Incremental Verification

Uri Juhasz

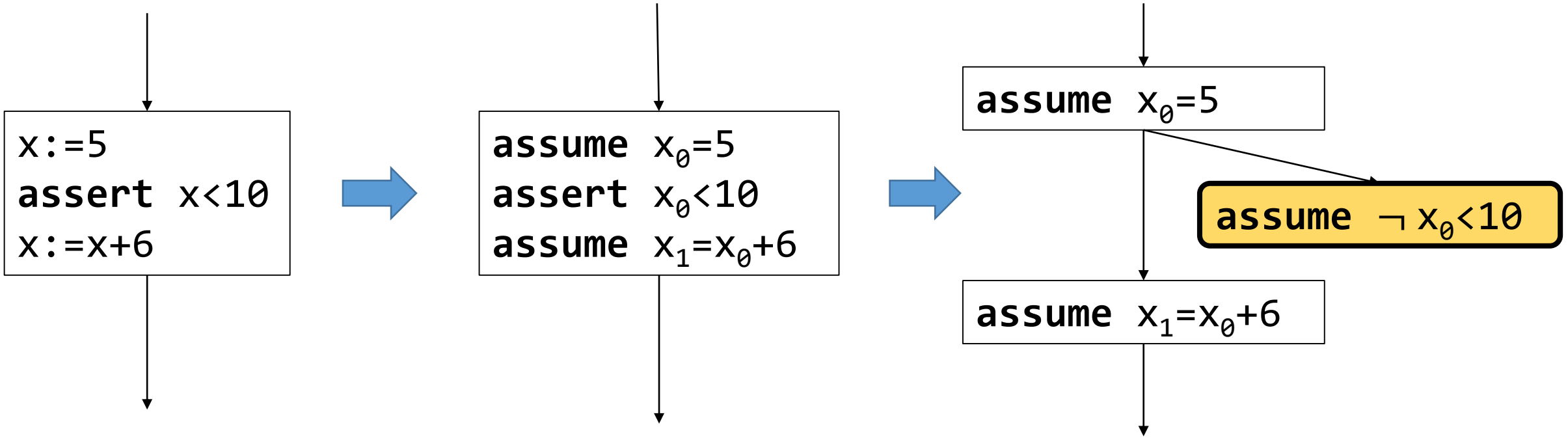
Examiner: Prof. Dr. Peter Müller

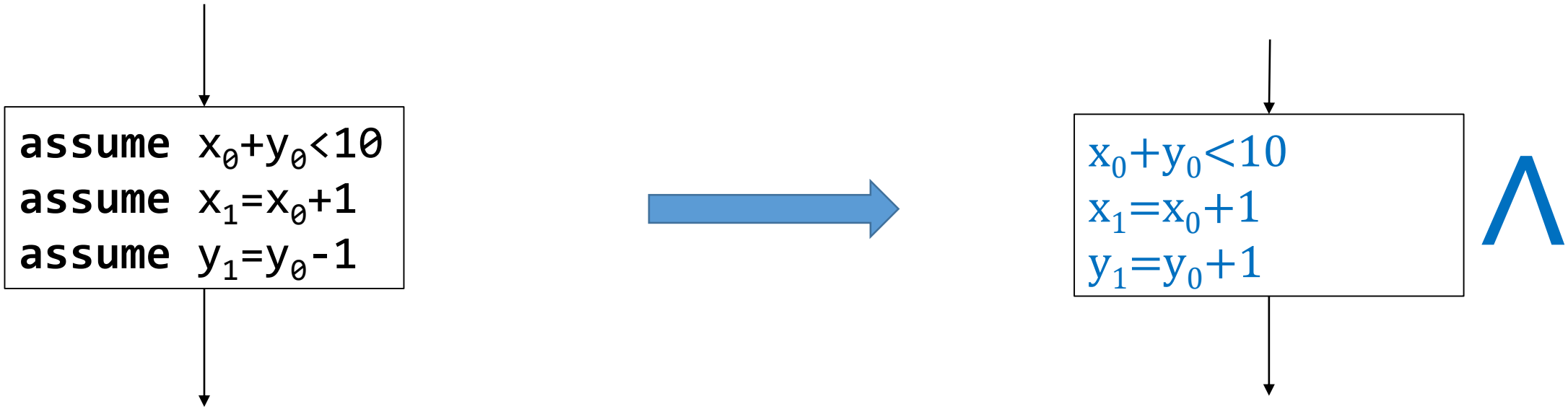
Co-examiners: Prof. Dr. Martin Vechev

Prof. Dr. Clark Barrett

Prof. Dr. Arie Gurfinkel

7.11.2016


x:=5
assert x<10
x:=x+6
assume x_0=5
assert x_0<10
assume x_1=x_0+6
assume x_0=5
assume ¬ x_0<10
assume x_1=x_0+6

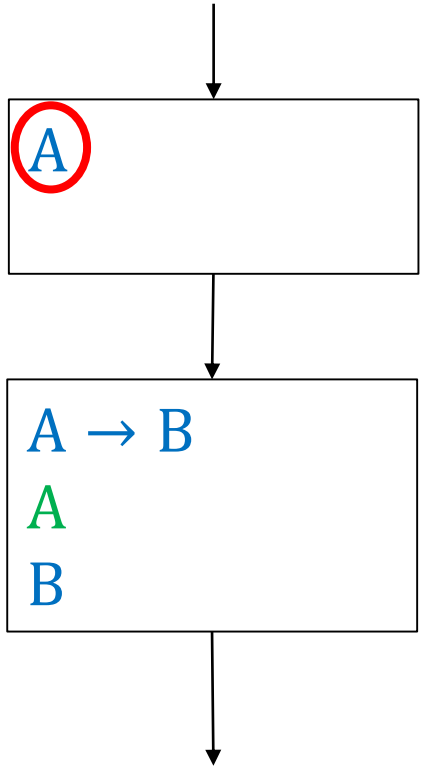

assume $x_0+y_0<10$
assume $x_1=x_0+1$
assume $y_1=y_0-1$
$x_0+y_0<10$
$x_1=x_0+1$
$y_1=y_0+1$
∧

Deduction

$$\frac{A \quad A \rightarrow B}{B}$$

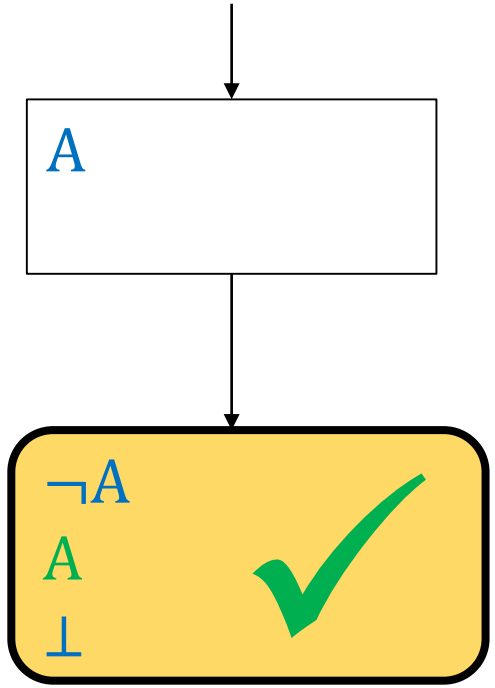
$A \rightarrow B$
A
B

Propagation



Propagation

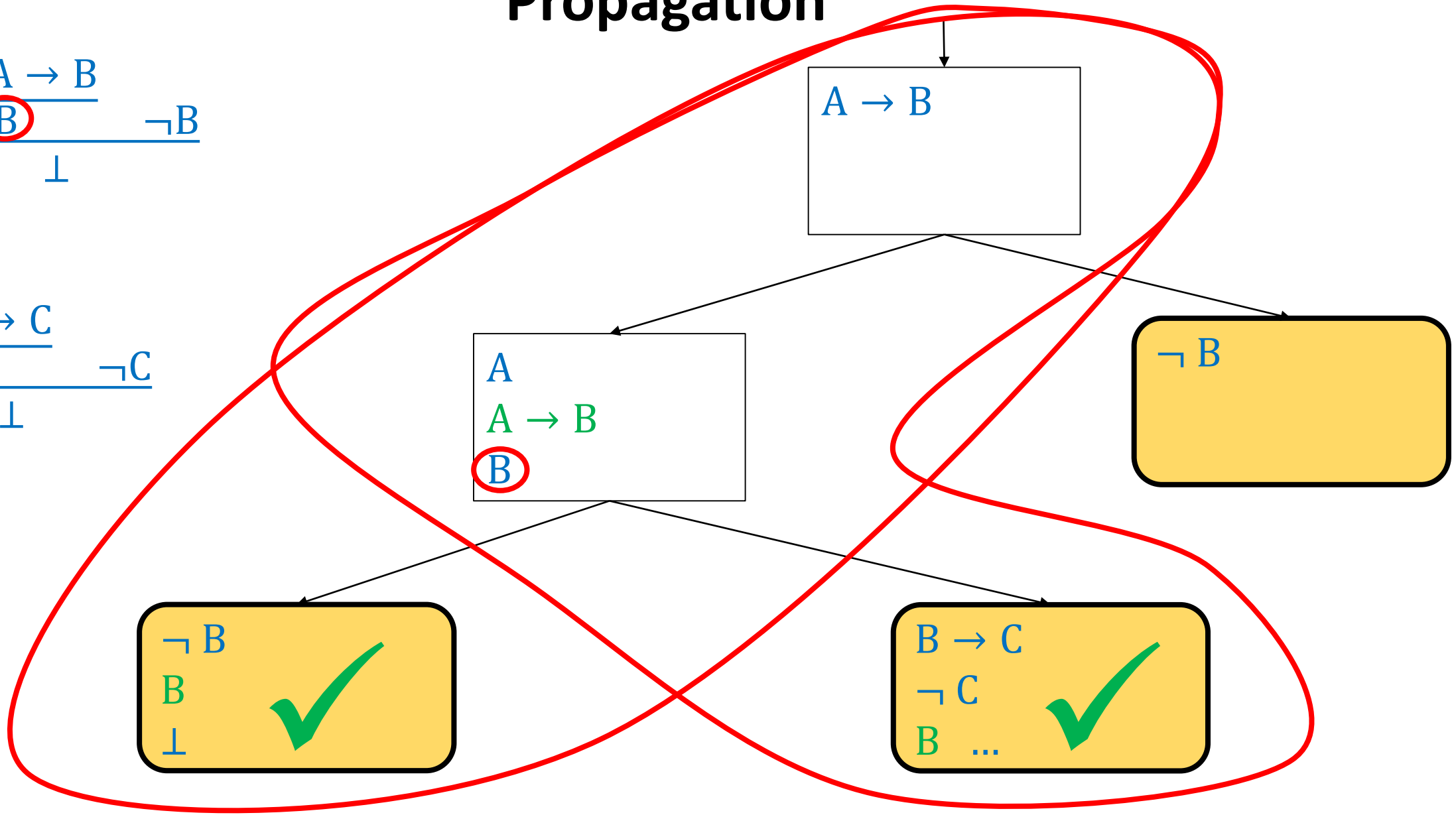
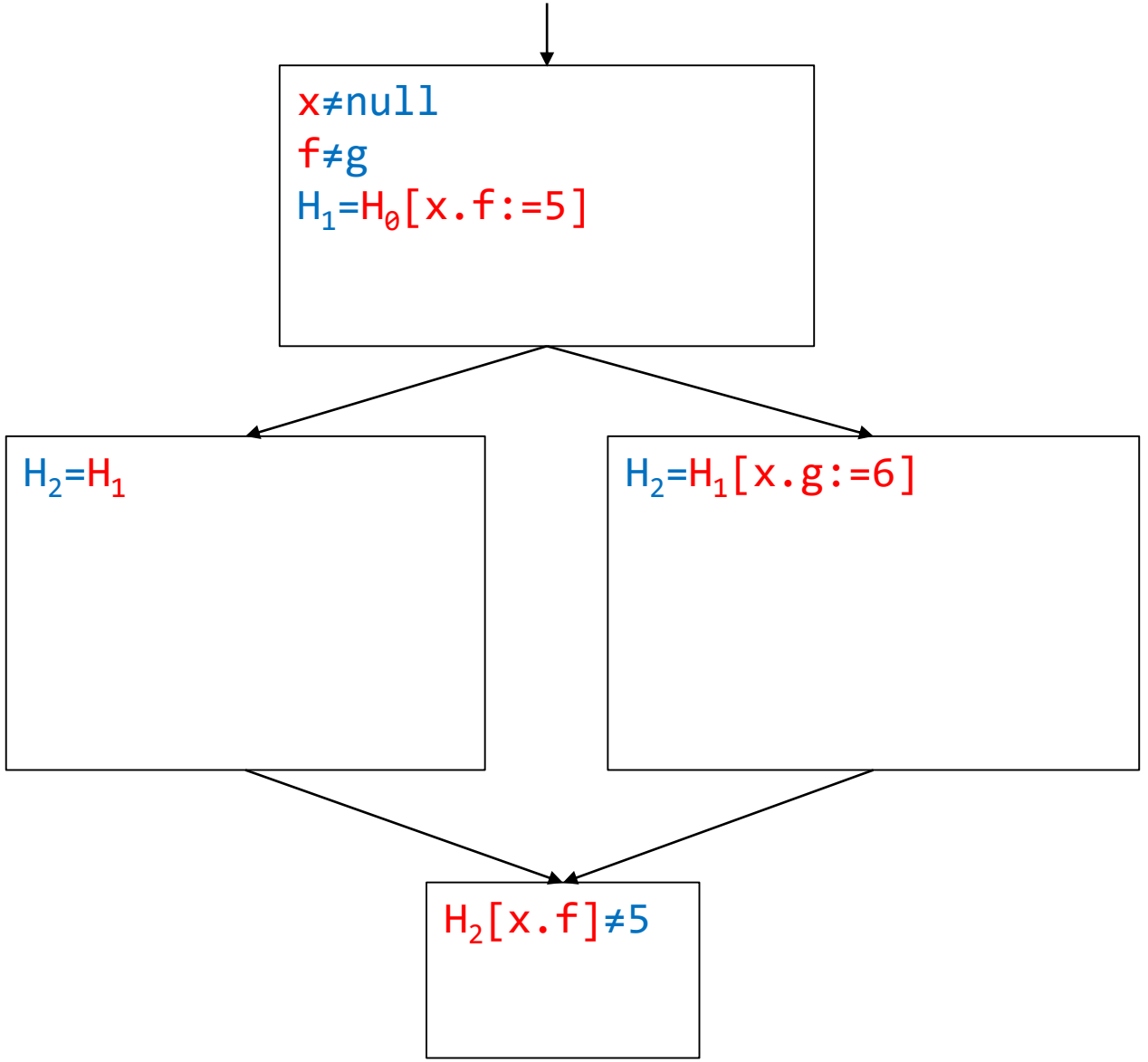
$$\frac{A \quad \neg A}{\bot}$$



Propagation

$$\frac{A \quad A \to B}{B} \qquad \frac{B \quad \neg B}{\bot}$$

$$\frac{B \quad B \to C}{C} \qquad \frac{C \quad \neg C}{\bot}$$



```
method p(a,b : Int)
  a:=5
  if (*)
     x.g:=6
  assert x.f=5
```