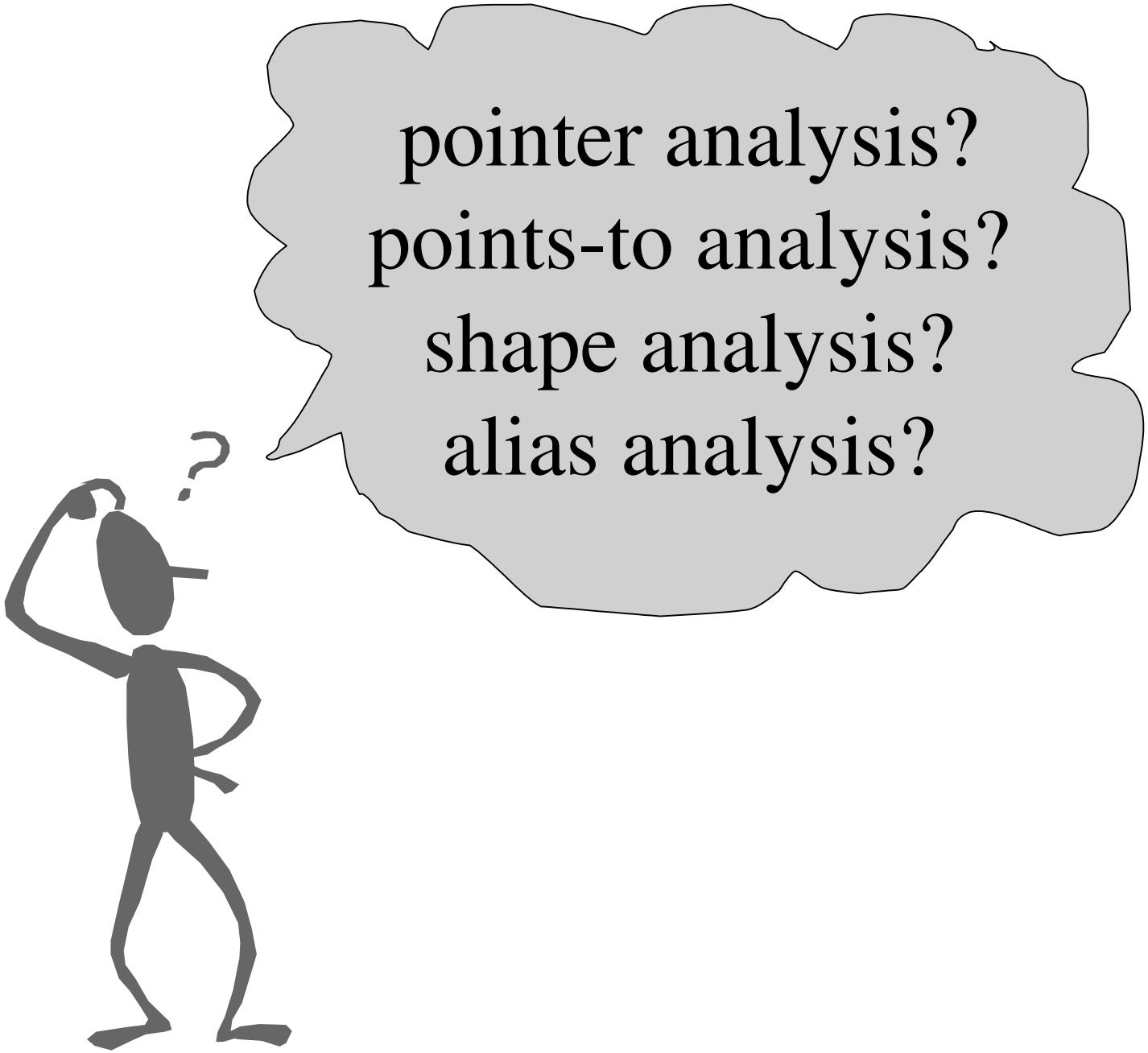
Parametric Shape Analysis via 3-Valued Logic

Mooly Sagiv
Thomas Reps
Reinhard Wilhelm


pointer analysis?
points-to analysis?
shape analysis?
alias analysis?

The Shape-Analysis Problem

For every program point,
compute a finite characterization
of the possible “shapes” of the
heap-allocated data structures.

The Shape-Analysis Problem

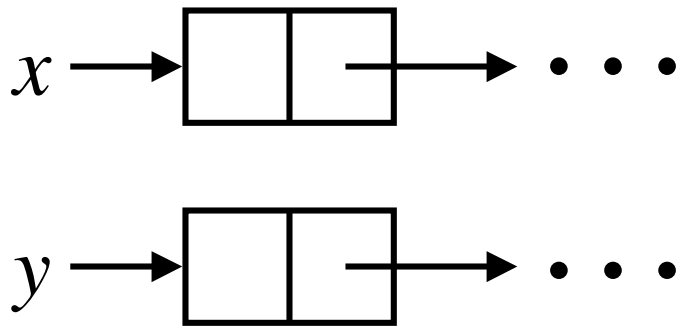
For every program point,
compute a finite characterization
of the possible "shapes" of the
heap-allocated data structures.

The Shape-Analysis Problem

For every program point,
compute a finite characterization
of the possible "shapes" of the
heap-allocated data structures.

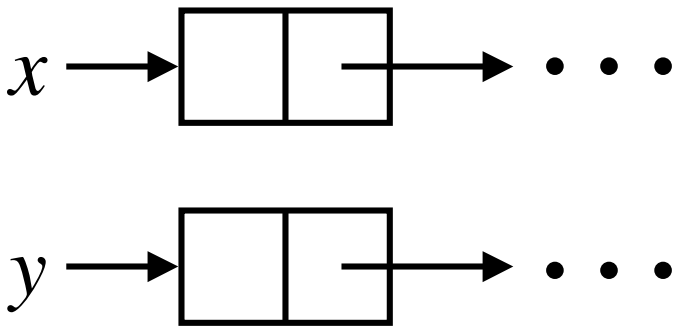
Formalizing “. . .”

Informal:

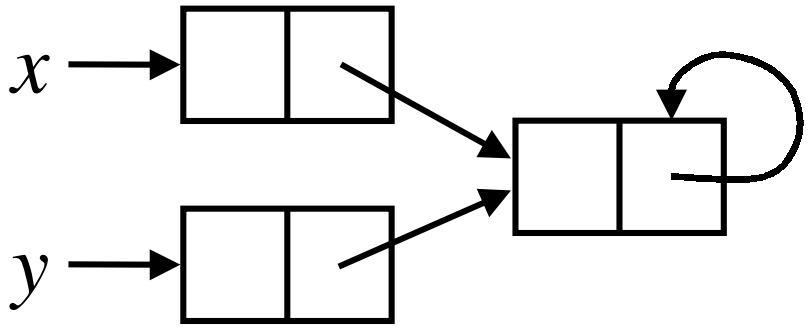


Formalizing “. . .”

Informal:

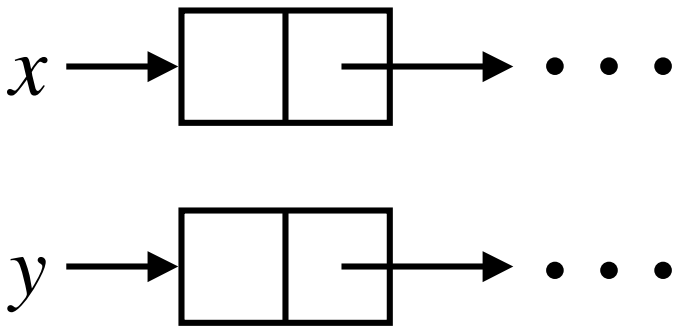


Formal:

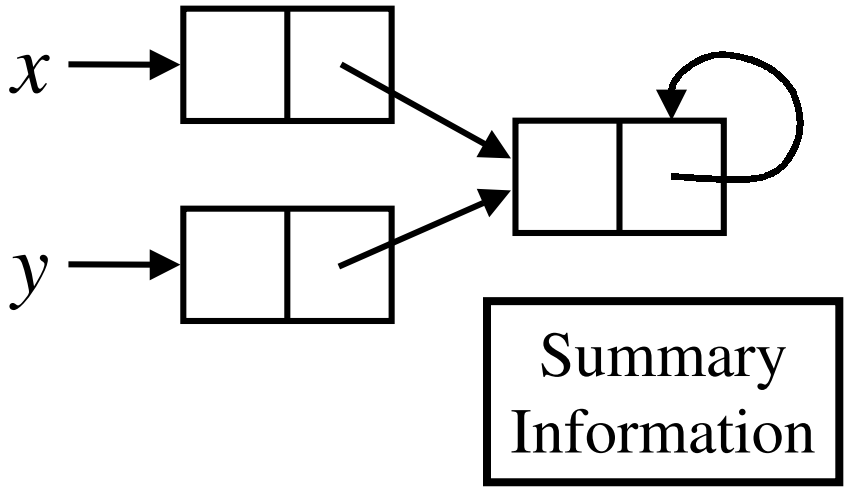


Formalizing “. . .”

Informal:

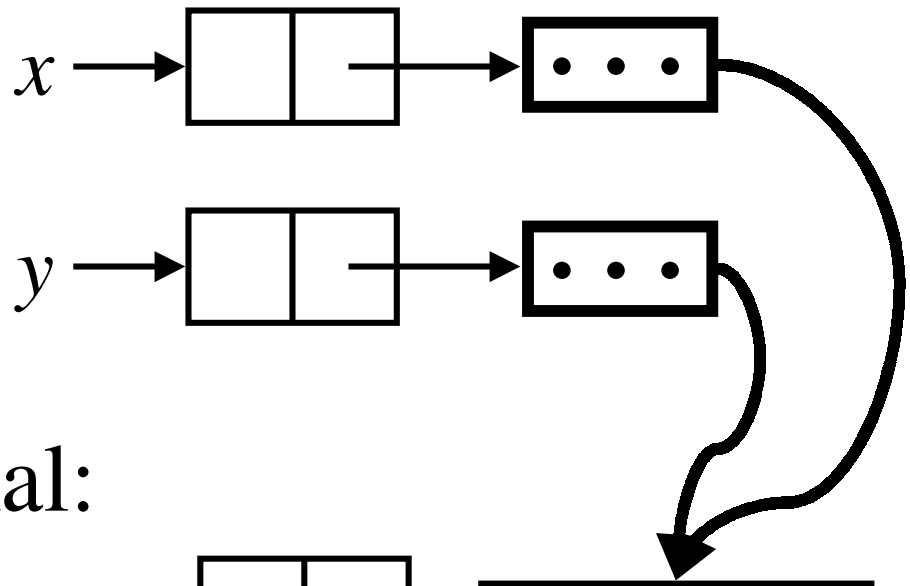


Formal:

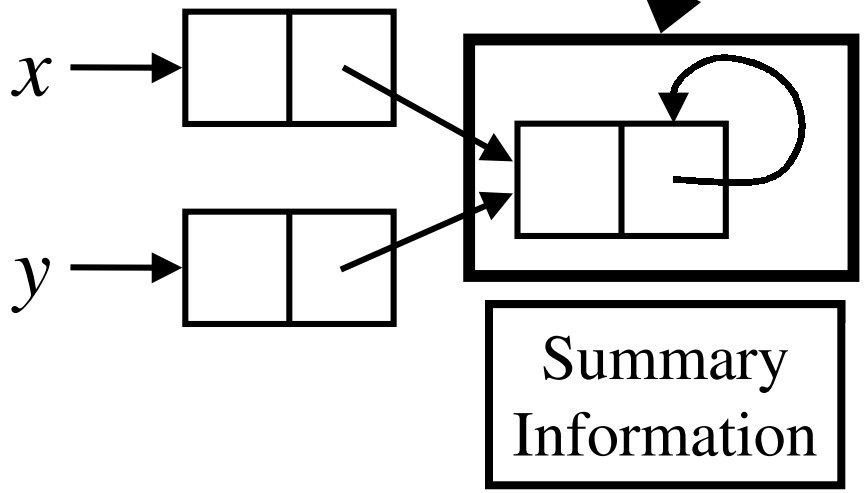


Formalizing “. . .”

Informal:



Formal:



Why Shape Analysis?

- Capture storage invariants
  - *x* points to an acyclic list, cyclic list, tree, dag, etc.
- May-alias information
- Identify (absence of) sharing
  - *x* and *y* point to structures that do not share cells
- "Dynamization" of static structure-description formalisms
  - e.g., ADDS annotations [Hendren 94]

What's New?

- Parametric framework for a class of shape-analysis algorithms
- "Rational reconstruction" of a number of previous shape-analysis methods
  - [Jones & Muchnick 81]
  - [Chase, Wegman, & Zadeck 90]
  - [Stransky 93]
  - [Assmann & Weinhardt 93]
  - [Pleyvak, Chien, & Karamcheti 93]
  - [Wang 94]
  - [Sagiv, Reps, & Wilhelm 96, 98]
- New shape-analysis methods
- General abstraction principle $\Rightarrow$ Much simpler proofs
- Basis for a tool that generates shape-analysis algorithms

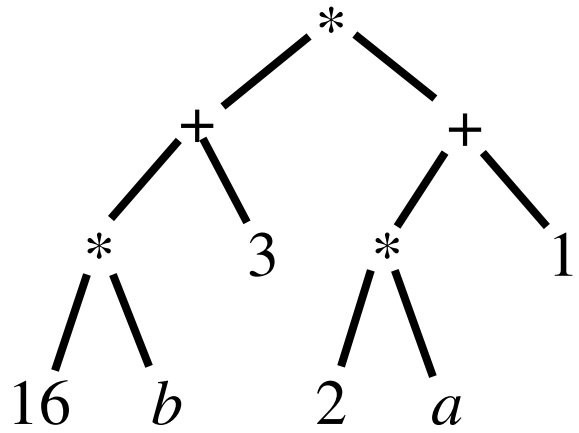
Abstract Interpretation

Abstract Interpretation

$f(a,b) = (16 * b + 3) * (2 * a + 1)$

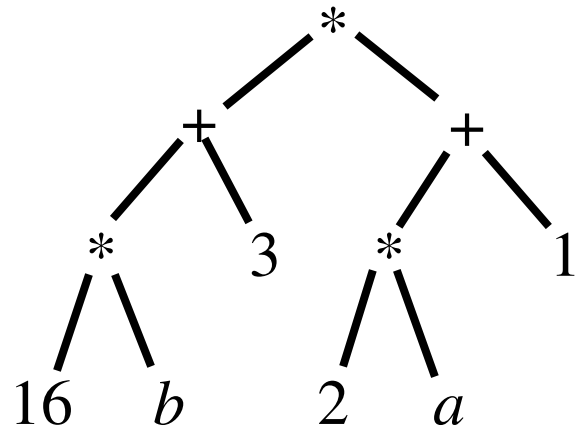
Abstract Interpretation

$f(a,b) = (16 * b + 3) * (2 * a + 1)$



Abstract Interpretation

$f(a,b) = (16 * b + 3) * (2 * a + 1)$

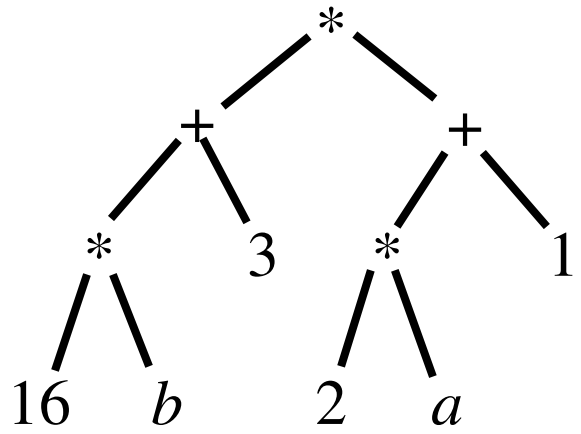


+	0	1	2	3	…
0	0	1	2	3	…
1	1	2	3	4	…
2	2	3	4	5	…
3	3	4	5	6	…
⋮	⋮	⋮	⋮	⋮	

*	0	1	2	3	…
0	0	0	0	0	…
1	0	1	2	3	…
2	0	2	4	6	…
3	0	3	6	9	…
⋮	⋮	⋮	⋮	⋮	

Abstract Interpretation

$f(a,b) = (16 * b + 3) * (2 * a + 1)$

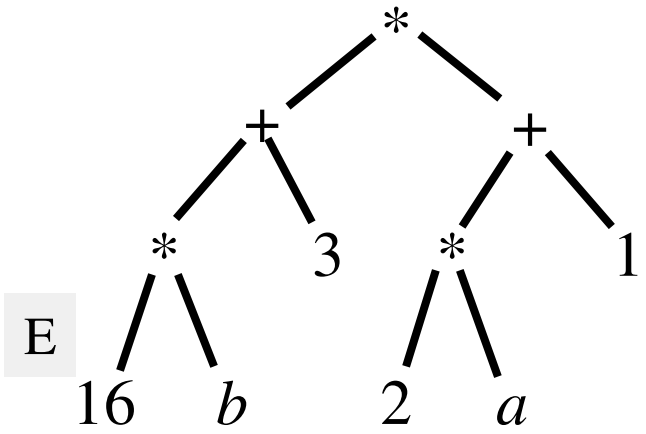


$+'$	?	O	E
?	?	?	?
O	?	E	O
E	?	O	E

$*'$	?	O	E
?	?	?	E
O	?	O	E
E	E	E	E

Abstract Interpretation

$f(a,b) = (16 * b + 3) * (2 * a + 1)$

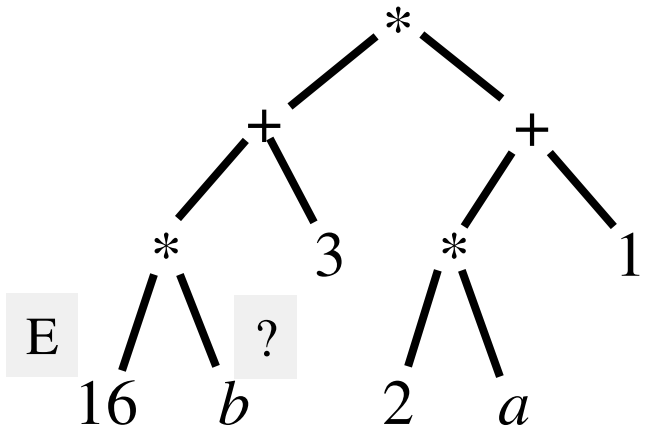


+′	?	O	E
?	?	?	?
O	?	E	O
E	?	O	E

*′	?	O	E
?	?	?	E
O	?	O	E
E	E	E	E

Abstract Interpretation

$f(a,b) = (16 * b + 3) * (2 * a + 1)$

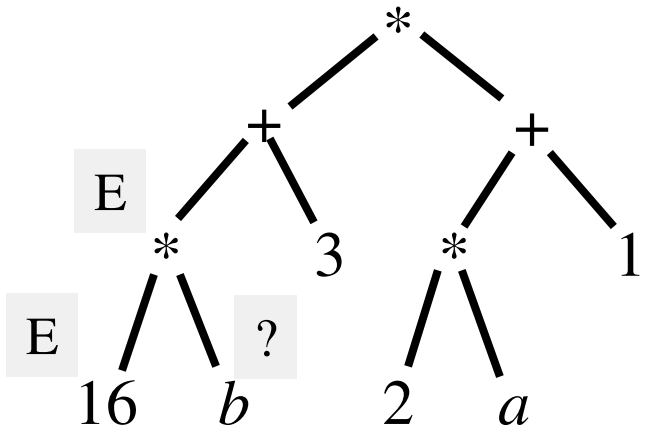


+′	?	O	E
?	?	?	?
O	?	E	O
E	?	O	E

*′	?	O	E
?	?	?	E
O	?	O	E
E	E	E	E

Abstract Interpretation

$f(a,b) = (16 * b + 3) * (2 * a + 1)$

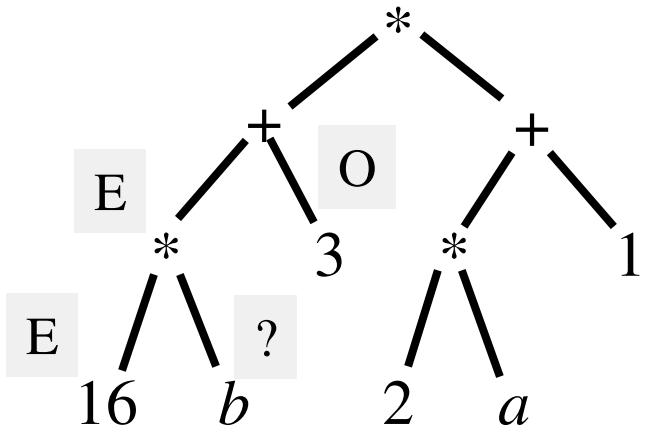


+′	?	O	E
?	?	?	?
O	?	E	O
E	?	O	E

*′	?	O	E
?	?	?	E
O	?	O	E
E	E	E	E

Abstract Interpretation

$f(a,b) = (16 * b + 3) * (2 * a + 1)$

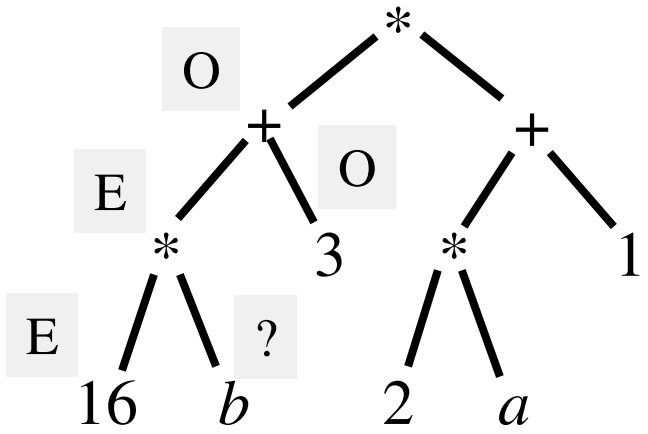


+′	?	O	E
?	?	?	?
O	?	E	O
E	?	O	E

*′	?	O	E
?	?	?	E
O	?	O	E
E	E	E	E

Abstract Interpretation

$f(a,b) = (16 * b + 3) * (2 * a + 1)$

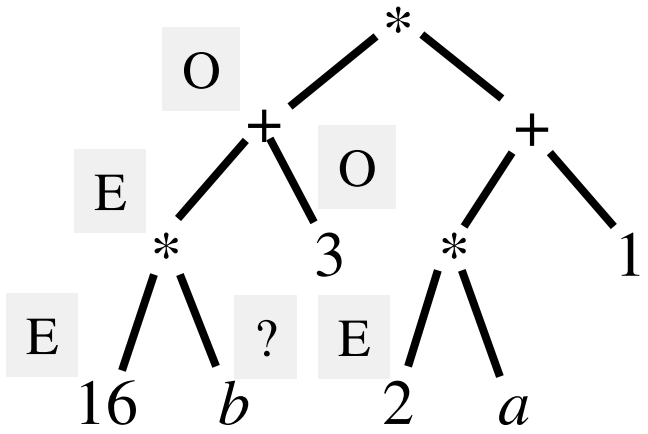


$+'$	?	O	E
?	?	?	?
O	?	E	O
E	?	O	E

$*'$	?	O	E
?	?	?	E
O	?	O	E
E	E	E	E

Abstract Interpretation

$f(a,b) = (16 * b + 3) * (2 * a + 1)$

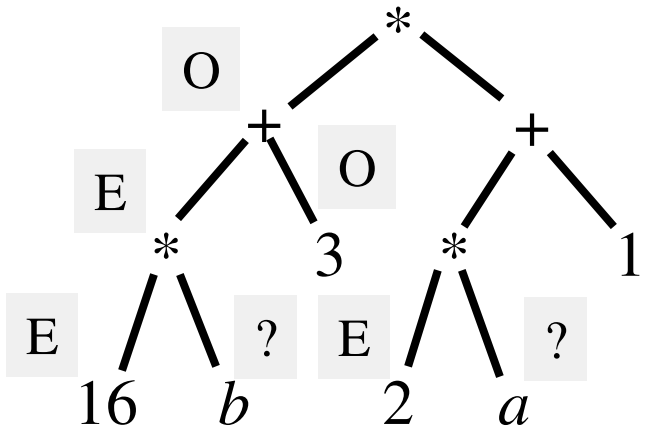


+′	?	O	E
?	?	?	?
O	?	E	O
E	?	O	E

*′	?	O	E
?	?	?	E
O	?	O	E
E	E	E	E

Abstract Interpretation

$f(a,b) = (16 * b + 3) * (2 * a + 1)$

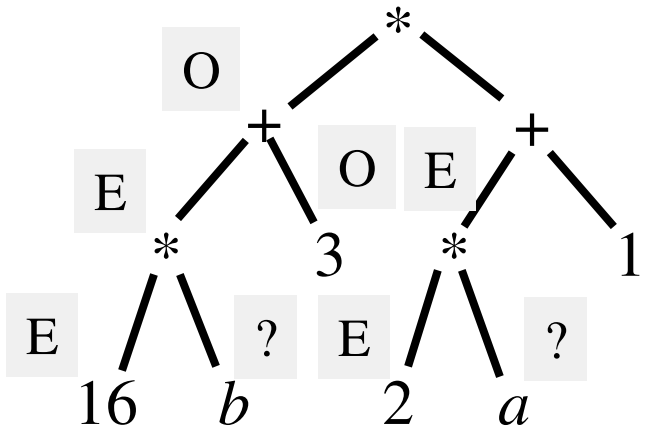


+′	?	O	E
?	?	?	?
O	?	E	O
E	?	O	E

*′	?	O	E
?	?	?	E
O	?	O	E
E	E	E	E

Abstract Interpretation

$f(a,b) = (16 * b + 3) * (2 * a + 1)$

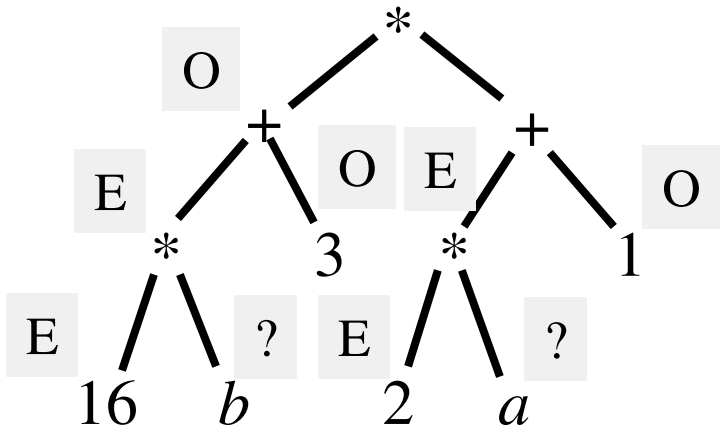


+′	?	O	E
?	?	?	?
O	?	E	O
E	?	O	E

*′	?	O	E
?	?	?	E
O	?	O	E
E	E	E	E

Abstract Interpretation

$f(a,b) = (16 * b + 3) * (2 * a + 1)$

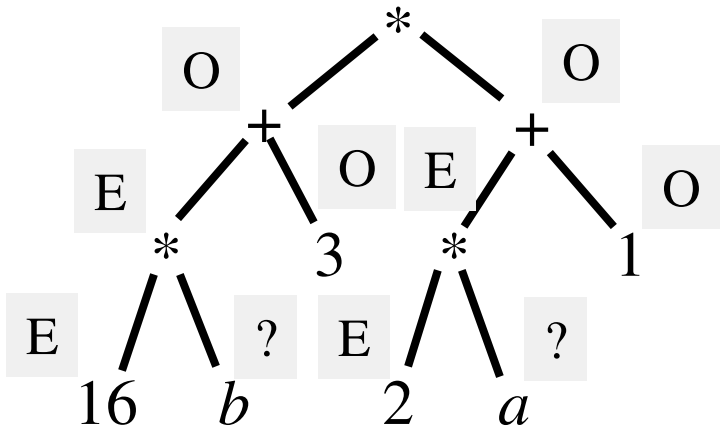


+′	?	O	E
?	?	?	?
O	?	E	O
E	?	O	E

*′	?	O	E
?	?	?	E
O	?	O	E
E	E	E	E

Abstract Interpretation

$f(a,b) = (16 * b + 3) * (2 * a + 1)$

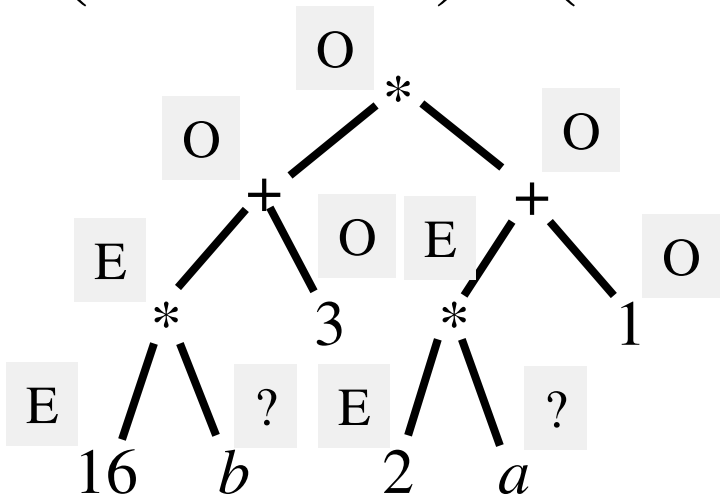


$+'$	?	O	E
?	?	?	?
O	?	E	O
E	?	O	E

$*'$	?	O	E
?	?	?	E
O	?	O	E
E	E	E	E

Abstract Interpretation

$f(a,b) = (16 * b + 3) * (2 * a + 1)$

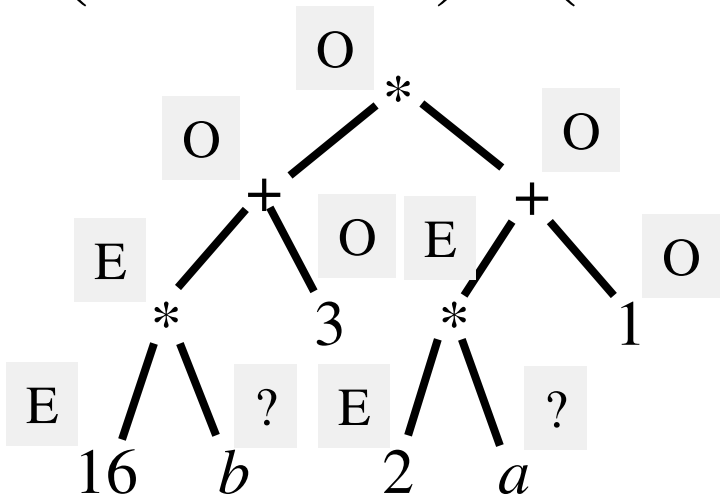


+′	?	O	E
?	?	?	?
O	?	E	O
E	?	O	E

*′	?	O	E
?	?	?	E
O	?	O	E
E	E	E	E

Abstract Interpretation

$f(a,b) = (16 * b + 3) * (2 * a + 1)$

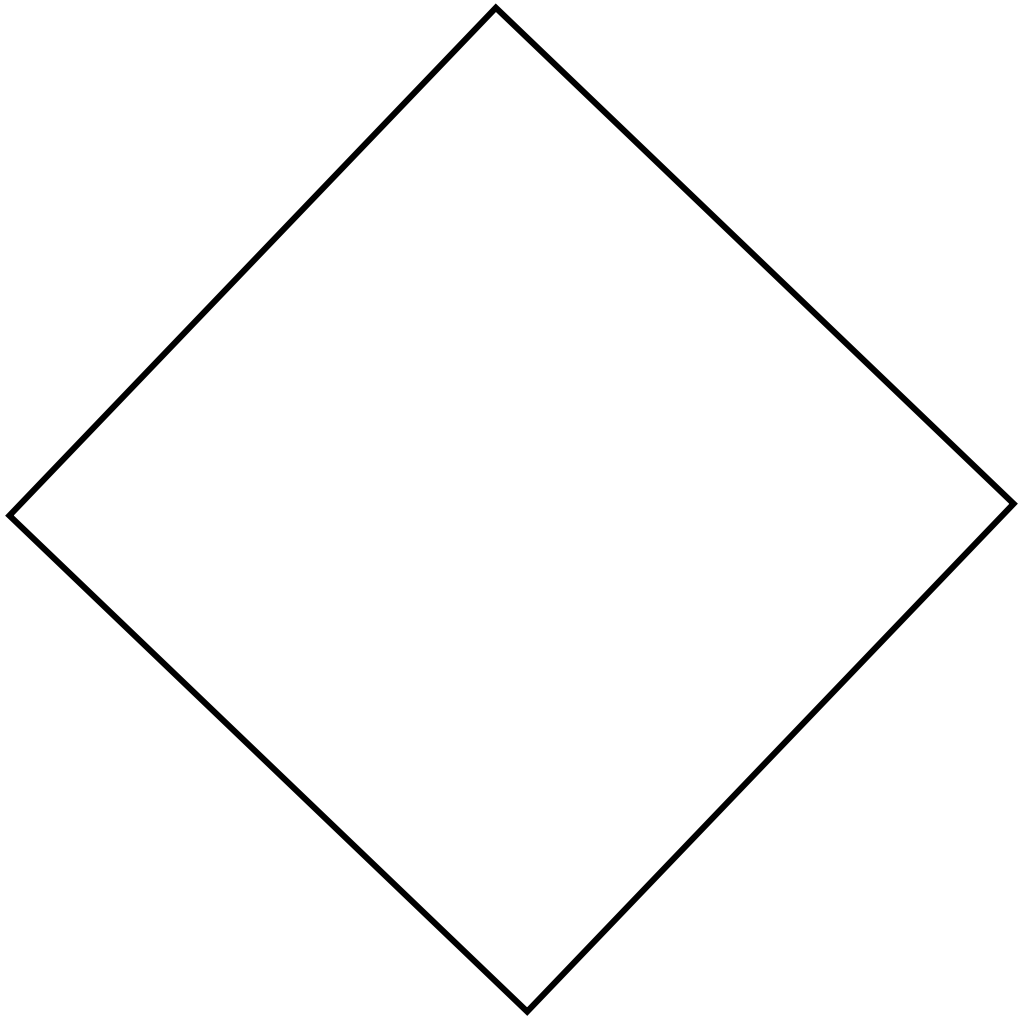


$+'$	?	O	E
?	?	?	?
O	?	E	O
E	?	O	E

$*'$	?	O	E
?	?	?	E
O	?	O	E
E	E	E	E

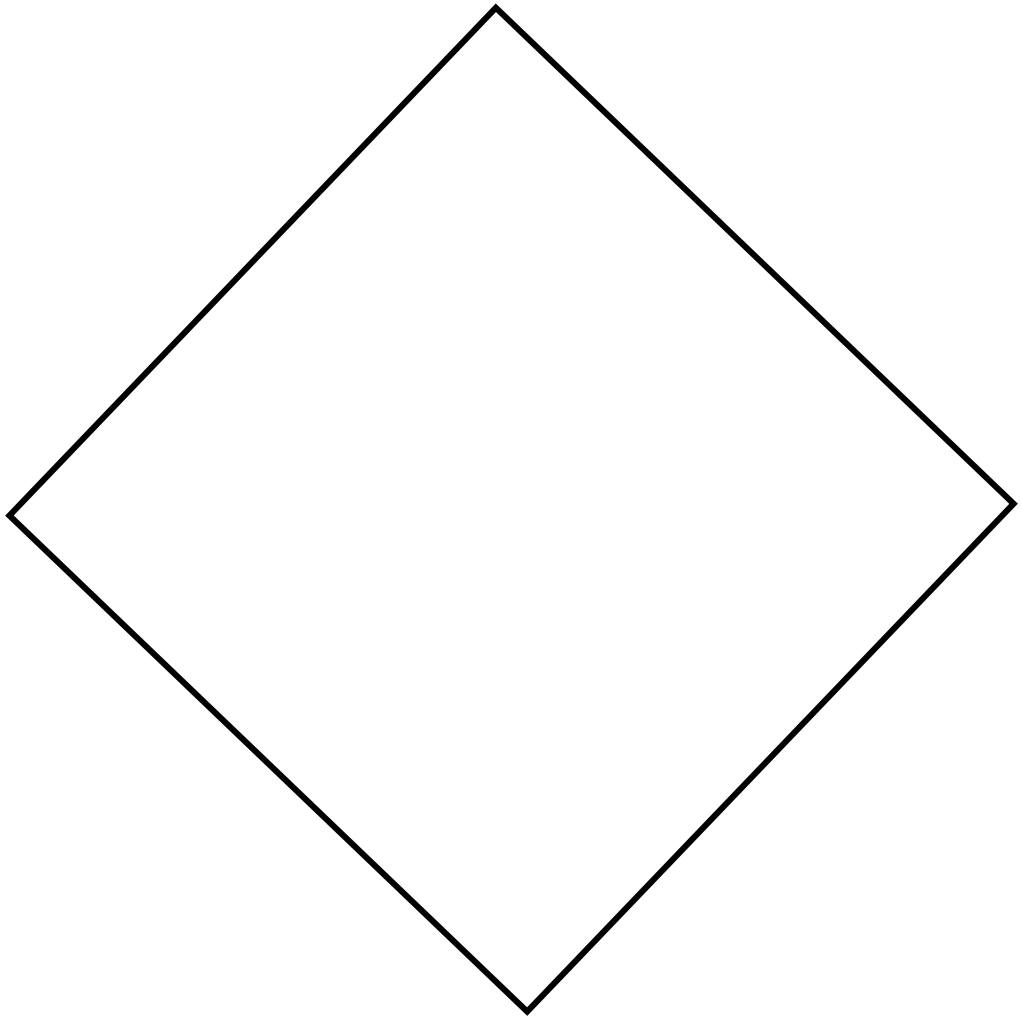
$$f : _ \times _ \to \mathrm{O}$$

Abstract Interpretation

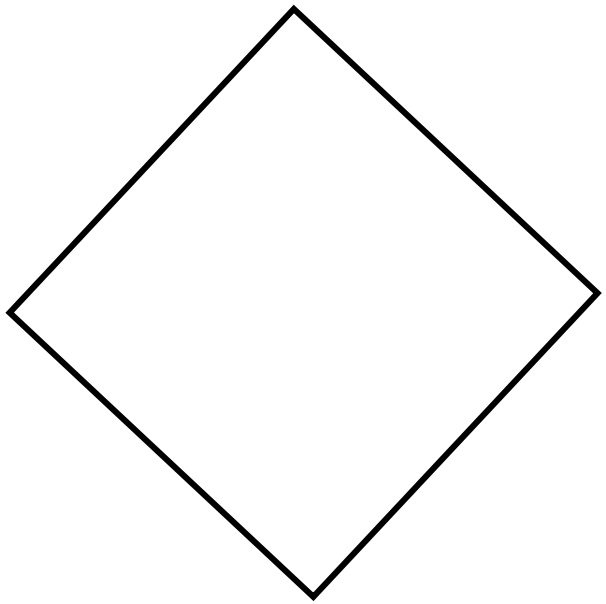


Concrete

Abstract Interpretation

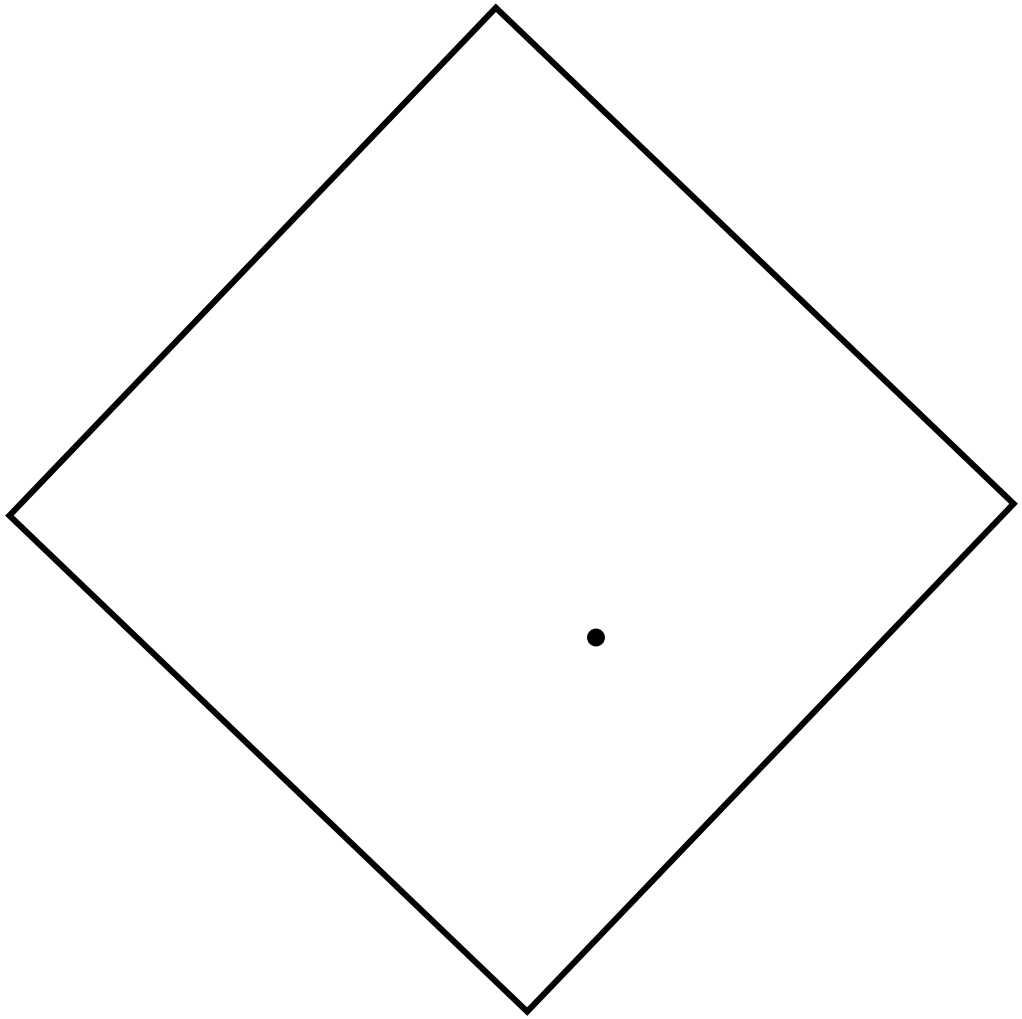


Concrete

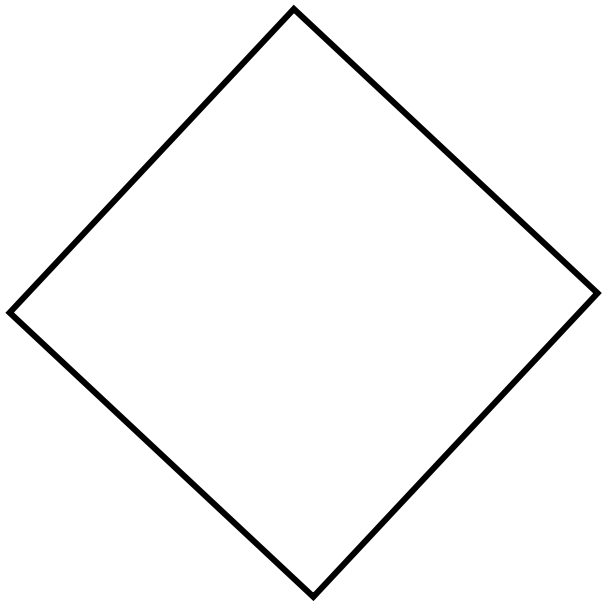


Abstract

Abstract Interpretation

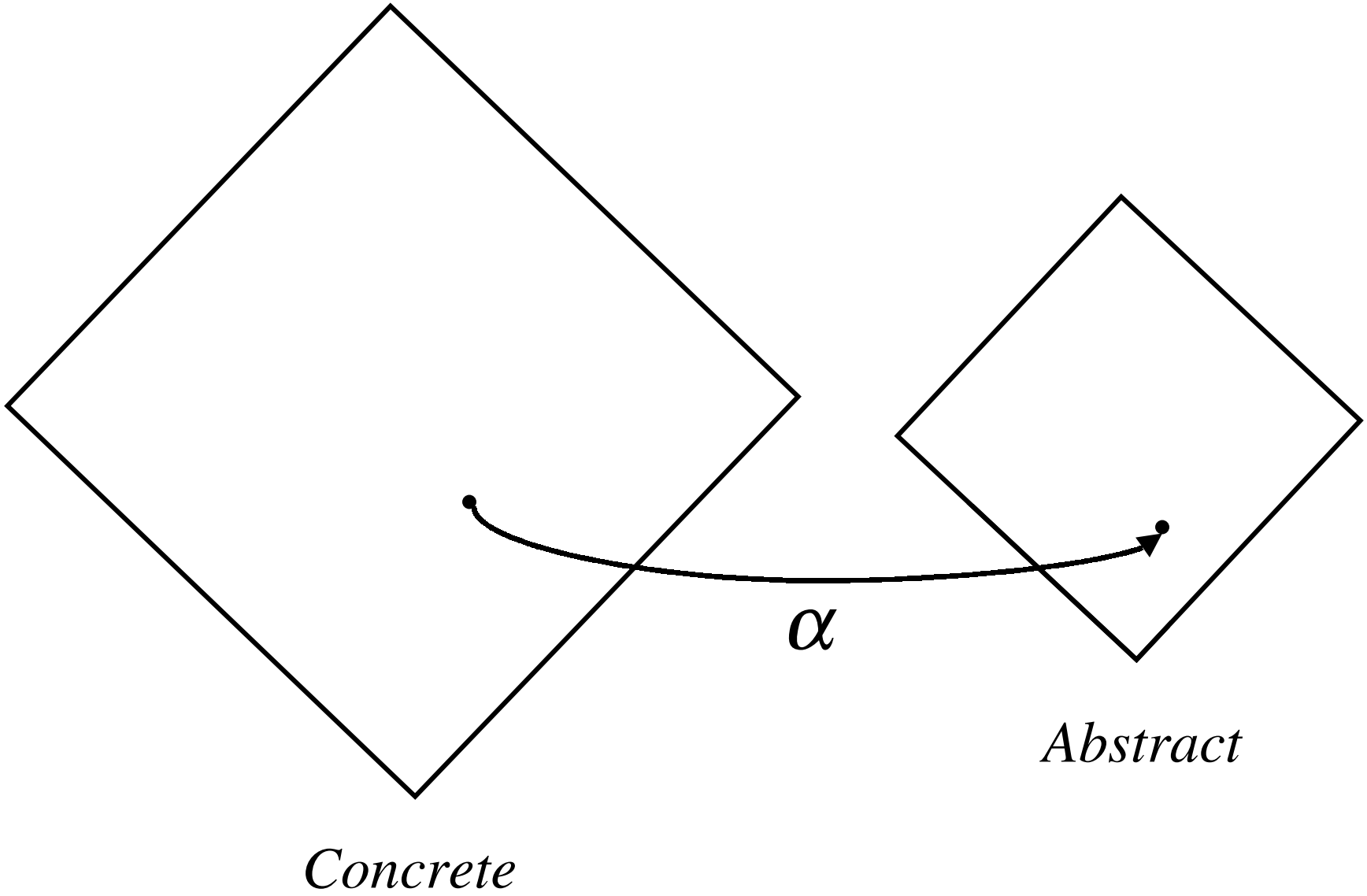


Concrete

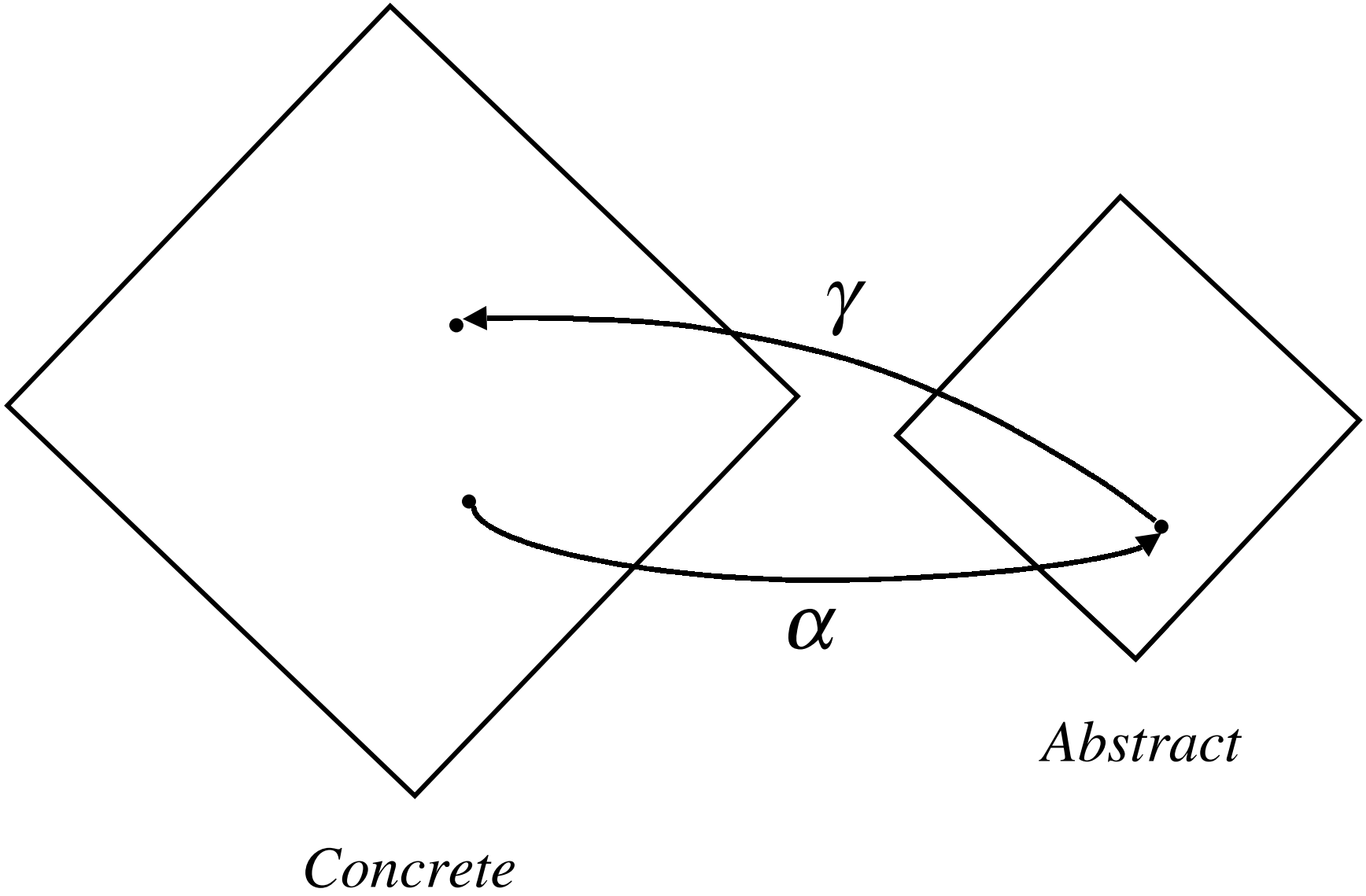


Abstract

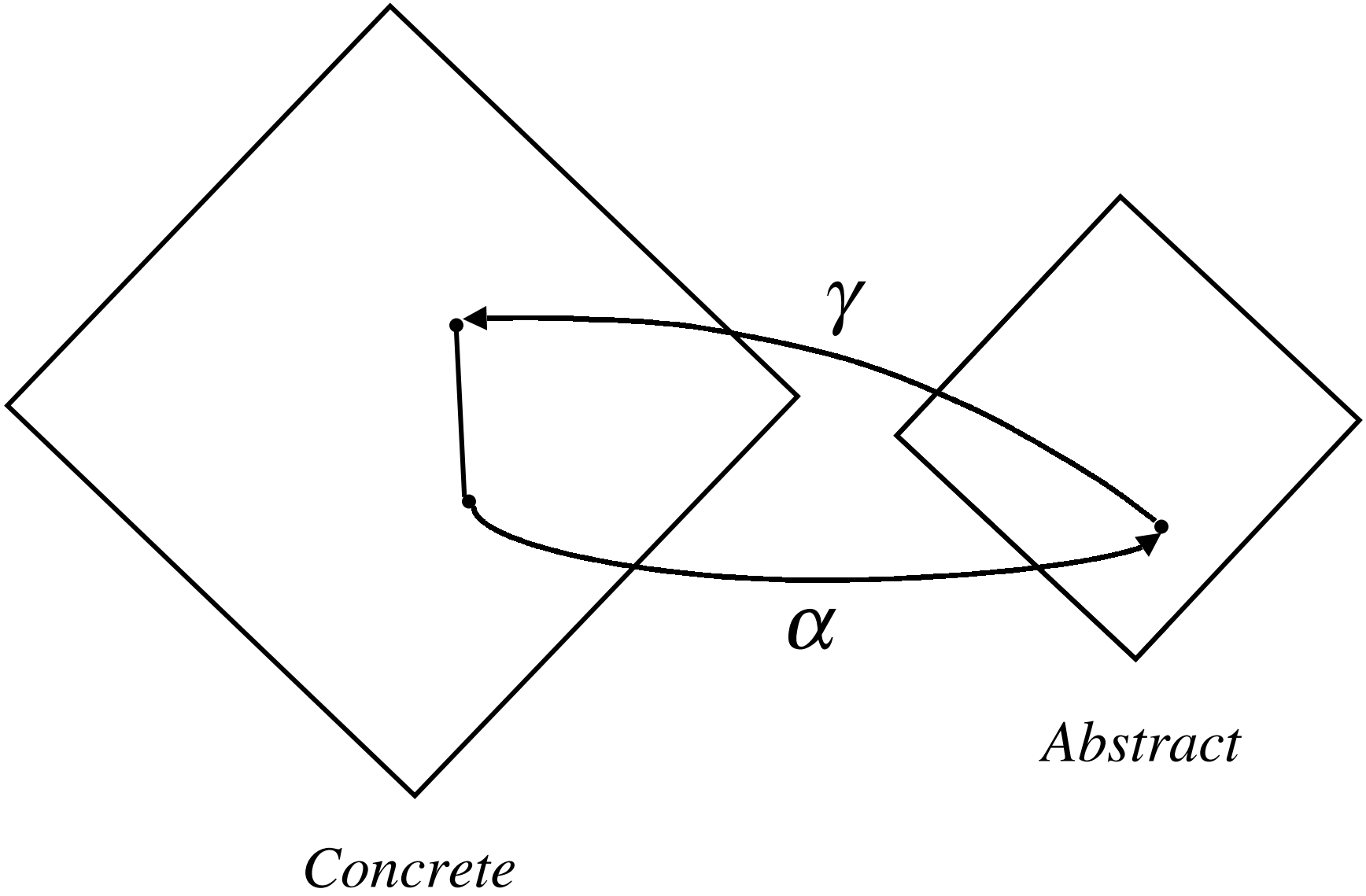
Abstract Interpretation



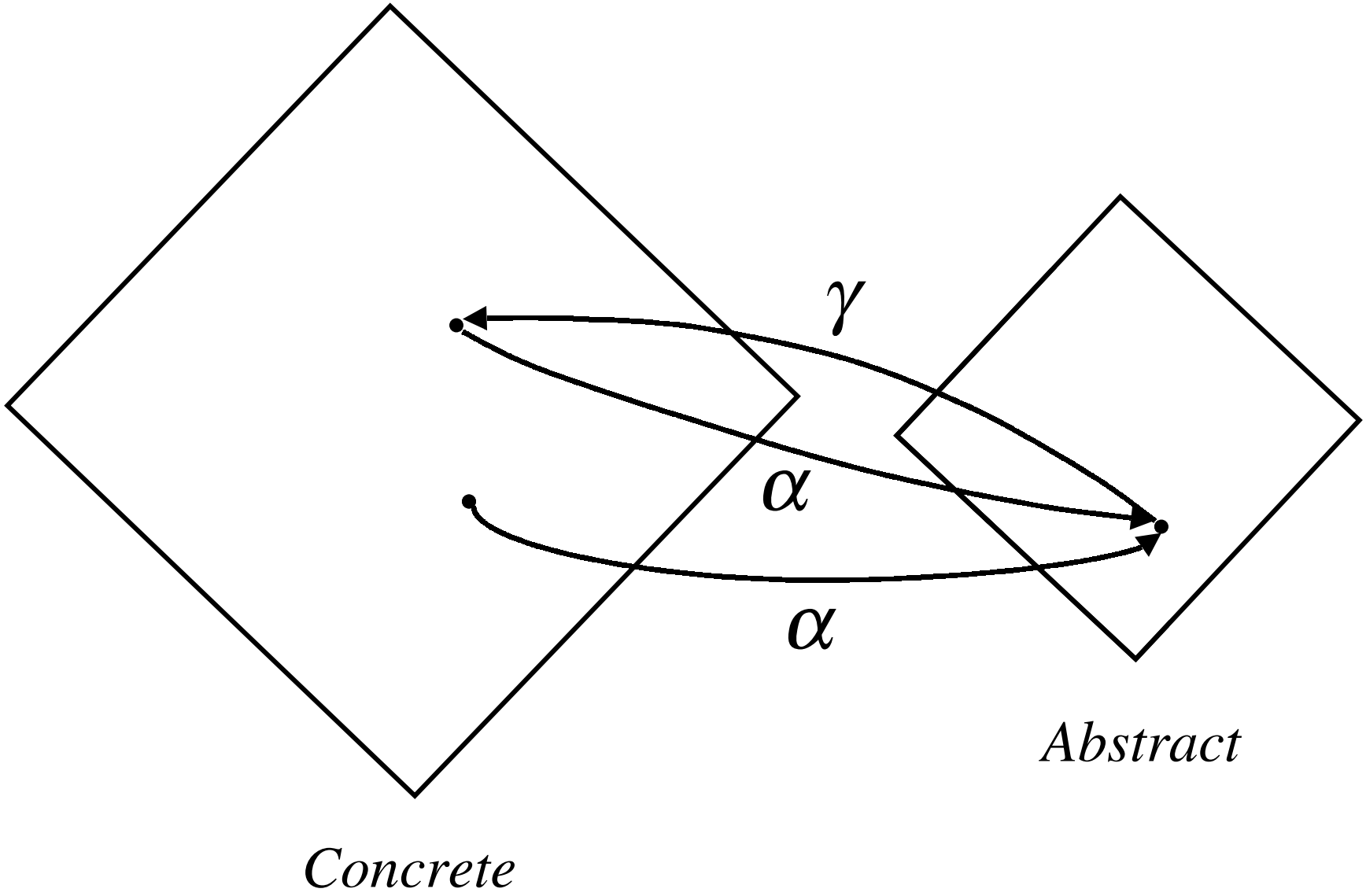
Abstract Interpretation



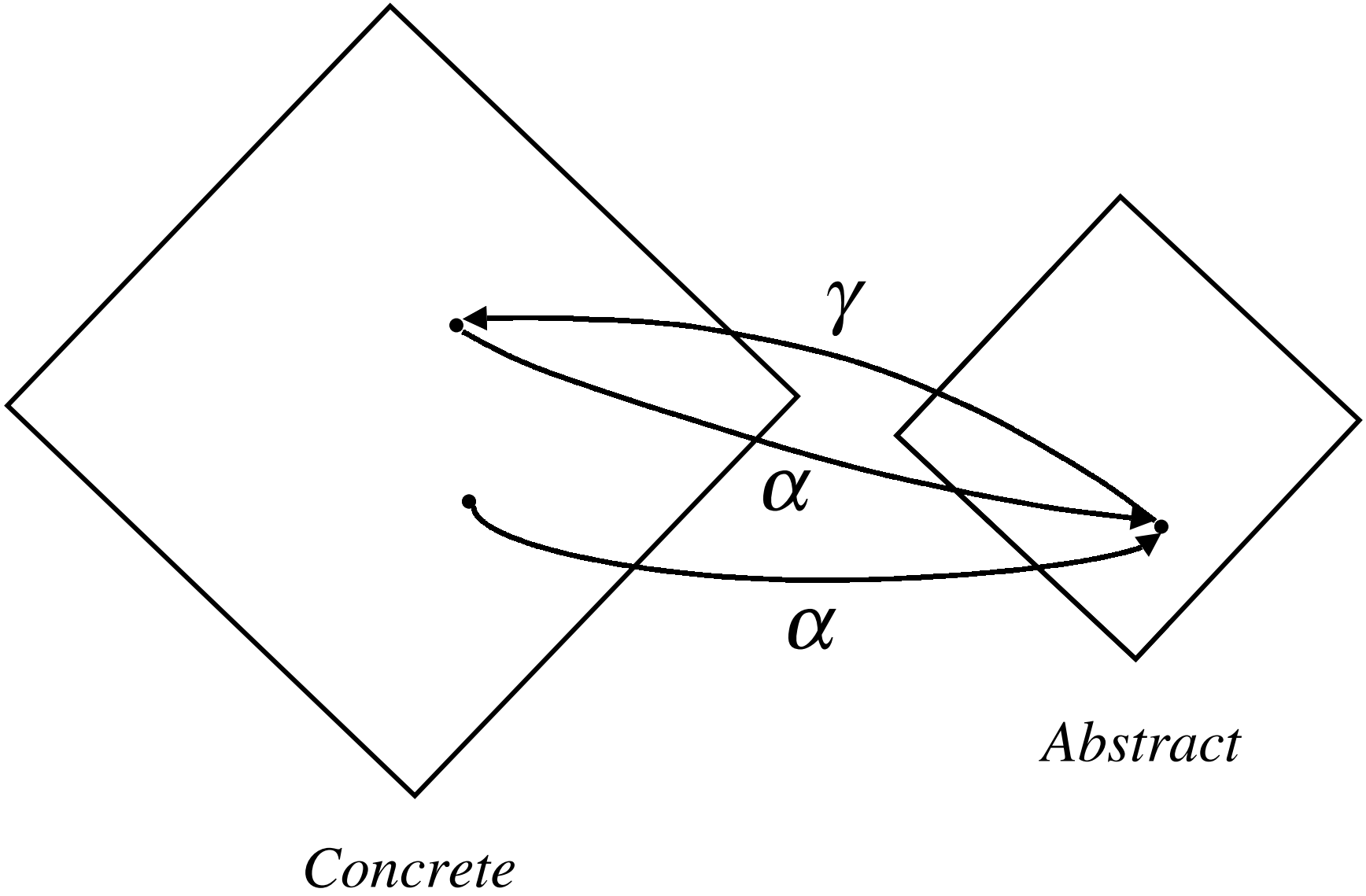
Abstract Interpretation



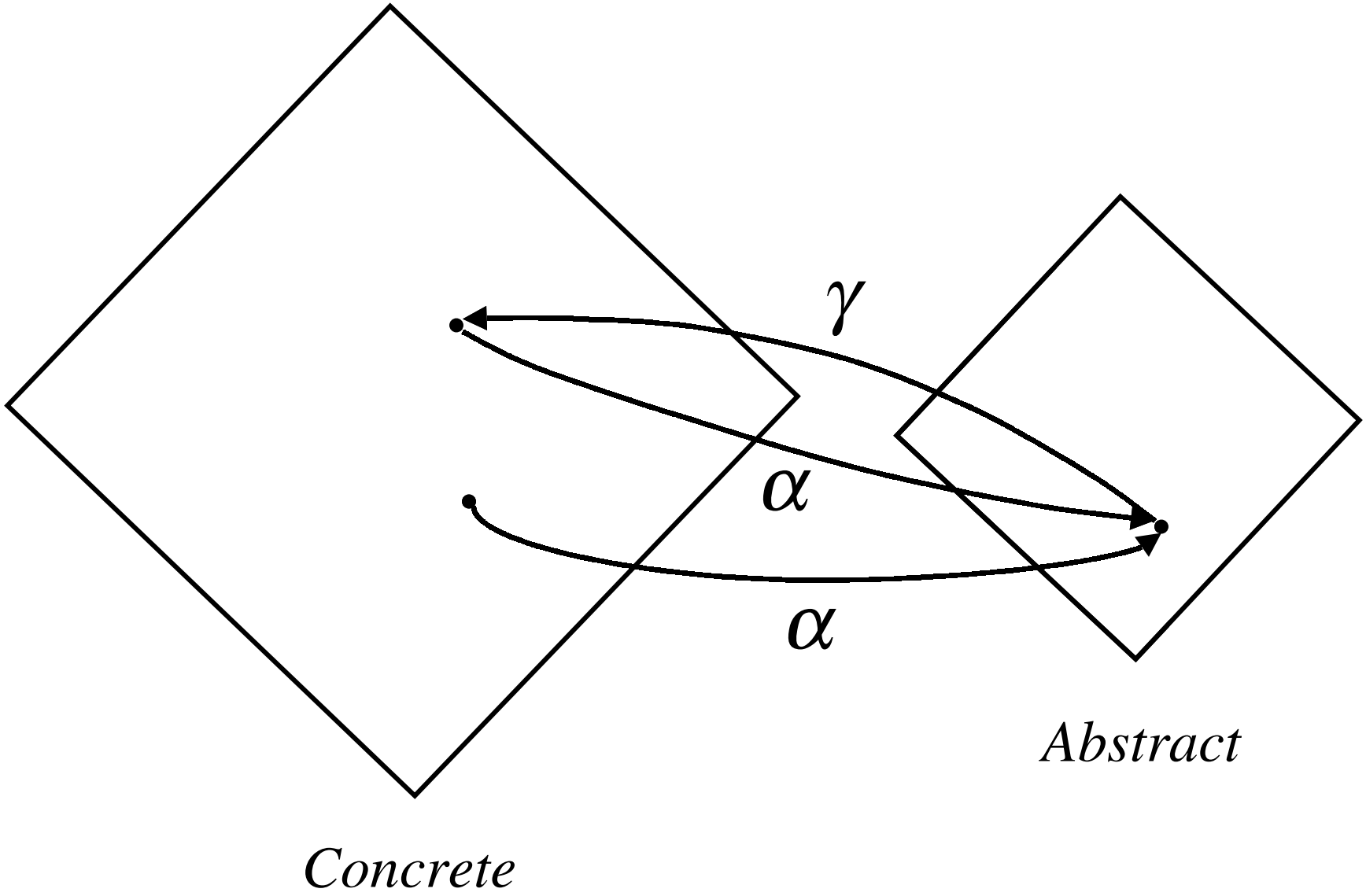
Abstract Interpretation



Abstract Interpretation



Abstract Interpretation



Outline

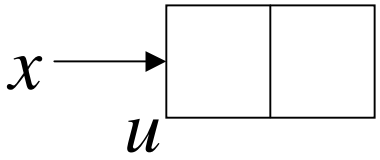
- Using logic to describe stores
- Using logic to express store transformations
- Forming abstractions of stores
- Three-valued logic
- Using three-valued logic to express transformations of abstract stores

Using Logic to Describe Stores

- Predicate Symbols
  - Whether variable x points to location u:
    - $x(u)$
  - Pointer fields:
    - $n(u_1, u_2)$
    - $car(u_1, u_2)$
    - $cdr(u_1, u_2)$

Using Logic to Describe Stores

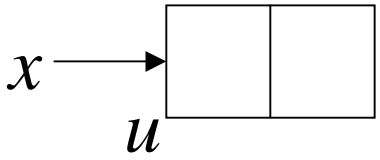
- Predicate Symbols
  - Whether variable x points to location u:
    - $x(u)$



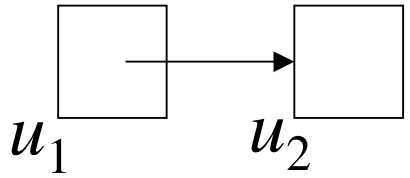
  - Pointer fields:
    - $n(u_1, u_2)$
    - $car(u_1, u_2)$
    - $cdr(u_1, u_2)$

Using Logic to Describe Stores

- Predicate Symbols
  - Whether variable x points to location u:
    - $x(u)$



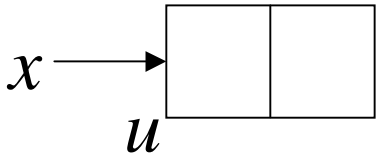
  - Pointer fields:
    - $n(u_1, u_2)$



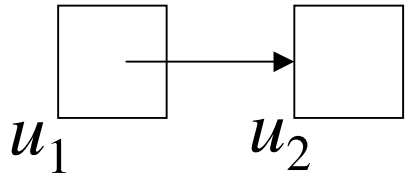
    - $car(u_1, u_2)$
    - $cdr(u_1, u_2)$

Using Logic to Describe Stores

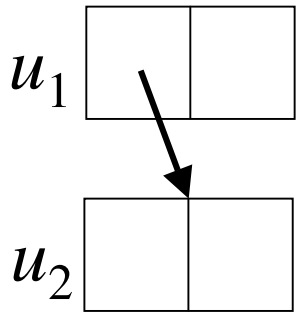
- Predicate Symbols
  - Whether variable x points to location u:
    - $x(u)$



  - Pointer fields:
    - $n(u_1, u_2)$



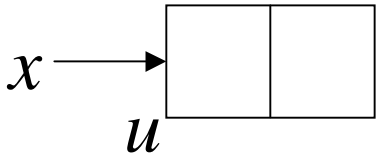
    - $car(u_1, u_2)$



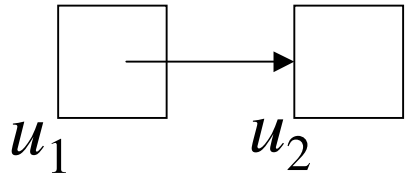
    - $cdr(u_1, u_2)$

Using Logic to Describe Stores

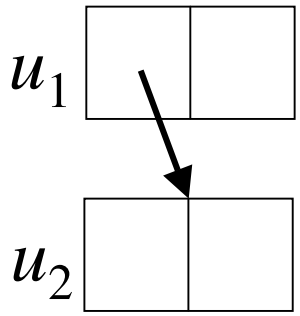
- Predicate Symbols
  - Whether variable x points to location u:
    - $x(u)$



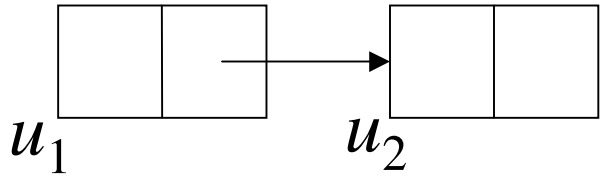
  - Pointer fields:
    - $n(u_1, u_2)$



    - $car(u_1, u_2)$



    - $cdr(u_1, u_2)$



Using Logic to Describe Stores

- Formulas: Other Properties of Locations

Using Logic to Describe Stores

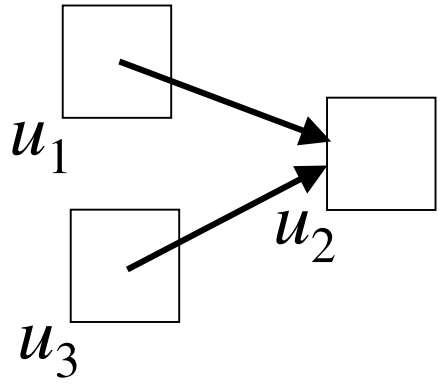
- Formulas: Other Properties of Locations

$$is(v) \triangleq \exists\, v_1, v_2 : n(v_1, v) \wedge n(v_2, v) \wedge v_1 \neq v_2$$

Using Logic to Describe Stores

- Formulas: Other Properties of Locations

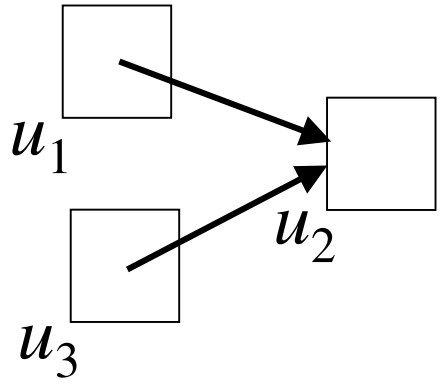
$$is(v) \triangleq \exists\, v_1, v_2 : n(v_1, v) \wedge n(v_2, v) \wedge v_1 \neq v_2$$



Using Logic to Describe Stores

- Formulas: Other Properties of Locations

$$is(v) \triangleq \exists\, v_1, v_2 : n(v_1, v) \wedge n(v_2, v) \wedge v_1 \neq v_2$$

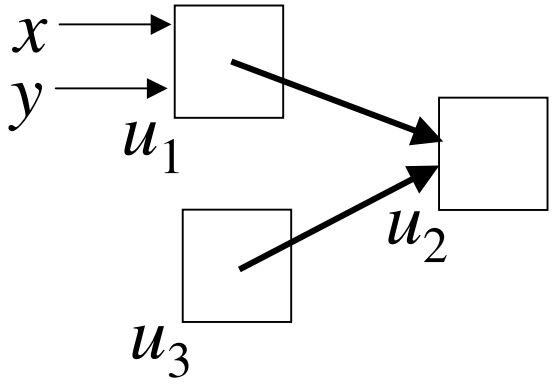


$is(u_1) = 0$ $\quad$ $is(u_2) = 1$ $\quad$ $is(u_3) = 0$

Using Logic to Describe Stores

- Formulas: Other Properties of Locations

$$is(v) \triangleq \exists\, v_1, v_2 : n(v_1, v) \wedge n(v_2, v) \wedge v_1 \neq v_2$$

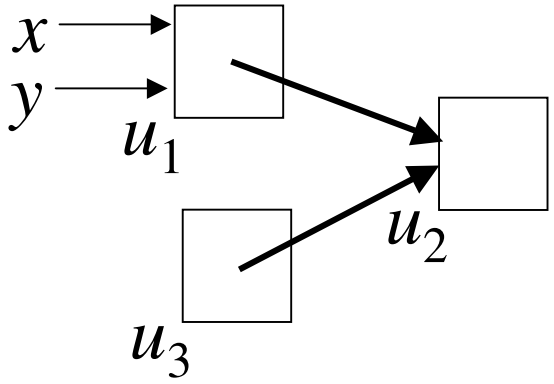


$$is(u_1) = 0 \qquad is(u_2) = 1 \qquad is(u_3) = 0$$

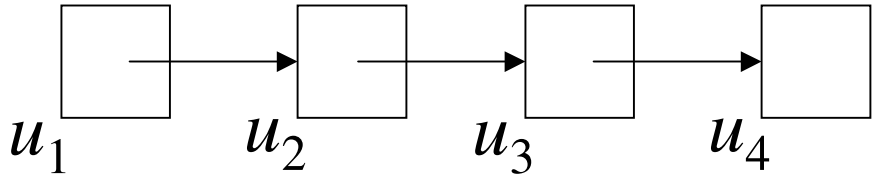
Using Logic to Describe Stores

- Formulas: Other Properties of Locations

$$is(v) \triangleq \exists\, v_1, v_2 : n(v_1, v) \wedge n(v_2, v) \wedge v_1 \neq v_2$$



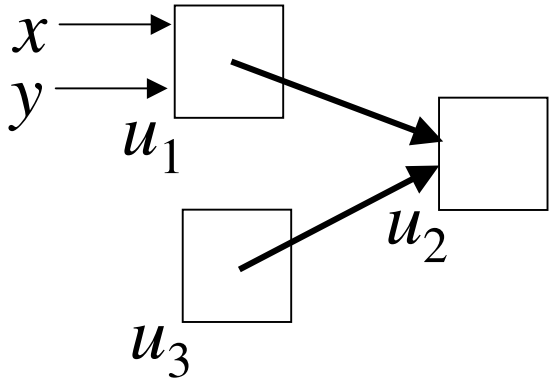
$is(u_1) = 0$ $\quad$ $is(u_2) = 1$ $\quad$ $is(u_3) = 0$



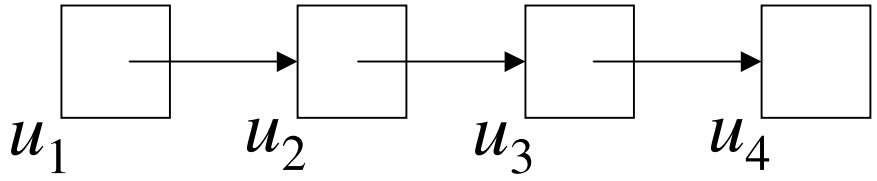
Using Logic to Describe Stores

- Formulas: Other Properties of Locations

$$is(v) \triangleq \exists\, v_1, v_2 : n(v_1, v) \wedge n(v_2, v) \wedge v_1 \neq v_2$$



$is(u_1) = 0 \qquad is(u_2) = 1 \qquad is(u_3) = 0$



$is(u_1) = 0 \qquad is(u_2) = 0 \qquad is(u_3) = 0 \qquad is(u_4) = 0$

First-Order Logic (Syntax)

First-Order Logic (Syntax)

- Vocabulary
  - Predicate symbols: $p_1, p_2, \ldots, p_n$
  - Constant symbols: $c_1, c_2, \ldots, c_m$
  - Function symbols: $f_1, f_2, \ldots, f_k$

First-Order Logic (Syntax)

- Vocabulary
  - Predicate symbols: $p_1, p_2, \ldots, p_n$
  - Constant symbols: $c_1, c_2, \ldots, c_m$
  - Function symbols: $f_1, f_2, \ldots, f_k$
- Formulas
  - Variables
  - Equality-predicate symbol: $=$
  - Logical-constant symbols: $\underline{0}$, $\underline{1}$
  - Connectives: $\wedge, \vee, \neg$
  - Quantifiers: $\forall, \exists$

First-Order Logic (Syntax)

- Vocabulary
  - Predicate symbols: $p_1, p_2, \ldots, p_n$
  - ~~Constant symbols: $c_1, c_2, \ldots, c_m$~~
  - ~~Function symbols: $f_1, f_2, \ldots, f_k$~~
- Formulas
  - Variables
  - Equality-predicate symbol: $=$
  - Logical-constant symbols: $\underline{0}$, $\underline{1}$
  - Connectives: $\wedge, \vee, \neg$
  - Quantifiers: $\forall, \exists$

First-Order Logic (Semantics)

- Truth values: 0, 1
- Logical structures
  - Individuals: $U = \{u_1, u_2, \ldots, u_n\}$
  - Predicates: $[\![p_i]\!]: U^{arity(p_i)} \rightarrow \{0, 1\}$

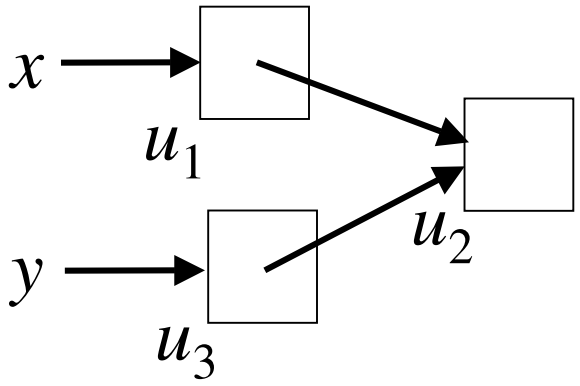
First-Order Logic (Semantics)

- Truth values: 0, 1
- Logical structures
  - Individuals: $U = \{u_1, u_2, \ldots, u_n\}$
  - Predicates: $[\![p_i]\!]: U^{arity(p_i)} \rightarrow \{0, 1\}$

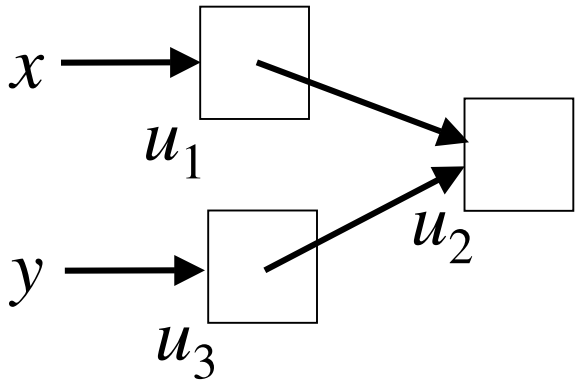
<u>In Our Application</u>

Logical structures = Concrete stores

An Example

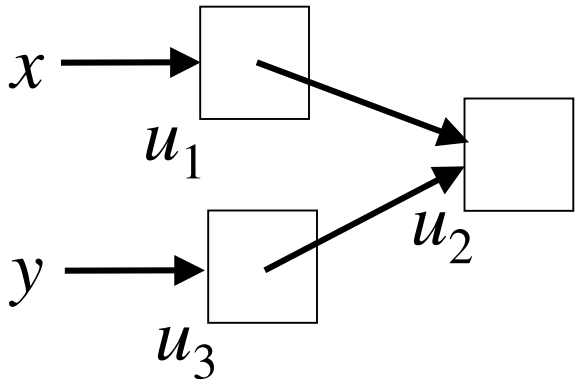


An Example



Individuals: $U = \{u_1, u_2, u_3\}$

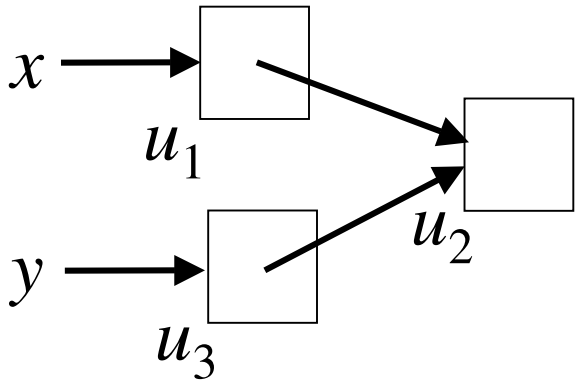
An Example



Individuals: $U = \{u_1, u_2, u_3\}$

Predicates:

An Example

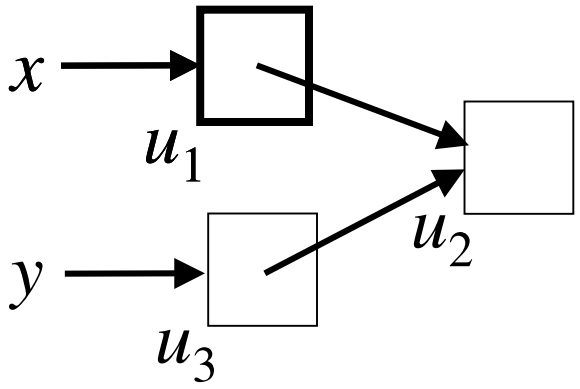


Individuals: $U = \{u_1, u_2, u_3\}$

Predicates:

	$x(u)$	$y(u)$
u_1	1	0
u_2	0	0
u_3	0	1

An Example

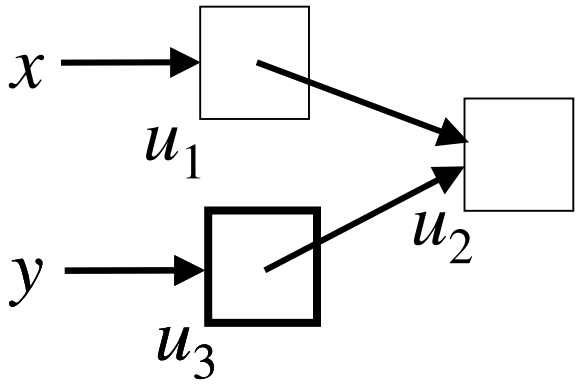


Individuals: $U = \{u_1, u_2, u_3\}$

Predicates:

	$x(u)$	$y(u)$
u_1	1	0
u_2	0	0
u_3	0	1

An Example

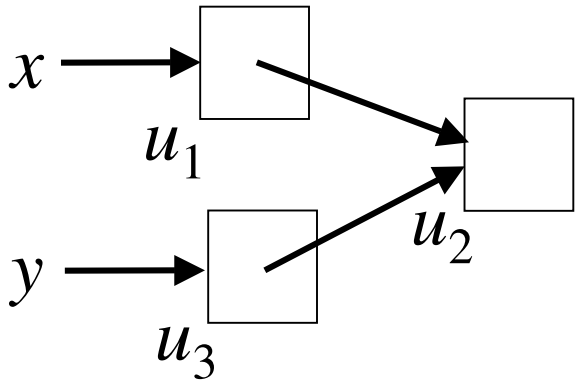


Individuals: $U = \{u_1, u_2, u_3\}$

Predicates:

	$x(u)$	$y(u)$
u_1	1	0
u_2	0	0
u_3	0	1

An Example



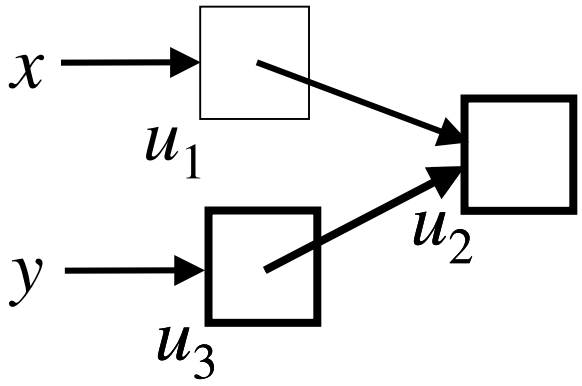
Individuals: $U = \{u_1, u_2, u_3\}$

Predicates:

	$x(u)$	$y(u)$
u_1	1	0
u_2	0	0
u_3	0	1

n	u_1	u_2	u_3
u_1	0	1	0
u_2	0	0	0
u_3	0	1	0

An Example



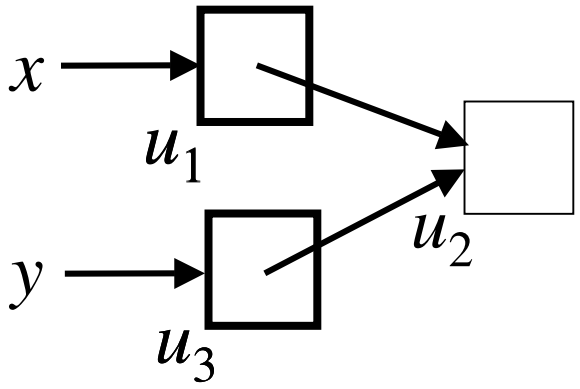
Individuals: $U = \{u_1, u_2, u_3\}$

Predicates:

	$x(u)$	$y(u)$
u_1	1	0
u_2	0	0
u_3	0	1

n	u_1	u_2	u_3
u_1	0	1	0
u_2	0	0	0
u_3	0	1	0

An Example



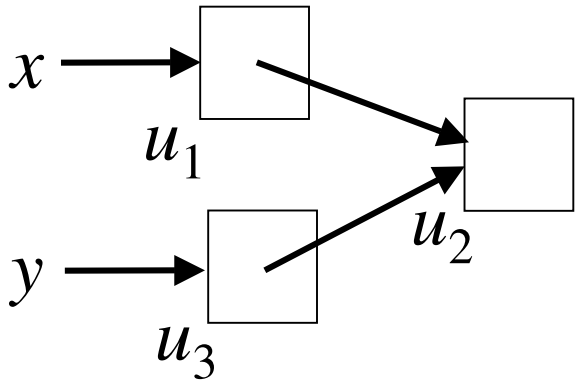
Individuals: $U = \{u_1, u_2, u_3\}$

Predicates:

	$x(u)$	$y(u)$
u_1	1	0
u_2	0	0
u_3	0	1

n	u_1	u_2	u_3
u_1	0	1	0
u_2	0	0	0
u_3	0	1	0

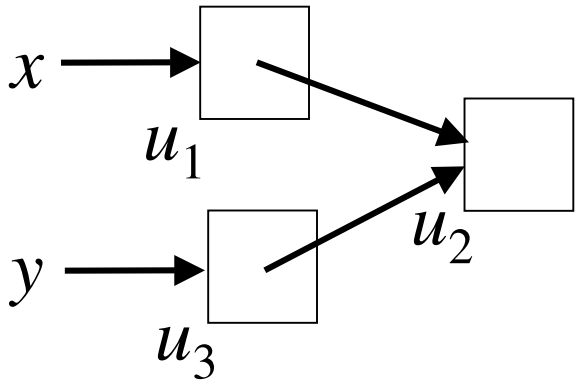
Example (Cont'd)



Individuals: $U = \{u_1, u_2, u_3\}$

Predicates:

Example (Cont'd)

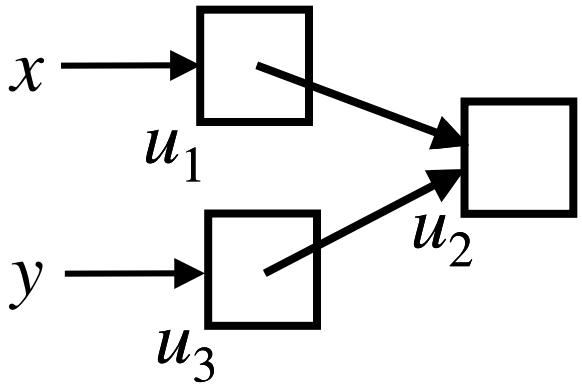


Individuals: $U = \{u_1, u_2, u_3\}$

Predicates:

	$is(u)$
u_1	0
u_2	1
u_3	0

Example (Cont'd)



Individuals: $U = \{u_1, u_2, u_3\}$

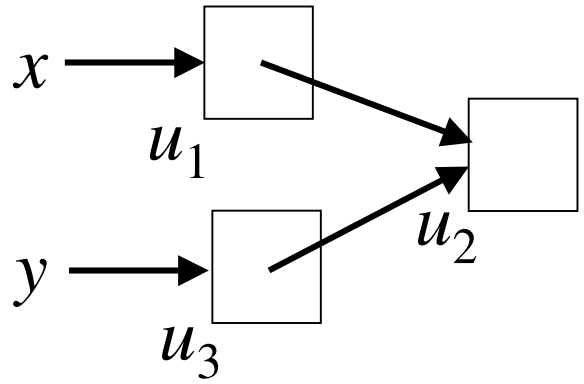
Predicates:

	$is(u)$
u_1	0
u_2	1
u_3	0

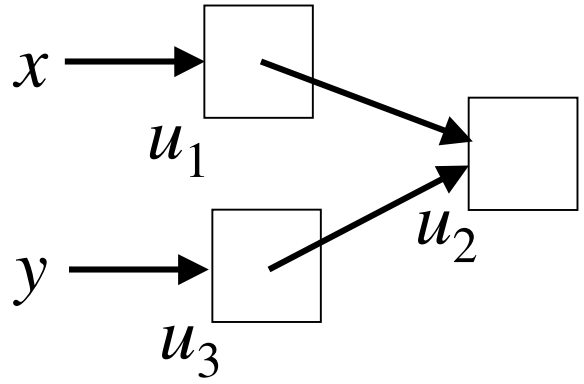
First-Order Logic (Semantics)

- Assignments
  - Z: free variables $\mapsto$ individuals
- Meaning of a formula $[\![\varphi]\!](Z)$

Meaning of a Formula

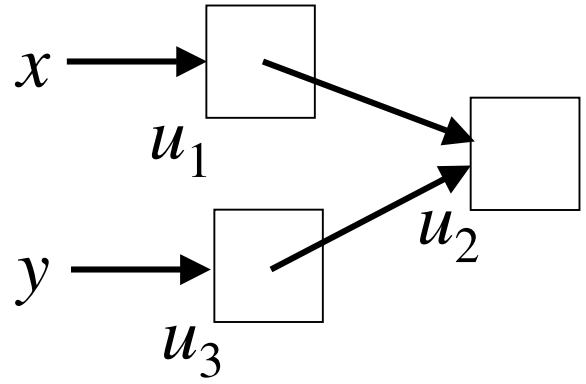


Meaning of a Formula



$$\varphi(v,v_1,v_2) \triangleq n(v_1,v) \wedge n(v_2,v) \wedge v_1 \neq v_2$$

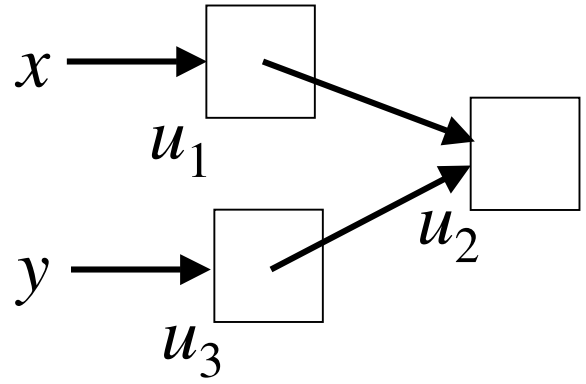
Meaning of a Formula



$$\varphi(v,v_1,v_2) \triangleq n(v_1,v) \wedge n(v_2,v) \wedge v_1 \neq v_2$$

$$Z = \{\ v \mapsto u_2,\ v_1 \mapsto u_1,\ v_2 \mapsto u_3\ \}$$

Meaning of a Formula



$$\varphi(v,v_1,v_2) \triangleq n(v_1,v) \wedge n(v_2,v) \wedge v_1 \neq v_2$$

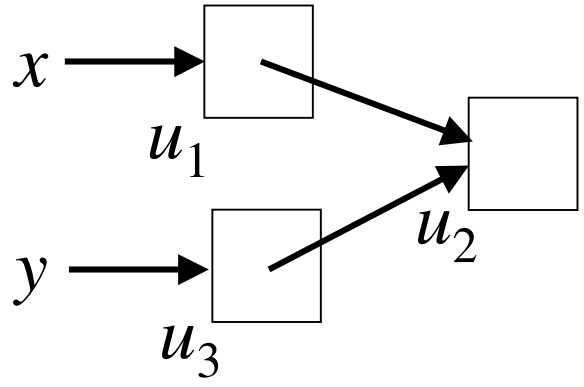
$$Z = \{\ v \mapsto u_2,\ v_1 \mapsto u_1,\ v_2 \mapsto u_3\ \}$$

$$[\![\varphi(v,v_1,v_2)]\!](Z) = ???$$

Meaning of a Formula $[\![\varphi]\!](Z)$

- $[\![\underline{0}]\!]\,(Z) = 0$
- $[\![\underline{1}]\!]\,(Z) = 1$
- $[\![p_i(v_1, \ldots, v_k)\,]\!](Z) = [\![p_i\,]\!](Z(v_1), \ldots, Z(v_k))$
- $[\![\varphi_1 \wedge \varphi_2]\!](Z) = [\![\varphi_1\,]\!](Z) \wedge [\![\varphi_2]\!](Z)$
- $[\![\varphi_1 \vee \varphi_2]\!](Z) = [\![\varphi_1\,]\!](Z) \vee [\![\varphi_2]\!](Z)$
- Negation, quantification, . . .

Meaning of a Formula



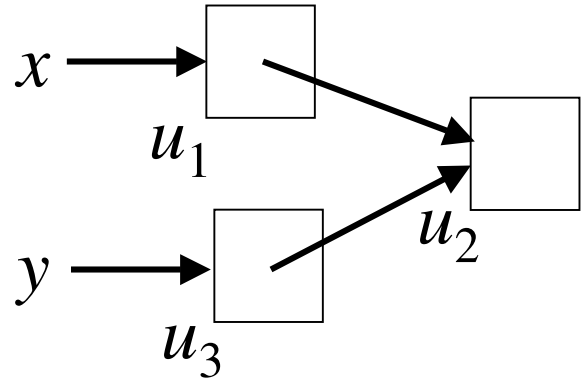
$$\varphi\,(v,v_1,v_2) \triangleq n(v_1,v) \wedge n(v_2,v) \wedge v_1 \neq v_2$$

$$Z = \{\ v \mapsto u_2,\ v_1 \mapsto u_1,\ v_2 \mapsto u_3\}$$

$$[\![\varphi]\!](Z) = [\![n(v_1,v) \wedge n(v_2,v) \wedge v_1 \neq v_2]\!](Z)$$

$$= \quad 1 \quad \wedge \quad 1 \quad \wedge \quad 1$$

Meaning of a Formula



$$\varphi\,(v,v_1,v_2) \triangleq n(v_1,v) \wedge n(v_2,v) \wedge v_1 \neq v_2$$

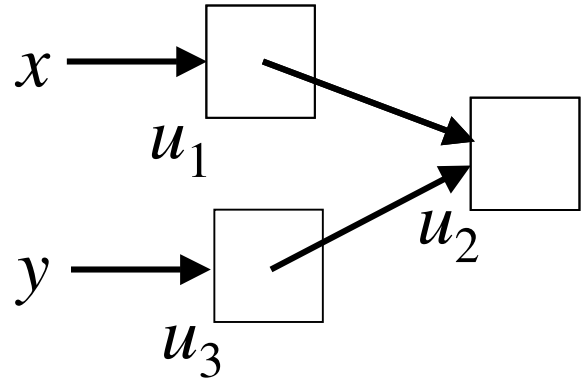
$$Z = \{\ v \mapsto u_2,\ v_1 \mapsto u_1,\ v_2 \mapsto u_3\}$$

$$[\![\varphi]\!](Z) = [\![n(v_1,v) \wedge n(v_2,v) \wedge v_1 \neq v_2]\!](Z)$$

$$= [\![n]\!](u_1, u_2) \wedge [\![n]\!](u_3, u_2) \wedge u_1 \neq u_3$$

$$= \quad 1 \quad \wedge \quad 1 \quad \wedge \quad 1$$

Meaning of a Formula



$$\varphi\,(v,v_1,v_2) \triangleq n(v_1,v) \wedge n(v_2,v) \wedge v_1 \neq v_2$$

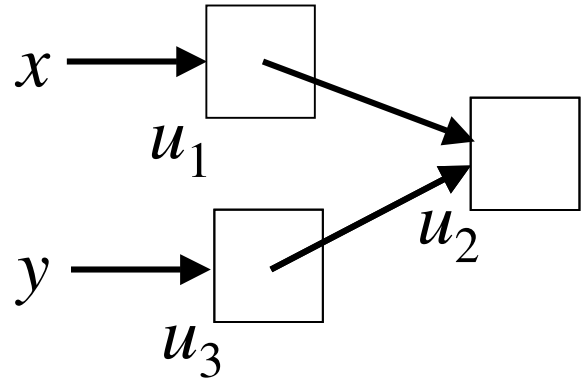
$$Z = \{\, v \mapsto u_2,\ v_1 \mapsto u_1,\ v_2 \mapsto u_3 \}$$

$$[\![\varphi]\!](Z) = [\![n(v_1,v) \wedge n(v_2,v) \wedge v_1 \neq v_2]\!](Z)$$

$$= \underline{[\![n]\!](u_1,\ u_2)} \wedge [\![n]\!](u_3,\ u_2) \wedge u_1 \neq u_3$$

$$= \quad 1 \quad \wedge \quad 1 \quad \wedge \quad 1$$

Meaning of a Formula



$$\varphi\,(v,v_1,v_2) \triangleq n(v_1,v) \wedge n(v_2,v) \wedge v_1 \neq v_2$$

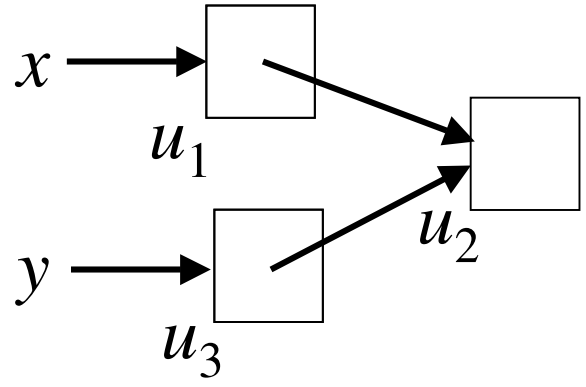
$$Z = \{\, v \mapsto u_2,\ v_1 \mapsto u_1,\ v_2 \mapsto u_3 \}$$

$$[\![\varphi]\!](Z) = [\![n(v_1,v) \wedge n(v_2,v) \wedge v_1 \neq v_2]\!](Z)$$

$$= [\![n]\!](u_1, u_2) \wedge \underline{[\![n]\!](u_3, u_2)} \wedge u_1 \neq u_3$$

$$= \quad 1 \quad \wedge \quad 1 \quad \wedge \quad 1$$

Meaning of a Formula



$$\varphi\,(v,v_1,v_2) \triangleq n(v_1,v) \wedge n(v_2,v) \wedge v_1 \neq v_2$$

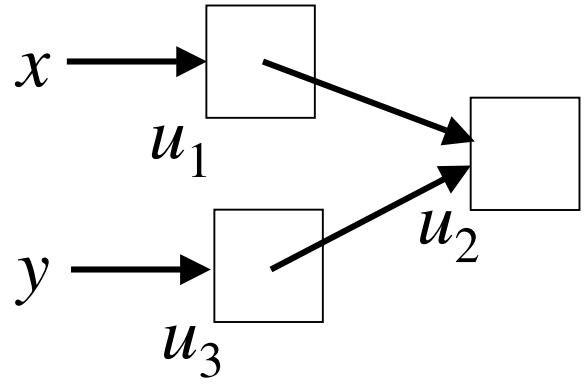
$$Z = \{\ v \mapsto u_2,\ v_1 \mapsto u_1,\ v_2 \mapsto u_3\}$$

$$[\![\varphi]\!](Z) = [\![n(v_1,v) \wedge n(v_2,v) \wedge v_1 \neq v_2]\!](Z)$$

$$= [\![n]\!](u_1, u_2) \wedge [\![n]\!](u_3, u_2) \wedge \underline{u_1 \neq u_3}$$

$$= \quad 1 \quad \wedge \quad 1 \quad \wedge \quad 1$$

Meaning of a Formula



$$\varphi\,(v,v_1,v_2) \triangleq n(v_1,v) \wedge n(v_2,v) \wedge v_1 \neq v_2$$

$$Z = \{\ v \mapsto u_2,\ v_1 \mapsto u_1,\ v_2 \mapsto u_3\}$$

$$[\![\varphi]\!](Z) = [\![n(v_1,v) \wedge n(v_2,v) \wedge v_1 \neq v_2]\!](Z)$$

$$= [\![n]\!](u_1, u_2) \wedge [\![n]\!](u_3, u_2) \wedge u_1 \neq u_3$$

$$= \quad 1 \quad \wedge \quad 1 \quad \wedge \quad 1$$

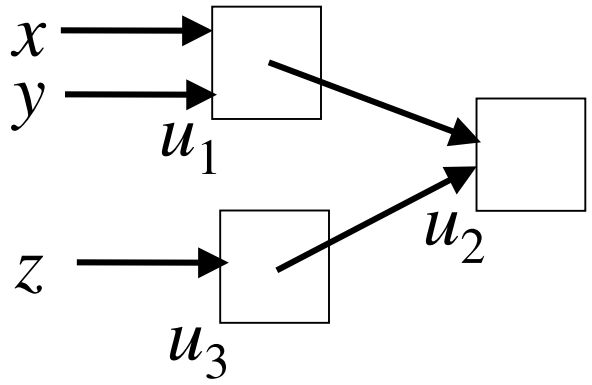
$$= \ 1$$

Outline

- Using logic to describe stores
- Using logic to express store transformations
- Forming abstractions of stores
- Three-valued logic
- Using three-valued logic to express transformations of abstract stores

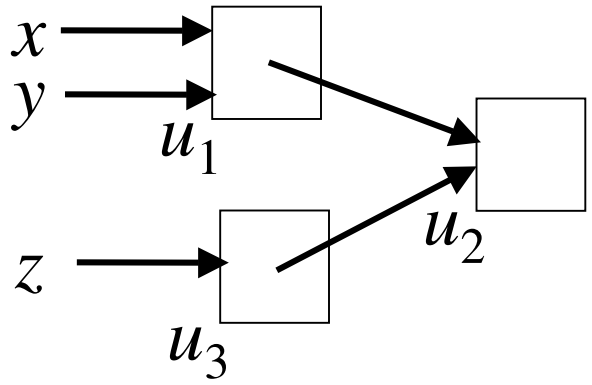
Using Logic to Change Stores

Before:



Using Logic to Change Stores

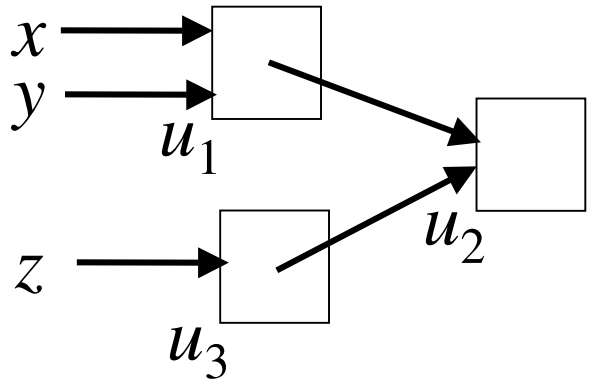
Before:



	$x(u)$	$y(u)$	$z(u)$
u_1	1	1	0
u_2	0	0	0
u_3	0	0	1

Using Logic to Change Stores

Before:



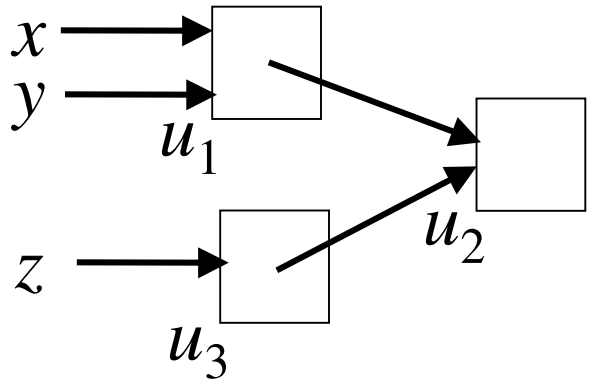
	$x(u)$	$y(u)$	$z(u)$
u_1	1	1	0
u_2	0	0	0
u_3	0	0	1

n	u_1	u_2	u_3
u_1	0	1	0
u_2	0	0	0
u_3	0	1	0

Using Logic to Change Stores

$x = \text{null}$

Before:



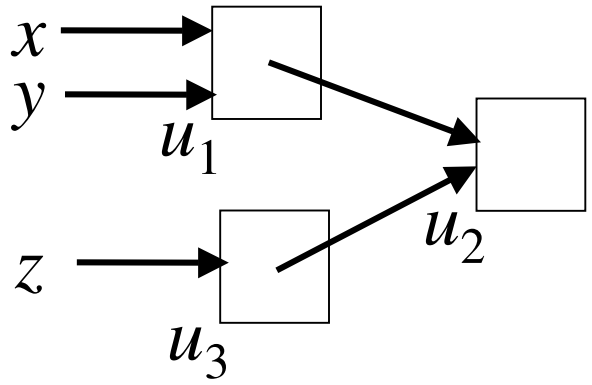
	$x(u)$	$y(u)$	$z(u)$
u_1	1	1	0
u_2	0	0	0
u_3	0	0	1

n	u_1	u_2	u_3
u_1	0	1	0
u_2	0	0	0
u_3	0	1	0

Using Logic to Change Stores

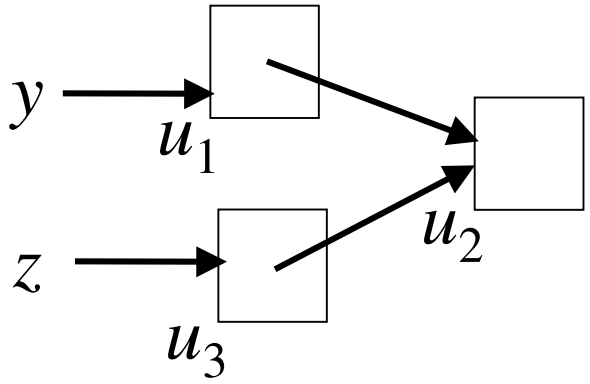
x = null

Before:



	$x(u)$	$y(u)$	$z(u)$
u_1	1	1	0
u_2	0	0	0
u_3	0	0	1

After:

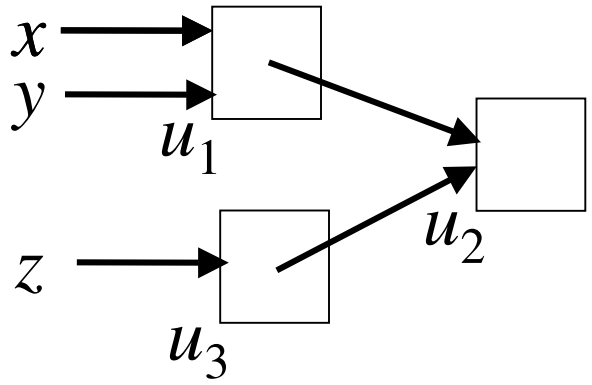


n	u_1	u_2	u_3
u_1	0	1	0
u_2	0	0	0
u_3	0	1	0

Using Logic to Change Stores

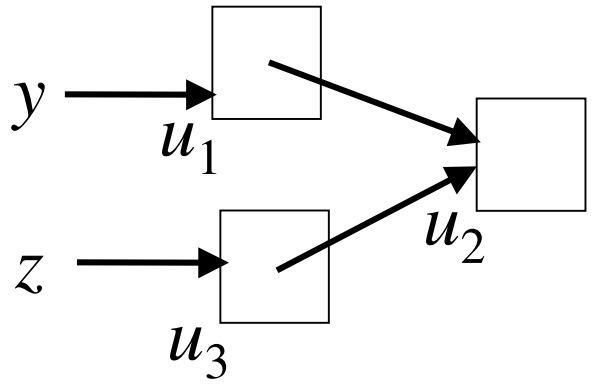
x = null

Before:



	$x(u)$	$y(u)$	$z(u)$
u_1	1	1	0
u_2	0	0	0
u_3	0	0	1

After:

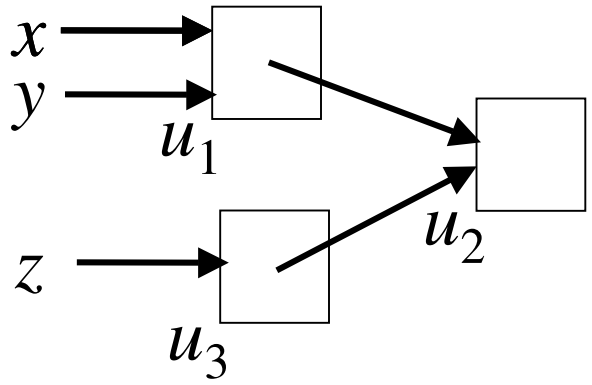


n	u_1	u_2	u_3
u_1	0	1	0
u_2	0	0	0
u_3	0	1	0

Using Logic to Change Stores

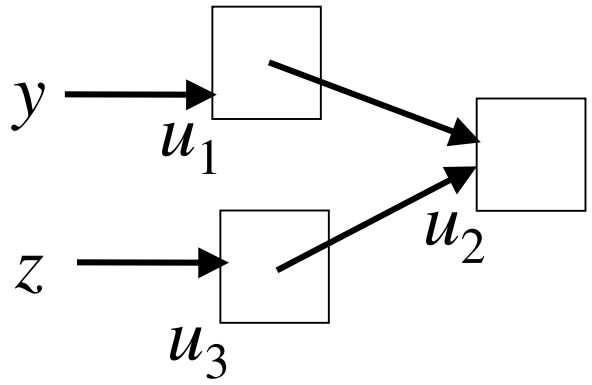
x = null

Before:



	$x(u)$	$y(u)$	$z(u)$
u_1	0	1	0
u_2	0	0	0
u_3	0	0	1

After:

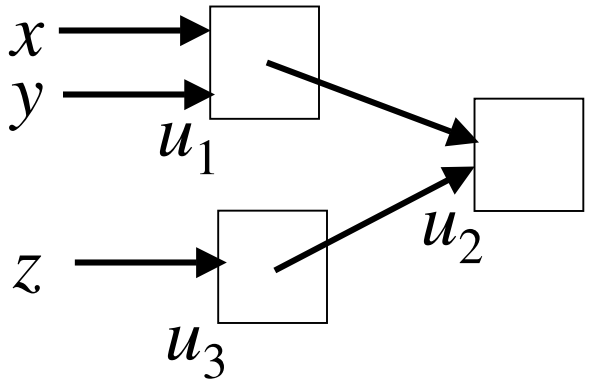


n	u_1	u_2	u_3
u_1	0	1	0
u_2	0	0	0
u_3	0	1	0

Predicate-Alteration Formulas for x = null

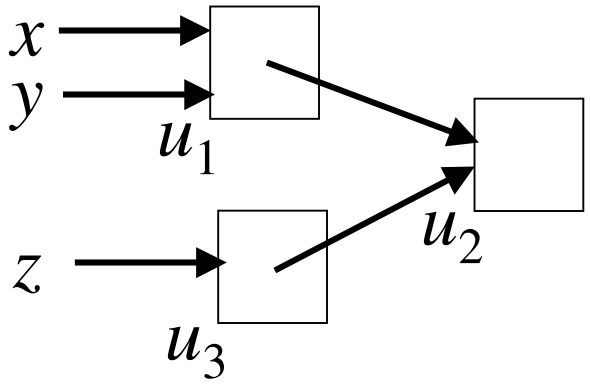
Predicate-Alteration Formulas for x = null

Old:

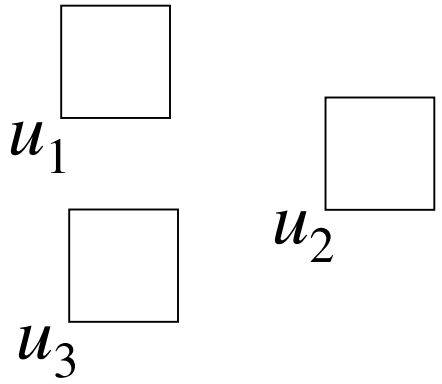


Predicate-Alteration Formulas for x = null

Old:

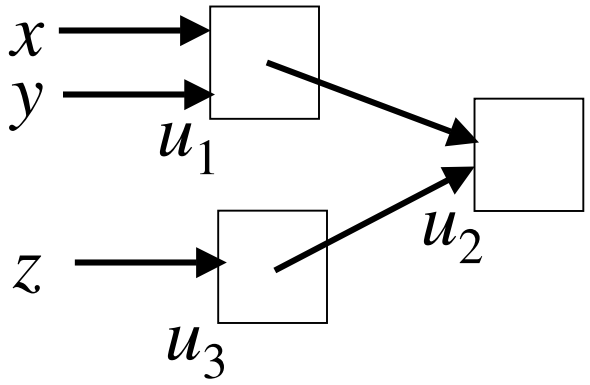


New:

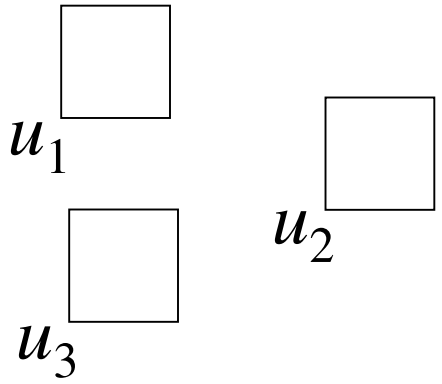


Predicate-Alteration Formulas for x = null

Old:



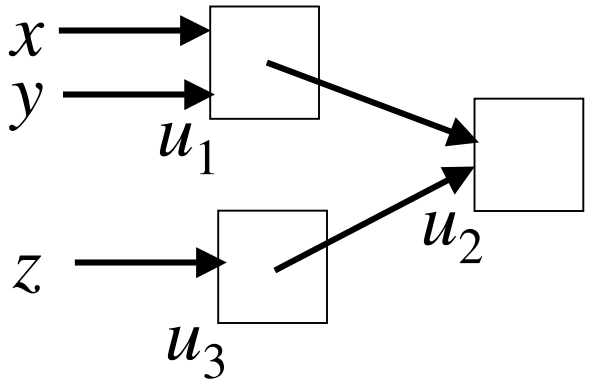
New:



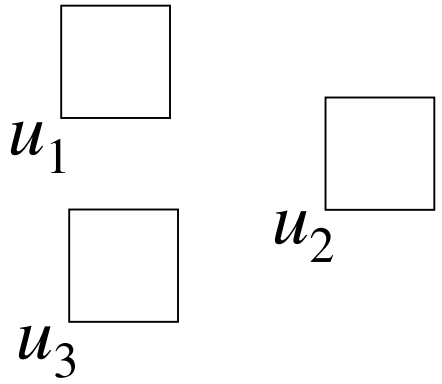
	$x(u)$	$y(u)$	$z(u)$
u_1	1	1	0
u_2	0	0	0
u_3	0	0	1

Predicate-Alteration Formulas for x = null

Old:



New:

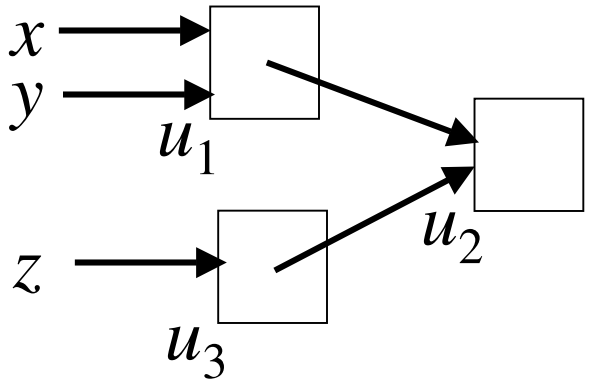


$$\varphi_x^{[x = \text{null}]}(v) \triangleq \underline{0}$$

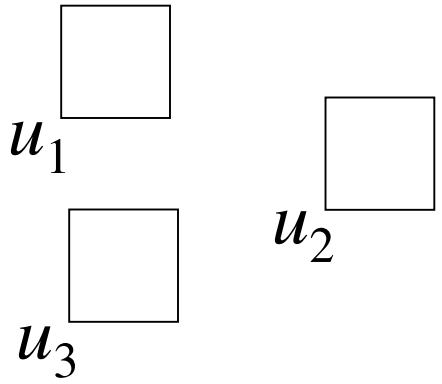
	$x(u)$	$y(u)$	$z(u)$
u_1	1	1	0
u_2	0	0	0
u_3	0	0	1

Predicate-Alteration Formulas for x = null

Old:



New:

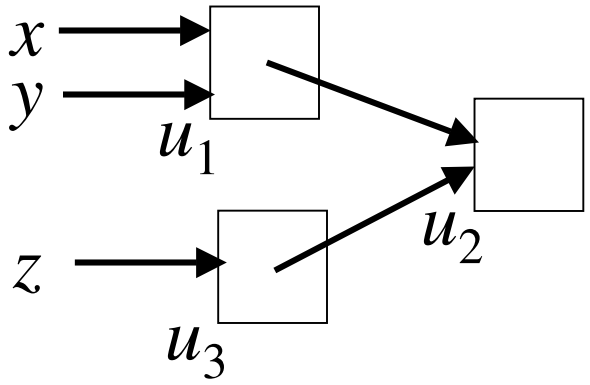


$$\varphi_x^{[x = \text{null}]}(v) \triangleq \boxed{\underline{0}}$$

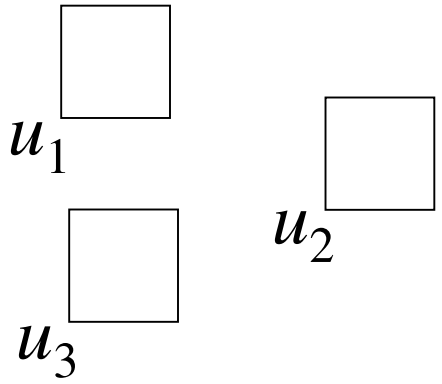
	$x(u)$	$y(u)$	$z(u)$
u_1	1	1	0
u_2	0	0	0
u_3	0	0	1

Predicate-Alteration Formulas for x = null

Old:



New:



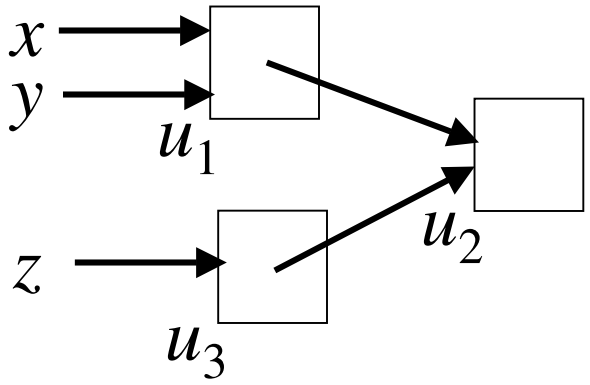
$$\varphi_x^{[x = \text{null}]}(v) \triangleq \underline{0}$$

	$x(u)$	$y(u)$	$z(u)$
u_1	1	1	0
u_2	0	0	0
u_3	0	0	1

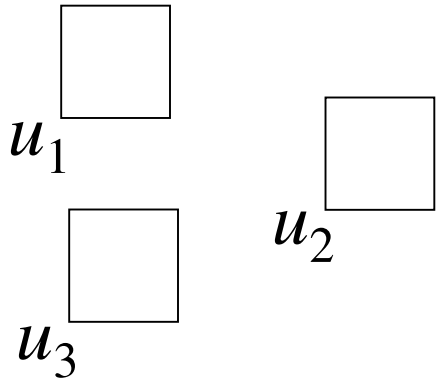
	$\varphi_x(u)$	$\varphi_y(u)$	$\varphi_z(u)$
u_1	0		
u_2	0		
u_3	0		

Predicate-Alteration Formulas for x = null

Old:



New:

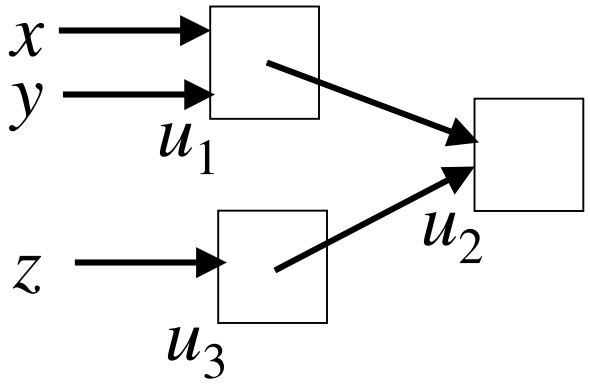


	$x(u)$	$y(u)$	$z(u)$
u_1	1	1	0
u_2	0	0	0
u_3	0	0	1

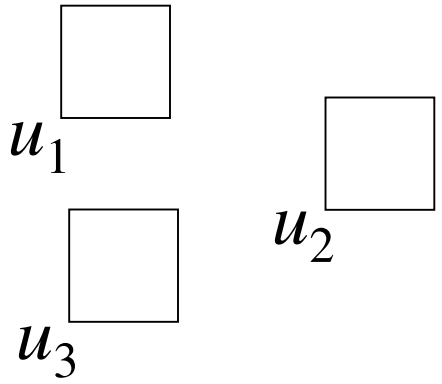
	$\varphi_x(u)$	$\varphi_y(u)$	$\varphi_z(u)$
u_1	0		
u_2	0		
u_3	0		

Predicate-Alteration Formulas for x = null

Old:



New:



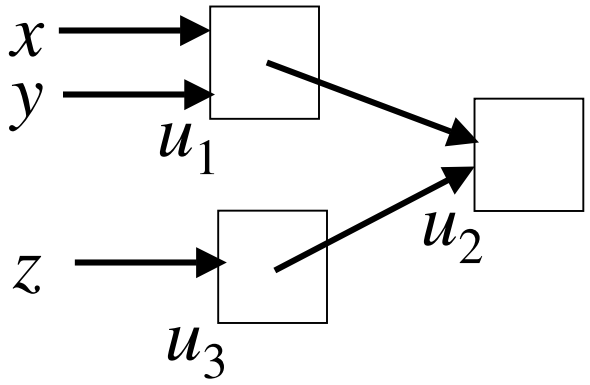
$$\varphi_y^{[x = \text{null}]}(v) \triangleq y(v)$$

	$x(u)$	$y(u)$	$z(u)$
u_1	1	1	0
u_2	0	0	0
u_3	0	0	1

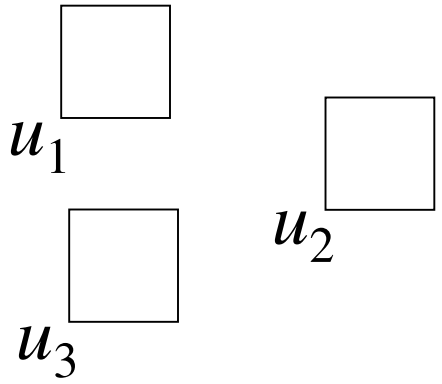
	$\varphi_x(u)$	$\varphi_y(u)$	$\varphi_z(u)$
u_1	0		
u_2	0		
u_3	0		

Predicate-Alteration Formulas for x = null

Old:



New:



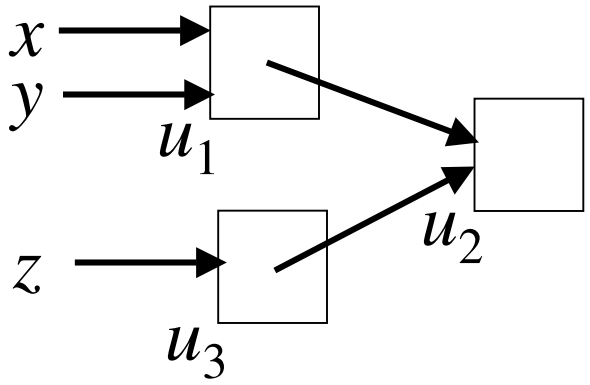
$$\varphi_y^{[x = \text{null}]}(v) \triangleq \boxed{y(v)}$$

	$x(u)$	$y(u)$	$z(u)$
u_1	1	1	0
u_2	0	0	0
u_3	0	0	1

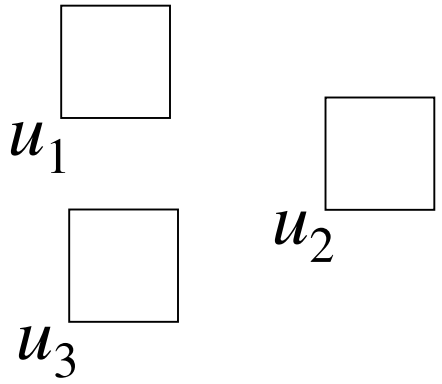
	$\varphi_x(u)$	$\varphi_y(u)$	$\varphi_z(u)$
u_1	0		
u_2	0		
u_3	0		

Predicate-Alteration Formulas for x = null

Old:



New:



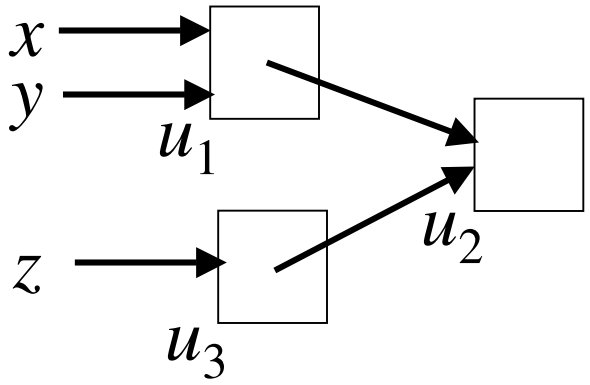
$$\varphi_y^{[x = \text{null}]}(v) \triangleq y(v)$$

	$x(u)$	$y(u)$	$z(u)$
u_1	1	1	0
u_2	0	0	0
u_3	0	0	1

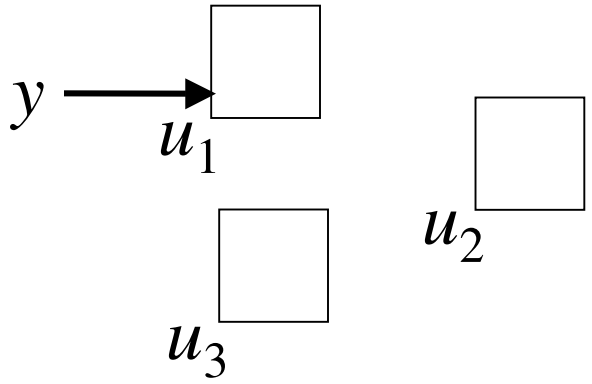
	$\varphi_x(u)$	$\varphi_y(u)$	$\varphi_z(u)$
u_1	0	1	
u_2	0	0	
u_3	0	0	

Predicate-Alteration Formulas for x = null

Old:



New:



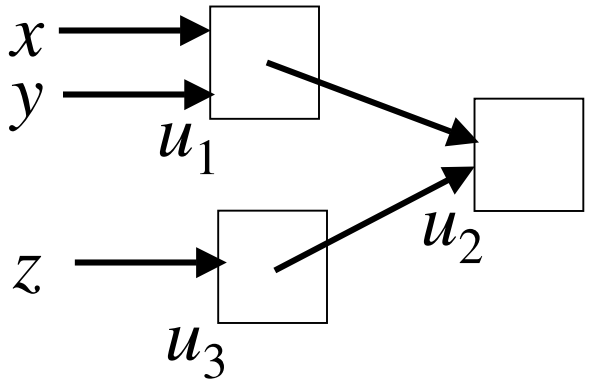
$$\varphi_y^{[x = \text{null}]}(v) \triangleq y(v)$$

	$x(u)$	$y(u)$	$z(u)$
u_1	1	1	0
u_2	0	0	0
u_3	0	0	1

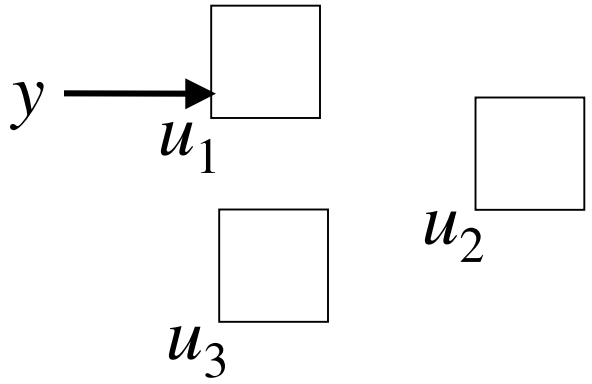
	$\varphi_x(u)$	$\varphi_y(u)$	$\varphi_z(u)$
u_1	0	1	
u_2	0	0	
u_3	0	0	

Predicate-Alteration Formulas for x = null

Old:



New:

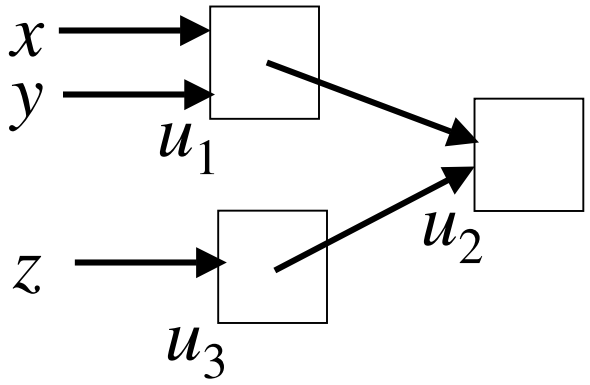


	$x(u)$	$y(u)$	$z(u)$
u_1	1	1	0
u_2	0	0	0
u_3	0	0	1

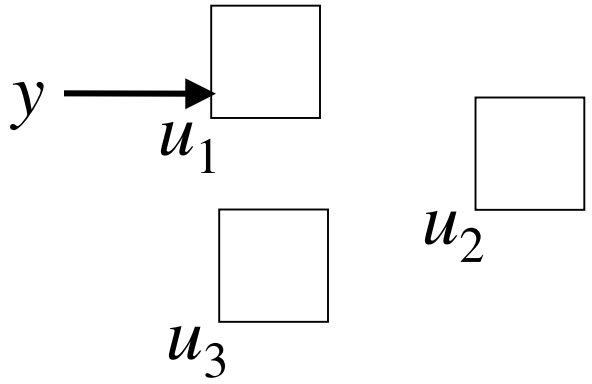
	$\varphi_x(u)$	$\varphi_y(u)$	$\varphi_z(u)$
u_1	0	1	
u_2	0	0	
u_3	0	0	

Predicate-Alteration Formulas for x = null

Old:



New:



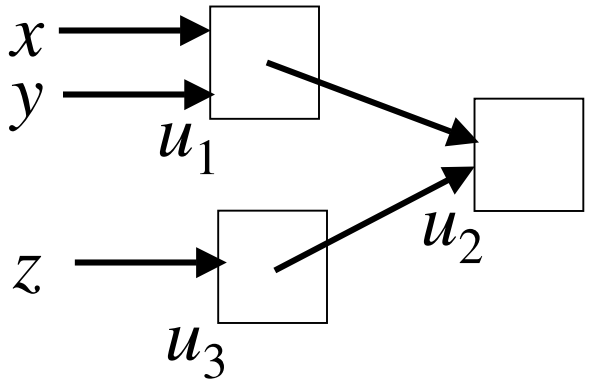
$$\varphi_z^{[x = \text{null}]}(v) \triangleq z(v)$$

	$x(u)$	$y(u)$	$z(u)$
u_1	1	1	0
u_2	0	0	0
u_3	0	0	1

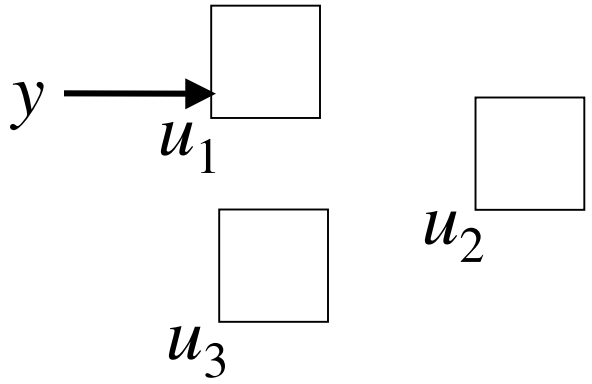
	$\varphi_x(u)$	$\varphi_y(u)$	$\varphi_z(u)$
u_1	0	1	
u_2	0	0	
u_3	0	0	

Predicate-Alteration Formulas for x = null

Old:



New:



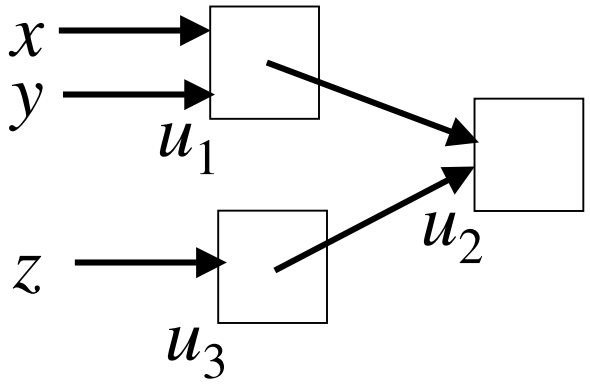
$$\varphi_z^{[x = \text{null}]}(v) \triangleq \boxed{z(v)}$$

	$x(u)$	$y(u)$	$z(u)$
u_1	1	1	0
u_2	0	0	0
u_3	0	0	1

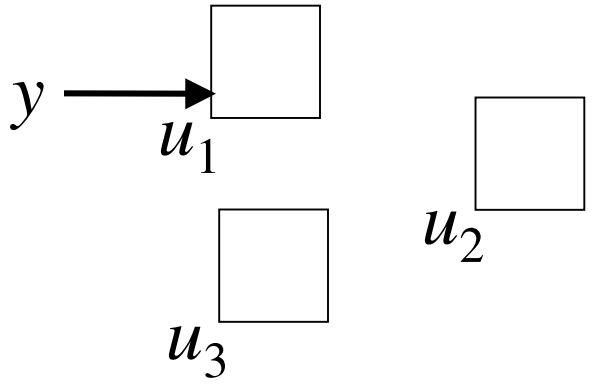
	$\varphi_x(u)$	$\varphi_y(u)$	$\varphi_z(u)$
u_1	0	1	
u_2	0	0	
u_3	0	0	

Predicate-Alteration Formulas for x = null

Old:



New:



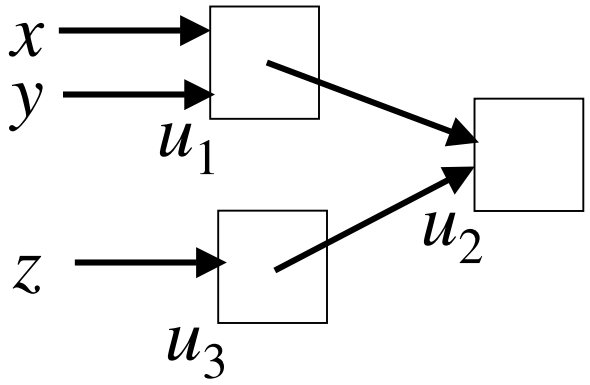
$$\varphi_z^{[x = \text{null}]}(v) \triangleq z(v)$$

	$x(u)$	$y(u)$	$z(u)$
u_1	1	1	0
u_2	0	0	0
u_3	0	0	1

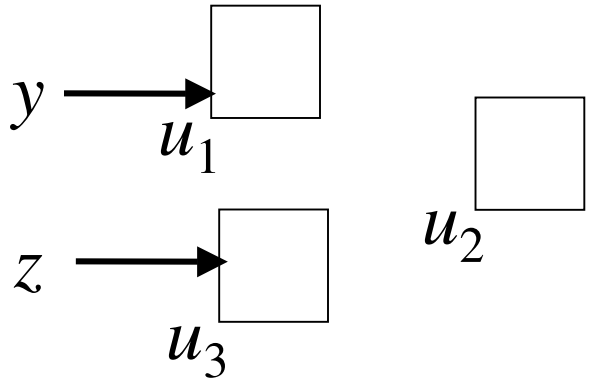
	$\varphi_x(u)$	$\varphi_y(u)$	$\varphi_z(u)$
u_1	0	1	0
u_2	0	0	0
u_3	0	0	1

Predicate-Alteration Formulas for x = null

Old:



New:



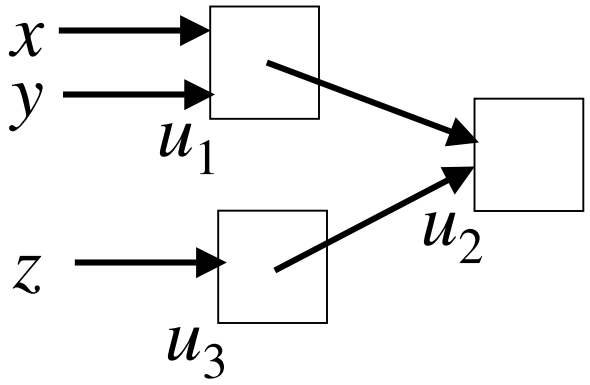
$$\varphi_z^{[x = \text{null}]}(v) \triangleq z(v)$$

	$x(u)$	$y(u)$	$z(u)$
u_1	1	1	0
u_2	0	0	0
u_3	0	0	1

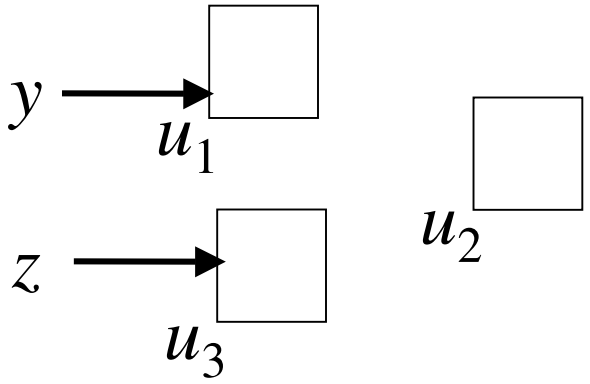
	$\varphi_x(u)$	$\varphi_y(u)$	$\varphi_z(u)$
u_1	0	1	0
u_2	0	0	0
u_3	0	0	1

Predicate-Alteration Formulas for x = null

Old:



New:

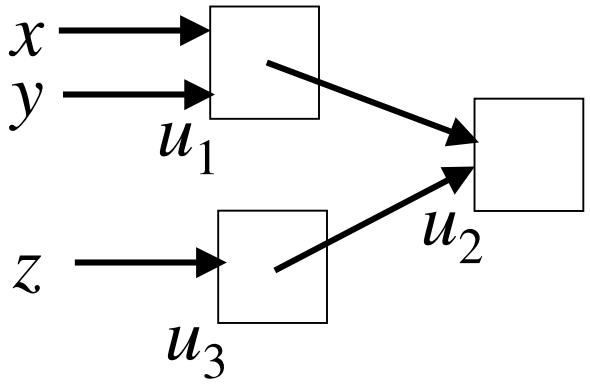


	$x(u)$	$y(u)$	$z(u)$
u_1	1	1	0
u_2	0	0	0
u_3	0	0	1

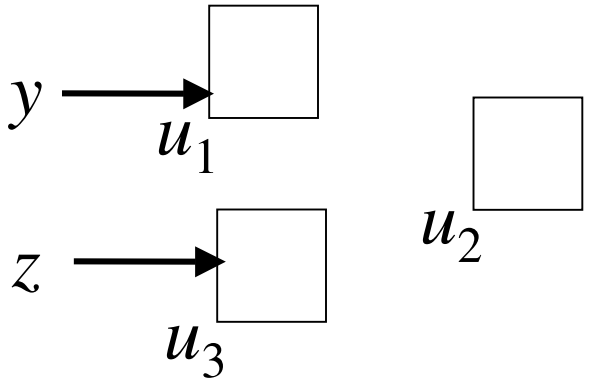
	$\varphi_x(u)$	$\varphi_y(u)$	$\varphi_z(u)$
u_1	0	1	0
u_2	0	0	0
u_3	0	0	1

Predicate-Alteration Formulas for x = null

Old:

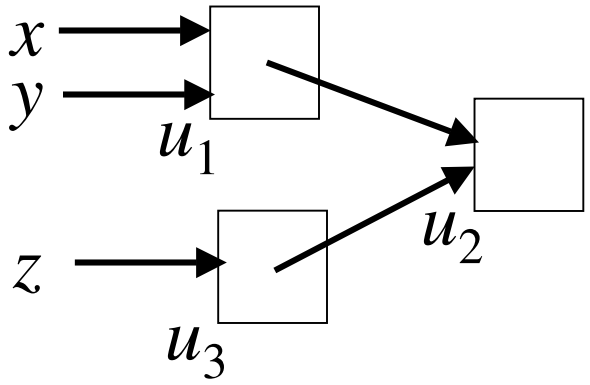


New:

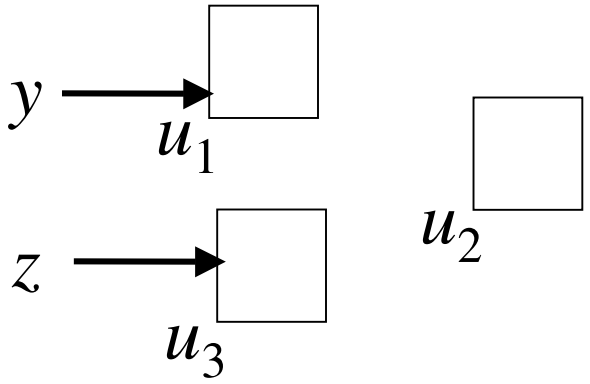


Predicate-Alteration Formulas for x = null

Old:



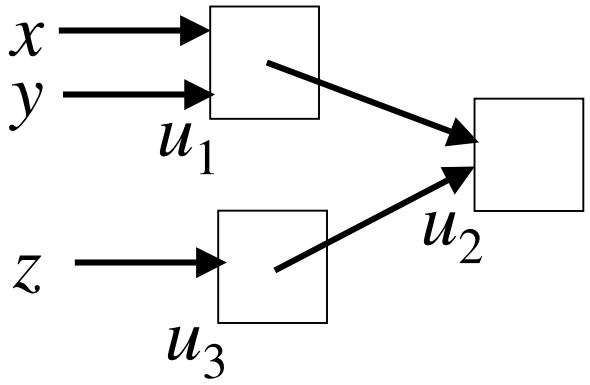
New:



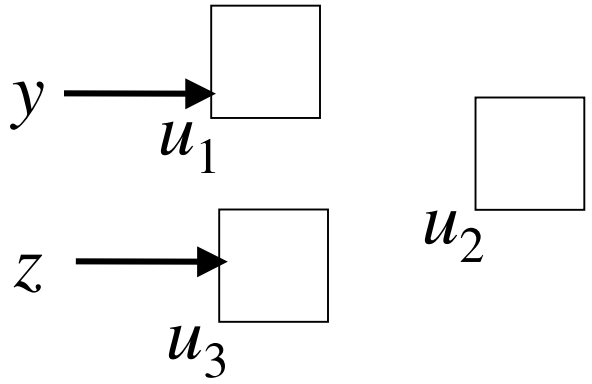
n	u_1	u_2	u_3
u_1	0	1	0
u_2	0	0	0
u_3	0	1	0

Predicate-Alteration Formulas for x = null

Old:



New:

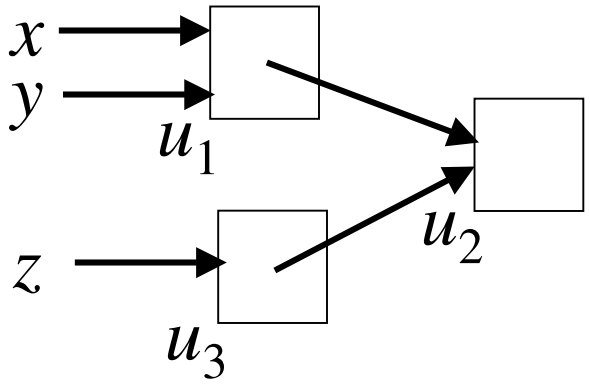


$$\varphi_n^{[x = \text{null}]}(v_1, v_2) \triangleq n(v_1, v_2)$$

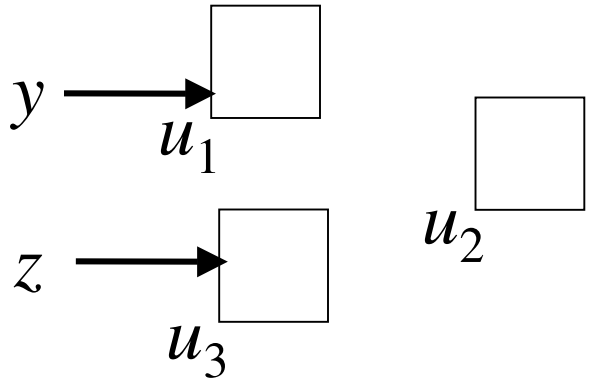
n	u_1	u_2	u_3
u_1	0	1	0
u_2	0	0	0
u_3	0	1	0

Predicate-Alteration Formulas for x = null

Old:



New:



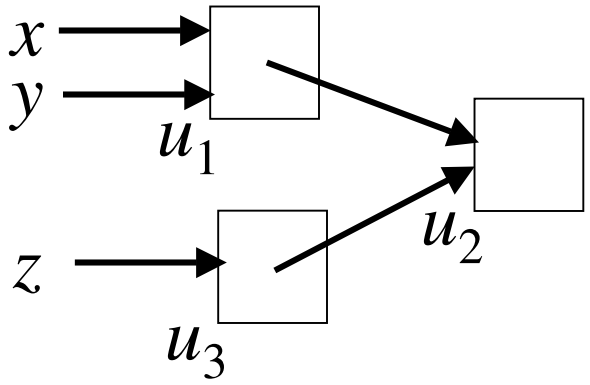
$$\varphi_n^{[x = \text{null}]}(v_1, v_2) \triangleq n(v_1, v_2)$$

n	u_1	u_2	u_3
u_1	0	1	0
u_2	0	0	0
u_3	0	1	0

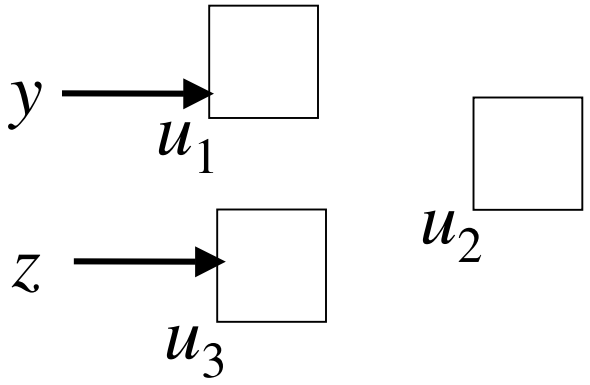
φ_n	u_1	u_2	u_3
u_1			
u_2			
u_3			

Predicate-Alteration Formulas for x = null

Old:



New:



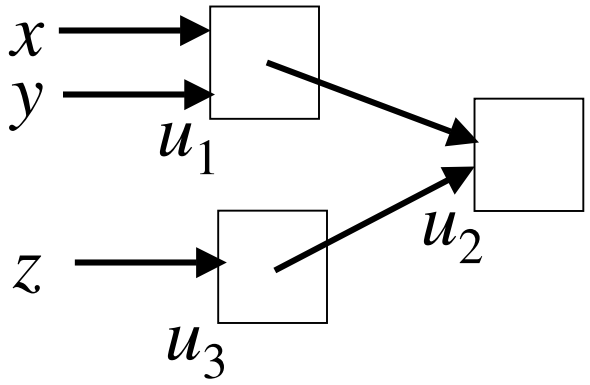
$$\varphi_n^{[x = \text{null}]}(v_1, v_2) \triangleq \boxed{n(v_1, v_2)}$$

n	u_1	u_2	u_3
u_1	0	1	0
u_2	0	0	0
u_3	0	1	0

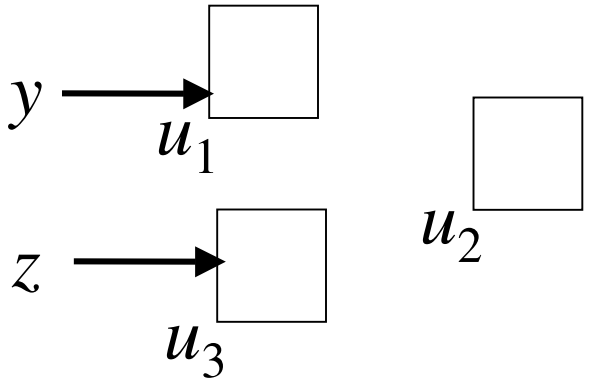
φ_n	u_1	u_2	u_3
u_1			
u_2			
u_3			

Predicate-Alteration Formulas for x = null

Old:



New:



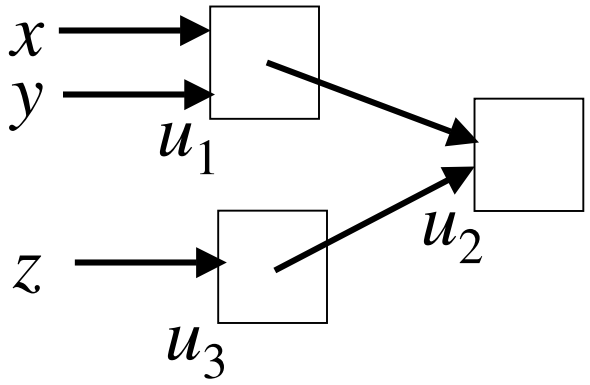
$$\varphi_n^{[x = \text{null}]}(v_1, v_2) \triangleq n(v_1, v_2)$$

n	u_1	u_2	u_3
u_1	0	1	0
u_2	0	0	0
u_3	0	1	0

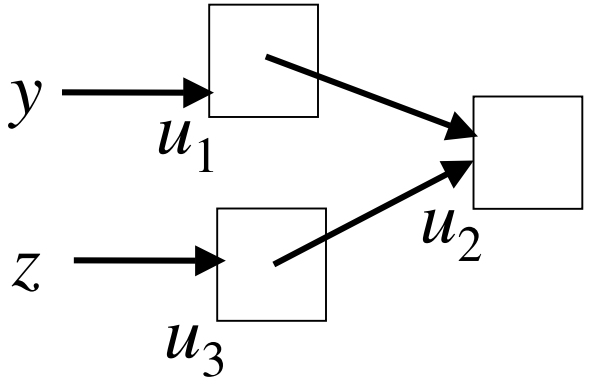
φ_n	u_1	u_2	u_3
u_1	0	1	0
u_2	0	0	0
u_3	0	1	0

Predicate-Alteration Formulas for x = null

Old:



New:



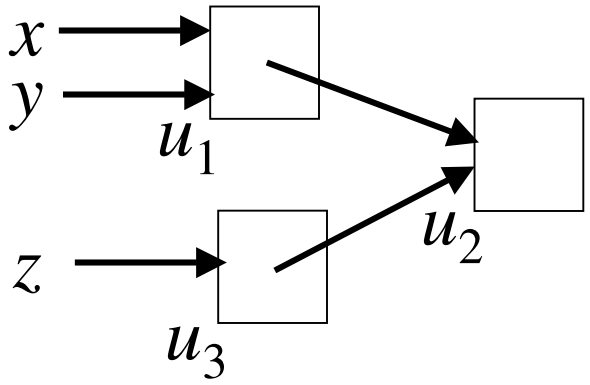
$$\varphi_n^{[x = \text{null}]}(v_1, v_2) \triangleq n(v_1, v_2)$$

n	u_1	u_2	u_3
u_1	0	1	0
u_2	0	0	0
u_3	0	1	0

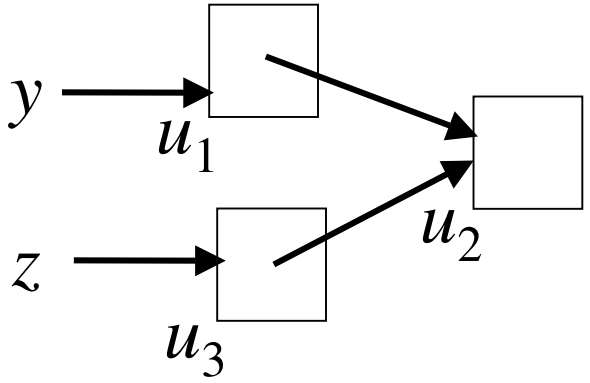
φ_n	u_1	u_2	u_3
u_1	0	1	0
u_2	0	0	0
u_3	0	1	0

Predicate-Alteration Formulas for x = null

Old:



New:

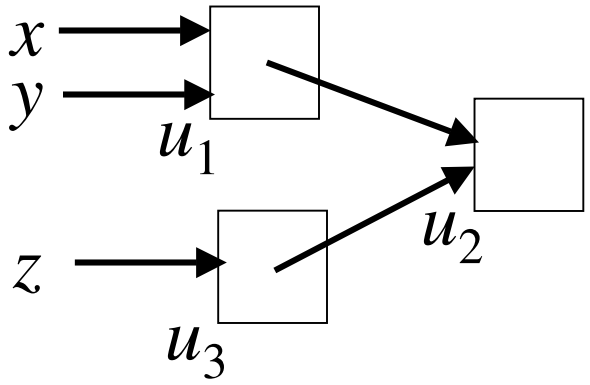


n	u_1	u_2	u_3
u_1	0	1	0
u_2	0	0	0
u_3	0	1	0

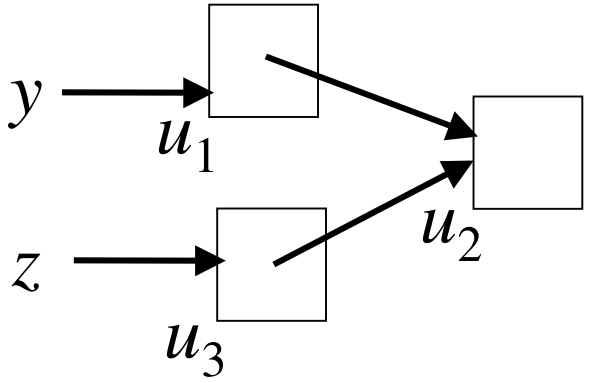
φ_n	u_1	u_2	u_3
u_1	0	1	0
u_2	0	0	0
u_3	0	1	0

Predicate-Alteration Formulas for x = null

Old:



New:

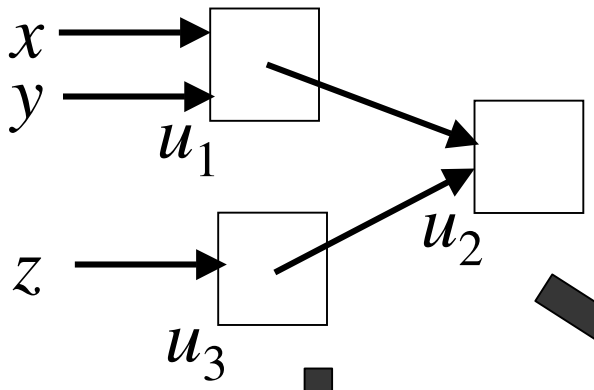


	$\varphi_x(u)$	$\varphi_y(u)$	$\varphi_z(u)$
u_1	0	1	0
u_2	0	0	0
u_3	0	0	1

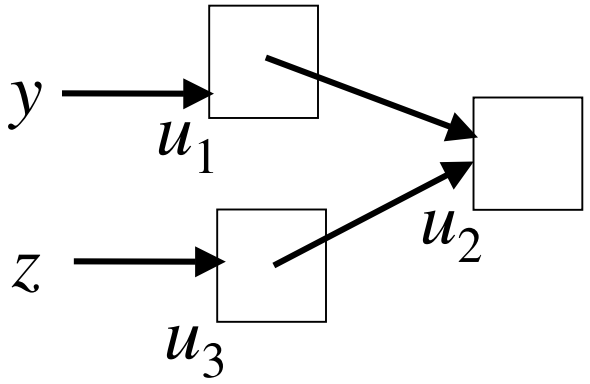
φ_n	u_1	u_2	u_3
u_1	0	1	0
u_2	0	0	0
u_3	0	1	0

Predicate-Alteration Formulas for x = null

Old:



New:

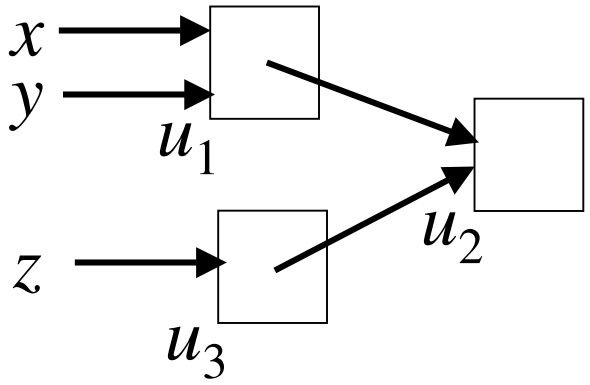


	$\varphi_x(u)$	$\varphi_y(u)$	$\varphi_z(u)$
u_1	0	1	0
u_2	0	0	0
u_3	0	0	1

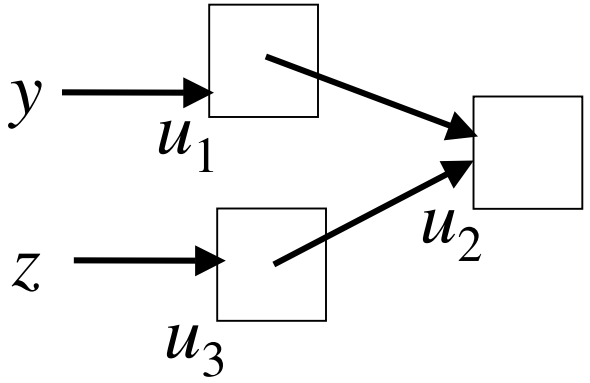
φ_n	u_1	u_2	u_3
u_1	0	1	0
u_2	0	0	0
u_3	0	1	0

Predicate-Alteration Formulas for x = null

Old:



New:

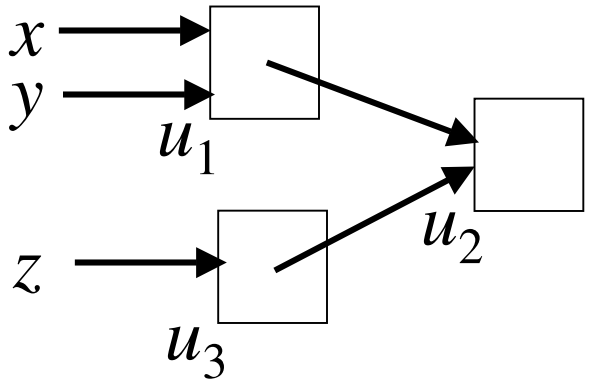


	$\varphi_x(u)$	$\varphi_y(u)$	$\varphi_z(u)$
u_1	0	1	0
u_2	0	0	0
u_3	0	0	1

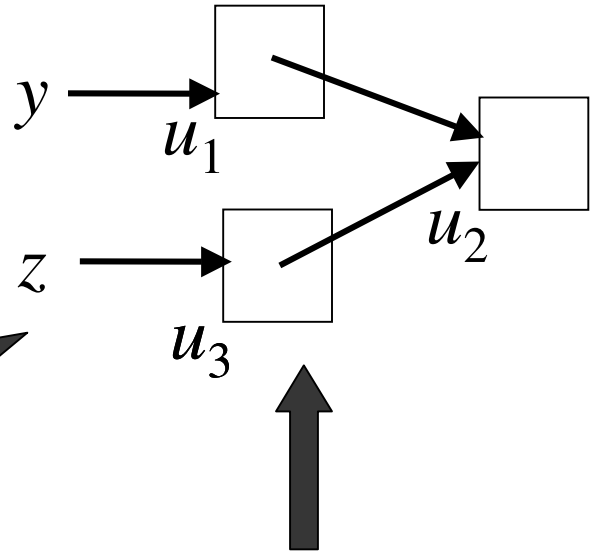
φ_n	u_1	u_2	u_3
u_1	0	1	0
u_2	0	0	0
u_3	0	1	0

Predicate-Alteration Formulas for x = null

Old:



New:

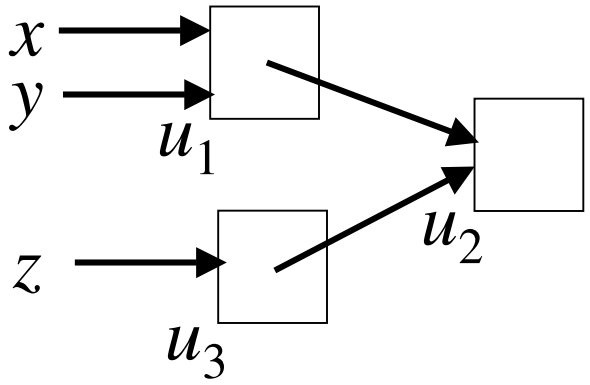


	$\varphi_x(u)$	$\varphi_y(u)$	$\varphi_z(u)$
u_1	0	1	0
u_2	0	0	0
u_3	0	0	1

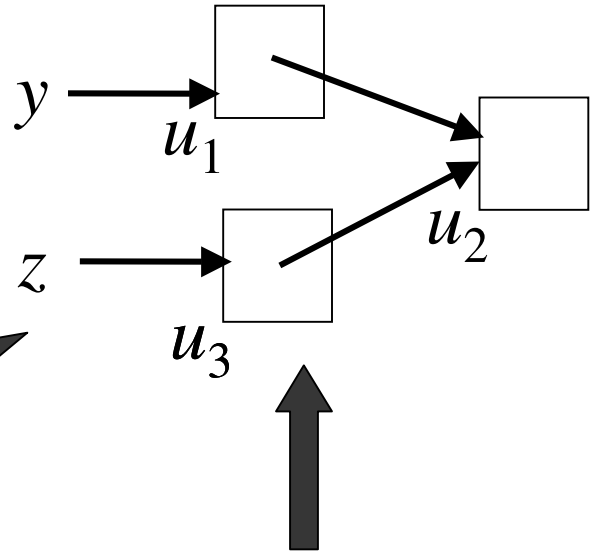
φ_n	u_1	u_2	u_3
u_1	0	1	0
u_2	0	0	0
u_3	0	1	0

Predicate-Alteration Formulas for x = null

Old:



New:



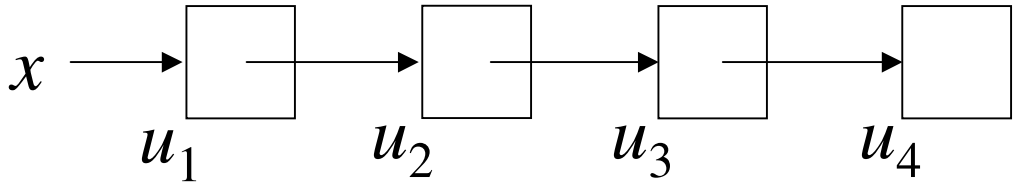
	$\varphi_x(u)$	$\varphi_y(u)$	$\varphi_z(u)$
u_1	0	1	0
u_2	0	0	0
u_3	0	0	1

φ_n	u_1	u_2	u_3
u_1	0	1	0
u_2	0	0	0
u_3	0	1	0

Outline

- Using logic to describe stores
- Using logic to express store transformations
- Forming abstractions of stores
- Three-valued logic
- Using three-valued logic to express transformations of abstract stores

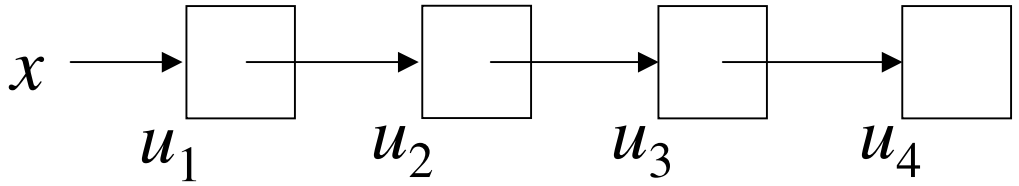
The Abstraction Principle



	$x(u)$	$y(u)$
u_1	1	0
u_2	0	0
u_3	0	0
u_4	0	0

n	u_1	u_2	u_3	u_4
u_1	0	1	0	0
u_2	0	0	1	0
u_3	0	0	0	1
u_4	0	0	0	0

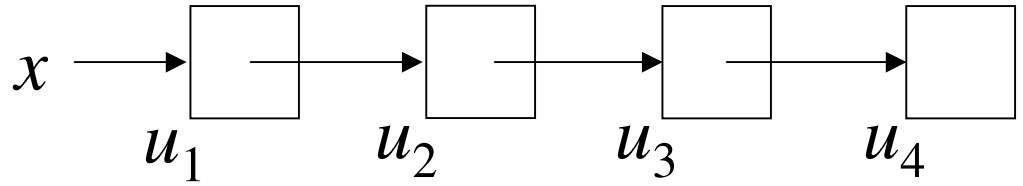
The Abstraction Principle



	$x(u)$	$y(u)$
u_1	1	0
u_2	0	0
u_3	0	0
u_4	0	0

n	u_1	u_2	u_3	u_4
u_1	0	1	0	0
u_2	0	0	1	0
u_3	0	0	0	1
u_4	0	0	0	0

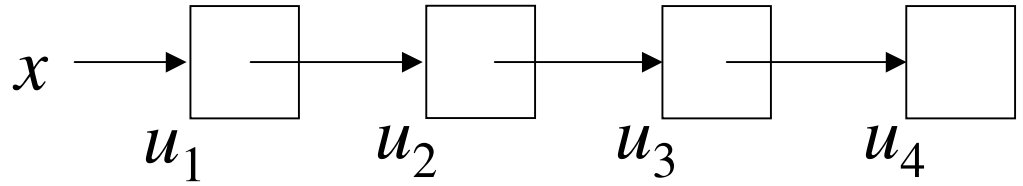
The Abstraction Principle



	$x(u)$	$y(u)$
u_1	1	0
u_2	0	0
u_3	0	0
u_4	0	0

n	u_1	u_2	u_3	u_4
u_1	0	1	0	0
u_2	0	0	1	0
u_3	0	0	0	1
u_4	0	0	0	0

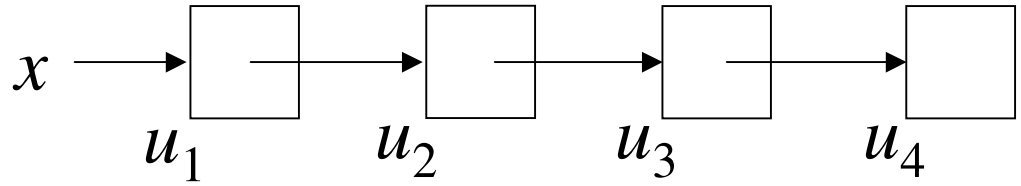
The Abstraction Principle



	$x(u)$	$y(u)$
u_1	{1}	{0}
u_{234}	{0}	{0}

n	u_1	u_2	u_3	u_4
u_1	0	1	0	0
u_2	0	0	1	0
u_3	0	0	0	1
u_4	0	0	0	0

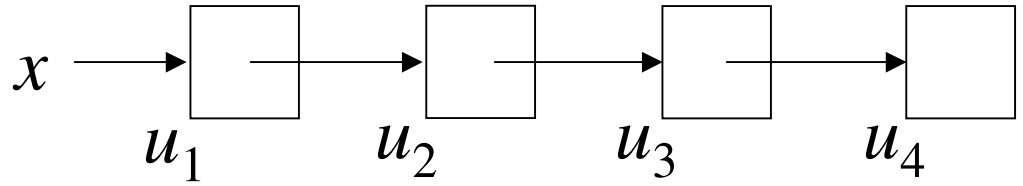
The Abstraction Principle



	$x(u)$	$y(u)$
u_1	{1}	{0}
u_{234}	{0}	{0}

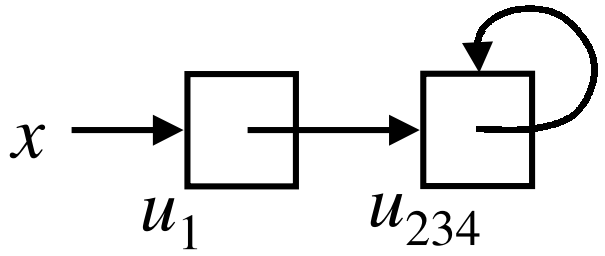
n	u_1	u_{234}
u_1	{0}	{0,1}
u_{234}	{0}	{0,1}

The Abstraction Principle

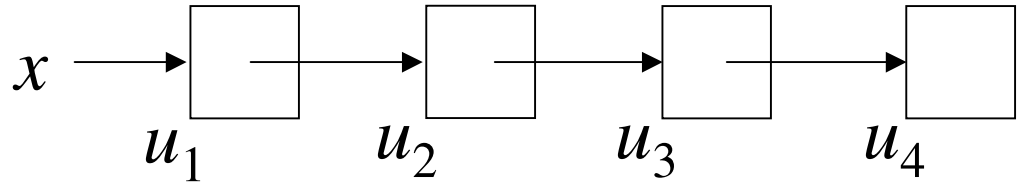


	$x(u)$	$y(u)$
u_1	{1}	{0}
u_{234}	{0}	{0}

n	u_1	u_{234}
u_1	{0}	{0,1}
u_{234}	{0}	{0,1}

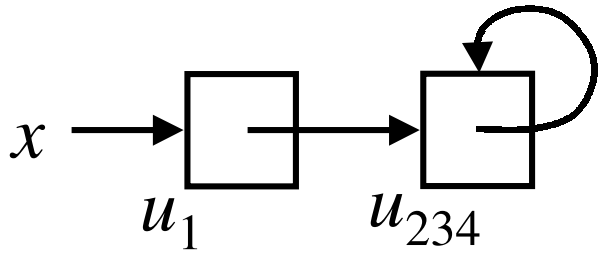


The Abstraction Principle



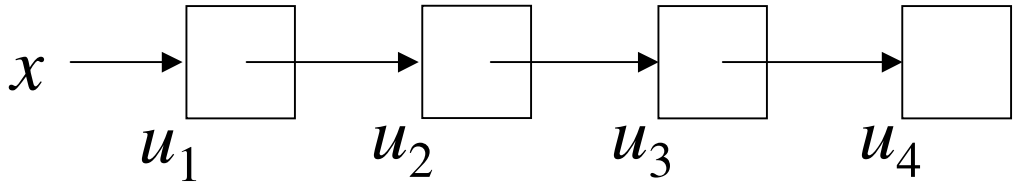
	$x(u)$	$y(u)$
u_1	{1}	{0}
u_{234}	{0}	{0}

n	u_1	u_{234}
u_1	{0}	{0,1}
u_{234}	{0}	{0,1}

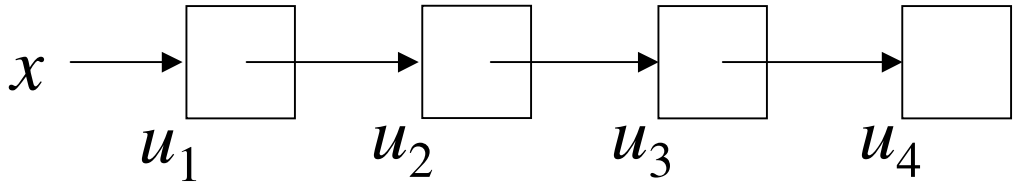


Summary Information {0,1}

The Abstraction Principle

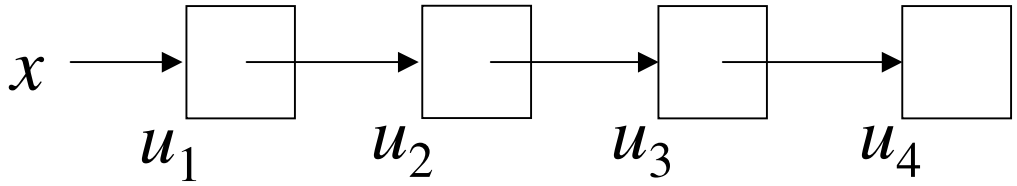


The Abstraction Principle



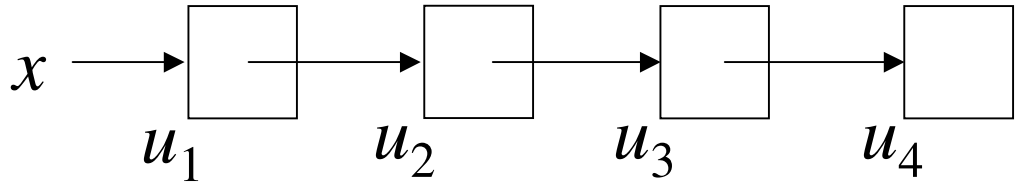
	$is(u)$
u_1	0
u_2	0
u_3	0
u_4	0

The Abstraction Principle



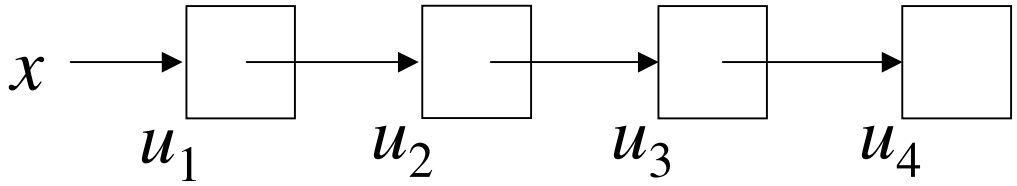
	$is(u)$
u_1	0
u_2	0
u_3	0
u_4	0

The Abstraction Principle



	$is(u)$
u_1	{0}
u_{234}	{0}

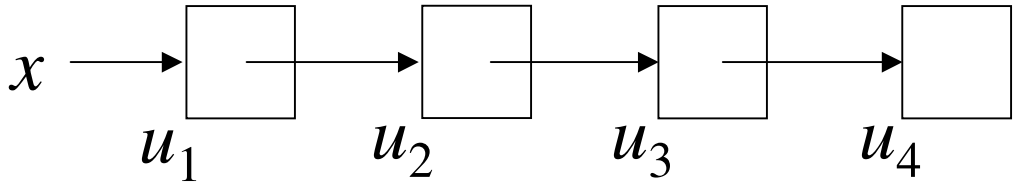
The Abstraction Principle



	$is(u)$
u_1	$\{0\}$
u_{234}	$\{0\}$

$=$	u_1	u_2	u_3	u_4
u_1	1	0	0	0
u_2	0	1	0	0
u_3	0	0	1	0
u_4	0	0	0	1

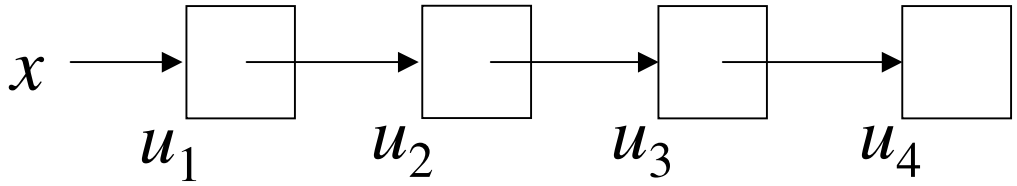
The Abstraction Principle



	$is(u)$
u_1	$\{0\}$
u_{234}	$\{0\}$

$=$	u_1	u_2	u_3	u_4
u_1	1	0	0	0
u_2	0	1	0	0
u_3	0	0	1	0
u_4	0	0	0	1

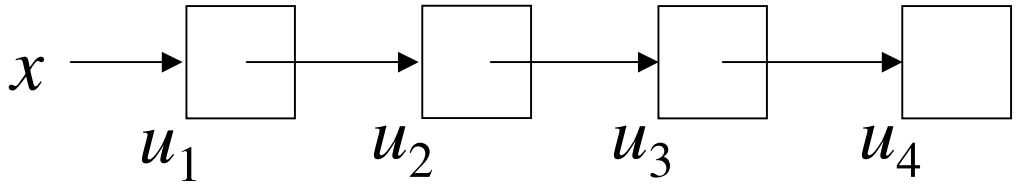
The Abstraction Principle



	$is(u)$
u_1	$\{0\}$
u_{234}	$\{0\}$

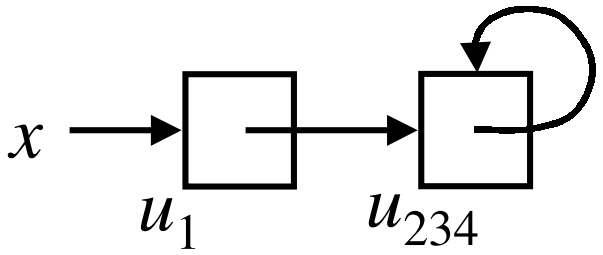
$=$	u_1	u_{234}
u_1	$\{1\}$	$\{0\}$
u_{234}	$\{0\}$	$\{0,1\}$

The Abstraction Principle

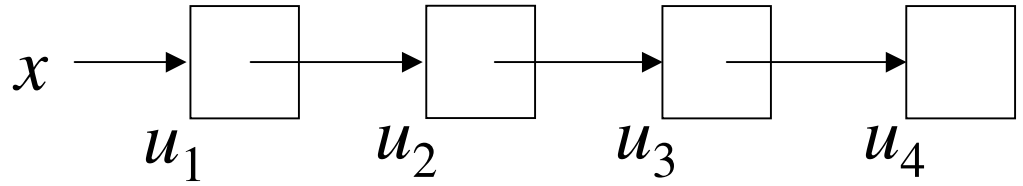


	$is(u)$
u_1	$\{0\}$
u_{234}	$\{0\}$

$=$	u_1	u_{234}
u_1	$\{1\}$	$\{0\}$
u_{234}	$\{0\}$	$\{0,1\}$

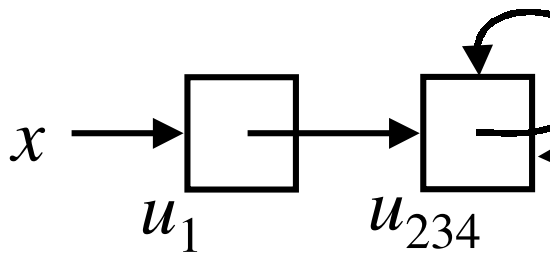


The Abstraction Principle



	$is(u)$
u_1	{0}
u_{234}	{0}

=	u_1	u_{234}
u_1	{1}	{0}
u_{234}	{0}	{0,1}



The Abstraction Principle

- Select some subset A of the predicate symbols
- Partition the individuals U^S of structure S into equivalence classes based on the values of their A predicates

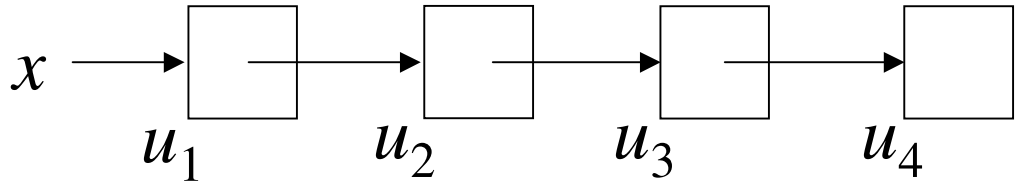
  $-u \mapsto [u]_A$
- Form the "union-quotient" of S with respect to $\{[u]_A \mid u \in U^S\}$

Example

- $A = \{v \mid v$ is a program variable$\}$
  - [Chase, Wegman, & Zadeck 90]
  - [Sagiv, Reps, & Wilhelm 96, 98]

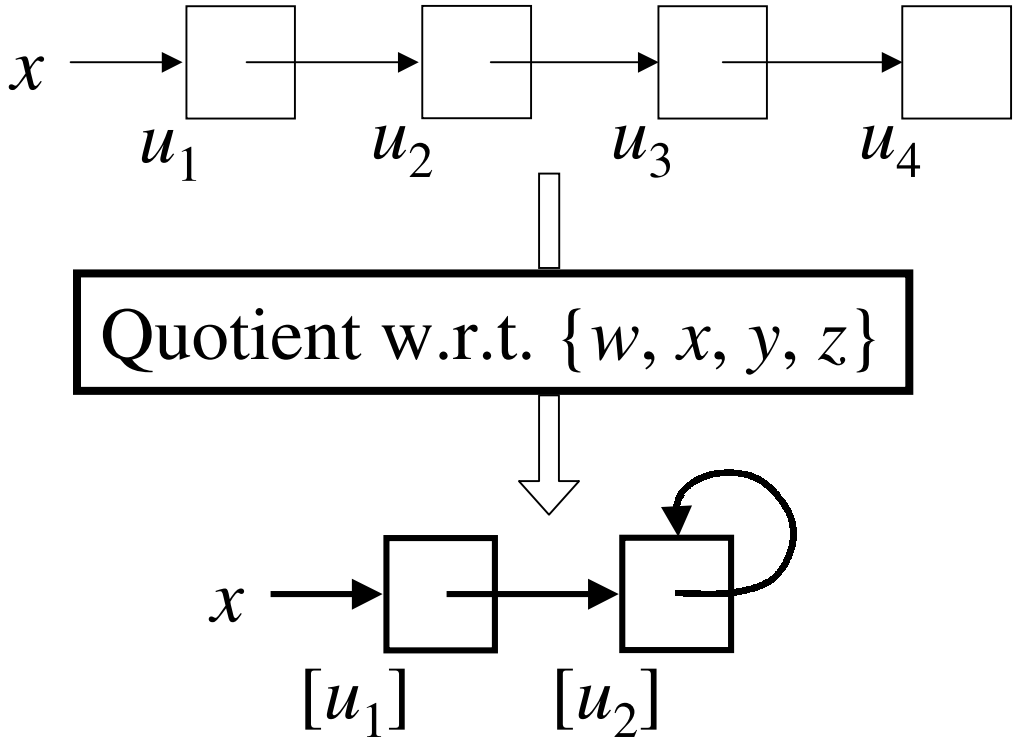
Example

- $A = \{v \mid v \text{ is a program variable}\}$
  - [Chase, Wegman, & Zadeck 90]
  - [Sagiv, Reps, & Wilhelm 96, 98]



Example

- $A = \{v \mid v \text{ is a program variable}\}$
  - [Chase, Wegman, & Zadeck 90]
  - [Sagiv, Reps, & Wilhelm 96, 98]



Outline

- Using logic to describe stores
- Using logic to express store transformations
- Forming abstractions of stores
- Three-valued logic
- Using three-valued logic to express transformations of abstract stores

Two- vs. Three-Valued Logic

$\{1\} \sqsubsetneq_3 \{0,1\}$

Two- vs. Three-Valued Logic

Two-valued logic

0 1

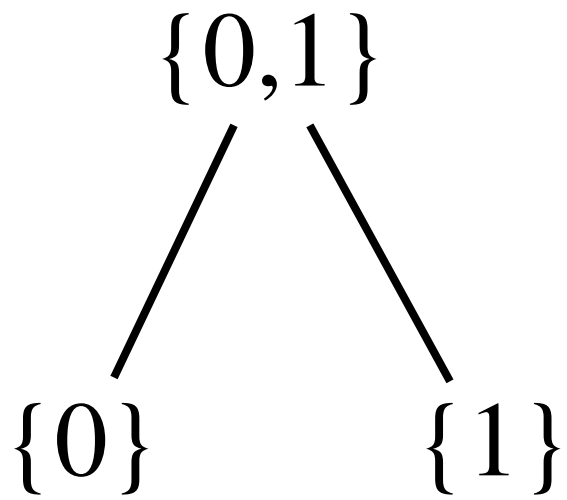
$\{1\} \sqsubsetneq_3 \{0,1\}$

Two- vs. Three-Valued Logic

Two-valued logic

0 1

Three-valued logic



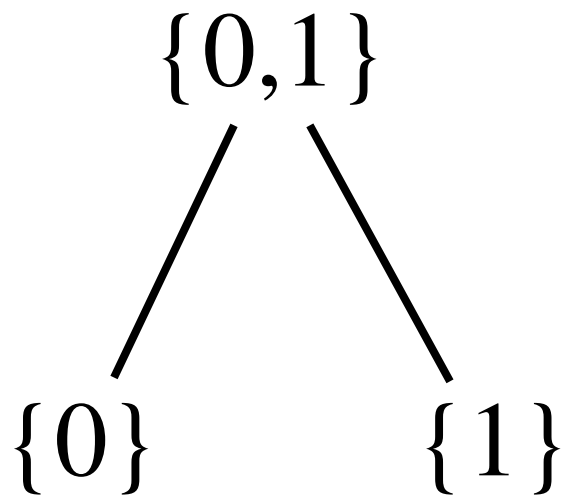
$\{1\} \sqsubsetneq_3 \{0,1\}$

Two- vs. Three-Valued Logic

Two-valued logic

0 1

Three-valued logic



$\{0\} \sqsubsetneq_3 \{0,1\}$

$\{1\} \sqsubsetneq_3 \{0,1\}$

Two- vs. Three-Valued Logic

Two- vs. Three-Valued Logic

Two-valued logic

Two- vs. Three-Valued Logic

Two-valued logic

$\wedge$	1	0
1	1	0
0	0	0

Two- vs. Three-Valued Logic

Two-valued logic

$\wedge$	1	0
1	1	0
0	0	0

$\vee$	1	0
1	1	1
0	1	0

Two- vs. Three-Valued Logic

Two-valued logic

$\wedge$	1	0
1	1	0
0	0	0

$\vee$	1	0
1	1	1
0	1	0

Three-valued logic

Two- vs. Three-Valued Logic

Two-valued logic

$\wedge$	1	0
1	1	0
0	0	0

$\vee$	1	0
1	1	1
0	1	0

Three-valued logic

$\wedge$	{1}	{0,1}	{0}
{1}	{1}	{0,1}	{0}
{0,1}	{0,1}	{0,1}	{0}
{0}	{0}	{0}	{0}

Two- vs. Three-Valued Logic

Two-valued logic

$\wedge$	1	0
1	1	0
0	0	0

$\vee$	1	0
1	1	1
0	1	0

Three-valued logic

$\wedge$	{1}	{0,1}	{0}
{1}	{1}	{0,1}	{0}
{0,1}	{0,1}	{0,1}	{0}
{0}	{0}	{0}	{0}

Two- vs. Three-Valued Logic

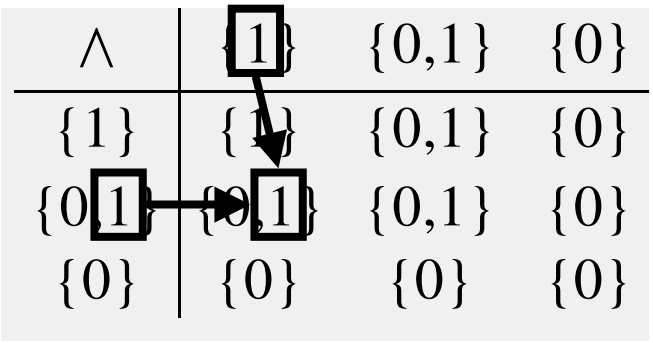
Two-valued logic

$\wedge$	1	0
1	1	0
0	0	0

$\vee$	1	0
1	1	1
0	1	0

Three-valued logic

$\wedge$	{1}	{0,1}	{0}
{1}	{1}	{0,1}	{0}
{0,1}	{0,1}	{0,1}	{0}
{0}	{0}	{0}	{0}



Two- vs. Three-Valued Logic

Two-valued logic

$\wedge$	1	0
1	1	0
0	0	0

$\vee$	1	0
1	1	1
0	1	0

Three-valued logic

$\wedge$	{1}	{0,1}	{0}
{1}	{1}	{0,1}	{0}
{0,1}	{0,1}	{0,1}	{0}
{0}	{0}	{0}	{0}

$\vee$	{1}	{0,1}	{0}
{1}	{1}	{1}	{1}
{0,1}	{1}	{0,1}	{0,1}
{0}	{1}	{0,1}	{0}

Two- vs. Three-Valued Logic

Two-valued logic

$\wedge$	1	0
1	1	0
0	0	0

$\vee$	1	0
1	1	1
0	1	0

Three-valued logic

$\wedge$	{1}	{0,1}	{0}
{1}	{1}	{0,1}	{0}
{0,1}	{0,1}	{0,1}	{0}
{0}	{0}	{0}	{0}

$\vee$	{1}	{0,1}	{0}
{1}	{1}	{1}	{1}
{0,1}	{1}	{0,1}	{0,1}
{0}	{1}	{0,1}	{0}

Two- vs. Three-Valued Logic

Two-valued logic

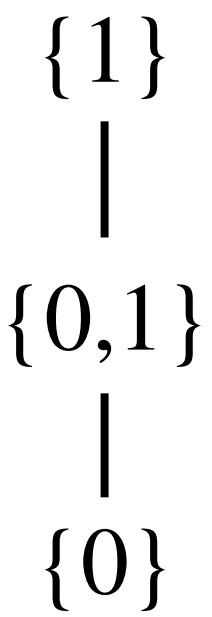
$\wedge$	1	0
1	1	0
0	0	0

$\vee$	1	0
1	1	1
0	1	0

Three-valued logic

$\wedge$	{1}	{0,1}	{0}
{1}	{1}	{0,1}	{0}
{0,1}	{0,1}	{0,1}	{0}
{0}	{0}	{0}	{0}

$\vee$	{1}	{0,1}	{0}
{1}	{1}	{1}	{1}
{0,1}	{1}	{0,1}	{0,1}
{0}	{1}	{0,1}	{0}

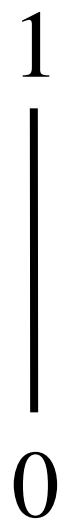


Two- vs. Three-Valued Logic

Two-valued logic

$\wedge$	1	0
1	1	0
0	0	0

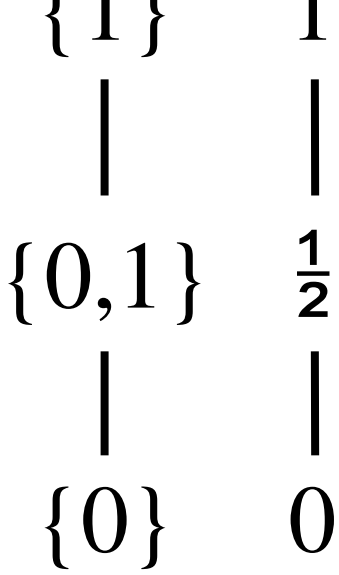
$\vee$	1	0
1	1	1
0	1	0



Three-valued logic

$\wedge$	{1}	{0,1}	{0}
{1}	{1}	{0,1}	{0}
{0,1}	{0,1}	{0,1}	{0}
{0}	{0}	{0}	{0}

$\vee$	{1}	{0,1}	{0}
{1}	{1}	{1}	{1}
{0,1}	{1}	{0,1}	{0,1}
{0}	{1}	{0,1}	{0}



First-Order Logic (Semantics)

- Truth values: 0, 1, $\frac{1}{2}$
- Logical structures
  - Individuals: $U = \{u_1, u_2, \ldots, u_n\}$
  - Predicates: $[\![p_i]\!]: U^{arity(p_i)} \rightarrow \{0, 1, \frac{1}{2}\}$

First-Order Logic (Semantics)

- Truth values: 0, 1, $\underline{\mathbf{\frac{1}{2}}}$
- Logical structures
  - Individuals: $U = \{u_1, u_2, \ldots, u_n\}$
  - Predicates: $[\![p_i]\!]: U^{arity(p_i)} \rightarrow \{0, 1, \underline{\mathbf{\frac{1}{2}}}\}$

First-Order Logic (Semantics)

- Truth values: 0, 1, $\underline{\frac{1}{2}}$
- Logical structures
  - Individuals: $U = \{u_1, u_2, \ldots, u_n\}$
  - Predicates: $[\![p_i]\!]: U^{arity(p_i)} \rightarrow \{0, 1, \underline{\frac{1}{2}}\}$

<u>In Our Application</u>

3-valued logical structures = Abstract stores

The Abstraction Principle

- Select some subset A of the predicate symbols
- Partition the individuals U^S of structure S into equivalence classes based on the values of their A predicates

  $-u \mapsto [u]_A$
- Form the "union-quotient" of S with respect to $\{[u]_A \mid u \in U^S\}$

Abstraction Conserves Predicates

$$S \xrightarrow{Abs(A)} S^{\#} = S/[u]_A$$

$$u \mapsto [u]_A$$

$$[\![p]\!]^S (u_1, \ldots, u_k) \sqsubseteq_3 [\![p]\!]^{S^{\#}} ([u_1]_A, \ldots, [u_k]_A)$$

Abstraction Conserves Predicates

$$S \xrightarrow{Abs(A)} S^{\#} = S/[u]_A$$

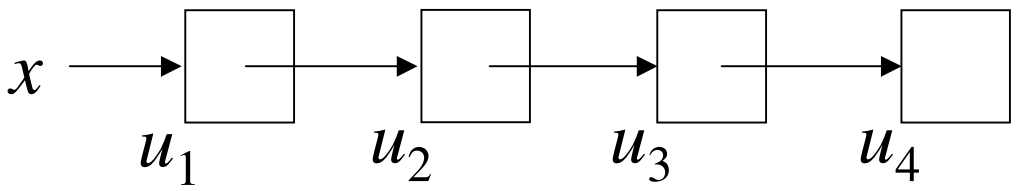
$$u \mapsto [u]_A$$

$$[\![p]\!]^S (u_1, \ldots, u_k) \sqsubseteq_3 [\![p]\!]^{S^{\#}} ([u_1]_A, \ldots, [u_k]_A)$$

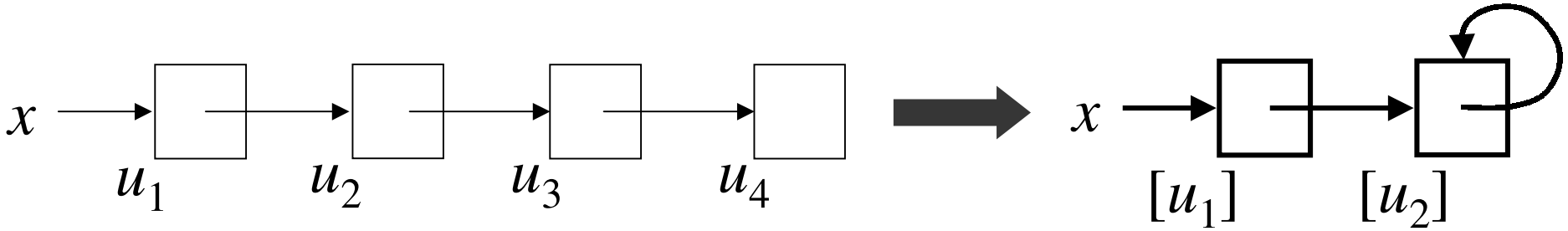
"Form the 'union-quotient' of S
with respect to $\{[u]_A \mid u \in U^S\}$"

$$[\![p]\!]^{S}(u_1,\ldots,u_k) \sqsubseteq_3 [\![p]\!]^{S^\#}([u_1]_A,\ldots,[u_k]_A)$$

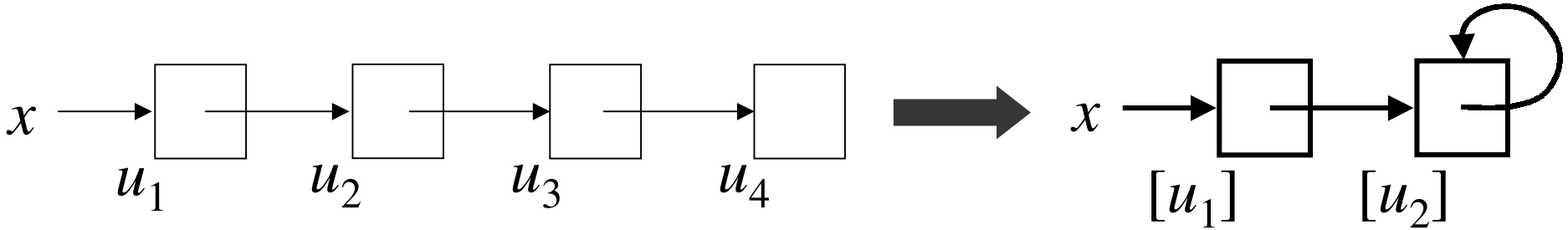
$$[\![p]\!]^{S}(u_1,\ldots,u_k) \sqsubseteq_3 [\![p]\!]^{S^\#}([u_1]_A,\ldots,[u_k]_A)$$



$$[\![p]\!]^{S}(u_1,\ldots,u_k) \sqsubseteq_3 [\![p]\!]^{S^\#}([u_1]_A,\ldots,[u_k]_A)$$

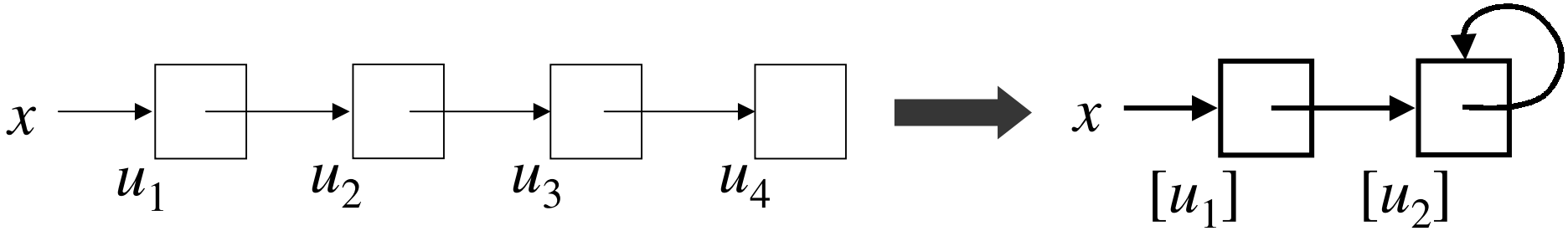


$$[\![p]\!]^{S}(u_1,\ldots,u_k) \sqsubseteq_3 [\![p]\!]^{S^{\#}}([u_1]_A,\ldots,[u_k]_A)$$



	$x(u)$	$y(u)$
u_1	1	0
u_2	0	0
u_3	0	0
u_4	0	0

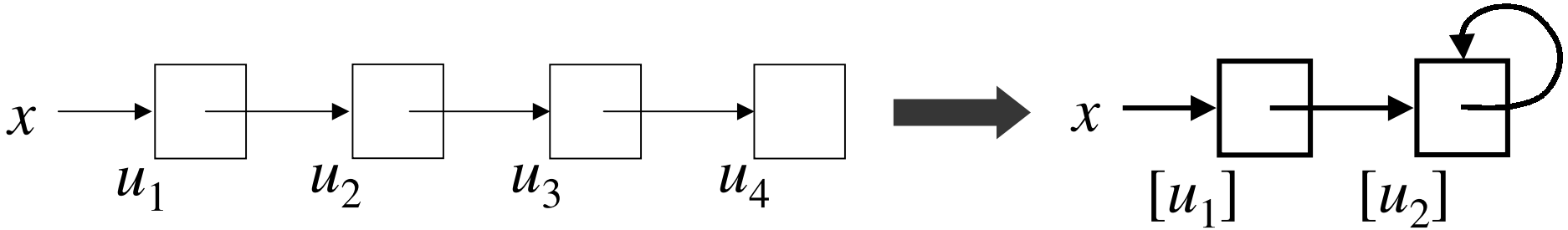
$$[\![p]\!]^{S}(u_1,\ldots,u_k) \sqsubseteq_3 [\![p]\!]^{S^{\#}}([u_1]_A,\ldots,[u_k]_A)$$



	$x(u)$	$y(u)$
u_1	1	0
u_2	0	0
u_3	0	0
u_4	0	0

	$x(u)$	$y(u)$
$[u_1]$	1	0
$[u_2]$	0	0

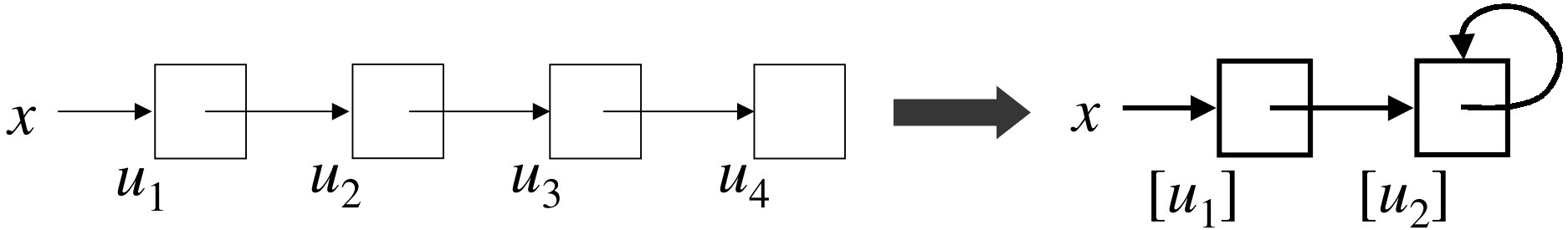
$$[\![p]\!]^{S}(u_1,\ldots,u_k) \sqsubseteq_3 [\![p]\!]^{S^\#}([u_1]_A,\ldots,[u_k]_A)$$



	$x(u)$	$y(u)$
u_1	1	0
u_2	0	0
u_3	0	0
u_4	0	0

	$x(u)$	$y(u)$
$[u_1]$	1	0
$[u_2]$	0	0

$$[\![p]\!]^{S}(u_1,\ldots,u_k) \sqsubseteq_3 [\![p]\!]^{S^\#}([u_1]_A,\ldots,[u_k]_A)$$

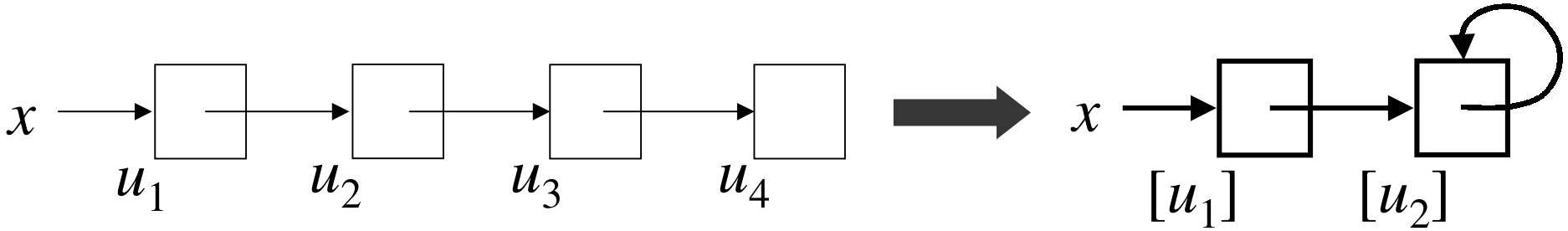


	$x(u)$	$y(u)$
u_1	1	0
u_2	0	0
u_3	0	0
u_4	0	0

	$x(u)$	$y(u)$
$[u_1]$	1	0
$[u_2]$	0	0

n	u_1	u_2	u_3	u_4
u_1	0	1	0	0
u_2	0	0	1	0
u_3	0	0	0	1
u_4	0	0	0	0

$$[\![p]\!]^{S}(u_1,\ldots,u_k) \sqsubseteq_3 [\![p]\!]^{S^{\#}}([u_1]_A,\ldots,[u_k]_A)$$



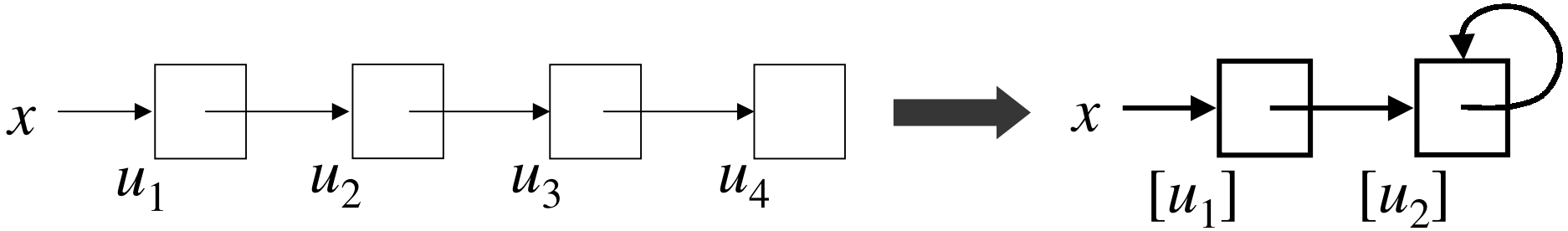
	$x(u)$	$y(u)$
u_1	1	0
u_2	0	0
u_3	0	0
u_4	0	0

	$x(u)$	$y(u)$
$[u_1]$	1	0
$[u_2]$	0	0

n	u_1	u_2	u_3	u_4
u_1	0	1	0	0
u_2	0	0	1	0
u_3	0	0	0	1
u_4	0	0	0	0

n	$[u_1]$	$[u_2]$
$[u_1]$	0	1/2
$[u_2]$	0	1/2

$$[\![p]\!]^{S}(u_1,\ldots,u_k) \sqsubseteq_3 [\![p]\!]^{S^\#}([u_1]_A,\ldots,[u_k]_A)$$



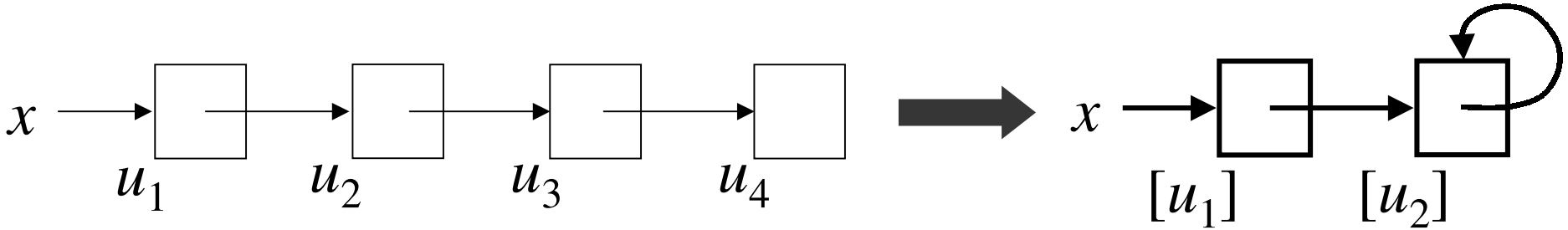
	$x(u)$	$y(u)$
u_1	1	0
u_2	0	0
u_3	0	0
u_4	0	0

	$x(u)$	$y(u)$
$[u_1]$	1	0
$[u_2]$	0	0

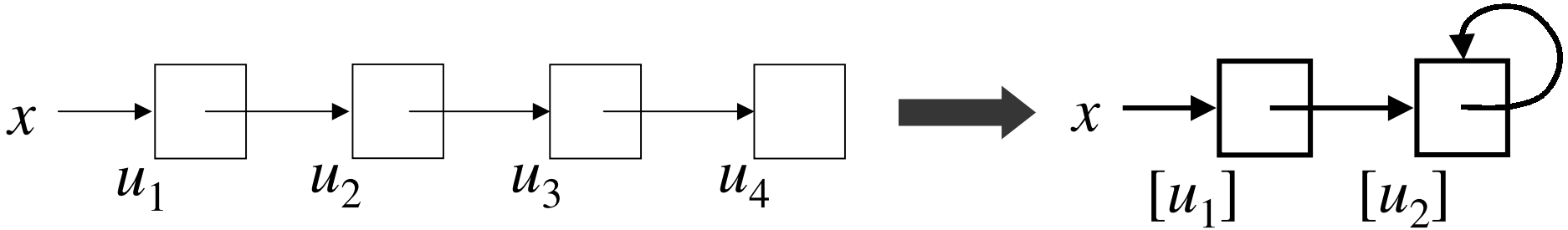
n	u_1	u_2	u_3	u_4
u_1	0	1	0	0
u_2	0	0	1	0
u_3	0	0	0	1
u_4	0	0	0	0

n	$[u_1]$	$[u_2]$
$[u_1]$	0	1/2
$[u_2]$	0	1/2

$$[\![p]\!]^{S}(u_1,\ldots,u_k) \sqsubseteq_3 [\![p]\!]^{S^\#}([u_1]_A,\ldots,[u_k]_A)$$

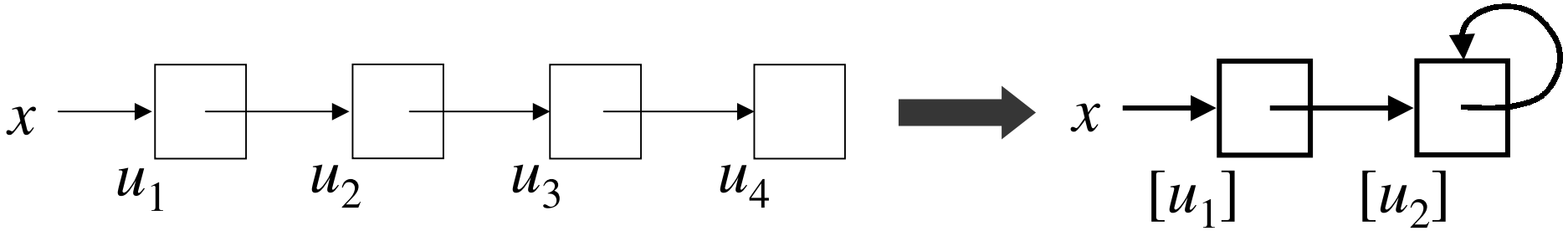


$$[\![p]\!]^{S}(u_1,\ldots,u_k) \sqsubseteq_3 [\![p]\!]^{S^\#}([u_1]_A,\ldots,[u_k]_A)$$



	$is(u)$
u_1	0
u_2	0
u_3	0
u_4	0

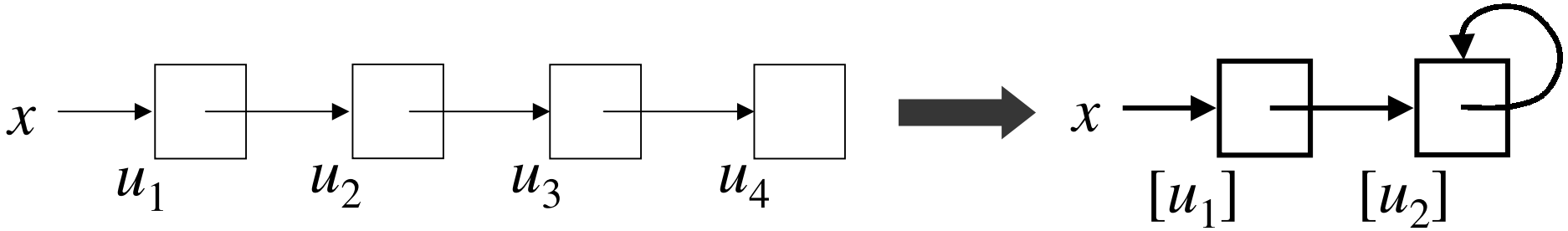
$$[\![p]\!]^{S}(u_1,\ldots,u_k) \sqsubseteq_3 [\![p]\!]^{S^{\#}}([u_1]_A,\ldots,[u_k]_A)$$



	$is(u)$
u_1	0
u_2	0
u_3	0
u_4	0

	$is(u)$
$[u_1]$	0
$[u_2]$	0

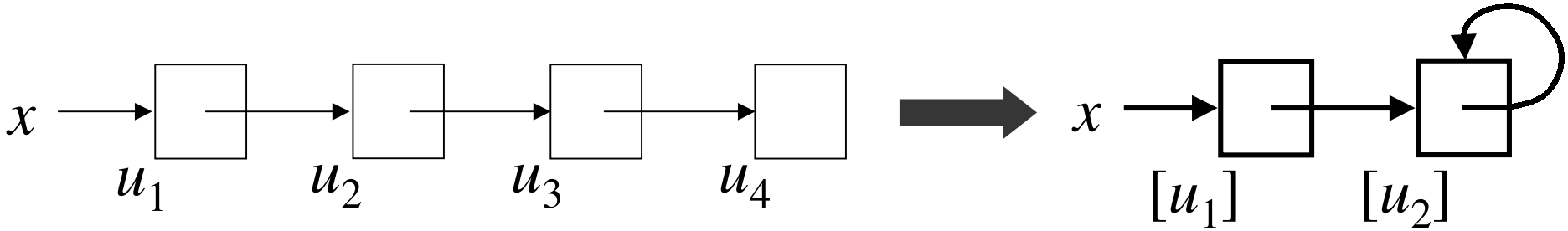
$$[\![p]\!]^{S}(u_1,\ldots,u_k) \sqsubseteq_3 [\![p]\!]^{S^{\#}}([u_1]_A,\ldots,[u_k]_A)$$



	is(u)
u_1	0
u_2	0
u_3	0
u_4	0

	is(u)
$[u_1]$	0
$[u_2]$	0

$$[\![p]\!]^{S}(u_1,\ldots,u_k) \sqsubseteq_3 [\![p]\!]^{S^\#}([u_1]_A,\ldots,[u_k]_A)$$

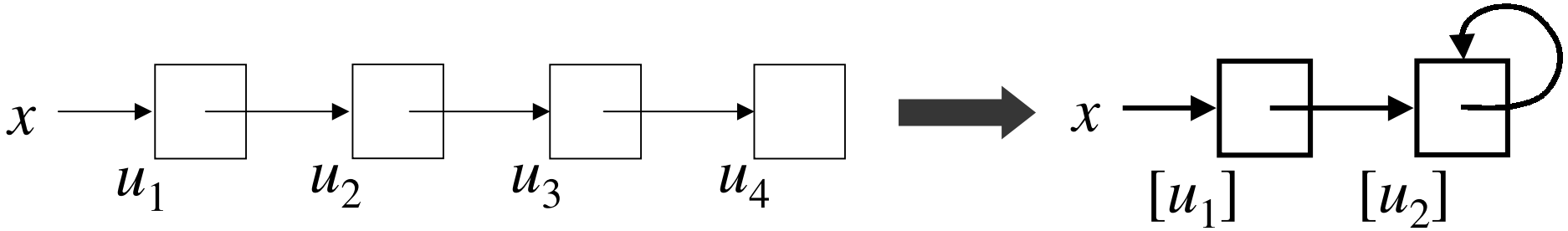


	$is(u)$
u_1	0
u_2	0
u_3	0
u_4	0

	$is(u)$
$[u_1]$	0
$[u_2]$	0

$=$	u_1	u_2	u_3	u_4
u_1	1	0	0	0
u_2	0	1	0	0
u_3	0	0	1	0
u_4	0	0	0	1

$$[\![p]\!]^{S}(u_1,\ldots,u_k) \sqsubseteq_3 [\![p]\!]^{S^\#}([u_1]_A,\ldots,[u_k]_A)$$



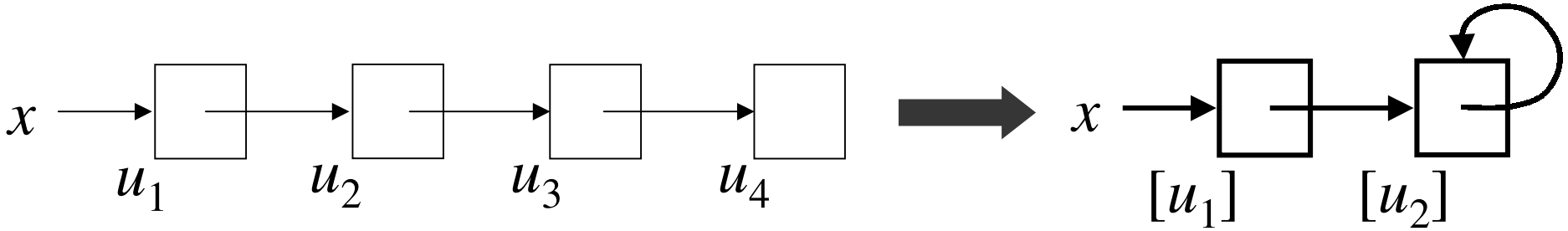
	$is(u)$
u_1	0
u_2	0
u_3	0
u_4	0

	$is(u)$
$[u_1]$	0
$[u_2]$	0

$=$	u_1	u_2	u_3	u_4
u_1	1	0	0	0
u_2	0	1	0	0
u_3	0	0	1	0
u_4	0	0	0	1

$=$	$[u_1]$	$[u_2]$
$[u_1]$	1	0
$[u_2]$	0	1/2

$$[\![p]\!]^{S}(u_1,\ldots,u_k) \sqsubseteq_3 [\![p]\!]^{S^\#}([u_1]_A,\ldots,[u_k]_A)$$



	$is(u)$
u_1	0
u_2	0
u_3	0
u_4	0

	$is(u)$
$[u_1]$	0
$[u_2]$	0

$=$	u_1	u_2	u_3	u_4
u_1	1	0	0	0
u_2	0	1	0	0
u_3	0	0	1	0
u_4	0	0	0	1

$=$	$[u_1]$	$[u_2]$
$[u_1]$	1	0
$[u_2]$	0	1/2

Abstraction Conserves Properties

$$S \xrightarrow{Abs(A)} S^{\#} = S/[u]_A$$

$$u \mapsto [u]_A$$

$$[\![p]\!]^S(u_1, \ldots, u_k) \sqsubseteq_3 [\![p]\!]^{S^{\#}}([u_1]_A, \ldots, [u_k]_A)$$

Abstraction Conserves Properties

$$S \xrightarrow{Abs(A)} S^{\#} = S/[u]_A$$

$$u \mapsto [u]_A$$

$$[\![p]\!]^S(u_1, \ldots, u_k) \sqsubseteq_3 [\![p]\!]^{S^{\#}}([u_1]_A, \ldots, [u_k]_A)$$

$$\underline{[\![\varphi]\!]^S(u_1, \ldots, u_k) \sqsubseteq_3 [\![\varphi]\!]^{S^{\#}}([u_1]_A, \ldots, [u_k]_A)}$$

Abstraction Conserves Properties

$$S \xrightarrow{Abs(A)} S^{\#} = S/[u]_A$$

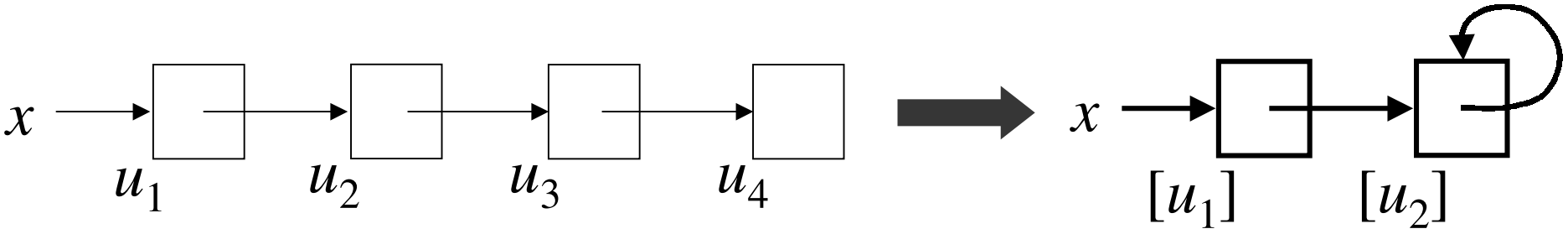
$$u \mapsto [u]_A$$

$$[\![p]\!]^S(u_1, \ldots, u_k) \sqsubseteq_3 [\![p]\!]^{S^{\#}}([u_1]_A, \ldots, [u_k]_A)$$

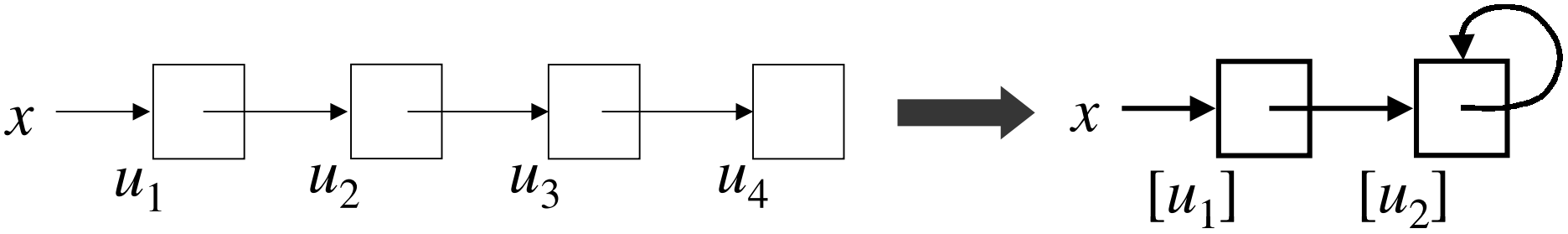
$$\underline{[\![\varphi]\!]^S(u_1, \ldots, u_k) \sqsubseteq_3 [\![\varphi]\!]^{S^{\#}}([u_1]_A, \ldots, [u_k]_A)}$$

Evaluating a formula extracts information conservatively

$$[\![\varphi]\!]^{S}(u_1, \ldots, u_k) \sqsubseteq_3 [\![\varphi]\!]^{S^\#}([u_1]_A, \ldots, [u_k]_A)$$

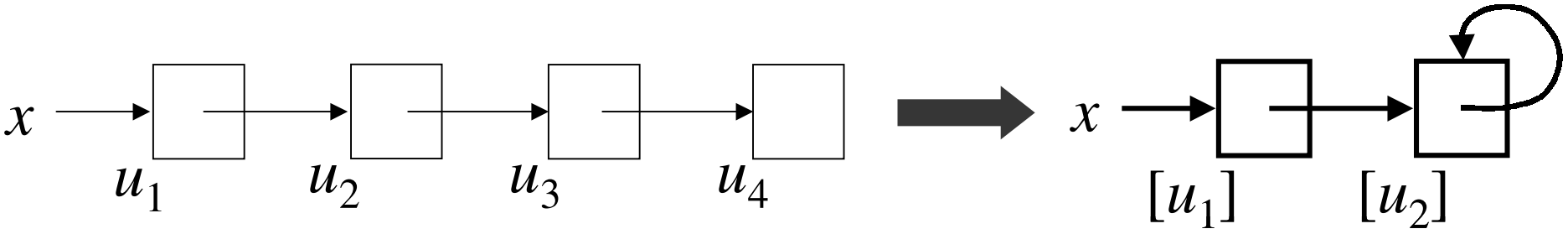


$$[\![\varphi]\!]^{S}(u_1, \ldots, u_k) \sqsubseteq_3 [\![\varphi]\!]^{S^\#}([u_1]_A, \ldots, [u_k]_A)$$



$$\varphi(v) \triangleq \exists\, v_1, v_2 : n(v_1, v) \wedge n(v_2, v) \wedge v_1 \neq v_2$$

$$[\![\varphi]\!]^{S}(u_1, \ldots, u_k) \sqsubseteq_3 [\![\varphi]\!]^{S^\#}([u_1]_A, \ldots, [u_k]_A)$$

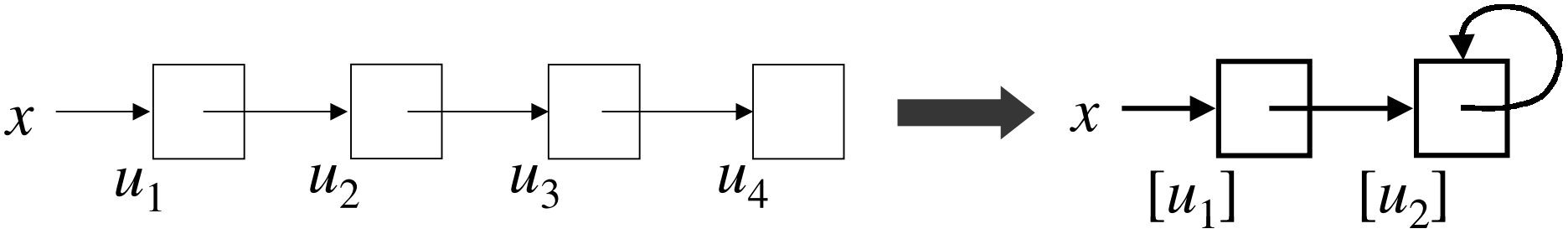


$$\varphi(v) \triangleq \exists\, v_1, v_2 : n(v_1, v) \wedge n(v_2, v) \wedge v_1 \neq v_2$$

	$[\![\varphi]\!]^{S}(u)$
u_1	0
u_2	0
u_3	0
u_4	0

	$[\![\varphi]\!]^{S^\#}(u)$
$[u_1]$	0
$[u_2]$	1/2

$$[\![\varphi]\!]^{S}(u_1, \ldots, u_k) \sqsubseteq_3 [\![\varphi]\!]^{S^\#}([u_1]_A, \ldots, [u_k]_A)$$



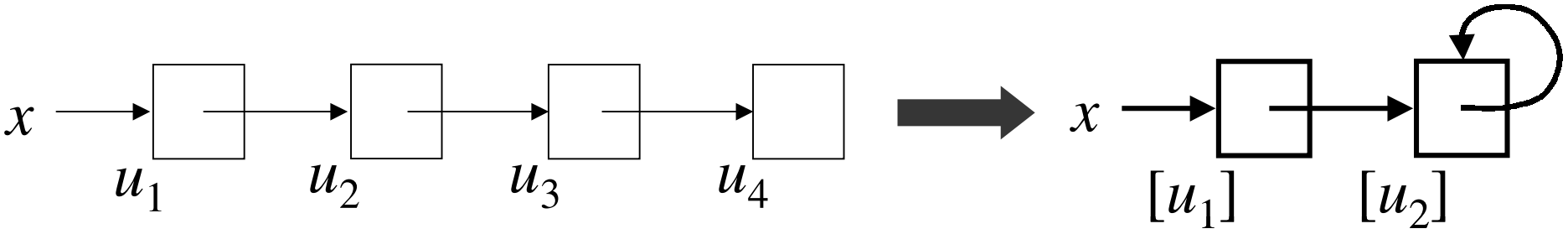
$$\varphi(v) \triangleq \exists\, v_1, v_2 : n(v_1, v) \wedge n(v_2, v) \wedge v_1 \neq v_2$$

	$[\![\varphi]\!]^{S}(u)$
u_1	0
u_2	0
u_3	0
u_4	0

$\sqsubseteq$

	$[\![\varphi]\!]^{S^\#}(u)$
$[u_1]$	0
$[u_2]$	1/2

$$[\![\varphi]\!]^{S}(u_1, \ldots, u_k) \sqsubseteq_3 [\![\varphi]\!]^{S^\#}([u_1]_A, \ldots, [u_k]_A)$$



$$\varphi(v) \triangleq \exists\, v_1, v_2 : n(v_1, v) \wedge n(v_2, v) \wedge v_1 \neq v_2$$

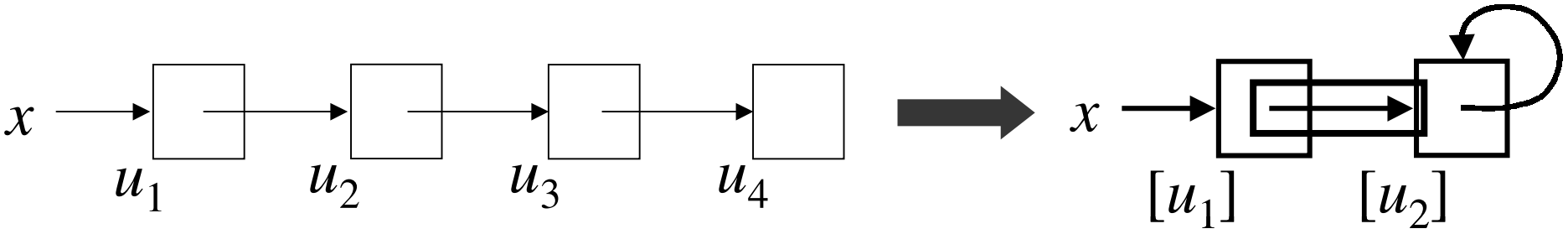
For $[\![\varphi]\!]^{S^\#}([u_2])$,
let $v_1 = [u_1]$,
and $v_2 = [u_2]$

	$[\![\varphi]\!]^{S}(u)$
u_1	0
u_2	0
u_3	0
u_4	0

$\sqsubseteq$

	$[\![\varphi]\!]^{S^\#}(u)$
$[u_1]$	0
$[u_2]$	1/2

$$[\![\varphi]\!]^{S}(u_1, \ldots, u_k) \sqsubseteq_3 [\![\varphi]\!]^{S^\#}([u_1]_A, \ldots, [u_k]_A)$$



$$\varphi(v) \triangleq \exists\, v_1, v_2 : \underline{n(v_1, v)} \wedge n(v_2, v) \wedge v_1 \neq v_2$$

$\frac{1}{2}$

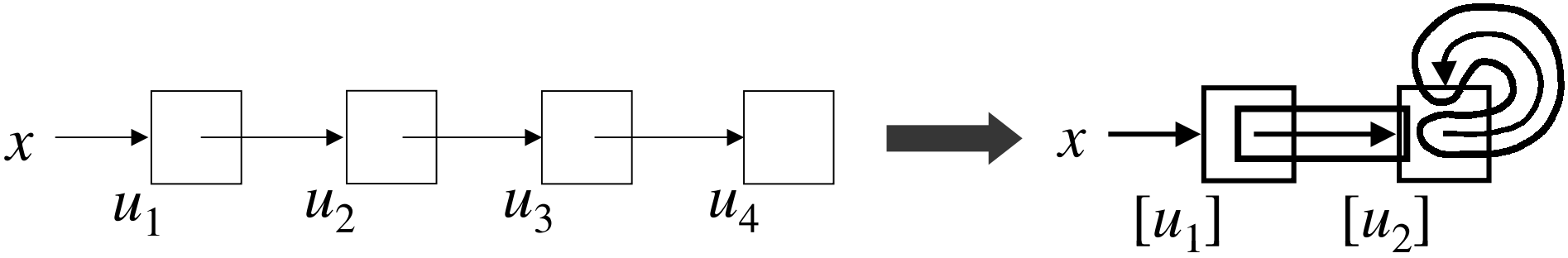
For $[\![\varphi]\!]^{S^\#}([u_2])$,
let $v_1 = [u_1]$,
and $v_2 = [u_2]$

	$[\![\varphi]\!]^{S}(u)$
u_1	0
u_2	0
u_3	0
u_4	0

$\sqsubseteq$

	$[\![\varphi]\!]^{S^\#}(u)$
$[u_1]$	0
$[u_2]$	1/2

$$[\![\varphi]\!]^{S}(u_1, \ldots, u_k) \sqsubseteq_3 [\![\varphi]\!]^{S^\#}([u_1]_A, \ldots, [u_k]_A)$$



$$\varphi(v) \triangleq \exists\, v_1, v_2 : \underline{n(v_1, v)} \wedge \underline{n(v_2, v)} \wedge v_1 \neq v_2$$

For $[\![\varphi]\!]^{S^\#}([u_2])$, let $v_1 = [u_1]$, and $v_2 = [u_2]$

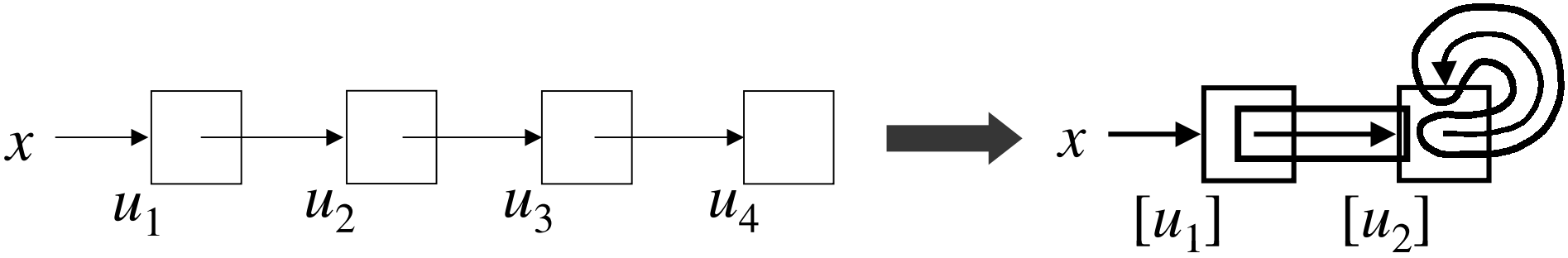
$\frac{1}{2} \quad \wedge \quad \frac{1}{2}$

	$[\![\varphi]\!]^{S}(u)$
u_1	0
u_2	0
u_3	0
u_4	0

$\sqsubseteq$

	$[\![\varphi]\!]^{S^\#}(u)$
$[u_1]$	0
$[u_2]$	1/2

$$[\![\varphi]\!]^{S}(u_1, \ldots, u_k) \sqsubseteq_3 [\![\varphi]\!]^{S^\#}([u_1]_A, \ldots, [u_k]_A)$$



$$\varphi(v) \triangleq \exists\, v_1, v_2 : \underline{n(v_1,v)} \wedge \underline{n(v_2,v)} \wedge \underline{v_1 \neq v_2}$$

$$\frac{1}{2} \quad \wedge \quad \frac{1}{2} \quad \wedge \quad 1$$

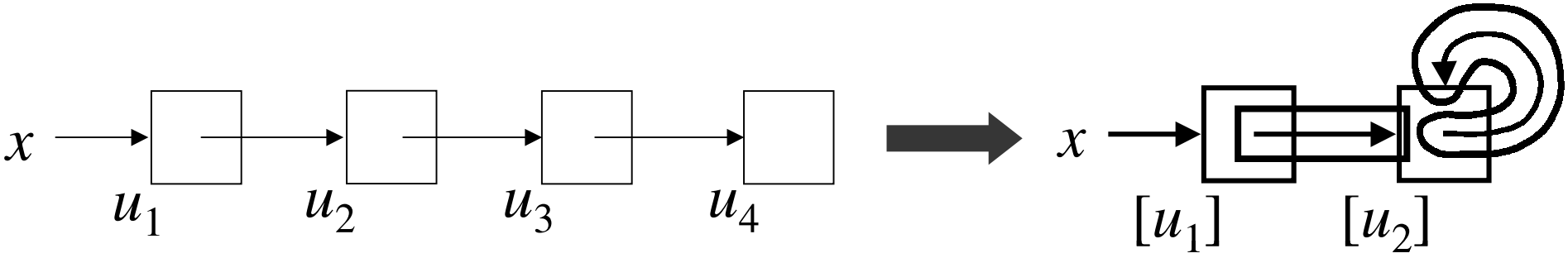
For $[\![\varphi]\!]^{S^\#}([u_2])$,
let $v_1 = [u_1]$,
and $v_2 = [u_2]$

	$[\![\varphi]\!]^{S}(u)$
u_1	0
u_2	0
u_3	0
u_4	0

$\sqsubseteq$

	$[\![\varphi]\!]^{S^\#}(u)$
$[u_1]$	0
$[u_2]$	1/2

$$[\![\varphi]\!]^{S}(u_1, \ldots, u_k) \sqsubseteq_3 [\![\varphi]\!]^{S^\#}([u_1]_A, \ldots, [u_k]_A)$$



$$\varphi(v) \triangleq \exists\, v_1, v_2 : \underline{n(v_1,v)} \wedge \underline{n(v_2,v)} \wedge \underline{v_1 \neq v_2}$$

For $[\![\varphi]\!]^{S^\#}([u_2])$, let $v_1 = [u_1]$, and $v_2 = [u_2]$

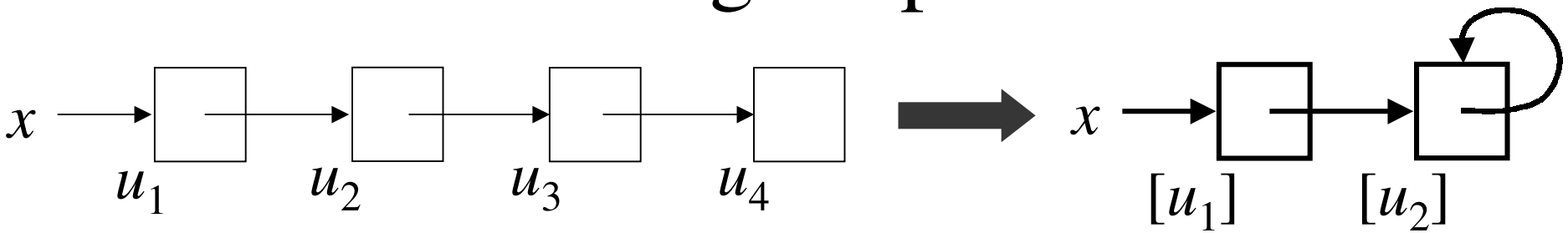
$$\tfrac{1}{2} \wedge \tfrac{1}{2} \wedge 1 = \tfrac{1}{2}$$

	$[\![\varphi]\!]^{S}(u)$
u_1	0
u_2	0
u_3	0
u_4	0

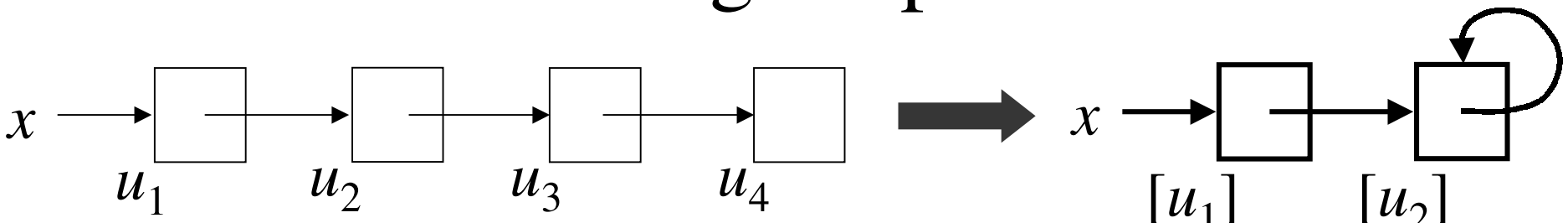
$\sqsubseteq$

	$[\![\varphi]\!]^{S^\#}(u)$
$[u_1]$	0
$[u_2]$	1/2

“Tracking Properties” Beats “Inferring Properties”

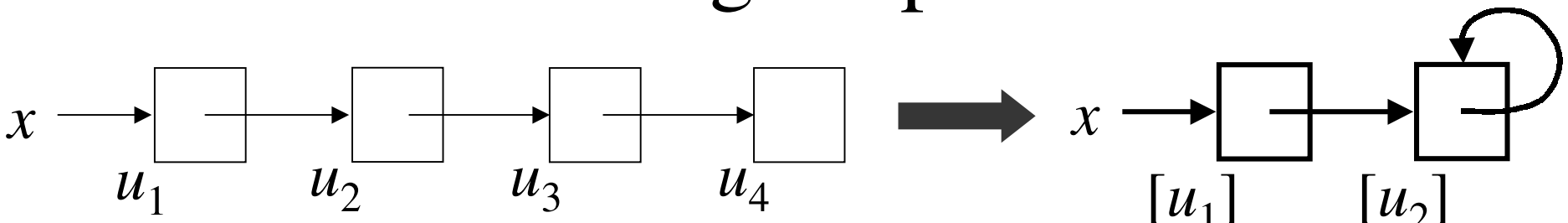


“Tracking Properties” Beats “Inferring Properties”



	$is(u)$
u_1	0
u_2	0
u_3	0
u_4	0

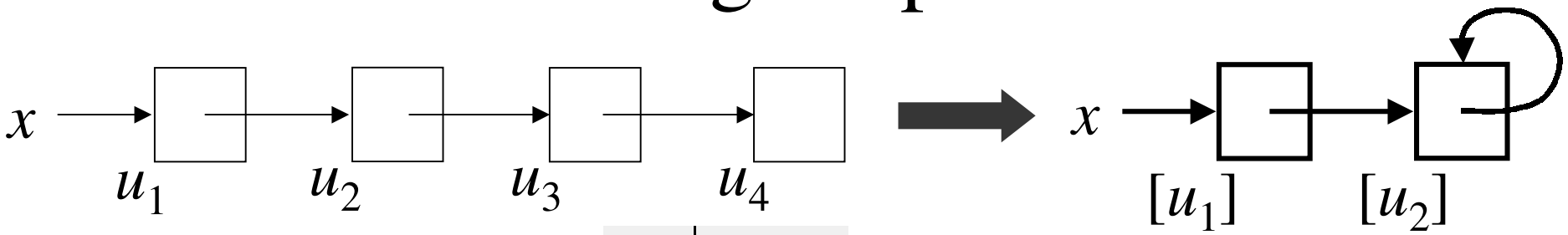
“Tracking Properties” Beats “Inferring Properties”



	$is(u)$
u_1	0
u_2	0
u_3	0
u_4	0

	$is(u)$
$[u_1]$	0
$[u_2]$	0

“Tracking Properties” Beats “Inferring Properties”

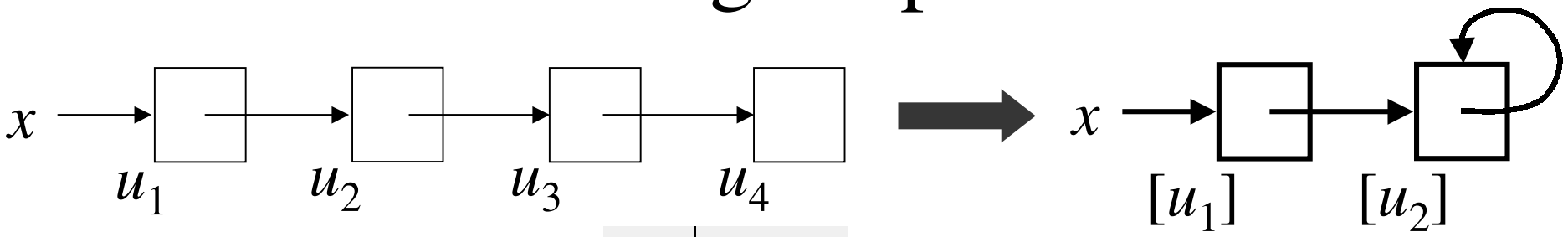


	$is(u)$
u_1	0
u_2	0
u_3	0
u_4	0

	$is(u)$
$[u_1]$	0
$[u_2]$	0

	$[\![\varphi]\!]^S(u)$
u_1	0
u_2	0
u_3	0
u_4	0

“Tracking Properties” Beats “Inferring Properties”



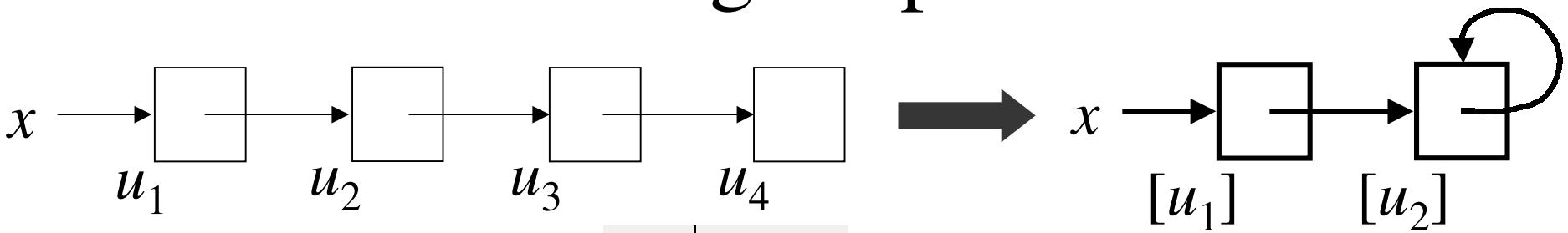
	$is(u)$
u_1	0
u_2	0
u_3	0
u_4	0

	$is(u)$
$[u_1]$	0
$[u_2]$	0

	$[\![\varphi]\!]^S(u)$
u_1	0
u_2	0
u_3	0
u_4	0

	$[\![\varphi]\!]^{S^\#}(u)$
$[u_1]$	0
$[u_2]$	1/2

“Tracking Properties” Beats “Inferring Properties”



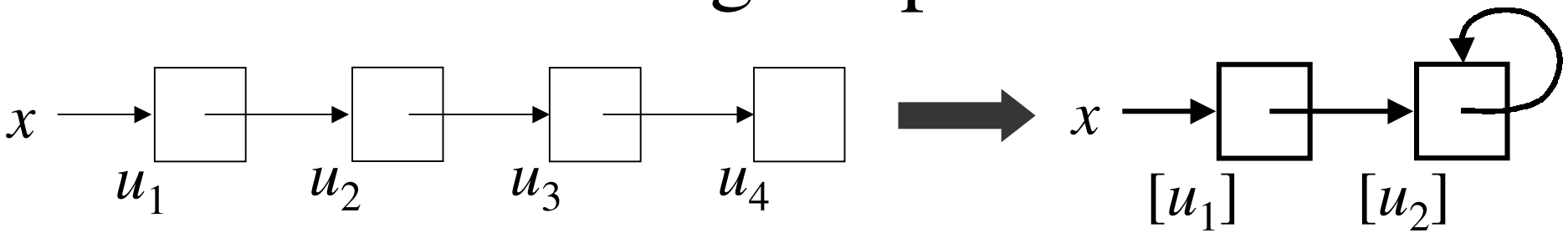
	$is(u)$
u_1	0
u_2	0
u_3	0
u_4	0

	$is(u)$
$[u_1]$	0
$[u_2]$	0

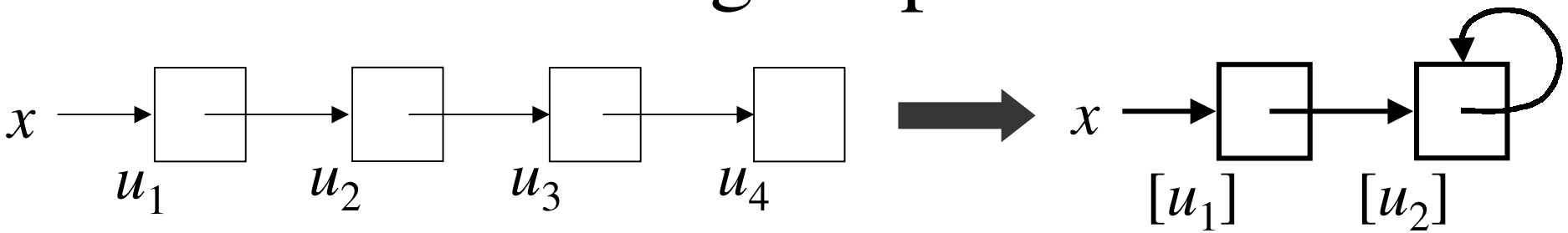
	$[\![\varphi]\!]^S(u)$
u_1	0
u_2	0
u_3	0
u_4	0

	$[\![\varphi]\!]^{S^\#}(u)$
$[u_1]$	0
$[u_2]$	1/2

“Tracking Properties” Beats “Inferring Properties”

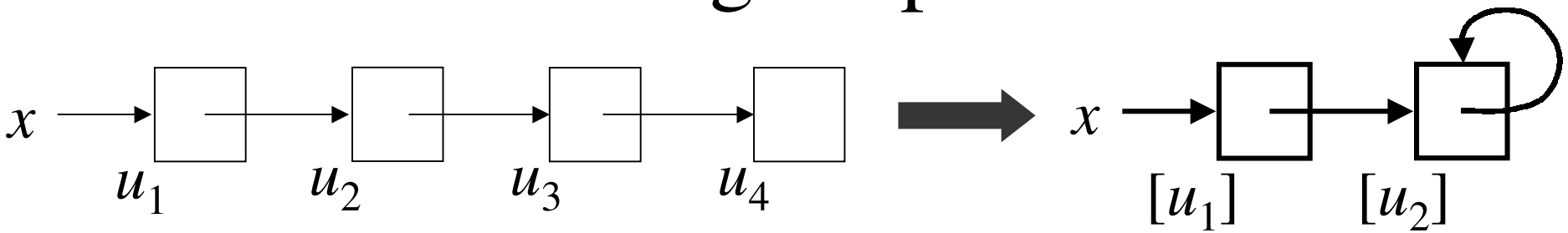


“Tracking Properties” Beats “Inferring Properties”



$$[\![p]\!]^{S}(u_1, \ldots, u_k) \sqsubseteq_3 [\![p]\!]^{S^{\#}}([u_1]_A, \ldots, [u_k]_A)$$

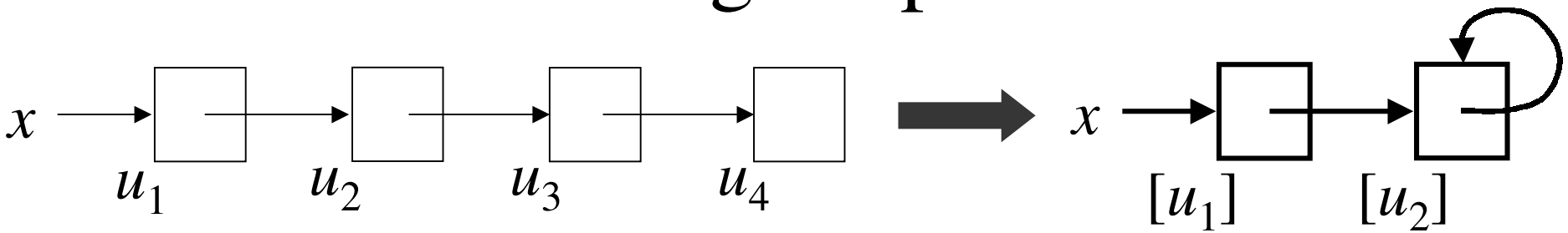
“Tracking Properties” Beats “Inferring Properties”



$$[\![p]\!]^{S}(u_1, \ldots, u_k) \sqsubseteq_3 [\![p]\!]^{S^{\#}}([u_1]_A, \ldots, [u_k]_A)$$

$$[\![\varphi_p]\!]^{S}(u_1, \ldots, u_k) \sqsubseteq_3 [\![\varphi_p]\!]^{S^{\#}}([u_1]_A, \ldots, [u_k]_A)$$

“Tracking Properties” Beats “Inferring Properties”

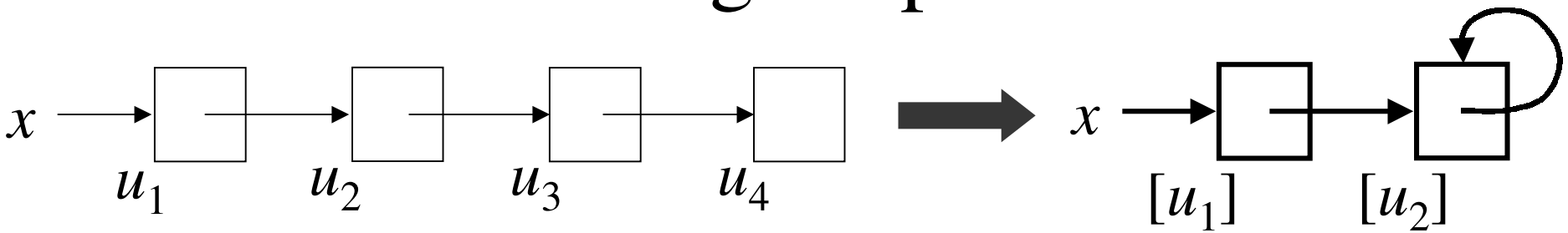


$$[\![p]\!]^S(u_1, \ldots, u_k) \sqsubseteq_3 [\![p]\!]^{S^\#}([u_1]_A, \ldots, [u_k]_A)$$

$$[\![\varphi_p]\!]^S(u_1, \ldots, u_k) \sqsubseteq_3 [\![\varphi_p]\!]^{S^\#}([u_1]_A, \ldots, [u_k]_A)$$

$$[\![\varphi_p]\!]^S(u_1, \ldots, u_k) = [\![p]\!]^S(u_1, \ldots, u_k)$$

“Tracking Properties” Beats “Inferring Properties”

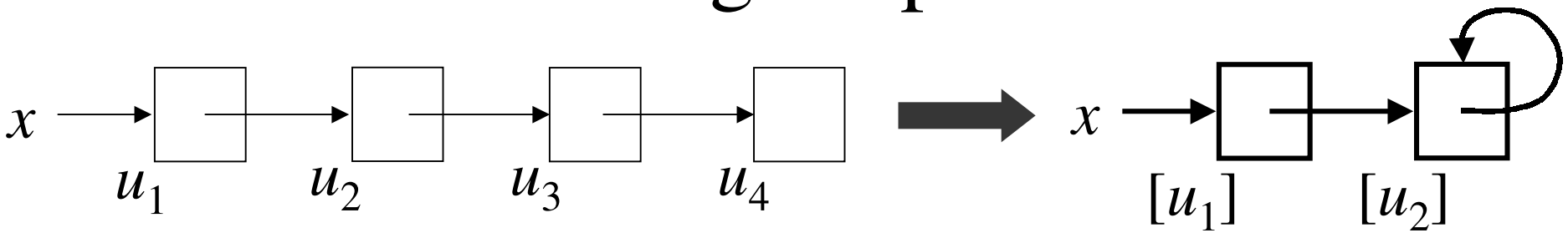


$$[\![p]\!]^S(u_1, \ldots, u_k) \sqsubseteq_3 [\![p]\!]^{S^\#}([u_1]_A, \ldots, [u_k]_A)$$

$$[\![\varphi_p]\!]^S(u_1, \ldots, u_k) \sqsubseteq_3 [\![\varphi_p]\!]^{S^\#}([u_1]_A, \ldots, [u_k]_A)$$

$$[\![\varphi_p]\!]^S(u_1, \ldots, u_k) = [\![p]\!]^S(u_1, \ldots, u_k)$$
$$\sqsubseteq_3 [\![p]\!]^{S^\#}([u_1]_A, \ldots, [u_k]_A)$$

“Tracking Properties” Beats “Inferring Properties”



$$[\![p]\!]^S(u_1, \ldots, u_k) \sqsubseteq_3 [\![p]\!]^{S^\#}([u_1]_A, \ldots, [u_k]_A)$$

$$[\![\varphi_p]\!]^S(u_1, \ldots, u_k) \sqsubseteq_3 [\![\varphi_p]\!]^{S^\#}([u_1]_A, \ldots, [u_k]_A)$$

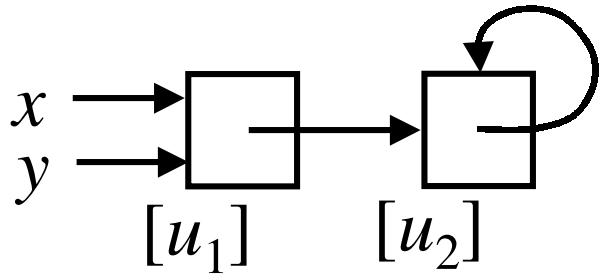
$$\begin{aligned} [\![\varphi_p]\!]^S(u_1, \ldots, u_k) &= [\![p]\!]^S(u_1, \ldots, u_k) \\ &\sqsubseteq_3 [\![p]\!]^{S^\#}([u_1]_A, \ldots, [u_k]_A) \\ &\sqsubseteq_3 [\![\varphi_p]\!]^{S^\#}([u_1]_A, \ldots, [u_k]_A) \end{aligned}$$

Outline

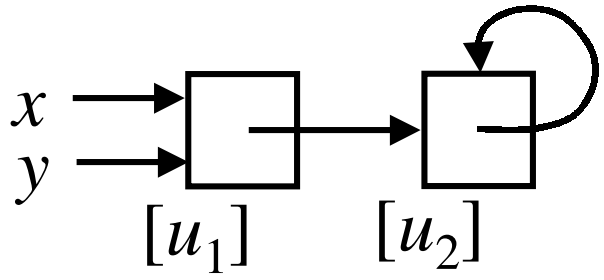
- Using logic to describe stores
- Using logic to express store transformations
- Forming abstractions of stores
- Three-valued logic
- Using three-valued logic to express transformations of abstract stores

Example

Example

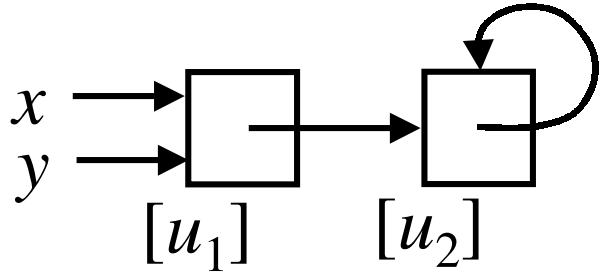


Example

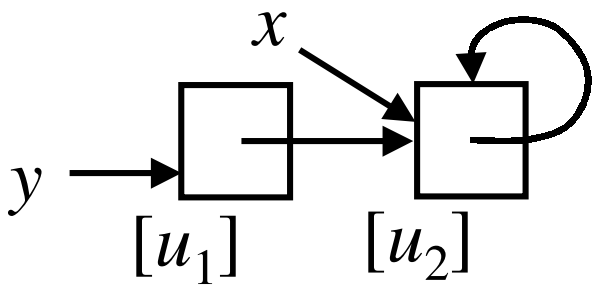


$$x = y \rightarrow n$$

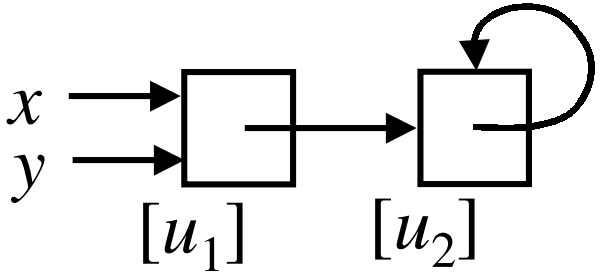
Example



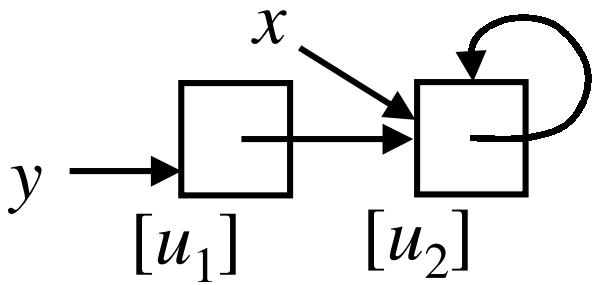
$$x = y \rightarrow n$$



Example

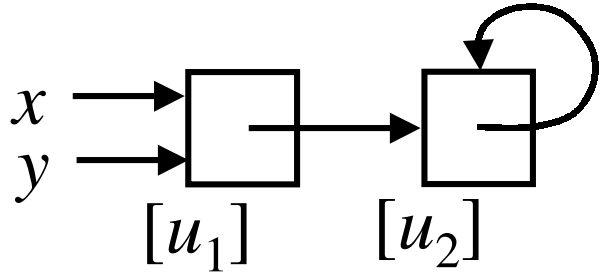


$$x = y \rightarrow n$$



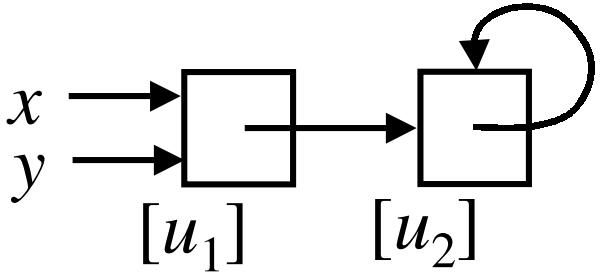
"Rational reconstruction" of
[Chase, Wegman, & Zadeck 90]

Example (~[CWZ 90])

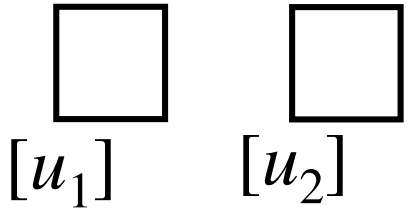


$x = y \rightarrow n$

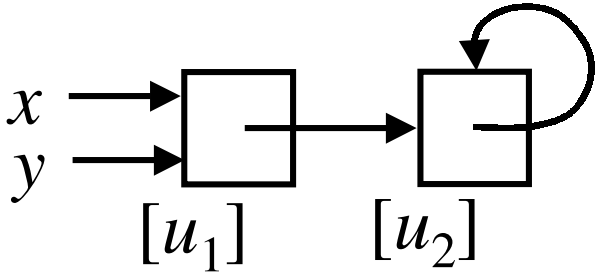
Example (~[CWZ 90])



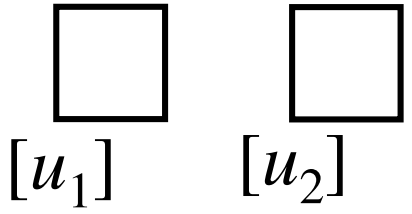
$x = y \rightarrow n$



Example (~[CWZ 90])

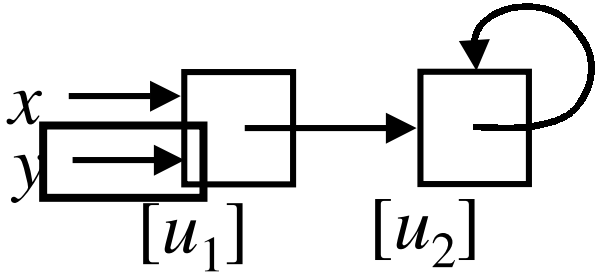


$x = y \rightarrow n$

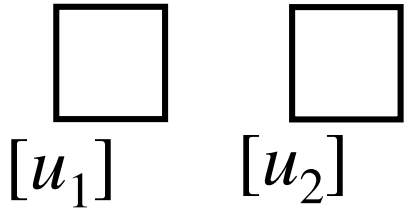


$$\varphi_x^{[x = y \rightarrow n]}(v) \triangleq \exists\, v_1 : y(v_1) \wedge n(v_1, v)$$

Example (~[CWZ 90])

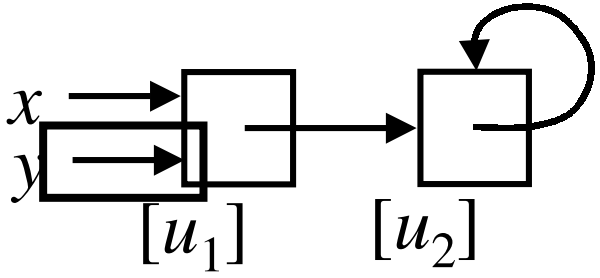


$x = y \rightarrow n$

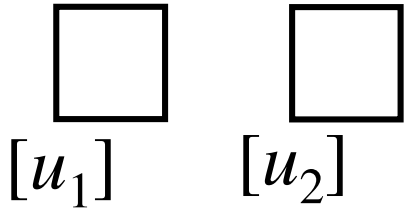


$$\varphi_x^{[x = y \rightarrow n]}(v) \triangleq \exists\, v_1 : \underline{y(v_1)} \wedge n(v_1, v)$$

Example (~[CWZ 90])



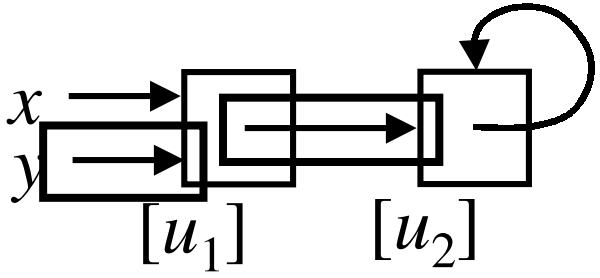
$x = y \rightarrow n$



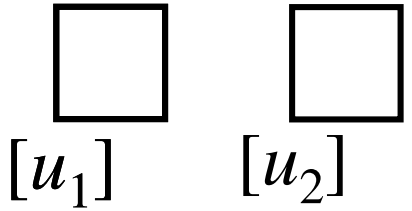
$$\varphi_x^{[x = y \rightarrow n]}(v) \triangleq \exists\, v_1 : \underline{y(v_1)} \wedge n(v_1, v)$$

1

Example (~[CWZ 90])



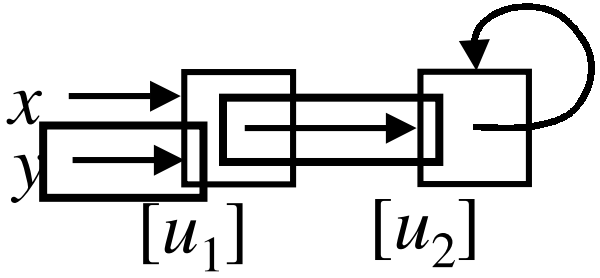
$x = y \rightarrow n$



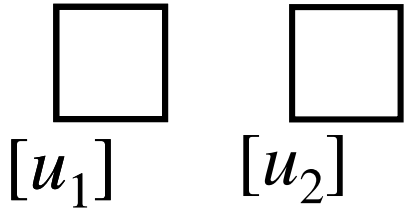
$$\varphi_x^{[x = y \rightarrow n]}(v) \triangleq \exists\, v_1 : \underline{y(v_1)} \wedge \underline{n(v_1, v)}$$

1

Example (~[CWZ 90])

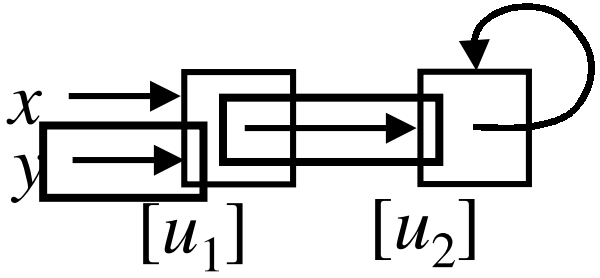


$$x = y \rightarrow n$$

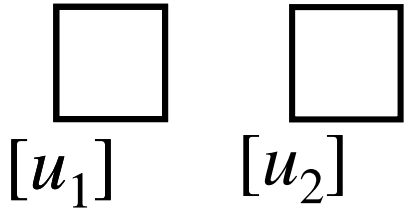


$$\varphi_x^{[x = y \rightarrow n]}(v) \triangleq \exists\, v_1 : \underset{1}{y(v_1)} \wedge \underset{\frac{1}{2}}{n(v_1, v)}$$

Example (~[CWZ 90])

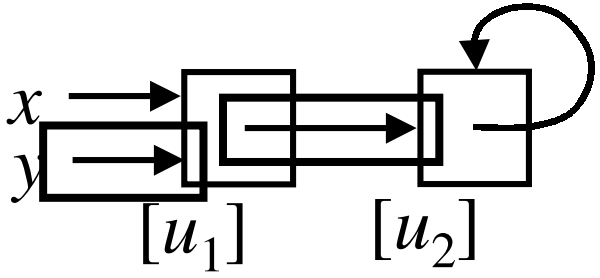


$$x = y \rightarrow n$$

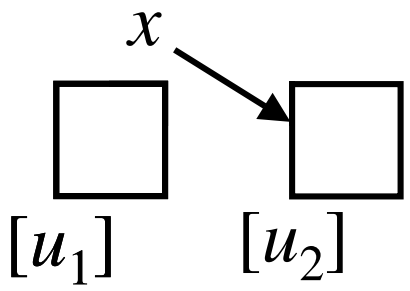


$$\varphi_x^{[x = y \rightarrow n]}(v) \triangleq \exists\, v_1 : \underbrace{\underbrace{y(v_1)}_{1} \wedge \underbrace{n(v_1,v)}_{\frac{1}{2}}}_{\frac{1}{2}}$$

Example (~[CWZ 90])

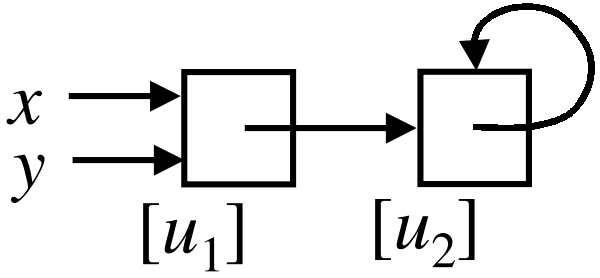


$$x = y \rightarrow n$$

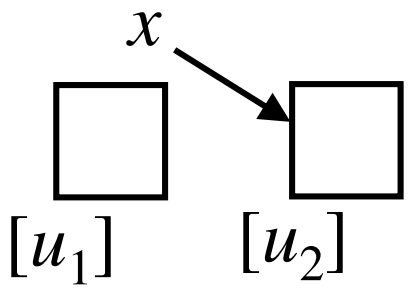


$$\varphi_x^{[x = y \rightarrow n]}(v) \triangleq \exists\, v_1 : \underbrace{\underbrace{y(v_1)}_{1} \wedge \underbrace{n(v_1,v)}_{\frac{1}{2}}}_{\frac{1}{2}}$$

Example (~[CWZ 90])

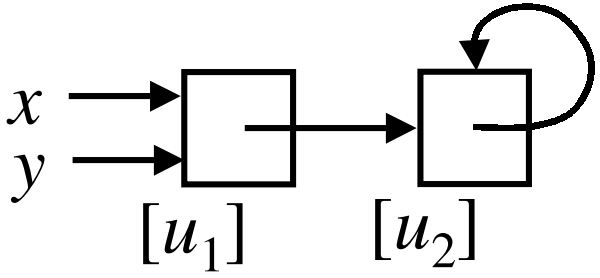


$x = y \rightarrow n$

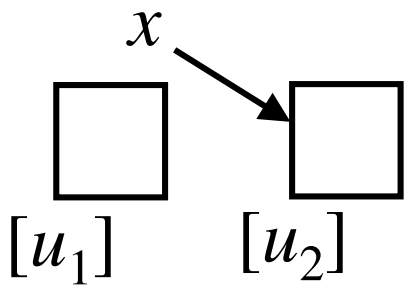


$$\varphi_x^{[x = y \rightarrow n]}(v) \triangleq \exists\, v_1 : y(v_1) \wedge n(v_1, v)$$

Example (~[CWZ 90])



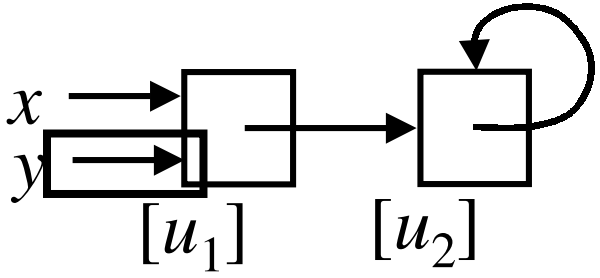
$$x = y \rightarrow n$$



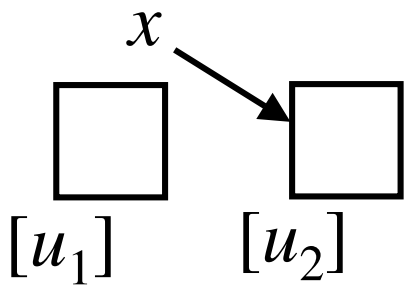
$$\varphi_x^{[x = y \rightarrow n]}(v) \triangleq \exists\, v_1 : y(v_1) \wedge n(v_1, v)$$

$$\varphi_y^{[x = y \rightarrow n]}(v) \triangleq y(v)$$

Example (~[CWZ 90])



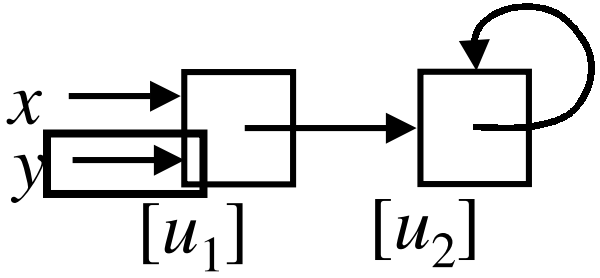
$$x = y \rightarrow n$$



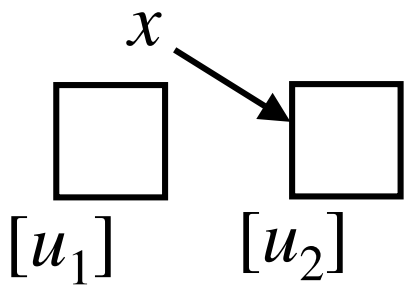
$$\varphi_x{}^{[x = y \rightarrow n]}(v) \triangleq \exists\, v_1 : y(v_1) \wedge n(v_1, v)$$

$$\varphi_y{}^{[x = y \rightarrow n]}(v) \triangleq \underline{y(v)}$$

Example (~[CWZ 90])



$$x = y \rightarrow n$$

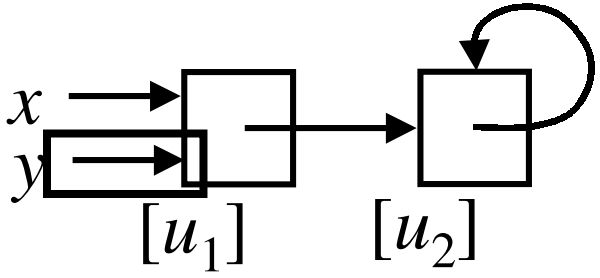


$$\varphi_x{}^{[x = y \rightarrow n]}(v) \triangleq \exists\, v_1 : y(v_1) \wedge n(v_1, v)$$

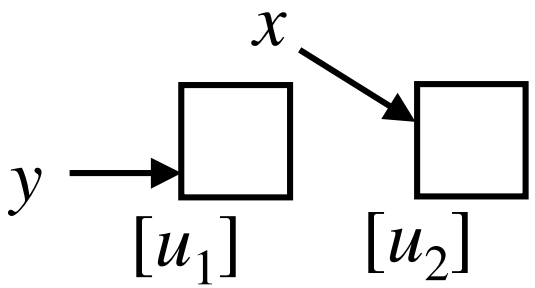
$$\varphi_y{}^{[x = y \rightarrow n]}(v) \triangleq \underline{y(v)}$$

1

Example (~[CWZ 90])



$$x = y \rightarrow n$$

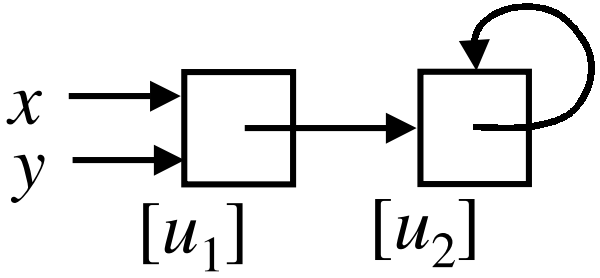


$$\varphi_x^{[x = y \rightarrow n]}(v) \triangleq \exists\, v_1 : y(v_1) \wedge n(v_1, v)$$

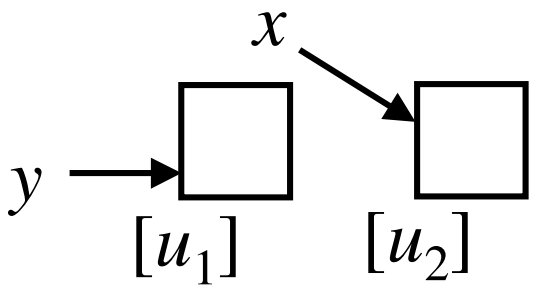
$$\varphi_y^{[x = y \rightarrow n]}(v) \triangleq \underline{y(v)}$$

1

Example (~[CWZ 90])



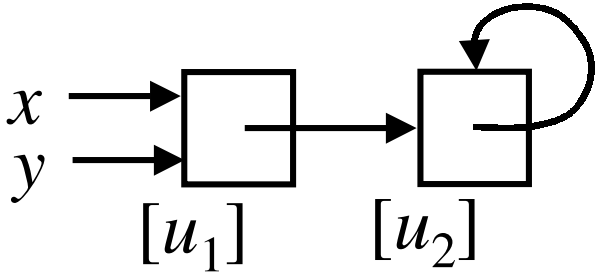
$$x = y \rightarrow n$$



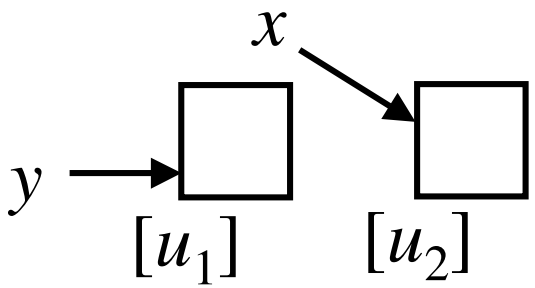
$$\varphi_x^{[x = y \rightarrow n]}(v) \triangleq \exists\, v_1 : y(v_1) \wedge n(v_1, v)$$

$$\varphi_y^{[x = y \rightarrow n]}(v) \triangleq y(v)$$

Example (~[CWZ 90])



$$x = y \rightarrow n$$

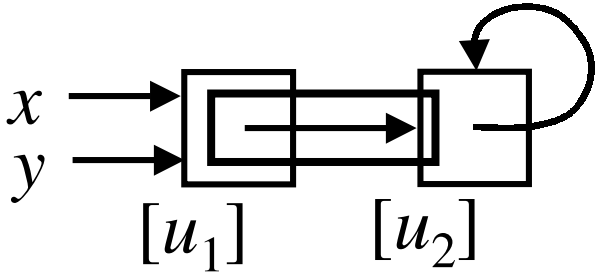


$$\varphi_x^{[x = y \rightarrow n]}(v) \triangleq \exists\, v_1 : y(v_1) \wedge n(v_1, v)$$

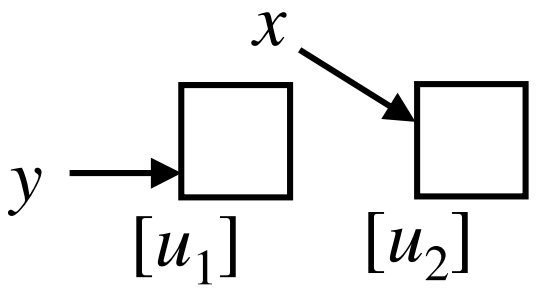
$$\varphi_y^{[x = y \rightarrow n]}(v) \triangleq y(v)$$

$$\varphi_n^{[x = y \rightarrow n]}(v_1, v_2) \triangleq n(v_1, v_2)$$

Example (~[CWZ 90])



$$x = y \rightarrow n$$

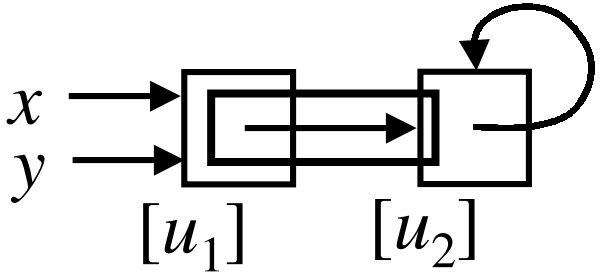


$$\varphi_x^{[x = y \rightarrow n]}(v) \triangleq \exists\, v_1 : y(v_1) \wedge n(v_1, v)$$

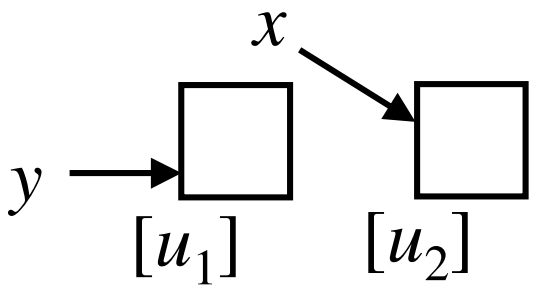
$$\varphi_y^{[x = y \rightarrow n]}(v) \triangleq y(v)$$

$$\varphi_n^{[x = y \rightarrow n]}(v_1, v_2) \triangleq \underline{n(v_1, v_2)}$$

Example (~[CWZ 90])



$$x = y \rightarrow n$$



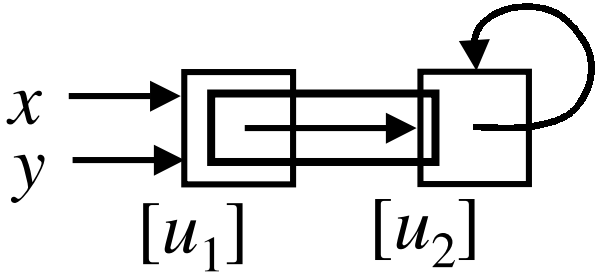
$$\varphi_x^{[x = y \rightarrow n]}(v) \triangleq \exists\, v_1 : y(v_1) \wedge n(v_1, v)$$

$$\varphi_y^{[x = y \rightarrow n]}(v) \triangleq y(v)$$

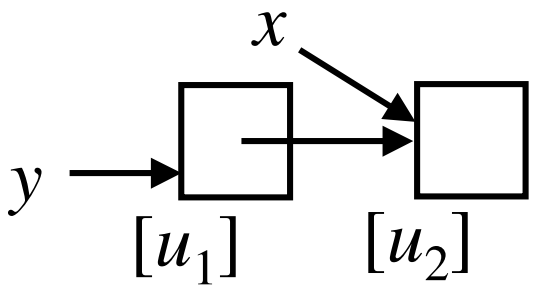
$$\varphi_n^{[x = y \rightarrow n]}(v_1, v_2) \triangleq \underline{n(v_1, v_2)}$$

$$\frac{1}{2}$$

Example (~[CWZ 90])



$$x = y \rightarrow n$$



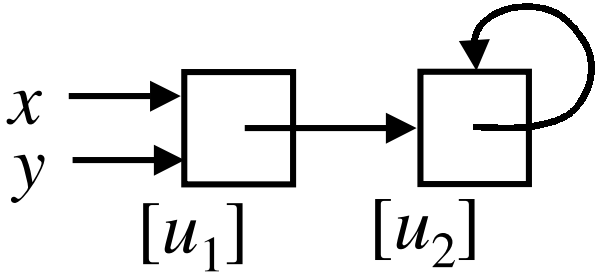
$$\varphi_x^{[x = y \rightarrow n]}(v) \triangleq \exists\, v_1 : y(v_1) \wedge n(v_1, v)$$

$$\varphi_y^{[x = y \rightarrow n]}(v) \triangleq y(v)$$

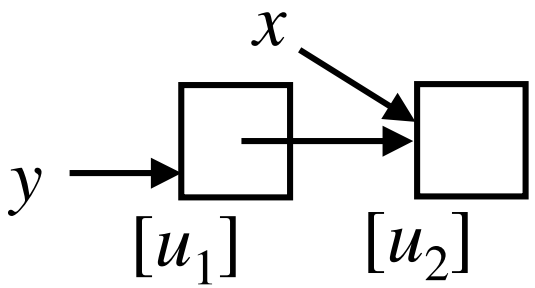
$$\varphi_n^{[x = y \rightarrow n]}(v_1, v_2) \triangleq \underline{n(v_1, v_2)}$$

$$\frac{1}{2}$$

Example (~[CWZ 90])



$$x = y \rightarrow n$$

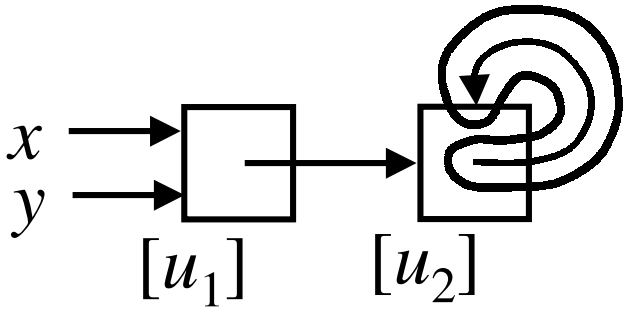


$$\varphi_x^{[x = y \rightarrow n]}(v) \triangleq \exists\, v_1 : y(v_1) \wedge n(v_1, v)$$

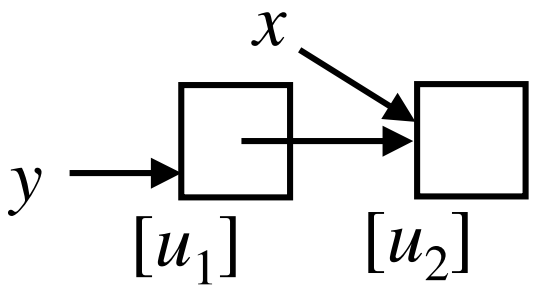
$$\varphi_y^{[x = y \rightarrow n]}(v) \triangleq y(v)$$

$$\varphi_n^{[x = y \rightarrow n]}(v_1, v_2) \triangleq n(v_1, v_2)$$

Example (~[CWZ 90])



$x = y \rightarrow n$

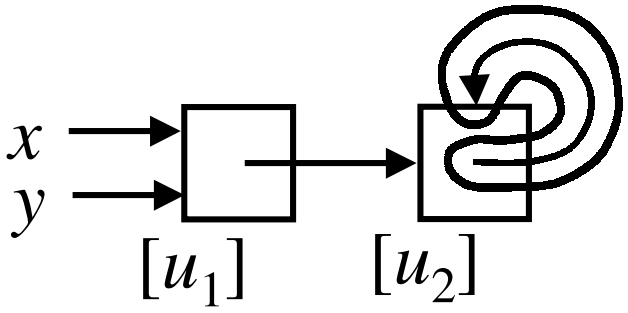


$$\varphi_x^{[x = y \rightarrow n]}(v) \triangleq \exists\, v_1 : y(v_1) \wedge n(v_1, v)$$

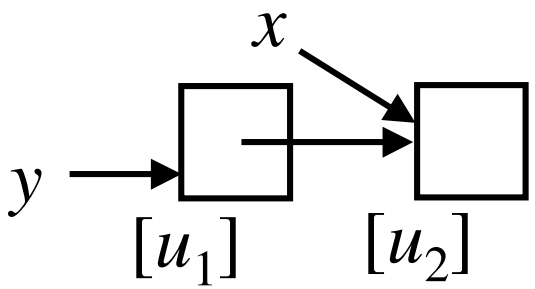
$$\varphi_y^{[x = y \rightarrow n]}(v) \triangleq y(v)$$

$$\varphi_n^{[x = y \rightarrow n]}(v_1, v_2) \triangleq \underline{n(v_1, v_2)}$$

Example (~[CWZ 90])



$x = y \rightarrow n$



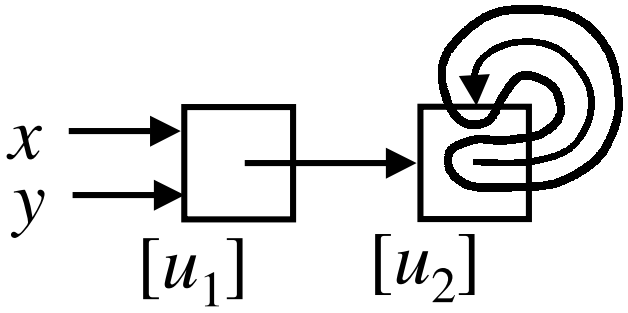
$$\varphi_x^{[x = y \rightarrow n]}(v) \triangleq \exists\, v_1 : y(v_1) \wedge n(v_1, v)$$

$$\varphi_y^{[x = y \rightarrow n]}(v) \triangleq y(v)$$

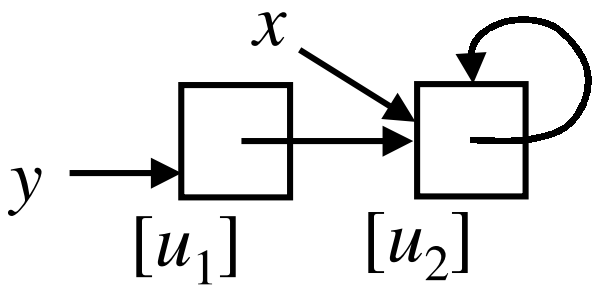
$$\varphi_n^{[x = y \rightarrow n]}(v_1, v_2) \triangleq \underline{n(v_1, v_2)}$$

$$\frac{1}{2}$$

Example (~[CWZ 90])



$x = y \rightarrow n$



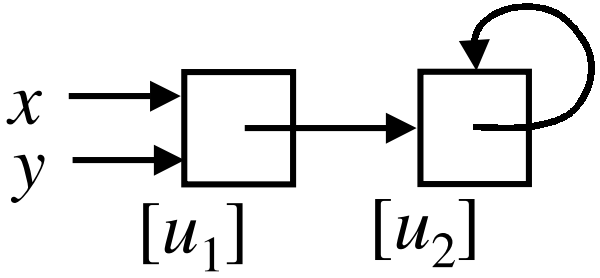
$$\varphi_x^{[x = y \rightarrow n]}(v) \triangleq \exists\, v_1 : y(v_1) \wedge n(v_1, v)$$

$$\varphi_y^{[x = y \rightarrow n]}(v) \triangleq y(v)$$

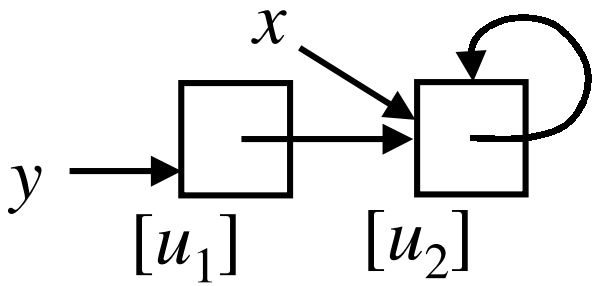
$$\varphi_n^{[x = y \rightarrow n]}(v_1, v_2) \triangleq \underline{n(v_1, v_2)}$$

$$\frac{1}{2}$$

Example (~[CWZ 90])



$x = y \rightarrow n$

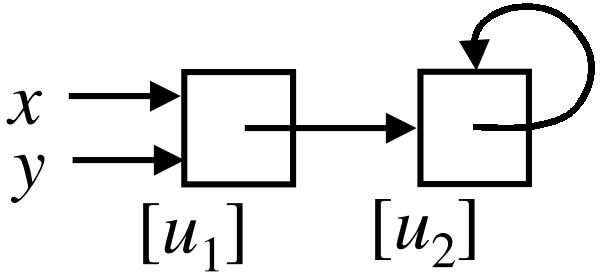


$$\varphi_x^{[x = y \rightarrow n]}(v) \triangleq \exists\, v_1 : y(v_1) \wedge n(v_1, v)$$

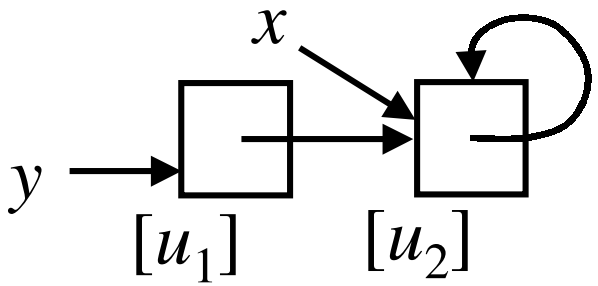
$$\varphi_y^{[x = y \rightarrow n]}(v) \triangleq y(v)$$

$$\varphi_n^{[x = y \rightarrow n]}(v_1, v_2) \triangleq n(v_1, v_2)$$

Example (~[CWZ 90])



$x = y \rightarrow n$



$$\varphi_x^{[x = y \rightarrow n]}(v) \triangleq \exists\, v_1 : y(v_1) \wedge n(v_1, v)$$

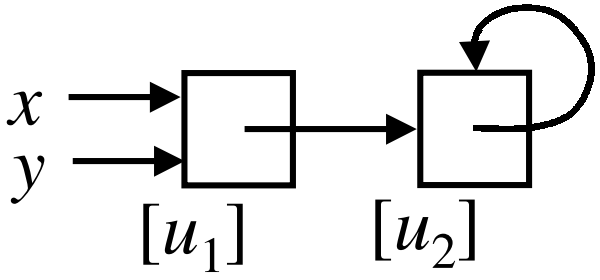
$$\varphi_y^{[x = y \rightarrow n]}(v) \triangleq y(v)$$

$$\varphi_n^{[x = y \rightarrow n]}(v_1, v_2) \triangleq n(v_1, v_2)$$

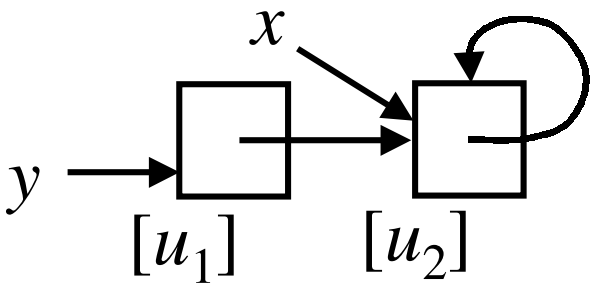
$$\varphi_{is}^{[x = y \rightarrow n]}(v) \triangleq is(v)$$

Materialization

[Chase, Wegman, & Zadeck 90]

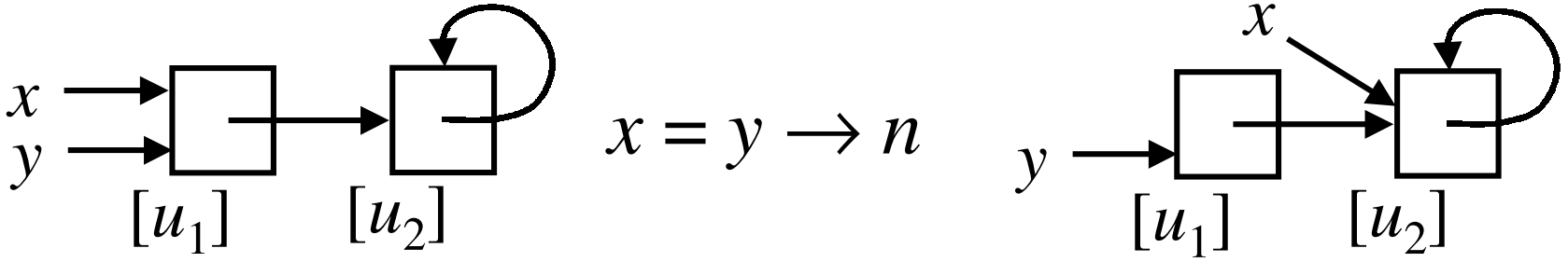


$x = y \rightarrow n$

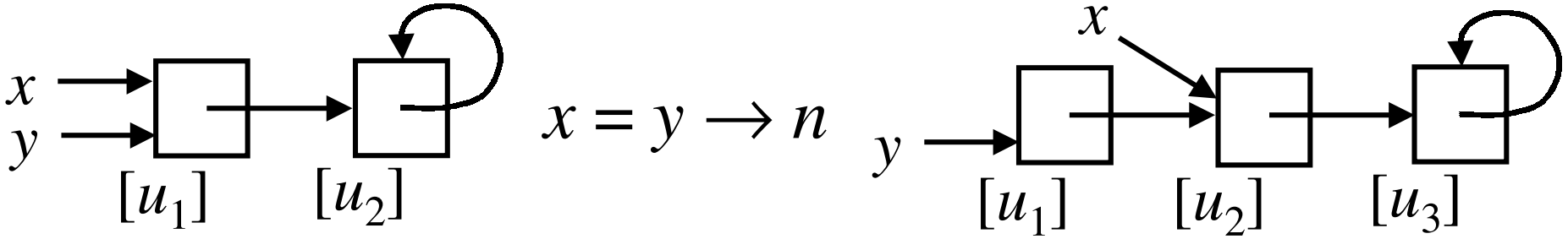


Materialization

[Chase, Wegman, & Zadeck 90]

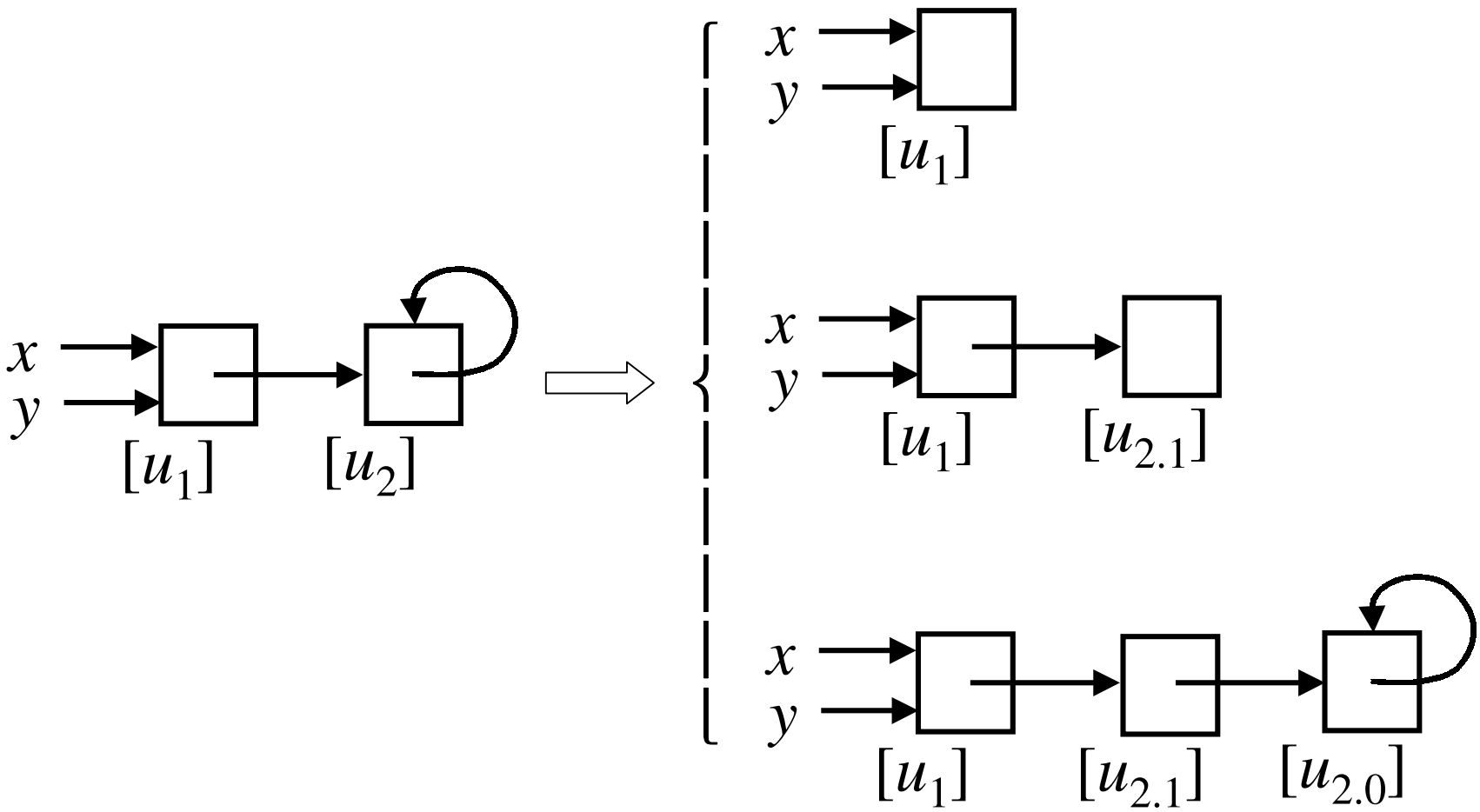


[Sagiv, Reps, & Wilhelm 96, 98]



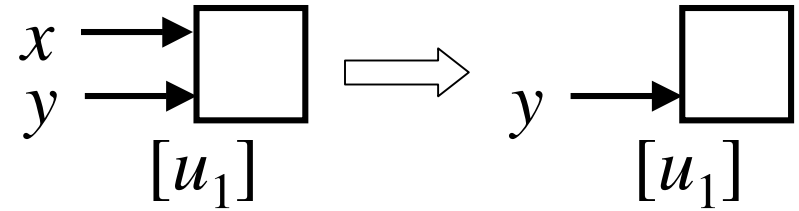
(1) Triplicate the Structure

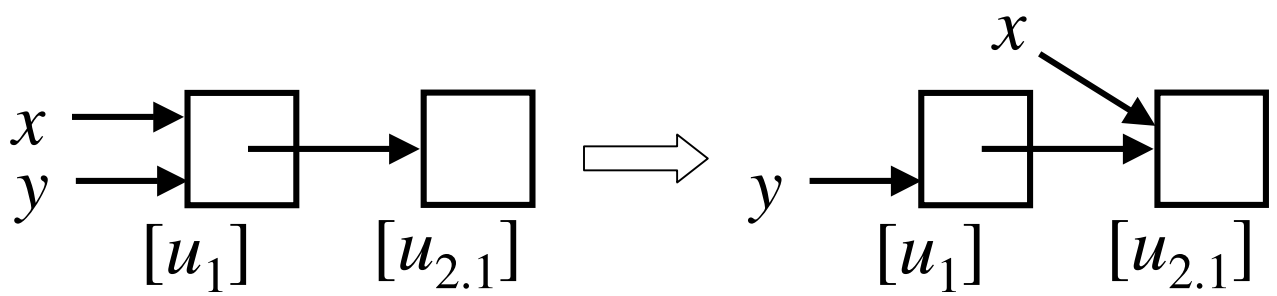
$$\varphi_x^{[x = y \rightarrow n]}(v) \triangleq \exists\, v_1 : y(v_1) \wedge n(v_1, v)$$

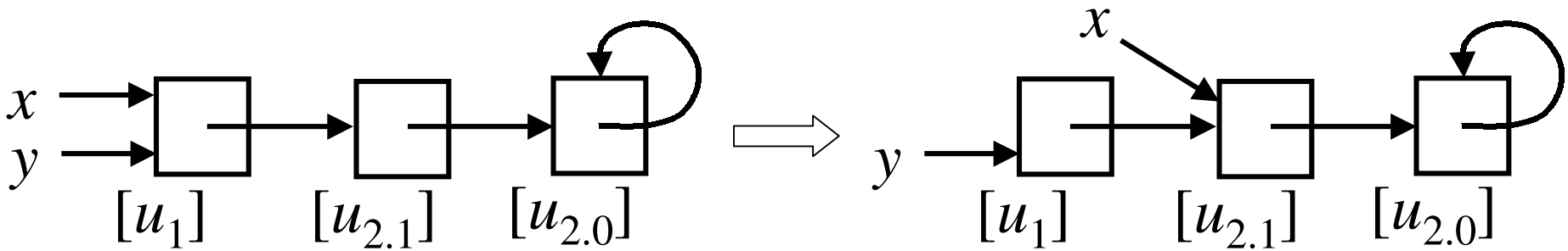


(2) Evaluate Predicate-Alteration Formulas

$$\varphi_x^{[x=y \to n]}(v) \triangleq \exists\, v_1 : y(v_1) \wedge n(v_1, v)$$





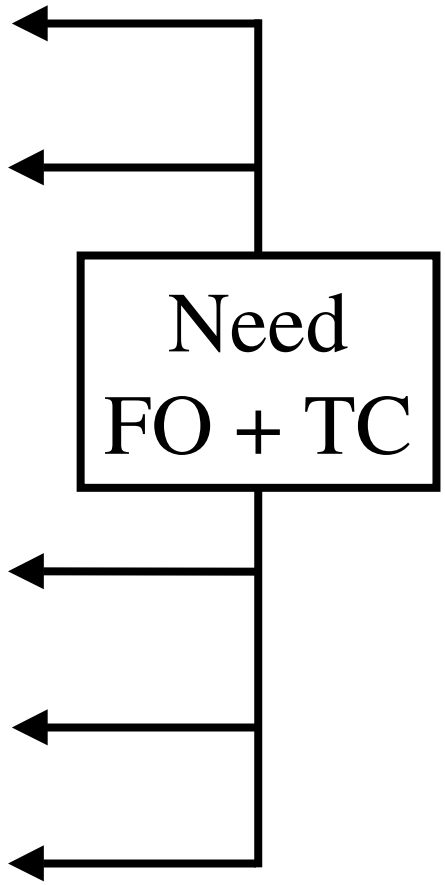


Additional Abstraction Predicates

- reachable-from-variable-x(v)
- acyclic-along-dimension-d(v)
  - à la ADDS
- doubly-linked(v)
- tree(v)
- dag(v)
- AVL trees:
  - balanced(v), left-heavy(v), right-heavy(v)
  - . . . but not via height arithmetic

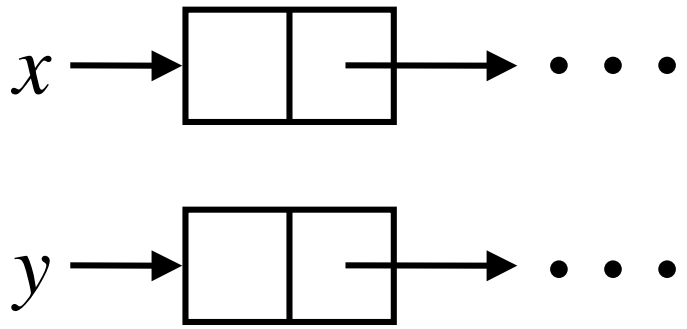
Additional Abstraction Predicates

- reachable-from-variable-$x(v)$
- acyclic-along-dimension-$d(v)$
  - à la ADDS
- doubly-linked(v)
- tree(v)
- dag(v)
- AVL trees:
  - balanced(v), left-heavy(v), right-heavy(v)
  - . . . but not via height arithmetic



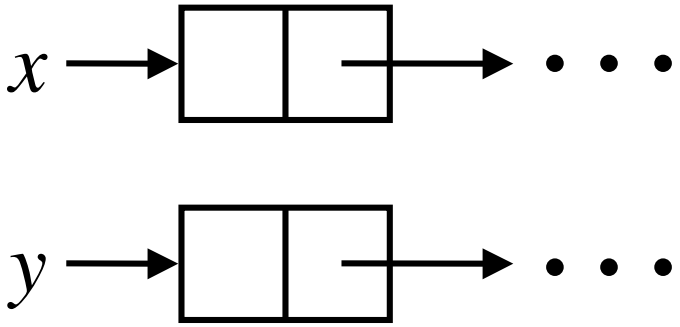
Formalizing “. . .”

Informal:

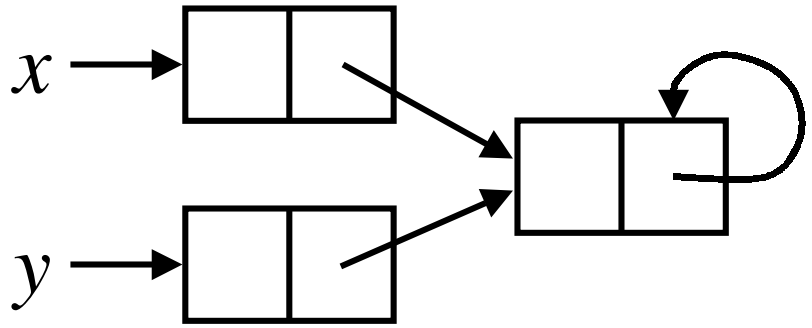


Formalizing “. . .”

Informal:

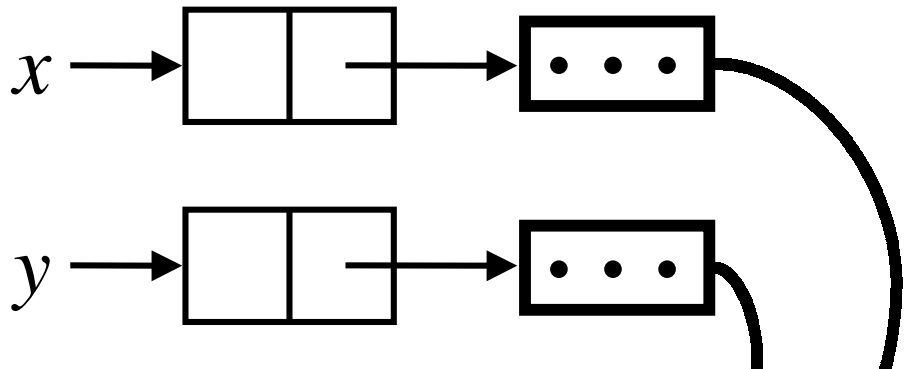


Formal:

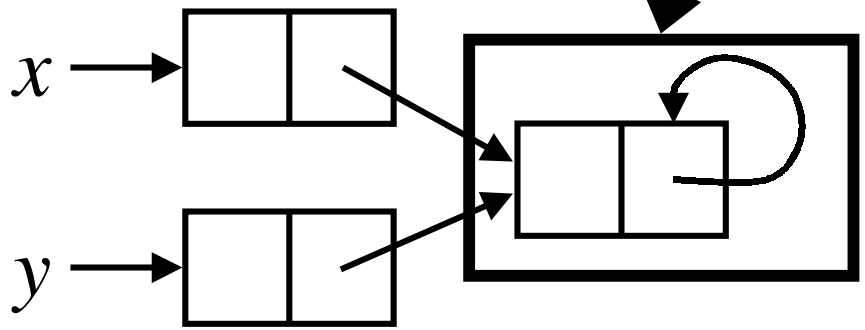


Formalizing “. . .”

Informal:

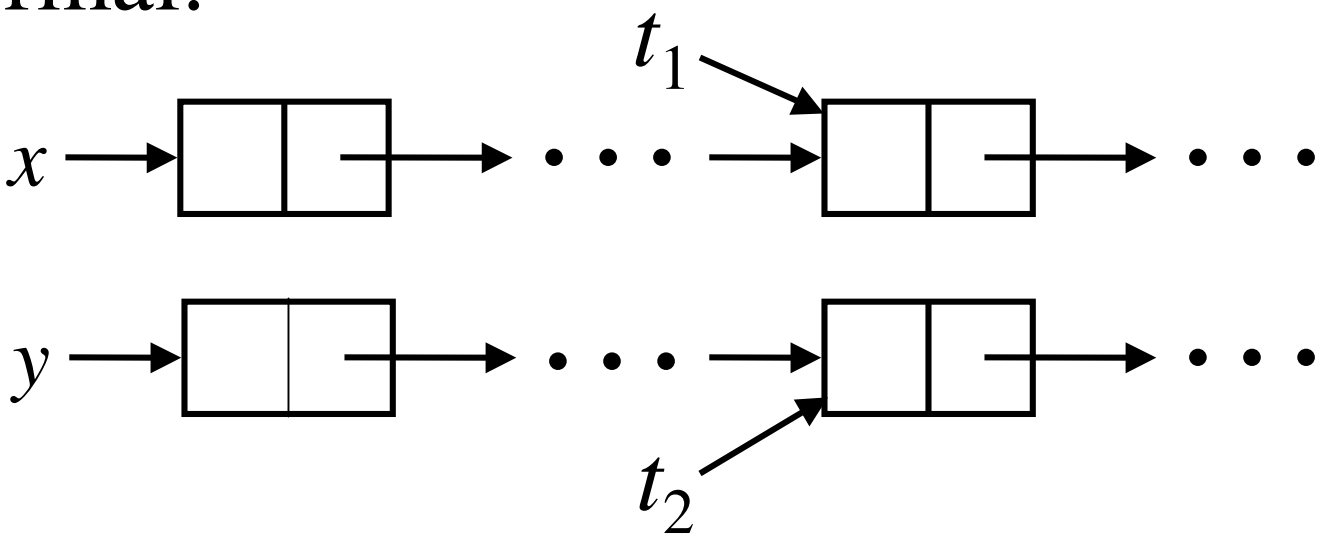


Formal:



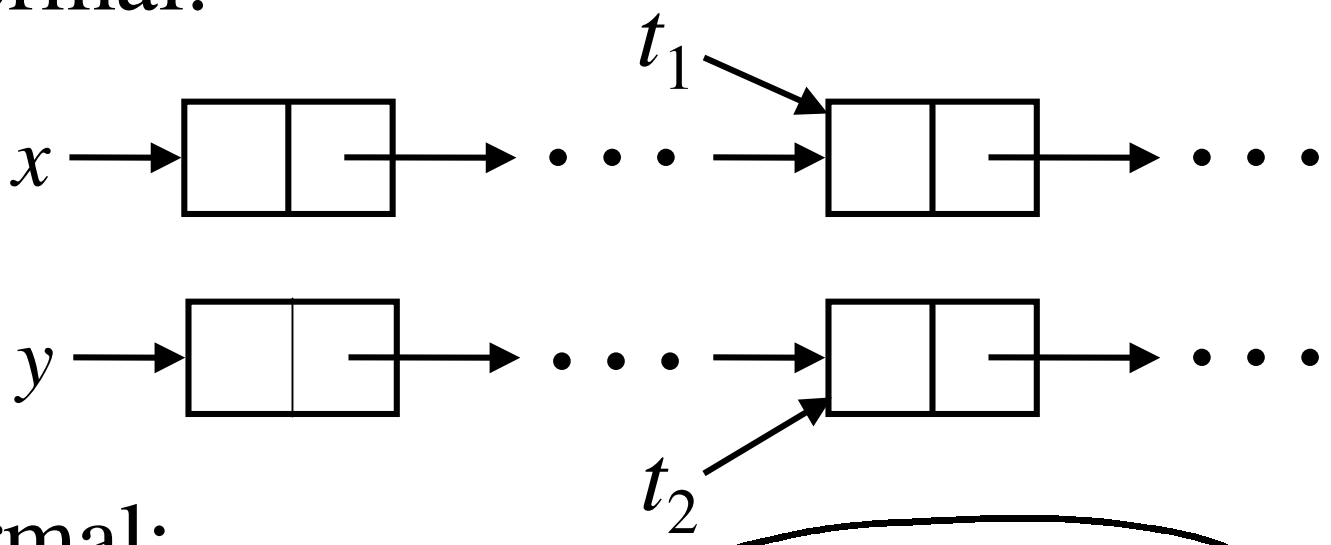
Formalizing “. . .”

Informal:

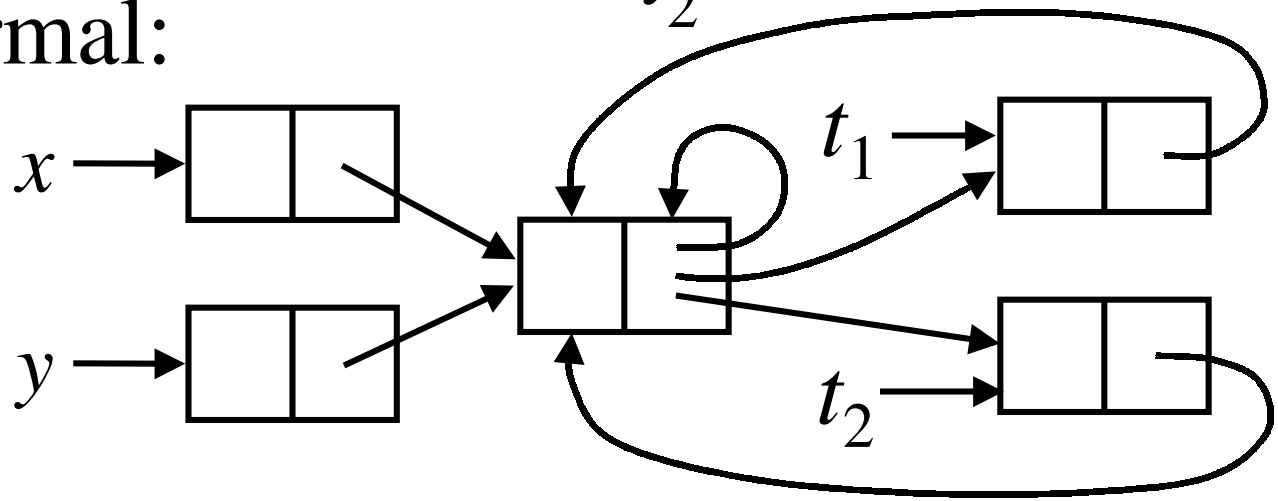


Formalizing “. . .”

Informal:

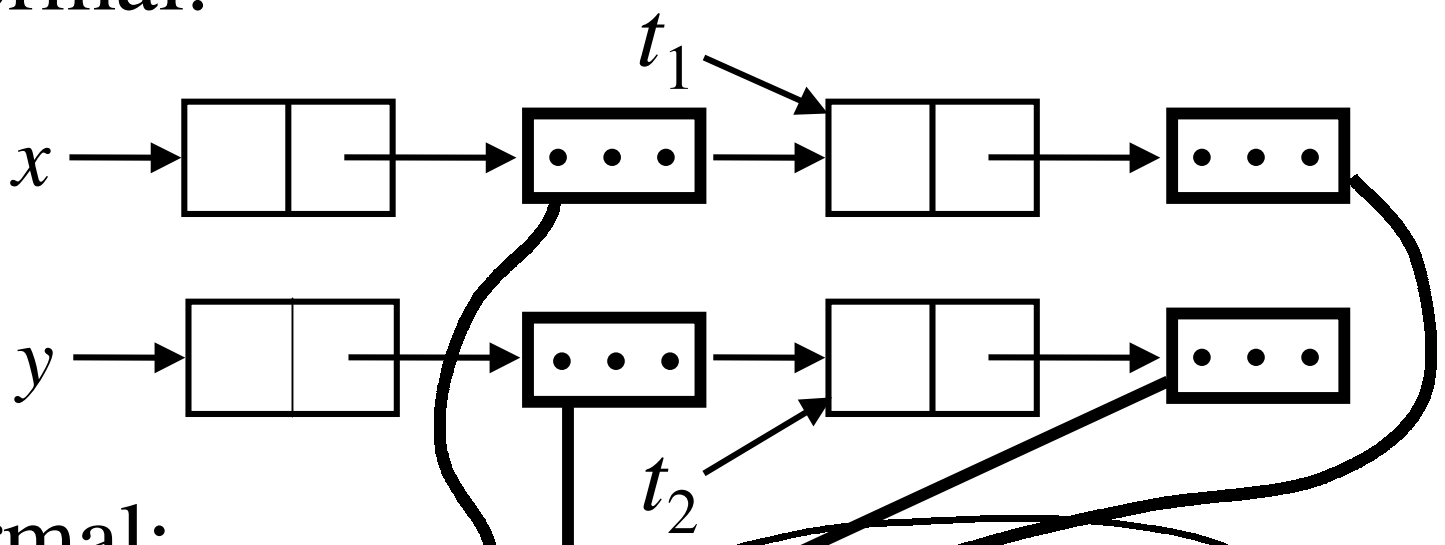


Formal:

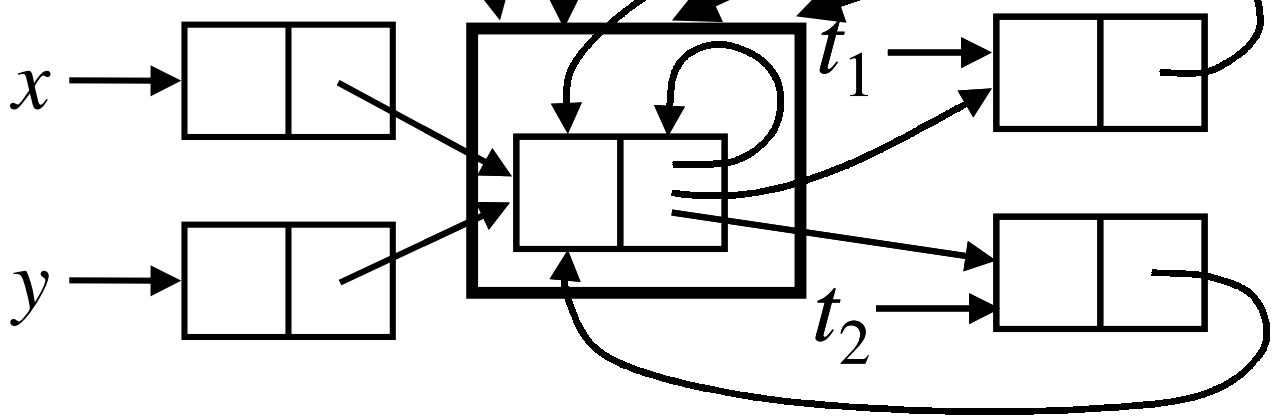


Formalizing “. . .”

Informal:

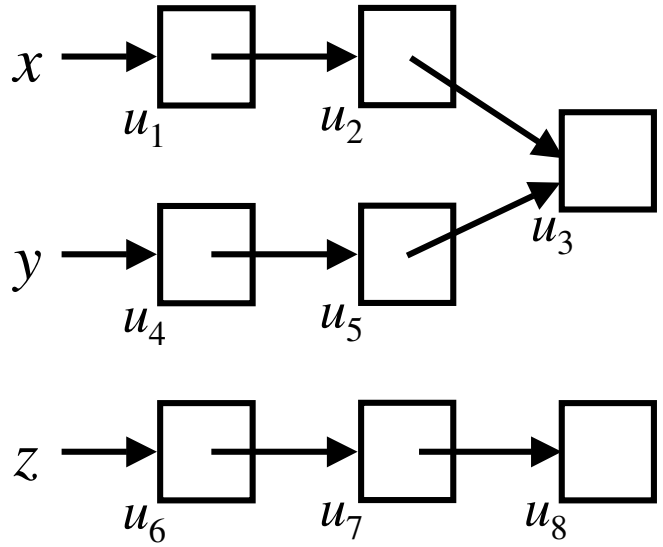


Formal:

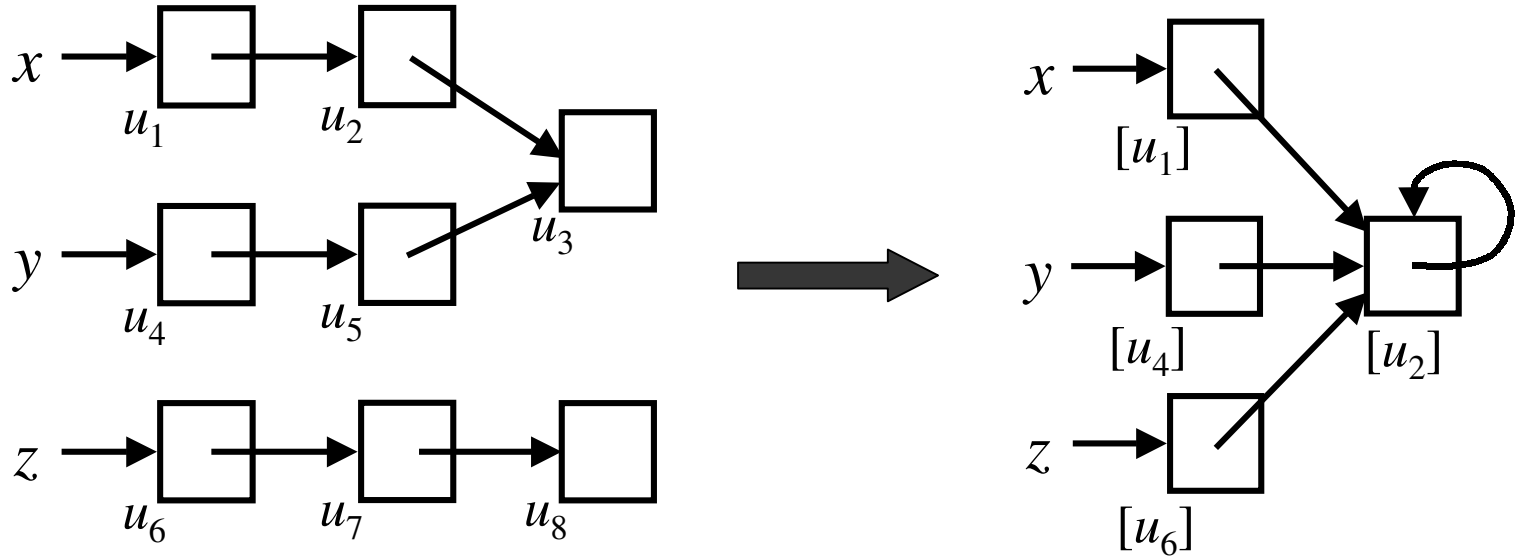


Treatment of Sharing ([SRW 96,98])

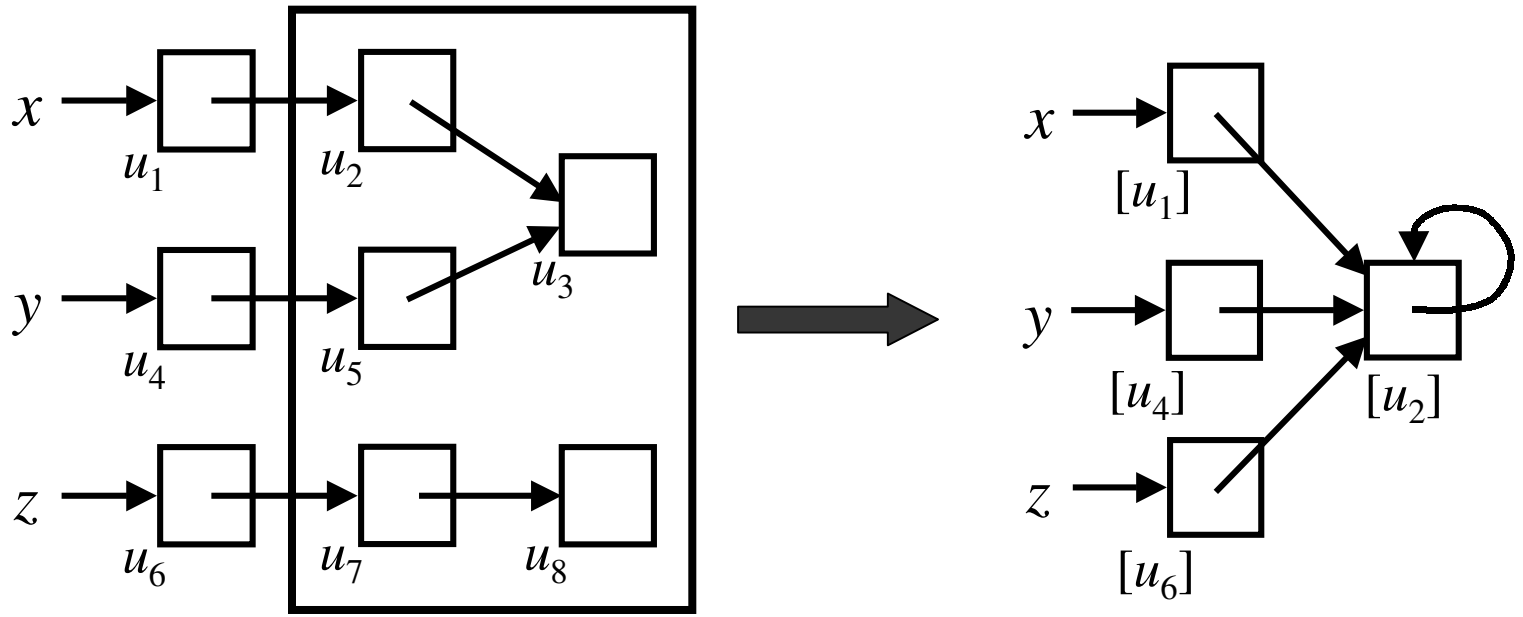
Treatment of Sharing ([SRW 96,98])



Treatment of Sharing ([SRW 96,98])

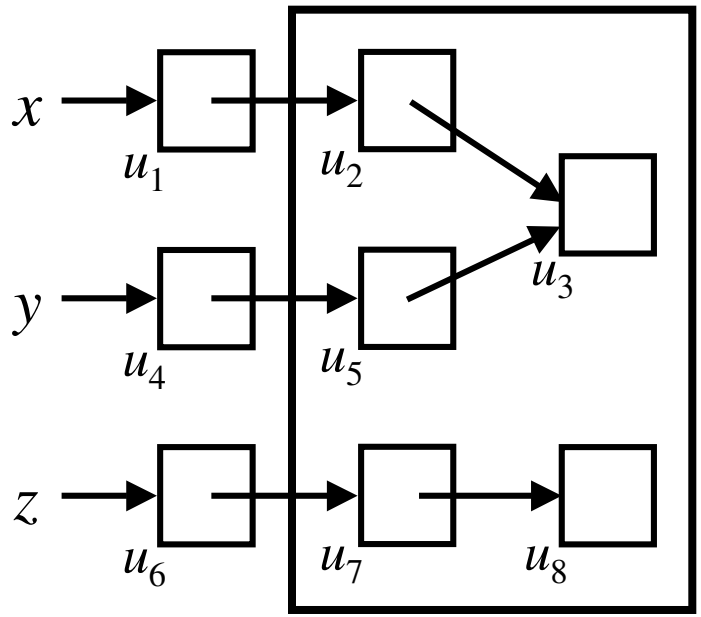


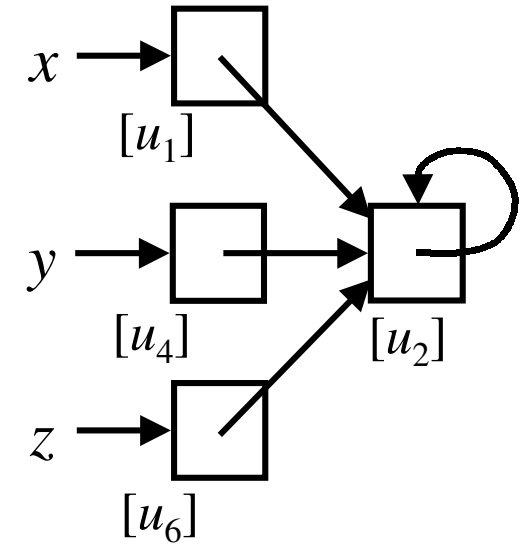
Treatment of Sharing ([SRW 96,98])



	$is(u)$
u_2	0
u_3	1
u_5	0
u_7	0
u_8	0

Treatment of Sharing ([SRW 96,98])

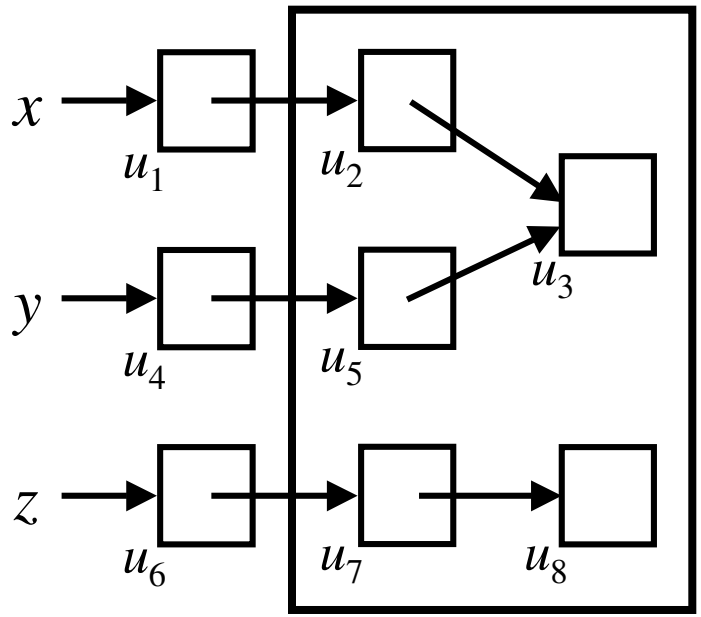


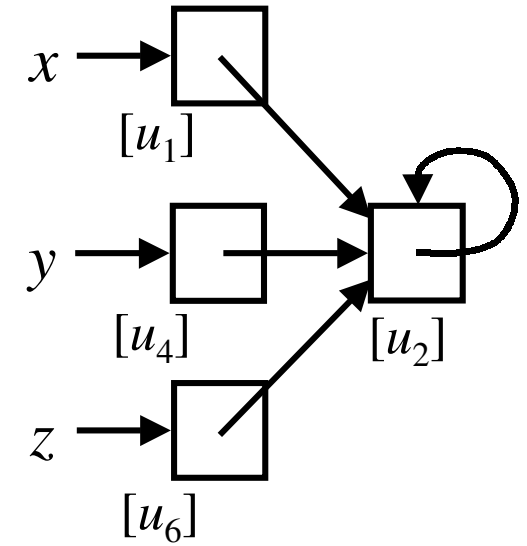


	$is(u)$
u_2	0
u_3	1
u_5	0
u_7	0
u_8	0

	$is(u)$
$[u_2]$	$\{0,1\}$

Treatment of Sharing ([SRW 96,98])

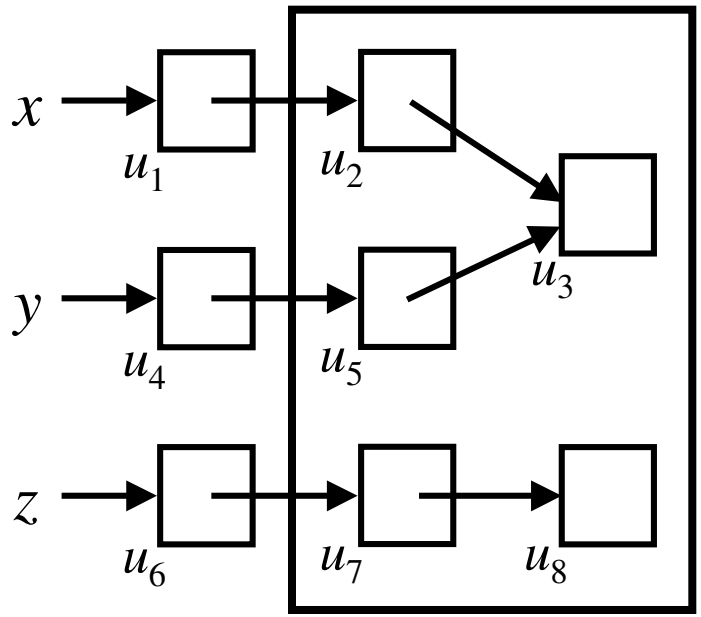


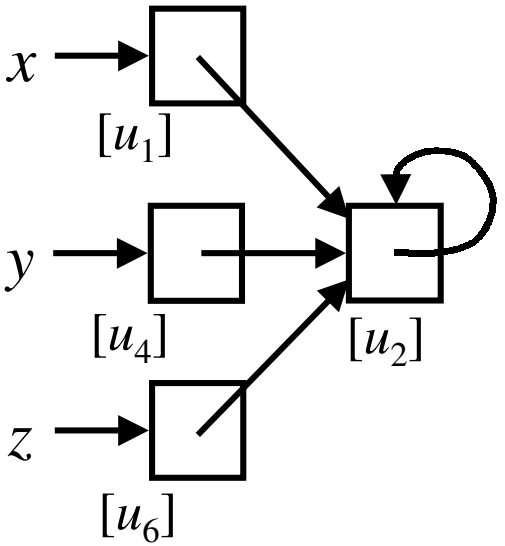


	$is(u)$
u_2	0
u_3	1
u_5	0
u_7	0
u_8	0

	$is(u)$
$[u_2]$	$\{0,1\}$

Treatment of Sharing ([SRW 96,98])





	$is(u)$
u_2	0
u_3	1
u_5	0
u_7	0
u_8	0

	$is(u)$
$[u_2]$	$\{0, \boxed{1}\}$

$\therefore$ z may point to a shared list

An Alternative to [SRW96,98]

An Alternative to [SRW96,98]

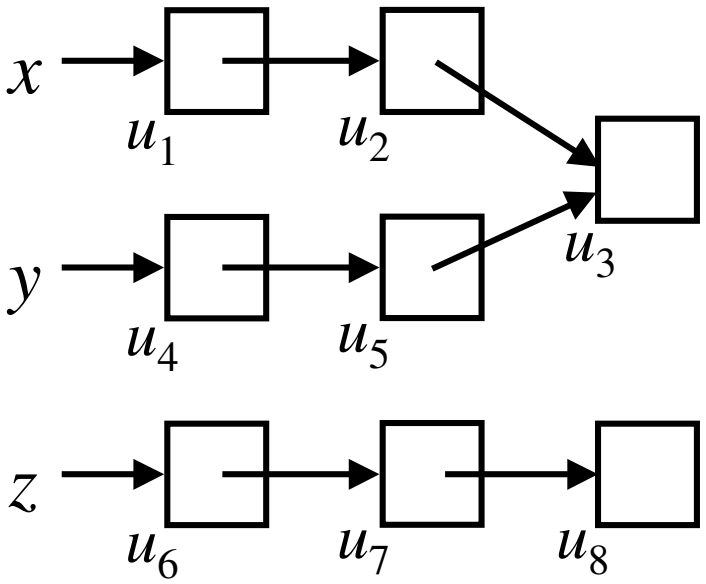
- $A = \{v \mid v \text{ is a program variable}\} \cup \{is\}$

An Alternative to [SRW96,98]

- $A = \{v \mid v \text{ is a program variable}\} \cup \{is\}$

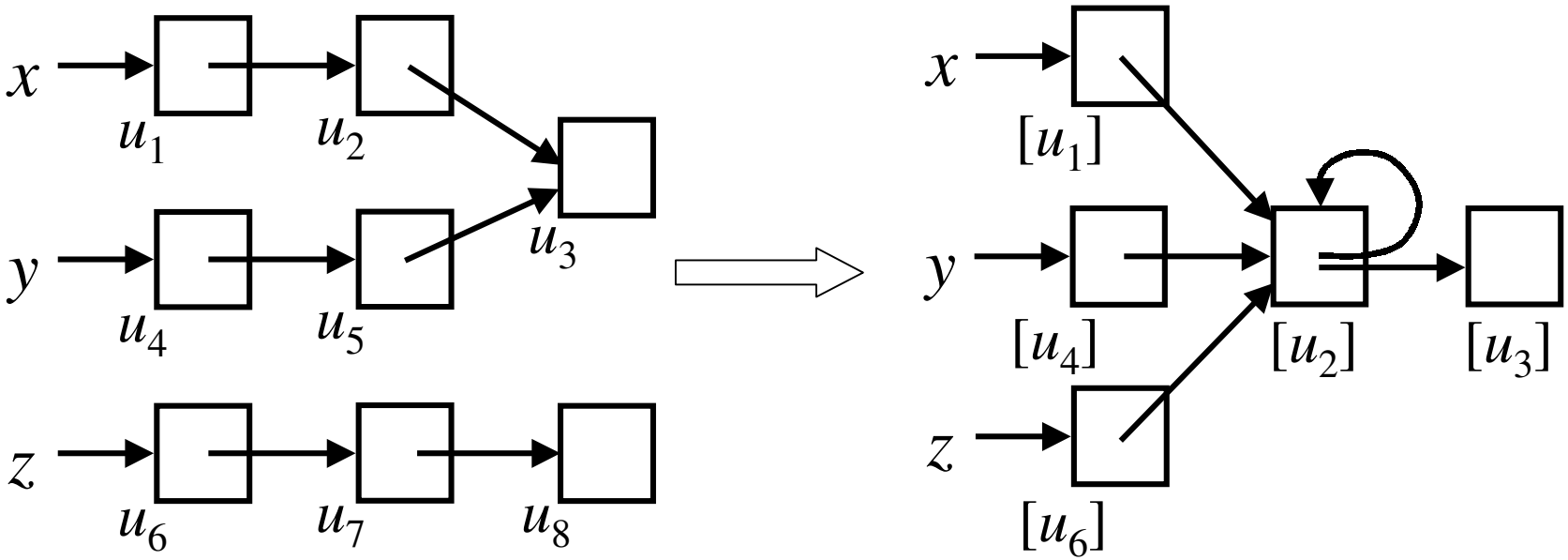
An Alternative to [SRW96,98]

- $A = \{v \mid v \text{ is a program variable}\} \cup \{is\}$



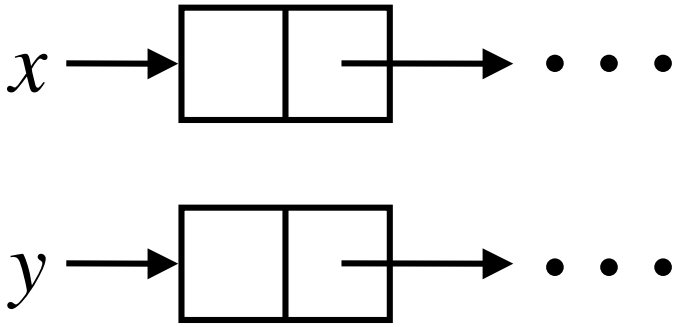
An Alternative to [SRW96,98]

- $A = \{v \mid v \text{ is a program variable}\} \cup \{is\}$

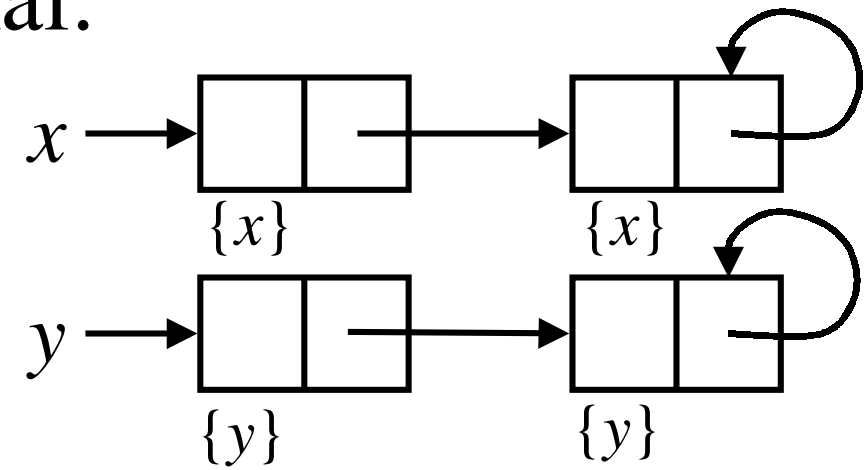


Formalizing “. . .”

Informal:

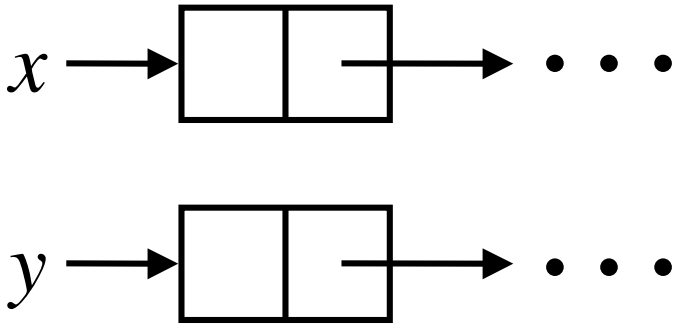


Formal:

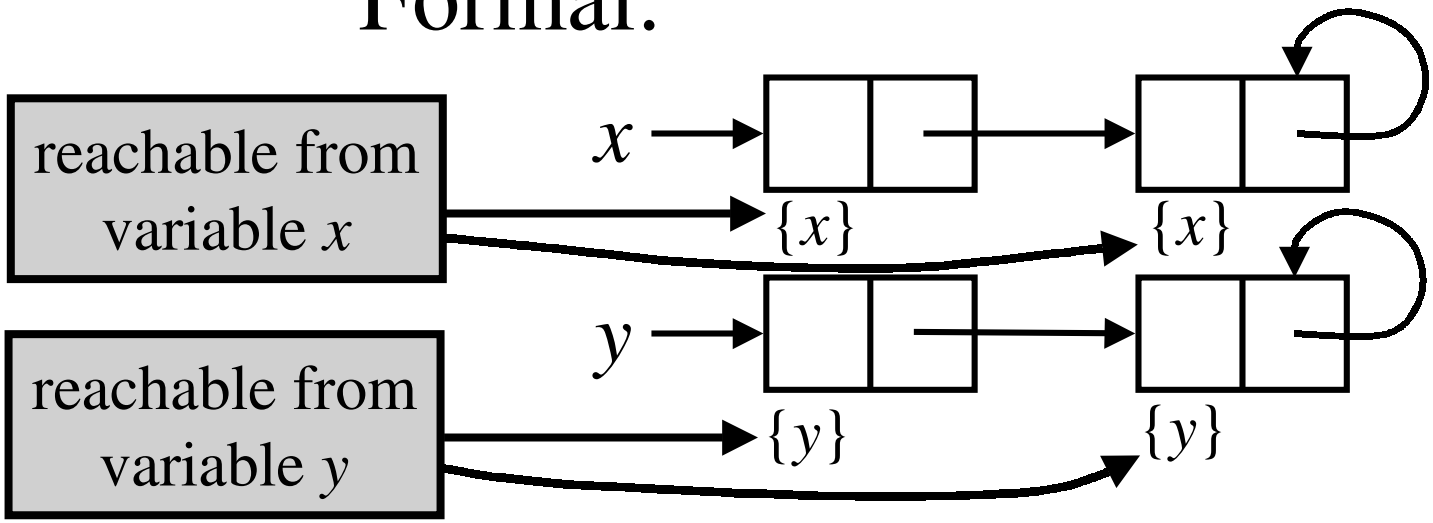


Formalizing “. . .”

Informal:

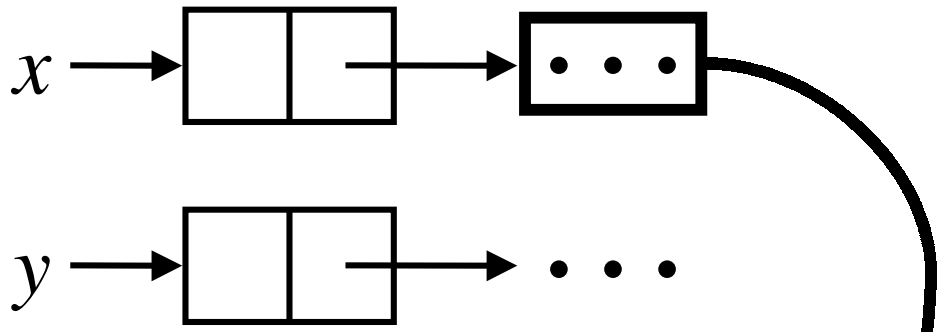


Formal:

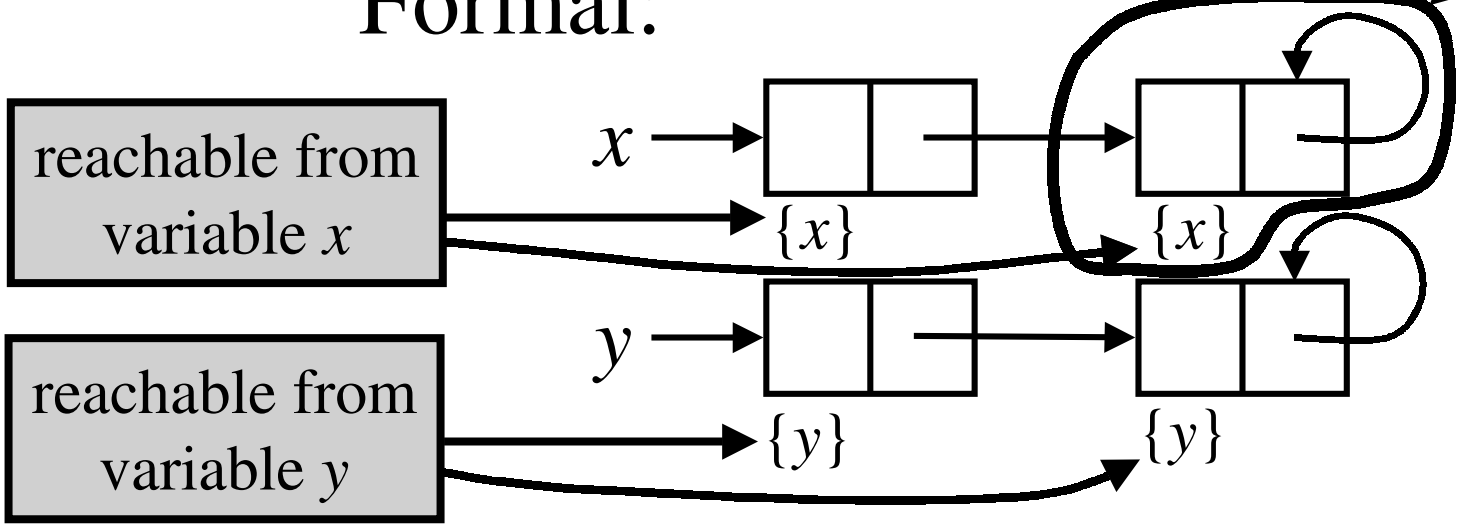


Formalizing “. . .”

Informal:

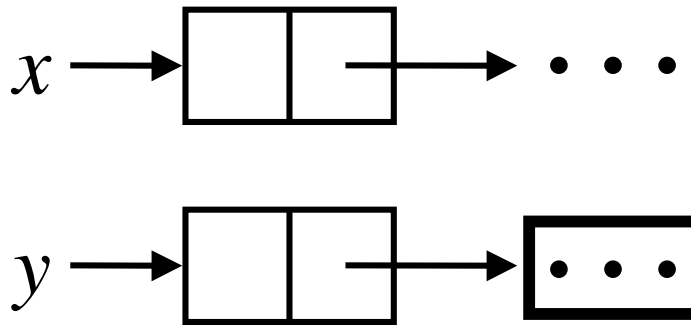


Formal:

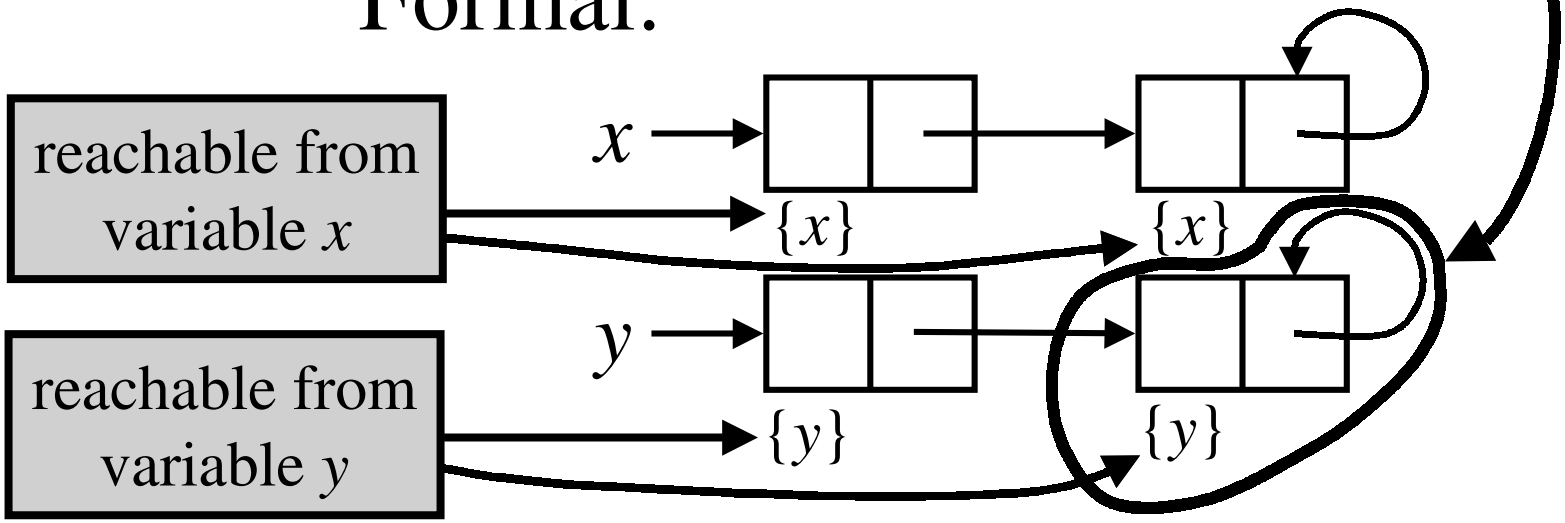


Formalizing “. . .”

Informal:

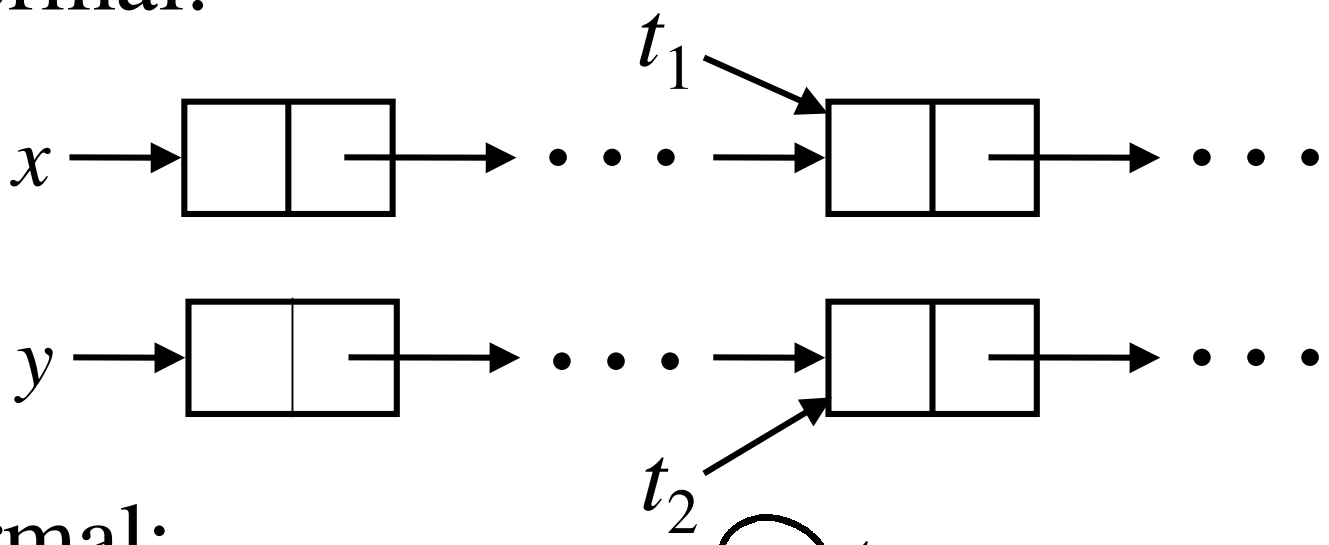


Formal:

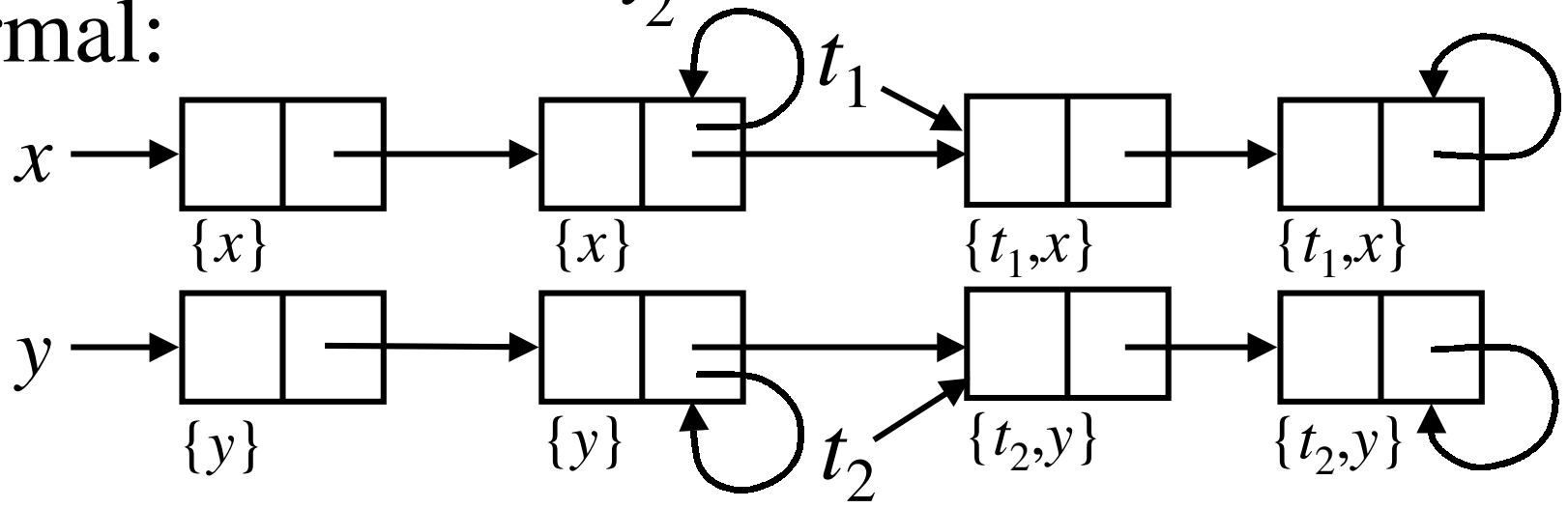


Formalizing “. . .”

Informal:

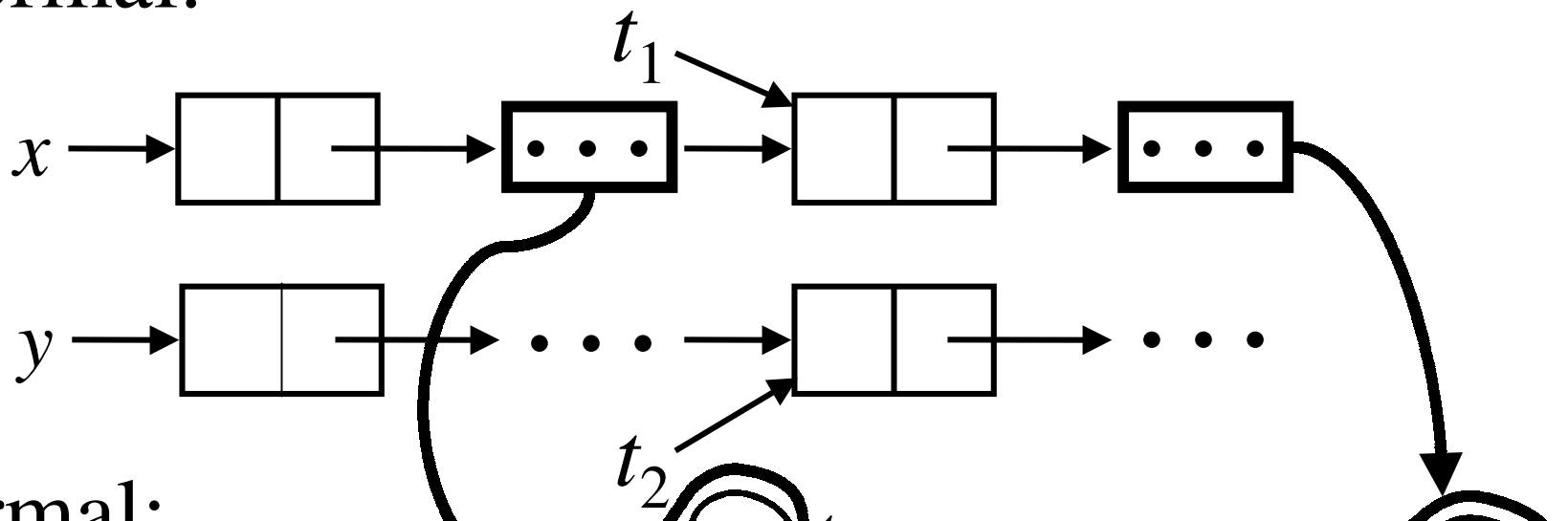


Formal:

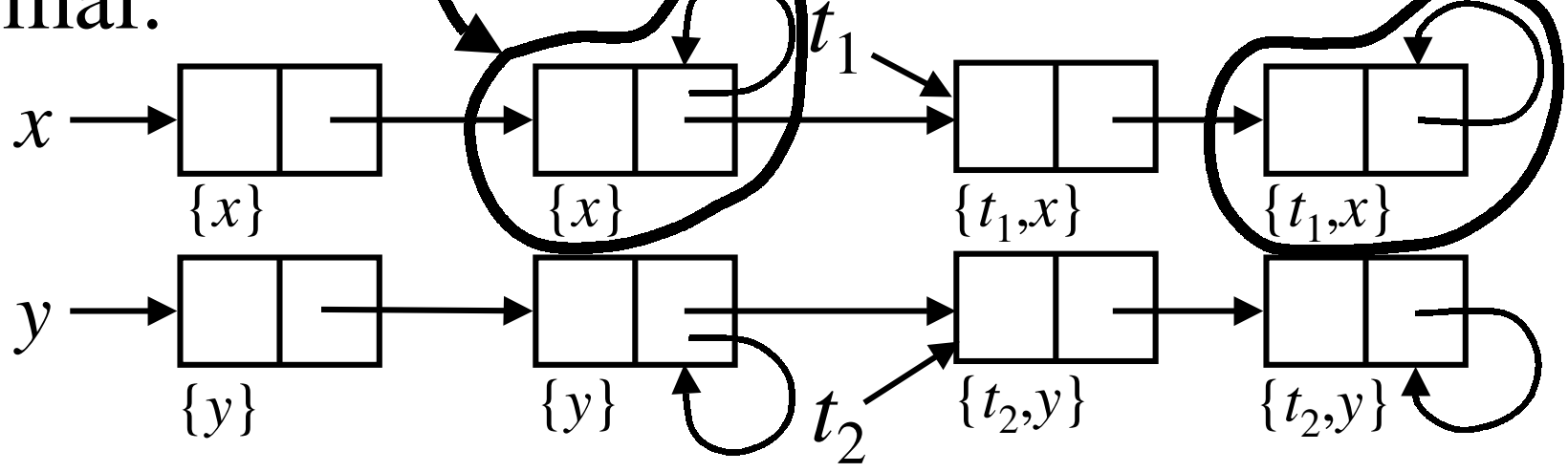


Formalizing “. . .”

Informal:

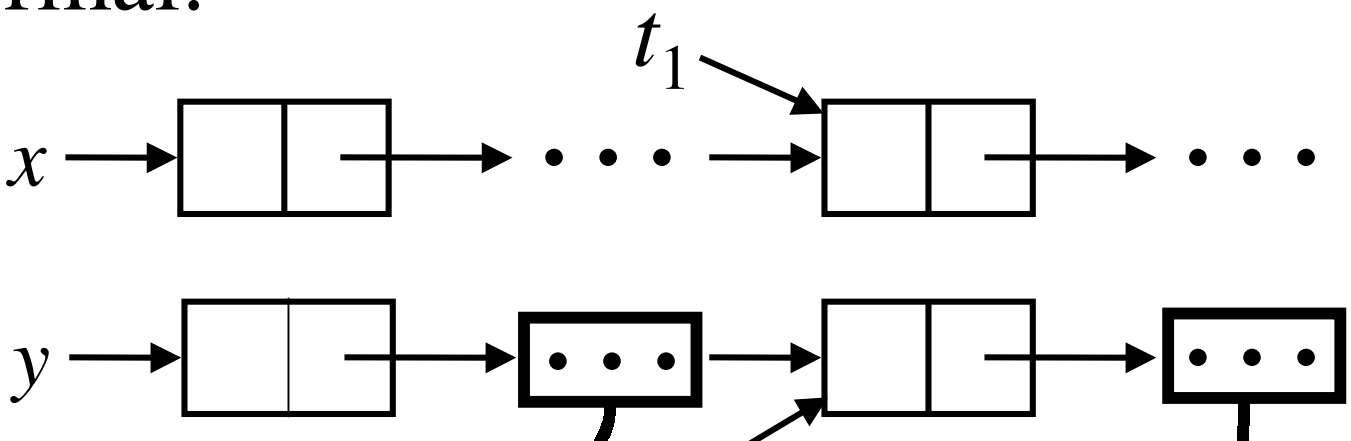


Formal:

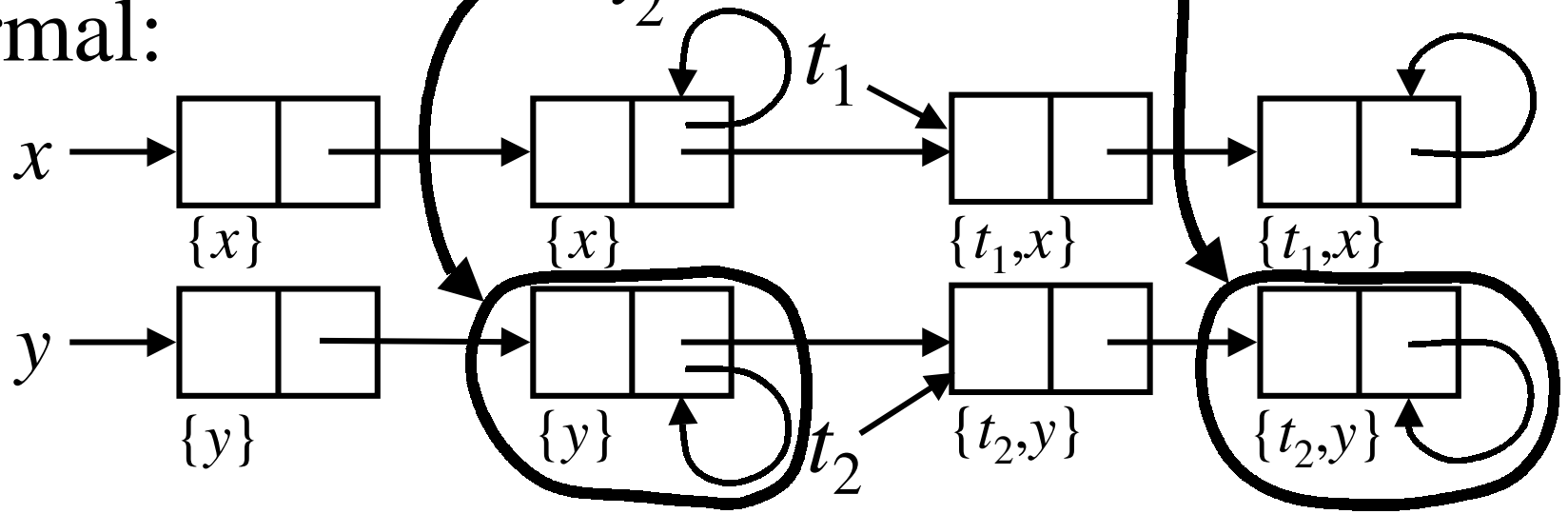


Formalizing “. . .”

Informal:



Formal:



Summary

- Parametric framework
- Three-valued logic arises from abstraction
- Three-valued logic also allows:
  - Materialization
  - Conservative extraction of properties
  - Interpretation of program conditions
- Simpler proofs