中国科学院软件研究所学术年会'2020
暨计算机科学国家重点实验室开放周

学术论文

# Unbounded-Time Safety Verification of Stochastic Differential Dynamics◇
# 随机微分系统的无穷时间安全性验证

**Shenghua Feng[1,2,*], Mingshuai Chen[3], Bai Xue[1,2], Sriram Sankaranarayanan[4], Naijun Zhan[1,2]**

[1]SKLCS, Institute of Software, CAS, Beijing, China
[2]University of Chinese Academy of Sciences, Beijing, China
[3]Lehrstuhl für Informatik 2, RWTH Aachen University, Aachen, Germany
[4]University of Colorado, Boulder, USA
*Contact: fengsh@ios.ac.cn ◇: To be appeared in CAV'20

## Introduction

We propose a method for bounding the probability that a stochastic differential equation (SDE) system violates a safety specification over the infinite time horizon. SDEs are mathematical models of stochastic processes that capture how states evolve continuously in time. They are widely used in numerous applications such as engineered systems (e.g., modeling how pedestrians move in an intersection), computational finance (e.g., modeling stock option prices), and ecological processes (e.g., population change over time).

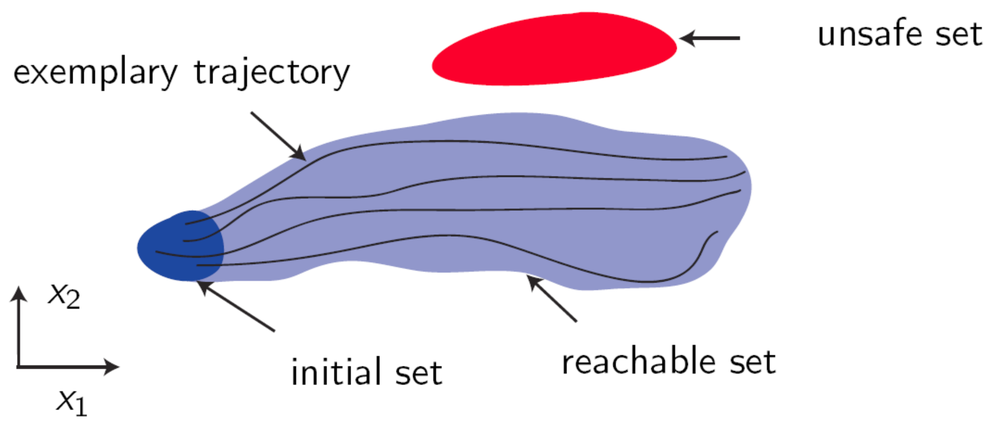


Figure 1. Visual illustration of safety verification problem. A reduction based approach is presented to bound the unsafe probability w.r.t. a stochastic system.

Previously the safety verification problem has been tackled over finite and infinite time horizons using a diverse set of approaches. The approach in this paper attempts to connect the two views by first identifying a finite time bound, beyond which the probability of a safety violation can be bounded by a negligibly small number. This is achieved by discovering an exponential barrier certificate that proves exponentially converging bounds on the probability of safety violations over time. Once the finite time interval is found, a finite-time verification approach is used to bound the probability of violation over this interval.

*keywords: Stochastic Differential Equations (SDEs), Unbounded safety verification, Failure probability bound, Barrier certificates.*

## METHODOLOGY

Observe that for any $0 \leq T < \infty$,

$$P(\exists t \geq 0\colon \tilde{X}_t \in \mathcal{X}_u) \leq P(\exists t \in [0,T]\colon \tilde{X}_t \in \mathcal{X}_u) + P(\exists t \geq T\colon \tilde{X}_t \in \mathcal{X}_u)$$

Our approach consists of three parts:

1. Bounding $P(\exists t \geq T\colon \tilde{X}_t \in \mathcal{X}_u)$ by a exponential decreasing function of $T$.
2. Bounding $P(\exists t \in [0,T]\colon \tilde{X}_t \in \mathcal{X}_u)$ by a time-dependent barrier certificate.
3. Choosing $T$ and summing the above two bound, we can obtain the total bound.

The generation of a exponential decreasing bound boils down to a semi-definite programming (SDP) [1]:

$$\begin{aligned}
\underset{a,\alpha}{\texttt{minimize}} \quad & \alpha \\
\texttt{subject to} \quad & V^a(\mathbf{x}) \geq \mathbf{0} \quad \text{for } \mathbf{x} \in \mathcal{X} \\
& \mathcal{A}V^a(\mathbf{x}) \leq -\Lambda V^a(\mathbf{x}) \quad \text{for } \mathbf{x} \in \mathcal{X} \\
& \Lambda V^a(\mathbf{x}) \leq \mathbf{0} \quad \text{for } \mathbf{x} \in \partial\mathcal{X} \\
& V^a(\mathbf{x}) \geq \mathbf{1} \quad \text{for } \mathbf{x} \in \mathcal{X}_u \\
& V^a(\mathbf{x}) \leq \alpha\mathbf{1} \quad \text{for } \mathbf{x} \in \mathcal{X}_0
\end{aligned}$$

Similarly, bounding the finite time unsafe probability reduce to solve the following SDP:

$$\begin{aligned}
\underset{b,\beta}{\texttt{minimize}} \quad & \beta \\
\texttt{subject to} \quad & H^b(t,\mathbf{x}) \geq 0 \quad \text{for } (t,\mathbf{x}) \in [0,T] \times \mathcal{X} \\
& \mathcal{A}H^b(t,\mathbf{x}) \leq 0 \quad \text{for } (t,\mathbf{x}) \in [0,T] \times (\mathcal{X} \setminus \mathcal{X}_u) \\
& \frac{\partial H^b}{\partial t} \leq 0 \quad \text{for } (t,\mathbf{x}) \in [0,T] \times \partial\mathcal{X}] \\
& H^b(t,\mathbf{x}) \geq 1 \quad \text{for } (t,\mathbf{x}) \in [0,T] \times \mathcal{X}_u \\
& H^b(0,\mathbf{x}) \leq \beta \quad \text{for } \mathbf{x} \in \mathcal{X}_0
\end{aligned}$$

For different $T$, solving the corresponding SDP, we can finally obtain the unsafe probability over infinite time horizon.

## Experiments

**Example 1 (Population growth)** *Consider the stochastic system*

$$\mathrm{d}X_t = b(X_t)\,\mathrm{d}t + \sigma(X_t)\,\mathrm{d}W_t,$$

*Suppose that the state space is restricted within $\mathcal{X} = \{\mathbf{x} \mid \mathbf{x} \geq 0\}$ with $b(X_t) = -X_t$ and $\sigma(X_t) = \sqrt{2}/2X_t$. We instantiate the $\infty$-safety problem as $\mathcal{X}_0 = \{\mathbf{x} \mid \mathbf{x} = 1\}$ and $\mathcal{X}_u = \{\mathbf{x} \mid \mathbf{x} \geq 2\}$, namely, we expect that the population does not diverge beyond 2.*

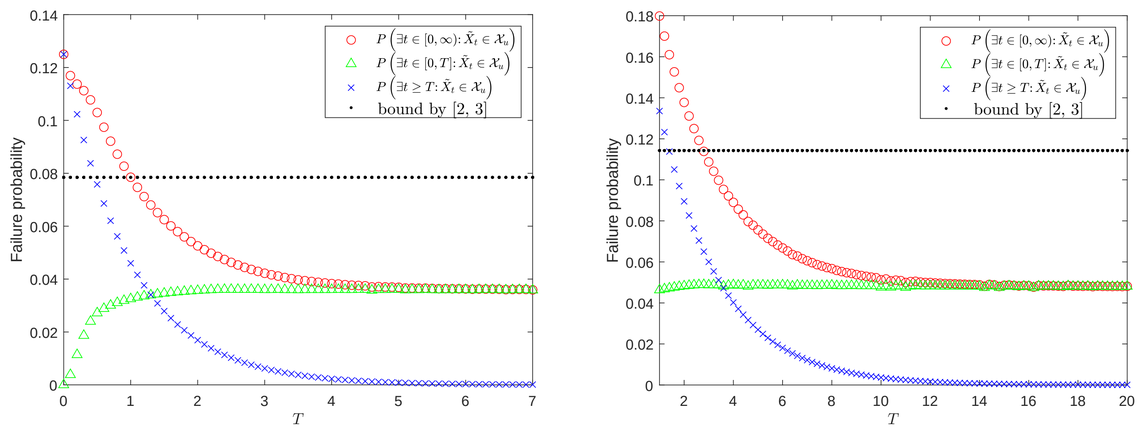


Figure 2. Different choices of $T$ lead to different bounds on the failure probability (with the time-dependent stochastic barrier certificates of degree 4). Note that '○' = '×' + '△' and '•' depicts the overall bound on the failure probability produced by the method in [2, 3].

**Example 2 (Harmonic oscillator)** *Consider a two-dimensional harmonic oscillator with noisy damping:*

$$\mathrm{d}X_t = \begin{pmatrix} 0 & \omega \\ -\omega & -k \end{pmatrix} X_t\,\mathrm{d}t + \begin{pmatrix} 0 & 0 \\ 0 & -\sigma \end{pmatrix} X_t\,\mathrm{d}W_t,$$

*with constants $\omega = 1, k = 7$ and $\sigma = 2$. We instantiate the $\infty$-safety problem as $\mathcal{X} = \mathbb{R}^n$, $\mathcal{X}_0 = \{(x_1,x_2) \mid -1.2 \leq x_1 \leq 0.8, -0.6 \leq x_2 \leq 0.4\}$ and $\mathcal{X}_u = \{(x_1,x_2) \mid |x_1| \geq 2\}$.*

## Reference

[1] Pablo A Parillo. Semidefinite programming relaxation for semialgebraic problems. *Mathematical Programming Ser. B*, 96(2):293–320, 2003.

[2] Stephen Prajna, Ali Jadbabaie, and George J Pappas. Stochastic safety verification using barrier certificates. In *CDC'04*, volume 1, pages 929–934. IEEE, 2004.

[3] Stephen Prajna, Ali Jadbabaie, and George J. Pappas. A framework for worst-case and stochastic safety verification using barrier certificates. *IEEE Trans. Automat. Contr.*, 52(8):1415–1428, 2007.