

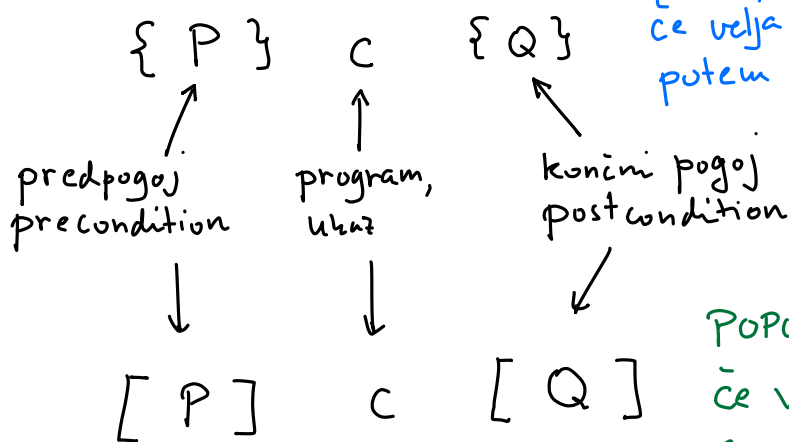
Dokazovanje pravilnosti

Specifikacija: Kaj bi spletni radi imeli?
Opis, kaj naj koda počne

Implementacija: Koda, ki ustreza specifikaciji

Hoarova logika

Hoarove trojice



DELNA PRAVILNOST:
če velja P in se C ustavi,
potem velja Q

POPOLNA PRAVILNOST:
če velja P, potem
se C ustavi in velja Q

Primer: Zamenjaj vrednosti spremenljivk x in y:

$$\{x=m \wedge y=n\} \ C \ \{x=n \wedge y=m\}$$

① $t := x; x := y; y := t$



zadošča tudi $[x=m \wedge y=n] \ C \ [x=n \wedge y=m]$

② $x := y; y := x$



③ $\text{while true do skip done}$



vendar ne zadošča
 $[x=m \wedge y=n] \ C \ [x=n \wedge y=m]$

④ $x:=1; y:=1; m:=1; n:=1$ ✓ ni bilo mišljeno, da spreminjamo m in n .

Da se znebimo ④, zahtevamo, da m in n ne smemo spreminjati:
 m in n sta duhova (ghost variable)

Popravimo zahtevo:

$$\{x=m \wedge y=n\} \subset \{x=n \wedge y=m\}$$

in m, n duhova

Primer: $\{true\} \subset \{x \leq y\}$

Rešitev: $x:=0; y:=0$ ✓

"Uredi x in y po velikosti." m, n duhova

čudno: $\{x=m \wedge y=n\} \subset \{x \leq y \wedge (x=m \vee x=n) \wedge (y=m \vee y=n)\}$

$x:=y$ ✓ ni mišljeno

2. poskus: $\{x=m \wedge y=n\} \subset \left\{ \begin{array}{l} (m < n \Rightarrow x=m \wedge y=n) \wedge \\ (m \geq n \Rightarrow x=n \wedge y=m) \end{array} \right\}$

$$\begin{array}{cc} (m < n \Rightarrow P) \vee (m \geq n \Rightarrow Q) & \\ \perp & \perp \\ \perp \Rightarrow P & \perp \Rightarrow Q \\ \top & \top \end{array}$$

$\{x=m \wedge y=n\} \subset \{x = \min(m, n) \wedge y = \max(m, n)\}$

Pišemo:

$\{P\}$
 \subset
 $\{Q\}$

$\{P_1\}$
 $C_1;$
 $\{P_2\}$
 $C_2;$
 $\{P_3\}$
 \vdots

$\{x \leq 10\}$
 $x := x + 2$
 $\{x \leq 12\}$

Strongest postcondition
hajmucnejši končni pogoj

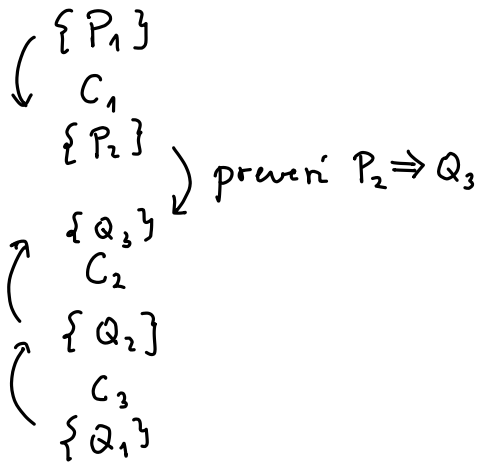
~~$\{x \leq 2\}$~~ $\{x \leq 6\}$
 $x := 2 * x$
 $\{x \leq 12\}$

Weakest precondition,
najšibkejši predpogoj

Pravila sklepanja

$$\frac{P' \Rightarrow P \quad \{P\} \subset \{Q\} \quad Q \Rightarrow Q'}{\{P'\} \subset \{Q'\}} \quad \text{I}$$

Uporaba:



$$\frac{\{P_1\} \subset \{Q_1\} \quad \{P_2\} \subset \{Q_2\}}{\{P_1 \wedge P_2\} \subset \{Q_1 \wedge Q_2\}} \quad \text{II}$$

Kaj pa $\{P\} \subset \{Q_1 \wedge Q_2\}$

$$\frac{P \Rightarrow P \wedge P \quad \frac{\{P\} \subset \{Q_1\} \quad \{P\} \subset \{Q_2\}}{\{P \wedge P\} \subset \{Q_1 \wedge Q_2\}} \quad \text{II} \quad Q_1 \wedge Q_2 \Rightarrow Q_1 \wedge Q_2}{\{P\} \subset \{Q_1 \wedge Q_2\}} \quad \text{I}$$

$\{x \leq 7\}$
 $y := x + 3$
 $\{x \leq 7\}$

$\{P\} \rightarrow$ spremenljivke x_1, \dots, x_n
 $C \rightarrow$ ne spremenljiva spremenljivka iz P
 $\{P\}$

$\{x \leq 7\}$
 $x := x - 3$ ✓
 $\{x \leq 7\}$

$FV(\dots)$ vse spremenljivke
 $FA(\dots)$ vse, ki se pojavijo
 levo od $:=$

$FA(\text{ if false then } \underline{x := 5} \text{ else } \underline{y := 7}) = \{x, y\}$

Pogojni stavki:

| | |
|--|---------------------------------|
| $\{P \wedge b\} c_1 \{Q\}$ | $\{P \wedge \neg b\} c_2 \{Q\}$ |
| $\{P\}$ if b then c_1 else c_2 $\{Q\}$ | |

$\{P\}$

if b then

$\{P \wedge b\}$

c_1

$\{Q\}$

else

$\{P \wedge \neg b\}$

c_2

$\{Q\}$

$\{Q\}$

$\{P\}$

$c_1;$

$\{Q\}$

c_2

$\{Q\}$

Pravilo za ;

| | |
|-------------------------|-------------------|
| $\{P\} c_1 \{Q\}$ | $\{Q\} c_2 \{R\}$ |
| $\{P\} c_1 ; c_2 \{R\}$ | |

Zanka while :

$$\frac{\{P \wedge b\} c \{P\}}{\{P\} \text{ while } b \text{ do } c \text{ done } \{P \wedge \neg b\}}$$

P se imenuje invarianta zanke

$\{P\}$

while b do

$\{P \wedge b\}$

c

$\{P\}$

done

$\{P \wedge \neg b\}$

$\{P\}$ \Downarrow uporabimo možgane

$\{P'\}$

P' invarianta

while b do

$\{P' \wedge b\}$

c

$\{P'\}$

done

$\{P' \wedge \neg b\}$

\Downarrow

$\{Q\}$

$\{P[x \mapsto e]\}$

$x := e$

$\{P\}$

$\{7^3 - 5 \cdot 7 \leq 200\}$

$x := 7$

$\{x^3 - 5x \leq 200\}$

Zapis: $P[x \mapsto e]$

"U formuli P zamenjamo x z e "
Substitucija ali zamenjava

$(x \leq 8 \vee y + x = 3) [x \mapsto 3 + z]$

\Downarrow

$(3 + z \leq 8 \vee y + (3 + z) = 3)$

$\{P[x \mapsto e]\} x := e \{P\}$

$s := 0;$

$i := 0;$

64-bit

while $i < 100$ do

$s := s + i;$

$i := i + 1$

done

"e se zmanjša"

$$\frac{[P \wedge b \wedge e = z] \text{ c } [P \wedge e < z]}{[P] \text{ while } b \text{ do } c \text{ done } [P \wedge \neg b]}$$

z duh

e je naravno število,
ali količina, ki se
ne more v nedogled
zmanjševati, npr:

$$\underbrace{e \in \mathbb{Z} \wedge e > -17}_{e + 17}$$

$$x \leq y \Rightarrow x \leq \frac{x+y}{2} \leq y$$

$$x \leq y \Rightarrow x \leq \frac{x+y}{2}$$

Preverimo:

$$x = \frac{x+x}{2} \leq \frac{x+y}{2} \quad \text{ker } x \leq y$$

Obi-wan error
off-by-one error

while $i < b$ do

$p := p * a;$

$i := i + 1$

done

| i | p | $p = a^i$ |
|-----|-------|-----------|
| 0 | 1 | ✓ |
| 1 | a | ✓ |
| 2 | a^2 | ✓ |
| 3 | a^3 | ✓ |