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 :-)

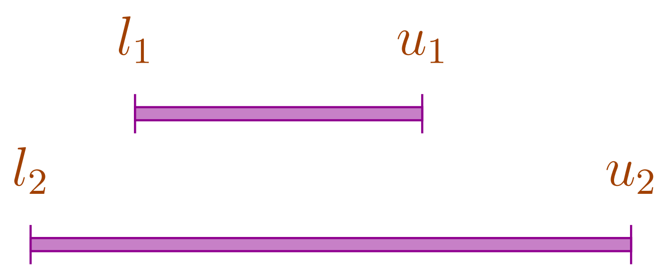
Idea 1:

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

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

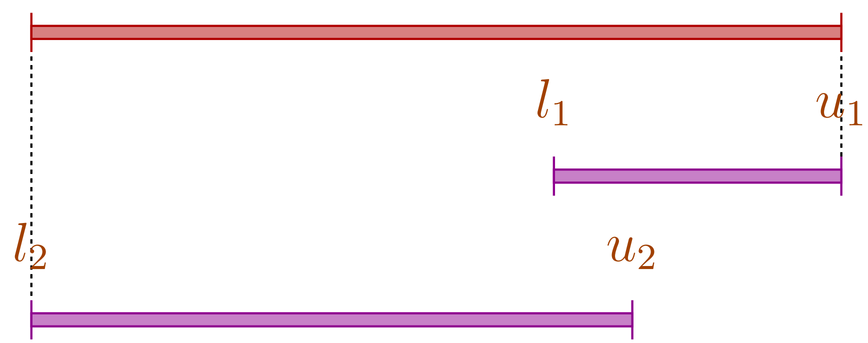
Partial Ordering:

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



Thus:

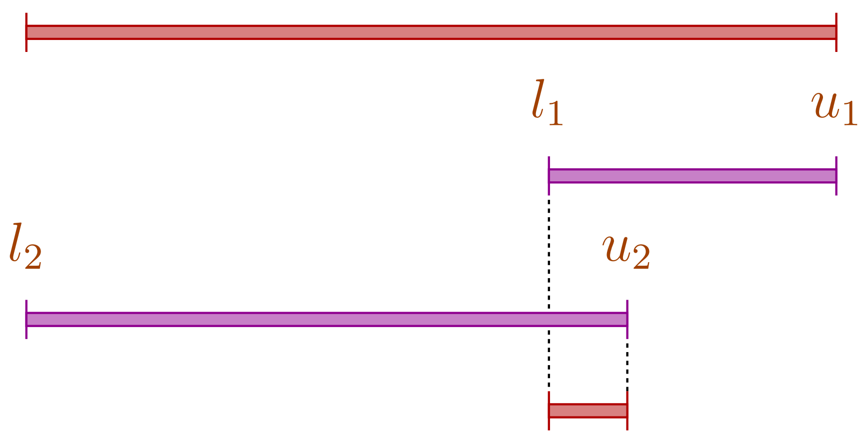
$$[l_1, u_1] \sqcup [l_2, u_2] \quad = \quad [l_1 \sqcap l_2, u_1 \sqcup u_2]$$



Thus:

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

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



Caveat:

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

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

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

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:

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

Computing with intervals: Interval Arithmetic :-)

Addition:

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

:-)

Negation:

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

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:

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

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

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

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

- 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:

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

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:

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

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:

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

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

Better Exploitation of Conditions:

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

where :

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

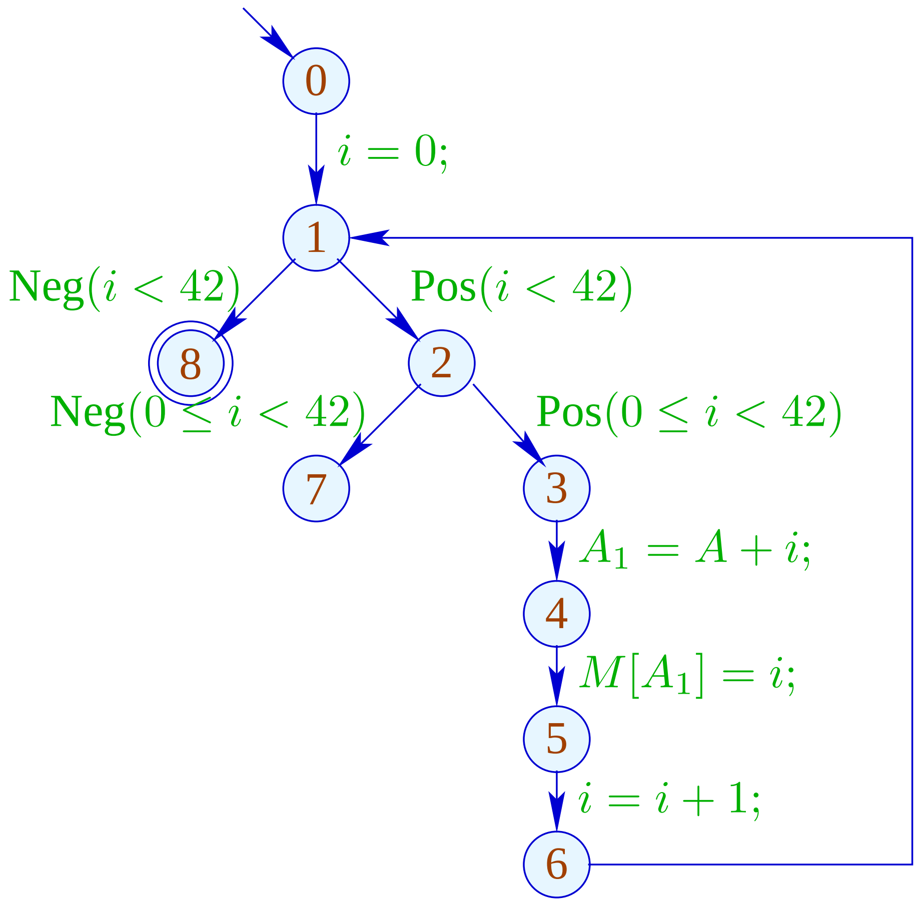
Better Exploitation of Conditions (cont.):

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

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	$\bot$	
8	42	42