Software Verification

Borsetto Riccardo 5th December 2022



Table of Contents



- 1 Language
- 2 Abstract Interpreter
- 3 List Functions
- 4 Extended Sign
- 5 Intervals
- 6 Examples

Language



```
Abinop \ni aop ::= + | - | * | \setminus

Aexp \ni e ::= x | n | -e | e_1 aop e_2

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

Bexp \ni b ::= true | false | e_1 bop e_2 | b_1 \wedge b_2 | b_1 \vee b_2 | \neg b

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

Table of Contents



- 1 Language
- 2 Abstract Interpreter
- 3 List Functions
- 4 Extended Sign
- 5 Intervals
- 6 Examples

Abstract Interpreter



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

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

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

$$AI(S_{1}; S_{2})(w)(s^{\sharp}) := (u^{\sharp}, invs_{1} +_{List(\mathbb{S})} invs_{2})$$

$$\text{with } (u^{\sharp}, invs_{2}) := AI(S_{2})(w)(t^{\sharp})$$

$$(t^{\sharp}, invs_{1}) := AI(S_{1})(w)(s^{\sharp})$$

$$AI(\mathbf{if } b \mathbf{ then } S_{1} \mathbf{ else } S_{2})(w)(s^{\sharp}) := (t^{\sharp} \vee_{\mathbb{S}} u^{\sharp}, invs_{1} +_{List(\mathbb{S})} invs_{2})$$

$$\text{with } (t^{\sharp}, invs_{1}) := (AI(S_{1})(w) \circ \mathcal{B}^{\sharp}(b))(s^{\sharp})$$

$$(u^{\sharp}, invs_{2}) := (AI(S_{2})(w) \circ \mathcal{B}^{\sharp}(\neg b))(s^{\sharp})$$

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

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

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



$$egin{align*} \mathcal{B}^{\sharp}: \mathbf{Bexp} &
ightarrow \mathbb{S}
ightarrow \mathbb{S} \ \mathcal{B}^{\sharp}(true)(s^{\sharp}) := s^{\sharp} \ \mathcal{B}^{\sharp}(false)(s^{\sharp}) := oldsymbol{eta}_{\mathbb{S}} \ \mathcal{B}^{\sharp}(e_{1} ext{ bop } e_{2})(s^{\sharp}) := FINIRE \ \mathcal{B}^{\sharp}(b_{1} \wedge b_{2})(s^{\sharp}) := (\mathcal{B}^{\sharp}(b_{2}) \circ \mathcal{B}^{\sharp}(b_{1}))(s^{\sharp}) \ \mathcal{B}^{\sharp}(b_{1} ee b_{2})(s^{\sharp}) := \mathcal{B}^{\sharp}(b_{1})(s^{\sharp}) ee_{\mathbb{S}} \mathcal{B}^{\sharp}(b_{2})(s^{\sharp}) \end{aligned}$$



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

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



$$\begin{split} \operatorname{wid}: (\mathbb{S} \to \mathbb{S} \times \operatorname{List}(\mathbb{S})) \to \operatorname{bool} \to \mathbb{S} \to \mathbb{S} \\ \operatorname{wid}(f)(b)(s^{\sharp})(t^{\sharp}) &:= \begin{cases} t^{\sharp} & \text{if is-inv}(f)(s^{\sharp})(t^{\sharp}) \\ \operatorname{wid}(f)(b)(s^{\sharp})(t^{\sharp} \; \nabla_{\mathbb{S}} \; u^{\sharp}) & \text{otherwise} \end{cases} \\ \operatorname{with} \; u^{\sharp} &:= \pi_{1}(\operatorname{step}(f)(b)(s^{\sharp})(t^{\sharp})) \end{split}$$

Narrowing



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

Abstract Least Fixed Point



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

Table of Contents



- 1 Language
- 2 Abstract Interpreter
- 3 List Functions
- 4 Extended Sign
- 5 Intervals
- 6 Examples

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

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

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



$$a_1 \leq_A a_2 := a_1 \vee_A a_2 = a_2$$

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

State Widening



$$s^{\sharp} \;
abla_{\mathbb{S}} \; t^{\sharp} := egin{cases} t^{\sharp} & ext{if } s^{\sharp} = ot_{\mathbb{S}} \ map(f_{t^{\sharp}})(s^{\sharp}) & ext{otherwise} \end{cases}$$
 with $f_{t^{\sharp}}(x,a) := (x,a \;
abla \; ext{lookup}(t^{\sharp})(x))$

State Narrowing



$$s^{\sharp} \; \Delta_{\mathbb{S}} \; t^{\sharp} := egin{cases} ot_{\mathbb{S}} & ext{if} \; s^{\sharp} = ot_{\mathbb{S}} \ map(f_{t^{\sharp}})(s^{\sharp}) & ext{otherwise} \end{cases}$$
 with $f_{t^{\sharp}}(x,a) := (x,a \; \Delta \; \mathsf{lookup}(t^{\sharp})(x))$

Table of Contents



- 1 Language
- 2 Abstract Interpreter
- 3 List Functions
- 4 Extended Sign
- 5 Intervals
- 6 Examples

Extended Sign



```
A := ExtSign
\mathbb{S} := List(String \times ExtSign) \cup \{\star\}
\perp_{\mathbb{S}} := \star
\top_{\mathbb{S}} := []
ExtSign \ni a ::= \bot | < 0 | = 0 | > 0 | \le 0 | \ne 0 | \ge 0 | \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



						$\neq 0$		
	\perp	> 0	= 0	< 0	≥ 0	$\neq 0$	≤ 0	T

Addition



+	\perp	< 0	= 0	> 0	≤ 0	= 0	≥ 0	Т
上	\perp							
< 0	T	< 0						
= 0	\perp	< 0	= 0					
> 0	\perp	T	> 0	> 0				
<u>≤</u> 0	丄	< 0	≤ 0	Т	≤ 0			
<i>≠</i> 0	丄	Т	$\neq 0$	Т	Т	Т		
≥ 0	工	Т	≥ 0	> 0	Т	Т	≥ 0	
T	\perp	Т	Т	Т	Т	Т	Т	Т

Subtraction



_		< 0	= 0	> 0	<u>≤</u> 0	= 0	≥ 0	Т
		T	L	L	L	T	L	L
< 0	\perp	T	> 0	> 0	Т	T	> 0	Т
= 0	上	< 0	= 0	> 0	<u>≤</u> 0	<i>≠</i> 0	≥ 0	Т
> 0	T	< 0	< 0	Т	< 0	T	Т	Т
<u>≤</u> 0		T	≥ 0	> 0	Т	T	≥ 0	T
<i>≠</i> 0		T	<i>≠</i> 0	Т	Т	Т	Т	T
≥ 0	上	< 0	≤ 0	Т	S 0	Т	Т	T
T	上	T	Т	Т	Т	Т	Т	Т

Multiplication



*		< 0	= 0	> 0	<u>≤</u> 0	= 0	≥ 0	T
上	上							
< 0		> 0						
= 0		= 0	= 0					
> 0	T	< 0	= 0	> 0				
<u>≤</u> 0		≥ 0	= 0	≤ 0	≥ 0			
<i>≠</i> 0		<i>≠</i> 0	= 0	<i>≠</i> 0	Т	<i>≠</i> 0		
≥ 0		≤ 0	= 0	≥ 0	S 0	Т	≥ 0	
Τ	上	Τ	= 0	Т	Т	Т	Т	Т

Division



/	1	< 0	= 0	> 0	≤ 0	= 0	≥ 0	Т
		T	T	T	T	T		L
< 0		> 0	= 0	< 0	≥ 0	<i>≠</i> 0	≤ 0	T
= 0	上					T		上
> 0		< 0	= 0	> 0	S 0	<i>≠</i> 0	≥ 0	T
<u>≤</u> 0		> 0	= 0	< 0	≥ 0	<i>≠</i> 0	≤ 0	T
<i>≠</i> 0		<i>≠</i> 0	= 0	$\neq 0$	Т	<i>≠</i> 0	T	T
≥ 0	上	< 0	= 0	> 0	S 0	<i>≠</i> 0	≥ 0	T
Τ	上	$\neq 0$	= 0	$\neq 0$	Т	$\neq 0$	Т	Т

Equal



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

Equal



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

Not Equal



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

Not Equal



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

Less Than



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

Less Than



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

Greater Than



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

Greater Than



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

Less Than or Equal



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

Less Than or Equal



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

Greater Than or Equal



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

Greater Than or Equal



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

Join



V		< 0	= 0	> 0	<u>≤</u> 0	= 0	≥ 0	Т
	上							
< 0	< 0	< 0						
= 0	= 0	<u>≤</u> 0	= 0					
> 0	> 0	≥ 0	≥ 0	> 0				
<u>≤</u> 0	≤ 0	≤ 0	≤ 0	Т	≤ 0			
= 0	<i>≠</i> 0	<i>≠</i> 0	Т	<i>≠</i> 0	Т	<i>≠</i> 0		
≥ 0	≥ 0	Т	≥ 0	≥ 0	T	Т	≥ 0	
Т	Т	Т	Т	Т	Т	Т	Т	Τ

Table of Contents



- 1 Language
- 2 Abstract Interpreter
- 3 List Functions
- 4 Extended Sign
- 5 Intervals
- 6 Examples

Intervals



```
\begin{split} 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{split}
```

α on Singletons



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

Opposite



_	上	$[-\infty,b]$	[a,b]	$[a,+\infty)$	T
		$[-b,+\infty)$	[-b, -a]	$(-\infty, -a]$	\top

Addition



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

Subtraction



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

Multiplication



+	Τ	(-∞, b)		[a, b]		[a, +∞)		T	
1	T	1		1		1		1	
(−∞, d]		$b > 0 \lor d > 0$	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 \lor a < 0	Т	-	
(-∞, u)	Ť	$b \leq 0 \land d \leq 0$	$[bd, +\infty)$	$(a \ge 0 \land b \ge 0) \land (a \ne 0 \lor b \ne 0)$ $(a = 0 \land b = 0)$	$(-\infty, max(ad, bd)]$ [0,0]	$d \le 0 \land a \ge 0$	$(-\infty, ad]$	'	
[c, d]	1	$(c < 0 \land d > 0) \lor (c > 0 \land d < 0)$ $(c \le 0 \land d \le 0) \land (c \ne 0 \lor d \ne 0)$ $(c \ge 0 \land d \ge 0) \land (c \ne 0 \lor d \ne 0)$ $(c \ge 0 \land d \ge 0) \land (c \ne 0 \lor d \ne 0)$ $(c = 0 \land d = 0)$	T $[min(bc, bd), +\infty)$ $(-\infty, max(bc, bd)]$ [0, 0]	[min(ac, ad, bc, bd), max(ac, ad, bc	, bd)]	$(c < 0 \land d > 0) \lor (c > 0 \land d < 0)$ $(c \le 0 \land d \le 0) \land (c \ne 0 \lor d \ne 0)$ $(c \ge 0 \land d \ge 0) \land (c \ne 0 \lor d \ne 0)$ $(c \ge 0 \land d \ge 0) \land (c \ne 0 \lor d \ne 0)$ $(c = 0 \land d = 0)$	$(-\infty, max(ac, ad)]$ $[min(ac, ad), +\infty)$ [0, 0]	c = d = 0 $c \neq 0 \lor d \neq 0$	[0,0] T
[c, +∞)	Ţ	$b > 0 \lor c < 0$	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	т	
	L	$b \le 0 \land c \ge 0$	$(-\infty, bc]$	$(a \ge 0 \land b \ge 0) \land (a \ne 0 \lor b \ne 0)$ $(a = 0 \land b = 0)$	$[min(ac, bc), +\infty)$ [0, 0]	$a \ge 0 \land c \ge 0$	(-∞, ac]		
Т	1	Т		a = b = 0 $a \neq 0 \lor b \neq 0$	[0,0] T	Т		Т	

Division



		17 - 15		17.0				_	
/	1	$(-\infty, b]$		[a, b]		$[a, +\infty)$		1	
1	1	1		1		1		1	
		d < 0	$[min(0, b/d), +\infty)$	d < 0	[min(0, b/d), max(0, a/d)]	d < 0	$(-\infty, max(a/d, 0)]$		
$(-\infty, d]$	1	d = 0	$(-\infty, b]/(-\infty, -1]$	d = 0	$[a, b]/(-\infty, -1]$	d = 0	$[a, +\infty)/(-\infty, -1]$	T	
		otherwise	T	otherwise	$[a, b]/(-\infty, -1] \vee [a, b]/[1, d]$	otherwise	T		
		c = d = 0	1	c = d = 0	1	c = d = 0	1		
İ		$0 < c \le d$	$(-\infty, max(b/c, b/d)]$	$0 < c \le d \lor c \le d < 0$	[min(a/c, a/d, b/c, b/d), max(a/c, a/d, b/c, b/d)]	$0 < c \le d$	$[min(a/c, a/d), +\infty)$	c = d = 0	\perp
[c, d]	١. ا	0 = c < d	$(-\infty, b]/[1, d]$	0 = c < d	[a, b]/[1, d]	0 = c < d	$[a, +\infty)/[1, d]$	İ	
[c,u]	-	$c \le d < 0$		c < d = 0	[a, b]/[c, -1]		$(-\infty, max(a/c, a/d)]$		
		c < d = 0	$(-\infty, b]/[c, -1]$	c < 0 < d	$[a, b]/[c, -1] \vee [a, b]/[1, d]$	c < d = 0	$[a, +\infty)/[c, -1]$	otherwise	Т
		otherwise	T	2 4 0 4 0	[a, b]/[c, -1] v [a, b]/[1, b]	otherwise	T		
		c > 0	$(-\infty, max(0, b/c)]$	c > 0	[min(0, a/c), max(0, b/c)]	c > 0	$[min(a/c, 0), +\infty)$		_
$[c, +\infty)$	1	c = 0	$(-\infty, b]/[1, +\infty)$	c = 0	$[a, b]/[1, +\infty)$	c = 0	$[a, +\infty)/[1, +\infty)$	T	
		otherwise	T	otherwise	$[a, b]/[c, -1] \vee [a, b]/[1, +\infty)$	otherwise	T		
T	1	Т		$[a, b]/(-\infty, -1] \vee [a, b]/$	$(1, +\infty)$	T		T	

Equal



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

Equal



x = e	Τ	$(-\infty, b]$		[a, b]		$[a, +\infty)$		Т
1	T	1		1		1		1
		$b \le d$	s#	a > d	1	a > d	1	
$(-\infty, d]$	1	b > d	$s^{\#}[x\mapsto (-\infty,d]]$	$a \le d \land b > d$ $a \le d \land b \le d$	$s^{\#}[x \mapsto [a, d]]$ $s^{\#}$	$a \le d$	$s^{\#}[x\mapsto [a,d]]$	$s^{\#}[x \mapsto (-\infty, d]]$
		b < c	Τ	$b < c \lor a > d$	Τ.	a > d	Τ	
[c, d]	_	$c \le b \le d$	$s^{\#}[x\mapsto [c,b]]$	$b > d \land a < c$ $b > d \land a \ge c$	$s^{\#}[x \mapsto [c, d]]$ $s^{\#}[x \mapsto [a, d]]$	a < c	$s^\#[x\mapsto [c,d]]$	$s^{\#}[x \mapsto [c, d]]$
		b > d	$s^\#[x\mapsto [c,d]]$	$c \le b \le d \land a < c$ $c \le b \le d \land c \le a \le d$	$s^{\#}[x \mapsto [c,b]]$ $s^{\#}$	$c \le a \le d$	$s^{\#}[x\mapsto [a,d]]$	
		b < c	1	b < c	1	a < c	$s^{\#}[x \mapsto [c, +\infty)]$	
$[c, +\infty)$	1	$b \ge c$	$s^{\#}[x\mapsto [c,b]]$	$b \ge c \land a < c$ $a \ge c$	$s^{\#}[x \mapsto [c, b]]$ $s^{\#}$	$a \ge c$	s#	$s^{\#}[x \mapsto [c, +\infty)]$
Т	Τ	s#		s [#]		s#		s [#]

Not Equal



$e_1 \neq e_2$	1	$(-\infty,b]$	[a, b]		$[a,+\infty)$	T
		上	1			
$[-\infty,d]$	T	s [#]	s [#]		s [#]	s [#]
[c, d]		s [#]	a = b = c = d otherwise	⊥ s [#]	s [#]	s [#]
$[c,+\infty)$	上	s [#]	s [#]		s [#]	s [#]
Τ	T	s [#]	s [#]		s [#]	s [#]

Not Equal



X	$\neq e$	Τ	$(-\infty, b]$	[a, b]	$[a, +\infty)$	Т
1	-	\perp	\perp	1	1	Τ.
(-	$-\infty, d$	Τ	s [#]	s#	s#	s#
[~ d]		$b=c=d$ $s^{\#}[x\mapsto (-\infty,b-1]]$	$a = c = d \land a \neq b s^{\#}[x \mapsto [a+1,b]]$ $b = c = d \land a \neq b s^{\#}[x \mapsto [a,b-1]]$	$a=c=d$ $s^{\#}[x\mapsto [a+1,+\infty)]$	c#
Į.	[c, d]		otherwise s#	$a = b = c = d$ \perp otherwise $s^{\#}$	otherwise s#	3
[0	$(0,+\infty)$	Τ	s [#]	s#	s#	s#
T		Τ	s [#]	s [#]	s [#]	s#

Less Than



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

Less Than



x < e	1	$(-\infty, b]$	[a, b]	$[a, +\infty)$	T
1	1	1	1	1	1
		$b \ge d$ $s^{\#}[x \mapsto (-\infty, d-1]]$		$a \ge d$ \perp	
$(-\infty, d]$	1	$b < d s^{\#}$	$\begin{vmatrix} a < d \land b \ge d & s^{\#}[x \mapsto [a, d-1]] \\ a < d \land b < d & s^{\#} \end{vmatrix}$	$a < d$ $s^{\#}[x \mapsto [a, d-1]]$	$s^{\#}[x \mapsto (-\infty, d-1]]$
		$b \ge d$ $s^{\#}[x \mapsto (-\infty, d-1]]$	$a \ge d$ \perp	$a \ge d$ \perp	
[c, d]	1	$b < d s^{\#}$	$ \begin{array}{ll} a < d \wedge b \geq d & s^{\#}[x \mapsto [a, d-1]] \\ a < d \wedge b < d & s^{\#} \end{array} $	$a < d s^{\#}[x \mapsto [a, d-1]]$	$s^{\#}[x \mapsto (-\infty, d-1]]$
$[c, +\infty)$	1	s#	s#	s#	s [#]
Т	1	s#	s [#]	s [#]	s#

Less Than or Equal



$e_1 \leq e_2$	上	$(-\infty,b]$	[a, b]		$[a, +\infty]$)	Т
	上	上	上				
$(-\infty,d]$		s [#]	a > d	\perp	a > d	\perp	s [#]
$(-\infty, u]$		3"	$a \leq d$	$s^{\#}$	$a \leq d$	$s^\#$	3"
[_ d]		s [#]	a > d	\perp	a > d	\perp	s [#]
[c,d]		5"	$a \leq d$	$s^\#$	$a \leq d$	$s^\#$	5"
$[c,+\infty)$		s [#]	s [#]		s [#]		s [#]
Т	上	s [#]	s [#]		s [#]		s [#]

Less Than or Equal



$x \le e$	Τ	$(-\infty, b]$	[a, b]	$[a, +\infty)$	Т
1	1	Τ	1	_	1
		$b > d$ $s^{\#}[x \mapsto (-\infty, d]]$	a > d ⊥	a > d ⊥	
$[-\infty, d]$	1	b < d s#	$a \le d \land b > d$ $s^{\#}[x \mapsto [a, d]]$	2 < d s#[v \sqrta [a d]]	$s^{\#}[x \mapsto (-\infty, d]]$
		. — .	$a \leq a \land b \leq a s$ "		
		$b > d$ $s^{\#}[x \mapsto (-\infty, d]]$	a > d ⊥	a > d ⊥	
[c, d]	1		$a \le d \land b > d$ $s^{\#}[x \mapsto [a, d]]$	$a \le d$ $s^{\#}[x \mapsto [a, d]]$	$s^{\#}[x \mapsto (-\infty, d]]$
			$a \le d \land b \le d$ $s^\#$		
$[c, +\infty)$	1		s#	s#	s#
Τ	\perp	s#	s#	s#	s#

Greater Than



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

Greater Than



x > e	1	$(-\infty, b]$	[a, b]	$[a, +\infty)$	Т
1	\perp	Т	1	Τ	1
$(-\infty, d]$	Τ.	s [#]	s#	s#	s [#]
		$b \le c \perp$	$b \le c$ \perp	$a \le c$ $s^{\#}[x \mapsto [c+1, +\infty)]$	
[c, d]	1	$b>c$ $s^{\#}[x\mapsto [c+1,b]]$	$\begin{array}{ll} b > c \wedge a \leq c & s^{\#}[x \mapsto [c+1,b]] \\ b > c \wedge a > c & s^{\#} \end{array}$	a > C 5"	$s^{\#}[x \mapsto [c+1,+\infty)]$
		$b \le c$ \perp	$b \le c$ \perp	$a \le c$ $s^{\#}[x \mapsto [c+1, +\infty)]$	
$[c, +\infty)$	1	$b > c$ $s^{\#}[x \mapsto [c+1,b]]$	$b > c \land a \le c s^{\#}[x \mapsto [c+1, b]]$ $b > c \land a > c s^{\#}$	$a>c$ $s^{\#}$	$s^{\#}[x \mapsto [c+1,+\infty)]$
Т	Τ	s#	s [#]	s#	s [#]

Greater Than or Equal



$e_1 \geq e_2$	1	$(-\infty,b]$	[a, b]	$[a,+\infty)$	Т
上		上	上		
$(-\infty,d]$		s [#]	s [#]	s [#]	s [#]
[c, d]		$b < c \perp$	$b < c \perp$	s [#]	s#
		$b \ge c s^\#$	$b \ge c$ $s^{\#}$	3"	3"
$[c,+\infty)$		$b < c \perp$	$b < c \perp$	s [#]	s#
		$b \ge c s^\#$	$b \ge c$ $s^{\#}$	3"	5"
Т	1	s [#]	s [#]	s [#]	s [#]

Greater Than or Equal



$x \ge e$	Τ	$(-\infty, b]$	[a, b]	$[a, +\infty)$	Т
1	Τ.	1	Τ	上	1
$[-\infty, d]$	1	s [#]	s [#]	s [#]	s [#]
		b < c ⊥	b < c ⊥	$a < c$ $s^{\#}[x \mapsto [c, +\infty)]$	
[c, d]	Τ	$b \ge c s^{\#}[x \mapsto [c, b]]$	$b \ge c \land a < c s^{\#}[x \mapsto [c, b]]$ $b \ge c \land a \ge c s^{\#}$	$a \ge c$ $s^\#$	$s^{\#}[x \mapsto [c, +\infty)]$
		b < c ⊥	b < c ⊥	$a < c$ $s^{\#}[x \mapsto [c, +\infty)]$	
$[c, +\infty)$	1	$b \ge c$ $s^{\#}[x \mapsto [c, b]]$	$b \ge c \land a < c s^{\#}[x \mapsto [c, b]]$ $b \ge c \land a \ge c s^{\#}$	$a \ge c$ $s^\#$	$s^{\#}[x \mapsto [c, +\infty)]$
Τ	1	s#	s#	s#	s#

Join



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

Widen



∇	1	$(-\infty,b]$		[a, b]		$[a, +\infty)$	T	
\perp		$(-\infty,b]$		[a, b]		$[a, +\infty)$		
(d]	$(-\infty, d]$	$d \leq b$	$(-\infty,b]$	$d \leq b$	$(-\infty,b]$	Т		_
$(-\infty, u]$	$(-\infty, u]$	otherwise	Т	otherwise	Т	'		'
		$d \le b$	$(-\infty,b]$	$a \le c \land d \le b$	[a, b]	a < c	$[a, +\infty)$	_
[c, d]	[c, d]	$u \leq b$	$[-\infty, b]$	$a \le c \land d > b$	$[a, +\infty)$	a <u>></u> c	$[a, +\infty)$	'
[c, a]	[c, u]	otherwise	_	$a > c \wedge d \leq b$	$(-\infty,b]$	otherwise	Т	_
		Other wise	'	otherwise	Τ	Other wise	'	'
$[c, +\infty)$	[c +\infty]	Т		$a \leq c$	$[a,+\infty)$	a ≤ c	$[a,+\infty)$	T T
[c,+∞)	[c, +∞)	'		otherwise	Т	otherwise	Т	'
Τ	Т	Т		Т		Т		T

Narrow



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

Table of Contents



- 1 Language
- 2 Abstract Interpreter
- 3 List Functions
- 4 Extended Sign
- 5 Intervals
- 6 Examples



$$P :=$$
 while $x \neq 0$ 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)]) = (\bot_{\mathbb{S}}, [[(x, > 0)]])$$



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

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



$$P := x := 40$$
; while $x \neq 0$ do $x := x - 1$
 $AI_{ExtSign}(P)(false)(\top_{\mathbb{S}}) = ([(x, = 0)], [\top_{\mathbb{S}}])$ in 1 iteration
 $AI_{Int}(P)(false)(\top_{\mathbb{S}}) = ([(x, [0, 0])], [[(x, [0, 40])]])$ in 40 iterations
 $AI_{Int}(P)(true)(\top_{\mathbb{S}}) = ([(x, [0, 0])], [[(x, (-\infty, 40])]])$ in $1 + 1$ iterations



```
\begin{split} P := & \text{ while } x \geq 0 \text{ do } (x := x - 1; y := y + 1) \\ & AI_{Int}(P)(false)([(x,[10,10]),(y,[0,0])]) \text{ loops} \\ & AI_{Int}(P)(true)([(x,[10,10]),(y,[0,0])]) = \\ & ([(x,[-1,-1]),(y,[0,+\infty))],[[(x,[-1,10]),(y,[0,+\infty))]]) \\ & \text{ in } 1 + 1 \text{ iterations} \end{split}
```



$$\begin{split} P := & \ \, \textbf{while} \,\, x < 10 \,\, \textbf{do} \,\, x := x + 1 \\ AI_{Int}(P)(false)([(x,[0,0])]) = \\ & \quad ([(x,[10,10])],[[(x,[0,10])]]) \,\, \text{in} \,\, 10 \,\, \text{iterations} \\ AI_{Int}(P)(true)([(x,[0,0])]) = \\ & \quad ([(x,[10,10])],[[(x,[0,10])]]) \,\, \text{in} \,\, 1 + 1 \,\, \text{iterations} \end{split}$$



```
\begin{split} P := & \text{ while } x \leq 100 \text{ do } x := x+1 \\ & AI_{Int}(P)(false)([(x,[1,1])]) = \\ & ([(x,[101,101])],[[(x,[1,101])]]) \text{ in } 101 \text{ iterations} \\ & AI_{Int}(P)(true)([(x,[1,1])]) = \\ & ([(x,[101,101])],[[(x,[1,101])]]) \text{ in } 1+1 \text{ iterations} \end{split}
```



```
P := x := 0; while x < 40 do x := x + 1

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

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



```
\begin{split} P := & \ x := 0; \\ & \ \text{while } 1 = 1 \text{ do} \\ & \ (\text{if } y = 0 \text{ then} \\ & \ (x := x + 1; \text{if } x < 40 \text{ then } x := 0 \text{ else skip}) \\ & \ \text{else skip}) \\ & Al_{Int}(P)(false)([(y,[0,1])]) = (\bot_{\mathbb{S}}, [[(x,[0,40])]]) \text{ in } 40 \text{ iterations} \\ & Al_{Int}(P)(true)([(y,[0,1])]) = (\bot_{\mathbb{S}}, [[(x,[0,+\infty))]]) \text{ in } 1 + 1 \text{ iterations} \end{split}
```



```
P := i := 1;
while i \le 3 do
(j := 1;
while j \le i do j := j + 1;
i := i + 1)
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])]])
```



```
P := i := 1:
        while i < 4 do
           (i := 0;
           while i < 3 do
                 (k := 0;
                 while k < 5 do (z := i * i * k; k := k + 1);
                 i := i + 1
           i := i + 1
AI_{Int}(P)(false)(\top_{\mathbb{S}}) = ([(i, [5, 5])], [..., [(i, [1, 5])]])
AI_{Int}(P)(true)(\top_{\mathbb{S}}) = ([(i, [5, 5])], [[(i, [1, 5])]])
```