Safety Verification of Nonlinear Autonomous System via Occupation Measures

Ximing Chen, Shaoru Chen, Victor M. Preciado

***Abstract*—In this paper, we introduce a flexible notion of safety verification for nonlinear autonomous systems by measuring how much time the system spends in given unsafe regions. We consider this problem in the particular case of nonlinear systems with a polynomial dynamics and unsafe regions described by a collection of polynomial inequalities. In this context, we can quantify the amount of time spent in the unsafe regions as the solution to an infinite-dimensional linear program (LP). This LP measures the volume of the unsafe region with respect to the occupation measure of the system trajectories. Using Lasserre hierarchy, we approximate the solution to the infinite-dimensional LP using a sequence of finite-dimensional semidefinite programs (SDPs). The solutions to the SDPs in this hierarchy provide monotonically converging upper bounds on the optimal solution to the infinite-dimensional LP. Finally, we validate the performance of our framework using numerical simulations.**

I. Introduction

Our ability to provide safety certificates about the behavior of complex systems is critical in many engineering applications, such as air traffic control [1], life support devices [2], motion planning in robotics manipulations [3], and connected autonomous vehicles [4, 5]. Although safety verification is a mature area with many success stories [6, 7], the verification of nonlinear dynamical systems over nonconvex unsafe regions remains a challenging problem [8, 9].

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 methods [10–12], and (ii) Lyapunov function methods [13–16]. Essentially, reachable set methods aim to find a set containing all possible states at a given time, for a given set of initial conditions. Subsequently, if the reachable set does not intersect with the pre-specified unsafe regions, the system is considered to be safe. For example, in [10] the reachable set is found for continuous-time linear systems, whereas in [11] and [12] the reachable sets are computed via approximations for nonlinear dynamical systems. In [17], the authors applied a reachable set method to plan safe trajectories for autonomous vehicles.

While reachable set methods can be used to obtain quantitative guarantees for safety, the reliability of the result largely depends on the assumptions made about the system, as well as the form of the unsafe regions. For instance, calculating the volume of the intersection of two sets, such as the reachable set and the unsafe regions, can become computationally challenging [9], jeopardizing the practical application of reachable set methods. An alternative approach to safety verification is based on using Lyapunov-like functions. In [14], the authors proposed the use of barrier certificates for safety verification of nonlinear systems. In contrast with the reachable set method, this line of work does not require to solve differential equations and is computationally more tractable. Furthermore, it also allows to provide safety certificates for various types of hybrid [13] and stochastic systems [15].

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. To illustrate this point, let us consider the operation of a solar-powered autonomous vehicle. Naturally, regions without solar exposure are considered to be unsafe, since the battery of the vehicle could be drained after a period of time. However, it would be inefficient to plan a path for the vehicle completely avoiding all these shaded regions. Instead, a more suitable requirement would be that the amount of time the vehicle spends in the shaded regions is bounded. More generally, this framework can be useful in those situations where the system is able to tolerate the exposure to a deteriorating agent, such as excessive heat or radiation, for a limited amount of time.

In this paper, we consider this alternative, more flexible notion of safety. More precisely, we aim to compute the time that a (nonlinear) system spends in the unsafe regions. In particular, we focus our analysis on the case of systems described by a polynomial dynamics and unsafe regions described by a collection of polynomial inequalities. To calculate the amount of time spent in the unsafe regions, we use *occupation measures* to quantify how much time the system trajectory spends in a particular set [18]. Using this alternative viewpoint of the system dynamics, the safety quantity of interest can be calculated by finding the volume of the unsafe region with respect to the occupation measure [19]. The usage of occupation measures allows us to leverage powerful numerical procedures developed in the context of control of polynomial systems [20–22].

The contribution of this paper is threefold. First, we

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.

formulate a flexible notion of safety allowing a trade-off between safety and performance. Second, we provide an *exact* formulation of the problem under consideration in terms of an infinite-dimensional LP. Furthermore, we provide a hierarchy of relaxations that can be efficiently solved using semidefinite programming. Finally, we provide numerical examples to demonstrate the applicability of our method.

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

Notations: We use bold symbols to represent real-valued vectors. 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 $\mathcal{S}$ is defined by $\mathbf{1}_{\mathcal{S}}(\cdot)$. We use $\delta_{\mathbf{x}}$ to denote the Dirac measure centered on a fixed point $\mathbf{x} \in \mathbb{R}^n$ and we use $\otimes$ to denote the product between two measures. The ring of polynomials in $\mathbf{x}$ with real coefficients is denoted by $\mathbb{R}[\mathbf{x}]$, and $\mathbb{R}[\mathbf{x}]_r$ denotes the subset of polynomials of degree $\leq r$. Given $\mathbf{x} \in \mathbb{R}^n$ and $\boldsymbol{\alpha} \in \mathbb{N}^n$, we let $\mathbf{x}^{\boldsymbol{\alpha}}$ denote the quantity $\mathbf{x}^{\boldsymbol{\alpha}} = \prod_{i=1}^n x_i^{\alpha_i}$. Let $|\boldsymbol{\alpha}| = \sum_{i=1}^n \alpha_i$ and $\mathbb{N}^n_r = \{\boldsymbol{\alpha} \in \mathbb{N}^n \mid |\boldsymbol{\alpha}| \leq r\}$.

II. Problem Statement

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

$$\begin{aligned} \dot{\mathbf{x}}(t) &= f(t, \mathbf{x}), \quad t \in [0, T] \\ \mathbf{x}(0) &= \mathbf{x}_0 \end{aligned} \tag{1}$$

where $\mathbf{x}(t) \in \mathbb{R}^n$ is the state vector, $\mathbf{x}_0$ is the initial condition, and $T > 0$ is the terminal time. We consider that the states of (1) are constrained to live 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 $\mathbf{x}_0$, with $\mathbf{x}_0 \in \mathcal{X}_0 \subseteq \mathcal{X}$. In this paper, we are interested in the case that the set $\mathcal{X}$ is semi-algebraic, as stated below.

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

$$K = \{\mathbf{x} \in \mathbb{R}^n \mid g_i(\mathbf{x}) \geq 0, \forall i \in [m]\}. \tag{2}$$

As mentioned above, we assume that the set $\mathcal{X}$ can be defined using polynomials $g_i^{\mathcal{X}}(\mathbf{x}) \in \mathbb{R}[\mathbf{x}]$, as follows:

$$\mathbf{x}(t) \in \mathcal{X} = \{\mathbf{x} \in \mathbb{R}^n \mid g_i^{\mathcal{X}}(\mathbf{x}) \geq 0, \forall i \in [n_{\mathcal{X}}]\} \tag{3}$$

for all $t \in [0, T]$.

In this paper, we consider the following problem:

Problem 1. *Consider a* compact *and* semi-algebraic *set $\mathcal{X}$, defined by* (3)*, and $\mathcal{X}_u \subseteq \mathcal{X}$, defined by:*

$$\mathcal{X}_u = \{\mathbf{x} \in \mathbb{R}^n \mid g_i^{\mathcal{X}_u}(\mathbf{x}) \geq 0, \forall i \in [n_{\mathcal{X}_u}]\}. \tag{4}$$

Given the autonomous system described in (1)*, with $x_0 \sim \mu_0(\mathcal{X}_0)$, where μ_0 is a probability distribution supported on $\mathcal{X}_0$, compute the expected amount of time that the system trajectory spends in the unsafe region $\mathcal{X}_u$.*

Notice that this expected time can be computed as:

$$\mathbb{E}\left[\int_0^T \mathbf{1}_{\mathcal{X}_u}(\mathbf{x}(t))dt\right], \tag{5}$$

where the expectation in (5) is taken with respect to the distribution of the initial condition $\mathbf{x}_0$. 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., $\mu_0 = \delta_{\mathbf{x}_0}$.

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 expectation in (5) can be computed via an infinite-dimensional linear program – see Subsection III-C and Subsection III-D. To explain our approach, we first introduce some notions of 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 μ by

$$\langle h, \mu \rangle = \int_{\mathcal{S}} h d\mu. \tag{6}$$

By Riesz-Markov-Kakutani representation theorem [23], 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 μ, denoted by $\texttt{supp}(\mu)$, is the smallest closed set $C \subseteq \mathcal{S}$ such that $\mu(\mathcal{S} \setminus C) = 0$ where smallest is understood in the set-inclusion sense.

B. Occupation measures and Liouville equation

Given an initial condition $\mathbf{x}_0$, let $\mathbf{x}(t \mid \mathbf{x}_0)$ be the solution to (1). Given a trajectory $\mathbf{x}(t \mid \mathbf{x}_0)$, we define the *occupation measure* $\mu(\cdot \mid \mathbf{x}_0)$ of $\mathbf{x}(t \mid \mathbf{x}_0)$ as

$$\mu(A \times B \mid \mathbf{x}_0) = \int_{[0,T]\cap A} \mathbf{1}_B(\mathbf{x}(t \mid \mathbf{x}_0))dt \tag{7}$$

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 that the state trajectory $\mathbf{x}(t \mid \mathbf{x}_0)$ spends in the set B. Similarly, we define the *final measure* $\mu_T(\cdot \mid \mathbf{x}_0)$ as

$$\mu_T(B \mid \mathbf{x}_0) = \mathbf{1}_B(\mathbf{x}(T \mid \mathbf{x}_0)) \tag{8}$$

for $B \subseteq \mathcal{X}$. Notice that the occupation measure $\mu(\cdot \mid \mathbf{x}_0)$ is supported on $[0,T]\times\mathcal{X}$ whereas the final measure $\mu_T(\cdot \mid \mathbf{x}_0)$ is supported on $\mathcal{X}$.

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

$$v \mapsto \mathcal{L}v = \frac{\partial v}{\partial t} + \nabla v \cdot f(t, \mathbf{x}). \tag{9}$$

The *adjoint operator* $\mathcal{L}^* : \mathcal{M}([0,T]\times\mathcal{X}) \to \mathcal{C}^1([0,T]\times\mathcal{X})^*$ is given by

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

From (9), we have that

$$\begin{aligned} v(T, \mathbf{x}(T \mid \mathbf{x}_0)) &= v(0, \mathbf{x}_0) + \int_0^T \frac{d}{dt} v(t, \mathbf{x}(t \mid \mathbf{x}_0))dt \\ &= v(0, \mathbf{x}_0) + \int_{[0,T]\times\mathcal{X}} \mathcal{L}v(t, \mathbf{x})d\mu(t, \mathbf{x} \mid \mathbf{x}_0) \\ &= v(0, \mathbf{x}_0) + \langle \mathcal{L}v, \mu(\cdot \mid \mathbf{x}_0)\rangle. \end{aligned} \tag{11}$$

Hence, we can further rewrite (11) as

$$\langle v, \delta_T \otimes \mu_T(\cdot \mid \mathbf{x}_0)\rangle = \langle v, \delta_0 \otimes \delta_{\mathbf{x}_0}\rangle + \langle \mathcal{L}v, \mu(\cdot \mid \mathbf{x}_0)\rangle. \tag{12}$$

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

$$\delta_T \otimes \mu_T(\cdot \mid \mathbf{x}_0) = \delta_0 \otimes \delta_{\mathbf{x}_0} + \mathcal{L}^*\mu(\cdot \mid \mathbf{x}_0). \tag{13}$$

Essentially, (13) describes the evolution of the distribution of states, given an initial distribution, under the flow of the dynamics (1) – see [24] for a more detailed discussions.

The measures defined in (7) and (8) depend on a given initial condition $\mathbf{x}_0$. In what follows, we extend these definitions to handle the case when the system is evolving from a set of possible initial conditions. Given an initial distribution μ_0 with $\mathtt{supp}(\mu_0) \subseteq \mathcal{X}_0$, we define the *average occupation measure* $\mu \in \mathcal{M}([0,T] \times \mathcal{X})$ as

$$\mu(A \times B) = \int_{\mathcal{X}_0} \mu(A \times B \mid \mathbf{x}_0)d\mu_0 \tag{14}$$

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

$$\mu_T(B) = \int_{\mathcal{X}_0} \mu_T(B \mid \mathbf{x}_0)d\mu_0. \tag{15}$$

By integrating the left- and right-hand side of (11) with respect to μ_0, we have that

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

Note that any family of solutions $\mathbf{x}(t)$ of (1) with an initial distribution μ_0 induces an occupation measure (14) and a final measure (15) satisfying (16). Conversely, for any tuple of measures (μ_0, μ, μ_T) satisfying (16), one can identify a distribution on the admissible trajectories starting from μ_0 whose average occupation measure and average final measure coincide with μ and μ_T, respectively (see Lemma 3 in [21] and Lemma 6 in [25] 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 the final measure, defined in (14) and (15). According to the definition of average occupation measure, we have that

$$\begin{aligned} \mathbb{E}\left[\int_0^T \mathbf{1}_{\mathcal{X}_u}(\mathbf{x}(t))dt\right] &= \int_{\mathcal{X}_0}\int_0^T \mathbf{1}_{\mathcal{X}_u}(\mathbf{x}(t))dtd\mu_0 \\ &= \int_{\mathcal{X}_0} \mu([0,T] \times \mathcal{X}_u \mid \mathbf{x}_0)d\mu_0 \\ &= \mu([0,T] \times \mathcal{X}_u). \end{aligned} \tag{17}$$

Leveraging the above measure-theoretical formulation, the value in (5) is equal to

$$\mu([0,T] \times \mathcal{X}_u). \tag{18}$$

Subsequently, finding the solution to Problem 1 is equivalent to finding the *volume* of the set $[0,T] \times \mathcal{X}_u$, where this 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 $g : [0,T] \times \mathcal{X} \to \mathbb{R}$, such that $g(t, \mathbf{x}) > 0, \forall (t, \mathbf{x}) \in [0,T] \times \mathcal{X}_u$, consider the following optimization problem

$$\begin{aligned} \mathtt{P}: \quad & \sup \int g d\widetilde{\mu} \\ & \text{subject to } \widetilde{\mu} + \widehat{\mu} = \mu \\ & \qquad \delta_T \otimes \mu_T = \delta_0 \otimes \mu_0 + \mathcal{L}^*\mu \\ & \qquad \mu, \widehat{\mu} \in \mathcal{M}_+([0,T] \times \mathcal{X}) \\ & \qquad \widetilde{\mu} \in \mathcal{M}_+([0,T] \times \mathcal{X}_u) \\ & \qquad \mu_T \in \mathcal{M}_+(\mathcal{X}) \end{aligned} \tag{19}$$

where the supremum is taken over a tuple of measures $(\widetilde{\mu}, \widehat{\mu}, \mu, \mu_T) \in \mathcal{M}_+([0,T] \times \mathcal{X}_u) \times \mathcal{M}_+([0,T] \times \mathcal{X}) \times \mathcal{M}_+([0,T] \times \mathcal{X}) \times \mathcal{M}_+(\mathcal{X})$. The constraint $\widetilde{\mu} + \widehat{\mu} = \mu$ is equivalent to $\widetilde{\mu} \leq \mu$, i.e., the measure $\widetilde{\mu}$ is dominated by μ. Using duality brackets, we can write the objective in (19) as $\langle g, \widetilde{\mu}\rangle$. It follows that (19) is a linear program in the decision variable $(\widetilde{\mu}, \widehat{\mu}, \mu, \mu_T)$. Denote by $\sup \mathtt{P}$ the optimal value of $\mathtt{P}$ and by $\max \mathtt{P}$ the supremum attained. When $g \equiv 1$, we

show below that the optimal value to the above program, if it exists, is equal to (5).

Theorem 1. *Let $\mathcal{X}_u$ be a compact and semi-algebraic subset of $\mathcal{X}$ and $\mathcal{B}$ be the Borel σ-algebra of Borel subsets of $[0,T]\times\mathcal{X}$. Let $\widetilde{\mu}^* \in \mathcal{M}([0,T]\times\mathcal{X}_u)$ be defined by*

$$\widetilde{\mu}^*(S) = \mu(S \cap [0,T]\times\mathcal{X}_u), \forall S \in \mathcal{B}. \tag{20}$$

Given a polynomial $g : [0,T]\times\mathcal{X} \to \mathbb{R}$, if $g(t,\mathbf{x}) > 0, \forall (t,\mathbf{x}) \in [0,T]\times\mathcal{X}_u$, then $\widetilde{\mu}^*$ is the $\widetilde{\mu}$-component of an optimal solution to P. *Furthermore,* $\sup \mathtt{P} = \max \mathtt{P} = \int g d\widetilde{\mu}^*$. *In particular, if $g \equiv 1$, then* $\max \mathtt{P} = \mu([0,T]\times\mathcal{X}_u)$.

Proof. See appendix A. □

As a result of Theorem 1, the solution of P is equal to the expected time in (5). In the next subsection, we consider the Lagrangian dual of P.

D. Dual infinite-dimensional program

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

$$\begin{aligned} \mathtt{D}: \inf_{v,w} & \int v(0,\mathbf{x}) d\mu_0 \\ \text{s.t. } & w(t,\mathbf{x}) - g(t,\mathbf{x}) \geq 0, \forall (t,\mathbf{x}) \in [0,T]\times\mathcal{X}_u \\ & -\mathcal{L}v(t,\mathbf{x}) - w(t,\mathbf{x}) \geq 0, \forall (t,\mathbf{x}) \in [0,T]\times\mathcal{X} \\ & v(T,\mathbf{x}) \geq 0, \forall \mathbf{x} \in \mathcal{X} \\ & w(t,\mathbf{x}) \geq 0, \forall (t,\mathbf{x}) \in [0,T]\times\mathcal{X} \end{aligned} \tag{21}$$

where the decision variables in the above program are the continuously differentiable function $v(t,\mathbf{x}) \in \mathcal{C}^1([0,T]\times\mathcal{X})$ and the continuous function $w(t,\mathbf{x}) \in \mathcal{C}([0,T]\times\mathcal{X})$. The dual problem 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 infinite-dimensional linear program.

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

Proof. See appendix A. □

Consequently, the value of (5) can be obtained by solving (19) or (21). However, these two optimization problems are taking arguments from a tuple of measures or a tuple of continuous functions; hence both programs are hard infinite-dimensional optimization problems. In the next section, we leverage recent results from the multi-dimensional moment problem [26] to approximate the solution to (19). Furthermore, we show that it is possible to obtain increasingly tighter bounds 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 by solving an infinite-dimensional linear program. Although the optimal solutions to P or D provide exact solutions to Problem 1, it is computationally intractable to solve them. 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. We utilize tools developed in the context of the multi-dimensional moment problem allowing 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 equivalent to

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

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

$$\begin{aligned} &\int_{\mathcal{X}} v(T,\mathbf{x}) d\mu_T = \int_{\mathcal{X}} v(0,\mathbf{x}) d\mu_0 + \int_{[0,T]\times\mathcal{X}} \mathcal{L}v d\mu \\ &\text{for all } v(t,\mathbf{x}) = t^a \mathbf{x}^{\boldsymbol{\alpha}}, (a,\boldsymbol{\alpha}) \in \mathbb{N}\times\mathbb{N}^n, \end{aligned} \tag{23}$$

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

Since $v(t,\mathbf{x})$ is a monomial, the integration of v with respect to a measure μ results in a moment of μ. Therefore, (23) is a linear constraint on the moments of μ_0, μ and μ_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 $\widetilde{\mu}, \widehat{\mu}, \mu, \mu_T$. As required by (19), these measures must be supported on certain specified sets. To formalize this idea, in order to obtain an 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 characterizing the relationship between sequences of numbers and moments of measures.

A. Multi-dimensional K-moment problem

Given an $\mathbb{R}^n$-valued random variable $\mathbf{x} \sim \nu$ and an integer vector $\boldsymbol{\alpha} \in \mathbb{N}^n$, the $\boldsymbol{\alpha}$-moment of $\mathbf{x}$ is defined as $\mathbb{E}[\mathbf{x}^{\boldsymbol{\alpha}}] = \int_{\mathbb{R}^n} \prod_{i=1}^n x_i^{\alpha_i} d\nu$. Moreover, we define the *order* of an $\boldsymbol{\alpha}$-moment to be $|\boldsymbol{\alpha}|$. Finally, a sequence $\mathbf{y} = \{y_{\boldsymbol{\alpha}}\}_{\boldsymbol{\alpha}\in\mathbb{N}^n}$ indexed by $\boldsymbol{\alpha}$ is called a *multi-sequence*. Given a multi-sequence $\mathbf{y} = \{y_{\boldsymbol{\alpha}}\}_{\boldsymbol{\alpha}\in\mathbb{N}^n}$, we define the linear functional $L_{\mathbf{y}} : \mathbb{R}[\mathbf{x}] \to \mathbb{R}$ as

$$f(\mathbf{x}) = \sum_{\boldsymbol{\alpha}\in\mathbb{N}^n} f_{\boldsymbol{\alpha}} \mathbf{x}^{\boldsymbol{\alpha}} \mapsto L_{\mathbf{y}}(f) = \sum_{\boldsymbol{\alpha}\in\mathbb{N}^n} f_{\boldsymbol{\alpha}} y_{\boldsymbol{\alpha}}. \tag{24}$$

The introduction of the above functional, often known as the *Riesz functional* [27], is convenient to express the moments of random variables. More specifically, let $\mathbf{x}$ be an $\mathbb{R}^n$-valued random variable with corresponding probability measure ν and let f be a polynomial in $\mathbf{x}$. Then, the expectation of $f(\mathbf{x})$ is equal to

$$\int f(\mathbf{x})d\nu = \int \sum_{\boldsymbol{\alpha}\in\mathbb{N}^n} f_{\boldsymbol{\alpha}}\mathbf{x}^{\boldsymbol{\alpha}}d\nu = \sum_{\boldsymbol{\alpha}\in\mathbb{N}^n} f_{\boldsymbol{\alpha}}y_{\boldsymbol{\alpha}} = L_{\mathbf{y}}(f)$$

where $y_{\boldsymbol{\alpha}}$ is the $\boldsymbol{\alpha}$-moment of $\mathbf{x}$.

Definition 2. *Let $K \subseteq \mathbb{R}^n$ be a closed set. Let $\mathbf{y} = \{y_{\boldsymbol{\alpha}}\}_{\boldsymbol{\alpha}\in\mathbb{N}^n}$ be an infinite real multi-sequence. A measure ν on $\mathbb{R}^n$ is said to be a K-representing measure for $\mathbf{y}$ if*

$$y_{\boldsymbol{\alpha}} = \int_{\mathbb{R}^n} \mathbf{x}^{\boldsymbol{\alpha}}d\nu \text{ for all } \boldsymbol{\alpha} \in \mathbb{N}^n \tag{25}$$

and $\texttt{supp}(\nu) \subseteq K$. If $\mathbf{y}$ has a K-representing measure, we say that $\mathbf{y}$ is K-feasible.

Note that not all multi-sequences are K-feasible, since there may not exist a measure supported on K 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. These conditions involve *moment matrices* and *localizing matrices*, defined below.

Definition 3. [26] *Let $\mathbf{y}_{n,2r} = \{y_{\boldsymbol{\alpha}}\}_{\boldsymbol{\alpha}\in\mathbb{N}^n_{2r}}$ be a (finite) real multi-sequence. The* moment matrix *of $\mathbf{y}_{n,2r}$, denoted by $M_r(\mathbf{y}_{n,2r})$, is defined as the real matrix indexed by $\mathbb{N}^n_r$ whose entries are*

$$[M_r(\mathbf{y}_{n,2r})]_{\boldsymbol{\alpha},\boldsymbol{\beta}} = y_{\boldsymbol{\alpha}+\boldsymbol{\beta}} \tag{26}$$

for all $\boldsymbol{\alpha}, \boldsymbol{\beta} \in \mathbb{N}^n_r$.

To better explain how the moment matrix is constructed, we consider $n = 2$, $r = 1$ and $\mathbf{y}_{2,2} = \{y_{00}, y_{01}, y_{10}, y_{11}, y_{02}, y_{20}\}$ as an example. According to Definition 3, we have that

$$M_1(\mathbf{y}_{2,2}) = \begin{bmatrix} y_{00} & y_{10} & y_{01} \\ y_{10} & y_{20} & y_{11} \\ y_{01} & y_{11} & y_{02} \end{bmatrix}.$$

Similarly, we define the *localizing matrices* as follows.

Definition 4. *Consider a polynomial $g(\mathbf{x}) = \sum_{\boldsymbol{\gamma}\in\mathbb{N}^n} u_{\boldsymbol{\gamma}}\mathbf{x}^{\boldsymbol{\gamma}}$. Given a finite multi-sequence $\mathbf{y}_{n,2r} = \{y_{\boldsymbol{\alpha}}\}_{\boldsymbol{\alpha}\in\mathbb{N}^n_{2r}}$, the localizing matrix of $\mathbf{y}_{n,2r}$ with respect to g, denoted by $M_r(g, \mathbf{y}_{n,2r})$, is the real matrix indexed by $\mathbb{N}^n_r$ whose entries are*

$$[M_r(g, \mathbf{y}_{n,2r})]_{\boldsymbol{\alpha},\boldsymbol{\beta}} = \sum_{\boldsymbol{\gamma}\in\mathbb{N}^n} u_{\boldsymbol{\gamma}}y_{\boldsymbol{\gamma}+\boldsymbol{\alpha}+\boldsymbol{\beta}} \tag{27}$$

for all $\boldsymbol{\alpha}, \boldsymbol{\beta} \in \mathbb{N}^n_r$.

Under specific assumptions on the set K, it is possible to state necessary and sufficient conditions for K-feasibility of $\mathbf{y}$ using moment and localizing matrices. Such a method is built upon an algebraic characterization of the relationship between polynomials and sum-of-squares (SOS) polynomials.

Definition 5. (Sum-of-squares polynomial) *A polynomial $p : \mathbb{R}^n \to \mathbb{R}$ is a sum-of-squares polynomial if p can be written as*

$$p(\mathbf{x}) = \sum_{j\in J} p_j(\mathbf{x})^2, \ \mathbf{x} \in \mathbb{R}^n \tag{28}$$

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 $\mathbf{y}$ is K-feasible in terms of moment and localizing matrices.

Theorem 3. (Putinar's Positivstellensatz [28]) *Consider an infinite multi-sequence $\mathbf{y} = \{y_{\boldsymbol{\alpha}}\}_{\boldsymbol{\alpha}\in\mathbb{N}^n}$ and a collection of polynomials $g_i : \mathbb{R}^n \to \mathbb{R}$ for all $i \in [m]$. Define a compact semi-algebraic set $K = \{\mathbf{x} \in \mathbb{R}^n \mid g_i(\mathbf{x}) \geq 0, \ i \in [m]\}$. Assume that there exists a polynomial $u = u_0 + \sum_{j=1}^m u_i g_i$ where u_i are SOS polynomials for all $i \in \{0\} \cup [m]$ such that the set $\{\mathbf{x} \mid u(\mathbf{x}) \geq 0\}$ is compact. Then, $\mathbf{y}$ has a K-representing measure if and only if*

$$\begin{aligned} &M_r(\mathbf{y}) \succeq 0 \text{ and} \\ &M_r(g_j, \mathbf{y}) \succeq 0, \text{ for all } j \in [m] \text{ and } r \in \mathbb{N}. \end{aligned} \tag{29}$$

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

B. Finite-dimensional approximations

1) SDP relaxation of P*:* As mentioned above, in the relaxed version of P, we aim to optimize over sequences of moments of a tuple of measures $(\widetilde{\mu}, \widehat{\mu}, \mu, \mu_T)$. We use $(\widetilde{\mathbf{y}}, \widehat{\mathbf{y}}, \mathbf{y}, \mathbf{y}_T)$ to denote the moment sequences of the corresponding measures, respectively. On the one hand, since μ is supported on $[0, T] \times \mathcal{X}$, the elements in the moment sequence $\mathbf{y}$ are of the form $y_{\boldsymbol{\alpha}}$ where $\boldsymbol{\alpha} \in \mathbb{N} \times \mathbb{N}^n$. On the other hand, since μ_T is supported on $\mathcal{X}$, the elements in $\mathbf{y}_T$ are of the form $y_{\boldsymbol{\alpha}}$ where $\boldsymbol{\alpha} \in \mathbb{N}^n$. Using the Riesz functional (24) on (23), we obtain

$$\begin{aligned} &L_{\mathbf{y}_T}(v(T, \cdot)) - L_{\mathbf{y}}(\mathcal{L}v) = L_{\mathbf{y}_0}(v(0, \cdot)) \\ &\text{for all } v(t, \mathbf{x}) = t^a\mathbf{x}^{\boldsymbol{\alpha}} \text{ and } a + |\boldsymbol{\alpha}| \leq 2r. \end{aligned} \tag{30}$$

Applying the Riesz functional on the first linear constraint in P, we have that

$$\begin{aligned} &L_{\widetilde{\mathbf{y}}}(w) + L_{\widehat{\mathbf{y}}}(w) = L_{\mathbf{y}}(w) \\ &\text{for all } w(t, \mathbf{x}) = t^a\mathbf{x}^{\boldsymbol{\alpha}} \text{ and } a + |\boldsymbol{\alpha}| \leq 2r. \end{aligned} \tag{31}$$

Both equations in (31) are linear with respect to the elements in $\mathbf{y}, \widetilde{\mathbf{y}}, \widehat{\mathbf{y}}, \mathbf{y}_T$; hence, it is possible to write them compactly into a linear equation, as follows:

$$A_r(\widetilde{\mathbf{y}}, \widehat{\mathbf{y}}, \mathbf{y}, \mathbf{y}_T) = b_r. \tag{32}$$

From Theorem 3, since $\texttt{supp}(\mu) \subseteq [0, T] \times \mathcal{X}$, the moment and localizing matrices of $\mathbf{y}$ with respect to $g_i^{\mathcal{X}}$ are positive semidefinite for all positive integers $r \in \mathbb{N}$. Let

$$d_i^{\mathcal{X}_u} = \lceil \frac{\deg \ g_i^{\mathcal{X}_u}}{2} \rceil \ \forall i \in [n_{\mathcal{X}_u}], \ d_j^{\mathcal{X}} = \lceil \frac{\deg \ g_j^{\mathcal{X}}}{2} \rceil \ \forall j \in [n_{\mathcal{X}}]$$

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:

$$\begin{aligned}
\mathtt{P_r}: \quad & \underset{(\widetilde{\mathbf{y}},\widehat{\mathbf{y}},\mathbf{y},\mathbf{y}_T)}{\text{maximize}} \; L_{\widetilde{\mathbf{y}}}(g) \\
& \text{subject to } A_r(\widetilde{\mathbf{y}},\widehat{\mathbf{y}},\mathbf{y},\mathbf{y}_T) = b_r \\
& \qquad M_r(\widetilde{\mathbf{y}}) \succeq 0, \;\; M_{r-1}(t(T-t),\widetilde{\mathbf{y}}) \succeq 0 \\
& \qquad M_{r-d_i^{\mathcal{X}_u}}(g_i^{\mathcal{X}_u},\widetilde{\mathbf{y}}) \succeq 0, \forall i \in [n_{\mathcal{X}_u}] \\
& \qquad M_r(\widehat{\mathbf{y}}) \succeq 0, M_{r-1}(t(T-t),\widehat{\mathbf{y}}) \succeq 0 \\
& \qquad M_{r-d_i^{\mathcal{X}}}(g_i^{\mathcal{X}},\widehat{\mathbf{y}}) \succeq 0, \forall i \in [n_{\mathcal{X}}] \\
& \qquad M_r(\mathbf{y}) \succeq 0, \;\; M_{r-1}(t(T-t),\mathbf{y}) \succeq 0 \\
& \qquad M_{r-d_i^{\mathcal{X}}}(g_i^{\mathcal{X}},\mathbf{y}) \succeq 0, \forall i \in [n_{\mathcal{X}}] \\
& \qquad M_r(\mathbf{y}_T) \succeq 0, \\
& \qquad M_{r-d_i^{\mathcal{X}}}(g_i^{\mathcal{X}},\mathbf{y}_T) \succeq 0, \forall i \in [n_{\mathcal{X}}].
\end{aligned} \tag{33}$$

In this program, the decision variable is the 4-tuple of finite multi-sequences $(\widetilde{\mathbf{y}},\widehat{\mathbf{y}},\mathbf{y},\mathbf{y}_T)$. Furthermore, $\mathtt{P_r}$ is an SDP and, thus, can be solved using off-the-shelf software. 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 $\mathtt{P_r}$. Furthermore, as shown in D, the decision variables are $v(t,\mathbf{x}) \in \mathcal{C}^1([0,T]\times\mathcal{X})$ and $w(t,\mathbf{x}) \in \mathcal{C}([0,T]\times\mathcal{X})$. The relaxed program is obtained by restricting the functions in (21) to polynomials of degrees up to $2r$, and then replacing the non-negativity constraint with sum-of-squares constraints [29]. To formalize this argument, we first need to introduce some notations.

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

$$\begin{aligned}
Q_r(A) = \big\{ q \in & \mathbb{R}[\mathbf{x}]_r \mid \exists \text{ SOS } \{s_k\}_{k\in[m]\cup\{0\}} \subset \mathbb{R}[x]_r \\
& \text{s.t. } q = s_0 + \sum_{k\in[m]} h_k s_k \big\}.
\end{aligned} \tag{34}$$

Following a process similar to [30], the relaxed dual program, denoted by $\mathtt{D_r}$, can be written as follows

$$\begin{aligned}
\mathtt{D_r}: \quad & \text{minimize} \int v(0,\cdot) d\mu_0 \\
& \text{subject to } w - g \in Q_{2r}([0,T]\times\mathcal{X}_u) \\
& \qquad -\mathcal{L}v - w \in Q_{2r}([0,T]\times\mathcal{X}) \\
& \qquad v(T,\cdot) \in Q_{2r}(\mathcal{X}) \\
& \qquad w \in Q_{2r}([0,T]\times\mathcal{X}).
\end{aligned} \tag{35}$$

In this program, we optimize over the vector of polynomials $(w,v) \in \mathbb{R}[t,\mathbf{x}]_{2r} \times \mathbb{R}[t,\mathbf{x}]_{2r}$.

Notice that $\mathtt{P}_r$ and $\mathtt{D}_r$ provide approximate solutions to P and D, respectively. In the next theorem, we show that there is no duality gap between $\mathtt{P}_r$ and $\mathtt{D_r}$ and that the optimal values of $\mathtt{P}_r$ and $\mathtt{D}_r$ converge to the optimal values of P and D, respectively, as r increases.

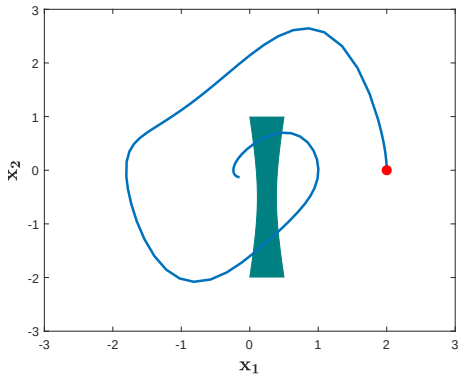

Figure 1: Trajectory $\mathbf{x}(t)$, where $t \in [0,10]$, of the Van der Pol system (blue curve) with initial condition $\mathbf{x}_0 = [2,0]^T$ (red circle). The unsafe region $\mathcal{X}_u$ is depicted by the nonconvex colored set.

Theorem 4. *Given a positive integer $r \in \mathbb{N}$, let $p_r^\star$ and $d_r^\star$ be the optimal values of $\mathtt{P}_r$ and $\mathtt{D}_r$, respectively. If $\mathcal{X}_u$ and $\mathcal{X}$ have nonempty interior, then $p_r^\star = d_r^\star$. Furthermore,*

$$d_r^* = p_r^\star \downarrow p^\star = d^\star. \tag{36}$$

Proof. See appendix A. □

As a result of this theorem, $p_r^\star$ is a non-increasing function of r and it converges asymptotically to $p^\star$. From Theorem 1, $p^\star$ is equal to the expected time the system spends in the unsafe region, as expressed in (5).

V. Numerical Examples

In this section, we provide a numerical example to illustrate our framework. We complete all numerical simulations using YALMIP [31] (for sum-of-squares programs) and MOSEK [32] (for semidefinite programs).

In particular, we evaluate our framework on the Van der Pol oscillator – a second order nonlinear dynamical system whose dynamics is given by

$$\begin{aligned}
\dot{x}_1 &= -x_2 \\
\dot{x}_2 &= x_1 + (x_1^2 - 1)x_2.
\end{aligned} \tag{37}$$

Moreover, we consider the following parameter settings (see Figure 1): (i) the final time is set to be $T = 10$, (ii) the initial condition is set to be $\mathbf{x}(0) = \mathbf{x}_0 = [2,0]^\top$, and (iii) the unsafe region is specified by a nonconvex two-dimensional semi-algebraic set $\mathcal{X}_u = \{(x_1,x_2) \in \mathbb{R}^2 \mid 52(x_1 - 0.25)^2 - (x_2 + 0.5)^2 \leq 1, 0 \leq x_1 \leq 0.5, -2 \leq x_2 \leq 1\}$. To ease the numerical computations, we adopt proper scaling of the system's coordinates 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 the Van der Pol oscillator spends (approximately) 0.9446 seconds in the unsafe region $\mathcal{X}_u$. We demonstrate our upper bounds on this time using $\mathtt{D}_r$ with varying values of r in Figure 2.

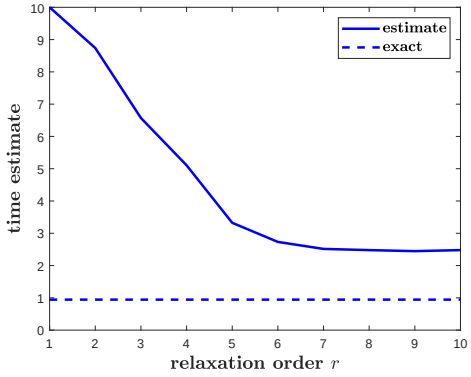

Figure 2: This figure shows the exact value (dashed line) and the approximation (solid line) to (5) using $\mathtt{D}_r$ with different values of r. The system dynamics under consideration is the Van der Pol system (37), whereas the initial distribution is $\mu_0 = \delta_{[2,0]^\top}$.

VI. Conclusion

In this paper, we have proposed a flexible safety verification notion for nonlinear autonomous systems described via polynomial dynamics and unsafe regions described via polynomial inequalities. Instead of verifying safety by checking whether the dynamics completely avoids the unsafe regions, we consider the system to be safe if it spends less than a certain amount of time in these regions. This more flexible notion can be of relevance in, for example, solar-powered vehicles where the vehicle should avoid spending too much time is dark areas. More generally, this framework can be useful in those situations where the system is able to tolerate the exposure to a deteriorating agent, such as excessive heat or radiation, for a limited amount of time. In this paper, we first propose an infinite-dimensional LP over the space of measures whose solution is equal to the (expected) time our (nonlinear) system spends in the (possibly nonconvex) unsafe regions. We then approximate the solution of the LP through a monotonically converging sequence of upper bounds by solving a hierarchy of SDPs. We have validated our approach via a simple example involving a nonlinear Van der Pol oscillator. As future work, we are working on the problem of path planning using the flexible safety notion herein proposed.

Appendix A

Proof of Theorem 1. First, we show that when the initial distribution μ_0 and the system dynamics (1) are given, the Liouville equation (16) has a unique solution (μ, μ_T) up to a subset of $[0,T]\times\mathcal{X}$ of Lebesgue measure zero and (μ,μ_T) coincide with the average occupation measure defined by (14) and the average final measure defined by (15). Let (μ,μ_T) be a pair of measures satisfying (16). From [21, Lemma 3], μ can be disintegrated as $d\mu(t,\mathbf{x}) = d\mu_t(\mathbf{x})dt$ where dt is the Lebesgue measure on $[0,T]$. $\mu_t(\mathbf{x})$ is a stochastic kernel on $\mathcal{X}$ given t and can be interpreted as the distribution of the states at time t following the evolution of (1) with $\mathbf{x}_0 \sim \mu_0$. $\mu_t(\mathbf{x})$ is uniquely defined dt-almost everywhere. As proved in [21, Lemma 3], μ_t satisfies a continuity equation which implies μ and μ_T coincide with the average occupation measure and the average final measure generated by the family of absolutely continuous admissible trajectories of (1) starting from μ_0.

Then solving $\mathtt{P}$ can be decomposed into two steps: first find a feasible $(\mu,\mu_T)\in\mathcal{M}_+([0,T]\times\mathcal{X})\times\mathcal{M}_+(\mathcal{X})$ to the Liouville equation $\delta_T\otimes\mu_T = \delta_0\otimes\mu_0 + \mathcal{L}^*\mu$ and then solve the following optimization problem:

$$\mathtt{Q}: \quad \sup_{\widetilde{\mu}}\{\int g d\widetilde{\mu} : \widetilde{\mu}\le\mu; \widetilde{\mu}\in\mathcal{M}_+([0,T]\times\mathcal{X}_u)\}. \quad (38)$$

Since $\mathcal{X}$ and $\mathcal{X}_u$ are compact with $\mathcal{X}_u\subseteq\mathcal{X}$, by [19, Theorem 3.1] the restriction $\widetilde{\mu}^*$ of μ to $\mathcal{X}_u$ defined by (20) is the unique optimal solution to $\mathtt{Q}$ and $\sup\mathtt{Q} = \max\mathtt{Q} = \int g d\widetilde{\mu}^* = \int_{\mathcal{X}_u} g d\mu$.

As the feasible μ in $\mathtt{P}$ coincides with the average occupation measure in (14), $\widetilde{\mu}^*$ is also the $\widetilde{\mu}$-component of an optimal solution to $\mathtt{P}$ and $\sup\mathtt{P} = \max\mathtt{P} = \int g d\widetilde{\mu}^*$. When $g\equiv 1$, we have $\max\mathtt{P} = \mu([0,T]\times\mathcal{X}_u)$ with μ being the average occupation measure defined in (14). □

Proof of Theorem 2. The proof follows the same lines as that of [21, Theorem 2]. Define

$$\mathbf{C} = \mathcal{C}([0,T]\times\mathcal{X}_u)\times\mathcal{C}([0,T]\times\mathcal{X})\times\mathcal{C}([0,T]\times\mathcal{X})\times\mathcal{C}(\mathcal{X})$$

$$\mathbf{M} = \mathcal{M}([0,T]\times\mathcal{X}_u)\times\mathcal{M}([0,T]\times\mathcal{X})\times\mathcal{M}([0,T]\times\mathcal{X})\times\mathcal{M}(\mathcal{X})$$

and let $\mathcal{K}$ and $\mathcal{K}'$ denote the positive cones of $\mathbf{C}$ and $\mathbf{M}$, respectively. By Riesz-Markov-Kakutani representation theorem [23], $\mathcal{K}'$ is the topological dual of the cone $\mathcal{K}$. The infinite dimensional linear program $\mathtt{P}$ can be written as:

$$\begin{aligned} \sup \quad & \langle\gamma, c\rangle \\ \text{s.t.} \quad & \mathcal{A}'\gamma = \beta, \quad \gamma\in\mathcal{K}' \end{aligned} \quad (39)$$

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

The dual to (39) can be interpreted as:

$$\begin{aligned} \inf \quad & \langle\beta, z\rangle \\ \text{s.t.} \quad & \mathcal{A}z - c\in\mathcal{K} \end{aligned} \quad (40)$$

where the infimum is over $z=(v,w)\in\mathcal{C}^1([0,T]\times\mathcal{X})\times\mathcal{C}([0,T]\times\mathcal{X})$, the linear operator $\mathcal{A}:\mathcal{C}^1([0,T]\times\mathcal{X})\times\mathcal{C}([0,T]\times\mathcal{X})\to\mathbf{C}$ is given by $\mathcal{A}z = (w, w, -\mathcal{L}v - w, v(T,\cdot))$ and satisfies the adjoint property $\langle\mathcal{A}'\gamma, z\rangle = \langle\gamma,\mathcal{A}z\rangle$. The linear program (40) is exactly (21).

From [33, Theorem 3.10], there is no duality gap between (39) and (40) if the supremum of (39) is finite and the

set $P = \{(\mathcal{A}'\gamma, \langle\gamma, c\rangle) \mid \gamma \in \mathcal{K}'\}$ is closed in the weak* topology of $\mathcal{K}'$. Since $\widetilde{\mu}$ is dominated by the average occupation measure μ and its underlying support is compact, the supremum of (39) is finite. To prove that P is closed, consider a sequence $\gamma_k = (\widetilde{\mu}^k, \widehat{\mu}^k, \mu^k, \mu_T^k) \in \mathcal{K}'$ such that $\mathcal{A}'\gamma_k \to a$ and $\langle\gamma_k, c\rangle \to b$ as $k \to \infty$ for some $(a, b) \in \mathcal{C}^1([0,T] \times \mathcal{X})^* \times \mathcal{M}([0,T] \times \mathcal{X}) \times \mathbb{R}$. Consider the test function $z_1 = (T - t, 0)$ which gives $\langle\mathcal{A}'\gamma_k, z_1\rangle = \mu^k([0,T] \times \mathcal{X}) \to \langle a, z_1\rangle < \infty$; since the measures μ^k are non-negative, this implies $\{\mu^k\}$ is bounded. By taking $z_2 = (1, -1)$, we have $\langle\mathcal{A}'\gamma_k, z_2\rangle = \mu_T^k(\mathcal{X}) + \widetilde{\mu}^k([0,T] \times \mathcal{X}_u) + \widehat{\mu}^k([0,T] \times \mathcal{X}) - \mu^k([0,T] \times \mathcal{X}) \to \langle a, z_2\rangle < \infty$; since $\{\mu^k\}$ is bounded, by similar arguments the sequences $\{\widetilde{\mu}^k\}$, $\{\widehat{\mu}^k\}$ and $\{\mu_T^k\}$ are bounded as well.

As a result, $\{\gamma_k\}$ is bounded and we can find a ball B in $\mathbf{M}$ with $\{\gamma_k\} \subset B$. From the weak* compactness of the unit ball (Alaoglu's theorem [34, Section 5.10, Theorem 1]) there is a subsequence $\{\gamma_{k_i}\}$ that weak*-converges to some $\gamma \in \mathcal{K}'$. Notice that $\mathcal{A}'$ is weak*-continuous because $\mathcal{A}z \in \mathbf{C}$ for all $z \in \mathcal{C}^1([0,T] \times \mathcal{X}) \times \mathcal{C}([0,T] \times \mathcal{X})$. So $(a, b) = \lim_{i\to\infty}(\mathcal{A}'\gamma_{k_i}, \langle\gamma_{k_i}, c\rangle) = (\mathcal{A}'\gamma, \langle\gamma, c\rangle) \in P$ by the continuity of $\mathcal{A}'$ and P is closed. □

Proof of Theorem 4. The proof of strong duality follows from standard SDP duality theory. Let $\Delta_\mu = (\widetilde{\mu}, \widehat{\mu}, \mu, \mu_T)$ be the optimal solution to $\mathtt{P}$ and $\Delta_y = (\widetilde{\mathbf{y}}, \widehat{\mathbf{y}}, \mathbf{y}, \mathbf{y_T})$ be their corresponding moment sequences. Any finite truncation of Δ_y gives a feasible solution to $\mathtt{P_r}$. As $\mathcal{X}$ and $\mathcal{X}_u$ have non-empty interior, we have the truncation of Δ_y is strictly feasible for $\mathtt{P_r}$. By Slater's condition [35], there is no duality gap between $\mathtt{P_r}$ and $\mathtt{D_r}$, i.e., $p_r^* = d_r^*$.

The proof of convergence follows from [20, Theorem 3.6]. Since $[0,T]$, $\mathcal{X}$ and $\mathcal{X}_u$ are compact sets, we can assume after appropriate scaling $T = 1$ and $\mathcal{X} \times \mathcal{X}_u \subseteq [-1,1]^{n_\mathcal{X}} \times [-1,1]^{n_{\mathcal{X}_u}}$, which implies that the feasible set of the semidefinite program $\mathtt{P_r}$ is compact. Let $\Delta_r^* = (\widetilde{\mathbf{y}}_r^*, \widehat{\mathbf{y}}_r^*, \mathbf{y}_r^*, \mathbf{y_T}_r^*)$ be the optimal solution of $\mathtt{P_r}$ and complete the finite vectors $(\widetilde{\mathbf{y}}_r^*, \widehat{\mathbf{y}}_r^*, \mathbf{y}_r^*, \mathbf{y_T}_r^*)$ with zeros to make them infinite sequences. By a standard diagonal argument, there is a subsequence $\{r_k\}$ and a tuple of infinite vectors $\Delta^* = (\widetilde{\mathbf{y}}^*, \widehat{\mathbf{y}}^*, \mathbf{y}^*, \mathbf{y_T}^*)$ such that $\Delta_{r_k}^* \to \Delta^*$ as $k \to \infty$, where the convergence is interpreted as elementary-wise. Since the infinite vector $\widetilde{\mathbf{y}}^*$ in Δ^* is the limit point of a subsequence of the optimal solutions $\widetilde{\mathbf{y}}_r^*$ of $\mathtt{P_r}$, $\widetilde{\mathbf{y}}^*$ satisfies all the constraints in $\mathtt{P_r}$ as $r \to \infty$. Then by *Putinar's Positivstellensatz*, $\widetilde{\mathbf{y}}^*$ has a representing measure $\widetilde{\mu}^*$ supported on $[0,T] \times \mathcal{X}_u$. Similarly, $\widehat{\mathbf{y}}^*, \mathbf{y}^*$ and $\mathbf{y_T}^*$ have their representing measures $\widehat{\mu}^*, \mu^*$ and μ_T^* with corresponding supports, respectively.

As problem $\mathtt{P_r}$ is a relaxation of $\mathtt{P}$, $p_r^* \geq p^*$ for each r. Thus we have $\lim_{k\to\infty} \sup \mathtt{P_{r_k}} = \lim_{k\to\infty} L_{\widetilde{\mathbf{y}}_{r_k}^*}(g) = L_{\widetilde{\mathbf{y}}^*}(g) = \int g d\widetilde{\mu}^* \geq p^*$. On the other hand, $\mathcal{A}_r(\Delta^*) = \lim_{k\to\infty} \mathcal{A}_r(\Delta_{r_k}^*) = b_r$ for each $r \in \mathbb{N}$. Let $(\widetilde{\mu}^*, \widehat{\mu}^*, \mu^*, \mu_T^*)$ be the tuple of representing measures of Δ^*. As measures on compact sets are determined by moments, $(\widetilde{\mu}^*, \widehat{\mu}^*, \mu^*, \mu_T^*)$ is a feasible solution to $\mathtt{P}$ which implies $\int g d\widetilde{\mu}^* \leq p^*$. Hence $\int g d\widetilde{\mu}^* = p^*$ and $(\widetilde{\mu}^*, \widehat{\mu}^*, \mu^*, \mu_T^*)$ is an optimal solution of $\mathtt{P}$. For any r we have $p_r^* \geq p_{r+1}^*$ because as r increases, the constraints in $\mathtt{P_r}$ become more restrict. As a result, $p_{r_k}^* \downarrow p^*$ and furthermore $p_r^* \downarrow p^*$. By strong duality, $d_r^* = p_r^* \downarrow p^* = d^*$. □

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. Ariyur, "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] A. Bemporad, F. D. Torrisi, and M. Morari, "Optimization-based verification and stability characterization of piecewise affine and hybrid systems," in *International Workshop on Hybrid Systems: Computation and Control*. Springer, 2000, pp. 45–58.

[7] A. Chutinan and B. H. Krogh, "Computational techniques for hybrid system verification," *IEEE Transactions on Automatic Control*, vol. 48, no. 1, pp. 64–75, 2003.

[8] B.Bollobás, "Volume estimates and rapid mixing," *Flavors of geometry*, vol. 31, pp. 151–182, 1997.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] S. Prajna, "Barrier certificates for nonlinear model validation," *Automatica*, vol. 42, no. 1, pp. 117–126, 2006.

[15] 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.

[16] 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.

[17] 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.

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

[19] 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.

[20] 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.

[21] 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.

[22] 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.

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

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

[25] 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.

[26] J. B. Lasserre, *Moments, positive polynomials and their applications*. World Scientific, 2009, vol. 1.

[27] ——, *An introduction to polynomial and semi-algebraic optimization*. Cambridge University Press, 2015, vol. 52.

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

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

[30] 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.

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

[32] A. Mosek, "The mosek optimization toolbox for matlab manual," 2015.

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

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

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