Compositional and Contract-based Verification for Autonomous Driving on Road Networks

Lucas Liebenwein, Wilko Schwarting, Cristian-Ioan Vasile,
Jonathan DeCastro, Javier Alonso-Mora, Sertac Karaman, Daniela Rus

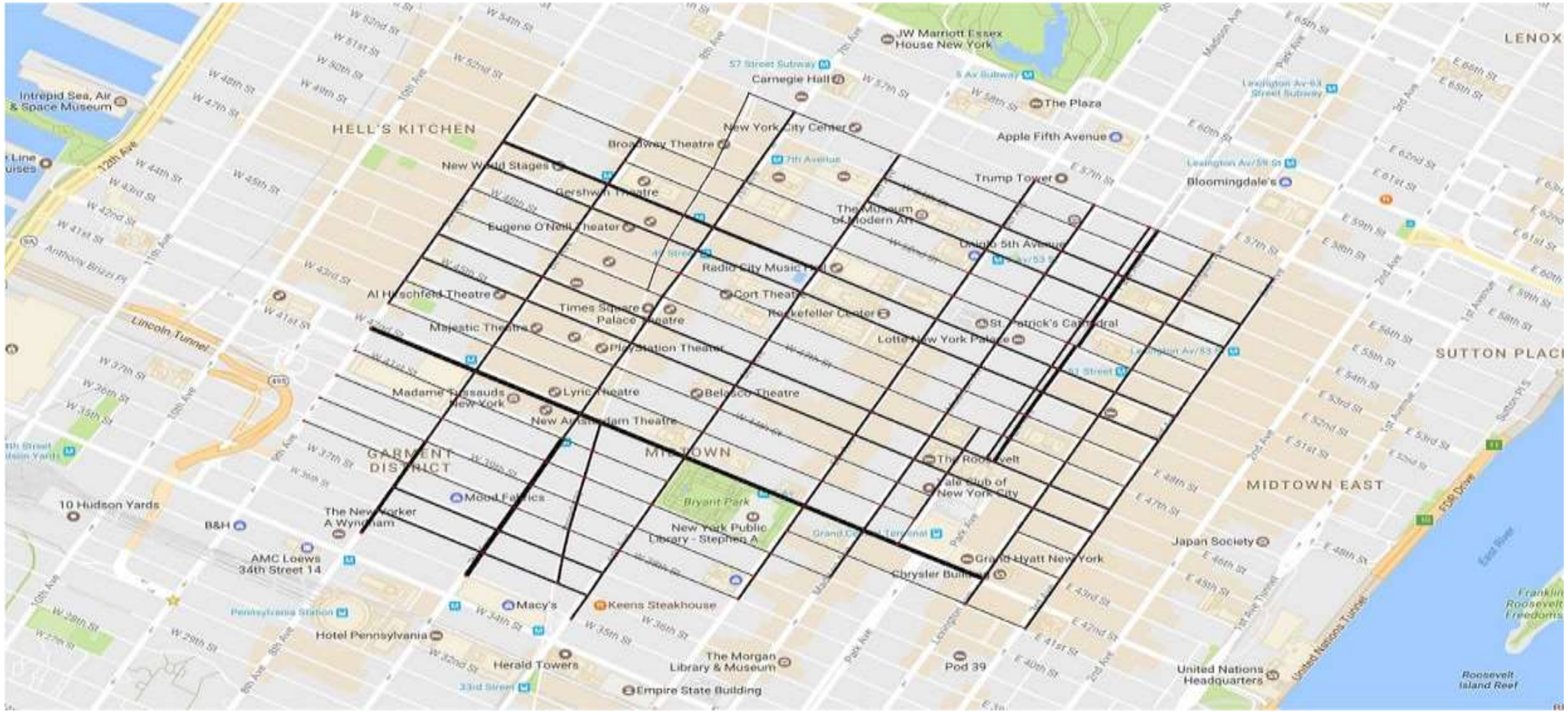
lucasl@mit.edu

TOYOTA RESEARCH INSTITUTE

Massachusetts Institute of Technology

CSAIL

How can we obtain safety guarantees?



Problem Definition

Problem Definition

Verification Components		
System	Model	Specification – Controller Contract $\mathcal{S}$
• **Controller:** $$\mathbf{u}_{\boldsymbol{k}} = C\left(\boldsymbol{z}_k^{0:N}\right),$$ where $\boldsymbol{z}_k^i$ is state of car i at time k with **The controller is assumed to abide by the controller contract $\mathcal{S}$.**		

Problem Definition

Verification Components		
System	Model	Specification – Controller Contract $\mathcal{S}$

• **Controller:** $\mathbf{u}_{\boldsymbol{k}} = C\left(\mathbf{z}_k^{0:N}\right)$,
where $\boldsymbol{z}_k^i$ is state of car i at time k with
 	
The controller is assumed to abide by the controller contract $\mathcal{S}$.
	• **Ego-Car:** $V = (\mathcal{Z}, \mathcal{R}, \mathcal{U}, f, h)$ with $z_{k+1} = f(z_k)$, where
	$\dot{\mathbf{z}} = \begin{bmatrix} \dot{x} \\ \dot{y} \\ \dot{\theta} \\ \dot{\delta} \\ \dot{v} \end{bmatrix} = \begin{bmatrix} v\cos(\theta) \\ v\sin(\theta) \\ \frac{v}{L}\tan(\delta) \\ 0 \\ 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix} \underbrace{\begin{bmatrix} u^\delta \\ u^a \end{bmatrix}}_{\mathbf{u}}$
	
	• **Road Geometries:** $m = (\mathcal{Z}, \mathfrak{I}, \mathfrak{D}, S, A)$
	  • Straight Roads
	  • Intersections
	
	• **Traffic Model**: $T = (\mathcal{V}(0), \mathfrak{I}, \mathfrak{D}, S)$
	  • Spline Representation
	  • Traffic Scheduler	

Problem Definition

Verification Components		
System	Model	Specification – Controller Contract $\mathcal{S}$

• **Controller:** $\mathbf{u}_k = C(\mathbf{z}_k^{0:N})$, where $\mathbf{z}_k^i$ is state of car i at time k with
 	
The controller is assumed to abide by the controller contract $\mathcal{S}$.
	• **Ego-Car:** $V = (\mathcal{Z}, \mathcal{R}, \mathcal{U}, f, h)$ with $z_{k+1} = f(z_k)$, where $\dot{\mathbf{z}} = \begin{bmatrix} \dot{x} \\ \dot{y} \\ \dot{\theta} \\ \dot{\delta} \\ \dot{v} \end{bmatrix} = \begin{bmatrix} v\cos(\theta) \\ v\sin(\theta) \\ \frac{v}{L}\tan(\delta) \\ 0 \\ 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix} \underbrace{\begin{bmatrix} u^\delta \\ u^a \end{bmatrix}}_{\mathbf{u}}$
	
	• **Road Geometries:** $m = (\mathcal{Z}, \mathfrak{I}, \mathfrak{O}, S, A)$
	  • Straight Roads
	  • Intersections
	
	• **Traffic Model**: $T = (\mathcal{V}(0), \mathfrak{I}, \mathfrak{O}, S)$
	  • Spline Representation
	  • Traffic Scheduler
		• **Safety:** $\inf_{\mathbf{z} \in B(\mathbf{z}_k), \mathbf{o} \in O_k} \lvert\mathbf{z} - \mathbf{o}\rvert > \pi_{safety}$
		
		• **Speed Limit:** $\lvert v\rvert \leq v_{max}$
		
		• **Dynamic Limitation:** $\lvert\delta\rvert \leq \delta_{max}$, $\lvert u^\delta\rvert \leq \dot{\delta}_{max}$, $a_{min} \leq u^a \leq a_{max}$

Technical Challenges

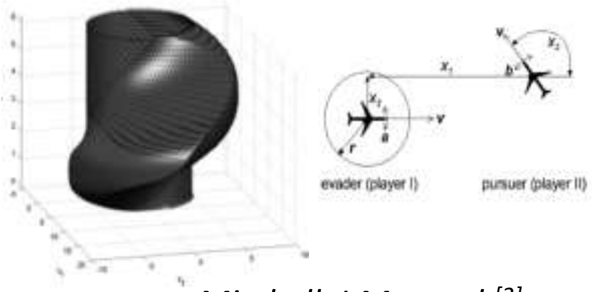
- Verification is HARD
- Computational tractability often not feasible
- Model complexity increases cost
- Realistic scenarios requires scalable models

Technical Challenges

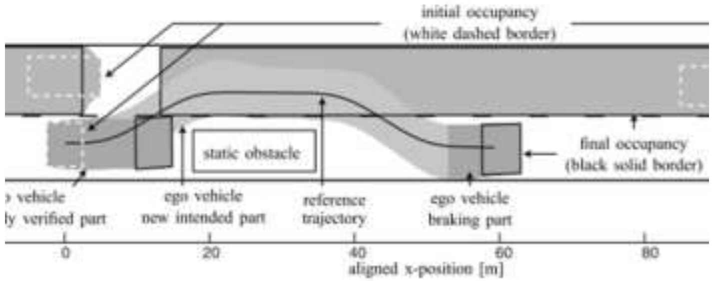
- Verification is HARD
- Computational tractability often not feasible
- Model complexity increases cost
- Realistic scenarios requires scalable models

How do we maintain computational tractability while capturing realistic scenarios?

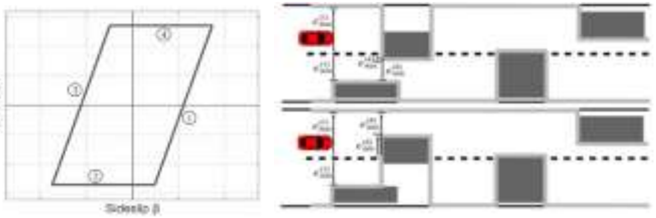
Related Work



Mitchell, I.M., et.al.[2]



Althoff, M., et.al.[3]



Erlien, S.M., et.al.[4]

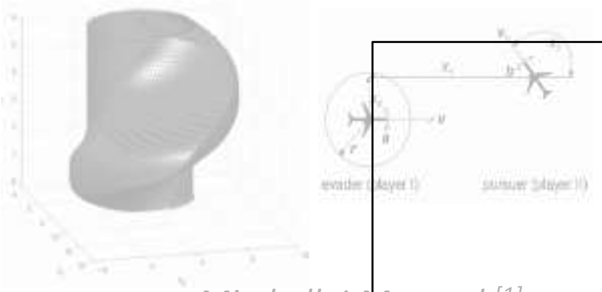
- Backwards Reachability from Goal
- Formulation as Hamilton-Jacobi PDE
- Solution over Discretized State Space

- Online Verification of Planned Maneuvers
- Rough Approximations for Reachable Sets
- Safe Backup Trajectory

- Shared Steering Control
- Safety Guarantees through Dynamical and Road Constraints
- MPC Looks for Possible Trajectory to Ensure Safety

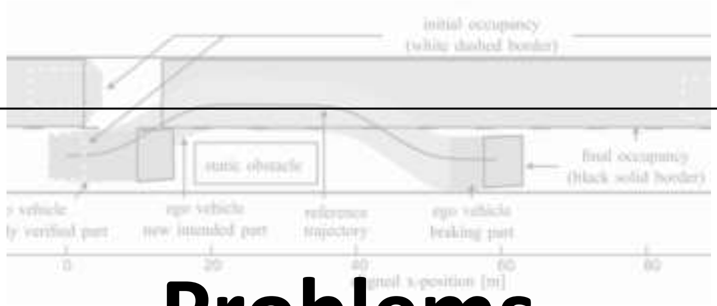
[2] Mitchell, I.M., et. al.: A time-dependent Hamilton-Jacobi formulation of reachable sets for continuous dynamic games. IEEE Transactions on Automatic Control 50(7), 947–957 (2005)
[3] Althoff, M., et.al.: Online Verification of Automated Road Vehicles Using Reachability Analysis. IEEE Trans. Robotics 30(4), 903–918 (2014)
[4] Erlien, S.M., et. Al.: Shared steering control using safe envelopes for obstacle avoidance and vehicle stability. IEEE Transactions on Intelligent Transportation Systems 17(2), 441–451 (2016)

Related Work



Mitchell, I.M., et.al.[1]

- Backwards Reachability from Goal
- Formulation as Hamilton-Jacobi PDE
- Solution over Discretized State Space



Althoff, M., et.al.[2]

- Online Verification of Planned Maneuvers
- Rough Approximations for Reachable Sets
- Safe Backup Trajectory

Erlien, S.M., et.al.[3]

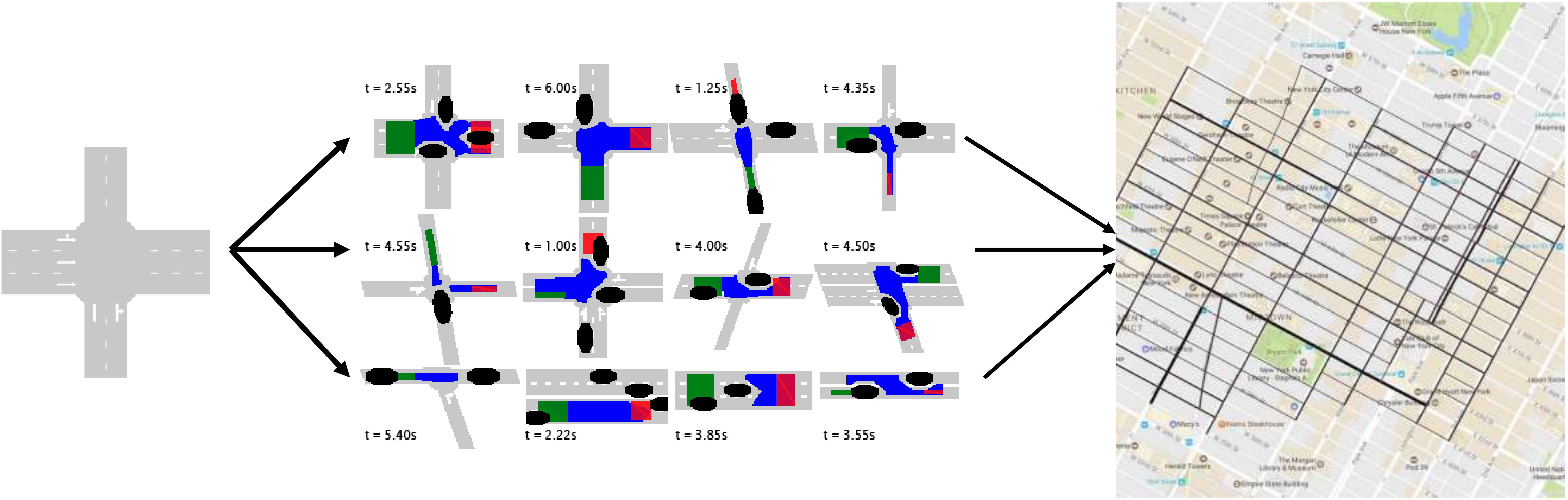
- Shared Steering Control
- Safety Guarantees through Dynamical and Road Constraints
- MPC looks for possible trajectory to ensure safety

Problems

- **Accurate but very specific**
- **More general but low-fidelity**

[1] Mitchell, I.M., et. al.: A time-dependent Hamilton-Jacobi formulation of reachable sets for continuous dynamic games. IEEE Transactions on Automatic Control 50(7), 947–957 (2005)
[2] Althoff, M., et.al.: Online Verification of Automated Road Vehicles Using Reachability Analysis. IEEE Trans. Robotics 30(4), 903–918 (2014)
[3] Erlien, S.M., et. Al.: Shared steering control using safe envelopes for obstacle avoidance and vehicle stability. IEEE Transactions on Intelligent Transportation Systems 17(2), 441–451 (2016)

Two Step Approach

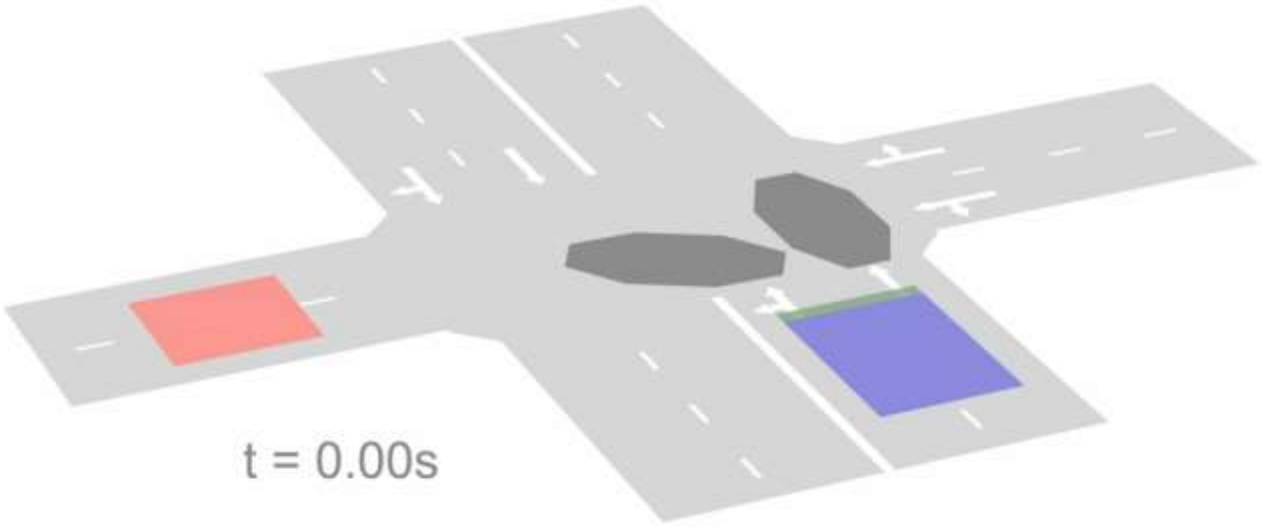


Library of Road Geometries

Parallel Local Verification

Global Guarantees

Local Verification – Results



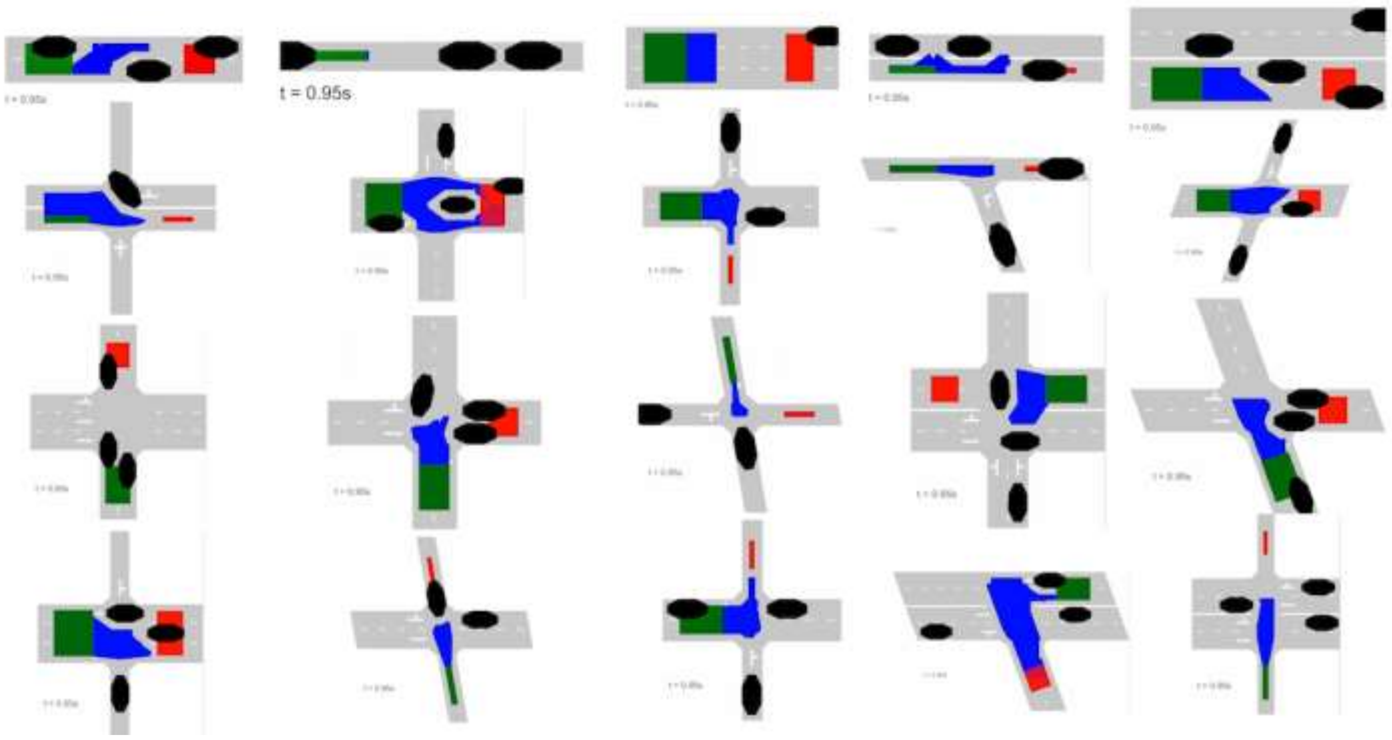
= Ego Car

= Other Car

= Entry Region

= Exit Region

Local Verification – Results



= Ego Car

= Other Car

= Entry Region

= Exit Region

Global Guarantees – Results

= Ego Car

= Other Car

= Entry Region

= Exit Region

Global Guarantees – Results

= Ego Car

= Other Car

= Entry Region

= Exit Region

Compositional and Contract-based Verification for Autonomous Driving on Road Networks

Lucas Liebenwein, Wilko Schwarting, Cristian-Ioan Vasile,
Jonathan DeCastro, Javier Alonso-Mora, Sertac Karaman, Daniela Rus

lucasl@mit.edu