Problem set 0

Theodore S. Norvell
6892

January 11, 2020

Q0 Binary search.

(a) Solve the following problem in pseudo code. (See my notes on pseudo code for guidelines.)

Input: A sequence (possibly empty) a of integers and an integer 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.

(b) Code your solution in the programing language of your choice. 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)
```

For Python

```
def search( x, a ) :
    ”’ x is an int
        s is a tuple or list of int, sorted from smallest to largest
        returns -1 if x is nowhere in s and otherwise returns an index i such that x[i] == s”’
```

(c) Test your code on a wide variety of inputs including arrays of lengths 0 to 10 with x in a number of positions (e.g. first, last, neither) and where a does not contain x, including where x is bigger than every item in a, smaller than every item in a, and bigger than some and smaller than other.

(d) Did your code pass every test? If so, congratulations. Many professional programmer do not pass this simple test.

(e) If you used a loop above, try again using recursion. If you used recursion, try it again using a loop instead.

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. Proof outline conditions

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)

```
$\{0 \le i < a.\mathrm{length} \land \neg\,(\exists k \in \{0,..i\} \cdot a(k) = x)\}$
$f := (a(i) = x)$
$\{0 \le i < a.\mathrm{length} \land f = (\exists k \in \{0,..i+1\} \cdot a(k) = x)\}$
$i := i+1$
$\{0 \le i \le a.\mathrm{length} \land f = (\exists k \in \{0,..i\} \cdot a(k) = x)\}$
```

(d)

```
$\{A : N > 0\}$
$p, m := 1, a(0)$
$\{B : 1 \le p \le N \land (\forall i \in \{0,..p\} \cdot a(m) \ge a(i))\}$
while $p < N$ do
    $\{C : 1 \le p < N \land (\forall i \in \{0,..p\} \cdot a(m) \ge a(i))\}$
    if $a(p) \ge a(m)$ then
        $\{D : 1 \le p < N \land a(p) \ge a(m) \land (\forall i \in \{0,..p\} \cdot a(m) \ge a(i))\}$
        $m := p$
    end if
    $\{E : 1 \le p < N \land (\forall i \in \{0,..p+1\} \cdot a(m) \ge a(i))\}$
    $p := p+1$
end while
$\{F : \forall i \in \{0,..N\} \cdot a(m) \ge a(i)\}$
```

Q3. GCD

(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 provably correct according to the rules presented in class. Try to make each assertion as weak as you can.[0] Try to state

[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 $a = b \lor b > a$. 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 $a < b$.

all assertions as simply as you can. You may assume that a and b hold natural numbers (i.e. nonnegative integers).

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

(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:

```
{$a = A > 0 \wedge b = B > 0$}
skip
{$I :$                              }
while $a \neq b$ do
      {$P :$                              }
      if $b < a$ then
            {$Q :$                              }
            $a := a - b$
      else
            {$R :$                              }
            $b := b - a$
      end if
end while
{$a = \gcd(A, B)$}
```

(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. Sequences of assignments.

(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 Square roots.

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. (I.e., $(\lfloor x\rfloor = i) \Leftrightarrow (i \le x < i+1)$ for all $x \in \mathbb{R}$ and $i \in \mathbb{Z}$.) 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
    $\{I \wedge i \neq 0\}$
    $i := i - 1$
    $x := 100x + p \operatorname{div} 100^i$
    $p := p \bmod 100^i$
    $y := x - 100a^2$
    $d := \max\{b \in \{0, ..10\} \mid b(20a + b) \le y\}$
    $a := 10a + d$
end while
$\{a = \left\lfloor\sqrt{X}\right\rfloor$
```

By the way, the algorithm works just as well in any base greater than 2. For the base-2 case, replace the 20 with $10 + 10$ and so $100_{(2)}$; then it work for base 2 also. The binary case is particularly nice as the line

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

can be written as

$$d := \textbf{if } 100_{(2)}a + 1 \le y \textbf{ then } 1 \textbf{ else } 0 \textbf{ end if}$$

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 or that

$$P_0 \wedge P_n \Rightarrow Q$$

is universally true.

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