Automated Formal Verification of Dynamical Systems

Mark Wetzlinger
m.wetzlinger@tum.de

Supervisors: Matthias Althoff & Samarjit Chakraborty

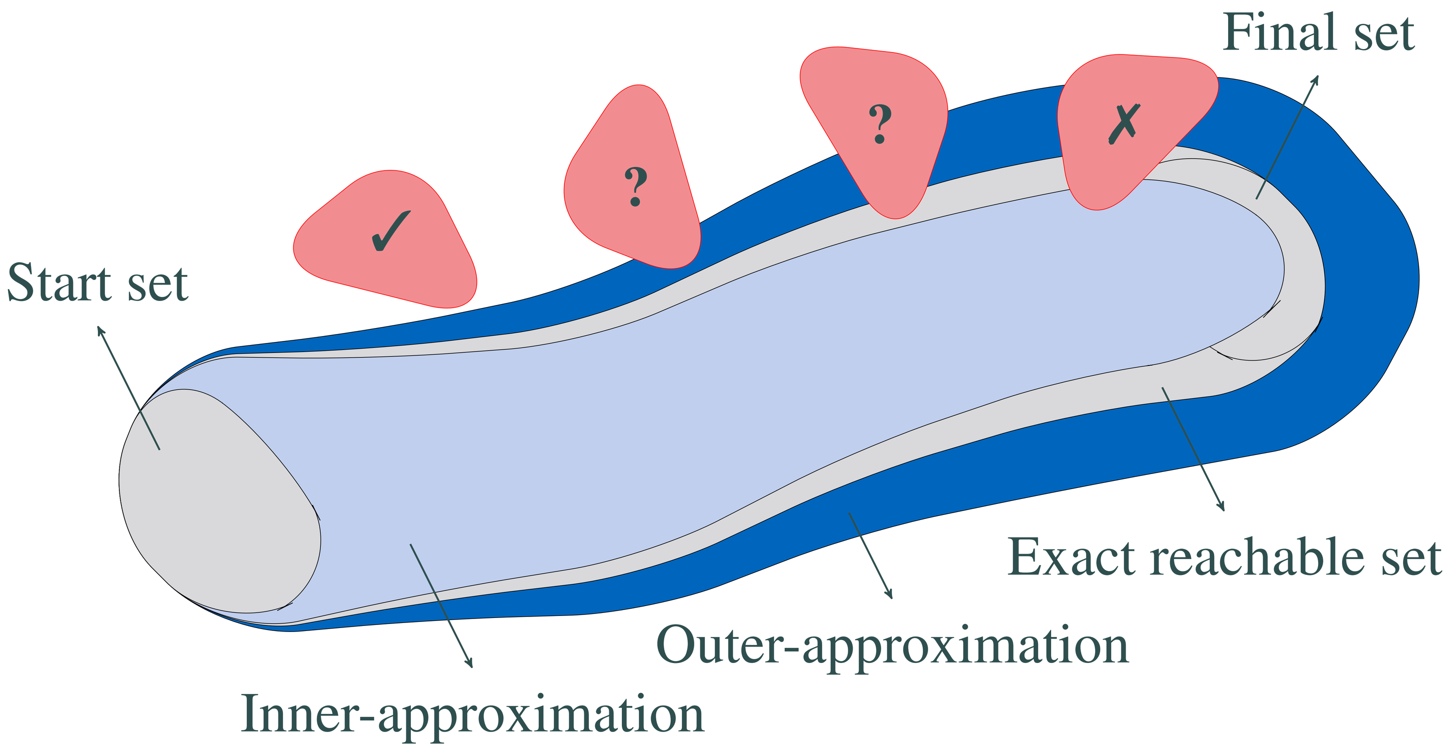
Collaborators: Niklas Kochdumper (Stony Brook University) & Adrian Kulmburg (TUM) & Stanley Bak (Stony Brook University)

ConVeY

Motivation

How to provide **safety guarantees** for cyber-physical systems in the presence of uncertainties?
The **reachable set** represents all possible future behaviors, but only **inner-/outer-approximations** are computable.

Verification: For a given system, uncertainties, and time horizon, are **any unwanted states reachable** (red sets)?



We cannot always prove or disprove safety with the computed inner-/outer-approximations.
$\longrightarrow$ **Tighter approximations** are required!

Background

We consider linear time-invariant (LTI) systems

$$\dot{x}(t) = Ax(t) + Bu(t), \quad x \in \mathbb{R}^n, u \in \mathbb{R}^m$$

and nonlinear systems

$$\dot{x}(t) = f(x(t), u(t)), \quad x \in \mathbb{R}^n, u \in \mathbb{R}^m,$$

with an uncertain initial state $x(t_0) \in \mathcal{X}^0 \subset \mathbb{R}^n$ and uncertain inputs $\forall t: u(t) \in \mathcal{U} \subset \mathbb{R}^m$.

Approach

A) *Automated Verification of Linear Systems*
Steps to automate reachability computation [1, 4]:

1. **Error bounds** for all sources of **over-approximation**:
   – enclosures of the homogeneous/particular solutions,
   – operations under which zonotopes are not closed.
2. **Automatically tune algorithm parameters** such that total error remains below a user-provided maximum error.

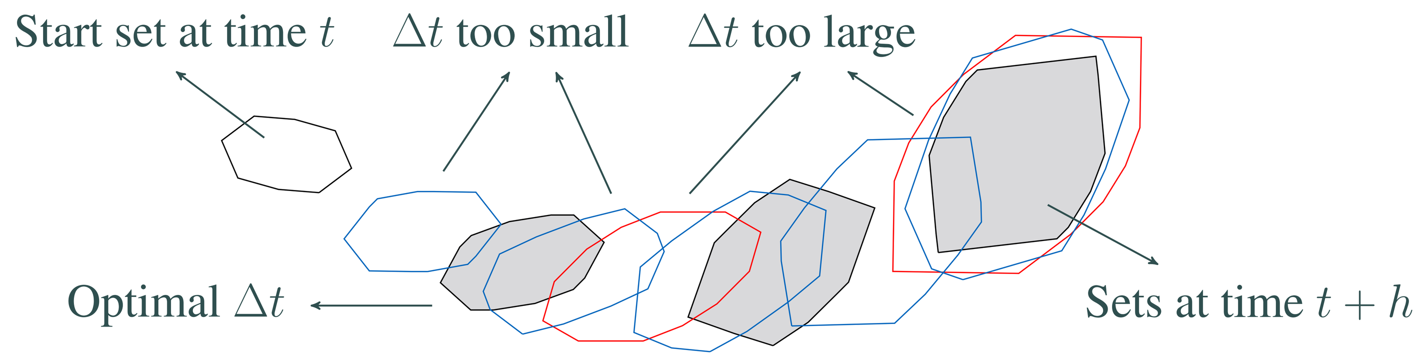
Verification: **Iteratively refine** the maximum error [4].

Convergence: Safety can be **verified or falsified for all safety specifications** not requiring the *exact* reachable set.

Alternative approach [5]: Skip explicit computation of errors, convergence via automated parameter tuning only.

B) *Automated Reachability Analysis of Nonlinear Systems*
Tight reachable sets by **local parameter optimization** [2]:

1. Measure influence of parameters on reachable set size
2. Compare different time step sizes over fixed horizon



$\longrightarrow$ **Optimal time step size** via scalar cost function.

Side result: Introduction of **gain order**, i.e., change in local approximation error due to change in time step size [3].

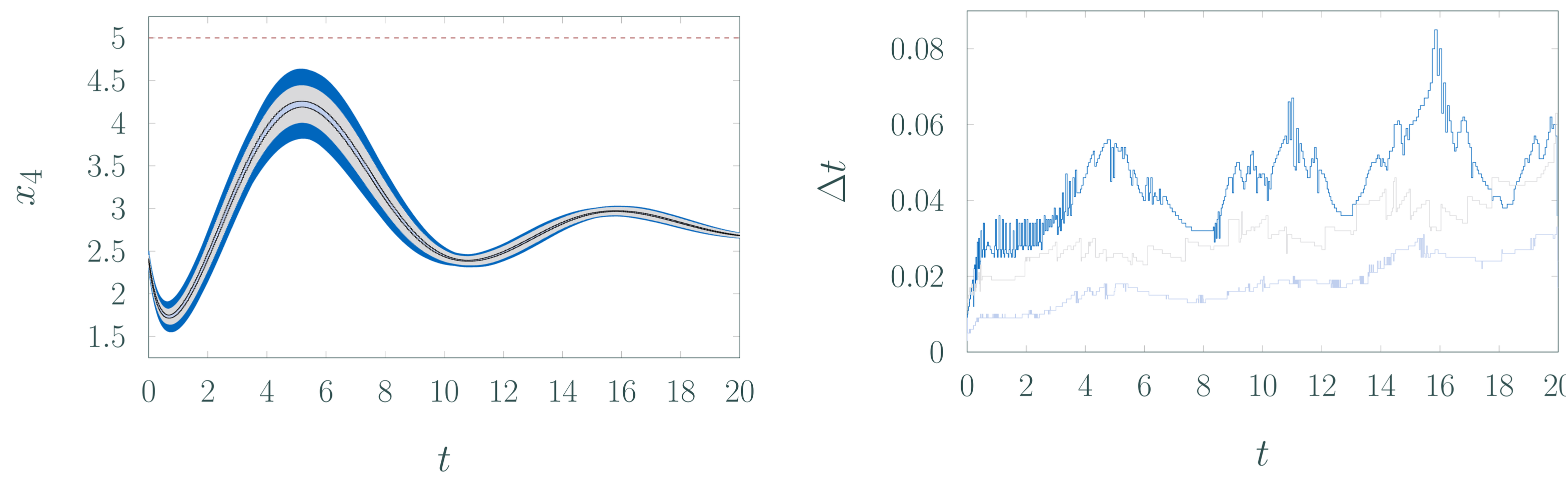
Evaluation

A) Comparison of [5] to state-of-the-art reachability tools on benchmarks from the **ARCH competition** (excerpt):

Benchmark			Our approach			Time comparison			
Identifier	n	m	Safe?	Time	Refs.	CORA	HyDRA	JuliaReach	SpaceEx
HEAT01	125	0	✓	0.17s	2	2.2s	13.2s	**0.13s**	4.2s
HEAT02	1000	0	✓	**2.2s**	2	9.3s	160s	32s	—
CBC01	201	0	✓	**0.11s**	2	7.1s	—	1.4s	313s
CBC02	1001	0	✓	**2.2s**	2	—	—	—	—
CBC03	2001	0	✓	**28s**	3	—	—	—	—
CBF01	200	1	✓	**0.27s**	2	30s	—	12s	319s
CBF02	1000	1	✓	**3.7s**	2	—	—	—	—
CBF03	2000	1	✓	**49s**	3	—	—	—	—
ISSC01-ISS02	273	0	✓	**0.11s**	1	1.3s	—	1.4s	29s
ISSF01-ISS01	270	3	✓	**0.49s**	2	59s	—	10s	49s

$\longrightarrow$ all benchmarks solved correctly and fast.

B) Nonlinear system ($n = 7$) from ARCH competition:



Specification (dashed) satisfied for increasing initial set sizes. Time step size Δt adapts to current dynamics.

References

[1] M. Wetzlinger et al. "Adaptive parameter tuning for reachability analysis of linear systems". In: *CDC*. 2020.

[2] M. Wetzlinger et al. "Adaptive Parameter Tuning for Reachability Analysis of Nonlinear Systems". In: *HSCC*. 2021.

[3] M. Wetzlinger et al. "Adaptive reachability algorithms for nonlinear systems using abstraction error analysis". In: *NAHS* 46 (2022).

[4] M. Wetzlinger et al. "Fully automated verification of linear systems using inner- and outer-approximations of reachable sets". In: *arXiv:2209.09321*. 2022.

[5] M. Wetzlinger et al. "Fully automated verification of linear systems using reachability analysis with support functions". In: *HSCC*. 2023.