \{n \leq 2\}$. This requires location annotations in the assertion network.

2 Exercise 2

Now do this program:

var $n := 0$			
p_0:	**do** 10 times:	q_0:	**do** 10 times:
p_1:	**var** $x := n$;	q_1:	**var** $y := n$;
p_2:	$x := x + 1$;	q_2:	$y := y + 1$;
p_3:	$n := x$;	q_3:	$n := y$;
p_4:	**od**	q_5:	**od**

1. Transcribe the program above into transition diagrams for P and Q.
2. Find an inductive assertion network to prove the Hoare triple $\{n = 0\}\ P||Q\ \{n > 1\}$.
3. Find another assertion network to prove $\{n = 0\}\ P||Q\ \{n \leq 20\}$.

Hint: you'll almost certainly want to introduce an explicit loop counter.

3 Exercise 3

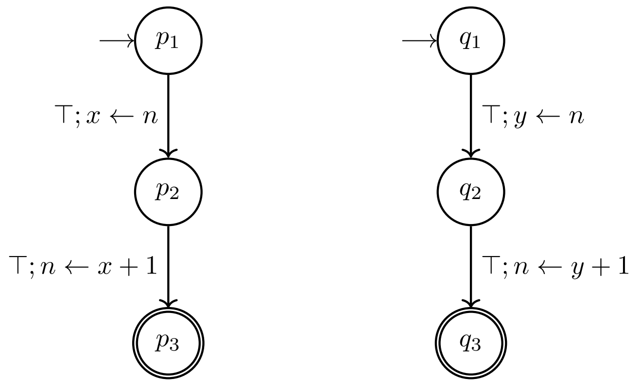
Now do this program:

var *turn* $\leftarrow 1$			
forever do		**forever do**	
p_1	*non-critical section*	q_1	*non-critical section*
p_2	**await** $turn = 1$;	q_2	**await** $turn = 2$;
p_3	**critical section**	q_3	**critical section**
p_4	$turn \leftarrow 2$	q_4	$turn \leftarrow 1$

1. Transcribe the program above into transition diagrams for P and Q.
2. Find an inductive assertion network that allows you to prove mutual exclusion.

4 Exercise 1 solution

1. Here are the transition diagrams:



   Note that for the purposes of the transition diagram, we introduced the extra locations p_3 and q_3, which is the state after both instructions of the respective process have been executed.

2. Here are the assertion networks:

$$\begin{array}{ll} \mathcal{P}(p_1) = n \geq 0 & \mathcal{Q}(q_1) = n \geq 0 \\ \mathcal{P}(p_2) = x \geq 0 & \mathcal{Q}(q_2) = y \geq 0 \\ \mathcal{P}(p_3) = n > 0 & \mathcal{Q}(q_3) = n > 0 \end{array}$$

   Here, we need to resist the temptation of annotating the entry locations with the precondition $n = 0$. This assertion would not be robust to interference, hence we weaken $=$ to $\geq$. n can change beneath our feet, but at least it can't shrink beneath our feet.

   By the Owicki-Gries method, we have the following tasks in front of us to prove the Hoare triple $\{n = 0\}\ P||Q\ \{n > 0\}$.

   (a) Prove $\mathcal{P}$ inductive.

   The following proof obligations arise. They are the instantiations of the general schema $\mathcal{P}(\ell_i) \wedge g \Rightarrow \mathcal{P}(\ell_j) \circ f$, for each of the two transitions in the diagram.

$$n \geq 0 \wedge \top \Rightarrow n \geq 0 \quad (1) \qquad\qquad x \geq 0 \wedge \top \Rightarrow x + 1 > 0 \quad (2)$$

   None of them are very exciting. (1) is vacuously true, and (2) follows by elementary arithmetic. This is a good sign—usually, discharging the proof obligations is the easy part of the proof. The tricky part is finding the annotations that make it easy.

   (b) Prove $\mathcal{Q}$ inductive.

   The following proof obligations arise.

$$n \geq 0 \wedge \top \Rightarrow n \geq 0 \quad (1) \qquad\qquad y \geq 0 \wedge \top \Rightarrow y + 1 > 0 \quad (2)$$

   These are identical to the proof obligations for $\mathcal{P}$, up to variable renaming.

   (c) Prove interference freedom for $\mathcal{P}$.

   The following proof obligations arise. They are all instances of the general schema

$$\mathcal{P}(p) \wedge \mathcal{Q}(q) \wedge g \Rightarrow \mathcal{P}(p) \circ f$$

$$n \geq 0 \land n \geq 0 \Rightarrow n \geq 0 \quad (1) \qquad n \geq 0 \land y \geq 0 \Rightarrow y+1 \geq 0 \quad (2)$$

$$x \geq 0 \land n \geq 0 \Rightarrow x \geq 0 \quad (3) \qquad x \geq 0 \land y \geq 0 \Rightarrow x \geq 0 \quad (4)$$

$$n > 0 \land n \geq 0 \Rightarrow n > 0 \quad (5) \qquad n > 0 \land y \geq 0 \Rightarrow y+1 > 0 \quad (6)$$

Proof obligations 1–2 is for interference with the annotation at location p_1, obligations 3–4 for location p_2, and obligations $5--6$ for location p_3. Odd-numbered obligations are for the $q_1 \to q_2$ transition, and even-numbered obligations for the $q_2 \to q_3$ transition. The proof obligations are all trivial to discharge.

(d) Show that the precondition implies the entry annotations, and that the exit annotations imply the postcondition. The (trivial) proof obligations are as follows:

$$n = 0 \Rightarrow n \geq 0 \land n \geq 0 \qquad n > 0 \land n > 0 \Rightarrow n > 0$$

That was a lot of work for a trivial program, wasn't it?

True. It would have been much easier to model-check this program with Spin, or to construct all possible interleavings manually. The true power of Owicki-Gries becomes apparent only in larger examples: when the number of interleavings is intractably large, or even infinite, the number of proof obligations is proportional to the number of locations and transitions, not the number of states and behaviours.

3. Now let's prove $\{n = 0\}\ P||Q\ \{n \leq 2\}$. This deceptively simple example is often used to illustrate the limitations of Owicki-Gries reasoning without location annotations. Proving it requires location annotations in the assertions. Here's the (much messier) assertion network:

$$\begin{aligned}
\mathcal{P}(p_1) &= (Q@q_3 \land n = 1) \lor (\neg Q@q_3 \land n = 0)\\
\mathcal{P}(p_2) &= 0 \leq x \leq 1 \land (x = 1 \Rightarrow Q@q_3)\\
\mathcal{P}(p_3) &= n \leq 2\\
\\
\mathcal{Q}(q_1) &= (P@p_3 \land n = 1) \lor (\neg P@p_3 \land n = 0)\\
\mathcal{Q}(q_2) &= 0 \leq y \leq 1 \land (y = 1 \Rightarrow P@P_3)\\
\mathcal{Q}(q_3) &= n \leq 2
\end{aligned}$$

Without location annotations, we'd be stuck trying to prove that the p_1 annotation cannot be interferred with by the $q_2 \to q_3$ transition. You may want to try for yourself to convince yourself of this.

The non-interference proof obligation we get for that transition like this:

$$(\bot \land n = 1) \lor (\neg\bot \land n = 0) \land 0 \leq y \leq 1 \land (y = 1 \Rightarrow \bot) \Rightarrow (\top \land y+1 = 1) \lor (\neg\top \land y+1 = 0)$$

...which simplifies to

$$n = 0 \land 0 \leq y \leq 1 \land y \neq 1 \Rightarrow y + 1 = 1$$

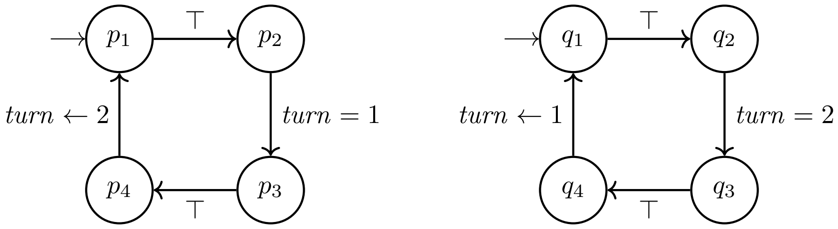
...which is equivalent to

$$n = 0 \land y = 0 \Rightarrow y + 1 = 1$$

which is trivial. You may want to check some other proof obligations for yourself.

5 Exercise 3 solution

1. Here are the transition diagrams:



2. Here's the assertion network:

$$\begin{array}{ll}
\mathcal{P}(p_1) = \top & \mathcal{Q}(q_1) = \top \\
\mathcal{P}(p_2) = \top & \mathcal{Q}(q_2) = \top \\
\mathcal{P}(p_3) = (turn = 1) & \mathcal{Q}(q_3) = (turn = 2) \\
\mathcal{P}(p_4) = (turn = 1) & \mathcal{Q}(q_4) = (turn = 2)
\end{array}$$

Inductivity is straightforward. Mutual exclusion follows because

$$\mathcal{P}(p_3) \wedge \mathcal{Q}(q_3) \quad \Leftrightarrow \quad (turn = 1) \wedge (turn = 2) \quad \Leftrightarrow \quad \bot$$

No meaningful interference is possible here. Q cannot interfere with the P's assertion $turn = 1$ because Q never assigns any other value to $turn$ other than 1. Same thing, mutatis mutandis, holds for P's interference with Q's only assertion $turn = 2$.