Counterexample-Guided Synthesis of Safety Contracts

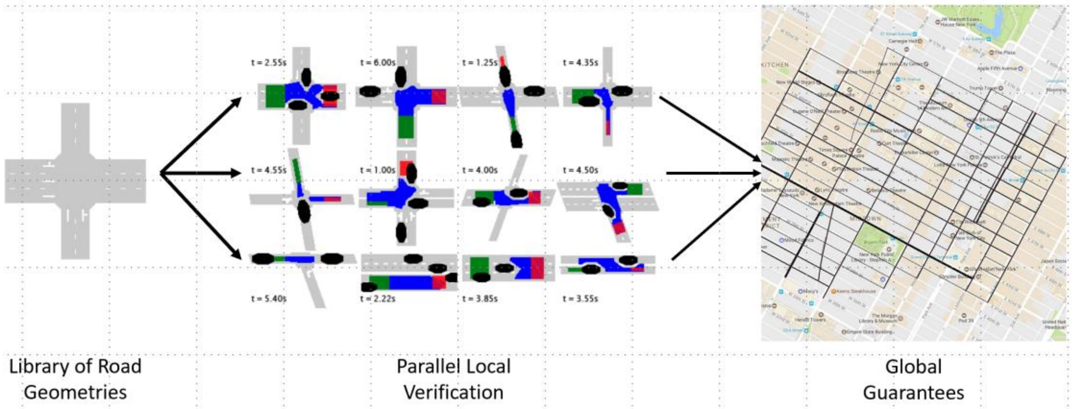
Jon DeCastro(TRI), Lucas Liebenwein, **Cristian-Ioan Vasile**

Overview

- Scalable verification and safety guarantees
- Scalability with respect to
  - Space: size of road network
  - Fleet: number of vehicles
  - Specification: rules of the roads
  - **Traffic: driving scenarios (NEW!)**
- Vision:
  “Provide long-term safety guarantees for autonomous vehicle deployment”

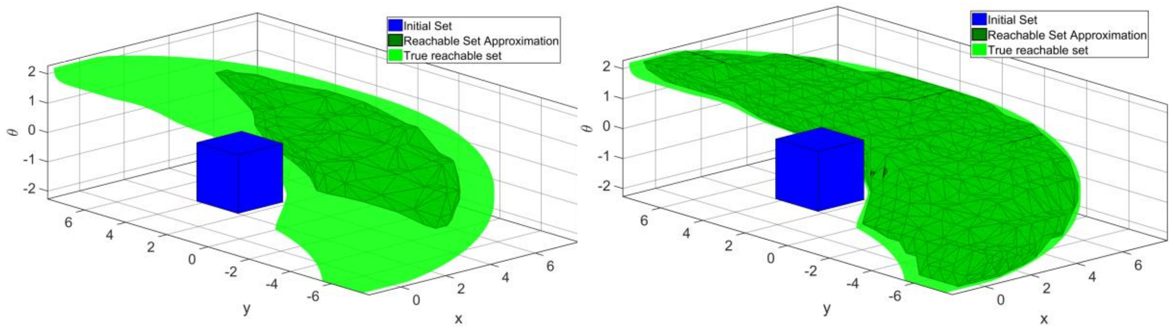
Prior Work

- Scalable verification through assume-guarantee contracts



[1] Liebenwein, Lucas et al. "Compositional and Contract-based Verification for Autonomous Driving on Road Networks." International Symposium on Robotics Research (ISRR), 2017, Puerto Varas, Chile

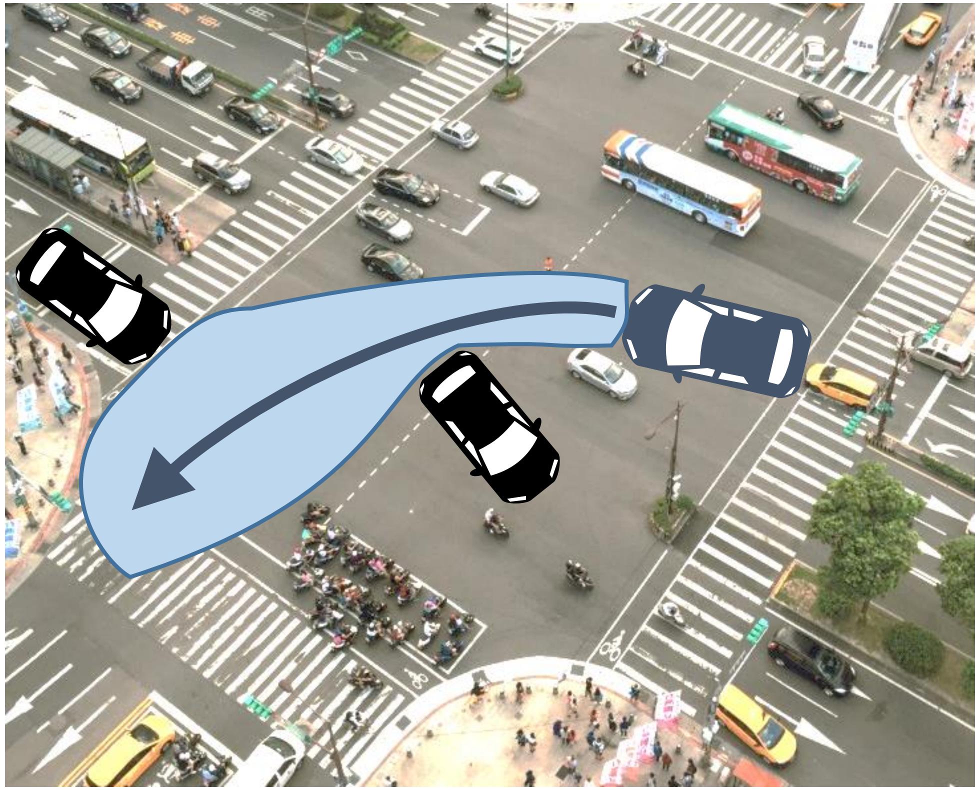
- Sampling-based reachability analysis



[2] Liebenwein*, Lucas, Cenk Baykal*, et al. "Sampling-Based Approximation Algorithms for Reachability Analysis with Provable Guarantees." Proceedings of Robotics: Science and Systems, 2018, Pittsburgh, Pennsylvania

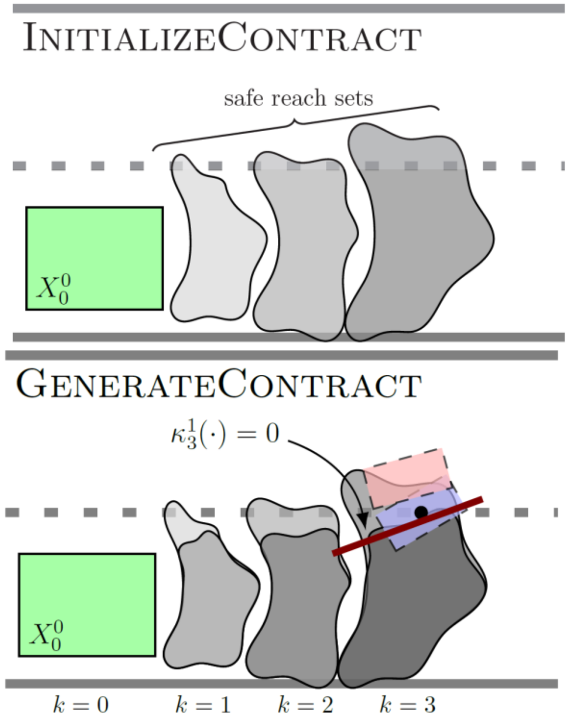
Safety Contracts

- Use easy-to-implement, explainable contracts
- Contract = set of state space constraints
- Contracts help to guard against other traffic participants

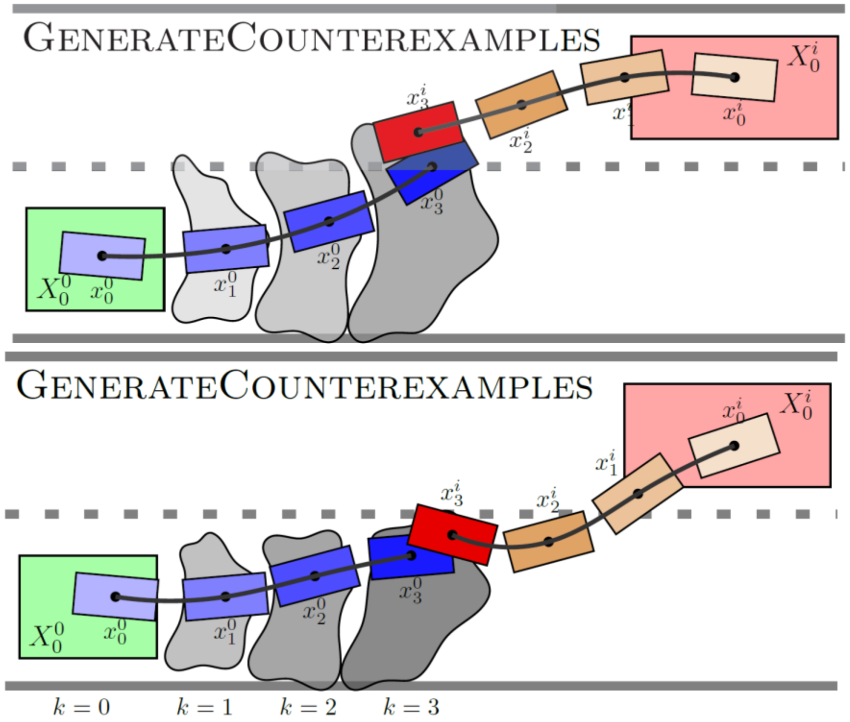


Overview

Candidate contracts with reachability analysis

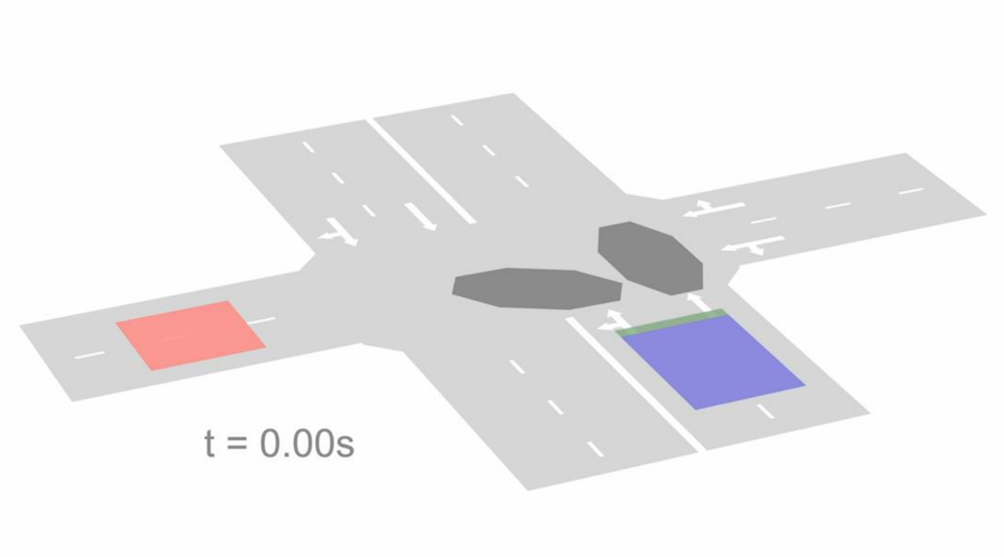


Refinement through falsification-based counterexamples



Generate Candidate Contracts

- Same principle as in ISRR’17
- Reachability analysis with
  - road segment
  - fixed traffic scenario
  - safety constraints
- Can leverage modular approach to verification



= Ego Car = Other Car = Entry Region = Exit Region

Generate Counterexamples

- Refinement of contract through falsification
- We try to find traffic trajectories such that
  - The behavior is “expectable”
  - The candidate contract cannot guard the ego-car
- Direct collocation **stochastic** quadratic program (SQP)

$$
\begin{aligned}
\max_{h,\bar{u},\bar{w},\bar{x}} \; & p(\bar{w}) \\
\text{s.t. } & x_{k+1} - x_k = h f_{collocation}, \quad \forall k = 0, \ldots, T-1 && \text{(dynamics)} \\
& x_k \in \mathcal{X}, \quad \forall k = 0, \ldots, T \\
& u_k \in \mathcal{U}, \quad \forall k = 0, \ldots, T-1 \\
& x_0 \in \mathcal{X}_0, \quad u_0 \in \mathcal{U} && \text{(initial conditions)} \\
& \psi(x_T) \leq 0 && \text{(safety specification)} \\
& \kappa_k^j(x_k) \leq 0, \quad \forall j = 1, \ldots, Q, \; \forall k = 0, \ldots, T && \text{(contracts)} \\
& p(\bar{w}) \geq \alpha T && \text{(chance constraint)}
\end{aligned}
$$

Rules of the Road and Behavior

- The safety contract of the ego-car consider rules of the roads

Table 1: Rules of the road for highway scenarios.

No.	Rule	Constraint set
1	Don't drive in the left lanes.	$\{0 \leq x_c^0 \leq L, -n_{right} \cdot W \leq y_c^0 \leq 0\}$
2	If driving behind another car, keep a reasonable distance away to avoid collision if it suddenly stops.	$\{x_c^i - x_c^0 \geq \epsilon_x^{safe}\, v^0 \mid \forall i\ .\ x_c^i - x_c^0 \geq 0 \wedge \lvert y_c^i - y_c^0 \rvert < W\}$
3	If you want to slow down, give clear warning and do not inconvenience drivers behind you.	$\{x_c^0 - x_c^i \geq \epsilon_x^{safe}\, v^0 \mid \forall i\ .\ x_c^0 - x_c^i \geq 0 \wedge \lvert y_c^i - y_c^0 \rvert < W\}$
4	Don't cross solid lines.	$\{\xi_x^\ell \leq x_c^0 \leq \zeta_x^\ell \wedge - n_{right} \cdot W \leq y_c^0 \leq 0 \mid 1 \leq \ell \leq n_{solid}\}$
5	Overtake on the left when it is safe.	$\{y_c^0 - y_c^i > W \wedge v^0 > v^i \mid$ $\forall i\ .\ v^i > 0 \wedge \lvert x_c^0 - x_c^i \rvert \leq \epsilon_x^{overtake} \wedge$ $\nexists j\ .(\ \lvert x_c^j - x_c^i \rvert \leq \epsilon_x^{safe-overtake} \wedge y_c^0 - y_c^j \leq W)\}$
6	If another vehicle is trying to overtake you keep right and don't accelerate. If necessary, slow down and pull over.	$\{u_a^0 \leq 0 \wedge y_c^i - y_c^0 \geq W \wedge y_c^0 \leq 0 \mid$ $\forall i\ .\ y_c^i - y_c^0 \leq 1.5W \wedge v^i > 0 \wedge \lvert x_c^i - x_c^0 \rvert \leq \epsilon_x^{overtake}\}$
7	If passing oncoming traffic, leave sufficient lateral space to not get hit. If obstructed, slow down.	$\{y_c^i - y_c^0 \geq \epsilon_y^{safe} \mid y_c^i \geq 0 \wedge v^i \leq 0\}$
8	Don't drive abnormally slowly such that you impede the progress of other vehicles. Don't drive above the speed limit or abnormally fast.	$\{\lvert v^0 - \bar{v} \rvert \leq \epsilon_v, \lvert v^0 \rvert \leq \epsilon_v^{legal}\}$

- The traffic agents are modelled as **probabilistic** IDM agents

Table 2: Parameters used to model driver behaviors for the traffic cars.

	Description	Symbol	Driving Style Normal	Driving Style Aggressive
IDM	Reference speed (m/s)	v_{ref}	10	1.5
	Maximum acceleration (m/s^2)	a	1	4
	Comfortable deceleration (m/s^2)	b	3	6
	Minimum-desired net distance (m)	s_0	1	0.5
	Time headway to lead vehicle (s)	t_h	0.1	0.05
	Free-road exponent	δ	4	4
Pure-Pursuit	Lookahead distance (m)	s_{look}	15	10
Perception	Range (m)	$s_{perception}$	100	100
Disturbances	Steering angle variance (rad^2)	σ_δ	0.1	5
	Acceleration variance (m^2/s^4)	σ_a	0.1	2.5

Tuning of Behavior

Strict Rule Set

Relaxed Rule Set

Normal Driving Style

Aggressive Driving Style

Table 1: Rules of the road for highway scenarios.

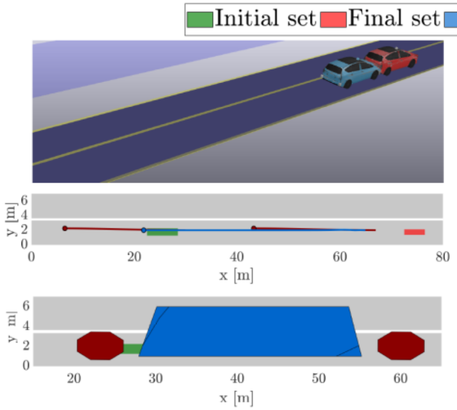
No.	Rule	Constraint set
1	Don't drive in the left lanes.	$\{0 \leq x_c^0 \leq L, -n_{right} \cdot W \leq y_c^0 \leq 0\}$
2	If driving behind another car, keep a reasonable distance away to avoid collision if it suddenly stops.	$\{x_c^i - x_c^0 \geq \epsilon_x^{safe} v^0 \mid \forall i \,.\, x_c^i - x_c^0 \geq 0 \wedge \lvert y_c^i - y_c^0 \rvert < W\}$
3	If you want to slow down, give clear warning and do not inconvenience drivers behind you.	$\{x_c^0 - x_c^i \geq \epsilon_x^{safe} v^0 \mid \forall i \,.\, x_c^0 - x_c^i \geq 0 \wedge \lvert y_c^i - y_c^0 \rvert < W\}$
4	Don't cross solid lines.	$\{\xi_x^\ell \leq x_c^0 \leq \zeta_x^\ell \wedge -n_{right} \cdot W \leq y_c^0 \leq 0 \mid 1 \leq \ell \leq n_{solid}\}$
5	Overtake on the left when it is safe.	$\{y_c^0 - y_c^i > W \wedge v^0 > v^i \mid \forall i \,.\, v^i > 0 \wedge \lvert x_c^0 - x_c^i \rvert \leq \epsilon_x^{overtake} \wedge \nexists j \,.(\lvert x_c^j - x_c^i \rvert \leq \epsilon_x^{safe-overtake} \wedge y_c^0 - y_c^j \leq W)\}$
6	If another vehicle is trying to overtake you keep right and don't accelerate. If necessary, slow down and pull over.	$\{u_a^0 \leq 0 \wedge y_c^i - y_c^0 \geq W \wedge y_c^0 \leq 0 \mid \forall i \,.\, y_c^i - y_c^0 \leq 1.5W \wedge v^i > 0 \wedge \lvert x_c^i - x_c^0 \rvert \leq \epsilon_x^{overtake}\}$
7	If passing oncoming traffic, leave sufficient lateral space to not get hit. If obstructed, slow down.	$\{y_c^i - y_c^0 \geq \epsilon_y^{safe} \mid y_c^i \geq 0 \wedge v^i \leq 0\}$
8	Don't drive abnormally slowly such that you impede the progress of other vehicles. Don't drive above the speed limit or abnormally fast.	$\{\lvert v^0 - \bar{v} \rvert \leq \epsilon_v, \lvert v^0 \rvert \leq \epsilon_v^{legal}\}$

Table 2: Parameters used to model driver behaviors for the traffic cars.

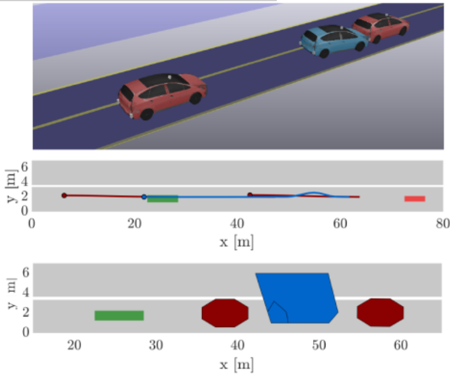
	Description	Symbol	Driving Style: Normal	Driving Style: Aggressive
IDM	Reference speed (m/s)	v_{ref}	10	1.5
	Maximum acceleration (m/s^2)	a	1	4
	Comfortable deceleration (m/s^2)	b	3	6
	Minimum-desired net distance (m)	s_0	1	0.5
	Time headway to lead vehicle (s)	t_h	0.1	0.05
	Free-road exponent	δ	4	4
Pure-Pursuit	Lookahead distance (m)	s_{look}	15	10
Perception	Range (m)	$s_{perception}$	100	100
Disturbances	Steering angle variance (rad^2)	σ_δ	0.1	5
	Acceleration variance (m^2/s^4)	σ_a	0.1	2.5

Results

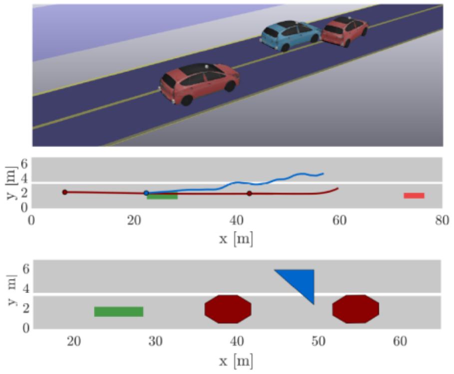
- Multiple iterations, same rules



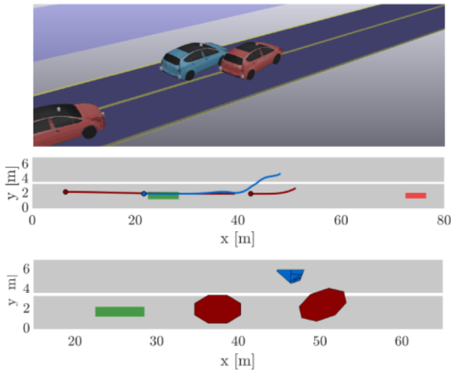
(a) Iteration 2



(b) Iteration 3

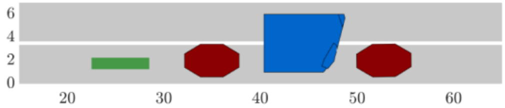


(c) Iteration 7

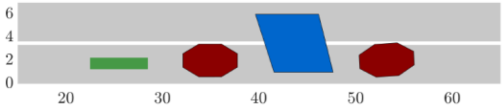


(d) Iteration 14

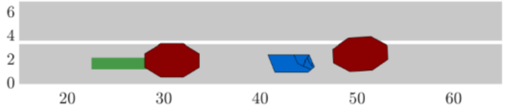
- Same iterations, different rules



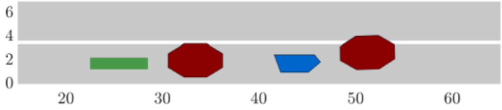
(a) Relaxed rules, normal driving



(b) Relaxed rules, aggressive driving



(c) Strict rules, normal driving



(d) Strict rules, aggressive driving

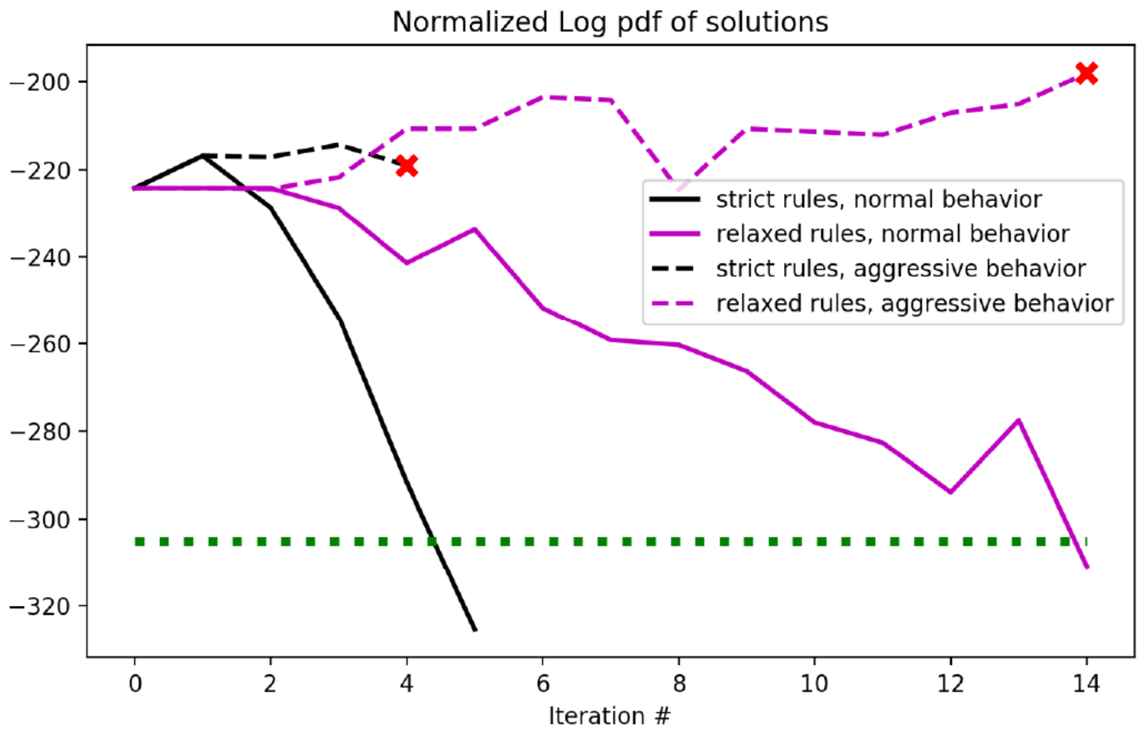
TOYOTA RESEARCH INSTITUTE

Massachusetts Institute of Technology

CSAIL

Explainability

- Probabilistic Modelling of Agents
- Falsification is used to capture a wide array of likely counterexamples
- Probabilities help to assess the usefulness of contracts
- Rules allow to tune behaviors



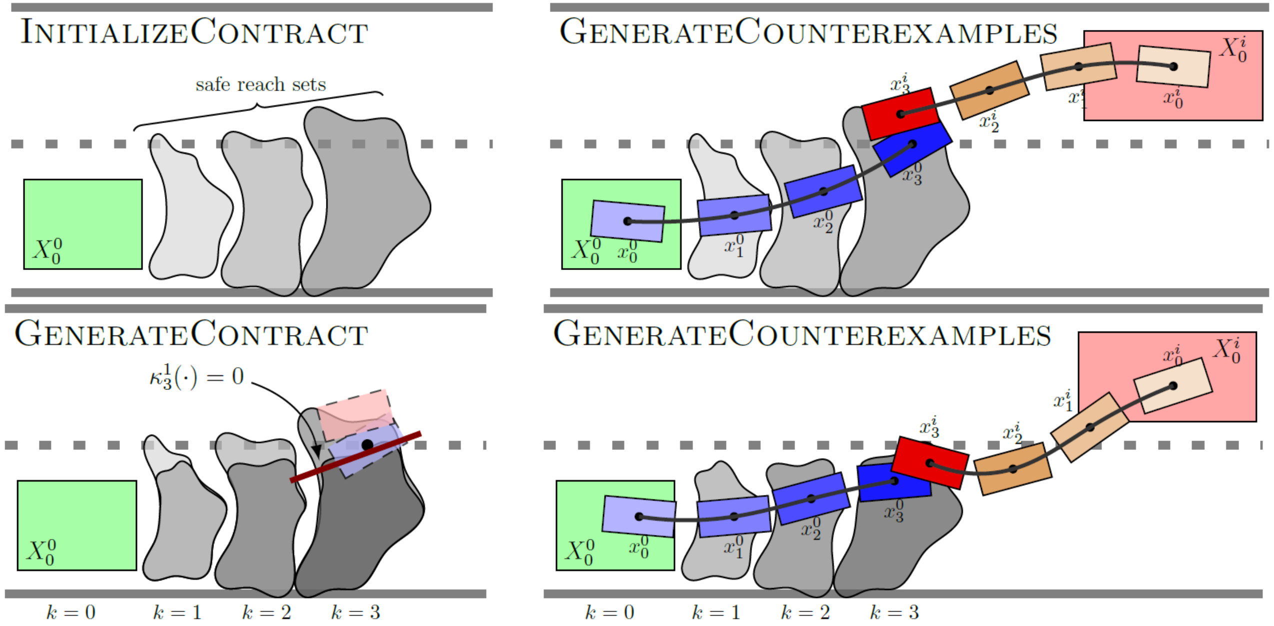
TOYOTA RESEARCH INSTITUTE

Massachusetts Institute of Technology

CSAIL

Conclusion

- Probabilistic safety contracts through **verification** and **falsification**
- Scalability and explainability
- **Outlook:**
  - More scenarios
  - Advanced rules of the roads
  - Intuitive contracts → use logical predicates?



TOYOTA RESEARCH INSTITUTE

Massachusetts Institute of Technology

CSAIL