CS477 Formal Software Development Methods

Elsa L Gunter
2112 SC, UIUC
egunter@illinois.edu
http://courses.engr.illinois.edu/cs477

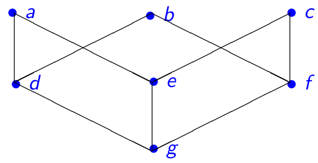
Slides based in part on previous lectures by Mahesh Vishwanathan, and by Gul Agha

May 14, 2013

Partial orders and Complete Lattices

A partial order on a set S is a binary relation $\leq$ on S such that

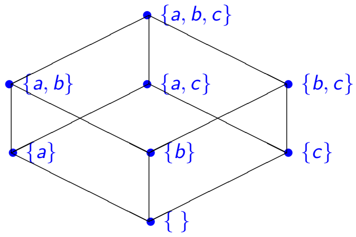
- **[Refl]** $s \leq s$ for all $s \in S$
- **[Antisym]** $s \leq t$ and $t \leq s$ impilies $s = t$, for all $s, t \in S$
- **[Trans]** $s \leq t$ and $t \leq u$ impilies $s \leq u$, for all $s, t, \in S$

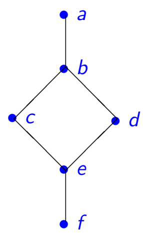


Upper Bounds and Complete Latices

- In a partial order $(S, \leq)$, given $X \subseteq S$, y is an upper bound for X if for all $x \in X$ we have $x \leq y$.
- y is a least upper bound of X, y is an upper bound of X and whenever z is an upper bound of X, $y \leq z$.
- **Note:** Least upper bounds are unique.
- A complete lattice is a partial order $(L, \leq)$ such that for all $X \subseteq S$ there exists a (unique) least upper bound.
- Write $\mathrm{lub}(X)$ or $\bigvee X$ for the least upper bound of X.
- Write $x \vee y$ for $\bigvee\{x, y\}$
- **Note:** $x \vee y = x \iff y \leq x$
- **Note:** Given a set S, $(\mathcal{P}(S), \subseteq)$ is a complete lattice.
- Write $\bot = \bigvee\{\ \}$ and $\top = bigveeS$

Example Complete Lattices





Partial Orders, Functions, and Complete Lattices

- Let X be an arbitrary set and A and B be partial orders.
- A function $f : A \to B$ is order-preserving if, for all $x, y \in A$ with $x \leq y$ we have $f(x) \leq f(y)$
- Function $f, g : X \to A$ may be ordered by pointwise comparrison:
  - Write $f \leq_{fun} g$ to mean that for all $x \in X$ we have $f(x) \leq g(x)$
  - Will leave off the subcript in general
- **Fact:** $(\{f \,.\, f : X \to B\}, \leq_{fun})$ is a partial order.
- **Fact:** $(\{f \,.\, f : X \to B\}, \leq_{fun})$ is a complete lattice if B is.
- **Fact:** $(\{f \,.\, f : A \to B,\ f \text{ order-preserving}\} \leq_{fun})$ is a complete lattice if B is.

Control-Flow Graphs

A Control-Flow Graph is a tuple (N, I, K, E) where

- N is a finite set of nodes
- $I : N \to \{\mathrm{Entry}, \mathrm{Exit}, \mathrm{i{:=}e}, \mathrm{if b}, \}$
- $K = \{\mathrm{yes}, \mathrm{no}, \mathrm{seq}\}$
- $E \subseteq N \times K \times N$ such that
  - for all $m \in N$ we have $|\{n \,.\, \exists k \in K.\,(m, k, n) \in E\}| \leq 2$
  - if $m \in N$ and $I(m) = \mathrm{Exit}$ then $|\{n \,.\, \exists k \in K.\,(m, k, n) \in E\}| = 0$
  - if $m \in N$ and $I(m) = \mathrm{Entry}$ or $I(m) = i := e$ for some identifier i and expression e, then $|\{k, n \,.\, (m, k, n) \in E\}| = 1$
  - if $m \in N$ and $I(m) = \mathrm{if}\ b$ for some boolean expression b, then $|\{n \,.\, \exists k \in K.\,(m, k, n) \in E\}| = 2$
- $k : E \to \{\mathrm{seq}, \mathrm{yes}, \mathrm{no}\}$ such that
  - if $(m, k, n) \in E$ and $I(m) = \mathrm{Entry}$ or $I(m) = i := e$, then $k = \mathrm{seq}$
  - if $m, \in N$ and $I(m) = \mathrm{if}\ b$, then $\{k \,.\, (m, k, n) \in E\} = \{\mathrm{yes}, \mathrm{no}\}$

Abstract Interpretation

- Let (N, I, K, E) be a control flow graph.
- An abstract interpretation of control flow graphs is a pair $(A, \mathcal{I})$ where
  - A is a complete latice and
  - $\mathcal{I} : ((E \to A) \times E) \to A$ (think *next state information vector*)
  - for all $a, b \in A$, for all $e \in E$, if $a \leq b$ then $\mathcal{I}(e, a) \leq \mathcal{I}(e, b)$

Abstract Semantics

- Can define $\overline{\mathcal{I}} : (E \to A) \to (E \to A)$ by $\overline{\mathcal{I}}(f)(e) = \mathcal{I}(f, e)$
- **Fact:** $\overline{\mathcal{I}}$ is order-preserving
- **Tarski's Fixed-Point Theorem:** If A is a complete lattice and $f : A \to A$ is order-preserving, then f has both a least and a greatest fixed-point (may or may not be the same).
- **Fact:** There exist $c : E \to A$ such that $oI(c) = c$, and that c is the least such.
- Write $\mu\overline{\mathcal{I}}$ for the least fixed point of $\overline{\mathcal{I}}$
- $\mu\overline{\mathcal{I}}$ is the abstract semantics of (N, I, K, E) with respect to $(A, \mathcal{I})$.

Standard Interpretation and Semantics

- Let (N, I, K, E) be a control flow graph with labels using variables from Var
- Let $Val = values \cup \{\top, \bot\}$, the extended set of values, ordered as before; $val : Exp \to Val$
- Let $Env = \mathcal{P}(\{\rho \,.\, \rho : Var \to Val\})$. Env is a complete lattice.
- Let $States = E \times Env$
- $\text{next\_state} : States \to States$; $\text{next\_state}((m, k, n), \rho)$ defined by cases on $I(n)$:
  - $I(n) \neq \text{Enter}$
  - $I(n) = \text{Exit} \Rightarrow \text{next\_state}((m, k, n), \rho) = ((m, k, n), \rho)$
  - $I(n) = (i := e)$, then n has unique successor node p, $(n, \text{suc}, p) \in E$.

$$\text{next\_state}((m, k, n), \rho) = ((n, \text{suc}, p), \rho[i \mapsto val(e, \rho)])$$

- Let $Interp(\theta, (m, k, n))$ is the lifting of next_state to sets of environments
  - $I(m) = \text{Enter} \Rightarrow Interp(\theta, (m, k, n)) = \{\bot_{Env}\}$
  - $I(m) \neq \text{Exit} \Rightarrow$
    $Interp(\theta, (m, k, n)) =$
    $\{\rho \mid \exists m',\ k',\ \rho' \,.\, (m', k', m) \in E \wedge$
    $\rho' \in \theta((m', k', m)) \wedge$
    $\text{next\_state}((m', k', m), \rho') = ((m, k, n), \rho)\}$
- If θ tells all the environments we might come into our edge with, $Interp(\theta, (m, k, n))$ tells us the set of environemts we may leave with
- **Fact:** $(Env, Interp)$ is an abtract interpretation
- μ *overlineInterp* tells us the best knowledge we can know statically about our program

Soundness of Abstract Semantics

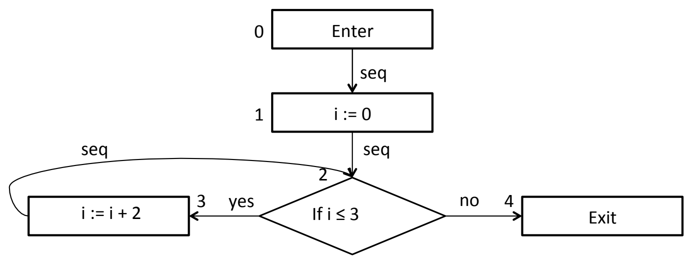
Fact: An abstract interpretation $(A, \mathcal{I})$ is sound (or consistent) with respect to $(Env, Interp)$ if and only if there exist $\alpha,\ \beta$ such that

- $\alpha : Env \to A$, $\beta : A \to Env$
- $\alpha,\ \beta$ order preserving
- For all $a \in A$ have $\alpha(\beta(a)) = a$
- For all $S \in Env$, have $S \leq \beta(\alpha(S))$ – We have more possibilities

Example

Consider the following control flow graph (N, I, K, E) where:

- $Var = \{i\}$, $val = \mathbb{Z}$
- $N = \{0, 1, 2, 3, 4, 5, 6\}$
- $I(0) = \text{Enter}$, $I(1) = \texttt{i:=0}$, $I(2) = \texttt{if 1} \leq \texttt{3}$, $I(3) = \texttt{i:=i+2}$, $I(4) = \text{Exit}$
- $K = \{\text{yes}, \text{no}, \text{seq}\}$
- $E = \left\{ \begin{array}{l} (0, \text{seq}, 1),\ (1, \text{seq}, 2), \\ (2, \text{yes}, 3),\ (2, \text{no}, 4), \\ (3, \text{seq}, 2) \end{array} \right\}$



Example: next_state

- $\text{next\_state}((0, \text{seq}, 1), \rho) = ((1, \text{seq}, 2)\{i \mapsto \bot\})$
- $\text{next\_state}((1, \text{seq}, 2), \rho) = ((2, \text{yes}, 3), \{i \mapsto 0\})$
- $\text{next\_state}((2, \text{yes}, 3), \rho) = ((3, \text{seq}, 2), \rho)$
- if $\rho(i) \leq 1$ then $\text{next\_state}((3, \text{seq}, 2), \rho) = ((2, \text{yes}, 3), \{i \mapsto \rho(i) + 2\})$
- if $\rho > 1$ then $\text{next\_state}((3, \text{seq}, 2), \rho) = ((2, \text{no}, 4), \{i \mapsto \rho(i) + 2\})$

Example: *Interp*

Let Θ map edges to sets of environments. *Interp* will tell us the set of environments next_state will associate with each edge assuming Θ gives a set of (possibly) possible environments for each predecessor edge:

- $\mathit{Interp}(\Theta, (0, \text{seq}, 1)) = \{\{i \mapsto \bot\}\}$
- $\mathit{Interp}(\Theta, (1, \text{seq}, 2)) = \{\rho \mid \exists \rho' \in \Theta(0, \text{seq}, 1) \,.\, \rho = \rho'[i \mapsto 0]\}$
  $= \{\{i \mapsto 0\}\}$ if $\Theta(0, \text{seq}, 1) \neq \{\,\}$ since $\mathit{Var} = \{i\}$
- $\mathit{Interp}(\Theta, (2, \text{yes}, 3)) = \Theta(1, \text{seq}, 2) \cup \{\rho \in \Theta(3, \text{seq}, 2) \mid \rho(i) \leq 3\}$
- $\mathit{Interp}(\Theta, (3, \text{seq}, 2)) = \{\rho \mid \exists \rho' \in \Theta(2, \text{yes}, 3) \,.\, \rho = \rho`[i \mapsto \rho'(i) + 2]\}$
- $\mathit{Interp}(\Theta, (2, \text{no}, 4)) = \{\rho \in \Theta(3, \text{seq}, 2) \mid \rho(i) > 3\}$

- $\overline{\mathit{Interp}}(\Theta)(e) = \mathit{Interp}(\Theta, e)$
- $\overline{\mathit{Interp}}^0(\Theta)(e) = \{\,\}$ $\quad \overline{\mathit{Interp}}^{n+1}(\Theta)(e) = \overline{\mathit{Interp}}(\overline{\mathit{Interp}}^n(\Theta))(e)$

Example: μ*Interp*

- $\mu \mathit{Inter} : E \to \mathcal{P}(\mathit{Env})$
- Start with minimal Θ_0 assigning no evnironments to any edge: $\Theta_0(e) = \{\,\}$
- $\mu \mathit{Interp}(e) = \bigcup_{n \in \mathbb{N}} \overline{\mathit{Interp}}^n(e)$
- $\mu \mathit{Interp}(0, \text{seq}, 1) = \{ \quad \}$
- $\mu \mathit{Interp}(1, \text{seq}, 2) = \{ \quad \}$
- $\mu \mathit{Interp}(2, \text{yes}, 3) = \{ \quad \}$
- $\mu \mathit{Interp}(3, \text{seq}, 2) = \{ \quad \}$
- $\mathit{Interp}(\Theta, (2, \text{no}, 4)) = \{ \quad \}$

Example: μ*Interp*

- $\mu \mathit{Inter} : E \to \mathcal{P}(\mathit{Env})$
- Start with minimal Θ_0 assigning no evnironments to any edge: $\Theta_0(e) = \{\,\}$
- $\mu \mathit{Interp}(e) = \bigcup_{n \in \mathbb{N}} \overline{\mathit{Interp}}^n(e)$
- $\mu \mathit{Interp}(0, \text{seq}, 1) = \{\{i \mapsto \bot\}\}$
- $\mu \mathit{Interp}(1, \text{seq}, 2) = \{ \quad \}$
- $\mu \mathit{Interp}(2, \text{yes}, 3) = \{ \quad \}$
- $\mu \mathit{Interp}(3, \text{seq}, 2) = \{ \quad \}$
- $\mathit{Interp}(\Theta, (2, \text{no}, 4)) = \{ \quad \}$

Example: μ*Interp*

- $\mu \mathit{Inter} : E \to \mathcal{P}(\mathit{Env})$
- Start with minimal Θ_0 assigning no evnironments to any edge: $\Theta_0(e) = \{\,\}$
- $\mu \mathit{Interp}(e) = \bigcup_{n \in \mathbb{N}} \overline{\mathit{Interp}}^n(e)$
- $\mu \mathit{Interp}(0, \text{seq}, 1) = \{\{i \mapsto \bot\}\}$
- $\mu \mathit{Interp}(1, \text{seq}, 2) = \{\{i \mapsto 0\}\}$
- $\mu \mathit{Interp}(2, \text{yes}, 3) = \{ \quad \}$
- $\mu \mathit{Interp}(3, \text{seq}, 2) = \{ \quad \}$
- $\mathit{Interp}(\Theta, (2, \text{no}, 4)) = \{ \quad \}$

Example: $\mu Interp$

- $\mu Inter : E \to \mathcal{P}(Env)$
- Start with minimal Θ_0 assigning no evnironments to any edge: $\Theta_0(e) = \{\,\}$
- $\mu Interp(e) = \bigcup_{n\in\mathbb{N}} \overline{Interp}^n(e)$
- $\mu Interp(0, \text{seq}, 1) = \{\{i \mapsto \bot\}\}$
- $\mu Interp(1, \text{seq}, 2) = \{\{i \mapsto 0\}\}$
- $\mu Interp(2, \text{yes}, 3) = \{\{i \mapsto 0\}, \quad \}$
- $\mu Interp(3, \text{seq}, 2) = \{ \quad \}$
- $Interp(\Theta, (2, \text{no}, 4)) = \{ \quad \}$

Example: $\mu Interp$

- $\mu Inter : E \to \mathcal{P}(Env)$
- Start with minimal Θ_0 assigning no evnironments to any edge: $\Theta_0(e) = \{\,\}$
- $\mu Interp(e) = \bigcup_{n\in\mathbb{N}} \overline{Interp}^n(e)$
- $\mu Interp(0, \text{seq}, 1) = \{\{i \mapsto \bot\}\}$
- $\mu Interp(1, \text{seq}, 2) = \{\{i \mapsto 0\}\}$
- $\mu Interp(2, \text{yes}, 3) = \{\{i \mapsto 0\}, \quad \}$
- $\mu Interp(3, \text{seq}, 2) = \{\{i \mapsto 2\}, \quad \}$
- $Interp(\Theta, (2, \text{no}, 4)) = \{ \quad \}$

Example: $\mu Interp$

- $\mu Inter : E \to \mathcal{P}(Env)$
- Start with minimal Θ_0 assigning no evnironments to any edge: $\Theta_0(e) = \{\,\}$
- $\mu Interp(e) = \bigcup_{n\in\mathbb{N}} \overline{Interp}^n(e)$
- $\mu Interp(0, \text{seq}, 1) = \{\{i \mapsto \bot\}\}$
- $\mu Interp(1, \text{seq}, 2) = \{\{i \mapsto 0\}\}$
- $\mu Interp(2, \text{yes}, 3) = \{\{i \mapsto 0\}, \{i \mapsto 2\}\}$
- $\mu Interp(3, \text{seq}, 2) = \{\{i \mapsto 2\}, \quad \}$
- $Interp(\Theta, (2, \text{no}, 4)) = \{ \quad \}$

Example: $\mu Interp$

- $\mu Inter : E \to \mathcal{P}(Env)$
- Start with minimal Θ_0 assigning no evnironments to any edge: $\Theta_0(e) = \{\,\}$
- $\mu Interp(e) = \bigcup_{n\in\mathbb{N}} \overline{Interp}^n(e)$
- $\mu Interp(0, \text{seq}, 1) = \{\{i \mapsto \bot\}\}$
- $\mu Interp(1, \text{seq}, 2) = \{\{i \mapsto 0\}\}$
- $\mu Interp(2, \text{yes}, 3) = \{\{i \mapsto 0\}, \{i \mapsto 2\}\}$
- $\mu Interp(3, \text{seq}, 2) = \{\{i \mapsto 2\}, \{i \mapsto 4\}\}$
- $Interp(\Theta, (2, \text{no}, 4)) = \{ \quad \}$

Example: $\mu Interp$

- $\mu Inter : E \to \mathcal{P}(Env)$
- Start with minimal Θ_0 assigning no evnironments to any edge: $\Theta_0(e) = \{\,\}$
- $\mu Interp(e) = \bigcup_{n\in\mathbb{N}} \overline{Interp}^n(e)$
- $\mu Interp(0, \text{seq}, 1) = \{\{i \mapsto \bot\}\}$
- $\mu Interp(1, \text{seq}, 2) = \{\{i \mapsto 0\}\}$
- $\mu Interp(2, \text{yes}, 3) = \{\{i \mapsto 0\}, \{i \mapsto 2\}\}$
- $\mu Interp(3, \text{seq}, 2) = \{\{i \mapsto 2\}, \{i \mapsto 4\}\}$
- $Interp(\Theta, (2, \text{no}, 4)) = \{\{i \mapsto 4\}\}$

Example: $\mu Interp$

- $\mu Inter : E \to \mathcal{P}(Env)$
- Start with minimal Θ_0 assigning no evnironments to any edge: $\Theta_0(e) = \{\,\}$
- $\mu Interp(e) = \bigcup_{n\in\mathbb{N}} \overline{Interp}^n(e)$
- $\mu Interp(0, \text{seq}, 1) = \{\{i \mapsto \bot\}\}$
- $\mu Interp(1, \text{seq}, 2) = \{\{i \mapsto 0\}\}$
- $\mu Interp(2, \text{yes}, 3) = \{\{i \mapsto 0\}, \{i \mapsto 2\}\}$
- $\mu Interp(3, \text{seq}, 2) = \{\{i \mapsto 2\}, \{i \mapsto 4\}\}$
- $Interp(\Theta, (2, \text{no}, 4)) = \{\{i \mapsto 4\}\}$