Script **generated by TTT**

Title: Seidl: Programmoptimierung (18.11.2015)

Date: Wed Nov 18 10:19:07 CET 2015

Duration: 90:50 min

Pages: 45

To prove $(**)$, we show for every expression e :

$(***)$ $\quad ([\![e]\!]\,\rho) \;\Delta\; ([\![e]\!]^\sharp\,D) \quad$ whenever $\quad \rho \;\Delta\; D$

To prove $(***)$, we show for every operator $\Box$:

$$(x \,\Box\, y) \;\Delta\; (x^\sharp \,\Box^\sharp\, y^\sharp) \qquad \text{whenever} \quad x \;\Delta\; x^\sharp \wedge y \;\Delta\; y^\sharp$$

This precisely was how we have defined the operators $\Box^\sharp$.

Now, $(**)$ is proved by case distinction on the edge labels *lab* .

Let $s = (\rho, \mu) \;\Delta\; D$. In particular, $\bot \neq D \;:\; Vars \to \mathbb{Z}^\top$

Case $\boxed{x = e;}$:

S

$$\begin{array}{lll} \rho_1 & = & \rho \oplus \{x \mapsto [\![e]\!]\,\rho\} \qquad \mu_1 \;=\; \mu \\ D_1 & = & D \oplus \{x \mapsto [\![e]\!]^\sharp\,D\} \end{array}$$

S U T

$\Longrightarrow \qquad (\rho_1, \mu_1) \;\Delta\; D_1$

Case $\boxed{x = M[e];}$:

$$\begin{array}{lll} \rho_1 & = & \rho \oplus \{x \mapsto \mu\,([\![e]\!]^\sharp \rho)\} \qquad \mu_1 \;=\; \mu \\ D_1 & = & D \oplus \{x \mapsto \top\} \end{array}$$

$\Longrightarrow \qquad (\rho_1, \mu_1) \;\Delta\; D_1$

Case $\boxed{M[e_1] = e_2;}$:

$$\begin{array}{lll} \rho_1 & = & \rho \qquad \mu_1 \;=\; \mu \oplus \{[\![e_1]\!]^\sharp \rho \mapsto [\![e_2]\!]^\sharp \rho\} \\ D_1 & = & D \end{array}$$

$\Longrightarrow \qquad (\rho_1, \mu_1) \;\Delta\; D_1$

Case $\boxed{\mathrm{Neg}(e)}$: $(\rho_1, \mu_1) = s$ where:

$$
\begin{array}{lrcl}
 & 0 & = & [\![e]\!]\,\rho \\
 & & \Delta & [\![e]\!]^\sharp\, D \\
\Longrightarrow & 0 & \sqsubseteq & [\![e]\!]^\sharp\, D \\
\Longrightarrow & \bot & \neq & D_1 \;=\; D \\
\Longrightarrow & \multicolumn{3}{l}{(\rho_1, \mu_1)\ \Delta\ D_1}
\end{array}
$$

Case $\boxed{\mathrm{Pos}(e)}$: $(\rho_1, \mu_1) = s$ where:

$$
\begin{array}{lrcl}
 & 0 & \neq & [\![e]\!]\,\rho \\
 & & \Delta & [\![e]\!]^\sharp\, D \\
\Longrightarrow & 0 & \neq & [\![e]\!]^\sharp\, D \\
\Longrightarrow & \bot & \neq & D_1 \;=\; D \\
\Longrightarrow & \multicolumn{3}{l}{(\rho_1, \mu_1)\ \Delta\ D_1}
\end{array}
$$

To prove $(*)$, we show for every edge k :

$$
(**) \qquad
\begin{tikzcd}
s \arrow[r, "{[\![k]\!]}"] \arrow[d, dash, "\Delta"'] & s_1 \arrow[d, dash, dotted, "\Delta"] \\
D \arrow[r, "{[\![k]\!]^\sharp}"'] & D_1
\end{tikzcd}
$$

Then $(*)$ follows by induction.

We show:

$(*)$ If $s\ \Delta\ D$ and $[\![\pi]\!]\, s$ is defined, then:

$$([\![\pi]\!]\, s)\ \ \Delta\ \ ([\![\pi]\!]^\sharp\, D)$$

$$
\begin{tikzcd}
s \arrow[r, "{[\![\pi]\!]}"] \arrow[d, dash, "\Delta"'] & s_1 \arrow[d, dash, dotted, "\Delta"] \\
D \arrow[r, "{[\![\pi]\!]^\sharp}"'] & D_1
\end{tikzcd}
$$

We conclude:

The assertion $(*)$ is true.

The MOP-Solution:

$$\mathcal{D}^*[v] = \bigsqcup\{[\![\pi]\!]^\sharp\, D_\top \mid \pi : start \to^* v\}$$

where $D_\top\, x = \top \qquad (x \in Vars)$.

We conclude:

The assertion $(*)$ is true.

The MOP-Solution:

$$\mathcal{D}^*[v] = \bigsqcup\{[\![\pi]\!]^\sharp\, D_\top \mid \pi : start \to^* v\}$$

where $D_\top\, x = \top \qquad (x \in Vars)$.

By $(*)$, we have for all initial states s and all program executions π which reach v :

$$([\![\pi]\!]\, s) \;\Delta\; (\mathcal{D}^*[v])$$

$x \mapsto 5$

We conclude:

The assertion $(*)$ is true.

The MOP-Solution

$$\mathcal{D}^*[v] = \bigsqcup\{[\![\pi]\!]^\sharp\, D_\top \mid \pi : start \to^* v\}$$

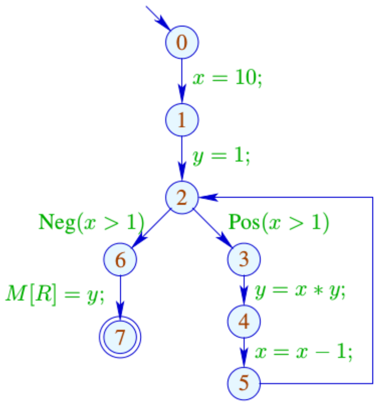
where $D_\top\, x = \top \qquad (x \in Vars)$.

By $(*)$, we have for all initial states s and all program executions π which reach v :

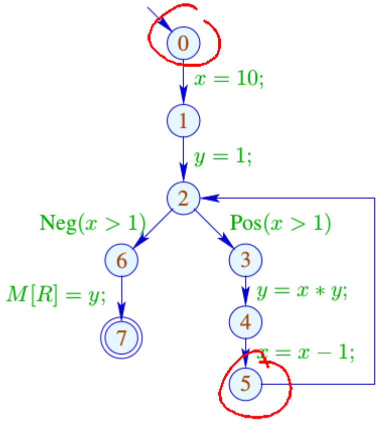
$$([\![\pi]\!]\, s) \;\Delta\; (\mathcal{D}^*[v]) \;\sqsubseteq\; \mathcal{D}[v]$$

In order to approximate the MOP, we use our constraint system ...

Example



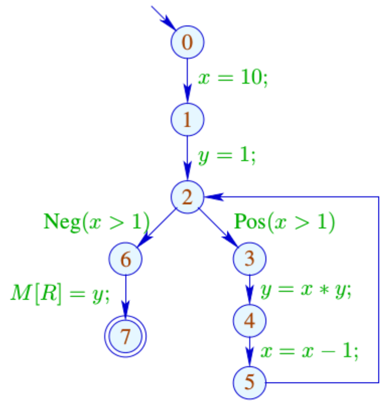
Example



$\perp$

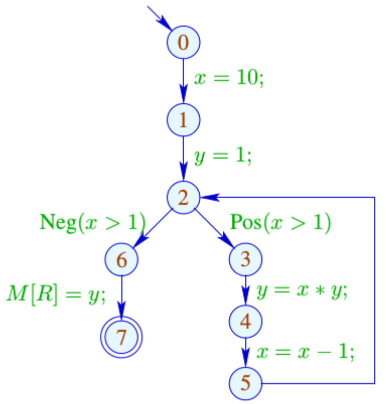
	1	
	x	y
0	$\top$	$\top$
1	10	$\top$
2	10	1
3	10	1
4	10	10
5	9	10
6	$\perp$	
7	$\perp$	

Example



	1		2	
	x	y	x	y
0	$\top$	$\top$	$\top$	$\top$
1	10	$\top$	10	$\top$
2	10	1	$\top$	$\top$
3	10	1	$\top$	$\top$
4	10	10	$\top$	$\top$
5	9	10	$\top$	$\top$
6	$\perp$		$\top$	$\top$
7	$\perp$		$\top$	$\top$

Example



	1		2		3	
	x	y	x	y	x	y
0	$\top$	$\top$	$\top$	$\top$		
1	10	$\top$	10	$\top$		
2	10	1	$\top$	$\top$		
3	10	1	$\top$	$\top$		
4	10	10	$\top$	$\top$	ditto	
5	9	10	$\top$	$\top$		
6	$\perp$		$\top$	$\top$		
7	$\perp$		$\top$	$\top$		

Conclusion

Although we compute with concrete values, we fail to compute everything ...

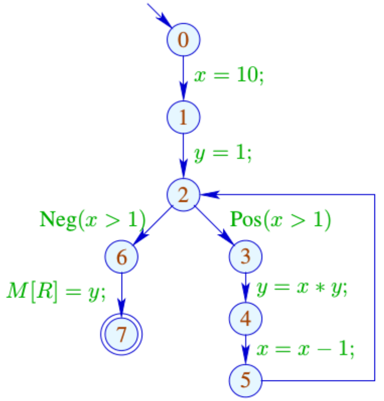
The fixpoint iteration, at least, is guaranteed to terminate:

For n program points and m variables, we maximally need: $n \cdot (m + 1)$ rounds.

Caveat

The effects of edge are not distributive !!!

Example



	1		2		3	
	x	y	x	y	x	y
0	$\top$	$\top$	$\top$	$\top$		
1	10	$\top$	10	$\top$		
2	10	1	$\top$	$\top$		
3	10	1	$\top$	$\top$		
4	10	10	$\top$	$\top$	ditto	
5	9	10	$\top$	$\top$		
6	$\bot$		$\top$	$\top$		
7	$\bot$		$\top$	$\top$		

Conclusion

Although we compute with concrete values, we fail to compute everything ...

The fixpoint iteration, at least, is guaranteed to terminate:

For n program points and m variables, we maximally need: $n \cdot (m+1)$ rounds.

Caveat

The effects of edge are not distributive !!!

Counter Example: $f = [\![x = x + y;]\!]^\sharp$

$$\begin{array}{llll}
\text{Let} & D_1 & = & \{x \mapsto 2, y \mapsto 3\} \\
 & D_2 & = & \{x \mapsto 3, y \mapsto 2\} \\
\text{Dann} & f\, D_1 \sqcup f\, D_2 & = & \{x \mapsto 5, y \mapsto 3\} \sqcup \{x \mapsto 5, y \mapsto 2\} \\
 & & = & \{x \mapsto 5, y \mapsto \top\} \\
 & & \neq & \{x \mapsto \top, y \mapsto \top\} \\
 & & = & f\, \{x \mapsto \top, y \mapsto \top\} \\
 & & = & f\, (D_1 \sqcup D_2)
\end{array}$$

We conclude:

The least solution $\mathcal{D}$ of the constraint system in general yields only an upper approximation of the MOP, i.e.,

$$\mathcal{D}^*[v] \quad \sqsubseteq \quad \mathcal{D}[v]$$

We conclude:

The least solution $\mathcal{D}$ of the constraint system in general yields only an upper approximation of the MOP, i.e.,

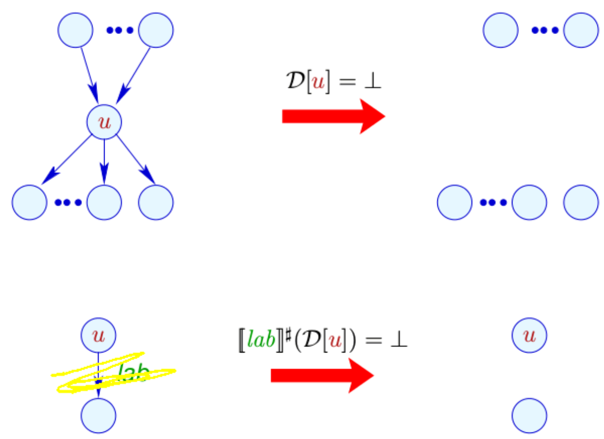
$$\mathcal{D}^*[v] \quad \sqsubseteq \quad \mathcal{D}[v]$$

As an upper approximation, $\mathcal{D}[v]$ nonetheless describes the result of every program execution π which reaches v :

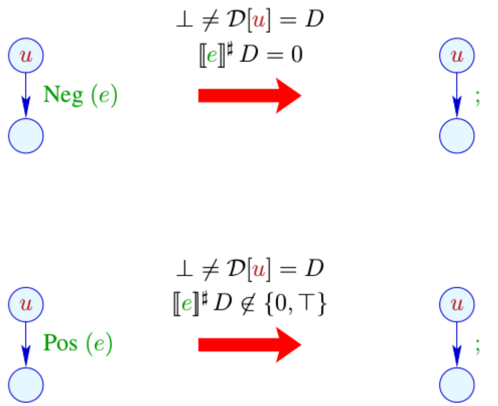
$$(\llbracket \pi \rrbracket\, (\rho, \mu)) \;\; \Delta \;\; (\mathcal{D}[v])$$

whenever $\llbracket \pi \rrbracket\, (\rho, \mu)$ is defined.

Transformation 4: Removal of Dead Code



Transformation 4 (cont.): Removal of Dead Code



Extensions

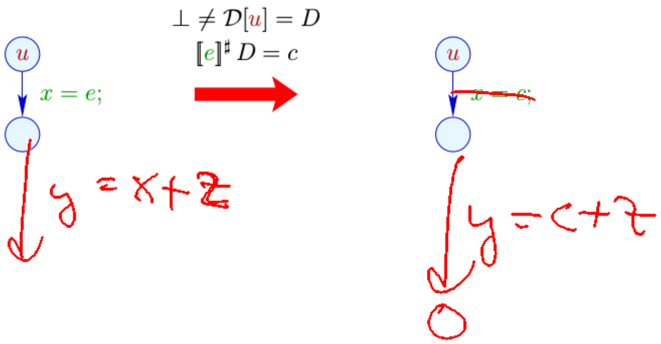
- Instead of complete right-hand sides, also subexpressions could be simplified:

$$x + (3 * y) \quad \xRightarrow{\{x \mapsto \top, y \mapsto 5\}} \quad x + 15$$

... and further simplifications be applied, e.g.:

$$\begin{array}{rcl} x * 0 & \Longrightarrow & 0 \\ x * 1 & \Longrightarrow & x \\ x + 0 & \Longrightarrow & x \\ x - 0 & \Longrightarrow & x \\ & \dots & \end{array}$$

Transformation 4 (cont.): Simplified Expressions



Extensions

- Instead of complete right-hand sides, also subexpressions could be simplified:

$$x + (3 * y) \xRightarrow{\{x \mapsto \top, y \mapsto 5\}} x + 15$$

... and further simplifications be applied, e.g.:

$$\begin{array}{rcl} x * 0 & \Longrightarrow & 0 \\ x * 1 & \Longrightarrow & x \\ x + 0 & \Longrightarrow & x \\ x - 0 & \Longrightarrow & x \\ & \ldots & \end{array}$$

Extensions

- Instead of complete right-hand sides, also subexpressions could be simplified:

$$x + (3 * y) \xRightarrow{\{x \mapsto \top, y \mapsto 5\}} x + 15$$

... and further simplifications be applied, e.g.:

$$\begin{array}{rcl} x * 0 & \Longrightarrow & 0 \\ x * 1 & \Longrightarrow & x \\ x + 0 & \Longrightarrow & x \\ x - 0 & \Longrightarrow & x \\ & \ldots & \end{array}$$

- So far, the information of conditions has not yet be optimally exploited:

$$\text{if } (x == 7)$$
$$y = x + 3;$$

Even if the value of x before the if statement is unknown, we at least know that x definitely has the value 7 — whenever the then-part is entered.

Therefore, we can define:

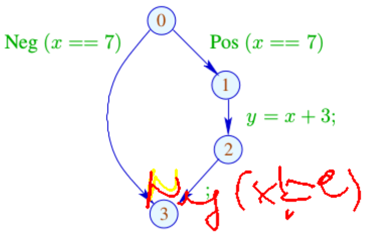
$$[\![\text{Pos}\,(x == e)]\!]^\sharp\, D = \begin{cases} D & \text{if} \quad [\![x == e]\!]^\sharp\, D = 1 \\ \perp & \text{if} \quad [\![x == e]\!]^\sharp\, D = 0 \\ D_1 & \text{otherwise} \end{cases}$$

where

$$D_1 = D \oplus \{x \mapsto (D\, x \sqcap [\![e]\!]^\sharp\, D)\}$$

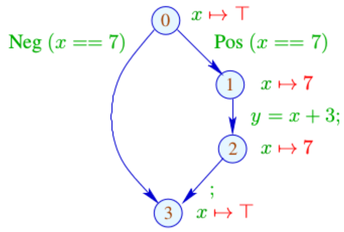
The effect of an edge labeled $\text{Neg}\,(x \neq e)$ is analogous.

Our Example



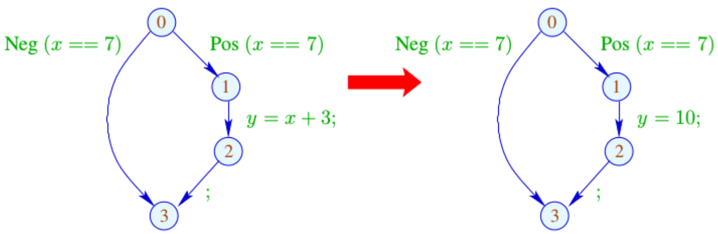
The effect of an edge labeled $\text{Neg}\,(x \neq e)$ is analogous.

Our Example



The effect of an edge labeled $\text{Neg}\,(x \neq e)$ is analogous.

Our Example



1.5 Interval Analysis

Observation

- Programmers often use global constants for switching debugging code on/off.

  $\Longrightarrow$

  Constant propagation is useful !

- In general, precise values of variables will be unknown — perhaps, however, a tight interval !!!

Example

for $(i = 0; i < 42; i++)$

~~if~~ $\cancel{(0 \leq i \wedge i < 42)}$ {

$A_1 = A + i;$

$M[A_1] = i;$

}

// A start address of an array

// if the array-bound check

The inner check is superfluous.

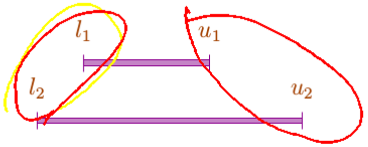
Idea 1

Determine for every variable x an (as tight as possible) interval of possible values:

$$\mathbb{I} = \{[l, u] \mid l \in \mathbb{Z} \cup \{-\infty\}, u \in \mathbb{Z} \cup \{+\infty\}, l \leq u\}$$

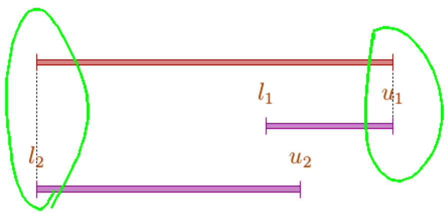
Partial Ordering: $[-\infty, +\infty]$

$$[l_1, u_1] \sqsubseteq [l_2, u_2] \quad \text{iff} \quad l_2 \leq l_1 \wedge u_1 \leq u_2$$



Thus:

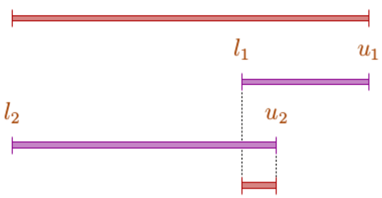
$$[l_1, u_1] \sqcup [l_2, u_2] \quad = \quad [l_1 \sqcap l_2, u_1 \sqcup u_2]$$



Thus:

$$[l_1, u_1] \sqcup [l_2, u_2] \quad = \quad [l_1 \sqcap l_2, u_1 \sqcup u_2]$$

$$[l_1, u_1] \sqcap [l_2, u_2] \quad = \quad [l_1 \sqcup l_2, u_1 \sqcap u_2]$$ whenever $(l_1 \sqcup l_2) \leq (u_1 \sqcap u_2)$



Caveat

→ $\mathbb{I}$ is not a complete lattice !

→ $\mathbb{I}$ has infinite ascending chains, e.g.,

$$[0,0] \sqsubset [0,1] \sqsubset [-1,1] \sqsubset [-1,2] \sqsubset \dots$$

Description Relation:

$$z \,\Delta\, [l,u] \qquad \text{iff} \qquad l \leq z \leq u$$

Concretization:

$$\gamma\,[l,u] = \{z \in \mathbb{Z} \mid l \leq z \leq u\}$$

Caveat

→ $\mathbb{I}$ is not a complete lattice !

→ $\mathbb{I}$ has infinite ascending chains, e.g.,

$$[0,0] \sqsubset [0,1] \sqsubset [-1,1] \sqsubset [-1,2] \sqsubset \dots$$

Caveat

→ $\mathbb{I}$ is not a complete lattice !

→ $\mathbb{I}$ has infinite ascending chains, e.g.,

$$[0,0] \sqsubset [0,1] \sqsubset [-1,1] \sqsubset [-1,2] \sqsubset \dots$$

[1, 17]

Description Relation:

$$z \,\Delta\, [l,u] \qquad \text{iff} \qquad l \leq z \leq u$$

Concretization:

$$\gamma\,[l,u] = \{z \in \mathbb{Z} \mid l \leq z \leq u\}$$

Example

$$\begin{array}{rcl} \gamma\,[0,7] & = & \{0,\dots,7\} \\ \gamma\,[0,\infty] & = & \{0,1,2,\dots,\} \end{array}$$

Computing with intervals: Interval Arithmetic

Addition:

$$\begin{array}{rcll} [l_1,u_1] +^\sharp [l_2,u_2] & = & [l_1+l_2, u_1+u_2] & \text{where} \\ -\infty + \_ & = & -\infty & \\ +\infty + \_ & = & +\infty & \\ // & & -\infty + \infty & \text{cannot occur !} \end{array}$$

Negation:

$$-^\sharp [l, u] \quad = \quad [-u, -l]$$

Multiplication:

$$\begin{array}{rcl} [l_1, u_1] \,*^\sharp\, [l_2, u_2] & = & [a, b] \qquad \text{where} \\ a & = & l_1 l_2 \sqcap l_1 u_2 \sqcap u_1 l_2 \sqcap u_1 u_2 \\ b & = & l_1 l_2 \sqcup l_1 u_2 \sqcup u_1 l_2 \sqcup u_1 u_2 \end{array}$$

Example

$$\begin{array}{rcl} [0, 2] \,*^\sharp\, [3, 4] & = & [0, 8] \\ [-1, 2] \,*^\sharp\, [3, 4] & = & [-4, 8] \\ [-1, 2] \,*^\sharp\, [-3, 4] & = & [-6, 8] \\ [-1, 2] \,*^\sharp\, [-4, -3] & = & [-8, 4] \end{array}$$

Division: $\quad [l_1, u_1] \,/^\sharp\, [l_2, u_2] \;=\; [a, b]$

- If 0 is not contained in the interval of the denominator, then:

$$\begin{array}{rcl} a & = & l_1/l_2 \sqcap l_1/u_2 \sqcap u_1/l_2 \sqcap u_1/u_2 \\ b & = & l_1/l_2 \sqcup l_1/u_2 \sqcup u_1/l_2 \sqcup u_1/u_2 \end{array}$$

- If: $l_2 \leq 0 \leq u_2$, we define:

$$[a, b] \;=\; [-\infty, +\infty]$$

$$[a, b] = [l_1, u_1] \,/^\sharp\, [l_2, -1] \;\sqcup\; [l_1, u_1] \,/^\sharp\, [1, u_2]$$

Equality:

$$[l_1, u_1] ==^\sharp [l_2, u_2] \;=\; \begin{cases} [1, 1] & \text{if } l_1 = u_1 = l_2 = u_2 \\ [0, 0] & \text{if } u_1 < l_2 \vee u_2 < l_1 \\ [0, 1] & \text{otherwise} \end{cases}$$

$$[1, 2] ==^\sharp [3, 2]$$
$$= [0, 1]$$

Equality:

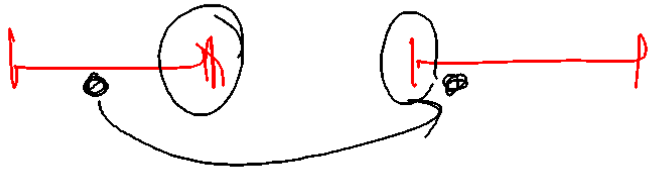
$$[l_1, u_1] ==^\sharp [l_2, u_2] \;=\; \begin{cases} [1, 1] & \text{if } l_1 = u_1 = l_2 = u_2 \\ [0, 0] & \text{if } u_1 < l_2 \vee u_2 < l_1 \\ [0, 1] & \text{otherwise} \end{cases}$$

Example

$$\begin{array}{rcl} [42, 42] ==^\sharp [42, 42] & = & [1, 1] \\ [0, 7] ==^\sharp [0, 7] & = & [0, 1] \\ [1, 2] ==^\sharp [3, 4] & = & [0, 0] \end{array}$$

Less:

$$[l_1, u_1] <^\sharp [l_2, u_2] = \begin{cases} [1,1] & \text{if} \quad u_1 < l_2 \\ [0,0] & \text{if} \quad u_2 \leq l_1 \\ [0,1] & \text{otherwise} \end{cases}$$



Less:

$$[l_1, u_1] <^\sharp [l_2, u_2] = \begin{cases} [1,1] & \text{if} \quad u_1 < l_2 \\ [0,0] & \text{if} \quad u_2 \leq l_1 \\ [0,1] & \text{otherwise} \end{cases}$$

Example

$$[1,2] <^\sharp [9,42] = [1,1]$$
$$[0,7] <^\sharp [0,7] = [0,1]$$
$$[3,4] <^\sharp [1,2] = [0,0]$$