Die abstrakten Kanten-Effekte $[\![k]\!]^\sharp$ setzen wir wieder zu den Effekten von Pfaden $\pi = k_1 \ldots k_r$ zusammen durch:

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

Idee zur Korrektheit: Abstrakte Interpretation

Cousot, Cousot 1977

Aufstellen einer Beschreibungsrelation Δ zwischen konkreten Werten und deren Beschreibungen mit:

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

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

// liefert Menge der beschriebenen Werte :-)

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

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

Konkretisierung:

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

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

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

Konkretisierung:

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

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

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

Konkretisierung:

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

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

(3) Zustände:

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

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

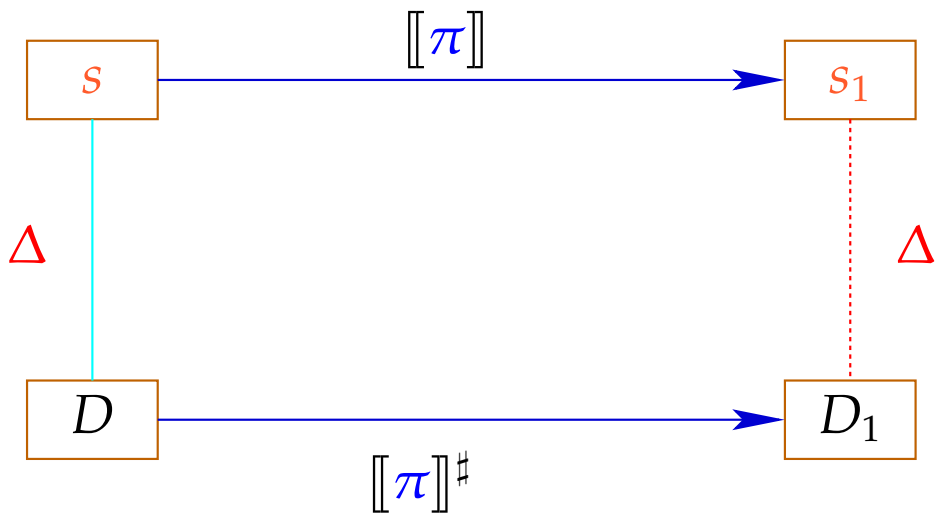
Konkretisieruing:

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

Wir zeigen:

$(*)$ Gilt $s \;\Delta\; D$ und ist $[\![\pi]\!]\, s$ definiert, dann gilt auch:

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



Die abstrakte Semantik simuliert die konkrete :-)

Insbesondere gilt:

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

Die abstrakte Semantik simuliert die konkrete :-)

Insbesondere gilt:

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

Praktisch heißt das z.B., dass für $D\,x = -7$ gilt:

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

Zum Beweis von $(*)$ zeigen wir für jede Kante k :

$(**)$

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

Dann folgt $(*)$ mittels Induktion :-)

Zum Beweis von $(**)$ zeigen wir für jeden Ausdruck e :

$(***)$ $(\llbracket e \rrbracket\, \rho)\ \Delta\ (\llbracket e \rrbracket^{\sharp}\, D)$ sofern nur $\rho\ \Delta\ D$

Zum Beweis von $(**)$ zeigen wir für jeden Ausdruck e :

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

Zum Beweis von $(***)$ zeigen wir für jeden Operator $\Box$:

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

Zum Beweis von $(**)$ zeigen wir für jeden Ausdruck e :

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

Zum Beweis von $(***)$ zeigen wir für jeden Operator $\Box$:

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

So hatten wir die Operatoren $\Box^\sharp$ aber gerade definiert :-)

Nun zeigen wir $(**)$ durch Fallunterscheidung nach der Kanten-Beschriftung lab .

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

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

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

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

Fall $\boxed{x = M[R];}$:

$$\begin{array}{lcl} \rho_1 & = & \rho \oplus \{x \mapsto \mu\,(\rho\, R)\} \\ D_1 & = & D \oplus \{x \mapsto \top\} \end{array} \qquad \mu_1 = \mu$$

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

Fall $\boxed{M[R_1] = R_2;}$:

$$\begin{array}{lcl} \rho_1 & = & \rho \\ D_1 & = & D \end{array} \qquad \mu_1 = \mu \oplus \{\rho\, R_1 \mapsto \rho\, R_2\}$$

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

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

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

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

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

:-)

Wir schließen: Die Behauptung $(*)$ stimmt :-))

Die MOP-Lösung:

$$\mathcal{D}^*[v] \;=\; \bigsqcup\{[\![\pi]\!]^\sharp\, D_0 \mid \pi : \mathit{start} \to^* v\}$$

wobei $D_0\, x = \top \qquad (x \in \mathit{Vars})$.

Wir schließen: Die Behauptung $(*)$ stimmt :-))

Die MOP-Lösung:

$$\mathcal{D}^*[v] \;=\; \bigsqcup\{[\![\pi]\!]^\sharp\, D_0 \mid \pi : \mathit{start} \to^* v\}$$

wobei $D_0\, x = \top \qquad (x \in \mathit{Vars})$.

Wegen $(*)$ gilt für alle Anfangszustände s und alle Berechnungen π , die v erreichen:

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

Wir schließen: Die Behauptung $(*)$ stimmt :-))

Die MOP-Lösung:

$$\mathcal{D}^*[v] \;=\; \bigsqcup\{[\![\pi]\!]^\sharp\, D_0 \mid \pi : \mathit{start} \to^* v\}$$

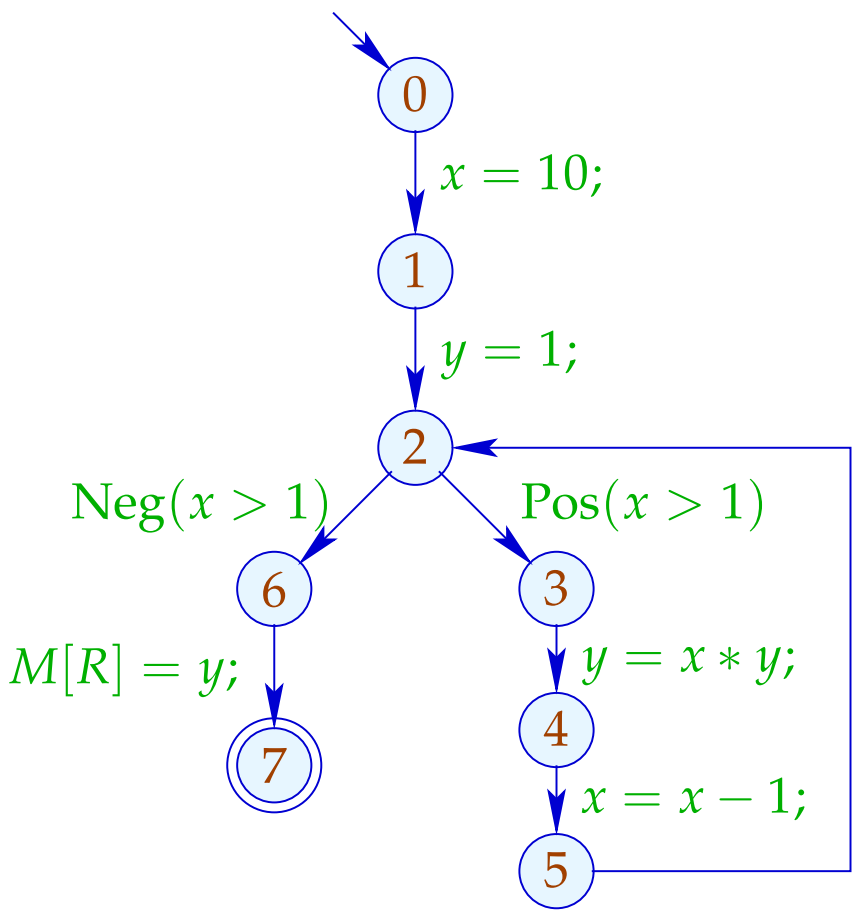
wobei $D_0\, x = \top \qquad (x \in \mathit{Vars})$.

Wegen $(*)$ gilt für alle Anfangszustände s und alle Berechnungen π , die v erreichen:

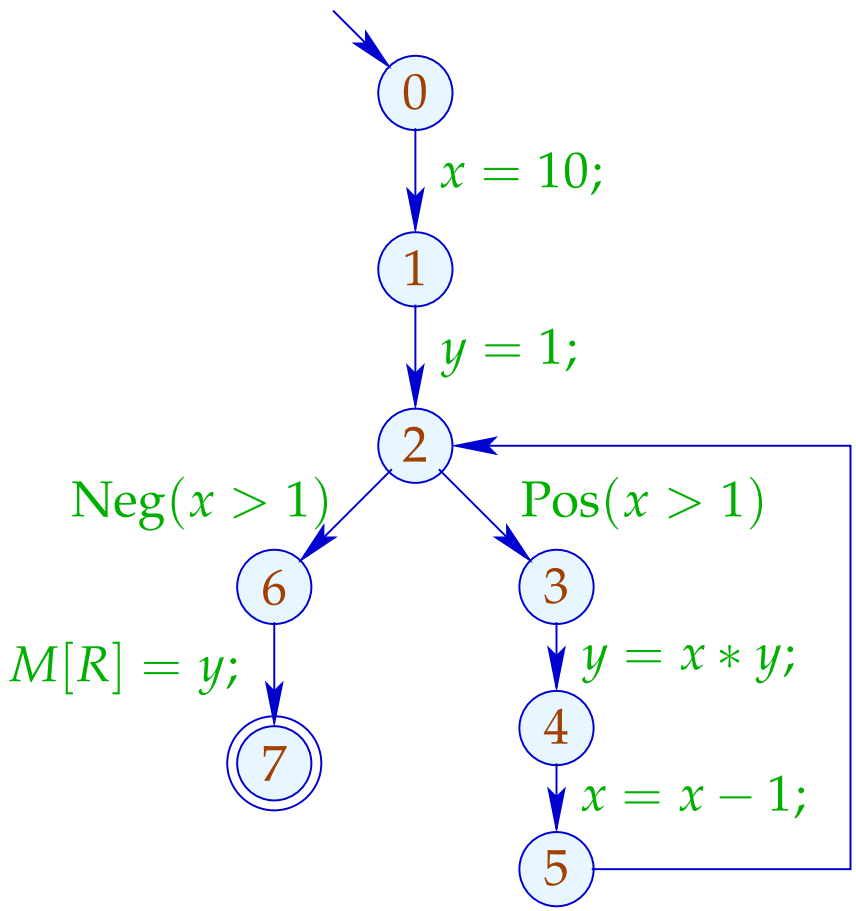
$$([\![\pi]\!]\, s) \;\Delta\; (\mathcal{D}^*[v])$$

Zur Approximation des MOP benutzen wir unser Constraint-System :-))

Beispiel:

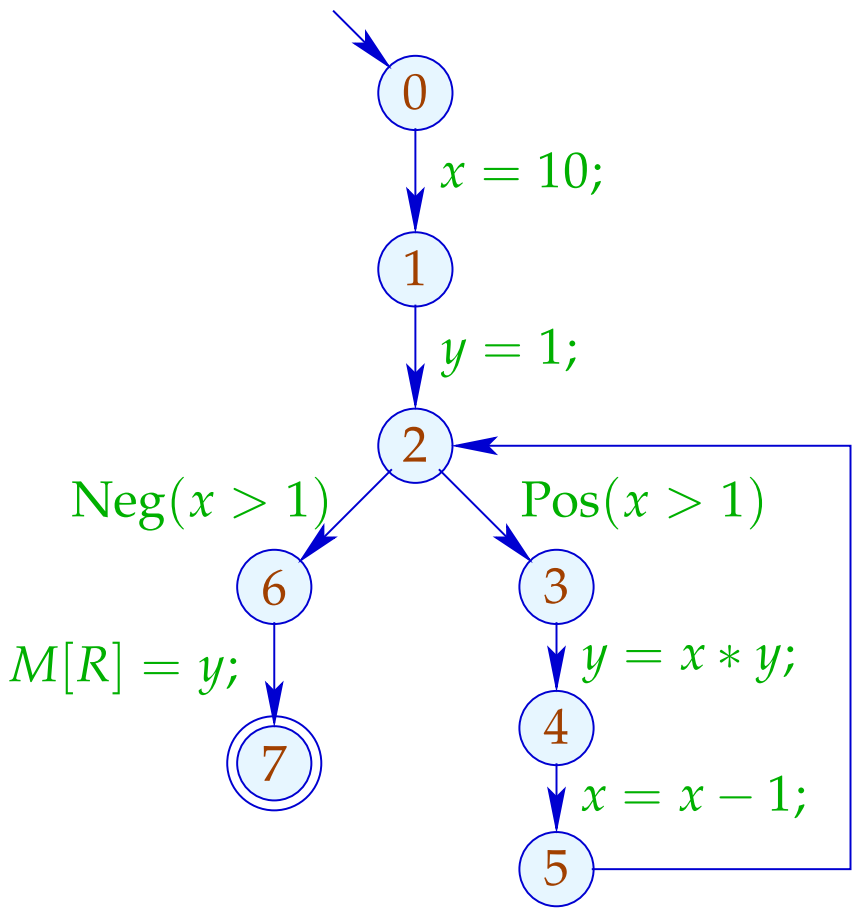


Beispiel:



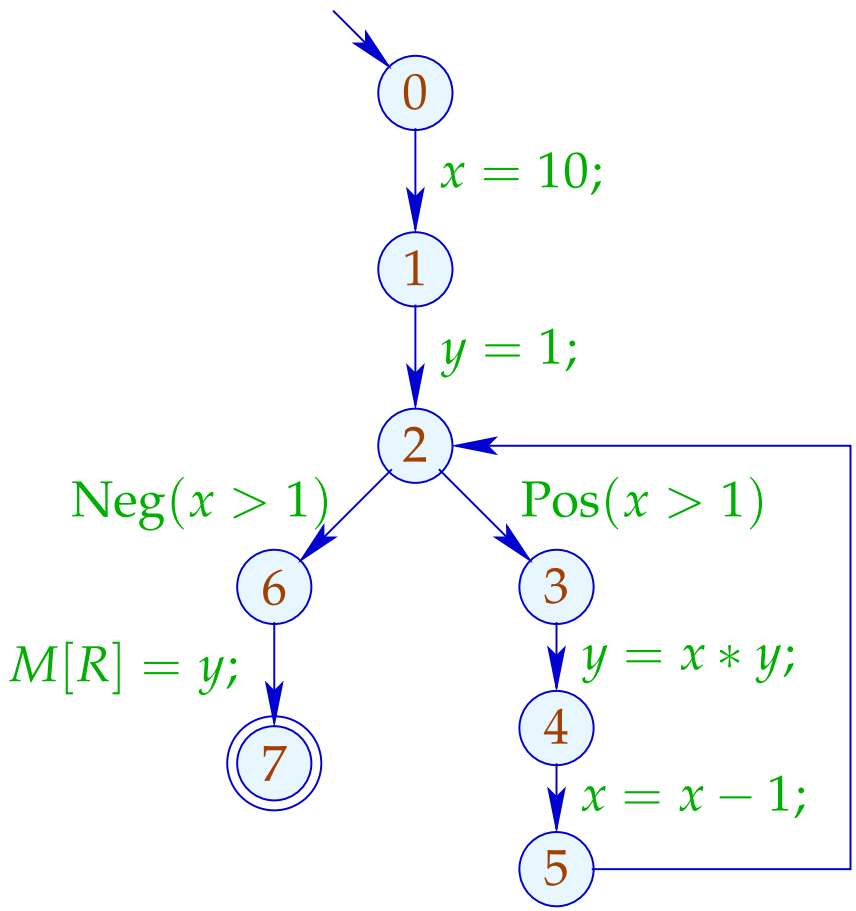
	1	
	x	y
0	$\top$	$\top$
1	10	$\top$
2	10	1
3	10	1
4	10	10
5	9	10
6	$\bot$	
7	$\bot$	

Beispiel:



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

Beispiel:



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

Fazit:

Obwohl wir mit konkreten Zahlen rechnen, kriegen wir nicht alles raus :-(

Dafür terminiert die Fixpunkt-Iteration garantiert:

Für n Programmpunkte und m Variablen benötigen wir maximal: $n \cdot (m + 1)$ Runden :-)

Achtung:

Die Kanten-Effekte sind nicht distributiv !!!

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

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

:-((

Wir schließen:

Die kleinste Lösung $\mathcal{D}$ des Constraint-Systems liefert i.a. nur eine obere Approximation des MOP, d.h.:

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

Wir schließen:

Die kleinste Lösung $\mathcal{D}$ des Constraint-Systems liefert i.a. nur eine obere Approximation des MOP, d.h.:

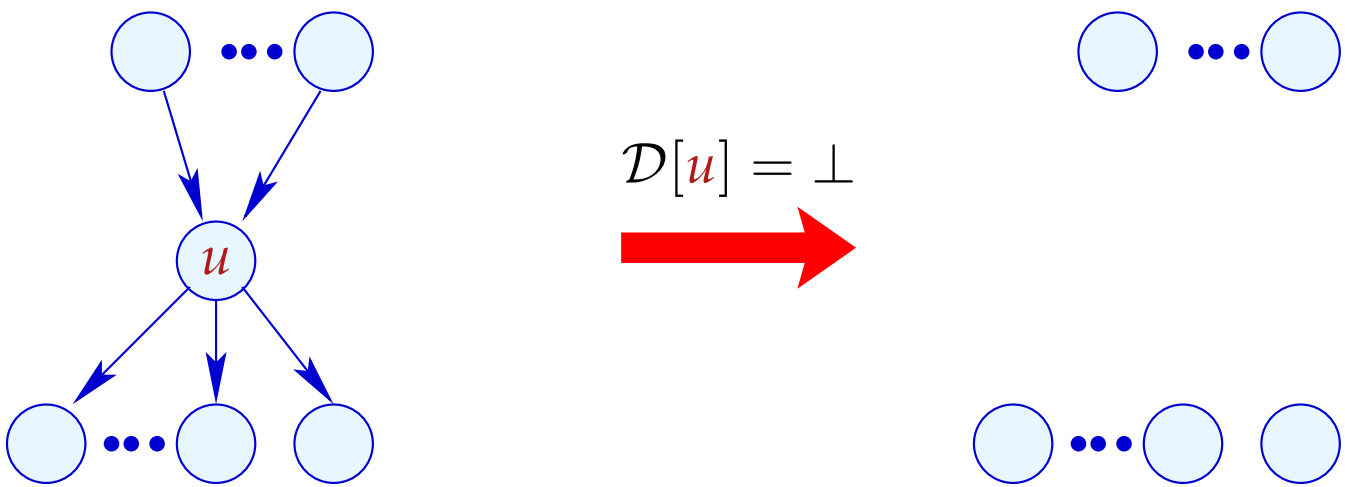
$$\mathcal{C}^*[v] \quad \sqsubseteq \quad \mathcal{C}[v]$$

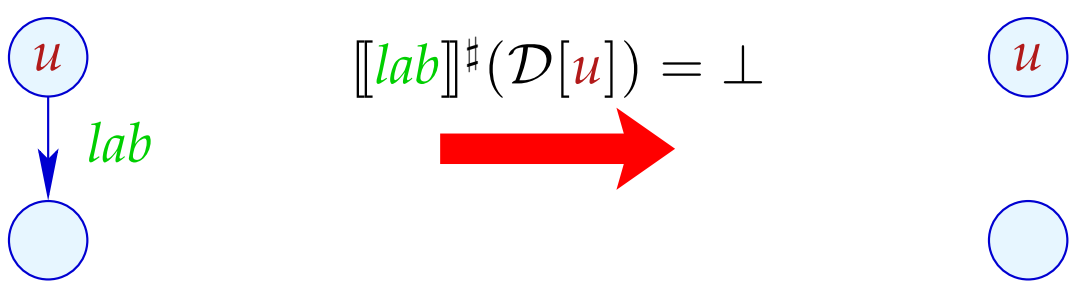
Als obere Approximation beschreibt $\mathcal{C}[v]$ trotzdem das Ergebnis jeder Berechnung π, die in v endet:

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

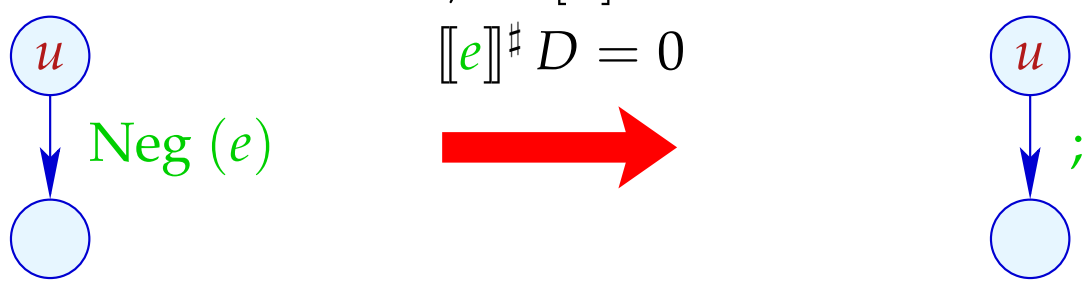
wann immer $\llbracket \pi \rrbracket\,(\rho, \mu)$ definiert ist ;-))

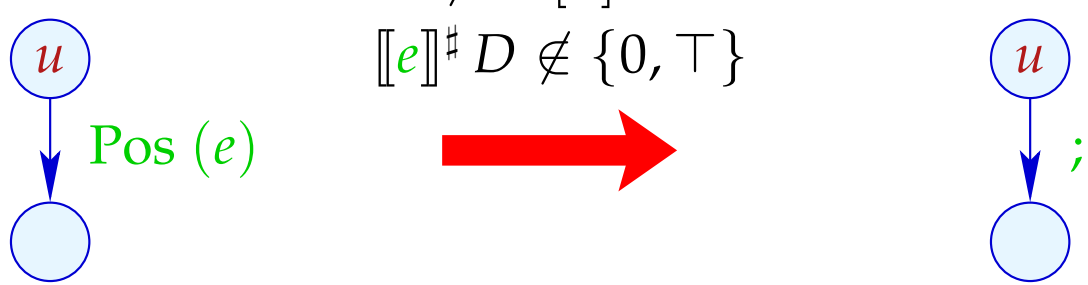
Transformation 5: Beseitigung von totem Code



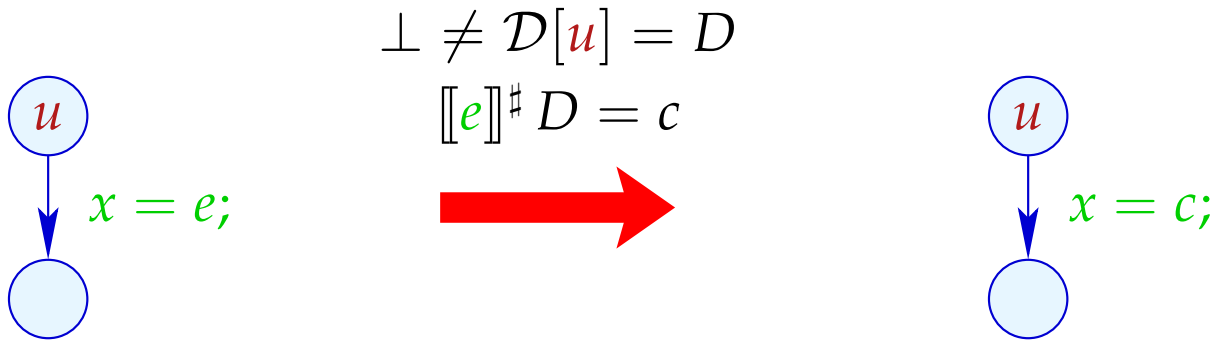


Transformation 5 (Forts.): Beseitigung von totem Code





Transformation 5 (Forts.): Vereinfachte Zuweisungen



Erweiterungen:

- Statt ganzer rechter Seiten kann man auch Teilausdrücke vereinfachen:

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

... und weitere Vereinfachungsregeln anwenden, etwa:

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

$$\ldots$$

- Bisher haben wir die Information von Bedingungen nicht optimal ausgenutzt:

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

Selbst wenn wir den Wert von x vor der if-Abfrage nicht kennen, wissen wir doch, dass bei Betreten des then-Teils x stets den Wert 7 hat :-)

Wir könnten darum definieren:

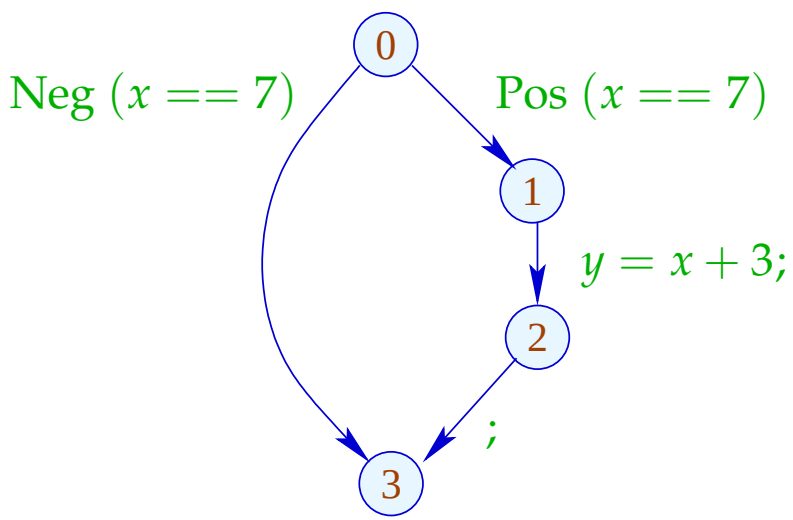
$$[\![\text{Pos}\,(x == e)]\!]^\sharp\, D = \begin{cases} D & \text{falls} \quad [\![x == e]\!]^\sharp\, D = 1 \\ \bot & \text{falls} \quad [\![x == e]\!]^\sharp\, D = 0 \\ D_1 & \text{sonst} \end{cases}$$

wobei

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

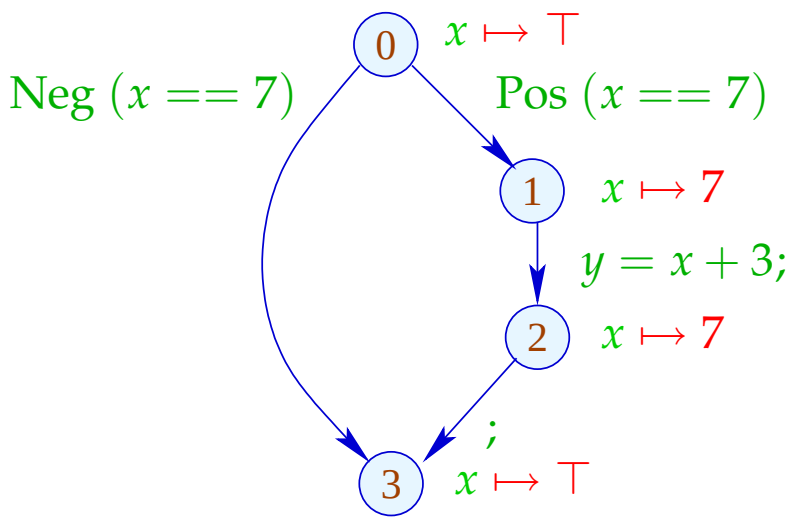
Analog sieht der Kanteneffekt für $\text{Neg}\,(x \neq e)$ aus :-)

Unser Beispiel:



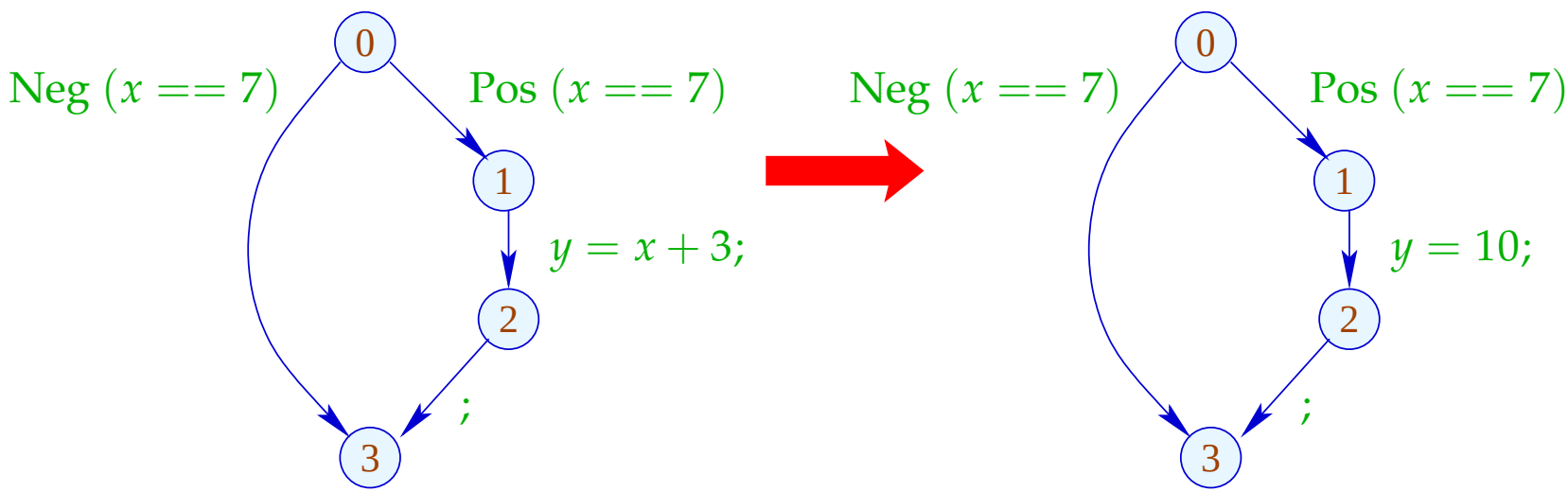
Analog sieht der Kanteneffekt für $\text{Neg}\,(x \neq e)$ aus :-)

Unser Beispiel:



Analog sieht der Kanteneffekt für $\text{Neg}\,(x \neq e)$ aus :-)

Unser Beispiel:



1.5 Intervall-Analyse

Beobachtung:

- Programmiererinnen benutzen oft globale Konstanten, um Debug-Code ein oder aus zu schalten

  $\Longrightarrow$

  Konstantenpropagation ist hilfreich :-)

- Im allgemeinen wird aber der Wert von Variablen nicht bekannt sein — möglicherweise aber ein Intervall !!!

Beispiel:

$$
\begin{array}{l}
\text{for } (i = 0; i < 42; i{+}{+}) \\
\quad \text{if } (0 \leq i \wedge i < 42)\{ \\
\qquad A_1 = A + i; \\
\qquad M[A_1] = i; \\
\quad \} \\
\quad // \quad A \text{ Anfangsadresse eines Felds} \\
\quad // \quad \text{if ist Array-Bound-Check}
\end{array}
$$

Offenbar ist die innere Abfrage überflüssig :-)

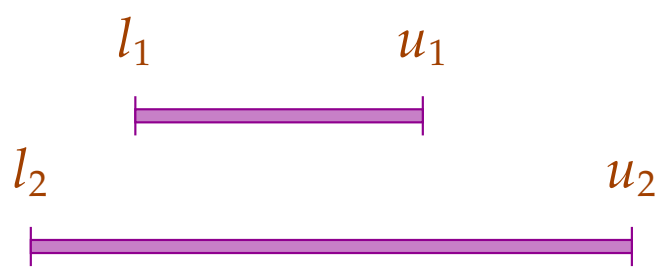
Idee 1:

Bestimme für jede Variable x ein (möglichst kleines :-) Intervall für die möglichen Werte:

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

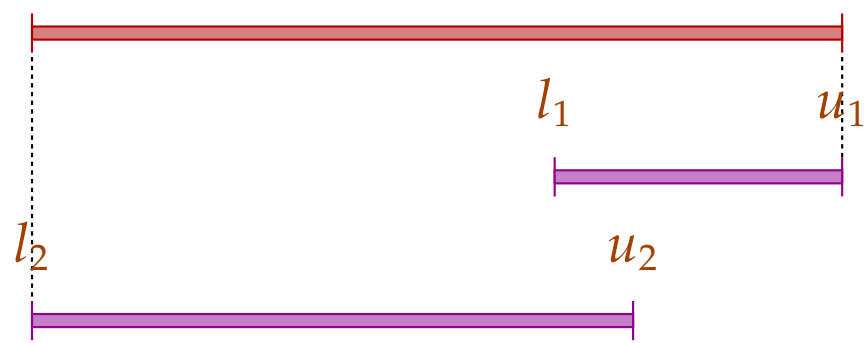
Partielle Ordnung:

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



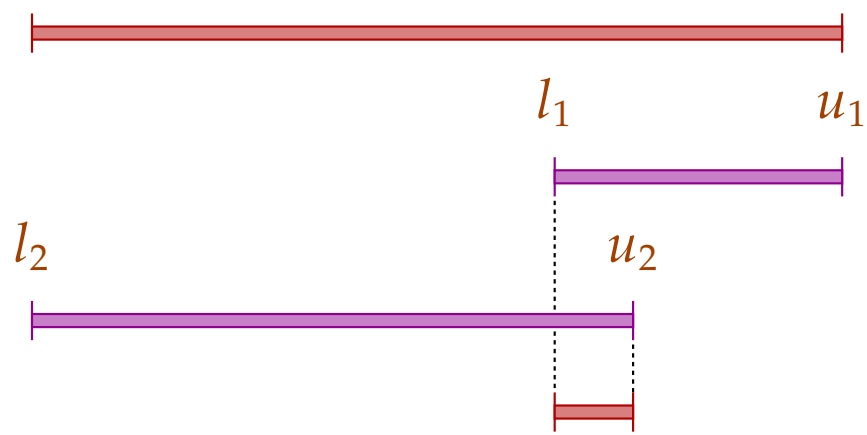
Damit:

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



Damit:

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



Achtung:

$\rightarrow$ $\mathbb{I}$ ist kein vollständiger Verband :-)

$\rightarrow$ $\mathbb{I}$ besitzt unendliche aufsteigende Ketten, z.B.

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

Achtung:

$\rightarrow$ $\mathbb{I}$ ist kein vollständiger Verband :-)

$\rightarrow$ $\mathbb{I}$ besitzt unendliche aufsteigende Ketten, z.B.

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

Beschreibungsrelation:

$$z \;\Delta\; [l,u] \qquad \text{gdw.} \qquad l \leq z \leq u$$

Konkretisierung:

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

Beispiel:

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

Rechnen mit Intervallen: Intervall-Arithmetik :-)

Addition:

$$\begin{aligned} [l_1,u_1] +^\sharp [l_2,u_2] &= [l_1+l_2, u_1+u_2] \qquad \text{wobei} \\ -\infty + _ &= -\infty \\ +\infty + _ &= +\infty \\ // \quad & -\infty + \infty \quad \text{kommt nicht vor} \quad \text{:-)} \end{aligned}$$

Negation:

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

Multiplikation:

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

Beispiel:

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

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

- Ist 0 nicht im Nenner-Intervall enthalten, sei:

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

- Gilt: $l_2 \leq 0 \leq u_2$, setzen wir:

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

Gleichheit:

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

Gleichheit:

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

Beispiel:

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