Integrating Loop Acceleration into Bounded Model Checking

Florian Frohn and Jürgen Giesl

Programming Languages and Verification, RWTH Aachen University, Germany

September 11, 2024

Setting

Safety Problems by Example

Pre Variables: x, y Post Variables: x', y' (domain: $\mathbb{Z}$ – in this talk)

Start States: $\psi_s := x \leq 0 \land y \leq 0$ Error States: $\psi_e := y \geq 100$

Transition Formula: $\tau := \underbrace{(x < 100 \land x' = x + 1 \land y' = y)}_{\tau_i} \lor \underbrace{(x = 100 \land x' = 0 \land y' = y + 1)}_{\tau_r}$ (QF)

Example (Transition Relation)

$(23, 42) \to_\tau (24, 42)$ as $[x/23, y/42, x'/24, y'/42] \models \tau$

Dependency Graphs

Safety Problems by Example

Pre Variables: x, y Post Variables: x', y' (domain: $\mathbb{Z}$ – in this talk)

Start States: $\psi_s := x \leq 0 \land y \leq 0$ Error States: $\psi_e := y \geq 100$

Transition Formula: $\tau := \underbrace{(x < 100 \land x' = x + 1 \land y' = y)}_{\tau_i} \lor \underbrace{(x = 100 \land x' = 0 \land y' = y + 1)}_{\tau_r}$ (QF)

Example (Transition Relation)

$(23, 42) \to_\tau (24, 42)$ as $[x/23, y/42, x'/24, y'/42] \models \tau$

Dependency Graphs

Safety Problems by Example

Pre Variables: x, y Post Variables: x', y' (domain: $\mathbb{Z}$ – in this talk)

Start States: $\psi_s := x \leq 0 \land y \leq 0$ Error States: $\psi_e := y \geq 100$

Transition Formula: $\tau := \underbrace{(x < 100 \land x' = x + 1 \land y' = y)}_{\tau_i} \lor \underbrace{(x = 100 \land x' = 0 \land y' = y + 1)}_{\tau_r}$ (QF)

Example (Transition Relation)

$(23, 42) \to_\tau (24, 42)$ as $[x/23, y/42, x'/24, y'/42] \models \tau$

Dependency Graphs

Safety Problems by Example

Pre Variables: x, y Post Variables: x', y' (domain: $\mathbb{Z}$ – in this talk)

Start States: $\psi_s := x \leq 0 \wedge y \leq 0$ Error States: $\psi_e := y \geq 100$

Transition Formula: $\tau := \underbrace{(x < 100 \wedge x' = x + 1 \wedge y' = y)}_{\tau_i} \vee \underbrace{(x = 100 \wedge x' = 0 \wedge y' = y + 1)}_{\tau_r}$ (QF)

Example (Transition Relation)

$(23, 42) \to_\tau (24, 42)$ as $[x/23, y/42, x'/24, y'/42] \models \tau$

Dependency Graphs

Safety Problems by Example

Pre Variables: x, y Post Variables: x', y' (domain: $\mathbb{Z}$ – in this talk)

Start States: $\psi_s := x \leq 0 \wedge y \leq 0$ Error States: $\psi_e := y \geq 100$

Transition Formula: $\tau := \underbrace{(x < 100 \wedge x' = x + 1 \wedge y' = y)}_{\tau_i} \vee \underbrace{(x = 100 \wedge x' = 0 \wedge y' = y + 1)}_{\tau_r}$ (QF)

Example (Transition Relation)

$(23, 42) \to_\tau (24, 42)$ as $[x/23, y/42, x'/24, y'/42] \models \tau$

Dependency Graphs

Safety Problems by Example

Pre Variables: x, y Post Variables: x', y' (domain: $\mathbb{Z}$ – in this talk)

Start States: $\psi_s := x \leq 0 \wedge y \leq 0$ Error States: $\psi_e := y \geq 100$

Transition Formula: $\tau := \underbrace{(x < 100 \wedge x' = x + 1 \wedge y' = y)}_{\tau_i} \vee \underbrace{(x = 100 \wedge x' = 0 \wedge y' = y + 1)}_{\tau_r}$ (QF)

Example (Transition Relation)

$(23, 42) \to_\tau (24, 42)$ as $[x/23, y/42, x'/24, y'/42] \models \tau$

Dependency Graphs

Setting

Safety Problems by Example

Pre Variables: x, y Post Variables: x', y' (domain: $\mathbb{Z}$ – in this talk)

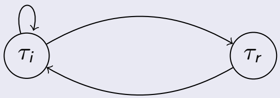
Start States: $\psi_s := x \le 0 \land y \le 0$ Error States: $\psi_e := y \ge 100$

$$\text{Transition Formula: } \tau := \underbrace{(x < 100 \land x' = x + 1 \land y' = y)}_{\tau_i} \lor \underbrace{(x = 100 \land x' = 0 \land y' = y + 1)}_{\tau_r} \qquad \text{(QF)}$$

Example (Transition Relation)

$(23, 42) \to_\tau (24, 42)$ as $[x/23, y/42, x'/24, y'/42] \models \tau$

Dependency Graphs



SMT-based BMC

Leading Example

Start States: $\psi_s := x \leq 0 \land y \leq 0$ Error States: $\psi_e := y \geq 100$

Transition Formula: $\tau := (x < 100 \land x' = x + 1 \land y' = y) \lor (x = 100 \land x' = 0 \land y' = y + 1)$

BMC

$b \leftarrow 0$; add($\mathrm{vr}_b(\psi_s)$) where $\mathrm{vr}_b(x) := x_b, \mathrm{vr}_b(x') := x_{b+1}, \ldots$

while $\top$ **do**

- push(); add($\mathrm{vr}_b(\psi_e)$)
- **if** check() = sat **then** **return** trace() **else** pop(); add($\mathrm{vr}_b(\tau)$)
- **if** check() = unsat **then** **return** safe **else** b++

- $\mathrm{vr}_0(\psi_s) \land \mathrm{vr}_0(\psi_e) \curvearrowright$ unsat
- $\mathrm{vr}_0(\psi_s) \land \mathrm{vr}_0(\tau) \land \mathrm{vr}_1(\psi_e) \curvearrowright$ unsat
- $\mathrm{vr}_0(\psi_s) \land \mathrm{vr}_0(\tau) \land \mathrm{vr}_1(\tau) \land \mathrm{vr}_2(\psi_e) \curvearrowright$ unsat
- $\ldots$
- $\mathrm{vr}_0(\psi_s) \land \mathrm{vr}_0(\tau) \land \ldots \land \mathrm{vr}_{10099}(\tau) \land \mathrm{vr}_{10100}(\psi_e) \curvearrowright$ sat
- trace() $= [\tau_i]_{i=0}^{b-1}$

SMT-based BMC

Leading Example

Start States: $\psi_s := x \leq 0 \wedge y \leq 0$ Error States: $\psi_e := y \geq 100$

Transition Formula: $\tau := (x < 100 \wedge x' = x + 1 \wedge y' = y) \vee (x = 100 \wedge x' = 0 \wedge y' = y + 1)$

BMC

$b \leftarrow 0$; $\mathrm{add}(\mathrm{vr}_b(\psi_s))$ where $\mathrm{vr}_b(x) := x_b, \mathrm{vr}_b(x') := x_{b+1}, \ldots$

while $\top$ **do**

  push(); $\mathrm{add}(\mathrm{vr}_b(\psi_e))$

  if check() $=$ sat **then** **return** trace() **else** pop(); $\mathrm{add}(\mathrm{vr}_b(\tau))$

  if check() $=$ unsat **then** **return** safe **else** b++

- $\mathrm{vr}_0(\psi_s) \wedge \mathrm{vr}_0(\psi_e) \curvearrowright$ unsat
- $\mathrm{vr}_0(\psi_s) \wedge \mathrm{vr}_0(\tau) \wedge \mathrm{vr}_1(\psi_e) \curvearrowright$ unsat
- $\mathrm{vr}_0(\psi_s) \wedge \mathrm{vr}_0(\tau) \wedge \mathrm{vr}_1(\tau) \wedge \mathrm{vr}_2(\psi_e) \curvearrowright$ unsat
- ...
- $\mathrm{vr}_0(\psi_s) \wedge \mathrm{vr}_0(\tau) \wedge \ldots \wedge \mathrm{vr}_{10099}(\tau) \wedge \mathrm{vr}_{10100}(\psi_e) \curvearrowright$ sat
- $\mathrm{trace}() = [\tau_i]_{i=0}^{b-1}$ where $\tau_i = \bigwedge\{\ell \in \mathit{literals}(\tau) \mid \mathrm{vr}_i(\ell)$ is true in current model$\}$

Slooow, basically brute force!

SMT-based BMC

Leading Example

Start States: $\psi_s := x \leq 0 \wedge y \leq 0$ Error States: $\psi_e := y \geq 100$

Transition Formula: $\tau := (x < 100 \wedge x' = x + 1 \wedge y' = y) \vee (x = 100 \wedge x' = 0 \wedge y' = y + 1)$

BMC

$b \leftarrow 0$; $\quad \mathrm{add}(\mathrm{vr}_b(\psi_s))$ where $\mathrm{vr}_b(x) := x_b, \mathrm{vr}_b(x') := x_{b+1}, \ldots$

while $\top$ **do**

  push(); $\quad \mathrm{add}(\mathrm{vr}_b(\psi_e))$

  if check() $=$ sat **then** **return** trace() **else** pop(); $\quad \mathrm{add}(\mathrm{vr}_b(\tau))$

  if check() $=$ unsat **then** **return** safe **else** b++

- $\mathrm{vr}_0(\psi_s) \wedge \mathrm{vr}_0(\psi_e) \curvearrowright$ unsat
- $\mathrm{vr}_0(\psi_s) \wedge \mathrm{vr}_0(\tau) \wedge \mathrm{vr}_1(\psi_e) \curvearrowright$ unsat
- $\mathrm{vr}_0(\psi_s) \wedge \mathrm{vr}_0(\tau) \wedge \mathrm{vr}_1(\tau) \wedge \mathrm{vr}_2(\psi_e) \curvearrowright$ unsat
- $\ldots$
- $\mathrm{vr}_0(\psi_s) \wedge \mathrm{vr}_0(\tau) \wedge \ldots \wedge \mathrm{vr}_{10099}(\tau) \wedge \mathrm{vr}_{10100}(\psi_e) \curvearrowright$ sat
- $\mathrm{trace}() = [\tau_i]_{i=0}^{b-1}$ where $\tau_i = \bigwedge\{\ell \in \mathit{literals}(\tau) \mid \mathrm{vr}_i(\ell) \text{ is true in current model}\}$

Slooow, basically brute force!

Leading Example

Start States: $\psi_s := x \leq 0 \land y \leq 0$ Error States: $\psi_e := y \geq 100$

Transition Formula: $\tau := (x < 100 \land x' = x + 1 \land y' = y) \lor (x = 100 \land x' = 0 \land y' = y + 1)$

BMC

$b \leftarrow 0$; add($\mathsf{vr}_b(\psi_s)$) where $\mathsf{vr}_b(x) := x_b, \mathsf{vr}_b(x') := x_{b+1}, \ldots$

while $\top$ **do**

  push(); add($\mathsf{vr}_b(\psi_e)$)

  if check() = sat **then** **return** trace() **else** pop(); add($\mathsf{vr}_b(\tau)$)

  if check() = unsat **then** **return** safe **else** b++

- $\mathsf{vr}_0(\psi_s) \land \mathsf{vr}_0(\psi_e) \curvearrowright$ unsat
- $\mathsf{vr}_0(\psi_s) \land \mathsf{vr}_0(\tau) \land \mathsf{vr}_1(\psi_e) \curvearrowright$ unsat
- $\mathsf{vr}_0(\psi_s) \land \mathsf{vr}_0(\tau) \land \mathsf{vr}_1(\tau) \land \mathsf{vr}_2(\psi_e) \curvearrowright$ unsat
- ...
- $\mathsf{vr}_0(\psi_s) \land \mathsf{vr}_0(\tau) \land \ldots \land \mathsf{vr}_{10099}(\tau) \land \mathsf{vr}_{10100}(\psi_e) \curvearrowright$ sat
- trace() = $[\tau_i]_{i=0}^{b-1}$

Slooow, basically brute force!

SMT-based BMC

Leading Example

Start States: $\psi_s := x \leq 0 \land y \leq 0$ Error States: $\psi_e := y \geq 100$

Transition Formula: $\tau := (x < 100 \land x' = x + 1 \land y' = y) \lor (x = 100 \land x' = 0 \land y' = y + 1)$

BMC

$b \leftarrow 0$; add($\text{vr}_b(\psi_s)$) where $\text{vr}_b(x) := x_b, \text{vr}_b(x') := x_{b+1}, \ldots$

while $\top$ **do**

  push(); add($\text{vr}_b(\psi_e)$)
  if check() = sat **then** **return** trace() **else** pop(); add($\text{vr}_b(\tau)$)
  if check() = unsat **then** **return** safe **else** b++

- $\text{vr}_0(\psi_s) \land \text{vr}_0(\psi_e) \curvearrowright$ unsat
- $\text{vr}_0(\psi_s) \land \text{vr}_0(\tau) \land \text{vr}_1(\psi_e) \curvearrowright$ unsat
- $\text{vr}_0(\psi_s) \land \text{vr}_0(\tau) \land \text{vr}_1(\tau) \land \text{vr}_2(\psi_e) \curvearrowright$ unsat
- ...
- $\text{vr}_0(\psi_s) \land \text{vr}_0(\tau) \land \ldots \land \text{vr}_{10099}(\tau) \land \text{vr}_{10100}(\psi_e) \curvearrowright$ sat
- trace() = $[\tau_i]_{i=0}^{b-1}$ where $\tau_i = \bigwedge\{\ell \in \text{literals}(\tau) \mid \text{vr}_i(\ell)$ is true in current model$\}$

Slooow, basically brute force!

SMT-based BMC

Leading Example

Start States: $\psi_s := x \leq 0 \land y \leq 0$ Error States: $\psi_e := y \geq 100$

Transition Formula: $\tau := (x < 100 \land x' = x + 1 \land y' = y) \lor (x = 100 \land x' = 0 \land y' = y + 1)$

BMC

$b \leftarrow 0$; add($\mathrm{vr}_b(\psi_s)$) where $\mathrm{vr}_b(x) := x_b, \mathrm{vr}_b(x') := x_{b+1}, \ldots$

while $\top$ **do**

  push(); add($\mathrm{vr}_b(\psi_e)$)

  if check() = sat **then** **return** trace() **else** pop(); add($\mathrm{vr}_b(\tau)$)

  if check() = unsat **then** **return** safe **else** b++

- $\mathrm{vr}_0(\psi_s) \land \mathrm{vr}_0(\psi_e) \curvearrowright$ unsat
- $\mathrm{vr}_0(\psi_s) \land \mathrm{vr}_0(\tau) \land \mathrm{vr}_1(\psi_e) \curvearrowright$ unsat
- $\mathrm{vr}_0(\psi_s) \land \mathrm{vr}_0(\tau) \land \mathrm{vr}_1(\tau) \land \mathrm{vr}_2(\psi_e) \curvearrowright$ unsat
- ...
- $\mathrm{vr}_0(\psi_s) \land \mathrm{vr}_0(\tau) \land \ldots \land \mathrm{vr}_{10099}(\tau) \land \mathrm{vr}_{10100}(\psi_e) \curvearrowright$ sat
- trace() $= [\tau_i]_{i=0}^{b-1}$ where $\tau_i = \bigwedge\{\ell \in \mathit{literals}(\tau) \mid \mathrm{vr}_i(\ell)$ is true in current model$\}$

Slooow, basically brute force!

SMT-based BMC

Leading Example

Start States: $\psi_s := x \leq 0 \wedge y \leq 0$ Error States: $\psi_e := y \geq 100$

Transition Formula: $\tau := (x < 100 \wedge x' = x + 1 \wedge y' = y) \vee (x = 100 \wedge x' = 0 \wedge y' = y + 1)$

BMC

$b \leftarrow 0$; $\mathsf{add}(\mathsf{vr}_b(\psi_s))$ where $\mathsf{vr}_b(x) := x_b, \mathsf{vr}_b(x') := x_{b+1}, \ldots$

while $\top$ **do**

  push(); $\mathsf{add}(\mathsf{vr}_b(\psi_e))$

  if check() $=$ sat **then** **return** trace() **else** pop(); $\mathsf{add}(\mathsf{vr}_b(\tau))$

  if check() $=$ unsat **then** **return** safe **else** b++

- $\mathsf{vr}_0(\psi_s) \wedge \mathsf{vr}_0(\psi_e) \curvearrowright$ unsat
- $\mathsf{vr}_0(\psi_s) \wedge \mathsf{vr}_0(\tau) \wedge \mathsf{vr}_1(\psi_e) \curvearrowright$ unsat
- $\mathsf{vr}_0(\psi_s) \wedge \mathsf{vr}_0(\tau) \wedge \mathsf{vr}_1(\tau) \wedge \mathsf{vr}_2(\psi_e) \curvearrowright$ unsat
- ...
- $\mathsf{vr}_0(\psi_s) \wedge \mathsf{vr}_0(\tau) \wedge \ldots \wedge \mathsf{vr}_{10099}(\tau) \wedge \mathsf{vr}_{10100}(\psi_e) \curvearrowright$ sat
- trace() $= [\tau_i]_{i=0}^{b-1}$ where $\tau_i = \bigwedge\{\ell \in \mathit{literals}(\tau) \mid \mathsf{vr}_i(\ell)$ is true in current model$\}$

Slooow, basically brute force!

Leading Example

Start States: $\psi_s := x \leq 0 \land y \leq 0$ Error States: $\psi_e := y \geq 100$

Transition Formula: $\tau := (x < 100 \land x' = x + 1 \land y' = y) \lor (x = 100 \land x' = 0 \land y' = y + 1)$

BMC

$b \leftarrow 0$; add($\mathsf{vr}_b(\psi_s)$) where $\mathsf{vr}_b(x) := x_b, \mathsf{vr}_b(x') := x_{b+1}, \ldots$

while $\top$ **do**

    push(); add($\mathsf{vr}_b(\psi_e)$)
    if check() = sat **then** **return** trace() **else** pop(); add($\mathsf{vr}_b(\tau)$)
    if check() = unsat **then** **return** safe **else** b++

- $\mathsf{vr}_0(\psi_s) \land \mathsf{vr}_0(\psi_e) \curvearrowright$ unsat
- $\mathsf{vr}_0(\psi_s) \land \mathsf{vr}_0(\tau) \land \mathsf{vr}_1(\psi_e) \curvearrowright$ unsat
- $\mathsf{vr}_0(\psi_s) \land \mathsf{vr}_0(\tau) \land \mathsf{vr}_1(\tau) \land \mathsf{vr}_2(\psi_e) \curvearrowright$ unsat
- $\ldots$
- $\mathsf{vr}_0(\psi_s) \land \mathsf{vr}_0(\tau) \land \ldots \land \mathsf{vr}_{10099}(\tau) \land \mathsf{vr}_{10100}(\psi_e) \curvearrowright$ sat
- trace() $= [\tau_i]_{i=0}^{b-1}$ where $\tau_i = \bigwedge\{\ell \in \mathit{literals}(\tau) \mid \mathsf{vr}_i(\ell) \text{ is true in current model}\}$

Slooow, basically brute force!

SMT-based BMC

Leading Example

Start States: $\psi_s := x \leq 0 \land y \leq 0$ Error States: $\psi_e := y \geq 100$

Transition Formula: $\tau := (x < 100 \land x' = x + 1 \land y' = y) \lor (x = 100 \land x' = 0 \land y' = y + 1)$

BMC

$b \leftarrow 0$; add$(\mathrm{vr}_b(\psi_s))$ where $\mathrm{vr}_b(x) := x_b, \mathrm{vr}_b(x') := x_{b+1}, \ldots$

while $\top$ **do**

  push(); add$(\mathrm{vr}_b(\psi_e))$

  if check() = sat **then** **return** trace() **else** pop(); add$(\mathrm{vr}_b(\tau))$

  if check() = unsat **then** **return** safe **else** b++

- $\mathrm{vr}_0(\psi_s) \land \mathrm{vr}_0(\psi_e) \curvearrowright$ unsat
- $\mathrm{vr}_0(\psi_s) \land \mathrm{vr}_0(\tau) \land \mathrm{vr}_1(\psi_e) \curvearrowright$ unsat
- $\mathrm{vr}_0(\psi_s) \land \mathrm{vr}_0(\tau) \land \mathrm{vr}_1(\tau) \land \mathrm{vr}_2(\psi_e) \curvearrowright$ unsat
- ...
- $\mathrm{vr}_0(\psi_s) \land \mathrm{vr}_0(\tau) \land \ldots \land \mathrm{vr}_{10099}(\tau) \land \mathrm{vr}_{10100}(\psi_e) \curvearrowright$ sat
- trace() $= [\tau_i]_{i=0}^{b-1}$ where $\tau_i = \bigwedge\{\ell \in \mathit{literals}(\tau) \mid \mathrm{vr}_i(\ell)$ is true in current model$\}$

Slooow, basically brute force!

Leading Example

$$\tau := \underbrace{(x < 100 \land x' = x + 1 \land y' = y)}_{\tau_i} \lor \underbrace{(x = 100 \land x' = 0 \land y' = y + 1)}_{\tau_r}$$

Definition (Acceleration)

A function with $\mathrm{accel}(\tau) := \tau^{\oplus}$ where $\to_{\tau^{\oplus}} \subseteq \to_{\tau}^{+}$.

Example

How? Many techniques, e.g…

Acceleration

Leading Example

$$\tau := \underbrace{(x < 100 \land x' = x + 1 \land y' = y)}_{\tau_i} \lor \underbrace{(x = 100 \land x' = 0 \land y' = y + 1)}_{\tau_r}$$

Definition (Acceleration)

A function with $\mathrm{accel}(\tau) := \tau^{\oplus}$ where $\to_{\tau^{\oplus}} \subseteq \to_{\tau}^{+}$.

Example

How? Many techniques, e.g...

Leading Example

$$\tau := \underbrace{(x < 100 \land x' = x + 1 \land y' = y)}_{\tau_i} \lor \underbrace{(x = 100 \land x' = 0 \land y' = y + 1)}_{\tau_r}$$

Definition (Acceleration)

A function with $\mathrm{accel}(\tau) := \tau^{\oplus}$ where $\to_{\tau^{\oplus}} \subseteq \to_{\tau}^{+}$.

Example

$$\tau := \tau_i \lor \tau_r$$

$$\tau_i := x < 100 \land x' = x + 1 \land y' = y$$

$$\tau_i^{\oplus} := x + n - 1 < 100 \land x' = x + n \land y' = y \land n > 0$$

How? Many techniques, e.g...

- monotonicity criteria: $\tau_i \implies x < x'$
- recurrence solving

Leading Example

$$\tau := \underbrace{(x < 100 \wedge x' = x + 1 \wedge y' = y)}_{\tau_i} \vee \underbrace{(x = 100 \wedge x' = 0 \wedge y' = y + 1)}_{\tau_r}$$

Definition (Acceleration)

A function with $\mathrm{accel}(\tau) := \tau^{\oplus}$ where $\to_{\tau^{\oplus}} \subseteq \to_{\tau}^{+}$.

Example

$$\tau := \tau_i \vee \tau_r$$

$$\tau_i := \quad x < 100 \wedge x' = x + 1 \wedge y' = y$$

$$\tau_i^{\oplus} := x + n - 1 < 100 \wedge x' = x + n \wedge y' = y \wedge n > 0$$

How? Many techniques, e.g...

- monotonicity criteria: $\tau_i \implies x < x'$
- recurrence solving

Leading Example

$$\tau := \underbrace{(x < 100 \land x' = x + 1 \land y' = y)}_{\tau_i} \lor \underbrace{(x = 100 \land x' = 0 \land y' = y + 1)}_{\tau_r}$$

Definition (Acceleration)

A function with $\mathrm{accel}(\tau) := \tau^{\oplus}$ where $\to_{\tau^{\oplus}} \subseteq \to_{\tau}^{+}$.

Example

$$\begin{aligned}
\tau &:= \tau_i \lor \tau_r \\
\tau_i &:= \quad x < 100 \land x' = x + 1 \land y' = y \\
\tau_i^{\oplus} &:= x + n - 1 < 100 \land x' = x + n \land y' = y \land n > 0
\end{aligned}$$

How? Many techniques, e.g...

- monotonicity criteria: $\tau_i \implies x < x'$
- recurrence solving

Leading Example

$$\tau := \underbrace{(x < 100 \land x' = x + 1 \land y' = y)}_{\tau_i} \lor \underbrace{(x = 100 \land x' = 0 \land y' = y + 1)}_{\tau_r}$$

Definition (Acceleration)

A function with $\mathrm{accel}(\tau) := \tau^{\oplus}$ where $\to_{\tau^{\oplus}} \subseteq \to_{\tau}^{+}$.

Example

$$\begin{aligned} \tau &:= \tau_i \lor \tau_r \\ \tau_i &:= x < 100 \land x' = x + 1 \land y' = y \\ \tau_i^{\oplus} &:= x + n - 1 < 100 \land x' = x + n \land y' = y \land n > 0 \end{aligned}$$

How? Many techniques, e.g...

- monotonicity criteria: $\tau_i \implies x < x'$
- recurrence solving

Leading Example

$$\tau := \underbrace{(x < 100 \land x' = x + 1 \land y' = y)}_{\tau_i} \lor \underbrace{(x = 100 \land x' = 0 \land y' = y + 1)}_{\tau_r}$$

Definition (Acceleration)

A function with $\mathrm{accel}(\tau) := \tau^{\oplus}$ where $\to_{\tau^{\oplus}} \subseteq \to_{\tau}^{+}$.

Example

$$\begin{aligned}\tau &:= \tau_i \lor \tau_r \\ \tau_i &:= \phantom{x+n-1<100\land{}} x < 100 \land x' = x + 1 \land y' = y \\ \tau_i^{\oplus} &:= x + n - 1 < 100 \land x' = x + n \land y' = y \land n > 0\end{aligned}$$

How? Many techniques, e.g...

- monotonicity criteria: $\tau_i \implies x < x'$
- recurrence solving

Leading Example

$$\tau := \underbrace{(x < 100 \land x' = x + 1 \land y' = y)}_{\tau_i} \lor \underbrace{(x = 100 \land x' = 0 \land y' = y + 1)}_{\tau_r}$$

Definition (Acceleration)

A function with $\mathsf{accel}(\tau) := \tau^{\oplus}$ where $\to_{\tau^{\oplus}} \subseteq \to_{\tau}^{+}$.

Example

$$\begin{aligned} \tau &:= \tau_i \lor \tau_r \\ \tau_i &:= \; x < 100 \land x' = x + 1 \land y' = y \\ \tau_i^{\oplus} &:= x + n - 1 < 100 \land x' = x + n \land y' = y \land n > 0 \end{aligned}$$

How? Many techniques, e.g...

- monotonicity criteria: $\tau_i \implies x < x'$
- recurrence solving

Acceleration

Leading Example

$$\tau := \underbrace{(x < 100 \wedge x' = x + 1 \wedge y' = y)}_{\tau_i} \vee \underbrace{(x = 100 \wedge x' = 0 \wedge y' = y + 1)}_{\tau_r}$$

Definition (Acceleration)

A function with $\mathrm{accel}(\tau) := \tau^{\oplus}$ where $\to_{\tau^{\oplus}} \subseteq \to_{\tau}^{+}$.

Example

$$\begin{aligned} \tau &:= \tau_i \vee \tau_r \\ \tau_i &:= \; x < 100 \wedge x' = x + 1 \wedge y' = y \\ \tau_i^{\oplus} &:= x + n - 1 < 100 \wedge x' = x + n \wedge y' = y \wedge n > 0 \end{aligned}$$

How? Many techniques, e.g...

- monotonicity criteria: $\tau_i \implies x < x'$
- recurrence solving

ABMC

Leading Example

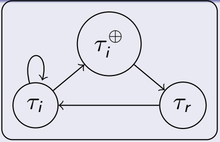
$$\text{Start States: } \psi_s := x \leq 0 \land y \leq 0 \qquad \text{Error States: } \psi_e := y \geq 100$$

$$\text{Transition Formula: } \tau := \underbrace{(x < 100 \land x' = x + 1 \land y' = y)}_{\tau_i} \lor \underbrace{(x = 100 \land x' = 0 \land y' = y + 1)}_{\tau_r}$$

$$\tau_i^{\oplus} := x + n \leq 100 \land x' = x + n \land y' = y \land n > 0$$

ABMC

$b \leftarrow 0$; add(vr$_b(\psi_s)$)
if check() $=$ unsat **then return** safe
while $\top$ **do**
  push(); add(vr$_b(\psi_e)$)
  if check() $=$ sat **then** **return** $\vec{\tau}$
  else
    pop(); $\vec{\tau} \leftarrow$ trace();
    if $\vec{\tau}$ *ends with loop* $\vec{\tau}^{\circlearrowleft}$ **then**
      add(vr$_b(\tau \lor \text{accel}(\vec{\tau}^{\circlearrowleft}))$)
    else add(vr$_b(\tau)$)
  if check() $=$ unsat **then** **return** safe **else** b++



b	$\vec{\tau}$	SMT Problem	Model
0	[]	$\text{vr}_0(\psi_s) \land \text{vr}_0(\tau)$	$[x_1/1, \ldots, /0]$
1	$[\tau_i]$	$\ldots \land \text{vr}_1(\tau \lor \tau_i^{\oplus})$	$\ldots \cup [x_2/100, y_2/0]$
2	$[\tau_i, \tau_i^{\oplus}]$	$\ldots \land \text{vr}_2(\tau)$	$\ldots \cup [x_3/0, y_3/1]$
3	$[\tau_i, \tau_i^{\oplus}, \tau_r]$	$\ldots \land \text{vr}_3(\tau \lor \text{accel}(\vec{\tau}^{\circlearrowleft}))$	$\ldots \cup [x_4/0, y_4/100]$
4		$\ldots \land \text{vr}_4(\psi_e)$	

ABMC

Leading Example

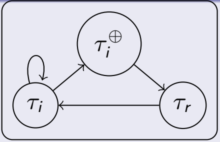
Start States: $\psi_s := x \leq 0 \wedge y \leq 0$ Error States: $\psi_e := y \geq 100$

$$\text{Transition Formula: } \tau := \underbrace{(x < 100 \wedge x' = x + 1 \wedge y' = y)}_{\tau_i} \vee \underbrace{(x = 100 \wedge x' = 0 \wedge y' = y + 1)}_{\tau_r}$$

$$\tau_i^{\oplus} := x + n \leq 100 \wedge x' = x + n \wedge y' = y \wedge n > 0$$

ABMC

$b \leftarrow 0$; add($\mathrm{vr}_b(\psi_s)$)
if check() = unsat **then return** safe
while $\top$ **do**
  push(); add($\mathrm{vr}_b(\psi_e)$)
  if check() = sat **then return** $\vec{\tau}$
  else
    pop(); $\vec{\tau} \leftarrow$ trace();
    if $\vec{\tau}$ *ends with loop* $\vec{\tau}^{\circlearrowleft}$ **then**
      add($\mathrm{vr}_b(\tau \vee \mathrm{accel}(\vec{\tau}^{\circlearrowleft}))$)
    else add($\mathrm{vr}_b(\tau)$)
  if check() = unsat **then return** safe **else** b++



b	$\vec{\tau}$	SMT Problem	Model
0	$[]$	$\mathrm{vr}_0(\psi_s) \wedge \mathrm{vr}_0(\tau)$	$[x_1/1, \ldots /0]$
1	$[\tau_i]$	$\ldots \wedge \mathrm{vr}_1(\tau \vee \tau_i^{\oplus})$	$\ldots \cup [x_2/100, y_2/0]$
2	$[\tau_i, \tau_i^{\oplus}]$	$\ldots \wedge \mathrm{vr}_2(\tau)$	$\ldots \cup [x_3/0, y_3/1]$
3	$[\tau_i, \tau_i^{\oplus}, \tau_r]$	$\ldots \wedge \mathrm{vr}_3(\tau \vee \mathrm{accel}(\vec{\tau}^{\circlearrowleft}))$	$\ldots \cup [x_4/0, y_4/100]$
4		$\ldots \wedge \mathrm{vr}_4(\psi_e)$	

Leading Example

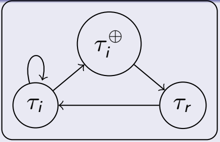
$$\text{Start States: } \psi_s := x \leq 0 \land y \leq 0 \qquad \text{Error States: } \psi_e := y \geq 100$$

$$\text{Transition Formula: } \tau := \underbrace{(x < 100 \land x' = x + 1 \land y' = y)}_{\tau_i} \lor \underbrace{(x = 100 \land x' = 0 \land y' = y + 1)}_{\tau_r}$$

$$\tau_i^{\oplus} := x + n \leq 100 \land x' = x + n \land y' = y \land n > 0$$

ABMC

$b \leftarrow 0$; $\mathrm{add}(\mathrm{vr}_b(\psi_s))$
if check() = unsat **then return** safe
while $\top$ **do**
  push(); $\mathrm{add}(\mathrm{vr}_b(\psi_e))$
  if check() = sat **then return** $\vec{\tau}$
  else
    pop(); $\vec{\tau} \leftarrow$ trace();
    if $\vec{\tau}$ *ends with loop* $\vec{\tau}^{\circlearrowleft}$ **then**
      $\mathrm{add}(\mathrm{vr}_b(\tau \lor \mathrm{accel}(\vec{\tau}^{\circlearrowleft})))$
    else $\mathrm{add}(\mathrm{vr}_b(\tau))$
  if check() = unsat **then return** safe **else** b++



b	$\vec{\tau}$	SMT Problem	Model
0	$[]$	$\mathrm{vr}_0(\psi_s) \land \mathrm{vr}_0(\tau)$	$[x_1/1, \ldots /0]$
1	$[\tau_i]$	$\ldots \land \mathrm{vr}_1(\tau \lor \tau_i^{\oplus})$	$\ldots \cup [x_2/100, y_2/0]$
2	$[\tau_i, \tau_i^{\oplus}]$	$\ldots \land \mathrm{vr}_2(\tau)$	$\ldots \cup [x_3/0, y_3/1]$
3	$[\tau_i, \tau_i^{\oplus}, \tau_r]$	$\ldots \land \mathrm{vr}_3(\tau \lor \mathrm{accel}(\vec{\tau}^{\circlearrowleft}))$	$\ldots \cup [x_4/0, y_4/100]$
4		$\ldots \land \mathrm{vr}_4(\psi_e)$	

ABMC

Leading Example

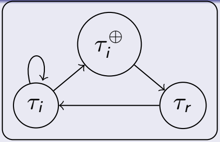
$$\text{Start States: } \psi_s := x \leq 0 \land y \leq 0 \qquad \text{Error States: } \psi_e := y \geq 100$$

$$\text{Transition Formula: } \tau := \underbrace{(x < 100 \land x' = x + 1 \land y' = y)}_{\tau_i} \lor \underbrace{(x = 100 \land x' = 0 \land y' = y + 1)}_{\tau_r}$$

$$\tau_i^{\oplus} := x + n \leq 100 \land x' = x + n \land y' = y \land n > 0$$

ABMC

$b \leftarrow 0$; add($\mathrm{vr}_b(\psi_s)$)
if check() $=$ unsat **then return** safe
while $\top$ **do**
  push(); add($\mathrm{vr}_b(\psi_e)$)
  if check() $=$ sat **then return** $\vec{\tau}$
  else
    pop(); $\vec{\tau} \leftarrow$ trace();
    if $\vec{\tau}$ *ends with loop* $\vec{\tau}^{\circlearrowleft}$ **then**
      add($\mathrm{vr}_b(\tau \lor \mathrm{accel}(\vec{\tau}^{\circlearrowleft}))$)
    else add($\mathrm{vr}_b(\tau)$)
  if check() $=$ unsat **then return** safe **else** b++



b	$\vec{\tau}$	SMT Problem	Model
0	[]	$\mathrm{vr}_0(\psi_s) \land \mathrm{vr}_0(\tau)$	$[x_1/1, \ldots /0]$
1	$[\tau_i]$	$\ldots \land \mathrm{vr}_1(\tau \lor \tau_i^{\oplus})$	$\ldots \cup [x_2/100, y_2/0]$
2	$[\tau_i, \tau_i^{\oplus}]$	$\ldots \land \mathrm{vr}_2(\tau)$	$\ldots \cup [x_3/0, y_3/1]$
3	$[\tau_i, \tau_i^{\oplus}, \tau_r]$	$\ldots \land \mathrm{vr}_3(\tau \lor \mathrm{accel}(\vec{\tau}^{\circlearrowleft}))$	$\ldots \cup [x_4/0, y_4/100]$
4		$\ldots \land \mathrm{vr}_4(\psi_e)$	

Leading Example

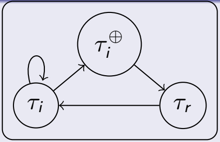
$$\text{Start States: } \psi_s := x \leq 0 \land y \leq 0 \qquad \text{Error States: } \psi_e := y \geq 100$$

$$\text{Transition Formula: } \tau := \underbrace{(x < 100 \land x' = x + 1 \land y' = y)}_{\tau_i} \lor \underbrace{(x = 100 \land x' = 0 \land y' = y + 1)}_{\tau_r}$$

$$\tau_i^{\oplus} := x + n \leq 100 \land x' = x + n \land y' = y \land n > 0$$

ABMC

$b \leftarrow 0$; add($\mathrm{vr}_b(\psi_s)$)
if check() $=$ unsat **then return** safe
while $\top$ **do**
  push(); add($\mathrm{vr}_b(\psi_e)$)
  if check() $=$ sat **then return** $\vec{\tau}$
  else
    pop(); $\vec{\tau} \leftarrow$ trace();
    if $\vec{\tau}$ *ends with loop* $\vec{\tau}^{\circlearrowleft}$ **then**
      add($\mathrm{vr}_b(\tau \lor \mathrm{accel}(\vec{\tau}^{\circlearrowleft}))$)
    else add($\mathrm{vr}_b(\tau)$)
  if check() $=$ unsat **then return** safe **else** b++



b	$\vec{\tau}$	SMT Problem	Model
0	[]	$\mathrm{vr}_0(\psi_s) \land \mathrm{vr}_0(\tau)$	$[x_1/1, \ldots, /0]$
1	$[\tau_i]$	$\ldots \land \mathrm{vr}_1(\tau \lor \tau_i^{\oplus})$	$\ldots \cup [x_2/100, y_2/0]$
2	$[\tau_i, \tau_i^{\oplus}]$	$\ldots \land \mathrm{vr}_2(\tau)$	$\ldots \cup [x_3/0, y_3/1]$
3	$[\tau_i, \tau_i^{\oplus}, \tau_r]$	$\ldots \land \mathrm{vr}_3(\tau \lor \mathrm{accel}(\vec{\tau}^{\circlearrowleft}))$	$\ldots \cup [x_4/0, y_4/100]$
4		$\ldots \land \mathrm{vr}_4(\psi_e)$	

ABMC

Leading Example

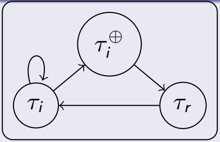
Start States: $\psi_s := x \leq 0 \land y \leq 0$ Error States: $\psi_e := y \geq 100$

$$\text{Transition Formula: } \tau := \underbrace{(x < 100 \land x' = x + 1 \land y' = y)}_{\tau_i} \lor \underbrace{(x = 100 \land x' = 0 \land y' = y + 1)}_{\tau_r}$$

$$\tau_i^{\oplus} := x + n \leq 100 \land x' = x + n \land y' = y \land n > 0$$

ABMC

$b \leftarrow 0$; add($\mathrm{vr}_b(\psi_s)$)
if check() $=$ unsat **then return** safe
while $\top$ **do**
  push(); add($\mathrm{vr}_b(\psi_e)$)
  if check() $=$ sat **then return** $\vec{\tau}$
  else
    pop(); $\vec{\tau} \leftarrow$ trace();
    if *$\vec{\tau}$ ends with loop $\vec{\tau}^{\circlearrowleft}$* **then**
      add($\mathrm{vr}_b(\tau \lor \mathrm{accel}(\vec{\tau}^{\circlearrowleft}))$)
    else add($\mathrm{vr}_b(\tau)$)
  if check() $=$ unsat **then return** safe **else** $b{+}{+}$



b	$\vec{\tau}$	SMT Problem	Model
0	[]	$\mathrm{vr}_0(\psi_s) \land \mathrm{vr}_0(\tau)$	$[x_1/1, \ldots /0]$
1	$[\tau_i]$	$\ldots \land \mathrm{vr}_1(\tau \lor \tau_i^{\oplus})$	$\ldots \cup [x_2/100, y_2/0]$
2	$[\tau_i, \tau_i^{\oplus}]$	$\ldots \land \mathrm{vr}_2(\tau)$	$\ldots \cup [x_3/0, y_3/1]$
3	$[\tau_i, \tau_i^{\oplus}, \tau_r]$	$\ldots \land \mathrm{vr}_3(\tau \lor \mathrm{accel}(\vec{\tau}^{\circlearrowleft}))$	$\ldots \cup [x_4/0, y_4/100]$
4		$\ldots \land \mathrm{vr}_4(\psi_e)$	

Leading Example

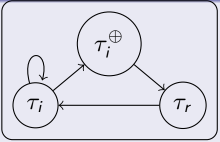
Start States: $\psi_s := x \leq 0 \wedge y \leq 0$ Error States: $\psi_e := y \geq 100$

Transition Formula: $\tau := \underbrace{(x < 100 \wedge x' = x + 1 \wedge y' = y)}_{\tau_i} \vee \underbrace{(x = 100 \wedge x' = 0 \wedge y' = y + 1)}_{\tau_r}$

$$\tau_i^{\oplus} := x + n \leq 100 \wedge x' = x + n \wedge y' = y \wedge n > 0$$

ABMC

$b \leftarrow 0$; add(vr$_b(\psi_s)$)
if check() $=$ unsat **then return** safe
while $\top$ **do**
  push(); add(vr$_b(\psi_e)$)
  if check() $=$ sat **then return** $\vec{\tau}$
  else
    pop(); $\vec{\tau} \leftarrow$ trace();
    if $\vec{\tau}$ *ends with loop* $\vec{\tau}^{\circlearrowleft}$ **then**
      add(vr$_b(\tau \vee$ accel$(\vec{\tau}^{\circlearrowleft})))$
    else add(vr$_b(\tau)$)
  if check() $=$ unsat **then return** safe **else** b++



b	$\vec{\tau}$	SMT Problem	Model
0	[]	vr$_0(\psi_s) \wedge$ vr$_0(\tau)$	$[x_1/1, \ldots, /0]$
1	$[\tau_i]$	$\ldots \wedge$ vr$_1(\tau \vee \tau_i^{\oplus})$	$\ldots \cup [x_2/100, y_2/0]$
2	$[\tau_i, \tau_i^{\oplus}]$	$\ldots \wedge$ vr$_2(\tau)$	$\ldots \cup [x_3/0, y_3/1]$
3	$[\tau_i, \tau_i^{\oplus}, \tau_r]$	$\ldots \wedge$ vr$_3(\tau \vee$ accel$(\vec{\tau}^{\circlearrowleft}))$	$\ldots \cup [x_4/0, y_4/100]$
4		$\ldots \wedge$ vr$_4(\psi_e)$	

Leading Example

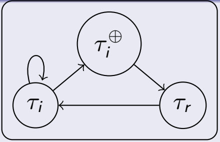
Start States: $\psi_s := x \leq 0 \land y \leq 0$ Error States: $\psi_e := y \geq 100$

$$\text{Transition Formula: } \tau := \underbrace{(x < 100 \land x' = x + 1 \land y' = y)}_{\tau_i} \lor \underbrace{(x = 100 \land x' = 0 \land y' = y + 1)}_{\tau_r}$$

$$\tau_i^{\oplus} := x + n \leq 100 \land x' = x + n \land y' = y \land n > 0$$

ABMC

$b \leftarrow 0$; $\mathsf{add}(\mathsf{vr}_b(\psi_s))$
if check() = unsat **then return** safe
while $\top$ **do**
  push(); $\mathsf{add}(\mathsf{vr}_b(\psi_e))$
  if check() = sat **then return** $\vec{\tau}$
  else
    pop(); $\vec{\tau} \leftarrow$ trace();
    if $\vec{\tau}$ *ends with loop* $\vec{\tau}^{\circlearrowleft}$ **then**
      $\mathsf{add}(\mathsf{vr}_b(\tau \lor \mathsf{accel}(\vec{\tau}^{\circlearrowleft})))$
    else $\mathsf{add}(\mathsf{vr}_b(\tau))$
  if check() = unsat **then return** safe **else** $b{+}{+}$



b	$\vec{\tau}$	SMT Problem	Model
0	[]	$\mathsf{vr}_0(\psi_s) \land \mathsf{vr}_0(\tau)$	$[x_1/1, \ldots/0]$
1	$[\tau_i]$	$\ldots \land \mathsf{vr}_1(\tau \lor \tau_i^{\oplus})$	$\ldots \cup [x_2/100, y_2/0]$
2	$[\tau_i, \tau_i^{\oplus}]$	$\ldots \land \mathsf{vr}_2(\tau)$	$\ldots \cup [x_3/0, y_3/1]$
3	$[\tau_i, \tau_i^{\oplus}, \tau_r]$	$\ldots \land \mathsf{vr}_3(\tau \lor \mathsf{accel}(\vec{\tau}^{\circlearrowleft}))$	$\ldots \cup [x_4/0, y_4/100]$
4		$\ldots \land \mathsf{vr}_4(\psi_e)$	

Leading Example

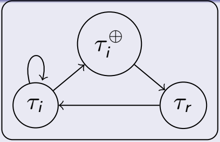
Start States: $\psi_s := x \leq 0 \wedge y \leq 0$ Error States: $\psi_e := y \geq 100$

$$\text{Transition Formula: } \tau := \underbrace{(x < 100 \wedge x' = x + 1 \wedge y' = y)}_{\tau_i} \vee \underbrace{(x = 100 \wedge x' = 0 \wedge y' = y + 1)}_{\tau_r}$$

$$\tau_i^{\oplus} := x + n \leq 100 \wedge x' = x + n \wedge y' = y \wedge n > 0$$

ABMC

$b \leftarrow 0$; add($\mathrm{vr}_b(\psi_s)$)
if check() $=$ unsat **then return** safe
while $\top$ **do**
  push(); add($\mathrm{vr}_b(\psi_e)$)
  if check() $=$ sat **then return** $\vec{\tau}$
  else
    pop(); $\vec{\tau} \leftarrow$ trace();
    if $\vec{\tau}$ *ends with loop* $\vec{\tau}^{\circlearrowleft}$ **then**
      add($\mathrm{vr}_b(\tau \vee \mathrm{accel}(\vec{\tau}^{\circlearrowleft}))$)
    else add($\mathrm{vr}_b(\tau)$)
  if check() $=$ unsat **then return** safe **else** b++



b	$\vec{\tau}$	SMT Problem	Model
0	[]	$\mathrm{vr}_0(\psi_s) \wedge \mathrm{vr}_0(\tau)$	$[x_1/1, \ldots /0]$
1	$[\tau_i]$	$\ldots \wedge \mathrm{vr}_1(\tau \vee \tau_i^{\oplus})$	$\ldots \cup [x_2/100, y_2/0]$
2	$[\tau_i, \tau_i^{\oplus}]$	$\ldots \wedge \mathrm{vr}_2(\tau)$	$\ldots \cup [x_3/0, y_3/1]$
3	$[\tau_i, \tau_i^{\oplus}, \tau_r]$	$\ldots \wedge \mathrm{vr}_3(\tau \vee \mathrm{accel}(\vec{\tau}^{\circlearrowleft}))$	$\ldots \cup [x_4/0, y_4/100]$
4		$\ldots \wedge \mathrm{vr}_4(\psi_e)$	

Leading Example

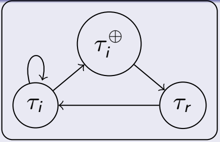
Start States: $\psi_s := x \leq 0 \land y \leq 0$ Error States: $\psi_e := y \geq 100$

$$\text{Transition Formula: } \tau := \underbrace{(x < 100 \land x' = x + 1 \land y' = y)}_{\tau_i} \lor \underbrace{(x = 100 \land x' = 0 \land y' = y + 1)}_{\tau_r}$$

$$\tau_i^{\oplus} := x + n \leq 100 \land x' = x + n \land y' = y \land n > 0$$

ABMC

$b \leftarrow 0$; add($\mathsf{vr}_b(\psi_s)$)
if check() $=$ unsat **then return** safe
while $\top$ **do**
  push(); add($\mathsf{vr}_b(\psi_e)$)
  if check() $=$ sat **then return** $\vec{\tau}$
  else
    pop(); $\vec{\tau} \leftarrow$ trace();
    if $\vec{\tau}$ *ends with loop* $\vec{\tau}^{\circlearrowleft}$ **then**
      add($\mathsf{vr}_b(\tau \lor \mathsf{accel}(\vec{\tau}^{\circlearrowleft}))$)
    else add($\mathsf{vr}_b(\tau)$)
  if check() $=$ unsat **then return** safe **else** b++



b	$\vec{\tau}$	SMT Problem	Model
0	[]	$\mathsf{vr}_0(\psi_s) \land \mathsf{vr}_0(\tau)$	$[x_1/1, \ldots /0]$
1	$[\tau_i]$	$\ldots \land \mathsf{vr}_1(\tau \lor \tau_i^{\oplus})$	$\ldots \cup [x_2/100, y_2/0]$
2	$[\tau_i, \tau_i^{\oplus}]$	$\ldots \land \mathsf{vr}_2(\tau)$	$\ldots \cup [x_3/0, y_3/1]$
3	$[\tau_i, \tau_i^{\oplus}, \tau_r]$	$\ldots \land \mathsf{vr}_3(\tau \lor \mathsf{accel}(\vec{\tau}^{\circlearrowleft}))$	$\ldots \cup [x_4/0, y_4/100]$
4		$\ldots \land \mathsf{vr}_4(\psi_e)$	

ABMC

Leading Example

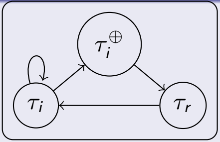
Start States: $\psi_s := x \leq 0 \land y \leq 0$ Error States: $\psi_e := y \geq 100$

$$\text{Transition Formula: } \tau := \underbrace{(x < 100 \land x' = x + 1 \land y' = y)}_{\tau_i} \lor \underbrace{(x = 100 \land x' = 0 \land y' = y + 1)}_{\tau_r}$$

$$\tau_i^{\oplus} := x + n \leq 100 \land x' = x + n \land y' = y \land n > 0$$

ABMC

$b \leftarrow 0$; add($\text{vr}_b(\psi_s)$)
if check() = unsat **then return** safe
while $\top$ **do**
  push(); add($\text{vr}_b(\psi_e)$)
  if check() = sat **then return** $\vec{\tau}$
  else
    pop(); $\vec{\tau} \leftarrow$ trace();
    if $\vec{\tau}$ *ends with loop* $\vec{\tau}^{\circlearrowleft}$ **then**
      add($\text{vr}_b(\tau \lor \text{accel}(\vec{\tau}^{\circlearrowleft}))$)
    else add($\text{vr}_b(\tau)$)
  if check() = unsat **then return** safe **else** $b{+}{+}$



b	$\vec{\tau}$	SMT Problem	Model
0	[]	$\text{vr}_0(\psi_s) \land \text{vr}_0(\tau)$	$[x_1/1, \ldots/0]$
1	$[\tau_i]$	$\ldots \land \text{vr}_1(\tau \lor \tau_i^{\oplus})$	$\ldots \cup [x_2/100, y_2/0]$
2	$[\tau_i, \tau_i^{\oplus}]$	$\ldots \land \text{vr}_2(\tau)$	$\ldots \cup [x_3/0, y_3/1]$
3	$[\tau_i, \tau_i^{\oplus}, \tau_r]$	$\ldots \land \text{vr}_3(\tau \lor \text{accel}(\vec{\tau}^{\circlearrowleft}))$	$\ldots \cup [x_4/0, y_4/100]$
4		$\ldots \land \text{vr}_4(\psi_e)$	

Leading Example

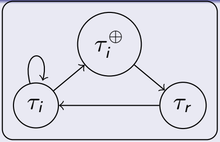
Start States: $\psi_s := x \leq 0 \wedge y \leq 0$ Error States: $\psi_e := y \geq 100$

$$\text{Transition Formula: } \tau := \underbrace{(x < 100 \wedge x' = x + 1 \wedge y' = y)}_{\tau_i} \vee \underbrace{(x = 100 \wedge x' = 0 \wedge y' = y + 1)}_{\tau_r}$$

$$\tau_i^{\oplus} := x + n \leq 100 \wedge x' = x + n \wedge y' = y \wedge n > 0$$

ABMC

$b \leftarrow 0$; add($\mathrm{vr}_b(\psi_s)$)
if check() = unsat **then return** safe
while $\top$ **do**
  push(); add($\mathrm{vr}_b(\psi_e)$)
  if check() = sat **then return** $\vec{\tau}$
  else
    pop(); $\vec{\tau} \leftarrow$ trace();
    if $\vec{\tau}$ *ends with loop* $\vec{\tau}^{\circlearrowleft}$ **then**
      add($\mathrm{vr}_b(\tau \vee \mathrm{accel}(\vec{\tau}^{\circlearrowleft}))$)
    else add($\mathrm{vr}_b(\tau)$)
  if check() = unsat **then return** safe **else** b++



b	$\vec{\tau}$	SMT Problem	Model
0	[]	$\mathrm{vr}_0(\psi_s) \wedge \mathrm{vr}_0(\tau)$	$[x_1/1, \ldots/0]$
1	$[\tau_i]$	$\ldots \wedge \mathrm{vr}_1(\tau \vee \tau_i^{\oplus})$	$\ldots \cup [x_2/100, y_2/0]$
2	$[\tau_i, \tau_i^{\oplus}]$	$\ldots \wedge \mathrm{vr}_2(\tau)$	$\ldots \cup [x_3/0, y_3/1]$
3	$[\tau_i, \tau_i^{\oplus}, \tau_r]$	$\ldots \wedge \mathrm{vr}_3(\tau \vee \mathrm{accel}(\vec{\tau}^{\circlearrowleft}))$	$\ldots \cup [x_4/0, y_4/100]$
4		$\ldots \wedge \mathrm{vr}_4(\psi_e)$	

ABMC

Leading Example

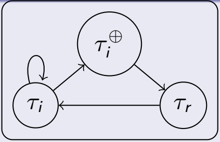
Start States: $\psi_s := x \leq 0 \land y \leq 0$ Error States: $\psi_e := y \geq 100$

$$\text{Transition Formula: } \tau := \underbrace{(x < 100 \land x' = x + 1 \land y' = y)}_{\tau_i} \lor \underbrace{(x = 100 \land x' = 0 \land y' = y + 1)}_{\tau_r}$$

$$\tau_i^{\oplus} := x + n \leq 100 \land x' = x + n \land y' = y \land n > 0$$

ABMC

$b \leftarrow 0;$ $\mathsf{add}(\mathsf{vr}_b(\psi_s))$
if $\mathsf{check}() = \mathsf{unsat}$ **then return** safe
while $\top$ **do**
  $\mathsf{push}();$ $\mathsf{add}(\mathsf{vr}_b(\psi_e))$
  if $\mathsf{check}() = \mathsf{sat}$ **then return** $\vec{\tau}$
  else
    $\mathsf{pop}();$ $\vec{\tau} \leftarrow \mathsf{trace}();$
    if *$\vec{\tau}$ ends with loop $\vec{\tau}^{\circlearrowleft}$* **then**
      $\mathsf{add}(\mathsf{vr}_b(\tau \lor \mathsf{accel}(\vec{\tau}^{\circlearrowleft})))$
    else $\mathsf{add}(\mathsf{vr}_b(\tau))$
  if $\mathsf{check}() = \mathsf{unsat}$ **then return** safe **else** $b{+}{+}$



b	$\vec{\tau}$	SMT Problem	Model
0	[]	$\mathsf{vr}_0(\psi_s) \land \mathsf{vr}_0(\tau)$	$[x_1/1, \ldots/0]$
1	$[\tau_i]$	$\ldots \land \mathsf{vr}_1(\tau \lor \tau_i^{\oplus})$	$\ldots \cup [x_2/100, y_2/0]$
2	$[\tau_i, \tau_i^{\oplus}]$	$\ldots \land \mathsf{vr}_2(\tau)$	$\ldots \cup [x_3/0, y_3/1]$
3	$[\tau_i, \tau_i^{\oplus}, \tau_r]$	$\ldots \land \mathsf{vr}_3(\tau \lor \mathsf{accel}(\vec{\tau}^{\circlearrowleft}))$	$\ldots \cup [x_4/0, y_4/100]$
4		$\ldots \land \mathsf{vr}_4(\psi_e)$	

ABMC

Leading Example

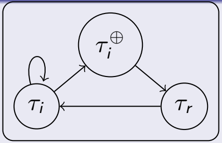
Start States: $\psi_s := x \leq 0 \land y \leq 0$ Error States: $\psi_e := y \geq 100$

$$\text{Transition Formula: } \tau := \underbrace{(x < 100 \land x' = x + 1 \land y' = y)}_{\tau_i} \lor \underbrace{(x = 100 \land x' = 0 \land y' = y + 1)}_{\tau_r}$$

$$\tau_i^{\oplus} := x + n \leq 100 \land x' = x + n \land y' = y \land n > 0$$

ABMC

$b \leftarrow 0;\quad \mathsf{add}(\mathsf{vr}_b(\psi_s))$
if check() $=$ unsat **then return** safe
while $\top$ **do**
  push(); $\quad \mathsf{add}(\mathsf{vr}_b(\psi_e))$
  if check() $=$ sat **then** **return** $\vec{\tau}$
  else
    pop(); $\quad \vec{\tau} \leftarrow$ trace();
    if $\vec{\tau}$ *ends with loop* $\vec{\tau}^{\circlearrowleft}$ **then**
      $\mathsf{add}(\mathsf{vr}_b(\tau \lor \mathsf{accel}(\vec{\tau}^{\circlearrowleft})))$
    else $\mathsf{add}(\mathsf{vr}_b(\tau))$
  if check() $=$ unsat **then** **return** safe **else** $b{+}{+}$



b	$\vec{\tau}$	SMT Problem	Model
0	[]	$\mathsf{vr}_0(\psi_s) \land \mathsf{vr}_0(\tau)$	$[x_1/1, \ldots /0]$
1	$[\tau_i]$	$\ldots \land \mathsf{vr}_1(\tau \lor \tau_i^{\oplus})$	$\ldots \cup [x_2/100, y_2/0]$
2	$[\tau_i, \tau_i^{\oplus}]$	$\ldots \land \mathsf{vr}_2(\tau)$	$\ldots \cup [x_3/0, y_3/1]$
3	$[\tau_i, \tau_i^{\oplus}, \tau_r]$	$\ldots \land \mathsf{vr}_3(\tau \lor \mathsf{accel}(\vec{\tau}^{\circlearrowleft}))$	$\ldots \cup [x_4/0, y_4/100]$
4		$\ldots \land \mathsf{vr}_4(\psi_e)$	

Leading Example

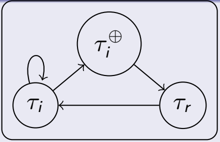
Start States: $\psi_s := x \leq 0 \land y \leq 0$ Error States: $\psi_e := y \geq 100$

Transition Formula: $\tau := \underbrace{(x < 100 \land x' = x + 1 \land y' = y)}_{\tau_i} \lor \underbrace{(x = 100 \land x' = 0 \land y' = y + 1)}_{\tau_r}$

$$\tau_i^{\oplus} := x + n \leq 100 \land x' = x + n \land y' = y \land n > 0$$

ABMC

$b \leftarrow 0$; add($\mathrm{vr}_b(\psi_s)$)
if check() $=$ unsat **then return** safe
while $\top$ **do**
  push(); add($\mathrm{vr}_b(\psi_e)$)
  if check() $=$ sat **then return** $\vec{\tau}$
  else
    pop(); $\vec{\tau} \leftarrow$ trace();
    if $\vec{\tau}$ *ends with loop* $\vec{\tau}^{\circlearrowleft}$ **then**
      add($\mathrm{vr}_b(\tau \lor \mathrm{accel}(\vec{\tau}^{\circlearrowleft}))$)
    else add($\mathrm{vr}_b(\tau)$)
  if check() $=$ unsat **then return** safe **else** b++



b	$\vec{\tau}$	SMT Problem	Model
0	[]	$\mathrm{vr}_0(\psi_s) \land \mathrm{vr}_0(\tau)$	$[x_1/1, \ldots /0]$
1	$[\tau_i]$	$\ldots \land \mathrm{vr}_1(\tau \lor \tau_i^{\oplus})$	$\ldots \cup [x_2/100, y_2/0]$
2	$[\tau_i, \tau_i^{\oplus}]$	$\ldots \land \mathrm{vr}_2(\tau)$	$\ldots \cup [x_3/0, y_3/1]$
3	$[\tau_i, \tau_i^{\oplus}, \tau_r]$	$\ldots \land \mathrm{vr}_3(\tau \lor \mathrm{accel}(\vec{\tau}^{\circlearrowleft}))$	$\ldots \cup [x_4/0, y_4/100]$
4		$\ldots \land \mathrm{vr}_4(\psi_e)$	

Leading Example

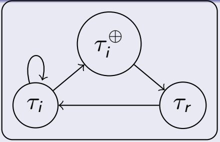
Start States: $\psi_s := x \leq 0 \wedge y \leq 0$ Error States: $\psi_e := y \geq 100$

$$\text{Transition Formula: } \tau := \underbrace{(x < 100 \wedge x' = x + 1 \wedge y' = y)}_{\tau_i} \vee \underbrace{(x = 100 \wedge x' = 0 \wedge y' = y + 1)}_{\tau_r}$$

$$\tau_i^{\oplus} := x + n \leq 100 \wedge x' = x + n \wedge y' = y \wedge n > 0$$

ABMC

$b \leftarrow 0$; add($\mathrm{vr}_b(\psi_s)$)
if check() = unsat **then return** safe
while $\top$ **do**
  push(); add($\mathrm{vr}_b(\psi_e)$)
  if check() = sat **then return** $\vec{\tau}$
  else
    pop(); $\vec{\tau} \leftarrow$ trace();
    if $\vec{\tau}$ *ends with loop* $\vec{\tau}^{\circlearrowleft}$ **then**
      add($\mathrm{vr}_b(\tau \vee \mathrm{accel}(\vec{\tau}^{\circlearrowleft}))$)
    else add($\mathrm{vr}_b(\tau)$)
  if check() = unsat **then return** safe **else** b++



b	$\vec{\tau}$	SMT Problem	Model
0	[]	$\mathrm{vr}_0(\psi_s) \wedge \mathrm{vr}_0(\tau)$	$[x_1/1, \ldots /0]$
1	$[\tau_i]$	$\ldots \wedge \mathrm{vr}_1(\tau \vee \tau_i^{\oplus})$	$\ldots \cup [x_2/100, y_2/0]$
2	$[\tau_i, \tau_i^{\oplus}]$	$\ldots \wedge \mathrm{vr}_2(\tau)$	$\ldots \cup [x_3/0, y_3/1]$
3	$[\tau_i, \tau_i^{\oplus}, \tau_r]$	$\ldots \wedge \mathrm{vr}_3(\tau \vee \mathrm{accel}(\vec{\tau}^{\circlearrowleft}))$	$\ldots \cup [x_4/0, y_4/100]$
4		$\ldots \wedge \mathrm{vr}_4(\psi_e)$	

ABMC

Leading Example

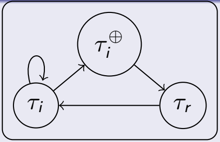
Start States: $\psi_s := x \leq 0 \land y \leq 0$ Error States: $\psi_e := y \geq 100$

$$\text{Transition Formula: } \tau := \underbrace{(x < 100 \land x' = x + 1 \land y' = y)}_{\tau_i} \lor \underbrace{(x = 100 \land x' = 0 \land y' = y + 1)}_{\tau_r}$$

$$\tau_i^{\oplus} := x + n \leq 100 \land x' = x + n \land y' = y \land n > 0$$

ABMC

$b \leftarrow 0$; add($\mathrm{vr}_b(\psi_s)$)
if check() = unsat **then return** safe
while $\top$ **do**
  push(); add($\mathrm{vr}_b(\psi_e)$)
  if check() = sat **then** **return** $\vec{\tau}$
  else
    pop(); $\vec{\tau} \leftarrow$ trace();
    if $\vec{\tau}$ *ends with loop* $\vec{\tau}^{\circlearrowleft}$ **then**
      add($\mathrm{vr}_b(\tau \lor \mathrm{accel}(\vec{\tau}^{\circlearrowleft}))$)
    else add($\mathrm{vr}_b(\tau)$)
  if check() = unsat **then** **return** safe **else** b++



b	$\vec{\tau}$	SMT Problem	Model
0	[]	$\mathrm{vr}_0(\psi_s) \land \mathrm{vr}_0(\tau)$	$[x_1/1, \ldots /0]$
1	$[\tau_i]$	$\ldots \land \mathrm{vr}_1(\tau \lor \tau_i^{\oplus})$	$\ldots \cup [x_2/100, y_2/0]$
2	$[\tau_i, \tau_i^{\oplus}]$	$\ldots \land \mathrm{vr}_2(\tau)$	$\ldots \cup [x_3/0, y_3/1]$
3	$[\tau_i, \tau_i^{\oplus}, \tau_r]$	$\ldots \land \mathrm{vr}_3(\tau \lor \mathrm{accel}(\vec{\tau}^{\circlearrowleft}))$	$\ldots \cup [x_4/0, y_4/100]$
4		$\ldots \land \mathrm{vr}_4(\psi_e)$	

ABMC

Leading Example

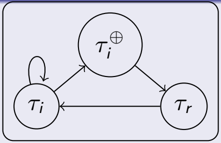
Start States: $\psi_s := x \leq 0 \land y \leq 0$ Error States: $\psi_e := y \geq 100$

$$\text{Transition Formula: } \tau := \underbrace{(x < 100 \land x' = x + 1 \land y' = y)}_{\tau_i} \lor \underbrace{(x = 100 \land x' = 0 \land y' = y + 1)}_{\tau_r}$$

$$\tau_i^{\oplus} := x + n \leq 100 \land x' = x + n \land y' = y \land n > 0$$

ABMC

$b \leftarrow 0$; add($\mathrm{vr}_b(\psi_s)$)
if check() $=$ unsat **then return** safe
while $\top$ **do**
  push(); add($\mathrm{vr}_b(\psi_e)$)
  if check() $=$ sat **then return** $\vec{\tau}$
  else
    pop(); $\vec{\tau} \leftarrow$ trace();
    if $\vec{\tau}$ *ends with loop* $\vec{\tau}^{\circlearrowleft}$ **then**
      add($\mathrm{vr}_b(\tau \lor \mathrm{accel}(\vec{\tau}^{\circlearrowleft}))$)
    else add($\mathrm{vr}_b(\tau)$)
  if check() $=$ unsat **then return** safe **else** b++



b	$\vec{\tau}$	SMT Problem	Model
0	[]	$\mathrm{vr}_0(\psi_s) \land \mathrm{vr}_0(\tau)$	$[x_1/1, \ldots/0]$
1	$[\tau_i]$	$\ldots \land \mathrm{vr}_1(\tau \lor \tau_i^{\oplus})$	$\ldots \cup [x_2/100, y_2/0]$
2	$[\tau_i, \tau_i^{\oplus}]$	$\ldots \land \mathrm{vr}_2(\tau)$	$\ldots \cup [x_3/0, y_3/1]$
3	$[\tau_i, \tau_i^{\oplus}, \tau_r]$	$\ldots \land \mathrm{vr}_3(\tau \lor \mathrm{accel}(\vec{\tau}^{\circlearrowleft}))$	$\ldots \cup [x_4/0, y_4/100]$
4		$\ldots \land \mathrm{vr}_4(\psi_e)$	

ABMC

Leading Example

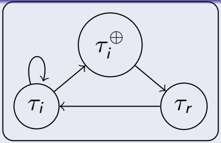
Start States: $\psi_s := x \leq 0 \land y \leq 0$ Error States: $\psi_e := y \geq 100$

Transition Formula: $\tau := \underbrace{(x < 100 \land x' = x + 1 \land y' = y)}_{\tau_i} \lor \underbrace{(x = 100 \land x' = 0 \land y' = y + 1)}_{\tau_r}$

$$\tau_i^{\oplus} := x + n \leq 100 \land x' = x + n \land y' = y \land n > 0$$

ABMC

$b \leftarrow 0$; add($\mathrm{vr}_b(\psi_s)$)
if check() = unsat **then return** safe
while $\top$ **do**
  push(); add($\mathrm{vr}_b(\psi_e)$)
  if check() = sat **then return** $\vec{\tau}$
  else
    pop(); $\vec{\tau} \leftarrow$ trace();
    if $\vec{\tau}$ *ends with loop* $\vec{\tau}^{\circlearrowleft}$ **then**
      add($\mathrm{vr}_b(\tau \lor \mathrm{accel}(\vec{\tau}^{\circlearrowleft}))$)
    else add($\mathrm{vr}_b(\tau)$)
  if check() = unsat **then return** safe **else** b++



b	$\vec{\tau}$	SMT Problem	Model
0	[]	$\mathrm{vr}_0(\psi_s) \land \mathrm{vr}_0(\tau)$	$[x_1/1, \dots/0]$
1	$[\tau_i]$	$\dots \land \mathrm{vr}_1(\tau \lor \tau_i^{\oplus})$	$\dots \cup [x_2/100, y_2/0]$
2	$[\tau_i, \tau_i^{\oplus}]$	$\dots \land \mathrm{vr}_2(\tau)$	$\dots \cup [x_3/0, y_3/1]$
3	$[\tau_i, \tau_i^{\oplus}, \tau_r]$	$\dots \land \mathrm{vr}_3(\tau \lor \mathrm{accel}(\vec{\tau}^{\circlearrowleft}))$	$\dots \cup [x_4/0, y_4/100]$
4		$\dots \land \mathrm{vr}_4(\psi_e)$	

Leading Example

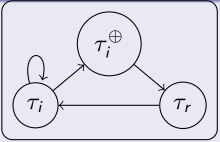
Start States: $\psi_s := x \leq 0 \wedge y \leq 0$ Error States: $\psi_e := y \geq 100$

$$\text{Transition Formula: } \tau := \underbrace{(x < 100 \wedge x' = x + 1 \wedge y' = y)}_{\tau_i} \vee \underbrace{(x = 100 \wedge x' = 0 \wedge y' = y + 1)}_{\tau_r}$$

$$\tau_i^{\oplus} := x + n \leq 100 \wedge x' = x + n \wedge y' = y \wedge n > 0$$

ABMC

$b \leftarrow 0$; add($\mathsf{vr}_b(\psi_s)$)
if check() $=$ unsat **then return** safe
while $\top$ **do**
  push(); add($\mathsf{vr}_b(\psi_e)$)
  if check() $=$ sat **then return** $\vec{\tau}$
  else
    pop(); $\vec{\tau} \leftarrow$ trace();
    if $\vec{\tau}$ *ends with loop* $\vec{\tau}^{\circlearrowleft}$ **then**
      add($\mathsf{vr}_b(\tau \vee \mathsf{accel}(\vec{\tau}^{\circlearrowleft}))$)
    else add($\mathsf{vr}_b(\tau)$)
  if check() $=$ unsat **then return** safe **else** b++



b	$\vec{\tau}$	SMT Problem	Model
0	[]	$\mathsf{vr}_0(\psi_s) \wedge \mathsf{vr}_0(\tau)$	$[x_1/1, \ldots /0]$
1	$[\tau_i]$	$\ldots \wedge \mathsf{vr}_1(\tau \vee \tau_i^{\oplus})$	$\ldots \cup [x_2/100, y_2/0]$
2	$[\tau_i, \tau_i^{\oplus}]$	$\ldots \wedge \mathsf{vr}_2(\tau)$	$\ldots \cup [x_3/0, y_3/1]$
3	$[\tau_i, \tau_i^{\oplus}, \tau_r]$	$\ldots \wedge \mathsf{vr}_3(\tau \vee \mathsf{accel}(\vec{\tau}^{\circlearrowleft}))$	$\ldots \cup [x_4/0, y_4/100]$
4		$\ldots \wedge \mathsf{vr}_4(\psi_e)$	

Leading Example

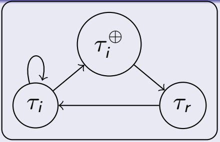
Start States: $\psi_s := x \leq 0 \wedge y \leq 0$ Error States: $\psi_e := y \geq 100$

Transition Formula: $\tau := \underbrace{(x < 100 \wedge x' = x + 1 \wedge y' = y)}_{\tau_i} \vee \underbrace{(x = 100 \wedge x' = 0 \wedge y' = y + 1)}_{\tau_r}$

$$\tau_i^{\oplus} := x + n \leq 100 \wedge x' = x + n \wedge y' = y \wedge n > 0$$

ABMC

$b \leftarrow 0$; add($\mathrm{vr}_b(\psi_s)$)
if check() = unsat **then return** safe
while $\top$ **do**
  push(); add($\mathrm{vr}_b(\psi_e)$)
  if check() = sat **then return** $\vec{\tau}$
  else
    pop(); $\vec{\tau} \leftarrow$ trace();
    if $\vec{\tau}$ *ends with loop* $\vec{\tau}^{\circlearrowleft}$ **then**
      add($\mathrm{vr}_b(\tau \vee \mathrm{accel}(\vec{\tau}^{\circlearrowleft}))$)
    else add($\mathrm{vr}_b(\tau)$)
  if check() = unsat **then return** safe **else** b++



b	$\vec{\tau}$	SMT Problem	Model
0	[]	$\mathrm{vr}_0(\psi_s) \wedge \mathrm{vr}_0(\tau)$	$[x_1/1, \ldots/0]$
1	$[\tau_i]$	$\ldots \wedge \mathrm{vr}_1(\tau \vee \tau_i^{\oplus})$	$\ldots \cup [x_2/100, y_2/0]$
2	$[\tau_i, \tau_i^{\oplus}]$	$\ldots \wedge \mathrm{vr}_2(\tau)$	$\ldots \cup [x_3/0, y_3/1]$
3	$[\tau_i, \tau_i^{\oplus}, \tau_r]$	$\ldots \wedge \mathrm{vr}_3(\tau \vee \mathrm{accel}(\vec{\tau}^{\circlearrowleft}))$	$\ldots \cup [x_4/0, y_4/100]$
4		$\ldots \wedge \mathrm{vr}_4(\psi_e)$	

ABMC

Leading Example

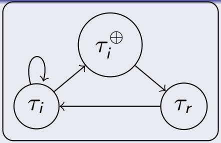
Start States: $\psi_s := x \leq 0 \land y \leq 0$ Error States: $\psi_e := y \geq 100$

Transition Formula: $\tau := \underbrace{(x < 100 \land x' = x + 1 \land y' = y)}_{\tau_i} \lor \underbrace{(x = 100 \land x' = 0 \land y' = y + 1)}_{\tau_r}$

$$\tau_i^{\oplus} := x + n \leq 100 \land x' = x + n \land y' = y \land n > 0$$

ABMC

$b \leftarrow 0;$ $\quad \mathrm{add}(\mathrm{vr}_b(\psi_s))$
if check() $=$ unsat **then return** safe
while $\top$ **do**
  push(); $\quad \mathrm{add}(\mathrm{vr}_b(\psi_e))$
  if check() $=$ sat **then return** $\vec{\tau}$
  else
    pop(); $\quad \vec{\tau} \leftarrow$ trace();
    if $\vec{\tau}$ *ends with loop* $\vec{\tau}^{\circlearrowleft}$ **then**
      $\mathrm{add}(\mathrm{vr}_b(\tau \lor \mathrm{accel}(\vec{\tau}^{\circlearrowleft})))$
    else $\mathrm{add}(\mathrm{vr}_b(\tau))$
  if check() $=$ unsat **then return** safe **else** $b{+}{+}$



b	$\vec{\tau}$	SMT Problem	Model
0	[]	$\mathrm{vr}_0(\psi_s) \land \mathrm{vr}_0(\tau)$	$[x_1/1, \ldots/0]$
1	$[\tau_i]$	$\ldots \land \mathrm{vr}_1(\tau \lor \tau_i^{\oplus})$	$\ldots \cup [x_2/100, y_2/0]$
2	$[\tau_i, \tau_i^{\oplus}]$	$\ldots \land \mathrm{vr}_2(\tau)$	$\ldots \cup [x_3/0, y_3/1]$
3	$[\tau_i, \tau_i^{\oplus}, \tau_r]$	$\ldots \land \mathrm{vr}_3(\tau \lor \mathrm{accel}(\vec{\tau}^{\circlearrowleft}))$	$\ldots \cup [x_4/0, y_4/100]$
4		$\ldots \land \mathrm{vr}_4(\psi_e)$	

ABMC

Leading Example

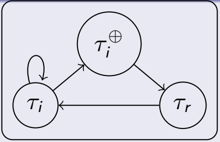
Start States: $\psi_s := x \leq 0 \land y \leq 0$ Error States: $\psi_e := y \geq 100$

$$\text{Transition Formula: } \tau := \underbrace{(x < 100 \land x' = x + 1 \land y' = y)}_{\tau_i} \lor \underbrace{(x = 100 \land x' = 0 \land y' = y + 1)}_{\tau_r}$$

$$\tau_i^{\oplus} := x + n \leq 100 \land x' = x + n \land y' = y \land n > 0$$

ABMC

$b \leftarrow 0$; add($\mathrm{vr}_b(\psi_s)$)
if check() $=$ unsat **then return** safe
while $\top$ **do**
  push(); add($\mathrm{vr}_b(\psi_e)$)
  if check() $=$ sat **then return** $\vec{\tau}$
  else
    pop(); $\vec{\tau} \leftarrow$ trace();
    if $\vec{\tau}$ *ends with loop* $\vec{\tau}^{\circlearrowleft}$ **then**
      add($\mathrm{vr}_b(\tau \lor \mathrm{accel}(\vec{\tau}^{\circlearrowleft}))$)
    else add($\mathrm{vr}_b(\tau)$)
  if check() $=$ unsat **then return** safe **else** b++



b	$\vec{\tau}$	SMT Problem	Model
0	[]	$\mathrm{vr}_0(\psi_s) \land \mathrm{vr}_0(\tau)$	$[x_1/1, \ldots /0]$
1	$[\tau_i]$	$\ldots \land \mathrm{vr}_1(\tau \lor \tau_i^{\oplus})$	$\ldots \cup [x_2/100, y_2/0]$
2	$[\tau_i, \tau_i^{\oplus}]$	$\ldots \land \mathrm{vr}_2(\tau)$	$\ldots \cup [x_3/0, y_3/1]$
3	$[\tau_i, \tau_i^{\oplus}, \tau_r]$	$\ldots \land \mathrm{vr}_3(\tau \lor \mathrm{accel}(\vec{\tau}^{\circlearrowleft}))$	$\ldots \cup [x_4/0, y_4/100]$
4		$\ldots \land \mathrm{vr}_4(\psi_e)$	

Leading Example

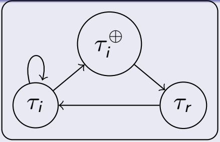
Start States: $\psi_s := x \leq 0 \wedge y \leq 0$ Error States: $\psi_e := y \geq 100$

$$\text{Transition Formula: } \tau := \underbrace{(x < 100 \wedge x' = x + 1 \wedge y' = y)}_{\tau_i} \vee \underbrace{(x = 100 \wedge x' = 0 \wedge y' = y + 1)}_{\tau_r}$$

$$\tau_i^{\oplus} := x + n \leq 100 \wedge x' = x + n \wedge y' = y \wedge n > 0$$

ABMC

$b \leftarrow 0$; add($\mathrm{vr}_b(\psi_s)$)
if check() $=$ unsat **then return** safe
while $\top$ **do**
  push(); add($\mathrm{vr}_b(\psi_e)$)
  if check() $=$ sat **then return** $\vec{\tau}$
  else
    pop(); $\vec{\tau} \leftarrow$ trace();
    if $\vec{\tau}$ *ends with loop* $\vec{\tau}^{\circlearrowleft}$ **then**
      add($\mathrm{vr}_b(\tau \vee \mathrm{accel}(\vec{\tau}^{\circlearrowleft}))$)
    else add($\mathrm{vr}_b(\tau)$)
  if check() $=$ unsat **then return** safe **else** b++



b	$\vec{\tau}$	SMT Problem	Model
0	[]	$\mathrm{vr}_0(\psi_s) \wedge \mathrm{vr}_0(\tau)$	$[x_1/1, \ldots/0]$
1	$[\tau_i]$	$\ldots \wedge \mathrm{vr}_1(\tau \vee \tau_i^{\oplus})$	$\ldots \cup [x_2/100, y_2/0]$
2	$[\tau_i, \tau_i^{\oplus}]$	$\ldots \wedge \mathrm{vr}_2(\tau)$	$\ldots \cup [x_3/0, y_3/1]$
3	$[\tau_i, \tau_i^{\oplus}, \tau_r]$	$\ldots \wedge \mathrm{vr}_3(\tau \vee \mathrm{accel}(\vec{\tau}^{\circlearrowleft}))$	$\ldots \cup [x_4/0, y_4/100]$
4		$\ldots \wedge \mathrm{vr}_4(\psi_e)$	

Leading Example

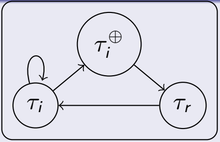
Start States: $\psi_s := x \leq 0 \land y \leq 0$ Error States: $\psi_e := y \geq 100$

$$\text{Transition Formula: } \tau := \underbrace{(x < 100 \land x' = x + 1 \land y' = y)}_{\tau_i} \lor \underbrace{(x = 100 \land x' = 0 \land y' = y + 1)}_{\tau_r}$$

$$\tau_i^{\oplus} := x + n \leq 100 \land x' = x + n \land y' = y \land n > 0$$

ABMC

$b \leftarrow 0$; add($\mathrm{vr}_b(\psi_s)$)
if check() = unsat **then return** safe
while $\top$ **do**
  push(); add($\mathrm{vr}_b(\psi_e)$)
  if check() = sat **then return** $\vec{\tau}$
  else
    pop(); $\vec{\tau} \leftarrow$ trace();
    if $\vec{\tau}$ *ends with loop* $\vec{\tau}^{\circlearrowleft}$ **then**
      add($\mathrm{vr}_b(\tau \lor \mathrm{accel}(\vec{\tau}^{\circlearrowleft}))$)
    else add($\mathrm{vr}_b(\tau)$)
  if check() = unsat **then return** safe **else** b++



b	$\vec{\tau}$	SMT Problem	Model
0	[]	$\mathrm{vr}_0(\psi_s) \land \mathrm{vr}_0(\tau)$	$[x_1/1, \ldots /0]$
1	$[\tau_i]$	$\ldots \land \mathrm{vr}_1(\tau \lor \tau_i^{\oplus})$	$\ldots \cup [x_2/100, y_2/0]$
2	$[\tau_i, \tau_i^{\oplus}]$	$\ldots \land \mathrm{vr}_2(\tau)$	$\ldots \cup [x_3/0, y_3/1]$
3	$[\tau_i, \tau_i^{\oplus}, \tau_r]$	$\ldots \land \mathrm{vr}_3(\tau \lor \mathrm{accel}(\vec{\tau}^{\circlearrowleft}))$	$\ldots \cup [x_4/0, y_4/100]$
4		$\ldots \land \mathrm{vr}_4(\psi_e)$	

ABMC

Leading Example

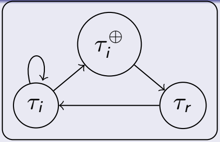
Start States: $\psi_s := x \leq 0 \land y \leq 0$ Error States: $\psi_e := y \geq 100$

Transition Formula: $\tau := \underbrace{(x < 100 \land x' = x + 1 \land y' = y)}_{\tau_i} \lor \underbrace{(x = 100 \land x' = 0 \land y' = y + 1)}_{\tau_r}$

$$\tau_i^{\oplus} := x + n \leq 100 \land x' = x + n \land y' = y \land n > 0$$

ABMC

$b \leftarrow 0$; add($\mathrm{vr}_b(\psi_s)$)
if check() = unsat **then return** safe
while $\top$ **do**
  push(); add($\mathrm{vr}_b(\psi_e)$)
  if check() = sat **then return** $\vec{\tau}$
  else
    pop(); $\vec{\tau} \leftarrow$ trace();
    if $\vec{\tau}$ *ends with loop* $\vec{\tau}^{\circlearrowleft}$ **then**
      add($\mathrm{vr}_b(\tau \lor \mathrm{accel}(\vec{\tau}^{\circlearrowleft}))$)
    else add($\mathrm{vr}_b(\tau)$)
  if check() = unsat **then return** safe **else** b++



b	$\vec{\tau}$	SMT Problem	Model
0	[]	$\mathrm{vr}_0(\psi_s) \land \mathrm{vr}_0(\tau)$	$[x_1/1, \ldots /0]$
1	$[\tau_i]$	$\ldots \land \mathrm{vr}_1(\tau \lor \tau_i^{\oplus})$	$\ldots \cup [x_2/100, y_2/0]$
2	$[\tau_i, \tau_i^{\oplus}]$	$\ldots \land \mathrm{vr}_2(\tau)$	$\ldots \cup [x_3/0, y_3/1]$
3	$[\tau_i, \tau_i^{\oplus}, \tau_r]$	$\ldots \land \mathrm{vr}_3(\tau \lor \mathrm{accel}(\vec{\tau}^{\circlearrowleft}))$	$\ldots \cup [x_4/0, y_4/100]$
4		$\ldots \land \mathrm{vr}_4(\psi_e)$	

ABMC

Leading Example

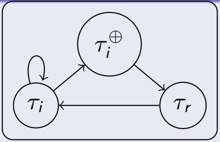
Start States: $\psi_s := x \leq 0 \land y \leq 0$ Error States: $\psi_e := y \geq 100$

$$\text{Transition Formula: } \tau := \underbrace{(x < 100 \land x' = x + 1 \land y' = y)}_{\tau_i} \lor \underbrace{(x = 100 \land x' = 0 \land y' = y + 1)}_{\tau_r}$$

$$\tau_i^{\oplus} := x + n \leq 100 \land x' = x + n \land y' = y \land n > 0$$

ABMC

$b \leftarrow 0$; add($\mathrm{vr}_b(\psi_s)$)
if check() $=$ unsat **then return** safe
while $\top$ **do**
  push(); add($\mathrm{vr}_b(\psi_e)$)
  if check() $=$ sat **then return** $\vec{\tau}$
  else
    pop(); $\vec{\tau} \leftarrow$ trace();
    if *$\vec{\tau}$ ends with loop $\vec{\tau}^{\circlearrowleft}$* **then**
      add($\mathrm{vr}_b(\tau \lor \mathrm{accel}(\vec{\tau}^{\circlearrowleft}))$)
    else add($\mathrm{vr}_b(\tau)$)
  if check() $=$ unsat **then return** safe **else** b++



b	$\vec{\tau}$	SMT Problem	Model
0	[]	$\mathrm{vr}_0(\psi_s) \land \mathrm{vr}_0(\tau)$	$[x_1/1, \ldots/0]$
1	$[\tau_i]$	$\ldots \land \mathrm{vr}_1(\tau \lor \tau_i^{\oplus})$	$\ldots \cup [x_2/100, y_2/0]$
2	$[\tau_i, \tau_i^{\oplus}]$	$\ldots \land \mathrm{vr}_2(\tau)$	$\ldots \cup [x_3/0, y_3/1]$
3	$[\tau_i, \tau_i^{\oplus}, \tau_r]$	$\ldots \land \mathrm{vr}_3(\tau \lor \mathrm{accel}(\vec{\tau}^{\circlearrowleft}))$	$\ldots \cup [x_4/0, y_4/100]$
4		$\ldots \land \mathrm{vr}_4(\psi_e)$	

ABMC

Leading Example

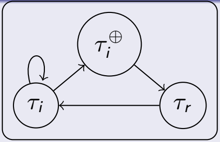
Start States: $\psi_s := x \le 0 \land y \le 0$ Error States: $\psi_e := y \ge 100$

Transition Formula: $\tau := \underbrace{(x < 100 \land x' = x + 1 \land y' = y)}_{\tau_i} \lor \underbrace{(x = 100 \land x' = 0 \land y' = y + 1)}_{\tau_r}$

$$\tau_i^{\oplus} := x + n \le 100 \land x' = x + n \land y' = y \land n > 0$$

ABMC

$b \leftarrow 0$; add($\mathrm{vr}_b(\psi_s)$)
if check() = unsat **then return** safe
while $\top$ **do**
  push(); add($\mathrm{vr}_b(\psi_e)$)
  if check() = sat **then return** $\vec{\tau}$
  else
    pop(); $\vec{\tau} \leftarrow$ trace();
    if *$\vec{\tau}$ ends with loop $\vec{\tau}^{\circlearrowleft}$* **then**
      add($\mathrm{vr}_b(\tau \lor \mathrm{accel}(\vec{\tau}^{\circlearrowleft}))$)
    else add($\mathrm{vr}_b(\tau)$)
  if check() = unsat **then return** safe **else** b++



b	$\vec{\tau}$	SMT Problem	Model
0	[]	$\mathrm{vr}_0(\psi_s) \land \mathrm{vr}_0(\tau)$	$[x_1/1, \dots /0]$
1	$[\tau_i]$	$\dots \land \mathrm{vr}_1(\tau \lor \tau_i^{\oplus})$	$\dots \cup [x_2/100, y_2/0]$
2	$[\tau_i, \tau_i^{\oplus}]$	$\dots \land \mathrm{vr}_2(\tau)$	$\dots \cup [x_3/0, y_3/1]$
3	$[\tau_i, \underbrace{\tau_i^{\oplus}, \tau_r}_{\vec{\tau}^{\circlearrowleft}}]$	$\dots \land \mathrm{vr}_3(\tau \lor \mathrm{accel}(\vec{\tau}^{\circlearrowleft}))$	$\dots \cup [x_4/0, y_4/100]$
4		$\dots \land \mathrm{vr}_4(\psi_e)$	

Leading Example

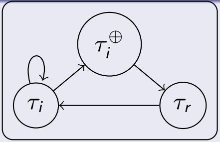
$$\text{Start States: } \psi_s := x \leq 0 \land y \leq 0 \qquad \text{Error States: } \psi_e := y \geq 100$$

$$\text{Transition Formula: } \tau := \underbrace{(x < 100 \land x' = x + 1 \land y' = y)}_{\tau_i} \lor \underbrace{(x = 100 \land x' = 0 \land y' = y + 1)}_{\tau_r}$$

$$\tau_i^{\oplus} := x + n \leq 100 \land x' = x + n \land y' = y \land n > 0$$

ABMC

$b \leftarrow 0$; add($\mathsf{vr}_b(\psi_s)$)
if check() $=$ unsat **then return** safe
while $\top$ **do**
  push(); add($\mathsf{vr}_b(\psi_e)$)
  if check() $=$ sat **then return** $\vec{\tau}$
  else
    pop(); $\vec{\tau} \leftarrow$ trace();
    if $\vec{\tau}$ *ends with loop* $\vec{\tau}^{\circlearrowleft}$ **then**
      add($\mathsf{vr}_b(\tau \lor \mathsf{accel}(\vec{\tau}^{\circlearrowleft}))$)
    else add($\mathsf{vr}_b(\tau)$)
  if check() $=$ unsat **then return** safe **else** b++



b	$\vec{\tau}$	SMT Problem	Model
0	[]	$\mathsf{vr}_0(\psi_s) \land \mathsf{vr}_0(\tau)$	$[x_1/1, \ldots/0]$
1	$[\tau_i]$	$\ldots \land \mathsf{vr}_1(\tau \lor \tau_i^{\oplus})$	$\ldots \cup [x_2/100, y_2/0]$
2	$[\tau_i, \tau_i^{\oplus}]$	$\ldots \land \mathsf{vr}_2(\tau)$	$\ldots \cup [x_3/0, y_3/1]$
3	$\underbrace{[\tau_i, \tau_i^{\oplus}, \tau_r]}_{\vec{\tau}^{\circlearrowleft}}$	$\ldots \land \mathsf{vr}_3(\tau \lor \mathsf{accel}(\vec{\tau}^{\circlearrowleft}))$	$\ldots \cup [x_4/0, y_4/100]$
4		$\ldots \land \mathsf{vr}_4(\psi_e)$	

Leading Example

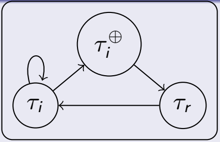
$$\text{Start States: } \psi_s := x \leq 0 \wedge y \leq 0 \qquad \text{Error States: } \psi_e := y \geq 100$$

$$\text{Transition Formula: } \tau := \underbrace{(x < 100 \wedge x' = x + 1 \wedge y' = y)}_{\tau_i} \vee \underbrace{(x = 100 \wedge x' = 0 \wedge y' = y + 1)}_{\tau_r}$$

$$\tau_i^{\oplus} := x + n \leq 100 \wedge x' = x + n \wedge y' = y \wedge n > 0$$

ABMC

$b \leftarrow 0$; add($\mathrm{vr}_b(\psi_s)$)
if check() = unsat **then return** safe
while $\top$ **do**
  push(); add($\mathrm{vr}_b(\psi_e)$)
  if check() = sat **then return** $\vec{\tau}$
  else
    pop(); $\vec{\tau} \leftarrow$ trace();
    if $\vec{\tau}$ *ends with loop* $\vec{\tau}^{\circlearrowleft}$ **then**
      add($\mathrm{vr}_b(\tau \vee \mathrm{accel}(\vec{\tau}^{\circlearrowleft}))$)
    else add($\mathrm{vr}_b(\tau)$)
  if check() = unsat **then return** safe **else** b++



b	$\vec{\tau}$	SMT Problem	Model
0	[]	$\mathrm{vr}_0(\psi_s) \wedge \mathrm{vr}_0(\tau)$	$[x_1/1, \ldots /0]$
1	$[\tau_i]$	$\ldots \wedge \mathrm{vr}_1(\tau \vee \tau_i^{\oplus})$	$\ldots \cup [x_2/100, y_2/0]$
2	$[\tau_i, \tau_i^{\oplus}]$	$\ldots \wedge \mathrm{vr}_2(\tau)$	$\ldots \cup [x_3/0, y_3/1]$
3	$\underbrace{[\tau_i, \tau_i^{\oplus}, \tau_r]}_{\vec{\tau}^{\circlearrowleft}}$	$\ldots \wedge \mathrm{vr}_3(\tau \vee \mathrm{accel}(\vec{\tau}^{\circlearrowleft}))$	$\ldots \cup [x_4/0, y_4/100]$
4		$\ldots \wedge \mathrm{vr}_4(\psi_e)$	

ABMC

Leading Example

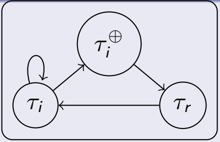
Start States: $\psi_s := x \leq 0 \land y \leq 0$ Error States: $\psi_e := y \geq 100$

$$\text{Transition Formula: } \tau := \underbrace{(x < 100 \land x' = x + 1 \land y' = y)}_{\tau_i} \lor \underbrace{(x = 100 \land x' = 0 \land y' = y + 1)}_{\tau_r}$$

$$\tau_i^{\oplus} := x + n \leq 100 \land x' = x + n \land y' = y \land n > 0$$

ABMC

$b \leftarrow 0$; add($\mathrm{vr}_b(\psi_s)$)
if check() = unsat **then return** safe
while $\top$ **do**
  push(); add($\mathrm{vr}_b(\psi_e)$)
  if check() = sat **then return** $\vec{\tau}$
  else
    pop(); $\vec{\tau} \leftarrow$ trace();
    if $\vec{\tau}$ *ends with loop* $\vec{\tau}^{\circlearrowleft}$ **then**
      add($\mathrm{vr}_b(\tau \lor \mathrm{accel}(\vec{\tau}^{\circlearrowleft}))$)
    else add($\mathrm{vr}_b(\tau)$)
  if check() = unsat **then return** safe **else** b++



b	$\vec{\tau}$	SMT Problem	Model
0	[]	$\mathrm{vr}_0(\psi_s) \land \mathrm{vr}_0(\tau)$	$[x_1/1, \dots /0]$
1	$[\tau_i]$	$\dots \land \mathrm{vr}_1(\tau \lor \tau_i^{\oplus})$	$\dots \cup [x_2/100, y_2/0]$
2	$[\tau_i, \tau_i^{\oplus}]$	$\dots \land \mathrm{vr}_2(\tau)$	$\dots \cup [x_3/0, y_3/1]$
3	$\underbrace{[\tau_i, \tau_i^{\oplus}, \tau_r]}_{\vec{\tau}^{\circlearrowleft}}$	$\dots \land \mathrm{vr}_3(\tau \lor \mathrm{accel}(\vec{\tau}^{\circlearrowleft}))$	$\dots \cup [x_4/0, y_4/100]$
4		$\dots \land \mathrm{vr}_4(\psi_e)$	

ABMC

Leading Example

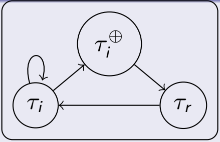
Start States: $\psi_s := x \leq 0 \land y \leq 0$ Error States: $\psi_e := y \geq 100$

Transition Formula: $\tau := \underbrace{(x < 100 \land x' = x + 1 \land y' = y)}_{\tau_i} \lor \underbrace{(x = 100 \land x' = 0 \land y' = y + 1)}_{\tau_r}$

$$\tau_i^{\oplus} := x + n \leq 100 \land x' = x + n \land y' = y \land n > 0$$

ABMC

$b \leftarrow 0$; add($\mathrm{vr}_b(\psi_s)$)
if check() = unsat **then return** safe
while $\top$ **do**
  push(); add($\mathrm{vr}_b(\psi_e)$)
  if check() = sat **then return** $\vec{\tau}$
  else
    pop(); $\vec{\tau} \leftarrow$ trace();
    if $\vec{\tau}$ *ends with loop* $\vec{\tau}^{\circlearrowleft}$ **then**
      add($\mathrm{vr}_b(\tau \lor \mathrm{accel}(\vec{\tau}^{\circlearrowleft}))$)
    else add($\mathrm{vr}_b(\tau)$)
  if check() = unsat **then return** safe **else** b++



b	$\vec{\tau}$	SMT Problem	Model
0	[]	$\mathrm{vr}_0(\psi_s) \land \mathrm{vr}_0(\tau)$	$[x_1/1, \ldots /0]$
1	$[\tau_i]$	$\ldots \land \mathrm{vr}_1(\tau \lor \tau_i^{\oplus})$	$\ldots \cup [x_2/100, y_2/0]$
2	$[\tau_i, \tau_i^{\oplus}]$	$\ldots \land \mathrm{vr}_2(\tau)$	$\ldots \cup [x_3/0, y_3/1]$
3	$[\underbrace{\tau_i, \tau_i^{\oplus}, \tau_r}_{\vec{\tau}^{\circlearrowleft}}]$	$\ldots \land \mathrm{vr}_3(\tau \lor \mathrm{accel}(\vec{\tau}^{\circlearrowleft}))$	$\ldots \cup [x_4/0, y_4/100]$
4		$\ldots \land \mathrm{vr}_4(\psi_e)$	

Leading Example

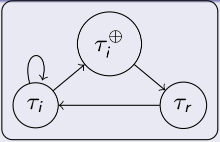
$$\text{Start States: } \psi_s := x \leq 0 \land y \leq 0 \qquad \text{Error States: } \psi_e := y \geq 100$$

$$\text{Transition Formula: } \tau := \underbrace{(x < 100 \land x' = x + 1 \land y' = y)}_{\tau_i} \lor \underbrace{(x = 100 \land x' = 0 \land y' = y + 1)}_{\tau_r}$$

$$\tau_i^{\oplus} := x + n \leq 100 \land x' = x + n \land y' = y \land n > 0$$

ABMC

$b \leftarrow 0$; add($\mathsf{vr}_b(\psi_s)$)
if check() $=$ unsat **then return** safe
while $\top$ **do**
  push(); add($\mathsf{vr}_b(\psi_e)$)
  if check() $=$ sat **then return** $\vec{\tau}$
  else
    pop(); $\vec{\tau} \leftarrow$ trace();
    if $\vec{\tau}$ *ends with loop* $\vec{\tau}^{\circlearrowleft}$ **then**
      add($\mathsf{vr}_b(\tau \lor \mathsf{accel}(\vec{\tau}^{\circlearrowleft}))$)
    else add($\mathsf{vr}_b(\tau)$)
  if check() $=$ unsat **then return** safe **else** b++



b	$\vec{\tau}$	SMT Problem	Model
0	[]	$\mathsf{vr}_0(\psi_s) \land \mathsf{vr}_0(\tau)$	$[x_1/1, \ldots/0]$
1	$[\tau_i]$	$\ldots \land \mathsf{vr}_1(\tau \lor \tau_i^{\oplus})$	$\ldots \cup [x_2/100, y_2/0]$
2	$[\tau_i, \tau_i^{\oplus}]$	$\ldots \land \mathsf{vr}_2(\tau)$	$\ldots \cup [x_3/0, y_3/1]$
3	$\underbrace{[\tau_i, \tau_i^{\oplus}, \tau_r]}_{\vec{\tau}^{\circlearrowleft}}$	$\ldots \land \mathsf{vr}_3(\tau \lor \mathsf{accel}(\vec{\tau}^{\circlearrowleft}))$	$\ldots \cup [x_4/0, y_4/100]$
4		$\ldots \land \mathsf{vr}_4(\psi_e)$	

Leading Example

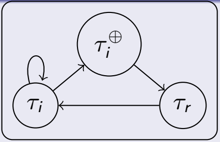
Start States: $\psi_s := x \leq 0 \land y \leq 0$ Error States: $\psi_e := y \geq 100$

$$\text{Transition Formula: } \tau := \underbrace{(x < 100 \land x' = x + 1 \land y' = y)}_{\tau_i} \lor \underbrace{(x = 100 \land x' = 0 \land y' = y + 1)}_{\tau_r}$$

$$\tau_i^{\oplus} := x + n \leq 100 \land x' = x + n \land y' = y \land n > 0$$

ABMC

$b \leftarrow 0;$ add($\mathrm{vr}_b(\psi_s)$)
if check() $=$ unsat **then return** safe
while $\top$ **do**
  push(); add($\mathrm{vr}_b(\psi_e)$)
  if check() $=$ sat **then return** $\vec{\tau}$
  else
    pop(); $\vec{\tau} \leftarrow$ trace();
    if $\vec{\tau}$ *ends with loop* $\vec{\tau}^{\circlearrowleft}$ **then**
      add($\mathrm{vr}_b(\tau \lor \mathrm{accel}(\vec{\tau}^{\circlearrowleft}))$)
    else add($\mathrm{vr}_b(\tau)$)
  if check() $=$ unsat **then return** safe **else** b++



b	$\vec{\tau}$	SMT Problem	Model
0	[]	$\mathrm{vr}_0(\psi_s) \land \mathrm{vr}_0(\tau)$	$[x_1/1, \ldots/0]$
1	$[\tau_i]$	$\ldots \land \mathrm{vr}_1(\tau \lor \tau_i^{\oplus})$	$\ldots \cup [x_2/100, y_2/0]$
2	$[\tau_i, \tau_i^{\oplus}]$	$\ldots \land \mathrm{vr}_2(\tau)$	$\ldots \cup [x_3/0, y_3/1]$
3	$\underbrace{[\tau_i, \tau_i^{\oplus}, \tau_r]}_{\vec{\tau}^{\circlearrowleft}}$	$\ldots \land \mathrm{vr}_3(\tau \lor \mathrm{accel}(\vec{\tau}^{\circlearrowleft}))$	$\ldots \cup [x_4/0, y_4/100]$
4		$\ldots \land \mathrm{vr}_4(\psi_e)$	

Leading Example

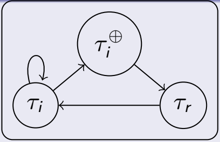
$$\text{Start States: } \psi_s := x \le 0 \wedge y \le 0 \qquad \text{Error States: } \psi_e := y \ge 100$$

$$\text{Transition Formula: } \tau := \underbrace{(x < 100 \wedge x' = x + 1 \wedge y' = y)}_{\tau_i} \vee \underbrace{(x = 100 \wedge x' = 0 \wedge y' = y + 1)}_{\tau_r}$$

$$\tau_i^{\oplus} := x + n \le 100 \wedge x' = x + n \wedge y' = y \wedge n > 0$$

ABMC

$b \leftarrow 0$; add($\mathrm{vr}_b(\psi_s)$)
if check() $=$ unsat **then return** safe
while $\top$ **do**
  push(); add($\mathrm{vr}_b(\psi_e)$)
  if check() $=$ sat **then return** $\vec{\tau}$
  else
    pop(); $\vec{\tau} \leftarrow$ trace();
    if $\vec{\tau}$ *ends with loop* $\vec{\tau}^{\circlearrowleft}$ **then**
      add($\mathrm{vr}_b(\tau \vee \mathrm{accel}(\vec{\tau}^{\circlearrowleft}))$)
    else add($\mathrm{vr}_b(\tau)$)
  if check() $=$ unsat **then return** safe **else** b++



b	$\vec{\tau}$	SMT Problem	Model
0	[]	$\mathrm{vr}_0(\psi_s) \wedge \mathrm{vr}_0(\tau)$	$[x_1/1, \ldots/0]$
1	$[\tau_i]$	$\ldots \wedge \mathrm{vr}_1(\tau \vee \tau_i^{\oplus})$	$\ldots \cup [x_2/100, y_2/0]$
2	$[\tau_i, \tau_i^{\oplus}]$	$\ldots \wedge \mathrm{vr}_2(\tau)$	$\ldots \cup [x_3/0, y_3/1]$
3	$\underbrace{[\tau_i, \tau_i^{\oplus}, \tau_r]}_{\vec{\tau}^{\circlearrowleft}}$	$\ldots \wedge \mathrm{vr}_3(\tau \vee \mathrm{accel}(\vec{\tau}^{\circlearrowleft}))$	$\ldots \cup [x_4/0, y_4/100]$
4		$\ldots \wedge \mathrm{vr}_4(\psi_e)$	

ABMC

Leading Example

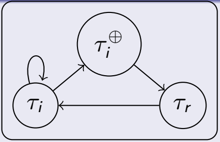
Start States: $\psi_s := x \leq 0 \land y \leq 0$ Error States: $\psi_e := y \geq 100$

Transition Formula: $\tau := \underbrace{(x < 100 \land x' = x + 1 \land y' = y)}_{\tau_i} \lor \underbrace{(x = 100 \land x' = 0 \land y' = y + 1)}_{\tau_r}$

$$\tau_i^{\oplus} := x + n \leq 100 \land x' = x + n \land y' = y \land n > 0$$

ABMC

$b \leftarrow 0$; add($\mathrm{vr}_b(\psi_s)$)
if check() $=$ unsat **then return** safe
while $\top$ **do**
  push(); add($\mathrm{vr}_b(\psi_e)$)
  if check() $=$ sat **then** **return** $\vec{\tau}$
  else
    pop(); $\vec{\tau} \leftarrow$ trace();
    if $\vec{\tau}$ *ends with loop* $\vec{\tau}^{\circlearrowleft}$ **then**
      add($\mathrm{vr}_b(\tau \lor \mathrm{accel}(\vec{\tau}^{\circlearrowleft}))$)
    else add($\mathrm{vr}_b(\tau)$)
  if check() $=$ unsat **then** **return** safe **else** b++



b	$\vec{\tau}$	SMT Problem	Model
0	[]	$\mathrm{vr}_0(\psi_s) \land \mathrm{vr}_0(\tau)$	$[x_1/1, \ldots/0]$
1	$[\tau_i]$	$\ldots \land \mathrm{vr}_1(\tau \lor \tau_i^{\oplus})$	$\ldots \cup [x_2/100, y_2/0]$
2	$[\tau_i, \tau_i^{\oplus}]$	$\ldots \land \mathrm{vr}_2(\tau)$	$\ldots \cup [x_3/0, y_3/1]$
3	$[\underbrace{\tau_i, \tau_i^{\oplus}, \tau_r}_{\vec{\tau}^{\circlearrowleft}}]$	$\ldots \land \mathrm{vr}_3(\tau \lor \mathrm{accel}(\vec{\tau}^{\circlearrowleft}))$	$\ldots \cup [x_4/0, y_4/100]$
4		$\ldots \land \mathrm{vr}_4(\psi_e)$	

Evaluation

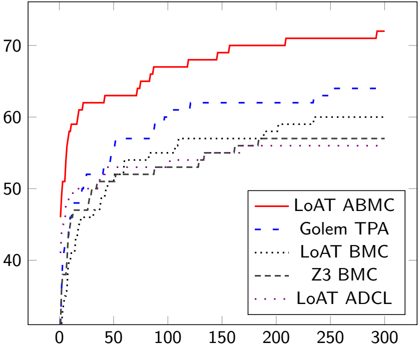
CHC-Comp '23 Benchmarks	unsafe ✓	safe ✓
LoAT ABMC	72	75
Golem TPA	64	83
LoAT BMC	60	36
Z3 BMC	57	21
LoAT ADCL	56	0
Golem BMC	55	20
Spacer (Z3)	51	151
Eldarica	46	107

x: runtime in s
y: unsat proofs

x: length of c.ex.
y: unsat proofs

Evaluation

CHC-Comp '23 Benchmarks	unsafe ✓	safe ✓
LoAT ABMC	72	75
Golem TPA	64	83
LoAT BMC	60	36
Z3 BMC	57	21
LoAT ADCL	56	0
Golem BMC	55	20
Spacer (Z3)	51	151
Eldarica	46	107

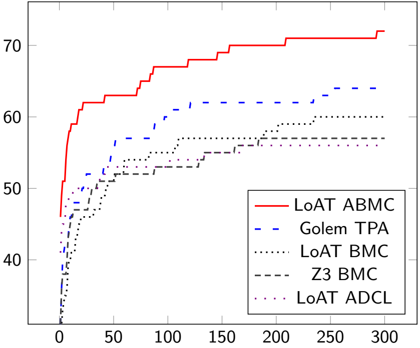


x: runtime in s
y: unsat proofs

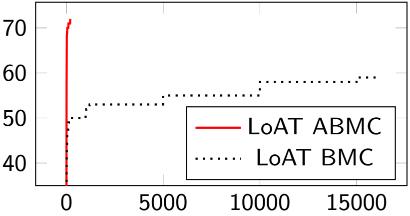
x: length of c.ex.
y: unsat proofs

Evaluation

CHC-Comp '23 Benchmarks	unsafe ✓	safe ✓
LoAT ABMC	72	75
Golem TPA	64	83
LoAT BMC	60	36
Z3 BMC	57	21
LoAT ADCL	56	0
Golem BMC	55	20
Spacer (Z3)	51	151
Eldarica	46	107



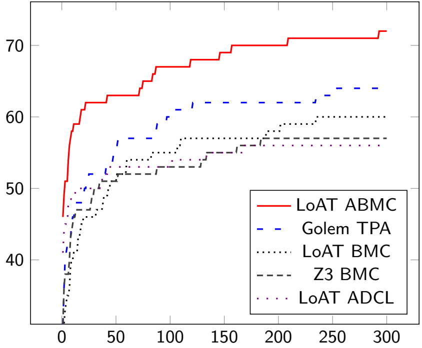
x: runtime in s
y: unsat proofs



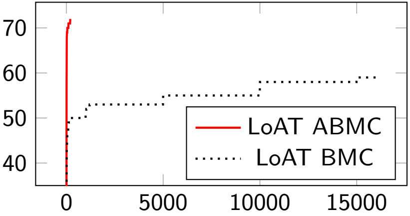
x: length of c.ex.
y: unsat proofs

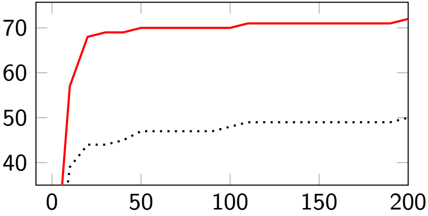
Evaluation

CHC-Comp '23 Benchmarks	unsafe ✓	safe ✓
LoAT ABMC	72	75
Golem TPA	64	83
LoAT BMC	60	36
Z3 BMC	57	21
LoAT ADCL	56	0
Golem BMC	55	20
Spacer (Z3)	51	151
Eldarica	46	107



x: runtime in s
y: unsat proofs





x: length of c.ex.
y: unsat proofs

Acceleration rocks!

See paper for...

- **lazy exploration of dependency graph**
- **heuristics to fine-tune acceleration**
- **proving safety via Blocking Clauses**

`https://loat-developers.github.io/LoAT/`

Acceleration rocks!

See paper for...

- **lazy exploration of dependency graph**
- **heuristics to fine-tune acceleration**
- **proving safety via Blocking Clauses**

https://loat-developers.github.io/LoAT/

Acceleration rocks!

See paper for...

- **lazy exploration of dependency graph**
- **heuristics to fine-tune acceleration**
- **proving safety via Blocking Clauses**

https://loat-developers.github.io/LoAT/

Acceleration rocks!

See paper for...

- **lazy exploration of dependency graph**
- **heuristics to fine-tune acceleration**
- **proving safety via Blocking Clauses**

https://loat-developers.github.io/LoAT/

Acceleration rocks!

See paper for...

- **lazy exploration of dependency graph**
- **heuristics to fine-tune acceleration**
- **proving safety via Blocking Clauses**

https://loat-developers.github.io/LoAT/

Acceleration rocks!

See paper for...

- **lazy exploration of dependency graph**
- **heuristics to fine-tune acceleration**
- **proving safety via Blocking Clauses**

`https://loat-developers.github.io/LoAT/`