Introduction to Software Verification - HW No. 3

Winter 2022-2023

TA in charge of the HW: Roy Deutch

Pay attention: an answer without explanation will not be checked.

Question 1

For every pair φ_1, φ_2 write which of the next statements is correct:

1. $\varphi_1 \Rightarrow \varphi_2$ and $\varphi_1 \Leftarrow \varphi_2$
2. $\varphi_1 \nRightarrow \varphi_2$ and $\varphi_1 \Leftarrow \varphi_2$
3. $\varphi_1 \Rightarrow \varphi_2$ and $\varphi_1 \nLeftarrow \varphi_2$
4. $\varphi_1 \nRightarrow \varphi_2$ and $\varphi_1 \nLeftarrow \varphi_2$

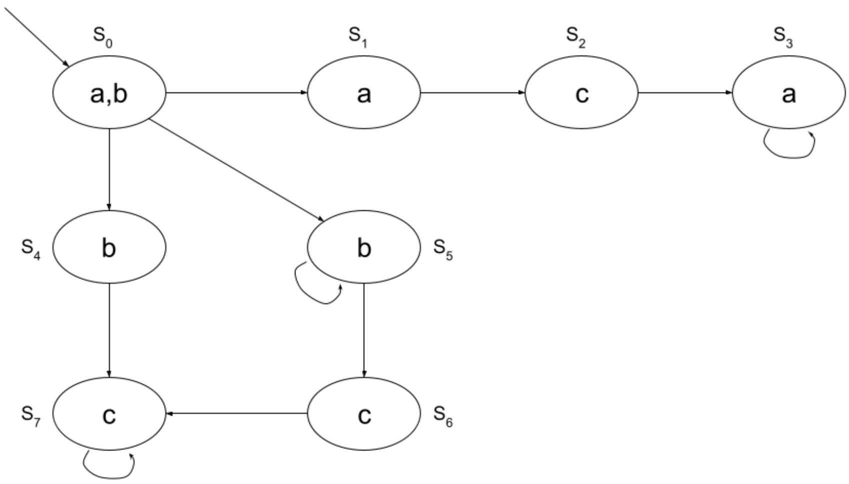
In sections A-H you don't need to explain your answer.
In sections I-J you need to prove your answer (prove in case the implication is correct, and bring a counterexample in case the implication is not correct)

A. $\varphi_1 = EG(p \wedge q); \varphi_2 = EGp \wedge EGq$
B. $\varphi_1 = AG(p \wedge q); \varphi_2 = AGp \wedge AGq$
C. $\varphi_1 = AG(Fp \wedge q); \varphi_2 = A(Fp \wedge Gq)$
D. $\varphi_1 = E(pU(qUr)); \varphi_2 = E(pUq) \wedge E(pUr)$
E. $\varphi_1 = AG((\neg p) \rightarrow AX(\neg p)); \varphi_2 = EG(\neg p)$
F. $\varphi_1 = AGAGp; \varphi_2 = AGp$
G. $\varphi_1 = AFp \wedge AXFq; \varphi_2 = AFq \wedge AXFp$
H. $\varphi_1 = AFAGp; \varphi_2 = AFGp$
I. $\varphi_1 = EGEFp; \varphi_2 = EGFp$
J. $\varphi_1 = AFAXp; \varphi_2 = AXAFp$

Question 2

Given the next structure:

$AP = \{a, b, c\}$



In each of the next section answer if $M \vDash \varphi$.
Explain your answer.

1. $\varphi = EXXb$
2. $\varphi = A[(EXa)U(EXc)]$
3. $\varphi = E[bU(aU(Gc))]$
4. $\varphi = A[aU(cUb)]$
5. $\varphi = AG[c \rightarrow (Xa \rightarrow GXb)]$
6. $\varphi = AFG(a \vee c)$

Question 3

Given a Kripke structure $M = (S, R, L)$ and a fairness condition $F = \{f_1,..., f_m\} \subseteq 2^S$ as studied in the lectures. I.e a path $\pi = s_0, s_1,...$ is fair if for all $1 \le i \le m$ we have $f_i \cap inf(\pi) \ne \emptyset$.

A. **Definition:** For $M = (S, R, L)$ we define that a path $\pi = s_0, s_1,...$ is *existential-fair* regarding existential-fairness condition $H = \{h_1,..., h_n\} \subseteq 2^S$ if **exists** $1 \le i \le n$ such that: $h_i \subseteq inf(\pi)$.

   Given a fairness condition F, find an existential-fairness condition H, such that: for any path π, π is existential-fair regarding H if and only if π is fair regarding F. prove your answer.

B. **Definition:** For $M = (S, R, L)$ we define that a path $\pi = s_0, s_1,...$ is *general-fair* regarding general-fairness condition $H = \{h_1,..., h_n\} \subseteq 2^S$ if **for all** $1 \le i \le n$ we have: $inf(\pi) \subseteq h_i$.

   Pay attention: The inclusion direction is opposite to the one that appears in the *existential-fair definition*, and the demand is for all i.
   Given a general-fairness condition H, find a fairness condition F, such that: for any path π, π is general-fair regarding H if and only if π is **not** fair regarding F. prove your answer.

Question 4

Given a Kripke structure $M = (S, R, L)$ in which any state is colored in black or white.
The black states are satisfying the atomic formula b, and the white states are satisfying the atomic formula w.
And formally, the structure M is over $AP = \{b, w\}$ such that for all $s \in S$ we have $L(s) = \{b\}$ or $L(s) = \{w\}$.

Let's define that a path in the structure will be called a legal if there is exactly one color switch in it.

A. Write a CTL formula ϕ, such that for all $s \in S$ we have $M, s \models \phi$ if and only if exists a legal path from s. justify the correctness of your formula.
B. Write an explicit algorithm, efficient as possible, which marks all the states that have a legal path from them. Explain the algorithm's correctness.

Good luck!