

Program verification: Proof calculus

CS242 Formal Specification and Verification

University of Warwick

Autumn term 2006

Partial correctness

$$\frac{(\phi) C_1 (\eta) \quad (\eta) C_2 (\psi)}{(\phi) C_1; C_2 (\psi)} \text{Composition}$$

$$\frac{}{(\psi[E/x]) x = E (\psi)} \text{Assignment}$$

$$\frac{(\phi \wedge B) C_1 (\psi) \quad (\phi \wedge \neg B) C_2 (\psi)}{(\phi) \text{ if } B \{C_1\} \text{ else } \{C_2\} (\psi)} \text{If-statement}$$

$$\frac{(\psi \wedge B) C (\psi)}{(\psi) \text{ while } B \{C\} (\psi \wedge \neg B)} \text{Partial-while}$$

$$\frac{\vdash_{\text{AR}} \phi' \rightarrow \phi \quad (\phi) C (\psi) \quad \vdash_{\text{AR}} \psi \rightarrow \psi'}{(\phi') C (\psi')} \text{Implied}$$

Total correctness

$$\frac{(\eta \wedge B \wedge 0 \leq E = E_0) C (\eta \wedge 0 \leq E < E_0)}{(\eta \wedge 0 \leq E) \text{ while } B \{C\} (\eta \wedge \neg B)} \text{Total-while}$$