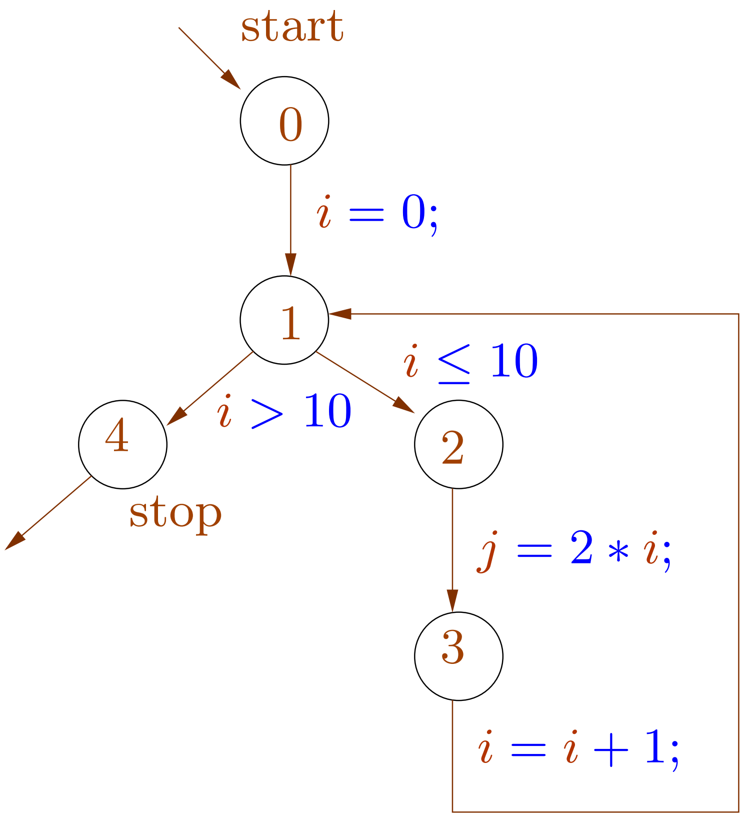
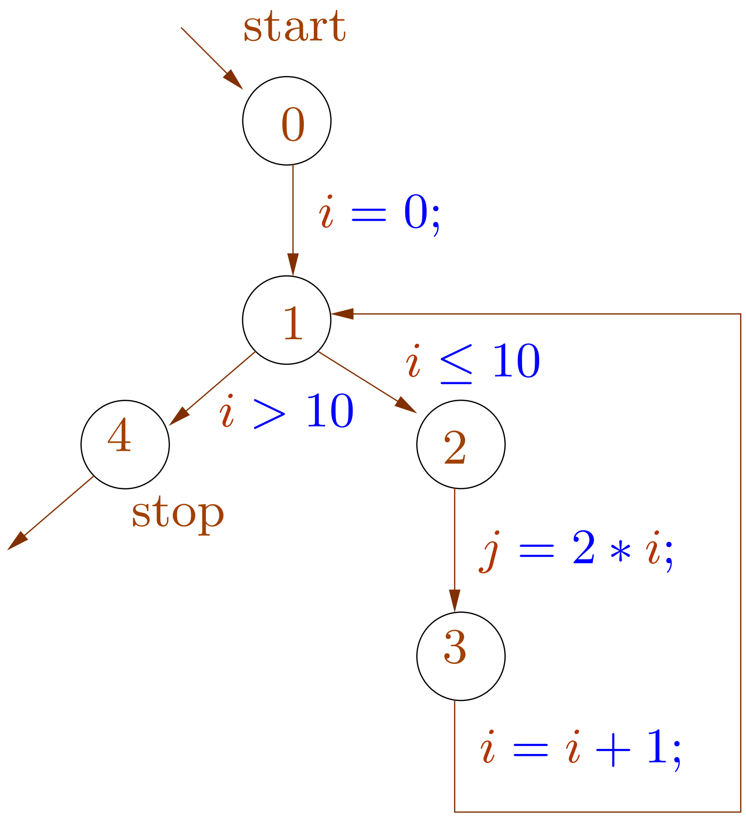
An idea: do iterative computation of reachable states.



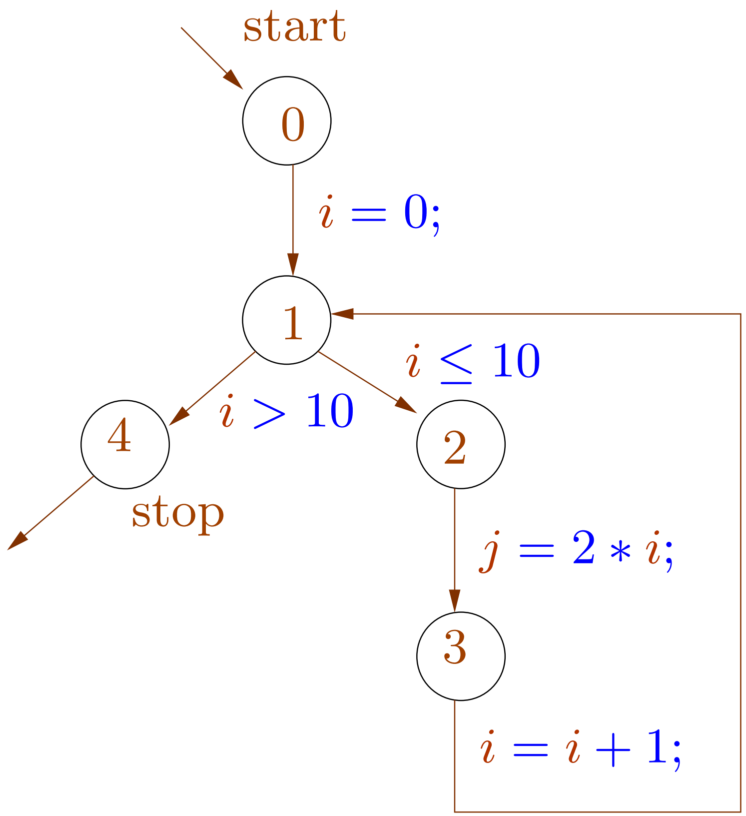
$\mathcal{V}[0]$	$\emptyset$
$\mathcal{V}[1]$	$\emptyset$
$\mathcal{V}[2]$	$\emptyset$
$\mathcal{V}[3]$	$\emptyset$
$\mathcal{V}[4]$	$\emptyset$

An idea: do iterative computation of reachable states.



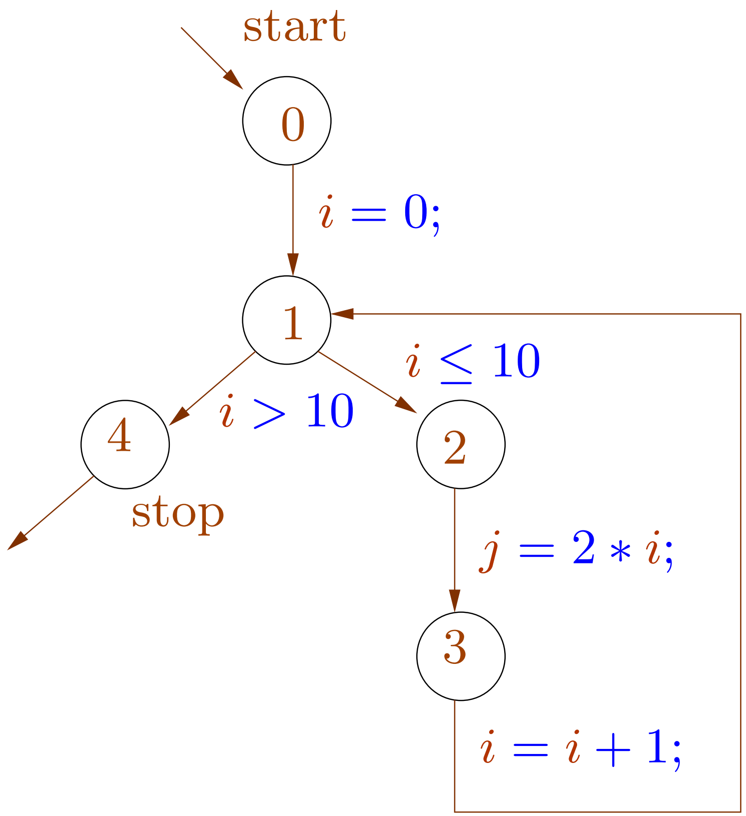
$\mathcal{V}[0]$	$\emptyset$	$\mathbb{Z} \times \mathbb{Z}$
$\mathcal{V}[1]$	$\emptyset$	
$\mathcal{V}[2]$	$\emptyset$	
$\mathcal{V}[3]$	$\emptyset$	
$\mathcal{V}[4]$	$\emptyset$	

An idea: do iterative computation of reachable states.



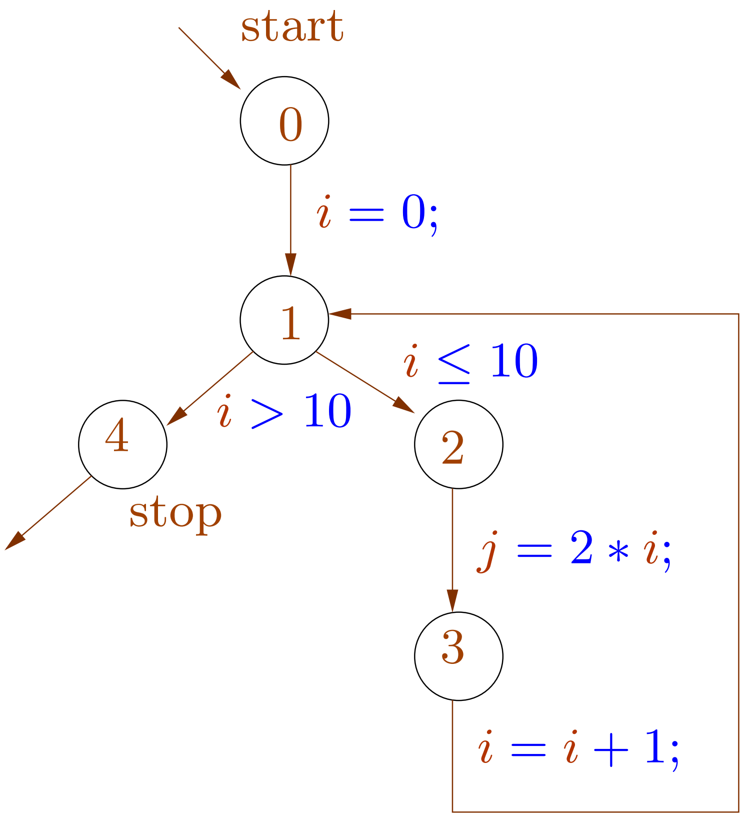
$\mathcal{V}[0]$	$\emptyset$	$\mathbb{Z} \times \mathbb{Z}$
$\mathcal{V}[1]$	$\emptyset$	$\{0\} \times \mathbb{Z}$
$\mathcal{V}[2]$	$\emptyset$	
$\mathcal{V}[3]$	$\emptyset$	
$\mathcal{V}[4]$	$\emptyset$	

An idea: do iterative computation of reachable states.



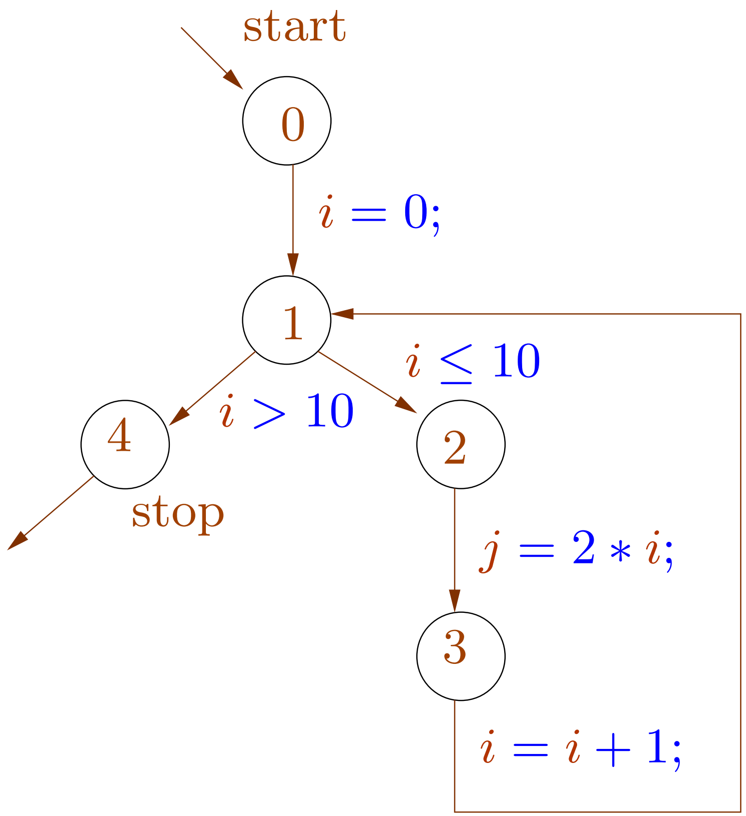
$\mathcal{V}[0]$	$\emptyset$	$\mathbb{Z} \times \mathbb{Z}$
$\mathcal{V}[1]$	$\emptyset$	$\{0\} \times \mathbb{Z}$
$\mathcal{V}[2]$	$\emptyset$	$\{0\} \times \mathbb{Z}$
$\mathcal{V}[3]$	$\emptyset$	
$\mathcal{V}[4]$	$\emptyset$	

An idea: do iterative computation of reachable states.



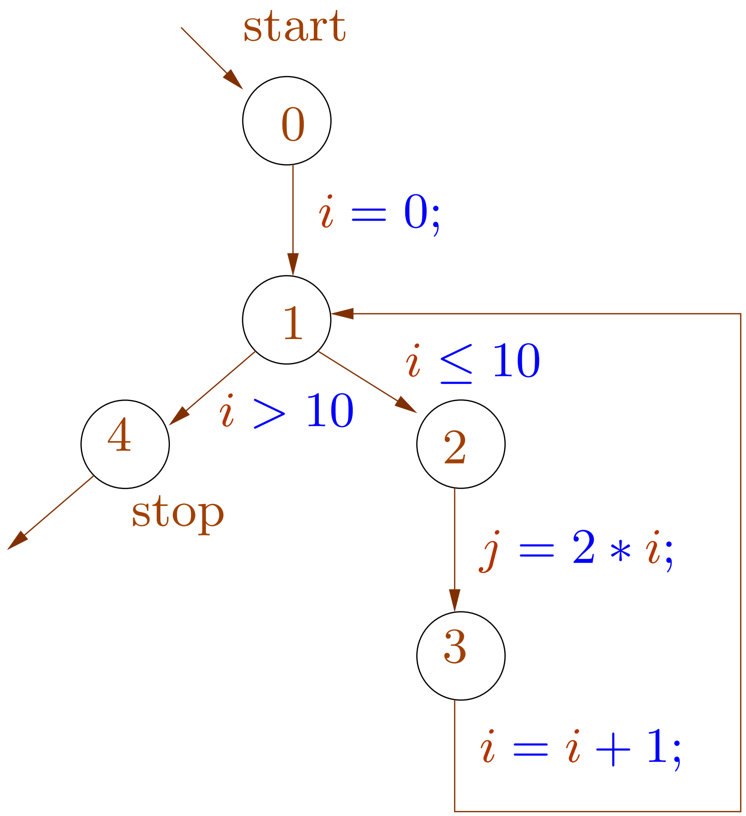
$\mathcal{V}[0]$	$\emptyset$	$\mathbb{Z} \times \mathbb{Z}$
$\mathcal{V}[1]$	$\emptyset$	$\{0\} \times \mathbb{Z}$
$\mathcal{V}[2]$	$\emptyset$	$\{0\} \times \mathbb{Z}$
$\mathcal{V}[3]$	$\emptyset$	$\{(0, 0)\}$
$\mathcal{V}[4]$	$\emptyset$	

An idea: do iterative computation of reachable states.



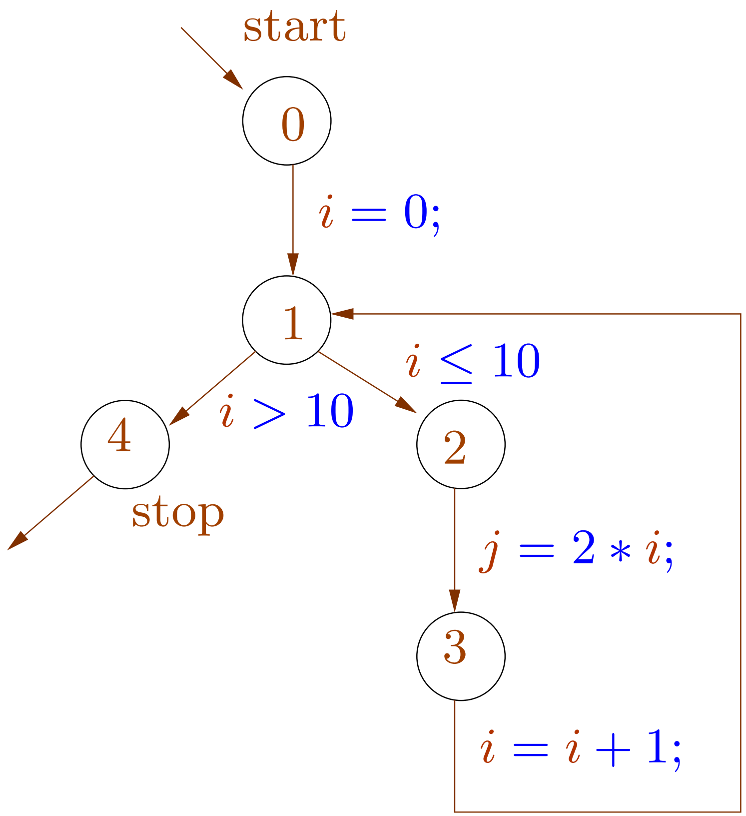
$\mathcal{V}[0]$	$\emptyset$	$\mathbb{Z} \times \mathbb{Z}$	
$\mathcal{V}[1]$	$\emptyset$	$\{0\} \times \mathbb{Z}$	$\{0, 1\} \times \mathbb{Z}$
$\mathcal{V}[2]$	$\emptyset$	$\{0\} \times \mathbb{Z}$	
$\mathcal{V}[3]$	$\emptyset$	$\{(0, 0)\}$	
$\mathcal{V}[4]$	$\emptyset$		

An idea: do iterative computation of reachable states.



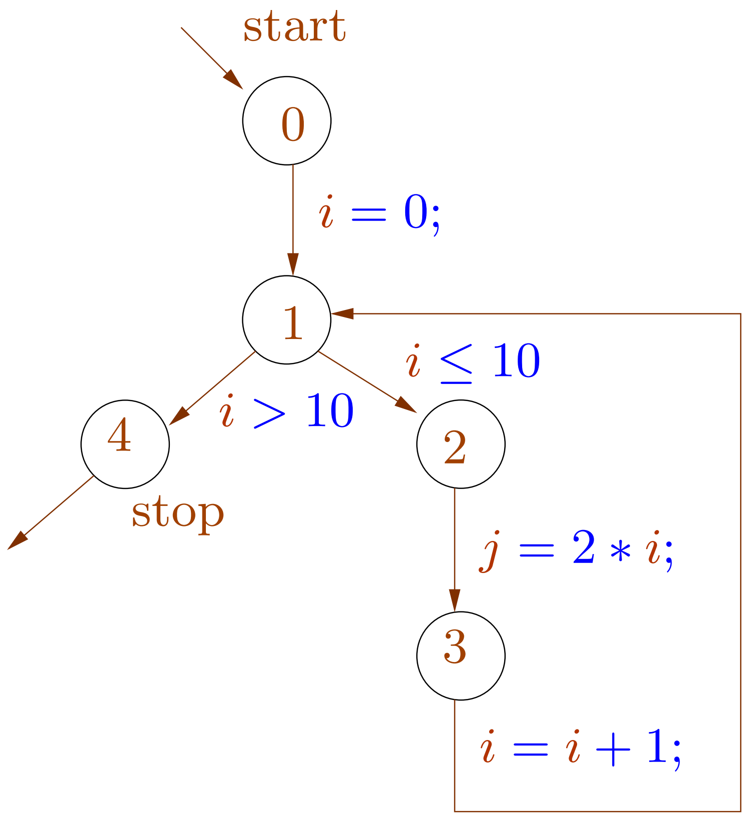
$\mathcal{V}[0]$	$\emptyset$	$\mathbb{Z} \times \mathbb{Z}$	
$\mathcal{V}[1]$	$\emptyset$	$\{0\} \times \mathbb{Z}$	$\{0, 1\} \times \mathbb{Z}$
$\mathcal{V}[2]$	$\emptyset$	$\{0\} \times \mathbb{Z}$	$\{0, 1\} \times \mathbb{Z}$
$\mathcal{V}[3]$	$\emptyset$	$\{(0, 0)\}$	
$\mathcal{V}[4]$	$\emptyset$		

An idea: do iterative computation of reachable states.



$\mathcal{V}[0]$	$\emptyset$	$\mathbb{Z} \times \mathbb{Z}$	
$\mathcal{V}[1]$	$\emptyset$	$\{0\} \times \mathbb{Z}$	$\{0, 1\} \times \mathbb{Z}$
$\mathcal{V}[2]$	$\emptyset$	$\{0\} \times \mathbb{Z}$	$\{0, 1\} \times \mathbb{Z}$
$\mathcal{V}[3]$	$\emptyset$	$\{(0, 0)\}$	$\{(0, 0), (1, 2)\}$
$\mathcal{V}[4]$	$\emptyset$		

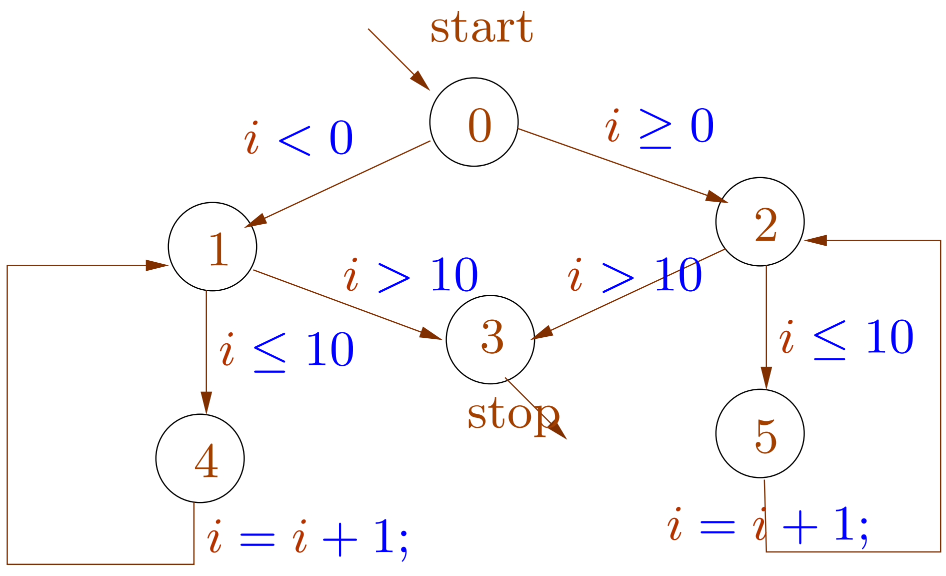
An idea: do iterative computation of reachable states.



$\mathcal{V}[0]$	$\emptyset$	$\mathbb{Z} \times \mathbb{Z}$		
$\mathcal{V}[1]$	$\emptyset$	$\{0\} \times \mathbb{Z}$	$\{0, 1\} \times \mathbb{Z}$	
$\mathcal{V}[2]$	$\emptyset$	$\{0\} \times \mathbb{Z}$	$\{0, 1\} \times \mathbb{Z}$	$\ldots$
$\mathcal{V}[3]$	$\emptyset$	$\{(0, 0)\}$	$\{(0, 0), (1, 2)\}$	
$\mathcal{V}[4]$	$\emptyset$			

Problem: too many iterations, infinite loops.

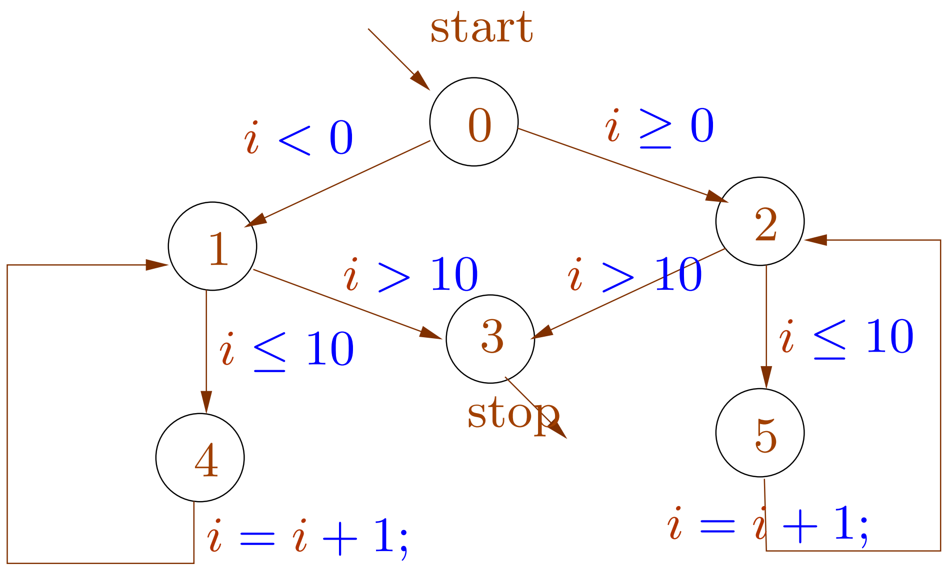
Solution: approximate computation of possible states.



0	$\emptyset$	$\mathbb{Z}$	$\mathbb{Z}$
1	$\emptyset$	$\mathbb{Z}^-$	$\mathbb{Z}$
2	$\emptyset$	$\mathbb{Z}^+$	$\mathbb{Z}^+$
3	$\emptyset$	$\mathbb{Z}^+$	$\mathbb{Z}^+$
4	$\emptyset$	$\mathbb{Z}^-$	$\mathbb{Z}$
5	$\emptyset$	$\mathbb{Z}^+$	$\mathbb{Z}^+$

Problem: too many iterations, infinite loops.

Solution: approximate computation of possible states.



0	$\emptyset$	$\mathbb{Z}$	$\mathbb{Z}$
1	$\emptyset$	$\mathbb{Z}^-$	$\mathbb{Z}$
2	$\emptyset$	$\mathbb{Z}^+$	$\mathbb{Z}^+$
3	$\emptyset$	$\mathbb{Z}^+$	$\mathbb{Z}^+$
4	$\emptyset$	$\mathbb{Z}^-$	$\mathbb{Z}$
5	$\emptyset$	$\mathbb{Z}^+$	$\mathbb{Z}^+$

Interpretation of our result:

the values of i at node 1 is included in $\mathbb{Z}$

the values of i at node 2 is included in $\mathbb{Z}^+$

This information we obtain is accurate.

In general we have some domain $\mathbb{D}$.

Examples: $2^{\mathcal{S}}$, $2^{\mathbb{Z}}$, $\{\emptyset, \mathbb{Z}^-, \mathbb{Z}^+, \mathbb{Z}\}$, the set of intervals over $\mathbb{Z}$.

In general we have some domain $\mathbb{D}$.

Examples: $2^{\mathcal{S}}$, $2^{\mathbb{Z}}$, $\{\emptyset, \mathbb{Z}^-, \mathbb{Z}^+, \mathbb{Z}\}$, the set of intervals over $\mathbb{Z}$.

We require an ordering $\sqsubseteq$ on the elements of this domain.

$\emptyset \sqsubseteq \mathbb{Z}^-$ $\quad$ $\emptyset \sqsubseteq \mathbb{Z}^+$ $\quad$ $\mathbb{Z}^- \sqsubseteq \mathbb{Z}$ $\quad$ $\mathbb{Z}^+ \sqsubseteq \mathbb{Z}$

Read $x \sqsubseteq y$ as "y is imprecise information compared to x".

In general we have some domain $\mathbb{D}$.

Examples: $2^{\mathcal{S}}$, $2^{\mathbb{Z}}$, $\{\emptyset, \mathbb{Z}^-, \mathbb{Z}^+, \mathbb{Z}\}$, the set of intervals over $\mathbb{Z}$.

We require an ordering $\sqsubseteq$ on the elements of this domain.

$\emptyset \sqsubseteq \mathbb{Z}^- \qquad \emptyset \sqsubseteq \mathbb{Z}^+ \qquad \mathbb{Z}^- \sqsubseteq \mathbb{Z} \qquad \mathbb{Z}^+ \sqsubseteq \mathbb{Z}$

Read $x \sqsubseteq y$ as "y is imprecise information compared to x".

We further require operations like least upper bounds.

$$\mathbb{Z}^- \sqcup \mathbb{Z}^+ = \mathbb{Z}$$

A digression: complete lattices

Recall: a set $\mathbb{D}$ with relation $\sqsubseteq$ is a partial order if the following conditions hold for all $x, y, z \in \mathbb{D}$.

- Reflexivity: $x \sqsubseteq x$.
- Antisymmetry: $x \sqsubseteq y$ and $y \sqsubseteq x$ then $x = y$.
- Transitivity: if $x \sqsubseteq y$ and $y \sqsubseteq z$ then $x \sqsubseteq z$.

An element $d \in \mathbb{D}$ is called an upper bound of a set $X \subseteq \mathbb{D}$ if $x \sqsubseteq d$ for all $x \in X$.

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

- d is an upper bound of X
- $d \sqsubseteq d'$ for every upper bound d' of X

An element $d \in \mathbb{D}$ is called an upper bound of a set $X \subseteq \mathbb{D}$ if $x \sqsubseteq d$ for all $x \in X$.

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

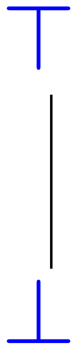
- d is an upper bound of X
- $d \sqsubseteq d'$ for every upper bound d' of X

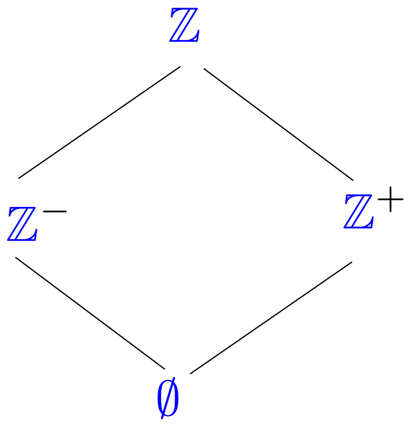
A partial order $(\mathbb{D}, \sqsubseteq)$ is called a complete lattice if every $X \subseteq \mathbb{D}$ has a least upper bound $\bigsqcup X$.

We write $x \sqcup y$ for $\bigsqcup\{x, y\}$.

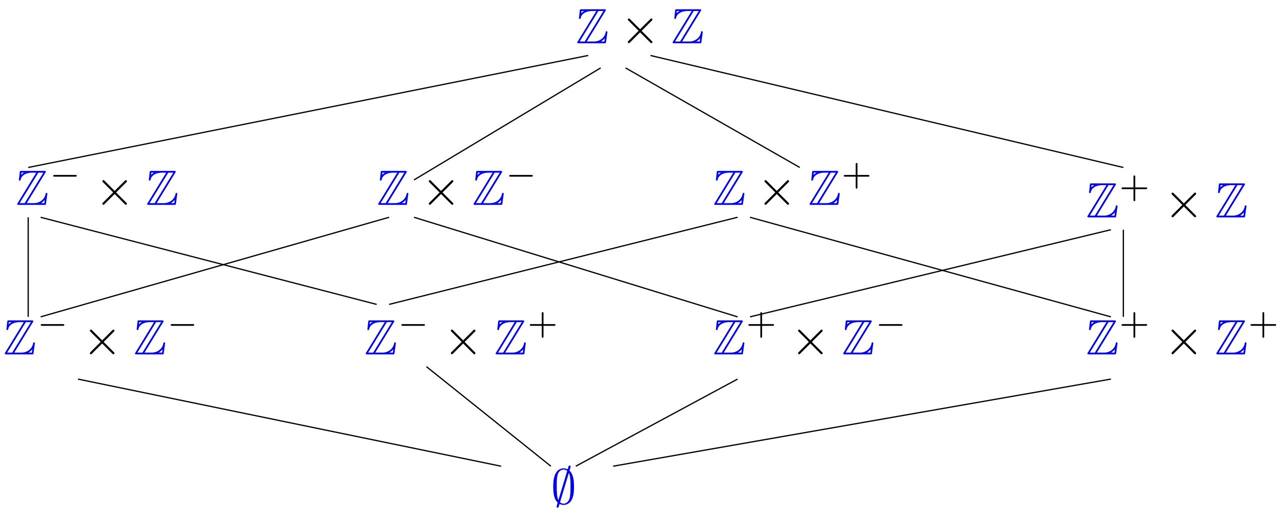
For $(2^{\mathcal{S}}, \subseteq)$ we have $\bigsqcup X = \bigcup X$.

Some complete lattices.

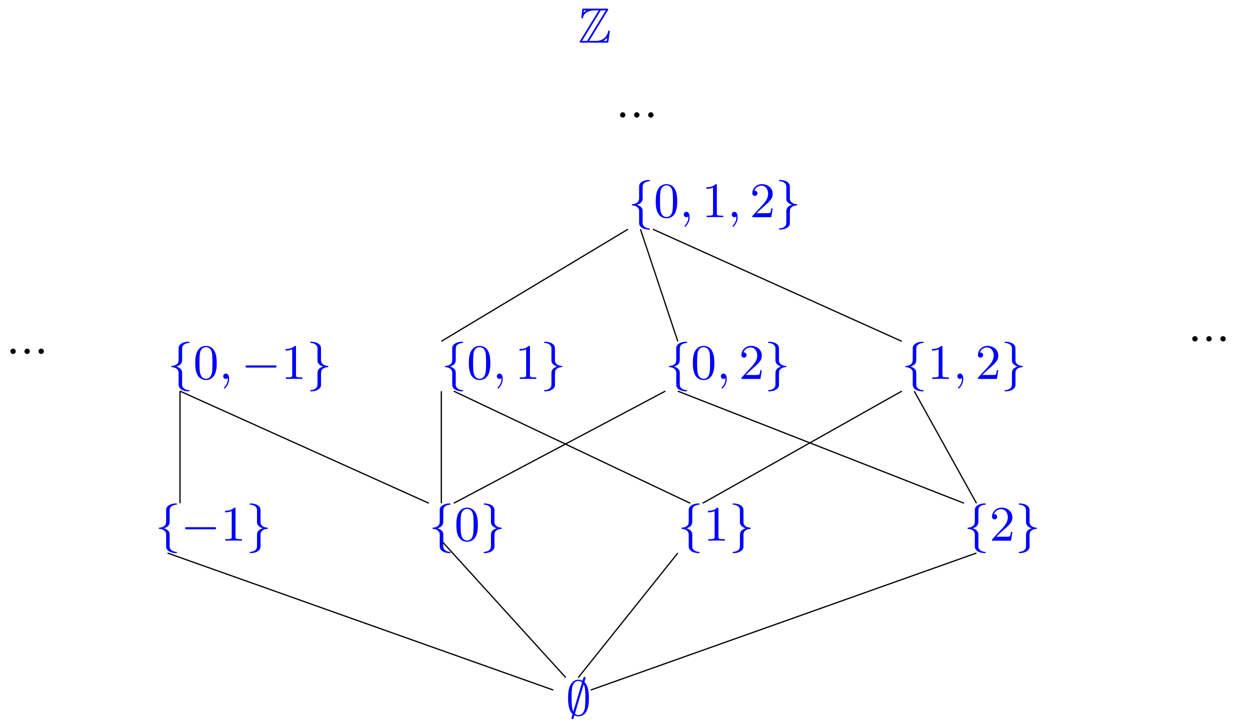




$$\mathbb{Z}^- = \{x \in \mathbb{Z} \mid x < 0\}$$
$$\mathbb{Z}^+ = \{x \in \mathbb{Z} \mid x \geq 0\}$$



An infinite complete lattice : $(2^{\mathbb{Z}}, \subseteq)$.



Every complete lattice has

- a top element: $\top = \bigsqcup \mathbb{D}$
- a bottom element: $\bot = \bigsqcup \emptyset$

Further every $X \subseteq \mathbb{D}$ has a greatest lower bound $\bigsqcap X$.

For $(2^{\mathcal{S}}, \subseteq)$ we have $\bigsqcap X = \bigcap X$.

Consider the set of lower bounds of X:

$$L = \{l \in \mathbb{D} \mid \forall x \in X, l \leq x\}$$

and define

$$g = \bigsqcup L$$

Claim: g is the greatest lower bound of X.

(1) g is a lower bound of X:

Consider any $x \in X$.

$l \leq x$ for all $l \in L$, i.e. x is an upper bound of L.

Hence $g = \bigsqcup L \sqsubseteq x$.

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

Let l be any other lower bound of X.

Then $l \in L$.

Hence $l \sqsubseteq \bigsqcup L = g$.

A function $f : \mathbb{D}_1 \to \mathbb{D}_2$ is called monotone if:

$$f(x) \sqsubseteq f(y) \text{ whenever } x \sqsubseteq y$$

A function $f : \mathbb{D}_1 \rightarrow \mathbb{D}_2$ is called monotone if:

$$f(x) \sqsubseteq f(y) \text{ whenever } x \sqsubseteq y$$

The function $f : \mathbb{Z} \rightarrow \mathbb{Z}$ defined as $f(x) = x + 1$ is monotone.

Note: $(\mathbb{Z}, \leq)$ is not a complete lattice.

A function $f : \mathbb{D}_1 \to \mathbb{D}_2$ is called monotone if:

$$f(x) \sqsubseteq f(y) \text{ whenever } x \sqsubseteq y$$

The function $f : \mathbb{Z} \to \mathbb{Z}$ defined as $f(x) = x + 1$ is monotone.

Note: $(\mathbb{Z}, \leq)$ is not a complete lattice.

The transformations induced by the program edges are monotone:

$$\text{Recall: } [\![l]\!]^\sharp \; : 2^{\mathcal{S}} \to 2^{\mathcal{S}}$$

$$[\![l]\!]^\sharp \; V = \{ [\![l]\!] \; \rho \mid \rho \in V \text{ and } [\![l]\!] \; \text{ is defined for } \rho \}.$$

$$\text{Hence if } V_1 \subseteq V_2 \text{ then } [\![l]\!]^\sharp \; V_1 \subseteq [\![l]\!]^\sharp \; V_2.$$

Some facts:

If $f : \mathbb{D}_1 \longrightarrow \mathbb{D}_2$ and $g : \mathbb{D}_2 \longrightarrow \mathbb{D}_3$ are monotone then the composition $g \circ f : \mathbb{D}_1 \longrightarrow \mathbb{D}_3$ is monotone.

Some facts:

If $f : \mathbb{D}_1 \longrightarrow \mathbb{D}_2$ and $g : \mathbb{D}_2 \longrightarrow \mathbb{D}_3$ are monotone then the composition $g \circ f : \mathbb{D}_1 \longrightarrow \mathbb{D}_3$ is monotone.

If $\mathbb{D}_2$ is a complete lattice then the set $[\mathbb{D}_1 \longrightarrow \mathbb{D}_2]$ of monotone functions $f : \mathbb{D}_1 \longrightarrow \mathbb{D}_2$ is a complete lattice,

where $f \sqsubseteq g$ iff $f(x) \sqsubseteq g(x)$ for all $x \in \mathbb{D}_1$.

For $F \subseteq [\mathbb{D}_1 \longrightarrow \mathbb{D}_2]$ we have

$$\bigsqcup F = f \text{ with } f(x) = \bigsqcup \{g(x) \mid g \in F\} \quad .$$

For our program analysis problem, we want the least solution of the constraint system

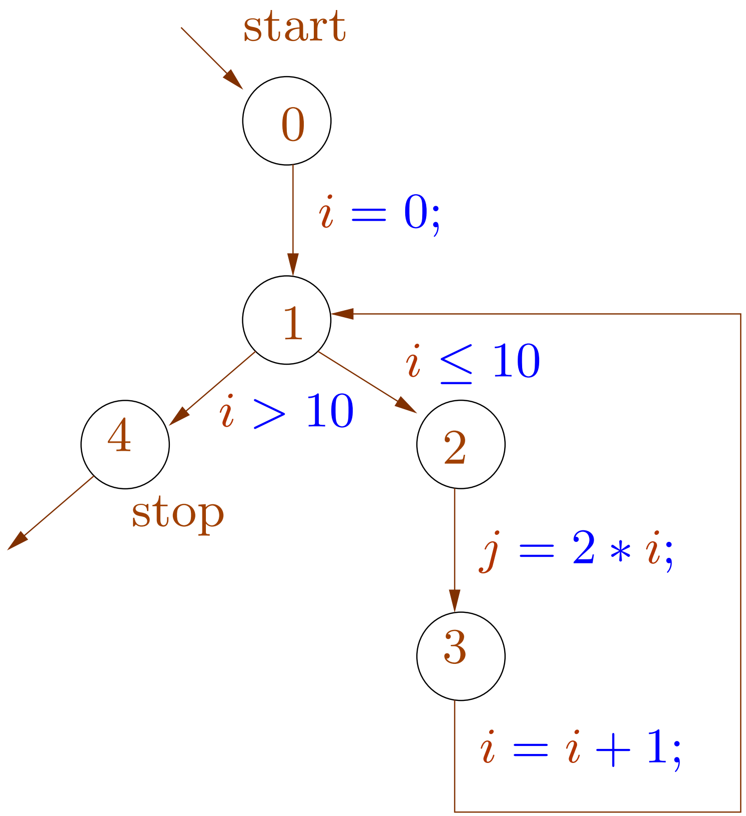
$$\begin{array}{ll} \mathcal{V}[0] \supseteq \mathcal{S} & (0 \text{ is the } \textit{start} \text{ node}) \\ \mathcal{V}[v] \supseteq [\![l]\!]^\sharp\ \mathcal{V}[u] & \text{for every edge } (u, l, v). \end{array}$$

We have the domain $\mathbb{D} = 2^{\mathcal{S}}$. Choose a variable for each set $\mathcal{V}[v]$.

We obtain a constraint system of the form

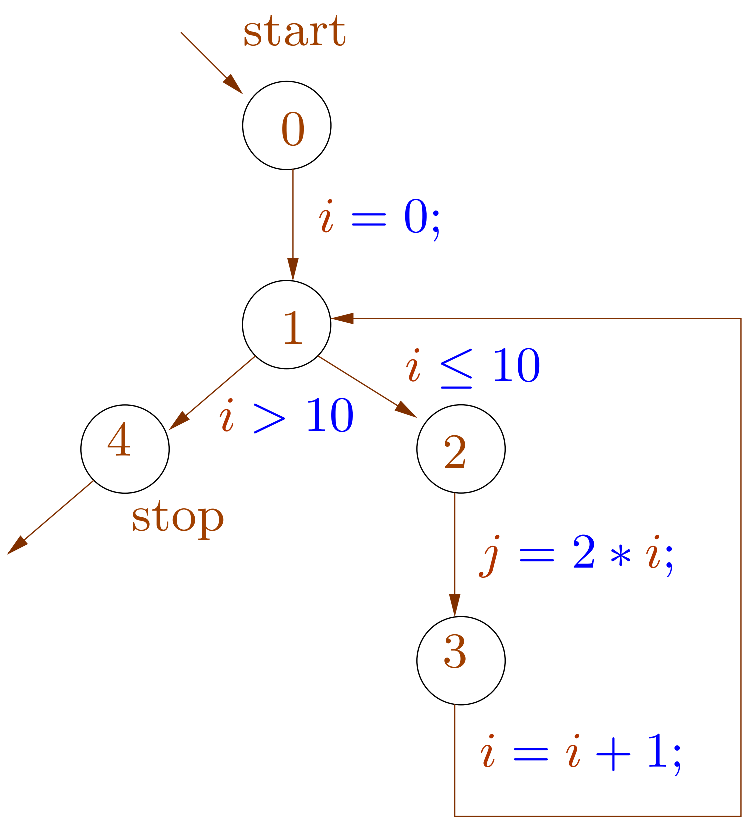
$$x_i \sqsupseteq f_i(x_1, \ldots, x_n) \qquad (1 \leq i \leq n)$$

Example



$$
\begin{aligned}
\mathcal{V}[0] &\supseteq \quad \mathcal{S} \\
\mathcal{V}[1] &\supseteq \quad [\![i = 0;]\!]\ \mathcal{V}[0] \\
\mathcal{V}[1] &\supseteq \quad [\![i = i{+}1;]\!]\ \mathcal{V}[3] \\
\mathcal{V}[2] &\supseteq \quad [\![i \leq 10]\!]\ \mathcal{V}[1] \\
\mathcal{V}[3] &\supseteq \quad [\![j = 2{*}i;]\!]\ \mathcal{V}[2] \\
\mathcal{V}[4] &\supseteq \quad [\![i > 10]\!]\ \mathcal{V}[1]
\end{aligned}
$$

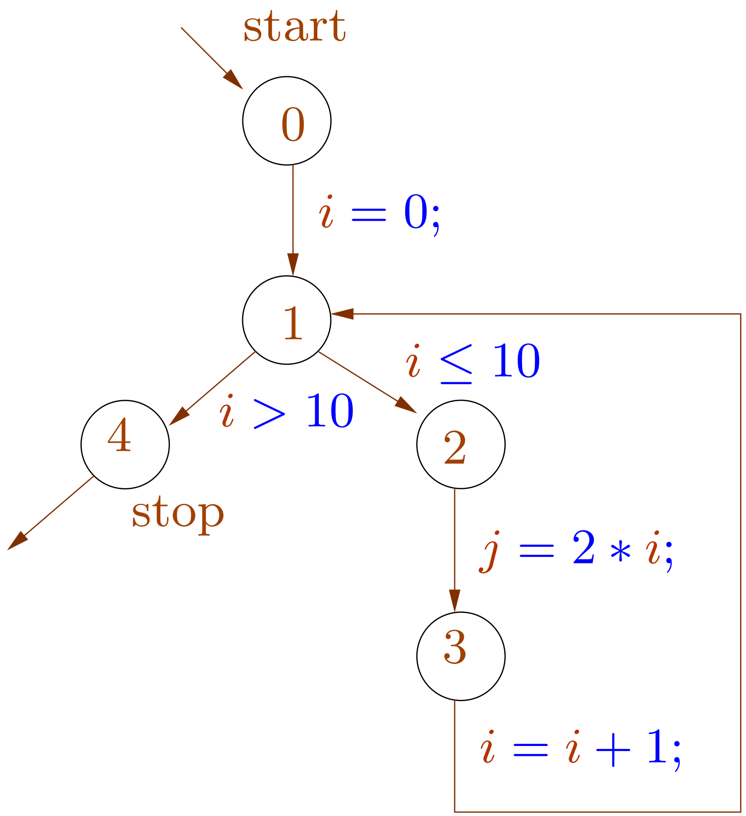
Example



$$
\begin{aligned}
\mathcal{V}[0] &\supseteq \quad \mathcal{S} \\
\mathcal{V}[1] &\supseteq \quad [\![i = 0;]\!] \; \mathcal{V}[0] \\
\mathcal{V}[1] &\supseteq \quad [\![i = i{+}1;]\!] \; \mathcal{V}[3] \\
\mathcal{V}[2] &\supseteq \quad [\![i \leq 10]\!] \; \mathcal{V}[1] \\
\mathcal{V}[3] &\supseteq \quad [\![j = 2{*}i;]\!] \; \mathcal{V}[2] \\
\mathcal{V}[4] &\supseteq \quad [\![i > 10]\!] \; \mathcal{V}[1]
\end{aligned}
$$

Transforms to ...

Example



$$
\begin{aligned}
\mathcal{V}[0] &\supseteq \quad \mathcal{S} \\
\mathcal{V}[1] &\supseteq \quad ([\![i = 0;]\!]\ \mathcal{V}[0] \\
&\qquad \cup [\![i = i+1;]\!]\ \mathcal{V}[3]) \\
\mathcal{V}[2] &\supseteq \quad [\![i \leq 10]\!]\ \mathcal{V}[1] \\
\mathcal{V}[3] &\supseteq \quad [\![j = 2*i;]\!]\ \mathcal{V}[2] \\
\mathcal{V}[4] &\supseteq \quad [\![i > 10]\!]\ \mathcal{V}[1]
\end{aligned}
$$

Since $\mathbb{D}$ is a lattice, $\mathbb{D}^n$ is also a lattice where

$$(d_1, \ldots, d_n) \sqsubseteq (d'_1, \ldots, d'_n) \text{ iff } d_i \sqsubseteq d'_i \text{ for } 1 \leq i \leq n$$

The functions $f_i : \mathbb{D}^n \to \mathbb{D}$ are monotone.

Define $F : \mathbb{D}^n \to \mathbb{D}^n$ as

$$F(y) = (f_1(y), \ldots, f_n(y)) \text{ where } y = (x_1, \ldots, x_n)$$

F is also monotone.

We need least solution of $y \sqsupseteq F(y)$.

Idea: use iteration

Start with the least element $\perp$ and compute the sequence

$\perp, F(\perp), F^2(\perp), F^3(\perp), \ldots$.

Do we always reach the least solution in this way?

Example: the complete lattice of Booleans: $\mathbb{D} = \{\bot, \top\}$.

Constraint system:

$$x \sqsupseteq y \vee z$$
$$y \sqsupseteq x \wedge y \wedge z$$
$$z \sqsupseteq \top$$

The iteration:

x	$\bot$			
y	$\bot$			
z	$\bot$			

We have $F^2(\bot) = F^3(\bot)$.

Example: the complete lattice of Booleans: $\mathbb{D} = \{\bot, \top\}$.

Constraint system:

$$x \sqsupseteq y \vee z$$

$$y \sqsupseteq x \wedge y \wedge z$$

$$z \sqsupseteq \top$$

The iteration:

x	$\bot$	$\bot$		
y	$\bot$	$\bot$		
z	$\bot$	$\top$		

We have $F^2(\bot) = F^3(\bot)$.

Example: the complete lattice of Booleans: $\mathbb{D} = \{\bot, \top\}$.

Constraint system:

$$x \sqsupseteq y \vee z$$

$$y \sqsupseteq x \wedge y \wedge z$$

$$z \sqsupseteq \top$$

The iteration:

x	$\bot$	$\bot$	$\top$	
y	$\bot$	$\bot$	$\bot$	
z	$\bot$	$\top$	$\top$	

We have $F^2(\bot) = F^3(\bot)$.

Example: the complete lattice of Booleans: $\mathbb{D} = \{\perp, \top\}$.

Constraint system:

$$x \sqsupseteq y \vee z$$

$$y \sqsupseteq x \wedge y \wedge z$$

$$z \sqsupseteq \top$$

The iteration:

x	$\perp$	$\perp$	$\top$	$\top$
y	$\perp$	$\perp$	$\perp$	$\perp$
z	$\perp$	$\top$	$\top$	$\top$

We have $F^2(\perp) = F^3(\perp)$.

Such an iteration produces an ascending chain

$$\bot \sqsubseteq F(\bot) \sqsubseteq F^2(\bot) \sqsubseteq F^3(\bot) \ldots$$

By induction: (1) Clearly $\bot \sqsubseteq F(\bot)$.

(2) Further if $F^i(\bot) \sqsubseteq F^{i+1}(\bot)$ then by monotonicity $F^{i+1}(\bot) \sqsubseteq F^{i+2}(\bot)$

Such an iteration produces an ascending chain

$$\perp \sqsubseteq F(\perp) \sqsubseteq F^2(\perp) \sqsubseteq F^3(\perp) \ldots$$

By induction: (1) Clearly $\perp \sqsubseteq F(\perp)$.

(2) Further if $F^i(\perp) \sqsubseteq F^{i+1}(\perp)$ then by monotonicity $F^{i+1}(\perp) \sqsubseteq F^{i+2}(\perp)$

Further if $F^k(\perp) = F^{k+1}(\perp)$ for some k
then clearly $F^k(\perp)$ is some solution of the constraint $F(x) \sqsubseteq x$.

Such an iteration produces an ascending chain

$$\perp \sqsubseteq F(\perp) \sqsubseteq F^2(\perp) \sqsubseteq F^3(\perp) \ldots$$

By induction: (1) Clearly $\perp \sqsubseteq F(\perp)$.

(2) Further if $F^i(\perp) \sqsubseteq F^{i+1}(\perp)$ then by monotonicity $F^{i+1}(\perp) \sqsubseteq F^{i+2}(\perp)$

Further if $F^k(\perp) = F^{k+1}(\perp)$ for some k
then clearly $F^k(\perp)$ is some solution of the constraint $F(x) \sqsubseteq x$.

Is it also the least solution of $F(x) \sqsubseteq x$?

Such an iteration produces an ascending chain

$$\perp \sqsubseteq F(\perp) \sqsubseteq F^2(\perp) \sqsubseteq F^3(\perp) \ldots$$

By induction: (1) Clearly $\perp \sqsubseteq F(\perp)$.

(2) Further if $F^i(\perp) \sqsubseteq F^{i+1}(\perp)$ then by monotonicity $F^{i+1}(\perp) \sqsubseteq F^{i+2}(\perp)$

Further if $F^k(\perp) = F^{k+1}(\perp)$ for some k
then clearly $F^k(\perp)$ is some solution of the constraint $F(x) \sqsubseteq x$.

Is it also the least solution of $F(x) \sqsubseteq x$?

Yes ...

Claim: If a is a solution of $F(x) \sqsubseteq x$ then $F^k(\perp) \sqsubseteq a$ for all k.

By induction: Clearly $\perp \sqsubseteq a$

Further if $F^k(\perp) \sqsubseteq a$ then by monotonicity we have $F^{k+1}(\perp) \sqsubseteq F(a) \sqsubseteq a$.

Claim: If a is a solution of $F(x) \sqsubseteq x$ then $F^k(\perp) \sqsubseteq a$ for all k.

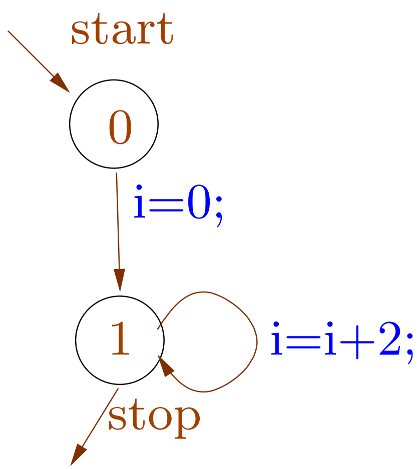
By induction: Clearly $\perp \sqsubseteq a$

Further if $F^k(\perp) \sqsubseteq a$ then by monotonicity we have $F^{k+1}(\perp) \sqsubseteq F(a) \sqsubseteq a$.

Hence if $F^{k+1}(\perp) = F^k(\perp)$ for any k then $F^k(\perp)$ is least solution of $F(x) \sqsubseteq x$.

Such a k always exists if the lattice is finite.

What in case of infinite lattices?



Constraint system:

$$\mathcal{V}[0] \supseteq \mathbb{Z}$$

$$\mathcal{V}[1] \supseteq \{0\} \cup \{x+2 \mid x \in \mathcal{V}[1]\}$$

The least solution:

$$\mathcal{V}[0] = \mathbb{Z} \text{ and } \mathcal{V}[1] = \{2n \mid n \geq 0\}.$$

Iteration doesn't terminate:

	$\perp$	$F(\perp)$	$F^2(\perp)$	$F^3(\perp)$	
$\mathcal{V}[0]$	$\emptyset$	$\mathbb{Z}$	$\mathbb{Z}$	$\mathbb{Z}$	$\ldots$
$\mathcal{V}[1]$	$\emptyset$	$\{0\}$	$\{0, 2\}$	$\{0, 2, 4\}$	