# Verification of Delayed Differential Dynamics
## *Based on Validated Simulation*[⋆]

**Mingshuai Chen[1], Martin Fränzle[2], Yangjia Li[1], P. N. Mosaad[2], Naijun Zhan[1]**

[1]State Key Lab. of Computer Science, Institute of Software, CAS, China
[2]Dpt. of Computing Science, C. v. Ossietzky Universität Oldenburg, Germany

✉ chenms@ios.ac.cn ☞ lcs.ios.ac.cn/~chenms/

⋆ To appear in Proc. of FM 2016, Springer.

**Abstract**

Verification by simulation, based on covering the set of time-bounded trajectories of a dynamical system evolving from the initial state set by means of a finite sample of initial states plus a sensitivity argument, has recently attracted interest due to the availability of powerful simulators for rich classes of dynamical systems. System models addressed by such techniques involve ordinary differential equations (ODEs) and can readily be extended to delay differential equations (DDEs). In doing so, the lack of validated solvers for DDEs, however, enforces the use of numeric approximations such that the resulting verification procedures would have to resort to (rather strong) assumptions on numerical accuracy of the underlying simulators, which lack formal validation or proof. In this work, we pursue a closer integration of the numeric solving and the sensitivity-related state bloating algorithms underlying verification by simulation, together yielding a safe enclosure algorithm for DDEs suitable for use in automated formal verification. The key ingredient is an on-the-fly computation of piecewise linear, local error bounds by nonlinear optimization, with the error bounds uniformly covering sensitivity information concerning initial states as well as integration error.

## Motivation

The presence of feedback delays in most dynamical systems reduces controllability due to the impossibility of immediate reaction and enhances likelihood of transient overshoot or even oscillation in the feedback system, e.g.

$$\begin{cases} \dot{x}(t) = -x(t) \\ x(0) = 1 \end{cases} \qquad \begin{cases} \dot{x}(t) = -x(t-1) \\ x([-1,0]) \equiv 1 \end{cases}$$

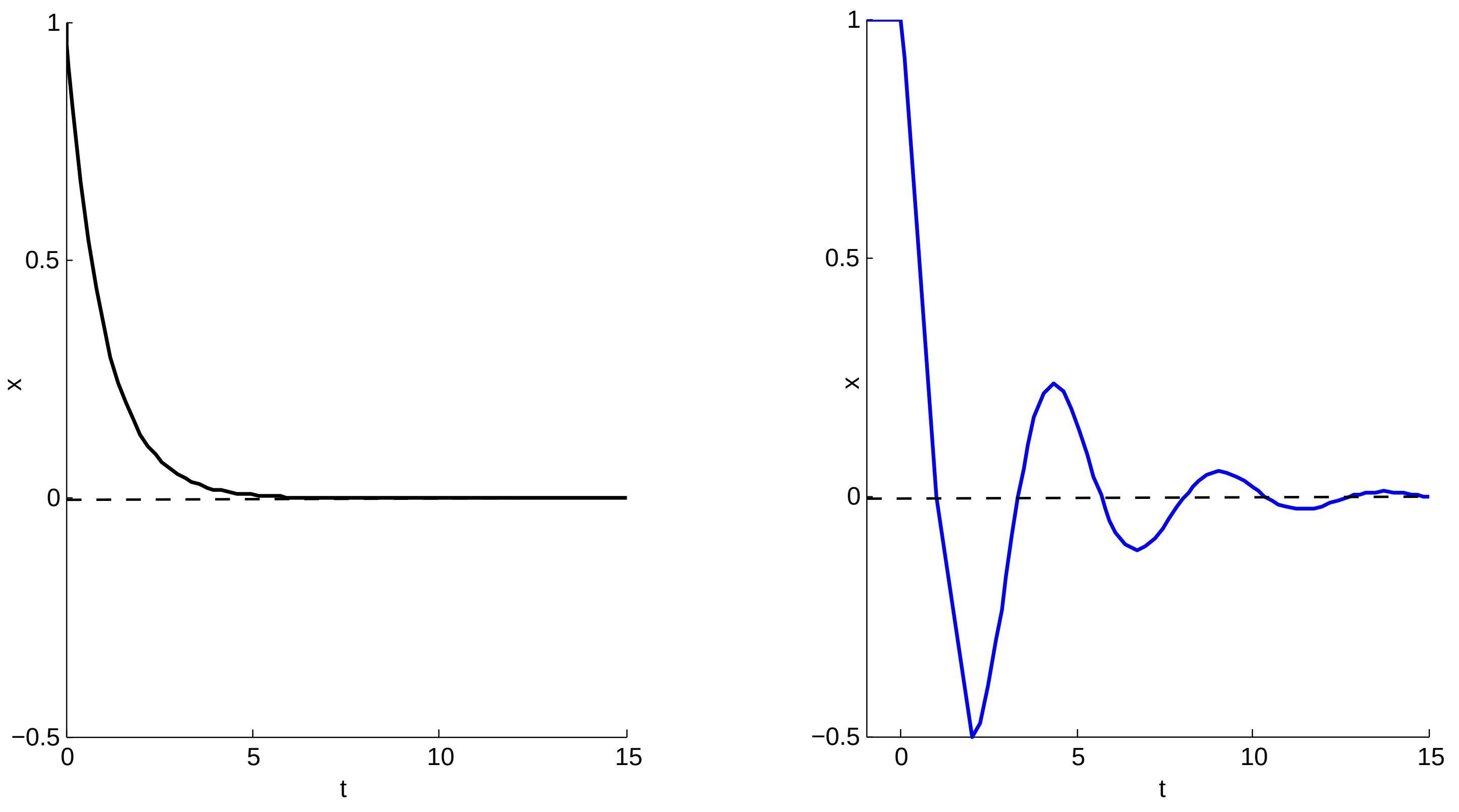


**Figure 1:** One single time delay renders an originally stable system oscillating.

## Problem Formulation

- Delayed dynamical systems:

$$\begin{cases} \dot{\mathbf{x}}(t) &= \boldsymbol{f}(\mathbf{x}(t), \mathbf{x}(t-r_1), \ldots, \mathbf{x}(t-r_k)), \quad t \in [0, \infty) \\ \mathbf{x}(t) &\equiv \mathbf{x}_0 \in \Theta, \quad t \in [-r_k, 0] \end{cases}$$

The unique *solution* (*trajectory*): $\xi_{\mathbf{x}_0}(t) : [-r_k, \infty) \mapsto \mathbb{R}^n$.

- Safety verification: given a time bound $T \in \mathbb{R}$, an initial set $\mathcal{X}_0 \subseteq \Theta$, and an unsafe set $\mathcal{U} \subseteq \mathbb{R}^n$, weather

$$\forall \mathbf{x}_0 \in \mathcal{X}_0 : \quad \left(\bigcup_{t \le T} \xi_{\mathbf{x}_0}(t)\right) \cap \mathcal{U} = \emptyset \quad ?$$

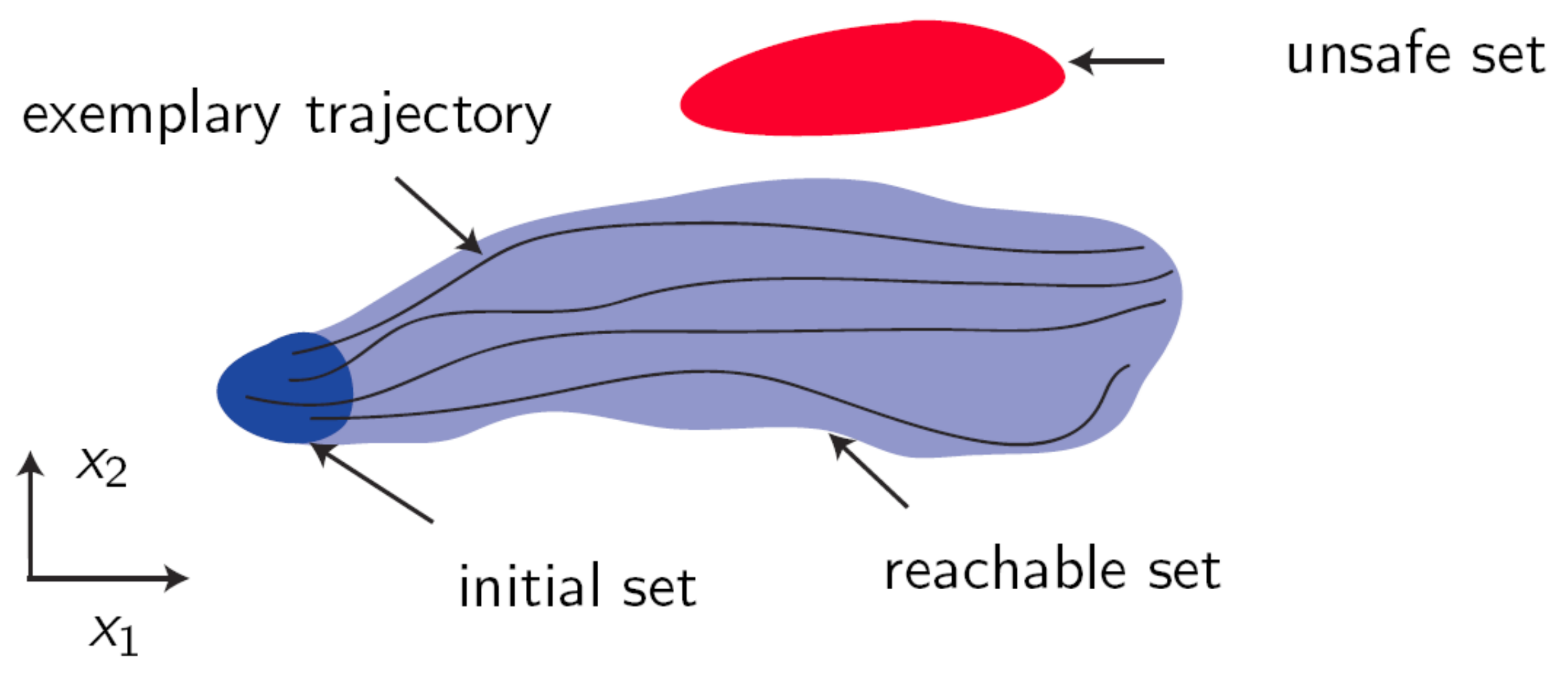


**Figure 2:** System is safe, if no trajectory enters the unsafe set.

## Simulation-Based Verification (cf. [1–4])

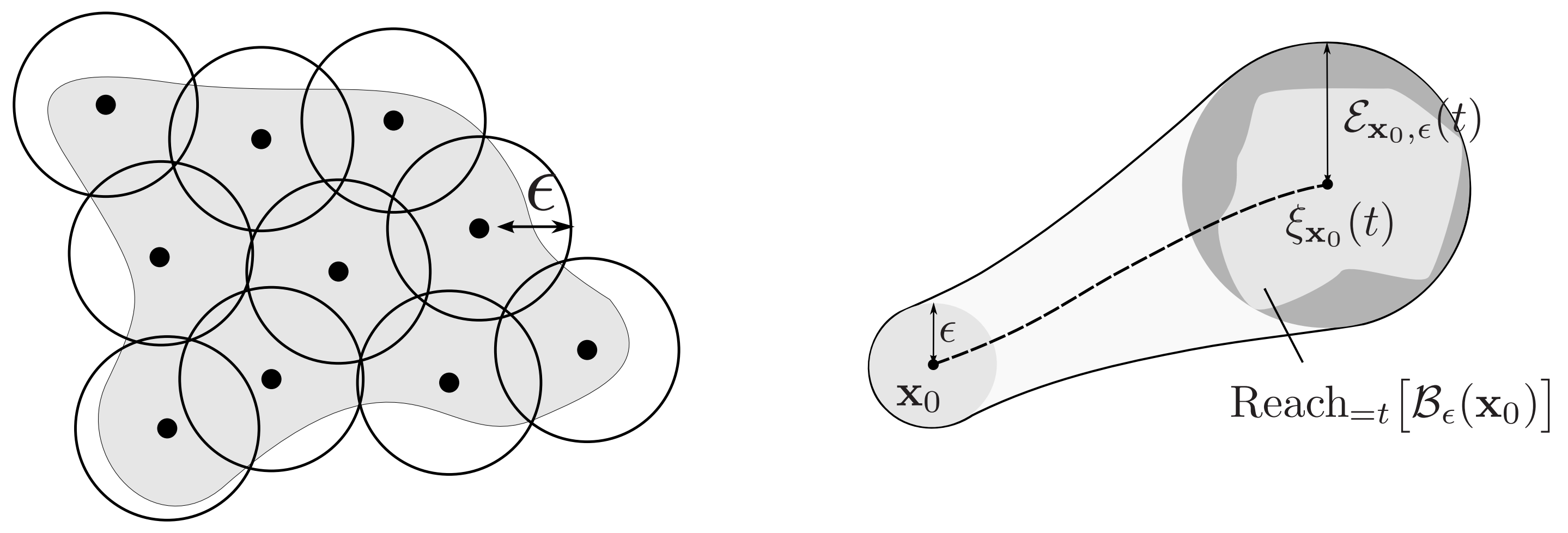

$\epsilon$
$\mathcal{E}_{\mathbf{x}_0,\epsilon}(t)$
$\xi_{\mathbf{x}_0}(t)$
$\epsilon$
$\mathbf{x}_0$
$\mathrm{Reach}_{=t}[\mathcal{B}_\epsilon(\mathbf{x}_0)]$

**Figure 3:** Left: a finite $\epsilon$-cover of the initial set of states. Right: trigger a simulation from each sample point $\mathbf{x}_0$, then a bloating of the simulated trajectory with a quantitative sensitivity argument thus pessimistically over-approximates the reachable set w.r.t. arbitrary initial states within $\mathcal{B}_\epsilon(\mathbf{x}_0)$.

## Validated Simulation

- We propose a local error bound

$$E(t) = \begin{cases} d_0, & \text{if } t = 0, \\ E(t_i) + (t - t_i)e_{i+1}, & \text{if } t \in [t_i, t_{i+1}]. \end{cases}$$

which yields the *validation property*

$$\xi_{\mathbf{x}_0}(t) \in \mathcal{B}_{E(t)}\left(\frac{(t-t_i)\mathbf{y}_i + (t_{i+1}-t)\mathbf{y}_{i+1}}{t_{i+1}-t_i}\right), \texttt{for each } t \in [t_i, t_{i+1}].$$

- Computing the bound by nonlinear optimization:

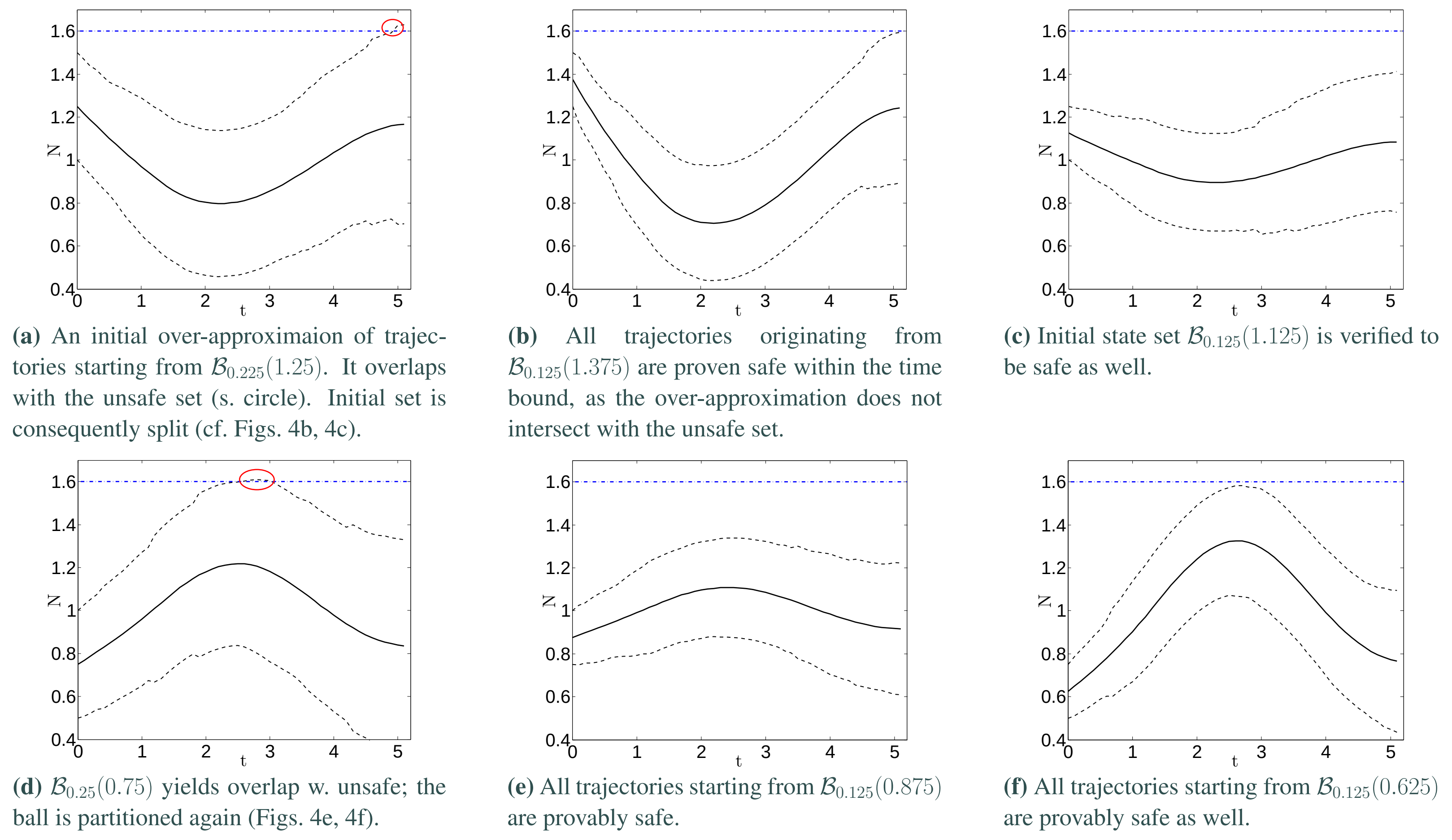
$$e_n = \textbf{Find} \text{ minimum } e \text{ s.t.} \begin{cases} \|\boldsymbol{f}(\mathbf{x} + t * \mathbf{f}, \mathbf{u} + t * \mathbf{g}) - \boldsymbol{f}(\mathbf{y}_n, \mathbf{y}_{n-m})\| \le e - \sigma, \text{ for} \\ \forall t \in [0, \tau] \\ \forall \mathbf{x} \in \mathcal{B}_{\mathbf{d}_n}(\mathbf{y}_n) \\ \forall \mathbf{u} \in \mathcal{B}_{\mathbf{d}_{n-m}}(\mathbf{y}_{n-m}) \\ \forall \mathbf{f} \in \mathcal{B}_e(\boldsymbol{f}(\mathbf{y}_n, \mathbf{y}_{n-m})) \\ \forall \mathbf{g} \in \mathcal{B}_{e_{n-m}}(\boldsymbol{f}(\mathbf{y}_{n-m}, \mathbf{y}_{n-2m})); \end{cases}$$

where $\tau$ is the variable stepsize, and $m$ is an offset s.t. $\mathbf{y}_{n-m}$ locates the delayed approximation at $t_n - r$. The optimization can be further solved by HySAT-II in a dually existential form.

- The simulation algorithm is proven sound and robustly complete.

## Experimental Results

1. Delayed Logistic Equation $\dot{N}(t) = N(t)[1 - N(t-r)]$:



**(a)** An initial over-approximaion of trajectories starting from $\mathcal{B}_{0.225}(1.25)$. It overlaps with the unsafe set (s. circle). Initial set is consequently split (cf. Figs. 4b, 4c).

**(b)** All trajectories originating from $\mathcal{B}_{0.125}(1.375)$ are proven safe within the time bound, as the over-approximation does not intersect with the unsafe set.

**(c)** Initial state set $\mathcal{B}_{0.125}(1.125)$ is verified to be safe as well.

**(d)** $\mathcal{B}_{0.25}(0.75)$ yields overlap w. unsafe; the ball is partitioned again (Figs. 4e, 4f).

**(e)** All trajectories starting from $\mathcal{B}_{0.125}(0.875)$ are provably safe.

**(f)** All trajectories starting from $\mathcal{B}_{0.125}(0.625)$ are provably safe as well.

**Figure 4:** The logistic system is proven safe through 6 rounds of simulation with base stepsize $\tau_0 = 0.1$. Delay $r = 1.3$, initial state set $\mathcal{X}_0 = \{N | N \in [0.5, 1.5]\}$, time bound $T = 5$s, unsafe set $\{N | N > 1.6\}$.

2. Delayed Microbial Growth $\dot{S}(t) = 1 - S(t) - f(S(t))x(t), \quad \dot{x}(t) = \mathrm{e}^{-r} f(S(t-r))x(t-r) - x(t)$:

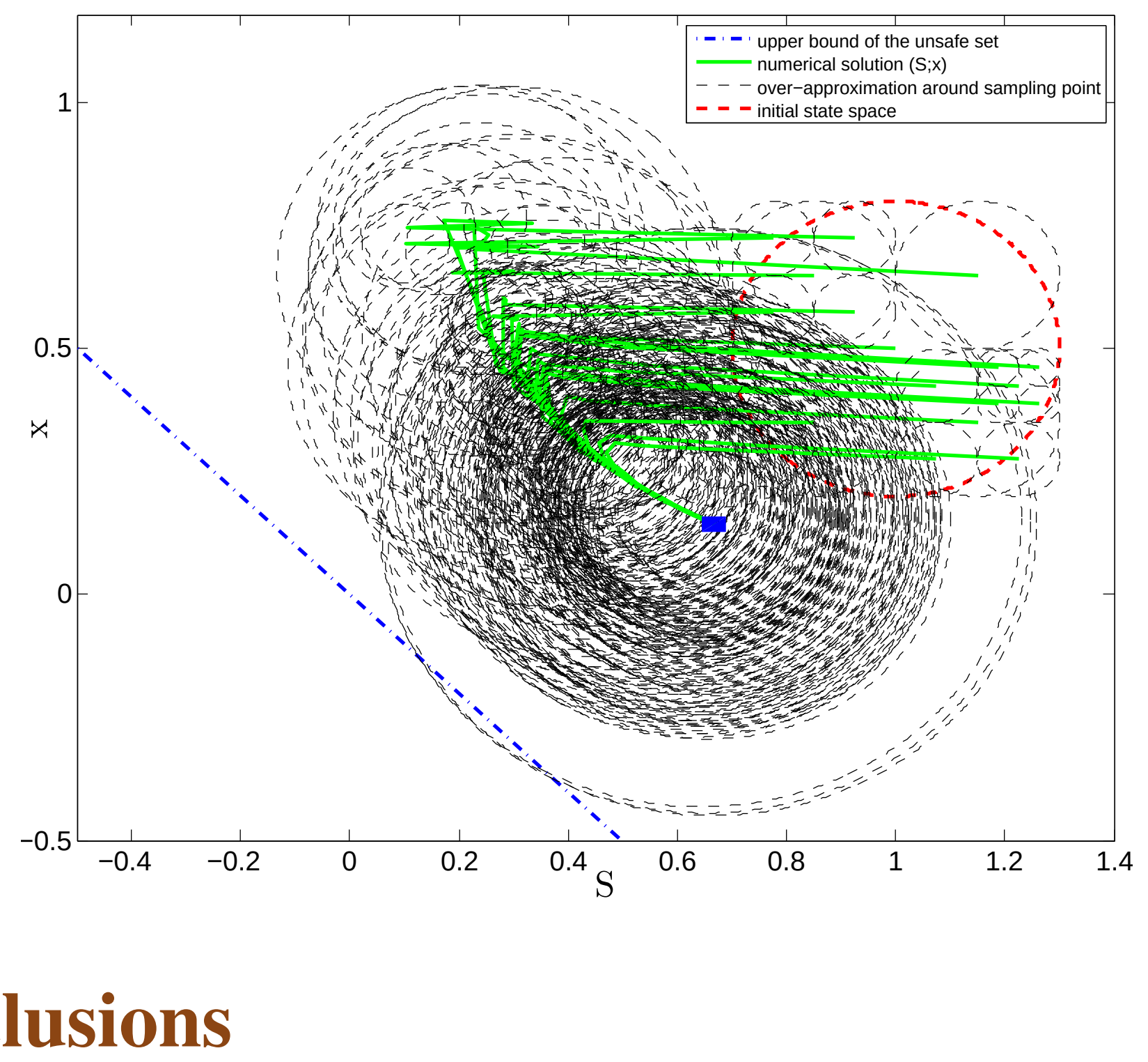


**Figure 5:** Here different rounds of simulation are depicted together in the phase space of $S$ and $x$. The system is proven safe by 17 rounds of simulation with $\tau_0 = 0.45$. The simulated trajectories start from within a cover of $\mathcal{X}_0$ (the red dashed circle on the right) and converge eventually to a *basin of attraction* (marked by a small blue rectangle). Here, $\alpha = 2\mathrm{e}$, $\beta = 1$, $r = 0.9$, $\mathcal{X}_0 = \mathcal{B}_{0.3}((1; 0.5))$, $\mathcal{U} = \{(S; x) | S + x < 0\}$, $T = 8$s.

## Conclusions

- An approach for automated formal verification of time-bounded reachability properties of a class of systems that feature delayed differential dynamics governed by DDEs with multiple delays.
- A prototypical implementation of a validated solver for DDEs, by which we have successfully demonstrated the method on several benchmark systems involving delayed differential dynamics.

## References

[1] Alexandre Donzé and Oded Maler. Systematic simulation using sensitivity analysis. In *Hybrid Systems: Computation and Control*, pages 174–189. Springer, 2007.

[2] Parasara Sridhar Duggirala, Sayan Mitra, and Mahesh Viswanathan. Verification of annotated models from executions. In *Proceedings of the Eleventh ACM International Conference on Embedded Software*, page 26. IEEE Press, 2013.

[3] Antoine Girard and George J. Pappas. Approximate bisimulation: A bridge between computer science and control theory. *European Journal of Control*, 17(5–6):568–578, 2011.

[4] Tarik Nahhal and Thao Dang. Test coverage for continuous and hybrid systems. In *CAV 2007*, volume 4590 of *Lecture Notes in Computer Science*, pages 449–462. Springer, 2007.