

Assignment 9 (Solution)

Exercise 1

Recall (see slide 19 from the lecture) 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 31. Apply the transformer to compute the result of:

Solution:

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

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

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

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

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

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

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 slides 14-15 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. Does it approximate t_1 and t_2 ?

Solution:

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

Yes, it approximates t_1 and t_2 .

- 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 14-15 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

Consider the following program:

```

foo (int x) {
1:   y := 0
2:   while (x > 0 && x <= 100)
3:       y := y + x
4:       x := x - 1
      end
5: }
```

- Compute the least fixpoint $\text{lfp}F^i$ of the program using the interval domain abstraction and the widening operator given on slide 57.

Solution:

$\{1 \mapsto \{x \mapsto [-\infty, +\infty], y \mapsto [-\infty, +\infty]\},$
 $\{2 \mapsto \{x \mapsto [-\infty, +\infty], y \mapsto [0, +\infty]\},$
 $\{3 \mapsto \{x \mapsto [1, 100], y \mapsto [0, +\infty]\},$
 $\{4 \mapsto \{x \mapsto [1, 100], y \mapsto [1, +\infty]\},$
 $\{5 \mapsto \{x \mapsto [-\infty, +\infty], y \mapsto [0, +\infty]\},$

- Does there exist a concrete trace such that x has value 10 at label 5? What are the possible values for x at label 5?

Solution:

No, it's impossible. The set of possible concrete values is $\mathbb{Z} \setminus \{1, 2, \dots, 100\}$.