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.

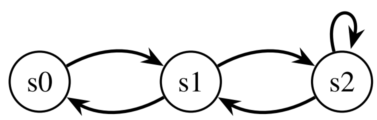
Homework 1 (CTL): ComS/CprE/SE 412, ComS 512

Due-date: Feb 15 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) $\mathtt{EX}(p)$
$\{s_1, s_2\}$

(b) $\mathtt{EX}(q)$
$\{s_1, s_2\}$

(c) $\mathtt{AX}(p)$
$\{s_1\}$

(d) $\mathtt{AX}(q)$
$\{\}$

(e) $\mathtt{AG}(p)$
$\{\}$

(f) $\mathtt{EG}(p)$
$\{s_2\}$

(g) $\mathtt{AF}(p)$
$\{s_0, s_1, s_2\}$

(h) $\mathtt{AG}(\mathtt{EX}(p))$
$\{\}$

(i) $\mathtt{AG}(\mathtt{AF}(p))$
$\{s_0, s_1, s_2\}$

(15pts)

2. Express the following statements as CTL formula: (15 pts)

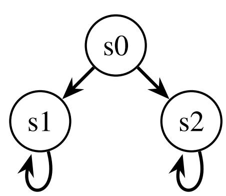
   (a) Along all paths **withdraw-money** is never true after **invalid-login**.
   $\texttt{AG}(\textbf{invalid-login} \Rightarrow \texttt{AX}(\texttt{AG}(\neg\textbf{withdraw-money})))$

   (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.
   $\texttt{AG}(\textbf{open} \Rightarrow \texttt{A}(\textbf{open}\ \texttt{U}\ \neg\textbf{open} \wedge \textbf{request-to-move}))$

   It is possible to interprete the English "until request-to-move" to include the case that no "request-to-move" occurs ever. In that scenario, does the English statement expressible in CTL?

   (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.
   $\texttt{AG}(\textbf{request-site-update} \Rightarrow \texttt{AF}(\textbf{updating-site} \wedge \texttt{AX}(\texttt{AF}(\textbf{update-complete}))))$

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 $\texttt{EX}(p \wedge q)$.

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

   We have done this problem as part of the lecture. The first property captures the following. A state s satisfies the property iff along all paths from s and in all states of every path, p holds then s must satisfy $\texttt{AF}(q)$. The second property on the other hand states that s satisfies the property iff along all paths if there is a state t where p holds, then t must satisfy $\texttt{AF}(q)$.

   The two properties are not equivalent. Draw a KS and identify a state that satisfies one property but does not satisfy the other. Hint: consider a KS with a state s such that there is a state reachable from s that satisfies p and there is another state reachable from s that does not satisfy p. Complete the contruction.

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 $\mathtt{AX}(p)$ is stronger than $\mathtt{EX}(p)$ we can write:

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

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

Prove or disprove $\mathtt{EF}(\mathtt{AG}(p))$ is stronger than $\mathtt{EF}(\mathtt{EG}(p))$.

Let $\mathtt{AG}(p)$ be φ and $\mathtt{EG}(p)$ be ψ. Therefore, the claim to prove/disprove is $\mathtt{EF}(\varphi)$ is stronger than $\mathtt{EF}(\psi)$. In other words, the claim is φ is stronger than ψ.

$$\begin{aligned} \forall s.s \in [\![\mathtt{AG}(p)]\!] &\Longleftrightarrow \forall \pi \in \text{Path}(s).\forall i \geq 0.\pi[i] \in [\![p]\!] \\ &\Longrightarrow \exists \pi \in \text{Path}(s).\forall i \geq 0.\pi[i] \in [\![p]\!] \\ &\Longleftrightarrow s \in [\![\mathtt{EG}(p)]\!] \end{aligned}$$

(5 pts)

5. **Extra Credit.** We will define a new operator $A\circ$ as follows. A state s satisfies $\mathtt{A}(\varphi_1 \circ \varphi_2)$ 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.

   The propositional constant false is never satisfiable. Therefore, the first condition above is not satisfiable. The condition two is satisfiable and it is expressed as $\mathtt{AG}(p)$

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

   In this case, the second condition is not satisfiable. The first condition is satisfiable only when the first state in the path satisfies p. Therefore, the property is expressible as p.

(10pts)