Symbolic and Numerical Techniques for Verification and Synthesis of Cyber-Physical Systems

PI: Parasara Sridhar Duggirala, University of North Carolina at Chapel Hill

THE UNIVERSITY of NORTH CAROLINA at CHAPEL HILL

This projected is aimed at improving the scalability of verification and synthesis techniques applied in Cyber-Physical Systems. In the prior work, the PI proposed and improved the representation called **generalized star sets** that are useful in computing reachable sets not only Cyber-Physical Systems, but also for Neural Networks.

Challenges in verification of Cyber-Physical Systems:

- Curse of dimensionality.
- Trajectories are nonlinear functions of states and involves matrix exponentials: $e^{At} = I + \frac{At}{1!} + \frac{(At)^2}{2!} + \cdots$
- Verification tools often ignore model uncertainties and return only one counter-example for system designer.

Contributions to other Cyber-Physical Systems projects:

- The reachable set representation called **generalized star** proposed by the PI is also useful in analyzing safety of neural network guided control systems.
- The techniques for generating counter-examples can be extended to other disciplines like software and hardware verification.

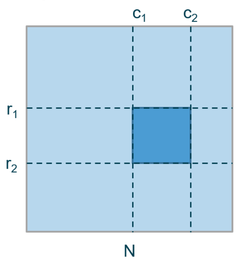
Technical contributions: (over the last year): Robust Reachable Set and Counterexample Search.

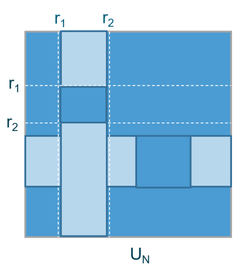
Q: When can we compute efficient reachable sets efficiently?

A: If a structural property of the system holds.

Q: If property doesn't hold?

A: Compute **statistically robust reachable set**.



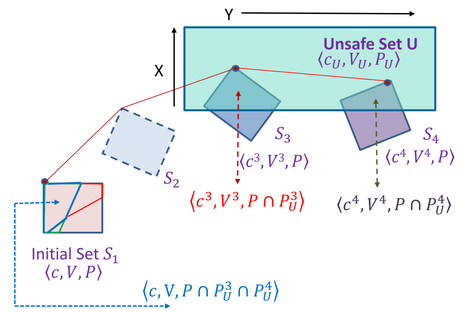


Q: What are the various types of counter-examples useful for control designers?

A: Taxonomy – **longest, deepest, robust** counter-examples.

Q: How to generate them?

A: Use generalized star representation, formulate it as MILP or SMT-Optimization.



Broader Impacts for Society: These techniques help in designing and analyzing robust Cyber-Physical Systems

Broader Impacts for Industry: 1) Proved safety of satellite rendezvous systems. 2) Counter-examples help system designer diagnose the faults in CPS.

References: Bineet Ghosh and Parasara Sridhar Duggirala. Robust reachable set: Accounting for uncertainties in linear dynamical systems. ACM Transactions on Embedded Computing Systems (TECS),18(5s):1–22, 2019.

Bineet Ghosh and Parasara Sridhar Duggirala. Reachability of linear uncertain systems: Sampling based approaches. UNC Tech Report, 2021.

Manish Goyal, David Bergman, and Parasara Sridhar Duggirala. Generating longest counterexample: On the cross-roads of mixed integer linear programming and SMT. In 2020 American Control Conference (ACC), pages 1823–1829. IEEE, 2020.

Manish Goyal and Parasara Sridhar Duggirala. Extracting counterexamples induced by safety violation in linear hybrid systems. Automatica, 117:109005, 2020.

2021 NSF Cyber-Physical Systems Principal Investigators' Meeting
June 2-4, 2021

Award ID#: 1935724