

Programmverifikation

jhenkel@gmx.de

Beweisschema für Schleifen - Totale Korrektheit

Allgemeines Beweisschema

$\text{pre} \Rightarrow \text{wp}(\text{body}, \text{post})$

body

post

Partielle Korrektheit

pre

$\Rightarrow \text{pre} / = \text{wp}(\text{init}, \text{post} /)$

from

init

invariant

inv

post /
 $\Rightarrow \text{inv}$

Terminierung

pre

$\Rightarrow \text{pre} / = \text{wp}(\text{init}, \text{post} /)$

from

init

invariant

inv

post /
 $\Rightarrow \text{var} > 0 \text{ or } \text{var} = 0 \text{ and } \text{cond}$

Zusätzliche Anforderung
an das Programm:
 $\text{var} = 0 \Rightarrow \text{cond}$

variant

var

until

cond

loop

body

$\text{inv} \text{ and not } \text{cond}$

$\Rightarrow \text{pre} 2 = \text{wp}(\text{body}, \text{post} 2)$

post2
 $\Rightarrow \text{inv}$

end

$\text{inv} \text{ and } \text{cond}$
 $\Rightarrow \text{post}$

Beweisschema für if-Sprachkonstrukt

$\text{pre} \Rightarrow \text{cond} \text{ and } \text{pre} /$
or not $\text{cond} \text{ and } \text{pre} 2$

if

cond

then

body1

else

body2

$\text{pre} 2 = \text{wp}(\text{body} 2, \text{post})$

post

end

end

loop

body

$\text{inv} \text{ and not } \text{cond} \text{ and}$

$\text{var} > 0 \text{ and } \text{var} = Y$

$\Rightarrow \text{pre} 2 = \text{wp}(\text{body}, \text{post} 2)$

post2

$\text{var} \geq 0 \text{ and } \text{var} < Y$