Introduction to Abstract Interpretation

What is an Abstraction?

The Galois Insertion

Proving Correctness

Widening Operator

These notes are based on lecture notes made available by Jeff Foster (CMSC 631, Fall 2003), David Schmidt, and Alex Aiken

What is an Abstraction?

A property from some domain

Blue (color)

Planet (classification)

6000..7000km (radius)
**Abstraction Function**

The abstraction function $\alpha$ maps each concrete set within the lattice to the best abstract value.

**Concrete Domain**

- Integers
- $\{0, 1, 2, \ldots\}$
- $\{0, 2, 4, 6, \ldots\}$
- $\{0, 42\}$
- $\phi$

**Abstract Domain**

- Integers
- Non-negative
- Non-negative even
- $\{0.42\}$

**Concretization Function**

The concretization function $\gamma$ maps each abstract value to concrete values it represents.

**Concrete Domain**

- Integers
- $\{0, 1, 2, \ldots\}$
- $\{0, 2, 4, 6, \ldots\}$
- $\{0, 42\}$
- $\phi$

**Abstract Domain**

- Integers
- Non-negative
- Non-negative even
- $\{0.42\}$

CS653 Lecture Abstract Interpretation 3
**Composing \( \alpha \) and \( \gamma \)**

Abstraction followed by concretization is sound but imprecise.

\[
\gamma \circ \alpha
\]

\( \alpha \) and \( \gamma \) Form a Galois insertion

\( \alpha \) and \( \gamma \) are monotonic

– recall: \( f \) is monotonic if \( x \leq y \) implies \( f(x) \leq f(y) \), order preserving

\[
S \subseteq \gamma(\alpha(S)) \quad \text{for any concrete set } S
\]

\[
\alpha(\gamma(A)) = A \quad \text{for any abstract element } A
\]
Source Language

- Integers and multiplication
  - \( e ::= i \mid e \ast e \)

- Standard semantics of the program
  - \( \text{Eval} : e \rightarrow \text{Int} \)
  - \( \text{Eval}(i) = i \)
  - \( \text{Eval}(e_1 \ast e_2) = \text{Eval}(e_1) \times \text{Eval}(e_2) \)

Abstraction

- Define an abstract semantics that computes only the sign of the result

<table>
<thead>
<tr>
<th>( \times )</th>
<th>( + )</th>
<th>( 0 )</th>
<th>( - )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( + )</td>
<td>( + )</td>
<td>( 0 )</td>
<td>( - )</td>
</tr>
<tr>
<td>( 0 )</td>
<td>( 0 )</td>
<td>( 0 )</td>
<td>( 0 )</td>
</tr>
<tr>
<td>( - )</td>
<td>( - )</td>
<td>( 0 )</td>
<td>( + )</td>
</tr>
</tbody>
</table>

\( \text{AEval} : e \rightarrow \{-, 0, +\} \)

\( \text{AEval}(i) = \begin{cases} 
+ & i > 0 \\
0 & i = 0 \\
- & i < 0 
\end{cases} \)

\( \text{AEval}(e_1 \ast e_2) = \text{AEval}(e_1) \times \text{AEval}(e_2) \)
Soundness

- We can show our abstraction correctly predicts the sign of an expression
- Proof: by structural induction on e
  - Eval(e) > 0 iff AEval(e) = +
  - Eval(e) = 0 iff AEval(e) = 0
  - Eval(e) < 0 iff AEval(e) = -

Abstraction and Concretization

- Concretization function $\gamma$
  - $\gamma(\tau) = \text{all integers}$
  - $\gamma(+) = \{i \mid i > 0\}$
  - $\gamma(0) = \{0\}$
  - $\gamma(-) = \{i \mid i < 0\}$
  - $\gamma(\bot) = \emptyset$
- Abstraction function maps concrete values (sets of integers) to smallest valid abstract element
  - $\alpha(S) = \{\bot\} \cup \{0 \mid \exists i < 0\} \cup \{\bot\} \cup \{+ \mid \exists i < 0\}$

CMSC 631, Fall 2003
Definition

- An abstract interpretation consists of
  - A concrete domain \( S \) and an abstract domain \( A \)
  - Concretization and abstraction functions that form a Galois insertion [of \( A \) into \( S \)]
  - A (sound) abstract semantic function

- Recall: \( \alpha \) and \( \gamma \) form a Galois insertion if
  - \( \alpha \) and \( \gamma \) are monotone
  - \( S \subseteq \gamma(\alpha(S)) \) or \( \text{id} \leq \gamma \circ \alpha \) for any concrete set \( S \)
  - \( A = \alpha(\gamma(A)) \) or \( \text{id} = \alpha \circ \gamma \) for any abstract element \( A \)

Soundness, Again

- Our abstraction is sound if
  - \( \text{Eval}(e) \in \gamma(\text{AEval}(e)) \)

- Soundness proof: next
Conditions for Correctness

- We can show that if
  - $\alpha$ and $\gamma$ form a Galois insertion
  - Abstract operations $\text{op}$ are locally correct
    - $\gamma(\text{op}(a_1, ..., a_n)) \supseteq \text{op}(\gamma(a_1), ..., \gamma(a_n))$
    - Note: We’ve extended $\text{op}$ pointwise to sets
      - i.e., if $S$ and $T$ are sets, $S + T = \{s + t \mid s \in S, t \in T\}$
- Then the abstract interpretation is sound

Proof: Show $\text{Eval}(e) \in \gamma(\text{AEval}(e))$

- By structural induction on expressions
  - Base cases: an integer $i$, so $\text{Eval}(i) = i$
    - if $i < 0$ then $\gamma(\text{AEval}(i)) = \gamma(-) = \{j \mid j < 0\}$
    - Other cases similar
  - Induction: for any operation
    - $\text{Eval}(e_1 \text{ op } e_2)$
      - $= \text{Eval}(e_1) \text{ op } \text{Eval}(e_2)$ by definition of $\text{Eval}$
      - $\in \gamma(\text{AEval}(e_1)) \text{ op } \gamma(\text{AEval}(e_2))$ by induction
      - $\subseteq \gamma(\text{AEval}(e_1) \text{ op } \text{AEval}(e_2))$ by local correctness of $\text{op}$
      - $= \gamma(\text{AEval}(e_1 \text{ op } e_2))$ by definition of $\text{AEval}$
Widening (see perspectives paper for an example)