Program Verification with Hoare Axioms

- **Definition 1**: A piece of code S is correct with respect to precondition p and postcondition q if whenever assertion p is true prior to the execution of S and S is executed then it terminates and q is true at its termination. A piece of code S is partially correct with respect to precondition p and postcondition q if whenever assertion p is true prior to the execution of S and S is executed and if it terminates then q is true at its termination. Partial correctness is denoted by \( p \{S\} q \).

1. Axiom of Composition: \((p_1 \{S_1\} p_2) \wedge (p_2 \{S_2\} p_3) \Rightarrow p_1 \{S_1; S_2\} p_3\).

2. Axioms of Consequence: \((p_1 \Rightarrow p_2) \wedge (p_2 \{S\} p_3) \Rightarrow p_1 \{S\} p_3\) \((p_1 \{S\} p_2) \wedge (p_2 \Rightarrow p_3) \Rightarrow p_1 \{S\} p_3\).

3. If-then Axiom: \((p \wedge \text{condition}) \{S\} p_2 \Rightarrow p_1 \{\text{if condition then } S\} p_2\).

4. If-then-else Axiom: \((p \wedge \text{condition} \{S_1\} p_2) \wedge (p \wedge \neg \text{condition} \{S_2\} p_2) \Rightarrow p_1 \{\text{if condition then } S_1 \text{ else } S_2\} p_2\).

5. Iteration Axiom: \((p \wedge \text{condition}) \{S\} p \Rightarrow p \{\text{while condition do } S\} (\neg \text{condition} \wedge p)\).

6. Axiom of Assignment: \((p(E) \{x := E\} p(x)\).

Program Verification with Weakest Preconditions

- **Definition 2**: The weakest precondition for code S and postcondition q is the weakest assertion p so that if p is a precondition and code S is executed then it terminates and q is true at its termination. This is denoted as \( p = \text{wp}(S, q) \). Thus for any assertion r so that r \{S\} q is true and S terminates given precondition r, then \( r \Rightarrow p \). Conversely, if \( r \Rightarrow \text{wp}(S, q) \) then r \{S\} q is true and S terminates given precondition r.

**Theorem 1**: \( \text{wp}(\text{skip}, q) = q \).

**Theorem 2**: \( \text{wp}(S_1; S_2, q) = \text{wp}(S_1, \text{wp}(S_2, q)) \).

**Theorem 3**: \( \text{wp}(x := E, q(x)) = E \) is defined and q(E).

**Theorem 4**: \( \text{wp}(\text{if } \text{cond then } S, q) = (\text{cond } \Rightarrow \text{wp}(S, q)) \wedge (\neg \text{cond } \Rightarrow q) = (\text{cond } \wedge \text{wp}(S, q)) \vee (\neg \text{cond } \wedge q) \).

**Theorem 5**: \( \text{wp}(\text{if } \text{cond then } S_1 \text{ else } S_2, q) = (\text{cond } \Rightarrow \text{wp}(S_1, q)) \wedge (\neg \text{cond } \Rightarrow \text{wp}(S_2, q)) = (\text{cond } \wedge \text{wp}(S_1, q)) \vee (\neg \text{cond } \wedge \text{wp}(S_2, q)) \).