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: $((p_1 \wedge condition)\{S\}p_2) \wedge ((p_1 \wedge \neg condition) \Rightarrow p_2)$

$\Rightarrow p_1\{\textbf{if}\ condition\ \textbf{then}\ S\}\ p_2$.

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

$\Rightarrow p_1\{\textbf{if}\ condition\ \textbf{then}\ S_1\ \textbf{else}\ S_2\}\ p_2$.

5. Iteration Axiom: $(p \wedge condition)\{S\}p$

$\Rightarrow p\{\textbf{while}\ condition\ \textbf{do}\ S\}(\neg condition \wedge p)$.

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 $p = wp(S, q)$. Thus for any assertion r so that r {S} q is true and S terminates given precondition r, then $r \Rightarrow p$. Conversely, if $r \Rightarrow wp(S, q)$ then r {S} q is true and S terminates given precondition r.

Theorem 1: $wp(\textbf{skip}, q) = q$.

Theorem 2: $wp(S_1;S_2, q) = wp(S_1, wp(S_2, q))$.

Theorem 3: $wp(x := E, q(x)) =$ E is defined and $q(E)$.

Theorem 4: $wp(\textbf{if}\ cond\ \textbf{then}\ S, q) = (cond \Rightarrow wp(S, q)) \wedge (\neg cond \Rightarrow q)$

$= (cond \wedge wp(S, q)) \vee (\neg cond \wedge q)$.

Theorem 5: $wp(\textbf{if}\ cond\ \textbf{then}\ S_1\ \textbf{else}\ S_2, q)$

$= (cond \Rightarrow wp(S_1, q)) \wedge (\neg cond \Rightarrow wp(S_2, q))$

$= (cond \wedge wp(S_1, q)) \vee (\neg cond \wedge wp(S_2, q))$