University of New South Wales
School of Computer Science and Engineering
System Modelling and Design (COMP2111)

FINAL TAKE-HOME EXAM — Term 1, 2022

Instructions:

- This exam has eight questions, for a total of 100 marks.
- **Produce a single PDF of your answers to all questions, with size less than 6MB and entitled "exam.pdf".**
- Submit your work using the `give` web interface, or by running (on a CSE machine): `give cs2111 exam exam.pdf` .
- You must include the following statement in your PDF file:
  I declare that all of the work submitted for this exam is my own work, completed without assistance from anyone else.
- The time allowed is **24 hours**: from **8AM** on Tuesday 10th May to **8AM** on Wednesday 11th May 2022.
- A reference sheet of logical laws is provided for your convenience.
- You must adhere to the UNSW student conduct requirements listed at `https://student.unsw.edu.au/conduct` .
- Every student receives a different version of the exam.
- You can ask questions on Ed during the exam! **Make sure they are private**; I might declassify if they are of general interest. I will check Ed often, except when I sleep. In a pinch, you can also e-mail questions to cs2111@cse.unsw.edu.au.
- Don't leave submission until the last minute—submit early and often! Remember that `give` allows you to resubmit several times before the deadline.

Laws of Boolean Algebra

Associativity	$x \vee (y \vee z) = (x \vee y) \vee z$	$x \wedge (y \wedge z) = (x \wedge y) \wedge z$
Commutativity	$x \vee y = y \vee x$	$x \wedge y = y \wedge x$
Distribution	$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$	$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$
Identity	$x \vee 0 = x$	$x \wedge 1 = x$
Complement	$x \vee x' = 1$	$x \wedge x' = 0$

Derived laws

Idempotence	$x \vee x = x$	$x \wedge x = x$
Annihilation	$x \vee 1 = 1$	$x \wedge 0 = 0$
Double complement	$(x')' = x$	

Inference rules for Hoare Logic

$$\frac{}{\{\varphi[e/x]\}\ x := e\ \{\varphi\}} \quad \text{(ass)}$$

$$\frac{\{\varphi\}\ P\ \{\psi\} \qquad \{\psi\}\ Q\ \{\rho\}}{\{\varphi\}\ P; Q\ \{\rho\}} \quad \text{(seq)}$$

$$\frac{\{\varphi \wedge g\}\ P\ \{\psi\} \qquad \{\varphi \wedge \neg g\}\ Q\ \{\psi\}}{\{\varphi\}\ \textbf{if}\ g\ \textbf{then}\ P\ \textbf{else}\ Q\ \textbf{fi}\ \{\psi\}} \quad \text{(if)}$$

$$\frac{\{\varphi \wedge g\}\ P\ \{\varphi\}}{\{\varphi\}\ \textbf{while}\ g\ \textbf{do}\ P\ \textbf{od}\ \{\varphi \wedge \neg g\}} \quad \text{(loop)}$$

$$\frac{\varphi' \to \varphi \qquad \{\varphi\}\ P\ \{\psi\} \qquad \psi \to \psi'}{\{\varphi'\}\ P\ \{\psi'\}} \quad \text{(cons)}$$

Inference rules for Natural Deduction

$\dfrac{A \quad B}{A \land B}$ (∧-I)	$\dfrac{A}{A \lor B}$ (∨-I1)	$\dfrac{B}{A \lor B}$ (∨-I2)
$\dfrac{A \land B}{A}$ (∧-E1)	$\dfrac{A \land B}{B}$ (∧-E2)	$\dfrac{A \quad \neg A}{\bot}$ (¬-E)
$\dfrac{A \to B \quad A}{B}$ (→-E)	$\dfrac{A \leftrightarrow B \quad A}{B}$ (↔-E1)	$\dfrac{A \leftrightarrow B \quad B}{A}$ (↔-E2)
$\dfrac{A \lor B \quad \begin{matrix}[A] \\ \vdots \\ C\end{matrix} \quad \begin{matrix}[B] \\ \vdots \\ C\end{matrix}}{C}$ (∨-E)	$\dfrac{\begin{matrix}[A] \\ \vdots \\ B\end{matrix}}{A \to B}$ (→-I)	$\dfrac{\begin{matrix}[A] \\ \vdots \\ B\end{matrix} \quad \begin{matrix}[B] \\ \vdots \\ A\end{matrix}}{A \leftrightarrow B}$ (↔-I)
$\dfrac{\begin{matrix}[A] \\ \vdots \\ \bot\end{matrix}}{\neg A}$ (¬-I)	$\dfrac{\begin{matrix}[\neg A] \\ \vdots \\ \bot\end{matrix}}{A}$ (IP)	$\dfrac{\bot}{A}$ (X)

$\dfrac{}{a = a}$ (=-I)	$\dfrac{a = b \quad A(a)}{A(b)}$ (=-E1)	$\dfrac{a = b \quad A(b)}{A(a)}$ (=-E2)
$\dfrac{A(c) \quad {\scriptstyle (1,2,3)}}{\forall x A(x)}$ (∀-I)	$\dfrac{A(c) \quad {\scriptstyle (2)}}{\exists x A(x)}$ (∃-I)	$\dfrac{\forall x A(x)}{A(c)}$ (∀-E)
$\dfrac{\exists x A(x) \quad \begin{matrix}[A(c)] \\ \vdots \\ B\end{matrix} \quad {\scriptstyle (1,2,4)}}{B}$ (∃-E)		(1): c is arbitrary (2): x is not free in $A(c)$ (3): c is not free in $A(x)$ (4): c is not free in B

Questions

Each answer should be justified where appropriate, and 2–3 sentences should be sufficient.

Question 1 (5 marks)

Which lambda-calculus term is both a Church number and a Church Boolean?

Question 2 (5 marks)

Consider the following truth table for a propositional formula involving the three variables A, B, C:

A	B	C	φ
F	F	F	T
F	F	T	F
F	T	F	T
F	T	T	F
T	F	F	F
T	F	T	T
T	T	F	F
T	T	T	T

Give a conjunctive normal form (CNF) formula that has the same truth table as φ.

Question 3 (10 marks)

Given a binary relation $R \subseteq E \times E$, the *reflexive and transitive closure of* R, written R^*, is defined inductively by the following rules:

$$\frac{x \in E}{x\ R^*\ x} \qquad\qquad \frac{x\ R\ y \qquad y\ R^*\ z}{x\ R^*\ z}$$

Prove that $(R^*)^* \subseteq R^*$.

Hint: This will almost certainly require an induction. But induction on what?

Question 4 (5 marks)

Prove using natural deduction that the following holds:

$$\vdash \quad B \rightarrow \neg\neg B$$

Use only the basic rules (these are the ones given in the preamble), and none of the derived rules. In particular, don't use the double negation elimination (DNE) rule.

Question 5 (10 marks)

Consider a vocabulary consisting of the binary predicate symbol $<$ and the constant symbols 0 and 1. For each of the following, give a sentence in predicate logic over this vocabulary that...

(a) ...is false in every model. (2 marks)

(b) ...is true iff the domain of discourse has more than two elements. (4 marks)

(c) ...is true in the standard model of the integers, but not in the standard model of the real numbers. (4 marks)

Question 6 (20 marks)

We want to write a program in $\mathcal{L}^+$ that shuffles the values of three variables x, y, z. Like shuffling a deck of cards, except 52 of them would get too tedious. It has the following requirements:

1. The final values of the variables x, y, z must be a permutation of the initial values.
2. Every permutation of the initial values must be a possible result of running the program.
3. No auxiliary variables other than x, y, z should be used. Instead, assume there is a command $\textbf{swap}(a, b)$, that atomically swaps the values of the variables a and b.

(a) Write a program P in $\mathcal{L}^+$ that meets all of these requirements. (4 marks)

(b) Write a Hoare triple that captures the first requirement above. (4 marks)

(c) Let P be the program you wrote in (a). Show that if it holds that

$$\models \{\varphi\}\ P\ \{\psi\}$$

then it must also hold that

$$\models \{\varphi\}\ \mathsf{skip}\ \{\psi\}$$

(4 marks)

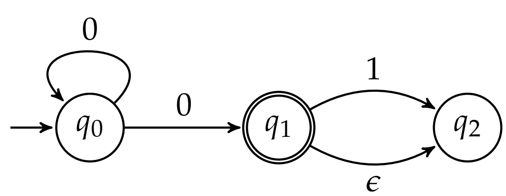
Hint: you don't need to use the Hoare logic inference rules for this question; reasoning about the semantics of Hoare triples should suffice.

(d) Based on your answer to (c), show that the second requirement cannot be expressed with a Hoare triple. (4 marks)

(e) Let P the program you wrote in (a). Write a logical proposition about the relation $[\![P]\!]$ that captures the first requirement. (4 marks)

Question 7 (20 marks)

Consider the following NFA.



Follow the subset construction method to make an equivalent DFA. You may (but don't have to) make a picture; instead, answer the following questions about it:

(a) Which states are reachable from the initial state $\{q_0\}$ in your DFA? (4 marks)

(b) Which states are accepting in your DFA? (4 marks)

(c) If we remove the unreachable states from the DFA, is the resulting DFA minimal? [1] Explain why if so; otherwise, explain how a smaller but equivalent DFA can be constructed. (4 marks)

(d) Give a regular expression whose language is the same as the above NFA. (4 marks)

(e) Every regular language is accepted by a unique minimal DFA. Is there such a thing as a *maximal* DFA that accepts a given regular language? Explain your answer. (4 marks)

Question 8 (25 marks)

The following transition system models a particular program with four variables: two Boolean variables a, b and two natural-number variables y, z.

The states are functions from variable names to values. The transitions are given by the following rules. First, a and b can be set to false at any time:

$$\frac{}{s \longrightarrow s[a \mapsto \bot]}\ (1) \qquad \frac{}{s \longrightarrow s[b \mapsto \bot]}\ (2)$$

a can be set to true, but only if y is currently smaller than z. Similar constraints apply to when b may be set to true.

$$\frac{s(y) < s(z)}{s \longrightarrow s[a \mapsto \top]}\ (3) \qquad \frac{s(z) < s(y)}{s \longrightarrow s[b \mapsto \top]}\ (4)$$

If a (resp. b) is currently false, y (resp. z) can be assigned any number larger than z (resp. y).

$$\frac{s(a) = \bot \qquad s(z) < n}{s \longrightarrow s[y \mapsto n]}\ (5) \qquad \frac{s(b) = \bot \qquad s(y) < n}{s \longrightarrow s[z \mapsto n]}\ (6)$$

The initial state is one where y, z are both 0, and a, b are both false.

[1] Minimal with respect to the number of states. So in other words: is there a DFA with fewer states that accepts the same language?

The goal is to prove that from the initial state, we cannot reach a state where both a and b are true at the same time.

(a) $\neg a \vee \neg b$ is *not* a preserved invariant. Which of the transitions (1)–(6) can cause this candidate invariant to be violated? (5 marks)

(b) Give a preserved invariant that implies $\neg a \vee \neg b$. (5 marks)

Hint: when a is true, what must be true about the other variables? Also, same question but for b.

(c) Briefly explain why your invariant is true in the initial state. (5 marks)

(d) Explain briefly why each of the rules (1)–(6) maintain your invariant. (5 marks)

(e) Are the above questions asking you to prove a safety property, or a liveness property? Explain. (5 marks)

Dont forget to submit your work and include the statement given on the front page.

— END OF EXAM —