Idee:

Entwerfe eine Analyse, die für jedes u

- die Werte ermittelt, die Variablen sicher haben;
- mitteilt, ob u überhaupt erreichbar ist :-)

Idee:

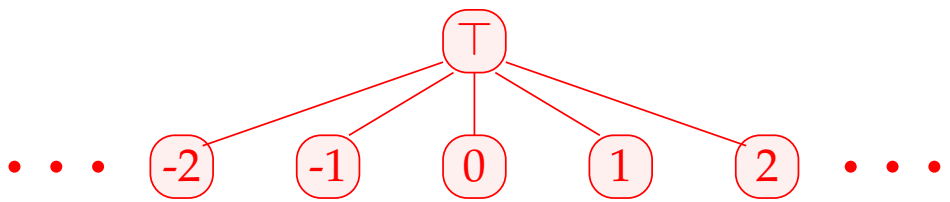
Entwerfe eine Analyse, die für jedes u

- die Werte ermittelt, die Variablen sicher haben;
- mitteilt, ob u überhaupt erreichbar ist :-)

Den vollständigen Verband konstruieren wir in zwei Schritten.

(1) Die möglichen Werte für Variablen:

$$\mathbb{Z}^\top = \mathbb{Z} \cup \{\top\} \qquad \text{mit} \quad x \sqsubseteq y \quad \text{gdw. } y = \top \text{ oder } x = y$$



Achtung: $\mathbb{Z}^\top$ ist selbst kein vollständiger Verband :-(

(2) $\mathbb{D} = (\mathit{Vars} \to \mathbb{Z}^\top)_\bot = (\mathit{Vars} \to \mathbb{Z}^\top) \cup \{\bot\}$

// $\bot$ heißt: "nicht erreichbar" :-))

mit $D_1 \sqsubseteq D_2$ gdw. $\bot = D_1$ oder

$D_1\, x \sqsubseteq D_2\, x \quad (x \in \mathit{Vars})$

Bemerkung: $\mathbb{D}$ ist ein vollständiger Verband :-)

Achtung: $\mathbb{Z}^\top$ ist selbst kein vollständiger Verband :-(

(2) $\mathbb{D} = (\mathit{Vars} \to \mathbb{Z}^\top)_\bot = (\mathit{Vars} \to \mathbb{Z}^\top) \cup \{\bot\}$

// $\bot$ heißt: "nicht erreichbar" :-))

mit $D_1 \sqsubseteq D_2$ gdw. $\bot = D_1$ oder

$D_1\, x \sqsubseteq D_2\, x \quad (x \in \mathit{Vars})$

Bemerkung: $\mathbb{D}$ ist ein vollständiger Verband :-)

Betrachte dazu $X \subseteq \mathbb{D}$. O.E. $\bot \notin X$.

Dann $X \subseteq \mathit{Vars} \to \mathbb{Z}^\top$.

Ist $X = \emptyset$, dann $\bigsqcup X = \bot \in \mathbb{D}$:-)

Ist $X \neq \emptyset$, dann ist $\bigsqcup X = D$ mit

$$
\begin{aligned}
D\,x &= \bigsqcup\{f\,x \mid f \in X\} \\
&= \begin{cases} z & \text{falls} \quad f\,x = z \quad (f \in X) \\ \top & \text{sonst} \end{cases}
\end{aligned}
$$

:-))

Ist $X \neq \emptyset$, dann ist $\bigsqcup X = D$ mit

$$
\begin{aligned}
D\,x &= \bigsqcup\{f\,x \mid f \in X\} \\
&= \begin{cases} z & \text{falls} \quad f\,x = z \quad (f \in X) \\ \top & \text{sonst} \end{cases}
\end{aligned}
$$

:-))

Zu jeder Kante $k = (_, lab, _)$ konstruieren wir eine Effekt-Funktion $[\![k]\!]^\sharp = [\![lab]\!]^\sharp : \mathbb{D} \to \mathbb{D}$, die die konkrete Berechnung simuliert.

Offenbar ist $[\![lab]\!]^\sharp \bot = \bot$ für alle lab :-)

Sei darum nun $\bot \neq D \in Vars \to \mathbb{Z}^\top$.

Idee:

- Wir benutzen D, um die Werte von Ausdrücken zu ermitteln.

Idee:

- Wir benutzen D, um die Werte von Ausdrücken zu ermitteln.
- Für manche Teilausdrücke erhalten wir $\top$:-)

Idee:

- Wir benutzen D, um die Werte von Ausdrücken zu ermitteln.
- Für manche Teilausdrücke erhalten wir $\top$:-)

  $\Longrightarrow$

  Wir müssen die konkreten Operatoren $\Box$ durch abstrakte Operatoren $\Box^\sharp$ ersetzen, die mit $\top$ umgehen können:

$$a \,\Box^\sharp\, b = \begin{cases} \top & \text{falls} \quad a = \top \text{ oder } b = \top \\ a \,\Box\, b & \text{sonst} \end{cases}$$

Idee:

- Wir benutzen D, um die Werte von Ausdrücken zu ermitteln.
- Für manche Teilausdrücke erhalten wir $\top$:-)

  $\Longrightarrow$

  Wir müssen die konkreten Operatoren $\Box$ durch abstrakte Operatoren $\Box^\sharp$ ersetzen, die mit $\top$ umgehen können:

$$a \,\Box^\sharp\, b = \begin{cases} \top & \text{falls} \quad a = \top \text{ oder } b = \top \\ a \,\Box\, b & \text{sonst} \end{cases}$$

- Mit den abstrakten Operatoren können wir eine abstrakte Ausdrucks-Auswertung definieren:

$$[\![e]\!]^\sharp \;:\; (\mathit{Vars} \to \mathbb{Z}^\top) \to \mathbb{Z}^\top$$

Abstrakte Ausdrucksauswertung ist wie konkrete Ausdrucksauswertung, aber mit abstrakten Werten und Operatoren. Hier:

$$\begin{aligned} [\![c]\!]^\sharp D &= c \\ [\![e_1 \,\square\, e_2]\!]^\sharp D &= [\![e_1]\!]^\sharp D \,\square^\sharp\, [\![e_2]\!]^\sharp D \end{aligned}$$

... analog für unäre Operatoren :-)

Abstrakte Ausdrucksauswertung ist wie konkrete Ausdrucksauswertung, aber mit abstrakten Werten und Operatoren. Hier:

$$\begin{aligned} [\![c]\!]^\sharp D &= c \\ [\![e_1 \,\square\, e_2]\!]^\sharp D &= [\![e_1]\!]^\sharp D \,\square^\sharp\, [\![e_2]\!]^\sharp D \end{aligned}$$

... analog für unäre Operatoren :-)

Beispiel: $D = \{x \mapsto 2, y \mapsto \top\}$

$$\begin{aligned} [\![x + 7]\!]^\sharp D &= [\![x]\!]^\sharp D \,+^\sharp\, [\![7]\!]^\sharp D \\ &= 2 \,+^\sharp\, 7 \\ &= 9 \end{aligned}$$

$$\begin{aligned} [\![x - y]\!]^\sharp D &= 2 \,-^\sharp\, \top \\ &= \top \end{aligned}$$

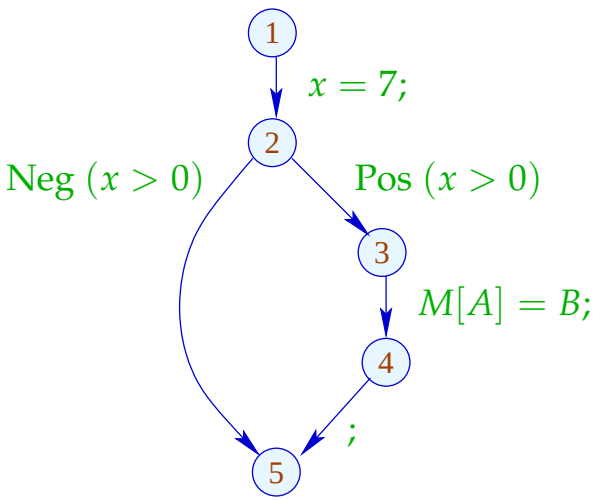
Damit erhalten wir für die Kanten-Effekte $[\![lab]\!]^\sharp$:

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

... sofern $D \neq \bot$:-)

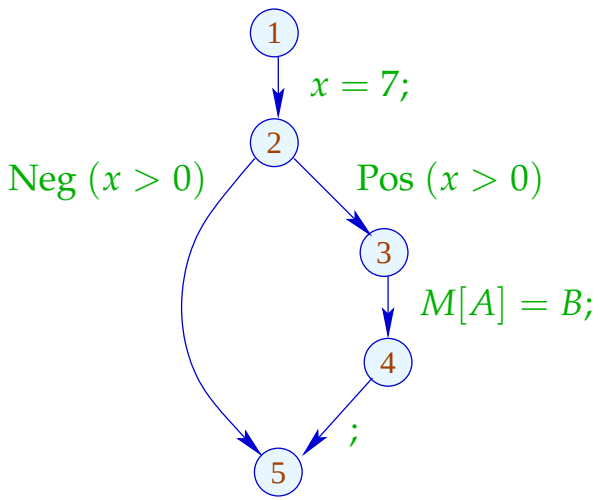
An *start* gilt $D_\perp = \{x \mapsto \top \mid x \in \mathit{Vars}\}$.

Beispiel:



An *start* gilt $D_\perp = \{x \mapsto \top \mid x \in \mathit{Vars}\}$.

Beispiel:



1	$\{x \mapsto \top\}$
2	$\{x \mapsto 7\}$
3	$\{x \mapsto 7\}$
4	$\{x \mapsto 7\}$
5	$\perp \sqcup \{x \mapsto 7\} = \{x \mapsto 7\}$

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

Patrick Cousot, ENS, Paris

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

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

Konkretisierung:

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

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

(3) Zustände:

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

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

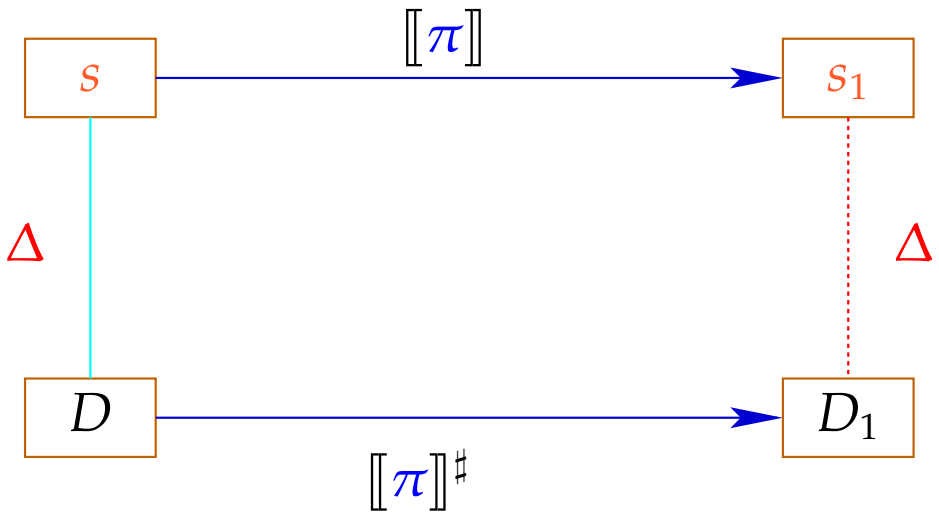
Konkretisieruing:

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

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 :-)

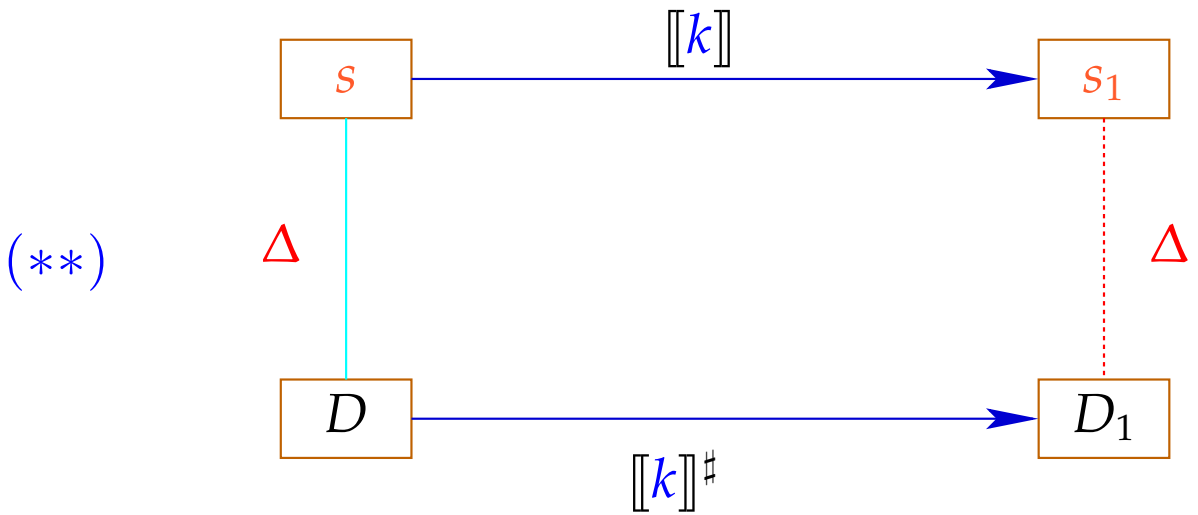
Insbesondere gilt:

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

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 :



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 $\square$:

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

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

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

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

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

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

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

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:

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

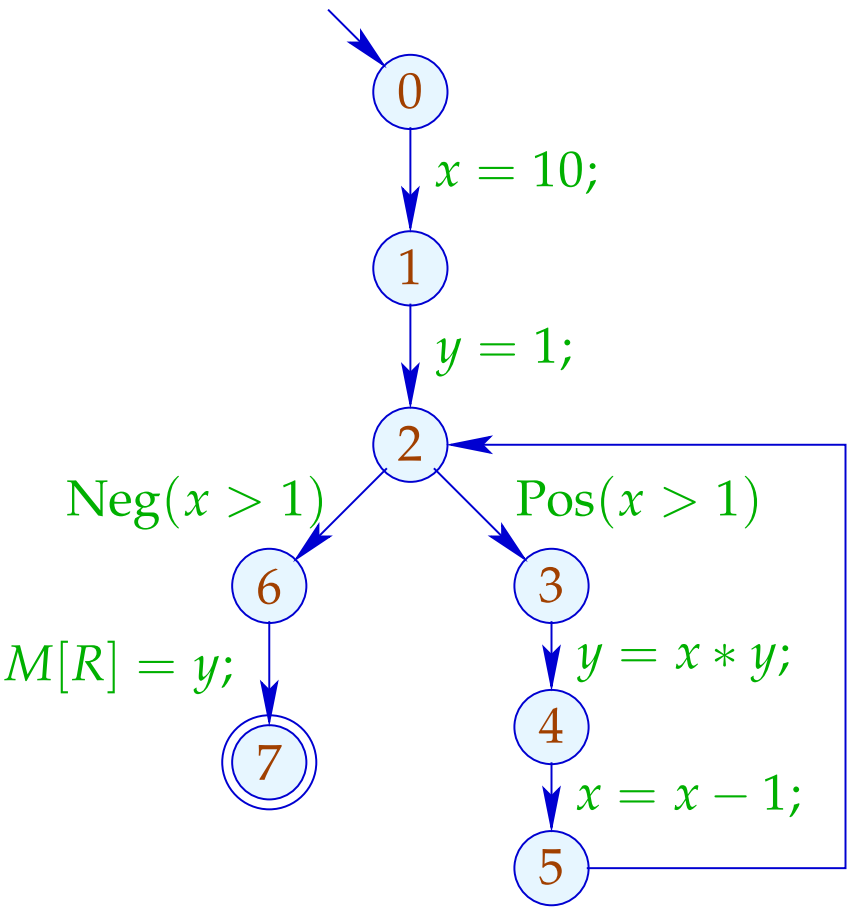
wobei $D_0\, x = \top \qquad (x \in \mathit{Vars})$.

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

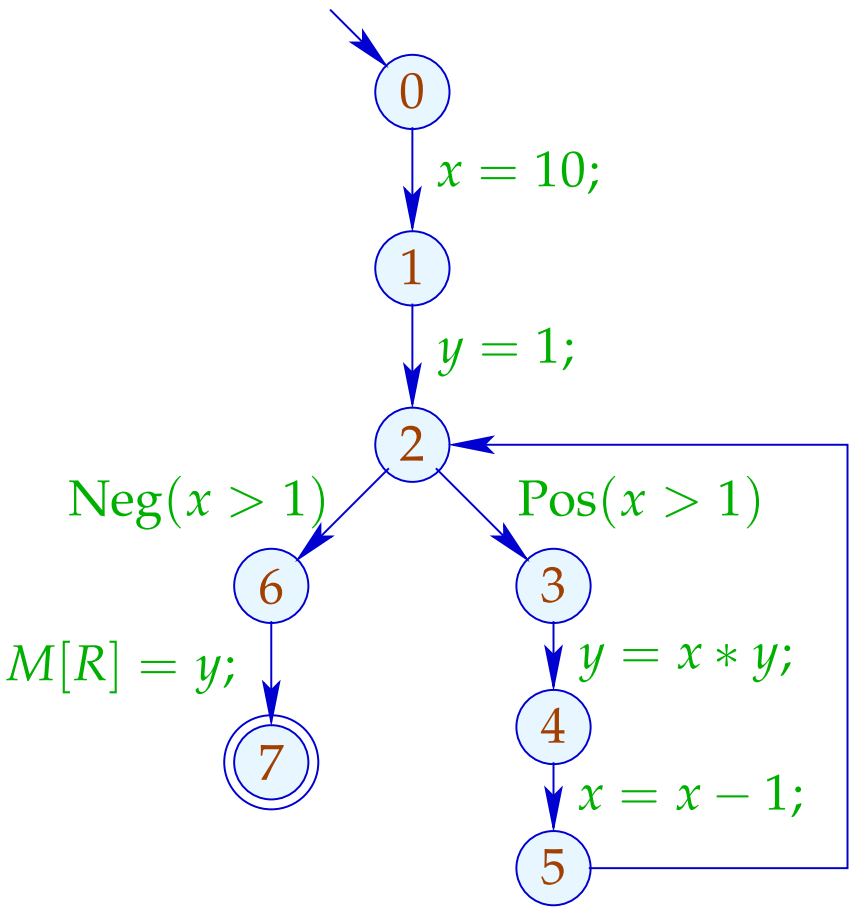
$$([\![\pi]\!]\, s) \;\Delta\; (\mathcal{D}^*[v])$$

Zur Approximation des MOP benutzen wir unser Ungleichungssystem :-))

Beispiel:

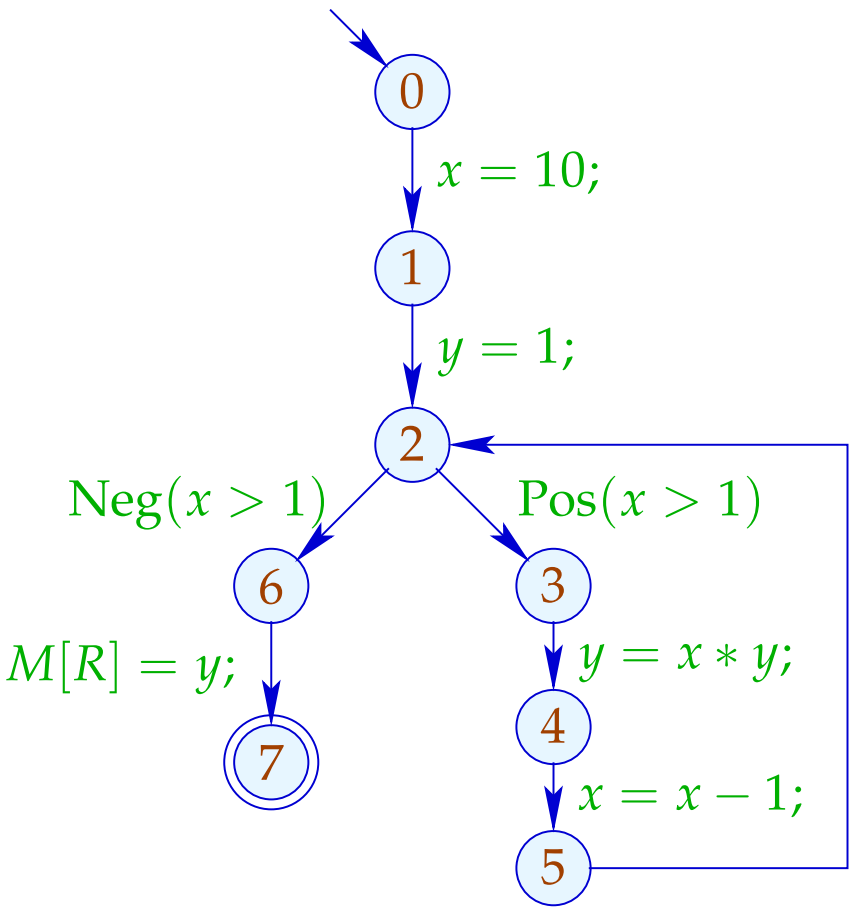


Beispiel:



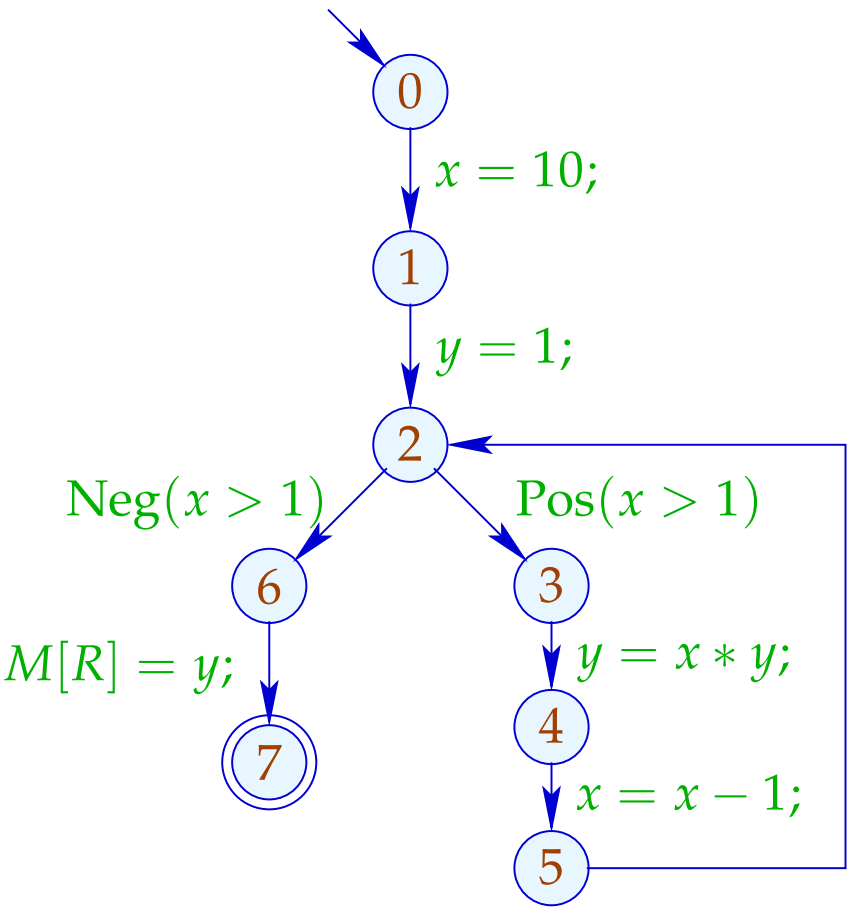
	1	
	x	y
0	$\top$	$\top$
1	10	$\top$
2	10	1
3	10	1
4	10	10
5	9	10
6	$\bot$	
7	$\bot$	

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 Ungleichungssystems liefert i.a. nur eine obere Approximation des MOP, d.h.:

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

Wir schließen:

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

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

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

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

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