Question:

How can we compute $\mathcal{A}[u]$ for every program point u ??

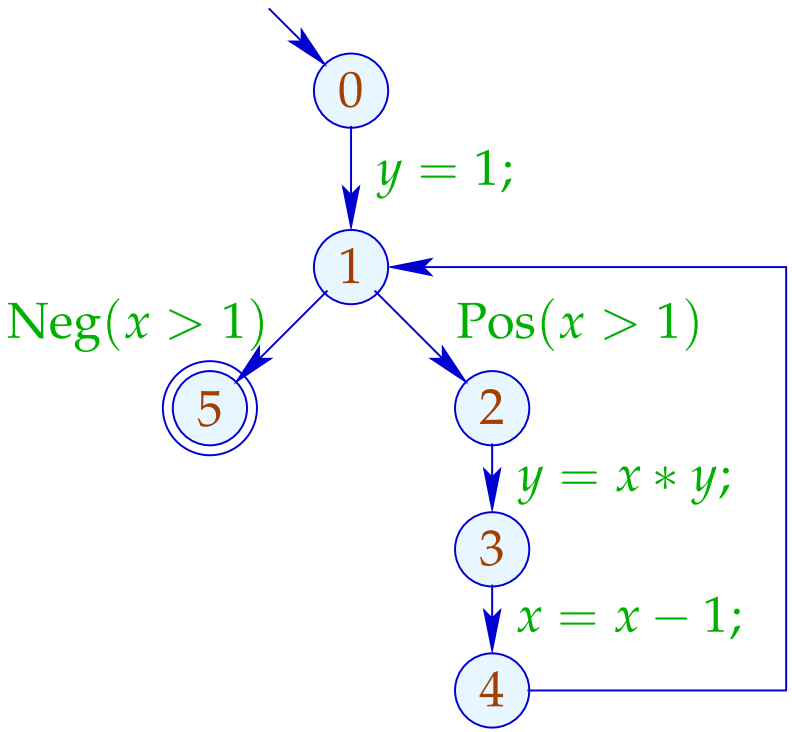
We collect all restrictions to the values of $\mathcal{A}[u]$ into a system of constraints:

$$\begin{array}{lcll} \mathcal{A}[start] & \subseteq & \emptyset & \\ \mathcal{A}[v] & \subseteq & [\![k]\!]^\sharp\,(\mathcal{A}[u]) & k = (u, _, v) \quad \text{edge} \end{array}$$

Wanted:

- a maximally large solution (??)
- an algorithm which computes this :-)

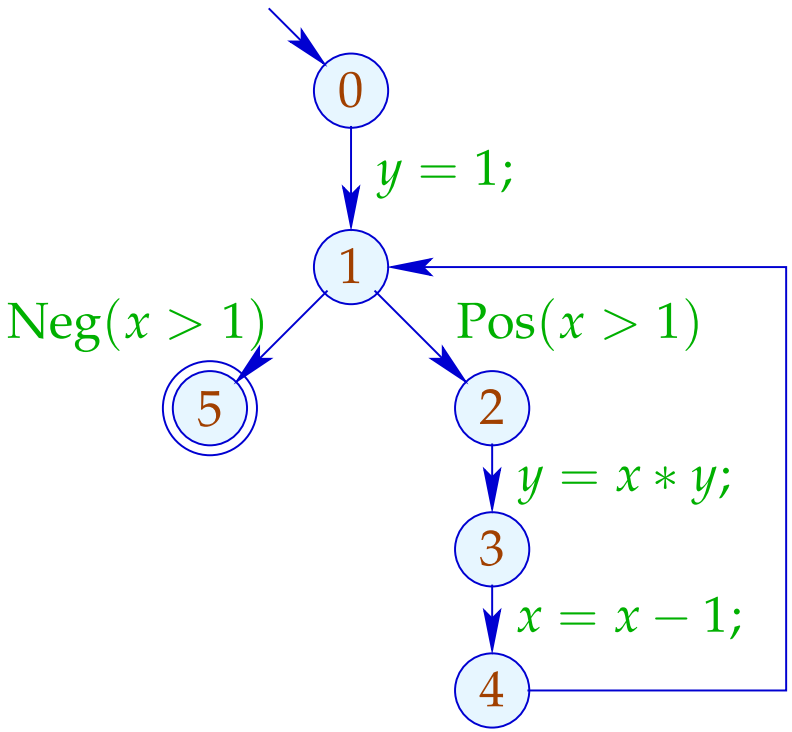
Example:



Wanted:

- a maximally large solution (??)
- an algorithm which computes this :-)

Example:

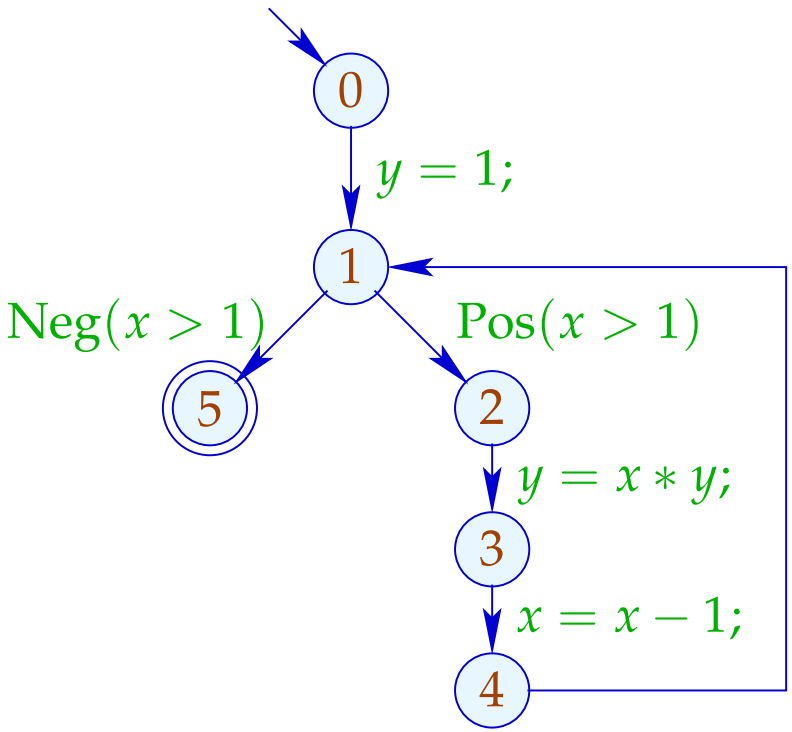


$$\mathcal{A}[0] \quad \subseteq \quad \emptyset$$

Wanted:

- a maximally large solution (??)
- an algorithm which computes this :-)

Example:

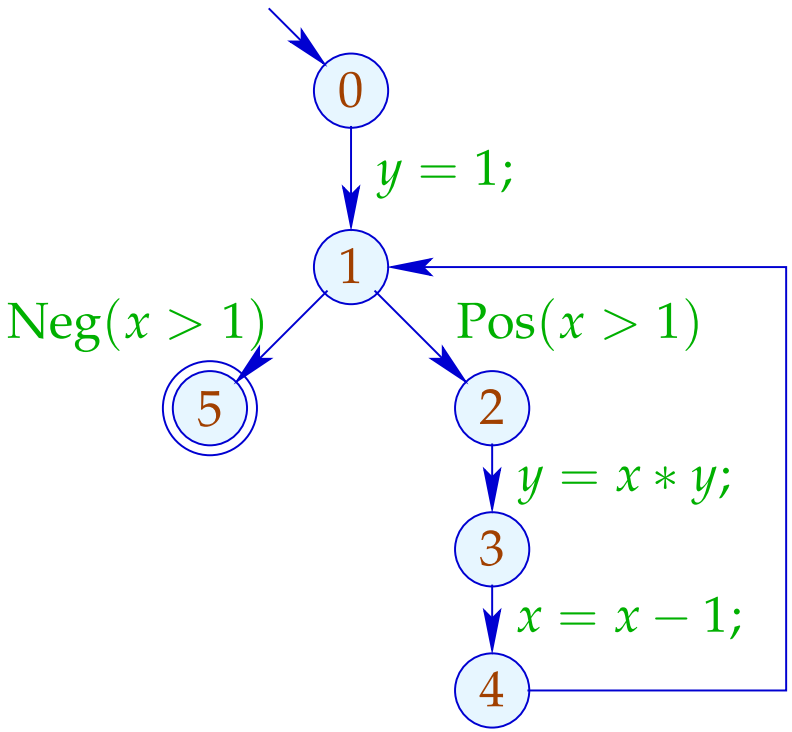


$$\begin{aligned} \mathcal{A}[0] &\subseteq \emptyset \\ \mathcal{A}[1] &\subseteq (\mathcal{A}[0] \cup \{1\}) \backslash Expr_y \\ \mathcal{A}[1] &\subseteq \mathcal{A}[4] \end{aligned}$$

Wanted:

- a maximally large solution (??)
- an algorithm which computes this :-)

Example:

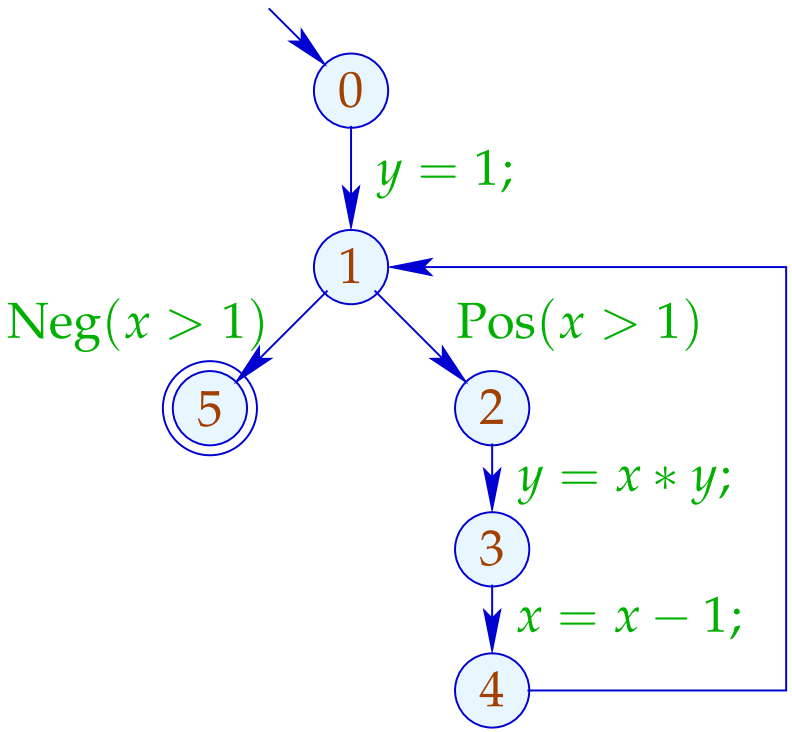


$$
\begin{aligned}
\mathcal{A}[0] &\subseteq \emptyset \\
\mathcal{A}[1] &\subseteq (\mathcal{A}[0] \cup \{1\}) \backslash Expr_y \\
\mathcal{A}[1] &\subseteq \mathcal{A}[4] \\
\mathcal{A}[2] &\subseteq \mathcal{A}[1] \cup \{x > 1\}
\end{aligned}
$$

Wanted:

- a maximally large solution (??)
- an algorithm which computes this :-)

Example:

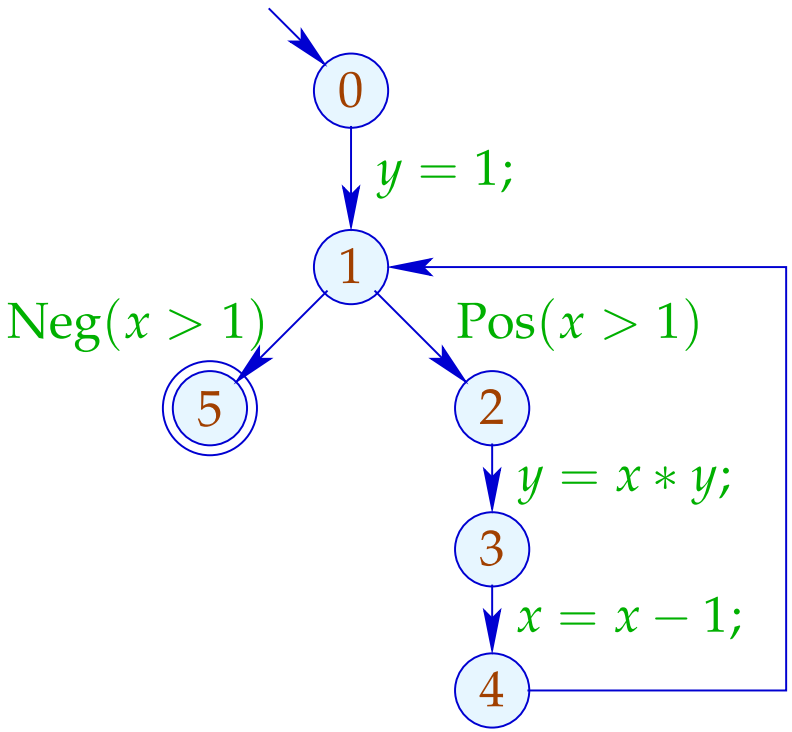


$$
\begin{aligned}
\mathcal{A}[0] &\subseteq \emptyset \\
\mathcal{A}[1] &\subseteq (\mathcal{A}[0] \cup \{1\}) \backslash Expr_y \\
\mathcal{A}[1] &\subseteq \mathcal{A}[4] \\
\mathcal{A}[2] &\subseteq \mathcal{A}[1] \cup \{x > 1\} \\
\mathcal{A}[3] &\subseteq (\mathcal{A}[2] \cup \{x * y\}) \backslash Expr_y
\end{aligned}
$$

Wanted:

- a maximally large solution (??)
- an algorithm which computes this :-)

Example:

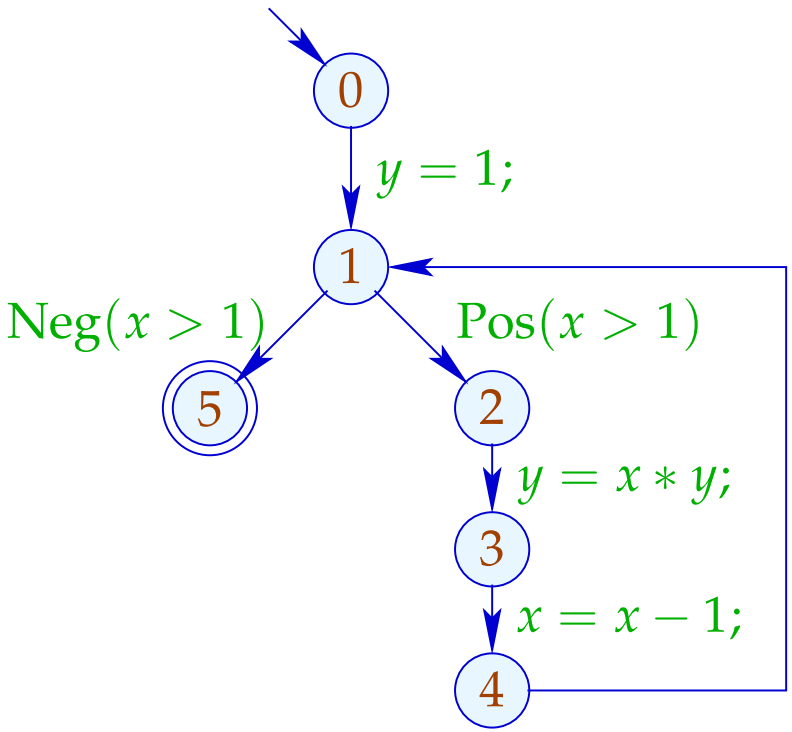


$$
\begin{aligned}
\mathcal{A}[0] &\subseteq \emptyset \\
\mathcal{A}[1] &\subseteq (\mathcal{A}[0] \cup \{1\}) \backslash Expr_y \\
\mathcal{A}[1] &\subseteq \mathcal{A}[4] \\
\mathcal{A}[2] &\subseteq \mathcal{A}[1] \cup \{x > 1\} \\
\mathcal{A}[3] &\subseteq (\mathcal{A}[2] \cup \{x * y\}) \backslash Expr_y \\
\mathcal{A}[4] &\subseteq (\mathcal{A}[3] \cup \{x - 1\}) \backslash Expr_x
\end{aligned}
$$

Wanted:

- a maximally large solution (??)
- an algorithm which computes this :-)

Example:

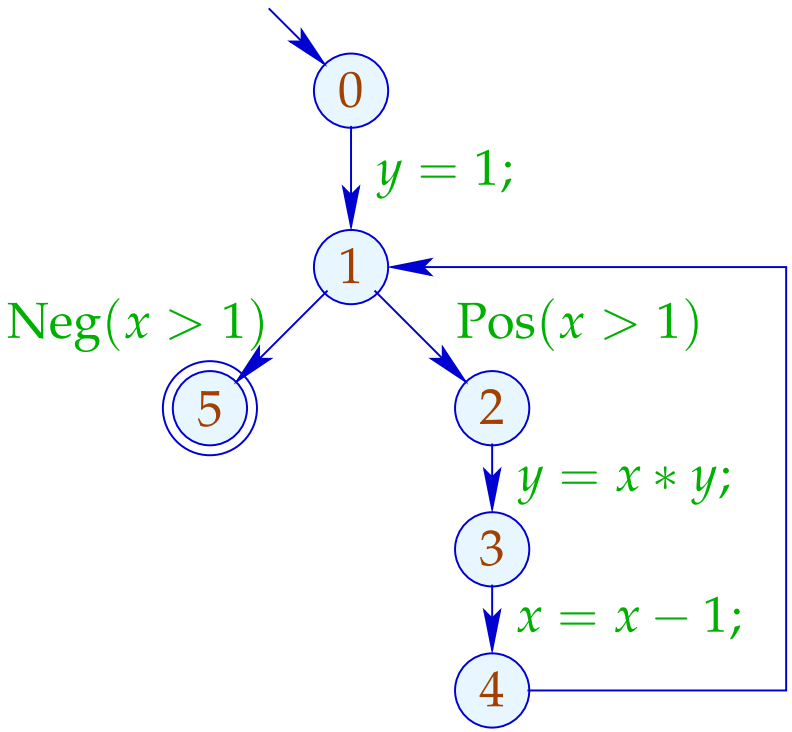


$$
\begin{array}{lcl}
\mathcal{A}[0] & \subseteq & \emptyset \\
\mathcal{A}[1] & \subseteq & (\mathcal{A}[0] \cup \{1\}) \backslash Expr_y \\
\mathcal{A}[1] & \subseteq & \mathcal{A}[4] \\
\mathcal{A}[2] & \subseteq & \mathcal{A}[1] \cup \{x > 1\} \\
\mathcal{A}[3] & \subseteq & (\mathcal{A}[2] \cup \{x * y\}) \backslash Expr_y \\
\mathcal{A}[4] & \subseteq & (\mathcal{A}[3] \cup \{x - 1\}) \backslash Expr_x \\
\mathcal{A}[5] & \subseteq & \mathcal{A}[1] \cup \{x > 1\}
\end{array}
$$

Wanted:

- a maximally large solution (??)
- an algorithm which computes this :-)

Example:



Solution:

$$
\begin{aligned}
\mathcal{A}[0] &= \emptyset \\
\mathcal{A}[1] &= \{1\} \\
\mathcal{A}[2] &= \{1, x > 1\} \\
\mathcal{A}[3] &= \{1, x > 1\} \\
\mathcal{A}[4] &= \{1\} \\
\mathcal{A}[5] &= \{1, x > 1\}
\end{aligned}
$$

Observation:

- The possible values for $\mathcal{A}[u]$ form a complete lattice:

$$\mathbb{D} = 2^{Expr} \quad \text{with} \quad B_1 \sqsubseteq B_2 \quad \text{iff} \quad B_1 \supseteq B_2$$

Observation:

- The possible values for $\mathcal{A}[u]$ form a complete lattice:

$$\mathbb{D} = 2^{Expr} \quad \text{with} \quad B_1 \sqsubseteq B_2 \quad \text{iff} \quad B_1 \supseteq B_2$$

- The functions $[\![k]\!]^\sharp : \mathbb{D} \to \mathbb{D}$ are monotonic, i.e.,

$$[\![k]\!]^\sharp(B_1) \sqsubseteq [\![k]\!]^\sharp(B_2) \quad \text{iff} \quad B_1 \sqsubseteq B_2$$

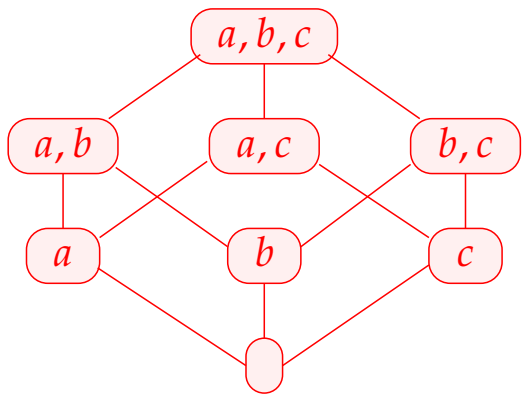
Background 2: complete Lattices

A set $\mathbb{D}$ together with a relation $\sqsubseteq \subseteq \mathbb{D} \times \mathbb{D}$ is a partial order if for all $a, b, c \in \mathbb{D}$,

$$
\begin{array}{lll}
a \sqsubseteq a & & \textit{reflexivity} \\
a \sqsubseteq b \wedge b \sqsubseteq a & \Longrightarrow \; a = b & \textit{anti-symmetry} \\
a \sqsubseteq b \wedge b \sqsubseteq c & \Longrightarrow \; a \sqsubseteq c & \textit{transitivity}
\end{array}
$$

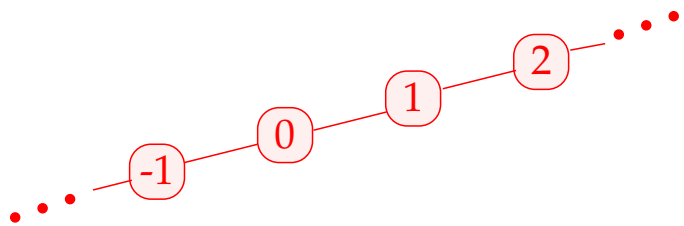
Examples:

1. $\mathbb{D} = 2^{\{a,b,c\}}$ with the relation "$\subseteq$" :

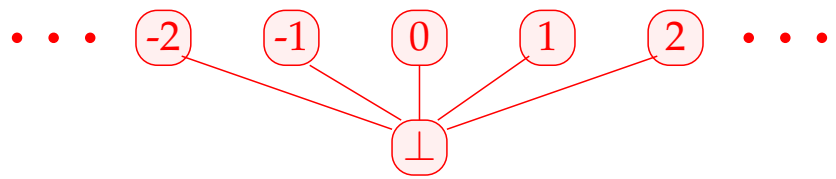


3. $\mathbb{Z}$ with the relation "$=$" :

3. $\mathbb{Z}$ with the relation "$\leq$" :



4. $\mathbb{Z}_\perp = \mathbb{Z} \cup \{\perp\}$ with the ordering:



$d \in \mathbb{D}$ is called upper bound for $X \subseteq \mathbb{D}$ if

$$x \sqsubseteq d \qquad \text{for all } x \in X$$

$d \in \mathbb{D}$ is called upper bound for $X \subseteq \mathbb{D}$ if

$$x \sqsubseteq d \qquad \text{for all } x \in X$$

d is called least upper bound (lub) if

1. d is an upper bound and
2. $d \sqsubseteq y$ for every upper bound y of X.

$d \in \mathbb{D}$ is called upper bound for $X \subseteq \mathbb{D}$ if

$$x \sqsubseteq d \qquad \text{for all } x \in X$$

d is called least upper bound (lub) if

1. d is an upper bound and
2. $d \sqsubseteq y$ for every upper bound y of X.

Warning:

- $\{0, 2, 4, \ldots\} \subseteq \mathbb{Z}$ has no upper bound!
- $\{0, 2, 4\} \subseteq \mathbb{Z}$ has the upper bounds $4, 5, 6, \ldots$

A complete lattice (cl) $\mathbb{D}$ is a partial ordering where every subset $X \subseteq \mathbb{D}$ has a least upper bound $\bigsqcup X \in \mathbb{D}$.

Note:

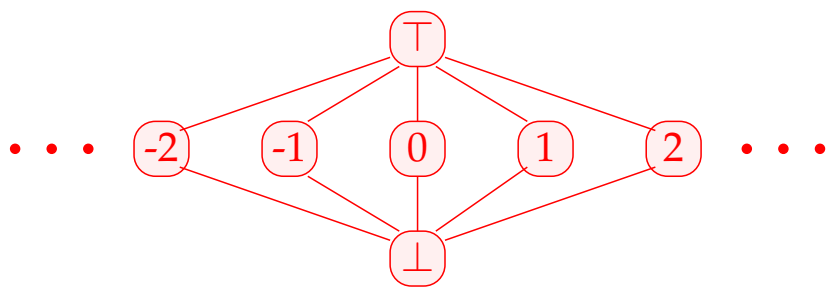
Every complete lattice has

$\rightarrow$ a least element $\bot = \bigsqcup \emptyset \in \mathbb{D}$;

$\rightarrow$ a greatest element $\top = \bigsqcup \mathbb{D} \in \mathbb{D}$.

Examples:

1. $\mathbb{D} = 2^{\{a,b,c\}}$ is a cl :-)
2. $\mathbb{D} = \mathbb{Z}$ with "$=$" is not.
3. $\mathbb{D} = \mathbb{Z}$ with "$\leq$" is neither.
4. $\mathbb{D} = \mathbb{Z}_\perp$ is also not :-(
5. With an extra element $\top$, we obtain the flat lattice $\mathbb{Z}^\top_\perp = \mathbb{Z} \cup \{\perp, \top\}$:



We have:

Theorem:

If $\mathbb{D}$ is a complete lattice, then every subset $X \subseteq \mathbb{D}$ has a greatest lower bound $\bigsqcap X$.

We have:

Theorem:

If $\mathbb{D}$ is a complete lattice, then every subset $X \subseteq \mathbb{D}$ has a greatest lower bound $\bigsqcap X$.

Proof:

Construct $U = \{u \in \mathbb{D} \mid \forall\, x \in X :\ u \sqsubseteq x\}$.

// the set of all lower bounds of X :-)

We have:

Theorem:

If $\mathbb{D}$ is a complete lattice, then every subset $X \subseteq \mathbb{D}$ has a greatest lower bound $\bigsqcap X$.

Proof:

Construct $U = \{u \in \mathbb{D} \mid \forall\, x \in X :\ u \sqsubseteq x\}$.

// the set of all lower bounds of X :-)

Set: $g := \bigsqcup U$

Claim: $g = \bigsqcap X$

(1) g is a lower bound of X :

Assume $x \in X$. Then:

$u \sqsubseteq x$ for all $u \in U$

$\Longrightarrow$ x is an upper bound of U

$\Longrightarrow$ $g \sqsubseteq x$:-)

(1) g is a lower bound of X :

Assume $x \in X$. Then:

$u \sqsubseteq x$ for all $u \in U$

$\Longrightarrow$ x is an upper bound of U

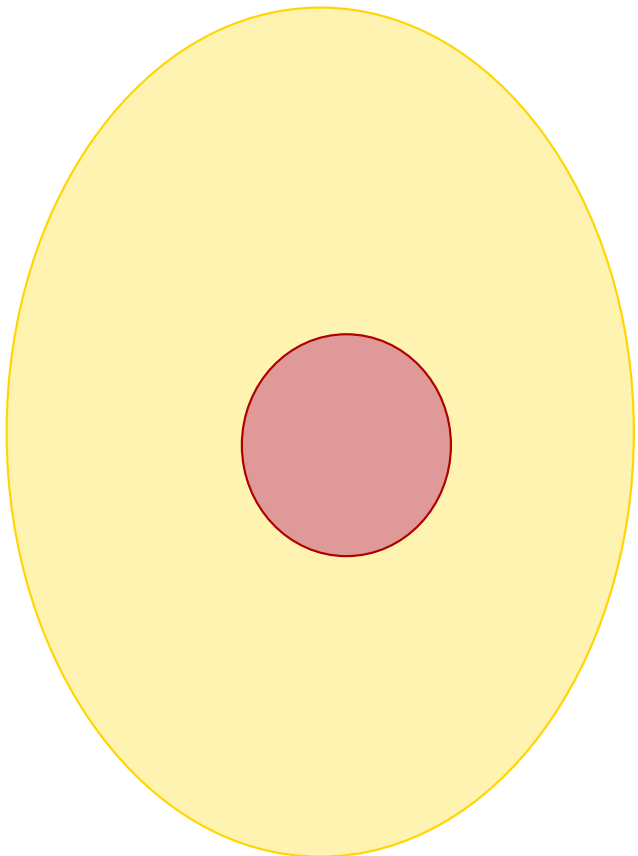
$\Longrightarrow$ $g \sqsubseteq x$:-)

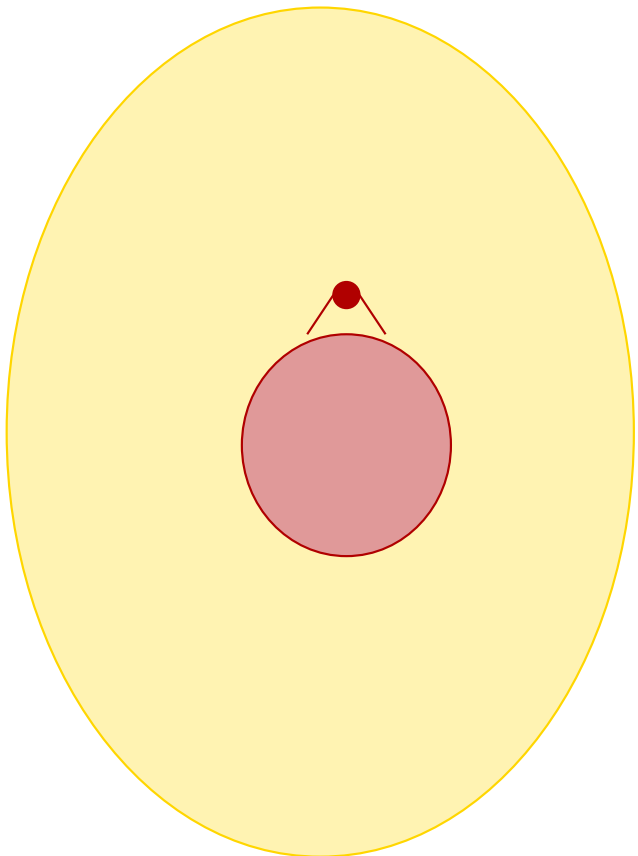
(2) g is the greatest lower bound of X :

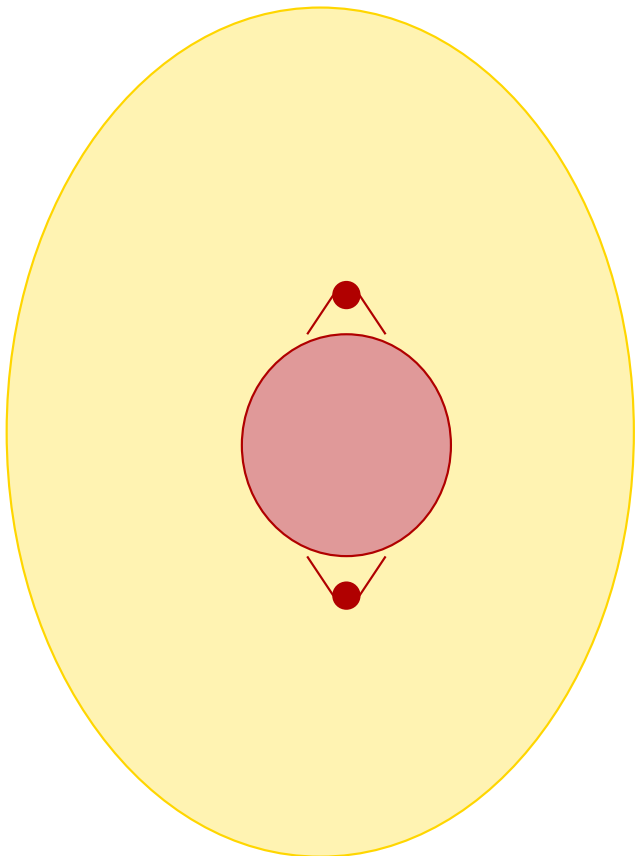
Assume u is a lower bound of X. Then:

$u \in U$

$\Longrightarrow$ $u \sqsubseteq g$:-))







We are looking for solutions for systems of constraints of the form:

$$x_i \quad \sqsupseteq \quad f_i(x_1, \ldots, x_n) \qquad\qquad (*)$$

We are looking for solutions for systems of constraints of the form:

$$x_i \quad \sqsupseteq \quad f_i(x_1, \ldots, x_n) \qquad\qquad (*)$$

where:

x_i	unknown	here:	$\mathcal{A}[u]$
$\mathbb{D}$	values	here:	2^{Expr}
$\sqsubseteq \subseteq \mathbb{D} \times \mathbb{D}$	ordering relation	here:	$\supseteq$
$f_i \colon \mathbb{D}^n \to \mathbb{D}$	constraint	here:	...

We are looking for solutions for systems of constraints of the form:

$$x_i \quad \sqsupseteq \quad f_i(x_1, \ldots, x_n) \qquad (*)$$

where:

x_i	unknown	here:	$\mathcal{A}[u]$
$\mathbb{D}$	values	here:	2^{Expr}
$\sqsubseteq \subseteq \mathbb{D} \times \mathbb{D}$	ordering relation	here:	$\supseteq$
$f_i \colon \mathbb{D}^n \to \mathbb{D}$	constraint	here:	...

Constraint for $\mathcal{A}[v]$ $(v \neq start)$:

$$\mathcal{A}[v] \quad \subseteq \quad \bigcap \{ [\![k]\!]^\sharp (\mathcal{A}[u]) \mid k = (u, _, v) \text{ edge} \}$$

We are looking for solutions for systems of constraints of the form:

$$x_i \quad \sqsupseteq \quad f_i(x_1, \ldots, x_n) \qquad\qquad (*)$$

where:

x_i	unknown	here:	$\mathcal{A}[u]$
$\mathbb{D}$	values	here:	2^{Expr}
$\sqsubseteq \subseteq \mathbb{D} \times \mathbb{D}$	ordering relation	here:	$\supseteq$
$f_i \colon \mathbb{D}^n \to \mathbb{D}$	constraint	here:	...

Constraint for $\mathcal{A}[v]$ $(v \neq start)$:

$$\mathcal{A}[v] \quad \subseteq \quad \bigcap \{ [\![k]\!]^\sharp (\mathcal{A}[u]) \mid k = (u, _, v) \text{ edge} \}$$

Because:

$$x \sqsupseteq d_1 \wedge \ldots \wedge x \sqsupseteq d_k \quad \text{iff} \quad x \sqsupseteq \bigsqcup \{d_1, \ldots, d_k\} \qquad \text{:-)}$$

A mapping $f : \mathbb{D}_1 \to \mathbb{D}_2$ is called monotonic, if $f(a) \sqsubseteq f(b)$ for all $a \sqsubseteq b$.

A mapping $f : \mathbb{D}_1 \to \mathbb{D}_2$ is called monotonic, if $f(a) \sqsubseteq f(b)$ for all $a \sqsubseteq b$.

Examples:

(1) $\mathbb{D}_1 = \mathbb{D}_2 = 2^U$ for a set U and $f\,x = (x \cap a) \cup b$.

Obviously, every such f is monotonic :-)

A mapping $f : \mathbb{D}_1 \to \mathbb{D}_2$ is called monotonic, is $f(a) \sqsubseteq f(b)$ for all $a \sqsubseteq b$.

Examples:

(1) $\mathbb{D}_1 = \mathbb{D}_2 = 2^U$ for a set U and $f\,x = (x \cap a) \cup b$.

Obviously, every such f is monotonic :-)

(2) $\mathbb{D}_1 = \mathbb{D}_2 = \mathbb{Z}$ (with the ordering "$\leq$"). Then:

- $\mathsf{inc}\,x = x + 1$ is monotonic.
- $\mathsf{dec}\,x = x - 1$ is monotonic.

A mapping $f : \mathbb{D}_1 \to \mathbb{D}_2$ is called monotonic, is $f(a) \sqsubseteq f(b)$ for all $a \sqsubseteq b$.

Examples:

(1) $\mathbb{D}_1 = \mathbb{D}_2 = 2^U$ for a set U and $f\,x = (x \cap a) \cup b$.

Obviously, every such f is monotonic :-)

(2) $\mathbb{D}_1 = \mathbb{D}_2 = \mathbb{Z}$ (with the ordering "$\leq$"). Then:

- $\mathsf{inc}\,x = x + 1$ is monotonic.
- $\mathsf{dec}\,x = x - 1$ is monotonic.
- $\mathsf{inv}\,x = -x$ is not monotonic :-)

Theorem:

If $f_1 : \mathbb{D}_1 \to \mathbb{D}_2$ and $f_2 : \mathbb{D}_2 \to \mathbb{D}_3$ are monotonic, then also $f_2 \circ f_1 : \mathbb{D}_1 \to \mathbb{D}_3$:-)

Theorem:

If $f_1 : \mathbb{D}_1 \to \mathbb{D}_2$ and $f_2 : \mathbb{D}_2 \to \mathbb{D}_3$ are monotonic, then also $f_2 \circ f_1 : \mathbb{D}_1 \to \mathbb{D}_3$:-)

Theorem:

If $\mathbb{D}_2$ is a complete lattice, then the set $[\mathbb{D}_1 \to \mathbb{D}_2]$ of monotonic functions $f : \mathbb{D}_1 \to \mathbb{D}_2$ is also a complete lattice where

$$f \sqsubseteq g \quad \text{iff} \quad f\,x \sqsubseteq g\,x \quad \text{for all } x \in \mathbb{D}_1$$

Theorem:

If $f_1 : \mathbb{D}_1 \to \mathbb{D}_2$ and $f_2 : \mathbb{D}_2 \to \mathbb{D}_3$ are monotonic, then also $f_2 \circ f_1 : \mathbb{D}_1 \to \mathbb{D}_3$:-)

Theorem:

If $\mathbb{D}_2$ is a complete lattice, then the set $[\mathbb{D}_1 \to \mathbb{D}_2]$ of monotonic functions $f : \mathbb{D}_1 \to \mathbb{D}_2$ is also a complete lattice where

$$f \sqsubseteq g \quad \text{iff} \quad f\,x \sqsubseteq g\,x \quad \text{for all } x \in \mathbb{D}_1$$

In particular for $F \subseteq [\mathbb{D}_1 \to \mathbb{D}_2]$,

$$\bigsqcup F = f \quad \text{mit} \quad f\,x = \bigsqcup \{g\,x \mid g \in F\}$$

For functions $f_i\, x = a_i \cap x \cup b_i$, the operations "$\circ$", "$\sqcup$" and "$\sqcap$" can be explicitly defined by:

$$
\begin{aligned}
(f_2 \circ f_1)\, x &= \boxed{a_1 \cap a_2} \cap x \cup \boxed{a_2 \cap b_1 \cup b_2} \\
(f_1 \sqcup f_2)\, x &= \boxed{(a_1 \cup a_2)} \cap x \cup \boxed{b_1 \cup b_2} \\
(f_1 \sqcap f_2)\, x &= \boxed{(a_1 \cup b_1) \cap (a_2 \cup b_2)} \cap x \cup \boxed{b_1 \cap b_2}
\end{aligned}
$$

Wanted: minimally small solution for:

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

where all $f_i : \mathbb{D}^n \to \mathbb{D}$ are monotonic.

Wanted: minimally small solution for:

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

where all $f_i : \mathbb{D}^n \to \mathbb{D}$ are monotonic.

Idea:

- Consider $F : \mathbb{D}^n \to \mathbb{D}^n$ where

$$F(x_1, \ldots, x_n) = (y_1, \ldots, y_n) \quad \text{with} \quad y_i = f_i(x_1, \ldots, x_n).$$

Wanted: minimally small solution for:

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

where all $f_i : \mathbb{D}^n \to \mathbb{D}$ are monotonic.

Idea:

- Consider $F : \mathbb{D}^n \to \mathbb{D}^n$ where

  $$F(x_1, \ldots, x_n) = (y_1, \ldots, y_n) \quad \text{with} \quad y_i = f_i(x_1, \ldots, x_n).$$

- If all f_i are monotonic, then also F :-)

Wanted: minimally small solution for:

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

where all $f_i : \mathbb{D}^n \to \mathbb{D}$ are monotonic.

Idea:

- Consider $F : \mathbb{D}^n \to \mathbb{D}^n$ where

  $$F(x_1, \ldots, x_n) = (y_1, \ldots, y_n) \quad \text{with} \quad y_i = f_i(x_1, \ldots, x_n).$$

- If all f_i are monotonic, then also F :-)
- We successively approximate a solution. We construct:

  $$\underline{\bot}, \quad F\,\underline{\bot}, \quad F^2\,\underline{\bot}, \quad F^3\,\underline{\bot}, \quad \ldots$$

Hope: We eventually reach a solution ... ???

Example: $\mathbb{D} = 2^{\{a,b,c\}}, \quad \sqsubseteq = \subseteq$

$$\begin{array}{lcl} x_1 & \supseteq & \{a\} \cup x_3 \\ x_2 & \supseteq & x_3 \cap \{a, b\} \\ x_3 & \supseteq & x_1 \cup \{c\} \end{array}$$

Example: $\mathbb{D} = 2^{\{a,b,c\}}, \quad \sqsubseteq = \subseteq$

$$\begin{aligned} x_1 &\supseteq \{a\} \cup x_3 \\ x_2 &\supseteq x_3 \cap \{a, b\} \\ x_3 &\supseteq x_1 \cup \{c\} \end{aligned}$$

The Iteration:

	0	1	2	3	4
x_1	$\emptyset$				
x_2	$\emptyset$				
x_3	$\emptyset$				

Example: $\mathbb{D} = 2^{\{a,b,c\}}, \quad \sqsubseteq = \subseteq$

$$\begin{array}{lcl} x_1 & \supseteq & \{a\} \cup x_3 \\ x_2 & \supseteq & x_3 \cap \{a, b\} \\ x_3 & \supseteq & x_1 \cup \{c\} \end{array}$$

The Iteration:

	0	1	2	3	4
x_1	$\emptyset$	$\{a\}$			
x_2	$\emptyset$	$\emptyset$			
x_3	$\emptyset$	$\{c\}$			

Example: $\mathbb{D} = 2^{\{a,b,c\}}, \quad \sqsubseteq = \subseteq$

$$\begin{array}{lcl} x_1 & \supseteq & \{a\} \cup x_3 \\ x_2 & \supseteq & x_3 \cap \{a, b\} \\ x_3 & \supseteq & x_1 \cup \{c\} \end{array}$$

The Iteration:

	0	1	2	3	4
x_1	$\emptyset$	$\{a\}$	$\{a, c\}$		
x_2	$\emptyset$	$\emptyset$	$\emptyset$		
x_3	$\emptyset$	$\{c\}$	$\{a, c\}$		

Example: $\mathbb{D} = 2^{\{a,b,c\}}, \quad \sqsubseteq = \subseteq$

$$\begin{aligned} x_1 &\supseteq \{a\} \cup x_3 \\ x_2 &\supseteq x_3 \cap \{a, b\} \\ x_3 &\supseteq x_1 \cup \{c\} \end{aligned}$$

The Iteration:

	0	1	2	3	4
x_1	$\emptyset$	$\{a\}$	$\{a, c\}$	$\{a, c\}$	
x_2	$\emptyset$	$\emptyset$	$\emptyset$	$\{a\}$	
x_3	$\emptyset$	$\{c\}$	$\{a, c\}$	$\{a, c\}$	

Example: $\mathbb{D} = 2^{\{a,b,c\}}, \quad \sqsubseteq = \subseteq$

$$\begin{aligned} x_1 &\supseteq \{a\} \cup x_3 \\ x_2 &\supseteq x_3 \cap \{a, b\} \\ x_3 &\supseteq x_1 \cup \{c\} \end{aligned}$$

The Iteration:

	0	1	2	3	4
x_1	$\emptyset$	$\{a\}$	$\{a, c\}$	$\{a, c\}$	dito
x_2	$\emptyset$	$\emptyset$	$\emptyset$	$\{a\}$	
x_3	$\emptyset$	$\{c\}$	$\{a, c\}$	$\{a, c\}$	

Theorem

- $\underline{\bot}, F\,\underline{\bot}, F^2\,\underline{\bot}, \ldots$ form an ascending chain :

$$\underline{\bot} \quad \sqsubseteq \quad F\,\underline{\bot} \quad \sqsubseteq \quad F^2\,\underline{\bot} \quad \sqsubseteq \quad \ldots$$

- If $F^k\,\underline{\bot} = F^{k+1}\,\underline{\bot}$, a solution is obtained which is the least one :-)
- If all ascending chains are finite, such a k always exists.

Theorem

- $\underline{\bot}, F\,\underline{\bot}, F^2\,\underline{\bot}, \ldots$ form an ascending chain :

$$\underline{\bot} \quad \sqsubseteq \quad F\,\underline{\bot} \quad \sqsubseteq \quad F^2\,\underline{\bot} \quad \sqsubseteq \quad \ldots$$

- If $F^k\,\underline{\bot} = F^{k+1}\,\underline{\bot}$, a solution is obtained which is the least one :-)
- If all ascending chains are finite, such a k always exists.

Proof

The first claim follows by complete induction:

Foundation: $F^0\,\underline{\bot} = \underline{\bot} \sqsubseteq F^1\,\underline{\bot}$:-)

Step: Assume $F^{i-1}\,\underline{\bot} \sqsubseteq F^{i}\,\underline{\bot}$. Then

$$F^{i}\,\underline{\bot} = F\,(F^{i-1}\,\underline{\bot}) \sqsubseteq F\,(F^{i}\,\underline{\bot}) = F^{i+1}\,\underline{\bot}$$

since F monotonic :-)

Step: Assume $F^{i-1}\,\underline{\bot} \sqsubseteq F^{i}\,\underline{\bot}$. Then

$$F^{i}\,\underline{\bot} = F\,(F^{i-1}\,\underline{\bot}) \sqsubseteq F\,(F^{i}\,\underline{\bot}) = F^{i+1}\,\underline{\bot}$$

since F monotonic :-)

Conclusion:

If $\mathbb{D}$ is finite, a solution can be found which is definitely the least :-)

Question:

What, if $\mathbb{D}$ is not finite ???