# Formal Methods and Functional Programming

## Axiomatic Semantics

**Peter Müller**

Chair of Programming Methodology
ETH Zurich

# Axiomatic Semantics of IMP

- Skip

$$\frac{}{\{\ \mathbf{P}\ \}\ \mathtt{skip}\ \{\ \mathbf{P}\ \}}\ (\textsc{Skip}_{Ax})$$

- Assignment

$$\frac{}{\{\ \mathbf{P}[x \mapsto e]\ \}\ x\ \mathtt{:=}\ e\ \{\ \mathbf{P}\ \}}\ (\textsc{Ass}_{Ax})$$

- Sequential composition

$$\frac{\{\ \mathbf{P}\ \}\ s\ \{\ \mathbf{Q}\ \} \quad \{\ \mathbf{Q}\ \}\ s'\ \{\ \mathbf{R}\ \}}{\{\ \mathbf{P}\ \}\ s;s'\ \{\ \mathbf{R}\ \}}\ (\textsc{Seq}_{Ax})$$

# Axiomatic Semantics of IMP (cont'd)

- Conditional statement

$$\frac{\{\, b \land \mathbf{P} \,\}\; s \;\{\, \mathbf{Q} \,\} \quad \{\, \neg b \land \mathbf{P} \,\}\; s' \;\{\, \mathbf{Q} \,\}}{\{\, \mathbf{P} \,\}\; \texttt{if}\ b\ \texttt{then}\ s\ \texttt{else}\ s'\ \texttt{end} \;\{\, \mathbf{Q} \,\}}\ (\textsc{If}_{Ax})$$

- Loop statement

$$\frac{\{\, b \land \mathbf{P} \,\}\; s \;\{\, \mathbf{P} \,\}}{\{\, \mathbf{P} \,\}\; \texttt{while}\ b\ \texttt{do}\ s\ \texttt{end} \;\{\, \neg b \land \mathbf{P} \,\}}\ (\textsc{Wh}_{Ax})$$

- Rule of consequence

$$\frac{\{\, \mathbf{P}' \,\}\; s \;\{\, \mathbf{Q}' \,\}}{\{\, \mathbf{P} \,\}\; s \;\{\, \mathbf{Q} \,\}}\ (\textsc{Cons}_{Ax}) \qquad \textit{if } \mathbf{P} \models \mathbf{P}' \textit{ and } \mathbf{Q}' \models \mathbf{Q}$$

# Total Correctness

- Loop

$$\frac{\{\ b \land \mathbf{P} \land e = Z\ \}\ s\ \{\ \Downarrow \mathbf{P} \land e < Z\ \}}{\{\ \mathbf{P}\ \}\ \texttt{while}\ b\ \texttt{do}\ s\ \texttt{end}\ \{\ \Downarrow \neg b \land \mathbf{P}\ \}}\ (\textsc{WhTot}_{Ax})\ \text{if}\ b \land \mathbf{P} \models 0 \leq e$$