CSE 503

Software Engineering

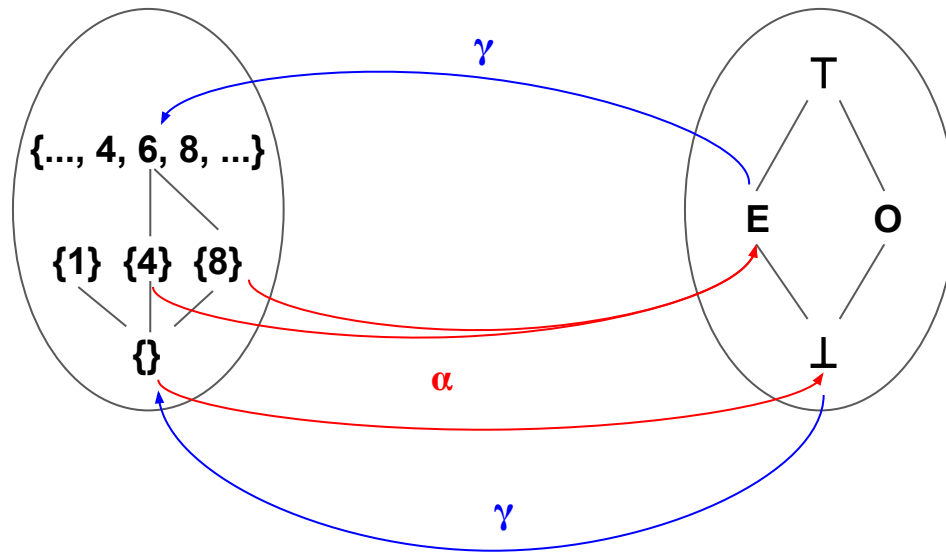### Winter 2021

Abstract Interpretation

January 15, 2021

Recap: abstraction and concretization functions
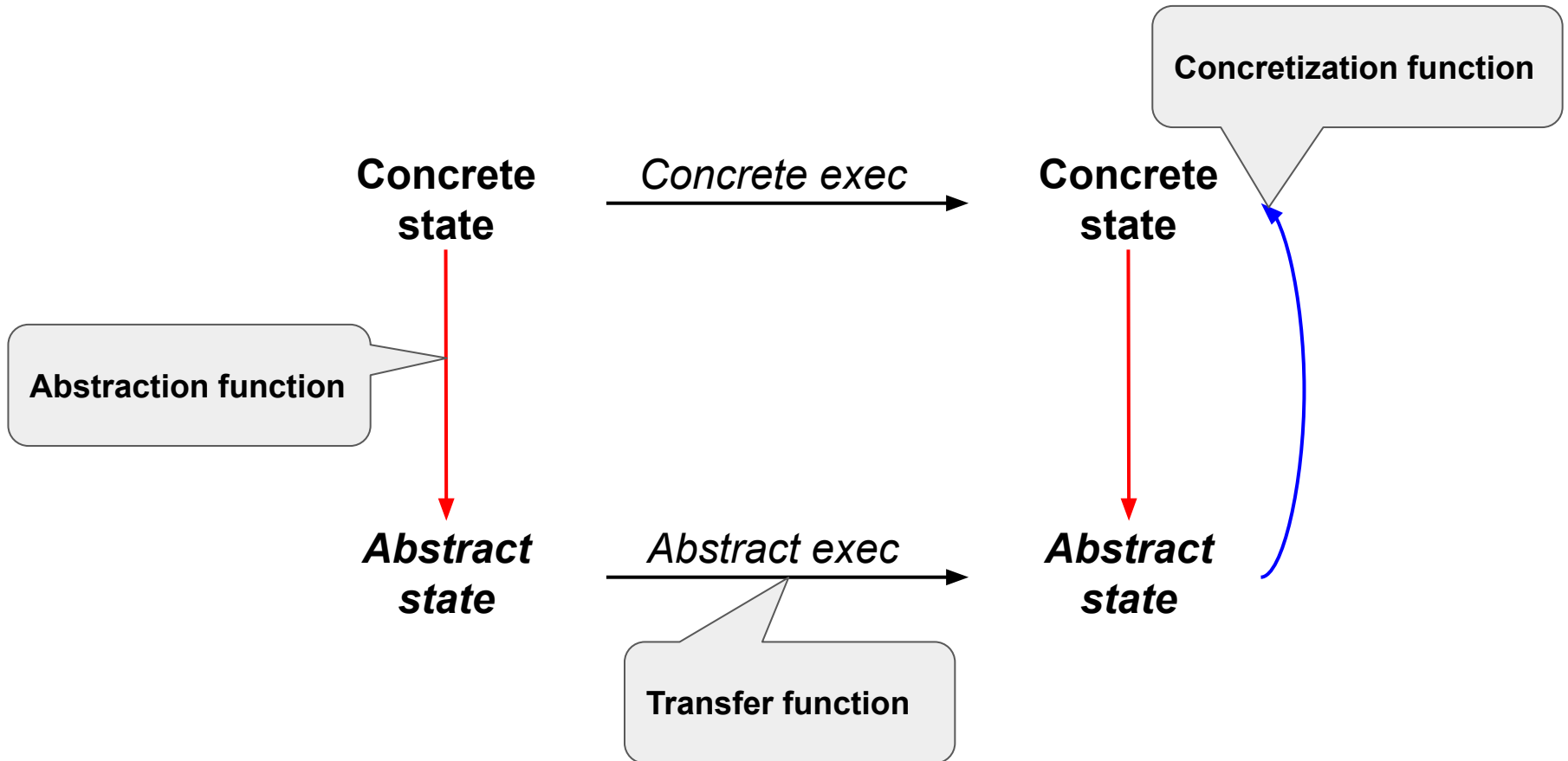

- Abstraction function α: C -> A
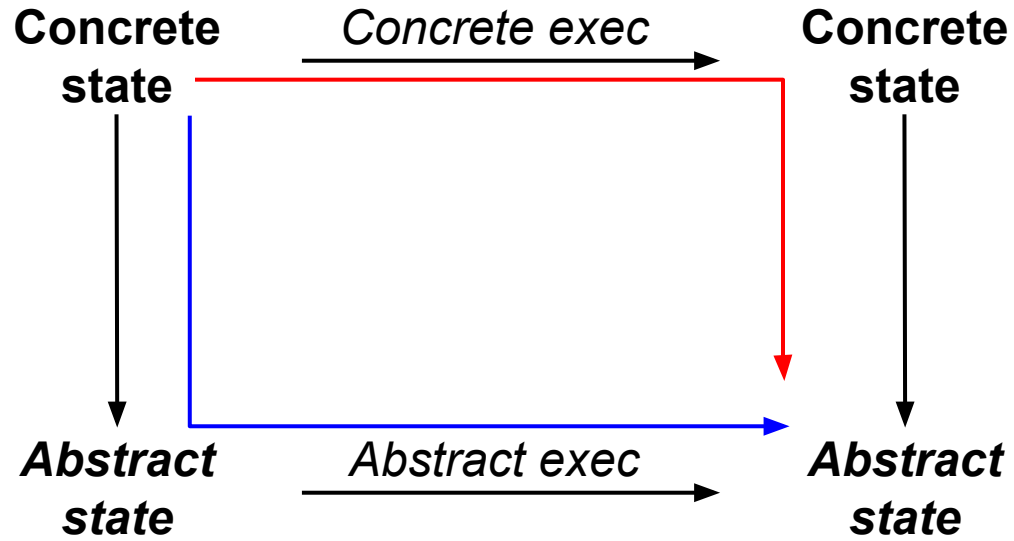- Concretization function γ: A -> C

Recap: transfer function

Recap: approximation

Recap: approximation

Concrete state — *Concrete exec* → **Concrete state**

Abstract state — *Abstract exec* → **Abstract state**
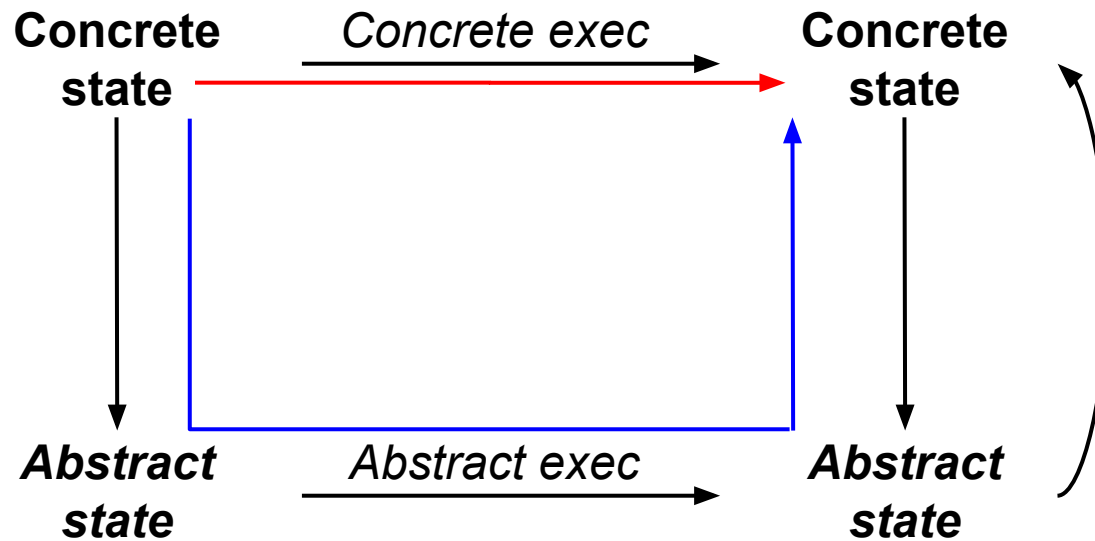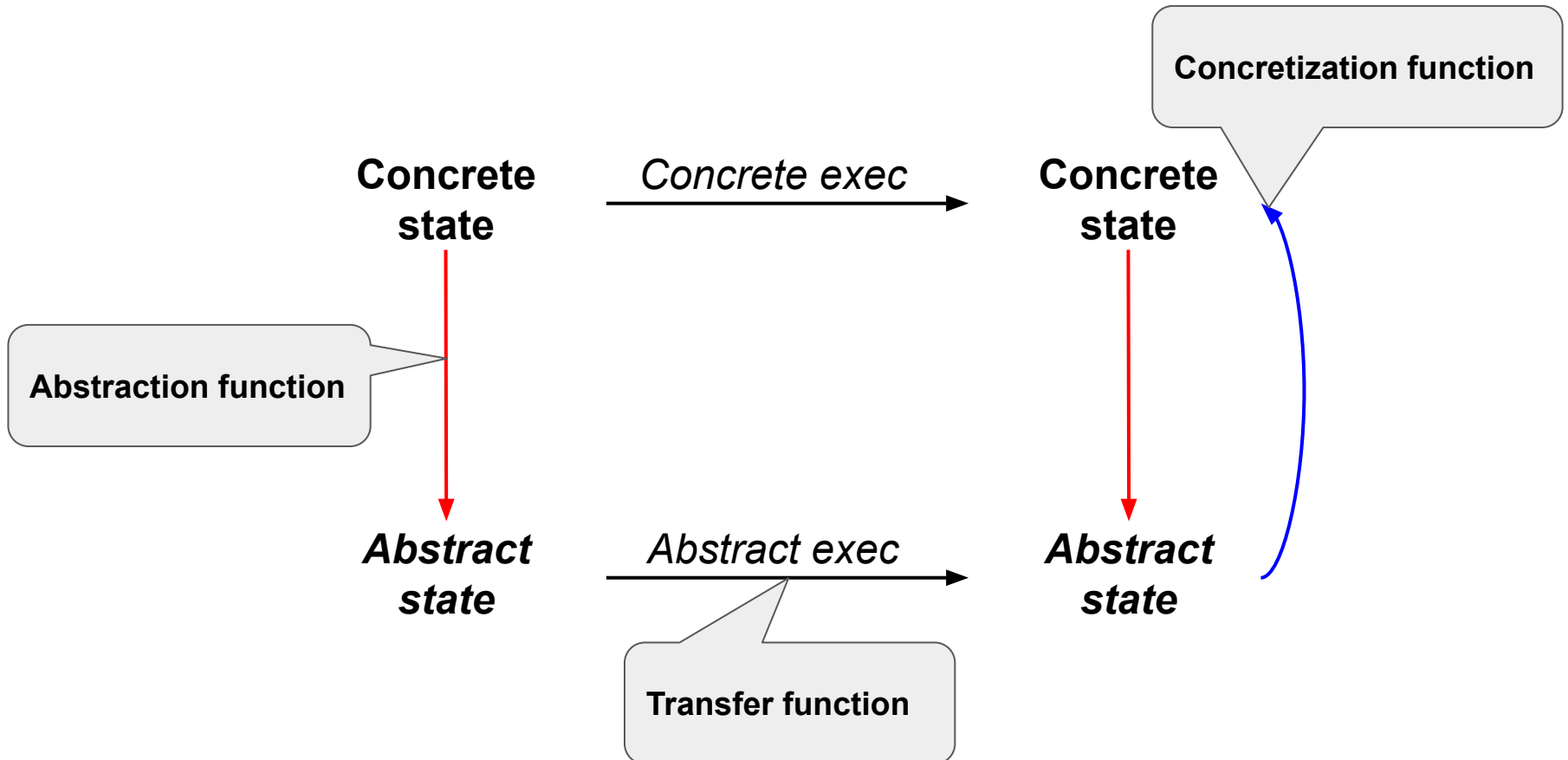
Today

More on Abstract Interpretation
- Galois connection
- Transfer function vs. lub (vs. glb)
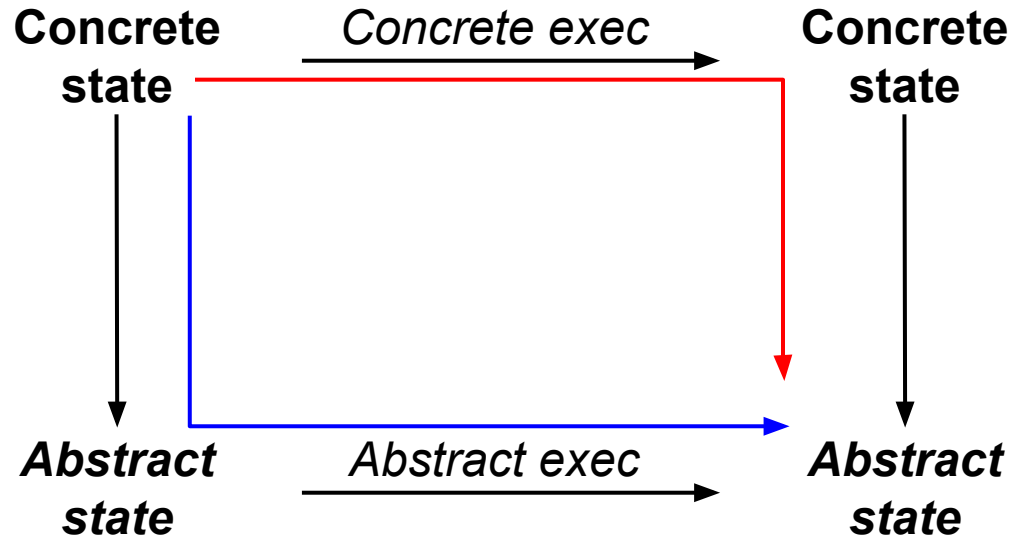- Exercise: concrete examples

Next week
- Wrap up Abstract Interpretation
- CheckerFramework tutorial
- Hands-on applications
- Move on to dynamic and hybrid analyses

Abstract interpretation: big picture
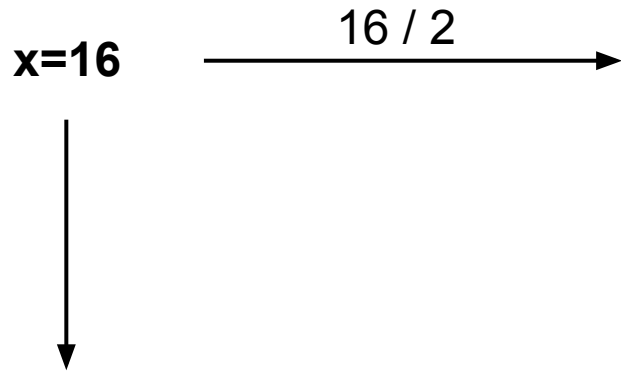
Abstract interpretation: soundness

Sound approximation and safe approximation are synonyms.

Abstract interpretation: soundness example

Abstract domain: {*odd, even$_2$, even$_4$, ?*}

x=16   16 / 2 →

Abstract interpretation: soundness example

Abstract domain: {*odd, even$_2$, even$_4$, ?*}

x=16 $\xrightarrow{\quad 16 / 2 \quad}$ **x=8**

x=even$_4$

Abstract interpretation: soundness example

Abstract domain: {*odd, $even_2$, $even_4$, ?*}

x=16 $\xrightarrow{16\ /\ 2}$ **x=8** $\xrightarrow{8\ /\ 2}$ **x=4**

x=$even_4$

Abstract interpretation: soundness example

Abstract domain: {*odd, even$_2$, even$_4$, ?*}

$x=16$ $\xrightarrow{\ 16\ /\ 2\ }$ $x=8$ $\xrightarrow{\ 8\ /\ 2\ }$ $x=4$

$x=16 \downarrow$

$x=even_4$ $\xrightarrow{\ even_4\ /\ 2\ }$ $x=even_2$

Abstract interpretation: soundness example

Abstract domain: {*odd, even$_2$, even$_4$, ?*}

$x=16$ $\xrightarrow{\text{16 / 2}}$ $x=8$ $\xrightarrow{\text{8 / 2}}$ $x=4$

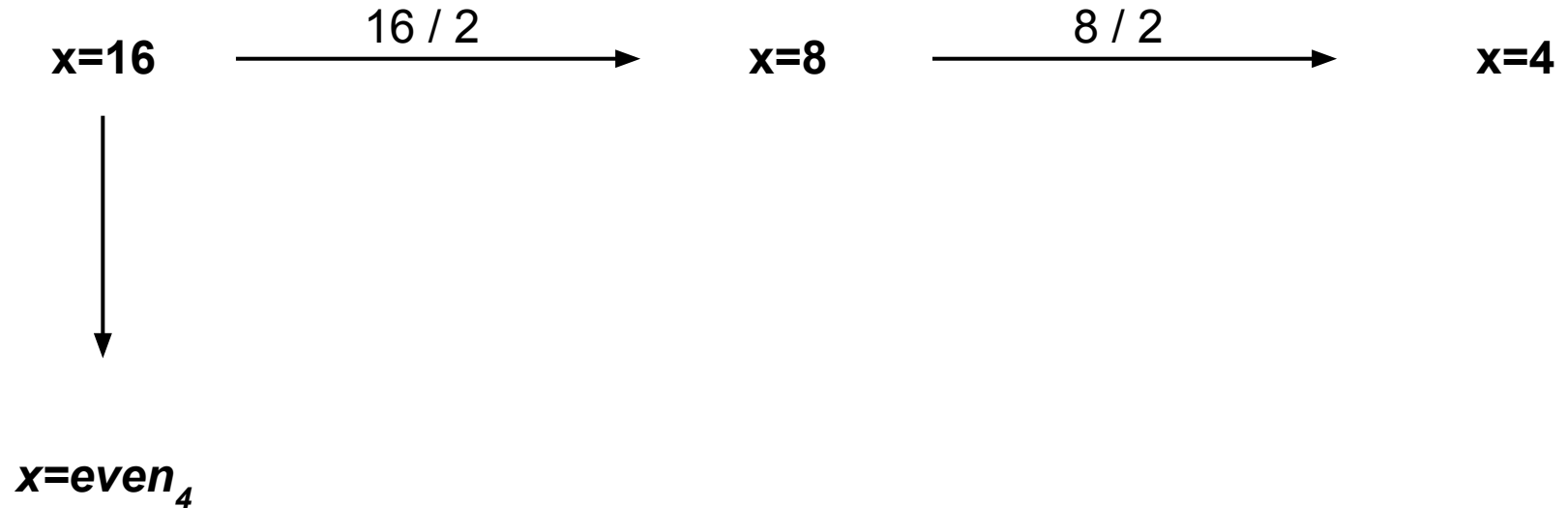$x=$*even*$_4$ $\xrightarrow{\text{even}_4 \text{ / 2}}$ $x=$*even*$_2$ $\xrightarrow{\text{even}_2 \text{ / 2}}$ $x=?$
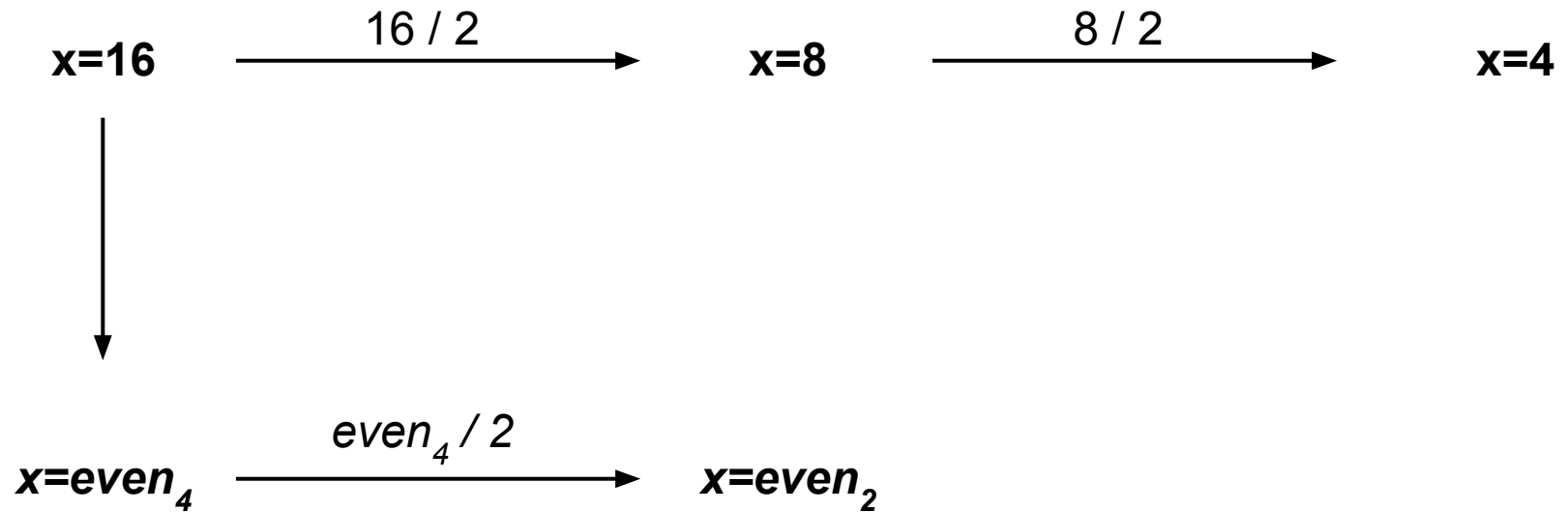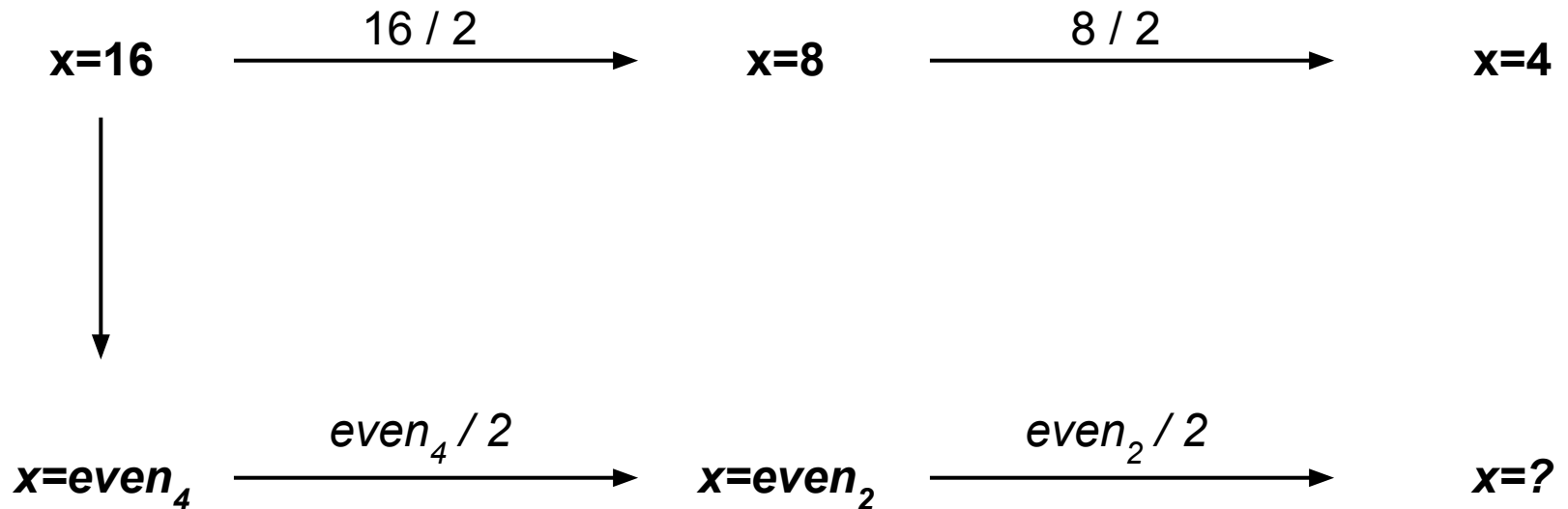
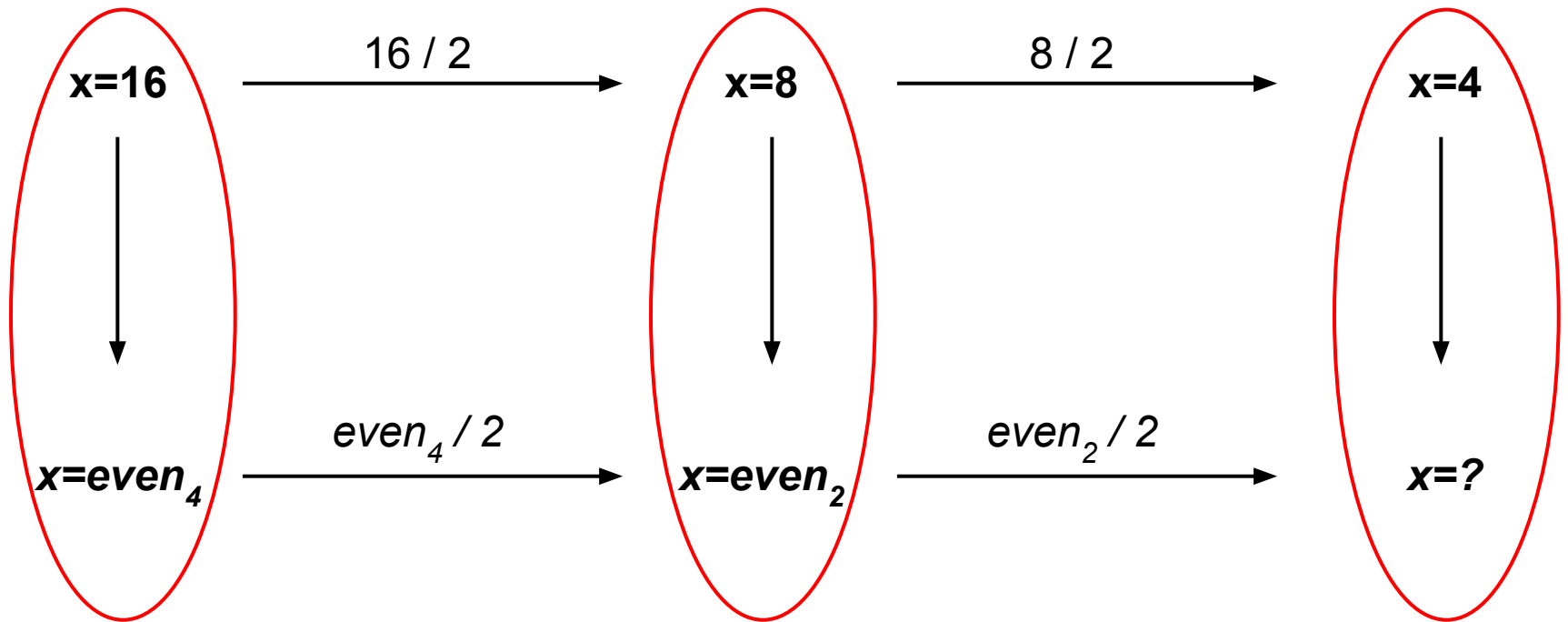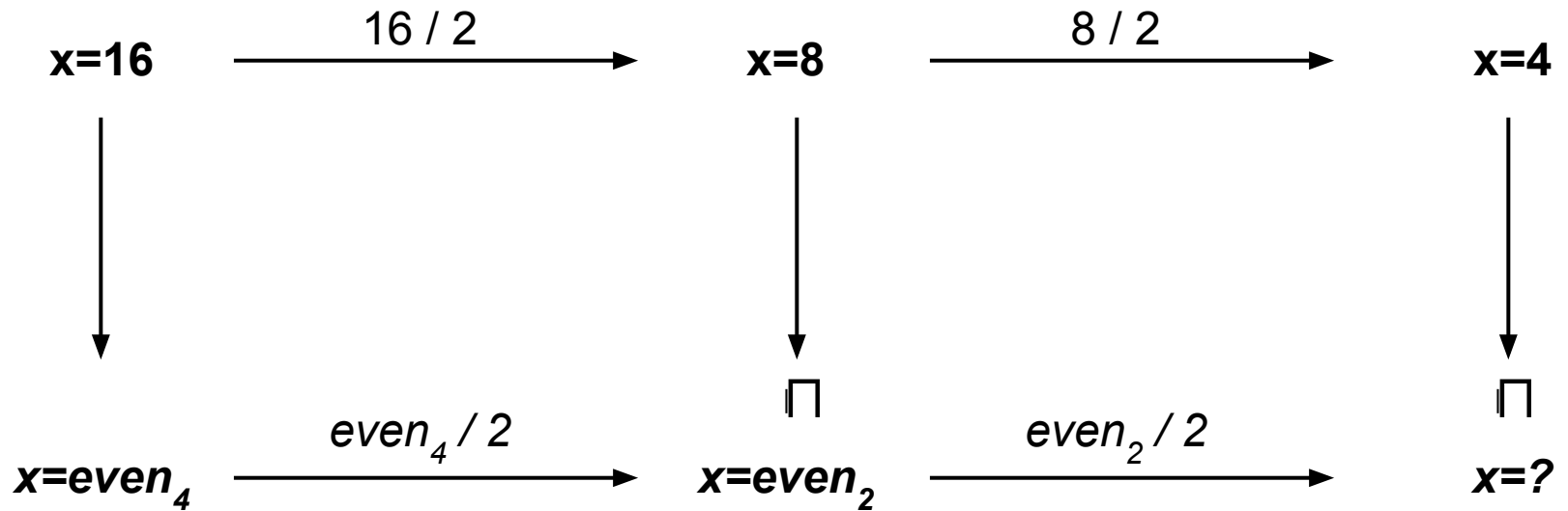# Abstract interpretation: soundness example

Abstract domain: {*odd, even$_2$, even$_4$, ?*}

Abstract interpretation: soundness example

Abstract domain: {*odd, even$_2$, even$_4$, ?*}

$x=16$ $\xrightarrow{\quad 16\,/\,2 \quad}$ $x=8$ $\xrightarrow{\quad 8\,/\,2 \quad}$ $x=4$

$x=even_4$ $\xrightarrow{\quad even_4\,/\,2 \quad}$ $x=even_2$ $\xrightarrow{\quad even_2\,/\,2 \quad}$ $x=?$

Abstract interpretation: soundness
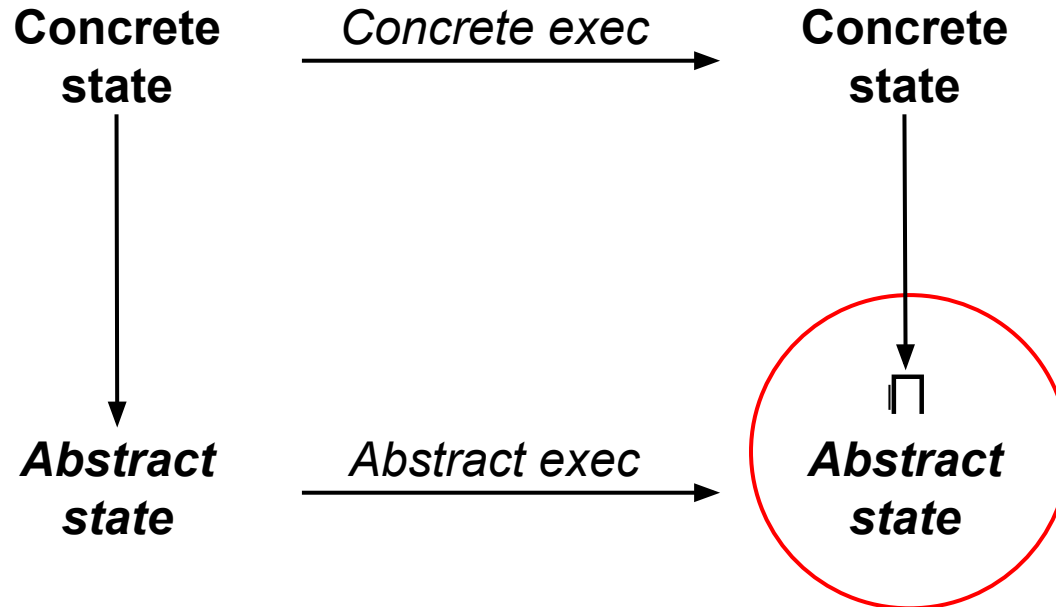
What properties must be satisfied by the abstraction, concretization, and transfer functions?

Sound approximation: properties

Concrete ($P(\mathbb{N})$)   Abstract
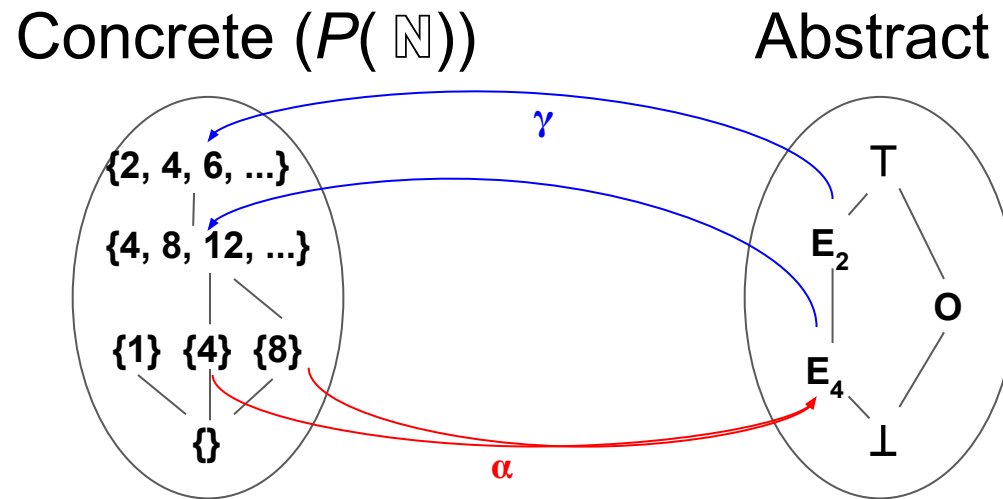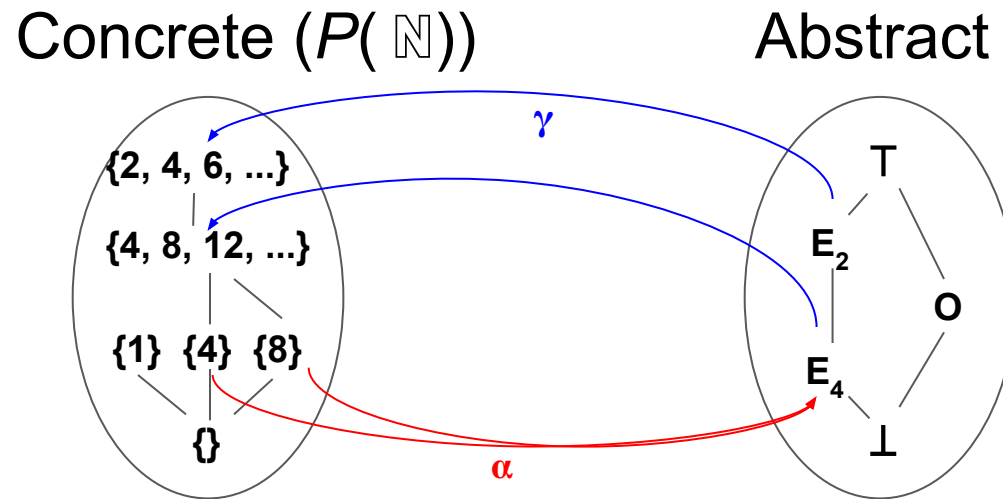
$\{2, 4, 6, ...\}$

$\{4, 8, 12, ...\}$

$\{1\}$ $\{4\}$ $\{8\}$

$\{\}$

γ

α

$\top$

E_2

O

E_4

$\bot$

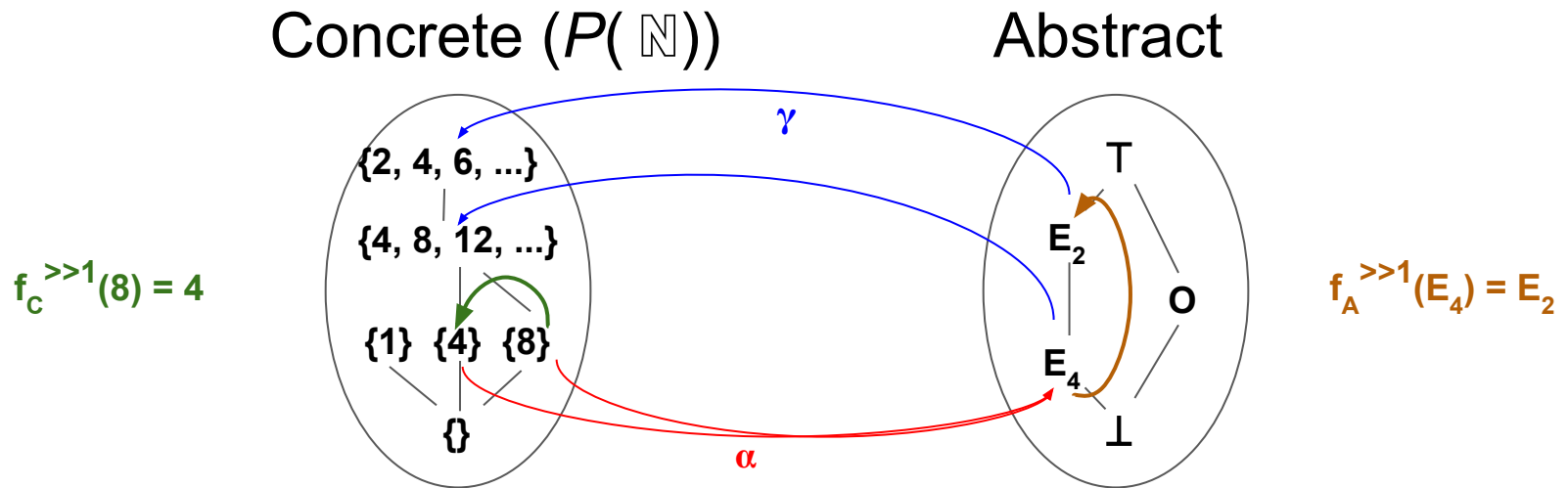**What properties must α and γ satisfy?**

Sound approximation: galois connection

Galois connection

- $\alpha: C \rightarrow A$
- $\gamma: A \rightarrow C$
- $\forall c \in C: c \leq \gamma(\alpha(c))$
- γ and α are order preserving

Sound approximation: properties

Concrete ($P(\mathbb{N})$)   Abstract

$f_C^{>>1}(8) = 4$

$f_A^{>>1}(E_4) = E_2$

{2, 4, 6, ...}

{4, 8, 12, ...}

{1} {4} {8}

{}

$\top$

E_2

O

E_4

$\bot$

γ

α

What properties must the transfer function(s) satisfy?

Sound approximation: consistency

Concrete ($P(\mathbb{N})$)   Abstract

$f_C^{>>1}(8) = 4$

$f_A^{>>1}(E_4) = E_2$
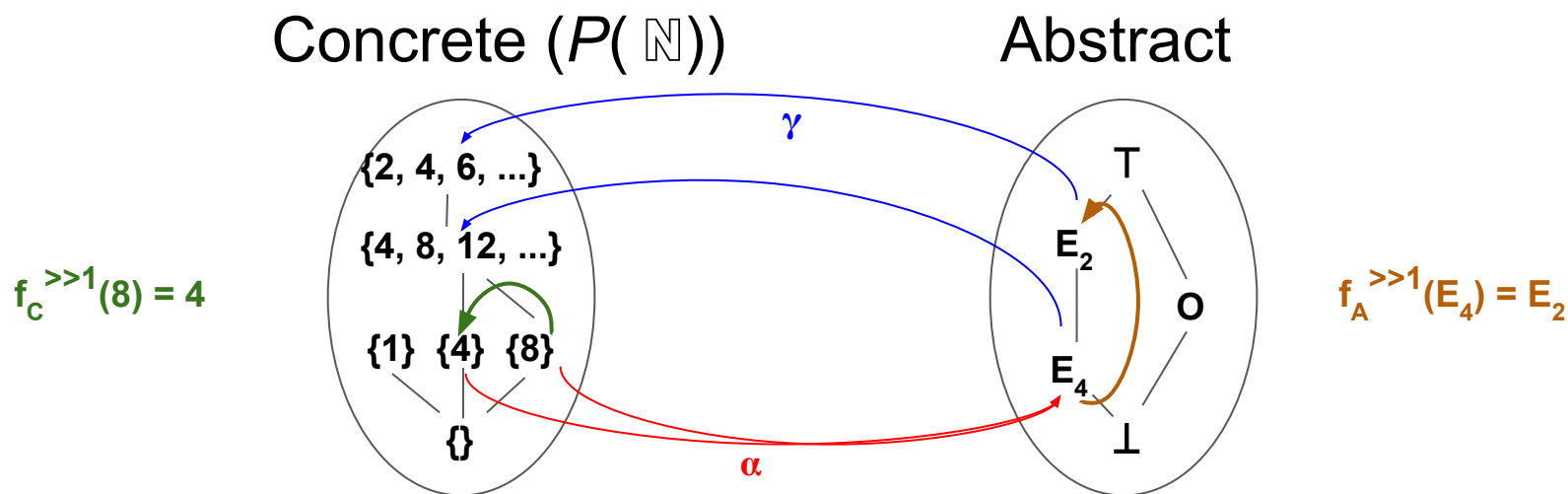
Transfer function

- Consistent with concrete function
  - c: concrete state; c' = f_C(c)
  - a: α(c)
  - a' = f_A(a)
  - c'' = γ(a')
  - c' $\leq$ c''

Sound approximation: properties
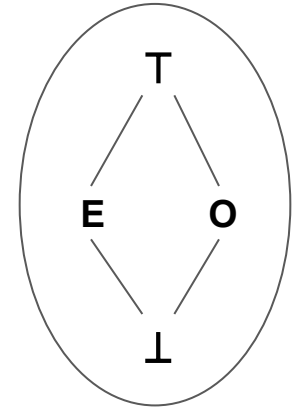
Transfer function

- $f_A^+: A \times A \to A$

Lub

- lub: $A \times A \to A$

+	E	O	T	...
E	E	O	T	
O	O	E	T	
T	T	T	T	
...				

lub(E, O) = T

What properties must the lub function satisfy?
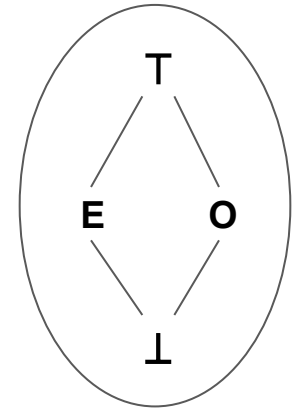
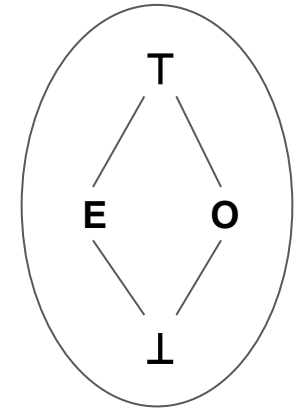# Sound approximation: monotonicity

Transfer function

- $f_A^+: A \times A \rightarrow A$
- may not be monotone

Lub

- lub: $A \times A \rightarrow A$
- must be monotone

+	E	O	T	...
E	E	O	T	
O	O	E	T	
T	T	T	T	
...				

lub(E, O) = T

Sound approximation: example

Transfer function

- $f_A^+: A \times A \to A$
- may not be monotone

Lub

- lub: $A \times A \to A$
- must be monotone

+	E	O	T	...
E	E	O	T	
O	O	E	T	
T	T	T	T	
...				

lub(E, O) = T


```
int x = even();

if (x < 10) {
  x = x + 1;
} else {
  x = x + 2;
}
print(x);
```
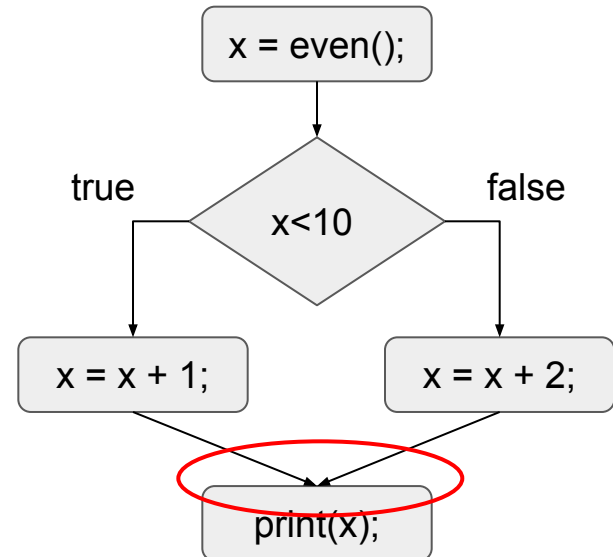
Small-group exercise

- ● Work through two examples:
  - ○ Join vs. meet operation (`f(int a, int b, int c): int`)

    ```
    if (cond) {
      x = a * b;
    } else {
      x = a * c;
    }
    return(x);
    ```

    Which parameters (`a`, `b`, `c`)
    - ● will definitely be used?
    - ● may be used?
    (cond is independent of the parameters)

  - ○ Termination/fix point iteration

    ```
    int x = 2;
    while (x < 10) {
      x = x + 2;
    }
    ```

    Is the value of x after the loop an even number? Use an abstract domain with {odd, 2, $even_2$, and $even_4$}

- ● Report to class (random call)

Answers to the questions for the above two examples:
https://docs.google.com/document/d/1bkAIBigNjFoi5wLyKwhj0ticybMmF4yTX4o74B5e5oo