McMaster University
Department of Computing and Software
Musa Al-hassy

COMP SCI 3EA3 — Software Specification and Correctness

January 30, 2017

Name _____ Student Number _____

Special Instructions:

- This examination paper includes 4 pages (including this cover page) and 6 questions.
  You are responsible for ensuring that your copy of the paper is complete. Bring any discrepancy to the attention of your invigilator.
- This is a **closed book** examination.
  No books, notes, texts, calculator or academic aids of any kind are permitted.
- **Read each question completely and carefully** before answering it.
- Answer all questions.
- **In doubt, document!**

Contents

1 How to express oneself? — 6 marks —

1. Give a grammar for *terms*.

2. Give the inductive principle for the type of extended integers,

$$\mathsf{Maybe}_{\mathbb{Z}} ::= \mathbb{Z} \mid \bot$$

—you need not worry about type coercion—

2 ACSL Formalisation — 9 marks —

1. Using

```
/*@ axiomatic Context
{
  logic real join(real x, real y);
  logic real meet(real x, real y);
}
*/
```

as lattice operations over the reals, *specify* the *Golden Rule* in ACSL notation.

```
//@ lemma GR:                                                    ; // FILL IN THE BLANK
```

2. Specify the axioms needed to make `(real , op , e)` into a *monoid* in ACSL notation.

```
/*@ axiomatic MonoidAxioms
{
  logic real e;
  logic real op(real x, real y);

  axiom opAxiom:                                                 ; // FILL IN THE BLANK
  axiom eAxiom:                                                  ; // FILL IN THE BLANK
}
*/
```

3 Erroneous Specfication — 8 marks —

Given the problem

"write a program to calculate the mean of two numbers x and y"

one proposed specfication is

$$\{\ true\ \}\ ?\ \{\ mean = (x + y)/2\ \}$$

1. As *succinctly* as possible, explain why this is a *bad* specification.

2. In the Hoare-triple format, give a correct specification conveying the intended behaviour.

4 Half The Quadrivia — 8 marks —

1. State the "Leibniz rule".

2. Using the "duality principle for lattices" form the dual of the statement $x \sqcap y \sqsubseteq x$ and *simplify* as much as possible.

5 Mental Execution — 8 marks —

Give precondition and postcondition formulae for the following program.

$$\{\ \boxed{!}\ \}\ r, x := 1, 0;\ \textbf{do}\ x \neq B \to r := r \cdot A; x := x + 1\ \textbf{od}\ \{\ \boxed{!}\ \}$$

6 Complete The Proof — 10 marks —

All boxes are worth 1 mark, while the first box of part 2 is worth 4 marks.
Fill in the blank boxes with the appropriate *names* of theorems or properties.

1.

Proving $p \wedge q \equiv q \wedge p$**:**

$p \wedge q$
$=$ { ! }
$p \equiv q \equiv p \vee q$
$=$ { ! , which says $p \equiv q \;\equiv\; q \equiv p$ }
$q \equiv p \equiv p \vee q$
$=$ { ! , which says $p \vee q \;\equiv\; q \vee p$ }
$q \equiv p \equiv q \vee p$
$=$ { ! , again }
$q \wedge p$

2. In an arbitrary lattice $(L, \sqsubseteq, \sqcap, \sqcup)$,

Proving $x \sqcup x = x$**:**

$x \sqcup x$
$=$ { The principle of ! says two items are identical precicely when they share identical ancestors, ie $l = r \equiv (\forall\, a \mid a \in L \bullet l \sqsubseteq a \equiv r \sqsubseteq a)$
So for any a in our lattice, we have
$x \sqcup x \sqsubseteq a$
$=$ { ! }
$x \sqsubseteq a \wedge x \sqsubseteq a$
$=$ { ! }
$x \sqsubseteq a$
hence $x \sqcup x = x$. }
x