

Activity: Proof Outlines

A. Why?

Full formal proofs are long and tedious; proof outlines are much easier to write.

B. Outcomes

By the end of the activity you should

- Be able to fill in a proof outline for short programs.

C. Questions

1. Find p_1 and p_2 to complete the following proof outline. What predicate logic obligations are there for this outline? Also, if you have time, calculate any textual substitutions necessary.

$$\{n \geq 0\} \{p_1\} x := 0; \{p_2\} y := 1 \{y = 2^x \wedge 0 \leq x \leq n\}$$

$$p_1 \equiv p_2[y := 1] \equiv (y = 2^x \wedge 0 \leq x \leq n)[y := 1][x := 0] \equiv 1 = 2^0 \wedge 0 \leq 0 \leq n$$

$$p_2 \equiv (y = 2^x \wedge 0 \leq x \leq n)[y := 1] \equiv 1 = 2^x \wedge 0 \leq x \leq n$$

2. Find p_1 – p_4 to complete the following proof outline. What predicate logic obligations are there for this outline? Also, if you have time, calculate any textual substitutions necessary.

$\{p\}$ **if** $x < y$ **then**

$$\{p \wedge x < y\} \{p_1\} m := x \{p_2\}$$

else

$$\{p \wedge x \geq y\} \{p_3\} m := y \{p_4\}$$

fi $\{q\}$

where $p \equiv 0 \leq x \wedge 0 \leq y$ and $q \equiv 0 \leq m \leq x \wedge m \leq y$.

It's easiest for this problem to work backwards from the postcondition q :

$p_2 \equiv p_4 \equiv q$ because we want q to be true regardless of which if-else branch we take.

$p_1 \equiv p_2[m := x]$ because of the assignment statement

$$p_1 \equiv q[m := x] \equiv (0 \leq m \leq x \wedge m \leq y)[m := x] \equiv 0 \leq x \leq x \wedge x \leq y$$

Similarly, $p_3 \equiv p_4[m := y]$ because of the assignment statement

$$p_3 \equiv q[m := y] \equiv (0 \leq m \leq x \wedge m \leq y)[m := y] \equiv 0 \leq y \leq x \wedge y \leq y$$

Since $p \wedge x < y$ is next to p_1 , we need $p \wedge x < y \rightarrow p_1$.

I.e., $(0 \leq x \wedge 0 \leq y) \wedge x < y \rightarrow (0 \leq x \leq x \wedge x \leq y)$ [this is valid]

Similarly, we need $p \wedge x \geq y \rightarrow p_3$

I.e., $(0 \leq x \wedge 0 \leq y) \wedge x \geq y \rightarrow (0 \leq y \leq x \wedge y \leq y)$ [this is valid too]