SE 504 (Formal Methods and Models)
Spring 2019
HW #3: wp, Expression Calculation, Catenation, Selection
Due: 6pm, Friday, March 1

Let S be a program and Q be a predicate (over the state space of S). The expression wp.S.Q (read "weakest precondition of S with respect to Q") refers to the weakest predicate P satisfying the Hoare triple {P} S {Q}. In other words

$$\{P\}\ S\ \{Q\} \ \equiv\ [P \Rightarrow \text{wp}.S.Q]$$

Among the laws pertaining to wp are these:

wp skip law: $[\text{wp}.\textbf{skip}.Q \equiv\ Q]$

wp assignment law: $[\text{wp}.(x := E).Q \equiv\ Q(x := E)]$

wp catenation law: $[\text{wp}.(S_1; S_2).Q \equiv \text{wp}.S_1.(\text{wp}.S_2.Q)]$

The wp catenation law says, in effect, that the weakest solution to $\{?\}\ S_1; S_2\ \{Q\}$ is none other than wp.S_1.R (i.e., the weakest solution to $\{?\}\ S_1\ \{R\}$), where R is wp.S_2.Q (i.e., the weakest solution to $\{?\}\ S_2\ \{Q\}$).

That is, to obtain the weakest precondition for the catenation $S_1; S_2$ (with respect to a post-condition Q), we first find the weakest precondition for S_2 (with respect to Q), which serves as our "intermediate assertion" between S_1 and S_2.

In problems 1-3, simplify the given expression as much as possible. Use the wp laws given above, as well as well-known theorems from arithmetic, algebra, and logic. Regarding Problem 2, note that catenation is associative, meaning that $(S_1; S_2); S_3$ and $S_1; (S_2; S_3)$ are equivalent programs. Problem 3, despite being worded differently, is the same kind of problem as the ones preceding it.

1. $\text{wp}.(i := i - 2 * j;\ j := j + i).(2i \geq j)$

2. $\text{wp}.(y := x - y;\ x := x - y;\ y := y + x).(x = Y\ \wedge\ y = X)$

3. Determine the weakest predicate P that makes this Hoare Triple true:

$$\{P\}\ i := i - 1;\ sum := sum + b.i\ \{sum = (+j \mid i \leq j < \#b\ :\ b.j)\ \wedge\ 0 \leq i \leq \#b\}$$

Continued on next page ...

In each of problems 4 through 6, calculate an expression that, when substituted for E, makes the given Hoare Triple valid. Each occurrence of $\mathtt{C}$ denotes a *rigid variable* (in the terminology of Gries and Schneider), not a program variable. Thus, the expression you give as your answer should not include any occurrences of $\mathtt{C}$. Also, simplify your expression as far as possible by making use of algebra and/or the given pre-condition.

4. $\{y = x^2\}\ x, y := x + 3, y + E\ \{y = x^2 - 5\}$

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

6. $\{P \wedge 0 < m \leq r\}\ q, r := E, r - m\ \{P \wedge r \geq 0\}$, where $P : \mathtt{C} = q \cdot m + r$

The remaining problems involve Hoare Triples whose programs include both a selection command and a catenation of commands.

Recall that if **IF** is the program

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

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

7. Prove
$\{P \ \wedge \ i < \#b\}$
if $b.i \ > \ 0 \ \rightarrow \ sum \ := \ sum + b.i;\ i := i + 1$
$[]\ b.i \ \leq \ 0 \ \rightarrow \ i := i + 1$
fi
$\{P \ \wedge \ i \leq \#b\}$

where $P : 0 \leq i \ \wedge \ sum \ = \ (+j \mid 0 \leq j < i \ \wedge \ b.j > 0 \ : \ b.j)$

Notice that the first branch of the selection command is a catenation of two assignment commands. Thus, in showing that that branch behaves as intended, you must make use of a catenation law.

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

Hint 2: A quantification range of the form $P \wedge R$, where R does not mention a dummy, can, in some circumstances, be simplified to either P or *false*, the former when R can be reduced to *true* and the latter when R can be reduced to *false*.

Hint 3: Theorem (3.84a) tells us that the conjunction $(e = f) \wedge P$ is equivalent to $(e = f) \wedge P'$, where P' is obtained from P by replacing one or more occurrences of e by f. If e is a dummy and f is not, this is one way of getting rid of a dummy in a conjunct. (See Hint 2.)

Continued on next page ...

8. 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 the program is a catenation of a selection command and an assignment command. Thus, to show that the Hoare Triple is valid you must make use of a catenation law.