CSCI 740 - Programming Language Theory

Lecture 28

Galois Connection

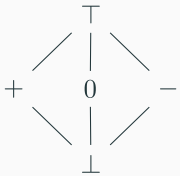
Instructor: Hossein Hojjat

November 8, 2017

Abstract Domain

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

Example: Sign Abstract Domain



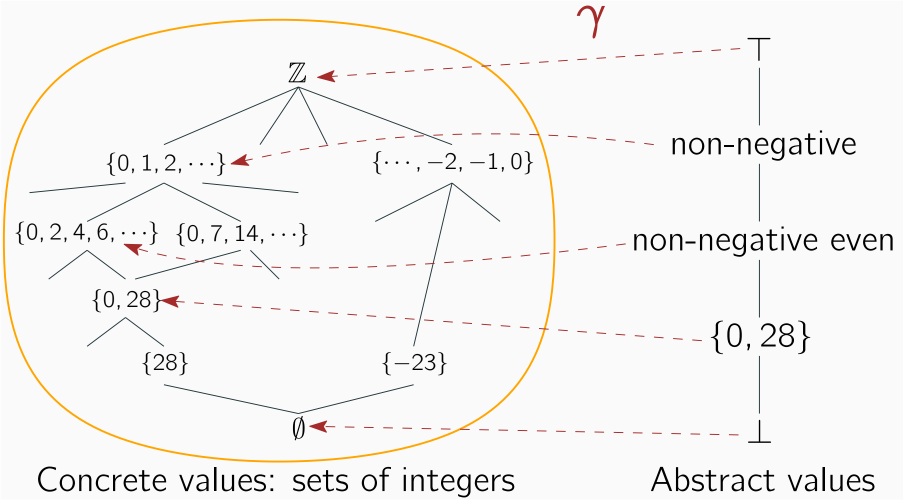
- Set of abstract values $\{\bot, +, 0, -, \top\}$
- Relation $\leq$ that is
  - Reflexive
  - Anti-symmetric
  - Transitive
- Least upper bound (lub, $\sqcup$) and greatest lower bound (glb, $\sqcap$) exists for any pair of elements
  - So it's a lattice

α and γ

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

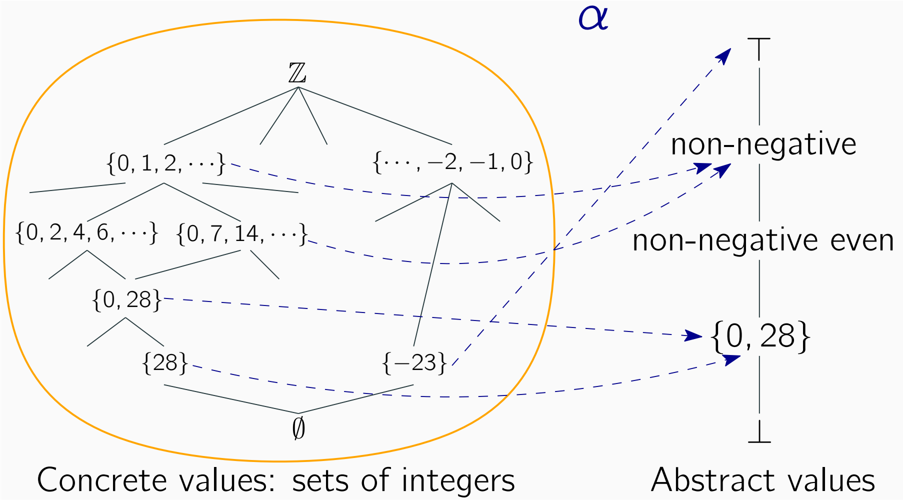
- **Abstraction Function:** $\alpha : 2^C \rightarrow \mathit{Abs}$
  Maps a value in the program to the "best" abstract value
- **Concretization Function:** $\gamma : \mathit{Abs} \rightarrow 2^C$
  Maps an abstract value to a set of values in the program

Abstraction Example



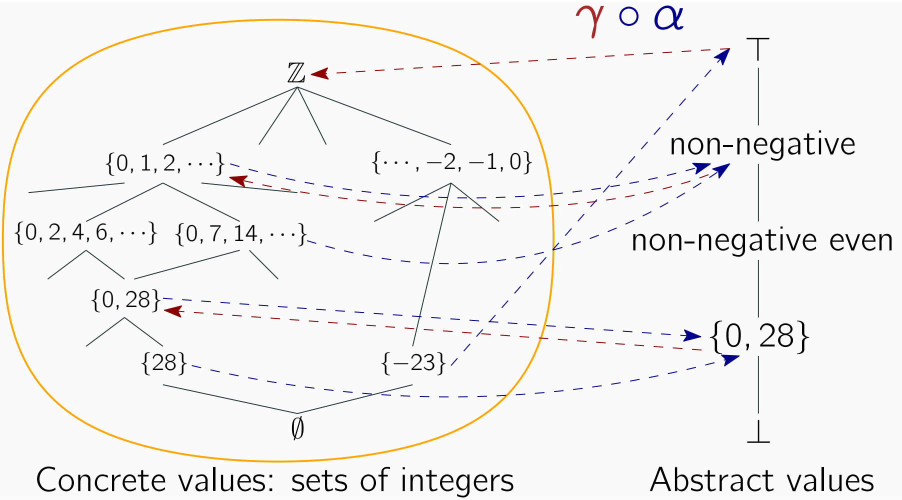
Concretization function γ maps each abstract value to concrete values it represents

Abstraction Example



Abstraction function α maps each concrete set to the best abstract value (least imprecise)

Abstraction Example



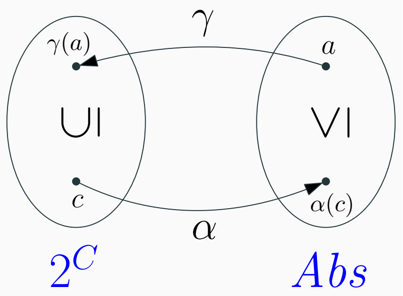
Abstraction followed by concretization is sound but imprecise

Galois Connection

- α and γ 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. α and γ are monotonic
2. α and γ form a Galois connection
3. Abstract operations op^A are locally correct

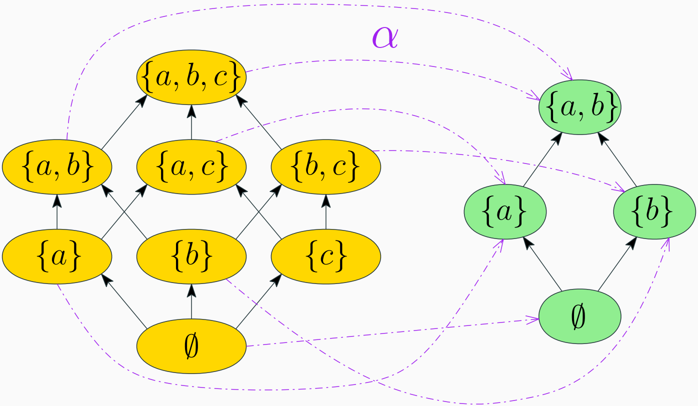
$$\gamma(a_1\ \mathsf{op}^A\ a_2) \supseteq \gamma(a_1)\ \mathsf{op}\ \gamma(a_2)$$

Key Property of Galois Connections

Theorem. The abstraction and concretization functions uniquely determine each other

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

Example



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

Galois connection: Intervals and Subsets

Concretization

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

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

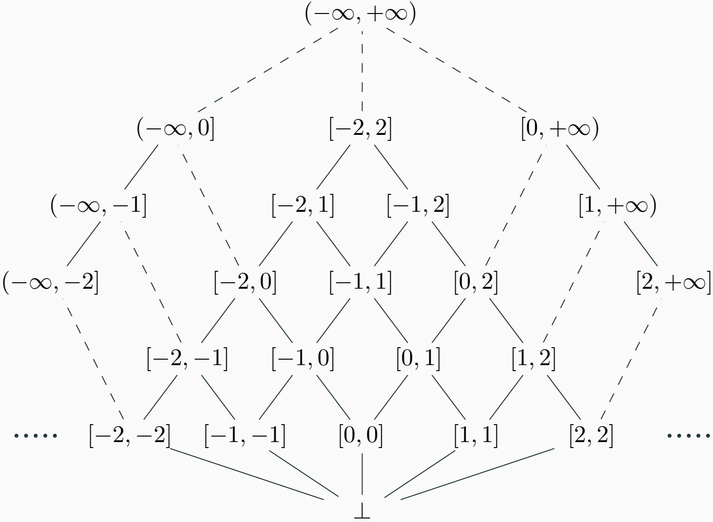
Abstraction

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

$$\alpha : S \rightarrow [\textit{inf}\ S, \textit{sup}\ S]$$

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

Lattice of Intervals



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

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

Best Abstraction of an Operation

- For a concrete monotone operation $\mathsf{op} : C \to C$ we define an abstract operation $\mathsf{op}^A : A \to A$ by

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

  It is the best possible abstraction of op

Best Interval Operations

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

$$+^A : \text{Inteval} \to \text{Interval}$$

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

Note.

- We have extended mathematical $+$ to operate over $+\infty$ and $-\infty$
  - e.g. $\forall x \neq -\infty : x + \infty = \infty$

Best Interval Operations

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

$$+^A : \text{Inteval} \to \text{Interval}$$

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

Note.

- We have extended mathematical $+$ to operate over $+\infty$ and $-\infty$
  - e.g. $\forall x \neq -\infty : x + \infty = \infty$

Exercise. Prove

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