

**Problem 1.1.** Bounded model checking is a symbolic algorithm used in practice to find bugs in systems. In contrast to reachability, which checks if the target is reached in *some* (unspecified) number of steps, the bounded model checking algorithm checks if the target is reached within a fixed  $k$  number of steps. Fix a constant  $k$  for the bound. Given a symbolic representation of a Boolean program with initial states  $Init(X)$ , transition relation  $T(X, X')$ , target states  $Target(X)$ , show how you can write a Boolean formula  $\phi$  such that  $\phi$  is satisfiable iff there is a path from  $Init$  to  $Target$  of length at most  $k$ .

**Problem 1.2.** Express the following property in CTL: from every state of the system, there is a way to eventually bring the system to an initial state (assume you have a proposition  $init$  expressing that a state is initial).

Express the property “on every path the proposition  $p$  is true infinitely many times” in CTL. This property can be used to specify the useful property that a server does not “hang”.

Consider the property “there is a path on which the proposition  $p$  is true infinitely many times.” Argue why the formula  $\exists\Box\exists\Diamond p$  does not capture the intent of the property. It is known that this property *cannot* be expressed by any formula in CTL.

**Problem 1.3.** Does the accessibility property

$$\forall\Box(pc_1 = \text{req} \rightarrow \forall\Diamond(pc_1 = \text{in}))$$

hold the Peterson’s protocol? (If so, give an informal but precise argument why. If not, argue why not and give an explicit counterexample.)

Express the following *finite accessibility property* in CTL: if process 1 is requesting to go to the critical section, then process 1 can go to the critical section after at most one entry of process 2 to the critical section.

**Problem 1.4.** In this problem, we explore *abstract reachability analysis*. Let  $\mathcal{S} = (X, X_0, \{\cdot\}, \rightarrow)$  be a (not necessarily finite) system. Let  $\equiv$  be an equivalence relation on  $X$ . For a state  $s \in X$ , we write  $[s]$  for the equivalence class of  $s$ , and for a set  $X' \subseteq X$ , we write  $[X'] = \{[s] \mid s \in X'\}$ . Define the

quotient system  $\mathcal{S}_{\equiv} = (X_{\equiv}, X_{0,\equiv}, \{\cdot\}, \rightarrow_{\equiv})$  as follows:  $X_{\equiv} = \{[s] \mid s \in X\}$  is the set of equivalence classes of  $\equiv$ ,  $X_{0,\equiv} = \{[s] \mid s \in X_0\}$ ,  $[s] \rightarrow_{\equiv} [t]$  if  $s \rightarrow t$  for every  $s, t \in X$ .

Let  $X^T \subseteq X$ . Show that for every system  $\mathcal{S}$  and every equivalence relation  $\equiv$ , if  $X^T$  is reachable in  $\mathcal{S}$  then  $[X^T]$  is reachable in  $\mathcal{S}_{\equiv}$ . Show by example that the converse of this result may not be true. The above result is useful in its contrapositive form: if  $[X^T]$  is *not* reachable in  $\mathcal{S}_{\equiv}$ , it is not reachable in  $\mathcal{S}$ .

In general, reachability analysis on  $\mathcal{S}$  may not terminate. Can you give a condition on  $\equiv$  so that reachability analysis on  $\mathcal{S}_{\equiv}$  is guaranteed to terminate?

An equivalence relation is *stable* if for every equivalence class  $S$  of  $\equiv$ , we have that  $pre(S)$  is a union of equivalence classes of  $\equiv$ . Show that for any system  $\mathcal{S}$  and stable equivalence relation  $\equiv$ , if  $X_{0,\equiv}$  and  $X^T$  are each unions of equivalence classes of  $\equiv$ , then  $X^T$  is reachable in  $\mathcal{S}$  iff  $[X^T]$  is reachable in  $\mathcal{S}_{\equiv}$ .