Lecture 16

Monday, March 23, 2020 4:47 PM

- Hello!

- Homework 1 sample solutions uploaded to website

- Homework 2 uploaded to website

April 15 W	April 29 W	May 13 W
HW 2 due	HW3 due	HW 4
		May 13 Project reports due

Release HW3: April 1

Release HW 4: April 15

- Project presentations
  - Option 1: Skip the project presentation

    Only go by report

  - Option 2: We schedule one-on-one meetings

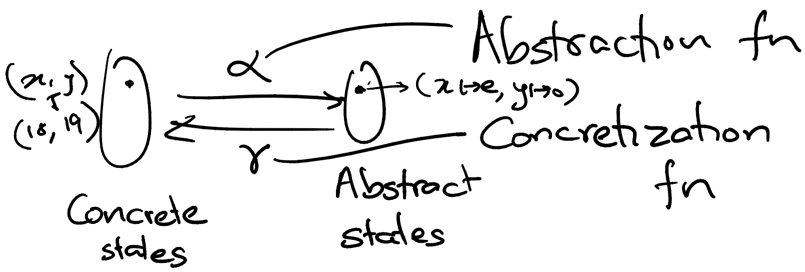
    May 6 – 13

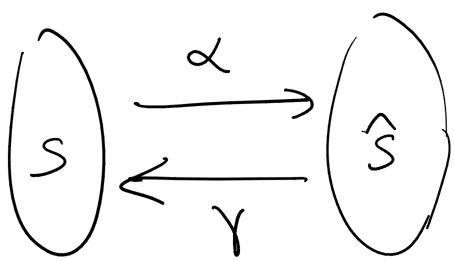
    Report + Presentation.

- Predicate abstraction
- Software model checking
- Counter-example guided abstraction refinement

- Abstract interpretation

Cousot & Cousot POPL 1977





Concrete states

Possibly infinite

Abstract states

(For predicate abs. necessarily finite)

$s = (x \mapsto 18, y \mapsto 19, \dots)$

$$\alpha(s) = (\pi_1(s), \pi_2(s), \pi_3(s))$$

$\alpha((x \mapsto 18, y \mapsto 19, \ldots))$

$\pi_1 = (x \text{ is even})$

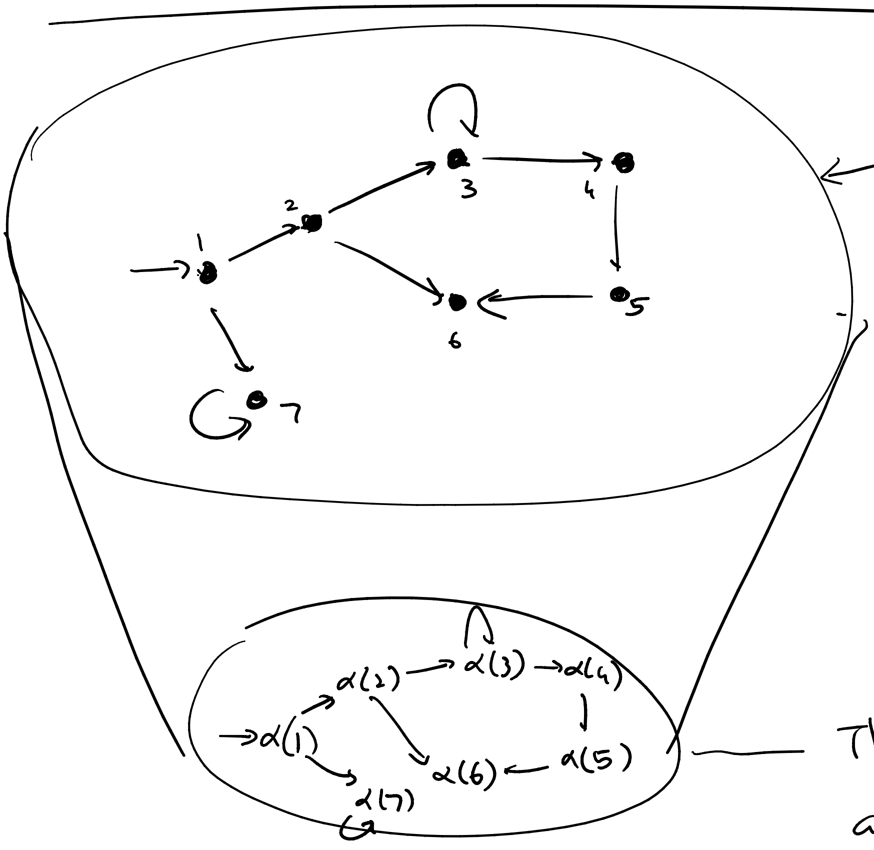
$\pi_2 = (y \text{ is even})$

$\pi_3 = (x > y)$

$$\alpha(s) = (\pi_1(s), \pi_2(s), \pi_3(s)) = (\text{true}, \text{false}, \text{false})$$

$\boxed{\begin{array}{l} \#\text{ of concrete states: infinite} \\ \#\text{ of abstract states: } 2^3 = 8 \end{array}}$

$$\gamma((\text{true}, \text{false}, \text{false})) = \{(x \mapsto 2, y \mapsto 3), (x \mapsto 14, y \mapsto 17), \cancel{(x \mapsto 12, y \mapsto 18)}, \cancel{(x \mapsto 13, y \mapsto 19)}, \ldots\}$$

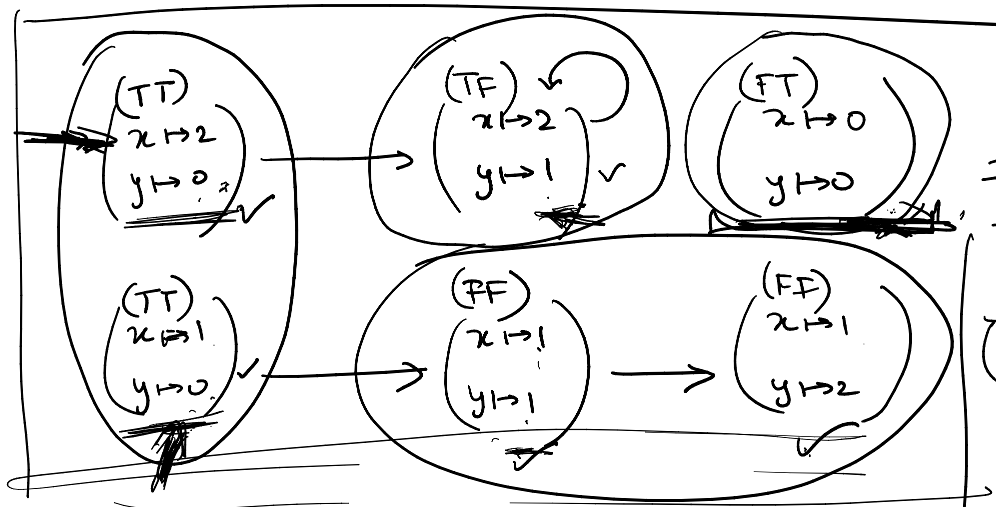


Concrete space
Infinite.

There are only 8 abstract states

Abstract transition graph

Abstract transition graph is finite.



x:=2, y:=0
if (x ≠ 2 or y ≠ 1) { y:=y+1 }

(x=2 and y=1)
⇑
x≠2 or y≠1

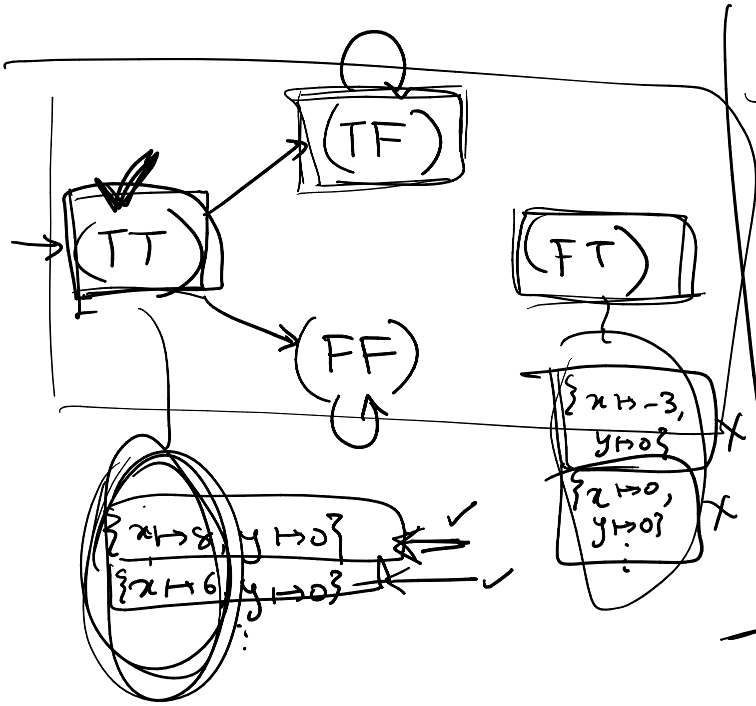
Predicates:

$P_1 = (x > y)$

$P_2 = (y = 0)$

Abstract State $= \mathbb{B} \times \mathbb{B}$

(4 abstract states in all).



assert (x>y or y≠0)

Yes, program satisfies the property. No violating state is reachable.

Option 1: Every concrete state in γ(FT) violates the assertion

Option 2: Some concrete state in γ(FT) violates the assertion.

Question: Is there any concrete state $s \in \gamma(TT)$

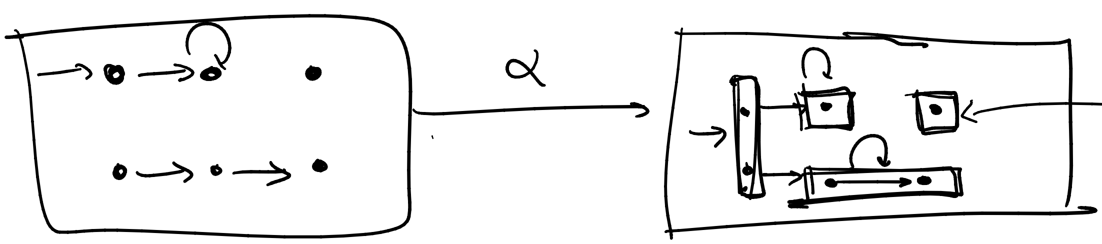
Question: Is there any concrete state
$s \in \gamma(\top)$
which violates the assertion?

Every concrete state $s \in \gamma(\top)$
satisfies the assertion.

$$(x > y \text{ and } y = 0 \text{ and } \overline{\text{assertion}})\ \exists xy.$$

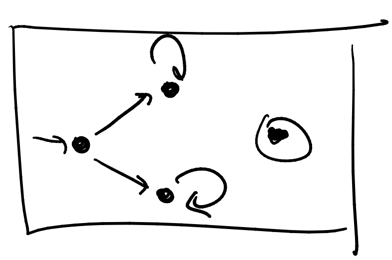
$$(x > y \text{ and } y = 0 \text{ and } \overline{x > y \text{ or } y \neq 0})\ \exists xy$$

$$(\underbrace{x > y \text{ and } y = 0}_{\text{Abstract state}} \text{ and } \underbrace{x \not> y \text{ and } y = 0}_{\text{Assertion violation.}})\ \exists xy$$

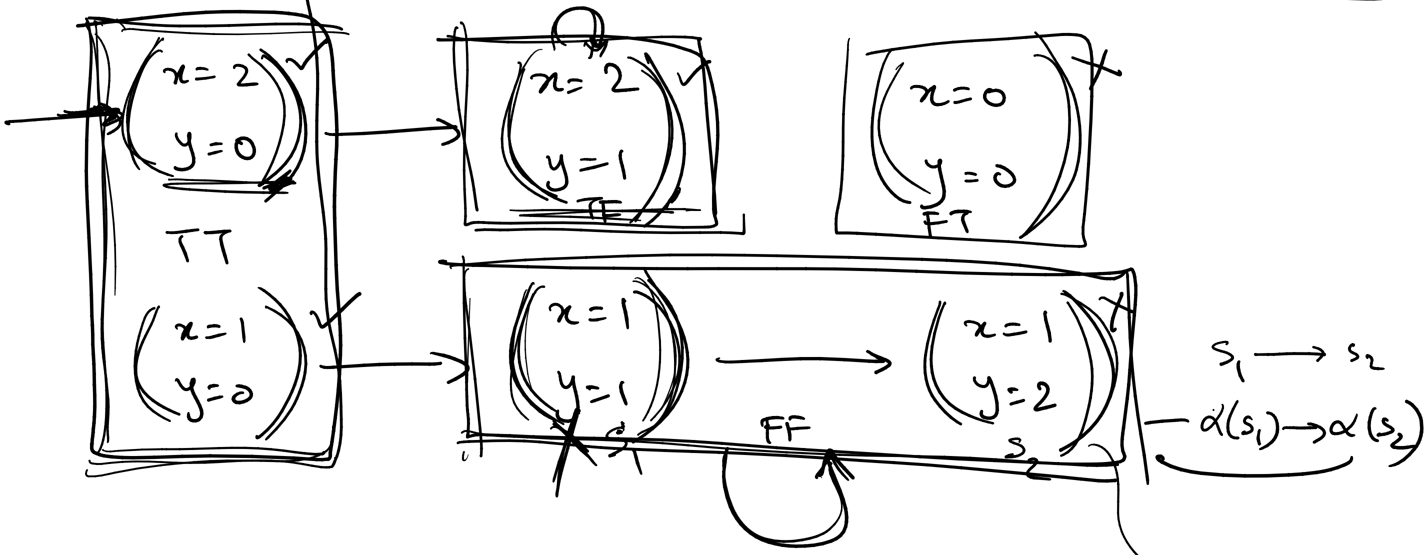


There are concrete states here which violate the assertion.

- Every reachable concrete state satisfies the assertion.

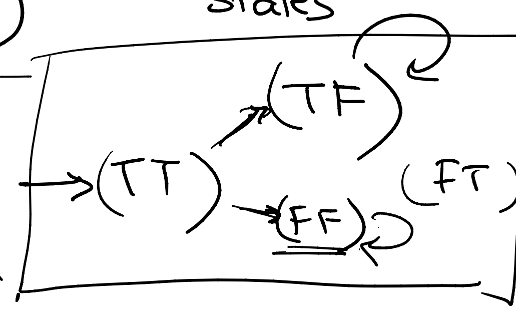


- Therefore, the program satisfies the property.



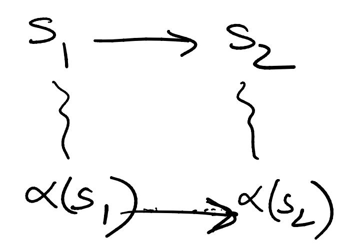
Concrete states

Predicates: $P_1 = (x > y)$ $P_2 = (y = 0)$



Assertion: Always $x > y$.

- From the abstract transition graph, it *appears* that $(x=1, y=1)$ is reachable
- But in the concrete transition graph $(x=1\ y=1)$ is unreachable.
- Program satisfies the assertion.

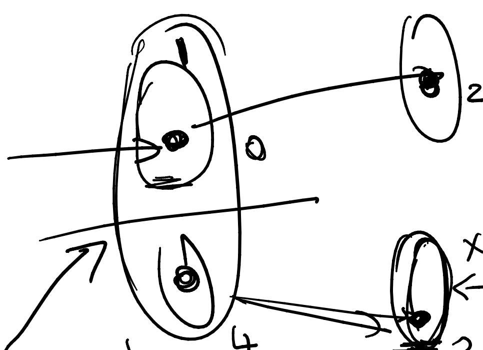


Edge drawing rule: $\forall$ pair of concrete states s_1 s_2

If $\underbrace{s_1 \rightarrow s_2}_{\text{concrete}}$ then draw $\underbrace{\alpha(s_1) \rightarrow \alpha(s_2)}_{\text{abstract}}$.

<u>Claim</u>: If every reachable abstract state is safe, then the program satisfies the assertion.

~~Claim~~: If there is an unsafe abstract state which is reachable in the <u>abstract transition graph</u>, then the program violates the assertion



(0 → 3) : Counterexample

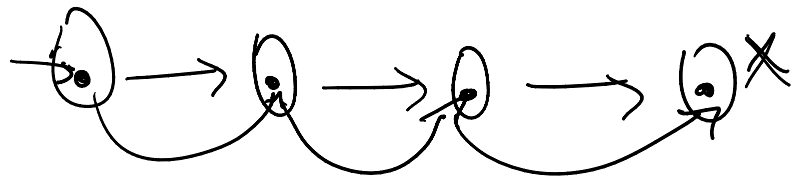
<u>It appears</u> as if this state is reachable. But this is an illusion.

This abstract state is aggregating too many concrete states.

If counterexample is feasible, <u>then the</u>

If counterexample is feasible, then the program is unsafe.

If counterexample is infeasible, then don't know / can't say.

Cex: 

Feasible

& there are no other feasible counterexamples, then the program is safe.