Summer, 2020

Computer-Aided Verification
Oral exam

Question 2 [Fixpoints]

Let K be a Kripke structure with a finite set of states $\mathcal{S}$ and alphabet Σ. Let L be the complete lattice $(2^{\mathcal{S}}, \subseteq, \cup, \cap, \top, \bot)$, where $\top = \mathcal{S}$ and $\bot = \emptyset$. Let $f : L \to L$ be a monotonic function. Recall that a function $f : L \to L$ is monotonic if for all $x, y \subseteq \mathcal{S}$, we have that $x \subseteq y \Rightarrow f(x) \subseteq f(y)$.

(a) Consider the sequence $w = S_0, S_1, S_2, \ldots$, given by $S_0 = \bot$ and $S_{i+1} = f(S_i)$ for $i \geq 0$. Prove that the sequence w reaches a fixpoint of f, i.e., prove that there exists an $i \in \mathbb{N}$ such that $S_i = S_{i+1}$.

(b) **Extra credit: 10 points** Prove that the sequence w reaches the least fixpoint of f.

(c) Let p and q be two atomic propositions in Σ. Let V be the set of states where $p \,\mathsf{U}\, q$ holds. Find a function $g : L \to L$ such that V is a fixpoint of g. Is V the least fixpoint of your function, the greatest fixpoint, or neither?

Question 3 (20 points) [Temporal logics]

The syntax of CTL can be defined by the following grammar:

$$\varphi ::= p \mid \neg\varphi \mid \varphi_1 \vee \varphi_2 \mid \varphi_1 \wedge \varphi_2 \mid \mathsf{EX}\,\varphi \mid \varphi_1 \ \mathsf{EU}\,\varphi_2 \mid \mathsf{EG}\,\varphi.$$

The syntax of LTL can be defined by the following grammar:

$$\varphi ::= p \mid \neg\varphi \mid \varphi_1 \vee \varphi_2 \mid \varphi_1 \wedge \varphi_2 \mid \mathsf{X}\,\varphi \mid \varphi_1\,\mathsf{U}\,\varphi_2.$$

Note that these definitions are equivalent to those we had in class. This question explores why we need one more temporal operator in CTL.

(a) Express $\mathsf{F}\,\varphi$ in terms of the until (U) operator in LTL.

(b) Express $\mathsf{G}\,\varphi$ in terms of the eventually (F) operator in LTL.

(c) We would like to define $\mathsf{EG}\,\varphi$ in CTL in the same way as we have defined $\mathsf{G}\,\varphi$ in LTL. Can you define $\mathsf{EF}\,\varphi$ in terms of the EU operator? Can you define $\mathsf{EG}\,\varphi$ in terms of the EF operator?

Question 4 (20 points) [Büchi automata]
Let us consider the alphabet $\Sigma = \{p, q\}$.

(a) Give a Büchi automaton A_1 for the language of infinite words that satisfy the LTL formula $\mathsf{G}\,\mathsf{F}\,p$.

(b) Give a Büchi automaton A_2 for the language of infinite words that satisfy the LTL formula $\mathsf{F}\,\mathsf{G}\,q$.

(c) Given two Büchi automata B_1 and B_2, describe how to construct an automaton B_3 such that $L(B_3) = L(B_1) \cap L(B_2)$.

(d) Use your construction to give a Büchi automaton A_3 such that $L(A_3) = L(A_1) \cap L(A_2)$ (where A_1 and A_2 are the two automata from points (a) and (b)).

(e) Give a Büchi automaton A_1 for the language of infinite words that satisfy the LTL formula $\mathsf{G}\,\mathsf{F}\,p \wedge \mathsf{F}\,\mathsf{G}\,q$ using the construction we saw in class. Did you get the same result as in (d)?

Question 6 (20 points) [SAT-based model checking]

Let K be a Kripke structure. Let $\mathit{Init}(s)$ be a predicate that holds for a state s if s is an initial state of K. Let $\mathit{Trans}(s, s')$ be a formula that holds for two states s and s' if there is a transition in K from s to s'. Let $\mathit{Bad}(s)$ be a predicate on states of K.

(a) Bounded model checking.
Write a formula that is satisfiable if and only if there is a path of length 3 from an initial state to a state s where $\mathit{Bad}(s)$ holds.

(b) Proving inductive properties using satisfiability solving.
Recall that the formula $\psi_1 = \mathit{Init}(s) \rightarrow \neg \mathit{Bad}(s)$ is valid if there is no initial state for which Bad holds. Write a formula ψ_2 that is valid if and only if all transitions from states where $\neg \mathit{Bad}$ holds lead to states where $\neg \mathit{Bad}$ holds.

(i) If ψ_1 is valid and ψ_2 is valid, can we conclude that $\neg \mathit{Bad}$ holds for all reachable states?

(ii) How can we use a SAT solver to check validity of ψ_1 and ψ_2?