

Some problems for CS181u

Problem Symbolic Execution. Consider the code shown here.

```
0.  foo(int x, int y){
1.      if(x > y){
2.          z = x - y;
3.      } else {
4.          z = y - x;
5.      }
6.      if(z < 0){
7.          assert(false);
8.      }
9. }
```

Complete the following:

- i. Let X , Y , and Z be symbolic values representing x , y , and z . Draw the symbolic execution tree that results from symbolically executing `foo(X,Y)`.
- ii. According to your symbolic execution tree, is it possible for there to be an assertion violation? If yes, provide concrete values of x and y that would cause the error. (Assume that we think of x and y as infinite precision integers. I.e. there is no integer overflow.)

Problem Symbolic Model Checking. Consider the transition system $\mathcal{M} = (S, R, I)$:

- $S = \{0, 1\}$ is the set of states,
- $I = \{0\}$ is the set of initial states,
- $R = \{(0, 1), (1, 0)\}$ defines the transition relation,
- $AP = \{p\}$ is the set of atomic propositions, and
- L is the labeling function with $L(0) = \emptyset$, and $L(1) = \{p\}$.

Let's use a single boolean variable x to encode the states of this transition system.

- State 0: $\neg x$
- State 1: x

Complete the following:

- Draw the transition diagram for \mathcal{M} .
- Write a Boolean logic formula for the set of states that correspond to property p .
- Write a Boolean logic formula that represents the transition relation R using the variable x and a new variable x' which represents the “next state”.
- Draw the reduced ordered binary decision diagram (ROBDD) for the transition relation R . Use variable ordering x, x' .

- v. Recall that for a property ϕ and symbolic transition relation R , we can compute $EX \phi$ using the equivalence

$$EX \phi \equiv \exists V' : R \wedge \phi[V'/V]$$

where V' is the set of “next state” variables and $\phi[V'/V]$ indicates replacing variables V with V' in ϕ .

Write an expression for $EX p$ involving existential quantification, variables x and x' , and the expressions for p (from problem ii.) and R (from problem iii.), by applying the logical equivalence given above.

- vi. Recall that for a formula f and variable v' , we can get rid of v' in the expression $\exists v' : f$ using the

$$\exists v : f \equiv f[F/v'] \vee f[T/v']$$

Compute $EX p$ using your expression from problem (v.) by applying the equivalence and simplifying.

- vii. The result of problem (vi.) should be a Boolean formula with a single variable x that corresponds to the set of states satisfying $EX p$. Which states (i.e. state numbers) from the original transition system does this expression encode?

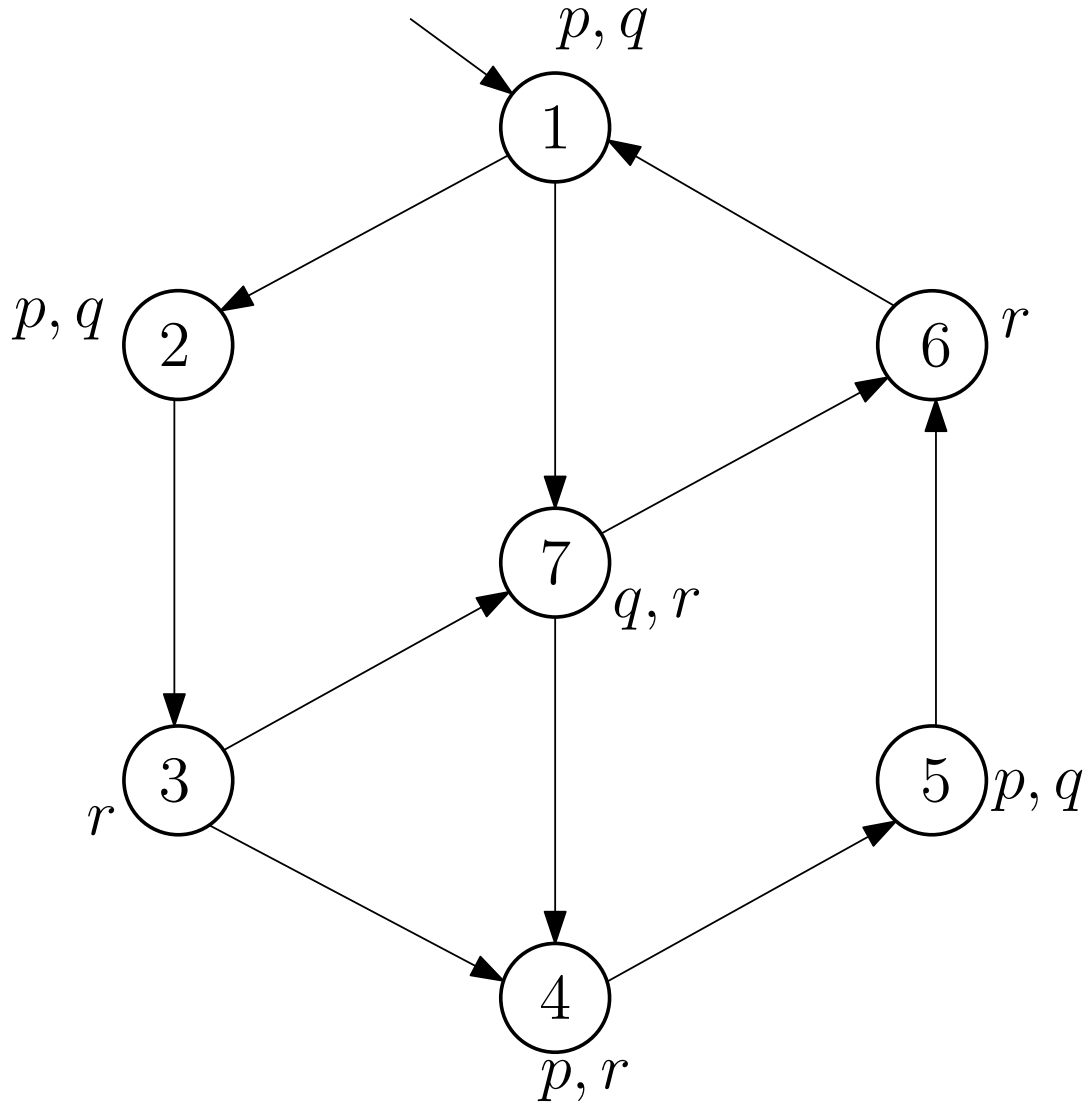
- viii. Does $\mathcal{M} \models EX p$? (yes or no)

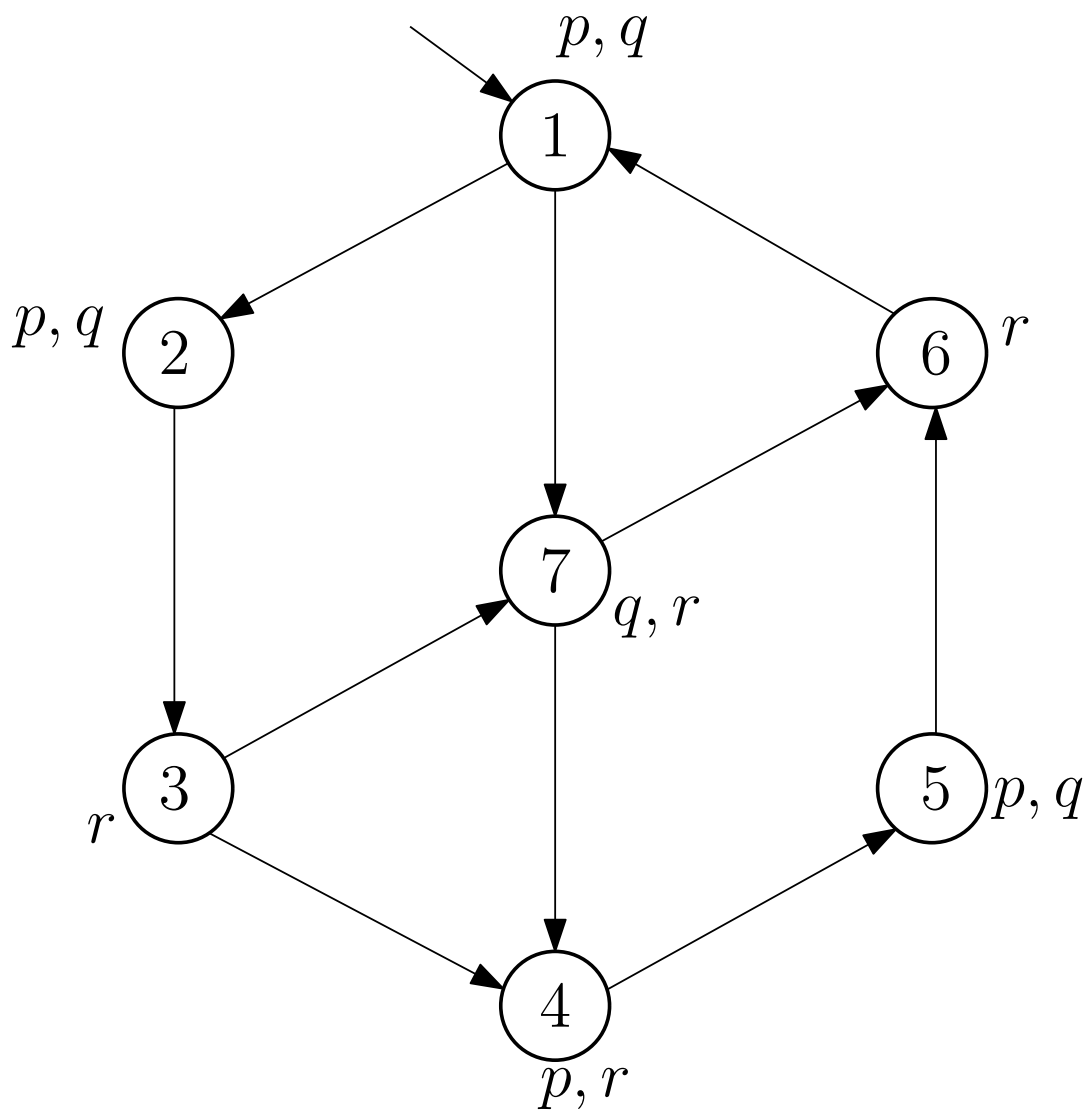
Problem Temporal Logic for Transition Systems. The following problems cover transition systems, CTL, and LTL.

Which of the specifications in plain English below convey the mathematical meaning of the CTL formula $AG (p \rightarrow (q \text{ AU } r))$? Circle a single correct answer.

- a. Any reachable state in which p is true has a path from it on which r is eventually true, and until then q is true.
- b. If p is true in every reachable state, then there is a path along which q holds, until r becomes true.
- c. If p holds in every reachable state, then for any path along which q holds continuously, r becomes true.
- d. For any reachable state in which p is true, then, on any path from that state, q holds until r becomes true, and r is guaranteed to become true eventually.
- e. If p is true in every reachable state, then on every path there is a state at which r is true, and q is true until then.

Problem CTL Model Checking (20 points). Consider the transition system, \mathcal{M} , shown here, with atomic propositions $AP = \{p, q, r\}$. Use the CTL model checking algorithm to determine if $\mathcal{M} \models \phi$, where $\phi = \neg EG (p EU \neg q)$. Show your work by numbering your steps as you label nodes of the diagram. The transition system is given twice in case you would like to illustrate your steps in two separate phases.





Problem Büchi Automata for LTL Formulas (25 points). Recall that any LTL formula can be associated with a Büchi Automaton. Assuming that set of atomic propositions AP is $\{p, q\}$, label each of the given Büchi Automata with its corresponding LTL formula from the provided list. Each formula should correspond to exactly one automaton.

a. $F p$

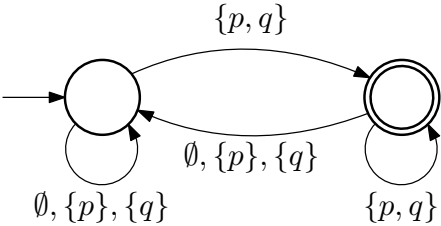
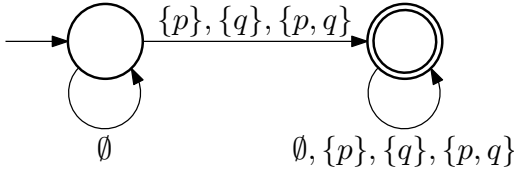
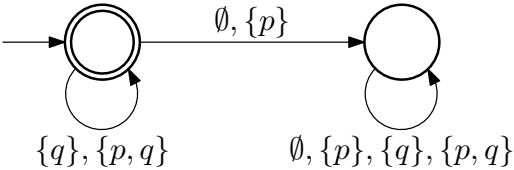
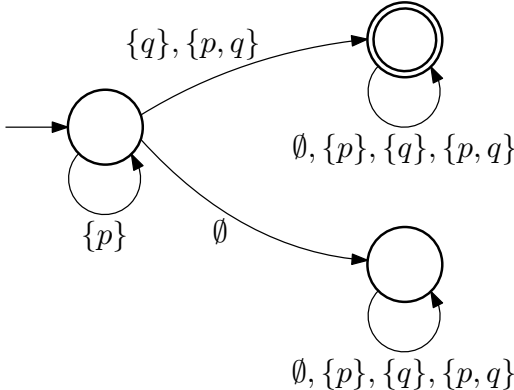
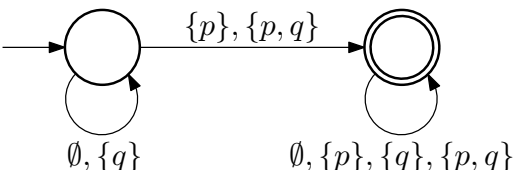
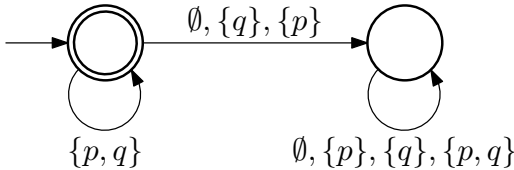
c. $G (p \wedge q)$

e. $p U q$

b. $G q$

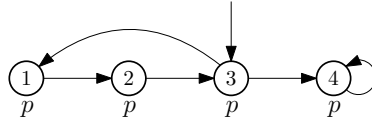
d. $F (p \vee q)$

f. $G F (p \wedge q)$

 <p>Your answer: _____</p>	 <p>Your answer: _____</p>
 <p>Your answer: _____</p>	 <p>Your answer: _____</p>
 <p>Your answer: _____</p>	 <p>Your answer: _____</p>

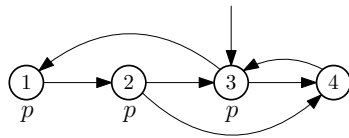
Problem CTL Properties. 16 points total (1 point each). For each transition system, determine if each of the four computation tree logic (CTL) properties hold (yes / no).

A.



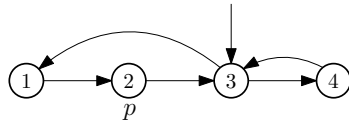
- i. $AG\ p$ _____ ii. $EG\ p$ _____ iii. $AF\ p$ _____ iv. $EF\ p$ _____

B.



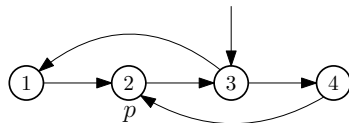
- i. $AG\ p$ _____ ii. $EG\ p$ _____ iii. $AF\ p$ _____ iv. $EF\ p$ _____

C.



- i. $AG\ p$ _____ ii. $EG\ p$ _____ iii. $AF\ p$ _____ iv. $EF\ p$ _____

D.



- i. $AG\ p$ _____ ii. $EG\ p$ _____ iii. $AF\ p$ _____ iv. $EF\ p$ _____