SE 504 (Formal Methods and Models)
Spring 2022
HW #3: Proofs of Programs Involving Selection Commands
Due: 5pm, Friday, Feb. 25

Recall that if **IF** is the program **if** $B_0 \rightarrow S_0$ [] $B_1 \rightarrow S_1$ **fi**

then $\{P\}$ IF $\{Q\} \quad \equiv \quad [P \Rightarrow (B_0 \vee B_1)] \ \wedge \ \{P \wedge B_0\}\ S_0\ \{Q\} \ \wedge \ \{P \wedge B_1\}\ S_1\ \{Q\}$
which generalizes in the natural way when **IF** has more than two branches.

1. Prove (where p, q, and r are boolean variables)
$\{r\}$
if $\neg p \ \rightarrow \ skip$
[] $p \ \rightarrow \ r := q$
fi
$\{r \quad \equiv \quad p \Rightarrow q\}$

2. Prove
$\{P : x > y\}$
if $x > z \ \rightarrow \ x, z := z, x$
[] $y < z \ \rightarrow \ z, y := y, z$
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 $[\neg(B_0 \vee B_1) \ \Rightarrow \ \neg P]$

3. Prove
$\{P \ \wedge \ 0 \leq k < \#b\}$
if $b.k \leq 0 \ \rightarrow \ sum, k := sum - b.k, k + 1$
[] $b.k \geq 0 \ \rightarrow \ sum := sum + b.k; k := k + 1$
fi
$\{P\}$

4. Prove
$\{P \ \wedge \ 0 \leq k < \#b\}$
if $b.k \leq 0 \ \rightarrow \ sum := sum - b.k$
[] $b.k \geq 0 \ \rightarrow \ sum := sum + b.k$
fi
$; k := k + 1$
$\{P\}$

where $P : sum = (+i \mid 0 \leq i < k \ : \ |b.i|)$ and where $|x|$ is the absolute value of x, defined as follows:

$$[(|x| = x \ \equiv \ x \geq 0) \ \wedge \ (|x| = -x \ \equiv \ x \leq 0)]$$

Notice that, in Problem 3, the two guarded commands (nested inside the selection command) are different in form, in that one is a multiple assignment and the other is a catenation. Hence, their proofs should not be mirror images of each other.

Notice that, in Problem 4, the program is a catenation of a selection command and an assignment command. Thus, to show that the Hoare Triple is valid you should make use of a catenation law to provide the appropriate postcondition for the selection command.