Un linguaggio di programmazione imperativo

Espressioni aritmetiche $\mathbb{E}$

$\forall z \in \mathbb{Z} \quad z \in \mathbb{E} \qquad \forall e_1, e_2 \in \mathbb{E} \quad (e_1 + e_2),\ (e_1 - e_2),\ -e_1,\ (e_1 * e_2),\ (e_1 / e_2),\ (e_1 \% e_2) \in \mathbb{E}$

Espressioni logiche $\mathbb{B}$

$true, false \in \mathbb{B} \qquad \forall b_1, b_2 \in \mathbb{B} \quad (b_1 \,\&\, b_2),\ (b_1 \mid b_2),\ !\, b_1 \in \mathbb{B}$

$\forall e_1, e_2 \in \mathbb{E} \quad (e_1 < e_2),\ (e_1 == e_2),\ (e_1 != e_2),\ (e_1 <= e_2) \in \mathbb{B}$

Comandi $\mathbb{C}$

skip $\in \mathbb{C}$

v := e $\in \mathbb{C}$ (v: variabile, e: espr. aritmetica)

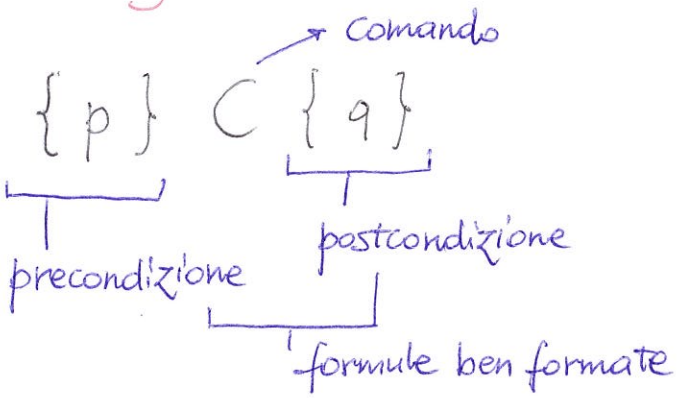
if B then C else D endif $\in \mathbb{C}$ (B: espr. logica; C, D: comandi)

C ; D $\in \mathbb{C}$ (C, D: comandi)

while B do C endwhile $\in \mathbb{C}$ (B: espr. logica; C: comando)

Logica di Hoare

Tripla



Regola di derivazione

$$\frac{T_1, \dots, T_M, f_1, \dots, f_n}{T}$$

premesse

conclusione

T_i tripla
f_i formula ben formata

Dimostrazione

$$\dfrac{\dfrac{\dfrac{}{T_1} \quad f_1}{T_2} \qquad \dfrac{\dfrac{}{T_3} \quad \dfrac{}{T_4}}{T_5} \qquad f_2}{T_6}$$

Logica di Hoare — regole di derivazione

① $\dfrac{}{\{p\}\ \text{skip}\ \{p\}}$ skip

② $\dfrac{\{p\}\ C\ \{p'\} \quad \{p'\}\ D\ \{q\}}{\{p\}\ C;D\ \{q\}}$ sequenza, composizione

③ $\dfrac{\{p \wedge B\}\ C\ \{q\} \quad \{p \wedge \neg B\}\ D\ \{q\}}{\{p\}\ \text{if } B \text{ then } C \text{ else } D \text{ endif}\ \{q\}}$ scelta

④ Obiettivo $\{x > 0\}\ C\ \{x = 2^y\}$

Supponiamo $\vdash \{x \geq 0\}\ C\ \{x = 2^y\}$

Osserviamo $x > 0 \rightarrow x \geq 0 \quad \Rightarrow \models \{x > 0\}\ C\ \{x = 2^y\}$

$$\frac{p \rightarrow p' \quad \{p'\}\ C\ \{q\}}{\{p\}\ C\ \{q\}}$$ implicazione, conseguenza (I)

$$\frac{\{p\}\ C\ \{q\} \quad q \rightarrow q'}{\{p\}\ C\ \{q'\}}$$

Logica di Hoare - regole di derivazione

Assegnamento

$$x := y + 2 \quad \{x \geq 0\}$$

Quale precondizione garantisce la postcondizione richiesta ?

$$\vDash \{\underbrace{y \geq -2}_{P}\} \; x := \underbrace{y+2}_{E} \; \{\underbrace{x \geq 0}_{q}\}$$

(5)

$$\frac{}{\{\underbrace{q[E/x]}_{\text{sostituisco ogni occorrenza di } x \text{ in } q \text{ con } E}\} \; x := E \; \{q\}} \quad \text{assegnamento}$$