

# 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  $\pi = s_0 \rightarrow s_5 \rightarrow s_5$ .

- $M, \pi^2 \models b$
- $M, \pi^1 \models Xb$
- $M, \pi^0 \models XXb$
- $M \models E[XXb]$

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

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

Additionally:

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

$$\Rightarrow \forall u \in \{s_1, s_4, s_5\}, u \models EXc$$

$$\Rightarrow v \models EXc \Rightarrow \pi^1 \models EXc$$

$$\Rightarrow M, \pi \models (EXa)U(EXc)$$

3. True. Let  $\pi = s_0 \rightarrow s_4 \rightarrow s_7$ .

- $M, \pi^2 \models Gc$
- $M, \pi^1 \models a$
- $M, \pi^1 \models aU(Gc)$
- $M, \pi^0 \models b$
- $M, \pi^0 \models bU(U(Gc))$
- $M \models E[bU(U(Gc))]$

4. True. Let  $\pi = s_0 \rightarrow *$ .

- $s_0 \models b$
  - $s_0 \models cUb$
  - $s_0 \models a(cUb)$
  - $\pi \models a(cUb)$
- $\Rightarrow M \models A[a(cUb)]$

### Question 3

#### Part A.

Let:  $H := \{f_1 \times f_2 \times, \dots, \times f_m\}$ .

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 exist since  $h$  is a combination of  $f_i$ .

More formally, let  $h[i] := \text{argmin}_{s_i \in h \cap f_i}$  (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.  $\forall i \in [m], f_i \cap \text{inf}(\pi) \neq \emptyset$
2.  $\forall i \in [m], \exists s_i, s_i \in f_i \wedge s_i \in \text{inf}(\pi)$
3.  $\forall i \in [m], \exists s_i \in f_i, s_i \in \text{inf}(\pi)$
4.  $\exists s_1, s_2, \dots, s_m, \forall i \in [m], s_i \in f_i \wedge s_i \in \text{inf}(\pi)$
5.  $\exists h \in H, \forall i \in [m], h[i] \in f_i \wedge h[i] \in \text{inf}(\pi)$
6.  $\exists h \in H, (\forall i \in [m], h[i] \in f_i) \wedge (\forall i \in [m], h[i] \in \text{inf}(\pi))$
7.  $\exists h \in H, (h \subseteq \text{inf}(\pi)) \wedge (\forall i \in [m], h[i] \in \text{inf}(\pi))$
8.  $\exists h \in H, (h \subseteq \text{inf}(\pi)) \wedge (\text{true})$
9.  $\exists h \in H, h \subseteq \text{inf}(\pi)$

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

## Question 4

### Part A.

Let  $\phi_{B \rightarrow W} := b \wedge E(bU(EGw))$ ,  
 Let  $\phi_{W \rightarrow B} := w \wedge E(wU(EGb))$ .

The meaning of  $\phi_{B \rightarrow W}$  is that there exists a path that starts with at-least one  $b$ , and then continues being  $b$  right untill the point where there exists a path satisfying  $Gw$ , meaning it is  $w$  exclusively from forever. In other words - by concatenating the 'inner' path that satisfies  $Gw$  with the suffix of the path that satisfies  $\phi_{B \rightarrow W}$ , we get a path that has exactly one transision from  $b$  to  $w$  and no transisions from  $w$  to  $b$ .

Symmetrically,  $\phi_{W \rightarrow B}$  means there exists a path from the initial node that has exactly one transision from  $w$  to  $b$  and no other transisions.

So  $\phi_{W \rightarrow B} \vee \phi_{B \rightarrow W}$  is a satisfactory and required for the existance of a legal path.

Let  $\phi := \phi_{W \rightarrow B} \wedge \phi_{B \rightarrow W}$ .

So  $M, s \models \phi$  means that there exists a legal path from  $s$ .

To describe  $\phi$  explicitly:

$$\phi = (b \wedge E(bU(EGw))) \vee (w \wedge E(wU(EGb)))$$

## Part B.

Define an algorithm for verifying  $\phi$  as follows:

1. Create  $M' := (S, R', L)$ , where  $R' := \{(s, s') \in R \mid l(s) = l(s')\}$  meaning nodes are now connected if they have the same color.
2. Find the maximally connected componenets of  $M'$  - each componenet has uniform color.
3. Mark with  $C$  all components that have a circle, and recursively mark it with  $C$  all nodes that have a path to a component with  $C$ .
4. Now each component that has an inifinite path of just one color is marked with  $C$ . Moreover, each node that has an inifinite path of uniform color is within a component that is marked with  $C$ .
5. Mark all black components that have  $C$  with  $E(wU(EGb))$  - note how all nodes within such a component actually satisfy this formula in the origina kripke structure.
6. Symmetrically, mark all white components that have  $C$  with  $E(bU(EGw))$ .
7. Look at all edges (in the original structure) that go from componenets of different colors. If there exists such edge between a white component and a  $E(wU(EGb))$  component, mark the white component with  $w \wedge E(wU(EGb))$ , moreover, mark all white components leading to said white component also with  $w \wedge E(wU(EGb))$ .  
Note how each node within these white components indeed satisfy  $w \wedge E(wU(EGb))$  in the original structure.  
Symmetrically, if there exists an edge between a black component and a  $E(bU(EGw))$  component, mark the black component with  $b \wedge E(bU(EGw))$  and all black components leading to said black component with  $b \wedge E(bU(EGw))$  also.
8. Now any node is legal iff it is marked with either  $w \wedge E(wU(EGb))$  or  $b \wedge E(bU(EGw))$ , since if it was a legal node it either had to go from white to black or black to white - which in either case would mean it is marked with either  $w \wedge E(wU(EGb))$  or  $b \wedge E(bU(EGw))$  respectively.