DryVR: Data-driven verification and compositional reasoning for automotive systems

Chuchu Fan, Bolun Qi, Sayan Mitra, Mahesh Viswannathan

University of Illinois at Urbana-Champaign

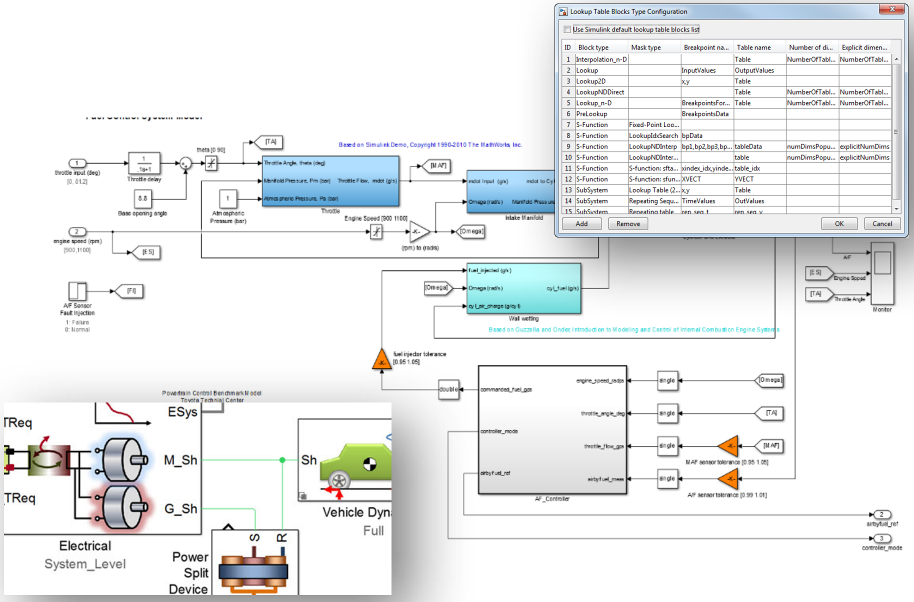
CAV 2017, Heidelberg, Germany

Hybrid modelling: theory vs. reality

Control systems in textbook

$$\frac{dx}{dt} = f(x,u); u = g(x)$$

Control system in reality



"All models are wrong, some are useful"

DryVR

Gain serenity to accept models as they are

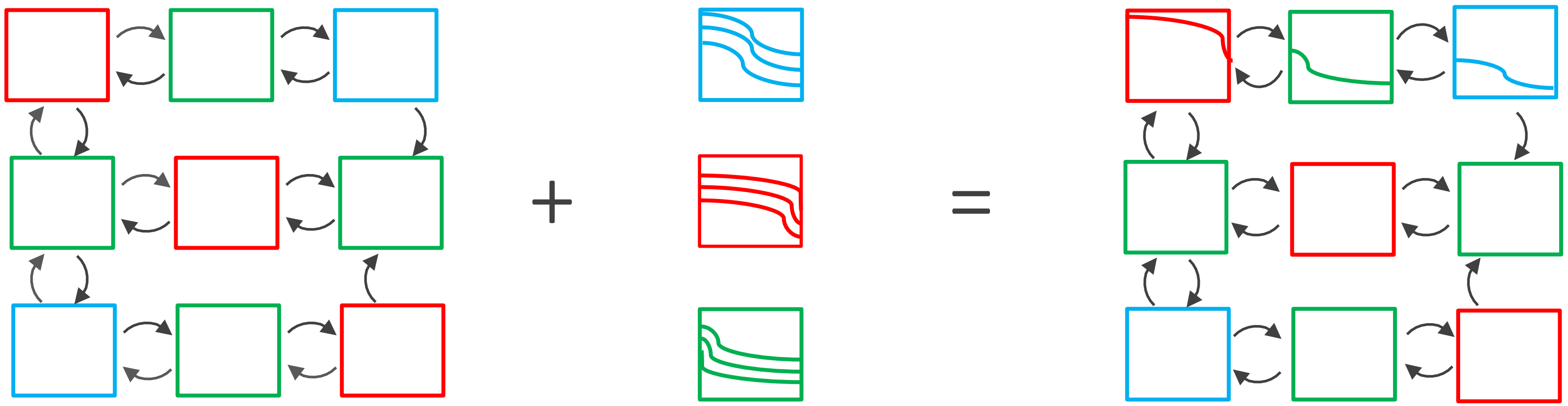
https://github.com/qibolun/DryVR

A new view of knowledge in hybrid models

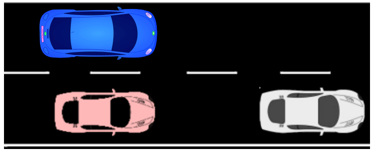
Complete information of switching structure

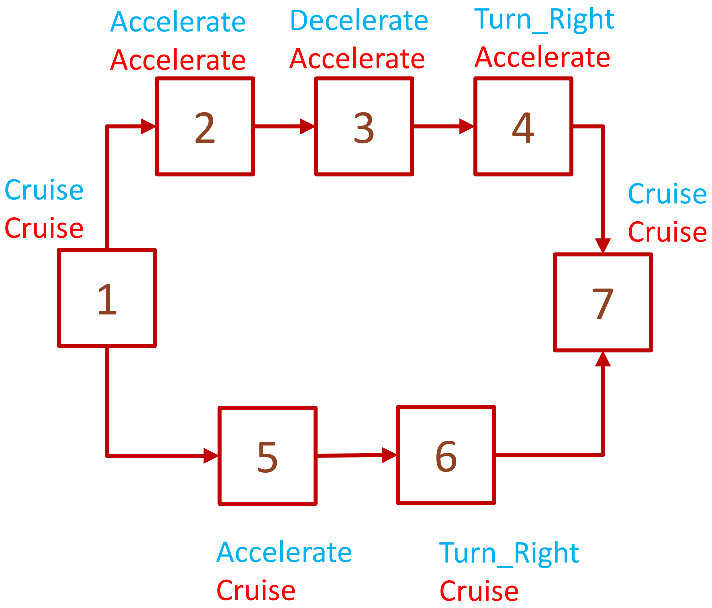
Executable access to mode dynamics

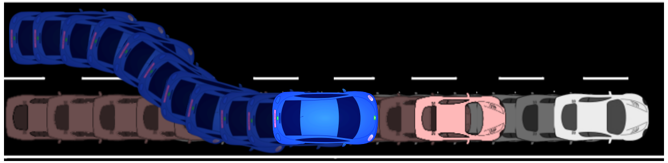
DryVR's Executable hybrid model

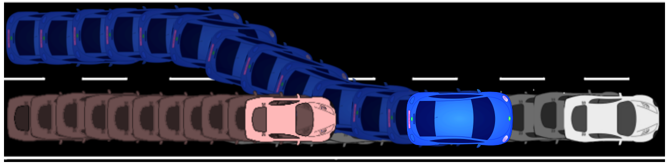


DryVR model of lane merge

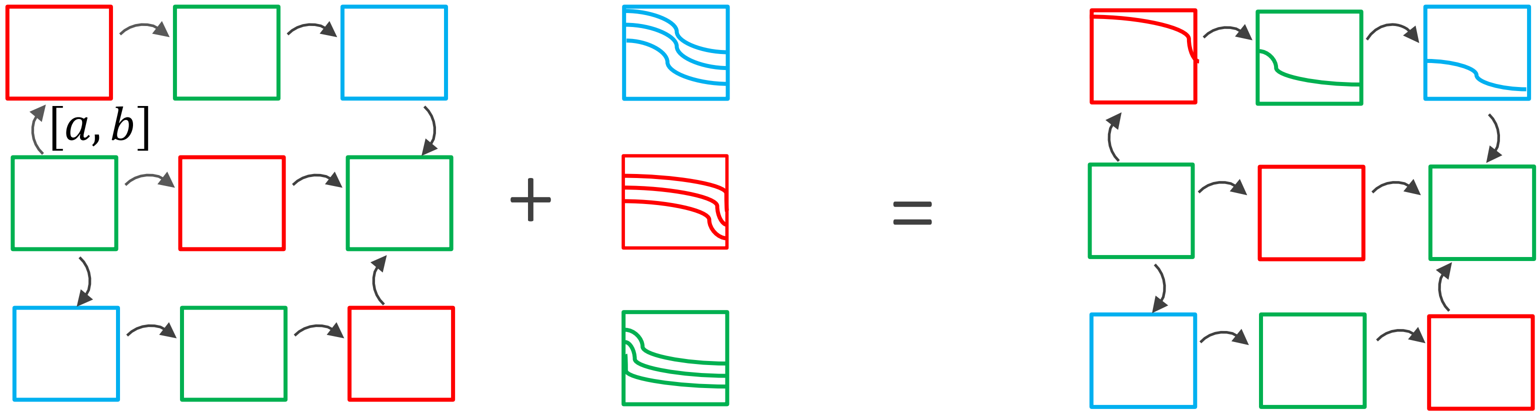








DryVR model semantics



Transition graph

Trace: $l_1, t_1, l_2, t_2, \ldots, l_k$

Black-box simulator

Trajectory: $\tau(t)$

Labeled trajectory set: $\langle \tau, l \rangle \in \mathcal{TL}$

Hybrid system $\mathcal{H} = \langle \mathcal{L}, \Theta, G, \mathcal{TL} \rangle$

State: a point in $\mathbb{R}^n \times \mathcal{L}$

$Reach = \{\langle x, l \rangle |$ for some $v, t, \langle x, l \rangle$ is reachable from $\Theta\}$

$Reach|v$: all states reachable in vertex v

Outline

Proof rules

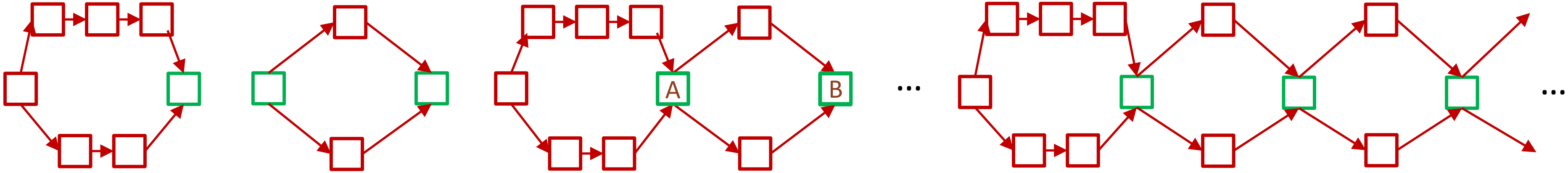
Bounded model checking

Case studies

Composition for unbounded time analysis

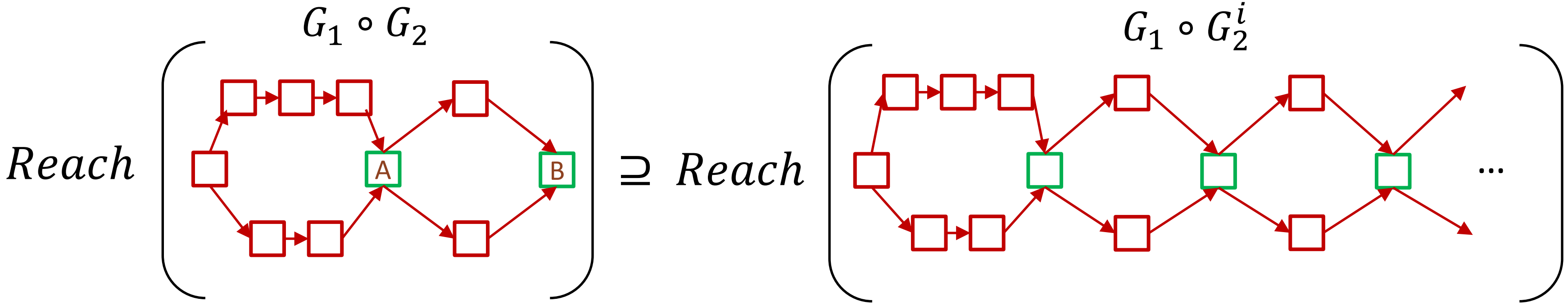
If $Reach|B \subseteq Reach|A$ then

$G_1 \circ G_2 = G_1 \circ G_2 \quad \ldots \quad G_1 \circ G_2^i$



Composition for unbounded time analysis

If $Reach|B \subseteq Reach|A$ then

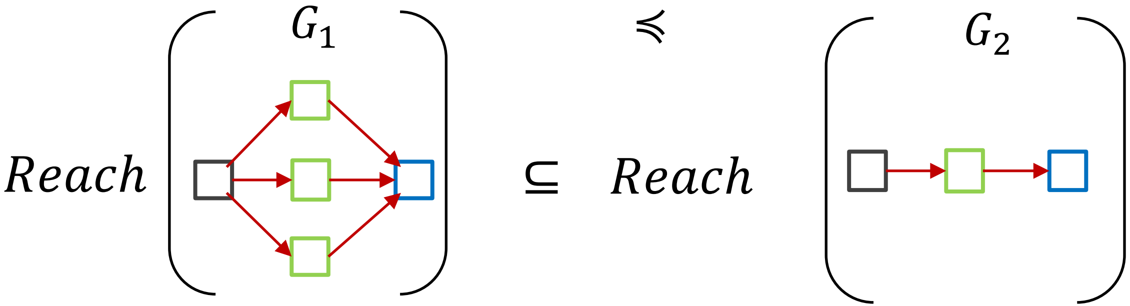


Reasoning about behavior containment

Trace containment $G_1 \preccurlyeq G_2$

Trajectory containment $\mathcal{TL}_1 \preccurlyeq \mathcal{TL}_2$

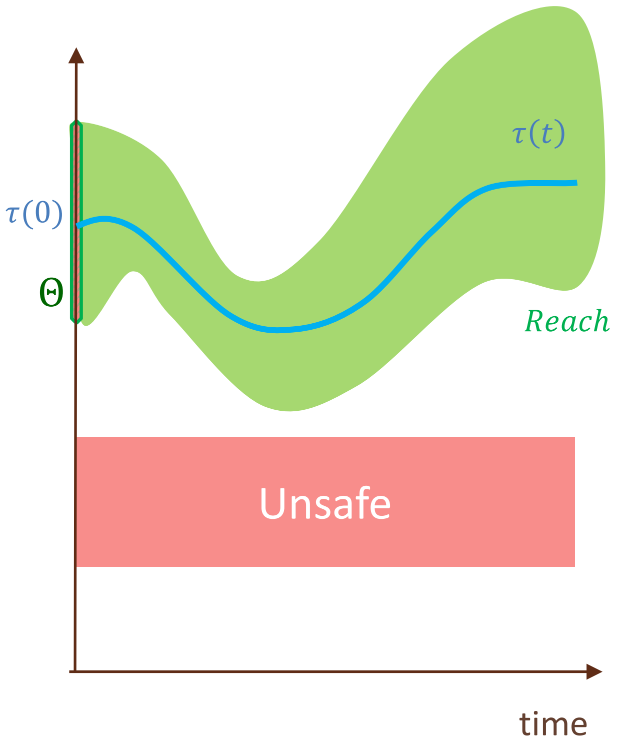
If $\Theta_1 \subseteq \Theta_2, G_1 \preccurlyeq G_2, \mathcal{TL}_1 \preccurlyeq \mathcal{TL}_2$, then



Simulation-driven bounded verification

Safety problem: given initial set Θ and unsafe set U, decide

$$Reach \cap U = \emptyset?$$



Simulation-driven bounded verification

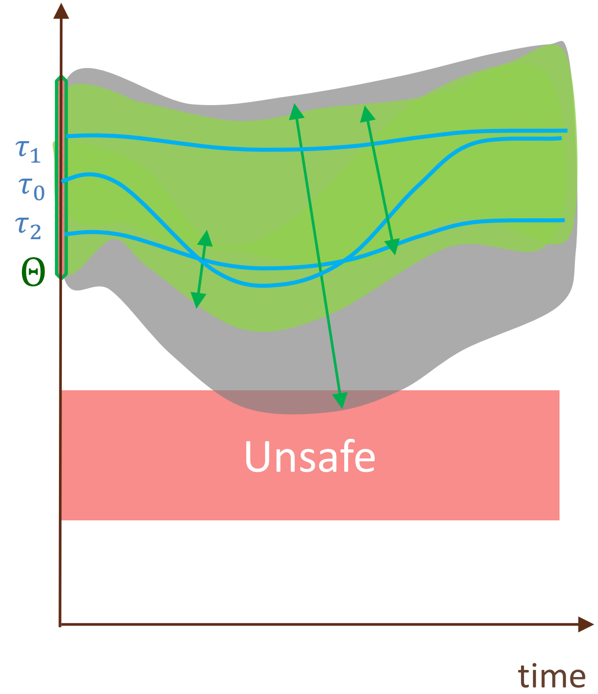
Simulation-driven verification for a single vertex v

- Simulate → Generalization → Check and refine

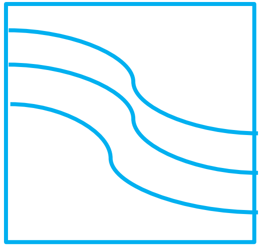
Discrepancy β bounds distance between neighboring trajectories

$$\|\tau_1(t) - \tau_2(t)\| \le \beta(\tau_1(0), \tau_2(0), t),$$

- From a single simulation of $\tau_1(t)$ and discrepancy β over-approximate the reach set from a neighborhood of $\tau_1(0)$
- Earlier approaches use $f(x), \frac{\partial f(x)}{\partial x}$ [Duggirala et al. TACAS 15] [Fan et al. CAV 15-16] inapplicable



Learning discrepancy from data



Global exponential discrepancy function

$$\beta(x_1, x_2, t) = |x_1 - x_2| K e^{\gamma t}$$

For any pair of trajectories τ_1 and τ_2 in mode 

$$\forall t \in [0, T], |\tau_1(t) - \tau_2(t)| \leq |\tau_1(0) - \tau_2(0)| K e^{\gamma t}$$

Taking logarithm and rearrange:

$$\forall t, \ln \frac{|\tau_1(t) - \tau_2(t)|}{|\tau_1(0) - \tau_2(0)|} \leq \gamma t + \ln K$$

Learning linear separators

For a subset $S \subseteq \mathbb{R} \times \mathbb{R}$, a linear separator is a pair $(a, b) \in \mathbb{R}^2$ such that

$$\forall (x, y) \in S, x \leq ay + b$$

Algorithm:

1. Draw k pairs $(x_1, y_1), \ldots, (x_k, y_k)$ from S according to $\mathcal{D}$.
2. Find $(a, b) \in \mathbb{R}^2$ such that $x_i \leq a y_i + b$ for all $i \in \{1, \ldots, k\}$.

Proposition [Valiant 84]: Let $\epsilon, \delta \in \mathbb{R}^+$. If $k \geq \frac{1}{\epsilon} \ln \frac{1}{\delta}$ then with probability $1 - \delta$, the above algorithm finds (a, b) such that $err_{\mathcal{D}}(a, b) < \epsilon$.

- $err_{\mathcal{D}}(a, b) = \mathcal{D}(\{(x, y) \in S \mid x > ay + b\})$

Learning discrepancy from data

Solve the LP problem:

$$\min \quad 2c \ln K + c(c+1)\gamma T$$ --- Volume of the reach set

$$\text{s.t.} \quad \forall i, j, s, \ln \frac{|\tau_i(t_s) - \tau_j(t_s)|}{|\tau_i(0) - \tau_j(0)|} \leq \gamma t_s + \ln K$$

1 million testing show 96% accuracy for 10 training trajectories, and >99.9% for 20

Other discrepancy shapes in paper: piece-wise exponential, global polynomial, piece-wise polynomial

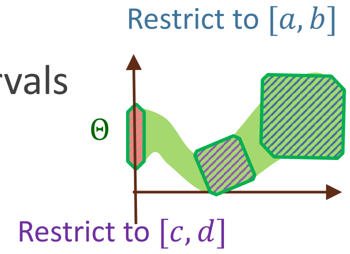
Bounded safety algorithm

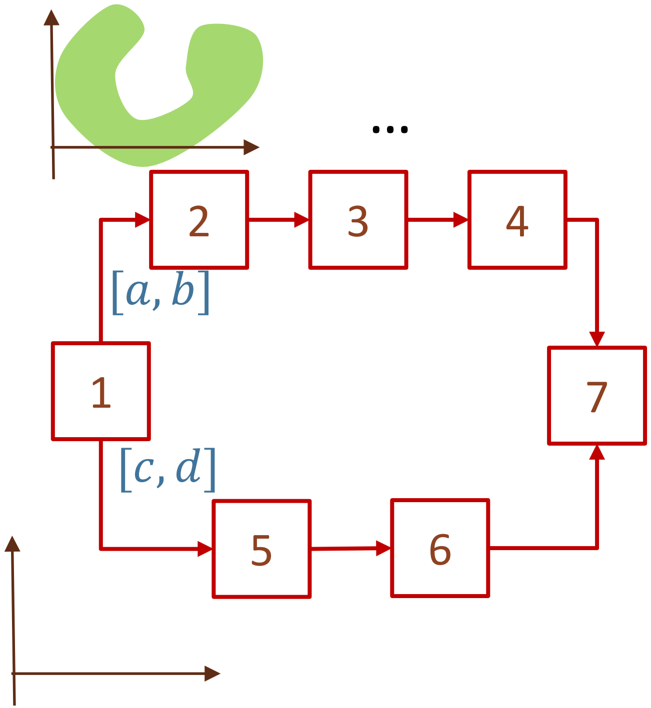
1. Compute reach set from Θ: proceeds on G in a topologically sorted order

2. Refinement:
   - Split Θ to smaller sets
   - Split transition time interval to smaller intervals

Guarantee: Assuming that the learned discrepancy function is correct:

- Soundness
- Relative completeness
- Discrepancy has $err_{\mathcal{D}}(a,b) < \epsilon$ with $\geq \frac{1}{\epsilon}\ln\frac{1}{\delta}$ samples

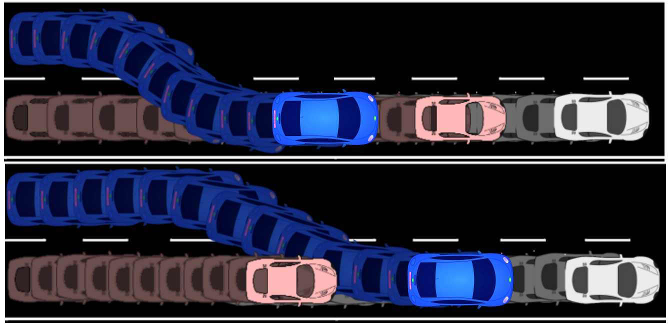


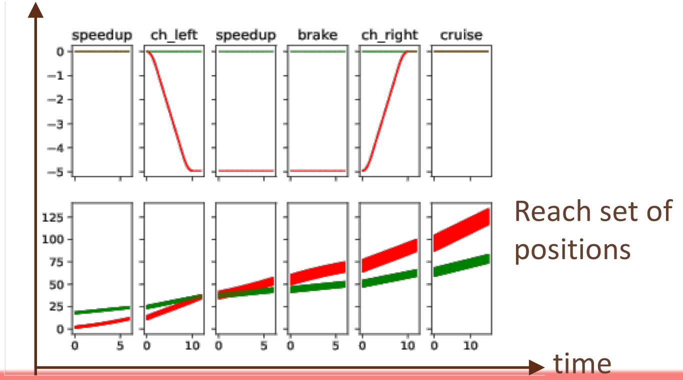


Automotive maneuvers

https://github.com/qibolun/DryVR

Model	Time horizon	Unsafe set	# Refinement	Safe	Run time
Auto-passing	50	Collision	4	✔	208s
	50	Collision	5	✘	152s
Lane-merge	50	Collision	0	✔	55s
	50	Collision	0	✘	38s
Lane-merge-highway	50	Collision	4	✔	197s
	50	Collision	0	✘	21s
Powertrain	80	Air/Fuel out of bound	2	✔	217s
Automatic transmission	50	Engine speed too high	2	✔	109s

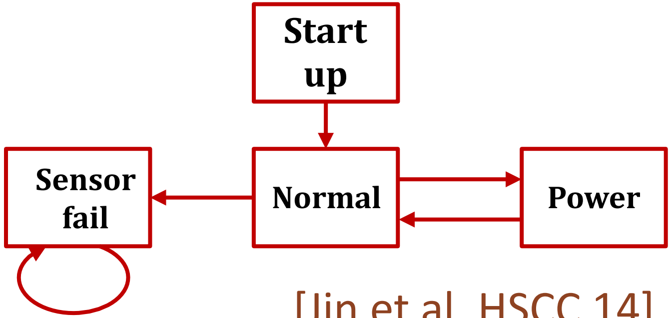




Case studies: Engine control

Model	Time horizon	Unsafe set	# Refinement	Safe	Run time
Auto-passing	50	Collision	4	✔	208s
	50	Collision	5	✘	152s
Lane-merge	50	Collision	0	✔	55s
	50	Collision	0	✘	38s
Lane-merge-highway	50	Collision	4	✔	197s
	50	Collision	0	✘	21s
Powertrain	80	Air/Fuel out of bound	2	✔	217s
Automatic transmission	50	Engine speed too high	2	✔	109s

https://github.com/qibolun/DryVR

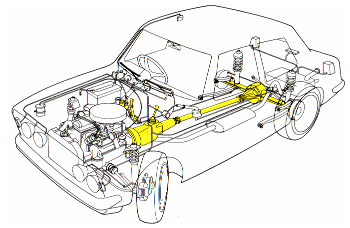


[Jin et al. HSCC 14]

Case studies: transmission control

https://github.com/qibolun/DryVR

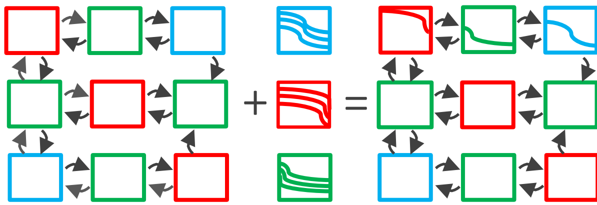
Model	Time horizon	Unsafe set	# Refinement	Safe	Run time
Auto-passing	50	Collision	4	✔	208s
	50	Collision	5	✘	152s
Lane-merge	50	Collision	0	✔	55s
	50	Collision	0	✘	38s
Lane-merge-highway	50	Collision	4	✔	197s
	50	Collision	0	✘	21s
Powertrain	80	Air/Fuel out of bound	2	✔	217s
Automatic transmission	50	Engine speed too high	2	✔	109s



Conclusion

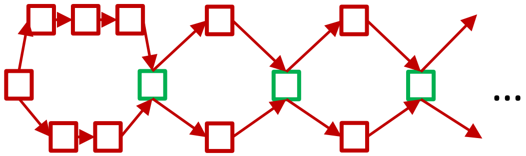
A fresh perspective (DryVR's model) on modeling hybrid systems

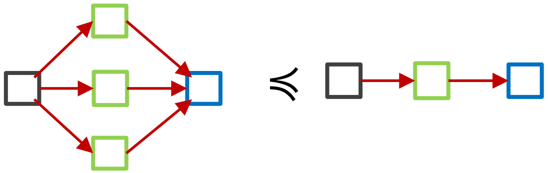
- white box transition graph + black box simulator
- Case studies ADAS / AV



Enables types of static-dynamic analysis

- Black-box => discrepancy functions with probabilistic guarantees
- Bounded verification [Sound and relatively complete]
- Proof rules for sequential composition for unbounded time verification and behavior containment





Future: More expressive white boxes, synthesis, monitoring,

Links and references

Textbook picture links:

https://images.google.com/

References :

[Fan et al ATVA 15] Fan, Chuchu, and Sayan Mitra. "Bounded verification with on-the-fly discrepancy computation." International Symposium on Automated Technology for Verification and Analysis. Springer International Publishing, 2015.

[Fan 16 et al CAV 16] Fan, Chuchu, et al. "Automatic Reachability Analysis for Nonlinear Hybrid Models with C2E2." International Conference on Computer Aided Verification. Springer International Publishing, 2016.

[Duggirala et al TACAS 15] Duggirala, Parasara Sridhar, et al. "C2E2: A Verification Tool for Stateflow Models." TACAS. 2015.

[Valiant 84] Valiant, Leslie G. "A theory of the learnable." Communications of the ACM 27.11 (1984): 1134-1142.

[Jin et al. HSCC 14] Jin, X., Deshmukh, J. V., Kapinski, J., Ueda, K., & Butts, K. (2014, April). Powertrain control verification benchmark. In Proceedings of the 17th international conference on Hybrid systems: computation and control (pp. 253-262). ACM.

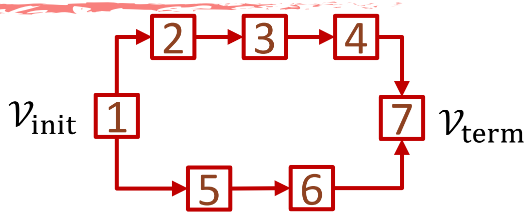
Thank you

for your precious time and attention

DryVR model semantics

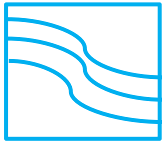
Transition graph:

- Trace: $l_1, t_1, l_2, t_2, \ldots, l_k$



Black-box simulator

- Trajectory: $\tau(t)$
- Labeled trajectory set: $\langle \tau, l \rangle \in \mathcal{TL}$



Hybrid system $\mathcal{H} = \langle \mathcal{L}, \Theta, G, \mathcal{TL} \rangle$

- State: a point in $\mathbb{R}^n \times \mathcal{L}$
- Initial states: $\Theta \times \mathcal{L}_{\text{init}}$
- $Reach = \{\langle x, l \rangle |$ for some $v, t, \langle x, l \rangle$ is reachable from $\Theta\}$
- $Reach|v$: all states reachable in vertex v

Learning linear separators (cont.)

For a subset $\Gamma \subseteq \mathbb{R}\times\mathbb{R}$, a linear separator is a pair $(a, b) \in \mathbb{R}^2$ such that

$$\forall (x, y) \in \Gamma, x \leq ay + b$$

$$\forall \left(\ln \frac{|\tau_1(t) - \tau_2(t)|}{|\tau_1(0) - \tau_2(0)|}, t \right) \in \Gamma, \ln \frac{|\tau_1(t) - \tau_2(t)|}{|\tau_1(0) - \tau_2(0)|} \leq \gamma t + \ln K$$

Proposition [Valiant 84]: Let $\epsilon, \delta \in \mathbb{R}^+$. If $k \geq \frac{1}{\epsilon} \ln \frac{1}{\delta}$ then with probability $1 - \delta$, the above algorithm finds (a, b) such that $err_{\mathcal{D}}(a, b) < \epsilon$.

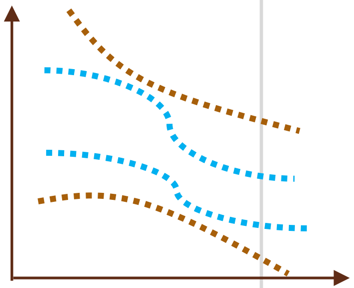
- $err_{\mathcal{D}}(a, b) = \mathcal{D}(\{(x, y) \in \Gamma \mid x > ay + b\})$

Safety verification problem

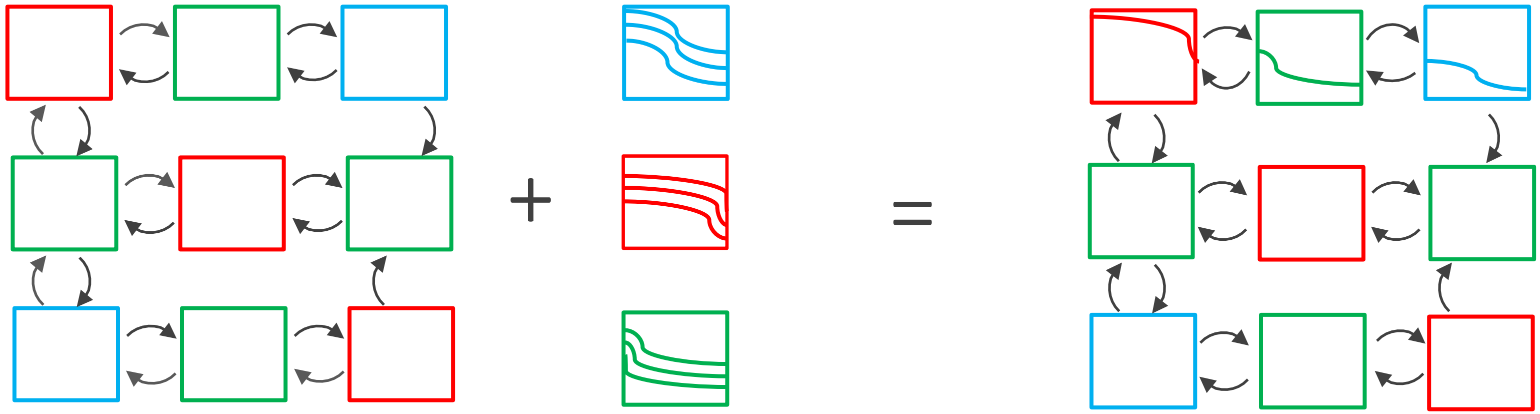
Is there a behavior of system S violating safety requirement R within time bound T?

Yes -> bug-trace -> design improvement

No -> safety proof -> certification



DryVR model semantics



Transition graph

Trace: $l_1, t_1, l_2, t_2, \ldots, l_k$

Black-box simulator

Trajectory: $\tau(t)$

Labeled trajectory set:

$\langle \tau, l \rangle \in \mathcal{TL}$

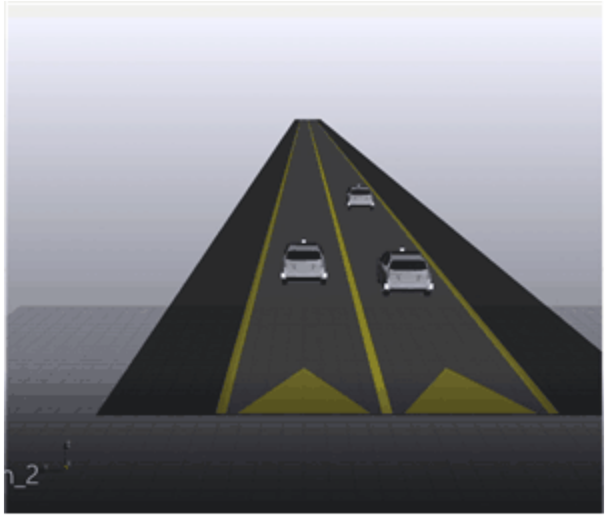
Hybrid system $\mathcal{H} = \langle \mathcal{L}, \Theta, G, \mathcal{TL} \rangle$

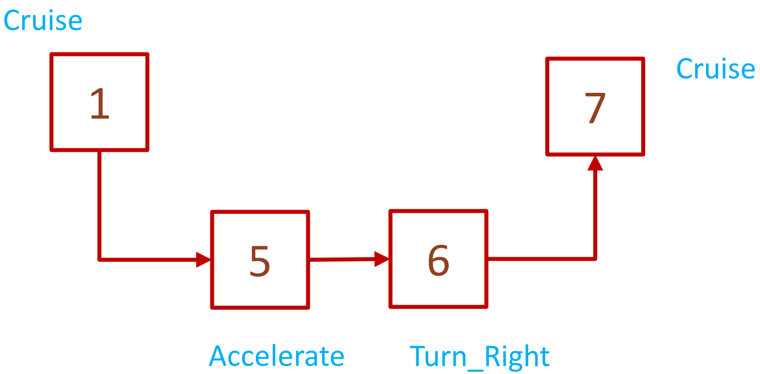
State: a point in $\mathbb{R}^n \times \mathcal{L}$

$Reach = \{\langle x, l \rangle |$ for some $v, t, \langle x, l \rangle$ is reachable from $\Theta\}$

$Reach|v$: all states reachable in vertex v

DryVR's model of lane merge





DryVR's model of lane merge