

Activity: Simple Program Verification Proofs

A. Why?

Verification of small programs with just assignment and if-else is a good base for verifying larger programs and programs with loops.

B. Outcomes

By the end of the activity you should

- Be able to write a short proof of correctness for simple programs involving a sequence of assignments and if-else.

C. Questions

1. Using the assignment and sequence rules, fill in the rest of the formal proof below.

| Line | Claim | Rule |
|------|--|---------------|
| 1 | $\{ ??? \} i := i+1 \{ 0 \leq i \leq n, s+i = \text{sum}(0, i) \}$ | Assignment |
| 2 | $\{ ??? \} s := s+i \{ 0 \leq i \leq n, s = \text{sum}(0, i) \}$ | Assignment |
| 3 | $\{ ??? \} i := i+1; s := s+i \{ 0 \leq i \leq n, s = \text{sum}(0, i) \}$ | Sequence 1, 2 |

2. Using the assignment, skip, precondition strengthening, and if-else rules, fill in the rest of the formal proof below.

| Line | Claim | Rule |
|------|---|------------------------------|
| 1 | $\{ ??? \} y := -x \{ y \geq 0 \}$ | Assignment |
| 2 | $x = y \wedge x < 0 \rightarrow -x \geq 0$ | Predicate logic |
| 3 | $\{ ??? \} y := -x \{ y \geq 0 \}$ | Strengthen Precondition 2, 1 |
| 4 | $\{ ??? \} \text{skip} \{ y \geq 0 \}$ | Skip |
| 5 | $x = y \wedge x \geq 0 \rightarrow y \geq 0$ | Predicate logic |
| 6 | $\{ x = y \wedge x \geq 0 \} \text{skip} \{ ??? \}$ | Strengthen Precondition 5, 4 |
| 7 | $\{ x = y \} \text{if } x < 0 \text{ then } y := -x \text{ else skip fi } \{ y \geq 0 \}$ | If, 3, 6 |