

Lyapunov Abstractions for Inevitability of Hybrid Systems

Parasara Sridhar Duggirala & Sayan Mitra

{duggira3, mitras}@illinois.edu

University of Illinois at Urbana-Champaign

HSCC, CPSWeek, Beijing

April, 2012

Inevitability Property

- **Definition.** A set of **states S** of **system A** is **inevitable** if every execution starting from arbitrary state reaches S in bounded time
- **Examples:**
 - Autonomous vehicle reaches destination
 - Routing protocol recovers from failures
 - Traffic control protocol **does not** deadlock

} in bounded time

Inevitability of Hybrid Systems

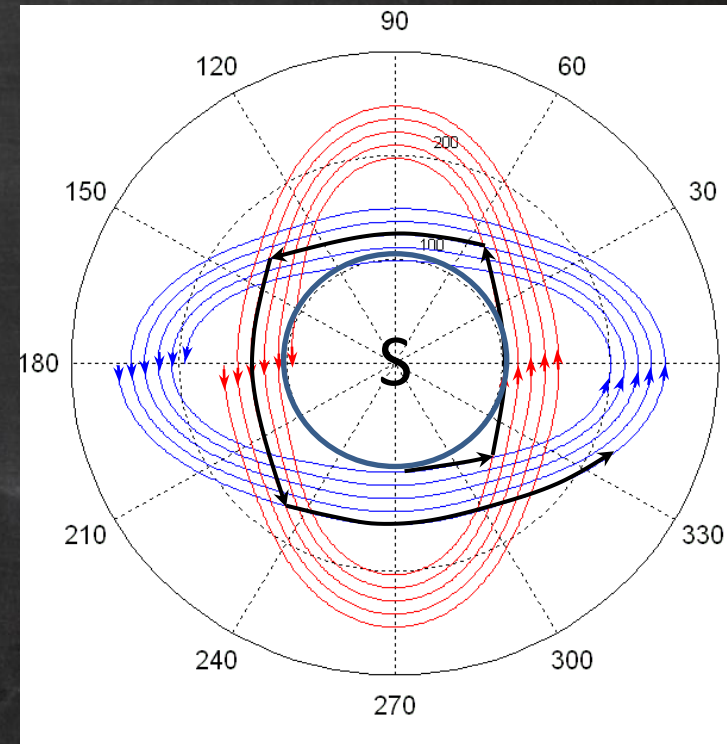
If S is inevitable for each of the individual dynamical subsystems, S may not be inevitable for combined hybrid system

Goal: Design algorithm for verifying inevitability of HA. Given

- (a) HA A and a set S , it should either produce
- (b) a proof that S is inevitable OR
- (c) a counter-example behavior of A that does not ever reach S

What is a proof?

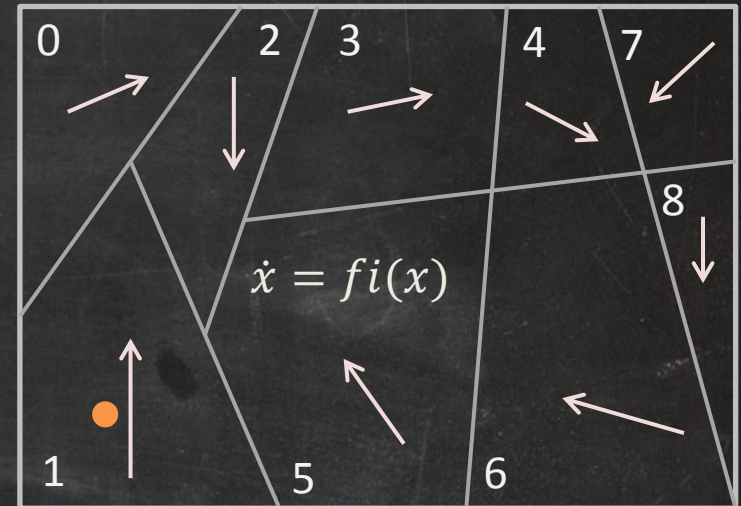
What is a counter-example ?



Hybrid Automata (HA)

- $A = \langle X, L, Q_0, D, T \rangle$
- L : set of *locations*
- X : set of *continuous variables* $\{x_1, x_2, v_1, v_2\}$
- Q : state space = $\mathbb{R}^4 \times L$
- $D \subseteq Q \times Q$ *discrete transitions*
- T : *trajectories* each $\tau \in T, \tau : [0, t] \rightarrow Q$
- over which continuous variables flow according to $\dot{x} = fi(x)$
 - Rectangular HA: $\dot{x} \in [a_i, b_i]$
 - Linear HA: $\dot{x} = Aix + bi$
- An *execution* of A is a sequence $\tau_0, \tau_1, \tau_2, \dots$
- Assume A is *non-blocking*, i.e, if time diverges along **every** execution

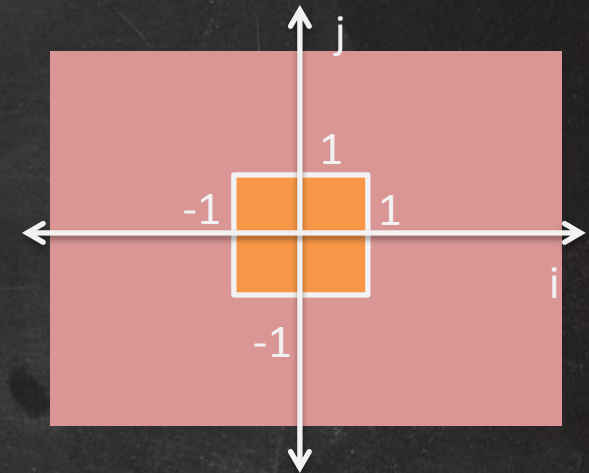
guard



Termination of Programs: An Example

```
integer i,j; /* initially arbitrary */
while (|i| > 1 or |j| > 1)
    { i = i + j; j = j - 1; }
```

- Program terminates if transition relation T_A is *well-founded*
- *Transition relation*
- T_A : If ($|i| > 1$ OR $|j| > 1$) then ($i' = i+j$ AND $j' = j-1$)
- For above program T_A is not well-founded
- $(4,2) \rightarrow (6,1) \rightarrow (7,0) \rightarrow (7,-1) \rightarrow (6,-2) \rightarrow (4,-3) \dots$
- $(-4,2) \rightarrow (-2,1) \rightarrow (-1,1)$ stops
- But, $I \wedge T_A$ is, where $I \triangleq |i + j(j+1)/2| \leq 1 \wedge j \leq 1$



Does not have infinite chains $q_0 q_1 \dots$ where $q_i T_A q_{i+1}$
 $T_1 = \{ \langle q, q' \rangle \mid q' = q + 1 \}$
 $T_2 = \{ \langle q, q' \rangle \mid q' = q + 1 \wedge q' < 5 \}$

Outline

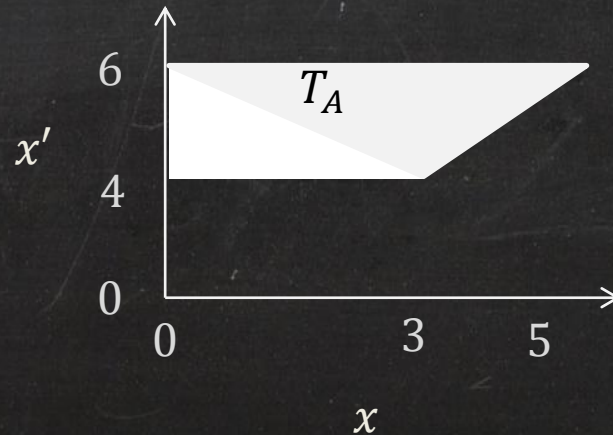
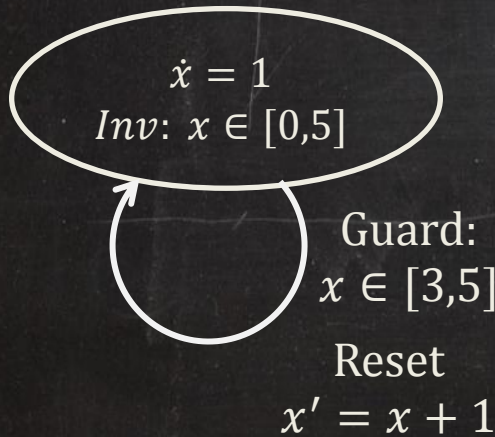
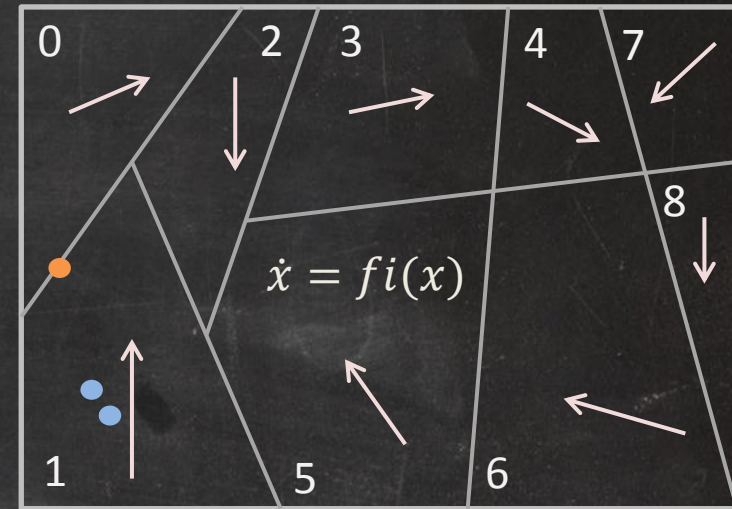
- Background
- Hybrid Step Relation
- Abstraction Refinement Algorithm
 - Rectangular systems
- Conclusions

Hybrid Step Relation

Definition. $T_A \subseteq Q \times Q$ **hybrid step relation (HSR)**

$(q, q') \in T_A \iff$ there exists q'' such that there exists a trajectory from q to q'' and a transition from q'' to q'

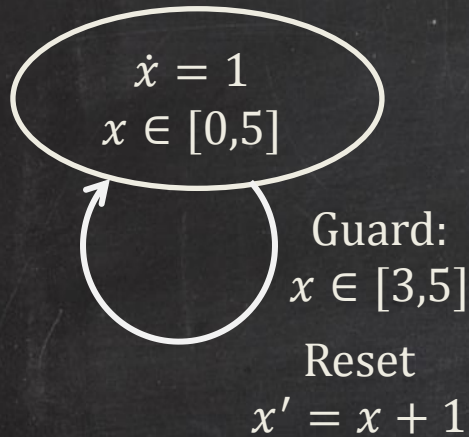
Example:



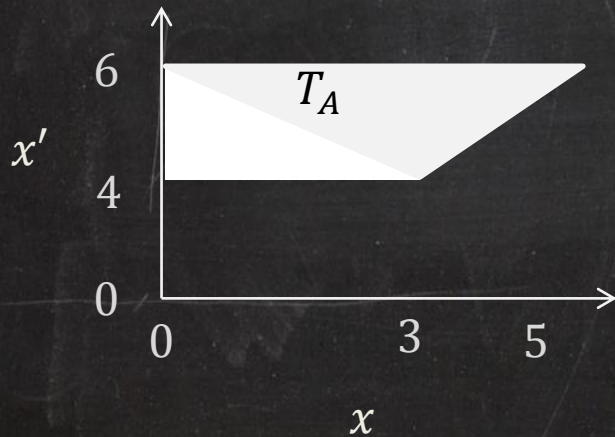
$0 \leq x \leq 5$ AND
 $\exists t: 3 \leq x + t \leq 5$ AND
 $x + t + 1 = x'$
 After quantifier elimination

$0 \leq x \leq 5$ AND
 $x + 1 \leq x'$ AND
 $4 \leq x' \leq 6$

Is it possible to perform this self-loop infinitely many times ?



- (0,4) (4,5) (5,6) stop
- All finite sequences



$$0 \leq x \leq 5 \text{ AND } x + 1 \leq x' \text{ AND } 4 \leq x' \leq 6$$

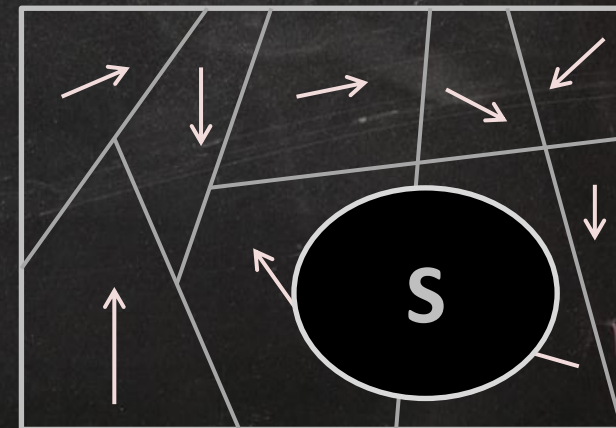
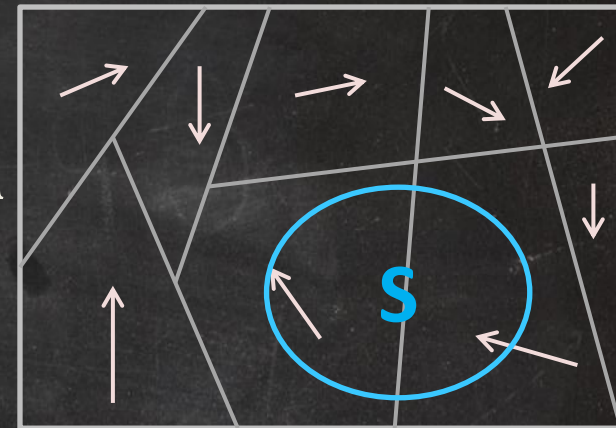
Inevitability and Well-foundedness

Theorem 1. S is inevitable for A iff hybrid-step relation $T_{A/S}$ for A/S is **well-founded**

Definition: $A/S =$ obtained by removing S from A

Remove transitions from S

All trajectories stop at S



Proof Sketch

- **Theorem 1.** S is inevitable for A iff hybrid-step relation $T_{A/S}$ for A/S is well-founded
- ($T_{A/S}$ Well-founded $\Rightarrow S$ is inevitable for A)
 - If $T_{A/S}$ is well founded then there are no infinite chains outside S
 - Every execution outside S has finitely many transitions
 - Since, finite duration elapses between transitions (local nonblocking), total time outside S is also finite \Rightarrow Since, A is non-blocking, S is inevitable
- (S is inevitable for $A \Rightarrow T_{A/S}$ Well-founded)
 - Suppose there is an infinite decreasing chain $q_0 q_1 \dots$ in $T_{A/S}$
 - Chain corresponds to an execution α with infinitely many transitions outside S
 - Time diverges in α (nonZeno) outside S , which contradicts inevitability of S

Hybrid Step Relations for Loops

Theorem 1. S is inevitable for A iff $T_{A/S} \subseteq R$, R is well-founded

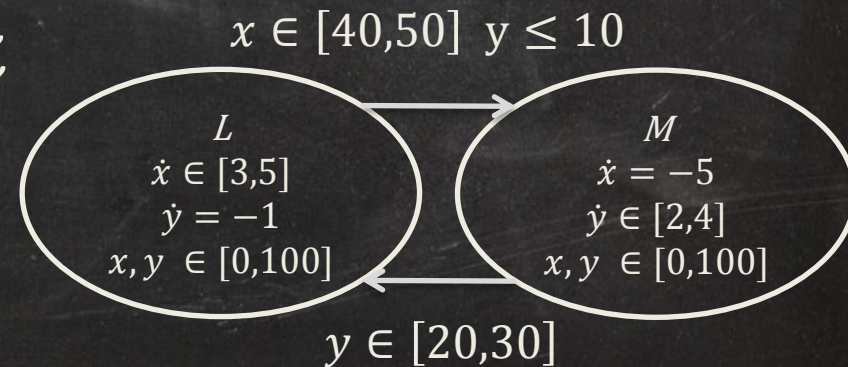
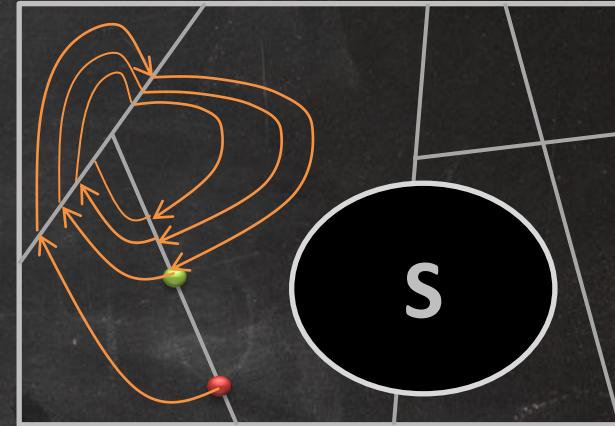
Using [Podelski & Rybalchenko 2004]

Theorem 2. S is inevitable for A iff $T_{A/S}^+ \subseteq \bigcup_{i=1}^n R_i$, where $\{R_i\}$ is a collection of well-founded relations and $T_{A/S}^+$ is the transitive closure of $T_{A/S}$

- $(a, c) \in T_{A/S}^+$ iff $a T_{A/S} b_1 T_{A/S} b_2 T_{A/S} \dots T_{A/S} c$
- $(q, q') \in T_{A/S}^+$ iff there is execution $\alpha: q$ to q'
- Need to show that every execution is well-founded
- Suffices to consider loops, i.e., executions starting and ending at the same location $q.\text{loc} = q'.\text{loc}$

Using Disjoint Union of Well-founded Relations

- For every loop O , find a well-founded relation R_i containing T_O
- Example, Rectangular HA:
- $T_{MLM} =$
 $(x, y \in [0, 100] \text{ AND } x' \in [40, 50] \text{ AND } y' \leq 10 \text{ AND } x' - x \in [-25, -1] \text{ AND } y' \geq y + 2)$
- T_{MLM} can be computed and
- Well-foundedness of T_{MLM} can be checked using linear functions over x, x', y, y' e.g. using **Rankfinder**



General Dynamics

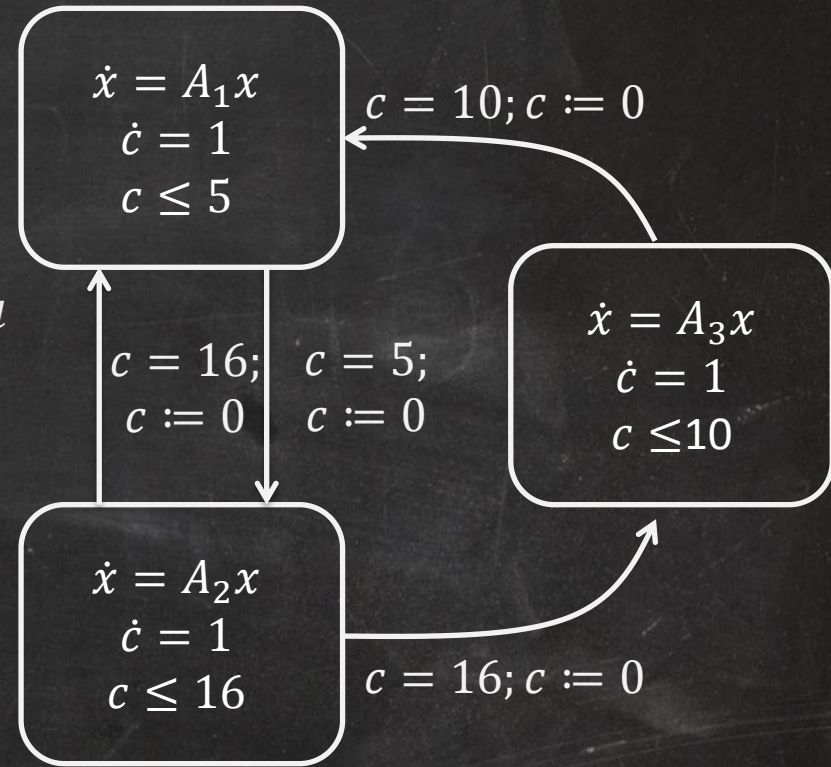
- For a location $l \in L$ suppose we have a Lyapunov-like function $V_l: \mathbb{R}^4 \rightarrow \mathbb{R}$ with
 - **(stable)** $\exists \lambda_l < 0$ and $B_l > 0$ such that for any trajectory τ in $l \in L$, $V_l(\tau(t)) \leq B_l e^{\lambda_l t} V_l(\tau(0))$
 - OR
 - **(unstable)** $\exists \lambda_l > 0$ and $B_l > 0$ such that for any trajectory τ in $l \in L$, $V_l(\tau(t)) \leq B_l e^{\lambda_l t} V_l(\tau(0))$
- We can over-approximate T_A^+ hybrid step relation if we know bounds on dwell time

Lyapunov Abstraction

- $\mathcal{V} = \{V_{l,i}\}_{i=1}^k$: Collection of k Lyapunov functions for location l
- Abstraction: $\beta: \mathbb{R}^n \rightarrow \mathbb{R}^k$
 - $\beta_{\mathcal{V}}(x) = V_{l,1}(x), \dots, V_{l,k}(x)$ where $x.loc = l$
- Abstraction of HSR
 - $\beta_{\mathcal{V}}(\Gamma) = \{(y, y') \mid \exists x, x': \beta(y) = x \wedge \beta(x') = y'\}$
- **Theorem:** If $\beta_{\mathcal{V}}(\Gamma)$ is well-founded then so is Γ .
- Next: Steps, Loops, and Gamma (Γ)

Example: Time Triggered Linear HA

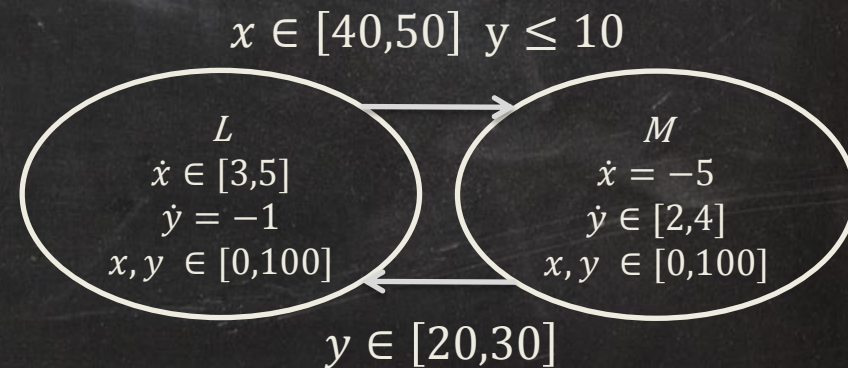
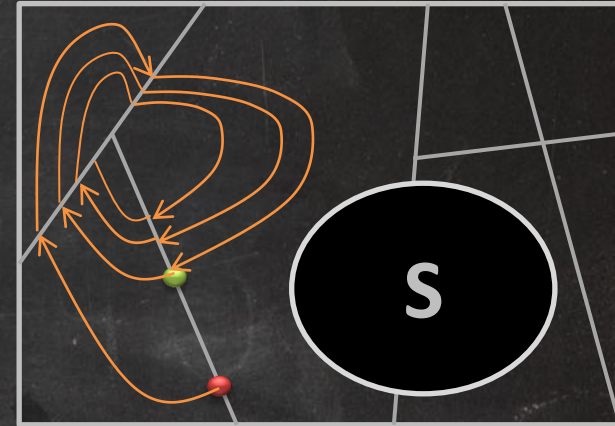
- Clock (c) constrains dwell time at each location
 - Unstable: upper bound
 - Stable: lower bound
- Guards overapproximated by level sets of $V_{i,l}$
- $\mu_{i,l,m}$: Bound on growth of $V_{i,l}(x) \leq \mu_{i,l,m} V_{i,m}(x')$
- $(y, y') \in \beta \Leftrightarrow \exists y''$ such that
 - $y_i'' \leq B_l e^{\lambda_l D} y_i$ where D : lower bound
 - $G_{i,min} \leq y_i'' \leq G_{i,max}$
- $y_i' \leq \mu_{i,l,m} y_i'' \leq \mu_{i,l,m} B_l e^{\lambda_l D} y_i$
- $y_i' \leq \frac{y_i}{K} \wedge y_i \geq c_i$



$$A_1 = \begin{bmatrix} -1 & 0 \\ 5 & -3 \end{bmatrix} \quad A_2 = \begin{bmatrix} 2 & 1 \\ 0 & -1 \end{bmatrix} \quad A_3 = \begin{bmatrix} -4 & -2 \\ 0 & -9 \end{bmatrix}$$

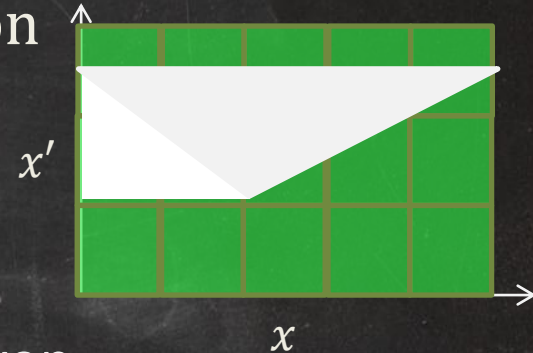
Using Disjoint Union of Well-founded Relations

- For every loop O , find a well-founded relation R_i containing T_O
- For Rectangular HA and TTLHA we can compute (approximate) T_O
- Well-foundedness of T_O can be checked using linear functions over x, x', y, y' e.g. using **Rankfinder**
- **But there may be infinitely many loops to consider**
- We will abstract each T_O with an abstract transition relation



Abstracting Loop HSRs with Transition Predicates

- Given $\mathcal{P} = \{P_1, \dots, P_m\}$ a collection of transition predicates, i.e., each $P_i \subseteq Q \times Q$
- $abs_{\mathcal{P}}(T_0) \supseteq T_0$ is the smallest superset of T_0 constructed by intersecting P_i 's
- **Observe.** If \mathcal{P} is finite, $abs_{\mathcal{P}}$ has finite range; even with infinitely many loops there are a finite number of $abs_{\mathcal{P}}(T_0)$'s to check
- **Theorem 3.** S inevitable for A if there exist (1) predicates $\mathcal{P} = \{P_1, \dots, P_m\}$ and (2) well-formed relations $\mathcal{R} = \{R_1, \dots, R_n\}$ such that for every loop O of A/S, $abs_{\mathcal{P}}(T_0) \subseteq R_i$



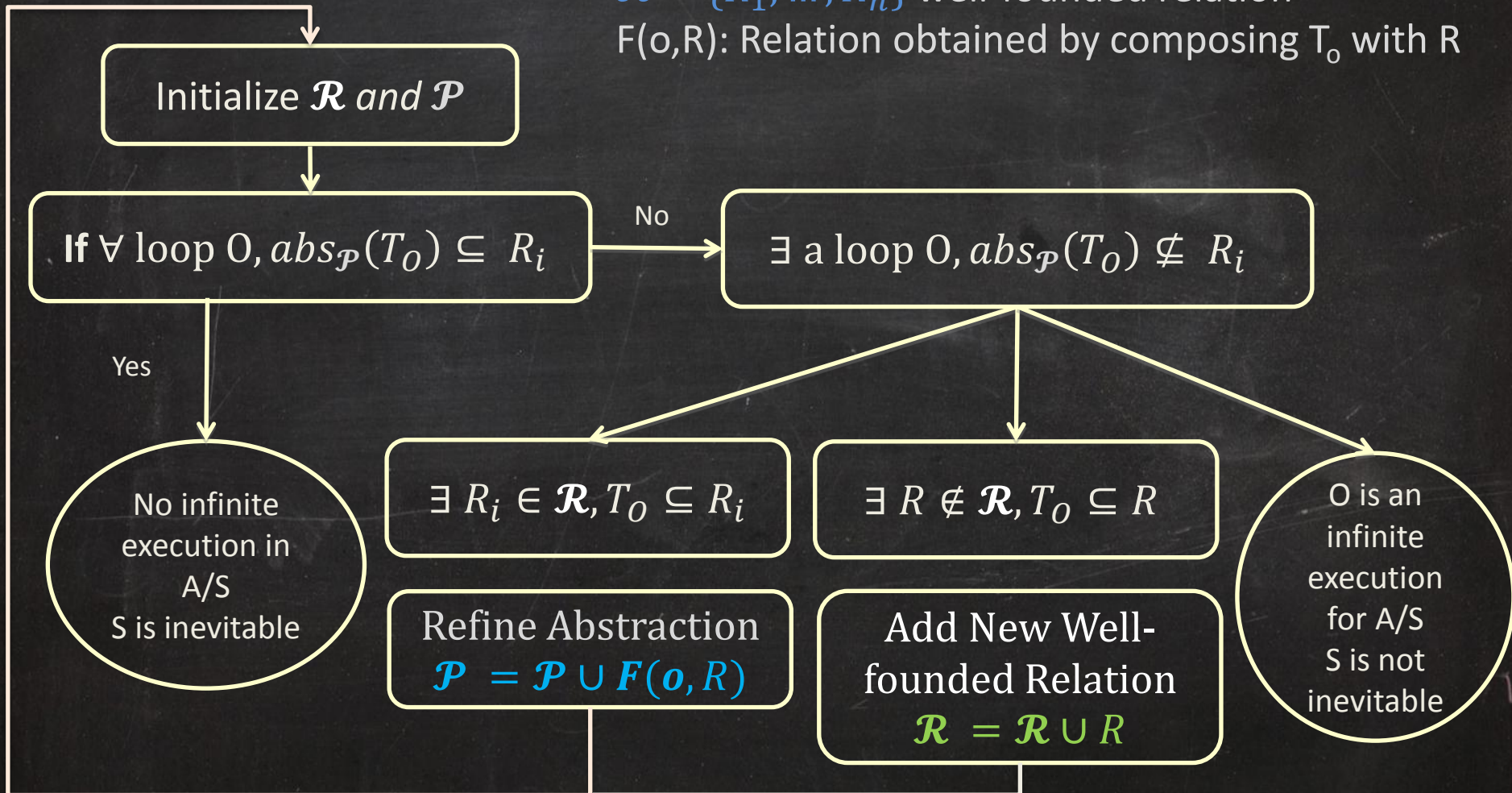
Abstraction-Refinement Algorithm

T_o : Transition relation for loop o

$\mathcal{P} = \{P_1, \dots, P_m\}$ transition predicates

$\mathcal{R} = \{R_1, \dots, R_n\}$ well-founded relation

$F(o, R)$: Relation obtained by composing T_o with R



Bringing it all together

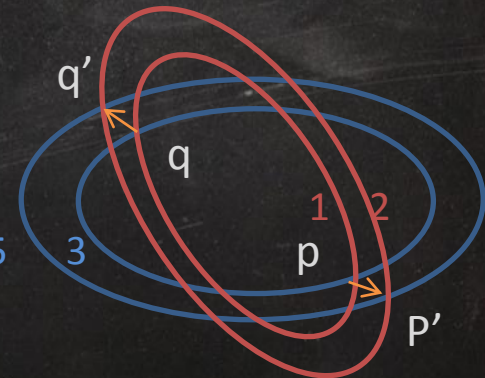
- Inevitability of HA A to set S
- Prove well-foundedness of $T_{A/S}$
- Prove well-foundedness of abstract loop transition relations $\text{abs}_p(T_0)$ that constitute $T_{A/S}$
- Completeness
 - For rectangular initialized HA, guaranteed to terminate
 - **Linear TTHA symmetric** with respect to the k Lyapunov functions: if $x T_L x'$, then **for all** $q \in \text{Abs}^{-1}_V(x)$ **there exists** $q' \in \text{Abs}^{-1}_V(x')$ such that $q T_A q'$

Problem (n, L)	Unstable locations	Time (sec)
(2,5)	2	0.01
(2,10)	3	0.14
(2,20)	5	1.88
(2,40)	8	88.94
(2,50)	9	392.85
(3,20)	5	2.02
(3,40)	8	38.11
(4,20)	5	100.49
(4,40)	8	110.34

$$V_1(q) = 1 \quad V_2(q) = 3$$

$$V_1(q') = 2 \quad V_2(q) = 5$$

$$\langle (1,3), (2,5) \rangle \in T_L$$



Ongoing and future directions

- What additional (robustness) assumption are needed for completeness of inevitability verification?
- Nonlinear Ranking Functions
- Invariant generation + Ranking
- Extension to networked and distributed hybrid systems

Questions ?



Acknowledgment

- The presented research is funded by
 - National Science Foundation
 - John Deere Co.