The First Four Rules

Axiom 1: Skip

\[
\{p\} \text{skip} \{p\}
\]

Axiom 2: Assignment

\[
\{p[u := t]\} u := t\{p\}
\]

Rule 3: Composition

\[
\frac{\{p\} S_1 \{r\}, \{r\} S_2 \{q\}}{\{p\} S_1; S_2 \{q\}}
\]

Rule 4: Conditional

\[
\frac{\{p \land B\} S_1 \{q\}, \{p \land \neg B\} S_2 \{q\}}{\{p\} \text{if } B \text{ then } S_1 \text{ else } S_2 \text{ fi} \{q\}}
\]

Rule 5: Loop

\[
\frac{\{p \land B\} S \{p\}}{\{p\} \text{while } B \text{ do } S \text{ od} \{p \land \neg B\}}
\]

Rule 6: Consequence

\[
p \rightarrow p_1, \{p_1\} S \{q_1\}, q_1 \rightarrow q
\[
\frac{}{\{p\} S \{q\}}
\]
Triples

**Problem 1)** Let postcondition \( q \equiv x = 10 \). Let program \( S \) be \( x := y \ast 2 \). Use Axiom 2 to derive the precondition such that \( \models \{p\}S\{q\} \).

**Problem 2)** Let postcondition \( q \equiv x > 5 \). Let \( S_1 \) be \( x := x + 10 \). Let \( S_2 \) be \texttt{skip}. Choose a precondition \( p \) and test \( B \) such that \( \models \{p\} \text{ if } B \text{ then } S_1 \text{ else } S_2 \text{ fi } \{q\} \). Try to make \( p \) as un-restrictive as you can.

**Problem 3)** Suppose we have \( \models \{p\}S\{q\} \). Suppose now I also have a random assertion \( r \). Do you think we also have \( \models \{p\}S\{q \lor r\} \)? Why or why not?
Weakness

Problem 4) Rank the following logical assertions from strongest to weakest. Note that the ranking is not necessarily linear.

• $a \equiv \text{false}$
• $b \equiv \text{true}$
• $c \equiv x > 10 \lor y < 10$
• $d \equiv x > 10$
• $e \equiv x > 5 \lor y < 5$
• $f \equiv x > 5 \land y < 5$
• $g \equiv x > 5$

Problem 5) What can you say about $x + y = 10$ in regards to the ordering of the previous question?

Problem 6) Suppose $\{x > 0\} S \{y < 0\}$. Which of the following are also true?

1. $\{x > 0\} S \{y < 0 \lor x > 0\}$.
2. $\{x > 0 \land y < 0\} S \{y < 0\}$.
3. $\{y < 0\} S \{x > 0\}$.
4. $\{x > 0\} S \{y < 0 \land x > 0\}$.
5. $\{x > 0 \lor y < 0\} S \{y < 0\}$.
6. $\{x > 0\} S \{y < 10\}$.
7. $\{x > -10\} S \{y < 0\}$. 
Loop Invariants

We want to take the product of the elements of an array.

- The postcondition is \( r \equiv x = \prod_{j=0}^{\lvert A \rvert - 1} a[j] \).
- The loop invariant is \( p \equiv x = \prod_{j=0}^{i} a[j] \).
- The loop bound is \( i < \lvert A \rvert \).

**Problem 7)** Write the code to establish the loop invariant, and give a proof outline for it.

**Problem 8)** Write the loop, and show that the loop body preserves the loop invariant.

**Problem 9)** Show that the loop achieves the postcondition on termination.