Dokazovanje pravilnosti programov

- Specifikacija → opis, kaj naj program dela
- Implementacija → program, koda

Hoareova Logika

$\{P\}\,c\,\{Q\}$ — če velja P in se c konča, po izvedbi c velja Q

- P — predpogoj (precondition)
- c — ukaz
- Q — končni pogoj (postcondition)

$true \Rightarrow \varphi$ je ekvivalentno φ

$false \Rightarrow \varphi$ — " — $true$

Pravila sklepanja za Hoarovo logiko

$$\frac{P' \Rightarrow P \qquad \{P\}\,c\,\{Q\} \qquad Q \Rightarrow Q'}{\{P'\}\,c\,\{Q'\}} \quad \rightarrow \quad \{P'\} \Rightarrow \{P\}\ c\ \{Q\} \Rightarrow \{Q'\}$$

$$\frac{\{P_1\}\,c\,\{Q_1\} \qquad \{P_2\}\,c\,\{Q_2\}}{\{P_1 \wedge P_2\}\,c\,\{Q_1 \wedge Q_2\}}$$

$\{x = 3\}$
$x := 5$
$\{x = 3\}$

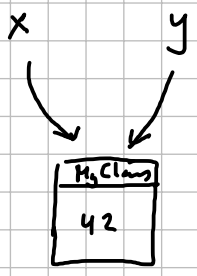
$$\frac{FV(P) \cap FA(c) = \varnothing}{\{P\}\,c\,\{P\}}$$

c ne vpliva na izjavo P, če c ne spreminja vrednosti spremenljivk iz P

Aliasing - "vzdevkanje"

Java:

```
MyClass x = new MyClass(42);
MyClass y = x;
{ P(x) }
  y.change();
{ P(x) }
```



multiply(A, B, C)
V matriko C shrani A · C

multiply(A, B, B)

$$\frac{\{ P \wedge b \}\ c_1\ \{ Q \} \qquad \{ P \wedge \neg b \}\ c_2\ \{ Q \}}{\{ P \}\ \texttt{if b then } c_1 \texttt{ else } c_2 \texttt{ end } \{ Q \}}$$

{P}
if b then
  {P ∧ b}
  C1
  {Q}
else
  {P ∧ ¬b}
  C2
  {Q}
end
{Q}

$$\frac{\{ P \}\ c_1\ \{ Q \} \qquad \{ Q \}\ c_2\ \{ R \}}{\{ P \}\ c_1 ; c_2\ \{ R \}}$$

{P}
C1;
{Q}
C2
{R}

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

P invarianta zanke

```
{ P }
while b do
    { P ∧ b }
    c
    { P }
done
{ P ∧ ¬ b }
{ true } ⇒
{ 8 > 5 }
x := 8        ← e
{ x > 5 }
  P
```

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

V P zamenjaj
x z e

```
while b do
    c
done
```

količina, ki se zmanjšuje

z je dvh (za nastavljanje spremenljivk)

$$\frac{[P \wedge b \wedge e = z]\ c\ [P \wedge e < z] \qquad z \notin FA(c)}{[P]\ \texttt{while b do c done}\ [\neg b \wedge P]}$$

c ne spremeni z

```
[ b ≥ 0 ]
i := 0 ;
p := 1 ;
while i < b do
   p := p * a ;
   i := i + 1
done
[ p = a ^ b ]
```

i	p	P = a^i	b - i
0	1	✓	b
1	a	✓	b - 1
2	a^2	✓	b - 2
3	a^3	✓	
⋮	⋮		

Količina b - i se zmanjšuje. in velja $b - i \geq 0$. Zakaj?

$b - i \geq 0$
$b \geq i$
$i \leq b$