You can review the latex source for this assignment-file to learn and use latex to prepare your homework submission. You will see the use of macros (to write uniformly formatted text), different text-styles (emphasized, bold-font), different environments (figures, enumerations).

It is not required that you use exactly this latex source to prepare your submission.

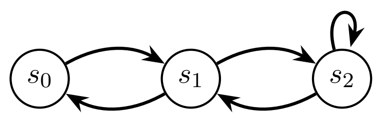
Homework 1 (CTL): ComS/CprE/SE 412, ComS 512

Due-date: Feb 7 at 11:59PM.

Submit online on Canvas two files: the source file in latex format and the pdf file generated from latex. Name your files: ⟨your-net-id⟩-hw1.⟨tex/pdf⟩.

Homework must be individual's original work. Collaborations and discussions of any form with any students or other faculty members or soliciting solutions on online forums are not allowed. Please review the academic dishonesty policy on our syllabus. If you have any questions/doubts/concerns, post your questions/doubts/concerns on Piazza and ask TA/Instructor.

1. Consider the following Kripke structure, with $p \in L(s_0) \cap L(s_2)$ and $q \in L(s_2)$.



Identify the set of states that satisfy each of the following:

(a) $\mathtt{EX}(q)$
(b) $\mathtt{AX}(p)$
(c) $\mathtt{AX}(q)$
(d) $\mathtt{AG}(p)$
(e) $\mathtt{EG}(p)$
(f) $\mathtt{AF}(p)$
(g) $\mathtt{AG}(\mathtt{EX}(p))$
(h) $\mathtt{AG}(\mathtt{AF}(p))$

(16 pts)

Answer: The tree of computation is -

(a) $\{s_1, s_2\}$
(b) $\{s_1\}$
(c) $\{\}$
(d) $\{\}$
(e) $\{s_2\}$
(f) $\{s_0, s_1, s_2\}$

(g) $\{s_1, s_2\}$

(h) $\{s_0, s_1, s_2\}$

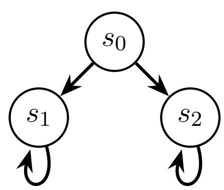
2. Express the following statements as CTL formula: (4+4+6 pts)

   (a) Along all paths **withdraw-money** is never true after **invalid-login**.
   Answer: AG (**invalid-login** $\Rightarrow$ AXAG **withdraw-money**)

   (b) Along all execution sequences of an elevator behavior, if the elevator door is **open** then the door remains **open** until a **request-to-move** is sent to the elevator.
   Answer: AG ((**open** $\Rightarrow$ AG **open**) U **request-to-move**)

   (c) Whenever proposition **request-site-update** is true in a state, it is followed in zero or more steps by a state where proposition **updating-site** is true, which in turn is followed in one or more steps by a state where **update-complete** is true.
   Answer: AG ((**request-site-update** $\Rightarrow$AF **updating-site**) $\Rightarrow$ AXAF **update-complete**)

3. To disprove that two CTL formula are equivalent, you are required to draw a Kripke structure and identify a state in that structure, which satisfies one of the formula and does not satisfy the other. For instance, in order to disprove that $\texttt{EX}(p) \ \wedge \ \texttt{EX}(q)$ and $\texttt{EX}(p \ \wedge \ q)$ are equivalent, we can draw the following the Kripke structure:



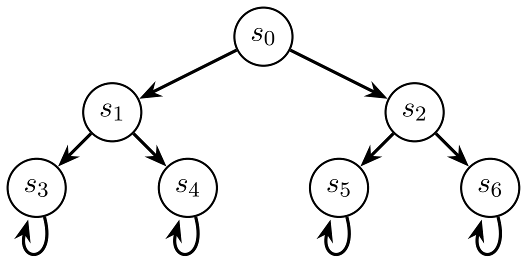
$L(s_1) = \{p\}$, $L(s_2) = \{q\}$

We present the labels for the relevant states in the Kripke structure and state that s_0 satisfies $\texttt{EX}(p) \wedge \texttt{EX}(q)$ and s_0 does not satisfy $\texttt{EX}(p \wedge q)$. This is because there exists a path from s_0 where in the very next state s_1 the proposition p is true; thus conforming that s_0 satisfies $\texttt{EX}(p)$ (similarly, one can justify the satisfiability of $\texttt{EX}(q)$ at state s_0). On the other hand, there exists no path from s_0, where in the very next state both p and q are satisfied.

Disprove that the two CTL formula $\texttt{AF}(p \wedge q)$ and $\texttt{AF}(p) \wedge \texttt{AF}(q)$ are equivalent. (5 pts)

Answer:

$\texttt{AF}(p \wedge q)$ implies that $p \wedge q$ is true sometimes in all possible future states from starting state. However, $\texttt{AF}(p) \wedge \texttt{AF}(q)$ says that "In all possible future states, p must be true, and in all possible future states, q must be true". Therefore, p and q does not necessarily true in one state to satisfy $\texttt{AF}(p) \wedge \texttt{AF}(q)$, but $\texttt{AF}(p \wedge q)$ demands p and q to be true in the same state.



$L(s_1) = \{p\}$, $L(s_3) = \{q\}$, $L(s_4) = \{q\}$
$L(s_2) = \{q\}$, $L(s_5) = \{p\}$, $L(s_6) = \{p\}$

The above Kripke structure satisfies $\texttt{AF}(p) \wedge \texttt{AF}(q)$, but it does not satisfy $\texttt{AF}(p \wedge q)$. Therefore, it can be said that these two properties are not equivalent.

4. To prove that one formula (say, φ_1) is "stronger" than another (say, φ_2), you need to prove that whenever in any state in any Kripke structure φ_1 holds, φ_2 holds in that state as well. In other words, φ_1 is "stronger" than φ_2 if and only if $\varphi_1 \Rightarrow \varphi_2$ is a tautology (always evaluates to true). For instance, to prove that $\texttt{AX}(p)$ is stronger than $\texttt{EX}(p)$ we can write:

$$\begin{aligned} \forall s.s \in [\![\texttt{AX}(p)]\!] &\Leftrightarrow \forall \pi \in Path(s) : \pi[1] \in [\![p]\!] \\ &\Rightarrow \exists \pi \in Path(s) : \pi[1] \in [\![p]\!] \\ &\Rightarrow s \in [\![\texttt{EX}(p)]\!] \end{aligned}$$

To disprove that $\texttt{EX}(p)$ is stronger that $\texttt{AX}(p)$, you will draw a Kripke structure and present a state in the Kripke structure that satisfies $\texttt{EX}(p)$ but does not satisfy $\texttt{AX}(p)$ (see the Kripke structure example in the previous problem).

Prove or disprove $\texttt{AG}(p \wedge q)$ is stronger than $\texttt{AG}(p \Rightarrow \texttt{AF}(q))$.

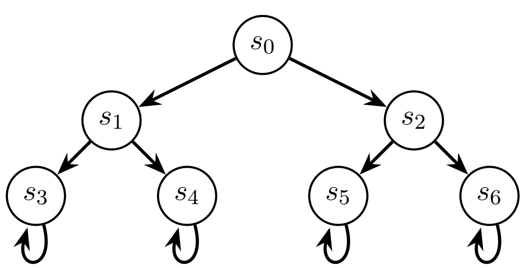
Answer:

Let's simplify $\texttt{AG}(p \Rightarrow \texttt{AF}(q))$.

$$\begin{aligned} \forall s.s \in [\![\texttt{AG}(p \Rightarrow \texttt{AF}(q))]\!] &\Leftrightarrow \forall \pi \in Path(s) : \pi[0] \in [\![p \Rightarrow \texttt{AF}(q)]\!] \\ &\Rightarrow \forall \pi \in Path(s) : \pi[0] \in [\![\neg p \vee \texttt{AF}(q)]\!] \\ &\Rightarrow \forall \pi \in Path(s) : \pi[0] \in [\![\texttt{AF}(q)]\!] \\ &\Rightarrow \forall \pi \in Path(s) : \pi[0] \in [\![q]\!] \end{aligned}$$

When $\texttt{AG}(p \Rightarrow \texttt{AF}(q))$ holds in s, it is immediately true that $p \Rightarrow \texttt{AF}(q)$ holds for all successors of s, including s itself. We can rewrite $p \Rightarrow \texttt{AF}(q)$ as $\neg p \vee \texttt{AF}(q)$, which implies either $\neg p$ or $\texttt{AF}(q)$ true in s and its successors. without loss of generality, we can write q holds in state s.

$\texttt{AG}(p \wedge q)$ implies $p \wedge q$ holds in all successors of s including s itself. As both p and q holds in state s, which immediately implies $p \Rightarrow \texttt{AF}(q)$ true at that state. The Kripke structure satisfying $\texttt{AG}(p \wedge q)$ is provided below.



$L(s_1) = \{p, q\}, L(s_3) = \{p, q\}, L(s_4) = \{p, q\}$
$L(s_2) = \{p, q\}, L(s_5) = \{p, q\}, L(s_6) = \{p, q\}$

So, we can say that the formula $\texttt{AG}(p \wedge q)$ is stronger than $\texttt{AG}(p \Rightarrow \texttt{AF}(q))$.

(5 pts)

5. **Extra Credit for 412; Required problem for 512.** We will define a new operator $A\circ$ as follows. A state s satisfies $\texttt{A}(\varphi_1 \circ \varphi_2)$ if and only if for all paths starting from s at least one of the following holds

- there exists a state where φ_2 is satisfied and before that φ_1 holds in all states in the path
- all states in the path satisfy φ_1 and not φ_2

Prove or disprove that

(a) $A(p \circ \text{false})$ can be expressed in CTL.

(b) $A(\text{false} \circ p)$ can be expressed in CTL.

(10pts)