Correctness of Abstract Interpretation

Deepak D'souza and K. V. Raghavan

Summary: What is an abstract interpretation (AI)?

- Given:
  - A complete join semi-lattice D. This is the "abstract" semantic domain.
  - A monotonic "abstract" transfer functions $f_{MN} : D \rightarrow D$ for each arc $M \rightarrow N$ in the control-flow graph.
- Output: A map $\overline{D}$ from program points to elements in D.
- Ideal output: $\mathrm{JOP}_{\overline{D}}$
  - for any program point p $\mathrm{JOP}_{\overline{D}}[p]$ is the join of all values obtained by propagating initial value $d_0 \in D$ through transfer functions of all paths in the CFG that end at p, *where*
  - transfer function of a path is the composition of the transfer functions of the arcs on the path.

Summary: What does Killdall's algorithm compute?

- In general $\mathrm{JOP}_{\overline{D}}$ is not computable.
- Killdall's algorithm computes $\mathrm{LFP}_{\overline{D}}(\overline{F})$, which is the least fix point of the vectorized transfer function $\overline{F}$.
  - Killdall requires D to contain no infinite ascending chains.
- In general $\mathrm{LFP}_{\overline{D}} \geq \mathrm{JOP}_{\overline{D}}$.
  - They are equal when lattice is finite and functions are distributive.

Summary: Theorems

- Knaster-Tarski theorem:
  - Guarantees presence of a fix point.
  - Fix points form a complete lattice.
  - $\mathrm{LFP}_D(f) \geq \bigsqcup_{i \geq 0}(f^i(\bot))$, if f is monotonic.
  - $\mathrm{LFP}_D(f) = \bigsqcup_{i \geq 0}(f^i(\bot))$, if f is continuous.
  - D needs to be a complete join semi-lattice. D may contain infinite ascending chains.

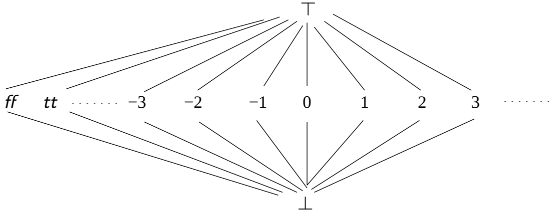
Summary: Theorems

- Knaster-Tarski theorem:
  - Guarantees presence of a fix point.
  - Fix points form a complete lattice.
  - $\mathrm{LFP}_D(f) \geq \bigsqcup_{i \geq 0}(f^i(\bot))$, if f is monotonic.
  - $\mathrm{LFP}_D(f) = \bigsqcup_{i \geq 0}(f^i(\bot))$, if f is continuous.
  - D needs to be a complete join semi-lattice. D may contain infinite ascending chains.

Exercise: Consider example in slide 51 in data-flow analysis slide set. Compute $\bigsqcup_{i \geq 0}(\overline{F}^i(\bot))$.

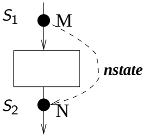
Static (i.e., collecting) semantics

- Lattice of values: $(Val_\bot, \leq_{Val_\bot}, \sqcup_{Val_\bot})$



- *Env* is (normally) a map $e : Var \to Val_\bot$. *However, in general, it can be any semantic domain.*
- Program semantics is given by the *nstate* function:

$nstate(M, S_1 \in 2^{Env}) = (N, S_2 \in 2^{Env})$.



Static (i.e., collecting) semantics – contd.

- Initial environment S_0 is given. Normally, it is: $\{\lambda x.\bot\}$.
- Static semantics SS is a map $ProgramPoints \rightarrow 2^{Env}$.
- At each program point N,

$$\mathrm{SS}(N) = \{e \mid nstate_p(E, S_0) = (N, S), p \text{ is a path } E \rightsquigarrow N, e \in S\}$$

where E is entry point of CFG.

Static (i.e., collecting) semantics – contd.

- Initial environment S_0 is given. Normally, it is: $\{\lambda x.\bot\}$.
- Static semantics SS is a map $\mathit{ProgramPoints} \rightarrow 2^{\mathit{Env}}$.
- At each program point N,

$$\mathrm{SS}(N) = \{e \mid \mathit{nstate}_p(E, S_0) = (N, S), p \text{ is a path } E \rightsquigarrow N, e \in S\}$$

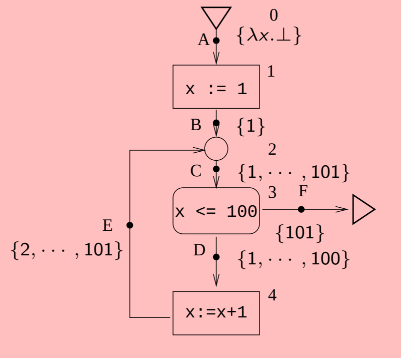
  where E is entry point of CFG.
- Static semantics can also be phrased as an AI:
  - Concrete lattice $C : (2^{\mathit{Env}}, \subseteq)$, $\bot = \phi$, $\top = \mathit{Env}$, $\sqcup = \cup$.
  - Initial value: $\{\lambda x.\bot\}$
  - Transfer function $= \overline{\mathit{nstate}}$
  - Static semantics $= \mathrm{JOP}_{\overline{C}}$; i.e., $\mathrm{SS}(N) = \mathrm{JOP}_{\overline{C}}[N]$.
  - Notice that framework is distributive:

$$\mathit{nstate}(S_1 \sqcup S_2) = \mathit{nstate}(S_1) \sqcup \mathit{nstate}(S_2)$$

  - Hence, $\mathrm{JOP}_{\overline{C}} = \mathrm{LFP}_{\overline{C}}(\overline{\mathit{nstate}})$

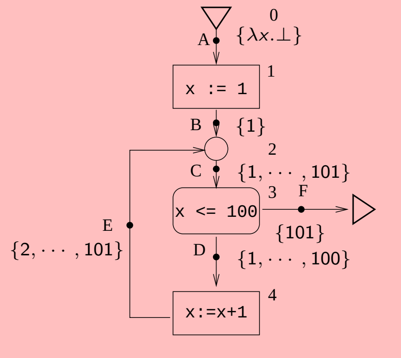
Sample program

$\mathrm{JOP}_{\overline{C}} =$



Sample program

$\text{JOP}_{\overline{C}} =$



Exercise: Find a non-minimal fixpoint of this program.

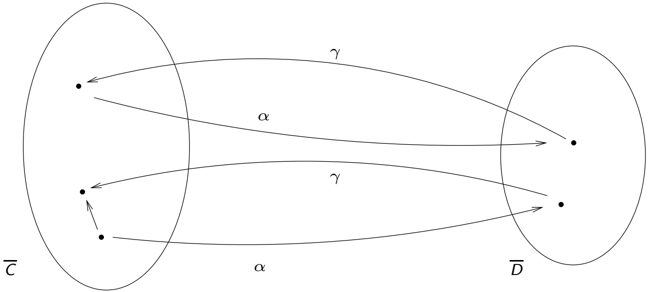
Conditions for correctness of an AI

Should exist maps

- $\alpha : C \to D$ (abstraction)
- $\gamma : D \to C$ (concretization)

such that

- α and γ are monotonic
- $\gamma(\alpha(e)) \geq e$
- $\alpha(\gamma(d)) = d$



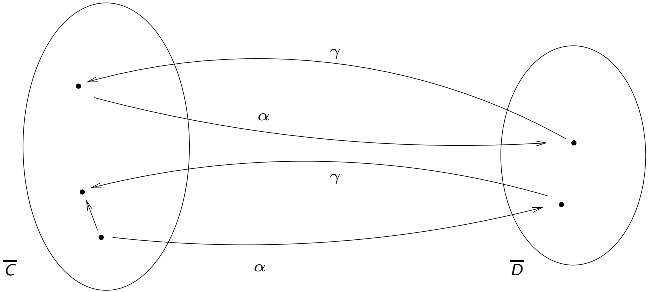
Conditions for correctness of an AI

Should exist maps

- $\alpha : C \rightarrow D$ (abstraction)
- $\gamma : D \rightarrow C$ (concretization)

such that

- α and γ are monotonic
- $\gamma(\alpha(e)) \geq e$
- $\alpha(\gamma(d)) = d$



In this case (α, γ) are said to form a Galois connection.

Illustration of Galois connection

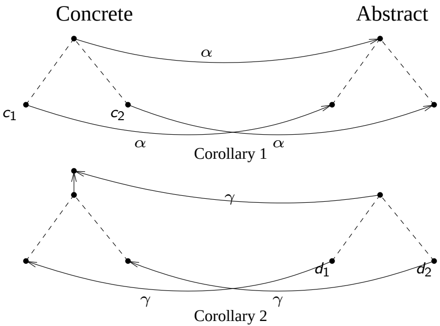
For constant propagation, the following mappings form a galois connection:

$$\alpha(S) = \{(x, c) \mid c = \sqcup_{Val_\perp}(\{e(x) | e \in S\})\}$$

$$\gamma(P) = \{e \in Env \mid \text{for each } (x, c) \in P : e(x) \leq_{Val_\perp} c\}$$

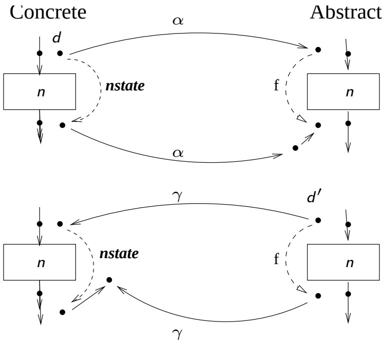
Corollaries

If (α, γ) form a Galois connection then the concrete and abstract join operators satisfy the following properties.



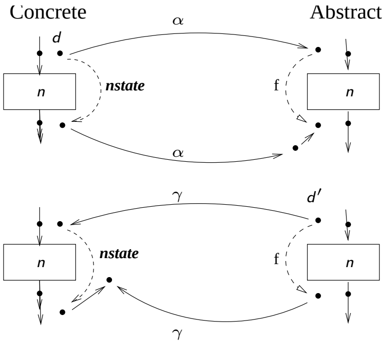
Conditions for correctness – continued

Transfer functions should satisfy one of the following (each of them implies the other):



Conditions for correctness – continued

Transfer functions should satisfy one of the following (each of them implies the other):

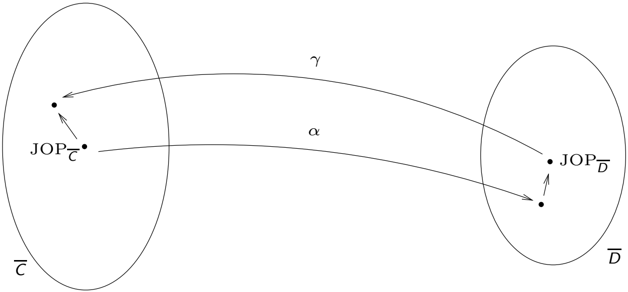


Exercise: Illustrate first condition above using constant propagation example. Let n be "z = x + y", and let + be strict on its arguments. Demonstrate a situation where
$\alpha(f_{n,concrete}(S)) < f_{n,abstract}(\alpha(S))$

Theorem: Correctness of AI

If (α, γ) form a Galois connection *and* transfer functions satisfy the property mentioned above *and* $\alpha(S_0) \leq d_0$ then:

- $\overline{\alpha}(\mathrm{JOP}_{\overline{C}}) \leq \mathrm{JOP}_{\overline{D}}$
- $\mathrm{JOP}_{\overline{C}} \leq \overline{\gamma}(\mathrm{JOP}_{\overline{D}})$



More on correctness of AI

- We showed just now that $\overline{\gamma}(\mathrm{JOP}_{\overline{D}}) \geq \mathrm{JOP}_{\overline{C}}$.
- We have already shown that $\mathrm{LFP}_{\overline{D}} \geq \mathrm{JOP}_{\overline{D}}$ (see slide 74, data-flow analysis slides).
- We know γ is monotonic.
- Therefore, $\overline{\gamma}(\mathrm{LFP}_{\overline{D}}) \geq \mathrm{JOP}_{\overline{C}}$.

More on correctness of AI

- We showed just now that $\overline{\gamma}(\mathrm{JOP}_{\overline{D}}) \geq \mathrm{JOP}_{\overline{C}}$.
- We have already shown that $\mathrm{LFP}_{\overline{D}} \geq \mathrm{JOP}_{\overline{D}}$ (see slide 74, data-flow analysis slides).
- We know γ is monotonic.
- Therefore, $\overline{\gamma}(\mathrm{LFP}_{\overline{D}}) \geq \mathrm{JOP}_{\overline{C}}$.

In other words, the concretization of the result of abstract interpretation is an over-approximation of the collecting semantics.

Proof of corollaries

Proof of Corollary 2:

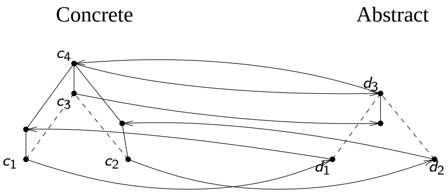
- $d_1 \sqcup d_2$ is $\geq$ both d_1 and d_2 (property of join)
- Therefore, due to monotonicity of γ, $\gamma(d_1 \sqcup d_2)$ is $\geq$ both $\gamma(d_1)$ and $\gamma(d_2)$.
- Therefore, by property of join, $\gamma(d_1 \sqcup d_2) \; \geq \; \gamma(d_1) \sqcup \gamma(d_2)$. $\Box$.

Proof of Corollary 1:

- Using an argument similar to above it can be shown that $\alpha(c_1 \sqcup c_2) \; \geq \; \alpha(c_1) \sqcup \alpha(c_2)$.

Proof of Corollary 1 – continued

We now need to show that $\alpha(c_1 \sqcup c_2) \leq \alpha(c_1) \sqcup \alpha(c_2)$. This would complete the proof.



- (Rightward arrows are α's and leftward arrows are γ's.)
- $\gamma(d_1) \geq c_1$ and $\gamma(d_2) \geq c_2$ (by defn. of Galois connection).
- $c_4 = \gamma(d_3 = (d_1 \sqcup d_2))$ is $\geq$ both $\gamma(d_1)$ and $\gamma(d_2)$ (by monotonicity of γ).
- Therefore, c_4 is $\geq$ both c_1 and c_2 (by transitivity of $\geq$).
- Therefore, $c_4 \geq (c_3 = (c_1 \sqcup c_2))$ (by property of join).
- $\alpha(c_4) = d_3$ (by defn. of Galois connection). Therefore, $d_3 \geq \alpha(c_3)$ (by monotonicity of α). $\square$

Proof of correctness theorem

We give a proof that $\overline{\alpha}(\mathrm{JOP}_{\overline{C}}) \leq \mathrm{JOP}_{\overline{D}}$.

- **Lemma:** Consider any edge $M \rightarrow N$. Let d be an abstract value c be a concrete value at M such that $\alpha(c) \leq d$. $\alpha(f_{MN,concrete}(c)) \leq f_{MN,abstract}(d)$.
  Proof: The first condition on transfer functions tells us that $\alpha(f_{MN,concrete}(c)) \leq f_{MN,abstract}(\alpha(c))$. Using the lemma's prerequisite $\alpha(c) \leq d$, and by monotonicity of $f_{MN,abstract}$, we get $f_{MN,abstract}(\alpha(c)) \leq f_{MN,abstract}(d)$. Therefore $\alpha(f_{MN,concrete}(c)) \leq f_{MN,abstract}(d)$
- Consider any path p in the CFG starting from the entry point E. We will prove using induction that for any $i >= 0$, where p^i is the prefix of p containing i edges, $\alpha(f_{p^i,concrete}(S_0)) \leq f_{p^i,abstract}(d_0)$, where $f_{p^i,concrete}$ ($f_{p^i,abstract}$) is the composition of the concrete (abstract) transfer functions of the edges in p^i.
- Base case ($i = 0$): The property reduces to $\alpha(S_0) \leq d_0$. This is a pre-requisite of the theorem.

Proof – continued

- Inductive case: The inductive hypothesis is that $\alpha(f_{p^{i-1},concrete}(S_0)) \leq f_{p^{i-1},abstract}(d_0)$. Let the i^{th} edge of p be $L \to M$. Applying the lemma above on this edge we get $\alpha(f_{LM,concrete}(f_{p^{i-1},concrete}(S_0))) \leq f_{LM,abstract}(f_{p^{i-1},abstract}(d_0))$. This reduces to $\alpha(f_{p^{i},concrete}(S_0)) \leq f_{p^{i},abstract}(d_0)$. The inductive case is done.
- From the result proved above we derive

$$\alpha(c_p) \leq d_p \tag{1}$$

  where p is any path, $c_p = f_{p,concrete}(S_0)$ and $d_p = f_{p,abstract}(d_0)$.
- Let N be any program point, and let $P_N = \{p \mid p \text{ is a path from } E \text{ to } N\}$.

Proof – continued

- Property (1), plus the property of joins, gives us

$$\bigsqcup_{p \in P_N} (\alpha(c_p)) \leq \bigsqcup_{p \in P_N} (d_p) \quad (2)$$

$$= \mathrm{JOP}_{\overline{D}}[N] \quad (3)$$

- By Corollary 1 we have

$$\bigsqcup_{p \in P_N} (\alpha(c_p)) = \alpha(\bigsqcup_{p \in P_N} (c_p)) \quad (4)$$

$$= \alpha(\mathrm{JOP}_{\overline{C}}[N]) \quad (5)$$

- Using Properties 3 and 5, and extending over all program points N we get

$$\overline{\alpha}(\mathrm{JOP}_{\overline{C}}) \leq \mathrm{JOP}_{\overline{D}}$$

  We are done.

More results

- From the previous result we can derive the other result in the AI correctness theorem:

$$\begin{aligned} \overline{\alpha}(\mathrm{JOP}_{\overline{C}}) &\leq \mathrm{JOP}_{\overline{D}} && \text{(previous result)} \\ \overline{\gamma}(\overline{\alpha}(\mathrm{JOP}_{\overline{C}})) &\leq \overline{\gamma}(\mathrm{JOP}_{\overline{D}}) && \text{(monotonicity of } \gamma\text{)} \\ \mathrm{JOP}_{\overline{C}} &\leq \overline{\gamma}(\mathrm{JOP}_{\overline{D}}) && \text{(property of Galois connection)} \end{aligned}$$

- It can also be shown that

$$\begin{aligned} \overline{\alpha}(\mathrm{LFP}_{\overline{C}}) &\leq \mathrm{LFP}_{\overline{D}} \\ \mathrm{LFP}_{\overline{C}} &\leq \overline{\gamma}(\mathrm{LFP}_{\overline{D}}) \end{aligned}$$