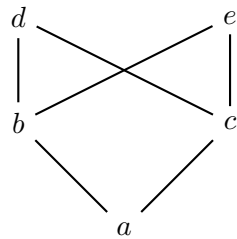


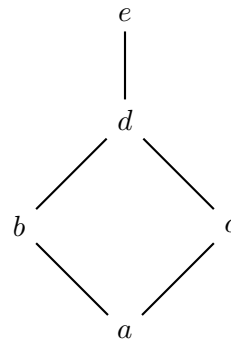
Exercise 9

Exercise 1

Are (a) and (b) complete lattices?



(a)



(b)

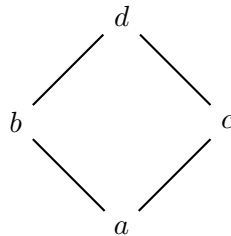
Solution:

(a) is not a complete lattice because $d \sqcup e$ does not exist.

(b) is a complete lattice.

Exercise 2

Consider the lattice $L = (A, \sqsubseteq)$, where $A = \{a, b, c, d\}$. The partial order $\sqsubseteq \subseteq A \times A$ is depicted in the Hasse diagram below.

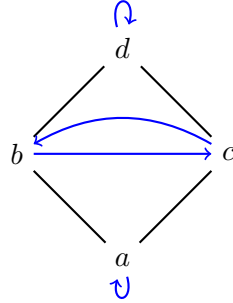


1. List the elements of \sqsubseteq .

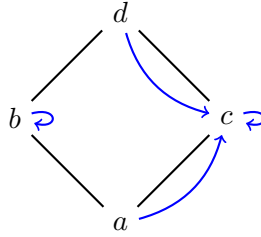
Solution:

$$\sqsubseteq = \{(a, a), (b, b), (c, c), (d, d), (a, b), (a, c), (b, d), (c, d), (a, d)\}$$

2. Consider the following functions $f, g : A \mapsto A$



Function f



Function g

- Is f monotone? Is g monotone?

Solution:

f is monotone.

g is not monotone because $b \sqsubseteq d$ but $g(b) = b \not\sqsubseteq g(d) = c$.

- List the set $Fix(f)$ of fixpoints of f , and the set $Red(f)$ of post-fixpoints of f .

Solution:

$Fix(f) = \{a, d\}$.

$Red(f) = \{a, d\}$.

- List the sets of fixpoints/post-fixpoints of the function g .

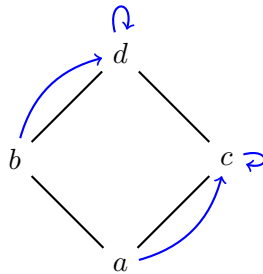
Solution:

$Fix(g) = \{b, c\}$.

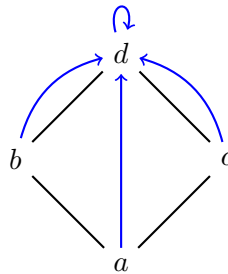
$Red(g) = \{b, c, d\}$.

Exercise 3

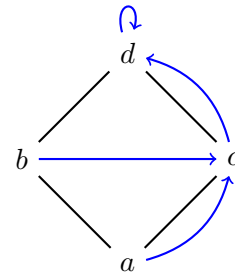
1. Consider the following three functions: $f, g, h : A \mapsto A$, defined below:



Function f



Function g



Function h

- Does g approximate f ?

Solution:

Yes, g approximates f .

- Does h approximate f ?

Solution:

No, h does not approximate f because $f(b) = d \not\sqsubseteq h(b) = c$.

2. Let $R = \mathbb{R} \cup \{-\infty, +\infty\}$ and $Z = \mathbb{Z} \cup \{-\infty, +\infty\}$, where \mathbb{R} is the set of rational numbers and \mathbb{Z} is the set of integers.

(R, \leq) and (Z, \leq) are complete lattices.

Let $\alpha : R \mapsto Z$ as $\alpha(x) = \lceil x \rceil$. (Here $\lceil x \rceil$ rounds-up x to the nearest integer.)

Let $\gamma : Z \mapsto R$ as $\gamma(x) = x$.

Consider the function $f : R \mapsto R$ defined as $f(x) = x^2$.

- Give two functions $g, h : Z \mapsto Z$ that approximate f . Which one is more precise?

Solution:

$$g(x) = |x + 1|^2$$

$$h(x) = \begin{cases} x^2 & \text{if } x \geq 0 \\ (|x| + 1)^2 & \text{otherwise} \end{cases}$$

h is more precise.

- Give a function $k : Z \mapsto Z$ that approximates any function $f : R \mapsto R$.

Solution:

$$k(x) = +\infty.$$

Exercise 4

Recall that an interval transformer for an action a is defined as:

$$\llbracket a \rrbracket_i : (Var \mapsto L^i) \mapsto (Var \mapsto L^i)$$

where $L^i = \{[x, y] \mid x, y \in \mathbb{Z}^\infty, x \leq y\} \cup \{\perp_i\}$ are the interval domain's elements (see slide 17 from the lecture).

1. Consider the interval maps:

$$m_1 = x \mapsto [-3, 8], y \mapsto [0, 5]$$

$$m_2 = x \mapsto [-3, 8], y \mapsto \perp_i$$

The interval transformer for \leq is defined on slide 33. Apply the transformer to compute the result of:

$$\llbracket x \leq y \rrbracket(m_1) = \quad \quad \quad \llbracket x \leq y \rrbracket(m_2) =$$

$$\llbracket 3 \leq 5 \rrbracket(m_1) = \quad \quad \quad \llbracket 3 \leq 5 \rrbracket(m_2) =$$

$$\llbracket 5 \leq 3 \rrbracket(m_1) = \quad \quad \quad \llbracket 5 \leq 3 \rrbracket(m_2) =$$

Solution:

$$\llbracket x \leq y \rrbracket(m_1) = y \mapsto [-3, 5], y \mapsto [0, 5]$$

$$\llbracket 3 \leq 5 \rrbracket(m_1) = x \mapsto [-3, 8], y \mapsto [0, 5]$$

$$\llbracket 5 \leq 3 \rrbracket(m_1) = x \mapsto \perp_i, y \mapsto \perp_i$$

$$\llbracket x \leq y \rrbracket(m_2) = x \mapsto \perp_i, y \mapsto \perp_i$$

$$\llbracket 3 \leq 5 \rrbracket(m_2) = x \mapsto \perp_i, y \mapsto \perp_i$$

$$\llbracket 5 \leq 3 \rrbracket(m_2) = x \mapsto \perp_i, y \mapsto \perp_i$$

2. Define the interval transformer for assignment:

Solution:

$$\llbracket x := a \rrbracket(m) = m[x \mapsto [p, q]] \text{ where } \langle a, m \rangle \Downarrow_i [p, q]$$

3. Define the multiplication expression for interval elements:

Solution:

Let

$$\langle a_1, m \rangle \Downarrow_i [p, q]$$

$$\langle a_2, m \rangle \Downarrow_i [r, s]$$

$$A = \{p * r, p * s, q * r, q * s\}$$

Then,

$$\langle a_1 * a_2, m \rangle \Downarrow_i [\min(A), \max(A)]$$

4. Define the interval transformer for equality:

Solution:

Let

$$\llbracket x = y \rrbracket(m) = m[x \mapsto m(x) \sqcap_i m(y), y \mapsto m(x) \sqcap_i m(y)]$$

Recall that if $m(x) = [p, q]$ and $m(y) = [r, s]$ then

$$[p, q] \sqcap_i [r, s] = \begin{cases} [\max(p, r), \min(q, s)] & \text{if } \max(p, r) \leq \min(q, s) \\ \perp_i & \text{otherwise} \end{cases}$$

Exercise 5

Consider the following program:

```
foo (int x) {  
1   y := 2  
2   if (x <= y)  
3       z := 3 * x  
   else  
4       z := y  
5   z := y * z  
6 }
```

- Give two concrete traces t_1 and t_2 of the program.

Solution:

Trace t_1 for `foo(1)`:

$(y := 2; (\text{if } (x \leq y) \ z := 3 * x; \text{ else } z := y;); z := y * z, \{x \mapsto 1, y \mapsto 0, z \mapsto 0\})$
 $\rightarrow ((\text{if } (x \leq y) \ z := 3 * x; \text{ else } z := y;); z := y * z, \{x \mapsto 1, y \mapsto 2, z \mapsto 0\})$
 $\rightarrow (z := 3 * x; z := y * z, \{x \mapsto 1, y \mapsto 2, z \mapsto 0\})$
 $\rightarrow (z := y * z, \{x \mapsto 1, y \mapsto 2, z \mapsto 3\})$
 $\rightarrow \{x \mapsto 1, y \mapsto 2, z \mapsto 6\}$

Trace t_2 for `foo(5)`:

$(y := 2; (\text{if } (x \leq y) \ z := 3 * x; \text{ else } z := y;); z := y * z, \{x \mapsto 5, y \mapsto 0, z \mapsto 0\})$
 $\rightarrow ((\text{if } (x \leq y) \ z := 3 * x; \text{ else } z := y;); z := y * z, \{x \mapsto 5, y \mapsto 2, z \mapsto 0\})$
 $\rightarrow (z := y; z := y * z, \{x \mapsto 5, y \mapsto 2, z \mapsto 0\})$
 $\rightarrow (z := y * z, \{x \mapsto 5, y \mapsto 2, z \mapsto 2\})$
 $\rightarrow \{x \mapsto 5, y \mapsto 2, z \mapsto 4\}$

- Apply the interval abstraction function α^i given on slide 19 from the lecture on the set $\{t_1, t_2\}$.

Solution:

$\{1 \mapsto \{x \mapsto [1, 5], y \mapsto [0, 0], z \mapsto [0, 0]\},$
 $\{2 \mapsto \{x \mapsto [1, 5], y \mapsto [2, 2], z \mapsto [0, 0]\},$
 $\{3 \mapsto \{x \mapsto [1, 1], y \mapsto [2, 2], z \mapsto [0, 0]\},$
 $\{4 \mapsto \{x \mapsto [5, 5], y \mapsto [2, 2], z \mapsto [0, 0]\},$
 $\{5 \mapsto \{x \mapsto [1, 5], y \mapsto [2, 2], z \mapsto [2, 3]\},$
 $\{6 \mapsto \{x \mapsto [1, 5], y \mapsto [2, 2], z \mapsto [4, 6]\},$

- Compute the least fixpoint $\text{lfp} F^i$ of the program using the interval domain abstraction.

Solution:

$\{1 \mapsto \{x \mapsto [-\infty, +\infty], y \mapsto [-\infty, +\infty], z \mapsto [-\infty, +\infty]\},$
 $\{2 \mapsto \{x \mapsto [-\infty, +\infty], y \mapsto [2, 2], z \mapsto [-\infty, +\infty]\},$
 $\{3 \mapsto \{x \mapsto [-\infty, 2], y \mapsto [2, 2], z \mapsto [-\infty, +\infty]\},$
 $\{4 \mapsto \{x \mapsto [3, +\infty], y \mapsto [2, 2], z \mapsto [-\infty, +\infty]\},$
 $\{5 \mapsto \{x \mapsto [-\infty, +\infty], y \mapsto [2, 2], z \mapsto [-\infty, 6]\},$
 $\{6 \mapsto \{x \mapsto [-\infty, +\infty], y \mapsto [2, 2], z \mapsto [-\infty, 12]\},$

- Give a concrete trace $t \in \gamma^i(\text{lfp} F^i)$ that is not a valid trace. Here γ^i is the concretization function; see slides 19-20 from the lecture.

Solution:

$(y := 2; (\text{if } (x \leq y) \ z := 3 * x; \text{ else } z := y;); z := y * z, \{x \mapsto 0, y \mapsto 0, z \mapsto 0\})$
 $\rightarrow ((\text{if } (x \leq y) \ z := 3 * x; \text{ else } z := y;); z := y * z, \{x \mapsto 5, y \mapsto 2, z \mapsto 0\})$
 $\rightarrow \star$