Introduction to Software Verification 236342, Homework 3

Yosef Goren 211515606, Andrew Elashkin 336127675

January 3, 2023

Question 1

A. 3

B. 1

C. 3

D. 2

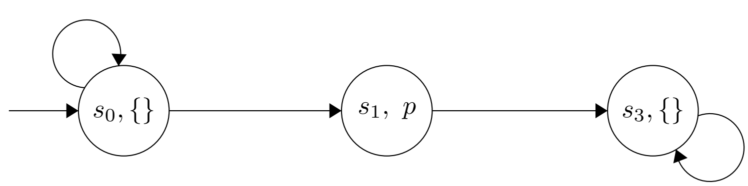
E. 4

F. 1

G. 4

H. 3

I. 2. $\phi_1 \not\Rightarrow \phi_2$: A counterexample of the kripke structure M and path π, that satisfies ϕ_1, but not ϕ_2 is below. Assume $\pi = s_0, s_0, s_0, ...$, then the pair $M, \pi \models \phi_1$, but $M, \pi \not\models \phi_2$.



$\phi_2 \Rightarrow \phi_1$:

$$M, \pi \models EGFp \Rightarrow$$

$$\forall i \geq 0, (M, \pi_i) \models Fp \Rightarrow$$

Since we know that the path pi_i exists, we can say that for every node s_i in the path pi_i there is such a path:

$$\forall i \geq 0, (M, s_i) \models EFp \Rightarrow$$

$$M, \pi \models EGEFp$$

J. 1.

$\phi_1 \Rightarrow \phi_2$:

$$M, s \models AFAXp = A[trueUAXp] \Rightarrow$$

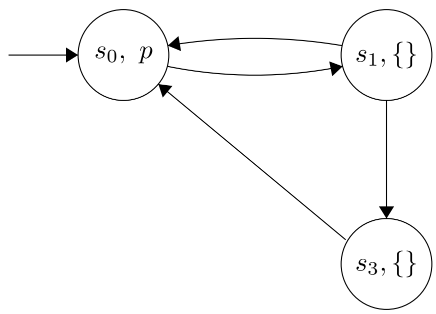
For every path π starting at s:

$$\pi \models FAXp \Rightarrow \exists i \geq 0, \pi_i \models AXp \Rightarrow$$

$$\pi_i \models AFXp \Rightarrow \pi \models AFXp \Rightarrow$$

$$\pi \models XAFp \Rightarrow M, s \models AXAFp$$

$\phi_2 \not\Rightarrow \phi_1$: A counterexample of the kripke structure M and path π, that satisfies ϕ_2, but not ϕ_1 is below. Assume $\pi = s_0, s_1, s_0, s_1, ...$, then the pair $M, \pi \models \phi_2$, but $M, \pi \not\models \phi_1$.



Question 2

1. Correct.
2. Wrong.
3. Wrong.
4. Wrong.
5. 4
6. Wrong.

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

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

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

4. True. Let $\pi = s_0 \to *$.
   - $s_0 \models b$
   - $s_0 \models cUb$
   - $s_0 \models aU(cUb)$
   - $\pi \models aU(cUb)$

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

5. False. Let $\pi = s_0 \to s_1 \to s_2 \to s_3 \to s_3 \to ...$
   On this path $s_2 \models c$, meaning that $(Xa \to GXb)$ also needs to be satisfied for the formula to hold. $s_2 \models Xa$, but $s_3 \not\models GXb$ and so the formula does not hold for any path.

6. False. $\phi_1 = FG(a \vee c)$ has to hold for any path from s_0. Let $\pi = s_0 \to s_5 \to s_5 \to ...$
   $FG(a \vee c)$ does not hold for this path and so $M \not\models \phi$.

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

Part A.

Let $\phi_{B \to W} := b \wedge E(bU(EGw))$,
Let $\phi_{W \to B} := w \wedge E(wU(EGb))$.
The meaning of $\phi_{B \to W}$ 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 $\phi_{B \to W}$, we get a path that has exactly one transision from b to w and no transisions from w to b.
Symmetrically, $\phi_{W \to B}$ means there exists a path from the initial node that has exactly one transision from w to b and no other transisions.
So $\phi_{W \to B} \vee \phi_{B \to W}$ is a satisfactory and required for the existance of a legal path.
Let $\phi := \phi_{W \to B} \wedge \phi_{B \to W}$.
So $M, s \models \phi$ means that there exists a legal path from s.
To describe ϕ explicitly:

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

Part B.

Define an algorithm for verifying ϕ 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 maximaly 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.