Assignment 9: Solution

Exercise 1

1. Inference rules for v, $a_1 - a_2$, and $a_1 * a_2$:

$$\frac{}{\langle v, \sigma\rangle \Downarrow_a v} \qquad \frac{\langle a_1, \sigma\rangle \Downarrow_a v_1 \qquad \langle a_2, \sigma\rangle \Downarrow_a v_2}{\langle a_1 - a_2, \sigma\rangle \Downarrow_a v_1 - v_2} \qquad \frac{\langle a_1, \sigma\rangle \Downarrow_a v_1 \qquad \langle a_2, \sigma\rangle \Downarrow_a v_2}{\langle a_1 * a_2, \sigma\rangle \Downarrow_a v_1 * v_2}$$

2. Inference rules for true, false, $\neg b$ and $b_1 \vee b_2$:

$$\frac{}{\langle \mathsf{true}, \sigma\rangle \Downarrow_b \mathsf{true}} \qquad \frac{}{\langle \mathsf{false}, \sigma\rangle \Downarrow_b \mathsf{false}} \qquad \frac{\langle b, \sigma\rangle \Downarrow_b \mathsf{true}}{\langle \neg b, \sigma\rangle \Downarrow_b \mathsf{false}} \qquad \frac{\langle b, \sigma\rangle \Downarrow_b \mathsf{false}}{\langle \neg b, \sigma\rangle \Downarrow_b \mathsf{true}}$$

$$\frac{\langle b_1, \sigma\rangle \Downarrow_b \mathsf{true}}{\langle b_1 \vee b_2, \sigma\rangle \Downarrow_b \mathsf{true}} \qquad \frac{\langle b_2, \sigma\rangle \Downarrow_b \mathsf{true}}{\langle b_1 \vee b_2, \sigma\rangle \Downarrow_b \mathsf{true}} \qquad \frac{\langle b_1, \sigma\rangle \Downarrow_b \mathsf{false} \qquad \langle b_2, \sigma\rangle \Downarrow_b \mathsf{false}}{\langle b_1 \vee b_2, \sigma\rangle \Downarrow_b \mathsf{false}}$$

3. Show that $\langle (x-2 \leq y) \wedge (\neg \mathsf{false}), \sigma\rangle \Downarrow_b \mathsf{true}$, where $\sigma = \{x \mapsto 1, y \mapsto 2\}$:

$$\dfrac{\dfrac{\dfrac{\langle x, \sigma\rangle \Downarrow_a 1 \qquad \langle 1, \sigma\rangle \Downarrow_a 1}{\langle x+1, \sigma\rangle \Downarrow_a 2} \qquad \langle y, \sigma\rangle \Downarrow_a 2}{\langle x+1 \leq y, \sigma\rangle \Downarrow_b \mathsf{true}} \qquad \dfrac{\langle \mathsf{false}, \sigma\rangle \Downarrow_b \mathsf{false}}{\langle \neg \mathsf{false}, \sigma\rangle \Downarrow_b \mathsf{true}}}{\langle (x+1 \leq y) \wedge (\neg \mathsf{false}), \sigma\rangle \Downarrow_b \mathsf{true}}$$

Exercise 2

1. The program P can be defined as:
   if $x \leq 0$ **then** $x := x * (-1)$ **else skip**

2. The longest trace is:

   $c_0 \equiv \langle \textbf{if } x \leq 0 \textbf{ then } x := x * (-1) \textbf{ else skip}, \{x \mapsto -1\}\rangle$

   $\rightarrow c_1 \equiv \langle \textbf{if } \mathsf{true} \textbf{ then } x := x * (-1) \textbf{ else skip}, \{x \mapsto -1\}\rangle$

   $\rightarrow c_2 \equiv \langle x := x * (-1), \{x \mapsto -1\}\rangle$

   $\rightarrow c_3 \equiv \langle x := 1, \{x \mapsto -1\}\rangle$

   $\rightarrow c_4 \equiv \langle \{x \mapsto 1\}\rangle$

For the steps $c_1 \to c_2$ and $c_3 \to c_4$ we do not need any hypotheses. For the other two steps the hypotheses are:

$$\frac{\langle x \leq 0, \{x \mapsto -1\}\rangle \Downarrow_b \mathsf{true}}{c_0 \to c_1} \qquad \frac{\langle x * (-1), \{x \mapsto -1\}\rangle \Downarrow_a 1}{c_2 \to c_3}$$

Exercise 3

pc	x	y
0	$\bot$	$\bot$
1	$\bot$	$\bot$
2	$\bot$	$\bot$
3	$\bot$	$\bot$
4	$\bot$	$\bot$
5	$\bot$	$\bot$
6	$\bot$	$\bot$

$\to$

pc	x	y
0	$\top$	$\top$
1	$\bot$	$\bot$
2	$\bot$	$\bot$
3	$\bot$	$\bot$
4	$\bot$	$\bot$
5	$\bot$	$\bot$
6	$\bot$	$\bot$

$\to$

pc	x	y
0	$\top$	$\top$
1	*even*	$\top$
2	$\bot$	$\bot$
3	$\bot$	$\bot$
4	$\bot$	$\bot$
5	$\bot$	$\bot$
6	$\bot$	$\bot$

$\to$

pc	x	y
0	$\top$	$\top$
1	*even*	$\top$
2	*even*	$\top$
3	$\bot$	$\bot$
4	$\bot$	$\bot$
5	$\bot$	$\bot$
6	*even*	$\top$

$\to$

pc	x	y
0	$\top$	$\top$
1	*even*	$\top$
2	*even*	$\top$
3	$\bot$	$\bot$
4	*even*	$\top$
5	$\bot$	$\bot$
6	*even*	$\top$

$\to$

pc	x	y
0	$\top$	$\top$
1	*even*	$\top$
2	*even*	$\top$
3	$\bot$	$\bot$
4	*even*	$\top$
5	*even*	*odd*
6	*even*	$\top$

Exercise 4

The domains Sign and Interval are comparable. Parity is not comparable with both Sign and Interval.

1. The Interval domain is more precise than Sign. This is because any state expressed with the Sign domain can be expressed with the Interval domain. The converse does not hold, there are states expressed using the Interval domain that cannot be expressed using the Sign domain.

2. The following program can be verified using the Interval domain, but it cannot be verified with the Parity domain:

   ```
   int x = 1;
   assert x > 0;
   ```

   The following program can be verified using the Parity domain, but it cannot be verified with the Interval domain:

```
foo(int i) {
  x := 2*i;
  assert x is even;
}
```