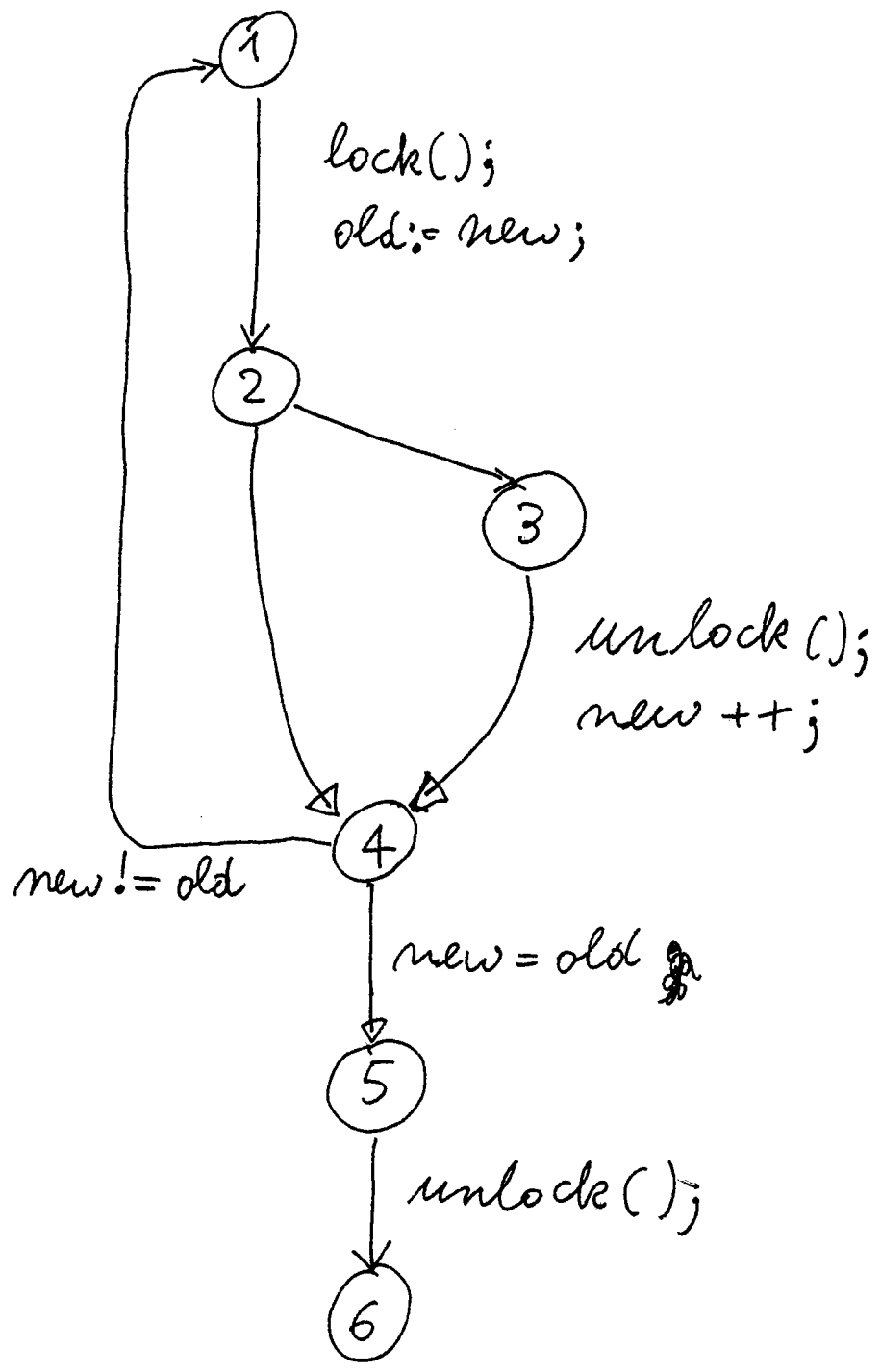
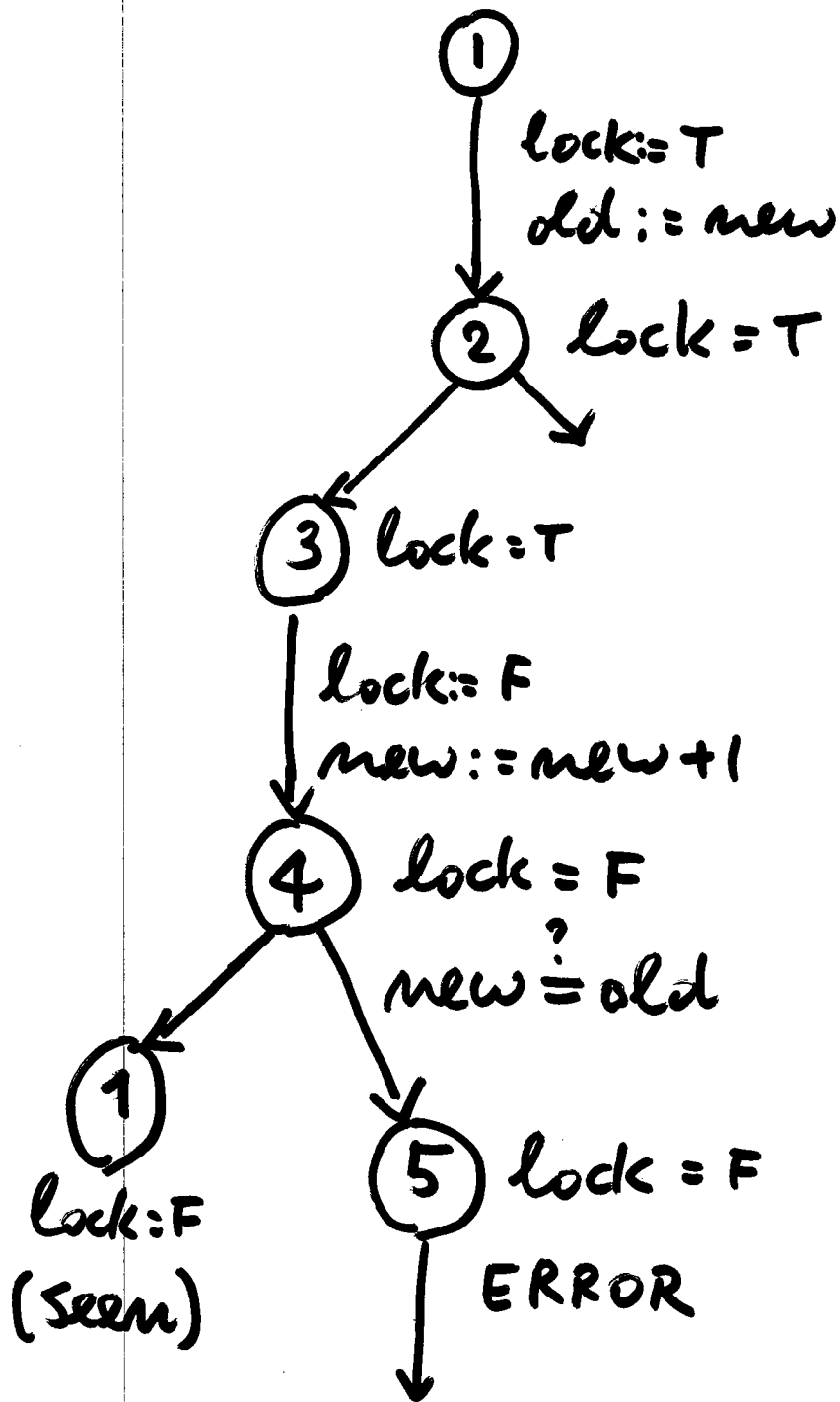


```
1: do {
    lock();
    old = new;
2:   if (*) {
3:       unlock();
        new++;
    }
4: } while (new != old);
5: unlock();
6: exit;
```

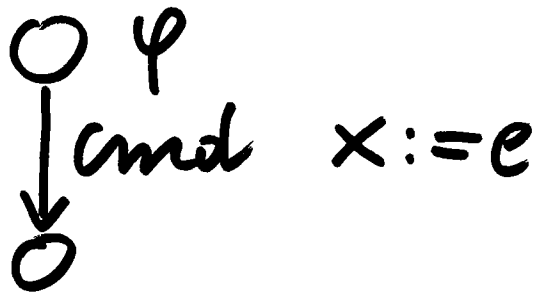


Explore, with pred: lock = T



How to explore and track predicates.

ex:  
(new=old)



$\gamma$

P can be true

iff:

$\varphi \rightarrow \wedge P[e/x] \text{ sat}$

P can be false

iff:

$\varphi \rightarrow \neg P[e/x] \text{ sat}$

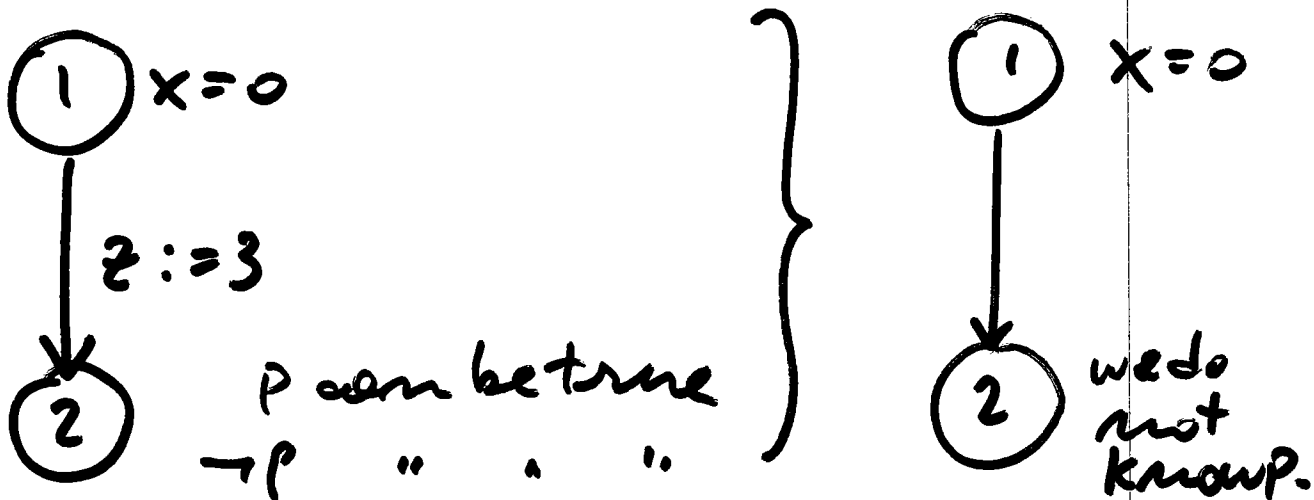
P can be true  
iff:

$\varphi \wedge \gamma \wedge P \text{ sat.}$

Ex:

$P: y = 0$

$\varphi: x = 0$



Can P hold at 2? yes.

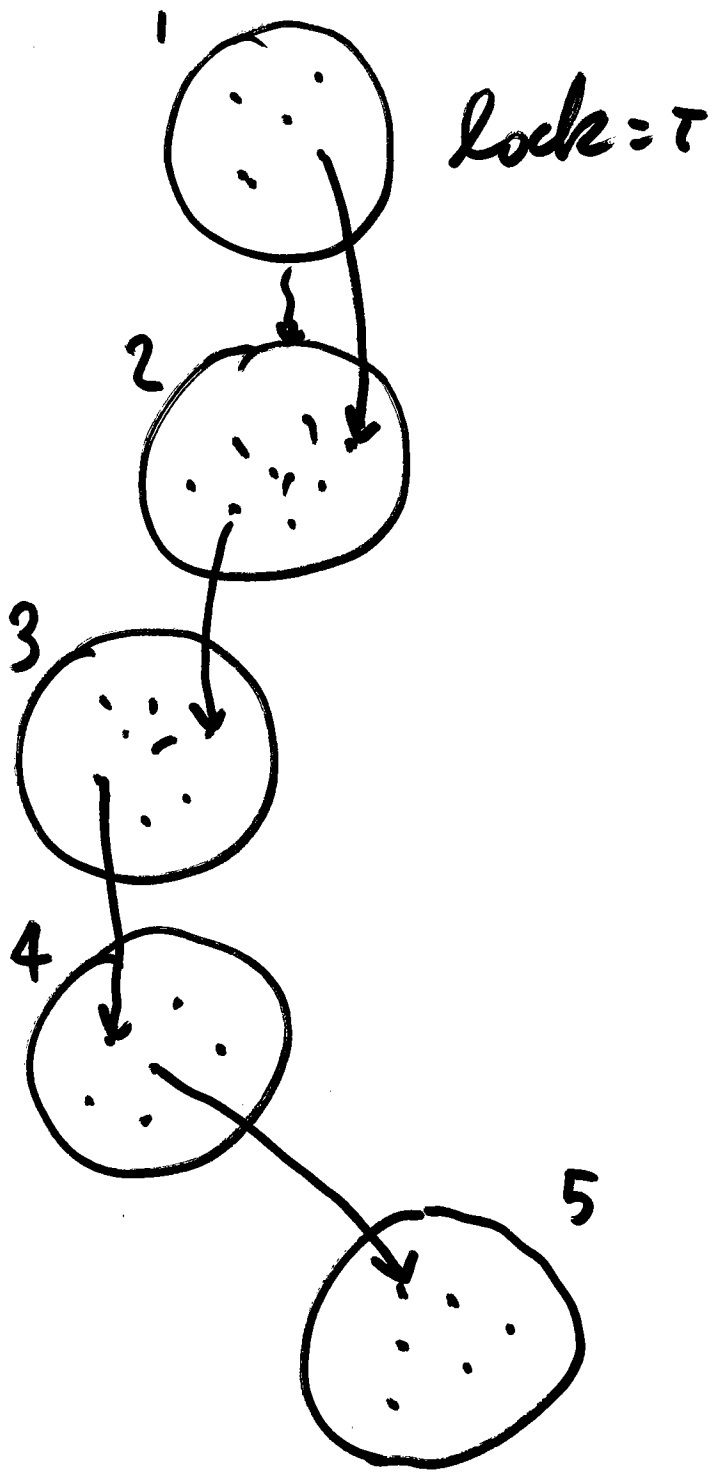
$x=0 \hat{\wedge} [(y=0) [3/z]]$

$x=0 \wedge y=0$  sat?

Can P be false?

$x=0 \wedge (y \neq 0) [3/z]$  sat

$x=0 \wedge y \neq 0$  sat yy



# Single Static Assignment (SSA) form:

①

$lock_1 := T$

$old_1 := new_0$

②

③

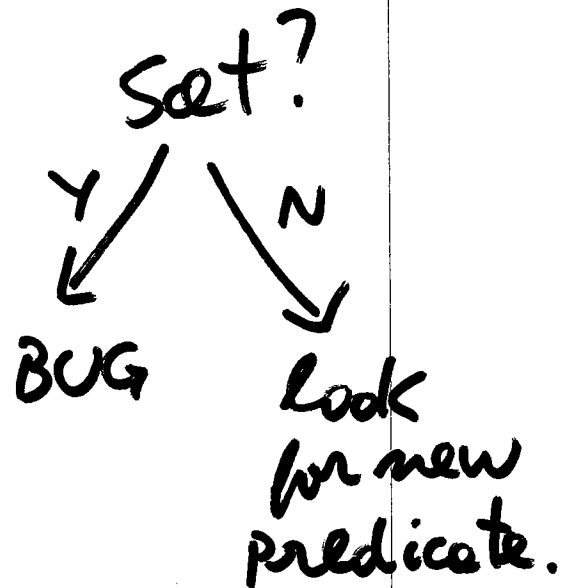
$lock_2 := F$

$new_1 := new_0 + 1$

④

$new_1 \stackrel{?}{=} old_1$

⑤



Thm: The path can be followed iff the conj of the SSA formulas is satisfiable.

$(lock_1 = T) \wedge (old_1 = new_0) \wedge (lock_2 = F)$

$\wedge (new_1 = new_0 + 1) \wedge (new_1 = old_1)$

# Interpolation Theorem (FOL)

Suppose this is valid:

$$\varphi(\bar{x}, \bar{y}) \rightarrow \psi(\bar{y}, \bar{z})$$

Then, there is some  $\gamma(\bar{y})$

st

$$\varphi(\bar{x}, \bar{y}) \rightarrow \gamma(\bar{y}) \rightarrow \psi(\bar{y}, \bar{z}).$$

are valid.

~~Master~~ Craig's  
interpolant.

$\varphi \wedge \psi$  is unsat. ( $\varphi \rightarrow \neg \psi$  valid)

By interpolation, you can  
find  $\gamma$  on the shared vars  
st.

$$\varphi \rightarrow \gamma$$

$$\gamma \rightarrow \neg \psi$$

$\gamma$  is a witness of your  
inability to follow the  
path.

$\varphi$



$\psi$

# Computing Craig's Mutex.

① True

~~lock<sub>1</sub> := true~~  
 $\boxed{\text{old}_1 = \text{new}_0}$

②  
③

~~old<sub>1</sub> := new<sub>0</sub> ∧ lock<sub>2</sub> := F~~  
∧ new<sub>1</sub> := new<sub>0</sub> + 1

④

$\exists \text{new}_0. (\text{old}_1 = \text{new}_0 \wedge \text{new}_1 = \text{new}_0 + 1)$

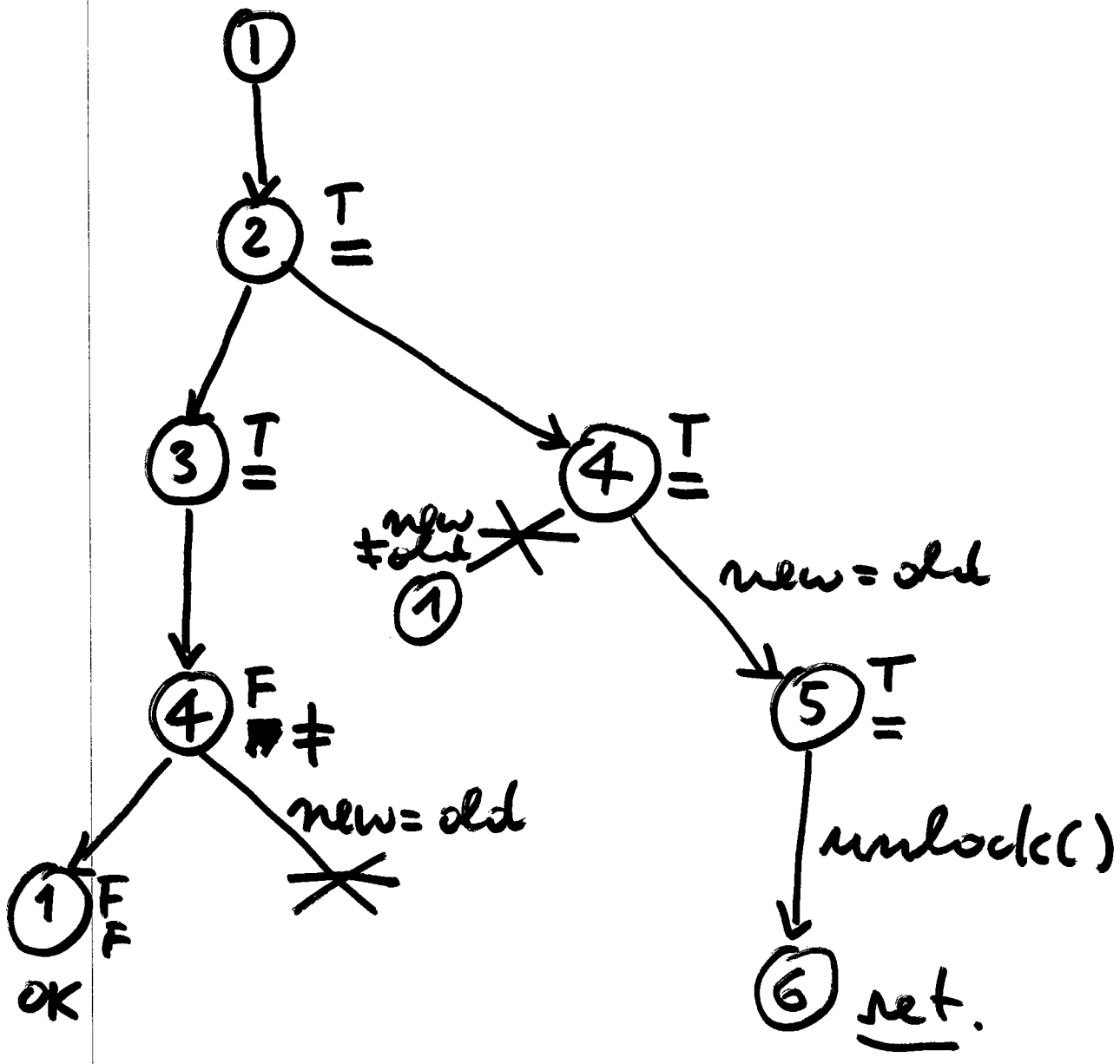
$\downarrow$   
 $\boxed{\text{new}_1 = \text{old}_1 + 1}$

- 
- $\psi$  }  
- }  
 $\psi$  }
- implied by  $\psi$
  - on common (newest) vars
  - implies  $\neg\psi$ .

---

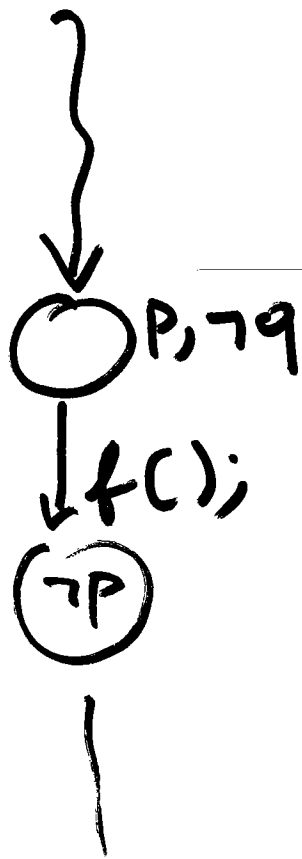
Pick a Craig interpolant of new pred.

1) lock = T      2) old = new



# Dealing with Procedures

- 1) inline
- 2) PDA reachab.
- 3) Summaries.



Summary

