

Exercise 10 (Solution)

Exercise 1

Recall (see slide 19 from the lecture “Applications”) that an interval transformer for an *action* has the type:

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

where L^i are the elements of the interval domain ($L^i = \{[x, y] \mid x, y \in \mathbb{Z}^\infty, x \leq y\} \cup \{\perp_i\}$).

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 28. Apply the transformer to compute the result of:

Solution:

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

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

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

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

$$\llbracket 3 \leq 5 \rrbracket(m_2) = x \mapsto [-3, 8], y \mapsto \perp_i$$

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

2. Define the interval transformer for assignment:

Solution:

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

3. Define the multiplication expression for interval elements:

Solution:

$$\text{Let } \langle a_1, m \rangle \Downarrow_i [p, q], \langle a_2, m \rangle \Downarrow_i [r, s], A = \{p * r, p * s, q * r, q * s\}$$

$$\text{Then, } \langle a_1 * a_2, m \rangle \Downarrow_i [\min(A), \max(A)].$$

4. Define the interval transformer for equality:

Solution:

Let

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

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 2

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)`:

$(1, \{x \mapsto 1, y \mapsto 0, z \mapsto 0\}) \rightarrow (2, \{x \mapsto 1, y \mapsto 2, z \mapsto 0\})$
 $\rightarrow (3, \{x \mapsto 1, y \mapsto 2, z \mapsto 0\}) \rightarrow (5, \{x \mapsto 1, y \mapsto 2, z \mapsto 3\})$
 $\rightarrow (6, \{x \mapsto 1, y \mapsto 2, z \mapsto 6\})$

Trace t_2 for `foo(5)`:

$(1, \{x \mapsto 5, y \mapsto 0, z \mapsto 0\}) \rightarrow (2, \{x \mapsto 5, y \mapsto 2, z \mapsto 0\})$
 $\rightarrow (4, \{x \mapsto 5, y \mapsto 2, z \mapsto 0\}) \rightarrow (5, \{x \mapsto 5, y \mapsto 2, z \mapsto 2\})$
 $\rightarrow (6, \{x \mapsto 5, y \mapsto 2, z \mapsto 4\})$

- Apply the interval abstraction function α^i given on slide 21 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 21-22 from the lecture.

Solution:

$(1, \{x \mapsto 0, y \mapsto 0, z \mapsto 0\}) \rightarrow (2, \{x \mapsto 5, y \mapsto 2, z \mapsto 0\}) \rightarrow \dots$

Exercise 3

Give two programs that are output equivalent (i.e. for the same initial state they result in the same final state) under the concrete domain, and they are not output equivalent under the interval domain.

Solution:

Program P_1

```

1      x := 2
2      sq_x := x*x
3      i = 0

```

Program P_2

```

1      x := 2
2      sq_x := 0
3      i := x
4      while (i > 0) do
5          sq_x := sq_x + x
6          i := i - 1

```

The programs are equivalent because for any initial state the programs' final state is $\{x \mapsto 2, sq_x \mapsto 4, i \mapsto 0\}$.

If we compute P_1 's least fixed point under the interval domain, at the end of P_1 we have $\{x \mapsto [2, 2], sq_x \mapsto [4, 4], i \mapsto [0, 0]\}$.

For P_2 we have $\{x \mapsto [2, 2], sq_x \mapsto [0, 4], i \mapsto [0, 0]\}$.