Meeting 19

Today

Rest of Semester

Intervals & Widening (AI Wrap Up)

Reading Papers

- "Three Pass Process"
- Questions to Ask
  - What's the contribution?

Presenting Papers

- What's the contribution?
- Pass 1.5-2
  - Example

Writing Papers

- What's the contribution?
Abstract Interpretation

Review Recipe for Static Analysis Design

(1) What is your programming language/program/examples?

Concrete "world" / Concrete domain

n ∈ ℤ  see String

§ : Var → Val

(2) Concrete Semantics

"God's Analysis"

collecting semantics
(3) Abstraction?

\[
\text{abstract store } \hat{\varphi} : \text{Var} \rightarrow \text{Sign}
\]

Is this good? Is it sound?

\[\rho : \hat{D} \rightarrow \text{POD}\]

Relationship between abstract store and concrete set

Gallàis' connection

(4) Abstract semantics?

\[\hat{\Gamma} \downarrow \text{ "How to interpret with abstract values?"} \]

\[\hat{\Gamma} \downarrow + \oplus + = + \quad \text{(example)}\]

Local Soundness

\[
\hat{\delta}(\hat{v}_1 \oplus \hat{v}_2) \supseteq \{v_1 + v_2 \mid v_1 \in \hat{\delta}(\hat{v}_1) \text{ and } v_2 \in \hat{\delta}(\hat{v}_2)\}
\]
Collecting Semantics

= a bunch of recursive equations
  (well-defined b/c of the fixed point theorem)

Abstract semantics =

a bunch of recursive equations

What's different

HOPE! (of computability)
Assume finite height lattice of height \( h \).

At each step, at least one program point has an element that goes up 1 step.

\( O(h \cdot n) \)

\( n = \text{size of CFG} \)
Concrete

$P(Z)$

Abstract

$\hat{\cdot} = \perp \downarrow |(n, m] \cap (-\infty, m]|$

$[n, \infty) | \top$

for $n, m \in \mathbb{Z}$

Application:

Array bounds checking
\[ \mathcal{X} : \text{Interval} \rightarrow P(\mathbb{Z}) \]

\[ \mathcal{X}(\mathbb{I}) \overset{\text{def}}{=} \{3\} \]

\[ \mathcal{X}(\mathbb{Z}) \overset{\text{def}}{=} \mathbb{Z} \]

\[ \mathcal{X}([n, m]) \overset{\text{def}}{=} \{ x \mid n \leq x \leq m \text{ and } x \in \mathbb{Z} \} \]

\[ \mathcal{X}(\mathbb{I}) \overset{\text{def}}{=} \mathcal{X}(\mathbb{I}_1) \leq \mathcal{X}(\mathbb{I}_2) \]

Define judgmentally

\[ \frac{n' \leq n \quad m \leq m'}{[n, m] \subseteq [n', m']} \]
\[ [0, 1] \subseteq [0, 2] \subseteq [0, 3] \subseteq \ldots \]

\[
i = 0 \quad [0, 0] \\
\text{while } (i \leq n) \quad \exists \]

\[
i = i + 1 \quad [0, 0] \quad [0, 1] \quad [0, 2] \quad \ldots \quad [0, \infty) \\
\quad [1, 1] \quad [1, 2] \quad [1, 3] \quad \ldots \quad [1, \infty)
\]

\[\boxed{\text{Wider}}\] "Sound Inductive Invariant Guesse"
\[ \nabla : \mathcal{D} \times \mathcal{D} \to \mathcal{D} \]

(1) upper bound
\[ x \leq x \forall y \text{ and } y \leq x \forall y \]
for \( x, y \in \mathcal{D} \)

(2) "terminates" / "converges"

\[ x_0 \leq x_1 \leq x_2 \leq \ldots \]

Then the chain

\[ x_0 \leq (x_0 \nabla x_1) \leq (x_0 \nabla x_1 \nabla x_2) \leq \ldots \]

stabilizes