CS 245

Program Verification

Integer Expression grammar

$$E ::= n \mid x \mid (-E) \mid (E+E) \mid (E-E) \mid (E*E)$$

n is an integer

x is an integer variable

boolean expression grammar

$$B ::= \text{true} \mid \text{false} \mid (!B) \mid (B \,\&\, B) \mid (B \,||\, B) \mid (E < E)$$

Equality test for integer expressions:

$$E_1 == E_2$$

is given by

$$!(E_1 < E_2) \wedge !(E_2 < E_1)$$

In addition

$(E_1 \; != \; E_2)$

is used to write

$!(E_1 == E_2)$

Command grammar

$$C ::= x = E \mid C ; C \mid \text{if } B \{C\} \text{ else } \{C\}$$
$$\mid \text{while } B \{C\}$$

Proof calculus for partial correctness

$$\frac{}{\{\ \Psi[E/x]\ \}\ x = E\ ;\ \{\ \Psi\ \}}\ \text{Assignment}$$

$$\frac{\langle \phi \rangle \; c_1 \; \langle \eta \rangle \qquad \langle \eta \rangle \; c_2 \; \langle \psi \rangle}{\langle \phi \rangle \; c_1 ; c_2 \; \langle \psi \rangle}$$

composition

$$\frac{\{\phi \wedge B\}\ c_1\ \{\psi\} \qquad \{\phi \wedge \neg B\}\ c_2\ \{\psi\}}{\{\phi\}\ \text{if } B \{c_1\} \text{ else } \{c_2\}\ \{\psi\}}$$

if-statement

$$\frac{\{\!|\ \phi_1\ |\!\}\ c_1\ \{\!|\ \psi\ |\!\} \qquad \{\!|\ \phi_2\ |\!\}\ c_2\ \{\!|\ \psi\ |\!\}}{\{\!|\ (\mathcal{B} \to \phi_1) \wedge (\neg\mathcal{B} \to \phi_2)\ |\!\}\ \text{if } \mathcal{B} \text{ the } \{c_1\} \text{ else } \{c_2\}\ \{\!|\ \psi\ |\!\}}$$

modified- if

$$\frac{\{\eta \wedge B\}\ C\ \{\eta\}}{\{\eta\}\ \text{while } B \{C\}\ \{\eta \wedge \neg B\}}$$

partial-while

$$\frac{\phi' \hookrightarrow \phi \qquad \llbracket \phi \rrbracket \subseteq \llbracket \psi \rrbracket \qquad \psi \to \psi'}{\llbracket \phi' \rrbracket \subseteq \llbracket \psi' \rrbracket}$$

implied

$$\frac{\{\eta \wedge B \wedge 0 \leq E = E_0\}\, C\, \{\eta \wedge 0 \leq E < E_0\}}{\{\eta \wedge 0 \leq E\}\ \text{while}\ B\ \{C\}\ \{\eta \wedge \neg B\}}$$

total
while