Control Structures and Proof Rules

We will consider the three basic control structures of imperative programming. A *command* C denotes a (possibly compound) statement formed form the atomic statements using the control structures. A series of commands can be enclosed in **begin** … **end** to form a single syntactic unit. The control structures we investigate are (where B is a Boolean-valued expression):

- sequential execution — $C_1 ; C_2$

- conditional — **if** B **then** C_1 **else** C_2
- while-loop — **while** B **do** C

Each of these control structures has an associated proof rule — based on properties of its components, we infer properties of the compound statement. These are as follows:

Sequential rule

$$\frac{\vdash \{P\}\, C_1\, \{Q\}, \vdash \{Q\}\, C_2\, \{R\}}{\vdash \{P\}\, C_1 ; C_2\, \{R\}}$$

Conditional rule

$$\frac{\vdash \{P \wedge B\}\, C_1\, \{R\}, \vdash \{P \wedge \neg B\}\, C_2\, \{R\}}{\vdash \{P\}\, \textbf{if } B \textbf{ then } C_1 \textbf{ else } C_2\, \{R\}}$$

While rule

$$\frac{\vdash \{P \wedge B\}\, C\, \{P\}}{\vdash \{P\}\, \textbf{while } B \textbf{ do } C\, \{P \wedge \neg B\}}$$