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 3 (CTL): ComS/CprE/SE 412, ComS 512

Due-date: Mar 19 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⟩-hw3.⟨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. Recall that in NuSMV, a system satisfies a CTL property if and only if every start state in the system satisfies the property, under consideration.

   Specifically, let a system be $M = (S, S_0, T, L)$, where S is the set of states in the system, $S_0 \subseteq S$ is the set of start states in the system, T is the transition relation and L is the labeling function; and φ be a CTL property. Then, the system satisfies φ, denoted by $M \models \varphi$ if and only if $S_0 \subseteq [\![\varphi]\!]_M$.

   You are asked to verify whether the following requirement is satisfied by a system encoded in NuSMV.

   *It is always possible to reach a state where **reset** is true from at least one of the start states of the system.*

   Furthermore, if the system conforms to the requirement, you are also asked to present a witness, i.e., at least one sequence of system evolution that leads to a state where **reset** is true.

   Explain whether or not it is possible to verify such a requirement for a system in NuSMV. If your answer is affirmative, then explain how you may be able to present a witness using NuSMV.

   (10pts)

   Consider the property $\texttt{EG}(\neg\texttt{reset})$. If this property is not satisfied by the system, then there exists at least one start start that does not satisfy $\texttt{EG}(\neg\texttt{reset})$. In other words, at least one start state satisfies $\neg\texttt{EG}(\neg\texttt{reset})$, which is equivalent to $\texttt{AF}(\texttt{reset})$.

   In order to find a witness, we need to identify a path where `reset` is eventually true. Consider the property $\texttt{AG}(\neg\texttt{reset})$. As there is at least one start state, where $\texttt{AF}(\texttt{reset})$ is satisfied, therefore, there is at least one start state, where $\texttt{EF}(\texttt{reset})$ is satisfied. In other words, such a state will not satisfy the property $\texttt{AG}(\neg\texttt{reset})$ and will generate a counter-example as a witness.

   If you have answered that the witness cannot be generated because it is impossible to guarantee that the start state that satisfies $\texttt{AG}(\texttt{reset})$ will be used in the second step to generate the witness, then you will get full points.

2. Consider $f : \mathcal{P}(S) \to \mathcal{P}(S)$ a monotonically non-decreasing function defined over a finite set S. We will use $\overline{X}$ to denote $S - X$ for any $X \subseteq S$, and will use $\texttt{lfp}(.)$ and $\texttt{gfp}(.)$ to denote the least fixed point and the greatest fixed point of functions, respectively.

Consider two functions $g_1, g_2 : \mathcal{P}(S) \to \mathcal{P}(S)$ such that

$$\forall Z \subseteq S : f(Z) = \overline{g_1(Z)}$$

$$\forall Z \subseteq S : f(Z) = \overline{g_2(\overline{Z})}$$

Prove or disprove the following:

(a) g_1 is monotonically non-decreasing.

(b) g_2 is monotonically non-decreasing.

(c) $\texttt{lfp}(f)$ is equal $\overline{\texttt{gfp}(g_2)}$.

(10pts)

(a) g_1 is not monotonically non-decreasing. Consider $X \subseteq Y$. Therefore, $\overline{X} \supseteq \overline{Y}$ and $f(X) \subseteq f(Y)$.
Therefore, $\overline{X} \supseteq \overline{Y}$ implies $g_1(\overline{X}) \subseteq g_1(\overline{Y})$.

(b) Follow the same strategy as above to prove that g_2 is monotonically non-decreasing.

(c) Use Tarski-Knaster theorem.

$$f(\emptyset) = \overline{g_2(S)}$$

$$f(f(\emptyset)) = \overline{g_2(\overline{f(\emptyset)})} = \overline{g_2(\overline{\overline{g_2(S)}})} = \overline{g_2(g_2(S))}$$

Proceeding further, $f^{|S|}(\emptyset) = \overline{g_2^{|S|}(S)}$.

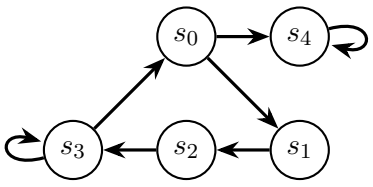
3. Consider the following functions defined of sets of Kripke structure (S, T, L):

$$R_\forall(Z) = \{s \mid \forall s'.(s, s') \in T \Rightarrow s' \in Z\}$$
$$I_\varphi(Z) = [\![\varphi]\!]_M \cup R_\forall(Z)$$
$$K_\varphi(Z) = [\![\varphi]\!]_M \cap R_\forall(Z)$$

In the above φ denotes CTL formula. We know that $[\![\texttt{AF}(\varphi)]\!]_M$ is the least fixed point of I_φ.

(a) Show that $[\![\texttt{AG}(\varphi)]\!]_M$ is the greatest fixed point K_φ.

(b) For the following Kripke structure with $b \in L(s_3)$, $\{a, b\} \subseteq L(s_2)$, $a \in L(s_1)$ and $b \in L(s_4)$,



find the semantics of the following CTL formula using fixed point computations of relevant functions (present the steps of your computation)

i. $\texttt{AG}(\texttt{AF}(b))$

ii. $\texttt{AF}(\texttt{AG}(b))$

(20pts)

(a)

$$\begin{aligned}
[\![\mathtt{AG}(\varphi)]\!] &= \{s \mid \forall \pi \in Paths(s).\forall i \geq 0.\pi[i] \in [\![\varphi]\!]\} \\
&= \{s \mid \forall \pi \in Paths(s).\pi[0] \in [\![\varphi]\!] \wedge \forall i \geq 1.\pi[i] \in [\![\varphi]\!]\} \\
&= \{s \mid s \in [\![\varphi]\!]\} \cap \{s \mid \forall \pi \in Paths(s).\forall i \geq 1.\pi[i] \in [\![\varphi]\!]\} \\
&= [\![\varphi]\!] \cap \{s \mid \forall \pi \in Paths(s).\pi[1] \in [\![\mathtt{AG}(\varphi)]\!]\} \\
&= [\![\varphi]\!] \cap R_\forall([\![\mathtt{AG}(\varphi)]\!]) \\
&= K_\varphi([\![\mathtt{AG}(\varphi)]\!])
\end{aligned}$$

Hence, $[\![\mathtt{AG}(\varphi)]\!]$ is a fixed point of K_φ.
Next, assume that there exists a $Z = K_\varphi(Z)$ such that $Z \supset [\![\mathtt{AG}(\varphi)]\!]$. Therefore, there exists a state s such that $s \in Z$ and $s \notin [\![\mathtt{AG}(\varphi)]\!]$.

$$\begin{aligned}
& s \in Z \wedge s \notin [\![\mathtt{AG}(\varphi)]\!] \\
\Rightarrow\ & s \in K_\varphi(Z) \wedge s \notin K_\varphi([\![\mathtt{AG}(\varphi)]\!]) \\
\Rightarrow\ & s \in [\![\varphi]\!] \cap R_\forall(Z) \wedge s \notin ([\![\varphi]\!] \cap R_\forall([\![\mathtt{AG}(\varphi)]\!])) \\
\Rightarrow\ & s \in [\![\varphi]\!] \wedge s \in R_\forall(Z) \wedge s \notin R_\forall([\![\mathtt{AG}(\varphi)]\!])
\end{aligned}$$

Therefore, the next states of s can be partitioned into S_1 and S_2 such that: $S_1 \cap [\![\mathtt{AG}(\varphi)]\!] = \emptyset$ and $S_2 \subseteq [\![\mathtt{AG}(\varphi)]\!]$. Furthermore, $S_1 \cup S_2 \subseteq Z$. Note that, the computation tree rooted at any states in S_2 satisfy the property $\mathtt{AG}(\varphi)$ and hence all states in those computation trees satisfy φ. Furthermore, all states in S_1 has exactly the same property as s, i.e., these states belong to the semantics of φ, do not belong to the semantics of $\mathtt{AG}(\varphi)$ and belong to the set Z.

Proceeding further, we can inductively construct a computation tree rooted at s such that all states in the computation tree satisfy φ (as they all belong to the semantics of φ) but s does not belong the semantics of $\mathtt{AG}(\varphi)$ (as per our assumption). This is logically inconsistent with the semantics of $\mathtt{AG}(\varphi)$. Hence our assumption that $Z \supset [\![\mathtt{AG}(\varphi)]\!]$ is invalid, and $[\![\mathtt{AG}(\varphi)]\!]$ is the greatest fixed point of K_φ.

Another way to prove that $[\![\mathtt{AG}(\varphi)]\!]$ is indeed the greatest fixed point of K_φ: here is the outline. Assume that there is some fixed point Z of K_φ such that $Z \supset [\![\mathtt{AG}(\varphi)]\!]$. Therefore, there exists a state s such that $s \in Z$ and $s \notin [\![\mathtt{AG}(\varphi)]\!]$.

$$\begin{aligned}
& s \in Z \\
\Rightarrow\ & s \in K_\varphi(Z) \\
\Rightarrow\ & s \in [\![\varphi]\!] \cap R_\forall(Z) \\
\Rightarrow\ & s \in [\![\varphi]\!] \wedge \forall s \rightarrow s'.s' \in Z
\end{aligned}$$

Therefore, along all paths in the computation tree rooted at s, φ is satisfied in every state. I.e., s satisfies $\mathtt{AG}(\varphi)$. This leads to a contradiction.

(b-i) $[\![\texttt{AG}(\texttt{AF}(b))]\!]$ is the greatest fixed point of $K_{\texttt{AF}(b)}$ and $[\![\texttt{AF}(b)]\!]$ is least fixed point of I_b. Therefore,

$$\begin{aligned} K_{\texttt{AF}(b)}(S) &= [\![\texttt{AF}(b)]\!] \cap R_\forall(S) \\ &= I_b^5(\emptyset) \cap S \end{aligned}$$

We need to first compute $I_b^5(\emptyset)$.

$$\begin{aligned} I_b(\emptyset) &= [\![b]\!] \cup R_\forall(\emptyset) \\ &= \{s_2, s_3, s_4\} \end{aligned}$$

$$\begin{aligned} I_b^2(\emptyset) &= [\![b]\!] \cup R_\forall(I_b(\emptyset)) \\ &= \{s_2, s_3, s_4\} \cup \{s_2, s_1, s_4\} \\ &= \{s_1, s_2, s_3, s_4\} \end{aligned}$$

$$\begin{aligned} I_b^3(\emptyset) &= [\![b]\!] \cup R_\forall(I_b^2(\emptyset)) \\ &= \{s_2, s_3, s_4\} \cup \{s_2, s_1, s_4, s_0\} \\ &= S = I_b^4(\emptyset) = I_b^5(\emptyset) \text{ Think about why we do not need to explicitly compute } I^4 \text{ and } I^5 \end{aligned}$$

Proceeding further,

$$\begin{aligned} K_{\texttt{AF}(b)}(S) &= I_b^5(\emptyset) \cap S \\ &= S \text{ This is a fixed point: we do not need to do any more computation} \end{aligned}$$

The semantics of $\texttt{AG}(\texttt{AF}(b))$ is the set of all states.

(b-ii) Exercise.