

Worst-Case Risk Quantification under Distributional Ambiguity using Kernel Mean Embedding in Moment Problem

Jia-Jie Zhu, Wittawat Jitkrittum, Moritz Diehl, Bernhard Schölkopf

Abstract—In order to anticipate rare and impactful events, we propose to quantify the worst-case risk under distributional ambiguity using a recent development in kernel methods — the kernel mean embedding. Specifically, we formulate the generalized moment problem whose ambiguity set (i.e., the moment constraint) is described by constraints in the associated reproducing kernel Hilbert space in a nonparametric manner. We then present the tractable optimization formulation and its theoretical justification. As a concrete application, we numerically test the proposed method in characterizing the worst-case constraint violation probability in the context of a constrained stochastic control system.

I. INTRODUCTION

We begin our discussion with the black swan metaphor, which was visited in a recent popular book [1]. It is argued that extremely rare events, like a black swan, may potentially have a huge impact on the underlying system. However, given limited historical data, statistical inference is prone to failures in predicting black swans. This issue is also relevant to optimization and control. Consider the illustrative Fig. 1 of a stochastic control system. All the sampled state trajectories (denoted by x_t , in blue) satisfy some underlying state constraint, which is staying below the curve (denoted by $c(x_t) \leq 0$, in red). If we are interested in estimating the constraint violation probability at a certain time from this empirical dataset, a naive Monte Carlo estimate yields

$$P(c(X_t) > 0) \approx \sum_{i=1}^N \frac{1}{N} \mathbb{1}\{c(x_t^{(i)}) > 0\} = 0,$$

i.e., zero violation probability. This is sometimes referred to as the zero-count problem, also known as the silent evidence or inductivist turkey. However, just like the black swan metaphor, the constraint violation event may be rare but potentially impactful to the system.

The key here is to capture the concept of distributional ambiguity, i.e., we are uncertain about our knowledge of the probability measure itself. For example, the classical Cantelli’s inequality for a zero mean unit variance random

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 798321, the German Federal Ministry for Economic Affairs and Energy (BMWi) via eco4wind (0324125B) and DyConPV (0324166B), and by DFG via Research Unit FOR 2401.

Jia-Jie Zhu, Wittawat Jitkrittum, and Bernhard Schölkopf are with the Empirical Inference Department, Max Planck Institute for Intelligent Systems, Tübingen, Germany. {jjzhu, wittawat, bs}@tuebingen.mpg.de

Moritz Diehl is with the Department of Microsystems Engineering, University of Freiburg, Freiburg, Germany. moritz.diehl@imtek.uni-freiburg.de

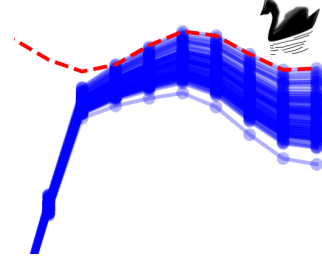


Fig. 1: Rare constraint violation event as the black swan

variable $X \sim P$ states $P(X > c) \leq \frac{1}{1+c^2}$, regardless of what distribution P is. It is commonly argued in the literature of optimization and control, e.g., [2], [3], that such bounds are pessimistic. However, if P is subject to perturbations, then the statistics such as mean and variance may become uncertain. We refer to such uncertainty in distributions as *ambiguity*. For example, in machine learning applications such as [4], individual data samples themselves may be perturbed by an adversarial or nature. Consequently, the original already-conservative bound may fail to hold. From this point of view, we must ask, “how can nature perturb the empirical data distribution to hurt us the most?”

Generalized moment problem: In the mathematics literature, this is the study of the moment problem such as the classical moment problems of Stieltjes, Hausdorff, and Hamburger a century ago. In a nutshell, a generalized moment problem can be abstractly written as

$$\underset{P \in \mathcal{C}}{\text{maximize}} \mathbb{E}_P l(x), \quad (1)$$

where \mathcal{C} is a set of probability measures. In this paper, we refer to \mathcal{C} as the *ambiguity set*. For example, $\mathcal{C} = \{P \mid \int \phi_i(x) dP(x) = m_i, i = 1 \dots p\}$ where ϕ_i ’s are some given moment functions and m_i ’s are moments. This optimization problem searches for the *worst-case risk* — expected value of $l(x)$ under the *worst-case distribution*.

The literature related to the moment problem is vast spanning over decades. We now discuss a thread of modern computational approaches to deriving a bound (e.g., right-hand-side of Cantelli’s inequality). The early work of [5] contains the duality approach to the moment problem. Subsequently, [6] proved strong duality using conic linear programming and the finite dimension reduction results from [7]. Modern computational approaches such as [8], [9], [10] proposed SDP formulations for the moment problem under the assumption that the moment functions are polynomial-representable. Subsequently and built on that work, [2] used Choquet theory to study a few classes of non-degenerative

TABLE I: Examples of distributional ambiguity descriptions

[10], [2], [11], [12]	Known first p moments
[14]	Prokhorov metric
[19]	ϕ -divergence
[15]	Wasserstein metric
This paper	RKHS metric

distributions (e.g. unimodal) to reduce the conservativeness of the bound. [11] showed that a worst-case probability problem admits exact SDP reformulation under the conditions that constraint set is a quadratic inequality and ambiguous distributions share the first two moments. Under similar ambiguity assumptions, [12] also used Choquet theory for the non-degenerative classes of distributions to derive exact reformulations under polyhedral constraints. Another related thread of work is the distributionally robust optimization (DRO) (e.g., [13], [14], [15], [16], [17], [18]), as well as related approaches in data-driven robust optimization such as [19], [20], which studies decision-making under distributional ambiguity. In a nutshell, it aims to find a decision after the worst-case distribution in (1) is assumed. Therefore, while this paper does not study DRO, the moment problem naturally becomes the inner optimization problem for DRO.

At the core of those works is the description for the ambiguity set, e.g., the set of distributions \mathcal{C} in (1). We summarize a few example approaches taken in Table I. To characterize ambiguity, this paper summons a recent development in kernel methods, the kernel mean embedding. This framework can represent probability distributions as functionals in the reproducing kernel Hilbert space. This elegant structural mapping allows us to cast worst-case probability measures as decision variables of optimization problems, as we shall introduce shortly.

The *main contributions* of this paper are in using the kernel mean embedding for distributional ambiguity description, as well as the novel tractable formulations (e.g. (3),(4)) and their theoretical justification (e.g. we prove a novel convergence result in Proposition 1). We then demonstrate how to use them in practice in the context of quantifying worst-case constraint violation probability of a stochastic control system.

Organization: The paper is organized as follows. Sec. II presents the background on the kernel mean embedding framework. We then propose our main method in Sec. III, whose proofs are deferred to later in Sec. V (application-driven readers may choose to skip the proofs). In Sec. IV, we analyze the proposed method in two numerical experiments: a synthetic worst-case probability problem and a stochastic control problem. The paper is concluded in Sec. VI.

Notation: In this paper, $\mathcal{X} \subseteq \mathbb{R}^n$ denotes the domain or input space of interest, e.g., the state space of a system. \mathcal{M} denotes the vector space of all signed measures defined on $\mathcal{B}(\mathcal{X})$, where $\mathcal{B}(\mathcal{X})$ is the Borel algebra. \mathcal{P} denotes the set of all probability measures on $\mathcal{B}(\mathcal{X})$. \mathcal{H} denotes the reproducing kernel Hilbert space associated with the kernel in the context. \int denotes the Stieltjes integral for both discrete and continuous distributions. M often denotes the

number of data samples we have. δ_x is the Dirac measure at x . By embedding, we refer to the kernel mean embedding which we shall introduce next.

II. PRELIMINARIES ON KERNEL MEAN EMBEDDING

In this section, we give a brief overview of the kernel mean embedding — a modern development in kernel methods — which enables us to describe distributional ambiguity non-parametrically. We start with the definition of a kernel. A symmetric function $k: \mathcal{X} \times \mathcal{X} \rightarrow \mathbb{R}$ is said to be a positive definite kernel if for any $N \in \mathbb{Z}^+$, any $\{x_1, \dots, x_N\} \subset \mathcal{X}$, and any $\alpha_1, \dots, \alpha_N \in \mathbb{R}$, we have $\sum_{i=1}^N \sum_{j=1}^N \alpha_i \alpha_j k(x_i, x_j) \geq 0$. We will subsequently refer to a positive definite kernel simply as a kernel. Given a kernel k , the Moore-Aronszajn theorem [21] guarantees the existence of a Hilbert space \mathcal{H} of real-valued functions, and a map $\phi: \mathcal{X} \rightarrow \mathcal{H}$, such that $\langle f, \phi(x) \rangle_{\mathcal{H}} = f(x)$ for all $f \in \mathcal{H}$, $x \in \mathcal{X}$, where $\langle \cdot, \cdot \rangle := \langle \cdot, \cdot \rangle_{\mathcal{H}}$ denotes the inner product on \mathcal{H} . This property is known as the reproducing property, and \mathcal{H} is known as the reproducing kernel Hilbert space (RKHS) associated with the kernel k . The map ϕ is commonly known as a feature map. The reproducing property implies that $k(x, x') = \langle \phi(x), \phi(x') \rangle$ for any $x, x' \in \mathcal{X}$. Therefore, we interchangeably write $k(x, \cdot)$ and $\phi(x)$.

The kernel mean embedding [22] is a technique that gives nonparametric representations of distributions in an RKHS. More precisely, given a probability distribution P and a kernel k , the (kernel mean) embedding of P is defined as

$$\mu_P(\cdot) = \int k(x, \cdot) dP(x), \quad (2)$$

which is simply the expectation of the feature map under distribution P . If $\mathbb{E}_{x \sim P} k(x, x) < \infty$, then μ_P exists and is in \mathcal{H} [22]. One may also view $\mu_P \in \mathcal{H}$ as a vectorial representation of P in \mathcal{H} . For example, if $\mathcal{X} = \mathbb{R}$, $\phi(x) := (x, x^2)^\top$, then $k(x, y) = xy + x^2y^2$, and $\mu_P = (\mathbb{E}_{x \sim P}[x], \mathbb{E}_{x \sim P}[x^2])^\top$ which contains the first two moments of P . More generally, if the kernel k is *characteristic*, then the kernel mean map $P \mapsto \mu_P$ is injective so that μ_P is unique for any distribution P [23]. An example of the characteristic kernel is the Gaussian kernel $k(x, y) = \exp\left(-\frac{\|x-y\|_2^2}{2\sigma^2}\right)$ for any bandwidth $\sigma \in (0, \infty)$. This kernel defines an infinite-dimensional feature map ϕ .

The embedding can be used to define a distance between two distributions. Specifically, given two Borel probability measures P, Q , and a characteristic kernel, one can show that $\|\mu_P - \mu_Q\|_{\mathcal{H}}$ defines a proper distance in the associated RKHS \mathcal{H} . This distance is also known as the maximum mean discrepancy (MMD) [24]. Note that $\|f\|_{\mathcal{H}} := \sqrt{\langle f, f \rangle_{\mathcal{H}}}$ for any $f \in \mathcal{H}$. It follows that

$$\begin{aligned} \|\mu_P - \mu_Q\|_{\mathcal{H}}^2 &= \mathbb{E}_{x, x' \sim P} k(x, x') \\ &\quad - 2\mathbb{E}_{x \sim P} \mathbb{E}_{y \sim Q} k(x, y) + \mathbb{E}_{y, y' \sim Q} k(y, y'), \end{aligned}$$

which can be estimated with the plug-in estimator using the samples from P and Q by virtue of the kernel trick [24].

This paper's idea is to use the embedding and the distance in RKHS to characterize the distributional ambiguity and perform optimization. [25] already contains the idea of using embedding as optimization variables. However, that work used regularized formulations without rigorously characterizing the distributions corresponding to the solutions. [26] used embedding to estimate the probability, but did not solve optimization problems or anticipating the worst case. Their convergence result also requires the function to be in the Besov space, as opposed to Proposition. 1.

III. KERNEL MEAN EMBEDDING MOMENT PROBLEM

Suppose we have formed an understanding of our data in the form of the data distribution embedding $\mu_{\hat{P}}$. For example, $\mu_{\hat{P}}$ can be given by the empirical embedding $\mu_{\hat{P}} = \frac{1}{M} \sum \phi(x_i)$ given data samples $\{x_i\}_{i=1}^M$. Alternatively, it can also be the embedding of a continuous distribution such as $\mu_{\hat{P}} = \int \phi(x) d\hat{P}(x)$, $\hat{P} \sim N(\mu, \sigma)$. We now propose the kernel mean embedding moment problem (KME-MP)

$$\begin{aligned} & \underset{P, \mu}{\text{maximize}} && \int l(x) dP(x) \\ & \text{subject to} && \|\mu - \mu_{\hat{P}}\|_{\mathcal{H}} \leq \epsilon \\ & && \int \phi(x) dP(x) = \mu \\ & && P \in \mathcal{P}, \mu \in \mathcal{H}, \end{aligned} \quad (3)$$

where $l(x)$ is a bounded cost function of interest. The optimal value of (3) is referred to as the worst-case risk. $\|\cdot\|_{\mathcal{H}}$ is the Hilbert space norm. The second constraint is the embedding mapping. \mathcal{P} is the set of all probability measures. Our formulation above made obvious that, intuitively, the embedding μ may be viewed as a *generalized moment vector*. Using the *kernel trick*, the RKHS structure allows us to work with infinite-dimensional moment vector μ , therefore generalizing the moment problem (1).

In the optimization problems of this paper, we focus on empirical embeddings of the form $\mu = \sum_{i=1}^N \alpha_i \phi(z_i)$ with the expansion coefficient $\alpha_i \in \mathbb{R}$ and expansion points $z_i \in \mathcal{X}$ (also called locations), for $i = 1 \dots N$. This can also be thought of as a finite-sample estimator of (2). Using this representation, a concrete version of problem 3 is given by

$$\begin{aligned} & \underset{\alpha}{\text{maximize}} && \sum_{i=1}^N \alpha_i l(z_i) \\ & \text{subject to} && \left\| \sum_{i=1}^N \alpha_i \phi(z_i) - \sum_{i=1}^M \frac{1}{M} \phi(x_i) \right\|_{\mathcal{H}} \leq \epsilon, \end{aligned}$$

where $\{x_i\}_{i=1}^M$ is the data set we have in hand. Using the kernel trick, the constraint can be written as the convex quadratic constraint

$$\alpha^\top K_z \alpha - 2 \frac{1}{M} \alpha^\top K_{zx} \mathbf{1} + \frac{1}{M^2} \mathbf{1}^\top K_x \mathbf{1} \leq \epsilon^2,$$

where K_z, K_{zx}, K_x are the gram matrices associated with the kernel $K_z = [k(z_i, z_j)]_{ij}, K_{zx} = [k(z_i, x_j)]_{ij}, K_x = [k(x_i, x_j)]_{ij}$, $\mathbf{1}$ is a vector of 1's, $\mathbf{1} = [1, \dots, 1]^\top$, and $\alpha := (\alpha_1, \dots, \alpha_N)^\top$.

Remark. One may alternatively choose to make $\{z_i\}_{i=1}^N$ decision variables of the optimization formulation, e.g., in machine learning applications [27]. However, doing so will make the optimization intractable.

Given we have solved the above optimization problem and obtained an embedding $\mu^* = \sum_{i=1}^N \alpha_i^* \phi(z_i) \in \mathcal{H}$, it does not always correspond to a probability distribution.

Therefore, we must establish a few theoretical results whose proofs are deferred to Sec. V. They lead to the main optimization formulation of this paper. Following that, we apply our method to characterize the worst-case constraint violation probability.

Lemma 1. Suppose we have an embedding of the form $\mu_P = \sum_{i=1}^N \alpha_i \phi(x_i)$ with $N < \infty$, then the corresponding signed measure P is a probability measure if and only if $\sum_{i=1}^N \alpha_i = 1, \alpha_i \geq 0$.

Thus, we obtain the practical form of the KME-MP problem

$$\begin{aligned} & \underset{\alpha}{\text{maximize}} && \sum_{i=1}^N \alpha_i l(z_i) \\ & \text{subject to} && \alpha^\top K_z \alpha - 2 \frac{1}{M} \alpha^\top K_{zx} \mathbf{1} + \frac{1}{M^2} \mathbf{1}^\top K_x \mathbf{1} \leq \epsilon^2 \\ & && \sum_{i=1}^N \alpha_i = 1, \alpha_i \geq 0, i = 1 \dots N. \end{aligned} \quad (4)$$

This optimization problem is by itself convex and tractable. It does not need a dual reformulation for the purpose of this paper. This is different from, e.g., methods using Wasserstein metric. It does not need a dual reformulation for this paper's purpose. This is different from, e.g., methods using Wasserstein metric. The feasibility of this problem is trivially assured.

Lemma 2. If the new expansion points contain the original data points $\{z_i\}_{i=1}^N \supseteq \{x_i\}_{i=1}^M$ and $\epsilon > 0$, the optimization problem (4) is strictly feasible.

Moreover, we have the following relationship between the practical formulation (4) and the original formulation (3).

Proposition 1. Suppose $l(x)$ is a bounded, lower semicontinuous function. Let P^* be the solution of the original formulation (3). $\{\alpha_i^*\}_{i=1}^N$ is the solution of (4) with $\{z_i\}_{i=1}^N$ sampled from a distribution that has common support with P^* , i.e., $\{z_i\}_{i=1}^N \sim Q_z, \text{supp}(Q_z) \supseteq \text{supp}(P^*)$. Then

$$\sum_{i=1}^N \alpha_i^* l(z_i) \xrightarrow{N \rightarrow \infty} \int l(x) dP^*(x).$$

Furthermore, $\sum_{i=1}^N \alpha_i^* l(z_i) \leq \int l(x) dP^*(x)$, i.e., the optimal value of (4) converges to that of (3) from below.

We give a novel proof in Sec. V-C.

Remark. In practice, we may not know what $\text{supp}(P^*)$ is in order to sample $\{z_i\}_{i=1}^N \sim Q_z$ with common support.

However, we typically have domain knowledge that where the samples may live, e.g., for states of a dynamical system. This motivates us, in finite-sample cases, to restrict the sampling on a compact domain. We may simply use a uniform sampling or gridding on some set that contains the whole feasible set. Importantly, we also want to sample points that may violate the constraints, as will be made clear in the next application.

This result of convergence from below is particularly useful, e.g. in stress testing models, as we may make the following intuitive statement. “The worst-case cost is at least as bad as $\sum_{i=1}^N \alpha_i^* l(z_i)$.” This is sometimes referred to as a *robust lower bound*. Hence, our optimization formulation could be understood as searching for a maximized lower bound to the worst-case risk.

Application: evaluating the worst-case probability

One application of the proposed method is to evaluate the worst-case probability of a certain event. For example, this arises in stochastic control when dealing with a chance constraint of form $P(X \in C) \geq 1 - \delta$. In the context of this paper, we consider the presence of ambiguity in the underlying distribution P , i.e., $P \in \mathcal{C}$ for some ambiguity set \mathcal{C} . We are interested in evaluating

$$\underset{P}{\text{maximize}} P(X \notin C) \quad \text{subject to} \quad P \in \mathcal{C} \subseteq \mathcal{P}.$$

Chance constraints with ambiguity is also referred to as distributionally robust chance constraints. Intuitively, by solving this optimization, we are evaluating the worst-case tail probability of the risk. Obviously, optimization with respect to probability distribution is a special case of the moment problem (3) with the cost function $l(x)$ given by the indicator function $\mathbb{1}\{x \notin C\}$. Hence, we have the following concrete formulation adapted from (4).

$$\begin{aligned} & \underset{\alpha}{\text{maximize}} \quad \sum_{i=1}^N \alpha_i \mathbb{1}\{z_i \notin C\} \\ & \text{subject to} \quad \alpha^\top K_z \alpha - 2 \frac{1}{M} \alpha^\top K_{zx} \mathbf{1} + \frac{1}{M^2} \mathbf{1}^\top K_x \mathbf{1} \leq \epsilon^2 \\ & \quad \sum_{i=1}^N \alpha_i = 1, \alpha_i \geq 0, i = 1 \dots N. \end{aligned} \quad (5)$$

Our convergence result in Proposition 1 applies since $\mathbb{1}\{x \notin C\}$ is bounded and lower semicontinuous if C is closed.

Remark. (Geometric interpretation) We may also view the KME expansion $\sum_{i=1}^N \alpha_i \phi(z_i)$ as putting probability mass α_i on location z_i . Then the worst-case risk can be interpreted as an adversarial, such as nature, trying to move the mass to incur the worst cost. This draws a connection between our approach and optimal transportation metric-based approach such as [15]. We later demonstrate this interpretation in Sec. IV, Fig. 3.

Alternative ambiguity set with known first p moments

Ambiguity sets with known first p moments are typically studied separately from metric-ball constraints. We now propose the following unified view using KME. Let us consider

the polynomial kernel of order p : $k(x, x') = (x^\top x' + 1)^p$. For simplicity, we set $p = 2$. We consider (4) associated with this kernel, obtaining the following moment problem under known first p moments. The derivation is provided in Sec. V.

$$\begin{aligned} & \underset{P \in \mathcal{P}, \mu_P}{\text{maximize}} \quad \sum_{i=1}^N \alpha_i l(z_i) \\ & \text{subject to} \quad \alpha^\top K_z \alpha \\ & \quad - 2 \sum_{i=1}^N \alpha_i (z_i^\top \mathbb{E} x x^\top z_i + 2 \mathbb{E} x^\top z_i + 1) \\ & \quad + \text{Tr}(\mathbb{E} x x^\top \mathbb{E} x x^\top) + 2 \mathbb{E} x^\top \mathbb{E} x + 1 \leq \epsilon^2 \\ & \quad \sum_{i=1}^N \alpha_i = 1, \alpha_i \geq 0, i = 1 \dots N, \end{aligned} \quad (6)$$

where $K_z = [k(z_i, z_j)]_{ij}$ again denotes the Gram matrix. However, the polynomial kernel is not characteristic: the mapping $\int \phi(x) dP(x) = \mu_P$ is finite-dimensional. Intuitively speaking, it can not distinguish all distributions that share the (finitely many) known moments, hence incurring ambiguity. Problem (6) is convex, nonetheless.

Remark. The first p moments are typically estimated from data. Therefore, it is sometimes argued that one may skip the estimation step and favor directly using nonparametric formulation such as KME-MP (4). Nonetheless, the computational procedure is similar. For this reason as well as clarity, this paper focuses on (4) instead of (6).

IV. NUMERICAL EXPERIMENT

In this section, we solve the proposed optimization problem (4), (5) to quantify the worst-case risk in synthetic example and a stochastic control problem. We focus on describing experimental results and their implications. Additional detailed descriptions of the experimental setup are given in the appendix, in Sec. VII.

A. Synthetic worst-case probability problem

Suppose X is a real-valued random variable whose distribution is *unknown* to us. We only have access to the empirical data samples $\{x_i\}_{i=1}^M$. We are interested in quantifying the worst-case violation probability of the event $\{X \leq c\}$. To this end, we cast the problem in the form of (3).

$$\begin{aligned} & \underset{P \in \mathcal{P}, \mu \in \mathcal{H}}{\text{maximize}} \quad P(X > c) \\ & \text{subject to} \quad \|\mu - \mu_{\hat{P}}\|_{\mathcal{H}} \leq \epsilon, \int \phi(x) dP(x) = \mu, \end{aligned}$$

where $\mu_{\hat{P}} = \sum_{i=1}^M \frac{1}{M} \phi(x_i)$ is the mean embedding of the empirical data distribution.

To estimate the worst-case violation probability, we solve the proposed tractable optimization formulation (5) with various levels of ambiguity ϵ . As a result, we obtain the solution to (5), $\{\alpha_i^*\}_{i=1}^N$, as well as the corresponding worst-case violation probability. We plot this quantity in Fig. 2. As we can observe from the figure, the proposed method is able

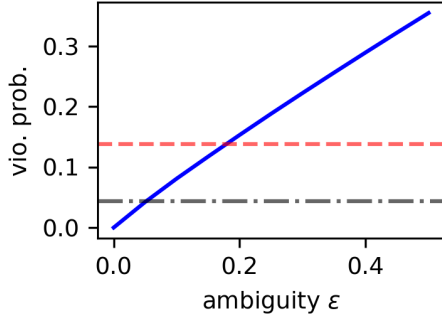


Fig. 2: (blue line) This figure depicts the value of worst-case violation probability (y -axis), i.e., $\sup_P P(x > c)$ changes with respect to the various allowed ambiguity level ϵ (x -axis) in the worst-case risk quantification problem. As we increase the ambiguity level ϵ , the worst-case violation probability exceeds both Chernoff's (gray dashed) and Cantelli's (red dashed) bound. See Appendix VII-A for more details.

to estimate the worst-case value as the ambiguity level ϵ increases. See the figure caption for more details.

Let us first recall classical Cantelli's inequality mentioned in the introduction. It bounds the tail probability of any distribution sharing the first two moments. In our dataset, Cantelli's inequality yields a tail bound $P(x \geq 2.5) \leq \frac{1}{1+2.5^2} \approx 0.138$, which is of course not sharp. For example, a sharper bound in this case is given by the Chernoff's bound. $P(x \geq 2.5) \leq \exp(-2.5^2/2) \approx 0.044$. Even pessimistic bounds are subject to violation under distributional ambiguity. As we can observe in Fig. 2, with a large enough ambiguity level ϵ , the worst-case risk exceeds that of the bounds given by the Chernoff's and Cantelli's inequality. This implies the importance of anticipating distributional ambiguity that may defeat even conservative safety bounds.

We now analyze the behavior of our approach more carefully. As we have discussed in Sec. III, we may interpret the coefficient α_i of the embedding $\sum_{i=1}^N \alpha_i \phi(z_i)$ as the mass of this discrete distribution at location x_i . For simplicity of viewing, we first sample a small set of $M = 10$ points $\{x_i\}_{i=1}^M$ to be our empirical data samples. In this case, all sampled points are on the left side of $c = 2.5$. The naive Monte Carlo estimate of the violation probability yields $P(X > c) \approx \sum_{i=1}^N \frac{1}{N} \mathbb{1}\{x_i > c\} = 0$. Recall this is the phenomenon of silent evidence discussed in the introduction. We now demonstrate that, by applying the proposed method, we are able to anticipate the potential violation with limited data.

We then solve the optimization problem (5) and plot the expansion weights $\{\alpha_i\}_{i=1}^N$ in Fig. 3 for various ambiguity levels ϵ . Similar to our geometric interpretation of (5), the mass is “transported” from left-hand-side of c (constraint satisfaction), to the right-hand-side (constraint violation). This is reminiscent of the worst-case risk characterized by optimal transport metric, e.g., in [15].

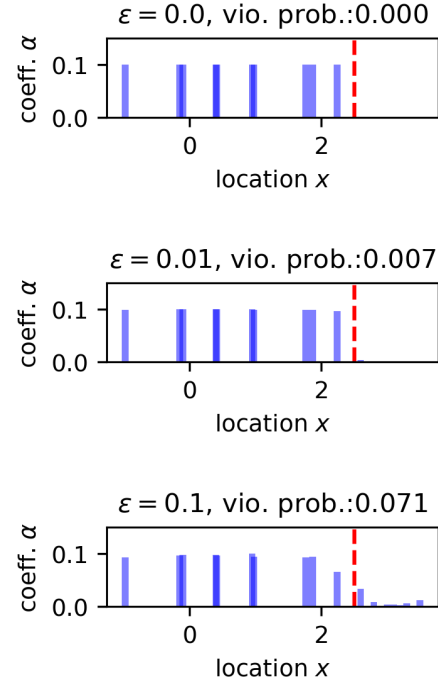


Fig. 3: Examining the worst-case constraint violation behavior under different ambiguity level. The (blue) vertical bars indicate the mass (height) allocated at a certain location x (horizontal axis). The (red) bar indicates the constraint level $c = 2.5$. (top) $\epsilon = 0$, no distributional ambiguity is allowed. All the mass stayed within the constraint. (middle) $\epsilon = 0.01$, a small amount of mass is shifted to the right side. The violation probability is 0.7%. (bottom) $\epsilon = 0.1$, violation probability 7.1%. More mass is allowed to be moved to the violation side due to a larger tolerance of ambiguity. See Appendix VII-A for more details.

B. Worst-case constraint violation in stochastic control

In this experiment, we are interested in the constrained stochastic optimal control problem (OCP). We consider the system model of the Van der Pol oscillator

$$\frac{d}{dt} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} x_2 \\ -0.1(1 - x_1^2)x_2 - x_1 + u \end{bmatrix}.$$

This example was adapted from [28]. The goal of the control design is to steer the system state x_1 as high as possible while staying below the bound (for simplicity, we use the constraint $x_1 \leq 1.5$). This is formulated as the following uncertain OCP.

$$\begin{aligned} & \underset{x(\cdot), u(\cdot)}{\text{minimize}} && \int_0^T \|x_1(t) - 3.0\|_2^2 dt \\ & \text{subject to} && \dot{x}(t) = f(x(t), u(t)), \quad \forall t \in [0, T] \\ & && -40 \leq u(t) \leq 40, \quad \forall t \in [0, T] \\ & && -0.25 \leq x_1(t) \leq 1.5, \quad \forall t \in [0, T] \\ & && x(0) = s, \end{aligned} \quad (7)$$

where the initial state s is uncertain. To work with the nonlinear dynamics, we adopt the scenario MPC [29] to solve

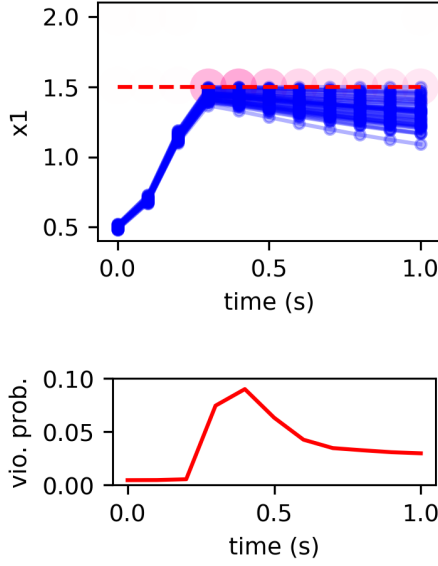


Fig. 4: This figure is best viewed in color. In this simulation, the ambiguity level is set to $\epsilon = 0.01$. (top) State trajectory (blue) of the solution to the stochastic OCP. The constraint is to stay below the (red dashed) line. The (pink) shaded area denotes violation mass is transported to this location. The higher the mass, the darker the shade. (bottom) is the plot of the worst-case violation probability $\sup_P P(x > 1.5)$ under ambiguity by solving the optimization problem (5). The horizontal axis is time. See Appendix VII-B for more details.

for the optimal control input. The state trajectory associated with the OCP solution is plotted in Fig. 4 (top).

Furthermore, we assume there is ambiguity in the state distribution \mathbb{P}_{x_t} . Given the empirical data distribution $\hat{\mathbb{P}}_{x_t} = \frac{1}{N} \sum \delta_{x_{t_i}}$ at time t , we are interested in quantifying the worst-case violation probability

$$\sup_P P(X_t > 1.5) \text{ subject to } \|\mu_P - \mu_{\hat{\mathbb{P}}_{x_t}}\|_{\mathcal{H}} \leq \epsilon.$$

The recent work of [30] has advocated using embedding for representing and propagating uncertainty. We now demonstrate our framework can use this representation to stress test the control design. To this end, we solve (5) and plot the worst-case violation probability at each time-step in Fig. 4 (bottom). There is no violation in the beginning as the initial states are far from the constraint boundary. However, as the system is steered closer to the boundary, the worst-case violation probability rises.

Similar to the previous example, we visualize the geometric interpretation in Fig. 4 (top), illustrated as the shaded area (pink). The darkness of the shade is proportional to the amount of the violation probability mass. We may interpret our method as transporting mass to the locations of violation states to create a worst-case distribution. Unlike previous approaches such as [12], our method does not require the constraint region to be polyhedral. We now test the case

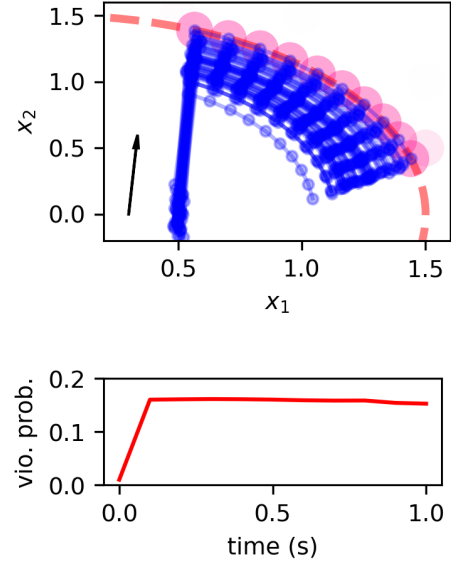


Fig. 5: This figure is best viewed in color. The dynamics is the same as that in Fig. 4 except for we try to quantify the worst-case violation probability for the non-polyhedral constraint regions, $\sup_P P\{\sqrt{(x_1^2 + x_2^2)} > 1.5\}$ under ambiguity. (top) is the phase plot of the system. (arrow) indicates the direction of the state trajectory over time. The (red) boundary is a circle. The (black) arrow indicates the direction of the state over time. The worst-case violation is shaded in (pink) color. (bottom) plots the violation probability in time.

where the event has a simple non-nonlinear multivariate constraint $\{\sqrt{(x_1^2 + x_2^2)} \leq 1.5\}$. (In fact, it does not need to be quadratic either.) Fig. 5 illustrates the resulting phase plot of the system and the worst-case violation probability. The interpretation is similar to Fig. 4.

The implication of this experiment is interesting from the perspective of optimal control design. Traditional stochastic control aims to bound most of the probability mass of the uncertainty to stay within bound — such as constraint tightening in stochastic MPC (cf. [3], [31]). We aim to reason beyond this; Although all the stochastic control trajectories in our experiment satisfy the constraints, we were able to quantify non-zero worst-case violation probability. To robustify against the worst-case risk under the distributional ambiguity quantified by this paper, the control design must be *distributionally robust*.

V. PROOFS OF THEORETICAL RESULTS

A. Proof of Lemma 1

Proof. Consider a convex combination of N Dirac measures $P = \sum_{i=1}^N \alpha_i \delta_{z_i}$. Its embedding is $\mu_P = \sum_{i=1}^N \alpha_i \phi(z_i)$. Obviously, P is a probability measure if and only if $\sum_{i=1}^N \alpha_i = 1, \alpha_i \geq 0$. The conclusion follows. \square

B. Proof of Lemma 2

Proof. Since $\{x_i\}_{i=1}^M \subseteq \{z_i\}_{i=1}^N$, we can trivially choose $\sum_{i=1}^N \alpha_i \phi(z_i) = \sum_{i=1}^M \frac{1}{M} \phi(x_i)$ which is strictly feasible.

□ Since P^* is the probability measure that attains the worst-case objective value, we always have

$$\sum_{i=1}^N \alpha_i^* l(z_i) \leq \int l(x) dP^*(x), \forall N \in \mathbb{Z}^+. \quad (12)$$

Combining (11) and (12), we obtain the convergence. □

C. Proof of Proposition 1

Proof. Let \mathcal{D} be the space of all convex combinations of Dirac measures supported on \mathcal{X} . It is a fact \mathcal{D} is dense in the space of all probability distributions \mathcal{P} on \mathcal{X} . Its proof can be found in standard texts, e.g., [32] Theorem 6.3. Hence, there exists a sequence of probability measures $Q_n \in \mathcal{D}$ that converges to P^* weakly, i.e. $Q_n \Rightarrow P^*$. Let $Q_n = \sum_{i=1}^{K^{(n)}} \gamma_i^{(n)} \delta_{y_i^{(n)}}$, where $\sum_{i=1}^{K^{(n)}} \gamma_i^{(n)} = 1, \gamma_i^{(n)} \geq 0$ for $i = 1 \dots K^{(n)}$. By the Portmanteau theorem, this weak convergence implies

$$\liminf_{n \rightarrow \infty} \int l(x) dQ_n(x) \geq \int l(x) dP^*(x), \quad (8)$$

for any bounded lower semicontinuous function l . Note we assume $\text{supp}(Q_n) \subseteq \text{supp}(P^*)$, since otherwise we could replace Q_n by its restriction to $\text{supp}(P^*)$.

Now we prove that $\liminf_{N \rightarrow \infty} \sum_{i=1}^N \alpha_i^* l(z_i) \geq \int l(x) dQ_n(x)$ for a given n . Due to the assumptions that the $\{z_i\}_{i=1}^N$ are generated from the distribution whose support contains $\text{supp}(P^*)$, we have for any support point $y_i^{(n)}$ of Q_n ,

$$\text{dist}(\{z_i\}_{i=1}^N, y_i^{(n)}) := \min_{z \in \{z_i\}_{i=1}^N} d(z, y_i^{(n)}) \xrightarrow{N \rightarrow \infty} 0,$$

where d is the usual distance on \mathcal{X} . Therefore, there exists a sequence $\{z_i^{(n),N}\}_{N=1}^\infty$ such that $z_i^{(n),N} \in \{z_i\}_{i=1}^N$ and

$$d(z_i^{(n),N}, y_i^{(n)}) \xrightarrow{N \rightarrow \infty} 0. \quad (9)$$

For fixed n , we use $\{z_i^{(n),N}\}_{N=1}^\infty$ to construct a sequence of distributions $\hat{Q}_n^N := \sum_{i=1}^{K^{(n)}} \gamma_i^{(n)} \delta_{z_i^{(n),N}}$ that will converge weakly to Q_n , where $K^{(n)}, \gamma_i^{(n)}$ are from the definition of Q_n . Due to the lower semicontinuity of l and (9), we have

$$\begin{aligned} \liminf_{N \rightarrow \infty} \int l(x) d\hat{Q}_n^N(x) &= \sum_{i=1}^{K^{(n)}} \gamma_i^{(n)} \left(\liminf_{N \rightarrow \infty} l(z_i^{(n),N}) \right) \\ &\geq \sum_{i=1}^{K^{(n)}} \gamma_i^{(n)} l(y_i^{(n)}) = \int l(x) dQ_n(x). \end{aligned} \quad (10)$$

As $\{\alpha_i^*\}_{i=1}^N$ attains the maximum of (4) and $z_i^{(n),N} \in \{z_i\}_{i=1}^N$,

$$\sum_{i=1}^N \alpha_i^* l(z_i) \geq \sum_{i=1}^{K^{(n)}} \gamma_i^{(n)} l(z_i^{(n),N}).$$

In the above inequality, we let $N \rightarrow \infty$ and use (10),

$$\liminf_{N \rightarrow \infty} \sum_{i=1}^N \alpha_i^* l(z_i) \geq \sum_{i=1}^{K^{(n)}} \gamma_i^{(n)} l(y_i^{(n)}) = \int l(x) dQ_n(x).$$

Now we let $n \rightarrow \infty$ and use (8), we obtain

$$\begin{aligned} \liminf_{N \rightarrow \infty} \sum_{i=1}^N \alpha_i^* l(z_i) &\geq \liminf_{n \rightarrow \infty} \int l(x) dQ_n(x) \\ &\geq \int l(x) dP^*(x). \end{aligned} \quad (11)$$

D. RKHS ambiguity set with known first p moments

The embedding associated with this kernel is

$$\begin{aligned} \hat{\mu} &= \int k(x, \cdot) dP(x) = \int (x^\top (\cdot) + 1)^2 dP(x) \\ &= (\cdot)^\top \mathbb{E} x x^\top (\cdot) + 2 \mathbb{E} x^\top (\cdot) + 1 \end{aligned} \quad (13)$$

By virtue of the kernel trick,

$$\begin{aligned} \|\mu_P - \hat{\mu}\|_{\mathcal{H}} &= \left\| \sum_{i=1}^N \alpha_i \phi(x_i) - \int k(x, \cdot) dP(x) \right\| \\ &= \alpha^\top K_z \alpha - 2 \sum_{i=1}^N \alpha_i \int k(x, z_i) dP(x) \\ &\quad + \int \int k(x, x') dP(x) dP(x') \\ &= \alpha^\top K_z \alpha - 2 \sum_{i=1}^N \alpha_i (z_i^\top \mathbb{E} x x^\top z_i + 2 \mathbb{E} x^\top z_i + 1) \\ &\quad + \text{Tr}(\mathbb{E} x x^\top \mathbb{E} x x^\top) + 2 \mathbb{E} x^\top \mathbb{E} x + 1. \end{aligned} \quad (14)$$

This results in (6).

VI. CONCLUSION

In this paper, we introduced the kernel mean embedding framework as a tool for solving generalized moment problems. We presented tractable constrained optimization formulations with the ambiguity sets described by RKHS distance as well as practical solution methods. Through theoretical analysis and numerical experiments, we demonstrate how the proposed method can characterize the worst-case risk under distributional ambiguity. Therefore, we view the kernel mean embedding as a promising tool for robust optimization and control under distributional ambiguity.

REFERENCES

- [1] N. N. Taleb, *The Black Swan: The Impact of the Highly Improbable*. Random house, 2007, vol. 2.
- [2] I. Popescu, "A Semidefinite Programming Approach to Optimal-Moment Bounds for Convex Classes of Distributions," *Mathematics of Operations Research*, vol. 30, no. 3, pp. 632–657, Aug. 2005.
- [3] M. Farina, L. Giulioni, and R. Scattolini, "Stochastic linear Model Predictive Control with chance constraints – A review," *Journal of Process Control*, vol. 44, pp. 53–67, Aug. 2016.
- [4] A. Sinha, H. Namkoong, and J. Duchi, "Certifying Some Distributional Robustness with Principled Adversarial Training," pp. 1–41, 2017.
- [5] K. Isii, "On sharpness of tchebycheff-type inequalities," *Annals of the Institute of Statistical Mathematics*, vol. 14, no. 1, pp. 185–197, Dec. 1962.
- [6] A. Shapiro, "On Duality Theory of Conic Linear Problems," in *Semi-Infinite Programming*, P. Pardalos, M. Á. Goberna, and M. A. López, Eds. Boston, MA: Springer US, 2001, vol. 57, pp. 135–165.
- [7] W. W. Rogosinski, "Moments of Non-Negative Mass," p. 28.

- [8] J. B. Lasserre, "Bounds on measures satisfying moment conditions," *The Annals of Applied Probability*, vol. 12, no. 3, pp. 1114–1137, 2002.
- [9] D. Bertsimas and J. Sethuraman, "Moment problems and semidefinite optimization," in *Handbook of Semidefinite Programming*. Springer, 2000, pp. 469–509.
- [10] D. Bertsimas and I. Popescu, "Optimal Inequalities in Probability Theory: A Convex Optimization Approach," *SIAM Journal on Optimization*, vol. 15, no. 3, pp. 780–804, Jan. 2005.
- [11] L. Vandenbergh, S. Boyd, and K. Comanor, "Generalized Chebyshev Bounds via Semidefinite Programming," *SIAM Review*, vol. 49, no. 1, pp. 52–64, Jan. 2007.
- [12] B. P. G. Van Parys, P. J. Goulart, and D. Kuhn, "Generalized Gauss inequalities via semidefinite programming," *Mathematical Programming*, vol. 156, no. 1-2, pp. 271–302, Mar. 2016.
- [13] E. Delage and Y. Ye, "Distributionally Robust Optimization Under Moment Uncertainty with Application to Data-Driven Problems," *Operations Research*, vol. 58, no. 3, pp. 595–612, June 2010.
- [14] E. Erdoğan and G. Iyengar, "Ambiguous chance constrained problems and robust optimization," *Mathematical Programming*, vol. 107, no. 1, pp. 37–61, June 2006.
- [15] P. Mohajerin Esfahani and D. Kuhn, "Data-driven distributionally robust optimization using the Wasserstein metric: Performance guarantees and tractable reformulations," *Mathematical Programming*, vol. 171, no. 1, pp. 115–166, Sept. 2018.
- [16] B. Van Parys, D. Kuhn, P. Goulart, and M. Morari, "Distributionally Robust Control of Constrained Stochastic Systems," *IEEE Transactions on Automatic Control*, pp. 1–1, 2015.
- [17] S. Zymler, D. Kuhn, and B. Rustem, "Distributionally robust joint chance constraints with second-order moment information," *Mathematical Programming*, vol. 137, no. 1-2, pp. 167–198, Feb. 2013.
- [18] D. Bertsimas, M. Sim, and M. Zhang, "Adaptive Distributionally Robust Optimization," *Management Science*, vol. 65, no. 2, pp. 604–618, May 2018.
- [19] A. Ben-Tal, D. den Hertog, A. De Waegenaere, B. Melenberg, and G. Rennen, "Robust Solutions of Optimization Problems Affected by Uncertain Probabilities," *Management Science*, vol. 59, no. 2, pp. 341–357, Feb. 2013.
- [20] D. Bertsimas, N. Kallus, and V. Gupta, *Data-Driven Robust Optimization*. Springer Berlin Heidelberg, 2017, publication Title: Mathematical Programming.
- [21] A. Berlinet and C. Thomas-Agnan, *Reproducing Kernel Hilbert Spaces in Probability and Statistics*. Springer Science & Business Media, 2011.
- [22] A. Smola, A. Gretton, L. Song, and B. Schölkopf, "A hilbert space embedding for distributions," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 4754 LNAI, pp. 13–31, 2007.
- [23] B. K. Sriperumbudur, K. Fukumizu, and G. R. G. Lanckriet, "Universality, Characteristic Kernels and RKHS Embedding of Measures," *Journal of Machine Learning Research*, vol. 12, no. Jul, pp. 2389–2410, 2011.
- [24] A. Gretton, K. M. Borgwardt, M. J. Rasch, B. Schölkopf, and A. Smola, "A kernel two-sample test," *Journal of Machine Learning Research*, vol. 13, no. Mar, pp. 723–773, 2012.
- [25] J.-J. Zhu, B. Schölkopf, and M. Diehl, "A Kernel Mean Embedding Approach to Reducing Conservativeness in Stochastic Programming and Control," *arXiv preprint arXiv:2001.10398*, 2020.
- [26] M. Kanagawa and K. Fukumizu, "Recovering Distributions from Gaussian RKHS Embeddings," p. 9.
- [27] F. Bach, S. Lacoste-Julien, and G. Obozinski, "On the Equivalence between Herding and Conditional Gradient Algorithms," *arXiv:1203.4523 [cs, math, stat]*, Sept. 2012.
- [28] J. A. E. Andersson, J. Gillis, G. Horn, J. B. Rawlings, and M. Diehl, "CasADi: A software framework for nonlinear optimization and optimal control," *Mathematical Programming Computation*, vol. 11, no. 1, pp. 1–36, Mar. 2019.
- [29] G. Calafiore and M. Campi, "The scenario approach to robust control design," *IEEE Transactions on Automatic Control*, vol. 51, no. 5, pp. 742–753, May 2006, conference Name: IEEE Transactions on Automatic Control.
- [30] J.-J. Zhu, K. Muandet, M. Diehl, and B. Schölkopf, "A New Distribution-Free Concept for Representing, Comparing, and Propagating Uncertainty in Dynamical Systems with Kernel Probabilistic Programming," *arXiv:1911.11082 [cs, eess, math, stat]*, Nov. 2019.
- [31] A. Mesbah, "Stochastic Model Predictive Control: An Overview and Perspectives for Future Research," *IEEE Control Systems Magazine*, vol. 36, no. 6, pp. 30–44, Dec. 2016, conference Name: IEEE Control Systems Magazine.
- [32] K. R. Parthasarathy, *Probability Measures on Metric Spaces*. Academic Press, July 2014.
- [33] A. Wachter and L. T. Biegler, "On the implementation of a primal–dual interior point filter line search algorithm for large-scale nonlinear programming, mathematical programming," *Math. Program*, vol. 106, no. 1.
- [34] F. Pedregosa, G. Varoquaux, A. Gramfort, V. Michel, B. Thirion, O. Grisel, M. Blondel, P. Prettenhofer, R. Weiss, and V. Dubourg, "Scikit-learn: Machine learning in Python," *Journal of machine learning research*, vol. 12, no. Oct, pp. 2825–2830, 2011.

VII. APPENDIX: DETAILED EXPERIMENTAL SETUP

All the experiments are implemented using Python with optimization solver IPOPT [33]. The stochastic control experiment used the CasADi library [28]. We used the Gaussian kernel $k(x, y) = \exp\left(-\frac{\|x-y\|_2^2}{2\sigma^2}\right)$ with bandwidth σ set to be $\text{median}(\{\|x_i - x_j\|_2/\sqrt{2} \mid i, j = 1, \dots, N\})$. This is a common practice known as the median heuristic [24]. We also used sum-of-kernel practice to combine different widths to form a new kernel. Our specific implementation of kernel computation is adapted from [34].

A. Setup for Sec. IV-A

For the simulation to produce Fig. 2, we generate $M = 100$ data samples $\{x_i\}_{i=1}^M \stackrel{i.i.d.}{\sim} N(0, 1)$ (distribution unknown to the optimizer) and set $c = 2.5$. To form the new expansion points $\{z_i\}_{i=1}^N$ in (5), we first generate a set of $L = 100$ grid points on $\{y_i\}_{i=1}^L$ on $[0, 5]$, then we add the original data samples $\{x_i\}_{i=1}^M$ to the grid points to form the new expansion points. That is, the set of new expansion points $\{z_i\}_{i=1}^N$ consists of both the grid points and the original expansion points $\{z_i\}_{i=1}^N = \{y_i\}_{i=1}^L \cup \{x_i\}_{i=1}^M$, $N = 200$ in total.

For the experiment in Fig. 3, we add $L = 10$ new expansion points $\{y_i\}_{i=1}^L$ to the other side of $c = 2.5$ (by simply gridding the interval $[c, c + 1]$). Together with the original expansion points $\{x_i\}_{i=1}^M$, they form the set of expansion points $\{z_i\}_{i=1}^N$ for the new embedding $\sum_{i=1}^N \alpha_i \phi(z_i)$.

B. Setup for Sec. IV-B

For the scenario MPC simulation, we sample the i.i.d. uncertainty realizations $\{s_1, \dots, s_n\} \sim N(m, \Sigma)$, where $m = [0.5 \ 0]^T$, $\Sigma = \begin{bmatrix} 0.01^2 & 0 \\ 0 & 0.1^2 \end{bmatrix}$. Then, the scenarios are propagated through the nonlinear dynamics. The continuous-time dynamics is transcribed with numerical integration. The total time horizon is 1.0s and we consider 10 control steps in this experiment.