Correct-By-Construction Barrier Certificate Synthesis for Safety Verification of Continuous Dynamical Systems

Promit Panja André Platzer

Karlsruhe Institute of Technology
{*promit.panja, andre.platzer*}*@kit.edu*

12.12.2025

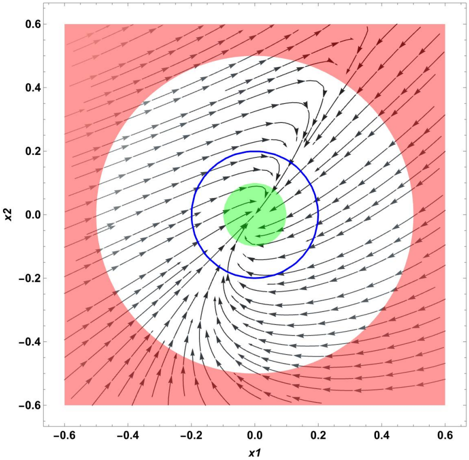
Introduction

$$Init \rightarrow [(\mathrm{Ctrl}; \textcolor{blue}{\mathrm{ODEs}})^*]Safe$$

The key to establishing the safety of a cyber-physical system for an unbounded time horizon are **invariants**.

Introduction

Barrier Certificates (BCs) are a class of **differential invariants** witnessing the safety of *continuous* and *hybrid dynamical systems*.



$x \in \mathcal{X} \subseteq \mathbb{R}^n$

$f : \mathbb{R}^n \to \mathbb{R}^n$

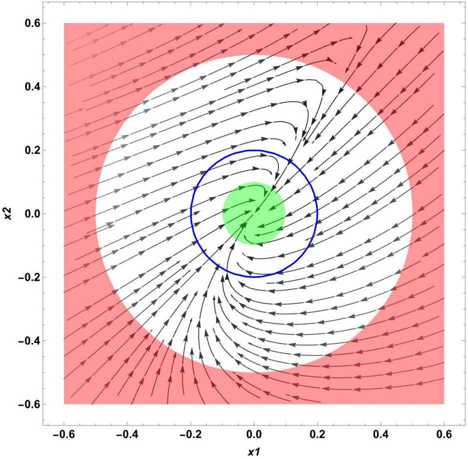
$$x' = f(x)$$

Set of **initial** states: $\mathcal{X}_I \subseteq \mathcal{X}$

Set of **unsafe** states: $\mathcal{X}_U \subseteq \mathcal{X}$

Introduction

In this paper we focus on *Barrier Certificates (BCs)* **witnessing** safety of **continuous dynamical systems**.



$x \in \mathbb{R}^n, f : \mathbb{R}^n \to \mathbb{R}^n$

$$x' = f(x)$$

$B : \mathbb{R}^n \to \mathbb{R}$, for some fixed $\lambda \in \mathbb{R}$

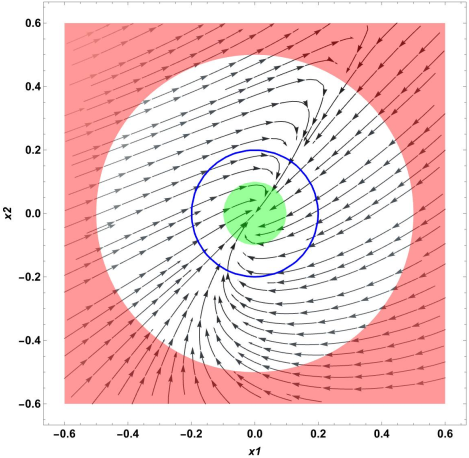
$$B(x) \leq 0 \quad \forall x \in \mathcal{X}_I$$

$$B(x) > 0 \quad \forall x \in \mathcal{X}_U$$

$$L_f B(x) \leq \lambda B(x) \quad \forall x \in \mathcal{X}$$

Introduction

For a template polynomial $B(x, \gamma) = \sum_i^n \gamma_i b_i(x), \gamma \in \mathbb{Q}$.



- Can be searched efficiently using *Sum-of-Squares (SOS)* decomposition and *Semidefinite Programming (SDP)*.
- Numerical SDP solvers using interior-point methods have *polynomial* time worst-case complexity.

Problem: Validity of BCs

Numerical Errors

Small round-off errors in numerical solvers may lead to invalid invariants.

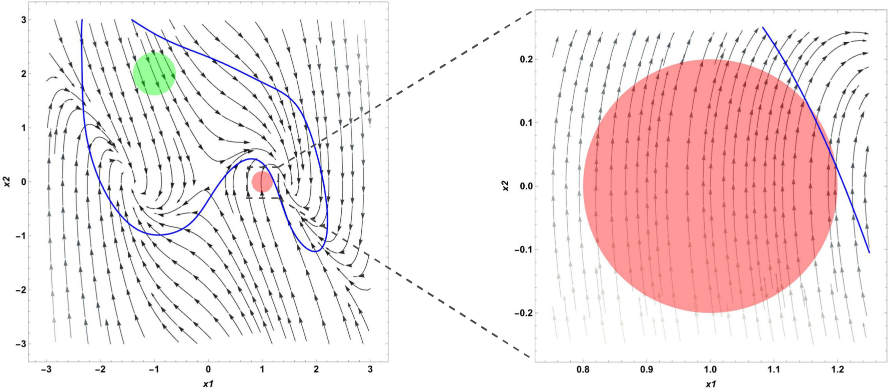


Figure: An invalid BC synthesized using SDP.

Problem: Validity of BCs

- Trusting a BC requires an independent post-synthesis verification using **Quantifier Elimination**.
- Of course, the entire the BC synthesis is pointless if the subsequent verification **fails** or symbolic real arithmetic decision procedures **time out**.

Possible Solution: Witness Driven Verification

- Find a *real arithmetic* **witness** for the synthesized BC.
- The **witness** proves the validity of the BC **witnessing** safety.
- In other words, find a ”**witness** of a **witness**”.

Decision Procedure (Real Nullstellensatz)

- The Real Nullstellensatz enables a *complete* proof method for the universal fragment of real arithmetic.
- A given set of **equations** $\{g_1(x) = 0, g_2(x) = 0, \ldots, g_i(x) = 0\}$ **do not** have a common solution *iff* there exists a polynomial of the form $1 + \varphi_1^2 + \varphi_2^2 + \cdots + \varphi_m^2$ contained in the ideal generated by the set.
- Given a *candidate* witness it is sufficient to prove its membership in the ideal generated by the system of polynomial equations i.e., show $1 + \varphi_1^2 + \varphi_2^2 + \cdots + \varphi_m^2 \in (G)$.

Decision Procedure

Find the witness $1 + \varphi_1^2 + \varphi_2^2 + \cdots + \varphi_m^2$ for Real Nullstellensatz.

Decision Procedure (Gröbner Bases)

- Gröbner bases provide a sound and efficient method for proving ideal membership.
- $1 + \varphi_1^2 + \varphi_2^2 + \cdots + \varphi_m^2 \in (G)$ is equivalent to $\mathrm{red}_G(1 + \varphi_1^2 + \varphi_2^2 + \cdots + \varphi_m^2) = 0$, where G is a Gröbner basis.
- $1 + \underbrace{\varphi_1^2 + \varphi_2^2 + \cdots + \varphi_m^2}_{SOS} \equiv 1 + p^T Qp$
- Compute $\mathrm{red}_G(1 + p^T Qp) = 0$, for **linear constraints** in Q

Decision Procedure

Find Q by encoding $\mathrm{red}_G(1 + p^T Qp) = 0$ in an SDP.

Synthesis and Decision Procedure

1. Solve an **SOS program** for BC synthesis.
2. Take the synthesized BC then solve *another* **SOS program** for finding the real arithmetic witness.

Intuition

Can we exploit the SOS structure of the BC constraints and the real arithmetic witness?

Correct-by-Construction BCs

- We present a new framework for synthesizing a **valid BC** and its **witness of validity**.
- Both can be found by solving a **single** SOS optimization program.

Combined Procedure

BC Constraints $+$ Real Arithmetic Witness Constraints.

Symbolic Witness Construction

- For a template polynomial $B(x,\gamma) = \sum_i^n \gamma_i b_i(x)$.
- We write the negation of the BC conditions and encode them into equations by introducing fresh variables s_1, s_2, s_3

$$(B(x,\gamma) + \sigma_1(x)g_I(x))s_1^2 = 1 \tag{1a}$$

$$B(x,\gamma) - \sigma_2(x)g_U(x) - \epsilon = s_2^2 \tag{1b}$$

$$-L_f B(x,\gamma) + \lambda B(x,\gamma) - \sigma_3(x)g_D(x) = s_3^2. \tag{1c}$$

Symbolic Witness Construction

- Next we construct the Gröbner basis for the corresponding system of equations

$$
\begin{aligned}
f_1 &= (B(x,\gamma) + \sigma_1(x) g_I(x)) s_1^2 - 1 = 0 \\
f_2 &= B(x,\gamma) - \sigma_2(x) g_U(x) - \epsilon - s_2^2 = 0 \\
f_3 &= -L_f B(x,\gamma) + \lambda B(x,\gamma) - \sigma_3(x) g_D(x) - s_3^2 = 0.
\end{aligned}
$$

- For a fixed term ordering $s_1 \succ s_2 \succ s_3 \succ x_1 \succ x_2 \succ \ldots$ is already a Gröbner basis.

$$G = \{f_1, f_2, f_3\}. \tag{2}$$

- Compute $\mathrm{red}_G(1 + p^T Q p) = 0$, for linear constraints in Q.

Monomial Basis Selection for $p^T Qp$

- Take a closer look at the first Gröbner base

$$f_1 = (B(x,\gamma) + \sigma_1(x) g_l(x)) s_1^2 - 1,$$

- We can rewrite it in this from

$$1 + s_1^2 (\underbrace{-B(x,\gamma) - \sigma_1(x) g_l(x)}_{\text{SOS}}).$$

- We can exploit this SOS structure

$$1 + s_1^2 P(x,\gamma), \;\; \text{where} \;\; P(x,\gamma) = -B(x,\gamma) - \sigma_1(x) g_l(x),$$

$$1 + p^T Qp = 1 + s_1^2 P(x,\gamma)$$

- p must be chosen such that it includes s_1 times all the standard monomials up to a degree d of $P(x,\gamma)$ such that $p^T Qp$ can express every monomial appearing in the expansion of the right-hand side.

Combined Procedure

Combined SOS Program

BC constraints + Witness constraints

$$
\begin{aligned}
\text{find} \quad & \gamma, Q \\
\text{subject to} \quad & -B(x,\gamma) - \sigma_1(x) g_I(x) \geq 0 \\
& B(x,\gamma) - \sigma_2(x) g_U(x) - \epsilon \geq 0 \\
& -L_f B(x,\gamma) + \lambda B(x,\gamma) - \sigma_3(x) g_D(x) \geq 0 \\
& \mathrm{red}_G(1 + p^T Q p) = 0 \\
& Q \succeq 0.
\end{aligned} \tag{3}
$$

The existence of a solution that *satisfies the constraints* will **guarantee** the existence of a valid BC $B(x)$ and its witness of validity $1 + p^T Qp$.

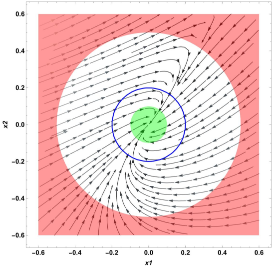
Handling Floating-Point Inaccuracies

Rationalize the parameters

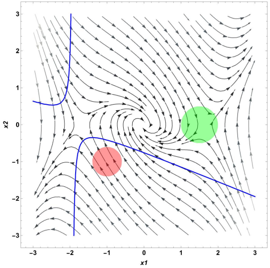
One important step is rationalizing the values of the parameters because of often occurring floating-point inaccuracies in numerical SDP solvers.

1. Rationalize the entries of matrix Q.
2. Check for semidefiniteness of the resulting matrix, $Q \succeq 0$.

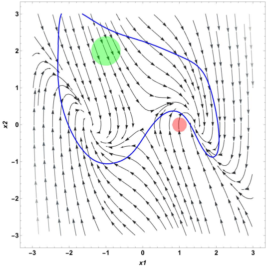
Experimental Results



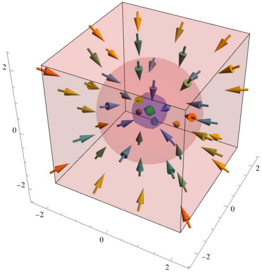
(a) Example 1



(b) Example 2



(c) Example 3



(d) Example 4

Figure: The region shaded red represents the set of unsafe states $\mathcal{X}_U$, the region shaded green represents the set of initial states $\mathcal{X}_I$, and the solid blue line (translucent blue surface in Example 4) represents the zero level set $B(x) = 0$ of the found valid BC $B(x)$.

Conclusion

- Correctness is extremely important when synthesizing invariants for safety proofs.
- A misleading safety witness that, in fact, does not imply safety is not useful.

- We presented a **combined framework** that unifies the barrier certificate synthesis with the real algebraic witness synthesis.
- Combining Gröbner bases and SDP for the Real Nullstellensatz proving the validity of the resulting barrier certificate makes it **correct-by-construction**.