



# CSCI 740 - Programming Language Theory

---

Lecture 28

Galois Connection

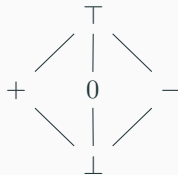
Instructor: Hossein Hojjat

November 8, 2017

# Abstract Domain

- An abstract domain is a lattice
- Elements in the lattice are called abstract values

**Example:** Sign Abstract Domain

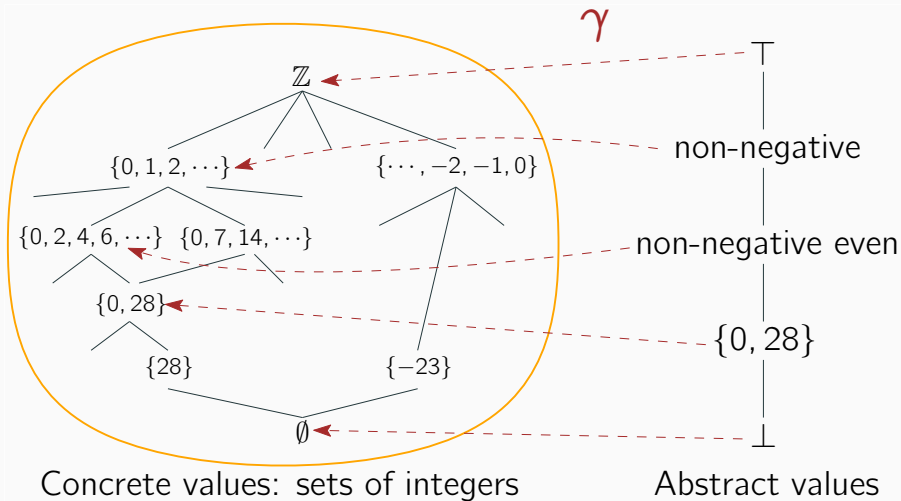


- Set of abstract values  $\{\perp, +, 0, -, \top\}$
- Relation  $\leq$  that is
  - Reflexive
  - Anti-symmetric
  - Transitive
- Least upper bound (lub,  $\sqcup$ ) and greatest lower bound (glb,  $\sqcap$ ) exists for any pair of elements
  - So it's a lattice

Need to relate elements in the lattice with concrete states in the program

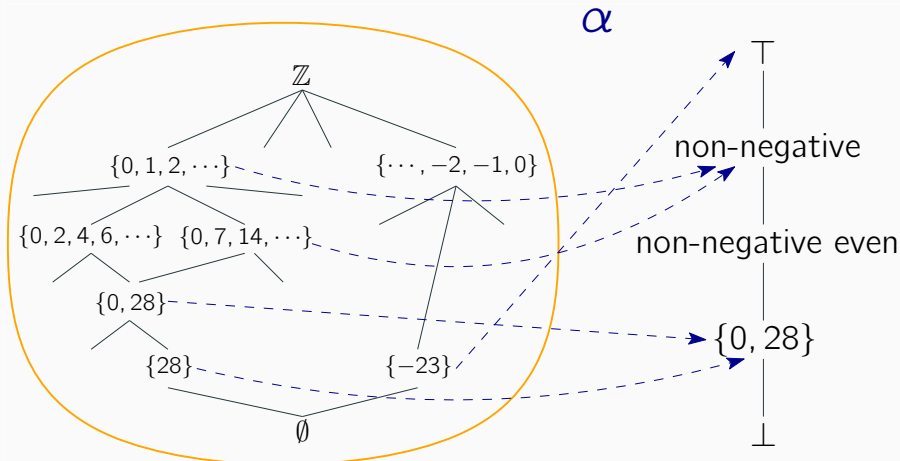
- **Abstraction Function:**  $\alpha : 2^C \rightarrow Abs$   
Maps a value in the program to the “best” abstract value
- **Concretization Function:**  $\gamma : Abs \rightarrow 2^C$   
Maps an abstract value to a set of values in the program

# Abstraction Example



Concretization function  $\gamma$  maps each abstract value to concrete values it represents

# Abstraction Example

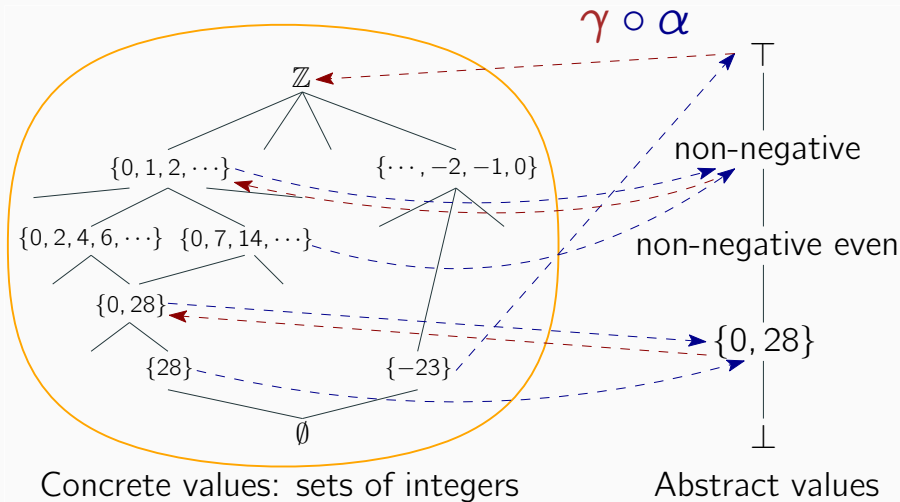


Concrete values: sets of integers

Abstract values

Abstraction function  $\alpha$  maps each concrete set to the best abstract value  
(least imprecise)

# Abstraction Example



Abstraction followed by concretization is sound but imprecise

# Galois Connection

- $\alpha$  and  $\gamma$  are monotonic
- Recall:  $f$  is monotonic if  $x \leq y \Rightarrow f(x) \leq f(y)$
- Also called “order preserving”

## Galois Connection:

A pair of functions

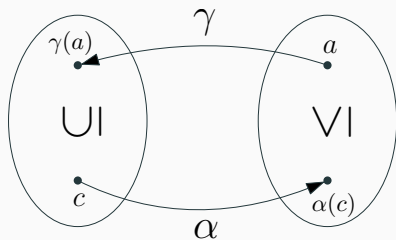
(Abstraction)  $\alpha : 2^C \rightarrow Abs$

and

(Concretization)  $\gamma : Abs \rightarrow 2^C$

such that

$$\forall a \in Abs. \forall c \in 2^C. c \subseteq \gamma(a) \Leftrightarrow \alpha(c) \leq a$$



# Correctness Conditions

Three conditions guarantee correctness in general:

1.  $\alpha$  and  $\gamma$  are monotonic
2.  $\alpha$  and  $\gamma$  form a Galois connection
3. Abstract operations  $\text{op}^A$  are locally correct

$$\gamma(a_1 \text{ op}^A a_2) \supseteq \gamma(a_1) \text{ op } \gamma(a_2)$$



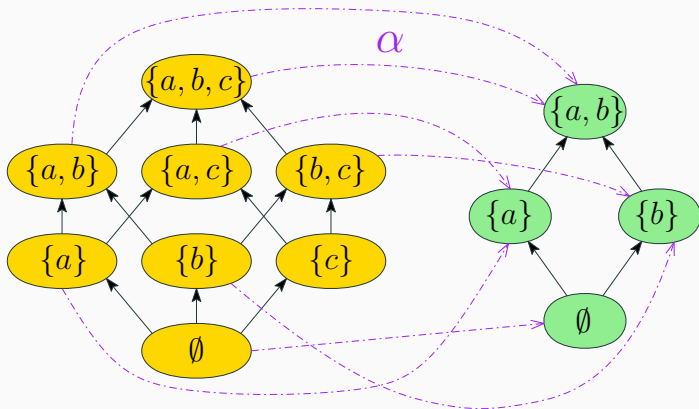
# Key Property of Galois Connections

**Theorem.** The abstraction and concretization functions uniquely determine each other

$$\gamma(a) = \bigcup \{c \in 2^C \mid \alpha(c) \leq a\}$$

$$\alpha(c) = \bigcap \{a \in Abs \mid c \subseteq \gamma(a)\}$$

## Example



- $\gamma(\{a\}) = \cup\{\ell \mid \alpha(\ell) \leq \{a\}\} = \emptyset \cup \{a\} \cup \{a, c\} = \{a, c\}$
- $\gamma(\{b\}) = \cup\{\ell \mid \alpha(\ell) \leq \{b\}\} = \emptyset \cup \{b\} \cup \{b, c\} = \{b, c\}$
- $\gamma(\{a, b\}) = \emptyset \cup \{a, b\} \cup \{b, c\} \cup \dots \cup \{a, b, c\} = \{a, b, c\}$

## Concretization

$$\gamma : [m, n] \rightarrow \{x \in \mathbb{Z} \mid m \leq x \leq n\}$$

- $m$  and  $n$  are potentially infinite, and  $\gamma(\perp) = \emptyset$  and  $\gamma(top) = \mathbb{Z}$

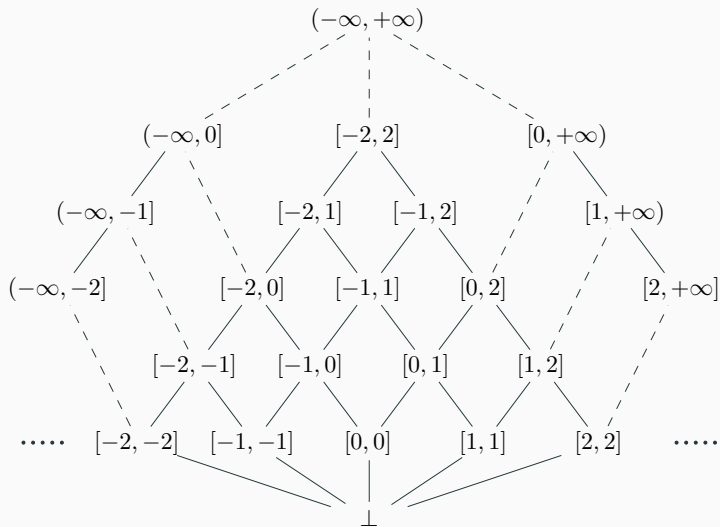
## Abstraction

- if  $S$  is empty:  $\alpha(S) = \perp$ , else

$$\alpha : S \rightarrow [inf S, sup S]$$

- $inf$  and  $sup$  are taken in  $\mathbb{Z} \cup \{-\infty, +\infty\}$

# Lattice of Intervals



$$[a, b] \sqcup [c, d] = [\min(a, c), \max(b, d)]$$

$$[a, b] \sqcap [c, d] = [\max(a, c), \min(b, d)]$$

# Best Abstraction of an Operation

- For a concrete operation  $\text{op} : C \rightarrow C$  we define an abstract operation  $\text{op}^A : A \rightarrow A$  by

$$\text{op}^A(x) = \alpha \circ \text{op} \circ \gamma(x)$$

It is the best possible abstraction of  $\text{op}$

# Best Interval Operations

- Let  $+$  be the standard integer addition
- What is the best abstraction for intervals?

$$+^A : \text{Interval} \rightarrow \text{Interval}$$

$$\begin{aligned} [a, b] +^A [c, d] &= \alpha(\gamma([a, b]) + \gamma([c, d])) \\ &= \alpha(\{x \mid a \leq x \leq b\} + \{y \mid c \leq y \leq d\}) \\ &= \alpha(\{x + y \mid a \leq x \leq b, c \leq y \leq d\}) \\ &= \alpha(\{x \mid a + c \leq x \leq b + d\}) \\ &= [a + c, b + d] \end{aligned}$$

# Best Interval Operations

- Let  $+$  be the standard integer addition
- What is the best abstraction for intervals?

$$+^A : \text{Interval} \rightarrow \text{Interval}$$

$$\begin{aligned} [a, b] +^A [c, d] &= \alpha(\gamma([a, b]) + \gamma([c, d])) \\ &= \alpha(\{x \mid a \leq x \leq b\} + \{y \mid c \leq y \leq d\}) \\ &= \alpha(\{x + y \mid a \leq x \leq b, c \leq y \leq d\}) \\ &= \alpha(\{x \mid a + c \leq x \leq b + d\}) \\ &= [a + c, b + d] \end{aligned}$$

**Exercise.** Prove

$$[a, b] \times^A [c, d] = [\min(ac, ad, bc, bd), \max(ac, ad, bc, bd)]$$