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 non-linear 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 paper proposes a set of verification conditions that can build a new type of barrier certificate: the Darboux-type barrier certificate made of Darboux polynomials. Compared with existing barrier certificate which gives a rough over approximation of the reachable set, 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 using 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 alone 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 Gröbner 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. [10] checked its forward invariance by verifying it on a finite number of points selected by δ—sampling from the set. Bobbi et al. [4] 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 methods with less 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 time number of first-order ordinary differential equations

$$\dot{x} = f(x),$$

where $x$ denotes the derivative of $x$ with respect to the time variable $t$, and $f(x)$ is called vector field $f(x) = (f_1(x), \ldots, f_n(x))$ defined on an open set $\psi \subseteq \mathbb{R}^n$. We assume that $f$ satisfies the local Lipschitz condition, which ensures that given $x = x_0$, there exists a time $T > 0$ and a unique trajectory $\tau : [0, T] \rightarrow \mathbb{R}^n$ such that $\tau(t) = x_0$. And $x(t)$ is called a solution of (1) that starts at a certain initial state $x_0$, that is, $x(0) = x_0$. Namely, $x(t)$ is also called a trajectory of (1) from $x_0$.

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

Definition 1. (Hybrid system) A hybrid system $H : (V, L, T, \Theta, D, \Psi, \ell_0)$ consists of the following components:

- $V = \{x_1, \ldots, x_n\}$, 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 $\varphi$, written as $s \models \varphi$, if $\varphi$ holds on the state $s$. We will also write $s \models \varphi_1 \land \varphi_2$ for two assertions $\varphi_1, \varphi_2$ to denote that $\varphi_2$ is true at least in all the states in which $\varphi_1$ is true;

- $L$, a finite set of locations;

- $T$, a set of (discrete) transitions. Each transition $\tau : (\ell, \ell', g_\tau, \rho_\tau) \in T$ consists of a prelocation $\ell \in L$, a postlocation $\ell' \in L$, the guard condition $g_\tau$ over $V$, and an assertion $\rho_\tau$ over $V \cup V'$ representing the next-state relation, where $V' = \{x_1', \ldots, x_n'\}$ denotes the next-state variables. Note that the transition $\tau$ can take place only if $g_\tau$ holds;

- $\Theta$, an assertion specifying the initial condition;

- $D$, a map that associates each location $\ell \in L$ to a differential rule (also known as a vector field) $D(\ell)$, an autonomous system $\dot{x}_i = f_i(x)$ for each $x_i \in V$, written briefly as $\dot{x} = f(x)$. The differential rule at a location specifies how the system variables evolve in that location;

- $\Psi$, 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 $H : (V, L, T, \Theta, D, \Psi, \ell_0)$, we mean the tuple $(\ell, x) \in L \times \mathbb{R}^n$ where $n$ is the number of program variables in $H$. A trajectory [31] of $H$ is an infinite sequence of states $(\ell_0, x_0), (\ell_1, x_1), \ldots, (\ell_i, x_i), (\ell_{i+1}, x_{i+1}), \ldots$ such that

- [Initiation] $\ell_0 = \ell_0$ and $x_0 \models \Theta$;

- [Discrete Consequence] There exists a transition $\tau : (\ell, \ell', g_\tau, \rho_\tau)$ such that $\ell_i = \ell, \ell_{i+1} = \ell'$ and $(x_i, x_{i+1}) \models \rho_\tau(x_i, x_{i+1})$ if $g_\tau$ holds, or

- [Continuous Consequence] $\ell_i = \ell_{i+1} = \ell$, and there exists a time interval $\delta > 0$ and a smooth (continuous and differentiable to all orders) function $f : [0, \delta] \rightarrow \mathbb{R}^n$ s.t. $f$ evolves from $x_i$ to $x_{i+1}$ according to the differential rule $D(\ell)$ at location $\ell$, while satisfying the location invariant $\Psi(\ell)$. Formally,

$$- f(0) = x_i, f(\delta) = x_{i+1} \text{ and } \forall t \in [0, \delta), f(t) \models \Psi(\ell),$$

- $\forall t \in [0, \delta), (f(t) \models D(\ell))$.

A state $(\ell, x)$ is called a reachable state of a hybrid system $H$ from the initial state set $\Theta$ if it appears in some trajectory of $H$. During a continuous flow, the discrete location $\ell_t$ is maintained and the continuous state variables $x$ evolve according to the differential equations $x = f(x)$, with $x$ satisfying the location invariant $\Psi(\ell_t)$. At the state $(\ell, x)$, if the guard condition $g(\ell_t, \ell'_t)$ is met, the system may undergo a transition to location $\ell_{t+1}$, and $x$ will take the new value $x'$, which is determined by the reset map $\rho(\ell_t, \ell'_t)$.

Given a hybrid system $H$ with prespecified unsafe assertion $X_u$, we say that the system $H$ is safe if all trajectories of $H$ starting from the initial condition $\Theta$ at the initial location $\ell_0$ 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 $H : (V, L, T, \Theta, D, \Psi, \ell_0)$ and an unsafe assertion $X_u$, determine whether $H$ 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 \( f(x) \) be a vector field \( f : (f_1(x), \ldots, f_n(x)) \), the Lie derivative of a smooth function \( g(x) \) with respect to \( f(x) \) is given by

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

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

\[
\mathcal{L}_f(p(x)) = p(x)
\]

where \( c(x) \in \mathbb{R}[x] \) is a polynomial called the cofactor. When \( c(x) \) is a zero polynomial, \( p(x) \) 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 \( p(x) \) is a Darboux polynomial with respect to \( f(x) \), and \( x(t) \) is a trajectory of (1) starting from \( x_0 \), i.e., \( x(0) = x_0 \). If \( p(x_0) \geq 0 \), then \( p(x(t)) \geq 0 \) for all \( t > 0 \).

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

\[
\frac{d(p(x(t)))}{p(x(t))} = c(x(t)) \, dt.
\]

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

\[
p(x(t)) = p(x_0) \cdot e^{\int c(x(s)) \, ds}.
\]

We then derive that \( p(x(t)) \geq 0 \) for all \( t > 0 \) if \( p(x_0) \geq 0 \).

3. DARBOUX POLYNOMIALS 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 \( \Theta \) and an unsafe set \( X_u \), a barrier certificate is a real-valued function \( p(x) \) of states satisfying that \( p(x) \geq 0 \) for any point \( x \) in the reachable set \( R \) and \( p(x) < 0 \) for any point in the unsafe set \( X_u \) (called general constraint hereafter). Therefore, if there exists such a function \( p(x) \), we can assert that \( R \cap X_u = \emptyset \), which has determined the system cannot reach a state in the unsafe set from the initial set. In fact, the condition \( p(x) \geq 0 \) can be seen as an inductive invariant for the specified barrier certificate \( p(x) \). However, the exact reachable set is really computation hard, so we cannot determine whether \( p(x) \geq 0 \) 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 \( \Theta, X_u \) 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 \( \Theta \) and \( X_u \), if there exists a barrier certificate, i.e., a real-valued function \( p(x) \) which is a Darboux polynomial, satisfying the following formulae:

- (i) \( \Theta \models p(x) \geq 0 \),
- (ii) \( X_u \models p(x) < 0 \),

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

Proof. If there is a Darboux polynomial \( p(x) \) which satisfies conditions (i) and (ii) above, then \( p(x_0) \geq 0 \) holds for any point \( x_0 \) chosen from the initial set \( \Theta \). Therefore, based on lemma 1, \( p(x(t)) \) will keep non-negative for any state along the trajectory from the point \( x_0 \). And it cannot evolve to \( X_u \) because of \( X_u \models p(x) < 0 \) 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 \( p_t(x) \) are also known as barrier certificates.

Theorem 2. Let \( H = (V, L, T, \Theta, D, \Psi, \ell_0) \) be a hybrid system, and \( X_u(\ell) \) be the unsafe assertion at location \( \ell \). Suppose for each location \( \ell \in L \), there exists a Darboux polynomial \( p_t(x) \), that satisfy the following conditions:

- (i) \( \Theta \models p_t(x) \geq 0 \),
- (ii) \( g(\ell, \ell') \land \rho(\ell, \ell') \models p_t(\lambda_{\ell,\ell'}(x)) p_t(x) \geq 0 \), where \( \lambda_{\ell,\ell'}(x) \) is the next state specified by \( \rho(\ell, \ell') \) in relation to the previous state \( x \), and \( \lambda_{\ell,\ell'}(x) \in \mathbb{R}[x] \) is a nonnegative polynomial, for any transition \((\ell', \ell, g, \rho)\) going out of \( \ell \),
- (iii) \( X_u(\ell) \models p_t(x) < 0 \),

then \( p_t(x) \) is a barrier certificate of the hybrid system \( H \) at location \( \ell \), and the safety of \( H \) is guaranteed.

Proof. From condition (i), \( p_t(x) \) is nonnegative over the initial state given by \( \Theta \). And Lemma 1 implies that \( p_t(x) \) cannot become negative during the continuous flow. Moreover, condition (ii) guarantees that \( p_t(x) \) keeps non-negative during a discrete transition. Thus, \( p_t(x) \geq 0 \) is an inductive invariant of \( H \) at location \( \ell \). Then, condition (iii) implies that all reachable states of \( H \) 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 \( p(x) = 0 \) can be regard as a “barrier” between possible system trajectories and the given unsafe region. If choosing an initial point \( x(t_0) \) from a given set which goes along the state function, it would not change the sign of \( p(x(t)) \) for \( t \geq t_0 \) afterwards. In other words, it will not go across the guard \( p(x) = 0 \). 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 problems. 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 $p_i(x) = \sum_{\alpha} p_{i,\alpha} x^\alpha$, where $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$, $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}_{\geq 0}^n$ with $\sum_{i=1}^n \alpha_i \leq d$, and $p_{i,\alpha} \in \mathbb{R}$ being parameters. We can rewrite $p_i(x) = c_i^T \ell_i(x)$, where $\ell_i(x)$ is the (column) vector of all monomials in $x_1, \ldots, x_n$ with total degree $\leq d$, and $c_i \in \mathbb{R}^n$ is the coefficient vector of $p_i(x)$ with $\nu = \binom{n}{\mathbb{Z}_{\geq 0}^n}$.

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

$$\begin{aligned}
\text{find } p_i(x) \in \mathbb{R}[x], \forall \ell \in L &\text{ s.t. } L_i(p_i(x)) = c_i(x) \cdot p_i(x), \\
&\Theta \mathrel{\lvert} p_{i,\ell}(x) \geq 0, \\
g(\ell, \ell') \mathrel{\land} \rho(\ell, \ell') = p_i(x') - \lambda_{\ell,\nu} \mathrel{\lvert} p_{i,\ell}(x) \geq 0, \\
X_\ell(x) \mathrel{\lvert} p_{i,\ell}(x) < 0.
\end{aligned}$$

(2)

Observing the equality constraint in (2), we can set the degree of the cofactor $c_i(x)$. Similar to the template of $p_i(x)$, let the coefficients of $c_i(x)$ be parameters, and write $c_i(x)$ as $c_i(x) = c_i^T \ell_i(x)$, where $c_i$ and $T_i(x)$ are the coefficient vector and the monomial vector of $c_i(x)$, respectively. We can rewrite the equality constraint in (2) as a quadratic system with the variables $p$, $c_i$ by sorting the coefficients with respect to the variables $x$, that is,

$$L_i(p_i(x)) = c_i(x) \cdot p_i(x) \iff T_i(p, c_i) = 0. \quad (3)$$

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

$$\Omega_{\ell, \ell'} = [\tilde{p}_{i,\ell}(x) \geq 0, \quad (4)$$

where $\Omega_{\ell, \ell'} = \{x \in \mathbb{R}^n \mathrel{\lvert} g(\ell, \ell') \mathrel{\land} \rho(\ell, \ell')\}$.

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

$$\begin{aligned}
\text{find } p_i \in \mathbb{R}^n, \forall \ell \in L &\text{ s.t. } F_i(p_i, c_i) = 0, \\
&\tilde{p}_{i,\ell}(x, p_i) \geq 0, \quad \forall x \in \Theta, \\
&\tilde{p}_{i,\ell'}(x, p_i, p_{i,\ell'}) \geq 0, \quad \forall x, x' \in \Omega_{\ell, \ell'}, \\
&\tilde{p}_{i,\ell}(x, p_i) < 0, \quad \forall x \in X_\ell(x).
\end{aligned}$$

(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) 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 $p, c, c_i$ in the polynomial optimization problem (5) is not small. Taking into 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.,

$$-p(x, p) - \epsilon \geq 0 \implies p(x, p) < 0.$$

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

$$p^T = [p_{i,0}, p_{i,1}, \ldots], \quad c^T = [c_{i,0}, c_{i,1}, \ldots].$$

The dimension of $p$ is denoted as $\omega$ hereafter.

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

$$\begin{aligned}
\text{find } p &\text{ s.t. } F(p, c) = 0, \\
&\tilde{p}_{i,\ell}(x, p) \geq \epsilon, \quad \forall x \in \Omega_{\ell, i}, i = 1, 2, \ldots, k.
\end{aligned} \quad (6)$$

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

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 $\omega_i, 1 \leq i \leq k$, we let us first construct a rectangular mesh $M$ in $\omega_i$ with a mesh spacing $r \in \mathbb{R}_+$ (say $r = 0.05$) and mesh point set $\chi_i = \{x_1, x_2, \ldots, x_{\omega_i}\}$. Given a continuously differentiable function $\phi(x)$ over the compact domain $\Omega_i$ and let $x \in \Omega_i$ and $x + \Delta x \in \Omega_i$ be chosen randomly, then the mean value theorem yields that

$$|\phi(x + \Delta x) - \phi(x)| \leq m(|\Delta x|) \sup_{x \in \Omega_i} \|\nabla \phi(x)\|_{\infty}, \quad (7)$$

where $m = \sup_{x \in \Omega_i} \|\nabla \phi(x)\|_{\infty}$.

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

$$p_i(x, p) - \delta_i \geq 0, \quad 1 \leq j \leq m_i \implies \tilde{p}_{i,\ell}(x, p) \geq 0, \quad \forall x \in \Omega_{\ell, i}. \quad (8)$$

We should illustrate how to determine $\delta_i$. In fact, when given objective system $H$, each $\omega_i$ is determined. Then the associate $\delta_i$ can be determined, after deciding the sampling mesh spacing size $r$. For simplify, we just compute $\delta_i = m_{\Omega_{\ell, i}} \in \mathbb{R}_{>0}$ where $m_{\Omega_{\ell, i}} = \sup_{x \in \Omega_{\ell, i}} \|\nabla \phi(x)\|_{\infty}$.

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

$$\begin{aligned}
\text{find } p &\text{ s.t. } F(p, c) = 0, \\
&\tilde{p}_{i,\ell}(x, p) - \delta_i \geq 0, \quad 1 \leq i \leq k, \quad 1 \leq j \leq m_i, \\
&-E \cdot p + D \geq 1, \quad \omega \cdot p + D \geq 1.
\end{aligned}$$
where $E \in \mathbb{R}^{n \times n}$ 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 $\delta_i$, 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:

$\begin{align*}
\text{min} & \quad \| \mathbf{c} \|_2 \quad \text{s.t.} \quad \mathbf{F}(\mathbf{p}, \mathbf{c}) = 0, \\
& \quad \mathbf{A} \cdot \mathbf{p} \geq \mathbf{b},
\end{align*}$

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

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

**Remark 1.** The smaller the mesh size is, the closer each $\delta_i$ gets to zero, i.e., $\lim_{\delta_i \to 0} \mathbf{c}(i) = \mathbf{c}$. Moreover, it wouldn’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 $\delta = 0.1$ for the fixed coefficient bound $D = 1$ in the sequel of the 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 following nonlinear system:

$\begin{align*}
\dot{x} &= -x + 2x^2y \\
y &= -y
\end{align*}$

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

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

will never enter the unsafe region

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

As explained in Section 4, we first set the degree $d = 1$, the mesh size $s = 0.5$ for $\Theta$ and $X_u$, then set the template for the Darboux polynomial $p(x, y)$ and its co-factor $c(x, y)$ as $p(x, y) = p_x x + p_y y + p_0$ and $c(x, y) = c_1 x + c_2 y + c_3$, respectively.

Let $\mathbf{p} = [p_1, p_2, p_0]^T$ 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:

$\begin{align*}
\text{min} & \quad \| \mathbf{c} \|_2 \\
\text{s.t.} & \quad f_1(\mathbf{p}, \mathbf{c}) = f_2(\mathbf{p}, \mathbf{c}) = \cdots = f_{11}(\mathbf{p}, \mathbf{c}) = 0, \\
& \quad A \cdot \mathbf{p} \geq \mathbf{b},
\end{align*}$

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 $\mathbf{p}^{(0)} = [0.5, 2, 0]^T$, 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 cross-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:

$\min_{\mathbf{c}} \| F(\mathbf{p}^*, \mathbf{c}) \|_2$. Likewise, once $\mathbf{c}$ is fixed by $\mathbf{c}^*$, then (9) is translated into the following problem:

$\begin{align*}
\text{min} & \quad \| \mathbf{p} \|_2 \\
\text{s.t.} & \quad F(\mathbf{p}, \mathbf{c}^*) = 0, \\
& \quad A \cdot \mathbf{p} \geq \mathbf{b},
\end{align*}$

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 $\mathbf{p}^{(k)} = [p_1^{(k)}, \ldots, p_{11}^{(k)}]^T$, which is the optimal value obtained from the $k$-th iteration, we need solve the optimal value for $\mathbf{c}$, i.e.,

$\min_{\mathbf{c}} \| F(\mathbf{p}^{(k)}, \mathbf{c}) \|_2$.□

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

$\min_{\mathbf{e}} \| F(\mathbf{e}^{(k)} + \Delta \mathbf{e}) \|_2$,

$\mathbf{e}^{(k+1)} := \mathbf{e}^{(k)} + \Delta \mathbf{e} \neq 0$. (13)

For convenience, we denote the solution of (13) as $
\Delta \mathbf{e} = \text{update}_1(F)$. □
Let $c$ be fixed by $c^{(k+1)}$, and then update $p$ by solving the following optimization problem
\[
\begin{aligned}
\min \left[ |\Delta p| \right] & \quad \text{subject to} \\
F(p^{(k)} + \Delta p), c^{(k+1)} &= 0, \\
A \cdot (p^{(k)} + \Delta p) &\geq b,
\end{aligned}
\] (14)
where $p^{(k+1)} = p^{(k)} + \Delta p \neq 0$. Similarly, the solution of (14) is denoted by
\[
\Delta p = \text{update}_2(F).
\]

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

**Algorithm 1** LS-QP alternating projection

**Require:** Sampling point set $\chi$ and functions $F$;

**Ensure:** Darboux polynomial $p(x)$

1: Establish the optimization problem (11) from $\chi$ and $F$;
2: Generate some initial vectors $c^{(0)}$ and $p^{(0)}$;
3: for $k = 1, 2, \ldots$ do;
4: \quad $c^{(k)} = c^{(k-1)} + \text{update}_1(F, p^{(k-1)})$;
5: \quad $p^{(k)} = p^{(k-1)} + \text{update}_2(F, c^{(k)})$;
6: end for.

\[† \text{ See Remark 4 in this section for stopping criteria.}\]

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

**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 $||\text{update}_1(F, p^{(k-1)})|| < \sigma$ and $||\text{update}_2(F, c^{(k)})|| < \sigma$ at $k$-th iteration for a given tolerance $\sigma$(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.

**Example 2.** Consider the the hybrid system depicted in Figure 2, where
\[
f_1(x) = \begin{bmatrix} x_1 - x_1x_2 \\ -x_2 + x_1x_2 \end{bmatrix}, \quad f_2(x) = \begin{bmatrix} x_1 + x_1^2x_2 \\ x_2 + x_1x_2 \end{bmatrix}.
\]
The system starts in location $\ell_1$ 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
\[
X_1(\ell_1) = \{(x_1, x_2) \in \mathbb{R}^2 : 0 \leq x_1, 1 \leq x_2 \leq -1\}.
\]
By applying our method, we can obtain two Darboux polynomials at locations $\ell_1$ and $\ell_2$:
\[
r_{\ell_1}(x) = 0.7332x_1, \quad r_{\ell_2}(x) = 0.7332x_1x_2,
\]
which satisfy all the conditions in Theorem 2. Then, the safety property of this system is guaranteed.

**Example 3.** Consider the hybrid system depicted in Figure 3, where
\[
f_1(x) = \begin{bmatrix} -x_1 + x_1x_2 \\ -x_2 \end{bmatrix}, \quad f_2(x) = \begin{bmatrix} -x_1 + 2x_1^2x_2 \\ -x_2 \end{bmatrix}.
\]
The system starts in location $\ell_1$ 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
\[ X_u(t_2) = \{(x_1, x_2) \in \mathbb{R}^2 : (x_1 - 2)^2 + (x_2 - 2)^2 \leq 0.25\}. \]

By applying our method, we can obtain two Darboux polynomials at locations \( \ell_1 \) and \( \ell_2 \):
\[
\begin{align*}
p_{\ell_1}(x) &= 0.7332x_2, \\
p_{\ell_2}(x) &= -0.2711x_1x_2 + 0.2711,
\end{align*}
\]
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 \( \{B_\ell(x), \forall \ell \in L\} \) such that the following conditions hold:
\[
\begin{align*}
B_{\ell_0}(x) &\leq 0 \forall x \in \Theta, \\
B_{\ell_0}(x) - B_{\ell}(x) &> 0 \forall x \in \Theta, \\
\gamma_{\ell, \ell'} B_{\ell}(x') &\geq 0 \forall x' \in g(\ell, \ell', x), \\
B_{\ell}(x) &> 0 \forall x \in X_u(\ell),
\end{align*}
\]
for some real numbers \( \lambda_\ell \) 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 \( \{B_\ell(x), \forall \ell \in L\} \), each of which satisfies
\[
\begin{align*}
B_{\ell_0}(x) &\leq 0 \forall x \in \Theta, \\
B_{\ell_0}(x) - B_{\ell}(x) &> 0 \forall x \in \Theta, \\
B_{\ell}(x) &> 0 \forall x \in X_u(\ell)
\end{align*}
\]
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 \( \rho(x) \). 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; \( \text{Fail} \) means that the method fails to find the barrier certificates with degree \( \leq 6 \).

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


<table>
<thead>
<tr>
<th>ID</th>
<th>n</th>
<th>( \deg(B) )</th>
<th>LMI</th>
<th>( \deg(p) )</th>
<th>BMI</th>
<th>( \deg(p) )</th>
<th>LS-QP</th>
<th>( \deg(p) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>2</td>
<td>Fail</td>
<td>1</td>
<td>0.8744</td>
<td>1</td>
<td>0.4534</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>2</td>
<td>Fail</td>
<td>2</td>
<td>0.8744</td>
<td>2</td>
<td>0.6348</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>2</td>
<td>Fail</td>
<td>1</td>
<td>1.001</td>
<td>1</td>
<td>1.0154</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>2</td>
<td>2</td>
<td>Fail</td>
<td>2</td>
<td>1.001</td>
<td>2</td>
<td>1.0154</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>2</td>
<td>2</td>
<td>Fail</td>
<td>3</td>
<td>5.0523</td>
<td>2</td>
<td>1.3333</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>2</td>
<td>2</td>
<td>Fail</td>
<td>1</td>
<td>1.001</td>
<td>2</td>
<td>1.0154</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>2</td>
<td>2</td>
<td>0.2916</td>
<td>2</td>
<td>1.4047</td>
<td>1</td>
<td>0.317</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>2</td>
<td>2</td>
<td>0.2916</td>
<td>2</td>
<td>1.4047</td>
<td>2</td>
<td>0.9237</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>3</td>
<td>3</td>
<td>0.4623</td>
<td>2</td>
<td>1.001</td>
<td>Fail</td>
<td>2</td>
<td>0.9237</td>
</tr>
<tr>
<td>10</td>
<td>2</td>
<td>2</td>
<td>10.8844</td>
<td>2</td>
<td>1.001</td>
<td>Fail</td>
<td>1</td>
<td>0.9237</td>
</tr>
<tr>
<td>11</td>
<td>2</td>
<td>2</td>
<td>27.2566</td>
<td>2</td>
<td>65.3519</td>
<td>1</td>
<td>14.0610</td>
<td></td>
</tr>
</tbody>
</table>
Appendix: Benchmark Examples

System 1 [25].

\[
\begin{bmatrix}
\dot{x}_1 \\
\dot{x}_2 \\
\end{bmatrix} = \begin{bmatrix}
x_1 + 2x_3^2 x_2 \\
-x_2
\end{bmatrix}.
\]

- The local condition: \( \{ x \in \mathbb{R}^2 : -2 \leq x_1, x_2 \leq 2 \} \);
- The initial set: \( \{ x \in \mathbb{R}^2 : -1/2 \leq x_1, 1/2 \leq x_2 \leq 3/2 \} \);
- The unsafe set: \( \{ x \in \mathbb{R}^2 : (x_1 - 3/2)^2 + (x_2 - 1/2)^2 \leq 1/4 \} \);
- The computed Darboux polynomial \( p(x) = -0.7959x_1 + 0.7195 \).

System 2 [25].

\[
\begin{bmatrix}
x_1 \\
x_2 \\
x_3
\end{bmatrix} = \begin{bmatrix}
x_1 - x_1 x_2 \\
x_2 - 2x_2 x_3 \\
x_3 + x_3 x_1 + x_3 x_2
\end{bmatrix}.
\]

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

System 3 [25].

\[
\begin{bmatrix}
\dot{x}_1 \\
\dot{x}_2 \\
\dot{x}_3
\end{bmatrix} = \begin{bmatrix}
x_1 (1 - x_1 - x_2 - x_3) \\
x_2 (1 - x_2 - x_1 - x_3) \\
x_3 (1 - x_1 - x_2 - x_3)
\end{bmatrix}.
\]

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

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: \( \{ x \in \mathbb{R}^2 : -2 \leq x_1, x_2 \leq 2 \} \);
- The initial set: \( \{ x \in \mathbb{R}^2 : 0 \leq x_1, x_2 \leq 1 \} \);
- The unsafe set: \( \{ x \in \mathbb{R}^2 : (x_1 + 1/2)^2 + (x_2 + 1/2)^2 \leq 1/4 \} \);
- The computed Darboux polynomial \( p(x) = 0.5689x_1 + 0.5689x_2 \).

System 5 [9].

\[
\begin{bmatrix}
\dot{x}_1 \\
\dot{x}_2 \\
\dot{x}_3
\end{bmatrix} = \begin{bmatrix}
x_1 x_2 + x_2^2 - x_1 x_3 \\
x_2 x_3 + x_2 x_3 + x_2^2 \\
x_2 x_3 - x_2^2
\end{bmatrix}.
\]

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

System 6 [9].

\[
\begin{bmatrix}
\dot{x}_1 \\
\dot{x}_2
\end{bmatrix} = \begin{bmatrix}
x_1 x_2 + x_1 x_2 + 3x_2^2 \\
x_1 x_2 + 2x_2^2
\end{bmatrix}.
\]

- The local condition: \( \{ x \in \mathbb{R}^2 : -2 \leq x_1, x_2 \leq 2 \} \);
- The initial set: \( \{ x \in \mathbb{R}^2 : -1/2 \leq x_1, 1/2 \leq x_2 \leq 3/2 \} \);