Software Verification

Borsetto Riccardo

Univerisità degli Studi di Padova

5th December 2022

Language

```
Abinop \ni aop ::= + | - | * | \
Aexp \ni e ::= x \mid n \mid -e \mid e_1 aop e_2

Bbinop \ni bop ::= = | \neq | < | \leq | > | \geq

Bexp \ni b ::= true \mid false \mid e_1 bop e_2 \mid b_1 \land b_2 \mid b_1 \lor b_2 \mid \neg b

While \ni S ::= x := e \mid skip \mid S_1; S_2 \mid if \ b then S_1 else S_2 \mid b while b do S
```

Abstract Interpreter

$$AI: \textbf{While} \rightarrow bool \rightarrow \mathbb{S} \rightarrow \mathbb{S} \times List(\mathbb{S})$$

$$AI(x := e)(w)(s^{\sharp}) := (s^{\sharp}[x \mapsto \mathcal{A}^{\sharp}(e)(s^{\sharp})], [])$$

$$AI(\textbf{skip})(w)(s^{\sharp}) := (s^{\sharp}, [])$$

$$AI(S_1; S_2)(w)(s^{\sharp}) := (u^{\sharp}, invs_1 +_{List(\mathbb{S})} invs_2)$$

$$\text{with } (u^{\sharp}, invs_2) := AI(S_2)(w)(t^{\sharp})$$

$$(t^{\sharp}, invs_1) := AI(S_1)(w)(s^{\sharp})$$

$$AI(\textbf{if } b \textbf{ then } S_1 \textbf{ else } S_2)(w)(s^{\sharp}) := (t^{\sharp} \vee_{\mathbb{S}} u^{\sharp}, invs_1 +_{List(\mathbb{S})} invs_2)$$

$$\text{with } (t^{\sharp}, invs_1) := (AI(S_1)(w) \circ \mathcal{B}^{\sharp}(b))(s^{\sharp})$$

$$(u^{\sharp}, invs_2) := (AI(S_2)(w) \circ \mathcal{B}^{\sharp}(\neg b))(s^{\sharp})$$

$$AI(\textbf{while } b \textbf{ do } S)(w)(s^{\sharp}) := (\mathcal{B}^{\sharp}(\neg b)(t^{\sharp}), invs)$$

$$\text{with } (t^{\sharp}, invs) := ab\text{-lfp}(AI(S)(w))(b)(t^{\sharp})(w)$$

Abstract Semantics of arithmetic expressions

$$egin{aligned} \mathcal{A}^{\sharp}: \mathbf{Aexp} &
ightarrow \mathbb{S}
ightarrow A \ &\mathcal{A}^{\sharp}(n)(s^{\sharp}) := lpha_{singleton}(n) \ &\mathcal{A}^{\sharp}(x)(s^{\sharp}) := \operatorname{lookup}_{\mathbb{S}}(s^{\sharp})(x) \ &\mathcal{A}^{\sharp}(e_1 ext{ aop } e_2)(s^{\sharp}) := \mathcal{A}^{\sharp}(e_1)(s^{\sharp}) ext{ aop}^{A} \mathcal{A}^{\sharp}(e_2)(s^{\sharp}) \ &\mathcal{A}^{\sharp}(-e)(s^{\sharp}) := -^{A} \mathcal{A}^{\sharp}(e)(s^{\sharp}) \end{aligned}$$

Abstract Semantics of boolean expressions

$$egin{align*} \mathcal{B}^{\sharp}: \mathbf{Bexp} &
ightarrow \mathbb{S}
ightarrow \mathbb{S} \ \mathcal{B}^{\sharp}(true)(s^{\sharp}) := s^{\sharp} \ \mathcal{B}^{\sharp}(false)(s^{\sharp}) := oldsymbol{eta} \ \mathcal{B}^{\sharp}(e_1 ext{ bop } e_2)(s^{\sharp}) := \ \mathcal{B}^{\sharp}(b_1 \wedge b_2)(s^{\sharp}) := (\mathcal{B}^{\sharp}(b_2) \circ \mathcal{B}^{\sharp}(b_1))(s^{\sharp}) \ \mathcal{B}^{\sharp}(b_1 ee b_2)(s^{\sharp}) := \mathcal{B}^{\sharp}(b_1)(s^{\sharp}) ee \mathcal{B}^{\sharp}(b_2)(s^{\sharp}) \end{aligned}$$

Step

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

Invariant Check

$$\begin{array}{l} \text{is-inv}: (\mathbb{S} \to \mathbb{S} \times \textit{List}(\mathbb{S})) \to \mathbb{S} \to \mathbb{S} \to \textit{bool} \\ \\ \text{is-inv}(f)(s^{\sharp})(t^{\sharp}) := t^{\sharp} \sqsubseteq_{\mathbb{S}} u^{\sharp} \\ \\ \text{with } u^{\sharp} := \pi_{1}(\textit{step}(f)(b)(s^{\sharp})(t^{\sharp})) \end{array}$$

Steps

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

Widening

$$egin{aligned} \mathsf{wid} : (\mathbb{S} o \mathbb{S} imes \mathit{List}(\mathbb{S})) o bool o \mathbb{S} o \mathbb{S} \ & \mathsf{wid}(f)(b)(s^\sharp)(t^\sharp) := egin{cases} t^\sharp & \mathsf{if is\text{-}inv}(f)(s^\sharp)(t^\sharp) \ & \mathsf{wid}(f)(b)(s^\sharp)(t^\sharp) \nabla_{\mathbb{S}} \ u^\sharp) & \mathsf{otherwise} \end{cases} \ & \mathsf{with} \ u^\sharp := \pi_1(\mathit{step}(f)(b)(s^\sharp)(t^\sharp)) \end{aligned}$$

Narrowing

$$\begin{array}{l} \mathsf{nar} : (\mathbb{S} \to \mathbb{S} \times \mathit{List}(\mathbb{S})) \to \mathit{bool} \to \mathbb{S} \to \mathbb{S} \to \mathbb{S} \times \mathit{List}(\mathbb{S}) \\ \mathsf{nar}(f)(b)(s^{\sharp})(t^{\sharp}) := \begin{cases} (v^{\sharp}, [v^{\sharp}]) & \text{if is-inv}(f)(s^{\sharp})(v^{\sharp}) \\ (z^{\sharp}, \mathit{invs}_1 +_{\mathit{List}(\mathbb{S})} \mathit{invs}_2) & \text{otherwise} \end{cases} \\ \mathsf{with} \ u^{\sharp} := \pi_1(\mathsf{step}(f)(b)(s^{\sharp})(t^{\sharp})) \\ v^{\sharp} := t^{\sharp} \ \Delta_{\mathbb{S}} \ u^{\sharp} \\ (w^{\sharp}, \mathit{invs}_1) := \mathsf{step}(f)(b)(s^{\sharp})(v^{\sharp}) \\ (z^{\sharp}, \mathit{invs}_2) := \mathsf{nar}(f)(b)(s^{\sharp})(v^{\sharp}\Delta_{\mathbb{S}} w^{\sharp}) \end{array}$$

Abstract Least Fixed Point

$$\begin{split} \mathsf{ab\text{-}lfp} : (\mathbb{S} \to \mathbb{S} \times \mathit{List}(\mathbb{S})) \to \mathit{bool} \to \mathbb{S} \to \mathit{bool} \to \mathbb{S} \times \mathit{List}(\mathbb{S}) \\ \mathsf{ab\text{-}lfp}(f)(b)(s^\sharp)(w) := \begin{cases} \mathsf{nar}(f)(b)(s^\sharp)(t^\sharp) & \text{if } w \\ \mathsf{steps}(f)(b)(s^\sharp)(s^\sharp) & \text{otherwise} \end{cases} \\ \mathsf{with} \ t^\sharp := \mathsf{wid}(f)(b)(s^\sharp)(s^\sharp). \end{aligned}$$

Abstract State Update

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

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

Abstract State Join

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

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

Abstract State Lookup

 $lookup_{\mathbb{S}}(s^{\sharp})(x)$ defined using recursion

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

Partial order

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

State Widening

$$s^{\sharp}
abla_{\mathbb{S}} t^{\sharp} := egin{cases} t^{\sharp} & \textit{ifs}^{\sharp} = ot_{\mathbb{S}} \ \textit{map}(f_{t^{\sharp}})(s^{\sharp}) & \textit{otherwise} \end{cases}$$
 with $f_{t^{\sharp}}(x,a) := (x, a \Delta \textit{lookup}(t^{\sharp})(x)).$

State Narrowing

$$s^\sharp \Delta_\mathbb{S} t^\sharp := egin{cases} ot \mathbb{S} & \textit{ifs}^\sharp = ot \mathbb{S} \\ \textit{map}(f_{t^\sharp})(s^\sharp) & \textit{otherwise} \end{cases}$$
 with $f_{t^\sharp}(x,a) := (x,a\Delta lookup(t^\sharp)(x)).$

Extended Sign

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

α on Singletons

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

Addition

+	1	< 0	= 0	> 0	≤ 0	= 0	≥ 0	Т
上	\perp							
< 0		< 0						
= 0	上	< 0	= 0					
> 0	\perp	Т	> 0	> 0				
<u>≤</u> 0	T	< 0	≤ 0	Т	≤ 0			
<i>≠</i> 0		Т	<i>≠</i> 0	Т	Т	Т		
≥ 0	1	Т	≥ 0	> 0	Т	Т	≥ 0	
Т	Т	Т	Т	Т	Т	Т	Т	Т

Subtraction

_	Τ	< 0	= 0	> 0	≤ 0	= 0	≥ 0	Т
上	\vdash	\perp	\perp	上	\perp	上		\perp
< 0	\perp	Т	> 0	> 0	Τ	Т	> 0	T
= 0	\perp	< 0	= 0	> 0	≤ 0	<i>≠</i> 0	≥ 0	T
> 0	\perp	< 0	< 0	Т	< 0	Т	Т	T
<u>≤</u> 0	\perp	Т	≥ 0	> 0	Т	Т	≥ 0	T
<i>≠</i> 0	\perp	Т	<i>≠</i> 0	Т	Τ	Т	Т	Т
≥ 0	工	< 0	≤ 0	Т	≤ 0	Т	Т	T
Т		Т	Т	Т	Т	Т	Т	Т

Multiplication

*	1	< 0	= 0	> 0	≤ 0	= 0	≥ 0	Т
	T							
< 0	T	> 0						
= 0	1	= 0	= 0					
> 0		< 0	= 0	> 0				
<u>≤</u> 0		≥ 0	= 0	≤ 0	≥ 0			
<i>≠</i> 0	T	<i>≠</i> 0	= 0	<i>≠</i> 0	Т	<i>≠</i> 0		
≥ 0		≤ 0	= 0	≥ 0	≤ 0	Т	≥ 0	
Т	1	Т	= 0	Т	Т	Т	Т	Т

Division

/	1	< 0	= 0	> 0	≤ 0	= 0	≥ 0	Т
上	\perp	\perp	\perp	上	上	上		1
< 0	1	> 0	= 0	< 0	≥ 0	<i>≠</i> 0	≤ 0	Т
= 0	\perp		\perp	上				1
> 0	丄	< 0	= 0	> 0	≤ 0	≠ 0	≥ 0	Т
<u>≤</u> 0	T	> 0	= 0	< 0	≥ 0	<i>≠</i> 0	≤ 0	Т
<i>≠</i> 0		<i>≠</i> 0	= 0	<i>≠</i> 0	Т	<i>≠</i> 0	Т	Т
≥ 0		< 0	= 0	> 0	≤ 0	<i>≠</i> 0	≥ 0	Т
Т	Τ	<i>≠</i> 0	= 0	<i>≠</i> 0	Т	<i>≠</i> 0	Т	Т

$e_1=e_2$		< 0	= 0	> 0	≤ 0	= 0	≥ 0	Т
< 0	T	s [#]						
= 0	1	1	s [#]					
> 0	1	T	T	s [#]				
<u>≤</u> 0		s [#]	s [#]	1	s [#]			
<i>≠</i> 0	T	s [#]		s [#]	s [#]	s [#]		
≥ 0		1	s [#]					
Т	1	s [#]						

x = e	Τ	< 0	= 0	> 0	≤ 0	≠ 0	≥ 0	Т
\perp	T	1	Τ	Τ	1		1	
< 0	T	s#	Τ	Τ	$s^{\#}[x\mapsto <0]$	$s^{\#}[x \mapsto < 0]$	1	$s^{\#}[x\mapsto <0]$
= 0	\perp	\perp	s [#]	\perp	$s^{\#}[x \mapsto = 0]$	Τ	$s^{\#}[x \mapsto = 0]$	$s^{\#}[x\mapsto=0]$
> 0	\perp	\perp	1	s [#]	1	$s^{\#}[x\mapsto>0]$	$s^{\#}[x \mapsto > 0]$	$s^{\#}[x \mapsto > 0]$
≤ 0	\perp	s [#]	s [#]	1	s [#]	$s^{\#}[x\mapsto <0]$	$s^{\#}[x \mapsto = 0]$	$s^{\#}[x\mapsto\leq 0]$
$\neq 0$	\perp	s [#]	1	s [#]	$s^{\#}[x\mapsto <0]$	s [#]	$s^{\#}[x \mapsto > 0]$	$s^{\#}[x\mapsto\neq 0]$
≥ 0	\perp	1	s [#]	s [#]	$s^{\#}[x \mapsto = 0]$	$s^{\#}[x\mapsto>0]$	s [#]	$s^{\#}[x\mapsto\geq 0]$
Т	\perp	s [#]	s [#]	s [#]	s [#]	s [#]	s [#]	s [#]

$e_1 \neq e_2$	1	< 0	= 0	> 0	≤ 0	= 0	≥ 0	Т
< 0		s [#]						
= 0	1	s [#]	T					
> 0	1	s [#]	s [#]	s [#]				
<u>≤</u> 0	上	s [#]	s [#]	s [#]	s [#]			
<i>≠</i> 0		s [#]						
≥ 0	上	s [#]						
Т	1	s [#]						

$x \neq e$	1	< 0	= 0	> 0	<u>≤</u> 0	= 0	≥ 0	Т
1	1	Τ	1	1	1	1		1
< 0	T	s#	s#	s#	s#	s#	s#	s [#]
= 0		s [#]	Τ	s [#]	$s^{\#}[x\mapsto <0]$	s [#]	$s^{\#}[x\mapsto>0]$	$s^{\#}[x\mapsto\neq 0]$
> 0		s [#]	s [#]	s [#]		s [#]	s [#]	s [#]
≤ 0		s [#]	s [#]	s [#]	s [#]	s [#]	s [#]	s [#]
= 0	1	s [#]	s [#]	s [#]	s [#]	s [#]	s [#]	s [#]
≥ 0	1	s [#]	s [#]	s [#]	s [#]	s [#]	s [#]	s [#]
Τ	1	s [#]	s [#]	s [#]	s [#]	s [#]	s [#]	s [#]

$e_1 < e_2$		< 0	= 0	> 0	≤ 0	= 0	≥ 0	Τ
							T	
< 0	T	s [#]			s [#]	s [#]		s [#]
= 0	上	s [#]			s [#]	s [#]		s [#]
> 0	1	s [#]						
≤ 0		s [#]		T	s [#]	s [#]	T	s [#]
<i>≠</i> 0	T	s [#]						
≥ 0	上	s [#]						
Т	1	s [#]						

x < e	Τ	< 0	= 0	> 0	<u>≤</u> 0	≠ 0	≥ 0	Т
	Т	Τ	Τ	Τ	1		Τ	1
< 0	Т	s#	Т	Т	$s^{\#}[x\mapsto <0]$	$s^{\#}[x\mapsto < 0]$	Т	$s^{\#}[x\mapsto <0]$
= 0	Т	s [#]	1	1	$s^{\#}[x\mapsto <0]$	$s^{\#}[x\mapsto <0]$	1	$s^{\#}[x\mapsto <0]$
> 0	Т	s [#]	s [#]	s [#]	s [#]	s [#]	s [#]	s [#]
≤ 0	Т	s [#]	1	1	$s^{\#}[x\mapsto <0]$	$s^{\#}[x\mapsto <0]$	1	$s^{\#}[x\mapsto <0]$
= 0	Т	s [#]	s [#]	s [#]	s [#]	s [#]	s [#]	s [#]
≥ 0	1	s [#]	s [#]	s [#]	s [#]	s [#]	s [#]	s [#]
T	T	s [#]	s [#]	s [#]	s [#]	s [#]	s [#]	s [#]

$e_1 > e_2$		< 0	= 0	> 0	≤ 0	= 0	≥ 0	Т
	1		T			T	1	1
< 0	T	s [#]						
= 0	上		上	s [#]	上	s [#]	s [#]	s [#]
> 0	1	T	T	s [#]	T	s [#]	s [#]	s [#]
<u>≤</u> 0		s [#]						
<i>≠</i> 0	T	s [#]						
≥ 0		1	1	s [#]		s [#]	s [#]	s [#]
Τ	1	s [#]						

x > e	T	< 0	= 0	> 0	≤ 0	= 0	≥ 0	Т
\perp	T	Τ	Τ	Τ	Τ	1		
< 0	T	s#	s#	s#	s#	s#	s#	s#
= 0	1	1	Τ	s [#]	Τ	$s^{\#}[x \mapsto > 0]$	$s^{\#}[x \mapsto > 0]$	$s^{\#}[x \mapsto > 0]$
> 0	1	1	Τ	s [#]	Τ	$s^{\#}[x \mapsto > 0]$	$s^{\#}[x\mapsto>0]$	$s^{\#}[x \mapsto > 0]$
≤ 0	1	s [#]	s [#]	s [#]				
= 0	1	s [#]	s [#]	s [#]				
≥ 0	1	1	1	s [#]	1	$s^{\#}[x \mapsto > 0]$	$s^{\#}[x\mapsto>0]$	$s^{\#}[x \mapsto > 0]$
Τ	1	s [#]	s [#]	s [#]				

$e_1 \leq e_2$	T	< 0	= 0	> 0	≤ 0	= 0	≥ 0	Т
上	上		上	上	上	上		
< 0		s [#]			s [#]	s [#]	T	s [#]
= 0	1	s [#]	s [#]	T	s [#]	s [#]	s [#]	s [#]
> 0	1	s [#]						
<u>≤</u> 0	上	s [#]	s [#]	T	s [#]	s [#]	s [#]	s [#]
<i>≠</i> 0		s [#]						
≥ 0	上	s [#]						
Т	上	s [#]						

$x \leq e$	Τ	< 0	= 0	> 0	≤ 0	≠ 0	≥ 0	Τ
\perp	\perp	\perp	Τ	1	Τ	\perp	1	1
< 0	T	s#	T	Τ	$s^{\#}[x\mapsto <0]$	$s^{\#}[x\mapsto <0]$	1	$s^{\#}[x\mapsto <0]$
= 0	\perp	s [#]	s [#]	\perp	s [#]	$s^{\#}[x \mapsto < 0]$	$s^{\#}[x \mapsto = 0]$	$s^{\#}[x\mapsto\leq 0]$
> 0	\perp	s [#]	s [#]	s [#]	s [#]	s [#]	s [#]	s [#]
≤ 0	\perp	s [#]	s [#]	1	s [#]	$s^{\#}[x\mapsto <0]$	$s^{\#}[x \mapsto = 0]$	$s^{\#}[x\mapsto\leq 0]$
$\neq 0$	\perp	s [#]	s [#]	s [#]	s [#]	s [#]	s [#]	s [#]
≥ 0	Т	s [#]	s [#]	s [#]	s [#]	s [#]	s [#]	s [#]
Т	\perp	s [#]	s [#]	s [#]	s [#]	s [#]	s [#]	s [#]

$e_1 \geq e_2$	T	< 0	= 0	> 0	≤ 0	= 0	≥ 0	Т
	L		T				T	1
< 0	T	s [#]						
= 0	上		s [#]					
> 0	T	T	上	s [#]	上	s [#]	s [#]	s [#]
<u>≤</u> 0	上	s [#]						
<i>≠</i> 0	T	s [#]						
≥ 0	上	1	s [#]					
Τ	上	s [#]						

$x \ge e$	Τ	< 0	= 0	> 0	≤ 0	≠ 0	≥ 0	Т
	T	1	Τ	Τ	1		1	1
< 0	T	s#	s#	s#	s#	s#	s#	s [#]
= 0	Τ	\perp	s [#]	s [#]	$s^{\#}[x \mapsto = 0]$	$s^{\#}[x \mapsto > 0]$	s [#]	$s^{\#}[x\mapsto \geq 0]$
> 0	Τ	\perp	\perp	s [#]	1	$s^{\#}[x\mapsto>0]$	$s^{\#}[x \mapsto > 0]$	$s^{\#}[x\mapsto>0]$
≤ 0		s [#]	s [#]	s [#]	s [#]	s [#]	s [#]	s [#]
$\neq 0$	1	s [#]	s [#]	s [#]	s [#]	s [#]	s [#]	s [#]
≥ 0	Τ	1	s [#]	s [#]	$s^{\#}[x\mapsto=0]$	$s^{\#}[x \mapsto > 0]$	s [#]	$s^{\#}[x\mapsto\geq 0]$
Т	\perp	s [#]	s [#]	s [#]	s [#]	s [#]	s [#]	s [#]

Join

V	Τ	< 0	= 0	> 0	≤ 0	= 0	≥ 0	Т
	\perp							
< 0	< 0	< 0						
= 0	= 0	≤ 0	= 0					
> 0	> 0	≥ 0	≥ 0	> 0				
<u>≤</u> 0	≤ 0	≤ 0	≤ 0	Т	≤ 0			
= 0	<i>≠</i> 0	<i>≠</i> 0	Τ	<i>≠</i> 0	Т	<i>≠</i> 0		
≥ 0	≥ 0	Т	≥ 0	≥ 0	Т	Т	≥ 0	
Т	Т	Т	Т	Т	Т	Т	Т	Т

Join

V	1	$(-\infty,b]$	[a, b]	$[a,+\infty)$	Т
1	1	$(-\infty,b]$	[a, b]	$[a,+\infty)$	Т
$[-\infty,d]$	$(-\infty, d]$	$(-\infty, max(b, d)]$	$(-\infty, max(b, d)]$	\top	Т
[c, d]	[c, d]	$(-\infty, max(b, d)]$	[min(a,c), max(b,d)]	$[min(a,c),+\infty)$	Т
$[c,+\infty)$	$[c,+\infty)$	Т	$[min(a,c),+\infty)$	$[min(a,c),+\infty)$	Т
Т	Т	Т	Т	Τ	Т

Addition

+	1	$(-\infty,b]$	[a, b]	$[a,+\infty)$	T
	上				
$[-\infty,d]$	上	$(-\infty, b+d]$			
[c, d]	T	$(-\infty, b+d]$	[a+c,b+d]		
$[c,+\infty)$		Т	$[a+c,+\infty)$	$[a+c,+\infty)$	
Т	1	Т	Т	Т	T

Subtraction

_	1	$(-\infty,b]$	[a, b]	$[a,+\infty)$	T
	上				\perp
$(-\infty,d]$	T	Т	$[a-d,+\infty)$	$[a-d,+\infty)$	T
[c, d]	T	$(-\infty, b-c]$	[a-d,b-c]	$[a-d,+\infty)$	Т
$[c,+\infty)$		$(-\infty, b-c]$	$(-\infty, b-c]$	Т	T
Т	1	Т	Т	Т	T

Multiplication

*	1	$(-\infty, b]$		[a, b]		[a, +∞)	
1	I	1		1		Τ	
$(-\infty, d]$	Ι.	$b > 0 \lor d > 0$	Т	$(a < 0 \land b > 0) \lor (a > 0 \land b < 0)$ $(a \le 0 \land b \le 0) \land (a \ne 0 \lor b \ne 0)$	\top $[min(ad, bd), +\infty)$	d > 0 ∨ a < 0	Т
(-∞, a)	_	$b \le 0 \land d \le 0$	$[bd, +\infty)$	$(a \ge 0 \land b \ge 0) \land (a \ne 0 \lor b \ne 0)$ $(a = 0 \land b = 0)$	$(-\infty, max(ad, bd)]$ [0, 0]	$d \le 0 \land a \ge 0$	$(-\infty, ad]$
[c, d]	Τ	$ \begin{array}{l} (c < 0 \land d > 0) \lor (c > 0 \land d < 0) \\ (c \le 0 \land d \le 0) \land (c \ne 0 \lor d \ne 0) \\ (c \ge 0 \land d \ge 0) \land (c \ne 0 \lor d \ne 0) \\ (c \ge 0 \land d \ge 0) \land (c \ne 0 \lor d \ne 0) \\ (c = 0 \land d = 0) \end{array} $	T $[min(bc, bd), +\infty)$ $(-\infty, max(bc, bd)]$ $[0, 0]$	[min(ac, ad, bc, bd), max(ac, ad, bc	:, bd)]	$ \begin{array}{l} (c < 0 \land d > 0) \lor (c > 0 \land d < 0) \\ (c \le 0 \land d \le 0) \land (c \ne 0 \lor d \ne 0) \\ (c \ge 0 \land d \ge 0) \land (c \ne 0 \lor d \ne 0) \\ (c \ge 0 \land d \ge 0) \land (c \ne 0 \lor d \ne 0) \\ (c = 0 \land d = 0) \end{array} $	$(-\infty, max$ $[min(ac, a$ $[0, 0]$
[c, +∞)		$b > 0 \lor c < 0$	Т	$(a < 0 \land b > 0) \lor (a > 0 \land b < 0)$ $(a \le 0 \land b \le 0) \land (a \ne 0 \lor b \ne 0)$	$(-\infty, max(ac, bc)]$	a < 0 ∨ c < 0	Т
[5, +∞)	_	$b \le 0 \land c \ge 0$	$(-\infty,bc]$	$(a \ge 0 \land b \ge 0) \land (a \ne 0 \lor b \ne 0)$ $(a = 0 \land b = 0)$	$[min(ac, bc), +\infty)$ [0, 0]	$a \ge 0 \land c \ge 0$	$(-\infty,ac]$
Т	Τ	Т		$ \begin{aligned} a &= b = 0 \\ a &\neq 0 \lor b \neq 0 \end{aligned} $	[0, 0] T	Т	

Division

		17 0		II. o				-	_
/		$(-\infty, b]$		[a, b]		[a, +∞)		1	_
1	1	1		1		1		1	
		$d \le 0$	$[\min(0,b/d),+\infty)$	$d \le 0$ $d > 0 \land a = b = 0$	[min(0, a/d, b/d), max(0, a/d, b/d)] [0, 0]	$d \le 0$	$(-\infty, \max(a/d, 0)]$		
(-∞, d]	1	otherwise	Т	$d > 0 \land a \ge 0 \land b > 0$ $d > 0 \land a < 0 \land b \le 0$ otherwise	$(-\infty, max(a/d, b/d)]$ $[min(a/d, b/d), +\infty)$ \top	otherwise	Т	Т	
		c = d = 0 $0 < c \le d$	\perp $(-\infty, max(b/c, b/d)]$	c = d = 0	1	c = d = 0 $0 < c \le d$	$\lim_{min(a/c, a/d), +\infty)}^{\perp}$	c = d = 0	Ι
[c, d]	Τ.	$0 = c < d \land b \le 0$ $c \le d < 0$	$(-\infty, b/d]$ $[min(b/c, b/d), +\infty)$	c < 0 < d	$[\mathit{min}(0, a/c, b/c), \mathit{max}(0, a/c, b/c)] \vee [\mathit{min}(0, a/d, b/d), \mathit{max}(0, a/d, b/d)]$	$0 = c < d \land a \ge 0$ $c \le d < 0$	$[a/d, +\infty)$ $(-\infty, max(a/c, a/d)]$	otherwise	т
	1	otherwise	T	otherwise	[min(a/c, a/d, b/c, b/d), max(a/c, a/d, b/c, b/d)]	otherwise	T	l	
	Г	c ≥ 0	$(-\infty, \max(0, b/c)]$	$c \ge 0$ $c < 0 \land a = b = 0$	[min(0, a/c, b/c), max(0, a/c, b/c)] [0, 0]	$c \ge 0$	$[\mathit{min}(a/c,0),+\infty)$		ī
[c,+∞)	1	otherwise	Т	$c < 0 \land a \ge 0 \land b > 0$ $c < 0 \land a < 0 \land b \le 0$ otherwise	$[min(a/c, b/c), +\infty)$ $(-\infty, max(a/c, b/c)]$ \top	otherwise	Т	Т	
Т	Τ	Т		a = b = 0 otherwise	[0, 0] T	Т		T	

$e_1 = e_2$	Τ	$(-\infty,b]$	[a, b]	$[a, +\infty)$	Т
Τ	Т	Τ		1	1
$(-\infty, d]$	1	s [#]	if $a > d$ then \perp else $s^{\#}$	if $a > d$ then \perp else $s^{\#}$	s#
[c, d]	1	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#
$[c,+\infty)$	Т	if $b < c$ then \perp else $s^\#$	if $b < c$ then \perp else $s^\#$	s [#]	s#
Т	Τ	s [#]	s [#]	s [#]	s#

x = e	T	$(-\infty,b]$		[a, b]	
1	\perp	1			
		$b \le d$	s [#]	a > d	
$[-\infty,d]$	⊥	b > d	$s^{\#}[x\mapsto (-\infty,d]]$	$a \leq d \wedge b > d$	$s^{\#}[x \mapsto [a,d]]$
		<i>b ></i> u	3 · [x + 7 (∞, u]]	$a \leq d \wedge b \leq d$	<i>s</i> [#]
		b < c	\perp	$b < c \lor a > d$	Τ
	1	c < b < d	$s^{\#}[x \mapsto [c,b]]$	$b > d \wedge a < c$	$s^{\#}[x \mapsto [c,d]]$
[c,d]		$\perp \mid c \geq b \geq a$		$b > d \wedge a \geq c$	$s^{\#}[x \mapsto [a,d]]$
		b > d	$s^{\#}[x \mapsto [c,d]]$	$c \leq b \leq d \land a < c$	$s^{\#}[x \mapsto [c,b]]$
		<i>b ></i> u	5 [X + 7 [c, u]]	$c \leq b \leq d \land c \leq a \leq d$	s [#]
		b < c	\perp	b < c	
$[c,+\infty)$	_	b > c	$s^{\#}[x \mapsto [c,b]]$	$b \geq c \wedge a < c$	$s^{\#}[x \mapsto [c,b]]$
		_	5 [X + 7 [C, D]]	$a \ge c$	s [#]
Τ	上	s [#]		s [#]	

$e_1 \neq e_2$	1	$(-\infty,b]$	[a, b]	$[a,+\infty)$	Т
		1	1		
$(-\infty,d]$	上	s [#]	s [#]	s [#]	s [#]
[c,d]	上	s [#]	$a = b = c = d$ \perp otherwise $s^{\#}$	s [#]	s [#]
$[c,+\infty)$		s#	s#	s#	s#
Т	1	s [#]	s [#]	s [#]	s [#]

$x \neq e$	T	$(-\infty,b]$	[a, b]			
	T					
$(-\infty,d]$	1	$s^{\#}$	s [#]			
					$b = c = d$ $s^{\#}[x \mapsto (-\infty, b-1]]$	$a = c = d \wedge a \neq b$ $s^{\#}[x \mapsto [a+1,$
[c,d]		$b=c=d$ $s^{-1}[x\mapsto (-\infty,b-1]]$	$b = c = d \land a \neq b$ $s^{\#}[x \mapsto [a, b - b]$			
[c, a]		otherwise s [#]	$a = b = c = d$ \perp			
		otherwise 3"	otherwise $s^{\#}$			
$[c,+\infty)$	上	s [#]	s#			
Т	1	s [#]	s [#]			

$e_1 < e_2$		$[-\infty,b]$	[a, b]		$[a, +\infty]$)	Τ
	上	上	上				上
$(-\infty,d]$		s [#]	$a \ge d$		$a \ge d$		s#
$[-\infty, u]$		3"	a < d	$s^{\#}$	a < d	$s^\#$	3"
[c, d]		s [#]	$a \ge d$		$a \ge d$		s [#]
[c,d]			a < d	$s^{\#}$	a < d	$s^\#$	5"
$[c,+\infty)$	上	s [#]	s [#]		s [#]		s [#]
Т	上	s [#]	s [#]		s [#]		s [#]

<i>x</i> < <i>e</i>	\perp	$(-\infty,b]$	[a, b]	$[a,+\infty)$
1	1	<u></u>	<u>T</u>	
		$b \ge d$ $s^{\#}[x \mapsto (-\infty, d -$	1]] $a \ge d$ \perp	$a \ge d$ \perp
$[-\infty,d]$	1	$b < d s^{\#}$	$\begin{vmatrix} a \ge d & \pm \\ a < d \land b \ge d & s^{\#}[x \mapsto [a, d-1]] \\ a \le d \land b \le d & s^{\#} \end{vmatrix}$	2 < d s#[v \
		b < a - s	$a < d \land b < d s^{\#}$	a Cu 3 [A
		$b \ge d$ $s^{\#}[x \mapsto (-\infty, d -$		$a \ge d$ \perp
[c,d]	1	$b < d s^{\#}$	$a < d \wedge b \ge d$ $s^{\#}[x \mapsto [a, d-1]]$	$a < d s^{\#}[x \mapsto$
		b < u s	$a < d \land b < d s^{\#}$	a Cu 3 [A
$[c,+\infty)$	1	s [#]	s [#]	s#
Т	I	s [#]	s [#]	s#

$e_1 \leq e_2$	1	$(-\infty,b]$	[a, b]		$[a, +\infty]$)	Т
	上	上					
(~ d]		s#	a > d		a > d		s#
$[-\infty,d]$	—	3"	$a \leq d$	$s^\#$	$a \leq d$	$s^{\#}$	3"
[م م]		s [#]	a > d		a > d	上	s [#]
[c,d]		5"	$a \leq d$	$s^{\#}$	$a \leq d$	$s^{\#}$	5"
$[c,+\infty)$	上	s [#]	s [#]		s [#]		s [#]
Т	T	s [#]	s [#]		s [#]		s [#]

$x \leq e$	1	$(-\infty,b]$	[a, b]	$[a, +\infty)$	
1	1	上	<u></u>	1	
		$b>d$ $s^{\#}[x\mapsto (-\infty,d]]$	$a > d$ \perp	a > d ⊥	
$(-\infty,d]$	1	$b < d s^{\#}$	$\begin{vmatrix} a > d & \pm \\ a \le d \land b > d & s^{\#}[x \mapsto [a, d]] \\ a \le d \land b \le d & s^{\#} \end{vmatrix}$	$a < d s^{\#}[x \mapsto [a, d]]$	
		$b > d$ $s^{\#}[x \mapsto (-\infty, d]]$	$ a>d$ \perp	$\mid a > d \perp$	
[c, d]	_	$b \le d s^\#$	$\begin{vmatrix} a \le d \land b > d & s^{\#}[x \mapsto [a, d]] \\ a \le d \land b \le d & s^{\#} \end{vmatrix}$	$a \leq d$ $s^{\#}[x \mapsto [a, d]]$	
[- \		s#	a \le u \land b \le u \le s	s#	
$[c,+\infty)$		_	-	_	
Т	Ī	s [#]	s [#]	s [#]	

$e_1 > e_2$	T	$(-\infty,b]$	[a, b]	$[a,+\infty)$	Т
上	1	上	上		
$(-\infty,d]$	1	s [#]	s [#]	s [#]	s [#]
[c, d]	1	$b \le c \perp$	$b \le c \perp$	s#	s#
		$b>c$ $s^{\#}$	$b>c$ $s^{\#}$	3"	3"
$[c,+\infty)$	1	$b \le c \perp$	$b \le c \perp$	s#	s#
		$b>c$ $s^{\#}$	$b>c$ $s^{\#}$	3	3
Т		s [#]	s [#]	s [#]	s [#]

	-	/ /1	r 11	r , \	
x > e		$(-\infty,b]$	[a, b]	$[a,+\infty)$	
1	Ĺ	Т		1	
$(-\infty,d]$		s [#]	s#	s [#]	
[c, d]	1	$b \leq c$ \perp	$b \le c$ \perp	$a \le c$ $s^{\#}[x \mapsto [c +$	
		$b > c$ $s^{\#}[x \mapsto [c+1,b]]$	$b > c \land a \le c$ $s^{\#}[x \mapsto [c+1,b]]$	$a > c$ $s^{\#}$	
		2 × 5 5 [x. / [e + 1, b]]	$b>c \wedge a>c$ $s^{\#}$		
	1	$b \le c$ \perp	$b \le c$ \perp	$a \leq c$ $s^{\#}[x \mapsto [c + c]]$	
$[c,+\infty)$		\perp	$b > c$ $s^{\#}[x \mapsto [c+1,b]]$	$b > c \land a \le c$ $s^{\#}[x \mapsto [c+1,b]]$	$a>c$ $s^{\#}$
			D / C / a / C 3"		
Τ	Т	s [#]	s#	s [#]	

$e_1 \geq e_2$		$(-\infty,b]$	[a, b]	$[a,+\infty)$	Т
上	1	上	上		1
$(-\infty,d]$	1	s [#]	s [#]	s [#]	s#
[c, d]	1	$b < c \perp$	$b < c \perp$	s#	s#
		$b \geq c$ $s^{\#}$	$b \geq c$ $s^{\#}$	3"	3"
$[c,+\infty)$	1	$b < c \perp$	$b < c \perp$	s#	s#
		$b \geq c$ $s^{\#}$	$b \geq c s^{\#}$) 3	3"
Т	1	s [#]	s [#]	s [#]	s [#]

$x \ge e$	\perp	$(-\infty,b]$	[a, b]	$[a,+\infty)$
1	\perp	1	T	
$(-\infty,d]$	\perp	s [#]	$s^{\#}$	s [#]
		$b < c \perp$	$b < c$ \perp	$a < c$ $s^{\#}[x \vdash$
[c, d]		$b \geq c s^{\#}[x \mapsto [c,b]]$	$b \ge c \land a < c s^{\#}[x \mapsto [c,b]]$	$a \ge c$ $s^\#$
			$b \geq c \wedge a \geq c s^{\#}$	
		$b < c \perp$	$b < c$ \perp	$a < c$ $s^{\#}[x \vdash$
$[c,+\infty)$	上	$\left \begin{array}{c c} \bot & b \geq c & s^{\#}[x \mapsto [c,b]] \end{array}\right $	$b \ge c \land a < c s^{\#}[x \mapsto [c,b]]$	$a > c$ $s^{\#}$
			$D \geq C \land a \geq C S''$	<u> </u>
T	\perp	s [#]	$s^{\#}$	s [#]