ILLINOIS

Approximate Partial Order Reduction

Chuchu Fan, Zhenqi Huang & Sayan Mitra

University of Illinois at Urbana-Champaign

FM, FLOC, OXFORD

JULY 2018

data-driven reachability

Given a system model A, initial set $\Theta \subseteq Q$, and unsafe set $U \subseteq Q$, does there exist an execution of A from Θ that hits U ?

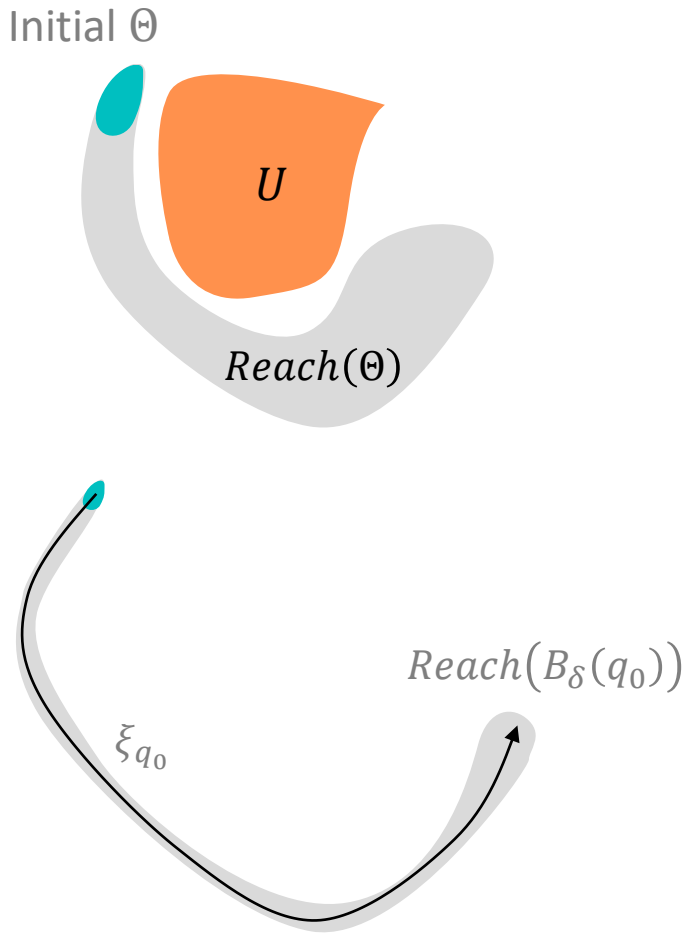
Check $Reach(\Theta) \cap U = \emptyset$?

For deterministic systems *simulation data + sensitivity analysis* have proven to be effective [Fan CAV16, TACAS 15, Huang CAV14]

- From a single execution ξ_{q_0} form initial state q_0 and static sensitivity analysis compute $Reach(B_\delta(q_0))$
- Take union, check safety, and refine with smaller δ as needed

Nondeterministic challenge: $Reach(\Theta, \Sigma) \cap U = \emptyset$?

- Many concurrent executions $\xi_{q_0,\tau}$ from q_0 following different action sequences $\tau \in \Sigma$
- Combinatorial explosion Σ + state space explosion Θ



partial order reduction + sensitivity analysis

Partial order reduction (POR):

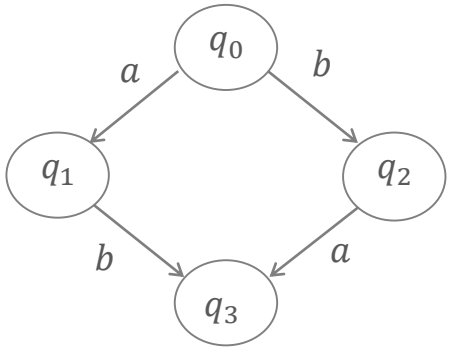
- If actions commute, then explore only one of the *equivalent* executions
- Can give exponential savings in computing $Reach(\mathrm{q}_0, \Sigma)$

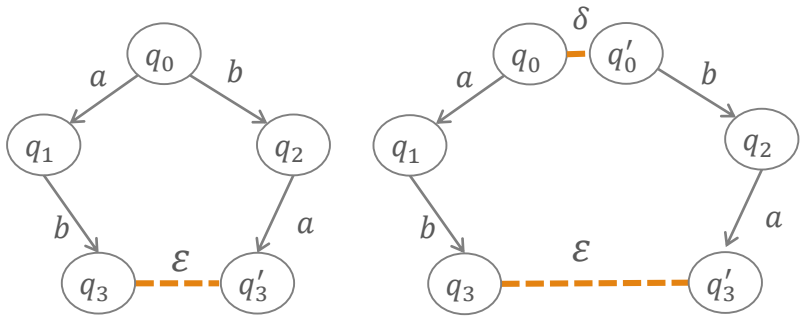
In our models, actions do not commute exactly, but approximately

We need to generalize a single execution $\xi(q_0, \tau)$ to compute $Reach(B_\delta(q_0), B_\varepsilon(\tau))$ where $B_\varepsilon(\tau)$ traces ε-equivalent to τ

Hurdles

- q_3 and q_3' may not satisfy the same actions
- Need to estimate impact of equivalent traces on similar (but not identical) states





model

A labeled transition system $\mathcal{A}$ is a tuple $\langle X \cup L, \Theta, A, \rightarrow \rangle$ where

- X: real-valued variables, L: finite-valued variables
- $Q = Val(X \cup L)$: the set of states,
- Θ: initial states,
- A: finite set of actions,
- $\rightarrow$: $Q \times A \times Q$ is a transition relation, $guard(a) = \{q \in Q \mid \exists q' \in Q , q \xrightarrow{a} q'\}$

A finite action sequences $\tau = a_0 a_1 \dots, a_{n-1}$ is called a trace

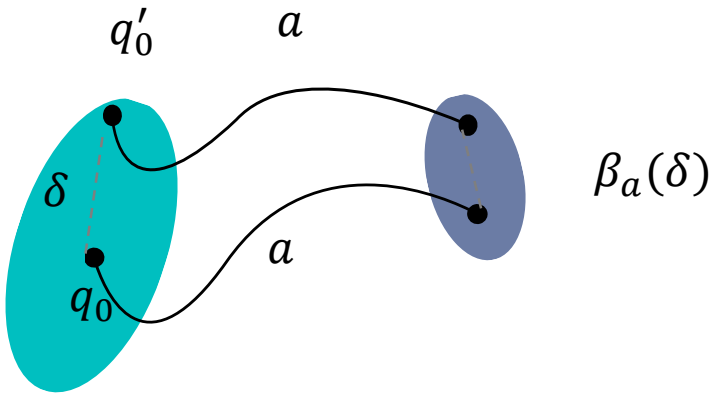
A state $q_0 \in Q$ and τ uniquely specifies a potential execution $\xi_{q_0,\tau} = q_0, a_0, q_1, a_1, \dots, a_{n-1}, q_n$

A valid execution satisfy $q_0 \in \Theta$ and for each i, $q_i \in guard(a_i)$

sensitivity to initial states: discrepancy

Discrepancy for action $a \in A$ is a continuous function $\beta_a: \mathbb{R}^+ \to \mathbb{R}^+$ such that for any q_0, q_0',

- $|a(q_0) - a(q_0')| \leq \beta_a(|q_0 - q_0'|)$
- as $\delta \to 0$, $\beta_a(\delta) \to 0$



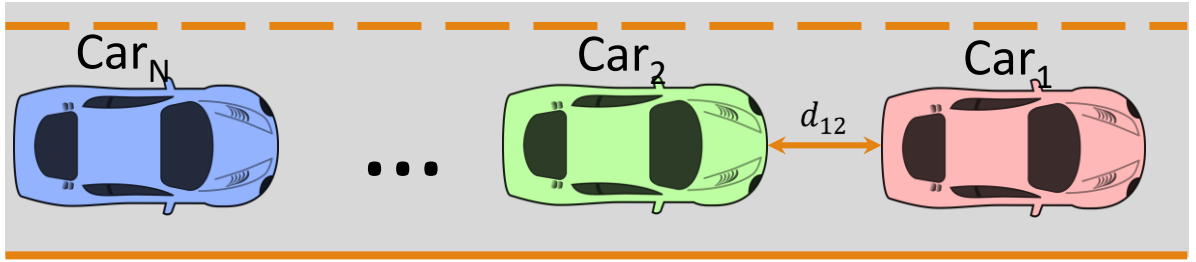
β_a can be computed using Lipschitz constant, matrix measures, etc. [Duggirala EMSOFT 13, Fan ACM TECS 16]

Proposition: Given a trace $\tau = a_0 a_1 \ldots a_{n-1}$, for any q_0, q_0',

$$\left|\xi_{q_0,\tau} - \xi_{q_0',\tau}\right| \leq \beta_{a_{n-1}} \cdots \beta_{a_0}(|q_0 - q_0'|)$$

example: platoon

A platoon of N cars on a single lane
Each car chooses 1 of 3 actions at each step:
a (accelerate), b (brake), or c (cruise)



Car$_1$ can choose any action at each time step

Others try to keep safe distance d with predecessor
by choosing a if $d > 50$, b if $d < 30$, else c

Safety requirement (U): Cars do not collide

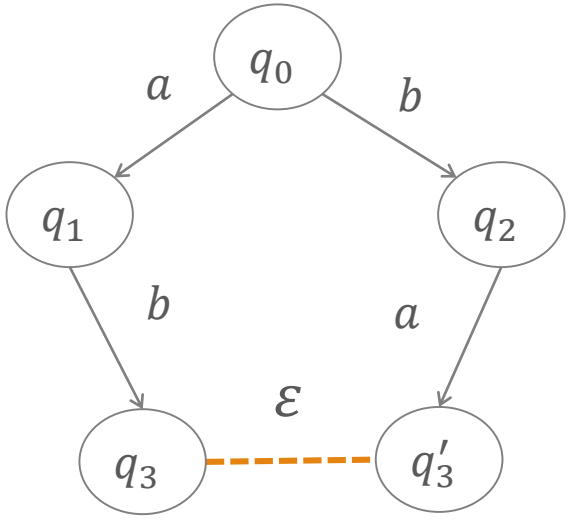
Car$_1$ has 3 choices: 3^{10}executions of length 10
4 cars with different initial separation:
$3^{4^{10}}$executions

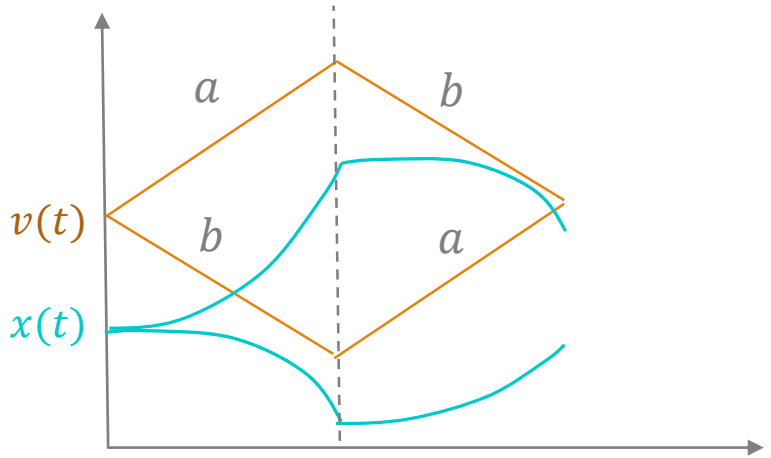
$$x \leftarrow \begin{bmatrix} 1 & \Delta t & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & \Delta t \\ 0 & 0 & 0 & 1 \end{bmatrix} + \begin{bmatrix} acc_1(\Delta t)^2/2 \\ acc_1 \Delta t \\ acc_2(\Delta t)^2/2 \\ acc_2 \Delta t \end{bmatrix} = Ax + v(m), \text{ where}$$

$m[1] =$ accelerate, $m[2] =$ brake, then $acc_1 > 0\ acc_2 < 0$

For any q, q', m, $\beta_a(|q.x - q'.x|) = |A||q.x - q'.x|$, with
$\Delta t = 0.1, \beta_a(|q.x - q'.x|_2) = 1.06|q.x - q'.x|_2$

actions commute approximately





Two actions are ε-*independent* $a \sim^{\varepsilon} b$ if $ab(q_0).L = ba(q_0).L$ and $|ab(q_0).X - ba(q_0).X| < \varepsilon$

ε-independence is symmetric but not transitive

ε-equivalent traces

A trace $\tau = a_0 a_1 \ldots, a_{n-1}$ and an action a are ε–independent $\tau \sim^{\varepsilon} a$ iff each $a_i \sim^{\varepsilon} a$

ε-equivalent traces: $\tau \equiv^{\varepsilon} \tau'$ if τ' can be constructed from τ by performing a sequence of swaps of consecutive ε-independent actions

E.g., if $a_0 \sim^{\varepsilon} a_1$ and $a_0 \sim^{\varepsilon} a_2$, then $a_0 a_1 a_2 \equiv^{\varepsilon} a_1 a_0 a_2 \equiv^{\varepsilon} a_1 a_2 a_0$

$\equiv^{\varepsilon}$ is a symmetric, reflexive and transitive relation of Σ

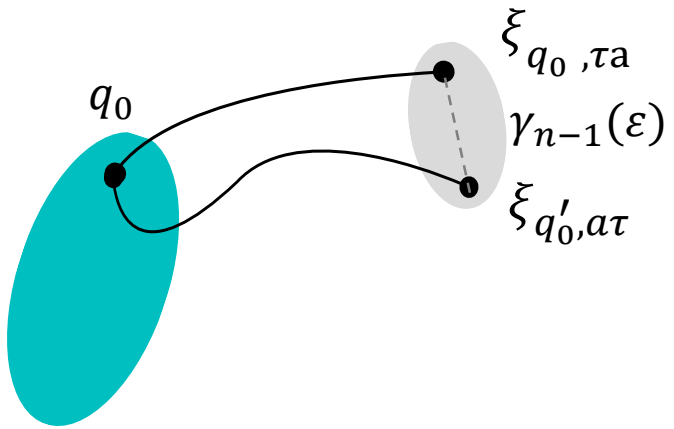
Idea:

- Use representative member τ of $\equiv^{\varepsilon}$ to compute $Reach(q_0, B_{\varepsilon}(\tau))$
- Use discrepancy to compute $Reach(B_{\delta}(q_0), B_{\varepsilon}(\tau))$

boundung ε-equivalent executions

Lemma: For any initial state $q_0 \in Q$, action $a \in A$, trace $\tau \in \Sigma$, if $\tau \sim^{\varepsilon} a$, then $\left|\xi_{q_0,\tau a} - \xi_{q_0,a\tau}\right| \leq \gamma_{n-1}(\varepsilon)$,

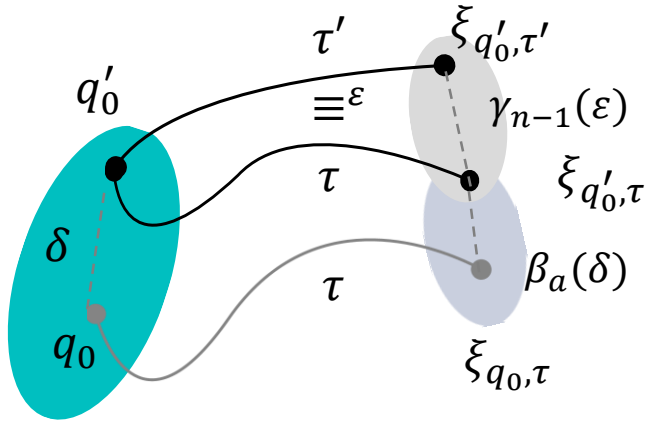
where $\gamma_{n-1}(\varepsilon) = \sum_{i=0}^{n-1} \beta_{\max}^{i}(\varepsilon)$ and $\beta_{\max} = \max_{b\in\tau}\{\beta_b\}$



(δ, ε)-trace equivalent discrepancy

Given $q_0 \in Q$, trace $\tau \in \Sigma$, and constants $\delta, \varepsilon \geq 0$, $r(\delta, \varepsilon, q_0, \tau) > 0$ is called a (δ, ε)-trace equivalent discrepancy if for all $q_0' \in B_\delta(q_0)$ and $\tau \equiv^\varepsilon \tau'$

$$\left| \xi_{q_0,\tau} - \xi_{q_0',\tau'} \right| \leq r$$



computing (δ, ε)-discrepancy via earliest positions

Lemma: (δ, ε)-Ted for $\xi_{q_0,\tau a}$ is given by

$$r' = \begin{cases} \beta_a(r) & Earliest(\tau, a, \varepsilon) = len(\tau) \\ \beta_a(r) + \gamma_{len(\tau)-k-1}(\varepsilon) & Earliest(\tau, a, \varepsilon) < len(\tau) \end{cases}$$

where r is a (δ, ε)-Ted for $\xi_{q_0,\tau}$.

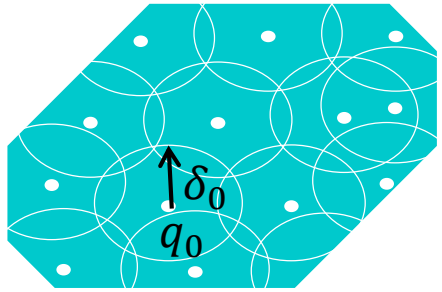
Earliest position of a on τ is $Earliest(\tau, a, \varepsilon) = \min_{\phi a \eta \equiv^{\varepsilon} \tau a, a \notin \eta} \text{len}(\phi)$

E.g., if $a_0 \sim^{\varepsilon} a_1$ and $a_0 \sim^{\varepsilon} a_2$, then $Earliest(a_0 a_1, a_2, \varepsilon) = 1$

Earliest(.) can be computed using $O(\text{len}(\tau)^2)$

reachability

Step 1: Partition Θ to be δ_0-balls



Initial Set Θ

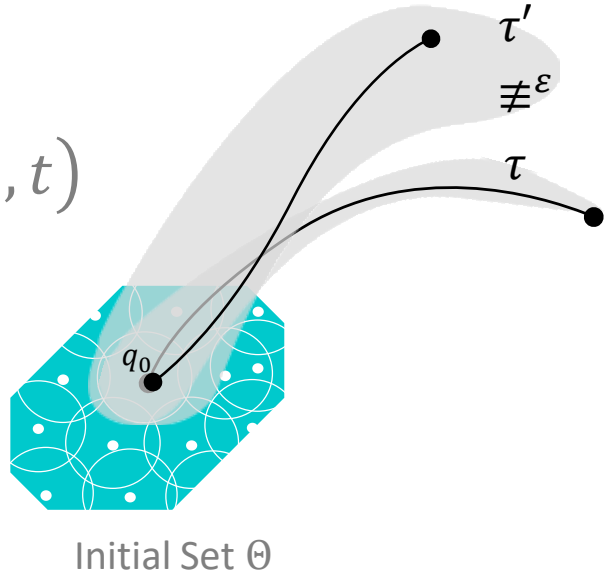
reachability

Step 1: Partition Θ to be δ_0-balls

Step 2: For each δ_0-ball $\mathcal{B}_{\delta_0}(q_0)$, construct $\mathbf{Reach}\left(\mathcal{B}_{\delta_0}(q_0), t\right)$

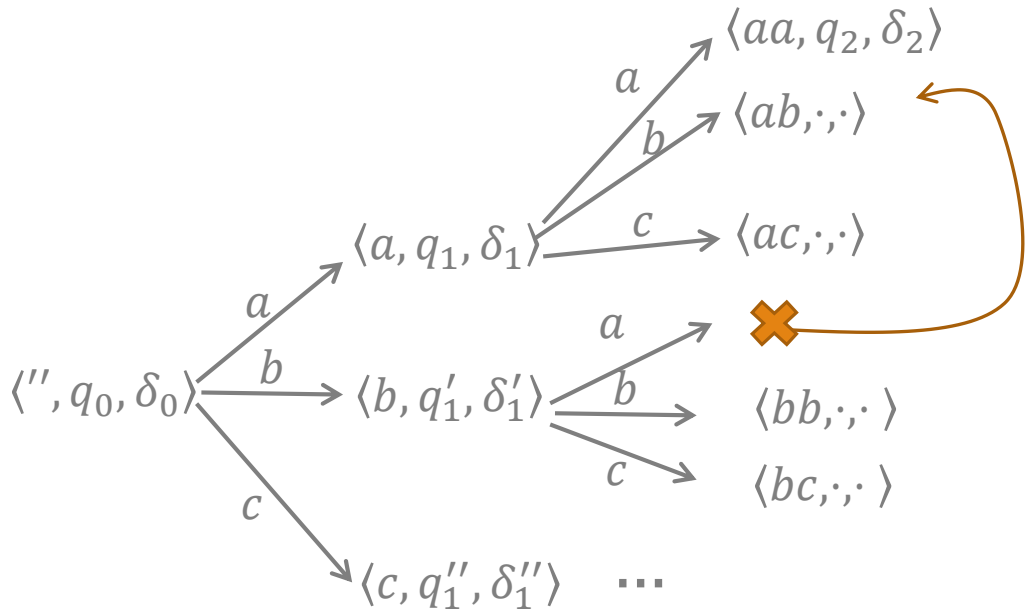
- For each $t \leq T$, find all representative traces $\{\tau_t\}$
- Representative traces are mutually non-ε-equivalent
- For each τ_t, bloat $\xi_{q_0,\tau_t}.\mathbf{lstate}$ with its (δ_0, ε)-ted

Union, check safety, refine…



savings

Suppose 3 actions with $a \sim^{\varepsilon} b$ and $a \sim^{\varepsilon} c$. All of them are enabled at each steps. Reach set at t is stored as tuples $R_t = \{\langle \tau_t, q_t, \delta_t \rangle\}$, with $q_t = \xi_{q_0,\tau_t}$ and δ_t is a (δ_0, ε)-ted for ξ_{q_0,τ_t}



If there are k actions in total and they are mutually ε-independent, then R_t contains at most $\binom{t+k-1}{k-1}$ tuples, compared with k^t potential traces.

The algorithm can reduce the number of executions explored by $O(t!)$

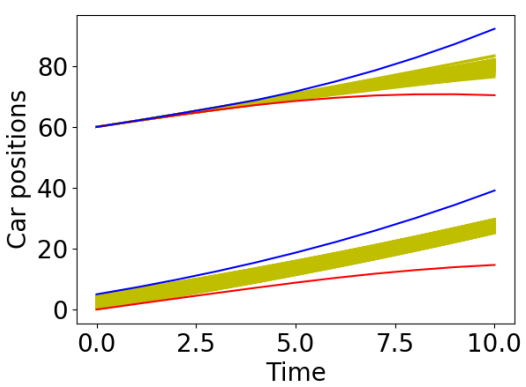
soundness and precision

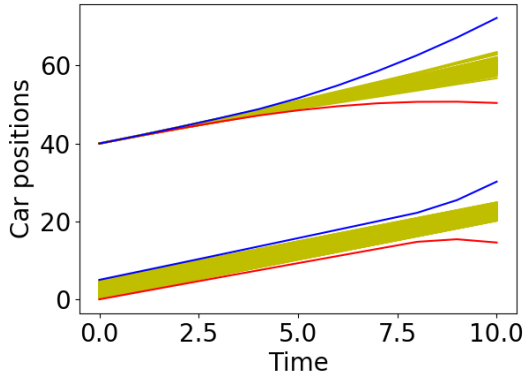
Theorem (soundness): The reachability algorithms indeed computes an over-approximation of $\mathbf{Reach}(\Theta, \Sigma)$.

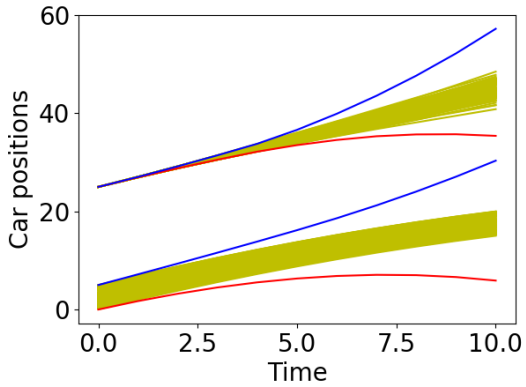
Theorem (precision): The over-approximation can be made arbitrarily precise by reducing the size of δ_0, ε.

(As δ_0 and ε go to 0, the algorithm actually converges to a simulation algorithm which simulates every valid execution from each initial state)

experiments: platoon







		Approximate POR	Brute Force (single initial)
2-car platoon	# traces explored	43758(max)	9^{10}
	Run time	5.1ms	2.9s
4-car platoon	# traces explored	7986	81^{10}
	Run time	62.3ms	6.2s

conclusion

- Approximate partial order reduction generalizes the traditional independence by allowing approximately commuting actions

- This notion works naturally with reachability algorithms that generalize individual executions to cover--- δ-close initial states, and follow different, but ε-independent, action sequences

- Over-approximations made arbitrarily precise by reducing δ, ε

Future directions

- Combine with symmetry reduction
- Applications to autonomous vehicle interactions

collaborators

Chuchu Fan

Zhenqi Huang