UNIVERSITY OF TORONTO  
Faculty of Arts & Science

DECEMBER 2021 EXAMINATIONS

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:
• Fill out your name and student number on the front of the answer booklet. All answers are 
  written in the answer booklet, not on the question pages.
• Do not begin writing the actual 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 offense.
• 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 
  offense.
• 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, 5 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.

NAME_________________________________________________________

STUDENT NUMBER_____________________________________________

Students must hand in all examination materials at the end.
1[9] Let $x$ be an integer variable. What is the exact precondition for $x'<5$ to be refined by $x': x+(1,2)$?

2 Let $a$, $b$, and $c$ be integer variables. Express each of the following as simply as possible without using sequential or concurrent composition. Ignore time. Prove that your expression is equivalent to the given expression.

(a)[9] $a := a+b. \ b' = a+b. \ c := a+b$

(b)[9] $a := a+b. \ (b := a-b \ || \ a := a-b)$

(c)[9] $\text{if } a > 0 \ \text{then } b := a-1 \ \text{else } \text{ok fi} \ || \ \text{if } a \leq 0 \ \text{then } a := b+1 \ \text{else } \text{ok fi}$

3 Given two natural number variables $x$ and $y$, write a program to find their product $x*y$ using only addition, subtraction, and test for zero, but not multiplication.

(a)[9] Write all specifications and refinements. Ignore time.

(b)[15] Prove your refinements.

4 Let $i$ be an integer variable, and let $P$ be a specification such that

$$P = i := i-1. \ \text{if } i = 0 \ \text{then } i := 3 \ \text{else } P \ \text{fi}$$

(a)[1] Add recursive time.

(b)[15] Using recursive construction, find the weakest fixed-point (weakest solution for $P$), including time. You do not need to prove that recursive construction results in the weakest solution.

5 A theory provides three names: zero, increase, and inquire. It is presented by an implementation. Let $u: \text{bin}$ be the user's variable, and let $v: \text{nat}$ be the implementer's variable. The axioms are

$$\text{zero} = v := 0$$

$$\text{increase} = v := v+1$$

$$\text{inquire} = u := \text{even } v$$

We want to use data transformation to replace $v$ with $w: \text{bin}$.

(a)[9] Is $\top$ a data transformer? Prove.

(b)[15] Regardless whether $\top$ is a transformer or not, use it as a transformer to transform inquire.

end of exam