McMaster University
Department of Computing and Software
Musa Al-hassy

COMP SCI 3EA3
Quiz 4
Solution Hints

COMP SCI 3EA3 — Software Specification and Correctness

March 6, 2017

Name _____ Student Number _____

Special Instructions:

- This examination paper includes 4 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!**

All the questions are closely related to or directly from the lectures and sheets!

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:

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

Solution Hints:

Using the heuristic of "Deleting a Conjunct" to obtain an invariant,

we can delete the second part then construct an algorithm as is done in class to obtain

$\{\, 0 \le N \,\}$
$x := 0$
$;\{\,\text{Invaraint } 0 \le x \wedge x^2 \le N\,,\ \text{Bound } N - x^2\,\}$
do $(x+1) * (x+1) \le N \to$
  $x := x + 1$
od
$\{\, x^2 \le N < (x+1)^2 \,\}$

Alternatively, deleting the first part and working from there yields the algorithm

$\{\, 0 \le N \,\}$
$x := N$
$;\{\,\text{Invaraint } 0 \le x \wedge N < (x+1)^2\,,\ \text{Bound } x\,\}$
do $x * x > N \to$
  $x := x - 1$
od
$\{\, x^2 \le N < (x+1)^2 \,\}$

Of-course for either of these to be accepted, we would need to exhibit the detailed steps needed to obtain them as presented above, or at least present the associated proof obligations of initialisation, invariance, termination, etc. It would behoove the reader to carry out the details of each derivation!
A more succinct solution would be:

> The integer square root of 'N', as specified in the problem, is the largest integer i in $0..N$ with $i^2 \le N$ and so we may use (dual) theorem "Linear Search" to obtain a program. We construct our program as follows —note that every triple is a theorem and so needs a proof, which is referenced/easily-proved on the side!—
>
> $\{\, 0 \le N \,\}$
> skip
> $;\{\,(\exists \mathsf{X} : \mathbb{Z} \mid \mathsf{X} \le N \wedge \mathsf{X}^2 \le N)\,\}$ ..... skip-rule with $\exists$-Introduction and $0^2 = 0$
> $x := N$
> $;$**do** $\neg(x * x \le N) \to$
> $x := x - 1$
> **od**
> $;\{\, x = (\uparrow\ i : \mathbb{Z} \mid i \le N \wedge i^2 \le N)\,\}$ ..... Linear Search
> skip
> $\{\, x^2 \le N < (x+1)^2 \,\}$ ..... skip-rule with the above given fact
>
> We clean up this proof outline by only keeping the first and last assertions, then we use the fact that skip is the unit of sequencing to remove those and finally use properties of the order on the naturals to rewrite the loop guard; resulting in:

$$\{0 \le N\}\ x := N; \textbf{do}\ x * x > N \to x := x - 1\ \textbf{od}\ \{x^2 \le N < (x+1)^2\}$$

Notice that the top-right algorithm presented above is identical to this last algorithm!
Exercise: realise the integer square root problem more efficiently as an instance of "Binary Search".

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": $(\exists i \bullet R)$

   Solution Hints:

   $$\begin{array}{ll} & \exists i \bullet R \\ = & \quad \{\ \text{definitions}\ \} \\ & \exists i \bullet i^2 \le N \\ \Leftarrow & \quad \{\ \exists\text{-Introduction}\ \} \\ & 0^2 \le N \\ = & \quad \{\ \text{arithmetic : definition of Square and zero of multiplication}\ \} \\ & 0 \le N \end{array}$$

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

   Solution Hints:

   $$\begin{array}{ll} & \exists r : \mathbb{N} \bullet \forall i \bullet R \Rightarrow \mathsf{abs}\, i \le r \\ = & \quad \{\ \text{definitions}\ \} \\ & \exists r : \mathbb{N} \bullet \forall i \bullet i^2 \le N \Rightarrow \mathsf{abs}\, i \le r \\ = & \quad \{\ \text{aiming to make the left-sides of the } \le\text{'s similar, so use Identity of } \wedge \text{ and Expansion}\ \} \\ & \exists r : \mathbb{N} \bullet \forall i \bullet \mathsf{abs}\, i \le i^2 \le N \Rightarrow \mathsf{abs}\, i \le r \\ \Leftarrow & \quad \{\ \text{'}N\text{' looks like a good candidate for '}r\text{', so we strengthen —via } \exists\text{-Introduction— to use it in-place of '}r\text{'}\ \} \\ & \forall i \bullet \mathsf{abs}\, i \le i^2 \le N \Rightarrow \mathsf{abs}\, i \le N \\ \Leftarrow & \quad \{\ \text{Transitivity of order}\ \} \\ & \mathit{true} \end{array}$$

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

   Solution Hints:

   $$\begin{array}{ll} & x \le y \wedge x^2 > N \\ \Rightarrow & \quad \{\ \text{Monotoncity of Square}\ \} \\ & x^2 \le y^2 \wedge x^2 > N \\ = & \quad \{\ \text{Dual order and symmetry of } \wedge\ \} \\ & y^2 \ge x^2 \wedge x^2 > N \\ \Rightarrow & \quad \{\ \text{Transitivity}\ \} \\ & y^2 > N \end{array}$$

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

Solution Hints:

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,

$$\begin{array}{lll} \text{“Involution”} & x^{\smile\smile} & = \ x \\ \text{“Contravariance”} & (x \oplus y)^{\smile} & = \ y^{\smile} \oplus x^{\smile} \end{array}$$

Now, we calculate:

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

$$\begin{array}{ll} & e^{\smile} \\ = & \quad \{ \quad \text{Identity} \quad \} \\ & e \oplus e^{\smile} \\ = & \quad \{ \quad \text{Involution} \quad \} \\ & e^{\smile\smile} \oplus e^{\smile} \\ = & \quad \{ \quad \text{Contravariance} \quad \} \\ & (e \oplus e^{\smile})^{\smile} \\ = & \quad \{ \quad \text{Identity} \quad \} \\ & e^{\smile\smile} \\ = & \quad \{ \quad \text{Involution} \quad \} \\ & e \end{array}$$

Notice that we did not make use of the monoid structure, we really just needed the left identity property.
The purpose of this exercise is to test your comfort with using an “interface” rather than an “implementation”.