Formal Methods
Tutorial 7
Program Verification, Timed Automata, CTL

Department of Computer Science & Engineering,
Indian Institute of Technology, Kharagpur

1. Compute the Weakest Precondition for the following code snippets, given the postcondition:

   1.1 Code Snippet 1:

   ```
   a := 2*(b-1)-1
   {a>0}
   ```

   1.2 Code Snippet 2:

   ```
   a := a+2*b-1
   {a>1}
   ```

   1.3 Code Snippet 3:

   ```
   a := 2*b+1
   b := a-3
   {b < 0}
   ```

1.4 Code Snippet 4:

```
a := 3*(2*b+a)
b := 2*a-1
{b>5}
```

1.5 Code Snippet 5:

```
if(a==b)
    b=2*a+1;
else
    b=2*a;
{b>1}
```

2. (Timed Automata) Model an automatic door.
   The door has a sensor that detects that a person is approaching it. When it detects that a person is approaching, the sensor asserts the `open` signal. The door has a delay of 1 second before it responds. It then takes another 2 seconds to open. It is assumed that a person takes 5 seconds to cross the door after the person is sensed. The door must remain open during this time. If no person is sensed, the door closes after the stipulated time. The door takes 2 seconds to close. If the door is open or hasn't closed fully, and another person is detected as approaching, the door must open according to the rules mentioned previously.

3. (CTL)

3.1 State the syntax of CTL state and path formulas.

3.2 Write the CTL formula for the following statements

3.2.1 For two resources, $crit_1$ and $crit_2$ can't be simultaneously true.

3.2.2 Each red light phase is preceded by a yellow light phase.

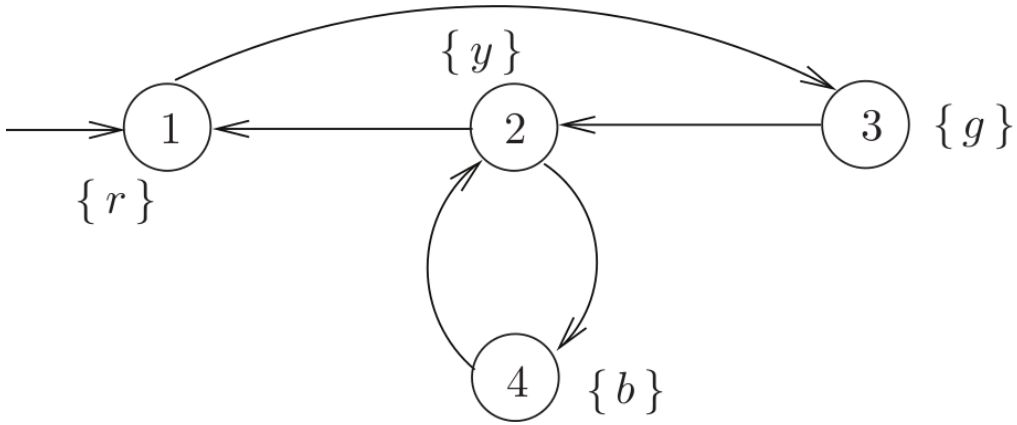
3.2.3 The traffic light is infinitely often green.

3.2.4 Every request will eventually be granted.

3.2.5 The AP *start* is true only in the start states. Express the property, In every reachable state it is possible to return(via 0 or more transitions) to one of the starting states.

3. (CTL contd.)

3.3 Consider the following TS over $AP = \{b, g, r, y\}$, and indicate for each of the following CTL formulae the set of states for which these formulae hold.



3.3.1 $\forall\Diamond y$
3.3.2 $\forall\Box y$
3.3.3 $\forall\Box\forall\Diamond y$
3.3.4 $\forall\Diamond g$
3.3.5 $\exists\Diamond g$
3.3.6 $\exists\Box y$
3.3.7 $\exists\Box\neg g$
3.3.8 $\forall(b \cup \neg b)$
3.3.9 $\exists(b \cup \neg b)$
3.3.10 $\forall(\neg b \cup \exists\Diamond b)$
3.3.11 $\forall(g \cup \forall(y \cup r))$
3.3.12 $\forall(\neg b \cup b)$

3. (CTL contd.)

3.4 Check for the equivalence of each of the formula pairs whether the CTL formula is equivalent to the LTL formula

3.4.1 $\forall\Box\forall \bigcirc a$ and $\Box \bigcirc a$

3.4.2 $\forall\Diamond(a \wedge \exists \bigcirc a)$ and $\Diamond(a \wedge \bigcirc a)$