SE 504 (Formal Methods and Models)
Spring 2017
HW #3: Selection
Due: 4pm, Monday, February 27

Recall that if **IF** is the program

$$\textbf{if } B_0 \rightarrow S_0 \; [] \; B_1 \rightarrow S_1 \textbf{ fi}$$

then $\{P\}$ IF $\{Q\} \quad \equiv \quad [P \Rightarrow (B_0 \vee B_1)] \;\wedge\; \{P \wedge B_0\}\; S_0\; \{Q\} \;\wedge\; \{P \wedge B_1\}\; S_1\; \{Q\}$

1. Prove

```
{$P : x = \mathrm{X}$}
if $x <= 0 \;\rightarrow\; skip$
[] $x >= 0 \;\rightarrow\; x := -x$
fi
{$Q : x = -|\mathrm{X}|$}
```

The absolute value function is defined to satisfy this condition:

$$(|z| = z \;\equiv\; z \geq 0) \;\wedge\; (|z| = -z \;\equiv\; z \leq 0)$$

2. Prove

```
{$P : y > x$}
if $y > z \;\rightarrow\; y, z := z, y$
[] $z > x \;\rightarrow\; z, x := x, z$
fi
{$Q : y \leq z \;\vee\; z \leq x$}
```

Hint: By Contrapositive (Gries, 3.61), $[P \;\Rightarrow\; B_0 \vee B_1]$ is equivalent to $[\neg(B_0 \vee B_1) \;\Rightarrow\; \neg P]$

3. Prove

```
{$P : prod = (\prod i \mid 0 \leq i < k \;\wedge\; b.i \neq 0 \;:\; b.i) \;\wedge\; 0 \leq k < \#b$ }
if $b.k = 0 \;\rightarrow\; skip$
[] $b.k \neq 0 \;\rightarrow\; prod := prod * b.k$
fi
{$Q : prod = (\prod i \mid 0 \leq i \leq k \;\wedge\; b.i \neq 0 \;:\; b.i)$}
```

Hint 1: A quantification range such as $0 \leq i \leq n \;\wedge\; R$ can be rewritten as the disjunction $(0 \leq i < n \;\wedge\; R) \vee (i = n \;\wedge\; R)$ (first by rewriting $0 \leq i \leq n$ as $0 \leq i < n \vee i = n$ and then applying (3.46)), after which *Range Split* (8.16) is applicable.

Hint 2: A quantification range of the form $P \wedge R$, where R has no free occurrences of a dummy, can, in some circumstances, be simplified to either P or *false*, the former when R can be determined to be *true* and the latter when R can be determined to be *false*.

4. Prove

```
{$P : y = \mathtt{Y} \ \wedge\ \mathtt{Y} > 0 \ \wedge\ \mathtt{C} = x^y \cdot r$}
**if** isEven.$y$ $\rightarrow$ $x, y := x * x, y$ div 2
[] $\neg$isEven.$y$ $\rightarrow$ $r, y := r * x, y - 1$
**fi**
{$Q : 0 \leq y < \mathtt{Y} \ \wedge\ \mathtt{C} = x^y \cdot r$}
```

In carrying out the proof, you may appeal to the following theorems:

$$[z > 0 \ \Rightarrow\ 0 \leq z \text{ div } 2 < z]$$

$$[\text{isEven}.y \ \equiv\ (2(y \text{ div } 2) = y)]$$

5. Prove

```
{$P \ \wedge\ 0 \leq p < q < \#b$}
**if** $b.p \ \geq\ b.q \ \rightarrow\ p \ :=\ p + 1$
[] $b.p \ \leq\ b.q \ \rightarrow\ q \ :=\ q - 1$
**fi**
{$P \ \wedge\ 0 \leq p \leq q < \#b$}
```

where $P : b.p$ **min** $b.q = (\text{MIN } i \mid 0 \leq i \leq p \ \vee\ q \leq i < \#b \ :\ b.i)$

Note that predicate P corresponds to the statement that the lesser of $b.p$ and $b.q$ is the minimum among all the values that occur in either of the segments $b[0..p]$ or $b[q..\#b)$. (It does *not* say that $b.p$ (respectively, $b.q$) is the minimum among the elements in $b[0..p]$ (respectively, $b[q..\#b)$).)

Also note that while it is not possible to apply Split Off Term (8.23) to a quantification whose range is a disjunction, as here, you can get the effect of doing so by first applying Range Split (either (8.16) or (8.18) works here) to split the quantification into two separate ones, then applying Split Off Term, and then applying Range Split again to merge the two quantifications back into one.

In doing the proof, you may find useful these theorems with respect to the min operator:

1. $(x \leq y) \equiv (x = x$ **min** $y)$ (This serves as a definition of min.)
2. $(x \geq y) \equiv (y = x$ **min** $y)$ (Same as above, but with x and y swapped.)
3. $(x = x$ **min** $y) \vee (y = x$ **min** $y)$ (The minimum of two values is one of them.)
4. $x = x$ **min** x (min is idempotent)