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.:

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

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

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

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:

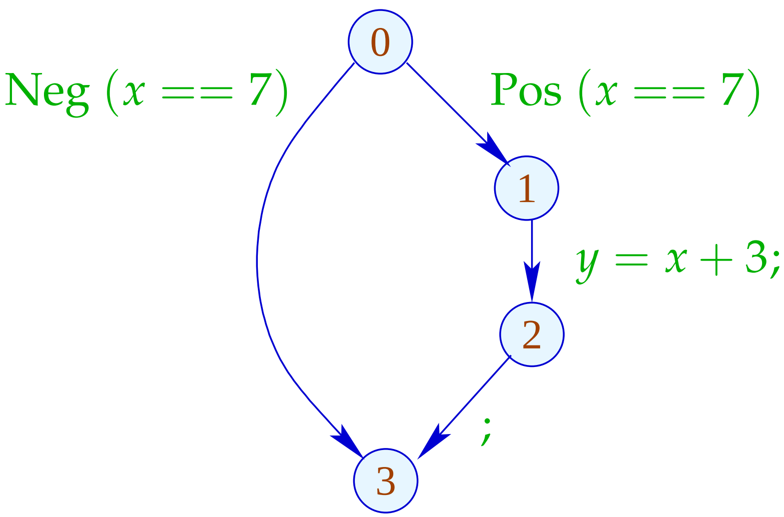
$$[\![\text{Pos}\,(x == e)]\!]^\sharp\, D = \begin{cases} D & \text{if} \quad [\![x == e]\!]^\sharp\, D = 1 \\ \bot & \text{if} \quad [\![x == e]\!]^\sharp\, D = 0 \\ D_1 & \text{otherwise} \end{cases}$$

where

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

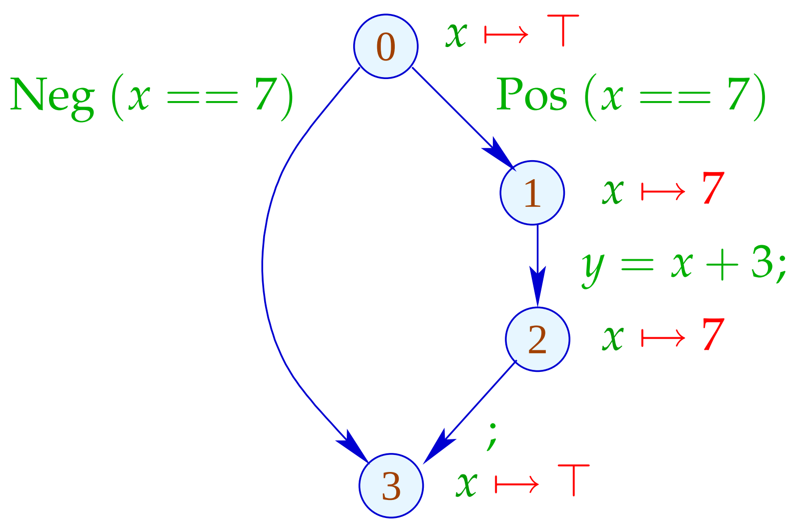
The effect of an edge labeled $\text{Neg}\,(x \neq e)$ is analogous :-)

Our Example:



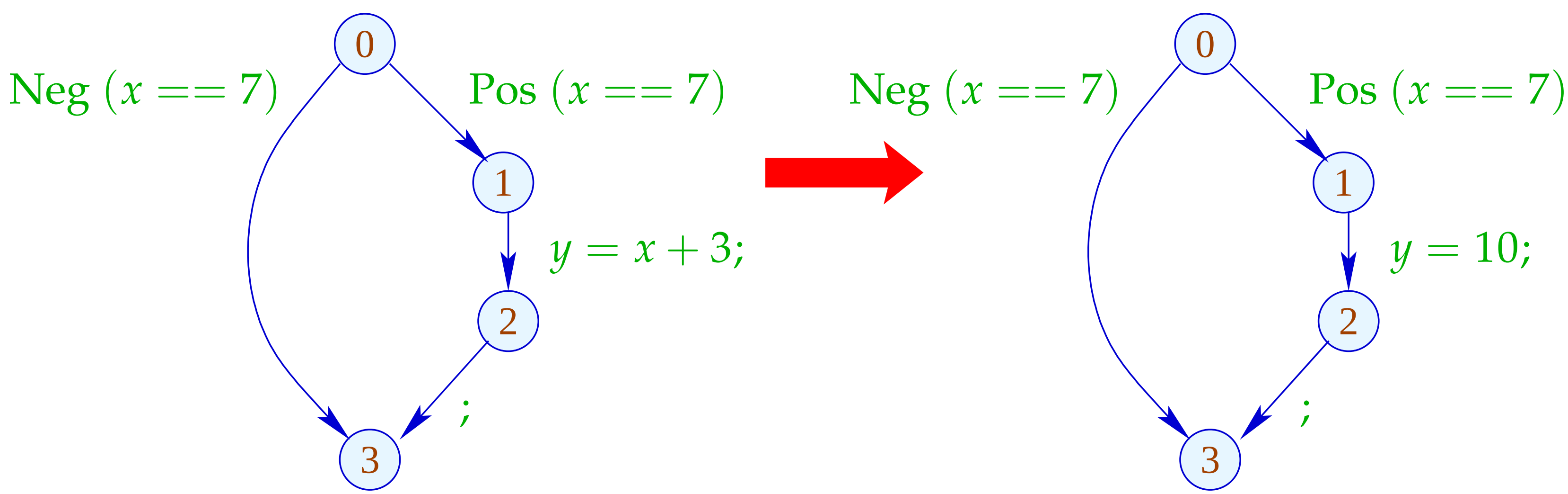
The effect of an edge labeled $\text{Neg}\,(x \neq e)$ is analogous :-)

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:

$$\text{for } (i = 0; i < 42; i{+}{+})$$
$$\quad \text{if } (0 \leq i \wedge i < 42)\{$$
$$\qquad A_1 = A + i;$$
$$\qquad M[A_1] = i;$$
$$\quad \}$$

// A start address of an array

// if the array-bound check

Obviously, the inner check is superfluous :-)

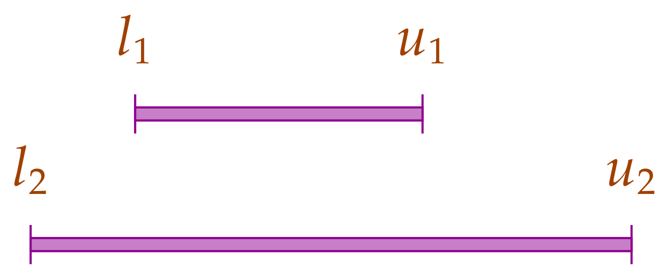
Idea 1:

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

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

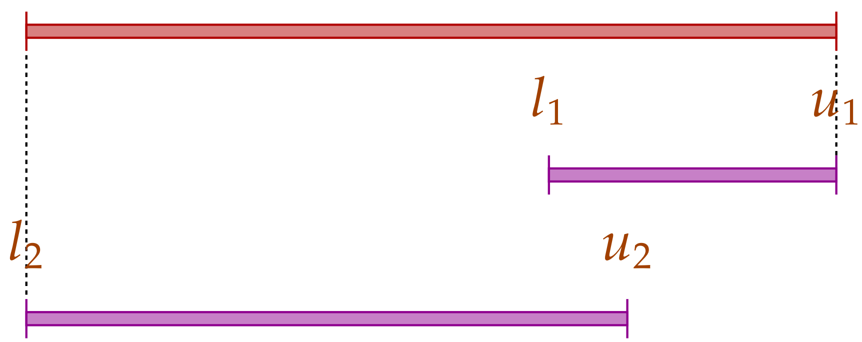
Partial Ordering:

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



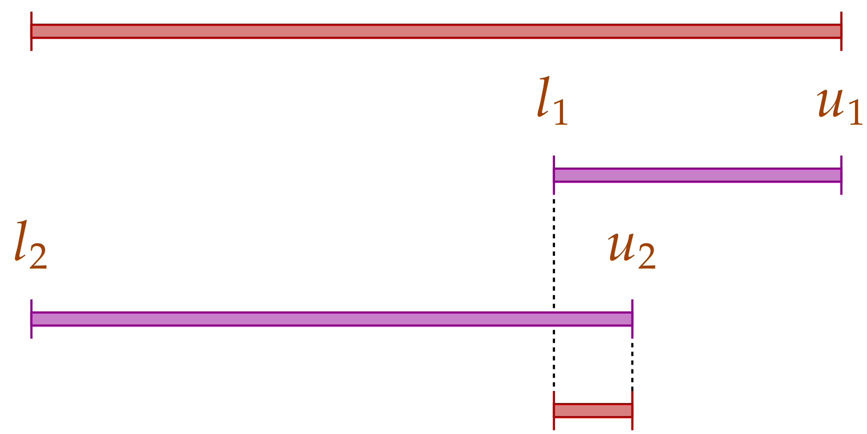
Thus:

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



Thus:

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



Warning:

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

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

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

Warning:

$\rightarrow$ $\mathbb{I}$ 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:

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

Computing with intervals: Interval Arithmetic :-)

Addition:

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

Negation:

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

Multiplication:

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

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

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

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

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

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

Equality:

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

Equality:

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

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:

$$\begin{aligned} [1,2] <^\sharp [9,42] &= [1,1] \\ [0,7] <^\sharp [0,7] &= [0,1] \\ [3,4] <^\sharp [1,2] &= [0,0] \end{aligned}$$

By means of $\mathbb{I}$ we construct the complete lattice:

$$\mathbb{D}_{\mathbb{I}} = (\mathit{Vars} \to \mathbb{I})_{\perp}$$

Description Relation:

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

The abstract evaluation of expressions is defined analogously to constant propagation. We have:

$$([\![e]\!]\; \rho) \;\Delta\; ([\![e]\!]^{\sharp}\; D) \qquad \text{whenever} \qquad \rho \;\Delta\; D$$

The Effects of Edges:

$$
\begin{array}{lll}
[\![;]\!]^\sharp\, D & = & D \\
[\![x = e;]\!]^\sharp\, D & = & D \oplus \{x \mapsto [\![e]\!]^\sharp\, D\} \\
[\![x = M[e];]\!]^\sharp\, D & = & D \oplus \{x \mapsto \top\} \\
[\![M[e_1] = e_2;]\!]^\sharp\, D & = & D \\
[\![\mathrm{Pos}\,(e)]\!]^\sharp\, D & = & \left\{ \begin{array}{lll} \bot & \text{if} & [0,0] = [\![e]\!]^\sharp\, D \\ D & \text{otherwise} & \end{array} \right. \\
[\![\mathrm{Neg}\,(e)]\!]^\sharp\, D & = & \left\{ \begin{array}{lll} D & \text{if} & [0,0] \sqsubseteq [\![e]\!]^\sharp\, D \\ \bot & \text{otherwise} & \end{array} \right.
\end{array}
$$

... given that $D \neq \bot$:-)

Better Exploitation of Conditions:

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

where :

$$D_1 \quad = \quad \begin{cases} D \oplus \{x \mapsto (D\,x) \sqcap ([\![e_1]\!]^\sharp\, D)\} & \text{if } e \equiv x == e_1 \\ D \oplus \{x \mapsto (D\,x) \sqcap [-\infty, u]\} & \text{if } e \equiv x \leq e_1, [\![e_1]\!]^\sharp\, D = [\_, u] \\ D \oplus \{x \mapsto (D\,x) \sqcap [l, \infty]\} & \text{if } e \equiv x \geq e_1, [\![e_1]\!]^\sharp\, D = [l, \_] \end{cases}$$

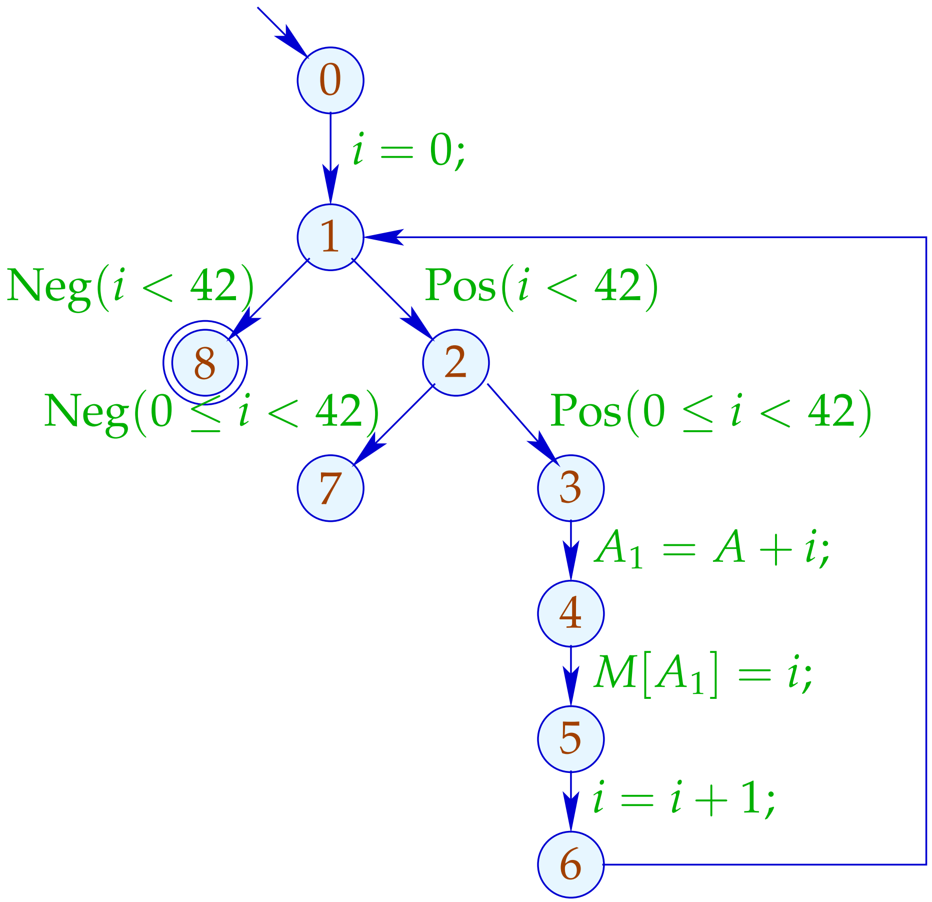
Better Exploitation of Conditions (cont.):

$$[\![\mathrm{Neg}\,(e)]\!]^\sharp\, D \;=\; \begin{cases} \bot & \text{if} \quad [0,0] \not\sqsubseteq [\![e]\!]^\sharp\, D \\ D_1 & \text{otherwise} \end{cases}$$

where :

$$D_1 \;=\; \begin{cases} D \oplus \{x \mapsto (D\,x) \sqcap ([\![e_1]\!]^\sharp\, D)\} & \text{if } e \equiv x \;\neq\; e_1 \\ D \oplus \{x \mapsto (D\,x) \sqcap [-\infty, u]\} & \text{if } e \equiv x \;>\; e_1, [\![e_1]\!]^\sharp\, D = [\_, u] \\ D \oplus \{x \mapsto (D\,x) \sqcap [l, \infty]\} & \text{if } e \equiv x \;<\; e_1, [\![e_1]\!]^\sharp\, D = [l, \_] \end{cases}$$

Example:



	i	
	l	u
0	$-\infty$	$+\infty$
1	0	42
2	0	41
3	0	41
4	0	41
5	0	41
6	1	42
7	$\perp$	
8	42	42

Problem:

$\rightarrow$ The solution can be computed with RR-iteration — after about 42 rounds :-(

$\rightarrow$ On some programs, iteration may never terminate :-((

Idea 1: Widening

- Accelerate the iteration — at the prize of imprecision :-)
- Allow only a bounded number of modifications of values !!!

... in the Example:

- dis-allow updates of interval bounds in $\mathbb{Z}$ ...

$\Longrightarrow$ a maximal chain:

$$[3, 17] \sqsubset [3, +\infty] \sqsubset [-\infty, +\infty]$$

Formalization of the Approach:

Let $x_i \sqsupseteq f_i\,(x_1, \ldots, x_n)\,, \quad i = 1, \ldots, n$ (1)

denote a system of constraints over $\mathbb{D}$ where the f_i are not necessarily monotonic.

Nonetheless, an accumulating iteration can be defined. Consider the system of equations:

$$x_i \;=\; x_i \sqcup f_i\,(x_1, \ldots, x_n)\,, \quad i = 1, \ldots, n \qquad (2)$$

We obviously have:

(a) $\underline{x}$ is a solution of (1) iff $\underline{x}$ is a solution of (2).

(b) The function $G : \mathbb{D}^n \to \mathbb{D}^n$ with
$G\,(x_1, \ldots, x_n) = (y_1, \ldots, y_n)\,, \quad y_i = x_i \sqcup f_i\,(x_1, \ldots, x_n)$
is increasing, i.e., $\underline{x} \sqsubseteq G\,\underline{x}$ for all $\underline{x} \in \mathbb{D}^n$.

(c) The sequence $G^k \underline{\perp}$, $k \geq 0$, is an ascending chain:

$$\underline{\perp} \sqsubseteq G\,\underline{\perp} \sqsubseteq \ldots \sqsubseteq G^k\,\underline{\perp} \sqsubseteq \ldots$$

(d) If $G^k\,\underline{\perp} = G^{k+1}\,\underline{\perp} = \underline{y}$, then $\underline{y}$ is a solution of (1).

(e) If $\mathbb{D}$ has infinite strictly ascending chains, then (d) is not yet sufficient ...

but: we could consider the modified system of equations:

$$x_i = x_i \sqcup\!\!\!\!\sqcup\, f_i(x_1, \ldots, x_n)\,, \quad i = 1, \ldots, n \qquad (3)$$

for a binary operation widening:

$$\sqcup\!\!\!\!\sqcup : \mathbb{D}^2 \to \mathbb{D} \qquad \text{with} \qquad v_1 \sqcup v_2 \sqsubseteq v_1 \sqcup\!\!\!\!\sqcup\, v_2$$

(RR)-iteration for (3) still will compute a solution of (1) :-)

... for Interval Analysis:

- The complete lattice is: $\mathbb{D}_{\mathbb{I}} \;=\; (\mathit{Vars} \to \mathbb{I})_{\perp}$
- the widening $\sqcup$ is defined by:

$$\perp \sqcup D \;=\; D \sqcup \perp \;=\; D \qquad \text{and for} \quad D_1 \neq \perp \neq D_2:$$

$$\begin{array}{rcl} (D_1 \sqcup D_2)\, x & = & (D_1\, x) \sqcup (D_2\, x) \qquad \text{where} \\ [l_1, u_1] \sqcup [l_2, u_2] & = & [l, u] \qquad \text{with} \\ l & = & \begin{cases} l_1 & \text{if} \quad l_1 \leq l_2 \\ -\infty & \text{otherwise} \end{cases} \\ u & = & \begin{cases} u_1 & \text{if} \quad u_1 \geq u_2 \\ +\infty & \text{otherwise} \end{cases} \end{array}$$

$\Longrightarrow$ $\sqcup$ is not commutative !!!

Example:

$$
\begin{aligned}
[0,2] \sqcup [1,2] &= [0,2] \\
[1,2] \sqcup [0,2] &= [-\infty,2] \\
[1,5] \sqcup [3,7] &= [1,+\infty]
\end{aligned}
$$

→ Widening returns larger values more quickly.

→ It should be constructed in such a way that termination of iteration is guaranteed :-)

→ For interval analysis, widening bounds the number of iterations by:

$$\#\mathit{points} \cdot (1 + 2 \cdot \#\mathit{Vars})$$

Conclusion:

- In order to determine a solution of (1) over a complete lattice with infinite ascending chains, we define a suitable widening and then solve (3) :-)

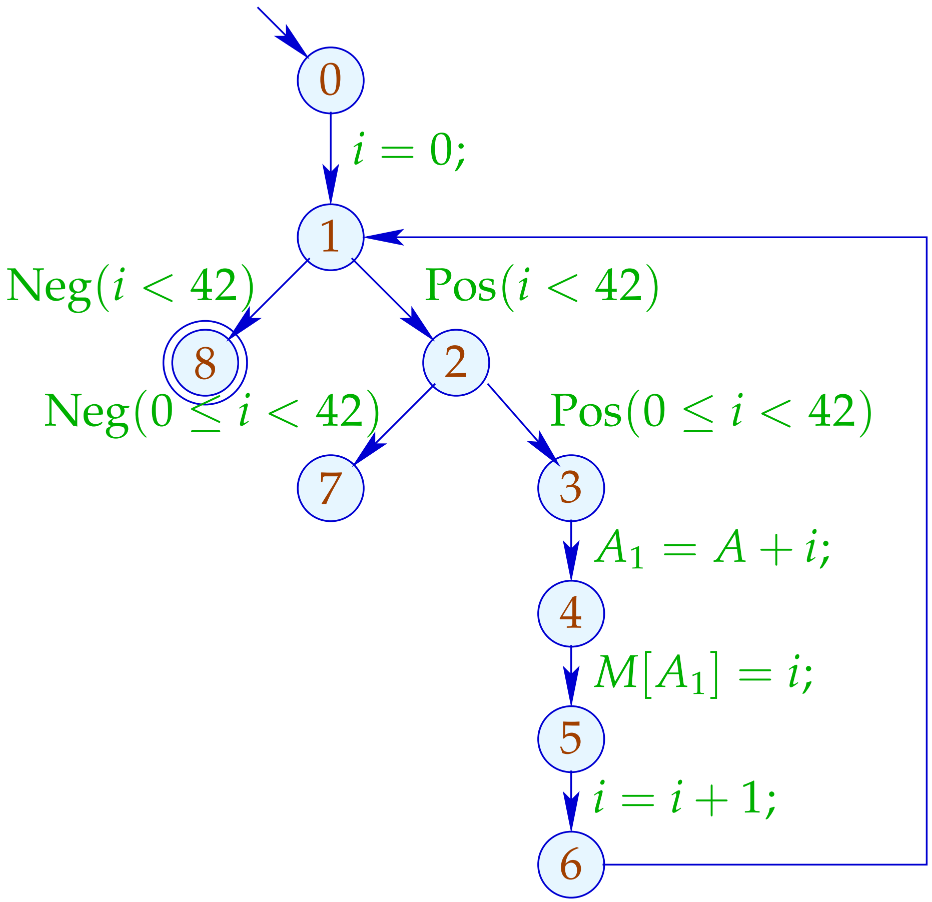
- Warning: The construction of suitable widenings is a dark art !!!

  Often $\sqcup$ is chosen dynamically during iteration such that

  $\longrightarrow$ the abstract values do not get too complicated;

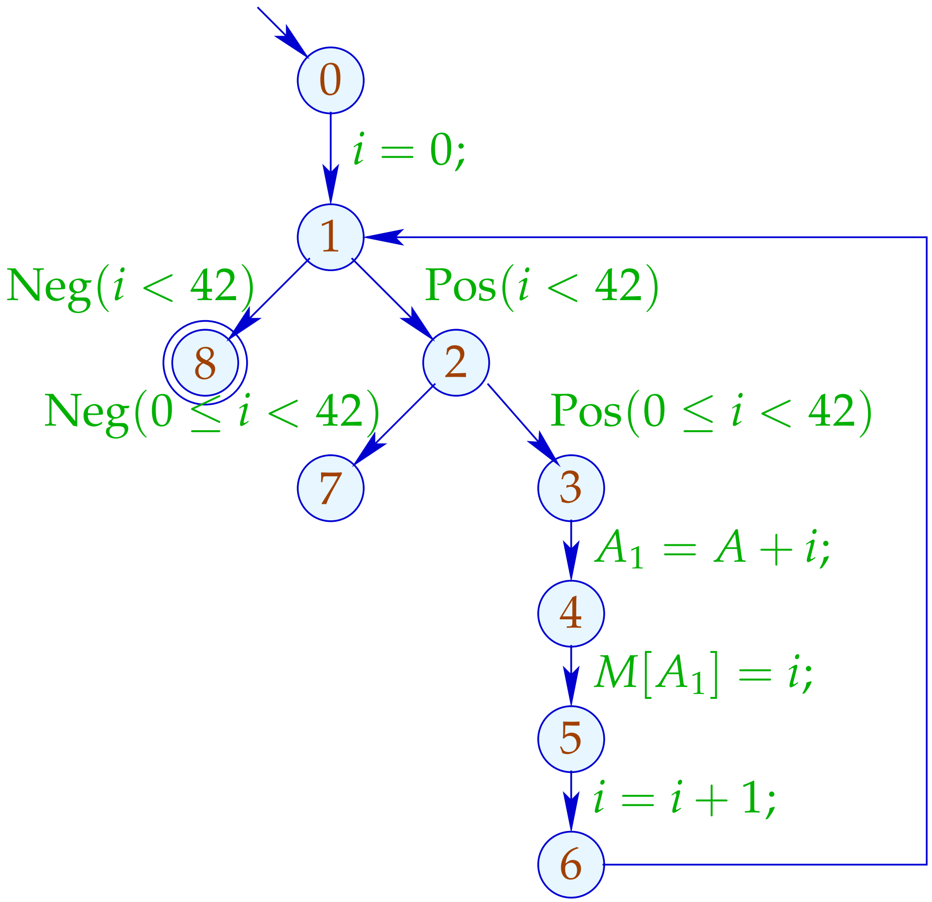
  $\longrightarrow$ the number of updates remains bounded ...

Our Example:



	1	
	l	u
0	$-\infty$	$+\infty$
1	0	0
2	0	0
3	0	0
4	0	0
5	0	0
6	1	1
7	$\perp$	
8	$\perp$	

Our Example:



	1		2		3	
	l	u	l	u	l	u
0	$-\infty$	$+\infty$	$-\infty$	$+\infty$		
1	0	0	0	$+\infty$		
2	0	0	0	$+\infty$		
3	0	0	0	$+\infty$		
4	0	0	0	$+\infty$	dito	
5	0	0	0	$+\infty$		
6	1	1	1	$+\infty$		
7	$\perp$		42	$+\infty$		
8	$\perp$		42	$+\infty$		

... obviously, the result is disappointing :-(

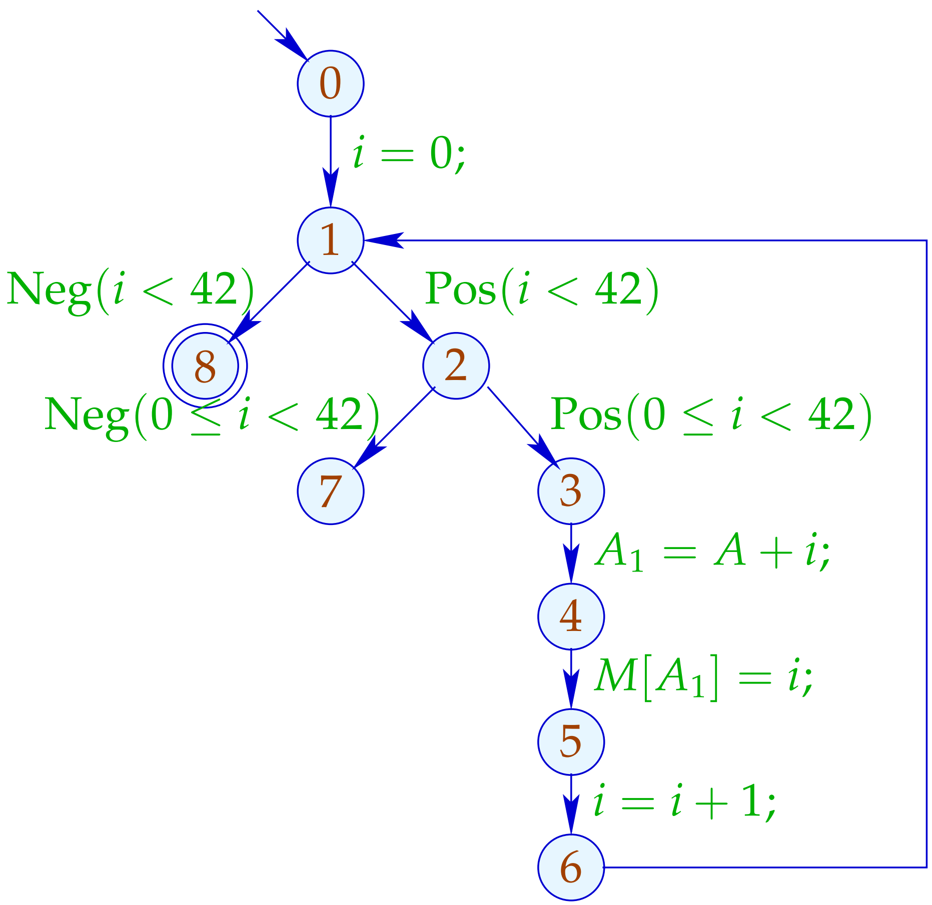
Idea 2:

In fact, acceleration with $\sqcup$ need only be applied at sufficiently many places!

A set I is a loop separator, if every loop contains at least one point from I :-)

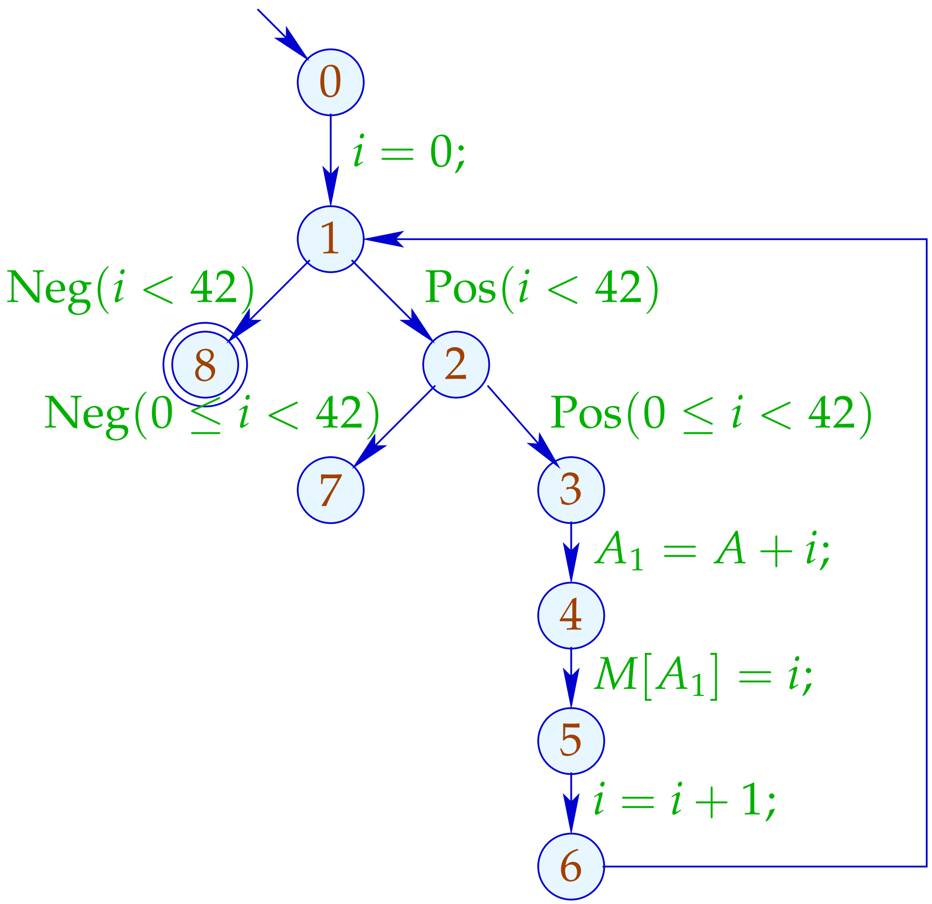
If we apply widening only at program points from such a set I, then RR-iteration still terminates !!!

In our Example:



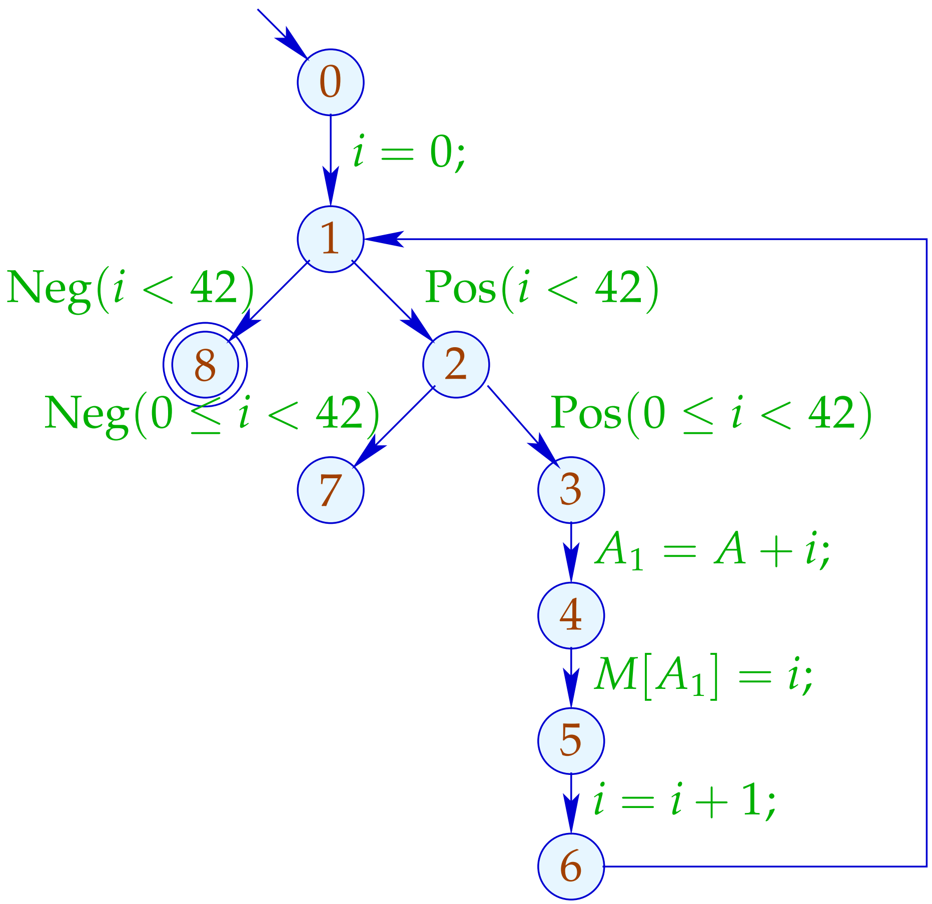
$$I_1 = \{1\} \quad \text{or:}$$
$$I_2 = \{2\} \quad \text{or:}$$
$$I_3 = \{3\}$$

The Analysis with $I = \{1\}$:



	1		2		3	
	l	u	l	u	l	u
0	$-\infty$	$+\infty$	$-\infty$	$+\infty$	dito	
1	0	0	0	$+\infty$		
2	0	0	0	41		
3	0	0	0	41		
4	0	0	0	41		
5	0	0	0	41		
6	1	1	1	42		
7	$\perp$		$\perp$			
8	$\perp$		42	$+\infty$		

The Analysis with $I = \{2\}$:



	1		2		3	
	l	u	l	u	l	u
0	$-\infty$	$+\infty$	$-\infty$	$+\infty$		
1	0	0	0	42		
2	0	0	0	$+\infty$		
3	0	0	0	41		
4	0	0	0	41	dito	
5	0	0	0	41		
6	1	1	1	42		
7	$\bot$		42	$+\infty$		
8	$\bot$		42	42		

Discussion:

- Both runs of the analysis determine interesting information :-)
- The run with $I = \{2\}$ proves that always $i = 42$ after leaving the loop.
- Only the run with $I = \{1\}$ finds, however, that the outer check makes the inner check superfluous :-(

How can we find a suitable loop separator I ???

Idea 3: Narrowing

Let $\underline{x}$ denote any solution of (1), i.e.,

$$x_i \sqsupseteq f_i\,\underline{x} \;, \qquad i = 1, \ldots, n$$

Then for monotonic f_i,

$$\underline{x} \sqsupseteq F\,\underline{x} \sqsupseteq F^2\,\underline{x} \sqsupseteq \ldots \sqsupseteq F^k\,\underline{x} \sqsupseteq \ldots$$

// Narrowing Iteration

Idea 3: Narrowing

Let $\underline{x}$ denote any solution of (1), i.e.,

$$x_i \sqsupseteq f_i \, \underline{x} \ , \qquad i = 1, \ldots, n$$

Then for monotonic f_i,

$$\underline{x} \sqsupseteq F \, \underline{x} \sqsupseteq F^2 \, \underline{x} \sqsupseteq \ldots \sqsupseteq F^k \, \underline{x} \sqsupseteq \ldots$$

// Narrowing Iteration

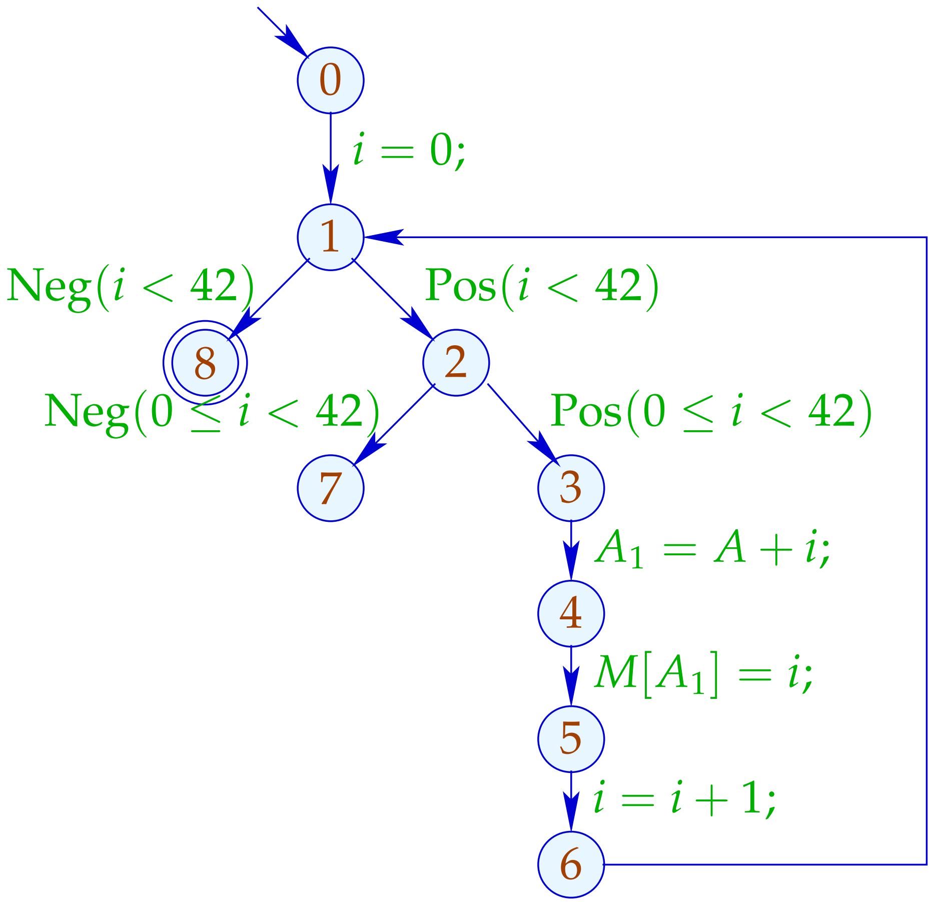
Every tuple $F^k \, \underline{x}$ is a solution of (1) :-)

$\Longrightarrow$

Termination is no problem anymore:
we stop whenever we want :-))

// The same also holds for RR-iteration.

Narrowing Iteration in the Example:



	0	
	l	u
0	$-\infty$	$+\infty$
1	0	$+\infty$
2	0	$+\infty$
3	0	$+\infty$
4	0	$+\infty$
5	0	$+\infty$
6	1	$+\infty$
7	42	$+\infty$
8	42	$+\infty$