SE 504 (Formal Methods and Models)
Spring 2019
HW #2: Skip, Assignment, and Selection
Due: 5:00pm, Friday Feb. 15

In each of problems 1 and 2, prove the given Hoare Triple. Recall that the Hoare Triple Law for the `skip` command is $\{\mathrm{P}\}\ \text{skip}\ \{\mathrm{Q}\} \equiv [P \Rightarrow Q]$.

1. $\{k > 6\}$ skip $\{k > 6\}$.

2. $\{k > 6\}$ skip $\{k \neq 2\}$.

In each of problems 3 and 4, find the weakest solution to the given "equation". Recall that the weakest solution to $Y : \{Y\}\ x := E\ \{Q\}$ is $Q(x := E)$.

3. $Y : \{Y\}\ x := x - 5\ \{(x + 1) \cdot (x - 3) \leq 0\}$
(Note that $a \cdot b\ \leq\ 0\ \ \equiv\ \ (a \leq 0\ \wedge\ b \geq 0)\ \vee\ (a \geq 0\ \wedge\ b \leq 0)$

4. $Y : \{Y\}\ x, y := x - y, y - x\ \{x \leq y\}$

In Problems 5 and 6, prove the given Hoare Triple. Keep in mind the Hoare Triple law for assignment:

$$\{P\}\ x := E\ \{Q\}\ \equiv\ [P \Rightarrow Q(x := E)]$$

In problem 6, `min` is the operator that yields the smaller of its two operands. (We write it between its two operands, just like other arithmetic operators.) Note that this operation lacks an identity element, but it is associative and commutative, so it serves well as a quantifier as long as the quantification's range is not empty. Also, it may help to recall the **Split off term** (8.23) rule from the text by Gries and Schneider. A slightly more general way to state that rule is

Split off term: Provided $a < b$,

$$(\star i \,|\, a \leq i < b\ :\ P)\ \ =\ \ (\star i \,|\, a \leq i < b - 1\ :\ P)\ \star\ P(i := b - 1)$$

For that matter, we can split off the "first" term rather than the "last"; doing so, we get another version:

$$(\star i \,|\, a \leq i < b\ :\ P)\ \ =\ \ P(i := a)\ \star\ (\star i \,|\, a + 1 \leq i < b\ :\ P)$$

5. $\{\neg z\}\ x, y := x \wedge z, x \vee y\ \{z\ \equiv\ x \wedge y\}$

6. $\{P \wedge 0 \leq i < n\}\ i, x := i - 1, x$ `min` $f.i\ \{P\}$, where $P :\ x = (\min j \mid i < j < n\ :\ f.j)$

Recall that if **IF** is the program

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

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

7. Prove
$\{P : x = \mathrm{X}\}$
if $x >= 0 \ \to \ skip$
$[] \ x <= 0 \ \to \ x := -x$
fi
$\{Q : x = |\mathrm{X}|\}$

The absolute value function is defined to satisfy this condition:

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

8. Prove
$\{P : x > y\}$
if $x > z \ \to \ x, z := z, x$
$[] \ y < z \ \to \ z, y := y, z$
fi
$\{Q : x \leq z \ \vee \ z \leq y\}$

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

9. Prove
$\{P : sum = (\sum i \mid 0 \leq i < k \ \wedge \ b.i > 0 \ : \ b.i) \ \wedge \ 0 \leq k < \#b \ \}$
if $b.k <= 0 \ \to \ skip$
$[] \ b.k >= 0 \ \to \ sum := sum + b.k$
fi
$\{Q : sum = (\sum i \mid 0 \leq i \leq k \ \wedge \ b.i > 0 \ : \ b.i)\}$

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*.

10. Prove
$\{P : y = \mathtt{Y} \ \wedge \ \mathtt{Y} > 0 \ \wedge \ \mathtt{C} = x^y \cdot r\}$
if isEven.$y \ \to \ x, y := x * x, y \text{ div } 2$
$[] \ \neg$isEven.$y \ \to \ r, y := r * x, y - 1$
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:

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

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