Model Checking, SS2011: Exercise Sheet 7

May 25, 2011

Exercise 7.1. Let the formulas $\rho_1,\ \ldots,\ \rho_3,\ \varphi$ be given. Prove or refute the following proposition.

$$\exists I\ .\ \exists J\ .\ (\mathit{post}(\rho_1,\ \varphi) \models I) \wedge (\mathit{post}(\rho_2,\ I) \models J) \wedge (\mathit{post}(\rho_3,\ J) \models \bot)$$

$$\equiv$$

$$\exists I\ .\ \mathit{post}(\rho_1, \varphi) \models I \wedge \mathit{post}(\rho_3, \mathit{post}(\rho_2, I)) \models \bot$$

Exercise 7.2. Let the predicates $\rho_1(v,\ v'),\ \rho_2(v,\ v'),\ I(v)$ be given. Prove the following proposition.

$$\exists I\ .\ (\mathit{post}(\rho_1(v,\ v'),\ \varphi(v)) \models I(v)) \wedge (\mathit{post}(\rho_2(v,\ v'),\ I(v)) \models \bot)$$

$$\equiv$$

$$\exists I\ .\ (\forall v^*\ .\ \forall v''\ .\ \rho_1(v'',\ v^*) \wedge \varphi(v'') \rightarrow I(v^*)) \wedge (\forall v\ .\ \forall v^*\ .\ \rho_2(v^*,\ v) \wedge I(v^*) \rightarrow \bot)$$

Exercise 7.3. An interpolant I of formulas A and B is a formula such that:

1. $A \wedge B \models \bot$,
2. $A \models I$,
3. $I \wedge B \models \bot$, and
4. $\mathit{Symb}(I) \subseteq \mathit{Symb}(A) \cap \mathit{Symb}(B)$,

where $\mathit{Symb}(\varphi) := \{\text{variables occurring in } \varphi\}$. Prove the following proposition.

$$I(v^*) \text{ is an interpolant of } \rho_1(v'',\ v^*) \wedge \varphi(v'') \text{ and } \rho_2(v^*,\ v)$$

$$\text{if and only if}$$

$$(\mathit{post}(\rho_1(v,\ v'),\ \varphi(v)) \models I(v)) \wedge (\mathit{post}(\rho_2(v,\ v'),\ I(v)) \models \bot)$$

Exercise 7.4. Consider program P from exercise 2.6. Consider the following proposition.

$$(post(\rho_1,\ pc = l_1) \models I) \wedge (post(\rho_2,\ I) \models J) \wedge (post(\rho_3,\ J) \models \bot) \qquad (1)$$

Use the proposition you proved in exercise 7.3 to give formulas I and J that satisfy (1). Give I first, then give J.

Exercise 7.5. Consider program P from exercise 2.6. and the set $Preds := pc = l_i$. Execute PredAbstrRefine (see blackboard notes from class 7) on P, replace *Preds* for the empty set in line 1. Hints:

1. Instead of executing the call to PredAbst in line 3, draw the reachability tree corresponding to the call.
2. Use the proposition you proved in exercise 7.3.

Exercise 7.6. Let $\rho := (\rho_1(v_0,\ v_1) \circ \ldots \circ \rho_n(v_{n-1},\ v_n))$. Prove the following proposition.

$$\begin{array}{ll} \exists \phi_0(v_0)\ . & (\varphi_{init}(v_0) \models \phi_0(v_0))\ \wedge \\ & (post\,(\rho(v_0,\ v_n),\ \phi_0(v_0)) \wedge \varphi_{error}(v_n) \models \bot) \end{array}$$

$$\equiv$$

$$\begin{array}{ll} \exists \phi_0(v_0)\ . & (\forall v_0\ .\ \varphi_{init}(v_0) \rightarrow \phi_0(v_0)) \wedge \\ & (\forall v_n\ .\ \forall v_0\ .\ (\rho(v_0,\ v_n) \wedge \varphi_{error}(v_n) \wedge \phi_0(v_0) \rightarrow \bot)) \end{array}$$

Exercise 7.7. Let $Interp(A,\ B)$ be the interpolant of A and B. Let $\rho := (\rho_1(v_0,\ v_1) \circ \ldots \circ \rho_n(v_{n-1},\ v_n))$. Let

$$\phi_0 := Interp\,(\varphi_{init}(v_0),\ \rho \wedge \varphi_{error}(v_n)) \qquad (2)$$

Prove that ϕ_0 satisfies the following proposition.

$$(\varphi_{init}(v_0) \models \phi_0(v_0))\ \wedge\ (post\,(\rho(v_0,\ v_n),\ \phi_0(v_0)) \wedge \varphi_{error}(v_n) \models \bot)$$

Exercise 7.8. Let $\rho := (\rho_{i+1}(v_i,\ v_{i+1}) \circ \ldots \circ \rho_n(v_{n-1},\ v_n))$. Prove the following proposition.

$$\begin{array}{ll} \exists \phi_i(v_i)\ . & (post(\rho_i(v_{i-1},\ v_i),\ \phi_{i-1}(v_{i-1})) \models \phi_i(v_i))\ \wedge \\ & (post\,(\rho(v_i,\ v_n),\ \phi_i(v_i)) \wedge \varphi_{error}(v_n) \models \bot) \end{array}$$

$$\equiv$$

$$\begin{array}{ll} \exists \phi_i(v_i)\ . & (\forall v_i\ .\ \forall v_{i-1}\ .\ \rho_i(v_{i-1},\ v_i) \wedge \phi_{i-1}(v_{i-1}) \rightarrow \phi_i(v_i)) \wedge \\ & (\forall v_n\ .\ \forall v_i\ .\ (\rho(v_i,\ v_n) \wedge \varphi_{error}(v_n) \wedge \phi_i(v_i) \rightarrow \bot)) \end{array}$$

Exercise 7.9. Let $Interp(A,\ B)$ be the interpolant of A and B. Let $\rho := (\rho_{i+1}(v_i,\ v_{i+1}) \circ \ldots \circ \rho_n(v_{n-1},\ v_n))$. Let

$$\phi_i := Interp\,(\rho_i(v_{i-1},\ v_i) \wedge \phi_{i-1}(v_{i-1}),\ \rho(v_i,\ v_n) \wedge \varphi_{error}(v_n)) \tag{3}$$

Prove that ϕ_i satisfies the following proposition.

$$(post(\rho_i(v_{i-1},\ v_i),\ \phi_{i-1}(v_{i-1})) \models \phi_i(v_i)) \wedge (post\,(\rho(v_i,\ v_n),\ \phi_i(v_i)) \wedge \varphi_{error}(v_n) \models \bot)$$

Exercise 7.10. Consider the following propositions.

$$Symb(I) \subseteq Symb(A) \cap Symb(B \wedge C) \tag{4}$$

$$Symb(J) \subseteq Symb(A \wedge B) \cap Symb(C) \tag{5}$$

$$Symb(I) \subseteq Symb(A) \tag{6}$$

$$Symb(J) \subseteq Symb(I \wedge B) \cap Symb(C) \tag{7}$$

Refute that propositions (4) and (5) imply (6) and (7).

Exercise 7.11. Consider propositions (4), (5), (6), (7) from exercise 7.10. Consider the following proposition.

$$I \wedge B \models J \tag{8}$$

Prove that propositions (4), (5), and (8) imply (6) and (7).

Exercise 7.12. Consider the following code fragment

```
x = 1;
assert(x = 1);
```

Consider the program P corresponding to the fragment, where

1. $\varphi_{init} = (pc = 1)$
2. $\varphi_{error} = (pc = 4)$
3. $\rho_1 = (pc = 1 \wedge pc' = 2 \wedge x' = 1)$
4. $\rho_2 = (pc = 2 \wedge pc' = 3 \wedge x = 1 \wedge x' = x)$
5. $\rho_3 = (pc = 2 \wedge pc' = 4 \wedge x \neq 1 \wedge x' = x)$

Do the following.

1. Draw the abstract reachability tree of P using $Preds = \bigcup_{i \in 1..4}\{pc = i\}$.
2. Show that the possible counterexample path is spurious.
3. Use definitions (2) and (3) to find new predicates $\phi_0,\ \phi_1,\ \phi_2$ that refine the set $Preds$.
4. Draw the abstract reachability tree of P using $Preds' = Preds \cup \{\phi_0,\ \phi_1,\ \phi_2\}$.