

Termination Resilience Static Analysis

15th Meeting of IFIP WG 1.9/2.15 Verified Software

“Verified Software and Applications: Mathematical and Formal Solutions”

Caterina Urban (joint work with **Naïm Moussaoui Remil**)

Inria & École Normale Supérieure | Université PSL

Which Non-Termination Alarm is Worse?

function f(x) {

1 ...

2 $z \leftarrow 10$

3 if (...) 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



← 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 ...
```

```
2 z ← 10
```

```
3 if ( ... ) 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

Robust Non-Termination

\exists **Input** \forall **Non-Deterministic Choices** : Program Diverges

function $f(x)$ {demonic non-determinism

1 ...

2 $z \leftarrow 10$

3 **if** (...) **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



← diverges when $x = 0$

Termination Resilience

\forall **Inputs** \exists **Non-Deterministic Choice** : **Program Terminates**

function $f(x)$ {

1 ...

2 $z \leftarrow 10$

3 **if** (...) **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



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

← angelic non-determinism

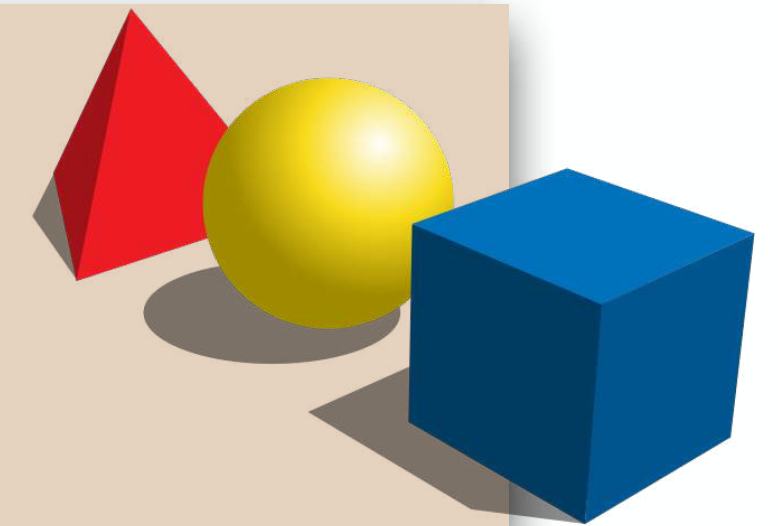
Termination Resilience Static Analysis

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

€ 10 +
€ 40 +
€ 30 +
€ 10

€ 90

COMPLETENESS

€ 9.95 +
€ 35.85 +
€ 27.95 +
€ 4.85

€ 78.60

FALSE ALARM

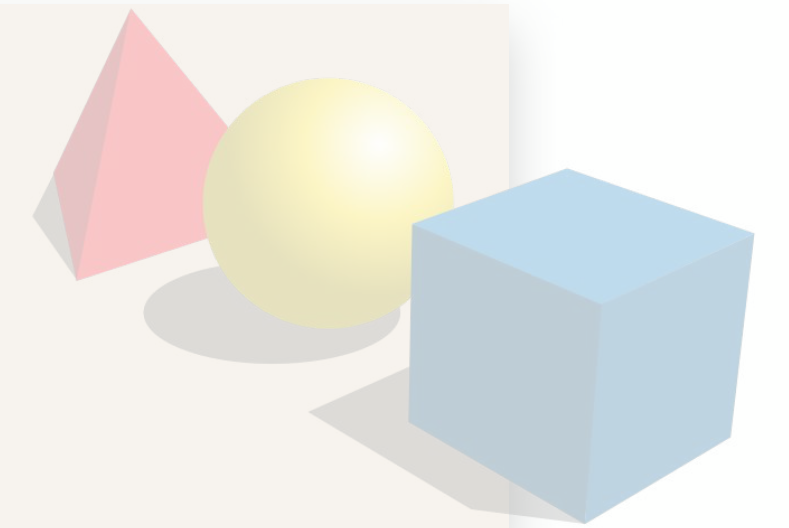
Termination Resilience Static Analysis

3-Step Recipe

practical tools
targeting specific programs



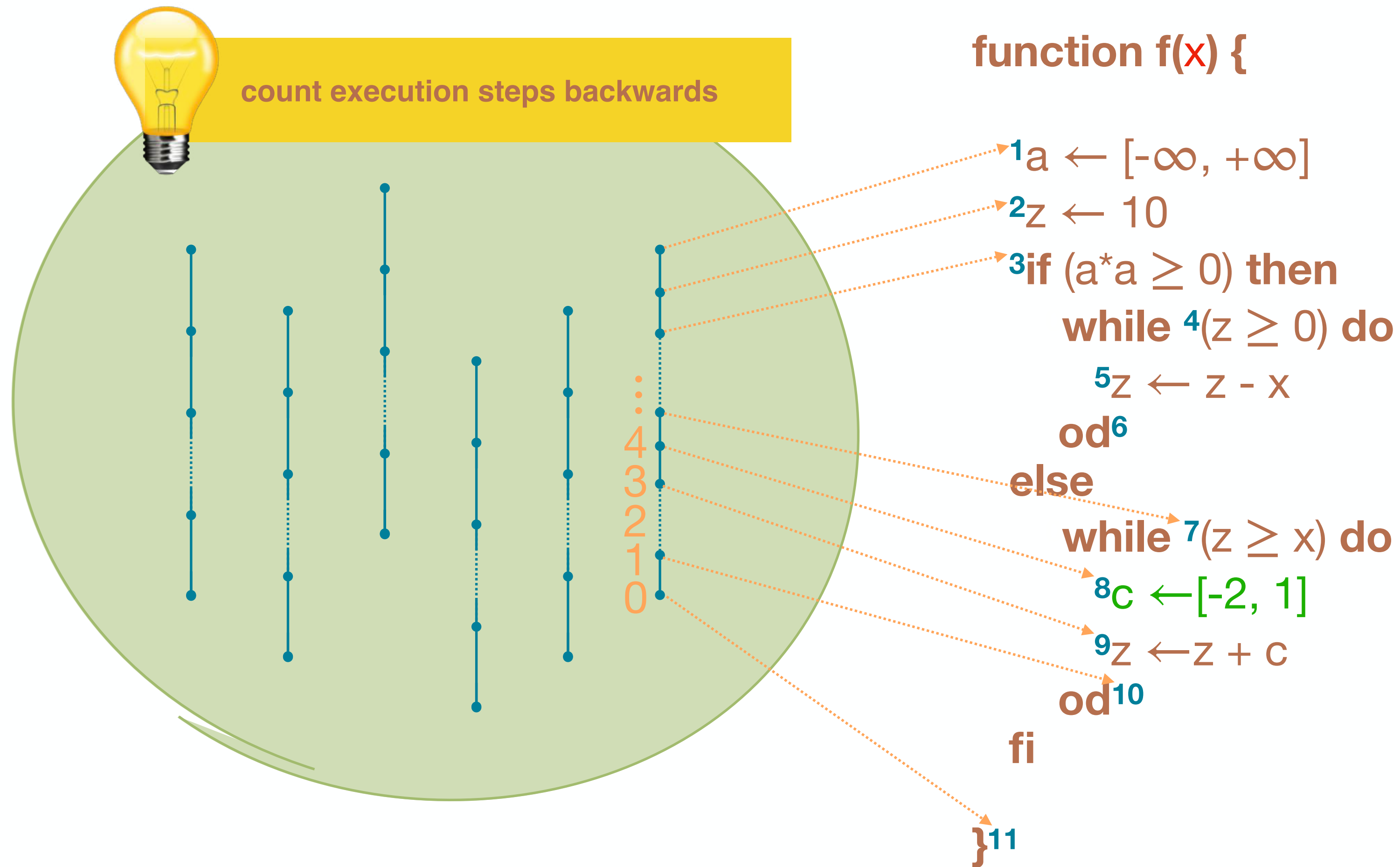
abstract semantics, abstract domains
algorithmic approaches to decide program properties



concrete semantics
mathematical models of the program behavior



Termination Resilience Semantics



Termination Resilience Semantics

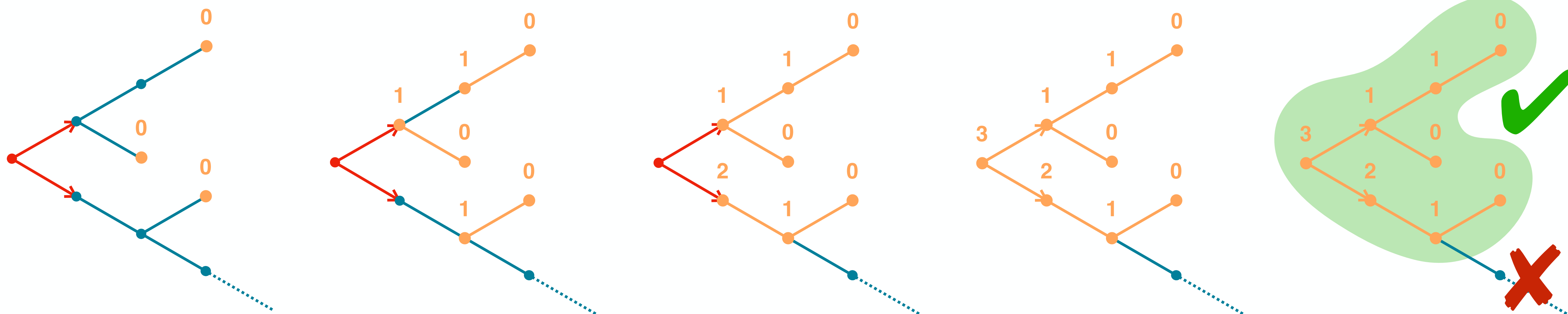
$f_1 \sqsubseteq f_2 \stackrel{\text{def}}{=} \text{dom}(f_1) \subseteq \text{dom}(f_2) \wedge \forall x \in \text{dom}(f_1): f_1(x) \leq f_2(x)$

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

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

$\text{pre}_{\tau^r}(X) \stackrel{\text{def}}{=} \{s \mid \exists s' \in X: \langle s, s' \rangle \in \tau^r\}$ (regular transitions)

totally undefined function



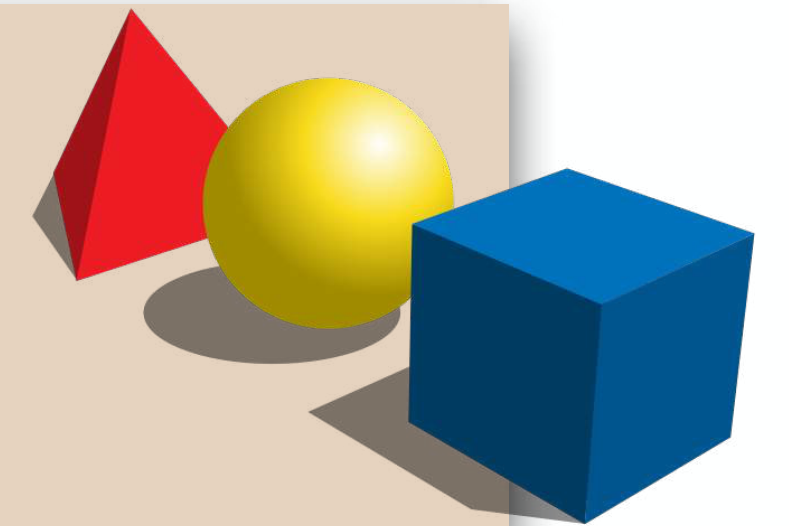
Termination Resilience Static Analysis

3-Step Recipe

practical tools
targeting specific programs



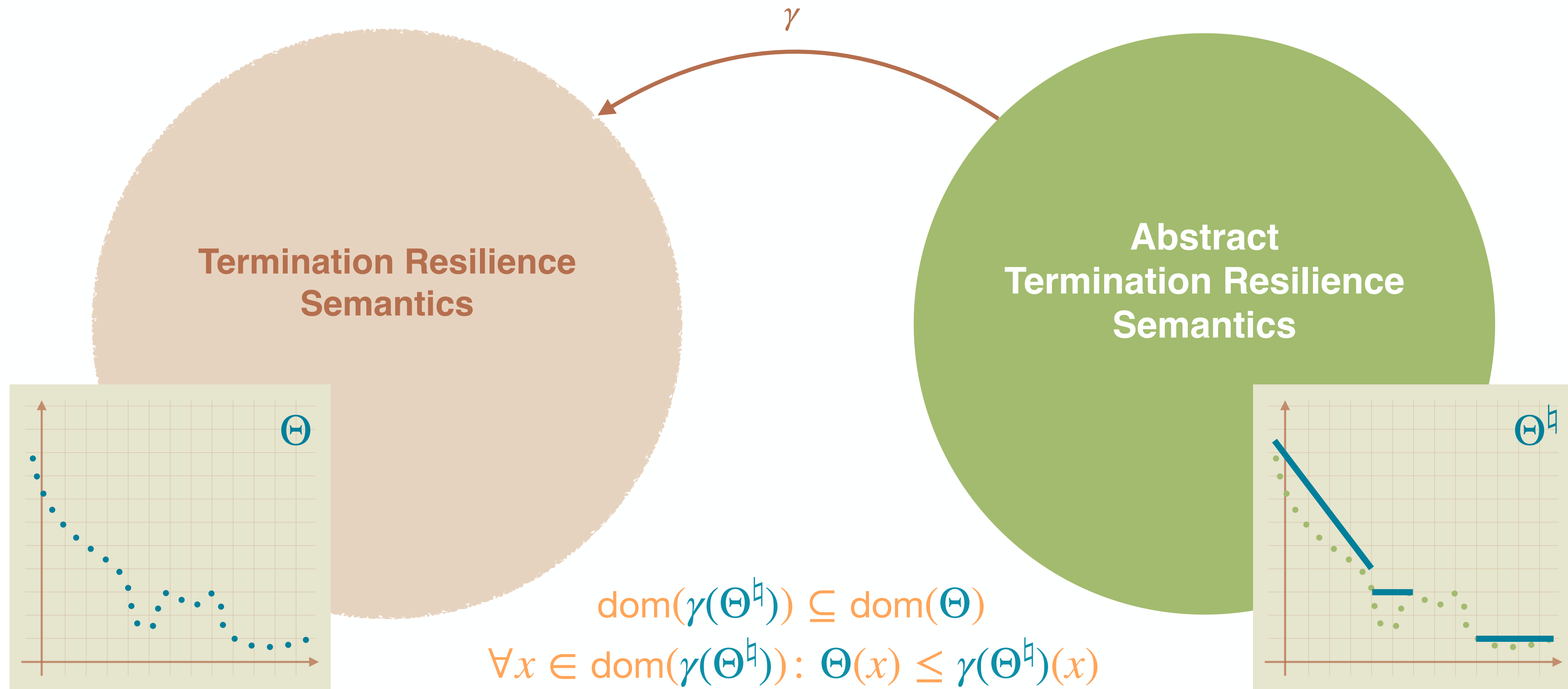
abstract semantics, abstract domains
algorithmic approaches to decide program properties



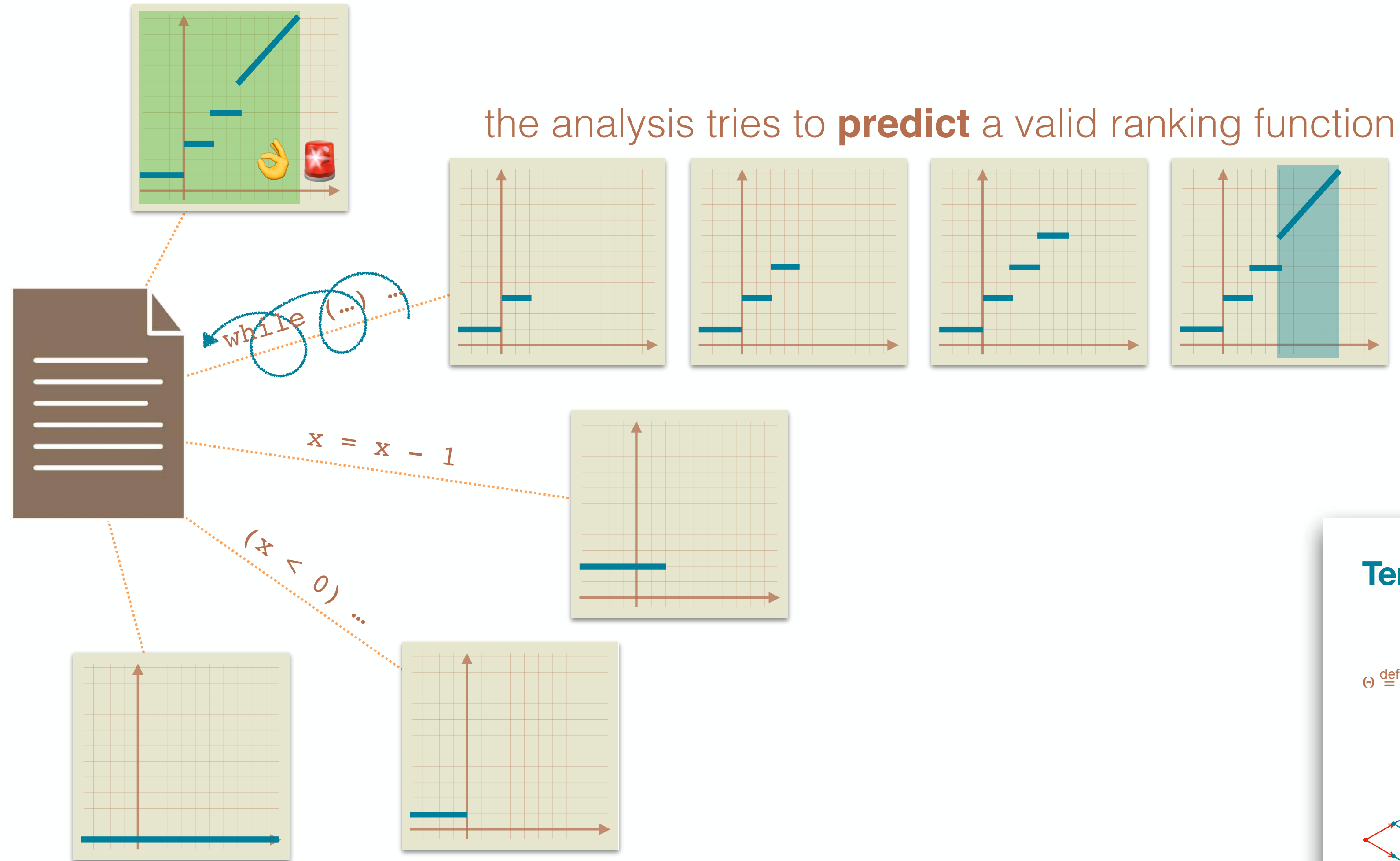
concrete semantics
mathematical models of the program behavior



Piecewise-Defined Ranking Functions



Termination Resilience Static Analysis



Termination Resilience Semantics

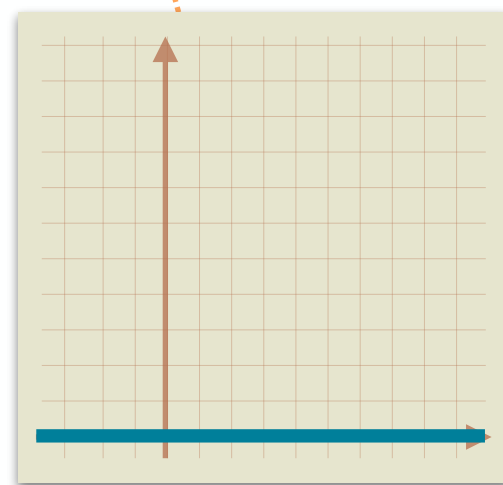
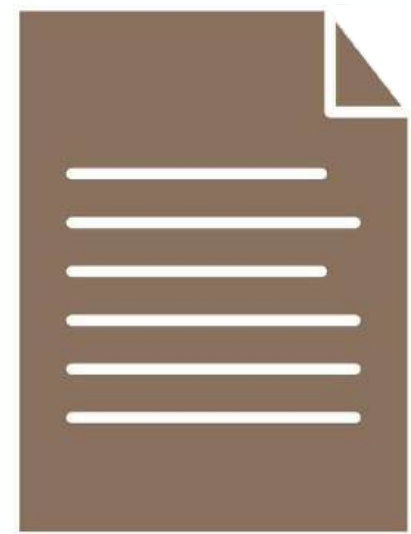
$$f_1 \sqsubseteq f_2 \stackrel{\text{def}}{=} \text{dom}(f_1) \subseteq \text{dom}(f_2) \wedge \forall x \in \text{dom}(f_1): f_1(x) \leq f_2(x)$$

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

$\text{pre}_r(X) \stackrel{\text{def}}{=} \{s \mid \forall s': \langle s, s' \rangle \in \tau^i \Rightarrow s' \in X\}$ (input transitions)
 $\text{pre}_r(X) \stackrel{\text{def}}{=} \{s \mid \exists s' \in X: \langle s, s' \rangle \in \tau^r\}$ (regular transitions)

totally undefined function

Termination Resilience Static Analysis



Termination Resilience Static Analysis

Static Backward Analysis

```
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
```

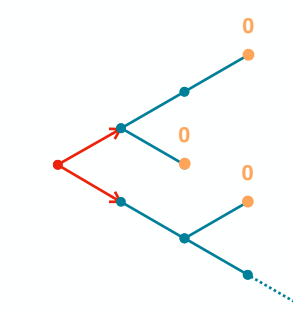
$\lambda x z a c. 0$

Termination Resilience Semantics

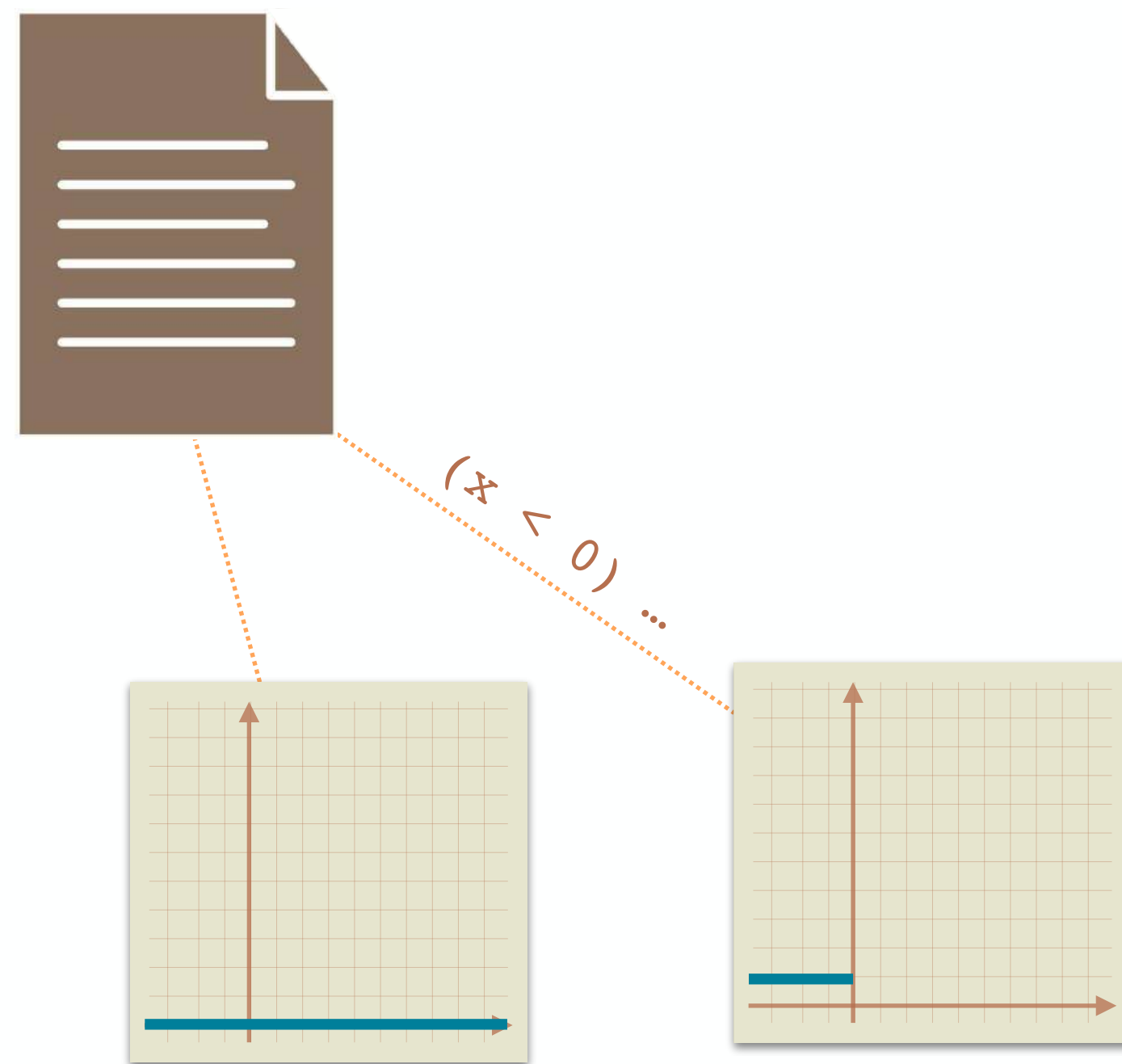
$f_1 \sqsubseteq f_2 \stackrel{\text{def}}{=} \text{dom}(f_1) \subseteq \text{dom}(f_2) \wedge \forall x \in \text{dom}(f_1) : f_1(x) \leq f_2(x)$

$\Theta \stackrel{\text{def}}{=} \text{lfp}_{\emptyset} \lambda f \lambda s . \left\{ \begin{array}{l} 0 \\ \text{final states } s \in \Omega_r \end{array} \right.$

totally undefined function



Termination Resilience Static Analysis



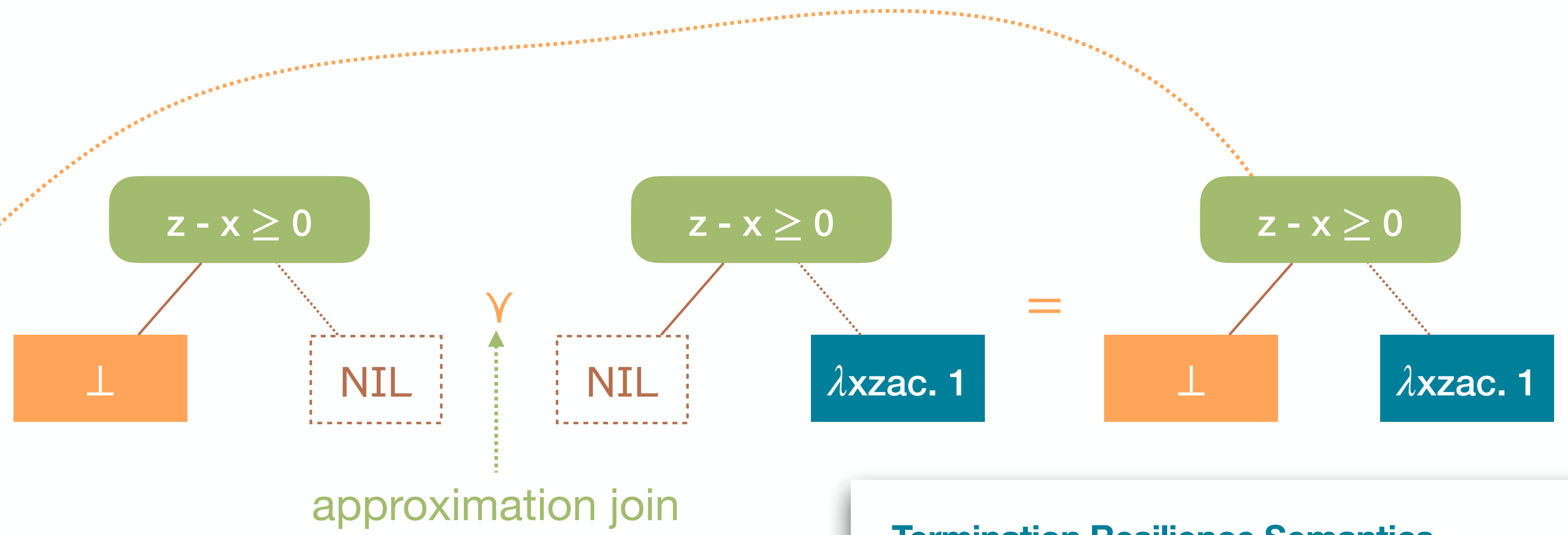
Termination Resilience Static Analysis

Boolean Conditions

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
    
```

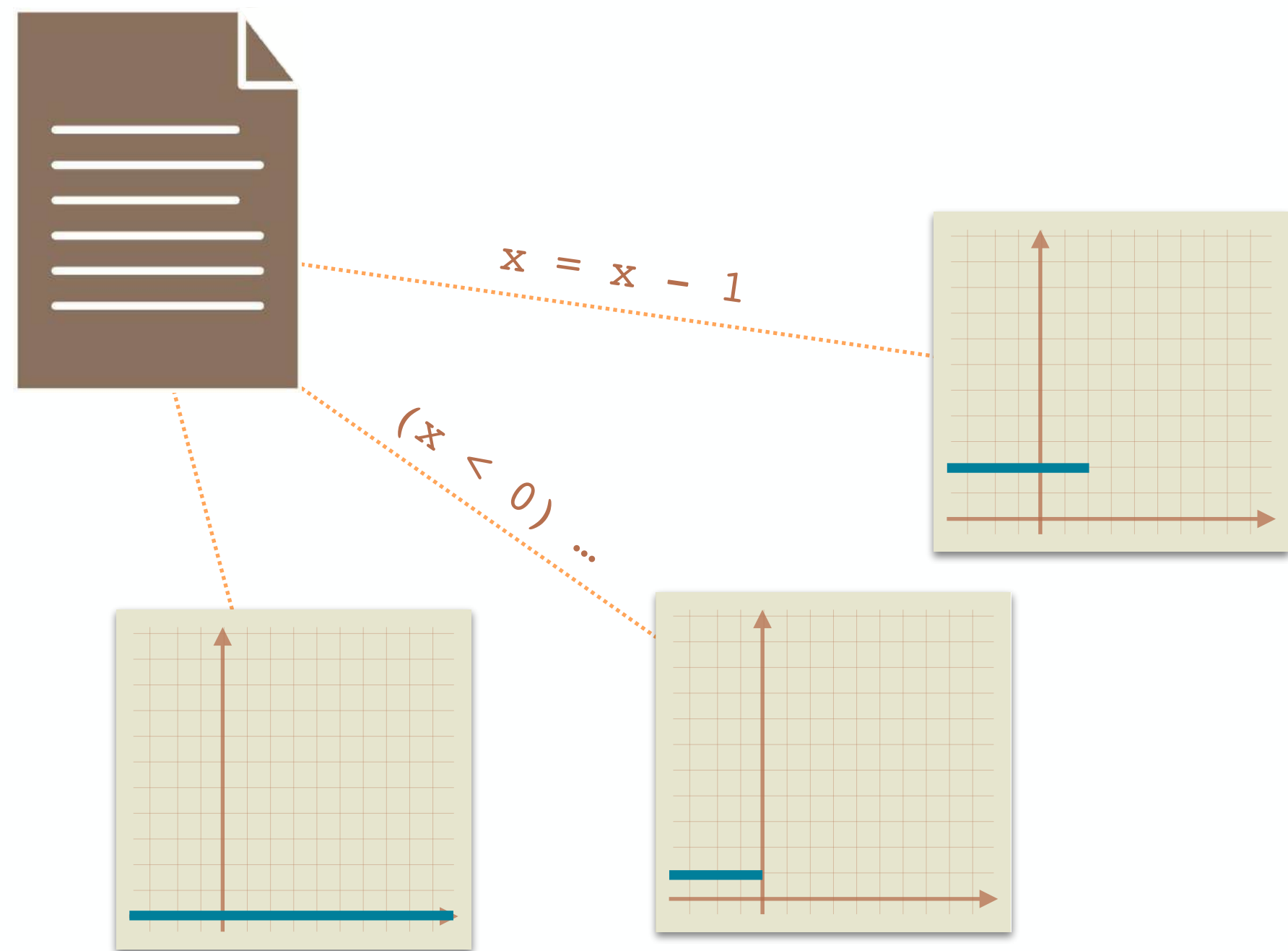


Termination Resilience Semantics

$f_1 \sqsubseteq f_2 \stackrel{\text{def}}{=} \text{dom}(f_1) \subseteq \text{dom}(f_2) \wedge \forall x \in \text{dom}(f_1): f_1(x) \leq f_2(x)$
 $\Theta \stackrel{\text{def}}{=} \text{lfp}_{\perp} \lambda f \lambda s. \begin{cases} 0 & \text{final states } s \in \Omega_{\tau} \\ \sup\{f(s') + 1 \mid \langle s, s' \rangle \in \tau\} & s \in \tilde{\text{pre}}_{\tau}(\text{dom}(f)) \\ \inf\{f(s') + 1 \mid \langle s, s' \rangle \in \tau\} & s \in \text{pre}_{\tau}(\text{dom}(f)) \end{cases}$
 $\tilde{\text{pre}}_{\tau}(X) \stackrel{\text{def}}{=} \{s \mid \forall s': \langle s, s' \rangle \in \tau^i \Rightarrow s' \in X\}$
 $\text{pre}_{\tau}(X) \stackrel{\text{def}}{=} \{s \mid \exists s' \in X: \langle s, s' \rangle \in \tau^r\}$

totally undefined function
 input transitions
 regular transitions

Termination Resilience Static Analysis



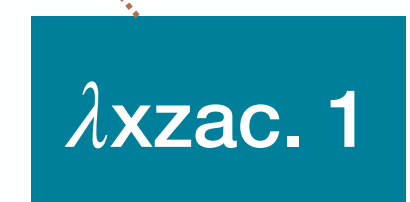
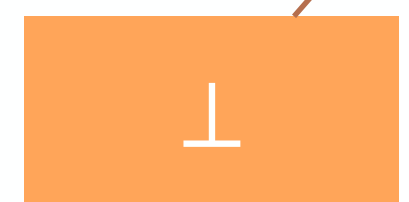
Termination Resilience Static Analysis

Variable Assignment

```

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
    
```

$$z - x \geq 0$$



$$z + c - x \geq 0$$



Termination Resilience Semantics

$f_1 \sqsubseteq f_2 \stackrel{\text{def}}{=} \text{dom}(f_1) \subseteq \text{dom}(f_2) \wedge \forall x \in \text{dom}(f_1): f_1(x) \leq f_2(x)$
 $\Theta \stackrel{\text{def}}{=} \text{lfp}_{\perp} \lambda f \lambda s. \begin{cases} 0 & \text{final states } s \in \Omega_{\tau} \\ \sup\{f(s') + 1 \mid \langle s, s' \rangle \in \tau\} & s \in \tilde{\text{pre}}_{\tau}(\text{dom}(f)) \\ \inf\{f(s') + 1 \mid \langle s, s' \rangle \in \tau\} & s \in \text{pre}_{\tau}(\text{dom}(f)) \end{cases}$
 $\tilde{\text{pre}}_{\tau}(X) \stackrel{\text{def}}{=} \{s \mid \forall s': \langle s, s' \rangle \in \tau^i \Rightarrow s' \in X\}$
 $\text{pre}_{\tau}(X) \stackrel{\text{def}}{=} \{s \mid \exists s' \in X: \langle s, s' \rangle \in \tau^r\}$

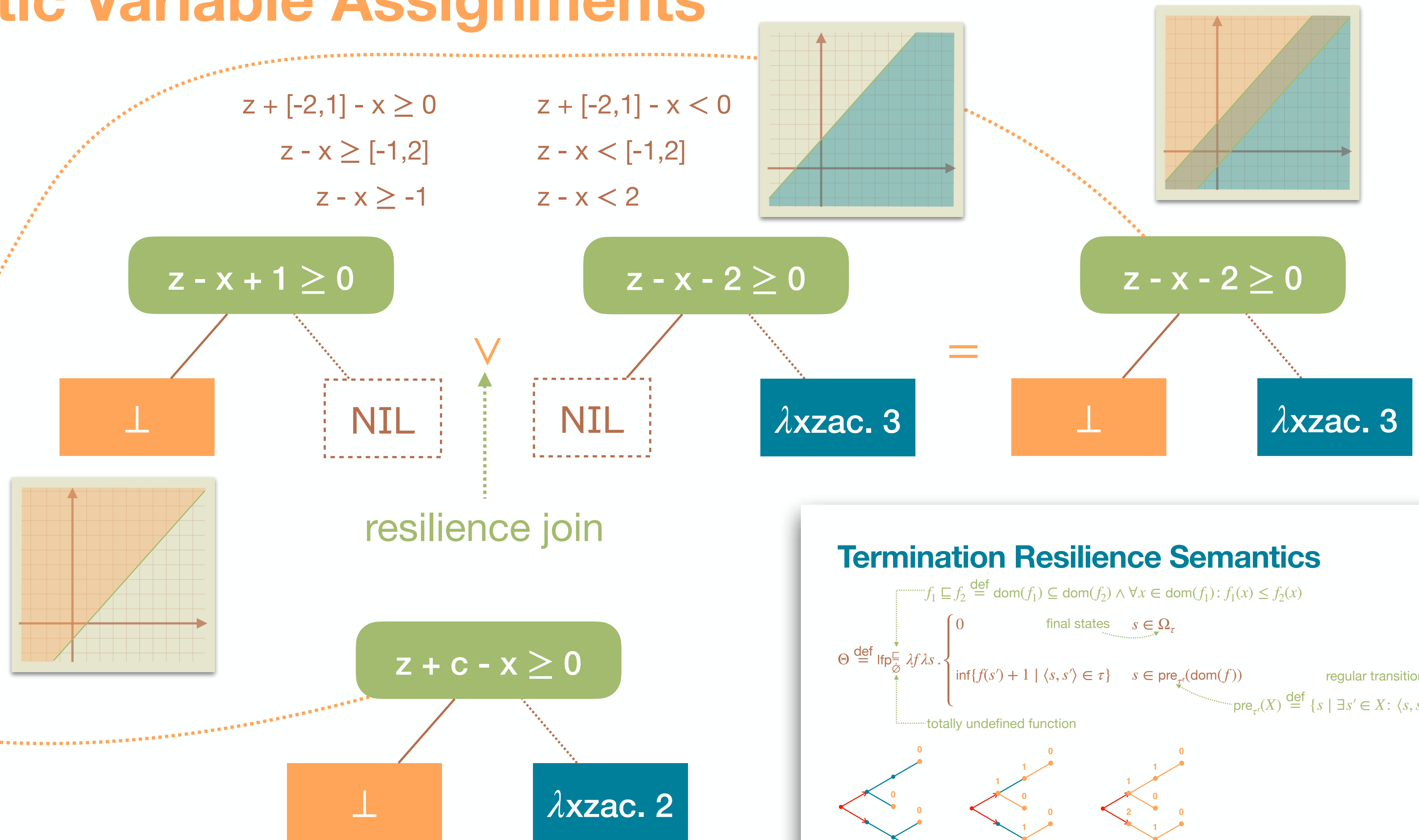
totally undefined function
 input transitions
 regular transitions

Termination Resilience Static Analysis

Non-Deterministic Variable Assignments

```

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

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

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

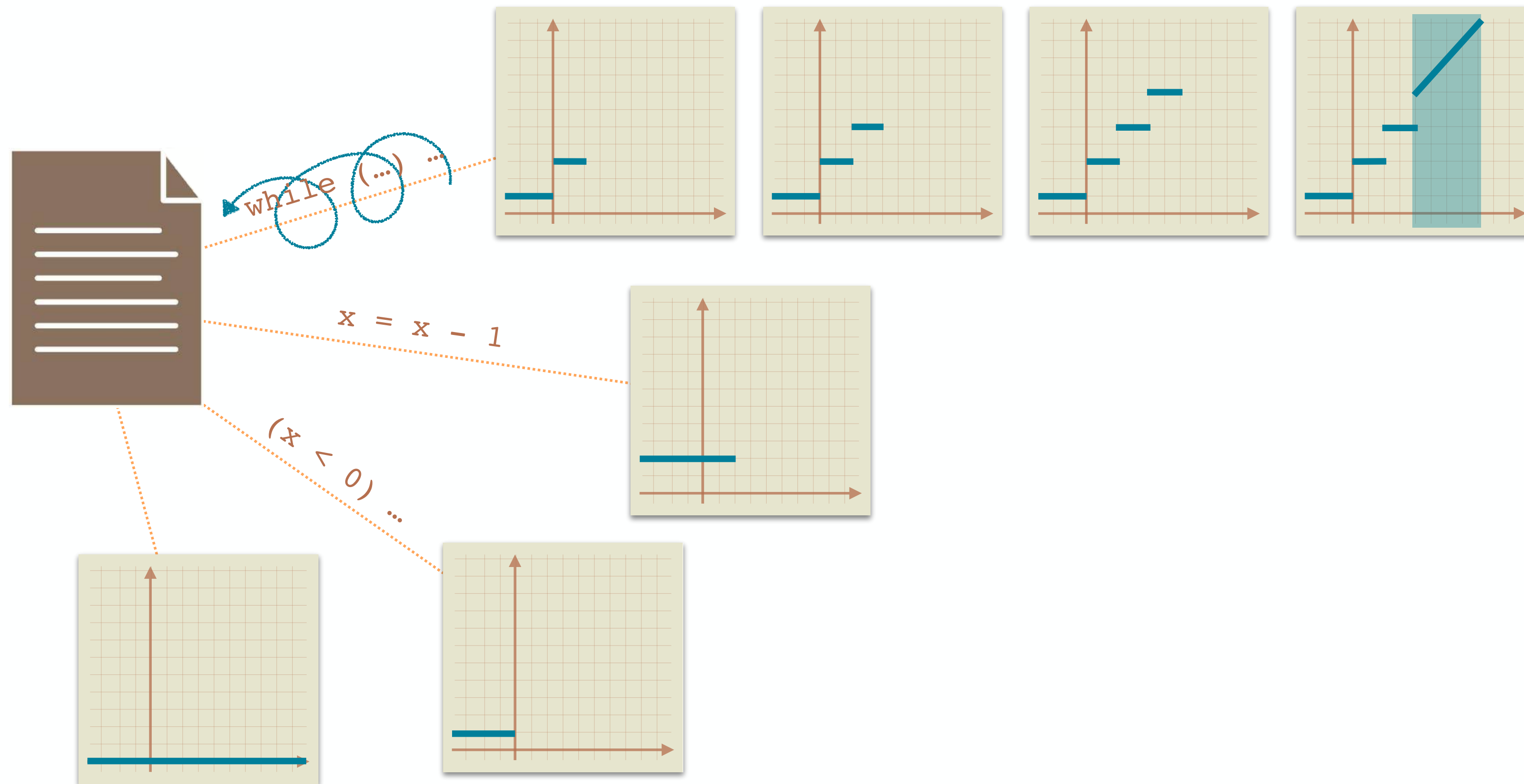
$\text{pre}_{\tau}(X) \stackrel{\text{def}}{=} \{s \mid \exists s' \in X: \langle s, s' \rangle \in \tau\}$

totally undefined function

regular transitions

Termination Resilience Static Analysis

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



Termination Resilience Static Analysis

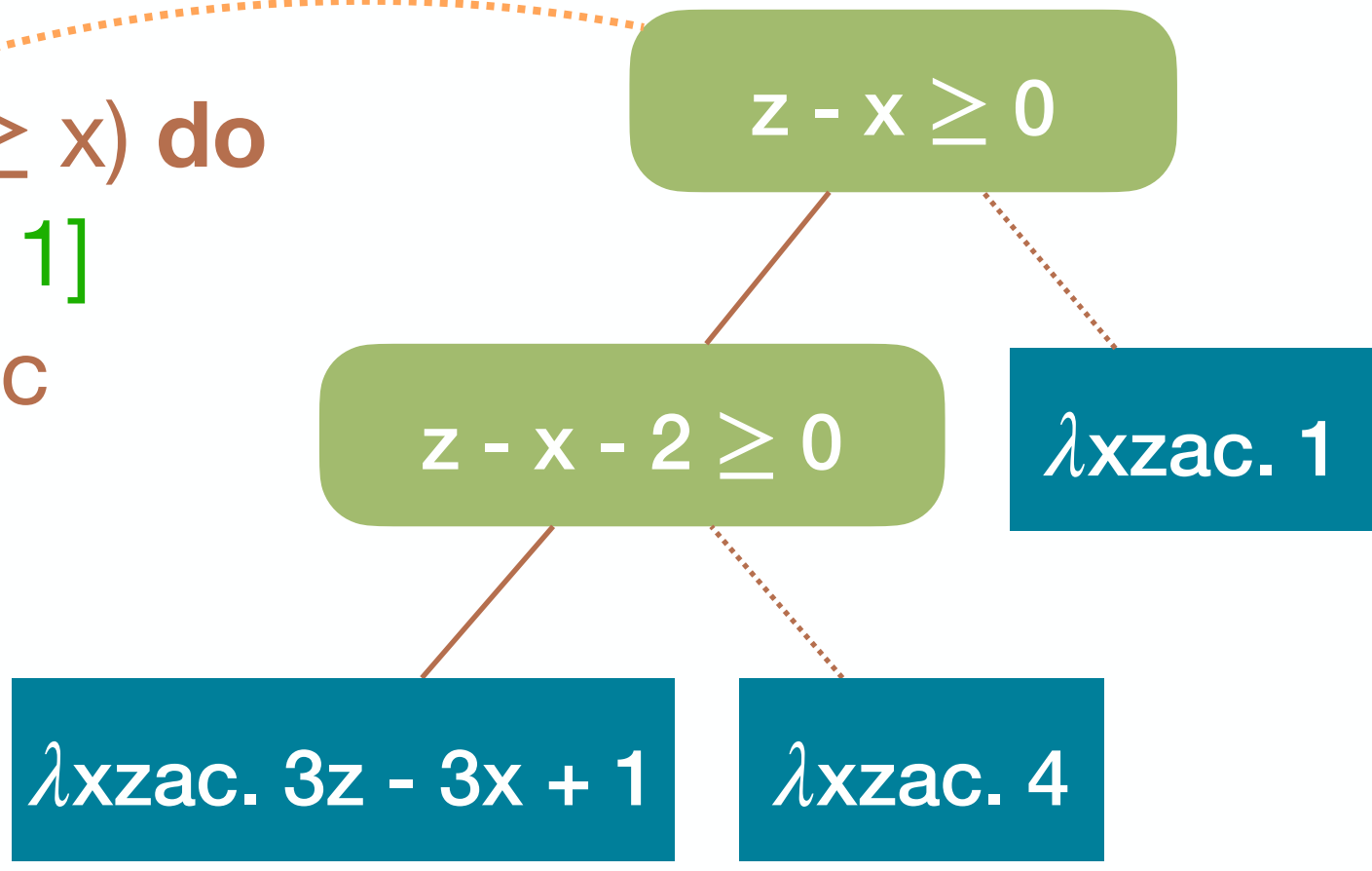
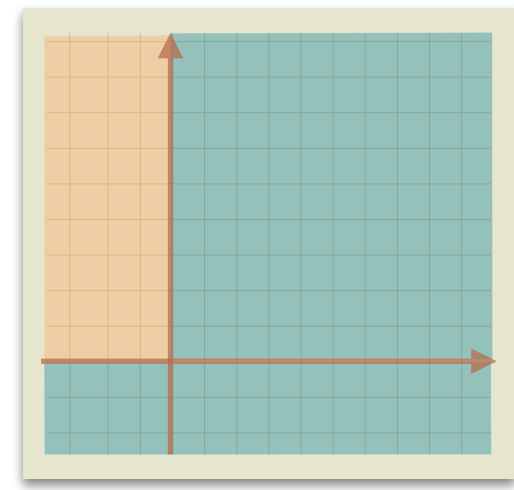
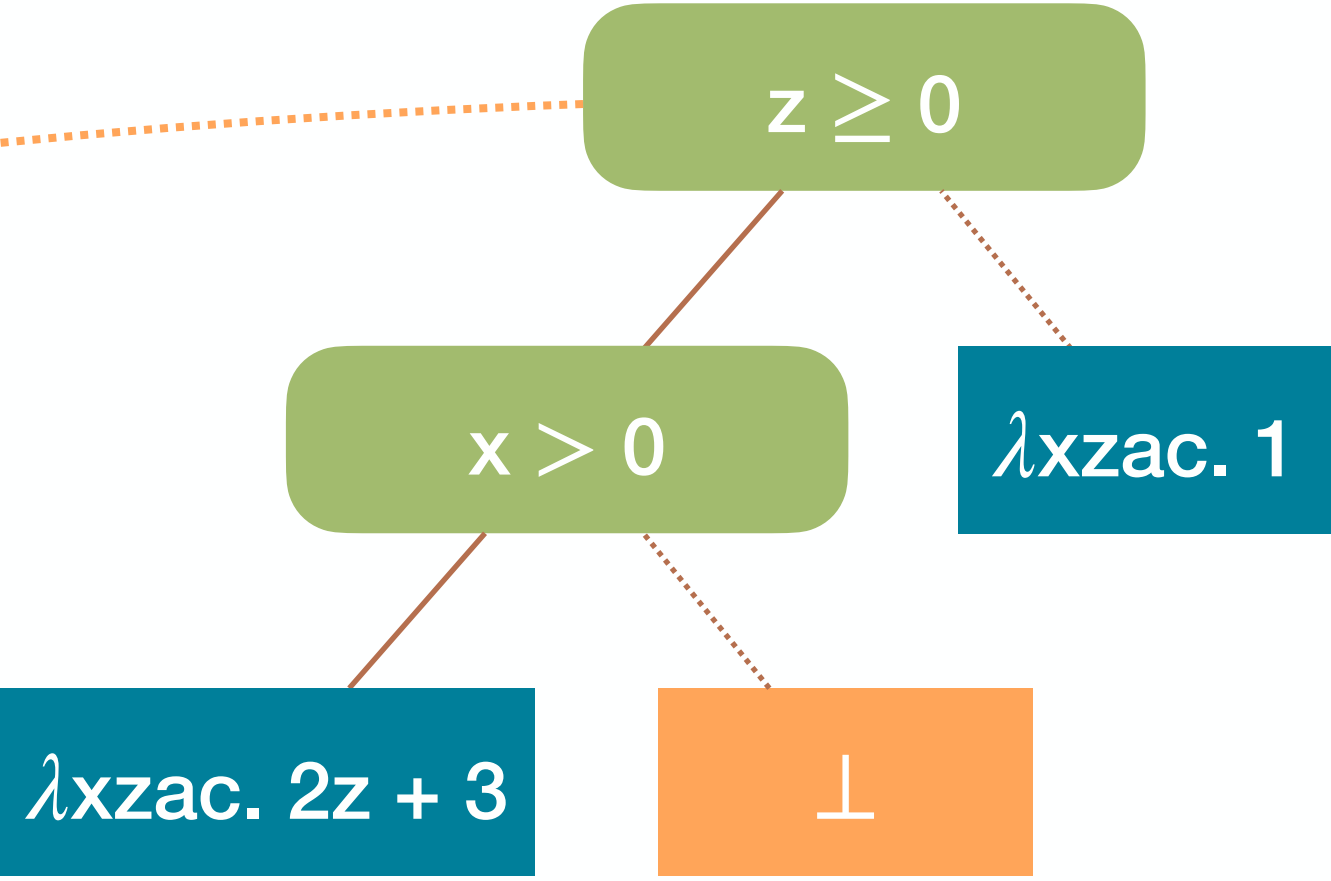
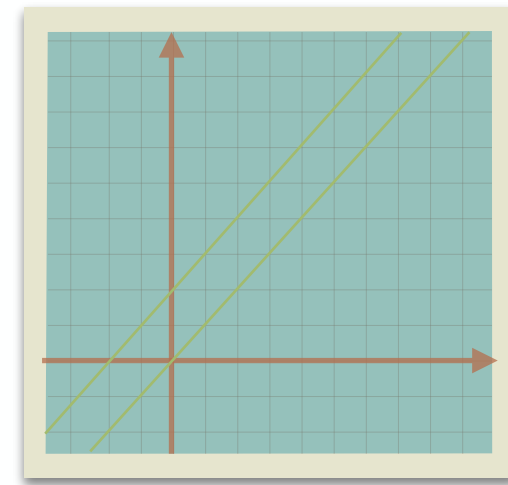
Loops

function f(x) {

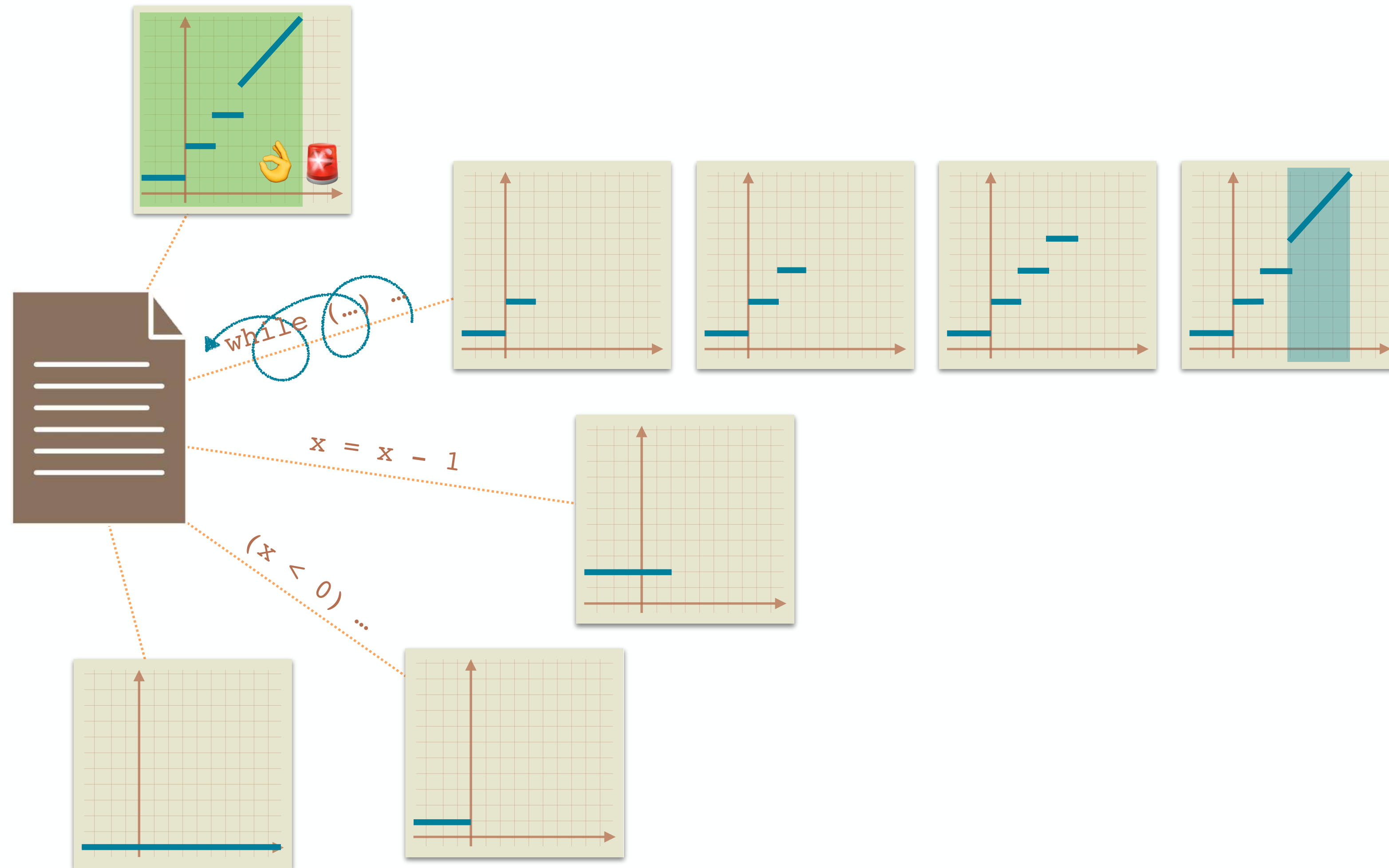
```

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



Termination Resilience Static Analysis

Approximation Join or Resilience Join?

function $f(x)$ {

1 $a \leftarrow [-\infty, +\infty]$

2 $z \leftarrow 10$

3 **if** ($a \cdot a \geq 0$) **then**

while ⁴($z \geq 0$) **do**

⁵ $z \leftarrow z - x$

od⁶

else

while ⁷($z \geq x$) **do**

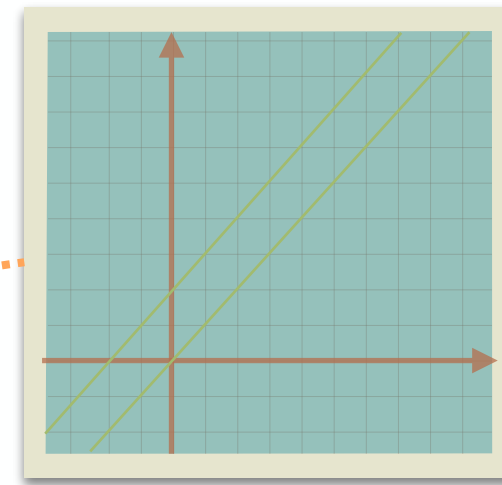
⁸ $c \leftarrow [-2, 1]$

⁹ $z \leftarrow z + c$

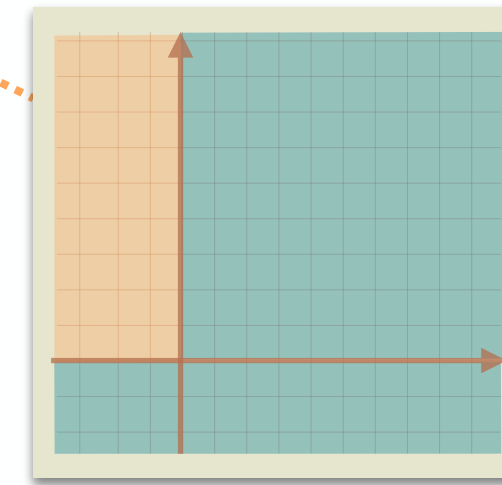
od¹⁰

fi

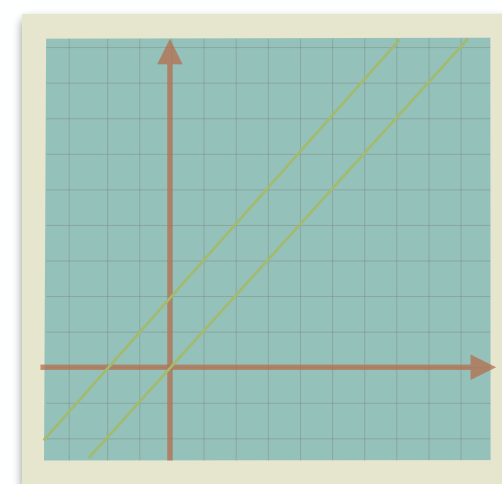
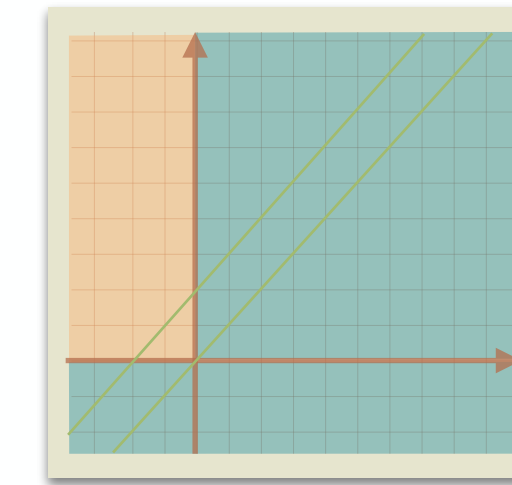
}¹¹



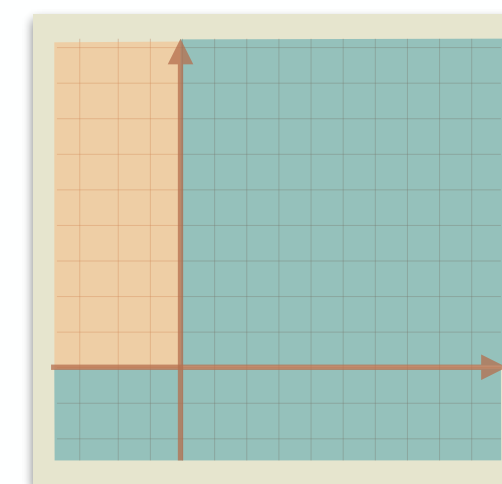
\vee



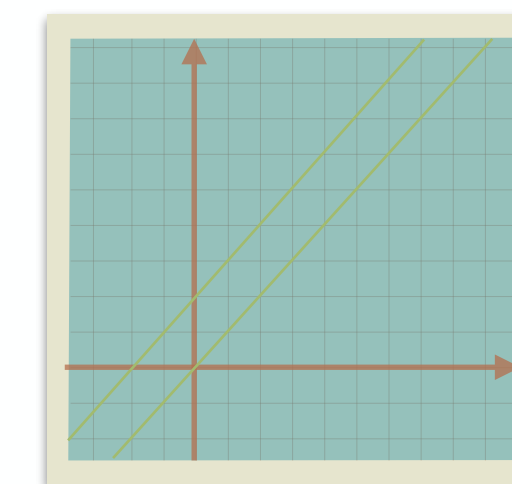
=



\vee



=

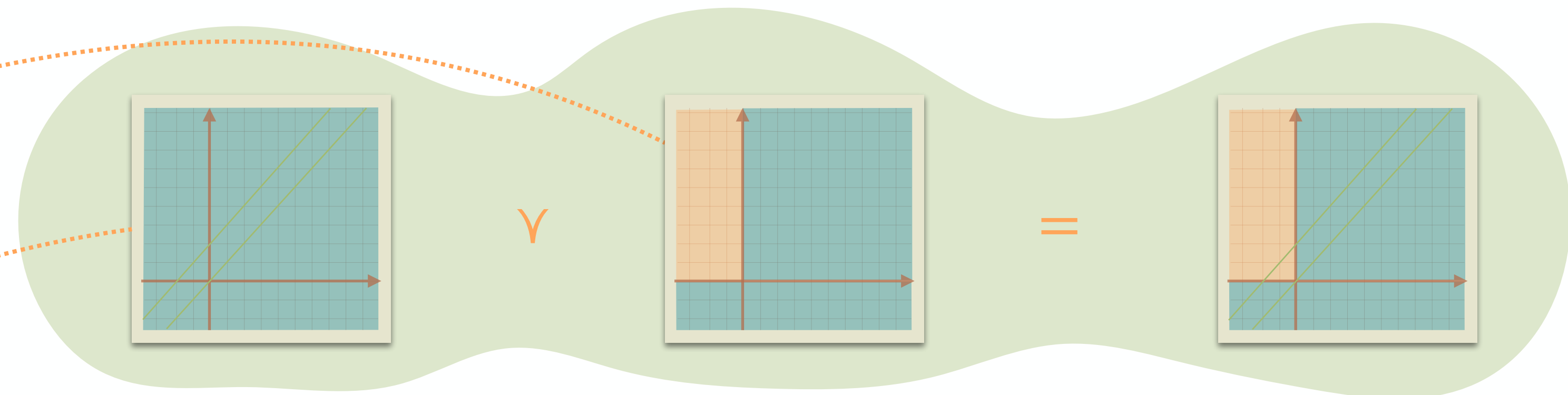


Termination Resilience Static Analysis

Approximation Join or Resilience Join?

function $f(x)$ {

```
1  $a \leftarrow [-\infty, +\infty]$   
2  $z \leftarrow 10$   
3 if ( $a \cdot a \geq 0$ ) then  
   while  $z \geq 0$  do  
     5  $z \leftarrow z - x$   
   od  
 else  
   while  $z \geq x$  do  
     8  $c \leftarrow [-2, 1]$   
     9  $z \leftarrow z + c$   
   od  
 fi  
}11
```



Termination Resilience Static Analysis

function $f(x)$ {

1 $a \leftarrow [-\infty, +\infty]$

2 $z \leftarrow 10$

3 if $(a \cdot a \geq 0)$ then

while $z \geq 0$ do

5 $z \leftarrow z - x$

od

else

while $z \geq x$ do

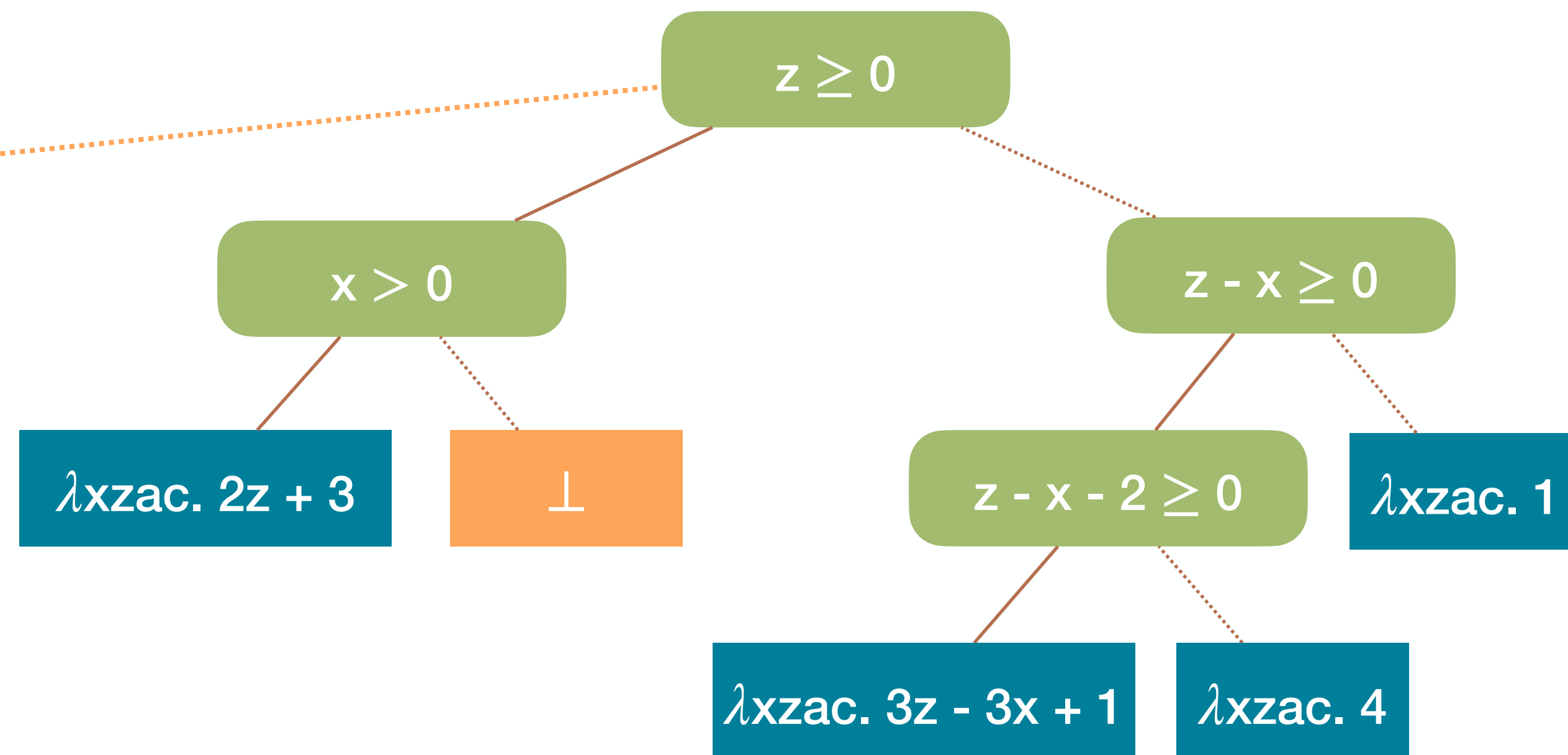
8 $c \leftarrow [-2, 1]$

9 $z \leftarrow z + c$

od

fi

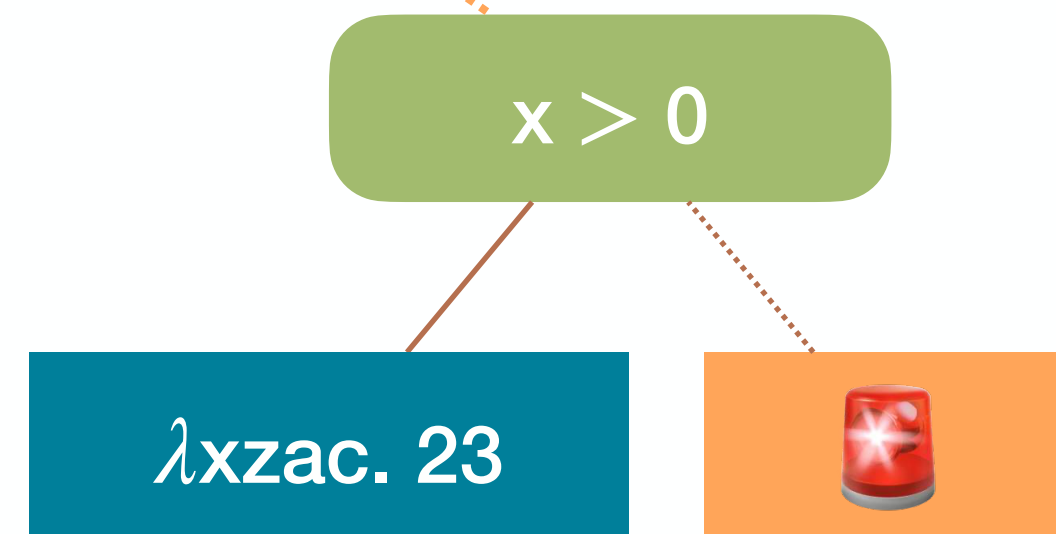
}¹¹



Termination Resilience Static Analysis

function $f(x)$ {

```
1  $a \leftarrow [-\infty, +\infty]$ 
2  $z \leftarrow 10$ 
3 if ( $a \cdot a \geq 0$ ) 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
```



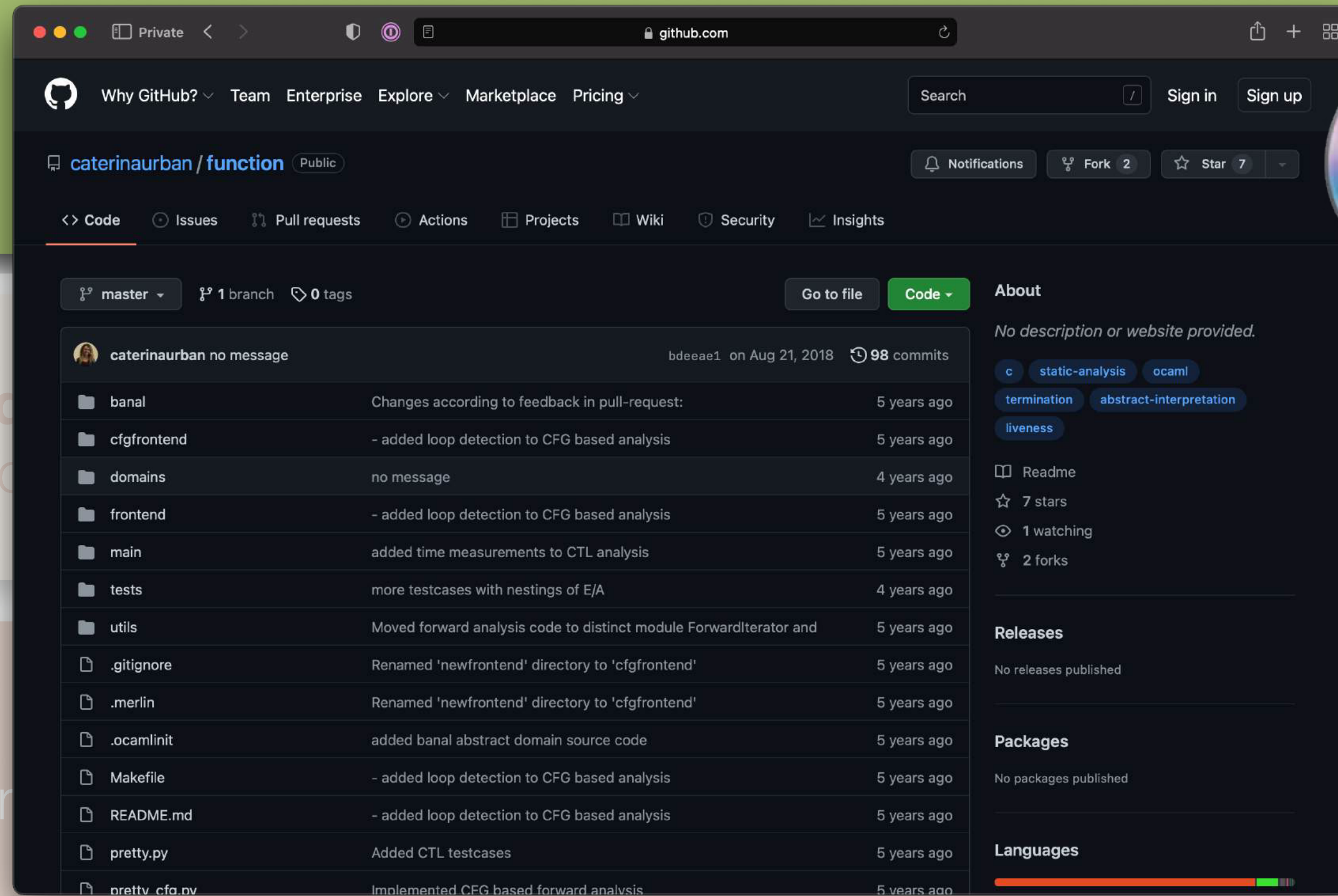
Termination Resilience Static Analysis

3-Step Recipe

practical tools
targeting specific programs

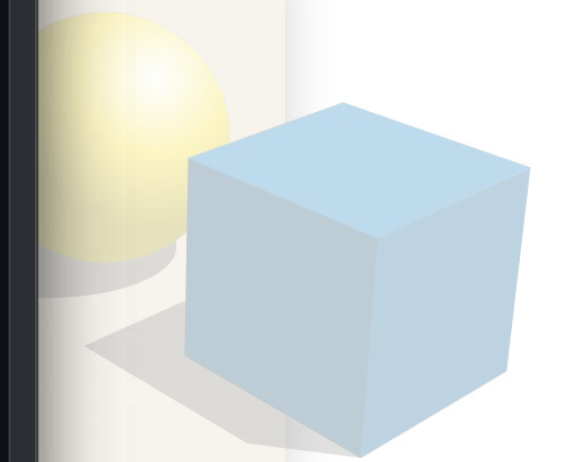
abstract semantics, abstract c
algorithmic approaches to dec

concrete semantics
mathematical models of the pr



The screenshot shows a GitHub repository page for 'caterinaurban/function'. The repository is public and has 7 stars and 2 forks. The commit history is visible, showing various updates to the codebase over time. The repository includes several directories and files, such as 'banal', 'cfgfrontend', 'domains', 'frontend', 'main', 'tests', 'utils', '.gitignore', '.merlin', '.ocamlinit', 'Makefile', 'README.md', 'pretty.py', and 'pretty_cfg.py'.

File/Directory	Commit Message	Time Ago
banal	Changes according to feedback in pull-request:	5 years ago
cfgfrontend	- added loop detection to CFG based analysis	5 years ago
domains	no message	4 years ago
frontend	- added loop detection to CFG based analysis	5 years ago
main	added time measurements to CTL analysis	5 years ago
tests	more testcases with nestings of E/A	4 years ago
utils	Moved forward analysis code to distinct module ForwardIterator and	5 years ago
.gitignore	Renamed 'newfrontend' directory to 'cfgfrontend'	5 years ago
.merlin	Renamed 'newfrontend' directory to 'cfgfrontend'	5 years ago
.ocamlinit	added banal abstract domain source code	5 years ago
Makefile	- added loop detection to CFG based analysis	5 years ago
README.md	- added loop detection to CFG based analysis	5 years ago
pretty.py	Added CTL testcases	5 years ago
pretty_cfg.py	Implemented CFG based forward analysis	5 years ago



Termination Resilience Static Analysis

Open Questions

practical tools

Termination Resilience Static Analysis

3-Step Recipe

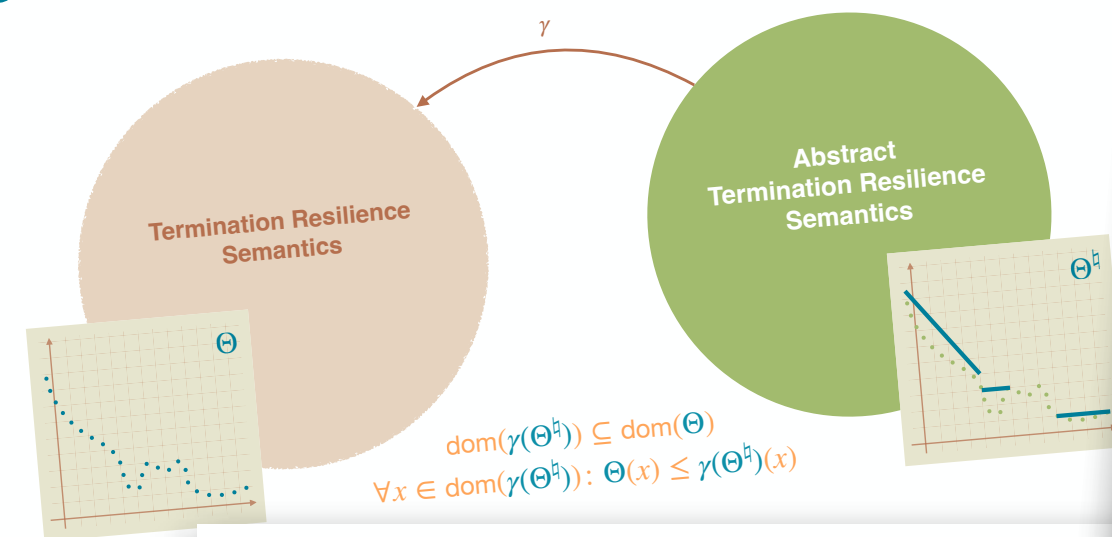
- practical tools
targeting specific programs
- abstract semantics, abstract domains
algorithmic approaches to deal with
- concrete semantics
mathematical models

Experimental Evaluation

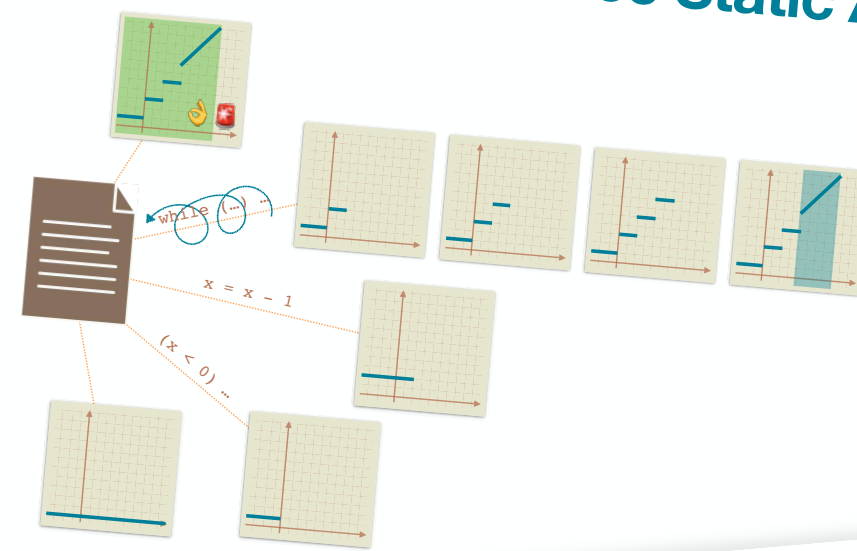
Benchmark	Property	Verified	Alarms	TO	Time
SV-COMP 2024	Termination	0	119	0	3.5s
	Termination Resilience	61	58	0	3.6s
Raad et al @ OOPSLA 2024	Termination	0	36	0	0.5s
	Termination Resilience	16	20	0	0.5s
Shi et al. @ FSE 2022	Termination	0	85	0	2.0s
	Termination Resilience	57	28	0	2.2s
Benchmark	Property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

abstract semantics
abstract domains

Piecewise-Defined Ranking Functions

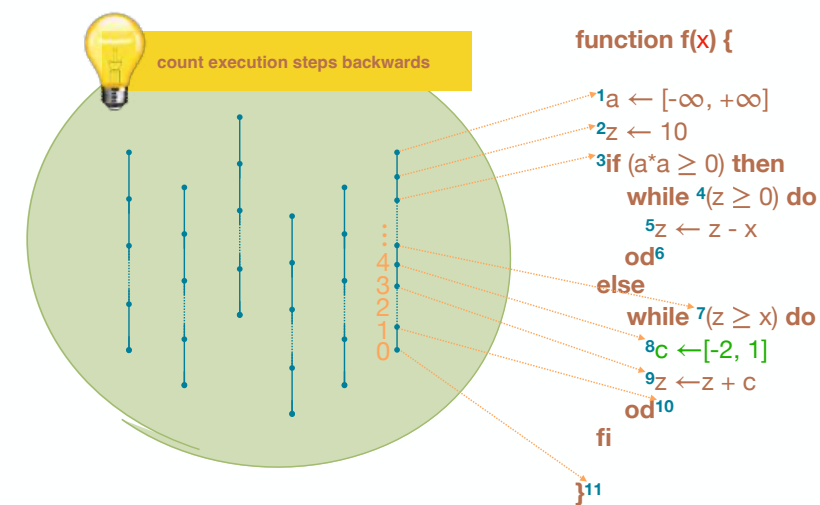


Termination Resilience Static Analysis

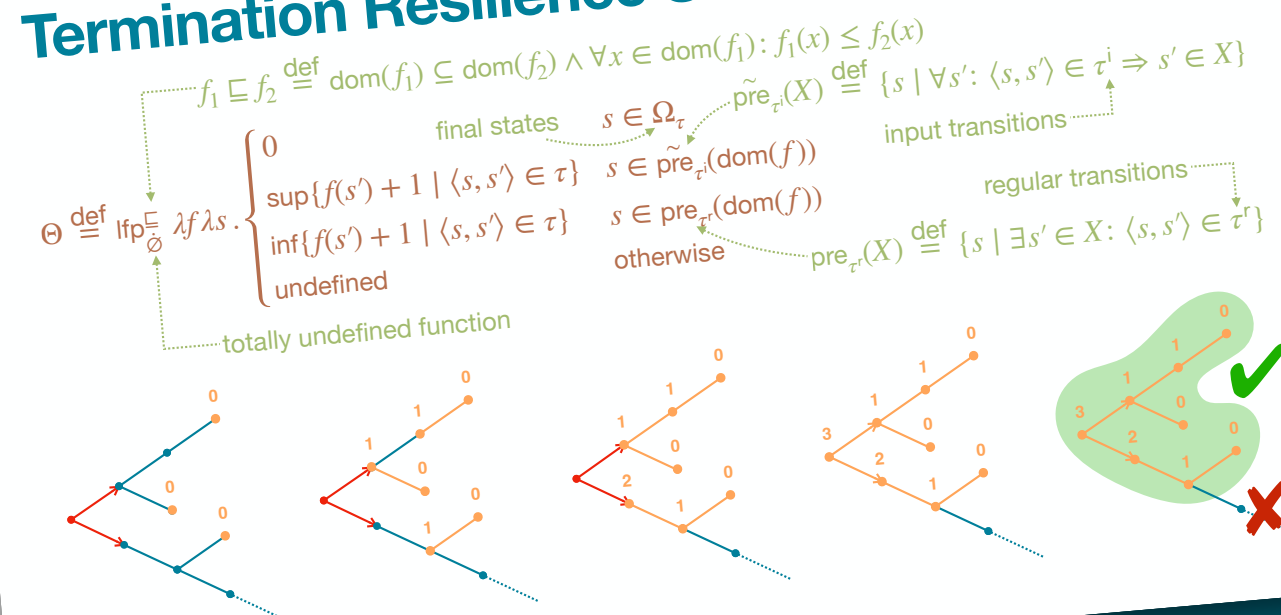


concrete semantics

Termination Resilience Semantics



Termination Resilience Semantics



Termination Resilience Static Analysis

Approximation Join or Resilience Join?

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

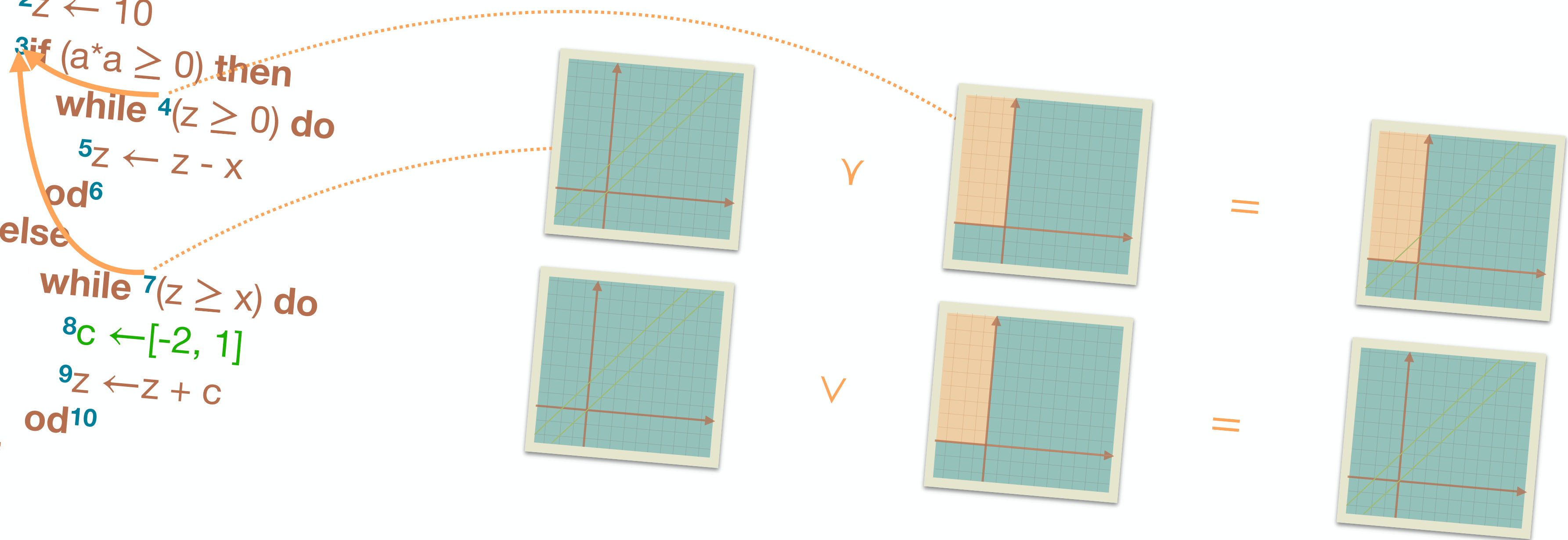
$^8 c \leftarrow [-2, 1]$

$^9 z \leftarrow z + c$

 od¹⁰

fi

}¹¹



Termination (Resilience) Static Analysis

Pointer-Manipulating Programs

```
function f(*a, n) {
```

```
    1 *p ← a
```

```
    while 2(p < a + n) then
```

```
        3 if (*p = 0) do
```

```
            4 p ← a
```

```
        else
```

```
            5 p ← p + 1
```

```
        fi
```

```
    od6
```

```
}7
```

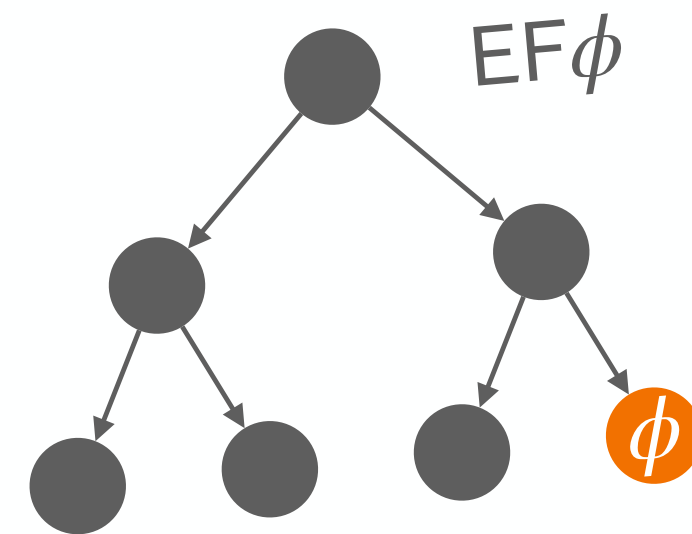
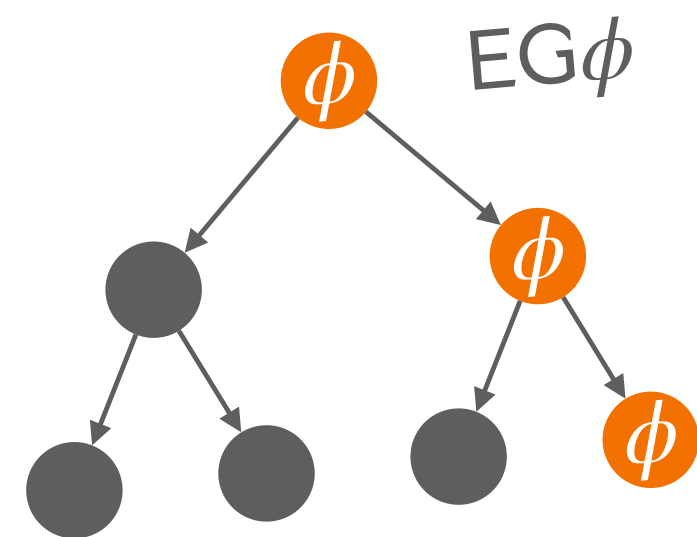
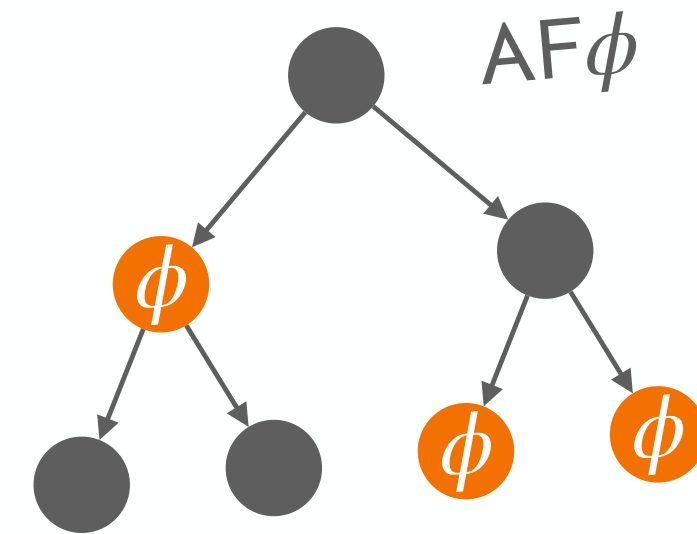
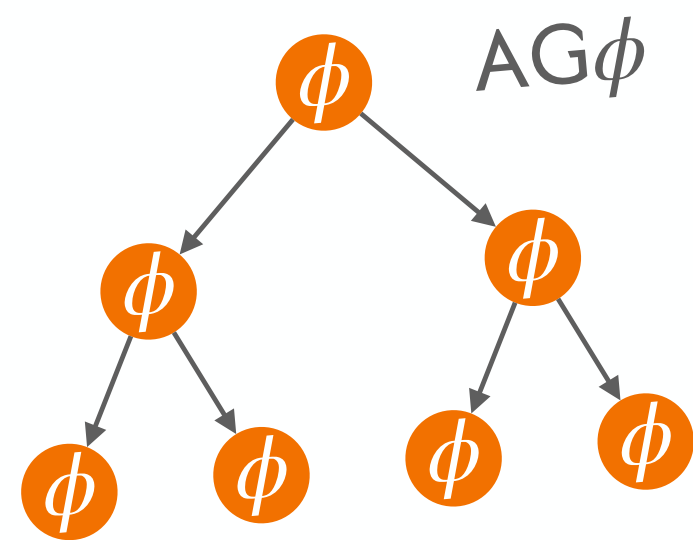
Computation Tree Logic (CTL)

Branching Temporal Logic

$\phi ::= a \mid \neg\phi \mid \phi \wedge \phi \mid \phi \vee \phi \mid AX\phi \mid AG\phi \mid A(\phi U \phi) \mid EX\phi \mid EG\phi \mid E(\phi U \phi)$

$AF\phi \equiv A(\text{true} U \phi)$

$EF\phi \equiv E(\text{true} U \phi)$



Termination Resilience Static Analysis

Open Questions

practical tools

Termination Resilience Static Analysis

3-Step Recipe

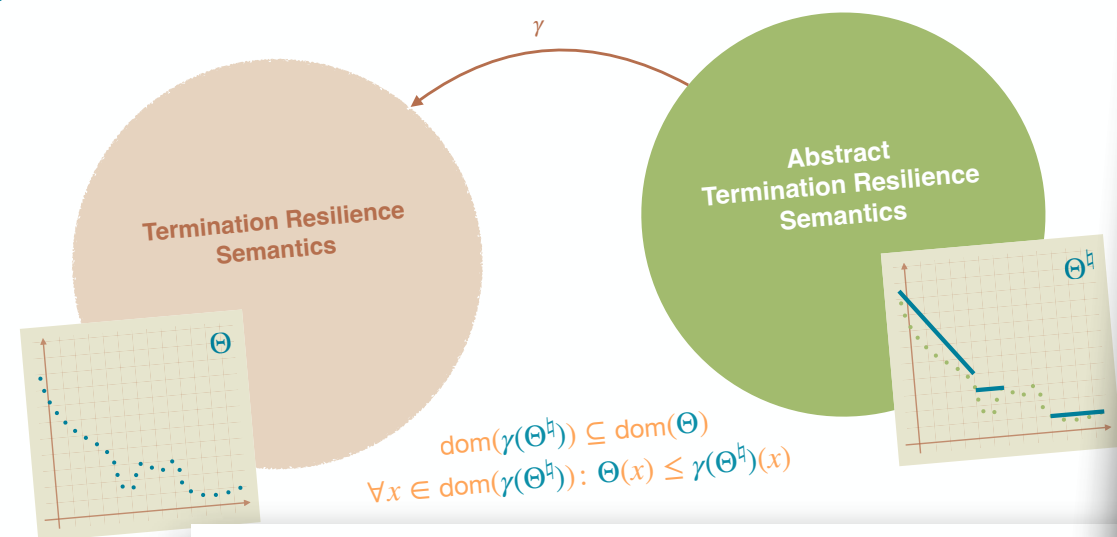
- practical tools
targeting specific programs
- abstract semantics, abstract domains
algorithmic approaches to deal with uncertainty
- concrete semantics
mathematical models

Experimental Evaluation

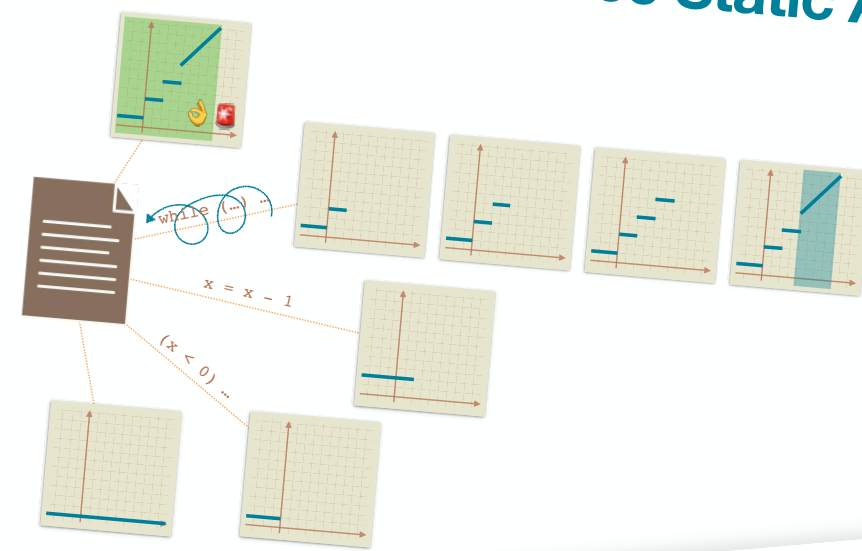
Benchmark	Property	Verified	Alarms	TO	Time
SV-COMP 2024	Termination	0	119	0	3.5s
	Termination Resilience	61	58	0	3.6s
Raad et al @ OOPSLA 2024	Termination	0	36	0	0.5s
	Termination Resilience	16	20	0	0.5s
Shi et al. @ FSE 2022	Termination	0	85	0	2.0s
	Termination Resilience	57	28	0	2.2s
Benchmark	Property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

abstract semantics
abstract domains

Piecewise-Defined Ranking Functions

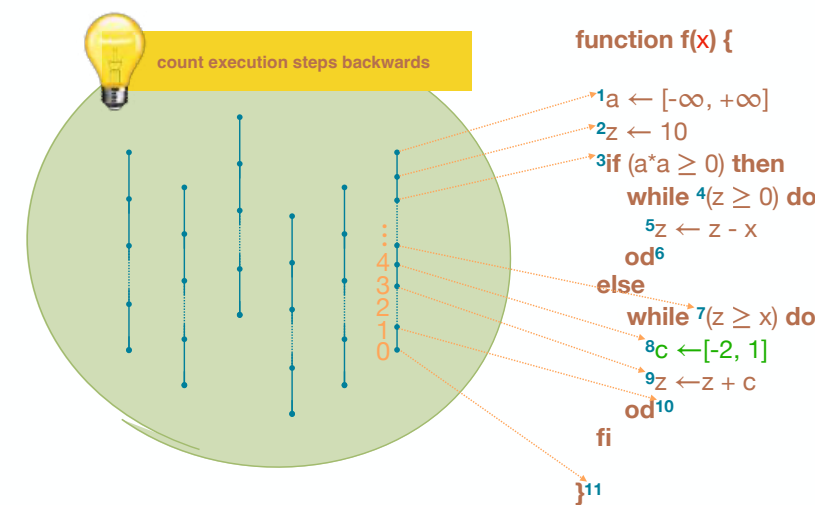


Termination Resilience Static Analysis

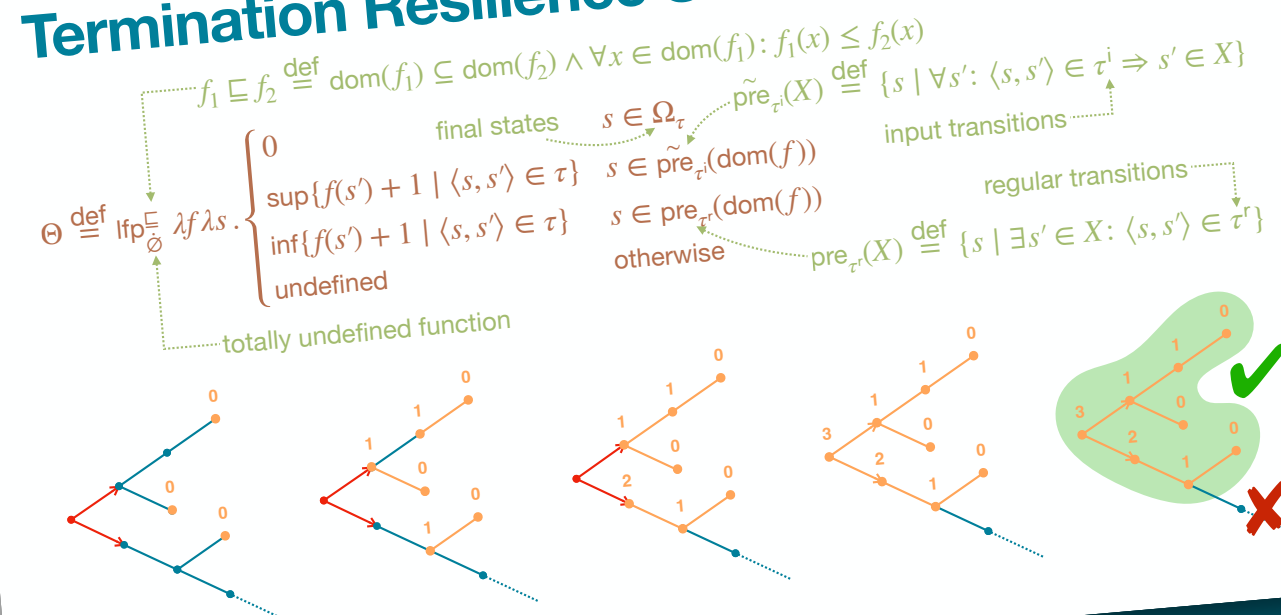


concrete semantics

Termination Resilience Semantics



Termination Resilience Semantics



THANKS!