Software Verification

Borsetto Riccardo

Univerisità degli Studi di Padova

5th December 2022

Join

V	上	< 0	= 0	> 0	<u>≤</u> 0	= 0	≥ 0	Т
1	上							
< 0	< 0	< 0						
= 0	= 0	≤ 0	= 0					
> 0	> 0	≥ 0	≥ 0	> 0				
<u>≤ 0</u>	≤ 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	Т	Т	≥ 0	
Т	Т	Т	Т	Т	Т	Т	Т	Т

Addition

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

Subtraction

_	\perp	< 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	≠ 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
1	上							
< 0	T	> 0						
= 0	1	= 0	= 0					
> 0	1	< 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

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

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

	>	0	_			<i>S</i> [₩]					
	\leq	0	1	s [#]	s [#]		s [#]				
	\neq	0	1	s [#]	T	s [#]	s [#]	s [#]			
Ì	\geq	0	上	T	s [#]	s [#]	s [#]	s [#]	s [#]		
Ì	Τ		上	s [#]	s [#]	s [#]	s [#]	s [#]	s [#]	s#	
•									•		_
x =	: e	\perp	< 0	=0	> 0	≤ 0		≠	0		≥ 0
L		\perp		1				1			
< 0	1	\perp	s [#]	1			→< 0		[x →<	< 0]	
= 0)	\perp	T	s [#]		s#[x	$\mapsto = 0$]			$s^{\#}[x \mapsto =$
> 0)	\perp			s [#]				$[x \mapsto >$	> 0]	$s^{\#}[x\mapsto>$
- 0		- 1	-#-	-#-		-#-		-//	- F	. 01	-# r

	\leq	0	1	s [#]	s [#]		s [#]					
	\neq	0		s [#]	丄	s [#]	s [#]	s [#]				
	\geq	0	1	T	s [#]							
Ī	Т			s [#]	s#							
_			*								_	
	_	-	< n	0	> 0	 0			<u> </u>			0
x =	е	上	< 0	=0	> 0	≤ 0		≠	U		\geq	U
\perp		\perp	上		上	上		_			\perp	
< 0		\perp	s [#]	1			→< 0		$[x \mapsto <$	< 0]	Τ	
= 0		\perp	1	s [#]	1	s#[x	$\mapsto = 0$]			s [#]	$[x \mapsto =$
> 0		T			s [#]			s [#]	$[x \mapsto >$	> 0]	s [#]	$[x \mapsto >$
≤ 0		\perp	s [#]	s [#]		s [#]			$[x \mapsto <$	< 0]		$[x \mapsto =$
≠ 0		\perp	s [#]	1	s [#]	s#[x	→< 0] s#			s [#]	$[x \mapsto >$
				- 77	177	11 -		- 17				

s[#]

s#

 \perp s# s[#]

s#

s#

 $s^{\#}[x \mapsto = 0] \quad s^{\#}[x \mapsto > 0]$

S# 5 + 1 = + 1

s[#]

s# ≥ 200

≥ 0 ⊤

	$e_1 \neq e_2$	T	< 0	= 0	> 0	≤ 0	<i>≠</i> 0	≥ 0	T
	\perp	\perp							
	< 0	\perp	s [#]						
	= 0	T	s [#]						
Ī	> 0	\perp	s [#]	s [#]	s [#]				
ĺ	≤ 0		s [#]	s [#]	s [#]	s [#]			
ſ	<i>≠</i> 0	上	s [#]						
ĺ	≥ 0	\perp	s [#]						
	Τ	1	s [#]						

					_	-					
	<	0		s [#]	s [#]	s [#]	s [#]				
	#	0		s [#]	s [#]	s [#]	s [#]	s [#]			
	2	0		s [#]	s [#]	s [#]	s [#]	s [#]	s [#]		
	Т		1	s [#]	s [#]	s [#]	s [#]	s [#]	s [#]	s [#]	
,											
$x \neq$	۱. م		~ 0	= 0	\ n	/ 0		/	0	Λ	
' '			< 0	— U	> 0	≤ 0		≠	$0 \mid \geq$	U	
1		<u> </u>		_ U	> 0 ⊥	<u>≥ 0</u>		 	<u>∪ </u>	U	
		<u></u>	< 0 ⊥ s [#]	$\frac{-0}{\perp}$ $s^{\#}$	> 0 ⊥ s [#]	<u></u>		<i>∓</i> ⊥ <i>s</i> [#]	I		
)	<u>+</u>		1		 	→< C			:	>
)	<u>+</u>	⊥ s [#]	1		 	→< C			$\frac{1}{2}[x \mapsto]$	>
 < 0 = 0))	<u>+</u>	⊥ s [#] s [#]		⊥ s [#] s [#]	$\frac{1}{s^{\#}}$ $s^{\#}[x]$	→< 0	$\begin{bmatrix} & & & & & & & & & & & & & & & & & & &$		$\frac{1}{2}[x \mapsto 2]$	>

-	. •		-	-	-	_				
7	0	上	s [#]	s [#]	s [#]	s [#]	s [#]			
2	0	1	s [#]	s [#]	s [#]	s [#]	s [#]	s [#]		
T	-	1	s [#]	s [#]	s [#]	s [#]	s [#]	s [#]	s [#]	
$x \neq e$	1	< 0	=0	> 0	≤ 0		\neq	0 ≥	0	
	1	1	1	Ι Τ	1					
< 0	1	s [#]	s [#]	s [#]	s [#]		s [#]	s [#]		
= 0	1	s [#]	1	s [#]	s#[x	$\rightarrow < 0$)] s#	s [#]	$[x \mapsto]$	>
> 0	1	s [#]	s [#]	s [#]	s [#]		s [#]	s [#]	:	
S 0	1	s [#]	s [#]	s [#]	s [#]		s#	s [#]		
≠ 0	1	s [#]	s [#]	s [#]	s [#]		s [#]	s [#]		

s[#]

s#

s[#]

s#

s[#]

s#

s[#]

s#

s[#]

s# 🍙

s[#]

s[#] ▶

s[#] s#[;

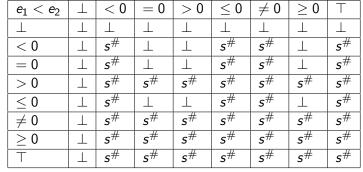
s# s# s[#]

s[#]

S#₀

0]

ŧ



	\leq	0	1	s [#]		上	s [#]	s [#]	1	s [#]	
	\neq	0	上	s [#]	s [#]	s [#]	s [#]	s [#]	s [#]	s [#]	
	\geq	0	上	s [#]	s [#]	s [#]	s [#]	s [#]	s [#]	s [#]]
	Т		上	s [#]	s [#]	s [#]	s [#]	s [#]	s [#]	s#	1
,			,						•		_
						1 . 0					` ^
<i>x</i> <	(e		< 0	=0	> 0	≤ 0		\neq	0		≥ 0
\perp		Т				1		1			\perp
< 0)	1	s [#]	T	1		$\rightarrow < 0$		$[x\mapsto <$		1
= 0)	丄	s [#]	T		s#[x	$\rightarrow < 0$)] s#	$[x\mapsto <$	(0]	
> C)	\perp	s [#]	s [#]	s [#]	s [#]		s [#]			$s^{\#}$
≤ 0)	Τ	s [#]	上	上		$\mapsto < 0$		$[x\mapsto <$	(0]	\perp
/ 0			-#-	-#-	-#-	-//					-#-

	\leq	0		S [₩]	\perp	<u></u>	s [∓]	$s^{\#}$		s [₩]	
Γ	\neq	0		s [#]	s [#]	s [#]	s [#]	s [#]	s [#]	s [#]	
	\geq	0		s [#]	s [#]	s [#]	s [#]	s [#]	s [#]	s [#]	
	Т		1	s [#]	s [#]	s [#]	s [#]	s [#]	s [#]	s [#]	
											_
		. 1			_						
x <	e		< 0	=0	> 0	≤ 0		≠	0		≥ 0
1		\perp	1	T	T	1					
< 0		\perp	s [#]	T	T	s#[x	→< 0] s#	$[x \mapsto <$		
= 0		\perp	s [#]	T	T		→< 0] s#	$[x \mapsto <$	[0]	
> 0		\perp	$s^{\#}$	s [#]	s [#]	s [#]		s#			s [#]
≤ 0		\perp	$s^{\#}$	1		s#[x	$\rightarrow < 0$] s#	$[x \mapsto <$	(0]	\perp
<i>≠</i> 0		\perp	$s^{\#}$	s [#]	s [#]	s [#]		s [#]			s [#]

s#

s#

s#

s#

s[#]

 $s^{\#}$

s[#]

s#

s[#]

s# 🗇 🕨

s#[; s#[; s# s#[;

s[#]

s[#]

~s#~

s[#]

s#_

$e_1 > e_2$	Т	< 0	= 0	> 0	S 0	<i>≠</i> 0	≥ 0	Т
\perp	上			上	\perp			\perp
< 0	上	s [#]	s [#]	s [#]	s [#]	$s^\#$	s [#]	s [#]
= 0	上			s [#]		$s^{\#}$	s [#]	s [#]
> 0	上	T		s [#]	T	s [#]	s [#]	s [#]
≤ 0	上	s [#]						
= 0	上	s [#]						
≥ 0	上	T	T	s [#]	T	s [#]	s [#]	s [#]
Т	上	s [#]	s [#]	s [#]	$s^{\#}$	s [#]	s [#]	s [#]

		-				•		_	•	•	
	<u> </u>	0	1	s [#]	s [#]	s [#]	s [#]	s [#]	s [#]	s [#]	
	\neq	0	上	s [#]	s [#]	s [#]	s [#]	s [#]	s [#]	s [#]	
	\geq	0	上	T	1	s [#]		s [#]	s [#]	s [#]	
	Т		1	s [#]	s [#]	s [#]	s [#]	s [#]	s [#]	s [#]	
x >	> e	1	< 0	= 0	> 0	≤ 0	<i>≠</i> 0		<u> </u>	0	
x >	» e	<u></u>	1	= 0 	> 0 	≤ 0 ⊥	≠ 0 ⊥		 		
x > 		<u></u>	< 0 ⊥ s [#]	= 0 ⊥ s [#]		≤ 0 ⊥ s [#]	≠ 0 ⊥ s [#]		$\begin{array}{c c} \geq & \\ \perp & \\ s^{\#} \end{array}$		
)		1	1	1	1		→> 0	$\begin{bmatrix} - \\ \bot \\ s^\# \\ 0 \end{bmatrix}$	[x →:	
)		1	1		1	⊥ s [#] s [#] [x		$\begin{bmatrix} - \\ \bot \\ s^\# \\ 0 \end{bmatrix}$	[x →:	> >
)	 	1	1	⊥ s [#] s [#]	1	⊥ s [#] s [#] [x		$\begin{bmatrix} - \\ \bot \\ s^\# \\ 0 \end{bmatrix}$	$[x \mapsto]$	> >

	U		5"	5"	5"	5	5	5"	5"	
\neq	0	1	s [#]							
\geq	0	1	1	T	s [#]	T	s [#]	s [#]	s [#]	
T		1	s [#]							
					•					
x > e	上	< 0	= 0	> 0	≤ 0	$\neq 0$		$ \geq$	0	
	1	1	T	1	1	1				
< 0	丄	s [#]		s [#]						
= 0	1		工	s [#]		s#[x	$\mapsto > 0$)] s#	$[x \mapsto]$	>
> 0	丄	1	上	s [#]	上	s#[x	$\mapsto > 0$)] s#	$[x \mapsto]$	>
≤ 0	1	s [#]		s [#]						
<i>≠</i> 0	上	s [#]		s [#]						

s[#]

s#

s#

s#

s#

s[#] s#[;

s[#]

s#[;

s#

0]

 $s^{\#}[x\mapsto>0] \quad s^{\#}[x\mapsto>0]$

s[#]

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

$x \le e$	\perp	< 0	= 0	> 0	≤ 0	$\neq 0$	≥ 0
\perp	\perp	\perp	\perp	\perp			\perp
< 0	\perp	s [#]	\perp	\perp	$s^{\#}[x\mapsto <0]$	$s^{\#}[x\mapsto <0]$	\perp
= 0	\perp	s [#]	s [#]		$s^{\#}$	$s^{\#}[x\mapsto <0]$	$s^{\#}[x \mapsto =$
> 0		s [#]	s [#]	s [#]	s [#]	s [#]	$s^{\#}$
≤ 0	\perp	s [#]	s [#]		s [#]	$s^{\#}[x\mapsto <0]$	$s^{\#}[x \mapsto =$
<i>≠</i> 0	\perp	s [#]	s [#]	s [#]	$s^{\#}$	s [#]	s [#]
≥ 0	\perp	s [#]	s [#]	s [#]	s [#]	s [#]	s [#]
Τ	\perp	s [#]	s [#]	s [#]	s#	s#	_S # _₹ 990

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

$x \ge e$	\perp	< 0	= 0	> 0	≤ 0	$ \neq 0$	≥ 0
	\perp	\perp	\perp	\perp			\perp
< 0	\perp	s [#]	s [#]	s [#]	$s^{\#}$	s [#]	$s^{\#}$
= 0	\perp		s [#]	s [#]	$s^{\#}[x\mapsto=0]$	$s^{\#}[x\mapsto>0]$	$s^{\#}$
> 0		T		s [#]		$s^{\#}[x\mapsto>0]$	$s^{\#}[x \mapsto >$
≤ 0	\perp	s [#]	s [#]	s [#]	s [#]	s [#]	$s^{\#}$
<i>≠</i> 0	\perp	s [#]	s [#]	s [#]	$s^{\#}$	s [#]	s [#]
≥ 0	\perp		s [#]	s [#]	$s^{\#}[x\mapsto=0]$	$s^{\#}[x\mapsto>0]$	s [#]
Т	丄	s [#]	s [#]	s [#]	s [#]	s#	<i>s</i> # ≥ ∞ < ○

Sample frame title

This is some text in the first frame. This is some text in the first frame. This is some text in the first frame.