Intro to Software Verification - Homework 3

Yosef Goren & Andrew

December 18, 2022

Question 1

A. 3

B. 1

C. 3

D. 2

E. 1

Question 2

1. True. Let $\pi = s_0 \to s_5 \to s_5$.
   - $M, \pi^2 \models b$
   - $M, \pi^1 \models Xb$
   - $M, \pi^0 \models XXb$
   - $M \models E[XXb]$

2. True. Let π be an arbitrary path in M.
   π must be in the form $s_0 \to v \to *$ where $v \in \{s_1, s_4, s_5\}$.
   We want to prove $M, \pi \models (EXa)U(EXc)$.

   $$((s_0, s_1) \in M) \land (s_1 \models a) \Rightarrow s_0 \models EXa \Rightarrow \pi^0 \models EXa$$

   Additionally:

   $$\forall u \in \{s_1, s_4, s_5\}, \exists u' : (u, u') \in M \land u' \models c$$

   $$\Rightarrow \forall u \in \{s_1, s_4, s_5\}, u \models EXc$$
   $$\Rightarrow v \models EXc \Rightarrow \pi^1 \models EXc$$
   $$\Rightarrow M, \pi \models (EXa)U(EXc)$$

3. True. Let $\pi = s_0 \to s_4 \to s_7$.
    - $M, \pi^2 \models Gc$
    - $M, \pi^1 \models a$
    - $M, \pi^1 \models aU(Gc)$
    - $M, \pi^0 \models b$
    - $M, \pi^0 \models bU(U(Gc))$
    - $M \models E[bU(U(Gc))]$
4. True. Let $\pi = s_0 \to *$.

    - $s_0 \models b$
    - $s_0 \models cUb$
    - $s_0 \models a(cUb)$
    - $\pi \models a(cUb)$

    $\Rightarrow M \models A[a(cUb)]$

Question 3

Part A.

Let: $H := \{f_1 \times f_2 \times, ..., \times f_m\}$.
In other words, H is the set of all possible combinations of the m functions in F.
For any $h \in H, i \in [m]$, let $h[i]$ be an item within h which was chosen from f_i - one must exists since h is a combination of f_i.
More formally, let $h[i] := argmin_{i|s_i \in h \cap f_i}$ (the minimal item in h from f_i).

Proof.
The following logical formulas are equivalent (and the transition from one to the other is trivial):

1. $\forall i \in [m], f_i \cap inf(\pi) \neq \emptyset$
2. $\forall i \in [m], \exists s_i, s_i \in f_i \wedge s_i \in inf(\pi)$
3. $\forall i \in [m], \exists s_i \in f_i, s_i \in inf(\pi)$
4. $\exists s_1, s_2, ..., s_m, \forall i \in [m], s_i \in f_i \wedge s_i \in inf(\pi)$
5. $\exists h \in H, \forall i \in [m], h[i] \in f_i \wedge h[i] \in inf(\pi)$
6. $\exists h \in H, (\forall i \in [m], h[i] \in f_i) \wedge (\forall i \in [m], h[i] \in inf(\pi))$
7. $\exists h \in H, (h \subseteq inf(\pi)) \wedge (\forall i \in [m], h[i] \in inf(\pi))$
8. $\exists h \in H, (h \subseteq inf(\pi)) \wedge (true)$
9. $\exists h \in H, h \subseteq inf(\pi)$

Part B.

For any $i \in [m], \bar{f}_i := S \setminus f_i$.
Let $h := \bigcap_{i=1}^{m} \bar{f}_i, H := \{h\}$.

Proof.
The following series of formulas are equivalent:

1. $\forall i \in [m], f_i \cap inf(\pi) = \emptyset$
2. $\forall i \in [m], \bar{f}_i \cap inf(\pi) = inf(\pi)$
3. $\forall i \in [m], inf(\pi) \subseteq \bar{f}_i$
4. $\forall i \in [m], \forall s \in inf(\pi), s \in \bar{f}_i$
5. $\forall s \in inf(\pi), \forall i \in [m], s \in \bar{f}_i$
6. $\forall s \in inf(\pi), s \in \bigcap_{i=1}^{m} \bar{f}_i$
7. $inf(\pi) \subseteq bigcap_{i=1}^{m} \bar{f}_i$
8. $inf(\pi) \subseteq h$
9. $\forall h' \in H, inf(\pi) \subseteq h'$

Question 4