CMPSCI 266 - Formal Specification and Verification

Verification Condition Generation Rules For Pascal

V1: Assignment

$$\frac{P\{A\}R}{P\{A;x:=e\}R}\ \begin{matrix}x\\ e\end{matrix}$$

V2: Consequence

$$\frac{P\{A\}Q,\ Q\rightarrow R}{P\{A;\text{assert } Q\}R} \qquad \frac{P\rightarrow Q}{P\{\}Q} \qquad \frac{P\{A\}Q\rightarrow R}{P\{A;Q\text{-if}\}R}$$

V3: Iteration

$$\frac{P\{A\}R,\ R\&B\{S\}R,\ R\&\tilde{}B\rightarrow Q}{P\{A;\text{assert } R;\text{ while } B \text{ do } S\}Q}$$

V4: Conditional

$$\frac{P\{A;B\text{-if};S1\}R,\ P\{A;\tilde{}B\text{-if};S2\}R}{P\{A;\text{if } B \text{ then } S1 \text{ else } S2\}R}$$

$$\frac{P\{A;B\text{-if};S\}R,\ P\{A;\tilde{}B\text{-if}\}R}{P\{A;\text{if } B \text{ then } S\}R}$$

V5: Repeat

$$\frac{P\{A;S\}Q,\ Q\&\tilde{}B\{S\}Q,\ Q\&B\rightarrow R}{P\{A;\text{assert } Q;\text{repeat } S \text{ until } B\}R}$$

V6: Compound

$$\frac{P\{S1;...;Sn\}R}{P\{\text{begin } S1;...;Sn \text{ end}\}R}$$

Note: "&" is logical AND and "˜" is logical NOT.