SE 504 (Formal Methods and Models)
Spring 2020
HW #2: Skip, Assignment, and Selection
Due: 7:20pm, Thursday, Feb. 13

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

1. $\{k < 2\}$ skip $\{k \neq 5\}$.

2. $\{k > 2 \ \wedge \ r \neq 7\}$ skip $\{k > 1 \ \vee \ k < -5\}$.

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 $Q(x := E) \ \wedge \texttt{isDef}.E$.

3. $Y : \{Y\}\ x := x + 4\ \{(x + 2) \cdot (x - 1) \geq 0\}$
(Note that $a \cdot b \ \geq \ 0 \quad \equiv \quad a = 0 \ \vee \ b = 0 \ \vee \ (a > 0 \ \equiv \ b > 0)$.)

4. $Y : \{Y\}\ x, y := x - (3 * y), y - x\ \{x > y\}$

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

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

In problem 6, `max` is the operator that yields the larger 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 $a < b$,

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

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

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

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

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

In each of problems 7-9, calculate an expression E that makes the given Hoare triple valid. Each occurrence of an upper case $\mathtt{C}$ denotes a *rigid variable* (to use the terminology introduced by Gries and Schneider on page 181), not a program variable. Thus, the expression you give as your final answer for E should not include any occurrences of $\mathtt{C}$.

For all these, use the standard technique of proving $[P \Rightarrow Q(x := G)]$ (where P is the precondition, Q is the postcondition, and $x := G$ is the assignment) by assuming the antecedant and showing the consequent while at the same time solving for E. Take advantage of opportunities to make use of the assumption for the purpose of replacing an expression by another expression assumed to be equal to it.

7. $\{y = x^2\}\ x, y := x - 1, y - E\ \{y = x^2\}$

8. $\{\mathtt{C} = m - j\}\ m, j := E, m - j\ \{\mathtt{C} = 2m - j\}$

9. $\{\mathtt{C} = k \cdot m \wedge \mathtt{isEven}.k\}\ k, m := E, 2 * m\ \{\mathtt{C} = k \cdot m\}$

Relevant to the last problem is the theorem $\mathtt{isEven}.r \ \equiv\ (r \ \mathtt{div}\ 2 = r/2)$.

Recall that if **IF** is the program

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

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

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

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

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