Rules and Axioms

Rule A1: Decomposition

\[ \Gamma, \{ \varphi \} S \{ \psi \}, \quad \Gamma, \{ \psi \} S \{ \text{true} \} \]
\[ \{ \varphi \} S \{ \psi \} \]

Axiom A2: Invariance

\[ \{ \varphi \} S \{ \varphi \} \]
where free(\varphi) \cap change(S) = \phi

Rule A3: Disjunction

\[ \{ \varphi \} S \{ \psi \}, \{ \tau \} S \{ \psi \} \]
\[ \{ \varphi \lor \tau \} S \{ \psi \} \]

Rule A4: Conjunction

\[ \{ \varphi_1 \} S \{ \psi_1 \}, \{ \varphi_2 \} S \{ \psi_2 \} \]
\[ \{ \varphi_1 \land \varphi_2 \} S \{ \psi_1 \land \psi_2 \} \]

Rule A5: \exists-Introduction

\[ \{ \varphi \} S \{ \psi \} \]
\[ \{ \exists x : \varphi \} S \{ \psi \} \]
where x does not occur in S or in free(\psi).

Rule A6: Invariance

\[ \{ \varphi \} S \{ \psi \} \]
\[ \{ \varphi \land \psi \} S \{ \psi \land \psi \} \]
where free(\varphi) \cap change(S) = \phi

Rule A7: Substitution

\[ \{ \varphi \} S \{ \psi \} \]
\[ \{ \varphi[\overline{u} := \overline{t}] \} S \{ \psi[\overline{u} := \overline{t}] \} \]
where \overline{u} \notin var(S) \land \overline{t} \notin change(S).
Proof System 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

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

Rule 7: Loop II

\[
\frac{\{p \land B\}S\{p\},\ \{p \land b \land t = z\}S\{t < z\},\ p \rightarrow t \geq 0}{\{p\} \text{while } B \text{ do } S \text{ od } \{p \land \neg B\}}
\]

where \( t \) is an integer expression and \( z \) is an integer variable that does not appear in \( p, B, t, \) or \( S \).
Rule 8: Recursion
\[
\{p_1 \} P_1 \{ q_1 \}, \ldots, \{ p_n \} P_n \{ q_n \} \vdash \{ p \} S \{ q \},
\{ p_1 \} P_1 \{ q_1 \}, \ldots, \{ p_n \} P_n \{ q_n \} \vdash \{ p_i \} S_i \{ q_i \}, \ i \in \{ 1, \ldots, n \},
\]
where \( D = P_1 :: S_1, \ldots, P_n :: S_n \) (this rule is not covered in class).

Rule 9: Recursion II
(not covered in class)

Rule 10: Block
\[
\{ p \} \overline{x} := \overline{t} ; S \{ q \}
\]
\[
\frac{}{\{ p \} \text{begin local } \overline{x} := \overline{t} ; S \text{ end } \{ q \}}
\]
where \( \text{var}(\overline{x}) \cap \text{free}(q) = \phi \)

Rule 11: Instantiation
(not covered in class)

Rule 12: Recursion III
(not covered in class)

Rule 13: Recursion IV
(not covered in class)

Axiom 14: Assignment to Instance Variables
\[
\{ p[u := t] \} u := t \{ p \}
\]
where \( u \) is a (simple or subscripted) instance variable.

Rule 15: Instantiation II — Method Instantiation
\[
\{ p \} y.m \{ q \}
\]
\[
\frac{}{\{ p[y := s] \} s.m \{ q[y := s] \}}
\]
where \( D \) is the set of method declarations, \( y \not\in \text{var}(D) \) and \( \text{var}(s) \cap \text{change}(D) = \phi \).
Rule 16: Recursion V

\[
\begin{align*}
\{p_1\} P_1\{q_1\}, \ldots, \{p_n\} P_n\{q_n\} & \vdash \{p\} S\{q\}, \\
\{p_1\} P_1\{q_1\}, \ldots, \{p_n\} P_n\{q_n\} & \vdash \\
\{p_i\} & \text{begin local this := } s_i; S_i \text{ end } \{q_i\}, i \in \{1, \ldots, n\}
\end{align*}
\]

where \(m_i :: S_i \in D\) for \(i \in \{1, \ldots, n\}\). Its simplified version is

\[
\begin{align*}
\{p\} & \text{begin local this := } s; S \text{ end } \{q\} \\
\{p\} & s.m\{q\}
\end{align*}
\]

where \(D = m :: S\).