Problem set 0 — my solution

Theodore S. Norvell
6892

September 21, 2017

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

$$\sum_{\underline{i}\in\{j,..k\}} f(\underline{i}) \tag{0}$$
$$\{\underline{i}\in\{j,..k\} \mid P(\underline{i})\} \tag{1}$$
$$\left(\forall \underline{i}\in\{j,..k\}\cdot \underline{i} < m^2\right) \tag{2}$$

(b) Perform the following substitutions.
Solution:

$$\left(\sum_{i\in\{j,..k\}} f(i)\right)[j : j+1] \text{ is } \left(\sum_{i\in\{j+1,..k\}} f(i)\right) \tag{3}$$
$$\{i\in\{j,..k\} \mid P(i)\}\,[i : i+1] \text{ is } \{i\in\{j,..k\} \mid P(i)\} \tag{4}$$
$$\left(\forall i\in\{j,..k\}\cdot i < m^2\right)[m : i] \text{ is } \left(\forall n\in\{j,..k\}\cdot n < i^2\right) \tag{5}$$

Q2. For each of the following proof outlines, write down all conditions that must be universally true —according to our rules— in order for the proof-outline to be correct
(a) $\{P\}\ k := k+1\ \{\forall i\in\{0,..k\}\cdot a(i) < b()\}$

Solution: The proof outline is correct if

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

is universally true.

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

Solution: The proof outline is correct if

$$0 \le x < n \Rightarrow 1 \le x + 1 \le n$$

is universally true —which it is.

(c)

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

Solution: The proof outline is correct if

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

is universally true —which it is— and

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

is universally true —which it obviously is.

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).

[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 $a < b$.

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

Solution: Let I be the postcondition $a > 0 \wedge b > 0 \wedge \gcd(a, b) = \gcd(A, B)$. Q and R are easy to find. We substitute and then simplify using the laws above. To find Q start with $I[a : a - b]$ and then simplify as follows

$$
\begin{array}{cl}
 & I\,[a : a - b] \\
= & \text{Substitute} \\
 & a - b > 0 \wedge b > 0 \wedge \gcd(a - b, b) = \gcd(A, B) \\
= & \text{Add } b \text{ to both sides of } a - b > a. \\
 & a > b \wedge b > 0 \wedge \gcd(a - b, b) = \gcd(A, B) \\
= & \text{Use laws (8) and (6).} \\
 & a > b \wedge b > 0 \wedge \gcd(a, b) = \gcd(A, B)
\end{array}
$$

Use the last line for Q. Clearly $Q \Rightarrow I[a : a - b]$ is universally true since $Q = I[a : a - b]$ is universally true. Furthermore, of all the conditions X such that $X \Rightarrow I[a : a - b]$ is universally true, Q is a weakest one.[1]

Finding R is similar.

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

P needs to be the weakest assertion that implies both $b < a \Rightarrow Q$ and $a \leq b \Rightarrow R$. Which means that P should be equivalent to $(b < a \Rightarrow Q) \wedge (a \leq b \Rightarrow R)$. Let's see if we can simplify this

[1] As proof of this, suppose that $X \Rightarrow I[a : a - b]$ is universally true. Then $X \Rightarrow Q$ is universally true, so either Q is weaker than X or Q is equivalent to X.

$$
\begin{array}{ll}
 & (b < a \Rightarrow Q) \wedge (a \leq b \Rightarrow R) \\
= & \quad \text{expand } Q \text{ and } R \\
 & \quad\quad (b < a \Rightarrow a > b \wedge b > 0 \wedge \gcd(a,b) = \gcd(A,B)) \\
 & \wedge \quad (a \leq b \Rightarrow a > 0 \wedge b > a \wedge \gcd(a,b) = \gcd(A,B)) \\
= & \quad \text{factor out the common part} \\
 & \quad\quad (b < a \Rightarrow a > b \wedge b > 0) \\
 & \wedge \quad (a \leq b \Rightarrow a > 0 \wedge b > a) \\
 & \wedge \quad \gcd(a,b) = \gcd(A,B) \\
= & \quad \text{rewrite the inequations} \\
 & \quad\quad (b < a \Rightarrow a > b > 0) \\
 & \wedge \quad (a \leq b \Rightarrow b > a > 0) \\
 & \wedge \quad \gcd(a,b) = \gcd(A,B) \\
= & \quad \text{simplify the inequations} \\
 & \quad\quad a \neq b \wedge a > 0 \wedge b > 0 \\
 & \wedge \quad \gcd(a,b) = \gcd(A,B)
\end{array}
$$

So P is

$$P : a \neq b \wedge a > 0 \wedge b > 0 \wedge \gcd(a,b) = \gcd(A,B)$$

(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.

Solution:

- $P \wedge b < a \Rightarrow Q$.
- $P \wedge b \geq a \Rightarrow R$
- $Q \Rightarrow I[a : a - b]$
- $R \Rightarrow I[b : b - a]$

By the way P, Q, and R were derived in the solution to part (a), these must be 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
$\{I : a > 0 \wedge b > 0 \wedge \gcd(a, b) = \gcd(A, B)\}$
while $a \neq b$ do
    $\{P : a \neq b \wedge a > 0 \wedge b > 0 \wedge \gcd(a, b) = \gcd(A, B)\}$
    if $b < a$ then
        $\{Q : a > b \wedge b > 0 \wedge \gcd(a, b) = \gcd(A, B)\}$
        $a := a - b$
    else
        $\{R : a > 0 \wedge b > a \wedge \gcd(a, b) = \gcd(A, B)\}$
        $b := b - a$
    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.

Solution: The 3 additional formulae are

- $a = A > 0 \wedge b = B > 0 \Rightarrow I$
- $I \wedge a \neq b \Rightarrow P$
- $I \wedge a = b \Rightarrow a = \gcd(A, B)$

The first is universally true by a one-point law. That the second is universally true is trivial. The third is universally true by one-point and by (8). Let's look at the last one in detail

$$
\begin{array}{ll}
 & I \wedge a = b \\
= & \text{Expand } I. \\
 & a > 0 \wedge b > 0 \wedge \gcd(a, b) = \gcd(A, B) \wedge a = b \\
= & \text{One-point law.} \\
 & a > 0 \wedge \gcd(a, a) = \gcd(A, B) \wedge a = b \\
= & (8) \\
 & a > 0 \wedge a = \gcd(A, B) \wedge a = b \\
\Rightarrow & \\
 & a = \gcd(A, B)
\end{array}
$$

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.

Solution: We put $R[y:f]$ in the middle. Now the assignment rule says that the second triple is correct and the first is correct, if $P \Rightarrow R[y:f][x:e]$ is universally true.

(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.

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

Solution: We need to know if

$$(x = Y \wedge y = X)\,[x : x - y][y : x - y][x : x + y]$$

is implied by $x = X \wedge y = Y$. Doing the substitutions and some algebra we get

$$\begin{aligned}
& (x = Y \wedge y = X)\,[x : x - y][y : x - y][x : x + y] \\
= \quad & \\
& (x - y = Y \wedge y = X)\,[y : x - y][x : x + y] \\
= \quad & \\
& (x - (x - y) = Y \wedge x - y = X)\,[x : x + y] \\
= \quad & \\
& (x + y) - ((x + y) - y) = Y \wedge (x + y) - y = X \\
= \quad & \\
& y = Y \wedge x = X
\end{aligned}$$

which is trivially implied by $x = X \wedge y = Y$.

Q5 Were you ever taught to find square roots by hand? In this outline, all variable are natural numbers. The $\lfloor\rfloor$ function gives the largest integer not larger than its argument. You might want to insert some of the omitted assertions first.[2]

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

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

Solution: Let I be $a = \lfloor\sqrt{x}\rfloor \wedge p < 100^i \wedge X = x \times 100^i + p$
Initialization establishes the invariant if

$$\left(p = X \wedge p < 100^i\right) \Rightarrow I[a : 0][x : 0]$$

is universally true, i.e., if

$$\left(p = X \wedge p < 100^i\right) \Rightarrow \left(0 = \left\lfloor\sqrt{0}\right\rfloor \wedge p < 100^i \wedge X = 0 \times 100^i + p\right)$$

is universally true.

The loop terminates in an acceptable state if

$$I \wedge i = 0 \Rightarrow a = \left\lfloor\sqrt{X}\right\rfloor$$

is universally true.

The loop body starts out right if (as is trivial)

$$I \wedge i \neq 0 \Rightarrow I \wedge i \neq 0$$

[2] As the omitted assertions are omitted, you may wonder what they were. Don't worry, you can always put in the "weakest precondition". The weakest precondition of an assignment $x := e$ with respect to a postcondition Q is just $Q[x : e]$. In this example and the next the omitted assertions are all preconditions of an assignment.

is universally true.

The loop invariant is preserved if it is universally true that

$$
\begin{aligned}
& I \wedge i \neq 0 \\
\Rightarrow\ & I[a : a + 10d] \\
& \quad [d : \max\{b \in \{0, ..10\} \mid b(20a + b) \leq y\}] \\
& \qquad [y : x - 100a^2] \\
& \qquad\quad [p : p \bmod 100^i] \\
& \qquad\qquad [x : 100x + p \operatorname{div} 100^i] \\
& \qquad\qquad\quad [i : i - 1]
\end{aligned}
$$

After making the substitutions, this boils down to the question of whether it is universally true that

$$
\begin{aligned}
& I \wedge i \neq 0 \\
\Rightarrow \quad & 10a + d = \left\lfloor \sqrt{100x + p \operatorname{div} 100^{i-1}} \right\rfloor \\
& \wedge\, p \bmod 100^{i-1} < 100^{i-1} \\
& \wedge\, X = \left(100x + p \operatorname{div} 100^{i-1}\right) \times 100^{i-1} + p \bmod 100^{i-1}
\end{aligned}
$$

where d is $\max\left\{b \in \{0, ..10\} \mid b(20a + b) \leq 100x + p \operatorname{div} 100^{i-1} - 100a^2\right\}$. I won't prove that this is universally true here, since the question didn't ask for proof. However, I'd invite you to prove it yourself.

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.

Solution: If Q is universally true then for any values of the variables $P \Rightarrow Q$ simplifies to $P \Rightarrow$ true and that simplifies to true and so is universally true.

(b) Unsatisfiable precondition. It is sufficient to show that P is unsatisfiable[3]

Solution: If P is unsatisfiable then for any values of the variables $P \Rightarrow Q$ simplifies to false $\Rightarrow Q$ and that simplifies to true and so is universally true.

(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

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

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.

Solution: I'll just consider the case where there are two conjuncts. By shunting $P_0 \wedge P_1 \Rightarrow Q$ can be rewritten as $P_1 \Rightarrow (P_0 \Rightarrow Q)$. If $(P_0 \Rightarrow Q)$ is universally true then $P_1 \Rightarrow (P_0 \Rightarrow Q)$ can be rewritten as $P_1 \Rightarrow$ true, which is clearly 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.

Solution: I'll just consider the case where there are two conjuncts. First let's investigate how P distributes over $Q_0 \wedge Q_1$

$$\begin{aligned} & P \Rightarrow Q_0 \wedge Q_1 \\ = \quad & \\ & \neg P \vee (Q_0 \wedge Q_1) \\ = \quad & \\ & (\neg P \vee Q_0) \wedge (\neg P \vee Q_1) \\ = \quad & \\ & (P \Rightarrow Q_0) \wedge (P \Rightarrow Q_1) \end{aligned}$$

Now if $(P \Rightarrow Q_0)$ is universally true and $(P \Rightarrow Q_1)$ is also universally true, then so is their conjunction and hence $P \Rightarrow Q_0 \wedge Q_1$ is universally true.
