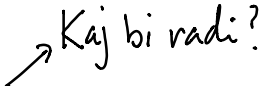
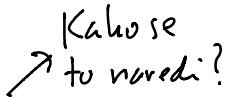


Dokazovanje pravilnosti programov

Specifikacija: opis, kaj naj program počne  Kaj bi radi?

Implementacija: je konkreten program, ki počne,
kar zahteva specifikacija.  Kako se to naredi?

```
t := x;  
x := y;  
y := t;
```

Hoarova logika

Hoarova trojica

$\{P\} C \{Q\}$
 predpogoj
(precondition)  končni pogoj
(postcondition)

P, Q logični formulici
 C ukaz (koda)

Delna pravilnost $\{P\} \subset \{Q\}$ $\leftarrow$ ne zagotavlja, da se C ustavi!
 Če velja P in če se C ustavi, bo veljal Q.

Popolna pravilnost $[P] \subset [Q]$ $\leftarrow$ zagotavlja, da se C ustavi.
 Če velja P, potem se C ustavi in veljal bo Q.

Primer:

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

$$\begin{array}{l} \{x=m \wedge y=n\} \\ \subset \\ \{x=n \wedge y=m\} \end{array}$$

$$\begin{array}{l} \{x=m \wedge y=n\} \\ t:=x; x:=y; y:=t \\ \{x=n \wedge y=m\} \end{array}$$



$\times$ $\begin{array}{l} [x=m \wedge y=n] \\ \text{while true do skip done} \\ [x=n \wedge y=m] \end{array}$

$$\begin{array}{l} \{x=m \wedge y=n\} \\ \text{while true do skip done} \\ \{x=n \wedge y=m\} \end{array}$$



$$\begin{array}{l} \{x=m \wedge y=n\} \\ x:=0; y:=0; m:=0; n:=0; \quad \checkmark \text{?!} \\ \{x=n \wedge y=m\} \end{array}$$

$$\begin{array}{l} \{x=m \wedge y=n\} \\ t:=x; x:=y; y:=t \\ \{x=n \wedge y=m\} \end{array}$$

m in n naj bosta duhova (ghost variable)

To pomeni, da se m in n ne smeta uporabljati v programu.

$$\begin{array}{l} \{x=m \wedge y=n\} \\ t:=x; x:=y; y:=t; \text{skip}; \text{skip}; \text{skip} \\ \{x=n \wedge y=m\} \end{array}$$

$$\begin{array}{l} \{x=m \wedge y=n\} \\ x:=x+y; \\ y:=x-y; \\ x:=x-y; \\ \{x=n \wedge y=m\} \end{array}$$



Primer: $\{ \text{true} \} \leftarrow$ ni nobene predpostavke

C

$\{ x \leq y \}$

$\{ \text{true} \}$

$x := 0;$

$y := 10;$

$\{ x \leq y \}$ ✓

Primer: $\{ x = m \wedge y = n \}$

if $x < y$ then

Skip

else

$t := x; x := y; y := t$

end

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

Pravila Hoarove logike

$$\frac{A_1 \quad A_2 \quad \dots \quad A_n}{B}$$

← predpostavke
← sklep
"če veljajo $A_1, \dots, A_n$,
potem velja tudi B ."

$P \equiv \forall x. \exists z. y + z = x$
 $FV(P) = \{y\}$

x in z sta vezani spremenljivki
(x in z sta lokalni spremenljivki)

$a \Rightarrow \text{false} \quad \neg Q$

Primeri

$\{ \text{true} \} \text{ c } \{ \text{true} \}$ velja vedno
 $\{ \text{true} \} \text{ c } \{ \text{false} \}$ c se ne ustavi

$\{ \text{false} \} \text{ c } \{ \text{true} \}$ velja vedno

$\{ \text{false} \} \text{ c } \{ \text{false} \}$ velja vedno

$[\text{true}] \text{ c } [\text{true}]$ c se ustavi

$[\text{true}] \text{ c } [\text{false}]$ nikoli ne velja

$[\text{false}] \text{ c } [\text{true}]$ vedno velja

$[\text{false}] \text{ c } [\text{false}]$ vedno velja

$$\text{true} \wedge P \Leftrightarrow P$$

$$\text{true} \wedge "c \text{ se ustavi}" \Rightarrow \text{false}$$

$$"c \text{ se ustavi}" \Rightarrow \text{false}$$

$$\neg "c \text{ se ustavi}"$$

Primeri:

$\{ x \leq y \}$
 $s := (x + y) / 2$
 $\{ x \leq s \leq y \}$

$\{ x \leq y \}$

$\{ x \leq (x+y)/2 \leq y \}$

$s := (x+y)/2;$

$\{ x \leq s \leq y \}$

$\Rightarrow ?$

Predpostavimo $x \leq y$

Preverimo $x \leq (x+y)/2$ 1:2

$$\Leftrightarrow 2x \leq x+y \quad 1-x$$

$$\Leftrightarrow x \leq y \quad \checkmark$$

Preverimo $(x+y)/2 \leq y$ 1:2

$$x+y \leq 2y \quad 1-y$$

$$x \leq y \quad \checkmark$$

Primer:

$\{ x \leq 7 \}$
 $x := x + 3$
 $\{ x \leq 10 \}$

$\{ x \leq 7 \}$

$\{ x+3 \leq 10 \}$

$x := x + 3;$

$\{ x \leq 10 \}$

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

P je $x \leq 10$

e je $x+3$

$P[x \mapsto e]$ je $x+3 \leq 10$

$$\{x \leq 7\}$$

$$\{(x+3)-3 \leq 7\}$$

$$x := x+3;$$

$$\{x-3 \leq 7\}$$

$$\{true\}$$

$$\{5=5\}$$

$$x := 5;$$

$$\{x=5\}$$

$$P \dots x=5$$

$$e \dots 5$$

$$P[x \mapsto e] \quad 5=5$$

```

while i < b do
  { i < b, ?Q }
  p := p * a;
  i := i + 1
  { ?Q }
done

```

