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...
  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 ≥ 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 $x = 0$ (while loop at 4)

← diverges when $c \geq 0$ (while loop at 7)

← non-deterministic value choice (at 8)

Robust Non-Termination

∃ Input ∀ Non-Deterministic Choices : Program Diverges

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

}11
```

Termination Resilience

∀ Inputs ∃ 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]
        9z ←z + c
      od10
  fi

}11
```

👌 ⟵ terminates when **c < 0**, **independently of the value of x**

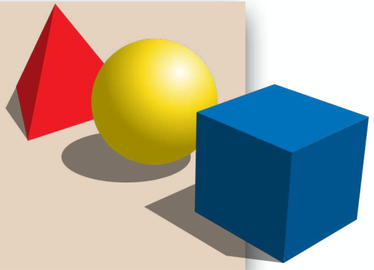
angelic non-determinism

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

€ 10 +
€ 40 +
€ 30 +
€ 10

€ 90

COMPLETENESS

€ 9.95 +
€ 35.85 +
€ 27.95 +
€ 4.85

€ 78.60

FALSE ALARM

Termination Resilience Static Analysis

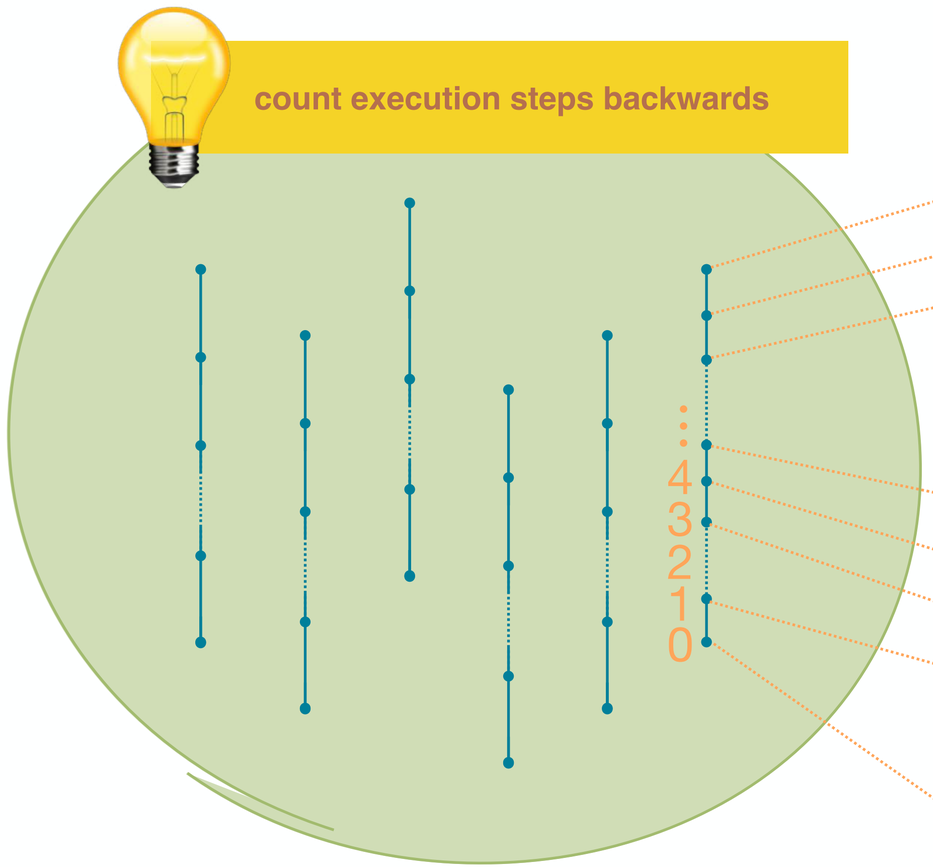
3-Step Recipe

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




```
function f(x) {

  1a ← [-∞, +∞]
  2z ← 10
  3if (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

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

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

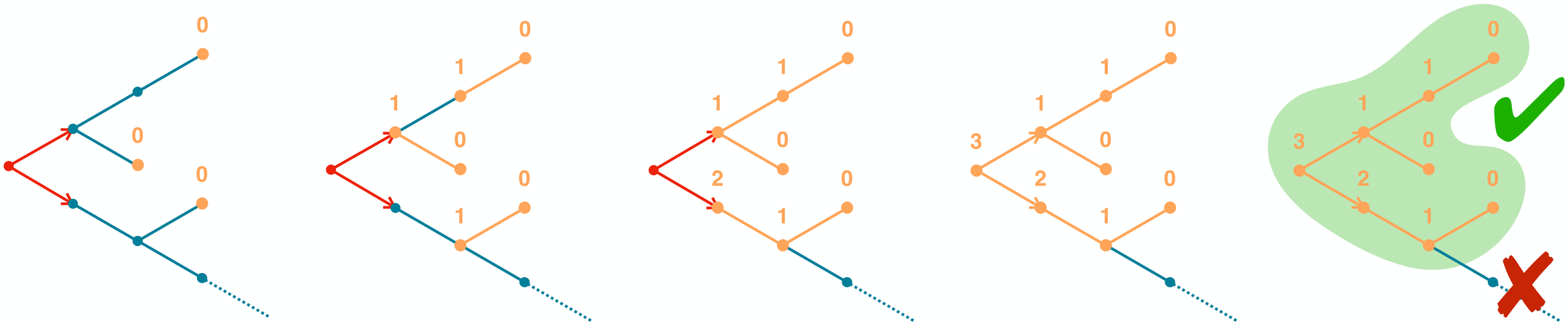
totally undefined function

$$\widetilde{\mathrm{pre}}_{\tau^{\mathsf{i}}}(X) \overset{\text{def}}{=} \{s \mid \forall s' \colon \langle s, s' \rangle \in \tau^{\mathsf{i}} \Rightarrow s' \in X\}$$

input transitions

$$\mathrm{pre}_{\tau^{\mathsf{r}}}(X) \overset{\text{def}}{=} \{s \mid \exists s' \in X \colon \langle s, s' \rangle \in \tau^{\mathsf{r}}\}$$

regular transitions

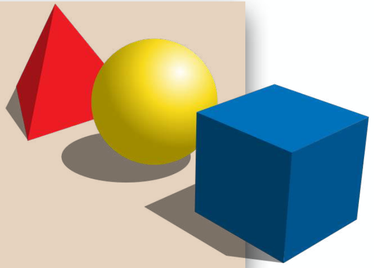


Termination Resilience Static Analysis

3-Step Recipe

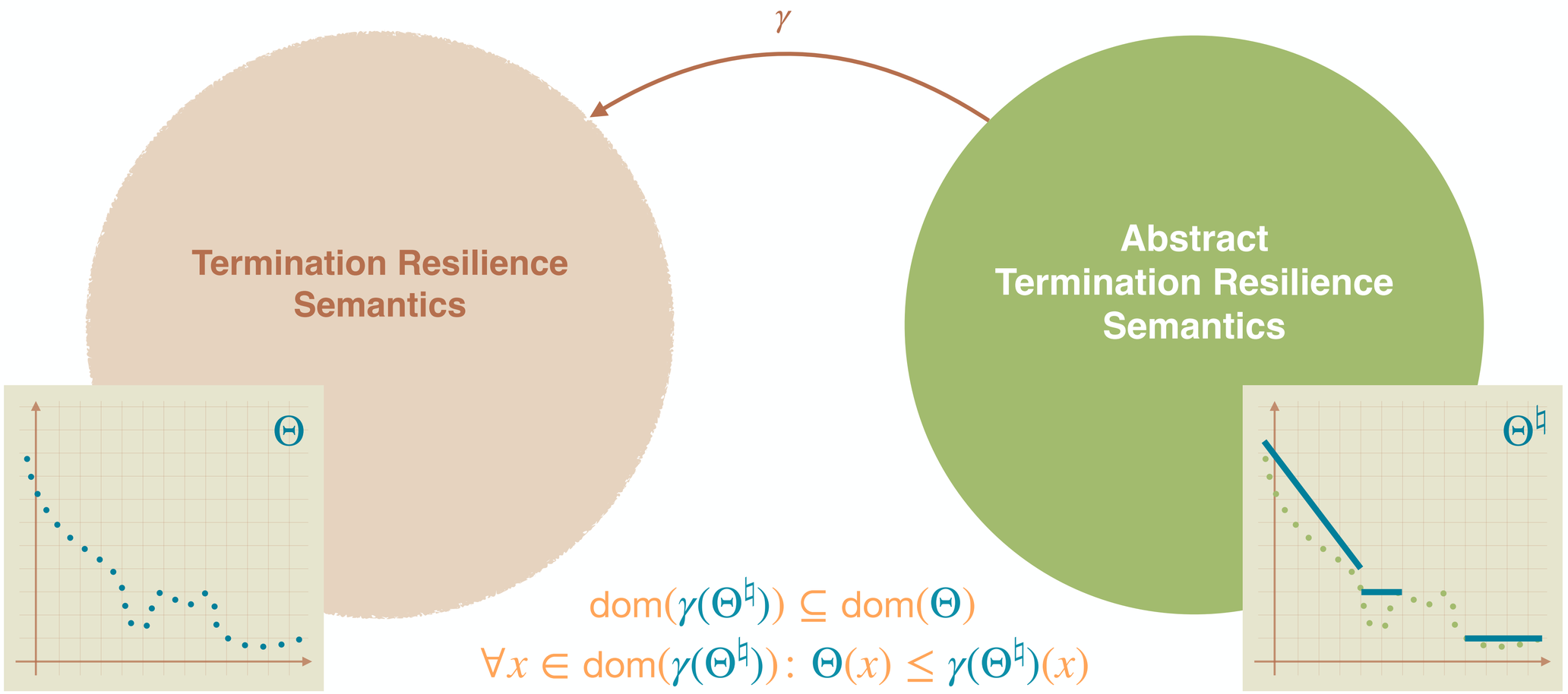
practical tools
targeting specific programs

abstract semantics, abstract domains
algorithmic approaches to decide program properties

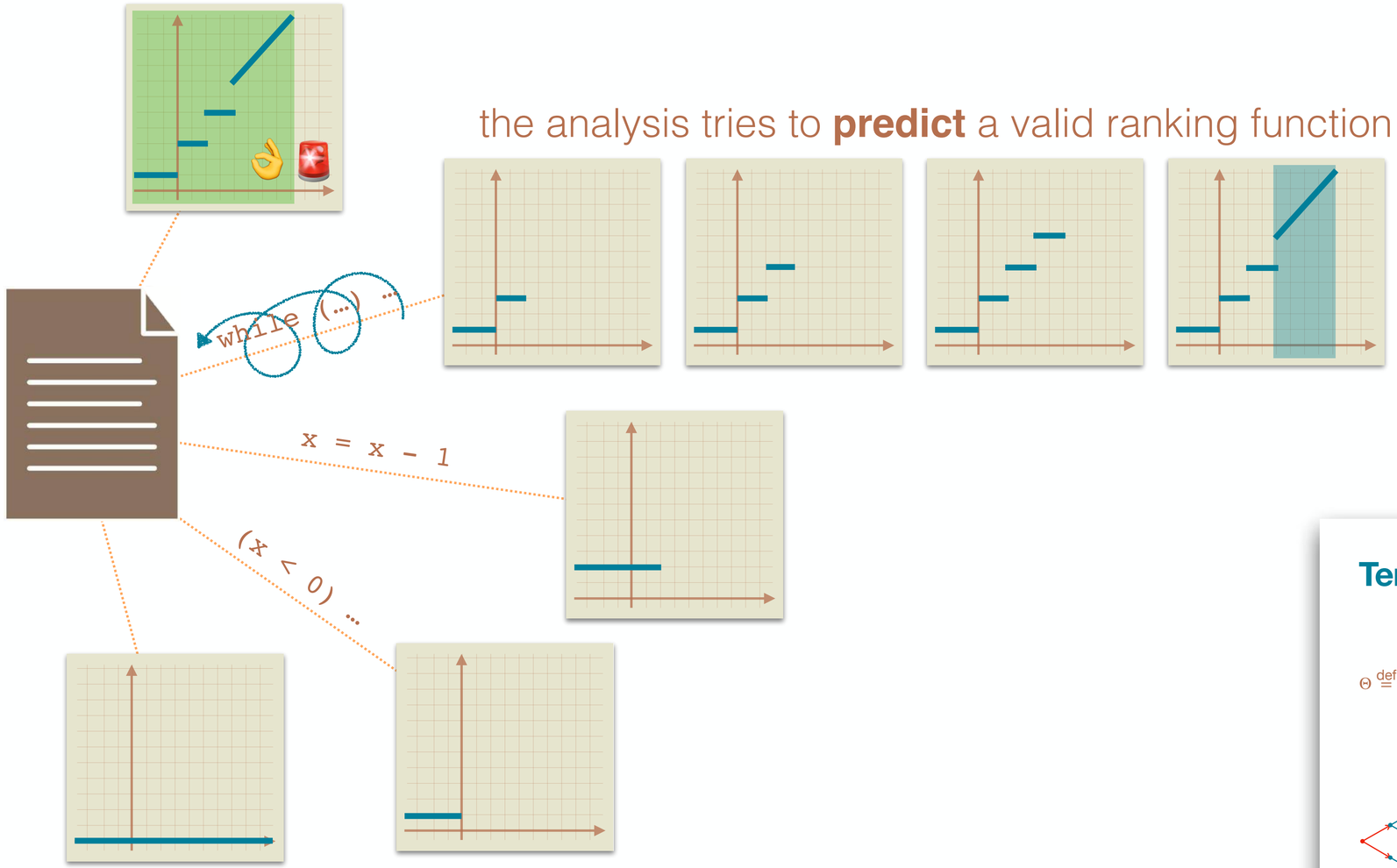


concrete semantics
mathematical models of the program behavior

Piecewise-Defined Ranking Functions



Termination Resilience Static Analysis



Termination Resilience Semantics

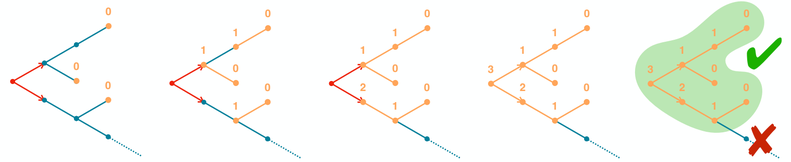
$$f_1 \sqsubseteq f_2 \stackrel{\text{def}}{=} \mathrm{dom}(f_1) \subseteq \mathrm{dom}(f_2) \wedge \forall x \in \mathrm{dom}(f_1) \colon f_1(x) \leq f_2(x)$$

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

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

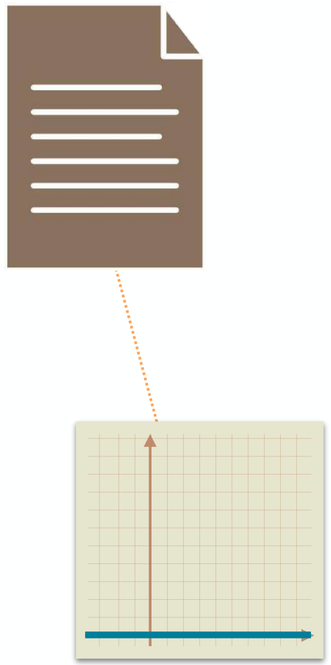
$$\mathrm{pre}_{\tau^\mathrm{r}}(X) \stackrel{\text{def}}{=} \{s \mid \exists s' \in X \colon \langle s, s' \rangle \in \tau^\mathrm{r}\} \quad \text{regular transitions}$$

totally undefined function



13

Termination Resilience Static Analysis

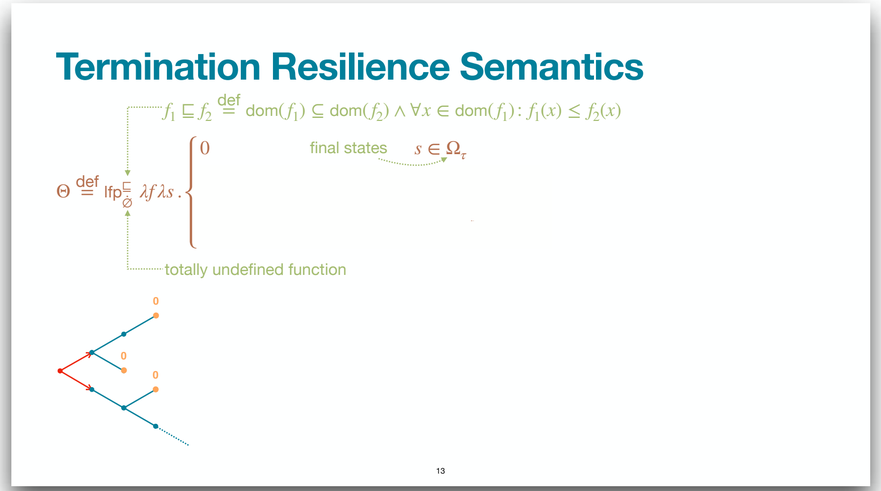


Termination Resilience Static Analysis

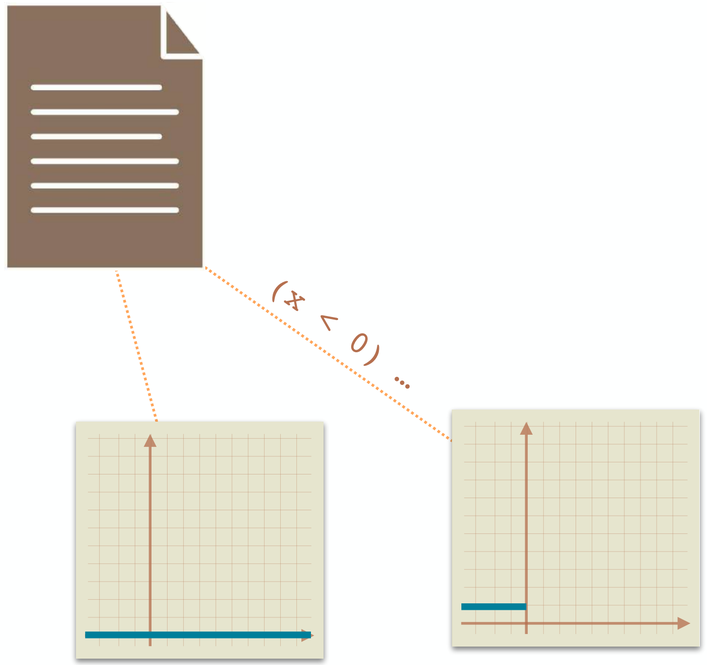
Static Backward Analysis

```
function f(x) {

  1a ← [-∞, +∞]
  2z ← 10
  3if (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
```

λxzac. 0



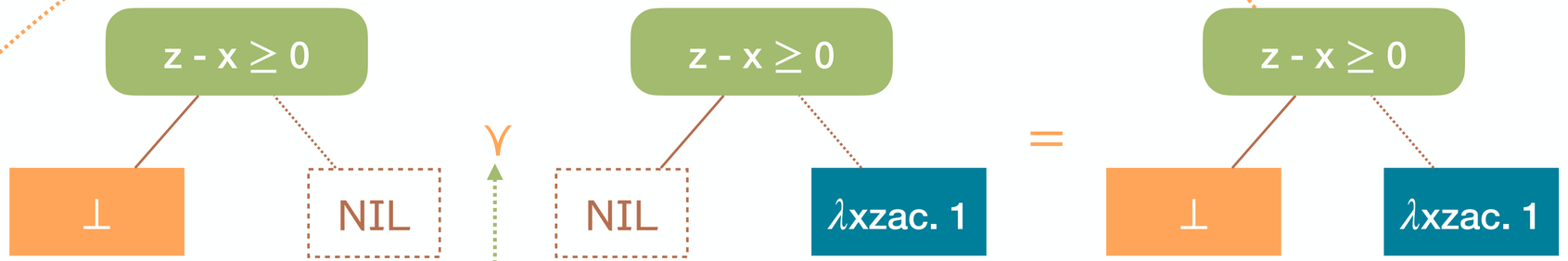
Termination Resilience Static Analysis



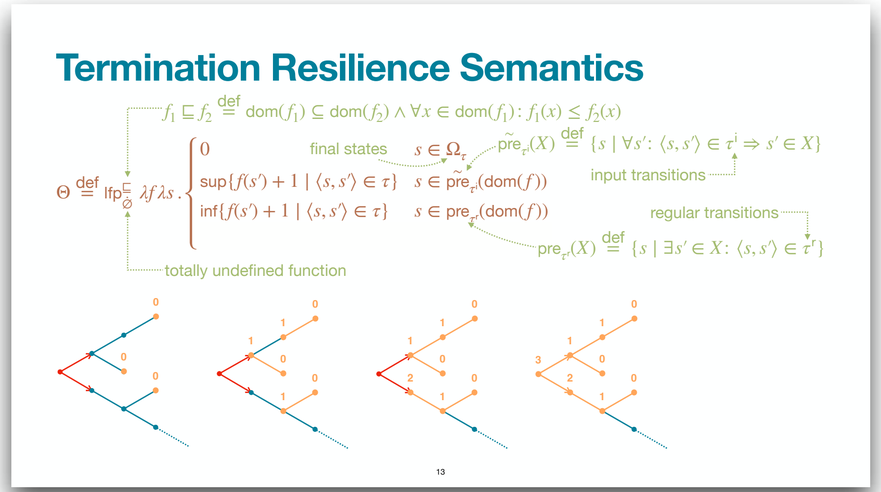
Termination Resilience Static Analysis

Boolean Conditions

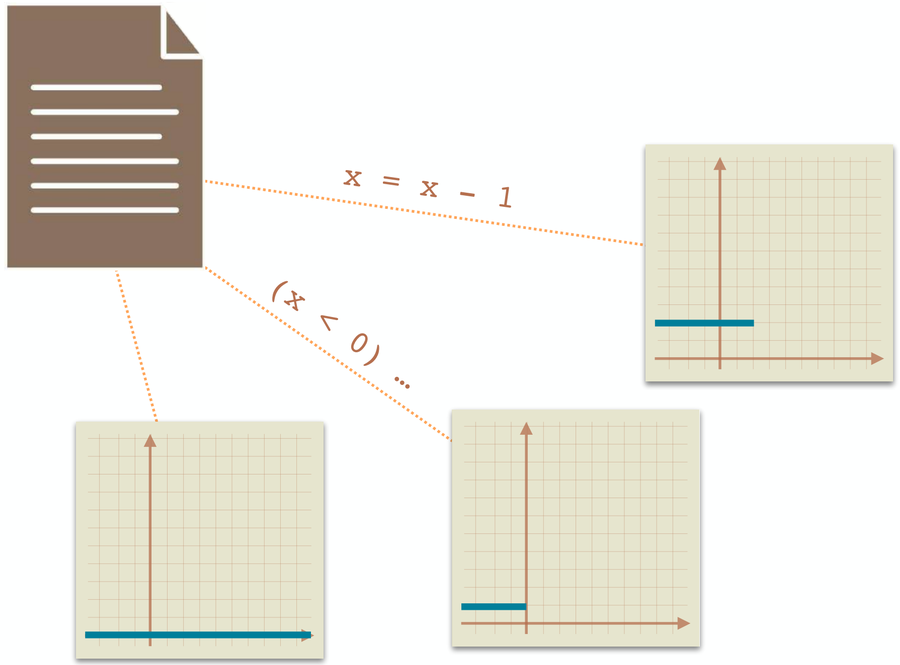
```
function f(x) {
  1a ← [-∞, +∞]
  2z ← 10
  3if (a*a ≥ 0) then
      while 4(z ≥ 0) do
        5z ← z - x
      od6
  else
      while 7(z ≥ x) do
        8c ←[-2, 1]
        9z ←z + c
      od10
  fi
}11
```



λxzac. 0



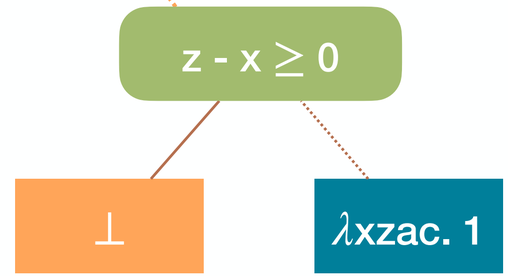
Termination Resilience Static Analysis

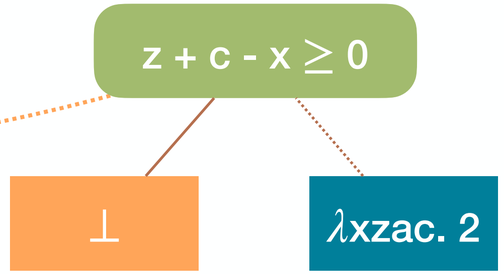


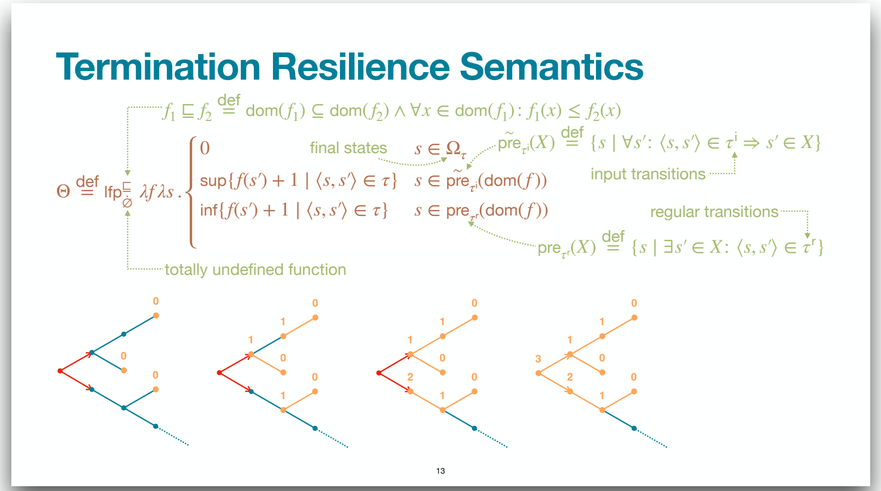
Termination Resilience Static Analysis

Variable Assignment

```
function f(x) {

  1a ← [-∞, +∞]
  2z ← 10
  3if (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
```



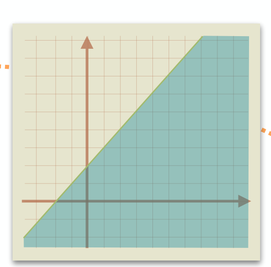


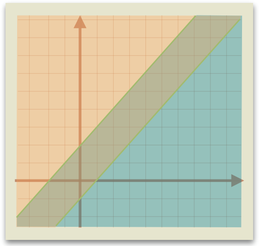


Termination Resilience Static Analysis

Non-Deterministic Variable Assignments

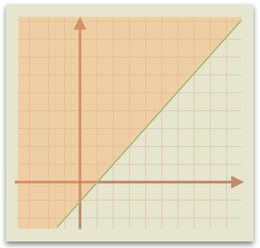
```
function f(x) {

  1a ← [-∞, +∞]
  2z ← 10
  3if (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
```

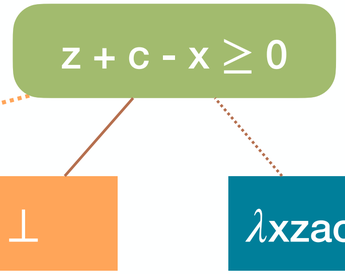


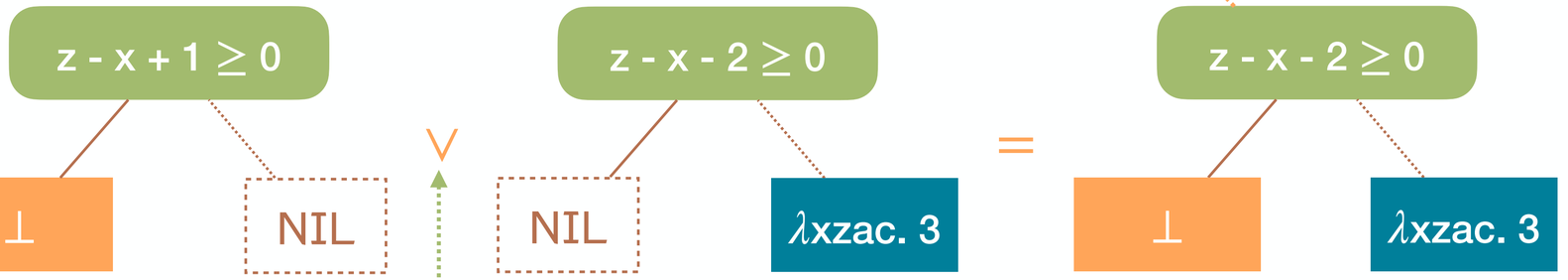


z + [-2,1] - x ≥ 0
z - x ≥ [-1,2]
z - x ≥ -1

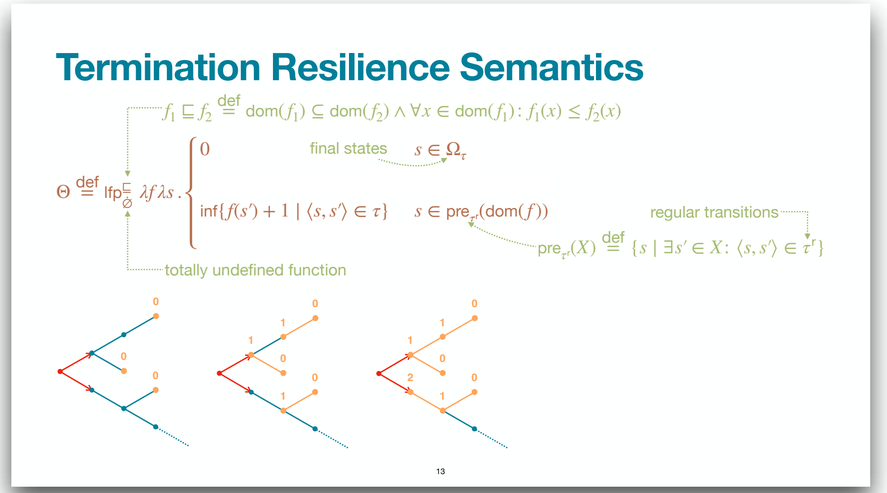
z + [-2,1] - x < 0
z - x < [-1,2]
z - x < 2





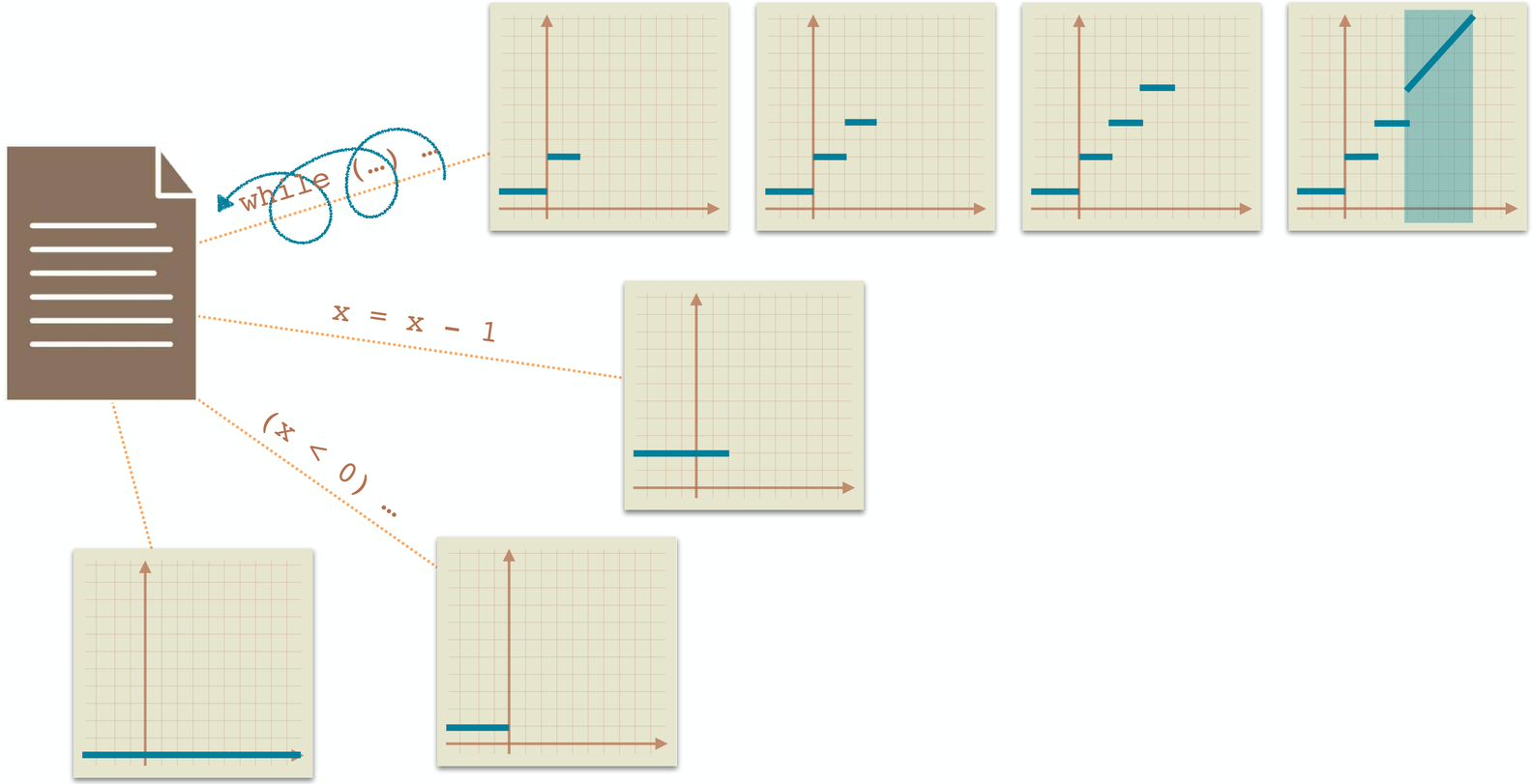


resilience join



Termination Resilience Static Analysis

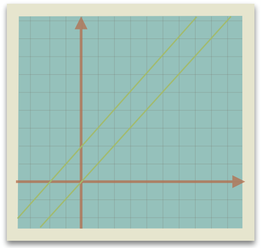
the analysis tries to **predict** a valid ranking function

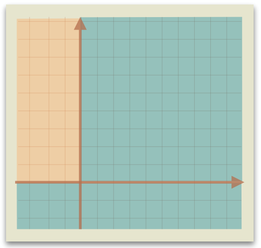


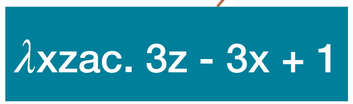
Termination Resilience Static Analysis

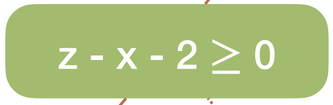
Loops

```
function f(x) {

  1a ← [-∞, +∞]
  2z ← 10
  3if (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
```

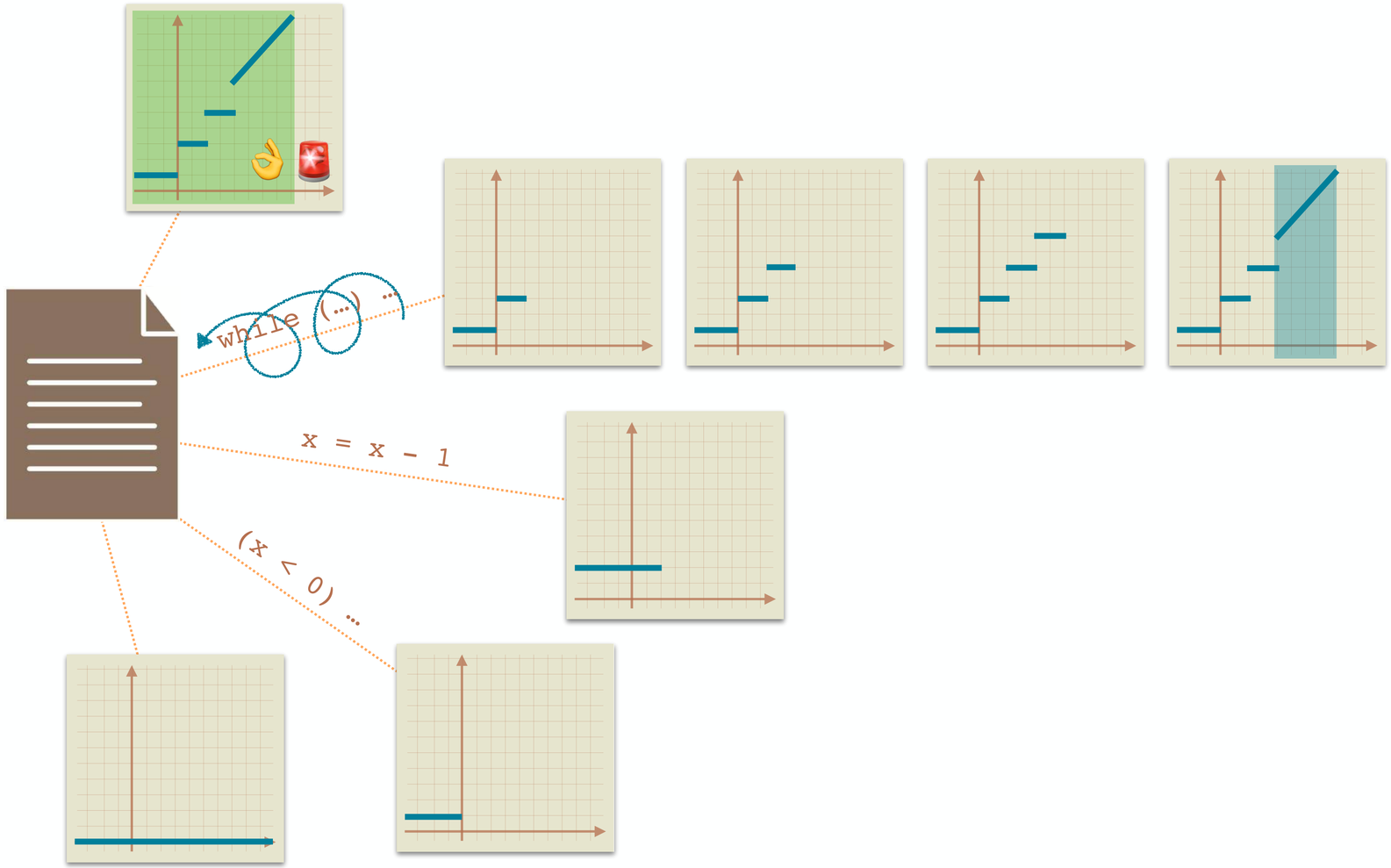








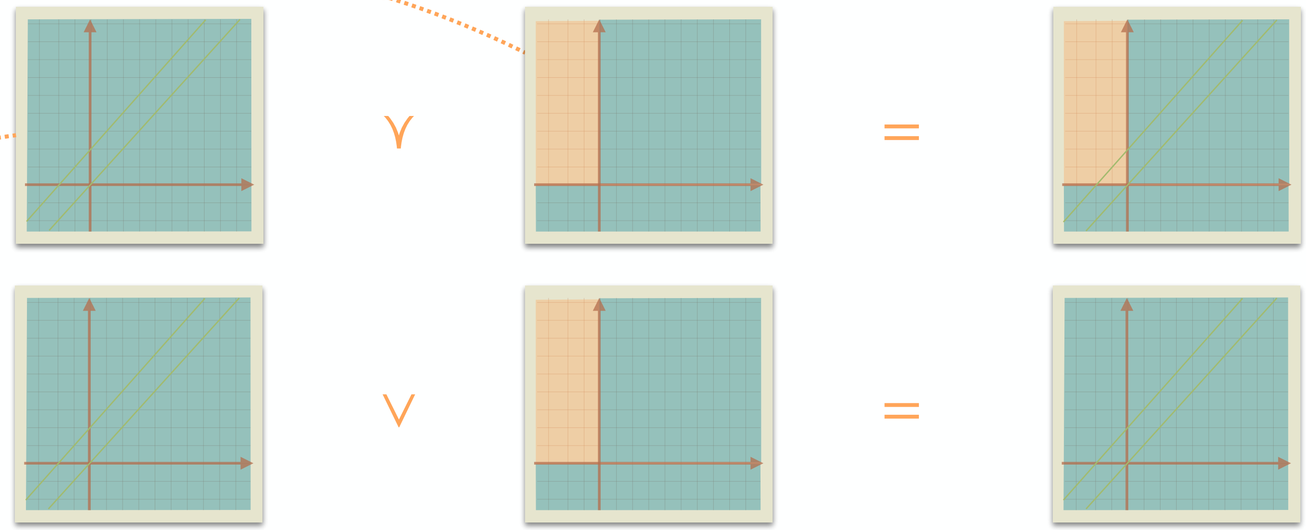
Termination Resilience Static Analysis



Termination Resilience Static Analysis

Approximation Join or Resilience Join?

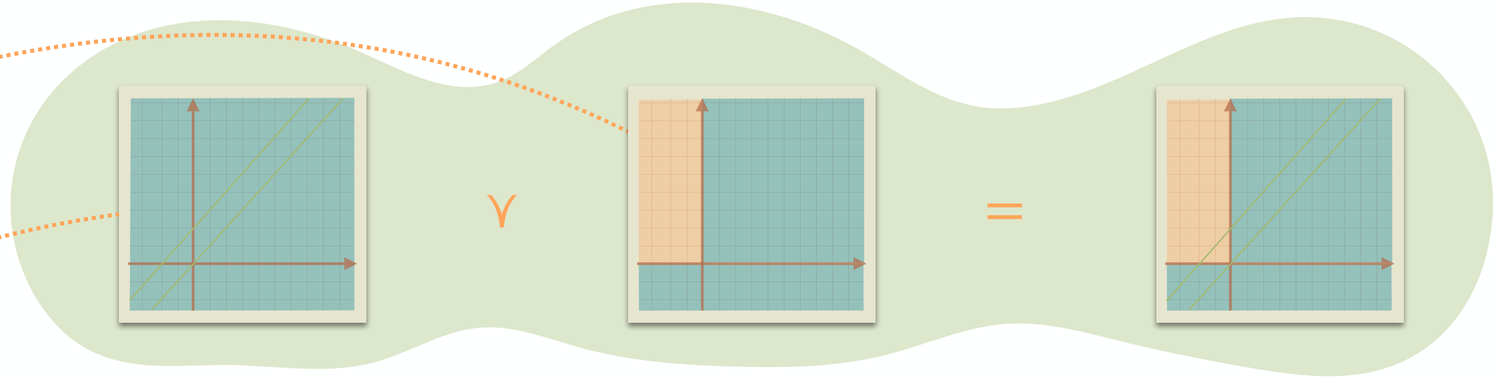
```
function f(x) {
  1a ← [-∞, +∞]
  2z ← 10
  3if (a*a ≥ 0) then
     while 4(z ≥ 0) do
       5z ← z - x
     od6
  else
     while 7(z ≥ x) do
       8c ←[-2, 1]
       9z ←z + c
     od10
  fi
}11
```



Termination Resilience Static Analysis

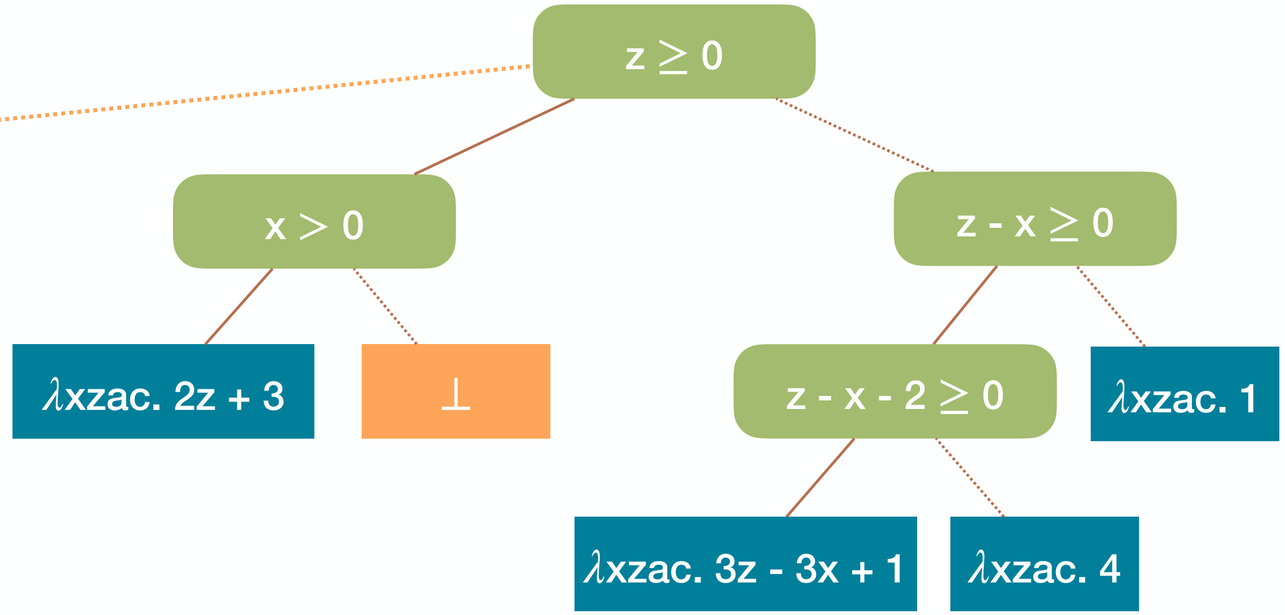
Approximation Join or Resilience Join?

```
function f(x) {
  1a ← [-∞, +∞]
  2z ← 10
  3if (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
```



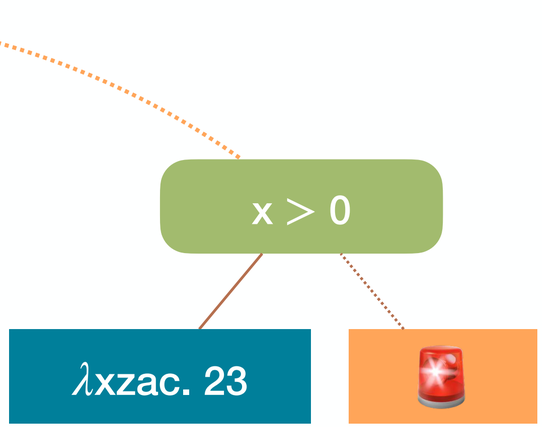
Termination Resilience Static Analysis

```
function f(x) {

  1a ← [-∞, +∞]
  2z ← 10
  3if (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
      od[6]
  else
      while [7](z ≥ x) do
        [8]c ←[-2, 1]
        [9]z ←z + c
      od[10]
  fi

}[11]
```



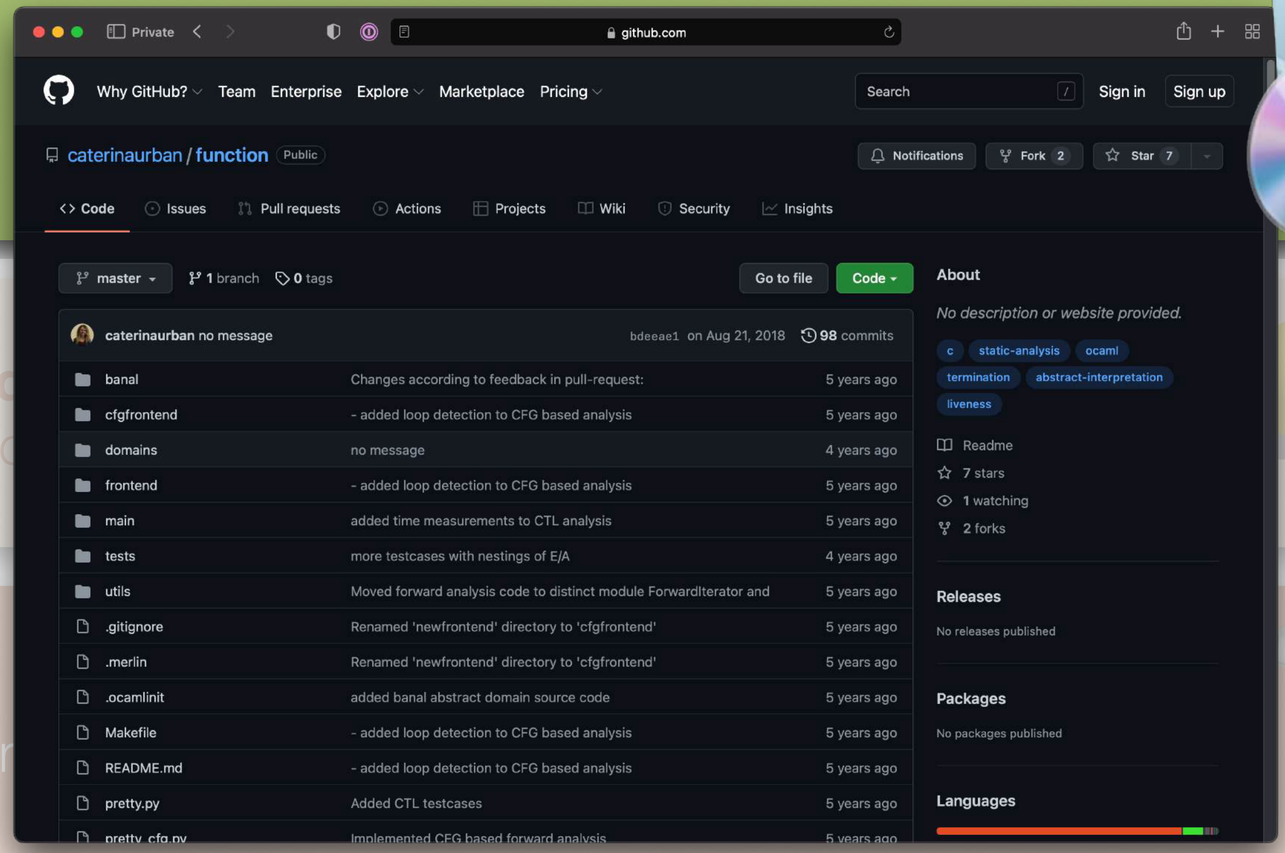
Termination Resilience Static Analysis

3-Step Recipe

practical tools
targeting specific programs

abstract semantics, abstract
algorithmic approaches to de

concrete semantics
mathematical models of the pr



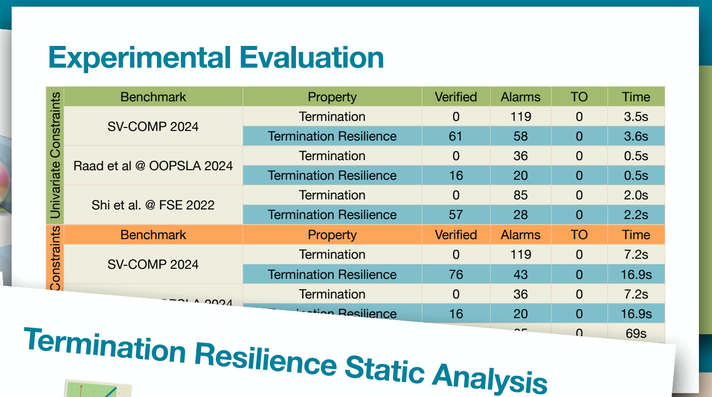
Termination Resilience Static Analysis

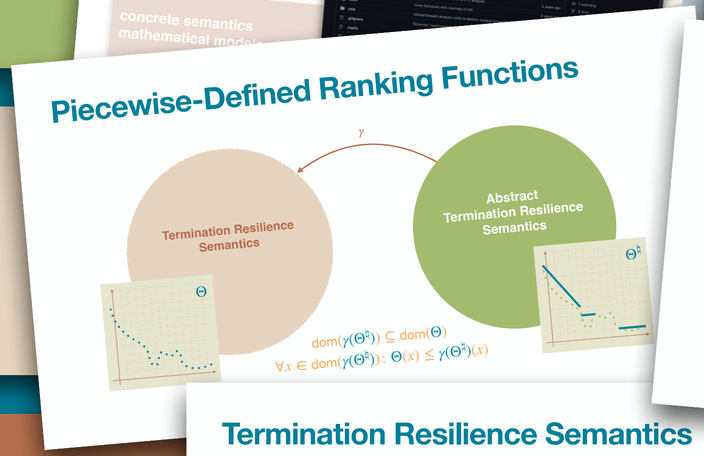
Open Questions

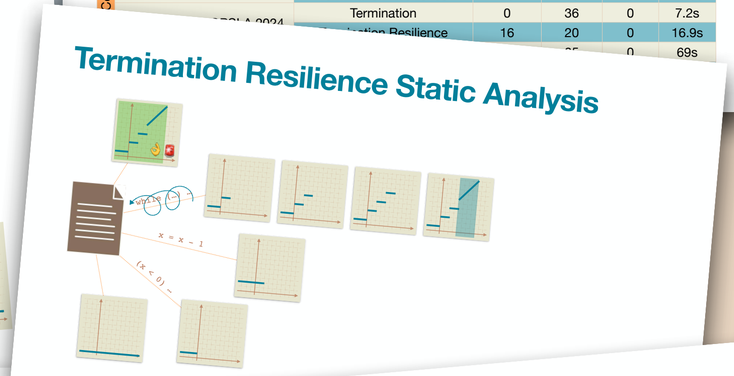
practical tools

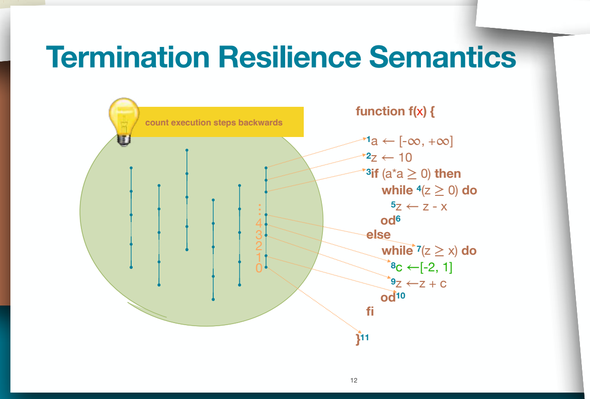
abstract semantics
abstract domains

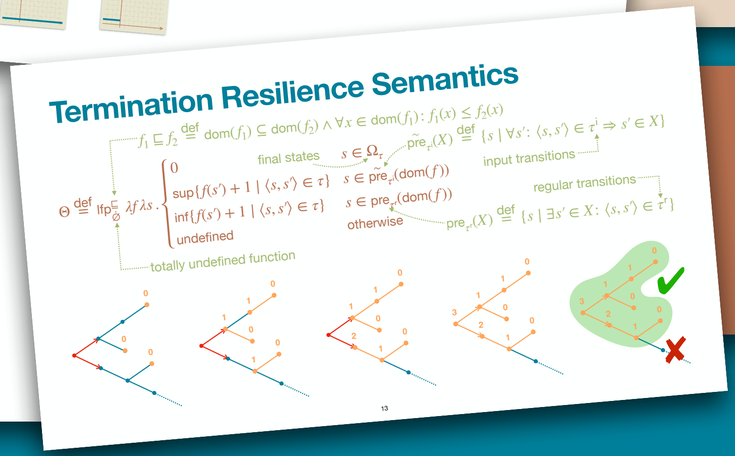
concrete semantics

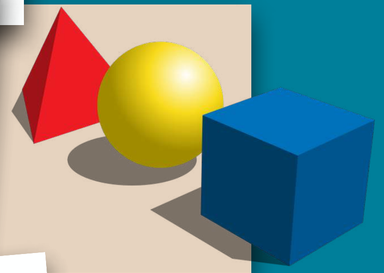








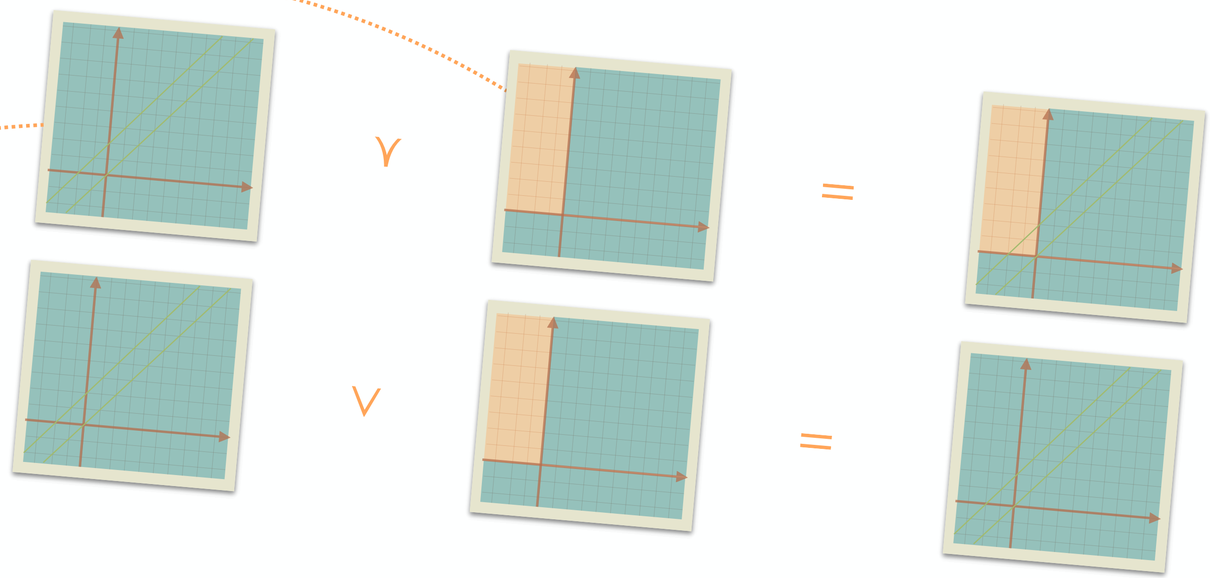




Termination Resilience Static Analysis

Approximation Join or Resilience Join?

```
function f(x) {

  1a ← [-∞, +∞]
  2z ← 10
  3if (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

Pointer-Manipulating Programs

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

  1*p ← a

  while 2(p < a + n) then
    3if (*p = 0) do
       4p ← a
    else
       5p ← p + 1
    fi
  od6

}7
```

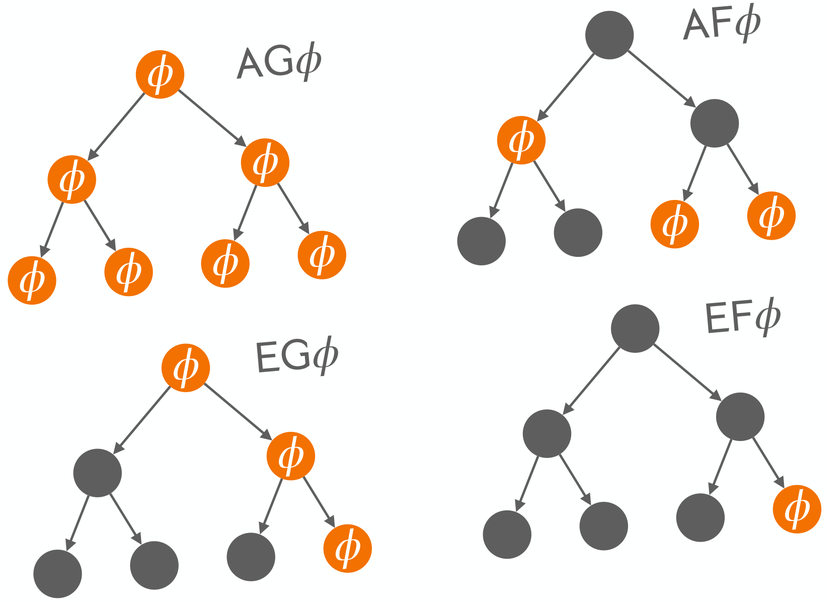
Computation Tree Logic (CTL)

Branching Temporal Logic

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

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

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



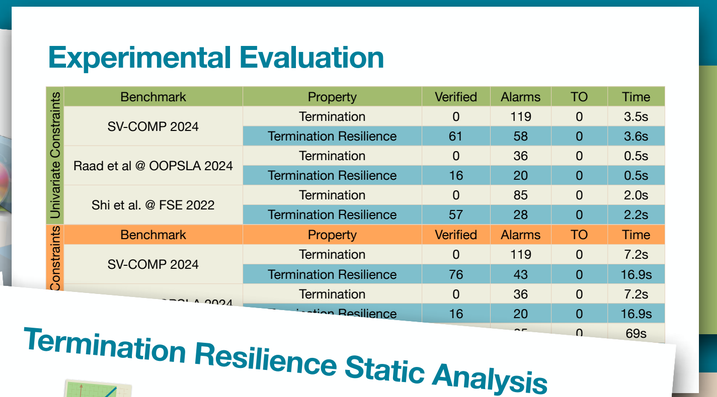
Termination Resilience Static Analysis

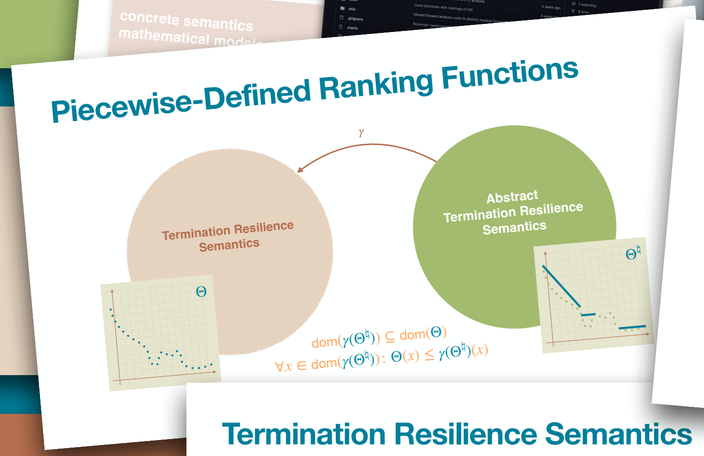
Open Questions

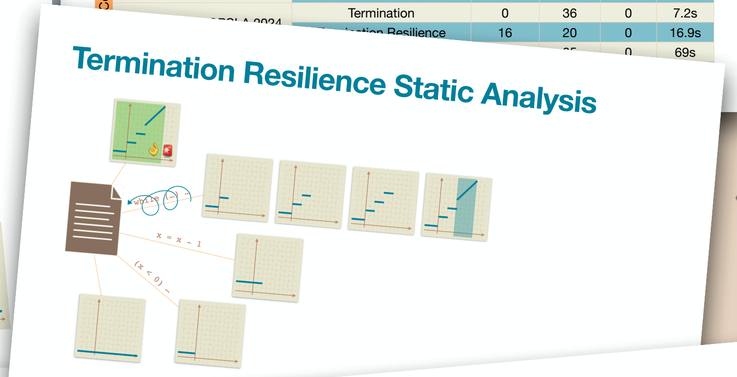
practical tools

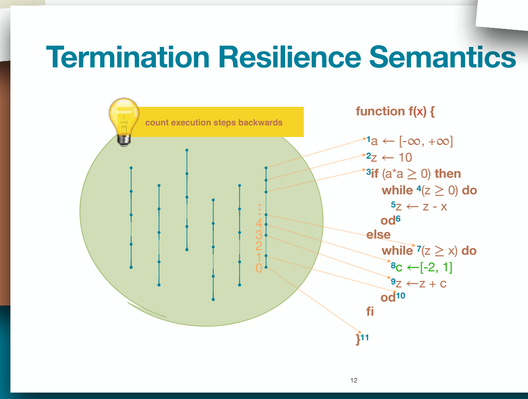
abstract semantics
abstract domains

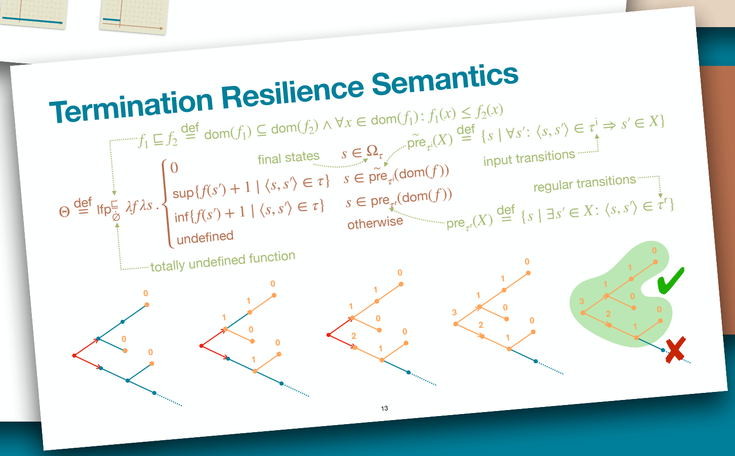
concrete semantics

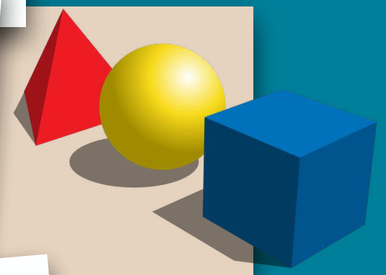












THANKS!