Problem set 0

Theodore S. Norvell
6892

September 21, 2017

Q0 Take the "binary search challenge".

Solve the following problem in the language of your choice (e.g. Java, C, or pseudo-code). Don't test your code. Email me your solution.

Input: An array (possibly empty) a of numbers (let's say integers) and a number x. The array is sorted from smallest to largest.

Output: If x occurs in a, any index at which it occurs. If x does not occur in the array, -1.

Your solution should run in time roughly proportional to the log of the length of the array. A strategy to accomplish this goal is to try to eliminate roughly half of the remaining places in the array in each iteration of a loop. For Java you may wish to use this method signature

```
static int search(int x, int[] a)
```

for C/C++, you may wish to use this function signature

```
int search(int x, int *a, int len)
```

Q1 (a) Substitutions. For each of the following expressions, underline the bound occurrences in the following

$$\sum_{i\in\{j,..k\}} f(i) \tag{0}$$

$$\{i \in \{j,..k\} \mid P(i)\} \tag{1}$$

$$\left(\forall i \in \{j,..k\} \cdot i < m^2\right) \tag{2}$$

(b) Perform the following substitutions.

$$\left(\sum_{i\in\{j,..k\}} f(i)\right)[j : j+1] \tag{3}$$

$$\{i \in \{j,..k\} \mid P(i)\}\,[i : i+1] \tag{4}$$

$$\left(\forall i \in \{j,..k\} \cdot i < m^2\right)[m : i] \tag{5}$$

Q2. For each of the following proof outlines, write down all conditions that must be universally true —according to our rules— in order to show the proof-outline to be correct

(a) $\{P\}\ k := k+1\ \{\forall i \in \{0,..k\} \cdot a(i) < b(i)\}$

(b) $\{0 \le x < n\}\ x := x+1\ \{1 \le x \le n\}$

(c)

$$
\begin{array}{l}
\{0 \le i < a.\text{length} \wedge \neg\, (\exists k \in \{0, ..i\} \cdot a(k) = x)\} \\
f := (a(i) = x) \\
\{0 \le i < a.\text{length} \wedge f = (\exists k \in \{0, ..i+1\} \cdot a(k) = x)\} \\
i := i + 1 \\
\{0 \le i \le a.\text{length} \wedge f = (\exists k \in \{0, ..i\} \cdot a(k) = x)\}
\end{array}
$$

Q3. (a) The gcd function enjoys the following properties.

$$\forall x, y \in \mathbb{N} \cdot x < y \Rightarrow \gcd(x, y) = \gcd(x, y - x) \tag{6}$$

$$\forall x, y \in \mathbb{N} \cdot \gcd(x, y) = \gcd(y, x) \tag{7}$$

$$\forall x \in \mathbb{N} \cdot x > 0 \Rightarrow \gcd(x, x) = x \tag{8}$$

Fill in the blanks with assertions that make the outline below correct and verifiable using the rules presented in class. Try to make each assertion as weak as you can.[0] Try to state all assertions as simply as you can. You may assume that a and b hold natural numbers (i.e. nonnegative integers).

$$
\begin{array}{l}
\{P : \qquad\qquad\qquad\qquad\qquad\qquad \} \\
\text{if } b < a \text{ then} \\
\qquad \{Q : \qquad\qquad\qquad\qquad\qquad\qquad \} \\
\qquad a := a - b \\
\text{else} \\
\qquad \{R : \qquad\qquad\qquad\qquad\qquad\qquad \} \\
\qquad b := b - a \\
\text{end if} \\
\{a > 0 \wedge b > 0 \wedge \gcd(a, b) = \gcd(A, B)\}
\end{array}
$$

(b) List all formulae that need to be shown universally true in order to show the proof outline is correct. (Hint: There should be 4.) Check that they are universally true.

(c) Building on part (a), find a loop invariant I that makes the following outline correct:

$$
\begin{array}{l}
\{a = A > 0 \wedge b = B > 0\} \\
\text{skip} \\
\{I : \qquad\qquad\qquad\qquad\qquad\qquad \} \\
\text{while } a \ne b \text{ do} \\
\qquad \{P : \qquad\qquad\qquad\qquad\qquad\qquad \} \\
\qquad \text{if } b < a \text{ then} \\
\qquad\qquad \{Q : \qquad\qquad\qquad\qquad\qquad\qquad \} \\
\qquad\qquad a := a - b \\
\qquad \text{else} \\
\qquad\qquad \{R : \qquad\qquad\qquad\qquad\qquad\qquad \} \\
\qquad\qquad b := b - a \\
\qquad \text{end if} \\
\text{end while} \\
\{a = \gcd(A, B)\}
\end{array}
$$

[0] A condition X is called equivalent to a condition Y if $X = Y$ is universally true. For example $a \le b$ is equivalent to $a = b \vee b > a$. A condition Y is called weaker than a condition X iff $X \Rightarrow Y$ is universally true and they are not equivalent. For example $a \le b$ is weaker than $a < b$.

(d) List all formulae that need to be shown universally true, aside from those you listed in part (b). (Hint: There should be 3.) Check that they are universally true; if they are not, you may need to go back to part (a) and use a stronger P.

Q4. (a) We will say that a proof outline with missing internal assertions is correct if there is some way to fill in the missing assertions that makes the outline correct. Prove the following derived rule:

If $P \Rightarrow R[y : f][x : e]$ is universally true, then $\{P\}\ x := e\ y := f\ \{R\}$ is correct.

(b) More generally:

If $P \Rightarrow R[x_{n-1} : e_{n-1}] \cdots [x_1 : e_1]\,[x_0 : e_0]$ is universally true, then

$$\{P\}\ x_0 := e_0\ x_0 := e_0\ \cdots\ x_{n-1} := e_{n-1}\ \{R\} \text{ is correct.}$$

Apply this rule to determine whether the following proof outline is correct.

$$\{x = X \wedge y = Y\}\ x := x + y\ y := x - y\ x := x - y\ \{x = Y \wedge y = X\}$$

Q5. Were you ever taught to find square roots by hand? In this outline, all variables hold natural numbers. The $\lfloor\rfloor$ function gives the largest integer not larger than its argument. Write down all conditions that must be universally true —according to our rules— in order for the proof-outline below to be correct. You may want to first add additional assertions. Check each of these conditions to see whether they are universally true.

$\{p = X \wedge p < 100^i\}$
$x := 0$
$a := 0$
$\left\{I : a = \lfloor\sqrt{x}\rfloor \wedge p < 100^i \wedge X = x \times 100^i + p\right\}$
while $i \neq 0$ do
  $\{I \wedge i \neq 0\}$
  $i := i - 1$
  $x := 100x + p \operatorname{div} 100^i$
  $p := p \operatorname{mod} 100^i$
  $y := x - 100a^2$
  $d := \max\{b \in \{0, ..10\} \mid b(20a + b) \leq y\}$
  $a := 10a + d$
end while
$\{a = \left\lfloor\sqrt{X}\right\rfloor$

By the way, the algorithm works just as well in bases 2, 4, 8, etc. and so is suitable for a fast hardware implementation. (For the base-2 case, consider 20 as meaning $10 + 10$ and so 100.) The binary case is particularly nice as the line

$$d := \max\{b \in \{0, ..10\} \mid b(20a + b) \leq y\}$$

can be written as

$$d := \textbf{if } 100a + 1 \leq y \textbf{ then } 1 \textbf{ else } 0 \textbf{ end if}$$

Q6. Here are some techniques for showing implications are universally true. In each case the conclusion is that

$$P \Rightarrow Q$$

is universally true. Show that each technique works.

(a) It is sufficient to show that Q is universally true.

(b) Unsatisfiable precondition. It is sufficient to show that P is unsatisfiable[1]

(c) Subsetting the precondition: If P is of the form $P_0 \wedge P_1 \wedge \cdots \wedge P_n$ it is sufficient to show that

$$P' \Rightarrow Q$$

is universally true, where P' is the conjunction of some subset of the conjuncts of P. For example it is sufficient to show

$$P_0 \Rightarrow Q$$

is universally true.

(d) By parts: If Q is of the form $Q = Q_0 \wedge Q_1 \wedge \cdots \wedge Q_n$ it is sufficient to show that

$$P \Rightarrow Q_i$$

is universally true for each i.

[1] Which is equivalent to saying $\neg P$ is universally true..