CSC410

Assignment 5

Due on November 24, 2020 at 11:59pm

Assignment Format and Guidelines on Submission

Submit a properly **typed** PDF on Markus. No handwritten assignment will be accepted. Unless otherwise specified, no English words will be marked.

This assignment will be released gradually in parts. You have the LTL part now. The CTL and model checking parts will be released about a week later, to keep in line with the schedule of the course. You are **strongly advised** to finish the parts that are released early, so that you have time for the remaining parts when they are released. If you do not pace yourself, this will become a big hassle for you near the deadline.

This assignment will be longer than the previous ones. Around 7 problems are planned. Keep in mind that it is designed for a group of 3 or 4 students and you have collectively 20 days to get it done.

List of files to submit:

- `a5.pdf` which will include the cleanly **typed** solutions to the problems.

Problem 1: Symbolic Testing (20 points)

Consider the following function foo

```
1  int foo(int x, int y)
2  {
3      if (x < y) {
4          x = -x ;
5          y = -y;
6      }
7      if (x <= y){
8          x = -x;
9          y = -y;
10     } else{
11         int z = x;
12         x = y;
13         y = z;
14     }
15     assert(x < y);
16 }
```

(a) Enumerate all the paths (regardless of feasibility) in foo where each path is given as a sequence of line numbers (e.g. 3,4,5,10,11,12,18) .

(b) Are all the paths listed above feasible? Prove the paths are not feasible as such by filling instances of a table in the below format (please check tutorial 4 slide 8 and 10 for the format). At the end of each, write a short English description to sum up the result of the table.

Line No.	Assignment	Path Condition

(c) Of all the feasible paths, would any result in an assertion violation? Prove your claim using symbolic execution. Fill in a table in the above format again and conclude your argument using a short English description.

Line No.	Assignment	Path Condition

LTL Problems

Problem 2 (12 points)

Let us assume we have a system with only one observable component: a colour LED light bulb. This light bulb can be of colours white (w), red (r), green (g), and blue (b) when it is on, or it can be off (o). The system changes state every second, and the status of the light accordingly changes (or remains the same). Note that it is assumed that the light is always exactly one colour.

Translate each of the following English specification for this simple system to an LTL formula.

(a) The light bulb turns red exactly once (but it can remain red for any duration).

(b) The light bulb stays on forever, changes colour every second, and alternates between red and white.

(c) The light bulb stays on forever, alternates between colours red, blue, and white (in that order), staying at each colour for an arbitrarily long (non-zero but finite) amount of time.

(d) The light bulb can only turn white if it has been previously at least once blue, once green, and once red (but not necessarily in that order).

Problem 3 (30 points)

Which one of the following equivalences hold? Give a formal proof for the correct ones and provide a counterexample for the incorrect ones. A counterexample is an infinite path that satisfies one side and not the other. You may not use any of the equivalences from the lecture/book as a boost. You are meant to prove these from scratch whenever they hold.

(a) $\varphi \,\mathtt{U}\, \neg\varphi \equiv \mathit{true}$

(b) $(\Diamond\Box\varphi_1) \wedge (\Diamond\Box\varphi_2) \equiv \Diamond(\Box\varphi_1 \wedge \Box\varphi_2)$

(c) $\Box\Diamond\varphi \implies \Box\Diamond\psi \equiv \Box(\varphi \implies \Diamond\psi)$

(d) $\varphi \,\mathtt{U}\, (\psi \vee \neg\varphi) \equiv \Box\varphi \implies \Diamond\psi$

(e) $\bigcirc\Diamond\varphi \equiv \Diamond \bigcirc \varphi$

Problem 4 (10 points)

Recall that satisfiability and validity of LTL formulas are defined in the same way as propositional logic formulas. An LTL formula φ is **satisfiable** if and only if there exists a path π that satisfies it ($\exists\pi : \pi \models \varphi$). An LTL formula φ is valid if and only if all paths π satisfy it ($\forall\pi : \pi \models \varphi$). Note that validity of φ can also be reformulated as the equality $\varphi \equiv \mathit{true}$.

For the formulas below, determine if the formula is satisfiable, unsatisfiable, or valid. Formally justify your answer.

(a) $\Diamond b \implies (a \,\mathtt{U}\, b)$.

(b) $\bigcirc(a \vee \Diamond a) \implies \Diamond a$

CTL Problems

To be released later ...