Constant Propagation Analysis

Daniel Loscos Barroso
<dloscos@ucm.es>

January 3, 2020

In this paper we look to provide an abstract interpretation framework to perform constant propagation analysis using variable interval analysis as a base.

Out concrete domain will be **Interval** and our abstract domain will be $\mathbb{Z}_{\perp}^{\top}$.

$\forall i \in \textbf{Interval} \mid\mid \emptyset \sqsubseteq i$
$\forall i = [i_1, i_2], j = [j_1, j_2] \in \textbf{Interval} \mid\mid i \sqsubseteq j \iff j_1 \leq i_1 \;\&\; i_2 \leq j_2$ where $\forall i \in \mathbb{Z} || inf < i < inf$.

1.

First we define: $\alpha : \textbf{Interval} \to \mathbb{Z}_{\perp}^{\top}$, $\gamma : \mathbb{Z}_{\perp}^{\top} \to \textbf{Interval}$ and prove that $(\textbf{Interval}, \alpha, \gamma, \mathbb{Z}_{\perp}^{\top})$ is a Galois connection.

The abstraction function $\alpha : \textbf{Interval} \to \mathbb{Z}_{\perp}^{\top}$ is defined as follows:

$\alpha(\emptyset) = \perp$.
$\alpha([k, k]) = k \quad \forall k \in \mathbb{Z}$.
$\alpha(i) = \top$ otherwise.

The concretization function $\gamma : \mathbb{Z}_{\perp}^{\top} \to \textbf{Interval}$ is defined as:

$\gamma(\perp) = \emptyset$.
$\gamma(k) = [k, k]$.
$\gamma(\top) = [-inf, inf]$

To prove that $(\textbf{Interval}, \alpha, \gamma, \mathbb{Z}_{\perp}^{\top})$ is a Galois connection we need to prove the following properties:

A) α is monotonically increasing:

This means that $\forall i \sqsubseteq j \in \textbf{Interval} \Rightarrow \alpha(i) \sqsubseteq \alpha(j) \in \mathbb{Z}_{\perp}^{\top}$. We distinguish the following cases:

If $i = \emptyset$, then $\emptyset \sqsubseteq j$ and $\alpha(i) = \perp \sqsubseteq \alpha(j) \quad \forall j \in \textbf{Interval}$.

If $i = [k, k]$, with $k \in \mathbb{Z}$ then $i \sqsubseteq j = [j_1, j_2]$ if $j = i$ or $j_1 < k, k \leq j_2$ or $j_1 \leq k, k < j_2$:

- $j = i \Rightarrow \alpha(i) = \alpha(j) \Rightarrow \alpha(i) \sqsubseteq \alpha(j)$.
- $j_1 < k, k \leq j_2 \Rightarrow j \neq \perp, j_1 \neq j_2 \Rightarrow \alpha(i) = k \sqsubseteq \top = \alpha(j)$.
- $j_1 \leq k, k < j_2 \Rightarrow j \neq \perp, j_1 \neq j_2 \Rightarrow \alpha(i) = k \sqsubseteq \top = \alpha(j)$.

If $i = [i_1, i_2]$ with $i_1 < i_2$ then $i \sqsubseteq j = [j_1, j_2]$ if $j = i$ or $j_1 < i_1, i_2 \leq j_2$ or $j_1 \leq i_1, i_2 < j_2$:

- $j = i \Rightarrow \alpha(i) = \alpha(j) \Rightarrow \alpha(i) \sqsubseteq \alpha(j)$.
- $j_1 < i_1, i_2 \leq j_2 \Rightarrow j \neq \bot, j_1 \neq j_2 \Rightarrow \alpha(i) = \top \sqsubseteq \top = \alpha(j)$.
- $j_1 \leq k, k < j_2 \Rightarrow j \neq \bot, j_1 \neq j_2 \Rightarrow \alpha(i) = \top \sqsubseteq \top = \alpha(j)$.

B) γ is monotonically increasing:

This means that $\forall i \sqsubseteq j \in \mathbb{Z}_\bot^\top \Rightarrow \gamma(i) \sqsubseteq \gamma(j) \in$ **Interval**. We distinguish the following cases:

If $i = \bot$ then $i \sqsubseteq j$ and $\gamma(i) \sqsubseteq \gamma(j) \quad \forall j \in \mathbb{Z}_\bot^\top$.

If $i \in \mathbb{Z}_\bot^\top = k \in \mathbb{Z}$ then $i \sqsubseteq j \in \mathbb{Z}_\bot^\top$ if $i = j$ or $j = \top$:

- $j = i \Rightarrow \gamma(i) = \gamma(j) \Rightarrow \gamma(i) = [k, k] \sqsubseteq [k, k] = \gamma(j)$.
- $j = \top \Rightarrow \gamma(j) = [-inf, inf] \Rightarrow \gamma(i) = [k, k] \sqsubseteq [-inf, inf] = \gamma(j)$.

If $i \in \mathbb{Z}_\bot^\top = \top$ then $i \sqsubseteq j \in \mathbb{Z}_\bot^\top \Rightarrow j = \top \Rightarrow \gamma(i) = [-inf, inf] \sqsubseteq [-inf, inf] = \gamma(j)$.

C) $\gamma \circ \alpha \sqsupseteq id$:

We want to prove that $x \sqsubseteq \gamma(\alpha(x)) \quad \forall x \in$ **Interval**.

If $x = \emptyset \Rightarrow \gamma(\alpha(x)) = \gamma(\bot) = \emptyset \sqsupseteq \emptyset$.
If $x = [k, k], k \in \mathbb{Z} \Rightarrow \gamma(\alpha(x)) = \gamma(k) = [k, k] \sqsupseteq [k, k]$.
Otherwise $\gamma(\alpha(x)) = \gamma(\top) = [-inf, inf] \sqsupseteq i \quad \forall i \in$ **Interval** (including x, of course).

D) $\alpha \circ \gamma \sqsubseteq id$:

We want to prove that $\alpha(\gamma(x)) \sqsubseteq x \quad \forall x \in \mathbb{Z}_\bot^\top$.

If $x = \bot \Rightarrow \alpha(\gamma(x)) = \alpha(\emptyset) = \bot \sqsubseteq \bot$.
If $x = k \Rightarrow \alpha(\gamma(x)) = \alpha([k, k]) = k \sqsubseteq k$.
If $x = \top \Rightarrow \alpha(\gamma(x)) = \alpha([-inf, inf]) = \top \sqsubseteq \top$.

Since all the properties are satisfied, we have proven that $(\textbf{Interval}, \alpha, \gamma, \mathbb{Z}_\bot^\top)$ is indeed a Galois connection.

2.

Let $\textbf{State}^\# = \textbf{Var} \to \textbf{Interval}$ and $\textbf{State}^{\#\#} = \textbf{Var} \to \mathbb{Z}_\bot^\top$. then we can extend the previous Galois connection to $\textbf{State}^\#$ and $\textbf{State}^{\#\#}$ with the following functions:

$\alpha' : \textbf{State}^\# \to \textbf{State}^{\#\#}$
$\alpha'(s) = s[v_1 \to \alpha(I_1), ...v_i \to \alpha(I_i)...] \quad \forall v_k \in \textbf{Var}$ defined in $s \in \textbf{State}^\#$ as $v_k \to I_k$.

$\gamma' : \textbf{State}^{\#\#} \to \textbf{State}^\#$
$\gamma'(s) = s[v_1 \to \gamma(Z_1), ...v_i \to \gamma(Z_i)...] \quad \forall v_k \in \textbf{Var}$ defined in $s \in \textbf{State}^{\#\#}$ as $v_k \to Z_k$.

3.

We can define an abstract interpreter $[\![e]\!]^{\#\#} : \textbf{State}^{\#\#} \to \mathbb{Z}_\perp^\top$ that determines whether the result of an arithmetic expression must be constant at runtime: if $[\![e]\!]^{\#\#} = k \in \mathbb{Z}$ then, we can conclude that the expression is constant. If $[\![e]\!]^{\#\#} = \perp$ or $\top$, then we cannot conclude that the expression is constant.

Since our variable interval analysis used additional operations, we will include those as well in our abstract interpreter:

$[\![n]\!]^{\#\#} = \lambda\sigma.n.$
$[\![var]\!]^{\#\#} = \lambda\sigma.\sigma(var)$
$[\![-e]\!]^{\#\#} = \lambda\sigma.(\ominus_1([\![e]\!]^{\#\#}\sigma))$
$[\![e_1 + e_2]\!]^{\#\#} = \lambda\sigma.(([\![e_1]\!]^{\#\#}\sigma) \oplus ([\![e_2]\!]^{\#\#}\sigma))$
$[\![e_1 - e_2]\!]^{\#\#} = \lambda\sigma.(([\![e_1]\!]^{\#\#}\sigma) \ominus ([\![e_2]\!]^{\#\#}\sigma))$
$[\![e_1 * e_2]\!]^{\#\#} = \lambda\sigma.(([\![e_1]\!]^{\#\#}\sigma) \otimes ([\![e_2]\!]^{\#\#}\sigma))$
$[\![e_1 / e_2]\!]^{\#\#} = \lambda\sigma.(([\![e_1]\!]^{\#\#}\sigma) \oslash ([\![e_2]\!]^{\#\#}\sigma))$

Were the functions $\ominus_1, \oplus, \ominus, \otimes$ and $\oslash$ are defined as follows:

$\ominus_1 \perp = \perp$
$\ominus_1 \top = \top$
$\ominus_1 x = -x \quad \forall x \in \mathbb{Z}$

$\oplus$ and $\otimes$ are commutative
$\perp \oplus x = \perp \quad \forall x \in \mathbb{Z}_\perp^\top$
$\top \oplus x = \top \quad \forall x \in \mathbb{Z}^\top$
$x \oplus y = (x + y) \quad \forall x, y \in \mathbb{Z}$

$\perp \ominus x = \perp \quad \forall x \in \mathbb{Z}_\perp^\top$
$x \ominus \perp = \perp \quad \forall x \in \mathbb{Z}_\perp^\top$
$\top \ominus x = \top \quad \forall x \in \mathbb{Z}^\top$
$x \ominus \top = \top \quad \forall x \in \mathbb{Z}^\top$
$x \ominus y = (x - y) \quad \forall x, y \in \mathbb{Z}$

$\perp \otimes x = \perp \quad \forall x \in \mathbb{Z}_\perp^\top$
$0 \otimes x = 0 \quad \forall x \in \mathbb{Z}^\top$
$\top \otimes x = \top \quad \forall x \in \mathbb{Z}^\top \backslash \{0\}$
$x \otimes y = (x * y) \quad \forall x, y \in \mathbb{Z}$

$\perp \oslash x = \perp \quad \forall x \in \mathbb{Z}_\perp^\top$
$x \oslash \perp = \perp \quad \forall x \in \mathbb{Z}_\perp^\top$
$0 \oslash x = 0 \quad \forall x \in \mathbb{Z}^\top$
$x \oslash 0 = \top \quad \forall x \in \mathbb{Z}_\perp^\top \backslash \{0\}$
$\top \oslash x = \top \quad \forall x \in \mathbb{Z}^\top \backslash \{0\}$
$x \oslash \top = \top \quad \forall x \in \mathbb{Z}^\top \backslash \{0\}$
$x \oslash y = (x/y) \quad \forall x, y \in \mathbb{Z} \backslash \{0\}$
$0 \oslash 0$ is not defined

4.

Finally, we show that the interpreter is correct by proving that $\alpha([\![e]\!]^{\#}(\gamma'(s))) \sqsubseteq [\![e]\!]^{\#\#}(s) \quad \forall s \in \textbf{State}^{\#\#}$.

Constants

If $e = n \Rightarrow [\![n]\!]^{\#\#} = \lambda\sigma.n$ and $[\![n]\!]^{\#} = \lambda\sigma.[n,n] \Rightarrow \alpha([\![n]\!]^{\#}(\gamma'(s))) = \alpha([n,n]) = n = [\![n]\!]^{\#\#}(s)$ independently of $s \in \mathbf{State}^{\#\#}$.

Variables

If $e = var \Rightarrow [\![var]\!]^{\#\#} = \lambda\sigma.\sigma(var)$ and $[\![var]\!]^{\#} = \lambda\sigma.\sigma(var)$. Now we distinguish three possible cases regarding $s \in \mathbf{State}^{\#\#}$:

- $s(var) = \bot$**:** $\Rightarrow \alpha([\![var]\!]^{\#}(\gamma'(s))) = \alpha(\emptyset) = \bot = [\![var]\!]^{\#\#}(s)$.
- $s(var) = z \in \mathbb{Z}$**:** $\Rightarrow \alpha([\![var]\!]^{\#}(\gamma'(s))) = \alpha([z,z]) = z = [\![var]\!]^{\#\#}(s)$.
- $s(var) = \top$**:** $\Rightarrow \alpha([\![var]\!]^{\#}(\gamma'(s))) = \alpha([-inf, inf]) = \top = [\![var]\!]^{\#\#}(s)$.

Induction Hypothesis

These are the base cases for the proof by structural induction on the rest of expressions. Our induction hypothesis will be that $\alpha([\![e]\!]^{\#}(\gamma'(s))) \sqsubseteq [\![e]\!]^{\#\#}(s) \quad \forall s \in \mathbf{State}^{\#\#}$. which has the following implications:

- $[\![e]\!]^{\#\#}(s) = \bot \Rightarrow \alpha([\![e]\!]^{\#}(\gamma'(s))) = \bot \Rightarrow [\![e]\!]^{\#}(\gamma'(s)) = \emptyset$.
- $[\![e]\!]^{\#\#}(s) = z \in \mathbb{Z} \Rightarrow \alpha([\![e]\!]^{\#}(\gamma'(s))) = \bot$ or $z \Rightarrow [\![e]\!]^{\#}(\gamma'(s)) = \emptyset$ or $[z,z]$.
- $[\![e]\!]^{\#\#}(s) = \top \Rightarrow \alpha([\![e]\!]^{\#}(\gamma'(s))) =$ anything $\in \mathbb{Z}_{\bot}^{\top} \Rightarrow [\![e]\!]^{\#}(\gamma'(s)) =$ anything $\in$ **Interval**.

Negation

If $e = -e_1 \Rightarrow [\![-e_1]\!]^{\#\#} = \lambda\sigma.(\ominus_1([\![e_1]\!]^{\#\#}\sigma))$ and $[\![-e_1]\!]^{\#} = \lambda\sigma.(-_1([\![e_2]\!]^{\#\#}\sigma))$ where:

- $-_1\emptyset = \emptyset$
- $-_1[i_1, i_2] = [-i_2, -i_1]$ (of course we have that $-(-inf) = inf$)

We now distinguish cases regarding the values of $[\![e_1]\!]^{\#\#}(s)$:

If $[\![e_1]\!]^{\#\#}(s) = \bot$ then $[\![e]\!]^{\#\#}(s) = \bot$ and by the IH $[\![e_1]\!]^{\#}(\gamma'(s)) = \emptyset \Rightarrow \alpha([\![e]\!]^{\#}(\gamma'(s))) = \alpha(\emptyset) = \bot = [\![e]\!]^{\#\#}(s)$.

If $[\![e_1]\!]^{\#\#}(s) = \top$, then $[\![e]\!]^{\#\#}(s) = \top$ which is the topmost element of the lattice, so the property holds.

Finally if $[\![e_1]\!]^{\#\#}(s) = a \in \mathbb{Z}$ then $[\![e]\!]^{\#\#}(s) = -a$ and by the IH $[\![e_1]\!]^{\#}(\gamma'(s)) = \emptyset$ or $[a,a]$. Therefore $[\![e]\!]^{\#}(\gamma'(s)) = \emptyset$ or $[-a,-a] \Rightarrow \alpha([\![e]\!]^{\#}(\gamma'(s))) = \bot$ or $-a$ both of which are $\sqsubseteq -a$.

Addition

If $e = e_1+e_2 \Rightarrow [\![e_1+e_2]\!]^{\#\#} = \lambda\sigma.(([\![e_1]\!]^{\#\#}\sigma)\oplus([\![e_2]\!]^{\#\#}\sigma))$ and $[\![e_1+e_2]\!]^{\#} = \lambda\sigma.(([\![e_1]\!]^{\#\#}\sigma)+_2([\![e_2]\!]^{\#\#}\sigma))$ where:

- $+_2$, $+_-$ and $+_+$ are commutative
- $\emptyset +_2 i = \emptyset \quad \forall i \in$ **Interval**
- $[i_1, i_2] +_2 [j_1, j_2] = [i_1 +_- j_1, i_2 +_+ j_2]$

- $-inf +_- k = -inf \quad \forall k \in \mathbb{Z}^{inf}_{-inf}$
- $inf +_- k = inf \quad \forall k \in \mathbb{Z}^{inf}$
- $a +_- b = a + b \quad \forall a, b \in \mathbb{Z}$
- $inf +_+ k = inf \quad \forall k \in \mathbb{Z}^{inf}_{-inf}$
- $-inf +_+ k = -inf \quad \forall k \in \mathbb{Z}_{-inf}$
- $a +_+ b = a + b \quad \forall a, b \in \mathbb{Z}$

We now distinguish cases regarding the values of $[\![e_1]\!]^{\#\#}(s)$ and $[\![e_2]\!]^{\#\#}(s)$:

If $[\![e_1]\!]^{\#\#}(s)$ or $[\![e_2]\!]^{\#\#}(s) = \bot$ then $[\![e]\!]^{\#\#}(s) = \bot$ and by the IH $[\![e_1]\!]^{\#}(\gamma'(s))$ or $[\![e_2]\!]^{\#}(\gamma'(s)) = \emptyset \Rightarrow \alpha([\![e]\!]^{\#}(\gamma'(s))) = \alpha(\emptyset) = \bot = [\![e]\!]^{\#\#}(s)$.

If $[\![e_1]\!]^{\#\#}(s) \neq \bot$, $[\![e_2]\!]^{\#\#}(s) \neq \bot$ and one of them is equal to $\top$, then $[\![e]\!]^{\#\#}(s) = \top$ which is the topmost element of the lattice, so the property holds.

Finally if $[\![e_1]\!]^{\#\#}(s) = a$, $[\![e_2]\!]^{\#\#}(s) = b$, $a, b \in \mathbb{Z}$ then $[\![e]\!]^{\#\#}(s) = a + b$ and by the IH $[\![e_1]\!]^{\#}(\gamma'(s)) = \emptyset$ or $[a, a]$ and $[\![e_2]\!]^{\#}(\gamma'(s)) = \emptyset$ or $[b, b]$. Therefore $[\![e]\!]^{\#}(\gamma'(s)) = \emptyset$ or $[a + b, a + b] \Rightarrow \alpha([\![e]\!]^{\#}(\gamma'(s))) = \bot$ or $a + b$ both of which are $\sqsubseteq a + b$.

Subtraction

If $e = e_1 - e_2 \Rightarrow [\![e_1 - e_2]\!]^{\#\#} = \lambda\sigma.(([\![e_1]\!]^{\#\#}\sigma) \ominus ([\![e_2]\!]^{\#\#}\sigma))$ and $[\![e_1 - e_2]\!]^{\#} = \lambda\sigma.(([\![e_1]\!]^{\#\#}\sigma) -_2 ([\![e_2]\!]^{\#\#}\sigma))$ where:

- $\emptyset -_2 i = i -_2 \emptyset = \emptyset \quad \forall i \in$ **Interval**
- $[i_1, i_2] -_2 [j_1, j_2] = [i_1 -_- j_2, i_2 -_+ j_1]$
- $-inf -_- k = -inf \quad \forall k \in \mathbb{Z}^{inf}_{-inf}$
- $k -_- inf = -inf \quad \forall k \in \mathbb{Z}^{inf}$
- $inf -_- z = inf \quad \forall z \in \mathbb{Z}$
- $z -_- -inf = inf \quad \forall z \in \mathbb{Z}$
- $a -_- b = a - b \quad \forall a, b \in \mathbb{Z}$
- $inf -_+ k = inf \quad \forall k \in \mathbb{Z}^{inf}_{-inf}$
- $k -_+ -inf = inf \quad \forall k \in \mathbb{Z}^{inf}$
- $-inf -_+ z = -inf \quad \forall z \in \mathbb{Z}$
- $z -_+ inf = -inf \quad \forall z \in \mathbb{Z}$
- $a -_+ b = a - b \quad \forall a, b \in \mathbb{Z}$

We now distinguish cases regarding the values of $[\![e_1]\!]^{\#\#}(s)$ and $[\![e_2]\!]^{\#\#}(s)$:

If $[\![e_1]\!]^{\#\#}(s)$ or $[\![e_2]\!]^{\#\#}(s) = \bot$ then $[\![e]\!]^{\#\#}(s) = \bot$ and by the IH $[\![e_1]\!]^{\#}(\gamma'(s))$ or $[\![e_2]\!]^{\#}(\gamma'(s)) = \emptyset \Rightarrow \alpha([\![e]\!]^{\#}(\gamma'(s))) = \alpha(\emptyset) = \bot = [\![e]\!]^{\#\#}(s)$.

If $[\![e_1]\!]^{\#\#}(s) \neq \bot$, $[\![e_2]\!]^{\#\#}(s) \neq \bot$ and one of them is equal to $\top$, then $[\![e]\!]^{\#\#}(s) = \top$ which is the topmost element of the lattice, so the property holds.

Finally if $[\![e_1]\!]^{\#\#}(s) = a$, $[\![e_2]\!]^{\#\#}(s) = b$, $a, b \in \mathbb{Z}$ then $[\![e]\!]^{\#\#}(s) = a - b$ and by the IH $[\![e_1]\!]^{\#}(\gamma'(s)) = \emptyset$ or $[a, a]$ and $[\![e_2]\!]^{\#}(\gamma'(s)) = \emptyset$ or $[b, b]$. Therefore $[\![e]\!]^{\#}(\gamma'(s)) = \emptyset$ or $[a - b, a - b] \Rightarrow \alpha([\![e]\!]^{\#}(\gamma'(s))) = \bot$ or $a - b$ both of which are $\sqsubseteq a - b$.

Multiplication

If $e = e_1 * e_2 \Rightarrow [\![e_1 * e_2]\!]^{\#\#} = \lambda\sigma.(([\![e_1]\!]^{\#\#}\sigma) \otimes ([\![e_2]\!]^{\#\#}\sigma))$ and $[\![e_1 * e_2]\!]^{\#} = \lambda\sigma.(([\![e_1]\!]^{\#\#}\sigma) *_2 ([\![e_2]\!]^{\#\#}\sigma))$ where:

- $*_2$ is commutative
- $\emptyset *_2 i = \emptyset \quad \forall i \in$ **Interval**
- $[i_1, i_2] *_2 [j_1, j_2] = [min(M), max(M)]$ where $M = \{i_1 * j_1, i_1 * j_2, i_2 * j_1, i_2 * j_2\}$
- $inf * inf = inf$
- $-inf * inf = -inf$
- $-inf * -inf = inf$
- $0 * k = 0 \quad \forall k \in \mathbb{Z}^{inf}_{-inf}$
- $inf * k = inf \quad \forall k \in \mathbb{Z}, k > 0$
- $inf * k = -inf \quad \forall k \in \mathbb{Z}, k < 0$
- $-inf * k = -inf \quad \forall k \in \mathbb{Z}, k > 0$
- $-inf * k = inf \quad \forall k \in \mathbb{Z}, k < 0$
- $a * b = a * b \quad \forall a, b \in \mathbb{Z}$ (as expected).

We now distinguish cases regarding the values of $[\![e_1]\!]^{\#\#}(s)$ and $[\![e_2]\!]^{\#\#}(s)$:

If $[\![e_1]\!]^{\#\#}(s)$ or $[\![e_2]\!]^{\#\#}(s) = \bot$ then $[\![e]\!]^{\#\#}(s) = \bot$ and by the IH $[\![e_1]\!]^{\#}(\gamma'(s))$ or $[\![e_2]\!]^{\#}(\gamma'(s)) = \emptyset \Rightarrow \alpha([\![e]\!]^{\#}(\gamma'(s))) = \alpha(\emptyset) = \bot = [\![e]\!]^{\#\#}(s)$.

If $[\![e_1]\!]^{\#\#}(s) \neq \bot$, $[\![e_2]\!]^{\#\#}(s) \neq \bot$ and one of them is equal to 0, then $[\![e]\!]^{\#\#}(s) = 0$ and by the IH either $[\![e_1]\!]^{\#}(\gamma'(s)) = \emptyset$ or $[0, 0]$ or $[\![e_2]\!]^{\#}(\gamma'(s)) = \emptyset$ or $[0, 0]$. Therefore $[\![e]\!]^{\#}(\gamma'(s)) = \emptyset$ or $[0, 0] \Rightarrow \alpha([\![e]\!]^{\#}(\gamma'(s))) = \bot$ or 0 both of which are $\sqsubseteq 0$.

If $[\![e_1]\!]^{\#\#}(s) \neq \bot$ or 0, $[\![e_2]\!]^{\#\#}(s) \neq \bot$ or 0 and one of them is equal to $\top$, then $[\![e]\!]^{\#\#}(s) = \top$ which is the topmost element of the lattice, so the property holds.

Finally if $[\![e_1]\!]^{\#\#}(s) = a$, $[\![e_2]\!]^{\#\#}(s) = b$, $a, b \in \mathbb{Z}\backslash\{0\}$ then $[\![e]\!]^{\#\#}(s) = a*b$ and by the IH $[\![e_1]\!]^{\#}(\gamma'(s)) = \emptyset$ or $[a, a]$ and $[\![e_2]\!]^{\#}(\gamma'(s)) = \emptyset$ or $[b, b]$. Therefore $[\![e]\!]^{\#}(\gamma'(s)) = \emptyset$ or $[a * b, a * b] \Rightarrow \alpha([\![e]\!]^{\#}(\gamma'(s))) = \bot$ or $a * b$ both of which are $\sqsubseteq a * b$.

Division

If $e = e_1/e_2 \Rightarrow [\![e_1/e_2]\!]^{\#\#} = \lambda\sigma.(([\![e_1]\!]^{\#\#}\sigma) \oslash ([\![e_2]\!]^{\#\#}\sigma))$ and $[\![e_1/e_2]\!]^{\#} = \lambda\sigma.(([\![e_1]\!]^{\#\#}\sigma)/_2([\![e_2]\!]^{\#\#}\sigma))$ where:

- $\emptyset/_2 i = \emptyset \quad \forall i \in$ **Interval**
- $i/_2\emptyset = \emptyset \quad \forall i \in$ **Interval**
- If $j_1 * j_2 \leq 0 \Rightarrow [i_1, i_2]/_2[j_1, j_2] = [-inf, inf]$
- If $j_1 * j_2 > 0 \Rightarrow [i_1, i_2]/_2[j_1, j_2] = [min(M), max(M)]$ where $M = \{i_1/j_1, i_1/j_2, i_2/j_1, i_2/j_2\}$
- $inf/inf = inf$
- $inf/ - inf = -inf$
- $-inf/inf = -inf$

- $-inf/-inf = inf$
- $0/k = 0 \quad \forall k \in \mathbb{Z}_{-inf}^{inf} \backslash \{0\}$
- $inf/k = inf \quad \forall k \in \mathbb{Z}, k \geq 0$
- $inf/k = -inf \quad \forall k \in \mathbb{Z}, k < 0$
- $-inf/k = -inf \quad \forall k \in \mathbb{Z}, k \geq 0$
- $-inf/k = inf \quad \forall k \in \mathbb{Z}, k < 0$
- $z/0 = -inf \quad \forall z \in \mathbb{Z}_{-inf}, z < 0$
- $z/0 = inf \quad \forall k \in \mathbb{Z}^{inf}, z > 0$
- $a/b = a */b \quad \forall a, b \in \mathbb{Z} \backslash \{0\}$ (as expected).
- The function / is not defined for 0/0, however we define it for infinity values in the way that is most conservative for the analysis

We now distinguish cases regarding the values of $[\![e_1]\!]^{\#\#}(s)$ and $[\![e_2]\!]^{\#\#}(s)$:

If $[\![e_1]\!]^{\#\#}(s)$ or $[\![e_2]\!]^{\#\#}(s) = \bot$ then $[\![e]\!]^{\#\#}(s) = \bot$ and by the IH $[\![e_1]\!]^{\#}(\gamma'(s))$ or $[\![e_2]\!]^{\#}(\gamma'(s)) = \emptyset \Rightarrow \alpha([\![e]\!]^{\#}(\gamma'(s))) = \alpha(\emptyset) = \bot = [\![e]\!]^{\#\#}(s)$.

If $[\![e_1]\!]^{\#\#}(s) = [\![e_2]\!]^{\#\#}(s) = 0$, then $[\![e]\!]^{\#\#}(s)$ is not defined.

If $[\![e_1]\!]^{\#\#}(s) \neq \bot$ or 0, $[\![e_2]\!]^{\#\#}(s) = 0$, then $[\![e]\!]^{\#\#}(s) = \top$ which is the topmost element of the lattice, so the property holds.

If $[\![e_1]\!]^{\#\#}(s) = 0$, $[\![e_2]\!]^{\#\#}(s) \neq \bot$ or 0 then $[\![e]\!]^{\#\#}(s) = 0$ and by the IH either $[\![e_1]\!]^{\#}(\gamma'(s)) = \emptyset$ or $[0, 0]$. Therefore $[\![e]\!]^{\#}(\gamma'(s)) = \emptyset$ or $[0, 0] \Rightarrow \alpha([\![e]\!]^{\#}(\gamma'(s))) = \bot$ or 0 both of which are $\sqsubseteq 0$.

If $[\![e_1]\!]^{\#\#}(s) \neq \bot$ or 0, $[\![e_2]\!]^{\#\#}(s) \neq \bot$ or 0 and one of them is equal to $\top$, then $[\![e]\!]^{\#\#}(s) = \top$ which is the topmost element of the lattice, so the property holds.

Finally if $[\![e_1]\!]^{\#\#}(s) = a$, $[\![e_2]\!]^{\#\#}(s) = b$, $a, b \in \mathbb{Z} \backslash \{0\}$ then $[\![e]\!]^{\#\#}(s) = a/b$ and by the IH $[\![e_1]\!]^{\#}(\gamma'(s)) = \emptyset$ or $[a, a]$ and $[\![e_2]\!]^{\#}(\gamma'(s)) = \emptyset$ or $[b, b]$. Therefore $[\![e]\!]^{\#}(\gamma'(s)) = \emptyset$ or $[a/b, a/b] \Rightarrow \alpha([\![e]\!]^{\#}(\gamma'(s))) = \bot$ or a/b both of which are $\sqsubseteq a/b$.

Conclusion

With this last case we have proven that the interpreter is correct by proving that every numerical expression satisfies$\alpha([\![e]\!]^{\#}(\gamma'(s))) \sqsubseteq [\![e]\!]^{\#\#}(s) \quad \forall s \in \mathbf{State}^{\#\#}$.