CS 260: Assignment #3

Due on Tuesday, November 3, 2015

Prof. Hardekopf

Chad Spensky

	$\bot$	$\mathbb{Z}-$	0	$\mathbb{Z}+$	$\top$
$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$
$\mathbb{Z}-$	$\bot$	$\mathbb{Z}-$	$\mathbb{Z}-$	$\top$	$\top$
0	$\bot$	$\mathbb{Z}-$	0	$\mathbb{Z}+$	$\top$
$\mathbb{Z}+$	$\bot$	$\top$	$\mathbb{Z}+$	$\mathbb{Z}+$	$\top$
$\top$	$\bot$	$\top$	$\top$	$\top$	$\top$

(a) Addition

	$\bot$	$\mathbb{Z}-$	0	$\mathbb{Z}+$	$\top$
$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$
$\mathbb{Z}-$	$\bot$	$\top$	$\mathbb{Z}-$	$\mathbb{Z}-$	$\top$
0	$\bot$	$\mathbb{Z}+$	0	$\mathbb{Z}-$	$\top$
$\mathbb{Z}+$	$\bot$	$\mathbb{Z}+$	$\mathbb{Z}+$	$\top$	$\top$
$\top$	$\bot$	$\top$	$\top$	$\top$	$\top$

(b) Subtraction

	$\bot$	$\mathbb{Z}-$	0	$\mathbb{Z}+$	$\top$
$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$
$\mathbb{Z}-$	$\bot$	$\mathbb{Z}+$	0	$\mathbb{Z}-$	$\top$
0	$\bot$	0	0	0	0
$\mathbb{Z}+$	$\bot$	$\mathbb{Z}-$	0	$\mathbb{Z}+$	$\top$
$\top$	$\bot$	$\top$	0	$\top$	$\top$

(c) Multiplication

	$\bot$	$\mathbb{Z}-$	0	$\mathbb{Z}+$	$\top$
$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$
$\mathbb{Z}-$	$\bot$	$\mathbb{Z}+$	$\bot$	$\mathbb{Z}-$	$\top$
0	$\bot$	0	$\bot$	0	0
$\mathbb{Z}+$	$\bot$	$\mathbb{Z}-$	$\bot$	$\mathbb{Z}+$	$\top$
$\top$	$\bot$	$\top$	$\bot$	$\top$	$\top$

(d) Division

Figure 1: Arithmetic Tables

1 Arithmetic Operators

In a separate PDF document generated from Latex, formalize the abstract arithmetic operators on the integer abstract domain (i.e., addition, subtraction, multiplication, and division) and prove that they are all monotone (hint: the easiest way to formalize operators on finite abstract domains is usually to give them as a table).

For a function to be monotone, we must show that the function $f : \mathbb{S} \to \mathbb{S}'$, the following holds $\forall x, y \in S : x \sqsubseteq y \Rightarrow f(x) \sqsubseteq f(y)$ We define our abstraction function as $\alpha^{\#} : \mathbb{Z} \to \mathbb{Z}^{\#} = \{\bot, \mathbb{Z}-, 0, \mathbb{Z}+, \top\}$ where $\top = \mathbb{Z}$. We define $(x, y) \sqsubseteq (x', y')$ for $x, y, x', y' \in \mathbb{Z}^{\#} \iff x \sqsubseteq y$ and $x' \sqsubseteq y'$. For the cases where $x = (\bot, *)$, the result $\bot$ is trivially $\sqsubseteq y, \forall y \in \mathbb{Z}^{\#}$, and similarly with $x = (*, \top)$, which yields $\top$.

For convenience, the table for each operation can be found in Figure **??**.

1.1 Addition

Thus, for $x, y \in \mathbb{Z}$ we can show a proof by cases. Since addition is commutative, without loss of generality, we denote $(x, y) \in (\mathbb{Z}^{\#}, \mathbb{Z}^{\#})$ where $x \sqsubseteq y$. Our addition function is $f^{+} : (\mathbb{Z}^{\#}, \mathbb{Z}^{\#}) \to \mathbb{Z}^{\#}$.

$x = (\mathbb{Z}-, \mathbb{Z}-)$

- $y = (\mathbb{Z}-, \mathbb{Z}-) \Rightarrow \alpha^{\#}(x) \sqsubseteq \alpha^{\#}(y) \Rightarrow \mathbb{Z}- \sqsubseteq \mathbb{Z}-$
- $y = (\mathbb{Z}-, \top) \Rightarrow \alpha^{\#}(x) \sqsubseteq \alpha^{\#}(0) \Rightarrow \mathbb{Z}- \sqsubseteq \top$

- $y = (\top, \top) \Rightarrow \alpha^{\#}(x) \sqsubseteq \alpha^{\#}(y) \Rightarrow \mathbb{Z}- \sqsubseteq \top$

$x = (0, 0)$

- $y = (0, 0) \Rightarrow \alpha^{\#}(x) \sqsubseteq \alpha^{\#}(0) \Rightarrow 0 \sqsubseteq 0$
- $y = (0, \top) \Rightarrow \alpha^{\#}(x) \sqsubseteq \alpha^{\#}(y) \Rightarrow 0 \sqsubseteq \top$
- $y = (\top, \top) \Rightarrow \alpha^{\#}(x) \sqsubseteq \alpha^{\#}(y) \Rightarrow 0 \sqsubseteq \top$

$x = (\mathbb{Z}+, \mathbb{Z}+)$

- $y = (\mathbb{Z}+, \mathbb{Z}+) \Rightarrow \alpha^{\#}(x) \sqsubseteq \alpha^{\#}(0) \Rightarrow \mathbb{Z}+ \sqsubseteq \mathbb{Z}+$
- $y = (\mathbb{Z}+, \top) \Rightarrow \alpha^{\#}(x) \sqsubseteq \alpha^{\#}(y) \Rightarrow \mathbb{Z}+ \sqsubseteq \top$
- $y = (\top, \top) \Rightarrow \alpha^{\#}(x) \sqsubseteq \alpha^{\#}(y) \Rightarrow \mathbb{Z}+ \sqsubseteq \top$

$\square$

1.2 Subtraction

For subtraction, commutativity does not hold, so we will outline the possible cases below. A similar logic holds for $\top$ and $\perp$ as it did it addition. However note that $\forall x = (*, \top), (\top, *) \alpha^{\#}(x) = \top$ and is thus trivially is will satisfy monotonicity for any $x' \sqsubseteq (*, \top)$ or $(\top, *)$. Thus, the only remaining comparisons are where $(x, y) = (x', y')$, which also trivially hold. A proof by cases as done in the addition would also be possible, but unnecessary. $\square$

1.3 Multiplication

A similar argument to our proof in subtraction and addition hold here, i.e., $\perp$ will always satisfy our requirement, and given that multiplication is commutative, we again can assume $(x, y) \Rightarrow x \sqsubseteq y$. $(\mathbb{Z}-, \top), (\mathbb{Z}+, \top)$, and $(\top, \top)$ will also hold under the same logic, however 0 is a special case here. However, the identity trivially holds, i.e.,$x = (0, \top), y = (0, \top) \Rightarrow 0 \sqsubseteq 0$ as does $x = (\top, \top), y = (\top, \top) \Rightarrow \top \sqsubseteq \top$. Thus satisfying the requirement to be monotone. $\square$

1.4 Division

The same logic as before applies again to every case but $(\top, 0)$ and $(0, \top)$. However since the identity will trivially hold, and $\alpha^{\#}((\top, 0)) = \perp \sqsubseteq \alpha^{\#}((\top, \top)) = \top$ and $\alpha^{\#}((0, \top)) = 0 \sqsubseteq \alpha^{\#}((\top, \top)) = \top$, we again have shown that the function is monotone. $\square$