McMaster University
Department of Computing and Software
Musa Al-hassy

COMP SCI 3EA3 — Software Specification and Correctness

March 6, 2017

Name _____ Student Number _____

Special Instructions:

- This examination paper includes 5 pages (including this cover page) and 3 questions.
  You are responsible for ensuring that your copy of the paper is complete. Bring any discrepancy to the attention of your invigilator.
- **Read each question completely and carefully** before answering it.
- Answer all questions.
- **In doubt, document!**

Contents

1 Program Construction: integer square root — 10 marks —

Solve for ? in the following triple, for $N : \mathbb{Z}$,

$$\{0 \le N\} \; ? \; \{x^2 \le N < (x+1)^2\}$$

—remember that a such a triple is a theorem and so requires a proof!—

Notice that the non-negative integer square root of N is the largest number below N whose square is also below N:

$$x^2 \le N < (x+1)^2 \quad \equiv \quad x \;=\; (\uparrow\; i : \mathbb{Z} \;|\; i \le N \;\wedge\; i^2 \le N)$$

2 The Devil's In The Details — 10 marks —

The type of all variables in this question is the naturals $\mathbb{N}$.

The previous question mentioned the following fact,

$$x^2 \le N < (x+1)^2 \quad \equiv \quad x = (\uparrow i \mid i \le N \wedge i^2 \le N)$$

This theorem is an instance of the theorem of "local characterisation of integer extrema"; assuming the provisos are satisfied. You may need some of the following properties: for any a, b and c,

$R : i^2 \le N$	—This equivales the above '$i \le N \wedge i^2 \le N$'—
"Assumption"	$0 \le N$
"Square"	$a^2 = a \cdot a$
"Monotonicity of Square"	$a \le b \quad \Rightarrow \quad a^2 \le b^2$
"Absolute Value"	$\mathsf{abs}\, a = a \uparrow -a$
"Expansion"	$\mathsf{abs}\, a \le a^2$
"Transitivity"	$a \ge b \wedge b > c \quad \Rightarrow \quad a > c$

To prove,

1. "R is non-empty": $(\exists i \bullet R)$

Here is the list from the previous page: for any a, b and c,

$R \,:\, i^2 \le N$	
"Assumption"	$0 \le N$
"Square"	$a^2 = a \cdot a$
"Monotonicity of Square"	$a \le b \;\Rightarrow\; a^2 \le b^2$
"Absolute Value"	$\mathsf{abs}\, a = a \uparrow -a$
"Expansion"	$\mathsf{abs}\, a \le a^2$
"Transitivity"	$a \ge b \wedge b > c \;\Rightarrow\; a > c$

2. "R is finite": $(\exists r : \mathbb{N} \bullet \forall i \bullet R \Rightarrow \mathsf{abs}\, i \le r)$

$$\exists r : \mathbb{N} \bullet \forall i \bullet R \Rightarrow \mathsf{abs}\, i \le r$$
$= \{ \quad \}$
$$\exists r : \mathbb{N} \bullet \forall i \bullet i^2 \le N \Rightarrow \mathsf{abs}\, i \le r$$
$= \{ \quad \}$
$$\exists r : \mathbb{N} \bullet \forall i \bullet \mathsf{abs}\, i \le i^2 \le N \Rightarrow \mathsf{abs}\, i \le r$$
$\Leftarrow \{ \quad \}$
$$\forall i \bullet \mathsf{abs}\, i \le i^2 \le N \Rightarrow \mathsf{abs}\, i \le N$$
$\Leftarrow \{ \quad \}$
$$\mathit{true}$$

3. "$\neg R$ is monotonic": by shunting, it suffices to show that for any integers x and y, $\quad x \le y \wedge x^2 > N \;\Rightarrow\; y^2 > N$

3 (Bonus) Contravariant Involutions are Necessarily Unit-Preserving — 6 marks —

In this bonus exercise, we'd like to prove the following properties:

$$-0 = 0 \qquad \frac{1}{1} = 1 \qquad \mathsf{I_n}^* = \mathsf{I_n} \qquad \mathsf{Id}^{-1} = \mathsf{Id} \qquad \mathsf{rev}\ [\,] = [\,]$$

(The third is conjugate-transpose of matrices, after that is inverses of functions, and the last one is reversal on lists.)
Rather than prove each of these results directly, we abstract the settings and prove a unifying result.
Suppose $(M, \oplus, e)$ is a monoid and $\_^{\smile} : M \to M$ is a contravariant involution; that is, for all x and y,

"Involution"	$x^{\smile\smile}$	=	x
"Contravariance"	$(x \oplus y)^{\smile}$	=	$y^{\smile} \oplus x^{\smile}$

Now, we calculate:

Proving $e^{\smile} = e$**:**

$e^{\smile}$
= { ☐ }
$e \oplus e^{\smile}$
= { ☐ }
$e^{\smile\smile} \oplus e^{\smile}$
= { ☐ }
$(e \oplus e^{\smile})^{\smile}$
= { ☐ }
$e^{\smile\smile}$
= { ☐ }
e

The purpose of this exercise is to test your comfort with using an "interface" rather than an "implementation".