Multi-Pushdown Automata with Data

joint work with

Parosh Abdulla

M. Faouzi Atig

Outline

- Background
- Model
- Gap-Order Constraints
- Signatures
- Reachability Algorithm
- Applications

Background

concurrent recursive programs

undecidable in general

"decidable under bounded context switch"

concurrent recursive programs with data

current presentation

"decidable for ordered data under bounded context switch"

Multiple-Stack Processes

Multiple-Stack Processes + Data

Boolean recursive programs

undecidable in general

recursive programs with data

"decidable for ordered data"

Pushdown Processes

Pushdown Processes + Data

Outline

- Background
- Model
- Gap-Order Constraints
- Signatures
- Reachability Algorithm
- Applications

- Syntax
- Configurations
- Runs
- Reachability

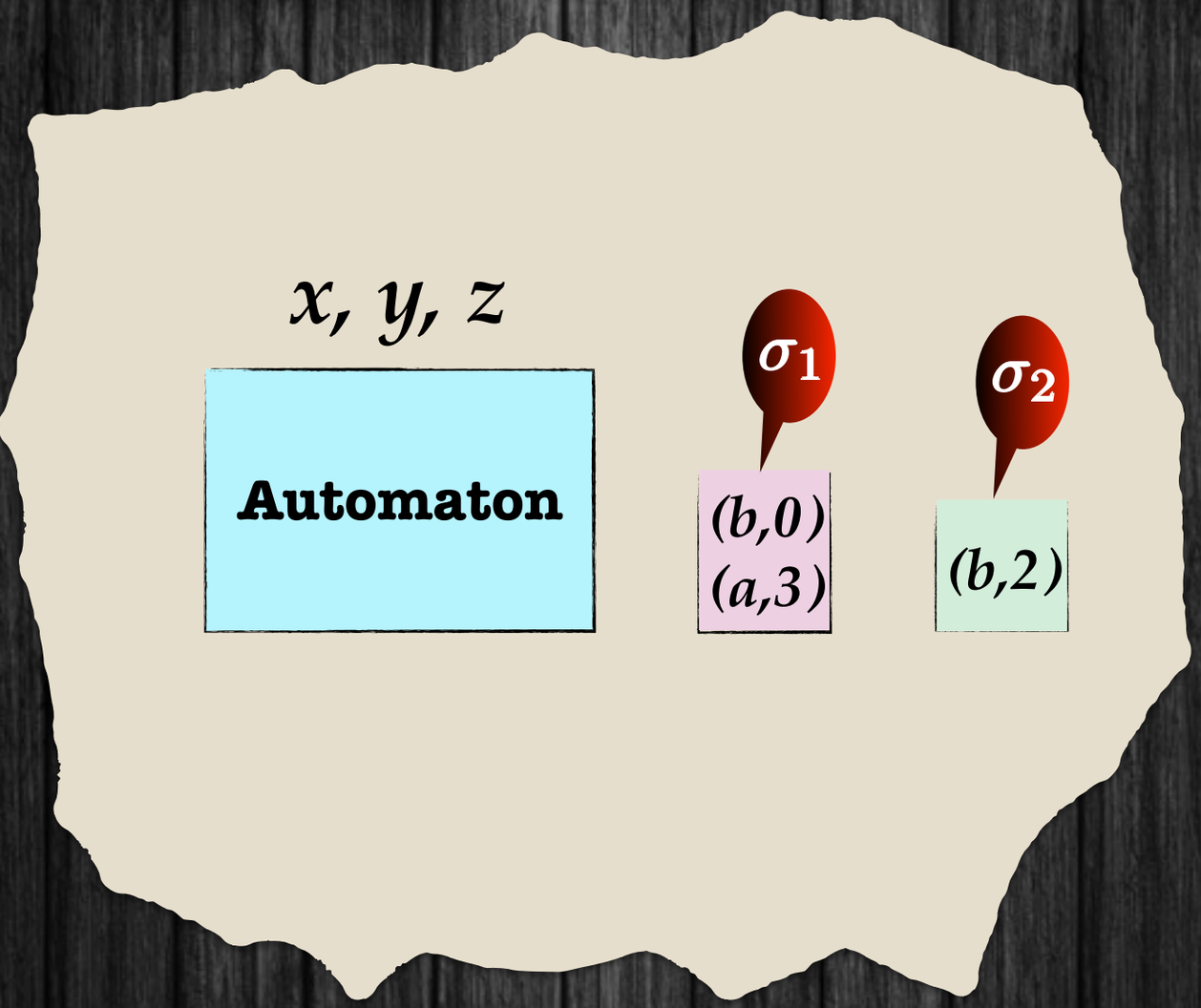
Model

finite set of variables over $\mathbb{N}$

x, y, z

finite set of stacks

σ_1, σ_2



Model

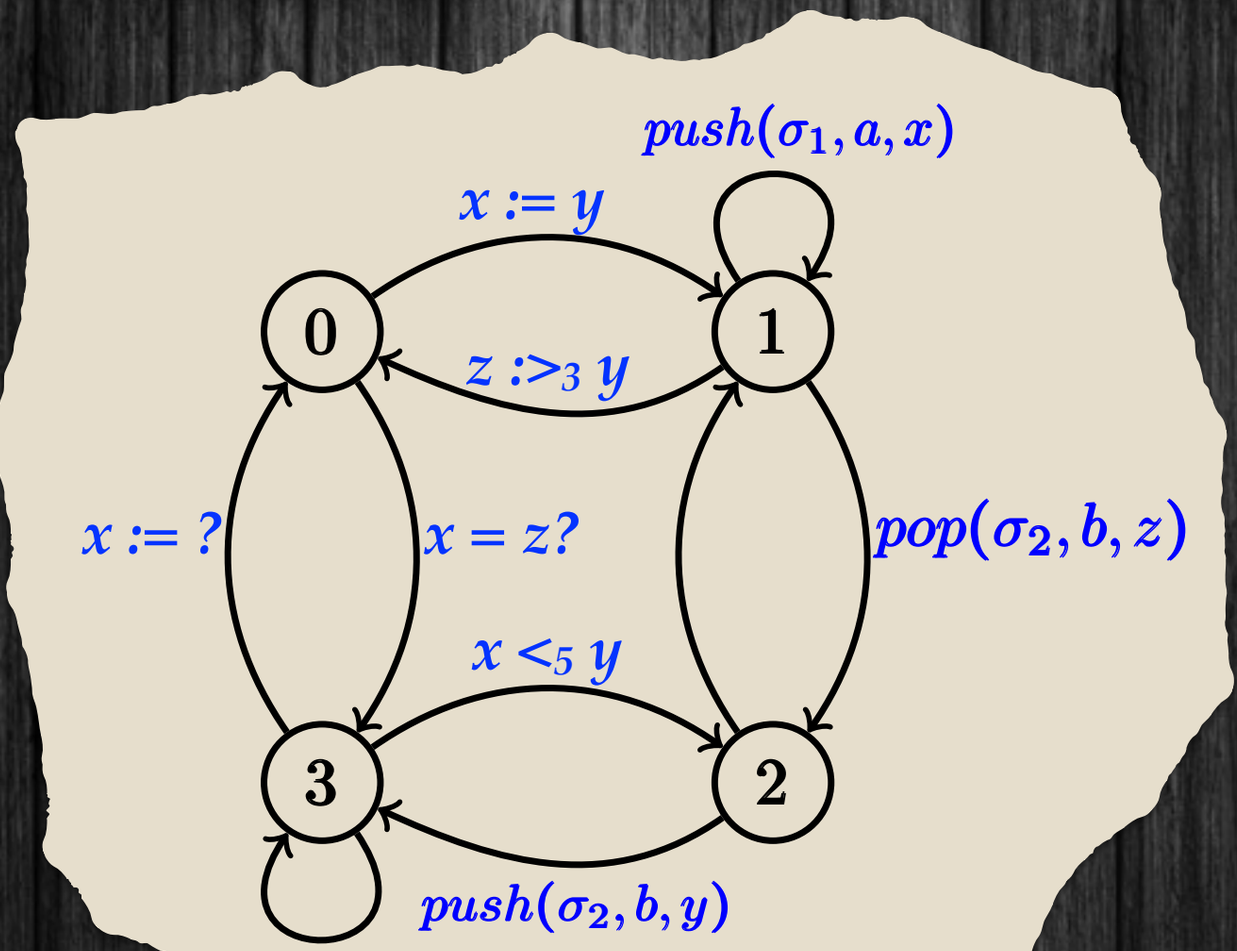
finite set of variables over $\mathbb{N}$

x, y, z

finite set of stacks

σ_1, σ_2

$v(x)$: current value of x



Model

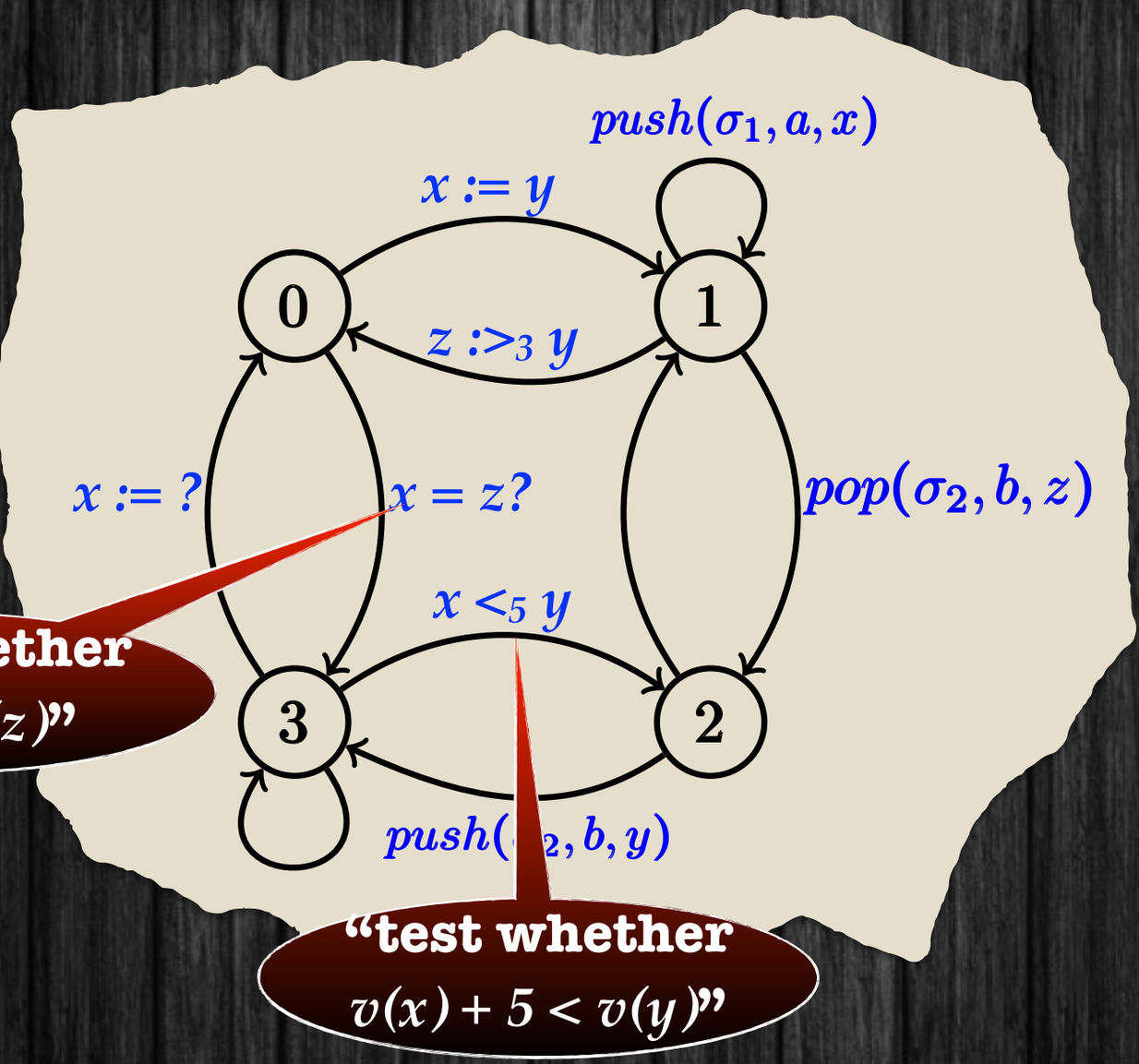
finite set of variables over $\mathbb{N}$

x, y, z

finite set of stacks

σ_1, σ_2

$v(x)$: current value of x



"test whether $v(x) = v(z)$"

"test whether $v(x) + 5 < v(y)$"

Model

finite set of variables over $\mathbb{N}$

x, y, z

$v(x)$: current value of x

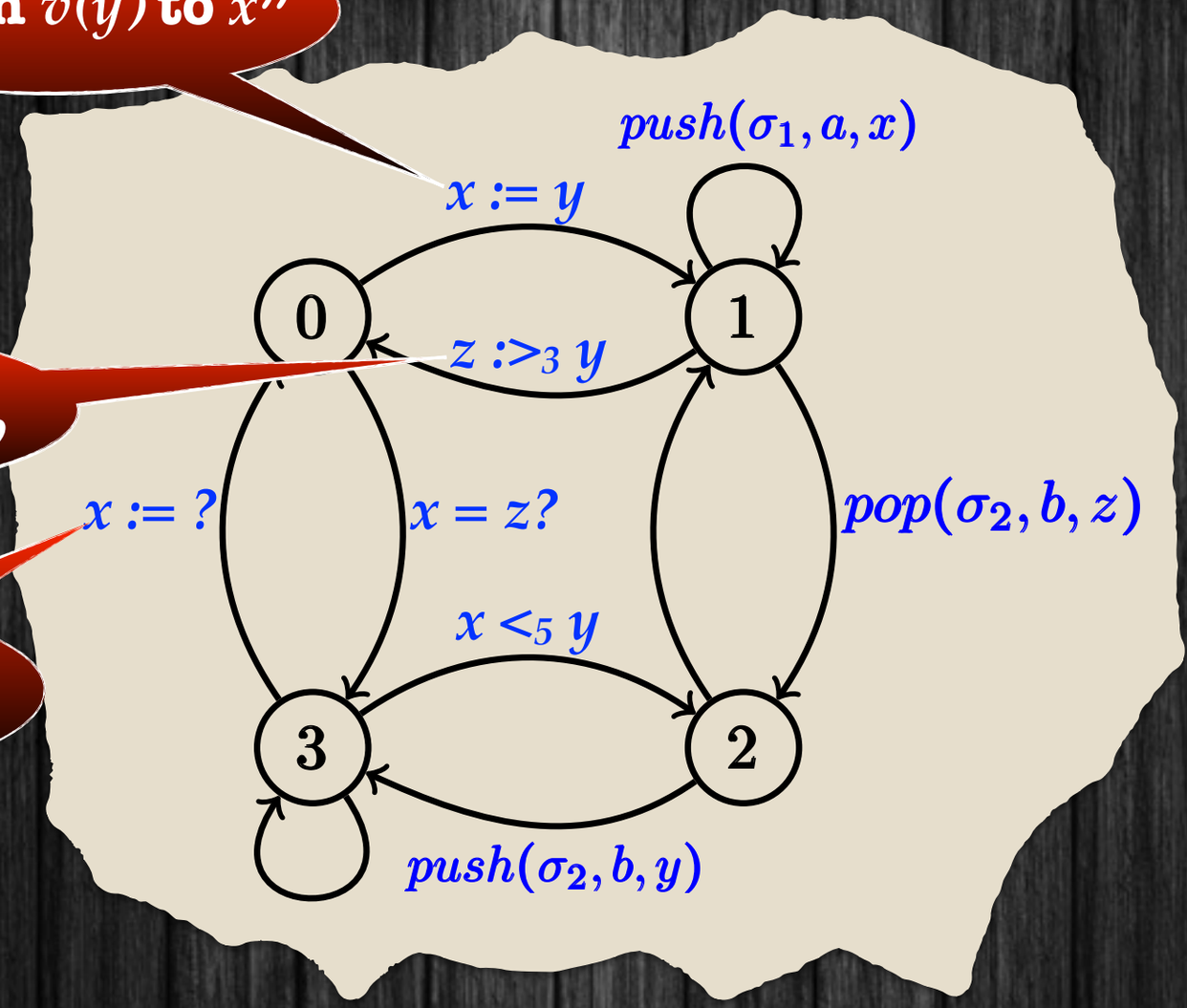
finite set of stacks

σ_1, σ_2

"assign $v(y)$ to x"

"assign some $u > v(y) + 3$ to z"

"assign some u to y"



Model

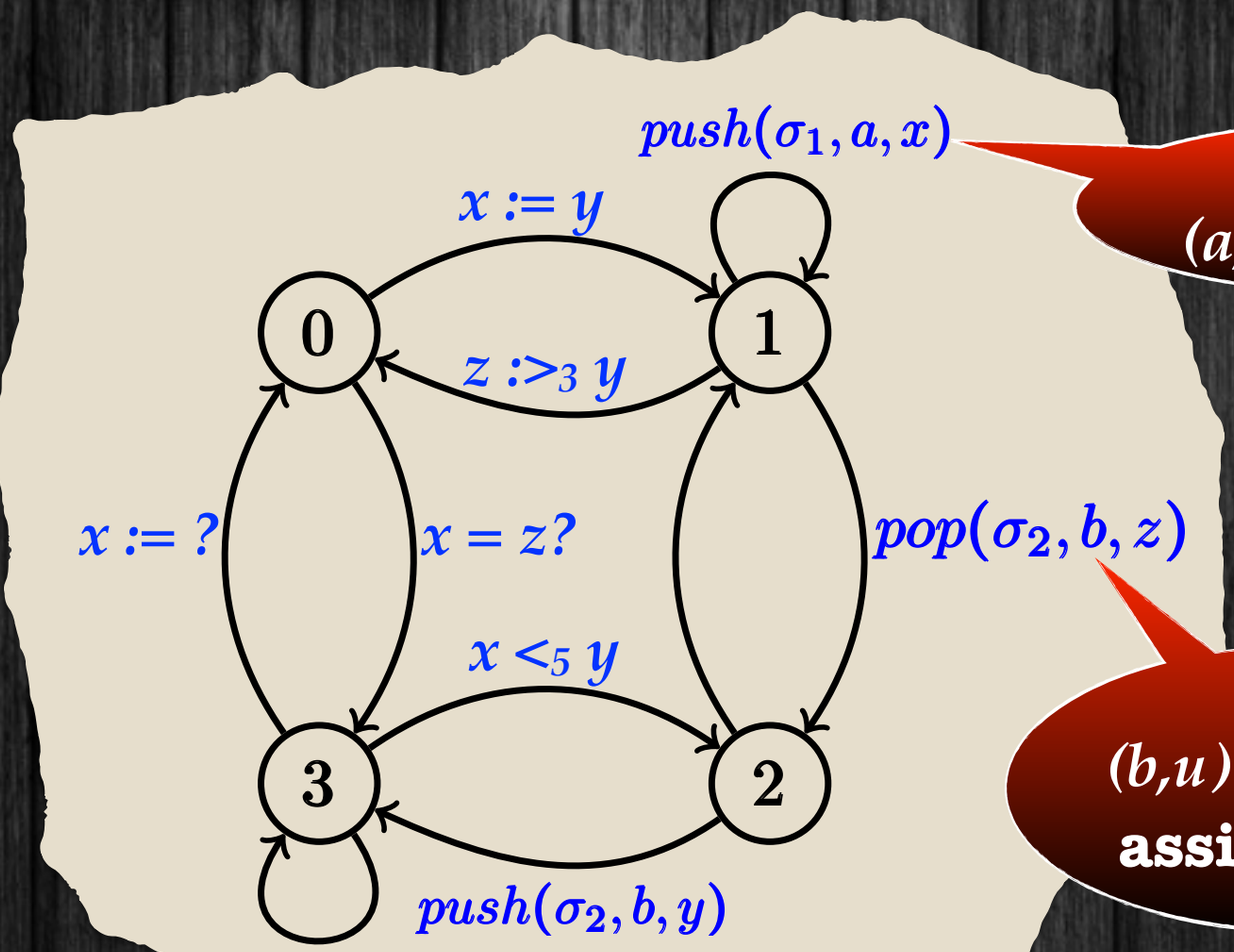
finite set of variables over $\mathbb{N}$

x, y, z

$v(x)$: current value of x

finite set of stacks

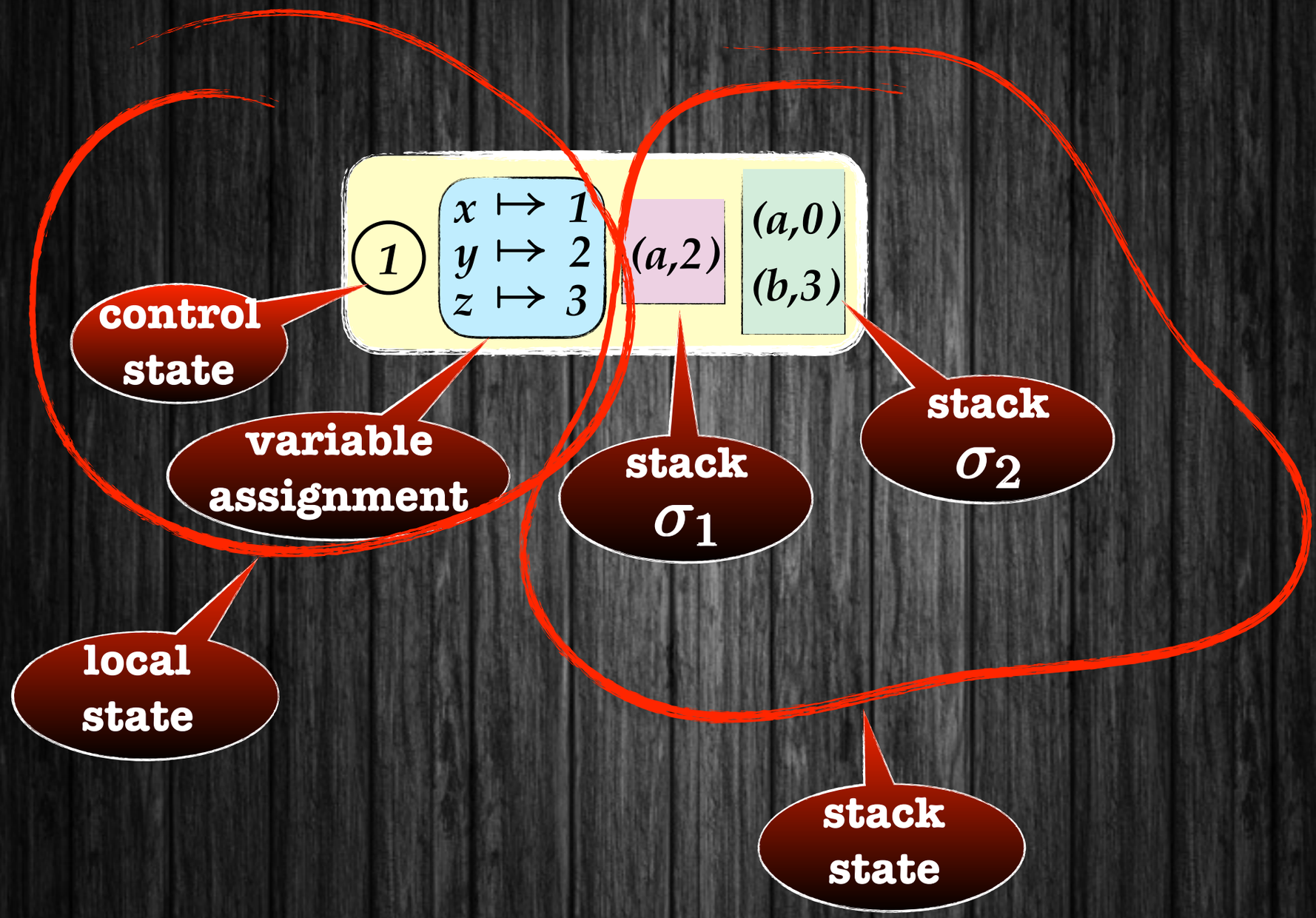
σ_1, σ_2



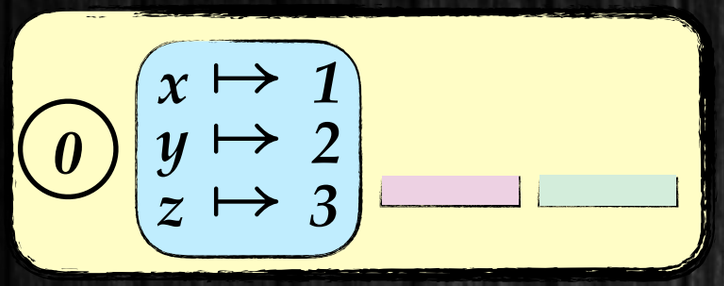
"push $(a, v(x))$ to σ_1"

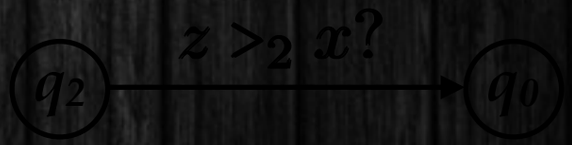
"pop (b, u) from σ_2 , assign u to z"

Configurations

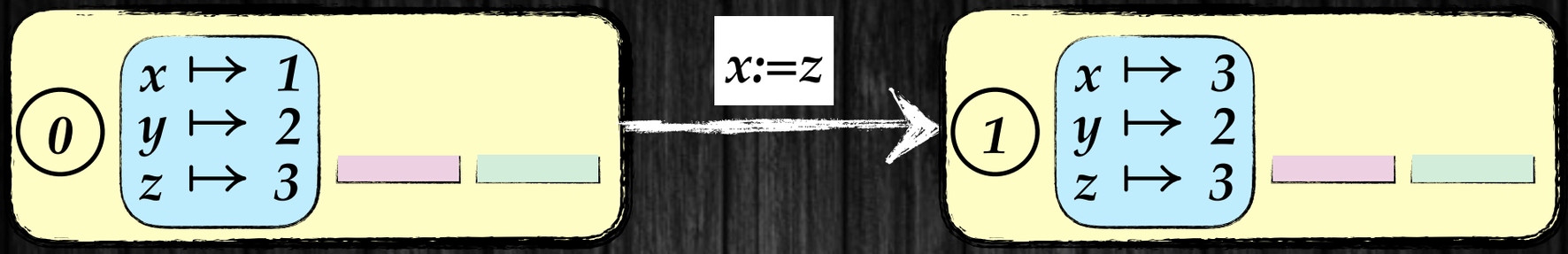


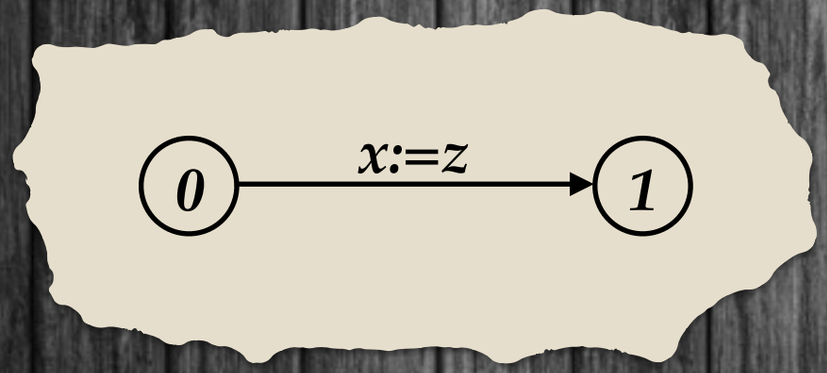
Runs

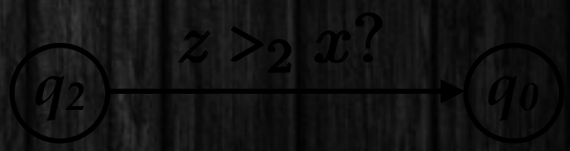




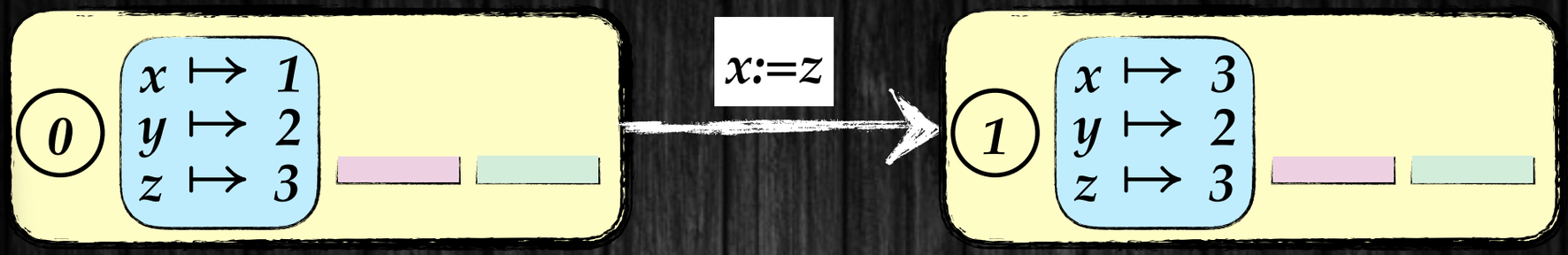
Runs



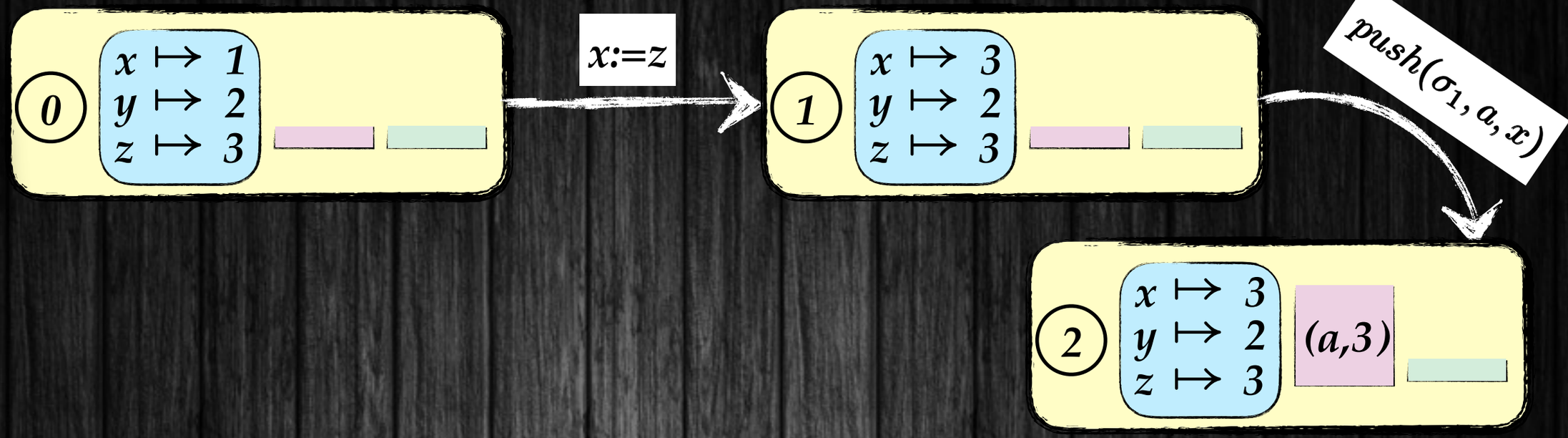


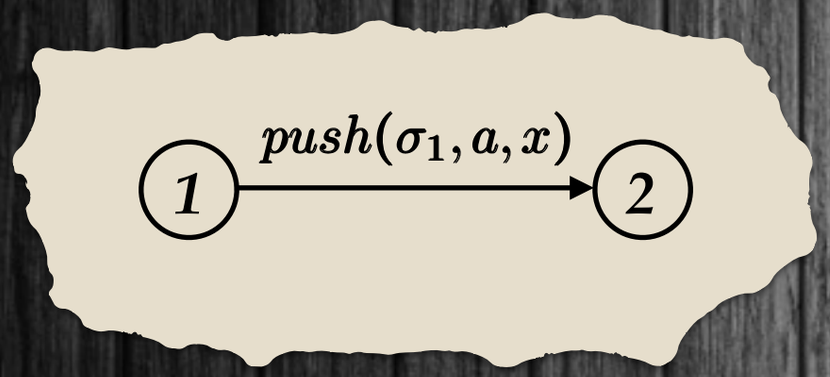


Runs

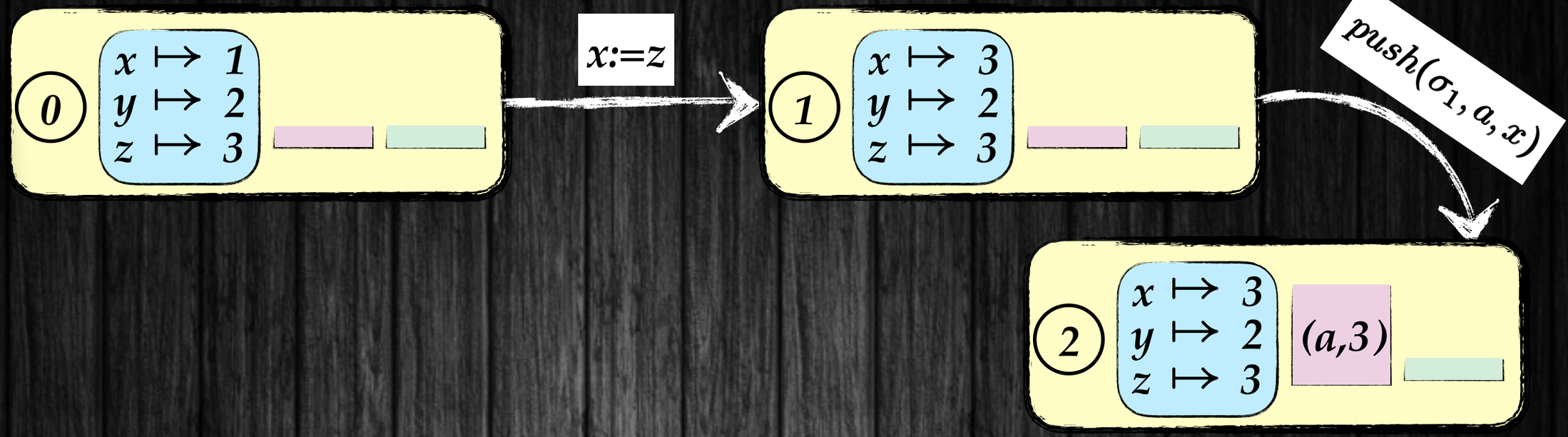


Runs

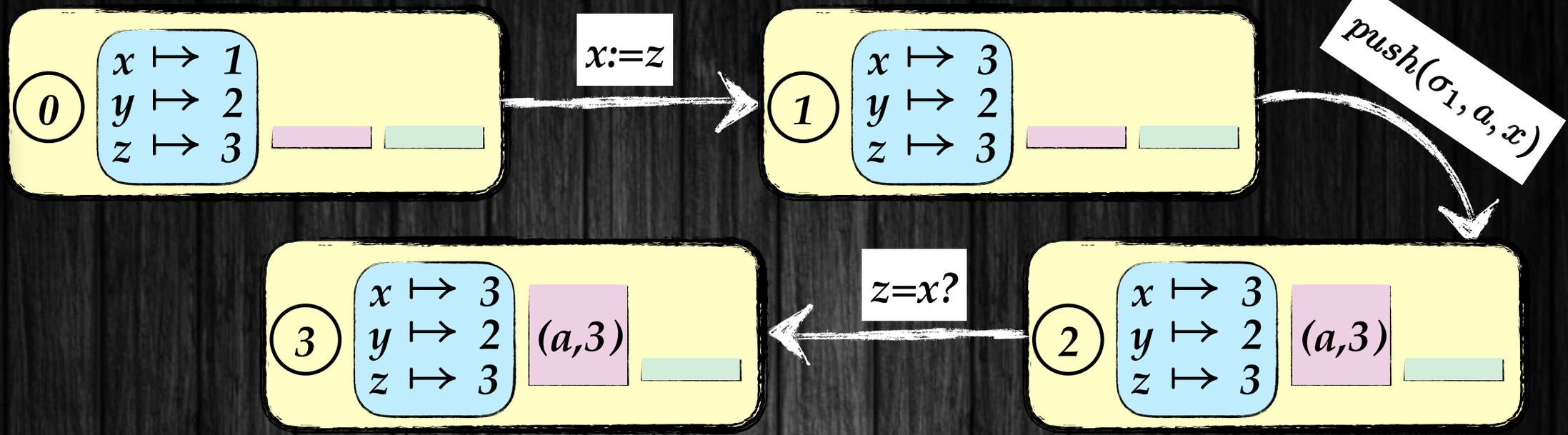


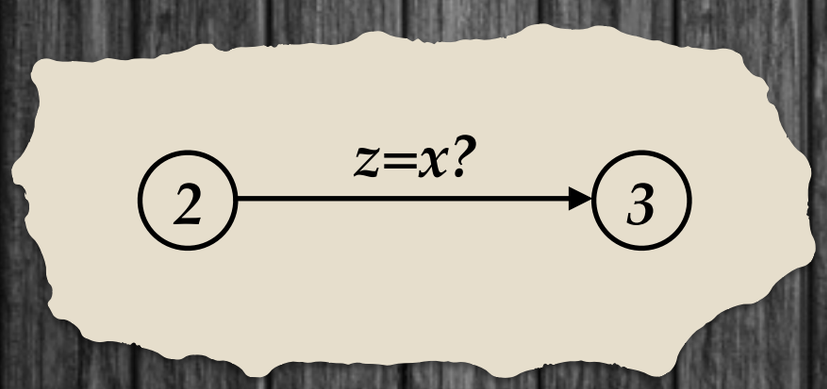


Runs

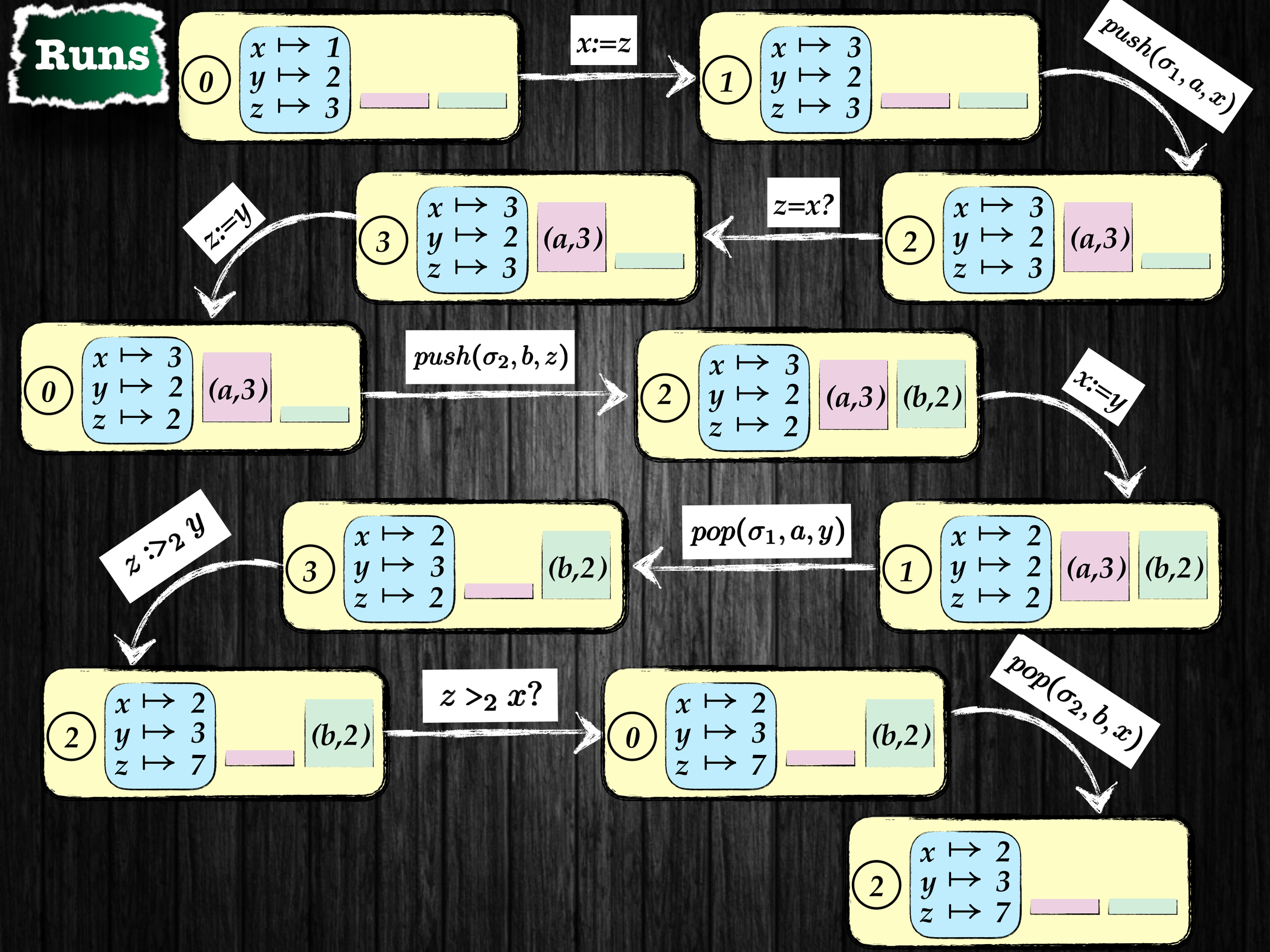

0
$x \mapsto 1$
$y \mapsto 2$
$z \mapsto 3$
$x{:=}z$
1
$x \mapsto 3$
$y \mapsto 2$
$z \mapsto 3$
$push(\sigma_1, a, x)$
2
$x \mapsto 3$
$y \mapsto 2$
$z \mapsto 3$
$(a,3)$

Runs





Runs


0
x ↦ 1
y ↦ 2
z ↦ 3
x:=z
1
x ↦ 3
y ↦ 2
z ↦ 3
push(σ1, a, x)
2
x ↦ 3
y ↦ 2
z ↦ 3
(a,3)
z=x?
3
x ↦ 3
y ↦ 2
z ↦ 3
(a,3)
z:=y
0
x ↦ 3
y ↦ 2
z ↦ 2
(a,3)
push(σ2, b, z)
2
x ↦ 3
y ↦ 2
z ↦ 2
(a,3)
(b,2)
x:=y
1
x ↦ 2
y ↦ 2
z ↦ 2
(a,3)
(b,2)
pop(σ1, a, y)
3
x ↦ 2
y ↦ 3
z ↦ 2
(b,2)
z :=2 y
2
x ↦ 2
y ↦ 3
z ↦ 7
(b,2)
z >2 x?
0
x ↦ 2
y ↦ 3
z ↦ 7
(b,2)
pop(σ2, b, x)
2
x ↦ 2
y ↦ 3
z ↦ 7

Reacha

0 $x \mapsto 1$ $y \mapsto 2$ $z \mapsto 3$

$x{:=}z$

1 $x \mapsto 3$ $y \mapsto 2$ $z \mapsto 3$

$push(\sigma_1, a, x)$

empty stack

empty stack

local state

$z{:=}y$

3 $y \mapsto 2$ $z \mapsto 3$ $(a,3)$

$z{=}x?$

2 $x \mapsto 3$ $y \mapsto 2$ $z \mapsto 3$ $(a,3)$

0 $x \mapsto 3$ $y \mapsto 2$ $z \mapsto 2$ $(a,3)$

0 $x \mapsto 1$ $y \mapsto 2$ $z \mapsto 3$

$*$

2 $x \mapsto 2$ $y \mapsto 3$ $z \mapsto 7$

local state

local state

$x{:=}y$

$z :=_2 y$

2 $(a,3)$ $(b,2)$

$z >_2 x?$

2 $x \mapsto 2$ $y \mapsto 3$ $z \mapsto 7$ $(b,2)$

0 $x \mapsto 2$ $y \mapsto 3$ $z \mapsto 7$ $(b,2)$

$pop(\sigma_2, b, x)$

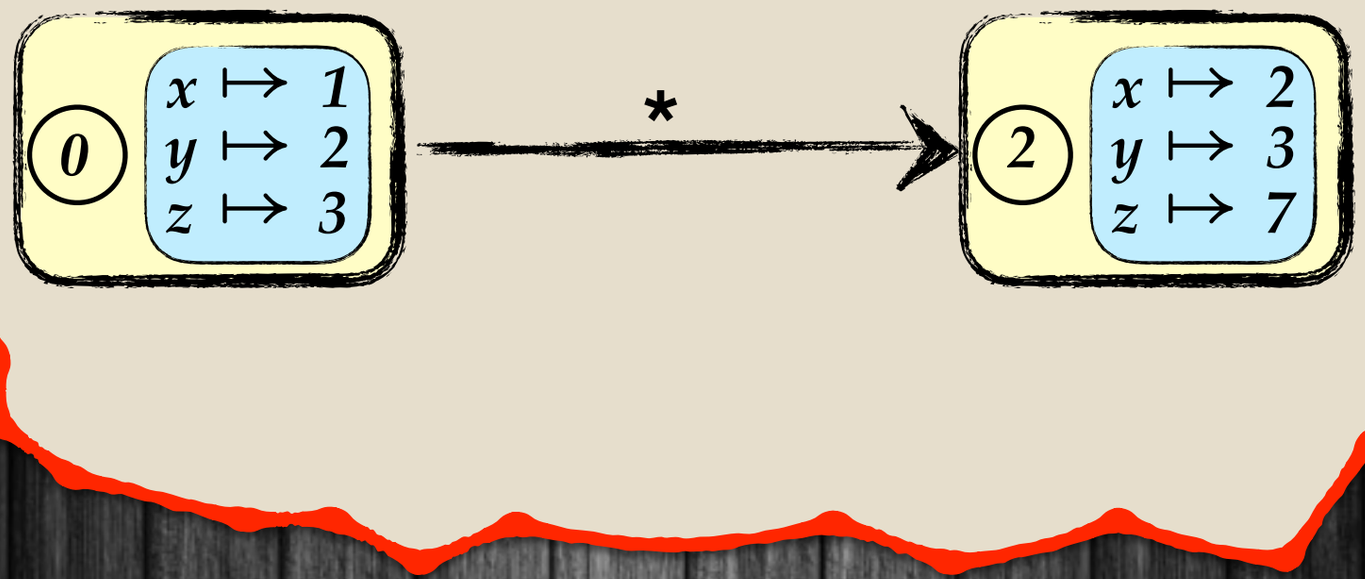
empty stack

empty stack

local state

2 $x \mapsto 2$ $y \mapsto 3$ $z \mapsto 7$

Reach. Reachability Problem



Instance: (q_s, v_s) and (q_t, v_t)

local state

local state

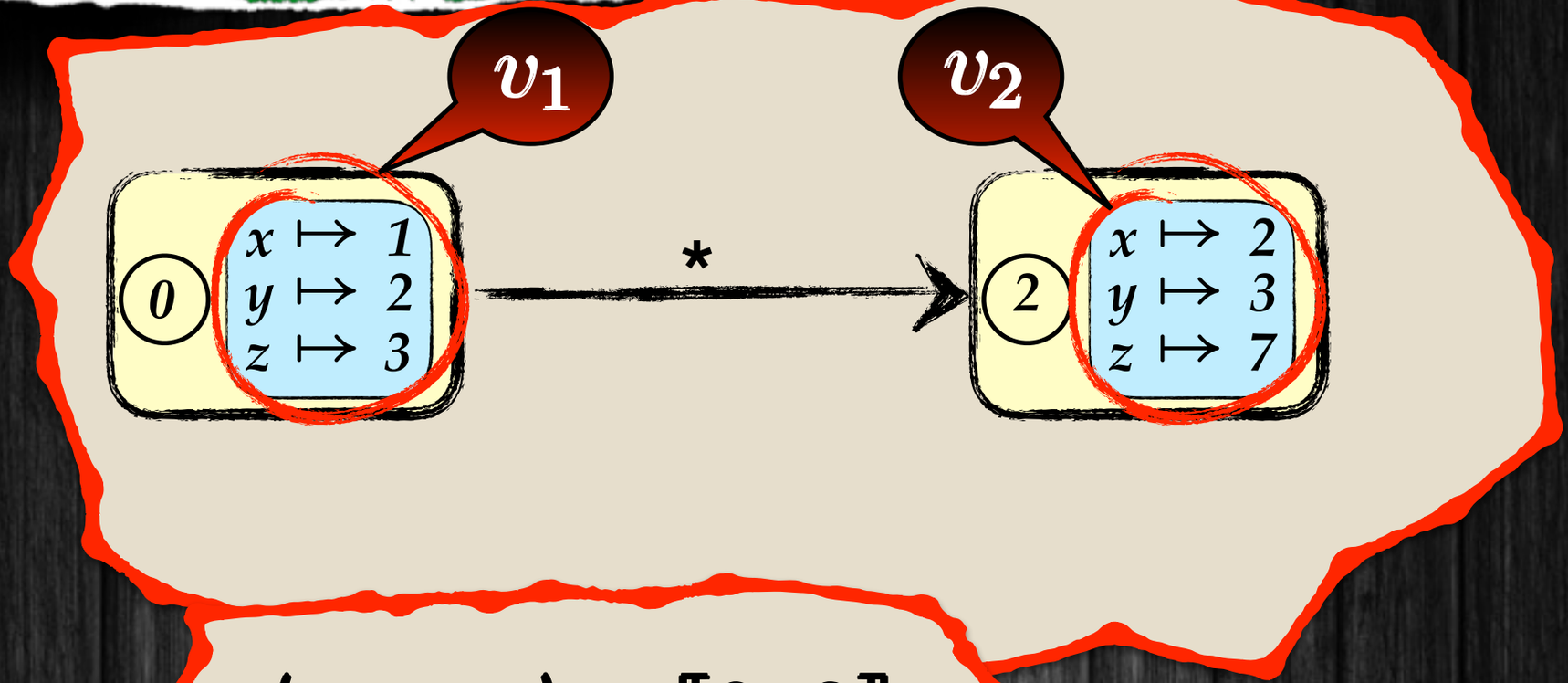
Question: $(q_s, v_s) \xrightarrow{*} (q_t, v_t)$?

Reach. Reachability Relations

$$[\![q_s, q_t]\!] =$$

$$\left\{ \langle v_s, v_t \rangle \;\middle|\; \boxed{q_s \;\; v_s} \xrightarrow{\;*\;} \boxed{q_t \;\; v_t} \right\}$$

Reach. Reachability Relations



$$\langle v_1, v_2 \rangle \in [\![0, 2]\!]$$

$[\![q_s, q_t]\!] =$

$$\left\{ \langle v_s, v_t \rangle \;\middle|\; \boxed{q_s \;\; v_s} \xrightarrow{\;*\;} \boxed{q_t \;\; v_t} \right\}$$

Outline

- Background
- Model
- Gap-Order Constraints
- Signatures
- Reachability Algorithm
- Applications

- Syntax
- Saturation
- Quantifier elimination
- Entailment

Gap-Order Constraints

finite set of variables

x, y, z, u

conjunction of constraints

ϕ

equality

gap

$x = y$

$y <_2 z$

$z <_3 u$

$x <_2 u$

$v_1 : \{ x \mapsto 2,\ y \mapsto 2,\ z \mapsto 6,\ u \mapsto 10 \}$

$v_1 \in [\![\phi]\!]$

$v_2 : \{ x \mapsto 1,\ y \mapsto 2,\ z \mapsto 6,\ u \mapsto 10 \}$

$v_2 \notin [\![\phi]\!]$

$v_3 : \{ x \mapsto 2,\ y \mapsto 2,\ z \mapsto 3,\ u \mapsto 10 \}$

$v_3 \notin [\![\phi]\!]$

Gap-Order Constraints Saturation

$x = y$
$y <_2 z$
$z <_3 u$
~~$x <_? u$~~

+

$x <_2 z$
$y <_6 u$
$x <_6 u$

→

$x = y$
$y <_2 z$
$z <_3 u$
$x <_2 z$
$y <_6 u$
$x <_6 u$

saturated

Gap-Order Quantifier Elimination

$\exists y.$

$x = y$

$y <_2 z$

$z <_3 u$

$x <_2 z$

$y <_6 u$

$x <_6 u$

saturated

Gap-Order Quantifier Elimination

$$\exists y.\ \{\ x \neq y,\ y <_2 z,\ z <_3 u,\ x <_2 z,\ y <_6 u,\ x <_6 u\ \} = \{\ z <_3 u,\ x <_2 z,\ x <_6 u\ \}$$

saturated

Gap-Order Constraints Entailment

ϕ_1

$x = y$

$z <_3 u$

$x = y$

$y <_5 z$

$z <_4 u$

$x <_2 z$

$y <_6 u$

$x <_6 u$

ϕ_2

Gap-Order Constraints Entailment

ϕ_1

$x = y$
$z <_3 u$

ϕ_2

$x = y$
$y <_5 z$
$z <_4 u$
$x <_2 z$
$y <_6 u$
$x <_6 u$

$\phi_1 \sqsubseteq \phi_2$

Gap-Order Constraints Entailment

ϕ_1

$x = y$

$z <_3 u$

$x = y$

$y <_5 z$

$z <_4 u$

$x <_2 z$

$y <_6 u$

$x <_6 u$

ϕ_2

$\phi_1 \sqsubseteq \phi_2$ → $[\![\phi_2]\!] \subseteq [\![\phi_1]\!]$

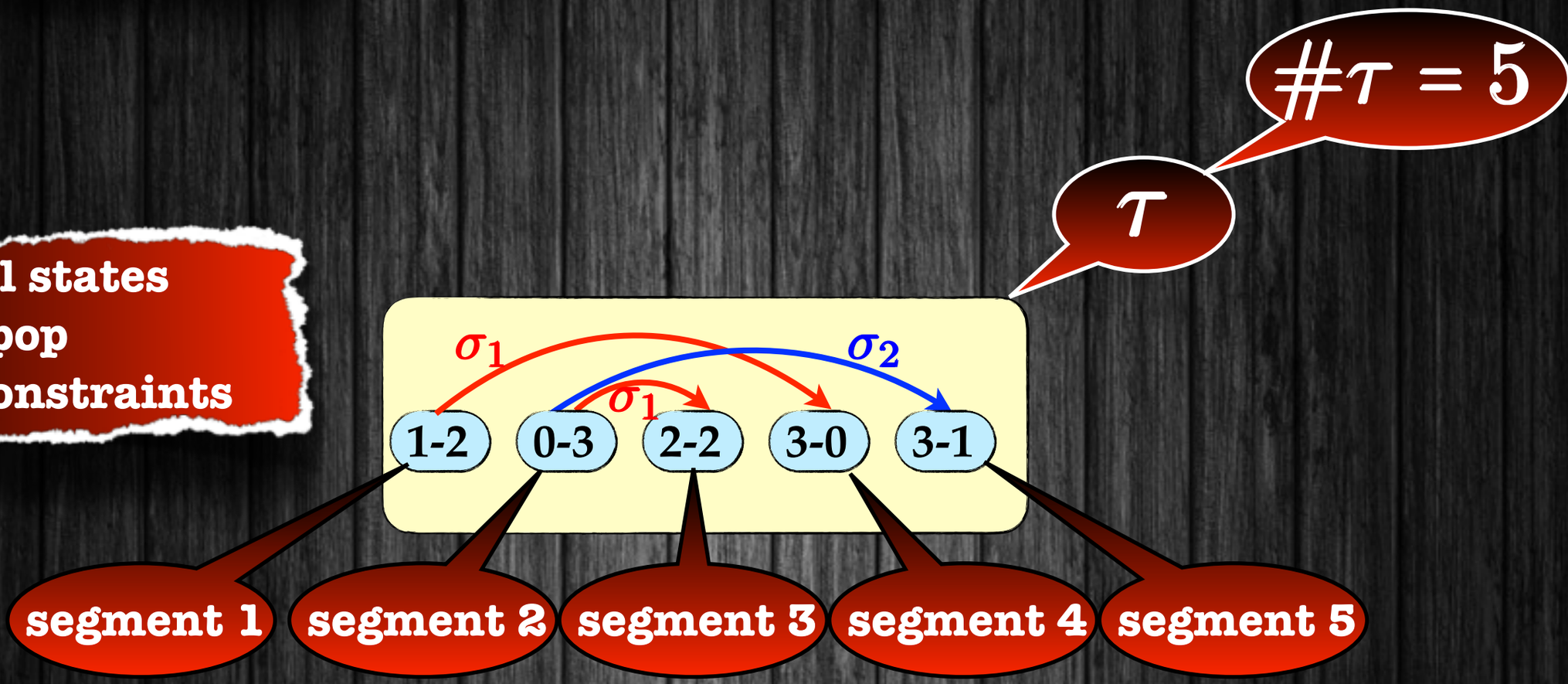
Outline

- Background
- Model
- Gap-Order Constraints
- Signatures
- Reachability Algorithm
- Applications

- Syntax
- Entailment
- Atomic signatures
  - Internal transitions
  - Stack transitions
- Composition
  - Shuffling
  - Contraction
- Monotonicity

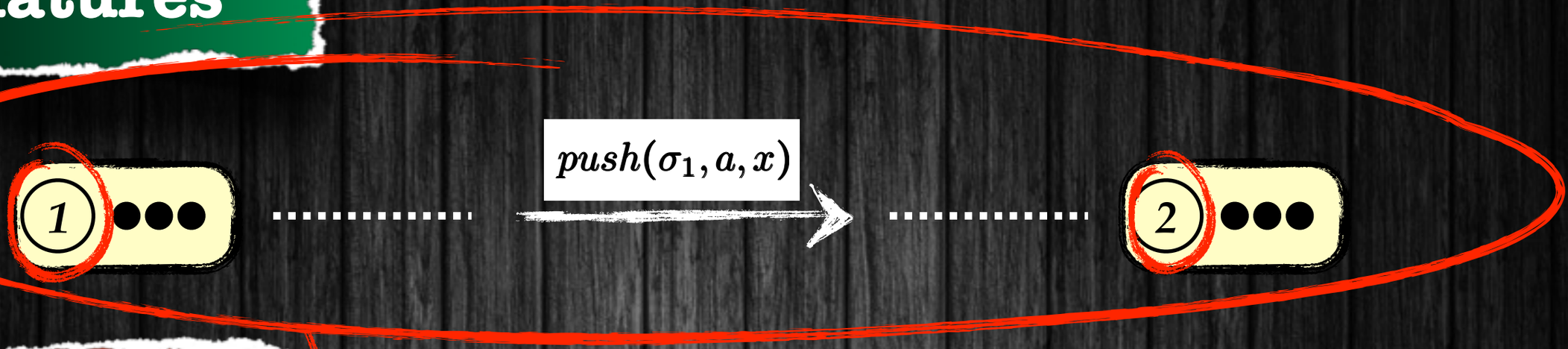
Signatures

- control states
- push/pop
- data constraints

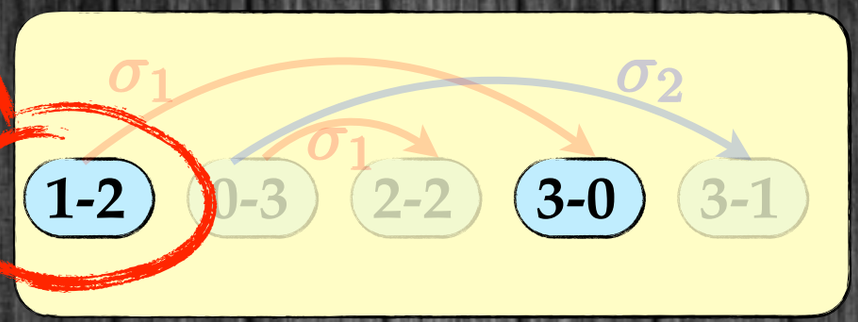


- segment: “part of run”
- signature: parts of runs with "holes" in between

Signatures

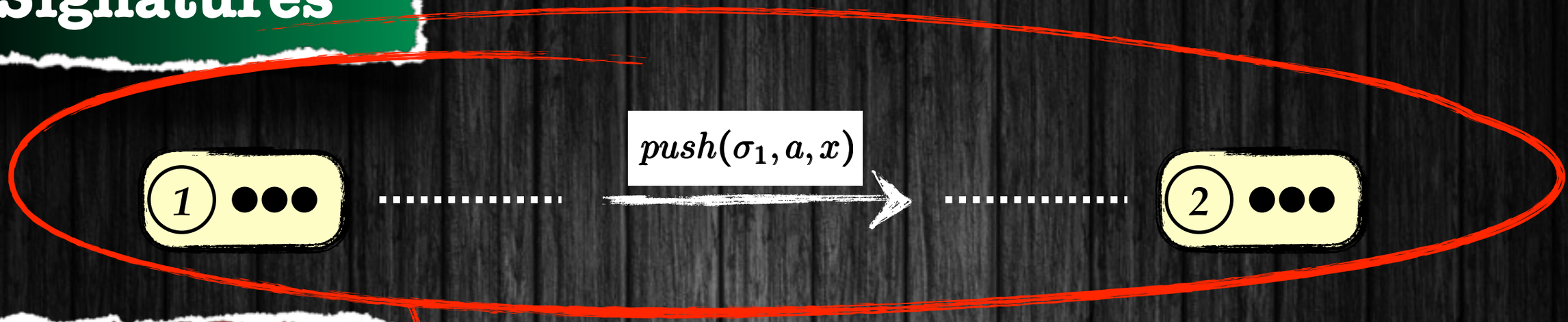


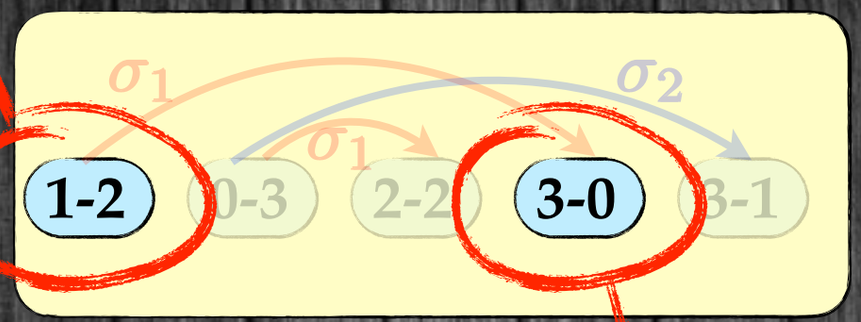
- control states ✓
- push/pop
- data constraints

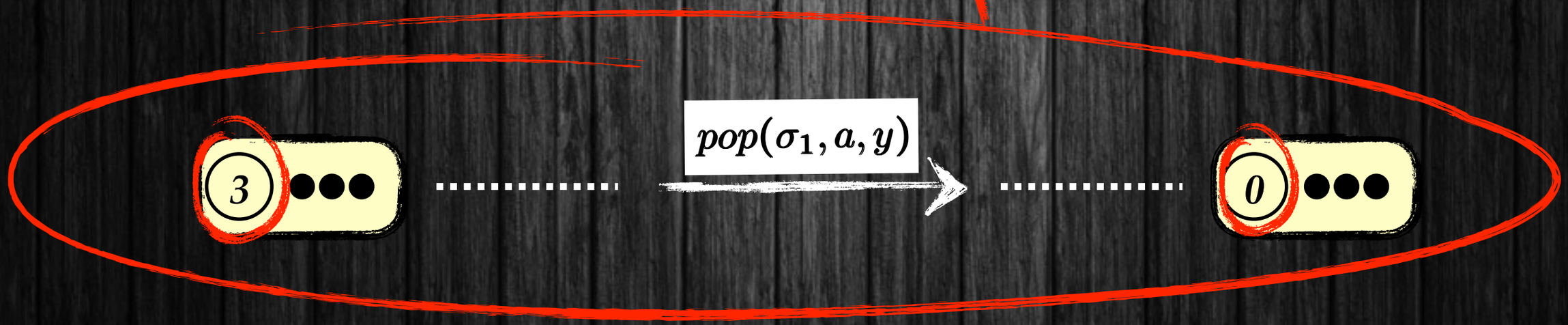


Signatures

- control states ✓
- push/pop
- data constraints

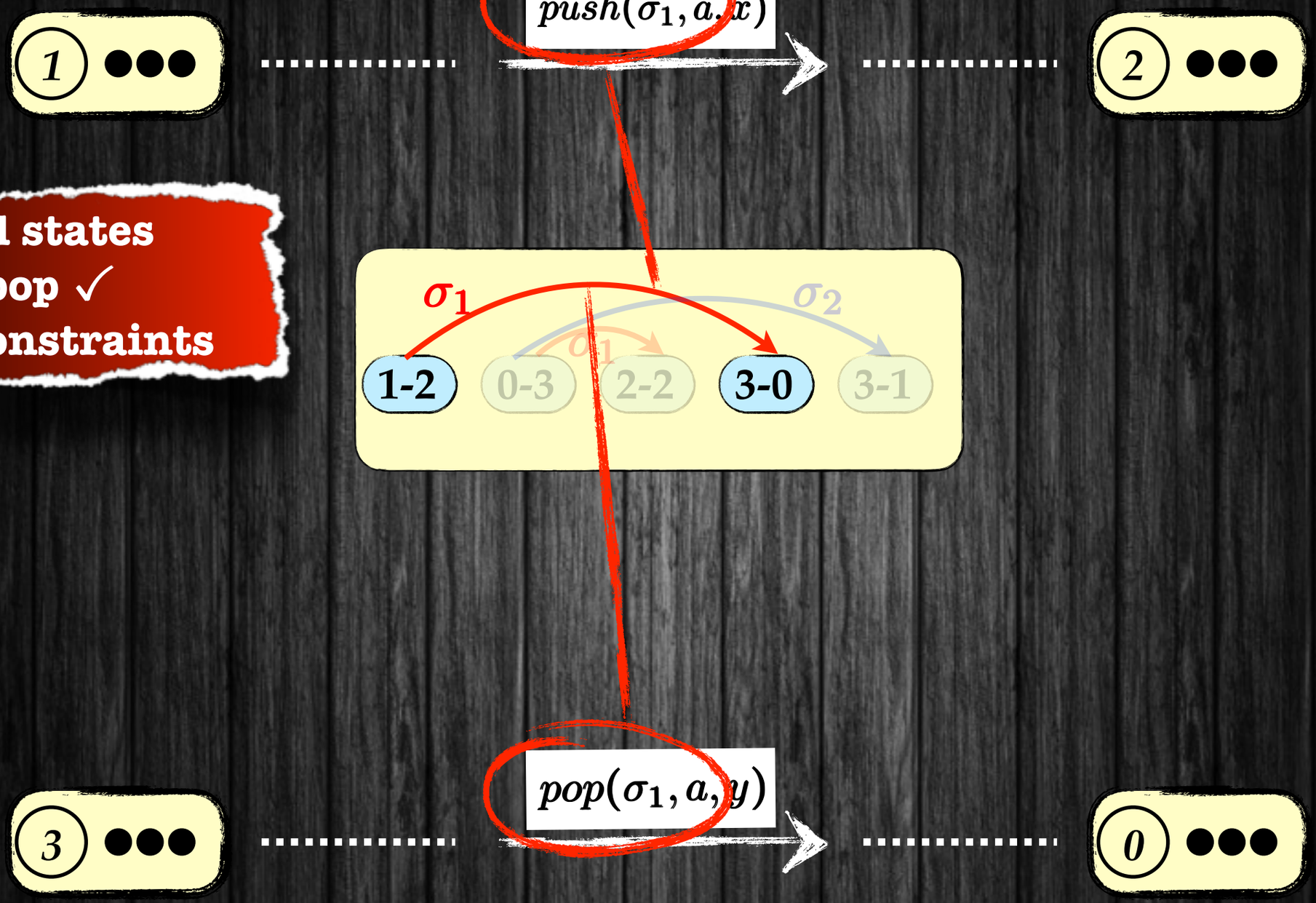






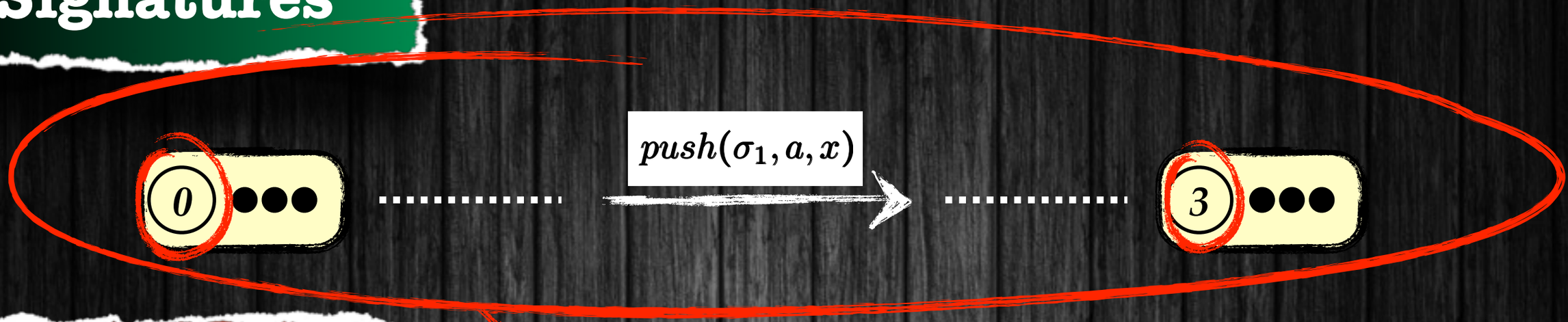
Signatures

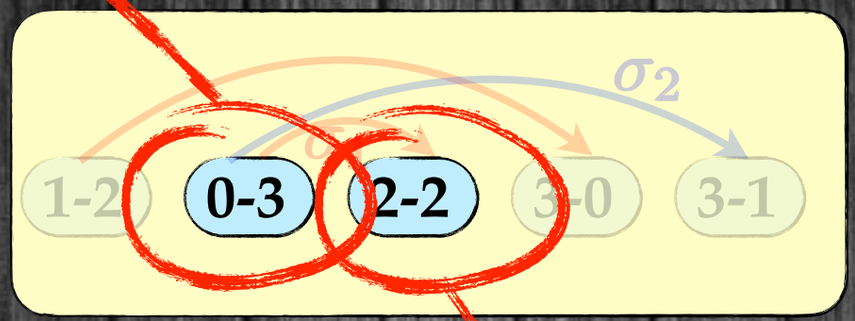
- control states
- push/pop ✓
- data constraints

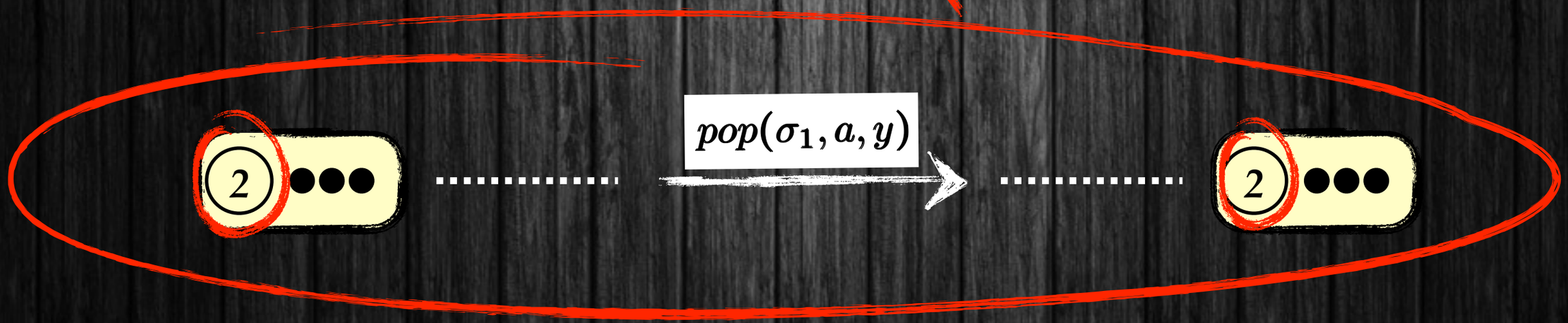


Signatures

- control states ✓
- push/pop
- data constraints

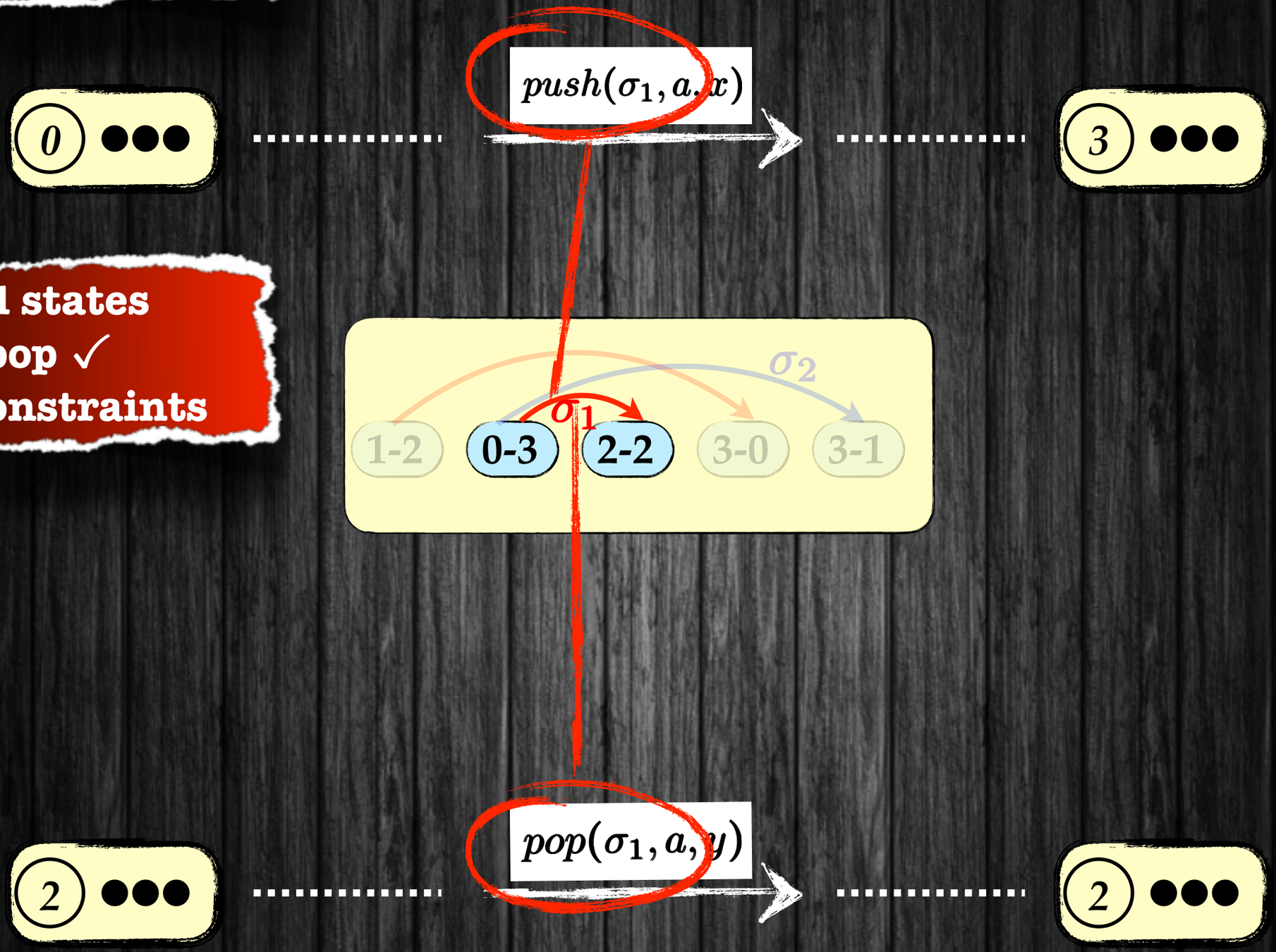






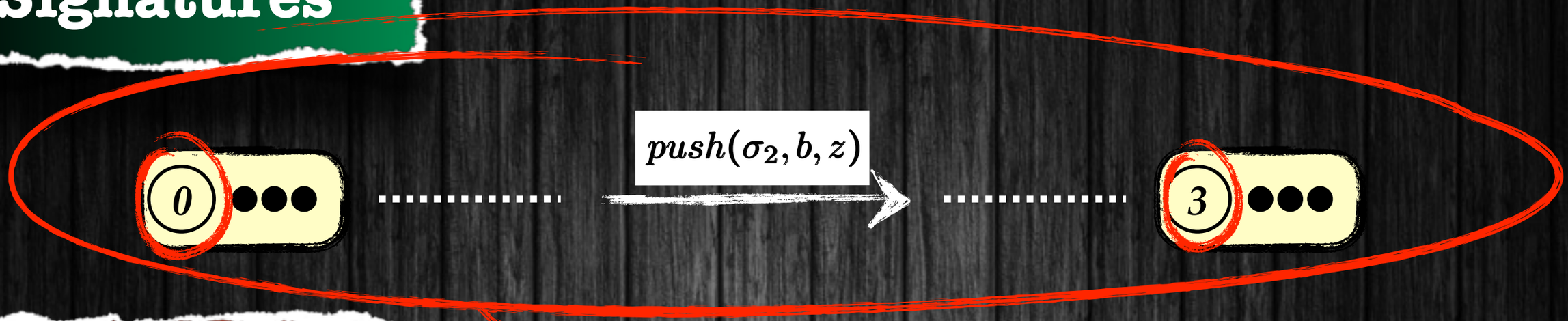
Signatures

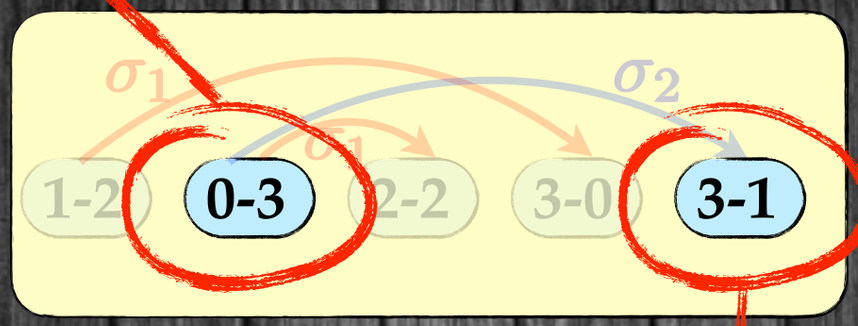
- control states
- push/pop ✓
- data constraints

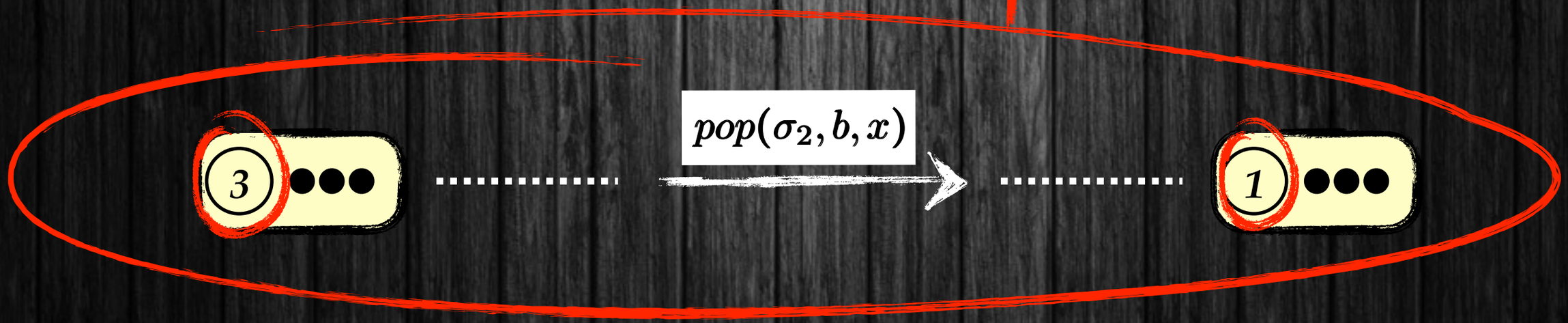


Signatures

- control states ✓
- push/pop
- data constraints

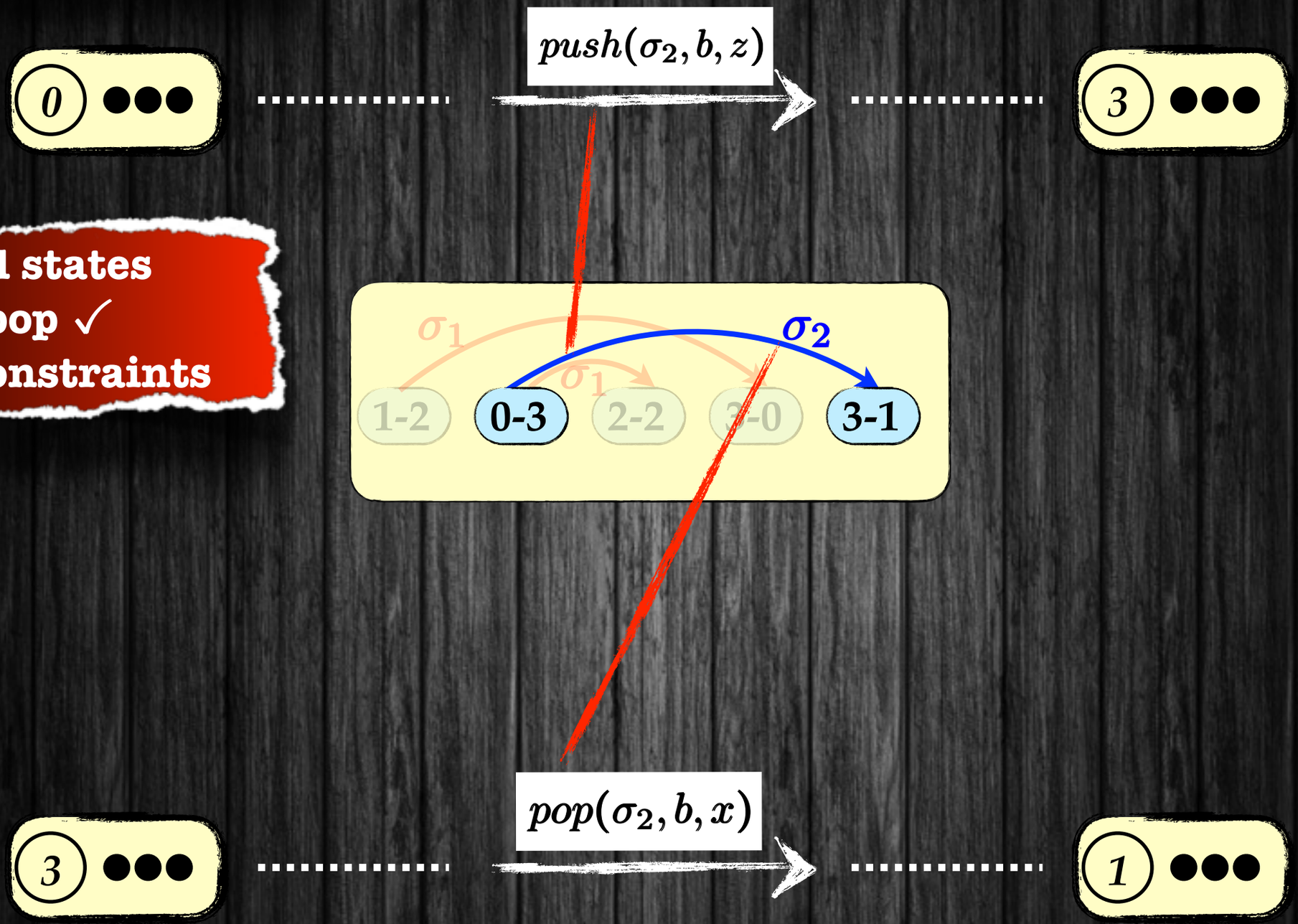






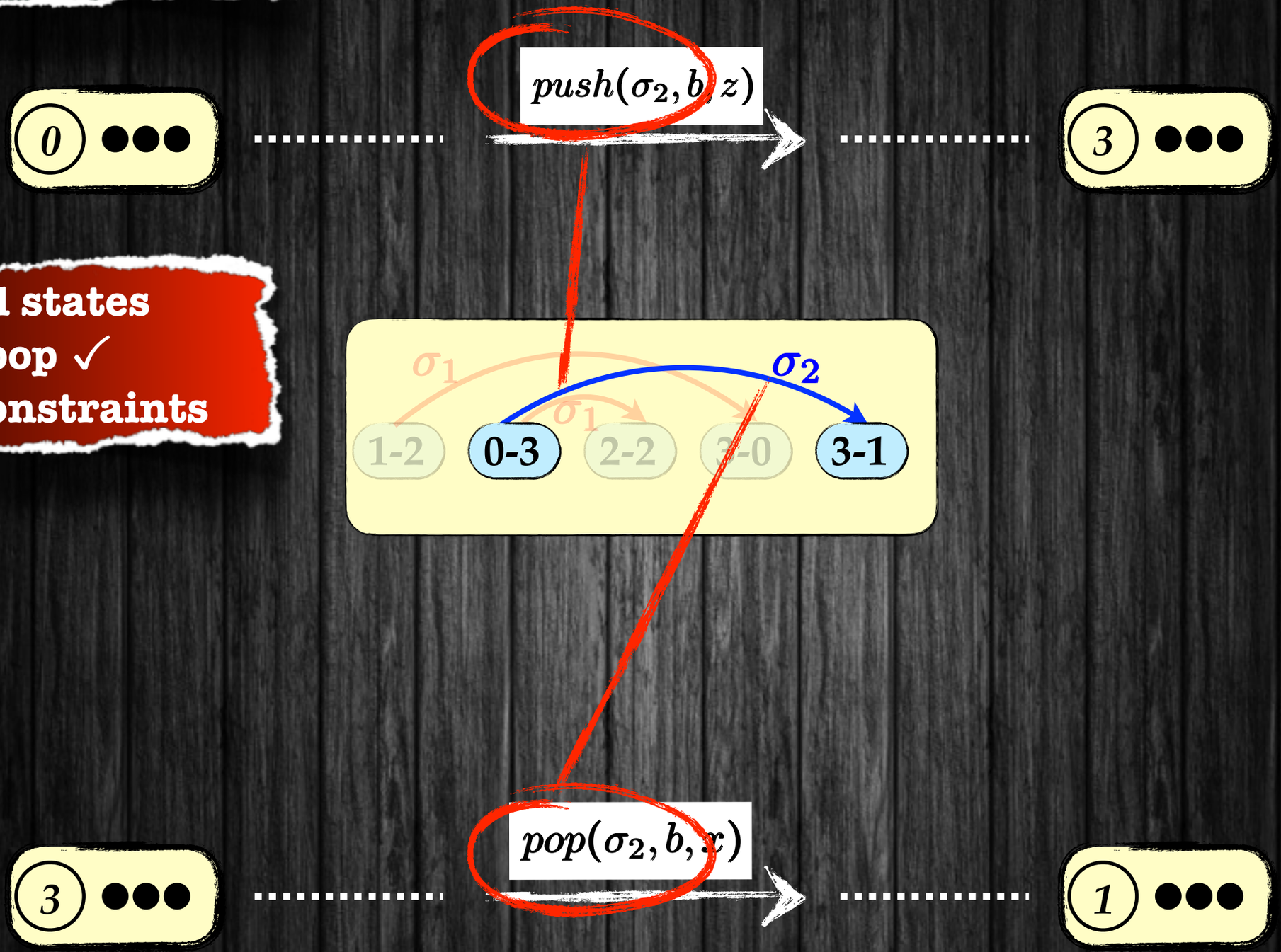
Signatures

- control states
- push/pop ✓
- data constraints

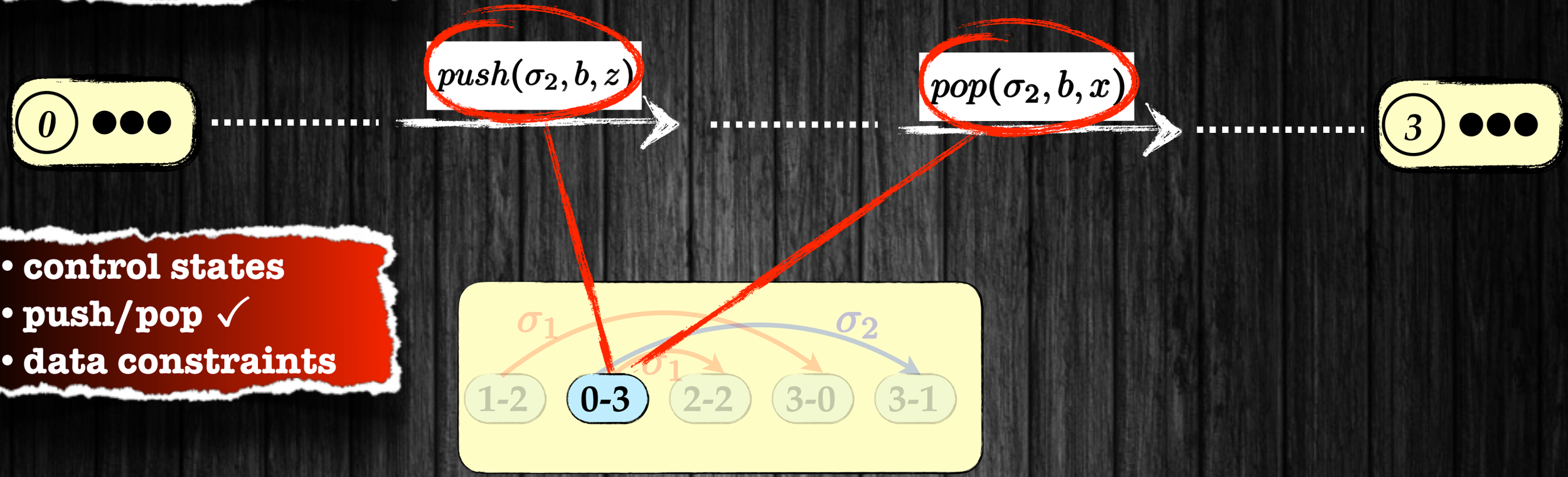


Signatures

- control states
- push/pop ✓
- data constraints



Signatures



- control states
- push/pop ✓
- data constraints

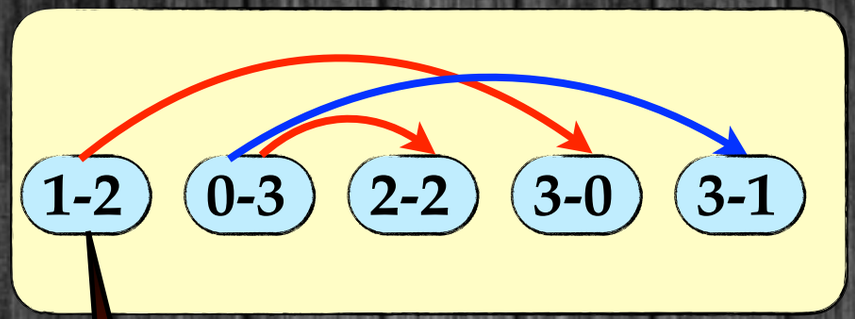
“push/pop operations within same segment not shown”

Signatures

finite set of variables

x, y, z

- control states
- push/pop
- data constraints ✓



segment 1

value of x at the start of segment 1

value of x at the end of segment 1

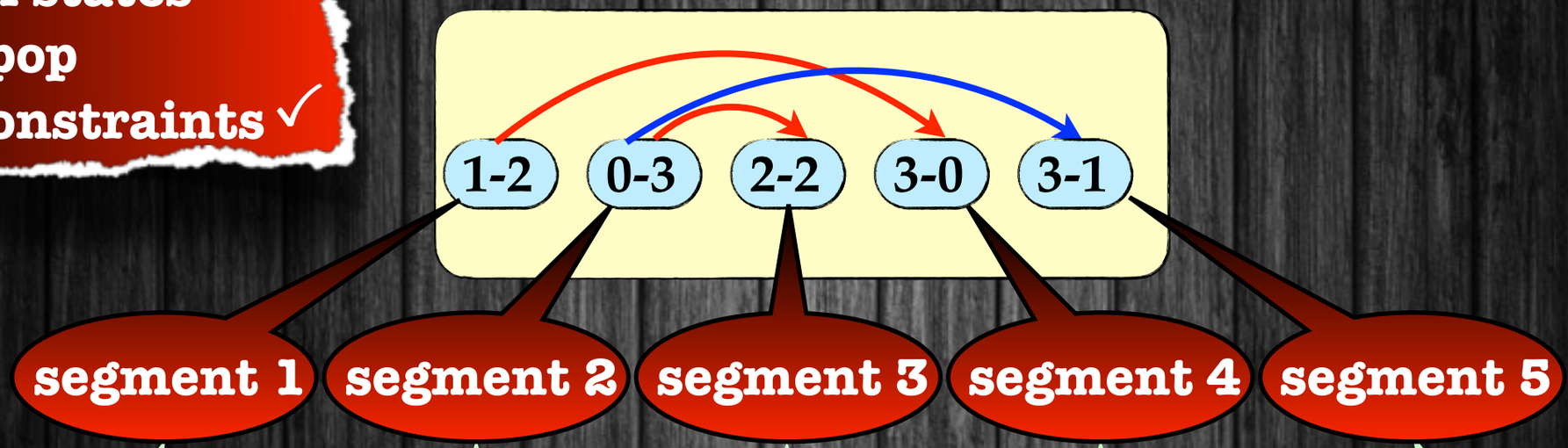
$x^1_s, x^1_t,$
$y^1_s, y^1_t,$
z^1_s, z^1_t

Signatures

finite set of variables

x, y, z

- control states
- push/pop
- data constraints ✓



$x^1_s, x^1_t, y^1_s, y^1_t, z^1_s, z^1_t$

$x^2_s, x^2_t, y^2_s, y^2_t, z^2_s, z^2_t$

$x^3_s, x^3_t, y^3_s, y^3_t, z^3_s, z^3_t$

$x^4_s, x^4_t, y^4_s, y^4_t, z^4_s, z^4_t$

$x^5_s, x^5_t, y^5_s, y^5_t, z^5_s, z^5_t$

Signatures

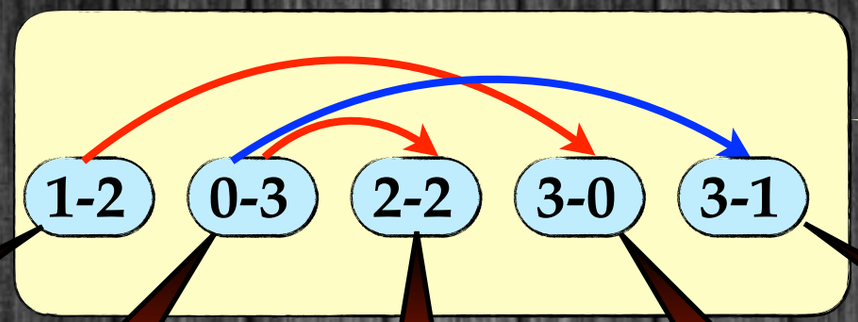
finite set of variables

x, y, z

- control states
- push/pop
- data constraints ✓

gap-order constraint

$$x_t^1 <_3 y_s^2$$
$$z_t^3 = x_s^4$$
$$y_t^5 <_4 z_s^2$$
$$y_t^2 <_2 x_s^1$$
$$x_t^1 = y_s^4$$
$$z_t^2 <_2 x_s^5$$



segment 1 | segment 2 | segment 3 | segment 4 | segment 5

$x_s^1, x_t^1, y_s^1, y_t^1, z_s^1, z_t^1$

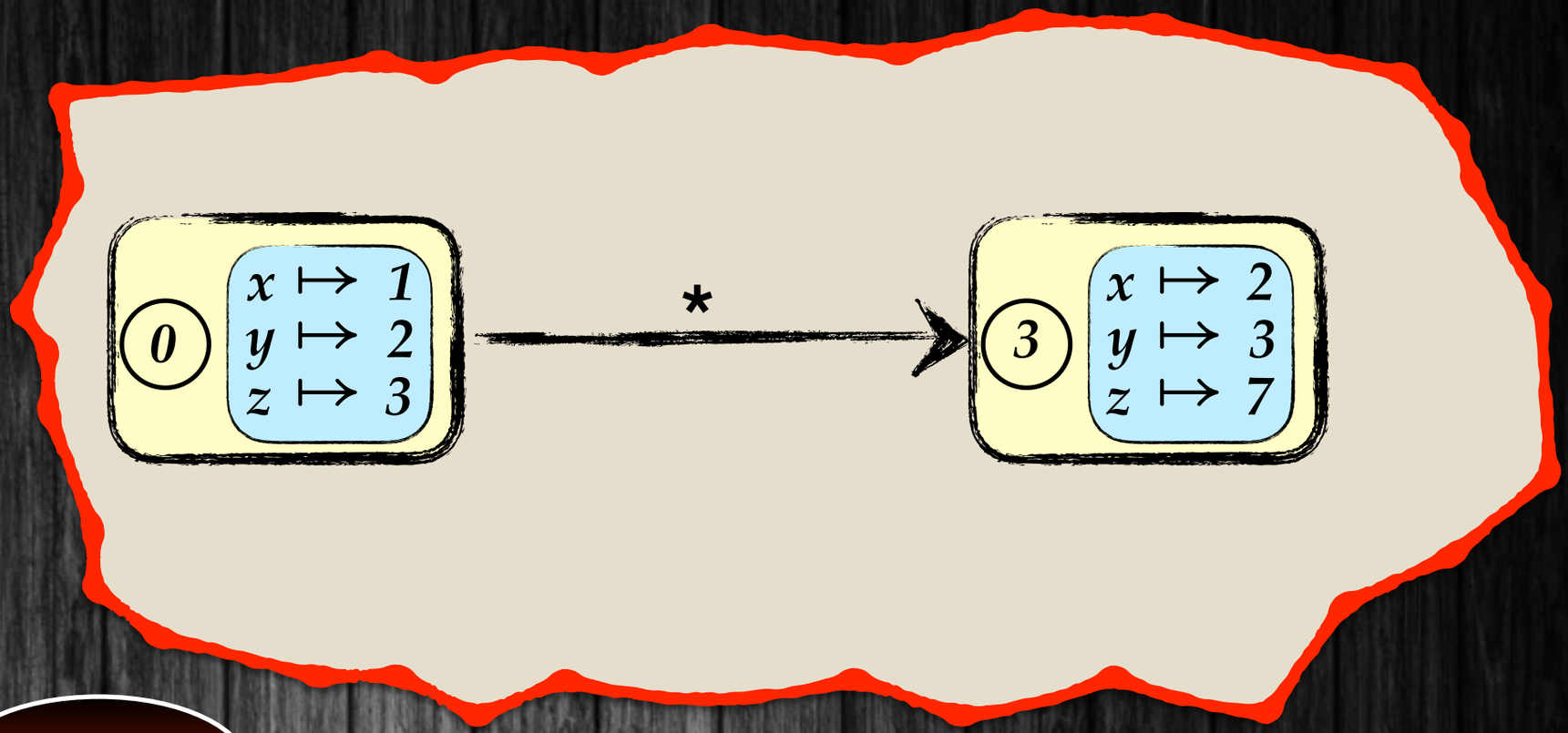
$x_s^2, x_t^2, y_s^2, y_t^2, z_s^2, z_t^2$

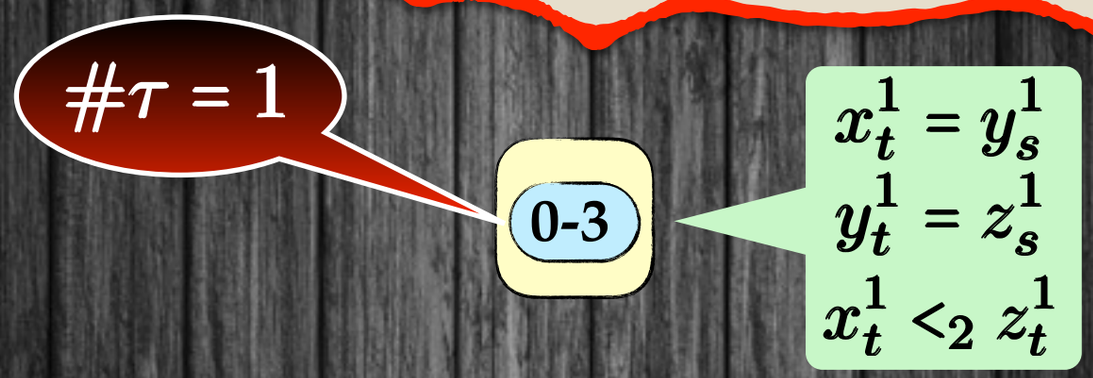
$x_s^3, x_t^3, y_s^3, y_t^3, z_s^3, z_t^3$

$x_s^4, x_t^4, y_s^4, y_t^4, z_s^4, z_t^4$

‘the gap between the value of x at the start of segment 5 and the value of z at the end of segment 2 is more than 2”

Signatures



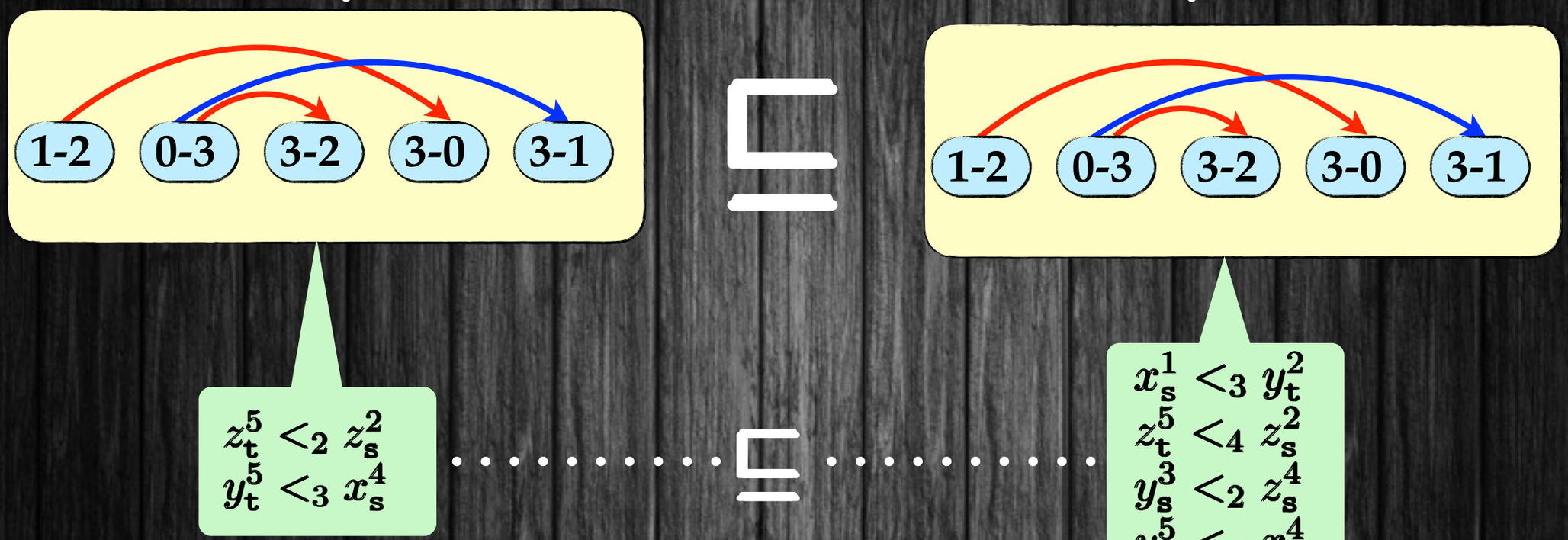


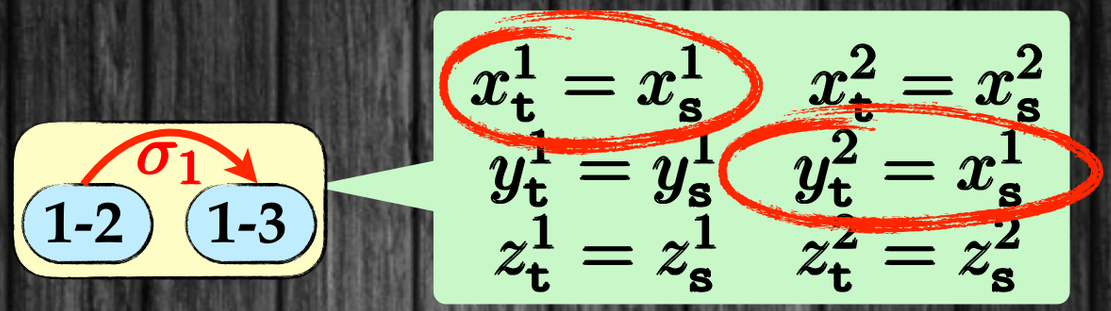
“push/pop operations within same segment not shown”

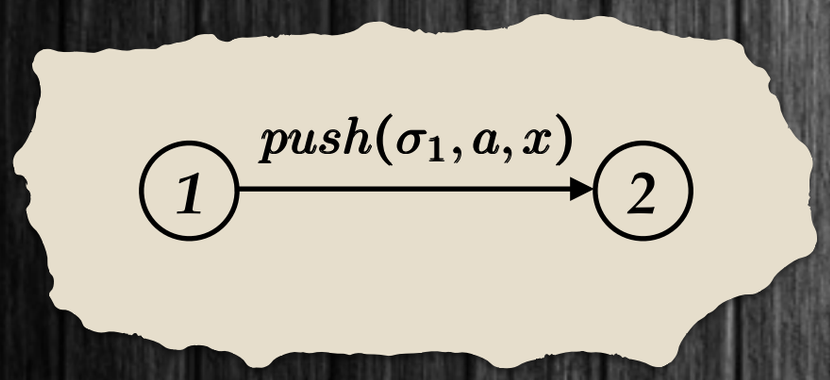
“single-node signatures characterize full runs”

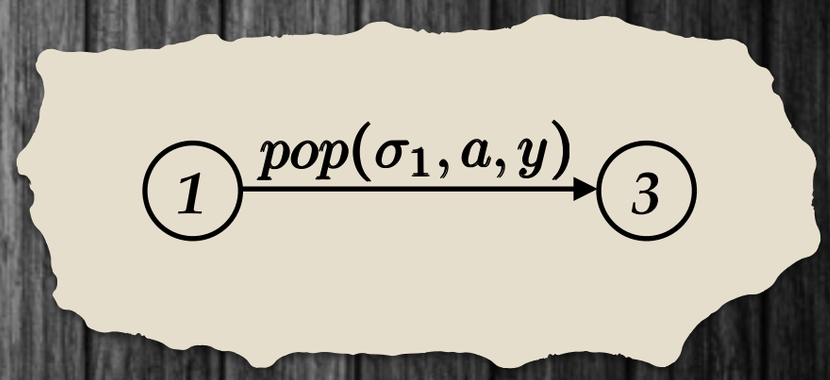
“single-node signatures characterise reachability relations”

Signatures Entailment



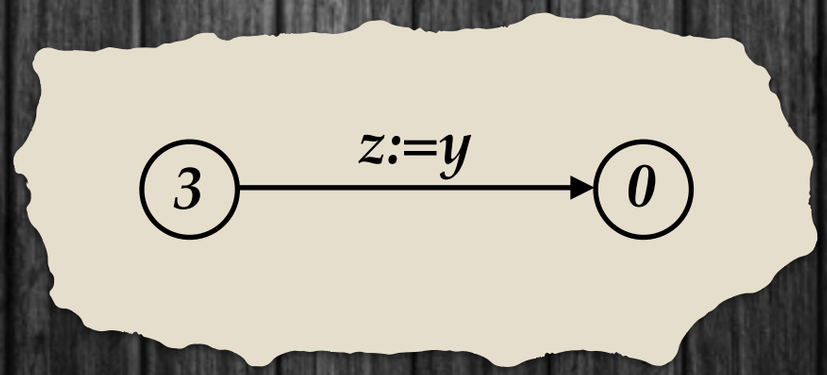

σ_1
1-2
1-3
$x_t^1 = x_s^1$
$x_t^2 = x_s^2$
$y_t^1 = y_s^1$
$y_t^2 = x_s^1$
$z_t^1 = z_s^1$
$z_t^2 = z_s^2$

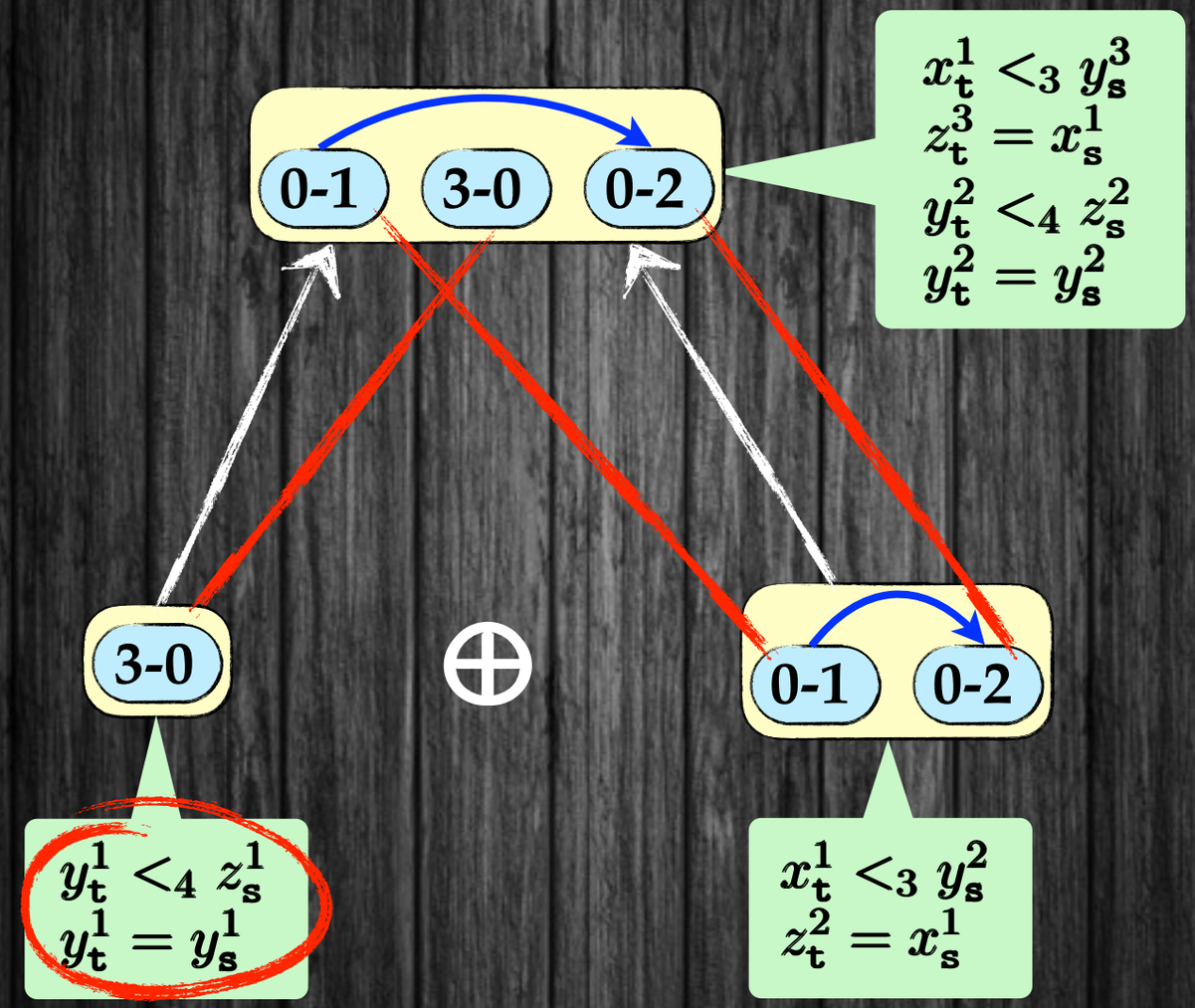

$push(\sigma_1, a, x)$
1
2


$pop(\sigma_1, a, y)$
1
3

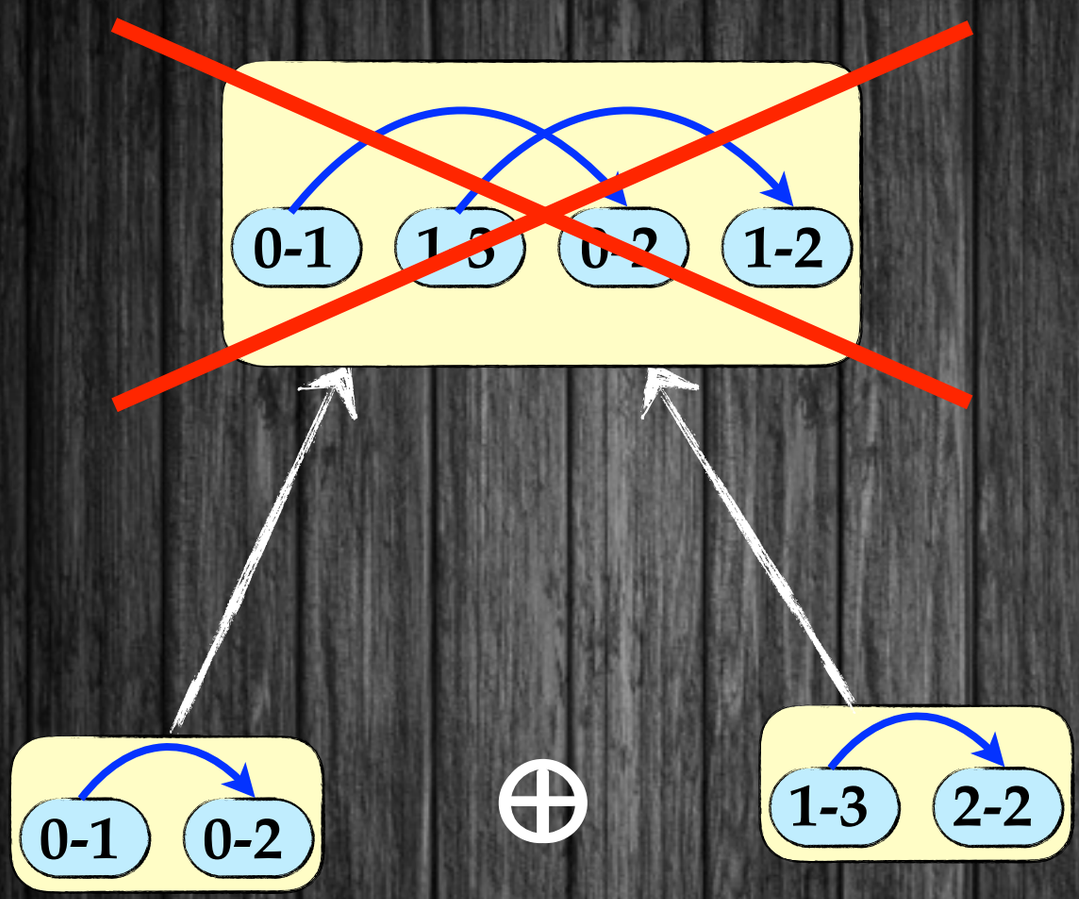
3-0

$$x_{\mathbf{t}}^1 = x_{\mathbf{s}}^1$$
$$y_{\mathbf{t}}^1 = y_{\mathbf{s}}^1$$
$$z_{\mathbf{t}}^1 = y_{\mathbf{s}}^1$$



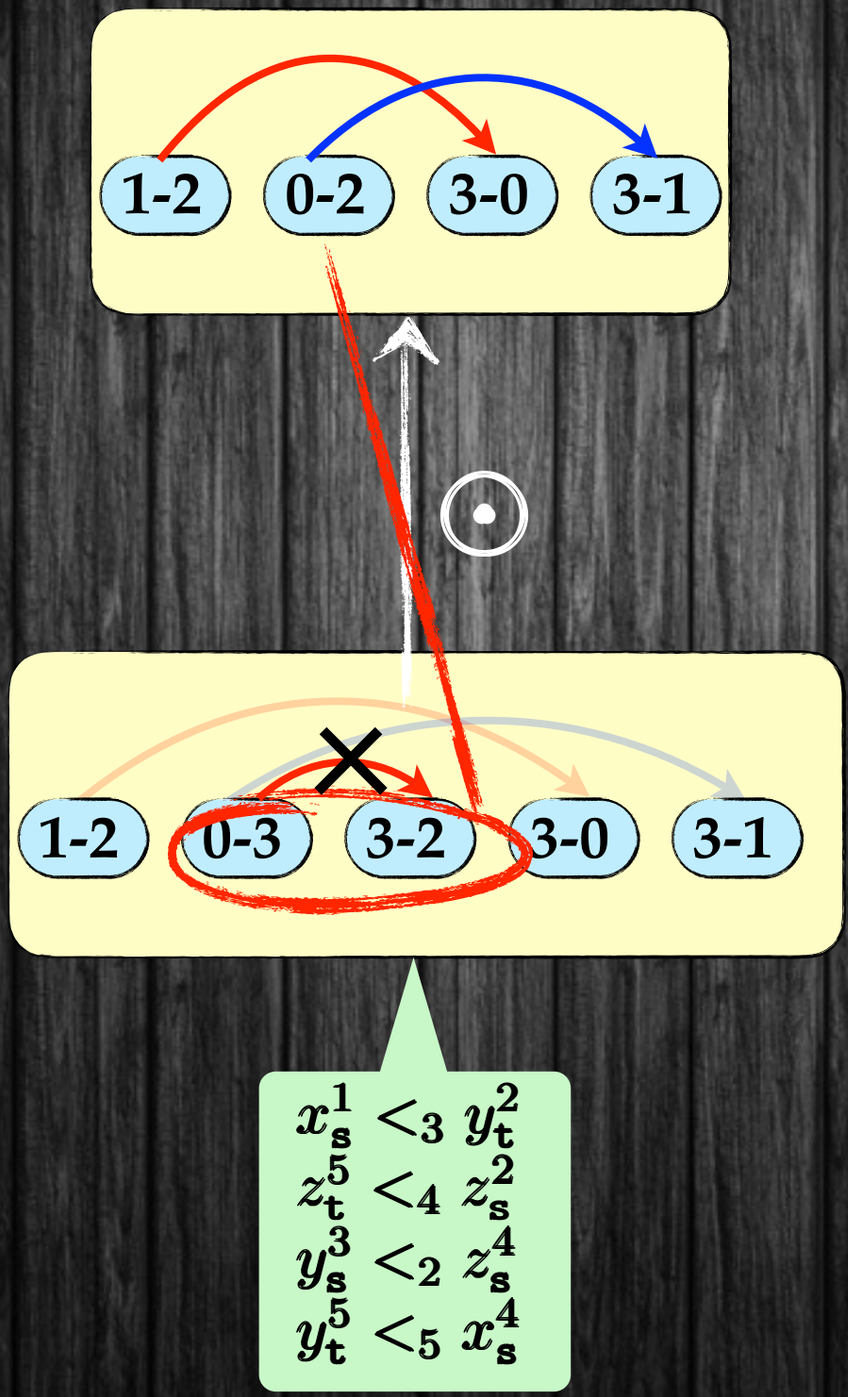

0-1
3-0
0-2
$x_t^1 <_3 y_s^3$
$z_t^3 = x_s^1$
$y_t^2 <_4 z_s^2$
$y_t^2 = y_s^2$
3-0
$y_t^1 <_4 z_s^1$
$y_t^1 = y_s^1$
⊕
0-1
0-2
$x_t^1 <_3 y_s^2$
$z_t^2 = x_s^1$

Signatures | Combining Signatu | Shuffling



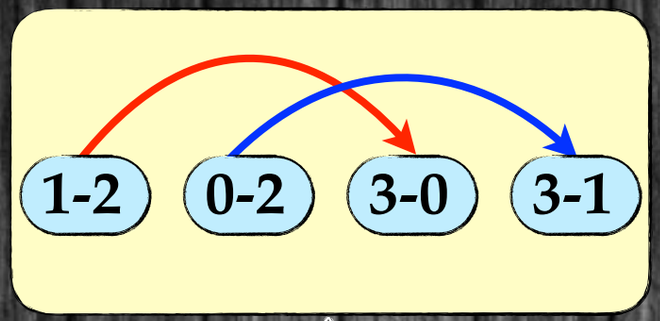
Signatures | Combining Signatu | Contraction

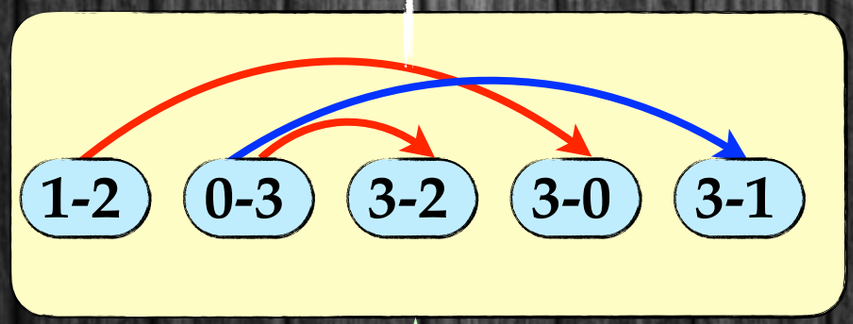
- control states
- push/pop ✓
- data constraints



Signatures | Combining Signatu | Contraction

- control states
- push/pop
- data constraints ✓



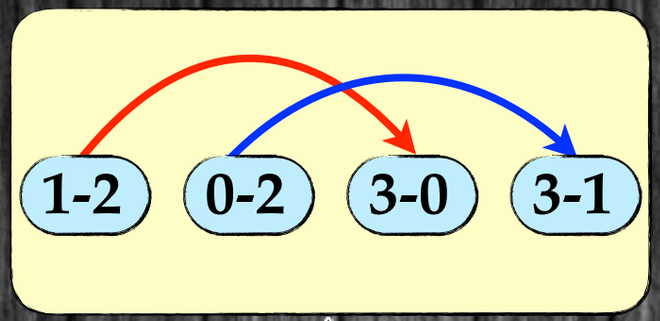


1. equating variables
2. saturation
3. variable elimination
4. renaming

$$
\begin{aligned}
x^1_{\mathbf{s}} &<_3 y^2_{\mathbf{t}} \\
z^5_{\mathbf{t}} &<_4 z^2_{\mathbf{s}} \\
y^3_{\mathbf{s}} &<_2 z^4_{\mathbf{s}} \\
y^5_{\mathbf{t}} &<_5 x^4_{\mathbf{s}}
\end{aligned}
$$

Signatures | Combining Signatu | Contraction

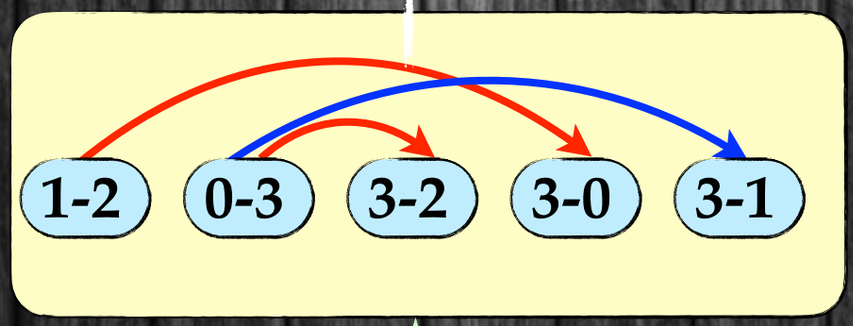
- control states
- push/pop
- data constraints ✓



$$x^1_{\mathbf{s}} <_3 y^2_{\mathbf{t}} \quad z^5_{\mathbf{t}} <_4 z^2_{\mathbf{s}} \quad y^3_{\mathbf{s}} <_2 z^4_{\mathbf{s}} \quad y^5_{\mathbf{t}} <_5 x^4_{\mathbf{s}}$$

+

$$x^3_{\mathbf{s}} = x^2_{\mathbf{t}} \quad y^3_{\mathbf{s}} = y^2_{\mathbf{t}} \quad z^3_{\mathbf{s}} = z^2_{\mathbf{t}}$$

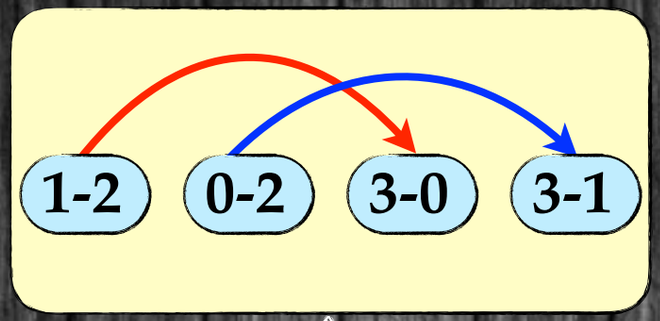


$$x^1_{\mathbf{s}} <_3 y^2_{\mathbf{t}} \quad z^5_{\mathbf{t}} <_4 z^2_{\mathbf{s}} \quad y^3_{\mathbf{s}} <_2 z^4_{\mathbf{s}} \quad y^5_{\mathbf{t}} <_5 x^4_{\mathbf{s}}$$

1. equating variables ✓
2. saturation
3. variable elimination
4. renaming

Signatures | Combining Signatu | Contraction

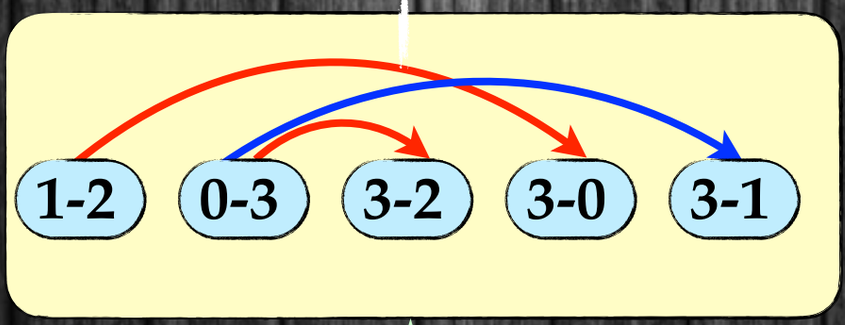
- control states
- push/pop
- data constraints ✓



$$\exists\ x^2_{\mathbf{t}}\ y^2_{\mathbf{t}}\ z^2_{\mathbf{t}}\ x^3_{\mathbf{s}}\ y^3_{\mathbf{s}}\ z^3_{\mathbf{s}}.$$

$$\begin{array}{l} x^1_{\mathbf{s}} <_3 y^2_{\mathbf{t}} \\ z^5_{\mathbf{t}} <_4 z^2_{\mathbf{s}} \\ y^3_{\mathbf{s}} <_2 z^4_{\mathbf{s}} \\ y^5_{\mathbf{t}} <_5 x^4_{\mathbf{s}} \end{array} + \begin{array}{l} x^3_{\mathbf{s}} = x^2_{\mathbf{t}} \\ y^3_{\mathbf{s}} = y^2_{\mathbf{t}} \\ z^3_{\mathbf{s}} = z^2_{\mathbf{t}} \end{array}$$

$$\begin{array}{l} x^1_{\mathbf{s}} <_3 y^3_{\mathbf{s}} \\ y^2_{\mathbf{t}} <_2 z^4_{\mathbf{s}} \\ x^1_{\mathbf{s}} <_6 z^4_{\mathbf{s}} \end{array}$$

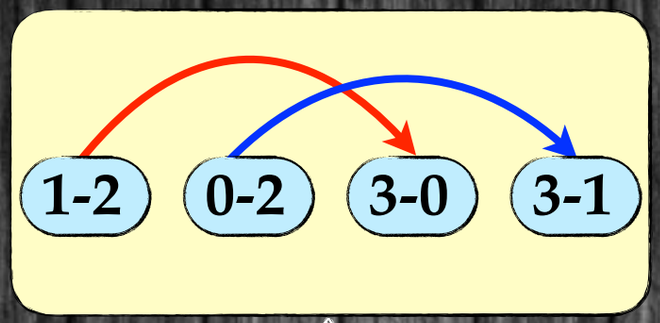


$$\begin{array}{l} x^1_{\mathbf{s}} <_3 y^2_{\mathbf{t}} \\ z^5_{\mathbf{t}} <_4 z^2_{\mathbf{s}} \\ y^3_{\mathbf{s}} <_2 z^4_{\mathbf{s}} \\ y^5_{\mathbf{t}} <_5 x^4_{\mathbf{s}} \end{array}$$

1. equating variables
2. saturation
3. variable elimination ✓
4. renaming

Signatures | Combining Signatu | Contraction

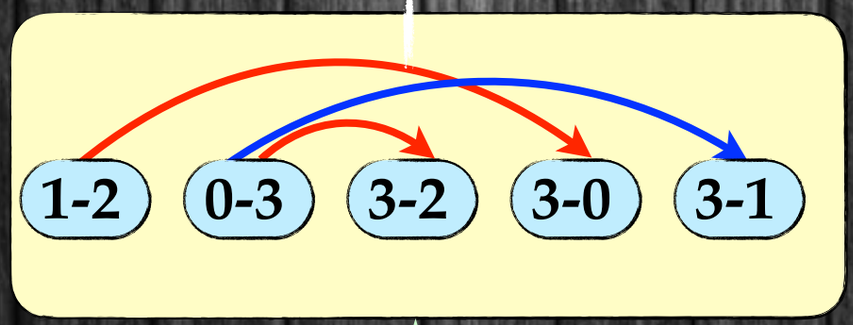
- control states
- push/pop
- data constraints ✓



$$z_{\mathbf{t}}^{5} <_4 z_{\mathbf{s}}^{2}$$

$$y_{\mathbf{t}}^{5} <_5 x_{\mathbf{s}}^{4}$$

$$x_{\mathbf{s}}^{1} <_6 z_{\mathbf{s}}^{4}$$

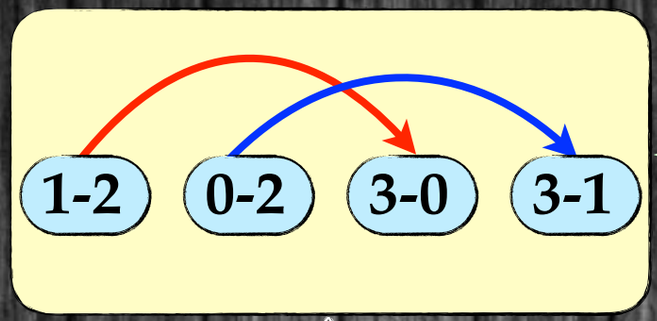


$$x_{\mathbf{s}}^{1} <_3 y_{\mathbf{t}}^{2}$$
$$z_{\mathbf{t}}^{5} <_4 z_{\mathbf{s}}^{2}$$
$$y_{\mathbf{s}}^{3} <_2 z_{\mathbf{s}}^{4}$$
$$y_{\mathbf{t}}^{5} <_5 x_{\mathbf{s}}^{4}$$

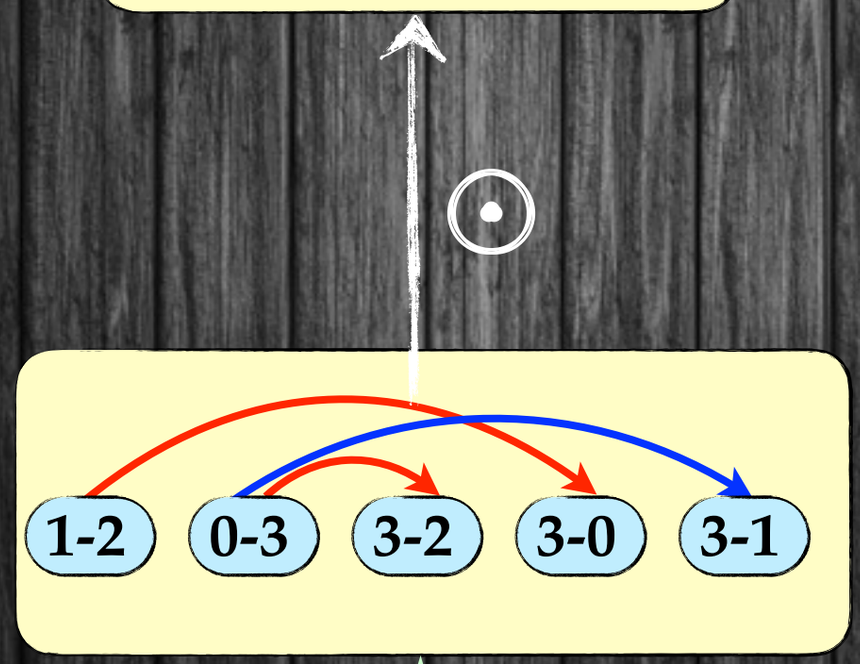
1. equating variables
2. saturation
3. variable elimination
4. renaming ✓

Signatures | Combining Signatu | Contraction

- control states
- push/pop
- data constraints ✓

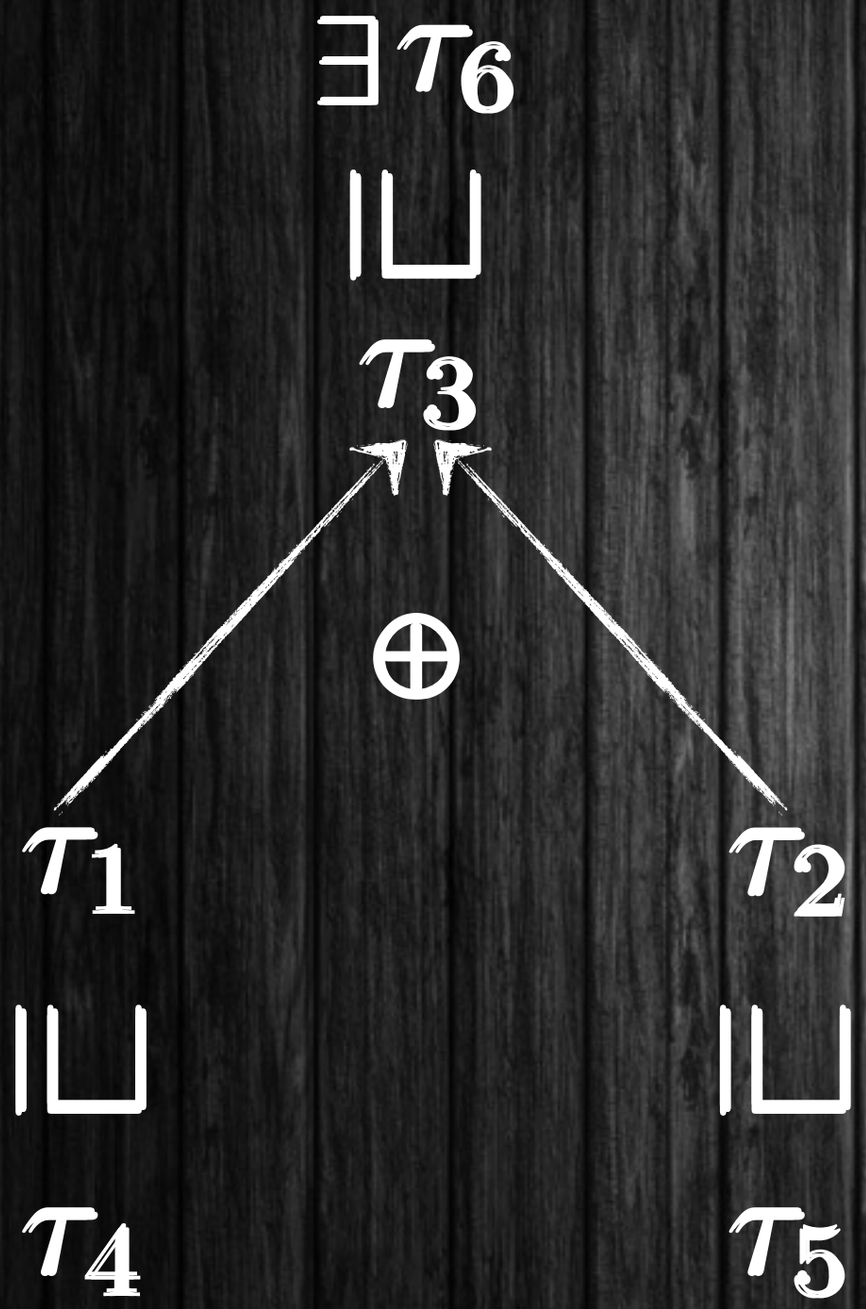


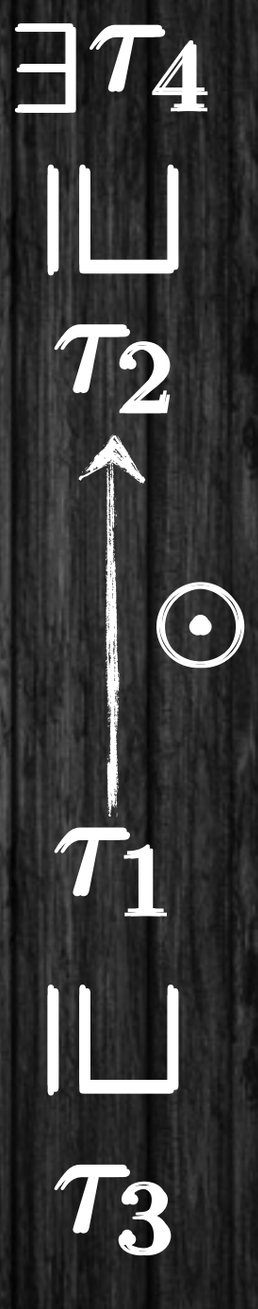
$$y_t^4 <_5 x_s^3$$
$$z_t^4 <_4 z_s^2$$
$$x_s^1 <_6 z_s^3$$



$$x_s^1 <_3 y_t^2$$
$$z_t^5 <_4 z_s^2$$
$$y_s^3 <_2 z_s^4$$
$$y_t^5 <_5 x_s^4$$

1. equating variables
2. saturation
3. variable elimination
4. renaming ✓


$\exists \tau_6$
$\sqcup\!\!\sqcup$
τ_3
$\oplus$
τ_1
$\sqcup\!\!\sqcup$
τ_4
τ_2
$\sqcup\!\!\sqcup$
τ_5


$\exists \tau_4$
$\sqcup\!\!\sqcup$
τ_2
$\odot$
τ_1
$\sqcup\!\!\sqcup$
τ_3

Outline

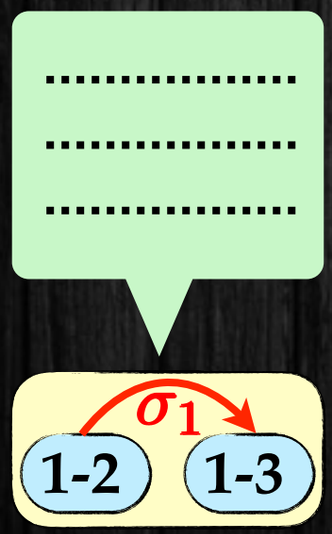
- Background
- Model
- Gap-Order Constraints
- Signatures
- Reachability Algorithm
- Applications

  - Derivation Trees
  - Algorithm

Derivation Trees

$\mathcal{T}$

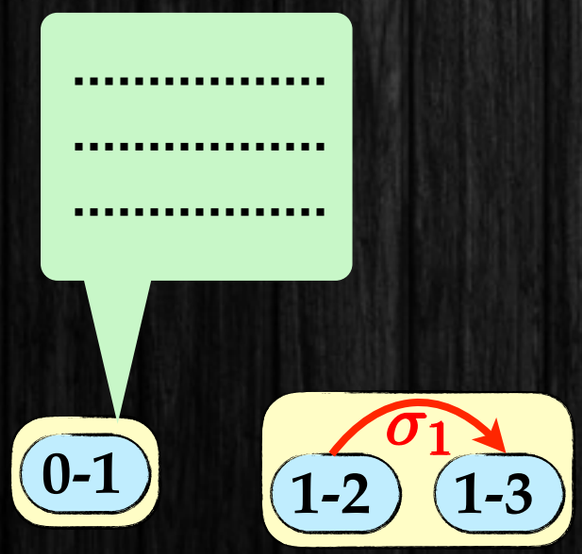
- start with leafs
- leaf: atomic signature



Derivation Trees

$\mathcal{T}$

- start with leafs
- leaf: atomic signature



Derivation Trees

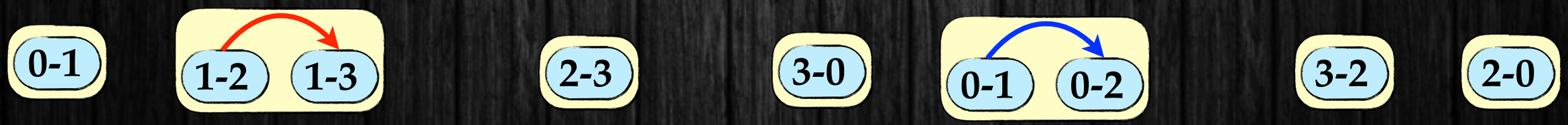
$\mathcal{T}$

- start with leafs
- leaf: atomic signature

Derivation Trees

$\mathcal{T}$

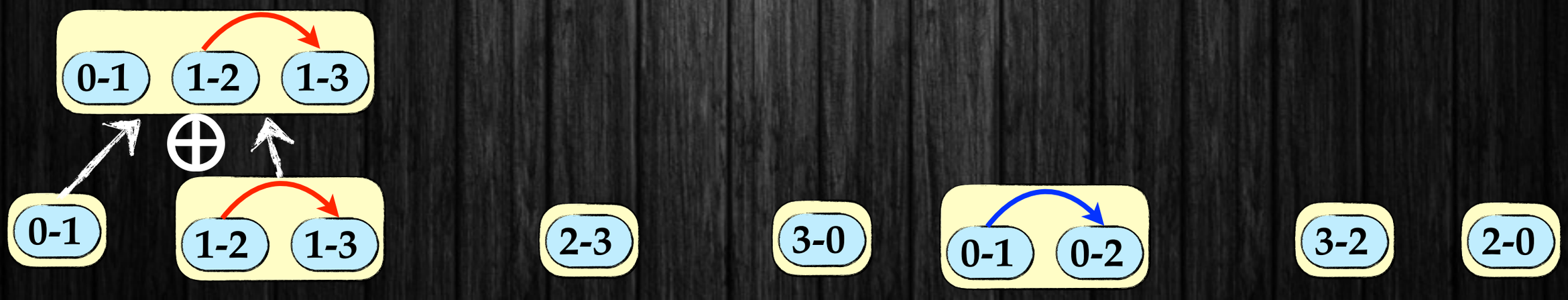
- apply $\oplus$ and $\odot$



Derivation Trees

$\mathcal{T}$

- apply $\oplus$ and $\odot$



Derivation Trees

$\mathcal{T}$

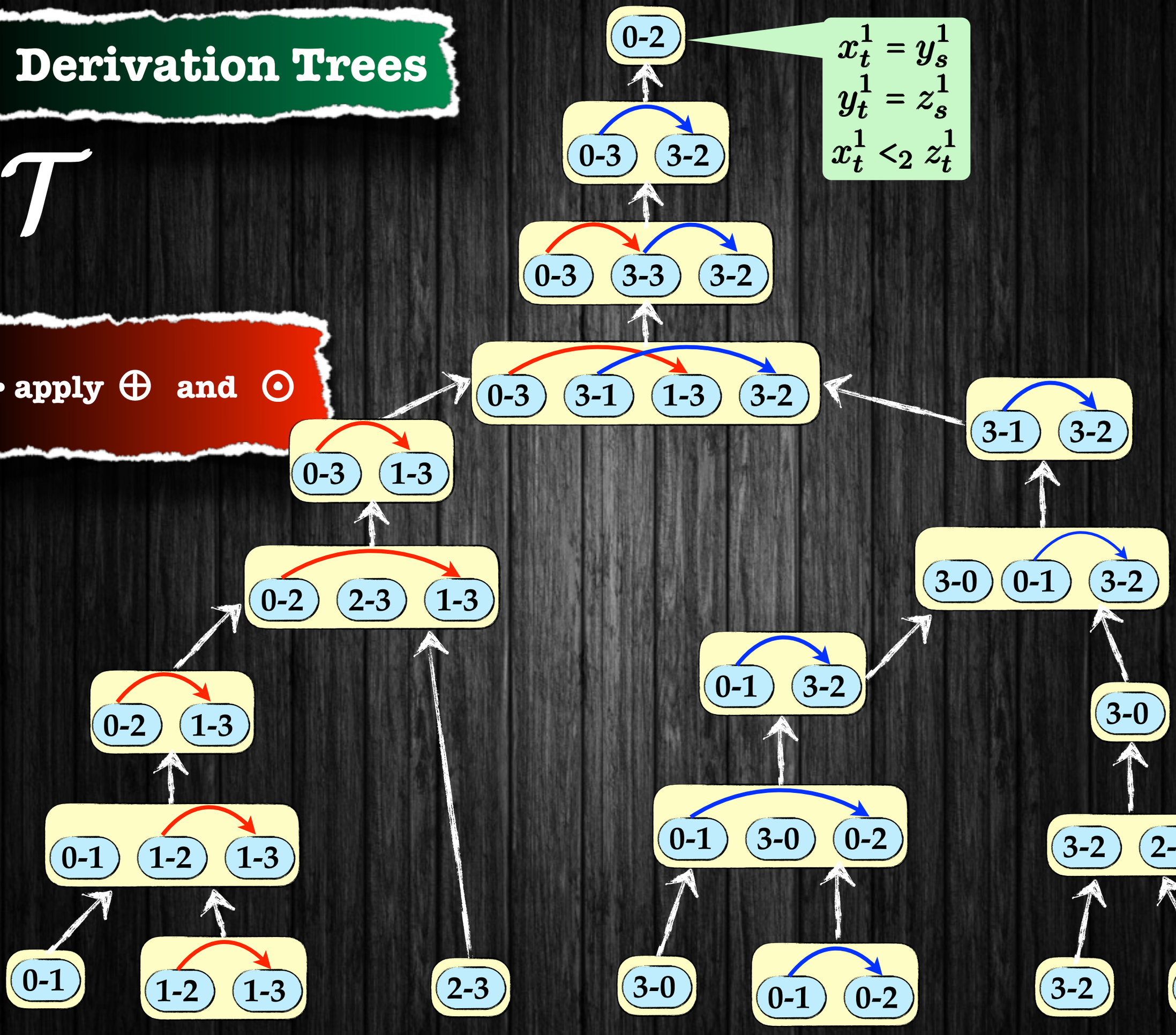
- apply $\oplus$ and $\odot$

Derivation Trees

$\mathcal{T}$

- apply $\oplus$ and $\odot$

$$x_t^1 = y_s^1$$
$$y_t^1 = z_s^1$$
$$x_t^1 <_2 z_t^1$$



Derivation Trees

$\mathcal{T}$

τ_{root}

$\#\tau_{root} = 1$

$x_t^1 = y_s^1$
$y_t^1 = z_s^1$
$x_t^1 <_2 z_t^1$

0-2

0-3 3-2

0-3 3-3 3-2

0-3 3-1 1-3 3-2

0-3 1-3

3-1 3-2

0-2 2-3 1-3

3-0 0-1 3-2

0-2 1-3

0-1 3-2

0-1 1-2 1-3

3-0

0-1 3-0 0-2

3-2 2-0

0-1

1-2 1-3

2-3

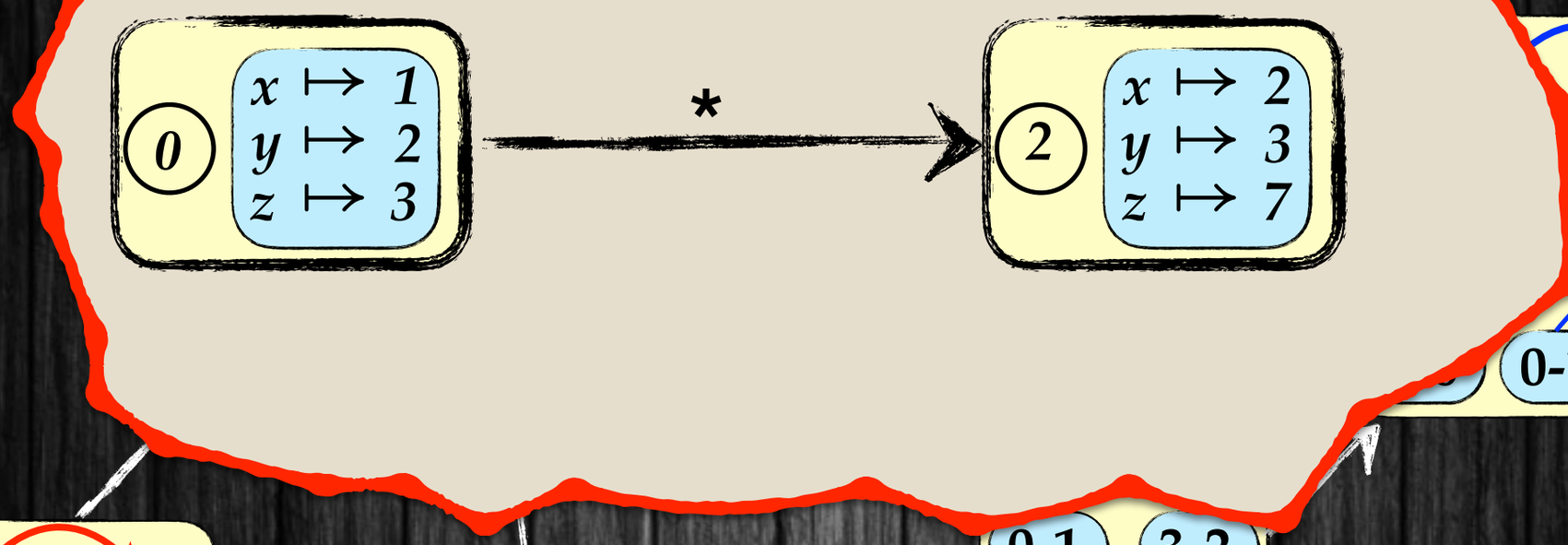
0-1 0-2

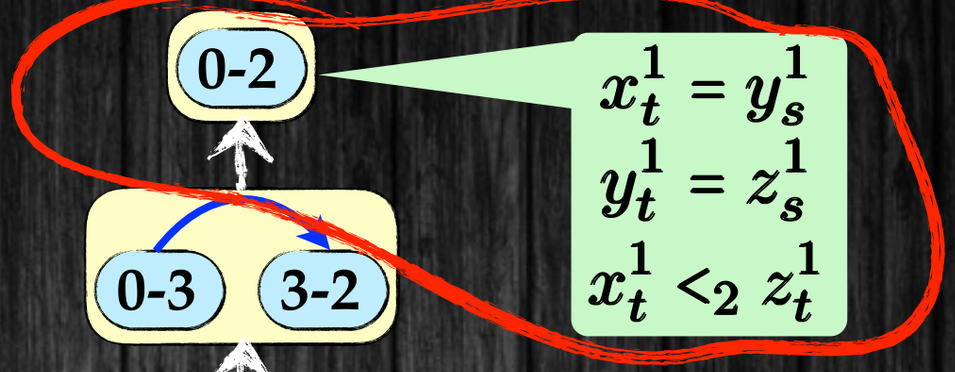
3-2

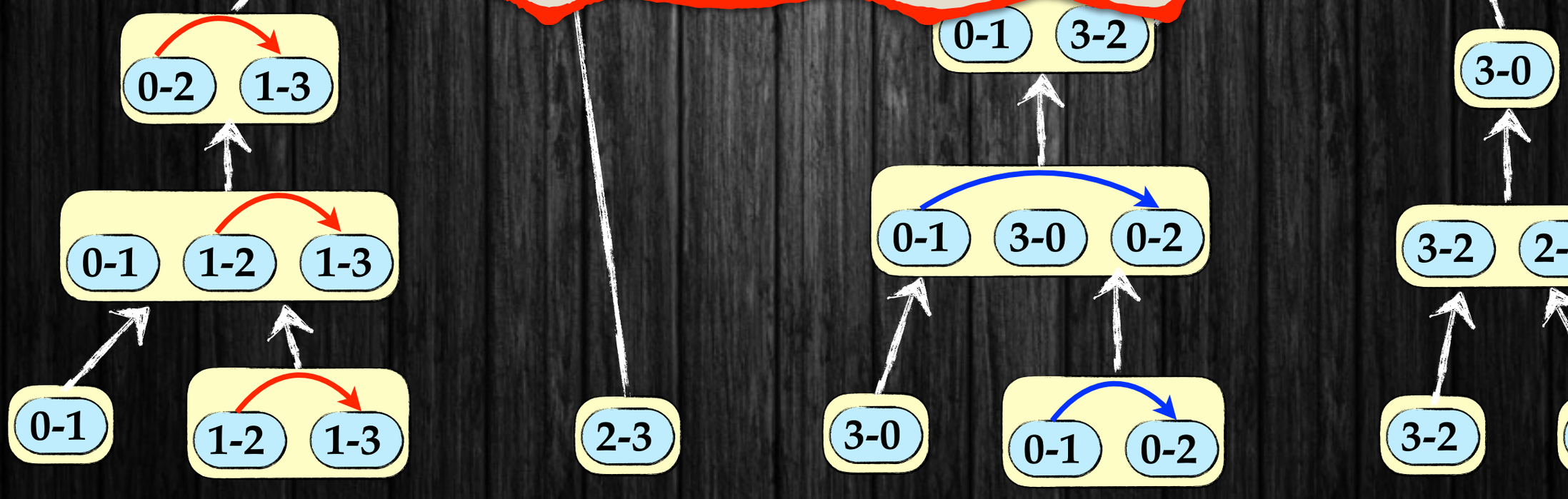
2-0

Derivation Trees

$\mathcal{T}$







Derivation Trees

$\mathcal{T}$

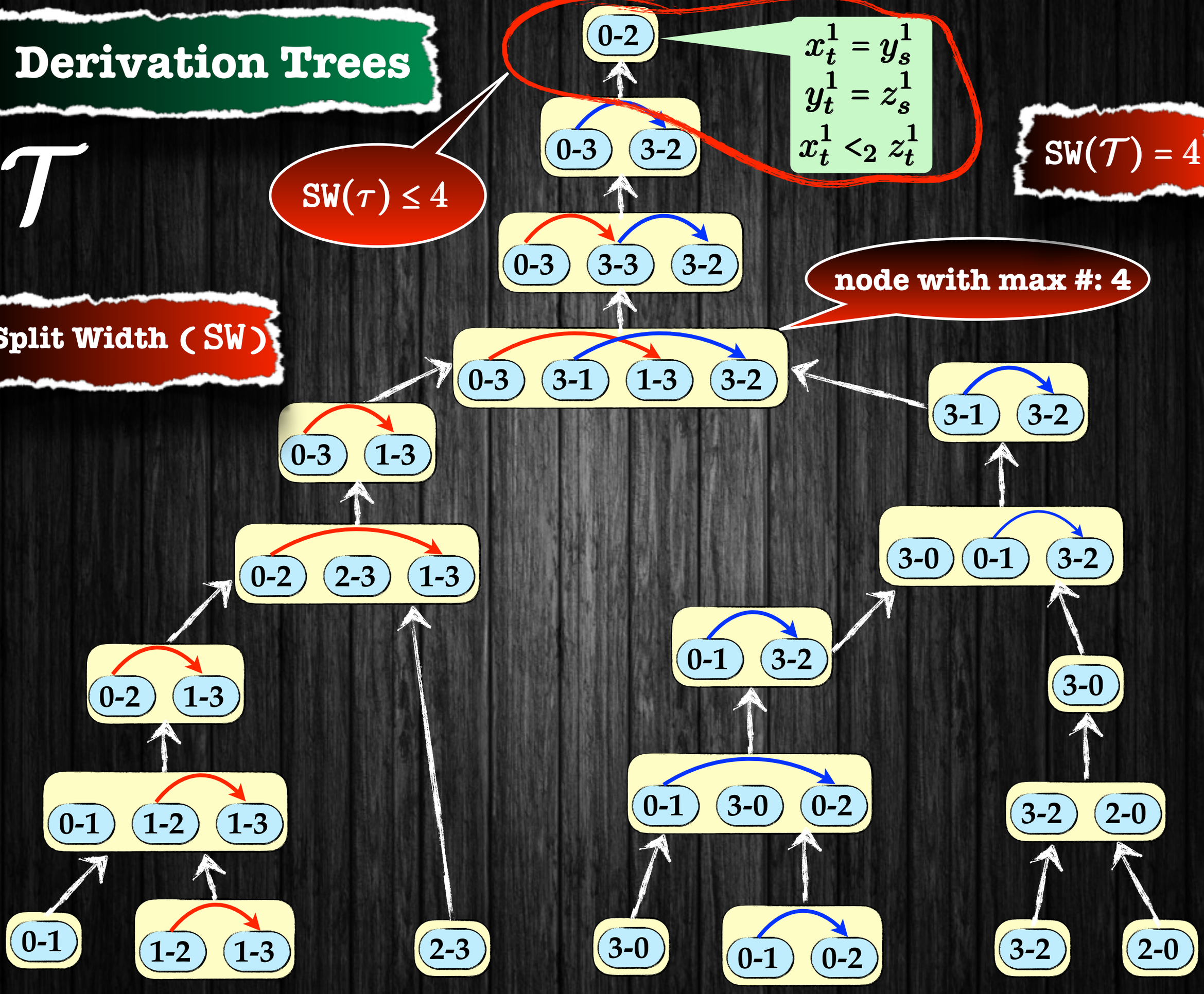
$\mathrm{SW}(\tau) \leq 4$

$x_t^1 = y_s^1$
$y_t^1 = z_s^1$
$x_t^1 <_2 z_t^1$

$\mathrm{SW}(\mathcal{T}) = 4$

Split Width (SW)

node with max #: 4



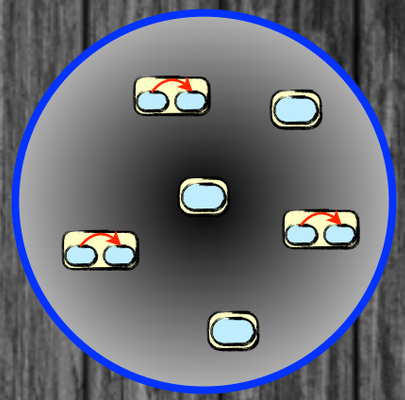
Reachability Algorithm

Generate all $\tau : \mathtt{SW}(\tau) \leq k$

Reachability Algorithm

Generate all $\tau : \mathtt{SW}(\tau) \leq k$

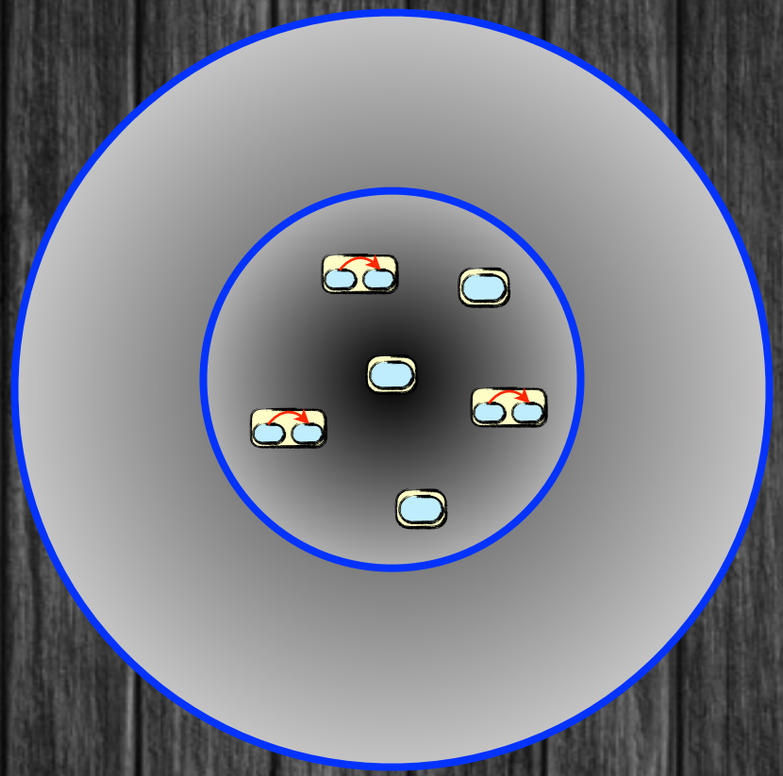
Build all atomic signatures



Reachability Algorithm

Generate all $\tau : \mathrm{SW}(\tau) \leq k$

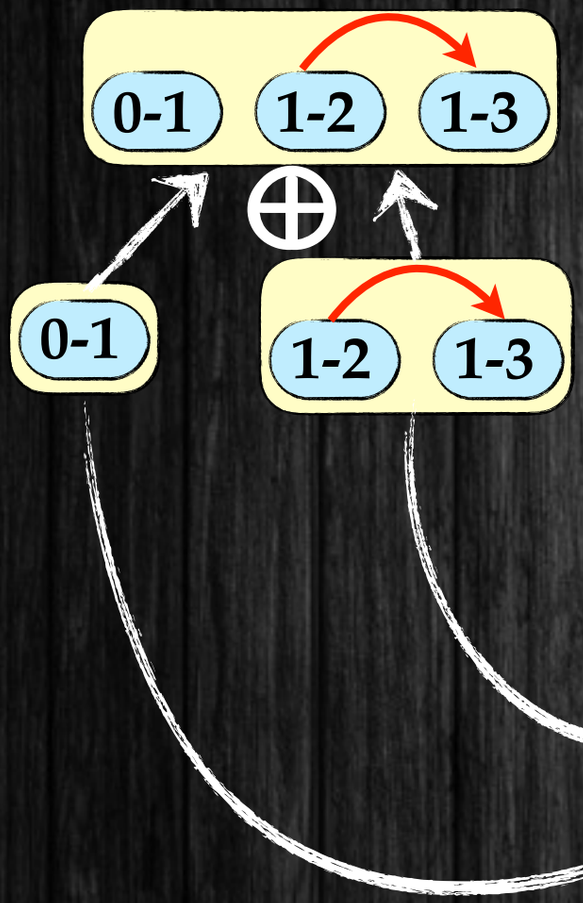
- apply $\oplus$ and $\odot$

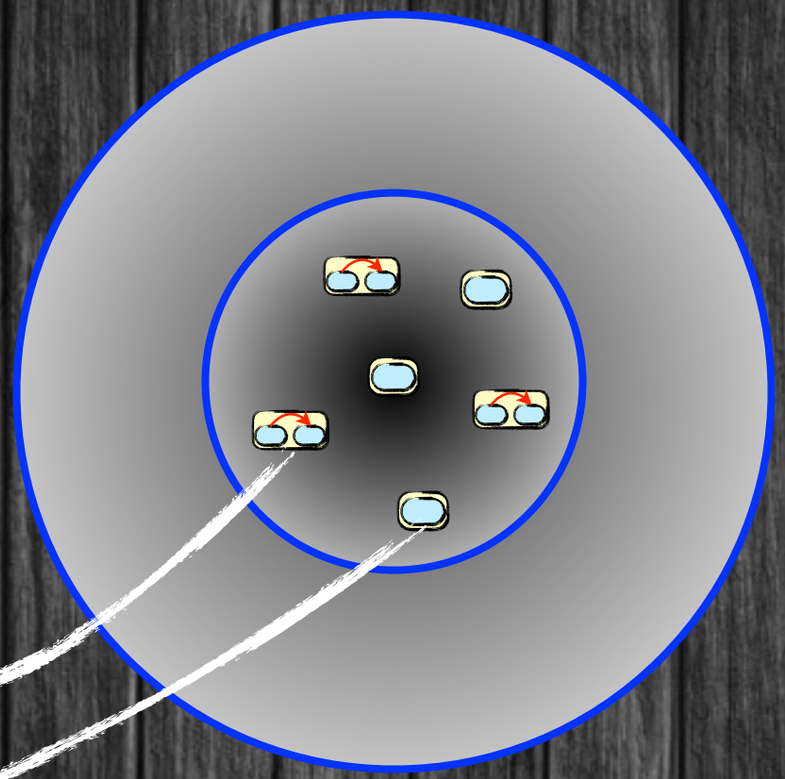


Reachability Algorithm

Generate all $\tau : \mathrm{SW}(\tau) \leq k$

- apply $\oplus$ and $\odot$

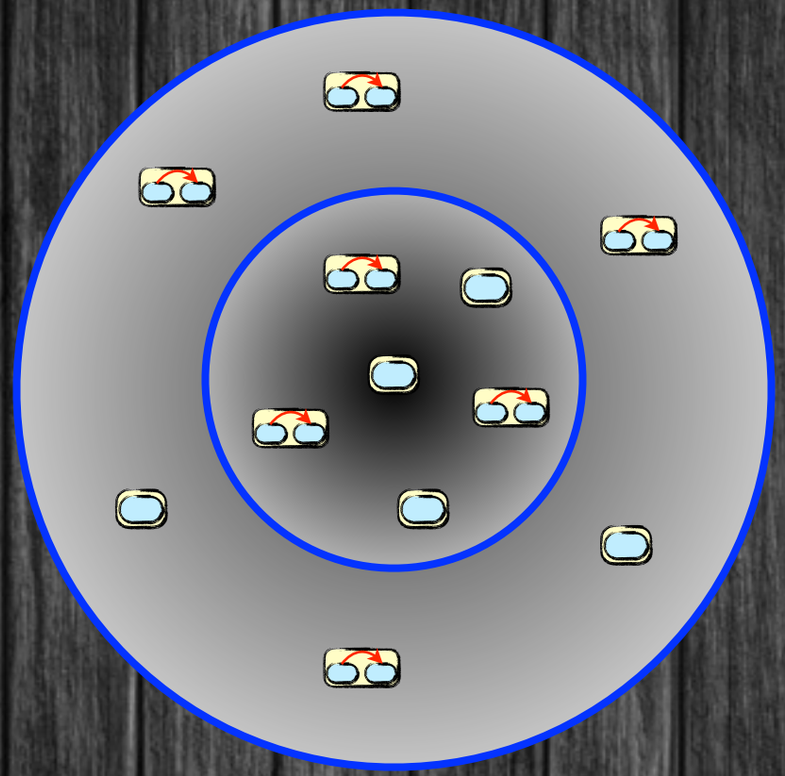




Reachability Algorithm

Generate all $\tau : \mathrm{SW}(\tau) \leq k$

- apply $\oplus$ and $\odot$

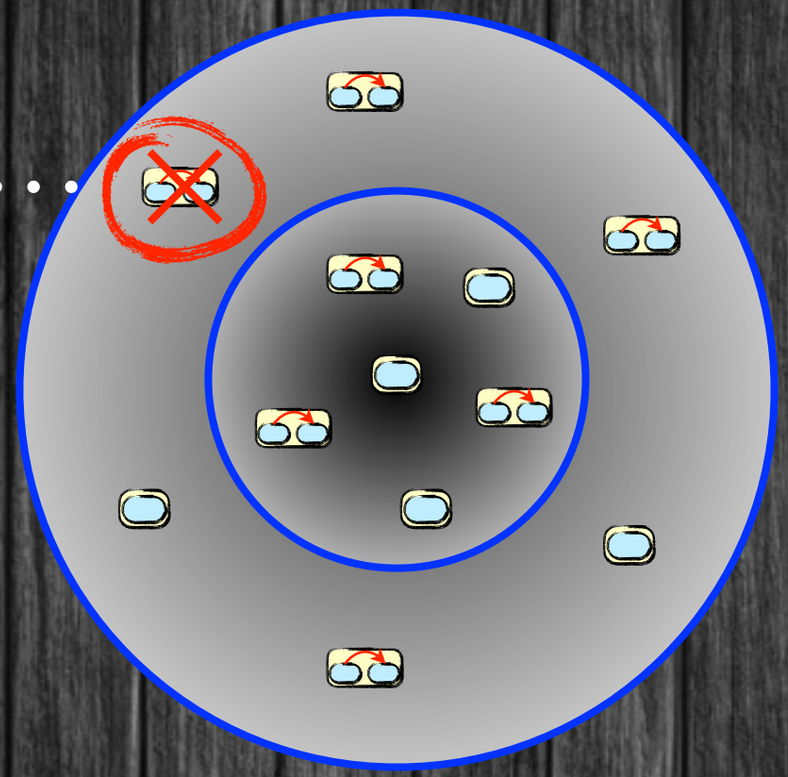


Reachability Algorithm

Generate all $\tau : \mathrm{SW}(\tau) \leq k$

- apply $\oplus$ and $\odot$

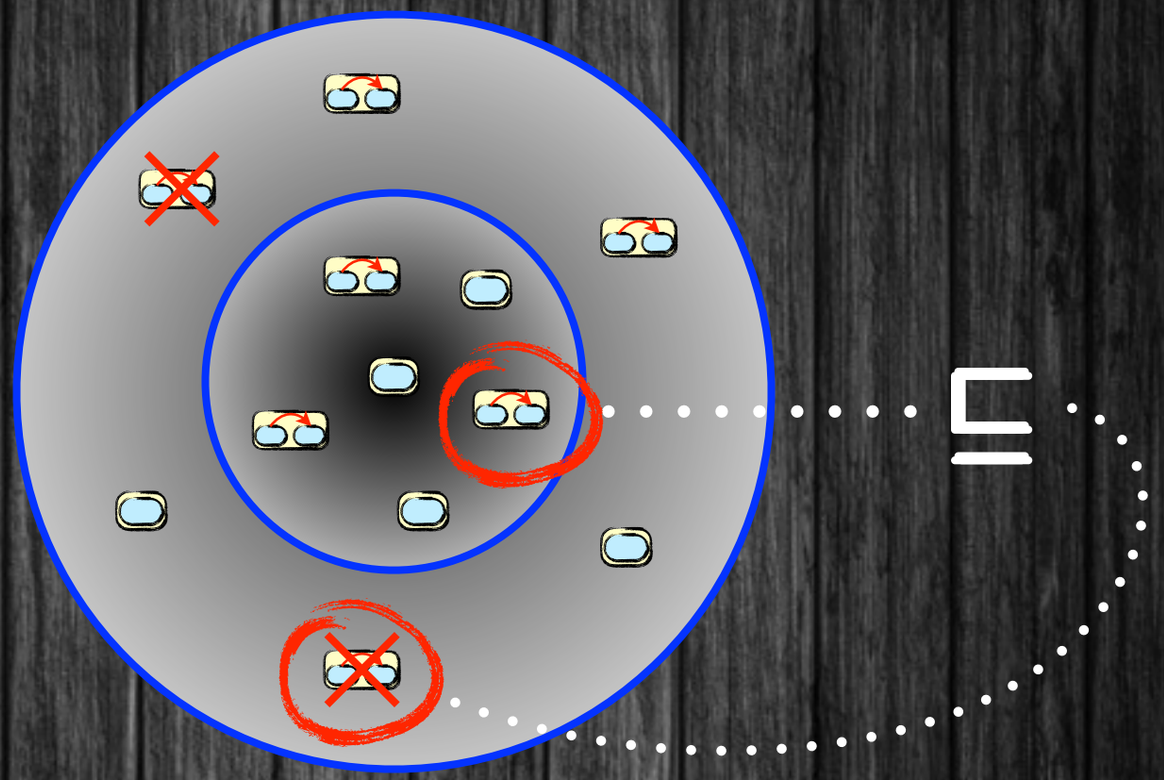
$\mathrm{SW}(\ ) > k$ · · · · · · · · · ·



Reachability Algorithm

Generate all $\tau : \mathrm{SW}(\tau) \leq k$

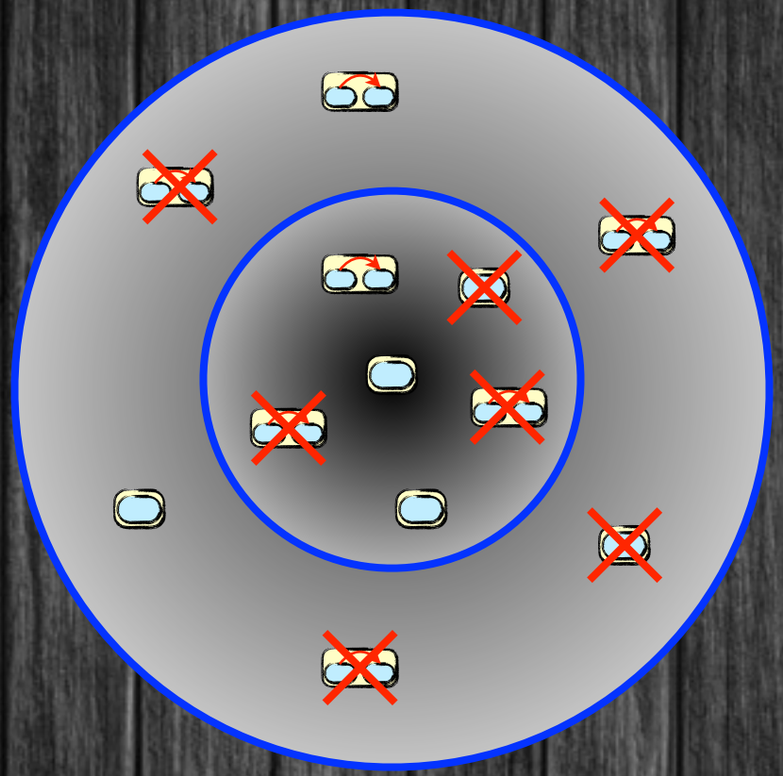
- apply $\oplus$ and $\odot$



Reachability Algorithm

Generate all $\tau : \mathrm{SW}(\tau) \leq k$

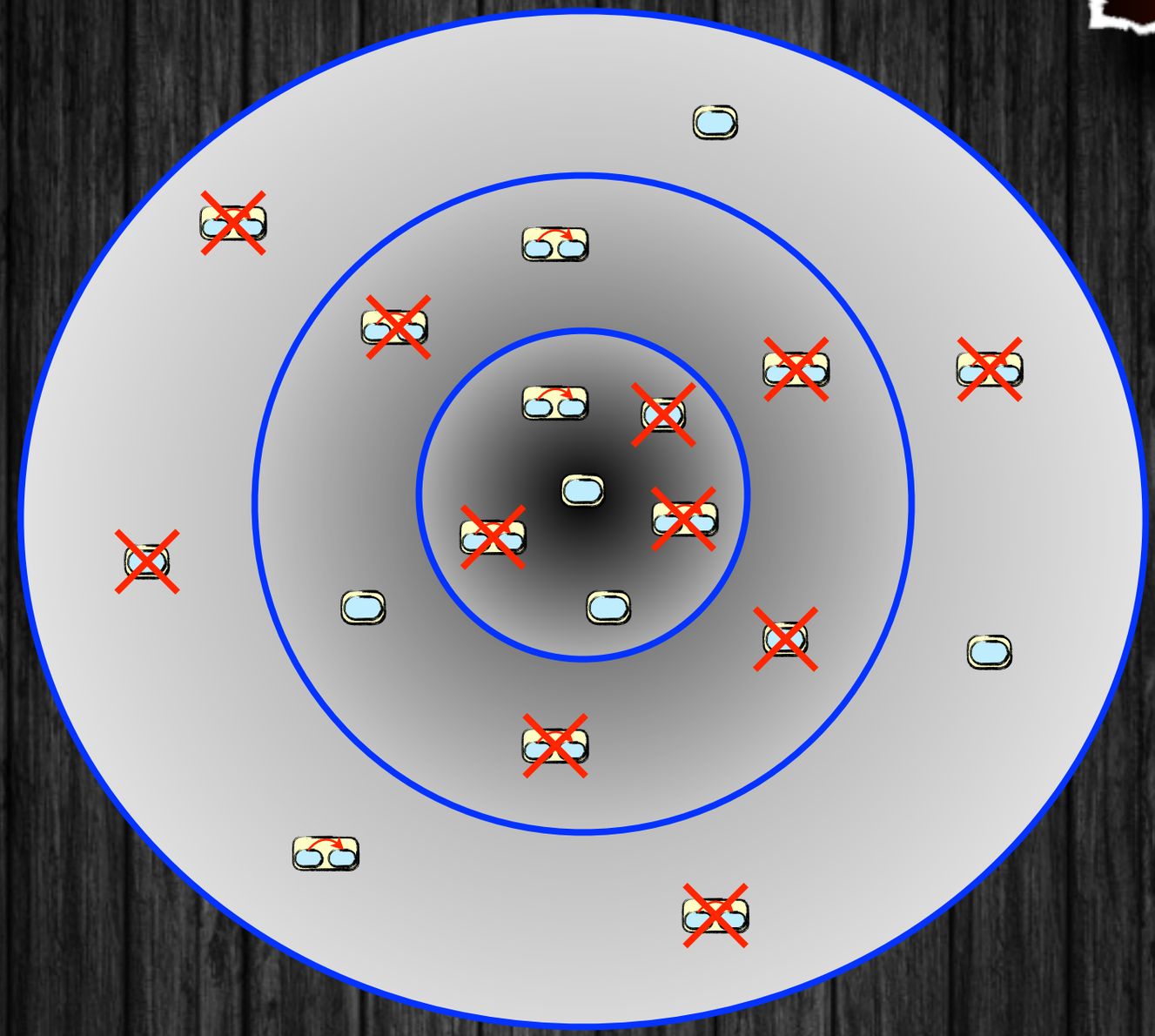
- apply $\oplus$ and $\odot$



Reachability Algorithm

Generate all $\tau : \mathrm{SW}(\tau) \leq k$

- apply $\oplus$ and $\odot$



Reachability Algorithm

Generate all $\tau : \mathrm{SW}(\tau) \leq k$

- apply $\oplus$ and $\odot$

Reachability Algorithm

Generate all $\tau : \mathrm{SW}(\tau) \leq k$

- apply $\oplus$ and $\odot$

Reachability Algorithm

Generate all $\tau : \mathrm{SW}(\tau) \leq k$

- apply $\oplus$ and $\odot$

Reachability Algorithm

Generate all $\tau : \mathrm{SW}(\tau) \leq k$

- apply $\oplus$ and $\odot$

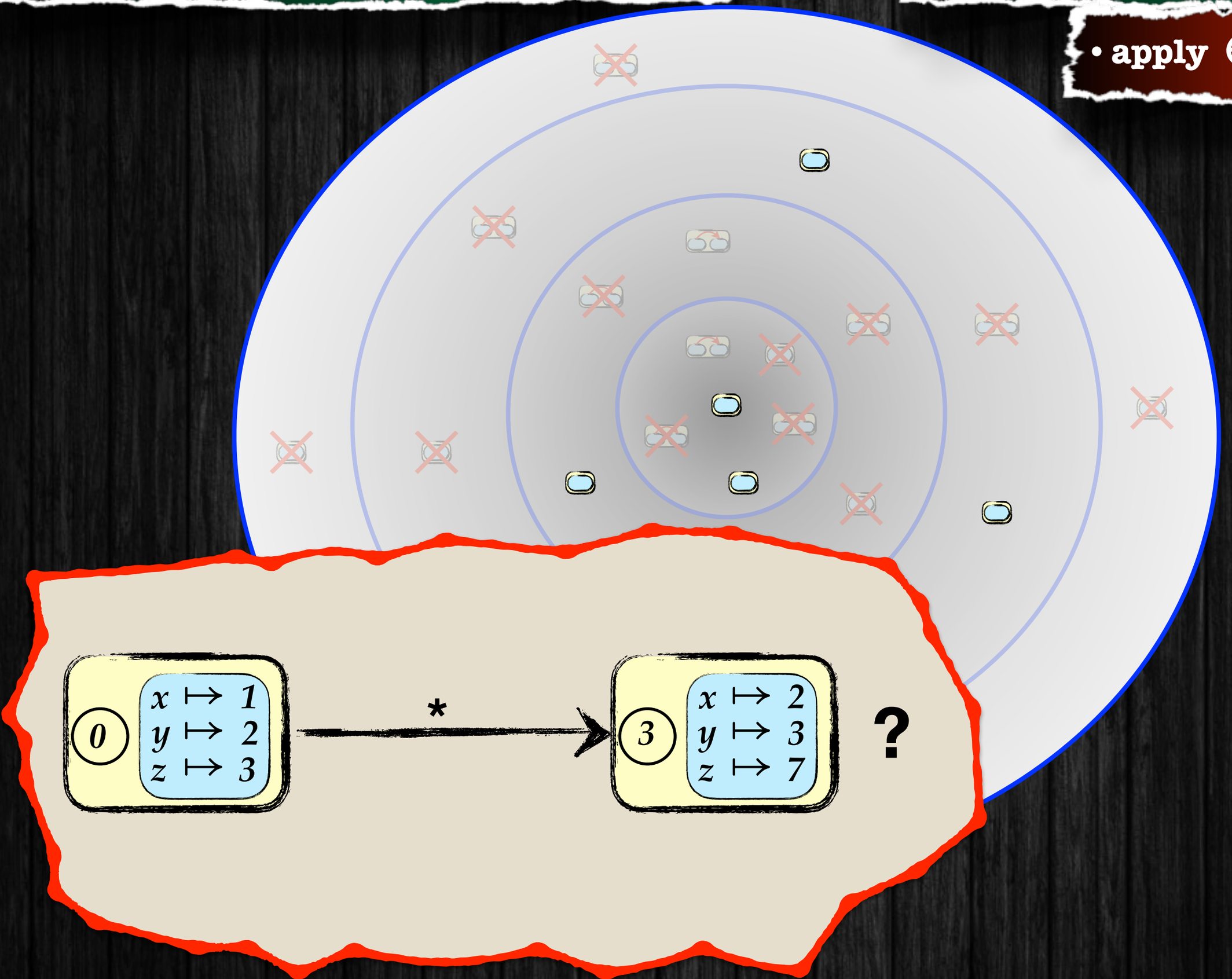
Termination:

- finitely many signatures with $\mathrm{SW} \leq k$
- $\sqsubseteq$ WQO (Dickson's lemma)

Reachability Algorithm

Generate all $\tau : \mathrm{SW}(\tau) \leq k$

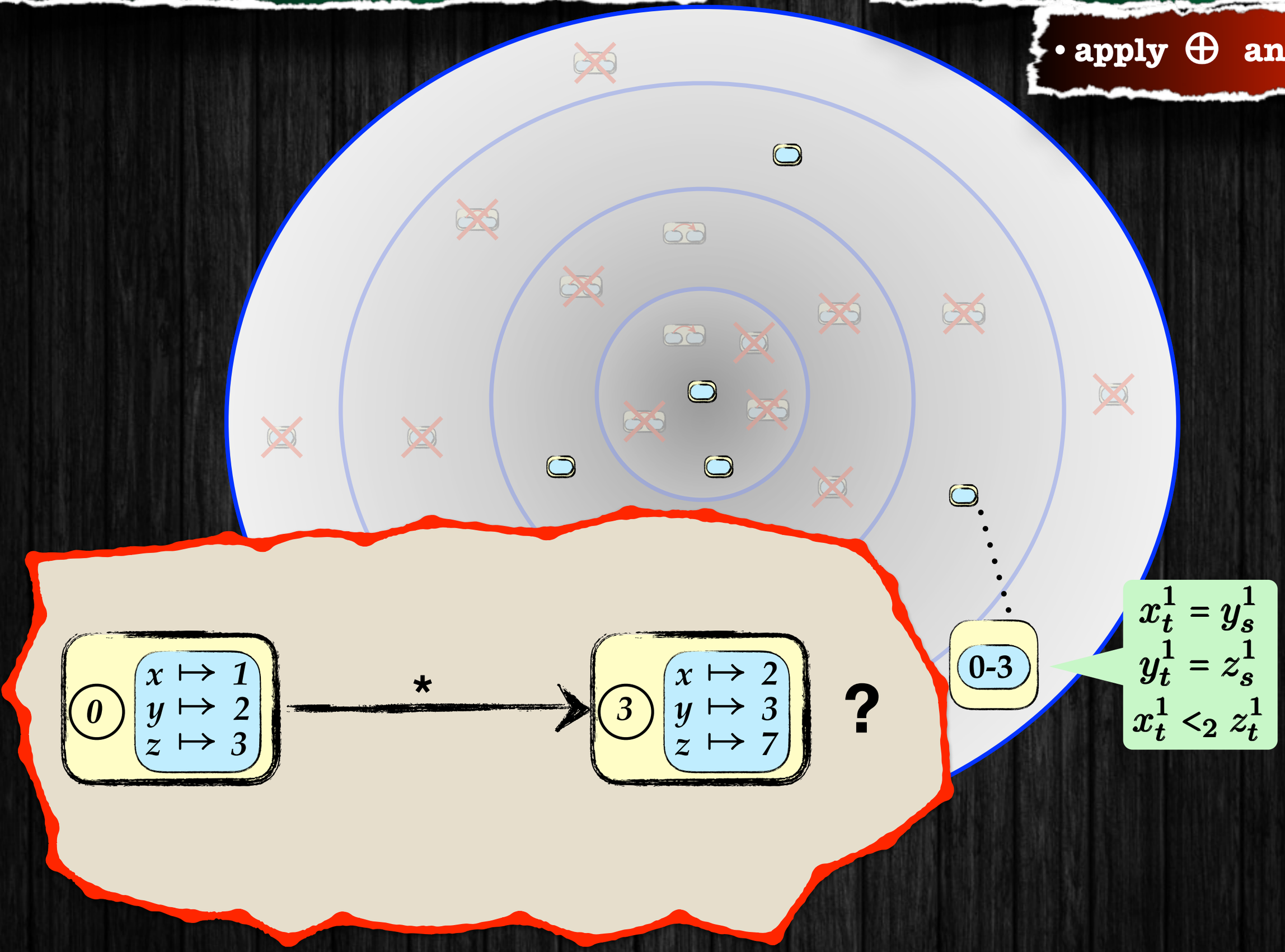
- apply $\oplus$ and $\odot$



Reachability Algorithm

Generate all $\tau : \mathrm{SW}(\tau) \leq k$

- apply $\oplus$ and $\odot$



Outline

- Background
- Model
- Gap-Order Constraints
- Signatures
- Reachability Algorithm
- Applications

Applications: Decidability

- Single-Stack $\mathtt{SW} = 3$
- k-context bounded runs $\mathtt{SW} = k + 2$
- k-scope bounded $\mathtt{SW} = k + 2$
- k-phase bounded $\mathtt{SW} = 2^k$
- ordered-stack runs $\mathtt{SW} = 2^k$