

Termination Resilience Static Analysis

Seminari di Informatica, Università di Parma

Caterina Urban

Inria & École Normale Supérieure | Université PSL

Which Non-Termination Alarm is Worse?

```
function f(x) {
```

```
1...
2z ← 10
3if ( ... ) then
    while 4(z ≥ 0) do
        5z ← z - x
    od6
else
    while 7(z ≥ x) do
        8c ← [-2, 1]
        9z ← z + c
    od10
fi
```

```
}11
```



diverges when $x = 0$



diverges when $c \geq 0$

non-deterministic value choice

Which Non-Termination Alarm is Worse?

Robust Non-Termination

```
function f(x) {
```

```
1...
2z ← 10
3if ( ... ) then
    while 4(z ≥ 0) do
        5z ← z - x
    od6
else
    while 7(z ≥ x) do
        8c ← [-2, 1]
        9z ← z + c
    od10
fi
```

```
}11
```



diverges when $x = 0$



diverges when $c \geq 0$

Robust Non-Termination

$\exists \text{ Input } \forall \text{ Non-Deterministic Choices : Program Diverges}$

```
function f(x){  
    1...  
    2z ← 10  
    3if ( ... ) then  
        while 4(z ≥ 0) do  
            5z ← z - x  
        od6  
    else  
        while 7(z ≥ x) do  
            8c ← [-2, 1]  
            9z ← z + c  
        od10  
    fi  
}11
```



← diverges when $x = 0$

Termination Resilience

$\forall \text{ Inputs } \exists \text{ Non-Deterministic Choice : Program Terminates}$

```
function f(x) {  
    1...  
    2z ← 10  
    3if ( ... ) then  
        while 4(z ≥ 0) do  
            5z ← z - x  
            od6  
    else  
        while 7(z ≥ x) do  
            8c ← [-2, 1] ←  terminates when c < 0, independently of the value of x  
            9z ← z + c  
            od10  
    fi  
}11
```

terminates when $c < 0$, independently of the value of x

angelic non-determinism

Termination Resilience Static Analysis

3-Step Recipe

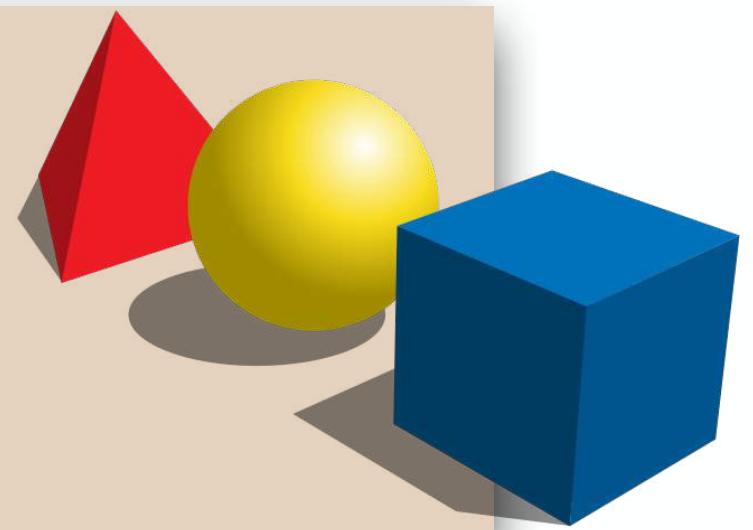
practical tools

targeting specific programs



abstract semantics, abstract domains

algorithmic approaches to decide program properties



concrete semantics

mathematical models of the program behavior



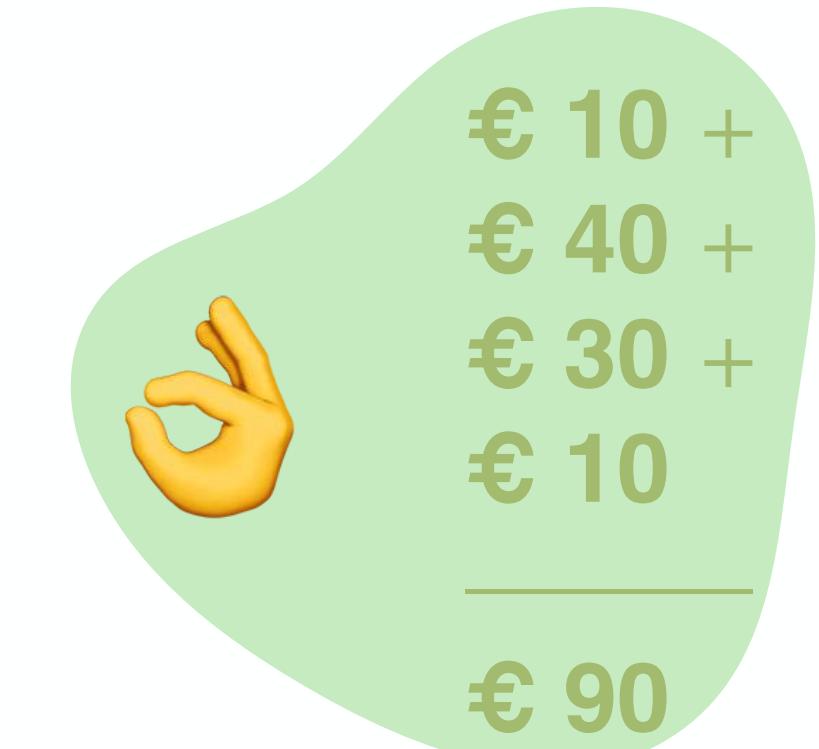
Static Analysis by Abstract Interpretation



PROPERTY OF INTEREST



SOUNDNESS



COMPLETENESS



€ 9.95 +
€ 35.85 +
€ 27.95 +
€ 4.85
€ 78.60



FALSE ALARM

Termination Resilience Static Analysis

3-Step Recipe

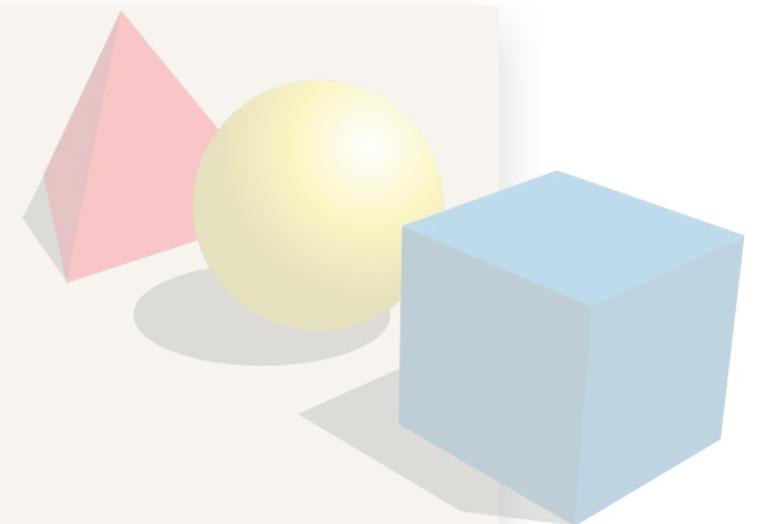
practical tools

targeting specific programs



abstract semantics, abstract domains

algorithmic approaches to decide program properties

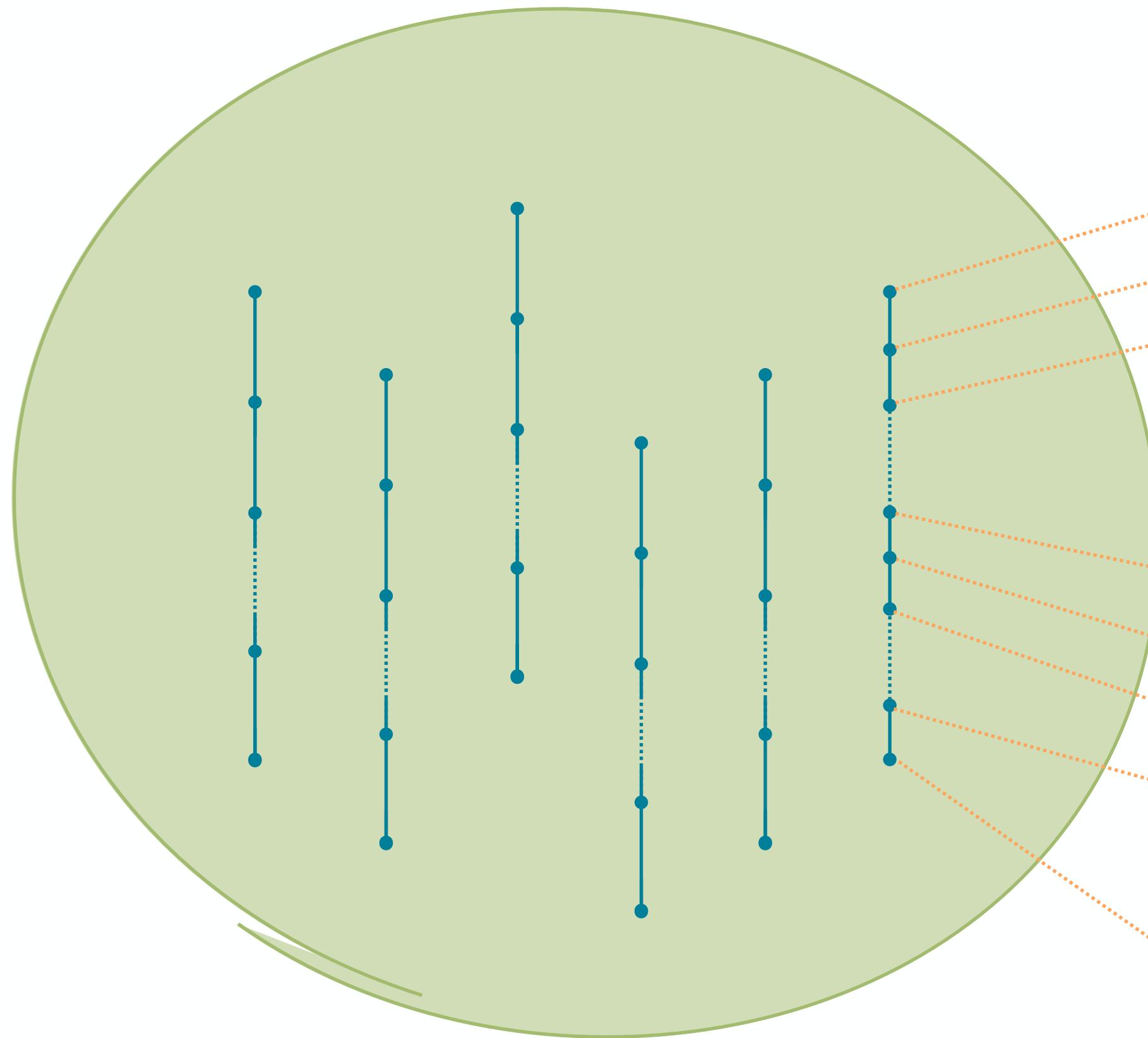


concrete semantics

mathematical models of the program behavior



Trace Semantics



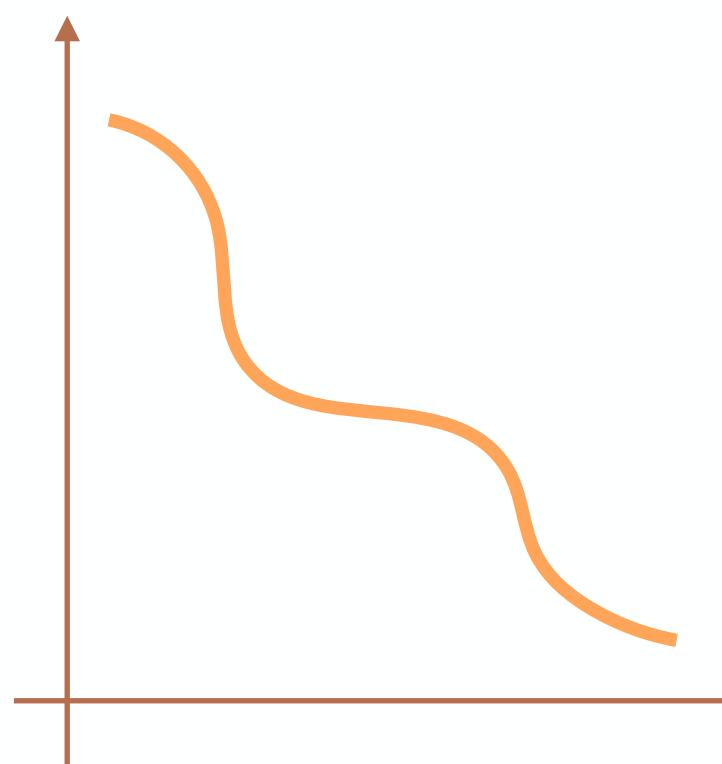
```
function f(x) {  
    1 a ← [-∞, +∞]  
    2 z ← 10  
    3 if (a*a ≥ 0) then  
        while 4(z ≥ 0) do  
            5 z ← z - x  
            od 6  
        else  
            while 7(z ≥ x) do  
                8 c ← [-2, 1]  
                9 z ← z + c  
            od 10  
        fi  
    }11
```



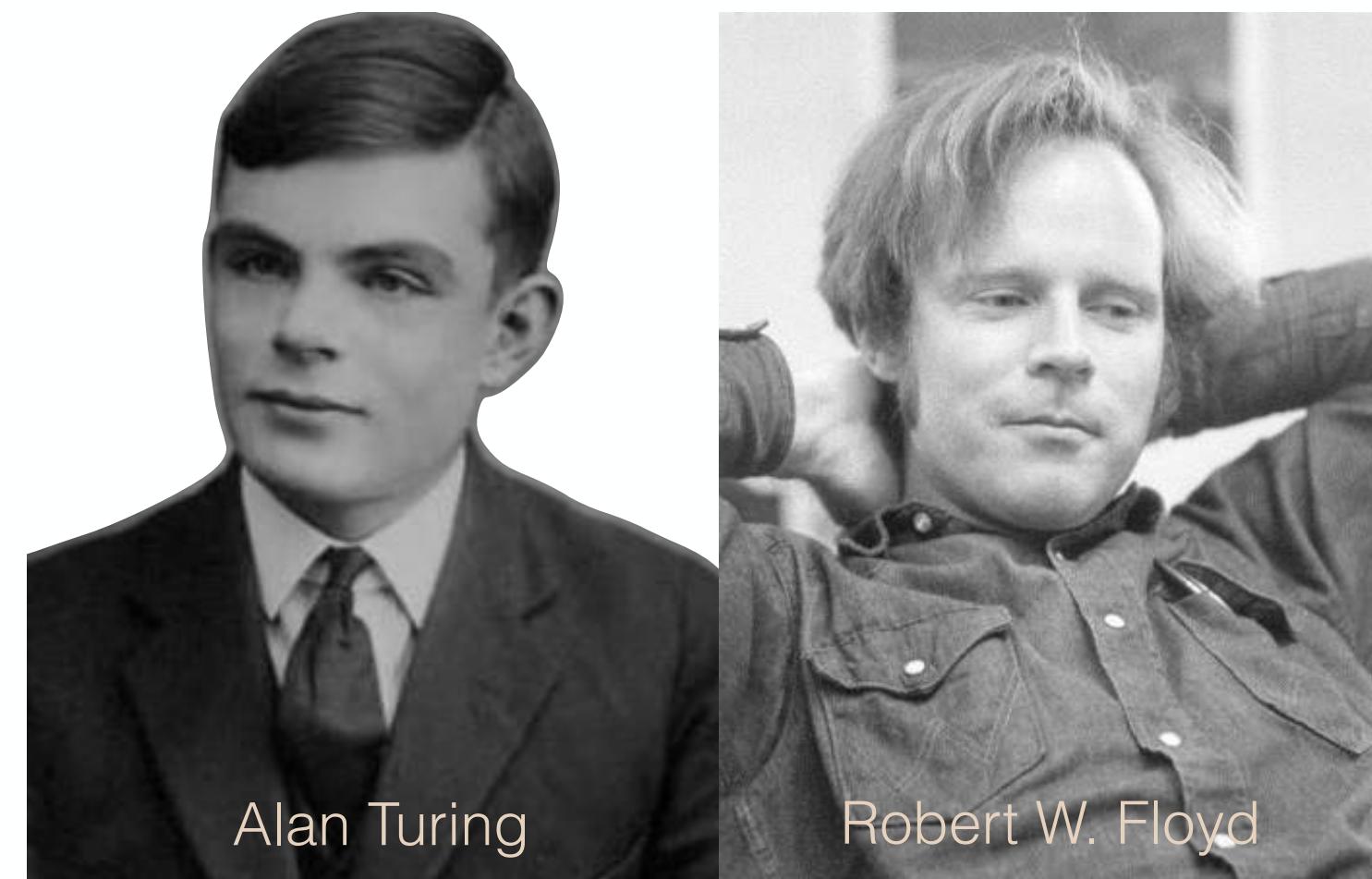
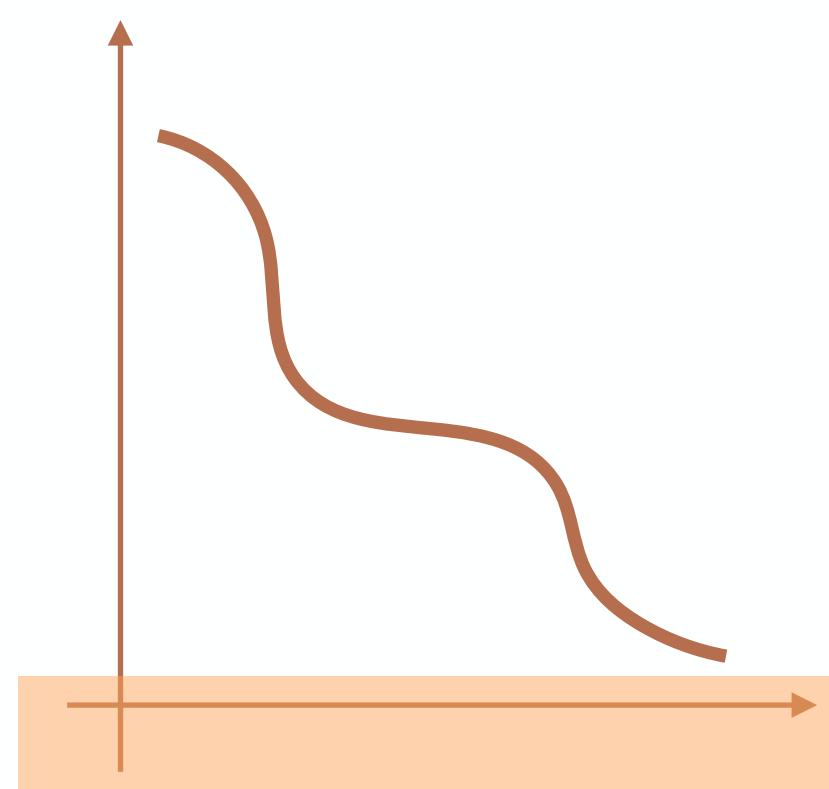
Ranking Functions

Traditional Method for Proving Termination

strictly decreasing along the execution of a program...



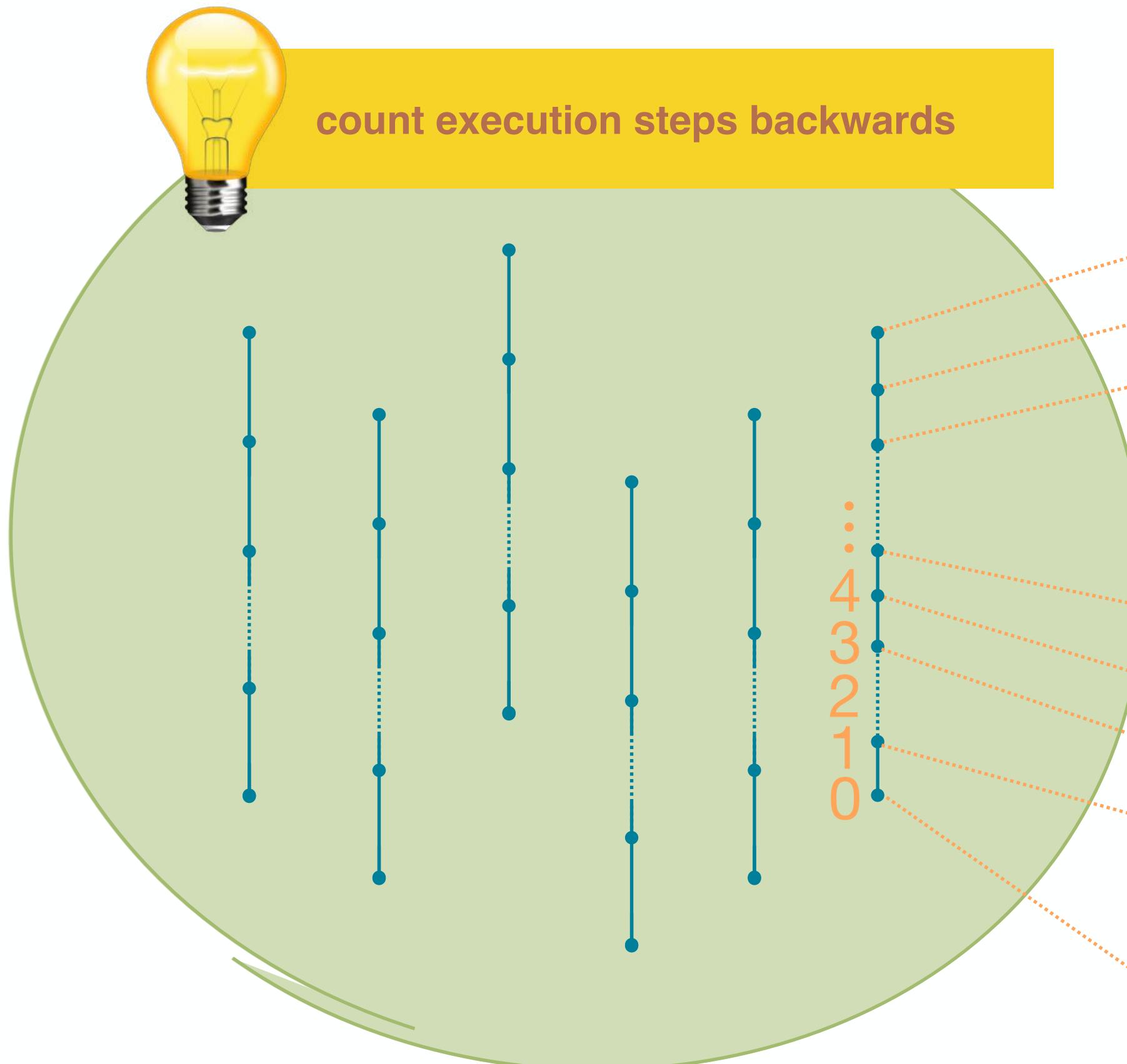
...and well-founded



Alan Turing

Robert W. Floyd

Termination Resilience Semantics



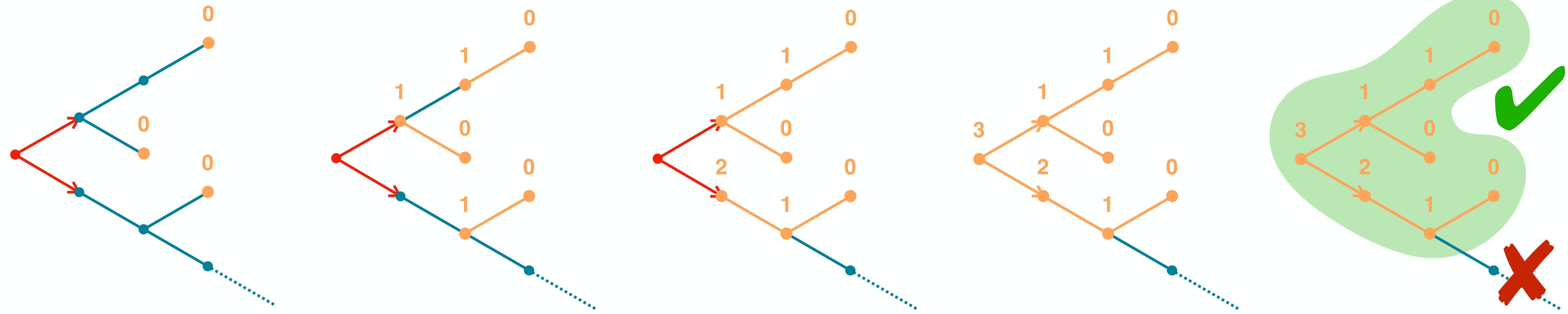
```
function f(x) {  
    1 a ← [-∞, +∞]  
    2 z ← 10  
    3 if (a*a ≥ 0) then  
        while 4(z ≥ 0) do  
            5 z ← z - x  
            od 6  
        else  
            while 7(z ≥ x) do  
                8 c ← [-2, 1]  
                9 z ← z + c  
            od 10  
        fi  
    }11
```



Termination Resilience Semantics

$$\Theta \stackrel{\text{def}}{=} \text{lfp}_{\subseteq \emptyset} \lambda f \lambda s . \begin{cases} 0 & \text{final states} \\ \sup\{f(s') + 1 \mid \langle s, s' \rangle \in \tau\} & s \in \tilde{\text{pre}}_{\tau^i}(X) \\ \inf\{f(s') + 1 \mid \langle s, s' \rangle \in \tau\} & s \in \text{pre}_{\tau^i}(\text{dom}(f)) \\ \text{undefined} & \text{otherwise} \end{cases}$$

$f_1 \sqsubseteq f_2 \stackrel{\text{def}}{=} \text{dom}(f_1) \subseteq \text{dom}(f_2) \wedge \forall x \in \text{dom}(f_1) : f_1(x) \leq f_2(x)$
 $\tilde{\text{pre}}_{\tau^i}(X) \stackrel{\text{def}}{=} \{s \mid \forall s' : \langle s, s' \rangle \in \tau^i \Rightarrow s' \in X\}$
 input transitions
 $\text{regular transitions}$
 $\text{totally undefined function}$



Termination Resilience Semantics

$$\Theta \stackrel{\text{def}}{=} \text{lfp}_{\dot{\emptyset}}^{\sqsubseteq} \lambda f \lambda s . \begin{cases} 0 & s \in \Omega_{\tau} \\ \sup\{f(s') + 1 \mid \langle s, s' \rangle \in \tau\} & s \in \tilde{\text{pre}}_{\tau^i}(\text{dom}(f)) \\ \sup\{f(s') + 1 \mid \langle s, s' \rangle \in \tau\} & s \in \text{pre}_{\tau^r}(\text{dom}(f)) \\ \text{undefined} & \text{otherwise} \end{cases}$$



the existence of the fixpoint is not guaranteed

$$\begin{array}{l} \text{1 } x \leftarrow [-\infty, +\infty] \\ \text{while } \text{2 } (x \neq 0) \text{ do} \\ \quad \text{3 } x \leftarrow [-\infty, +\infty] \\ \text{od } \text{4 } \end{array} \xrightarrow{\hspace{1cm}} \lambda x . \begin{cases} 1 & x = 0 \\ \text{undefined} & \text{otherwise} \end{cases} \quad \lambda x . \begin{cases} 3 & x = 0 \\ \text{undefined} & \text{otherwise} \end{cases} \quad \dots$$

Termination Resilience Static Analysis

3-Step Recipe

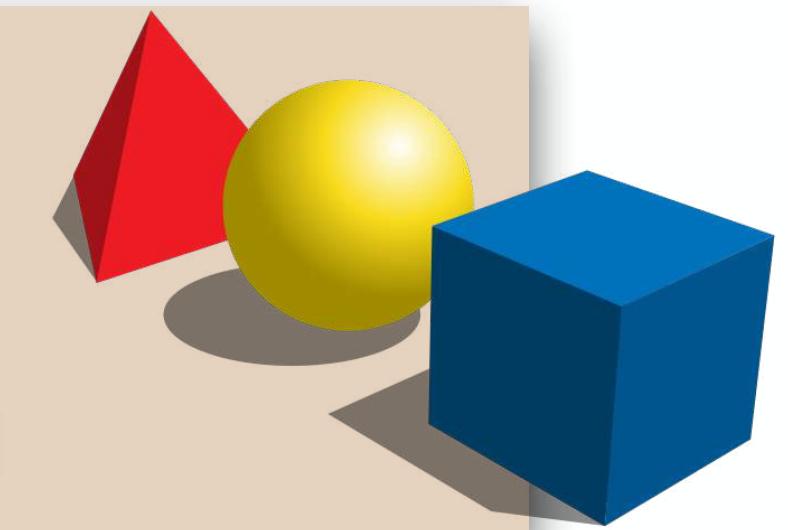
practical tools

targeting specific programs



abstract semantics, abstract domains

algorithmic approaches to decide program properties

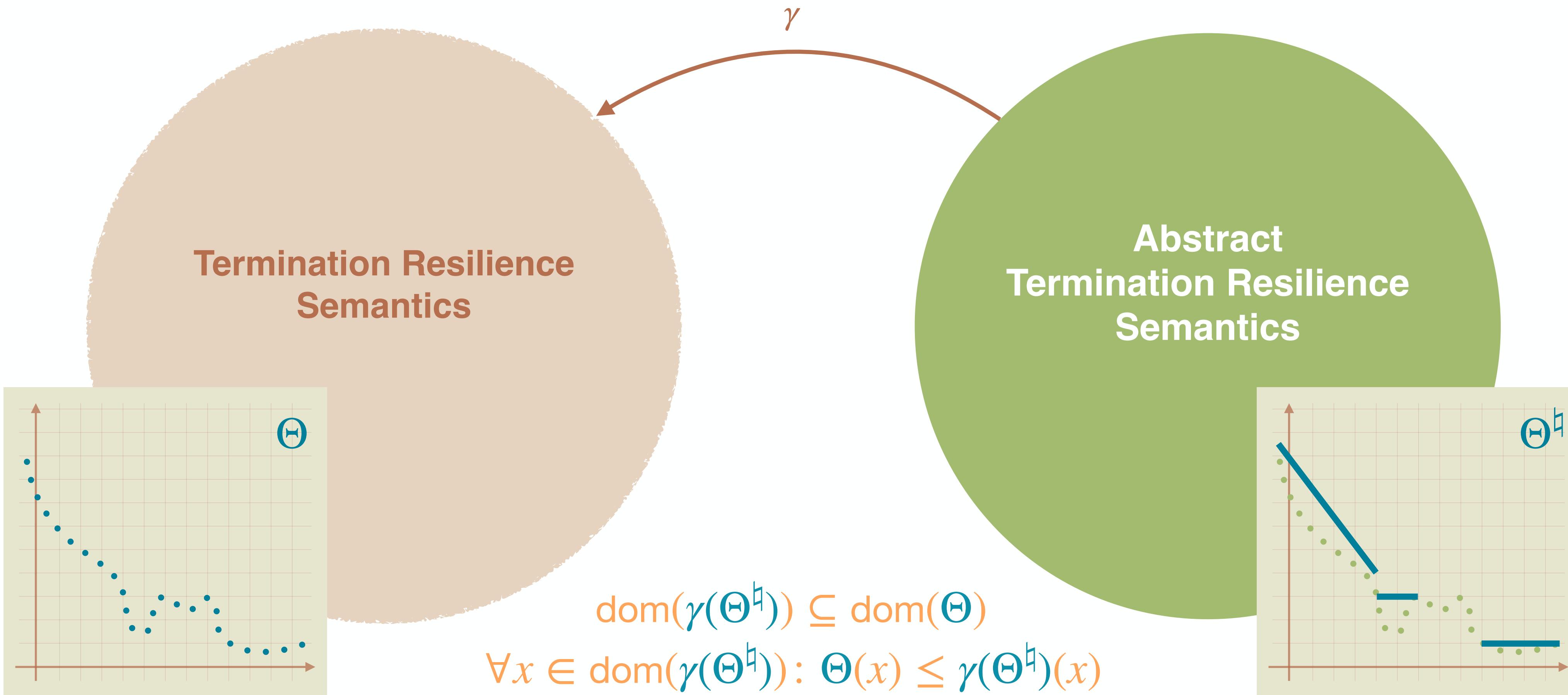


concrete semantics

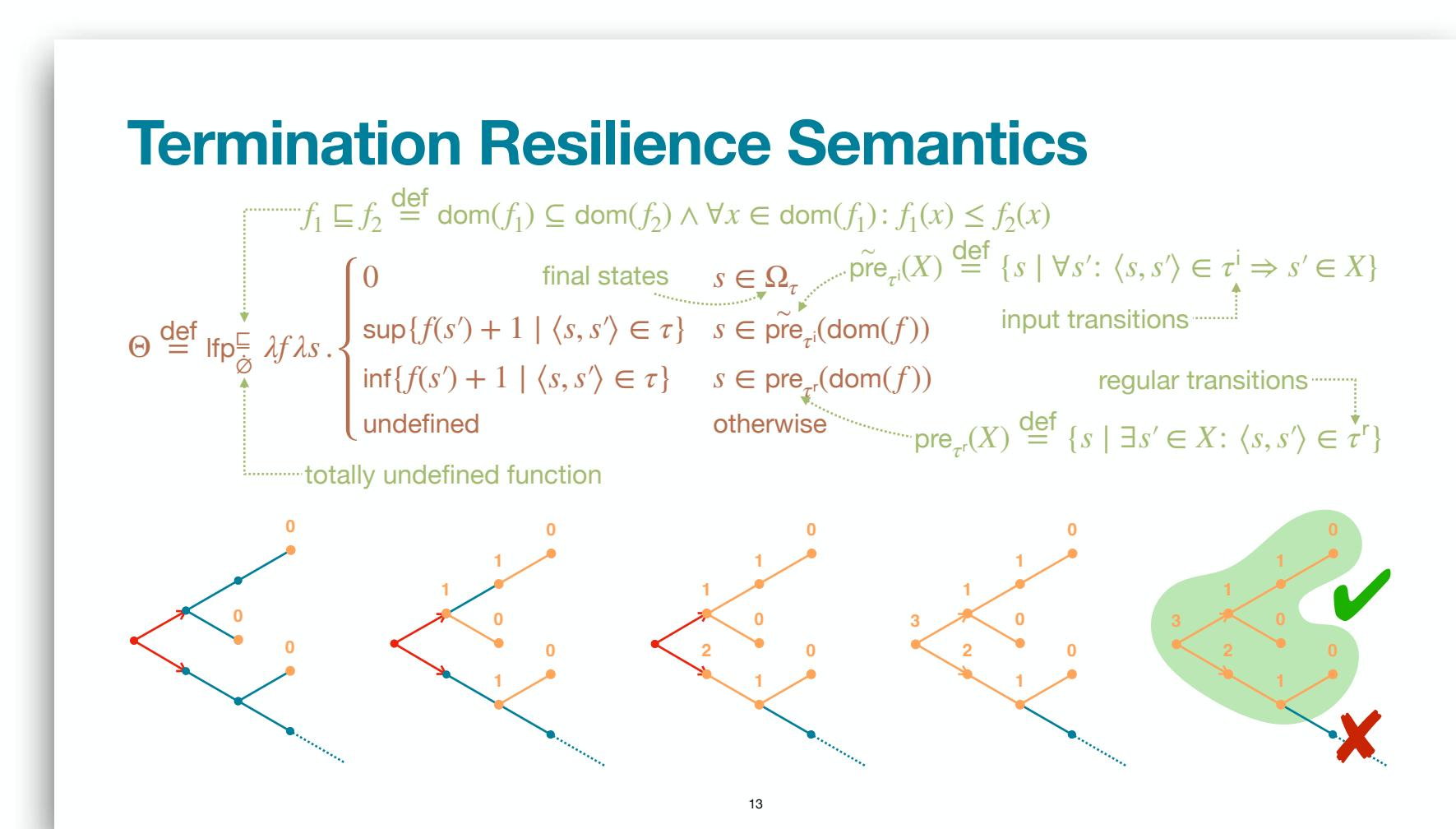
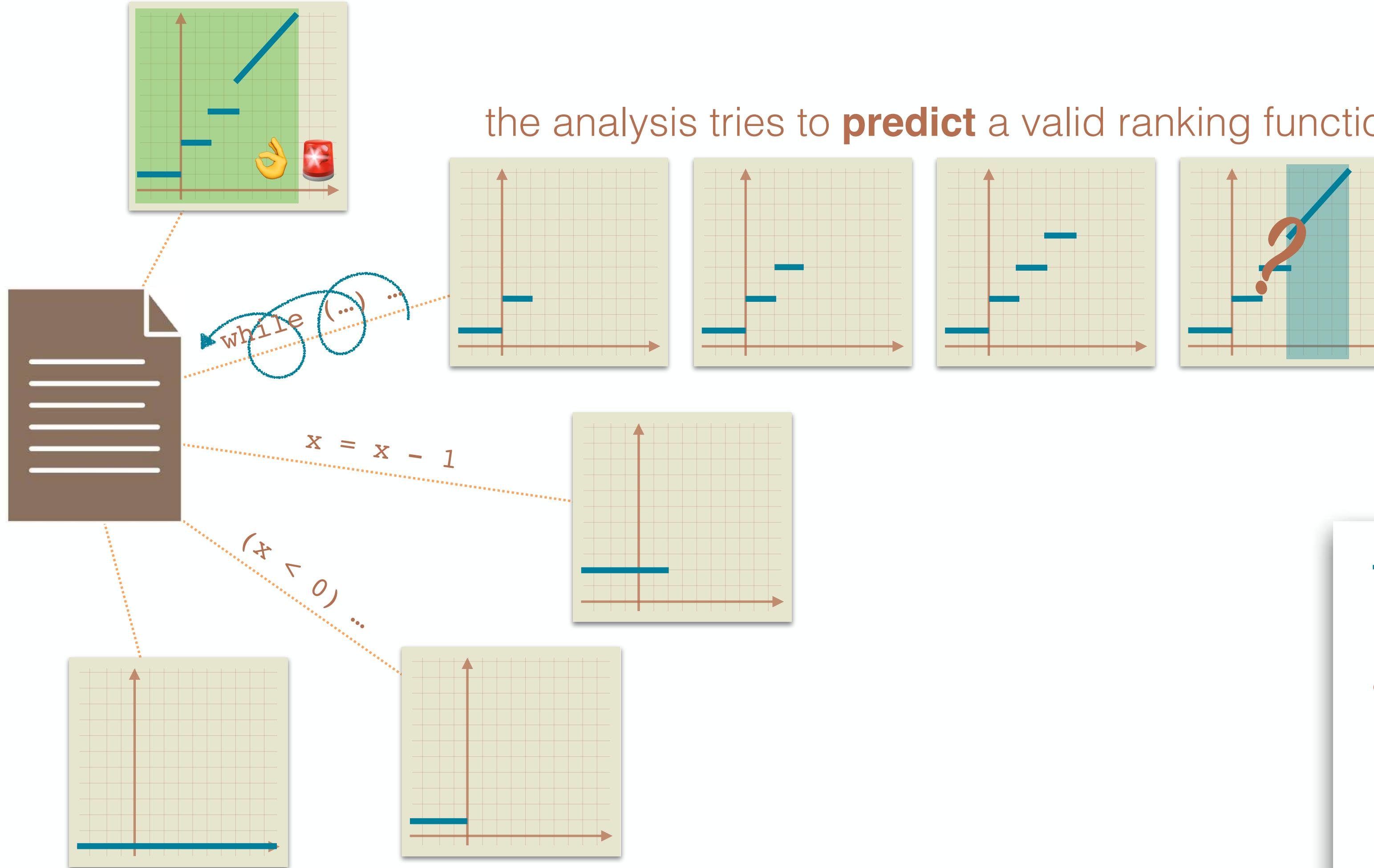
mathematical models of the program behavior



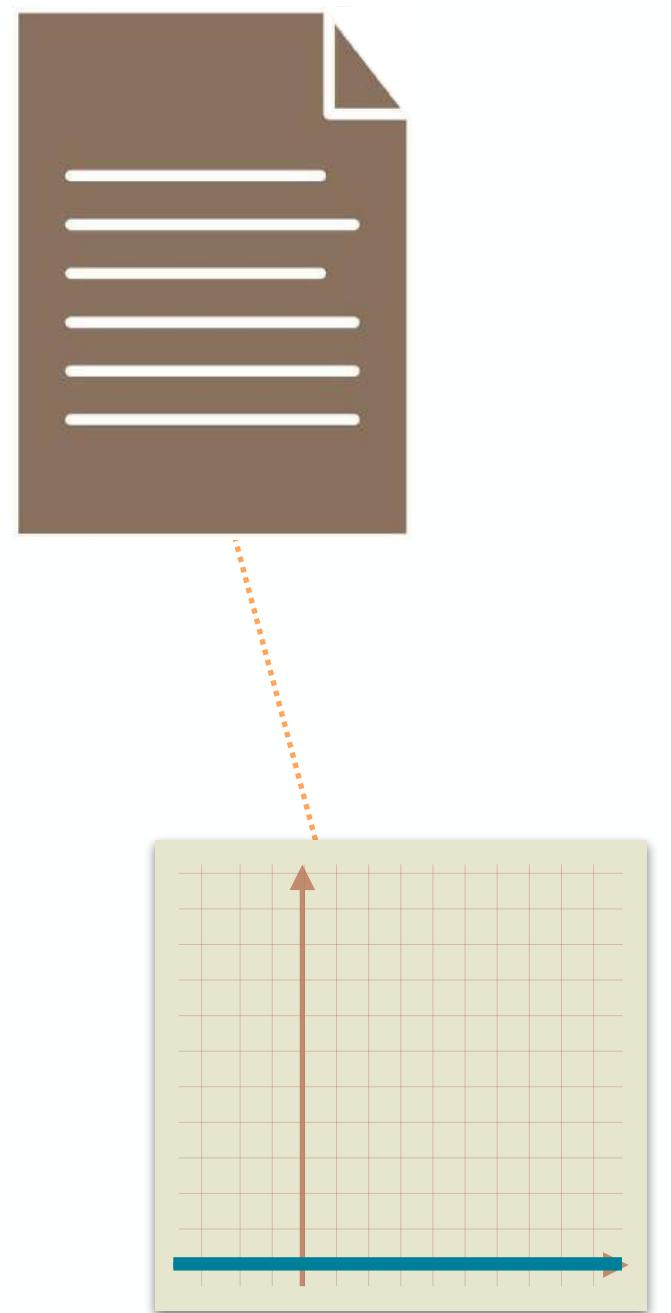
Piecewise-Defined Ranking Functions



Termination Resilience Static Analysis



Termination Resilience Static Analysis



Termination Resilience Static Analysis

Static Backward Analysis

```

function f(x) {
    1 a  $\leftarrow [-\infty, +\infty]$ 
    2 z  $\leftarrow 10$ 
    3 if (a*a  $\geq 0$ ) then
        while 4(z  $\geq 0$ ) do
            5 z  $\leftarrow z - x$ 
        od6
    else
        while 7(z  $\geq x$ ) do
            8 c  $\leftarrow [-2, 1]$ 
            9 z  $\leftarrow z + c$ 
        od10
    fi
}11

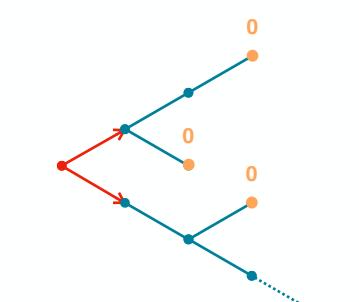
```

$\lambda x z a c . \ 0$

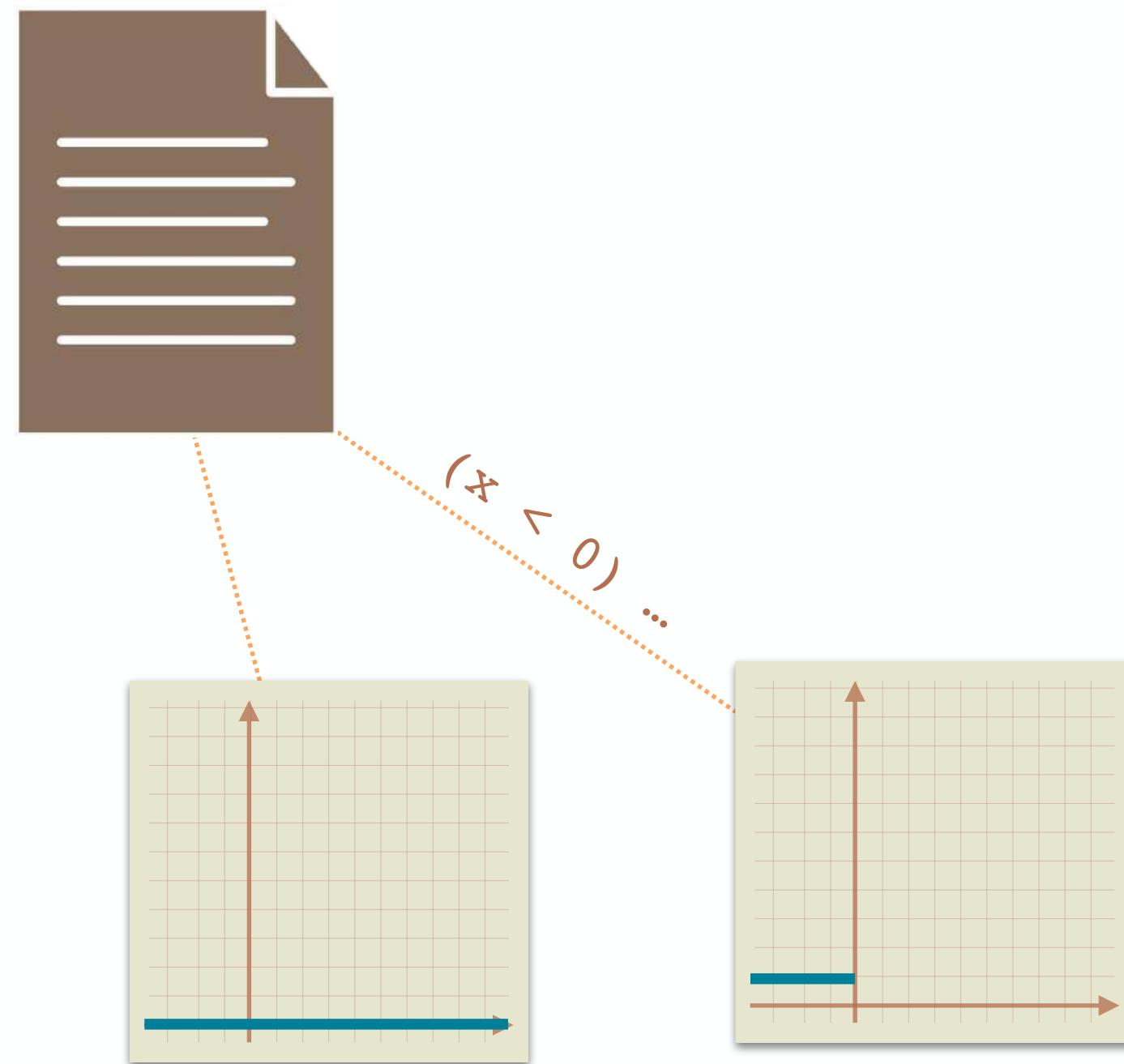
Termination Resilience Semantics

$$f_1 \sqsubseteq f_2 \stackrel{\text{def}}{=} \text{dom}(f_1) \subseteq \text{dom}(f_2) \wedge \forall x \in \text{dom}(f_1) : f_1(x) \leq f_2(x)$$

$$\Theta \stackrel{\text{def}}{=} \text{lfp}_{\emptyset}^{\sqsubseteq} \lambda f \lambda s . \begin{cases} 0 & \text{final states } s \in \Omega_{\tau} \\ \text{totally undefined function} & \end{cases}$$



Termination Resilience Static Analysis



Termination Resilience Static Analysis

Boolean Conditions

function $f(x)$ {

1 $a \leftarrow [-\infty, +\infty]$
 2 $z \leftarrow 10$
 3 if ($a^*a \geq 0$) then
 4 while ($z \geq 0$) do
 5 $z \leftarrow z - x$
 od⁶

else
 while ($z \geq x$) do

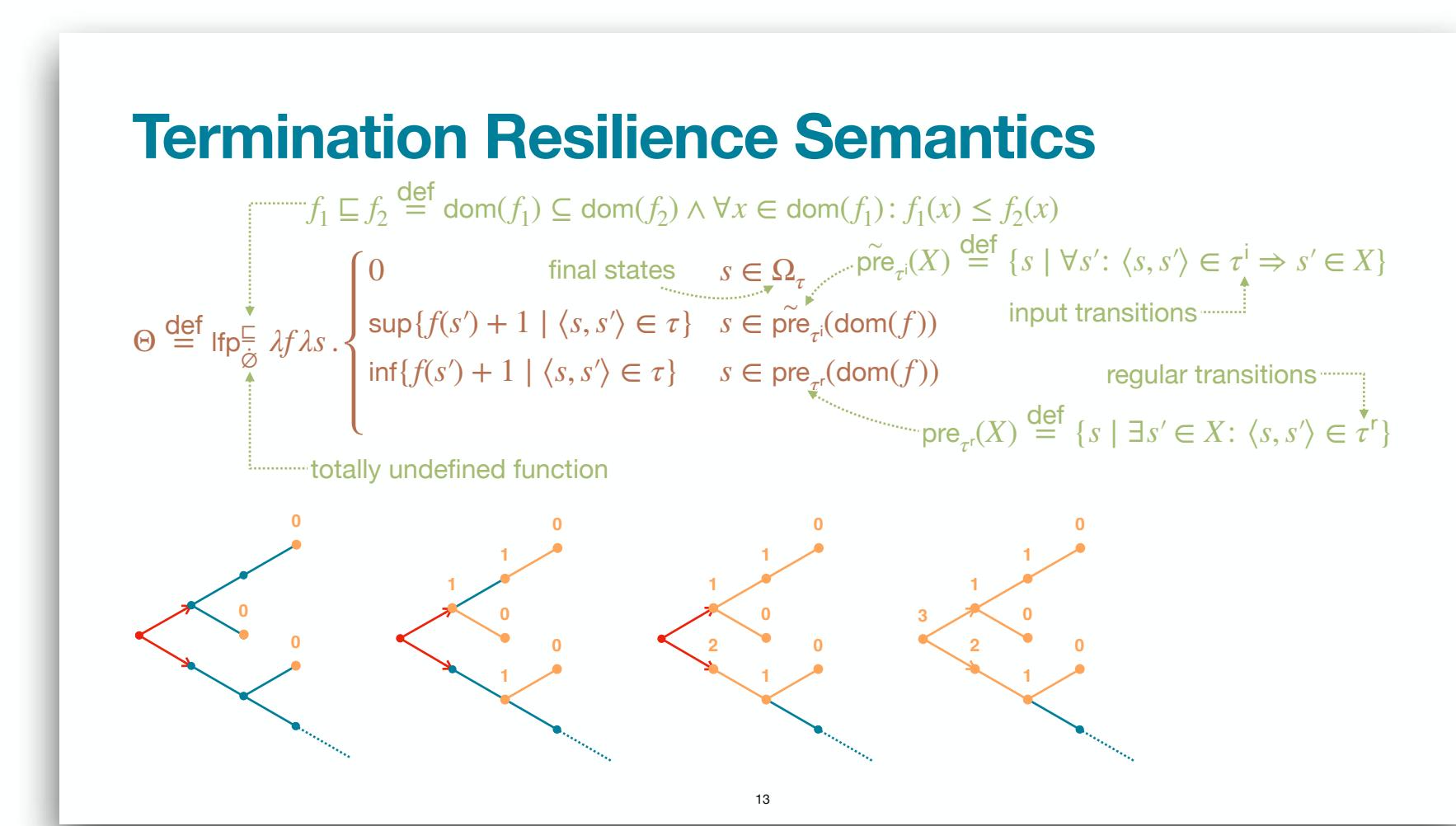
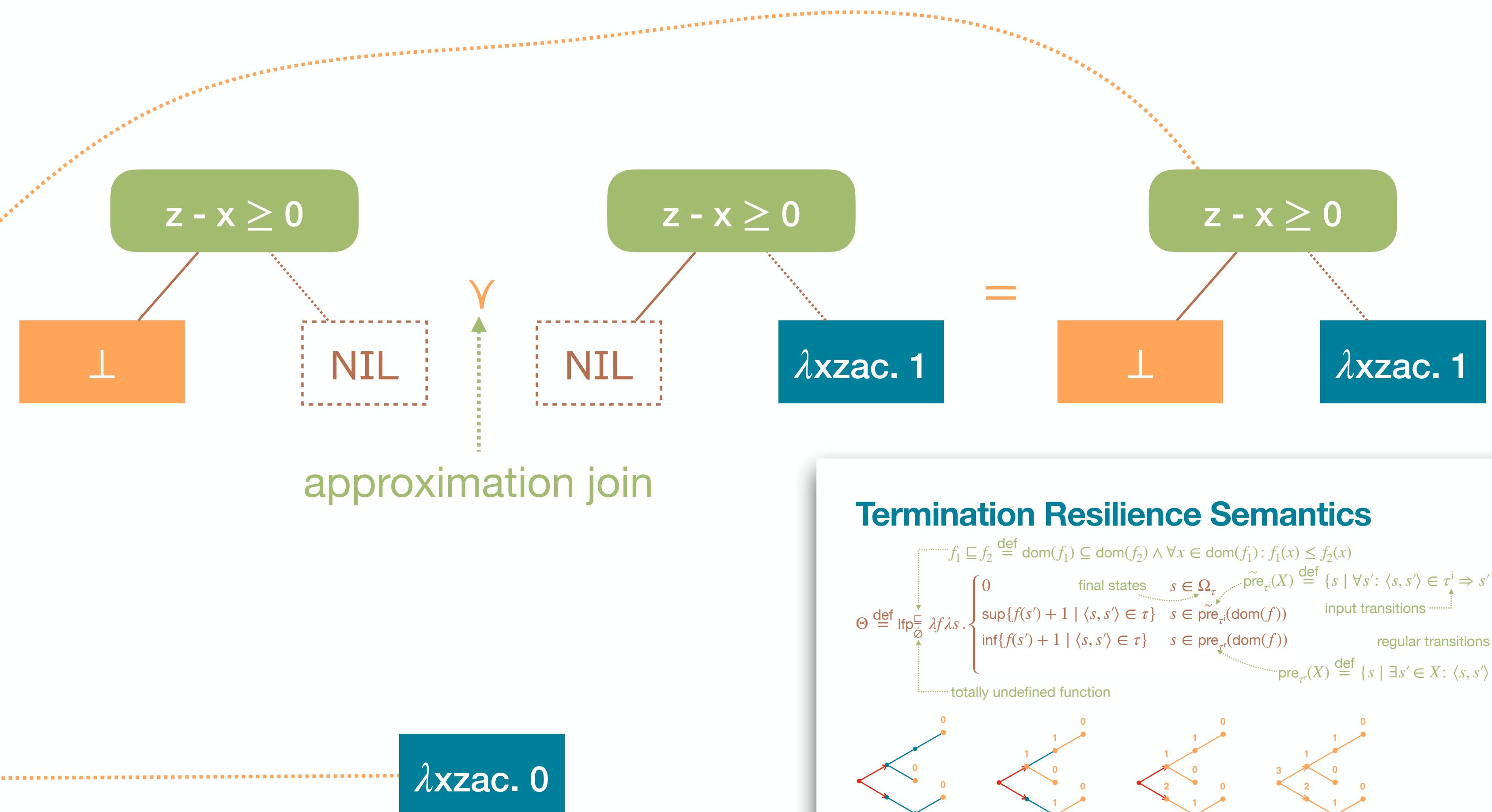
8 $c \leftarrow [-2, 1]$

9 $z \leftarrow z + c$

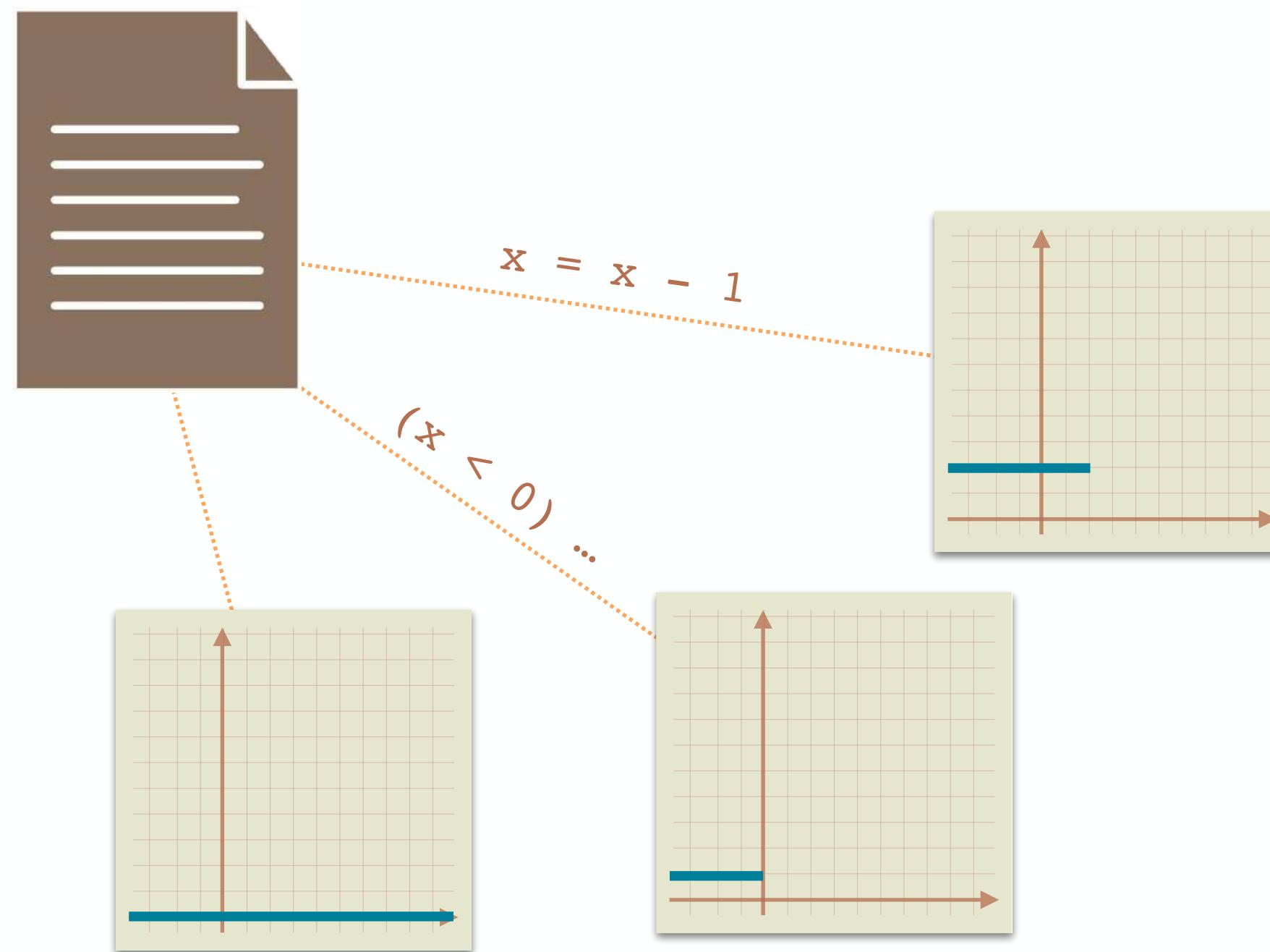
od¹⁰

fi

}¹¹



Termination Resilience Static Analysis



Termination Resilience Static Analysis

Variable Assignment

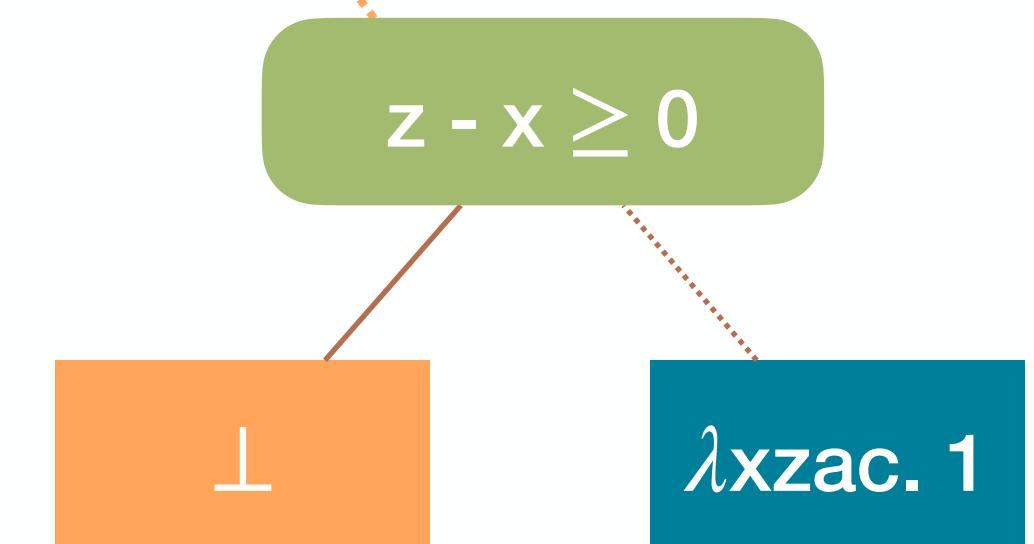
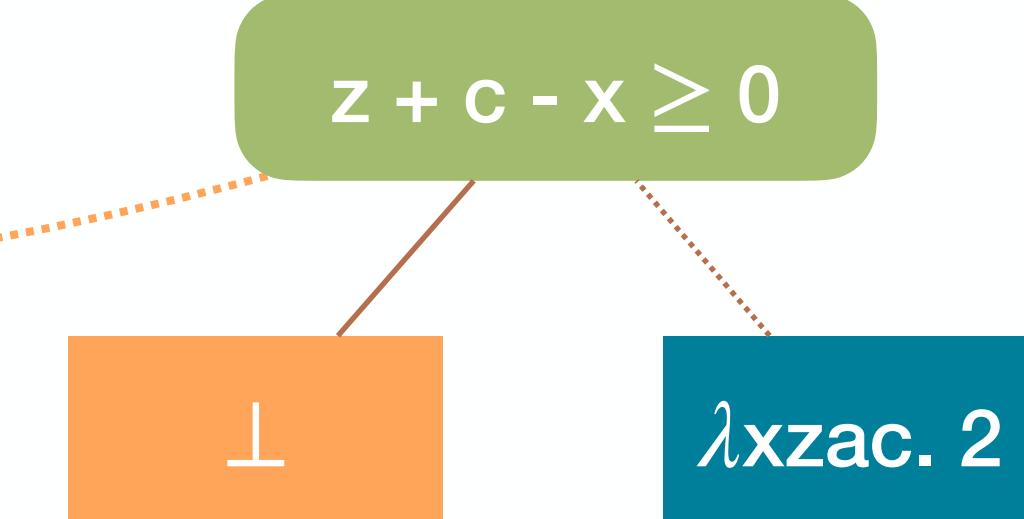
function $f(x)$ {

1 $a \leftarrow [-\infty, +\infty]$
 2 $z \leftarrow 10$
 3 if ($a^*a \geq 0$) then
 while 4 ($z \geq 0$) do
 5 $z \leftarrow z - x$
 od 6

else
 while 7 ($z \geq x$) do
 8 $c \leftarrow [-2, 1]$
 9 $z \leftarrow z + c$
 od 10

fi

} 11



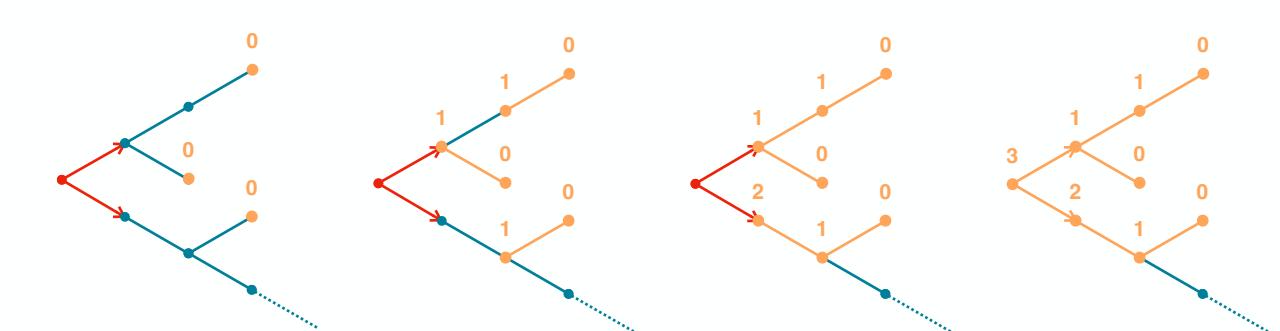
Termination Resilience Semantics

$$\Theta \stackrel{\text{def}}{=} \text{lfp}_{\subseteq \emptyset} \lambda f \lambda s . \begin{cases} 0 & \text{final states} \\ \sup\{f(s') + 1 \mid \langle s, s' \rangle \in \tau\} & s \in \tilde{\text{pre}}_{\tau}(X) \\ \inf\{f(s') + 1 \mid \langle s, s' \rangle \in \tau\} & s \in \text{pre}_{\tau}(X) \\ & \text{totally undefined function} \\ & s \in \Omega_{\tau} \\ & s \in \tilde{\text{pre}}_{\tau}(\text{dom}(f)) \\ & s \in \text{pre}_{\tau}(\text{dom}(f)) \end{cases}$$

$\tilde{\text{pre}}_{\tau}(X) \stackrel{\text{def}}{=} \{s \mid \forall s' : \langle s, s' \rangle \in \tau^i \Rightarrow s' \in X\}$

input transitions

$\text{regular transitions}$



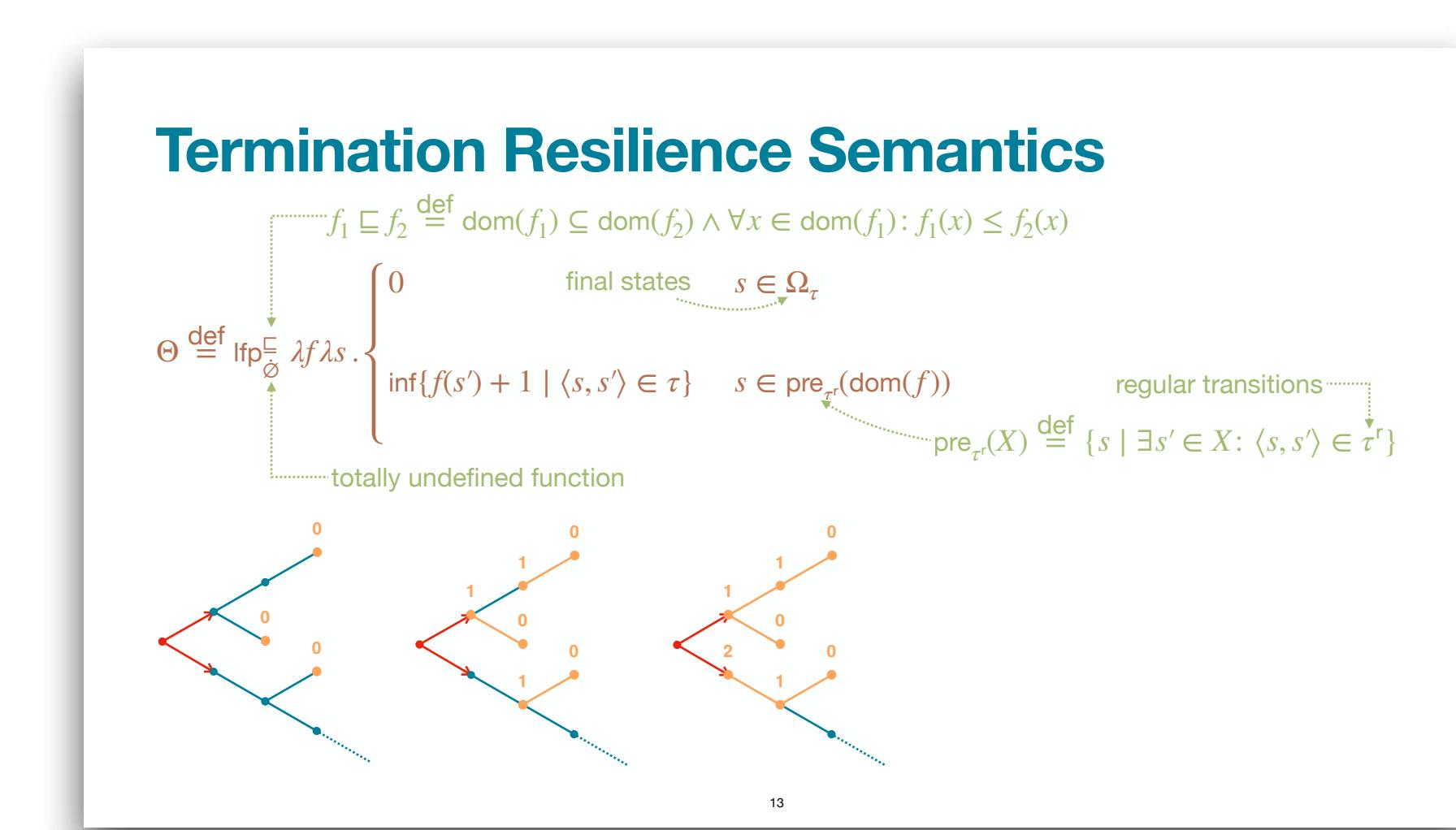
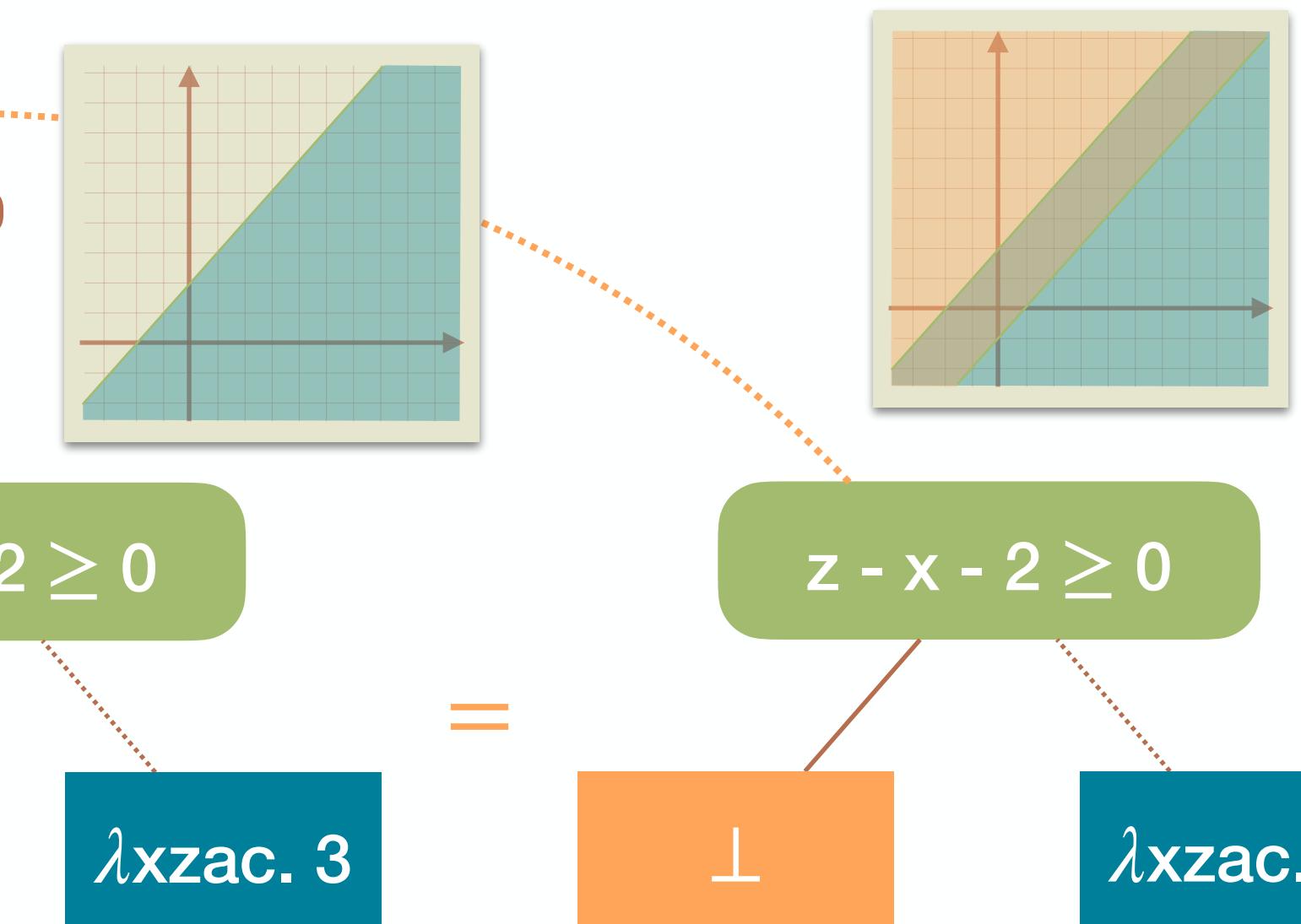
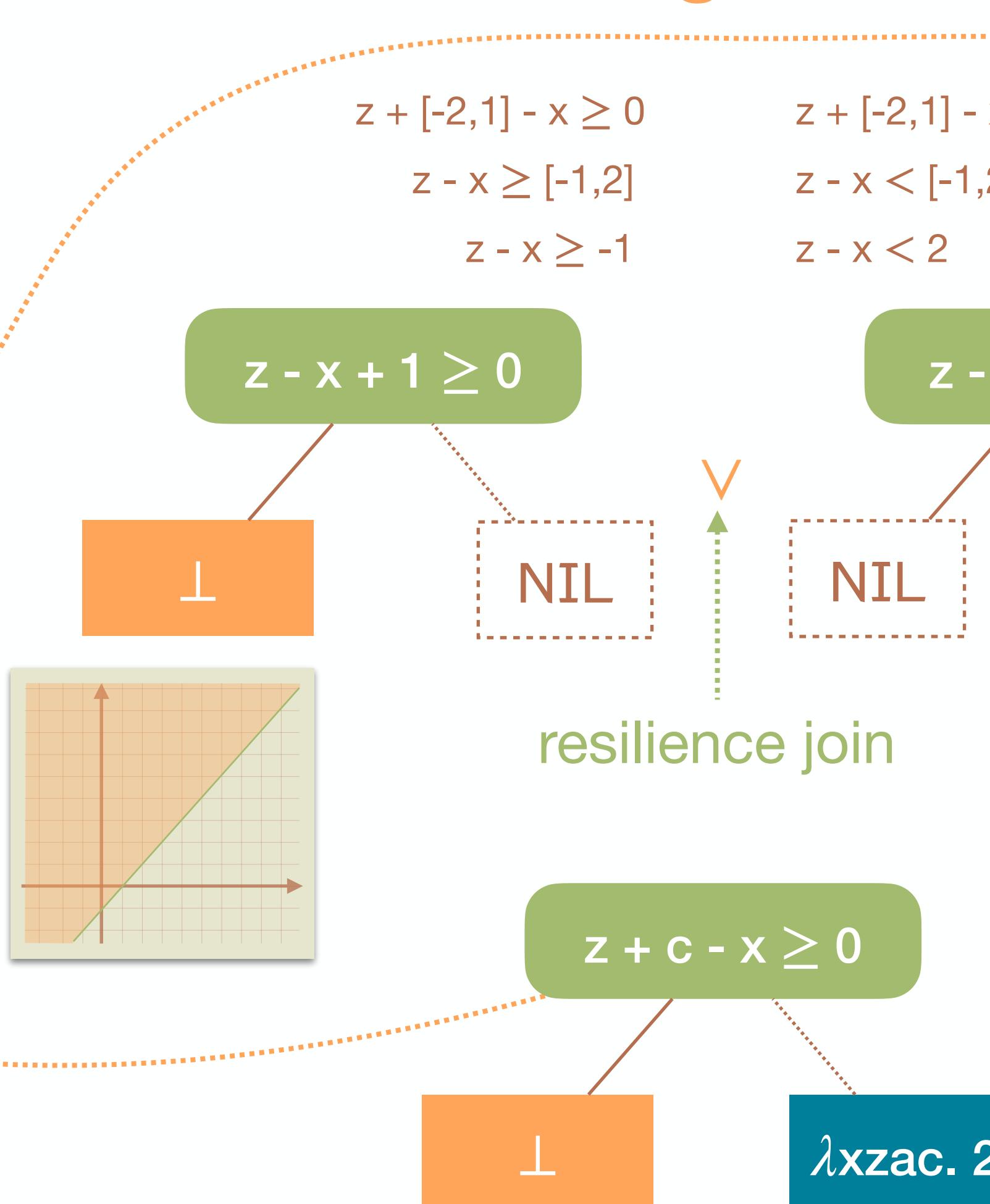
Termination Resilience Static Analysis

Non-Deterministic Variable Assignments

```

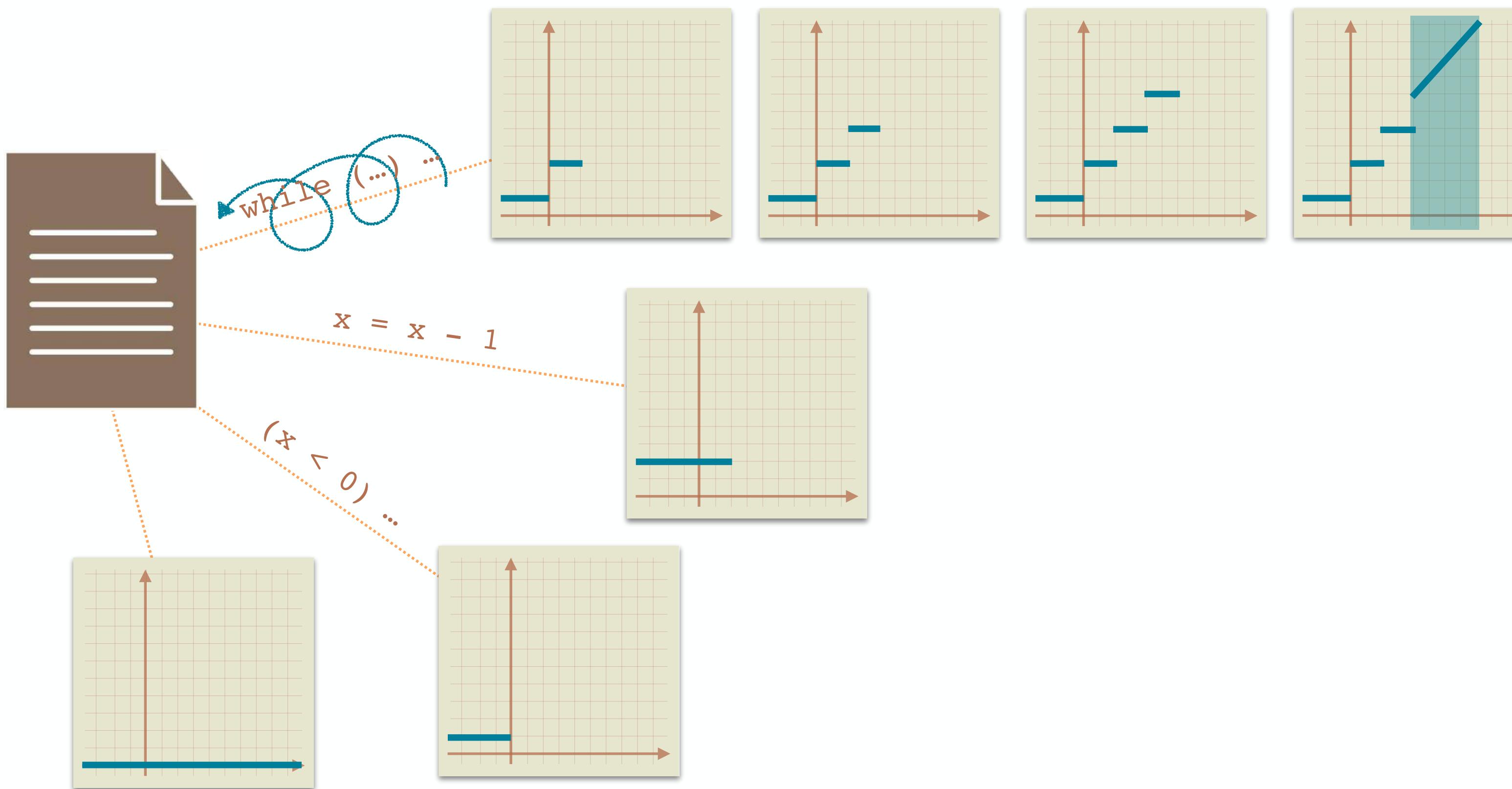
function f(x) {
    1 a  $\leftarrow [-\infty, +\infty]$ 
    2 z  $\leftarrow 10$ 
    3 if (a*a  $\geq 0$ ) then
        while 4(z  $\geq 0$ ) do
            5 z  $\leftarrow z - x$ 
        od6
    else
        while 7(z  $\geq x)$  do
            8 c  $\leftarrow [-2, 1]$ 
            9 z  $\leftarrow z + c$ 
        od10
    fi11
}

```



Termination Resilience Static Analysis

the analysis tries to **predict** a valid ranking function



Termination Resilience Static Analysis

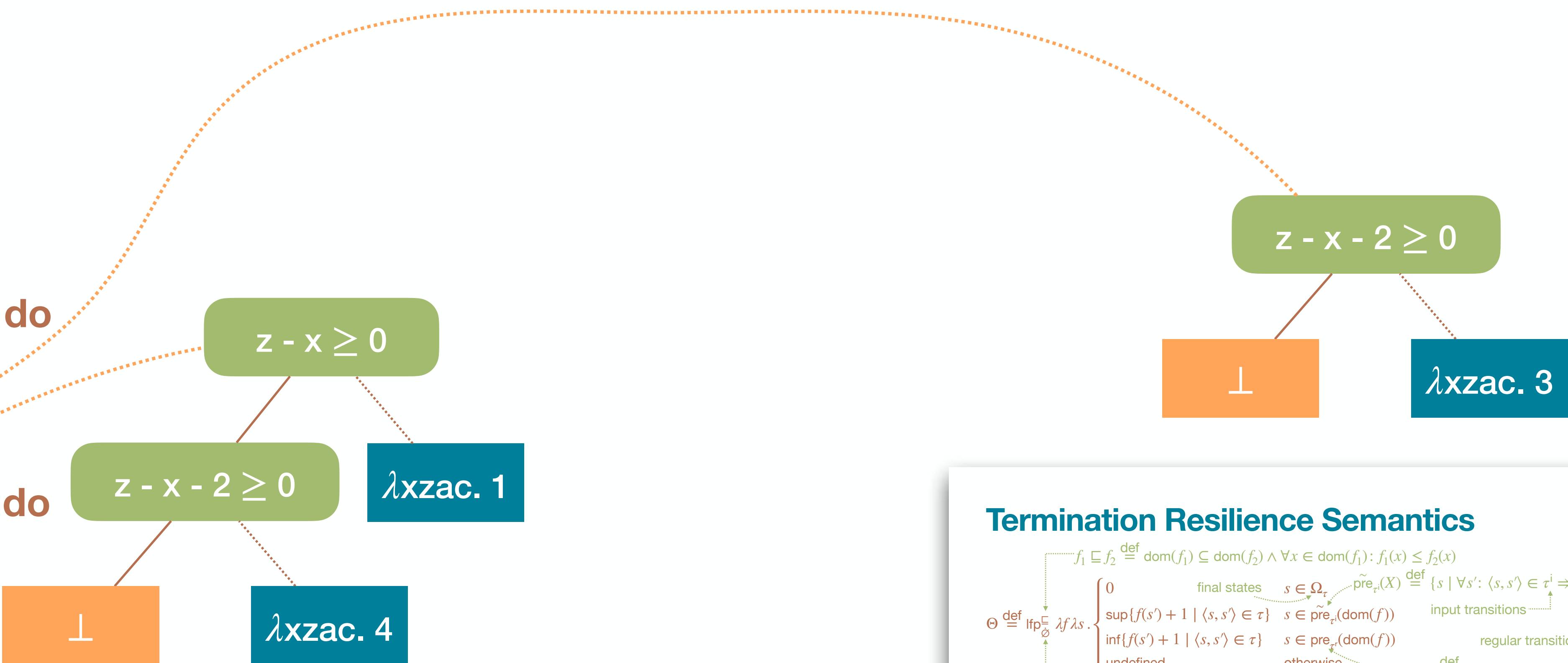
Loops

function f(x) {

```

1 a ← [-∞, +∞]
2 z ← 10
3 if (a*a ≥ 0) then
    while 4(z ≥ 0) do
        5z ← z - x
        od6
else
    while 7(z ≥ x) do
        8c ← [-2, 1]
        9z ← z + c
        od10
fi
}11

```



Termination Resilience Semantics

$$\Theta \stackrel{\text{def}}{=} \text{lfp}_{\sqsubseteq \emptyset} \lambda f \lambda s . \begin{cases} 0 & \text{final states} \\ \sup\{f(s') + 1 \mid \langle s, s' \rangle \in \tau\} & \\ \inf\{f(s') + 1 \mid \langle s, s' \rangle \in \tau\} & \\ \text{undefined} & \end{cases}$$

totally undefined function

$f_1 \sqsubseteq f_2 \stackrel{\text{def}}{=} \text{dom}(f_1) \subseteq \text{dom}(f_2) \wedge \forall x \in \text{dom}(f_1) : f_1(x) \leq f_2(x)$

$\tilde{\text{pre}}_{\tau}(X) \stackrel{\text{def}}{=} \{s \mid \forall s' : \langle s, s' \rangle \in \tau^i \Rightarrow s' \in X\}$

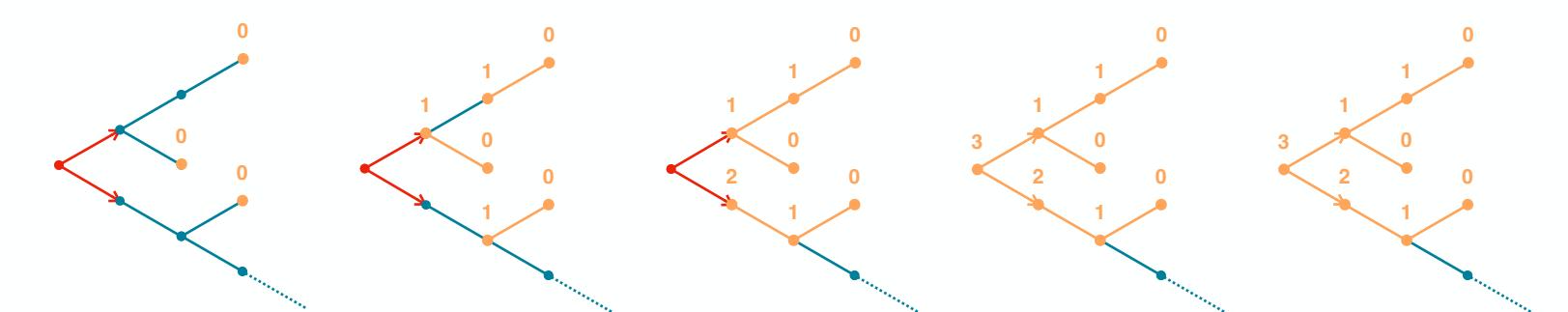
$s \in \Omega_{\tau}$

$s \in \tilde{\text{pre}}_{\tau}(\text{dom}(f))$

$s \in \text{pre}_{\tau}(\text{dom}(f))$

input transitions

$\text{regular transitions}$



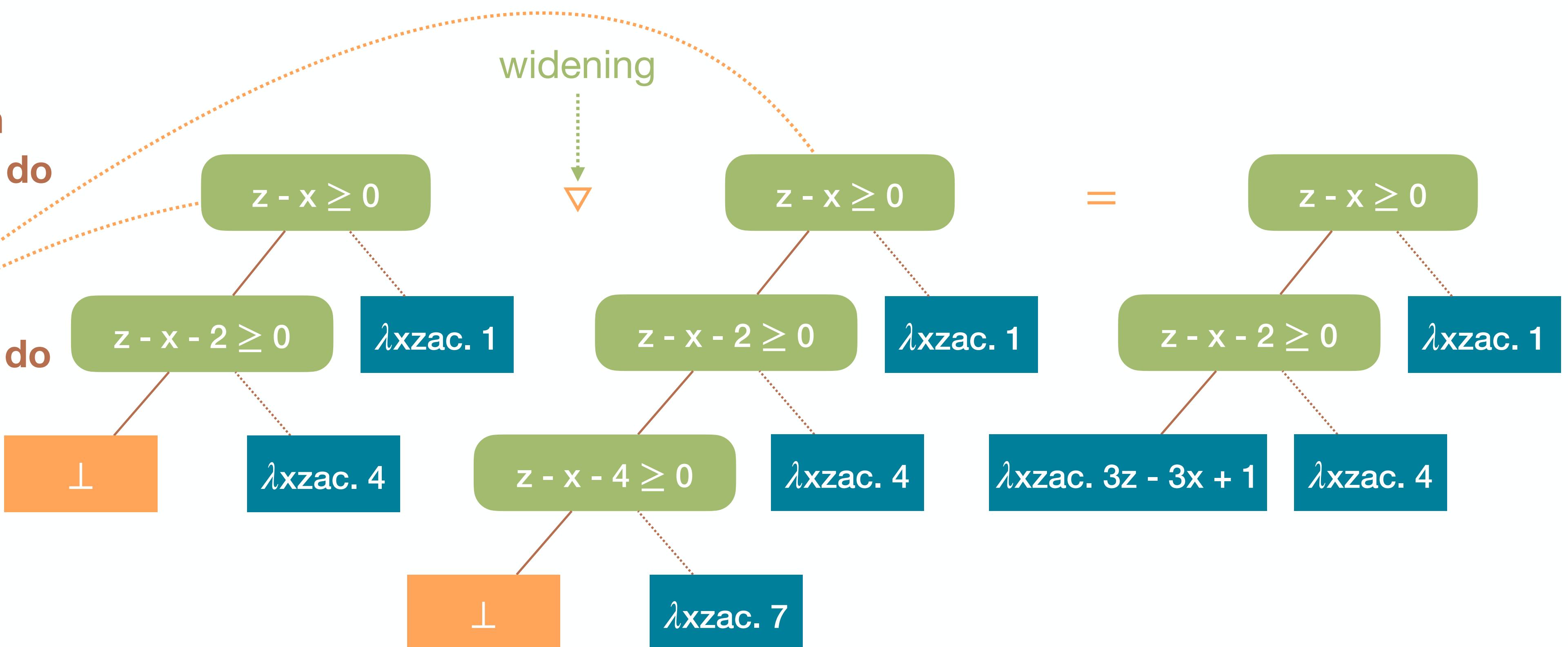
Termination Resilience Static Analysis

Loops

function f(x) {

```

1 a ← [-∞, +∞]
2 z ← 10
3 if (a*a ≥ 0) then
    while 4(z ≥ 0) do
        5 z ← z - x
        od6
    else
        while 7(z ≥ x) do
            8 c ← [-2, 1]
            9 z ← z + c
            od10
    fi
}
```



Termination Resilience Static Analysis

Loops

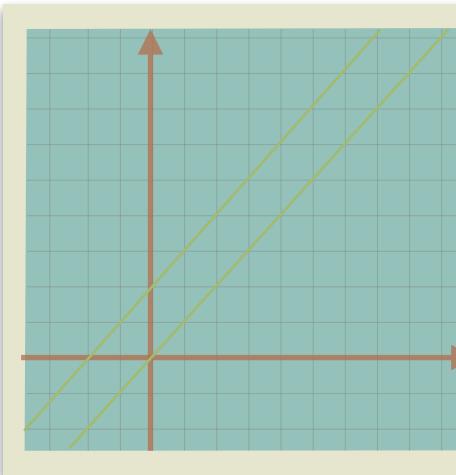
function $f(x)$ {

¹a $\leftarrow [-\infty, +\infty]$
²z $\leftarrow 10$
³if ($a^*a \geq 0$) then
 while ⁴($z \geq 0$) do
⁵ z $\leftarrow z - x$
⁶od

else
 while ⁷($z \geq x$) do
⁸ c $\leftarrow [-2, 1]$
⁹ z $\leftarrow z + c$
¹⁰od

fi

¹¹}

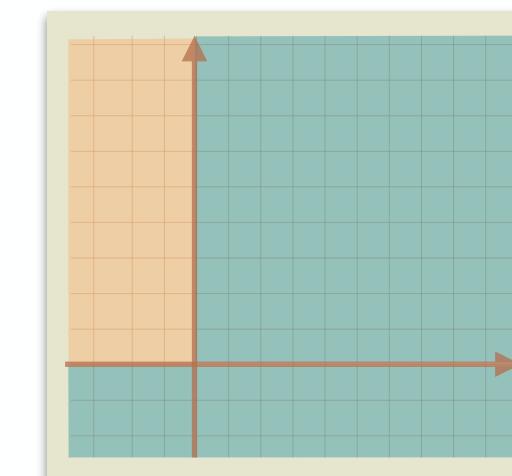


$z - x \geq 0$

$\lambda x z a c. 1$

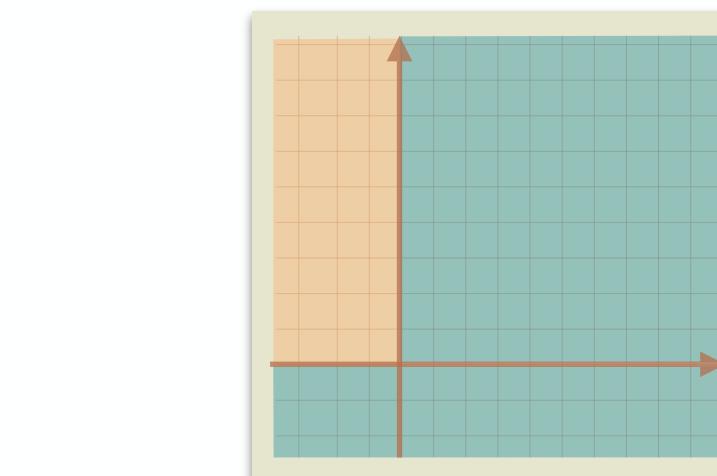
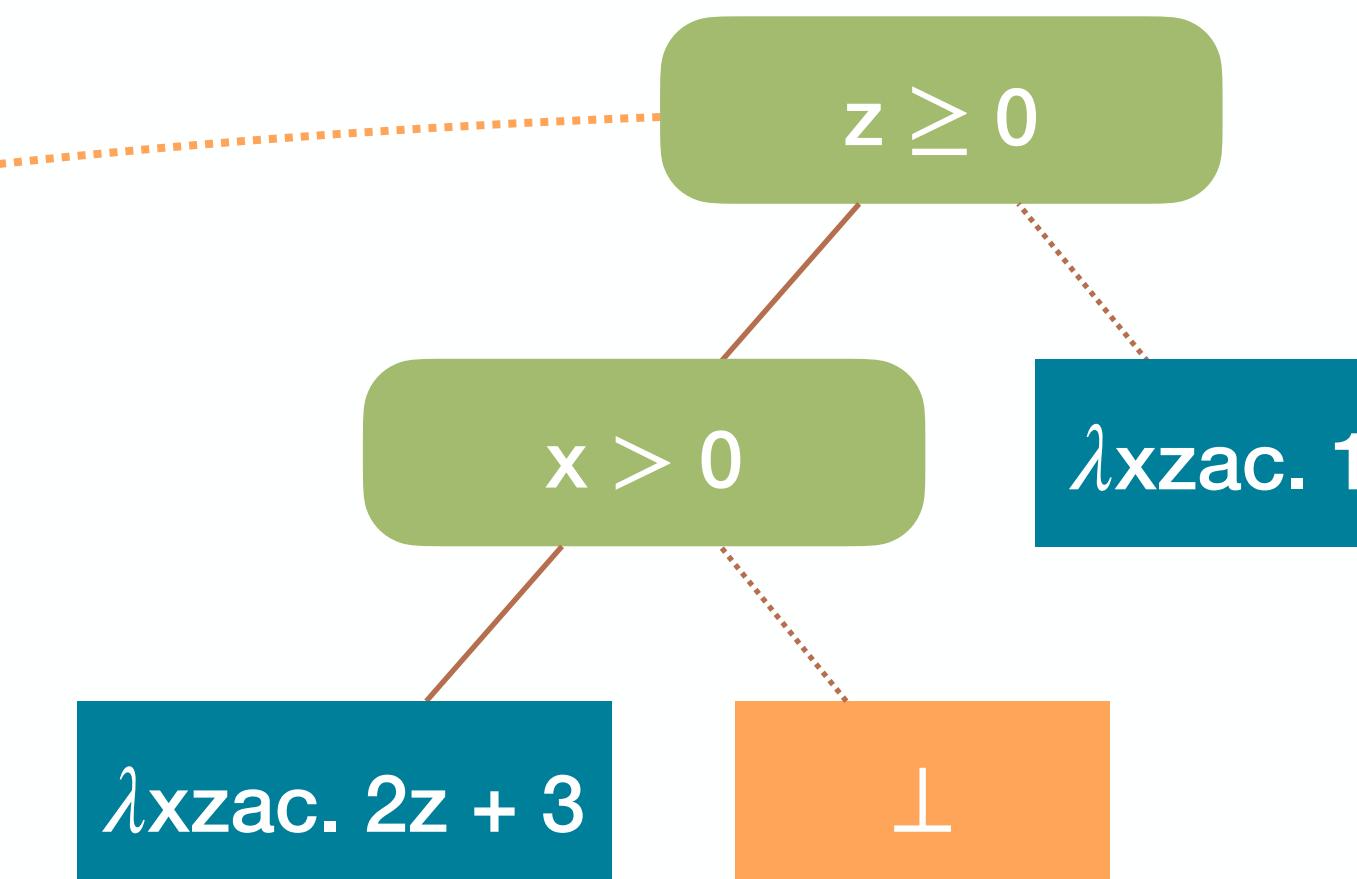
$\lambda x z a c. 4$

$z - x - 2 \geq 0$



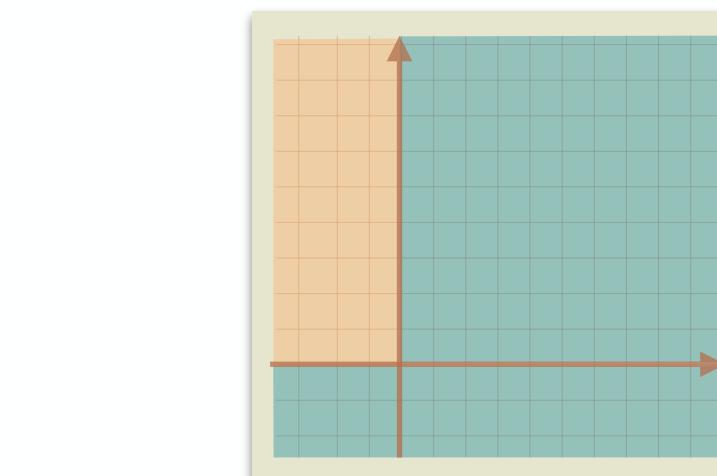
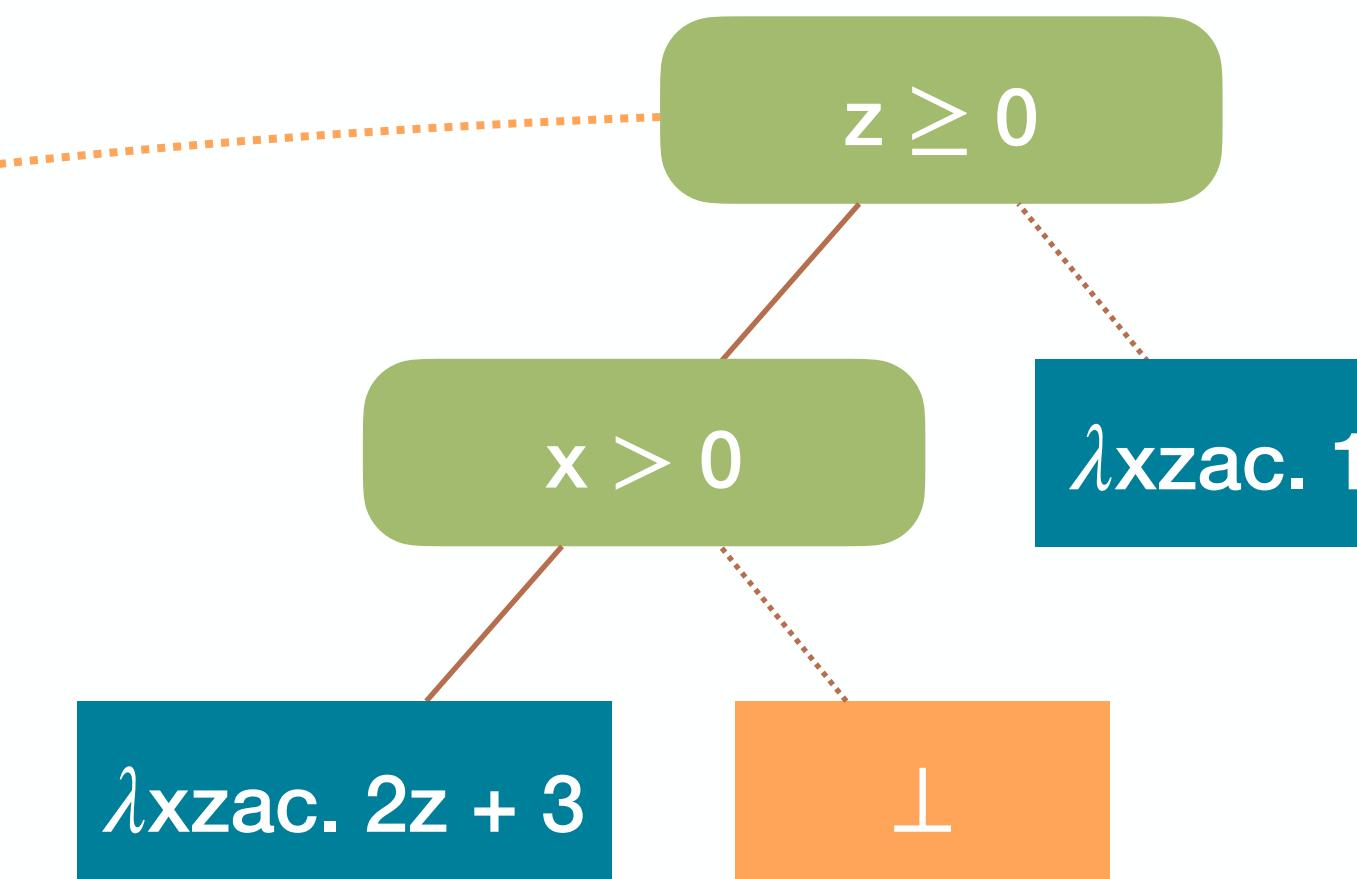
$\lambda x z a c. 2z + 3$

\perp



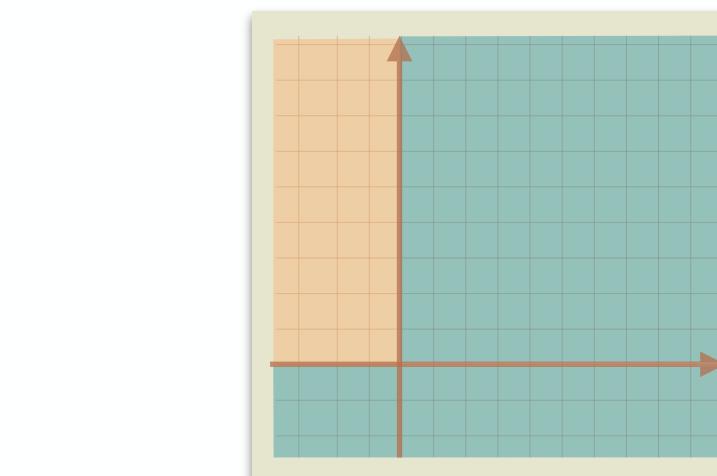
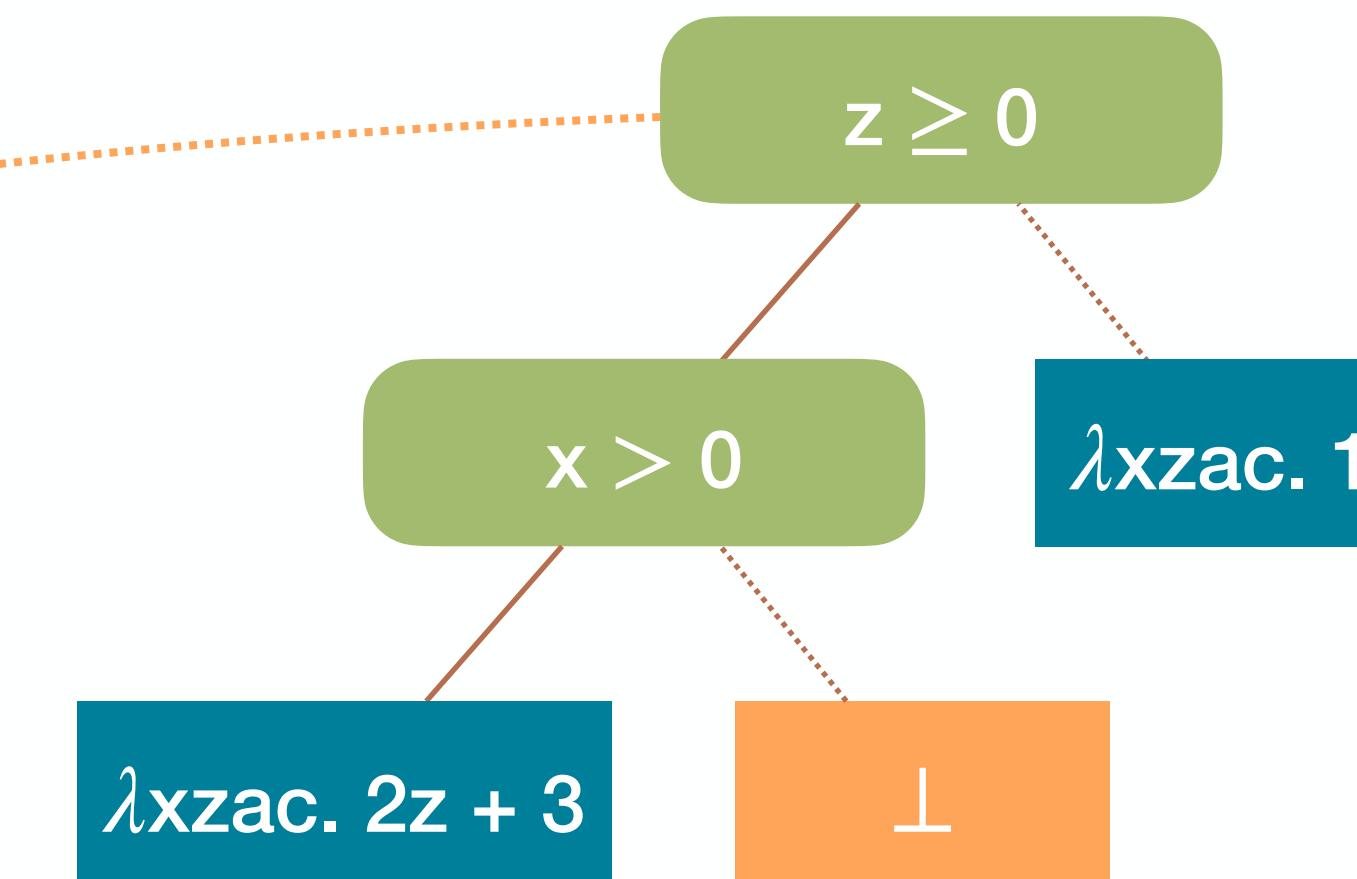
$\lambda x z a c. 2z + 3$

\perp



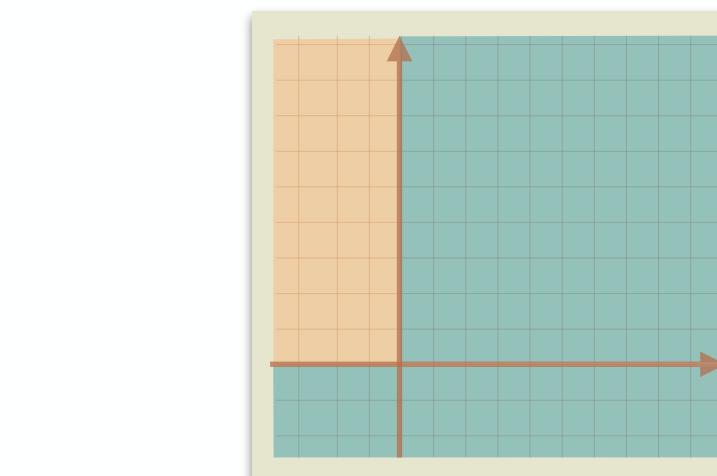
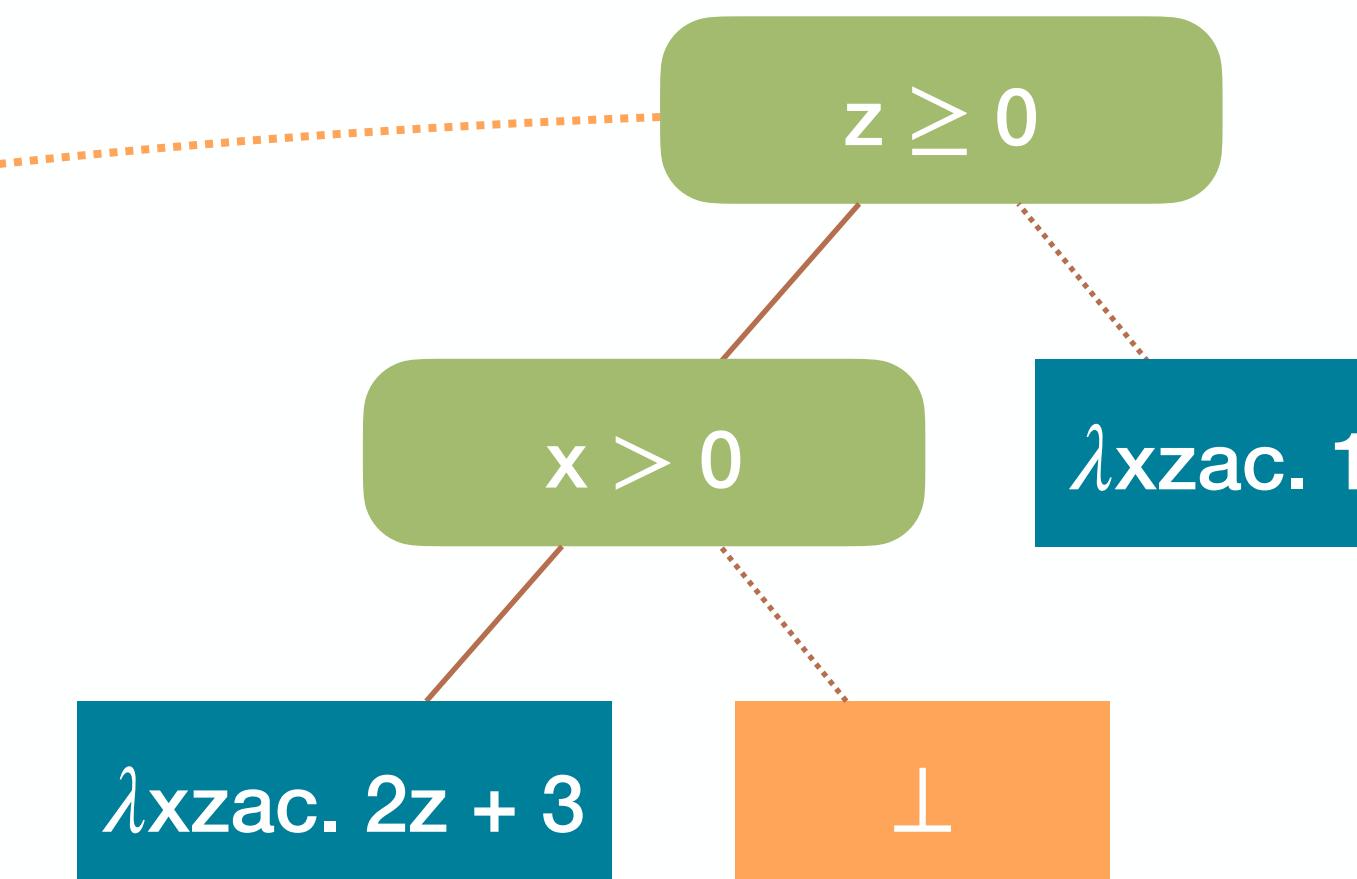
$\lambda x z a c. 2z + 3$

\perp



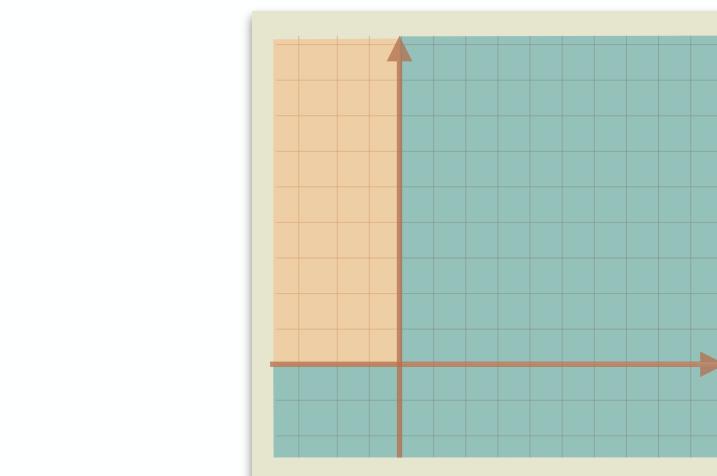
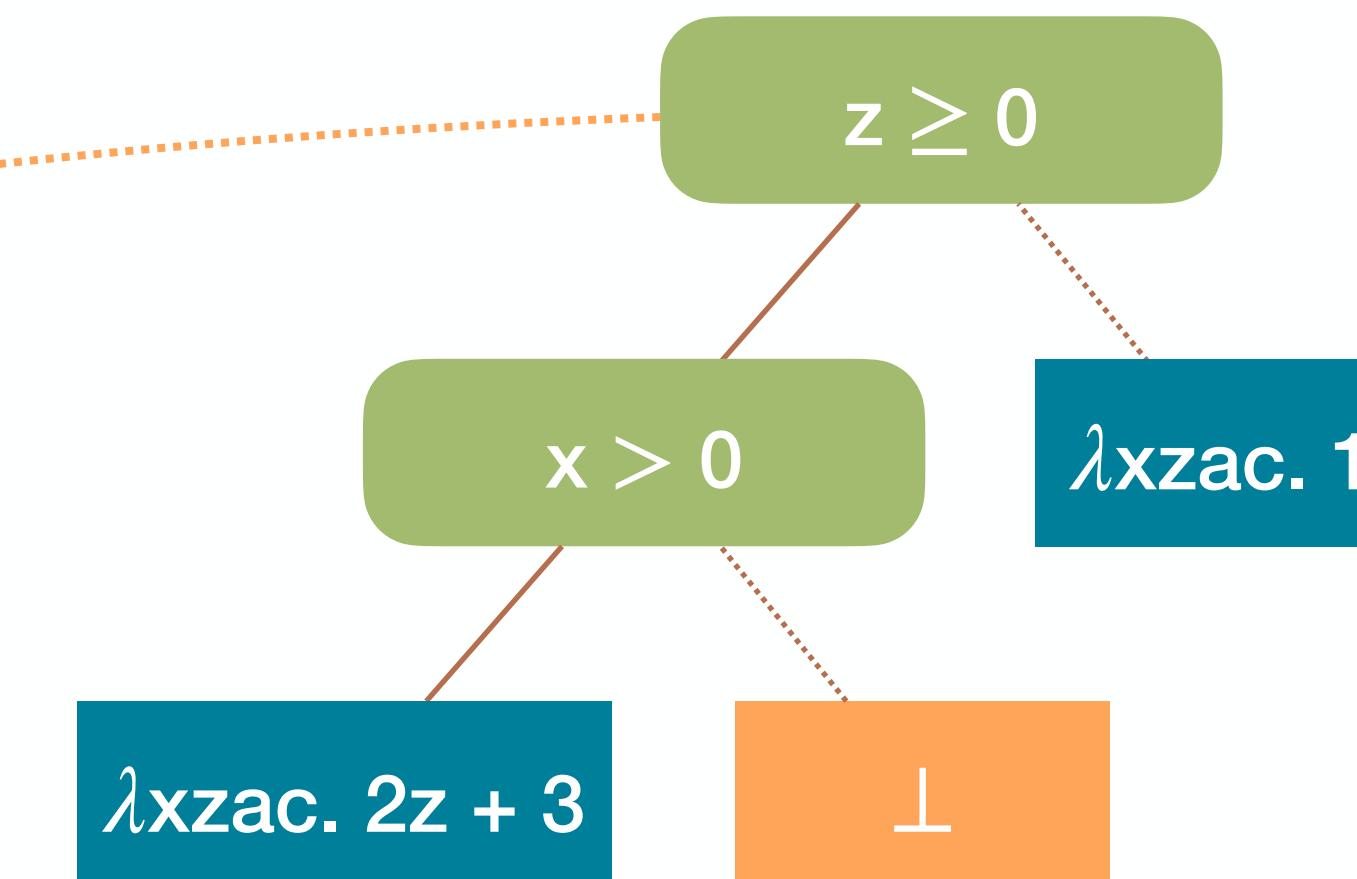
$\lambda x z a c. 2z + 3$

\perp



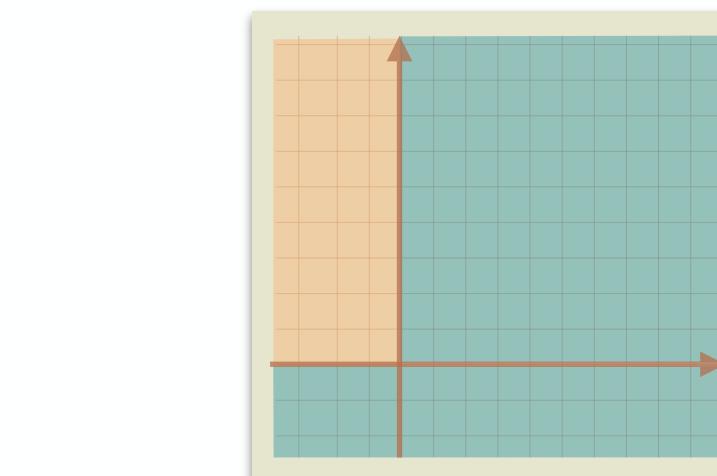
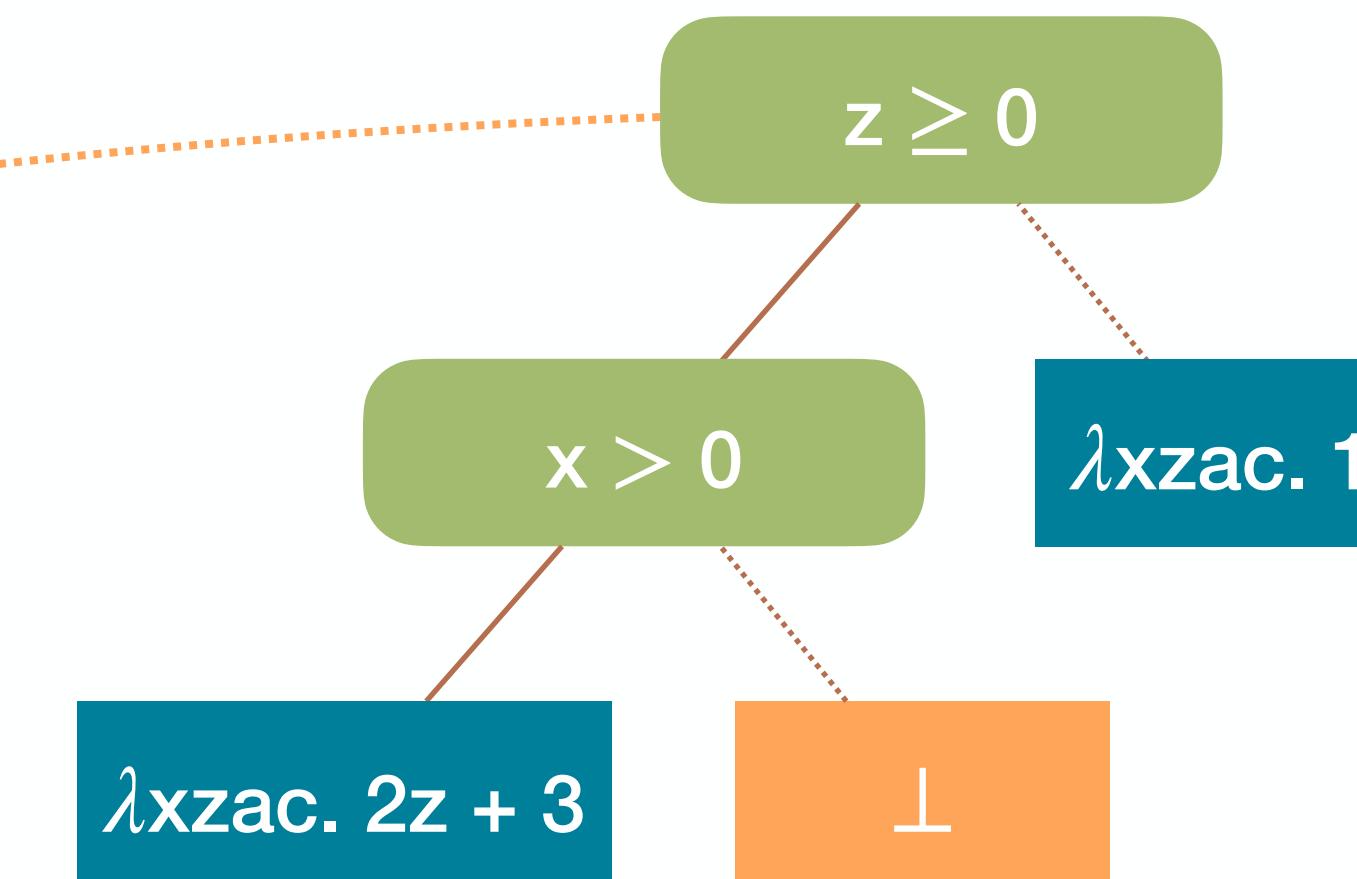
$\lambda x z a c. 2z + 3$

\perp



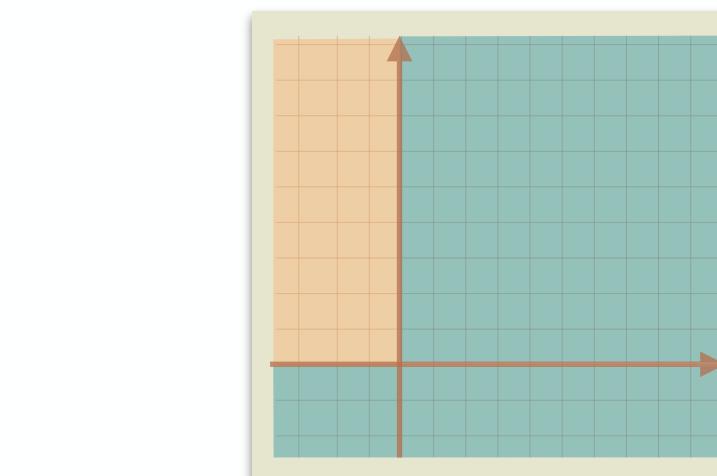
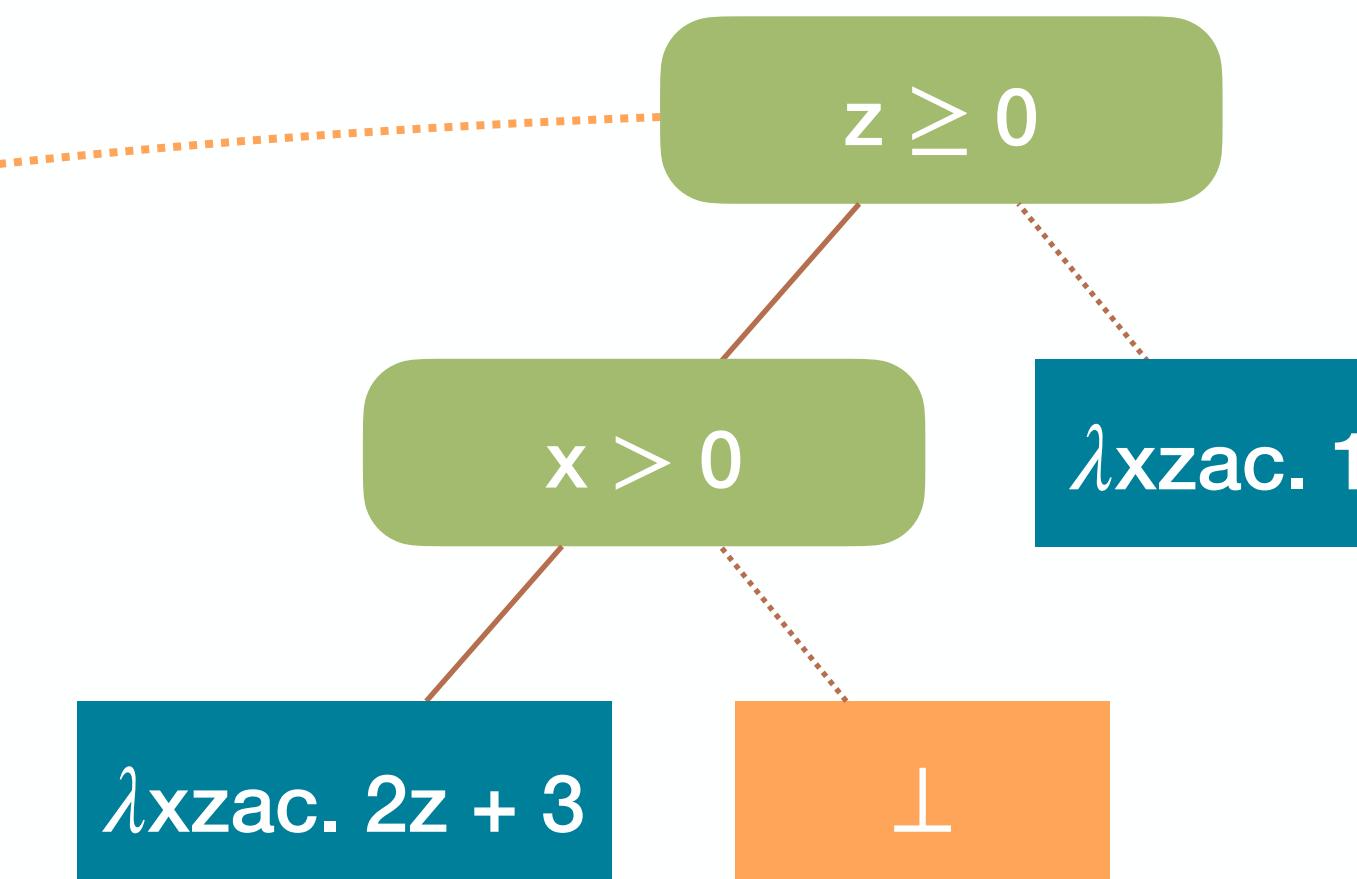
$\lambda x z a c. 2z + 3$

\perp



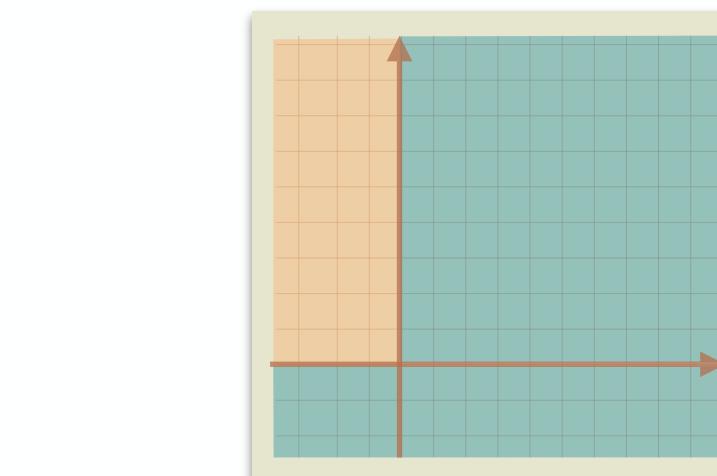
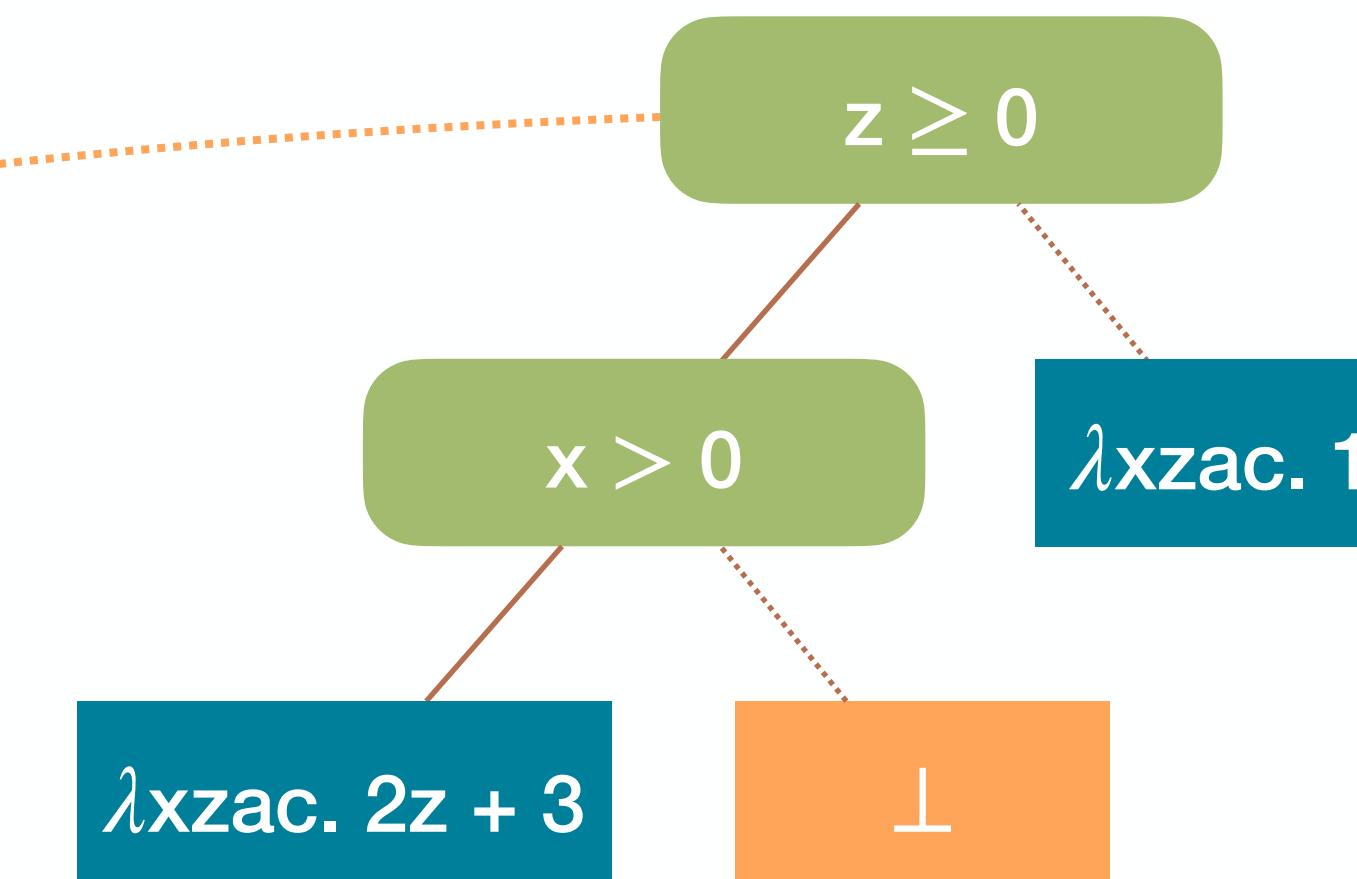
$\lambda x z a c. 2z + 3$

\perp



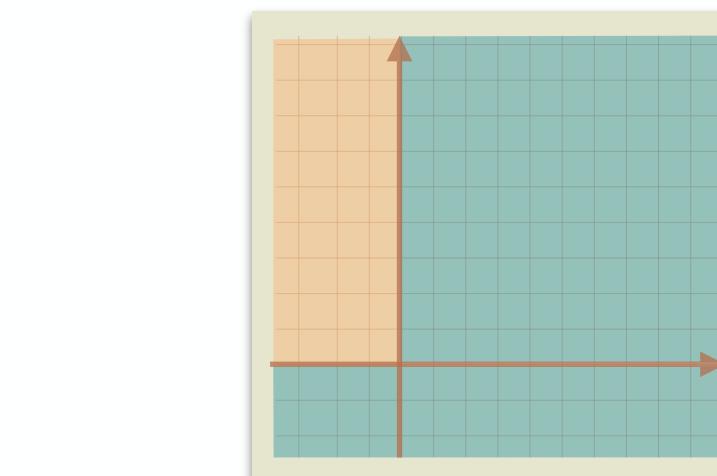
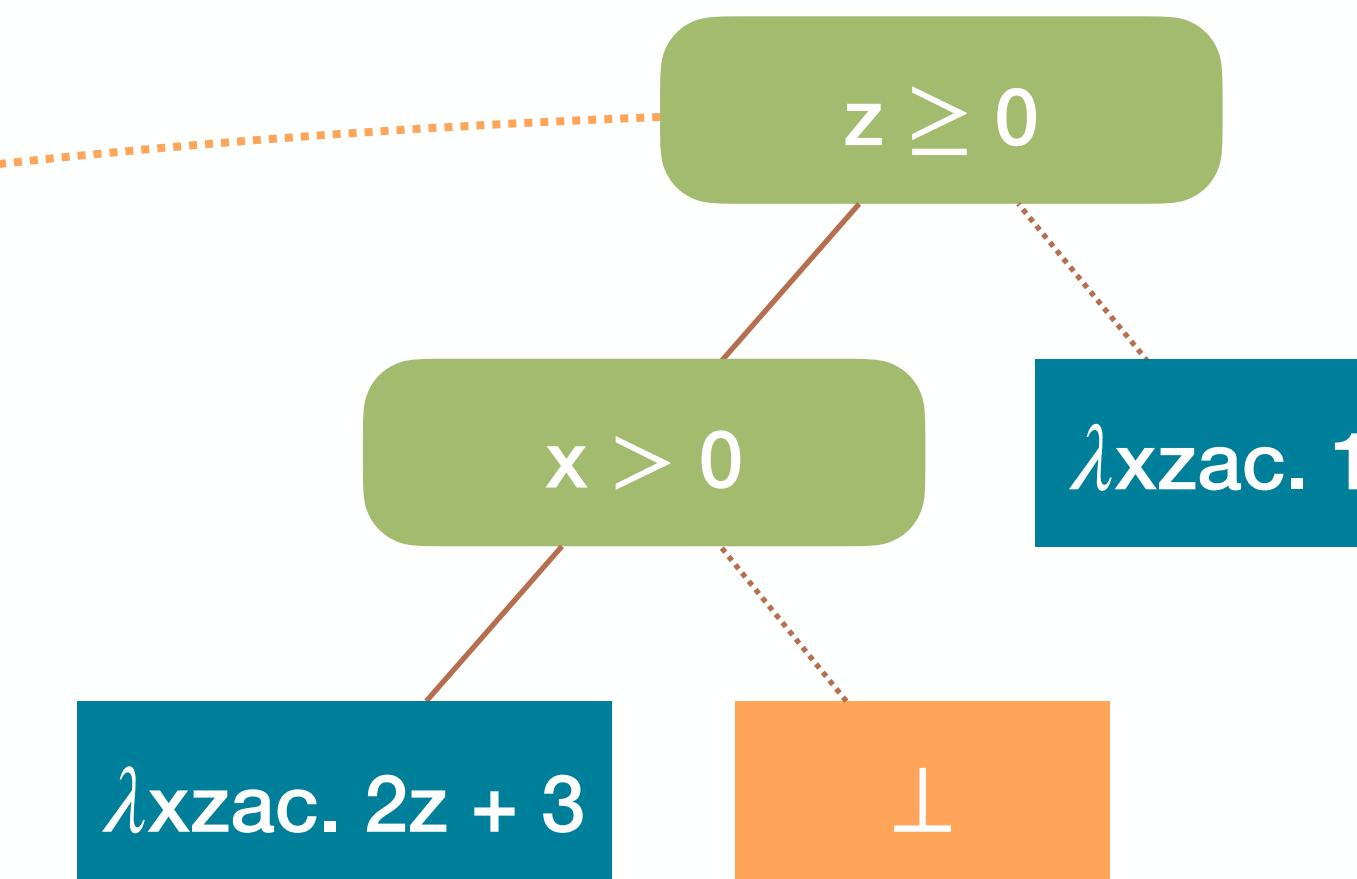
$\lambda x z a c. 2z + 3$

\perp



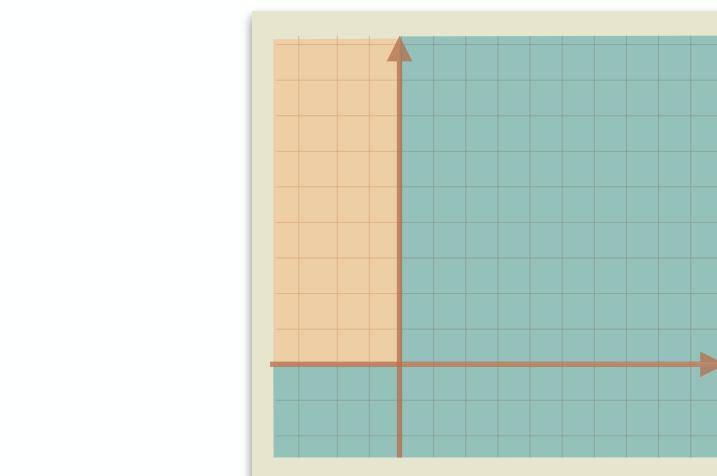
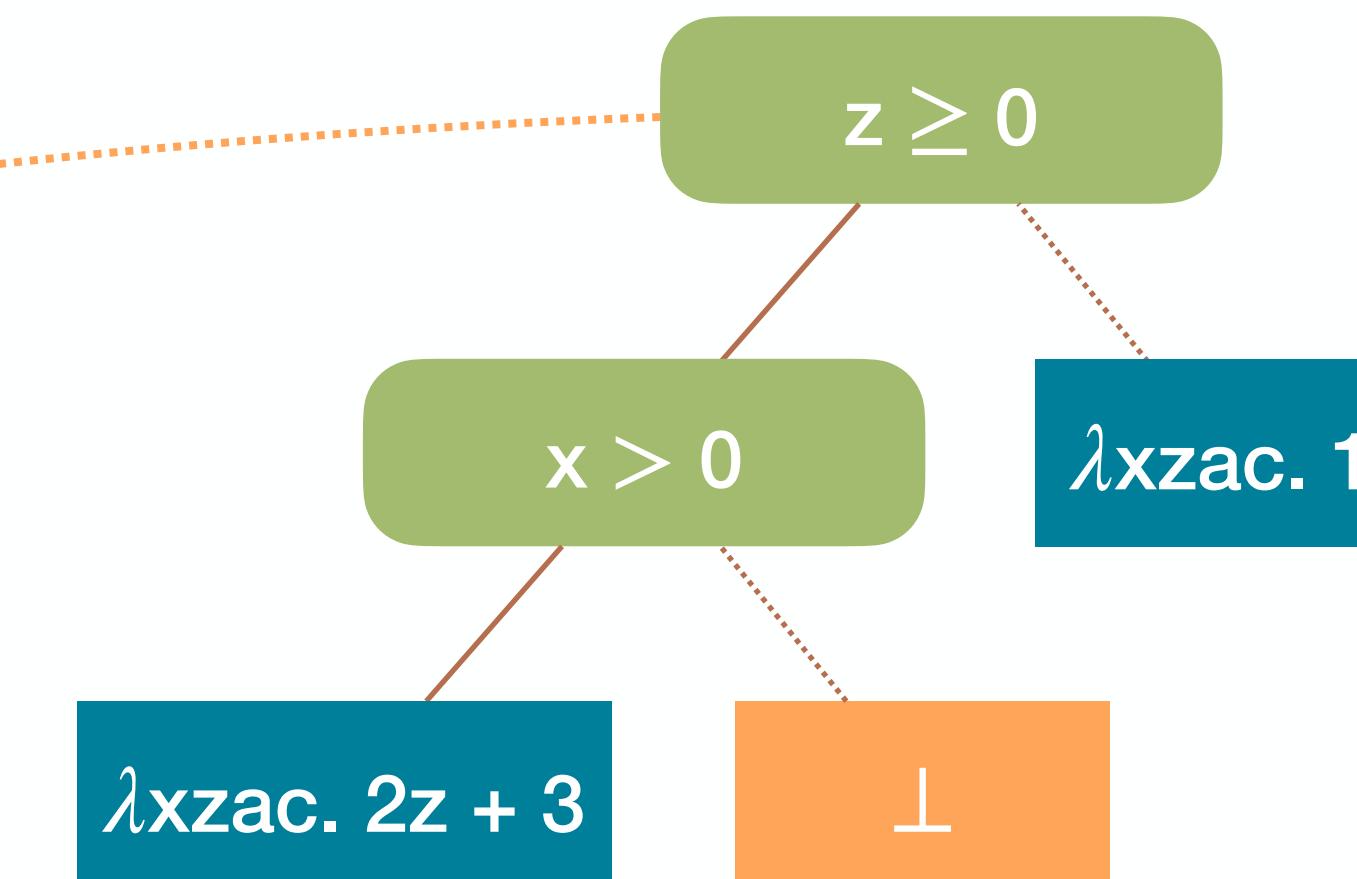
$\lambda x z a c. 2z + 3$

\perp



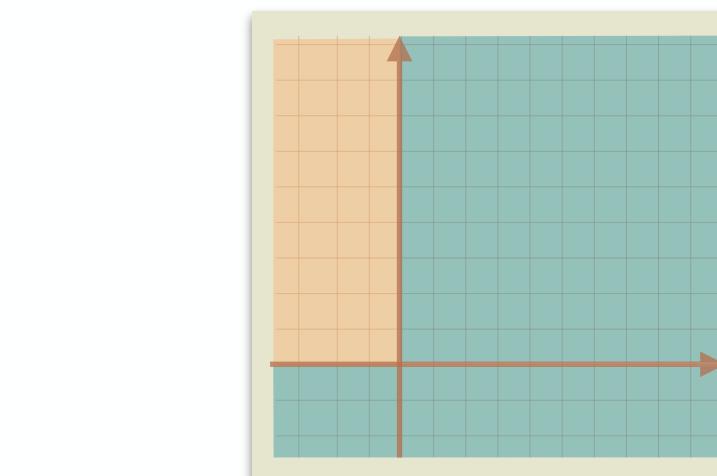
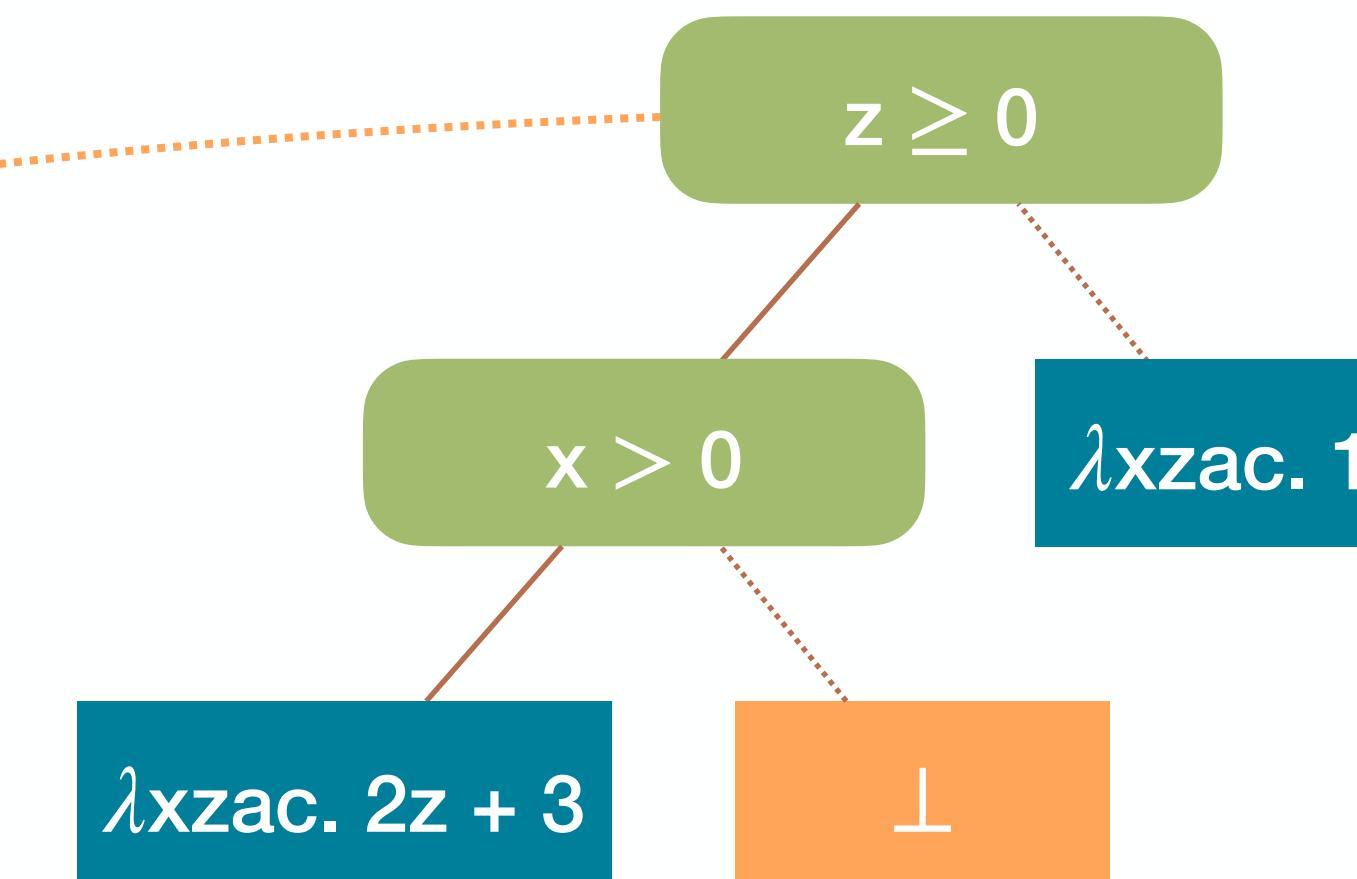
$\lambda x z a c. 2z + 3$

\perp



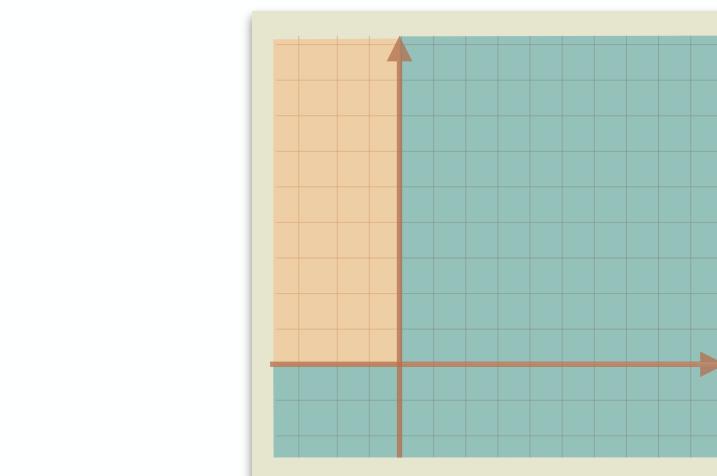
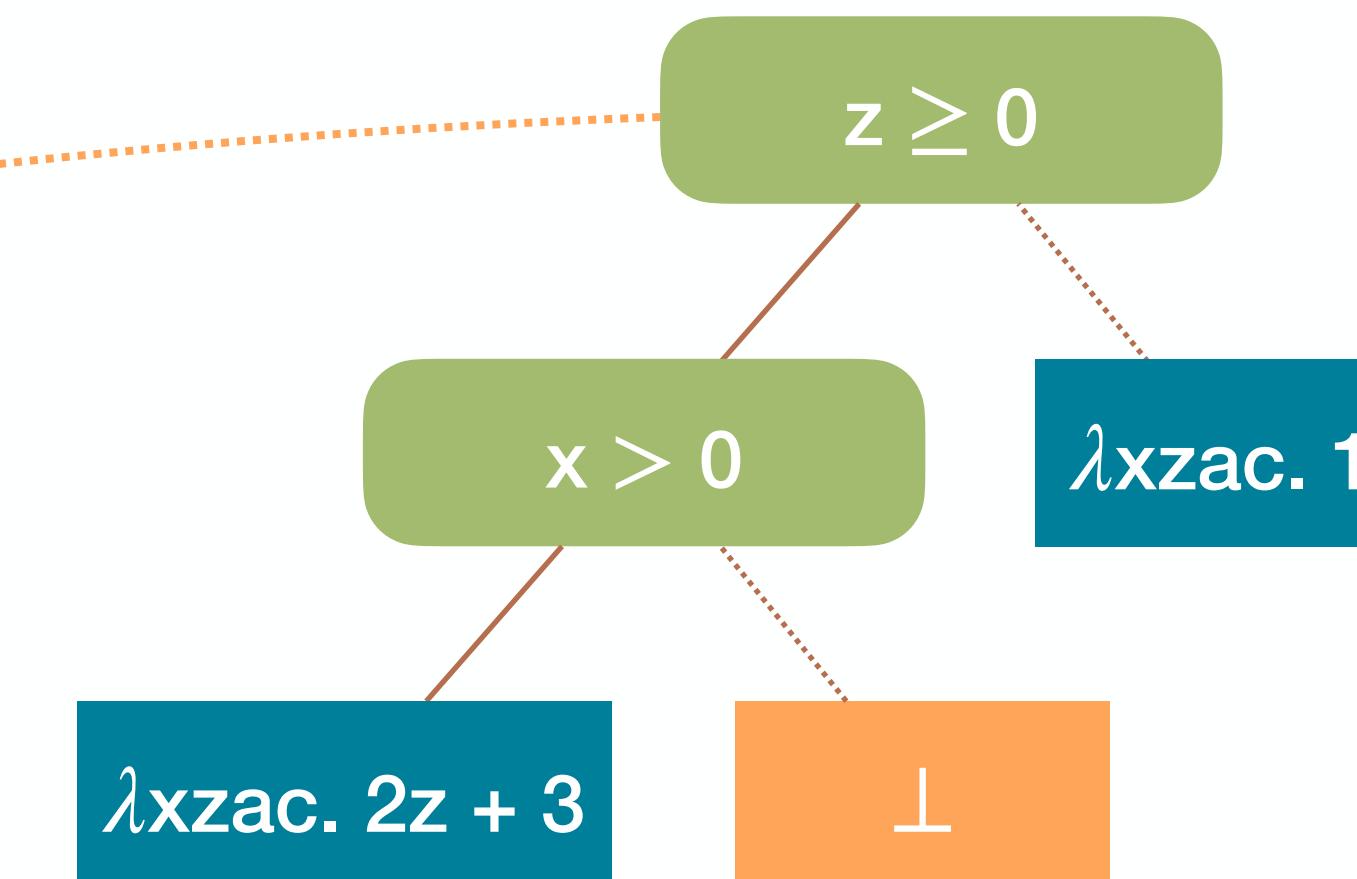
$\lambda x z a c. 2z + 3$

\perp



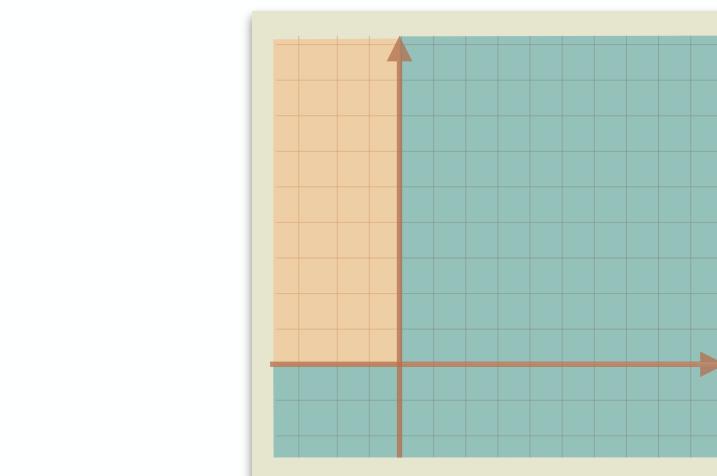
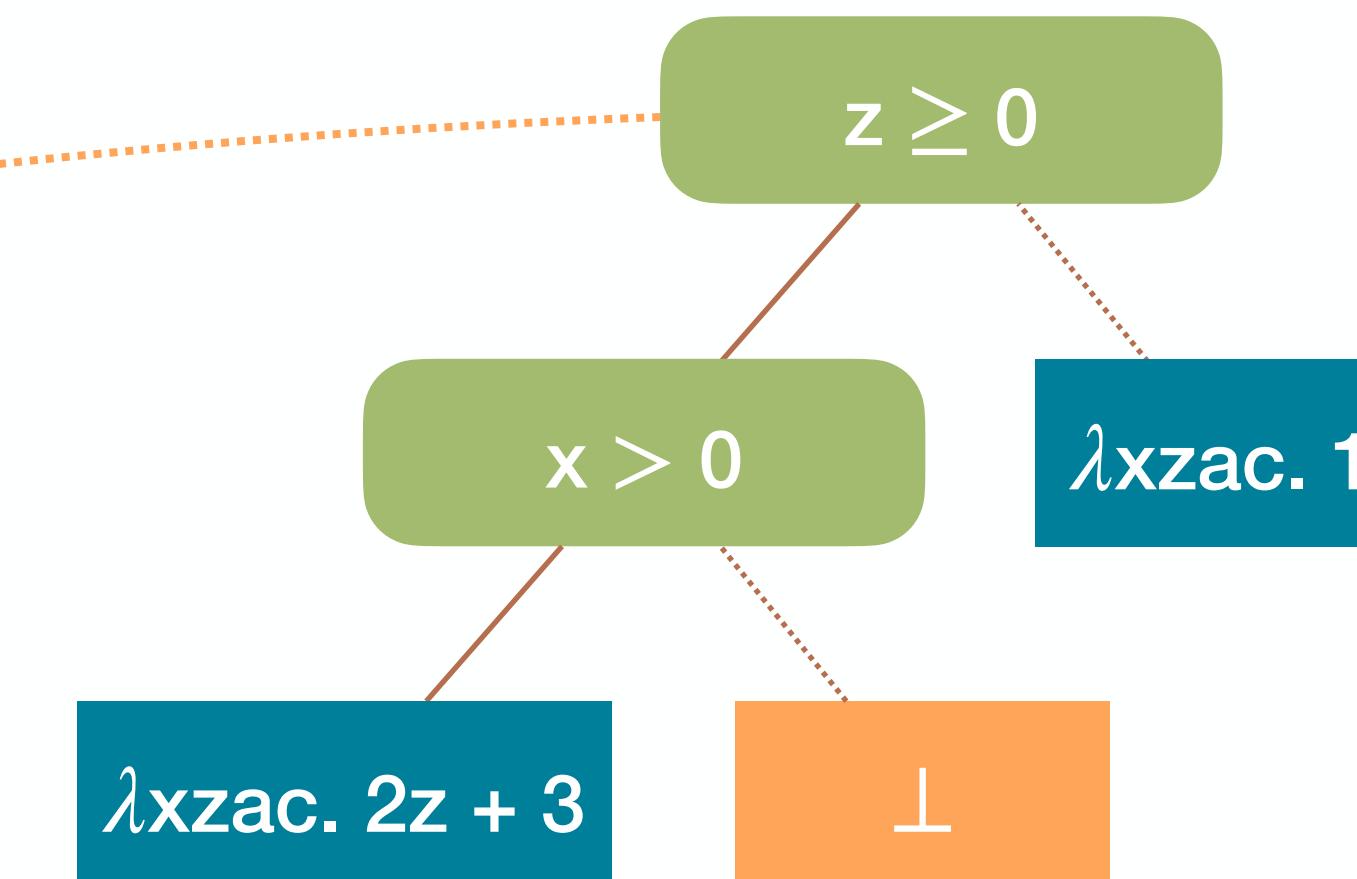
$\lambda x z a c. 2z + 3$

\perp



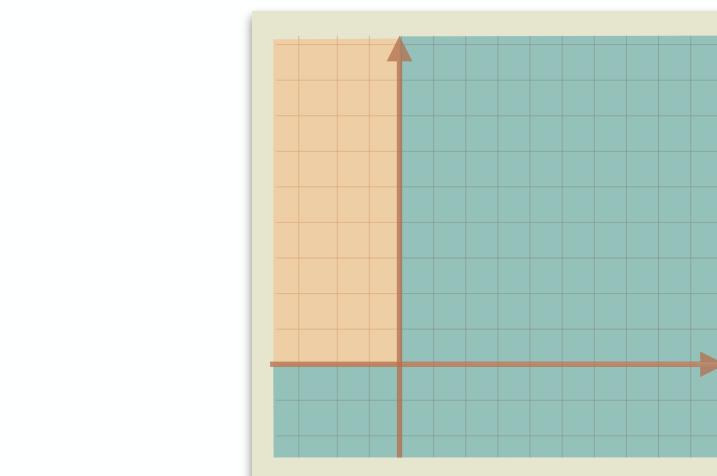
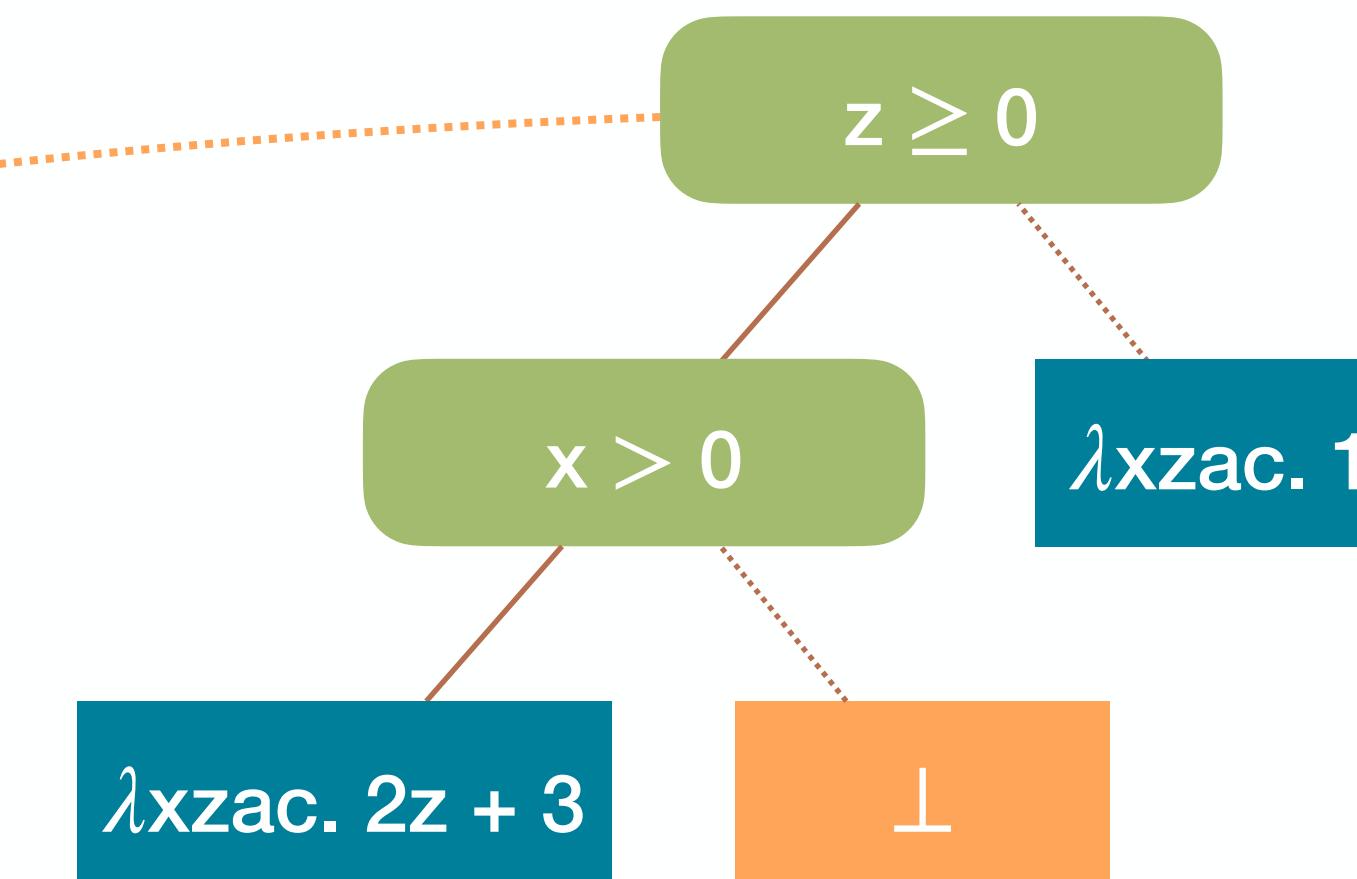
$\lambda x z a c. 2z + 3$

\perp



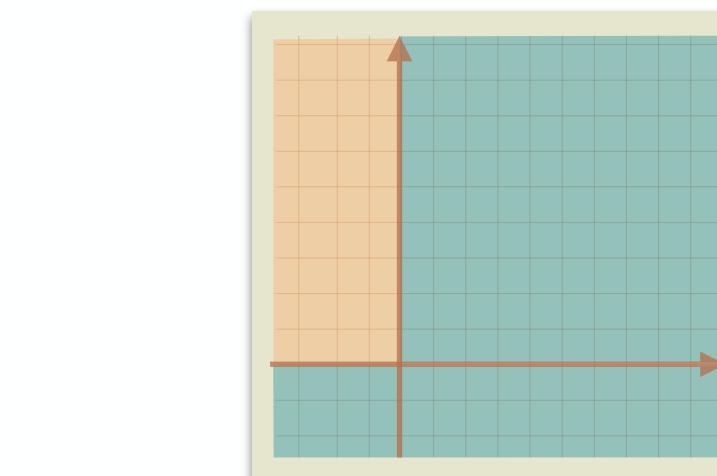
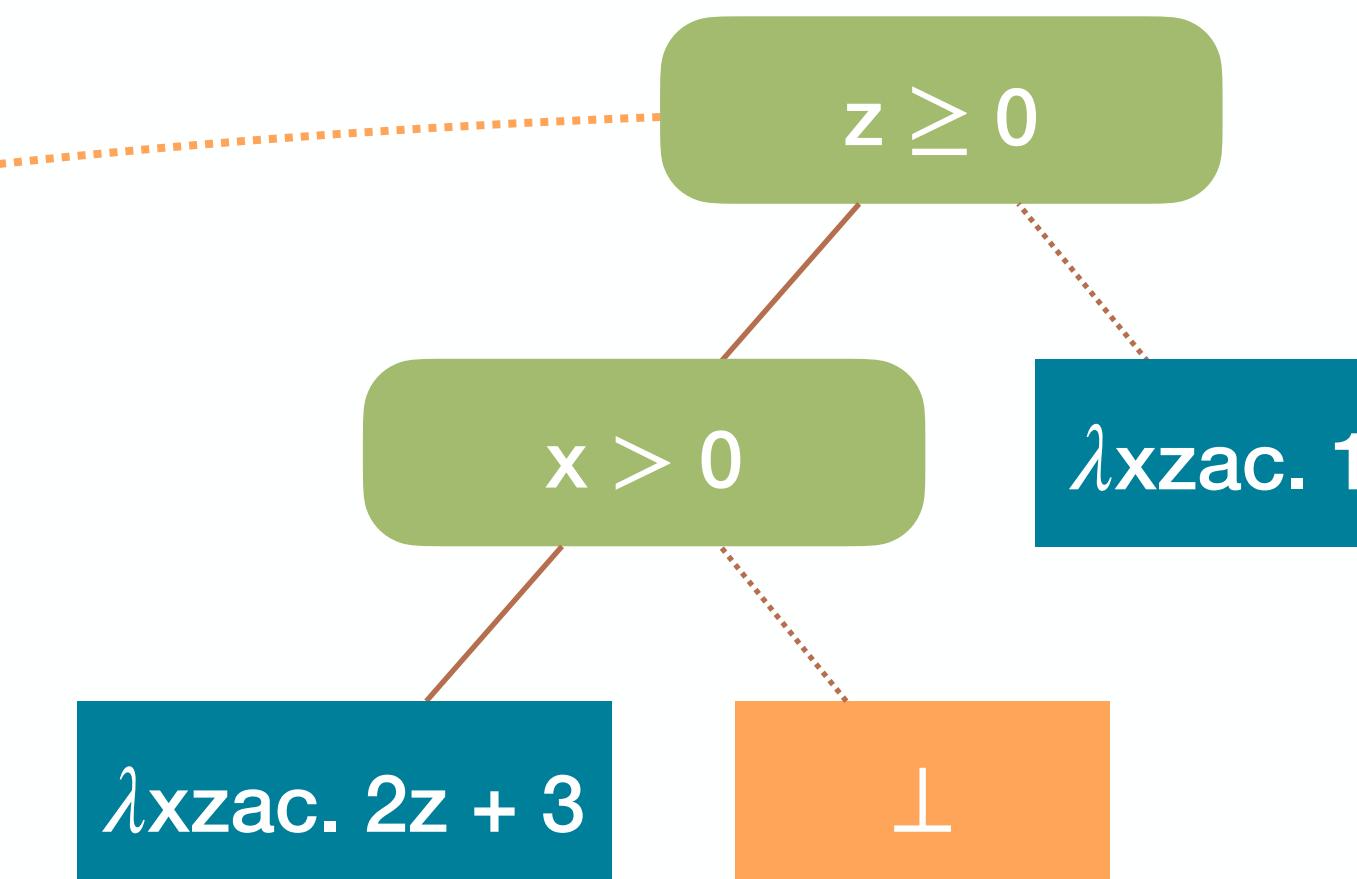
$\lambda x z a c. 2z + 3$

\perp



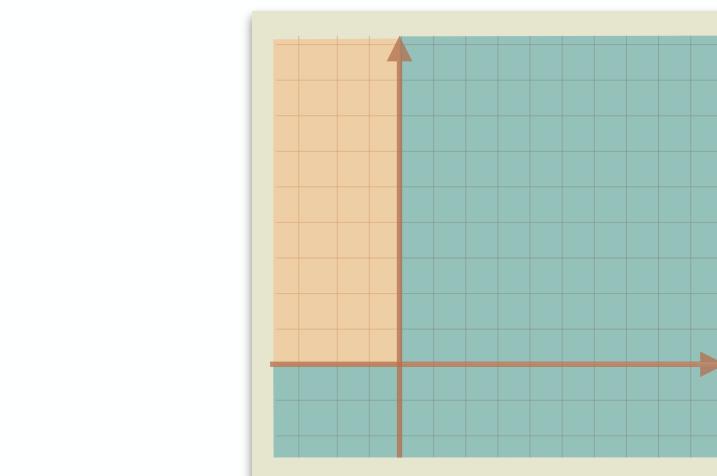
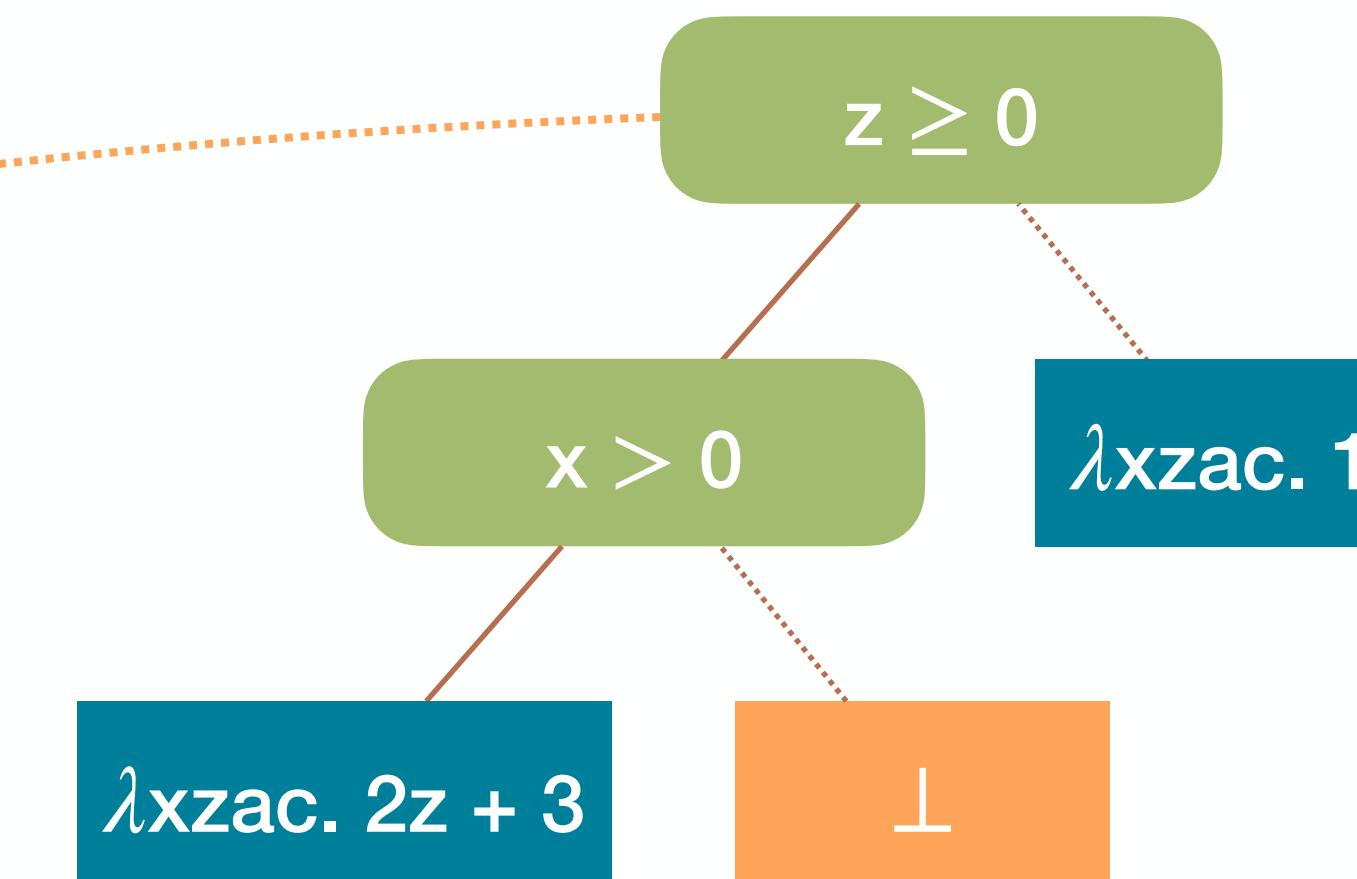
$\lambda x z a c. 2z + 3$

\perp



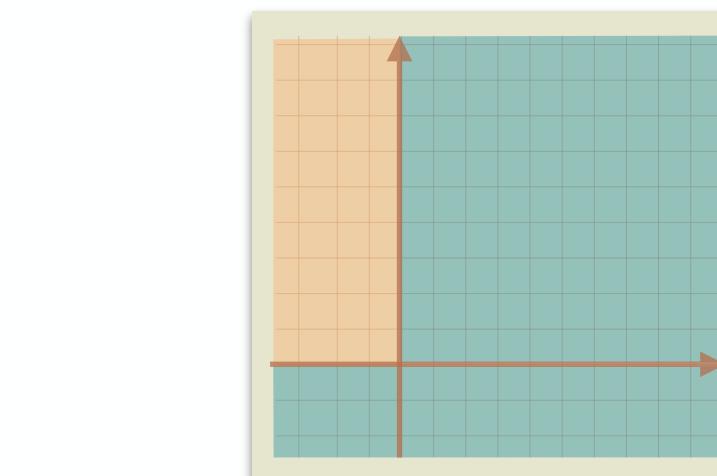
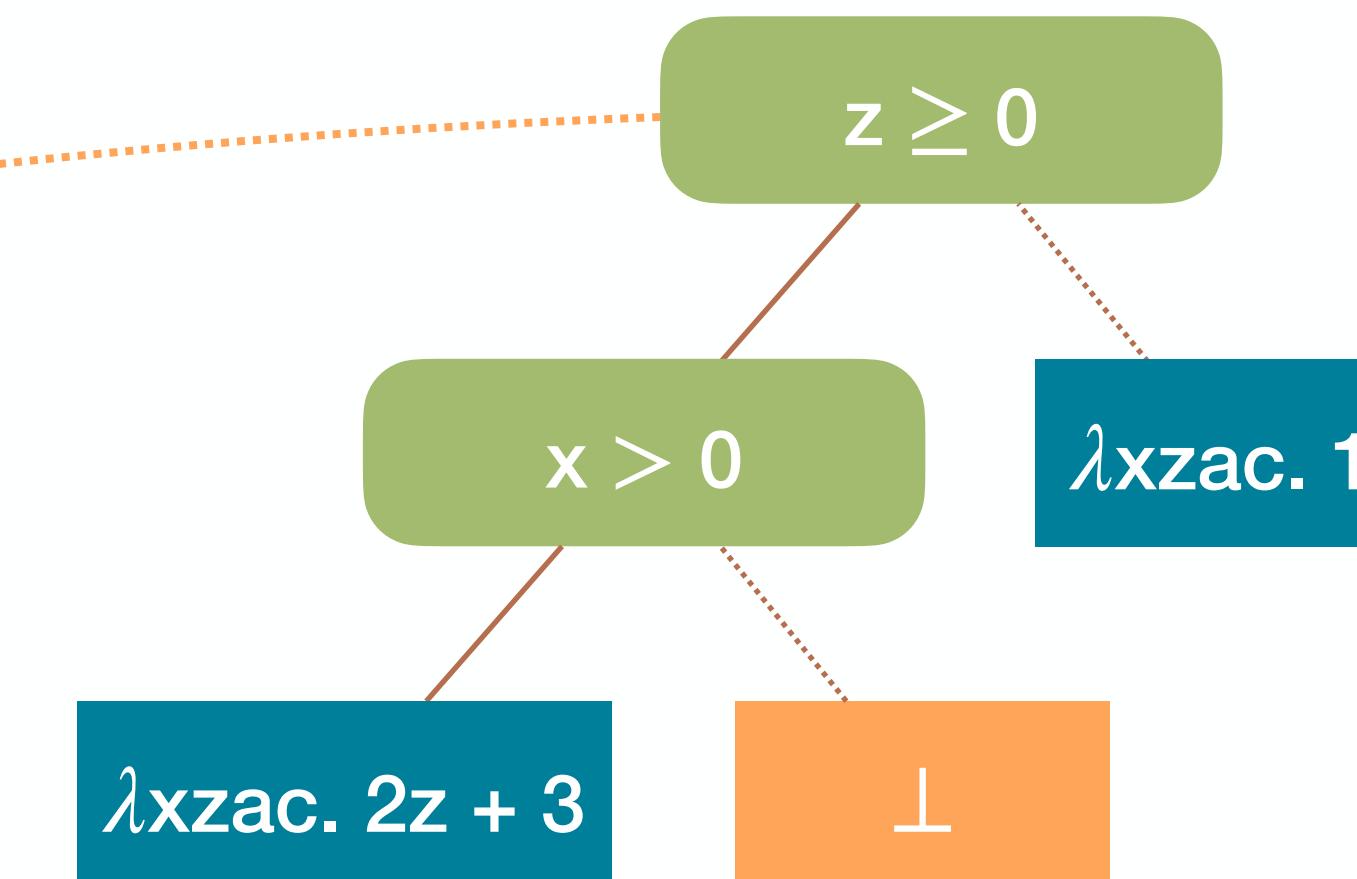
$\lambda x z a c. 2z + 3$

\perp



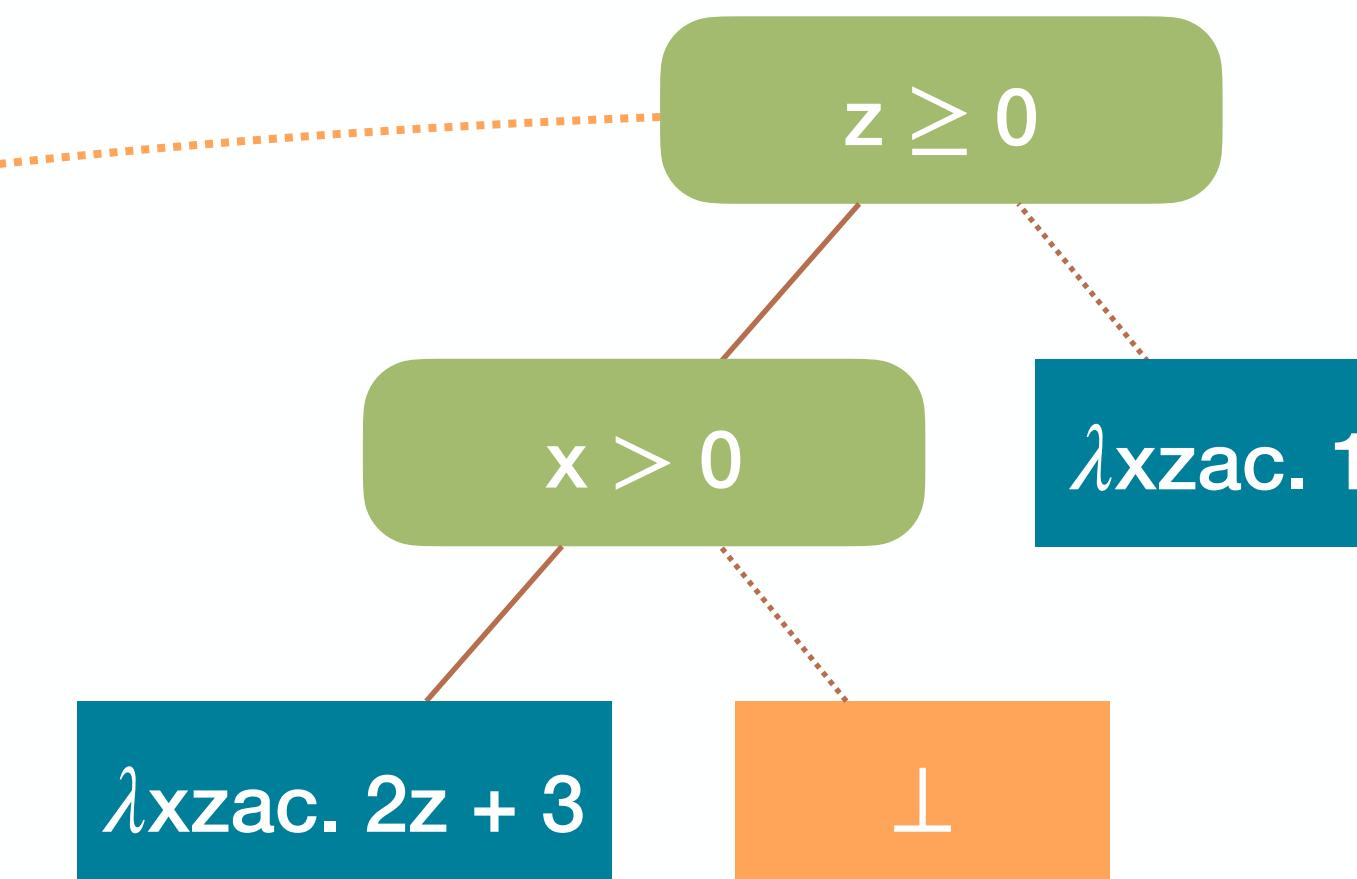
$\lambda x z a c. 2z + 3$

\perp

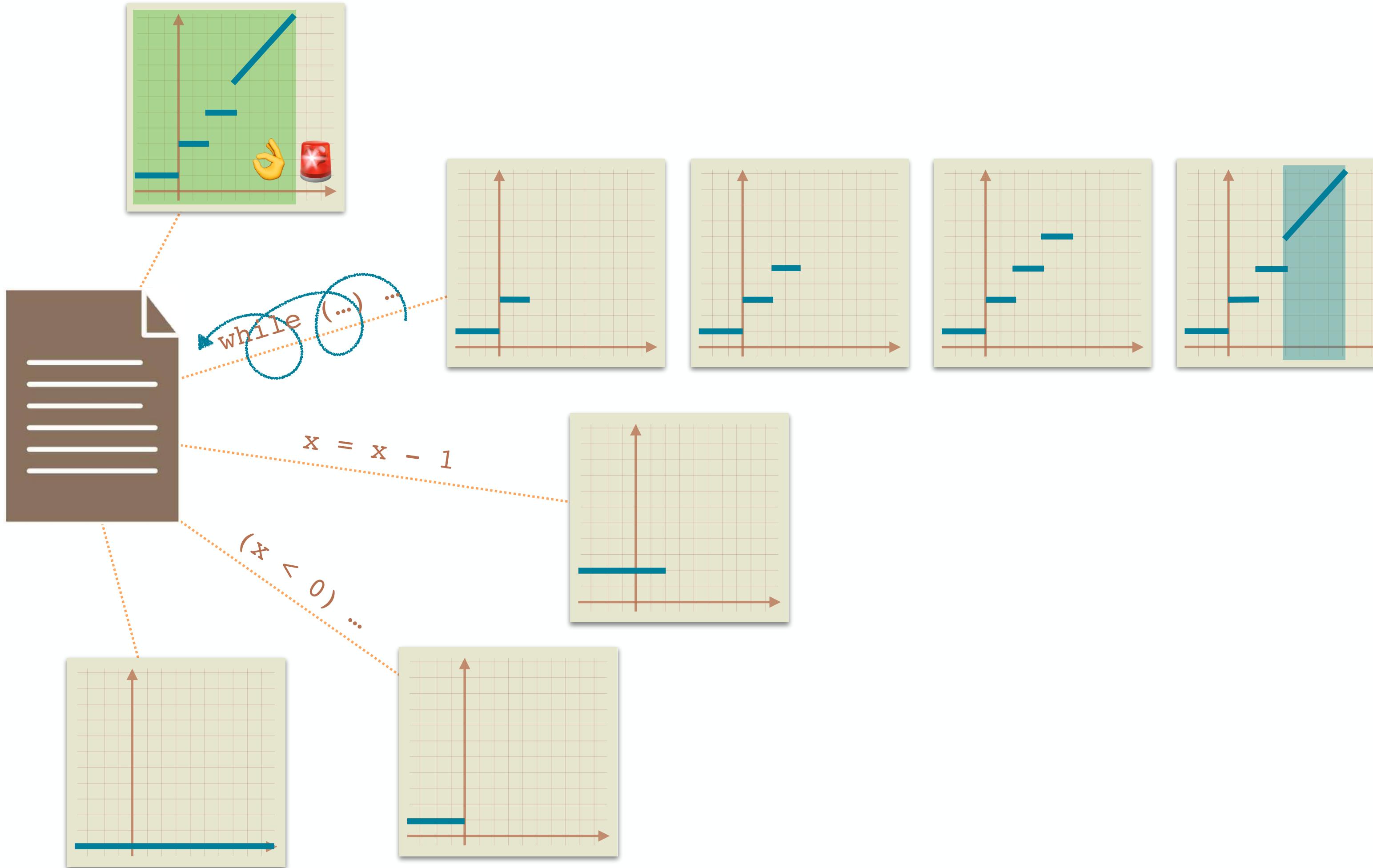


$\lambda x z a c. 2z + 3$

\perp



Termination Resilience Static Analysis

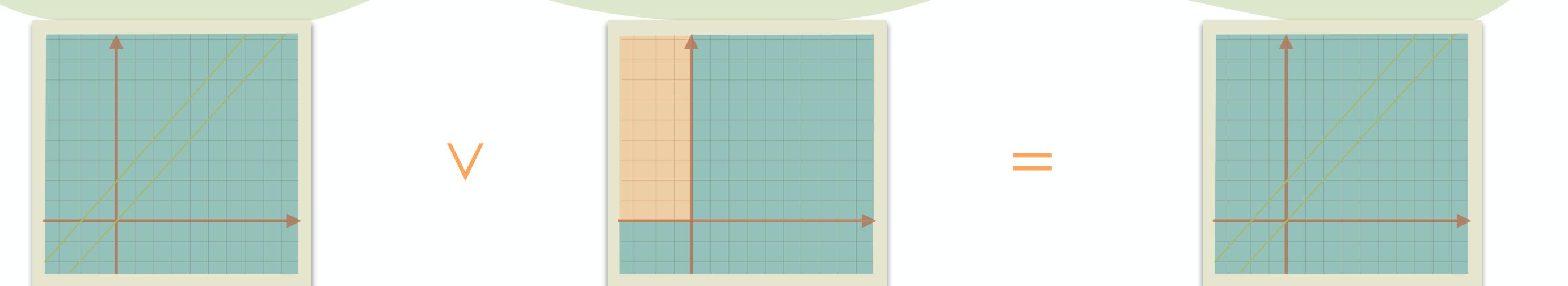
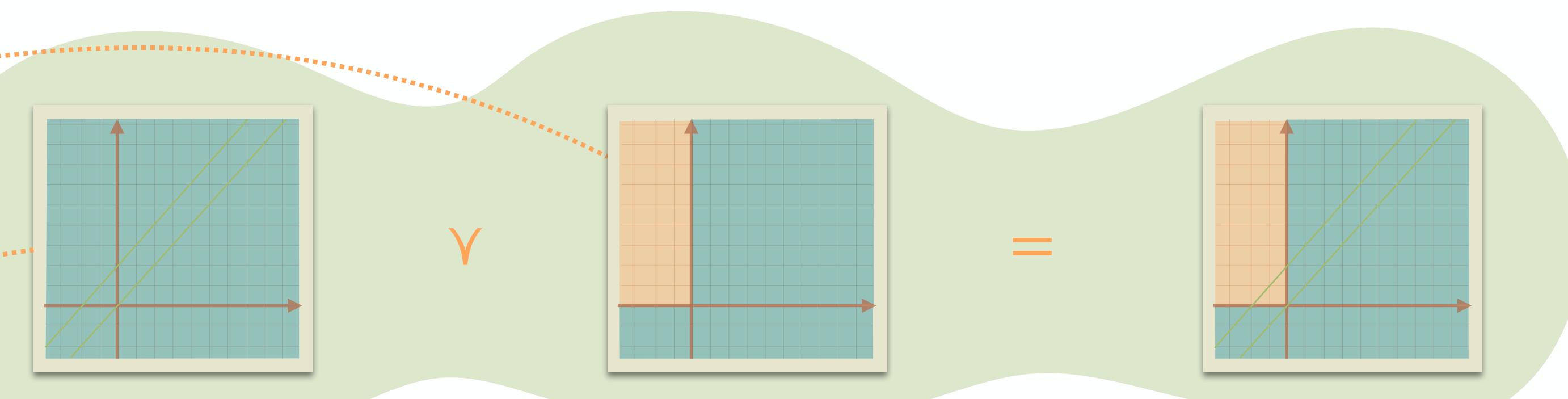


Termination Resilience Static Analysis

Approximation Join or Resilience Join?

function $f(x)$ {

```
1 a ←  $[-\infty, +\infty]$ 
2 z ← 10
3 if ( $a^*a \geq 0$ ) then
4   while  $(z \geq 0)$  do
5     z ←  $z - x$ 
6   od6
7 else
8   while  $(z \geq x)$  do
9     c ←  $[-2, 1]$ 
10    z ←  $z + c$ 
11  od10
fi
```



}¹¹

Termination Resilience Static Analysis

function f(x) {

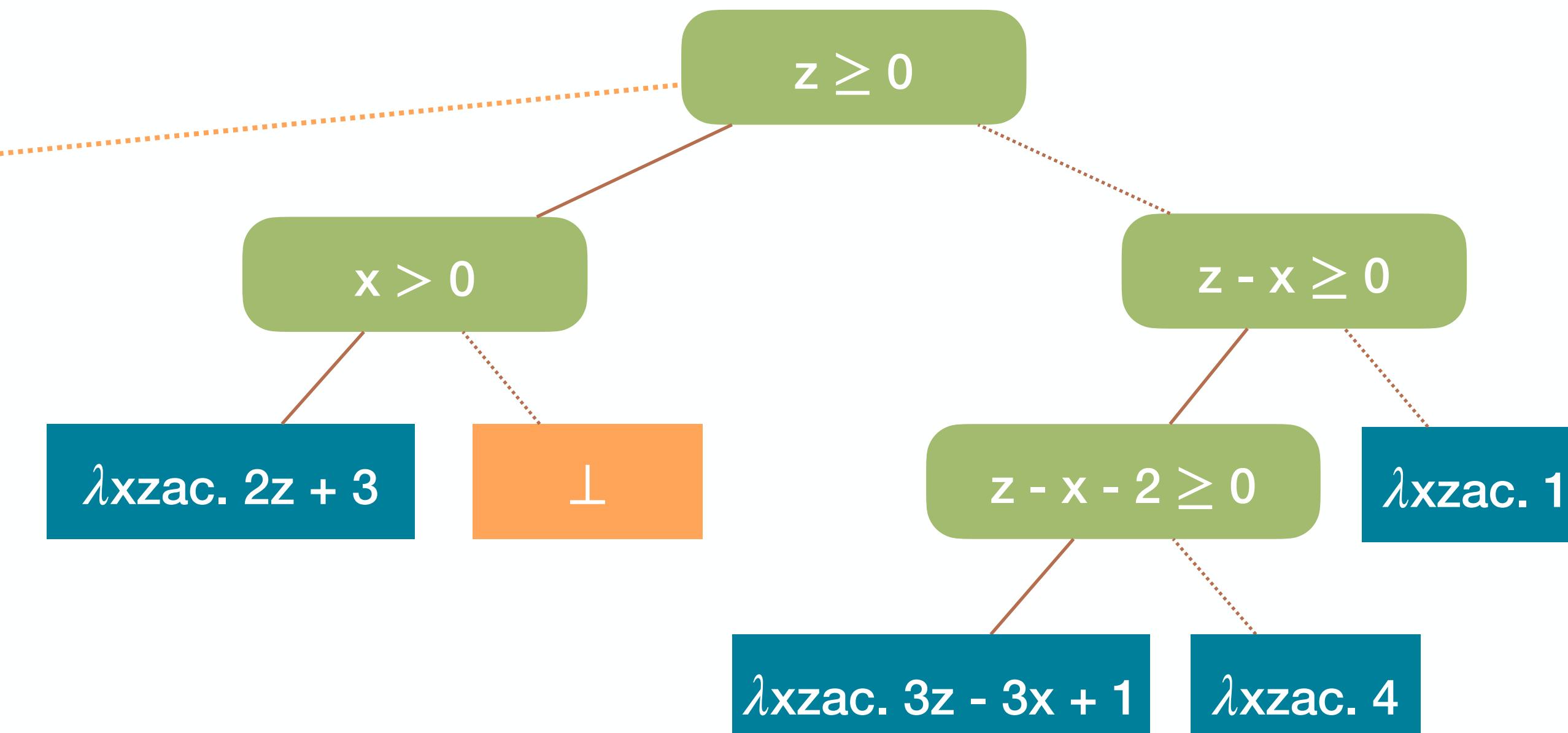
```
1 a ← [-∞, +∞]  
2 z ← 10  
3 if (a*a ≥ 0) then  
    while 4(z ≥ 0) do  
        5z ← z - x  
od6
```

```
else  
    while 7(z ≥ x) do
```

```
    8c ← [-2, 1]  
    9z ← z + c  
od10
```

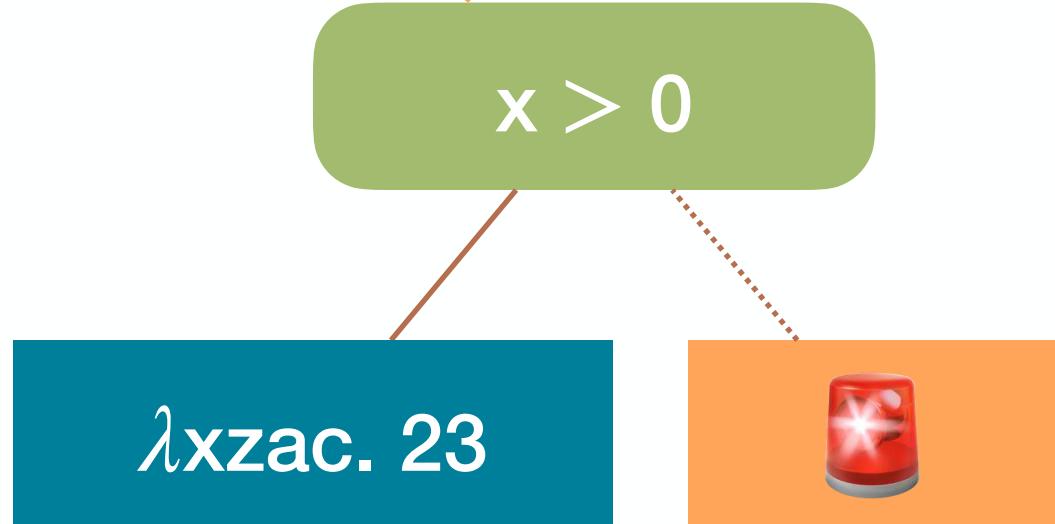
fi

}¹¹



Termination Resilience Static Analysis

```
function f(x) {  
    1 a ← [-∞, +∞]  
    2 z ← 10  
    3 if (a*a ≥ 0) then  
        while 4(z ≥ 0) do  
            5 z ← z - x  
        od6  
    else  
        while 7(z ≥ x) do  
            8 c ← [-2, 1]  
            9 z ← z + c  
        od10  
    fi  
}11
```



Termination Resilience Static Analysis

3-Step Recipe

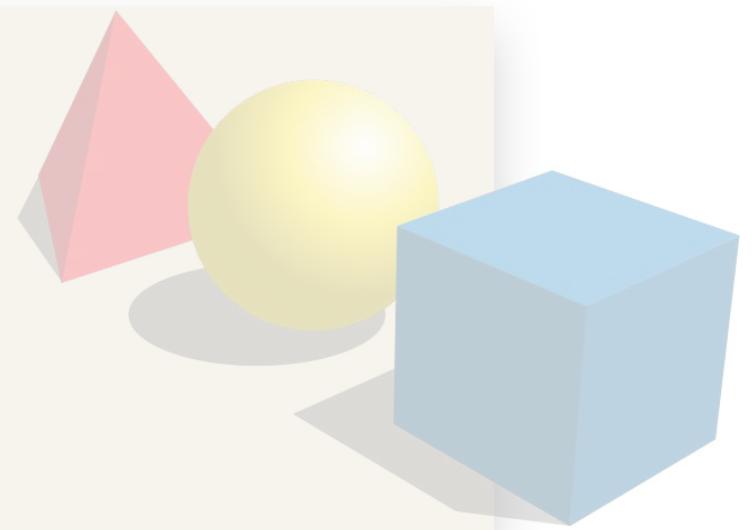
practical tools

targeting specific programs



abstract semantics, abstract domains

algorithmic approaches to decide program properties



concrete semantics

mathematical models of the program behavior

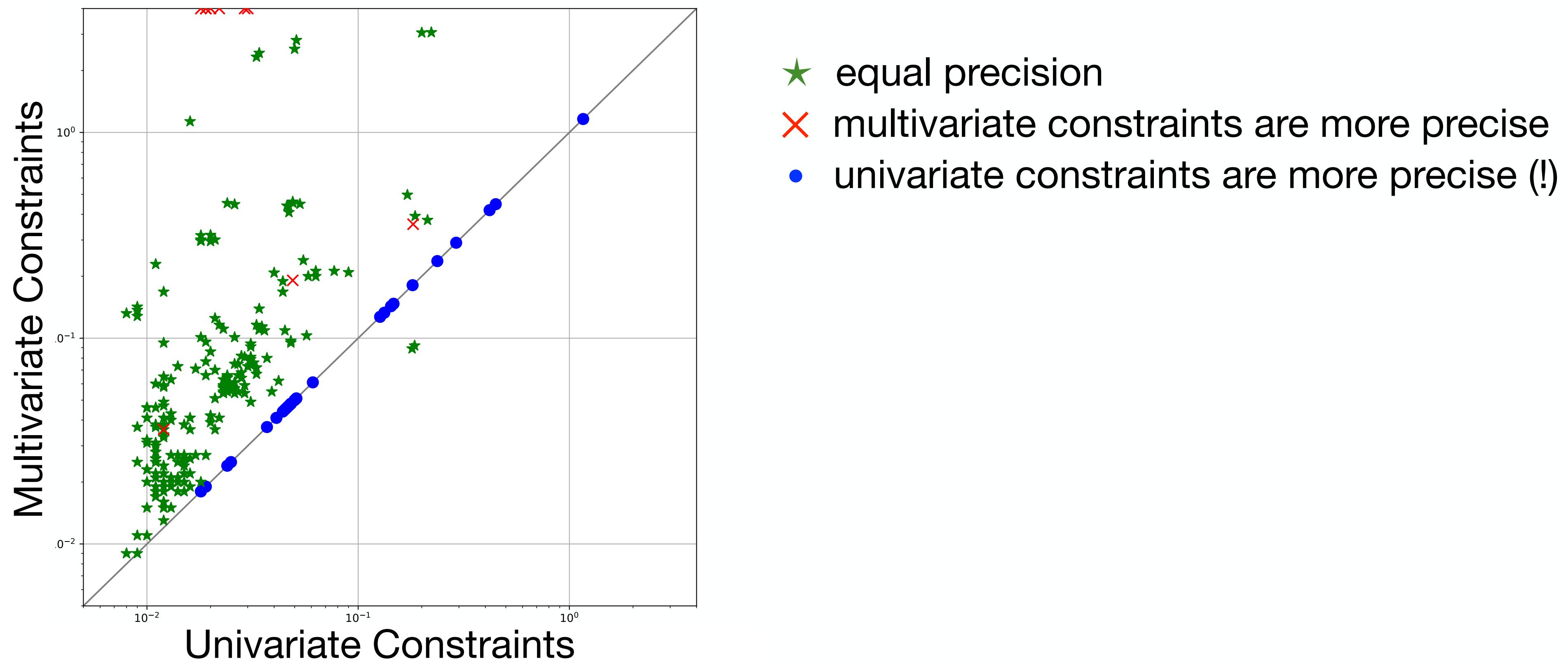


Experimental Evaluation

	Benchmark	Property	Verified	Alarms	TO	Time
Univariate Constraints	SV-COMP 2024	Termination	0	119	0	3.5s
		Termination Resilience	61	58	0	3.6s
	Raad et al @ OOPSLA 2024	Termination	0	36	0	0.5s
		Termination Resilience	16	20	0	0.5s
Multivariate Constraints	Shi et al. @ FSE 2022	Termination	0	85	0	2.0s
		Termination Resilience	57	28	0	2.2s
	SV-COMP 2024	Property	Verified	Alarms	TO	Time
		Termination	0	119	0	7.2s
Multivariate Constraints	Raad et al @ OOPSLA 2024	Termination Resilience	76	43	0	16.9s
		Termination	0	36	0	7.2s
	Shi et al. @ FSE 2022	Termination Resilience	16	20	0	16.9s
		Termination	0	85	0	69s
		Termination Resilience	49	28	8	500s

Experimental Evaluation

Univariate vs Multivariate Constraints



Termination Resilience Static Analysis

3-Step Recipe

practical tools

abstract semantics
abstract domains

concrete semantics

Experimental Evaluation Univariate vs Multivariate Constraints

A scatter plot comparing the precision of univariate and multivariate constraints. The y-axis is 'Multivariate Constraints' and the x-axis is 'Univariate Constraints'. Data points include green stars for equal precision, red crosses for multivariate more precise, and blue dots for univariate more precise.

Piecewise-Defined Ranking Functions

Diagram showing the relationship between Termination Resilience Semantics (brown circle) and Abstract Termination Resilience Semantics (green circle). It illustrates how a ranking function γ is defined over an abstract domain Θ^b and its concrete counterpart Θ . The text states $\text{dom}(\gamma(\Theta^b)) \subseteq \text{dom}(\Theta)$ and $\forall x \in \text{dom}(\gamma(\Theta^b)): \Theta(x) \leq \gamma(\Theta^b)(x)$.

Termination Resilience Static Analysis

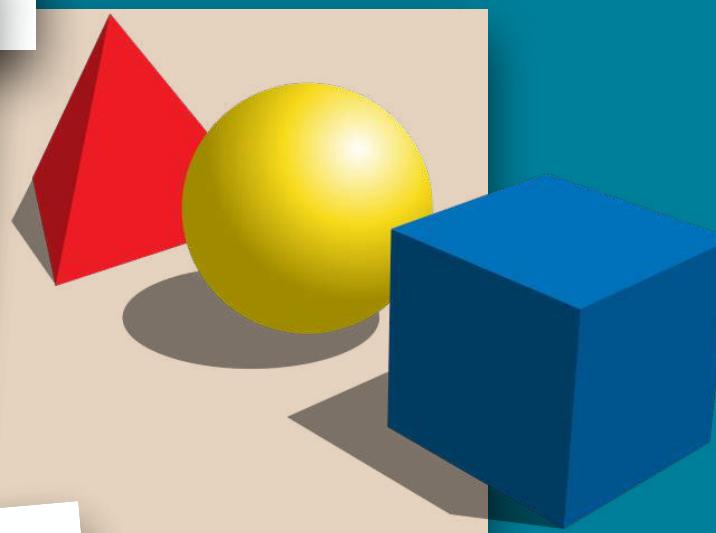
Diagram showing the analysis process. A document leads to a sequence of ranking function plots. Annotations include $x = x - 1$ and $\gamma < 0$.

Termination Resilience Semantics

Diagram showing a function $f(x)$ with code and a state transition graph. The code includes a while loop and an if-else statement. The graph shows nodes labeled 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11.

Termination Resilience Semantics

Formal definitions of termination resilience semantics. $f_1 \sqsubseteq f_2 \stackrel{\text{def}}{=} \text{dom}(f_1) \subseteq \text{dom}(f_2) \wedge \forall x \in \text{dom}(f_1): f_1(x) \leq f_2(x)$. $\Theta \stackrel{\text{def}}{=} \text{lfp}_{\emptyset}^{\sqsubseteq} \lambda f \lambda s . \begin{cases} 0 & \text{final states } s \in \Omega_{\tau} \\ \sup\{f(s') + 1 \mid \langle s, s' \rangle \in \tau\} & s \in \text{pre}_{\tau}(\text{dom}(f)) \\ \inf\{f(s') + 1 \mid \langle s, s' \rangle \in \tau\} & s \in \text{pre}_{\tau}(\text{dom}(f)) \\ \text{undefined} & \text{otherwise} \end{cases}$. $\text{pre}_{\tau}(X) \stackrel{\text{def}}{=} \{s \mid \forall s' \in X: \langle s, s' \rangle \in \tau\}$. $\text{pre}_{\tau}(X) \stackrel{\text{def}}{=} \{s \mid \exists s' \in X: \langle s, s' \rangle \in \tau\}$.



THANKS!