Software Verification

Borsetto Riccardo
5th December 2022

Università
degli Studi
di Padova

Table of Contents

Language

$$
\begin{aligned}
&\textbf{Abinop} \ni \text{aop} ::= + \mid - \mid * \mid \backslash \\
&\textbf{Aexp} \ni e ::= x \mid n \mid -e \mid e_1 \ \text{aop} \ e_2 \\
&\textbf{Bbinop} \ni \text{bop} ::= = \mid \neq \mid < \mid \leq \mid > \mid \geq \\
&\textbf{Bexp} \ni b ::= \mathit{true} \mid \mathit{false} \mid e_1 \ \text{bop} \ e_2 \mid b_1 \wedge b_2 \mid b_1 \vee b_2 \mid \neg b \\
&\textbf{While} \ni S ::= x := e \mid \textbf{skip} \mid S_1 ; S_2 \mid \textbf{if} \ b \ \textbf{then} \ S_1 \ \textbf{else} \ S_2 \\
&\qquad\qquad\quad \mid \textbf{while} \ b \ \textbf{do} \ S
\end{aligned}
$$

Table of Contents

Abstract Interpreter

Università degli Studi di Padova

$$
\begin{aligned}
&\mathit{AI} : \textbf{While} \to \mathit{bool} \to \mathbb{S} \to \mathbb{S} \times \mathit{List}(\mathbb{S}) \\
&\quad \mathit{AI}(x := e)(w)(s^\sharp) := (s^\sharp[x \mapsto \mathcal{A}^\sharp(e)(s^\sharp)], []) \\
&\quad \mathit{AI}(\textbf{skip})(w)(s^\sharp) := (s^\sharp, []) \\
&\quad \mathit{AI}(S_1; S_2)(w)(s^\sharp) := (u^\sharp, \mathit{invs}_1 +_{\mathit{List}(\mathbb{S})} \mathit{invs}_2) \\
&\qquad\qquad \text{with } (u^\sharp, \mathit{invs}_2) := \mathit{AI}(S_2)(w)(t^\sharp) \\
&\qquad\qquad\qquad (t^\sharp, \mathit{invs}_1) := \mathit{AI}(S_1)(w)(s^\sharp) \\
&\quad \mathit{AI}(\textbf{if } b \textbf{ then } S_1 \textbf{ else } S_2)(w)(s^\sharp) := (t^\sharp \vee_{\mathbb{S}} u^\sharp, \mathit{invs}_1 +_{\mathit{List}(\mathbb{S})} \mathit{invs}_2) \\
&\qquad\qquad \text{with } (t^\sharp, \mathit{invs}_1) := (\mathit{AI}(S_1)(w) \circ \mathcal{B}^\sharp(b))(s^\sharp) \\
&\qquad\qquad\qquad (u^\sharp, \mathit{invs}_2) := (\mathit{AI}(S_2)(w) \circ \mathcal{B}^\sharp(\neg b))(s^\sharp) \\
&\quad \mathit{AI}(\textbf{while } b \textbf{ do } S)(w)(s^\sharp) := (\mathcal{B}^\sharp(\neg b)(t^\sharp), \mathit{invs}) \\
&\qquad\qquad \text{with } (t^\sharp, \mathit{invs}) := \text{ab-lfp}(\mathit{AI}(S)(w))(b)(t^\sharp)(\ldots)
\end{aligned}
$$

$$
\begin{aligned}
&\mathcal{A}^\sharp : \textbf{Aexp} \to \mathbb{S} \to A\\
&\quad \mathcal{A}^\sharp(n)(s^\sharp) := \alpha_{singleton}(n)\\
&\quad \mathcal{A}^\sharp(x)(s^\sharp) := \mathsf{lookup}_{\mathbb{S}}(s^\sharp)(x)\\
&\quad \mathcal{A}^\sharp(e_1 \text{ aop } e_2)(s^\sharp) := \mathcal{A}^\sharp(e_1)(s^\sharp) \text{ aop}^A \mathcal{A}^\sharp(e_2)(s^\sharp)\\
&\quad \mathcal{A}^\sharp(-e)(s^\sharp) := -^A \mathcal{A}^\sharp(e)(s^\sharp)
\end{aligned}
$$

Abstract Semantics of boolean expressions

$$\mathcal{B}^\sharp : \textbf{Bexp} \to \mathbb{S} \to \mathbb{S}$$

$$\mathcal{B}^\sharp(\mathit{true})(s^\sharp) := s^\sharp$$

$$\mathcal{B}^\sharp(\mathit{false})(s^\sharp) := \bot_{\mathbb{S}}$$

$$\mathcal{B}^\sharp(e_1 \text{ bop } e_2)(s^\sharp) := \mathit{FINIRE}$$

$$\mathcal{B}^\sharp(b_1 \wedge b_2)(s^\sharp) := (\mathcal{B}^\sharp(b_2) \circ \mathcal{B}^\sharp(b_1))(s^\sharp)$$

$$\mathcal{B}^\sharp(b_1 \vee b_2)(s^\sharp) := \mathcal{B}^\sharp(b_1)(s^\sharp) \vee_{\mathbb{S}} \mathcal{B}^\sharp(b_2)(s^\sharp)$$

Step

$$
\begin{aligned}
\text{step} &: (\mathbb{S} \to \mathbb{S} \times \mathit{List}(\mathbb{S})) \to \mathit{bool} \to \mathbb{S} \to \mathbb{S} \to \mathbb{S} \times \mathit{List}(\mathbb{S}) \\
\text{step}(f)(b)(s^\sharp)(t^\sharp) &:= (s^\sharp \vee_{\mathbb{S}} u^\sharp, \mathit{invs}) \\
&\quad \text{with } (u^\sharp, \mathit{invs}) := f(\mathcal{B}^\sharp(b)(t^\sharp))
\end{aligned}
$$

Invariant Check

$$\text{is-inv} : (\mathbb{S} \to \mathbb{S} \times \mathit{List}(\mathbb{S})) \to \mathbb{S} \to \mathbb{S} \to \mathit{bool}$$

$$\text{is-inv}(f)(s^\sharp)(t^\sharp) := t^\sharp \sqsubseteq_{\mathbb{S}} u^\sharp$$

$$\text{with } u^\sharp := \pi_1(\mathit{step}(f)(b)(s^\sharp)(t^\sharp))$$

Steps

$$\text{steps} : (\mathbb{S} \to \mathbb{S} \times \mathit{List}(\mathbb{S})) \to \mathit{bool} \to \mathbb{S} \to \mathbb{S} \to \mathbb{S} \times \mathit{List}(\mathbb{S})$$

$$\text{steps}(f)(b)(s^\sharp)(t^\sharp) := \begin{cases} (t^\sharp, [t^\sharp]) & \text{if is-inv}(f)(s^\sharp)(t^\sharp) \\ (v^\sharp, \mathit{invs}_1 +_{\mathit{List}(\mathbb{S})} \mathit{invs}_2) & \text{otherwise} \end{cases}$$

$$\begin{aligned} \text{with } (u^\sharp, \mathit{invs}_1) &:= \text{step}(f)(b)(s^\sharp)(t^\sharp) \\ (v^\sharp, \mathit{invs}_2) &:= \text{steps}(f)(b)(s^\sharp)(u^\sharp) \end{aligned}$$

Widening

UNIVERSITÀ DEGLI STUDI DI PADOVA

$$\text{wid} : (\mathbb{S} \to \mathbb{S} \times \mathit{List}(\mathbb{S})) \to \mathit{bool} \to \mathbb{S} \to \mathbb{S} \to \mathbb{S}$$

$$\text{wid}(f)(b)(s^\sharp)(t^\sharp) := \begin{cases} t^\sharp & \text{if is-inv}(f)(s^\sharp)(t^\sharp) \\ \text{wid}(f)(b)(s^\sharp)(t^\sharp \ \nabla_{\mathbb{S}} \ u^\sharp) & \text{otherwise} \end{cases}$$

$$\text{with } u^\sharp := \pi_1(\mathit{step}(f)(b)(s^\sharp)(t^\sharp))$$

Narrowing

$$\mathrm{nar} : (\mathbb{S} \to \mathbb{S} \times List(\mathbb{S})) \to bool \to \mathbb{S} \to \mathbb{S} \to \mathbb{S} \times List(\mathbb{S})$$

$$\mathrm{nar}(f)(b)(s^\sharp)(t^\sharp) := \begin{cases} (v^\sharp, [v^\sharp]) & \text{if is-inv}(f)(s^\sharp)(v^\sharp) \\ (z^\sharp, invs_1 +_{List(\mathbb{S})} invs_2) & \text{otherwise} \end{cases}$$

$$\begin{aligned} \text{with } u^\sharp &:= \pi_1(\mathrm{step}(f)(b)(s^\sharp)(t^\sharp)) \\ v^\sharp &:= t^\sharp \ \Delta_{\mathbb{S}} \ u^\sharp \\ (w^\sharp, invs_1) &:= \mathrm{step}(f)(b)(s^\sharp)(v^\sharp) \\ (z^\sharp, invs_2) &:= \mathrm{nar}(f)(b)(s^\sharp)(v^\sharp \Delta_{\mathbb{S}} w^\sharp) \end{aligned}$$

Abstract Least Fixed Point

$$\text{ab-lfp} : (\mathbb{S} \to \mathbb{S} \times \mathit{List}(\mathbb{S})) \to \mathit{bool} \to \mathbb{S} \to \mathit{bool} \to \mathbb{S} \times \mathit{List}(\mathbb{S})$$

$$\text{ab-lfp}(f)(b)(s^\sharp)(w) := \begin{cases} \text{nar}(f)(b)(s^\sharp)(t^\sharp) & \text{if } w \\ \text{steps}(f)(b)(s^\sharp)(s^\sharp) & \text{otherwise} \end{cases}$$

$$\text{with } t^\sharp := \text{wid}(f)(b)(s^\sharp)(s^\sharp).$$

Table of Contents

$s^\sharp[x \mapsto a]$ defined using recursion

$$\begin{cases} \bot_{\mathbb{S}}[x \mapsto a] := [(x, a)] \\ \top_{\mathbb{S}}[x \mapsto a] := [(x, a)] \\ ((y, a') :: ts^\sharp)[x \mapsto a] := \begin{cases} (y, a) :: ts^\sharp & \text{if } x = y \\ (y, a') :: ts^\sharp[x \mapsto a] & \text{otherwise} \end{cases} \end{cases}$$

Abstract State Join

$s^\sharp \vee_{\mathbb{S}} t^\sharp$ defined using recursion

$$\begin{cases} \bot_{\mathbb{S}} \vee_{\mathbb{S}} t^\sharp := t^\sharp \\ \top_{\mathbb{S}} \vee_{\mathbb{S}} t^\sharp := \top_{\mathbb{S}} \\ ((x, a) :: ts^\sharp) \vee_{\mathbb{S}} t^\sharp := (ts^\sharp \vee_{\mathbb{S}} t^\sharp)[x \mapsto a \vee_A \mathrm{lookup}(t^\sharp)(x)] \end{cases}$$

Abstract State Lookup

$\text{lookup}_{\mathbb{S}}(s^\sharp)(x)$ defined using recursion

$$
\begin{cases}
\text{lookup}_{\mathbb{S}}(\bot_{\mathbb{S}})(x) := \bot_A \\
\text{lookup}_{\mathbb{S}}(\top_{\mathbb{S}})(x) := \top_A \\
\text{lookup}_{\mathbb{S}}((y, a) :: ts^\sharp)(x) := \begin{cases} a & \text{if } x = y \\ \text{lookup}_{\mathbb{S}}(ts^\sharp)(x) & \text{otherwise} \end{cases}
\end{cases}
$$

Partial order

$$
\begin{aligned}
a_1 \leq_A a_2 &:= \; a_1 \vee_A a_2 = a_2 \\
s^\sharp \sqsubseteq_{\mathbb{S}} t^\sharp &:= \; (s^\sharp = \bot_{\mathbb{S}}) \vee \forall x, \mathsf{lookup}(s^\sharp)(x) \leq_A \mathsf{lookup}(t^\sharp)(x)
\end{aligned}
$$

State Widening

Università degli Studi di Padova

$$s^\sharp \ \nabla_{\mathbb{S}} \ t^\sharp := \begin{cases} t^\sharp & \text{if } s^\sharp = \bot_{\mathbb{S}} \\ map(f_{t^\sharp})(s^\sharp) & \text{otherwise} \end{cases}$$

$$\text{with } f_{t^\sharp}(x, a) := (x, a \ \nabla \ \text{lookup}(t^\sharp)(x))$$

State Narrowing

$$s^\sharp \; \Delta_{\mathbb{S}} \; t^\sharp := \begin{cases} \bot_{\mathbb{S}} & \text{if } s^\sharp = \bot_{\mathbb{S}} \\ map(f_{t^\sharp})(s^\sharp) & \text{otherwise} \end{cases}$$

$$\text{with } f_{t^\sharp}(x, a) := (x, a \; \Delta \; \text{lookup}(t^\sharp)(x))$$

Table of Contents

Extended Sign

$$A := \mathit{ExtSign}$$
$$\mathbb{S} := \mathit{List}(\mathit{String} \times \mathit{ExtSign}) \cup \{\star\}$$
$$\bot_{\mathbb{S}} := \star$$
$$\top_{\mathbb{S}} := []$$
$$\mathit{ExtSign} \ni a ::= \bot \mid < 0 \mid = 0 \mid > 0 \mid \leq 0 \mid \neq 0 \mid \geq 0 \mid \top$$

α on Singletons

$$\alpha_{singleton}(n) := \begin{cases} = 0 & \text{if } n = 0 \\ < 0 & \text{if } n < 0 \\ > 0 & \text{otherwise} \end{cases}$$

Opposite

$-$	$\perp$	< 0	$= 0$	> 0	≤ 0	$\neq 0$	≥ 0	$\top$
	$\perp$	> 0	$= 0$	< 0	≥ 0	$\neq 0$	≤ 0	$\top$

Addition

$+$	$\perp$	< 0	$= 0$	> 0	≤ 0	$\neq 0$	≥ 0	$\top$
$\perp$	$\perp$							
< 0	$\perp$	< 0						
$= 0$	$\perp$	< 0	$= 0$					
> 0	$\perp$	$\top$	> 0	> 0				
≤ 0	$\perp$	< 0	≤ 0	$\top$	≤ 0			
$\neq 0$	$\perp$	$\top$	$\neq 0$	$\top$	$\top$	$\top$		
≥ 0	$\perp$	$\top$	≥ 0	> 0	$\top$	$\top$	≥ 0	
$\top$	$\perp$	$\top$	$\top$	$\top$	$\top$	$\top$	$\top$	$\top$

Subtraction

$-$	$\bot$	< 0	$= 0$	> 0	≤ 0	$\neq 0$	≥ 0	$\top$
$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$
< 0	$\bot$	$\top$	> 0	> 0	$\top$	$\top$	> 0	$\top$
$= 0$	$\bot$	< 0	$= 0$	> 0	≤ 0	$\neq 0$	≥ 0	$\top$
> 0	$\bot$	< 0	< 0	$\top$	< 0	$\top$	$\top$	$\top$
≤ 0	$\bot$	$\top$	≥ 0	> 0	$\top$	$\top$	≥ 0	$\top$
$\neq 0$	$\bot$	$\top$	$\neq 0$	$\top$	$\top$	$\top$	$\top$	$\top$
≥ 0	$\bot$	< 0	≤ 0	$\top$	≤ 0	$\top$	$\top$	$\top$
$\top$	$\bot$	$\top$	$\top$	$\top$	$\top$	$\top$	$\top$	$\top$

Multiplication

$*$	$\perp$	< 0	$= 0$	> 0	≤ 0	$\neq 0$	≥ 0	$\top$
$\perp$	$\perp$							
< 0	$\perp$	> 0						
$= 0$	$\perp$	$= 0$	$= 0$					
> 0	$\perp$	< 0	$= 0$	> 0				
≤ 0	$\perp$	≥ 0	$= 0$	≤ 0	≥ 0			
$\neq 0$	$\perp$	$\neq 0$	$= 0$	$\neq 0$	$\top$	$\neq 0$		
≥ 0	$\perp$	≤ 0	$= 0$	≥ 0	≤ 0	$\top$	≥ 0	
$\top$	$\perp$	$\top$	$= 0$	$\top$	$\top$	$\top$	$\top$	$\top$

Division

$/$	$\bot$	< 0	$= 0$	> 0	≤ 0	$\neq 0$	≥ 0	$\top$
$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$
< 0	$\bot$	> 0	$= 0$	< 0	≥ 0	$\neq 0$	≤ 0	$\top$
$= 0$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$
> 0	$\bot$	< 0	$= 0$	> 0	≤ 0	$\neq 0$	≥ 0	$\top$
≤ 0	$\bot$	> 0	$= 0$	< 0	≥ 0	$\neq 0$	≤ 0	$\top$
$\neq 0$	$\bot$	$\neq 0$	$= 0$	$\neq 0$	$\top$	$\neq 0$	$\top$	$\top$
≥ 0	$\bot$	< 0	$= 0$	> 0	≤ 0	$\neq 0$	≥ 0	$\top$
$\top$	$\bot$	$\neq 0$	$= 0$	$\neq 0$	$\top$	$\neq 0$	$\top$	$\top$

Equal

$e_1 = e_2$	$\perp$	< 0	$= 0$	> 0	≤ 0	$\neq 0$	≥ 0	$\top$
$\perp$	$\perp$							
< 0	$\perp$	$s^\#$						
$= 0$	$\perp$	$\perp$	$s^\#$					
> 0	$\perp$	$\perp$	$\perp$	$s^\#$				
≤ 0	$\perp$	$s^\#$	$s^\#$	$\perp$	$s^\#$			
$\neq 0$	$\perp$	$s^\#$	$\perp$	$s^\#$	$s^\#$	$s^\#$		
≥ 0	$\perp$	$\perp$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	
$\top$	$\perp$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$

Equal

$x = e$	$\perp$	< 0	$= 0$	> 0	≤ 0	$\neq 0$	≥ 0	$\top$
$\perp$	$\perp$	$\perp$	$\perp$	$\perp$	$\perp$	$\perp$	$\perp$	$\perp$
< 0	$\perp$	$s^{\#}$	$\perp$	$\perp$	$s^{\#}[x \mapsto < 0]$	$s^{\#}[x \mapsto < 0]$	$\perp$	$s^{\#}[x \mapsto < 0]$
$= 0$	$\perp$	$\perp$	$s^{\#}$	$\perp$	$s^{\#}[x \mapsto = 0]$	$\perp$	$s^{\#}[x \mapsto = 0]$	$s^{\#}[x \mapsto = 0]$
> 0	$\perp$	$\perp$	$\perp$	$s^{\#}$	$\perp$	$s^{\#}[x \mapsto > 0]$	$s^{\#}[x \mapsto > 0]$	$s^{\#}[x \mapsto > 0]$
≤ 0	$\perp$	$s^{\#}$	$s^{\#}$	$\perp$	$s^{\#}$	$s^{\#}[x \mapsto < 0]$	$s^{\#}[x \mapsto = 0]$	$s^{\#}[x \mapsto \leq 0]$
$\neq 0$	$\perp$	$s^{\#}$	$\perp$	$s^{\#}$	$s^{\#}[x \mapsto < 0]$	$s^{\#}$	$s^{\#}[x \mapsto > 0]$	$s^{\#}[x \mapsto \neq 0]$
≥ 0	$\perp$	$\perp$	$s^{\#}$	$s^{\#}$	$s^{\#}[x \mapsto = 0]$	$s^{\#}[x \mapsto > 0]$	$s^{\#}$	$s^{\#}[x \mapsto \geq 0]$
$\top$	$\perp$	$s^{\#}$	$s^{\#}$	$s^{\#}$	$s^{\#}$	$s^{\#}$	$s^{\#}$	$s^{\#}$

Not Equal

$e_1 \neq e_2$	$\perp$	< 0	$= 0$	> 0	≤ 0	$\neq 0$	≥ 0	$\top$
$\perp$	$\perp$							
< 0	$\perp$	$s^{\#}$						
$= 0$	$\perp$	$s^{\#}$	$\perp$					
> 0	$\perp$	$s^{\#}$	$s^{\#}$	$s^{\#}$				
≤ 0	$\perp$	$s^{\#}$	$s^{\#}$	$s^{\#}$	$s^{\#}$			
$\neq 0$	$\perp$	$s^{\#}$	$s^{\#}$	$s^{\#}$	$s^{\#}$	$s^{\#}$		
≥ 0	$\perp$	$s^{\#}$	$s^{\#}$	$s^{\#}$	$s^{\#}$	$s^{\#}$	$s^{\#}$	
$\top$	$\perp$	$s^{\#}$	$s^{\#}$	$s^{\#}$	$s^{\#}$	$s^{\#}$	$s^{\#}$	$s^{\#}$

Not Equal

Università degli Studi di Padova

$x \neq e$	$\bot$	< 0	$= 0$	> 0	≤ 0	$\neq 0$	≥ 0	$\top$
$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$
< 0	$\bot$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$
$= 0$	$\bot$	$s^\#$	$\bot$	$s^\#$	$s^\#[x \mapsto < 0]$	$s^\#$	$s^\#[x \mapsto > 0]$	$s^\#[x \mapsto \neq 0]$
> 0	$\bot$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$
≤ 0	$\bot$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$
$\neq 0$	$\bot$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$
≥ 0	$\bot$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$
$\top$	$\bot$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$

Less Than

Università degli Studi di Padova

$e_1 < e_2$	$\bot$	< 0	$= 0$	> 0	≤ 0	$\neq 0$	≥ 0	$\top$
$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$
< 0	$\bot$	$s^\#$	$\bot$	$\bot$	$s^\#$	$s^\#$	$\bot$	$s^\#$
$= 0$	$\bot$	$s^\#$	$\bot$	$\bot$	$s^\#$	$s^\#$	$\bot$	$s^\#$
> 0	$\bot$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$
≤ 0	$\bot$	$s^\#$	$\bot$	$\bot$	$s^\#$	$s^\#$	$\bot$	$s^\#$
$\neq 0$	$\bot$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$
≥ 0	$\bot$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$
$\top$	$\bot$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$

Less Than

$x < e$	$\bot$	< 0	$= 0$	> 0	≤ 0	$\neq 0$	≥ 0	$\top$
$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$
< 0	$\bot$	$s^\#$	$\bot$	$\bot$	$s^\#[x \mapsto < 0]$	$s^\#[x \mapsto < 0]$	$\bot$	$s^\#[x \mapsto < 0]$
$= 0$	$\bot$	$s^\#$	$\bot$	$\bot$	$s^\#[x \mapsto < 0]$	$s^\#[x \mapsto < 0]$	$\bot$	$s^\#[x \mapsto < 0]$
> 0	$\bot$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$
≤ 0	$\bot$	$s^\#$	$\bot$	$\bot$	$s^\#[x \mapsto < 0]$	$s^\#[x \mapsto < 0]$	$\bot$	$s^\#[x \mapsto < 0]$
$\neq 0$	$\bot$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$
≥ 0	$\bot$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$
$\top$	$\bot$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$

Greater Than

$e_1 > e_2$	$\perp$	< 0	$= 0$	> 0	≤ 0	$\neq 0$	≥ 0	$\top$
$\perp$	$\perp$	$\perp$	$\perp$	$\perp$	$\perp$	$\perp$	$\perp$	$\perp$
< 0	$\perp$	$s^{\#}$	$s^{\#}$	$s^{\#}$	$s^{\#}$	$s^{\#}$	$s^{\#}$	$s^{\#}$
$= 0$	$\perp$	$\perp$	$\perp$	$s^{\#}$	$\perp$	$s^{\#}$	$s^{\#}$	$s^{\#}$
> 0	$\perp$	$\perp$	$\perp$	$s^{\#}$	$\perp$	$s^{\#}$	$s^{\#}$	$s^{\#}$
≤ 0	$\perp$	$s^{\#}$	$s^{\#}$	$s^{\#}$	$s^{\#}$	$s^{\#}$	$s^{\#}$	$s^{\#}$
$\neq 0$	$\perp$	$s^{\#}$	$s^{\#}$	$s^{\#}$	$s^{\#}$	$s^{\#}$	$s^{\#}$	$s^{\#}$
≥ 0	$\perp$	$\perp$	$\perp$	$s^{\#}$	$\perp$	$s^{\#}$	$s^{\#}$	$s^{\#}$
$\top$	$\perp$	$s^{\#}$	$s^{\#}$	$s^{\#}$	$s^{\#}$	$s^{\#}$	$s^{\#}$	$s^{\#}$

Greater Than

$x > e$	$\perp$	< 0	$= 0$	> 0	≤ 0	$\neq 0$	≥ 0	$\top$
$\perp$	$\perp$	$\perp$	$\perp$	$\perp$	$\perp$	$\perp$	$\perp$	$\perp$
< 0	$\perp$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$
$= 0$	$\perp$	$\perp$	$\perp$	$s^\#$	$\perp$	$s^\#[x \mapsto > 0]$	$s^\#[x \mapsto > 0]$	$s^\#[x \mapsto > 0]$
> 0	$\perp$	$\perp$	$\perp$	$s^\#$	$\perp$	$s^\#[x \mapsto > 0]$	$s^\#[x \mapsto > 0]$	$s^\#[x \mapsto > 0]$
≤ 0	$\perp$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$
$\neq 0$	$\perp$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$
≥ 0	$\perp$	$\perp$	$\perp$	$s^\#$	$\perp$	$s^\#[x \mapsto > 0]$	$s^\#[x \mapsto > 0]$	$s^\#[x \mapsto > 0]$
$\top$	$\perp$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$

Less Than or Equal

$e_1 \leq e_2$	$\bot$	< 0	$= 0$	> 0	≤ 0	$\neq 0$	≥ 0	$\top$
$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$
< 0	$\bot$	$s^{\#}$	$\bot$	$\bot$	$s^{\#}$	$s^{\#}$	$\bot$	$s^{\#}$
$= 0$	$\bot$	$s^{\#}$	$s^{\#}$	$\bot$	$s^{\#}$	$s^{\#}$	$s^{\#}$	$s^{\#}$
> 0	$\bot$	$s^{\#}$	$s^{\#}$	$s^{\#}$	$s^{\#}$	$s^{\#}$	$s^{\#}$	$s^{\#}$
≤ 0	$\bot$	$s^{\#}$	$s^{\#}$	$\bot$	$s^{\#}$	$s^{\#}$	$s^{\#}$	$s^{\#}$
$\neq 0$	$\bot$	$s^{\#}$	$s^{\#}$	$s^{\#}$	$s^{\#}$	$s^{\#}$	$s^{\#}$	$s^{\#}$
≥ 0	$\bot$	$s^{\#}$	$s^{\#}$	$s^{\#}$	$s^{\#}$	$s^{\#}$	$s^{\#}$	$s^{\#}$
$\top$	$\bot$	$s^{\#}$	$s^{\#}$	$s^{\#}$	$s^{\#}$	$s^{\#}$	$s^{\#}$	$s^{\#}$

Less Than or Equal

$x \leq e$	$\bot$	< 0	$= 0$	> 0	≤ 0	$\neq 0$	≥ 0	$\top$
$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$
< 0	$\bot$	$s^\#$	$\bot$	$\bot$	$s^\#[x \mapsto < 0]$	$s^\#[x \mapsto < 0]$	$\bot$	$s^\#[x \mapsto < 0]$
$= 0$	$\bot$	$s^\#$	$s^\#$	$\bot$	$s^\#$	$s^\#[x \mapsto < 0]$	$s^\#[x \mapsto = 0]$	$s^\#[x \mapsto \leq 0]$
> 0	$\bot$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$
≤ 0	$\bot$	$s^\#$	$s^\#$	$\bot$	$s^\#$	$s^\#[x \mapsto < 0]$	$s^\#[x \mapsto = 0]$	$s^\#[x \mapsto \leq 0]$
$\neq 0$	$\bot$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$
≥ 0	$\bot$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$
$\top$	$\bot$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$

Greater Than or Equal

$e_1 \geq e_2$	$\perp$	< 0	$= 0$	> 0	≤ 0	$\neq 0$	≥ 0	$\top$
$\perp$	$\perp$	$\perp$	$\perp$	$\perp$	$\perp$	$\perp$	$\perp$	$\perp$
< 0	$\perp$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$
$= 0$	$\perp$	$\perp$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$
> 0	$\perp$	$\perp$	$\perp$	$s^\#$	$\perp$	$s^\#$	$s^\#$	$s^\#$
≤ 0	$\perp$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$
$\neq 0$	$\perp$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$
≥ 0	$\perp$	$\perp$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$
$\top$	$\perp$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$

Greater Than or Equal

$x \geq e$	$\bot$	< 0	$= 0$	> 0	≤ 0	$\neq 0$	≥ 0	$\top$
$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$
< 0	$\bot$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$
$= 0$	$\bot$	$\bot$	$s^\#$	$s^\#$	$s^\#[x \mapsto = 0]$	$s^\#[x \mapsto > 0]$	$s^\#$	$s^\#[x \mapsto \geq 0]$
> 0	$\bot$	$\bot$	$\bot$	$s^\#$	$\bot$	$s^\#[x \mapsto > 0]$	$s^\#[x \mapsto > 0]$	$s^\#[x \mapsto > 0]$
≤ 0	$\bot$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$
$\neq 0$	$\bot$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$
≥ 0	$\bot$	$\bot$	$s^\#$	$s^\#$	$s^\#[x \mapsto = 0]$	$s^\#[x \mapsto > 0]$	$s^\#$	$s^\#[x \mapsto \geq 0]$
$\top$	$\bot$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$	$s^\#$

Join

$\vee$	$\bot$	< 0	$= 0$	> 0	≤ 0	$\neq 0$	≥ 0	$\top$
$\bot$	$\bot$							
< 0	< 0	< 0						
$= 0$	$= 0$	≤ 0	$= 0$					
> 0	> 0	≥ 0	≥ 0	> 0				
≤ 0	≤ 0	≤ 0	≤ 0	$\top$	≤ 0			
$\neq 0$	$\neq 0$	$\neq 0$	$\top$	$\neq 0$	$\top$	$\neq 0$		
≥ 0	≥ 0	$\top$	≥ 0	≥ 0	$\top$	$\top$	≥ 0	
$\top$	$\top$	$\top$	$\top$	$\top$	$\top$	$\top$	$\top$	$\top$

Table of Contents

Intervals

$$
\begin{aligned}
&A := \mathit{Int} \\
&\mathbb{S} := \mathit{List}(\mathit{String} \times \mathit{Int}) \cup \{\star\} \\
&\bot_{\mathbb{S}} := \star \\
&\top_{\mathbb{S}} := [] \\
&\mathit{Int} \ni c ::= \bot \mid (-\infty, b] \mid [a, b] \mid [a, +\infty) \mid \top
\end{aligned}
$$

α on Singletons

$$\alpha_{singleton}(n) := [n, n]$$

Opposite

$-$	$\perp$	$(-\infty, b]$	$[a, b]$	$[a, +\infty)$	$\top$
	$\perp$	$[-b, +\infty)$	$[-b, -a]$	$(-\infty, -a]$	$\top$

$+$	$\perp$	$(-\infty, b]$	$[a, b]$	$[a, +\infty)$	$\top$
$\perp$	$\perp$				
$(-\infty, d]$	$\perp$	$(-\infty, b+d]$			
$[c, d]$	$\perp$	$(-\infty, b+d]$	$[a+c, b+d]$		
$[c, +\infty)$	$\perp$	$\top$	$[a+c, +\infty)$	$[a+c, +\infty)$	
$\top$	$\perp$	$\top$	$\top$	$\top$	$\top$

Subtraction

$-$	$\bot$	$(-\infty, b]$	$[a, b]$	$[a, +\infty)$	$\top$
$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$
$(-\infty, d]$	$\bot$	$\top$	$[a-d, +\infty)$	$[a-d, +\infty)$	$\top$
$[c, d]$	$\bot$	$(-\infty, b-c]$	$[a-d, b-c]$	$[a-d, +\infty)$	$\top$
$[c, +\infty)$	$\bot$	$(-\infty, b-c]$	$(-\infty, b-c]$	$\top$	$\top$
$\top$	$\bot$	$\top$	$\top$	$\top$	$\top$

Multiplication

$*$	$\bot$	$(-\infty, b]$		$[a, b]$		$[a, +\infty)$		$\top$	
$\bot$	$\bot$	$\bot$		$\bot$		$\bot$		$\bot$	
$(-\infty, d]$	$\bot$	$b > 0 \vee d > 0$ $b \leq 0 \wedge d \leq 0$	$\top$ $[bd, +\infty)$	$(a < 0 \wedge b > 0) \vee (a > 0 \wedge b < 0)$ $(a \leq 0 \wedge b \leq 0) \wedge (a \neq 0 \vee b \neq 0)$ $(a \geq 0 \wedge b \geq 0) \wedge (a \neq 0 \vee b \neq 0)$ $(a = 0 \wedge b = 0)$	$\top$ $[min(ad, bd), +\infty)$ $(-\infty, max(ad, bd)]$ $[0, 0]$	$d > 0 \vee a < 0$ $d \leq 0 \wedge a \geq 0$	$\top$ $(-\infty, ad]$	$\top$	
$[c, d]$	$\bot$	$(c < 0 \wedge d > 0) \vee (c > 0 \wedge d < 0)$ $(c \leq 0 \wedge d \leq 0) \wedge (c \neq 0 \vee d \neq 0)$ $(c \geq 0 \wedge d \geq 0) \wedge (c \neq 0 \vee d \neq 0)$ $(c = 0 \wedge d = 0)$	$\top$ $[min(bc, bd), +\infty)$ $(-\infty, max(bc, bd)]$ $[0, 0]$	$[min(ac, ad, bc, bd), max(ac, ad, bc, bd)]$		$(c < 0 \wedge d > 0) \vee (c > 0 \wedge d < 0)$ $(c \leq 0 \wedge d \leq 0) \wedge (c \neq 0 \vee d \neq 0)$ $(c \geq 0 \wedge d \geq 0) \wedge (c \neq 0 \vee d \neq 0)$ $(c = 0 \wedge d = 0)$	$\top$ $(-\infty, max(ac, ad)]$ $[min(ac, ad), +\infty)$ $[0, 0]$	$c = d = 0$ $c \neq 0 \vee d \neq 0$	$[0, 0]$ $\top$
$[c, +\infty)$	$\bot$	$b > 0 \vee c < 0$ $b \leq 0 \wedge c \geq 0$	$\top$ $(-\infty, bc]$	$(a < 0 \wedge b > 0) \vee (a > 0 \wedge b < 0)$ $(a \leq 0 \wedge b \leq 0) \wedge (a \neq 0 \vee b \neq 0)$ $(a \geq 0 \wedge b \geq 0) \wedge (a \neq 0 \vee b \neq 0)$ $(a = 0 \wedge b = 0)$	$\top$ $(-\infty, max(ac, bc)]$ $[min(ac, bc), +\infty)$ $[0, 0]$	$a < 0 \vee c < 0$ $a \geq 0 \wedge c \geq 0$	$\top$ $(-\infty, ac]$	$\top$	
$\top$	$\bot$	$\top$		$a = b = 0$ $a \neq 0 \vee b \neq 0$	$[0, 0]$ $\top$	$\top$		$\top$	

Division

<table>
<tr><td>$/$</td><td>$\perp$</td><td colspan="2">$(-\infty, b]$</td><td colspan="2">$[a, b]$</td><td colspan="2">$[a, +\infty)$</td><td colspan="2">$\top$</td></tr>
<tr><td>$\perp$</td><td>$\perp$</td><td colspan="2">$\perp$</td><td colspan="2">$\perp$</td><td colspan="2">$\perp$</td><td colspan="2">$\perp$</td></tr>
<tr><td>$(-\infty, d]$</td><td>$\perp$</td><td>$d < 0$
$d = 0$
otherwise</td><td>$[min(0, b/d), +\infty)$
$(-\infty, b]/(-\infty, -1]$
$\top$</td><td>$d < 0$
$d = 0$
otherwise</td><td>$[min(0, b/d), max(0, a/d)]$
$[a, b]/(-\infty, -1]$
$[a, b]/(-\infty, -1] \vee [a, b]/[1, d]$</td><td>$d < 0$
$d = 0$
otherwise</td><td>$(-\infty, max(a/d, 0)]$
$[a, +\infty)/(-\infty, -1]$
$\top$</td><td colspan="2">$\top$</td></tr>
<tr><td>$[c, d]$</td><td>$\perp$</td><td>$c = d = 0$
$0 < c \leq d$
$0 = c < d$
$c \leq d < 0$
$c < d = 0$
otherwise</td><td>$\perp$
$(-\infty, max(b/c, b/d)]$
$(-\infty, b]/[1, d]$
$[min(b/c, b/d), +\infty)$
$(-\infty, b]/[c, -1]$
$\top$</td><td>$c = d = 0$
$0 < c \leq d \vee c \leq d < 0$
$0 = c < d$
$c < d = 0$
$c < 0 < d$</td><td>$\perp$
$[min(a/c, a/d, b/c, b/d), max(a/c, a/d, b/c, b/d)]$
$[a, b]/[1, d]$
$[a, b]/[c, -1]$
$[a, b]/[c, -1] \vee [a, b]/[1, d]$</td><td>$c = d = 0$
$0 < c \leq d$
$0 = c < d$
$c \leq d < 0$
$c < d = 0$
otherwise</td><td>$\perp$
$[min(a/c, a/d), +\infty)$
$[a, +\infty)/[1, d]$
$(-\infty, max(a/c, a/d)]$
$[a, +\infty)/[c, -1]$
$\top$</td><td>$c = d = 0$
otherwise</td><td>$\perp$
$\top$</td></tr>
<tr><td>$[c, +\infty)$</td><td>$\perp$</td><td>$c > 0$
$c = 0$
otherwise</td><td>$(-\infty, max(0, b/c)]$
$(-\infty, b]/[1, +\infty)$
$\top$</td><td>$c > 0$
$c = 0$
otherwise</td><td>$[min(0, a/c), max(0, b/c)]$
$[a, b]/[1, +\infty)$
$[a, b]/[c, -1] \vee [a, b]/[1, +\infty)$</td><td>$c > 0$
$c = 0$
otherwise</td><td>$[min(a/c, 0), +\infty)$
$[a, +\infty)/[1, +\infty)$
$\top$</td><td colspan="2">$\top$</td></tr>
<tr><td>$\top$</td><td>$\perp$</td><td colspan="2">$\top$</td><td colspan="2">$[a, b]/(-\infty, -1] \vee [a, b]/[1, +\infty)$</td><td colspan="2">$\top$</td><td colspan="2">$\top$</td></tr>
</table>

Equal

$e_1 = e_2$	$\perp$	$(-\infty, b]$	$[a, b]$	$[a, +\infty)$	$\top$
$\perp$	$\perp$	$\perp$	$\perp$	$\perp$	$\perp$
$(-\infty, d]$	$\perp$	$s^{\#}$	if $a > d$ then $\perp$ else $s^{\#}$	if $a > d$ then $\perp$ else $s^{\#}$	$s^{\#}$
$[c, d]$	$\perp$	if $b < c$ then $\perp$ else $s^{\#}$	if $a > d$ or $b < c$ then $\perp$ else $s^{\#}$	if $a > d$ then $\perp$ else $s^{\#}$	$s^{\#}$
$[c, +\infty)$	$\perp$	if $b < c$ then $\perp$ else $s^{\#}$	if $b < c$ then $\perp$ else $s^{\#}$	$s^{\#}$	$s^{\#}$
$\top$	$\perp$	$s^{\#}$	$s^{\#}$	$s^{\#}$	$s^{\#}$

Equal

$x = e$	$\perp$	$(-\infty, b]$	$[a, b]$	$[a, +\infty)$	$\top$
$\perp$	$\perp$	$\perp$	$\perp$	$\perp$	$\perp$
$(-\infty, d]$	$\perp$	$b \leq d \quad s^{\#}$ $b > d \quad s^{\#}[x \mapsto (-\infty, d]]$	$a > d \quad \perp$ $a \leq d \wedge b > d \quad s^{\#}[x \mapsto [a, d]]$ $a \leq d \wedge b \leq d \quad s^{\#}$	$a > d \quad \perp$ $a \leq d \quad s^{\#}[x \mapsto [a, d]]$	$s^{\#}[x \mapsto (-\infty, d]]$
$[c, d]$	$\perp$	$b < c \quad \perp$ $c \leq b \leq d \quad s^{\#}[x \mapsto [c, b]]$ $b > d \quad s^{\#}[x \mapsto [c, d]]$	$b < c \vee a > d \quad \perp$ $b > d \wedge a < c \quad s^{\#}[x \mapsto [c, d]]$ $b > d \wedge a \geq c \quad s^{\#}[x \mapsto [a, d]]$ $c \leq b \leq d \wedge a < c \quad s^{\#}[x \mapsto [c, b]]$ $c \leq b \leq d \wedge c \leq a \leq d \quad s^{\#}$	$a > d \quad \perp$ $a < c \quad s^{\#}[x \mapsto [c, d]]$ $c \leq a \leq d \quad s^{\#}[x \mapsto [a, d]]$	$s^{\#}[x \mapsto [c, d]]$
$[c, +\infty)$	$\perp$	$b < c \quad \perp$ $b \geq c \quad s^{\#}[x \mapsto [c, b]]$	$b < c \quad \perp$ $b \geq c \wedge a < c \quad s^{\#}[x \mapsto [c, b]]$ $a \geq c \quad s^{\#}$	$a < c \quad s^{\#}[x \mapsto [c, +\infty)]$ $a \geq c \quad s^{\#}$	$s^{\#}[x \mapsto [c, +\infty)]$
$\top$	$\perp$	$s^{\#}$	$s^{\#}$	$s^{\#}$	$s^{\#}$

Not Equal

$e_1 \neq e_2$	$\bot$	$(-\infty, b]$	$[a, b]$	$[a, +\infty)$	$\top$
$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$
$(-\infty, d]$	$\bot$	$s^{\#}$	$s^{\#}$	$s^{\#}$	$s^{\#}$
$[c, d]$	$\bot$	$s^{\#}$	$a = b = c = d$ $\bot$ otherwise $s^{\#}$	$s^{\#}$	$s^{\#}$
$[c, +\infty)$	$\bot$	$s^{\#}$	$s^{\#}$	$s^{\#}$	$s^{\#}$
$\top$	$\bot$	$s^{\#}$	$s^{\#}$	$s^{\#}$	$s^{\#}$

Not Equal

UNIVERSITÀ DEGLI STUDI DI PADOVA

$x \neq e$	$\bot$	$(-\infty, b]$	$[a, b]$	$[a, +\infty)$	$\top$
$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$
$(-\infty, d]$	$\bot$	$s^\#$	$s^\#$	$s^\#$	$s^\#$
$[c, d]$	$\bot$	$b = c = d$ $s^\#[x \mapsto (-\infty, b-1]]$ otherwise $s^\#$	$a = c = d \wedge a \neq b$ $s^\#[x \mapsto [a+1, b]]$ $b = c = d \wedge a \neq b$ $s^\#[x \mapsto [a, b-1]]$ $a = b = c = d$ $\bot$ otherwise $s^\#$	$a = c = d$ $s^\#[x \mapsto [a+1, +\infty)]$ otherwise $s^\#$	$s^\#$
$[c, +\infty)$	$\bot$	$s^\#$	$s^\#$	$s^\#$	$s^\#$
$\top$	$\bot$	$s^\#$	$s^\#$	$s^\#$	$s^\#$

Less Than

$e_1 < e_2$	$\perp$	$(-\infty, b]$	$[a, b]$	$[a, +\infty)$	$\top$
$\perp$	$\perp$	$\perp$	$\perp$	$\perp$	$\perp$
$(-\infty, d]$	$\perp$	$s^\#$	$a \geq d \quad \perp$ $a < d \quad s^\#$	$a \geq d \quad \perp$ $a < d \quad s^\#$	$s^\#$
$[c, d]$	$\perp$	$s^\#$	$a \geq d \quad \perp$ $a < d \quad s^\#$	$a \geq d \quad \perp$ $a < d \quad s^\#$	$s^\#$
$[c, +\infty)$	$\perp$	$s^\#$	$s^\#$	$s^\#$	$s^\#$
$\top$	$\perp$	$s^\#$	$s^\#$	$s^\#$	$s^\#$

Less Than

Università degli Studi di Padova

$x < e$	$\bot$	$(-\infty, b]$	$[a, b]$	$[a, +\infty)$	$\top$
$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$
$(-\infty, d]$	$\bot$	$b \geq d$ $\quad s^{\#}[x \mapsto (-\infty, d-1]]$ $b < d$ $\quad s^{\#}$	$a \geq d$ $\quad \bot$ $a < d \land b \geq d$ $\quad s^{\#}[x \mapsto [a, d-1]]$ $a < d \land b < d$ $\quad s^{\#}$	$a \geq d$ $\quad \bot$ $a < d$ $\quad s^{\#}[x \mapsto [a, d-1]]$	$s^{\#}[x \mapsto (-\infty, d-1]]$
$[c, d]$	$\bot$	$b \geq d$ $\quad s^{\#}[x \mapsto (-\infty, d-1]]$ $b < d$ $\quad s^{\#}$	$a \geq d$ $\quad \bot$ $a < d \land b \geq d$ $\quad s^{\#}[x \mapsto [a, d-1]]$ $a < d \land b < d$ $\quad s^{\#}$	$a \geq d$ $\quad \bot$ $a < d$ $\quad s^{\#}[x \mapsto [a, d-1]]$	$s^{\#}[x \mapsto (-\infty, d-1]]$
$[c, +\infty)$	$\bot$	$s^{\#}$	$s^{\#}$	$s^{\#}$	$s^{\#}$
$\top$	$\bot$	$s^{\#}$	$s^{\#}$	$s^{\#}$	$s^{\#}$

Less Than or Equal

$e_1 \leq e_2$	$\perp$	$(-\infty, b]$	$[a, b]$	$[a, +\infty)$	$\top$
$\perp$	$\perp$	$\perp$	$\perp$	$\perp$	$\perp$
$(-\infty, d]$	$\perp$	$s^\#$	$a > d$ $\perp$ $a \leq d$ $s^\#$	$a > d$ $\perp$ $a \leq d$ $s^\#$	$s^\#$
$[c, d]$	$\perp$	$s^\#$	$a > d$ $\perp$ $a \leq d$ $s^\#$	$a > d$ $\perp$ $a \leq d$ $s^\#$	$s^\#$
$[c, +\infty)$	$\perp$	$s^\#$	$s^\#$	$s^\#$	$s^\#$
$\top$	$\perp$	$s^\#$	$s^\#$	$s^\#$	$s^\#$

Less Than or Equal

$x \leq e$	$\bot$	$(-\infty, b]$	$[a, b]$	$[a, +\infty)$	$\top$
$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$
$(-\infty, d]$	$\bot$	$b > d \quad s^{\#}[x \mapsto (-\infty, d]]$ $b \leq d \quad s^{\#}$	$a > d \quad \bot$ $a \leq d \wedge b > d \quad s^{\#}[x \mapsto [a, d]]$ $a \leq d \wedge b \leq d \quad s^{\#}$	$a > d \quad \bot$ $a \leq d \quad s^{\#}[x \mapsto [a, d]]$	$s^{\#}[x \mapsto (-\infty, d]]$
$[c, d]$	$\bot$	$b > d \quad s^{\#}[x \mapsto (-\infty, d]]$ $b \leq d \quad s^{\#}$	$a > d \quad \bot$ $a \leq d \wedge b > d \quad s^{\#}[x \mapsto [a, d]]$ $a \leq d \wedge b \leq d \quad s^{\#}$	$a > d \quad \bot$ $a \leq d \quad s^{\#}[x \mapsto [a, d]]$	$s^{\#}[x \mapsto (-\infty, d]]$
$[c, +\infty)$	$\bot$	$s^{\#}$	$s^{\#}$	$s^{\#}$	$s^{\#}$
$\top$	$\bot$	$s^{\#}$	$s^{\#}$	$s^{\#}$	$s^{\#}$

Greater Than

Università degli Studi di Padova

$e_1 > e_2$	$\bot$	$(-\infty, b]$	$[a, b]$	$[a, +\infty)$	$\top$
$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$
$(-\infty, d]$	$\bot$	$s^\#$	$s^\#$	$s^\#$	$s^\#$
$[c, d]$	$\bot$	$b \le c \quad \bot$ $b > c \quad s^\#$	$b \le c \quad \bot$ $b > c \quad s^\#$	$s^\#$	$s^\#$
$[c, +\infty)$	$\bot$	$b \le c \quad \bot$ $b > c \quad s^\#$	$b \le c \quad \bot$ $b > c \quad s^\#$	$s^\#$	$s^\#$
$\top$	$\bot$	$s^\#$	$s^\#$	$s^\#$	$s^\#$

Greater Than

$x > e$	$\bot$	$(-\infty, b]$	$[a, b]$	$[a, +\infty)$	$\top$
$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$
$(-\infty, d]$	$\bot$	$s^\#$	$s^\#$	$s^\#$	$s^\#$
$[c, d]$	$\bot$	$b \leq c \quad \bot$ $b > c \quad s^\#[x \mapsto [c+1, b]]$	$b \leq c \quad \bot$ $b > c \wedge a \leq c \quad s^\#[x \mapsto [c+1, b]]$ $b > c \wedge a > c \quad s^\#$	$a \leq c \quad s^\#[x \mapsto [c+1, +\infty)]$ $a > c \quad s^\#$	$s^\#[x \mapsto [c+1, +\infty)]$
$[c, +\infty)$	$\bot$	$b \leq c \quad \bot$ $b > c \quad s^\#[x \mapsto [c+1, b]]$	$b \leq c \quad \bot$ $b > c \wedge a \leq c \quad s^\#[x \mapsto [c+1, b]]$ $b > c \wedge a > c \quad s^\#$	$a \leq c \quad s^\#[x \mapsto [c+1, +\infty)]$ $a > c \quad s^\#$	$s^\#[x \mapsto [c+1, +\infty)]$
$\top$	$\bot$	$s^\#$	$s^\#$	$s^\#$	$s^\#$

Greater Than or Equal

$e_1 \geq e_2$	$\bot$	$(-\infty, b]$	$[a, b]$	$[a, +\infty)$	$\top$
$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$
$(-\infty, d]$	$\bot$	$s^\#$	$s^\#$	$s^\#$	$s^\#$
$[c, d]$	$\bot$	$b < c$ $\bot$ $b \geq c$ $s^\#$	$b < c$ $\bot$ $b \geq c$ $s^\#$	$s^\#$	$s^\#$
$[c, +\infty)$	$\bot$	$b < c$ $\bot$ $b \geq c$ $s^\#$	$b < c$ $\bot$ $b \geq c$ $s^\#$	$s^\#$	$s^\#$
$\top$	$\bot$	$s^\#$	$s^\#$	$s^\#$	$s^\#$

Greater Than or Equal

$x \geq e$	$\bot$	$(-\infty, b]$	$[a, b]$	$[a, +\infty)$	$\top$
$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$
$(-\infty, d]$	$\bot$	$s^\#$	$s^\#$	$s^\#$	$s^\#$
$[c, d]$	$\bot$	$b < c$ $\bot$ $b \geq c$ $s^\#[x \mapsto [c, b]]$	$b < c$ $\bot$ $b \geq c \wedge a < c$ $s^\#[x \mapsto [c, b]]$ $b \geq c \wedge a \geq c$ $s^\#$	$a < c$ $s^\#[x \mapsto [c, +\infty)]$ $a \geq c$ $s^\#$	$s^\#[x \mapsto [c, +\infty)]$
$[c, +\infty)$	$\bot$	$b < c$ $\bot$ $b \geq c$ $s^\#[x \mapsto [c, b]]$	$b < c$ $\bot$ $b \geq c \wedge a < c$ $s^\#[x \mapsto [c, b]]$ $b \geq c \wedge a \geq c$ $s^\#$	$a < c$ $s^\#[x \mapsto [c, +\infty)]$ $a \geq c$ $s^\#$	$s^\#[x \mapsto [c, +\infty)]$
$\top$	$\bot$	$s^\#$	$s^\#$	$s^\#$	$s^\#$

Join

$\vee$	$\perp$	$(-\infty, b]$	$[a, b]$	$[a, +\infty)$	$\top$
$\perp$	$\perp$	$(-\infty, b]$	$[a, b]$	$[a, +\infty)$	$\top$
$(-\infty, d]$	$(-\infty, d]$	$(-\infty, max(b, d)]$	$(-\infty, max(b, d)]$	$\top$	$\top$
$[c, d]$	$[c, d]$	$(-\infty, max(b, d)]$	$[min(a, c), max(b, d)]$	$[min(a, c), +\infty)$	$\top$
$[c, +\infty)$	$[c, +\infty)$	$\top$	$[min(a, c), +\infty)$	$[min(a, c), +\infty)$	$\top$
$\top$	$\top$	$\top$	$\top$	$\top$	$\top$

Widen

<table>
<tr><td>∇</td><td>$\bot$</td><td colspan="2">$(-\infty, b]$</td><td colspan="2">$[a, b]$</td><td colspan="2">$[a, +\infty)$</td><td>$\top$</td></tr>
<tr><td>$\bot$</td><td>$\bot$</td><td colspan="2">$(-\infty, b]$</td><td colspan="2">$[a, b]$</td><td colspan="2">$[a, +\infty)$</td><td>$\top$</td></tr>
<tr><td rowspan="2">$(-\infty, d]$</td><td rowspan="2">$(-\infty, d]$</td><td>$d \leq b$</td><td>$(-\infty, b]$</td><td>$d \leq b$</td><td>$(-\infty, b]$</td><td colspan="2" rowspan="2">$\top$</td><td rowspan="2">$\top$</td></tr>
<tr><td>otherwise</td><td>$\top$</td><td>otherwise</td><td>$\top$</td></tr>
<tr><td rowspan="4">$[c, d]$</td><td rowspan="4">$[c, d]$</td><td rowspan="2">$d \leq b$</td><td rowspan="2">$(-\infty, b]$</td><td>$a \leq c \land d \leq b$</td><td>$[a, b]$</td><td rowspan="2">$a \leq c$</td><td rowspan="2">$[a, +\infty)$</td><td rowspan="2">$\top$</td></tr>
<tr><td>$a \leq c \land d > b$</td><td>$[a, +\infty)$</td></tr>
<tr><td rowspan="2">otherwise</td><td rowspan="2">$\top$</td><td>$a > c \land d \leq b$</td><td>$(-\infty, b]$</td><td rowspan="2">otherwise</td><td rowspan="2">$\top$</td><td rowspan="2">$\top$</td></tr>
<tr><td>otherwise</td><td>$\top$</td></tr>
<tr><td rowspan="2">$[c, +\infty)$</td><td rowspan="2">$[c, +\infty)$</td><td colspan="2" rowspan="2">$\top$</td><td>$a \leq c$</td><td>$[a, +\infty)$</td><td>$a \leq c$</td><td>$[a, +\infty)$</td><td rowspan="2">$\top$</td></tr>
<tr><td>otherwise</td><td>$\top$</td><td>otherwise</td><td>$\top$</td></tr>
<tr><td>$\top$</td><td>$\top$</td><td colspan="2">$\top$</td><td colspan="2">$\top$</td><td colspan="2">$\top$</td><td>$\top$</td></tr>
</table>

Narrow

Δ	$\bot$	$(-\infty, b]$	$[a, b]$	$[a, +\infty)$	$\top$
$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$
$(-\infty, d]$	$\bot$	$(-\infty, b]$	$[a, b]$	$[a, d]$	$(-\infty, d]$
$[c, d]$	$\bot$	$[c, b]$	$[a, b]$	$[a, d]$	$[c, d]$
$[c, +\infty)$	$\bot$	$[c, b]$	$[a, b]$	$[a, +\infty)$	$[c, +\infty)$
$\top$	$\bot$	$(-\infty, b]$	$[a, b]$	$[a, +\infty)$	$\top$

Table of Contents

Example 1

$$P := \textbf{ while } x \neq 0 \textbf{ do } x := x + 1$$

$$AI_{ExtSign}(P)(false)([(x, < 0)]) = ([(x, = 0)], [[(x, \top)]])$$

$$AI_{ExtSign}(P)(false)([(x, = 0)]) = ([(x, = 0)], [[(x, = 0)]])$$

$$AI_{ExtSign}(P)(false)([(x, > 0)]) = (\perp_{\mathbb{S}}, [[(x, > 0)]])$$

Example 2

$$P := \ x := x + y; y := y + 1$$

$$AI_{ExtSign}(P)(false)([(x, \ \leq 0), (y, \ < 0)]) = ([(x, \ < 0), (y, \top)], [])$$

Example 3

$P :=\ x := 40; \textbf{while } x \neq 0 \textbf{ do } x := x - 1$

$AI_{ExtSign}(P)(\mathit{false})(\top_{\mathbb{S}}) = ([(x,\ = 0)], [\top_{\mathbb{S}}])$ in 1 iteration

$AI_{Int}(P)(\mathit{false})(\top_{\mathbb{S}}) = ([(x, [0,0])], [[(x, [0,40])]])$ in 40 iterations

$AI_{Int}(P)(\mathit{true})(\top_{\mathbb{S}}) = ([(x, [0,0])], [[(x, (-\infty, 40])]])$ in $1+1$ iterations

Example 4

$P :=$ **while** $x \geq 0$ **do** $(x := x - 1; y := y + 1)$

$AI_{Int}(P)(\mathit{false})([(x, [10, 10]), (y, [0, 0])])$ loops

$AI_{Int}(P)(\mathit{true})([(x, [10, 10]), (y, [0, 0])]) =$

$$([(x, [-1, -1]), (y, [0, +\infty))], [[(x, [-1, 10]), (y, [0, +\infty))]])$$

in $1 + 1$ iterations

Example 5

$$P := \ \textbf{while}\ x < 10\ \textbf{do}\ x := x + 1$$

$$AI_{Int}(P)(\mathit{false})([(x,[0,0])]) =$$
$$([(x,[10,10])],[[(x,[0,10])]])\ \text{in 10 iterations}$$

$$AI_{Int}(P)(\mathit{true})([(x,[0,0])]) =$$
$$([(x,[10,10])],[[(x,[0,10])]])\ \text{in } 1+1 \text{ iterations}$$

Example 6

$$P := \textbf{ while } x \leq 100 \textbf{ do } x := x + 1$$

$$AI_{Int}(P)(\mathit{false})([(x, [1, 1])]) =$$

$$([(x, [101, 101])], [[(x, [1, 101])]]) \text{ in } 101 \text{ iterations}$$

$$AI_{Int}(P)(\mathit{true})([(x, [1, 1])]) =$$

$$([(x, [101, 101])], [[(x, [1, 101])]]) \text{ in } 1 + 1 \text{ iterations}$$

Example 7

$P := \ x := 0; \textbf{while } x < 40 \textbf{ do } x := x + 1$

$AI_{Int}(P)(\mathit{false})(\top_{\mathbb{S}}) = ([(x, [40, 40])], [[(x, [0, 40])]])$ in 40 iterations

$AI_{Int}(P)(\mathit{true})(\top_{\mathbb{S}}) = ([(x, [40, 40])], [[(x, [0, 40])]])$ in $1 + 1$ iterations

Example 8

$$
\begin{aligned}
P := \;& x := 0;\\
& \quad \textbf{while } 1 = 1 \textbf{ do}\\
& \qquad (\textbf{if } y = 0 \textbf{ then}\\
& \qquad\qquad (x := x + 1; \textbf{if } x < 40 \textbf{ then } x := 0 \textbf{ else skip})\\
& \qquad\ \textbf{else skip})
\end{aligned}
$$

$AI_{Int}(P)(false)([[(y,[0,1])]]) = (\bot_{\mathbb{S}}, [[(x,[0,40])]])$ in 40 iterations

$AI_{Int}(P)(true)([[(y,[0,1])]]) = (\bot_{\mathbb{S}}, [[(x,[0,+\infty))]])$ in $1+1$ iterations

Example 9

$$
\begin{aligned}
P := \;& i := 1; \\
& \quad \textbf{while } i \leq 3 \textbf{ do} \\
& \qquad (j := 1; \\
& \qquad \textbf{while } j \leq i \textbf{ do } j := j + 1; \\
& \qquad i := i + 1)
\end{aligned}
$$

$AI_{Int}(P)(false)(\top_{\mathbb{S}}) = ([(i, [4, 4])], [[(i, [1, 1]), (j, [1, 2])], [(i, [1, 2]), (j, [1, 3$

$AI_{Int}(P)(true)(\top_{\mathbb{S}}) = ([(i, [4, 4])], [[(i, [1, 4])]])$

Example 10

$$
\begin{aligned}
P :=\ & i := 1; \\
& \quad \textbf{while } i \leq 4 \textbf{ do} \\
& \quad\quad (j := 0; \\
& \quad\quad \textbf{while } j \leq 3 \textbf{ do} \\
& \quad\quad\quad (k := 0; \\
& \quad\quad\quad \textbf{while } k \leq 5 \textbf{ do } (z := i * j * k; k := k + 1); \\
& \quad\quad\quad j := j + 1) \\
& \quad\quad i := i + 1)
\end{aligned}
$$

$$AI_{Int}(P)(false)(\top_{\mathbb{S}}) = ([(i, [5, 5])], [\ldots, [(i, [1, 5])]])$$

$$AI_{Int}(P)(true)(\top_{\mathbb{S}}) = ([(i, [5, 5])], [[(i, [1, 5])]])$$