**Strongest Postconditions, Proof Rules, and Proofs**

*CS 536: Science of Programming, Spring 2021*

Due Wed Mar 24, 11:59 pm

---

**A. Why?**

- $sp(p, S)$ is the most information available about the result of running $S$ when $p$ holds.
- To prove validity of correctness triples, we use a proof system with axioms for atomic statements and rules of inference for compound statements.

**B. Outcomes**

After this homework, you should be able to

- Calculate the strongest postcondition of a loop-free program.
- Compare $sp$ and $wp$ approaches for proving simple programs.
- Verify and generate instances of the partial correctness proof rules.

**Note**

- You can use the looser sense of $\equiv$ from lecture.

**C. Problems [50 points total]**

*Lecture 13: Forward Assignment; Strongest Postconditions [22 points]*

1. [3 points] Give an example of an $S$ such that $\models \{T\} S \{sp(p, S)\}$ but $\not\models_{tot} \{T\} S \{sp(p, S)\}$.

2. [3 points] Syntactically calculate $sp(x = y \land x+y \leq n, \ x := f(x+y); \ y := g(x*y))$. Don't do any arithmetic simplification.

3. [16 = 2*2 + 4*3 points] Below, calculate each $sp$ or $wp$ result syntactically. If logical simplification is asked for, complete the syntactic calculation completely first. Below, $even(x) = x \% 2 = 0$ and $odd(x) = x \% 2 = 1$.

   a. Calculate and then logically simplify $sp(x=2^k, x := x/2)$.
   b. Calculate (but don't simplify) $wp(x := x/2, x = 2^k)$.
   c. Let $S = if\ odd(x)\ then\ x := x+1\ fi$. Calculate and then logically simplify $sp(x=x_0, S)$. Drop $x_0$ as part of the simplification.
   d. Using the same $S$ as in part (c), calculate and logically simplify $wp(S, even(x))$. 
e. Define the names below and calculate (but don’t simplify \( sp(p' \land p, S) \)).

\[
\begin{align*}
S &= \text{if } x < b[M] \text{ then } R := M \text{ else } L := M \text{ fi} \\
p &= L < R-1 \land M = (L+R)/2 \land b[L] \leq x < b[R] \\
p' &= L = L_0 \land R = R_0
\end{align*}
\]

f. For the same \( S \) as in part (e) and with \( p = L < R-1 \land b[L] \leq x < b[R] \), calculate (but don’t simplify) \( wp(S, p) \).

**Lectures 14 - 15: Proof Rules and Proofs pt 1 & 2 [28 points]**

For Problems 4 – 6, Determine the proof rules needed to calculate the predicate(s).

4. **[10 = 5 * 2 points]** Calculate \( p_1, p_2, \) and \( p_3 \) and (give the names and line references for) rules \( r_1 \) and \( r_2 \) in

1. \( \{ p_1 \} k := k+1 \{ x = 2^k \land k \leq n \} \) assignment
2. \( \{ p_2 \} x := x*2 \{ p_1 \} \) assignment
3. \( \{ p_2 \} x := x*2; k := k+1 \{ x = 2^k \land k \leq n \} \) sequence 2, 1
4. \( p \land k < n \rightarrow p_2, \) where \( p = x = 2^k \land k \leq n \) pred logic
5. \( \{ p \land k < n \} x := x*2; k := k+1 \{ p \} \) \( r_1 \)
6. \( \{ \text{inv } p \} \text{ while } k < n \text{ do } x := x*2; k := k+1 \text{ od } \{ p_3 \} \) \( r_2 \)

5. **[6 = 3 * 2 points]** Calculate \( q_1, q_2, \) and rule \( r_1 \) in

1. \( \{ r=X*Y-x*2*y \} y := 2*y \{ r=X*Y-x*y \} \) assignment
2. \( \{ q_1 \} x := x/2 \{ r=X*Y-x*2*y \} \) assignment
3. \( \{ q_1 \} x := x/2; y := 2*y \{ r=X*Y-x*y \} \) sequence 2, 1
4. \( \{ r+y=X*Y-x*y \} r := r+y \{ r=X*Y-x*y \} \) assignment
5. \( \{ q_2 \} x := x-1 \{ r+y=X*Y-x*y \} \) assignment
6. \( \{ q_2 \} x := x-1; r := r+y \{ r=X*Y-x*y \} \) sequence 5, 4
7. \( \{ r=X*Y-x*y \land \text{even}(x) \rightarrow q_1 \} \)

if \( \text{even}(x) \) then \( x := x/2; r := 2*r \)
else \( x := x/2; r := r+y \{ \text{X*Y=r-x*y} \} \)

6. **[12 = 6 * 2 points]** Let \( p_0 = r = r_0 \land x = x_0 \land y = y_0 \). Calculate \( q_1, q_2, q_3, q_4, q_5 \) and rule \( r_1 \) in*

1. \( \{ p_0 \land r=X*Y-x*y \land \text{even}(x) \} x := x/2 \{ q_1 \} \) assignment
2. \( \{ q_1 \} y := 2*y \{ q_2 \} \) assignment
3. \( \{ p_0 \land r=X*Y-x*y \land \text{even}(x) \} x := x/2; y := 2*y \{ q_2 \} \) sequence 1, 2
4. \( \{ p_0 \land r=X*Y-x*y \land \text{odd}(x) \} x := x-1 \{ q_4 \} \) assignment
5. \( \{ q_4 \} r := r+y \{ q_5 \} \) assignment
6. \( \{ p_0 \land r=X*Y-x*y \land \text{odd}(x) \} x := x-1; r := r+y \{ q_5 \} \) sequence, 5, 6
7. \( \{ p_0 \land r=X*Y-x*y \} \)

if \( \text{even}(x) \) then \( x := x/2; y := 2*y \)
else \( x := x-1; r := r+y \{ q_2 \lor q_5 \} \)

* Since \( p_0 = r = r_0 \land x = x_0 \land y = y_0 \) and we’re assigning to \( x \), you can argue that \( q_1 \) should include \( x_0 = x_0 \). But if you don’t mind, let’s drop the \( x_0 = x_0 \) clause from \( q_1 \), and similarly, let’s drop any \( y_0 = y_0 \) clause from \( q_2 \), etc.