The abstract effects of edges $[\![k]\!]^\sharp$ are again composed to the effects of paths $\pi = k_1 \ldots k_r$ by:

$$[\![\pi]\!]^\sharp = [\![k_r]\!]^\sharp \circ \ldots \circ [\![k_1]\!]^\sharp \quad : \mathbb{D} \to \mathbb{D}$$

Idea for Correctness: Abstract Interpretation

Cousot, Cousot 1977

Establish a description relation Δ between theconcrete values and their descriptions with:

$$x \,\Delta\, a_1 \quad \wedge \quad a_1 \sqsubseteq a_2 \quad \Longrightarrow \quad x \,\Delta\, a_2$$

Concretization: $\gamma\, a = \{x \mid x \,\Delta\, a\}$

// returns the set of described values :-)

(1) Values: $\Delta \subseteq \mathbb{Z} \times \mathbb{Z}^{\top}$

$$z \,\Delta\, a \quad \text{iff} \quad z = a \vee a = \top$$

Concretization:

$$\gamma\, a = \begin{cases} \{a\} & \text{if} \quad a \sqsubset \top \\ \mathbb{Z} & \text{if} \quad a = \top \end{cases}$$

(1) Values: $\Delta \subseteq \mathbb{Z} \times \mathbb{Z}^\top$

$$z \,\Delta\, a \quad \text{iff} \quad z = a \vee a = \top$$

Concretization:

$$\gamma\, a = \begin{cases} \{a\} & \text{if} \quad a \sqsubset \top \\ \mathbb{Z} & \text{if} \quad a = \top \end{cases}$$

(2) Variable Assignments: $\Delta \subseteq (\mathit{Vars} \to \mathbb{Z}) \times (\mathit{Vars} \to \mathbb{Z}^\top)_\perp$

$$\rho \,\Delta\, D \quad \text{iff} \quad D \neq \perp \;\wedge\; \rho\, x \sqsubseteq D\, x \quad (x \in \mathit{Vars})$$

Concretization:

$$\gamma\, D = \begin{cases} \emptyset & \text{if} \quad D = \perp \\ \{\rho \mid \forall\, x :\; (\rho\, x) \,\Delta\, (D\, x)\} & \text{otherwise} \end{cases}$$

Example: $\{x \mapsto 1, y \mapsto -7\} \;\; \Delta \;\; \{x \mapsto \top, y \mapsto -7\}$

(3) States:

$$\Delta \;\subseteq\; ((\mathit{Vars} \to \mathbb{Z}) \times (\mathbb{N} \to \mathbb{Z})) \times (\mathit{Vars} \to \mathbb{Z}^{\top})_{\bot}$$

$$(\rho, \mu) \;\Delta\; D \qquad \text{iff} \qquad \rho \;\Delta\; D$$

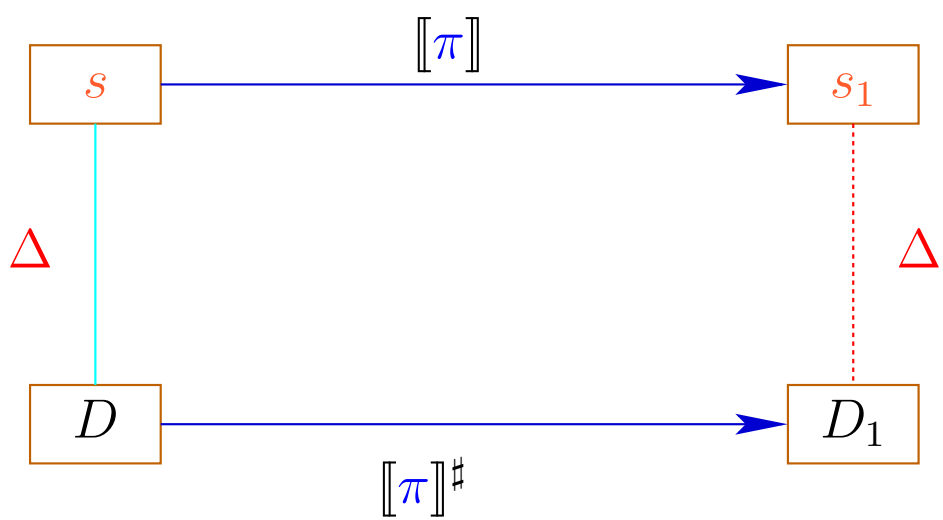
Concretization:

$$\gamma\, D = \begin{cases} \emptyset & \text{if} \quad D = \bot \\ \{(\rho, \mu) \mid \forall\, x :\; (\rho\, x) \;\Delta\; (D\, x)\} & \text{otherwise} \end{cases}$$

We show:

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

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



The abstract semantics simulates the concrete semantics :-)

In particular:

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

The abstract semantics simulates the concrete semantics :-)

In particular:

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

In practice, this means, e.g., that $D\, x = -7$ implies:

$$\begin{array}{rrcll} & \rho'\, x & = & -7 & \text{for all} \quad \rho' \in \gamma\, D \\ \Longrightarrow & \rho_1\, x & = & -7 & \text{for} \quad (\rho_1, \_) = [\![\pi]\!]\, s \end{array}$$

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

$(**)$

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

Then $(*)$ follows by induction :-)

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

$(***)$ $\quad (\llbracket e \rrbracket\, \rho) \;\; \Delta \;\; (\llbracket e \rrbracket^{\sharp}\, D) \quad$ whenever $\quad \rho \;\Delta\; D$

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

$(***)$ $(\llbracket e \rrbracket\, \rho)\ \Delta\ (\llbracket e \rrbracket^\sharp\, D)$ whenever $\rho\ \Delta\ D$

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

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

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

$(***)$ $(\llbracket e \rrbracket\, \rho)\ \Delta\ (\llbracket e \rrbracket^\sharp\, D)$ whenever $\rho\ \Delta\ D$

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 $\boxed{x = e;}$:

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

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

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

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

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

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

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

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

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

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

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

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

:-)

We conclude: The assertion $(*)$ is true :-))

The MOP-Solution:

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

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

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 :

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

We conclude: The assertion $(*)$ is true :-))

The MOP-Solution

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

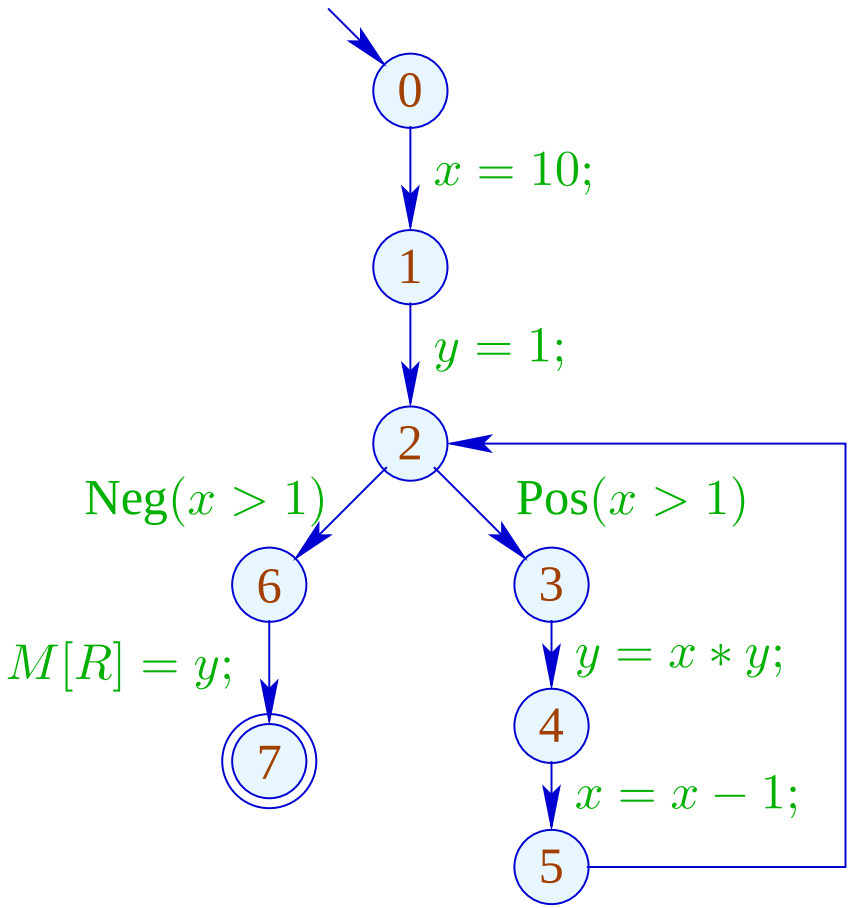
where $D_\top\, x = \top \qquad (x \in Vars)$.

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

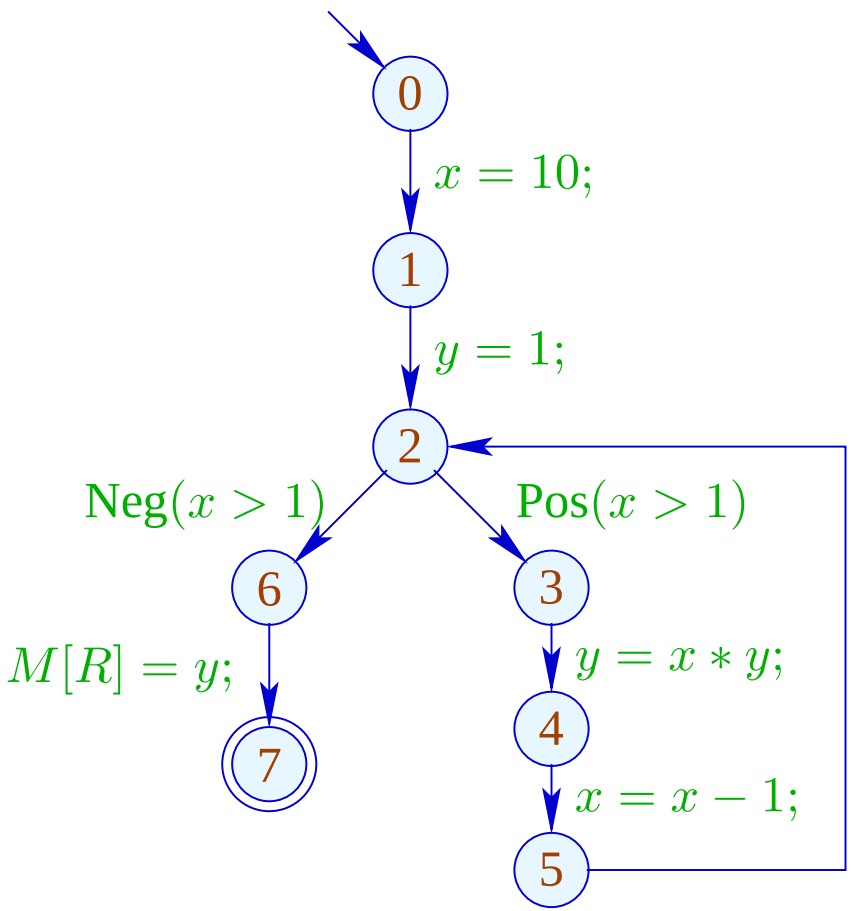
$$([\![\pi]\!]\, s) \;\Delta\; (\mathcal{D}^*[v])$$

In order to approximate the MOP, we use our constraint system :-))

Example:

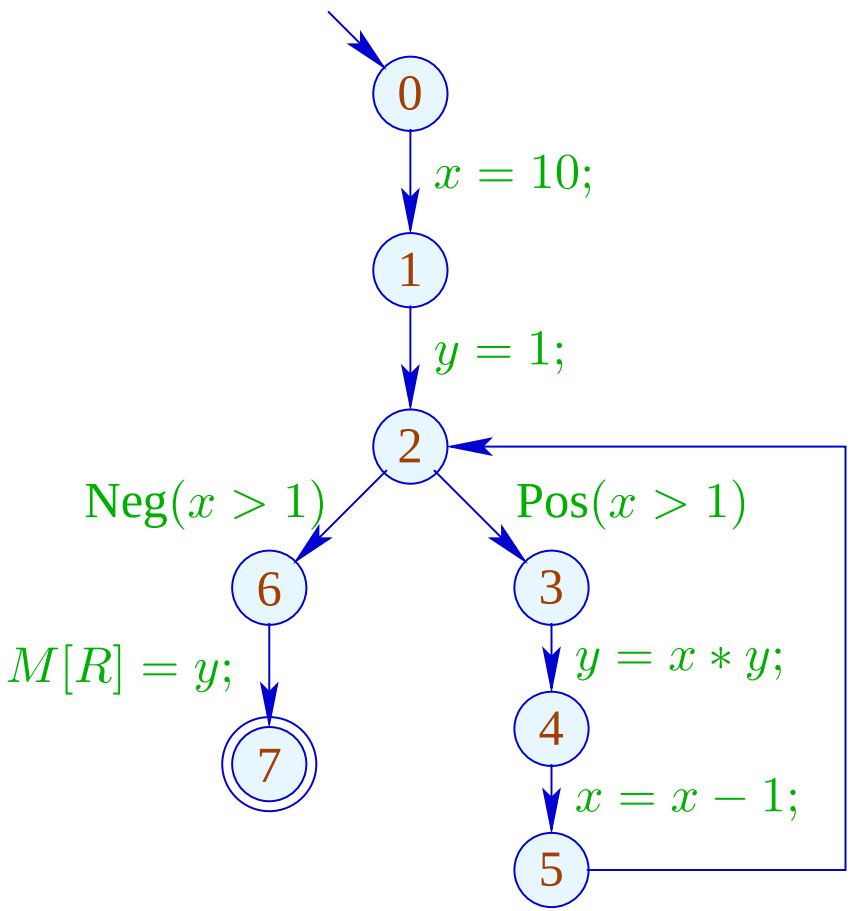


Example:



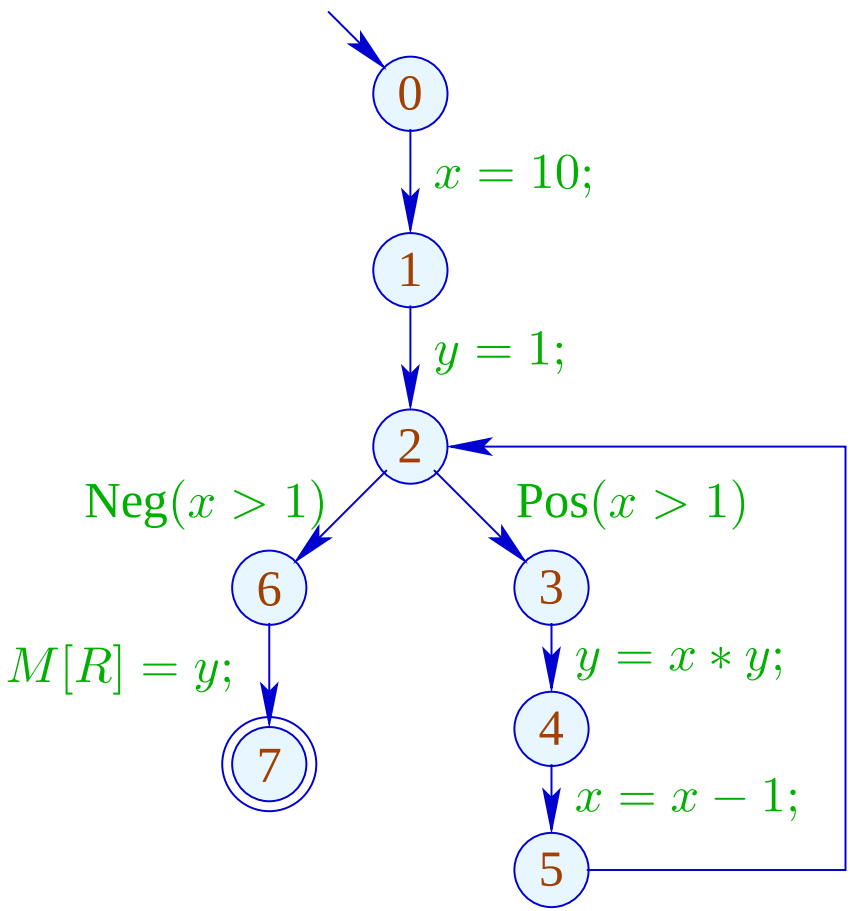
	1	
	x	y
0	$\top$	$\top$
1	10	$\top$
2	10	1
3	10	1
4	10	10
5	9	10
6	$\perp$	
7	$\perp$	

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	$\bot$		$\top$	$\top$
7	$\bot$		$\top$	$\top$

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	$\top$	$\top$	dito	
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: $f \;=\; [\![x = x + y;]\!]^\sharp$

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

:-((

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.,

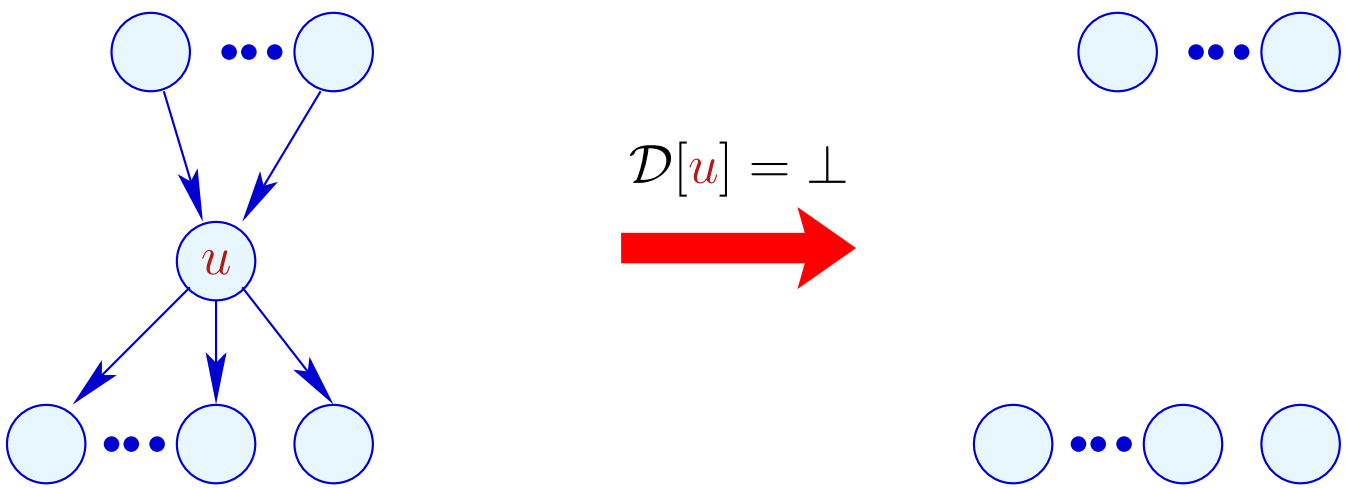
$$\mathcal{D}^*[v] \quad \sqsubseteq \quad \mathcal{D}[v]$$

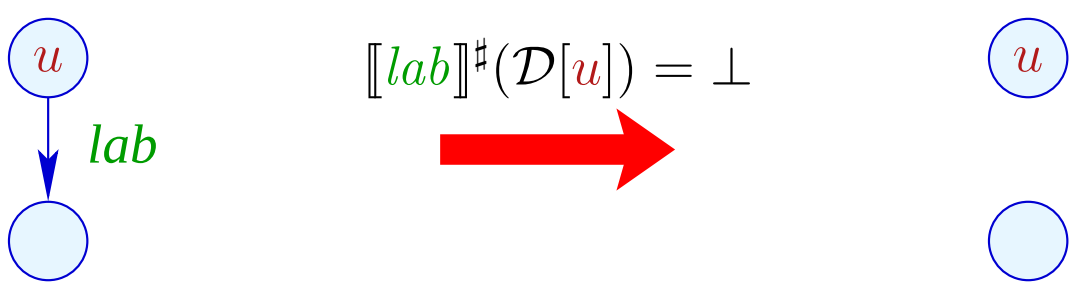
As an upper approximation, $\mathcal{D}[v]$ nonetheless describes the result of every program execution π which reaches v :

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

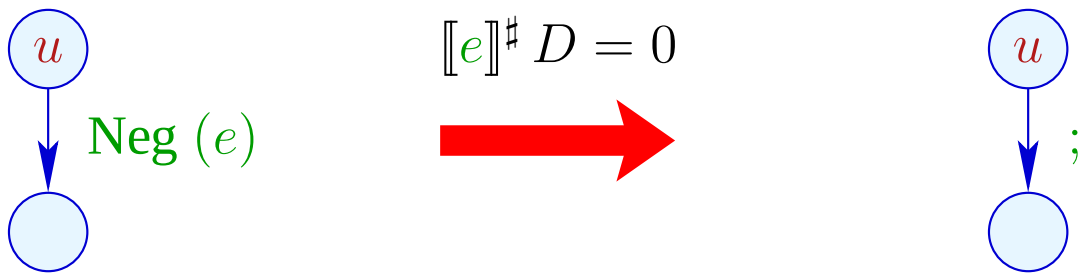
whenever $\llbracket \pi \rrbracket\,(\rho, \mu)$ is defined ;-))

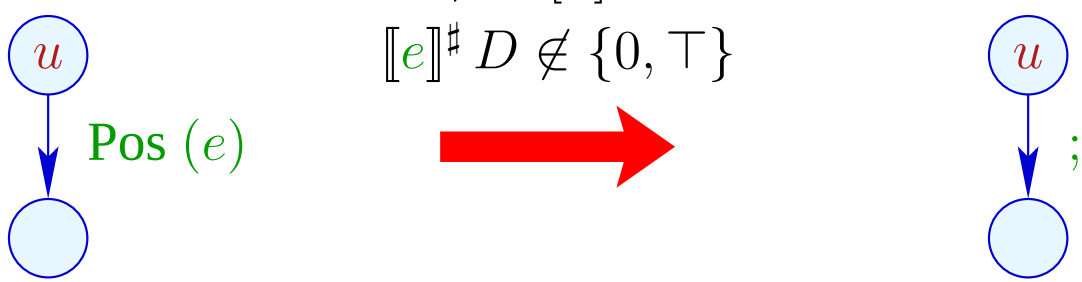
Transformation 4: Removal of Dead Code





Transformation 4 (cont.): Removal of Dead Code

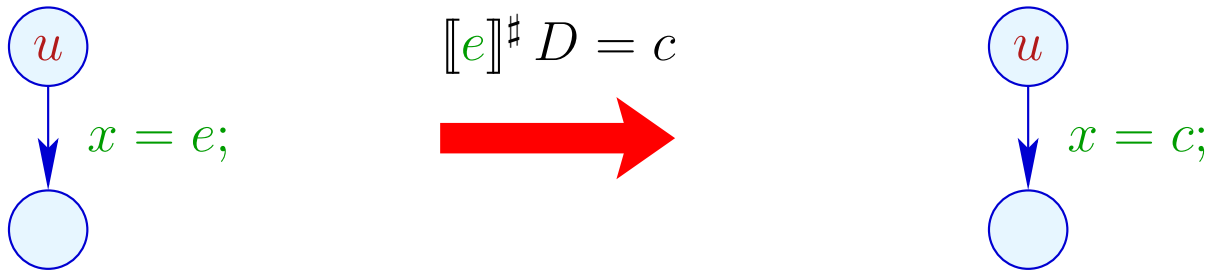




Transformation 4 (cont.): Simplified Expressions

$$\bot \neq \mathcal{D}[u] = D$$

$$[\![e]\!]^\sharp D = c$$



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.:

$$x * 0 \Longrightarrow 0$$
$$x * 1 \Longrightarrow x$$
$$x + 0 \Longrightarrow x$$
$$x - 0 \Longrightarrow x$$
$$\ldots$$

- 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:

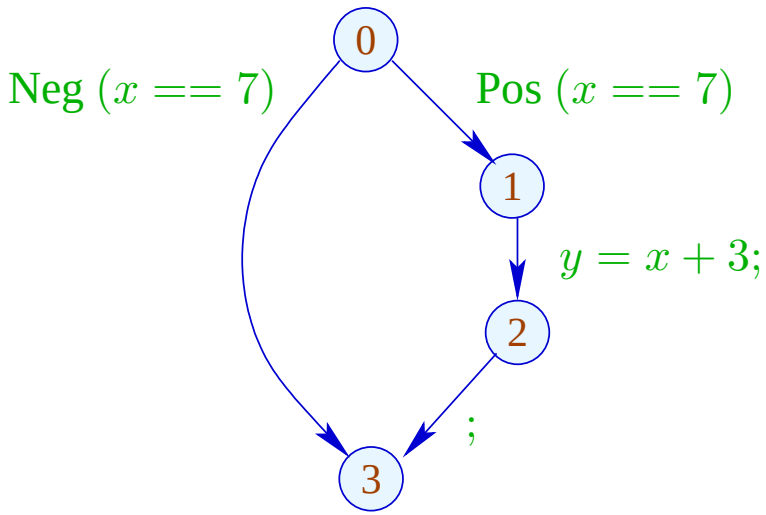
$$[\![\text{Pos}\,(x == e)]\!]^\sharp\, D = \begin{cases} D & \text{if} \quad [\![x == e]\!]^\sharp\, D = 1 \\ \bot & \text{if} \quad [\![x == e]\!]^\sharp\, D = 0 \\ D_1 & \text{otherwise} \end{cases}$$

where

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

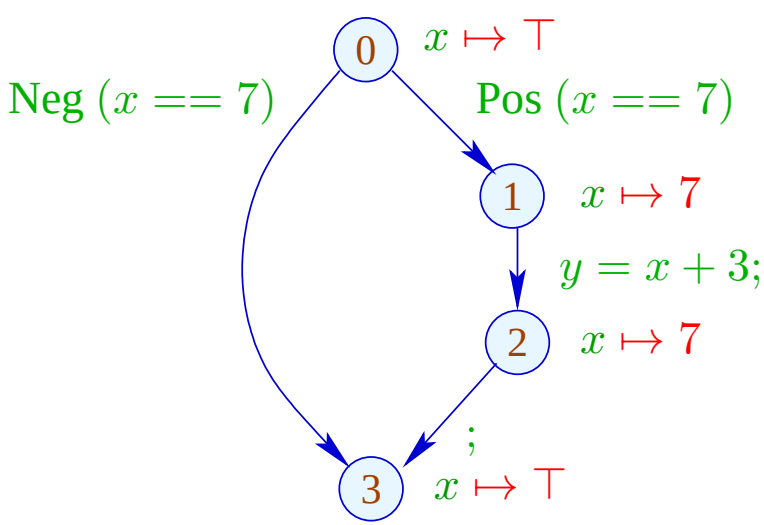
The effect of an edge labeled $\text{Neg}\,(x \neq e)$ is analogous :-)

Our Example:



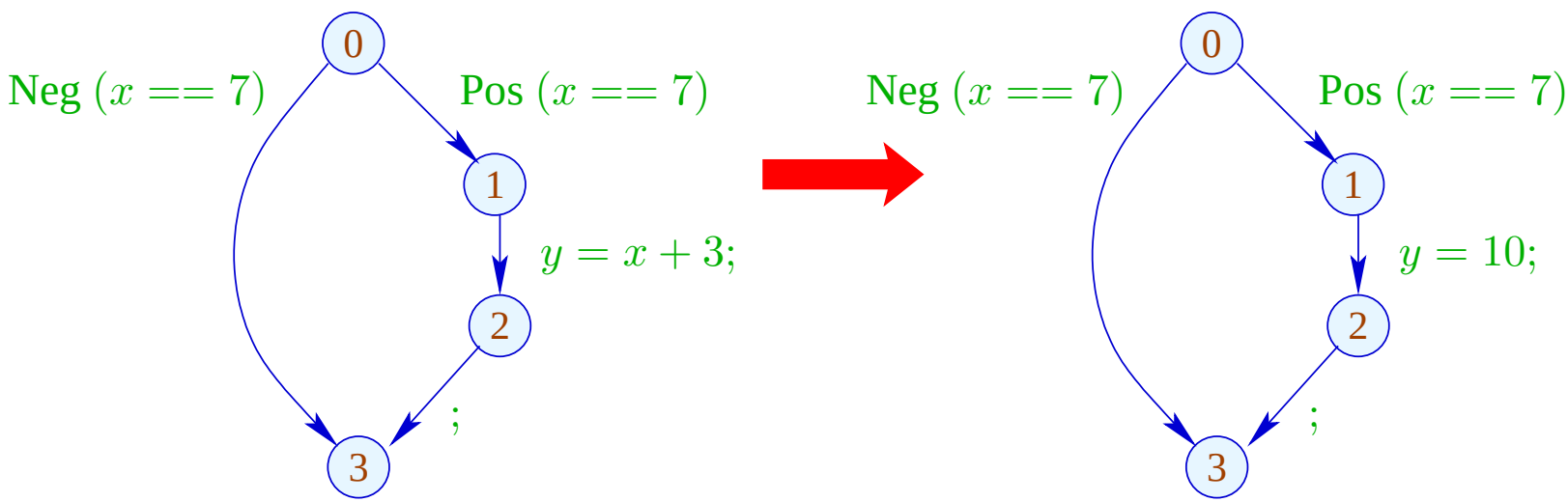
The effect of an edge labeled $\text{Neg}\,(x \neq e)$ is analogous :-)

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:

$$
\begin{array}{l}
\textsf{for}\ (i = 0; i < 42; i{+}{+}) \\
\quad \textsf{if}\ (0 \leq i \wedge i < 42)\{ \\
\qquad A_1 = A + i; \\
\qquad M[A_1] = i; \\
\quad \} \\
\quad // \quad A \text{ start address of an array} \\
\quad // \quad \textsf{if} \text{ the array-bound check}
\end{array}
$$

Obviously, the inner check is superfluous :-)

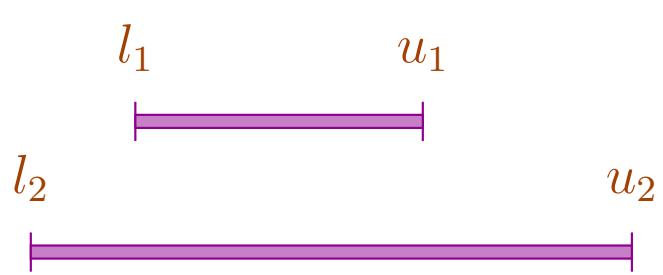
Idea 1:

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

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

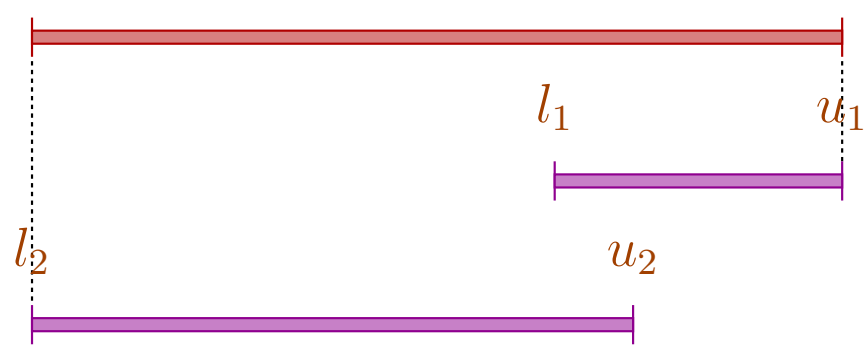
Partial Ordering:

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



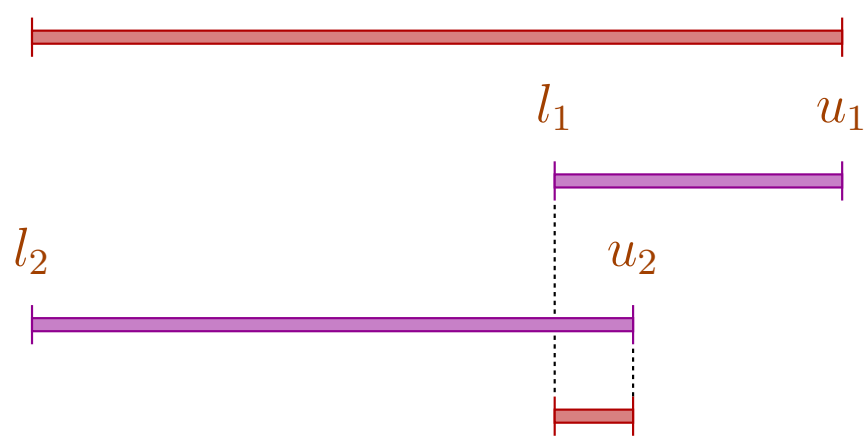
Thus:

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



Thus:

$$
\begin{aligned}
[l_1, u_1] \sqcup [l_2, u_2] &= [l_1 \sqcap l_2, u_1 \sqcup u_2] \\
[l_1, u_1] \sqcap [l_2, u_2] &= [l_1 \sqcup l_2, u_1 \sqcap u_2] \qquad \text{whenever } (l_1 \sqcup l_2) \leq (u_1 \sqcap u_2)
\end{aligned}
$$



Caveat:

$\rightarrow$ $\mathbb{I}$ is not a complete lattice :-)

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

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

Caveat:

$\rightarrow$ $\mathbb{I}$ is not a complete lattice :-)

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

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

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:

$$\begin{aligned} \gamma\,[0,7] &= \{0,\ldots,7\} \\ \gamma\,[0,\infty] &= \{0,1,2,\ldots,\} \end{aligned}$$

Computing with intervals: Interval Arithmetic :-)

Addition:

$$\begin{aligned} [l_1,u_1] +^{\sharp} [l_2,u_2] &= [l_1+l_2, u_1+u_2] \qquad \text{where} \\ -\infty + \_ &= -\infty \\ +\infty + \_ &= +\infty \\ // \quad & -\infty + \infty \quad \text{cannot occur} \quad \text{:-)} \end{aligned}$$

Negation:

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

Multiplication:

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

Example:

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