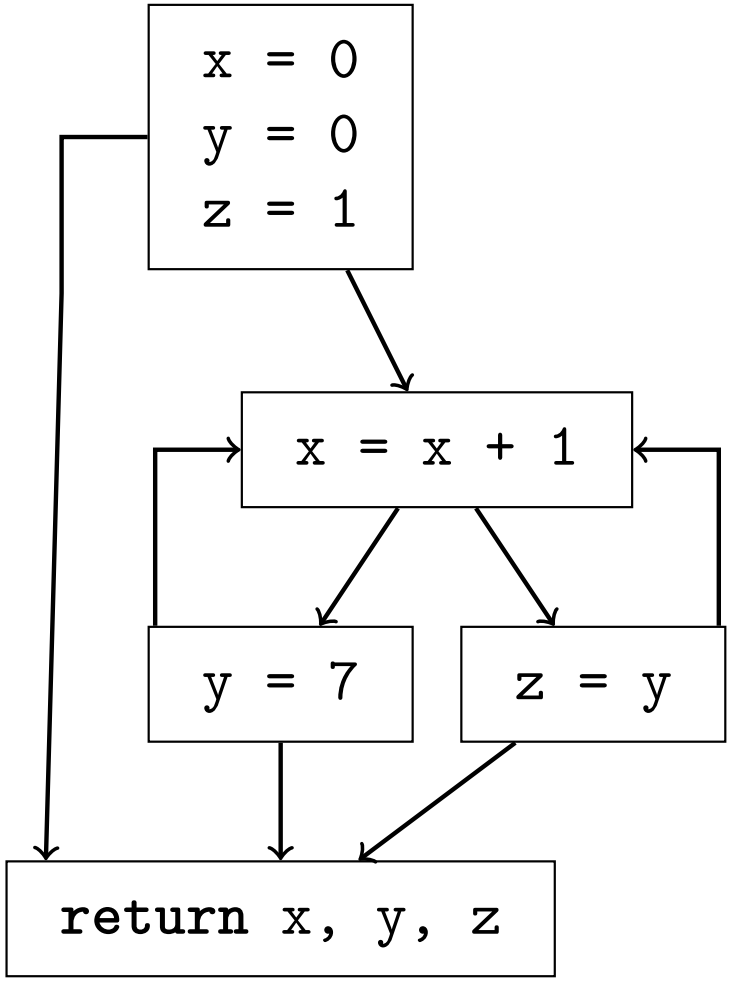
EDA045F: Program Analysis

LECTURE 2: DATAFLOW BONUS EXAMPLE

Christoph Reichenbach

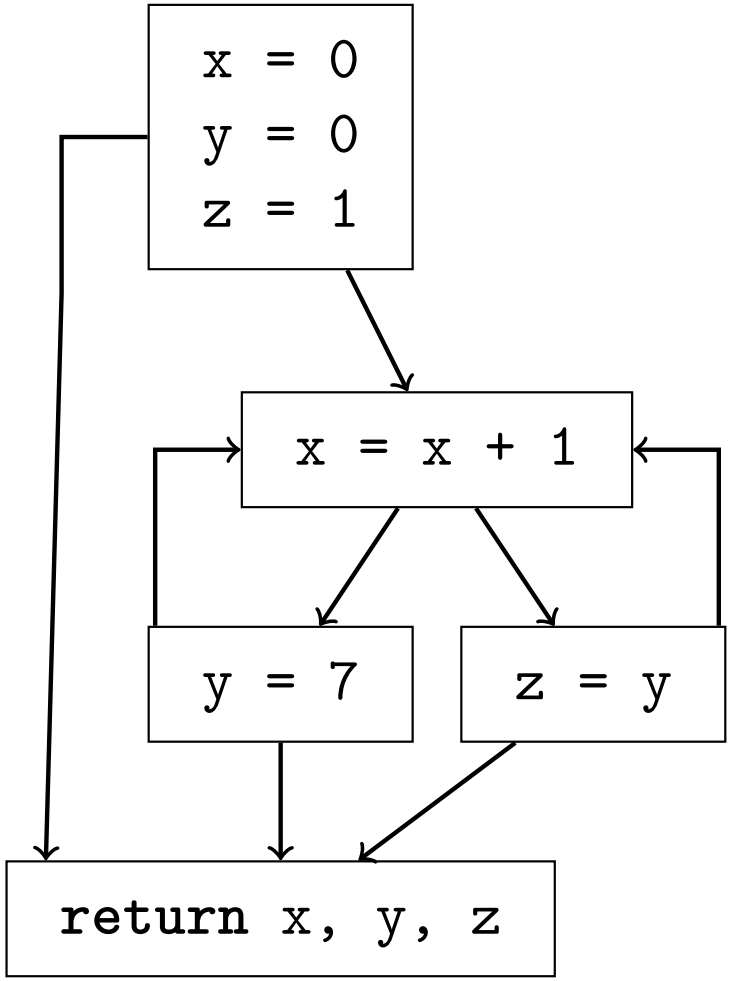
Example: Reaching Definitions

```
x = 0
y = 0
z = 1

while (x < 5) {
  x = x + 1
  if (x >= 2) {
    y = 7
  } else {
    z = y
} }

return x, y, z
```



Example: Reaching Definitions

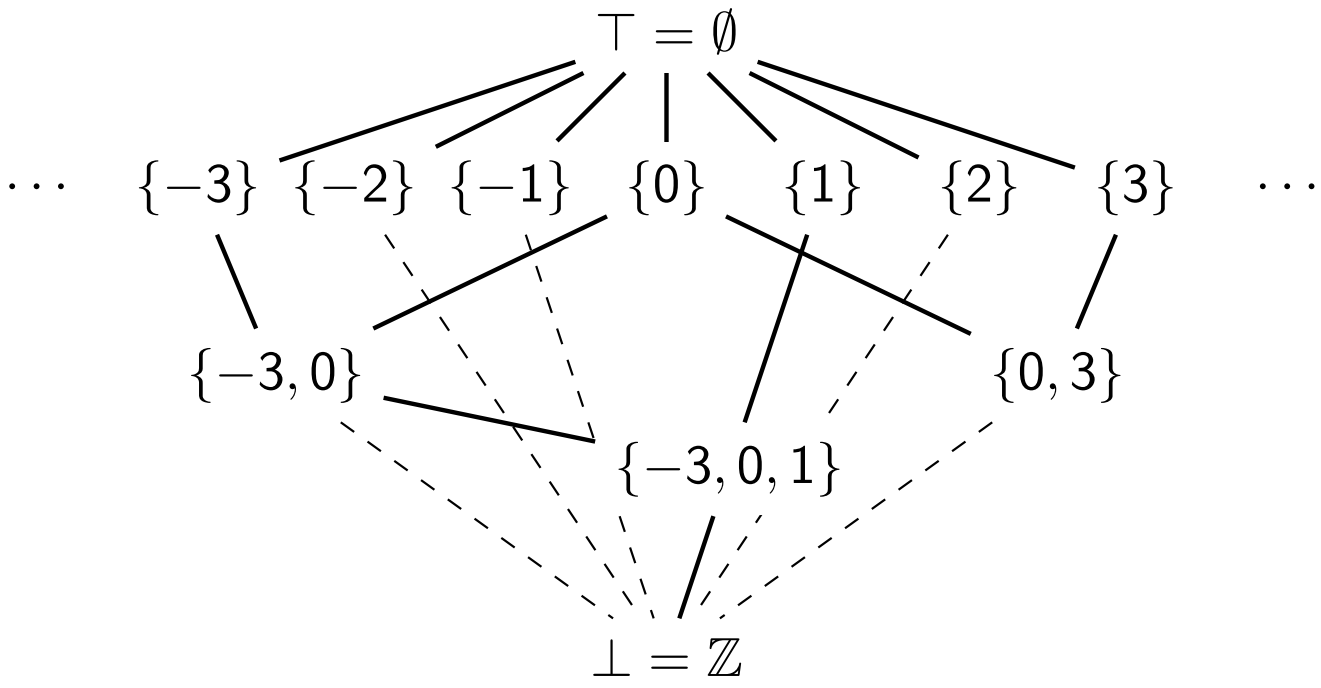
```
x = 0
y = 0
z = 1

while (x < 5) {
  x = x + 1
  if (x >= 2) {
    y = 7
  } else {
    z = y
} }

return x, y, z
```



Reaching Definitions: What values are possible?

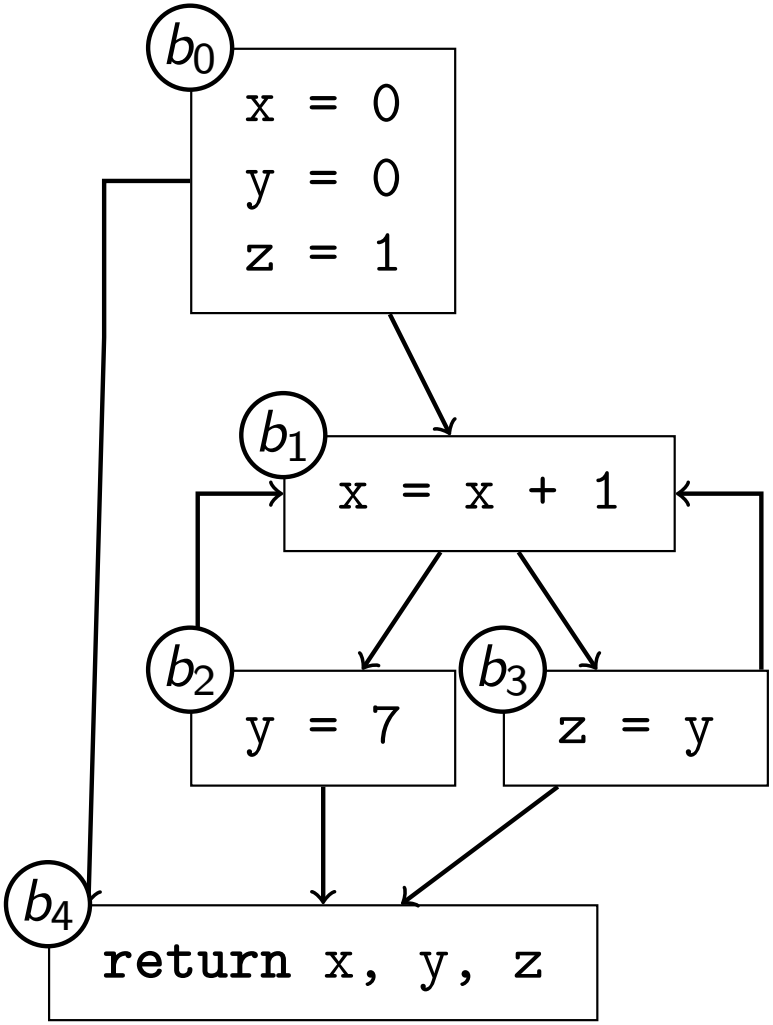
Example: Reaching Definitions

Designing our abstract domain:



- Capture sets of up to 3 possible numbers
- $\top$: $\emptyset$ (no possible numbers seen yet)
- $\bot$: More than 3 possible numbers
- Infinitely many elements, but finite height!

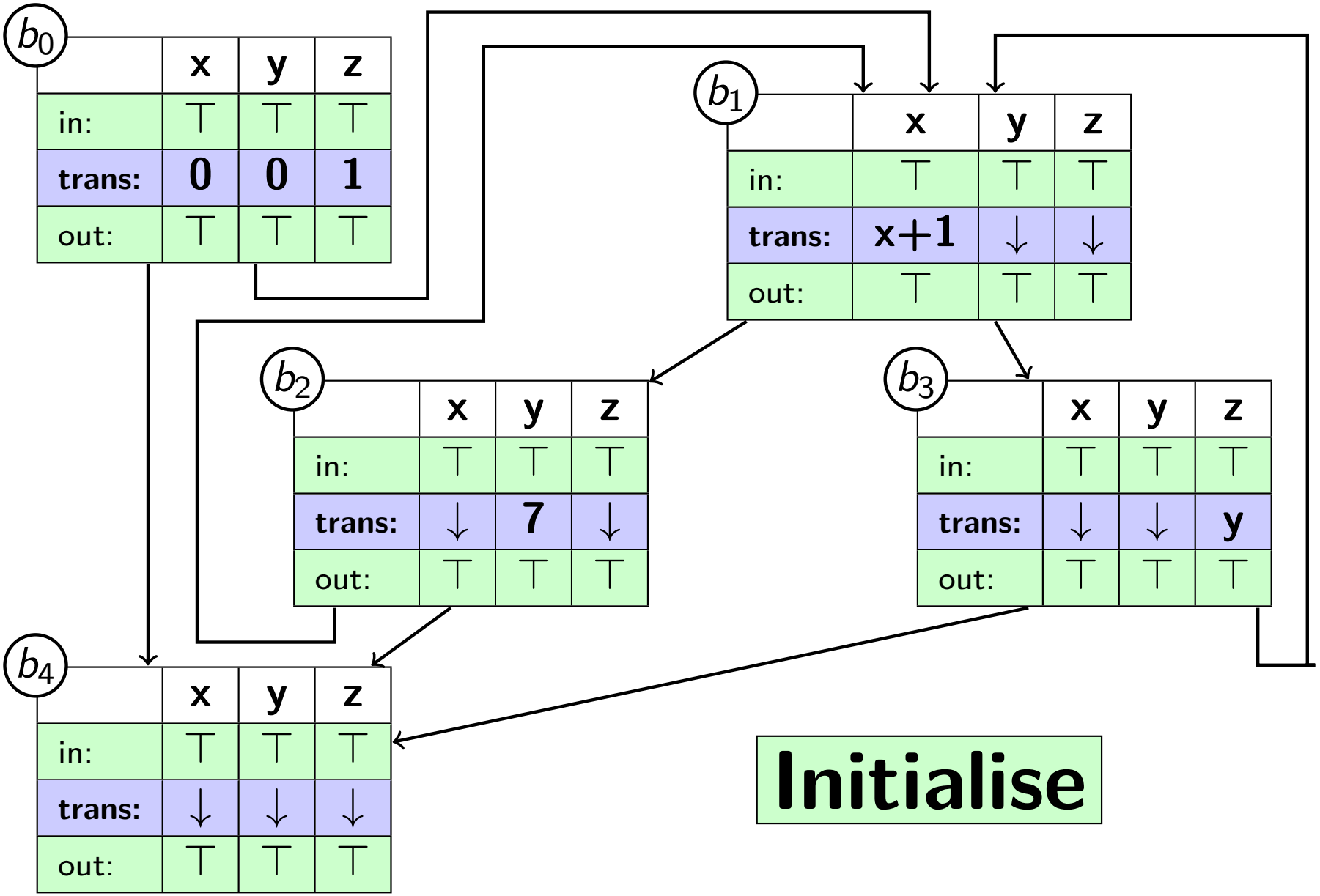
Example: Control-Flow Graph



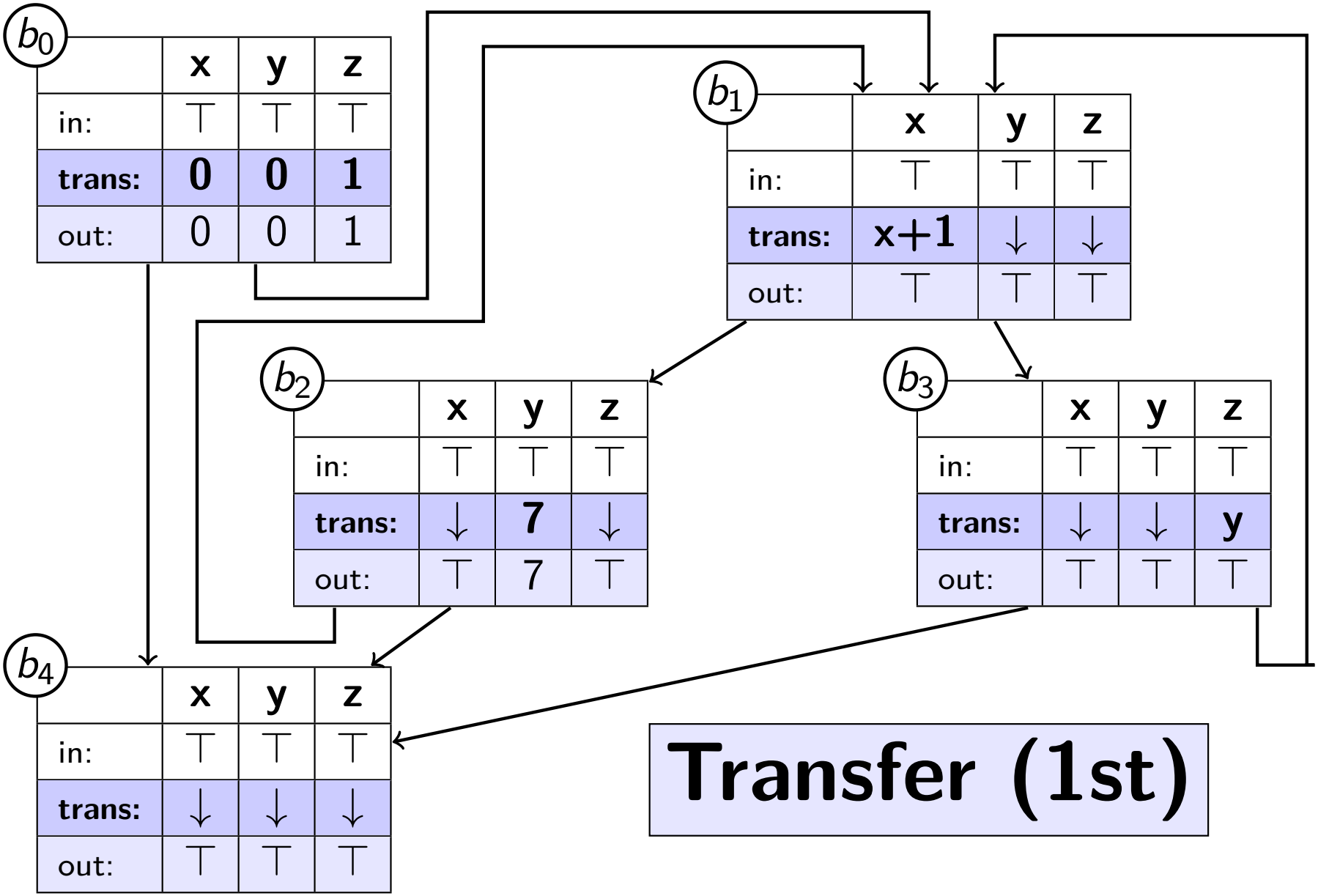
b	inputs	$trans_b$		
		x	y	z
b_0	$\emptyset$	0	0	1
b_1	$\{b_0, b_2, b_3\}$	$x+1$	y	z
b_2	$\{b_1\}$	x	7	z
b_3	$\{b_1\}$	x	y	y
b_4	$\{b_0, b_2, b_3\}$	x	y	z

$$merge_b = \bigcup_{s \in inputs_b} s$$

Example: Computing the Fixpoint



Example: Computing the Fixpoint



Transfer (1st)

Example: Computing the Fixpoint

b_0

	x	y	z
in:	$\top$	$\top$	$\top$
trans:	**0**	**0**	**1**
out:	0	0	1

b_1

	x	y	z
in:	0	0,7	1
trans:	**x+1**	$\downarrow$	$\downarrow$
out:	$\top$	$\top$	$\top$

b_2

	x	y	z
in:	$\top$	$\top$	$\top$
trans:	$\downarrow$	**7**	$\downarrow$
out:	$\top$	7	$\top$

b_3

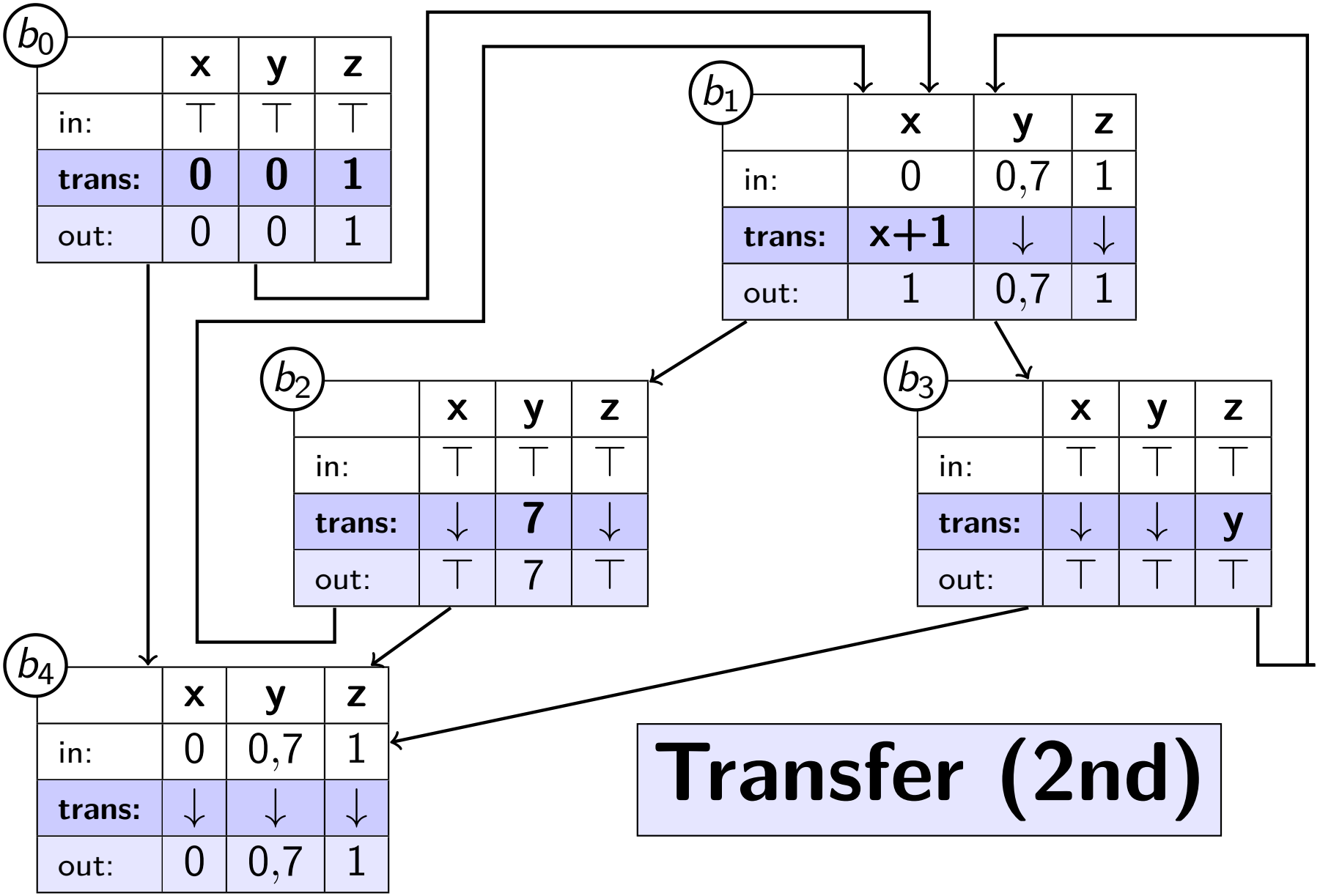
	x	y	z
in:	$\top$	$\top$	$\top$
trans:	$\downarrow$	$\downarrow$	**y**
out:	$\top$	$\top$	$\top$

b_4

	x	y	z
in:	0	0,7	1
trans:	$\downarrow$	$\downarrow$	$\downarrow$
out:	$\top$	$\top$	$\top$

Join (1st)

Example: Computing the Fixpoint



Transfer (2nd)

Example: Computing the Fixpoint

b_0

	x	y	z
in:	$\top$	$\top$	$\top$
trans:	**0**	**0**	**1**
out:	0	0	1

b_1

	x	y	z
in:	0	0,7	1
trans:	**x+1**	$\downarrow$	$\downarrow$
out:	1	0,7	1

b_2

	x	y	z
in:	1	0,7	1
trans:	$\downarrow$	**7**	$\downarrow$
out:	$\top$	7	$\top$

b_3

	x	y	z
in:	1	0,7	1
trans:	$\downarrow$	$\downarrow$	**y**
out:	$\top$	$\top$	$\top$

b_4

	x	y	z
in:	0	0,7	1
trans:	$\downarrow$	$\downarrow$	$\downarrow$
out:	0	0,7	1

Join (2nd)

Example: Computing the Fixpoint

b_0

	x	y	z
in:	$\top$	$\top$	$\top$
trans:	**0**	**0**	**1**
out:	0	0	1

b_1

	x	y	z
in:	0	0,7	1
trans:	**x+1**	$\downarrow$	$\downarrow$
out:	1	0,7	1

b_2

	x	y	z
in:	1	0,7	1
trans:	$\downarrow$	**7**	$\downarrow$
out:	1	7	1

b_3

	x	y	z
in:	1	0,7	1
trans:	$\downarrow$	$\downarrow$	**y**
out:	1	0,7	0,7

b_4

	x	y	z
in:	0	0,7	1
trans:	$\downarrow$	$\downarrow$	$\downarrow$
out:	0	0,7	1

Transfer (3rd)

Example: Computing the Fixpoint

b_0

	x	y	z
in:	$\top$	$\top$	$\top$
trans:	**0**	**0**	**1**
out:	0	0	1

b_1

	x	y	z
in:	0,1	0,7	0,1,7
trans:	**x+1**	$\downarrow$	$\downarrow$
out:	1	0,7	1

b_2

	x	y	z
in:	1	0,7	1
trans:	$\downarrow$	**7**	$\downarrow$
out:	1	7	1

b_3

	x	y	z
in:	1	0,7	1
trans:	$\downarrow$	$\downarrow$	**y**
out:	1	0,7	0,7

b_4

	x	y	z
in:	0,1	0,7	0,1,7
trans:	$\downarrow$	$\downarrow$	$\downarrow$
out:	0	0,7	1

Join (3rd)

Example: Computing the Fixpoint

b_0

	x	y	z
in:	$\top$	$\top$	$\top$
trans:	**0**	**0**	**1**
out:	0	0	1

b_1

	x	y	z
in:	0,1	0,7	0,1,7
trans:	**x+1**	$\downarrow$	$\downarrow$
out:	1,2	0,7	0,1,7

b_2

	x	y	z
in:	1	0,7	1
trans:	$\downarrow$	**7**	$\downarrow$
out:	1	7	1

b_3

	x	y	z
in:	1	0,7	1
trans:	$\downarrow$	$\downarrow$	**y**
out:	1	0,7	0,7

b_4

	x	y	z
in:	0,1	0,7	0,1,7
trans:	$\downarrow$	$\downarrow$	$\downarrow$
out:	0,1	0,7	0,1,7

Transfer (4th)

Example: Computing the Fixpoint

b_0

	x	y	z
in:	$\top$	$\top$	$\top$
trans:	**0**	**0**	**1**
out:	0	0	1

b_1

	x	y	z
in:	0,1	0,7	0,1,7
trans:	**x+1**	$\downarrow$	$\downarrow$
out:	1,2	0,7	0,1,7

b_2

	x	y	z
in:	1,2	0,7	0,1,7
trans:	$\downarrow$	**7**	$\downarrow$
out:	1	7	1

b_3

	x	y	z
in:	1,2	0,7	0,1,7
trans:	$\downarrow$	$\downarrow$	**y**
out:	1	0,7	0,7

b_4

	x	y	z
in:	0,1	0,7	0,1,7
trans:	$\downarrow$	$\downarrow$	$\downarrow$
out:	0,1	0,7	0,1,7

Join (4th)

Example: Computing the Fixpoint

b_0

	x	y	z
in:	$\top$	$\top$	$\top$
trans:	**0**	**0**	**1**
out:	0	0	1

b_1

	x	y	z
in:	0,1	0,7	0,1,7
trans:	**x+1**	$\downarrow$	$\downarrow$
out:	1,2	0,7	0,1,7

b_2

	x	y	z
in:	1,2	0,7	0,1,7
trans:	$\downarrow$	**7**	$\downarrow$
out:	1,2	7	0,1,7

b_3

	x	y	z
in:	1,2	0,7	0,1,7
trans:	$\downarrow$	$\downarrow$	**y**
out:	1,2	0,7	0,7

b_4

	x	y	z
in:	0,1	0,7	0,1,7
trans:	$\downarrow$	$\downarrow$	$\downarrow$
out:	0,1	0,7	0,1,7

Transfer (5th)

Example: Computing the Fixpoint

b_0

	x	y	z
in:	$\top$	$\top$	$\top$
trans:	**0**	**0**	**1**
out:	0	0	1

b_1

	x	y	z
in:	0,1,2	0,7	0,1,7
trans:	**x+1**	$\downarrow$	$\downarrow$
out:	1,2	0,7	0,1,7

b_2

	x	y	z
in:	1,2	0,7	0,1,7
trans:	$\downarrow$	**7**	$\downarrow$
out:	1,2	7	0,1,7

b_3

	x	y	z
in:	1,2	0,7	0,1,7
trans:	$\downarrow$	$\downarrow$	**y**
out:	1,2	0,7	0,7

b_4

	x	y	z
in:	0,1,2	0,7	0,1,7
trans:	$\downarrow$	$\downarrow$	$\downarrow$
out:	0,1	0,7	0,1,7

Join (5th)

Example: Computing the Fixpoint

b_0

	x	y	z
in:	$\top$	$\top$	$\top$
trans:	**0**	**0**	**1**
out:	0	0	1

b_1

	x	y	z
in:	0,1,2	0,7	0,1,7
trans:	**x+1**	$\downarrow$	$\downarrow$
out:	1,2,3	0,7	0,1,7

b_2

	x	y	z
in:	1,2	0,7	0,1,7
trans:	$\downarrow$	**7**	$\downarrow$
out:	1,2	7	0,1,7

b_3

	x	y	z
in:	1,2	0,7	0,1,7
trans:	$\downarrow$	$\downarrow$	**y**
out:	1,2	0,7	0,7

b_4

	x	y	z
in:	0,1,2	0,7	0,1,7
trans:	$\downarrow$	$\downarrow$	$\downarrow$
out:	0,1,2	0,7	0,1,7

Transfer (6th)

Example: Computing the Fixpoint

b_0

	x	y	z
in:	$\top$	$\top$	$\top$
trans:	**0**	**0**	**1**
out:	0	0	1

b_1

	x	y	z
in:	0,1,2	0,7	0,1,7
trans:	**x+1**	$\downarrow$	$\downarrow$
out:	1,2,3	0,7	0,1,7

b_2

	x	y	z
in:	1,2,3	0,7	0,1,7
trans:	$\downarrow$	**7**	$\downarrow$
out:	1,2	7	0,1,7

b_3

	x	y	z
in:	1,2,3	0,7	0,1,7
trans:	$\downarrow$	$\downarrow$	**y**
out:	1,2	0,7	0,7

b_4

	x	y	z
in:	0,1,2	0,7	0,1,7
trans:	$\downarrow$	$\downarrow$	$\downarrow$
out:	0,1,2	0,7	0,1,7

Join (6th)

Example: Computing the Fixpoint

b_0

	x	y	z
in:	$\top$	$\top$	$\top$
trans:	**0**	**0**	**1**
out:	0	0	1

b_1

	x	y	z
in:	0,1,2	0,7	0,1,7
trans:	**x+1**	$\downarrow$	$\downarrow$
out:	1,2,3	0,7	0,1,7

b_2

	x	y	z
in:	1,2,3	0,7	0,1,7
trans:	$\downarrow$	**7**	$\downarrow$
out:	1,2,3	7	0,1,7

b_3

	x	y	z
in:	1,2,3	0,7	0,1,7
trans:	$\downarrow$	$\downarrow$	**y**
out:	1,2,3	0,7	0,7

b_4

	x	y	z
in:	0,1,2	0,7	0,1,7
trans:	$\downarrow$	$\downarrow$	$\downarrow$
out:	0,1,2	0,7	0,1,7

Transfer (7th)

Example: Computing the Fixpoint

b_0

	x	y	z
in:	$\top$	$\top$	$\top$
trans:	**0**	**0**	**1**
out:	0	0	1

b_1

	x	y	z
in:	$\bot$	0,7	0,1,7
trans:	**x+1**	$\downarrow$	$\downarrow$
out:	1,2,3	0,7	0,1,7

b_2

	x	y	z
in:	1,2,3	0,7	0,1,7
trans:	$\downarrow$	**7**	$\downarrow$
out:	1,2,3	7	0,1,7

b_3

	x	y	z
in:	1,2,3	0,7	0,1,7
trans:	$\downarrow$	$\downarrow$	**y**
out:	1,2,3	0,7	0,7

b_4

	x	y	z
in:	$\bot$	0,7	0,1,7
trans:	$\downarrow$	$\downarrow$	$\downarrow$
out:	0,1,2	0,7	0,1,7

Join (7th)

Example: Computing the Fixpoint

b_0

	x	y	z
in:	$\top$	$\top$	$\top$
trans:	**0**	**0**	**1**
out:	0	0	1

b_1

	x	y	z
in:	$\bot$	0,7	0,1,7
trans:	**x+1**	$\downarrow$	$\downarrow$
out:	$\bot$	0,7	0,1,7

b_2

	x	y	z
in:	1,2,3	0,7	0,1,7
trans:	$\downarrow$	**7**	$\downarrow$
out:	1,2,3	7	0,1,7

b_3

	x	y	z
in:	1,2,3	0,7	0,1,7
trans:	$\downarrow$	$\downarrow$	**y**
out:	1,2,3	0,7	0,7

b_4

	x	y	z
in:	$\bot$	0,7	0,1,7
trans:	$\downarrow$	$\downarrow$	$\downarrow$
out:	$\bot$	0,7	0,1,7

Transfer (8th)

Example: Computing the Fixpoint

b_0

	x	y	z
in:	$\top$	$\top$	$\top$
trans:	**0**	**0**	**1**
out:	0	0	1

b_1

	x	y	z
in:	$\bot$	0,7	0,1,7
trans:	**x+1**	$\downarrow$	$\downarrow$
out:	$\bot$	0,7	0,1,7

b_2

	x	y	z
in:	$\bot$	0,7	0,1,7
trans:	$\downarrow$	**7**	$\downarrow$
out:	1,2,3	7	0,1,7

b_3

	x	y	z
in:	$\bot$	0,7	0,1,7
trans:	$\downarrow$	$\downarrow$	**y**
out:	1,2,3	0,7	0,7

b_4

	x	y	z
in:	$\bot$	0,7	0,1,7
trans:	$\downarrow$	$\downarrow$	$\downarrow$
out:	$\bot$	0,7	0,1,7

Join (8th)

Example: Computing the Fixpoint

b_0

	x	y	z
in:	$\top$	$\top$	$\top$
trans:	**0**	**0**	**1**
out:	0	0	1

b_1

	x	y	z
in:	$\bot$	0,7	0,1,7
trans:	**x+1**	$\downarrow$	$\downarrow$
out:	$\bot$	0,7	0,1,7

b_2

	x	y	z
in:	$\bot$	0,7	0,1,7
trans:	$\downarrow$	**7**	$\downarrow$
out:	$\bot$	7	0,1,7

b_3

	x	y	z
in:	$\bot$	0,7	0,1,7
trans:	$\downarrow$	$\downarrow$	**y**
out:	$\bot$	0,7	0,7

b_4

	x	y	z
in:	$\bot$	0,7	0,1,7
trans:	$\downarrow$	$\downarrow$	$\downarrow$
out:	$\bot$	0,7	0,1,7

Transfer (9th)

Example: Computing the Fixpoint

b_0

	x	y	z
in:	$\top$	$\top$	$\top$
trans:	**0**	**0**	**1**
out:	0	0	1

b_1

	x	y	z
in:	$\bot$	0,7	0,1,7
trans:	**x+1**	$\downarrow$	$\downarrow$
out:	$\bot$	0,7	0,1,7

b_2

	x	y	z
out:	$\bot$	7	0,1,7

b_3

	x	y	z
	$\bot$	0,7	0,1,7
	$\downarrow$	$\downarrow$	**y**
out:	$\bot$	0,7	0,7

Fixpoint reached

b_4

	x	y	z
in:	$\bot$	0,7	0,1,7
trans:	$\downarrow$	$\downarrow$	$\downarrow$
out:	$\bot$	0,7	0,1,7

Join (9th)

Example: Conclusion

```
x = 0
y = 0
z = 1

while (x < 5) {
  x = x + 1
  if (x >= 2) {
    y = 7
  } else {
    z = y
} }

return x, y, z
```

- Reached fixpoint after 9 iterations
- Return values:

  x : $\perp$ (unknown/any)
  y : 0 or 7
  z : 0 or 1 or 7
- Conservative approximation of reality
- Once x reached more than 3 values, algorithm gave up and went to $\perp$

Alternatives are possible:

- Faster $x + 1$: always $\perp$
- Bigger/smaller domain