COMP3153/9153
Homework 2

SPIN, LTL Model Checking

Due: April 3, 2020, 10am
Submission guidelines are given at the end of this document.

Exercise 1 (LTL) (15 Marks)

Question 1 We extend LTL by an operator $\mathbf{L}^n$ ($n \in \mathbb{N}$), which shall indicate that a formula is true if it occurs at least n-times on a path ρ. Formally, we define

$$\begin{aligned} &\rho \models \mathbf{L}^n \phi \\ &\iff \exists k_1 \dots k_n. \left(\rho[k_i] \models \phi \ \wedge \ k_i \neq k_j \ (\text{for } 0 \leqslant i, j \leqslant n \wedge i \neq j) \right). \end{aligned}$$

Prove that this extension is not more powerful than LTL, i.e. show that $\mathbf{L}^n$ can be expressed in terms of standard LTL.

Exercise 2 (Büchi Automata) (25 Marks)

Question 2 Give Büchi automata over the alphabet $\Sigma = \{a, b, c\}$ that accept the following languages.

- $L_1 = \{w \mid w \text{ contains only finitely many } a\text{s and } b\text{s}\}$;
- $L_2 = \{w \mid w \text{ contains the substring } abc \text{ infinitely often}\}$;
- $L_3 = (a + bc)^*((b + c)a^\omega + (abb^*)^\omega)$.

Please try to keep the automata simple. No automaton needs to have more than 10 nodes. You might get negative points if an automaton is too large.

Question 3

- Assume that Figure 1 depicts a finite automaton (finite state machine). Which language is accepted by the automaton?
- Assume that Figure 1 depicts a Büchi automaton. Which language is accepted by the automaton?

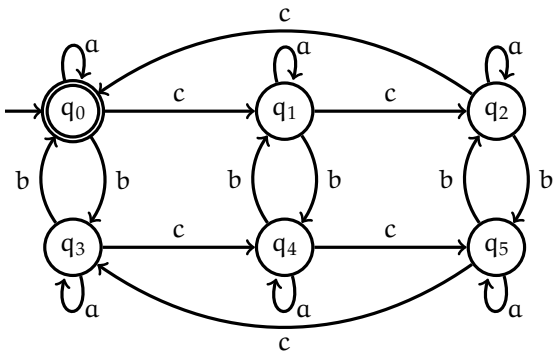

Figure 1: Automaton for Exercise 2

Exercise 3 (LTL Model Checking) (25 Marks)

Question 4 Assume that the set of atomic propositions is $\{p, q\}$. Give a Büchi automaton that accepts the language defined by the following LTL formula:

$$(\mathbf{G}\, p) \vee (p \wedge ((\mathbf{X}\, q) \vee \neg q))$$

Remember that the alphabet is $2^{cl(\Phi)}$, where Φ is the above formula.

There is no need to use the algorithm given in the lecture to derive the automaton; just provide the automaton and explain your answer.

Question 5 Consider two LTL formulae ϕ and ψ. Sketch an algorithm to check if the formulae are equivalent, i.e., $\phi \Longleftrightarrow \psi$.
Note: You can use the objects (e.g., Büchi automata) and algorithms (e.g., check for emptiness) that were presented for LTL model checking.

Exercise 4 (SPIN – Part I) (15 Marks)

The official webpage `http://spinroot.com` provides good overviews and manuals. See e.g. `http://spinroot.com/spin/Man/`.

A SPIN version of Peterson's mutual exclusion algorithm for **two** processes was introduced in Week 3 Friday. The code for the two processes is given here: `http://www.cse.unsw.edu.au/~cs3153/20T1/Week%2003/2Fri/Code.html` under "Third Attempt".

Question 6 Give a SPIN/Promela model for Peterson's algorithm for *three* processes. Briefly describe your algorithm in your own words.
Note: The probability of accessing the critical section should be the same for all processes.

Question 7 Use SPIN to verify the following properties for Peterson's algorithm with three processes:

1. Mutual exclusion: no two processes are in the critical section at the same time.

2. Deadlock freedom.

3. Eventual entry: If any process desires to enter its critical section, it will eventually do so.

Exercise 5 (SPIN – Part II) (20 Marks)

Refer to the Promela specification provided on the course website for a naïve system with two water tanks, modelling only the water levels of the tanks. There is a pump which tries to balance the levels. It succeeds if the water levels are equal.

Question 8 Describe in English words what the processes `Pump` does.

The final goal is to have the same water levels in both tanks. In this case the pump can be turned off.

Question 9 Use SPIN to check if the pump can always be switched off in the given scenario.

Question 10 In case the Pump cannot be switched off, modify the system in a way that the water levels are equal at the end. Prove it.

Question 11 Check whether your system *always* balances out the water levels for all initial water levels. If not modify your system to achieve this. The pump should be switched off as soon as the water levels are equal. Use SPIN to prove it.

Note: If you do experiments with SPIN, describe the procedure, provide the code and discuss SPIN's output. We want to see that you used SPIN and not a pen and paper analysis.

Submission Guidelines

- Due time: April 3, 2020, 10am. **No late submission allowed**.
- Submit one PDF file (`hw2.pdf`) using the CSE `give` system by typing the command `give cs3153 hw2 hw2.pdf` on a CSE terminal. Alternatively use the online submission page.
- It is highly recommended that you use LaTeX to prepare your document. A guide is provided on the course website.
