Pravilnost programov

```
x := y + 1;
y := 7
```

Ali deluje pravilno?
Ni odgovora.

```
static void sort(int[] a) {
    ⋮
}
```

Specifikacija: opis, kaj naj bi program počel.
funkcija kode

- podamo neformalno (v navadnem jeziku)
- kombinirane metode (jezik + matematika)
- kot logično izjavo (zapisana z logično formulo) ←

Hoarove trojice

$\{P\}\ C\ \{Q\}$

NE ZAGOTAVLJA, DA C USTAVI
Delna pravilnost

- P: predpogoj (precondition)
- C: program/koda
- Q: končni pogoj (post condition)

"Če velja P in če se C ustavi, potem velja Q."

$[P]\ c\ [Q]$

ZAGOTOVO SE c USTAVI.
Popolna pravilnost

"Če velja P, se c ustavi in velja Q."

Primer:

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

"c zamenja vrednosti spremenljivk x in y"

Na primer:

$X := X + y$
$y := X - y$
$X := X - y$

x	y
m	n
m+n	n
m+n	m
n	m

Posebni primeri:

$\{ true \}\ c\ \{ Q \}$ "nimamo predpogoja"

$\{ P \}\ c\ \{ true \}$ vedno velja, ni koristno

$[true]\ c\ [true]$ "Če velja true, se c ustavi in velja true"
⇕
"c se ustavi"

$\{ false \}\ c\ \{ Q \}$ "Če velja false in se c ustavi, potem Q"
"false ⇒ Q"
"true" vedno res

Pišemo:

$\{P\}$
c
$\{Q\}$

$\{P\}$ ← recimo, da velja P
C_1; ← izvedemo C_1
$\{Q\}$ ← potem velja Q (če se C_1 ustavi)
C_2 ← izvedemo C_2
$\{R\}$ ← velja R
...

Primer:

$\{true\}$
$x := 0;$
$\{x = 0\}$
$y := 1$
$\{x = 0 \wedge y = 1\}$
$\{x \leq y\}$

$\{true\}$
while true do
    skip
done
$\{x \leq y\}$

VELJA

$[true]$
while true do
    skip
done
$[x \leq y]$

NE VELJA

Primer: "koda c ureli x in y po velikosti, se. pravi manjšega od x in y shrani v x, večjega v y."

$[x = m \wedge y = n]$
if $y < x$ then
    $t := x;$
    $x := y;$
    $y := t$
else
    skip
end
$[x \leq y \wedge \{x, y\} = \{m, n\}]$

$[x = \min(m, n) \wedge y = \max(m, n)]$

- Specifikacija: zahteva/opis, kaj program počne.
- Implementacija: koda, ki zadošča (ali ne) specifikaciji

Pravila sklepanja

$\{x > 0\}$

$y := 7 + 7$

$\{x > 0\}$

Pogojni stavek:

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

if $y < x$ then

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

$t := x;$

$x := y;$

$y := t;$

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

else

$\{x = m \wedge y = n \wedge \neg(y < x)\}$

skip

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

end

...

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

Prirejanje

$\{P(x)\}$

$x := 7$

$\{x = 7 \wedge P(x)\}$

NI V REDU

$\{x < 3\}$

$x := 7$

$\{x = 7 \wedge x < 3\}$

???

$\{P(7)\}$ $\quad\quad$ $\{7 > 3\}$

$x := 7$ $\quad\quad$ $x := 7$

$\{P(x)\}$ $\quad\quad$ $\{x > 3\}$

Splošno:

$\{P(e)\}$

$x := e$

$\{P(x)\}$

Popolna pravilnost while:

while b do

C

done

Naravno število:
$15 > 10 > 9 > 8 > 7 > \ldots$ pridemo do 0, konec

Celo število, ki se zmanjšuje
$15 > 10 > 8 > 3 > 0 > -1 > -2 > -10 > \ldots$

Pozitivno realno število
$15 > 10 > 8.7 > \sqrt{2} > 1.17 > 0.8 > 0.08 > 0.008 > 0.0008 > \ldots$

Naloga: "C se ne ustavi"

$\{true\}\ C\ \{false\}$

$true \wedge P \Leftrightarrow P$

$(P \Rightarrow false) \Leftrightarrow \neg P$

"Če velja true in se c ustavi, potem velja false"
"Če se c ustavi, potem velja false" $\Leftrightarrow$ "c ustavi $\Rightarrow$ false" $\Leftrightarrow$ "$\neg$(c ustavi)"

Naloga: "C se ustavi"

$[true]\ C\ [true]$

"če velja true, potem se C ustavi in velja true"

$true \Rightarrow$ "C ustavi" $\wedge$ true

"C ustavi"

$(true \Rightarrow P) \Leftrightarrow P$

Naloga:

```
{ x ≤ y }
```

⇓ ✓ matematično sklepamo (vemo iz vrtca)

```
{ x ≤ (x+y)/2 ≤ y }
s := (x + y) / 2
```

✓

Kaj je P?

↓

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

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

$\{P(s)\}$

Vzamimo

$P(z) := (x \le z \le y)$

```
{ x ≤ s ≤ y }
```

$P(s)$

Naloga:

```
{ x ≤ 7 }
```

⇓ Sklepamo

```
{ x+3 ≤ 10 }
x := x + 3
```

$\{P(x+3)\}$

$x := x+3$

$\{P(x)\}$

$P(z) := (z \le 10)$

```
{ x ≤ 10 }
```

Naloge

```
{ b ≥ 0 }
i := 0 ;
{ b ≥ 0 ∧ i = 0 }
p := 1 ;
{ b ≥ 0 ∧ i = 0 ∧ p = 1 }
{ p = a^i ∧ i ≤ b }
while i < b do
   { i < b ∧ p = a^i ∧ i ≤ b }
   { i < b ∧ p·a = a^(i+1) }
   p := p * a ;
   { i < b ∧ p = a^(i+1) }
   { (i+1)-1 < b ∧ p = a^(i+1) }
   i := i + 1
   { i-1 < b ∧ p = a^i }
   { p = a^i ∧ i ≤ b }
done
{ i ≥ b ∧ p = a^i ∧ i ≤ b }
{ i = b ∧ p = a^i }
{ p = a ^ b }
```

$\{b \geq 0\}\ i := 0;\ \{b \geq 0\}$ $\quad \{0 = 0\}\ i := 0;\ \{i = 0\}$ $\quad P(z) := (z = 0)$

$P(z) := (z = z)$

$\{P(0)\}\ i := 0;\ \{P(i)\}$ $\quad \{0 = 0\}\ i := 0\ \{i = i\}$

i	p	$p = a^i$	$i \geq 0$
0	1	✓	✓
1	a	✓	✓
2	a^2	✓	✓
3	a^3		⋮
4	a^4		

✓ ⇓ ✓

nepotreben, ker imamo tudi $i \leq b$

⇓ ✓

← nazaj moramo pridelati še $i \leq b$

⇓ ✓

sledi →

Sklepamo: $i - 1 < b$

⇓

$i < b + 1$

⇓ ker sta i in b cela števila

$i \leq b$

⇓ ker $i \geq b$ in $i \leq b$ sledi $i = b$

⇓ ✓