Design and Analysis of Real-Time Systems

Foundations of Abstract Interpretation and Numerical Abstractions

Jan Reineke

Advanced Lecture, Summer 2013

Recap I: Galois Connections and Best Abstract Transformer

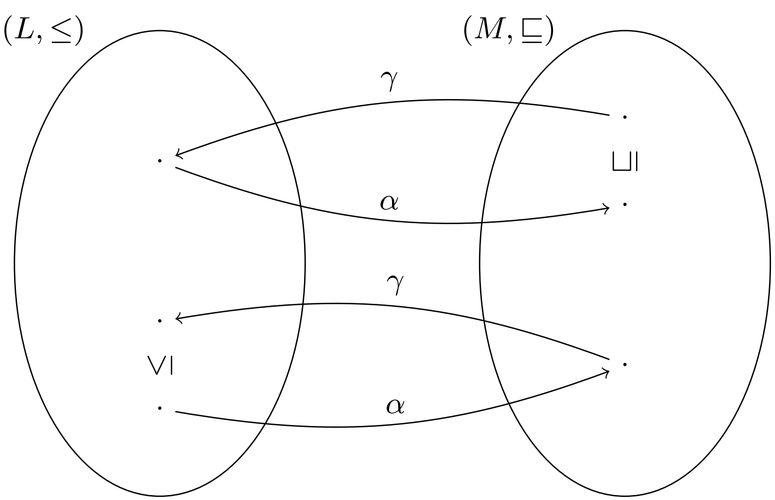
Notion of Galois connections:

Let $(L, \leq)$ *and* $(M, \sqsubseteq)$ *be partially ordered sets and* $\alpha \in L \to M$, $\gamma \in M \to L$. *We call* $(L, \leq) \overset{\gamma}{\underset{\alpha}{\leftrightarrows}} (M, \sqsubseteq)$ *a* Galois connection *if* α *and* γ *are monotone functions and*

$$\begin{array}{rcl} l & \leq & \gamma(\alpha(l)) \\ \alpha(\gamma(m)) & \sqsubseteq & m \end{array}$$

for all $l \in L$ *and* $m \in M$.

Graphically:



Recap I: Galois Connections and Best Abstract Transformer

Notion of Galois connections:

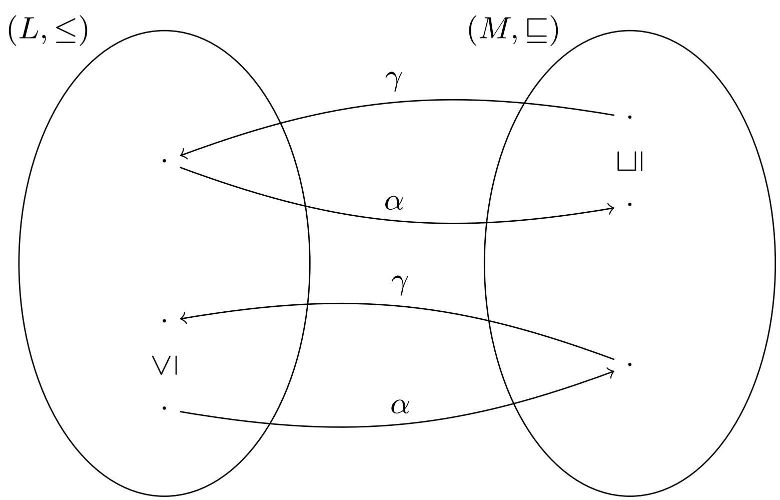
Let $(L, \leq)$ *and* $(M, \sqsubseteq)$ *be partially ordered sets and* $\alpha \in L \to M$, $\gamma \in M \to L$. *We call* $(L, \leq) \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} (M, \sqsubseteq)$ *a* Galois connection *if* α *and* γ *are monotone functions and*

$$\begin{array}{ccc} l & \leq & \gamma(\alpha(l)) \\ \alpha(\gamma(m)) & \sqsubseteq & m \end{array}$$

for all $l \in L$ *and* $m \in M$.

Why monotone?

Graphically:



Recap I: Galois Connections and Best Abstract Transformer

Notion of Galois connections:

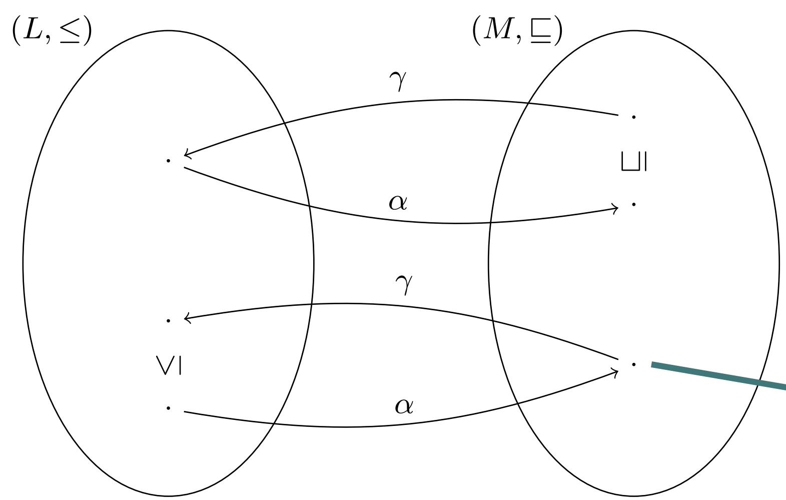
Let $(L, \leq)$ *and* $(M, \sqsubseteq)$ *be partially ordered sets and* $\alpha \in L \to M$, $\gamma \in M \to L$. *We call* $(L, \leq) \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} (M, \sqsubseteq)$ *a* Galois connection *if* α *and* γ *are monotone functions and*

$$\begin{array}{ccc} l & \leq & \gamma(\alpha(l)) \\ \alpha(\gamma(m)) & \sqsubseteq & m \end{array}$$

for all $l \in L$ *and* $m \in M$.

Why monotone?

Graphically:



For soundness.

Recap I: Galois Connections and Best Abstract Transformer

Notion of Galois connections:

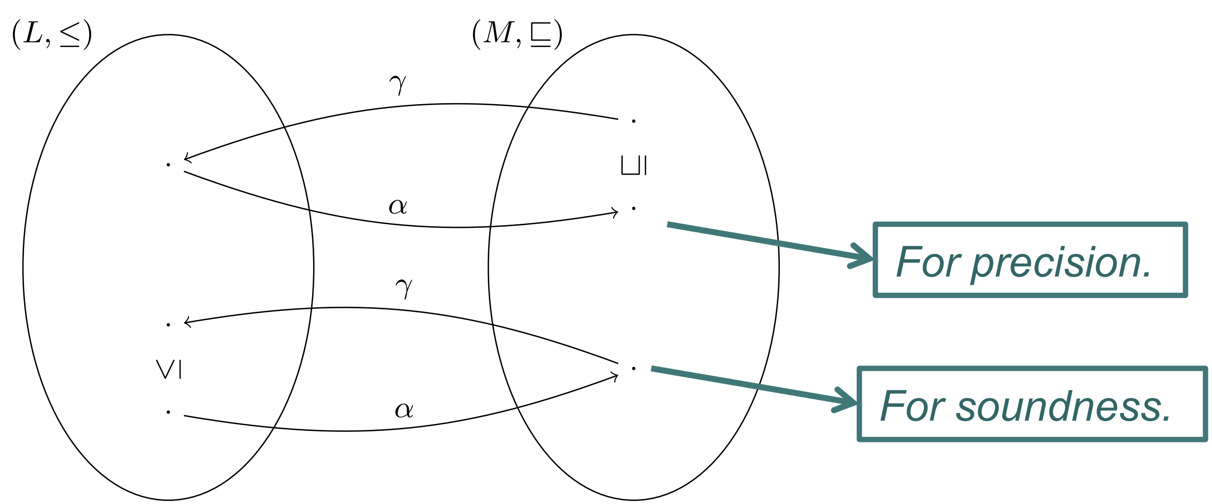
Let $(L, \leq)$ *and* $(M, \sqsubseteq)$ *be partially ordered sets and* $\alpha \in L \to M$, $\gamma \in M \to L$. *We call* $(L, \leq) \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} (M, \sqsubseteq)$ *a* Galois connection *if* α *and* γ *are monotone functions and*

$$\begin{aligned} l &\leq \gamma(\alpha(l)) \\ \alpha(\gamma(m)) &\sqsubseteq m \end{aligned}$$

for all $l \in L$ *and* $m \in M$.

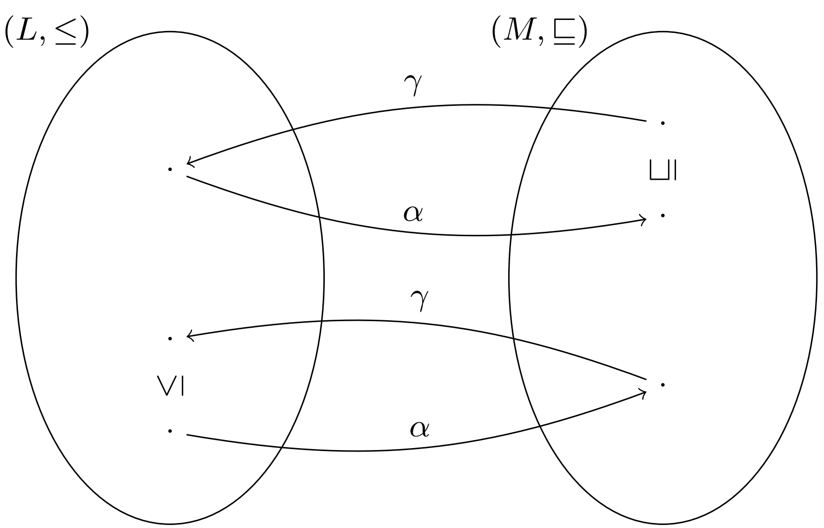
Why monotone?

Graphically:



Galois connections: Properties

Graphically:



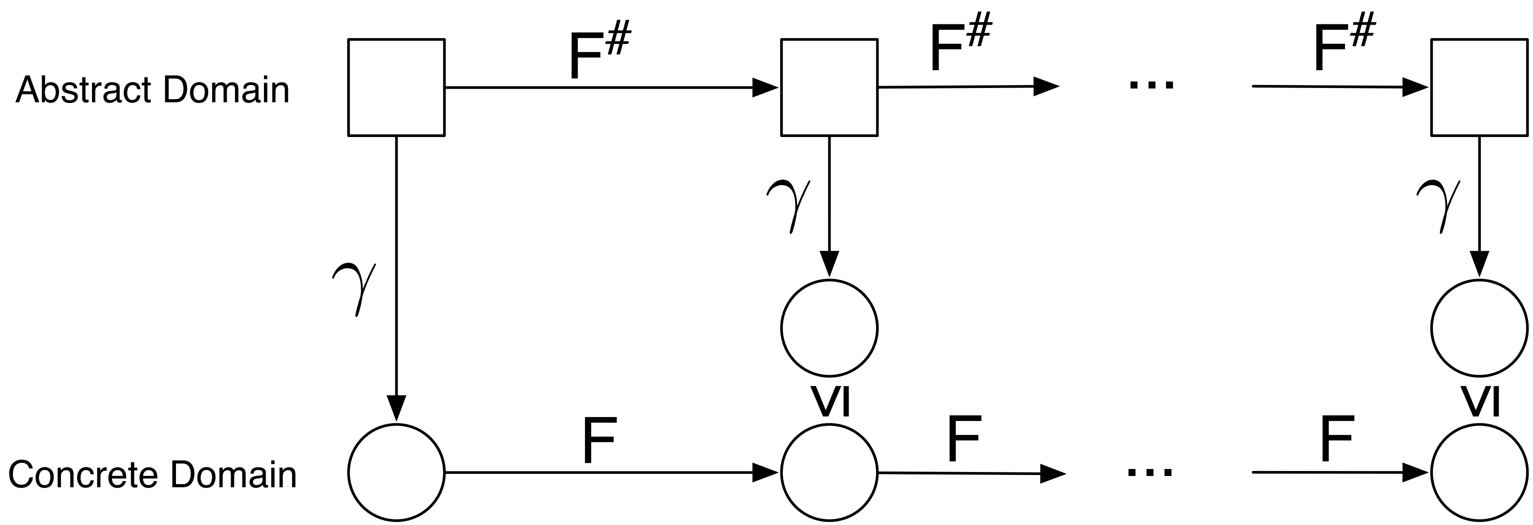
Properties:

1) *Can be used to systematically construct correct (and in fact the most precise) abstract operations:* $op^{\#} = \alpha \circ op \circ \gamma$
2) *a) Abstraction function uniquely determines concretization function*
   b) Concretization function uniquely determines abstraction function

Recap II: Tarski's Fixpoint Theorem and the Fixpoint Transfer Theorem

THEOREM 1 (KNASTER-TARSKI, 1955).
Assume $(D, \leq)$ *is a* complete lattice. *Then every* monotonic *function* $f : D \to D$ *has a* least fixed point $d_0 \in D$.

From Local to Global Correctness: Kleene Iteration



Fixpoint Transfer Theorem

Let $(L, \leq)$ and $(L^{\#}, \leq^{\#})$ be two lattices, $\gamma : L^{\#} \to L$ a monotone function, and $F : L \to L$ and $F^{\#} \to F^{\#}$ two monotone functions, with

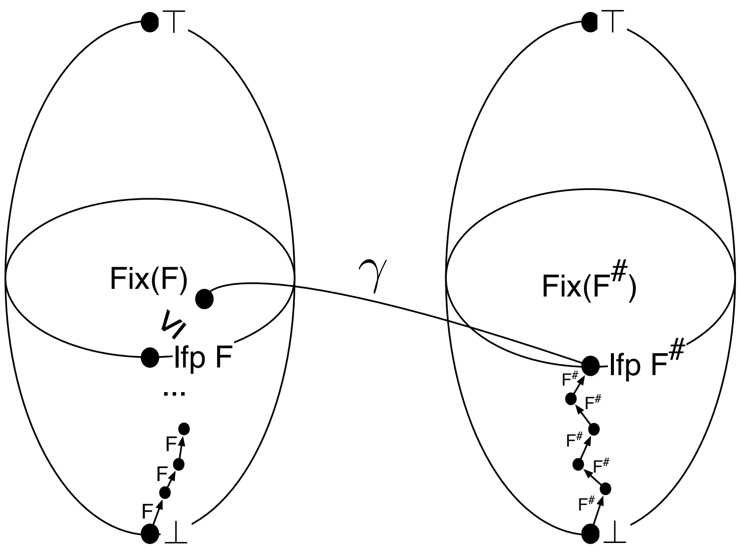
$$\forall l^{\#} \in L^{\#} : \gamma(F^{\#}(l^{\#})) \geq F(\gamma(l^{\#})).$$

Local Correctness

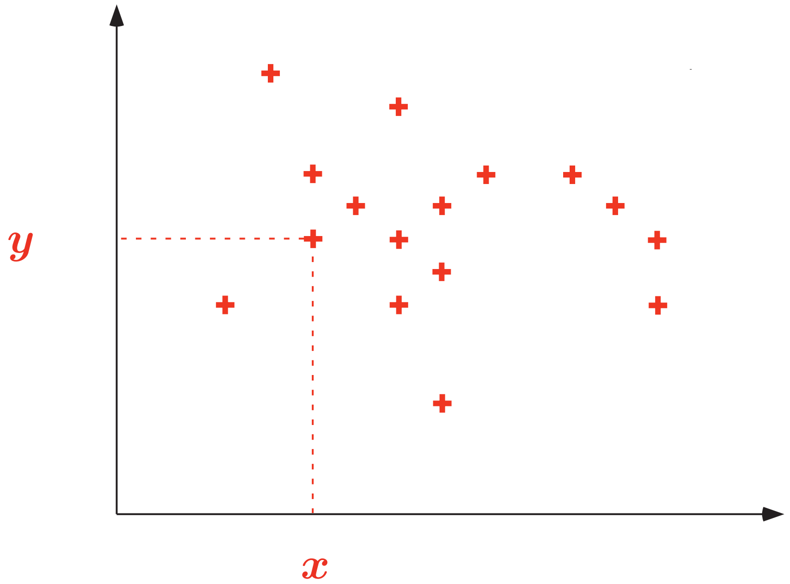
Then:

$$lfp\ F \leq \gamma(lfp\ F^{\#}).$$

Global Correctness

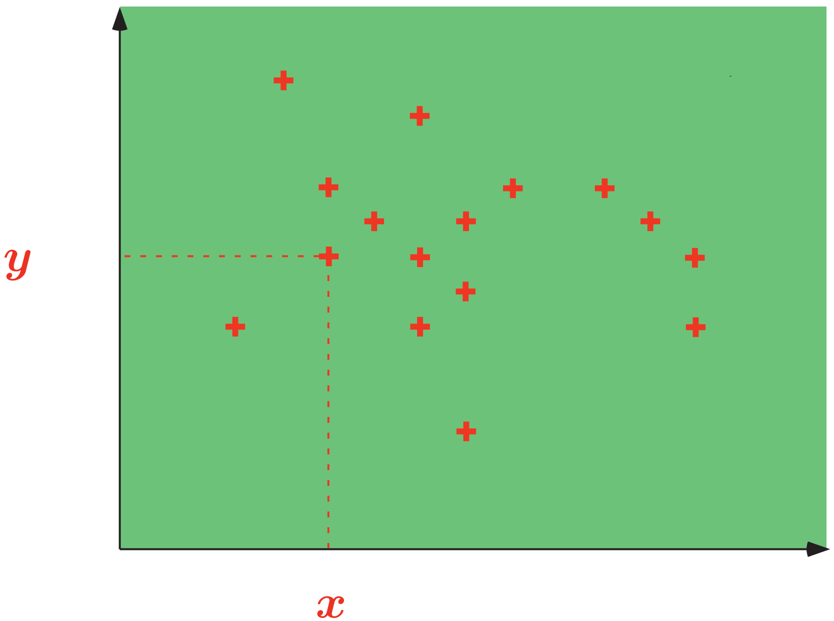


Overview: Numerical Abstractions



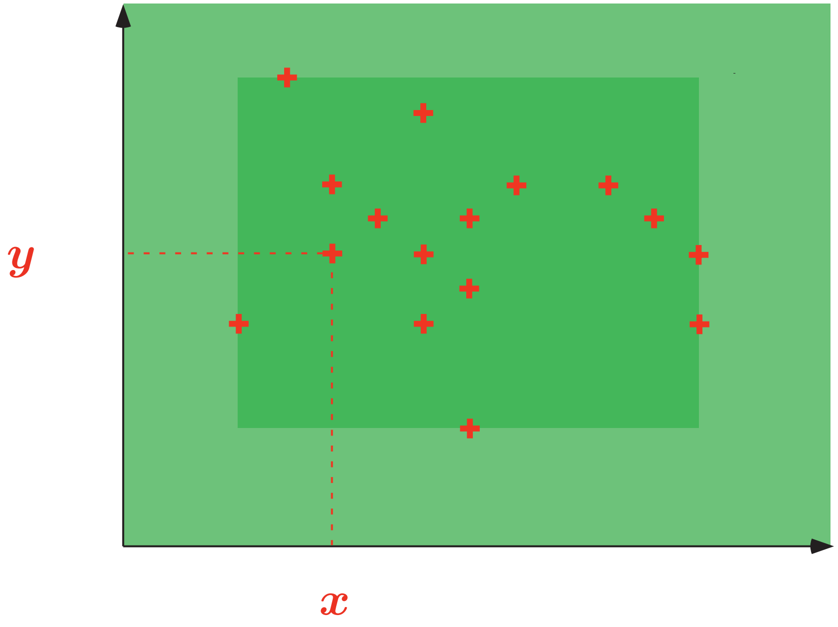
$$\{\ldots, \langle 19,\ 77 \rangle, \ldots, \langle 20,\ 03 \rangle, \ldots\}$$

Overview: Numerical Abstractions
Signs (Cousot & Cousot, 1979)



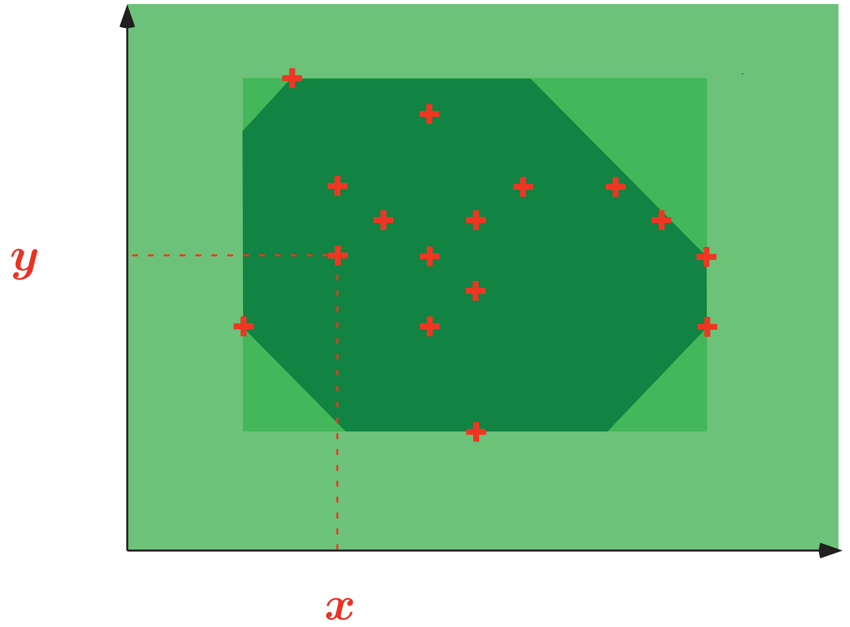
$$\begin{cases} x \geq 0 \\ y \geq 0 \end{cases}$$

Overview: Numerical Abstractions
Intervals (Cousot & Cousot, 1976)



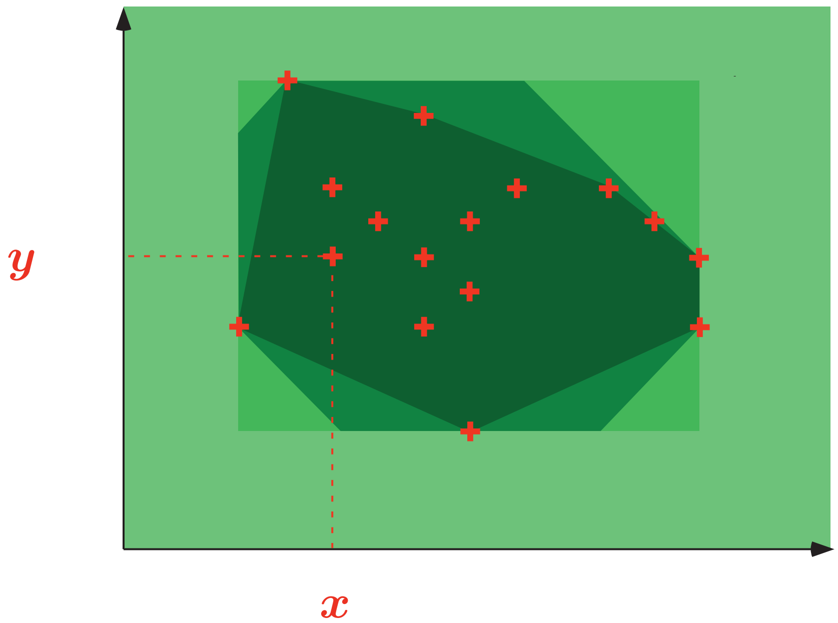
$$\begin{cases} x \in [19,\ 77] \\ y \in [20,\ 03] \end{cases}$$

Overview: Numerical Abstractions Octagons (Mine, 2001)



$$\begin{cases} 1 \leq x \leq 9 \\ x + y \leq 77 \\ 1 \leq y \leq 9 \\ x - y \leq 99 \end{cases}$$

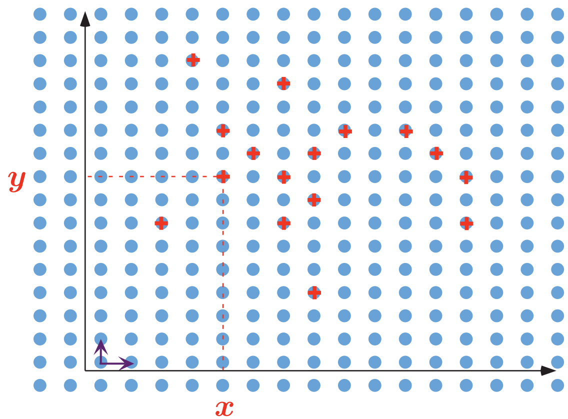
Overview: Numerical Abstractions
Polyhedra (Cousot & Halbwachs, 1978)



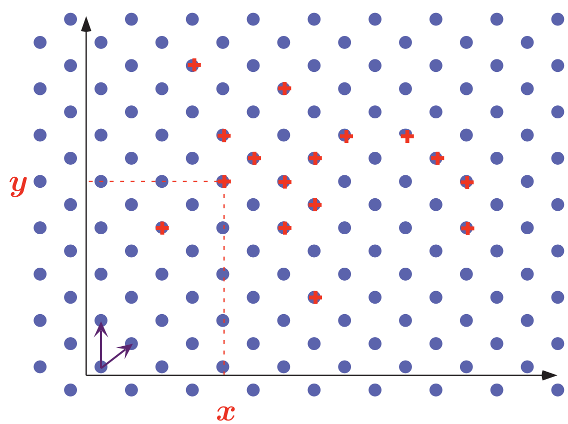
$$\begin{cases} 19x + 77y \leq 2004 \\ 20x + 03y \geq 0 \end{cases}$$

→ *Very Expensive…*

Overview: Numerical Abstractions Simple and Linear Congruences (Granger, 1989+1991)



$$\begin{cases} x = 19 \bmod 77 \\ y = 20 \bmod 99 \end{cases}$$



$$\begin{cases} 1x + 9y = 7 \bmod 8 \\ 2x - 1y = 9 \bmod 9 \end{cases}$$

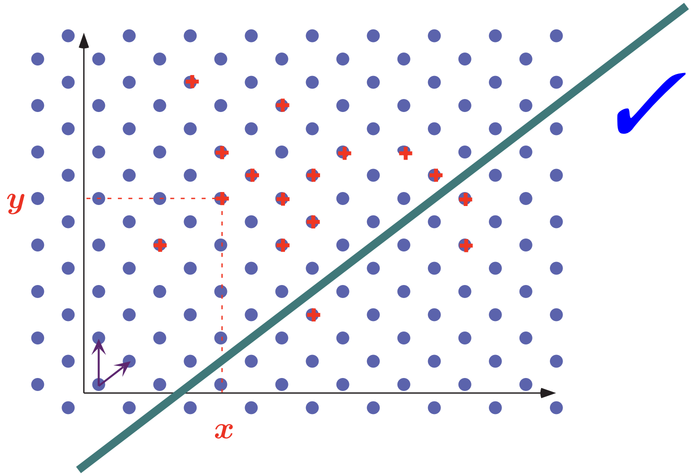
Numerical Abstractions

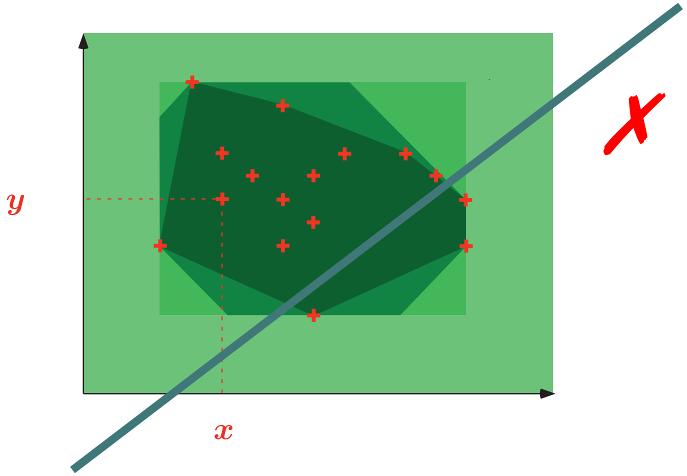
Which abstraction is the most precise?

Numerical Abstractions

Which abstraction is the most precise?

Depends on questions you want to answer!

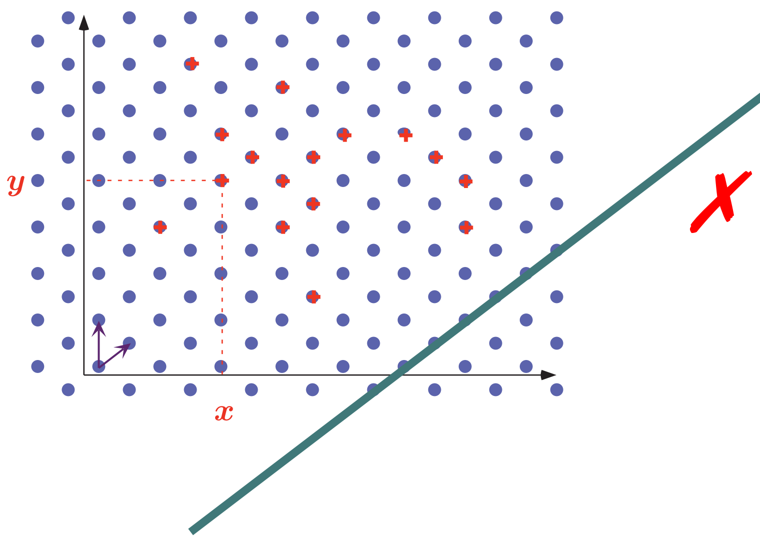


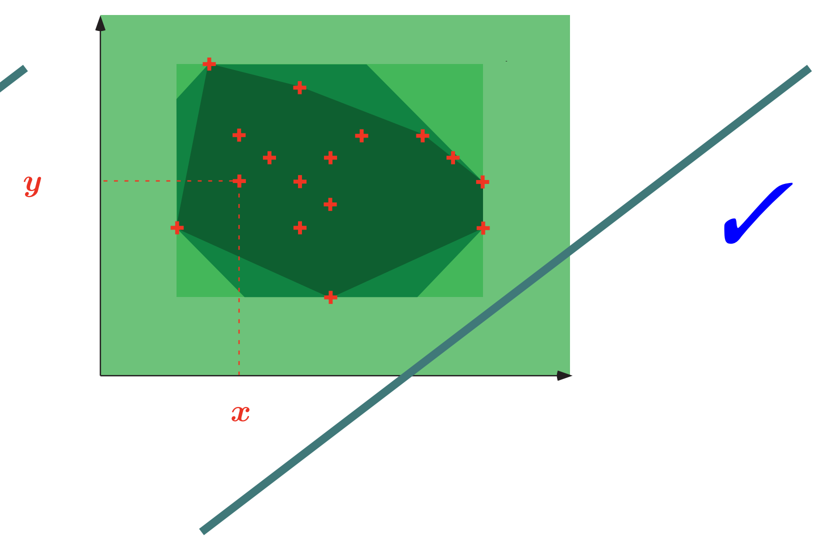


Numerical Abstractions

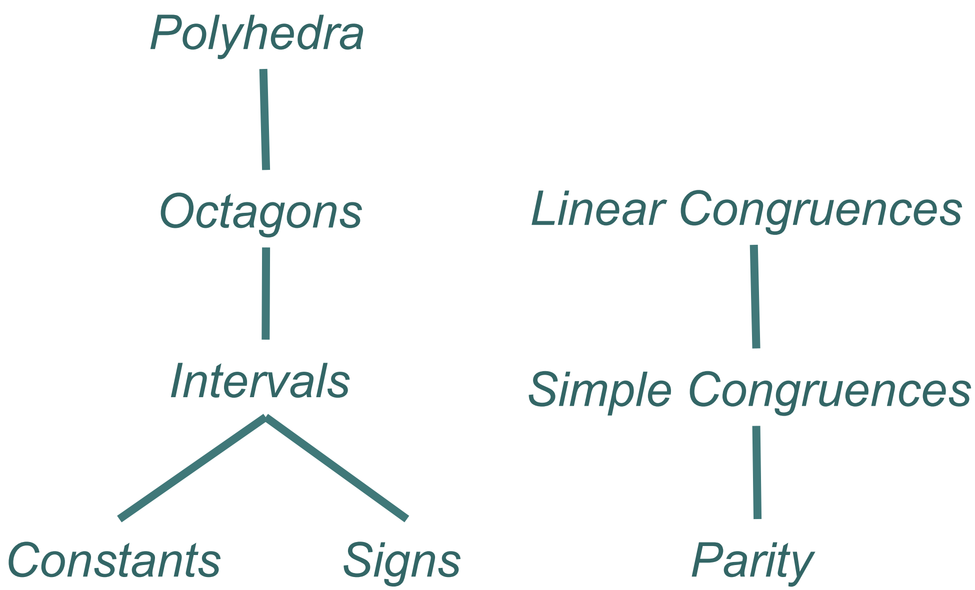
Which abstraction is the most precise?

Depends on questions you want to answer!

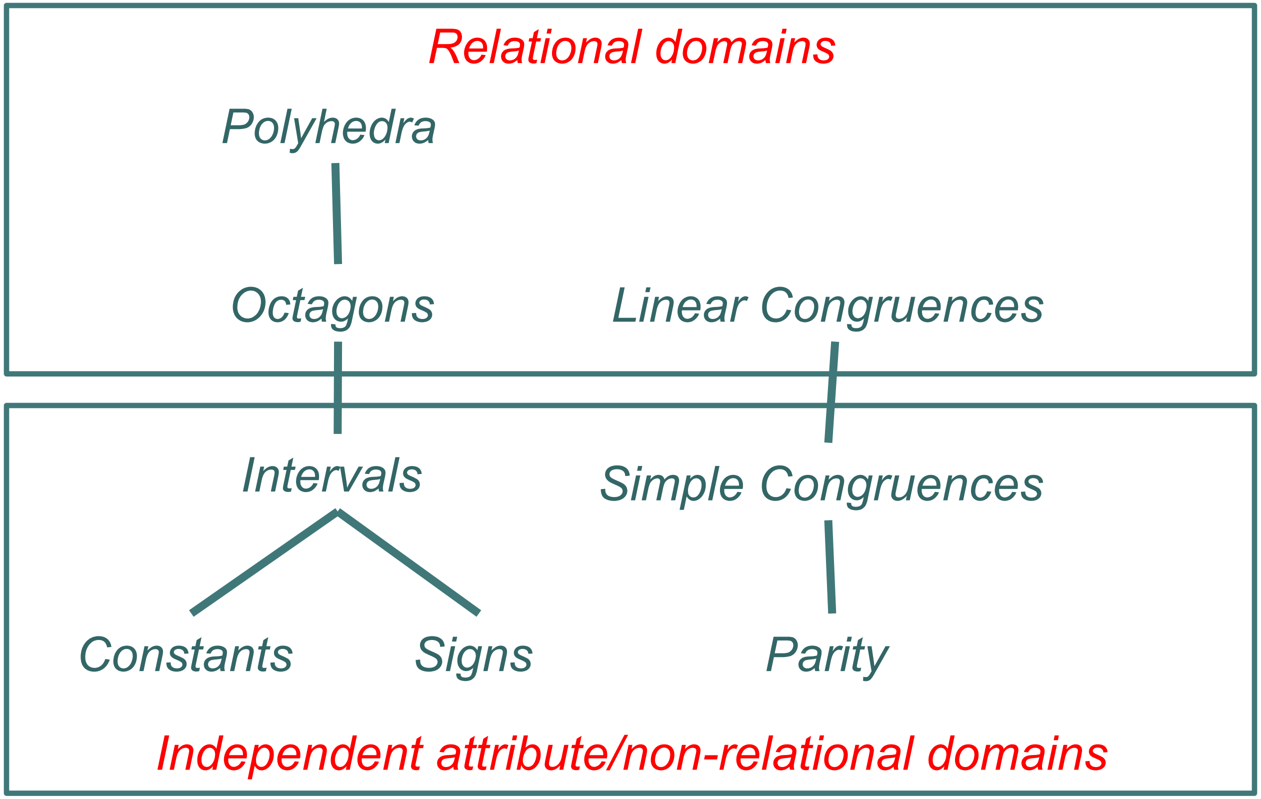




Partial Order of Abstractions



Partial Order of Abstractions



Characteristics of Non-relational Domains

- Non-relational/independent attribute abstraction:
  - Abstract each variable separately

$$(\mathcal{P}(\mathbb{Z}), \subseteq) \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} (\textsc{Numerical}, \sqsubseteq)$$

  - Maintains no relations between variable values
- Can be lifted to an abstraction of valuations of multiple variables in the expected way:

$$(\mathcal{P}(\mathit{Vars} \to \mathbb{Z}), \subseteq) \underset{\alpha_1}{\overset{\gamma_1}{\leftrightarrows}} (\mathit{Vars} \to \mathcal{P}(\mathbb{Z}), \leq) \underset{\alpha_2}{\overset{\gamma_2}{\leftrightarrows}} (\mathit{Vars} \to \textsc{Numerical}, \sqsubseteq)$$

$$\alpha_2(f) := \lambda x \in \mathit{Vars}.\alpha(f(x)) \qquad \gamma_2(f^\#) := \lambda x \in \mathit{Vars}.\gamma(f^\#(x))$$

The Interval Domain

Abstracts sets of values by enclosing interval

$$\textsc{Interval} = \{[l,u] \mid l \le u, l \in \mathbb{Z} \cup \{-\infty\}, u \in \mathbb{Z} \cup \{\infty\}\} \cup \{\bot\}$$

where $\le$ is appropriately extended from $\mathbb{Z} \times \mathbb{Z}$ to $(\mathbb{Z} \cup \{-\infty\}) \times (\mathbb{Z} \cup \{\infty\})$

Intervals are ordered by inclusion:

$$\bot \sqsubseteq x \quad \forall x \in \textsc{Interval}$$

$$[l,u] \sqsubseteq [l',u'] \ \textit{if} \ l' \le l \wedge u \le u'$$

$(\textsc{Interval}, \sqsubseteq)$ forms a complete lattice.

Concretization and Abstraction of Intervals

- Concretization:

$$\gamma(\bot) = \emptyset$$
$$\gamma([l, u]) = \{n \in \mathbb{Z} \mid l \leq n \leq u\}$$

- Abstraction:

$$\alpha(\emptyset) = \bot$$
$$\alpha(S) = [\inf S, \sup S]$$

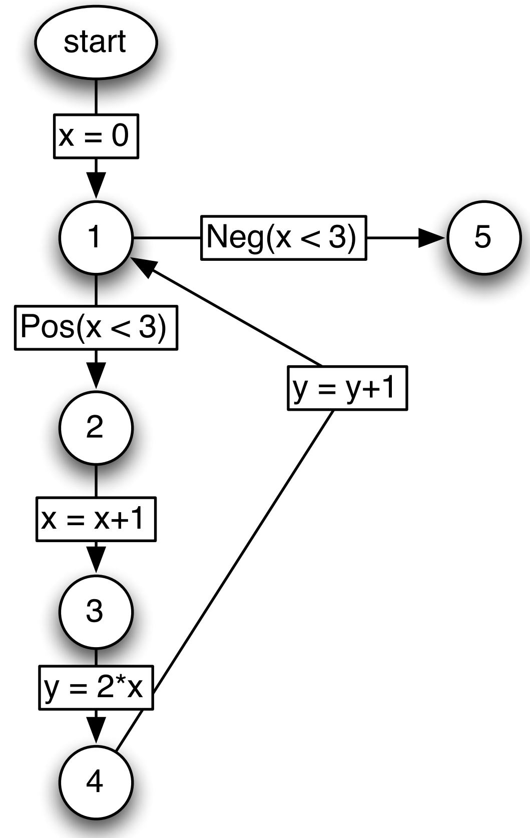
They form a Galois connection.

Interval Arithmetic

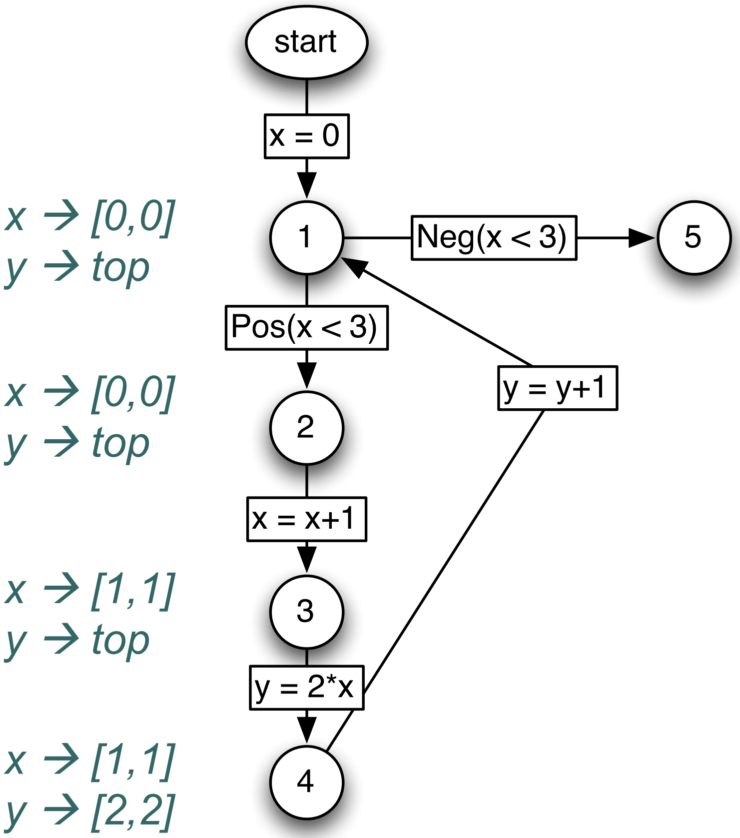
Calculating with Intervals:

$$
\begin{aligned}
[a, b] &\quad + \quad [c, d] &= \quad &[a + c, b + d] \\
[a, b] &\quad - \quad [c, d] &= \quad &[a - d, b - c] \\
[a, b] &\quad * \quad [c, d] &= \quad &[\min(ac, ad, bc, bd), \max(ac, ad, bc, bd)] \\
[a, b] &\quad / \quad [c, d] &= \quad &[a, b] * [1/d, 1/c], 0 \notin [c, d]
\end{aligned}
$$

Example: Interval Analysis



Example: Interval Analysis



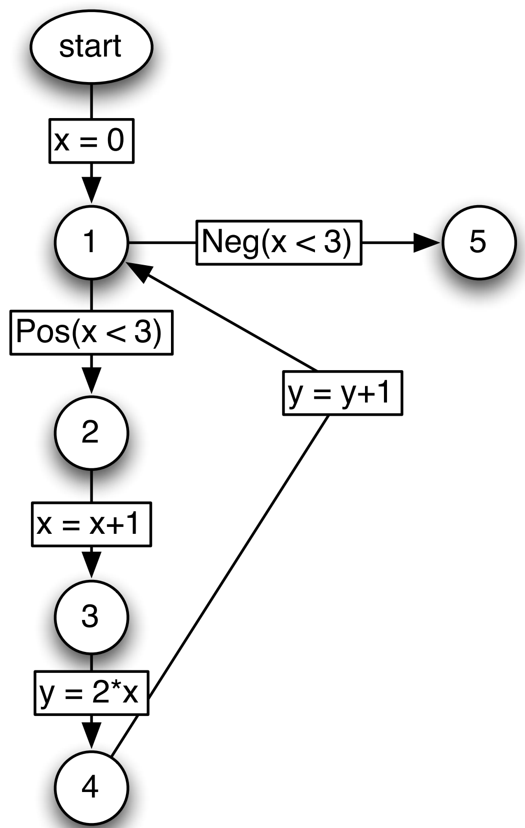
Example: Interval Analysis

x → [0,1]   x → [0,0]
y → [3,3]   y → top

x → [0,1]   x → [0,0]
y → [3,3]   y → top

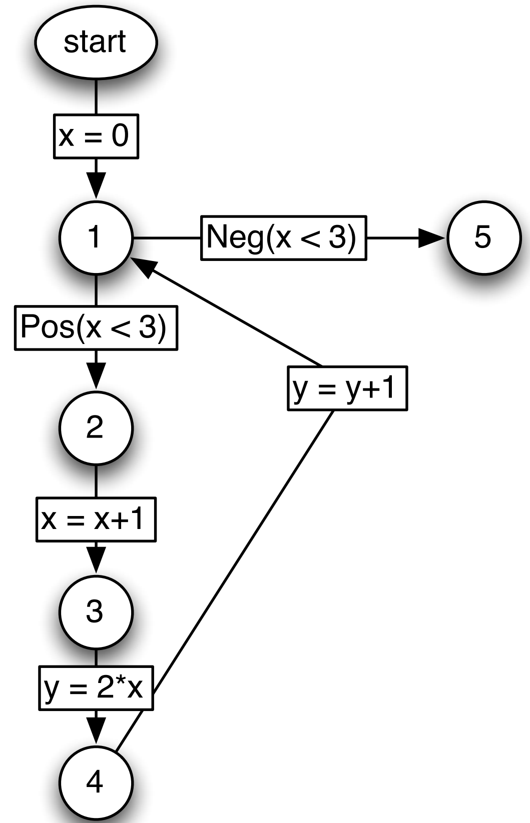
x → [1,2]   x → [1,1]
y → [3,3]   y → top

x → [1,2]   x → [1,1]
y → [2,4]   y → [2,2]



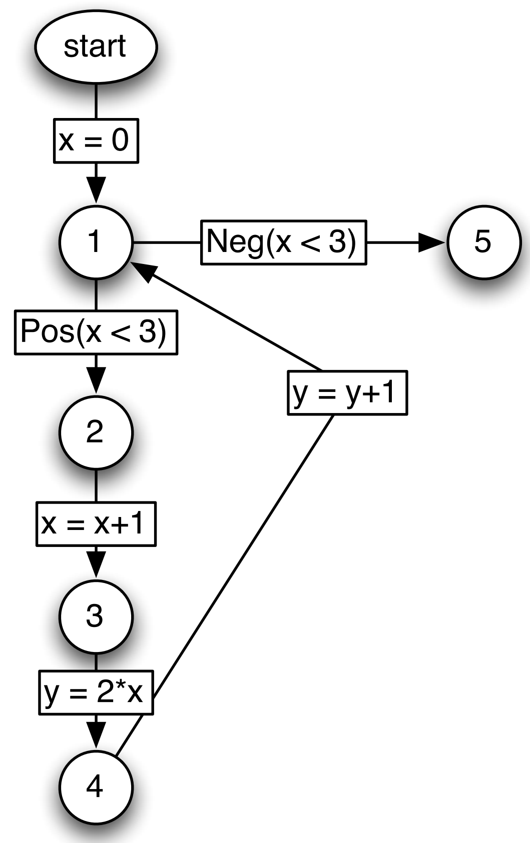
Example: Interval Analysis

x → [0,2] y → [3,5]	x → [0,1] y → [3,3]	x → [0,0] y → top
x → [0,2] y → [3,5]	x → [0,1] y → [3,3]	x → [0,0] y → top
x → [1,3] y → [3,5]	x → [1,2] y → [3,3]	x → [1,1] y → top
x → [1,3] y → [2,6]	x → [1,2] y → [2,4]	x → [1,1] y → [2,2]



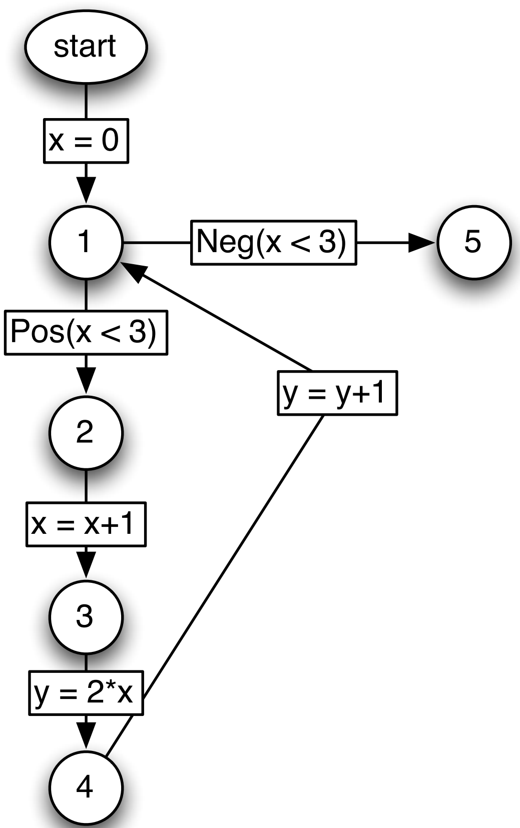
Example: Interval Analysis

x → [0,3] y → [3,7]	x → [0,2] y → [3,5]	x → [0,1] y → [3,3]	x → [0,0] y → top
	x → [0,2] y → [3,5]	x → [0,1] y → [3,3]	x → [0,0] y → top
	x → [1,3] y → [3,5]	x → [1,2] y → [3,3]	x → [1,1] y → top
	x → [1,3] y → [2,6]	x → [1,2] y → [2,4]	x → [1,1] y → [2,2]



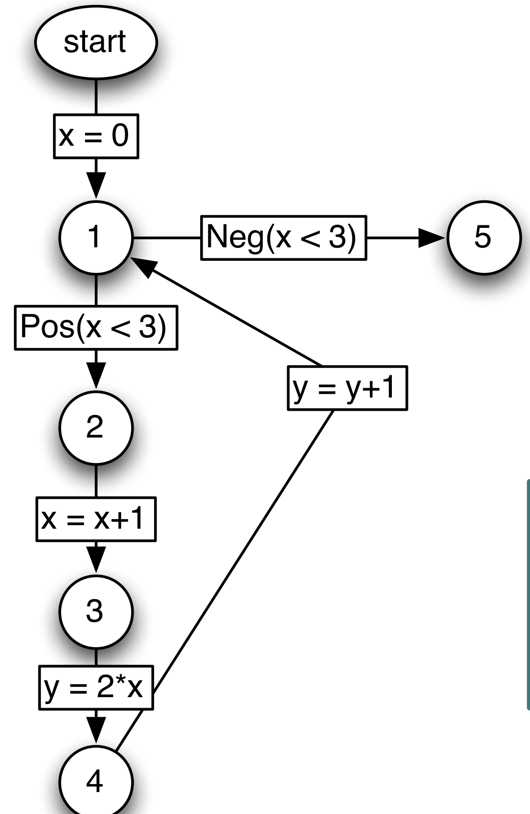
Example: Interval Analysis

x → [0,3] y → [3,7]	x → [0,2] y → [3,5]	x → [0,1] y → [3,3]	x → [0,0] y → top
	x → [0,2] y → [3,5]	x → [0,1] y → [3,3]	x → [0,0] y → top
	x → [1,3] y → [3,5]	x → [1,2] y → [3,3]	x → [1,1] y → top
	x → [1,3] y → [2,6]	x → [1,2] y → [2,4]	x → [1,1] y → [2,2]



x → [3,3]
y → [3,7]

Example: Interval Analysis



x → [0,3] y → [3,7] x → [0,2] y → [3,5] x → [0,1] y → [3,3] x → [0,0] y → top

x → [0,2] y → [3,5] x → [0,1] y → [3,3] x → [0,0] y → top

x → [1,3] y → [3,5] x → [1,2] y → [3,3] x → [1,1] y → top

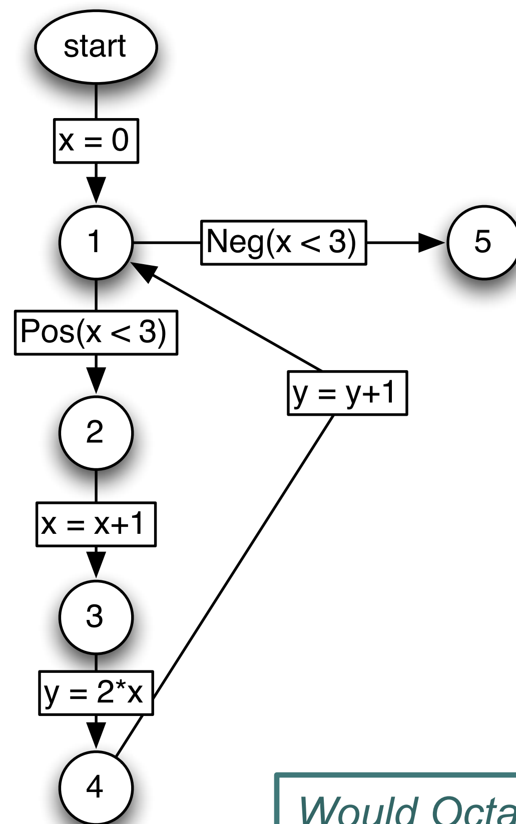
x → [1,3] y → [2,6] x → [1,2] y → [2,4] x → [1,1] y → [2,2]

x → [3,3] y → [3,7]

Imprecise due to non-relational analysis

Example: Interval Analysis

x → [0,3] y → [3,7]	x → [0,2] y → [3,5]	x → [0,1] y → [3,3]	x → [0,0] y → top
	x → [0,2] y → [3,5]	x → [0,1] y → [3,3]	x → [0,0] y → top
	x → [1,3] y → [3,5]	x → [1,2] y → [3,3]	x → [1,1] y → top
	x → [1,3] y → [2,6]	x → [1,2] y → [2,4]	x → [1,1] y → [2,2]



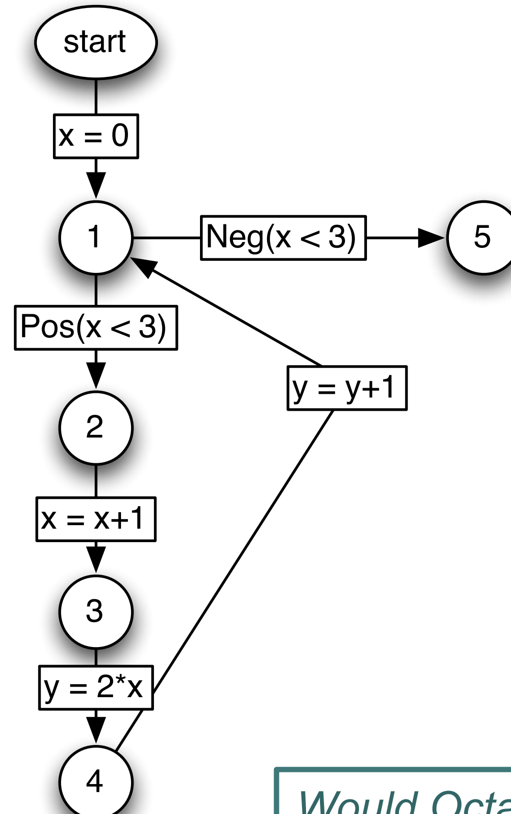
x → [3,3]
y → [3,7]

Imprecise due to non-relational analysis

Would Octagons determine that y must be 7 at program point 5?

Example: Interval Analysis

x → [0,3] y → [3,7]	x → [0,2] y → [3,5]	x → [0,1] y → [3,3]	x → [0,0] y → top
	x → [0,2] y → [3,5]	x → [0,1] y → [3,3]	x → [0,0] y → top
	x → [1,3] y → [3,5]	x → [1,2] y → [3,3]	x → [1,1] y → top
	x → [1,3] y → [2,6]	x → [1,2] y → [2,4]	x → [1,1] y → [2,2]



x → [3,3]
y → [3,7]

Imprecise due to non-relational analysis

Would Octagons determine that y must be 7 at program point 5?