Software Engineering Group
Department of Computer Science
Nanjing University
http://seg.nju.edu.cn

Technical Report No. NJU-SEG-2016-IW-001

2016-IW-001

Darboux-type Barrier Certificates for Safety Verification of Nonlinear Hybrid Systems

Xia Zeng, Wang Lin, Zhengfeng Yang, Xin Chen, Lilei Wang

EMSOFT 2016

Darboux-type Barrier Certificates for Safety Verification of Nonlinear Hybrid Systems [*]

Xia Zeng
Shanghai Key Laboratory of Trustworthy Computing
East China Normal University, Shanghai 200062, China
xzeng@ecnu.cn

Wang Lin
Key Laboratory of Mathematics Mechanization
AMSS, Beijing 100190, China
linwang@wzu.edu.cn

Zhengfeng Yang [†]
Shanghai Key Laboratory of Trustworthy Computing
East China Normal University, Shanghai 200062, China
zfyang@sei.ecnu.edu.cn

Xin Chen
State Key Laboratory for Novel Software Technology
Nanjing University, Jiangsu 210032, China
chenxin@nju.edu.cn

Lilei Wang
Shanghai Key Laboratory of Trustworthy Computing
East China Normal University, Shanghai 200062, China
llwang@stu.ecnu.edu.cn

ABSTRACT

Benefit from less computational difficulty, barrier certificate based method has attracted much attention in safety verification of hybrid systems. Barrier certificates are inherent existences of a hybrid system and may have different types. A set of well-defined verification conditions is a prerequisite for successfully identifying barrier certificates of a specific type. Therefore, how to define verification conditions that can identify barrier certificates invisible to existing conditions becomes an essential problem in barrier certificate based verification. This paper proposes a set of verification conditions that helps to construct a new type of barrier certificate, namely, the Darboux-type barrier certificate made of Darboux polynomial. The proposed verification conditions provide powerful aids in non-linear hybrid system verification as the Darboux-type barrier certificates can verify systems that may not be settled by existing verification conditions.

Furthermore, we give a novel computational approach, combining the sampling-based relaxation method with least-squares and quadratic programming (LS-QP) alternating projection, to find Darboux-type barrier certificates. We demonstrate on the benchmark examples from the literature that our verification conditions can enhance the capability of barrier certificate based approaches through successfully verifying those systems that are difficult to be handled by existing verification conditions, and our algorithm is efficient.

CCS Concepts

•Software and its engineering → Formal software verification; •Computing methodologies → Optimization algorithms;

Keywords

Safety verification; Hybrid systems; Darboux polynomial; Barrier certificate; Polynomial optimization

1. INTRODUCTION

Hybrid systems are dynamical systems governed by interacting discrete and continuous dynamics. They are widely used to modelling embedded systems consisting of computational and physical elements. Many safety-critical systems, e.g., aircrafts, automobiles, chemicals and nuclear power plants, and biological systems, operate semantically as nonlinear hybrid systems. The safety issues of those systems can be checked by safety verification of their models, i.e., examining whether the systems will reach a dangerous or unwanted configuration. Due to the intrinsic complexity, verification of hybrid systems presents a challenging problem.

Explicit computation of reachable sets is crucial for safety verification of hybrid systems. However, this kind of approach requires knowing the exact solution of the differential equations, thus its scalability is very restricted. Due to its less computational difficulty than reachable set computation, barrier certificate computation has attracted much attention [23, 15, 28]. A barrier certificate is a function of state that divides the state space into two parts. All system trajectories starting from a given set of initial conditions fall into one side of the barrier certificate while the unsafe re-

[*] This material is supported in part by the National Natural Science Foundation of China under Grants 61321064, 61361136002, 11471209, 11571350 and 61561146394, the Innovation Program of Shanghai Municipal Education Commission under Grant 14ZZ046, Project on the Integration of Industry, Education and Research of Jiangsu Province under Grant BY2014126-03. We would like to thank anonymous reviewers for their very valuable comments.

[†] Corresponding author

EMSOFT'16, October 01-07, 2016, Pittsburgh, PA, USA
© 2016 ACM. ISBN 978-1-4503-4485-2/16/10…$15.00
DOI: http://dx.doi.org/10.1145/2968478.2968484

gion locates on the other side. Compared with reachable set computation, a barrier function is much easier to compute, when encountering nonlinear systems. For a hybrid system, its barrier certificates are inherent existences and there may be many barrier certificates of different types.

A barrier certificate is identified as follows: first, predefine a set of verification conditions that corresponds to a specific type of barrier certificate; then, encode those conditions into some constraints on state variables and coefficients where the unknown coefficients are existentially quantified and state variables are universally quantified; finally, solve the quantifier-equipped constraints. A set of well-defined verification conditions is a prerequisite for success in catching barrier certificates of a specific type. Therefore, how to define new verification conditions of barrier certificates that are different from existing types to enrich the spectrum of computable barrier certificates is an essential problem in barrier certificate based verification.

This paper proposes a set of verification conditions that can build a new type of barrier certificate: the Darboux-type barrier certificate made of Darboux polynomial. Compared with existing barrier certificate which gives a rough over approximation of the reachable set, a Darboux-type barrier certificate gives a more precise characterization of trajectories of the system by ensuring that once a trajectory of the system enters the algebraic curve defined by the Darboux polynomials, it will never leave the curve afterwards. By catching Darboux-type barrier certificates, the proposed verification conditions provide an effective approach for verifying non-linear hybrid systems that may not be settled by existing verification conditions.

Specifically, the Darboux-type barrier certificate generation is addressed in two phases. In the first phase, we define a new barrier certificate, based on the concept of Darboux polynomials from computer algebra. Darboux polynomials indicate the invariant algebraic curves of continuous systems. Our method is based on adapting Darboux polynomials to provide a new barrier certificate that guarantees safety property of a semi-algebraic hybrid system. This key distinguishing feature of Darboux polynomials provides a new encoding to compute barrier certificates, thus guarantees that our method can yield barrier certificates that SOS relaxation is unable to produce (See Table 1). In the second phase, we propose a novel computational approach by utilizing the feature in the problem of Darboux-type barrier certificate generation. Concretely, a sampling-based method is applied to relax the problem of computing Darboux-type barrier certificates as a polynomial optimization problem with quadratic equalities and linear inequalities, which can subsequently be solved by applying a least-squares (LS) and quadratic programming (QP) alternating projection method. The benchmark examples from the literature show the efficiency of our algorithm.

The main contributions of this paper are summarized as follows: 1. We define a new barrier certificate based on adapting Darboux polynomials, which can be used to describe the inherent invariance property of the systems. 2. As an alternative to quantifier elimination or methods based on SOS relaxation, we suggest a new computational approach, combined with the sampling-based relaxation method and LS-QP alternating projection, to compute Darboux-type barrier certificates efficiently. 3. We provide a detailed experimental evaluation on a set of benchmarks, which shows the efficiency and practicability of our method.

The rest of this paper is organized as follows. We introduce some related notations about hybrid system and Darboux polynomial in Section 2. We define a new type of barrier certificate, based on Darboux polynomial, to verify the safety property of hybrid systems in Section 3. We transfer the problem of generating Darboux-type barrier certificates to a polynomial optimization problem in Section 4, and suggest a new computational method for solving this optimization problem in Section 5. Experiments on some benchmarks are shown to illustrate our method for computing Darboux-type barrier certificates in Section 6 before concluding.

1.1 Related work

The seminal works of using barrier certificates in safety verification of hybrid systems were proposed by Prajna et al. in [22, 23]. Following their line, H. Kong et al. [16, 15] proposed a barrier certificate defined over an exponential condition for semi-algebraic hybrid systems. L. Dai et al. [6] discussed how to relax the condition of barrier certificates in a general way without losing their convexity. Kapinski et al. [14, 13] presented a Lyapunov-based barrier certificate, which is more conservative but tractable than that proposed by Prajna. In [28], Sloth et al. proposed a new barrier certificate for a special class of hybrid systems consisting of many interconnected subsystems. Compared with the existing barrier certificate which defines a region acting as the over-approximation of the reachable set, our Darboux-type barrier certificate characterizes an algebraic curve that restricts the trajectories of the system from leaving it once they enter it.

Darboux-type invariants have been introduced for safety verification as well. M.Zaki [32, 33] suggested using Darboux-type invariants in safety verification of continuous systems. They divided the whole state space into several regions by Darboux polynomials and then verified the safety properties in the regions one by one. For a polynomial continuous system, Goubault et al. [9] used Darboux polynomials to find non-polynomial positive invariants and Lyapunov functions to verify reachability and stability properties. The computation of Darboux-type invariants is independent of verification properties, i.e., it does not consider the initial and unsafe constraints [32], usually it does not ensure the separation of the initial region from the unsafe region. As a result, unlike Darboux-type barrier certificates, the existence of Darboux-type invariants solely can not prove safety properties directly.

Computational methods helping to compute barrier certificates from conditions are another essential aspect worth studying. Symbolic computation based methods [10, 21, 30, 26, 27, 18, 29, 20], such as quantifier elimination or Grönber bases computation, have been applied to solve the quantification problem which can prove the existence of barrier certificates. However, due to the high computational complexity, they suffer from the scalability problem.

From a computational point of view, relaxation based methods provide much better efficiency at the cost of more conservative results. Among them, sum-of-squares (SOS) relaxation is the most popular one [23, 15, 6, 28, 31]. Instead of directly handling constraints with quantifiers, SOS relaxation converts them to more conservative constraints represented as either linear matrix inequalities (LMI) [15] or bilinear matrix inequalities (BMI) [23, 31]. In addition, to make the computation tractable, the degrees of the polynomial multipliers appearing in LMI or BMI must be bounded. As a result, the solution set of the bounded LMI or BMI might be contractive. K. Ghorbal et al. [8] studied how to balance the generality of verification conditions and the performance issues of computation. Besides, O. Bouissou et al. [2] applied interval analysis to find the barrier certificates for the dynamical systems whose initial and unsafe regions are all of the box form.

Simulation-guided approaches were also developed. Kapinski et al. [14] defined a new tractable Lyapunov-based barrier certificates. For the particular verification conditions, they combined simulation traces generation with stochastic global optimization to build the Lyapunov candidates, and then used the dReal SMT solver to verify the correctness. For a given set of Lipschitz-continuous dynamical systems, Kapinski et al. [13] checked its forward invariance by verifying it on a finite number of points selected by $\delta-$sampling from the set. Bobiti et al. [1] extended the result to discontinuous dynamics and enabled the verification of forward invariance for hybrid systems. In this paper, we combine the sampling-based relaxation method with least squares and quadratic programming (LS-QP) alternating projection to compute barrier certificates.

2. HYBRID SYSTEM

In this section, we briefly recall the definition of hybrid systems. Besides, we introduce a particular kind of polynomials for continuous systems, called Darboux polynomials.

A continuous dynamical system S is modeled by a finite number of first-order ordinary differential equations

$$\dot{\mathbf{x}} = \mathbf{f}(\mathbf{x}), \tag{1}$$

where $\dot{\mathbf{x}}$ denotes the derivative of $\mathbf{x}$ with respect to the time variable t, and $\mathbf{f}(\mathbf{x})$ is called vector field $\mathbf{f}(\mathbf{x}) = \langle f_1(\mathbf{x}), \cdots, f_n(\mathbf{x})\rangle$ defined on an open set $\psi \subseteq \mathbb{R}^n$. We assume that $\mathbf{f}$ satisfies the local Lipschitz condition, which ensures that given $\mathbf{x} = \mathbf{x}_0$, there exists a time $T > 0$ and a unique time trajectory $\tau : [0, T) \mapsto \mathbb{R}^n$ such that $\tau(t) = \mathbf{x}_0$. And $\mathbf{x}(t)$ is called a solution of (1) that starts at a certain initial state $\mathbf{x}_0$, that is, $\mathbf{x}(0) = \mathbf{x}_0$. Namely, $\mathbf{x}(t)$ is also called a trajectory of (1) from $\mathbf{x}_0$.

To model hybrid systems, we use the notion of hybrid automata [12, 27].

Definition 1. (Hybrid system) A *hybrid system* $\mathbf{H} : \langle V, L, \mathcal{T}, \Theta, \mathcal{D}, \Psi, \ell_0\rangle$ consists of the following components:

- $V = \{x_1, ..., x_n\}$, a set of real-valued system *variables*. A *state* is an interpretation of V, assigning to each $x_i \in V$ a real value. An *assertion* is a first-order formula over V. A state s satisfies an assertion φ, written as $s \models \varphi$, if φ holds on the state s. We will also write $\varphi_1 \models \varphi_2$ for two assertions φ_1, φ_2 to denote that φ_2 is true at least in all the states in which φ_1 is true;
- L, a finite set of locations;
- $\mathcal{T}$, a set of (discrete) transitions. Each transition $\tau : \langle \ell, \ell', g_\tau, \rho_\tau\rangle \in \mathcal{T}$ consists of a prelocation $\ell \in L$, a postlocation $\ell' \in L$, the guard condition g_τ over V, and an assertion ρ_τ over $V \cup V'$ representing the next-state relation, where $V' = \{x_1', ..., x_n'\}$ denotes the next-state variables. Note that the transition τ can take place only if g_τ holds;
- Θ, an assertion specifying the *initial* condition;
- $\mathcal{D}$, a map that associates each location $\ell \in L$ to a *differential rule* (also known as a *vector field*) $\mathcal{D}(\ell)$, an autonomous system $\dot{x}_i = f_{\ell,i}(V)$ for each $x_i \in V$, written briefly as $\dot{\mathbf{x}} = \mathbf{f}_\ell(\mathbf{x})$. The differential rule at a location specifies how the system variables evolve in that location;
- Ψ, a map that maps each location $\ell \in L$ to a *location condition (location invariant)* $\Psi(\ell)$, an assertion over V;
- $\ell_0 \in L$, the *initial location*. We assume that the initial condition satisfies the location invariant at the initial location, that is, $\Theta \models \Psi(\ell_0)$.

By a *state* of a hybrid system $\mathbf{H} : \langle V, L, \mathcal{T}, \Theta, \mathcal{D}, \Psi, \ell_0\rangle$, we mean the tuple $(\ell, \mathbf{x}) \in L \times \mathbb{R}^n$ where n is the number of program variables in $\mathbf{H}$. A trajectory [31] of $\mathbf{H}$ is an infinite sequence of states

$$\langle l_0, \mathbf{x}_0\rangle,\ \langle l_1, \mathbf{x}_1\rangle, \cdots, \langle l_i, \mathbf{x}_i\rangle,\ \langle l_{i+1}, \mathbf{x}_{i+1}\rangle, \cdots$$

such that

- **[Initiation]** $l_0 = \ell_0$ and $\mathbf{x}_0 \models \Theta$;

  Furthermore, for each consecutive pair $\langle l_i, \mathbf{x}_i\rangle, \langle l_{i+1}, \mathbf{x}_{i+1}\rangle$, one of the two *consecution* conditions holds:
- **[Discrete Consecution]** There exists a transition $\tau : \langle \ell, \ell', g_\tau, \rho_\tau\rangle$ such that $l_i = \ell, l_{i+1} = \ell'$ and $(\mathbf{x}_i, \mathbf{x}_{i+1}) \models \rho_\tau(\mathbf{x}_i, \mathbf{x}_{i+1})$ if g_τ holds, or
- **[Continuous Consecution]** $l_i = l_{i+1} = \ell$, and there exists a time interval $\delta > 0$ and a smooth (continuous and differentiable to all orders) function $f : [0, \delta] \to \mathbb{R}^n$ s.t. f evolves from $\mathbf{x}_i$ to $\mathbf{x}_{i+1}$ according to the differential rule $\mathcal{D}(\ell)$ at location ℓ, while satisfying the location invariant $\Psi(\ell)$. Formally,
  - $f(0) = \mathbf{x}_i, f(\delta) = \mathbf{x}_{i+1}$ and $\forall t \in [0, \delta], f(t) \models \Psi(\ell)$,
  - $\forall t \in [0, \delta), (f(t), \dot{f}(t)) \models \mathcal{D}(\ell)$.

A state $\langle \ell, \mathbf{x}\rangle$ is called a *reachable state* of a hybrid system $\mathbf{H}$ from the initial state set $\ell_0 \times \Theta$ if it appears in some trajectory of $\mathbf{H}$. During a continuous flow, the discrete location ℓ_i is maintained and the continuous state variables $\mathbf{x}$ evolve according to the differential equations $\dot{\mathbf{x}} = \mathbf{f}_{\ell_i}(\mathbf{x})$, with $\mathbf{x}$ satisfying the location invariant $\Psi(\ell_i)$. At the state $\langle \ell_i, \mathbf{x}\rangle$, if the guard condition $g(\ell_i, \ell_j)$ is met, the system may undergo a transition to location ℓ_j, and $\mathbf{x}$ will take the new value $\mathbf{x}'$, which is determined by the reset map $\rho(\ell_i, \ell_j)$.

Given a hybrid system $\mathbf{H}$ with prespecified unsafe assertion X_u, we say that the system $\mathbf{H}$ is *safe* if all trajectories of $\mathbf{H}$ starting from the initial condition Θ at the initial location ℓ_0, can not evolve to any state specified by X_u. The safety verification problem can now be stated as follows.

Problem 1. *Given a hybrid system* $\mathbf{H} : \langle V, L, \mathcal{T}, \Theta, \mathcal{D}, \Psi, \ell_0\rangle$ *and an unsafe assertion* X_u*, determine whether* $\mathbf{H}$ *is safe, namely, any state specified by* X_u *is not reachable.*

For safety verification of hybrid systems, the notion of barrier functions of hybrid systems plays an important role. In this paper, we will introduce new barrier functions based on Darboux polynomials for the safety verification of hybrid systems.

Definition 2. (Lie derivative [11]) Let $\mathbf{f}(\mathbf{x})$ be a vector field $\mathbf{f} : \langle f_1(\mathbf{x}), \cdots, f_n(\mathbf{x})\rangle$, the Lie derivative of a smooth function $g(\mathbf{x})$ with respect to $\mathbf{f}(\mathbf{x})$ is given by

$$\mathcal{L}_{\mathbf{f}}(g(\mathbf{x})) = (\nabla g) \cdot \mathbf{f}(\mathbf{x}) = \sum_{i=1}^{n} \left(\frac{\partial g}{\partial x_i} \cdot f_i \right).$$

Definition 3. (Darboux polynomial [5]) Let $\mathbf{f}(\mathbf{x})$ be a vector field $\mathbf{f} : \langle f_1(\mathbf{x}), \cdots, f_n(\mathbf{x})\rangle$, a polynomial $p(\mathbf{x}) \in \mathbb{R}[\mathbf{x}]$ is called a Darboux polynomial (eigenpolynomial, or a polynomial second integral) of $\mathbf{f}(\mathbf{x})$ if and only if

$$\mathcal{L}_{\mathbf{f}}(p(\mathbf{x})) = c(\mathbf{x}) \cdot p(\mathbf{x})$$

where $c(\mathbf{x}) \in \mathbb{R}[\mathbf{x}]$ is a polynomial called the cofactor. When $c(\mathbf{x})$ is a zero polynomial, $p(\mathbf{x})$ is also known as a first integral, otherwise it is called a proper Darboux polynomial.

The following lemma is provided to discover an inherent property of Darboux polynomials.

Lemma 1. *Let S be a continuous dynamical system defined by (1). Suppose $p(\mathbf{x})$ is a Darboux polynomial with respect to $\mathbf{f}(\mathbf{x})$, and $\mathbf{x}(t)$ is a trajectory of (1) starting from $\mathbf{x}_0$,i.e.,$\mathbf{x}(0) = \mathbf{x}_0$. If $p(\mathbf{x}_0) \geq 0$, then $p(\mathbf{x}(t)) \geq 0$ for all $t > 0$.*

Proof. Let $c(\mathbf{x})$ be the cofactor polynomial with respect to $p(\mathbf{x})$, i.e., $\mathcal{L}_{\mathbf{f}}(p(\mathbf{x})) = c(\mathbf{x}) \cdot p(\mathbf{x})$. It follows that

$$\frac{d(p(\mathbf{x}(t)))}{p(\mathbf{x}(t))} = c(\mathbf{x}(t))dt.$$

Thus, the above ODE has the solution of the following form:

$$p(\mathbf{x}(t)) = p(\mathbf{x}_0) \cdot e^{\int_0^t c(x(s))ds}.$$

We then derive that $p(\mathbf{x}(t)) \geq 0$ for all $t > 0$ if $p(\mathbf{x}_0) \geq 0$. □

3. DARBOUX POLYNOMIAL BASED BARRIER CERTIFICATES FOR SAFETY VERIFICATION

At first, we consider the barrier certificate condition for continuous systems in [23]. Given a continuous system S, an initial set Θ and an unsafe set X_u, a barrier certificate is a real-valued function $p(\mathbf{x})$ of states satisfying that $p(\mathbf{x}) \geq 0$ for any point $\mathbf{x}$ in the reachable set R and $p(\mathbf{x}) < 0$ for any point in the unsafe set X_u(called general constraint hereafter). Therefore, if there exists such a function $p(\mathbf{x})$, we can assert that $R \cap X_u = \emptyset$, which has determined the system can not reach a state in the unsafe set from the initial set. In fact, the condition $p(\mathbf{x}) \geq 0$ can be seen as an inductive invariant for the specified barrier certificate $p(\mathbf{x})$. However, the exact reachable set is really computation hard, so we can not determine whether $p(\mathbf{x}) \geq 0$ for the state from the reachable set R. In the following, we present a new barrier certificate which is a sufficient condition for general constraint.

Consider a continuous system S, and let Θ, X_u be the initial set and unsafe set respectively. Then the following theorem gives a new barrier certificate.

Theorem 1. *Given the continuous system S and the corresponding sets Θ and X_u, if there exists a barrier certificate, i.e., a real-valued function $p(\mathbf{x})$ which is a Darboux polynomial, satisfying the following formulae:*

(i) $\Theta \models p(\mathbf{x}) \geq 0$,

(ii) $X_u \models p(\mathbf{x}) < 0$,

then $p(\mathbf{x}) \geq 0$ is a barrier certificate of the continuous system S, and the safety of S is guaranteed.

Proof. If there is a Darboux polynomial $p(\mathbf{x})$ which satisfies conditions (i) and (ii) above, then $p(\mathbf{x}_0) \geq 0$ holds for any point $\mathbf{x}_0$ chosen from the initial set Θ. Therefore, based on lemma 1, $p(\mathbf{x}(t))$ will keep non-negative for any state along the trajectory from the point $\mathbf{x}_0$. And it can not evolve to X_u because of $X_u \models p(\mathbf{x}) < 0$ from the condition (ii). So the safety of the system is obvious. □

Next, we present the barrier certificate condition for hybrid systems. As stated in the following theorem, the specified Darboux polynomials $p_\ell(\mathbf{x})$ are also known as barrier certificates.

Theorem 2. *Let $\mathbf{H} : \langle V, L, \mathcal{T}, \Theta, \mathcal{D}, \Psi, \ell_0\rangle$ be a hybrid system, and $X_u(\ell)$ be the unsafe assertion at location ℓ. Suppose for each location $\ell \in L$, there exists a Darboux polynomial $p_\ell(\mathbf{x})$, that satisfy the following conditions:*

(i) $\Theta \models p_{\ell_0}(\mathbf{x}) \geq 0$,

(ii) $g(\ell, \ell') \wedge \rho(\ell, \ell') \models p_{\ell'}(\mathbf{x}') - \lambda_{\ell,\ell'}(\mathbf{x})p_\ell(\mathbf{x}) \geq 0$, *where $\mathbf{x}'$ is the next state specified by $\rho(\ell, \ell')$ in relation to the previous state $\mathbf{x}$, and $\lambda_{\ell,\ell'}(\mathbf{x}) \in \mathbb{R}[\mathbf{x}]$ is a nonnegative polynomial, for any transition $\langle \ell, \ell', g, \rho\rangle$ going out of ℓ,*

(iii) $X_u(\ell) \models p_\ell(\mathbf{x}) < 0$,

then $p_\ell(\mathbf{x})$ is a barrier certificate of the hybrid system $\mathbf{H}$ at location ℓ, and the safety of $\mathbf{H}$ is guaranteed.

Proof. From condition (i), $p_{\ell_0}(\mathbf{x})$ is nonnegative over the initial states given by Θ. And Lemma 1 implies that $p_\ell(\mathbf{x})$ cannot become negative during the continuous flow. Moreover, condition (ii) guarantees that $p_\ell(\mathbf{x})$ keeps nonnegative during a discrete transition. Thus, $p_\ell(\mathbf{x}) \geq 0$ is an inductive invariant of $\mathbf{H}$ at location ℓ. Then, condition (iii) implies that all reachable states of $\mathbf{H}$ lie outside the unsafe region specified by $X_u(\ell)$, which concludes that the safety of the system is guaranteed. □

According to Theorem 2, $\lambda_{\ell,\ell'}$ can be any nonnegative constants or polynomials. To ease computation, one prefers to assign them with simple fixed values. Remark that the Darboux polynomials can also be used to describe inductive condition of invariants, and then be applied to verify the safety of hybrid systems. In fact, Darboux polynomial $p(\mathbf{x}) = 0$ can be regard as a "barrier" between possible system trajectories and the given unsafe region. If choosing an initial point $\mathbf{x}(t_0)$ from a given set which goes along the state function, it would not change the sign of $p(\mathbf{x}(t))$ for $t \geq t_0$ afterwards. In other words, it will not go across the guard $p(\mathbf{x}) = 0$. In the hybrid case, a barrier certificate is constructed from a set of functions of continuous state indexed by the system location. And each function needs to satisfy the inequalities only within the invariant of the location [23]. The main difference is that Darboux polynomial can also be seen as the algebraic type barrier.

4. TRANSFER TO POLYNOMIAL OPTIMIZATION

In this section, we will discuss how to transfer the problem of generating Darboux-type barrier certificates for hybrid systems to polynomial optimization problem. For the predetermined template of Darboux polynomials, we show that the problem of finding Darboux polynomials is equivalent to the polynomial optimization problem with universal quantifiers, proceeded by eliminating the quantifiers as in the sampling points selection approach.

Let us predetermine a template of Darboux-type barrier certificates with the given degree d. We assume that $p_\ell(\mathbf{x}) = \sum_\alpha p_{\ell,\alpha}\mathbf{x}^\alpha$, where $\mathbf{x}^\alpha = x_1^{\alpha_1}\cdots x_n^{\alpha_n}$, $\alpha = (\alpha_1,\ldots,\alpha_n) \in \mathbb{Z}^n_{\geq 0}$ with $\sum_{i=1}^n \alpha_i \leq d$, and $p_{\ell,\alpha} \in \mathbb{R}$ being parameters. We can rewrite $p_\ell(\mathbf{x}) = \mathbf{p}_\ell^T \cdot T_\ell(\mathbf{x})$, where $T_\ell(\mathbf{x})$ is the (column) vector of all monomials in $x_1,\ldots,x_n$ with total degree $\leq d$, and $\mathbf{p}_\ell \in \mathbb{R}^\nu$ is the coefficient vector of $p_\ell(\mathbf{x})$ with $\nu = \binom{n+d}{n}$.

Theorem 2 provides a sufficient condition to verify the safety of hybrid system $\mathbf{H}$, by generating the Darboux polynomials which satisfy several constraints. For the given $\lambda_{\ell,\ell'} \in \mathbb{R}_+$, the later problem can be translated into the following problem

$$\begin{cases} \text{find} & p_\ell(\mathbf{x}) \in \mathbb{R}[\mathbf{x}], \forall \ell \in L \\ \text{s.t.} & \mathcal{L}_f(p_\ell(\mathbf{x})) = c_\ell(\mathbf{x}) \cdot p_\ell(\mathbf{x}), \\ & \Theta \models p_{\ell_0}(\mathbf{x}) \geq 0, \\ & g(\ell,\ell') \wedge \rho(\ell,\ell') \models p_{\ell'}(\mathbf{x}') - \lambda_{\ell,\ell'} \cdot p_\ell(\mathbf{x}') \geq 0, \\ & X_u(\ell) \models p_\ell(\mathbf{x}) < 0. \end{cases} \tag{2}$$

Observing the equality constraint in (2), we can get the degree of the cofactor $c_\ell(\mathbf{x})$. Similar to the template of $p_\ell(\mathbf{x})$, let the coefficients of $c_\ell(\mathbf{x})$ be parameters, and write $c_\ell(\mathbf{x})$ as $c_\ell(\mathbf{x}) = \mathbf{c}_\ell^T \cdot T_\ell(\mathbf{x})$, where $\mathbf{c}_\ell$ and $T_\ell(\mathbf{x})$ are the coefficient vector and the monomial vector of $c_\ell(x)$, respectively. We can rewrite the equality constraint in (2) as a quadratic system with the variables $\mathbf{p}_\ell, \mathbf{c}_\ell$ by sorting the coefficients with respect to the variables $\mathbf{x}$, that is,

$$L_f(p_\ell(\mathbf{x})) = c_\ell(\mathbf{x}) \cdot p_\ell(\mathbf{x}) \Longleftrightarrow F_\ell(\mathbf{p}_\ell, \mathbf{c}_\ell) = 0. \tag{3}$$

In addition, the variables of the third constraint in (2) are $\mathbf{x}, \mathbf{x}'$. From the guard condition $g(\ell,\ell')$ and the reset condition $\rho(\ell,\ell')$, one can just use the variables $\mathbf{x}$ to represent this constraint, that is,

$$\Omega_g(\ell,\ell') \models \tilde{p}_{\ell,\ell'}(\mathbf{x}) \geq 0, \tag{4}$$

where $\Omega_g(\ell,\ell') = \{\mathbf{x} \in \mathbb{R}^n | g(\ell,\ell') \wedge \rho(\ell,\ell')\}$.

Having (3) and (4), the problem (2) can be transformed into the following form

$$\begin{cases} \text{find} & \mathrm{p}_\ell \in \mathbb{R}^\nu, \quad \forall \ell \in L \\ \text{s.t.} & F_\ell(\mathbf{p}_\ell, \mathbf{c}_\ell) = 0, \\ & p_{\ell_0}(\mathbf{x}, \mathbf{p}_{\ell_0}) \geq 0, & \forall \mathbf{x} \in \Theta, \\ & \tilde{p}_{\ell,\ell'}(\mathbf{x}, \mathbf{p}_\ell, \mathbf{p}_{\ell'}) \geq 0, & \forall \mathbf{x}, \mathbf{x}' \in \Omega_{\ell,\ell'}, \\ & p_\ell(\mathbf{x}, \mathbf{p}_\ell) < 0, & \forall \mathbf{x} \in X_u(\ell). \end{cases} \tag{5}$$

By investigating (5), the last third constraints are the ones involving with universal quantifiers. The straightforward idea is to apply quantifier elimination methods to deal with (5). Moreover, there are several available computer algebra tools (such as QEPCAD [3]) to solve the problem. Nevertheless, quantifier elimination methods based on the cylindrical algebraic decomposition (CAD) are of high complexity. In addition, the number of the variables $\mathbf{p}_\ell, \mathbf{c}_\ell$ in the polynomial optimization problem (5) is not small. Taking the two limits into account, the typical quantifier elimination based on cylindrical algebraic decomposition is impractical. Hereafter we propose a novel method to solve (5) by means of eliminating universal quantifiers through checking sampling points.

Since the last constraint in (5) is a strict inequality, we can introduce a small positive real number $\epsilon \in \mathbb{R}_{>0}$ to relax this constraint to a non-strict one, i.e.,

$$-p_\ell(\mathbf{x}, \mathbf{p}_\ell) - \epsilon \geq 0 \Longrightarrow p_\ell(\mathbf{x}, \mathbf{p}_\ell) < 0.$$

Let us first use $\mathbf{p}$ and $\mathbf{c}$ to denote the whole coefficient vectors of the Darboux polynomials and the corresponding cofactors, respectively, i.e.,

$$\mathbf{p}^T = [\mathbf{p}_{\ell_0}^T, \mathbf{p}_{\ell_1}^T, \ldots], \quad \mathbf{c}^T = [\mathbf{c}_{\ell_0}^T, \mathbf{c}_{\ell_1}^T, \ldots].$$

The dimension of $\mathbf{p}$ is denoted as ω hereafter.

For ease of presentation, (5) can be rewritten as the following unified form:

$$\begin{cases} \text{find} & \mathbf{p} \\ \text{s.t.} & F(\mathbf{p}, \mathbf{c}) = 0, \\ & \tilde{p}_i(\mathbf{x}, \mathbf{p}) \geq 0, \quad \forall \mathbf{x} \in \Omega_i, i = 1, 2, \ldots, k. \end{cases} \tag{6}$$

where $F(\mathbf{p}, \mathbf{c}) = 0$ is the quadratic system consisting of all equations $F_\ell(\mathbf{p}_\ell, \mathbf{c}) = 0$ for each location $\ell \in L$, and $\tilde{p}_i(\mathbf{x}, \mathbf{p}) \geq 0, \forall \mathbf{x} \in \Omega_i, i = 1, \ldots, k$ represent the second, the third and the last relaxed ones in (5) for each location $\ell \in L$.

To avoid eliminating universal quantifiers directly, here we provide a relaxation technique to deal with (6), which is based on selecting sampling points. For each $\Omega_i, 1 \leq i \leq k$, let us first construct a rectangular mesh M in Ω_i with a mesh spacing $r \in \mathbb{R}_+$ (say $r = 0.05$) and mesh point set $\chi_i = \{\mathbf{x}_1, \mathbf{x}_2, \cdots, \mathbf{x}_{m_i}\}$. Given a continuously differentiable function $\phi(\mathbf{x})$ over the compact domain Ω, and let $\mathbf{x} \in \Omega$ and $\mathbf{x} + \Delta\mathbf{x} \in \Omega$ be chosen randomly, then the mean value theorem yields that

$$|\phi(\mathbf{x} + \Delta\mathbf{x}) - \phi(\mathbf{x})| \leq n\eta\|\Delta\mathbf{x}\|_\infty, \tag{7}$$

where $\eta = \sup_{\mathbf{x}\in\Omega}\|\nabla\phi(\mathbf{x})\|_\infty$.

By observing (6), the feasible solution satisfying the constraints is not unique, it is easy to verify that if $\mathbf{p}$ is the feasible solution, then $k\mathbf{p}$ ($\forall k \in \mathbb{R}_{>0}$) is also the feasible solution of (6). What the safety verification problem concentrates here is the existence of such $\mathbf{p}$ satisfying the constraints of (6). Therefore, it is reasonable for us to provide a bound D at first for searching the objective feasible solution $\mathbf{p}$ such that $\|\mathbf{p}\|_\infty \leq D$, which ensures that the coefficients of the polynomials $\tilde{p}(\mathbf{x}, \mathbf{p})$ are also bounded. In this case, from (7) we may select a minimal $\delta_i \in \mathbb{R}_{>0}$, such that the following implication is satisfied:

$$\tilde{p}_i(\mathbf{x}_j, \mathbf{p}) - \delta_i \geq 0,\ 1 \leq j \leq m_i \Longrightarrow \tilde{p}_i(\mathbf{x}, \mathbf{p}) \geq 0,\ \forall \mathbf{x} \in \Omega_i.$$

We should illustrate how to determine δ_i here. In fact, when given objective system $\mathbf{H}$, each Ω_i is determined. Then the associate δ_i can be determined, after deciding the sampling mesh spacing size r. For simplify, we may compute $\delta_i = n\eta_i r \in \mathbb{R}_{>0}$ where $\eta_i = \sup_{\mathbf{x}\in\Omega_i}\|\nabla\tilde{p}(\mathbf{x})_i\|_\infty$.

By using the above relaxation technique based on sampling points verification, (6) can be relaxed as the following polynomial optimization problem without quantifiers.

$$\begin{cases} \text{find} & \mathbf{p} \\ \text{s.t.} & F(\mathbf{p}, \mathbf{c}) = 0, \\ & \tilde{p}_i(\mathbf{x}_j, \mathbf{p}) - \delta_i \geq 0, \quad 1 \leq i \leq k, \quad 1 \leq j \leq m_i, \\ & -E \cdot \mathbf{p} + D \cdot \mathbf{1} \geq 0, \\ & E \cdot \mathbf{p} + D \cdot \mathbf{1} \geq 0. \end{cases} \tag{8}$$

where $E \in \mathbb{R}^{\omega\times\omega}$ is the identity matrix and $\mathbf{1}$ is a vector of all ones with the same dimension as $\mathbf{p}$.

According to the rule of the selection of δ_i, it is easy to show that the feasible solution of (8) is also the feasible one of (5). Moreover, (8) has a special structure, that is, all equalities are quadratic and all inequalities are linear. Therefore, (8) can yield the following matrix form:

$$\left\{\begin{array}{ll} \text{find} & \mathbf{p} \\ \text{s.t.} & F(\mathbf{p},\mathbf{c}) = 0, \\ & A\cdot\mathbf{p} \geq \mathbf{b}, \end{array}\right. \tag{9}$$

where A is a constant matrix and its row dimension is $\sum_{i=1}^{k} m_i$.

Summarizing the above considerations, generating the barrier certificates for hybrid systems is translated into the problem for computing a feasible solution of the polynomial optimization problem (9).

Remark 1. *The smaller the mesh size is, the closer each δ_i gets to zero, i.e., $\lim\limits_{r\to 0}\delta_i = 0$. Moreover, it would't lead to a dramatic rise in the computational cost because only a limited number of linear inequalities constraints are added into the problem.*

Remark 2. *To improve the efficiency of the computation in practice, actually, we choose a small $\delta_i = 0.1$ for the fixed coefficient bound $D = 1$ in the sequel of this paper. And a verification would be required to show whether the obtained $\mathbf{p}$ satisfies the associated inequalities over all points of the set after any feasible solution is obtained.*

5. LS-QP ALTERNATING PROJECTION

In Section 4, we have reduced the problem of safety verification of hybrid systems to the problem of polynomial optimization with quadratic equalities and linear inequalities. It is known that the polynomial optimization problem can be solved efficiently by algorithms such as Gauss-Newton iterations, trust region methods, interior-point methods. From (9), we can see that the number of the equations is large, which is related to the number of the system variables and the degree of the Darboux polynomial. This key feature determines that the performance of the typical numerical optimization methods for attacking (9) really depends on the chosen initial point, as illustrated by the following example.

Example 1. *[4] Consider the the following nonlinear system:*

$$\left\{\begin{array}{rl} \dot{x} = & -x + 2x^2 y \\ \dot{y} = & -y \end{array}\right.$$

We want to verify that all trajectories of the system starting from the initial set

$$\Theta = \{\mathbf{x} \in \mathbb{R}^2 : 1 \leq x \leq 2 \wedge -2 \leq y \leq -1\}$$

will never enter the unsafe region

$$X_u = \{\mathbf{x} \in \mathbb{R}^2 : 1 \leq x \leq 2 \wedge 1 \leq y \leq 2\}.$$

As explained in Section 4, we first set the degree $d = 1$, the mesh size $s = 0.5$ for Θ and X_u, then set the template for the Darboux polynomial $p(x,y)$ and its cofactor $c(x,y)$ as $p(x,y) = p_1\,x + p_2\,y + p_3$ and $c(x,y) = c_1\,x + c_2\,y + c_3$, respectively.

Let $\mathbf{p} = [p_1, p_2, p_3]^T$ and $\mathbf{c} = [c_1, c_2, c_3]^T$, to verify the safety of the above system, it suffices to obtain a feasible solution of the following polynomial optimization problem:

$$\left\{\begin{array}{ll} \text{find} & \mathbf{p} \\ \text{s.t.} & f_1(\mathbf{p},\mathbf{c}) = f_2(\mathbf{p},\mathbf{c}) = \cdots = f_{11}(\mathbf{p},\mathbf{c}) = 0, \\ & A\cdot\mathbf{p} \geq \mathbf{b}, \end{array}\right. \tag{10}$$

where $A \in \mathbb{R}^{18\times 3}$ and $\mathbf{b} = [0.1, 0.1, \ldots, 0.1]^T$.

Let us use the Matlab `fmincon` numeric optimization solver for which we choose the interior-point method option to solve (10). We select the initial solution $\mathbf{p}^{(0)}$ from the set $[-5,5]^3$ randomly, and then call `fmincon` to deal with (10). After 5000 trials by selecting initial solution $\mathbf{p}^{(0)}$, `fmincon` cannot yield any feasible solution for (10). The reason may lie in that the initial solution we selected is not close enough to the actual solution. Actually, if we choose the initial solution $\mathbf{p}^{(0)} = [0.2, 2, 0]^T$, which is very close to a feasible solution $[0, 2, 0]$, it turns out that `fmincon` can succeed to obtain the feasible solution. However, if the initial solution is chosen as $\tilde{\mathbf{p}}^{(0)} = [0.5, 2, 0]^T$, which is a bit further, no feasible solution can be found. This phenomenon also indicates the selection of initial solutions may seriously impact the result of the typical numeric optimization method for handling (9). □

In the sequel, we present a novel method, called LS-QP alternating projection hereafter, to deal with (9). In LS-QP alternating projection method, the problem (9) is tackled by an iterative scheme, which is carried on by computing the optimal solutions of a least-squares (LS) problem and a quadratic programming (QP) problem.

Investigating (9), $F(\mathbf{p},\mathbf{c})$ involves only cross terms between parameters of $\mathbf{p}$ and $\mathbf{c}$, which means there is no crossing product like $p_i p_j$ and $c_i c_j$ in the equations. Taking this special feature into account, an alternative projection method can be applied by fixing $\mathbf{p}$ and $\mathbf{c}$, respectively, which leads to a quadratic programming problem and a least-squares problem. Concretely speaking, if $\mathbf{p}$ is fixed by some numerical vector $\mathbf{p}^*$, (9) would become a least-squares problem: $\min_{\mathbf{c}} \|F(\mathbf{p}^*,\mathbf{c})\|$. Likewise, once $\mathbf{c}$ is fixed by $\mathbf{c}^*$, then (9) is translated into the following problem

$$\left\{\begin{array}{ll} \text{find} & \mathbf{p}, \\ \text{s.t.} & F(\mathbf{p},\mathbf{c}^*) = 0, \\ & A\cdot\mathbf{p} \geq \mathbf{b}. \end{array}\right. \tag{11}$$

which leads to a typical quadratic programming problem. As addressed above, the efficient strategy for solving (9) is to reduce dimensionality. Roughly speaking, we keep one variable vector fixed and then optimize for the other variable vector. Notably, the fixed value can be obtained by solving the above least-squares problem or quadratic programming problem.

At the $(k+1)$-th iteration, when $\mathbf{p}$ is fixed by $\mathbf{p}^{(k)} = [\mathbf{p}_1^{(k)}, \cdots, \mathbf{p}_s^{(k)}]^T$, which is the optimal value obtained from the k-th iteration, we need solve the optimal value for $\mathbf{c}$, i.e.,

$$\min_{\mathbf{c}} \|F(\mathbf{p}^{(k)},\mathbf{c})\|. \tag{12}$$

In this situation, (12) can also be rewritten as the following form with the updated variables

$$\begin{array}{l} \min \ \|F(\mathbf{p}^{(k)}, \mathbf{c}^{(k)} + \Delta\mathbf{c})\|, \\ \quad \mathbf{c}^{(k+1)} := \mathbf{c}^{(k)} + \Delta\mathbf{c} \neq 0. \end{array} \tag{13}$$

For convenience, we denote the solution of (13) as

$$\Delta\mathbf{c} = update_1(F).$$

Let $\mathbf{c}$ be fixed by $\mathbf{c}^{(k+1)}$, and then update $\mathbf{p}$ by solving the following optimization problem

$$\begin{cases} \min \ \|\Delta\mathbf{p}\| \\ \quad F((\mathbf{p}^{(k)}+\Delta\mathbf{p}),\mathbf{c}^{(k+1)})=0, \\ \quad A\cdot(\mathbf{p}^{(k)}+\Delta\mathbf{p})\geq\mathbf{b}, \end{cases} \tag{14}$$

where $\mathbf{p}^{(k+1)} := \mathbf{p}^{(k)} + \Delta\mathbf{p} \neq \mathbf{0}$. Similarly, the solution of (14) is denoted by

$$\Delta\mathbf{p} = update_2(F).$$

The geometric description of the LS-QP alternating projection method is depicted in Figure 1. Here $\mathbf{C}$ is the polyhedron defined by $A\cdot\mathbf{p}\geq\mathbf{b}$, and $\mathbf{P}$ is the manifold defined by $F(\mathbf{p},\mathbf{b})=0$. Suppose $\mathbf{p}^{(k)}$ and $\mathbf{c}^{(k)}$ have been produced after the k-th iteration. In this situation, for the fixed $\mathbf{p}^{(k)}$, $\mathbf{c}^{(k+1)}$ is computed by projecting $\mathbf{p}^{(k)}$ into $\mathbf{C}$. Afterwards $\mathbf{p}^{(k+1)}$ is obtained by projecting $\mathbf{c}^{(k+1)}$ into $\mathbf{P}$. Detailed procedures are summarized in Algorithm 1.

Algorithm 1 LS-QP alternating projection

```
Require: Sampling point set $\chi$ and functions $F$;
Ensure: Darboux polynomial $p(\mathbf{x})$;
  Establish the optimization problem (11) from $\chi$ and $F$;
  Generate some initial vectors $\mathbf{c}^{(0)}$ and $\mathbf{p}^{(0)}$;
  for $k = 1, 2, \cdots, ^{\dagger}$ do;
  $\mathbf{c}^{(k)} = \mathbf{c}^{(k-1)} + update_1(F, \mathbf{p}^{(k-1)})$;
  $\mathbf{p}^{(k)} = \mathbf{p}^{(k-1)} + update_2(F, \mathbf{c}^{(k)})$;
  end for.
    † See Remark 4 in this section for stopping criteria.
```

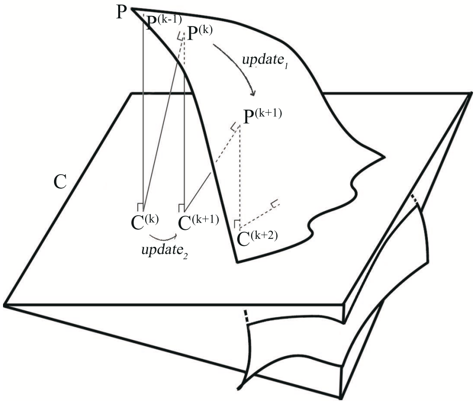

Figure 1: LS-QP alternating projection

Remark 3. *At the beginning of the alternating iteration, we can set $\mathbf{c}^{(0)}$ by selecting a random vector, and then obtain the associated vector $\mathbf{p}^{(0)}$ by solving the least squares problem with the known vector $\mathbf{c}^{(0)}$. Rather than choosing $\mathbf{c}^{0}$ randomly, we can select a random vector $\mathbf{p}^{(0)}$ at first, and then get the associated vector $\mathbf{c}^{(0)}$ by solving the corresponding quadratic programming problem with the given $\mathbf{p}^{(0)}$.*

Remark 4. *There are several options for the stopping criterion of the LS-QP alternating projection algorithm. The most typical way for the stopping criterion is to use a maximum number of iterations to ensure the termination of the algorithm. Therefore, Algorithm 1 will be terminated when one of the following cases occurs:*

- *When $\|update_1(F,\mathbf{p}^{(k-1)})\| < \sigma$ and $\|update_2(F,\mathbf{c}^{(k)})\| < \sigma$ at k-th iteration for a given tolerance σ (like, $\sigma = 10^{-5}$), Algorithm 1 will stop and return the current result; otherwise it will go to the next iteration.*
- *Given a time limit N and take account of the number of iterations, when the LS-QP alternating projection algorithm has been running so many times which exceeds the time limit N, the algorithm stops.*

6. EXPERIMENTS

Let us present some examples of safety verification for nonlinear hybrid systems based on Darboux polynomials.

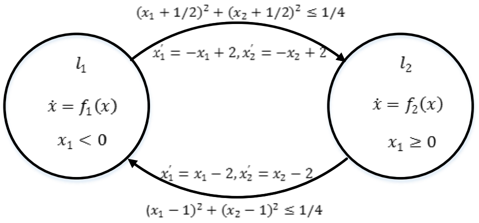
$(x_1+1/2)^2+(x_2+1/2)^2 \leq 1/4$
$x_1' = -x_1+2, x_2' = -x_2+2$
l_1
$\dot{x} = f_1(x)$
$x_1 < 0$
l_2
$\dot{x} = f_2(x)$
$x_1 \geq 0$
$x_1' = x_1-2, x_2' = x_2-2$
$(x_1-1)^2+(x_2-1)^2 \leq 1/4$

Figure 2: Hybrid system of Example 2

Example 2. *Consider the the hybrid system depicted in Figure 2, where*

$$f_1(\mathbf{x}) = \begin{bmatrix} x_1 - x_1x_2 \\ -x_2 + x_1x_2 \end{bmatrix}, \quad f_2(\mathbf{x}) = \begin{bmatrix} x_1 + x_1^2x_2 \\ x_2 + x_1x_2 \end{bmatrix}.$$

The system starts in location ℓ_1 with an initial state in

$$\Theta = \{(x_1,x_2)\in\mathbb{R}^2 : -2 \leq x_1, x_2 \leq -1\}.$$

We will verify that all trajectories of the system can never reach the states of

$$X_u(\ell_2) = \{(x_1,x_2)\in\mathbb{R}^2 : 0 \leq x_1 \leq 1, -2 \leq x_2 \leq -1\}.$$

By applying our method, we can obtain two Darboux polynomials at locations ℓ_1 and ℓ_2:

$$p_{\ell_1}(\mathbf{x}) = 0.7332x_1,$$
$$p_{\ell_2}(\mathbf{x}) = 0.7332x_1x_2,$$

which satisfy all the conditions in Theorem 2. Then, the safety property of this system is guaranteed. □

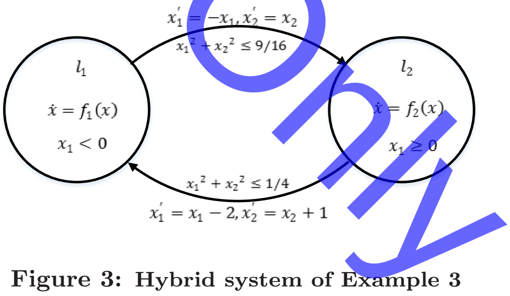

Figure 3: Hybrid system of Example 3

Example 3. *Consider the hybrid system depicted in Figure 3, where*

$$f_1(\mathbf{x}) = \begin{bmatrix} -x_1 + x_1x_2 \\ -x_2 \end{bmatrix}, \quad f_2(\mathbf{x}) = \begin{bmatrix} -x_1 + 2x_1^2x_2 \\ -x_2 \end{bmatrix}.$$

The system starts in location ℓ_1 with an initial state in

$$\Theta = \{(x_1,x_2)\in\mathbb{R}^2 : (x_1+2)^2 + (x_2-2)^2 \leq 0.25\}$$

We will verify that all trajectories of the system can never reach the states of

$$X_u(\ell_2) = \{(x_1, x_2) \in \mathbb{R}^2 : (x_1 - 2)^2 + (x_2 - 2)^2 \leq 0.25\}.$$

By applying our method, we can obtain two Darboux polynomials at locations ℓ_1 and ℓ_2:

$$\begin{aligned} p_{\ell_1}(\mathbf{x}) &= 0.7332x_2, \\ p_{\ell_2}(\mathbf{x}) &= -0.2711x_1x_2 + 0.2711, \end{aligned}$$

which satisfy all the conditions in Theorem 2. Then the safety property of the given system is guaranteed. □

As stated in Theorem 2 in [15], the problem of barrier certificate generation can be rewritten as that of computing a set of polynomial functions $\{B_\ell(\mathbf{x}), \forall \ell \in L\}$ such that the following conditions hold:

$$\left.\begin{array}{l} B_{\ell_0}(\mathbf{x}) \leq 0 \ \forall \mathbf{x} \in \Theta, \\ \dot{B}_\ell(\mathbf{x}) - \lambda_\ell B_\ell(\mathbf{x}) \leq 0 \ \forall \mathbf{x} \in \Psi(\ell), \\ \gamma_{\ell,\ell'} B_\ell(\mathbf{x}) - B_{\ell'}(\mathbf{x}') \geq 0 \ \forall \mathbf{x} \in g(\ell,\ell') \forall \mathbf{x}' \in \rho((\ell,\ell'),\mathbf{x}), \\ B_\ell(\mathbf{x}) > 0 \ \forall \mathbf{x} \in X_u(\ell), \end{array}\right\} \quad (15)$$

for some real numbers λ_ℓ, and non-negative real numbers $\gamma_{\ell,\ell'}$. According to Corollary 2 in [15], the SOS relaxation can be applied to convert the above problem to a linear matrix inequalities (LMI) problem, which is convex and can be solved with great efficiency. And as shown in Theorem 5 in [23], the problem of barrier certificate generation can be rewritten as that of computing a set of polynomial functions $\{B_\ell(\mathbf{x}), \forall \ell \in L\}$, each of which satisfies

$$\left.\begin{array}{l} B_{\ell_0}(\mathbf{x}) \leq 0 \ \forall \mathbf{x} \in \Theta, \\ \dot{B}_\ell(\mathbf{x}) \leq 0 \ \forall \mathbf{x} \in \Psi(\ell) \text{ s.t. } B_\ell(\mathbf{x}) = 0, \\ B_\ell(\mathbf{x}) \leq 0 \ \forall \mathbf{x} \in g(\ell,\ell') \forall \mathbf{x}' \in \rho((\ell,\ell'),\mathbf{x}) \text{ s.t. } B_{\ell'}(\mathbf{x}') \leq 0, \\ B_\ell(\mathbf{x}) > 0 \ \forall \mathbf{x} \in X_u(\ell). \end{array}\right\} \quad (16)$$

According to Algorithm 17 in [23], the above problem can be transformed to a bilinear matrix inequalities (BMI) problem, which is non-convex and NP-hard. We compared our Darboux-type barrier certificate based method with the existing barrier certificate based ones in [15, 23] over a set of benchmarks gathered from the related works. Table 1 shows the result. Here, the LMI problems yielded from (15) were settled by the Matlab toolbox *SOSTOOLS* [24] while the BMI problems yielded from (16) were solved by the Matlab toolbox *PENBMI* [17].

Algorithm 1 has been implemented in Matlab, and the performance is reported in Table 1. For each example, we first utilize the mesh points of the rectangular meshes with spacing $r = 0.05$ located in initial and unsafe regions respectively, and then eliminate universal quantifiers in problem (5) by linear inequalities. In this manner, we apply Algorithm 1 to obtain the Darboux-type barrier certificate $p(\mathbf{x})$. Noted that the experiments are performed on Intel(R) Core(TM) at 3.40GHz with 4GB of memory under Windows.

In Table 1, n denotes the number of the system variables; deg denotes the maximum degree of the polynomials in the vector fields; *LMI* and *BMI* refer to the computational methods for solving problems (15) and (16) respectively; deg(B) denotes the degree of the computed barrier certificates, and $T(s)$ represents the computation time in seconds; deg(p) represents the degree of the Darboux polynomials obtained via our LS-QP alternating projection algorithm; *Fail* means that the method fails to find the barrier certificates with degree ≤ 6.

Table 1: Algorithm Performance on Benchmarks

ID	n	deg	LMI		BMI		LS-QP	
			deg(B)	$T(s)$	deg(B)	$T(s)$	deg(p)	$T(s)$
1	2	2	*Fail*	-	2	0.8744	2	0.6508
2	3	2	*Fail*	-	*Fail*	-	1	0.4854
3	3	2	1	0.3751	1	1.1039	1	0.5154
4	2	2	*Fail*	-	*Fail*	-	1	0.3645
5	3	2	*Fail*	-	2	5.0523	2	1.6337
6	2	2	*Fail*	-	*Fail*	-	1	0.3155
7	2	2	2	0.2816	2	1.1407	1	0.3717
8	2	2	*Fail*	-	2	1.9511	2	0.9237
9	2	3	4	0.4623	2	1.0011	*Fail*	-
10	4	2	*Fail*	-	2	10.8846	1	7.0506
11	6	2	2	27.2306	2	65.3519	1	14.0614

For the 11 examples, the SOS relaxation based on BMI solving can yield barrier certificates for 8 of them while ours can cover 10. Our verification condition can facilitate the safety verification of systems embracing Darboux-type barrier certificates. It also enhances the capability of barrier certificate based approaches by enabling those systems that are difficult to be verified using existing verification conditions to be verifiable, like the systems in the example 2,4 and 6 in the experiment. At the same time, being a specific type of barrier certificate, there are some systems that can be verified by classical conditions much more easily than by ours as shown in the example 9. In addition, even for the systems that can be solved by both of them, there is no theoretical result predicting which method will produce lower-degree barrier certificates. From the table, we can see that the BMI conversion brings more expressiveness but at the cost of lower computation efficiency. The problem of Darboux-type barrier certificate generation is also non-convex. However, the proposed LS-QP alternating projection algorithm can solve it in much shorter time. Remarked that our obtained Darboux polynomials, regarded as the barrier certificates, in examples 10 and 11 are different from the results provided in [7] and [19], respectively.

7. CONCLUSION

In this paper, we have presented a new Darboux-type barrier certificate based method for verifying safety property of nonlinear hybrid systems. Our method is based on adapting Darboux polynomials to provide a new type of barrier certificate. This key distinguishing feature of Darboux polynomials provides a new encoding to compute barrier certificates, thus guarantees that our method can yield barrier certificates that SOS relaxation is unable to produce. Thanks to the feature in the problem of barrier certificate generation, a sampling-based method and a LS-QP alternating projection method are proposed for computing Darboux-type barrier certificates efficiently. Experiments on some benchmarks are given to illustrate the efficiency of our algorithm.

8. REFERENCES

[1] Bobiti, R., and Lazar, M. A delta-sampling verification theorem for discrete-time, possibly discontinuous systems. In *Proc. of the Hybrid Systems: Computation and Control (HSCC)* (2015), ACM, pp. 140–148.

[2] Bouissou, O., Chapoutot, A., Djaballah, A., and Kieffer, M. Computation of parametric barrier functions for dynamical systems using interval analysis. In *Proc. of the IEEE Conference on Decision and Control (CDC)* (2014), IEEE, pp. 753–758.

[3] Brown, C. W. QEPCAD B: a program for computing with semi-algebraic sets using CADs. *ACM SIGSAM Bulletin 37*, 4 (2003), 97–108.

[4] Brown, R. C., and Hinton, D. B. Lyapunov inequalities and their applications. In *Survey on Classical Inequalities*. Springer, 2000, pp. 1–25.

[5] Cheze, G. Computation of darboux polynomials and rational first integrals with bounded degree in polynomial time. *Journal of Complexity 27*, 2 (2011), 246–262.

[6] Dai, L., Gan, T., Xia, B., and Zhan, N. Barrier certificates revisited. *Journal of Symbolic Computation, In Press* (2015).

[7] Ferragut, A., and Gasull, A. Seeking darboux polynomials. *Acta Applicandae Mathematicae 139*, 1 (2015), 167–186.

[8] Ghorbal, K., Sogokon, A., and Platzer, A. A hierarchy of proof rules for checking positive invariance of algebraic and semi-algebraic sets. *Computer Languages, Systems, and Structures* (2016).

[9] Goubault, E., Jourdan, J.-H., Putot, S., and Sankaranarayanan, S. Finding non-polynomial positive invariants and lyapunov functions for polynomial systems through darboux polynomials. In *Proc. of the American Control Conference (ACC)* (2014), IEEE, pp. 3571–3578.

[10] Gulwani, S., and Tiwari, A. Constraint-based approach for analysis of hybrid systems. In *Proc. of the Computer Aided Verification (CAV)* (2008), vol. 5123, pp. 190–203.

[11] Halmos, P. R. *Finite-Dimensional Vector Spaces*. Springer, 1974.

[12] Henzinger, T. The theory of hybrid automata. In *Proc. of the IEEE Symposium on Logic in Computer Science (LICS)* (1996), pp. 278–292.

[13] Kapinski, J., and Deshmukh, J. Discovering forward invariant sets for nonlinear dynamical systems. In *Interdisciplinary Topics in Applied Mathematics, Modeling and Computational Science*. Springer, 2015, pp. 259–264.

[14] Kapinski, J., Deshmukh, J. V., Sankaranarayanan, S., and Aréchiga, N. Simulation-guided lyapunov analysis for hybrid dynamical systems. In *Proc. of the Hybrid Systems: Computation and Control (HSCC)* (2014), ACM, pp. 133–142.

[15] Kong, H., He, F., Song, X., Hung, W. N., and Gu, M. Exponential-condition-based barrier certificate generation for safety verification of hybrid systems. In *Proc. of the Computer Aided Verification (CAV)* (2013), Springer, pp. 242–257.

[16] Kong, H., Song, X., Han, D., Gu, M., and Sun, J. A new barrier certificate for safety verification of hybrid systems. *The Computer Journal 57*, 7 (2014), 1033–1045.

[17] Kočvara, M., and Stingl, M. PENBMI user's guide (version 2.0). Available at `http://www.penopt.com`, 2005.

[18] Liu, J., Zhan, N., and Zhao, H. Computing semi-algebraic invariants for polynomial dynamical systems. In *Proc. of the Embedded Software (EMSOFT)* (2011), ACM, pp. 97–106.

[19] Llibre, J., and Valls, C. On the integrability of the einstein–yang–mills equations. *Journal of Mathematical Analysis and Applications 336*, 2 (2007), 1203–1230.

[20] Matringe, N., Moura, A. V., and Rebiha, R. Generating invariants for non-linear hybrid systems by linear algebraic methods. In *Proc. of the Static Analysis*. Springer, 2010, pp. 373–389.

[21] Platzer, A., and Clarke, E. M. Computing differential invariants of hybrid systems as fixedpoints. *Formal Methods in System Design 35*, 1 (2009), 98–120.

[22] Prajna, S., and Jadbabaie, A. Safety verification of hybrid systems using barrier certificates. In *Proc. of the Hybrid Systems: Computation and Control (HSCC)* (2004), Springer, pp. 477–492.

[23] Prajna, S., Jadbabaie, A., and Pappas, G. A framework for worst-case and stochastic safety verification using barrier certificates. *IEEE Transactions on Automatic Control 52*, 8 (2007), 1415–1429.

[24] Prajna, S., Papachristodoulou, A., and Parrilo, P. Sostools: Sum of squares optimization toolbox for matlab, 2002. *URL: http://www. cds. caltech. edu/sostools*.

[25] Rachid Rebiha, Arnaldo V. Moura, N. M. Generating invariants for non-linear hybrid systems. *Theoretical Computer Science 594* (2015), 180–200.

[26] Rodríguez, E., and Tiwari, A. Generating polynomial invariants for hybrid systems. In *Proc. of the Hybrid Systems: Computation and Control (HSCC)* (2005), pp. 590–605.

[27] Sankaranarayanan, S., Sipma, H., and Manna, Z. Constructing invariants for hybrid systems. *Formal Methods in System Design 32* (2008), 25–55.

[28] Sloth, C., Pappas, G. J., and Wisniewski, R. Compositional safety analysis using barrier certificates. In *Proc. of the Hybrid Systems: Computation and Control (HSCC)* (2012), ACM, pp. 15–24.

[29] Sogokon, A., Ghorbal, K., Jackson, P. B., and Platzer, A. A method for invariant generation for polynomial continuous systems. In *Proc. of the Verification, Model Checking, and Abstract Interpretation (VMCAI)* (2016), Springer, pp. 268–288.

[30] Sturm, T., and Tiwari, A. Verification and synthesis using real quantifier elimination. In *Proc. of the International Symposium on Symbolic and Algebraic Computation (ISSAC)* (2011), ACM Press, pp. 329–336.

[31] Yang, Z., Wu, M., and Lin, W. Exact verification of hybrid systems based on bilinear SOS representation. *ACM Transactions on Embedded Computing Systems 14*, 1 (2015), 1–19.

[32] Zaki, M., Tahar, S., and Bois, G. Combining constraint solving and formal methods for the verification of analog designs. Tech. rep., Concordia University, 2007.

[33] Zaki, M., Tahar, S., and Bois, G. A symbolic approach for the safety verification of continuous systems. In *Proc. of the International Conference on Computational Sciences* (2007), pp. 93–100.

Appendix: Benchmark Examples

System 1 [25].

$$\begin{bmatrix} \dot{x_1} \\ \dot{x_2} \end{bmatrix} = \begin{bmatrix} -x_1 + 2x_1^2 x_2 \\ -x_2 \end{bmatrix},$$

- The local condition: $\{\mathbf{x} \in \mathbb{R}^2 : -2 \leq x_1, x_2 \leq 2\}$;

  The initial set: $\{\mathbf{x} \in \mathbb{R}^2 : -1/2 \leq x_1 \leq 1/2, 1/2 \leq x_2 \leq 3/2\}$;

  The unsafe set: $\{\mathbf{x} \in \mathbb{R}^2 : (x_1 - 3/2)^2 + (x_2 - 3/2)^2 \leq 1/4\}$.
- The computed Darboux polynomial $p(\mathbf{x}) = -0.7195 x_1 \cdot x_2 + 0.7195$.

System 2 [25].

$$\begin{bmatrix} \dot{x_1} \\ \dot{x_2} \\ \dot{x_3} \end{bmatrix} = \begin{bmatrix} x_1 - x_1 x_3 \\ x_2 - 2x_2 x_3 \\ -x_3 + x_3 x_1 + x_3 x_2 \end{bmatrix},$$

- The local condition: $\{\mathbf{x} \in \mathbb{R}^3 : -2 \leq x_1, x_2, x_3 \leq 2\}$;

  The initial set: $\{\mathbf{x} \in \mathbb{R}^3 : (x_1 - 1/2)^2 + (x_2 - 3/2)^2 + (x_3 - 3/2)^2 \leq 1/4\}$;

  The unsafe set: $\{\mathbf{x} \in \mathbb{R}^3 : (x_1 + 1/2)^2 + (x_2 + 1/2)^2 + (x_2 + 1/2)^2 \leq 1/4\}$.
- The computed Darboux polynomial $p(\mathbf{x}) = 0.7332 x_3$.

System 3 [25].

$$\begin{bmatrix} \dot{x_1} \\ \dot{x_2} \\ \dot{x_3} \end{bmatrix} = \begin{bmatrix} x_1(1 - x_1 - x_2 - x_3) \\ x_2(1 - x_1 - x_2 - x_3) \\ x_3(1 - x_1 - x_2 - x_3) \end{bmatrix},$$

- The local condition: $\{\mathbf{x} \in \mathbb{R}^3 : -2 \leq x_1, x_2, x_3 \leq 2\}$;

  The initial set: $\{\mathbf{x} \in \mathbb{R}^3 : x_1^2 + (x_2 + 1)^2 + (x_3 + 1)^2 \leq 0.25\}$;

  The unsafe set: $\{\mathbf{x} \in \mathbb{R}^3 : (x_1 - 1)^2 + (x_2 - 1)^2 + (x_3 - 1)^2 \leq 0.25\}$.
- The computed Darboux polynomial $p(\mathbf{x}) = -0.6166 x_1 - 0.9661 x_2 - 0.9661 x_3$.

System 4 [9].

$$\begin{bmatrix} \dot{x_1} \\ \dot{x_2} \end{bmatrix} = \begin{bmatrix} x_1^2 + x_1 x_2 + x_1 \\ x_1 x_2 + x_2^2 + x_2 \end{bmatrix},$$

- The local condition: $\{\mathbf{x} \in \mathbb{R}^2 : -2 \leq x_1, x_2 \leq 2\}$;

  The initial set: $\{\mathbf{x} \in \mathbb{R}^2 : 0 \leq x_1, x_2 \leq 1\}$;

  The unsafe set: $\{\mathbf{x} \in \mathbb{R}^2 : (x_1 + 1/2)^2 + (x_2 + 1/2)^2 \leq 1/4\}$.
- The computed Darboux polynomial $p(\mathbf{x}) = 0.5689 x_1 + 0.5689 x_2$.

System 5 [9].

$$\begin{bmatrix} \dot{x_1} \\ \dot{x_2} \\ \dot{x_3} \end{bmatrix} = \begin{bmatrix} x_1^2 + x_1 x_2 - x_1 x_3 \\ 2x_1 x_2 + x_2^2 \\ x_2 x_3 - 2x_3^2 \end{bmatrix},$$

- The local condition: $\{\mathbf{x} \in \mathbb{R}^3 : -2 \leq x_1, x_2, x_3 \leq 2\}$;

  The initial set: $\{\mathbf{x} \in \mathbb{R}^3 : (x_1 - 3/2)^2 + (x_2 - 1/2)^2 + (x_2 - 3/2)^2 \leq 1/4\}$;

  The unsafe set: $\{\mathbf{x} \in \mathbb{R}^3 : (x_1 - 1/2)^2 + (x_2 - 3/2)^2 + (x_2 - 3/2)^2 \leq 1/4\}$.
- The computed Darboux polynomial $p(\mathbf{x}) = 0.5024 x_1^2 - 0.0168 x_2 x_3$.

System 6 [9].

$$\begin{bmatrix} \dot{x_1} \\ \dot{x_2} \end{bmatrix} = \begin{bmatrix} x_1^2 + 2x_1 x_2 + 3x_2^2 \\ 4x_1 x_2 + 2x_2^2 \end{bmatrix},$$

- The local condition: $\{\mathbf{x} \in \mathbb{R}^2 : -2 \leq x_1, x_2 \leq 2\}$;

  The initial set: $\{\mathbf{x} \in \mathbb{R}^2 : -1/2 \leq x_1 \leq 1/2, 1/2 \leq x_2 \leq 3/2\}$;

  The unsafe set: $\{\mathbf{x} \in \mathbb{R}^2 : (x_1 - 3/2)^2 + (x_2 - 1/2)^2 \leq 1/4\}$.
- The computed Darboux polynomial $p(\mathbf{x}) = -0.2525 x_1 + 0.2525 x_2$.

System 7 [9].

$$\begin{bmatrix} \dot{x_1} \\ \dot{x_2} \end{bmatrix} = \begin{bmatrix} x_1 - x_1 x_2 \\ -x_2 + x_1 x_2 \end{bmatrix},$$

- The local condition: $\{\mathbf{x} \in \mathbb{R}^2 : -2 \leq x_1, x_2 \leq 2\}$;

  The initial set: $\{\mathbf{x} \in \mathbb{R}^2 : -1 \leq x_1 \leq 0, 1/2 \leq x_2 \leq 3/2\}$;

  The unsafe set: $\{\mathbf{x} \in \mathbb{R}^2 : 1/2 \leq x_1 \leq 3/2, 0 \leq x_2 \leq 1\}$.
- The computed Darboux polynomial $p(\mathbf{x}) = 0.7332 x_1$.

System 8 [32].

$$\begin{bmatrix} \dot{x_1} \\ \dot{x_2} \end{bmatrix} = \begin{bmatrix} x_2 + 2x_1 x_2 \\ -x_1 + 2x_1^2 - x_2^2 \end{bmatrix},$$

- The local condition: $\{\mathbf{x} \in \mathbb{R}^2 : -2 \leq x_1, x_2 \leq 2\}$;

  The initial set: $\{\mathbf{x} \in \mathbb{R}^2 : 0 \leq x_1 \leq 1, 1 \leq x_2 \leq 2\}$;

  The unsafe set: $\{\mathbf{x} \in \mathbb{R}^2 : x_1 + x_2^2 \leq 0\}$.
- The computed Darboux polynomial $p(\mathbf{x}) = -1 + 2x_1 - 1.6x_1^2 + 2.4x_2^2$.

System 9 [23].

$$\begin{bmatrix} \dot{x_1} \\ \dot{x_2} \end{bmatrix} = \begin{bmatrix} x_2 \\ -x_1 + \frac{1}{3}x_1^3 - x_2 \end{bmatrix},$$

- The local condition: $\{\mathbf{x} \in \mathbb{R}^2 : -2 \leq x_1, x_2 \leq 2\}$;

  The initial set: $\{(x_1, x_2) \in \mathbb{R}^2 : (x_1 - 1.5)^2 + x_2^2 \leq 0.25\}$;

  The unsafe set: $\{\mathbf{x} \in \mathbb{R}^2 : (x_1 + 1)^2 + (x_2 + 1)^2 \leq 0.16\}$.

System 10 [The Raychaudhuri polynomial system [7]].

$$\begin{bmatrix} \dot{x_1} \\ \dot{x_2} \\ \dot{x_3} \\ \dot{x_4} \end{bmatrix} = \begin{bmatrix} -\frac{1}{2}x_1^2 - \frac{1}{2}x_2^2 - \frac{1}{8}x_3^2 - 2x_2 x_3 + 2x_4^2 + 1 \\ -x_1 x_2 - 1 \\ -x_1 x_3 \\ -x_1 x_4 \end{bmatrix},$$

- The local condition: $\{\mathbf{x} \in \mathbb{R}^4 : -2 \leq x_1, x_2, x_3, x_4 \leq 2\}$;

  The initial set: $\{\mathbf{x} \in \mathbb{R}^4 : (x_1 - 1)^2 + (x_2 - 1)^2 + (x_3 - 1)^2 + (x_4 - 1)^2 \leq \frac{1}{4}\}$;

  The unsafe set: $\{\mathbf{x} \in \mathbb{R}^4 : (x_1 + 1)^2 + (x_2 + 1)^2 + (x_3 + 1)^2 + (x_4 + 1)^2 \leq \frac{1}{4}\}$.
- The computed Darboux polynomial $p(\mathbf{x}) = x_4$.

System 11 [Modified Einstein-Yang-Mills system [19]].

$$\begin{bmatrix} \dot{x_1} \\ \dot{x_2} \\ \dot{x_3} \\ \dot{x_4} \\ \dot{x_5} \\ \dot{x_6} \end{bmatrix} = \begin{bmatrix} x_1 x_3 \\ x_1 x_5 \\ (x_4 - x_3)x_3 - 2x_5^2 \\ -(x_4 - x_3)^2 + s(-ax_1^2 + x_6^2) \\ s x_2 x_6 + (x_3 - x_4)x_5 \\ 2x_2 x_5 - x_3 x_6 \end{bmatrix},$$

where $s = 1$ and $a = 1$.

- The local condition: $\{\mathbf{x} \in \mathbb{R}^6 : -2 \leq x_1, x_2, x_3, x_4,\ x_5,\ x_6 \leq 2\}$;

  The initial set: $\{\mathbf{x} \in \mathbb{R}^6 : 1 \leq x_1, x_2, x_3, x_4, x_5, x_6 \leq 2\}$;

  The unsafe set: $\{\mathbf{x} \in \mathbb{R}^2 : -1 \leq x_1, x_2, x_3, x_4,\ x_5,\ x_6 \leq -0.5\}$.
- The computed Darboux polynomial $p(\mathbf{x}) = 0.7332 x_1$.