LAST (FAMILY) NAME_____

FIRST (GIVEN) NAME_____

STUDENT NUMBER_____

UNIVERSITY OF TORONTO
Faculty of Arts & Science

DECEMBER 2024 EXAMINATION

CSC465H1F and CSC2104H1F
Formal Methods of Software Design

Duration: 2 hours

Aids allowed: one letter-sized page, both sides
and the laws from the textbook, 14 pages

Exam Reminders:

- State your name and student number on the top of this page and on the front of the answer booklet. All answers are written in the answer booklet, not on the question page.
- Do not begin writing the exam until the announcements have ended and the exam facilitator has started the exam.
- As a student, you help create a fair and inclusive writing environment. If you possess an unauthorized aid during an exam, you may be charged with an academic offence.
- Turn off and place all cell phones, smart watches, electronic devices, and unauthorized study materials in your bag under your desk. If it is left in your pocket, it may be an academic offence.
- When you are done your exam, raise your hand for someone to come and collect your exam. Do not collect your bag and jacket before your exam is handed in.
- If you are feeling ill and unable to finish your exam, please bring it to the attention of an exam facilitator so it can be recorded before leaving the exam hall.
- In the event of a fire alarm, do not check your cell phone when escorted outside.

Exam Format and Grading Scheme:
There is 1 question page, 8 questions, and 100 marks.
The value of each question is indicated in square brackets.
A blank answer is worth about one-third of the marks;
to that, marks will be added for readable and relevant and correct information,
and marks will be subtracted for unreadable or irrelevant or incorrect information.

Students must hand in all examination materials at the end.

start of exam

1[9] Let all variables be binary. Prove the following law of Binary Theory using the proof format of the course, and any laws listed. Do not use the Completion Rule.

$$(a \Rightarrow (p = x)) \wedge (\neg a \Rightarrow p) \;=\; p = (x \vee \neg a)$$

2[9] A list is bitonic if it is monotonic up to some index, and antimonotonic after that. For example, [1; 3; 4; 5; 5; 6; 4; 4; 3] is bitonic. One or both of the segments could be empty, in which case the list is also monotonic or antimonotonic. Express formally that L is bitonic. (You are not being asked to write a program.)

3 Let n be a natural state variable. Is the following specification implementable? Proof required.

(a)[9] $n := n-1$

(b)[9] $n>0 \Rightarrow (n := n-1)$

4[7] Let s and i be integer variables, and let L be a list of integers (not a variable). What is the exact precondition for $s' = \Sigma\, L\, [0;..i']$ to be refined by $(s := s + L\, i.\ \ i := i+1)$?

5 Let s and n be integer variables. Let Q be a specification defined as

$$Q \;=\; s' = s + n \times (n-1)/2$$

(a)[9] Prove the refinement

$$Q \;\Leftarrow\; n := n-1.\ \ s := s+n.\ \ Q$$

(b)[6] Add time according to the recursive measure, replace Q by a timing specification, and reprove the refinement.

6 A theory of widgets is presented in the form of some new syntax and some axioms. An implementation of widgets is written. In a couple of sentences, state:

(a)[6] How do we know whether the theory of widgets is consistent or inconsistent?

(b)[6] How do we know whether the theory of widgets is complete or incomplete?

(c)[6] How do we know whether the implementation of widgets is correct or incorrect?

7 Let u be a binary user's variable. Let a be an old binary implementer's variable. We replace a by a new integer implementer's variable x using the convention (from the C language) that 0 stands for $\bot$ and non-zero integers stand for $\top$.

(a)[3] What is the transformer?

(b)[9] Transform and implement $a := \neg a$.

8 Express the program

$$(x := 1.\ \ x := x+y) \;\|\; (y := 2.\ \ y := x+y)$$

as simply as possible without using assignments, sequential compositions, or concurrent compositions, where t is time, and x and y are

(a)[6] boundary variables and assignment takes time 0 (no proof needed).

(b)[6] interactive variables and assignment takes time 1 (no proof needed).

end of exam