CSCI 740 - Programming Language Theory

Lecture 30

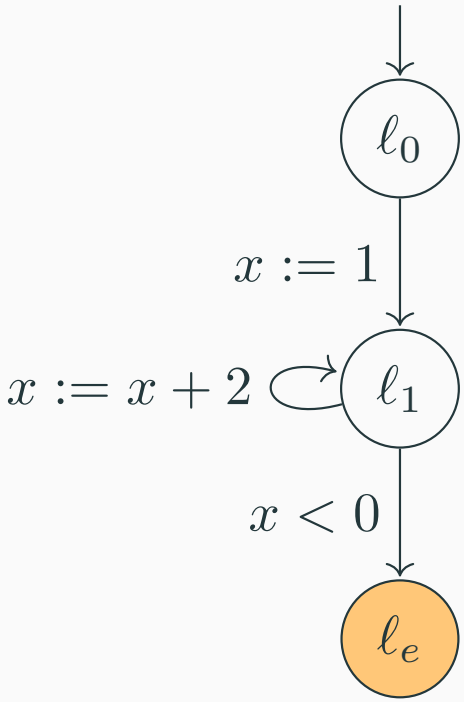
Widening and Narrowing

Instructor: Hossein Hojjat

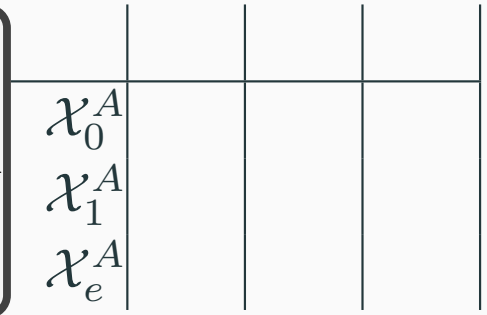
November 13, 2017

Example: Sign Abstraction

Use sign abstraction to prove error is unreachable Abs $= \{\top, +, 0, -, \bot\}$

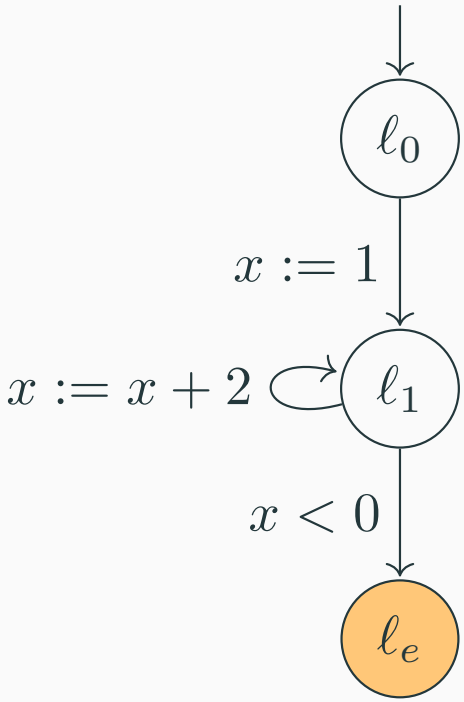


$$\mathcal{X}_0^A = \{x : \top\}$$
$$\mathcal{X}_1^A = [\![x := 1]\!]^A \mathcal{X}_0^A \sqcup [\![x := x + 2]\!]^A \mathcal{X}_1^A$$
$$\mathcal{X}_e^A = [\![x < 0]\!]^A \mathcal{X}_1^A$$



Example: Sign Abstraction

Use sign abstraction to prove error is unreachable Abs $= \{\top, +, 0, -, \bot\}$

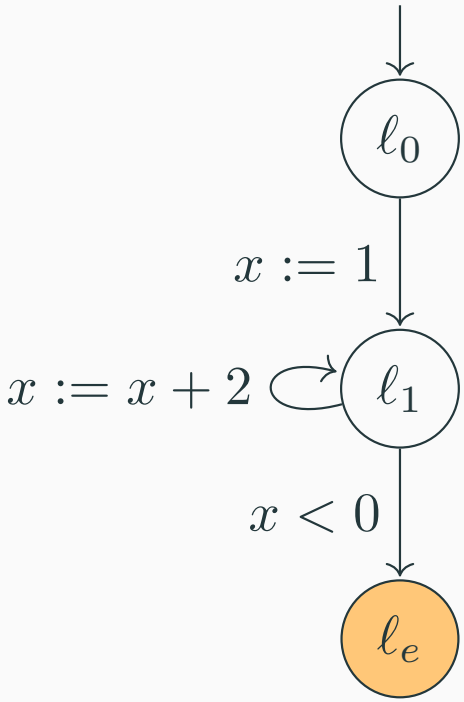


$$\mathcal{X}_0^A = \{x : \top\}$$
$$\mathcal{X}_1^A = [\![x := 1]\!]^A \mathcal{X}_0^A \sqcup [\![x := x + 2]\!]^A \mathcal{X}_1^A$$
$$\mathcal{X}_e^A = [\![x < 0]\!]^A \mathcal{X}_1^A$$

	init			
$\mathcal{X}_0^A$	$\top$			
$\mathcal{X}_1^A$	$\bot$			
$\mathcal{X}_e^A$	$\bot$			

Example: Sign Abstraction

Use sign abstraction to prove error is unreachable Abs $= \{\top, +, 0, -, \bot\}$



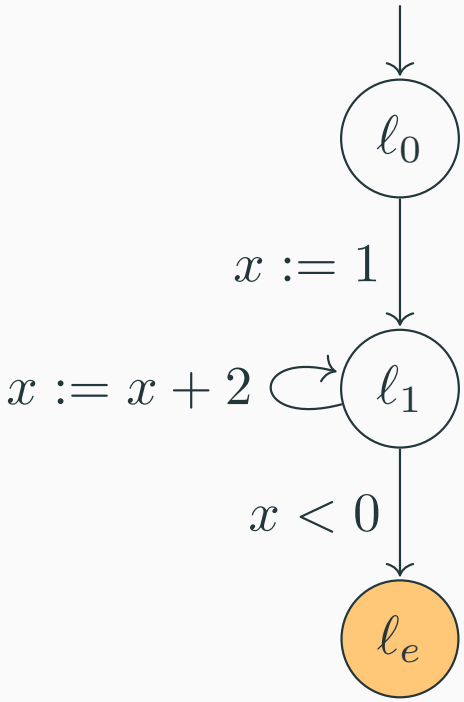
$$\mathcal{X}_0^A = \{x : \top\}$$
$$\mathcal{X}_1^A = [\![x := 1]\!]^A \mathcal{X}_0^A \sqcup [\![x := x + 2]\!]^A \mathcal{X}_1^A$$
$$\mathcal{X}_e^A = [\![x < 0]\!]^A \mathcal{X}_1^A$$

	init	ite1	
$\mathcal{X}_0^A$	$\top$	$\top$	
$\mathcal{X}_1^A$	$\bot$	$+$	
$\mathcal{X}_e^A$	$\bot$	$\bot$	

$$\begin{aligned}
\mathcal{X}_1^A &= [\![x := 1]\!]^A \mathcal{X}_0^A \sqcup [\![x := x + 2]\!]^A \mathcal{X}_1^A \\
&= [\![x := 1]\!]^A \{x : \top\} \sqcup [\![x := x + 2]\!]^A \{x : \bot\} \\
&= \{x : +\} \sqcup \{x : \bot\} \\
&= \{x : + \sqcup \bot\} \\
&= \{x : +\}
\end{aligned}$$

Example: Sign Abstraction

Use sign abstraction to prove error is unreachable Abs $= \{\top, +, 0, -, \bot\}$



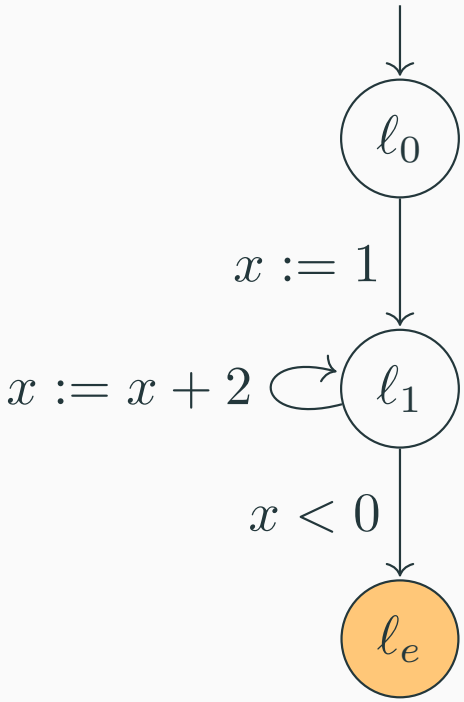
$$\mathcal{X}_0^A = \{x : \top\}$$
$$\mathcal{X}_1^A = [\![x := 1]\!]^A \mathcal{X}_0^A \sqcup [\![x := x + 2]\!]^A \mathcal{X}_1^A$$
$$\mathcal{X}_e^A = [\![x < 0]\!]^A \mathcal{X}_1^A$$

	init	ite1	ite2
$\mathcal{X}_0^A$	$\top$	$\top$	$\top$
$\mathcal{X}_1^A$	$\bot$	$+$	$+$
$\mathcal{X}_e^A$	$\bot$	$\bot$	$\bot$

$$\begin{aligned}
\mathcal{X}_1^A &= [\![x := 1]\!]^A \mathcal{X}_0^A \sqcup [\![x := x + 2]\!]^A \mathcal{X}_1^A \\
&= [\![x := 1]\!]^A \{x : \top\} \sqcup [\![x := x + 2]\!]^A \{x : +\} \\
&= \{x : +\} \sqcup \{x : +\} \\
&= \{x : + \sqcup +\} \\
&= \{x : +\}
\end{aligned}$$

Example: Sign Abstraction

Use sign abstraction to prove error is unreachable Abs $= \{\top, +, 0, -, \bot\}$



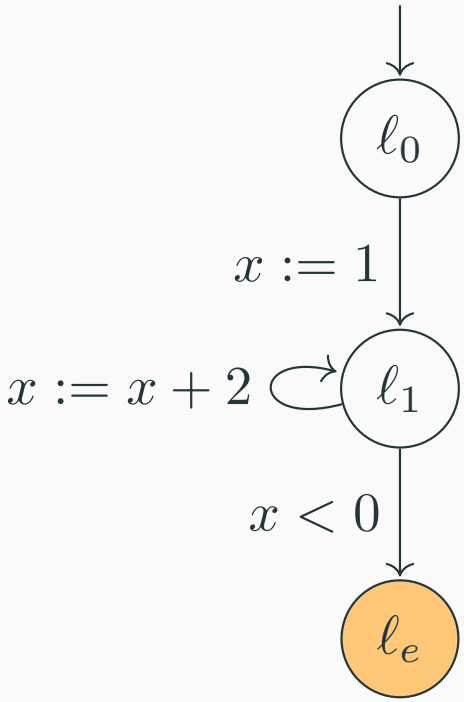
$$\mathcal{X}_0^A = \{x : \top\}$$
$$\mathcal{X}_1^A = [\![x := 1]\!]^A \mathcal{X}_0^A \sqcup [\![x := x + 2]\!]^A \mathcal{X}_1^A$$
$$\mathcal{X}_e^A = [\![x < 0]\!]^A \mathcal{X}_1^A$$

	init	ite1	ite2
$\mathcal{X}_0^A$	$\top$	$\top$	$\top$
$\mathcal{X}_1^A$	$\bot$	$+$	$+$
$\mathcal{X}_e^A$	$\bot$	$\bot$	$\bot$

fixpoint - error unreachable

Exercise: Interval Abstraction

Use interval abstraction to prove error is unreachable

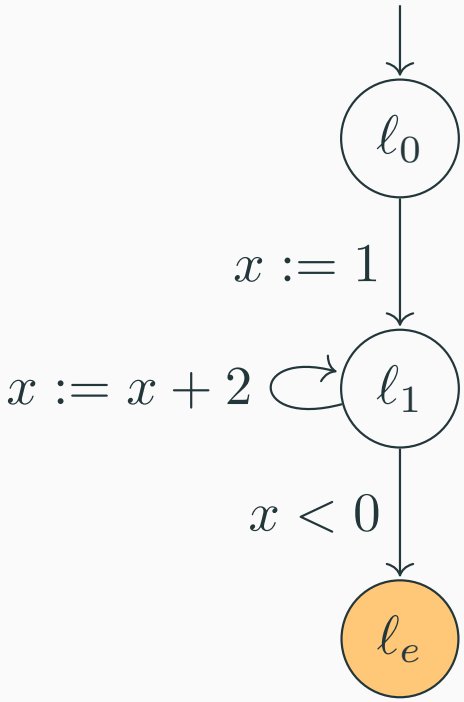


$$\mathcal{X}_0^A = \{x : \top\}$$
$$\mathcal{X}_1^A = [\![x := 1]\!]^A \mathcal{X}_0^A \sqcup [\![x := x + 2]\!]^A \mathcal{X}_1^A$$
$$\mathcal{X}_e^A = [\![x < 0]\!]^A \mathcal{X}_1^A$$

$\mathcal{X}_0^A$			
$\mathcal{X}_1^A$			
$\mathcal{X}_e^A$			

Exercise: Interval Abstraction

Use interval abstraction to prove error is unreachable

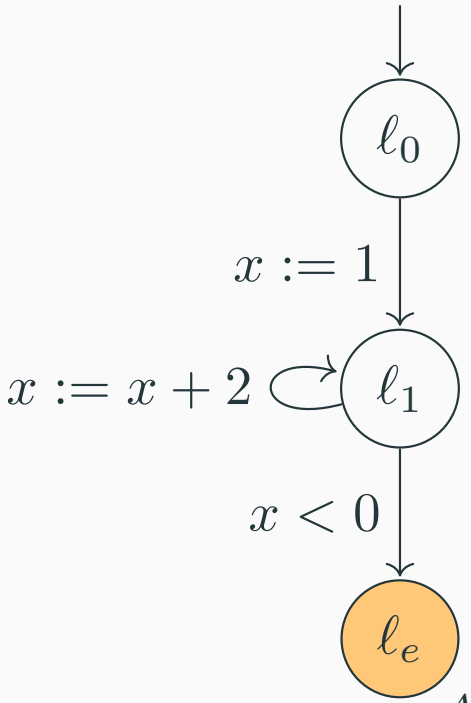


$$\mathcal{X}_0^A = \{x : \top\}$$
$$\mathcal{X}_1^A = [\![x := 1]\!]^A \mathcal{X}_0^A \sqcup [\![x := x + 2]\!]^A \mathcal{X}_1^A$$
$$\mathcal{X}_e^A = [\![x < 0]\!]^A \mathcal{X}_1^A$$

	init		
$\mathcal{X}_0^A$	$\top$		
$\mathcal{X}_1^A$	$\bot$		
$\mathcal{X}_e^A$	$\bot$		

Exercise: Interval Abstraction

Use interval abstraction to prove error is unreachable



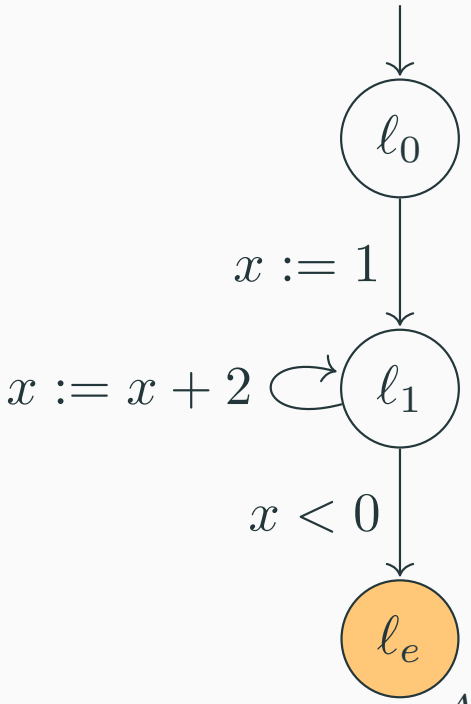
$$\mathcal{X}_0^A = \{x : \top\}$$
$$\mathcal{X}_1^A = [\![x := 1]\!]^A \mathcal{X}_0^A \sqcup [\![x := x + 2]\!]^A \mathcal{X}_1^A$$
$$\mathcal{X}_e^A = [\![x < 0]\!]^A \mathcal{X}_1^A$$

	init	ite1	
$\mathcal{X}_0^A$	$\top$	$\top$	
$\mathcal{X}_1^A$	$\bot$	$[1,1]$	
$\mathcal{X}_e^A$	$\bot$	$\bot$	

$$\begin{aligned}
\mathcal{X}_1^A &= [\![x := 1]\!]^A \mathcal{X}_0^A \sqcup [\![x := x + 2]\!]^A \mathcal{X}_1^A \\
&= [\![x := 1]\!]^A \{x : \top\} \sqcup [\![x := x + 2]\!]^A \{x : \ \bot \ \} \\
&= \{x : [1,1]\} \sqcup \{x : \bot\} \\
&= \{x : [1,1] \sqcup \bot\} \\
&= \{x : [1,1]\}
\end{aligned}$$

Exercise: Interval Abstraction

Use interval abstraction to prove error is unreachable



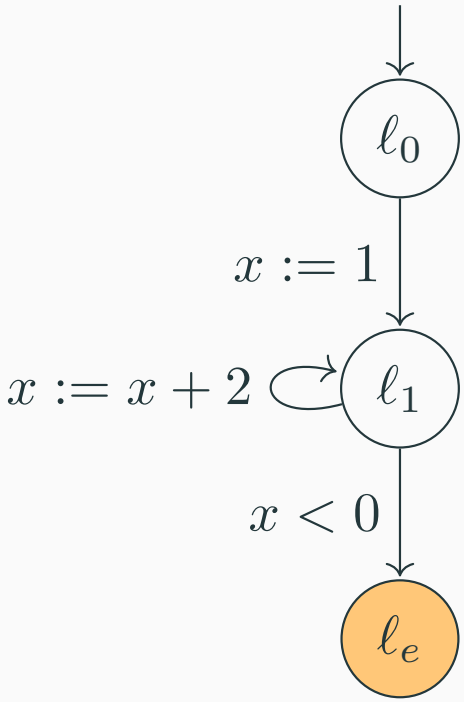
$$\mathcal{X}_0^A = \{x : \top\}$$
$$\mathcal{X}_1^A = [\![x := 1]\!]^A \mathcal{X}_0^A \sqcup [\![x := x + 2]\!]^A \mathcal{X}_1^A$$
$$\mathcal{X}_e^A = [\![x < 0]\!]^A \mathcal{X}_1^A$$

	init	ite1	ite2
$\mathcal{X}_0^A$	$\top$	$\top$	$\top$
$\mathcal{X}_1^A$	$\bot$	$[1,1]$	$[1,3]$
$\mathcal{X}_e^A$	$\bot$	$\bot$	$\bot$

$$\begin{aligned}
\mathcal{X}_1^A &= [\![x := 1]\!]^A \mathcal{X}_0^A \sqcup [\![x := x + 2]\!]^A \mathcal{X}_1^A \\
&= [\![x := 1]\!]^A \{x : \top\} \sqcup [\![x := x + 2]\!]^A \{x : [1,1]\} \\
&= \{x : [1,1]\} \sqcup \{x : [3,3]\} \\
&= \{x : [1,1] \sqcup [3,3]\} \\
&= \{x : [1,3]\}
\end{aligned}$$

Exercise: Interval Abstraction

Use interval abstraction to prove error is unreachable



$$\mathcal{X}_0^A = \{x : \top\}$$
$$\mathcal{X}_1^A = [\![x := 1]\!]^A \mathcal{X}_0^A \sqcup [\![x := x + 2]\!]^A \mathcal{X}_1^A$$
$$\mathcal{X}_e^A = [\![x < 0]\!]^A \mathcal{X}_1^A$$

	init	ite1	ite2
$\mathcal{X}_0^A$	$\top$	$\top$	$\top$
$\mathcal{X}_1^A$	$\bot$	$[1,1]$	$[1,3]$
$\mathcal{X}_e^A$	$\bot$	$\bot$	$\bot$

... will go on forever

$\mathcal{X}_1^A : \bot, [1,1], [1,3], [1,5], \cdots$

Widening & Narrowing

- Some interesting abstract domains have infinite lattices
  - Interval domain
- These domains have infinite ascending chains:
  - $[0, 0], [0, 1], [0, 2], \cdots$
- Abstraction interpretation usually provides only simpler computation but not convergence
- In some cases we may need to accelerate the fixpoint computation using widening
- If we do too much widening then we may need narrowing

Widening

- Intuition:
  widening operator $\triangledown : \mathcal{D} \to \mathcal{D}$ jumps ahead on a lattice $\langle \mathcal{D}, \leq \rangle$
- $\triangledown$ is like join $\sqcup$ but can be a bigger element of the lattice

$$x \leq x \triangledown y \qquad\qquad y \leq x \triangledown y$$

- For all increasing chains $x_0 \leq x_1 \leq \cdots$, the increasing chain (y_i) defined as

$$y_i = \begin{cases} x_0 & \text{if } i = 0; \\ y_{i-1} \triangledown x_i & \text{if } i > 0. \end{cases}$$

  eventually stabilizes (i.e., the chain is finite)
- In other words, iterated uses of widening operator becomes a fixpoint eventually

$$x_0 \triangledown x_1 \triangledown x_2 \triangledown x_3 \cdots$$

Widening for Intervals

- Jump ahead to infinity whenever interval bounds are not inclusive

$$[a,b]\triangledown\bot = [a,b]$$
$$\bot\triangledown[c,d] = [c,d]$$
$$[a,b]\triangledown[c,d] = \left[\begin{cases} a & \text{if } a \leq c \\ -\infty & \text{otherwise} \end{cases}, \begin{cases} b & \text{if } d \leq b \\ +\infty & \text{otherwise} \end{cases}\right]$$

Non-monotonicity

- Non monotonicity of widening
- $[0,1]\triangledown[0,2] =$
- $[0,2]\triangledown[0,2] =$

Widening for Intervals

- Jump ahead to infinity whenever interval bounds are not inclusive

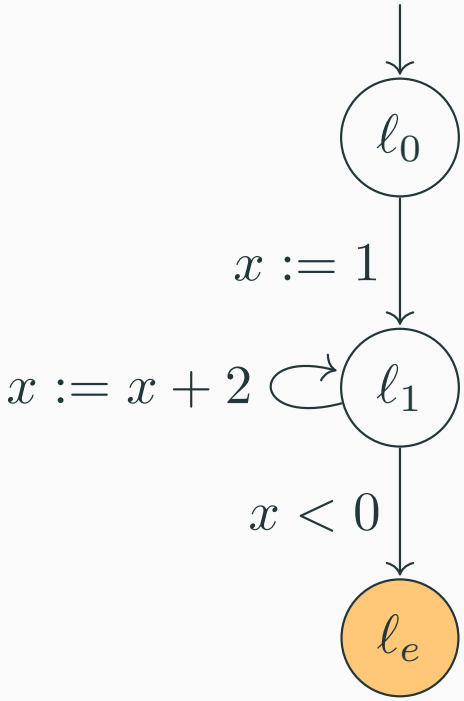
$$[a,b]\triangledown\bot = [a,b]$$
$$\bot\triangledown[c,d] = [c,d]$$
$$[a,b]\triangledown[c,d] = \left[\begin{cases} a & \text{if } a \leq c \\ -\infty & \text{otherwise} \end{cases}, \begin{cases} b & \text{if } d \leq b \\ +\infty & \text{otherwise} \end{cases}\right]$$

Non-monotonicity

- Non monotonicity of widening
- $[0,1]\triangledown[0,2] = [0,+\infty)$
- $[0,2]\triangledown[0,2] = [0,2]$

Interval Abstraction

Use interval abstraction (with widening) to prove error is unreachable



$$\mathcal{X}_0^A = \{x : \top\}$$
$$\mathcal{X}_1^A = [\![x := 1]\!]^A \mathcal{X}_0^A \sqcup [\![x := x + 2]\!]^A \mathcal{X}_1^A$$
$$\mathcal{X}_e^A = [\![x < 0]\!]^A \mathcal{X}_1^A$$

	init	ite1	ite2
$\mathcal{X}_0^A$	$\top$	$\top$	$\top$
$\mathcal{X}_1^A$	$\bot$	$[1,1]$	$[1,3]$
$\mathcal{X}_e^A$	$\bot$	$\bot$	$\bot$

$$\mathcal{X}_0^A = \top$$
$$\mathcal{X}_1^A = [1,1] \triangledown [1,3] = [1,+\infty)$$
$$\mathcal{X}_e^A = \bot$$

Iterations stabilize to a fix-point

Narrowing

- When widening is too aggressive we use a dual operator called narrowing
- $\triangle$ is like meet $\sqcap$ but can be a bigger element of the lattice

$$x \sqcap y \leq x \triangle y$$

- For all increasing chains $x_0 \leq x_1 \leq \cdots$, the increasing chain (y_i) defined as

$$y_i = \begin{cases} x_0 & \text{if } i = 0; \\ y_{i-1} \triangle x_i & \text{if } i > 0. \end{cases}$$

  eventually stabilizes (i.e., the chain is finite)

Narrowing for Intervals

$$[a,b] \triangle \bot = \bot$$

$$\bot \triangle [c,d] = \bot$$

$$[a,b] \triangle [c,d] = \left[\begin{Bmatrix} c & \text{if } a = -\infty \\ a & \text{otherwise} \end{Bmatrix}, \begin{Bmatrix} d & \text{if } b = +\infty \\ b & \text{otherwise} \end{Bmatrix} \right]$$