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 \{⊥, +, 0, −, ⊤\}
- Relation \( \leq \) that is
  - Reflexive
  - Anti-symmetric
  - Transitive
- Least upper bound (lub, ⊔) and greatest lower bound (glb, ⊓) 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**: \( \alpha : 2^C \rightarrow \text{Abs} \)
  Maps a value in the program to the “best” abstract value

- **Concretization Function**: \( \gamma : \text{Abs} \rightarrow 2^C \)
  Maps an abstract value to a set of values in the program
Abstraction Example

Concrete values: sets of integers
- \{0, 1, 2, \ldots\}
- \{0, 2, 4, 6, \ldots\}
- \{0, 7, 14, \ldots\}
- \{0, 28\}
- \{28\}
- \emptyset

Abstract values
- \mathbb{Z}
- \{\ldots, -2, -1, 0\}
- non-negative
- non-negative even
- \{0, 28\}
- \perp
- \gamma

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)
Concrete values: sets of integers

Abstract values

Abstraction followed by concretization is sound but imprecise
Galois Connection

- \( \alpha \) and \( \gamma \) are monotonic (also called “order preserving”)
- Given two partial orders \((A_1, \sqsubseteq_1)\) and \((A_2, \sqsubseteq_2)\), we call a function \( f : A_1 \rightarrow A_2 \) monotonic iff for all \( x, y \in A_1 \):
  \[ x \sqsubseteq_1 y \rightarrow f(x) \sqsubseteq_2 f(y) \]

**Galois Connection:**

A pair of functions

(Abstraction) \( \alpha : 2^C \rightarrow \text{Abs} \)

and

(Concretization) \( \gamma : \text{Abs} \rightarrow 2^C \)

such that

\[ \forall a \in \text{Abs}. \ \forall c \in 2^C. \ c \subseteq \gamma(a) \Leftrightarrow \alpha(c) \leq a \]
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

$$\gamma(a_1 \text{ op}^A a_2) \supseteq \gamma(a_1) \text{ op } \gamma(a_2)$$
Theorem. The abstraction and concretization functions uniquely determine each other

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

\[
\alpha(c) = \bigcap \{ a \in \text{Abs} \mid c \subseteq \gamma(a) \}
\]
\[ \gamma(\{a\}) = \bigcup \{ \ell \mid \alpha(\ell) \leq \{a\} \} = \emptyset \cup \{a\} \cup \{a, c\} = \{a, c\} \]
\[ \gamma(\{b\}) = \bigcup \{ \ell \mid \alpha(\ell) \leq \{b\} \} = \emptyset \cup \{b\} \cup \{b, c\} = \{b, c\} \]
\[ \gamma(\{a, b\}) = \emptyset \cup \{a, b\} \cup \{b, c\} \cup \cdots \cup \{a, b, c\} = \{a, b, c\} \]
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 \( \gamma(\text{top}) = \mathbb{Z} \)

Abstraction

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

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

- \( \inf \) and \( \sup \) are taken in \( \mathbb{Z} \cup \{-\infty, +\infty\} \)
Lattice of Intervals

\[ \begin{align*}
(a, b) \sqcup (c, d) &= [\min(a, c), \max(b, d)] \\
(a, b) \sqcap (c, d) &= [\max(a, c), \min(b, d)]
\end{align*} \]
• For a concrete monotone 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?

\[ +^A : \text{Interval} \rightarrow \text{Interval} \]

\[ [a, b] +^A [c, d] = \alpha(\gamma([a, b]) + \gamma([c, d])) \]

\[ = \alpha(\{x \mid a \leq x \leq b\} + \{y \mid c \leq y \leq d\}) \]

\[ = \alpha(\{x + y \mid a \leq x \leq b, c \leq y \leq d\}) \]

\[ = \alpha(\{x \mid a + c \leq x \leq b + d\}) \]

\[ = [a + c, b + d] \]

Note.

- We have extended mathematical \( + \) to operate over \( +\infty \) and \( -\infty \)
  - e.g. \( \forall x \neq -\infty : x + \infty = \infty \)
• Let \( + \) be the standard integer addition

• What is the best abstraction for intervals?

\[
+^A : \text{Interval} \rightarrow \text{Interval}
\]

\[
[a, b] +^A [c, d] = \alpha(\gamma([a, b]) + \gamma([c, d]))
\]

\[
= \alpha(\{x \mid a \leq x \leq b\} + \{y \mid c \leq y \leq d\})
\]

\[
= \alpha(\{x + y \mid a \leq x \leq b, c \leq y \leq d\})
\]

\[
= \alpha(\{x \mid a + c \leq x \leq b + d\})
\]

\[
= [a + c, b + d]
\]

**Note.**

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

**Exercise.** Prove

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