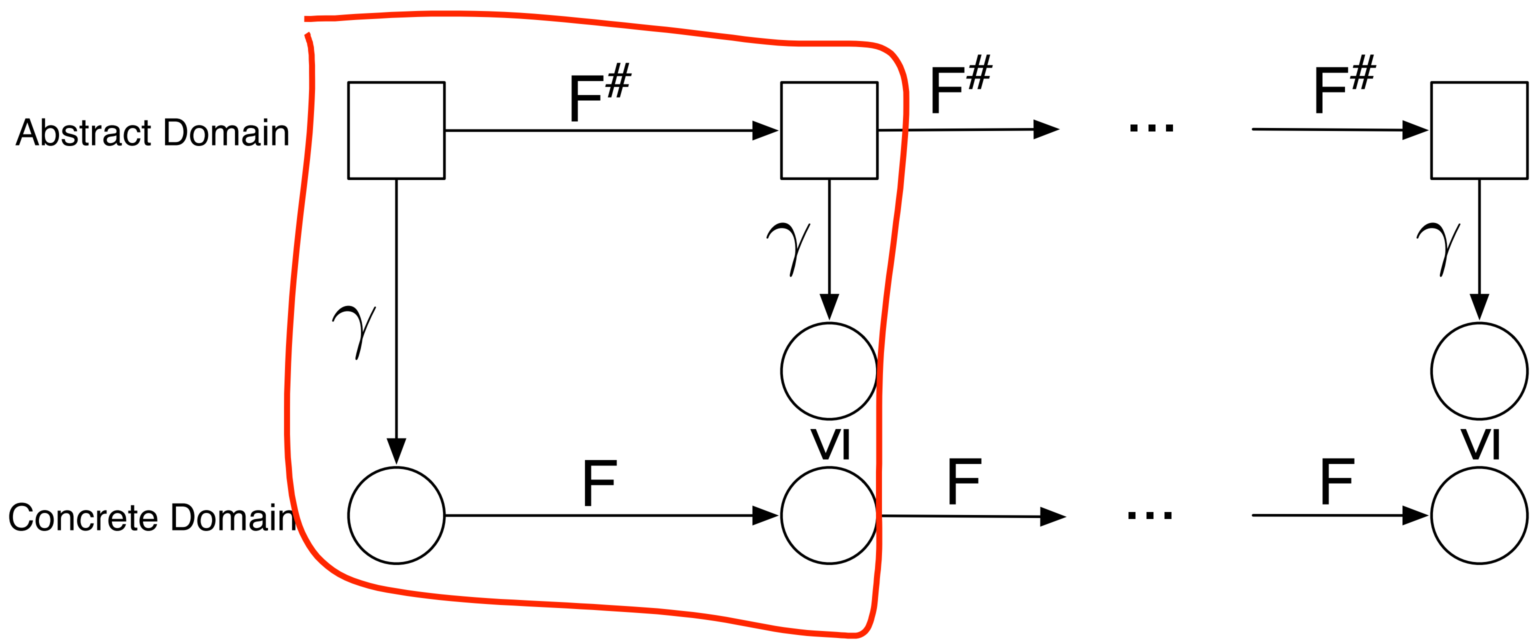
Verification of Real-Time Systems

Numerical Abstractions

Jan Reineke

Advanced Lecture, Summer 2015

Recap: From Local to Global Correctness: Kleene Iteration



Recap: Fixpoint Transfer Theorem

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

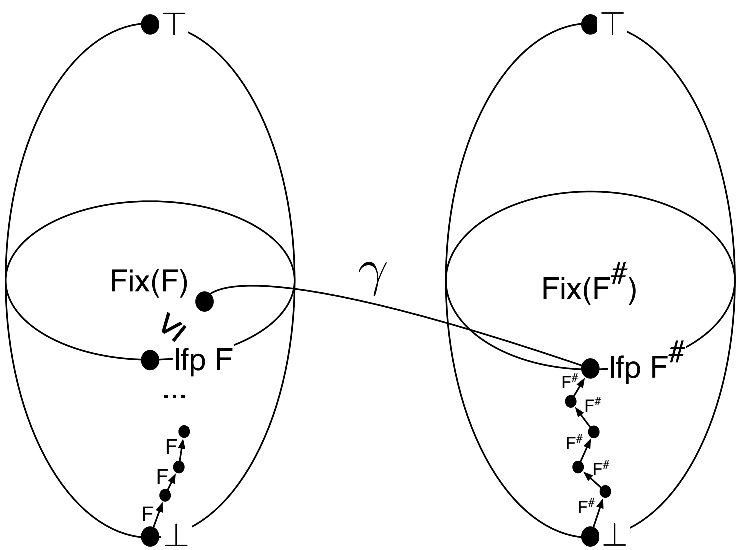
$$\forall l^{\#} \in L^{\#} : \gamma(F^{\#}(l^{\#})) \geq F(\gamma(l^{\#})).$$

Local Correctness

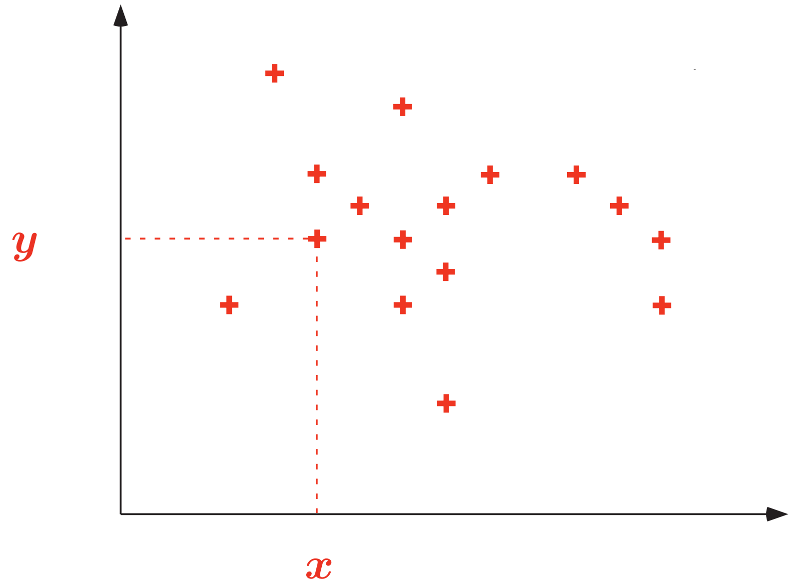
Then:

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

Global Correctness

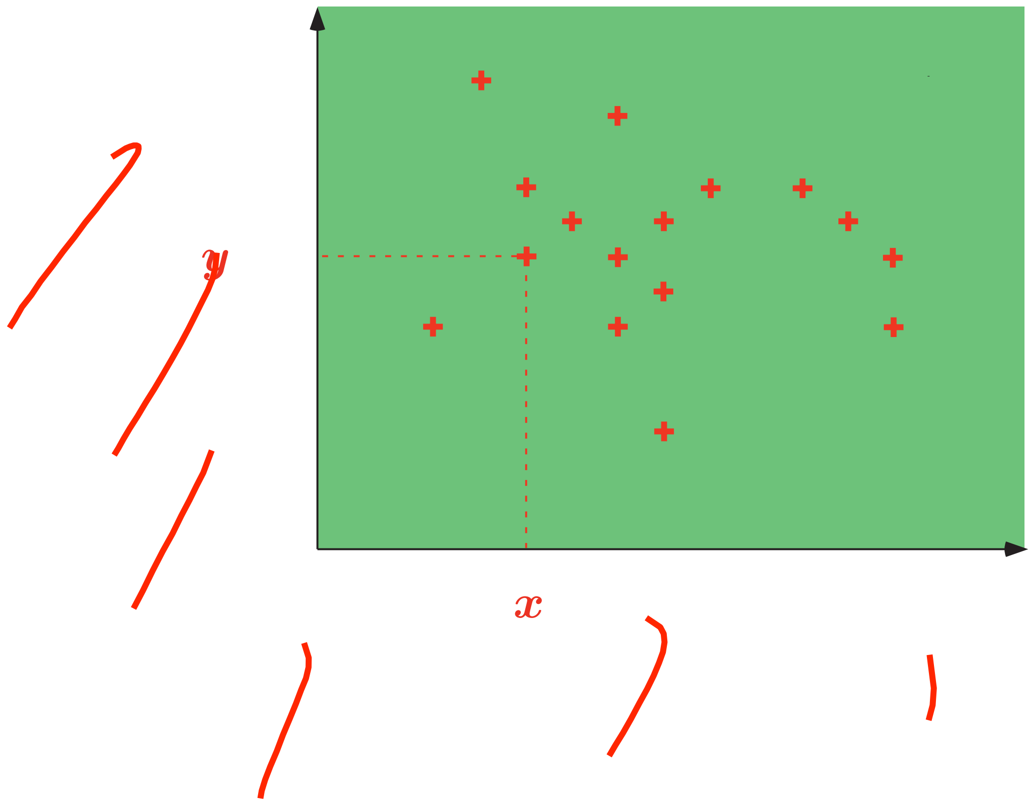


Overview: Numerical Abstractions



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

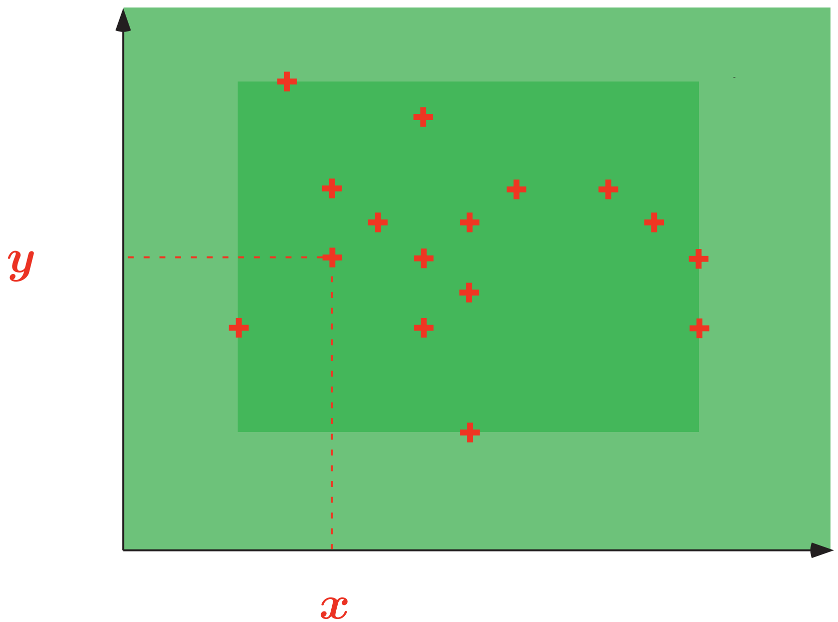
Overview: Numerical Abstractions
Signs (Cousot & Cousot, 1979)



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

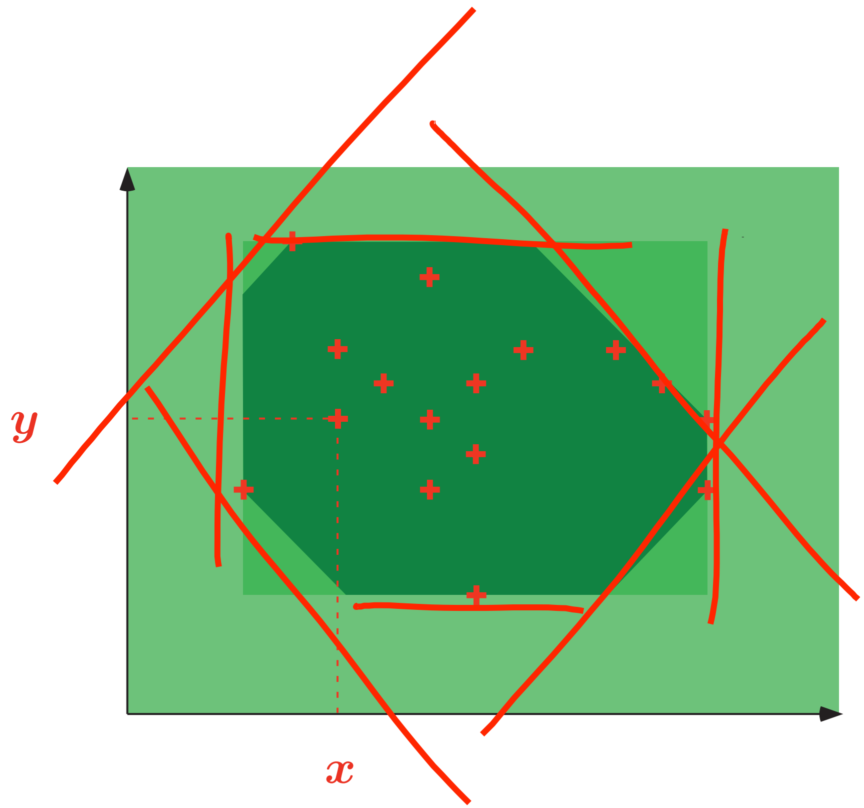
Overview: Numerical Abstractions
Intervals (Cousot & Cousot, 1976)

BOXES



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

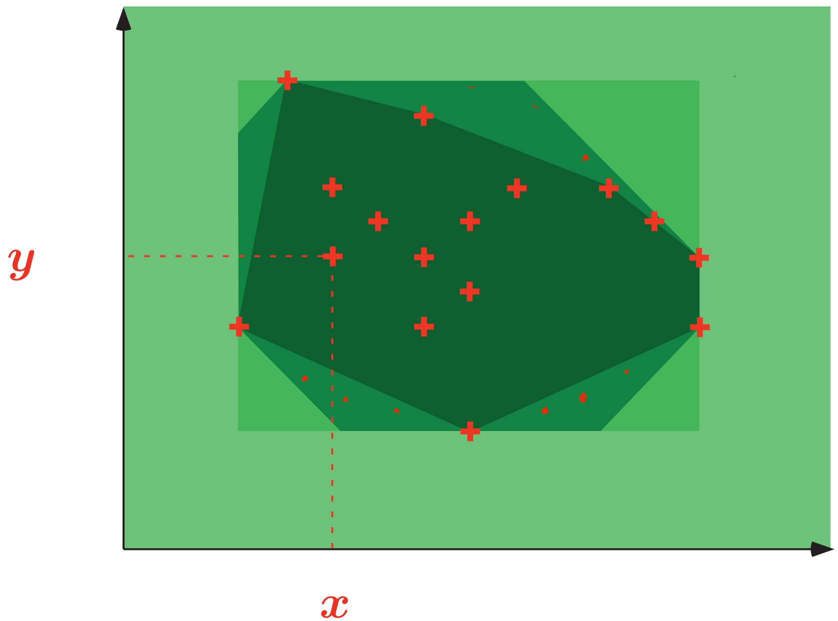
Overview: Numerical Abstractions
Octagons (Mine, 2001)



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

$x \geq y$

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



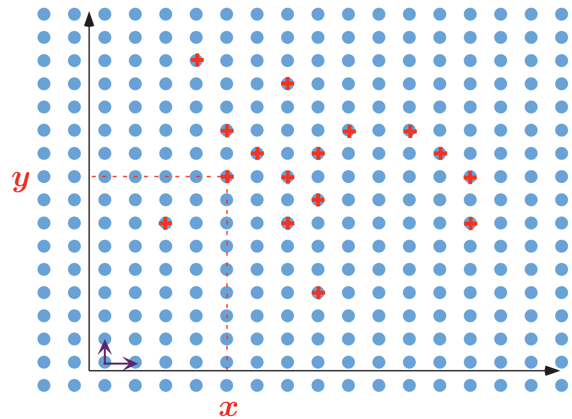
$$\begin{cases} 19x + 77y \leq 2004 \\ 20x + 03y \geq 0 \end{cases}$$

→ *Expensive…*

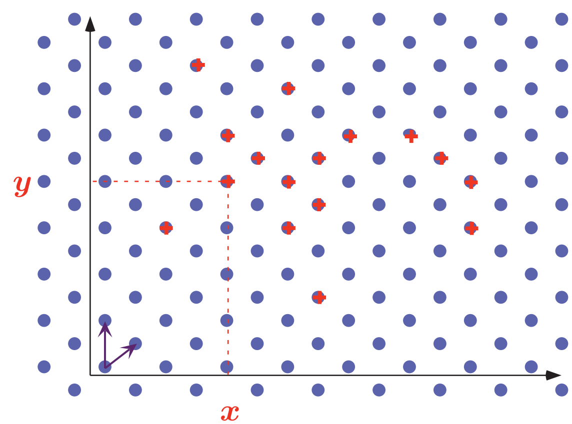
Overview: Numerical Abstractions Simple and Linear Congruences (Granger, 1989+1991)

odd ≡ 1 mod 2

even ≡ 0 mod 2



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

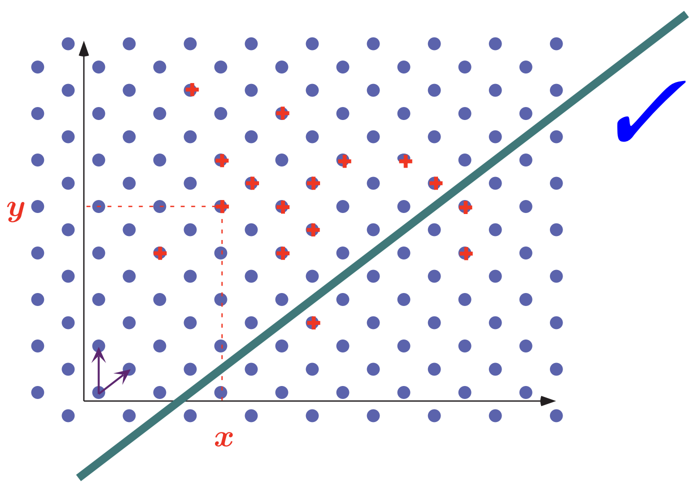


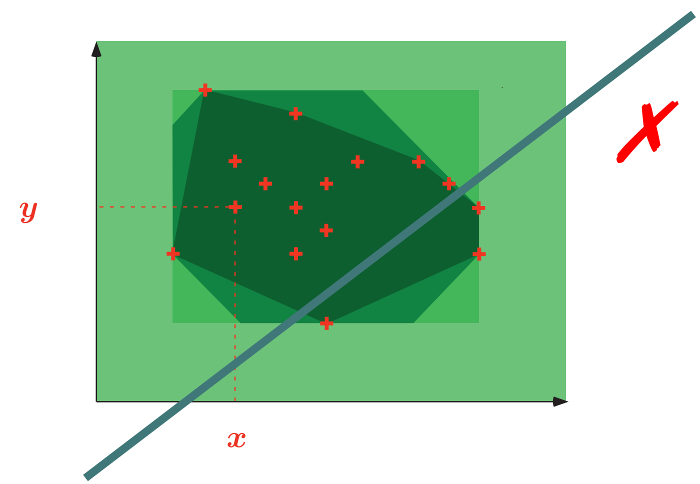
$$\begin{cases} 1x + 9y = 7 \bmod 8 \\ 2x - 1y = 9 \bmod 9 \end{cases}$$

Numerical Abstractions

Which abstraction is the most precise?

Depends on questions you want to answer!

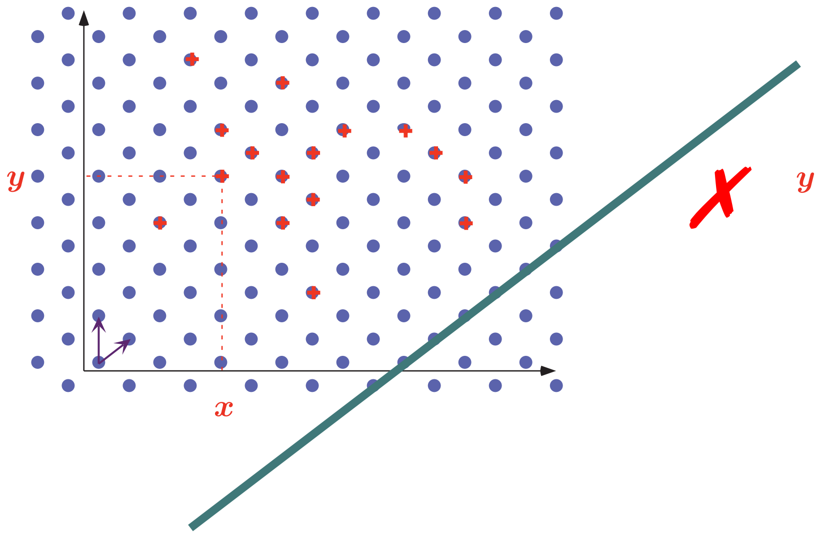


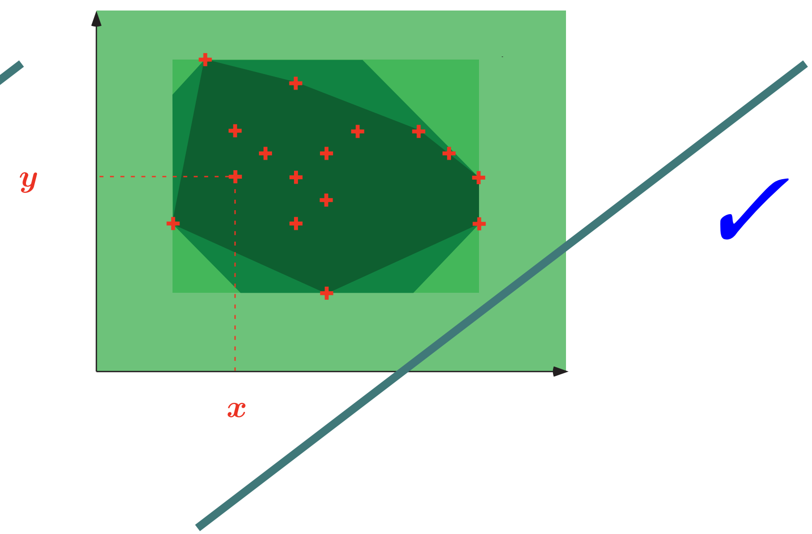


Numerical Abstractions

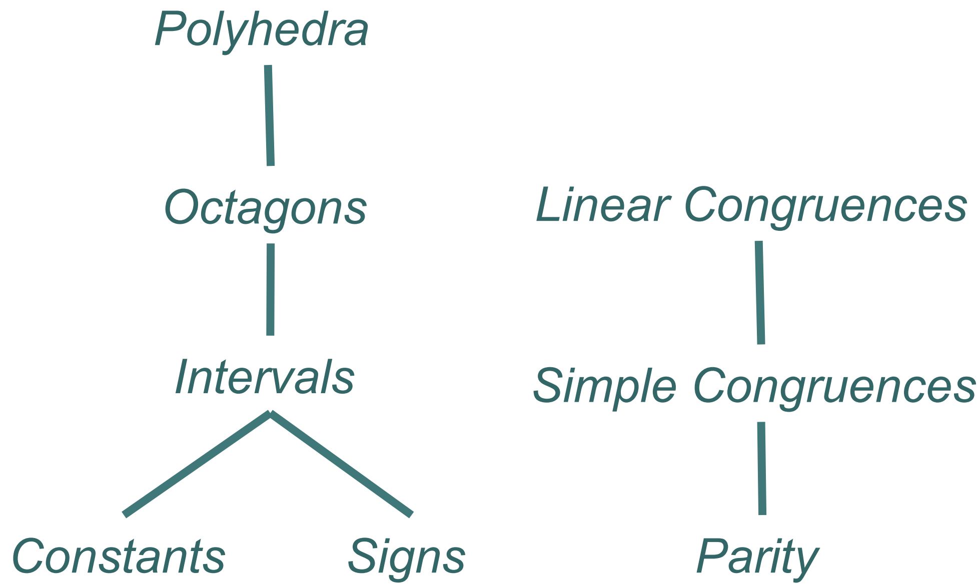
Which abstraction is the most precise?

Depends on questions you want to answer!

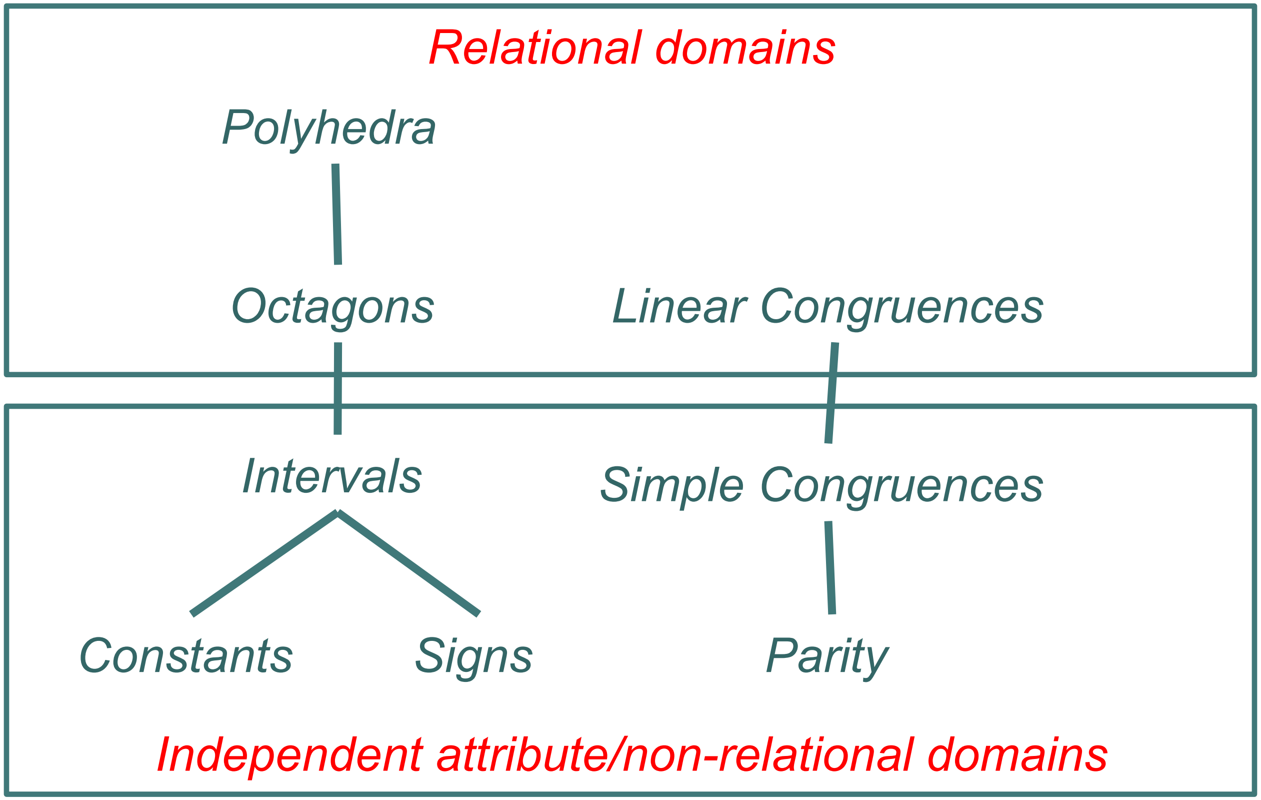




Partial Order of Abstractions



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

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

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

Intervals are ordered by inclusion:

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

$$[l,u] \sqsubseteq [l',u'] \; \mathit{if} \; l' \leq l \wedge u \leq u'$$

$(\textsc{Interval}, \sqsubseteq)$ 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

$x \cdot y = x \cdot \frac{1}{y}$

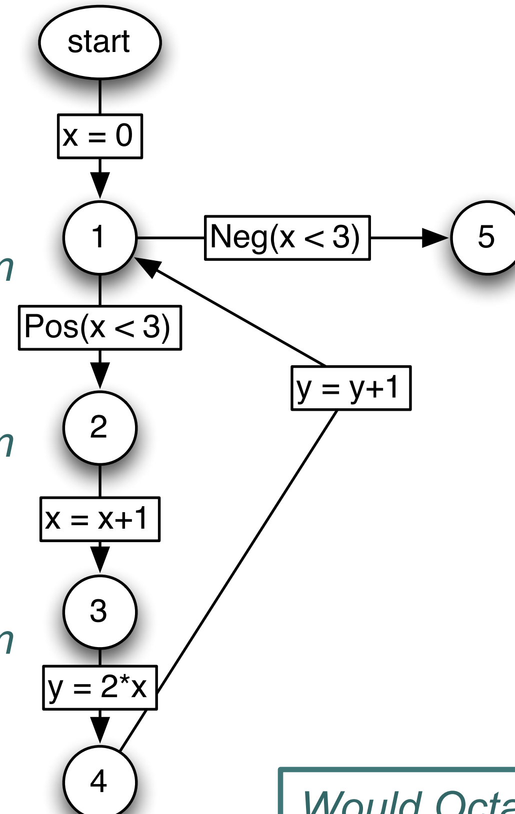
Calculating with Intervals:

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

$[a,b] * [1/d, 1]$ $\quad 0 \in [c,d],\ c < 0 < d$

$\cup\ [a,b] * [-1, 1/c]$

Example: Interval Analysis



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

4

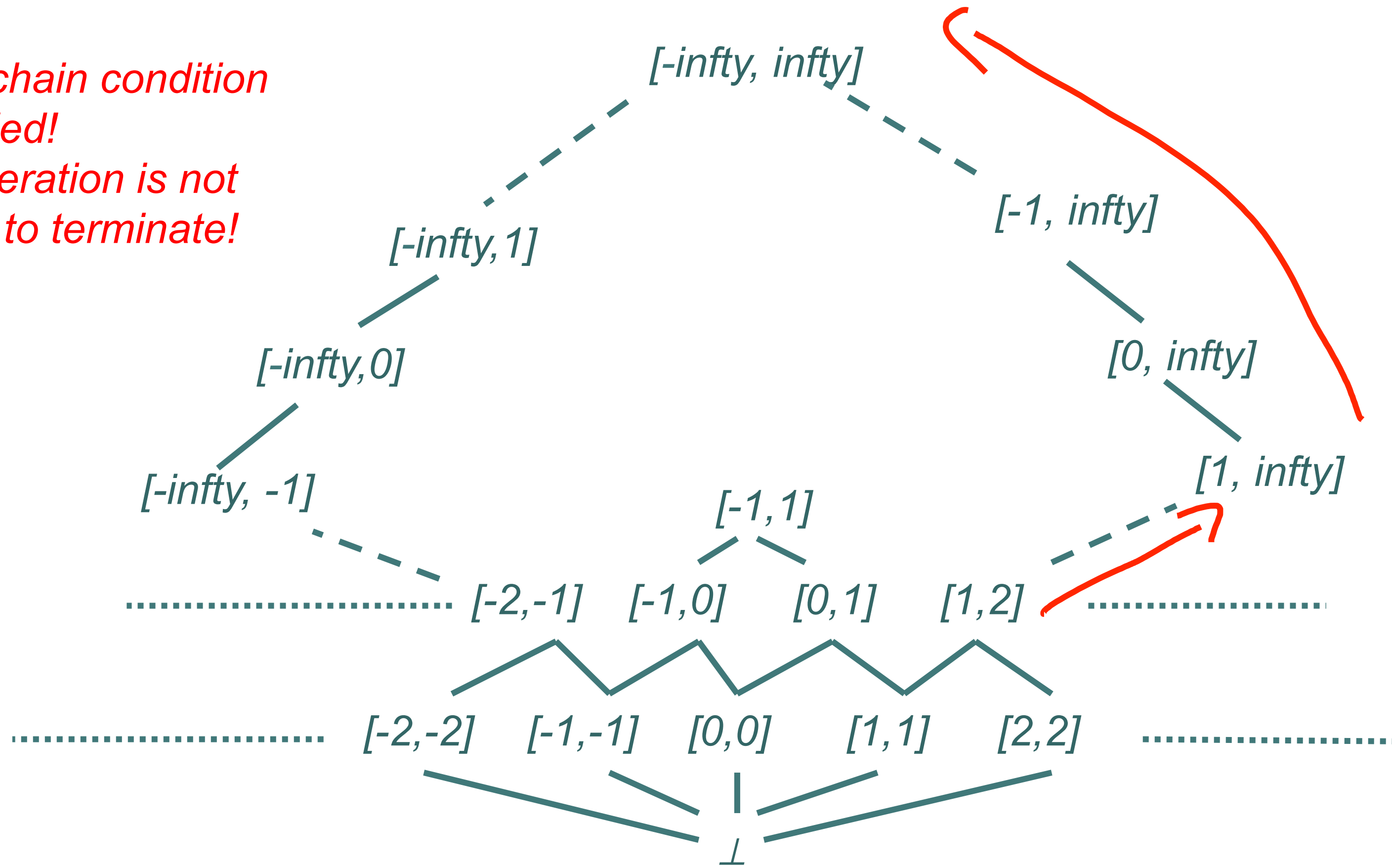
Imprecise due to non-relational analysis

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

$y = 2x + 1$

Intervals, Hasse diagram

Ascending chain condition is not satisfied!
→ Kleene iteration is not guaranteed to terminate!



Example: Interval Analysis

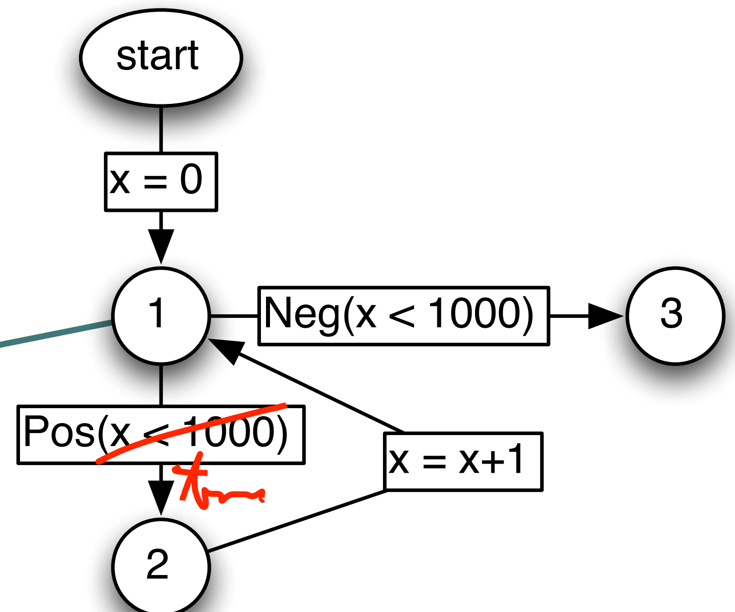
$$x \mapsto \bot$$

$$x \mapsto [0, 0]$$

$$x \mapsto [0, 1]$$

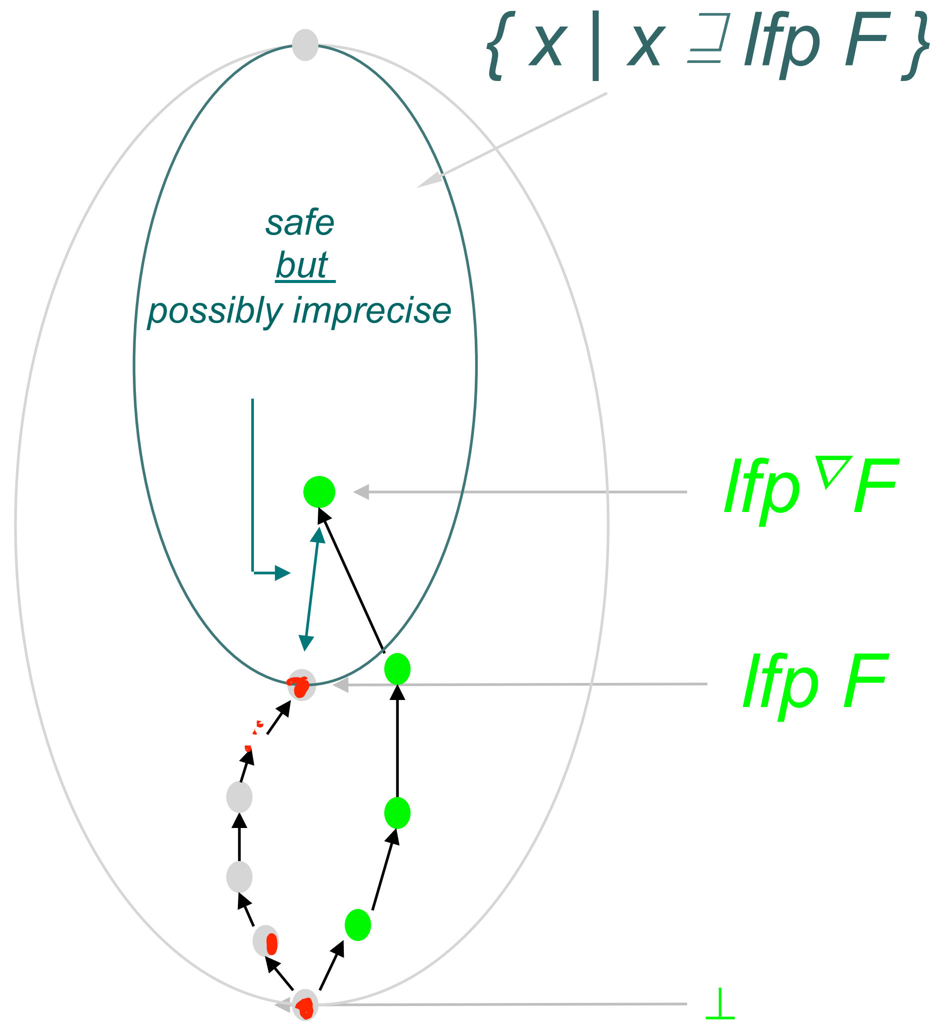
$$\ldots$$

1000 iterations later → $x \mapsto [0, 1000]$



Solution: Widening
"Enforce Ascending Chain Condition"

- Widening enforces the ascending chain condition during analysis.
- Accelerates termination by moving up the lattice more quickly.
- May yield imprecise results…



Widening: Formal Requirement

A widening ∇ is an operator $\nabla : D \times D \rightarrow D$ such that

1. Safety: $x \sqsubseteq (x \nabla y)$ and $y \sqsubseteq (x \nabla y)$ "upper bound"
2. Termination:

   forall ascending chains $x_0 \sqsubseteq x_1 \sqsubseteq \ldots$ the chain

$$y_0 = x_0$$
$$y_{i+1} = y_i \nabla x_{i+1}$$

   is finite.

Widening Operator for Intervals

Simplest solution:

$$\bot \nabla x = \; x \nabla \bot = x$$

$$[l,u]\nabla[l',u'] = \; \left[\begin{cases} l & : l' \geq l \\ -\infty & : l' < l \end{cases}, \begin{cases} u & : u' \leq u \\ \infty & : u' > u \end{cases} \right]$$

Example:

$$[3,5]\nabla[2,5] = [-\infty,5]$$

$$[3,5]\nabla[4,5] = [3,5]$$

$$[3,5]\nabla[4,6] = [3,\infty]$$

$$[3,5]\nabla[2,6] = [-\infty,\infty]$$

Example Revisited: Interval Analysis with Simple Widening

Standard Kleene Iteration:

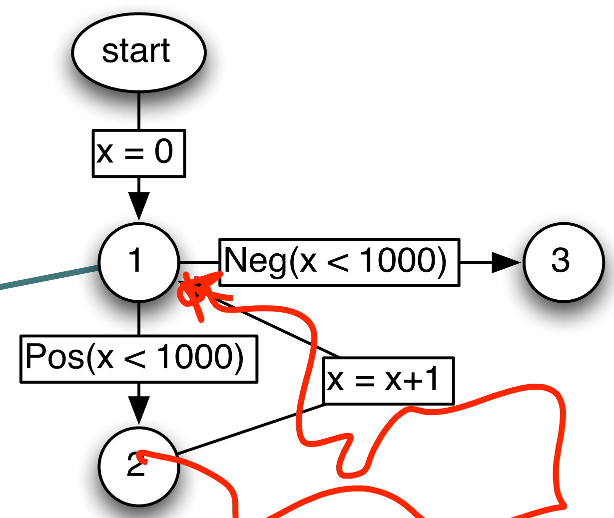
$$\bot \le F(\bot) \le F^2(\bot) \le F^3(\bot) \le \dots$$

Kleene Iteration with Widening: $F_\nabla(x) := x \nabla F(x)$

$$\bot \le F_\nabla(\bot) \le F_\nabla^2(\bot) \le F_\nabla^3(\bot) \le \dots$$

$x \mapsto [0,0]$

$x \mapsto [0,\infty]$



Do we need to apply widening at all program points?

→ *Quick termination but imprecise result!*

More Sophisticated Widening for Intervals

Define set of jump points (barriers) based on constants appearing in program, e.g.:

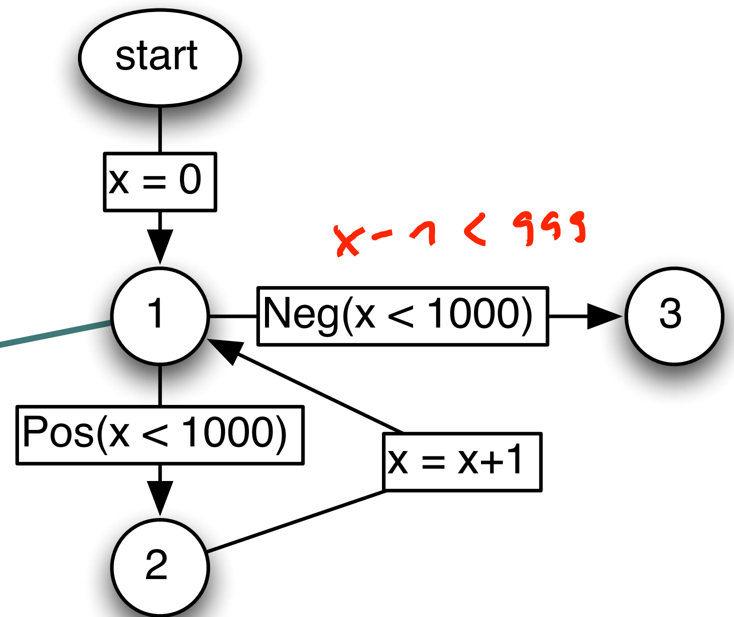
$$\mathcal{J} = \{-\infty, 0, 1, 1000, \infty\}$$

Intuition: "Don't jump to –infty, +infty immediately but only to next jump point."

$$[l, u] \nabla [l', u'] = \left[\begin{cases} l & : l' \geq l \\ \max\{x \in \mathcal{J} \mid x \leq l'\} & : l' < l \end{cases}, \begin{cases} u & : u' \leq u \\ \min\{x \in \mathcal{J} \mid x \geq u'\} & : u' > u \end{cases} \right]$$

Example Revisited:
Interval Analysis with Sophisticated Widening

$$x \mapsto [0, 0]$$
$$x \mapsto [0, 1]$$
$$x \mapsto [0, 1000]$$



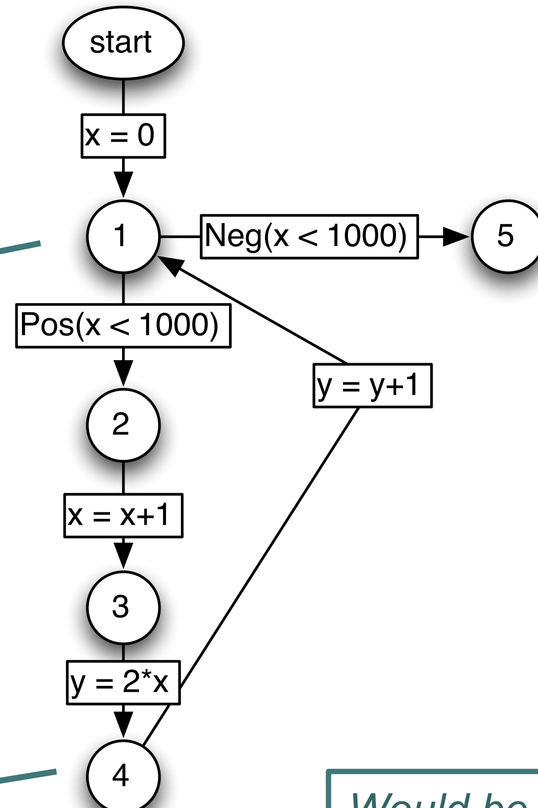
→ *More precise, potentially terminates more slowly.*

Another Example: Interval Analysis with Sophisticated Widening

$$x \mapsto [0, 0]$$

$$x \mapsto [0, 1]$$

$$x \mapsto [0, 1000]$$



$$y \mapsto [2, 2]$$

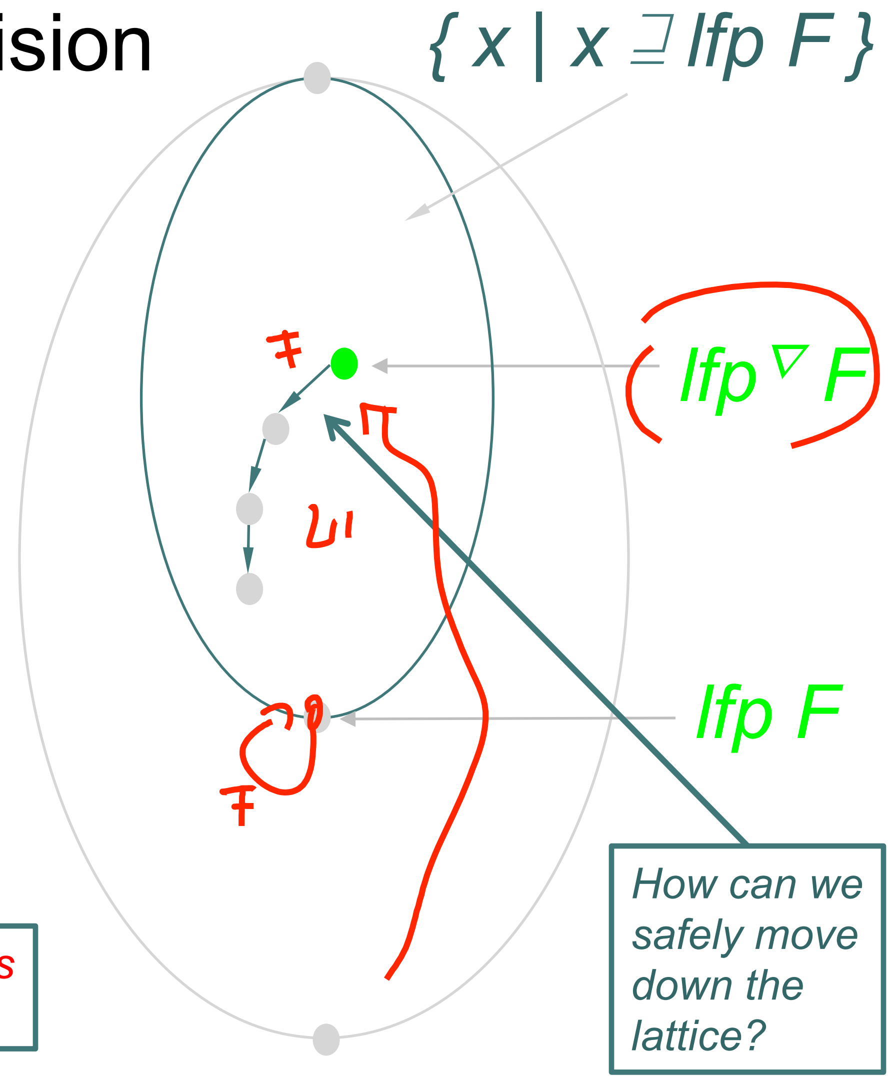
$$y \mapsto [2, 1000]$$

$$y \mapsto [2, \infty]$$

Would be [2, 2000] in least fixed point, but 2000 does not appear in the program…

Narrowing: Recovering Precision

- Widening may yield imprecise results by overshooting the least fixed point.
- Narrowing is used to approach the least fixed point from above.



Possible problem: infinite descending chains
Is it really a problem?

Narrowing: Recovering Precision

Widening terminates at a point $x \sqsupseteq \text{lfp } F$.

We can iterate:

$$x_0 = x$$
$$x_{i+1} = F(x_i) \sqcap x_i$$

Safety:

By monotonicity we know $F(x) \sqsupseteq F(\text{lfp } F) = \text{lfp } F$.
By induction we can easily show that $x_i \sqsupseteq \text{lfp } F$ for all i.

Termination:

Depends on existence of infinite descending chains.

Narrowing: Formal Requirement

A narrowing Δ is an operator $\Delta : D \times D \rightarrow D$ such that

1. Safety: $l \sqsubseteq x$ and $l \sqsubseteq y \;\rightarrow\; l \sqsubseteq (x \,\Delta\, y) \sqsubseteq x$
2. Termination:

   for all descending chains $x_0 \sqsupseteq x_1 \sqsupseteq \ldots$ the chain

   $$y_0 = x_0$$
   $$y_{i+1} = y_i \,\Delta\, x_{i+1}$$

   is finite.

Is $\sqcap$ ("meet") a narrowing operator on intervals?

Another Example Revisited: Interval Analysis with Widening and Narrowing

Result after Widening:

$x \mapsto [0,0]$

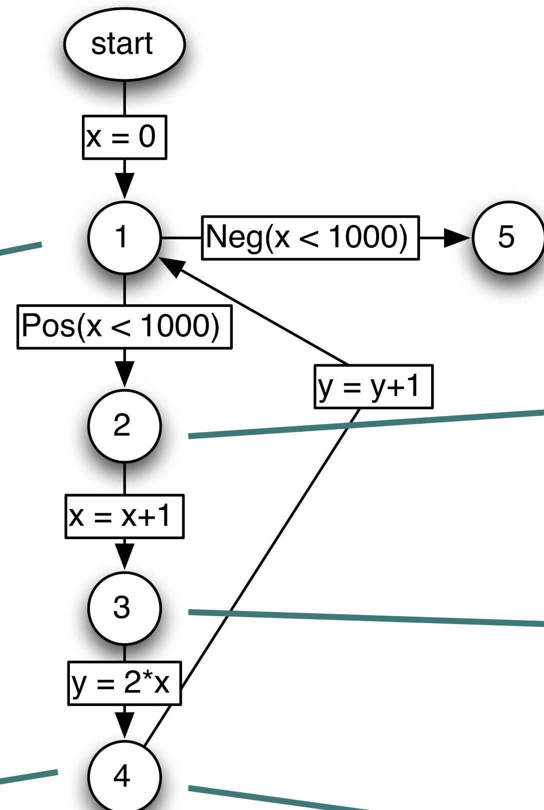
$x \mapsto [0,1]$

$x \mapsto [0,1000]$

$y \mapsto [2,2]$

$y \mapsto [2,1000]$

$y \mapsto [2,\infty]$



Result after Narrowing:

$x \mapsto [1000,1000]$

$y \mapsto [3,2001]$

$x \mapsto [0,999]$

$x \mapsto [1,1000]$

$y \mapsto [2,2000]$

→ *Precisely the least fixed point!*

Applications of Numerical Domains

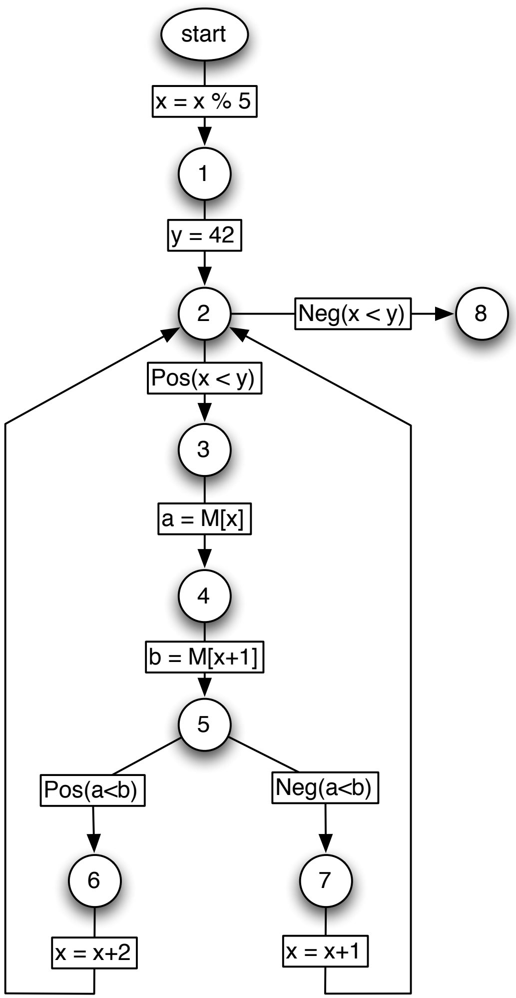
As input to other analyses:

- Cache Analysis
- Dependencies between memory accesses

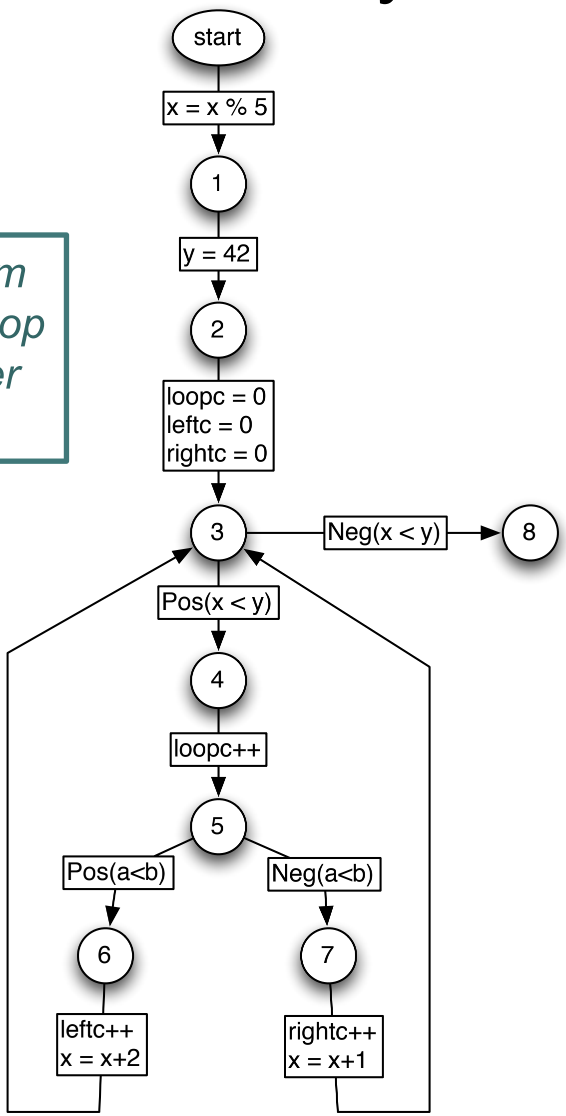
Loop Bound Analysis:

- Instrument program with loop iteration counters
- Determine maximal value of counter
- Requires relational analysis

Reduction:
Loop Bound Analysis to Value Analysis



Instrument program with counters of loop iterations and other interesting events



Summary

- Interval Analysis:

  A non-relational value analysis
- Widenings for termination in the presence of Infinite Ascending Chains
- Narrowings to recover precision
- Basic Approach to Loop Bound Analysis based on Value Analysis

Outlook

- Cache Abstractions
- Schedulability Analysis
- Cache-Related Preemption Delay
- Predictable Microarchitectures