

SE 504 Formal Methods and Models

HW #4 Spring 2009

Due: Thursday, March 5

Let  $S$  be a program and  $Q$  be a predicate (over the state space of  $S$ ). The expression  $\text{wp}.S.Q$  (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

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

Among the laws pertaining to wp are these:

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

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  $\text{wp}.S_1.R$  (i.e., the weakest solution to  $\{?\} S_1 \{R\}$ ), where  $R$  is  $\text{wp}.S_2.Q$  (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 some postcondition  $Q$ ), 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 4, despite being worded differently, is the same kind of problem as the first three.

1.  $\text{wp}.(i := j - i; j := j + i).(i \leq j)$
2.  $\text{wp}.(y := x - y; x := x - y; y := y + x).(x = Y \wedge y = X)$
3.  $\text{wp}.(x := x - y; x := x * x).(x > 4)$

4. Determine the weakest predicate  $P$  that makes the following true:

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

5. Calculate an expression  $E$  (containing no occurrences of  $A$ ) that makes the following true.

$$\{A = qb + r \wedge b \neq 0\} q := E; r := r - b \{A = qb + r\}$$

In Problems 6 and 7, all variables are of type `int`.

**6.** Prove

```
{P : x < z}
if x < y  → x, y := y, x
[] y < z  → y, z := z, y
fi
{Q : x ≥ y ∨ y ≥ z}
```

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

**7.** Prove

```
{P : y = Y ∧ Y > 0 ∧ C = xy · r}
if even.y  → x, y := x * x, y ÷ 2
[] ¬even.y → r := r * x; y := y - 1
fi
{Q : 0 ≤ y < Y ∧ C = xy · r}
```

In carrying out the proof, you may appeal to the following theorems:

$$[z > 0 \implies 0 \leq z \div 2 < z]$$

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