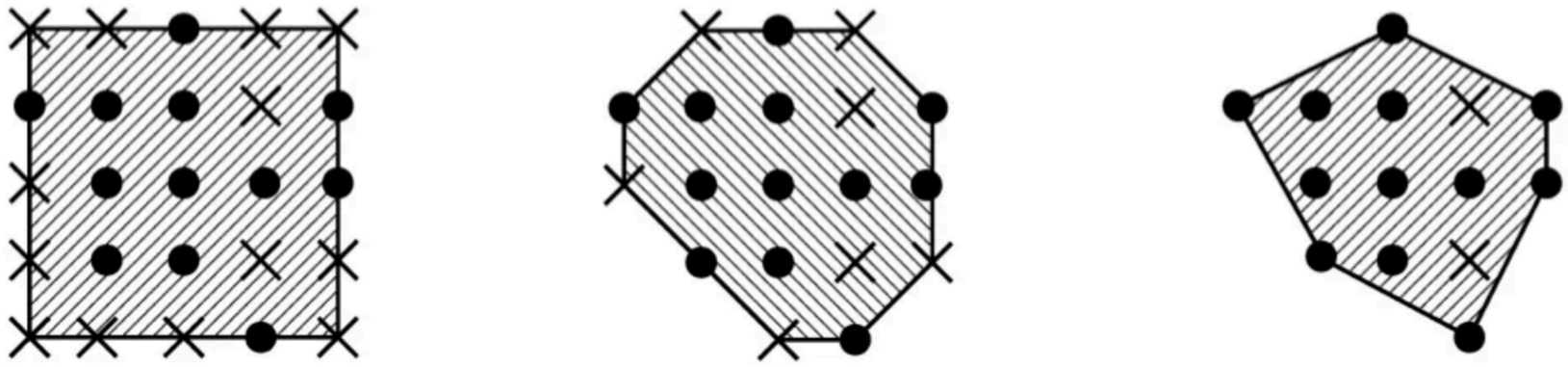
COSE419: Software Verification

Lecture 13 – Relational Analysis

Hakjoo Oh
2024 Spring

Relational Abstract Domains

- Intervals vs. Octagons vs. Polyhedra



- Focus: Core idea of the Octagon domain*

```
int a[10];
x = 0; y = 0;

while (x < 9) {
    x++; y++;
}

a[y] = 0;
```

Octagon analysis

$x : [9,9]$
$y : [9,9]$
$x - y : [0,0]$
$x + y : [18,18]$

Interval analysis

$x : [9,9]$
$y : [0,\infty]$

*Antoine Miné. The Octagon Abstract Domain. https://arxiv.org/abs/cs/0703084

Difference Bound Matrix (DBM)

- $(N+1) \times (N+1)$ matrix (N: the number of variables): e.g.,

$$\begin{array}{c} \\ 0 \\ x \\ y \end{array} \begin{array}{c} \begin{array}{ccc} 0 & x & y \end{array} \\ \begin{bmatrix} 0-0 & x-0 & y-0 \\ 0-x & x-x & y-x \\ 0-y & x-y & y-y \end{bmatrix} \end{array}$$

- Example

$$\begin{bmatrix} 0 & 10 & 10 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \iff \begin{array}{c} 0 \le x \le 10 \\ 0 \le y \le 10 \\ y - x \le 0 \\ x - y \le 0 \end{array} \qquad \begin{bmatrix} 0 & 10 & +\infty \\ -1 & 0 & -1 \\ 0 & 1 & 0 \end{bmatrix} \iff \begin{array}{c} 1 \le x \le 10 \\ 0 \le y \\ y - x \le -1 \\ x - y \le 1 \end{array}$$

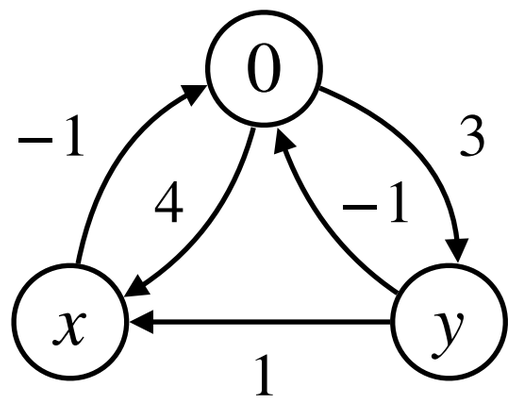
Difference Bound Matrix (DBM)

- A DBM represents a set of program states (N-dim points)

$$\gamma\left(\begin{bmatrix} 0 & 10 & +\infty \\ -1 & 0 & -1 \\ 0 & 1 & 0 \end{bmatrix}\right) = \{(x,y) \mid 1 \le x \le 10, 0 \le y, y - x \le -1, x - y \le 1\}$$

- A DBM can also be represented by a directed graph

$$\begin{array}{c} \\ 0 \\ x \\ y \end{array} \begin{array}{c} \begin{array}{ccc} 0 & x & y \end{array} \\ \begin{bmatrix} +\infty & 4 & 3 \\ -1 & +\infty & +\infty \\ -1 & 1 & +\infty \end{bmatrix} \end{array} \iff$$



Difference Bound Matrix (DBM)

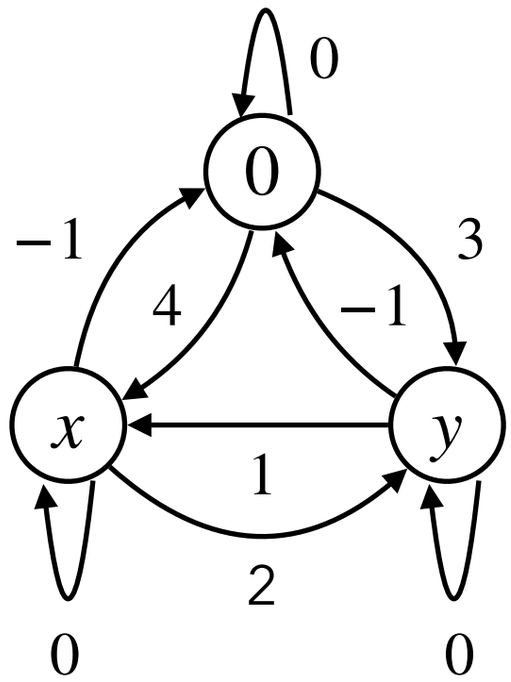
- Two different DBMs can represent the same set of points

$$\gamma\left(\begin{bmatrix} +\infty & 4 & 3 \\ -1 & +\infty & +\infty \\ -1 & 1 & +\infty \end{bmatrix}\right) = \gamma\left(\begin{bmatrix} 0 & 5 & 3 \\ -1 & +\infty & +\infty \\ -1 & 1 & +\infty \end{bmatrix}\right)$$

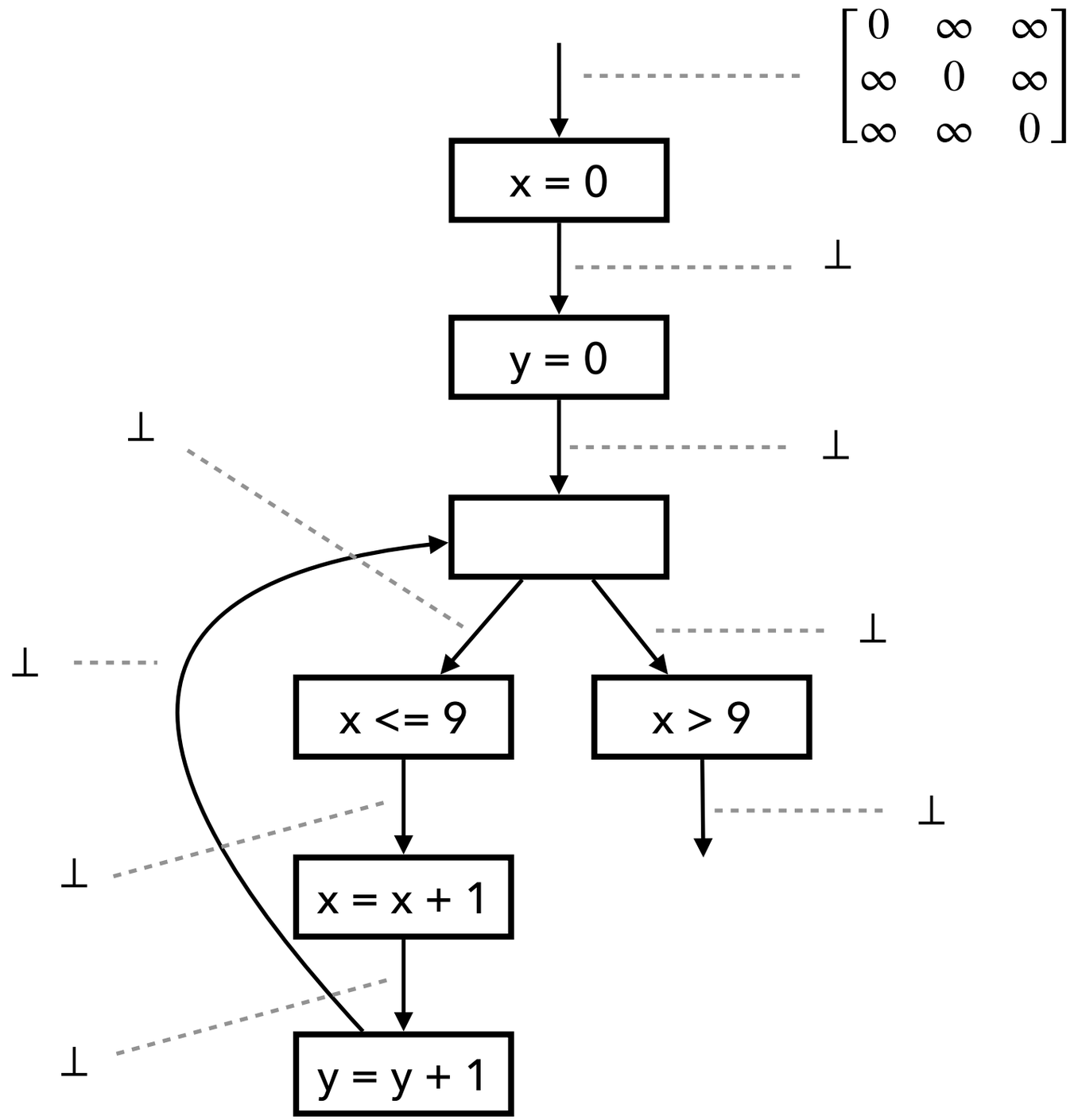
- Closure (normalization) via the Floyd-Warshall algorithm

$$\begin{bmatrix} +\infty & 4 & 3 \\ -1 & +\infty & +\infty \\ -1 & 1 & +\infty \end{bmatrix}^* = \begin{bmatrix} 0 & 4 & 3 \\ -1 & 0 & 2 \\ -1 & 1 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 0 & 5 & 3 \\ -1 & +\infty & +\infty \\ -1 & 1 & +\infty \end{bmatrix}^* = \begin{bmatrix} 0 & 4 & 3 \\ -1 & 0 & 2 \\ -1 & 1 & 0 \end{bmatrix}$$



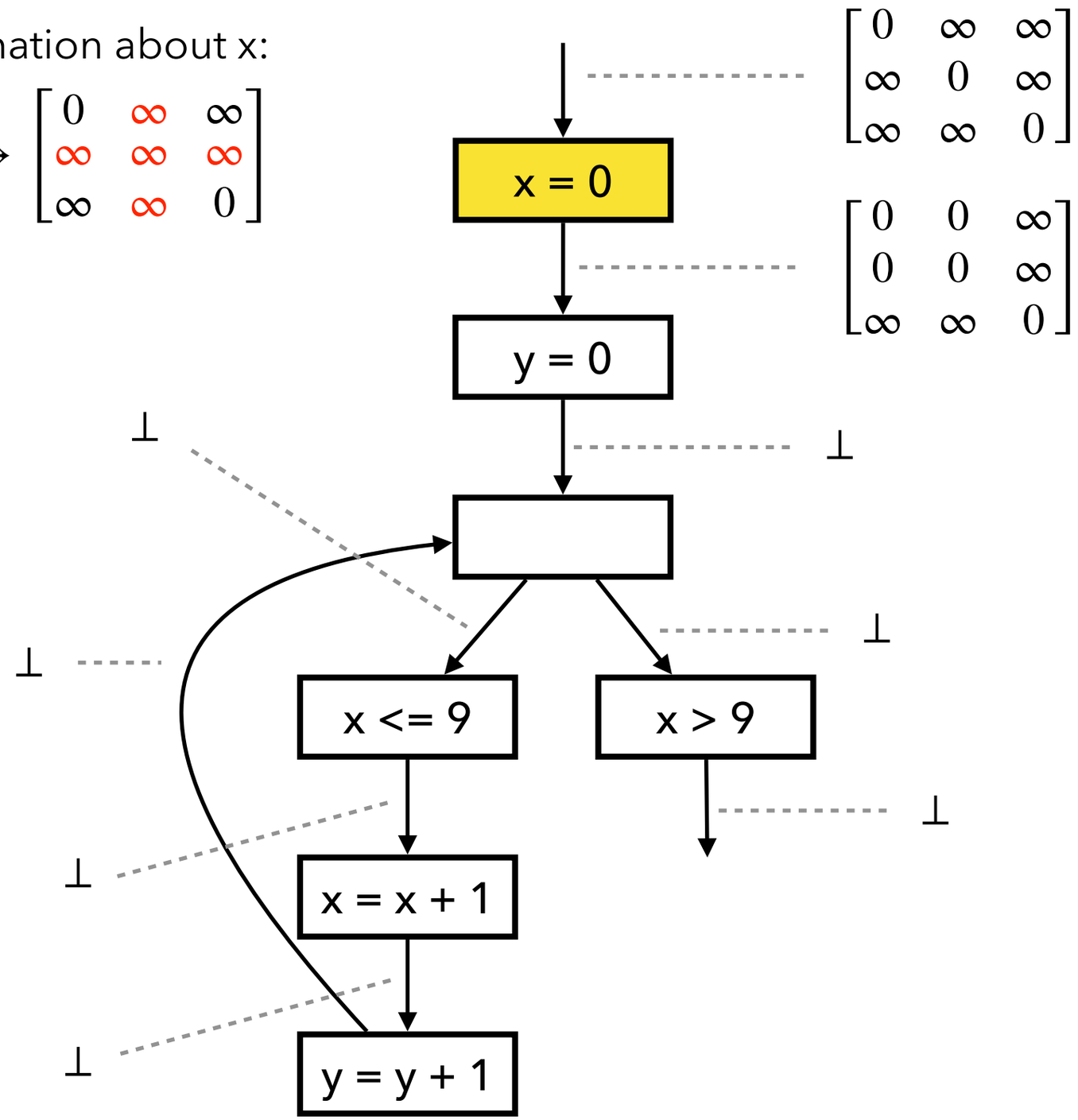
Fixed Point Comp. with Widening



Fixed Point Comp. with Widening

1. Remove information about x:

$$\begin{bmatrix} 0 & \infty & \infty \\ \infty & 0 & \infty \\ \infty & \infty & 0 \end{bmatrix} \rightarrow \begin{bmatrix} 0 & \infty & \infty \\ \infty & \infty & \infty \\ \infty & \infty & 0 \end{bmatrix}$$



$$\begin{bmatrix} 0 & \infty & \infty \\ \infty & 0 & \infty \\ \infty & \infty & 0 \end{bmatrix}$$

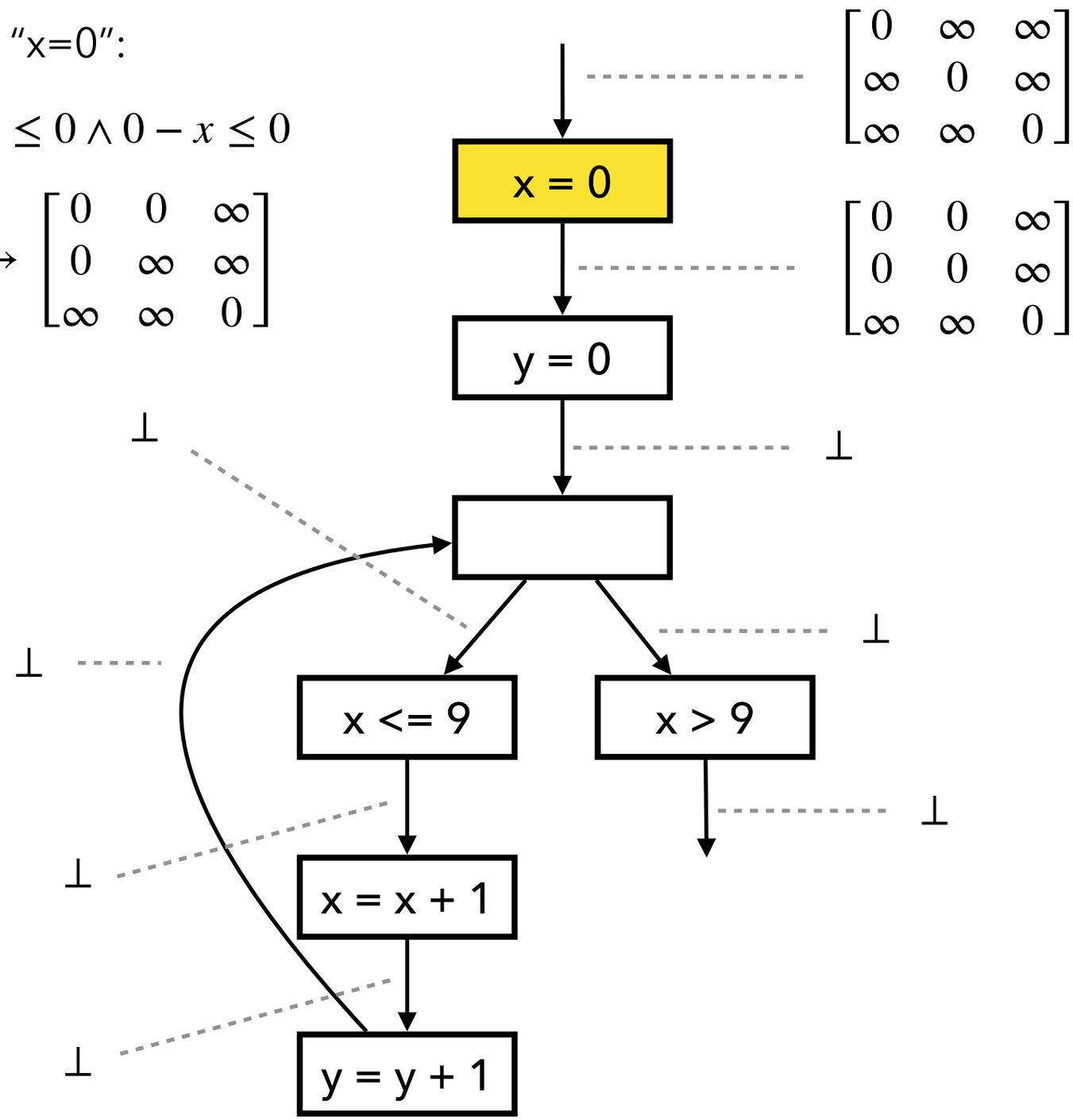
$$\begin{bmatrix} 0 & 0 & \infty \\ 0 & 0 & \infty \\ \infty & \infty & 0 \end{bmatrix}$$

Fixed Point Comp. with Widening

2. Add constraint “x=0”:

$$x = 0 \iff x - 0 \leq 0 \wedge 0 - x \leq 0$$

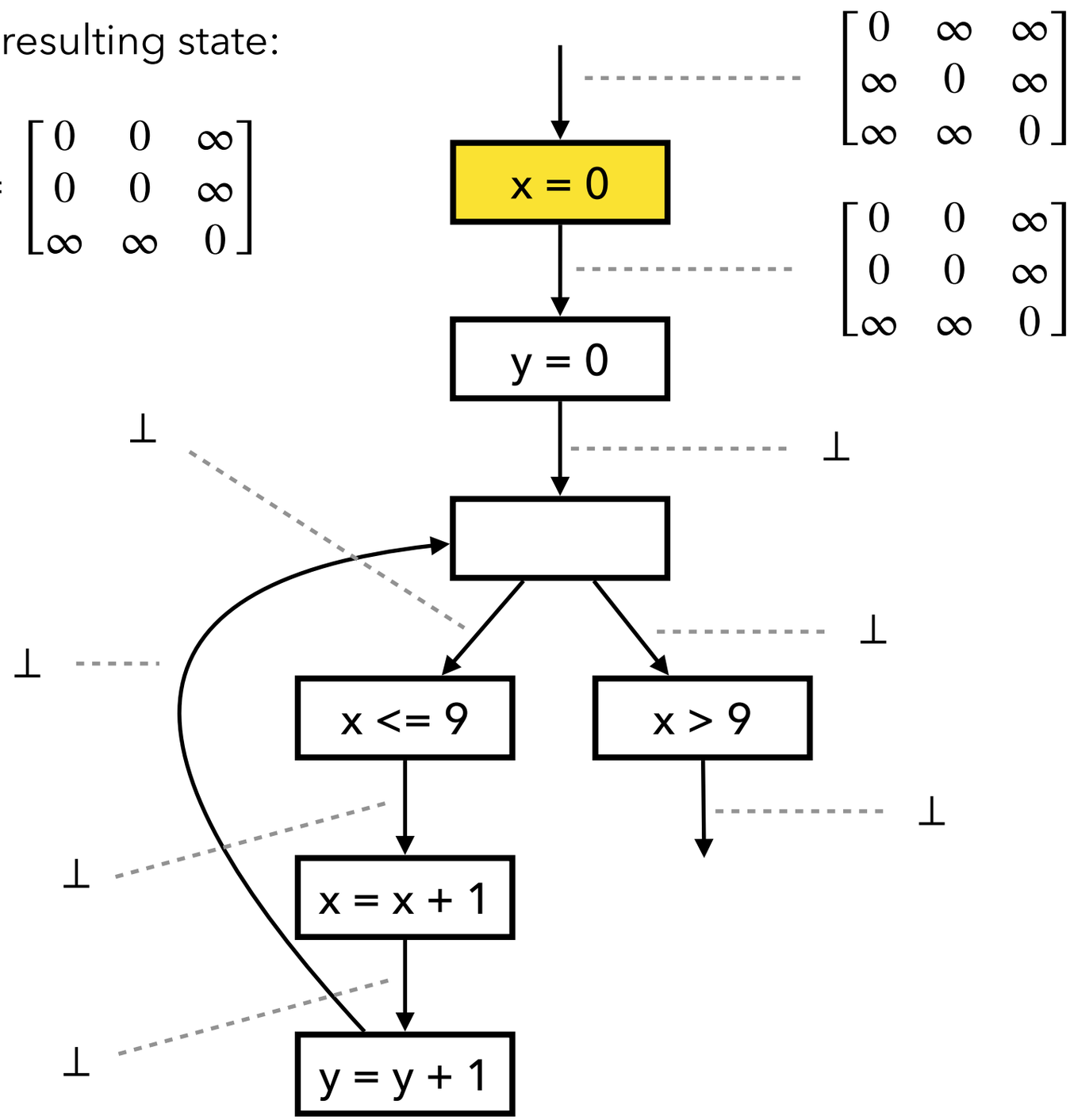
$$\begin{bmatrix} 0 & \infty & \infty \\ \infty & \infty & \infty \\ \infty & \infty & 0 \end{bmatrix} \rightarrow \begin{bmatrix} 0 & 0 & \infty \\ 0 & \infty & \infty \\ \infty & \infty & 0 \end{bmatrix}$$



Fixed Point Comp. with Widening

3. Normalize the resulting state:

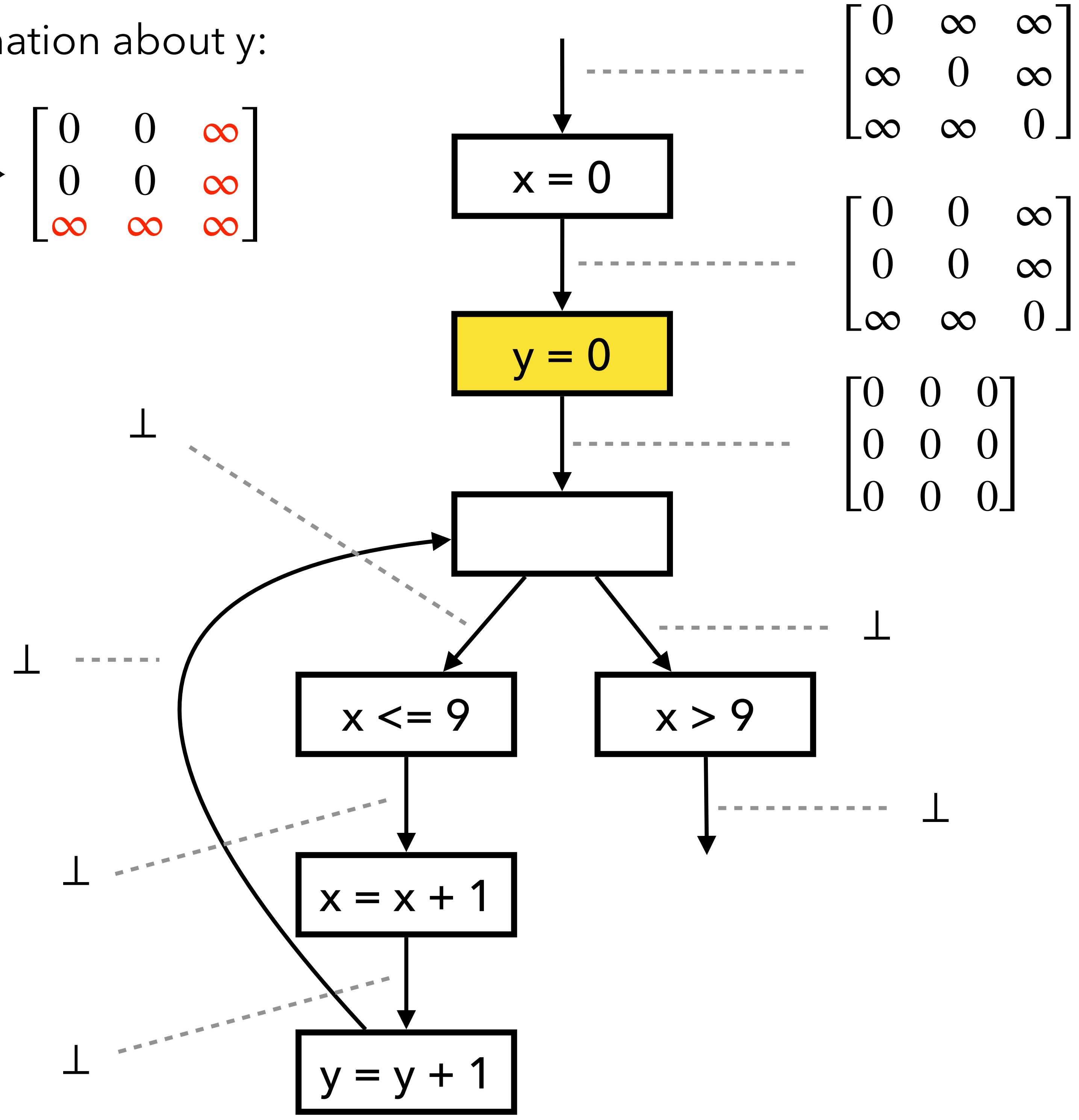
$$\begin{bmatrix} 0 & 0 & \infty \\ 0 & \infty & \infty \\ \infty & \infty & 0 \end{bmatrix}^{*} = \begin{bmatrix} 0 & 0 & \infty \\ 0 & 0 & \infty \\ \infty & \infty & 0 \end{bmatrix}$$



Fixed Point Comp. with Widening

1. Remove information about y:

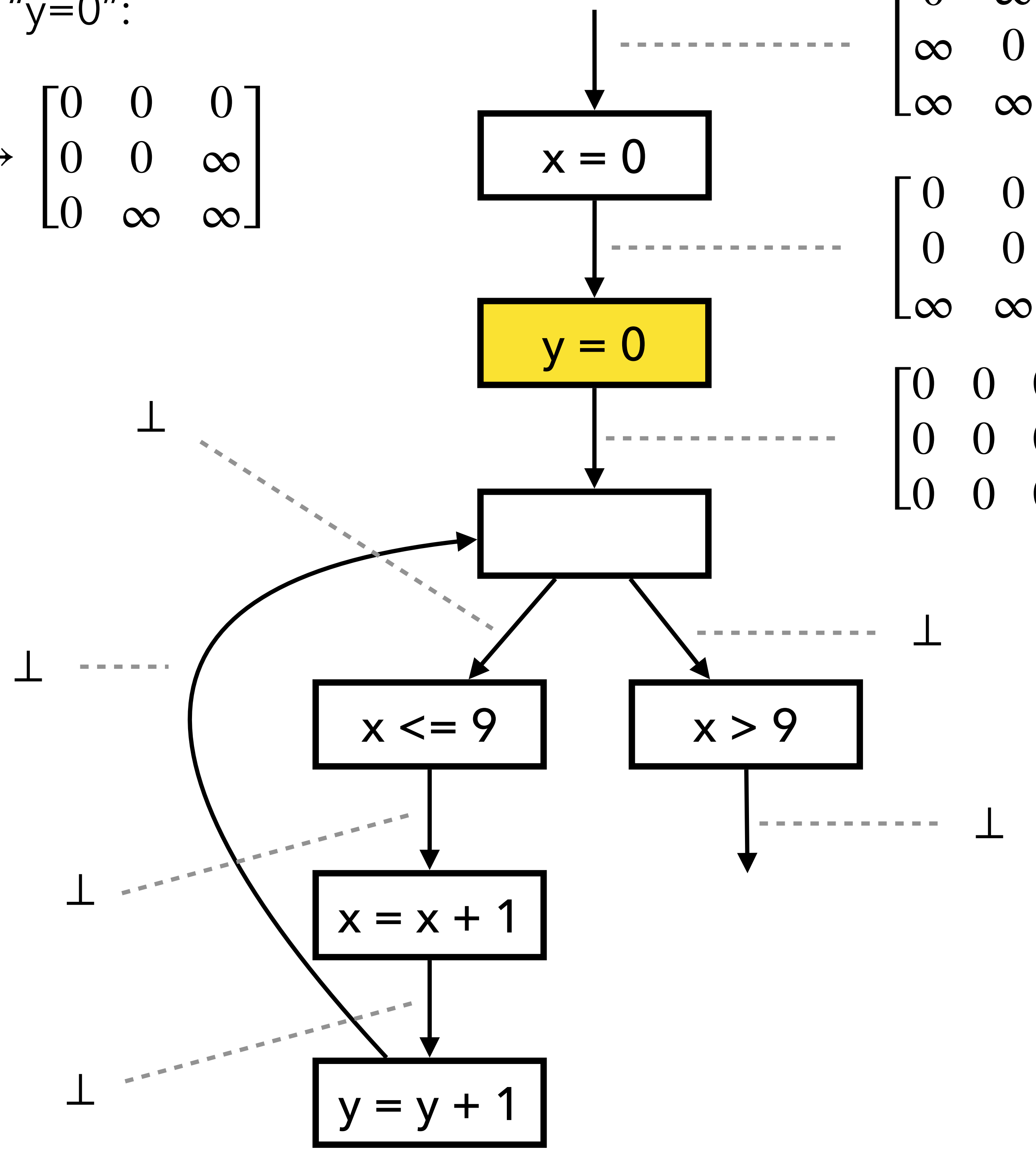
$$\begin{bmatrix} 0 & 0 & \infty \\ 0 & 0 & \infty \\ \infty & \infty & 0 \end{bmatrix} \rightarrow \begin{bmatrix} 0 & 0 & \infty \\ 0 & 0 & \infty \\ \infty & \infty & \infty \end{bmatrix}$$



Fixed Point Comp. with Widening

2. Add constraint "y=0":

$$\begin{bmatrix} 0 & 0 & \infty \\ 0 & 0 & \infty \\ \infty & \infty & \infty \end{bmatrix} \rightarrow \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & \infty \\ 0 & \infty & \infty \end{bmatrix}$$



$$\begin{bmatrix} 0 & \infty & \infty \\ \infty & 0 & \infty \\ \infty & \infty & 0 \end{bmatrix}$$

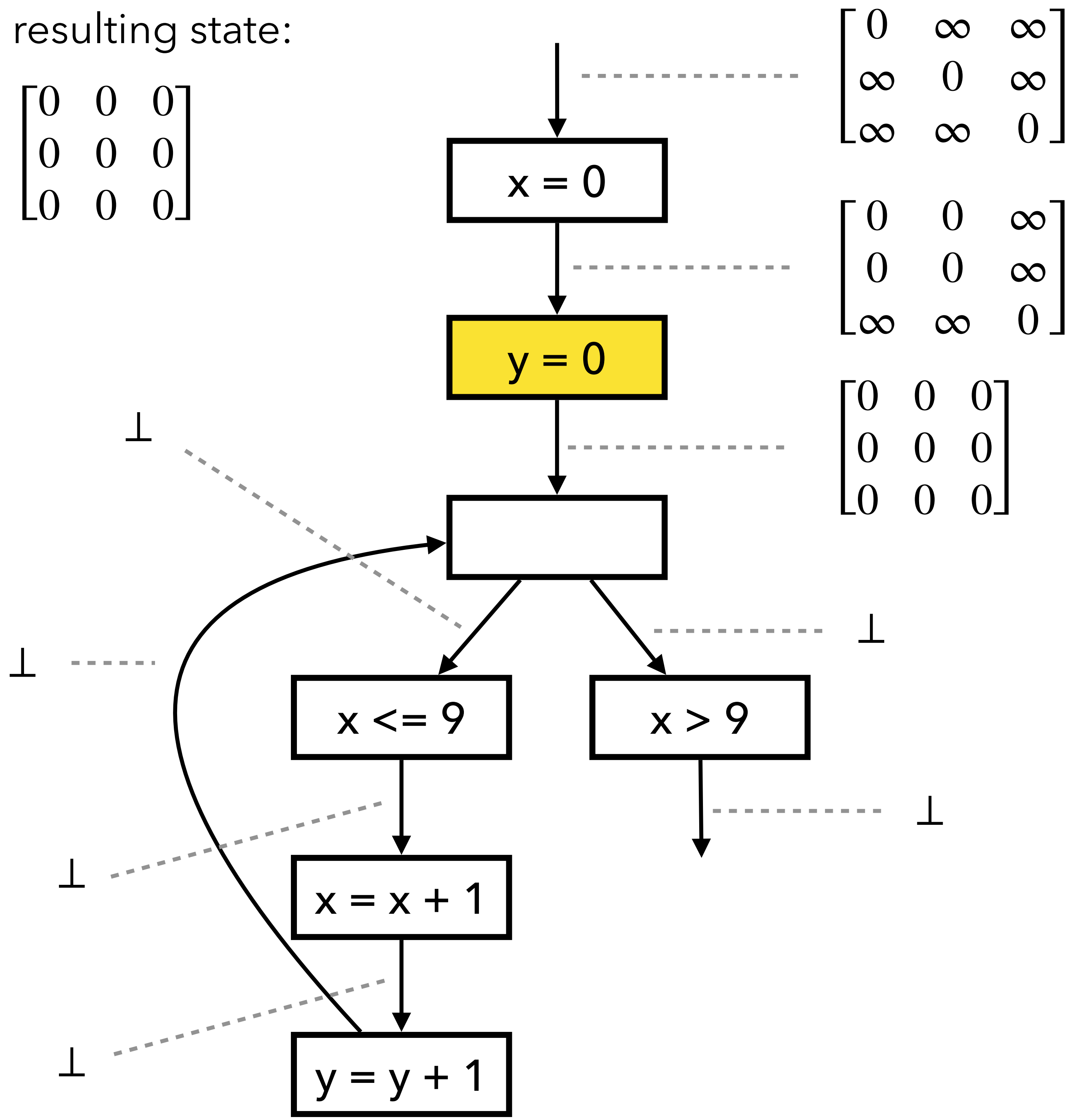
$$\begin{bmatrix} 0 & 0 & \infty \\ 0 & 0 & \infty \\ \infty & \infty & 0 \end{bmatrix}$$

$$\begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

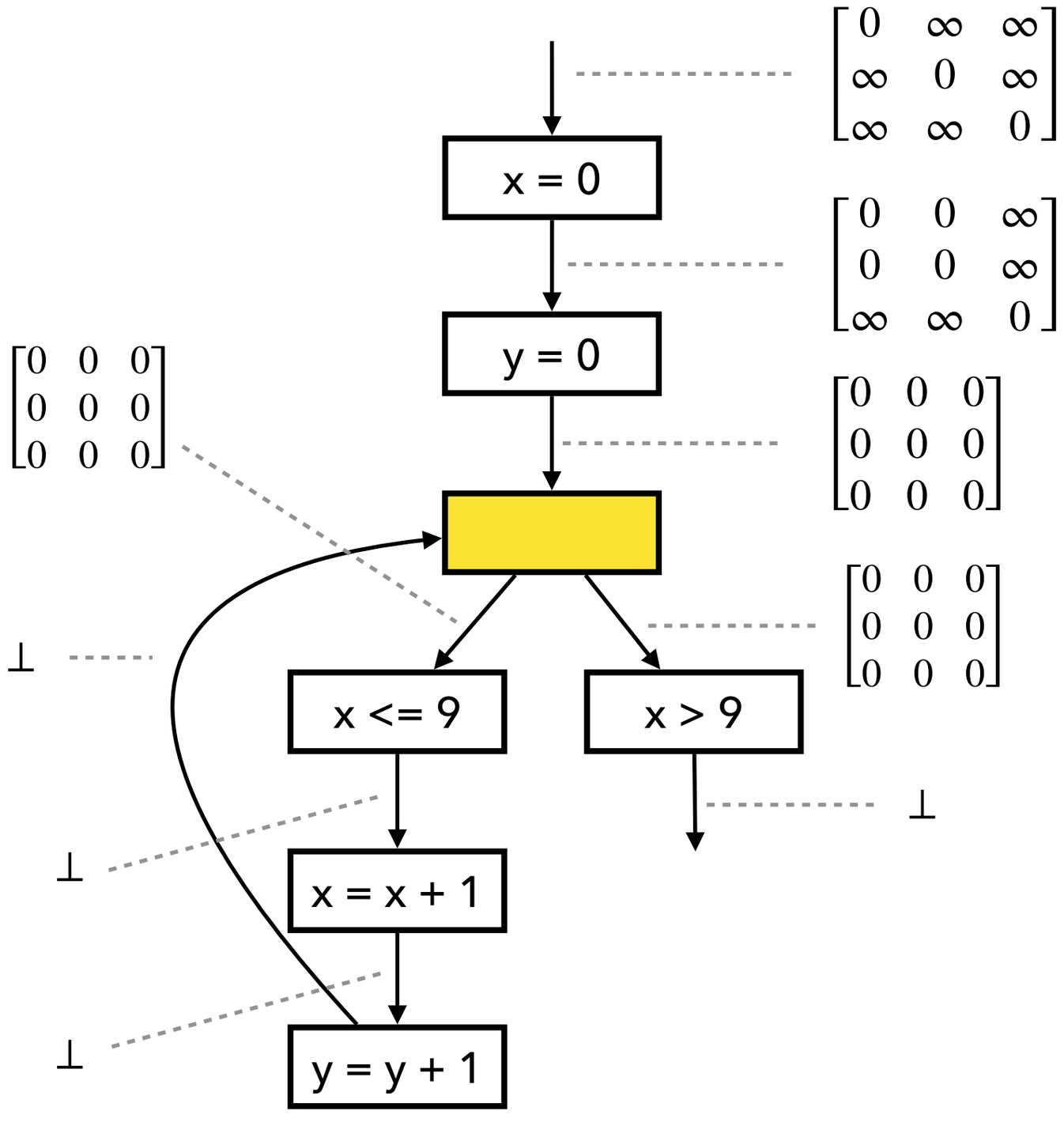
Fixed Point Comp. with Widening

3. Normalize the resulting state:

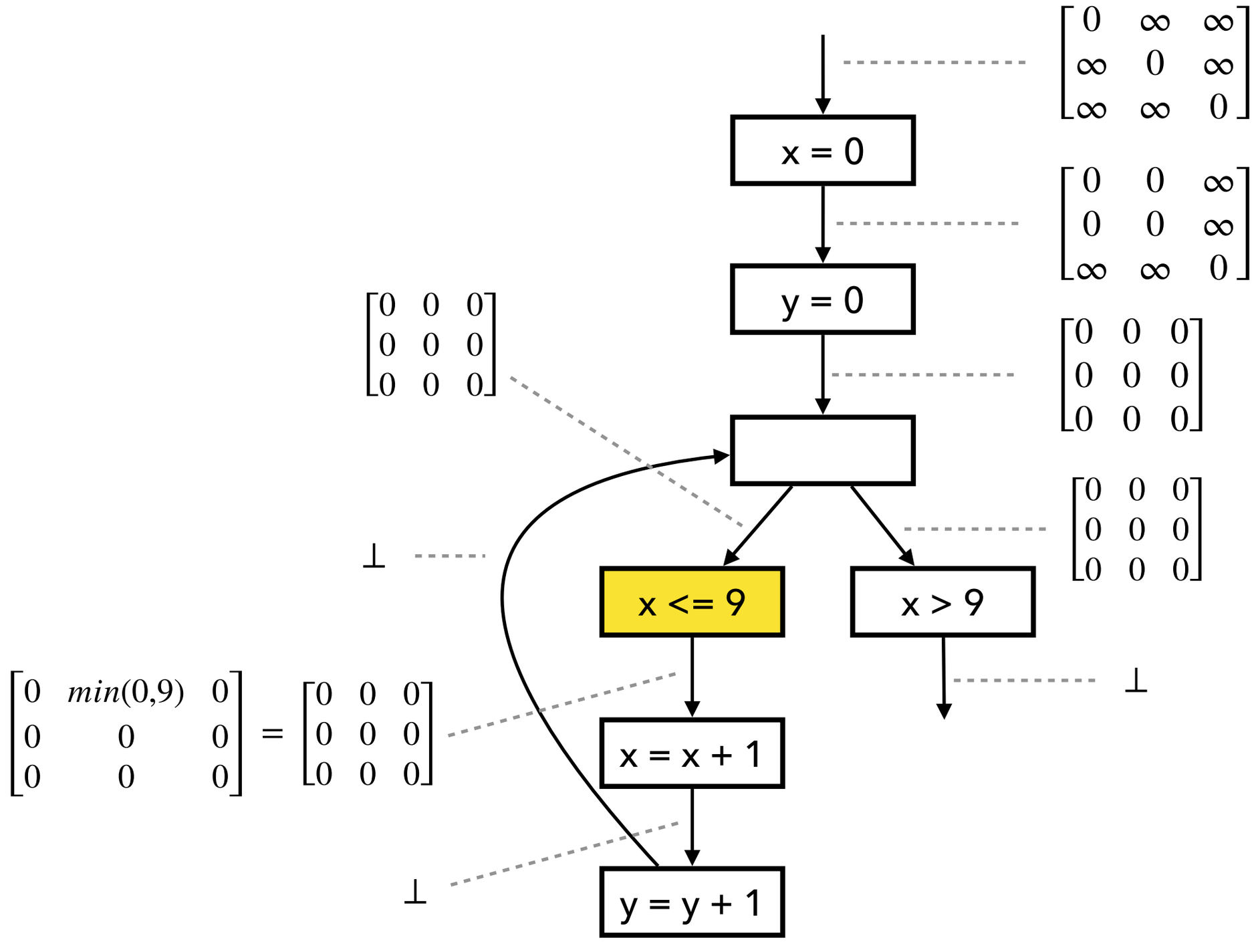
$$\begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & \infty \\ 0 & \infty & \infty \end{bmatrix}^* = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$



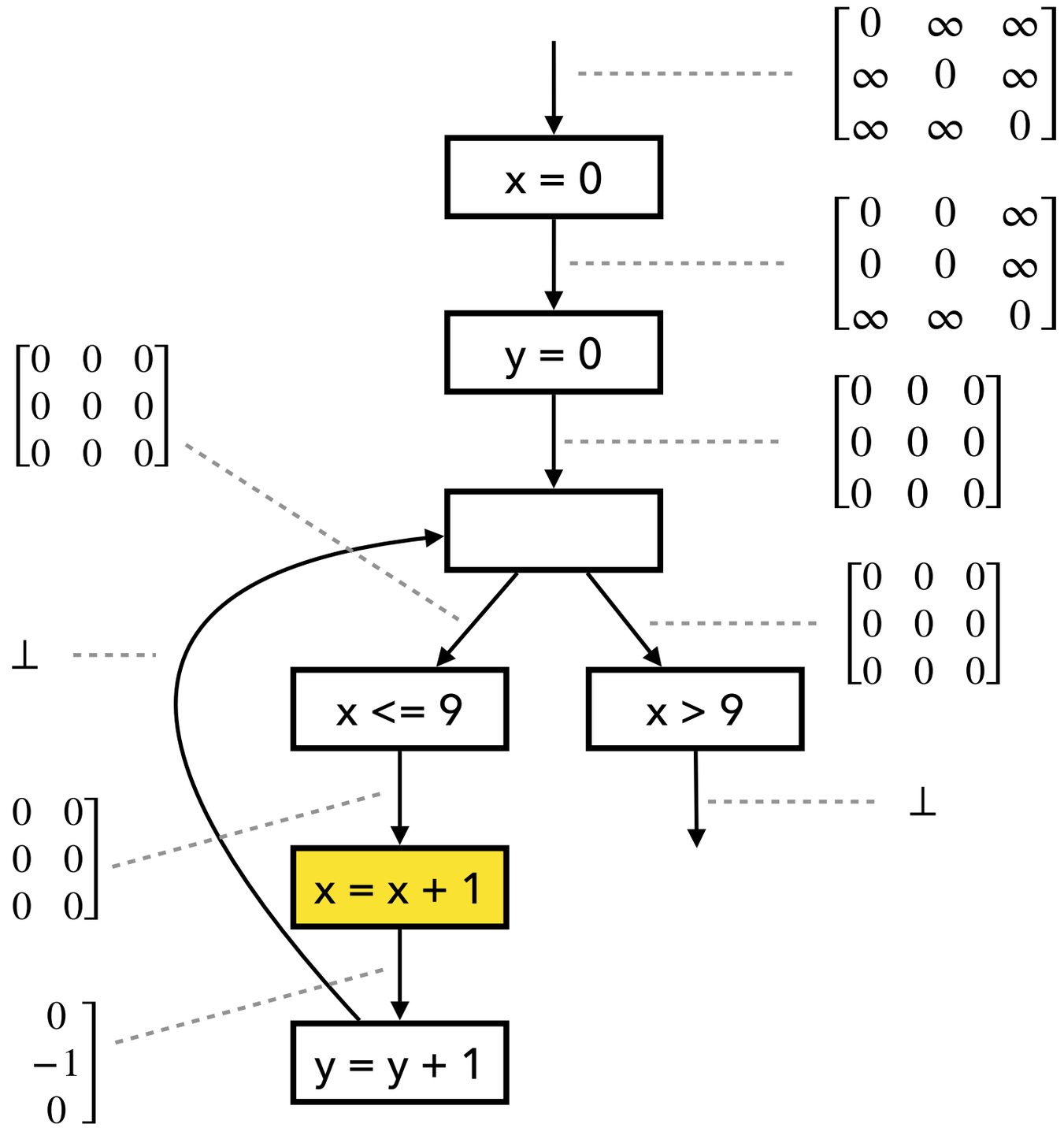
Fixed Point Comp. with Widening



Fixed Point Comp. with Widening



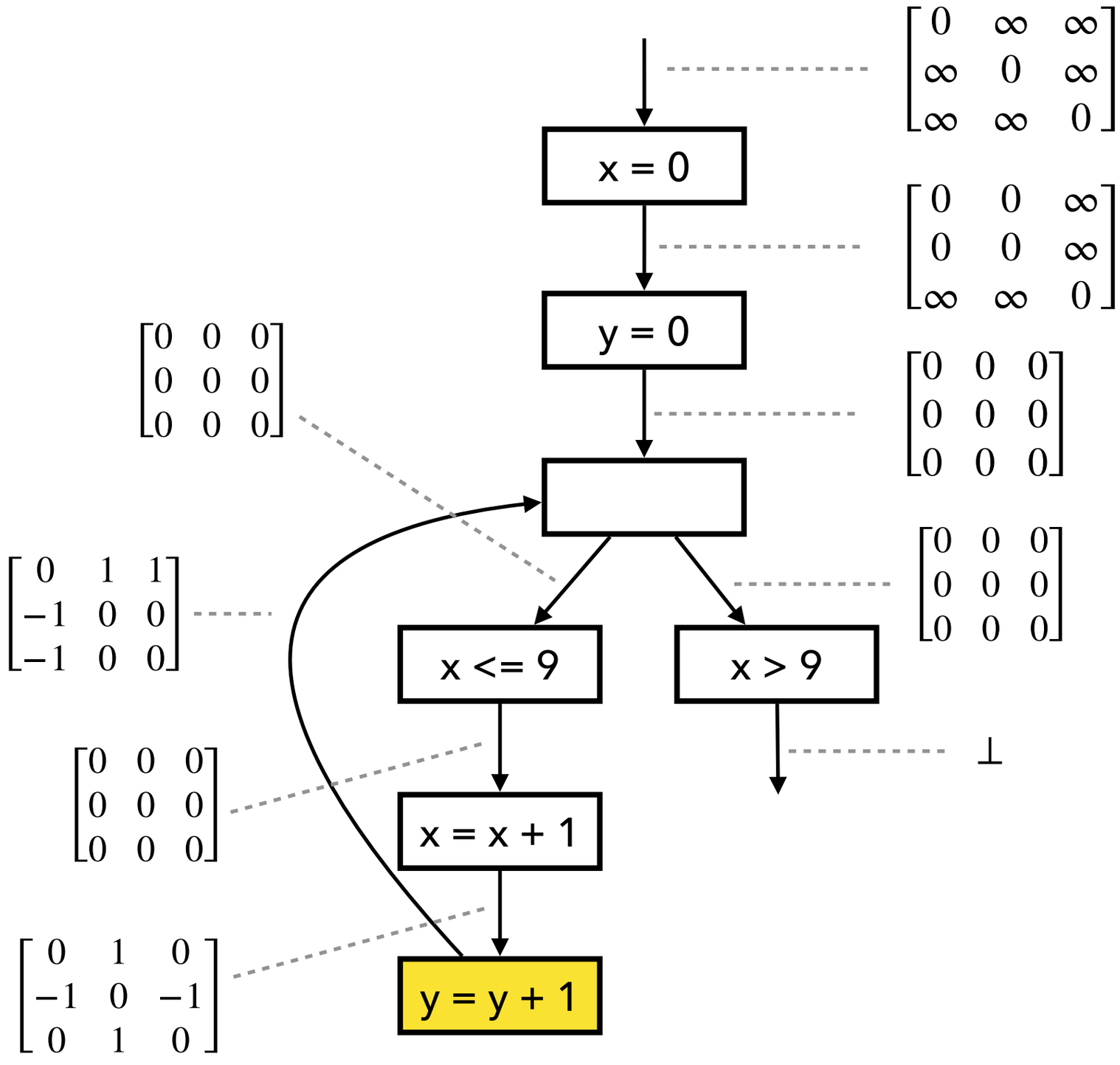
Fixed Point Comp. with Widening



$x - x' \leq c \rightarrow x - x' \leq c + 1$

$x' - x \leq c \rightarrow x' - x \leq c - 1$

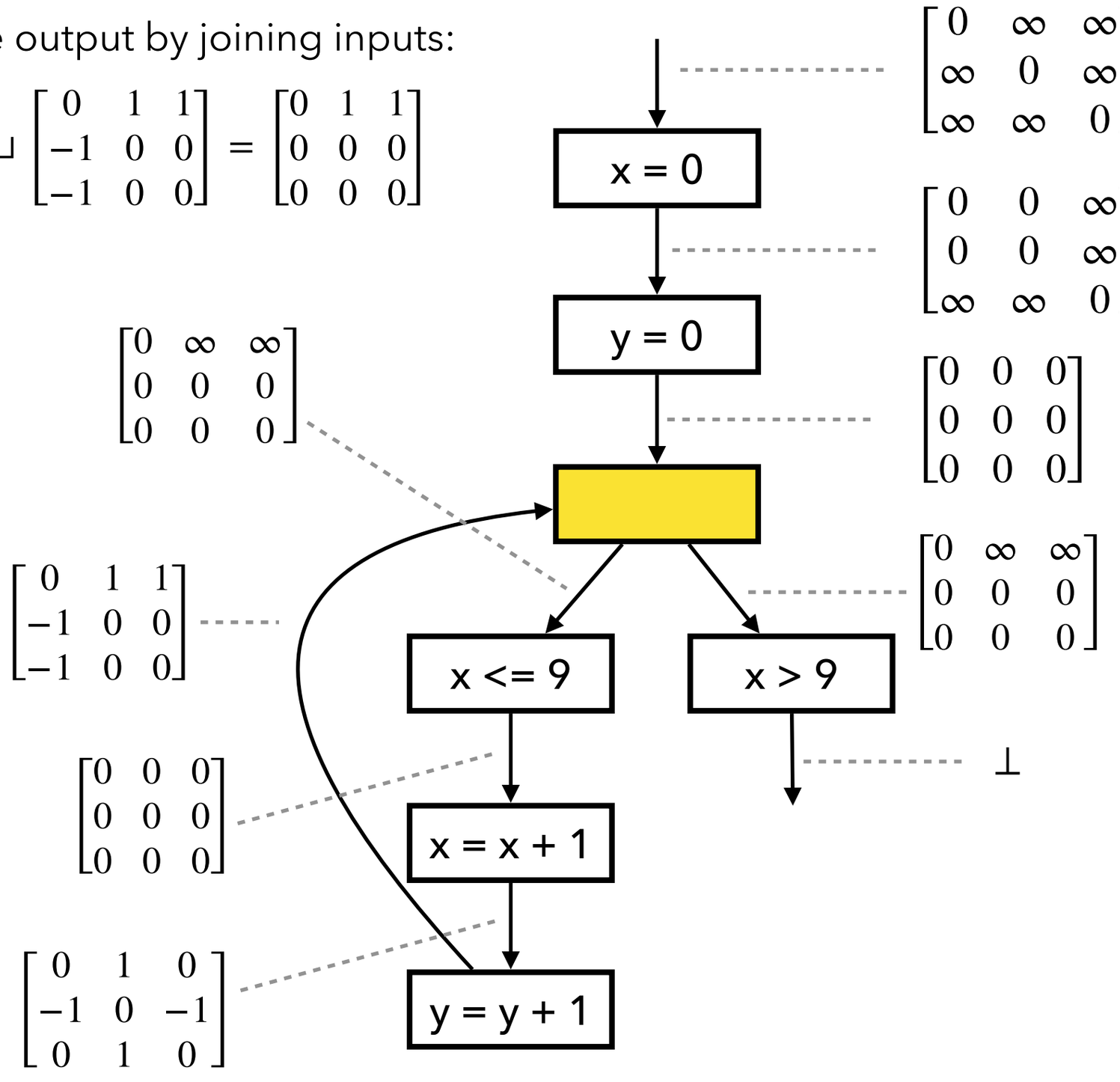
Fixed Point Comp. with Widening



Fixed Point Comp. with Widening

1. Compute output by joining inputs:

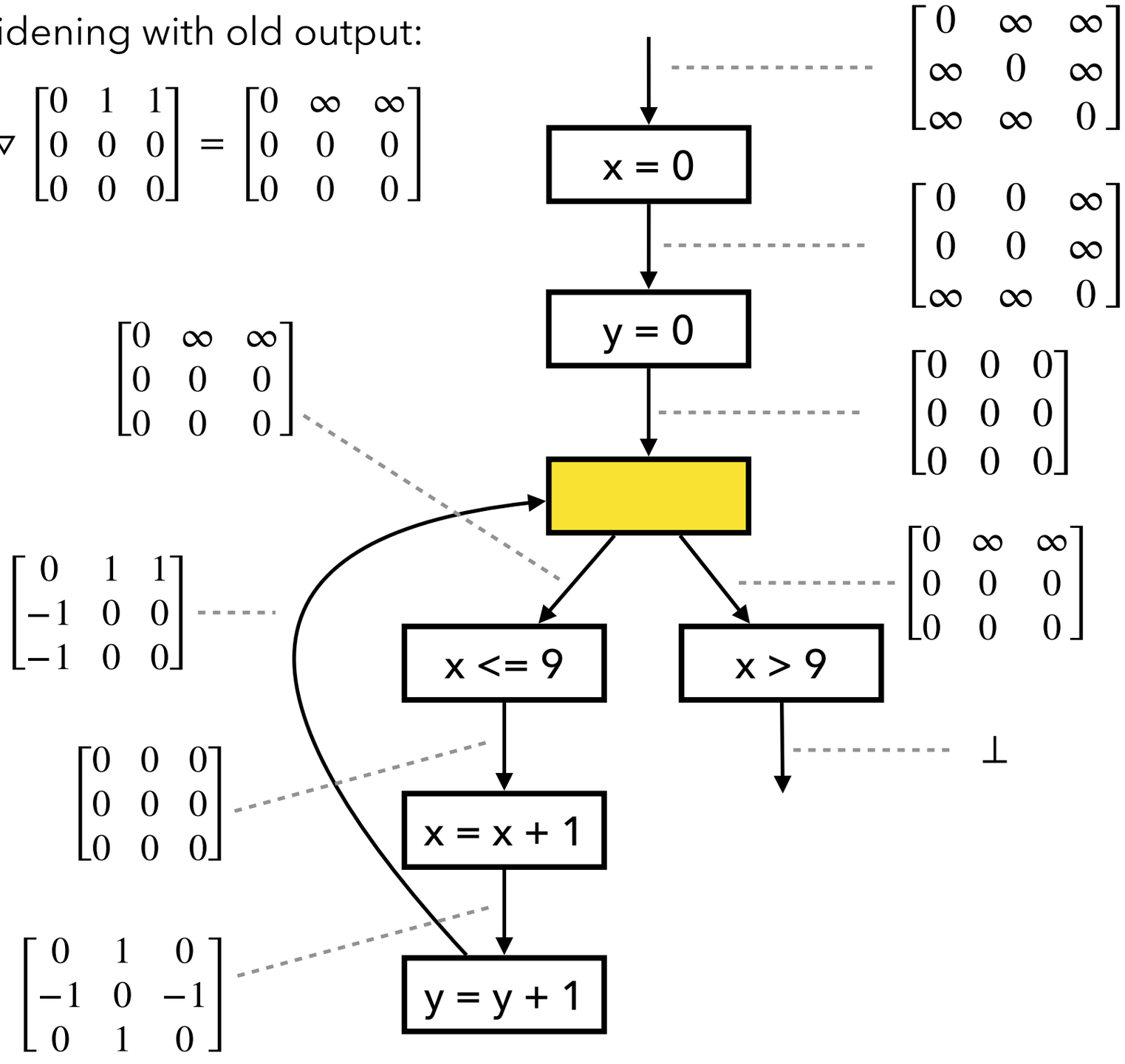
$$\begin{bmatrix}0&0&0\\0&0&0\\0&0&0\end{bmatrix} \sqcup \begin{bmatrix}0&1&1\\-1&0&0\\-1&0&0\end{bmatrix} = \begin{bmatrix}0&1&1\\0&0&0\\0&0&0\end{bmatrix}$$



Fixed Point Comp. with Widening

2. Apply widening with old output:

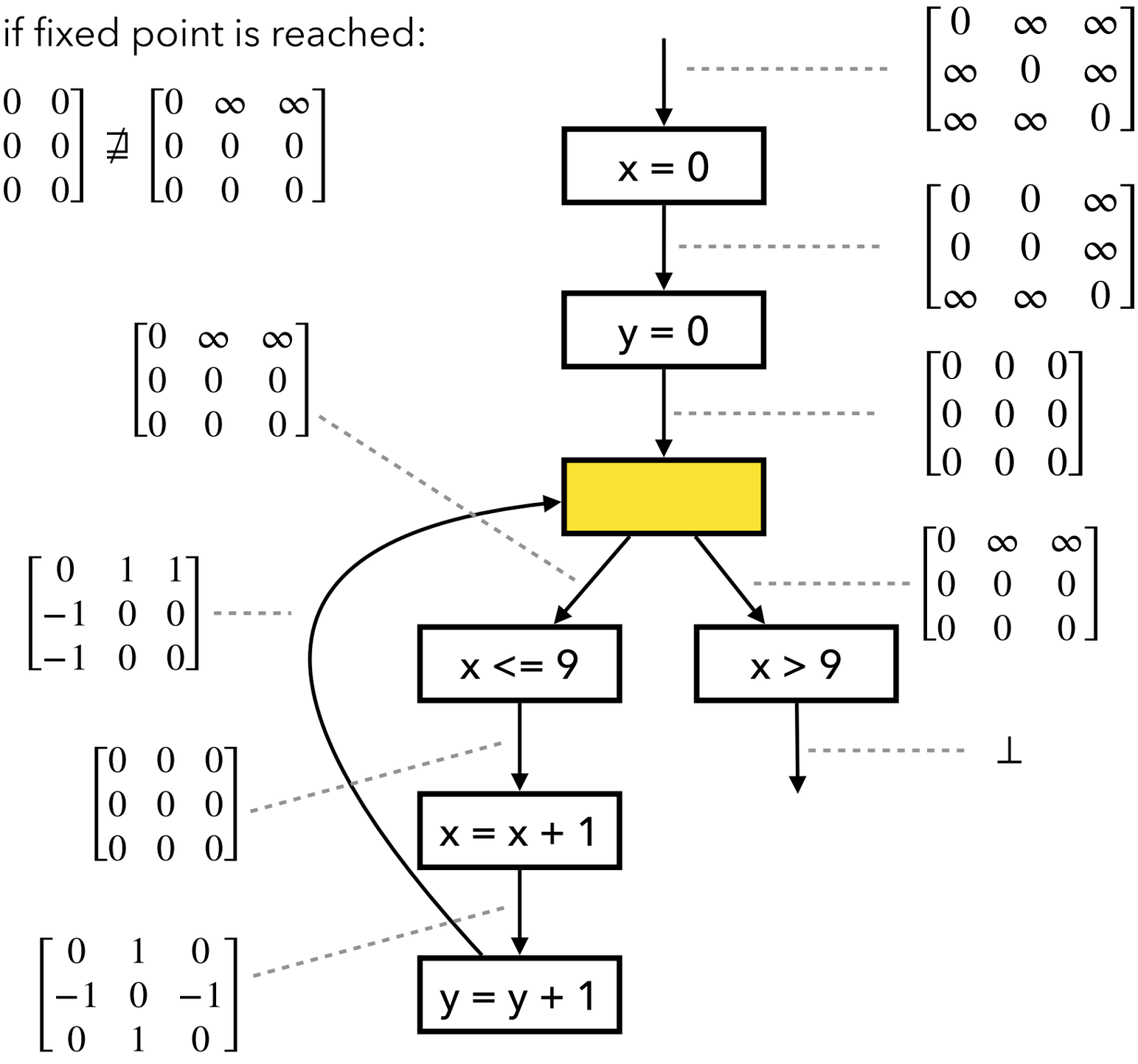
$$\begin{bmatrix}0&0&0\\0&0&0\\0&0&0\end{bmatrix} \triangledown \begin{bmatrix}0&1&1\\0&0&0\\0&0&0\end{bmatrix} = \begin{bmatrix}0&\infty&\infty\\0&0&0\\0&0&0\end{bmatrix}$$



Fixed Point Comp. with Widening

3. Check if fixed point is reached:

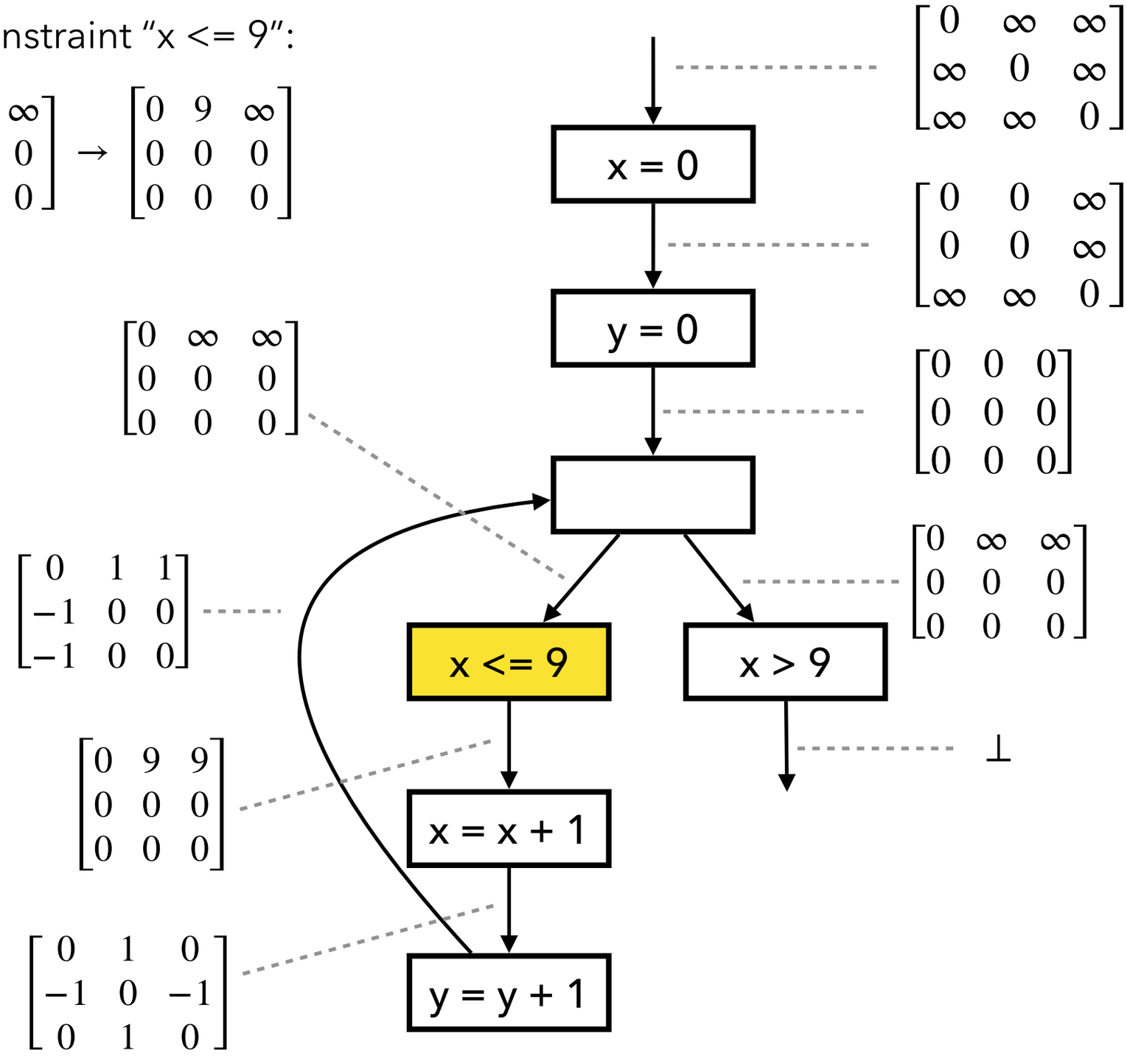
$$\begin{bmatrix}0 & 0 & 0\\ 0 & 0 & 0\\ 0 & 0 & 0\end{bmatrix} \not\equiv \begin{bmatrix}0 & \infty & \infty\\ 0 & 0 & 0\\ 0 & 0 & 0\end{bmatrix}$$



Fixed Point Comp. with Widening

1. Add constraint “x <= 9”:

$$\begin{bmatrix}0 & \infty & \infty\\ 0 & 0 & 0\\ 0 & 0 & 0\end{bmatrix} \rightarrow \begin{bmatrix}0 & 9 & \infty\\ 0 & 0 & 0\\ 0 & 0 & 0\end{bmatrix}$$



$$\begin{bmatrix}0 & \infty & \infty\\ \infty & 0 & \infty\\ \infty & \infty & 0\end{bmatrix}$$

$$\begin{bmatrix}0 & 0 & \infty\\ 0 & 0 & \infty\\ \infty & \infty & 0\end{bmatrix}$$

$$\begin{bmatrix}0 & 0 & 0\\ 0 & 0 & 0\\ 0 & 0 & 0\end{bmatrix}$$

$$\begin{bmatrix}0 & \infty & \infty\\ 0 & 0 & 0\\ 0 & 0 & 0\end{bmatrix}$$

$$\begin{bmatrix}0 & \infty & \infty\\ \infty & 0 & \infty\\ \infty & \infty & 0\end{bmatrix}$$

$$\begin{bmatrix}0 & 1 & 1\\ -1 & 0 & 0\\ -1 & 0 & 0\end{bmatrix}$$

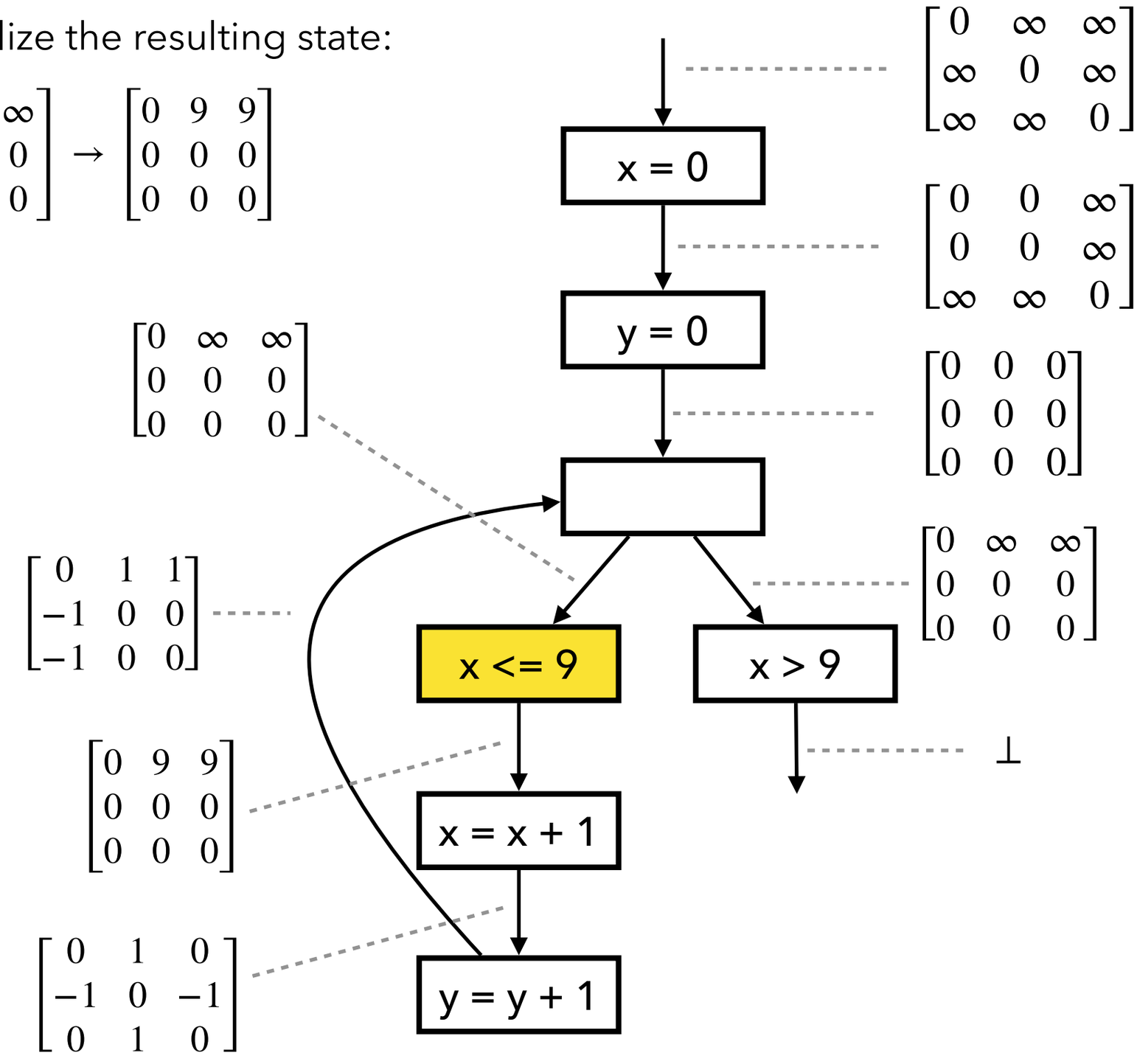
$$\begin{bmatrix}0 & 9 & 9\\ 0 & 0 & 0\\ 0 & 0 & 0\end{bmatrix}$$

$$\begin{bmatrix}0 & 1 & 0\\ -1 & 0 & -1\\ 0 & 1 & 0\end{bmatrix}$$

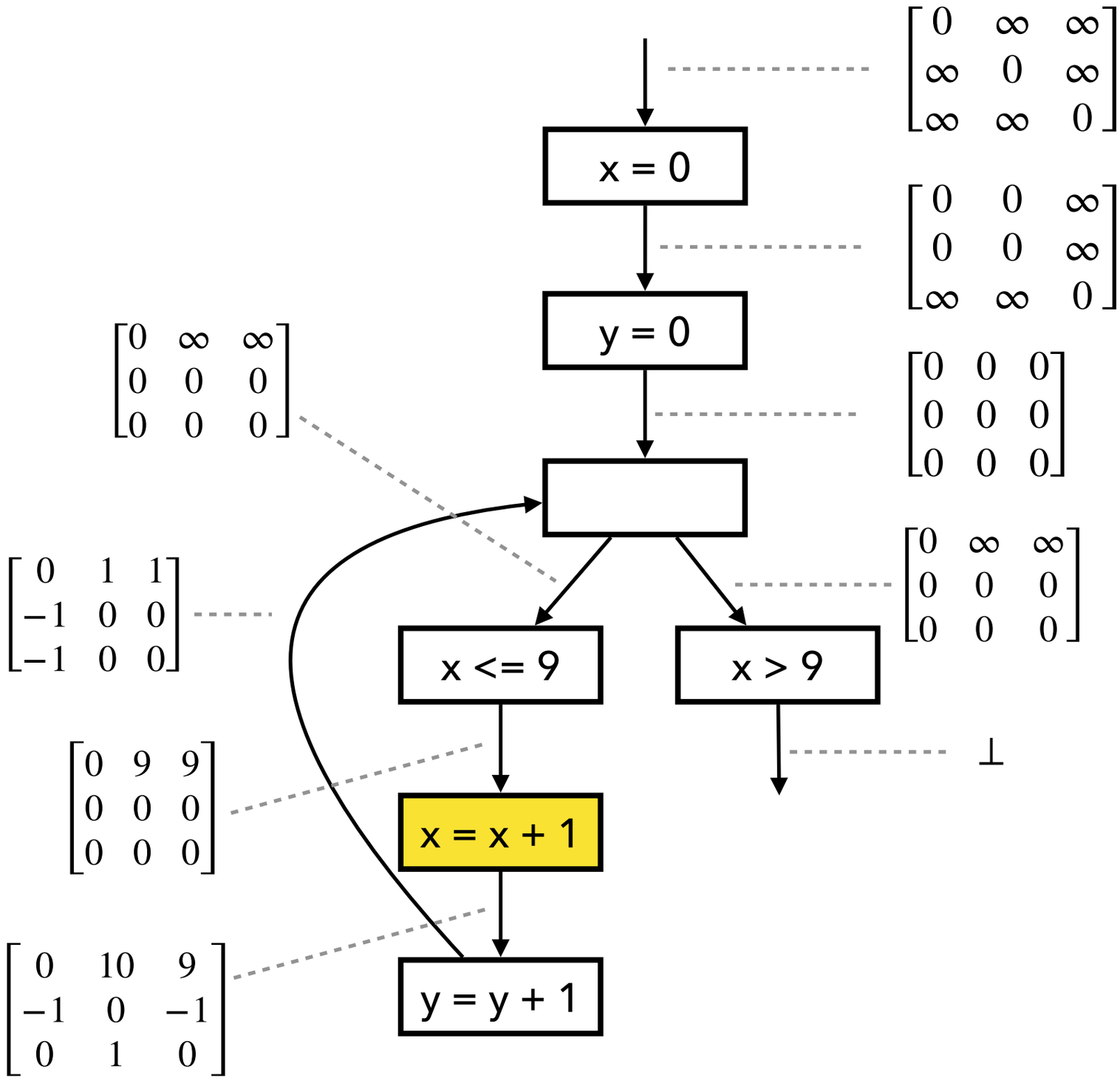
Fixed Point Comp. with Widening

2. Normalize the resulting state:

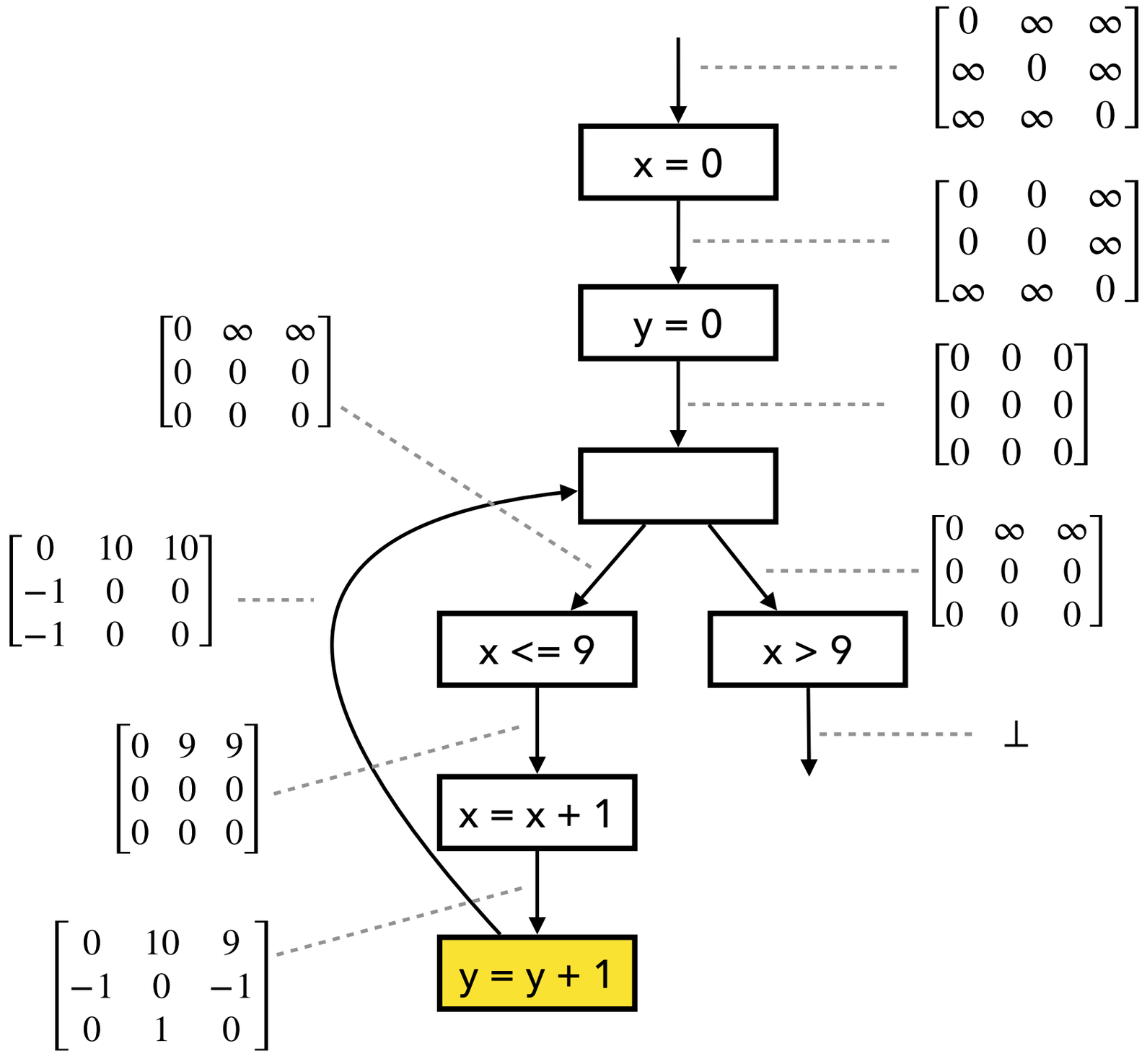
$$\begin{bmatrix} 0 & 9 & \infty \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \rightarrow \begin{bmatrix} 0 & 9 & 9 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$



Fixed Point Comp. with Widening



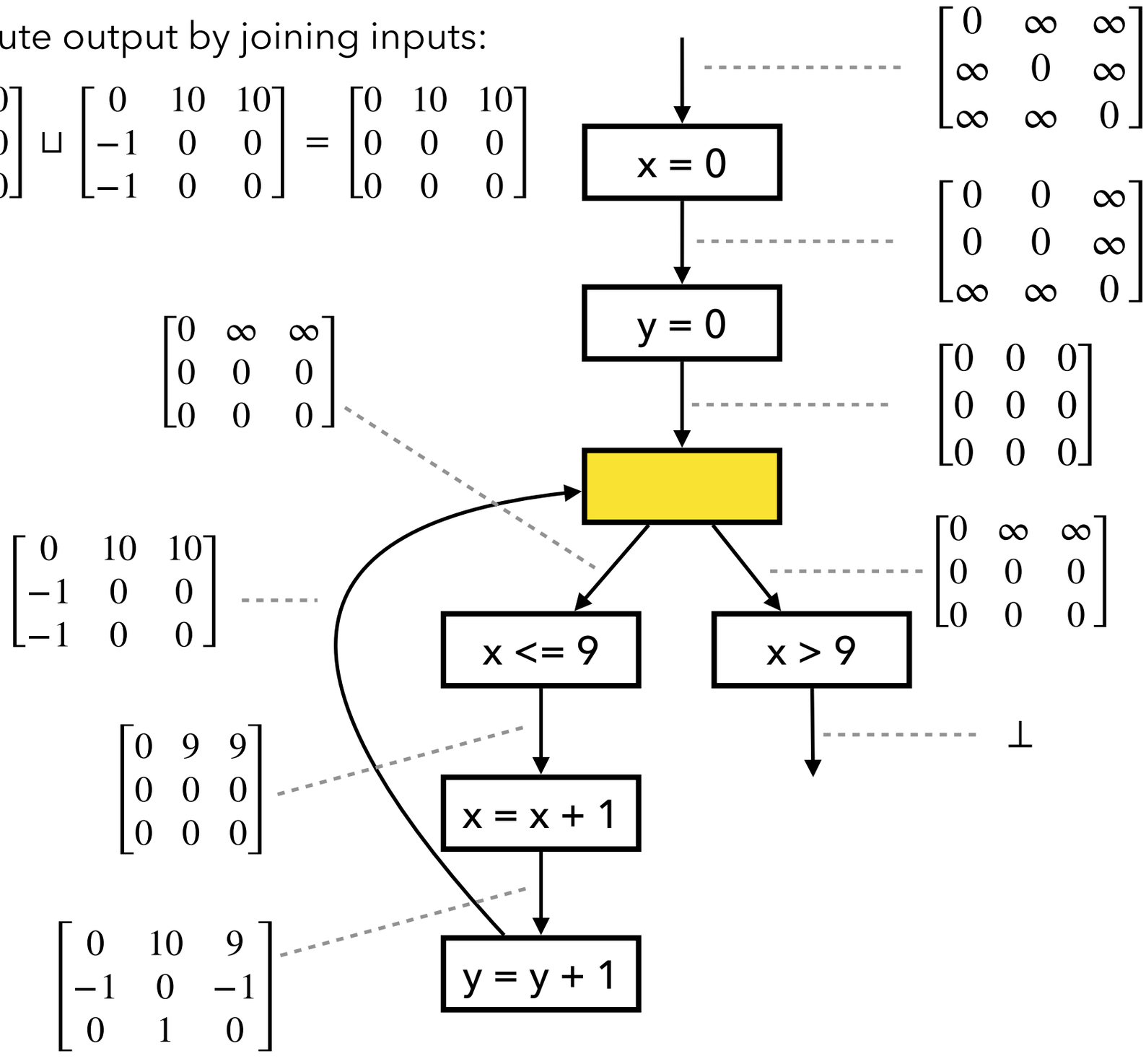
Fixed Point Comp. with Widening



Fixed Point Comp. with Widening

1. Compute output by joining inputs:

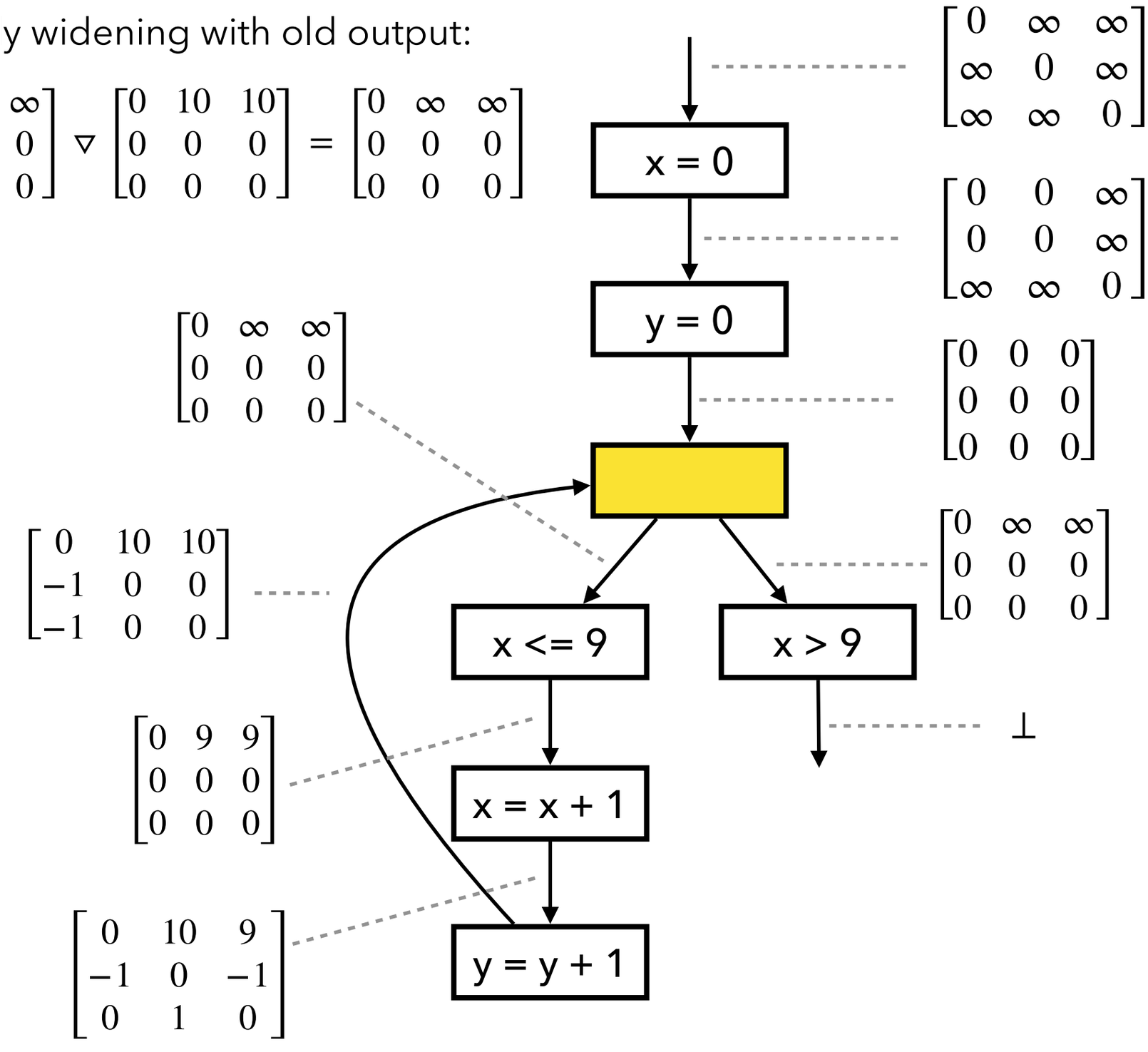
$$\begin{bmatrix}0&0&0\\0&0&0\\0&0&0\end{bmatrix} \sqcup \begin{bmatrix}0&10&10\\-1&0&0\\-1&0&0\end{bmatrix} = \begin{bmatrix}0&10&10\\0&0&0\\0&0&0\end{bmatrix}$$



Fixed Point Comp. with Widening

2. Apply widening with old output:

$$\begin{bmatrix}0 & \infty & \infty\\ 0 & 0 & 0\\ 0 & 0 & 0\end{bmatrix} \triangledown \begin{bmatrix}0 & 10 & 10\\ 0 & 0 & 0\\ 0 & 0 & 0\end{bmatrix} = \begin{bmatrix}0 & \infty & \infty\\ 0 & 0 & 0\\ 0 & 0 & 0\end{bmatrix}$$



$$\begin{bmatrix}0 & \infty & \infty\\ \infty & 0 & \infty\\ \infty & \infty & 0\end{bmatrix}$$

$$\begin{bmatrix}0 & 0 & \infty\\ 0 & 0 & \infty\\ \infty & \infty & 0\end{bmatrix}$$

$$\begin{bmatrix}0 & 0 & 0\\ 0 & 0 & 0\\ 0 & 0 & 0\end{bmatrix}$$

$$\begin{bmatrix}0 & \infty & \infty\\ 0 & 0 & 0\\ 0 & 0 & 0\end{bmatrix}$$

$$\begin{bmatrix}0 & \infty & \infty\\ 0 & 0 & 0\\ 0 & 0 & 0\end{bmatrix}$$

$$\begin{bmatrix}0 & 10 & 10\\ -1 & 0 & 0\\ -1 & 0 & 0\end{bmatrix}$$

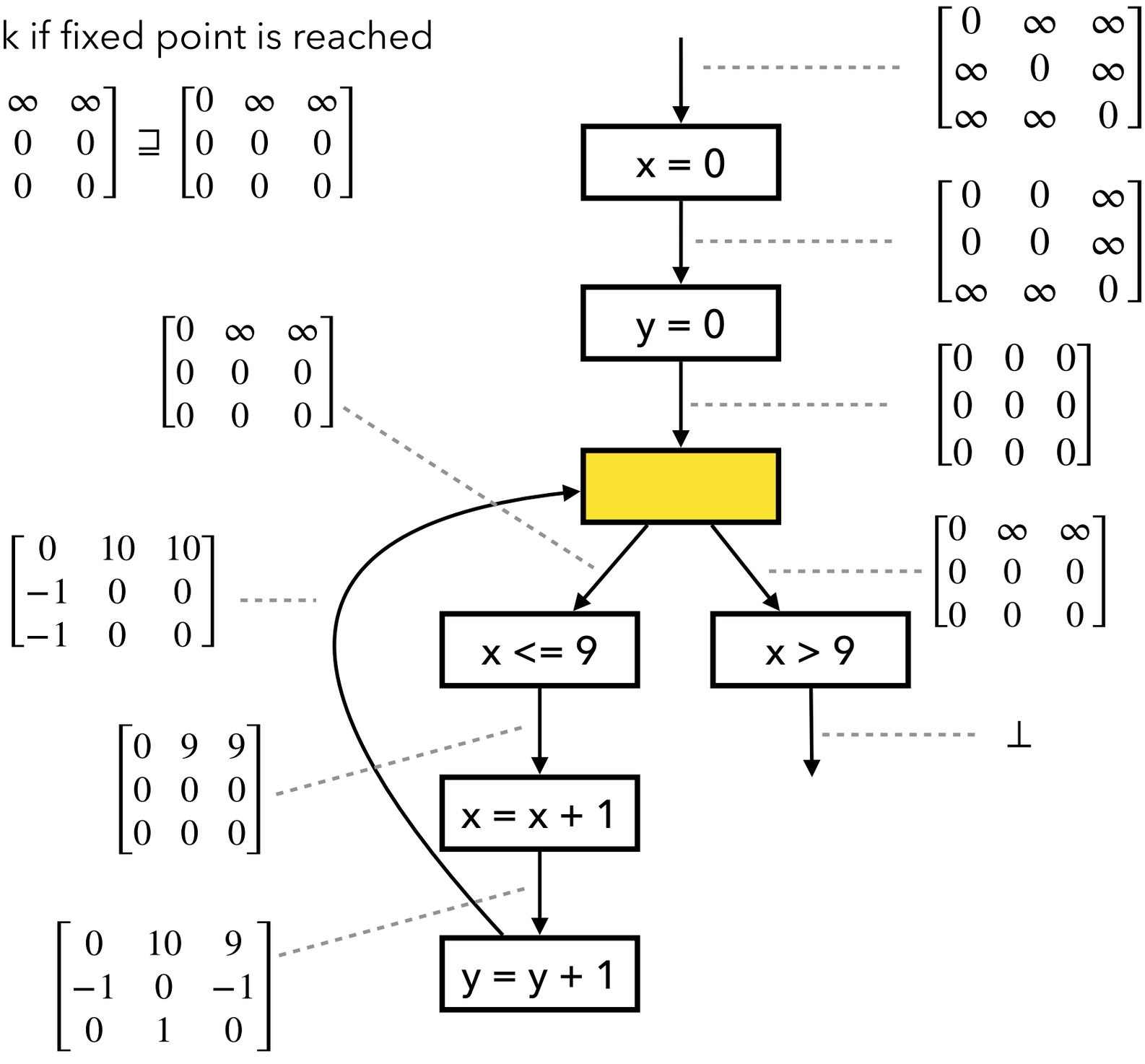
$$\begin{bmatrix}0 & 9 & 9\\ 0 & 0 & 0\\ 0 & 0 & 0\end{bmatrix}$$

$$\begin{bmatrix}0 & 10 & 9\\ -1 & 0 & -1\\ 0 & 1 & 0\end{bmatrix}$$

Fixed Point Comp. with Widening

3. Check if fixed point is reached

$$\begin{bmatrix} 0 & \infty & \infty \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \sqsupseteq \begin{bmatrix} 0 & \infty & \infty \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

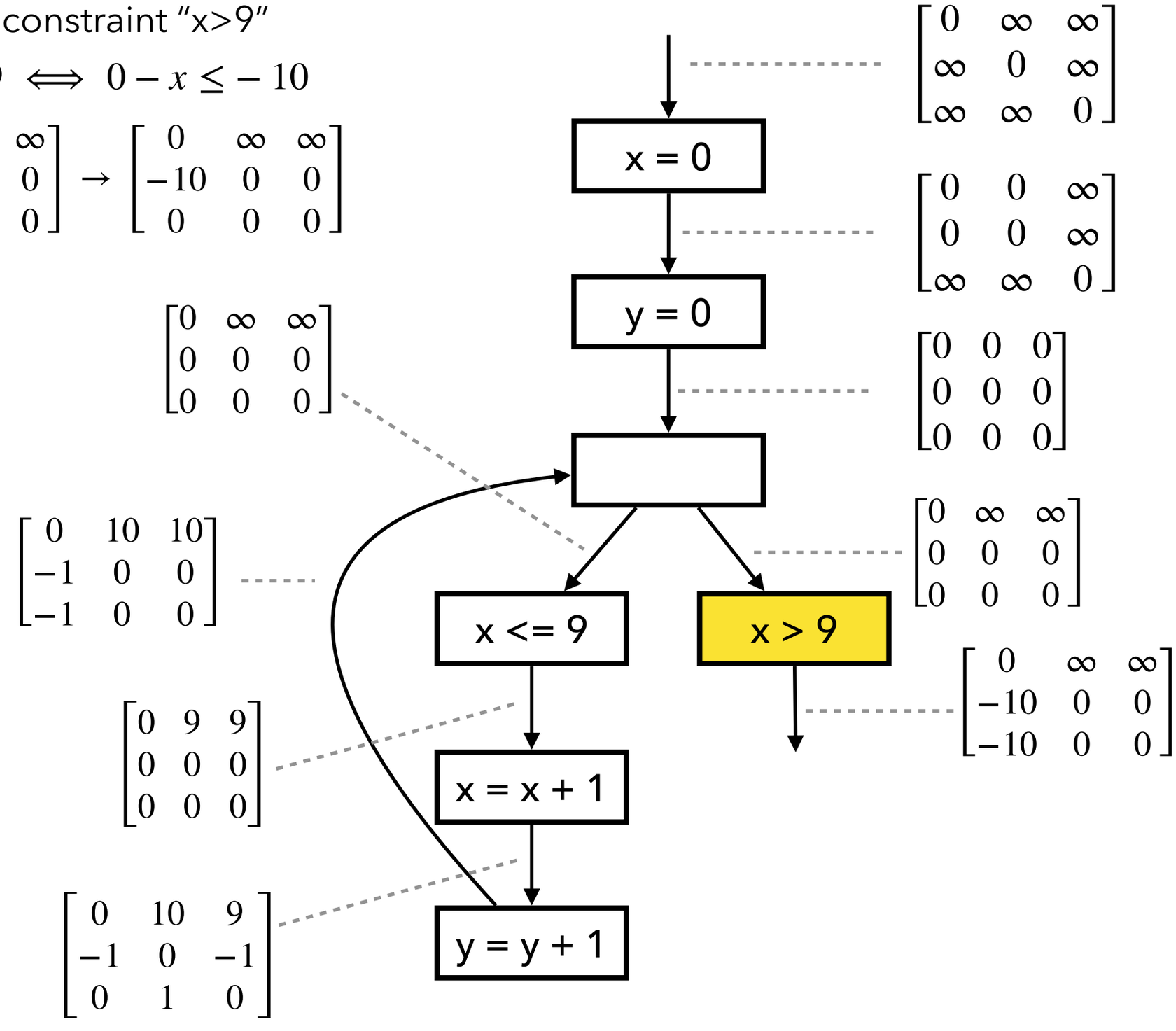


Fixed Point Comp. with Widening

1. Add constraint “x>9”

$$x > 9 \iff 0 - x \leq -10$$

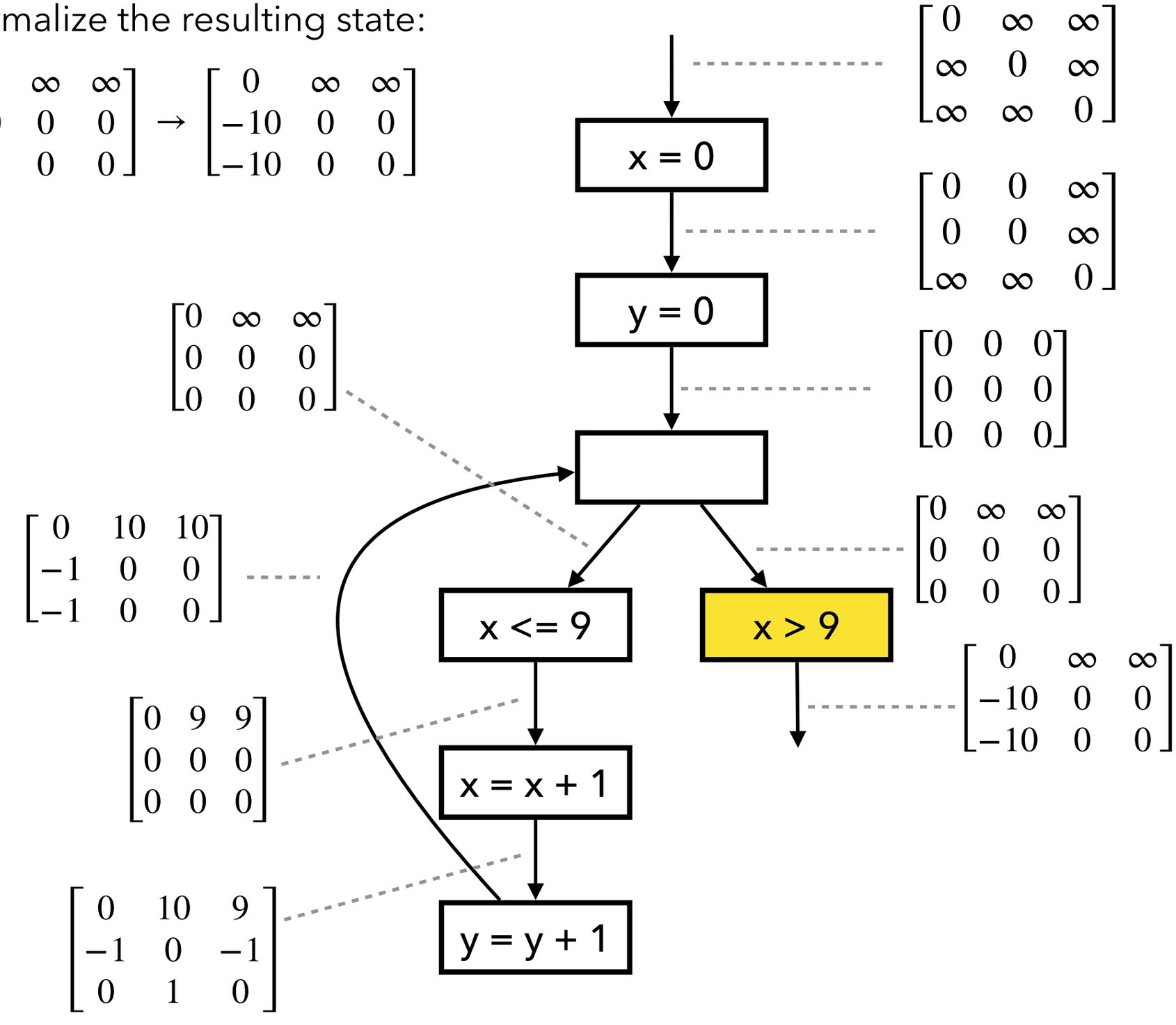
$$\begin{bmatrix} 0 & \infty & \infty \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \rightarrow \begin{bmatrix} 0 & \infty & \infty \\ -10 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$



Fixed Point Comp. with Widening

2. Normalize the resulting state:

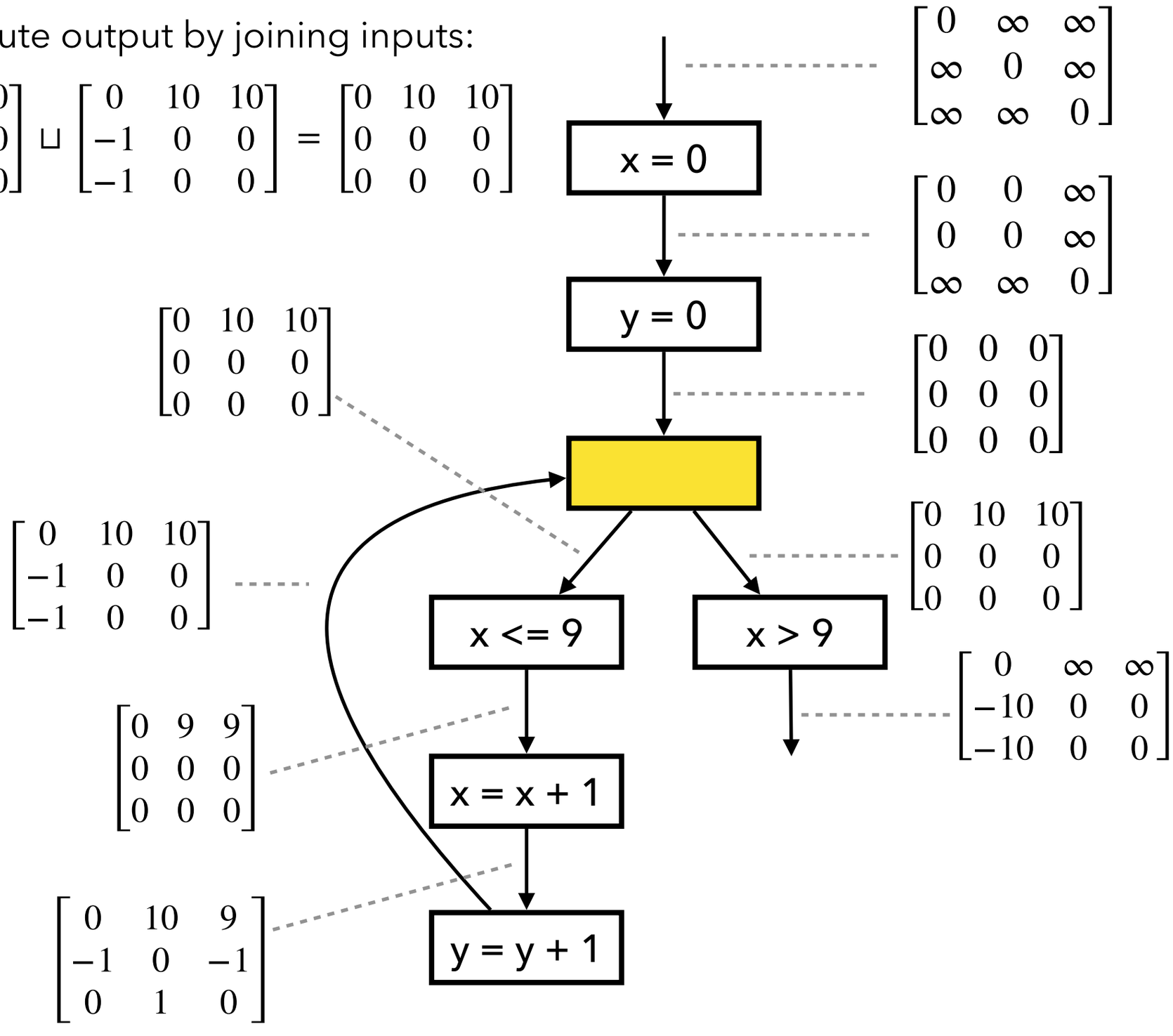
$$\begin{bmatrix} 0 & \infty & \infty \\ -10 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \rightarrow \begin{bmatrix} 0 & \infty & \infty \\ -10 & 0 & 0 \\ -10 & 0 & 0 \end{bmatrix}$$



Fixed Point Comp. with Narrowing

1. Compute output by joining inputs:

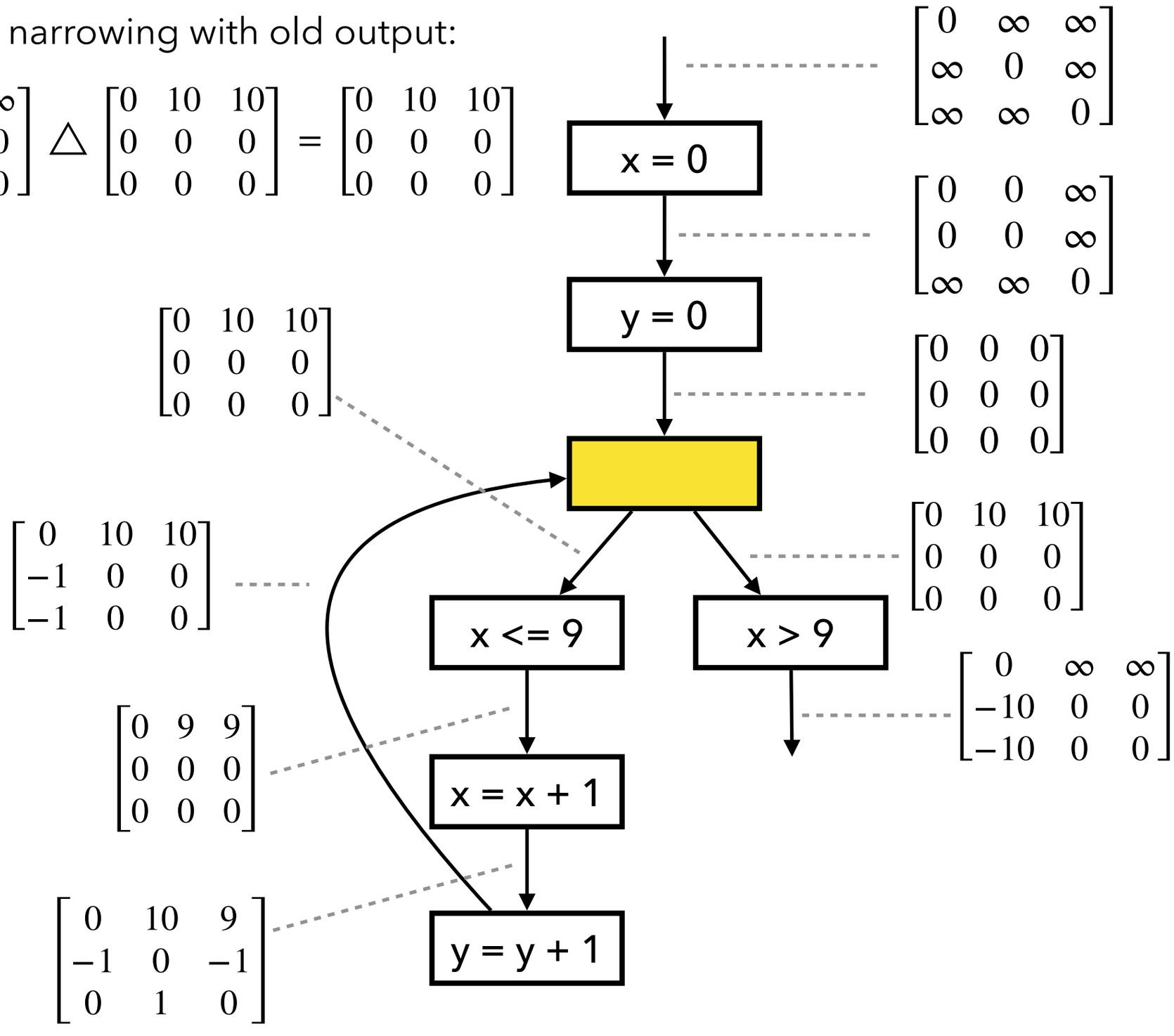
$$\begin{bmatrix}0&0&0\\0&0&0\\0&0&0\end{bmatrix} \sqcup \begin{bmatrix}0&10&10\\-1&0&0\\-1&0&0\end{bmatrix} = \begin{bmatrix}0&10&10\\0&0&0\\0&0&0\end{bmatrix}$$



Fixed Point Comp. with Narrowing

2. Apply narrowing with old output:

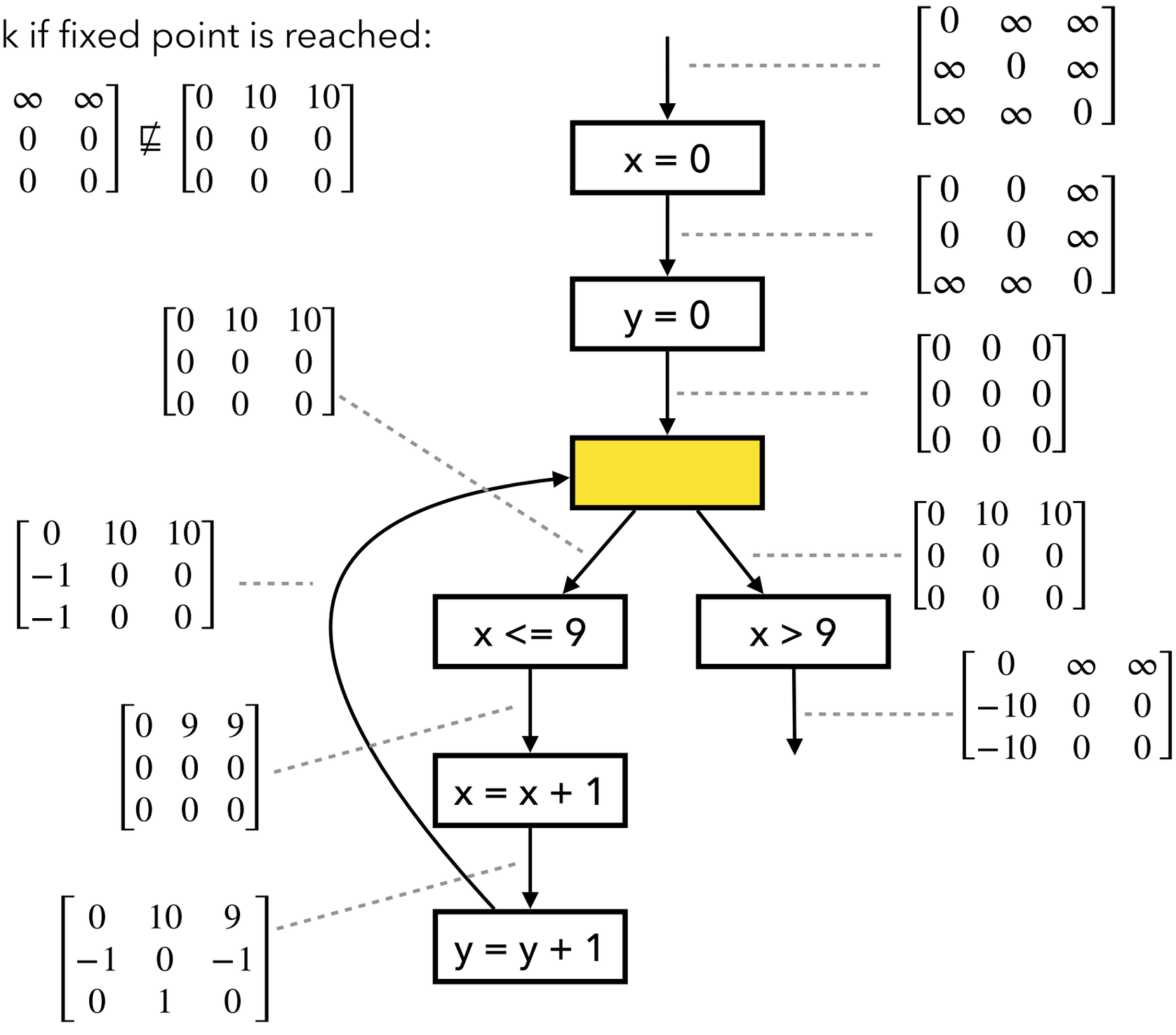
$$\begin{bmatrix} 0 & \infty & \infty \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \triangle \begin{bmatrix} 0 & 10 & 10 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 10 & 10 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$



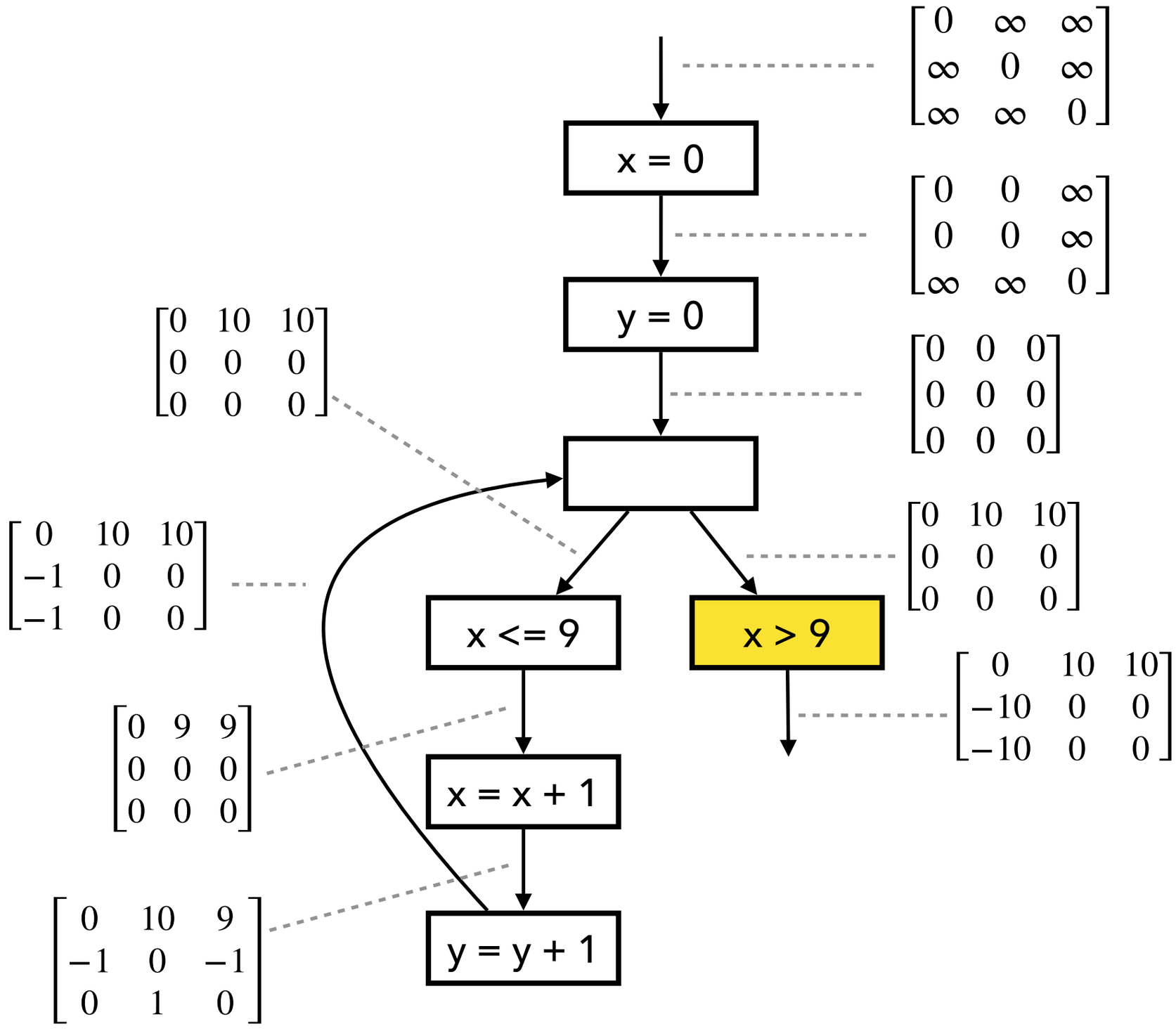
Fixed Point Comp. with Narrowing

3. Check if fixed point is reached:

$$\begin{bmatrix} 0 & \infty & \infty \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \not\subseteq \begin{bmatrix} 0 & 10 & 10 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$



Fixed Point Comp. with Narrowing



Exercise

Describe how the zone analysis works for the following example.

```
// a >= 0, b >= 0
q = 0;
r = a;
while (r >= b) {
   r = r - b;
   q = q + 1;
}
assert(q >= 0);
assert(r >= 0);
```