Concordia University

Department of Computer Science and Software Engineering

SOEN 331-S:

Formal Methods for Software Engineering

Assignment 4

Dr. Constantinos Constantinides, P.Eng.

constantinos.constantinides@concordia.ca

December 2, 2022

Contents

1 General information

Date posted: Tuesday 22 November, 2022.

Date due: Friday, 2 December, 2022, by 23:59.

Weight: 10% of the overall grade.

2 Introduction

You should find one partner and between the two of you should designate a team leader who will submit the assignment electronically. There are **5** problems in this assignment, with a total weight of **100** points.

3 Ground rules

This is an assessment exercise. You may not seek any assistance while expecting to receive credit. **You must work strictly within your team and seek no assistance for this assignment (e.g. from the teaching assistants, fellow classmates and other teams or external help)**. You should **not** discuss the assignment during tutorials. I am available to discuss clarifications in case you need any.

Both partners are expected to work relatively equally on each problem. Accommodating a partner who did not contribute will result in a penalty to both. You cannot give a "free pass" to your partner, with the promise that they will make up by putting more effort in a later assignment.

You must prepare this assignment in LaTeX.

If there is any problem in the team (such as lack of contribution, etc.), the team leader must contact me as soon as the problem appears.

This paragraph refers to Questions 1 - 2: The two binary temporal operators $\mathcal{U}$ and $\mathcal{W}$ are duals as one can be expressed in terms of the other.

1. (10 pts) Find a logically equivalent formula for $\phi \; \mathcal{W} \; \psi$ and provide a short reasoning to support your answer. Represent this equivalence between the two expressions with the appropriate logical connective, and support your reasoning.

2. (10 pts) Find a logically equivalent formula for $\phi \; \mathcal{U} \; \psi$, and provide a short reasoning to support your answer. Represent this equivalence between the two expressions with the appropriate logical connective, and support your reasoning.

3. (10 pts) Answer **either** Part 1 **or** Part 2.

   Part 1: Can we provide a logically equivalent formula for $\phi \; \mathcal{R} \; \psi$ in terms of $\mathcal{W}$? Support your answer.

   Part 2: Find logically equivalent formulas for $\Box\phi$ and $\Diamond\phi$. Do not deploy the duality relationship between the two. Provide a short reasoning to support your answer. Represent this equivalence between the two expressions with the appropriate logical connective.

   This paragraph refers to Questions 4 - 5: Consider a railroad with a single rail and a road level-crossing. We introduce the following propositions that represent events:

   a : A train is **a**pproaching.

   c : A train is **c**rossing.

   l : The **l**ight is blinking.

   b : The **b**arrier is down.

4. (15 pts) Express each of the following requirements formally. For each one, proceed to find a logically equivalent formula that captures the safety property of the system (i.e. in terms of "something bad never happens"):

   (a) (5 pts) When a train is crossing, the barrier must be down.

(b) (5 pts) If a train is approaching or crossing, then the light must be blinking.

(c) (5 pts) If the barrier is up and the light is off, then no train is coming or crossing.

5. (10 pts) Express each of the following requirements formally in terms of the *liveness* property (i.e. in terms of "something good eventually happens"):

   (a) (5 pts) When a train is approaching, it will eventually cross.

   (b) (5 pts) When a train is approaching and no train is crossing, then the barrier will eventually go down before the train crosses.

6. (45 pts) The behavior of a program is expressed by the following temporal formula:

$$\Box \left[\begin{array}{c} \textbf{start} \rightarrow (\phi \oplus \psi) \\ \\ \textbf{start} \rightarrow \tau \\ \\ \phi \rightarrow \bigcirc(\psi \; \mathcal{U} \; \chi) \\ \\ \psi \wedge \tau \rightarrow \bigcirc(\psi \; \mathcal{W} \; \chi) \\ \\ \tau \wedge \bigcirc\psi \rightarrow \bigcirc\omega \\ \\ \psi \wedge \omega \rightarrow \bigcirc^2\chi \\ \\ \omega \wedge \bigcirc^2\chi \rightarrow \bigcirc^2\sigma \\ \\ \psi \wedge \bigcirc\sigma \rightarrow \bigcirc^2\pi \\ \\ \psi \wedge \tau \rightarrow \sigma \; \mathcal{R} \; \pi \\ \\ \phi \wedge \bigcirc\psi \rightarrow \bigcirc^2\chi \end{array} \right]$$

(a) (20 pts) Visualize all models of behavior.

(b) (10 pts) Is the set of requirements satisfiable in *all* models of behavior? Explain why or why not.

(c) (10 pts) In the case where the set of requirements is not satisfiable, what modification(s) to the requirements would you make (you may temporarily assume the role of a stakeholder) in order to achieve satisfiability.

(d) (5 pts) Having resolved any possible conflicts in requirements, specify conditions (models of behavior), if any exist, under which the program can terminate. If none exist, please indicate so.

4 What to submit

You must prepare all your solutions in LaTeX and and produce a single `pdf` file. Name both your .tex and .pdf assignment files after the Concordia id of the person who will submit, e.g. `123456.pdf`, and submit both .tex and .pdf files at the Electronic Assignment Submission portal at

(`https://fis.encs.concordia.ca/eas`)

under **Assignment 4**.

END OF ASSIGNMENT.