Exam 2: COMS/CPRE/SE 412 & COMS 512

April 06, 2021

Time: 75 mins

Learning Outcomes

- Application of knowledge of computing and mathematics
- Ability to understand the implications of mathematical formalisms in computer science
- Ability to apply logic for formalizing requirement specifications.

You can consult lecture materials to answer any questions in this test. You are not allowed to collaborate in any form with anyone.

Question	Points	Score
1 (English to CTL)	12	
2 (CTL Equivalences)	10	
3 (Model Checking)	10	
4 (Fixed Point)	8	
5 (BDD)	10	
6 (Extra Credit)	10	
Total	50	

Questions

1. Express the following in CTL

   (a) Along all execution sequences of a submarine controller, if the hutch door is closed then the door remains in closed-state until ballast tanks are emptied.
   $\mathtt{AG}(closed \Rightarrow \mathtt{A}(closed\ \mathtt{U}\ emptied))$

   (b) Along all execution sequence access denied is never preceded by login-success (preceded does not necessarily mean immediately before).
   $\mathtt{AG}(login \Rightarrow \mathtt{AG}(\neg denied))$

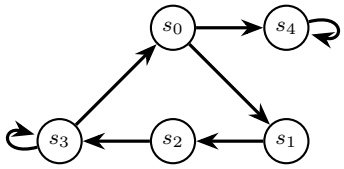
   (c) Along all executions, two threads accesses the critical sections in strict sequence. That is, for $i, j \in [1, 2]$, thread i enters the critical section, then thread j $(j \neq i)$ enters the critical section, then thread i enters the critical section, and so on (assume two threads never enter the critical section at the same time).
   $\neg\mathtt{EF}(c_i \wedge \mathtt{E}(c_i\ \mathtt{U}\ (\neg c_i \wedge \neg c_j) \wedge \mathtt{E}((\neg c_i \wedge \neg c_j)\ \mathtt{U}\ c_i)))$

2. Prove/disprove that the following pairs are equivalent:

   (a) $\mathtt{AF}(\mathtt{AX}(p))$ and $\mathtt{AX}(\mathtt{AF}(p))$ Has been done before.

   (b) $\neg\mathtt{A}(\neg p\ \mathtt{U}\ p)$ and $\mathtt{EG}(\neg p)$ $\mathtt{A}(\neg p\ \mathtt{U}\ p)$ is equivalent to $\mathtt{AG}(p)$.

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



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

   (a) $\mathtt{AG}(b \Rightarrow \mathtt{AF}(b \vee c))$
   $\mathtt{AF}(b \vee c)$ is satisfied in all states before all paths from every state lead to some state where b is satisfied (s_2, s_3, s_4). Therefore, the property is satisfied in all states as well.

   (b) $\mathtt{E}(\mathtt{EF}(b)\ \mathtt{U}\ \neg b)$
   All states except s_4 because s_4 does not have a path where eventually $\neg b$ is satisfied.

4. Fixed point problem:

   (a) **[512 only.]** We are given a function $f : \mathcal{P}(S) \to \mathcal{P}(S)$ where S is finite and f is monotonically non-decreasing function wrt $\subseteq$. We define a set $W = \{Z \mid f(Z) \subseteq Z \subseteq S\}$, i.e., W is set of all subsets Z of S such that $f(Z) \subseteq Z$. We further define V as intersection of all sets in W (denoted by $V = \bigcap W$).
   Prove or disprove that V is the least fixed point f.
   Claim 1: $\bigcap W$ is a fixed point of f.
   We know that $\bigcap W \subseteq Z$ for and $Z \in W$. Therefore, $\forall Z \in W : f(\bigcap W) \subseteq f(Z) \subseteq Z$ due to monotonicity of f and definition of W. Proceeding further,

   $$\begin{aligned} & f(\bigcap W) \subseteq \bigcap W \\ \Rightarrow\ & f(f(\bigcap W)) \subseteq f(\bigcap W) \text{ due to monotonicity of } f \\ \Rightarrow\ & f(\bigcap W) \in W \text{ due to defintion of } W \\ \Rightarrow\ & \bigcap W \subseteq f(\bigcap W) \end{aligned}$$

   Therefore, $f(\bigcap W) = \bigcap W$.
   Claim 2: $\bigcap W$ is the least fixed point of f.
   Consider any fixed point Y of f. $Y = f(Y)$ implies $f(Y) \subseteq Y$. Therefore, $Y \in W$. Proceeding further, $\bigcap W \subseteq Y$.

(b) **[412; for 512 this will be counted as extra credit.]** Consider two monotonically non-decreasing functions f_1 and f_2 over finite set of elements S (for $i \in [1,2]$, $f_i : \mathcal{P}(S) \rightarrow \mathcal{P}(S)$). Consider another function $g : \mathcal{P}(S) \rightarrow \mathcal{P}(S)$ such that

$$g(Z) = f_1(Z) \cup f_2(Z)$$

Prove that the following claim is valid: there exist some definitions for f_1 and f_2 such that the least fixed point of g is equal to the union of the least fixed point of f_1 and least fixed point of f_2.

(Hint: Think about the fixed point characterization of CTL)

Consider the fixed point characterizations of $\texttt{EF}(p)$, $\texttt{EF}(q)$ and $\texttt{EF}(p \vee q)$

5. Consider the following boolean function defined over a set of boolean variables $v_1, v_2, \ldots, v_n$:

$$f(v_1, v_2, \ldots, v_n) = \begin{cases} 1 & \text{if even number of } v_i's \text{ are true} \\ 0 & \text{otherwise} \end{cases}$$

(a) Draw an ROBDD when $n = 6$.

(b) Write the number of variable orderings (in terms of n) for which the ROBDD representation of the above function will be the smallest. Justify your answer.

Any ordering of variables will provide the smallest ROBDD. This is because the counting property does not depend on the ordering in which the variables are counted. There are $n!$ ordering.

6. **[Extra Credit.]** Prove or disprove the following:

For any Kripke structure a state satisfies $\texttt{AX}(q) \vee \texttt{AX}(\texttt{AX}(q)) \vee \texttt{AX}(\texttt{AX}(\texttt{AX}(q)))$ if and only if it also satisfies $\texttt{X}(q) \vee \texttt{X}(\texttt{X}(q)) \vee \texttt{X}(\texttt{X}(\texttt{X}(q)))$. [A state satisfies an LTL formula if and only if every path starting from the state belongs to the semantics of the LTL formula.]

Consider a Kripke structure with the following transition relations. s_0 has a transition to s_1 and s_1 has a transition to s_2, which has a self-loop. s_0 also has a transition to s_3 and s_3 has a transition to s_1. The proposition p is true only in state s_1.

Therefore, s_0 does not satisfy $\texttt{AX}(p)$ because it has a next state s_3 where p is not true. s_0 does not satisfy $\texttt{AX}(\texttt{AX}(p))$ because it has a a next to next state s_2 where p is not satisfied. Same goes for $\texttt{AX}(\texttt{AX}(\texttt{AX}(p)))$.

However, in case of LTL, we consider one path at a time. There are two path patterns, s_0 to s_1 to s_2 and remains in s_2, and s_0 to s_3 to s_1 to s_2 and remains in s_2. In the first path $\texttt{X}(p)$ is satisfied and in the second path $\texttt{X}(\texttt{X}(p))$ is satisfied.

Exam 2: ComS/CprE/SE 412, ComS 512

1. Express the following in CTL

   (a) Along all execution sequences of a submarine controller, if the hutch door is closed then the door remains in closed-state until ballast tanks are emptied.
   If ballastEmpty has to happen: $\texttt{AG}(doorClosed \Rightarrow \texttt{A}(doorClosed\ \texttt{U}\ ballastEmpty))$
   Else, Not possible in CTL because either door remains closed forever or door remains closed until ballast are emptied & disjunction over universal quantifier cannot encode property satisfiablity by part paths.

   (b) Along all execution sequence access denied is never preceded by login-success (preceded does not necessarily mean immediately before).
   $\texttt{AG}(loginSuccess \Rightarrow \texttt{AX}(\texttt{AG}(\neg accessDenied)))$

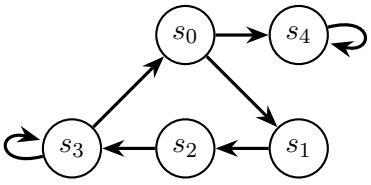
   (c) Along all executions, two threads accesses the critical sections in strict sequence. That is, for $i, j \in [1, 2]$,thread i enters the critical section, then thread $j(j \neq i)$ enters the critical section, then thread i enters the critical section, and so on (assume two threads never enter the critical section at the same time).
   There does not exist two consecutive accesses by thread i without thread j in between and two consecutive accesses by thread j without thread i in between.
   $\neg(\texttt{EF}((cs_i \wedge \texttt{E}(\neg cs_j\ \texttt{U}\ cs_i))) \vee \texttt{EF}((cs_j \wedge \texttt{E}(\neg cs_i\ \texttt{U}\ cs_j))))$

2. Prove/disprove that the following pairs are equivalent:

   (a) $\texttt{AF}(\texttt{AX}(p))$ and $\texttt{AX}(\texttt{AF}(p))$
   Not equivalent. $\texttt{AF}(\texttt{AX}(p))$ means that at some point in future, all the next states will satisfy p. $\texttt{AX}(\texttt{AF}(p))$ means that starting from next state, along all paths there there is a future state where p is true. In the KS below, if $p \in L(s_3) \wedge L(s_4)$, then $s_1 \models \texttt{AX}(\texttt{AF}(p))$ but $s_1 \not\models \texttt{AF}(\texttt{AX}(p))$.

   (b) $\neg\texttt{A}(\neg p\ \texttt{U}\ p)$ and $\texttt{EG}(\neg p)$
   $\neg\texttt{A}(\neg p\ \texttt{U}\ p)$ is same as $\neg\texttt{AF}(p) = \texttt{EG}(\neg p)$. Hence, equivalent.

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



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

   (a) $\texttt{AG}(b \Rightarrow \texttt{AF}(b \vee c))$
   $[\![b \vee c]\!] = [\![b]\!] = \{s_3, s_2, s_4\}$
   $[\![\texttt{AF}(b \vee c)]\!] = [\![\texttt{AF}(b)]\!] = \{s_3, s_2, s_1, s_4, s_0\}$
   $[\![b \Rightarrow \texttt{AF}(b \vee c)]\!] = S$
   $[\![\texttt{AG}(b \Rightarrow \texttt{AF}(b \vee c))]\!] = S$

(b) $\mathtt{E}(\mathtt{EF}(b)\ \mathtt{U}\ \neg b)$
$[\![\neg b]\!] = \{s_0, s_1\}$
$[\![\mathtt{EF}(b)]\!] = \{s_3, s_2, s_1, s_4, s_0\}$
$[\![\mathtt{E}(\mathtt{EF}(b)\ \mathtt{U}\ \neg b)]\!] = \{s_0, s_1, s_2, s_3\}$

4. Fixed point problem:

(a) **[512 only.]** We are given a function $f : \mathcal{P}(S) \to \mathcal{P}(S)$ where S is finite and f is monotonically non-decreasing function wrt $\subseteq$. We define a set $W = \{Z | f(Z) \subseteq Z \subseteq S\}$, i.e., W is set of all subsets Z of S such that $f(Z) \subseteq Z$. We further define V as intersection of all sets in W (denoted by $V = \cap W$). Prove or disprove that V is the least fixed point f.
Let $W = \{W_1, W_2, \ldots, W_k\}$, where $f(W_i) \subseteq W_i$.
It is also true that $\cap W \subseteq W_i$ for any $W_i \in W$ (intersection of sets is a subset of each set).
Because f is a non-decreasing monotone, $f(\cap W) \subseteq f(W_i)$ and from defn. of W, $f(W_i) \subseteq W_i$.

$$f(V) \subseteq W_i \text{ and } \cap_i W_i = \cap W = V \text{ contains } f(V) \tag{1}$$

$$f(V) \subseteq V \Rightarrow f(f(V)) \subseteq f(V) \tag{2}$$

Therefore, $f(V)$ is in W, by defn. of W. Let it be denoted by W_j.
Since , $\forall i, \cap W \subseteq W_i \Rightarrow \cap W \subseteq W_j = f(V) \Rightarrow V \subseteq f(V)$
Therefore, $f(V) \subseteq V$ and $V \subseteq f(V) \to f(V) = V$. Fixed point.

Let us assume, $f(Y) = Y$ and $Y \subset V$.
By definition of W, $Y \in W$.
Therefore, $V = \cap W$ must be a subset of Y.
So, $V = Y$ and hence, least fixed point.

(b) **[412;for 512 this will be counted as extra credit.]** Consider two monotonically non-decreasing functions f_1 and f_2 over finite set of elements S (for $i \in [1, 2]$, $f_i : \mathcal{P}(S) \to \mathcal{P}(S)$). Consider another function $g : \mathcal{P}(S) \to \mathcal{P}(S)$ such that $g(Z) = f_1(Z) \cup f_2(Z)$. Prove that the following claim is valid: there exist some definitions for f_1 and f_2 such that the least fixed point of g is equal to the union of the least fixed point of f_1 and least fixed point of f_2.(Hint: Think about the fixed point characterization of CTL)
Example 1. Let $f_1(Z) = [\![p]\!] \cup R_\exists(Z)$ and $f_2(Z) = [\![q]\!] \cup R_\exists(Z)$, then

$$g(Z) = [\![p]\!] \cup [\![q]\!] \cup R_\exists(Z) = [\![p \vee q]\!] \cup R_\exists(Z)$$

From fixed-point characterization of EF, we know that
$lfp(f_1) = \mathtt{EF}(p) \quad lfp(f_2) = \mathtt{EF}(q) \quad lfp(g) = \mathtt{EF}(p \vee q)$

$lfp(f_1) \vee lfp(f_2) = \mathtt{EF}(p) \vee \mathtt{EF}(q) = \mathtt{EF}(p \vee q) = lfp(g)$

Example 2. Let $f_1(Z) = [\![p]\!] \cup Z$ and $f_2(Z) = [\![q]\!] \cup Z$, then

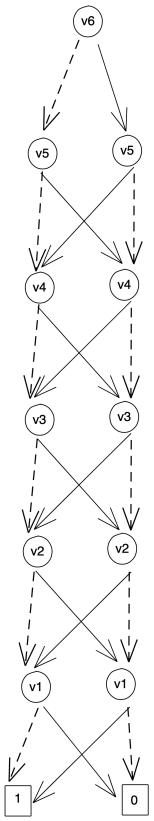
$$g(Z) = [\![p \vee q]\!] \cup Z$$

$lfp(f_1) = p,\ lfp(f_2) = q,\ \ lfp(g) = p \vee q$
$lfp(f_1) \vee lfp(f_2) = p \vee q = lfp(g)$

5. Consider the following boolean function defined over a set of boolean variables $v_1, v_2, ..., v_n$:

$$f(v_1, v_2, ..., v_n) = \begin{cases} 1, & \text{if even number of } v_i\text{'s are true} \\ 0, & \text{otherwise} \end{cases} \tag{3}$$

(a) Draw an ROBDD when n = 6.



(b) Write the number of variable orderings (in terms of n) for which the ROBDD representation of the above function will be the smallest. Justify your answer.

Because every variable value is needed to determine the value of f and there are no "short-circuited" paths, any order of variables will produce an ROBDD of smallest size. Hence, number of optimal orderings for n variables is $n!$

6. **[Extra Credit]** Prove or disprove the following:
For any Kripke structure a state satisfies $\mathtt{AX}(q) \vee \mathtt{AX}(\mathtt{AX}(q)) \vee \mathtt{AX}(\mathtt{AX}(\mathtt{AX}(q)))$ if and only if it also satisfies $\mathtt{X}(q) \vee \mathtt{X}(\mathtt{X}(q)) \vee \mathtt{X}(\mathtt{X}(\mathtt{X}(q)))$. [A state satisfies an LTL formula if and only if every path starting from the state belongs to the semantics of the LTL formula.]

Disprove. Paths via LTL can have q satisfied at different distance from the starting state but via CTL all paths need to satisfy q at same distance from starting state.