AUTOMATIC COMPUTATION OF BARRIER CERTIFICATES

Safety Verification for Hybrid Systems

Rémy Seassau, Frédéric Marcel Tchouli

November 27, 2022

INTRODUCTION

- Motivation for the Safety Verification Research Project
  - Safety verification is Very critical for cyber-physical systems!!
    (eg. autonomous automobile systems, automatic pilots)
  - However: Difficult to compute the exact space of reachable states in general
  - Barrier Certificates initially introduced by Prajna and Jadbabaie (2004)
    in the context of hybrid systems.

PROBLEM DEFINITION

Given a system of ODEs $x' = f(x)$ with evolution domain constraint $\mathcal{X} \subseteq \mathbb{R}^n$, and the sets $\mathcal{X}_0 \subseteq \mathbb{R}^n$, $\mathcal{X}_\mathrm{u} \subseteq \mathbb{R}^n$ of initial and unsafe states, respectively, the system is said to be safe if and only if:

$$\forall \mathbf{x}_0 \in \mathcal{X}_0,\, \forall t \geq 0 : ((\forall \tau \in [0,t].\boldsymbol{x}\left(\boldsymbol{x}_0, \tau\right) \in \mathcal{X}) \Rightarrow \boldsymbol{x}\left(\boldsymbol{x}_0, t\right) \notin \mathcal{X}_\mathrm{u}).$$

We say that the set $I \subseteq \mathbb{R}^n$ is a continuous invariant iff the following statement holds:

$$\forall \mathbf{x}_0 \in I,\, \forall t \geq 0 : ((\forall \tau \in [0,t] : \mathbf{x}\left(\mathbf{x}_0, \tau\right) \in \mathcal{X}) \Longrightarrow \mathbf{x}\left(\mathbf{x}_0, t\right) \in I)\,.$$

BARRIER CERTIFICATES

Barrier Certificates are a type of continuous invariant that allow us to verify the safety of a system.

They have several advantages:

- Don't require the computation of the reachable sets
- Can guarantee safety of nonlinear continuous dynamical systems
- If a system is safe, a barrier certificate is guaranteed to exists [2]

Unfortunately, we do not know that if a barrier certificate exists then we can automatically find it.

STRICT BARRIER

We define a strict barrier certificate as a function B on the state space $\mathcal{X}$ with the following properties:

$$x(t) \in \mathcal{X}_{\mathrm{u}} \implies B(x) > 0 \tag{1}$$

$$x(t) \in \mathcal{X}_0 \implies B(x) \leq 0 \tag{2}$$

$$B(x(t)) = 0 \implies \frac{\partial B}{\partial x} f(x) \leq 0 \tag{3}$$

The last condition can be interpreted as the derivative of a real function being negative, implying that the function is decreasing.

STRICT BARRIER

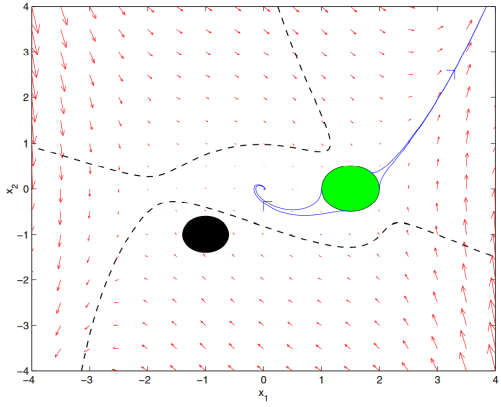

Figure: Phase portrait of a dynamical system equipped a barrier [1]

QUANTIFIER ELIMINATION

Quantifier Elimination: Goes from a quantified first-order logic formula to an equivalent formula that is quantifier-free.

How we use it: Create a template for the barrier where the coefficients are quantified.

Example: Consider $B(x) = ax^2 + bx$, condition (1) where $x \in \mathcal{X}_{\mathrm{u}} \implies B(x) > 0$ becomes

$$(\exists a, b) : x \in \mathcal{X}_{\mathrm{u}} \implies ax^2 + bx > 0$$

George Collins and Hoon Hong (1991) then provide a doubly exponential-time QE algorithm which (is optimal and) yields the complete set of possible Barrier Certificates.

CONVEX BARRIER

The convex barrier certificate generalizes the strict barrier certificate by strengthening condition (3). Specifically, we remove the condition that $B(x) = 0$:

$$B(x) = 0 \implies \frac{\partial B}{\partial x} f(x) \leq 0 \quad \longrightarrow \quad \frac{\partial B}{\partial x} f(x) \leq 0 \tag{4}$$

This barrier has the interesting property that it is convex (hence the name) which implies that we can compute it using numerical convex solvers.

SUM OF SQUARES

Sum of Squares optimization is a method that seeks to show that a give quantified function is a sum of functions squared, i.e.

$$f(x) = \sum_{i=1}^{n} f_i(x)^2$$

For example, consider the following function of x and y:

$$x^2 - 4xy + 7y^2 = (x - 2y)^2 + (\sqrt{3}y)^2$$

The fact that we use for encoding our barrier certificate computation is that if f is SOS, then necessarily $f(x) \geq 0$ for all x.

SUM OF SQUARES

If $\mathcal{X}_0 = \bigwedge_{i=1}^{N} p_i < 0$ and $\mathcal{X}_\mu = \bigwedge_{j=1}^{M} q_j < 0$ are semi-algebraic.
If $p_{\mathrm{a},d}$ is our template, $\varepsilon > 0$ is a small positive constant and $\sigma_{p_{i,j}}, \sigma_{q_{k,l}}$ are template SOS polynomials such that:

$$-p_{\mathrm{a},d} - \sum_{i,j} \sigma_{p_{i,j}} p_{i,j} \geq 0$$

$$p_{\mathrm{a},d} - \sum_{k,l} \sigma_{q_{k,l}} q_{k,l} - \varepsilon \geq 0$$

$$-\left(p_{\mathrm{a},d}\right)' \geq 0$$

Then the exponential type conditions are satisfied

The convex optimizers proceed similarly to the quantifier elimination solvers in the sense that we need to provide a template as input. Here however, the solver is numerical which can sometimes lead to incorrect solutions.

EXPONENTIAL BARRIER

The exponential barrier is a generalization of the convex barrier certificate. Specifically, let $\lambda \in \mathbb{R}$, we then replace condition (4):

$$\frac{\partial B}{\partial x} f(x) \leq 0 \quad \longrightarrow \quad \frac{\partial B}{\partial x} f(x) - \lambda B(x) \leq 0 \tag{5}$$

Notice that both certificates are equal when $\lambda = 0$.

The advantage of the exponential barrier is that it is less conservative than the C.B., but it is also convex. This means we can also use SOS to compute exponential barriers.

COMPUTING THE EXPONENTIAL BARRIER

We just need minor adjustments to the previous computations techniques to try and generate exponential barriers.

Quantifier Elimination: Here, we only need to replace the previous condition on the derivative with the new condition and to add λ to the quantifiers.

Sum Of Squares: For sum of squares, we use the same logic as for the convex barrier, applied to the whole of $\frac{\partial B}{\partial x} f(x) - \lambda B(x)$.

FURTHER TOPICS

- Testing the computation of different barrier types
- Heuristics of barrier template degree selection
- Exploration of a weaker exponential barrier

REFERENCES

[1] S. Prajna and A. Jadbabaie.
Safety verification of hybrid systems using barrier certificates.
In R. Alur and G. J. Pappas, editors, *Hybrid Systems: Computation and Control*, pages 477–492, Berlin, Heidelberg, 2004. Springer Berlin Heidelberg.

[2] S. Ratschan.
A robust finite-time converse theorem for inductive safety certificates of ordinary differential equations.
CoRR, abs/1701.03948, 2017.