SE 504 Formal Methods and Models
HW #3 Spring 2009
Due: Thursday, February 26

1. The Hoare Triple Law for Skip is

$$\{P\}\ \texttt{skip}\ \{Q\}\ \equiv\ [P \Rightarrow Q]$$

Use it to prove $\{x \geq 0 \Rightarrow y < 0\}$ `skip` $\{x > 0 \Rightarrow y \leq 0\}$

In each of problems 2 through 4, find the weakest solution to the given "equation". Recall that the weakest solution to $Y : \{Y\}\ x := E\ \{Q\}$ is $Q(x := E)$.

2. $Y : \{Y\}\ x := x - 1\ \{(x + 1) \cdot (x - 1) = 0\}$

3. $Y : \{Y\}\ x := x + 1\ \{x^2 - 2x - 3 \geq 0\}$

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

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 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 is associative and commutative, so it serves well as a quantifier. 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 $a < b$,

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

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

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

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

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

More on next page...

For each of the following Hoare triples, calculate an expression E that makes it hold. 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 $\mathtt{C}$.

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

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

9. $\{\mathtt{C} = p \cdot q \wedge \mathtt{isEven}.p\}\ p, q := p/2, E\ \{\mathtt{C} = p \cdot q\}$