McMaster University
Department of Computing and Software
Musa Al-hassy

COMP SCI 3EA3
Quiz 6
Solution Hints

COMP SCI 3EA3 — Software Specification and Correctness

April 03, 2017

Name _____ Student Number _____

Special Instructions:

- This examination paper includes 5 pages (including this cover page) and 2 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 Chop-away the hard stuff! — 5 marks — **2**

2 Replace the difficulties in your life! — 10 marks — **3**

This quiz consists of two main questions to solve one problem: Computing the integer logarithm base-7 of a given integer.

$$\{\ 1 \leq N\ \}\ ?\ \{\ 7^x \leq N < 7^{x+1}\ \}$$

You are asked to do so using the heuristic $(\star)$ "Programming is a *goal-oriented* activity"; where the first question requires the use of the technique of "Deleting a Conjunct" to find the invariant, and the second approach requires you to use the technique of "Replacing Constants/Expressions by Variables" to solve the problem.

Code without an explicit derivation *following* the outline of the ambient heuristic $(\star)$ receives **zero** marks.
You may not use any of the search schemas on the Theorem Sheet.

Besides the usual arithmetical results used in-class, you may need some of the following properties:
for any *natural numbers* a, b, c and d,

"Exponentiation at zero" $a^0 = 1$

"Strict-isotonicity of exponentiation" $b < d \equiv a^b < a^d$
$a < c \equiv a^b < c^b$

"Exponentiation is strictly expansive on the positives" $1 < d \equiv a < a^d$
$1 < a \equiv d < a^d$

"Naturals are discrete" $a < b \equiv a + 1 \leq b$

1 Chop-away the hard stuff! — 5 marks —

Solve the integer log base-7 problem by using the technique of "Deleting a Conjunct" to find the invariant —ambiently using the heuristic of "programming is a *goal-directed* activity" to guide your **derivation**!

$$\{\ 1 \le N\ \}\ ?\ \{\ 7^x \le N < 7^{x+1}\ \}$$

Solution Hints:
We are asked to ensure

$$R: \qquad 7^x \le N\ \wedge\ N < 7^{x+1}$$

The first conjunct is easily-truthified by $x := 0$ while the second is hard to truthify and so we take the former as invariant and the negation of the latter as loop guard. Let us name these pieces and simplify them as well to obtain,

$$P: \qquad 7^x \le N \qquad \text{and} \qquad B: \qquad 7^{x+1} \le N$$

The "P is easily-truthified by $x := 0$" claim is easily proven:

Proving $P[x := 0]$**:**

$P[x := 0]$
$=$ { Definitions }
$7^0 \le N$
$=$ { Arithmetic }
$1 \le N$
$=$ { Given fact about N }
true

By definition we have that $P \wedge \neg B \Rightarrow R$ and so we have the the invariant along with the negation of the loop guard indeed establish the required post-condition.

The next stage of the ambient heuristic is to find a bound function and so we calculate:

$P \wedge B$
$=$ { Definitions }
$7^x \le N\ \wedge\ 7^{x+1} \le N$
$\Rightarrow$ { Weakening and strict-isotonicity of exponentiation }
$7^x < 7^{x+1} \le N$
$=$ { Transitivity and Arithmetic }
$0 < N - 7^x$
$=$ { **define** $bf: N - 7^x$ }
$0 < bf$

Sweet! Now a subtraction can be decreased by decreasing its first argument or increasing its second. Since the first is a constant, we increase the second in the simplest possible fashion: incrementing x by 1. Does the loop-body candidate $x := x + 1$ maintain the invariant? Let's check!

Proving Assuming $P\ \wedge\ B$, we have $P[x := x + 1]$**:**

$P[x := x + 1]$
$=$ { Definitions }
$7^{x+1} \le N$
$=$ { This is just our assumption B }
true

Putting everything together we have the program

$$\{\ 1 \le N\ \}\ x := 0; \textbf{do}\ 7^{x+1} \le N \to x := x + 1\ \textbf{od}\ \{\ 7^x \le N < 7^{x+1}\ \}$$

Notice that this is an instance of Linear Search ;)

2 Replace the difficulties in your life! — 10 marks —

Solve the integer log base-7 problem by using the technique of "Replacing Constants/Expressions by Variables" to find the invariant —ambiently using the heuristic of "programming is a *goal-directed* activity" to guide your **derivation**!

$$\{\ 1 \le N\ \}\ ?\ \{\ 7^x \le N < 7^{x+1}\ \}$$

Solution Hints:
We are asked to ensure

$$R: \qquad 7^x \le N\ \wedge\ N < 7^{x+1}$$

We could almost establish this immediately by taking $x := 0$ for the left conjunct and $x := N$ for the right conjunct. We cannot take two values for a variable and so we resolve this conflict by introducing a new variable in-place of the expression $x+1$ to obtain invariant

$$P: \qquad 7^x \le N\ \wedge\ N < 7^y\ \wedge\ x+1 \le y$$

Moreover, if we additionally have $x+1 = y$ then we have our postcondition and so we take as loop-guard

$$B: \qquad x+1 \neq y$$

We're moving a bit fast, we need to pause and assert that P is initially true. Indeed, it is easily truthified by taking $x, y := 0, N$. Formally,

Proving $P[x, y := 0, N]$**:**

$P[x, y := 0, N]$
= { Definitions }
$7^0 \le N\ \wedge\ N < 7^N\ \wedge\ 0+1 \le N$
= { Exponentiation with zero and identity of addition }
$1 \le N\ \wedge\ N < 7^N\ \wedge\ 1 \le N$
= { Given fact about N and Identity of $\wedge$ }
$N < 7^N$
= { Exponentiation is strictly expansive with $N \ge 1$ }
true

Anyhow, the next stage of the ambient heuristic is to find a bound function and so we calculate:

$P \wedge B$
= { Definitions }
$7^x \le N\ \wedge\ N < 7^y \quad \wedge \quad x+1 \le y \quad \wedge \quad x+1 \neq y$
⇒ { Weakening }
$x+1 \le y \quad \wedge \quad x+1 \neq y$
= { Definition of strict inclusion }
$x+1 < y$
⇒ { Arithmetic and **define** $bf: y - x$ }
$0 < bf$

(Notice that we needed $x+1 \le y$ to make this calculation go through. Had we not placed it in P to begin with, we would adjust P at this point so that the calculation goes through.)

Now a subtraction can be decreased by decreasing its first argument or increasing its second. We can choose to increment x or to decrement y; rather than break symmetry, let us postpone which to choose and simply name the alteration 'm' and it has property $x < m < y$ within the loop-body since there we have $x+2 \le y$.

Does the loop-body candidate $x := m$ maintain the invariant? What should we be assigning to y, if anything at all? Rather than hazard a guess, let us calculate by solving for the *necessary* assignment, call it E. Assuming $P \wedge B$,

$$
\begin{array}{ll}
& P[x, y := m, E] \\
= & \quad \{ \text{ Definitions } \} \\
& 7^m \leq N \ \wedge \ N < 7^E \ \wedge \ m + 1 \leq E \\
= & \quad \{ \text{ For the right-most conjunct,} \\
& \quad \left[\begin{array}{ll} & m + 1 \leq E \\ = & \quad \{ \text{ Integers are discrete } \} \\ & m < E \\ = & \quad \{ \text{ The only expression involving '} m < \cdots \text{' is } \\ & \qquad m < y, \text{ so } \textbf{choose } E \text{ to be } y \ \} \\ & \mathit{true} \end{array} \right. \\
& \quad \text{and Identity of } \wedge \ \} \\
& 7^m \leq N \ \wedge \ N < 7^y \\
= & \quad \{ \text{ The right-conjunct is given in } P; \text{ and Identity of } \wedge \ \} \\
& 7^m \leq N
\end{array}
$$

Hence, the appropriate assignment is $x, y := m, y$, that is $x := m$, and it must be *guarded* by $7^m \leq N$. Perhaps assigning m to y is better and without any guard. Let E be the unknown assignment to x and assume $P \wedge B$, then:

$$
\begin{array}{ll}
& P[x, y := E, m] \\
= & \quad \{ \text{ Definitions } \} \\
& 7^E \leq N \ \wedge \ N < 7^m \ \wedge \ E + 1 \leq m \\
= & \quad \{ \text{ For the right-most conjunct,} \\
& \quad \left[\begin{array}{ll} & E + 1 \leq m \\ = & \quad \{ \text{ Integers are discrete } \} \\ & E < m \\ = & \quad \{ \text{ The only expression involving '} \cdots < m \text{' is } \\ & \qquad x < m, \text{ so } \textbf{choose } E \text{ to be } x \ \} \\ & \mathit{true} \end{array} \right. \\
& \quad \text{and Identity of } \wedge \ \} \\
& 7^x \leq N \ \wedge \ N < 7^m \\
= & \quad \{ \text{ The left-conjunct is given in } P; \text{ and Identity of } \wedge \ \} \\
& N < 7^m
\end{array}
$$

Hence, we have that $y := m$ needs to be guarded by $N < 7^m$.

We have calculated two guarded commands and, by the law of the excluded middle, the disjunction of the guards is always true and so we may put them together in a non-aborting alternative.

It remains to choose a value for m with $x < m < y$ given $x + 2 \leq y$. We choose the average —the natural choice that is symmetric in both x and y. Exercise: $x + 2 \leq y \ \Rightarrow \ x < (x + y) \div 2 < y$. Putting everything together, we have:

$$
\begin{array}{l}
\{ \, 1 \leq N \, \} \\
x, y := 0, N \\
; \textbf{do } \ x + 1 \neq y \ \rightarrow \\
\quad m := (x + y) \div 2 \\
\quad ; \ \textbf{if} \quad 7^m \leq N \quad \rightarrow \quad x := m \\
\qquad [] \quad 7^m > N \quad \rightarrow \quad y := m \\
\qquad \textbf{fi} \\
\ \textbf{od} \\
\{ \, 7^x \leq N < 7^{x+1} \, \}
\end{array}
$$

Notice that this is an instance of Binary Search ;)

Observe that the first algorithm starts with x being 0 and increments x at each iteration, then finishes with x being the integer $\log_7$ of N, and so it takes $\log_7 N$ steps to terminate. Whereas the second algorithm cuts the search space at each iteration and only stops when the space is of size two, and so takes $\log_2 N$ steps to terminate. While logs are asymptotically base-invariant, we have that the first 'linear search' is not only simpler but more efficient than the latter 'binary search' instance!

Binary Search is not *always* better than Linear Search!