Existence of least solutions: Knaster-Tarski

Fact: In a complete lattice $\mathbb{D}$, every monotone function $f : \mathbb{D} \to \mathbb{D}$ has a least fixpoint a.

> Fixpoint: an element x such that $f(x) = x$.
>
> Prefixpoint: an element x such that $f(x) \sqsubseteq x$.

Existence of least solutions: Knaster-Tarski

Fact: In a complete lattice $\mathbb{D}$, every monotone function $f : \mathbb{D} \to \mathbb{D}$ has a least fixpoint a.

> Fixpoint: an element x such that $f(x) = x$.
>
> Prefixpoint: an element x such that $f(x) \sqsubseteq x$.

Let $P = \{x \in \mathbb{D} \mid f(x) \sqsubseteq x\}$ (the set of prefixpoints).

The least fixpoint of f is $a = \bigsqcap P$.

(1) $a \in P$:

$$f(a) \sqsubseteq f(d) \sqsubseteq d \text{ for all } d \in P.$$

$$\Longrightarrow \quad f(a) \text{ is a lower bound of } P.$$

$$\Longrightarrow \quad f(a) \sqsubseteq a.$$

$\implies \qquad a$ is the least prefixpoint.

(2) $f(a) = a$:

$$
\begin{array}{ll}
 & f(a) \sqsubseteq a, \text{ from } (1) \\
\implies & f^2(a) \sqsubseteq f(a), \text{ by monotonicity} \\
\implies & f(a) \in P \\
\implies & a \sqsubseteq f(a)
\end{array}
$$

Hence a is the least prefixpoint and is also a fixpoint.

Hence a is also the least fixpoint.

Example 1: Consider partial order $\mathbb{D}_1 = \mathbb{N}$ with $0 \sqsubseteq 1 \sqsubseteq 2 \sqsubseteq \ldots$.

The function $f(x) = x+1$ is monotonic.

However it has no fixpoint.

Actually $\mathbb{D}_1$ is not a complete lattice.

Example 1: Consider partial order $\mathbb{D}_1 = \mathbb{N}$ with $0 \sqsubseteq 1 \sqsubseteq 2 \sqsubseteq \ldots$.

The function $f(x) = x+1$ is monotonic.

However it has no fixpoint.

Actually $\mathbb{D}_1$ is not a complete lattice.

Example 2: Now we consider $\mathbb{D}_2 = \mathbb{N} \cup \{\infty\}$.

This is a complete lattice.

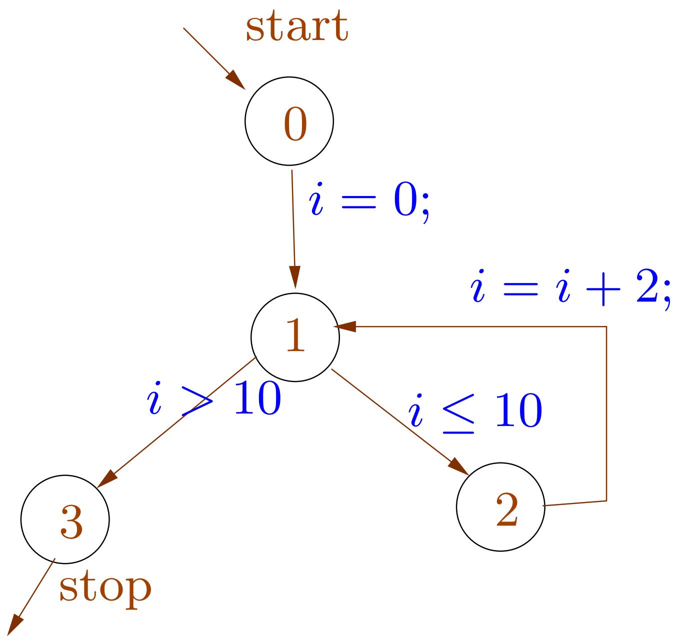
The function $f(x) = x+1$ is again monotonic.

The only fixpoint is ∞: $\infty+1 = \infty$.

Abstract Interpretation: Cousot, Cousot 1977

We use a suitable complete lattice as the domain of abstract values.

Example: intervals as abstract values:



$\mathcal{I}[0]$	$\bot$	$[-\infty, \infty]$	$[-\infty, \infty]$	$[-\infty, \infty]$	$[-\infty, \infty]$
$\mathcal{I}[1]$	$\bot$	$[0, 0]$	$[0, 2]$	$[0, 12]$	$[0, 12]$
$\mathcal{I}[2]$	$\bot$	$[0, 0]$	$[0, 2] \dots$	$[0, 10]$	$[0, 10]$
$\mathcal{I}[3]$	$\bot$	$\bot$	$\bot$	$[11, 12]$	$[11, 12]$

The analysis guarantees e.g. that at node 1 the value of i is always in the interval $[0, 12]$.

We have the set of concrete states $\mathcal{S} = (\mathsf{Vars} \to \mathbb{Z})$.

We choose a complete lattice $\mathbb{D}$ of abstract states.

We define an abstraction relation

$$\Delta \quad : \mathcal{S} \times \mathbb{D}$$

with the condition that

$$\rho \;\; \Delta \;\; a \quad \wedge \quad a \sqsubseteq b \quad \Longrightarrow \quad \rho \;\; \Delta \;\; b$$

$$\begin{tikzcd}
a \arrow[rr, "\sqsubseteq"] & & b \\
\rho \arrow[u, "\Delta"] \arrow[urr, dashed, "\Delta"'] & &
\end{tikzcd}$$

The concretization function: $\qquad \gamma(a) = \{\rho \mid \rho \;\; \Delta \;\; a\}$.

Example: For a program on two integer variables, $\mathsf{Vars} = \{x, y\}$.

The concrete states are from the set $\mathcal{S} = (\mathsf{Vars} \to \mathbb{Z})$ (or equivalently $\mathbb{Z}^2$).

For interval analysis, we choose the complete lattice

$$\mathbb{D}_{\mathbb{I}} = (\mathsf{Vars} \to \mathbb{I})_{\perp} = (\mathsf{Vars} \to \mathbb{I}) \cup \{\perp\}$$

where $\mathbb{I} = \{[l, u] \mid l \in \mathbb{Z} \cup \{-\infty\}, u \in \mathbb{Z} \cup \{\infty\}, l \leq u\}$ is the set of intervals.

Partial order on $\mathbb{I}$: $[l_1, u_1] \sqsubseteq [l_2, u_2]$ iff $l_1 \geq l_2$ and $u_1 \leq u_2$

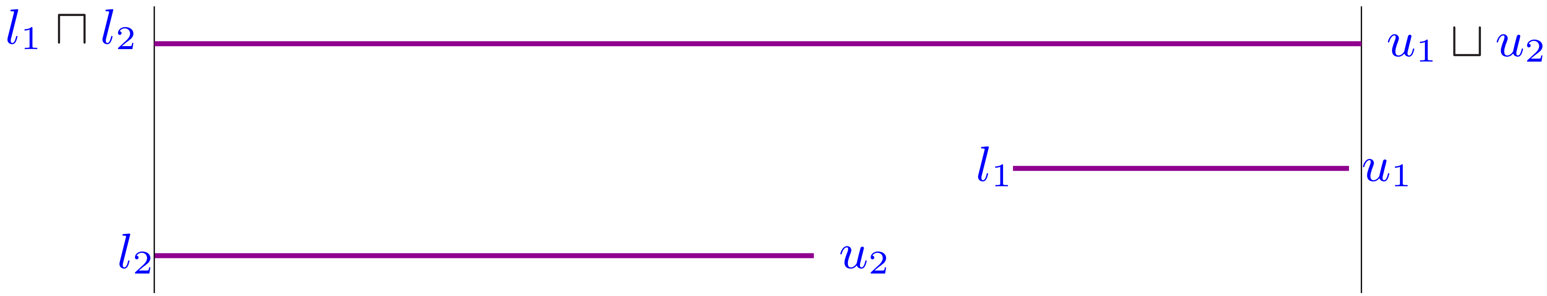
(As usual, $-\infty \leq n \leq \infty$ for all $n \in \mathbb{Z}$.)

Partial order on $\mathsf{Vars} \to \mathbb{I}$: $\quad D_1 \sqsubseteq D_2 \quad$ iff $D_1(x) \sqsubseteq D_2(x)$.

Extension to $(\mathsf{Vars} \to \mathbb{I})_\perp$: $\quad \perp \sqsubseteq D \quad$ for all D.

$(\mathsf{Vars} \to \mathbb{I})_\perp$ is a complete lattice. $(\mathsf{Vars} \to \mathbb{I})$ is not.

In particular we define $[l_1, u_1] \sqcup [l_2, u_2] = [l_1 \sqcap l_2, u_1 \sqcup u_2]$.



$\perp$ represents the "unreachable state": maps every variable to the "empty interval".

The abstraction relation:

$$\rho \ \Delta \ D \quad \text{iff} \quad D \neq \bot \ \text{ and } \ \rho(x) \ \Delta \ D(x) \text{ for each } x.$$

where $n \ \Delta \ [l, u]$ iff $l \leq n \leq u$.

The abstraction relation:

$$\rho \ \Delta \ D \quad \text{iff} \quad D \neq \bot \ \text{ and } \ \rho(x) \ \Delta \ D(x) \text{ for each } x.$$

where $n \ \Delta \ [l, u]$ iff $l \leq n \leq u$.

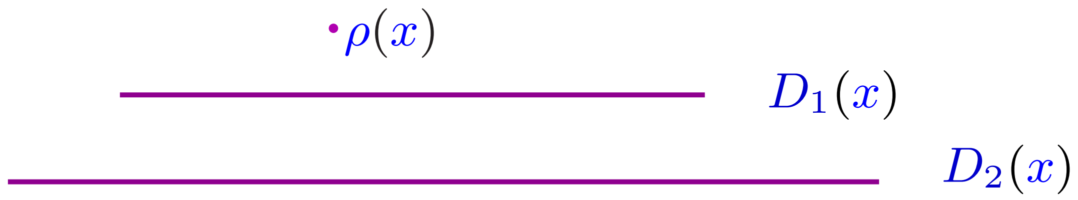
This satisfies the required condition:

Suppose $\rho \ \Delta \ D_1$ and $D_1 \sqsubseteq D_2$.

$\implies$ $D_1 \neq \bot$ and $D_2 \neq \bot$.

$\rho(x) \ \Delta \ D_1(x)$ and $D_1(x) \sqsubseteq D_2(x)$ for each x.

$\implies$ $\rho(x) \ \Delta \ D_1(x)$ for each x.



The concretization function:

$$\gamma(\bot) = \{\}$$

$$\gamma(D) = \{\rho \mid \rho(x) \ \ \Delta \ \ D(x)\}, \qquad \text{for } D \neq \bot$$

$$\begin{aligned}\gamma(\{x \mapsto [3,5], y \mapsto [0,7]\}) = \qquad & \{\{x \mapsto 3, y \mapsto 0\}, \{x \mapsto 3, y \mapsto 1\}, \\ & \ldots \{x \mapsto 3, y \mapsto 7\} \\ & \ldots \{x \mapsto 5, y \mapsto 0\} \ldots \{x \mapsto 5, y \mapsto 7\}\}\end{aligned}$$

Abstraction of the partial transformation induced by edges.

Recall the edges $k = (u, l, v)$ induce a partial transformation on concrete states:

$$[\![k]\!] \;=\; [\![l]\!] \;:\mathcal{S} \rightarrow \mathcal{S}$$

Now on our chosen domain $\mathbb{D}$ we define a monotonic abstract transformation:

$$[\![k]\!]^\sharp \;=\; [\![l]\!]^\sharp \;:\mathbb{D} \rightarrow \mathbb{D}$$

The abstract transformation should simulate the concrete transformation:

$$\text{if} \quad \rho \;\Delta\; a \quad \text{and} \quad [\![l]\!]\;\rho \text{ is defined} \quad \text{then} \quad [\![l]\!]\;\rho \;\Delta\; [\![l]\!]^\sharp\; a.$$

$$\begin{tikzcd}
a \arrow[rr, "{[\![k]\!]^\sharp}"] & & {} \\
\rho \arrow[u, "\Delta"] \arrow[rr, "{[\![k]\!]}"'] & & {} \arrow[u, dashed, "\Delta"']
\end{tikzcd}$$

Abstract transformation for interval analysis.

For concrete operators $\Box$ we define monotonic abstract operators $\Box^\sharp$ such that

$$x_1 \;\Delta\; a_1 \wedge \ldots \wedge x_n \;\Delta\; a_n \Longrightarrow \Box(x_1, \ldots, x_n) \;\Delta\; \Box^\sharp(a_1, \ldots, a_n)$$

$$\begin{array}{llllll}
\text{addition:} & [l_1, u_1] & +^\sharp & [l_2, u_2] & = [l_1 + l_2, u_1 + u_2]. \\
 & _ & + & \infty & = \infty \\
 & _ & + & -\infty & = \infty \\
 & & & & // \;\infty + -\infty \text{ is undefined.} \\
 & & & & \\
\text{substraction:} & & -^\sharp & [l, u] & = [-u, -l]
\end{array}$$

Multiplication: $[l_1, u_1] \quad *^\sharp \quad [l_2, u_2] \quad = [m, n]$ where

$$
\begin{aligned}
m &= l_1 l_2 \sqcap l_1 u_2 \sqcap u_1 l_2 \sqcap u_1 u_2 \\
n &= l_1 l_2 \sqcup l_1 u_2 \sqcup u_1 l_2 \sqcup u_1 u_2
\end{aligned}
$$

Example:

$$
\begin{array}{rcll}
[1, 3] & *^\sharp & [5, 8] & = [5, 24] \\
[-1, 3] & *^\sharp & [5, 8] & = [-8, 24] \\
[-1, 3] & *^\sharp & [-5, 8] & = [-15, 24] \\
[-1, 3] & *^\sharp & [-5, -8] & = [-24, 5]
\end{array}
$$

Equality test:

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

Example:

$$\begin{aligned} [7,7] &\quad ==^\sharp \quad [7,7] &&= [1,1] \\ [1,7] &\quad ==^\sharp \quad [9,12] &&= [0,0] \\ [1,7] &\quad ==^\sharp \quad [1,7] &&= [0,1] \end{aligned}$$

Inequality test:

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

Example:

$$\begin{aligned} [1,7] & \quad <^\sharp \quad [9,12] & = [1,1] \\ [9,12] & \quad <^\sharp \quad [1,7] & = [0,0] \\ [1,7] & \quad <^\sharp \quad [6,8] & = [0,1] \end{aligned}$$

Monotonic abstract evaluation of expressions

For $D \neq \bot$,

$$
\begin{aligned}
[\![x]\!]^\sharp \; D &= D(x) \\
[\![n]\!]^\sharp \; D &= [n, n] \\
[\![\Box(e_1, \ldots, e_n)]\!]^\sharp \; D &= \Box^\sharp([\![e_1]\!]^\sharp \; D, \ldots, [\![e_n]\!]^\sharp \; D)
\end{aligned}
$$

Monotonic abstract evaluation of expressions

For $D \neq \perp$,

$$\begin{aligned}
[\![x]\!]^\sharp\ D &= D(x)\\
[\![n]\!]^\sharp\ D &= [n, n]\\
[\![\Box(e_1, \ldots, e_n)]\!]^\sharp\ D &= \Box^\sharp([\![e_1]\!]^\sharp\ D, \ldots, [\![e_n]\!]^\sharp\ D)
\end{aligned}$$

Fact: $\rho \ \Delta \ D$ and $[\![e]\!]\ \rho$ is defined $\Longrightarrow [\![e]\!]\ \rho \ \Delta \ [\![e]\!]^\sharp\ D$.

Monotonic abstract evaluation of expressions

For $D \neq \bot$,

$$\begin{aligned} [\![x]\!]^\sharp\ D &= D(x) \\ [\![n]\!]^\sharp\ D &= [n, n] \\ [\![\Box(e_1, \ldots, e_n)]\!]^\sharp\ D &= \Box^\sharp([\![e_1]\!]^\sharp\ D, \ldots, [\![e_n]\!]^\sharp\ D) \end{aligned}$$

Fact: $\rho \ \ \Delta \ \ D$ and $[\![e]\!]\ \rho$ is defined $\Longrightarrow [\![e]\!]\ \rho \ \ \Delta \ \ [\![e]\!]^\sharp\ D$.

Case e is x: since $\rho \ \ \Delta \ \ D$ hence $[\![x]\!]\ \rho = \rho(x) \ \ \Delta \ \ D(x) = [\![x]\!]^\sharp\ D$

Monotonic abstract evaluation of expressions

For $D \neq \bot$,

$$
\begin{aligned}
[\![x]\!]^\sharp\ D &= D(x) \\
[\![n]\!]^\sharp\ D &= [n, n] \\
[\![\Box(e_1, \ldots, e_n)]\!]^\sharp\ D &= \Box^\sharp([\![e_1]\!]^\sharp\ D, \ldots, [\![e_n]\!]^\sharp\ D)
\end{aligned}
$$

Fact: $\rho \;\Delta\; D$ and $[\![e]\!]\ \rho$ is defined $\Longrightarrow [\![e]\!]\ \rho \;\Delta\; [\![e]\!]^\sharp\ D$.

Case e is x: since $\rho \;\Delta\; D$ hence $[\![x]\!]\ \rho = \rho(x) \;\Delta\; D(x) = [\![x]\!]^\sharp\ D$

Case e is n: $[\![n]\!]\ \rho = n \;\Delta\; [n, n] = [\![n]\!]^\sharp\ D$

Monotonic abstract evaluation of expressions

For $D \neq \bot$,

$$\begin{aligned}
[\![x]\!]^\sharp\ D &= D(x) \\
[\![n]\!]^\sharp\ D &= [n, n] \\
[\![\Box(e_1, \ldots, e_n)]\!]^\sharp\ D &= \Box^\sharp([\![e_1]\!]^\sharp\ D, \ldots, [\![e_n]\!]^\sharp\ D)
\end{aligned}$$

Fact: $\rho \ \Delta \ D$ and $[\![e]\!]\ \rho$ is defined $\Longrightarrow [\![e]\!]\ \rho \ \Delta \ [\![e]\!]^\sharp\ D$.

Case e is x: since $\rho \ \Delta \ D$ hence $[\![x]\!]\ \rho = \rho(x) \ \Delta \ D(x) = [\![x]\!]^\sharp\ D$

Case e is n: $[\![n]\!]\ \rho = n \ \Delta \ [n, n] = [\![n]\!]^\sharp\ D$

Case e is $\Box(e_1, \ldots, e_n)$: since each $[\![e_i]\!]\ \rho \ \Delta \ [\![e_i]\!]^\sharp\ D$ hence

$$\begin{aligned}
[\![\Box(e_1, \ldots, e_n)]\!]\ \rho &= \Box([\![e_1]\!]\ \rho, \ldots, [\![e_n]\!]\ \rho) \\
&\Delta \\
\Box^\sharp([\![e_1]\!]^\sharp\ D, \ldots, [\![e_n]\!]^\sharp\ D) &= [\![\Box^\sharp(e_1, \ldots, e_n)]\!]^\sharp\ D
\end{aligned}$$

Finally, the monotonic abstract transformations induced by edges

$$
\begin{array}{rrcl}
& [\![l]\!]^\sharp \; \bot & = & \bot \\
\text{For } D \neq \bot, & [\![;]\!]^\sharp \; D & = & D \\
& [\![x = e;]\!]^\sharp \; D & = & D \oplus \{x \mapsto [\![e]\!]^\sharp \; D\} \\
& [\![e]\!]^\sharp \; D & = & \begin{cases} \bot & \text{if } [\![e]\!]^\sharp \; D = [0,0] \\ D & \text{otherwise} \end{cases}
\end{array}
$$

Finally, the monotonic abstract transformations induced by edges

$$
\begin{array}{rrcl}
 & [\![l]\!]^\sharp\ \bot & = & \bot \\
\text{For } D \neq \bot, & [\![;]\!]^\sharp\ D & = & D \\
 & [\![x = e;]\!]^\sharp\ D & = & D \oplus \{x \mapsto [\![e]\!]^\sharp\ D\} \\
 & [\![e]\!]^\sharp\ D & = & \begin{cases} \bot & \text{if } [\![e]\!]^\sharp\ D = [0,0] \\ D & \text{otherwise} \end{cases}
\end{array}
$$

Next we must check the condition:

$$\rho \ \Delta \ D \quad \wedge \quad [\![l]\!]\ \rho = \rho_1 \quad \wedge \quad [\![l]\!]^\sharp\ D = D_1 \quad \Longrightarrow \quad \rho_1 \ \Delta \ D_1 .$$

Finally, the monotonic abstract transformations induced by edges

$$
\begin{array}{lrl}
 & [\![l]\!]^\sharp \; \bot & = \bot \\
\text{For } D \neq \bot, & [\![;]\!]^\sharp \; D & = D \\
 & [\![x = e;]\!]^\sharp \; D & = D \oplus \{x \mapsto [\![e]\!]^\sharp \; D\} \\
 & [\![e]\!]^\sharp \; D & = \begin{cases} \bot & \text{if } [\![e]\!]^\sharp \; D = [0,0] \\ D & \text{otherwise} \end{cases}
\end{array}
$$

Next we must check the condition:

$$\rho \;\;\Delta\;\; D \quad\wedge\quad [\![l]\!] \; \rho = \rho_1 \quad\wedge\quad [\![l]\!]^\sharp \; D = D_1 \quad\Longrightarrow\quad \rho_1 \;\;\Delta\;\; D_1.$$

Clearly $D \neq \bot$ here.

To check: $\rho \;\Delta\; D \;\wedge\; [\![l]\!]\,\rho = \rho_1 \;\wedge\; [\![l]\!]^\sharp\, D = D_1 \;\Longrightarrow\; \rho_1 \;\Delta\; D_1.$

Case l is ;

$$\rho_1 = \rho \;\Delta\; D = D_1.$$

To check: $\rho \;\Delta\; D \;\wedge\; [\![l]\!]\;\rho = \rho_1 \;\wedge\; [\![l]\!]^\sharp\; D = D_1 \implies \rho_1 \;\Delta\; D_1.$

Case l is ;

$$\rho_1 = \rho \;\Delta\; D = D_1.$$

Case l is $x = e$;

$$\rho_1 = \rho \oplus \{x \mapsto [\![e]\!]\;\rho\} \quad \text{and} \quad D_1 = D \oplus \{x \mapsto [\![e]\!]^\sharp\; D\}$$

As $[\![e]\!]\;\rho \;\Delta\; [\![e]\!]^\sharp\; D$ hence $\rho_1 \;\Delta\; D_1.$

To check: $\rho \;\Delta\; D \;\wedge\; [\![l]\!]\,\rho = \rho_1 \;\wedge\; [\![l]\!]^\sharp\, D = D_1 \implies \rho_1 \;\Delta\; D_1$.

Case l is ;

$$\rho_1 = \rho \;\Delta\; D = D_1.$$

Case l is $x = e$;

$$\rho_1 = \rho \oplus \{x \mapsto [\![e]\!]\,\rho\} \quad \text{and} \quad D_1 = D \oplus \{x \mapsto [\![e]\!]^\sharp\, D\}$$

As $[\![e]\!]\,\rho \;\Delta\; [\![e]\!]^\sharp\, D$ hence $\rho_1 \;\Delta\; D_1$.

Case e is some condition e

Since the tranformation $[\![e]\!]\,\rho$ is defined,

hence the expression evaluation $[\![e]\!]\,\rho \neq 0$, and $\rho_1 = \rho$.

Since $\rho \;\Delta\; D$,

hence the abstract expression evaluation $[\![e]\!]^\sharp\, D \neq [0, 0]$, and $D_1 = D$.

Recall, for a path $\pi = k_1 \ldots k_n$,

$$[\![\pi]\!]\ \rho = ([\![k_n]\!]\ \circ \ldots \circ [\![k_1]\!]\ )\rho$$

$$[\![\pi]\!]^\sharp\ D = ([\![k_n]\!]^\sharp\ \circ \ldots \circ [\![k_1]\!]^\sharp\ )D$$

We conclude from above:
if $\rho \;\; \Delta \;\; D$ and $[\![\pi]\!]\ \rho$ is defined then $[\![\pi]\!]\ \rho \;\; \Delta \;\; [\![\pi]\!]^\sharp\ D$.

$$\begin{tikzcd}
D \arrow[r, "{[\![k_1]\!]^\sharp}"] & {} & {} \arrow[r, "{[\![k_2]\!]^\sharp}"] & {} \arrow[r, "{[\![k_3]\!]^\sharp}"] & {} & \cdots & {} \arrow[r, "{[\![k_n]\!]^\sharp}"] & {} \\
\rho \arrow[u, "\Delta"] \arrow[r, "{[\![k_1]\!]}"'] & {} \arrow[u, dashed, "\Delta"] & {} \arrow[r, "{[\![k_2]\!]}"'] & {} \arrow[u, dashed, "\Delta"] \arrow[r, "{[\![k_3]\!]}"'] & {} \arrow[u, dashed, "\Delta"] & \cdots & {} \arrow[u, dashed, "\Delta"] \arrow[r, "{[\![k_n]\!]}"'] & {} \arrow[u, dashed, "\Delta"]
\end{tikzcd}$$

Merge over All Paths (MOP):

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

For any initial concrete state ρ and path $\pi : \mathit{start} \to^* v$, if $[\![\pi]\!]\ \rho$ is defined then

$$[\![\pi]\!]\ \rho \quad \Delta \quad \mathcal{D}^*[v]$$

Hence $\mathcal{D}^*[v]$ abstracts all states possible at node v.

Merge over All Paths (MOP):

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

For any initial concrete state ρ and path $\pi : start \to^* v$, if $[\![\pi]\!]\ \rho$ is defined then

$$[\![\pi]\!]\ \rho \quad \Delta \quad \mathcal{D}^*[v]$$

Hence $\mathcal{D}^*[v]$ abstracts all states possible at node v.

To compute it, we use the constraint system:

$$\begin{array}{lll} \mathcal{D}[start] & \sqsupseteq \top & \\ \mathcal{D}[v] & \sqsupseteq [\![k]\!]^\sharp\ \mathcal{D}[u] & \text{for edge } k = (u, l, v) \end{array}$$

Merge over All Paths (MOP):

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

For any initial concrete state ρ and path $\pi : start \to^* v$, if $[\![\pi]\!]\ \rho$ is defined then

$$[\![\pi]\!]\ \rho \quad \Delta \quad \mathcal{D}^*[v]$$

Hence $\mathcal{D}^*[v]$ abstracts all states possible at node v.

To compute it, we use the constraint system:

$$\begin{array}{lll} \mathcal{D}[start] & \sqsupseteq \top & \\ \mathcal{D}[v] & \sqsupseteq [\![k]\!]^\sharp\ \mathcal{D}[u] & \text{for edge } k = (u, l, v) \end{array}$$

How are the two related?

Merge over All Paths (MOP):

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

Theorem: Kam,Ullman 1975

Let $\mathcal{D}$ be the smallest solution of the constraint system

$$\begin{array}{lll} \mathcal{D}[start] & \sqsupseteq D_0 & \\ \mathcal{D}[v] & \sqsupseteq [\![k]\!]^\sharp\ \mathcal{D}[u] & \text{for edge } k = (u, l, v) \end{array}$$

Then we have

$$\begin{array}{lll} & \mathcal{D}[v] \sqsupseteq \mathcal{D}^*[v] & \text{for every } v \\ \text{In other words:} & \mathcal{D}[v] \sqsupseteq [\![\pi]\!]^\sharp\ D_0 & \text{for every } \pi : start \to^* v \end{array}$$

Proof: induction on the length of π:

Proof: induction on the length of π:

Case $\pi = \epsilon$ (empty path).

Proof: induction on the length of π:

Case $\pi = \epsilon$ (empty path).

$$[\![\pi]\!]^\sharp\ D_0 = D_0 \sqsubseteq \mathcal{D}[\mathit{start}]$$

Proof: induction on the length of π:

Case $\pi = \epsilon$ (empty path).

$$[\![\pi]\!]^\sharp \; D_0 = D_0 \sqsubseteq \mathcal{D}[start]$$

Induction step: $\pi = \pi' k$ for $k = (u, l, v)$.

Proof: induction on the length of π:

Case $\pi = \epsilon$ (empty path).

$$[\![\pi]\!]^\sharp\ D_0 = D_0 \sqsubseteq \mathcal{D}[start]$$

Induction step: $\pi = \pi' k$ for $k = (u, l, v)$.

$$\begin{array}{lll} [\![\pi']\!]^\sharp\ D_0 & \sqsubseteq \mathcal{D}[u] & \text{induction hypothesis} \\ [\![\pi]\!]^\sharp\ D_0 & = [\![k]\!]^\sharp\ ([\![\pi']\!]^\sharp\ D_0) & \\ & \sqsubseteq [\![k]\!]^\sharp\ (\mathcal{D}[u]) & \text{monotonicity} \\ & \sqsubseteq \mathcal{D}[v] & \mathcal{D} \text{ is a solution} \end{array}$$

Question:

Does the constraint system give us only an upper bound ?

Question:

Does the constraint system give us only an upper bound ?

Answer:

In general yes.

Question:

Does the constraint system give us only an upper bound ?

Answer:

In general yes.

Now let's assume that all the functions $[\![k]\!]^\sharp$ are distributive ...

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

- distributive, when $f(\bigsqcup X) = \bigsqcup\{f(x) \mid x \in X\}$ for all $\emptyset \neq X \subseteq \mathbb{D}_1$.
- strict, when $f(\bot) = \bot$.
- total distributive, when f is strict and distributive.

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

- distributive, when $f(\bigsqcup X) = \bigsqcup\{f(x) \mid x \in X\}$ for all $\emptyset \neq X \subseteq \mathbb{D}_1$.
- strict, when $f(\bot) = \bot$.
- total distributive, when f is strict and distributive.

Example 1: $\mathbb{D}_1 = \mathbb{D}_2 = (2^U, \subseteq)$ for some set U.

$f(x) = x \cap A \cup B$ for some $A, B \subseteq U$.

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

- distributive, when $f(\bigsqcup X) = \bigsqcup\{f(x) \mid x \in X\}$ for all $\emptyset \neq X \subseteq \mathbb{D}_1$.
- strict, when $f(\bot) = \bot$.
- total distributive, when f is strict and distributive.

Example 1: $\mathbb{D}_1 = \mathbb{D}_2 = (2^U, \subseteq)$ for some set U.

$f(x) = x \cap A \cup B$ for some $A, B \subseteq U$.

Strictness: $f(\emptyset) = B \implies$ strict only if $B = \emptyset$.

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

- distributive, when $f(\bigsqcup X) = \bigsqcup\{f(x) \mid x \in X\}$ for all $\emptyset \neq X \subseteq \mathbb{D}_1$.
- strict, when $f(\bot) = \bot$.
- total distributive, when f is strict and distributive.

Example 1: $\mathbb{D}_1 = \mathbb{D}_2 = (2^U, \subseteq)$ for some set U.

$f(x) = x \cap A \cup B$ for some $A, B \subseteq U$.

Strictness: $f(\emptyset) = B \implies$ strict only if $B = \emptyset$.

Distributivity:

$$\begin{aligned} f(x \cup y) &= (x \cup y) \cap A \cup B \\ &= (x \cap A) \cup (y \cap A) \cup B \\ &= (x \cap A \cup B) \cup (y \cap A \cup B) \qquad \text{Yes} \end{aligned}$$

Example 2: $\mathbb{D}_1 = \mathbb{D}_2 = \mathbb{N} \cup \{\infty\}, \quad f(x) = x+1.$

Example 2: $\mathbb{D}_1 = \mathbb{D}_2 = \mathbb{N} \cup \{\infty\}, \quad f(x) = x{+}1.$

Strictness: $f(\perp) = 0{+}1 = 1 \neq \perp$ No

Example 2: $\mathbb{D}_1 = \mathbb{D}_2 = \mathbb{N} \cup \{\infty\}, \quad f(x) = x+1.$

Strictness: $f(\bot) = 0+1 = 1 \neq \bot$ No

Distributivity: $f(\bigsqcup X) = 1 + \bigsqcup X = \bigsqcup\{x+1 \mid x \in X\} = \bigsqcup\{f(x) \mid x \in X\}$ for $\emptyset \neq X$ Yes

Example 2: $\mathbb{D}_1 = \mathbb{D}_2 = \mathbb{N} \cup \{\infty\}$, $\quad f(x) = x{+}1$.

Strictness: $f(\bot) = 0{+}1 = 1 \neq \bot$ No

Distributivity: $f(\bigsqcup X) = 1{+}\bigsqcup X = \bigsqcup\{x{+}1 \mid x \in X\} = \bigsqcup\{f(x) \mid x \in X\}$ for $\emptyset \neq X$ Yes

Example 3: $\mathbb{D}_1 = (\mathbb{N} \cup \{\infty\})^2$, $\quad \mathbb{D}_2 = \mathbb{N} \cup \{\infty\}$, $\quad f(x, y) = x{+}y$

Example 2: $\mathbb{D}_1 = \mathbb{D}_2 = \mathbb{N} \cup \{\infty\}, \quad f(x) = x+1.$

Strictness: $f(\bot) = 0+1 = 1 \neq \bot$ No

Distributivity: $f(\bigsqcup X) = 1+\bigsqcup X = \bigsqcup\{x+1 \mid x \in X\} = \bigsqcup\{f(x) \mid x \in X\}$ for $\emptyset \neq X$ Yes

Example 3: $\mathbb{D}_1 = (\mathbb{N} \cup \{\infty\})^2, \quad \mathbb{D}_2 = \mathbb{N} \cup \{\infty\}, \quad f(x, y) = x+y$

Strictness: $f(\bot) = 0+0 = 0 = \bot$ Yes

Example 2: $\mathbb{D}_1 = \mathbb{D}_2 = \mathbb{N} \cup \{\infty\}, \quad f(x) = x+1.$

Strictness: $f(\bot) = 0+1 = 1 \neq \bot$ No

Distributivity: $f(\bigsqcup X) = 1+\bigsqcup X = \bigsqcup\{x+1 \mid x \in X\} = \bigsqcup\{f(x) \mid x \in X\}$ for $\emptyset \neq X$ Yes

Example 3: $\mathbb{D}_1 = (\mathbb{N} \cup \{\infty\})^2, \quad \mathbb{D}_2 = \mathbb{N} \cup \{\infty\}, \quad f(x, y) = x+y$

Strictness: $f(\bot) = 0+0 = 0 = \bot$ Yes

Distributivity: $f((1, 4) \sqcup (4, 1)) = f(4, 4) = 8 \neq 5 = f(1, 4) \sqcup f(4, 1)$ No

Assumption: All nodes v are reachable from the node $start$.

(Unreachable nodes can always be deleted.)

Theorem: If all the edge transofrmations $[\![k]\!]^\sharp$ are distributive then $\mathcal{D}^*[v] = \mathcal{D}[v]$ for all v.

Assumption: All nodes v are reachable from the node $start$.

(Unreachable nodes can always be deleted.)

Theorem: If all the edge transofrmations $[\![k]\!]^\sharp$ are distributive then $\mathcal{D}^*[v] = \mathcal{D}[v]$ for all v.

Proof: We show that $\mathcal{D}^*$ satisfies the constraint system.

(1) For the *start* node:

$$
\begin{aligned}
\mathcal{D}^*[start] &= \bigsqcup\{[\![\pi]\!]^\sharp\ D_0 \mid \pi : start \to start\} \\
&\sqsupseteq [\![\epsilon]\!]^\sharp\ D_0 \\
&= D_0
\end{aligned}
$$

(1) For the *start* node:

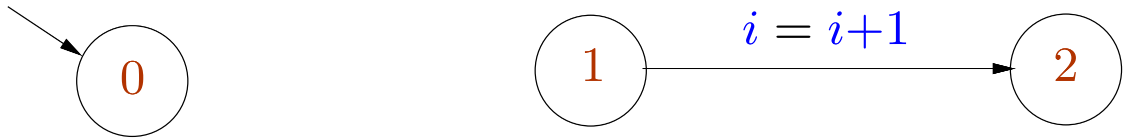
$$\begin{aligned}\mathcal{D}^*[start] &= \bigsqcup\{[\![\pi]\!]^\sharp\ D_0 \mid \pi : start \to start\}\\ &\sqsupseteq [\![\epsilon]\!]^\sharp\ D_0\\ &= D_0\end{aligned}$$

(2) For every edge $k = (u, l, v)$

$$\begin{aligned}\mathcal{D}^*[v] &= \bigsqcup\{[\![\pi]\!]^\sharp\ D_0 \mid \pi : start \to v\}\\ &\sqsupseteq \bigsqcup\{[\![\pi' k]\!]^\sharp\ D_0 \mid \pi' : start \to u\}\\ &= \bigsqcup\{[\![k]\!]^\sharp\ ([\![\pi']\!]^\sharp\ D_0) \mid \pi' : start \to u\}\\ &= [\![k]\!]^\sharp\ (\bigsqcup\{[\![\pi']\!]^\sharp\ D_0 \mid \pi' : start \to u\})\\ &= [\![k]\!]^\sharp\ (\mathcal{D}^*[u])\end{aligned}$$

since $\{\pi' \mid \pi' : start \to u\}$ is non-empty.

The result does not hold in case of unreachable nodes.



We consider $\mathbb{D} = \mathbb{N} \cup \{\infty\}$ with ordering $0 \sqsubseteq 1 \sqsubseteq 2 \sqsubseteq \ldots \sqsubseteq \infty$.

Abstraction relation: $n \;\; \Delta \;\; a$ iff $n \leq a$.

The abstract transformation for the second edge is defined by $[\![k]\!]^\sharp \; a = a+1$.

We choose $D_0 = 5$.

We have the constraints $\mathcal{D}[0] \sqsupseteq 5$ and $\mathcal{D}[2] \sqsupseteq \mathcal{D}[1]+1$.

We have

$$\mathcal{D}^*[2] = \bigsqcup \emptyset = 0$$
$$\mathcal{D}[2] = 0+1 = 1$$