Assignment 9 (Solution)

Exercise 1

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

$$[\![action]\!]_i : (Var \mapsto L^i) \mapsto (Var \mapsto L^i)$$

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

1. Consider the interval maps:

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

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

   The interval transformer for $\leq$ is defined on slide 28. Apply the transformer to compute the result of:

   Solution:

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

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

   $[\![5 \leq 3]\!](m_1) = \ x \mapsto \bot_i, y \mapsto \bot_i$

   $[\![x \leq y]\!](m_2) = \ x \mapsto \bot_i, y \mapsto \bot_i$

   $[\![3 \leq 5]\!](m_2) = \ x \mapsto \bot_i, y \mapsto \bot_i$

   $[\![5 \leq 3]\!](m_2) = \ x \mapsto \bot_i, y \mapsto \bot_i$

2. Define the interval transformer for assignment:

   Solution:

   $[\![x := a]\!]_i(m) = \ m[x \mapsto [p, q]]$ 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, $\langle a_1 * a_2, m\rangle \Downarrow_i [min(A), max(A)]$.

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)`:

  $(1, \{x \mapsto 1, y \mapsto 0, z \mapsto 0\}) \to (2, \{x \mapsto 1, y \mapsto 2, z \mapsto 0\})$

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

  $\to (6, \{x \mapsto 1, y \mapsto 2, z \mapsto 6\})$

  Trace t_2 for `foo(5)`:

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

  $\to (4, \{x \mapsto 5, y \mapsto 2, z \mapsto 0\}) \to (5, \{x \mapsto 5, y \mapsto 2, z \mapsto 2\})$

  $\to (6, \{x \mapsto 5, y \mapsto 2, z \mapsto 4\})$

- 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 $\mathsf{lfp}F^i$ 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 $t \in \gamma^i(\mathsf{lfp}F^i)$ that is not a valid trace. Here γ^i is the concretization function; see slides 21-22 from the lecture.

  Solution:

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

Exercise 3

What are the correct transformers for $-, /$ in the interval domain?

Solution

- Subtraction:

$$[l_1, u_1] - [l_2, u_2] = [l_1, u_1] + [-u_2, -l_2]$$

- Integer division:

  Let the set $S = \{l_1/l_2, l_1/u_2, u_1/l_2, u_1/u_2\}$

  If $0 \notin [l_2, u_2]$:

$$[l_1, u_1]/[l_2, u_2] = [min(S), max(S)]$$

  If $0 \in [l_2, u_2]$:

$$[l_1, u_1]/[l_2, u_2] = \top$$

  ,

Exercise 4

For the interval domain, what is $pair_<$ and $pair_=$?

Solution

$$pair_<([l_1, u_1], [l_2, u_2]) = ([l_1, u_1] \sqcap_i [-\infty, u_2 - 1], [l_1 + 1, \infty] \sqcap_i [l_2, u_2])$$

$$pair_=([l_1, u_1], [l_2, u_2]) = ([l_1, u_1] \sqcap_i [l_2, u_2], [l_1, u_1] \sqcap_i [l_2, u_2])$$

Exercise 5

Show 2 programs that are equivalent (for the same input state, they always produce the same output state) in the concrete but under the Interval domain, the invariants produced are not equivalent.

Solution

Program 1:

```
x = 2;
y = 1;
i = x * y;
x = 0;
```

Under the Interval domain, at the end of this program we have the invariant:

$x \mapsto [0,0], y \mapsto [1,1], i \mapsto [2,2]$

Program 2:

```
x = 2;
y = 1;
i = 0;
while (x > 0) do
  i = i + y;
  x = x - 1;
```

Under the Interval domain, at the end of this program, we have the invariant:

$x \mapsto [0,0], y \mapsto [1,1], i \mapsto [0,2]$

As we see, Program 1 and Program 2 are equivalent in the concrete, but under the Interval domain they produce different invariants.