Safety Verification of Nonlinear Autonomous System via Occupation Measures

Ximing Chen, Shaoru Chen, Victor M. Preciado

Abstract—In this paper, we introduce a new notion of safety verification of nonlinear systems by considering how much time the system spends in given unsafe regions. We formulate this problem as an infinite-dimensional linear program (LP) by computing the volume of the unsafe region with respect to occupation measures. Using Lasserre hierarchy of moment relaxations, a sequence of finite-dimensional semidefinite programs (SDPs) are solved which give monotonically converging upper bounds on the optimal value of the infinite-dimensional LP. Finally, we numerically validate the performance of our framework using several dynamical systems.

I. INTRODUCTION

The advances of technologies enable people to build complicated devices and systems. Along with the rise of these systems, there is an increasing need for developing frameworks to verify whether these systems will behave undesirably. The capability of providing a safety certificate for complicated systems can be critical in various engineering applications such as air traffic control [1], life support devices [2], motion planning in robotics manipulations [3] as well as connected autonomous vehicles [4, 5]. In principle, the objective of safety verification is to provide a quantitative certificate on the probability of a system evolving into some unsafe regions. Nonetheless, this problem is challenging when the underlying system is captured by nonlinear differential equations or the unsafe region is characterized by nonconvex algebraic objects [6, 7].

In the past decades, various solutions have been proposed to verify the safety of dynamical systems. The solution approaches often fall into the following two categories: (i) reachable set based methods and (ii) Lyapunov function based methods [8–11]. Essentially, reachable set based methods aim to find a set containing all possible states at a given time instance that evolve from a given initial condition. Subsequently, if the reachable set does not intersect with the pre-specified unsafe regions, the system can be considered as safe. For example, in [12] the reachable set is found for continuous-time linear systems whereas in [13] and [14], the reachable sets are computed via approximations for nonlinear dynamical systems. In [15], the author applied a reachable set based method to plan safe trajectories for autonomous vehicles.

While reachable set based methods can be used to obtain quantitative guarantees for safety, the reliability of the result largely depends on the assumptions on the system as well as the form of the unsafe regions. For instance, calculating the volume of the intersection of two sets can become computationally challenging [7]; hence jeopardizing the result given by reachable set based methods. An alternative approach to the safety verification problem is through Lyapunov-like functions. In [16], the authors proposed to construct barrier certificates for safety verification of nonlinear systems. Comparing with the reachable set based method, this line of work does not require to solve differential equations and is more computationally favorable. Furthermore, it is also amenable to provide safety certificates for various types of hybrid [8] and stochastic systems [10].

Despite a tremendous amount of solutions proposed to solve the safety verification problem, the majority of existing methods only provide binary safety certificates. More specifically, these certificates concern only whether the system is safe rather than how safe the system is. Lacking a detailed analysis of how unsafe a system is may result in a restricted and conservative design space. For example, we consider the operation of a solar-powered autonomous vehicle. Naturally, regions without solar exposure are considered to be unsafe. However, in this scenario, it is undesirable to plan a path for the vehicle that avoids all these regions. Instead, a more preferred requirement is that the amount of time the vehicle spends in this region is bounded.

In this paper, we propose to consider a different notion of safety. More precisely, we aim to compute the time that a (nonlinear) system spends in the unsafe regions. To calculate this value, we leverage a recent lifting technique called the occupation measure, i.e., a measure describing how much time the system trajectory spends in a particular set [16]. Using this alternative viewpoint on the system dynamics, the safety quantity of interest can be calculated by finding the volume of the unsafe region [17]. Occupation measure not only gives a natural description of safety, but also provides a powerful numerical procedure for various optimization problems of nonlinear systems with polynomial dynamics [18–20] by solving a sequence of semidefinite programs.

The contribution of this paper is threefold. First, we formulate a new safety certificate for nonlinear systems, which enriches the set of potential system design strategies by allowing a trade-off between safety and performance. Second, we provide an exact solution to the problem under consideration via infinite-dimensional linear programming. Furthermore, we provide convergent approximated solutions to the LP of interest. Finally, we provide numerical examples

The authors are with the Department of Electrical and Systems Engineering at the University of Pennsylvania, Philadelphia PA 19104. e-mail: {ximingch, srchen, preciado}@seas.upenn.edu.
to demonstrate the applicability of our method.

The rest of the paper is structured as follows. The safety verification problem formulation is given in Section II. In Section III, we introduce concepts in measure theory that are necessary for developing our solution framework. Based on those notions, we show that the problem under consideration can be solved using an infinite-dimensional linear program. In Section IV, we provide approximated solutions to the LP using a sequence of semidefinite or sum-of-squares programs. The performance of our framework is demonstrated through numerical experiments in Section V and we conclude the paper in Section VI.

**Notations:** We use bold symbols to represent vectors with real entries. Given \( n \in \mathbb{N} \), we use the shorthand notation \([n]\) to denote the set of integers \( \{1, \ldots, n\} \). The indicator function of a given set \( S \) is defined by \( 1_S(\cdot) \). We use \( \delta_x \) to denote the Dirac measure centered on a fixed point \( x \in \mathbb{R}^n \) and we denote by \( \otimes \) the product between measures. The ring of polynomials in \( x \) is denoted by \( \mathbb{R}[x] \). Let \( \mathbb{R}[x]_r \) be the set of polynomials in \( x \) of degree \( \leq r \).

II. Problem Statement

In this paper, we consider a continuous-time autonomous dynamical system whose dynamics are captured by the following equation:

\[
\dot{x}(t) = f(t, x), \quad t \in [0, T] \\
x(0) = x_0
\]

(1)

where \( x(t) \in \mathbb{R}^n \) is the state vector, \( x_0 \) is the initial condition and \( T > 0 \) is the terminal time. We consider that the states of (1) are constrained within the set \( \mathcal{X} \subseteq \mathbb{R}^n \) for all \( t \in [0, T] \). Furthermore, we consider that the system evolves from an initial condition \( x_0 \) with \( x_0 \in \mathcal{X}_0 \subseteq \mathcal{X} \). In this paper, we are interested in the case that the set \( \mathcal{X} \) is semi-algebraic.

**Definition 1.** A set \( K \subseteq \mathbb{R}^n \) is said to be a semi-algebraic set if there exist \( m \) polynomials \( g_i : \mathbb{R}^n \to \mathbb{R} \) such that

\[
K = \{ x \in \mathbb{R}^n \mid g_i(x) \geq 0, \forall i \in [m] \}.
\]

(2)

In other words, the set \( \mathcal{X} \) can be captured equivalently using polynomials as follows:

\[
x(t) \in \mathcal{X} \iff \{ x \in \mathbb{R}^n \mid g_i^X(x) \geq 0, \forall i \in [n, \bar{n}] \}
\]

(3)

for all \( t \in [0, T] \). The assumption on \( \mathcal{X} \) can be easily satisfied by picking \( \mathcal{X} \) as a large ball \( \{ x : M^2 - ||x||^2 \geq 0 \} \) with radius \( M \).

In this paper, we consider the following problem of safety verification:

**Problem 1.** Given compact and semi-algebraic sets \( \mathcal{X} \) defined by (3) and \( \mathcal{X}_0 \subseteq \mathcal{X} \) defined by

\[
\mathcal{X}_0 = \{ x \in \mathbb{R}^n \mid g_i^{X_0}(x) \geq 0, \forall i \in [n, \bar{n}] \},
\]

(4)

consider an autonomous system whose dynamics is captured by (1) with \( x_0 \in \mathcal{X}_0 \subseteq \mathcal{X} \). If \( x_0 \sim \mu_0(\mathcal{X}_0) \), find

\[
\mathbb{E} \left[ \int_0^T 1_{\mathcal{X}_0}(x(t))dt \right].
\]

(5)

Notice that the expectation in Problem 1 is taken with respect to the distribution on the initial condition \( x_0 \). Essentially, Problem 1 aims to estimate the expected amount of time out of \( T \) that the system trajectory spends in the unsafe region \( \mathcal{X}_0 \). Notice that the above formulation contains verifying the safety of autonomous systems \( \mathcal{X}_1 \) as a special case. More precisely, the system avoids passing through the region \( \mathcal{X}_0 \) if and only if (5) is zero. Therefore, the above formulation is able to provide a (binary) safety certificate for the system. We remark that the above formulation is also capable of providing safety certificate for the system when the initial state is known exactly, i.e., \( \mu_0 = \delta_{x_0} \).

III. Occupation Measure-Based Reformulation

In this section, we introduce a measure-theoretic approach to characterize the trajectories of the autonomous system described in (1) (presented in Subsection III-B). Using this method, we show that the value of (5) in Problem 1 can be computed via an infinite-dimensional linear program – see Subsection III-C and Subsection III-D. To explain our approach, we first introduce preliminaries in measure theory.

A. Notations and preliminaries

Given a topological space \( \mathcal{S} \), we denote by \( \mathcal{M}(\mathcal{S}) \) the space of finite signed Borel measures on \( \mathcal{S} \) and \( \mathcal{M}_+(\mathcal{S}) \) its positive cone. Let \( \mathcal{C}(\mathcal{S}) \) and \( \mathcal{C}^1(\mathcal{S}) \) be the space of continuous functions and continuously differentiable functions on \( \mathcal{S} \), respectively. The topological dual of \( \mathcal{M}(\mathcal{S}) \) and \( \mathcal{C}(\mathcal{S}) \) are denoted by \( \mathcal{M}(\mathcal{S})^* \) and \( \mathcal{C}(\mathcal{S})^* \).

Given a function \( h \in \mathcal{C}(\mathcal{S}) \) and a measure \( \mu \in \mathcal{M}(\mathcal{S}) \), we define the duality bracket between \( h \) and \( \mu \) by

\[
\langle h, \mu \rangle = \int_{\mathcal{S}} h d\mu.
\]

(6)

By Riesz-Markov-Kakutani representation theorem [21], when \( \mathcal{S} \) is locally compact Hausdorff, the dual space of \( \mathcal{C}(\mathcal{S}) \) is \( \mathcal{M}(\mathcal{S}) \), in which the norm of \( \mathcal{C}(\mathcal{S}) \) is the sup-norm of functions and the norm of \( \mathcal{M}(\mathcal{S}) \) is the total variation norm of measures. In the rest of the paper, we consider compact topological spaces \( \mathcal{S} \subseteq \mathbb{R}^n \). As a consequence, both local compactness and separability conditions required to form the duality between \( \mathcal{M}(\mathcal{S}) \) and \( \mathcal{C}(\mathcal{S}) \) are satisfied. Given a measure \( \mu \in \mathcal{M}(\mathcal{S}) \), the support of \( \mu \), denoted by \( \text{supp}(\mu) \), is the smallest closed set \( \mathcal{C} \subseteq \mathcal{S} \) such that \( \mu(\mathcal{S} \setminus \mathcal{C}) = 0 \) where smallest is understood in the set-inclusion sense.

B. Occupation measures and Liouville equation

Given an initial condition \( x_0 \), let \( x(t \mid x_0) \) be the solution to (1). Given a trajectory \( x(t \mid x_0) \), we define the occupation measure \( \mu(\cdot \mid x_0) \) on \( x(t \mid x_0) \) by

\[
\mu(A \times B \mid x_0) := \int_{[0,T] \cap A} 1_B(x(t \mid x_0))dt
\]

(7)
for all $A \times B \subseteq [0, T] \times \mathcal{X}$. Therefore, given sets $A$ and $B$, the value $\mu(A \times B)$ equals the total amount of time out of $A$ the state trajectory $x(t \mid x_0)$ spends in the set $B$. In other words, $\mu(\cdot \mid x_0)$ provides a certificate on how much time a given trajectory $x(t \mid x_0)$ occupies a certain set. In Section III.C, we will leverage this interpretation to reformulate the objective (5) in Problem 1. Similarly, we define the final measure $\mu_T(\cdot \mid x_0)$ by

$$\mu_T(B \mid x_0) = 1_B(x(T \mid x_0))$$

(8)

for all $B \subseteq \mathcal{X}$. Notice that the occupation measure $\mu(\cdot \mid x_0)$ is supported on $[0, T] \times \mathcal{X}$ whereas the final measure $\mu_T(\cdot \mid x_0)$ is supported on $\mathcal{X}$.

Given a test function $v \in C^1([0, T] \times \mathcal{X})$, we define the following operator $\mathcal{L}$:

$$v \mapsto \mathcal{L}v = \frac{\partial v}{\partial t} + \nabla v \cdot f(t, x).$$

(9)

In addition to $\mathcal{L}$, we define the adjoint operator $\mathcal{L}^* : \mathcal{M}([0, T] \times \mathcal{X}) \rightarrow C^1([0, T] \times \mathcal{X})^*$ using duality bracket \(\langle \cdot, \mathcal{L}^* \cdot \rangle\) by

$$\langle v, \mathcal{L}^* \nu \rangle = \langle \mathcal{L}v, \nu \rangle.$$ (10)

From (9), we have that

$$v(T, x(t \mid x_0)) = v(0, x_0) + \int_0^T \frac{d}{dt} v(t, x(t \mid x_0)) dt$$

$$= v(0, x_0) + \int_{[0,T] \times \mathcal{X}} \mathcal{L}(v, x) d\mu(t, x \mid x_0)$$

$$= v(0, x_0) + \langle \mathcal{L}v, \mu(\cdot \mid x_0) \rangle.$$ (11)

We can further rewrite (11) into

$$\langle v, \delta_T \otimes \mu_T(\cdot \mid x_0) \rangle = \langle v, \delta_0 \otimes \delta_{x_0} \rangle + \langle \mathcal{L}v, \mu(\cdot \mid x_0) \rangle.$$ (12)

In the view of (10), since the above equation holds for all $v \in C^1([0, T] \times \mathcal{X})$, we obtain the following equality:

$$\delta_T \otimes \mu_T(\cdot \mid x_0) = \delta_0 \otimes \delta_{x_0} + \mathcal{L}^* \mu(\cdot \mid x_0).$$ (13)

Essentially, (13) describes the evolution of the distribution of states given an initial distribution under the flow of the dynamics (11) – see (22) for more detailed discussions.

The aforementioned measures (7) and (5) are defined according to a given initial condition $x_0$. In what follows, we extend these measures to handle the case when the system is evolving from a set of initial conditions. Given an initial distribution $\mu_0$ with $\text{supp}(\mu_0) \subseteq \mathcal{X}$, we define the average occupation measure $\mu \in \mathcal{M}([0, T] \times \mathcal{X})$ by

$$\mu(A \times B) = \int_{x_0} \mu(A \times B \mid x_0) d\mu_0$$

(14)

and the average final measure $\mu_T \in \mathcal{M}(\mathcal{X})$ by

$$\mu_T(B) = \int_{x_0} \mu_T(B \mid x_0) d\mu_0.$$ (15)

By integrating the left- and right-hand-side of (11) with respect to $\mu_0$, using duality bracket (6) and the adjoint operator (10), we have that

$$\delta_T \otimes \mu_T = \delta_0 \otimes \mu_0 + \mathcal{L}^* \mu.$$ (16)

Note that any family of solutions $x(t)$ of (11) with an initial distribution $\mu_0$ induce an occupation measure (14) and a final measure (15) satisfying (16). Conversely, for any tuple of measures $(\mu_0, \mu, \mu_T)$ satisfying (16), one can identify a distribution on the admissible trajectories starting from $\mu_0$ whose average occupation measure and average final measure coincide with $\mu$ and $\mu_T$, respectively. See Lemma 3 in (19) and Lemma 6 in (23) for more details.

C. Infinite-dimensional linear program reformulation

Hereafter, we will show that the value in (5) can be obtained by solving a linear program on the occupation measure and final measure defined according to (14) and (15). According to the definition of average occupation measure, we have that

$$\mathbb{E} \left[ \int_0^T 1_{X_u} (x(t)) dt \right] = \int_{x_0} \int_0^T 1_{X_u} (x(t)) dt d\mu_0$$

$$= \int_{x_0} \mu([0, T] \times X_u | x_0) d\mu_0$$

(17)

$$= \mu([0, T] \times X_u).$$

Leveraging the above measure-theoretical formulation on the trajectories of the autonomous system, the value in (5) is equal to

$$\mu([0, T] \times X_u).$$ (18)

Subsequently, finding the solution to Problem (11) is equivalent to finding the volume of the set $[0, T] \times X_u$. In this case, the volume is measured using the average occupation measure instead of the Lebesgue measure. Next, we show that the value of (18) can be obtained by solving the following optimization problem. Given a polynomial $g : [0, T] \times \mathcal{X} \to \mathbb{R}$, where $g(t, x) > 0, \forall x \in [0, T] \times \mathcal{X}$, we consider the following optimization problem

$$P : \sup \int g d\mu$$

subject to $\tilde{\mu} + \hat{\mu} = \mu$

$$\delta_T \otimes \mu_T = \delta_0 \otimes \mu_0 + \mathcal{L}^* \mu$$

$$\tilde{\mu} \in \mathcal{M}_+([0, T] \times \mathcal{X})$$

$$\hat{\mu} \in \mathcal{M}_+([0, T] \times \mathcal{X})$$

$$\mu_T \in \mathcal{M}_+(\mathcal{X})$$

where the supremum is taken over a tuple of measures $(\tilde{\mu}, \hat{\mu}, \mu, \mu_T) \in \mathcal{M}_+([0, T] \times \mathcal{X}) \times \mathcal{M}_+([0, T] \times \mathcal{X}) \times \mathcal{M}_+([0, T] \times \mathcal{X}) \times \mathcal{M}_+([0, T] \times \mathcal{X})$. The constraint $\tilde{\mu} + \hat{\mu} = \mu$ is equivalent to $\tilde{\mu} \leq \mu$, i.e., the measure $\tilde{\mu}$ is dominated by measure $\mu$. Using the notion of duality bracket, we can write the objective in (19) as $(g, \mu)$. It follows that (19) is a linear program in the decision variable $(\tilde{\mu}, \hat{\mu}, \mu, \mu_T)$. Denote by $\text{sup} P$ the optimal value of $P$ and by $\text{max} \text{sup} P$ the supremum attained. When $g \equiv 1$, we show that the optimal value to the above program, if exists, is equal to (5) in the following theorem.
Theorem 1. Let $X_u$ be a compact and semi-algebraic subset of $X$ and $B$ be the Borel $\sigma$-algebra of Borel subsets of $[0, T] \times X_u$ Let $\mu^* \in \mathcal{M}([0, T] \times X_u)$ be defined by

$$\mu^*(S) = \mu(S \cap X_u), \forall S \in B. \quad (20)$$

Given a polynomial $g : [0, T] \times X \to \mathbb{R}$, if $g(t, x) > 0, \forall (t, x) \in [0, T] \times X_u$, then $\mu^*$ is the unique optimal solution to $P$. Furthermore, $\sup_P = \max_P = \int g d\mu^*$. In particular, if $g \equiv 1$, then $\max_P = \mu([0, T] \times X_u)$.

Proof. See Appendix A.

As a result of Theorem 1, we can compute the value of $\mu^*$ exactly by solving $P$. In the next subsection, we provide an alternative method to obtain the same value of interest by considering the Lagrangian dual of $P$.

D. Dual infinite-dimensional program

As mentioned in Section III-A, the dual space of $\mathcal{M}(S)$ is the Banach space of continuous functions on $S$ with the supremum norm. Let $\mathcal{C}_+(S) \subseteq C(S)$ be the set of continuous functions that are nonnegative on $S$. Using duality theory in conic optimization, the dual program of (19) is equal to

$$\mathcal{D} : \inf_{v \in \mathcal{W}} \int v(0, x) d\mu_0$$

s.t. $w(t, x) - g(t, x) \geq 0, \forall (t, x) \in [0, T] \times X_u$

$$- \mathcal{L}v(t, x) - w(t, x) \geq 0, \forall (t, x) \in [0, T] \times X$$

$$v(T, x) \geq 0, \forall x \in X$$

$$w(t, x) \geq 0, \forall (t, x) \in [0, T] \times X$$

(21)

where the decision variables in the above program are continuously differentiable function $v(t, x) \in C^1([0, T] \times X)$ and continuous function $w(t, x) \in C([0, T] \times X)$.

The dual problem $\mathcal{D}$ always provides an upper bound on the optimal value of the primal $P$. In the sequel, we show that the optimal values of (19) and (21) are actually equal. Thus, strong duality holds in this instance of infinite-dimensional linear program.

Theorem 2. Let $p^*$ and $d^*$ be the optimal values of $P$ and $D$, respectively. Then $p^* = d^*$, i.e., there is no duality gap between $P$ and $D$.

Proof. See Appendix A.

Consequently, the value of $\mu^*$ can be obtained by using (19) and (21). However, these two optimization problems are taking arguments from a tuple of measures and a tuple of continuous functions; hence both programs are infinite-dimensional. In order to solve for a solution in an infinite-dimensional program, in the next section, we leverage recent results from the multi-dimensional moment problem to approximate the solution to (19). Furthermore, we show that it is possible to obtain asymptotically precise estimates on (18) by solving a sequence of semidefinite programs.

IV. SEMIDEFINITE AND SUM-OF-SQUARES RELAXATION

In the previous section, we have shown that (5) can be computed using infinite-dimensional linear programs. Although the optimal solutions to $P$ and $D$ provide exact solutions to Problem 1, it is computationally intractable to obtain the solution. To address this issue, in Subsection IV-B we will provide a method to approximate the optimal solutions to $P$ and $D$ using sequences of semidefinite programs (SDPs) and sum-of-squares (SOS) programs, respectively. This approximation relies on the results in the multi-dimensional moment problem, which allow us to replace the tuple of measures in $P$ by sequences of moments.

The following observation plays a key role in our approximation scheme. Notice that the equality constraint in (19) is formulated using the occupation measure is equivalent to

$$\langle v, \delta_T \otimes \mu_T \rangle = \langle v, \delta_0 \otimes \mu_0 \rangle + \langle \mathcal{L}v, \mu \rangle \quad (22)$$

for all $v \in C([0, T] \times X)$. Since the set of polynomials are dense in $C([0, T] \times X)$ and $\mathbb{R}[t, X]$ is closed under addition and multiplication, (22) is equivalent to

$$\int_X v(T, x) d\mu_T = \int_X v(0, x) d\mu_0 + \int_{[0, T] \times X} \mathcal{L}v d\mu$$

(23)

for all $v(t, x) = t^n x^\alpha$, $(a, \alpha) \in N \times N^n$.

where $a \in \mathbb{N}$, $\alpha = (\alpha_1, \ldots, \alpha_n) \in N^n$ is a multi-index and $x^\alpha = x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$. Using the procedure above, the linear constraints in $P$ hold provided that (22) holds for all monomial functions $v(t, x)$. A standard relaxation of this constraint is to require that (22) holds for all monomials up to a given fixed degree $r$, i.e., $a + |\alpha| = a + \sum_{i=1}^n \alpha_i \leq r$.

Since $v(t, x)$ is a monomial, the integration of $v$ with respect to a measure $\mu$ results in a moment of $\mu$. Therefore, (23) is a linear constraint on the moments of $\mu_0$, $\mu$ and $\mu_T$. In this case, instead of finding a tuple of measures satisfying the constraints in (19), we aim to find (finite) sequences of numbers that satisfy the constraint (23). Moreover, the sequences of numbers are moments of measures $\mu_0, \mu, \mu_T$. As required by (19), these measures must be supported on certain specified sets. To formalize this idea, in order to obtain the approximated solution to (5), we want to find sequences of numbers that are moments of the tuple of measures feasible in (19). To better explain this approach, we first introduce necessary notions related to the multi-dimensional moment problem, which characterizes the relationship between sequences of numbers and moments of measures.

A. Multi-dimensional K-moment problem

Given $x \in \mathbb{R}^n$ and $\alpha \in \mathbb{N}^n$, we let $x^\alpha$ denote the quantity $x^\alpha = \prod_{i=1}^n x_i^{\alpha_i}$. Given an $\mathbb{R}^n$-valued random variable $x \sim \mu$ and an integer vector $\alpha \in \mathbb{N}^n$, the $\alpha$-moment of $x$ is defined as $E[x^\alpha] = \int_{\mathbb{R}^n} \prod_{i=1}^n x_i^{\alpha_i} d\mu$. Moreover, we define the order of an $\alpha$-moment to be $|\alpha| = \sum_{i=1}^n \alpha_i$ and $N^n_\alpha = \{\alpha \in \mathbb{N}^n \mid |\alpha| \leq \alpha\}$. Finally, a sequence $\mathbf{y} = \{y_\alpha\}_{\alpha \in \mathbb{N}^n}$
indexed by $\alpha$ is called a multi-sequence. Given a multi-sequence $y = \{y_\alpha\}_{\alpha \in \mathbb{N}^n}$, we define a linear functional $L_y : \mathbb{R}^n \to \mathbb{R}$ by
\[
f(x) = \sum_{\alpha \in \mathbb{N}^n} f_\alpha x^\alpha \vdash L_y(f) = \sum_{\alpha \in \mathbb{N}^n} f_\alpha y_\alpha. \tag{24}\]

The introduction of the above functional, often known as the Riesz functional \cite{Riesz_1932}, leads to convenience in expressing the moment of random variables. More specifically, let $x$ be an $\mathbb{R}^n$-valued random variable with corresponding probability measure $\nu$ and $f$ be a polynomial in $x$, then the expectation of $f(x)$ is equal to
\[
\int f(x) d\nu = \sum_{\alpha \in \mathbb{N}^n} f_\alpha x^\alpha d\nu = \sum_{\alpha \in \mathbb{N}^n} f_\alpha y_\alpha = L_y(f)
\]
where $y_\alpha$ is the $\alpha$-moment of $x$.

**Definition 2.** Given a closed set $K \subseteq \mathbb{R}^n$. Let $y = \{y_\alpha\}_{\alpha \in \mathbb{N}^n}$ be an infinite real multi-sequence. A measure $\nu$ on $\mathbb{R}^n$ is said to be a $K$-representing measure for $y$ if
\[
y_\alpha = \int x^\alpha d\nu \text{ for all } \alpha \in \mathbb{N}^n \tag{25}\]
and supp$(\nu) \subseteq K$. If $y$ has a $K$-representing measure, we say that $y$ is $K$-feasible.

Note that not all multi-sequences are feasible since there may not exist a measure whose moments match the values in the multi-sequence. A necessary and sufficient condition for the feasibility of the $K$-moment problem, restricted to the case when $K$ is semi-algebraic and compact, can be stated in terms of linear matrix inequalities involving moment matrices and localizing matrices defined below.

**Definition 3.** \cite{Parrilo_2004} Let $y_{n,2r} = \{y_\alpha\}_{\alpha \in \mathbb{N}_r^n}$ be a (finite) real multi-sequence. The moment matrix of $y_{n,2r}$, denoted by $M_r(y_{n,2r})$, is defined as the real matrix indexed by $\mathbb{N}_r^n$ and having the entries
\[
[M_r(y_{n,2r})]_{\alpha,\beta} = y_{\alpha+\beta} \tag{26}\]
for all $\alpha, \beta \in \mathbb{N}_r^n$.

To better explain how the moment matrix is constructed, we consider $n = 2$, $r = 1$ and $y_{2,2} = \{y_{00}, y_{01}, y_{10}, y_{11}, y_{02}, y_{20}\}$ as an example. According to Definition 3 we have that
\[
M_1(y) = \left[\begin{array}{ccc} y_{00} & y_{10} & y_{01} \\
 y_{10} & y_{20} & y_{11} \\
 y_{01} & y_{11} & y_{02} \end{array}\right].
\]

Similarly, we define the localizing matrices as follows.

**Definition 4.** Consider a polynomial $g(x) = \sum_{\gamma \in \mathbb{N}^n} u_\gamma x^\gamma$. Given a finite multi-sequence $y_{n,2r} := \{y_\alpha\}_{\alpha \in \mathbb{N}_r^n}$, the localizing matrix of $y_{n,2r}$ with respect to $g$, denoted by $M_r(g, y_{n,2r})$, is the real matrix indexed by $\mathbb{N}_r^n$ whose entries are
\[
[M_r(g, y_{n,2r})]_{\alpha,\beta} = \sum_{\gamma \in \mathbb{N}^n} u_\gamma y_{\gamma+\alpha+\beta} \tag{27}\]
for all $\alpha, \beta \in \mathbb{N}_r^n$.

Under specific assumptions on the set $K$, it is possible to state the necessary and sufficient conditions using moment and localizing matrices. Such a method is built upon algebraic characterization on the relationship between polynomials and sum-of-squares polynomials.

**Definition 5.** (Sum-of-squares polynomial) A polynomial $p : \mathbb{R}^n \to \mathbb{R}$ is a sum-of-squares (in short SOS) polynomial if $p$ can be written as
\[
p(x) = \sum_{j \in J} p_j(x)^2, \ x \in \mathbb{R}^n \tag{28}\]
for some finite family of polynomials $\{p_j \mid j \in J\}$.

The following result utilizes the properties of sum-of-squares polynomials to characterize when a multi-sequence $y$ is $K$-feasible in terms of moment and localizing matrices.

**Theorem 3.** (Putinar’s Positivstellensatz \cite{Putinar_1993}) Consider an infinite multi-sequence $y = \{y_\alpha\}_{\alpha \in \mathbb{N}^n}$ and a collection of polynomials $g_i : \mathbb{R}^n \to \mathbb{R}$ for all $i \in [m]$. Define a compact semi-algebraic set $K = \{x \in \mathbb{R}^n \mid g_i(x) \geq 0, \ i \in [m]\}$. Assume that there exists a polynomial $u = u_0 + \sum_{i=1}^{m} u_i g_i$, where $u_i$ are SOS polynomials for all $i \in \{0\} \cup [m]$ such that the set $\{x \mid u(x) \geq 0\}$ is compact. Then $y$ has a $K$-representing measure if and only if
\[
M_1(y) \succeq 0 \quad \text{and} \quad M_r(g_j, y) \succeq 0, \text{ for all } j \in [m] \text{ and } r \in \mathbb{N}. \tag{29}\]

In the following subsection, we will leverage this theorem to construct approximate solutions to $P$ and $D$.

**B. Finite-dimensional approximations**

1) SDP relaxation of $P$: As briefed in the previous subsection, we aim to optimize over sequences of moments of a tuple of measures $(\mu, \hat{\mu}, \mu, \mu_T)$ in the relaxed problem of $P$. We use $(\tilde{y}, \bar{y}, y, y_T)$ to denote the moment sequences of the corresponding measures, respectively. In particular, on the one hand, since $\mu$ is supported on $[0, T] \times \mathcal{X}$, the elements in the moment sequence $y$ is of the form $y_\alpha$ where $\alpha \in \mathbb{N} \times \mathbb{N}$. On the other hand, since $\mu_T$ is supported on $\mathcal{X}$, the elements in $y_T$ is of the form $y_\alpha$ where $\alpha \in \mathbb{N}^n$. Using the Riesz functional \cite{Riesz_1932} on \cite{Riesz_1932}, we have that
\[
L_{y_T}(v(T, \cdot)) - L_y(Lv) = L_{y_0}(v(0, \cdot)) \tag{30}\]
for all $v(t, x) = t^a x^\alpha$ and $a + |\alpha| \leq 2r$.

Applying the Riesz functional on the first linear constraint in $P$, we have that
\[
L\tilde{y}(w) + L\bar{y}(w) = L\hat{y}(w) \tag{31}\]
for all $w(t, x) = t^a x^\alpha$ and $a + |\alpha| \leq 2r$.

Both equations above are linear with respect to the elements in $y, \tilde{y}, \bar{y}, y_T$: hence, it is possible to write the above equality constraints compactly into a linear equation as follows:
\[
A_r(\tilde{y}, \bar{y}, y, y_T) = b_r. \tag{32}\]
From Theorem 3 since \( \text{supp}(\mu) \subseteq [0, T] \times \mathcal{X} \), the moment matrix of \( y \) and the localizing matrices of \( y \) with respect to \( g_0^X \) are positive semidefinite for all positive integers \( r \in \mathbb{N} \). Let

\[
d^X_0 = \left\lfloor \frac{\deg g_0^X}{2} \right\rfloor \quad \forall i \in [n_X], \quad d^Y_j = \left\lfloor \frac{\deg g_j^Y}{2} \right\rfloor \quad \forall j \in [n_X]
\]

where \( \deg \) denotes the degree of a polynomial. Given a fixed positive integer \( r \in \mathbb{N} \), we construct the \( r \)-th order relaxation of \( P \) as follows:

\[
P_r : \begin{align*}
\text{maximize} & \quad L_y(g) \\
\text{subject to} & \quad A_r(y, \tilde{y}, y, y_T) = b_r, \\
& \quad M_r(y) \succeq 0, \quad M_{r-1}(t(T-t), \tilde{y}) \succeq 0, \\
& \quad M_{r-d^X_0}(g^X_0, \tilde{y}) \succeq 0, \quad \forall i \in [n_X], \\
& \quad M_r(y) \succeq 0, \quad M_{r-1}(t(T-t), y) \succeq 0, \\
& \quad M_{r-d^X_0}(g^X_0, y) \succeq 0, \quad \forall i \in [n_X], \\
& \quad M_r(y_T) \succeq 0, \\
& \quad M_{r-d^X_0}(g^X_0, y_T) \succeq 0, \quad \forall i \in [n_X].
\end{align*}
\]

(33)

In this program, the decision variable is the 4-tuple of finite multi-sequences \((\tilde{y}, y, y_T)\). Furthermore, \( P_r \) is an SDP and thus can be solved by existing software efficiently. In addition to relaxing the primal LP \( P \), it is also possible to relax the dual LP \( D \) as shown next.

2) SOS relaxation of \( D \): To formulate the relaxed program of \( D \), we begin by considering the dual of \( P_r \). Furthermore, as shown in D, the decision variables are \( v(t, x) \in C([0, T] \times \mathcal{X}) \) and \( w(t, x) \in C([0, T] \times \mathcal{X}) \). The relaxed program is obtained by restricting the functions in \([31]\) to polynomials of degrees up to \( 2r \) and then replacing the non-negativity constraint with sum-of-squares constraints \([27]\). To formalize this argument, we first define the following notations.

Given a semi-algebraic set \( A = \{ x \in \mathbb{R}^n \mid h_i(x) \geq 0, h_i \in \mathbb{R}[x], \forall i \in [m] \} \), we define the \( r \)-th order quadratic module of \( A \) as

\[
Q_r(A) = \{ q \in \mathbb{R}[x]_r \mid \exists \text{SOS} \{ s_k \}_{k \in [m]} \cup \{ 0 \} \subseteq \mathbb{R}[x]_r \quad \text{s.t.} \quad q = s_0 + \sum_{k \in [m]} h_k s_k \}. 
\]

(34)

Following the process similar to \([28]\), the relaxed dual program, denoted by \( D_r \), is written as follows

\[
D_r : \begin{align*}
\text{minimize} & \quad l^T \text{vec}(v(0, \cdot)) \\
\text{subject to} & \quad w - g \in Q_{2r}([0, T] \times \mathcal{X}), \\
& \quad -L_v - w \in Q_{2r}([0, T] \times \mathcal{X}), \\
& \quad v(T, \cdot) \in Q_{2r}(\mathcal{X}), \\
& \quad w \in Q_{2r}([0, T] \times \mathcal{X})
\end{align*}
\]

where \( l \) is a vector containing the moments of the initial measure \( \mu_0 \). In this program, we optimize over the vector of polynomials \((w, v) \in \mathbb{R}[t, x]_{2r} \times \mathbb{R}[t, x]_{2r}\).

Notice that \( P_r \) and \( D_r \) provide approximate solutions to \( P \) and \( D \), respectively. Intuitively, as \( r \) increases, the gap between the optimal values of the relaxed program and the infinite-dimensional LP should decrease. In the next theorem, we show that there is no duality gap between \( P_r \) and \( D_r \) and that the optimal values of \( P_r \) and \( D_r \) converge to the optimal values of \( P \) and \( D \), respectively.

**Theorem 4.** Given a positive integer \( r \in \mathbb{N} \), let \( p^*_r \) and \( d^*_r \) be the optimal values of \( P_r \) and \( D_r \), respectively. If \( \mathcal{X}_u \) and \( \mathcal{X} \) have nonempty interior, then \( p^*_r = d^*_r \). Furthermore,

\[
p^*_r \downarrow p^* \quad \text{and} \quad d^*_r \downarrow d^*.
\]

(36)

**Proof.** See Appendix A

As a result of this theorem, \( p^*_r \) is a non-increasing function of \( r \) and it converges asymptotically to \( p^* \). From Theorem 1, \( p^* \) is equal to the safety quantity \( (5) \). We can thus conclude that \((5)\) can be obtained asymptotically.

**V. Numerical Examples**

In this section, we provide two examples to illustrate our framework in calculating \((5)\). We complete all numerical simulations using YALMIP \([29]\) (for sum-of-squares programs) and MOSEK \([30]\) (for semidefinite programs). We let \( g(t, x) = 1 \) in both examples.

**A. Univariate Constant Dynamics**

The value in \((5)\) is generally difficult to obtain. As a result, to illustrate the validity of our framework, we first provide a simple autonomous system to sharpen the reader’s intuition. More specifically, we start with an example concerning a univariate autonomous system where the time spent by the system in a given interval can be computed both analytically and numerically. In this case, we consider

\[
\dot{x} = 1
\]

(37)

and \( x(0) = x_0 \in \mathbb{R} \), i.e., \( \mu_0 = \delta_{x_0} \). By integrating over \((37)\), we have that \( x(t) = x_0 + t, t \in [0, T] \). Let \( T = 1 \) and consider the unsafe region \( \mathcal{X}_u = [0.4, 0.7] \). Furthermore, we denote by \( T_u \) the time spent in \( \mathcal{X}_u \). In this example, the following initial condition settings are considered: (i) \( x_0 = -0.7 \), and (ii) \( x_0 = -0.5 \). In the first case, the system \((37)\) does not reach \( \mathcal{X}_u \) (in time \([0, 1]\), which implies that \( T_u = 0 \). In the second case, the system stays in \( \mathcal{X}_u \) for \( T_u = 0.1 \) seconds.

We apply \( D_r \) to solve the above example. In each \( D_r \), polynomials of degree up to \( 2r \) are used. As illustrated in Figure 1, \( d^*_r \) decreases asymptotically in both case (i) and (ii). On the one hand, when the system does not enter \( \mathcal{X}_u \) (in the case \( x_0 = -0.7 \), \( d^*_r \) converges quickly to \( T_u = 0 \) when only polynomials of degree 4 are considered. On the other hand, when \( x_0 = -0.5 \), we obtain a non-increasing sequence of upper bounds on \( T_u = 0.1 \).
To further demonstrate our approach, we consider that $x_0 \sim \mu_0 = \text{Uniform}([-0.8, 0.3])$. In this case, we compute explicitly that the expected amount of time the system (37) spends in $X_u = [0, 0.4] \times [-0.5, 0.6]$ is 0.09. Using $D_r$, we obtain a sequence of non-increasing upper bounds on this value (see Figure 2).

### B. Van der Pol Oscillator

In this subsection, we evaluate our framework on the Van der Pol Oscillator – a second order nonlinear dynamical system whose dynamics is captured by

$$\begin{align*}
\dot{x}_1 &= -x_2 \\
\dot{x}_2 &= x_1 + (x_1^2 - 1)x_2.
\end{align*}$$

(38)

Moreover, we consider the following parameter settings (see Figure 3): (i) the final time is set to be $T = 10$, (ii) the initial condition is set to be $x(0) = x_0 = [2, 0]^T$, and (iii) the unsafe region is specified by a two-dimensional rectangle $X_u = [0, 0.5] \times [-2, 1]$. To ease the numerical computations, we adopt proper scaling to the coordinates of the system such that $T$ and $\mathcal{X}$ are normalized to be $T = 1$ and $\mathcal{X} = [-1, 1] \times [-1, 1]$, respectively. In this case, (5) cannot be computed analytically. However, through numerical simulation, we obtain that (38) spends (approximately) 1.2206 seconds in $X_u$. We demonstrate our upper bounds computed using $D_r$ with varying polynomial degrees $2r$ in Figure 4.

As pointed out in [17, Section 4], the convergence speed of the program $D_r$ (or $P_r$) is slow due to numerical problems encountered by the SDP solver – see Figure 1, 2 and 4 for illustrations. To address this issue, it is possible to apply Chebyshev polynomials basis instead of standard monomial basis to boost the convergence rate.

### VI. CONCLUSION

In this paper, we proposed a novel safety verification problem for nonlinear autonomous systems by evaluating how much time the system spends in a given unsafe region. To compute this safety certificate, an infinite-dimensional LP is posed over the space of measures which gives the exact solution. The solution of the LP can be approximated through a monotonically converging sequence of upper
Proof of Theorem 2 The proof follows the same lines as that of [19, Theorem 2]. Define
\[ C = C([0, T] \times X_0) \times C([0, T] \times X) \times C([0, T] \times X) \times C(X) \]
\[ M = M([0, T] \times X_0) \times M([0, T] \times X) \times M([0, T] \times X), \quad \text{and let } K \text{ and } K' \text{ denote the positive cones of } C \text{ and } M, \text{ respectively.} \]

By Riesz-Markov-Kakutani representation theorem [21], \( K' \) is the topological dual of the cone \( K \). The infinite dimensional linear program \( P \) can be written as:
\[
\begin{align*}
\sup_{\gamma} \ & \langle \gamma, c \rangle \\
\text{s.t.} \ & \ A' \gamma = \beta, \quad \gamma \in K'
\end{align*}
\]

where the supremum is taken over the vector \( \gamma = (\hat{\mu}, \hat{\mu}, \mu, \mu) \), the linear operator \( A' : K' \to C^1([0, T] \times X)^* \times M([0, T] \times X) \) is defined by \( A' \gamma = (\delta_T \otimes \mu - L' \mu - \hat{\mu} - \hat{\mu}) \) and \( \beta = (\delta_0 \otimes \mu_0, 0) \in C^1([0, T] \times X)^* \times M([0, T] \times X) \). The vector of functions in the objective is \( c = (g, 0, 0, 0) \). Define the duality bracket between a vector of measures \( \nu \in (\mathcal{M}(S))^p \) and a vector of functions \( h \in (\mathcal{C}(S))^p \) over a topological space \( S \) by
\[ \langle h, \nu \rangle = \sum_{i=1}^p \int_S [h_i] \, d[\nu_i]. \]

Then (43) can be interpreted as:
\[
\begin{align*}
\inf_{\beta} \ & \langle \beta, z \rangle \\
\text{s.t.} \ & \ Az - c \in K 
\end{align*}
\]

where the infimum is over \( z = (v, w) \in C^1([0, T] \times X) \times C([0, T] \times X) \), the linear operator \( L : C^1([0, T] \times X) \to \mathcal{C}([0, T] \times X) \) is given by \( A = (w, w, -Lv - wv(T(\cdot))) \) and satisfies the adjoint property \( \langle A' \gamma, z \rangle = \langle \gamma, Az \rangle \). The linear program (41) is exactly (41).

From [31, Theorem 3.10], there is no duality gap between (40) and (41) if the supremum of (40) is finite and the set \( P = \{(A' \gamma, (\gamma, c)) \mid \gamma \in K' \} \) is closed in the weak* topology of \( K' \). Since \( \hat{\mu} \) is dominated by the average occupation measure \( \mu \) and its underlying support is compact, the supremum of (40) is finite. To prove that \( P \) is closed, consider a sequence \( \gamma_k = (\hat{\mu}_k, \mu_k, \mu_k, \mu_k) \in K' \) such that \( A' \gamma_k \to a \) and \( (\gamma_k, c) \to b \) as \( k \to \infty \). Since the measures \( \mu_k \) are non-negative, this implies \( \mu_k \) is bounded. By taking \( z_0 = (1, -1) \), we have \( \langle A' \gamma_k, z_0 \rangle = \mu_k^1(0, T) + \hat{\mu}_k^2(0, T) + \mu_k(0, T) - \mu_k(0, T) \to \langle a, z_0 \rangle < \infty \) since \( \{\mu_k\} \) is bounded, by similar arguments the sequences \( \{\hat{\mu}_k\}, \{\mu_k\} \) and \( \{\mu_k\} \) are bounded as well.

As a result, \( \gamma_k \) is bounded and we can find a ball \( B \) in \( M \) with \( \{\gamma_k\} \subset B \). From the weak* compactness of the unit ball (Akaoglu's theorem [32, Section 5.10, Theorem 1]) there is a subsequence \( \{\gamma_{k_i}\} \) that weak*-converges to some \( \gamma \in K' \). Notice that \( A' \gamma \) is weak*-continuous because \( A \in C \) for all \( z \in C^1([0, T] \times X) \times C([0, T] \times X) \). So \( (a, b) = \lim_{i \to \infty} \langle A' \gamma_{k_i}, (\gamma_{k_i}, c) \rangle = \langle A' \gamma, (\gamma, c) \rangle \in B \) by the continuity of \( A' \) and \( P \) is closed. \( \square \)

Proof of Theorem 4 The proof of strong duality follows from standard SDP duality theory. Let \( \Delta = (\hat{\mu}, \mu, \mu, \mu) \) be the optimal solution to \( P \) and \( \Delta_y = (\tilde{y}, \tilde{y}, y, y_T) \) be their corresponding moment sequences. Any finite truncation of \( \Delta_y \) gives a feasible solution to \( P_z \). As \( X \times X_0 \) and \( X_0 \) have non-empty interior, we have the truncation of \( \Delta_y \) is strictly feasible for \( P_z \). By Slater's condition [33], there is no duality gap between \( P_z \) and \( D_z \), i.e., \( P_z = D_z^* \).

The proof of convergence follows from [18, Theorem 3.6]. Since \([0, T], X \text{ and } X_0 \) are compact sets, we can assume after appropriate scaling \( T = 1 \) and \( X \times X_0 \subseteq [-1, 1]^{n_x} \times [-1, 1]^{n_x} \), which implies that the feasible set of the semidefinite program \( P_z \) is compact. Let \( \Delta = (\tilde{y}, \tilde{y}, y, y_T) \) be the optimal solution to \( P_z \) and complete the finite vectors \( (\tilde{y}, \tilde{y}, y, y_T) \) with zeros to make them infinite sequences. By a standard diagonal argument, there is a subsequence \( \{r_k\} \) and a tuple of infinite vectors \( \Delta^* = (\tilde{y}, \tilde{y}, y, y_T) \) such that \( \Delta^* \to \Delta^* \) as \( k \to \infty \), where
the convergence is interpreted as elementary-wise. Since the infinite vector $\mathbf{y}^*$ in $\Delta^*$ is the limit point of a subsequence of the optimal solutions $\mathbf{y}^*_r$ of $P$, $p_r^*$ satisfies all the constraints in $P$, as $r \to \infty$. Then by Putinar's Positivstellensatz, $\mathbf{y}^*$ has a representing measure $\mu^*$ supported on $[0, T] \times \mathcal{X}_\gamma$. Similarly, $\mathbf{y}^*$, $y^*$ and $y_{r^*}$ have their representing measures $\mu^*_\gamma$, $\mu^*$ and $\mu^*_T$ with corresponding supports, respectively.

As problem $P_\gamma$ is a relaxation of $P$, $p_r^* \geq p^*$ for each $r$. Thus we have $\lim_{k \to \infty} \sup_{P_{\gamma}} = \lim_{k \to \infty} \sup_{L^*_\gamma} = L^*_\gamma(g) = \int g d\mu^* \geq p^*$. On the other hand, $A_r(\Delta^*) = \lim_{k \to \infty} A_r(\Delta^*_\gamma) = b_r$ for each $r \in \mathbb{N}$. Let $(\mu^*, \mu^*_\gamma, \mu^*, \mu^*_T)$ be the tuple of representing measures of $\Delta^*$. As measures on compact sets are determined by moments, $(\mu^*, \mu^*_\gamma, \mu^*, \mu^*_T)$ is a feasible solution to $P$ which implies $\int g d\mu^* \leq p^*$. Hence $\int g d\mu^* = p^*$ and $(\mu^*, \mu^*_\gamma, \mu^*, \mu^*_T)$ is an optimal solution of $P$. For any $r$ we have $p_r^* \geq p_{r+1}^*$ because as $r$ increases, the constraints in $P_{\gamma}$ become more restrict. As a result, $p_r^* \downarrow p^*$ and furthermore $p_r^* \downarrow p^* = d^*$. By strong duality, $d^* = p_r^* \downarrow p^* = d^*$.

**REFERENCES**

[1] J. Hu, M. Prandini, and S. Sastry, “Probabilistic safety analysis in three dimensional aircraft flight,” in *Proceedings of IEEE Conference on Decision and Control*, vol. 5. IEEE, 2003, pp. 5335-5340.

[2] S. Glavaski, A. Papachristodoulou, and K. Aryan, “Safety verification of controlled advanced life support system using barrier certificates,” in *International Workshop on Hybrid Systems: Computation and Control*. Springer, 2005, pp. 306-321.

[3] J. Ziegler and C. Stiller, “Fast collision checking for intelligent vehicle motion planning,” in *Intelligent Vehicles Symposium (IV), 2010 IEEE*. IEEE, 2010, pp. 518-522.

[4] M. Althoff, O. Stursberg, and M. Buss, “Safety assessment of autonomous cars using verification techniques,” in *Proceedings of American Control Conference*. IEEE, 2007, pp. 4154-4159.

[5] ——, “Model-based probabilistic collision detection in autonomous driving,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 10, no. 2, pp. 299-310, 2009.

[6] B. Bollbâs, “Volume estimates and rapid mixing,” *Flavors of geometry*, vol. 31, pp. 151-182, 1997.

[7] M. E. Dyer and A. M. Frieze, “On the complexity of computing the volume of a polyhedron,” *SIAM Journal on Computing*, vol. 17, no. 5, pp. 967-974, 1988.

[8] S. Prajna and A. Jadbabaie, “Safety verification of hybrid systems using barrier certificates,” in *International Workshop on Hybrid Systems: Computation and Control*. Springer, 2004, pp. 477-492.

[9] S. Prajna, “Barrier certificates for nonlinear model validation,” *Automatica*, vol. 42, no. 1, pp. 117-126, 2006.

[10] S. Prajna, A. Jadbabaie, and G. J. Pappas, “A framework for worst-case and stochastic safety verification using barrier certificates,” *IEEE Transactions on Automatic Control*, vol. 52, no. 8, pp. 1415-1428, 2007.

[11] C. Sloth, G. J. Pappas, and R. Wisniewski, “Compositional safety analysis using barrier certificates,” in *Proceedings of the 15th ACM international conference on Hybrid Systems: Computation and Control*. Citeseer, 2012, pp. 15-24.

[12] H. Anai and V. Weispfenning, “Reach set computations using real quantifier elimination,” in *International Workshop on Hybrid Systems: Computation and Control*. Springer, 2001, pp. 63-76.

[13] C. J. Tomlin, I. Mitchell, A. M. Bayen, and M. Oishi, “Computational techniques for the verification of hybrid systems,” *Proceedings of the IEEE*, vol. 91, no. 7, pp. 986–1001, 2003.

[14] E. Asarin, T. Dang, and A. Girard, “Reachability analysis of nonlinear systems using conservative approximation,” in *International Workshop on Hybrid Systems: Computation and Control*. Springer, 2003, pp. 20–35.

[15] S. Kousik, S. Vaskov, M. Johnson-Roberson, and R. Vasudevan, “Safe trajectory synthesis for autonomous driving in unforeseen environments,” in *ASME 2017 Dynamic Systems and Control Conference*. American Society of Mechanical Engineers, 2017.

[16] R. Vinter, “Convex duality and nonlinear optimal control,” *SIAM Journal on Control and Optimization*, vol. 31, no. 2, pp. 518–538, 1993.

[17] D. Henrion, J. B. Lasserre, and C. Savorgnan, “Approximate volume and integration for basic semialgebraic sets,” *SIAM Review*, vol. 51, no. 4, pp. 722–743, 2009.

[18] J. B. Lasserre, D. Henrion, C. Prieur, and E. Trélat, “Nonlinear optimal control via occupation measures and lmi-relaxations,” *SIAM Journal on Control and Optimization*, vol. 47, no. 4, pp. 1643–1666, 2008.

[19] D. Henrion and M. Korda, “Convex computation of the region of attraction of polynomial control systems,” *IEEE Transactions on Automatic Control*, vol. 59, no. 2, pp. 297–312, 2014.

[20] A. Majumdar, R. Vasudevan, M. M. Tobenkin, and R. Tedrake, “Convex optimization of nonlinear feedback controllers via occupation measures,” *The International Journal of Robotics Research*, vol. 33, no. 9, pp. 1209–1230, 2014.

[21] S. Kukutani, “Concrete representation of abstract (m)-spaces (a characterization of the space of continuous functions),” *Annals of Mathematics*, pp. 994–1024, 1941.

[22] V. I. Arnol’d, *Mathematical methods of classical mechanics*. Springer Science & Business Media, 2013, vol. 60.

[23] P. Zhao, S. Mohan, and R. Vasudevan, “Control synthesis for nonlinear optimal control via convex relaxations,” in *Proceedings of American Control Conference*. IEEE, 2017, pp. 2654–2661.

[24] J. B. Lasserre, *An introduction to polynomial and semialgebraic optimization*. Cambridge University Press, 2015, vol. 52.

[25] ——, *Moments, positive polynomials and their applications*. World Scientific, 2009, vol. 1.

[26] M. Putinar, “Positive polynomials on compact semi-algebraic sets,” *Indiana University Mathematics Journal*, vol. 42, no. 3, pp. 969–984, 1993.

[27] P. A. Parrilo, “Structured semidefinite programs and semialgebraic geometry methods in robustness and optimization,” Ph.D. dissertation, California Institute of Technology, 2000.

[28] S. Mohan and R. Vasudevan, “Convex computation of the reachable set for hybrid systems with parametric uncertainty,” in *Proceedings of American Control Conference*. IEEE, 2016, pp. 5141–5147.

[29] J. Löfberg, “Yalmip: A toolbox for modeling and optimization in matlab,” in *Proceedings of the CACSD Conference*, vol. 3, Taipei, Taiwan, 2004.

[30] A. Mosek, “The mosek optimization toolbox for matlab manual,” 2015.

[31] E. J. Anderson and P. Nash, *Linear programming in infinite-dimensional spaces: theory and applications*. John Wiley & Sons, 1987.

[32] D. G. Luenberger, *Optimization by vector space methods*. John Wiley & Sons, 1997.

[33] S. Boyd and L. Vandenberghe, *Convex optimization*. Cambridge university press, 2004.