Quantitative Verification Session 7 - Answers

December 07, 2017

PCTL

Exercise 1.1. Translate the following PCTL formulae to English

1. $send \implies P_{\geq 0.95}\ [\ F^{\leq 10}\ deliver\ ]$
   If a message is sent, then the probability of it being delivered within 10 steps is at least 0.95
2. $P_{\leq 0.05}\ [\ F\ err/total > 0.1\ ]$
   With probability at most 0.05, more than 10% of the NAND gate outputs are erroneous
3. $P_{=?}\ [\ F^{\leq t}\ reply\_count = k\ ]$
   What is the probability that the sender has received k acknowledgements within t clock-ticks?

Exercise 1.2. Translate the following specifications into PCTL formulae

1. The system with two processes satisfy mutual exclusion almost surely ($crit_i$ holds if process i is in the critical section)
   $P_{=1}[G\ \neg(crit_1 \wedge crit_2)]$
2. The probability that every request will eventually be granted with a probability greater than 0.95, is 0.99.
   $P_{=0.99}[G(request \implies P_{\geq 0.95}[F(response)])]$
3. The probability that component B fails before component A is less than 0.4
   $P_{<0.4}[\neg fail_A \cup fail_B]$
4. If the system is not operational, it almost surely reaches a state from which it has a greater than 0.99 chance of staying operational for 100 time units.
   $\neg oper \implies P_{\geq 1}[F(P_{>0.99}[G^{\leq 100} oper])]$

Exercise 2. Here we make the assumption that we want to know whether each of these PCTL formulae hold in the initial state.

- $P_{>0.8}[\neg a \cup FGb]$
  States which satisfy b = States which satisfy $Gb = \{4\}$
  States which satisfy $FGb = \{0, 1, 2, 4, 5\}$
  States which satisfy $a = \{1\}$
  States which satisfy $\neg a = \{0, 2, 3, 4, 5\}$
  $P_{>0.8}[\neg a \cup FGb] \equiv P_s(\{0,2,3,4,5\} \cup \{0,1,2,4,5\}) > 0.8$ – which is true since initial state is also a target state and the constraint is not violated.
- $P_{>0.8}[\neg a \cup^{\leq 3} Gb]$
  States which satisfy $Gb = \{4\}$
  States which satisfy $\neg a = \{0, 2, 3, 4, 5\}$
  $P_{>0.8}[\neg a \cup^{\leq 3} Gb] \equiv P_s(\{0,2,3,4,5\} \cup^{\leq 3} \{4\}) > 0.8$
  You can either perform value iteration for constrained reachability, or else manually list all paths

which reach {4} while staying within {0, 2, 3, 4, 5}. The possible paths are 0-2-4-4, 0-2-2-4, 0-2-5-4. The probability is therefore $0.9 * 0.5 * 1 + 0.9 * 0.1 * 0.5 + 0.9 * 0.3 * 0.7 = 0.684$. Hence the PCTL formula in question is false.

- $P_{>0.8}[\neg a \cup b]$
  Let us do this by solving the constrained reachability equations. We have

$$\begin{aligned} x_0 &= 0.9x_2 \\ x_1 &= 0 \\ x_2 &= 0.1x_2 + 0.3x_5 + 0.5 \\ x_3 &= 0 \\ x_4 &= 1 \\ x_5 &= 0.3x_5 + 0.7 \end{aligned}$$

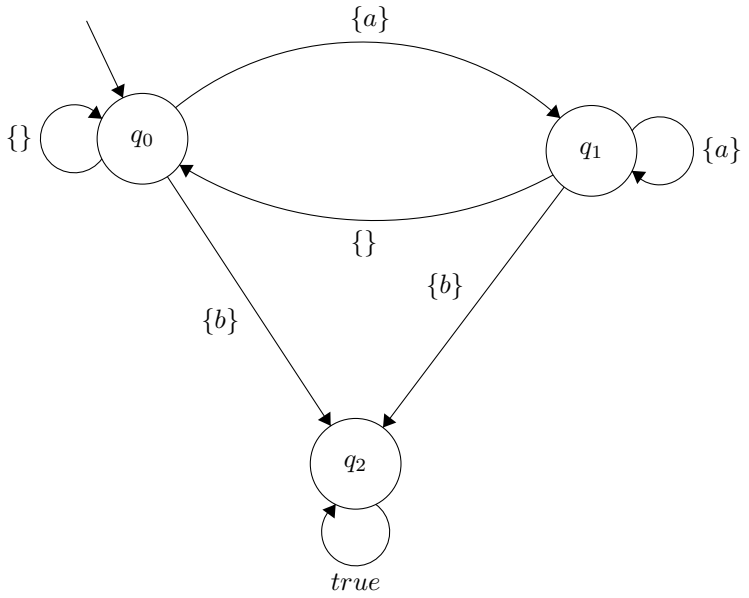
  From this, we get $x_0 = 0.8$, $x_2 = \frac{8}{9}$ and $x_5 = 1$. Since the initial state does not satisfy the formula with a probability > 0.8 (but only $= 0.8$), the answer is false.

PLTL

Exercise 3. Formalize the following specifications as PLTL formulae. You are free to make reasonable assumptions regarding the atomic propositions.

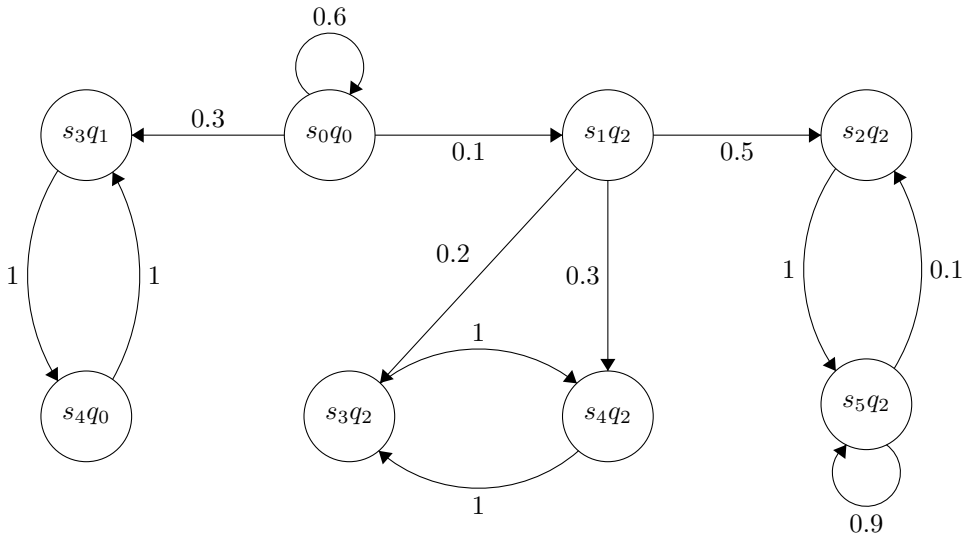
1. With probability 1, the server always eventually returns to a ready-state
   $P_{\geq 1}[GF\ ready]$
2. With probability at most 0.01, an irrecoverable error occurs
   $P_{\leq 0.01}[FG\ error]$

Exercise 4.1. Draw Rabin automata for the following LTL formulae: $\phi = G\neg b \wedge GFa$.



Accepting condition $\{(E_0, F_0)\} = \{(\{\}, \{q_1\})\}$. This means that the automaton accepts a word only if q_1 appears infinitely often.

Exercise 4.2. The Rabin automaton corresponding to the given LTL formula was drawn in *Exercise 4.1.*. Taking the product (as described in the lecture slides) of this Rabin automaton with the DTMC, we get the following DTMC.



The accepting state of this product DTMC is the set of states containing q_1, which is only s_3q_1 in this particular case. The probability of the LTL formula being satisfied is the probability of reaching $s_3q_1 = 0.3 + 0.3 * 0.6 + 0.3 * 0.6^2 + \cdots = 0.3 \times \frac{1}{1-0.6} = \frac{3}{4}$.